COMMUNITIES @ RISK
Targeted Digital Threats Against Civil Society
November 11, 2014
https://targetedthreats.net/
Acknowledgments

*Communities @ Risk: Targeted Digital Threats Against Civil Society* is a product of a collective effort conducted over a four year period.

The research and writing of this report was undertaken by Masashi Crete-Nishihata, Jakub Dalek, Ronald Deibert, Seth Hardy, Katharine Kleemola, Sarah McKune, Irene Poetranto, John Scott-Railton, Adam Senft, Byron Sonne, and Greg Wiseman.

In addition, we would like to thank Christopher Davis, Brandon Dixon, Phillipa Gill, Claudio Guarnieri, Bill Marczak, Morgan Marquis-Boire, Justin Wong, and Nart Villeneuve for their input and expertise, Jane Gowan for the report layout and cover design, and Andrew Hilts for the website design.

We thank VirusTotal for providing us with an intelligence subscription and to the developers of free information security tools, including Cuckoo Sandbox, URL Query, and PassiveTotal.

The Citizen Lab’s research into targeted digital threats is supported by a grant from the John D. and Catherine T. MacArthur Foundation.

We would especially like to thank the 10 civil society organizations that participated in the project and made this study possible.
[Technology is] this funny thing where it’s a life line, and then...maybe your ticket to jail.”
–Tibet Group 1

A civil society organization that works on China-related social justice issues receives an email from a program officer at one of its funders. She suggests that they review details of an upcoming meeting.

A Tibetan webmaster receives an email continuing a thread with several collaborators about developing a poster for an upcoming campaign.

These messages look like the mundane email traffic of everyday work. Most of us would not think twice about opening them. However, these two emails, and many more like them, are carefully crafted digital attacks.

These attackers had artfully composed the messages using private information that only the recipient and that person’s group of contacts would know, suggesting that at some point someone else in their organization or community had already likely been compromised.

The emails contain file attachments implanted with malware that exploits vulnerabilities in programs like Adobe’s PDF Reader and Microsoft Office, enabling distant attackers access to computers at the offices of the civil society organization, or the living room of the webmaster. The attackers then turn the computer into an ideal spying device: they take files, record keystrokes, and turn on the webcam and microphone. All of this monitoring begins with a seemingly inconsequential behavior: double clicking a benign-looking attachment.

These are not isolated incidents. The emails are real examples of an epidemic of targeted malware that is becoming a reality for human rights groups, journalists, and activists under threat from determined actors. Targeted attacks like these are organized in campaigns that persistently attempt to compromise systems and gain access to networks over long periods of time, while remaining undetected. They are custom-designed for specific targets and are conducted by highly motivated attackers. The objective is to extract information from compromised systems and monitor user activity.

*Attacks like these are best understood as a form of espionage.*
Abstract

Communities @ Risk: Targeted Digital Threats Against Civil Society is the culminating report of a multi-year, multi-group study on targeted digital threats. We define targeted digital threats as persistent attempts to compromise and infiltrate the networked devices and infrastructure of specific individuals, groups, organizations, and communities.

The study involved 10 civil society organizations (CSOs) that shared suspicious emails, network traffic, and other data with Citizen Lab researchers who conducted detailed, confidential analysis over a four year period. Citizen Lab researchers also paid site visits to the participating CSOs and interviewed them about their perceptions and the impacts of the digital attacks on their operations. Data from both the technical and contextual aspects of the research informs the report’s Key Findings:

- In the digital realm, CSOs face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.
- Counterintuitively, technical sophistication of malware used in these attacks is low, but the level of social engineering employed is high.
- Digital attacks against CSOs are persistent, adapting to targets in order to maintain access over time and across platforms.
- Targeted digital threats undermine CSOs’ core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety.
- Targeted digital threats extend the “reach” of the state (or other threat actors) beyond borders and into “safe havens.”

Remediation of the problem will require major efforts among several stakeholders, from the foundations that fund civil society, to the private sector, to governments.
EXECUTIVE SUMMARY

Introduction

The Internet and other digital technologies are a transformative, disruptive force throughout society, impacting governments, businesses, and CSOs. For the latter, social mobilization, advocacy, policy engagement, and internal operations and management are now deeply intertwined with the same mass market communications platforms most of us use daily, from instant messaging applications to Twitter. CSOs manage, often with few resources, to accomplish remarkable effects thanks to these technologies, leading some to predict a worldwide flourishing of rights, democracy, and individual empowerment.

While the positive outcomes for free expression and access to information are evident, we are only now beginning to get a handle on the new risks that digital technologies introduce. Among those risks, arguably the most well reported on and widely discussed have been those related to documents leaked to the press by Edward Snowden (See “The Snowden Disclosures”). The documents show in detail how the US National Security Agency (NSA) and its “Five Eyes” allies have been able, with considerable effort and resources, to exploit the Internet and other digital technologies as tools of mass surveillance for national security and foreign policy aims. Separate from the Snowden leaks, there have also been a growing number of case studies and reports of journalists or human rights defenders being targeted by governments with malicious software (malware) or even commercial spyware. Through this reporting, a more nuanced understanding of the risks associated with the Internet and digital technologies is developing among CSOs and the foundations that fund them. Secure tools, trainings, and other forms of support are a burgeoning field. Individuals working in areas at risk are beginning to understand that those very same technologies that provide liberating means of communication and organization can also be sources of insecurity. However, much remains to be done, particularly in the area of systematic, evidence-based research of targeted digital threats.
For the past 10 years, Citizen Lab has researched the use and impact of digital technologies within civil society, focusing in particular on their unintended consequences as potential sources of insecurity or threat. Our aim is to apply a systematic, mixed methods approach to this research, combining technical and social sciences with field research. We also consider principles of international human rights law as an important touchstone for our research, for at least two reasons. First, some CSOs and individuals appear to be targeted as a direct result of their human rights-related investigations and advocacy. Second, the use of digital attacks undermine such actors’ internationally-recognized human rights, including freedom of expression and right to privacy.

In 2009, we were part of a team that published the first open academic study documenting a major global cyber espionage campaign involving compromised computers in dozens of high-value targets around the world. The resulting report, entitled *Tracking GhostNet: Investigating a Cyber Espionage Network*, was followed up a year later with *Shadows in the Cloud: Investigating Cyber Espionage 2.0*. Both were organized as case studies starting with Tibetan groups as study subjects. Both generated unexpected and quite sensational findings concerning a range of other governments and businesses whose computers we found compromised by the same groups targeting our Tibetan study subjects. We hypothesized that these types of targeted digital attacks were likely not uncommon, and were affecting more than the few organizations we were studying.

Following these foundational case studies, we embarked on a plan to develop a multi-year, multi-group study on targeted digital threats. Our aim was to apply principles from comparative methods in other academic disciplines to the study of targeted digital threats against CSOs. We define “targeted digital threats” as persistent attempts to compromise and infiltrate the networked devices and infrastructure of specific individuals, groups, organizations and communities. Targeted digital threats are not widespread compromises of networked devices that affect

Civil society is feeling the heat around targeted attacks and surveillance and I think it’s affecting the public sphere and our ability to feel comfortable communicating in what used to be understood as a free and open medium.”

—Rights Group 2

[At the time of the 2008 Tibetan uprising] you could make all the noise you want in DC or in Seattle or in Paris, but when it came to actual Tibetans organizing on the ground inside...there was nothing...they had no knowledge, no capability... We saw...a generation of activists taken out because of the inability to support them safely...”

—Tibet Group 1
individuals or groups in an undifferentiated fashion. They are not the typical spam or financial fraud that one may encounter more or less randomly across the Internet—the equivalent of a digital “flu.” Rather, they are focused on specific targets, they persist over a period of time, and they are motivated by political objectives.

Outside of this study, Citizen Lab and its collaborators have engaged in parallel research projects on targeted digital threats against CSOs. These projects include several pathbreaking reports on commercial spyware (see “The Market for Lawful Intercept”) and targeted digital threats in and around the Syrian armed conflict (see “Syria and Targeted Digital Threats”). While we report primarily on the findings of the formal study in this document, lessons learned from those other projects inform our analysis. Together this body of work moves us towards mapping the targeted digital threat tactics and approaches of governments and other actors around the world and documents how these capabilities are used against CSOs.

Reflecting on the sum total of all of our various research projects on targeted digital threats, we observe that there are at least three distinct models that characterize the capacities and tactics of actors carrying out targeted digital attacks:

1. NATIONAL IN-HOUSE DEVELOPMENT AND OPERATIONS (APT)

In the first model, threat actors have capabilities and resources to develop their own customized malware and conduct wide scale operations. This level of capacity requires significant time and investment to develop, and is generally restricted to well-resourced actors like states. However, these kinds of operations can also be achieved through “cyber militia” groups that receive direct or tacit government support. Within the security industry, this approach is frequently referred to as the “Advanced Persistent Threat” (APT). At the high end of this model is the NSA’s Tailored Access Operations (TAO) group that reportedly has a large and highly trained staff with significant budgets for developing and implementing targeted digital attacks. While not as advanced as the NSA, China-based threat actors have been developing custom malware and carrying out extensive campaigns for the last 15 years. The attacks we document in this study are prime examples of the work of threat actors within this model.
EXECUTIVE SUMMARY

CHINA AND TARGETED DIGITAL THREATS

Public reports on malware campaigns originating from or related to China go back over a decade. In the past five years, the number of reports on these activities has exploded with high profile compromises documented against governments around the world and a large number of industries, including companies like Google, RSA, and Boeing. The United States has been particularly vocal on the threat these attacks pose to national security and commerce. The Commission on the Theft of American Intellectual Property claims intellectual property theft against the US is primarily orchestrated by China through cyber espionage and accounts for losses of up to 300 billion dollars a year. General Keith Alexander, former Director of the National Security Agency and Commander of United States Cyber Command, has called the theft of US intellectual property through cyber espionage the "greatest transfer of wealth in history."

While governments and businesses are often highlighted as victims, malware attacks against ethnic minority groups in China including Tibetans and Uighurs, and religious groups such as Falun Gong, go back to at least 2002, and possibly earlier.

Claims of attribution surrounding these attacks abound, with some analysts making direct connections to the Chinese government and military, and others drawing links to the Chinese hacker underground or universities. Conclusive proof that a targeted attack is the work of a state-sponsored attacker is often elusive. Regardless of how connected the Chinese government is to these attack campaigns, the years of documentation around these operations show that there are well-resourced and persistent threat actors originating from China.

2. RE-PURPOSED CRIMEWARE

The second model is best represented by campaigns conducted by parties involved in the Syrian civil war. These attacks primarily rely on basic Remote Access Trojans (RATs) that are circulated among hobbyists and criminals, but which we have found are deployed for political reasons and—in the case of Syria—in the context of armed conflict. This approach blurs the worlds of cybercrime and espionage, and is forged out of necessity and, to some degree, a kind of “do-it-yourself” mentality. These kinds of operations can be conducted by state actors and / or groups that may be directly sponsored, encouraged, or tacitly accepted by states. Early China-related operations followed this approach, but over time have become more organized and mature. A similar type of maturation process could occur in other contexts.
EXECUTIVE SUMMARY

SYRIA AND TARGETED DIGITAL THREATS

In January 2012, it was becoming clear to Syrian opposition groups that something was going on with their computers. Suspicious messages and social media postings directed them to download documents and programs purporting to contain useful information. Troublingly, some of the files were sent from the accounts of individuals detained by the regime. Early analysis by the opposition led to the conclusion that they were being targeted by malware attacks. Researchers from a number of groups, including Citizen Lab, began investigating and were eventually able to develop compelling evidence linking the attacks to the Assad regime.

Our research on Syria consists both of close work with targeted groups to identify and track malware campaigns, and the use of signatures and other techniques to identify malware in the wild. Taken together, these methods provide a useful but necessarily incomplete picture of the targeting, as attackers regularly refine their techniques, thus reducing the likelihood of being observed.

The lessons we draw from the Syrian case align with those from the formal study. Namely, attackers exploit the pervasive, constant use of mass market communications tools by the opposition, just as do threat actors that target participants in our study. Additionally, we consistently observe sophisticated social engineering and well-informed targeting, rather than a high degree of technical sophistication.

3. COMMERCIAL SPYWARE

The third approach relies on the procurement of commercial “lawful intercept” products and services that provide actors with turnkey surveillance solutions. Companies like FinFisher and Hacking Team are actively marketing surveillance suites to governments, law enforcement, and intelligence agencies. Actors that do not have an in-house capacity to develop and operate targeted digital attacks can now buy these capabilities directly from these companies. The high cost of these products and the claim by vendors that sales are restricted to government clients make this primarily a state-centric route, although it is conceivable that non-state actors could be clients too. Citizen Lab research has identified troubling evidence that these products and services are ending up in the hands of regimes that are using these powerful tools to actively target civil society.
THE MARKET FOR LAWFUL INTERCEPT

In parallel to work on targeted civil society groups, Citizen Lab researchers have conducted extensive investigation into the global proliferation of so-called “lawful interception” malware sold exclusively to governments. These tools allow governmental purchasers the ability to gain remote entry into, and monitor the computers and phones of their targets.

Research published by Citizen Lab as well as other investigative groups has demonstrated that some governments and security services abuse these tools by hacking political opponents and human rights groups, both domestically and in other jurisdictions. Despite the potential for abuse, the market for these tools is largely unregulated, which has helped the governmental customer base grow, and likely led to substantial profits for developers. Our scanning has enabled us to develop global lists of suspected government users of this technology. Meanwhile, our close work with victims in the United States, the United Kingdom, the United Arab Emirates, and Bahrain has helped us document the abusive use of these tools against human rights defenders, journalists, and civil society groups.

Similar to the threat actors featured in this study, the attack tools require effective social engineering campaigns to gain entry to targeted organizations. This requirement also results in the creation and transmission of links and files that can be collected and analyzed by researchers. However, we have seen commercial tools that provide more advanced network injection functionality. While these tools can be technically identified, they are challenging to systematically detect.

The findings in this report primarily reflect our research on campaigns that have followed the first model—specifically how China-based threat actors are targeting CSOs. Readers should be aware, therefore, of the limitations of our research. We note that our research into targeted threats within the formal study is largely “China facing.” Most of the participating CSOs have missions dedicated to human rights in the context of China, with Tibetan Groups representing the lion’s share of the study. Our technical data in particular is based primarily on data shared with us by Tibetan organizations, given our existing contacts in the community and prior research for the Tracking GhostNet and Shadows in the Cloud reports, and is thus skewed toward consideration of attacks against Tibetans. The findings reflect, in other words, one model of threat actor: the model emanating from China (which may or may not be state-linked). While these considerations are specific to the Groups (attackers and CSOs) we analyzed in the four-year formal study, we believe the findings are generalizable to other contexts.
The report combines two major sections:

1. The Executive Summary (which you are reading now) provides detail on how the study was organized and why we feel it is important to read, a high-level overview of the key findings of the research, and considerations about next steps for several stakeholder communities in responding to targeted digital threats.

2. The Extended Analysis explains our methodology, and examines the detailed data we gathered during the study period. It is the evidentiary basis for the claims we make in the Executive Summary, and will likely be of interest to a more specialized audience (although we hope everyone will read it).

STUDY BY THE NUMBERS

- Participating Groups: 10 CSOs
- Study Duration: 2010-2014
- Number of Emails Submitted: 817
- Malicious Payloads Identified: 2,814
- CVEs Identified: 24
- 0-days Identified: 1
- Malware Families Identified: 44

The entire report is written in language that assumes little or no prior knowledge of malware, computer network attacks, or other technical details. We have attempted to define key terms and concepts along the way, and for those requiring some help navigating technical terms, we have included a detailed glossary.

Accompanying the Executive Summary and the Extended Analysis, we are publishing other resources for the research community, including indicators of compromise, and a guide for further reading. Links to all of the documents can be found at targetedthreats.net.
Today, many are aware that individuals, communities, and CSOs face digital risks. It is common to hear warnings not to open unsolicited email attachments or to log onto untrusted WiFi networks. The number and frequency of reports about cyber espionage campaigns or major data breaches contributes to this growing awareness. However, documented evidence of the precise nature of digital risks facing CSOs remains scattered and mostly anecdotal. The situation might be likened to growing awareness around the health impacts of smoking prior to the publication of formal epidemiological studies undertaken by the Royal College of Physicians of London in 1962. We intuitively sense that there is a problem, common sense supports it, but there is a lack of empirical evidence based on formal, systematic research.

**FORMAL, COMPARATIVE ANALYSIS**

This report is the first of its kind of which we are aware to take a formal, systematic, and comparative approach to the study of targeted digital threats against civil society. The genesis of the project was our desire to build upon the focused case studies undertaken in *Tracking Ghostnet* and *Shadows in the Cloud*. While those studies involved technical forensics, interviews, and field research with the consent of several Tibet-related organizations, we felt a follow-on could be broader in scope, more rigorous, and self-consciously styled on formal comparative research methods common to the social and natural sciences. We aimed to better formalize the study of targeted digital threats, and begin making the topic a legitimate area of inquiry for academic research. At the same time, we were aware of a growing body of research in the private sector and within government on targeted digital threats, most of which is focused on attacks against industry or government agencies. Attacks on CSOs, on the other hand, have gone under-reported despite the fact that they are frequently included in the very same major cyber espionage campaigns investigated by those groups. We sought to rectify this imbalance.
KEY RESEARCH QUESTIONS

- Are civil society organizations selectively targeted for digital compromise? What commonalities exist across campaigns against civil society and entities in other sectors?
- What are the origins of targeted attacks against civil society organizations? Is attribution feasible? What, if any, conclusions regarding attribution can be drawn from the evidence obtained?
- What methods are employed to compromise civil society organizations? Have those methods changed over time?
- How technically advanced is malware used against civil society organizations, and how does it operate?
- How sophisticated are the social engineering techniques used against civil society actors?
- What level of knowledge or awareness do attackers exhibit concerning their targets?
- How do civil society organizations perceive and respond to targeted digital threats?
- What is the impact of digital threats on civil society groups?
- How can civil society best protect itself?
- What are the next steps for future research?

Our research plan had several components: First, we aimed to enrol a range of study groups to participate in the project over a significant period of time. Our feeling was that a manageable but larger sample size would give us a better indication of the range of digital threats. Doing so required a fairly substantial investment in outreach and engagement, in part to explain the framework of the study to interested groups, but also to assuage any concerns they might have about the risks of participating in the study. We needed to gain their trust. Our engagement included a public call on our website, email announcements, and outreach to individual organizations.

We were able to enroll 10 CSOs from a variety of sectors, eight of which are groups concentrated around rights issues related to China and Tibet. The concentration is the result of both our previous connections to some of the groups in prior research, and the fact that these communities have been targeted by digital attacks for at least 10 years. Many have a high level of awareness of digital threats, and also have a strong interest in being included in and supporting the aims of our study. To help control
CEMMUNITIES @ RISK
EXECUTIVE SUMMARY

(partially) for selection bias, we also enrolled two large human rights organizations focused on issues in multiple countries. (In subsequent phases of the project we expect to broaden our sample groups in size and focus.) We worked with the groups over a four-year period, observing their behavior, analyzing the malware samples we received from them, and interviewing them concerning their perceptions, practices, and common concerns. To protect the participants’ confidentiality, we refer to them throughout the report in generic terms (e.g., Tibet Group 2, China Group 1, Rights Group 2).

FULL ETHICAL REVIEW

The second component of our research plan was that we applied for and underwent a full ethical review of the study, and received approval from the University of Toronto’s research ethics office for our plan of research. Going through the ethical review was important for the following reasons.

First, much of the information shared with us is of a highly sensitive and confidential nature. It may reference detailed internal and strategic matters, or personally identifiable information that may put individuals at risk. Moreover, the fact of actual or potential compromise is itself a sensitive topic. Groups may be concerned that disclosing information about an attack could reveal vulnerabilities and encourage further intrusions. They may also fear that disclosure could subject them to embarrassment with communities served, funders, or the public at large. (On the other hand, some groups may see targeting as a sign that their work is significant enough to warrant such attention.) It is therefore essential to ensure that the rights of participants in the study are protected, and that they retain control over the use of confidential information and data.

Second, research on targeted threats—particularly when it involves technical research—may lead to unexpected results that raise ethical dilemmas. Technical investigations into malware may uncover command-and-control interfaces used by attackers, or repositories of sensitive data culled from targets. Researchers may even find themselves with the ability to issue commands directly to compromised computers. Research might also lead back to those suspected of orchestrating the attacks, or to previously unidentified targets, presenting questions of notification to law enforcement or victims, and whether to publicly disclose the suspected culprit(s). A pre-existing framework to guide an appropriate response is beneficial when encountering such circumstances.

The research protocol we submitted to the University of Toronto Office of Research
Ethics includes sections on conflicts of interest, research rationale and methods, participants, recruitment, possible risks and benefits, the consent process, and confidentiality. Additionally, Citizen Lab enters into a formal written consent agreement including confidentiality provisions with each participant, follows up with an oral explanation of the parameters of the study, and provides participants an opportunity to ask questions and discuss details before enrolling. Moving forward, we intend on further engaging the ethical questions around this type of research as a topic of study itself.

MIXED METHODS APPROACH

One of the distinguishing features of the report is the combination of methods employed to undertake the research. Citizen Lab has employed this mixed methods approach for several years, and it is particularly well suited to the challenges of our study.

Technical analysis

At the core of the analysis is the technical data we collected from the groups, including malware samples and network traffic. We analyzed malware samples using static and dynamic analysis tools as well as manual analysis to extract information on exploits, malware functionality, malware family, command-and-control infrastructure, and other properties of the malware code. By examining patterns in malware families, development cycles, shared infrastructure, and social engineering tactics, we identified relationships between attacks and, where possible, linked them to known malware campaigns and threat actors.

Field research, site visits, and interviews

We interviewed the study subjects in a semi-structured process. These sessions were, where practical, recorded, transcribed, and analyzed by researchers. We undertook site visits to all but one of the study groups to get a better sense of their on-the-ground experience. The input of the study groups gave us unique insight into their perceptions of targeted digital threats, their capacity to deal with them effectively, and the impact these kinds of threats can have on their daily operations. We identified emergent themes from the interviews that provide insights into how CSOs perceive targeted digital threats. A full overview of these themes is available in the Extended Analysis.

Contextual analysis

In addition to technical analysis and interviews, we conducted legal, social, and political analysis, including research of contextual details and social engineering particular to the attacks—such as timing, language employed, topic flagged in the email text, relevant
political climate, etc. This analysis relies on the background information provided by participating organizations, open source intelligence, and the expertise of our team in international law and human rights, and regional and country-specific history and politics.

We also engaged with civil society, including human rights groups and digital defenders reporting experiences of targeted digital attacks; exchanged information with individuals in the security community (including our technical advisory board); and liaised with other groups undertaking similar research.

OPEN DATA, OPEN METHODS, OPEN TOOLS

We have attempted to share as much as possible with the wider research community the data, the tools, and the methods we gathered, used, and developed during the course of this study. Accompanying the release of this report are datasets we are making openly available, including YARA signatures of malware families, MD5 hashes of samples, and lists of command-and-control servers. The intention of this data release is to help security researchers and network administrators identify and defend against the threats analyzed in our dataset. Additionally, we developed the Targeted Threat Index, a metric to characterize and quantify the social engineering and technical sophistication of targeted threats and assess their relative risk. We hope this metric will be adopted by other researchers and applied to other datasets. During the project, we developed a web-based malware repository “The SHARK” for managing our dataset. Although many similar platforms exist and are used by the security industry, most of them that we evaluated are either proprietary and / or were not suited to our specific requirements. We are in the process of planning a new version of The SHARK that will encompass what we have learned from developing our internal system, and it will be released open source. By openly publishing datasets, methods, and tools we hope to encourage and assist other researchers who may be interested in targeted digital threats and begin the process of building on accumulated knowledge.
Key Findings

We have identified several important findings regarding targeted digital threats based on data obtained through the formal study, our ad-hoc research, and our own long-term experience. These findings inform our recommendations to stakeholders. (An additional list of specific, more detailed findings is included in the Extended Analysis.)

1. In the digital realm, CSOs face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.

In recent years, a growing number of high profile security industry reports have cast a spotlight on targeted digital attacks against Fortune 500 companies and government agencies. These reports have received broad press coverage, triggered major public policy debates, and brought about government action. One of the main findings from the technical investigations is that some of the groups participating in our study are targeted by the same threat actors using the same techniques, tools, and infrastructure as those highlighted in industry reports. The inset “Campaigns Targeting CSOs and Government/Industry” provides a snapshot of the connections.
EXECUTIVE SUMMARY

CAMPAIGNS TARGETING CSOs AND GOVERNMENT/INDUSTRY

Through cluster analysis that groups attacks by common malware, development patterns, shared infrastructure, social engineering tactics, and other indicators, we have identified ten distinct attack clusters of which four have clear connections to campaigns that target government and private industry. These findings echo previous reports going back to at least 2008 (e.g. Tracking GhostNet) that have also shown threat actors targeting governments, private industry, and CSOs.

- **APT1 (Reported by Mandiant)**
  - Targeted 141 organizations from 20 industry sectors
  - Targeted Tibet Group 1, compromised Rights Group 1

- **DTL Campaigns (Reported by FireEye)**
  - Targeted government and 11 industry sectors
  - Targeted Tibet Groups 1, 2, 3, and 4

- **NetTraveler (Reported by Kaspersky)**
  - Targeted 350 organizations from NGOs, government, and industry
  - Known to target Tibetan and Uyghur CSOs
  - Targeted Tibet Groups 1, 2, 3, 4, and 5; China Group 3

- **PlugX Campaigns (Reported by TrendMicro, AlienVault)**
  - Targeted companies in Asia and US, and Tibetan CSOs
  - Targeted China Groups 1 and 2; Tibet Groups 1 and 2

For example, we found evidence that the prolific threat actor known as “APT1”—also referred to as “Comment Crew” or “Byzantine Candor,” which is known to have compromised numerous government entities and Fortune 500 companies—targeted Tibet Group 1 and significantly compromised Rights Group 1. The malware we examined incorporated much of the same code and used one of the same command-and-control servers as the APT1 attacks previously documented by security firm Mandiant.

Evidence of this type of cross-targeting is not coincidental. It shows that the actors behind campaigns like APT1 and others like them, place the same strategic value on penetrat-
ing CSOs as they do on companies and governments. Yet while digital intrusions against private sector or government actors have resulted in high-profile media coverage, criminal investigations, and increasingly forceful national policy responses, few avenues for escalation exist when those same intrusions are directed against CSOs. Governments that cooperate closely with, and speak loudly on behalf of industry actors concerning intellectual property theft, have not taken the same approach to protection of domestic civil society, which involves the far thornier issues of right to privacy and freedom of expression.

For example, while the US government has taken a strong political stance on Chinese cyber espionage against US companies—even filing a criminal indictment against members of the Chinese military for alleged hacking—we have not seen the US Attorney General demand an end to the persistent attacks of US-based NGOs that work on China-related human rights issues, despite the threats to life and liberty that could result. The political capital such a move would require, particularly in the aftermath of the Snowden disclosures, is perhaps considered too great by many governments; even those with active Internet freedom policy agendas have not fully addressed the question of cyber espionage against civil society.

Meanwhile, CSOs are hard-pressed to resolve matters themselves. CSOs reported to us an understanding of some of the digital risks they face, but in many cases noted a lack of capacity and resources to dedicate to the problem. With rare exceptions, they typically do not have the funding to hire technical security experts, or the opportunity to engage with government on digital defence or overall policy in a manner that protects their security and confidentiality needs. Some barely have dedicated IT staff, let alone staff that can handle APTs. Even if CSOs are able to undertake basic remediation after an attack, they are unlikely to be able to conduct the technical investigation and training necessary to fully understand and mitigate future threats.

If digital attacks of CSOs continue to spread unchecked, we risk the gradual erosion of many of the core institutions of a vibrant democratic society: NGOs, foundations, independent journalists, activists, and others—all of which have experienced and continue to experience targeted threats. The shared experience of targeted digital threats among civil society, the private sector, and government could lend itself to sharing of threat information and coordination of prevention and defense. Moreover, all three sectors stand to benefit from a comprehensive financially- and politically-supported bulwark against targeted digital threats; given the diversity of attacker targets, zero tolerance for and investigation of today’s attacks against CSOs may help prevent tomorrow’s attacks against a major company or government institution.
2. Counterintuitively, technical sophistication of malware used in these attacks is low, but the level of social engineering employed is high.

Targeted attacks against CSOs are rarely examples of ‘technical wizardry.’ Throughout the course of our study, we found that attacks frequently employed technically unsophisticated malware (relative, that is, to malware used by financially motivated cyber criminals and commercial lawful intrusion kits), some of which have been widely reported on for years. (Our Targeted Threat Index provides a detailed analysis of how we measure and rank sophistication.) Similarly, the majority of exploits we observed are for vulnerabilities that have been patched for long periods of time. In four years of documenting attacks using over 22 different exploits (CVEs) we observed only one zero-day exploit, suggesting that attackers targeting CSOs rarely see the necessity of using zero-days against what could be considered “soft targets.” This is not to suggest, however, that digital threats against CSOs never utilize advanced malware or zero-day exploits. We have encountered more technically sophisticated malware outside of the study, and in particular in our research of the commercial spyware used against CSOs.

Still, attackers appear to employ malware that is only as technically advanced as it needs to be to generate results, investing fewer resources to rely on known exploits so long as their targets remain susceptible to them for behavioral reasons. This approach works because key factors determining whether a compromise occurs are typically behavioral rather than technical in nature: whether the user triggers the exploit by choosing to open a malicious file or click on a malicious link; and whether the user has kept software fully up-to-date with all security patches that would render known exploits ineffective, which requires current licensing of the software (not possible for pirated copies sometimes utilized by under-resourced CSOs and activists). Once the compromise occurs, basic malware is no less dangerous than more advanced malware—even unsophisticated exploits can permit installation of RATs providing the ability to search for and exfiltrate files and contacts, activate a device’s video and audio recording, and log keystrokes.

At the same time, congruent with a lack of emphasis on technical sophistication, we find greater sophistication around the social engineering employed in attacks against CSOs. Social engineering is an attacker’s method of crafting the delivery vector for the malware—typically

“We just have never had the time to do any forensics on what we assume are like denial of service [attacks]...the load on the server starts to rapidly increase, and there are several IPs that are very suspicious and the only thing that we can do is mitigate, fix, and just move on.” — Rights Group 2
an email—in a manner designed to entice recipients to open the infected payload. Attackers often “spoo"f” the sender identity to appear as someone the target already knows and trusts; reference timely and target-specific issues and events; repurpose real content taken from other sources of interest to the target; or attempt to exploit the emotions of the target by addressing sensitive, provocative, or inflammatory subjects. Good social engineering thus requires some knowledge of a target’s contacts, areas of interest, and current priorities or activities. It is likely that attackers conduct some form of preliminary reconnaissance or otherwise “study up” on their targets to develop their social engineering, perhaps drawing on social media and other open source information, or leveraging information or credentials gleaned from existing access to the systems of others within the target’s circle of trust (what might be called “collateral compromise”). Thus attackers appear to invest primarily in knowing their targets, rather than creating or purchasing advanced malware.

The importance of social engineering relative to technical sophistication raises two major issues to consider in addressing targeted digital threats. First, on the positive side, our findings suggest that in many instances behavioral modifications and sensitivity to commonly relied-upon social engineering techniques may reduce the susceptibility of CSOs to targeted attacks. User education and awareness campaigns within communities at risk may help CSOs and others contend with evolving threats and adaptive techniques, especially if known risky behaviors (e.g. opening attachments or clicking on links from unverified sources) are widely communicated and understood.

Second, significant negative impacts flow from attackers’ reliance on social engineering that require a systemic response. Constant use of socially engineered emails as “bait” creates an environment in which it is increasingly difficult to authenticate genuine content and digital trust is eroded. At the same time, for many CSOs, responsiveness to digital communications and use of digital platforms are essential for the conduct of their work. For example, a malicious email that appears to be from an important sender, such as a funder, will likely be opened if that funder has not agreed upon secure means of contact with the CSO in advance. Coordinated, standardized measures for encryption and authentication among civil society actors and those entities with whom they are in regular contact (e.g., funders, journalists, and government officials) should be seen as a critical priority (see the “Next Steps” section below for elaboration).
3. Digital attacks against CSOs are persistent, adapting to targets in order to maintain access over time and across platforms.

The attacks against CSOs that we analyzed in our formal study, and that we have observed in our other research projects, are persistent and evolve in response to defences or changes in target communications behavior. By “persistent” we mean that the intrusion is designed to take place over a substantial period of time, avoiding detection, gathering and exfiltrating data, and preserving an attacker’s ability to issue a variety of commands to the infected system. They require a non-trivial investment of time and resource from a threat actor, in order to surreptitiously acquire access, monitor the infected system, search for and select data of interest, and maintain a low profile throughout the compromise. While the technical tools permitting such action run the gamut in sophistication and cost, ongoing human involvement—what amounts to a commitment to the target—is apparent. In the case of CSOs, that work on sensitive human rights issues and generally do not possess financial assets that would entice an attacker, it is highly probable that the motivation behind such an intrustion is political.

We have also found that attackers are adaptive, modifying or designing attacks for use against specific software (including mobile applications) and hardware to reflect new and emerging methods of communication among their targets. Attackers exhibit an evolving awareness of civil society technical trends and defenses, which is reflected in their attack techniques. As a general practice, attackers make improvements to the malware they employ. For numerous malware samples in our study we observed several versions of the malware appearing over time, showing evidence of technical improvements. Adaptations, however, go well beyond malware maintenance. They encompass a wide range of responses to new platforms and behaviors.

As civil society actors have leveraged new technologies to advance their goals, attackers have done so as well, designing social engineering strategies and malware around the technical platforms that have become popular with their targets. For example, Citizen Lab and other researchers have documented a rise in Mac and mobile malware. While the majority of the malware we observed in our study targeted Windows operating systems, we also observed malware designed for OS X and Android. Indeed, Mac malware is increasingly paired with Windows malware, allowing attackers to compromise the target’s computer without concern over which platform is used. In one instance, Tibet Group 1 and Citizen Lab tested the responsiveness of the attacker(s) behind one particularly well-crafted spoofing attempt by replying to the email, stating that the attached (malicious) Excel file could not be opened on the recipient’s Mac. Within four days, the attacker diligently followed up with a new file containing Mac malware.
Study participants have also experienced ongoing targeting of the various cloud-based and popular communications programs on which they rely. CSOs have flagged Skype, Twitter, Gmail, and mobile devices and applications as vectors of confirmed malicious activity. The latter in particular present what Tibet Group 1 terms “a whole new battleground.” For example, in late 2012 Tibetan community members began discussing alternative applications to mobile messaging application WeChat—owned by Chinese company Tencent—following concerns raised about its security. As part of this effort, an information security expert within the community sent an Android application package (APK) file for the alternative KakaoTalk messaging application to a private contact. Shortly thereafter, attackers circulated a maliciously repackaged version of the KakaoTalk file to Tibetan targets. The file was implanted with malware that added system permissions allowing attackers to collect user contacts, SMS message history, and cellular network location. The attackers were able to acquire the email and file because the original recipient’s account was compromised.

4. Targeted digital threats undermine CSOs’ core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety.

CSOs may experience a range of impacts resulting from targeted digital threats. In the most serious cases, staff or individuals with whom they are in contact may experience physical intimidation, abuse, detention, or imprisonment by authorities that stems in whole or in part from surreptitiously monitored communications. Although digital surveillance may not be the proximate cause of this harm, it provides the authorities with an opportunity or rationale that may not otherwise have existed to take such action—for example, when digital evidence reflecting opposition to government policy serves as the primary basis for sentencing an individual for subversion or subjecting them to torture. In environments where mere contact with a CSO may heighten scrutiny of an individual, when digital records reflecting such contact are stolen, physical harm is a real possibility.

The psychosocial impact of targeted digital threats on communities is profound. It’s like when you do all this work to secure peoples’ systems from surveillance and trying to help [them] avoid Chinese authorities monitoring them, and then everybody installs WeChat on their phones—so it’s like, ‘forget your laptop, forget the desktop, forget all of it—you’ve just perhaps given them complete access with this...’ Everything we do is undermined overnight by this app that everyone is using... [Tibetans] adopt this stuff super fast. Especially when it’s free...because it just facilitates community.”

—Tibet Group 1
CSOs and activists is also significant and requires further attention. Staff of CSOs where intrusions are suspected or discovered report a variety of psychosocial effects, including a sense of violation, a state of fear of physical harm to themselves or loved ones, and chillings effects on their speech and use of technology. Groups particularly hard hit over the years have reported a loss of morale or “malware fatigue” (feeling like the threat has existed forever and cannot be escaped), which can lead to feelings of resignation and to abandoning security practises. There are reputational consequences to digital threats as well. Despite their ubiquity, exposure still carries a stigma in certain contexts, as a targeted group may be unfairly perceived as somehow to blame for “allowing” an intrusion or serving as the “bait” in a spoofed email or other attack vector. Or, a malicious email may circulate damaging misinformation about a person or entity. These impacts affect not only the will and ability of CSOs to carry out their missions and properly prevent or remediate a digital compromise, but also staff health and retention, and adoption of important digital platforms over the long term.

The most common impacts of targeted digital threats are the financial burdens of preventing or remediating intrusions, and undermined organizational efficiency—the “nuisance value” of the intrusion. CSOs, often on tight budgets, can easily incur extensive security costs. Security assessments, remediation, secure communications infrastructure, and technically proficient staff are all expensive, and typically priced for a commercial market, not struggling nonprofits. In addition, CSOs may need to spend considerable staff time identifying and notifying people whose communications were exposed to the attackers. This effort may sap the capacity of CSOs to conduct their primary human rights-focused missions.

Finally, one critical impact unique to targeted digital threats is their potential to wholly degrade the communications of CSOs and, as demonstrated by the Tibetan experience, entire communities. An essential element of civil society work is communication with the constituents served and with those entities CSOs wish to reach through their advocacy. Communication is a crucial factor in conducting research, obtaining important information on topics of concern, and disseminating messages concerning such topics. Targeted digital threats exploit the importance of communication to CSOs, undermine their methods of reaching constitu-

“We were in the middle of a Skype conversation and we could hear screenshot sounds over Skype. Both of our computers were compromised and we had to clean up... It wasn't totally the end of the world, although it felt horrible...like a huge invasion... I think it sort of paralyzed us emotionally... for a few days.”

—Tibet Group 2
ents and audiences, and create a climate of fear and lack of trust. It is possible that the goal of certain targeted digital threats may ultimately be to make communication more troublesome or raise the costs of communication for civil society.

5. Targeted digital threats extend the “reach” of the state (or other threat actors) beyond borders and into “safe havens.”

Just as technology allows diaspora, exile movements, and international human rights groups to extend their reach and have greater connections with each other and the communities they are trying to support inside countries of concern, it also allows threat actors to do the same—with malicious intent. The China and Tibet Groups in our study are all advocating for issues from outside of mainland China. Rights Groups 1 and 2 are hubs that support regional offices spread around the world. Groups tend to perceive (quite reasonably) contacts, offices, staff, and associates closest to the adversary as the most at risk and their communication links between these entities as the most sensitive.

What might be easily overlooked, however, is the extent to which digital espionage also provides threat actors a means of leverage over individuals and groups that are located beyond the physical reach of repressive regimes. Individuals within these communities often faced persecution in their home countries, and established themselves elsewhere to seek refuge from violations of their human rights by the state. In the universe of targeted digital threats, no such safe havens exist. Attackers target individuals and groups outside of their jurisdictions to track those inside who have connections abroad, and / or to monitor activist movements and organization in the diaspora. Our research has shown that exiled journalists and human rights workers who have become naturalized citizens or refugees in democratic countries have had their computers and mobile devices compromised, their communications monitored, and their movements tracked—as if they were still in the country from which they fled. For those who assume that leaving a repressive country for one where civil liberties are protected solves the risks around persecution, targeted digital threats reopen the issue. Even those individuals who have never lived in the country and were born abroad can be drawn into the tentacles of a far-off regime as a consequence of their political advocacy.

“Files were literally disappearing from our server... We don’t know how much was actually taken... They were clearly letting us know that the files were gone... It took about a week of rebuilding and diagnosing everything... We had to order new servers, we had to write everything and then we had to reload everything...”

—China Group 1
THE SNOWDEN DISCLOSURES

Beginning in June 2013 onwards, a stream of highly classified documents leaked by former United States National Security Agency (NSA) contractor Edward Snowden has provided the public with an unprecedented view of the highly classified capabilities of the world’s most powerful signals intelligence agency, the NSA, and its allies in the United Kingdom (GCHQ), Canada (CSEC), Australia (ASD), and New Zealand (GCSB). They show an extraordinary effort across every layer of the global telecommunications infrastructure, from the code to satellites and everything in-between, to infiltrate, collect, and even subvert or destroy data that passes through it. The impacts of these disclosures, many of which are too early to discern, are far-reaching, and have generated intense debates about the proper balance between security and privacy.

With respect to our study, at least two considerations stem from the disclosures. First, we did not encounter in our research any concrete evidence of NSA or allied malware attacks or espionage campaigns. Unlike those that we documented and which are generally assumed to originate in some manner from China, any analogous operations undertaken by the NSA and its allies would likely be very difficult for us to discern given the high level of their sophistication and the steps undertaken to obfuscate their attribution. It is important to be clear that our lack of material evidence of such attacks does not mean that they did not or will not happen; indeed, Edward Snowden himself testified to the Council of Europe that “The NSA has specifically targeted either leaders or staff members in a number of civil and non-governmental organizations...including domestically within the borders of the United States.” The additional evidence provided by the disclosures may, over time, help inform future research into any such digital attacks, and we certainly intend to take them into consideration in subsequent Citizen Lab research.

The second consideration concerns perceptions of risk. Whereas prior to Snowden’s disclosures vague concerns about widespread digital spying were voiced by a minority and sometimes trivialized, afterwards those concerns have been given real substance and credibility, and are now increasingly seen as a practical risk that requires some kind of remediation. After Snowden, there are now many more organizations offering security tools and trainings from which CSOs can benefit.

As one of our study participants stated: “I don’t think it was until those attacks manifested at the end point of the user laptop that people really cared... [B]ecause that is visible for users in places that they understand—again your email, your Twitter account—even if they don’t understand the implications, the connections; how your email is the gateway for most of your life, they now see it as something real and personal... [T]he paranoia is not for crazies anymore.” —Rights Group 2
Responses and Next Steps

Our research into targeted digital threats provides a window into a troubling set of problems affecting CSOs, and thus by extension the health of civil society networks worldwide. We have identified some urgent considerations and next steps that should be taken to address the problems and begin the process of crafting effective solutions. Some of these points were raised by Citizen Lab study participants themselves. It is important to emphasize that solutions will require the involvement of multiple stakeholders, and there is no one single solution, technological or otherwise, that will stem the harm to CSOs from targeted digital threats. Accordingly, the following section puts forth considerations for next steps across multiple sectors.

FOR CIVIL SOCIETY GROUPS

CSOs are in the midst of what is likely to be a protracted contest for security, rights, and openness in the digital realm. Digital security considerations must inform their actions. At the same time, digital security is not (and should not be) their number one priority. Efforts to integrate digital security solutions with their operations must be aligned with their core mission. Initiatives to address digital security within these organizations must account for the organization’s purpose, needs, and constraints. Nevertheless, there are fundamental actions CSOs can take to empower themselves. These actions complement, but do not replace, necessary technical and financial investments.

Document incidents

A relatively straightforward (but often overlooked) aspect of addressing targeted digital threats is the documentation of incidents by CSOs. Understandably, when experiencing a digital compromise CSOs may direct their attention exclusively to remediating the problem and recovering any lost material. Documenting the details of precisely what happened, and preserving attack vectors, malware, or compromised devices for analysis and digital forensics, are likely far down the list of priorities. Yet this step could significantly enhance individual and collective knowledge of targeted digital threats, as well as
the ability of CSOs to prepare for future attacks or seek justice for past ones.

One of the main challenges in researching targeted digital threats, particularly around civil society compromises, is the lack of concrete data regarding the problem. Basic facts regarding the number of incidents experienced by CSOs, the nature and timing of the incidents, the suspected vector of compromise (e.g. malicious email, drive-by download), the individuals involved, and the impact of the attack are rarely kept in a systematic fashion. CSOs are often quite capable, however, of keeping such documentation, as many do this already for physical incidents, and the associated burdens are relatively low—primarily an investment of a small amount of staff time. Maintaining copies of the malware itself or imaging infected machines for digital forensics presents additional complexity, but is something that could also be considered by CSOs that have sufficient technical support.

Benefits of standardized documentation of targeted digital threats could include: better understanding among CSO leadership and funders of the current digital risks to the organization, and the areas requiring additional resources (funds, training, tools) or change in practices; preservation of evidence that may be essential to legal claims, or other advocacy CSOs may wish to pursue; and, establishment of a repository of targeted threat data which, if shared, would inform a variety of investigations by researchers, activists, and others into evolving digital threat patterns, trends, and potential solutions.

**Share knowledge and coordinate**

As this Citizen Lab study and much other research has shown, no entity or individual is immune from digital threats. A large number of CSOs have already gone through the process of discovering, mitigating, and recovering from a compromise; those who have not are increasingly aware of digital risks and the need to prepare for them. Given the common experience of civil society actors in confronting and responding to this problem, a *collective approach to digital threats* may yield greater benefits than attempting to tackle these threats in isolation.

First and foremost, CSOs will know they are not alone or to blame in their experience; second, details of attacks can be shared so that others have more knowledge of

"It all comes back to public awareness, education... If we could break it down for people in a way that they understand... and paint the bigger picture, it has an impact. Tibetans are probably more apt to listen than other communities because the stakes are so high...it’s just about the time and resources to stay on top of [the risks]."

—Tibet Group 1
current threats and can take preventive measures; and third, successful responses to the problem—perhaps emanating from entirely different communities or areas of interest—can be studied and adapted by other CSOs. We found that the Tibetan CSOs in particular have made significant strides in raising awareness of digital risks and encouraging digital hygiene through their adoption of a collective, community-based approach to the issue, including development of educational resources that provide security information reflecting Tibetan culture.

CSOs should also consider involving funders in collective efforts, communicating with them regularly about security issues and incidents. Digital security is an area in which funders can play an important role (see our specific recommendations to funders below), given their high-level vantage of the cross-sectoral trends affecting CSOs with which they work, and their capacity to bring resources to bear on the problem. They possess a unique ability to coordinate among CSOs. Funders, however, are not always aware of the digital security challenges faced by particular grantees. Sharing information regarding digital threats with funders can help illustrate areas of need, cultivate support, and disseminate learning across a significant portion of civil society.

**Encourage a culture of digital security awareness**

We frequently heard from CSOs staff were reluctant to confront such a complex problem as targeted digital threats, and that responsibility for digital security was often assumed to be siloed with the few individuals associated with the CSO who had technical expertise. One of our key takeaways from the study, however, is that individual human behavior is a critical facet of exposure. To address this problem, CSOs should gradually build a culture in which all staff, regardless of technical background, feel some responsibility for their own digital hygiene. While staff need not become technical experts, CSOs should attempt to raise the awareness of every staff member, from executive directors to interns—groups are only as strong as their weakest link—so that they can spot issues, reduce vulnerabilities, know where to go for further help, and educate others. Of course, there is no way to anticipate and warn against every form of digital threat; new technologies and new threats

> What I tell [staff] is ‘use your common sense, if you see something...suspicious, do not open it, or at least forward it to somebody to reveal it before you do anything about it.’ But sometimes, I know it’s probably difficult. I do not have any clever way to tell them, ‘If when you see this, don’t open it.’ It’s sometimes very difficult, [there are] just too many varieties of attacks.”

—China Group 1
emerge constantly, outpacing security awareness. In such an environment, it is important for CSOs to develop a framework for critical thinking and informed decision-making by their staff about digital threats, not tethered to any specific application, device, attack vector, or situation.

FOR FUNDERS

Funders are uniquely positioned within the civil society landscape to contend with targeted digital threats. Both funders themselves, as well as the grantees they support, are at risk for politically-motivated digital compromise. Funders thus have at least two core responsibilities related to targeted digital threats:

1. To help their grantees implement better security.
2. To secure themselves (thereby also preventing collateral compromise).

This dual responsibility presents a number of challenges and opportunities to grantmakers, who are, we suspect, still engaged in an internal learning process about their own digital security.

Securing grantees

Many of the CSOs discussed in this report are dependent to some degree on external funding. Grantmakers are no stranger to finding strategies to help their grantees manage risk. For the past decade or more, funders with grantees operating in high risk areas (e.g., human rights organizations) have placed higher priority on supporting the physical security of grantee organizations. However, as this report makes clear, physical and digital security are increasingly interconnected. Indeed, in the current climate of risk, a lack of attention to digital security can erode the gains made by investing in grantees’ physical security.

Funders are in a unique position to develop programs and funding lines that could help grantees make measurable improvements in their organizational security. However, funders face challenges around getting this right. Program staff, while often aware of the specific political and physical threats to grantees, are generally un-equipped to evaluate digital threats to grantees because of the kind of technical expertise it requires. This extends to their ability to evaluate the quality and appropriateness of security solutions offered by third parties. This issue becomes particularly sensitive in the context of funding digital security training and related services for CSOs that face direct threats from state and non-state actors; uninformed training, advice, and/or flawed products could have grave repercussions. Moreover, an occasional training is not an acceptable substitute for serious support with digital security. Funders should
ensure that the security programs they do support are not sporadic, piecemeal, or focused only on encouraging changes in behavior without comparable investments in well-developed technology, policies, and practices that can help organizations attain and maintain better security.

Funders need to identify and build robust practices around implementing and measuring the success of any programming around digital security for entire program portfolios. However, many Monitoring & Evaluation consultancies, at time of writing, have limited specialized expertise in digital security. Identifying the right partners will be important if digital security is to be given a sustainable place in grant portfolios. Some funders may also seek to make large grants directly to digital security support organizations. We encourage funders to conduct extensive diligence, and seek expert advice, before doing so.

We think funders may have an untapped internal capacity here: the CTO and other technical staff may be able to help evaluate potential providers of security services, or help to choose consultants who will do so.

Funders are also well-placed to gather critical data regarding targeted digital threats experienced by their grantees, as they can do so in an aggregated and anonymized fashion. Such aggregation represents a promising avenue for collaboration between funders, and a mechanism to provide concrete data—with identifying information carefully anonymized—about the civil society experience of targeted digital threats and the results of funder efforts to support security.

Funder: secure thyself

Funders constantly handle sensitive information about their grantees, and may be well aware of the ways in which it could be used against them. Most would be horrified to discover that their handling of confidential material brought risk to their most sensitive grantees. However, in some cases this type of compromise is clearly happening. While outside the scope of data collected in our report, there appears to be an epidemic of compromises against Western NGOs with international

“Certainly there is generally... a whole lot of cluelessness on the part of funders... Part of organizational development should be technological skills and the utilization of modern tools. Part of that needs to be how do you do so prudently and safely? I think that a lot of the funding models are very difficult for funding sustainable technology programs.” —Rights Group 1
portfolios. Some of these come from the same threat actors we have tracked in this report.

It would move the conversation forward to have a better understanding of the scale of compromises that have already taken place among major funding organizations. Funders should also consider the responsibilities they have to their grantees and partners concerning disclosure of breaches. Grantmakers are not the first sector to deal with this issue, and the emerging consensus is that balanced transparency (to the extent that is practical and does not further compromise confidentiality and security) can be positive.

**The bottom line**

Grantmakers occupy a critical position and are among the few who can directly put their resources where their concerns are, and help effectuate change at scale. If funders care about the continued success of their programming and the security of their grantees, attention to digital security needs to occupy a proportionate part of their activities. Funders need to make sure they are also secure: they should not be the party adding risk to their relationships with grantees. They should be part of the solution.

**FOR COMPANIES**

The technology sector benefits tremendously from the association of their tools with positive social change. In the past several years, we have observed that social media and technology companies are often publicly thrilled when their products turn up in use during periods of dramatic social change. We think this enthusiasm reflects a genuine, ambitious idealism about the transformative power of new technology. Yet we also observe that many of these platforms, especially when used without adequate precaution, serve as efficient vectors of attack against CSOs.

If the technology sector indeed has a strong commitment to a possible role for its projects in the civic realm, which includes civil society, this will entail some responsibilities, including:

- Understanding how CSOs make use of your services
- Tracking and mitigating specific threats to CSOs using your platforms
- Being transparent about appropriate uses and potential risks of a platform in specific contexts.
EXECUTIVE SUMMARY

Know your users
CSOs make creative and sometimes unexpected use of social media and communications platforms for all manner of strategic and tactical purposes. Yet these uses create new vulnerabilities and avenues of attack. As many of these attacks are highly targeted, they can fall below the radar of security teams who are looking for attacks with effects on a very large user base. Targeted digital threats often constitute an exceptionally high risk against a small number of users. Tracking these attacks, in our experience, often requires a close understanding of the practices and operations of targeted groups, and some communication with the groups about the threats they face.

We are aware of some companies that, often discretely, are developing the capacity to engage with civil society while managing reputational risks and allocation of staff time. In practice, this sometimes means careful collaboration with intermediary and partner organizations, including funders, policy groups, academics, and others that can help technology companies navigate the challenges.

Think creatively about flexible licensing
We have observed that CSOs are often stuck in least-common-denominator models of organizational security because they are unable to standardize software products and devices across their organization. This lack of software adaptability makes it hard to create a security policy or consistent set of security guidelines within an organization. Moreover, many of the tools and software used by CSOs are often counterfeit or expired. This situation leads to a practice of avoiding software and operating system updates. In still other cases, CSOs use free versions of tools and packages that offer lower levels of security than for-purchase versions.

A number of companies have shown that it is possible to provide reduced cost and free licenses to bonafide CSOs. Many companies have the resources to make this kind of commitment. However, we note that for these programs to be effective, the low-cost or free versions must not skimp on security features.

“
The market is offering tools with decreasing cost that simplify the use of targeted attacks against anyone in civil society by informal actors. So I think that it will be very, very important for us beyond the human rights movement to understand the role that the private sector is playing here, because we’re in a moment we could impact. But in general I think that’s one of the things that is missed the most.”

—Rights Group 2
**EXECUTIVE SUMMARY**

*Time for pro bono?*

We believe digital security is a right, regardless of ability to pay for services. We are in desperate need of ways to address CSOs digital insecurity that take into account the limits of CSOs’ and grantmakers’ resources. CSOs need sustained, expert technical services and consultation tailored to their specific needs and risk profiles. This kind of service, typically provided in-house or by consulting companies, is considered essential by the corporate and public sector, but the cost of quality service is out of reach for the vast majority of CSOs, with the exception of a few, very well-resourced ones based in North America and Europe.

The tech sector has substantial resources that can be tapped. As the sector professionalizes, as with law and medicine, it is time to examine pro bono models of support for digital security assistance to civil society. There are many people in the sector with extensive experience providing this kind of services and assistance, whether in incident response, the development of security policies, or assistance managing security services. Many developers and technologists would likely find it rewarding and meaningful to contribute time and resources to CSOs with the support and approval of their employers.

As a first step, we encourage technology companies to consult staff and management to ascertain interest in pro bono programs, and begin thinking through the other benefits, but also reputational risks and how they might be mitigated.

**FOR RESEARCH**

We see the *Communities @ Risk* report as the culmination of only the first phase of our formal study, and in subsequent phases of the project we intend to make adjustments to the research design and the scope of the project. In particular, we would like to expand the number and type of participants enrolled in the study. As mentioned above, the first phase of the research involved eight groups out of 10 whose activities and/or orientation were “China” or “Tibet facing,” and only two that were globally oriented. Moving forward, we will look to enrol groups from other regions and countries (e.g., Latin America, sub-Saharan Africa, Southeast Asia, and the Middle East), and include groups that are working in sectors not presently covered by our study groups, such as the environment, LGBT rights, or extractive resources. We also intend to undertake a dedicated research effort regarding journalists at risk—a particularly salient sub-category of civil society for which there are preliminary indications of targeting and uneven security practices.
One of the challenges of researching targeted digital threats is that evidence of the harms around such threats are often disparate, unconnected, and/or incomplete. For example, a member of a CSO may be detained because of a compromised device, but have no idea of the nature or even existence of the compromise in the first place. Likewise, a researcher in the computer security industry may have evidence of victims of a targeted computer espionage campaign, but have no channel to notify the victims of the breach before it is too late. Meanwhile, a public interest group may want to launch litigation around a specific case of targeted digital threats, but lack data preserved in a fashion that is useful as evidence in a court of law. Moving forward, we hope to encourage a better means of collecting, archiving, and organizing data among relevant stakeholders so that stories of harm are better documented and understood.

We also hope to improve upon the methods and tools available to research groups outside of Citizen Lab and among the wider communities of which we are a part. There were tools developed by other researchers, including affiliates and colleagues of Citizen Lab, from which we benefited tremendously, including Cuckoo Sandbox and Viper, a binary management and analysis framework for security researchers developed by Citizen Lab collaborator Claudio Guarnieri. Unfortunately, many other tools, methods, threat intelligence platforms, and repositories of data used by security researchers are proprietary and/or prohibitively expensive for researchers to employ. In the next phase of our research, we intend to explore and further develop tools, methods, and platforms for open data sharing.

Finally, throughout the course of our study we sought to publish timely reports on our website while also working on a separate track to publish in peer-reviewed journals and conferences. Our mixed methods approach to targeted digital threats fits uneasily into any one academic discipline and finding venues for publication of formal research of this sort is a challenge. However, we successfully published several papers in major academic conferences, held two annual summer institutes on mixed methods research on information controls, and helped develop a new fellowship program on interdisciplinary research, in which Citizen Lab will become one of several host organizations supporting a community of researchers working in this area. We hope to build upon this success moving forward, and contribute to a growing community of academic research around targeted digital threats. In the long run, a robust community of researchers producing rigorous, evidence-based, and impartial research on digital risks will offer a powerful form of support for civil society networks.
FOR GOVERNMENTS

While we recognize that governments have complex agendas and competing interests when it comes to cybersecurity, long-term solutions to targeted digital threats will require government involvement. Current debates concerning government reform naturally have emphasized mass surveillance, but the question of targeted cyber espionage and digital attacks against civil society actors also merits further consideration. This is not an issue on which governments should get a free pass by simply asserting espionage is an established feature of state intelligence; the ability to distinguish among targets in cyberspace and treat legitimate civil society actors as off-limits for such conduct is essential. States that support the right to privacy and freedom of expression online should take steps to raise the profile of targeted digital threats against civil society in their domestic policy and diplomacy, treating the matter as of equal priority to their defense of the private sector. Moreover, governments should take urgent action to reign in—and avoid driving the growth of—the increasingly dangerous and largely unregulated market for commercial spyware. In all of these efforts, it will be essential for government to engage with civil society in meaningful dialogue to inform appropriate solutions.
COMMUNITIES @ RISK
Targeted Digital Threats Against Civil Society
November 11, 2014
https://targetedthreats.net/
EXTENDED ANALYSIS:

2.1 Summary, Methodology, and Data Overview
Summary

Communities @ Risk: Targeted Digital Threats Against Civil Society reports on an intensive study that analyzes targeted digital threats against 10 civil society organizations (CSOs) over a period of four years.

The report combines two major sections:

1. The Executive Summary provides detail on how the study was organized and why we feel it is important to read, a high-level overview of the key findings of the research, and considerations about next steps for several stakeholder communities in responding to targeted digital threats.

2. The Extended Analysis explains our methodology, and examines the detailed data we gathered during the study period. It is the evidentiary basis for the claims we make in the Executive Summary, and will likely be of interest to a more specialized audience (although we hope everyone will read it).

KEY FINDINGS

In the Executive Summary, we outline five high-level findings. We summarize them again below, while adding more granular details that are given extended treatment in the analysis that follows.

In the digital realm, CSOs face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.

Through cluster analysis we identify 10 distinct targeted malware campaigns. We find that five of these campaigns have connections to threat actors, previously reported to have targeted government and private industries. CSOs have limited resources and technical capacity, which makes responding to threats a challenge. We generally find that, due to resource constraints, CSOs focus their digital security strategies on user education and behavioural change rather than expensive technical solutions.
Counterintuitively, technical sophistication of malware used in these attacks is low, but the level of social engineering employed is high.

We develop the Targeted Threat Index, a metric for quantifying and characterizing the sophistication of targeted malware attacks. Using this metric, we find that the technical sophistication of targeted malware delivered to CSOs in our study is relatively low (e.g., relative to commercial “lawful intrusion” surveillance kits and conventional financially motivated malware), with much more effort given to socially engineering messages to mislead users.

Digital attacks against CSOs are persistent, adapting to targets in order to maintain access over time and across platforms.

Our analysis of attacks against CSOs over four years allows us to track how attackers change tactics. For numerous malware samples, we observe several versions of the malware appearing over the course of our study. These multiple versions show evidence of technical improvements to complement increasingly refined social engineering techniques. In some cases, we observe threat actors quickly changing tactics to adapt to shifting platform adoption and user behaviour.

Targeted digital threats undermine CSOs’ core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety.

The impact of targeted digital attacks against technical systems is apparent and receives ample attention from researchers. However, we find evidence of wider impacts that are not always as obvious, including psychosocial strain and possible connections to physical harms (e.g., arrest and detention). Tracing connections between compromises and harm is challenging, because the relationship between digital compromises and the use of the compromised information by threat actors is indirect. Unlike the consequences of physical threats, which are often readily observable, the most serious impacts of digital threats are typically at least one step removed from the technology that has been exploited.

Targeted digital threats extend the “reach” of the state (or other threat actors) beyond borders and into “safe havens.”

The ways CSOs develop their perceptions of risk and threat stemming from targeted attacks depend in part on the physical proximity of their threat actor. Groups operating within the jurisdiction of a repressive regime have greater concerns over physical security and other direct interference from authorities. Conversely, groups situated
outside of a physical jurisdiction controlled by an adversary may prioritize digital
threats over physical threats. For groups in diaspora and exile communities, targeted
digital threats can be seen as a means for a powerful threat actor, such as a state, to
extend their reach beyond borders and into “safe areas.”

**EXTENDED ANALYSIS STRUCTURE**

The Extended Analysis is structured into the following three sections. Each of these
sections can be downloaded individually or read as a whole.

**Summary, Methodology, and Data Overview** outlines our mixed methods approach
which incorporates analysis of technical and contextual data using methodologies
from the field of information security and the social sciences, and presents a high level
overview of our dataset.

**Cluster Analysis** provides detailed technical analysis of 10 distinct targeted malware
campaigns.

**Civil Society Perspectives and Responses** reports on results from interview data and is
a window into how groups under threat think about and respond to digital threats.

We also are publishing data that provide indicators of compromise (including YARA
signatures of malware families, MD5 hashes of samples, and command-and-control
servers), which are available on our github account and accessible through our
project website.
Methodology

This section describes our methodology for data collection and analysis. Since our study involves the collection of potentially sensitive information from civil society organizations, and requires us to deal with personally identifiable information (PII), we consulted with the University of Toronto’s Research Ethics Review Board during the design of our study. The methods described below have been submitted to and approved by this board.

STUDY PARTICIPANTS

We recruited participants via three channels: (1) an open call on our website, (2) outreach to organizations with which we had prior relationships, and (3) referrals from participating groups. As part of the study, these groups agreed to share technical data (e.g., emails with suspicious attachments) and participate in interviews. Their identity and any PII shared with us were kept strictly confidential.

Organizations with a mission concerning the promotion or protection of human rights were eligible to participate.\(^1\) We also considered, on a case-by-case basis, organizations with a mission that does not directly address human rights, but which may engage in work related to human rights issues (e.g., media outlets that regularly report on human rights violations).

In total, 10 organizations participated in the study. The majority of these groups work on China-related rights issues, and five of these organizations focus specifically on Tibetan rights. The exceptions to the China- / Tibet-focused groups in our study are two large organizations that work on multiple human rights-related issues in various countries.

---

\(^1\) For purposes of this study, “human rights” means any or all of the rights enumerated under the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; and the International Covenant on Economic, Social and Cultural Rights.
<table>
<thead>
<tr>
<th>ORGANIZATION CODE</th>
<th>DESCRIPTION</th>
<th>ORGANIZATION SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rights Group 1</td>
<td>Human rights organization focused on multiple issues and countries</td>
<td>Large (over 100 employees)</td>
</tr>
<tr>
<td>Rights Group 2</td>
<td>Human rights organization focused on multiple issues and countries</td>
<td>Large (over 100 employees)</td>
</tr>
<tr>
<td>China Group 1</td>
<td>Human rights organization focused on rights and social justice issues related to China</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>China Group 2</td>
<td>Independent news organization reporting on China</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>China Group 3</td>
<td>Human rights organization focused on rights and social justice issues related to China</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 1</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 2</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 3</td>
<td>Independent news organization reporting on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 4</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 5</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
</tbody>
</table>

Tibet Groups

Dharamsala is a small city in northern India set on the foothills of the Himalayas. His Holiness the Dalai Lama (HHDL) has lived in Dharamsala since 1959 following his escape from Tibet. Dharamsala is the base of the Central Tibetan Administration, which administers programs and schools for Tibetan refugees living in India and advocates for the rights of Tibetans in Tibet. It is also home to many Tibetan NGOs and independent media groups, and thousands of Tibetan refugees. This high concentration of prominent Tibetan institutions makes Dharamsala a prime target for malware campaigns. It has been called one of the most hacked places in the world. For exiled Tibetans, this heightened level of digital risk compounds the many challenges of living as refugees in a developing country.

Three of the Tibet Groups in our study are headquartered in Dharamsala, and two
maintain regional offices there. Across these groups participants expressed challenges related to awareness of threats, low resources, and limited technical capacities.

Tibet Groups reported varying levels of awareness of digital risks in the community. While many participants noted that security awareness was generally increasing among Tibetans, others cautioned that some groups still do not have policies or response plans around targeted digital attacks and “continue to back burn things like security.”

A major challenge identified by the Tibet Groups is a lack of technical capacity and resources in the community. Most Tibetan NGOs do not have dedicated system administrators. In some groups, staff members responsible for web development also take on double duty as system administrators. In addition to local staff, there are transient volunteers who come into the community to help with technical projects. As one of these volunteers noted, however, when volunteers leave the community projects sometimes end up unmaintained or completely abandoned.

While the unique circumstances of the Tibetan exile community are challenging, some groups are also taking proactive measures to increase digital security awareness. For example, one of our participating organizations prioritizes digital security in the community within its mission, focusing on raising awareness and user education. These grassroots initiatives demonstrate a growing commitment to addressing security challenges, despite ever-present resource limitations.

China Groups

The three China Groups all work on issues related to human rights and politics in China, but from outside of mainland China. China Groups 1 and 3 each have a central office and one regional branch. China Group 2 operates an independent news website from an office with limited staff. China Group 1 has a program manager that oversees technical projects, but does not have a dedicated system administrator on staff. Instead the group outsources management of its information technology infrastructure to a private company. China Group 3 has had a dedicated system administrator since its founding.

The work of these groups is politically sensitive and has attracted attention from Chinese authorities. China Groups 1 and 2 especially have come under pressure for
human rights advocacy and the dissemination of sensitive news, respectively. As China Group 1 explained, “Chinese authorities ... have very clearly in public designated us as an anti-China organization.”

These groups are all highly aware of targeted digital threats, and have experienced numerous prior incidents. All of the groups had received targeted malware in the past and their websites are consistently blocked in China. The website of China Group 2 has been repeatedly hit by distributed denial-of-service attacks.

Rights Groups

Rights Groups 1 and 2 are much larger organizations relative to the others in our study. Both have over 100 employees, multiple offices, enterprise level computing infrastructures, and dedicated IT teams and support desks.

These groups act as hub organizations. Rights Group 1, for example, supports multiple regional offices and CSO partners around the world. Rights Group 2, similarly, operates regional branches and is responsible for a large group of staff operating in numerous field locations.

Both groups contend with securing their head offices and maintaining awareness of threats faced by field offices. These challenges show that while the Rights Groups have greater resources they must grapple with a potentially wider spectrum of threats in multiple contexts and countries.

DATA SOURCES

Email Submissions: The majority of data collected consisted of emails identified by participants as suspicious, which were forwarded to a dedicated mail server administered by our research team. When available, these submissions included full headers, file attachments, and/or links.

Relying on forwarded emails presents a collection bias as the recipients must be able to identify that the emails are suspicious and remember to forward the samples to our research team. This collection method also limits the threats studied to those that are sent over email. Additionally, collection of forwarded email samples does not allow us to verify if a targeted organization was successfully compromised by an attack, or the scope of the attack. Recognizing this limitation, we added two more data collection methods to complement the collection of emails.
Network Intrusion Detection System: As an optional study component, we offered to install a network intrusion detection system (NIDS) inside the networks of the participants. In total, seven groups opted into the NIDS project. We used a combination of community and commercial rulesets, as well as a set of custom rules based on threats we analyzed from the email submissions. By placing a NIDS inside an organization’s network, we were able to record incoming threats using vectors other than email, as well as detect and observe systems that had already been compromised.

Website Monitoring: We conducted external scans of the study organizations’ websites to monitor for potential compromises such as watering hole attacks. These scans were done with publicly available tools including Cyberspark and URL Query.

Interviews and Fieldwork: To gain insights into the experiences of our groups, we conducted a series of semi-structured interviews over a four-year period and made site visits to their offices and locales. While there have been previous technical studies on targeted threats affecting CSOs, it is rare that the context surrounding these attacks and the experiences of the people facing them are properly explored. Interviews and site visits help provide insight into these vital elements.

When possible we conducted interviews with a senior staff member responsible for organizational programming (e.g., executive director, program manager), and a staff member responsible for technical support (e.g., system administrator, webmaster). The interviews explored the organizations’ uses of and policies around technology, perceptions of digital security and threats, responses to threats, and the impact of threats. These interviews, coupled with site visits and participant observations, helped us understand the working conditions, routines, infrastructure, and local social and political context that form the day-to-day environment of our participants.

Interviews were held opportunistically and did not follow a set schedule. The total number of interviews per group is outlined in Table 2. The majority of interviews were audio recorded and transcribed. In some cases, conditions did not allow for audio recording and field notes were made instead. Interview transcripts were analyzed using line-by-line open coding of transcripts to identify emergent themes.3

### TABLE 2: List of interviews conducted with participating groups*

<table>
<thead>
<tr>
<th>GROUP</th>
<th>SUBJECTS</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>China Group 1</td>
<td>Executive Director, Program Manager (technical projects)</td>
<td>2010</td>
</tr>
<tr>
<td>China Group 3</td>
<td>System Administrator</td>
<td>2011</td>
</tr>
<tr>
<td>Rights Group 1</td>
<td>Chief Technical Officer, Program Manager</td>
<td>2012, 2014</td>
</tr>
<tr>
<td>Rights Group 2</td>
<td>Technical Officer</td>
<td>2011, 2014</td>
</tr>
<tr>
<td>Tibet Group 1</td>
<td>Executive Director, Program Director, Program Director (technical projects), Program Officer, Security Trainer</td>
<td>2011, 2012, 2013</td>
</tr>
<tr>
<td>Tibet Group 2</td>
<td>Executive Director</td>
<td>2013</td>
</tr>
<tr>
<td>Tibet Group 3</td>
<td>Editor-in-Chief</td>
<td>2014</td>
</tr>
<tr>
<td>Tibet Group 4</td>
<td>Technical Volunteer</td>
<td>2013</td>
</tr>
<tr>
<td>Tibet Group 5</td>
<td>Program Officer</td>
<td>2014</td>
</tr>
</tbody>
</table>

*NOTE: We were unable to conduct a site visit and interview with China Group 2, because they did not maintain participation in the project.*

## DATA ANALYSIS

### Malware Analysis:
We examined malware samples using static and dynamic analysis tools (e.g., IDA and OllyDbg), as well as manual analysis to extract information on exploits, malware functionality, malware family, command-and-control (C2) infrastructure, and other properties of the malware code (e.g., mutex and exported function names).

### Email Content Analysis:
We reviewed the subject line, body, and attachments for each submitted email and grouped the content into specific themes and categories. The header of each email was analyzed to determine if the sending email address was spoofed or the email address was otherwise designed to appear to come from a real person and / or organization. Indicators drawn from this analysis were used to assess the relative sophistication of the social engineering tactics found in the messages (we incorporate these indicators into our Targeted Threat Index described below). We conducted regular inter-rater reliability checks that flagged any potential edge cases and inconsistencies for discussion and re-evaluation.
Targeted Threat Index: We developed the Targeted Threat Index (TTI), which is a metric that characterizes and quantifies the sophistication of targeted attacks, to provide a consistent ranking of how advanced any given targeted malware attack is. The TTI score is calculated by taking a base value determined by the sophistication of the targeting method, which is then multiplied by a value for the technical sophistication of the malware. The base score can be used independently to compare emails, and the combined score gives an indication of the level of effort an attacker has put into individual threats.

Cluster Analysis: Through identification of patterns in malware families, development cycles, shared infrastructure, and social engineering tactics, we identified relationships between attacks and, when possible, linked them to known malware campaigns and threat actors.
DATA OVERVIEW
A high level overview of our datasets

EMAIL SUBMISSIONS
The malicious emails analyzed in this report span more than four years, from October 10, 2009 to December 31, 2013. During this period we collected 817 emails from the 10 groups participating in our study.

FIGURE 1: Cumulative number of email submissions per month during the study

Figure 1 shows the cumulative number of email submissions per month over the course of the study. Although the first formal submission was received on November 28, 2011, some groups had existing archives of malicious messages received by their members, and they provided us with these older emails. Tibet Group 1 ac-
counts for the highest number of submissions relative to the other groups as it was one of the first groups in the study and is persistently targeted. Tibet Groups 2 and 4, which joined the study at a later date (April 2012), show a similar submission rate to Tibet Group 1, suggesting these groups are targeted at a comparable level.

**FIGURE 2:** Malicious emails by type for groups submitting 25 or more emails

We classify emails as malicious if they include attached malware, a direct link to malware or a drive-by download site, or a link to a phishing page. Figure 2 shows the number of emails of each type for the groups that submitted at least 25 emails to our system. The most common technique employed in these emails was a malicious attachment to the message. However, we observe a higher rate of phishing attacks on the China Groups and the Rights Groups. In particular, 46% of the emails submitted by China Group 1, and 50% of the emails submitted by Rights Group 1, direct the user to a phishing website.

The rate of submissions to our project meant that it was feasible to manually analyze email attachments for malware as they were submitted. This analysis gives us higher confidence in our results than if we had automated the process. Antivirus (AV) signatures frequently fail to detect new or modified threats, and can overlook the kind of malicious payloads that can be identified with manual inspection (e.g., shellcode in an RTF exploit). In total, we analyzed 3,617 payload files and found 2,814 (78%) to be malicious.
MALWARE FAMILIES

We identified malware families through patterns in network traffic and characteristics in the code, such as strings seen in the binaries or names and locations of dropped files. In total, we identified 44 separate malware families (not including variants). The most frequently occurring families are Gh0st RAT, Surtr, Shadownet, Conime, Duojeen, and PlugX.

FIGURE 3: Malware family timeline
(The coloured dots represent attacks using a particular malware family against one of our study groups.)
CVEs

Common Vulnerabilities and Exposures (CVEs) is a dictionary of common names for publicly known security vulnerabilities. CVEs are each assigned a unique identifier code, with the form CVE-YYYY-NNNN, where YYYY indicates the year they were identified and NNNN are arbitrary digits. We identified 24 distinct CVEs used in 483 of the email attacks as displayed in Figure 4.

*FIGURE 4:* CVEs identified in samples during the study period.

(Vertical gray bars represent the date the CVE was created and orange dots represent targeted attacks using that CVE.)

The most common CVEs we observed were **CVE-2010-3333** (used in 112 attacks) and **CVE-2012-0158** (used in 294 attacks), which are both vulnerabilities in the way Microsoft Word handles RTF documents. Figure 4 clearly illustrates the shift in use from CVE-2010-3333 to CVE-2012-0158 in March and April of 2012. The popularity of these vulnerabilities is not limited to our dataset. They have been widely used in other attacks against a variety of targets.
During four years of tracking attacks against our groups, we observed only one zero-day exploit. This attack used the Flash vulnerability CVE-2012-5054, and was sent 22 days before the CVE entry was created.

These results show that vulnerabilities exploited by targeted malware attacks against CSOs are typically not technically advanced (compared with financially-motivated malware and commercial lawful intercept kits), and often use old (patched) vulnerabilities. For example, CVE-2012-0158 has been patched since April 10, 2012, but has remained the most common vulnerability used in attacks against the Tibet Groups for well over a year after the fix was issued. The repeated use of this vulnerability suggests the attackers are achieving successful compromises because target systems did not have the latest security updates. A possible explanation is that licensed software is cost-prohibitive for many organizations in the developing world, while pirated copies are easily available, leading many to use pirated operating systems and software.

**ANTIVIRUS DETECTION**

VirusTotal is a service that scans files through 53 different AV engines and provides a summary of malware detection results. We find that 369 of the 659 samples we received (56%) had been submitted to VirusTotal at the time of writing, with a median AV detection rate of 24% and mean detection rate of 25%. Detection rates were generally low, as 86% of these samples had a detection rate below 50%, meaning that less than half of the AV packages tested were able to identify them as malicious. These results suggest that simply running AV software, although potentially helpful, is not a very effective defence against these attacks.

**FIGURE 5:** Histogram of antivirus detection rates provided by VirusTotal
This low detection rate we observed is due in part to the extensive presence of CVE-2012-0158, which uses a number of techniques to hide the vulnerability from AV scanners.

One of the simplest of these detection-reducing techniques is modifying the RTF header, since Microsoft Word will still be able to open the file, but fewer AV scanners will detect it as malicious. Another basic technique is encrypting malicious document and providing a password to open the file in the associated email. Simply adding a password to malicious files can help prevent AV detection.

Since there are four ActiveX controllers—ListView, ListView2, TreeView, and TreeView2—affected by this vulnerability and there are no strict syntax restrictions, there can be a large variance in the document templates into which malicious payloads are inserted. These can cause newer templates to initially have lower detection rates.

A notable technique observed was the creation of a MIME HTML (MHTML) file that uses the vulnerable ActiveX controllers. By default, MHTML files are opened by a browser: however, they can also be opened by Microsoft Word, which will trigger the exploit. Since Microsoft Word may not be the default application to open the file, automated sandbox programs may fail to detect the file as malicious.

The older CVE-2010-3333 vulnerability had similar issues with AV detection, because of the wide number of ways to encode the vulnerability. A small change in the way the vulnerability was written could evade signature detection while remaining functionally the same.

Although AV definitions are updated to account for evasion tricks, the lag between the use of evasion techniques in the wild and definition updates results in temporarily low detection rates, and hence the likelihood of successful compromises.
EMAIL CONTENT ANALYSIS

Subject line, body, and attachments: The content of the subject line, body, and attachments for each submitted email were content coded into 134 categories grouped under eight themes:

- Country / Region (referring to a specific geographical country or region)
- Ethnic Groups (referring to a specific ethnic group)
- Event (referring to a specific event)
- Organizations (referring to specific organizations)
- People (referring to specific people)
- Political (reference to specific political issues)
- Technology (reference to technical support)
- Miscellaneous (content without clear context or categories that did not fall into one of the other themes)

Email headers: The header of each email was analyzed to determine if the sending email address was spoofed, or the email address was otherwise designed to appear to come from a real person and/or organization (for example, by registering an email account that resembles a legitimate sender’s name from a free email provider). We divide the results based on whether they attempted to spoof an organization or a specific person.

Results of this analysis confirm that message content and fraudulent senders are tailored to the interests of the target organizations.

Of the 520 total emails received by the Tibet Groups, 97% referenced content related to Tibetan issues. Email lures leveraged specific events of interest and respected persons in the Tibetan community. Emails referenced Tibetan-related events, including holidays (Tibetan New Year), anniversaries (His Holiness the Dalai Lama’s birthday), and protests (see Table 3). The most frequently referenced events were Tibetan self-immolations (31% of the emails leveraging event-related content).

"Some of the attachments actually cannot be detected as a virus...We’re not even sure if it...will cause any harm at all. It’s just that the antivirus [is] saying that ‘there’s no threat,’ but obviously there’s something wrong with it.”

—China Group 1
Of the 520 emails received by Tibet Groups, 272 (52%) were designed to appear to come from real organizations. In total 58 organizations were spoofed, of which 53 (91%) were Tibet-related groups (see Table 4). The most frequently spoofed organization was the Central Tibetan Administration. The identities of four of the Tibet Groups in our study (Tibet Groups 1, 2, 3, and 5) were frequently spoofed internally and to external contacts. The frequency of emails with fraudulent contacts from Tibetan organizations shows an effort to have the message appear to come from within the Tibetan community and leverage existing trust relationships.

“*The emotions of the immolations [are] being used against people to have them click on [attachments].”*—Tibet Group 1

---

**TABLE 3:** Breakdown of top five categories in the Event theme for Tibet Groups

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NUMBER OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Immolation *</td>
<td>56</td>
</tr>
<tr>
<td>Tibetan National Uprising Day</td>
<td>24</td>
</tr>
<tr>
<td>HHDL Birthday</td>
<td>19</td>
</tr>
<tr>
<td>Flame of Truth Rally</td>
<td>13</td>
</tr>
<tr>
<td>Kalon Tripa Election</td>
<td>9</td>
</tr>
</tbody>
</table>

*Self-immolations are a controversial form of protest that Tibetans have used as a statement of opposition to Chinese government practices concerning Tibet. These protests have escalated in recent years. At the time of writing, it is estimated that since 2009, approximately 132 Tibetans have self-immolated.*

---

**TABLE 4:** Breakdown of top five categories in the Spoofed Organizations theme for Tibet Groups

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NUMBER OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Tibetan Administration</td>
<td>58</td>
</tr>
<tr>
<td>Tibet Group 1</td>
<td>26</td>
</tr>
<tr>
<td>Tibet Group 2</td>
<td>13</td>
</tr>
<tr>
<td>Tibet Group 5</td>
<td>13</td>
</tr>
<tr>
<td>Tibet Group 3</td>
<td>11</td>
</tr>
</tbody>
</table>
We see a similar pattern for the China Groups. Of the 48 emails received by the China Groups, 46 (95%) referenced China. Content included references to Chinese political events such as the Communist Party of China (CPC) 18th Party Congress; the June 4, 1989 Tiananmen Square crackdown; and Chinese dissidents and prominent members of the CPC (see Table 5). Of the 48 emails, 13 (27%) spoofed real organizations (see Table 6). Two of our China Groups were spoofed (China Group 1, China Group 3). Rights Group 1 was also spoofed in one message to China Group 1. The remaining spoofed organizations were prominent human rights groups and intergovernmental organizations (e.g., the UN Office of the High Commissioner for Human Rights).

**TABLE 5:** Breakdown of top five categories in the Event theme for China Groups

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NO. OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jasmine Revolution</td>
<td>8</td>
</tr>
<tr>
<td>June 4, 1989, Tiananmen Square Crackdown</td>
<td>4</td>
</tr>
<tr>
<td>CPC 18th Party Congress</td>
<td>2</td>
</tr>
<tr>
<td>July 2009 Urumqi Riots</td>
<td>1</td>
</tr>
<tr>
<td>Chinese New Year</td>
<td>1</td>
</tr>
</tbody>
</table>

**TABLE 6:** Breakdown of top five spoofed organizations for China groups

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NO. OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>China Group 1</td>
<td>4</td>
</tr>
<tr>
<td>China Group 3</td>
<td>3</td>
</tr>
<tr>
<td>Office of the High Commissioner for Human Rights</td>
<td>3</td>
</tr>
<tr>
<td>Open Society Institute</td>
<td>2</td>
</tr>
<tr>
<td>Chinese Human Rights Defenders</td>
<td>2</td>
</tr>
</tbody>
</table>

The volume of email submissions from Rights Group 1 and Rights Group 2 was much lower than that from the Tibet and China Groups. However, we also observed content and email senders tailored to these organizations. Rights Group 1 received messages related to human rights issues in Africa and Russia. Of the 12 emails submitted, 92% were made to appear to come from Rights Group 1 email addresses (no other organizations were spoofed). The majority of these messages were phishing attempts with lures related to IT support, designed to gain access to Rights Group 1 email credentials. Rights Group 2 submitted two email samples, both of which were related to human rights issues in the Middle East. One message was made to appear to come from a Rights Group 2 email address.

While the content analysis results clearly show targeted attacks tailored to the interests of targeted groups, content coding alone does no provide a measure of the sophistication of social engineering used in the attacks. In the following section, we describe a metric to determine relative sophistication of attacks.
TARGETED THREAT INDEX

Our dataset includes a wide range of targeted malware threats that have varying levels of complexity. This range presents a challenge in ranking the relative sophistication of the malware and targeting tactics used by attackers.

While metrics such as the Common Vulnerability Scoring System exist for the purpose of communicating the level of severity and danger of a vulnerability, there is no standardized system for ranking the sophistication of targeted email attacks. This gap is likely because evaluating the sophistication of targeting is non-technical, and cannot be automated due to the requirement of a strong familiarity with the underlying subject material.

To address this gap, we developed the Targeted Threat Index (TTI) to assign a ranking score to the targeted malicious emails in our dataset. The TTI score is intended for use in prioritizing deeper analysis of incoming threats, as well as for getting an overall idea of how severely an organization is threatened.4

The TTI Score is calculated in two parts: (Social Engineering Sophistication Base Value) × (Technical Sophistication Multiplier) = TTI Score

TTI scores range from zero to 10, where 10 is the most sophisticated attack. Scores of zero are reserved for threats that are not targeted, even if they are malicious. For example, an email from a widely-spread spam campaign using an attached PDF or XLS file to bypass anti-spam filters would score zero. Sophisticated financially-motivated malware would also score zero if it was not part of a targeted attack.

Social Engineering Sophistication

To measure the targeting sophistication base value we assign a score that ranges from zero to five, which rates the social engineering techniques used to persuade a victim to open a malicious link or attachment. This score considers the content, presentation, and claimed sender identity of the email. This determination also includes the content of any associated files, as malware is often implanted into legitimate relevant documents to evade suspicion from users when the malicious documents are opened. The features for each score are detailed in Table 7 (for examples of emails with each of these scores see Appendix A).

<table>
<thead>
<tr>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 0     | Not targeted  
   - Recipient does not appear to be a specific target.  
   - Content is not relevant to recipient.  
   - The email is likely spam or a non-targeted phishing attempt. |
| 1     | Targeted, Not customized  
   - Recipient is a specific target.  
   - Content is not relevant to recipient or contains information that is obviously false with little to no validation required by the recipient.  
   - The email header and / or signature do not reference a real person or organization. |
| 2     | Targeted, Poorly customized  
   - Recipient is a specific target.  
   - Content is generally relevant to the target but has attributes that make it appear questionable (e.g., incomplete text, poor spelling and grammar, incorrect addressing).  
   - The email header and / or signature may reference a real person or organization. |
| 3     | Targeted, Customized  
   - Recipient is a specific target.  
   - Content is relevant to the target and may repurpose legitimate information (such as a news article, press release, or a conference or event website) and can be externally verified (e.g., message references information that can be found online). Or, the email text appears to repurpose legitimate email messages that may have been collected from public mailing lists or from compromised accounts.  
   - The email header and / or signature references a real person or organization. |
| 4     | Targeted, Personalized  
   - Recipient is a specific target.  
   - Email message is personalized for the recipient or target organization (e.g., specifically addressed or referring to individual and / or organization by name).  
   - Content is relevant to the target and may repurpose legitimate information that can be externally verified or appears to repurpose legitimate messages.  
   - The email header and / or signature references a real person or organization. |
| 5     | Targeted, Highly personalized  
   - Recipient is a specific target.  
   - Email is individually personalized and customized for the recipient and references confidential, sensitive information that is directly relevant to the target (e.g., internal meeting minutes, compromised communications from the organization).  
   - The email header and / or signature references a real person or organization. |
Figure 6 shows the targeting score for organizations in our study that submitted at least 50 emails. We can see that attackers targeting these groups put significant effort into the message lures. In particular more than half of the messages targeting the Tibet Groups in Figure 6 have a targeting score of 3 or higher. This result means threat actors are taking care to make the email appear to come from a legitimate individual or organization, and include relevant information (e.g., news reports or exchanges from public mailing lists). Higher targeting scores, which result from actions such as personalizing lures to an individual in the group, or including information that requires prior reconnaissance, were rare, but we nevertheless observed cases. For example, in the case of China Group 3, we observed an email that claimed to be from one of the organization’s funders and referenced a specific meeting they had planned that was not public knowledge (social engineering score: 5).

**FIGURE 6**: Social engineering base value of emails submitted per group (minimum 50 submissions)

![Figure 6: Social engineering base value of emails submitted per group (minimum 50 submissions)](image)

**Technical Sophistication**

The technical sophistication multiplier ranks the relative technical sophistication of malware. This score is determined by measuring how well the payload of the malware conceals its presence on a compromised machine. We use a multiplier because advanced malware requires significantly more resources to customize for a particular target.
We focus on the level of obfuscation used to hide program functionality and avoid detection for the following reasons:

- It allows the compromised system to remain infected for a longer period;
- It hinders analysts from dissecting a sample, developing instructions to detect the malware, and disinfecting a compromised system; and
- Since most commonly used remote access trojans (RATs) have the same core functionality (e.g., key-logging, running commands, exfiltrating data, controlling microphones and webcams, etc.) the level of obfuscation used to conceal what the malware is doing can be used to distinguish one RAT from another.

### TABLE 8: TTI technical sophistication multiplier

<table>
<thead>
<tr>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Not protected</strong>&lt;br&gt;The sample contains no code protection, like packing, obfuscation (e.g., simple rotation of interesting or identifying strings), or anti-reversing tricks.</td>
</tr>
<tr>
<td>1.25</td>
<td><strong>Minor protection</strong>&lt;br&gt;The sample contains a simple method of protection, including: code protection using publicly available tools where the reversing method is available (e.g., UPX packing); simple anti-reversing techniques like not using import tables, or a call to IsDebuggerPresent(); self-disabling in the presence of antivirus software.</td>
</tr>
<tr>
<td>1.5</td>
<td><strong>Multiple minor protection techniques</strong>&lt;br&gt;The sample contains multiple distinct minor code protection techniques (anti-reversing tricks, packing, virtual machine / reversing tools detection) that require some low-level knowledge. This level includes malware where code that contains the core functionality of the program is decrypted only in memory.</td>
</tr>
<tr>
<td>1.75</td>
<td><strong>Advanced protection</strong>&lt;br&gt;The sample contains minor code protection techniques along with at least one advanced protection method such as rootkit functionality or a custom virtualized packer.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Multiple advanced protection techniques</strong>&lt;br&gt;The sample contains multiple distinct advanced protection techniques (e.g., rootkit capability, virtualized packer, multiple anti-reversing techniques), and is clearly designed by a professional software engineering team.</td>
</tr>
</tbody>
</table>
Figure 7 shows the technical sophistication multiplier values for emails submitted by the different organizations in our study. Our results show that malware used to target the groups in our study was relatively simple. The highest multiplier value we observed is 1.5 and even that value is seen infrequently. The majority of malware observed is rated either 1 or 1.25 according to our technical scoring criteria, with Tibet Groups observing a higher fraction of malware rated 1.25 and China Groups observing a higher fraction rated 1.

**FIGURE 7:** Technical sophistication multiplier of emails submitted per group (minimum 50 submissions)

---

**Targeted Threat Index Results Overview**

The TTI metric can help us better characterize the relative threat posed by targeted malware in several ways. Table 9 shows the technical sophistication multiplier and maximum/minimum TTI scores for malware families observed in our dataset. Since we primarily find simple malware, with a technical sophistication multiplier of 1 or 1.25, this value does a poor job of differentiating the threat posed by the different malware families to the CSOs. However, by incorporating both the technical sophistication and targeting base value into the TTI metric, we can gain more insights into how effective these threats are in practice.

If we consider the malware families with the highest technical sophistication, we can
see that their TTI values are relatively low, with scores mostly ranging from 1.5 to 4.5 (and one notable exception of 7.5). These tend to be malware families that are regularly used in targeted malware campaigns known to researchers. In particular, PlugX and PoisonIvy have been found used together in targeted attacks, and PlugX is still in active use and under continuous improvement. Despite their technical sophistication, these threats are not well executed and pose less of a risk to CSOs in which users may be able to identify and avoid these threats.

In contrast, the top five malware families in terms of TTI have lower technical sophistication multipliers (1.25) but much higher levels of social engineering. A notable exception is one highly targeted attack (social engineering score 5.0) that used PlugX (technical sophistication score 1.5) resulting in a TTI value of 7.5 (the highest score in the dataset). While this attack has a higher technical sophistication score than the top five malware families, the high TTI score is due to the level of targeting.

<table>
<thead>
<tr>
<th>TECHNICAL SOPHISTICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Family</strong></td>
</tr>
<tr>
<td>PlugX</td>
</tr>
<tr>
<td>Gh0st RAT (LURKO), ShadowNet</td>
</tr>
<tr>
<td>Conime, Duojeen, IEXPLORE, GLASSES, cxpid, Enfal, Surtr, Vidgrab</td>
</tr>
<tr>
<td>Cookies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TTI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Family</strong></td>
</tr>
<tr>
<td>3102</td>
</tr>
<tr>
<td>nAspyUpdate</td>
</tr>
<tr>
<td>PlugX</td>
</tr>
<tr>
<td>PoisonIvy</td>
</tr>
<tr>
<td>WMIScriptKids</td>
</tr>
</tbody>
</table>
Communities @ Risk

EXTENDED ANALYSIS: 2.1 Summary, Methodology and Data Analysis

ANALYZING COMMERCIAL SPYWARE WITH THE TTI

Attacks using advanced commercial spyware such as FinFisher and DaVinci RCS do not necessarily rank higher on the TTI.

We analyzed a sample of FinFisher used against Bahraini activists and evaluated it with the TTI. The malware sample is technically advanced, scoring a 2.0, as a result of multiple advanced protection techniques, including a custom-written virtualized packer, MBR modification, and rootkit functionality. However, the email used in the attack is poorly customized and has several attributes that made it look suspicious to the intended target. The email attempts to reference an NGO called Bahrain Center for Human Rights, but mistakenly refers to it as “Human Rights Bahrain.” The message also lists the wrong name for the acting president of the group. It appears to come from a real journalist, Melissa Chan of Al Jazeera, but provides a suspicious gmail address (melissa.aljazeera@gmail.com). These attributes give the email a social engineering base value of 2. As a result, the attack scores an overall TTI score of 4.0, which is relatively low compared to many other attacks seen in our study. This result shows the importance of social engineering tactics: FinFisher is only effective if it is surreptitiously installed on a user’s computer, which in some cases requires opening a malicious file (however, both FinFisher and Hacking Team offer optional network injection products that permit remote attackers to infect a device without user interaction).

---

From: Melissa Chan <melissa.aljazeera@gmail.com>
To: 
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.
Similar results can be observed with respect to attacks using DaVinci RCS, developed by Italy-based company Hacking Team, which has been used against activists and independent media groups. RCS also scores a 2.0 on our technical sophistication scale. We analyzed a targeted attack using RCS against a dissident in the United Arab Emirates. The email appears to come from “Arabic Wikileaks” (arabic.wikileaks@gmail.com) and asks the recipient to read a “very important message.” Again, while the malware used in these attacks is technically sophisticated, the social engineering lure is poorly customized (social engineering base value 2), resulting in an overall TTI score of 4.0.

These results suggest that different threat actors possess varying levels and types of resources, and as a result use different attack methods. The majority of malware submitted in our study appears to be from actors that have in-house malware development capabilities, and the capacity to organize targeted campaigns. However, as this report shows, in many cases they spend significant effort on social engineering, but generally do not use technically advanced malware. Conversely, operators of FinFisher and DaVinci RCS have purchased advanced malware products, but in some cases paired them with relatively unsophisticated social engineering.

End of section. Find the full report at targetedthreats.net
EXTENDED ANALYSIS:

2.2
Cluster Analysis
Targeted malware attacks are typically not discrete events. Rather, they are a part of systematic campaigns that use common malware, C2 infrastructure and social engineering tactics to target groups repeatedly over long periods of time. Threat actors using common tools and techniques may target multiple groups within a community.

To cluster attacks into campaigns, we analyze technical and contextual indicators to identify patterns. Where possible we draw connections between these clusters and previously reported campaigns and threat actors.

Malware attacks are clustered into campaigns by commonalities and patterns across the following indicators:

- Email headers: Originating-IP or common email addresses seen in Reply-To, Sender or Envelope-From email headers.
- Shared C2 infrastructure: Domain names and IP addresses to which malware beacons and/or from which it downloads additional modules.
- Static analysis: Commonalities between unusual strings or data structures seen in the malware samples or the files they drop.
- Malware development: Observable changes made to specific malware families over time.
- Social engineering tactics: Contextual patterns in targeted organizations, spoofed senders, and content of messages.

Based on the attributes described above, we identify 10 distinct campaigns, which we present in detail in the following sections.
IEXPLORE Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>August 3, 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>May 21, 2012</td>
</tr>
<tr>
<td>Exploits</td>
<td>Windows: CVE-2010-0188; CVE-2010-3333</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Windows: IEXPLORE RAT (aka C0d0s0)</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 domains:</td>
</tr>
<tr>
<td></td>
<td>sixday.wikaba.com</td>
</tr>
<tr>
<td></td>
<td>msupdate02.selfip.com</td>
</tr>
<tr>
<td></td>
<td>msupdate02.selfip.info</td>
</tr>
<tr>
<td></td>
<td>xinxin20080628.gicp.net</td>
</tr>
<tr>
<td></td>
<td>humanbeing2009.gicp.net</td>
</tr>
<tr>
<td></td>
<td>saveworld.gicp.net</td>
</tr>
<tr>
<td></td>
<td>xinxin20080628.gicp.net</td>
</tr>
<tr>
<td></td>
<td>204.134.116.229</td>
</tr>
<tr>
<td></td>
<td>60.167.78.229</td>
</tr>
<tr>
<td></td>
<td>116.226.49.148</td>
</tr>
<tr>
<td></td>
<td>123.147.81.121</td>
</tr>
<tr>
<td></td>
<td>204.134.116.229</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, China Group 1, China Group 2</td>
</tr>
<tr>
<td>TTI range</td>
<td>2.5 - 5.0</td>
</tr>
</tbody>
</table>

BACKGROUND

The IEXPLORE campaigns involved custom-developed Windows malware targeting four of the study groups with a unique email and delivery method used for each attempt. Each email was tailored specifically for the target in terms of subject, content, and the way the malware was attached and hidden. In addition, there was evidence that the malware was under active development during the campaign. The IEXPLORE campaigns serves as a typical example of “APT”- style operations.
CAMPAIGN TIMELINE

Attacks in this campaign are linked by the use of IEXPL0RE RAT, which provides standard RAT functionality, including keylogging, file extraction, and control of microphone and webcam peripherals.5

We identified the IEXPL0RE campaign through analysis of three separate attacks using this malware that were sent to China Group 1, China Group 2, and Tibet Group 1. This first series of attacks clearly shows how the attackers carefully customized social engineering tactics to the interests of the three different groups.

Evidence of this campaign first emerged in an August 3, 2010 email to Tibet Group 1 that referenced a protest against the Shanghai Expo in Japan. The malicious attachment was a PDF using CVE-2010-0188 to deploy IEXPL0RE RAT.

---

Social engineering 2
Technical 1.25
TTI 2.5
MD5 6b04821ad588b0f918318064a07dd5d6
C2 msupdate02.selfip.com

On November 11, 2010, China Group 1 received multiple emails addressed to the organization’s director claiming to be from personal friends. The emails included an executable attachment in a password-protected archive, with the password provided in the body of the email. Packaging attachments in a RAR file makes them less likely to be discovered by an AV scanner. Password protecting the archive reduces the chances of AV detection even further. When executed, the malware connected to softwareupdate.8866.org (119.75.218.45). The level of personalization used in the message gives it a social engineering score of 4 and a total TTI of 5.0.

On November 19, 2010, China Group 2 received an email containing a story about a high-profile, high-rise apartment building fire in Shanghai. The message was written in Chinese and repurposed text from a news article on the event.

Attached to the email were four images and two executable files (.scr extensions) designed to look like images using the Unicode right-to-left override character. When each executable file is run, it will install and launch the malware, drop an image, open the image, and delete itself. The malware connects to xinxin20080628.gicp.net (114.60.106.156). The attack has a social engineering score of 3 and a total TTI of 3.75.

**FIGURE 8:** Image of a high-rise fire used to trick recipients into running the malware
The remaining attacks we analyzed targeted Tibetan groups exclusively.

On December 2, 2010, Tibet Group 1 received an email that included an Excel spreadsheet attached to an email that appeared to be from organizers of a conference on climate change.

---

From: Tenzin Tsundue <tentsundue@yahoo.com>
Subject: FW: It's time for climate action!

As some of you may know, GAIA is preparing to attend the COP 16 in Cancun as part of our campaigning on climate and waste issues. We'll be advocating for recycling as a climate change mitigation strategy, and trying to stop climate finance for incineration and landfill gas systems. Once more, we'll be proclaiming loud and clear that waste-to-energy technologies are a waste-of-energy and making alliances with other social movements for climate justice.

If you haven’t yet, get in touch with us to join in this amazing action time for climate justice and against waste-of-energy technologies!!
E-mail me to arrange how to meet up in Cancun and let’s plan further!!

Furthermore, we’re working on two action letters that we want to bring forward in these negotiations:

1. The first letter is to demand the creation of a Global Fund that will be directly accessible by wastepickers and other civil society groups; this would be the best way to support resource recovery programmes that reduce GHG emissions and ensure decent livelihoods for all workers in the recycling economy.

2. The second letter is to stop climate finance support to incineration and landfill gas systems, highlighting some of its major problems: energy from WTE is not renewable nor green but the opposite, it generates a huge amount of GHG emissions that should be counted instead of disguised, and it emits an amount of pollution far beyond what the Stockholm Convention allows, and no-one wants.

If you have the chance to arrange a meeting with climate negotiators in your country or in Cancun, please get in touch and we will provide more insight into these demands, as well as materials and preparation to have such conversations.

Looking forward to hearing from all of you soon, whether that is in Cancun or from your local community actions!

1 attachment: Contact.xls 141.0 KB
On January 11, 2011, Tibet Group 1 received an email about an annual review of Tibetan human rights issues that contained an executable file designed to appear to be a video of a speech by HHDL.

In July 2011, IEXPL0RE was sent to Tibet Group 1 again. This time it used a .rar archive file containing a malicious .hlp file.

Tibet Group 1 received two more emails with IEXPL0RE in late December 2011 and early January 2012. On December 22, an email referencing Uyghur refugees
was received; on January 6, an email in Chinese about Taiwan issues copied from a blog post was received. Both had .rar attachments with the same file, which used CVE-2010-3333. Each of these emails score a social engineering base value of 2.0, and a technical score of 1.25 for an overall TTI of 2.5.

On May 21, 2012, a newer version of the RAT payload was distributed via email in multiple RTF documents to Tibet Group 2. This attack was coupled with a higher degree of social engineering. Separate emails with the same payload and content were sent to both the Executive Director and Program Coordinator, addressing them by name. The email contained an invitation to a legitimate event and included the email signature of a real person, with an attached file purporting to contain information about the event. The sender notes that the recipients were identified as contacts for HHDL, and asks them for help contacting His Holiness in order to invite him to the event. This level of personalization gives the attack a social engineering score of 4 (total TTI 5.0)

The attached RTF file drops a DLL alongside a legitimate program vulnerable to DLL hijacking, allowing the malware to run without a warning to the victim that it is not digitally signed. StrokeIt, a program for using mouse gestures, uses a file named config.dll without verifying the authenticity of the file. By replacing config.dll with the RAT downloader, the malicious code is run while appearing legitimate to the operating system (see Figure 9).

**FIGURE 9:** Valid digital signature for StrokeIt program, which is used to launch malicious config.dll file

---

**OBSERVATIONS**

This series of attacks represents a typical ‘APT’-style campaign. Multiple groups were targeted, with each attack custom developed for each group, including tailored social engineering. The evolution of the RAT payload, as seen in the series of samples targeting Tibet Groups, suggests that the malware was under active development. The social engineering tactics and development cycles observed in this campaign demonstrates the organized and persistent nature of the attackers.
Mobile Malware

BACKGROUND

The use of malware targeting mobile platforms in espionage campaigns is relatively rare, but is likely a vector that will become more common due to the increasing ubiquity of mobile computing.

During investigations of C2 servers associated with the Luckycat campaign, Trend Micro found two malicious Android APKs in early stages of development that could collect device information, as well as download and upload files by remote command. Based on the available information, it was unclear how the attackers intended to deliver the mobile malware to targets.

In 2013, researchers at Kaspersky reported the compromise of an email account of a high-profile Tibetan activist that was then used by attackers to send targeted malware to the activist’s contacts. The emails referenced the World Uyghur Congress and included a malicious APK file that appeared to be an application with information on the event. The malware allowed attackers to collect data from infected devices including contacts, call logs, SMS messages, geolocation, and phone data (phone number, OS version, phone model, and SDK version).

Researchers in our group have also found evidence of commercial surveillance products that target multiple mobile platforms (e.g., Android, IOS, BlackBerry, Symbian) developed by Hacking Team and FinFisher.

In other recent work, researchers found that participants in the Occupy Central protests in Hong Kong received links through WhatsApp to an Android application that appeared to be associated with the protest organizers, but was actually malware that could send a variety of information back to attackers.

In our study, we identified the use of compromised Android applications sent as part of a targeted attack against a prominent figure in the Tibetan community. This attack lever-
aged a genuine email that was likely exfiltrated by attackers, and attached compromised versions of the chat application KakaoTalk and mobile radio application TuneIn.\(^6\)

**VECTOR OF ATTACK**

On December 4, 2012, an information security expert who works within the Tibetan community sent a private email to a member of the Tibetan Parliament in Exile, based in Dharamsala, India. That email attached genuine versions of Kakao Talk\(^7\) and TuneIn\(^8\) as APK files.

On January 16, 2013, an email purporting to be from this same information security expert was sent to a high profile political figure in the Tibetan community. The email contained the same text as the message from December 4, but attached compromised versions of the Kakao Talk and TuneIn Android APKs.

In order for the malware to be installed, the user must permit applications to be installed from sources other than the Google Play store. This permission is not enabled by default in Android. However, as many members of the Tibetan community (particularly those living in Tibetan areas in China) have restricted access to the Google Play service, they are required to permit applications to be installed from outside sources. It is common for APKs to be circulated outside of Google Play. In addition to permitting the “allow from unknown sources” option, the user must also approve the additional permissions requested by the application. Users may be duped into accepting these permissions by assuming they are required for the regular functionality of the application or by not reviewing them carefully before approving. Once these permissions are approved, they are used to authorize the additional data-gathering capabilities of the malware, which is configured to autostart on device boot.

We later confirmed that the original recipient of the legitimate email had his email account compromised. Therefore, it appears likely that the attackers harvested the

---


\(^7\) KakaoTalk is a chat app that is developed by a South Korean company (Kakao Corporation). Members of the Tibetan community have used KakaoTalk and other applications as alternatives to WeChat (another chat app popular in Asia) after concerns were raised regarding that application’s general security and the potential for Tencent (the China-based developer of WeChat) to monitor users at the behest of the Chinese government.

\(^8\) TuneIn is a media player application for listening to Internet Radio. TuneIn is used by Tibetans to listen to streams such as Voice of America’s Tibetan service, to engage with their culture, and to stay on top of world news.
original email from the compromised account, and over the course of a few weeks developed malicious versions of the attached APKs. The use of private information in this attack gives it a social engineering score of 5. The technical score of the malware is 1.25 (see the section below for details on the malware’s functionality). The total TTI is 6.25.

MALWARE ANALYSIS

The functionality and certificates used for the malicious versions of the KakaoTalk and TuneIn APKs are identical. Both applications were repackaged into modified APKs and signed with an illegitimate certificate (KakaoTalk malware MD5 cbc474e34f26b4afd-02932d8cae9e401 Tunein Malware MD5 ba760392f171e2f05d0352cc1e00190c). Below, we reproduce the original and fake certificates used for KakaoTalk. Notice that fields in the illegitimate certificate have been populated with what appears to be an assortment of nonsensical characters from a QWERTY keyboard:

Original legitimate certificate:

```
Owner: OU=kakaoteam, O=kakao, C=ko
Issuer: OU=kakaoteam, O=kakao, C=ko
Serial number: 4c707197
```

Illegitimate certificate:

```
Owner: CN=qwe, OU=asd, O=zxc, L=rty, ST=fgh, C=vbn
Issuer: CN=qwe, OU=asd, O=zxc, L=rty, ST=fgh, C=vbn
Serial number: a3e5475
```
The following permissions are added by the malware that do not exist in the legitimate version:

```
android.permission.GET_ACCOUNTS
android.permission.ACCESS_NETWORK_STATE
android.permission.READ_SMS
android.permissionINTERNET
android.permission.ACCESS_FINE_LOCATION
android.permission.WRITE_SETTINGS
android.permission.WRITE_SECURE_SETTINGS
android.permission.WRITE_APN_SETTINGS
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.PROCESS_OUTGOING_CALLS
android.permission.DEVICE_POWER
android.permission.ACCESS_CHECKIN_PROPERTIES
android.permissionINTERNET
android.permission.CHANGE_WIFI_STATE
android.permission.MODIFY_PHONE_STAT
android.permission.BLUETOOTH_ADMIN
android.permission.BLUETOOTH
android.permission.BIND_DEVICE_ADMIN
android.permission.USERS_POLICY_FORCE_LOCK
android.permission.CHANGE_CONFIGURATION
```

Note that two of the additional permissions requested by the malware are misspelled, rendering these permissions unusable:

```
adnroid.permission.ACCESS_CHECKIN_PROPERTIES
adnroid.permission.CHANGE_WIFI_STATE
```
The malicious versions of both applications have the same functionality enumerated below:

- On a periodic basis the user’s contacts, call history, SMS messages, and cellular network configuration are written to an encrypted file called info.txt.
- The malware periodically contacts the C2 server “android.uyghur.dnsd.me” to retrieve updated configuration information, such as URLs and login credentials. This configuration information directs the malware to an upload location for the info.txt file. The site hosting the C2 appears to emulate the appearance of the Baidu website (a Chinese search engine), but includes encrypted configuration data hidden in the comments. By masking the C2 as a seemingly innocuous website, requests would appear to be legitimate on casual inspection. The configuration data contained in the comments directs the malware to upload captured data from the device to an FTP server and contain a pointer to a new C2 that would allow the attackers to change the C2 should that need arise.
- The malware intercepts SMS messages and searches for a special code sent by the attacker, which, if detected, responds to the sender with the base station ID, tower ID, mobile network code and mobile area code of the infected phone in question. This message is not displayed to the user, and they are never made aware of it.

**OBSERVATIONS**

The compromised Android applications that we detected as part of our study, as well as mobile malware described by other security researchers, show that mobile devices are indeed targets for espionage attackers. These attacks serve as early examples of a trend that seems likely to grow alongside the rapid spread of mobile computing.

As described above, there are particular security risks for users residing in locations where access to standard secure channels for installing mobile applications is restricted. As users are required to distribute and install APKs of unknown provenance, they are at increased risk of malicious applications, particularly if those applications use fake certificates (as was the case in this attack).
OS X Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>May 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>Early 2013</td>
</tr>
<tr>
<td>Exploits</td>
<td>CVE-2009-0563; CVE-2011-3544; CVE-2012-0507 ; CVE-2009-3129</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Revir/IMuler, Olyx / Lamadai / PubSab, MacControl</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 domains: freeavg.sytes.com (Olyx.C), mail.hiserviceusa.com (Olyx.C), yahoo.xxuz.com (Olyx.C), coremail.info (SabPab.A), rtx556.onedumb.com (SabPab.A), <a href="http://www.teklimakan.org">www.teklimakan.org</a> (iMuler), IPs: 112.213.126.118 (Olyx.C), 100.42.217.91 (Olyx.C), 198.74.124.3 (SabPab.A), 199.192.152.100 (SabPab.A), 61.178.77.158 (MacControl)</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 3, Tibet Group 4</td>
</tr>
<tr>
<td>TTI Range</td>
<td>2.0 - 3.75</td>
</tr>
</tbody>
</table>

BACKGROUND

While Windows was the most commonly targeted operating system in our study, it was not the only platform targeted. Malware targeting OS X is increasingly paired with Windows malware, giving attackers a better chance of compromising the machine, whatever the operating system. This approach can take the form of code that determines the target’s operating system, such as a web page that uses JavaScript to detect the operating system and then download a cross-platform exploit with appropriate payload.

Four of the Tibet Groups in the study received targeted malware specifically designed for OS X. Tibet Groups 1, 2, and 4 received emails with malware in an attachment or link. Malware was detected on the network of Tibet Group 3 by a NIDS on their office network.

The OS X malware seen in our study ranges in sophistication from simple programs...
that rely entirely on social engineering, paired with targeted emails that are not customized for the target (TTI: 2.0), to moderately customized emails with malware that has minor code protection (TTI: 3.75). While the technical sophistication of the malware does not vary widely, all of the malware families observed show active and consistent development over the course of the study.

**MALWARE ANALYSIS**

The malicious emails used a combination of social engineering, and exploits against a variety of vulnerabilities, to install malware on the victim’s computer.

The vectors we observed include:

- An attached .zip file containing an executable
- An attached Word document using CVE-2009-0563
- A link to a Java .jar file using CVE-2011-3544
- A link to a Java .jar file using CVE-2012-0507

The subject and body text of all of the emails targeting the Tibet Groups contained information relating to Tibetan news and activities (e.g., current world events, upcoming rallies, and self-immolations).

We see Word document vectors first being sent in early 2013. Interestingly, these attacks use a vulnerability made public back in 2009. The use of this vulnerability may be due to the Java vulnerabilities having a higher chance of being patched by the Tibetan community, after they received substantial media attention. However, as the Word documents were all part of one campaign, it is likely just coincidence, as an email carrying the later Java vulnerability was received while the Word campaign was still underway.

We observed three malware families targeting OS X, all of which are simple RATs with low technical sophistication scores:

- Revir/IMuler (technical score: 1.0)
- Olyx/Lamadai/PubSab (technical score: 1.0)
- MacControl (technical score: 1.25)
Revir / IMuler

Revir and IMuler are names for individual components of one particular targeted attack for OS X, and are often used interchangeably. Revir is the name for the “dropper” or shell program that deploys the embedded malicious payload (in this case, IMuler), as well as a clean payload that is then opened to distract the user.

The clean payload that is used can differentiate the early variants of Revir that we have seen. Using the F-Secure naming scheme Revir.A carries a PDF and Revir.B carries a JPG. Later variants Revir.C and Revir.D allow for any type of clean decoy file, and also encrypt the payload.

IMuler acts as a simple remote access trojan, providing the attacker with the ability to upload and delete the victim’s files, download and run additional malware, and take screenshots. The variants we observed have no reverse engineering protection in the code, although later versions starting with IMuler.B will look for the Wireshark network analyzer and stop running to evade analysis if it is found.

We observed two attacks against Tibet Group 1 using the Revir/IMuler combination. The first, an email sent in May 2011, was a combination of Revir.B and IMuler.A and was the earliest Mac malware attack seen in the study. This email’s contents were about a legitimate event featuring HHDL. The second email, sent in September 2011, stepped up the attack by containing both Revir.A/IMuler.A and Revir.B/IMuler.A combinations. This email purported to be from a legitimate Tibetan rights organization and referred to an upcoming event.
The attack in September 2011 is particularly interesting because the Revir/IMuler components show very clear development progress compared to the version sent in May. The May version is a two-stage program. The initial program dropped as /tmp/host downloads a second program as /tmp/updtdata, which is then used for communication with the C2 server. The September version integrates the second program into the first, merging functionality. This change means that the download of a second executable is not required, eliminating a more suspicious component of the infection process.

The malware version sent in September 2011 was also used in another campaign reported by Eset in March 2012, using photos of a topless model as the lure to run the attachment.

**MacControl**

On September 7, 2012, we identified an attack targeting Tibet Group 2 using another malware family, MacControl. The samples seen from this family have a technical score of 1.25
This email repurposed content from Radio Free Asia and claimed to contain a list of self-immolations giving it a social engineering score of 3 (TTI 3.75). The attached executable connects to a C2 server at 61.178.77.158:80 and functions as a standard RAT.

Another email received by the same organization three weeks later contained a malicious Excel file that installed Gh0st RAT with the variant-identifying text LURK0. This RAT shared the same C2 as the MacControl, connecting back to 61.178.77.158 on port 8080.

This paring of MacControl with Gh0st RAT has been used in attacks against Uyghur users, as reported by Kaspersky and AlienVault.

Outside of our study participants, we have also seen MacControl campaigns similar to those reported by Kaspersky and AlienVault, targeting Tibetan and Uyghur communities. These differ slightly than those described above in that they use different flag text in the Gh0st RAT component, and connect to a nearby IP (61.178.77.169). They are also delivered using a Word vulnerability, while the email sent to the in-study recipient contained an executable inside a .zip file.

**Olyx / Lamadai / PubSab**

Olyx, Lamadai, and PubSab (or SabPub) are variants of the same malware that are differentiated by the C2 server used and the location where the malware hides on a compromised system. These names are often used interchangeably by different antivirus or security companies. Further complicating matters, there is often overlap between names: for example, Olyx.C is the same as Lamadai.B.
Olyx.A
» Threat location: /Library/Application Support/google/startp
» Launcher: ~/Library/LaunchAgents/www.google.com.tstart.plist

Olyx.B (Lamadai.A)
» Threat location: /Library/Audio/Plug-Ins/AudioServer
» Launcher: ~/Library/LaunchAgents/com.apple.DockActions.plist

Olyx.C (Lamadai.B)
» Threat location: Applications/Automator.app/Contents/MacOS/DockLight
» Launcher: ~/Library/LaunchAgents/com.apple.DockActions.plist

PubSab.A
» Threat location: ~/Library/Preferences/com.apple.PubSabAgent.pfile
» Launcher: ~/Library/LaunchAgents/com.apple.PubSabAgent.plist

Olyx.C was observed in emails sent to Tibet Group 1, and via a NIDS on the network of Tibet Group 3.

The campaign against Tibet Group 1 consisted of five emails that contained links to malicious .jar files that exploited Java vulnerabilities (CVE-2011-2544 or CVE-2012-0507). All of these emails appeared to come from real people or organizations, and referenced Tibetan themes giving them a social engineering score of 3. The malware is basic with a technical score of 1. The total TTI is 3.
FIGURE 12: Olyx/Lamadai/PubSab attacks

On January 29, 2013, the NIDS on the network of Tibet Group 3 detected evidence of a Java vulnerability being used to serve multi-platform malware pretending to be Adobe Flash Player. This sample was distributed through a web page that does web browser user agent detection. Tibet Group 3 did not submit any emails containing this link, so the specific attack vector used is unclear.

The website hosting the malware was hxxp://services.addons.mozilla.publicvm.com, and had an .xpi file for Firefox and a .jar containing Olyx.C for Mac. The way the malware was served was different than other similar attacks in that it checked both browser and OS, not just OS, to determine which malware program would be used.

On February 5, 2013, we received additional alerts that showed similar malicious pages were visited by Tibet Group 3, again without indication of the original attack vector. A web page was flagged by the NIDS due to a suspicious encoded string that decoded to a tinyurl.com redirector. This link led to a page on hxxp://adobeupdate.publicvm.com, which had attacks for IE, Firefox, Java (Windows, but not OS X), and...
a standard Windows binary. There may also have been an OS X attack, but we were unable to locate it from the information recorded by the NIDS.

The original page that served up the attack also had a distinctive comment in the script that identified it as a legitimate script from the website of the US State Department (www.state.gov). At the time of our analysis the server was hosting 100 other domains. The www.state.gov script we found on the page suggests the IP was hosting a fake US State Department website that included the malicious link.

**OBSERVATIONS**

Mac OS X was once commonly seen as a more secure alternative to Windows. Targeted groups in the Tibetan community shared this assumption. For example, in a 2008 *Washington Post* article on targeted attacks against Tibetan groups, a volunteer providing technical assistance to a Tibetan NGO noted that the group had attempted to mitigate attacks by using “more secure platforms such as Apple computers.” While the number of malware vectors targeting OS X is small compared to the many vulnerabilities used against Windows targets, it is clear that OS X malware is becoming an important tool for attackers targeting human rights organizations. All of the malware families described here are under active development and we will likely see more attacks targeting OS X at greater levels of technical sophistication.
DNF Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>November 26, 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>March 4, 2013</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td></td>
<td>Mac: CVE-2011-3544</td>
</tr>
<tr>
<td>Malware Families</td>
<td>cxgid, FAKEM (HTML variant), Olyx, Scar.hikn</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>China Group 1, Tibet Group 1, Tibet Group 2, Tibet Group 4</td>
</tr>
<tr>
<td>TTI Range</td>
<td>2.5 - 5.0</td>
</tr>
</tbody>
</table>

**BACKGROUND**

We identified the Domain Name Family (DNF) campaign by clustering attacks together on the basis of a set of malware families that communicate with domains registered under a series of suspicious names.

Analysis of attacks using Olyx Scar.hikn, cxgid, and FakeM malware families revealed that these samples connect to a set of domains that are registered to series of names: Mily Luna, Philip Fischer (adonis.fischer@yahoo.com), William Bottle (john.fielder@hotmail.com), and XieZhong Customer. Searching through domain registration information revealed a large number of domains registered under these names in a short time frame that were related to Tibet, Japan, education and business. All of these domains used a common hosting company called XinNet. Most of these domains have since expired, but historical registration data can be retrieved using services such as [DomainTools](#).
The registration information provided by “Mily Luna” includes conflicting fields (i.e., address in Nepal, but city and province as Hong Kong SAR), which further demonstrates that this information does not reflect a real user:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>miyazakihousou.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>PunnyCode</td>
<td>miyazakihousou.com</td>
</tr>
<tr>
<td>Creation Date</td>
<td>2009-02-01 10:53:24</td>
</tr>
<tr>
<td>Updated Date</td>
<td>2012-02-11 10:51:20</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>2013-02-01 10:47:33</td>
</tr>
</tbody>
</table>

Registrant:
- Organization: mily luna
- Name: mily luna
- Address: No.358, dapho road, Kathmandu, Nepal
- City: xianggangtebiexingzhengqu
- Province/State: xianggangtebiexingzhengqu
- Country: china
- Postal Code: 2000000

Some of these C2 domains are registered using email addresses at xiezhong.com. Through domain registration records, we were able to find more than 25 additional domains connected to this cluster, including many registered to “John Smith” (world-freeusa@gmail.com). While we did not see any malicious activity related to these domains, some of the domains are suspiciously named (kaspersky-ru.org, kaspersky-us.org, thetibetpost.net). In the case of kaspersky-us.org in particular, VirusTotal shows that only 1/51 antivirus products detect the site as malicious, but the one that does is made by Kaspersky. VirusTotal also includes a URL query report showing thetibetpost.net as malicious.

Figure 13 illustrates the connections between malware families, C2 domains, and the domain registrants in the DNF campaign. One FakeM sample used one of the Mily Luna and Xie Zhong domains as C2s. FakeM has been observed being used in conjunction with cxgid by other researchers, but we have not seen other reports identifying the infrastructure found in this cluster.
ADAPTIVE ATTACKERS

We observed DNF Campaign attacks between November 2010 and March 4, 2013 that targeted Tibet Group 1, Tibet Group 2, and Tibet Group 4. The social engineering scores of these emails were between 2-3 and the technical scores of the malware were 1.25 (TTI 2.5 – 3.75). In June 2011, we were sent an automated AV detection notice from China Group 1. The alert identified a sample that was also sent in emails to Tibet Group 1, and which connected to the DNF-related domain upgrade. support-microsoft.com. This link suggests a staff member of China Group 1 likely received a malicious email from the DNF campaign and opened the payload, triggering the AV detection.
Initially, attacks in this campaign exclusively used Windows malware. However, the attackers demonstrated their ability to quickly adapt tactics to meet new requirements.

On February 23, 2012, an email was sent to the director of Tibet Group 1. It addressed the director personally and appeared to come from Mr. Cheng Li, a prominent China scholar based at the Brookings Institution. The email requests the assistance of Tibet Group 1 in verifying information on Tibetan self-immolations. The name and title provided in the email all match real details for Mr. Cheng Li provided on his Brookings Institute staff page.

The director of Tibet Group 1 noted to us that at first it was flattering to be asked to consult a well-known China expert on Tibetan issues. However, the director quickly noticed that the email was sent from a suspicious AOL account (chengli.brookings@aol.com). This account appears to have been registered by the attackers for this specific attack. Attached to this email was an Excel spreadsheet that used CVE-2009-3129 to install cxgid malware. The malware connects to mail.miyazakihousou.com (112.213.126.18), which is a domain registered under the name Mily Luna.

---

**Social engineering** 4

**Technical** 1.25

**TTI** 5.0

**MD5** 64e2d3b91977bb0c293cac3e97669f03

**C2** mail.miyazakihousou.com (112.213.126.18)
The director of Tibet Group 1 flagged this message to us as one of the most targeted messages they had ever received. After consultations with Tibet Group 1, we decided to run an experiment on the attackers to test how responsive they would be to interaction from a target. Working with the director, we crafted a reply to “Cheng Li” and sent it on March 2:

“Thank you for your inquiry. I’d be happy to help out—I’m having trouble opening the document on my mac though, I think there may be an issue with the Chinese character font? I think if you sent me a Word version that might be easiest, as it would also allow me to make comments in the document.”

On March 6 “Cheng Li” replied, apologizing for his late response due to work-related travel. He encouraged the director to review information on Tibet issues on a website. The link provided pointed to a website containing a Java vulnerability that had payloads for both Windows and OSX systems. The payload for Windows was the same cxgid sample sent in the original email. The payload for OSX was Olyx and connected to mail.hiserviceusa.com (112.213.126.118). Both the malicious website and C2 were domains registered under the name Mily Luna.
### OBSERVATIONS

While other malware campaigns we identified typically use free subdomains, this cluster primarily relied on registered domains. The use of registered domains provided a useful variable around which to cluster attacks. Registered domains can also be blacklisted more easily than free services providing subdomains.

The DNF Campaign also demonstrates the adaptability of the attackers. Upon receiving a message from Tibet Group 1 indicating the targeted user was using a Mac, the attackers quickly responded with malware targeting OS X.
APT 1 Campaigns

| First Seen | April 2010 |
| Last Seen  | August 16, 2012 |
| Exploits    | N/A |
| Malware Families | Bangat, GLASSES, WARP, WEBC2-QBP |
| Infrastructure | C2 domains: ash22ld.compress.to, ewplus.com (compromised site), johnbell.longmusic.com, 66.228.132.8 (hard coded ip) |
| Targeted Groups | Tibet Group 1, Rights Group 1 |
| TTI Range   | 5.0 |

BACKGROUND

On February 19, 2013, Mandiant released a report that shed light on a prolific cyber espionage group they call APT1 (also referred to as “Comment Crew” or “Byzantine Candor”), which had targeted a large number of organizations in a wide range of industries, stealing terabytes of data. Mandiant’s report traced APT1 operations to China and claims that the group may in fact be the Second Bureau of the People’s Liberation Army General Staff Department’s Third Department, also known as Unit 61398.

APT1 has been active since at least 2006. Mandiant has observed the group breaching 141 organizations from 20 major industry sectors. Within Mandiant’s report there is no mention of CSOs as targets among these compromised organizations. However, in previous reports and released datasets, there are indications that civil society is targeted by APT1. Both Mandiant and Shadowserver have included a Tibetan-themed domain (tibethome.org) in their APT1-related domain lists, which suggests that Tibet-related organizations may have been targeted, but no further details on Tibet-related operations were included. In 2012, a Bloomberg article listed the nonprofit organization International Republican Institute among target organizations compromised by APT1 in June 2011, but no technical details of the attack were released.
In the course of our study, we found evidence that APT1 targeted Tibet Group 1,\(^\text{10}\) and successfully compromised the networks of Rights Group 1.

**TARGETING TIBET GROUP 1**

On April 28, 2010, the director of Tibet Group 1 was sent an email from a Yahoo! webmail address. The sender makes a personal plea to Tibet Group 1 to help find his Tibetan wife who he claimed went missing since after visiting Tibet.

![Email example](image)

Some details of the email immediately flag it as suspicious: the name in the email address is “Nate Herman” although the email body is signed “Martin Lee.” The forwarded email included full headers, so we were able to obtain more information about its origin (Yahoo! includes the sender’s source IP in the headers when an email is sent over the webmail interface). In this case, the originating IP was 69.95.255.26, which

---

\(^{10}\) We originally published analysis of the APT1 related attack against Tibet Group 1 in a blog post, Hardy, S. APT1’s GLASSES – Watching a Human Rights Organization, February 25, 2013, [https://citizenlab.org/2013/02/apt1s-glasses-watching-a-human-rights-organization](https://citizenlab.org/2013/02/apt1s-glasses-watching-a-human-rights-organization)
is registered to One Communications, Inc. / EarthLink Business, and is very close to IPs used in a similar attack—demonstrating that this attack is not isolated, and the IPs are likely being reused for other malware campaigns.

This email contains a link to a ZIP file located at hxxp://tcw.homier.com/attachments/details.zip (MD5: 6fb3ecc3db624a4912d-dbd2d565c4995). The “homier.com” domain belongs to Homier Distributing Company, Inc. and appears to have been compromised. A search for this subdomain shows other instances of malware hosted there, including a case detailed in a ThreatExpert report describing a malicious file stored in /images/update.bin, and another malicious program getting the file /attachments/SalaryAdjustment.zip.

Analysis of the files revealed malware that shares a number of similarities to malware described in Mandiant’s APT1 report that they call “GOGGLES” —a simple downloader that is controlled via encoded markers in files accessed over HTTP. The malware sent to Tibet Group 1 shares both a large percentage of code and the same C2 infrastructure as the program described in the APT1 report, which suggests the two pieces of malware are both used by APT1.

We call this malware GLASSES because it is related to GOGGLES, and used a compromised eyeglasses storefront website as its C2 server. The GOGGLES code is more sophisticated than the GLASSES code. In addition to a more effective method of hiding the command data, it also has more countermeasures to protect against reverse engineering and hide itself on the infected system. For this reason, it is very likely that GOGGLES is a later version of GLASSES.

COMPROMISING RIGHTS GROUP 1

In August 2012, Rights Group 1 was made aware of a serious compromise of their network infrastructure. Following incident response from a third party, Rights Group 1 shared workstation hard drives with the Citizen Lab that were suspected to have been compromised as part of the intrusion. The attackers had access to the network infrastructure of Rights Group 1 from January 2011 to August 2012. During this time the attackers were able to move laterally through the network, install RATs, extract sensitive data and passwords, and impersonate staff identities. The incident affected computers beyond the ones to which we had access, but these hard drives provide enough data to reveal malware and C2 infrastructure that is linked to APT1.

We conducted forensic analysis of six Windows workstation hard drives used by Rights Group 1 staff members. This analysis found that three of the drives were compromised by multiple versions of malware that matched a tool used by APT1 called Bangat, which is used to
establish footholds in a network and maintain persistence. Bangat has standard back-
door functionality, including features to start keyloggers, gather system information,
and take screenshots.

Comparing the samples retrieved from the compromised hard drives to Bangat
samples available from the Contagio APT1 malware collection reveals close similari-
ties. Rights Group 1 samples included the same functionality and important strings as
the APT1 contagio samples. These included temporary file names (~MC_[#]~, where #
are numbers) and DES key (!b=z&7?cc,MQ>) used for encryption. Binary comparison
between the two samples reveals an approximate 97% match.

One of the compromised hard drives included a variant of an HTTP backdoor used
by APT1 that Mandiant calls WARP. This malware has no RAT functionality and
is primarily used to gather system information and download stage two malware.
Therefore, we believe that WARP was used as a dropper to install Bangat onto the
compromised system.

Binary comparison between the WARP sample from Rights Group 1 and a WARP
sample from the Contagio APT1 malware collection (md5 C0134285A276AB933E-
2A2B9B33B103CD) revealed a 90% similarity. The main differences between samples
is that the Rights Group 1 sample does not have functions from wininet.dll in the
import table, and uses LoadLibrary and GetProcAddress to import them.

All three of the compromised hard drives included samples that communicated to
66.228.132.8 as a C2. This IP address also had an HTML comment on its default
webpage that indicated it also served as a C2 for WEBC2-QBP, another malware
family described by Mandiant in their APT1 report. The same C2 (66.228.132.8) was
also used by two Bangat samples in the Contagio APT1 collection (MD5s BD8B082B7
711BC980252F988BB0CA936, E1B6940985A23E5639450F8391820655).
TABLE 10: Overview of malware retrieved from compromised hard drives

<table>
<thead>
<tr>
<th>HARD DRIVE</th>
<th>MALWARE</th>
<th>FILE CREATION DATE</th>
<th>MD5</th>
<th>C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD1</td>
<td>Warp - Dropper for Bangat</td>
<td>n/a</td>
<td>2b941110e046a03894d-41f90272c3012</td>
<td>n/a</td>
</tr>
<tr>
<td>HD1</td>
<td>Bangat (irmon32.dll)</td>
<td>May 15, 2012</td>
<td>21afca59b9aaa26676adfbf72ccff7b9</td>
<td>hurrisonstone.dnset.com, dynossessfich.myMom.info</td>
</tr>
<tr>
<td>HD1</td>
<td>Bangat (Nwsapagent.dll)</td>
<td>July 5, 2012</td>
<td>429de63ec18eda4f0699b-2145bab5480</td>
<td>66.228.132.8</td>
</tr>
<tr>
<td>HD2</td>
<td>Bangat (rasauto32.dll)</td>
<td>June 11, 2012</td>
<td>45dc7e-b8e76143846f242940ff-369cb4</td>
<td>66.228.132.8</td>
</tr>
<tr>
<td>HD2</td>
<td>Bangat (Nwsapagent.dll)</td>
<td>June 19, 2012</td>
<td>429de63ec18eda4f0699b-2145bab5480</td>
<td>johnbell.longmusic.com</td>
</tr>
<tr>
<td>HD3</td>
<td>Bangat (rasauto32.dll)</td>
<td>June 11, 2012</td>
<td>5dc7e-b8e76143846f242940ff-369cb4</td>
<td>66.228.132.8</td>
</tr>
</tbody>
</table>

OBSERVATIONS

The APT1 campaigns illustrate one of the broader findings of this report. While large, resourceful threat actors like the APT1 group are frequently documented targeting government and industry, the same actors use similar tools, techniques, and procedures to target CSOs as well. While government and industry have the resources and expertise to respond to such threats, in many cases CSOs do not. Even large CSOs are vulnerable to this problem. While Rights Group 1 is a large and well-resourced organization relative to others in our study it was compromised for over a year-and-a-half before the threat was identified.
NetTraveler Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>April 30, 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>September 12, 2012</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails, Watering hole attacks</td>
</tr>
<tr>
<td>Exploits</td>
<td>Windows: CVE-2009-3129; CVE-2010-0188; CVE-2012-3333; CVE-2012-0158; Mac: CVE-2012-0507</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Windows: Conime, Gh0st RAT, RegSubDat, Netpass; Mac: Dockster</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 3, Tibet Group 4, Tibet Group 5, China Group 3</td>
</tr>
<tr>
<td>TTI Range</td>
<td>2.5 - 4.0</td>
</tr>
</tbody>
</table>

**BACKGROUND**

In June 2013, Kaspersky released a report detailing the operations of a threat actor that compromised over 350 victims in 40 different countries. Kaspersky called the main malware used in these campaigns “NetTraveler” after an internal string found in the tool, “NetTraveler is Running!” Targets identified in this report included Tibetan and Uyghur groups, the energy industry, military contractors, scientific research centres, universities, government institutions, and embassies.

The Kaspersky report identifies the IP 209.11.241.144 as a “mothership” server
used as a VPN and a C2 in the campaigns. We see 209.11.241.144 as a sender IP for 19 emails in our study. Searching for other emails that share the same malware we find a total of 34 emails, which we can split into seven campaigns based on how the common C2 infrastructure is used. Additionally, there was one email from this sender that we were not able to cluster, as the attachment was a password-protected ZIP file and the password was not evident. Attacks using infrastructure related to NetTraveler targeted all five of the Tibet Groups in our study as well as China Group 3.

NetTraveler operators are also known to use watering hole attacks against Tibetan websites. In December 2012, F-Secure reported on malware that relied on an entirely different method of attack and compromise but used the same infrastructure. A website related to HHDL at www.gyalwarinpoche.com was compromised and served the CVE-2012-0507 Java exploit (the same as used in the Flashback malware) to compromise computers running OS X. This malware, which F-Secure calls Dockster, connects back to the same IP that sent many of the malicious emails we observed, itsec.eicp.net:8088 (209.11.241.144). Kaspersky has documented similar watering hole attacks against Uyghur-related websites.

CAMPAIGN 1

The first appearance of an attack that used infrastructure related to NetTraveler was sent to China Group 3 on April 30, 2010. The email attached a PDF that used CVE-2010-0188, and connected to C2 servers at akashok.w63.1860host.com:80 (69.43.161.162) and ww2.akashok.w63.1860host.com:80 (204.13.161.108). The sender IP matches the mothership server identified by Kaspersky (209.11.241.144).

C2 traffic from this malware appears as follows:

```
GET /wl/netpass.asp?action=gettext HTTP/1.0
GET /wl/netpass.asp?hostid=...&hostname=...&hostip=...^filename=18155523-sys.log&filestart=0&filetext=begin::...
```

---

**From hu ping <huping@yahoo.com>**

Subject: [June4th Group:1420]RE:世博会开幕式灯光喷泉烟花表演取消 2010-04-30 02:32 PM

最新通知，基于安全考虑，世博会开幕式灯光喷泉烟花表演取消。
详情请见附件，请转发...

1 attachment: 世博会开幕式灯光喷泉烟花表演取消.pdf 904.6 KB
CAMPAIGN 2

The first of three campaigns using the Conime malware family involved seven emails, five of which were distinct, mostly concerning March 10th Tibetan Uprising demonstrations. Coinme samples used in these attacks have a technical score of 1.25. These emails were sent between February 13 and March 7, 2012 and were all targeted at Tibet Group 1. The campaign used a combination of malicious XLS and RTF documents exploiting CVE-2010-3333. The majority of these attacks score a TTI of 3.75. One email only scores 2.0 on social engineering sophistication and a 2.5 overall TTI. We see the mothership server (209.11.241.1440) and 120.50.35.60 used as a mail sender. All of the attacks in this campaign used 61.178.77.98 (without an associated DNS name) as a C2.

CAMPAIGN 3

The second of three campaigns using the Conime malware family involved seven emails, three of which were distinct, sent to Tibet Groups 1, 2, and 4. These emails all scored a social engineering sophistication value of 3.0, for a combined TTI of 3.75. Two of the distinct emails had an attached XLS document; one was encrypted, the other was not. The third email used a malicious RTF document exploiting CVE-2010-3333. The encrypted XLS was sent on July 25, 2012, and the other emails were sent between September 10 and 12, 2012. We again see 209.11.241.1440 as an email sender IP. All of these exploits dropped the same variant of Conime, which connected to gen2012.eicp.net:1080 (61.178.77.98) as a C2.

CAMPAIGN 4

The third campaign using Conime was more varied than the other two, and was targeted at Tibet Groups 1, 2, and 4. Fifteen emails were received, eleven of which were distinct (although one showed only minor changes), ranging from 2.0 to 4.0 on the
social engineering sophistication score. These emails were sent over a longer timeframe than the other campaigns, extending between June 14, 2012 and September 12, 2012. Vulnerabilities used included both major RTF (CVE-2010-3333, CVE-2012-0158) and XLS (CVE-2009-3129) versions. One email, received by Tibet Group 2, received a social engineering sophistication score of 4.0. This email was highlighted to us by the recipient as highly targeted, and referenced an upcoming conference call about grant funding. Like the previous two NetTraveler campaigns, the malware connected directly to 61.178.77.98.

CAMPAIGN 5

This campaign used a variant of Gh0st RAT, with a flag text of “Snow.” Identical emails, concerning a visit of HHDL to Portland, were sent to Tibet Groups 2 and 4 on January 28, 2013. The emails have a social engineering score of 2, with an overall TTI score of 2.5. The attackers again used 209.11.241.144 as a mail sender and 61.178.77.98 as a C2.

CAMPAIGN 6

This campaign used a different malware family, RegSubDat, which was contained in an RTF using CVE-2012-0158, attached to an email sent to Tibet Group 1. Again we see mail sent from 209.11.241.144, but in this case the malware connected to a different C2 server: itsec.eicp.net:443 (1.203.31.195). This attack scored 3.0 on the social engineering sophistication value for an overall TTI of 3.75.

CAMPAIGN 7

The final sample from the NetTraveler group was observed in an email message sent to Tibet Group 1 on March 15, 2012. This malware was sent from the same mother-ship server (209.11.241.144) described above, but rather than attaching the malicious file, as had been done for all prior attacks, this email contained a link to an infected XLS file. The file was hosted at www.eaglessey.com (120.50.35.46), but was no longer present when we attempted to access it.

OBSERVATIONS

The NetTraveler campaign serves as another example of a campaign that targets CSOs alongside industry and government targets. These campaigns are conducted by a prolific threat actor that has targeted a variety of different sectors. Our findings confirm the targeting of Tibetan groups identified by Kaspersky, as all five of our Tibet Groups were targeted. This campaign demonstrates an adaptive attacker that uses a variety of vulnerabilities for different applications, including targeting of both Mac and Windows platforms.
## PlugX Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>February 10, 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>January 15, 2013</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td>Exploits</td>
<td>CVE-2012-0158 (RTF, DOC, and XLS), CVE-2012-1889 (Internet Explorer), CVE-2012-5054 (Flash), CVE-2009-4324 (PDF), CVE-2007-5659 (PDF)</td>
</tr>
<tr>
<td>Malware Families</td>
<td>PlugX, Poison Ivy</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, China Group 1, China Group 2</td>
</tr>
<tr>
<td>TTI Range</td>
<td>1.5 - 7.5</td>
</tr>
</tbody>
</table>

### BACKGROUND

PlugX is a well-known family of malware that researchers have observed being used in targeted attacks against Tibetan organizations, NGOs, government institutions, and private companies.

Trend Micro has [published a report](https://www.trendmicro.com) on PlugX, describing a long-standing campaign that previously used Poison Ivy, another malware family. Jaime Blasco at Alien Vault [claims to have tracked down the author](https://www.alienvault.com) of PlugX, who is allegedly based at a Chinese security company.

The PlugX samples seen in our study can be clustered into four campaigns, based on email sender IP and C2 infrastructure. Examining email topics, vulnerabilities used, and compile paths (as described in the Alien Vault blog post) suggests that the four
campaigns are from the same source. We have also seen a Poison Ivy sample used in this campaign.

The attack vectors and vulnerabilities used in PlugX are more varied than other attacks in our dataset. The vulnerabilities used include instances of CVE-2012-0158 in three separate file formats, an Internet Explorer vulnerability (CVE-2012-1889) that will install PlugX as a drive-by download, and a Flash vulnerability (CVE-2012-5054) hosted on an external website. The earlier Poison Ivy attack used two older PDF vulnerabilities. The Flash vulnerability was particularly notable; it was a zero-day at the time of the attack, leaving any user who clicked the malicious link it was hosted on vulnerable to compromise.

CAMPAIGN 1

The first set of attacks consists of fifteen emails, five of which were unique, sent from May 11, 2012 to June 1, 2012. Tibet Group 1 and Tibet Group 2 were both targeted with at least four out of the five emails. These emails show many signs of coming from the same source, including a common return address of kandid77@rambler.ru, a sender IP of 98.126.14.13, and common C2 infrastructure.

Two different C2 domain names were used: systen.windowsdeupdate.com (TCP port 8080) and web.windowsdeupdate.com (UDP port 7070). These DNS names both pointed to the same IPs, which include 174.139.12.84 and 98.126.14.13.

All of these emails have a social engineering score of 3.0 and an overall TTI of 4.5. One example, sent to Tibet Group 2, spoofed a legitimate Tibetan official and contains a Word document that outlines the schedule of an actual European tour taken by the Dalai Lama.
CAMPAIGN 2

On May 22, 2012, an email was sent from the IP address 69.46.75.74 to Tibet Group 2, which claimed to be from an individual named Tsering Dolma, with an email signature belonging to the Central Tibetan Administration, and with the return address of ‘tdolma6248@yahoo.com.’ This email contained an attached RTF with CVE-2012-0158 that was used to install PlugX.
Three emails were sent to Tibet Group 2 and China Group 1 between June 15 and August 30, 2012. Each email had unique content, attack vectors, sender email address and IP, and vulnerability used. The vulnerabilities included a Word variant of CVE-2012-0158, the Flash vulnerability CVE-2012-5054, and Internet Explorer vulnerability CVE-2012-1889.
The Flash vulnerability CVE-2012-5054 was a zero-day at the time it was used in an attack against China Group 1. The attack was delivered in an email that was highly customized for the recipient and used a malicious link in the message as the vector. It referred to a group of individuals who had recently been involved in internal private meetings and appeared to be a forwarded message from the director of the organization. The highly targeted nature of this attack, combined with the technical sophistication of the PlugX malware family, resulted in a TTI score of 7.5, the highest seen in the study.

**CAMPAIGN 4**

The last campaign consisted of four unique emails sent to Tibet Groups 1 and 2 between December 22, 2012 and January 15, 2013. These emails all included attachments that used CVE-2012-0158. The C2 domain used was jinyuan2011.zapto.org:443, which resolved to 123.129.19.145 at the time of the attack. Three of these four emails scored 2.0 on the social engineering sophistication score (and 3.0 TTI overall), and one scored 3.0 on social engineering for an overall TTI of 4.5.

One of these four emails repurposed legitimate text about a Tibetan monk who had been detained:
This campaign was interesting in that it did not use the encrypted BOOT.LDR files, instead using NvSmartMax.dll.url, and logging keyboard data to NvSmart.hlp. This functionally corresponds to observations made by Kaspersky researchers that PlugX was becoming more mature. In particular, we observed that the identifying strings and logging data were removed in this campaign. It is particularly interesting that while the malware itself is being improved, potentially in response to published reports from threat researchers, the quality of the targeting in this campaign has gone down.

**POISON IVY**

In September 2012, Trend Micro described the use of PlugX in a campaign that had previously used the Poison Ivy RAT and targeted government and private companies in Japan. We also saw evidence in our study of Poison Ivy being used in conjunction with PlugX in an attack sent to China Group 2 on February 10, 2011, over a year
before our first observed PlugX attack. This email included a PDF with two vulnerabilities, CVE-2009-4324 and CVE-2007-5659.

---

Social engineering 1
Technical 1.5
TTI 1.5
MD5 49c9cf000fa1d789f3df8d739f997eb8
C2 sociapub.flower-show.org (14.102.252.142)

The Poison Ivy RAT connects to a C2 at sociapub.flower-show.org:8080 (14.102.252.142), the same Poison Ivy C2 domain observed by Trend Micro on July 11, 2012. This attack has also been seen elsewhere in the wild, as noted in a Threat Expert report describing the same malware seen with a different file size and MD5 hash (9ADFC6DD86D5FF36F2CAB781663E1075).
OBSERVATIONS

The PlugX campaign provides yet another example of a campaign that targets civil society organizations alongside government and industry groups, using the same infrastructure and malware to compromise targets. Aside from these similarities, the campaign otherwise had a number of unique characteristics that separated it from others in our research. Most notably, it was the only instance of a zero-day vulnerability seen in our study. Given that zero-days are highly effective, as software developers have yet to patch the vulnerability, they are highly lucrative and sought after. It is notable that the malicious attacks would use this zero-day to target a CSO, as once such an exploit is exposed it runs the risk of being identified and having the vulnerability fixed. The PlugX campaign also included a broader variety of attack vectors than what was seen in most campaigns. The attached files included the zero-day Flash vulnerability, an exploit for Internet Explorer, as well as the standard Microsoft Office exploits seen elsewhere.
TseringKanyaq Campaigns

| First Seen | May 4, 2012 |
| Last Seen | July 26, 2013 |
| Attack Vectors | Targeted malicious emails |
| Malware Families | Windows: Shadownet, Duojeen, Mac: PubSab |
| Targeted Groups | Tibet Group 1, Tibet Group 2, Tibet Group 4 |
| TTI Range | 3.0 - 3.75 |

BACKGROUND

Unlike the previous campaigns that were grouped by shared infrastructure or connections to previously reported threat actors, the “TseringKanyaq” cluster was first identified through contextual analysis.

This cluster consists of a series of attacks targeting Tibet Groups, which had either ‘tseringKanyaq@yahoo.com’ or ‘d.kanam@yahoo.com’ in the reply-to address field of the malicious emails. Following the identification of this pattern, further attacks that shared common infrastructure were linked.

The addresses ‘d.kanam@yahoo.com’ and ‘tseringKanyaq@yahoo.com’ do not match known email addresses or names of persons in the Tibetan community. However, “tseringKanyaq” may be a misspelling of Kanyag Tsering, a Tibetan monk from the Kirti Monastery in the Ngaba region of Tibet. This region has been the scene
of a number of Tibetan self-immolations, and Kanyag Tsering has provided reports of the incidents to international media. He is a well known and respected member of the Tibetan community who, due to his work in getting information from inside Tibet to journalists, has developed a significant media presence. We met with Kanyag Tsering and showed him our analysis of this cluster. He confirmed that the address ‘tseringKanyaq@yahoo.com’ does not belong to him. Despite the possible intentional similarity of ‘tseringKanyaq@yahoo.com’ to the name of a notable Tibetan monk, the purpose behind the consistent use of these addresses in the reply-to field is unknown.

We identified three malware families in this cluster, which were used to target Windows (ShadowNet and Duojeen) and OS X (PubSab). The ShadowNet malware family is associated with the ShadowNet espionage group, which was discovered by the Information Warfare Monitor and the ShadowServer Foundation in 2009 and was revealed to be targeting Tibetan organizations and Indian military and government institutions. The malware we found did not connect to infrastructure related to the previous ShadowNet campaign.

All three malware families used in the TseringKanyaq campaign were also used by the LuckyCat campaign, which was discovered by Trend Micro in 2012. LuckyCat is notable for targeting companies based in India and Japan working in aerospace, energy, engineering, shipping, and military research in addition to Tibetan activists. We find infrastructure connections between the TseringKanyaq and LuckyCat campaigns, which suggests some level of coordination.

EMAIL PROVIDER INFRASTRUCTURE

This campaign is marked by a period of gaps in which attacks stop and later re-emerge with similar identifying features (most notably the consistent use of the Reply-To addresses), some level of improvements to the malware C2 infrastructure, and/or changes to the social engineering tactics.

We divide these gaps into three distinct periods in which the attackers utilize different email providers to send attacks.

- 163.com: May 4, 2012 - July 9, 2012
- myopera.com: July 24, 2012 - September 5, 2012
- gmx.com: October 14, 2012 - July 26, 2013
Between these three periods there is no overlap in the use of these mail providers. We clearly observe the attackers moving from one provider to the next. The use of these different providers could be due to a number of possibilities: the domain provider may have shut down the accounts due to notifications or detection of abuse, changes to provider infrastructure may have created difficulties in maintaining the accounts, or the attackers may have moved on to the next domain infrastructure once the advantages of an alternate provider became apparent.

**163.COM CAMPAIGNS**

The first wave of attacks occurred between May 4 and July 9, 2012. Four email attacks were sent during this period targeting Tibet Groups 2 and 4. All of these attacks spoof prominent organizations in the Tibetan community and repurpose legitimate content, which gives them a social engineering sophistication base value of 3. All of the malware samples in this cluster have a technical score of 1.25, for a total TTI of 3.75.

The first attack on May 4, 2012, was sent to Tibet Group 2 with an email that repurposed content concerning a petition campaign. The actual email sender was psjiangzuo@163.com (174.139.21.26). The attached file dropped Duojeen malware that connects to www.xiuxiu.in (173.231.22.201).

The second attack on June 28, 2012, sent to Tibet Group 2, purported to come from Karma Yeshi, a member of the Tibetan Parliament in Exile (TPiE), and provided information (in Tibetan) on the Flame of Truth Rally, a campaign launched by the TPiE to express solidarity with Tibetans who have self-immolated. The actual sender of the mail is sysutiyubu@163.com (222.212.213.197). The attachment also drops Duojeen malware.
On July 5, 2012, Tibet Groups 2 and 4 both received identical emails with content related to a recent self-immolation. The malware used was ShadowNet, which leverages Windows Management Instrumentation (WMI), a system tool meant for administrators. Its intended usage as a tool for collecting system information and automation makes it an ideal mechanism for gathering and exfiltrating data. Use of legitimate Windows features can make it more difficult for administrators to identify activity as malicious.

The ShadowNet attacks used a WMI Script that contained links to one of three blogs to which the malware attempts to connect. The blog then has a string with encoded C2 information as shown in Figure 14 below.

**FIGURE 14:** Sample of blog post used to transmit C2 information to infected machines
Once a connection to the C2 is made, system information and data can be sent to the attackers. In the case of the July 5 attacks, the malware first connects to newwolfs21.blog.163.com, after which it retrieves the C2 newwolfs29.mezoka.com.

On July 9, 2012, Tibet Group 2 received two identical emails sent to two separate organizational accounts. The emails contained content regarding self-immolations. The malware used, Duojeen, retrieves system information, establishes a connection with zml.x.gg, and sends the collected information. It then retrieves second stage malware from http://newwolfs29.zxq.net/winxp.rar. As with the previous attack, the two emails were sent from different accounts: suzhonghechang@163.com (125.70.67.30) and nongzhijiuye@163.com (199.192.159.213).

FIGURE 15: Email sender, IP, and C2 infrastructure for 163.com tseringKanyaq emails
MYOPERA.COM CAMPAIGNS

From July 24 to September 5, 2012, the attackers moved their mail provider to myopera.com. The attacks continued to use ShadowNet and Duojeen malware and the same common C2 infrastructure as the previous campaign. During this period, we observed three attacks sent to Tibet Groups 1, 2, and 4, in some cases to multiple accounts within the organizations. All of these attacks spoofed prominent groups in the Tibetan community and repurposed legitimate content, which gives them a social engineering score of 3. All of the malware samples in this cluster have a technical score of 1.25, for a total TTI of 3.75. Interestingly, in this campaign we observed some emails being sent from Tor exit nodes, which shows the attackers making a new effort to hide their location.

Between July 24 and 25, Tibet Groups 1, 2, and 4 received identical emails that appeared to be from the Tibet Office in Brussels, with content regarding an upcoming rally.

---

From Rinzin Choeden <tibetbrussels@tibet.com>

Subject: am directed to send the attached letter regarding observation of solidarity rally on 8th Aug by the Tibetans all over the world as called upon by Kalon Tripa in Kashag's message on July, 2012.

To: 

Dear sir/madam,

I am directed to send the attached letter regarding observation of solidarity rally on 8th Aug by the Tibetans all over the world as called upon by Kalon Tripa in Kashag's message on July, 2012.

Kindly acknowledge the email please.

regards

Karma Choeying
Secretary
Bureau du Tibet, Brussels

---

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>cc0b8b8e42fdd59cc4b32b3a06e57281</td>
</tr>
<tr>
<td>C2</td>
<td>newwolfs29.mezoka.com (209.190.24.9)</td>
</tr>
</tbody>
</table>
The attached malware was ShadowNet, and it connected to newwolfs21.blog.163.com to retrieve C2 instructions. In each instance, the email was sent from a different account (newwolfs41@myopera.com, tenzin600@myopera.com, tibettibetan3@myopera.com, tenzin600@myopera.com, and mytenzin@myopera.com); however, the sender IP was the same for each account (184.82.49.114). We later discovered that this sender IP was also used as a C2.

During an investigation of one of the C2s used in the campaign (newwolfs20.x.gg/mits/) we found open directories that included a sample from the Sparksrv malware family, which we presume was intended to act as stage two malware. This sample used 184.82.49.114 as a C2.

Between July 25 and 26 Tibet Groups 1, 2, and 4 received identical emails that spoofed Karma Yeshi, a member of the TPiE, with an update on the Flame of Truth rally campaign. The malware in this case was Duojeen.

---

From karma Yeshi <karma1959@gmail.com>  
Subject Sign Petition  
To  

Flame of Truth Signature Campaign  
Dharamsala: July 24, 2012  
Through Worldwide “Flame of Truth” relay, Tibetan Parliament-in-exile appeal international community and people of the world to support the issue of Tibet through this signature campaign. We are going to submit signed petition to UN Headquarters in New York, UN Human Rights Council in Geneva and UN Information Centre in New Delhi on December 10, 2012 with following demands:  
1. The United Nations must discuss the issue of Tibet based on the resolutions that it has passed in 1959, 1961 and 1965, and continuously make efforts to fulfill the substance of these resolutions  
2. An independent international fact-finding delegations must immediately be sent to investigate the ongoing crisis in Tibet  
3. The United Nations must take special responsibility to ensure that the basic aspirations of the Tibetans inside Tibet are fulfilled  

TPIE's Committee on Flame of Truth Relay  
Dharamsala  

---  
Karma Yeshi (Mr.)  
Member of Parliament  
Tibetan Parliament-in-Exile  
Dharamsala (M.P.) India  

1 attachment: Sign Petition_NEW.doc 153.0 KB
In three of the attacks, the sender IP traced back to a Tor exit node maintained by the Chaos Computer Club in Germany. The timing of this shift in tactics is interesting, as it comes after a series of attacks that used a C2 as the mail sender. Using Tor to mask the real location of the mail sender may therefore have been an effort to improve operational security. However, the attackers use of Tor is inconsistent and following this series of attacks was observed only one other time.

**TABLE 11: IP address of email senders used during MyOpera campaign**

<table>
<thead>
<tr>
<th>SENDER</th>
<th>IP</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:mytenzin@myopera.com">mytenzin@myopera.com</a></td>
<td>31.172.30.4</td>
<td>Germany - Tor exit node</td>
</tr>
<tr>
<td><a href="mailto:tenzin600@myopera.com">tenzin600@myopera.com</a></td>
<td>62.113.219.3</td>
<td>Germany - Tor exit node</td>
</tr>
<tr>
<td><a href="mailto:tibettibetan3@myopera.com">tibettibetan3@myopera.com</a></td>
<td>31.172.30.3</td>
<td>Germany - Tor exit node</td>
</tr>
<tr>
<td><a href="mailto:tibettibetan3@myopera.com">tibettibetan3@myopera.com</a></td>
<td>50.136.226.40</td>
<td>US - Comcast</td>
</tr>
</tbody>
</table>

The final attack in this campaign was sent to Tibet Group 2 on September 5, 2012. It contains information regarding a hunger strike initiative undertaken by the Tibetan Youth Congress. The attachment contained Duojeen malware that connected to dplcoopsociety.us.dwyu.com (184.82.238.34).
GMX.COM CAMPAIGNS

From October 14, 2012 to July 26, 2013, the attackers switched to gmx.com as their mail provider. The use of gmx.com is interesting, because the email headers from this provider include a unique user ID number, which can be used to track malicious accounts using this service. However, we see no overlap in user IDs from the gmx.com accounts used in the attacks, which suggests that the attackers used a script to generate new accounts, and as a result the user ID number is always different.

Within this period we observe the attackers using reply-to ‘tseringKanyaq@yahoo.com’ and also beginning to use reply-to ‘d.kanam@yahoo.com’ in messages. We cluster attacks by these two accounts in the subsections below.

gmx.com ‘tseringKanyaq’ campaigns

From October 14, 2012 to July 26, 2013, we observed 11 attacks targeting Tibet Groups 1, 2, and 4, using the gmx.com mail provider and a reply-to address of ‘tseringKanyaq@yahoo.com.’
As with the previous campaigns, these messages all spoofed real people and organizations in the Tibetan community. Each email in this campaign has a social engineering sophistication score of 3 and a technical score of 1.25 for a total TTI of 3.75.

Five attacks in this campaign used ShadowNet connecting to www.tbtsociety.info (209.141.36.23), laraider2.he1.ifreeurl.com (46.21.152.227), or www.nedfortibt.info (216.83.45.18). Three attacks dropped Duojeen connecting to laraider2.he1.ifreeurl.com (46.21.152.227).

In one instance we see the connection of an email sender traced back to a Tor exit node (IP 77.247.181.165).

**FIGURE 17:** Email sender, IP, and C2 infrastructure for gmx.com tseringKanyaq emails
**gmx.com ‘d.kanam’ campaigns**

From December 18, 2012 to May 2, 2013, we observed 12 attacks targeting Tibet Groups 2 and 4 using the gmx mail provider and a reply-to address of ‘d.kanam@yahoo.com.’

Message lures in this campaign all spoofed real people and/or organizations and repurposed legitimate content from Tibetan groups. Each email in this campaign has a social engineering sophistication score of 3.

Seven attacks in this campaign used ShadowNet connecting to www.tbtso-ciety.info, laraidert2.he1.ifreeurl.com (46.21.152.227), and pomehra.typepad.com (204.9.177.195). Each of these attacks has a technical score of 1.25.

Two attacks used Duojeen connecting to www.tbtso-ciety.info (216.83.45.18). Each of these attacks has a technical score of 1.25.

Within this wave of attacks we also observed the use of PubSab implanted in Word documents that used the exploit CVE-2009-0563. In this instance the malware connected to coremail.info (198.74.124.3).
FIGURE 18: Email sender, IP, and C2 infrastructure for gmx.com d.kanam emails
CONNECTIONS TO LUCKYCAT CAMPAIGN

We identify a number of connections between the TseringKanyaq cluster and the LuckyCat campaign, as well as Sparksrv and Duojeen campaigns related to LuckyCat.

The LuckyCat campaign used a variety of malware including Duojeen, ShadowNet and PubSab, which we also see used in the TseringKanyaq campaigns. Beyond this common set of malware we also see connections to infrastructure linked to LuckyCat and related campaigns.

The LuckyCat campaign utilized a series of free hosting and VPS services for its C2 infrastructure. One of the VPS services is hosted on duojee.info. On July 6, 2011, Tibet Group 1 received a malicious email containing ShadowNet malware. While this sample does not include the reply-to address tseringkanyaq.yahoo.com or d.kanam@yahoo.com, the C2 infrastructure has connections to the campaign. The malware connects to and retrieves C2 information from appleboy1111.blogspot.com. We observed a previous version of the script with encoded C2 information that points to duojee.info. The script was then updated to point to www.tbtsociety.info (216.83.45.18), which is a C2 we see used repeatedly in the gmx.com campaigns. The transition to this C2 shows evidence of the attackers shifting infrastructure that was previously linked to LuckyCat to new infrastructure we see used in the TseringKanyaq campaign.

We also see connections to Sparksrv campaigns that have been linked to LuckyCat. Sparksrv is malware used by the LuckyCat campaign as a second stage tool to add additional functionality after the first stage dropper successfully infects a target. Our analysis of open directories on a TseringKanyaq-related C2 revealed Sparksrv on the server, which suggest it was also being used as a second stage in this campaign.

Trend Micro identifies rukiyeangel.dyndns.pro as a C2 used for Sparksrv campaigns related to LuckyCat. In two attacks sent on December 24, 2012 and April 10, 2013, we see the email sender IPs originating from 198.74.124.3 and 216.218.197.234, respectively. The IP 198.74.124.3 currently resolves to coremail.info, which was used as a C2 for PubSab attacks in the TseringKanyaq campaign. Passive DNS records show that 198.74.124.3 and 216.218.197.234 previously resolved to rukiyeangel.dyndns.pro.
OBSERVATIONS

This campaign has several interesting characteristics relative to others in our study. The ShadowNet malware is the only example of WMI malware we observed. While this quality makes the malware relatively easy to remove, it also makes it more difficult for the user to identify. This campaign also relies on a highly disposable C2 infrastructure.

This cluster is also the only campaign to be first identified through contextual clues rather than a strict reliance on shared code or C2 infrastructure. The frequent use of ‘tseringKanyaq@yahoo.com’ and “d.kanam@yahoo.com” in the Reply-to field is in some cases the only indicator tying the attacks together. Despite using a variety of different domains to send the malicious emails, it remains unclear why the same email address was reused so often.

Notably, this campaign also has links to other malware tools and campaigns related to ShadowNet and LuckyCat that have targeted a range of communities and sectors including Tibetans.
DTL Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>December 21, 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>July 4, 2013</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td>Exploits</td>
<td>Windows: CVE 2010-3333, CVE-2012-0158</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Windows: 9002, 3102, Mongal, Nsf, Boouset, Gh0st RAT, LURK0 (Gh0st RAT variant), CCTV0 (Gh0st RAT variant), Surtr (Remote and GtRemote), T5000</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 domains: dtl.eatuo.com, dtl.dnsd.me, dtl6.mooo.com, tbwm.wlyf.org</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 3, Tibet Group 4</td>
</tr>
<tr>
<td>TTI Range</td>
<td>2.5 - 6.75</td>
</tr>
</tbody>
</table>

**BACKGROUND**

We identified a distinct campaign of targeted malware attacks against Tibetan groups that used the shared infrastructure of four C2 domains (dtl.eatuo.com, dtl.dnsd.me, dtl6.mooo.com, tbwm.wlyf.org). Tracking the IP address resolution of these domains over time, we observed that at certain periods they resolve to the same IP and therefore belong to a shared C2 infrastructure. We call this cluster the DTL campaign, because of the use of “dtl” in most of the C2 server domain names. We see this infrastructure used for a series of campaigns that involve 9 malware families: T5000, 9002, Boouset, Mongal, Nsf, Gh0st RAT, LURK0 (Gh0st RAT variant), CCTV0 (Gh0st RAT variant), and Surtr. We also identified one other malware family (3102) that is likely related due to code overlap.

In November 2013, FireEye published a [report](#) that also identified the DTL cluster linking seven malware samples to four C2 domains, three of which we also observed (dtl.eatuo.com, dtl.dnsd.me, dtl6.mooo.com). FireEye only saw DTL campaigns using
the malware family 9002, which we observed being used for three attacks, of which one sample had a matching MD5 to one provided in the FireEye report (9f5e9e6b0c-87cad988f4a486e20bbc99). Our visibility into DTL campaigns only revealed Tibetan targets. However, one attack sent to a Tibet Group had an email body and attachment written in Uyghur. Other researchers have identified attacks related to the DTL campaigns targeting Uyghur groups. The Uyghur samples sent to the Tibet Group may therefore be the operators accidentally sending the wrong lure.

Interestingly, FireEye observed campaigns using DTL infrastructure targeting a range of government and industry entities, showing their scope goes beyond CSOs. Such targets included entities within the following sectors (using FireEye’s categories): U.S. federal government, state and local government, services/consulting/VAR, financial services, telecommunications, aerospace/defense/airlines, energy/utilities/petroleum refining, healthcare/pharmaceuticals, entertainment/media/hospitality, insurance, chemicals/manufacturing/mining, high-tech, and higher education.

MALWARE DEVELOPMENT PATTERNS

Of the nine malware families seen in DTL campaigns, the most frequently used were LURK0 and CCTV0, which are both variations of the Gh0st RAT codebase. LURK0 and CCTV0 are named for the five-character header that appears in network traffic when the malware is run. Both pieces of malware have standard RAT functionality including keylogging, file listing, and data exfiltration. Our observations of the DTL campaign show active development of these RATs over the period of two years that are unique to this cluster.

We found relations between malware samples using binary comparison tools to attempt to determine shared code bases, and comparing various identifiers in the samples. For example, LURK0 creates registry keys with names that are a variation on “DbxUpdate” and then uses a mutex to see if it is already running on the infected system. These names can be customized and used to attempt to distinguish between campaigns using the same malware family. Another useful feature for analysis is compilation times. Although these times can be easily modified, if related samples all have the same compilation date, they were likely created with the same builder. Through analysis of these features and tracking of shared C2 infrastructure we divide DTL-related attacks into a series of eight campaigns. We also discuss two related campaigns that, while not using the same infrastructure, use malware that shares code and identifying features and are likely developed by the same group.
CAMPAIGN 1: T5000

In 2011, four emails were sent to Tibet Group 1 with T5000 malware attached. On January 10, the group received an email with a .rar archive attachment containing an executable file. The email and attachment were in Chinese.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>2.5</td>
</tr>
<tr>
<td>MD5</td>
<td>2cf577eda241158e3c3b5431f30b9aeb</td>
</tr>
</tbody>
</table>
On June 1, they received an email with a very similar .rar, this time using the Unicode right-to-left override. We were unable to get either of these samples to connect to a C2, and it is possible that they were not functioning properly.

On July 11, Tibet Group 1 received an email in Tibetan, with a Microsoft Help (.hlp) file attached. The T5000 malware embedded in the file successfully connected to deepinlife.dyndns.info.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>604d501e9e0ce7c175060b8512f706b7</td>
</tr>
<tr>
<td>C2</td>
<td>deepinlife.dyndns.info</td>
</tr>
</tbody>
</table>
On July 26, Tibet Group 1 received the fourth of the emails, with another help file attached. This sample connected directly to 180.178.53.37 without DNS resolution.

T5000 is the first instance we see of the “DTL” name, using Dtl.dat as the name of the network configuration file. Although this campaign does not use DTL domain names for C2 servers, we can identify it as part of this cluster due to the shared sender IPs. All of these emails used gmx email account and were sent from either 66.103.141.24, 69.73.160.142, 65.124.5.107, 64.124.5.107, or 209.234.204.31.

In November 2013, Cylance reported on attacks using T5000 that targeted human rights groups and the automotive industry. The name they gave this threat actor was “Grand Theft Auto Panda,” as “they appear to be punching people in the face and stealing their cars.”
CAMPAIGN 2: LURK0 (SOFTMY.JKUB.COM)

In February 2011, Tibet Group 1 was sent two identical emails using LURK0 malware that used softmy.jkub.com as a C2. While this campaign does not use DTL-related C2s, the LURK0 samples have features that are otherwise unique to the DTL cluster. The samples originally created a registry key named “DbxUpdate” and a mutex named “111.” The components in these samples have compilation dates of “2010-09-26 04:31:01” and “2010-12-09 03:22:21.”

The emails sent repurposed text about Chinese authorities clamping down on activists following an online call for protests.

```
From: Wangdu Tsering <wtsering208@yahoo.com>
Subject: Chinese officials detain activists after online call for protests

Dear friend,
>From Internet.
Beijing: Chinese security officials have questioned or detained scores of activists and warned others against staging protests after an online call was made for demonstrations in 13 cities, campaigners said.

please read attachment for detail.

Wangdu

1 attachment: protest.doc 360.4 KB
```

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>2.5</td>
</tr>
<tr>
<td>MD5</td>
<td>37457f46709b793d13a25da0d4c896fa</td>
</tr>
<tr>
<td>C2</td>
<td>softmy.jkub.com</td>
</tr>
</tbody>
</table>

In May 2011, Tibet Group 1 was again targeted by attacks using LURK0 samples that connected to softmy.jkub.com. These samples created a folder named “DbxUpdateET” and a mutex named “ET” with compilation times in March 2011. The May and February attacks all utilized DLL hijacking of linkinfo.dll to maintain persistence on the system. The May emails, shown below, described a recent award ceremony.
hosted by the Canadian Multicultural Council. We were unable to find references to this event online and therefore cannot confirm if it was real.

---

Social engineering | 2
Technical | 1.25
TTI | 2.5
MD5 | f024c4febb69195750c7af06e15aa1f7
C2 | softmy.jkub.com

**CAMPAIGN 3: BOOUSET (DTL)**

In December 2011, multiple members of Tibet Group 1 were targeted by identical emails that appeared to be from a funder providing a report from a grantee. The attached word document dropped Boouset malware that connected to dtl.dnsd.me as a C2. This campaign is the first instance of attacks using DTL-related domains. Boouset is a simple piece of malware (technical score 1.0) with limited code obfuscation that sends unencrypted data back to the C2. It features standard RAT capabilities including a keylogger and the ability to execute remote commands. The social engineering score of these attacks is 3 (TTI 3).
CAMPAIGN 4: LURK0 - CRAZYTOWN EDITION (DTL)

From February 2 to March 14, 2012, a campaign of 10 LURK0 attacks targeted Tibet Groups 1 and 2 using dtl.dnsd.me and dtl.eatuo.com domains as C2s. These were the first LURK0 attacks to use DTL domains as a C2. These samples also performed DLL hijacking on linkinfo.dll and created a key named DbxUpdateET. The mutex name was changed to “ETUN.” These samples use the internal name “ButterFly.dll.” Nine of the attacks used a common tactic of attaching a rar file containing benign jpeg image files and shortcuts that actually link to a LURK0 dropper. These samples had August 15, 2011 as a compilation date.

The emails referenced a number of topics including writings from a Tibetan activist and a recap of a rally held the day before to commemorate the March 10th Tibetan Uprising Day. Another email spoofed the legitimate email address of an individual at the Tibet Bureau in Geneva, and attached a malicious document containing information on the organization of an undetermined election.

---

Dear,

Please find attached here the election member assignment per tsogchung. Due to resignation and leave of some of the local election commission member we will be contacting the Basel and Zurich tsogchung thumi later on the election member.

With wishes,

Dawa Gyatso
Under Secretary/Accountant
Tibet Bureau
Place de la Navigation 10
1201 Geneva

Tel. +41 22 738 79 40
Fax +41 22 738 79 41

1 attachment: election timetable thumi 2012.xls 152.0 KB
CAMPAIGN 5: LURK0 UNDER DEVELOPMENT

In late March 2012, another LURK0 attack was observed that had considerable differences from the previous wave of attacks. Although this new attack also used compressed .rar files as a vector, unlike previous attacks it did not perform a DLL hijack, instead dropping a file called win32.exe. This file writes several new files to disk: IconConfigEt.DAT, containing a DLL with the core RAT functionality; iexplore.exe, which copies IconConfigEt.DAT to IconCacheEt.DLL, overwrites the DAT file and then runs the DLL file; and temp.exe which simply creates a shortcut to iexplore.exe. This functionality changes the persistence mechanism from DLL hijacking to the creation of an executable that launches on startup with the innocuous name of ‘iexplore.exe.’ Once launched, this executable runs the DLL. This sample also features a new mutex name: “ER.” These emails spoofed recognized Tibetan NGOs and referenced content about self-immolations in Tibet, and as a result scored 3.0 on the social engineering sophistication base value. The technical score for these emails was 1.25 for a total TTI of 3.75.

An additional attack in May 2012 indicated further development. This attack utilized a trojaned Word document as the attack vector with password protection to hinder AV detection. The sample was similar to malware seen during the March attack but this time with a different mutex name (“ERXXXXXXX”) and different names for the droppers. Additionally, instead of using a separate DLL, the sample dropped two files named iexplore.exe. One of these files simply ran the other which was signed with a digital certificate issued to Shenzhen OuMing Keji Co., Ltd.

Emails sent to Tibet Group 1 as part of this attack included repurposed text about self-immolations in Tibet, as well as an email on celebrations of the birthday of HHDL.
CAMPAIGN 6: LURK0 (DTL)

In July 2012, another LURK0 campaign of 11 attacks emerged that targeted Tibet Groups 1, 2, and 4 using the dtl.dnsd.me domain as a C2. These LURK0 samples have additional features compared to prior versions. The version of the zlib compression library used for encrypting communications between infected hosts and the C2 was upgraded from 1.1.4 to 1.2.3. These samples also created an executable called iexplore.exe (instead of performing DLL hijacking like in the earlier attacks). However, compared to the previous attacks they featured fewer layers of droppers and extra files. Configuration data like campaign codes and C2 information were changed to being stored in configuration files that could be easily modified. These samples all featured a compilation date of “2012-05-28 05:35:16” and a mutex name of “ERXXXXXXXX” while maintaining the “DbxUpdateET” registry key name.

Two of these attacks had lures related to HHDL’s birthday and contained encrypted Word files with the password contained in the message body.

Five of these attacks used .doc implants with decoy documents containing what appears to be a Tibetan organization’s legitimate proposal to the European Instrument for Democracy and Human Rights (EIDHR). The timing of these attacks is noteworthy, as a genuine EIDHR call for proposals—including proposals for
“Actions Aimed at Fighting Cyber-Censorship and to Promote Internet Access and Secure Digital Communication”—was pending at the time, with a July 20 deadline for concept notes. The emails were received by the groups on July 16 and 17, just a few days before the deadline.

Three attacks had identical email lures referencing a South African group’s visit to Dharamsala, India that appear to have been repurposed from a legitimate private communication. The email appears to be a request to the Tibetan organizations hosting the planned trip, with the malicious attachment containing an authentic travel itinerary as a decoy. This is a highly targeted attack based on private communications, and as a result receives the highest social engineering sophistication score (5, TTI 6.75).

**CAMPAIGN 7: CCTV0**

In November 2012 a campaign targeted Tibet Groups 1, 2, and 4 using dtl.dnsd.me and dtl.eatuuo.com domains as C2s. The first wave of these samples had compilation dates of October 15, 2012 and later samples had compilation dates of November 11, 2012. These samples changed the five-character code visible in network traffic from ‘LURK0’ to ‘CCTV0’, which prevents strict IDS rules looking for “LURK0” in network traffic from detecting the malware. The samples featured an embedded DLL with the internal name “ETClientDLL.dll” instead of “ButterflyDll.dll” which was seen in earlier attacks. The initial samples in this wave would query a benign third-party website to determine
the user’s IP. When this website’s results page was modified by its creators, the samples would crash trying to parse the page, leading to the feature being removed in later samples. Another significant change to later samples was padding of the resource section of the executables with extra data, resulting in a larger file size to avoid AV heuristics. Executables were padded with random data to get a different hash every time, making it more difficult for malware researchers and AV companies to share indicators.

TTI scores for the 10 emails varied. Three identical emails were sent to Tibet Group 1 and multiple accounts at Tibet Group 2. The lures used in these attacks were relatively poorly customized.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>2.5</td>
</tr>
<tr>
<td>MD5</td>
<td>1c44d9cf686f53f1194cdee2aefb99c2</td>
</tr>
<tr>
<td>C2</td>
<td>dtl.dnsd.me (199.36.72.214)</td>
</tr>
</tbody>
</table>
Later attacks included lures with more detailed information.

---

**From:** Tenzin Gyalpo--Private Office <ohhdl@ymail.com>  
**Subject:** Schedule  
**Date:** 2012-11-20 04:46 AM

Dear Supporters and Friends,

In the attachment of "Schedule.xls" is the public schedule of His Holiness the Dalai Lama both in India as well as abroad. Please note that for many of these events, tickets are required in order to gain entrance. People are requested to contact the organizers directly or visit the websites given below for further information on tickets. In general, most of the events in India are free where as the majority of events abroad require paid tickets. For your information, as a long-standing policy His Holiness the Dalai Lama does not accept any fees for his talks. Where tickets need to be purchased, organizers are requested by our office to charge the minimum entrance fee in order to cover their costs only.

Please note that the dates are subject to change.

Contact
Office: ohhdl@dalailama.com
Website Feedback: webmaster@dalailama.com

Mailing address:
The Office of His Holiness the Dalai Lama  
Tshekchen Choeling  
P.O. McLeod Ganj  
Dharamsala  
Himachal Pradesh (H.P.) 176219  
India

Telephone:  
91 1892 221343  
91 1892 221879

Fax:  
91 1892 221813

---

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>16b82aa9f537811490f6f2e347ec106f</td>
</tr>
<tr>
<td>C2</td>
<td>mychangeip1.ddns.info (110.152.229.247)</td>
</tr>
</tbody>
</table>

The changes seen in samples used in this campaign provide insight into the development path of the LURK0 family. Although we did not find C2 infrastructure overlap with other campaigns using LURK0, we did find other similarities. Other campaigns
that used LURK0 continued to use an older version of zlib, retained the LURK0 network header, and used different internal names (such as continuing to use the Butterfly moniker). A possible explanation for this observation is that while threat actor groups may share tools, development and customization of malicious software is decentralized.

**CAMPAIGN 8: SURTR**

From November 2012 until September 2013, the primary malware used in the DTL campaign changed to a new family called Surtr. These attacks continued to use the same C2s as the earlier families. This malware targeted Tibet Groups 1, 2, and 4. Unlike other families in the DTL cluster, Surtr downloads an additional component that contains its main functionality after infection. We have seen two versions of this used with the internal names Remote and GmRemote.

Although the Surtr and LURK0/CCTV0 malware families do not share a large amount of code, they exhibit similarities in behaviour. While some of these similarities, such as the use of zlib in both LURK0/CCTV0 and Surtr, are likely coincidental, others are much more specific. For example, similar registry key names used for configuration information and campaign codes, expanding of the resource section to avoid identical hashes, and similar formatting for sending system information are some of the similarities. Internal names used for the NSFree family and the several LURK0/CCTV0 variations follow a similar scheme, such as the filenames ‘NSFreeDll’ and ‘BTFreeDll’ and the creation of folders named MicET, MicBT, and MicNS.

In addition to these similarities, LURK0/CCTV0 and Surtr have also been used in conjunction with one another. For example, during our analysis we observed LURK0 being downloaded and installed as a stage two after initial infection with Surtr.

---

11 We first reported technical details on Surtr in Kleemola, K., Hardy, S. “Surtr: Malware Family Targeting the Tibetan Community” Citizen Lab, August 2 2013, https://citizenlab.org/2013/08/surtr-malware-family-targeting-the-tibetan-community/
CAMPAIGN 9: 9002

In the first half of 2013, we observed three emails sent out to Tibet Groups 1, 2, and 4 containing the 9002 malware. On March 25, an email was sent to Tibet Groups 1 and 2 with a CVE-2012-0158 attachment from a gmx account with sender IP 66.103.141.24. A different email sent from another gmx account, with sender IP 64.124.5.107 and another malicious attachment, was then seen the next day, March 26, sent to the same groups.

Dear

Attached to this email I send you the record of last Thursday’s preliminary meeting for the Dalai Lama’s visit.

If you have any remarks or questions, please do not hesitate to contact me.

Kind regards,

Valérie

---

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>2c8ef540ae77f1184ddfd3e0a1f810b</td>
</tr>
<tr>
<td>C2</td>
<td>dtl.dnsd.me (74.121.190.38)</td>
</tr>
</tbody>
</table>
On May 13, 2013, we saw a similar pattern. A new email was sent from 209.234.204.31 using a gmx account to Tibet Groups 1, 2, and 3, again using CVE-2012-0158. This email was then seen again on May 14, sent to many other targets including more staff at Tibet Group 1, and a number of other Tibetan NGOs, and CTA offices.

All of the 9002 samples connected to C2 servers at dtl.dnsd.me and dtl.eatuo.com on port 3123. This campaign uses campaign codes of the form “Tmdd,” where m is the month and dd is the day (e.g., T315 for emails sent on March 15).

An interesting feature of the 9002 malware is that it shares exported function names and embedded filenames with Surtr, making it very likely that it was developed alongside Surtr by the same group.
RELATED 3102 CAMPAIGN

3102 is a family of malware that appears similar to 9002, but with additional protection and anti-reversing features. We observed one campaign using 3102 with techniques similar to the original 9002 campaign.

On November 18, 2013, Tibet Groups 1 and 2 each received an email with a Tibetan theme from a Yahoo! address. While these emails contained the same subject, body, and attachment using CVE-2012-0158, they each had different recipient lists visible in the To: and Cc: headers. The inclusion of visible recipient lists is a method also used in the 9002 campaign.

OBSERVATIONS

The DTL campaign is notable for the variety of malware families used, the active development cycles of the malware, and connections to targeting of government and private industry.

The malware development cycle used here was easily traceable, and during the course of our study we were able to identify a large number of changes made and their
effects. While most campaigns focused on the use of a small number of malware families, we identified upwards of 10 distinct families in this cluster. Although some of these families were variants of each other, the range of malware used demonstrates the adaptability of attackers and their persistence in developing new techniques to compromise their targets.

In this campaign we see DTL-related infrastructure that was also used in the attacks against industry and government targets that were reported by FireEye. However, we see little overlap in the malware families. The DTL attacks reported by FireEye exclusively used 9002, whereas we see 9002 and nine other families in our dataset. This lack of similarity suggests that DTL operators may differentiate the tools used in their operations based on the target type.
# Ongoing Surtr Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>August 1, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>ongoing</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td>Exploits</td>
<td>CVE-2012-0158</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Surtr (GtRemote, Remote), PlugX</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 Domains: carts.dnset.com; free1999.jkub.com; kevin.zzux.com; lenovo.wha.la; patton.mrslove.com; tibelds.ddns.us; tibetantimes.ezua.com; zeeza.info</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 4, Tibet Group 5</td>
</tr>
<tr>
<td>TTI Range</td>
<td>1.25 - 3.75</td>
</tr>
</tbody>
</table>

A new campaign using Surtr as the primary malware family emerged in August 2013, about one month after the DTL attacks stopped. This campaign’s C2 infrastructure consists of free ChangeIP domains. This campaign uses throwaway AOL and Gmail accounts designed to impersonate real people and legitimate organizations to deliver malicious emails. There is no overlap with infrastructure seen in any other campaigns, but this could simply be the result of the use of dynamic DNS and free subdomains.
Although this cluster uses dynamic DNS, the domains will often resolve to the same IPs at the same time, as shown in Table 12.
This is the only campaign outside of DTL that we have seen use Surtr. Like the DTL campaign, the primary attack vector is malicious email attachments using CVE-2012-0158.

We have identified 67 attacks related to this campaign since we first discovered it in August 2013. It began with two unique emails sent to Tibet Groups 2 and 4 on August 1, 2013. The message to Tibet Group 2 appeared to be an internal mailing list used by its steering committee and staff. The message requests that the list administrator approve a mailing list posting. The message sent to Tibet Group 4 purported to be from “Tibeta Associatio” (sic) and referenced Tibetan autonomy in the subject line but had no message in the email body. Both attacks use .rtf files that drop Surtr (GtRemote) and connect to free1999.jkub.com.

For the first year of the campaign, Surtr was used exclusively. In July 2014, this campaign began using a variant of PlugX. This version removed the identifying strings found in previous versions of the malware. The variant still used the DLL side loading technique found in previous versions, albeit with a different legitimate executable. It also contained the same functionality. A notable difference was that the malware did not load a properly formed executable into memory, in what appears to be an attempt to hinder analysis.

At the time of writing, this campaign remains the main source of attacks targeting Tibetan Groups, and we are continuing to monitor developments.
EXTENDED ANALYSIS:

2.3

Civil Society Perspectives and Responses
Over the course of the study we conducted interviews and site visits with nine of the 10 groups participating in our study. The interviews were intended to provide greater context into the perceptions and implications of the attacks documented in this report. The interviews were transcribed and coded to identify emergent themes. This section reflects those themes as section headers, which are as follows:

- Information communication technologies (ICTs) as an enabler and threat to civil society groups
- How our participants perceive digital risks and threats
- The impact of targeted attacks
- Civil society responses to targeted attacks

Each section, in turn, draws on participants’ responses, alongside our synthesis, to provide a window into how groups under threat think about and respond to digital threats. In general, we documented groups at different stages of addressing digital security. Some groups had taken on digital security as a core part of their mission before the study began. Others had only begun to notice issues about digital security a few years ago but by the time of interviewing spoke to us about digital threats as a structural problem for their operations. Still, many were in the process of trying to decide on what measures to take, and how to implement them systematically.

**ICT: Enabler and Threat to Civil Society Groups**

ICTs are central to the activities of the groups, and help them balance an historic asymmetry between them and powerful, well-resourced state interests.

> [Technology] is the only way you can have any serious impact if you’re a size like us and you are trying to go up against the Chinese government which has considerabl[y] more resources than us. So if you want to try to

---

12 We were unable to conduct interviews and a site visit with China Group 2.

have an impact, technology is the leverage.\textsuperscript{14}

The two large human rights organizations in our study both operate distributed programming across multiple countries with hundreds of staff and partner organizations. The size and complexity of these operations makes these groups highly reliant on technology.

\textit{Now we do work in more than 80 countries at any given time, and we have staff based in many cities across the world.}\textsuperscript{15}

The theme of diaspora communications was central to groups related to Tibet and China. The Tibet Groups, for example, find that technology enables them to reach into restricted environments from “safe” areas overseas.

\textit{In comparison to other communities, there is almost nowhere that is so physically separated because of the restraints imposed by China….Even in Pyongyang, you got foreign journalists...Tibet is just closed off....Technology is the only way that that can be bridged.}\textsuperscript{16}

ICTs are also the primary tool that organizations used to connect with the highly distributed and fractured community in the Tibetan diaspora and in Tibet.

\textit{Those of us born and raised in exile, and certainly our parents and other generations, crave to go home to this land they are so attached to. Then technology comes along and it’s like BOOM! You can have it all…on some level even though the Chinese are still there and physically we can’t do it, but in this other space we can.}\textsuperscript{17}
WECHAT: CONNECTIVITY AND RISKS

WeChat is a mobile chat application developed by Chinese company Tencent, which has gained huge user numbers around the world with a high concentration in China. Tibet Groups cited WeChat, which is highly popular in their community, as an example of the tension between connectivity and security. This connectivity was seen as beneficial, but not without risks.

“All new ground shows up like WeChat...and it threatens to both undermine [our efforts] and offers us some ideas for what it is people want and [what they’re] willing to compromise for the sake of connection.”—Director, Tibet Group 1

“All Tibetans in India and Nepal, Tibetans in the West are all being connected by using the same app...and forging these new connections...in some ways, we’re seeing really good things come out of it in terms of all the news we’re getting from Tibet and seeing all the footage from the self-immolations and protests coming from WeChat and in that sense it’s becoming important, but people are not so attuned to the risks.”—Program Officer, Tibet Group 1

Tibet Groups voiced concerns over the increasing popularity of WeChat due to censorship and surveillance requirements on companies operating in China, and the close relationship between Tencent and the Communist Party of China. Adding to these concerns are a series of documented incidents of Tibetans in Tibet being arrested for content they shared on WeChat, like images of HHDL.

Civil society and its champions are not the only groups who felt that technology could enable movements to push back against the status quo. A Tibetan group noted that they thought the Chinese government, was also very concerned about its potential.

...self immolations and protests...the Tibetan cultural pride, the songs...this is the reason the Chinese are cracking down so hard and going after everyone ..... the censorship and the surveillance is...[happening] because the technology has showed them what’s possible. There is a movement now where there wasn’t one or where it had almost disappeared before... the technology has enabled that.18

Yet the ability to connect is constantly eroded by efforts to monitor and interfere with groups’ activities. Participants also recognized that their reliance on technology intro-
duced new risks of monitoring, coercion, and electronic attack.

[Technology is] this funny thing where it’s a life line, and then it’s...maybe your ticket to jail.\textsuperscript{19}

Groups need members of their communities to maximize the use of ICTs but also to do so securely.

We...need this technology, but we need everybody to know how to use it and be able to be secure and be safe.\textsuperscript{20}

Targeted digital threats are also changing how some CSOs see the promise of technology.

I think that civil society is feeling the heat around targeted attacks and surveillance and I think it’s affecting the public sphere and our ability to feel comfortable communicating in what used to be understood as a free and open medium.\textsuperscript{21}

In practice, CSOs are in a constant process of navigating through new communication environments, and tradeoffs between connectivity and security. Contrasting theories have popularly characterized ICTs either as “liberation technologies” that can empower political movements, or as levers of control for governments to suppress these very same movements.\textsuperscript{22} Our participants suggest that the reality is somewhere in between.

How Civil Society Groups Perceive Risk and Threats

We tried to elicit participants’ informal “threat models” as a precursor to understanding how these models shaped their response to digital risks.\textsuperscript{23} All of the groups in our study work on political issues that can potentially be seen as threatening to specific authorities. The context of this work makes many groups perceive the attacks against them as politically motivated.

\textsuperscript{19} Tibet Group 1, Director, 2011
\textsuperscript{20} Tibet Group 1, Program Officer, 2011
\textsuperscript{21} Rights Group 2, Technical Officer, 2014
\textsuperscript{23} A threat model assesses the risk and relative impact of threats against an entity that are specific to the context in which it is situated.
Although political concerns were a backdrop to the attacks, groups tended to focus on the tactical goals of the attackers rather than the greater political objectives. Groups described the probable goals of attacks as efforts to “hinder our operations,” “keep an eye on things,” or cause as much “inconvenience and chaos as possible [to] somehow affect our ability to do what we do.”

While groups shared similar views on the operational objectives of attackers, their sense of risk stemming from attacks depended on the physical proximity of their adversary. A program manager with extensive field experience working with CSOs in multiple countries explained that groups operating within the jurisdiction of an adversary have greater concerns over physical security and other direct interference from authorities.

...in many places it’s a very physical sort of thing. Our biggest challenge...[was when]...local authorities wandered in and took computers. So it’s not like we expect the attacks to be all coming in over the wire. In most places where we operate it’s probably not even the easiest place for them to get at although it is certainly a lot more subtle.

If a group is situated outside of a physical jurisdiction controlled by an adversary then targeted digital threats may be a higher priority concern than physical threats.

Take for example Ukraine where they aren’t necessarily expecting a lot of challenges with their local government, but they might be a target for cross border action, that is one of the places where the digital threats become a particular vector or focus rather than just one of the many things that they are thinking about.

**DIASPORA AND EXILE COMMUNITY THREAT MODELS**

Many of the participants in our study working on China and Tibet issues are embedded within geographically distributed diaspora networks. Their missions often include collecting information from closed areas “inside,” while transmitting other information back in. As the director of an organization working on China explained:

---

24 Rights Group 1, Chief Technical Officer, 2011; Tibet Group 2, Executive Director, 2014

25 Rights Group 1, Program Manager, 2014

26 Rights Group 1, Program Manager, 2014
Our main target and focus is on the mainland. And so the people who [we] are trying to promote, the people who we are trying to give platforms for their issues and their problems and their voices are inside.\textsuperscript{27}

A central concern of these groups was the security of the bidirectional flow of information to and from at-risk persons in China and Tibet. A group working on China perceived its adversary as primarily interested in this information exchange.

Anyone who doesn’t want [our organization] to be able to safely and securely get information from inside...and send it back in. What kind of information? Individual case information, human rights information... Anyone who has an incentive not to have people know about it would have the incentive to compromise our operations and make it hard for us -- and that’s a lot of people.\textsuperscript{28}

Due to the antagonistic response these activities elicit from the Chinese government, the Tibet and China Groups generally perceived the actors behind targeted digital attacks on their community to be directed by or related to agents of the PRC.

I think in most cases, [the staff] believe it’s coming from China.\textsuperscript{29}

Tibetan groups in exile perceived Tibetans living “inside” as having the highest likelihood and impact of harm from digital attack. To demonstrate the potential consequences of targeted digital threats, a Tibetan security trainer explained how he presents the connection between actions outside affecting at-risk groups inside Tibet.

I kind of force them into thinking about like the risk associated with Tibetans inside Tibet, and also kind of like stress the fact ‘We are in a free country, we don’t have to worry about ourselves...What can the Chinese government do to me? Nothing. But what happens when you have done something that’s harming somebody else inside Tibet?’ ...that’s when a lot of people think about it a little more.\textsuperscript{30}

The threat models of groups working on China and Tibet show a priority given to digital threats due to the proximity of these groups to their perceived adversary and the years of persistent attacks they have experienced.

\textsuperscript{27} China Group 1, Director, 2010
\textsuperscript{28} China Group 1, Director, 2010
\textsuperscript{29} China Group 1, Technical Project Manager, 2014
\textsuperscript{30} Tibet Group 1, Digital security trainer, 2013
Our study exclusively addresses digital threats and does not cover all potential threats a group may face. While digital threats are a primary security concern for the majority of groups in our study, they are just one piece of a holistic risk environment for CSOs.

**Impact of Targeted Threats on Civil Society Groups**

Most participants were clear that they saw potentially severe consequences from targeted digital attacks, with the greatest danger being to communications with those “inside,” and hence vulnerable to arrest or harassment. Nevertheless, a few participants surprised us by noting that their organization downplayed the possibility of negative consequences from attacks (or had done so in the past). Often this reaction took the form of citing the ‘openness’ of their organization’s work, and suggesting that there was ‘nothing sensitive’ in their exposed data.

> This is an organization predicated on virtues of transparency...when I first came here there were a lot of conversations like, ‘Why should we encrypt our email, we are not hiding anything.’  

As evidence of attacks against that human rights organization piled up, however, perceptions began to change.

> ...there has been a sea change in the four years since I have been here...they recognize a riskier threat environment and how it is dealt with.  

Awareness of risks was, however, still a work in progress.

> ...in the last year or two any organization that I have been working with in a closed society or dealing with sensitive topics at least has some sort of hazy consideration that this stuff should be a concern and that’s maybe a change from

---

31 Tibet Group 1, Director, 2011  
32 Rights Group 1, Program Manager, 2014  
33 Rights Group 1, Program Manager, 2014
These responses raise an important issue: the relationship between digital compromises and the use of the compromised information by adversaries is indirect. Unlike the consequences of physical threats, which are often directly observable to a non-expert, the most serious impacts of digital threats are typically at least one step removed from the technology that has been exploited. Making the link between technological threats and “real-world” harm can be challenging, in part due to limited evidence.

... [there has] been little evidence of the direct impact on people’s safety as a result of some of these threats.... [but] our understanding of how surveillance and repressive practices have operated even in pre-digital times provides us with sufficient evidence to understand that there may be a connection. I believe that there has been an increase on the reach of this harm by specialist state actors... 

**CONNECTING SURVEILLANCE AND HARM**

We often heard stories of arrest and detention from groups in the study (and through other Citizen Lab projects) that appeared to be linked to electronic surveillance.

Members of the Tibetan community shared with us accounts of Chinese authorities confronting Tibetans with call records and chat transcripts during interrogations. Meanwhile, research on Ethiopia has revealed that detainees have been presented with similar evidence during interrogations.

In Syria there are also reports of interrogators presenting detainees with records of communications, and cases where accounts of detainees are used to seed malware to contact lists.

In Bahrain, meanwhile, activists were arrested after posting pseudonymous tweets critical of the government. The real identities of these persons may have been discovered by authorities through a technique in which an attacker sends the pseudonymous Twitter account a link to a webpage containing an embedded remote image. When the victim clicks on the link or opens the email, their IP address is revealed to the attacker. Authorities can then link the IP to the target’s true identity through their ISP.

We strongly suspect that these cases are only the tip of the iceberg, and that the digital element in many cases of harm goes unrecognized due to lack of investigation, not lack of incidents.
We also think, however, that by downplaying the consequences of targeted digital threats, some participants were showing us something interesting about the resilience and adaptability of their communication styles, which have co-existed with an adversary that has used extensive monitoring for many years.

...it can be a nuisance, it can be a distraction, it can waste time, but...in the grand scheme of things, it’s not as though the movement on a whole operates in a way that is dependent upon secure conversations.36

Nevertheless, the same participant was very clear that serious (even physical) harm could come to individuals and groups “inside” through targeted attacks against them or their contacts.

PSYCHOLOGICAL IMPACTS AND COPING STRATEGIES

While tracking the consequences of a targeted attack for networks of trust and reputation can be challenging and require investigation, some participants spoke in detail about the psychological impact of compromise.

It was quite upsetting. I think it sort of paralyzed us emotionally—the two of us that were affected—for a few days.37

In this incident, the emotional harm was perceived as more impairing, and less easily mitigated, than the breach to the computer system.

...the act of cleaning our computers was something that was relatively straightforward...but it was the emotional impact that sort of threw us.38

Further work is needed to document the connection between targeted digital threats and psychosocial strain to move towards a more complete understanding of how targeted individuals and organizations evolve and adapt their coping strategies. One interesting coping strategy prevalent among Tibet Groups was to explain attention from adversaries as a signal that their work was important, and was having an impact.

The reason you are a target is because you are doing something that is bothering somebody and to be proud actually of the work that you do that has drawn the attention of these people who clearly want to mess us up somehow.39
As one participant put it, the challenge was to balance the frustration of being compromised with feelings of encouragement:

...we work so hard the entire day and then at the end of the day when you find out that your website has been attacked and people can’t get access to it, you get frustrated, but at the same time you also get more encouraged to know that... feeling that your work is making an impact and the Chinese government has to go to the extent of spending time following us and attacking us and spending large amounts of money just for that.40

BEING TARGETED: A TEACHABLE MOMENT

Beyond trainings and awareness campaigns, what brought threats home, unsurprisingly, was being targeted or compromised. Being attacked personalized the problem, and turned warnings into tangible concerns.

[It] is visible for users in places that they understand—your email, your Twitter account—even if they don’t understand the implications, the connections...they now see it as something real and personal.41

Tibet Groups felt that the persistent targeting of their community has helped them raise awareness of digital security and highlight the need for vigilance.

It has made Tibetans more aware of the potential of the Chinese government. We always think about the Chinese government creating problems for us diplomatically, we don’t think of the cyber world...and how they can maneuver their way into it.42

[The attacks]... give us as a reminder to be more careful.43

Groups made it clear that greater awareness is a work in progress, and that documenting the connection between attacks and specific harms to individuals and groups is a promising way forward.

The basic goals should be to get people to realize that these threats are real... the

40 Tibet Group 3, Editor-in-Chief, 2014
41 Rights Group 2, Technical Officer, 2014
42 Tibet Group 3, Editor in Chief, 2014
43 Tibet Group 5, Program Officer, 2014
Civil Society Responses to Targeted Digital Threats

As groups struggled with targeted threats, many placed an emphasis on awareness raising and user education as a primary method of responding. These kinds of strategies are important for civil society and applicable to a variety of problems. The fact that many of the digital threats they experience rely on social engineering makes this a promising direction. However, responses from the groups also suggest that resource constraints, and limits on available technical expertise, may have constrained other avenues of response.

RESOURCE AND CAPACITY CONSTRAINTS

The most commonly mentioned challenge to addressing digital threats was, unsurprisingly, resource issues in general, and technical resources and skills in particular:

> Every community with a struggle is under-resourced, and if this hasn’t moved up the priority list, they don’t have the capacity to do this type of stuff or implement it or there’s not even enough awareness that is needed for them to be able to get people to pay attention.  

Organizations in the Global South

These challenges are especially acute for groups in the global South. All Tibet Groups in our study had their operations or a portion of their operations based in Dharamsala, India. In this context, the groups are operating within a refugee community grappling with persistent targeted attacks and conventional development challenges. Resources are sparse. These groups cannot afford enterprise computing infrastructures, or the expensive security solutions adopted by larger, well-resourced counterparts.

Complicating these challenges is the problem of “brain drain” of technically skilled people in the community. Participants told us many Tibetans with specialized technical training

44 Tibet Group 1, Program Director, 2011

45 Tibet Group 1, Director, 2011
leave Dharamsala in search of better job prospects elsewhere. Tibet Groups saw the need to create opportunities for Tibetans with technical skills to work in the community:

[Tibetans living in exile in India] are essentially a refugee population and all these folks want to get jobs. So, if we can actually bring them in and give them jobs in supporting their own community, that’s kind of a goal.46

Others, on the same topic, suggested that the problem was improving, slowly:

I think now it’s coming up slowly and slowly, but there was a time in the Tibetan community where we really lacked webmasters, where we really lacked people who are well equipped and who have good knowledge in terms of Internet security. 47

These challenges are not unique to the Tibet Groups. Rights Group 1 explained that local partners supported by the group faced similar technical capacity difficulties:

Security is hard and it’s much harder than it needs to be....the challenge of trying to keep your stuff in some kind of secure state as is currently defined is just well beyond what any typical partner organization is able to deal with...For most of our partners they are lucky if they have a young guy who understands a bit about computers.48

A particularly common problem for groups in the global South is the use of pirated software (unpatched or pre-backdoored software is often a source of insecurity). The use of pirated software is widespread in the Tibetan community due to prohibitive licensing costs. Similarly a program officer in a large rights group explained it is difficult to convince a local partner to purchase a software license “when you can jump out to the local market, [and] for a dollar buy a disk.”49

**Larger Organizations**

Two of our participating organizations, Rights Groups 1 and 2, had significantly higher technical capacities and financial resources, and they approached information security in a manner similar in some ways to a large company. For example, the groups have senior management in charge of security and technology, IT support teams / help desks, and occasionally hire companies to provide security consultations

---

46 Tibet Group 1, Program Director, 2011
47 Tibet Group 5, Program Officer, 2014
48 Rights Group 1, Program Manager, 2014
49 Rights Group 1, Program Manager, 2014
and incident response services. However, although the size and resources of these groups afford them certain advantages over smaller groups, they experience equally vexing security challenges.

The complexity of global operations and distributed staff and partners creates problems for introducing and sustaining security awareness, even as attacks seem to increase:

> We have seen a colossal uptake on attacks on the home office or we are just much more aware of them than we used to be. We anticipate that such things are also happening at the field office level and to our partners, but we have much less visibility into that.\(^{50}\)

The lack of network visibility among in-country offices was cited as a particular challenge:

> We don’t have a unified network with all our field offices... so we don’t have the same enterprise level of security and capacity there...[the field offices and NGO partners] have to face a range of threats that are from the physical world as well.\(^{51}\)

Both groups face challenges adapting technology policies for regional offices and partner organizations. Rights Group 2, for example, contended with securing its head office and maintaining awareness of threats faced by field offices:

> There’s not a lot of security awareness in the organization. There’s ... small pockets of knowledge, but the rest of the organization will prove to be the weakest link....people don’t understand, especially people that work in the field don’t understand the sensitivity of the work the organization does, so they tend to be a bit more lax about... certain things.\(^{52}\)

Bureaucratic processes were seen as hindering the adoption of new security policies, given the challenge of informing decision makers about emerging security issues:

> I think it has been very top-down, you know some [policy] comes from the top, they go to the bottom and there is no way to inform what’s going on in the decision process.\(^{53}\)

---

50 Rights Group 1, Program Manager, 2014  
51 Rights Group 1, Program Manager, 2014  
52 Rights Group 2, Technical Officer, 2014  
53 Rights Group 2, Technical Officer, 2011
TRAINING AND USER EDUCATION

While the two large groups were able to invest in security appliances and dedicated technology support, the other groups in our study focused on user education and awareness as the primary security strategy.

The majority of groups focused on internal training programs and training with partner groups. Five were able to conduct these trainings themselves, while four others drew on third-party support. These trainings varied widely, ranging from short explanations of security policies to sustained user education programs.

Several key themes emerged from our interviews about digital security trainings: the value of understanding the local context, the need for training based on organization-specific threat models, and the value of focusing on behavior rather than simply teaching a wide range of tools.

Training informed by local context and threat models

While user education and training were a major part of groups’ strategies, most highlighted the importance of situating trainings in local context and using accessible language and concepts.

*If we could break it down for people in a way that they understand, if we could give them metaphors and other ways to understand what exactly this means for us, and paint the bigger picture, it has an impact.*

Rights Group 1 explained that conducting formal risk assessments of its partner organizations was key in developing appropriate educational strategies.

Other groups engaged in training shared similar comments and noted the importance of ensuring trainings are in line with both technical and contextual realities. Several interviewees pointed out that keeping abreast of new technical developments and context-specific risks was challenging and time-consuming, highlighting the value of intermediary organizations that perform this role within a particular targeted civil society context. Indeed, Tibet Group 1 went so far as to structure its mission to focus on digital security awareness and education programs for the Tibetan community.

---

54 Rights Groups 1, 2; China Groups 1, 3; Tibet Group 1
55 Tibet Groups 2, 3, 4, 5
56 Tibet Group 1, Director, 2011
group provided training support to all the other Tibetan organizations who participated in the study.

**Moving Beyond Tools**

All of the groups identified a common set of user practices for preventing infection of malware: not opening unsolicited attachments, being careful with web links, keeping systems up-to-date, and generally remaining vigilant online. Explaining the safe and secure use of tools was an aspect of training, but many groups focused more on how to change behaviour and develop a security mindset rather than train specific tools.

> [We are] trying to equip people with a different mindset, so that they are changing their behaviors...so they...run through a mental filter before doing something.\(^{57}\)

Tibet Group 1, which regularly provided trainings to its peers, was particularly adamant about the need to focus on user behaviour over specific tools:

> We would really like to see resources shift from trying to mitigate problems through tools, to mitigating problems through education and educating people about their practices.\(^{58}\)

The Tibet Groups felt that user education had to be a community-wide effort and not something isolated to particular organizations or individuals. For example, some Tibetan groups have been promoting a “Detach from Attachments” campaign that encourages users to move away from sharing documents through email attachments and shift to alternative cloud-based platforms like Google Drive. The campaign uses a mix of humor and references to Tibetan culture and is a good example of user education that is connected to a specific threat model and local context.

Encouraging behavioural change and implementing new organizational policies can be challenging. Tibet Group 5 explained that while malicious attachments were a priority threat for the group, moving to alternative document platforms was difficult due in part to generational gaps in the group’s membership. Users from older generations, they explained, were resistant to changing familiar practices, like the use of attachments.

Understanding these organizational challenges and breaking down trainings into simple incremental steps that can be adapted to specific environments were identified as keys

---

57 Tibet Group 1, Director, 2011

58 Tibet Group 1, Program Director, 2011
to success. A Tibetan security trainer described the importance of showing people small victories from their point of view and demonstrating how they can learn to achieve ICT objectives in ways that are safe and secure, but also do not appear too difficult for them to use in their daily workflows. Others agreed, saying that their goal was to find techniques that made it “as simple as [possible] to do the right thing...”

Indeed, there were some cases where, if implemented effectively, modest behavior modifications could have a considerable impact. While we observed organizational challenges in implementing practices like “Detach from Attachments,” based on what we have seen, the campaign could be effective against some of the current threats against the Tibetan community. More than 80% of malware submitted to us by Tibet Groups used a malicious email attachment. Furthermore, for two of the Tibet Groups in our study, simply not opening attachments would mitigate more than 95% of targeted malware threats that use email as a vector.

However, this is just one mitigation strategy focused on a single vector of attack. Threat actors are highly motivated and will likely adapt their tactics as users change their behaviors. For example, it is possible that if every user in a particular community began to avoid opening attachments, attackers would move on to vectors such as watering hole attacks or attacks on cloud-based document platforms.

As the groups themselves noted, user education and awareness-raising activities need to be ongoing, and must be informed by local context, threat models, and the latest technical information.

59 Tibet Group 1, Security Trainer, 2013
60 Rights Group 1, Program Manager, 2014
61 This determination is based on two groups that had submitted at least 40 emails.
COMMUNITIES @ RISK
Targeted Digital Threats Against Civil Society
November 11, 2014
https://targetedthreats.net/
EXTENDED ANALYSIS:

2.1
Summary, Methodology, and Data Overview
Communities @ Risk: Targeted Digital Threats Against Civil Society reports on an intensive study that analyzes targeted digital threats against 10 civil society organizations (CSOs) over a period of four years.

The report combines two major sections:

1. The Executive Summary provides detail on how the study was organized and why we feel it is important to read, a high-level overview of the key findings of the research, and considerations about next steps for several stakeholder communities in responding to targeted digital threats.

2. The Extended Analysis explains our methodology, and examines the detailed data we gathered during the study period. It is the evidentiary basis for the claims we make in the Executive Summary, and will likely be of interest to a more specialized audience (although we hope everyone will read it).

KEY FINDINGS

In the Executive Summary, we outline five high-level findings. We summarize them again below, while adding more granular details that are given extended treatment in the analysis that follows.

In the digital realm, CSOs face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.

Through cluster analysis we identify 10 distinct targeted malware campaigns. We find that five of these campaigns have connections to threat actors, previously reported to have targeted government and private industries. CSOs have limited resources and technical capacity, which makes responding to threats a challenge. We generally find that, due to resource constraints, CSOs focus their digital security strategies on user education and behavioural change rather than expensive technical solutions.
Counterintuitively, technical sophistication of malware used in these attacks is low, but the level of social engineering employed is high.

We develop the Targeted Threat Index, a metric for quantifying and characterizing the sophistication of targeted malware attacks. Using this metric, we find that the technical sophistication of targeted malware delivered to CSOs in our study is relatively low (e.g., relative to commercial “lawful intrusion” surveillance kits and conventional financially motivated malware), with much more effort given to socially engineering messages to mislead users.

Digital attacks against CSOs are persistent, adapting to targets in order to maintain access over time and across platforms.

Our analysis of attacks against CSOs over four years allows us to track how attackers change tactics. For numerous malware samples, we observe several versions of the malware appearing over the course of our study. These multiple versions show evidence of technical improvements to complement increasingly refined social engineering techniques. In some cases, we observe threat actors quickly changing tactics to adapt to shifting platform adoption and user behaviour.

Targeted digital threats undermine CSOs’ core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety.

The impact of targeted digital attacks against technical systems is apparent and receives ample attention from researchers. However, we find evidence of wider impacts that are not always as obvious, including psychosocial strain and possible connections to physical harms (e.g., arrest and detention). Tracing connections between compromises and harm is challenging, because the relationship between digital compromises and the use of the compromised information by threat actors is indirect. Unlike the consequences of physical threats, which are often readily observable, the most serious impacts of digital threats are typically at least one step removed from the technology that has been exploited.

Targeted digital threats extend the “reach” of the state (or other threat actors) beyond borders and into “safe havens.”

The ways CSOs develop their perceptions of risk and threat stemming from targeted attacks depend in part on the physical proximity of their threat actor. Groups operating within the jurisdiction of a repressive regime have greater concerns over physical security and other direct interference from authorities. Conversely, groups situated
outside of a physical jurisdiction controlled by an adversary may prioritize digital threats over physical threats. For groups in diaspora and exile communities, targeted digital threats can be seen as a means for a powerful threat actor, such as a state, to extend their reach beyond borders and into “safe areas.”

EXTENDED ANALYSIS STRUCTURE

The Extended Analysis is structured into the following three sections. Each of these sections can be downloaded individually or read as a whole.

Summary, Methodology, and Data Overview outlines our mixed methods approach which incorporates analysis of technical and contextual data using methodologies from the field of information security and the social sciences, and presents a high level overview of our dataset.

Cluster Analysis provides detailed technical analysis of 10 distinct targeted malware campaigns.

Civil Society Perspectives and Responses reports on results from interview data and is a window into how groups under threat think about and respond to digital threats.

We also are publishing data that provide indicators of compromise (including YARA signatures of malware families, MD5 hashes of samples, and command-and-control servers), which are available on our github account and accessible through our project website.
Methodology

This section describes our methodology for data collection and analysis. Since our study involves the collection of potentially sensitive information from civil society organizations, and requires us to deal with personally identifiable information (PII), we consulted with the University of Toronto’s Research Ethics Review Board during the design of our study. The methods described below have been submitted to and approved by this board.

STUDY PARTICIPANTS

We recruited participants via three channels: (1) an open call on our website, (2) outreach to organizations with which we had prior relationships, and (3) referrals from participating groups. As part of the study, these groups agreed to share technical data (e.g., emails with suspicious attachments) and participate in interviews. Their identity and any PII shared with us were kept strictly confidential.

Organizations with a mission concerning the promotion or protection of human rights were eligible to participate. We also considered, on a case-by-case basis, organizations with a mission that does not directly address human rights, but which may engage in work related to human rights issues (e.g., media outlets that regularly report on human rights violations).

In total, 10 organizations participated in the study. The majority of these groups work on China-related rights issues, and five of these organizations focus specifically on Tibetan rights. The exceptions to the China-/Tibet-focused groups in our study are two large organizations that work on multiple human rights-related issues in various countries.

For purposes of this study, “human rights” means any or all of the rights enumerated under the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; and the International Covenant on Economic, Social and Cultural Rights.
TABLE 1: Study organizations

<table>
<thead>
<tr>
<th>ORGANIZATION CODE</th>
<th>DESCRIPTION</th>
<th>ORGANIZATION SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rights Group 1</td>
<td>Human rights organization focused on multiple issues and countries</td>
<td>Large (over 100 employees)</td>
</tr>
<tr>
<td>Rights Group 2</td>
<td>Human rights organization focused on multiple issues and countries</td>
<td>Large (over 100 employees)</td>
</tr>
<tr>
<td>China Group 1</td>
<td>Human rights organization focused on rights and social justice issues related to China</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>China Group 2</td>
<td>Independent news organization reporting on China</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>China Group 3</td>
<td>Human rights organization focused on rights and social justice issues related to China</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 1</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 2</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 3</td>
<td>Independent news organization reporting on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 4</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
<tr>
<td>Tibet Group 5</td>
<td>Human rights organization focused on Tibet</td>
<td>Small (1-20 employees)</td>
</tr>
</tbody>
</table>

Tibet Groups

Dharamsala is a small city in northern India set on the foothills of the Himalayas. His Holiness the Dalai Lama (HHDL) has lived in Dharamsala since 1959 following his escape from Tibet. Dharamsala is the base of the Central Tibetan Administration, which administers programs and schools for Tibetan refugees living in India and advocates for the rights of Tibetans in Tibet. It is also home to many Tibetan NGOs and independent media groups, and thousands of Tibetan refugees. This high concentration of prominent Tibetan institutions makes Dharamsala a prime target for malware campaigns. It has been called one of the most hacked places in the world. For exiled Tibetans, this heightened level of digital risk compounds the many challenges of living as refugees in a developing country.

Three of the Tibet Groups in our study are headquartered in Dharamsala, and two
maintain regional offices there. Across these groups participants expressed challenges related to awareness of threats, low resources, and limited technical capacities.

Tibet Groups reported varying levels of awareness of digital risks in the community. While many participants noted that security awareness was generally increasing among Tibetans, others cautioned that some groups still do not have policies or response plans around targeted digital attacks and “continue to back burn things like security.”

A major challenge identified by the Tibet Groups is a lack of technical capacity and resources in the community. Most Tibetan NGOs do not have dedicated system administrators. In some groups, staff members responsible for web development also take on double duty as system administrators. In addition to local staff, there are transient volunteers who come into the community to help with technical projects. As one of these volunteers noted, however, when volunteers leave the community projects sometimes end up unmaintained or completely abandoned.

While the unique circumstances of the Tibetan exile community are challenging, some groups are also taking proactive measures to increase digital security awareness. For example, one of our participating organizations prioritizes digital security in the community within its mission, focusing on raising awareness and user education. These grassroots initiatives demonstrate a growing commitment to addressing security challenges, despite ever-present resource limitations.

China Groups
The three China Groups all work on issues related to human rights and politics in China, but from outside of mainland China. China Groups 1 and 3 each have a central office and one regional branch. China Group 2 operates an independent news website from an office with limited staff. China Group 1 has a program manager that oversees technical projects, but does not have a dedicated system administrator on staff. Instead the group outsources management of its information technology infrastructure to a private company. China Group 3 has had a dedicated system administrator since its founding.

The work of these groups is politically sensitive and has attracted attention from Chinese authorities. China Groups 1 and 2 especially have come under pressure for
human rights advocacy and the dissemination of sensitive news, respectively. As China Group 1 explained, “Chinese authorities ... have very clearly in public designated us as an anti-China organization.”

These groups are all highly aware of targeted digital threats, and have experienced numerous prior incidents. All of the groups had received targeted malware in the past and their websites are consistently blocked in China. The website of China Group 2 has been repeatedly hit by distributed denial-of-service attacks.

Rights Groups

Rights Groups 1 and 2 are much larger organizations relative to the others in our study. Both have over 100 employees, multiple offices, enterprise level computing infrastructures, and dedicated IT teams and support desks.

These groups act as hub organizations. Rights Group 1, for example, supports multiple regional offices and CSO partners around the world. Rights Group 2, similarly, operates regional branches and is responsible for a large group of staff operating in numerous field locations.

Both groups contend with securing their head offices and maintaining awareness of threats faced by field offices. These challenges show that while the Rights Groups have greater resources they must grapple with a potentially wider spectrum of threats in multiple contexts and countries.

DATA SOURCES

Email Submissions: The majority of data collected consisted of emails identified by participants as suspicious, which were forwarded to a dedicated mail server administered by our research team. When available, these submissions included full headers, file attachments, and / or links.

Relying on forwarded emails presents a collection bias as the recipients must be able to identify that the emails are suspicious and remember to forward the samples to our research team. This collection method also limits the threats studied to those that are sent over email. Additionally, collection of forwarded email samples does not allow us to verify if a targeted organization was successfully compromised by an attack, or the scope of the attack. Recognizing this limitation, we added two more data collection methods to complement the collection of emails.
Network Intrusion Detection System: As an optional study component, we offered to install a network intrusion detection system (NIDS) inside the networks of the participants. In total, seven groups opted into the NIDS project. We used a combination of community and commercial rulesets, as well as a set of custom rules based on threats we analyzed from the email submissions. By placing a NIDS inside an organization’s network, we were able to record incoming threats using vectors other than email, as well as detect and observe systems that had already been compromised.

Website Monitoring: We conducted external scans of the study organizations’ websites to monitor for potential compromises such as watering hole attacks. These scans were done with publicly available tools including Cyberspark and URL Query.

Interviews and Fieldwork: To gain insights into the experiences of our groups, we conducted a series of semi-structured interviews over a four-year period and made site visits to their offices and locales. While there have been previous technical studies on targeted threats affecting CSOs, it is rare that the context surrounding these attacks and the experiences of the people facing them are properly explored. Interviews and site visits help provide insight into these vital elements.

When possible we conducted interviews with a senior staff member responsible for organizational programming (e.g., executive director, program manager), and a staff member responsible for technical support (e.g., system administrator, webmaster). The interviews explored the organizations’ uses of and policies around technology, perceptions of digital security and threats, responses to threats, and the impact of threats. These interviews, coupled with site visits and participant observations, helped us understand the working conditions, routines, infrastructure, and local social and political context that form the day-to-day environment of our participants.

Interviews were held opportunistically and did not follow a set schedule. The total number of interviews per group is outlined in Table 2. The majority of interviews were audio recorded and transcribed. In some cases, conditions did not allow for audio recording and field notes were made instead. Interview transcripts were analyzed using line-by-line open coding of transcripts to identify emergent themes.3

---

TABLE 2: List of interviews conducted with participating groups*

<table>
<thead>
<tr>
<th>GROUP</th>
<th>SUBJECTS</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>China Group 1</td>
<td>Executive Director, Program Manager (technical projects)</td>
<td>2010</td>
</tr>
<tr>
<td>China Group 3</td>
<td>System Administrator</td>
<td>2011</td>
</tr>
<tr>
<td>Rights Group 1</td>
<td>Chief Technical Officer, Program Manager</td>
<td>2012, 2014</td>
</tr>
<tr>
<td>Rights Group 2</td>
<td>Technical Officer</td>
<td>2011, 2014</td>
</tr>
<tr>
<td>Tibet Group 1</td>
<td>Executive Director, Program Director (technical projects), Program Officer, Security Trainer</td>
<td>2011, 2012, 2013</td>
</tr>
<tr>
<td>Tibet Group 2</td>
<td>Executive Director</td>
<td>2013</td>
</tr>
<tr>
<td>Tibet Group 3</td>
<td>Editor-in-Chief</td>
<td>2014</td>
</tr>
<tr>
<td>Tibet Group 4</td>
<td>Technical Volunteer</td>
<td>2013</td>
</tr>
<tr>
<td>Tibet Group 5</td>
<td>Program Officer</td>
<td>2014</td>
</tr>
</tbody>
</table>

*NOTE: We were unable to conduct a site visit and interview with China Group 2, because they did not maintain participation in the project.

DATA ANALYSIS

Malware Analysis: We examined malware samples using static and dynamic analysis tools (e.g., IDA and OllyDbg), as well as manual analysis to extract information on exploits, malware functionality, malware family, command-and-control (C2) infrastructure, and other properties of the malware code (e.g., mutex and exported function names).

Email Content Analysis: We reviewed the subject line, body, and attachments for each submitted email and grouped the content into specific themes and categories. The header of each email was analyzed to determine if the sending email address was spoofed or the email address was otherwise designed to appear to come from a real person and / or organization. Indicators drawn from this analysis were used to assess the relative sophistication of the social engineering tactics found in the messages (we incorporate these indicators into our Targeted Threat Index described below). We conducted regular inter-rater reliability checks that flagged any potential edge cases and inconsistencies for discussion and re-evaluation.
**Targeted Threat Index**: We developed the Targeted Threat Index (TTI), which is a metric that characterizes and quantifies the sophistication of targeted attacks, to provide a consistent ranking of how advanced any given targeted malware attack is. The TTI score is calculated by taking a base value determined by the sophistication of the targeting method, which is then multiplied by a value for the technical sophistication of the malware. The base score can be used independently to compare emails, and the combined score gives an indication of the level of effort an attacker has put into individual threats.

**Cluster Analysis**: Through identification of patterns in malware families, development cycles, shared infrastructure, and social engineering tactics, we identified relationships between attacks and, when possible, linked them to known malware campaigns and threat actors.
DATA OVERVIEW

A high level overview of our datasets

EMAIL SUBMISSIONS

The malicious emails analyzed in this report span more than four years, from October 10, 2009 to December 31, 2013. During this period we collected 817 emails from the 10 groups participating in our study.

**FIGURE 1:** Cumulative number of email submissions per month during the study

Figure 1 shows the cumulative number of email submissions per month over the course of the study. Although the first formal submission was received on November 28, 2011, some groups had existing archives of malicious messages received by their members, and they provided us with these older emails. Tibet Group 1 ac-
counts for the highest number of submissions relative to the other groups as it was one of the first groups in the study and is persistently targeted. Tibet Groups 2 and 4, which joined the study at a later date (April 2012), show a similar submission rate to Tibet Group 1, suggesting these groups are targeted at a comparable level.

FIGURE 2: Malicious emails by type for groups submitting 25 or more emails

We classify emails as malicious if they include attached malware, a direct link to malware or a drive-by download site, or a link to a phishing page. Figure 2 shows the number of emails of each type for the groups that submitted at least 25 emails to our system. The most common technique employed in these emails was a malicious attachment to the message. However, we observe a higher rate of phishing attacks on the China Groups and the Rights Groups. In particular, 46% of the emails submitted by China Group 1, and 50% of the emails submitted by Rights Group 1, direct the user to a phishing website.

The rate of submissions to our project meant that it was feasible to manually analyze email attachments for malware as they were submitted. This analysis gives us higher confidence in our results than if we had automated the process. Antivirus (AV) signatures frequently fail to detect new or modified threats, and can overlook the kind of malicious payloads that can be identified with manual inspection (e.g., shellcode in an RTF exploit). In total, we analyzed 3,617 payload files and found 2,814 (78%) to be malicious.
MALWARE FAMILIES

We identified malware families through patterns in network traffic and characteristics in the code, such as strings seen in the binaries or names and locations of dropped files. In total, we identified 44 separate malware families (not including variants). The most frequently occurring families are Gh0st RAT, Surtr, Shadownet, Conime, Duojeen, and PlugX.

FIGURE 3: Malware family timeline
(The coloured dots represent attacks using a particular malware family against one of our study groups.)
CVEs

Common Vulnerabilities and Exposures (CVEs) is a dictionary of common names for publicly known security vulnerabilities. CVEs are each assigned a unique identifier code, with the form CVE-YYYY-NNNN, where YYYY indicates the year they were identified and NNNN are arbitrary digits. We identified 24 distinct CVEs used in 483 of the email attacks as displayed in Figure 4.

FIGURE 4: CVEs identified in samples during the study period.
(Vertical gray bars represent the date the CVE was created and orange dots represent targeted attacks using that CVE.)

The most common CVEs we observed were CVE-2010-3333 (used in 112 attacks) and CVE-2012-0158 (used in 294 attacks), which are both vulnerabilities in the way Microsoft Word handles RTF documents. Figure 4 clearly illustrates the shift in use from CVE-2010-3333 to CVE-2012-0158 in March and April of 2012. The popularity of these vulnerabilities is not limited to our dataset. They have been widely used in other attacks against a variety of targets.
During four years of tracking attacks against our groups, we observed only one zero-day exploit. This attack used the Flash vulnerability CVE-2012-5054, and was sent 22 days before the CVE entry was created.

These results show that vulnerabilities exploited by targeted malware attacks against CSOs are typically not technically advanced (compared with financially-motivated malware and commercial lawful intercept kits), and often use old (patched) vulnerabilities. For example, CVE-2012-0158 has been patched since April 10, 2012, but has remained the most common vulnerability used in attacks against the Tibet Groups for well over a year after the fix was issued. The repeated use of this vulnerability suggests the attackers are achieving successful compromises because target systems did not have the latest security updates. A possible explanation is that licensed software is cost-prohibitive for many organizations in the developing world, while pirated copies are easily available, leading many to use pirated operating systems and software.

ANTIVIRUS DETECTION

VirusTotal is a service that scans files through 53 different AV engines and provides a summary of malware detection results. We find that 369 of the 659 samples we received (56%) had been submitted to VirusTotal at the time of writing, with a median AV detection rate of 24% and mean detection rate of 25%. Detection rates were generally low, as 86% of these samples had a detection rate below 50%, meaning that less than half of the AV packages tested were able to identify them as malicious. These results suggest that simply running AV software, although potentially helpful, is not a very effective defence against these attacks.

FIGURE 5: Histogram of antivirus detection rates provided by VirusTotal
This low detection rate we observed is due in part to the extensive presence of CVE-2012-0158, which uses a number of techniques to hide the vulnerability from AV scanners.

One of the simplest of these detection-reducing techniques is modifying the RTF header, since Microsoft Word will still be able to open the file, but fewer AV scanners will detect it as malicious. Another basic technique is encrypting malicious document and providing a password to open the file in the associated email. Simply adding a password to malicious files can help prevent AV detection.

Since there are four ActiveX controllers—ListView, ListView2, TreeView, and TreeView2—affected by this vulnerability and there are no strict syntax restrictions, there can be a large variance in the document templates into which malicious payloads are inserted. These can cause newer templates to initially have lower detection rates.

A notable technique observed was the creation of a MIME HTML (MHTML) file that uses the vulnerable ActiveX controllers. By default, MHTML files are opened by a browser: however, they can also be opened by Microsoft Word, which will trigger the exploit. Since Microsoft Word may not be the default application to open the file, automated sandbox programs may fail to detect the file as malicious.

The older CVE-2010-3333 vulnerability had similar issues with AV detection, because of the wide number of ways to encode the vulnerability. A small change in the way the vulnerability was written could evade signature detection while remaining functionally the same.

Although AV definitions are updated to account for evasion tricks, the lag between the use of evasion techniques in the wild and definition updates results in temporarily low detection rates, and hence the likelihood of successful compromises.
EMAIL CONTENT ANALYSIS

**Subject line, body, and attachments:** The content of the subject line, body, and attachments for each submitted email were content coded into 134 categories grouped under eight themes:

- Country / Region (referring to a specific geographical country or region)
- Ethnic Groups (referring to a specific ethnic group)
- Event (referring to a specific event)
- Organizations (referring to specific organizations)
- People (referring to specific people)
- Political (reference to specific political issues)
- Technology (reference to technical support)
- Miscellaneous (content without clear context or categories that did not fall into one of the other themes)

**Email headers:** The header of each email was analyzed to determine if the sending email address was spoofed, or the email address was otherwise designed to appear to come from a real person and / or organization (for example, by registering an email account that resembles a legitimate sender’s name from a free email provider). We divide the results based on whether they attempted to spoof an organization or a specific person.

Results of this analysis confirm that message content and fraudulent senders are tailored to the interests of the target organizations.

Of the 520 total emails received by the Tibet Groups, 97% referenced content related to Tibetan issues. Email lures leveraged specific events of interest and respected persons in the Tibetan community. Emails referenced Tibetan-related events, including holidays (Tibetan New Year), anniversaries (His Holiness the Dalai Lama’s birthday), and protests (see Table 3). The most frequently referenced events were Tibetan self-immolations (31% of the emails leveraging event-related content).

---

Some of the attachments actually cannot be detected as a virus...We’re not even sure if it...will cause any harm at all. It’s just that the antivirus [is] saying that ‘there’s no threat,’ but obviously there’s something wrong with it.”

—China Group 1
TABLE 3: Breakdown of top five categories in the Event theme for Tibet Groups

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NUMBER OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Immolation *</td>
<td>56</td>
</tr>
<tr>
<td>Tibetan National Uprising Day</td>
<td>24</td>
</tr>
<tr>
<td>HHDL Birthday</td>
<td>19</td>
</tr>
<tr>
<td>Flame of Truth Rally</td>
<td>13</td>
</tr>
<tr>
<td>Kalon Tripa Election</td>
<td>9</td>
</tr>
</tbody>
</table>

* Self-immolations are a controversial form of protest that Tibetans have used as a statement of opposition to Chinese government practices concerning Tibet. These protests have escalated in recent years. At the time of writing, it is estimated that since 2009, approximately 132 Tibetans have self-immolated.

Of the 520 emails received by Tibet Groups, 272 (52%) were designed to appear to come from real organizations. In total 58 organizations were spoofed, of which 53 (91%) were Tibet-related groups (see Table 4). The most frequently spoofed organization was the Central Tibetan Administration. The identities of four of the Tibet Groups in our study (Tibet Groups 1, 2, 3, and 5) were frequently spoofed internally and to external contacts. The frequency of emails with fraudulent contacts from Tibetan organizations shows an effort to have the message appear to come from within the Tibetan community and leverage existing trust relationships.

The emotions of the immolations [are] being used against people to have them click on [attachments].”

—Tibet Group 1

TABLE 4: Breakdown of top five categories in the Spoofed Organizations theme for Tibet Groups

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NUMBER OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Tibetan Administration</td>
<td>58</td>
</tr>
<tr>
<td>Tibet Group 1</td>
<td>26</td>
</tr>
<tr>
<td>Tibet Group 2</td>
<td>13</td>
</tr>
<tr>
<td>Tibet Group 5</td>
<td>13</td>
</tr>
<tr>
<td>Tibet Group 3</td>
<td>11</td>
</tr>
</tbody>
</table>
We see a similar pattern for the China Groups. Of the 48 emails received by the China Groups, 46 (95%) referenced China. Content included references to Chinese political events such as the Communist Party of China (CPC) 18th Party Congress; the June 4, 1989 Tiananmen Square crackdown; and Chinese dissidents and prominent members of the CPC (see Table 5). Of the 48 emails, 13 (27%) spoofed real organizations (see Table 6). Two of our China Groups were spoofed (China Group 1, China Group 3). Rights Group 1 was also spoofed in one message to China Group 1. The remaining spoofed organizations were prominent human rights groups and intergovernmental organizations (e.g., the UN Office of the High Commissioner for Human Rights).

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NO. OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jasmine Revolution</td>
<td>8</td>
</tr>
<tr>
<td>June 4, 1989, Tiananmen Square Crackdown</td>
<td>4</td>
</tr>
<tr>
<td>CPC 18th Party Congress</td>
<td>2</td>
</tr>
<tr>
<td>July 2009 Urumqi Riots</td>
<td>1</td>
</tr>
<tr>
<td>Chinese New Year</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NO. OF EMAIL RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>China Group 1</td>
<td>4</td>
</tr>
<tr>
<td>China Group 3</td>
<td>3</td>
</tr>
<tr>
<td>Office of the High Commissioner for Human Rights</td>
<td>3</td>
</tr>
<tr>
<td>Open Society Institute</td>
<td>2</td>
</tr>
<tr>
<td>Chinese Human Rights Defenders</td>
<td>2</td>
</tr>
</tbody>
</table>

The volume of email submissions from Rights Group 1 and Rights Group 2 was much lower than that from the Tibet and China Groups. However, we also observed content and email senders tailored to these organizations. Rights Group 1 received messages related to human rights issues in Africa and Russia. Of the 12 emails submitted, 92% were made to appear to come from Rights Group 1 email addresses (no other organizations were spoofed). The majority of these messages were phishing attempts with lures related to IT support, designed to gain access to Rights Group 1 email credentials. Rights Group 2 submitted two email samples, both of which were related to human rights issues in the Middle East. One message was made to appear to come from a Rights Group 2 email address.

While the content analysis results clearly show targeted attacks tailored to the interests of targeted groups, content coding alone does no provide a measure of the sophistication of social engineering used in the attacks. In the following section, we describe a metric to determine relative sophistication of attacks.
TARGETED THREAT INDEX

Our dataset includes a wide range of targeted malware threats that have varying levels of complexity. This range presents a challenge in ranking the relative sophistication of the malware and targeting tactics used by attackers.

While metrics such as the Common Vulnerability Scoring System exist for the purpose of communicating the level of severity and danger of a vulnerability, there is no standardized system for ranking the sophistication of targeted email attacks. This gap is likely because evaluating the sophistication of targeting is non-technical, and cannot be automated due to the requirement of a strong familiarity with the underlying subject material.

To address this gap, we developed the Targeted Threat Index (TTI) to assign a ranking score to the targeted malicious emails in our dataset. The TTI score is intended for use in prioritizing deeper analysis of incoming threats, as well as for getting an overall idea of how severely an organization is threatened.4

The TTI Score is calculated in two parts: (Social Engineering Sophistication Base Value) × (Technical Sophistication Multiplier) = TTI Score

TTI scores range from zero to 10, where 10 is the most sophisticated attack. Scores of zero are reserved for threats that are not targeted, even if they are malicious. For example, an email from a widely-spread spam campaign using an attached PDF or XLS file to bypass anti-spam filters would score zero. Sophisticated financially-motivated malware would also score zero if it was not part of a targeted attack.

Social Engineering Sophistication

To measure the targeting sophistication base value we assign a score that ranges from zero to five, which rates the social engineering techniques used to persuade a victim to open a malicious link or attachment. This score considers the content, presentation, and claimed sender identity of the email. This determination also includes the content of any associated files, as malware is often implanted into legitimate relevant documents to evade suspicion from users when the malicious documents are opened. The features for each score are detailed in Table 7 (for examples of emails with each of these scores see Appendix A).

---

### TABLE 7: TTI base value score

<table>
<thead>
<tr>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>Not targeted</strong>&lt;br&gt; - Recipient does not appear to be a specific target.&lt;br&gt; - Content is not relevant to recipient.&lt;br&gt; - The email is likely spam or a non-targeted phishing attempt.</td>
</tr>
<tr>
<td>1</td>
<td><strong>Targeted, Not customized</strong>&lt;br&gt; - Recipient is a specific target.&lt;br&gt; - Content is not relevant to recipient or contains information that is obviously false with little to no validation required by the recipient.&lt;br&gt; - The email header and / or signature do not reference a real person or organization.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Targeted, Poorly customized</strong>&lt;br&gt; - Recipient is a specific target.&lt;br&gt; - Content is generally relevant to the target but has attributes that make it appear questionable (e.g., incomplete text, poor spelling and grammar, incorrect addressing).&lt;br&gt; - The email header and / or signature may reference a real person or organization.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Targeted, Customized</strong>&lt;br&gt; - Recipient is a specific target.&lt;br&gt; - Content is relevant to the target and may repurpose legitimate information (such as a news article, press release, or a conference or event website) and can be externally verified (e.g., message references information that can be found online). Or, the email text appears to repurpose legitimate email messages that may have been collected from public mailing lists or from compromised accounts.&lt;br&gt; - The email header and / or signature references a real person or organization.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Targeted, Personalized</strong>&lt;br&gt; - Recipient is a specific target.&lt;br&gt; - Email message is personalized for the recipient or target organization (e.g., specifically addressed or referring to individual and / or organization by name).&lt;br&gt; - Content is relevant to the target and may repurpose legitimate information that can be externally verified or appears to repurpose legitimate messages.&lt;br&gt; - The email header and / or signature references a real person or organization.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Targeted, Highly personalized</strong>&lt;br&gt; - Recipient is a specific target.&lt;br&gt; - Email is individually personalized and customized for the recipient and references confidential, sensitive information that is directly relevant to the target (e.g., internal meeting minutes, compromised communications from the organization).&lt;br&gt; - The email header and / or signature references a real person or organization.</td>
</tr>
</tbody>
</table>
Figure 6 shows the targeting score for organizations in our study that submitted at least 50 emails. We can see that attackers targeting these groups put significant effort into the message lures. In particular more than half of the messages targeting the Tibet Groups in Figure 6 have a targeting score of 3 or higher. This result means threat actors are taking care to make the email appear to come from a legitimate individual or organization, and include relevant information (e.g., news reports or exchanges from public mailing lists). Higher targeting scores, which result from actions such as personalizing lures to an individual in the group, or including information that requires prior reconnaissance, were rare, but we nevertheless observed cases. For example, in the case of China Group 3, we observed an email that claimed to be from one of the organization’s funders and referenced a specific meeting they had planned that was not public knowledge (social engineering score: 5).

**Figure 6**: Social engineering base value of emails submitted per group (minimum 50 submissions)

<table>
<thead>
<tr>
<th></th>
<th>China Group 1</th>
<th>China Group 3</th>
<th>Tibet Group 1</th>
<th>Tibet Group 2</th>
<th>Tibet Group 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering Sophistication Base Value</td>
<td>0.2</td>
<td>0.4</td>
<td>0.6</td>
<td>0.8</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Technical Sophistication**

The technical sophistication multiplier ranks the relative technical sophistication of malware. This score is determined by measuring how well the payload of the malware conceals its presence on a compromised machine. We use a multiplier because advanced malware requires significantly more resources to customize for a particular target.
We focus on the level of obfuscation used to hide program functionality and avoid detection for the following reasons:

- It allows the compromised system to remain infected for a longer period;
- It hinders analysts from dissecting a sample, developing instructions to detect the malware, and disinfecting a compromised system; and
- Since most commonly used remote access trojans (RATs) have the same core functionality (e.g., key-logging, running commands, exfiltrating data, controlling microphones and webcams, etc.) the level of obfuscation used to conceal what the malware is doing can be used to distinguish one RAT from another.

**TABLE 8: TTI technical sophistication multiplier**

<table>
<thead>
<tr>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 1     | Not protected  
The sample contains no code protection, like packing, obfuscation (e.g., simple rotation of interesting or identifying strings), or anti-reversing tricks. |
| 1.25  | Minor protection  
The sample contains a simple method of protection, including: code protection using publicly available tools where the reversing method is available (e.g., UPX packing); simple anti-reversing techniques like not using import tables, or a call to IsDebuggerPresent(); self-disabling in the presence of antivirus software. |
| 1.5   | Multiple minor protection techniques  
The sample contains multiple distinct minor code protection techniques (anti-reversing tricks, packing, virtual machine / reversing tools detection) that require some low-level knowledge. This level includes malware where code that contains the core functionality of the program is decrypted only in memory. |
| 1.75  | Advanced protection  
The sample contains minor code protection techniques along with at least one advanced protection method such as rootkit functionality or a custom virtualized packer. |
| 2     | Multiple advanced protection techniques  
The sample contains multiple distinct advanced protection techniques (e.g., rootkit capability, virtualized packer, multiple anti-reversing techniques), and is clearly designed by a professional software engineering team. |
Figure 7 shows the technical sophistication multiplier values for emails submitted by the different organizations in our study. Our results show that malware used to target the groups in our study was relatively simple. The highest multiplier value we observed is 1.5 and even that value is seen infrequently. The majority of malware observed is rated either 1 or 1.25 according to our technical scoring criteria, with Tibet Groups observing a higher fraction of malware rated 1.25 and China Groups observing a higher fraction rated 1.

**FIGURE 7:** Technical sophistication multiplier of emails submitted per group (minimum 50 submissions)

---

**Targeted Threat Index Results Overview**

The TTI metric can help us better characterize the relative threat posed by targeted malware in several ways. Table 9 shows the technical sophistication multiplier and maximum / minimum TTI scores for malware families observed in our dataset. Since we primarily find simple malware, with a technical sophistication multiplier of 1 or 1.25, this value does a poor job of differentiating the threat posed by the different malware families to the CSOs. However, by incorporating both the technical sophistication and targeting base value into the TTI metric, we can gain more insights into how effective these threats are in practice.

If we consider the malware families with the highest technical sophistication, we can
see that their TTI values are relatively low, with scores mostly ranging from 1.5 to 4.5 (and one notable exception of 7.5). These tend to be malware families that are regularly used in targeted malware campaigns known to researchers. In particular, PlugX and PoisonIvy have been found used together in targeted attacks, and PlugX is still in active use and under continuous improvement. Despite their technical sophistication, these threats are not well executed and pose less of a risk to CSOs in which users may be able to identify and avoid these threats.

In contrast, the top five malware families in terms of TTI have lower technical sophistication multipliers (1.25) but much higher levels of social engineering. A notable exception is one highly targeted attack (social engineering score 5.0) that used PlugX (technical sophistication score 1.5) resulting in a TTI value of 7.5 (the highest score in the dataset). While this attack has a higher technical sophistication score than the top five malware families, the high TTI score is due to the level of targeting.

| TABLE 9: Top malware families in our dataset by technical sophistication multiplier and final TTI score |
|---|---|---|
| **TECHNICAL SOPHISTICATION** | | |
| Family | Max TTI | Technical Sophistication |
| PlugX | 7.5 | 1.5 |
| Gh0st RAT (LURKO), ShadowNet | 6.25 | 1.25 |
| Conime, Duojeen, IEXPLORE, GLASSES, cxpid, Enfal, Surtr, Vidgrab | 5 | 1.25 |
| Cookies | 5 | 1.0 |
| **TTI** | | |
| Family | Max TTI | Technical Sophistication |
| 3102 | 3 | 1.5 |
| nAspyUpdate | 1.5 | 1.5 |
| PlugX | 7.5 | 1.5 |
| PoisonIvy | 3 | 1.5 |
| WMIScriptKids | 3 | 1.5 |
ANALYZING COMMERCIAL SPYWARE WITH THE TTI

Attacks using advanced commercial spyware such as FinFisher and DaVinci RCS do not necessarily rank higher on the TTI.

We analyzed a sample of FinFisher used against Bahraini activists and evaluated it with the TTI. The malware sample is technically advanced, scoring a 2.0, as a result of multiple advanced protection techniques, including a custom-written virtualized packer, MBR modification, and rootkit functionality. However, the email used in the attack is poorly customized and has several attributes that made it look suspicious to the intended target. The email attempts to reference an NGO called Bahrain Center for Human Rights, but mistakenly refers to it as “Human Rights Bahrain.” The message also lists the wrong name for the acting president of the group. It appears to come from a real journalist, Melissa Chan of Al Jazeera, but provides a suspicious gmail address (melissa.aljazeera@gmail.com). These attributes give the email a social engineering base value of 2. As a result, the attack scores an overall TTI score of 4.0, which is relatively low compared to many other attacks seen in our study. This result shows the importance of social engineering tactics: FinFisher is only effective if it is surreptitiously installed on a user’s computer, which in some cases requires opening a malicious file (however, both FinFisher and Hacking Team offer optional network injection products that permit remote attackers to infect a device without user interaction).

From: Melissa Chan <melissa.aljazeera@gmail.com>
To: 
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.
Similar results can be observed with respect to attacks using DaVinci RCS, developed by Italy-based company Hacking Team, which has been used against activists and independent media groups. RCS also scores a 2.0 on our technical sophistication scale. We analyzed a targeted attack using RCS against a dissident in the United Arab Emirates. The email appears to come from “Arabic Wikileaks” (arabic.wikileaks@gmail.com) and asks the recipient to read a “very important message.” Again, while the malware used in these attacks is technically sophisticated, the social engineering lure is poorly customized (social engineering base value 2), resulting in an overall TTI score of 4.0.

These results suggest that different threat actors possess varying levels and types of resources, and as a result use different attack methods. The majority of malware submitted in our study appears to be from actors that have in-house malware development capabilities, and the capacity to organize targeted campaigns. However, as this report shows, in many cases they spend significant effort on social engineering, but generally do not use technically advanced malware. Conversely, operators of FinFisher and DaVinci RCS have purchased advanced malware products, but in some cases paired them with relatively unsophisticated social engineering.
EXTENDED ANALYSIS:

2.2
Cluster Analysis
Targeted malware attacks are typically not discrete events. Rather, they are a part of systematic campaigns that use common malware, C2 infrastructure and social engineering tactics to target groups repeatedly over long periods of time. Threat actors using common tools and techniques may target multiple groups within a community.

To cluster attacks into campaigns, we analyze technical and contextual indicators to identify patterns. Where possible we draw connections between these clusters and previously reported campaigns and threat actors.

Malware attacks are clustered into campaigns by commonalities and patterns across the following indicators:

- **Email headers**: Originating-IP or common email addresses seen in Reply-To, Sender or Envelope-From email headers.
- **Shared C2 infrastructure**: Domain names and IP addresses to which malware beacons and/or from which it downloads additional modules.
- **Static analysis**: Commonalities between unusual strings or data structures seen in the malware samples or the files they drop.
- **Malware development**: Observable changes made to specific malware families over time.
- **Social engineering tactics**: Contextual patterns in targeted organizations, spoofed senders, and content of messages.

Based on the attributes described above, we identify 10 distinct campaigns, which we present in detail in the following sections.
IEXPLORE Campaigns

First Seen | August 3, 2010
---|---
Last Seen | May 21, 2012
Exploits | Windows: CVE-2010-0188; CVE-2010-3333
Malware Families | Windows: IEXPLORE RAT (aka C0d0s0)
Infrastructure | C2 domains:
sixday.wikaba.com
msupdate02.selfip.com
msupdate02.selfip.info
xinxin20080628.gicp.net
humanbeing2009.gicp.net
saveworld.gicp.net
xinxin20080628.gicp.net
204.134.116.229
60.167.78.229
116.226.49.148
123.147.81.121
204.134.116.229
Targeted Groups | Tibet Group 1, Tibet Group 2, China Group 1, China Group 2
TTI range | 2.5 - 5.0

BACKGROUND

The IEXPLORE campaigns involved custom-developed Windows malware targeting four of the study groups with a unique email and delivery method used for each attempt. Each email was tailored specifically for the target in terms of subject, content, and the way the malware was attached and hidden. In addition, there was evidence that the malware was under active development during the campaign. The IEXPLORE campaigns serves as a typical example of “APT”-style operations.
CAMPAIGN TIMELINE

Attacks in this campaign are linked by the use of IEXPL0RE RAT, which provides standard RAT functionality, including keylogging, file extraction, and control of microphone and webcam peripherals.\(^5\)

We identified the IEXPL0RE campaign through analysis of three separate attacks using this malware that were sent to China Group 1, China Group 2, and Tibet Group 1. This first series of attacks clearly shows how the attackers carefully customized social engineering tactics to the interests of the three different groups.

Evidence of this campaign first emerged in an August 3, 2010 email to Tibet Group 1 that referenced a protest against the Shanghai Expo in Japan. The malicious attachment was a PDF using CVE-2010-0188 to deploy IEXPL0RE RAT.

---

On November 11, 2010, China Group 1 received multiple emails addressed to the organization’s director claiming to be from personal friends. The emails included an executable attachment in a password-protected archive, with the password provided in the body of the email. Packaging attachments in a RAR file makes them less likely to be discovered by an AV scanner. Password protecting the archive reduces the chances of AV detection even further. When executed, the malware connected to softwareupdate.8866.org (119.75.218.45). The level of personalization used in the message gives it a social engineering score of 4 and a total TTI of 5.0.

On November 19, 2010, China Group 2 received an email containing a story about a high-profile, high-rise apartment building fire in Shanghai. The message was written in Chinese and repurposed text from a news article on the event.

Attached to the email were four images and two executable files (.scr extensions) designed to look like images using the Unicode right-to-left override character. When each executable file is run, it will install and launch the malware, drop an image, open the image, and delete itself. The malware connects to xinxin20080628.gicp.net (114.60.106.156). The attack has a social engineering score of 3 and a total TTI of 3.75.

FIGURE 8: Image of a high-rise fire used to trick recipients into running the malware
The remaining attacks we analyzed targeted Tibetan groups exclusively.

On December 2, 2010, Tibet Group 1 received an email that included an Excel spreadsheet attached to an email that appeared to be from organizers of a conference on climate change.

---

From: Tenzin Tsundue <tentsundue@yahoo.com>
Subject: FW: It's time for climate action!

As some of you may know, GAIA is preparing to attend the COP 16 in Cancun as part of our campaigning on climate and waste issues. We'll be advocating for recycling as a climate change mitigation strategy, and trying to stop climate finance for incineration and landfill gas systems. Once more, we'll be proclaiming loud and clear that waste-to-energy technologies are a waste-of-energy and making alliances with other social movements for climate justice.

If you haven't yet, get in touch with us to join in this amazing action time for climate justice and against waste-of-energy technologies!!
E-mail me to arrange how to meet up in Cancun and let's plan further!!

Furthermore, we're working on two action letters that we want to bring forward in these negotiations:

1. The first letter is to demand the creation of a Global Fund that will be directly accessible by wastepickers and other civil society groups; this would be the best way to support resource recovery programmes that reduce GHG emissions and ensure decent livelihoods for all workers in the recycling economy.

2. The second letter is to stop climate finance support to incineration and landfill gas systems, highlighting some of its major problems: energy from WTE is not renewable nor green but the opposite, it generates a huge amount of GHG emissions that should be counted instead of disguised, and it emits an amount of pollution far beyond what the Stockholm Convention allows, and no-one wants.

If you have the chance to arrange a meeting with climate negotiators in your country or in Cancun, please get in touch and we will provide more insight into these demands, as well as materials and preparation to have such conversations.

Looking forward to hearing from all of you soon, whether that is in Cancun or from your local community actions!
On January 11, 2011, Tibet Group 1 received an email about an annual review of Tibetan human rights issues that contained an executable file designed to appear to be a video of a speech by HHDL.

In July 2011, IEXPL0RE was sent to Tibet Group 1 again. This time it used a .rar archive file containing a malicious .hlp file.

Tibet Group 1 received two more emails with IEXPL0RE in late December 2011 and early January 2012. On December 22, an email referencing Uyghur refugees
was received; on January 6, an email in Chinese about Taiwan issues copied from a blog post was received. Both had .rar attachments with the same file, which used CVE-2010-3333. Each of these emails score a social engineering base value of 2.0, and a technical score of 1.25 for an overall TTI of 2.5.

On May 21, 2012, a newer version of the RAT payload was distributed via email in multiple RTF documents to Tibet Group 2. This attack was coupled with a higher degree of social engineering. Separate emails with the same payload and content were sent to both the Executive Director and Program Coordinator, addressing them by name. The email contained an invitation to a legitimate event and included the email signature of a real person, with an attached file purporting to contain information about the event. The sender notes that the recipients were identified as contacts for HHDL, and asks them for help contacting His Holiness in order to invite him to the event. This level of personalization gives the attack a social engineering score of 4 (total TTI 5.0)

The attached RTF file drops a DLL alongside a legitimate program vulnerable to DLL hijacking, allowing the malware to run without a warning to the victim that it is not digitally signed. StrokeIt, a program for using mouse gestures, uses a file named config.dll without verifying the authenticity of the file. By replacing config.dll with the RAT downloader, the malicious code is run while appearing legitimate to the operating system (see Figure 9).

FIGURE 9: Valid digital signature for StrokeIt program, which is used to launch malicious config.dll file

OBSERVATIONS
This series of attacks represents a typical ‘APT’-style campaign. Multiple groups were targeted, with each attack custom developed for each group, including tailored social engineering. The evolution of the RAT payload, as seen in the series of samples targeting Tibet Groups, suggests that the malware was under active development. The social engineering tactics and development cycles observed in this campaign demonstrates the organized and persistent nature of the attackers.
Mobile Malware

BACKGROUND

The use of malware targeting mobile platforms in espionage campaigns is relatively rare, but is likely a vector that will become more common due to the increasing ubiquity of mobile computing.

During investigations of C2 servers associated with the Luckycat campaign, Trend Micro found two malicious Android APKs in early stages of development that could collect device information, as well as download and upload files by remote command. Based on the available information, it was unclear how the attackers intended to deliver the mobile malware to targets.

In 2013, researchers at Kaspersky reported the compromise of an email account of a high-profile Tibetan activist that was then used by attackers to send targeted malware to the activist’s contacts. The emails referenced the World Uyghur Congress and included a malicious APK file that appeared to be an application with information on the event. The malware allowed attackers to collect data from infected devices including contacts, call logs, SMS messages, geolocation, and phone data (phone number, OS version, phone model, and SDK version).

Researchers in our group have also found evidence of commercial surveillance products that target multiple mobile platforms (e.g., Android, IOS, BlackBerry, Symbian) developed by Hacking Team and FinFisher.

In other recent work, researchers found that participants in the Occupy Central protests in Hong Kong received links through WhatsApp to an Android application that appeared to be associated with the protest organizers, but was actually malware that could send a variety of information back to attackers.

In our study, we identified the use of compromised Android applications sent as part of a targeted attack against a prominent figure in the Tibetan community. This attack lever-
aged a genuine email that was likely exfiltrated by attackers, and attached compromised versions of the chat application KakaoTalk and mobile radio application TuneIn.\textsuperscript{6}

**VECTOR OF ATTACK**

On December 4, 2012, an information security expert who works within the Tibetan community sent a private email to a member of the Tibetan Parliament in Exile, based in Dharamsala, India. That email attached genuine versions of Kakao Talk\textsuperscript{7} and TuneIn\textsuperscript{8} as APK files.

On January 16, 2013, an email purporting to be from this same information security expert was sent to a high profile political figure in the Tibetan community. The email contained the same text as the message from December 4, but attached compromised versions of the Kakao Talk and TuneIn Android APKs.

In order for the malware to be installed, the user must permit applications to be installed from sources other than the Google Play store. This permission is not enabled by default in Android. However, as many members of the Tibetan community (particularly those living in Tibetan areas in China) have restricted access to the Google Play service, they are required to permit applications to be installed from outside sources. It is common for APKs to be circulated outside of Google Play. In addition to permitting the “allow from unknown sources” option, the user must also approve the additional permissions requested by the application. Users may be duped into accepting these permissions by assuming they are required for the regular functionality of the application or by not reviewing them carefully before approving. Once these permissions are approved, they are used to authorize the additional data-gathering capabilities of the malware, which is configured to autostart on device boot.

We later confirmed that the original recipient of the legitimate email had his email account compromised. Therefore, it appears likely that the attackers harvested the

---


\textsuperscript{7} KakaoTalk is a chat app that is developed by a South Korean company (Kakao Corporation). Members of the Tibetan community have used KakaoTalk and other applications as alternatives to WeChat (another chat app popular in Asia) after concerns were raised regarding that application’s general security and the potential for Tencent (the China-based developer of WeChat) to monitor users at the behest of the Chinese government.

\textsuperscript{8} TuneIn is a media player application for listening to Internet Radio. TuneIn is used by Tibetans to listen to streams such as Voice of America’s Tibetan service, to engage with their culture, and to stay on top of world news.
original email from the compromised account, and over the course of a few weeks developed malicious versions of the attached APKs. The use of private information in this attack gives it a social engineering score of 5. The technical score of the malware is 1.25 (see the section below for details on the malware's functionality). The total TTI is 6.25.

MALWARE ANALYSIS

The functionality and certificates used for the malicious versions of the KakaoTalk and TuneIn APKs are identical. Both applications were repackaged into modified APKs and signed with an illegitimate certificate (KakaoTalk malware MD5 cbc474e34f26b4afdf02932d8cae9e401 Tunein Malware MD5 ba760392f171e2f05d0352cc1e00190c). Below, we reproduce the original and fake certificates used for KakaoTalk. Notice that fields in the illegitimate certificate have been populated with what appears to be an assortment of nonsensical characters from a QWERTY keyboard:

Original legitimate certificate:

```
Owner: OU=kakaoteam, O=kakao, C=ko
Issuer: OU=kakaoteam, O=kakao, C=ko
Serial number: 4c707197
```

Illegitimate certificate:

```
Owner: CN=qwe, OU=asd, O=zxc, L=rty, ST=fgh, C=vbn
Issuer: CN=qwe, OU=asd, O=zxc, L=rty, ST=fgh, C=vbn
Serial number: a3e5475
```
The following permissions are added by the malware that do not exist in the legitimate version:

```java
android.permission.GET_ACCOUNTS
android.permission.ACCESS_NETWORK_STATE
android.permission.READ_SMS
android.permissionINTERNET
android.permission.ACCESS_FINE_LOCATION
android.permission.WRITE_SETTINGS
android.permission.WRITE_SECURE_SETTINGS
android.permission.WRITE_APN_SETTINGS
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.PROCESS_OUTGOING_CALLS
android.permission.DEVICE_POWER
android.permission.ACCESS_CHECKIN_PROPERTIES
android.permissionINTERNET
android.permission.CHANGE_WIFI_STATE
android.permission.MODIFY_PHONE_STAT
android.permission.BLUETOOTH_ADMIN
android.permission.BLUETOOTH
android.permission.BIND_DEVICE_ADMIN
android.permission.USES_POLICY_FORCE_LOCK
android.permission.CHANGE_CONFIGURATION
```

Note that two of the additional permissions requested by the malware are misspelled, rendering these permissions unusable:

```java
adnroid.permission.ACCESS_CHECKIN_PROPERTIES
adnroid.permission.CHANGE_WIFI_STATE
```
The malicious versions of both applications have the same functionality enumerated below:

- On a periodic basis the user’s contacts, call history, SMS messages, and cellular network configuration are written to an encrypted file called info.txt.
- The malware periodically contacts the C2 server “android.uyghur.dnsd.me” to retrieve updated configuration information, such as URLs and login credentials. This configuration information directs the malware to an upload location for the info.txt file. The site hosting the C2 appears to emulate the appearance of the Baidu website (a Chinese search engine), but includes encrypted configuration data hidden in the comments. By masking the C2 as a seemingly innocuous website, requests would appear to be legitimate on casual inspection. The configuration data contained in the comments directs the malware to upload captured data from the device to an FTP server and contain a pointer to a new C2 that would allow the attackers to change the C2 should that need arise.
- The malware intercepts SMS messages and searches for a special code sent by the attacker, which, if detected, responds to the sender with the base station ID, tower ID, mobile network code and mobile area code of the infected phone in question. This message is not displayed to the user, and they are never made aware of it.

**OBSERVATIONS**

The compromised Android applications that we detected as part of our study, as well as mobile malware described by other security researchers, show that mobile devices are indeed targets for espionage attackers. These attacks serve as early examples of a trend that seems likely to grow alongside the rapid spread of mobile computing.

As described above, there are particular security risks for users residing in locations where access to standard secure channels for installing mobile applications is restricted. As users are required to distribute and install APKs of unknown provenance, they are at increased risk of malicious applications, particularly if those applications use fake certificates (as was the case in this attack).
OS X Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>May 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>Early 2013</td>
</tr>
<tr>
<td>Exploits</td>
<td>CVE-2009-0563; CVE-2011-3544; CVE-2012-0507 ; CVE-2009-3129</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Revir/IMuler, Olyx / Lamadai / PubSab, MacControl</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 domains: freeavg.sytes.com (Olyx.C), mail.hiserviceusa.com (Olyx.C), yahoo.xxuz.com (Olyx.C), coremail.info (SabPab.A), rtx556.onedumb.com (SabPab.A), <a href="http://www.teklimakan.org">www.teklimakan.org</a> (iMuler), IPs: 112.213.126.118 (Olyx.C), 100.42.217.91 (Olyx.C), 198.74.124.3 (SabPab.A), 199.192.152.100 (SabPab.A), 61.178.77.158 (MacControl)</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 3, Tibet Group 4</td>
</tr>
<tr>
<td>TTI Range</td>
<td>2.0 - 3.75</td>
</tr>
</tbody>
</table>

BACKGROUND

While Windows was the most commonly targeted operating system in our study, it was not the only platform targeted. Malware targeting OS X is increasingly paired with Windows malware, giving attackers a better chance of compromising the machine, whatever the operating system. This approach can take the form of code that determines the target’s operating system, such as a web page that uses JavaScript to detect the operating system and then download a cross-platform exploit with appropriate payload.

Four of the Tibet Groups in the study⁹ received targeted malware specifically designed for OS X. Tibet Groups 1, 2, and 4 received emails with malware in an attachment or link. Malware was detected on the network of Tibet Group 3 by a NIDS on their office network.

The OS X malware seen in our study ranges in sophistication from simple programs

---

⁹ Tibet Groups 1, 2, 3, and 4
that rely entirely on social engineering, paired with targeted emails that are not customized for the target (TTI: 2.0), to moderately customized emails with malware that has minor code protection (TTI: 3.75). While the technical sophistication of the malware does not vary widely, all of the malware families observed show active and consistent development over the course of the study.

MALWARE ANALYSIS

The malicious emails used a combination of social engineering, and exploits against a variety of vulnerabilities, to install malware on the victim’s computer.

The vectors we observed include:

- An attached .zip file containing an executable
- An attached Word document using CVE-2009-0563
- A link to a Java .jar file using CVE-2011-3544
- A link to a Java .jar file using CVE-2012-0507

The subject and body text of all of the emails targeting the Tibet Groups contained information relating to Tibetan news and activities (e.g., current world events, upcoming rallies, and self-immolations).

We see Word document vectors first being sent in early 2013. Interestingly, these attacks use a vulnerability made public back in 2009. The use of this vulnerability may be due to the Java vulnerabilities having a higher chance of being patched by the Tibetan community, after they received substantial media attention. However, as the Word documents were all part of one campaign, it is likely just coincidence, as an email carrying the later Java vulnerability was received while the Word campaign was still underway.

We observed three malware families targeting OS X, all of which are simple RATs with low technical sophistication scores:

- Revir/IMuler (technical score: 1.0)
- Olyx/Lamadai/PubSab (technical score: 1.0)
- MacControl (technical score: 1.25)
Revir / IMuler

Revir and IMuler are names for individual components of one particular targeted attack for OS X, and are often used interchangeably. Revir is the name for the “dropper” or shell program that deploys the embedded malicious payload (in this case, IMuler), as well as a clean payload that is then opened to distract the user.

The clean payload that is used can differentiate the early variants of Revir that we have seen. Using the F-Secure naming scheme, Revir.A carries a PDF and Revir.B carries a JPG. Later variants Revir.C and Revir.D allow for any type of clean decoy file, and also encrypt the payload.

IMuler acts as a simple remote access trojan, providing the attacker with the ability to upload and delete the victim’s files, download and run additional malware, and take screenshots. The variants we observed have no reverse engineering protection in the code, although later versions starting with IMuler.B will look for the Wireshark network analyzer and stop running to evade analysis if it is found.

We observed two attacks against Tibet Group 1 using the Revir/IMuler combination. The first, an email sent in May 2011, was a combination of Revir.B and IMuler.A and was the earliest Mac malware attack seen in the study. This email’s contents were about a legitimate event featuring HHDL. The second email, sent in September 2011, stepped up the attack by containing both Revir.A/IMuler.A and Revir.B/IMuler.A combinations. This email purported to be from a legitimate Tibetan rights organization and referred to an upcoming event.
The attack in September 2011 is particularly interesting because the Revir/IMuler components show very clear development progress compared to the version sent in May. The May version is a two-stage program. The initial program dropped as /tmp/host downloads a second program as /tmp/updtdata, which is then used for communication with the C2 server. The September version integrates the second program into the first, merging functionality. This change means that the download of a second executable is not required, eliminating a more suspicious component of the infection process.

The malware version sent in September 2011 was also used in another campaign reported by Eset in March 2012, using photos of a topless model as the lure to run the attachment.

**MacControl**

On September 7, 2012, we identified an attack targeting Tibet Group 2 using another malware family, MacControl. The samples seen from this family have a technical score of 1.25.
This email repurposed content from Radio Free Asia and claimed to contain a list of self-immolations giving it a social engineering score of 3 (TTI 3.75). The attached executable connects to a C2 server at 61.178.77.158:80 and functions as a standard RAT.

Another email received by the same organization three weeks later contained a malicious Excel file that installed Gh0st RAT with the variant-identifying text LURK0. This RAT shared the same C2 as the MacControl, connecting back to 61.178.77.158 on port 8080.

This paring of MacControl with Gh0st RAT has been used in attacks against Uyghur users, as reported by Kaspersky and AlienVault.

Outside of our study participants, we have also seen MacControl campaigns similar to those reported by Kaspersky and AlienVault, targeting Tibetan and Uyghur communities. These differ slightly than those described above in that they use different flag text in the Gh0st RAT component, and connect to a nearby IP (61.178.77.169). They are also delivered using a Word vulnerability, while the email sent to the in-study recipient contained an executable inside a .zip file.

Olyx / Lamadai / PubSab

Olyx, Lamadai, and PubSab (or SabPub) are variants of the same malware that are differentiated by the C2 server used and the location where the malware hides on a compromised system. These names are often used interchangeably by different antivirus or security companies. Further complicating matters, there is often overlap between names: for example, Olyx.C is the same as Lamadai.B.
Olyx.A
» Threat location: /Library/Application Support/google/startp
» Launcher: ~/Library/LaunchAgents/www.google.com.tstart.plist

Olyx.B (Lamadai.A)
» Threat location: /Library/Audio/Plug-Ins/AudioServer
» Launcher: ~/Library/LaunchAgents/com.apple.DockActions.plist

Olyx.C (Lamadai.B)
» Threat location: Applications/Automator.app/Contents/MacOS/DockLight
» Launcher: ~/Library/LaunchAgents/com.apple.DockActions.plist

PubSab.A
» Threat location: ~/Library/Preferences/com.apple.PubSabAgent.pfile
» Launcher: ~/Library/LaunchAgents/com.apple.PubSabAgent.plist

Olyx.C was observed in emails sent to Tibet Group 1, and via a NIDS on the network of Tibet Group 3.

The campaign against Tibet Group 1 consisted of five emails that contained links to malicious .jar files that exploited Java vulnerabilities (CVE-2011-2544 or CVE-2012-0507). All of these emails appeared to come from real people or organizations, and referenced Tibetan themes giving them a social engineering score of 3. The malware is basic with a technical score of 1. The total TTI is 3.
On January 29, 2013, the NIDS on the network of Tibet Group 3 detected evidence of a Java vulnerability being used to serve multi-platform malware pretending to be Adobe Flash Player. This sample was distributed through a web page that does web browser user agent detection. Tibet Group 3 did not submit any emails containing this link, so the specific attack vector used is unclear.

The website hosting the malware was hxxp://services.addons.mozilla.publicvm.com, and had an .xpi file for Firefox and a .jar containing Olyx.C for Mac. The way the malware was served was different than other similar attacks in that it checked both browser and OS, not just OS, to determine which malware program would be used.

On February 5, 2013, we received additional alerts that showed similar malicious pages were visited by Tibet Group 3, again without indication of the original attack vector. A web page was flagged by the NIDS due to a suspicious encoded string that decoded to a tinyurl.com redirector. This link led to a page on hxxp://adobeupdate.publicvm.com, which had attacks for IE, Firefox, Java (Windows, but not OS X), and...
a standard Windows binary. There may also have been an OS X attack, but we were unable to locate it from the information recorded by the NIDS.

The original page that served up the attack also had a distinctive comment in the script that identified it as a legitimate script from the website of the US State Department (www.state.gov). At the time of our analysis the server was hosting 100 other domains. The www.state.gov script we found on the page suggests the IP was hosting a fake US State Department website that included the malicious link.

OBSERVATIONS

Mac OS X was once commonly seen as a more secure alternative to Windows. Targeted groups in the Tibetan community shared this assumption. For example, in a 2008 Washington Post article on targeted attacks against Tibetan groups, a volunteer providing technical assistance to a Tibetan NGO noted that the group had attempted to mitigate attacks by using “more secure platforms such as Apple computers.” While the number of malware vectors targeting OS X is small compared to the many vulnerabilities used against Windows targets, it is clear that OS X malware is becoming an important tool for attackers targeting human rights organizations. All of the malware families described here are under active development and we will likely see more attacks targeting OS X at greater levels of technical sophistication.
## DNF Campaigns

<table>
<thead>
<tr>
<th><strong>First Seen</strong></th>
<th>November 26, 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last Seen</strong></td>
<td>March 4, 2013</td>
</tr>
<tr>
<td><strong>Attack Vectors</strong></td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td><strong>Exploits</strong></td>
<td>Windows: CVE-2009-3129, CVE-2011-3544, CVE-2012-0158</td>
</tr>
<tr>
<td></td>
<td>Mac: CVE-2011-3544</td>
</tr>
<tr>
<td><strong>Malware Families</strong></td>
<td>cxgidi, FAKEM (HTML variant), Olyx, Scar.hikn</td>
</tr>
<tr>
<td><strong>Targeted Groups</strong></td>
<td>China Group 1, Tibet Group 1, Tibet Group 2, Tibet Group 4</td>
</tr>
<tr>
<td><strong>TTI Range</strong></td>
<td>2.5 - 5.0</td>
</tr>
</tbody>
</table>

### BACKGROUND

We identified the Domain Name Family (DNF) campaign by clustering attacks together on the basis of a set of malware families that communicate with domains registered under a series of suspicious names.

Analysis of attacks using Olyx Scar.hikn, cxgidi, and FakeM malware families revealed that these samples connect to a set of domains that are registered to series of names: Mily Luna, Philip Fischer (adonis.fischer@yahoo.com), William Bottle (john.fielder@hotmail.com), and XieZhong Customer. Searching through domain registration information revealed a large number of domains registered under these names in a short time frame that were related to Tibet, Japan, education and business. All of these domains used a common hosting company called XinNet. Most of these domains have since expired, but historical registration data can be retrieved using services such as [DomainTools](https://www.domaintools.com).
The registration information provided by “Mily Luna” includes conflicting fields (i.e., address in Nepal, but city and province as Hong Kong SAR), which further demonstrates that this information does not reflect a real user:

```
Domain Name : miyazakihousou.com
PunnyCode   : miyazakihousou.com
Creation Date: 2009-02-01 10:53:24
Updated Date: 2012-02-11 10:51:20
Expiration Date: 2013-02-01 10:47:33

Registrant:
  Organization : mily luna
  Name          : mily luna
  Address       : No.358,dapho road,Kathmandu, Nepal
  City          : xianggangtebiexingzhengqu
  Province/State: xianggangtebiexingzhengqu
  Country      : china
  Postal Code  : 2000000
```

Some of these C2 domains are registered using email addresses at xiezhong.com. Through domain registration records, we were able to find more than 25 additional domains connected to this cluster, including many registered to “John Smith” (worldfreeusa@gmail.com). While we did not see any malicious activity related to these domains, some of the domains are suspiciously named (kaspersky-ru.org, kaspersky-us.org, thetibetpost.net). In the case of kaspersky-us.org in particular, VirusTotal shows that only 1/51 antivirus products detect the site as malicious, but the one that does is made by Kaspersky. VirusTotal also includes a URL query report showing thetibetpost.net as malicious.

Figure 13 illustrates the connections between malware families, C2 domains, and the domain registrants in the DNF campaign. One FakeM sample used one of the Mily Luna and Xie Zhong domains as C2s. FakeM has been observed being used in conjunction with cxgid by other researchers, but we have not seen other reports identifying the infrastructure found in this cluster.
ADAPTIVE ATTACKERS

We observed DNF Campaign attacks between November 2010 and March 4, 2013 that targeted Tibet Group 1, Tibet Group 2, and Tibet Group 4. The social engineering scores of these emails were between 2-3 and the technical scores of the malware were 1.25 (TTI 2.5 – 3.75). In June 2011, we were sent an automated AV detection notice from China Group 1. The alert identified a sample that was also sent in emails to Tibet Group 1, and which connected to the DNF-related domain upgrade. support-microsoft.com. This link suggests a staff member of China Group 1 likely received a malicious email from the DNF campaign and opened the payload, triggering the AV detection.
Initially, attacks in this campaign exclusively used Windows malware. However, the attackers demonstrated their ability to quickly adapt tactics to meet new requirements.

On February 23, 2012, an email was sent to the director of Tibet Group 1. It addressed the director personally and appeared to come from Mr. Cheng Li, a prominent China scholar based at the Brookings Institution. The email requests the assistance of Tibet Group 1 in verifying information on Tibetan self-immolations. The name and title provided in the email all match real details for Mr. Cheng Li provided on his Brookings Institute staff page.

The director of Tibet Group 1 noted to us that at first it was flattering to be asked to consult a well-known China expert on Tibetan issues. However, the director quickly noticed that the email was sent from a suspicious AOL account (chengli.brookings@aol.com). This account appears to have been registered by the attackers for this specific attack. Attached to this email was an Excel spreadsheet that used CVE-2009-3129 to install cxgid malware. The malware connects to mail.miyazakihousou.com (112.213.126.18), which is a domain registered under the name Mily Luna.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>5.0</td>
</tr>
<tr>
<td>MD5</td>
<td>64e2d3b91977bb0c293cac3e97669f03</td>
</tr>
<tr>
<td>C2</td>
<td>mail.miyazakihousou.com (112.213.126.18)</td>
</tr>
</tbody>
</table>
The director of Tibet Group 1 flagged this message to us as one of the most targeted messages they had ever received. After consultations with Tibet Group 1, we decided to run an experiment on the attackers to test how responsive they would be to interaction from a target. Working with the director, we crafted a reply to “Cheng Li” and sent it on March 2:

“Thank you for your inquiry. I’d be happy to help out—I’m having trouble opening the document on my mac though, I think there may be an issue with the Chinese character font? I think if you sent me a Word version that might be easiest, as it would also allow me to make comments in the document.”

On March 6 “Cheng Li” replied, apologizing for his late response due to work-related travel. He encouraged the director to review information on Tibet issues on a website. The link provided pointed to a website containing a Java vulnerability that had payloads for both Windows and OSX systems. The payload for Windows was the same cxgid sample sent in the original email. The payload for OSX was Olyx and connected to mail.hiserviceusa.com (112.213.126.118). Both the malicious website and C2 were domains registered under the name Mily Luna.
OBSERVATIONS

While other malware campaigns we identified typically use free subdomains, this cluster primarily relied on registered domains. The use of registered domains provided a useful variable around which to cluster attacks. Registered domains can also be blacklisted more easily than free services providing subdomains.

The DNF Campaign also demonstrates the adaptability of the attackers. Upon receiving a message from Tibet Group 1 indicating the targeted user was using a Mac, the attackers quickly responded with malware targeting OS X.
APT 1 Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>April 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>August 16, 2012</td>
</tr>
<tr>
<td>Exploits</td>
<td>N/A</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Bangat, GLASSES, WARP, WEBC2-QBP</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 domains: ash22ld.compress.to, ewplus.com (compromised site), johnbell.longmusic.com, 66.228.132.8 (hard coded ip)</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Rights Group 1</td>
</tr>
<tr>
<td>TTI Range</td>
<td>5.0</td>
</tr>
</tbody>
</table>

BACKGROUND

On February 19, 2013, Mandiant released a report that shed light on a prolific cyber espionage group they call APT1 (also referred to as “Comment Crew” or “Byzantine Candor”), which had targeted a large number of organizations in a wide range of industries, stealing terabytes of data. Mandiant’s report traced APT1 operations to China and claims that the group may in fact be the Second Bureau of the People’s Liberation Army General Staff Department’s Third Department, also known as Unit 61398.

APT1 has been active since at least 2006. Mandiant has observed the group breaching 141 organizations from 20 major industry sectors. Within Mandiant’s report there is no mention of CSOs as targets among these compromised organizations. However, in previous reports and released datasets, there are indications that civil society is targeted by APT1. Both Mandiant and Shadowserver have included a Tibetan-themed domain (tibethome.org) in their APT1-related domain lists, which suggests that Tibet-related organizations may have been targeted, but no further details on Tibet-related operations were included. In 2012, a Bloomberg article listed the nonprofit organization International Republican Institute among target organizations compromised by APT1 in June 2011, but no technical details of the attack were released.
In the course of our study, we found evidence that APT1 targeted Tibet Group 1, and successfully compromised the networks of Rights Group 1.

TARGETING TIBET GROUP 1

On April 28, 2010, the director of Tibet Group 1 was sent an email from a Yahoo! webmail address. The sender makes a personal plea to Tibet Group 1 to help find his Tibetan wife who he claims went missing since after visiting Tibet.

---

From Nate Herman <nate.herman@yahoo.com>

Subject: save my Tibetan wife

To: [email]

Dear Sir/Madam,

My wife is a Tibetan. I could not hear from her since her last visiting to Tibet. A friend of mine told me to turn to [redacted] so I wrote this email to you. Hope you can help me. Details about my wife behind the link below.

http://tcw.homier.com/attachments/details.zip

All my best regards,
Martin Lee

---

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>5.0</td>
</tr>
<tr>
<td>MD5</td>
<td>6fb3ecc3db624a4912d7bd2d565c4995</td>
</tr>
<tr>
<td>C2</td>
<td>ewplus.com (204.14.88.45)</td>
</tr>
</tbody>
</table>

Some details of the email immediately flag it as suspicious: the name in the email address is “Nate Herman” although the email body is signed “Martin Lee.” The forwarded email included full headers, so we were able to obtain more information about its origin (Yahoo! includes the sender’s source IP in the headers when an email is sent over the webmail interface). In this case, the originating IP was 69.95.255.26, which

---

10 We originally published analysis of the APT1 related attack against Tibet Group 1 in a blog post, Hardy, S. APT1’s GLASSES – Watching a Human Rights Organization, February 25, 2013, https://citizenlab.org/2013/02/apt1s-glasses-watching-a-human-rights-organization
is registered to One Communications, Inc. / EarthLink Business, and is very close to IPs used in a similar attack—demonstrating that this attack is not isolated, and the IPs are likely being reused for other malware campaigns.

This email contains a link to a ZIP file located at http://tcw.homier.com/attachments/details.zip (MD5: 6fb3ecc3db624a4912d-dbd2d565c4995). The “homier.com” domain belongs to Homier Distributing Company, Inc. and appears to have been compromised. A search for this subdomain shows other instances of malware hosted there, including a case detailed in a ThreatExpert report describing a malicious file stored in /images/update.bin, and another malicious program getting the file /attachments/SalaryAdjustment.zip.

Analysis of the files revealed malware that shares a number of similarities to malware described in Mandiant’s APT1 report that they call “GOGGLES” —a simple downloader that is controlled via encoded markers in files accessed over HTTP. The malware sent to Tibet Group 1 shares both a large percentage of code and the same C2 infrastructure as the program described in the APT1 report, which suggests the two pieces of malware are both used by APT1.

We call this malware GLASSES because it is related to GOGGLES, and used a compromised eyeglasses storefront website as its C2 server. The GOGGLES code is more sophisticated than the GLASSES code. In addition to a more effective method of hiding the command data, it also has more countermeasures to protect against reverse engineering and hide itself on the infected system. For this reason, it is very likely that GOGGLES is a later version of GLASSES.

**COMPROMISING RIGHTS GROUP 1**

In August 2012, Rights Group 1 was made aware of a serious compromise of their network infrastructure. Following incident response from a third party, Rights Group 1 shared workstation hard drives with the Citizen Lab that were suspected to have been compromised as part of the intrusion. The attackers had access to the network infrastructure of Rights Group 1 from January 2011 to August 2012. During this time the attackers were able to move laterally through the network, install RATs, extract sensitive data and passwords, and impersonate staff identities. The incident affected computers beyond the ones to which we had access, but these hard drives provide enough data to reveal malware and C2 infrastructure that is linked to APT1.

We conducted forensic analysis of six Windows workstation hard drives used by Rights Group 1 staff members. This analysis found that three of the drives were compromised by multiple versions of malware that matched a tool used by APT1 called Bangat, which is used to
establish footholds in a network and maintain persistence. Bangat has standard back-door functionality, including features to start keyloggers, gather system information, and take screenshots.

Comparing the samples retrieved from the compromised hard drives to Bangat samples available from the Contagio APT1 malware collection reveals close similarities. Rights Group 1 samples included the same functionality and important strings as the APT1 contagio samples. These included temporary file names (~MC_[#]~, where # are numbers) and DES key (!b=z&7?cc,MQ>) used for encryption. Binary comparison between the two samples reveals an approximate 97% match.

One of the compromised hard drives included a variant of an HTTP backdoor used by APT1 that Mandiant calls WARP. This malware has no RAT functionality and is primarily used to gather system information and download stage two malware. Therefore, we believe that WARP was used as a dropper to install Bangat onto the compromised system.

Binary comparison between the WARP sample from Rights Group 1 and a WARP sample from the Contagio APT1 malware collection (md5 C0134285A276AB933E-2A2B9B33B103CD) revealed a 90% similarity. The main differences between samples is that the Rights Group 1 sample does not have functions from wininet.dll in the import table, and uses LoadLibrary and GetProcAddress to import them.

All three of the compromised hard drives included samples that communicated to 66.228.132.8 as a C2. This IP address also had an HTML comment on its default webpage that indicated it also served as a C2 for WEBC2-QBP, another malware family described by Mandiant in their APT1 report. The same C2 (66.228.132.8) was also used by two Bangat samples in the Contagio APT1 collection (MD5s BD8B082B7711BC980252F988BB0CA936, E1B6940985A23E5639450F8391820655).
TABLE 10: Overview of malware retrieved from compromised hard drives

<table>
<thead>
<tr>
<th>HARD DRIVE</th>
<th>MALWARE</th>
<th>FILE CREATION DATE</th>
<th>MD5</th>
<th>C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD1</td>
<td>Warp - Dropper for Bangat</td>
<td>n/a</td>
<td>2b941110e046a03894d-41f90272c3012</td>
<td>n/a</td>
</tr>
<tr>
<td>HD1</td>
<td>Bangat (irmon32.dll)</td>
<td>May 15, 2012</td>
<td>21afca59b9aaa26676adfb-f72cfff7b9</td>
<td>hurrisonstone.dnset.com, dynoressfich.myMom.info</td>
</tr>
<tr>
<td>HD1</td>
<td>Bangat (Nwsapagent.dll)</td>
<td>July 5, 2012</td>
<td>429de63e18eda4f0699b-2145bab5480</td>
<td>66.228.132.8</td>
</tr>
<tr>
<td>HD2</td>
<td>Bangat (rasauto32.dll)</td>
<td>June 11, 2012</td>
<td>45dc7eb8e76143846f242940ff-369cb4</td>
<td>66.228.132.8</td>
</tr>
<tr>
<td>HD2</td>
<td>Bangat (Nwsapagent.dll)</td>
<td>June 19, 2012</td>
<td>429de63e18eda4f0699b-2145bab5480</td>
<td>johnbell.longmusic.com</td>
</tr>
<tr>
<td>HD3</td>
<td>Bangat (rasauto32.dll)</td>
<td>June 11, 2012</td>
<td>5dc7eb8e76143846f242940ff-369cb4</td>
<td>66.228.132.8</td>
</tr>
</tbody>
</table>

OBSERVATIONS

The APT1 campaigns illustrate one of the broader findings of this report. While large, resourceful threat actors like the APT1 group are frequently documented targeting government and industry, the same actors use similar tools, techniques, and procedures to target CSOs as well. While government and industry have the resources and expertise to respond to such threats, in many cases CSOs do not. Even large CSOs are vulnerable to this problem. While Rights Group 1 is a large and well-resourced organization relative to others in our study it was compromised for over a year-and-a-half before the threat was identified.
NetTraveler Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>April 30, 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>September 12, 2012</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails, Watering hole attacks</td>
</tr>
</tbody>
</table>
| Exploits            | Windows: CVE-2009-3129; CVE-2010-0188; CVE-2012-3333; CVE-2012-0158  
                      | Mac: CVE-2012-0507              |
| Malware Families    | Windows: Conime, Gh0st RAT, RegSubDat, Netpass  
                      | Mac: Dockster                   |
| Infrastructure      | Email Sender IPs: 209.11.241.144  
                      | C2 domains: 209.11.241.144, akashok.w63.1860host.com:80 (69.43.161.162),  
                      | ww2.akashok.w63.1860host.com:80 (204.13.161.108), gen2012.eicp.net:1080 (61.178.77.98),  
                      | 61.178.77.98:8080, 61.178.77.98:1080, 61.178.77.98:80, itsec.eicp.net:443 (1.203.31.195),  
                      | www.eaglesey.com (120.50.35.46), itsec.eicp.net:8088 (209.11.241.144) |
| Targeted Groups     | Tibet Group 1, Tibet Group 2, Tibet Group 3, Tibet Group 4, Tibet Group 5, China Group 3 |
| TTI Range           | 2.5 - 4.0                       |

**BACKGROUND**

In June 2013, Kaspersky released a report detailing the operations of a threat actor that compromised over 350 victims in 40 different countries. Kaspersky called the main malware used in these campaigns “NetTraveler” after an internal string found in the tool, “NetTraveler is Running!” Targets identified in this report included Tibetan and Uyghur groups, the energy industry, military contractors, scientific research centres, universities, government institutions, and embassies.

The Kaspersky report identifies the IP 209.11.241.144 as a “mothership” server.
used as a VPN and a C2 in the campaigns. We see 209.11.241.144 as a sender IP for 19 emails in our study. Searching for other emails that share the same malware we find a total of 34 emails, which we can split into seven campaigns based on how the common C2 infrastructure is used. Additionally, there was one email from this sender that we were not able to cluster, as the attachment was a password-protected ZIP file and the password was not evident. Attacks using infrastructure related to NetTraveler targeted all five of the Tibet Groups in our study as well as China Group 3.

NetTraveler operators are also known to use watering hole attacks against Tibetan websites. In December 2012, F-Secure reported on malware that relied on an entirely different method of attack and compromise but used the same infrastructure. A website related to HHDL at www.gyalwarinpoche.com was compromised and served the CVE-2012-0507 Java exploit (the same as used in the Flashback malware) to compromise computers running OS X. This malware, which F-Secure calls Dockster, connects back to the same IP that sent many of the malicious emails we observed, itsec.eicp.net:8088 (209.11.241.144). Kaspersky has documented similar watering hole attacks against Uyghur-related websites.

CAMPAIGN 1

The first appearance of an attack that used infrastructure related to NetTraveler was sent to China Group 3 on April 30, 2010. The email attached a PDF that used CVE-2010-0188, and connected to C2 servers at akashok.w63.1860host.com:80 (69.43.161.162) and ww2.akashok.w63.1860host.com:80 (204.13.161.108). The sender IP matches the mothership server identified by Kaspersky (209.11.241.144).

C2 traffic from this malware appears as follows:

```
GET /wl/netpass.asp?action=gettext HTTP/1.0
GET /wl/netpass.asp?hostid=...&hostname=...&hostip=...&filename=18155523-sys.log&filestart=0&filetext=begin::...
```

![Email example](image)
CAMPAIGN 2

The first of three campaigns using the Conime malware family involved seven emails, five of which were distinct, mostly concerning March 10th Tibetan Uprising demonstrations. Coinme samples used in these attacks have a technical score of 1.25. These emails were sent between February 13 and March 7, 2012 and were all targeted at Tibet Group 1. The campaign used a combination of malicious XLS and RTF documents exploiting CVE-2010-3333. The majority of these attacks score a TTI of 3.75. One email only scores 2.0 on social engineering sophistication and a 2.5 overall TTI. We see the mothership server (209.11.241.1440) and 120.50.35.60 used as a mail sender. All of the attacks in this campaign used 61.178.77.98 (without an associated DNS name) as a C2.

CAMPAIGN 3

The second of three campaigns using the Conime malware family involved seven emails, three of which were distinct, sent to Tibet Groups 1, 2, and 4. These emails all scored a social engineering sophistication value of 3.0, for a combined TTI of 3.75. Two of the distinct emails had an attached XLS document; one was encrypted, the other was not. The third email used a malicious RTF document exploiting CVE-2010-3333. The encrypted XLS was sent on July 25, 2012, and the other emails were sent between September 10 and 12, 2012. We again see 209.11.241.1440 as an email sender IP. All of these exploits dropped the same variant of Conime, which connected to gen2012.eicp.net:1080 (61.178.77.98) as a C2.

CAMPAIGN 4

The third campaign using Conime was more varied than the other two, and was targeted at Tibet Groups 1, 2, and 4. Fifteen emails were received, eleven of which were distinct (although one showed only minor changes), ranging from 2.0 to 4.0 on the
social engineering sophistication score. These emails were sent over a longer timeframe than the other campaigns, extending between June 14, 2012 and September 12, 2012. Vulnerabilities used included both major RTF (CVE-2010-3333, CVE-2012-0158) and XLS (CVE-2009-3129) versions. One email, received by Tibet Group 2, received a social engineering sophistication score of 4.0. This email was highlighted to us by the recipient as highly targeted, and referenced an upcoming conference call about grant funding. Like the previous two NetTraveler campaigns, the malware connected directly to 61.178.77.98.

CAMPAIGN 5

This campaign used a variant of Gh0st RAT, with a flag text of “Snow.” Identical emails, concerning a visit of HHDL to Portland, were sent to Tibet Groups 2 and 4 on January 28, 2013. The emails have a social engineering score of 2, with an overall TTI score of 2.5. The attackers again used 209.11.241.144 as a mail sender and 61.178.77.98 as a C2.

CAMPAIGN 6

This campaign used a different malware family, RegSubDat, which was contained in an RTF using CVE-2012-0158, attached to an email sent to Tibet Group 1. Again we see mail sent from 209.11.241.144, but in this case the malware connected to a different C2 server: itsec.eicp.net:443 (1.203.31.195). This attack scored 3.0 on the social engineering sophistication value for an overall TTI of 3.75.

CAMPAIGN 7

The final sample from the NetTraveler group was observed in an email message sent to Tibet Group 1 on March 15, 2012. This malware was sent from the same mother-ship server (209.11.241.144) described above, but rather than attaching the malicious file, as had been done for all prior attacks, this email contained a link to an infected XLS file. The file was hosted at www.eaglessey.com (120.50.35.46), but was no longer present when we attempted to access it.

OBSERVATIONS

The NetTraveler campaign serves as another example of a campaign that targets CSOs alongside industry and government targets. These campaigns are conducted by a prolific threat actor that has targeted a variety of different sectors. Our findings confirm the targeting of Tibetan groups identified by Kaspersky, as all five of our Tibet Groups were targeted. This campaign demonstrates an adaptive attacker that uses a variety of vulnerabilities for different applications, including targeting of both Mac and Windows platforms.
PlugX Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>February 10, 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>January 15, 2013</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td>Exploits</td>
<td>CVE-2012-0158 (RTF, DOC, and XLS), CVE-2012-1889 (Internet Explorer), CVE-2012-5054 (Flash), CVE-2009-4324 (PDF), CVE-2007-5659 (PDF)</td>
</tr>
<tr>
<td>Malware Families</td>
<td>PlugX, Poison Ivy</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, China Group 1, China Group 2</td>
</tr>
<tr>
<td>TTI Range</td>
<td>1.5 - 7.5</td>
</tr>
</tbody>
</table>

**BACKGROUND**

PlugX is a well-known family of malware that researchers have observed being used in targeted attacks against Tibetan organizations, NGOs, government institutions, and private companies.

Trend Micro has published a report on PlugX, describing a long-standing campaign that previously used Poison Ivy, another malware family. Jaime Blasco at Alien Vault claims to have tracked down the author of PlugX, who is allegedly based at a Chinese security company.

The PlugX samples seen in our study can be clustered into four campaigns, based on email sender IP and C2 infrastructure. Examining email topics, vulnerabilities used, and compile paths (as described in the Alien Vault blog post) suggests that the four
campaigns are from the same source. We have also seen a Poison Ivy sample used in this campaign.

The attack vectors and vulnerabilities used in PlugX are more varied than other attacks in our dataset. The vulnerabilities used include instances of CVE-2012-0158 in three separate file formats, an Internet Explorer vulnerability (CVE-2012-1889) that will install PlugX as a drive-by download, and a Flash vulnerability (CVE-2012-5054) hosted on an external website. The earlier Poison Ivy attack used two older PDF vulnerabilities. The Flash vulnerability was particularly notable; it was a zero-day at the time of the attack, leaving any user who clicked the malicious link it was hosted on vulnerable to compromise.

CAMPAIGN 1

The first set of attacks consists of fifteen emails, five of which were unique, sent from May 11, 2012 to June 1, 2012. Tibet Group 1 and Tibet Group 2 were both targeted with at least four out of the five emails. These emails show many signs of coming from the same source, including a common return address of kandid77@rambler.ru, a sender IP of 98.126.14.13, and common C2 infrastructure.

Two different C2 domain names were used: systen.windowsdeupdate.com (TCP port 8080) and web.windowsdeupdate.com (UDP port 7070). These DNS names both pointed to the same IPs, which include 174.139.12.84 and 98.126.14.13.

All of these emails have a social engineering score of 3.0 and an overall TTI of 4.5. One example, sent to Tibet Group 2, spoofed a legitimate Tibetan official and contains a Word document that outlines the schedule of an actual European tour taken by the Dalai Lama.
EXTENDED ANALYSIS: 2.2 Cluster Analysis

Social engineering | 3  
Technical          | 1.5  
TTI                | 4.5  
MD5                | 1aa5d6e570575d0b001a48e62a412f14  
C2                 | systen.windowsdeupdate.com (174.139.12.84)

CAMPAIGN 2

On May 22, 2012, an email was sent from the IP address 69.46.75.74 to Tibet Group 2, which claimed to be from an individual named Tsering Dolma, with an email signature belonging to the Central Tibetan Administration, and with the return address of ‘tdolma6248@yahoo.com.’ This email contained an attached RTF with CVE-2012-0158 that was used to install PlugX.
EXTENDED ANALYSIS: 2.2 Cluster Analysis

CAMPAIGN 3

Three emails were sent to Tibet Group 2 and China Group 1 between June 15 and August 30, 2012. Each email had unique content, attack vectors, sender email address and IP, and vulnerability used. The vulnerabilities included a Word variant of CVE-2012-0158, the Flash vulnerability CVE-2012-5054, and Internet Explorer vulnerability CVE-2012-1889.
The Flash vulnerability CVE-2012-5054 was a zero-day at the time it was used in an attack against China Group 1. The attack was delivered in an email that was highly customized for the recipient and used a malicious link in the message as the vector. It referred to a group of individuals who had recently been involved in internal private meetings and appeared to be a forwarded message from the director of the organization. The highly targeted nature of this attack, combined with the technical sophistication of the PlugX malware family, resulted in a TTI score of 7.5, the highest seen in the study.

**CAMPAIGN 4**

The last campaign consisted of four unique emails sent to Tibet Groups 1 and 2 between December 22, 2012 and January 15, 2013. These emails all included attachments that used CVE-2012-0158. The C2 domain used was jinyuan2011.zapto.org:443, which resolved to 123.129.19.145 at the time of the attack. Three of these four emails scored 2.0 on the social engineering sophistication score (and 3.0 TTI overall), and one scored 3.0 on social engineering for an overall TTI of 4.5.

One of these four emails repurposed legitimate text about a Tibetan monk who had been detained:
This campaign was interesting in that it did not use the encrypted BOOT.LDR files, instead using NvSmartMax.dll.url, and logging keyboard data to NvSmart.hlp. This functionally corresponds to observations made by Kaspersky researchers that PlugX was becoming more mature. In particular, we observed that the identifying strings and logging data were removed in this campaign. It is particularly interesting that while the malware itself is being improved, potentially in response to published reports from threat researchers, the quality of the targeting in this campaign has gone down.

**POISON IVY**

In September 2012, Trend Micro described the use of PlugX in a campaign that had previously used the Poison Ivy RAT and targeted government and private companies in Japan. We also saw evidence in our study of Poison Ivy being used in conjunction with PlugX in an attack sent to China Group 2 on February 10, 2011, over a year
before our first observed PlugX attack. This email included a PDF with two vulnerabilities, CVE-2009-4324 and CVE-2007-5659.

---

**Social engineering**

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>1</th>
</tr>
</thead>
</table>

**Technical**

<table>
<thead>
<tr>
<th>Technical</th>
<th>1.5</th>
</tr>
</thead>
</table>

**TTI**

<table>
<thead>
<tr>
<th>TTI</th>
<th>1.5</th>
</tr>
</thead>
</table>

**MD5**

<table>
<thead>
<tr>
<th>MD5</th>
<th>49c9cf000fa1d789f3df8d739f997eb8</th>
</tr>
</thead>
</table>

**C2**

<table>
<thead>
<tr>
<th>C2</th>
<th>sociapub.flower-show.org (14.102.252.142)</th>
</tr>
</thead>
</table>

The Poison Ivy RAT connects to a C2 at sociapub.flower-show.org:8080 (14.102.252.142), the same Poison Ivy C2 domain observed by Trend Micro on July 11, 2012. This attack has also been seen elsewhere in the wild, as noted in a Threat Expert report describing the same malware seen with a different file size and MD5 hash (9ADFC6D86D5FF36F2CAB781663E1075).
OBSERVATIONS

The PlugX campaign provides yet another example of a campaign that targets civil society organizations alongside government and industry groups, using the same infrastructure and malware to compromise targets. Aside from these similarities, the campaign otherwise had a number of unique characteristics that separated it from others in our research. Most notably, it was the only instance of a zero-day vulnerability seen in our study. Given that zero-days are highly effective, as software developers have yet to patch the vulnerability, they are highly lucrative and sought after. It is notable that the malicious attacks would use this zero-day to target a CSO, as once such an exploit is exposed it runs the risk of being identified and having the vulnerability fixed. The PlugX campaign also included a broader variety of attack vectors than what was seen in most campaigns. The attached files included the zero-day Flash vulnerability, an exploit for Internet Explorer, as well as the standard Microsoft Office exploits seen elsewhere.
# TseringKanyaq Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>May 4, 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>July 26, 2013</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td></td>
<td>Mac: CVE-2009-0563, CVE-2012-0507, CVE-2013-1331</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Windows: Shadownet, Duojeen</td>
</tr>
<tr>
<td></td>
<td>Mac: PubSab</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Email sender: 163.com, myopera.com, gmx.com</td>
</tr>
<tr>
<td></td>
<td>C2 domains: newwolfs29.zxq.net, newwolfs21.blog.163.com, dplcoopsociety.us.dwyu.com, laraider2.he1.ifreeurl.com, pomehra.typepad.com, tbsociety.info, nedfortibt.info, duojeen.info, appleboy1111.blogspot.com, coremail.info</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 4</td>
</tr>
<tr>
<td>TTI Range</td>
<td>3.0 - 3.75</td>
</tr>
</tbody>
</table>

## BACKGROUND

Unlike the previous campaigns that were grouped by shared infrastructure or connections to previously reported threat actors, the “TseringKanyaq” cluster was first identified through contextual analysis.

This cluster consists of a series of attacks targeting Tibet Groups, which had either ‘tseringKanyaq@yahoo.com’ or ‘d.kanam@yahoo.com’ in the reply-to address field of the malicious emails. Following the identification of this pattern, further attacks that shared common infrastructure were linked.

The addresses ‘d.kanam@yahoo.com’ and ‘tseringKanyaq@yahoo.com’ do not match known email addresses or names of persons in the Tibetan community. However, “tseringKanyaq” may be a misspelling of Kanyag Tsering, a Tibetan monk from the Kirti Monastery in the Ngaba region of Tibet. This region has been the scene
of a number of Tibetan self-immolations, and Kanyag Tsering has provided reports of the incidents to international media. He is a well known and respected member of the Tibetan community who, due to his work in getting information from inside Tibet to journalists, has developed a significant media presence. We met with Kanyag Tsering and showed him our analysis of this cluster. He confirmed that the address ‘tseringKanyaq@yahoo.com’ does not belong to him. Despite the possible intentional similarity of ‘tseringKanyaq@yahoo.com’ to the name of a notable Tibetan monk, the purpose behind the consistent use of these addresses in the reply-to field is unknown.

We identified three malware families in this cluster, which were used to target Windows (ShadowNet and Duojeen) and OS X (PubSab). The ShadowNet malware family is associated with the ShadowNet espionage group, which was discovered by the Information Warfare Monitor and the ShadowServer Foundation in 2009 and was revealed to be targeting Tibetan organizations and Indian military and government institutions. The malware we found did not connect to infrastructure related to the previous ShadowNet campaign.

All three malware families used in the TseringKanyaq campaign were also used by the LuckyCat campaign, which was discovered by Trend Micro in 2012. LuckyCat is notable for targeting companies based in India and Japan working in aerospace, energy, engineering, shipping, and military research in addition to Tibetan activists. We find infrastructure connections between the TseringKanyaq and LuckyCat campaigns, which suggests some level of coordination.

**EMAIL PROVIDER INFRASTRUCTURE**

This campaign is marked by a period of gaps in which attacks stop and later re-emerge with similar identifying features (most notably the consistent use of the Reply-To addresses), some level of improvements to the malware C2 infrastructure, and/or changes to the social engineering tactics.

We divide these gaps into three distinct periods in which the attackers utilize different email providers to send attacks.

- 163.com: May 4, 2012 - July 9, 2012
- myopera.com: July 24, 2012 - September 5, 2012
- gmx.com: October 14, 2012 - July 26, 2013
Between these three periods there is no overlap in the use of these mail providers. We clearly observe the attackers moving from one provider to the next. The use of these different providers could be due to a number of possibilities: the domain provider may have shut down the accounts due to notifications or detection of abuse, changes to provider infrastructure may have created difficulties in maintaining the accounts, or the attackers may have moved on to the next domain infrastructure once the advantages of an alternate provider became apparent.

163.COM CAMPAIGNS

The first wave of attacks occurred between May 4 and July 9, 2012. Four email attacks were sent during this period targeting Tibet Groups 2 and 4. All of these attacks spoof prominent organizations in the Tibetan community and repurpose legitimate content, which gives them a social engineering sophistication base value of 3. All of the malware samples in this cluster have a technical score of 1.25, for a total TTI of 3.75.

The first attack on May 4, 2012, was sent to Tibet Group 2 with an email that repurposed content concerning a petition campaign. The actual email sender was psjiangzuo@163.com (174.139.21.26). The attached file dropped Duojeen malware that connects to www.xiuxiu.in (173.231.22.201).

The second attack on June 28, 2012, sent to Tibet Group 2, purported to come from Karma Yeshi, a member of the Tibetan Parliament in Exile (TPiE), and provided information (in Tibetan) on the Flame of Truth Rally, a campaign launched by the TPiE to express solidarity with Tibetans who have self-immolated. The actual sender of the mail is sysutiyubu@163.com (222.212.213.197). The attachment also drops Duojeen malware.
On July 5, 2012, Tibet Groups 2 and 4 both received identical emails with content related to a recent self-immolation. The malware used was ShadowNet, which leverages Windows Management Instrumentation (WMI), a system tool meant for administrators. Its intended usage as a tool for collecting system information and automation makes it an ideal mechanism for gathering and exfiltrating data. Use of legitimate Windows features can make it more difficult for administrators to identify activity as malicious.

The ShadowNet attacks used a WMI Script that contained links to one of three blogs to which the malware attempts to connect. The blog then has a string with encoded C2 information as shown in Figure 14 below.

**FIGURE 14:** Sample of blog post used to transmit C2 information to infected machines
Once a connection to the C2 is made, system information and data can be sent to the attackers. In the case of the July 5 attacks, the malware first connects to newwolfs21.blog.163.com, after which it retrieves the C2 newwolfs29.mezoka.com.

On July 9, 2012, Tibet Group 2 received two identical emails sent to two separate organizational accounts. The emails contained content regarding self-immolations. The malware used, Duojeen, retrieves system information, establishes a connection with zml.x.gg, and sends the collected information. It then retrieves second stage malware from http://newwolfs29.zxq.net/winxp.rar. As with the previous attack, the two emails were sent from different accounts: suzhonghechang@163.com (125.70.67.30) and nongzhijiiuye@163.com (199.192.159.213).

**FIGURE 15:** Email sender, IP, and C2 infrastructure for 163.com tseringKanyaq emails
MYOPERA.COM CAMPAIGNS

From July 24 to September 5, 2012, the attackers moved their mail provider to myopera.com. The attacks continued to use ShadowNet and Duojeen malware and the same common C2 infrastructure as the previous campaign. During this period, we observed three attacks sent to Tibet Groups 1, 2, and 4, in some cases to multiple accounts within the organizations. All of these attacks spoofed prominent groups in the Tibetan community and repurposed legitimate content, which gives them a social engineering score of 3. All of the malware samples in this cluster have a technical score of 1.25, for a total TTI of 3.75. Interestingly, in this campaign we observed some emails being sent from Tor exit nodes, which shows the attackers making a new effort to hide their location.

Between July 24 and 25, Tibet Groups 1, 2, and 4 received identical emails that appeared to be from the Tibet Office in Brussels, with content regarding an upcoming rally.

```
From Rinzin Choeden <tibetbrussels@tibet.com>

am directed to send the attached letter regarding observation of solidarity rally on 8th Aug by the Tibetans all over the world as called upon by Kalon Tripa in Kashag's message on July, 2012.

Dear sir/madam,

I am directed to send the attached letter regarding observation of solidarity rally on 8th Aug by the Tibetans all over the world as called upon by Kalon Tripa in Kashag's message on July, 2012.

Kindly acknowledge the email please.

regards

Karma Choeying
Secretary
Bureau du Tibet, Brussels
```

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>cc0b8b8e42fd59cc4b32b3a06e57281</td>
</tr>
<tr>
<td>C2</td>
<td>newwolfs29.mezoka.com (209.190.24.9)</td>
</tr>
</tbody>
</table>
The attached malware was ShadowNet, and it connected to newwolfs21.blog.163.com to retrieve C2 instructions. In each instance, the email was sent from a different account (newwolfs41@myopera.com, tenzin600@myopera.com, tibettibetan3@myopera.com, tenzin600@myopera.com, and mytenzin@myopera.com); however, the sender IP was the same for each account (184.82.49.114). We later discovered that this sender IP was also used as a C2.

During an investigation of one of the C2s used in the campaign (newwolfs20.x.gg/mits/) we found open directories that included a sample from the Sparksrv malware family, which we presume was intended to act as stage two malware. This sample used 184.82.49.114 as a C2.

Between July 25 and 26 Tibet Groups 1, 2, and 4 received identical emails that spoofed Karma Yeshi, a member of the TPiE, with an update on the Flame of Truth rally campaign. The malware in this case was Duojeen.
In three of the attacks, the sender IP traced back to a Tor exit node maintained by the Chaos Computer Club in Germany. The timing of this shift in tactics is interesting, as it comes after a series of attacks that used a C2 as the mail sender. Using Tor to mask the real location of the mail sender may therefore have been an effort to improve operational security. However, the attackers use of Tor is inconsistent and following this series of attacks was observed only one other time.

**TABLE 11: IP address of email senders used during MyOpera campaign**

<table>
<thead>
<tr>
<th>SENDER</th>
<th>IP</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:mytenzin@myopera.com">mytenzin@myopera.com</a></td>
<td>31.172.30.4</td>
<td>Germany - Tor exit node</td>
</tr>
<tr>
<td><a href="mailto:tenzin600@myopera.com">tenzin600@myopera.com</a></td>
<td>62.113.219.3</td>
<td>Germany - Tor exit node</td>
</tr>
<tr>
<td><a href="mailto:tibettibetan3@myopera.com">tibettibetan3@myopera.com</a></td>
<td>31.172.30.3</td>
<td>Germany - Tor exit node</td>
</tr>
<tr>
<td><a href="mailto:tibettibetan3@myopera.com">tibettibetan3@myopera.com</a></td>
<td>50.136.226.40</td>
<td>US - Comcast</td>
</tr>
</tbody>
</table>

The final attack in this campaign was sent to Tibet Group 2 on September 5, 2012. It contains information regarding a hunger strike initiative undertaken by the Tibetan Youth Congress. The attachment contained Duojeen malware that connected to dplcoopsociety.us.dwyu.com (184.82.238.34).
GMX.COM CAMPAIGNS

From October 14, 2012 to July 26, 2013, the attackers switched to gmx.com as their mail provider. The use of gmx.com is interesting, because the email headers from this provider include a unique user ID number, which can be used to track malicious accounts using this service. However, we see no overlap in user IDs from the gmx.com accounts used in the attacks, which suggests that the attackers used a script to generate new accounts, and as a result the user ID number is always different.

Within this period we observe the attackers using reply-to ‘tseringKanyaq@yahoo.com’ and also beginning to use reply-to ‘d.kanam@yahoo.com’ in messages. We cluster attacks by these two accounts in the subsections below.

gmx.com ‘tseringKanyaq’ campaigns

From October 14, 2012 to July 26, 2013, we observed 11 attacks targeting Tibet Groups 1, 2, and 4, using the gmx.com mail provider and a reply-to address of ‘tseringKanyaq@yahoo.com.’
As with the previous campaigns, these messages all spoofed real people and organizations in the Tibetan community. Each email in this campaign has a social engineering sophistication score of 3 and a technical score of 1.25 for a total TTI of 3.75.

Five attacks in this campaign used ShadowNet connecting to www.tbtsociety.info (209.141.36.23), laraider2.he1.ifreeurl.com (46.21.152.227), or www.nedfortibt.info (216.83.45.18). Three attacks dropped Duojeen connecting to laraider2.he1.ifreeurl.com (46.21.152.227).

In one instance we see the connection of an email sender traced back to a Tor exit node (IP 77.247.181.165).

**FIGURE 17:** Email sender, IP, and C2 infrastructure for gmx.com tseringKanyaq emails
gmx.com ‘d.kanam’ campaigns

From December 18, 2012 to May 2, 2013, we observed 12 attacks targeting Tibet Groups 2 and 4 using the gmx mail provider and a reply-to address of ‘d.kanam@yahoo.com.’

Message lures in this campaign all spoofed real people and / or organizations and repurposed legitimate content from Tibetan groups. Each email in this campaign has a social engineering sophistication score of 3.

Seven attacks in this campaign used ShadowNet connecting to www.tbtso-ciety.info, laraider2.he1.ifreeurl.com (46.21.152.227), and pomehra.typepad.com (204.9.177.195). Each of these attacks has a technical score of 1.25.

Two attacks used Duojeen connecting to www.tbtsociety.info (216.83.45.18). Each of these attacks has a technical score of 1.25.

Within this wave of attacks we also observed the use of PubSab implanted in Word documents that used the exploit CVE-2009-0563. In this instance the malware connected to coremail.info (198.74.124.3).
FIGURE 18: Email sender, IP, and C2 infrastructure for gmx.com d.kanam emails

Sender IP | Sender header | Email subject and date | C2 infrastructure
--- | --- | --- | ---
171.216.117.33 | lenzinodje3@gmx.com | [Tibetan Subject] 18 December 2012 | www.tbtworld.info
216.218.197.234 | lenzinodje4@gmx.com | [Tibetan Subject] 24 December 2012 | pomehra.typepad.com
198.74.124.3 | lenzinodje22@gmx.com | [Tibetan Subject] 7 January 2013 | www.tbsociety.info
198.74.124.3 | lenzinodje22@gmx.com | UN Human Rights Council 22nd Session 25 January 2013 | Shadownet / Duojeen
59.177.69.216 | lenzinodje21@gmx.com | [Tibet Group 2] 27 February 2013 | laraider2.he1.ifeareurl.com
77.247.181.165 | lenzinodje21@gmx.com | Shixing Dr. Tsering Sonam in Ottawa, invited to testify in Canadian parliament 11 March 2013 | 46.21.152.227
118.113.253.177 | lenzinodje21@gmx.com | [Tibet Group 2] 25 March 2013 | appleboy111111.blogspot.com
198.96.93.207 | lenzinodje21@gmx.com | [Tibetan subject] 2 May 2013 |
CONNECTIONS TO LUCKYCAT CAMPAIGN

We identify a number of connections between the TseringKanyaq cluster and the LuckyCat campaign, as well as Sparksrv and Duojeen campaigns related to LuckyCat.

The LuckyCat campaign used a variety of malware including Duojeen, ShadowNet and PubSab, which we also see used in the TseringKanyaq campaigns. Beyond this common set of malware we also see connections to infrastructure linked to LuckyCat and related campaigns.

The LuckyCat campaign utilized a series of free hosting and VPS services for its C2 infrastructure. One of the VPS services is hosted on duojee.info. On July 6, 2011, Tibet Group 1 received a malicious email containing ShadowNet malware. While this sample does not include the reply-to address tseringkanyaq@yahoo.com or d.kanam@yahoo.com, the C2 infrastructure has connections to the campaign. The malware connects to and retrieves C2 information from appleboy1111.blogspot.com. We observed a previous version of the script with encoded C2 information that points to duojee.info. The script was then updated to point to www.tbtsociety.info (216.83.45.18), which is a C2 we see used repeatedly in the gmx.com campaigns. The transition to this C2 shows evidence of the attackers shifting infrastructure that was previously linked to LuckyCat to new infrastructure we see used in the TseringKanyaq campaign.

We also see connections to Sparksrv campaigns that have been linked to LuckyCat. Sparksrv is malware used by the LuckyCat campaign as a second stage tool to add additional functionality after the first stage dropper successfully infects a target. Our analysis of open directories on a TseringKanyaq-related C2 revealed Sparksrv on the server, which suggest it was also being used as a second stage in this campaign.

Trend Micro identifies rukiyeangel.dyndns.pro as a C2 used for Sparksrv campaigns related to LuckyCat. In two attacks sent on December 24, 2012 and April 10, 2013, we see the email sender IPs originating from 198.74.124.3 and 216.218.197.234, respectively. The IP 198.74.124.3 currently resolves to coremail.info, which was used as a C2 for PubSab attacks in the TseringKanyaq campaign. Passive DNS records show that 198.74.124.3 and 216.218.197.234 previously resolved to rukiyeangel.dyndns.pro.
OBSERVATIONS

This campaign has several interesting characteristics relative to others in our study. The ShadowNet malware is the only example of WMI malware we observed. While this quality makes the malware relatively easy to remove, it also makes it more difficult for the user to identify. This campaign also relies on a highly disposable C2 infrastructure.

This cluster is also the only campaign to be first identified through contextual clues rather than a strict reliance on shared code or C2 infrastructure. The frequent use of ‘tseringKanyaq@yahoo.com’ and “d.kanam@yahoo.com” in the Reply-to field is in some cases the only indicator tying the attacks together. Despite using a variety of different domains to send the malicious emails, it remains unclear why the same email address was reused so often.

Notably, this campaign also has links to other malware tools and campaigns related to ShadowNet and LuckyCat that have targeted a range of communities and sectors including Tibetans.
DTL Campaigns

<table>
<thead>
<tr>
<th>First Seen</th>
<th>December 21, 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>July 4, 2013</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td>Exploits</td>
<td>Windows: CVE 2010-3333, CVE-2012-0158</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Windows: 9002, 3102, Mongal, Nsfree, Boouset, Gh0st RAT, LURK0 (Gh0st RAT variant), CCTV0 (Gh0st RAT variant), Surtr (Remote and GtRemote), T5000</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 domains: dtl.eatuo.com, dtl.dnsd.me, dtl6.mooo.com, tbwm.wlyf.org</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 3, Tibet Group 4</td>
</tr>
<tr>
<td>TTI Range</td>
<td>2.5 - 6.75</td>
</tr>
</tbody>
</table>

BACKGROUND

We identified a distinct campaign of targeted malware attacks against Tibetan groups that used the shared infrastructure of four C2 domains (dtl.eatuo.com, dtl.dnsd.me, dtl6.mooo.com, tbwm.wlyf.org). Tracking the IP address resolution of these domains over time, we observed that at certain periods they resolve to the same IP and therefore belong to a shared C2 infrastructure. We call this cluster the DTL campaign, because of the use of “dtl” in most of the C2 server domain names. We see this infrastructure used for a series of campaigns that involve 9 malware families: T5000, 9002, Boouset, Mongal, Nsfree, Gh0st RAT, LURK0 (Gh0st RAT variant), CCTV0 (Gh0st RAT variant), and Surtr. We also identified one other malware family (3102) that is likely related due to code overlap.

In November 2013, FireEye published a report that also identified the DTL cluster linking seven malware samples to four C2 domains, three of which we also observed (dtl.eatuo.com, dtl.dnsd.me, dtl6.mooo.com). FireEye only saw DTL campaigns using
the malware family 9002, which we observed being used for three attacks, of which one sample had a matching MD5 to one provided in the FireEye report (9f5e9e6b0c-87cad988f4a486e20bbc99). Our visibility into DTL campaigns only revealed Tibetan targets. However, one attack sent to a Tibet Group had an email body and attachment written in Uyghur. Other researchers have identified attacks related to the DTL campaigns targeting Uyghur groups. The Uyghur samples sent to the Tibet Group may therefore be the operators accidentally sending the wrong lure.

Interestingly, FireEye observed campaigns using DTL infrastructure targeting a range of government and industry entities, showing their scope goes beyond CSOs. Such targets included entities within the following sectors (using FireEye’s categories): U.S. federal government, state and local government, services/consulting/VAR, financial services, telecommunications, aerospace/defense/airlines, energy/utilities/petroleum refining, healthcare/pharmaceuticals, entertainment/media/hospitality, insurance, chemicals/manufacturing/mining, high-tech, and higher education.

MALWARE DEVELOPMENT PATTERNS

Of the nine malware families seen in DTL campaigns, the most frequently used were LURK0 and CCTV0, which are both variations of the Gh0st RAT codebase. LURK0 and CCTV0 are named for the five-character header that appears in network traffic when the malware is run. Both pieces of malware have standard RAT functionality including keylogging, file listing, and data exfiltration. Our observations of the DTL campaign show active development of these RATs over the period of two years that are unique to this cluster.

We found relations between malware samples using binary comparison tools to attempt to determine shared code bases, and comparing various identifiers in the samples. For example, LURK0 creates registry keys with names that are a variation on “DbxUpdate” and then uses a mutex to see if it is already running on the infected system. These names can be customized and used to attempt to distinguish between campaigns using the same malware family. Another useful feature for analysis is compilation times. Although these times can be easily modified, if related samples all have the same compilation date, they were likely created with the same builder. Through analysis of these features and tracking of shared C2 infrastructure we divide DTL-related attacks into a series of eight campaigns. We also discuss two related campaigns that, while not using the same infrastructure, use malware that shares code and identifying features and are likely developed by the same group.
CAMPAIGN 1: T5000

In 2011, four emails were sent to Tibet Group 1 with T5000 malware attached. On January 10, the group received an email with a .rar archive attachment containing an executable file. The email and attachment were in Chinese.

Social engineering | 2
Technical | 1.25
TTI | 2.5
MD5 | 2cf577eda241158e3c3b5431f30b9aeb
On June 1, they received an email with a very similar .rar, this time using the Unicode right-to-left override. We were unable to get either of these samples to connect to a C2, and it is possible that they were not functioning properly.

On July 11, Tibet Group 1 received an email in Tibetan, with a Microsoft Help (.hlp) file attached. The T5000 malware embedded in the file successfully connected to deepinlife.dyndns.info.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>604d501e9e0ce7c175060b8512f706b7</td>
</tr>
<tr>
<td>C2</td>
<td>deepinlife.dyndns.info</td>
</tr>
</tbody>
</table>
On July 26, Tibet Group 1 received the fourth of the emails, with another help file attached. This sample connected directly to 180.178.53.37 without DNS resolution.

T5000 is the first instance we see of the “DTL” name, using Dtl.dat as the name of the network configuration file. Although this campaign does not use DTL domain names for C2 servers, we can identify it as part of this cluster due to the shared sender IPs. All of these emails used gmx email account and were sent from either 66.103.141.24, 69.73.160.142, 65.124.5.107, 64.124.5.107, or 209.234.204.31.

In November 2013, Cylance reported on attacks using T500 that targeted human rights groups and the automotive industry. The name they gave this threat actor was “Grand Theft Auto Panda,” as “they appear to be punching people in the face and stealing their cars.”

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>2.5</td>
</tr>
<tr>
<td>MD5</td>
<td>6b7482e846643938b97e0078379763c5</td>
</tr>
<tr>
<td>C2</td>
<td>180.178.53.37</td>
</tr>
</tbody>
</table>
CAMPAIGN 2: LURK0 (SOFTMY.JKUB.COM)

In February 2011, Tibet Group 1 was sent two identical emails using LURK0 malware that used softmy.jkub.com as a C2. While this campaign does not use DTL-related C2s, the LURK0 samples have features that are otherwise unique to the DTL cluster. The samples originally created a registry key named “DbxUpdate” and a mutex named “111.” The components in these samples have compilation dates of “2010-09-26 04:31:01” and “2010-12-09 03:22:21.”

The emails sent repurposed text about Chinese authorities clamping down on activists following an online call for protests.

In May 2011, Tibet Group 1 was again targeted by attacks using LURK0 samples that connected to softmy.jkub.com. These samples created a folder named “DbxUpdateET” and a mutex named “ET” with compilation times in March 2011. The May and February attacks all utilized DLL hijacking of linkinfo.dll to maintain persistence on the system. The May emails, shown below, described a recent award ceremony.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>2.5</td>
</tr>
<tr>
<td>MD5</td>
<td>37457f46709b793d13a25da0d4c896fa</td>
</tr>
<tr>
<td>C2</td>
<td>softmy.jkub.com</td>
</tr>
</tbody>
</table>
hosted by the Canadian Multicultural Council. We were unable to find references to this event online and therefore cannot confirm if it was real.

In December 2011, multiple members of Tibet Group 1 were targeted by identical emails that appeared to be from a funder providing a report from a grantee. The attached word document dropped Boouset malware that connected to dtl.dnsd.me as a C2. This campaign is the first instance of attacks using DTL-related domains. Boouset is a simple piece of malware (technical score 1.0) with limited code obfuscation that sends unencrypted data back to the C2. It features standard RAT capabilities including a keylogger and the ability to execute remote commands. The social engineering score of these attacks is 3 (TTI 3).
CAMPAIGN 4: LURK0 - CRAZYTOWN EDITION (DTL)

From February 2 to March 14, 2012, a campaign of 10 LURK0 attacks targeted Tibet Groups 1 and 2 using dtl.dnsd.me and dtl.eatuo.com domains as C2s. These were the first LURK0 attacks to use DTL domains as a C2. These samples also performed DLL hijacking on linkinfo.dll and created a key named DbxUpdateET. The mutex name was changed to “ETUN.” These samples use the internal name “ButterFly.dll.” Nine of the attacks used a common tactic of attaching a rar file containing benign jpeg image files and shortcuts that actually link to a LURK0 dropper. These samples had August 15, 2011 as a compilation date.

The emails referenced a number of topics including writings from a Tibetan activist and a recap of a rally held the day before to commemorate the March 10th Tibetan Uprising Day. Another email spoofed the legitimate email address of an individual at the Tibet Bureau in Geneva, and attached a malicious document containing information on the organization of an undetermined election.
CAMPAIGN 5: LURK0 UNDER DEVELOPMENT

In late March 2012, another LURK0 attack was observed that had considerable differences from the previous wave of attacks. Although this new attack also used compressed .rar files as a vector, unlike previous attacks it did not perform a DLL hijack, instead dropping a file called win32.exe. This file writes several new files to disk: IconConfigEt.DAT, containing a DLL with the core RAT functionality; iexplore.exe, which copies IconConfigEt.DAT to IconCacheEt.DLL, overwrites the DAT file and then runs the DLL file; and temp.exe which simply creates a shortcut to iexplore.exe. This functionality changes the persistence mechanism from DLL hijacking to the creation of an executable that launches on startup with the innocuous name of ‘iexplore.exe.’ Once launched, this executable runs the DLL. This sample also features a new mutex name: “ER.” These emails spoofed recognized Tibetan NGOs and referenced content about self-immolations in Tibet, and as a result scored 3.0 on the social engineering sophistication base value. The technical score for these emails was 1.25 for a total TTI of 3.75.

An additional attack in May 2012 indicated further development. This attack utilized a trojaned Word document as the attack vector with password protection to hinder AV detection. The sample was similar to malware seen during the March attack but this time with a different mutex name (“ERXXXXXXXX”) and different names for the droppers. Additionally, instead of using a separate DLL, the sample dropped two files named iexplore.exe. One of these files simply ran the other which was signed with a digital certificate issued to Shenzhen OuMing Keji Co., Ltd.

Emails sent to Tibet Group 1 as part of this attack included repurposed text about self-immolations in Tibet, as well as an email on celebrations of the birthday of HHDL.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>216ca9c711ba602be9ec626d1d44ff99</td>
</tr>
<tr>
<td>C2</td>
<td>dtl.dnsd.me (192.198.85.101)</td>
</tr>
</tbody>
</table>
CAMPAIGN 6: LURK0 (DTL)

In July 2012, another LURK0 campaign of 11 attacks emerged that targeted Tibet Groups 1, 2, and 4 using the dtl.dnsd.me domain as a C2. These LURK0 samples have additional features compared to prior versions. The version of the zlib compression library used for encrypting communications between infected hosts and the C2 was upgraded from 1.1.4 to 1.2.3. These samples also created an executable called iexplore.exe (instead of performing DLL hijacking like in the earlier attacks). However, compared to the previous attacks they featured fewer layers of droppers and extra files. Configuration data like campaign codes and C2 information were changed to being stored in configuration files that could be easily modified. These samples all featured a compilation date of “2012-05-28 05:35:16” and a mutex name of “ERXXXXXXX” while maintaining the “DbxUpdateET” registry key name.

Two of these attacks had lures related to HHDL’s birthday and contained encrypted Word files with the password contained in the message body.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>2.5</td>
</tr>
<tr>
<td>MD5</td>
<td>f2a0787388dd6373336b3f23f204524a</td>
</tr>
<tr>
<td>C2</td>
<td>dtl.dnsd.me (184.105.64.183)</td>
</tr>
</tbody>
</table>

Five of these attacks used .doc implants with decoy documents containing what appears to be a Tibetan organization’s legitimate proposal to the European Instrument for Democracy and Human Rights (EIDHR). The timing of these attacks is noteworthy, as a genuine EIDHR call for proposals—including proposals for
“Actions Aimed at Fighting Cyber-Censorship and to Promote Internet Access and Secure Digital Communication”—was pending at the time, with a July 20 deadline for concept notes. The emails were received by the groups on July 16 and 17, just a few days before the deadline.

Three attacks had identical email lures referencing a South African group’s visit to Dharamsala, India that appear to have been repurposed from a legitimate private communication. The email appears to be a request to the Tibetan organizations hosting the planned trip, with the malicious attachment containing an authentic travel itinerary as a decoy. This is a highly targeted attack based on private communications, and as a result receives the highest social engineering sophistication score (5, TTI 6.75).

**CAMPAIGN 7: CCTV0**

In November 2012 a campaign targeted Tibet Groups 1, 2, and 4 using dtl.dnsd.me and dtl.eatuuo.com domains as C2s. The first wave of these samples had compilation dates of October 15, 2012 and later samples had compilation dates of November 11, 2012. These samples changed the five-character code visible in network traffic from ‘LURK0’ to ‘CCTV0’, which prevents strict IDS rules looking for “LURK0” in network traffic from detecting the malware. The samples featured an embedded DLL with the internal name “ETClientDLL.dll” instead of “ButterflyDll.dll” which was seen in earlier attacks. The initial samples in this wave would query a benign third-party website to determine
the user’s IP. When this website’s results page was modified by its creators, the samples would crash trying to parse the page, leading to the feature being removed in later samples. Another significant change to later samples was padding of the resource section of the executables with extra data, resulting in a larger file size to avoid AV heuristics. Executables were padded with random data to get a different hash every time, making it more difficult for malware researchers and AV companies to share indicators.

TTI scores for the 10 emails varied. Three identical emails were sent to Tibet Group 1 and multiple accounts at Tibet Group 2. The lures used in these attacks were relatively poorly customized.

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>2.5</td>
</tr>
<tr>
<td>MD5</td>
<td>1c44d9cf686f53f1194cdee2aefb99c2</td>
</tr>
<tr>
<td>C2</td>
<td>dtl.dnsd.me (199.36.72.214)</td>
</tr>
</tbody>
</table>
Later attacks included lures with more detailed information.

---

Dear Supporters and Friends:

In the attachment of "Schedule.xls" is the public schedule of His Holiness the Dalai Lama both in India as well as abroad. Please note that for many of these events, tickets are required in order to gain entrance. People are requested to contact the organizers directly or visit the websites given below for further information on tickets. In general, most of the events in India are free where as the majority of events abroad require paid tickets. For your information, as a long-standing policy His Holiness the Dalai Lama does not accept any fees for his talks. Where tickets need to be purchased, organizers are requested by our office to charge the minimum entrance fee in order to cover their costs only.

Please note that the dates are subject to change.

Contact
Office: ohhdl@dalailama.com
Website Feedback: webmaster@dalailama.com

Mailing address:
The Office of His Holiness the Dalai Lama
Trekchen Choeling
P.O. McLeod Ganj
Dharamsala
Himachal Pradesh (H.P.) 176219
India

Telephone:
91 1892 221343
91 1892 221879

Fax:
91 1892 221813

---

<table>
<thead>
<tr>
<th>Social engineering</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1.25</td>
</tr>
<tr>
<td>TTI</td>
<td>3.75</td>
</tr>
<tr>
<td>MD5</td>
<td>16b82aa9f537811490fdf2e347ec106f</td>
</tr>
<tr>
<td>C2</td>
<td>mychangeip1.ddns.info (110.152.229.247)</td>
</tr>
</tbody>
</table>

The changes seen in samples used in this campaign provide insight into the development path of the LURK0 family. Although we did not find C2 infrastructure overlap with other campaigns using LURK0, we did find other similarities. Other campaigns
that used LURK0 continued to use an older version of zlib, retained the LURK0 network header, and used different internal names (such as continuing to use the Butterfly moniker). A possible explanation for this observation is that while threat actor groups may share tools, development and customization of malicious software is decentralized.

**CAMPAIGN 8: SURTR**

From November 2012 until September 2013, the primary malware used in the DTL campaign changed to a new family called Surtr. These attacks continued to use the same C2s as the earlier families. This malware targeted Tibet Groups 1, 2, and 4. Unlike other families in the DTL cluster, Surtr downloads an additional component that contains its main functionality after infection. We have seen two versions of this used with the internal names Remote and GmRemote.

Although the Surtr and LURK0/CCTV0 malware families do not share a large amount of code, they exhibit similarities in behaviour. While some of these similarities, such as the use of zlib in both LURK0/CCTV0 and Surtr, are likely coincidental, others are much more specific. For example, similar registry key names used for configuration information and campaign codes, expanding of the resource section to avoid identical hashes, and similar formatting for sending system information are some of the similarities. Internal names used for the NSFree family and the several LURK0/CCTV0 variations follow a similar scheme, such as the filenames ‘NSFreeDll’ and ‘BTFreeDll’ and the creation of folders named MicET, MicBT, and MicNS.

In addition to these similarities, LURK0/CCTV0 and Surtr have also been used in conjunction with one another. For example, during our analysis we observed LURK0 being downloaded and installed as a stage two after initial infection with Surtr.

---

11 We first reported technical details on Surtr in Kleemola, K., Hardy, S. “Surtr: Malware Family Targeting the Tibetan Community” Citizen Lab, August 2 2013, https://citizenlab.org/2013/08/surtr-malware-family-targeting-the-tibetan-community/
CAMPBIGN 9: 9002

In the first half of 2013, we observed three emails sent out to Tibet Groups 1, 2, and 4 containing the 9002 malware. On March 25, an email was sent to Tibet Groups 1 and 2 with a CVE-2012-0158 attachment from a gmx account with sender IP 66.103.141.24. A different email sent from another gmx account, with sender IP 64.124.5.107 and another malicious attachment, was then seen the next day, March 26, sent to the same groups.

---

**Social engineering** | 3
---|---
**Technical** | 1.25
**TTI** | 3.75
**MD5** | 2c8ef540ae77f1184ddfdd3e0a1f810b
**C2** | dtl.dnsd.me (74.121.190.38)
On May 13, 2013, we saw a similar pattern. A new email was sent from 209.234.204.31 using a gmx account to Tibet Groups 1, 2, and 3, again using CVE-2012-0158. This email was then seen again on May 14, sent to many other targets including more staff at Tibet Group 1, and a number of other Tibetan NGOs, and CTA offices.

All of the 9002 samples connected to C2 servers at dtl.dnsd.me and dtl.eatuo.com on port 3123. This campaign uses campaign codes of the form “Tmdd,” where m is the month and dd is the day (e.g., T315 for emails sent on March 15).

An interesting feature of the 9002 malware is that it shares exported function names and embedded filenames with Surtr, making it very likely that it was developed alongside Surtr by the same group.
RELATED 3102 CAMPAIGN

3102 is a family of malware that appears similar to 9002, but with additional protection and anti-reversing features. We observed one campaign using 3102 with techniques similar to the original 9002 campaign.

On November 18, 2013, Tibet Groups 1 and 2 each received an email with a Tibetan theme from a Yahoo! address. While these emails contained the same subject, body, and attachment using CVE-2012-0158, they each had different recipient lists visible in the To: and Cc: headers. The inclusion of visible recipient lists is a method also used in the 9002 campaign.

---

Social engineering 2
Technical 1.25
TTI 2.5
MD5 6bd6b50af9361da2361ff34a8ca99274
C2 183.86.194.130

OBSERVATIONS

The DTL campaign is notable for the variety of malware families used, the active development cycles of the malware, and connections to targeting of government and private industry.

The malware development cycle used here was easily traceable, and during the course of our study we were able to identify a large number of changes made and their
effects. While most campaigns focused on the use of a small number of malware families, we identified upwards of 10 distinct families in this cluster. Although some of these families were variants of each other, the range of malware used demonstrates the adaptability of attackers and their persistence in developing new techniques to compromise their targets.

In this campaign we see DTL-related infrastructure that was also used in the attacks against industry and government targets that were reported by FireEye. However, we see little overlap in the malware families. The DTL attacks reported by FireEye exclusively used 9002, whereas we see 9002 and nine other families in our dataset. This lack of similarity suggests that DTL operators may differentiate the tools used in their operations based on the target type.
A new campaign using Surtr as the primary malware family emerged in August 2013, about one month after the DTL attacks stopped. This campaign’s C2 infrastructure consists of free ChangeIP domains. This campaign uses throwaway AOL and Gmail accounts designed to impersonate real people and legitimate organizations to deliver malicious emails. There is no overlap with infrastructure seen in any other campaigns, but this could simply be the result of the use of dynamic DNS and free subdomains.

<table>
<thead>
<tr>
<th>First Seen</th>
<th>August 1, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>ongoing</td>
</tr>
<tr>
<td>Attack Vectors</td>
<td>Targeted malicious emails</td>
</tr>
<tr>
<td>Exploits</td>
<td>CVE-2012-0158</td>
</tr>
<tr>
<td>Malware Families</td>
<td>Surtr (GtRemote, Remote), PlugX</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>C2 Domains: carts.dnset.com; free1999.jkub.com; kevin.zzux.com; lenovo.wha.la; patton.mrslove.com; tibelds-ddns.us; tibetantimes.ezua.com; zeeza.info</td>
</tr>
<tr>
<td>Targeted Groups</td>
<td>Tibet Group 1, Tibet Group 2, Tibet Group 4, Tibet Group 5</td>
</tr>
<tr>
<td>TTI Range</td>
<td>1.25 - 3.75</td>
</tr>
</tbody>
</table>
Although this cluster uses dynamic DNS, the domains will often resolve to the same IPs at the same time, as shown in Table 12.
This is the only campaign outside of DTL that we have seen use Surtr. Like the DTL campaign, the primary attack vector is malicious email attachments using CVE-2012-0158.

We have identified 67 attacks related to this campaign since we first discovered it in August 2013. It began with two unique emails sent to Tibet Groups 2 and 4 on August 1, 2013. The message to Tibet Group 2 appeared to be an internal mailing list used by its steering committee and staff. The message requests that the list administrator approve a mailing list posting. The message sent to Tibet Group 4 purported to be from “Tibeta Associatio” (sic) and referenced Tibetan autonomy in the subject line but had no message in the email body. Both attacks use .rtf files that drop Surtr (GtRemote) and connect to free1999.jkub.com.

For the first year of the campaign, Surtr was used exclusively. In July 2014, this campaign began using a variant of PlugX. This version removed the identifying strings found in previous versions of the malware. The variant still used the DLL side loading technique found in previous versions, albeit with a different legitimate executable. It also contained the same functionality. A notable difference was that the malware did not load a properly formed executable into memory, in what appears to be an attempt to hinder analysis.

At the time of writing, this campaign remains the main source of attacks targeting Tibetan Groups, and we are continuing to monitor developments.
EXTENDED ANALYSIS:

2.3

Civil Society Perspectives and Responses
Over the course of the study we conducted interviews and site visits with nine of the 10 groups participating in our study. The interviews were intended to provide greater context into the perceptions and implications of the attacks documented in this report. The interviews were transcribed and coded to identify emergent themes. This section reflects those themes as section headers, which are as follows:

- Information communication technologies (ICTs) as an enabler and threat to civil society groups
- How our participants perceive digital risks and threats
- The impact of targeted attacks
- Civil society responses to targeted attacks

Each section, in turn, draws on participants’ responses, alongside our synthesis, to provide a window into how groups under threat think about and respond to digital threats. In general, we documented groups at different stages of addressing digital security. Some groups had taken on digital security as a core part of their mission before the study began. Others had only begun to notice issues about digital security a few years ago but by the time of interviewing spoke to us about digital threats as a structural problem for their operations. Still, many were in the process of trying to decide on what measures to take, and how to implement them systematically.

**ICT: Enabler and Threat to Civil Society Groups**

ICTs are central to the activities of the groups, and help them balance an historic asymmetry between them and powerful, well-resourced state interests.

> [Technology] is the only way you can have any serious impact if you’re a size like us and you are trying to go up against the Chinese government which has considerable more resources than us. So if you want to try to

---

12 We were unable to conduct interviews and a site visit with China Group 2.

have an impact, technology is the leverage.\textsuperscript{14}

The two large human rights organizations in our study both operate distributed programming across multiple countries with hundreds of staff and partner organizations. The size and complexity of these operations makes these groups highly reliant on technology.

\textit{Now we do work in more than 80 countries at any given time, and we have staff based in many cities across the world.}\textsuperscript{15}

The theme of diaspora communications was central to groups related to Tibet and China. The Tibet Groups, for example, find that technology enables them to reach into restricted environments from “safe” areas overseas.

\textit{In comparison to other communities, there is almost nowhere that is so physically separated because of the restraints imposed by China…Even in Pyongyang, you got foreign journalists…Tibet is just closed off…Technology is the only way that that can be bridged.}\textsuperscript{16}

ICTs are also the primary tool that organizations used to connect with the highly distributed and fractured community in the Tibetan diaspora and in Tibet.

\textit{Those of us born and raised in exile, and certainly our parents and other generations, crave to go home to this land they are so attached to. Then technology comes along and it’s like BOOM! You can have it all...on some level even though the Chinese are still there and physically we can’t do it, but in this other space we can.}\textsuperscript{17}

\textsuperscript{14} China Group 1, Director, 2010

\textsuperscript{15} Rights Group 2, Technical Officer, 2011

\textsuperscript{16} Tibet Group 1, Program Officer, 2011

\textsuperscript{17} Tibet Group 1, Director, 2011
WECHAT: CONNECTIVITY AND RISKS

WeChat is a mobile chat application developed by Chinese company Tencent, which has gained huge user numbers around the world with a high concentration in China. Tibet Groups cited WeChat, which is highly popular in their community, as an example of the tension between connectivity and security. This connectivity was seen as beneficial, but not without risks.

“New ground shows up like WeChat...and it threatens to both undermine [our efforts] and offers us some ideas for what it is people want and [what they're] willing to compromise for the sake of connection.”—Director, Tibet Group 1

“Tibetans in India and Nepal, Tibetans in the West are all being connected by using the same app...and forging these new connections...in some ways, we're seeing really good things come out of it in terms of all the news we're getting from Tibet and seeing all the footage from the self-immolations and protests coming from WeChat and in that sense it's becoming important, but people are not so attuned to the risks.”—Program Officer, Tibet Group 1

Tibet Groups voiced concerns over the increasing popularity of WeChat due to censorship and surveillance requirements on companies operating in China, and the close relationship between Tencent and the Communist Party of China. Adding to these concerns are a series of documented incidents of Tibetans in Tibet being arrested for content they shared on WeChat, like images of HHDL.

Civil society and its champions are not the only groups who felt that technology could enable movements to push back against the status quo. A Tibetan group noted that they thought the Chinese government, was also very concerned about its potential.

...self immolations and protests...the Tibetan cultural pride, the songs...this is the reason the Chinese are cracking down so hard and going after everyone ..... the censorship and the surveillance is...[happening] because the technology has showed them what's possible. There is a movement now where there wasn’t one or where it had almost disappeared before... the technology has enabled that.18

Yet the ability to connect is constantly eroded by efforts to monitor and interfere with groups’ activities. Participants also recognized that their reliance on technology intro-
duced new risks of monitoring, coercion, and electronic attack.

[Technology is] this funny thing where it’s a life line, and then it’s...maybe your ticket to jail.¹⁹

Groups need members of their communities to maximize the use of ICTs but also to do so securely.

We...need this technology, but we need everybody to know how to use it and be able to be secure and be safe.²⁰

Targeted digital threats are also changing how some CSOs see the promise of technology.

I think that civil society is feeling the heat around targeted attacks and surveillance and I think it’s affecting the public sphere and our ability to feel comfortable communicating in what used to be understood as a free and open medium.²¹

In practice, CSOs are in a constant process of navigating through new communication environments, and tradeoffs between connectivity and security. Contrasting theories have popularly characterized ICTs either as “liberation technologies” that can empower political movements, or as levers of control for governments to suppress these very same movements.²² Our participants suggest that the reality is somewhere in between.

How Civil Society Groups Perceive Risk and Threats

We tried to elicit participants’ informal “threat models” as a precursor to understanding how these models shaped their response to digital risks.²³ All of the groups in our study work on political issues that can potentially be seen as threatening to specific authorities. The context of this work makes many groups perceive the attacks against them as politically motivated.

---

¹⁹ Tibet Group 1, Director, 2011

²⁰ Tibet Group 1, Program Officer, 2011

²¹ Rights Group 2, Technical Officer, 2014


²³ A threat model assesses the risk and relative impact of threats against an entity that are specific to the context in which it is situated.
Although political concerns were a backdrop to the attacks, groups tended to focus on the tactical goals of the attackers rather than the greater political objectives. Groups described the probable goals of attacks as efforts to “hinder our operations,” “keep an eye on things,” or cause as much “inconvenience and chaos as possible [to] somehow affect our ability to do what we do.”

While groups shared similar views on the operational objectives of attackers, their sense of risk stemming from attacks depended on the physical proximity of their adversary. A program manager with extensive field experience working with CSOs in multiple countries explained that groups operating within the jurisdiction of an adversary have greater concerns over physical security and other direct interference from authorities.

...in many places it’s a very physical sort of thing. Our biggest challenge...[was when]...local authorities wandered in and took computers. So it’s not like we expect the attacks to be all coming in over the wire. In most places where we operate it’s probably not even the easiest place for them to get at although it is certainly a lot more subtle.

If a group is situated outside of a physical jurisdiction controlled by an adversary then targeted digital threats may be a higher priority concern than physical threats.

Take for example Ukraine where they aren’t necessarily expecting a lot of challenges with their local government, but they might be a target for cross border action, that is one of the places where the digital threats become a particular vector or focus rather than just one of the many things that they are thinking about.

DIASPORA AND EXILE COMMUNITY THREAT MODELS

Many of the participants in our study working on China and Tibet issues are embedded within geographically distributed diaspora networks. Their missions often include collecting information from closed areas “inside,” while transmitting other information back in. As the director of an organization working on China explained:

---

24 Rights Group 1, Chief Technical Officer, 2011; Tibet Group 2, Executive Director, 2014
25 Rights Group 1, Program Manager, 2014
26 Rights Group 1, Program Manager, 2014
Our main target and focus is on the mainland. And so the people who [we] are trying to promote, the people who we are trying to give platforms for their issues and their problems and their voices are inside.27

A central concern of these groups was the security of the bidirectional flow of information to and from at-risk persons in China and Tibet. A group working on China perceived its adversary as primarily interested in this information exchange.

Anyone who doesn’t want [our organization] to be able to safely and securely get information from inside...and send it back in. What kind of information? Individual case information, human rights information... Anyone who has an incentive not to have people know about it would have the incentive to compromise our operations and make it hard for us -- and that’s a lot of people.28

Due to the antagonistic response these activities elicit from the Chinese government, the Tibet and China Groups generally perceived the actors behind targeted digital attacks on their community to be directed by or related to agents of the PRC.

I think in most cases, [the staff] believe it’s coming from China.29

Tibetan groups in exile perceived Tibetans living “inside” as having the highest likelihood and impact of harm from digital attack. To demonstrate the potential consequences of targeted digital threats, a Tibetan security trainer explained how he presents the connection between actions outside affecting at-risk groups inside Tibet.

I kind of force them into thinking about like the risk associated with Tibetans inside Tibet, and also kind of like stress the fact ‘We are in a free country, we don’t have to worry about ourselves...What can the Chinese government do to me? Nothing. But what happens when you have done something that’s harming somebody else inside Tibet?’ ...that’s when a lot of people think about it a little more.30

The threat models of groups working on China and Tibet show a priority given to digital threats due to the proximity of these groups to their perceived adversary and the years of persistent attacks they have experienced.
...most communities just aren’t...under as persistent, sophisticated and threatening attacks, so they just have not gotten to the same place in prioritizing digital security.31

Our study exclusively addresses digital threats and does not cover all potential threats a group may face. While digital threats are a primary security concern for the majority of groups in our study, they are just one piece of a holistic risk environment for CSOs.

Impact of Targeted Threats on Civil Society Groups

Most participants were clear that they saw potentially severe consequences from targeted digital attacks, with the greatest danger being to communications with those “inside,” and hence vulnerable to arrest or harassment. Nevertheless, a few participants surprised us by noting that their organization downplayed the possibility of negative consequences from attacks (or had done so in the past). Often this reaction took the form of citing the ‘openness’ of their organization’s work, and suggesting that there was ‘nothing sensitive’ in their exposed data.

This is an organization predicated on virtues of transparency...when I first came here there were a lot of conversations like, ‘Why should we encrypt our email, we are not hiding anything.’32

As evidence of attacks against that human rights organization piled up, however, perceptions began to change.

...there has been a sea change in the four years since I have been here...they recognize a riskier threat environment and how it is dealt with.33

Awareness of risks was, however, still a work in progress.

...in the last year or two any organization that I have been working with in a closed society or dealing with sensitive topics at least has some sort of hazy consideration that this stuff should be a concern and that’s maybe a change from

31 Tibet Group 1, Director, 2011
32 Rights Group 1, Program Manager, 2014
33 Rights Group 1, Program Manager, 2014
These responses raise an important issue: the relationship between digital compromises and the use of the compromised information by adversaries is indirect. Unlike the consequences of physical threats, which are often directly observable to a non-expert, the most serious impacts of digital threats are typically at least one step removed from the technology that has been exploited. Making the link between technological threats and “real-world” harm can be challenging, in part due to limited evidence.

... [there has] been little evidence of the direct impact on people’s safety as a result of some of these threats.... [but] our understanding of how surveillance and repressive practices have operated even in pre-digital times provides us with sufficient evidence to understand that there may be a connection. I believe that there has been an increase on the reach of this harm by specialist state actors...  

**CONNECTING SURVEILLANCE AND HARM**

We often heard stories of arrest and detention from groups in the study (and through other Citizen Lab projects) that appeared to be linked to electronic surveillance.

Members of the Tibetan community shared with us accounts of Chinese authorities confronting Tibetans with call records and chat transcripts during interrogations. Meanwhile, research on Ethiopia has revealed that detainees have been presented with similar evidence during interrogations.

In Syria there are also reports of interrogators presenting detainees with records of communications, and cases where accounts of detainees are used to seed malware to contact lists.

In Bahrain, meanwhile, activists were arrested after posting pseudonymous tweets critical of the government. The real identities of these persons may have been discovered by authorities through a technique in which an attacker sends the pseudonymous Twitter account a link to a webpage containing an embedded remote image. When the victim clicks on the link or opens the email, their IP address is revealed to the attacker. Authorities can then link the IP to the target’s true identity through their ISP.

We strongly suspect that these cases are only the tip of the iceberg, and that the digital element in many cases of harm goes unrecognized due to lack of investigation, not lack of incidents.
We also think, however, that by downplaying the consequences of targeted digital threats, some participants were showing us something interesting about the resilience and adaptability of their communication styles, which have co-existed with an adversary that has used extensive monitoring for many years.

...it can be a nuisance, it can be a distraction, it can waste time, but...in the grand scheme of things, it’s not as though the movement on a whole operates in a way that is dependent upon secure conversations.\textsuperscript{36}

Nevertheless, the same participant was very clear that serious (even physical) harm could come to individuals and groups “inside” through targeted attacks against them or their contacts.

**PSYCHOLOGICAL IMPACTS AND COPING STRATEGIES**

While tracking the consequences of a targeted attack for networks of trust and reputation can be challenging and require investigation, some participants spoke in detail about the psychological impact of compromise.

It was quite upsetting. I think it sort of paralyzed us emotionally—the two of us that were affected—for a few days.\textsuperscript{37}

In this incident, the emotional harm was perceived as more impairing, and less easily mitigated, than the breach to the computer system.

...the act of cleaning our computers was something that was relatively straight-forward...but it was the emotional impact that sort of threw us.\textsuperscript{38}

Further work is needed to document the connection between targeted digital threats and psychosocial strain to move towards a more complete understanding of how targeted individuals and organizations evolve and adapt their coping strategies. One interesting coping strategy prevalent among Tibet Groups was to explain attention from adversaries as a signal that their work was important, and was having an impact.

The reason you are a target is because you are doing something that is bothering somebody and to be proud actually of the work that you do that has drawn the attention of these people who clearly want to mess us up somehow.\textsuperscript{39}

\textsuperscript{36} Tibet Group 2, Director, 2014

\textsuperscript{37} Tibet Group 2, Director, 2014

\textsuperscript{38} Tibet Group 2, Director, 2014

\textsuperscript{39} Tibet Group 2, Director, 2014
As one participant put it, the challenge was to balance the frustration of being compromised with feelings of encouragement:

…we work so hard the entire day and then at the end of the day when you find out that your website has been attacked and people can’t get access to it, you get frustrated, but at the same time you also get more encouraged to know that… feeling that your work is making an impact and the Chinese government has to go to the extent of spending time following us and attacking us and spending large amounts of money just for that.\(^\text{40}\)

**BEING TARGETED: A TEACHABLE MOMENT**

Beyond trainings and awareness campaigns, what brought threats home, unsurprisingly, was being targeted or compromised. Being attacked personalized the problem, and turned warnings into tangible concerns.

>[It] is visible for users in places that they understand—your email, your Twitter account—even if they don’t understand the implications, the connections…they now see it as something real and personal.\(^\text{41}\)

Tibet Groups felt that the persistent targeting of their community has helped them raise awareness of digital security and highlight the need for vigilance.

>It has made Tibetans more aware of the potential of the Chinese government. We always think about the Chinese government creating problems for us diplomatically, we don’t think of the cyber world…and how they can maneuver their way into it.\(^\text{42}\)

>[The attacks]... give us as a reminder to be more careful.\(^\text{43}\)

Groups made it clear that greater awareness is a work in progress, and that documenting the connection between attacks and specific harms to individuals and groups is a promising way forward.

>The basic goals should be to get people to realize that these threats are real... the

---

\(^{40}\) Tibet Group 3, Editor-in-Chief, 2014

\(^{41}\) Rights Group 2, Technical Officer, 2014

\(^{42}\) Tibet Group 3, Editor in Chief, 2014

\(^{43}\) Tibet Group 5, Program Officer, 2014
As groups struggled with targeted threats, many placed an emphasis on awareness raising and user education as a primary method of responding. These kinds of strategies are important for civil society and applicable to a variety of problems. The fact that many of the digital threats they experience rely on social engineering makes this a promising direction. However, responses from the groups also suggest that resource constraints, and limits on available technical expertise, may have constrained other avenues of response.

**RESOURCE AND CAPACITY CONSTRAINTS**

The most commonly mentioned challenge to addressing digital threats was, unsurprisingly, resource issues in general, and technical resources and skills in particular:

> Every community with a struggle is under-resourced, and if this hasn’t moved up the priority list, they don’t have the capacity to do this type of stuff or implement it or there’s not even enough awareness that is needed for them to be able to [get] people to pay attention.  

**Organizations in the Global South**

These challenges are especially acute for groups in the global South. All Tibet Groups in our study had their operations or a portion of their operations based in Dharamsala, India. In this context, the groups are operating within a refugee community grappling with persistent targeted attacks and conventional development challenges. Resources are sparse. These groups cannot afford enterprise computing infrastructures, or the expensive security solutions adopted by larger, well-resourced counterparts.

Complicating these challenges is the problem of “brain drain” of technically skilled people in the community. Participants told us many Tibetans with specialized technical training

---

44 Tibet Group 1, Program Director, 2011

45 Tibet Group 1, Director, 2011
leave Dharamsala in search of better job prospects elsewhere. Tibet Groups saw the need to create opportunities for Tibetans with technical skills to work in the community:

[Tibetans living in exile in India] are essentially a refugee population and all these folks want to get jobs. So, if we can actually bring them in and give them jobs in supporting their own community, that’s kind of a goal.46

Others, on the same topic, suggested that the problem was improving, slowly:

I think now it’s coming up slowly and slowly, but there was a time in the Tibetan community where we really lacked webmasters, where we really lacked people who are well equipped and who have good knowledge in terms of Internet security. 47

These challenges are not unique to the Tibet Groups. Rights Group 1 explained that local partners supported by the group faced similar technical capacity difficulties:

Security is hard and it’s much harder than it needs to be….the challenge of trying to keep your stuff in some kind of secure state as is currently defined is just well beyond what any typical partner organization is able to deal with…For most of our partners they are lucky if they have a young guy who understands a bit about computers.48

A particularly common problem for groups in the global South is the use of pirated software (unpatched or pre-backdoored software is often a source of insecurity). The use of pirated software is widespread in the Tibetan community due to prohibitive licensing costs. Similarly a program officer in a large rights group explained it is difficult to convince a local partner to purchase a software license “when you can jump out to the local market, [and] for a dollar buy a disk.”49

Larger Organizations

Two of our participating organizations, Rights Groups 1 and 2, had significantly higher technical capacities and financial resources, and they approached information security in a manner similar in some ways to a large company. For example, the groups have senior management in charge of security and technology, IT support teams / help desks, and occasionally hire companies to provide security consultations

46 Tibet Group 1, Program Director, 2011
47 Tibet Group 5, Program Officer, 2014
48 Rights Group 1, Program Manager, 2014
49 Rights Group 1, Program Manager, 2014
and incident response services. However, although the size and resources of these groups afford them certain advantages over smaller groups, they experience equally vexing security challenges.

The complexity of global operations and distributed staff and partners creates problems for introducing and sustaining security awareness, even as attacks seem to increase:

*We have seen a colossal uptake on attacks on the home office or we are just much more aware of them than we used to be. We anticipate that such things are also happening at the field office level and to our partners, but we have much less visibility into that.*

The lack of network visibility among in-country offices was cited as a particular challenge:

*We don’t have a unified network with all our field offices... so we don’t have the same enterprise level of security and capacity there...[the field offices and NGO partners] have to face a range of threats that are from the physical world as well.*

Both groups face challenges adapting technology policies for regional offices and partner organizations. Rights Group 2, for example, contended with securing its head office and maintaining awareness of threats faced by field offices:

*There’s not a lot of security awareness in the organization. There’s ... small pockets of knowledge, but the rest of the organization will prove to be the weakest link....people don’t understand, especially people that work in the field don’t understand the sensitivity of the work the organization does, so they tend to be a bit more lax about... certain things.*

Bureaucratic processes were seen as hindering the adoption of new security policies, given the challenge of informing decision makers about emerging security issues:

*I think it has been very top-down, you know some [policy] comes from the top, they go to the bottom and there is no way to inform what’s going on in the decision process.*

50 Rights Group 1, Program Manager, 2014
51 Rights Group 1, Program Manager, 2014
52 Rights Group 2, Technical Officer, 2014
53 Rights Group 2, Technical Officer, 2011
TRAINING AND USER EDUCATION

While the two large groups were able to invest in security appliances and dedicated technology support, the other groups in our study focused on user education and awareness as the primary security strategy.

The majority of groups focused on internal training programs and training with partner groups. Five were able to conduct these trainings themselves, while four others drew on third-party support. These trainings varied widely, ranging from short explanations of security policies to sustained user education programs.

Several key themes emerged from our interviews about digital security trainings: the value of understanding the local context, the need for training based on organization-specific threat models, and the value of focusing on behavior rather than simply teaching a wide range of tools.

Training informed by local context and threat models

While user education and training were a major part of groups’ strategies, most highlighted the importance of situating trainings in local context and using accessible language and concepts.

If we could break it down for people in a way that they understand, if we could give them metaphors and other ways to understand what exactly this means for us, and paint the bigger picture, it has an impact.

Rights Group 1 explained that conducting formal risk assessments of its partner organizations was key in developing appropriate educational strategies.

Other groups engaged in training shared similar comments and noted the importance of ensuring trainings are in line with both technical and contextual realities. Several interviewees pointed out that keeping abreast of new technical developments and context-specific risks was challenging and time-consuming, highlighting the value of intermediary organizations that perform this role within a particular targeted civil society context. Indeed, Tibet Group 1 went so far as to structure its mission to focus on digital security awareness and education programs for the Tibetan community. The
group provided training support to all the other Tibetan organizations who participated in the study.

**Moving Beyond Tools**

All of the groups identified a common set of user practices for preventing infection of malware: not opening unsolicited attachments, being careful with web links, keeping systems up-to-date, and generally remaining vigilant online. Explaining the safe and secure use of tools was an aspect of training, but many groups focused more on how to change behaviour and develop a security mindset rather than train specific tools.

> [We are] trying to equip people with a different mindset, so that they are changing their behaviors...so they...run through a mental filter before doing something. 

Tibet Group 1, which regularly provided trainings to its peers, was particularly adamant about the need to focus on user behaviour over specific tools:

> We would really like to see resources shift from trying to mitigate problems through tools, to mitigating problems through education and educating people about their practices.

The Tibet Groups felt that user education had to be a community-wide effort and not something isolated to particular organizations or individuals. For example, some Tibetan groups have been promoting a “Detach from Attachments” campaign that encourages users to move away from sharing documents through email attachments and shift to alternative cloud-based platforms like Google Drive. The campaign uses a mix of humor and references to Tibetan culture and is a good example of user education that is connected to a specific threat model and local context.

Encouraging behavioural change and implementing new organizational policies can be challenging. Tibet Group 5 explained that while malicious attachments were a priority threat for the group, moving to alternative document platforms was difficult due in part to generational gaps in the group’s membership. Users from older generations, they explained, were resistant to changing familiar practices, like the use of attachments.

Understanding these organizational challenges and breaking down trainings into simple incremental steps that can be adapted to specific environments were identified as keys.
to success. A Tibetan security trainer described the importance of showing people small victories from their point of view and demonstrating how they can learn to achieve ICT objectives in ways that are safe and secure, but also do not appear too difficult for them to use in their daily workflows. Others agreed, saying that their goal was to find techniques that made it “as simple as [possible] to do the right thing...”

Indeed, there were some cases where, if implemented effectively, modest behavior modifications could have a considerable impact. While we observed organizational challenges in implementing practices like “Detach from Attachments,” based on what we have seen, the campaign could be effective against some of the current threats against the Tibetan community. More than 80% of malware submitted to us by Tibet Groups used a malicious email attachment. Furthermore, for two of the Tibet Groups in our study, simply not opening attachments would mitigate more than 95% of targeted malware threats that use email as a vector.

However, this is just one mitigation strategy focused on a single vector of attack. Threat actors are highly motivated and will likely adapt their tactics as users change their behaviors. For example, it is possible that if every user in a particular community began to avoid opening attachments, attackers would move on to vectors such as watering hole attacks or attacks on cloud-based document platforms.

As the groups themselves noted, user education and awareness-raising activities need to be ongoing, and must be informed by local context, threat models, and the latest technical information.

---

59 Tibet Group 1, Security Trainer, 2013
60 Rights Group 1, Program Manager, 2014
61 This determination is based on two groups that had submitted at least 40 emails.
COMMUNITIES @ RISK
Targeted Digital Threats Against Civil Society
November 11, 2014
https://targetedthreats.net/
GLOSSARY
Technical Glossary

ActiveX
A software framework created by Microsoft that allows for embedded objects such as scripts, images, movies, or programs to be added into other document types, like web pages. Malicious ActiveX controls are often used by attackers to gain unauthorized access to computer systems.

Advanced Persistent Threat (APT)
Advanced persistent threat (APT) is a term used to describe digital attacks that compromise computer systems with the intent of collecting data and monitoring communications without being noticed. They typically intend to persist for months or even years, and are generally associated with harvesting of information for political or economic purposes. The term is not to be confused with ‘APT1’, the name given to a specific threat actor group.

Android Application Package (APK)
A file format that is used to distribute software for the Android platform of mobile devices.

Antivirus (AV)
A class of applications that seek to identify malicious software, often by using a library of signatures previously identified as being associated with malicious software.

Attack Vector
The entry point by which an attacker gains unauthorized access to a computer system. Examples of an attack vector would be a malicious email attachment, sending a malicious link, or sending malicious files through an instant messaging program.

Backdoor
A method by which an attacker maintains access and control of a system after an initial compromise. This could be in the form of a hidden server listening on a port for an attacker to connect.

Beaconing
In terms of malicious network traffic, beaconing is a network pattern whereby malware
sends out network traffic to a command and control server (C2) at regular intervals. Beaconing traffic can serve as a “heartbeat” signal to inform the command and control server that a given client is active.

Botnet
A distinct network of machines, typically compromised by malware, that is controlled by attackers without the permission or knowledge of their owner.

Campaign
Campaigns are collections of targeted malware attacks that share some common infrastructure or resource. Targeted malware attacks are typically not one-off events, and in many cases malware samples can be grouped together as “campaigns” based on common C2 infrastructure, malware development, social engineering tactics, or static analysis of malware code.

Cluster
A grouping of malware samples that share common features. Examples of these commonalities include shared command and control infrastructure, shared originating IP address, shared tactics, or shared malware development branches.

Collateral Compromise
A computer compromise that results in the additional or unintended compromise of additional targets. An example would be the compromise of clients that use shared web hosting, when the intended attack target is just one client of many hosted on a given server.

Command-and-Control (C2)
Command-and-control (‘C2’ or ‘C&C’) servers are computers used to send and receive commands and data to computers infected with malware. Upon being infected with malware, a compromised computer will attempt to contact a C2, which issues it commands, sends additional malware to install and exfiltrates data. C2 infrastructure can take different forms, with the most common being a domain name either registered or compromised specifically to act as a C2. It is often possible to link different malware attacks together through their use of common C2 infrastructure.

Common Vulnerabilities and Exposures (CVEs)
A dictionary of common names for publicly known security vulnerabilities. CVEs are composed of the format: CVE-YYYY-NNNN, where YYYY references the year of discovery and NNNN references a unique number for the CVE. CVEs are commonly used to establish a common language when discussing security vulnerabilities.

Distributed Denial of Service (DDoS)
A type of attack in which a service is flooded with simultaneous requests in an effort to render a service unstable or unusable. When these requests are made with multiple computers or even botnets these type of attacks are considered “distributed”

**Dynamic-Link Library (DLL)**

A file used by other programs instead of directly by the user. They often contain features that are optional, or shared with multiple programs.

**DLL Hijacking**

DLL Hijacking is the technique of using a legitimate program with a malicious shared library that shares the name of a system library. Some programs, if not configured properly, will look for the shared library by name, with priority going to a library with that name in the current path. This allows an attacker to add malicious code to a program without modifying its valid digital signature.

**Defacement (website)**

A website defacement is a malicious act that replaces the contents of a website with content written by an attacker that has gained unauthorized access to a website. These messages can vary in content from lewd content to political statements.

**Domain Name Service (DNS)**

An Internet service analogous to a phone book that translates human friendly and easy-to-remember domain names to IP addresses. For example DNS translates domain.com into the IP address 65.254.244.180.

**Dynamic Domain Name Service (DDNS)**

A method of updating a DNS record in situations where the IP of a client can change, such as a home Internet connection. DDNS domains are often composed of two subdomains in the format {given_name}.{ddnsprovider}.com Free DDNS services are often favored by attackers for command and control domains as they do not require a user to provide proof of identity or payment where regular domain services do.

**Drive-by Download**

An unintended download of a file that is the result of simply visiting a malicious or compromised web page.

**Drop**

Any file that is created during the execution of malicious software.

**Exfiltration**

Exfiltration is the process of collecting data (such as documents, emails, contact lists, or even microphone or webcam data) from a compromised computer or device and
sending it back to the attacker. Attackers will traditionally encrypt and compress data before exfiltration.

Exploit
A piece of computer code that takes advantage of a flaw or glitch in software in order to cause a result that is either unexpected, unintended or malicious. Exploits are commonly used by attackers to gain unauthorized access to computer systems.

Flag Text
Flag text refers to a defining piece of text that is present in malicious network traffic (often a preamble) that ties it into a specific family or type of malware. For instance the Gh0st RAT family of malware will commonly use Gh0st as the flag text in its network traffic.

Hash
A hash is a string of hexadecimal characters that identifies a file; should the file change in any way, the hash will as well. Hashes are designed to be easy to compute from a file, enable checking to ensure that the file has not been changed, and to compare files to determine if they are identical.

Header (email)
A group of field/value pairs that precede email messages that describe routing information as well as meta data, and path information for emails. In computer security, email headers are valuable in determining spoofed senders and other anomalies in messages.

Header (file)
A file header refers to additional information, commonly metadata, that is placed at the start of a file or a block of data.

Infrastructure
In terms of computer security, infrastructure, refers to the totality of an attackers computer resources. Computer servers that are used for malicious means as well as IP addresses and compromised machines make up parts in a given attacking infrastructure.

Java
A programming language whose code must be executed through a virtual machine that is typically installed as a software package. Java programs are distributed as Java ARchive files (JARs). Flaws in how Java handles certain code are often exploited by attackers to compromise computer systems.

MD5
MD5 hashes, also called message digests, are often used to identify a file based on
its content. MD5s take the form of a string of hexadecimal data, such as ‘6fb3ecc3d-b624a4912ddbd2d565c4395’. If two files have the same hash, they are the same file. MD5s are frequently used to compare samples of malware from different sources to identify if they are the same.

Malware
Also known as malicious software, refers to software that is installed on a computer, often by deceit or trickery, that serves to disrupt operation, or gain unauthorized access to a given computer or its files.

Malware Family
A broad grouping of malicious software that share common features or development branch. Examples of malware families include ShadowNet, sparksrv or PlugX.

MIME HTML (MHTML)
An archive web page format that is used to wrap HTML code and associated files such as images, and scripts into a single file. This is commonly used in creating format rich e-mail messages. Attackers outlined in this report commonly exploit how these files are handled in Microsoft Word in order to compromise computer systems.

Mutex
Short for ‘mutual exclusion’, mutex is a process to prevent multiple threads of a program from accessing the same data at the same time.

Network Intrusion Detection System (NIDS)
A network appliance that the examines network traffic of a computer or network in order to detect patterns that are indicators of attack, compromise, or suspicion of either.

Obfuscation
Any attempt to hide the content or intent of a communication or a piece of data. Obfuscation is sometimes used by malware to hide the fact that it is malicious, or to make analysis more technically difficult or resource intensive.

Packet Capture (PCAP)
A file format that includes the totality of network traffic, including headers and payloads, for a given period of time, or based on particular criteria.

Passive DNS
An information service that records the results of DNS queries passively over a long period of time in order to track the historical values of DNS lookups.

Payload
The portion of a network transmission that is the intended purpose of that transmission.
For instance, if someone is logging into a website, the username and the password that is sent is a payload while any network headers or metadata are not. In computer security, a payload refers to the portion of a file that performs the malicious action.

**Remote Access Trojan (RAT)**

A remote access trojan (RAT) is a software tool that allows a user to remotely access and control another computer. While remotely controlling a computer is a common and legitimate form of system administration, the term ‘RAT’ is used to refer to surreptitious and illegitimate access to a remote computer. While the sophistication of RATs can vary, they often have a similar set of capabilities, such as the ability to exfiltrate data, take screen captures, enable webcams/microphones, and install additional software.

**Rich Text Format (RTF)**

A file format developed by Microsoft intended for text documents with a modest amount of formatting information. Exploits in how Microsoft Word handles this format are commonly used by the attackers outlined in this report.

**Social Engineering**

Deceiving an intended target of compromise by non technical means such as trickery, flattery, or appeal to authority. The composition of e-mail messages where there is a malicious attachment is a common form of social engineering.

**Spearphishing**

Spearphishing is a term to described the use of targeted email attacks designed to compromise a specific individual or group. Spearphishing is a more targeted form of phishing (attacks sent to a broader group of targets).

**Spoofing (email)**

A spoofed email is a technique whereby the original sender of a message is masked or outwardly replaced. This is typically used to deceive the recipient and assist in social engineering.

**Spyware**

A piece of software that gathers and sends information about the computer it is installed by without the owner’s consent or knowledge. Spyware ranges from web browser tracking cookies to expertly designed malicious programs.

**Stage 0 / Stage 1 / Stage 2 / etc.**

The staging system outlines the phases by which malware evolves and expands on a compromised computer system. Stage 0 refers to the initially received malicious file. Stage 1 refers to the malicious payload of that file. Stage 2 refers to any additional files that the payload may download from an external source once executed. Additional
stage numbers are used if the file downloads still more components.

The Onion Router (Tor)
An encrypted network service designed for anonymity and circumvention of Internet censorship. Tor is sometimes used by attackers to hide their true location of either themselves or command-and-control servers.

Trojan
A type of malware program that masquerades as another type of file but actually causes a computer system harm, like installing a backdoor or stealing user information.

Unicode Right-to-Left (RTL) Override
Unicode is a system for encoding and display of characters on a computer. There are currently over 110,000 characters that can be displayed with Unicode. Some Unicode characters have special meanings that alter the way text is displayed, instead of representing a specific character. The Unicode Right-to-Left (RTL) Override is an invisible character that, when displayed, changes the direction of text flow to the left. This is often used as a trick to hide the true extension of a file by displaying a file name backwards.

User Account Control (UAC)
A security feature of Microsoft Windows. Introduced in Windows Vista and Server 2008, this feature aimed to improve security by employing a more strict separation of user privileges. Properly implemented user privilege separation can make the execution of malware more difficult.

Virtual Private Network (VPN)
A method by which private computer networks can communicate through public networks. A commonly used VPN configuration, for example, allows remote employees to communicate with the computer network of their company. Malicious attackers sometimes use VPNs as a portion of their attack infrastructure.

Virtual Private Server (VPS)
A virtualized computer server that is sold by a company, often for the purposes of hosting a website or publicly accessible Internet service.

VirusTotal (VT)
A free service owned by Google Inc. that allows users to submit samples of suspicious files in order to be scanned by a variety of antivirus engines. These samples are made available to subscribers in the security community.

YARA signatures
YARA is a software tool used by malware researchers to identify and classify malware
samples. Each sample is given a signature, which lists identifying features of the malware. As part of this project, we have created YARA signatures for the malware we have identified.

**Watering Hole Attack**

A type of targeted attack in which a malicious actor compromises a website that is commonly visited by their intended victim(s). It is named a watering hole attack because the attacker seeks to attack or poison a commonly visited area (the watering hole) as a means to attack a certain group.

**Windows Management Instrumentation (WMI)**

A Windows abstraction layer that exposes information and notifications about software or hardware often for the purposes of system management software or system administration scripts. Attackers can write malicious WMI scripts in order to make malware more difficult to identify in cases of compromise.

**XOR**

XOR is the “exclusive or” logical operation. This operation is commonly used in cryptography although XOR alone is considered a very weak form of encryption. XOR encryption is sometimes used as a very basic method by which malware protects data such as the command and control server it uses.

**Zero-day**

Also known as “0day” is an attack that exploits a previously undocumented or unreleased flaw in software. Zero-day attacks are significant because they are difficult to discover (and hence costly for attackers to acquire and use) and difficult to defend against.
COMMUNITIES @ RISK
Targeted Digital Threats Against Civil Society
November 11, 2014
https://targetedthreats.net/
Appendix A:

Social Engineering Sophistication Score Examples
In this section, we provide specific examples of emails that would be assigned targeting scores described in The Extended Analysis.

Social Engineering Sophistication Score 1 (Targeted, Not Customized)

This email was sent to Tibet Group 1. The message content and sender are vague and do not relate to the interest of the group. The attachment is a Word document implanted with malware. The lack of relevant information in this message gives it a score of 1 (Targeted, Not customized).

Social Engineering Sophistication Score 2 (Targeted, Poorly Customized)

This email was sent to Tibet Group 1. It references Tibetan self-immolations, an issue of interest to the group. However, the sender does not appear to be a real person or organization and the message content is terse and does not reference information that can be externally validated. While this message references content relevant to the recipient, it does not appear to come from a real person or organization, or repurpose externally verifiable content, and therefore scores a 2 (Targeted, Poorly Customized).
Social Engineering Sophistication Score 3 (Targeted, Customized)

This email was sent to Tibet Group 2. On the surface it appears to be a professional email from “Palden Sangpo,” a consultant at the Tibet Career Centre. The email sender address and signature reference accurate contact details that can be easily verified through an Internet search. However, inspection of the email headers reveals the purported email sender address is fraudulent and the actual sender was albano_kuqo@gmx.com. The email generally addresses the organization, rather than the individual recipient. Therefore, this message scores a 3 (Targeted, Customized).

Social Engineering Sophistication Score 4 (Targeted, Personalized)

This email sent to Tibet Group 1 is directly addressed to the director of the group and purports to come from Cheng Li, a prominent China scholar based at the Brookings Institution. The message asks the recipient for information on recent Tibetan self-immolations. The email
address is made to appear to be from Cheng Li, but is actually sent from an AOL account (chengli.brookings@aol.com) that was registered by the attackers. The level of customization and personalization used in this message gives it a score of 4 (Targeted, Personalized).

Social Engineering Sophistication Score 5 (Targeted, Highly Personalized)

Targeting scores of 5 (Targeted, Highly Personalized) require use of internal information from the target organization that could not be obtained through open sources. For example, Tibet Group 2 and Tibet Group 3 received separate emails that contained specific personal details about a South African group’s visit to Dharamsala, India that appear to have been repurposed from a real private communication. The email was written as a request to the Tibetan organizations for help with the planned trip. The malicious attachment contains an authentic travel itinerary, which would be displayed after the user opens the document and becomes infected by the malware. The private information used in these messages suggests that the attackers likely obtained it through a prior compromise of the group’s communications.
FURTHER READING
CITIZEN LAB REPORTS


Seth Hardy, “What is an APT without a sensationalist name?” SecTor Conference, October 18, 2011, http://sector.ca/Media/Past-Events/what-is-an-apt-without-a-sensationalist-name-13636

Targeted malware attacks are particularly dangerous to NGOs and other organizations that take real-world risks while often having little if any IT security budget. This presentation describes a variety of targeted malware attacks observed in the wild against human rights organizations, and the techniques (both social and technical) that they use to be successful. It then looks at the technical details of a data exfiltration network: what information is being stolen, how it is leaving your network, and where it is going. The presentation concludes with observations on how this kind of targeted malware differs from those used for financial gain, and steps that organizations can take to defend themselves, even with very limited resources.


This post is the first in a series of analyses that the Citizen Lab prepared regarding the urgent and ongoing threat presented by information operations deployed against Tibetans and others who advocate for Tibetan rights and freedoms, including in Tibetan areas of China. The Citizen Lab is concerned with the apparent increase in the use of social engineering linked to the issue of self-immolation to target Tibetan activists with malware, as well as the reported increase in magnitude of information controls (in close coordination with more physical measures) utilized by the Chinese government in Tibetan areas.


The use of remote surveillance software against activists has been a feature of the ongoing conflict in Syria. The EFF and Citizen Lab report on the use of a new toolkit by a previously observed attacker, which has been circulating malware which surreptitiously installs BlackShades Remote Access Trojan (RAT) on victim’s machines.

The Citizen Lab analyzes a recent targeted malware attack against the Tibetan community which spoofs a June 14, 2012 resolution of the European Parliament on the human rights situation in Tibet. While such repurposing of authentic content for use as a malware delivery mechanism is not unusual, this incident raises serious questions surrounding the use of legitimate political resources for illegitimate ends.


This Citizen Lab posts analyzes several pieces of malware targeting Bahraini dissidents, which were shared with us by Bloomberg News. The analysis suggests that the malware used is FinSpy, part of the commercial intrusion kit, Finisher, distributed by the United Kingdom-based company, Gamma International.


The Citizen Lab has analyzed recent targeted malware attacks against Tibetan organizations that share a common payload —LURK malware—and command-and-control server, as well as several other features.


This report describes a Remote Access Trojan (RAT) that three human rights-related organizations taking part in our study received via email in 2011 and at the end of 2010. We refer to this RAT as the IEXPLORE RAT, after the name of the launcher program. This RAT has the ability to record user keystrokes (including passwords), copy and delete files, download and run new programs, and even use the computer’s microphone and camera to listen and watch the user in real-time.


This post describes our work analyzing several samples which appear to be mobile variants of the FinFisher Toolkit, and scanning we performed which identified more apparent FinFisher command and control servers.

In this Citizen Lab blog post, we report on malware campaigns targeting human rights groups using the PlugX Remote Access Trojan.


In this report, Citizen Lab Security Researcher Morgan Marquis-Boire describes analysis performed on malicious software used to compromise a high profile dissident residing in the United Arab Emirates. The findings indicate that the software is a commercial surveillance backdoor distributed by an Italian company known as Hacking Team. The report also describes the potential involvement of vulnerabilities sold by the French company, VUPEN.


In this report we found malware used in a targeted attack against a Tibetan human rights organization which was closely related to malware described by Mandiant. In their report, Mandiant described how APT1 (referred to as “Comment Crew” or “Byzantine Candor” in other reports) has targeted a large number of organizations in a wide range of industries, stealing terabytes of data. Our report demonstrates that APT1 is not only involved in industrial and corporate espionage, but also in attacks against civil society actors documented as early as 2010. This observation reflects other findings showing that in some cases the same threat actors and infrastructure are used to target government and industry are also used against civil society groups.


Canada Centre for Global Security Studies and Citizen Lab Director Ron Deibert and Senior Researcher Sarah McKune authored an article in CircleID on an often overlooked dimension of cyber threats and cyber espionage: the targeting of civil society actors.


This report describes the results of a comprehensive global Internet scan for the command-
and-control servers of FinFisher’s surveillance software. We have found command-and-control servers for FinSpy backdoors, part of Gamma International’s FinFisher “remote monitoring solution,” in a total of 25 countries: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam. The report also details the discovery of FinFisher in Ethiopia, which targets individuals using pictures of Ginbot 7, an Ethiopian opposition group, as bait to infect users. Additionally, it provides examination of a FinSpy Mobile sample found in the wild, which appears to have been used in Vietnam.


In January 2013, we were provided with a sample of a highly targeted attack delivered through email that contained compromised versions of two Android applications that are popular in the Tibetan community: KakaoTalk (a mobile messaging client) and TuneIn (an Internet radio application). The email message repurposed a legitimate private email message sent by an information security expert in the Tibetan community to a member of the Tibetan parliament-in-exile. The compromised versions of the Android applications contained malware that is is designed to send a user’s contacts, SMS message history, and cellular network location to attackers. The cellular network information gathered by this malware would only be useful to actors with detailed knowledge of the cellular communication provider’s technical infrastructure. These findings demonstrate the risks communities face from targeted mobile malware. While the majority of targeted attacks we observe are designed to exploit the Windows operating system, we are also observing attacks targeting OS X, Linux and Android. Attackers will continue to adopt new methods and widen targeting of platforms. We had this report translated into Tibetan and circulated amongst the community to raise user awareness of targeted mobile malware threats.


The report features new findings, as well as consolidates a year of our research on the commercial market for offensive computer network intrusion capabilities developed by Western companies. Taken together with our previous research into FinFisher, we can now assert that FinFisher’s command-and-control servers are currently active, or have been present, in 36 countries (Australia, Austria, Bahrain, Bangladesh, Brunei, Bulgaria, Canada, Czech Republic, Estonia, Ethiopia, Germany, Hungary, India, Indonesia, Japan, Latvia, Lithuania, Macedonia, Malaysia, Mexico, Mongolia, Netherlands, Nigeria, Pakistan, Panama, Qatar,
Romania, Serbia, Singapore, South Africa, Turkey, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.) We have also identified a FinSpy sample that appears to be specifically targeting Malay language speakers, masquerading as a document discussing Malaysia’s upcoming 2013 General Elections. We identify instances where FinSpy makes use of Mozilla’s Trademark and Code. The latest Malay-language sample masquerades as Mozilla Firefox in both file properties and in manifest.


Syria’s opposition has faced persistent targeting by Pro-Government Electronic Actors throughout the Syrian civil war. A pro-government group calling itself the Syrian Electronic Army has gained visibility throughout the conflict with high profile attacks against news organizations. Meanwhile, Syrian activists continue to be targeted with online attacks apparently for the purposes of accessing their private communications and stealing their secrets. Researchers have identified a common theme among the attacks against the Syrian opposition: sophisticated social engineering that is grounded in an awareness of the needs, interests, and weaknesses of the opposition. This report describes two types of attacks that follow this theme: One is a malicious installer of the circumvention tool Freagate, while the other is an e-mail attachment calling for jihad against Hezbollah and the Assad regime or promising interesting regional news. The report was translated into Arabic by Cyber Arabs.


In this report, we document the discovery of a malware family we call “Surtr,” which we have observed used in attacks against Tibetan groups since November 2012. This malware family continues to be used in campaigns and we are actively tracking its development and the threat actors and infrastructure behind its operation. Before we published our report, we prepared a special advisory for the Tibetan community that we circulated privately to increase user awareness. We also submitted technical details on the malware family to the DeepEnd Research Library of Malware Traffic patterns, which is a community resource that collects traffic analysis of malware families from open sources to help researchers identify and track these malware families and develop defenses against them.

Seth Hardy, “Targeted Threat Index,” Citizen Lab, October 18, 2013, https://citizenlab.org/2013/10/targeted-threat-index/

We published a short report on our first iteration of the Targeted Threat Index (TTI) following strong interest shown in the metric when we presented it at Canada’s premier information security Conference SecTor in October 2013. We later refined and iterated on the
TTI and produced an expanded version of the analysis for our Usenix Security 2014 paper submission.


Citizen Lab security researchers Morgan Marquis-Boire and John Scott-Railton along with Electronic Frontier Foundation (EFF) Global Policy Analyst Eva Galperin published a technical paper outlining how Syrian pro-government attackers targeted the opposition, as well as NGO workers and journalists, with social engineering and Remote Access Tools. The report builds on extensive previous research and writings by EFF and Citizen Lab to update what we know about malware campaigns targeting the Syrian opposition. The report’s accompanying piece was published in Wired magazine.


In February 2014, we reported on targeted attacks against the Ethiopian Satellite Television Service (ESAT), an independent satellite television, radio, and online news media outlet run by members of the Ethiopian diaspora, that we revealed to be using Remote Control System, sold exclusively to governments by Milan-based Hacking Team. The malware communicated with an IP address belonging to Ariave Satcom, a satellite provider that services Africa, Europe, and Asia.


This report maps out covert networks of “proxy servers” used to launder data that Hacking Team’s Remote Control System (RCS) exfiltrates from infected computers, through third countries, to an “endpoint,” which we believe represents the spyware’s government operator. This process is designed to obscure the identity of the government conducting the spying. For example, data destined for an endpoint in Mexico appears to be routed through four different proxies, each in a different country. This so-called “collection infrastructure” appears to be provided by one or more commercial vendors—perhaps including Hacking Team itself. Hacking Team advertises that their RCS spyware is “untraceable” to a specific government operator. However, we claim to identify a number of current or former government users of the spyware by pinpointing endpoints, and studying instances of RCS that we have observed. We suspect that agencies of these twenty-one governments are current
or former users of RCS: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan.


This report is a follow up to our previous report, titled “Mapping Hacking Team’s “Untraceable” Spyware,” which identifies 21 governments that we suspect are current or former users of Remote Control System (RCS). The report showed that computers infected with RCS send surveillance data back to the government operator through a series of servers in multiple third countries, called a proxy chain or circuit. We delve deeper into these proxy chains, and find that in at least 12 cases, US-based data centers are part of this dedicated foreign espionage infrastructure. Our analysis traces these proxy chains, and finds that US-based servers appear to assist the governments of Azerbaijan, Colombia, Ethiopia, Korea, Mexico, Morocco, Poland, Thailand, Uzbekistan, and the United Arab Emirates in their espionage and/or law enforcement operations.


In March 2014, we documented a malicious repackaging of Psiphon 3, which is a circumvention tool originally developed by the Citizen Lab, which was spun out into a private Canadian corporation in 2008. The malware contains both a functioning copy of Psiphon, and the njRAT trojan. When executed, the implant communicates with a Syrian command-and-control server. This is likely part of a targeted attack against the Syrian opposition by a known actor, not all users of Psiphon. This report was translated into Arabic and disseminated to at risk users. (https://citizenlab.org/2014/03/arabic-warning-maliciously-repackaged-psiphon/)


This report analyzes Hacking Team’s Android implant, and uses new documents to illustrate how their Remote Control System (RCS) interception product works. RCS is a surveillance malware toolkit marketed for “lawful interception” use. We identified and analyzed RCS Android implants that had lures with a political subtext suggesting targets in the Qatif Governorate of Saudi Arabia. Analysis of these implants revealed a range of surveillance functions.

Repressive nation-states have long monitored telecommunications to keep tabs on political dissent. The Internet and online social networks, however, pose novel technical challenges to this practice, even as they open up new domains for surveillance. We analyze an extensive collection of suspicious files and links targeting activists, opposition members, and nongovernmental organizations in the Middle East over the past several years. We find that these artifacts reflect efforts to attack targets’ devices for the purposes of eavesdropping, stealing information, and/or unmasking anonymous users. We describe attack campaigns we have observed in Bahrain, Syria, and the United Arab Emirates (UAE), investigating attackers, tools, and techniques. In addition to off-the-shelf remote access trojans and the use of third-party IP-tracking services, we identify commercial spyware marketed exclusively to governments, including Gamma’s FinSpy and Hacking Team’s Remote Control System (RCS). We describe their use in Bahrain and the UAE, and map out the potential broader scope of this activity by conducting global scans of the corresponding command-and-control servers. Finally, we frame the real-world consequences of these campaigns via strong circumstantial evidence linking hacking to arrests, interrogations, and imprisonment.


Targeted attacks on civil society and non-governmental organizations have gone underreported despite the fact that these organizations have been shown to be frequent targets of these attacks. In this paper, we shed light on targeted malware attacks faced by these organizations by studying malicious e-mails received by 10 civil society organizations (the majority of which are from groups related to China and Tibet issues) over a period of four years. Our study highlights important properties of malware threats faced by these organizations with implications on how these organizations defend themselves and how we quantify these threats. We find that the technical sophistication of malware we observe is fairly low, with more effort placed on socially engineering the e-mail content. Based on this observation, we develop the Targeted Threat Index (TTI), a metric which incorporates both social engineering and technical sophistication when assessing the risk of malware threats. We demonstrate that this metric is more effective than simple technical sophistication for identifying malware threats with the highest potential to successfully compromise victims. We also discuss how education efforts focused on changing user behaviour can help prevent
For two of the three Tibetan groups in our study simple steps such as avoiding the use of email attachments could cut document-based malware threats delivered through e-mail that we observed by up to 95%.


This report provides a detailed analysis of two products sold for facilitating targeted surveillance, known as network injection appliances. These products allow for the easy deployment of targeted surveillance implants and are being sold by commercial vendors to countries around the world. Compromising a target becomes as simple as waiting for the user to view unencrypted content on the Internet. While the technology required to perform such attacks has been understood for some time, there is limited documentation of the operation of these attacks by state actors. This report provides details on the use of such surveillance solutions including how they are built, deployed, and operated.

CIVIL SOCIETY REPORTS /CAMPAIGNS


Access, “Global Civil Society At Risk: One of these things is not like the other—A report on fake domain attacks,” August 2, 2013, https://www.accessnow.org/page/-/docs/Access%20Tech/FakeDomainsReport.pdf


Bytes for All Pakistan, “Loss of privacy is always permanent—Snags in hearing of FinFisher case at Lahore High Court,” August 22, 2014, [https://content.bytesforall.pk/node/143](https://content.bytesforall.pk/node/143)

Bytes for All Pakistan, “Notorious spy technology found in Pakistan,” May 1, 2013, [https://content.bytesforall.pk/node/99](https://content.bytesforall.pk/node/99)

Bytes for All Pakistan, “Online surveillance becomes a priority for the Human Rights Council, as Pakistan joins the wrong side of the debate,” September 25, 2013, [https://content.bytesforall.pk/node/111](https://content.bytesforall.pk/node/111)

Bytes for All Pakistan, “Oral Statement delivered by Bytes for All, Pakistan at 23rd Regular Session of the UN Human Rights Council,” June 14, 2013, [https://content.bytesforall.pk/node/103](https://content.bytesforall.pk/node/103)

Bytes for All Pakistan, “Privacy rights violations challenged in Lahore High Court,” May 8, 2013, [https://content.bytesforall.pk/node/100](https://content.bytesforall.pk/node/100)

Bytes for All Pakistan, “Update: Lahore High Court Orders Inquiry into FinFisher Usage in Pakistan,” May 15, 2013, [https://content.bytesforall.pk/node/101](https://content.bytesforall.pk/node/101)


Coalition Against Unlawful Surveillance Exports (CAUSE), [http://www.globalcause.net/](http://www.globalcause.net/)


Digital Defenders Partnership, [https://digitaldefenders.org/](https://digitaldefenders.org/)

Digital Rights Foundation, “Pakistan is a FinFisher customer, leak confirms,” August 22,


Eva Galperin and Morgan Marquis-Boire, “Fake Skype Encryption Tool Targeted at Syrian


Privacy International, “Has Hacking Team’s government trojan been used against journalists?,” August 7, 2012, https://www.privacyinternational.org/blog/has-hacking-teams-government-trojan-been-used-against-journalists


Privacy International, “Our OECD complaint against Gamma International and Trovicor,”


Ranking Digital Rights, http://rankingdigitalrights.org/


Tibet Action, “Mobile Phone Security,” https://tibetaction.net/mobile-security/


Tibet Action, “Think Before You Click,” https://tibetaction.net/think-before-you-click/


SECURITY INDUSTRY REPORTS AND RESOURCES


Contagio Malware Dump, http://contagiodump.blogspot.ca/


FURTHER READING


The Dark Visitor, http://www.thedarkvisitor.com/

**DIGITAL SECURITY TOOLS**

This section contains a series of guides and online resources on digital security. Digital security is highly specific to an individual or group’s context and environment, and no one guide or tool can address all possible risks. We do not endorse any particular products or services.


GOVERNMENT RESOURCES


Stop Digital Arms Trade, http://www.stopdigitalarms.eu/


INDUSTRY AND MULTI-STAKEHOLDER INITIATIVES

Global Network Initiative
http://www.globalnetworkinitiative.org/

The Global Network Initiative is a collection of ICT companies, civil society organizations, investors, and academics which aims to provide guidance, expertise and policy engagement to ICT companies on issues of protecting and advancing rights to privacy and freedom of expression.

Telecommunications Industry Dialogue
http://www.telecomindustrydialogue.org/home

The Telecommunications Industry Dialogue is a group of telecommunications operators and vendors who jointly address freedom of expression and privacy rights in the telecommunications sector in the context of the UN Guiding Principles on Business and Human Rights. The initiative was launched in March of 2013.
INTERNATIONAL ORGANIZATION AND INTERNATIONAL LEGAL RESOURCES

The following United Nations declaration and covenants form the basis for the definition of “human rights” used in this study:


A number of reports, guides and resolutions by United Nations bodies and the European Commission have specifically dealt with the issue of human rights and ICTs:


Frank La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,” April 17, 2013, http://www.ohchr.org/Docu-
