FinFisher: The Nexus Of Security and Human Rights

By Andrew Brieff

1 Abstract

In the wake of the Edward Snowden revelations about the NSA, Government surveillance has been thrust to the forefront of conversations around the world about the give and take between security and freedom. In America, the conversation mostly revolves around the potential for abuse that such power concentrated in the central government could produce. However, around the world, such surveillance techniques are already being used for the scare tactics and human rights abuses Americans are afraid of. In Bahrain, a journalist was followed, harassed, and beaten, all because the government was able to monitor his communications and whereabouts using complicated surveillance malware that often goes undetected by traditional means.[1]

In this project, I am going to analyze one particular software suite, FinFisher, which is a surveillance suite produced in Germany and the U.K. and used worldwide by governments to spy on criminals and political dissidents alike. I'll focus on its capabilities to extract information from an infected computer, and exactly how it is sent and organized by a central authority. I'll then demonstrate how this dangerous malware can be detected by a new security tool called Detekt, built by Amnesty International, Citizens Watch, and the Electronic Frontier Foundation working in unison. Finally, I'll

[1] Amnesty International "Detekt, new software tool in the 'cat and mouse' game against Big Brother November 2014

touch on the moral obligations Western governments may or may not have to make sure security software like FinFisher produced within its borders is not being used elsewhere to facilitate human rights violations.

2 Introduction

In 2011, Ahmed Mansoor, a UAE national, was released from jail, having served a sentence for the crimes of “owning an online discussion group” and “sign[ing] a pro-democracy petition.”[2] Jailing individuals for crimes such as these is a violation of the universal human right to expression, and the victim of an authoritarian government that sees maintaining power as more important than protecting the rights of its citizens. [3] Unfortunately, the human rights abuses perpetrated against Ahmed did not end with his release. As time passed, Ahmed began to realize that his “movements were at times monitored,” and was the victim of physical assault on at least two occasions. Curious as to how he was being tracked, Ahmed discovered that his computer was infected with spyware, and that the government was “monitor[ing] his every move.”[4]

Unfortunately, Ahmed’s story is all too familiar. Around the world, Authoritarian regimes use surveillance tactics to intimidate dissidents and repress expression. In 2011, after the overthrow of Egyptian President Hosni Mubarak, revolutionaries

[2] Amnesty International “Detekt, new software tool in the ‘cat and mouse’ game against Big Brother November 2014 www.amnesty.org

[3] United Nations “The Universal Declaration of Human Rights”

[4] Amnesty International “Detekt, new software tool in the ‘cat and mouse’ game against Big Brother November 2014 www.amnesty.org

discovered a 5 month trial of FinFisher in the offices of the security forces.[5] As in the UAE, the government was using surveillance techniques in its arsenal of weapons against human rights defenders. FinFisher is marketed by a company called Gamma Int, whose headquarters include Germany, UK, and Italy. Gamma Int. sells its software to governments and police departments, with little to no oversight over how it's being used to violate human rights. Customers include Mongolia, Qatar, South Africa, Bahrain, Australia, Belgium, Italy, Hungary, and Nigeria, among many others.[6] The following analysis will work to demonstrate how details about how FinFisher enters a system, how it gathers data and avoids detection, and how it communicates with its host network. It will also preview Detekt, a new software tool produced by Citizens Watch in collaboration with Amnesty International and the Electronics Frontier Foundation to detect the presence of FinFisher and other surveillance tools that may be used by governments to spy on its citizens.

3 To the Community

In the aftermath of the Edward Snowden leaks about the NSA, it is increasingly clear that we are living in new era of widespread government surveillance of citizens, for better or for worse. Private security firms operate out of Western nations with impunity, and sales of cyber surveillance tools face few regulations in comparison to sales of conventional weapons, and any laws existing are often ignored and unenforced.

[5] The Electronic Frontier Foundation "Spy Tech Companies & Their Authoritarian Customers, Part I: FinFisher And Amesys" Feb 6, 2012 www.eff.org

[6] WikiLeaks "SpyFiles4" Sept 15th, 2014 www.wikileaks.org

Privacy International, a London based charity that works to defend and promote the privacy rights worldwide, has threatened a lawsuit against the US government. In its letter to the U.K. secretary of state for business innovation, Privacy International present a summation about the their grievances with companies such as Gamma. They state "Plainly there is a very real risk, if not an inevitability, that surveillance equipment, such as the FinFisher products, has been, and continues to be, exported to countries where it is highly likely to be used for internal repression and breaches of human rights."[7] This is the heart of the issue: do we, as Western nations, have an obligation to ensure that software produced in our countries is not sold abroad to be used to facilitate government repression like that which has occurred in UAE? If so, the argument follows that if we do not regulate the sale of software such as FinFisher, we are indirectly responsible for the harassment of Ahmed Mansoor, and the countless cases of individuals being attacked for their political beliefs. There are legitimate uses for software such as FinSpy, such as to prevent terrorist attacks, and help track other dangerous criminals. But without proper oversight and controls over how FinSpy is being deployed, the potential for abuse is far too great to justify the possible positive contributions it might make towards safety.

While further analysis of FinFisher, in order to understand its signatures and facilitate its detection by those who are being targeted will be the primary focus of this paper, perhaps the most important idea to take away is that we need to have a conversation in our own countries about whether we are morally responsible for

[7] Bloomberg "Cyber Attacks on Activists traced to FinFisher Spyware of Gamma" July 25, 2012 www.bloomberg.com

allowing this technology to be produced and propagated. Already in the United Kingdom, the government is re evaluating how it regulates sales of surveillance software to foreign countries, and is beginning to enforce the need for licenses to export these products.[8] The Electronic Frontier Foundation offers a “Know Your Customer” standards checklist for companies looking to export surveillance software. The checklist outlines ways in which to determine if the customer for a particular product might use it to abuse human rights.

Applications: How is FinFisher Delivered?

While the exact method of delivery differs, FinFisher usually acts as a Trojan Horse, installing itself with the download of innocuous images or programs. According to the FinFisher training manual, unique Trojans are created by its FinSpy Agent software. [9] This section will analyze an email sent to a Bahraini activist which contained the FinFisher malware. While it can be expected that FinFisher often uses similar tactics to infiltrate a system, its method of entry may vary and precaution should always be taken to avoid spyware. Points of analysis are taken from Citizen Lab’s report *“From Bahrain With Love: FinFisher’s Spy Kit Exposed?”* In the report, Citizen Lab allows FinSpy to infect its machine to analyze its behavior. By analyzing how FinFisher extracts data and

[8] BitDefender “Exported UK Surveillance Tech Under Tighter Control: FinFisher License to Export Opens the Way” Sept 11, 2012 www.bitdefender.co.uk

[9] WikiLeaks “SpyFiles4” Sept 15th, 2014 www.wikileaks.org

obfuscates its actions, we can begin to build systems that detect its signatures and prevent it from being used to repress political expression in the future.[10]

In the case of Bahrain, activists were sent malicious emails with what looks like pictures to download from the crackdowns in the country. The emails seemed to be sent by Melissa Chan, who is a real reporter for Al Jazeera, a news network based in Qatar. From just the initial deception of disguising the attack as an email from a fellow human rights defender, it is clear that whoever is behind the attack is tailoring it to a specific target.

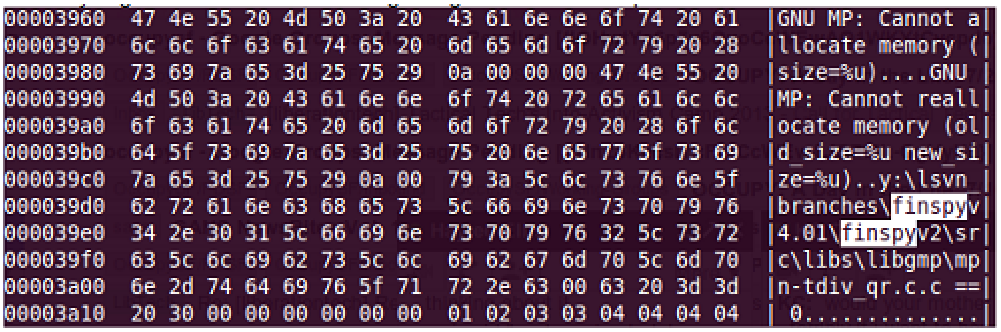
The email came attached with rar files, with innocuous titles such as "ArrestedSuspects.rar," and "MeetingXAgenda.rar." Inside each rar file were a collection of executable files masquerading as images and documents. The attacker used a strategy called RLO (Right to Left Override), which takes advantage of a built in system to display names right to left, like in Arabic or Hebrew. In this case, it allowed a file named "exe.Rajab1.jpg," to appear as a jpg, when it was really an exe file written in reverse.

Once executed, the file displays as image as promised, but also begins to execute commands on the system. It starts by copying itself to a folder on the drive, and running two processes, "driverw.sys" and "delete.bat." These processes start by using what is called "process hollowing," [11]which infects standard processes and uses them to disguise its own nefarious actions. In this case, FinFisher runs winlogon.exe, a legitimate windows process. However, before the first code is executed, FinFisher allocates the space where the legitimate code is stored, and replaces it with its own malicious code. The following image shows winlogon.exe after it has been infected by FinSpy. On the right, there exists a link to a

[10] CitizenLab "From Bahrain with Love: FinFisher's Spy Kit Exposed" July 2012 www.citizenlab.org

[11] CitizenLab "From Bahrain with Love: FinFisher's Spy Kit Exposed" July 2012 www.citizenlab.org

directory named finspy, which as an analysis of other infected processes shows, is a signature of the attack.[12]



```
00003960  47 4e 55 20 4d 50 3a 20  43 61 6e 6e 6f 74 20 61  |GNU MP: Cannot a|
00003970  6c 6c 6f 63 61 74 65 20  6d 65 6d 6f 72 79 20 28  |llocate memory (|
00003980  73 69 7a 65 3d 25 75 29  0a 00 00 00 47 4e 55 20  |size=%u)....GNU |
00003990  4d 50 3a 20 43 61 6e 6e  6f 74 20 72 65 61 6c 6c  |MP: Cannot reall|
000039a0  6f 63 61 74 65 20 6d 65  6d 6f 72 79 20 28 6f 6c  |ocate memory (ol|
000039b0  64 5f 73 69 7a 65 3d 25  75 20 6e 65 77 5f 73 69  |d_size=%u new_si|
000039c0  7a 65 3d 25 75 29 0a 00  79 3a 5c 6c 73 76 6e 5f  |ze=%u)..y:\lsvn_|
000039d0  62 72 61 6e 63 68 65 73  5c 66 69 6e 73 70 79 76  |branches\finspyv|
000039e0  34 2e 30 31 5c 66 69 6e  73 70 79 76 32 5c 73 72  |4.01\finspyv2\sr|
000039f0  63 5c 6c 69 62 73 5c 6c  69 62 67 6d 70 5c 6d 70  |c\libs\libgmp\mp|
00003a00  6e 2d 74 64 69 76 5f 71  72 2e 63 00 63 20 3d 3d  |n-tdiv_qr.c.c ==|
00003a10  20 30 00 00 00 00 00 00  01 02 03 03 04 04 04 04  | 0..............|
```

An analysis of svchost.exe shows that FinSpy has modified the boot sequence, with the following file appearing in the memory dump.

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

This allows FinSpy to persist, running every time the victim turns on his computer. So after the initial infection, FinSpy has already setup persistence, and hijacked many of Microsoft Windows most basic processes.

Application: Data Collection

When FinSpy or FinFisher is installed on a computer, it collects a wide range of data to export to its host server. This data is stored in a directory and encrypted before it is sent from the host computer. Files in this directory include “screenshots, keylogger data, audio from Skype calls, passwords” among many others. It creates and edits these files from within the winlogon.exe process, To obtain access to the victims online accounts, it attempts to locate the password store files for any web browsers installed on the system. It also writes to file screenshots of the desktop, of the file naming convention XXY1TTTTTTTT.dat, where X and

[12] ibid

Y are hexadecimal numbers, and T represents a unix timestamp. As I will show in the source code for Detekt, this naming convention for screenshots is one of the signatures by which FinFisher can be detected.

The data in the collection folder is encrypted before it is delivered to the host server, using AES-256-CBC, a symmetric key algorithm in wide use worldwide. Citizen Lab's analysis reveals that the algorithm uses the number stored in memory address 0x7ffe0014 to create its encryption keys. This memory address contains the lower order 4 bytes of the number of seconds since January 1st 1601. This produces a series of encryption keys that are predictable, because the Windows quantum clock is updated in a predictable fashion. In addition, any data is only partially encrypted. It only encrypts data that fits into one AES block, or 16 bytes. So any additional data is displayed in plaintext. These two properties allow the encrypted files to be displayed in full plaintext, reveal contact books, skype messages, and file transfer logs.

Application: Obfuscation

One of the primary reasons FinFisher is such a well sought after piece of software by governments and police departments around the world is that it is so hard to detect by conventional means. FinFisher is unrecognized by 40 of the top antivirus programs, and most victims don't realize their online behavior was being monitored until they are imprisoned and confronted with evidence taken from their computers.[13] The developers of the software went to great lengths to design the product such that it would be difficult to identify.

[13] WikiLeaks "SpyFiles4" Sept, 2014 www.wikileaks.org

The first method by which FinFisher hides its activities is a “virtualised packer.” This packer “converts the native x86 instructions of the malware into another custom language” chosen from 11 templates. At run-time, this new code is “interpreted by an obfuscated interpreter customized for that particular language.”[14] By using a virtualised packer, the software makes it harder for antivirus to analyze the malware, the crucial first step in responding to potential incidents.

The malware also uses techniques that prevent its code from being debugged. For example, it contains a line of code that exploits a problem in OllyDbg, a debugging software, that does not mask invalid floating point operation errors. By including a floating point with the value that crashes this system, FinSpy prevents this debugger from unpacking its code.

The final layer of obfuscation FinSpy uses is its ability to avoid detection by any major antivirus offering. It does this in a few specific ways, and tailors its efforts to the particular brand of AV software installed on the computer. FIrst, it calls ZwQuerySystemInformation, which returns a list of processes and modules running on the computer. It then walks this list looking for any AV software installed on the computer. It has included different injection solutions to infect each AV solution, and infects ZwQuerySystemInformation so that any other applications on the computer will not be able to see its own processes running.

[14] CitizenLab “From Bahrain with Love: FinFisher’s Spy Kit Exposed” July 2012 www.citizenlab.org

Application: Communication

In the particular case of the Bahraini activists, the program was found to be connecting to an IP address which belonged to Batelco, the primary telecommunications company in the country. The communications took place over the ports 22, 53, 80, 443, and 4111. The programs FinRelay and FinProxy are used worldwide to collect the data from victims computers, where there are eventually transferred to FinMaster, the final location of the data. These services are used to ensure the final destination and orchestrator of the attacks can remain anonymous.[15]

Detection: How to Defend Against FinSpy

The main action item for those who are concerned that they may be targeted by spyware such as FinSpy is to download a new tool called Detekt released by a group of human rights defenders including Privacy International, Amnesty International, and the Electronic Freedom Foundation. In the supplementary material attached, i will analyze how Detekt searches for the presence of FinSpy. This program is only the first step in the fight against surveillance technology. As more research is poured into exactly how to detect FinSpy, we will be able to better assist those in need overcome political repression. Unfortunately, Detekt is only a “tool of best effort,” as described by its founders.[16] A negative scan return from Detekt does not equal a clean bill of health, and

[15] WikiLeaks “SpyFiles4” Sept, 2014 ww.wikileaks.org

[16] Resist Surveillance “Detekt” https://resistsurveillance.org/

thus the program can only be used in the affirmative. Detekt attempts to verify the presence of FinSpy by checking for the presence of a few signature files on the infected system.

Conclusion: Security vs. Human Rights

In the absence of new government regulation to halt the spread of dangerous surveillance software like FinSpy, the ability to detect such software becomes all the more important. Gamma will not be the last company to operate in the growing surveillance technology industry, and protections must be put in place to protect human rights. Without adequate control over how this technology is exploited, it can be expected that more and more governments will turn to targeted online surveillance to track criminals and activists alike. Technology possesses an incredible potential to liberate people, as the use of facebook and twitter during the Arab Spring protests demonstrated. Unfortunately, repressive regimes also can harness the power of technology to crush freedom. The field of surveillance technology is still in its infancy, but it is important for the world community to step in now and ensure that the technology is used according to international standards for human rights, and not used to abuse power.

Citations:

1. Amnesty International "Detekt, new software tool in the 'cat and mouse' game against Big Brother November 2014 http://www.amnesty.org/en/news/detekt-new-software-tool-cat-and-mouse-game-against-big-brother-2014-11-21
2. United Nations "Universal Declaration of Human Rights" http://www.un.org/en/documents/udhr/
3. Electronic Frontier Foundation "Spy Tech Companies and Their Authoritatian Customers Part 1: FinFisher and Ameysys https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys
4. WikiLeaks "The SpyFiles 4" https://wikileaks.org/spyfiles4/customers.html
5. CitizenLab "From Bahrain With Love: FinFisher's SpyKit Exposed" https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/
6. BitDefender " Exported UK Surveillance Tech Under Tighter Control, FinFIsher License to Export Opens the Way" http://www.bitdefender.co.uk/security/exported-uk-surveillance-tech-under-tighter-control-finfisher-licence-to-export-opens-the-way.html
7. Bloomberg: Cyber Attacks on Activists Traced to FinFisher Spyware http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html
8. Resistence Surveillance "Detekt" https://resistsurveillance.org/