Pay No Attention to the Server Behind the Proxy

Mapping FinFisher's Continuing Proliferation

By Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune

OCTOBER 15, 2015
RESEARCH REPORT #64

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Suggested Citation

Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," Citizen Lab Research Report No. 64, University of Toronto, October 2015.

Acknowledgements

Special thanks to Citizen Lab colleagues Morgan Marquis-Boire and Claudio Guarnieri, as well as Ron Deibert and Masashi Crete-Nishihata. Special thanks to the Open Technology Fund. Thanks to Vern Paxson and Jason Passwaters.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

This post describes the results of Internet scanning we recently conducted to identify the users of FinFisher, a sophisticated and user-friendly spyware suite sold exclusively to governments. We devise a method for querying FinFisher's "anonymizing proxies" to unmask the true location of the spyware's master servers. Since the master servers are installed on the premises of FinFisher customers, tracing the servers allows us to identify which governments are likely using FinFisher. In some cases, we can trace the servers to specific entities inside a government by correlating our scan results with publicly available sources. Our results indicate 32 countries where at least one government entity is likely using the spyware suite, and we are further able to identify 10 entities by name. Despite the 2014 FinFisher breach, and subsequent disclosure of sensitive customer data, our scanning has detected more servers in more countries than ever before.

Executive Summary

FinFisher is a sophisticated computer spyware suite, written by Munich-based FinFisher GmbH, and sold exclusively to governments for intelligence and law enforcement purposes. Although marketed as a tool for fighting crime,[1] the spyware has been involved in a number of high-profile surveillance abuses. Between 2010 and 2012, Bahrain's government used FinFisher to monitor some of the country's top law firms, journalists, activists, and opposition political leaders.[2] Ethiopian dissidents in exile in the United Kingdom[3] and the United States[4] have also been infected with FinFisher spyware.

In 2012 and 2013, Citizen Lab researchers and collaborators,[5] published several reports analyzing FinFisher spyware, and conducted scanning that identified FinFisher command and control (C&C) servers in a number of countries. In our previous research, we were not yet able to differentiate between FinFisher *anonymizing proxies* and *master* servers, a distinction that we make in this work.

1 https://www.finfisher.com/FinFisher/index.html

2 https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

3 http://www.wired.co.uk/news/archive/2014-02/17/illegal-spying-ethiopian-refugee

4 https://www.eff.org/cases/kidane-v-ethiopia

5 See https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/, https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/, https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/, https://citizenlab.ca/2013/04/for-their-eyes-only-2/, https://community.rapid7.com/community/infosec/blog/2012/08/08/finfisher

When a government entity purchases FinFisher spyware, they receive a *FinSpy Master*—a C&C server that is installed on the entity's premises.[6] The entity may then set up *anonymizing proxies* (also referred to as "*proxies*" or "*FinSpy Relays*" in the FinFisher documentation), to obscure the location of their master. Infected computers communicate with the anonymizing proxy, which is "usually"[7] set up on a Virtual Private Server (VPS) provider in a third country. The proxy then forwards communications between a victim's computer and the Master server.

We first describe how we scanned the Internet for FinFisher servers and distinguished masters from proxies (**Part 1: Fishing for FinFisher**). We then outline our findings regarding 32 governments and 10 specific government entities that we believe are using FinFisher (**Part 2: Country Findings**). Finally, we highlight several cases that illuminate connections between different threat actors (**Part 3: A Deeper Analysis of Several Cases**), before concluding (**Conclusion**).

6 https://wikileaks.org/spyfiles4/documents/FinSpy-3.10-Specifications.doc

7 Id.

Part 1: Fishing for FinFisher

In this section, we describe our scans for FinFisher servers, and how we unmasked the true location of the master servers to identify governments using FinFisher.

Each FinFisher sample includes the address of one or more C&C servers that the spyware reports back to. These C&C servers are typically *FinSpy Relays*, which forward connections back and forth between a device infected with FinFisher, and a *FinSpy Master.* The purpose of the *FinSpy Relay* is explicitly to make it *"practically impossible"* (their emphasis) for a researcher to discover *"the location and country of the Headquarter [sic]".*[8]

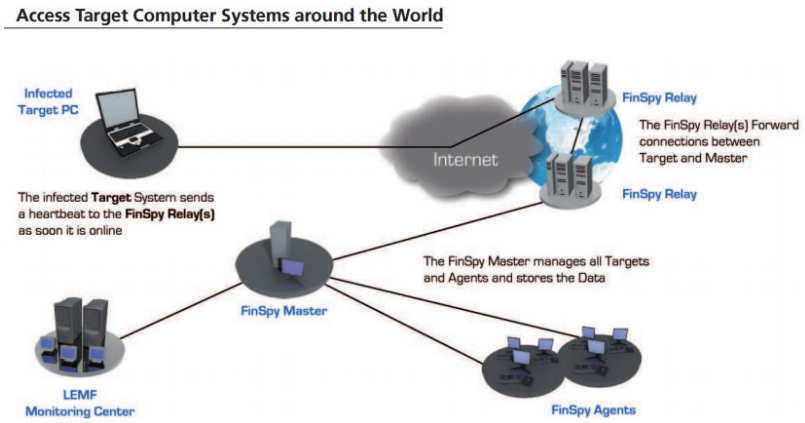

Figure 1: How targets infected with FinFisher communicate with the FinSpy Master via one or more FinSpy Relays.[9]

We employed *zmap*[10] to scan the entire IPv4 Internet (/0) several times since the end of December 2014 and throughout 2015, using a new FinFisher server fingerprint that we devised by analyzing FinFisher samples. Our scans yielded 135 servers matching our fingerprint, which we believe are a mix of FinSpy Masters and FinSpy Relays.

When one queries a FinFisher server, or types the server's address into a web browser, the server typically returns a *decoy page*. A decoy page is a page designed to disguise the fact that the server is a spyware server. We found some variation in the decoy pages used by FinFisher servers that we detected, though the bulk used either **www.google.com** or **www.yahoo.com**. Peculiarly, FinSpy Relays appear to return decoy pages fetched by their FinSpy Master, rather than directly fetching

8 Id.

9 https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

10 https://zmap.io/

the decoy pages themselves. **Thus, in many cases, the pages returned by the FinSpy Relays contain location data apparently about the FinSpy Master (e.g., certain Google and Yahoo pages embed the requester's IP address or localized weather), which can reveal the location of FinSpy Masters.**

Okay Google, What is my IP?

We noticed that when we issued a query like "What is my IP address?" to a Google-decoy FinFisher server, the server would respond with a different IP address. In the case below, a FinFisher server **206.190.159.xxx** (located in the United States) reported that its IP address was the Indonesian IP **112.78.143.xxx**, which matches a FinFisher server first detected in August 2012 by Claudio Guarnieri.[11] We hypothesize that 206.190.159.xxx is a FinFisher *proxy*, designed to obscure the location of the FinFisher *master*, which is at 112.78.143.xxx.

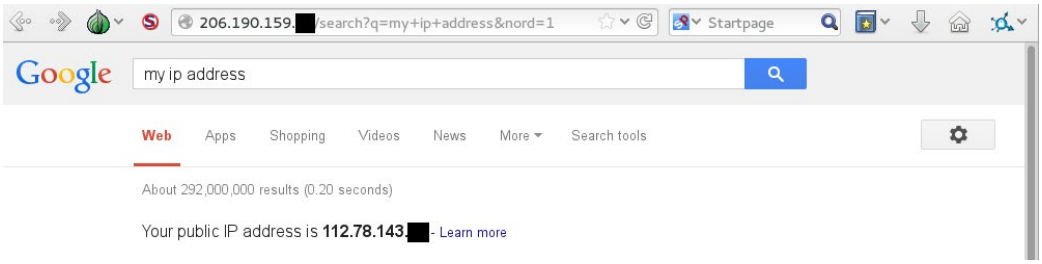

Figure 2: A FinFisher server in the US seems to be a proxy for a master in Indonesia.

Specifically, we sent queries of the form:

```
GET /search?q=my+ip+address&nord=1 HTTP/1.1
Host: [ip of server]
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:38.0) Gecko/20100101 Firefox/38.0
```

Figure 3: Queries we sent to Google-decoy FinFisher servers to reveal the IP address of the master.[12]

The fact that FinFisher proxies can apparently reveal the IP of the master is quite peculiar. We illustrate below how we believe a query like "What is my IP address?" is routed through FinSpy Relays to the FinSpy Master:

11 https://community.rapid7.com/community/infosec/blog/2012/08/08/finfisher

12 Google does not return the user's IP address unless a certain type of "User-Agent" header is included. In this example, we include a user agent used by the Tor Browser Bundle. The "nord=1" parameter turns off Google's SSL redirection.

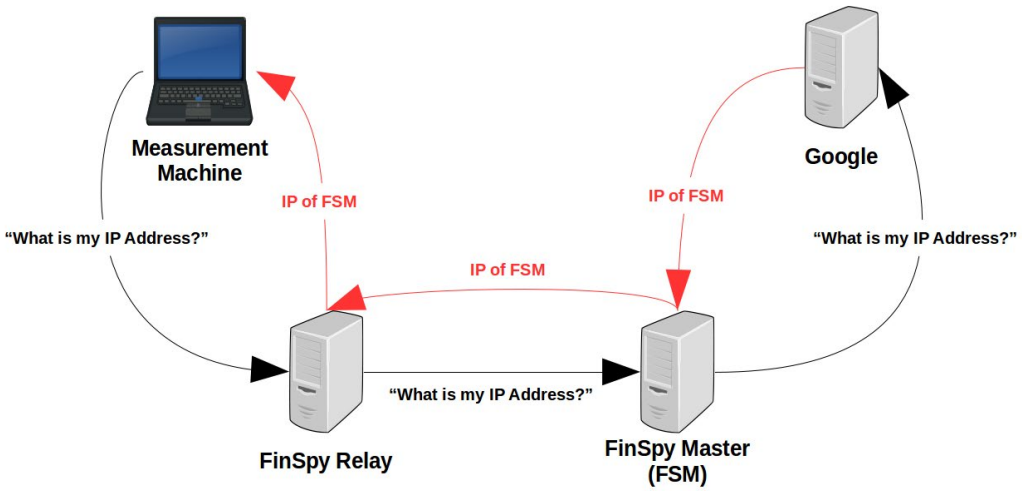

Figure 4: How we believe a "What is my IP address?" query is routed through FinSpy Relays to a FinSpy Master.

It appears that the "What is my IP Address?" query is delivered from our **Measurement Machine** by the **FinSpy Relay** to the **FinSpy Master**, and then submitted to **Google** by the **FinSpy Master**. Therefore, **Google** returns the IP address of the **FinSpy Master**, which is then sent back to the **Measurement Machine** via the **FinSpy Relay**.

How's the Weather in Caracas?

A significant number of FinFisher servers we detected used **www.yahoo.com** as their decoy page. While we were unable to devise a method to find the exact IP address of Yahoo-decoy FinFisher endpoints, we were still able to retrieve location information from Yahoo, by examining the *userLocation* object in the decoy page's source code. Yahoo utilizes a user's location to customize several elements of Yahoo's homepage, including weather and news.

Figure 5: Weather conditions in Caracas returned by a FinFisher server in Lithuania.

The userLocation object returned by 185.8.106.xxx (located in Lithuania) is shown below:

```
"userLocation":
   {"woeid":395269,
    "zip":"Caracas",
    "city":"Caracas",
    "state":"Distrito Federal",
    "country":"Venezuela",
    "countryCode":"VE",
    ...}
```

Figure 6: A FinFisher server in Lithuania seems to be a proxy for a master in Venezuela.

The userLocation object allows us to obtain city and country information for FinFisher endpoints, though we cannot determine their precise IP address. We issued a query similar to the following to each Yahoo-decoy FinFisher server to obtain a page with the userLocation object:

```
GET https://www.yahoo.com/ HTTP/1.1
Host: www.yahoo.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:38.0) Gecko/20100101 Firefox/38.0
```

Figure 7: Queries we sent to Yahoo-decoy FinFisher servers to reveal the location of the master.[13]

Since Yahoo, like Google, implements SSL redirection by default, we had to devise a method to talk to Yahoo in plain HTTP. While Google provides the "*nord=1"* URL parameter to avoid SSL redirection, Yahoo apparently does not have an analogous publicized solution. However, we found that by sending plain HTTP GET requests to the resource "https://www.yahoo.com/" we could communicate with www.yahoo.com in plain HTTP without triggering SSL redirection.

Other Decoys

While the majority of FinFisher servers we detected used either Google or Yahoo as a decoy page, we identified a number of other servers whose operators had apparently customized the decoy page to a different URL.

One server used the Italian news source **libero.it** as a decoy. We noted that libero.it sets the "Libero" cookie, which contains the IP address of the computer that visited the libero.it website. When accessing **185.8.106.xxx**, the Libero-decoy FinFisher server, the cookie was set to include the Italian IP **93.146.250.xxx**.[14] Servers that we

13 Yahoo does not return the userLocation object unless a certain type of "User-Agent" header is included. In some cases, we needed to substitute a country-specific version of Yahoo in the GET request (either **espanol.yahoo.com** or **maktoob.yahoo.com**).

14 We verified that the IP of our measurement machine was included in the Libero cookie when visiting the **libero.it** site directly.

traced to Macedonia used Macedonian newsmagazine **time.mk** as a decoy. Servers we traced to Taiwan used Taiwanese web portal **pchome.com.tw** as a decoy. We were unable to trace other servers which used file download site **filehippo.com** as a decoy. A handful of other untraceable servers returned custom HTML code as a decoy (e.g., a webpage with a META redirect to www.google.com).

General Comments

This design peculiarity is only the latest instance of fingerprintable anomalies in spyware decoy pages. FinFisher competitor Hacking Team formerly used decoy pages on its C&C server for Remote Control System (RCS), but apparently removed them[15] after our research revealed that anomalies in the decoy pages could be used to fingerprint RCS servers.[16] We have also previously used decoy pages to fingerprint FinFisher servers.[17] We believe that FinFisher or its clients may also be realizing that decoy pages are problematic, as we have observed fewer FinFisher servers returning decoy pages over time.

15 https://github.com/hackedteam/rcs-collector/commit/0a92297ff1cb52112be0a6ee6b8d398cf001ed1e

16 https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

17 See our previous fingerprints: https://github.com/citizenlab/spyware-scan/blob/master/ff/fingerprint-2.0.txt, https://github.com/citizenlab/spyware-scan/blob/master/ff/fingerprint-3.0.txt, https://github.com/citizenlab/spyware-scan/blob/master/ff/fingerprint-4.0.txt

Part 2: Country Findings

In this section, we provide a list of likely FinFisher government users identified by our scans, and also map out which FinSpy relays serve which FinSpy Masters.

Below, we identify 33 likely government users of FinFisher in 32 countries, based on the presence of a FinFisher master at an IP address in a country[18] or belonging to a specific government department.

Figure 8: Suspected FinFisher government users that were active at some point in 2015.

In presenting our scan results, we do not wish to disrupt or interfere with legitimately sanctioned investigations or other activities. Instead, we hope to ensure that citizens have the opportunity to hold their governments transparent and accountable. To this end, we identify government users, but redact certain details we have discovered about their infrastructure whose disclosure might interfere with legitimately sanctioned activities. Redacted details include the last octet of live IP addresses, and part of live domain names. **Appendix A** contains a full list of countries and servers.

Country	Specific entity if known
Angola	
Bangladesh	Directorate General of Forces Intelligence (DGFI)
Belgium	Federal Police

18 We assume that if a FinFisher master is located in a country, then an entity of that country's government is using the spyware. It is of course possible that government entities may be operating some surveillance from overseas sites. Though, we view this possibility as quite remote, given concerns about relying on foreign (and potentially untrusted) telecom infrastructure to operate surveillance infrastructure.

Country	Specific entity if known
Bosnia and Herzegovina	
Czech Republic	
Egypt	Technology Research Department (TRD)
Ethiopia	
Gabon	
Indonesia	National Encryption Body (Lembaga Sandi Negara)
	Unknown other entities
Italy	Unknown multiple entities
Jordan	
Kazakhstan	
Kenya	National Intelligence Service (NIS)
Lebanon	General Directorate of General Security
	Internal Security Forces (ISF)
Macedonia	
Malaysia	
Mexico	
Mongolia	Special State Security Department (SSSD)
Morocco	Conseil Superieur De La Defense Nationale (CSDN)
	Unknown other entities
Nigeria	Unknown multiple entities
Oman	
Paraguay	
Romania	
Saudi Arabia	
Serbia	Security Information Agency (BIA)
Slovenia	
Spain	
Taiwan	
Turkey	
Turkmenistan	
Venezuela	
South Africa	

The following is a list of countries where neither our previous research nor documents disclosed by Wikileaks[19] had previously found evidence of a FinFisher deployment: **Angola, Egypt, Gabon, Jordan, Kazakhstan, Kenya, Lebanon, Morocco, Oman, Paraguay, Saudi Arabia, Slovenia, Spain, Taiwan, Turkey, and Venezuela.**

19 https://wikileaks.org/hackingteam/emails/emailid/17309

In the diagram below, we map out FinFisher proxy networks: the FinSpy Relay servers we found, and the FinSpy Masters to which we linked them:

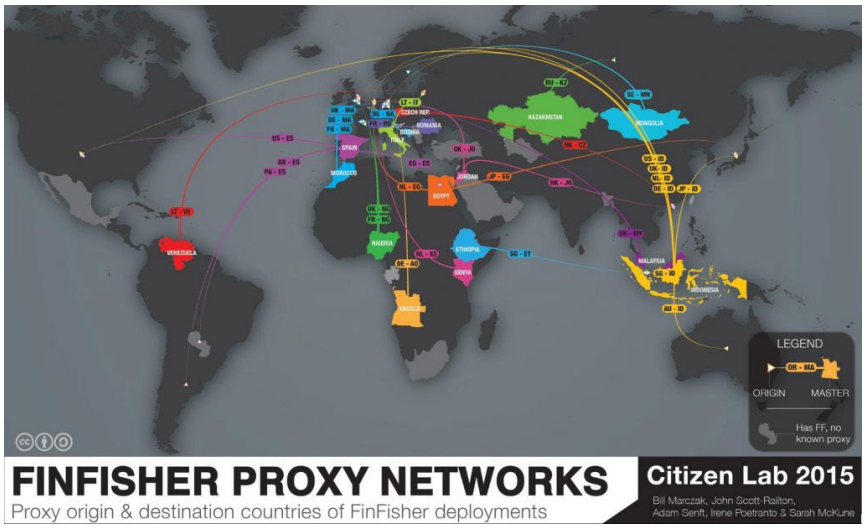

Figure 9: Links we established between FinSpy Relays and FinSpy Masters.

Given previous reports that observed weaknesses in certain cryptography that FinFisher uses to transmit information from an infected device to the FinSpy master,[20] locating FinFisher collection infrastructure in another country could potentially invoke concerns about "fourth party" collection, where a government collects data collected by another government's surveillance operation. We have also previously identified potential legal concerns regarding locating relays in other countries.[21]

Attribution to Specific Entities

We attributed some FinFisher Master servers to specific government entities by correlating our scan results with publicly available data, including emails from FinFisher's competitor Hacking Team. This section briefly describes how we identified these entities, and summarizes what is publicly known about their functions. While we do not provide a vignette for each country where we have identified FinFisher, we note that a number of countries have dubious or problematic histories of oversight of the security services.

20 See for example: http://2014.hack.lu/archive/2014/inside_spying_v1.4.pdf and https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-marczak.pdf

21 https://citizenlab.ca/2014/02/hacking-teams-us-nexus/

Bangladesh

Directorate General of Forces Intelligence (DGFI)

Our investigation uncovered a FinFisher server at an IP address in the same /30 as the mail server for Bangladesh's DGFI, **[redacted].dgfi.gov.bd**. Additionally, leaked Hacking Team emails claim that Bangladesh's DGFI is a FinFisher customer.[22]

Established in 1976, the Directorate General of Forces Intelligence (DGFI) is Bangladesh's military intelligence agency. The director of the agency holds the rank of Lieutenant General or Major General and directly reports to the Prime Minister.[23] In a report published in 2008, Human Rights Watch associated the DGFI with long-standing human rights violations (e.g., torture and extrajudicial killings) and the stifling of political opposition in the country.[24]

The US State Department has reported that the DGFI has previously conducted surveillance on citizens for their criticism of the government.[25] Leaked emails show that DGFI officials were engaged in discussions with FinFisher's competitor Hacking Team in June 2014.[26]

Belgium

Federal Police Service

Our investigation found a FinFisher server in a /28 assigned to Belgacom, denoted "SKY-5904592 / SOCC-2131136." This range of IP addresses also contained several servers returning SSL certificates issued by and to "Federal Police." Two IP addresses in this range were also pointed to by two subdomains of **raspol.be**, a domain name registered to "Massimo Moschettini / ISRD NTSU / Police Fédérale."

22 https://wikileaks.org/hackingteam/emails/emailid/547657

23 http://www.dgfi.gov.bd/index.php/about%20

24 https://www.hrw.org/report/2009/05/18/ignoring-executions-and-torture/impunity-bangladeshs-security-forces

25 http://www.state.gov/j/drl/rls/hrrpt/2013humanrightsreport/index.htm?year=2013&dlid=220388

26 https://wikileaks.org/hackingteam/emails/emailid/17309

Belgium's Federal Police Service was established in January 2001. The agency is headed by a General Commissioner who coordinates the work of five general directorates, including administrative police, judicial police, operational support, logistics, and human resources, as well as several departments that report directly to him/her.[27] Leaked Hacking Team emails have revealed the company's participation in a tender for "tactical interception of communications via computer systems" by the Belgian Federal Police.[28]

Serbia

Security Information Agency (BIA)

> Our investigation found a FinFisher server in the same /26 as **bia.gov.rs**, the website of Serbia's Security Information Agency (BIA). The server was also in the same /28 as a computer that identified itself to Shodan as "DPRODAN-PC".[29] According to the leaked Hacking Team emails, a person with the email dprodan@open.telekom.rs contacted Hacking Team in reference to a February 8, 2012 demo in Belgrade.[30] From February 7-9, 2012, Hacking Team was in Belgrade to give a demo to a potential client, Vladimir Djokic, who worked for the BIA according to his email address vladimirdj@bia.gov.rs.[31] Thus, we believe "dprodan" is also a BIA employee, and the FinFisher server we found belongs to the BIA.

Serbia's Security Information Agency (BIA) was created in 2002 by the Law on the Security Information Agency. BIA is a civil national security service and a part of the security-intelligence system of the Republic of Serbia.[32]

While the BIA is generally regarded as operating with appropriate oversight and as being free from major abuses, some elements of its electronic surveillance practices have been challenged. Prior to 2014, the Law on the Security Information Agency was considered to be not in compliance with the constitution. In 2012, a constitutional court struck down several provisions of the Law on the Security Information Agency, ruling that Articles 13, 14 and 15 of the Law, which govern the

27 http://www.police.ac.be/menu_58.htm

28 https://twitter.com/wikileaks/status/620025057650319360/photo/1

29 https://www.shodan.io/host/195.178.51.251

30 https://wikileaks.org/hackingteam/emails/emailid/765057

31 https://wikileaks.org/hackingteam/emails/emailid/761837

32 http://www.bia.gov.rs/eng/o-agenciji/zakon-o-bia.html

wiretapping of private communications, were unconstitutional.[33] The court ruled that these Articles were "not formulated clearly and precisely enough" and that citizens are "thus prevented from ascertaining which legal rule will be applied in the given circumstances and are thus deprived of the possibility to protect themselves from inadmissible restrictions of their right or arbitrary interference in their right to respect of their private life and correspondence".[34] Further, measures related to the ability of the BIA's Director to authorize wiretapping in some circumstances without a court order were also challenged.[35] The court delayed its decision in order to give legislators the opportunity to revise the offending Articles in the Law.[36] The amendments to the Law were adopted in June 2014.[37] While acknowledged as a positive step, these amendments have been criticized as remaining "insufficient to fully democratize surveillance that is carried out by the BIA".[38]

Leaked emails indicate that members of the Security Information Agency and the Ministry of Defense engaged in purchase negotiations with FinFisher's competitor Hacking Team.[39]

Egypt

Technology Research Department

> We found a FinFisher server at IP address 62.114.252.xxx. We also found an email in the leaked Hacking Team emails that, according to the headers, was sent from the same IP address.[40] The email was sent by Hacking Team employee Davide Romualdi on June 25, 2015, when he was scheduled to be performing delivery[41] in Egypt for Hacking Team customer TREVOR, identified as the TRD[42] (Technology Research Department).[43] Thus, we

33 http://www.bgcentar.org.rs/bgcentar/eng-lat/wp-content/uploads/2014/04/Human-Rights-in-Serbia-2013.pdf

34 http://www.bgcentar.org.rs/bgcentar/eng-lat/wp-content/uploads/2014/04/Human-Rights-in-Serbia-2013.pdf

35 http://ceas-serbia.org/root/images/CEAS_Plan_-_Total_Makeover.pdf

36 http://www.bgcentar.org.rs/bgcentar/eng-lat/wp-content/uploads/2015/03/Human-Rights-in-Serbia-2014.pdf

37 http://www.infobalkans.com/2014/06/25/serbian-government-adopts-amendments-bia-law

38 http://ceas-serbia.org/root/images/CEAS_Analysis_of_the_Law_on_Amendments_of_the_Law_on_the_Security_Intelligence_Agency.pdf

39 http://labs.rs/en/hacking-team-the-italian-job-of-serbian-security-services/

40 https://wikileaks.org/hackingteam/emails/emailid/1081335

41 https://wikileaks.org/hackingteam/emails/emailid/1030236

42 https://wikileaks.org/hackingteam/emails/emailid/14684

43 https://wikileaks.org/hackingteam/emails/emailid/602607

believe the email was sent from the premises of the TRD, and the IP address 62.114.252.xxx belongs to the TRD.

Egypt's troubling human rights situation has continued to deteriorate under President Abdel Fattah al-Sisi. In recent years, cases of mass arrests, significant violence against protesters and due process violations have increased.[44] Numerous Egyptian security agencies are permitted to conduct electronic surveillance, frequently with limited court oversight. In somes, personal data improperly collected from civil society actors has led to their arrest and imprisonment.[45] While there is limited open source information available about the activities of the Technology Research Department, we closely examine a malware campaign linked to TRD infrastructure in **Part 3** of this report.

Indonesia

National Encryption Body (Lembaga Sandi Negara)

Two of the FinFisher servers we found in Indonesia were in the same /28. We found an IP address in this same /28 included in the headers of an email sent by a Hacking Team employee[46] while he was in Indonesia[47] performing a demo for the National Encryption Body. The email was sent at 12:39 PM Jakarta time on February 6, 2013, and a meeting at the agency was set for 10:00 AM on the same day.[48] Thus, it seems probable that the email was sent from the premises of the National Encryption Body, and that the two FinFisher servers belong to the same organization.

The National Encryption Body is an agency headed by a director, who has the same stature as a minister and reports directly to the President. In a recent interview, the Body's current director, Major General Djoko Setyadi, describes the agency's responsibilities as, among others, securing state secrets and decrypting/decoding communication from would-be terrorists.[49]

44 https://www.hrw.org/world-report/2015/country-chapters/egypt

45 https://www.privacyinternational.org/sites/default/files/UPR_Egypt.pdf

46 https://wikileaks.org/hackingteam/emails/emailid/565854

47 https://wikileaks.org/hackingteam/emails/emailid/575806

48 https://wikileaks.org/hackingteam/emails/emailid/601732

49 http://news.detik.com/wawancara/2212177/lembaga-sandi-negara-hi-tech-dan-misterius

The threat of terrorism is a concern for Indonesia. Several bombing incidents have occurred in the country, including two Western hotels in the capital city of Jakarta in 2009. As the world's largest Muslim-majority country, the emergence of the Islamic State of Iraq and the Levant (ISIL or ISIS) has also resulted in concerns that their militant ideology will gain ground. It is believed that as many as 200 Indonesian citizens have headed to Syria to fight with ISIS.[50] Challenges from restive regions like Papua and Central Sulawesi are also ongoing. There are fears that the fight against these threats may be used as justification to perpetrate human rights abuses, such as to target others for their religious or political beliefs and to kill suspected militants unlawfully.

In 2013 Citizen Lab report, we identified at least twelve laws, two government regulations, and two ministerial regulations that govern wiretapping and interception in Indonesia. Although wiretapping and interception are helpful, and sometimes even necessary to expose crimes such as terrorism, drug trafficking and corruption, the lack of comprehensive legislation regulating their use in Indonesia means that there is an increased risk for misuse and privacy violations.[51]

Kenya

National Intelligence Service

> We found a FinFisher server in a range of IP addresses registered to a Kenyan user named “National Security Intelligence.” Kenya's National Intelligence Service (NIS) was formerly known as the National Security Intelligence Service (NSIS).

Kenya’s NSIS replaced the former Directorate of Security Intelligence (DSI), commonly known as the "Special Branch".[52] The NIS is known as one of Kenya’s security institutions with the biggest budgetary allocation—along with the Kenya National Defence Forces and the National Police Service—and considered to be among the country’s critical security organs in the new constitution.[53] In 2014, Human Rights Watch named the NIS, as well as the Anti-Terrorism Police Unit and

50 http://www.theguardian.com/world/2015/mar/11/indonesian-jihadis-could-be-galvanised-return-isis-fighters-analyst

51 https://citizenlab.ca/2013/10/igf-2013-exploring-communications-surveillance-indonesia/

52 https://wikileaks.org/gifiles/docs/51/5109873_-os-kenya-kenyan-intelligence-service-changes-name-boosts.html

53 http://www.standardmedia.co.ke/article/2000059031/nsis-and-police-boost-kenya-s-spy-networks?articleID=2000059031&story_title=nsis-and-police-boost-kenya-s-spy-networks&pageNo=3

other Kenyan intelligence agencies, as being implicated in abuses including torture, disappearances, and extrajudicial killings.[54]

The powers of the NIS were expanded significantly in December 2014 when the Parliament of Kenya rushed to pass the controversial Security Laws (Amendment) Bill.[55] The amendments came following a series of deadly terrorist attacks by the militant group al-Shabab, including the 2013 killing of 67 people at the Westgate shopping mall in Nairobi.[56] This bill expanded the powers of the NIS to monitor communications without a warrant, as well as expanding their powers to search and seize private property.[57] Article 62 of the amended bill authorized NIS agents to "do anything necessary to preserve national security" and to detain individuals on simply the suspicion of engaging in acts which pose a threat to national security.[58] Section 66 of the bill amended the National Intelligence Services Act, permitting the Director General of the NIS to monitor communications or "obtain any information, material, record, document or thing" in order to protect national security, without court oversight, leading rights organization Article 19 to argue that the amendment "effectively [gives] *carte blanche* to the Director-General to order mass surveillance of online communications".[59] While a court ruling in February 2015 struck down some provisions of the amendment, the provisions enhancing the powers of the NIS remained.[60]

Lebanon

General Directorate of General Security

> We found a FinFisher server in a range of IP addresses registered to a Lebanese user named "General_Security." We assume that "General_Security" is a reference to the General Directorate of General Security.

Lebanon's General Directorate of General Security was established in 1921 under

54 https://www.hrw.org/world-report/2015/country-chapters/kenya

55 http://www.bloomberg.com/news/articles/2014-12-11/kenya-mps-debate-tough-security-laws-criticized-by-opposition

56 http://www.bbc.com/news/world-africa-30592083

57 https://www.fidh.org/International-Federation-for-Human-Rights/Africa/kenya/16696-kenya-the-security-laws-amendment-act-must-be-repealed

58 https://www.hrw.org/news/2014/12/13/kenya-security-bill-tramples-basic-rights

59 https://www.article19.org/resources.php/resource/37800/en/kenya:-concerns-with-security-laws-(amendment)-bill

60 https://www.article19.org/resources.php/resource/37866/en/kenya:-high-court-ruling-on-security-amendment-act-a-victory-for-free-speech

Decree No. 1061.[61] The functions of the General Security include collecting and gathering intelligence, monitoring the media, and issuing passports and travel documents to Lebanese citizens.[62] The organization is categorized as a general directorate under the supervision of the Ministry of Internal Affairs.[63]

Although Lebanon has legislation (Law No. 140) which establishes safeguards and oversight protecting electronic communications from unlawful surveillance, there is a systemic practice of this law being ignored.[64] Privacy International has criticized the surveillance practices of Lebanon's intelligence agencies, suggesting that the agencies, including the General Directorate of General Security, operate without sufficient independent oversight, and that a lack of trust between different agencies leads the groups to operate their own operations out of view of the Ministry of the Interior.[65] Controversies surrounding government surveillance practices have become particularly salient in the wake of several recent high-profile assassinations, including the 2005 killing of Prime Minister Rafik Hariri. Organizations investigating the assassinations have had "unregulated access to the data of private citizens", including mobile phone records, which raises privacy concerns.[66]

Internal Security Forces

> We found a FinFisher server at a Lebanese IP address that was formerly pointed to by what was apparently a mail server with domain "[redacted].intelligence.isf.gov.lb" in 2012. We assume that the IP still belongs to the Internal Security Forces (ISF).

The Internal Security Forces (ISF) are the national police and security force of Lebanon. The ISF's creation was mandated by Decree 138 in 1959.[67] Throughout its history, the ISF has had a troubled record of human rights abuses, in spite of recent efforts to promote proper conduct within the organization. In consultation with the UN Human Rights Office, the ISF adopted a January 2012 code of conduct designed to ensure the forces' operations guaranteed respect for human rights and public freedoms, including "refraining from resorting to torture, cruel, inhumane

61 http://www.general-security.gov.lb/About-GS/Historical-overview.aspx

62 http://www.general-security.gov.lb/About-GS/functions.aspx

63 http://www.general-security.gov.lb/About-GS/sub1.aspx

64 https://www.privacyinternational.org/node/586

65 https://www.privacyinternational.org/sites/default/files/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf

66 https://www.privacyinternational.org/sites/default/files/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf

67 http://www.isf.gov.lb/arabic/download/isf-hist-en.pdf

and degrading treatment".[68] However, a number of incidents in recent years have called into questions the effectiveness of this code of conduct.

An extensive Human Rights Watch report in 2013 detailed dozens of instances of vulnerable individuals subject to physical abuse, torture and sexual assault at the hands of ISF officials.[69] In June 2015, five ISF officers were arrested after videos released on social media showed the officers beating prisoners.[70] The ISF and other state agencies have summoned and questioned bloggers, journalists, and activists over social media and blog posts critical of politicians.[71]

The organization also has a history of overreach in the collection of Lebanese citizens' private user data. In 2012, it was reported that the ISF had requested that the Ministry of Telecommunications turn over the content of all SMS text messages sent over a two month span for all users in Lebanon, followed later by a request for Lebanese users' login credentials for BlackBerry Messenger and Facebook.[72] The request was made following the assassination of the ISF's Information Branch head Wissam al-Hassan, and was rejected by the Ministry.[73]

Morocco

Conseil Superieur De La Defense Nationale (CSDN) / Supreme Council of National Defense

> We found a FinFisher server in a range of IP addresses registered to a Moroccan user named "Conseil Superieur De La Defense Nationale." We assume that this is a reference to the eponymous agency.

There is limited open source information available about the activities of the CSDN. Leaked Hacking Team emails indicate that the CSDN -- among other Moroccan Government agencies -- was a customer of FinFisher's competitor Hacking Team.

In 2012, spyware from Hacking Team was used against Mamfakinch, an award-

68 http://www.ohchr.org/EN/NewsEvents/Pages/ACodeofConducttohelpprotectHRLebanon.aspx

69 https://www.hrw.org/report/2013/06/26/its-part-job/ill-treatment-and-torture-vulnerable-groups-lebanese-police-stations

70 https://www.hrw.org/news/2015/06/26/lebanon-monitor-detention-combat-torture

71 http://www.state.gov/documents/organization/220575.pdf

72 https://www.eff.org/deeplinks/2012/12/lebanese-security-agency-user-data-request-sparks-controversy

73 http://www.mpt.gov.lb/index.php/en/about-mpt-2/mpt-in-press/118-the-ministry-of-communications-will-not-implement-any-data-request-if-it-touched-the-freedoms-of-the-lebanese-and-represented-an-assault-on-their-privacy

winning group of Moroccan citizen journalists.[74] Privacy International released a report detailing the impact of surveillance on the group, as well as other political activists and journalists.[75]

Mongolia

State Special Security Department (SSSD)

> We found a FinFisher server at a Mongolian IP address in the same /28 as an IP address pointed to by the domain "td.sssd.mn." We believe that "SSSD" is a reference to the Mongolian agency of the same name. We also found what appears to be a test or demonstration FinFisher sample, whose bait content includes emails apparently between Gamma Group and Mongolia's SSSD, discussing a visit by Gamma personnel to Mongolia.

There is limited open source information available about the SSSD; however, leaked emails from the spyware firm Hacking Team indicate that in 2012 the company was in contact with members of the SSSD.[76] Additional leaked emails from 2013 indicate that Hacking Team scheduled a product demonstration with the SSSD in April 2013.[77]

74 http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html

75 https://privacyinternational.org/?q=node/554

76 https://wikileaks.org/hackingteam/emails/emailid/594340

77 https://wikileaks.org/hackingteam/emails/emailid/590093

Part 3: A Deeper Analysis of Several Cases

The following section provides additional details for several countries

Egypt: Use of FinFisher illuminates connections between different groups

We noted an interesting connection between Egypt's Technology Research Department (TRD) and two other malware groups in the region: MOLERATS, and an as-yet uncharacterized group. We have previously observed both groups targeting UAE-based activists.

MOLERATS Attacks with FinFisher

We found an Egypt FinFisher sample, Egyptian_army.rar, hosted on **google.wwwhost.biz**.

```
SHA256:   1610fc805f980f5c70cec8e138ba800b01ebc86919f42b375cfb161ce6365a48
Filename: Egyptian_army.rar
```

Extracting the .rar file yields an .exe file.

```
SHA256:   94abf6df38f26530da2864d80e1a0b7cdfce63fd27b142993b89c52b3cee0389
Filename: صور ذبح الكساسبة على يد داعش بعد انقضاء المهلة.exe
```

The name of the .exe file promises pictures of Jordanian Air Force pilot burned alive by ISIS, a popular news story at the time.

We suspect that the domain name **google.wwwhost.biz** is linked to MOLERATS, a threat actor active in the Middle East region that appears to engage in politically motivated targeting. We describe the link below:

- **google.wwwhost.biz** had IP address **200.74.241.111** at the same time as **info.dynamic-dns.net**, which also had IP address **192.161.48.59**, shared with **update.ciscofreak.com**, which also had IP address **162.220.246.117**. This IP address is linked to several known MOLERATS domains, like **natco{1,2,3,4,5}.no-ip.net**,[78] and **uae.kim**.[79]
- **google.wwwhost.biz** also hosted two DarkComet samples, which communicated with **r.ddns.me**, which shared IP address **198.105.125.158** with **a.ddns.me**, which shared IP address **23.229.3.37** with MOLERATS

78 http://cyber-peace.org/wp-content/uploads/2014/01/Cyberattack_against_Israeli_and_Palestinian_targets.pdf

79 https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html

domain **test.cable-modem.org**.[80]

- **google.wwwhost.biz** also hosted a GMail phishing page, 64c1ef8e0923bf44aaa96caeb28a6c11, also hosted by **googlecombq6xx.ddns.net**, which shared IP address **131.72.136.28** with **tvnew.otzo.com**, which shared IP address **172.227.95.162** with several known MOLERATS domains, like **natco{1,2,3,4}.no-ip.net**,[81] and **uae.kim**.[82]
- **google.wwwhost.biz** served a Hotmail phishing page, 57ab5f60198d311226cdc246598729ea, also served by **google.com.r3irv2ykn0qnd7vr7sqv7kg2qho3ab5tngl5avxi5iimz1jxw9pa9.uae.kim; uae.kim** is a known MOLERATS domain.[83]

A significant portion of MOLERATS bait content we have observed indicates targeting of Israel and "political Islam" groups like Hamas. This MOLERATS activity could be accounted for by any number of intelligence agencies active in the region, or a Palestinian faction, but it is also possible that MOLERATS is a multi-faceted group with several interests and/or clients.

That MOLERATS apparently used spyware linked to the TRD suggests a possible connection between the TRD and MOLERATS.

The Curious Case of the Shared Exploit

We identified the following Word document uploaded to VirusTotal:

```
SHA256:   22deea26981bc6183ac3945da8274111e7fd7a35fbb6da601348cc6d66240114
Filename: تقرير سري للغاية.doc
```

The document, whose name translates to "A Highly Classifed Report" downloads a FinFisher sample from **http://workingulf.net/DFServ.exe**.

```
SHA256:   e2ecf89a49c125e0b4292645a41b5e97c0f7bf15d418faeac0d592205f083119
Filename: DFServ.exe
```

The sample communicates with 50.31.252.xxx and 95.170.82.xxx, which are proxies for 62.114.252.xxx, the FinFisher Master we associated with Egypt's TRD. The domain workingulf.net appears to be connected to the TRD, because it is linked to

80 http://cyber-peace.org/wp-content/uploads/2014/01/Cyberattack_against_Israeli_and_Palestinian_targets.pdf

81 http://cyber-peace.org/wp-content/uploads/2014/01/Cyberattack_against_Israeli_and_Palestinian_targets.pdf

82 https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html

83 https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html

a cluster of other domains, several of which were used to distribute TRD FinFisher samples.

We developed a fingerprint for the exploit, based on the presence of a 1.1MB binary embedded in the Word Document. A week later, we identified another instance of this same exploit (the binary was the same).

```
SHA256:   d759dcbebee18a65fda434ba1da5d348c16d9d3775fe1652a1dacf983ffc93b8
Filename: المستجدات.doc
```

This instance downloaded spyware from **http://wp.piedslibres.com/wp/wp-includes/js/Next.scr**, which appeared to be a hacked WordPress site.

```
SHA256:   08b32da8995ae094bfb703d7d975c3816cf04c075c32281e51158164d76cd655
Filename: Next.scr
```

Next.scr is a bespoke malware that exfiltrates system information and files via email. The malware logs into an email account on the C&C server via SMTP, and sends mail to another account on the same server. We have seen C&Cs including: **pal4u.net, pal2me.net,** and **shop8d.net**. All of the domains have similar registrant information, indicating the work of a single group.

The group appears to be based in Palestine. The use of a shared exploit suggests some link between the TRD and this group.

FinFly Web in the Wild

We traced **workingulf.net**, to a number of other domain names, including **news-youm7.com** (see **Figure 10** below).

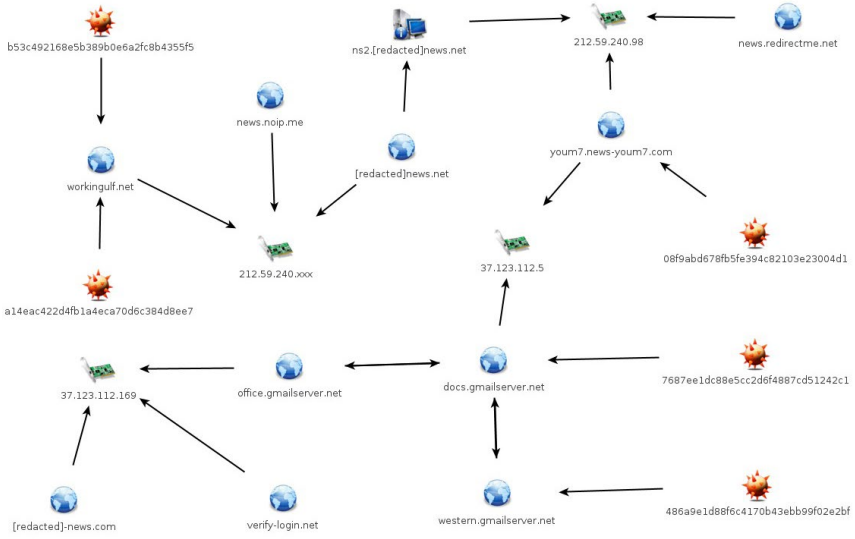

Figure 10: Domain names and IP addresses that we believe are associated with Egypt's TRD. We redact only live domains and IP addresses, and show full details for inactive ones.

We found a FinFly Web sample at **http://videos.news-youm7.com/youm7/videos/5671264.html**. FinFly Web is a FinFisher product that allows customers to create a website to infect targets with spyware. We identified the sample as FinFly Web given substantial similarity with leaked FinFly Web code.[84]

Figure 11: The FinFly Web page, asking users to install Adobe Reader XI. The download link points to a FinFisher spyware sample.

The FinFly Web page appears to have a number of deficiencies. The attacker appears to have copied a page from the website of Egyptian newspaper Youm7, which appears in the background of the Adobe Reader popup. The attacker apparently did not notice that the paths to the CSS resources are relative. Thus, the attack page tries to fetch CSS stylesheets and images from the attack site, rather than the legitimate page. Since the attacker neither copied these resources to the attack site, nor changed the relative paths to point to the legitimate site, the attack page looks malformatted. The attacker made the same mistake with the news ticker IFRAME, resulting in the "Not Found" message in the background. Also, the attacker entitled the page "Video: Islamic State Enters Egypt," but created a popup to install Adobe Reader, which is Adobe's product for viewing PDF files. It is likely that the attacker instead wanted to create a popup to install Adobe Flash, a plugin for viewing web videos. Additionally, the download link points to a .rar file,[85] which is suspicious as Adobe does not distribute its products in .rar files. Finally, the .exe inside the .rar file is not melded with the Adobe Reader setup program, so a victim who executes the file may become suspicious when no Adobe setup program runs.

84 https://github.com/FinFisher/FinFly-Web/blob/master/static_v2/jack.js

85 http://youm7.news-youm7.com/youm7/videos/acrobat-reader.rar

Italy: Shift from Hacking Team to FinFisher?

We identified one IP address in Italy (**2.228.65.xxx**) which served as a FinFisher server from 2014 to present. Earlier in 2014, and before our publication of our report on Hacking Team, the same IP address instead matched our fingerprint for Hacking Team spyware servers. This might indicate an Italian government agency switching from Hacking Team to FinFisher.

Oman: Eagle Eye Digital Solutions LLC

We found a FinFisher server running on IP address **37.139.27.xxx**, which is pointed to by two subdomains of **to70.org**, a domain name associated with an Omani company called "Eagle Eye Digital Solutions LLC" through historical WHOIS. The domain is currently registered to "Omantel," the largest telecom in Oman. Eagle Eye Digital Solutions LLC was founded by, and is run by, Warith Al-Maawali.[86] Leaked emails describe Warith as part of Oman's Ministry of Interior, as well as a reseller of FinFisher products.[87] Other sites apparently run by Eagle Eye include a major Omani online forum, "oman0.net." Eagle Eye founder Warith Al Maawali says the forum is *"one of the most active sites with the largest user-base in Oman."*

An archived version of Eagle Eye's website on the Wayback Machine showed Elaman GmbH as one of their partners, and "Security Organizations" as their clients. Elaman is known to be a reseller of FinFisher products.[88]

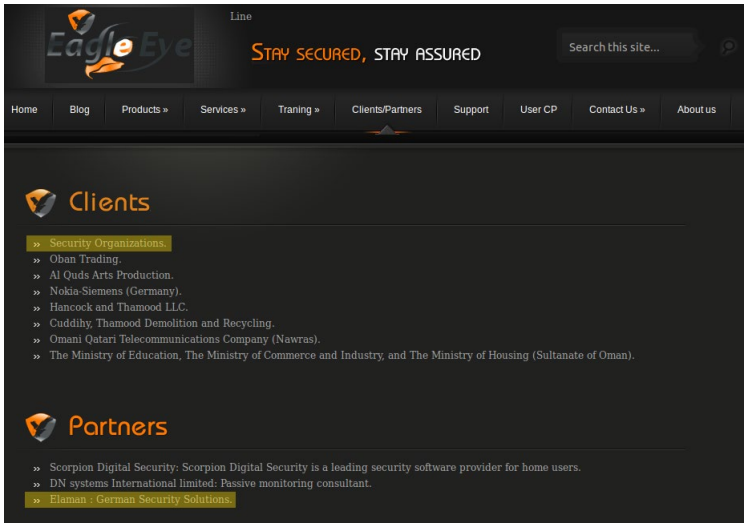

Figure 12: Old version of Eagle Eye's website showing FinFisher reseller Elaman as a partner, and "Security Organizations" as among the firm's clients.

86 https://www.linkedin.com/in/warith1977

87 https://wikileaks.org/hackingteam/emails/emailid/601907

88 https://surveillance.rsf.org/en/gamma-international/

Conclusion

In this report we provided the first update on Citizen Lab's previous FinFisher scanning work since a widely discussed 2014 hack of FinFisher. Despite the disclosure of sensitive customer data in that hack,[89] and the potential customer concerns this might cause, our latest scans have detected FinFisher servers in more countries than any previous round of scanning.

FinFisher is still being used by a number of previously identified government clients, including Ethiopia, which is the defendant in an ongoing lawsuit over previous FinFisher use.[90] We have also identified newly identified suspected customers, including: Angola, Egypt, Gabon, Jordan, Kazakhstan, Kenya, Lebanon, Morocco, Oman, Paraguay, Saudi Arabia, Slovenia, Spain, Taiwan, Turkey, and Venezuela.

While we may not be detecting all FinFisher installations, this report's methods improved on both our ability to detect installations, and to attribute FinFisher servers to specific governmental customers, whom we named. A key goal of this research is to provide a resource to those working on policy and research in this space. We also believe this kind of reporting is essential to help ensure that citizens have the opportunity to hold their governments accountable. To this end, we identify government users, but redact certain details about live infrastructure (like removing the last octet of IP addresses), whose disclosure might interfere with legitimately sanctioned activities.

The Global Intrusion Software Market: Difficult to Study, Tricky to Regulate

The market for intrusion software like FinFisher is challenging to track because the key players, from government customers to software developers, have a strong interest in keeping transactions private. However, several years of research, reporting, and revelations have made it clear that a growing list of countries have acquired, or are seeking these tools.

As customer lists grow, so should concern over the documented abuse potential of intrusion software. Some governments clearly believe that it can be used, with proper oversight, in the service of legitimate criminal investigations and intelligence

89 https://wikileaks.org/spyfiles4/customers.html

90 https://www.eff.org/cases/kidane-v-ethiopia

gathering. However, there are also well documented cases in which government customers have abused intrusion software to compromise political opponents within their borders, and overseas.

The current market seems to bypass some historic limits on the spread of advanced technical intrusion capabilities. Lack of a strong Science, Technology, Engineering and Mathematics (STEM) education, or absence of long term investment in research and development pipelines, are no longer impediments to obtaining computer exploitation and intrusion capabilities. These tools are now available for purchase by any government. Certainly, lack of development in STEM should not preclude a country from having access to sophisticated investigative tools. Indeed, an under-resourced state is likely to face security challenges that are just as serious as a more developed one.

However, it can be difficult even for democratic governments with a strong rule of law to oversee secret investigative capabilities like intrusion software. These tools are likely to be acquired and used by divisions that are professionally discreet in their budgeting and information sharing. The information they generate may also have its origins deliberately disguised before being shared with other departments or agencies. Intrusion software presents a challenge for accountability in any country, and the oversight authorities in under-resourced countries facing domestic or international security threats may be particularly ill-equipped in expertise and political clout, to identify or act on signs of misuse.

Previous research has shown that FinFisher has been used to target regime opponents in several cases. Notably, FinFisher has been used to hack Ethiopian and Bahraini democracy activists and opposition political figures. Meanwhile, research and revelations about Hacking Team's Remote Control System (RCS), a competitor product, have also made it clear that some government customers used these tools to target their political opponents, rather than security threats to their citizens.

Despite the well documented potential for abuse, the companies who develop and market these capabilities are reluctant and ill-equipped to conduct rigorous due diligence about potential customers, as recent revelations about Hacking Team have made clear.

The Wassenaar Arrangement, which regulates the export of weapons, as well as "dual use" technologies, was amended in 2013 to include items related to intrusion software, like FinFisher and Hacking Team's RCS. Now, as participants

like the European Union have undertaken their own implementations (or are still developing theirs as in the case of the United States), it remains to be seen whether or not this will lead to greater transparency and control, and what impact, if any, it will have on abusive surveillance.

We hope that continued evidence-based research of this sort will contribute to greater overall transparency about this market, and provide much-needed points of reference for policy making and tracking the impact of regulatory efforts.

Appendix A: List of FinFisher Servers

Server	FinSpy Master IP	Master Country	Date
41.63.169.xxx	41.63.169.xxx	Angola	12/2014
176.67.169.xxx	41.63.169.xxx	Angola	12/2014
81.246.44.xxx	81.246.44.xxx	Belgium	1/2015
78.46.172.xxx	80.65.75.xxx	Bosnia and Herzegovina	12/2014
180.235.133.xxx	80.95.253.xxx	Czech Republic	12/2014
50.31.252.xxx	62.114.252.xxx	Egypt	12/2014
95.170.82.xxx	62.114.252.xxx	Egypt	12/2014
197.156.66.xxx		Ethiopia	1/2015
206.190.159.xxx		Ethiopia	2/2015
197.231.66.xxx		Gabon	12/2014
176.67.169.xxx	118.97.103.xxx	Indonesia	12/2014
182.253.201.xxx	182.253.201.xxx	Indonesia	12/2014
50.31.240.xxx	112.78.143.xxx	Indonesia	12/2014
50.31.255.xxx	103.28.56.xxx	Indonesia	12/2014
46.23.72.xxx	118.97.103.xxx	Indonesia	12/2014
206.190.159.xxx	103.28.56.xxx	Indonesia	12/2014
83.170.112.xxx	118.97.103.xxx	Indonesia	12/2014
206.217.196.xxx	202.182.52.xxx	Indonesia	12/2014
216.119.149.xxx	118.97.103.xxx	Indonesia	12/2014
182.253.201.xxx	182.253.201.xxx	Indonesia	12/2014
103.28.57.xxx	103.28.57.xxx	Indonesia	12/2014
206.190.159.xxx	112.78.143.xxx	Indonesia	2/2015
182.253.201.xxx	182.253.201.xxx	Indonesia	3/2015
182.54.232.xxx	180.250.74.xxx	Indonesia	3/2015
2.228.65.xxx		Italy	12/2014
185.8.106.xxx	93.146.250.xxx	Italy	12/2014

Server	FinSpy Master IP	Master Country	Date
158.255.208.xxx		Jordan	12/2014
109.123.112.xxx		Jordan	12/2014
185.19.192.xxx		Kazakhstan	1/2015
178.208.76.xxx		Kazakhstan	2/2015
46.23.73.xxx	197.254.122.xxx	Kenya	3/2015
212.98.139.xxx	212.98.139.xxx	Lebanon	12/2014
77.42.156.xxx		Lebanon	12/2014
77.28.101.xxx		Macedonia	12/2014
77.28.102.xxx		Macedonia	12/2014
79.125.161.xxx		Macedonia	12/2014
213.136.89.xxx	211.25.14.xxx	Malaysia	12/2014
93.104.212.xxx		Malaysia	12/2014
118.101.145.xxx		Malaysia	12/2014
110.159.5.xxx		Malaysia	12/2014
201.122.183.xxx	201.122.183.xxx	Mexico	12/2014
31.192.226.xxx	103.230.82.xxx	Mongolia	12/2014
176.67.169.xxx		Morocco	12/2014
176.67.168.xxx	81.192.4.xxx	Morocco	12/2014
109.123.86.xxx	81.192.4.xxx	Morocco	12/2014
176.67.172.xxx	81.192.4.xxx	Morocco	12/2014
176.67.172.xxx	81.192.4.xxx	Morocco	12/2014
37.123.115.xxx	41.242.50.xxx	Nigeria	12/2014
176.67.172.xxx	204.14.42.xxx	Nigeria	2/2015
85.154.222.xxx		Oman	12/2014
146.185.163.xxx		Oman	5/2015
190.128.172.xxx		Paraguay	12/2014
158.255.215.xxx	95.76.221.xxx	Romania	12/2014
62.149.86.xxx		Saudi Arabia	12/2014
77.31.27.xxx		Saudi Arabia	1/2015
37.107.117.xxx		Saudi Arabia	2/2015
2.90.15.xxx		Saudi Arabia	5/2015
2.89.48.xxx		Saudi Arabia	5/2015
95.218.27.xxx		Saudi Arabia	5/2015
195.178.51.xxx		Serbia	12/2014
193.9.21.xxx		Slovenia	12/2014
105.224.57.xxx		South Africa	2/2015
105.228.145.xxx		South Africa	5/2015
192.96.200.xxx	79.144.61.xxx	Spain	12/2014
41.215.240.xxx	79.144.61.xxx	Spain	12/2014
62.87.109.xxx		Spain	12/2014

Server	FinSpy Master IP	Master Country	Date
209.59.205.xxx	79.144.61.xxx	Spain	12/2014
209.59.213.xxx	79.144.61.xxx	Spain	12/2014
212.166.246.xxx		Spain	12/2014
47.60.110.xxx		Spain	2/2015
190.14.38.xxx	79.144.61.xxx	Spain	2/2015
123.51.216.xxx		Taiwan	12/2014
212.156.217.xxx		Turkey	5/2015
217.174.229.xxx		Turkmenistan	12/2014
217.174.229.xxx		Turkmenistan	12/2014
217.174.229.xxx		Turkmenistan	12/2014
217.174.226.xxx		Turkmenistan	12/2014
185.8.106.xxx		Venezuela	12/2014
151.236.13.xxx	62.153.225.xxx	(Demonstration Server)	12/2014
158.255.212.xxx		(Demonstration Server)	12/2014
80.156.28.xxx		(Demonstration Server)	12/2014
151.236.23.xxx	62.153.225.xxx	(Demonstration Server)	12/2014
106.186.24.xxx	62.153.225.xxx	(Demonstration Server)	12/2014
117.102.124.xxx		(Demonstration Server)	5/2015
37.139.27.xxx			12/2014
151.236.13.xxx			12/2014
46.4.148.xxx			12/2014
185.15.245.xxx			12/2014
37.17.173.xxx			12/2014
95.170.88.xxx			12/2014
89.46.101.xxx			12/2014
194.58.97.xxx			12/2014
116.251.208.xxx			12/2014
212.71.232.xxx			12/2014
209.208.108.xxx			12/2014
198.105.122.xxx			12/2014
162.220.246.xxx			12/2014
188.122.76.xxx			12/2014
89.46.101.xxx			12/2014
190.97.165.xxx			12/2014
116.251.223.xxx			12/2014
192.64.11.xxx			12/2014
182.54.233.xxx			12/2014

Server	FinSpy Master IP	Master Country	Date
103.246.249.xxx			2/2015
117.121.243.xxx			2/2015
192.99.151.xxx			5/2015
162.220.246.xxx			5/2015
173.255.143.xxx			5/2015
179.43.160.xxx			6/2015
198.105.122.xxx			6/2015
50.31.255.xxx			6/2015
175.139.238.xxx			6/2015
131.72.138.xxx			6/2015
185.11.146.xxx			6/2015
105.228.147.xxx			6/2015