UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JOHN DOE, a.k.a. KIDANE, *Plaintiff*, v. FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA, *Defendant*.	Civ. No. 1:14-cv-00372-CKK **FIRST AMENDED COMPLAINT** **JURY TRIAL DEMANDED**

1. Plaintiff John Doe, aka Kidane ("Plaintiff" or "Mr. Kidane") brings this action against the Federal Democratic Republic of Ethiopia ("Defendant" or "Ethiopia") and alleges as follows:

PRELIMINARY STATEMENT

2. This is a straightforward case challenging the wiretapping and invasion of privacy of an American citizen at his home in suburban Maryland. The only significant difference between this an ordinary domestic wiretapping case is that the wiretapping was conducted by the government of Ethiopia.

3. Mr. Kidane is a U.S. citizen who was born in Ethiopia and who has been living in the U.S. for over 22 years.

4. Between late October 2012 and March 2013, Defendant caused Mr. Kidane's personal laptop computer in Maryland to become infected with clandestine computer programs known as FinSpy that, at a minimum, surreptitiously intercepted and contemporaneously

recorded dozens of Mr. Kidane's private Skype[1] Internet phone calls, recorded portions or complete copies of a number of emails sent by Mr. Kidane, and recorded a web search related to the history of sports medicine, conducted by Mr. Kidane's son for his ninth grade history class.

5. As described further below, Plaintiff is informed and believes that his computer became infected because of an email containing a Microsoft Word document attachment, sent by or on behalf of Defendant, that was thereafter forwarded to Plaintiff. The attachment then caused a clandestine client program to be surreptitiously downloaded onto his computer. The downloaded clandestine client program resident on Plaintiff's computer then took what amounts to complete control over the operating system. It began contemporaneously recording some, if not all, of the activities undertaken by users of the computer, including Plaintiff and members of his family, a copy of which was sent to a server in Ethiopia and controlled by Defendant.

6. The programs that accomplished the spying on the Kidane family computer in Maryland are collectively called FinSpy. FinSpy is a system for monitoring and gathering information from electronic devices, including computers and mobile phones, without the knowledge of the device's user. Finspy is sold exclusively to government agencies and is not available to hackers or the general public.

7. CitizenLab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada. CitizenLab focuses on advanced research and development at the intersection of digital media, global security, and human rights.

8. CitizenLab has investigated the use of FinSpy technology by governments to spy on human rights and democracy activists around the world. On March 13, 2013, the CitizenLab

[1] Skype is a voice-over-IP communication service provided by Microsoft. The Skype service allows users to use their computer to communicate with other users by voice (with a microphone), video (with a webcam), and text (via instant messaging). Users may also call numbers on the tranditional telephone network.

released a report on the proliferation of FinSpy. The report included a section describing the Ethiopian Government's use of FinSpy, and included identifying details of a FinSpy Master server in Ethiopia. As described in more detail below, and as demonstrated by the traces of FinSpy left on Mr. Kidane's computer, the FinSpy Master server in Ethiopia disclosed in CitizenLab's report is the same server that controlled the FinSpy target installation on Mr. Kidane's computer.

9. Five days after CitizenLab's report, on or around March 18, 2013, the FinSpy target installation on Mr. Kidane's computer was remotely uninstalled by a command sent by Defendant. However, in an apparent software malfunction, FinSpy's remote uninstall process failed to completely remove all traces of the software from Mr. Kidane's computer.

10. The FinSpy installation on Mr. Kidane's computer was active for at least four and a half months, from early November 2012 until the middle of March 2013. Plaintiff is informed and believes that throughout that period, Defendant Ethiopia caused the FinSpy programs installed on the Kidane family computer in Maryland to create contemporaneous recording of his activities in Maryland, which the FinSpy programs then sent to the FinSpy Master server located in Ethiopia.

11. Mr. Kidane seeks a declaration that Ethiopia's real-time recording of his private Skype communications, and related violations of his right to privacy including the recording of his own and his family's web browsing, was tortious and unlawful.

12. Mr. Kidane additionally seeks statutory damages under the Wiretap Act and damages for Ethiopia's intrusion upon his seclusion.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction and personal jurisdiction over the Federal Democratic Republic of Ethiopia pursuant to 28 U.S.C. § 1330 and the Foreign Sovereign Immunities Act (the "FSIA"), 28 U.S.C. §§ 1602, *et seq*., for the multiple tortious injuries occurring within the territory of the United States as alleged in this complaint. Process has been served on the Federal Democratic Republic of Ethiopia pursuant to 28 U.S.C. § 1608(a) (*see* ECF No. 18).

14. Specifically, this Court has subject matter jurisdiction over the Federal Democratic Republic of Ethiopia under 28 U.S.C. §§ 1603(a), 1605(a)(5), and 1606 as Defendant is a foreign state, which is not immune from any suit seeking money damages for "personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment"; and where the claim is not based on the lawful exercise of a "discretionary function," and does not arise out of "malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights."

15. As alleged in this complaint, Defendant or Defendant's officials or employees caused personal injury to Plaintiff, a U.S. citizen and resident of the United States, entirely at Plaintiff's residence in Silver Spring, Maryland, in the United States, through the tortious invasion of Plaintiff's privacy and the unlawful interception of Plaintiff's communications, wholly within the territory of the United States, in violation of the Wiretap Act, 18 U.S.C. §§ 2511, 2520.

16. Alternatively, this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, which confers upon district courts "original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States."

17. Moreover, this Court possesses supplemental jurisdiction over Plaintiff's additional claims pursuant to 28 U.S.C. § 1367(a).

18. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(f)(4) because Defendant is a foreign state.

PARTIES

19. Plaintiff John Doe, also known as Kidane, is an Ethiopian-born citizen of the United States, who currently and at all times relevant to this Complaint resided in Silver Spring, Maryland.

20. Plaintiff uses the name Kidane within the Ethiopian Diaspora in order to protect his family both in the United States and in Ethiopia. Plaintiff's use of the name Kidane was described in detail in Plaintiff's Motion for Leave to Proceed Anonymously, filed concurrently with the original Complaint in this action, and granted by the Court on March 5, 2014 (ECF No. 2). Plaintiff fears that his work within the Ethiopian Diaspora puts his life, and the lives of his family, at substantial risk. *See* Declaration of Kidane (ECF No. 1-1).

21. Defendant the Federal Democratic Republic of Ethiopia is a sovereign state located in East Africa.

FACTUAL ALLEGATIONS

SUPPRESSION OF DISSENT BY THE ETHIOPIAN GOVERNMENT

22. According to the State Department's Report on Human Rights Practices for 2012 in Ethiopia: "The most significant human rights problems [in Ethiopia] include[] restrictions on

freedom of expression and association through politically motivated trials and convictions of opposition political figures, activists, journalists, and bloggers, as well as increased restrictions on print media." [2]

23. In a May 16, 2012 press release, Amnesty International reports that: "The Ethiopian People's Revolutionary Democratic Front (EPDRF) has ruled for more than two decades. [Ethiopian Prime Minister Meles] Zenawi's government has systematically attempted to crush dissent in the country by jailing opposition members and journalists, firing on unarmed protesters, and using state resources to undermine political opposition."[3]

24. The Ethiopian government seeks to undermine political opposition abroad as well as at home. For example, according to the website for the United Nations High Commissioner for Refugees, summarizing an October 11, 2012 report by the Norwegian Broadcasting Corporation: "The Norwegian Broadcasting Corporation (NRK) reports that refugee espionage in Norway is widespread. The espionage often seeks information about refugees in opposition to the regime in their country of origin. This is confirmed by the Norwegian Police Security Service (PST), which adds that several countries carry out refugee espionage in Norway, especially countries in conflict. Rune Berglund Steen, from [the] Antiracism Centre in Oslo, says that: Based on the information I have collected since 2004/2005, it appears that Ethiopian refugee espionage is both systematic and comprehensive. It is shamelessly extensive. He claims that

[2] United States Department of State, Country Reports on Human Rights Practices for 2012, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2012&dlid=204120 (last visited December 20, 2013).

[3] Amnesty International, http://www.amnestyusa.org/news/press-releases/amnesty-international-urges-president-obama-to-speak-up-about-repression-human-rights-abuses-in-ethi (last visited December 20, 2013).

this has been going on for a long period and that the espionage has not been associated with legal consequences in Norway."[4]

25. One way in which the Ethiopian government monitors political dissidents at home and abroad is through the use of electronic surveillance. According to Freedom House's "Freedom on the Net 2013" report on Ethiopia: "In 2012, [Ethiopian] repression against bloggers and ICT users increased, with several arrests and at least one prosecution reported. The Telecom Fraud Offences law enacted in September 2012 toughened the ban on advanced Internet applications and established criminal liability for certain types of content communicated electronically. Furthermore, monitoring of online activity and interception of digital communications intensified, with the deployment of FinFisher surveillance technology against users confirmed in early 2013." [5]

FINSPY BACKGROUND

26. Exhibit B is a March 13, 2013 report by CitizenLab titled "You Only Click Twice: FinFisher's Global Proliferation." (FinSpy is a part of Gamma's FinFisher line of products.) The report describes the results of a comprehensive global scan of computers on the Internet to identify 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.

27. FinSpy is part of the FinFisher line of "IT Intrusion" products developed and marketed by the Gamma Group of Companies. The Gamma Group produces FinSpy spyware

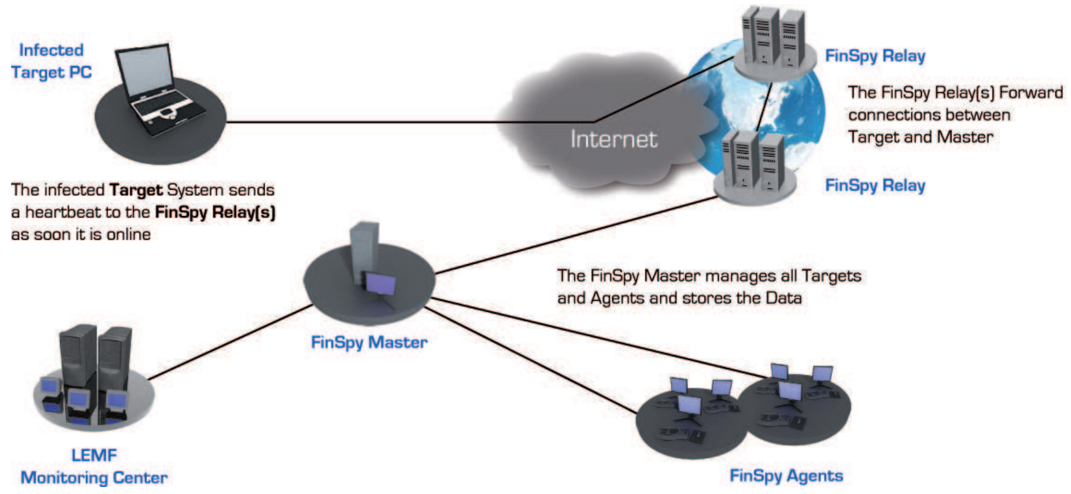
[4] UNHCR, http://www.unhcr.se/no/media/baltic-and-nordic-headlines/2012/october/12-16-october-2012.html (last visited December 20, 2013).

[5] Freedom House, http://www.freedomhouse.org/report/freedom-net/2013/Ethiopia (last visited December 20, 2013).

for Windows, Macintosh, and Linux computers, as well as iPhone, Android, Nokia/Symbian, Windows Phone, and Blackberry mobile devices.

28. FinSpy consists of a suite of surveillance software marketed by Gamma International, Ltd, a United Kingdom-based company and/or FinFisher GmbH, a German company (collectively "Gamma"). The software suite includes the target installation of a clandestine client program, one or more FinSpy Relays, and a FinSpy Master server (collectively "FinSpy"). Attached hereto as Exhibit A is a FinSpy sales brochure produced by Gamma.

29. The following diagram illustrates how the FinSpy software operates.


Infected
Target PC
Internet
FinSpy Relay
The FinSpy Relay(s) Forward connections between Target and Master
FinSpy Relay
The infected Target System sends a heartbeat to the FinSpy Relay(s) as soon it is online
The FinSpy Master manages all Targets and Agents and stores the Data
FinSpy Master
LEMF
Monitoring Center
FinSpy Agents

30. Gamma specifically asserts that "FinFisher solutions are sold to governmental agencies only."[6] Plaintiff is informed and believes that FinSpy is therefore unavailable to the general public.

31. According to Gamma's promotional materials, the system consists of client software designed to be covertly installed on a targeted device ("spyware") as well as infrastructure run by the government operator of the system to collect the data gathered by the

[6] FinFisher, http://www.finfisher.com/FinFisher/products_and_services.html (last visited January 9, 2014).

spyware and facilitate monitoring. Devices on which the spyware is installed are referred to as "infected devices."

32. Gamma performs testing of FinSpy against the 40 most popular computer programs for detecting viruses and spyware – known as anti-virus programs (*see* Exhibit A). Gamma routinely modifies FinSpy to prevent detection by anti-virus programs, and releases such updates for FinSpy to their customers.

33. Gamma employs sophisticated techniques to prevent detection and thwart analysis of how its FinSpy spyware works, such that FinSpy is designed specifically to subvert analysis tools used by security researchers.

34. FinSpy is written in a special programming language designed by Gamma. The language is translated into one that the computer can understand and execute as the spyware is run. Performing some kinds of analysis of the spyware require understanding and decoding this language. The spyware can be made to appear to have very different characteristics by making small changes to the language.

35. The infrastructure for collecting data gathered from infected devices consists of software and hardware components known as a FinSpy Master, and one or more FinSpy Relays. The FinSpy Master's job is to facilitate data gathering and monitoring of the devices. The FinSpy Master sends commands to infected devices and receives gathered information.

36. The FinSpy system contains a number of modules (sets of optional computer program components that enable various features) that the government operator may install on infected devices to facilitate different types of monitoring and the acquisition of different types of data from infected devices. For example, FinSpy contains a module for extracting saved

passwords from more than 20 different web browsers, e-mail programs, and chat programs, and capturing these passwords as the user types them in.

37. FinSpy also contains a module for the contemperaneous recording of Internet telephone calls, text messages, and file transfers transmitted through the Skype application, a module for covertly recording audio from a computer's microphone even when no Skype calls are taking place, a module for recording every keystroke on the computer, and a module for recording a picture of the contents displayed on a computer's screen.

38. The FinSpy Skype module uses functionality built into Skype for contemporaneously recording calls. Specifically, the Skype software allows other software to direct Skype to perform certain functions, such as recording call audio while the call is being made. When the FinSpy Skype module on an infected computer records Skype call audio, it does so contemporaneous to the call and without the user's knowledge or consent.

39. The FinSpy spyware is installed by way of a software executable (an executable is any computer file that contains commands for the computer to run, *e.g*., an application). A government agent can manually install a FinSpy executable on any computer he has physical or remote access to. If the government agent wishes to infect a computer that he does not have physical or remote access to, the agent may send the target a file that contains a FinSpy executable (*e.g*., via e-mail) and attempt to convince the target to open it on the target's own computer.

40. The types of files that a FinSpy operator may send include a FinSpy executable disguised as an image, or a FinSpy executable embedded in a Microsoft Word document. The government agent may attempt to convince the target to open the file by claiming that the file is

of interest to the target. When the target opens the file, he is presented with a legitimate image or Word Document, depending on the type of file.

41. In the case of the image, the target is tricked into opening the executable and is thus infected. The executable deletes itself, and replaces itself with the benign image displayed to the target. The target is therefore unaware that his computer has been infected.

42. In the case of the Microsoft Word document, the document contains a "macro" – a Microsoft Word feature designed to enable automation – that attempts to run the embedded FinSpy executable when the document is loaded. The Word document does not replace itself with a benign copy after the user is infected. Thus, opening the document again on another computer will also infect that computer. When the executable is run, it creates a directory ("FinSpy directory") on the target computer's disk that it uses to store files, including Skype audio calls, as FinSpy interepts them.

43. Each FinSpy executable contains a configuration file that dictates particular parameters of the operation of that instance of the spyware. One of the parameters specified by the configuration file is a list of one or more Internet addresses or Internet domain names, representing FinSpy Masters with which the spyware should communicate. That perameter is hard-coded into the executable and uniquely identifies the FinSpy Master responsible for that particular infection.

44. Gamma sells FinSpy licenses to governments that only allow a certain number of infected devices to be concurrently monitored (*see* Exhibit A). This number is dictated by the license agreement between Gamma and the government operator of FinSpy.

45. When a device is infected with FinSpy, it contacts the FinSpy Master, through the FinSpy Relay listed in its configuration file. If the number of infected devices is less than the

maximum number that the government operator has purchased licenses for monitoring, then the infection becomes active. If the number of devices being concurrently monitored is equal to the maximum number that are permitted to be concurrently monitored, the infection remains dormant, but periodically contacts the FinSpy Master server to check whether the number of infected devices has dropped below this threshold. If this happens, or if the government operator purchases more licenses from Gamma, then the infection becomes active.

46. When an infection becomes active, it contacts the FinSpy Relay to download modules, and begins capturing and sending information back to the FinSpy Master. In turn, the FinSpy Relay can send commands to an infected device.

47. On information and belief, these commands include the ability to remotely deactivate the spyware on an infected device (*see* Exhibit A). Commands also enable the government operator to specify a new Internet address or domain name as a FinSpy Relay, to install modules, to run custom programs on an infected device, to browse information stored on the device, and to enable or disable features such as live audio recording from the device's microphone.

48. Most of the FinSpy modules, including the module for recording Skype calls, behave in the following manner: The FinSpy module simultaneously records the audio data to the infected computer's disk as as the call proceeds, before then transmitting it to the FinSpy Master. In some cases, such as the case of the FinSpy Skype module, the module first contemporaneously intercepts and copies the data, unencrypted, to files on the infected computer's temporary folder on its hard disk. The module then encrypts the information, and writes it to an encrypted file in the FinSpy directory on the hard disk using a specialized naming

convention that identies files containing captured data. Thus, FinSpy makes a simultaneous recording of a target's Skype call, on his or her own computer.

49. Under the FinSpy naming convention, files containing incoming audio recorded during Skype calls begins with "snd" and ends in between one and four hexadecimal digits. A hexadecimal digital is a base-16 number, in which 0–9 represent values zero to nine, and A, B, C, D, E, F (or alternatively a–f) represent values ten to fifteen.

50. Under ideal conditions, the temporary file is deleted after the encrypted file is successfully written. However, security researchers have observed that FinSpy fails to delete temporary files in some cases.

51. Periodically, FinSpy transmits to the FinSpy Master all files matching the naming convention for files containing captured data. FinSpy deletes these files after it successfully transmits them to the FinSpy Master.

52. In the normal course of operation, whenever any program writes a file to a computer's disk, the computer automatically records the date and time that the file was written, and stores at least the latest such date (along with the file) on disk – previous dates are sometimes stored as well.

53. Security researchers have observed that in some cases, FinSpy interferes with this process, and backdates some files it writes by exactly one year. Plaintiff is informed and believes that such backdating is a feature of FinSpy that is designed to, in some cases, make the infection slightly more difficult to detect.

54. When a device is infected with FinSpy, the infection may persist on the computer – *i.e.*, when the computer is restarted, it will still be infected with FinSpy. One of the

ways this is achieved is by modifying the computer's boot process.[7] The spyware places itself on normally-unused parts of the disk that are not typically accessible to the computer's operating system. This is known as unpartitioned space. The computer's boot process is modified so that FinSpy is loaded before the computer's operating system. As the computer's operating system loads, FinSpy infects the operating system. Thus, even if FinSpy is removed from the areas of disk normally visible and accessible to the operating system, the boot process can still reinfect the computer when it is restarted.

THE SPECIFIC INFECTION OF PLAINTIFF'S COMPUTER BY FINSPY

55. On or around March 2013, the disk in Plaintiff's computer contained two Microsoft Word documents GKO2.doc and GKO2 (1).doc, which, in turn, contained FinSpy executables designed to infect computers running Microsoft Windows.

56. When the files are opened on a computer, they display several paragraphs of Amharic[8] text in Microsoft Word (*see* Exhibit C, email forwarded to Plaintiff, including original Word document text and accompanying English translation). At the same time, a macro in the document attempts to infect the user's computer with FinSpy. The date on these files were October 31, 2012 at 09:25:17 and October 31, 2012 at 09:25:46 respectively. The Amharic text found on Plaintiff's computer contains a not-so-veiled threat against the family of one of Plaintiff's acquaintences and implies that Defendant, the Government of Ethiopia, is behind both the threat and the email. On information and belief, Defendant created the document whose text appears at Exhibit C, and intentionally infected the document with FinSpy.

[7] A computer's boot process is the series of steps a computer takes automatically when powered on to load the operating system, *e.g.*, Micorosft Windows.

[8] Amharic is the official working language of the Federal Democratic Republic of Ethiopia.

57. On or around March 2013, there was a copy of FinSpy in GKO.doc and GKO (1).doc on Plaintiff's computer.

58. This copy of FinSpy contained a configuration file, hard-coded with an Internet Protocol ("IP")[9] address, 213.55.99.74, for a single FinSpy Relay.

59. The 213.55.99.74 IP address is in a block of addresses registered to Defendant Ethiopia's state-owned telecommunications company[10] – Ethio Telecom.

60. On information and belief, this relay is located inside Ethiopia, and its operator is the Defendant in this action.

61. Online security researchers have conducted several scans of various ranges of Internet address numbers. As a result of one such scan, the existence of the Ethiopian FinSpy Relay located at 213.55.99.74 was first disclosed on August 8, 2012 in a research blog post appearing on the website of Rapid7, a security firm.[11]

62. CitizenLab conducted subsequent scans that determined that the 213.55.99.74 address was a FinSpy Relay located in Ethiopia. These results were publicized on August 29, 2012, and March 13, 2013 (*see* Exhibit B). In both cases, the Relay was still operational at the time of publication.

63. The March 13, 2013 CitizenLab publication also reported on the discovery of a FinSpy infection executable disguised as an image of Ethiopian opposition leaders, which

[9] An IP address is a numeric value used to identify the network location of a computer or set of computers on the Internet. Every computer on the Internet needs to have an IP address in order to communicate with other computers on the Internet.

[10] IP addresses are allocated in blocks of consecutive addresses out of a worldwide pool of around four billion possible addresses though geographically based non-profit organizations known as regional Internet registries.

[11] Rapid7, Information Security: Analysis of the FinFisher Lawful Interception Malware, https://community.rapid7.com/community/infosec/blog/2012/08/08/finfisher (last visited November 13, 2013).

contained a configuration file containing the address of the same Ethiopian relay (*see* Exhibit B). On information and belief, the FinSpy infection executable discovered by CitizenLab was created by Defendant for the purpose of infecting the computers of those who sympathize with the political opponents of Defendant.

64. The hard disk in Plaintiff's computer contains a number of temporary files whose names are consistent with the temporary file naming convention used by FinSpy.

65. The FinSpy software recorded these files on Plaintiff's computer in Maryland, saving them simultaneously on that compuer without Plaintiff's knowledge or consent. Due to the operation of FinSpy, the recordings of Plaintiff's communications were made automatically, and entirely on Plaintiff's computer in the United States, without intervention of the Ethiopian Master server.

66. Specifically, the hard disk in Plaintiff's computer contains 244 files whose name begins with "snd" and ends in between one and four hexadecimal digits. FinSpy uses this naming convention for incoming audio recorded during Skype calls.

67. The hard disk contains 247 files whose name begins with "mic" and ends in one to four hexadecimal digits. FinSpy uses this naming convention for audio recorded from the microphone during Skype calls (outgoing audio).

68. FinSpy's Skype module operates as follows: after recording the two audio streams – incoming and outgoing – from a Skype call separately, these two streams are combined into a single file: the incoming audio is placed in the right stereo channel, and the outgoing audio is placed in the left stereo channel. Then this file is compressed to reduce size. FinSpy stores the result of this process in a temporary file whose name begins with "ogg" and ends in one to four hexadecimal digits.

69. The disk in Plaintiff's computer contains 83 such "ogg" files consistent with FinSpy's naming convention. These files contain portions or complete copies of Plaintiff's private and highly confidential Skype conversations.

70. Collectively, the traces of the FinSpy infection found on Plaintiff's computer are referred to as the "FinSpy trace files."

71. Under ideal conditions, FinSpy deletes these temporary files when it is done with them. The presence of the "snd," "mic," and "ogg" files is consistent with Skype calls that were recorded by FinSpy, and in the normal course of FinSpy's operation, would have been transmitted to the FinSpy Master by way of a FinSpy Relay (*see* Exhibit A for an illustration of the operation of a FinSpy Relay).

72. The earliest date observed on any of these FinSpy trace files was December 7, 2011 at 09:35:48.[12] This file appears have been backdated by exactly one year, consistent with FinSpy's observed behavior. The latest date observed on any of these FinSpy trace files was March 17, 2013 at 17:30:35.

73. FinSpy also stores temporary files whose names begin with "del" and end in one to four hexadecimal digits. The disk contains 1597 such files. The latest date observed on any of these files was March 18, 2013 at 08:58:24.

74. The disk in Plaintiff's computer also contains a folder ProtectedSvc that was used by FinSpy to store various components of FinSpy, including its code, configuration file, and encrypted files containing gathered data before they are sent to the server. Some of the non-Skype files recorded by FinSpy on Plaintiff's computer include recordings of his, and his family's, web search histories, including a record of Mr. Kidane's son's search related to sports

[12] All times are Eastern time and written in 24-hour format.

medicine. Several of the other files appear to be FinSpy records of other of Mr. Kidane's computer activity.

75. The date on the folder was October 31, 2011 at 09:26:39. On information and belief, the time on the ProtectedSvc folder was backdated by FinSpy by exactly one year. Therefore, Plaintiff is informed and believes that October 31, 2012 was the date Defendant Ethiopia infected his computer.

76. The ProtectedSvc folder on Plaintiff's computer also contains FinSpy code, a configuration file, and several encrypted files containing gathered data that were apparently not sent to the server. The most recent date associated with the folder is March 18, 2013 at 08:58:27. This is also the most recent date associated with any file on Plaintiff's disk that is consistent with a file written by or belonging to FinSpy. This is Plaintiff's best estimate for the last date of activity of FinSpy on Plaintiff's computer.

77. In summary, Plaintiff's computer was infected with FinSpy on October 31, 2012 at 09:26:39. The earliest date associated with files containing modules downloaded from the server is November 12, 2011 at 08:23:14. This is consistent with FinSpy's technique of backdating files by exactly one year, so the best available estimate for when the infection became active is November 12, 2012 at 08:23:14. During the time that the infection was active, FinSpy operated on Plaintiff's computer in Maryland to contemporaneously intercept his private Skype calls as well as private details of his family's computer usage, and record them to the computer's hard disk without Plaintiff's knowledge or consent. The infection appears to have been removed on March 18, 2013 at 08:58:27, just five days after CitizenLab's publication of its report disclosing Defendant Ethiopia's use of FinSpy and the technical details of the FinSpy Relay in use in Ethiopia. On information and belief, FinSpy is sold only to governments and government

agencies, and the instance of FinSpy that was present on Plaintiff's computer was hard-coded to report back to a server controlled by Defendant.

SUMMARY OF ALLEGATIONS

78. Gamma expressly represents that it only sells the FinSpy product to law enforcement and intelligence agencies.

79. Defendant Ethiopia controls all Ethiopian law enforcement and intelligence agencies.

80. On information and belief, Gamma sold the FinSpy software suite to Defendant Ethiopia.

81. Defendant Ethiopia intentionally distributed a Microsoft Word document infected with FinSpy.

82. Plaintiff's computer in Maryland was infected by a FinSpy executable created by Defendant on or around October 31, 2012 at 09:26:39 by that Microsoft Word file.

83. The FinSpy installation on Plaintiff's computer in Maryland directly resulted from the Microsoft Word document file intentionally created and intentionally infected with FinSpy by Ethiopia.

84. The FinSpy installation on Plaintiff's computer in Maryland took instructions from a FinSpy Relay controlled by Defendant Ethiopia.

85. On information and belief, the FinSpy Relay and FinSpy Master servers with which Plaintiff's computer in Maryland was controlled are located inside Ethiopia and controlled by Defendant Ethiopia.

86. The FinSpy installation on Plaintiff's computer in Maryland downloaded modules from this FinSpy Master server onto Platinff's computer on or around November 12, 2012 at 08:23:14.

87. On information and belief, the FinSpy software on Plaintiff's computer in Maryland used the downloaded modules to automatically intercept Plaintiff's private commmunications, resulting in a contemporaneous interception of Plaintiff's communications on his computer in Maryland.

88. Defendant Ethiopia attempted to remove the FinSpy software infection from Plaintiff's computer in Maryland on or around March 18, 2013 at 08:58:27, just five days after CitizenLab published technical details describing the FinSpy Relay operated by Defendant—the same server that was controlling Plaintiff's computer.

89. On information and belief, the FinSpy installation on Plaintiff's computer in Maryland was controled by Defendant Ethiopia at all times between October 2012 and March 2013.

90. On information and belief, Defendant Ethiopia did not obtain a warrant, work with the United States Department of State, or obtain any legal process to lawfully undertake a wiretapping of Plaintiff at his home in Maryland.

91. The knowledge that Defendant Ethiopia had access to Plaintiff's most sensitive private communications, including those involving this work with the Ethiopian Diaspora, puts Plaintiff at substantial unease and has caused him significant emotional distress. Defendant's actions have caused Plaintiff to fear for his safety, as well as that of his friends, family, and contacts.

FIRST CAUSE OF ACTION

Violation of the Wiretap Act, 18 U.S.C. § 2511

92. Plaintiff repeats and incorporates herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

93. The Wiretap Act prohibits the willful interception of any wire, oral, or electronic communication.

94. A private right of action is created by 18 U.S.C. § 2520 and is available to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used."

95. Defendant intentionally and willfully intercepted Plaintiff's private wire, oral, or electronic communications, using a software device on Plaintiff's computer at his home in Silver Spring, Maryland.

96. Among other data intercepted by Defendant, Plaintiff's private Skype calls were wire, oral, or electronic communications within the meaning of the Wiretap Act.

97. Defendant Ethiopia's contemporaneous acquisition of Plaintiff's private Skype phone calls, by the use of the FinSpy software present on Plaintiff's computer in the United States, is an interception within the meaning of the Wiretap Act because it is an acquisition of the contents of his communication by use of any electronic, mechanical, or other device.

98. Plaintiff had a reasonable expectation that his wire, oral, or electronic communications would remain private.

99. Plaintiff is a person whose wire, oral, or electronic communication were intercepted within the meaning of 18 U.S.C. § 2520.

100. Section 2520 provides for equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each violation of the Wiretap Act, and reasonable attorneys' fees as a result of the above-described violations.

SECOND CAUSE OF ACTION

Intrusion Upon Seclusion

101. Plaintiff repeats and incorporates herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

102. Defendant intentionally intruded upon and invaded the solitude and seclusion of Plaintiff.

103. Defendant intruded upon and invaded Plaintiff's private affairs and concerns by using a software device on Plaintiff's computer at his home in Silver Spring, Maryland, to record and monitor Plaintiff's and his family's computer private activities at their home in Maryland, and to transmit said recordings to servers it controlled in Ethiopia.

104. Plaintiff's private affairs and concerns, including his wire, oral, or electronic communications intercepted by Defendant, are not a matter of public concern.

105. The aforementioned intrusion upon seclusion was highly offensive to an ordinary, reasonable person.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court:

1. Declare that Defendant's actions as described above violated the Wiretap Act, and constituted an intrusion upon seclusion;

2. Award to Plaintiff damages, including statutory damages where available, for injury sustained by him as a result of Defendant's wrongdoing, in an amount to be proven at trial, including pre-judgment interest thereon;

3. Award to Plaintiff reasonable attorneys' fees and other costs and expenses of suit to the extent permitted by law; and

4. Grant Plaintiff such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff hereby requests a trial by jury for all issues so triable.

Dated: July 17, 2014

Respectfully submitted,

/s/ Nathan Cardozo
Nathan Cardozo (DC SBN 1018696)
Cindy Cohn (admitted *pro hac vice*)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel. (415) 436-9333
Fax (415) 436-9993
nate@eff.org

Richard M. Martinez (admitted *pro hac vice*)
Samuel L. Walling (admitted *pro hac vice*)
John K. Harting (admitted *pro hac vice*)
ROBINS, KAPLAN, MILLER & CIRESI L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402-2015
Tel.: (612) 349-8500
Fax: (612) 339-4181
rmmartinez@rkmc.com

Counsel for Plaintiff

Exhibit A

Exhibit A

FINSPY

FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face the current challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**.

Traditional Lawful Interception solutions face new **challenges** that can only be solved using active systems like FinSpy:
- Data not transmitted over any network
- Encrypted Communications
- Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

QUICK INFORMATION

Usage:	· Strategic Operations · Tactical Operations
Capabilities:	· Remote Computer Monitoring · Monitoring of Encrypted Communications
Content:	· Hardware/Software

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Computer – Example Features:

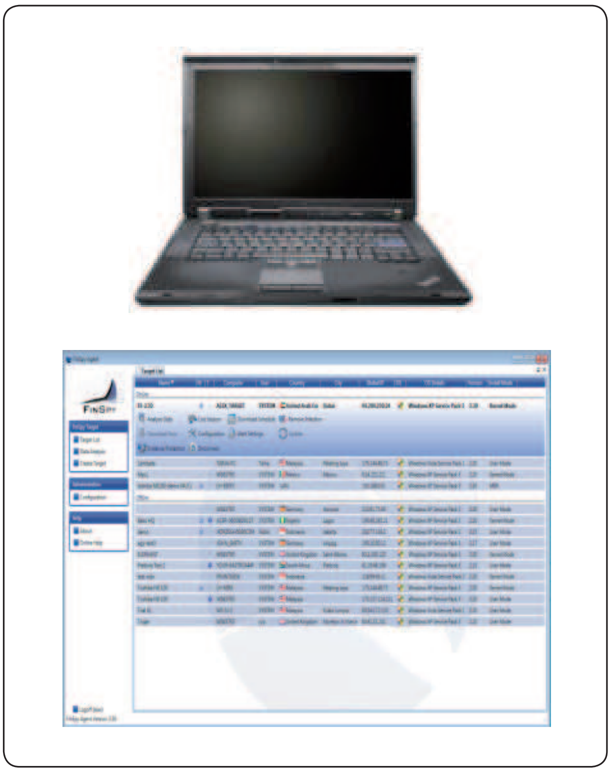
- Bypassing of 40 regularly tested Antivirus Systems
- **Covert Communication** with Headquarters
- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of **common communication** like Email, Chats and Voice-over-IP
- **Live Surveillance** through Webcam and Microphone
- **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**)

Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Security Data Encryption and Communication using **RSA 2048 and AES 256**
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality (LEMF)

For a full feature list please refer to the Product Specifications.

Product Components



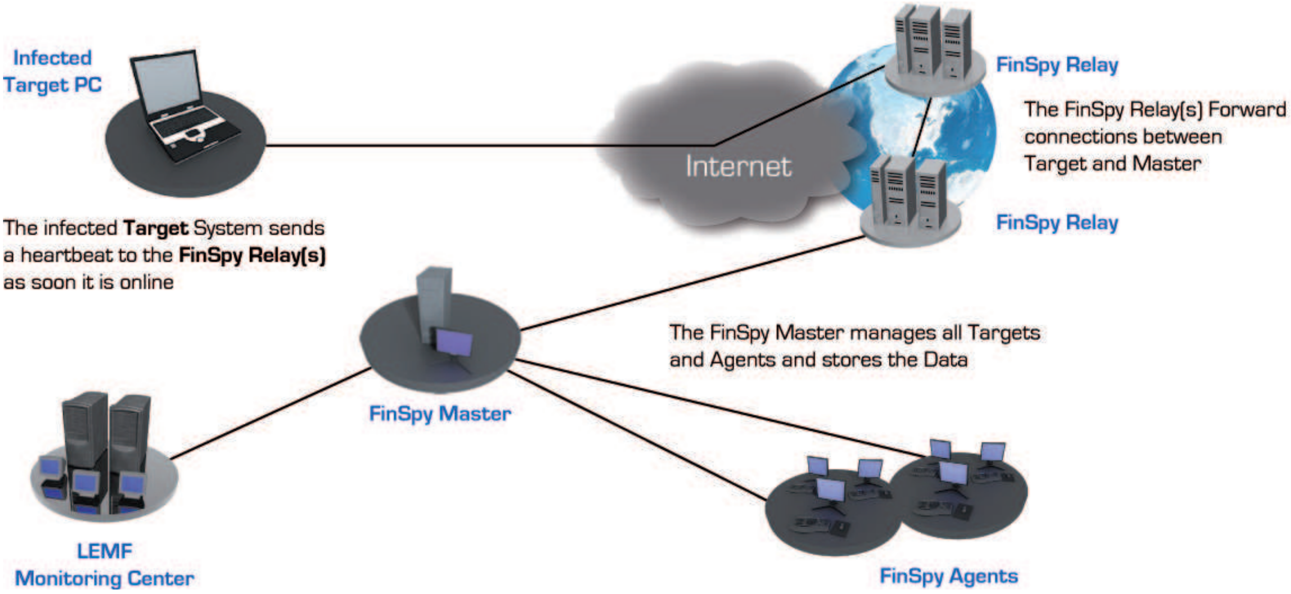
FinSpy Master and Proxy

- Full Control of Target Systems
- Evidence Protection for Data and Activity Logs
- Secure Storage
- Security-Clearance based User- and Target Management

FinSpy Agent

- Graphical User Interface for Live Sessions, Configuration and Data Analysis of Targets

Access Target Computer Systems around the World

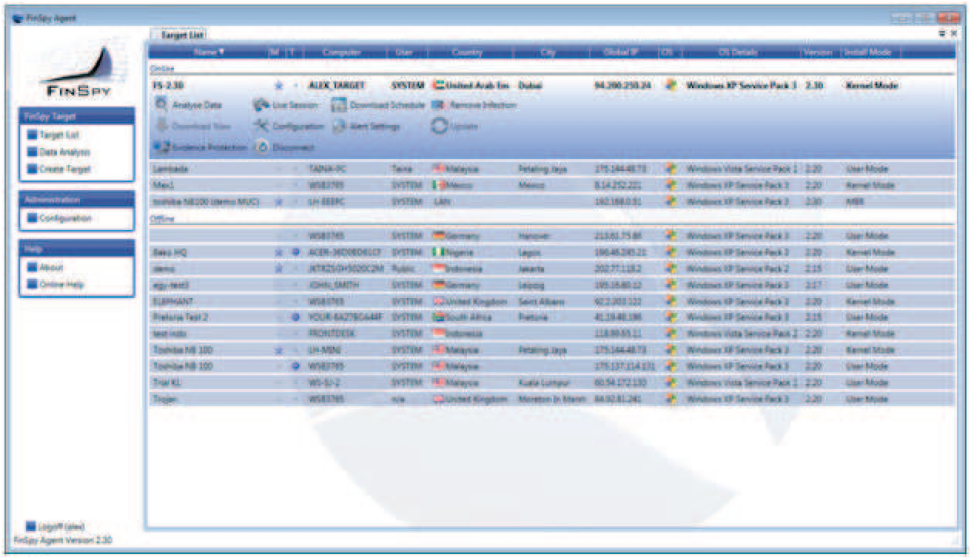


The FinSpy Relay(s) Forward connections between Target and Master

The infected **Target** System sends a heartbeat to the **FinSpy Relay(s)** as soon it is online

The FinSpy Master manages all Targets and Agents and stores the Data

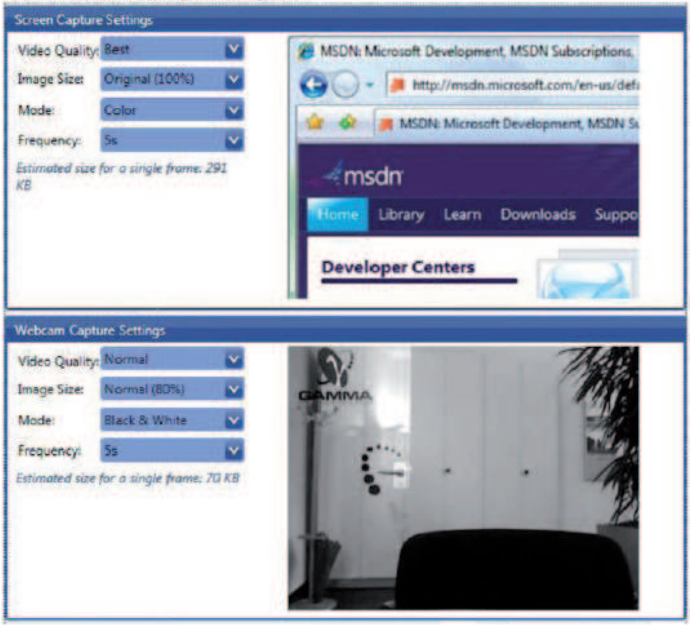
Easy to Use User Interface



Name ▼	M	T	Computer	User	Country	City	Global IP	OS	OS Details	Version	Install Mode
Online											
FS-2.30	★		**ALEX_TARGET**	**SYSTEM**	**United Arab Em**	**Dubai**	**94.200.250.24**		**Windows XP Service Pack 3**	**2.30**	**Kernel Mode**
Lambada			TAINA-PC	Taina	Malaysia	Petaling Jaya	175.144.48.73		Windows Vista Service Pack 1	2.20	User Mode
Maxi1			WS83765	SYSTEM	Mexico	Mexico	8.14.252.221		Windows XP Service Pack 3	2.20	Kernel Mode
toshiba NB100 (demo MUC)	★		LH-EEEPC	SYSTEM	LAN		192.168.0.51		Windows XP Service Pack 3	2.30	MBR
Offline											
			WS83765	SYSTEM	Germany	Hanover	213.61.75.86		Windows XP Service Pack 3	2.20	User Mode
Baku HQ	★	●	ACER-36DDEDE61CF	SYSTEM	Nigeria	Lagos	196.46.245.21		Windows XP Service Pack 3	2.20	Kernel Mode
demo	★		JXTRZG5H5020C2M	Public	Indonesia	Jakarta	202.77.118.2		Windows XP Service Pack 2	2.15	User Mode
egy-test3			JOHN_SMITH	SYSTEM	Germany	Leipzig	195.18.80.12		Windows XP Service Pack 3	2.17	User Mode
ELEPHANT			WS83765	SYSTEM	United Kingdom	Saint Albans	92.2.203.122		Windows XP Service Pack 3	2.20	Kernel Mode
Pretoria Test 2		●	YOUR-6A27BC4A4F	SYSTEM	South Africa	Pretoria	41.19.48.186		Windows XP Service Pack 3	2.15	User Mode
test indo			FRONTDESK	SYSTEM	Indonesia		118.99.65.11		Windows Vista Service Pack 2	2.20	Kernel Mode
Toshiba NB 100	★		LH-MINI	SYSTEM	Malaysia	Petaling Jaya	175.144.48.73		Windows XP Service Pack 3	2.20	Kernel Mode
Toshiba NB 100		●	WS83765	SYSTEM	Malaysia		175.137.114.131		Windows XP Service Pack 3	2.20	User Mode
Trial KL			WS-SJ-2	SYSTEM	Malaysia	Kuala Lumpur	60.54.172.130		Windows Vista Service Pack 1	2.20	User Mode
Trojan			WS83765	n/a	United Kingdom	Moreton In Marsh	84.92.81.241		Windows XP Service Pack 3	2.20	User Mode

Live and Offline Target Configuration

Screen & Webcam Configuration Options



Screen Capture Settings

Video Quality: Best

Image Size: Original (100%)

Mode: Color

Frequency: 5s

Estimated size for a single frame: 291 KB

MSDN: Microsoft Development, MSDN Subscriptions,
http://msdn.microsoft.com/en-us/defa
MSDN: Microsoft Development, MSDN Su
msdn
Home
Library
Learn
Downloads
Suppo
Developer Centers

Webcam Capture Settings

Video Quality: Normal

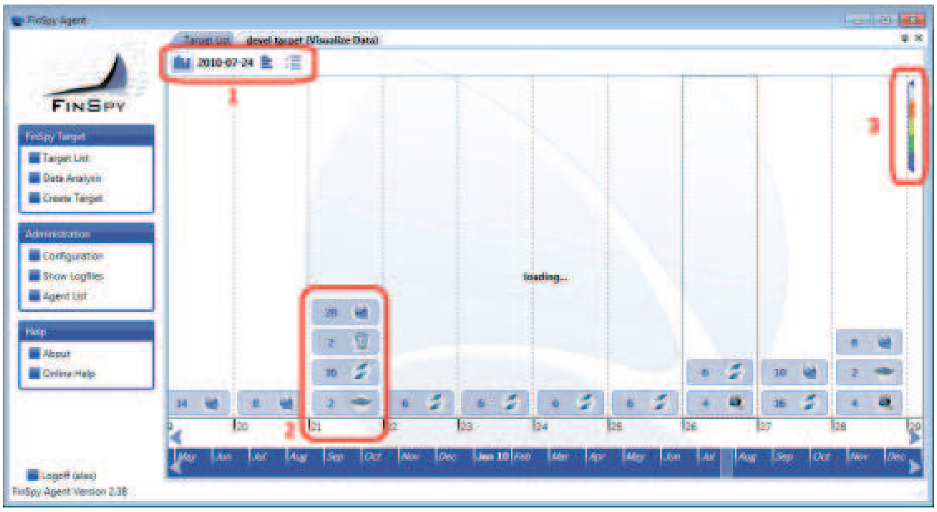
Image Size: Normal (80%)

Mode: Black & White

Frequency: 5s

Estimated size for a single frame: 70 KB

Full Intelligence on Target System



1. Multiple Data Views
2. Structured Data Analysis
3. Importance Levels for all recorded Files

FINSPY LICENSES

Outline

The FinSpy solution contains 3 types of product licenses:

A. Update License

The Update License controls whether **FinSpy** is able to retrieve new updates from the Gamma Update server. It is combined with the **FinFisher™ After Sales Support** module.After expiry, the **FinSpy** system will still be **fully functional** but no longer able to retrieve the newest versions and bug-fixes from the FinSpy Update server.

B. Agent License

The Agent License controls how many **FinSpy Agents** can login to the **FinSpy Master** in parallel.

Example:

- **5 Agent Licenses** are purchased.
- **FinSpy Agent** licenses can be installed on an unlimited number of systems, however
- Only 5 **FinSpy Agent** systems can login to the **FinSpy Master** and work with the **data at the same time**

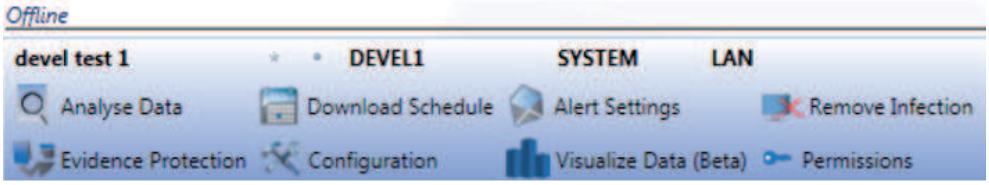
C. Target License

The Target License controls how many **FinSpy Targets** can be **active** in parallel.

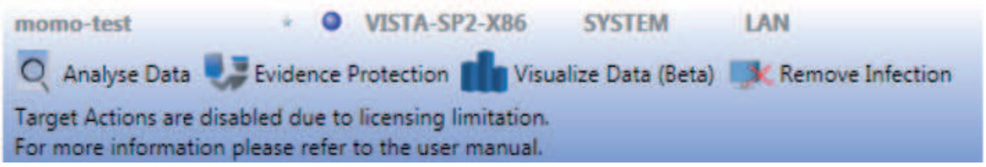
Active refers to **activated FinSpy Target** installations no matter whether the Target System is online or offline.

When **FinSpy Target** is deployed on a Target System and no Target Licenses are available, the **FinSpy Target** gets temporary deactivated and no recording and live access will be possible. As soon as a new License is available (e.g. by upgrading the existing License or de-infecting one of the active **FinSpy Targets**), the Target will be assigned the free license and it will be activated and begin recording and providing live access.

Screenshot active Target with License



Screenshot inactive Target without License



Target Actions are disabled due to licensing limitation.
For more information please refer to the user manual.

Exhibit B

Exhibit B

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 15 – March 2013

You Only Click Twice:

FinFisher's Global Proliferation

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

This post 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.

1. 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.

2. 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.

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.

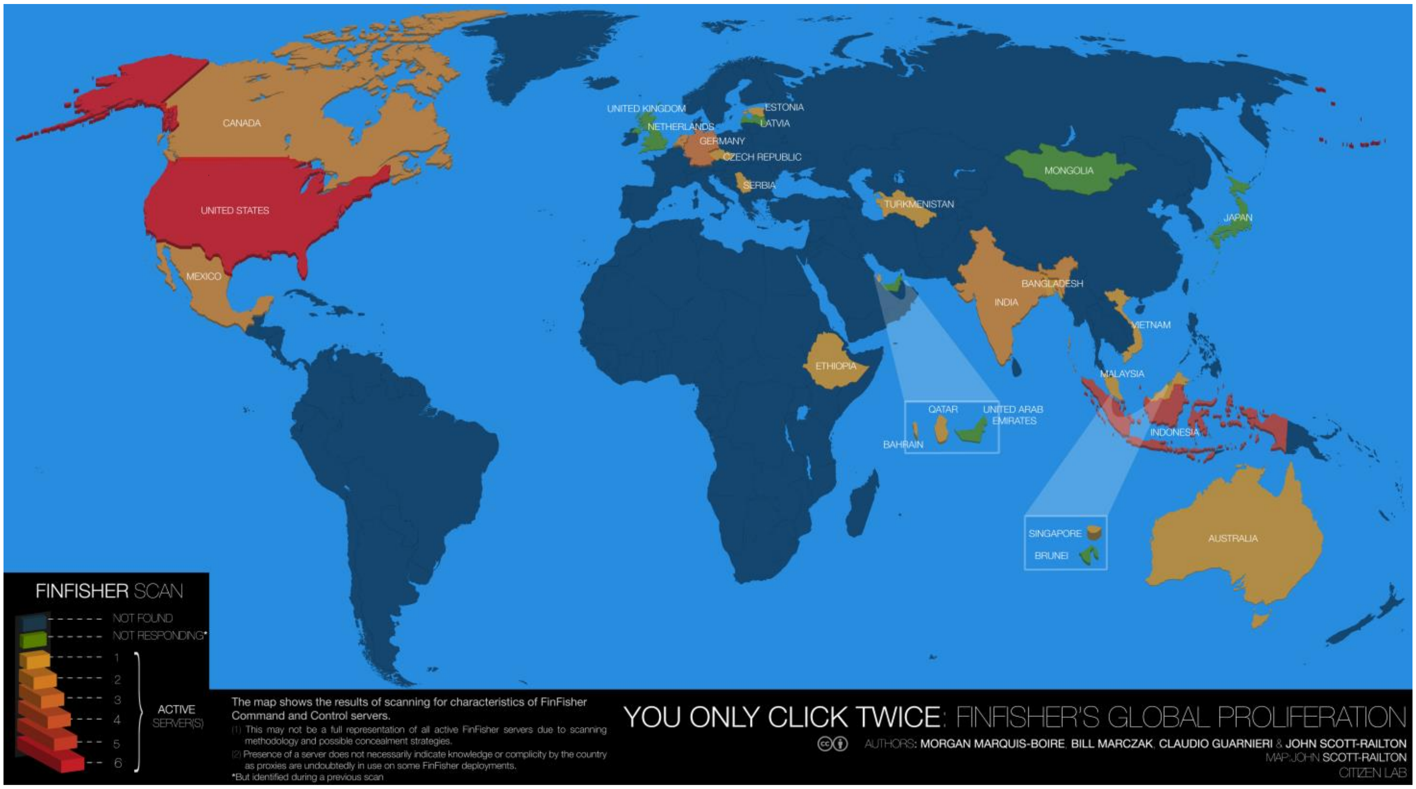
The complaint called previous Gamma statements into question, noting that at least two different versions (4.00 and 4.01) of FinSpy were found in Bahrain, and that Bahrain's server was a FinFisher product and was likely receiving updates from Gamma. This complaint, as laid out by Privacy International 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.

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.

FINFISHER: UPDATED GLOBAL SCAN



The map shows the results of scanning for characteristics of FinFisher Command and Control servers.

(1) This may not be a full representation of all active FinFisher servers due to scanning methodology and possible concealment strategies.

(2) Presence of a server does not necessarily indicate knowledge or complicity by the country as proxies are undoubtedly in use on some FinFisher deployments.

*But identified during a previous scan

AUTHORS: MORGAN MARQUIS-BOIRE, BILL MARCZAK, CLAUDIO GUARNIERI & JOHN SCOTT-RAILTON
MAP:JOHN SCOTT-RAILTON
CITIZEN LAB

Figure 1. Map of global FinFisher proliferation

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 below 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	GPLHost	Malaysia
187.188.xxx.xxx	Iusacell PCS	Mexico
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/.

3. ETHIOPIA AND VIETNAM: IN-DEPTH DISCUSSION OF NEW SAMPLES

3.1 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:

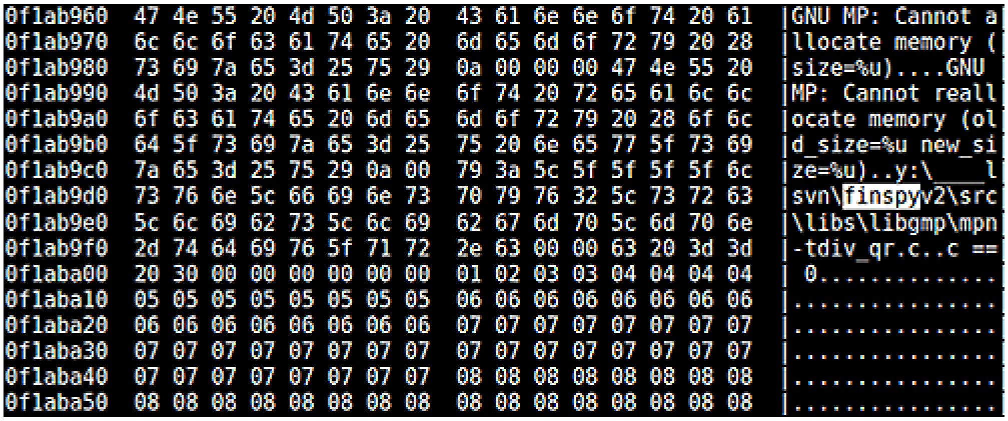
```
IP: 213.55.99.74
route: 213.55.99.0/24
descr: Ethio Telecom
origin: AS24757
mnt-by: ETC-MNT
member-of: rs-ethiotelecom
source: RIPE # Filtered
```

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:



```
0f1ab960  47 4e 55 20 4d 50 3a 20  43 61 6e 6e 6f 74 20 61  |GNU MP: Cannot a
0f1ab970  6c 6c 6f 63 61 74 65 20  6d 65 6d 6f 72 79 20 28  |llocate memory (
0f1ab980  73 69 7a 65 3d 25 75 29  0a 00 00 00 47 4e 55 20  |size=%u)....GNU 
0f1ab990  4d 50 3a 20 43 61 6e 6e  6f 74 20 72 65 61 6c 6c  |MP: Cannot reall
0f1ab9a0  6f 63 61 74 65 20 6d 65  6d 6f 72 79 20 28 6f 6c  |ocate memory (ol
0f1ab9b0  64 5f 73 69 7a 65 3d 25  75 20 6e 65 77 5f 73 69  |d_size=%u new_si
0f1ab9c0  7a 65 3d 25 75 29 0a 00  79 3a 5c 5f 5f 5f 5f 6c  |ze=%u)..y:\____l
0f1ab9d0  73 76 6e 5c 66 69 6e 73  70 79 76 32 5c 73 72 63  |svn\finspyv2\src
0f1ab9e0  5c 6c 69 62 73 5c 6c 69  62 67 6d 70 5c 6d 70 6e  |\libs\libgmp\mpn
0f1ab9f0  2d 74 64 69 76 5f 71 72  2e 63 00 00 63 20 3d 3d  |-tdiv_qr.c..c ==
0f1aba00  20 30 00 00 00 00 00 00  01 02 03 03 04 04 04 04  | 0..............
0f1aba10  05 05 05 05 05 05 05 05  06 06 06 06 06 06 06 06  |................
0f1aba20  06 06 06 06 06 06 06 06  07 07 07 07 07 07 07 07  |................
0f1aba30  07 07 07 07 07 07 07 07  07 07 07 07 07 07 07 07  |................
0f1aba40  07 07 07 07 07 07 07 07  08 08 08 08 08 08 08 08  |................
0f1aba50  08 08 08 08 08 08 08 08  08 08 08 08 08 08 08 08  |................
```

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

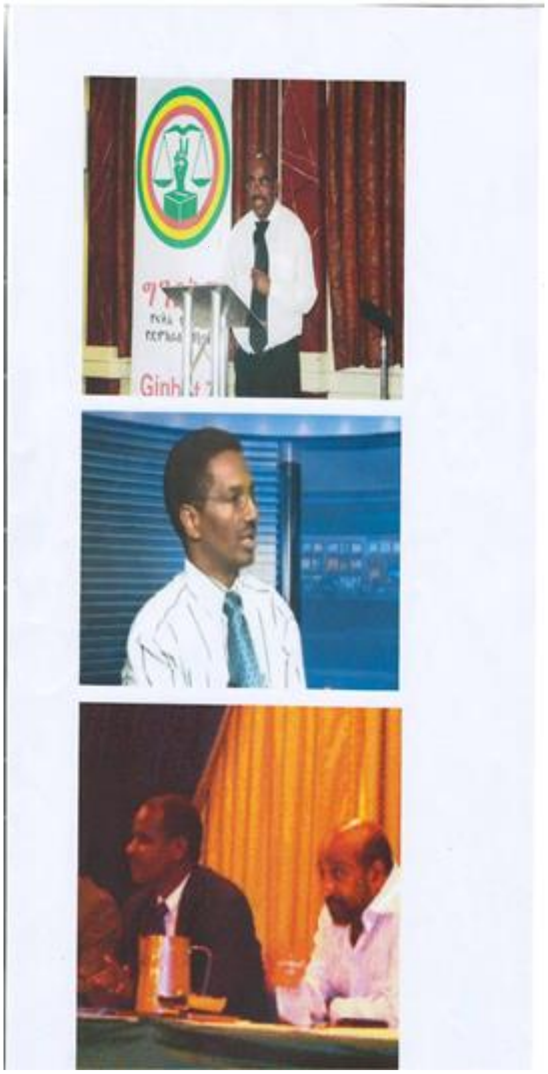


Figure 2. The image shown to the victim contains pictures of members of the Ginbot 7 Ethiopian opposition group

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.

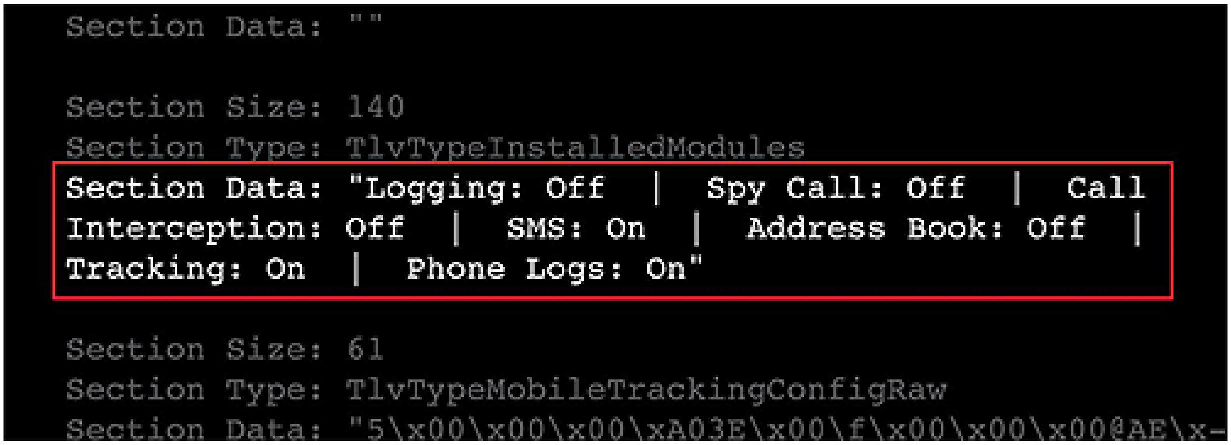
3.2 FinSpy Mobile in Vietnam

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:



```
Section Data: ""

Section Size: 140
Section Type: TlvTypeInstalledModules
Section Data: "Logging: Off  |  Spy Call: Off  |  Call
Interception: Off  |  SMS: On  |  Address Book: Off  |
Tracking: On  |  Phone Logs: On"

Section Size: 61
Section Type: TlvTypeMobileTrackingConfigRaw
Section Data: "5\x00\x00\x00\xA03E\x00\f\x00\x00\x00@AE\x-
```

Figure 3. Image of a section of a configuration file for the FinSpy Mobile sample

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]

4. 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 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.

ACKNOWLEDGEMENTS

We'd like to thank Eva Galperin and the Electronic Frontier Foundation (EFF), Privacy International, Bahrain Watch, and Drew Hintz.

MEDIA COVERAGE

Media coverage of the report includes HuffingtonPost Canada, Salon, The Verge, Bloomberg Business Week, TheYoungTurks.

FOOTNOTES

[1] https://www.gammagroup.com/

[2] Software Meant to Fight Crime Is Used to Spy on Dissidents, http://goo.gl/GDRMe, 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, July 25, 2012

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

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

[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/Mobile_Malware_Evolution_Part_6

[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

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

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

[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/

Exhibit C

Exhibit C

[redacted]

ወንድምህ በብቃቱና በችሎታው በውጪ ጉዳይ ሚኒስቴር በከፍተኛ የሃላፊነት ደረጃ ሲሰራ ቆይቶ አሁንም መንግስቱን ወክሎ የአንድ ታላቅ አገር ኢትዮጵያ አምባሳደር በመሆን ሃገሩንና ወገኑን በከፍተኛ ብቃት እያገለገለ ነው:: የኢትዮጵያ መንግስት መመዘኛ እከሌ ወንድሙ የት አለ? ምን ይሰራል? የሚለው ሳይሆን ብቃትና ችሎታ ብቻ መሆኑን ከዚህ የበለጠ ማረጋገጫ የምታገኝ አይመስለኝም:: አንተ ከገባህበት የጥፋት መንገድ ተመልሰህ ከኛ ጋር ለመስራት ተስማምተህ አድራሻ ተለዋውጠን የተወሰነ እንቅስቃሴ ጀምረን ስናበቃ የገባኸውን ቃል አጥፈህ በሰራኸው ስህተት ቤተሰቦችህ እንዲገላቱ ከማድረግ በስተቀር ከድርጅቱም በኩል እምነትን አላተረፍክም:: ቤተሰቦችህን ይዘህ ለንደን ድረስ በመሄድ “ሚስቴና ልጆቼ በወያኔ ታስረው ከኢትዮጵያ እንዲባረሩ ተደረገ ብለህ” አለቆችህን ለማሳመን ያደረከው ከንቱ ድካም ውጤት አላገኘህበትም:: አሁን ባለው ሁኔታ ከእኛም ከእነሱም ሳትሆን ባዶ ሜዳ ላይ መቅረትህን ለመረዳት የምትቸገር አይመስለኝም::

የጀመርከውን ስራ ለመቀጠል አሁንም ዕድሉ ዝግ አይደለም:: ወደ ትክክለኛው ሰላማዊ መንገድ ለመመለስ ጊዜው አላለፈም:: ፈቃደኛ ካልሆንክ ግን በተከታታይ የከፋ ጉዳት እንደሚደርስብህ ልታውቅ ይገባል:: መጨረሻ ላይ ይህን መልእክት ለሌሎች አሳልፈህ በመስጠት ምናልባት ታማኝነትን አገኛለሁ በሚል ሌላ ስህተት እንዳትሰራ ደግሜ እያሳሰብኩህ አሁንም ምላሽህን በሚቀጥሉት 24 ሰዓታት ውስጥ እጠብቃለሁ::

ሰገድ

Translation Services

[redacted]

Your brother held a high positon at the ministry of foreign affairs as a high ranking official as a result of his qualifications. He still serves the ministry and his country and fellow countrymen. Right now he serves his country and fellow citizens as an Ethiopian Ambasador in a prominant country. The Ethiopian government does not ask as to who is his brother or what his brother is doing? but the government judges him on his own merit alone. You cannot find any better evidence about the actions of the government other than this.

After you have agreed to come out of the wrong way you were in and agreed to work with us and exchanged addresses, started some activities, you broke your promises on your own mistake. You did not get trust even from the organization, you only made your family suffer. You took your family to London and complained by saying " Woyane [TPLF] imprisoned my wife and children and expelled them." This ineffective efort did not gain you the trust of your bosses. I do not think that you will have difficulty to understand that you are losing from us and them and that you are left alone.

The door is not yet closed to continue that assignment that you have started. It is not late to come back to the peaceful way. If you are not willing to cooperate with us, you should know that you will suffer from continuos and major attack. At last, I advise you not to make another mistake by passing this message to others in an anticipation of getting their trust. I warn you and ask you to contact me within the next 24 hours. I am waiting for your response.

Seged.

Subscribed and sworn to before me, in my presence, this 10th February 2014 a Notary Public in and for the State of Maryland.
Maurice Epps
Notary Public
My commission expires 12/30 20 17

○○○ End of Translation ○○○

CERTIFICATE OF TRANSLATION AND ACCURACY

Pursuant to 8 C.F.R. § 1003.33, I, Dinberu Melakehiwot, duly sworn upon oath, depose and certify that I am competent to translate the attached document from Amharic to English. I further certify that the foregoing translation is true and accurate to the best of my knowledge and abilities.

Signature of Translator: ---------------------------

የትክክለኛ ትርጉም ማረጋገጫ ሰርተፊኬት

በአሜሪካ መንግስት የፌደራል መንግስት ህግ አንቀፅ 8 የስደተኞች እና የዜግነት ክፍል ቁጥር 8ሲ ኤፍ አር 1003.33(8CFR 1003.33) መሰረት እኔ ድንበሩ መላከሕይወት የአማርኛ እና የእንግሊዘኛ ቋንቋዎች ሙሉ እውቀት ያለኝ ከመሆኑም በላይ በዚህ ቋንቋዎች ሙሉ በሙሉ መተርጎም እችላለሁ። ከዚህ በላይ የተመለከተዉን የእንግሊዘኛ መረጃ በትክክል የተረጎምኩ መሆኑን አረጋግጣለሁ። ከዚህ በተጨማሪም ይህ ትርጉም እውነተኛ እና ትክክለኛ መሆኑን አረጋግጣለሁ።

የተርጓሚው ፊርማ ---------------------------