CHAMPING AT THE CYBERBIT

Ethiopian Dissidents Targeted with New Commercial Spyware

By Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert

DECEMBER 6, 2017
RESEARCH REPORT #102

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Document Version: 1.0

Suggested Citation

Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. “Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware,” Citizen Lab Research Report No. 102, University of Toronto, December 2017.

Acknowledgements

This work was supported in part by the Center for Long Term Cybersecurity (CLTC) at UC Berkeley. Thanks also to Erik Zouave, Masashi Crete-Nishihata, Lex Gill, Etienne Maynier, Adam Senft, Miles Kenyon, Jawar Mohammed, Etana Habte, Henok Gabisa, and Felix Horne and Cynthia Wong from Human Rights Watch.

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

Key Findings

- This report describes how Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of our investigation, one of the authors of this report was also targeted.
- We found a public logfile on the spyware's command and control server and monitored this logfile over the course of more than a year. We saw the spyware's operators connecting from Ethiopia, and infected computers connecting from IP addresses in 20 countries, including IP addresses we traced to Eritrean companies and government agencies.
- Our analysis of the spyware indicates it is a product known as PC Surveillance System (PSS), a commercial spyware product with a novel exploit-free architecture. PSS is offered by Cyberbit -- an Israel-based cyber security company that is a wholly-owned subsidiary of Elbit Systems -- and marketed to intelligence and law enforcement agencies.
- We conducted Internet scanning to find other servers associated with PSS and found several servers that appear to be operated by Cyberbit themselves. The public logfiles on these servers seem to have tracked Cyberbit employees as they carried infected laptops around the world, apparently providing demonstrations of PSS to the Royal Thai Army, Uzbekistan's National Security Service, Zambia's Financial Intelligence Centre, the Philippine President's Malacañang Palace, ISS World Europe 2017 in Prague, and Milipol 2017 in Paris. Cyberbit also appears to have provided other demos of PSS in France, Vietnam, Kazakhstan, Rwanda, Serbia, and Nigeria.

1. Executive Summary

This report describes a campaign of targeted malware attacks apparently carried out by Ethiopia from 2016 until the present. In the attacks we document, targets receive via email a link to a malicious website impersonating an online video portal. When a target clicks on the link, they are invited to download and install an Adobe Flash update (containing spyware) before viewing the video. In some cases, targets are instead prompted to install a fictitious app called "Adobe PdfWriter" in order to view a PDF file. Our analysis traces the spyware to a heretofore unobserved player in the commercial spyware space: Israel's *Cyberbit*, a wholly-owned subsidiary of Elbit Systems. The spyware appears to be a product called *PC Surveillance System (PSS)*, recently renamed *PC 360*.

The attacks we first identified were targeted at Oromo dissidents based outside of Ethiopia, including the Oromia Media Network (OMN). Oromia is the largest regional ethnic state of Ethiopia by population and area, comprised mostly of the Oromo people.

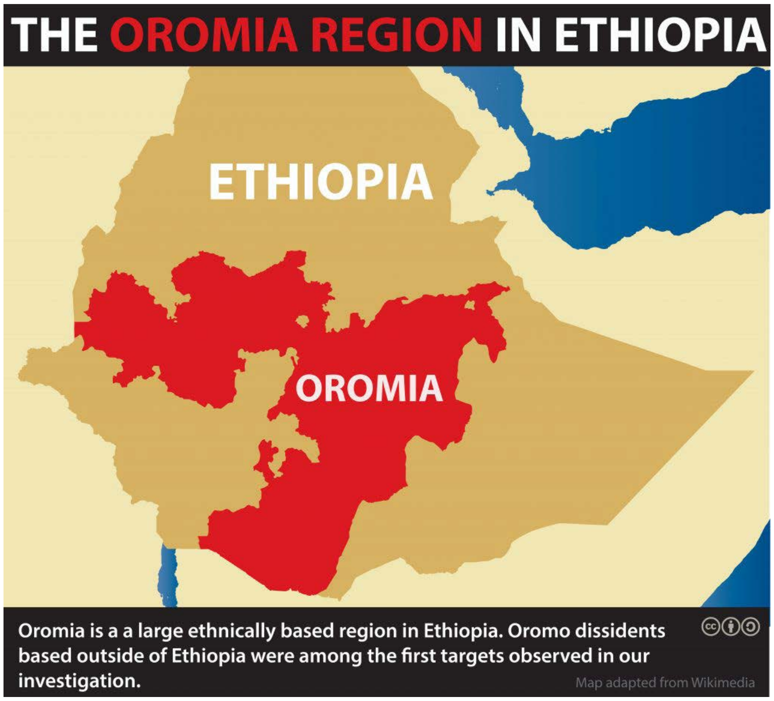

THE OROMIA REGION IN ETHIOPIA
ETHIOPIA
OROMIA
Oromia is a a large ethnically based region in Ethiopia. Oromo dissidents based outside of Ethiopia were among the first targets observed in our investigation.
Map adapted from Wikimedia

Figure 1: Oromia Region, Ethiopia

We later discovered that the spyware's command and control (C&C) server has a public logfile that appears to show both operator and victim activity, allowing us to gain insight into the identity of the operators and the targets. Based on our analysis of the logfile, it appears that the spyware's operators are inside Ethiopia, and that victims also include various Eritrean companies and government agencies.

We scanned the Internet for similar C&C servers and found what appear to be several servers used by Cyberbit. The public logfiles on those servers seem to have tracked Cyberbit employees as they carried infected laptops around the world, apparently providing demonstrations of PSS to various potential clients. The logfiles appear to place Cyberbit employees at IP addresses associated with the Royal Thai Army, Uzbekistan's National Security Service, Zambia's Financial Intelligence Centre, the Philippine President's Malacañang Palace, ISS World Europe 2017 in Prague, and Milipol 2017 in Paris. Cyberbit also appears to have provided other demos to clients we could not identify in France, Vietnam, Kazakhstan, Rwanda, Serbia, and Nigeria.

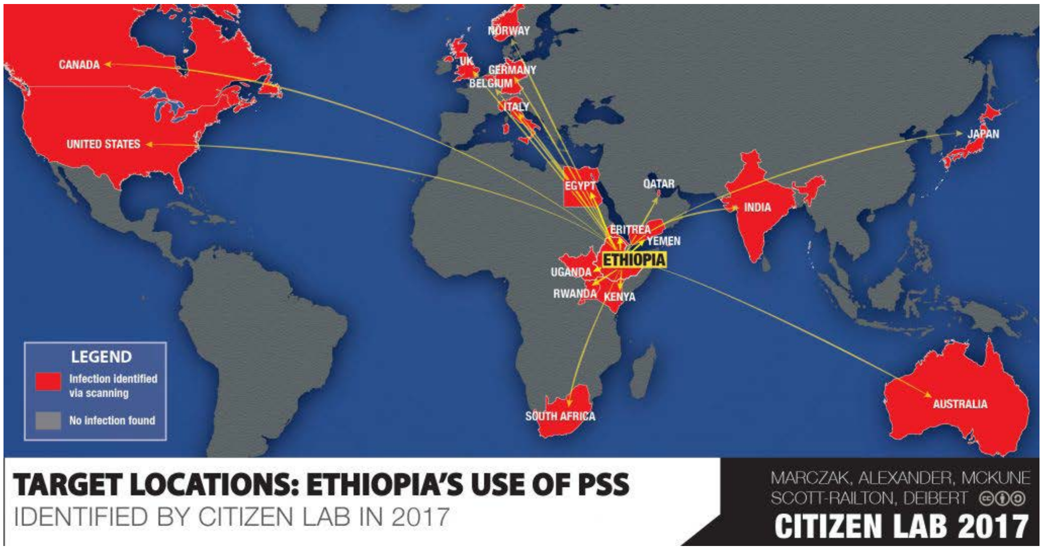


Figure 2: Countries with Ethiopian Cyberbit targets.

This report is the latest in a growing body of work that shows the wide abuse of nation-state spyware by authoritarian leaders to covertly surveil and invisibly sabotage entities they deem political threats. After FinFisher, Hacking Team, and NSO Group, Cyberbit is the fourth vendor of nation-state spyware whose tools we have seen abused, and the second based in Israel. Cyberbit's PSS is also not the first spyware that Ethiopia has abused outside of its borders: in 2015, we discovered that Ethiopia's Information Network Security Agency (INSA) was using Hacking Team's RCS spyware to target US-based journalists at the Ethiopian Satellite Television Service (ESAT). Ethiopia has also previously targeted dissidents using FinFisher's FinSpy spyware.

Citizen Lab has published a companion post outlining some of the legal and regulatory issues raised by this investigation. We also sent letters to Cyberbit and Adobe concerning the misuse of their respective products. Cyberbit responded on December 5, 2017, stating in part: *"we appreciate your concern and query and we are* *addressing it subject to the legal and contractual confidentiality obligations Cyberbit Solutions is bound by."* Adobe responded on December 6, 2017, stating in part: *"we have taken steps to swiftly address this issue, including but not limited to contacting Cyberbit and other relevant service providers."*

2. Background

2.1. Oromo Protests and Diaspora Media Outlets

Largely peaceful protests erupted in the Ethiopian state of Oromia in November 2015, in response to a government decision to pursue a development project involving the razing of a forest and football field. Protesters coalesced around opposition to a larger plan, the Addis Ababa Master Plan, which they feared would displace some of the 2 million Oromo residents living around Addis Ababa. The government labeled the protesters terrorists and responded with lethal force and arbitrary arrests. Over the next year, security forces killed over 1000 people, many of them from Oromia, during anti-government protests. This culminated in a state of emergency that was called in October 2016 that lasted over 10 months.

Oromia Media Network (OMN) is a US-based media channel that describes itself as an *"independent, nonpartisan and nonprofit news enterprise whose mission is to produce original and citizen-driven reporting on Oromia, the largest and most populous state in Ethiopia."* OMN broadcasts via satellite, and also has an Internet and social media presence. According to Human Rights Watch, OMN *"played a key role in disseminating information throughout Oromia during the protests."* The government has *"reportedly jammed OMN 15 times since it began operations in 2014"* and arrested individuals for providing information to OMN or displaying the channel in their businesses.

2.2. Cyberbit and PSS

Cyberbit is an Israel-based cyber security company and a wholly-owned subsidiary of Israeli defense and homeland security manufacturer and contractor Elbit Systems. Cyberbit was established in 2015 in order to *"consolidate Elbit Systems' activities relating to the Cyber Intelligence and Cyber Security markets."* Cyberbit merged with the NICE Cyber and Intelligence Division in 2015 after Elbit acquired that entity for approximately $158 million, with Cyberbit reportedly taking on the division's employees. Elbit had previously acquired *C4 Security* in June 2011 for $10.9 million; C4 described itself as *"specializ[ing] in information warfare, SCADA and military C&C syste*ms security." According to one employee's LinkedIn page, C4 also developed a product called *"PSS Surveillance System,"* billed as a *"solution[] for intelligence and law enforcement agencies."* Cyberbit marketing materials1 refer to what appears to be the same system: *"CYBERBIT PC Surveillance System (PSS)."* PSS is also referenced on Elbit's website as a solution *"for collection from personal computers."* Elbit reportedly will be reorganizing Cyberbit, effective as of 2018, to separate its defense and commercial businesses, with Cyberbit continuing to operate the *"C4i division and commercial cyber business."* Elbit's major subsidiaries are located in Israel and the United States, and Elbit is listed on the NASDAQ and the Tel Aviv Stock Exchange.

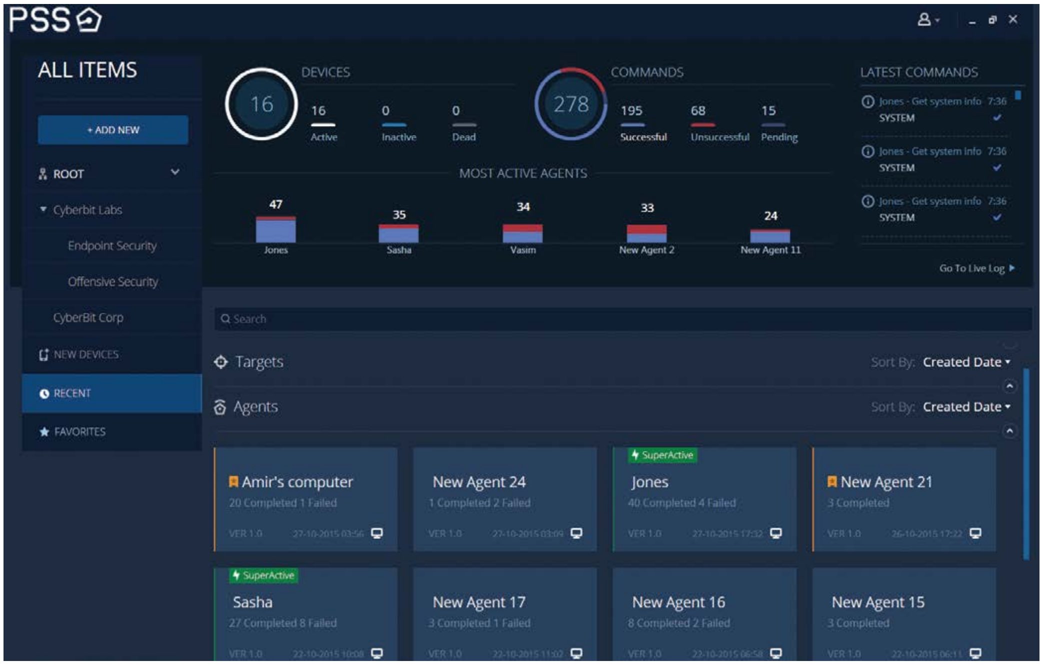

PSS
ALL ITEMS
+ ADD NEW
ROOT
Cyberbit Labs
Endpoint Security
Offensive Security
CyberBit Corp
NEW DEVICES
RECENT
FAVORITES
DEVICES
16
16 Active
0 Inactive
0 Dead
COMMANDS
278
195 Successful
68 Unsuccessful
15 Pending
MOST ACTIVE AGENTS
47 Jones
35 Sasha
34 Vasim
33 New Agent 2
24 New Agent 11
LATEST COMMANDS
Jones - Get system info 7:36 SYSTEM ✓
Jones - Get system info 7:36 SYSTEM ✓
Jones - Get system info 7:36 SYSTEM ✓
Go To Live Log
Search
Targets
Sort By: Created Date
Agents
Sort By: Created Date
Amir's computer 20 Completed 1 Failed VER 1.0 27-10-2015 03:56
New Agent 24 1 Completed 2 Failed VER 1.0 27-10-2015 03:09
SuperActive Jones 40 Completed 4 Failed VER 1.0 27-10-2015 17:32
New Agent 21 3 Completed VER 1.0 26-10-2015 17:22
SuperActive Sasha 27 Completed 8 Failed VER 1.0 22-10-2015 10:08
New Agent 17 3 Completed 1 Failed VER 1.0 22-10-2015 11:02
New Agent 16 8 Completed 2 Failed VER 1.0 22-10-2015 06:58
New Agent 15 3 Completed VER 1.0 22-10-2015 06:11

Figure 3: Screenshot of PSS Console (Source: Cyberbit Marketing Materials).

Cyberbit is the second Israel-based nation-state spyware vendor we have identified and analyzed, the other being NSO Group. The two companies operate in the same market and have even been connected with the same clients. In an extradition request for former Panamanian President Martinelli, Panama alleged that Martinelli had directed the purchase of two spyware products: PSS and NSO Group's Pegasus.

[1] We found these materials in a Google search. The materials are hosted in an Amazon S3 bucket whose name is cyberbit. Inspecting the source code of Cyberbit's website (https://web.archive.org/web/20170930094240/https://www.cyberbit.com/) yields several references to the same S3 bucket. Thus, we assume Cyberbit controls the S3 bucket named cyberbit and that the marketing materials are Cyberbit originals.

Additionally, a leaked Hacking Team email about NSO claims that: *"NSO only has mobile agents … Apparently the pc part is handled by another company, PSS."* Cyberbit describes PSS as *"a comprehensive solution for monitoring and extracting information from remote PCs."* As is standard in the marketing materials for spyware companies, Cyberbit represents that their design *"eliminat[es] the possibility that the operation will be traced back to the origin."*

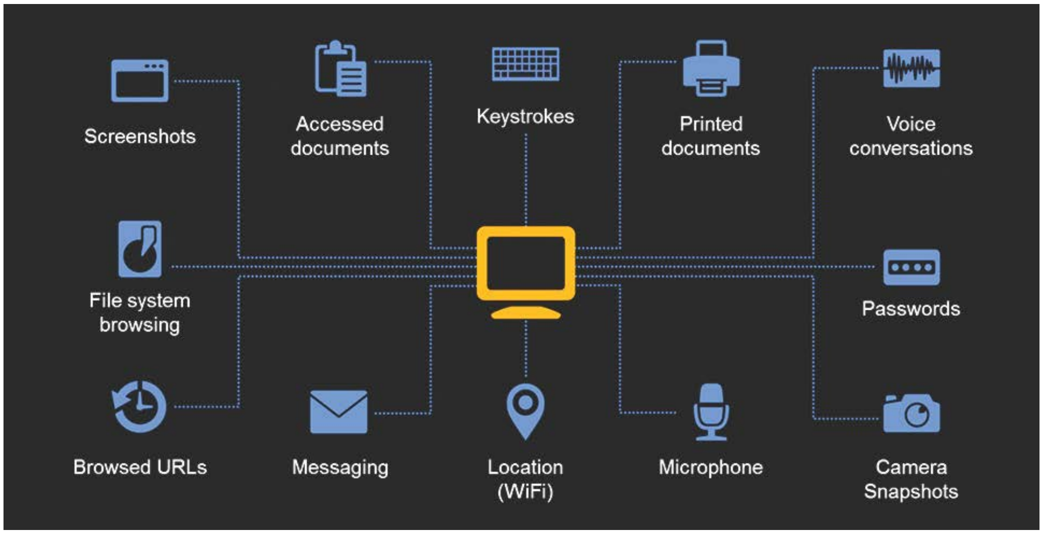


Figure 4: Data exfiltrated by PSS (Source: Cyberbit Marketing Materials).

Cyberbit says that PSS *"helps LEAs and intelligence organizations to reduce crime, prevent terrorism and maintain public safety by gaining access, monitoring, extracting and analyzing information from remote PCs."* Information that PSS can monitor and extract includes *"VoIP calls, files, emails, audio recordings, keylogs and virtually any information available on the target device."*

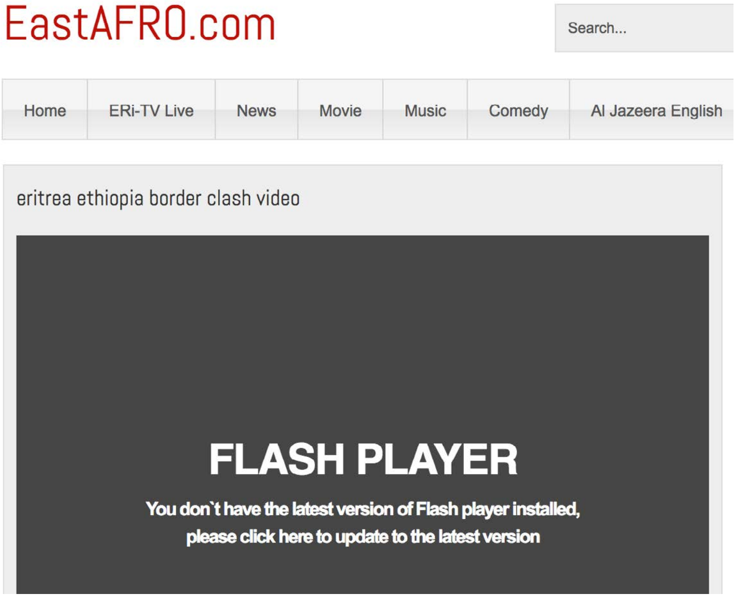
3. Targeting of Jawar Mohammed

Jawar Mohammed is the Executive Director of the Oromia Media Network (OMN). He is also a prolific activist, with more than 1.2 million followers on Facebook. October 2, 2016 was the annual Irreecha cultural festival, the most important Oromo cultural festival. Millions of people each year gather at the festival site in Bishoftu, near Addis Ababa. In 2016, *"scores of people"* died at the festival *"following a stampede triggered by security forces' use of teargas and discharge of firearms in response to an increasingly restive crowd."* Jawar was active at the time on social media in stoking the passions of Oromo on the ground, circulating both verified and unverified information. On October 4, 2016, while in Minneapolis, USA, Jawar received the email in **Figure 5**. He forwarded the email to Citizen Lab for analysis.

From: sbo radio <sbo.radio88[@]gmail.com>
Date: Tue, 4 Oct 2016 16:50:13 +0300
Subject: Fw: Confidential video made publicWhat do you think of this video ? In case you don't have the right version of adobe flash and can't watch the video, you can get the latest version of Adobe flash from Here
http://getadobeplayer[.]com/flashplayer/download/index7371.html.---------- Forwarded message ----------
From: sbo radio <sbo.radio88[@]gmail.com>
Date: Tue, Oct 10, 2014 at 4:23 PM
Subject: Video hints Eritrea and Ethiopia war is highly likely to continueDear Excellencies,Video : Eritrea and Ethiopia war likely to continue
http://www.eastafro[.]net/eritrea-ethiopia-border-clash-video.htmlregards,Sbo Radio
Mit freundlichen Grüßen

Figure 5: An email sent to Jawar on October 4, 2016. The sender most likely crafted the email to make it appear that this was a forwarded message.

The site **eastafro[.]net** appears to impersonate the (legitimate) Eritrean video website eastafro.com. When a target clicks on an operator-generated link to eastafro[.]net, JavaScript on the site checks to see whether the target is using Windows and whether their Adobe Flash Player is up to date. If the script detects a Windows user with an out-of-date Flash Player, it displays a message asking the user to update their Flash Player. If clicked, or after 15 seconds, the user is redirected to a page on **getadobeplayer[.]com**, which offers the user a real Flash Player update bundled with spyware.



You don`t have the latest version of Flash player installed, please click here to update to the latest version

Figure 6: Message displayed when a target clicks on a link to eastafro[.]net.

If the user downloads and installs the malicious Flash update, their computer is infected. It is clear that this is a targeted attack: if a user simply types in eastafro[.]net into their browser's address bar, they are redirected to the legitimate site, eastafro.com. If a user does the same with getadobeplayer[.]com, they are served a "403 Forbidden" message. Both sites have robots.txt files instructing search engines not to crawl them. Access to the spyware is granted only if the user clicks on a link sent by the operator.

In all, Jawar received eleven emails between 5/30/2016 and 10/13/2016, and one more than a year later on 11/22/2017. Each email contained links to what were purportedly videos on **eastafro[.]net**, or Adobe Flash Player updates on **getadobeplayer[.]com**. The 11/22/2017 email contained a link to eastafro[.]net that asked the target to install "Adobe's PdfWriter," a fictitious product. The download contained the same spyware as the malicious Adobe Flash Player updates, but was packaged with CutePDF Writer, *"a proprietary Portable Document Format converter and editor for Microsoft Windows developed by Acro Software,"* with no connection to Adobe.

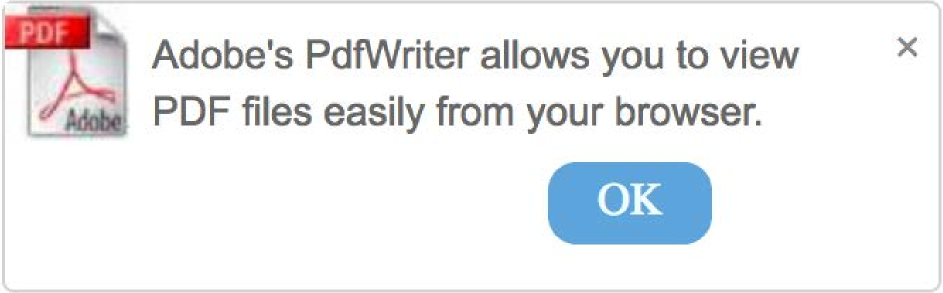

Adobe's PdfWriter allows you to view PDF files easily from your browser.

Figure 7: "Adobe PdfWriter" Installation Prompt.

In many cases, the operators appear to have registered their own accounts to send the infection attempts. However, the email address sbo.radio88[@]gmail.com used by operators to target Jawar is associated with the radio station of the Oromo Liberation Front (OLF). The account may have been compromised.

Date	Subject	Sender
5/30/2016	Ethiopia Struggling with inside Challenges!	eliassamare[@]gmail.com
6/15/2016	Tsorona Conflict Video!	eliassamare[@]gmail.com
6/29/2016	UN Report and Diaspora Reaction!	eliassamare[@]gmail.com
8/4/2016	Ethiopia and Current Options!	eliassamare[@]gmail.com
8/15/2016	Fwd: Triggering Ethiopia Protests!	eliassamare[@]gmail.com
9/5/2016	Saudi-Iran and the Red Sea!	eliassamare[@]gmail.com

Date	Subject	Sender
9/6/2016	Congrats – የኢሳት ፍሬዎች	wadewadejoe[@]gmail.com
9/22/2016	Is Funding Ethiopia the Right time Now?	eliassamare[@]gmail.com
10/4/2016	Fw: Confidential video made public	sbo.radio88[@]gmail.com
10/10/2016	Egypt-Ethiopia new tension!	awetnaeyu[@]gmail.com
10/13/2016	Confidential Videos made public	wadewadejoe[@]gmail.com
11/22/2017	Gov official interrogated following leakage of national security meeting minutes	lekanuguse2014[@]gmail.com

Table 1: Malicious emails received by Jawar.

The Ethiopian Government charged Jawar with terrorism in February 2017 under the criminal code; Jawar and OMN denied all charges.

4. Investigation to Find Additional Targets

We set out to find additional targets. We conducted targeting testing of members of the Oromo community using Himaya, our email scanning tool, to determine whether they had received any similar malicious messages. We also found a public logfile on the spyware's C&C server (Section 5.2); the logfile listed IP addresses of infected devices and we were able to identify additional victims based on their IP.

4.1. Other Targets

Etana Habte is a PhD candidate and Senior Teaching Fellow at SOAS, University of London. He is a frequent commentator on Ethiopian issues and appears regularly on OMN.

Date	Subject	Sender
12/9/2016	Let’s stop EU & the World Bank from funding $500 m to Ethiopia	shigut.gelleta[@]gmail.com
1/11/2017	Fwd: MONOSANTO (A multinational company)’s plan on Oromia	networkoromostudies2015[@]gmail.com

Table 2: Malicious emails received by Etana.

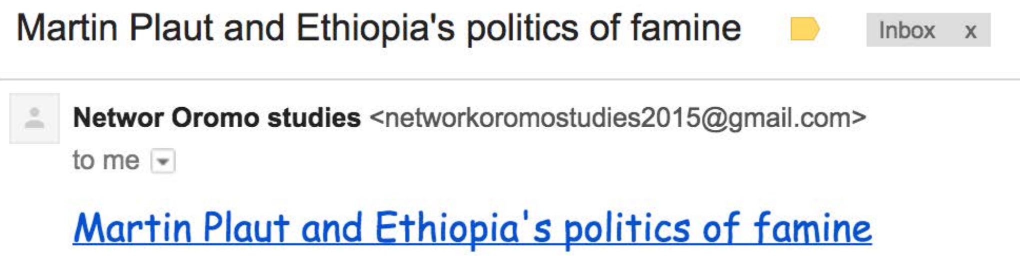
The address shigut.gelleta@gmail.com appears to be an account created by attackers designed to impersonate Shigut Geleta, a member of the OLF.

Dr. Henok Gabisa is a Visiting Academic Fellow who teaches at Washington and Lee University School of Law and is the founder of the Association of Oromo Public Defenders (Public Interest Lawyers Association) in Oromia.

Date	Subject	Sender
3/6/2017	Why did MONOSANTO target the Oromiya region?	networkoromostudies2015[@]gmail.com
3/13/2017	Democracy in Ethiopia: Can it be saved?	networkoromostudies2015[@]gmail.com

Table 3: Malicious emails received by Henok.

Bill Marczak is a researcher at Citizen Lab and an author of this report. Marczak was targeted after he asked another target to forward an email sent by operators. At the time, the target's email account was compromised (the target had been previously infected with this spyware). On March 29, 2017, while in San Francisco, USA, Marczak received a message entitled "Martin Plaut and Ethiopia's politics of famine," from networkoromostudies2015[@]gmail.com. The email contained a link to eastafro[.]net.



Martin Plaut and Ethiopia's politics of famine

Networ Oromo studies <networkoromostudies2015@gmail.com>
to me

Martin Plaut and Ethiopia's politics of famine

Figure 8: Message received by Citizen Lab Senior Research Fellow Bill Marczak. The use of the Comic Sans font is due to the attacker's font selection.

Other Targets: Several malicious emails we found were sent to multiple receipients, according to their headers. We found 39 additional email addresses of targets using this method; at least 12 addresses appear to be linked to targets active on Oromo issues, or working for Oromo groups.

4.2. Logfile Analysis

Peculiarly, we found a public logfile on the spyware's C&C server; the logfile recorded activity that allowed us to geolocate (or in some cases, identify) victims. We analyzed more than a year of logs showing victim (and operator) activity. Each logfile entry contains a unique identifier (a GUID) associated with the infection, a value indicating whether the entry records victim or operator activity, the IP address that the infected device (or operator) connected to the C&C server from, and finally a timestamp showing when the communication took place (for more details on the logfile, see **Section 4.3**). The format of the logfile allowed us to track infections as they moved between different IP addresses, such as when an infected target carried their laptop between home and work, or while traveling.

During more than a year of monitoring the server's logfiles, we observed 67 different GUIDs. All infections were operated by the same operator, who only ever used one IP address, which belongs to a satellite connection (except for a three hour period on a single day when the operator's activity "failed over" to two other IP addresses, one address in Ethiopia and one VPN, perhaps due to transient satellite connection failure). We identified 11 of the 67 GUIDs as likely resulting from testing by the operator, or execution by researchers, based on their apparent short duration. Further, we noted that some GUIDs likely referenced the same infected device, as they represented consecutive, non-overlapping infections whose IP addresses corresponded with the same Internet Service Provider (ISP). This was the case for two GUIDs in the UK, two in South Sudan, and 12 in Uganda.

We arrived at 43 GUIDs that we believe represent distinct infected devices. We then sought to geolocate each infection to a country. We first ran the MaxMind GeoLite 2 Country database on each IP and associated a set of countries with each infection. For each infection that had only one country associated with it, we examined a small number of IP addresses from the infection, to see whether those IPs looked like they were actually in that country, or whether geolocation may have been incorrect due to the IP being associated with a VPN or satellite connection.

For infections that MaxMind associated with multiple countries, we determined the dominant country, based on the country with the largest number of logfile entries for that infection. For the dominant country, we checked a small number of IP addresses to make sure the geolocation was correct. For the other countries, we checked each IP in an attempt to eliminate incorrect geolocation. We noted four infections that predominantly connected from satellite connections, which MaxMind geolocated to UK or UAE; we changed the geolocation of these devices to Eritrea, as the infections either "failed over" to IPs registered to EriTel, or shared the same satellite IP address as other infections that "failed over" to EriTel IPs.

Country	# Infected Devices
Eritrea	7
Canada	6
Germany	6
Australia	4
USA	4
South Africa	2

Table 4: Number of infections we geolocated to each country, for countries where we geolocated more than one infection.

Other countries in which we saw only a single infected device were: Belgium, Egypt, Ethiopia, UK, India, Italy, Japan, Kenya, Norway, Qatar, Rwanda, South Sudan, Uganda, and Yemen.

After we eliminated VPN IPs, and geolocated the four infections that predominantly connected from satellite connections, we found that 40 of 43 infections only ever communicated from a single country. The remaining three devices appear to have travelled between several countries. The three infections that traveled internationally are as follows:

- A device that twice travelled from Eritrea (via Germany) to the United Nations in Geneva. We geolocated this device to Eritrea.
- A device that predominantly connected from the University of Tsukuba in Japan that travelled to Eritrea. We geolocated this device to Japan.
- A device that predominantly connected from York University in Canada that travelled to Eritrea. We geolocated this device to Canada.

We were able to trace six of the infections (five in Eritrea, one abroad) to Eritrean government agencies or companies, suggesting that operators are likely targeting members of the Eritrean government in addition to Ethiopian dissidents.

4.3. Other Attacker Sites

During our analysis, we identified two other websites sharing the same IP address as getadobeplayer[.]com, which also appear to have been used by the same attackers to target victims with the same spyware: **diretube.co[.]uk** (impersonating **diretube[.]com**, an Ethiopian video site), and **meskereme[.]net** (impersonating **meskerem[.]net**, an Eritrean opposition website).

The **diretube.co[.]uk** site used the same Adobe Flash update ploy to direct users to malware on getadobeplayer[.]com, whereas the **meskereme[.]net** site displays a message saying "Problem reading Tigrinya? Install these fonts," with links to the fonts bundled with spyware. The legitimate website, meskerem[.]net displays the same message, but links to fonts without the spyware.

5. Attribution to Cyberbit and Ethiopia

This section describes how we attributed the spyware to Cyberbit and Ethiopia.

5.1. Digital Signature Points to Cyberbit

By monitoring getadobeplayer[.]com, we found and analyzed five samples of the spyware as it was updated over time.

MD5	Name
568d8c43815fa9608974071c49d68232	flashplayer20_a_install.exe
80b7121c4ecac1c321ca2e3f507104c2	flashplayer21_xa_install.exe
8d6ce1a256acf608d82db6539bf73ae7	flashplayer22_xa_install.exe
840c4299f9cd5d4df46ee708c2c8247c	flashplayer23_xa_install.exe
961730964fd76c93603fb8f0d445c6f2	flashplayer24_xa_install.exe

Table 5: The samples from getadobeplayer[.]com that we analyzed.

Each sample communicates with two command and control (C&C) servers: **time-local[.]com** and **time-local[.]net**.

We found a structurally similar sample (see **Section 7** for details on structural similarities) in VirusTotal:

```
MD5: 376f28fb0aa650d6220a9d722cdb108d
SHA1: c7b4b97369a2ca77e916d5175d162dc2b823763b
SHA256: c76d2a8c1c8865b1aa6512e13b77cbc7446022b7be3378f7233c5ca4a5e58116
```

That sample communicated with a C&C server at the following URL: **pssts1.nozonenet[.]com/ts8/ts8.php** (note the use of "PSS" in the URL). The sample also drops an EXE file containing a digital signature (valid as of the date submitted to VirusTotal) produced by a certificate with the following details:

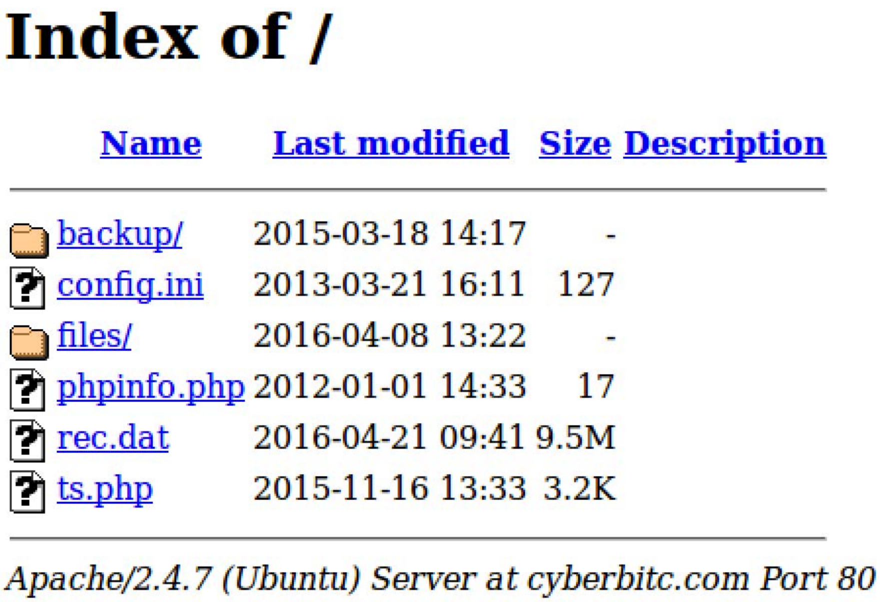
```
CN = C4 Security
O = C4 Security
STREET = 13 Noach Mozes St
L = Tel aviv
S = Gush Dan
PostalCode = 67442
C = IL
RFC822 Name=tal.barash@c4-security.com
```

Note that **c4-security.com** was the official website of C4 security, according to a brochure posted on the website of the Israeli Export Institute.

5.2. Public Logfile Analysis Points to Ethiopia and Cyberbit

While monitoring additional PSS C&C servers that we discovered during scanning (**Section 6.1**), we found that one of these servers temporarily exposed a directory listing in response to a normal GET / HTTP/1.1 request (**Figure 9**). The directory listing contained the text: "Apache/2.4.7 (Ubuntu) Server at cyberbitc[.]com Port 80," indicating that the server was associated with Cyberbit. The website **cyberbitc[.]com** is owned by Cyberbit and was used by Cyberbit before they acquired **cyberbit[.]com** in March 2017.[2]

[2] In January 2016, Cyberbit attempted to convince the WIPO Arbitration and Mediation Center to transfer the domain to it from Cyberbit A/S, but the panel refused and declared that Cyberbit had engaged in reverse domain name hijacking by bringing its complaint in bad faith. However, Cyberbit apparently purchased the domain in March 2017, judging by WHOIS records.



```
Index of /

     Name          Last modified     Size  Description
----------------------------------------------------------
  backup/         2015-03-18 14:17     -
  config.ini      2013-03-21 16:11   127
  files/          2016-04-08 13:22     -
  phpinfo.php     2012-01-01 14:33    17
  rec.dat         2016-04-21 09:41  9.5M
  ts.php          2015-11-16 13:33  3.2K
----------------------------------------------------------
Apache/2.4.7 (Ubuntu) Server at cyberbitc.com Port 80
```

Figure 9: Directory listing on one of the servers that earlier matched our fingerprint.

This directory listing also revealed the existence of several files, including a file called rec.dat, which at first glance we noticed was encoded in binary format. We suspected that rec.dat might be a logfile, as it appeared to be constantly updated on the C&C servers. We noticed that rec.dat existed on all of the C&C servers we detected in our scanning and were able to test (**Section 6.1**), including on time-local[.]com and time-local[.]net, the C&C servers associated with the spyware samples sent to Oromo targets.

5.2.1. Logfile Analysis Shows Ethiopian Operator

To verify our logfile hypothesis, we performed a test infection of a virtual machine using one of the samples sent to Oromo targets and we allowed the virtual machine to communicate with the C&C server. The traffic comprised HTTP POST requests (**Section 7.7**), each of which contained an agentid, a GUID initially {00000000-0000-0000-0000-000000000000} and later nonzero.

After the infection, we downloaded rec.dat and found that it contained a series of records, several with our IP address, and our agentid GUID, in binary form. Each record of the logfile is delimited by the string \x41\x41\x41 ('AAA') and can be parsed with the following regular expression:

```
'(.{4})\x00\x00(.)(.{4})(.{16})AAA'
```

The first group of four bytes is a UNIX timestamp, the second group of 1 byte is a *type* value (which, in our testing was always 2, 17, 21, 33, or 37), the third group of 4 bytes is an IP address, and the fourth group of 16 bytes is a GUID. The file appears to be a circular (i.e., size-capped) logfile stored in binary format whose maximum size is defined in config.ini to be 10MB. Old entries are removed from the front of the file as new entries are written to the end.

Peculiarly, we noticed additional entries in rec.dat with our GUID but with a different IP address, 207.226.46.xxx. We noticed that 207.226.46.xxx was also associated with every other GUID in rec.dat. We determined that this IP address is associated with a satellite connection.

Over a period of more than a year, we downloaded and analyzed this file at regular intervals, obtaining a total of 388 rec.dat samples from each of time-local[.]com and time-local[.]net (we also began pulling samples of rec.dat from new servers we detected in scanning). Our rec.dat files from time-local[.]com contain more than 32 million entries (more than 28 million entries are operator interactions and approximately 4 million are victim interactions).

In all of our rec.dat samples from time-local[.]com and time-local[.]net, we noted that entries in the logfile for all GUIDs with types 2, 21, and 33 only ever involved the IP address 207.226.46.xxx (except for a brief period of three hours on a single day, where we saw the activity "fail over" between 207.226.46.xxx and two other IP addresses, one VPN address, and one address in Ethiopia). Thus, we suspect that types 2, 21, and 33 represent interaction by the operator. We suspect that types 17 and 37 correspond to interactions by infected devices.

IP	Provider
207.226.46.xxx	Satellite Connection
197.156.86.xxx	Ethio Telecom
192.186.133.xxx	CyberGhost VPN

Table 6: IP addresses that the Ethiopian operator connected from.

That the attacker's activity "failed over" between their satellite IP and an Ethio Telecom address suggests that the operator is inside Ethiopia.

5.2.2. Thirteen Servers Show a Cyberbit Nexus

Our scanning found 15 PSS C&C servers in all. Of those, two were the Ethiopia servers. Of the remaining 13 we found, we suspect all are operated by Cyberbit, perhaps as demonstration or development servers. Ten of the servers' logfiles included the IP address 37.142.120.xxx, which is pointed to by a subdomain of cyberbit[.]net. Two other servers' logfiles included the IP address 64.251.13.xxx, which also appeared in the logfile of one of the seven servers, as an operator of infections connecting back from 37.142.13.xxx, an IP address pointed to by a subdomain of cyberbit[.]net.

One of the servers, pupki[.]co, was unavailable when we tried to fetch rec.dat. The domain name was registered to a "Yevgeniy Gavrikov". An individual by this name currently works as an "integration specialist" for Cyberbit, according to LinkedIn.

6. Other PSS Activity

6.1. Scanning for More C&C Servers

We fingerprinted the command and control (C&C) servers used by the spyware, **time-local[.]com** and **time-local[.]net**, based on the fact that they typically returned the following distinctive message upon a normal GET / HTTP/1.1 request:

```
PHP Configuration Error. Can not fetch xml request string
```

Over the course of our scanning, we found a total of 15 IP addresses matching this same fingerprint.

C&C IP Address	Domain Name[3]
51.15.48.xxx	
80.82.64.32	time-local[.]com
80.82.67.xxx	
80.82.79.44	time-local[.]net
89.248.170.xxx	
93.174.89.xxx	
93.174.91.xxx	
93.174.91.xxx	
94.102.53.xxx	
94.102.60.xxx	
94.102.63.xxx	
104.236.23.3	pupki[.]co

[3] We redact the domain names of non-Ethiopia servers that are still online.

C&C IP Address	Domain Name[3]
111.90.147.xxx	
185.125.230.xxx	
185.125.230.xxx	

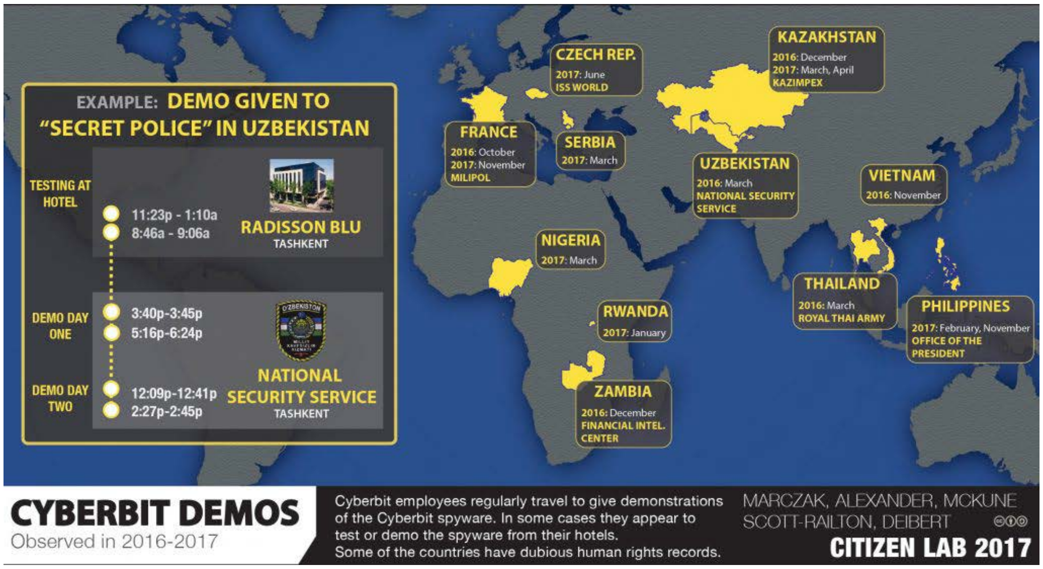
Table 7: PSS C&C servers we found in IPv4 scanning.

6.2. Demonstration Websites

By examining sites on the same IP address as eastafro[.]net, we found two additional sites: one site impersonating Download.com and one website impersonating the homepage of Avira Antivirus. These sites contained versions of several apps bundled with PSS, including Avira Antivirus, Ventrilo, Avast AntiVirus, and CCleaner. The versions of PSS we found talked to C&C servers in the list above that we identified as Cyberbit-run servers.

6.3. Public Logfile Analysis of Other Servers

In addition to the Ethiopia servers (**Section 5.2**), we analyzed the logfiles of 12 of the 13 other servers. We were able to identify what we believe are several product demonstrations to various clients around the world. Most of the demonstrations show similar patterns: activity during business hours from IP addresses that appear to belong to potential clients and activity off-hours at IP addresses that appear to belong to hotels. In a few cases, the activity is preceded or followed by activity from what appears to be airport Wi-Fi access points.



Cyberbit employees regularly travel to give demonstrations of the Cyberbit spyware. In some cases they appear to test or demo the spyware from their hotels. Some of the countries have dubious human rights records.

Figure 10: Cyberbit product demonstrations suggested by C&C logfiles.

In our analysis here, we introduce a notion of a *period of activity* to try and abstract away gaps between logfile entries that may be uninteresting. We say that a spyware infection is *active* between two logfile entries (we only include activity from the infected device here, i.e., types 17 and 37) if there is no more than an hour in between the entries. We omit periods of activity that are less than one minute from our consideration (except if they provide evidence that the infected device has moved). In each country case we present here, we are listing *all* the activity we found across the nine Cyberbit-operated C&C servers (perhaps excluding periods of activity less than a minute).

6.3.1. Timeline of Suspected Demonstrations

3/2016: Thailand (2 days). We found infections in Thailand from the IP 202.29.97.X, in AS4621, which appears to be an ASN used by various Thai universities. Tracerouting to 202.29.97.X yields the hop (royal-thai-army-to-902-1-5-gi-09-cr-pyt.uni.net.th). The IPs 202.29.97.(X-3) and 202.29.97.(X-1) return a TLS certificate whose CN is a subdomain of signalschool[.]net, which is registered to the Royal Thai Army's Signal School. We did note that 202.29.97.X also appears to be a VPN. Nevertheless, it seems that the IP is under the control of the Royal Thai Army. We also observed each infection changing between several IPs that appear to belong to various mobile data providers.

The table below lists *periods of activity* for each infection; the first column (**#**) indicates the number of the infection; the second and third columns provide the minimum and maximum date and time of the period of activity (in the country's local time, accounting for DST); the fourth column provides the duration of the period of activity (H:MM:SS); and the fifth column lists the location where the activity took place (or the likely identity of the agency receiving the demonstration).

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 09:22:17	Day 1 10:07:05	0:44:48	Royal Thai Army
2	Day 1 14:52:10	Day 1 15:38:13	0:46:03	Royal Thai Army
3	Day 2 14:45:51	Day 2 17:01:11	2:15:20	Royal Thai Army

Table 8: March 2016 suspected demo to Royal Thai Army.

3/2016: Uzbekistan (3 days). We found four infections in Uzbekistan. The first two were from an IP address pointed to by a subdomain of rdhotel[.]uz, which is registered by an individual who is listed on LinkedIn as the manager of the Radisson Blu in Tashkent. The latter two were from an IP address linked to Uzbekistan's National Security Service by the leaked Hacking Team emails.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 23:26:52	Day 2 00:10:00	0:43:08	Radisson Blu Tashkent
2	Day 2 08:46:20	Day 2 09:06:36	0:20:16	Radisson Blu Tashkent
3	Day 2 15:40:02	Day 2 15:45:52	0:05:50	National Security Service
3	Day 2 17:16:32	Day 2 18:24:42	1:08:10	National Security Service
4	Day 3 12:09:17	Day 3 12:41:35	0:32:18	National Security Service
4	Day 3 14:27:04	Day 3 14:53:39	0:26:35	National Security Service

Table 9: March 2016 suspected demo to Uzbekistan National Security Service.

10/2016: France (1 day). We found two infections in France on the same day in October 2016. The first appeared to be from an IP address associated with the airport Wi-Fi at Paris's Charles De Gaulle (CDG) airport. The second was from what appeared to be a landline IP address in Paris, which we could not attribute.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 11:19:15	Day 1 11:24:04	0:04:49	CDG Airport Wi-Fi
2	Day 1 15:24:55	Day 1 16:08:03	0:43:08	86.245.198.xxx

Table 10: October 2016 suspected demo to unknown clients in France.

11/2016: Vietnam (2 days). We found three infections in Vietnam. One was linked to an IP address that is numerically adjacent to another IP address that returns a web interface for an "HP MSM760 Controller" that displays the following information:

```
System name: Hilton Gardent Inn-HANOP
Location: Hanoi
```

We suspect that this activity is associated with the Hilton Garden Inn Hotel in Hanoi. The other activity appears to be from mobile broadband IP addresses; the identity of the potential client is not indicated by the data.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 16:34:36	Day 1 18:52:09	2:17:33	Hilton Garden Inn Hanoi
1	Day 1 18:52:48	Day 1 19:01:12	0:08:24	(Mobile Broadband)

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 19:35:50	Day 1 19:41:14	0:05:24	Hilton Garden Inn Hanoi
2	Day 2 11:34:24	Day 2 12:12:26	0:38:02	(Mobile Broadband)
3	Day 2 15:32:15	Day 2 17:13:41	1:41:26	(Mobile Broadband)

Table 11: November 2016 suspected demo to unknown clients in Vietnam.

12/2016: Kazakhstan (1 day). We found an infection from an IP address registered (according to WHOIS information) to "Saad Hotel LLP" with an address matching the Marriott Hotel in Astana.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 14:20:07	Day 1 14:35:39	0:15:32	Marriott Hotel Astana

Table 12: December 2016 suspected demo to unknown clients in Kazakhstan.

12/2016: Zambia (2 days). Most of the activity was from mobile broadband IPs. However, the second infection was from an IP pointed to by a subdomain of fic.gov[.]zm, the website for Zambia's Financial Intelligence Centre.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 21:23:21	Day 1 21:57:52	0:34:31	(Mobile Broadband)
1	Day 2 05:20:05	Day 2 05:43:38	0:23:33	(Mobile Broadband)
2	Day 2 11:00:52	Day 2 11:29:37	0:28:45	Financial Intelligence Centre

Table 13: December 2016 suspected demo to Zambia Financial Intelligence Centre.

1/2017: Rwanda (2 days). We could not attribute any of the IPs in Rwanda.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 17:10:48	Day 1 18:28:47	1:17:59	(Unknown Loc 1)
1	Day 1 22:49:12	Day 1 23:27:30	0:38:18	(Unknown Loc 2)
2	Day 1 23:30:16	Day 2 04:18:06	4:47:50	(Unknown Loc 2)
3	Day 2 09:14:59	Day 2 09:27:34	0:12:35	(Unknown Loc 1)
4	Day 2 09:54:15	Day 2 10:51:47	0:57:32	(Unknown Loc 1)

#	Activity Start (Local)	Activity End (Local)	Duration	Location
5	Day 2 10:01:45	Day 2 12:54:13	2:52:28	(Unknown Loc 1)

Table 14: January 2017 suspected demo to unknown clients in Rwanda.

2/2017: Philippines (5 days). We found an infection in February 2017 at 116.50.244.15. The IPs 116.50.244.10, 116.50.244.7, and 116.50.244.8 are pointed to by manila.newworldhotels.com or subdomains thereof. 116.50.244.7 is a Cisco VPN login page, which lists the "Group" as "New_World_Makati." We assume that the Manila New World Makati Hotel is also the owner of 116.50.244.15.

This was followed by an infection one day later at an IP address pointed to by a subdomain of malacanang.gov[.]ph, which is the website of Malacañang Palace. The palace is the primary residence and offices of the Philippine President (Rodrigo Duterte as of the date of the demo). The Malacañang Palace infection was followed by an infection from two other IP addresses in the Philippines.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 18:40:13	Day 1 18:55:01	0:14:48	New World Makati Hotel Manila
2	Day 2 12:01:08	Day 2 12:25:50	0:24:42	Malacañang Palace
3	Day 3 11:32:08	Day 3 11:53:13	0:21:05	112.198.102.xxx
3	Day 5 21:52:32	Day 5 22:28:55	0:36:23	202.57.61.xxx

Table 15: February 2017 suspected demo to Philippines Presidency.

3/2017: Kazakhstan (1 day). We found an infection from an IP address pointed to by kazimpex[.]kz. According to an article on IntelligenceOnline, Kazimpex is said to be closely linked with the "National Security Committee of the Republic of Kazakhstan" (KNB), an intelligence agency in Kazakhstan.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 11:29:55	Day 1 12:03:32	0:33:37	Kazimpex

Table 16: March 2017 suspected demo to Kazimpex in Kazakhstan.

3/2017: Serbia (2 days). We found activity from Serbia on a single IP address registered to "NBGP Properties Doo," which is the trading name of an apartment complex and business centre located adjacent to the Crowne Plaza in Belgrade.

Both NBGP and the Crowne Plaza are owned by Delta Holding, a major Serbian company. It is possible that activity from the IP 79.101.39.101 includes activity from both NBGP and the Crowne Plaza.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 12:20:42	Day 1 12:55:11	0:34:29	Delta Holding Complex
1	Day 2 00:15:30	Day 2 00:33:06	0:17:36	Delta Holding Complex
2	Day 2 00:51:04	Day 2 01:15:15	0:24:11	Delta Holding Complex
2	Day 2 06:58:53	Day 2 07:41:58	0:43:05	Delta Holding Complex

Table 17: March 2017 suspected demo to unknown clients in Serbia.

3/2017: Nigeria (2 days). We found one infection in Nigeria from two IPs. We could not identify the IPs.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 16:38:52	Day 1 17:11:57	0:33:05	(Unknown Loc 1)
1	Day 1 18:21:41	Day 1 19:13:24	0:51:43	(Unknown Loc 1)
1	Day 2 10:26:20	Day 2 11:43:28	1:17:08	(Unknown Loc 2)

Table 18: March 2017 suspected demo to unknown clients in Nigeria.

4/2017: Kazakhstan (1 day). We found an infection from the Marriott hotel in Astana, followed by an infection from an IP pointed to by a subdomain of mcmr[.]kz, the website of "Mobil Realty," a commercial real estate management company.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 12:26:04	Day 1 12:37:55	0:11:51	Marriott Hotel Astana
2	Day 1 18:09:50	Day 1 18:21:54	0:12:04	Mobil Realty

Table 19: April 2017 suspected demo to unknown clients in Kazakhstan.

6/2017: ISS World Europe (2 days). We saw four infections between 6/14/2017 and 6/15/2017 from IP address 82.142.85.165 in the Czech Republic. ISS World Europe 2017 was held in Prague, Czech Republic from 6/13/2017 - 6/15/2017, and Cyberbit gave a presentation on 6/13/2017, according to the schedule. This same IP address appears in the headers of leaked Hacking Team emails sent by two employees on 6/3/2015 and 6/4/2015. These employees mentioned that they would be attending ISS World Europe on 6/3/2015, held at the same venue as the 2017 ISS World Europe.

The IP address 82.142.85.165 may be associated with the Clarion Congress Hotel in Prague (the ISS World Europe venue).

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	2017-06-14 13:17:46	2017-06-14 13:52:04	0:34:18	ISS World Europe
3	2017-06-14 16:45:04	2017-06-14 17:27:33	0:42:29	ISS World Europe
3	2017-06-15 07:18:23	2017-06-15 07:19:38	0:01:15	ISS World Europe
4	2017-06-15 08:17:18	2017-06-15 09:36:03	1:18:45	ISS World Europe

Table 20: June 2017 suspected demo at ISS World Europe in Prague.

6/2017: Zambia (2 days). Most of the activity was from mobile broadband IPs.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day 1 19:00:54	Day 1 19:38:34	0:37:40	(Mobile Broadband)
2	Day 2 09:44:48	Day 2 10:22:28	0:37:40	(Mobile Broadband)
3	Day 2 14:36:18	Day 2 15:00:00	0:23:42	(Mobile Broadband)
3	Day 2 21:59:59	Day 2 22:19:09	0:19:10	(Mobile Broadband)

Table 21: June 2017 suspected demo to unknown clients in Zambia.

11/2017: Philippines (6 days). In November 2017, we observed what appeared to be two different Cyberbit employees travelling together from Israel to the New World Makati Hotel in Manila.

The infections started out in Israel, one on 10/15/2017 and one on 11/2/2017. While in Israel, and during the workweek (Sunday to Thursday), both infections connected from what appears to be Cyberbit's office (37.142.13.xxx, pointed to by two subdomains of cyberbit[.]net) during business hours (roughly 09:00 - 18:00 local time). After hours, the infections connected back from what we believe are home IP addresses of the employees. Each infection connected back from different home IPs during overlapping periods, which leads us to believe that the two infections represent different Cyberbit employees. It appears that each employee was carrying an infected laptop between home and the office each day (perhaps for spyware development and testing purposes).

After they last connected from Israel, one infection connected 15 hours later from Hong Kong for six minutes, between 14:52 and 14:58 local time. The infections then connected from the Philippines (116.50.244.xxx) as early as 22:41 local time, suggesting a flight itinerary from Tel Aviv to Manila, by way of Hong Kong.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
1	Day -1 15:46:24	Day -1 15:46:24	0:00:00	(DSL IP in Israel)
1	Day 1 14:52:15	Day 1 14:58:04	0:05:49	(Hong Kong)
1	Day 1 23:00:03	Day 1 23:56:11	0:56:08	New World Makati Hotel Manila
1	Day 3 20:19:20	Day 3 21:01:09	0:41:49	New World Makati Hotel Manila
1	Day 4 14:42:43	Day 4 14:44:39	0:01:56	(Mobile Broadband)
1	Day 4 16:14:21	Day 4 18:31:40	2:17:19	(Mobile Broadband)
1	Day 4 20:54:47	Day 5 08:00:09	11:05:22	New World Makati Hotel Manila
1	Day 9 09:05:14	Day 9 12:59:54	3:54:40	Cyberbit

Table 22: Employee #1 traveling from Israel to Manila; suspected demo to unknown clients.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
2	Day -1 15:00:24	Day -1 17:32:38	2:32:14	(DSL IP in Israel)
2	Day 1 22:41:32	Day 2 00:00:08	1:18:36	New World Makati Hotel Manila
2	Day 3 20:49:07	Day 3 21:07:51	0:18:44	New World Makati Hotel Manila
2	Day 4 10:30:03	Day 4 18:24:22	7:54:19	(Mobile Broadband)
2	Day 5 10:32:42	Day 5 10:56:48	0:24:06	(Mobile Broadband)
2	Day 5 13:04:42	Day 5 15:43:05	2:38:23	(Mobile Broadband)
2	Day 6 15:56:27	Day 6 17:47:18	1:50:51	New World Makati Hotel Manila
2	Day 9 09:13:20	Day 9 18:56:35	9:43:15	Cyberbit

Table 23: Employee #2 traveling from Israel to Manila; suspected demo to unknown clients.

11/2017: Milipol Paris (4 days): From 11/21/2017 - 11/24/2017, we found an infection active from an IP address 185.113.160.20, which appears to be associated with the

Paris Nord Villepinte exhibition center. The IP is pointed to by several subdomains of villepinte2017.dynu[.]net and also by pnv.vipnetwork[.]fr. The Milipol Paris 2017 exhibition was held between 11/21 and 11/24 and the Paris Nord Villepinte exhibition center. Thus, it appears that Cyberbit employees were performing demos there.

#	Activity Start (Local)	Activity End (Local)	Duration	Location
3	Day 1 08:15:24	Day 1 09:18:21	1:02:57	Milipol Paris
3	Day 1 10:44:02	Day 1 13:21:09	2:37:07	Milipol Paris
3	Day 1 14:50:25	Day 1 15:32:46	0:42:21	Milipol Paris
3	Day 2 08:29:27	Day 2 17:01:11	8:31:44	Milipol Paris
3	Day 3 08:10:28	Day 3 09:34:09	1:23:41	Milipol Paris
3	Day 3 13:02:05	Day 3 14:59:37	1:57:32	Milipol Paris
3	Day 3 15:43:03	Day 3 17:02:29	1:19:26	Milipol Paris
3	Day 4 08:31:07	Day 4 10:43:35	2:12:28	Milipol Paris

Table 24: November 2017 suspected demo at Milipol Paris.

6.3.2. Suspected Researcher Activity

We found several short-lived infections on Cyberbit-operated servers that seem less likely to be purposeful infections and more consistent with activity by cybersecurity researchers or other testing activity. We group activity that is temporally similar below, though it is unclear if this activity is related.

We found one infection in the **UK** on 11/10/2016 lasting ~15s.

We found one infection from **Google** on 2/7/2017 (lasting 11m), followed by three infections in **Germany** on 2/7/2017 and 2/8/2017. In Germany, there was one initial infection 14 minutes after the Google infection, with a single pingback. 2h10m later, there was an infection lasting 1 minute. 13h later, there was an infection with a single pingback.

We found an infection with a single pingback from an IP address in **Everett, Washington, USA** on 10/17/2017. We found two overlapping infections in **Russia** on 10/18/2017 (~2m each), followed 20 minutes later by two infections in **China,** 45 minutes apart (~30s each). We found a ~20s infection in Canada on 10/19/2017.

We found an infection with a single pingback from an IP address registered to **Brandon University in Canada** on 10/31/2017. We found two infections in **Norway** on 11/1/2017 (one infection with a single pingback, and one infection 3m30s later lasting for ~20s).

6.3.3. Unexplained Activity

We found several infections on the Cyberbit-operated PSS C&C servers that were long-running, and not from VPN connections or from countries where Cyberbit has a known presence. Thus, this activity did not immediately seem to represent demonstrations or development activity. We found one infection in **Iran** between 9/20/2016 and 11/22/2016. We found one infection in **Canada** between 3/7/2017 and 11/22/2017. We found one infection in **Finland** between 5/26/2017 and 11/28/2017. We found one infection in **Indonesia** from 10/28/2017 to 11/10/2017. We found one infection in **Slovakia** from a single IP address active between 11/1/2017 and 12/1/2017. We found one infection in **Ethiopia** from 10/25/2017 to 12/1/2017, with no known overlap with the Ethiopia client's IP address space.

6.4. Spoofed Code Signing Certificates?

We identified several cases where we suspect that the spyware operators, or Cyberbit themselves, obtained digital certificates in the names of real companies, including an Israeli intellectual property law firm.

One malicious Adobe Flash executable we found used by the Ethiopian operator was signed by an authenticode certificate issued by Comodo to a named entity called "Flashpoint IP."

```
CN = Flashpoint IP
O = Flashpoint IP
STREET = 2nd Raban Gamliel
L = Elad
S = Israel
PostalCode = 40800
C = IL
RFC822 Name=ben.wiseman@flashpoint-ip.com
```

We found a company called “Flash Point IP,” with the same street address as in the digital certificate, included the *Patent Attorneys Ledger* published by Israel’s Ministry of Justice. The website listed by the Ministry of Justice for the firm is **flashpointip.com**. However, the website in the certificate's RFC822 name appears to be a *lookalike domain that is subtly different*: **flashpoint-ip[.]com**.

We examined the WHOIS registration of the lookalike domain **flashpoint-ip[.]com**:

```
Registrant Name: BEN WISEMAN
Registrant Organization: FLASHPOINT IP LTD
Registrant Street: RABAN GAMLIEL 2
Registrant City: ELAD
Registrant State/Province: SHOMRON
Registrant Postal Code: 40800
Registrant Country: IL
Registrant Phone: +972.525649427
Registrant Email: BENWISEMAN99@GMAIL.COM
```

The firm's website, **flashpointip.com**, has a New York registration address, a different registrant name, and a @bezeqint.net contact address.

We found one additional domain, **cd-media4u[.]com,** registered with the same phone number as **flashpoint-ip[.]com**. The WHOIS information is:

```
Registrant Name: DAN WISEMAN
Registrant Organization: C. D. MEDIA LTD
Registrant Street: BEN YEHUDA 60
Registrant City: TEL AVIV
Registrant State/Province: TEL AVIV
Registrant Postal Code: 6343107
Registrant Country: IL
Registrant Phone: +972.525649427
Registrant Email: DANWISEMAN99@GMAIL.COM
```

Note the similar names **Dan Wiseman** and **Ben Wiseman** and the similar email addresses **danwiseman99@gmail.com** and **benwiseman99@gmail.com.** We found one reference to “CD Media Ltd” which appears to be an Israeli software publisher (http://www.cd-media.co.il/).

Given that we found two instances where the same entity (WHOIS phone number +972.525649427) registered what appear to be lookalike domains for two different Israeli companies, it is possible that these certificates may have been improperly obtained. This is not the first instance in which improperly obtained digital certificates may have been used with commercial spyware. Hacking Team appears to have obtained several digital certificates in the names of people whose passport photos appeared on a now-defunct site, **thewhistleblowers[.]org.**[4]

[4] e.g., https://web.archive.org/web/20150710202350/http://www.thewhistleblowers.org:80/?-cat=3874

[January 12, 2018 update: Following publication of this report, FlashPoint IP Ltd. (FPIP) confirmed in a letter to the Citizen Lab that “the referenced digital certificate...was not obtained by FPIP, and upon information and belief was obtained unlawfully... The alleged misuse of the FPIP name and address is absolutely illegal and without FPIP’s knowledge, and certainly was never approved by any authorized representative.” Additionally, FPIP noted that it sent a cease and desist letter to Cyberbit, which responded “with a general denial of any wrongdoing or unlawful activity on their part, and rejecting the assertions raised in the FPIP letter. Nonetheless, their letter mentioned (without any admission/consent or prejudice to their rights) that Cyberbit shall take steps to ensure that its products do not use the FPIP name or address or any certificate bearing the FPIP name.”]

We identified two further digital certificates used by the operators, in the names of "Etefaq Consulting Ltd," and "Emerging European Capital." These certificates were on samples we downloaded from getadobeplayer[.]com, as well as samples from the Avira Antivirus and Download.com impersonation websites (**Section 6.2**). Unfortunately, the signatures did not contain the RFC822 Name field, so we do not have any indications as to their legitimacy.

```
CN = Emerging European Capital
O = Emerging European Capital
STREET = Svaetoplukova 12
L = Bojnice
S = Slovakia
PostalCode = 97201
C = SK
```

We found what appears to be the website of "Emerging European Capital" (http://ee-cap.com), which is described as a company offering "Private Banking services to High Net Worth Individuals in Central and Eastern Europe." The address in the digital certificate matches an address listed on the website. The individual mentioned on the website, Martin Masar, appears to be a real individual, and is listed as serving on the Supervisory Board of Petrocommerce Ukraine Bank. However, without more information, we cannot know whether the digital certificate is legitimate or not.

```
CN = ETEFAQ CONSULTING LIMITED
O = ETEFAQ CONSULTING LIMITED
STREET = 1 MYKONOS STREET
L = NICOSIA
S = NICOSIA
PostalCode = 1045
C = CY
```

We found an "ETEFAQ CONSULTING LIMITED" in the Cyprus corporate registry (# HE 329071). However, the registered address did not match the address in the digital certificate. The company's line of business is unclear, and it appears to maintain a simple (hacked) website with a "Contact Us" form (http://etefaqconsulting.com/).

7. Technical Analysis of the Spyware

Altogether, we analyzed nine samples. This includes the sample from VirusTotal signed by the "C4 Security" certificate (**Section 5.1**), as well as five samples gathered from **getadobeplayer[.]com**, and three samples gathered from the Avira Antivirus and Download.com impersonation websites (**Section 6.2**).

Based on strings found during our analysis of configuration files used by the spyware, these samples cover versions of PSS ranging from v4.3.3 to 6.1.0. Major version changes contain changes to obfuscation techniques, overall structure, and general functionality, while minor version changes seem to contain smaller, less noticeable changes. The following analysis covers the general behavior and characteristics of PSS, with version-specific differences noted where appropriate.

MD5	Source	PSS Version
376f28fb0aa650d6220a9d722cdb108d	VirusTotal	4.3.3
568d8c43815fa9608974071c49d68232	getadobeplayer[.]com	5.7.5
80b7121c4ecac1c321ca2e3f507104c2	getadobeplayer[.]com	5.1.0
8d6ce1a256acf608d82db6539bf73ae7	getadobeplayer[.]com	5.9.7
840c4299f9cd5d4df46ee708c2c8247c	getadobeplayer[.]com	6.0.0
961730964fd76c93603fb8f0d445c6f2	getadobeplayer[.]com	6.0.0
0488cf9c58f895076311bf8e2d93bf63	Avira Antivirus Impersonation Website	6.0.0
ca782d91daea6d67dfc49d6e7baf39b0	Download.com Impersonation Website	6.0.0
f483fe294b4c3af1e3c8163200d60aae	Download.com Impersonation Website	6.1.0

Table 25: Versions of PSS we analyzed

7.1. Overview

Overall, the samples we analyzed are made up of four main components: the **Agent**, **LnkProxy**, **Payload DLL**, and **Pipeserver**. The **Agent** is the main program responsible for providing operators remote access to an infected machine and carries out most activity after infection. If the Agent is not installed with administrator privileges, then the **LnkProxy** facilitates the replacement of shortcut (lnk) and executable (exe) files with malicious versions that will try to trick the user into granting administrator privileges to the Agent. The **Payload DLL** is a small DLL file that is used to infect certain whitelisted DLLs as a persistence mechanism, to ensure that the Agent is running. Finally, the **Pipeserver** is used to coordinate access to global handles and perform network communication.

Each of these four components is packed and stored inside the initial spyware payload. The earliest version we analyzed (4.3.3) stored these files as either plaintext or as zlib compressed data. Later versions added AES-256-CBC encryption and the use of different keys per dropped component for additional obfuscation (**Section 7.3**).

7.2. Installation and Persistence

Once a victim executes one of the initial payloads (e.g., a fake Adobe Flash update), the spyware unpacks the Agent component (described in **Section 7.4**) and saves it to %TEMP%\Profile. Then, the spyware checks to see if it is running with administrator privileges. If so, then the spyware executes the dropped Agent; if not, then the spyware unpacks and installs the LnkProxy component (described in **Section 7.5**) in an attempt to trick the user into giving it administrator privileges.

Once the dropped Agent has been executed with administrator privileges, either via the main installer or by tricking the user via the LnkProxy technique, the Agent unpacks its configuration file into memory. Next, the Agent checks to see if there is already a version of PSS installed on the victim's system by checking for the existence of the storage directory used by the spyware. Depending on the configuration of the current and previous Agents, the Agent may either replace the existing agent or attempt to upgrade the old version. If PSS is not already installed, then the Agent begins installation.

The Agent creates its main **storage directory** at %CommonAppData%\Profile. Then, it writes its configuration file into the storage directory, using a name defined in the configuration file (versions 4.x and 5.x use the filename diskdrv.dll, while version 6.x uses igfxcls.cfg). The Agent then copies itself into the storage directory (versions 4.x and 5.x use the filename crisvc.exe for the agent, while version 6.x use the filename igfxcri.exe) while deleting the dropped copy from %TEMP%\Profile.

Next, the Agent unpacks and drops 32- and 64-bit versions of the PipeServer component into the storage directory. These files are named mssvt.dll and mssvt64.dll across all versions of PSS that we have analyzed.

After it has created the necessary files, the spyware sets up its persistence mechanism by infecting copies of certain DLLs on the system with the Payload DLL (which is not saved to disk as a standalone file). The infected copies are placed in the same folder as the executable that will load them, ensuring that the infected DLLs are loaded instead of their legitimate counterparts that may be in other folders (Windows will search the folder containing the application first). The DLLs we saw chosen for infection are related to common web browsers including Chrome, Firefox, and Internet Explorer. Since web browsers are some of the most commonly used applications on computers, these DLLs are a good choice to ensure that the spyware is running most of the time that the target device is being used.

Finally, the spyware initializes the appropriate PipeServer component by creating a new Desktop, referred to as a “HiddenDesktop” by the spyware and launching one or more of the EXEs whose DLLs have been replaced with infected versions on this new desktop. When an infected DLL is loaded (**Section 5.6**), it launches the PipeServer if not already running; the PipeServer in turn launches the Agent if not already running. The Agent then enters into its main command handling loop.

7.3. Obfuscation

The first version of the spyware we analyzed (4.3.3) stored most components as either plaintext data or as zlib compressed binary data. Version 5.x of PSS introduced the additional use of AES-256-CBC encryption for the components. Components obfuscated in this manner contain a short header struct followed by the AES-256-CBC encrypted, zlib compressed data:

```
struct HEADER {
    char[6]: magic_number
    uint32:  iv
    uint32:  checksum
    uint32:  length
}
```

In this header struct, magic_number is the magic_number for a 7z file [0x37, 0x7a, 0xbc, 0xaf, 0x27, 0x1c], iv is the first 4 bytes of the initialization vector used in the AES cipher, checksum is a CRC32 checksum of the data, and length is the length of the encrypted data. The initialization vector is padded with null bytes to the correct length for the AES-256-CBC cipher. Version 6.x added an additional data format for AES-256-CBC encrypted data that removes the magic_number. For all versions, the AES key is hardcoded in the executable performing the decryption. Beginning with version 6.x, the spyware additionally began to obfuscate strings, deobfuscating them only when needed.

Version 4.x drops all of its various components directly to disk in an unpacked form when installed. Starting with version 5.x, the spyware began to drop intermediate loader executables instead of final components. These loader executables store a component, often the Agent, in the same AES-256-CBC encrypted, zlib compressed format as above. When executed, these loaders mimic the Windows executable loader by unpacking their stored payload, mapping the unpacked PE file's sections into memory, and resolving any imports before jumping to the PE's entrypoint. This technique of storing the unpacked component only in memory is likely an attempt to evade static, file-based analysis and detection techniques.

Within the Agent component, the configuration file is an SQLite database obfuscated using bzip compression, followed by XOR encryption using both the current and previous bytes, along with one byte from the key. This obfuscation format, and an unusual 36-byte XOR key, the string DC615DA9-94B5-4477-9C33-3A393BC9E63F, are shared across all the samples we analyzed.

7.4. The Agent

The Agent is the central component of the spyware and is responsible for carrying out most of the behavior of PSS. The Agent is a feature-rich spyware capable of a wide range of behaviors. Across all samples we analyzed, we have seen the following capabilities:

- Audio/Video recording including scheduling recordings for a later time
- Reading browser history and stored passwords
- Filesystem operations including creating, deleting, moving, renaming, uploading, and downloading files
- Editing/Querying registry keys

- Geolocation based on available wifi networks
- Accessing Skype databases, call logs, and contacts
- Listing network connections and devices
- Starting/Stopping processes
- Taking screenshots
- Keylogging
- Accessing clipboard data
- Accessing recently used file list

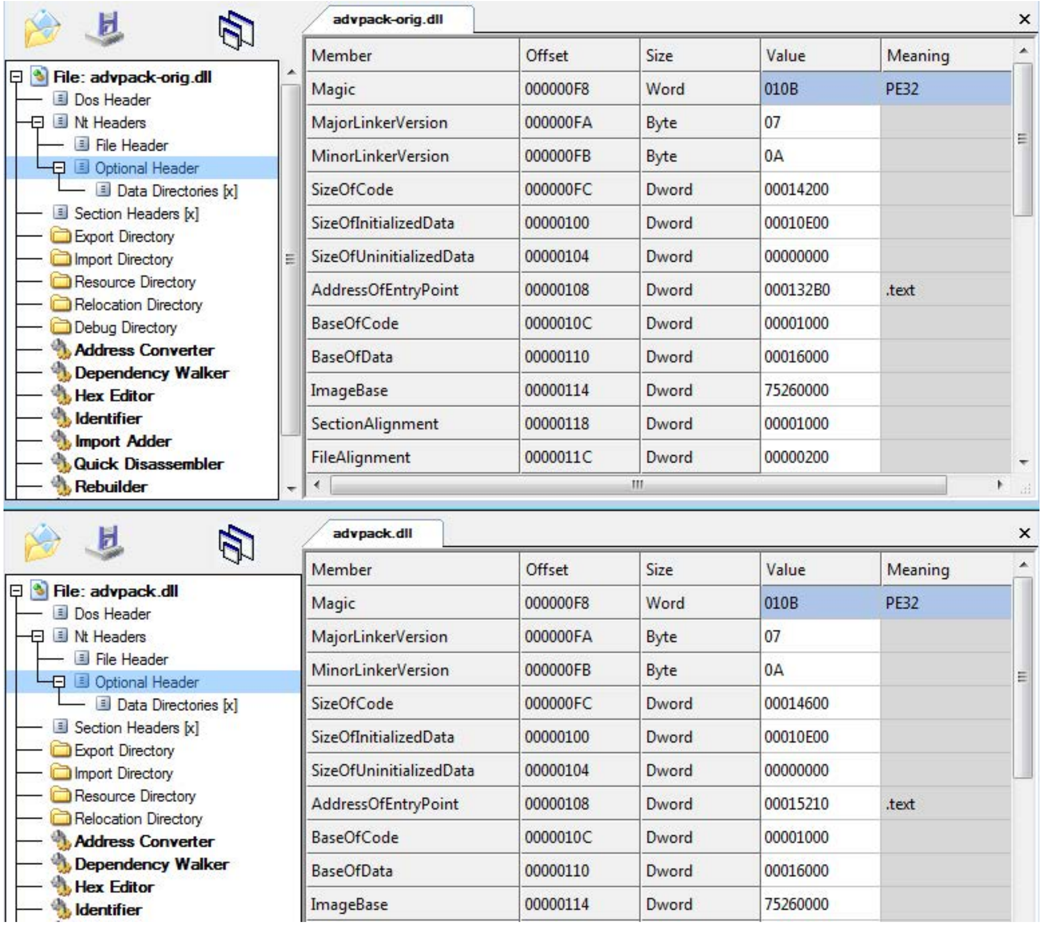
7.5. LnkProxy

The LnkProxy component is only used when the spyware is initially installed without Administrator privileges. In this scenario, the spyware searches through the Windows Desktop, Start Menu, and Quick Launch folders looking for lnk and exe files. Any files it finds are replaced with malicious copies designed to request administrator privileges, launch the legitimate application, and then launch the spyware. This process is designed to trick the user into giving PSS administrator privileges.

The LnkProxy makes a backup of all replaced files, which are restored upon spyware uninstallation or when the user unwittingly grants the spyware administrator privileges.

7.6. Payload DLL

The Payload component of the spyware is a short DLL that is used to infect whitelisted DLLs on the victim's system as a persistence mechanism. During installation, the spyware searches the victim's computer for targeted DLLs and for each that it finds it appends the Payload component to the targeted DLL's .text section. The entrypoint of the DLL is then changed to point to this appended code and the infected file is copied to the same directory as the application that uses the DLL. This ensures that the infected DLL is loaded by the application instead of the original, uninfected version. **Figure 11** shows an example of a modified binary infected with the Payload component.



advpack-orig.dll

Member	Offset	Size	Value	Meaning
Magic	000000F8	Word	010B	PE32
MajorLinkerVersion	000000FA	Byte	07	
MinorLinkerVersion	000000FB	Byte	0A	
SizeOfCode	000000FC	Dword	00014200	
SizeOfInitializedData	00000100	Dword	00010E00	
SizeOfUninitializedData	00000104	Dword	00000000	
AddressOfEntryPoint	00000108	Dword	000132B0	.text
BaseOfCode	0000010C	Dword	00001000	
BaseOfData	00000110	Dword	00016000	
ImageBase	00000114	Dword	75260000	
SectionAlignment	00000118	Dword	00001000	
FileAlignment	0000011C	Dword	00000200	

advpack.dll

Member	Offset	Size	Value	Meaning
Magic	000000F8	Word	010B	PE32
MajorLinkerVersion	000000FA	Byte	07	
MinorLinkerVersion	000000FB	Byte	0A	
SizeOfCode	000000FC	Dword	00014600	
SizeOfInitializedData	00000100	Dword	00010E00	
SizeOfUninitializedData	00000104	Dword	00000000	
AddressOfEntryPoint	00000108	Dword	00015210	.text
BaseOfCode	0000010C	Dword	00001000	
BaseOfData	00000110	Dword	00016000	
ImageBase	00000114	Dword	75260000	

Figure 11: Comparison of entrypoint before and after Payload infection.

The infected DLL starts by checking to ensure that the infected DLL is being loaded by the target program only. It does this by calling the original entrypoint for the infected DLL to get the ImagePathName field of the ProcessParameters struct in the Process Environment Block (PEB). The ImagePathName contains the path of the currently running executable. This is then compared to a hardcoded checksum value stored in the DLL as part of the infection process.

If this check succeeds, the Payload then performs its functions. It first checks to see if the PipeServer is currently loaded. It does this by decrypting an XOR-encrypted string in the DLL containing the location of the PipeServer component, calculating a checksum of this string, and then walking the InMemoryOrder list of loaded modules, checksumming the ImagePathName of each and comparing it to the checksum of the PipeServer's path. If the PipeServer is not currently loaded, the infected DLL loads the PipeServer component and transfers execution to it.

7.7. PipeServer

The PipeServer component starts by unpacking and loading a small configuration file. This is a small file containing ASCII strings separated by \x00's that define various config options used by the PipeServer. In version 6.x, this file is zlib compressed and encrypted using AES-256-CBC. After loading the configuration file, the PipeServer creates a series of threads, global events, and mutexes that are used to synchronize actions between components of the spyware, log messages, and communicate with the command and control server. Next, the PipeServer creates a named pipe for communication with running Agent components. Finally, the PipeServer starts an instance of the Agent if one is not already active before entering a main command handling loop. The spyware uses a XML-based networking protocol for command and control communication. Each request and response is sent as a "transaction." An example of the XML format used is given below.

```
<?xml version="1.0">
<transaction
    type="fromagent"
    agentid="<ID>"
    sn="<NUM>"
    crc="<CRC>"
    encoding="base64"
    encryption="aes-256"
    compression="<zip|none>">
        <DATA>
</transaction>
```

DATA is the information to be communicated and is compressed, encrypted, and encoded as described in the response attributes. The AES key used can be either a master key included in the Agent's configuration or an individual private key created after the malware has been installed and initialized. The master key is hard-coded and is the same across all samples we analyzed.

8. Conclusion

We have uncovered the use of PC Surveillance System (PSS) spyware by what appears to be agencies of the Ethiopian government to target dozens of individuals. Our investigation shows these targets include an Oromo media outlet based in the United States, OMN, a PhD student, and a lawyer who have worked on Oromo issues, as well as a Citizen Lab Research Fellow, Bill Marczak. Our analysis also indicates apparent demonstrations of the spyware in several other countries where leaders have exhibited authoritarian tendencies, and/or where there are political corruption and accountability challenges, such as Nigeria, Philippines, Rwanda, Uzbekistan, and Zambia.

The habitual misuse of spyware by the Ethiopian government against civil society targets is testament to the lack of repercussions for such behavior by states and complicity within the commercial spyware industry that supplies them. Evidence indicating the Ethiopian government's misuse of spyware (including Hacking Team's RCS and Gamma Group's FinSpy) against journalists, activists, and others has been laid out in prior research over multiple years, as well as in a lawsuit filed in US federal court. In a portentous ruling, that suit was dismissed on grounds that a tort is not committed entirely in the US -- a showing of which was required to obtain jurisdiction over a foreign sovereign -- when a government's digital espionage is conceived of and operated from overseas, despite the fact that the infection occurs and harm is experienced within the US. The digital nature of the tort essentially allowed a foreign government to violate US laws with impunity. Unsurprisingly, as this report makes clear, the extraterritorial targeting continues, as do spyware sales to Ethiopia.

This report also uncovers another player in the nation-state spyware business: Cyberbit, the company that provides PSS. As a provider of powerful surveillance technology, Cyberbit has the responsibility under both Israel's export control regime as well as the UN Guiding Principles on Business and Human Rights to concern itself with the potential for human rights abuses facilitated through use of its product. The fact that PSS wound up in the hands of Ethiopian government agencies, which for many years have demonstrably misused spyware to target civil society, raises urgent questions around Cyberbit's corporate social responsibility and due diligence efforts, and the effectiveness of Israel's export controls in preventing human rights abuses. The apparent locations of PSS demonstrations reinforce those concerns. Moreover, the manner in which the PSS spyware operates suggests that, to achieve infection, the spyware preys on user trust in legitimate third-party companies and software, such as Adobe Systems, or the code-signing certificate verification process. These techniques undermine security in the larger digital ecosystem and contravene terms of service as well as clear legal standards that exist in many jurisdictions to prevent appropriation of intellectual property. If spyware companies themselves incorporate such techniques in order to build a successful product, action is necessary to address the negative externalities that result. We have sent a letter to Cyberbit regarding these issues and received a response.

As we explore in a separate analysis, while lawful access and intercept tools have legitimate uses, the significant insecurities and illegitimate targeting we have documented that arise from their abuse cannot be ignored. In the absence of stronger norms and incentives to induce state restraint, as well as more robust regulation of spyware companies, we expect that authoritarian and other politically corrupt leaders will continue to obtain and use spyware to covertly surveil and invisibly sabotage the individuals and institutions that hold them to account.