UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 46 – August 2014

Schrodinger's Cat Video and the Death of Clear-Text

Morgan Marquis-Boire

Read Morgan Marquis-Boire's op-ed in The Intercept on the report's findings.

Read the report's accompanying piece in the Washington Post. This was published on the Washington Post's front page [see PDF and PDF].

The report's findings have also been covered by Washington Post's The Switch blog, Schneier on Security, Heise Online [in German], The Verge, Tech Times, Techdirt, Gizmodo, Network World, Engadget, Marie Claire [in French], Slate [in French], Glamour [in French], and the Huffington Post.

"… while Web 1.0 was invented so that theoretical physicists could publish research online, Web 2.0 was created so that people could publish cute photos of their cats."

– Ethan Zuckerman (2007)

"Hidden in the dashboard
The unseen mechanized eye
Under surveillance
The road is full of cat's eyes"

– *The Spy in the Cab*, Bauhaus (1980)

KEY FINDINGS

- Commercial network injection appliances are actively targeting Google's YouTube and Microsoft's Live services in order to install surveillance implants on targets across the globe.

- Documents indicate that a prototype for targeted surveillance network injection appliances sold to the governments of Oman and Turkmenistan was designed by CloudShield Technologies, a US Department of Defense contractor.[1]
- This report reveals never before seen documentation on the operation of Network Injection appliances from both Hacking Team and FinFisher and provides source code for an early prototype of FinFisher's FinFly ISP product.

INTRODUCTION

While there has been much discussion about the use of software described as 'implants' or 'backdoors' to perform targeted surveillance, this report is about the less well understood method by which most targeted surveillance is delivered: network injection. Taking advantage of security flaws in major web presences (such as Google's 'YouTube' and Microsoft's 'Live')[2], vendors have started selling turnkey solutions that enable easy installation of targeted surveillance software at scale.

This report provides a detailed analysis of two products sold for facilitating targeted surveillance known as network injection appliances. These products allow for the easy deployment of targeted surveillance implants and are being sold by commercial vendors to countries around the world. Compromising a target becomes as simple as waiting for the user to view unencrypted content on the Internet.

While the technology required to perform such attacks has been understood for some time, there is limited documentation of the operation of these attacks by state actors. This report provides details on the use of such surveillance solutions including how they are built, deployed, and operated.

NETWORK INJECTORS

Software to perform man-in-the-middle attacks on networks has been available for some time. For example, in 2000, Dug Song released a suite of tools called 'dsniff' for capturing passwords on a switched network. Interestingly in 2001, Alberto Ornaghi and Marco Valleri, the founders of Milan based surveillance company Hacking Team, wrote a popular open source tool, 'Ettercap' which enabled active interception and manipulation of traffic on local area networks. In 2007, Francisco Amato released 'EvilGrade', a tool to intercept updates for popular applications and replace them with a malicious payload.

In recent years, this type of technology has not received much attention from the security community, as the technical aspects of these types of attacks, and solutions to to them, are well understood. If traffic is properly encrypted,[3] it cannot be tampered with, and such attacks will fail. Additionally, performing this type of attack reliably at scale requires control of an Internet Service Provider (ISP) or Internet Exchange (IX) and the resources to purchase the hardware required to intercept and manipulate traffic at volume.

Over the last few years, there has been an increase in the public awareness of state-sponsored hacking for the purposes of espionage and surveillance. Traffic interception and manipulation provide an obvious method for an attacker with resources and the power to enlist the cooperation of, or compel, network providers. It enables the installation of surveillance implants on target hosts without the need to resort to unreliable methods such as spear-phishing.

In many surveillance operations, physical access to target systems cannot be achieved and covert installation of a remote monitoring solution is required to be able to monitor a target. Network injectors provide a countrywide solution to this problem that can be integrated into an ISP's access and / or core network to install

the remote monitoring solution on selected target systems. Basically, this is the logical extension of a man-in-the-middle attack for an adversary that owns the wires in the ground or can coerce a service provider.

Network injectors generally take the form of appliances based on carrier grade server technology. High-speed traffic interception allow attackers to identify victim traffic. Once this action has occurred, the traffic can be modified in a variety of ways. Early solutions infected executable files downloaded by the target or injected fake software updates for popular software.[4] This document will describe how the most recent versions of these solutions infect targets on-the-fly by injecting malicious code into the traffic streams of popular websites.

RECENT REVELATIONS

Documents leaked by Edward Snowden have revealed that the NSA uses man-in-the-middle network injection infrastructure to deliver malware implants for the purposes of targeted surveillance. One such system, known as QUANTUMINSERT, is illustrated below:

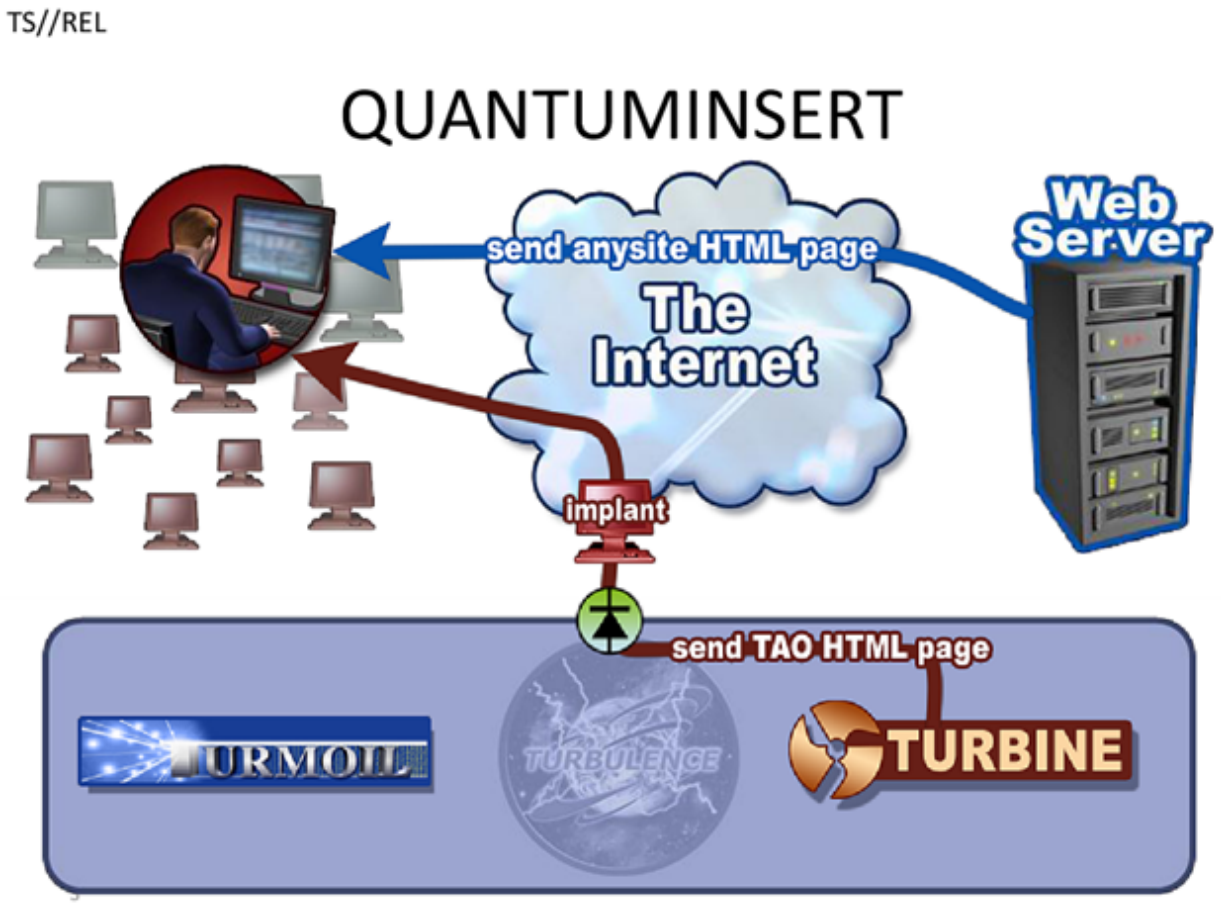

Figure 1: Schematic of NSA's QUANTUMINSERT system. (Source)

As described by Nicholas Weaver in Wired magazine:

"All it takes is a single request from a victim passing a wiretap for exploitation to occur. Once the QUANTUM wiretap identifies the victim, it simply packet injects a 302 redirect to a FOXACID server. Now

the victim's browser starts talking to the FOXACID server, which quickly takes over the victim's computer. The NSA calls this QUANTUMINSERT."

The use of this system against European telecommunications provider Belgacom was documented last year.

The Intercept revealed that the NSA was using a system known as TURBINE to:

"…increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants."

Earlier reports based on the Snowden documents revealed that the NSA had compromised between 85,000 and 100,000 targets using such techniques.

For a longer discussion of Five Eyes capabilities in this area, see Claudio Guarnieri's blog post, *The Internet is Compromised*.

WHY USE NETWORK INJECTION?

The advantages of using such network injection techniques are obvious when compared to other common attack vectors such as spear-phishing or watering-hole attacks. These kinds of attacks rely on a target being tricked into opening a file or viewing malicious content, whereas, network injection allows the exploitation of any target that views any clear-text content on the Internet provided that they pass through a network point that the attacker controls. While major providers are making efforts to encrypt parts of their networks, a significant portion of the Internet's traffic is still unencrypted, allowing for easy manipulation. Even pages that serve their own content securely are likely to use unencrypted traffic from a variety of advertising networks or other third parties.

Provided that the attacker can persuade a sufficiently large carrier to install a network injection apparatus, they can be reasonably certain of the success of any attack. While an attacker would still need an exploit to escape from the context of the target's browser, one of the browser plugins (such as flash, java, quicktime, etc.) or similar is likely to provide a low cost avenue for this. This type of capability obviates the need for spear-phishing or more clumsy attacks provided the target is in the attacker's domain of influence.

This type of approach also allows for the 'tasking' of a specific target. Rather than performing a manual operation, a target can be entered into the system which will wait for them to browse to an appropriate website and then perform the required injection of malicious code into their traffic stream. As such, this could be described as 'hacking on easy mode'.

While the scope of the NSA's system may have surprised many in the public, it has been generally assumed that the best funded spy agency in the world would possess advanced capability. What is perhaps more surprising is that this capability is being developed by Western vendors for sale on the commercial market.

BACKGROUND ON THE 'LAWFUL INTERCEPT' MARKET

Over the last few years, a burgeoning commercial intrusion industry providing exploits and malware as lawful interception products has gained notoriety. In 2012, Jerry Lucas, the president of TeleStrategies, the company which runs the surveillance showcase ISS World (commonly known as the 'Wiretapper's Ball') said in a New York Times article:

"The market for such technologies has grown to $5 billion a year from nothing 10 years ago"

While such products have traditionally been custom developed by a few nation states, the commercialization of this market has increased the ability of regimes to purchase advanced surveillance capabilities from vendors based in liberal democracies. Despite the fact that this technology is commonly sold as 'lawful interception', it has been used to target activists, journalists, dissidents, and human rights workers. Prior research by The Citizen Lab has tracked the usage of lawful intercept surveillance technology sold by FinFisher and Hacking Team against political and civil society targets including Bahrain Watch, Mamfakinch in Morocco, human rights activist Ahmed Mansoor in the UAE, and ESAT, a US-based news service focusing on Ethiopia.

FinFisher, developed in Munich, is a line of remote intrusion and surveillance software marketed and allegedly sold exclusively to law enforcement and intelligence agencies. Until 2013, it was distributed by the UK based Gamma Group International. Hacking Team is a Milan-based company which, by their own account, sells commercial hacking software to law enforcement in "several dozen countries" on "six continents". Citizen Lab has tracked the use of FinFisher to 25 different countries and Hacking Team to 22 different countries. These server location findings should not be considered to be a definitive list; in fact, Hacking Team is claimed to have been used in up to 60 countries worldwide.

Both FinFisher and Hacking Team sell network injection solutions, enabling easy compromise of targets on a country-wide basis. This ability in the hands of states that lack a robust rule of law raises concerns for high risk groups, as our work has shown.

FinFly ISP

In 2011, Wikileaks began publishing "The Spy Files", an archive of leaked brochures and other promotional material from commercial vendors of surveillance products. Among the documents were advertisements for a product called "FinFly ISP". Produced by Gamma International, this network injection product deploys remote monitoring agents on target systems with the assistance of an ISP. One of the use cases highlighted by the sales brochure was:

"*The customer deployed FinFly ISP within the main Internet Service Provider of their country. It was combined with FinFly Web to remotely infect Targets that visited government offensive websites by covertly injecting the FinFly Web code into the targeted websites.*"

A video advertisement for this product was uploaded to YouTube and can be found here.

Citizen Lab was contacted by individuals involved in the design of an early version of this surveillance product. In addition to documentation on the operation of this appliance, Citizen Lab was also sent source code. We have no way to verify independently the authenticity of the material presented to us, but we are presenting it in this report for outside review.

These materials appear to indicate that a prototype of FinFly was created with the help of Sunnyvale, CA based company CloudShield Technologies (now a subsidiary of Leidos, previously Science Applications International Corporation (SAIC), a contractor to the US military and intelligence community).

Below you can see a screenshot of the prototype displaying the FinFly ISP solution running on CloudShield products. The solution is written in CloudShield's custom language, RAVE.

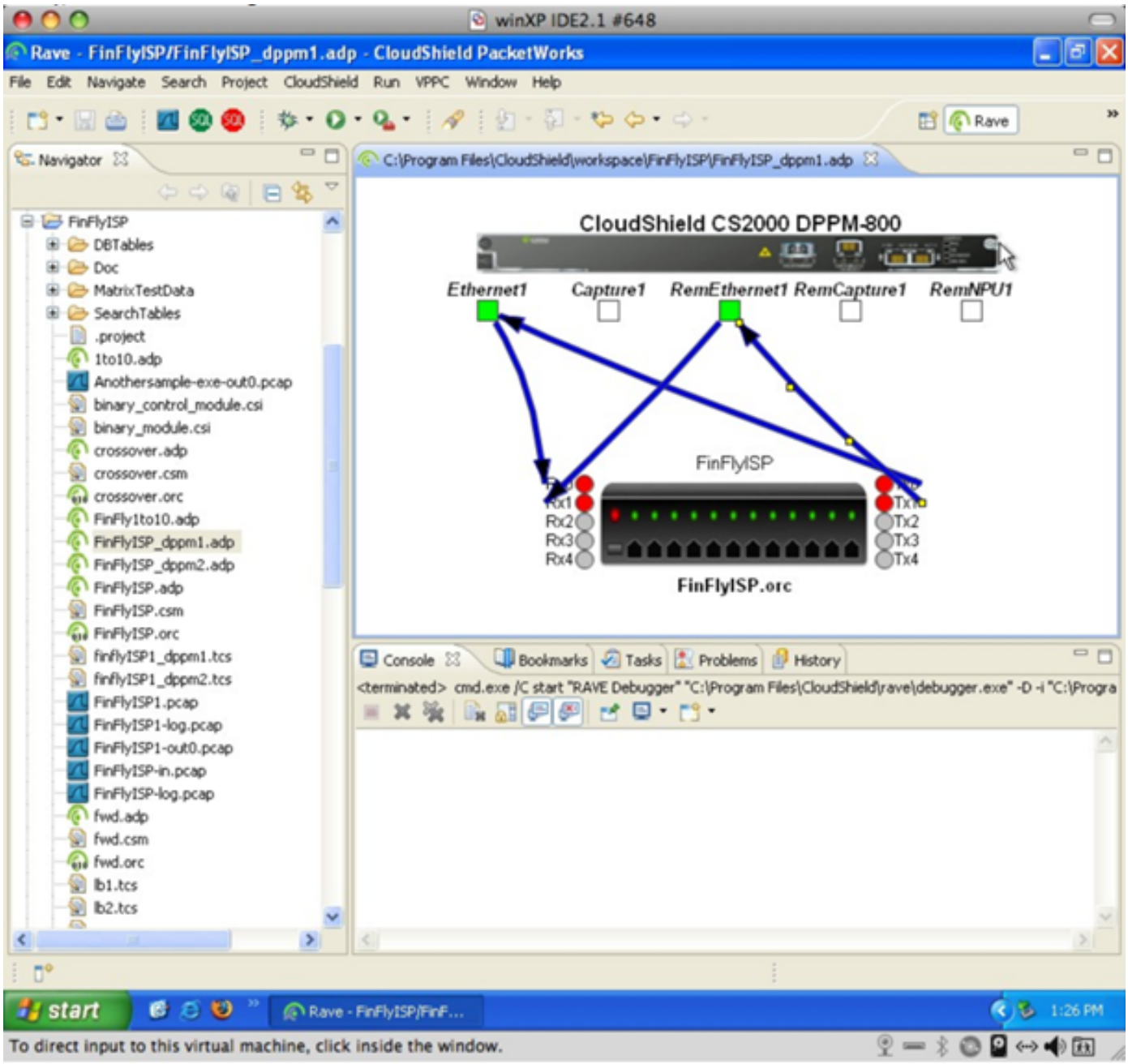

Figure 2: Screenshot of FinFly prototype running on CloudShield's PacketWorks software

A sample of the prototype FinFly ISP code can be found below:

```
  // A local structure for TargetTable entries
  // +------+-----+-----+------+-------+-------+------+--------+----------+
  // |Target|Bin  |Upd  |Trojan|UTrojan|Compltd|Failed|Radius  | Reserved |
  // |  IP  |Mode |Mode |  ID  |  ID   |Count  |count |TableID |          |
  // +------+-----+-----+------+-------+-------+------+--------+----------+
  // | (32) | (8) | (8) |  (8) | (8)   |  (16) | (16) |  (8)   |   (24)   |
  // +------+-----+-----+------+-------+-------+------+--------+----------+
  .var32 L32_TargetTableData
  .var32 L32_TT_TargetIP      @L32_TargetTableData          // Target IP
  .var16 L16_TT_ModeFlags     @L32_TargetTableData + 4      // A 16 bit
alias for both mode bytes
  .var8  L8_TT_BinaryMode     @L32_TargetTableData + 4      // Binary Mode
flag
  .var8  L8_TT_UpdateMode     @L32_TargetTableData + 5      // Update Mode
flag
  .var8  L8_TT_TrojanID       @L32_TargetTableData + 6      // Row # in
indexMatrix referencing trojan for Binary infection
  .var8  L8_TT_UTrojanID      @L32_TargetTableData + 7      // Row # in
indexMatrix referencing trojan for Update infection
  .var16 L16_TT_Completed     @L32_TargetTableData + 8      // Counter for
completed infections
  .var16 L16_TT_Failed        @L32_TargetTableData + 10     // Counter for
failed attempts
  .var8  L8_TT_RadiusTID      @L32_TargetTableData + 12     // Index into
Radius names table
  .var8  L8_TT_Reserved1      @L32_TargetTableData + 13   // Reserved for
future use
  .var16 L16_TT_Reserved2     @L32_TargetTableData + 14     // Reserved for
future use
  .var32 L32_TT_Row
      // Row number in database
```

Figure 3: Sample of FinFly ISP source code

Binary Mode is a flag to enable detection of a windows binary PE header on the wire, modify it in transit and inject loader + payload into the download ahead of the real binary. The real icon is preserved. Upon execution, the downloaded file would run the loader which executed the payload then cleaned the downloaded file on disk, such that it was the originally requested file. By this time, the payload would be memory resident. Finally, the real binary would be executed. This technique would work even with self-checking binaries. **Update Mode** is a flag to simulate reponses of update checks for iTunes, WinAmp, and other popular applications at the time. These responses were served from FinFly and spoofed applications into updating with infected versions. It is possible to set both flags for a target. **TrojanID** is the payload to inject. FinFly could be loaded with several different trojans and a target dependent payload could be set. **UTrojanID** is the payload for update mode. These columns contain an ID which references the trojan from a simple RAM based filesystem created at load time with pre-built arrays. **Compltd Count** is the number of confirmed infections based on the fact that the target TCP/IP stack had acknowledged all the packets sent to it at the end of the

session. **Failed Count** counted unsuccessful infection attempts based on lack of clean FIN flag exchange at the end of the session.

Subsequent to this, a version was created with the help of the Swiss company Dream Lab Technologies AG. Documentation leaked by Wikileaks asserts that this system was deployed in Oman:

"This offer is based upon a request of Thomas Fischer of Gamma International as well as on various conversations between Gamma International, Dreamlab Technologies AG and the end customer."

Wikileaks documents also assert this to have been deployed in Turkmenistan.

The cost of this product for that bid is detailed below:

7. Order form quotation no. 3104351.2

Details for the ordering of the service: „Infection Proxy Project 1"

	Description	Net worth CHF
	Network analysis	32'400.00
	Project Management and Documentation	48'000.00
	Installation of hardware and software	57'600.00
	On Site assembly in Turkmenistan	43'200.00
	Training	9'000.00
	Fixnet	153'954.80
	Tmcell	286449.90
	Management Infrastructure	69'060.00
	Monitoring and Alarming Option	94'755.00
	System Maintenance / per call-out (On-site variant)	16'000.00
	Co-ordination meetings per call-out	5'400.00
	Software Maintenance	59'000.00
	Total	**874'819.70**

Please fill in as appropriate.

Conditions

Prices
Prices do not include VAT and shipping costs and are in CHF.

Expenses
Travel expenses are not included in the offer.

Payment Conditions
30% down payment, 30% at time of delivery, 20% after installation, and 20% after the final acceptance of the end-user/customer, in accordance with the co-operation agreement.

Deadlines
The precise dates have yet to be defined.

Validity of this quotation
This offer has a validity of 8 weeks from the date of issuance.

Figure 4: Order form for the FinFly ISP installation in Turkmenistan

The above order form indicates a total cost of 874,819.70 Swiss Francs (CHF) or approximately 1 million US dollars. This includes a 43,200CHF fee for "On Site assembly in Turkmenistan".

A logical diagram of how the equipment is installed into a network and how the operation works:

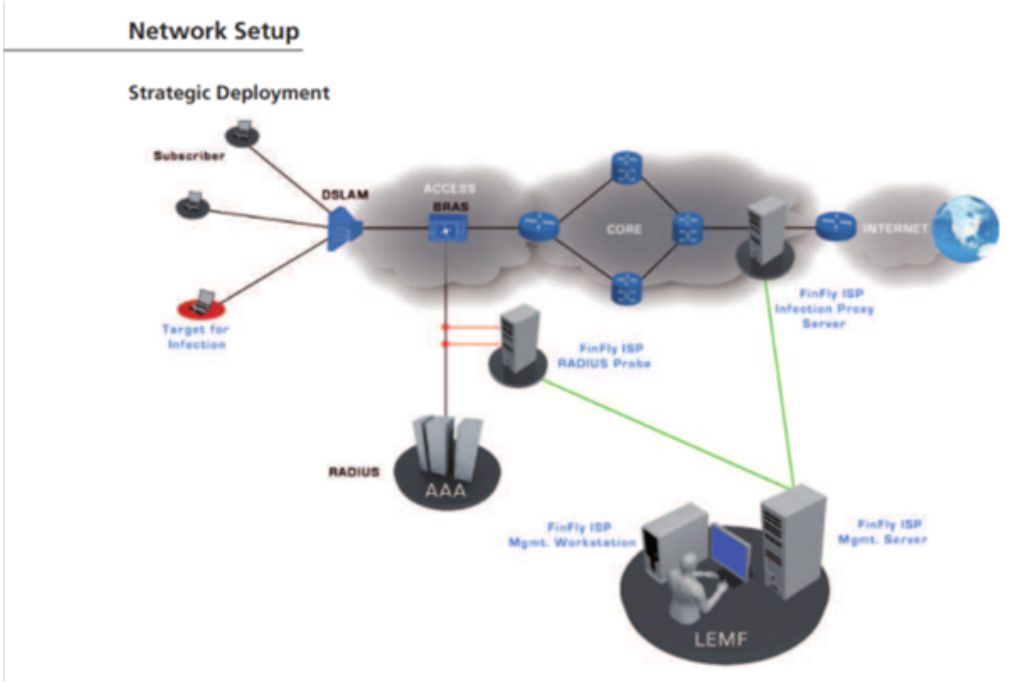

Figure 5: Diagram of FinFly installation.

A network diagram of the infection proxy integration into an ISP environment can be found below:

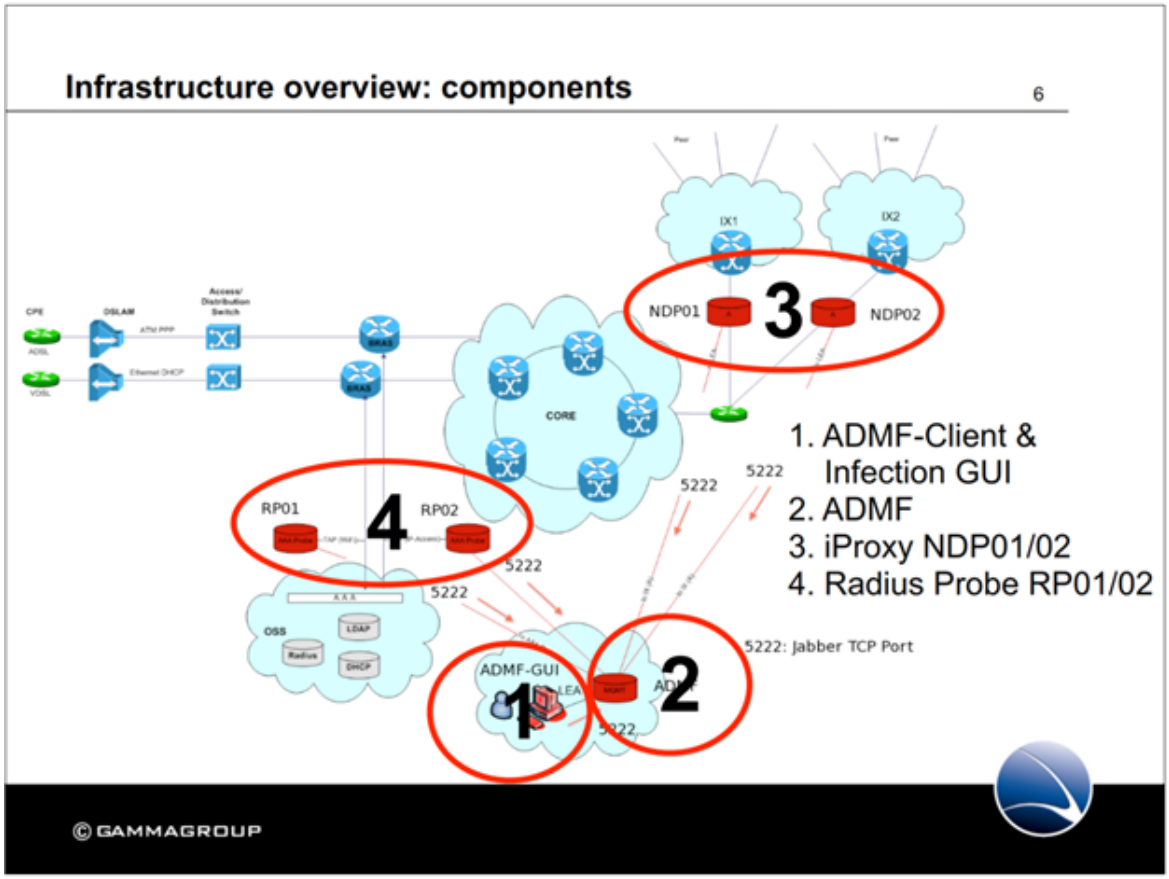

Figure 6: Diagram of FinFly integration into an ISP environment

The following slides describe the process of infecting targets:

Use Case → Infection

22

Step	Direction	Action content	Details
1	GUI -> ADMF	Infect a target	Send infection information Target information / infection mode
2	ADMF -> Radius probe	Start monitoring and set a trap on this target	Actual IP address of target is known
3	Radius -> ADMF -> NDP / iProxy	Handover actual IP address	IP address
4	iProxy -> NDP	Iproxy requests NDP to analyse the datastream on IP address and „interesting" traffic	Target IP address
5	NDP -> iProxy	Handover traffic matching the request	Stream is redirected to iProxy
6	iProxy	changes the traffic and modifies the data by adding the infection parts	

© GAMMAGROUP

Figure 7: Gamma presentation slides describing FinFly target infection process

This shows how target selection occurs. In the administrative GUI, target information is entered (presumably a name). The subject's IP address is then looked up in a RADIUS database and monitoring of the target's traffic begins. The target's traffic is analyzed for a stream suitable for injection. Once this stream is found, the traffic is modified and the malicious traffic injected.

Use Case → Infection

23

Step	Direction	Action content	Details
6	iProxy	changes the traffic and modifies the data by adding the infection parts	
7	iProxy -> NDP	iProxy sends the modifed traffic back to NDP	
8	NDP Reinject	NDP recalculates checksums, resequences TCP/IP packets and reinjects the traffic into the stream	
9	Target infection done	Data successfully sent to target	

© GAMMAGROUP

Figure 8: Gamma presentation slides describing FinFly target infection process.

The malicious traffic is checked to ensure that the modified traffic looks authentic and will be accepted by the target. Checksums are tested, TCP/IP packets are resequenced, and the modified and now malicious traffic is sent to the target.

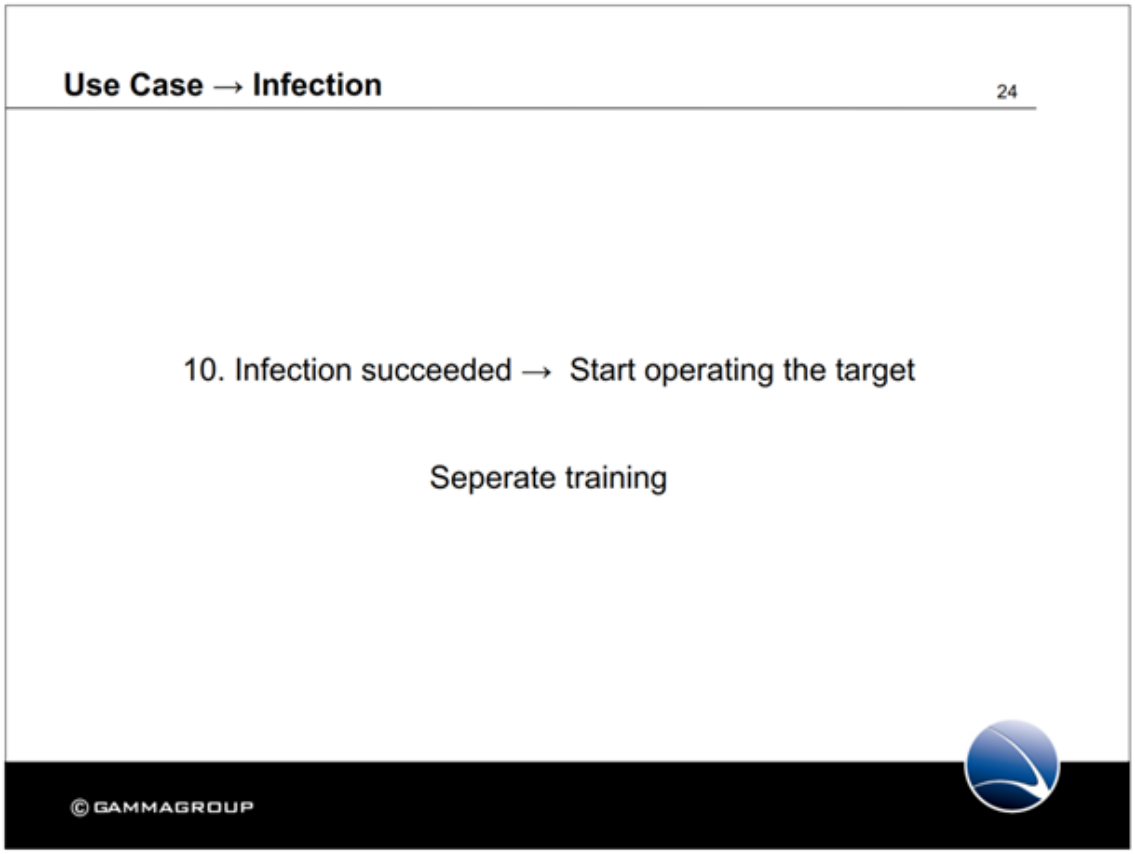

Figure 9: Gamma presentation slides describing FinFly target infection process

Once the target is infected, the surveillance operation can begin.

Historically, FinFly ISP was able to infect files that are downloaded by the target on-the-fly or infect the target by sending fake software updates for popular software.[5]

The latest promotional literature on the FinFly offering boasts:

"The new release now integrates Gamma's powerful remote infection application FinFly Web to infect Targets on-the-fly by just visiting any website."

FinFly Web appears to be the component of the FinFly architecture that infects any clear-text page in order to offer malware as a download. It appears that a recent (unrelated) leak[6] has made the FinFly Web component of the FinFly architecture available on Github.

This appears to be a screenshot of this being used live in Bahrain:[7]

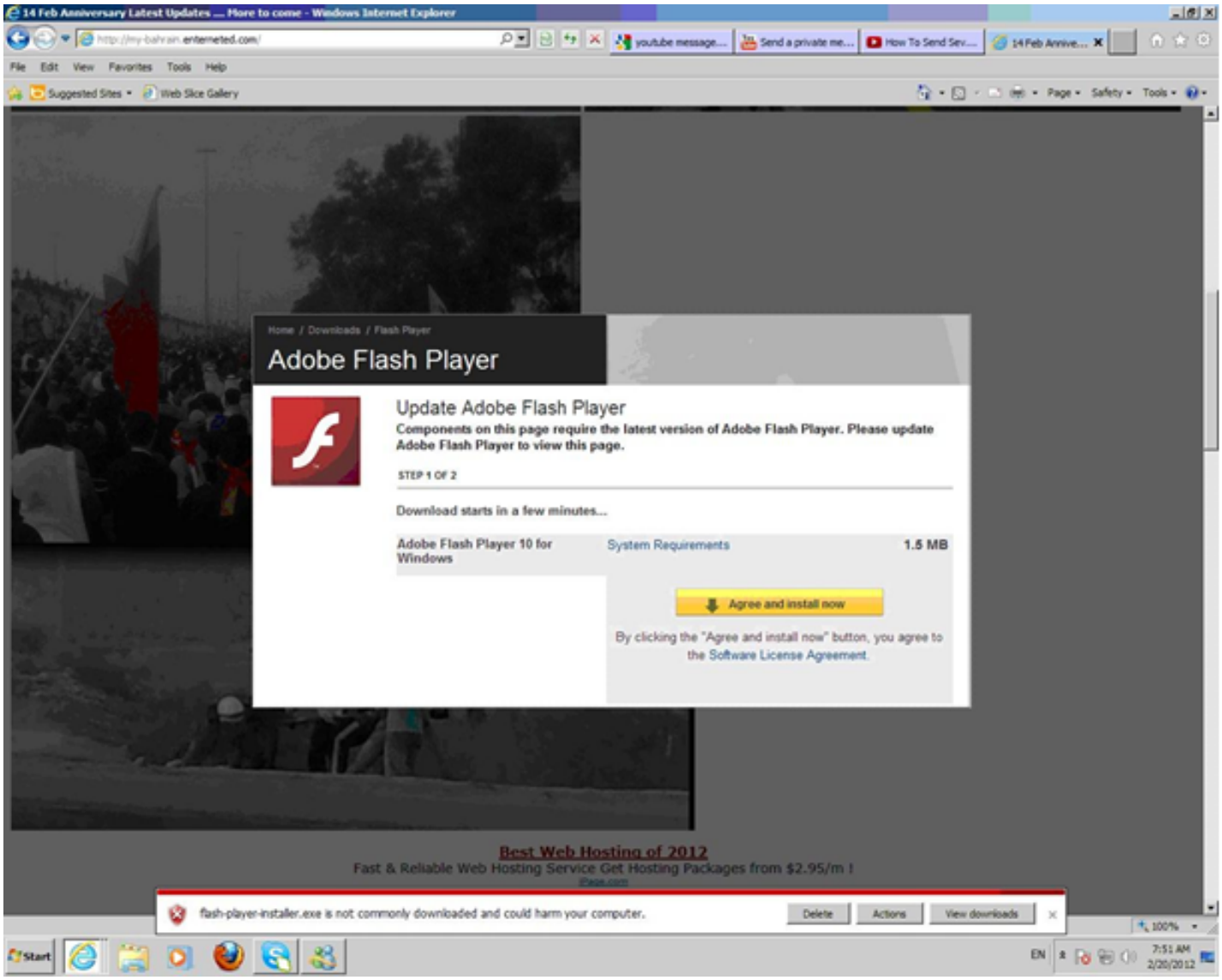

Figure 10: Screenshot of FinFly Web product being used in Bahrain

This seems to show the use of FinFly Web to offer visitors to the website a fake flash update in order to facilitate the installation of malware. Presumably, the operators either did not pay for, or did not decide to use the FinFly Exploit Portal which would have allowed silent installation of a backdoor as per the example in the product description:

"A Target was identified within a Discussion Board but no direct or Email contact was possible. The Agency created a Webserver containing an Internet Explorer 0-day Exploit which deployed the Payload on the Target System once the Target opened the URL that was sent to him through a private message in the Discussion Board."

The same recent document releases include an internal "FAQ" document, apparently for FinFisher salespeople, that may indicate an association with the well known exploit vendor VUPEN, although this cannot be independently verified :

"Q: Can you supply a list of the current exploits?
A: Yes but we need to do this individually for each request as the available exploits change on a regular basis.

Q: Can we name the supplier?
A: Yes you can mention that we work with VUPEN here"

The feature overview for FinFly Exploit portal claims:

- Full Access to Web Portal and Exploit Generator
- Strategic Operations
- Deploys Remote Monitoring Solution on Target System through Files and Server .
- Government-Grade 0-Day Exploits which function on multiple Systems and Patch-levels without further modification
- At least 4 major Exploits (common Browser/Mail/File-Viewer Software) permanently available
- 30 day warranty for every Exploit within the Portal
- Permanently updated 1-Day Exploits for various Software

HACKING TEAM

The Milan-based "Hacking Team S.R.L." provides similar services to the FinFisher suite sold by Gamma Group. On Hacking Team's website they state:

"…we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities."

Their primary offering is surveillance malware for OSX, Windows, Linux, iOS, Android, BlackBerry, and Windows Mobile. As a delivery mechanism for this malware, they sell a network injection appliance designed to be deployed in an ISP in a similar manner to FinFly ISP.

In Hacking Team's documentation, they define their Network Injector as a:

"Hardware component that monitors the target's network traffic and injects an agent into selected Web resources. It comes in two versions, Appliance or Tactical: the former is for deployment at the ISP, the latter for use on the field."

8

The Network Injector

Presentation

Introduction

Network Injector allows you to tap the target's HTTP connections and inject an agent on the device.

Figure 11: Hacking Team's RCS 9 Technician Guide

They stipulate:

"Resources that can be infected by RCS are any type of files. NOTE: Network Injector is not able to monitor FTP or HTTPS connections."[8]

In addition to network injection, Hacking Team's offering provides:

- Wifi password cracking
- The ability to fake wifi Access Points
- Traffic monitoring for compromised networks
- Injection in non-ISP environments (ie hotels)

This functionality would not create the paper trail of an ISP-based deployment. As with IMSI catchers and similar tools, this raises important questions about whether jurisdictions where it is deployed have the proper structures for judicial oversight. As it is portable, and doesn't require the cooperation of an ISP, it could conceivably also be used for foreign hostile intelligence gathering.

Hacking Team has filed for patents on a "Method and Device for Network Traffic Manipulation" as can be seen below:

US 20130132571A1

(19) **United States**

(12) **Patent Application Publication**

Ornaghi et al.

(10) **Pub. No.: US 2013/0132571 A1**

(43) **Pub. Date: May 23, 2013**

(54) **METHOD AND DEVICE FOR NETWORK TRAFFIC MANIPULATION**

(75) Inventors: **Alberto Ornaghi**, Treviglio (IT); **Marco Valleri**, Lecce (IT); **Daniele Milan**, Robecchetto Con Induno (IT); **Valeriano Bedeschi**, Milano (IT)

(73) Assignee: **HT S.R.L.**, MILANO (IT)

(21) Appl. No.: **13/813,496**

(22) PCT Filed: **Aug. 3, 2010**

(86) PCT No.: **PCT/IT2010/000352**

§ 371 (c)(1), (2), (4) Date: **Jan. 31, 2013**

Publication Classification

(51) **Int. Cl.**
H04L 29/08 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 29/08099*** (2013.01)
USPC **709/224**

(57) **ABSTRACT**

A device for manipulating data traffic related to a target connected to a data communications network whose elements communicate by means of an HTTP protocol comprises: a redirection device, which is adapted to be connected to the data communications network by means of a plurality of sniffing interfaces and a packet sending interface; a proxy, which is adapted to be connected to the data communications network by means of an HTTP connection interface, a packet receiving interface and a packet injection interface; and is characterized in that the redirection device is configured to monitor, by means of the sniffing interfaces, the network traffic in order to identify within the network traffic at least one data packet associated with the target and to redirect, by means of the packet sending interface, the at least one data packet associated with the target toward the proxy.

Figure 12: Hacking Team's patent application for "Method and Device for Network Traffic Manipulation". (Source)

Bibliographic data: CA2807011 (A1) — 2012-02-09

In my patents list | EP Register | Report data error | Print

METHOD AND DEVICE FOR NETWORK TRAFFIC MANIPULATION

Page bookmark	CA2807011 (A1) - METHOD AND DEVICE FOR NETWORK TRAFFIC MANIPULATION
Inventor(s):	ORNAGHI ALBERTO [IT]; VALLERI MARCO [IT]; MILAN DANIELE [IT]; BEDESCHI VALERIANO [IT] +
Applicant(s):	HT S R L [IT] +
Classification:	- international: *H04L29/08*
	- cooperative: H04L29/08099; H04L29/12066; H04L61/1511; H04L67/025; H04L67/2804; H04L67/2814; H04L67/02
Application number:	CA20102807011 20100803
Priority number(s):	WO2010IT00352 20100803
Also published as:	WO2012017457 (A1) US2013132571 (A1) SG187244 (A1) MX2013001429 (A) KR20130096250 (A) → more

Figure 13: Hacking Team's patent application for "Method and Device for Network Traffic Manipulation". (Source)

The patent filing provides a breakdown on the design of the network injection appliance:

> A device (50) for manipulating data traffic related to a target (20') connected to a data communications network whose elements communicate by means of the HTTP protocol comprises: a redirection device (90), which is adapted to be connected to the data communications network by means of a plurality of sniffing interfaces (110) and a packet sending interface (120); a proxy (100), which is adapted to be connected to the data communications network by means of an HTTP connection interface (130), a packet receiving interface (120') and a packet injection interface (140); and is characterized in that the redirection device (90) is configured to monitor, by means of the sniffing interfaces (110), the network traffic in order to identify within the network traffic at least one data packet associated with the target (20') and to redirect, by means of the packet sending interface (120), the at least one data packet associated with the target (20') toward the proxy (100), said proxy (100) being configured to send, by means of the HTTP connection interface (130), an HTTP request toward elements of the data communications network, said HTTP request being based on the content of the data packet associated with the target (20'), and to send, by means of the packet injection interface (140), data to the target (20'), said data being based on the data received in response to the HTTP request.

Figure 14: Hacking Team's patent application for "Method and Device for Network Traffic Manipulation". (Source)

Exploitation of Google and Microsoft

As described in the Citizen Lab report Police Story: Hacking Team's Government Surveillance Malware, material was provided to the Citizen Lab which appears to document the operation of several Hacking Team products. As stated previously, we have no knowledge as to the origin of the documents, and whoever sent them took steps to conceal their identity. While **the authenticity of these documents is unverified**, we have not identified inconsistencies with what is currently known about Hacking Team RCS.

The Hacking Team Network Injector monitors all HTTP connections and, following the injection rules, identifies the target's connections and injects the agent into the connections, linking it to the resources the target is downloading from the Internet.

Below is a screenshot from Hacking Team's network injection appliance.

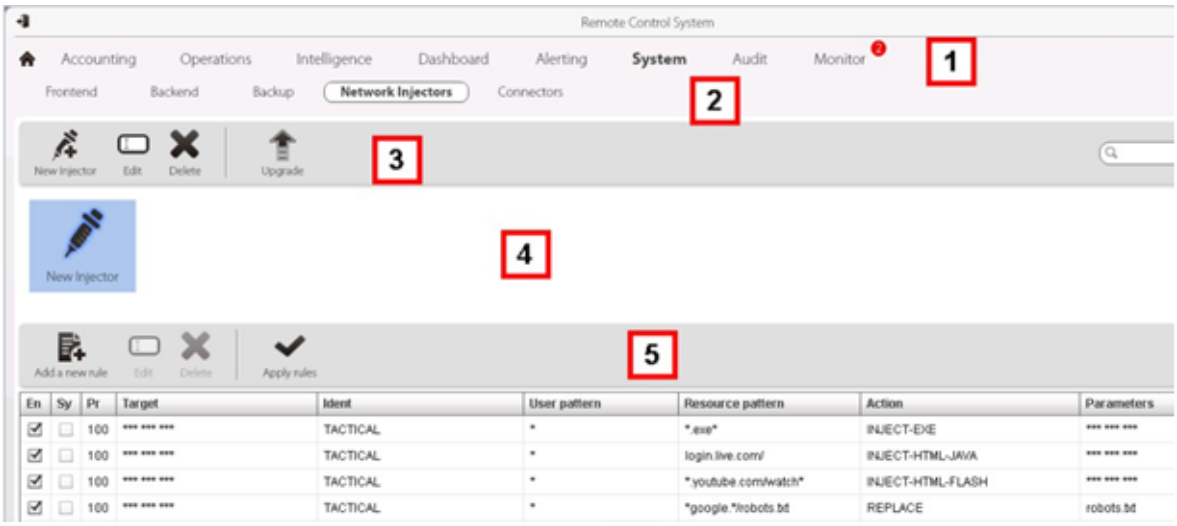

Figure 15: Image Source: "Hacking Team, RCS 9: The hacking suite for governmental interception, System Administrator's Guide," 2013

Network Injectors allow for automatic identification of target devices and infect them according to the rules set via their control software. As shown above, the appliance exploits YouTube users by injecting malicious HTML-FLASH into the video stream. From the description of the rule targets below, this appears to be a custom payload designed for YouTube.

Description

Infection method that will be applied to the resource indicated in **Resource pattern**:

Method	***Function***
INJECT-EXE	Infects the downloaded EXE file in real time. The agent is installed when the target runs the EXE file.
INJECT-HTML-FILE	Lets you add the HTML code provided in the file in the visited web page. Please contact HackingTeam technicians for further details.
INJECT-HTML-FLASH	Blocks videos on youtube and requires the user to install a fake Flash update to view them. The agent is installed when the target installs the update.
INJECT-UPGRADE	Notifies the Java Runtime Environment on the device that an update is available. The agent is installed when the target installs the update. Does not refer to **Resource pattern**.
REPLACE	Replaces the resource set in the **Resource pattern** with the supplied file. Tip: this type of action is very effective when used in combination with Exploit generated documents.

Figure 16: Image Source: "Hacking Team, RCS 9: The hacking suite for governmental interception, System Administrator's Guide," 2013

While this infection method requires user interaction to accept the fake Flash update, it is also possible to bundle the payload with an exploit in order to silently install the surveillance agent.

To provide an example of how a deployment of a tactical surveillance implant would work using a system like this, we refer you to the illustration below (click to enlarge):

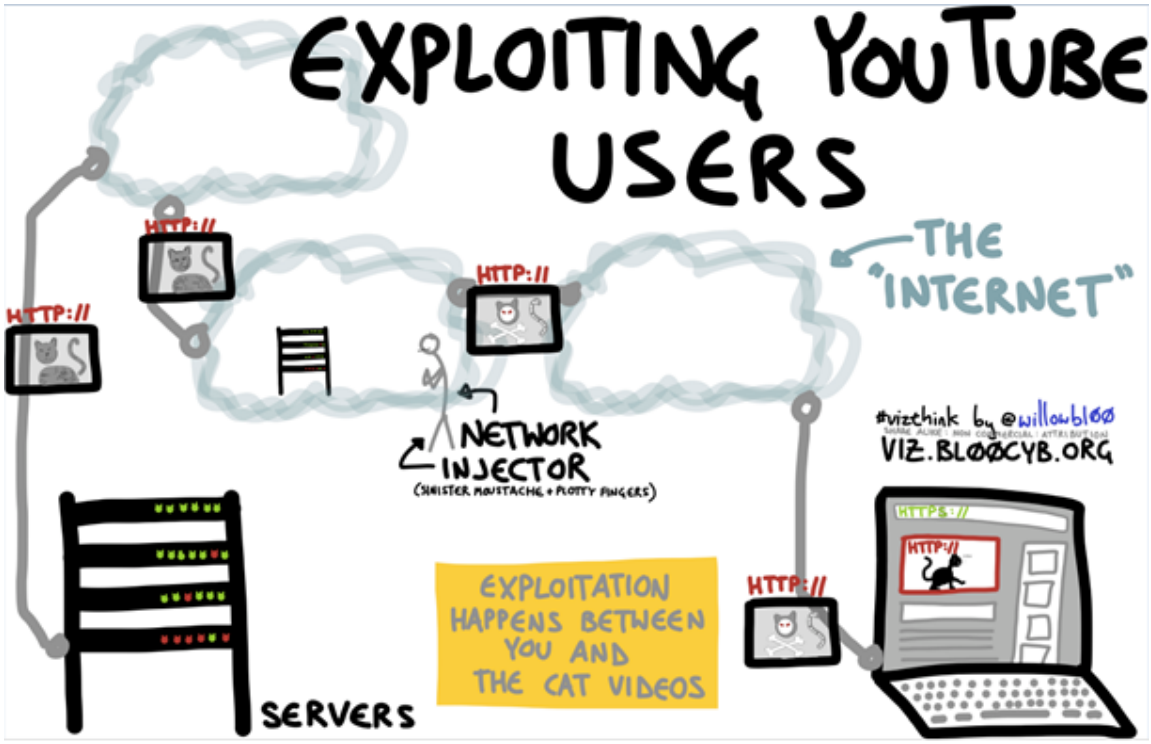

Figure 17: A diagram explaining the exploitation of YouTube Users [Illustration by Willow Brugh]

In this diagram, the user (watching a cute cat video) is represented by the laptop, and YouTube is represented by the server farm full of digital cats. You can observe our attacker using a network injection appliance and subverting the beloved pastime of watching cute animal videos on YouTube.

A step-by-step breakdown of how such an attack might occur is as follows:

1. A target is selected and their name is entered into the Network Injection GUI.
2. The target's traffic stream is located based on their ISP's RADIUS records.
3. As per the rule on the network injector (as shown in Figure 14), the appliance waits for the target to visit YouTube.
4. When this traffic is identified, it is redirected to the network injection appliance.
5. The legitimate video is blocked and malicious flash (SWF) is injected into the clear-text portion of the traffic. (Represented by the kitty skull and cross bones.)
6. The target is presented with a dialogue to upgrade their flash installation. If this upgrade is accepted the malicious SWF enables the installation of a 'scout agent' which provides target validation.
7. If the target is assessed as correct (i.e., the desired person), and safe for install (not a malware analysis honeypot), then the full agent is deployed.

8. Surveillance of the target commences.

gdata-issues
Server-side issues and feature requests

Project Home | Issues

New issue | Search | All issues | for youtube https | Search | Advanced search | Search tips | Subscriptions

Issue 2964: On secure page get_video_info redirects to non-HTTPS video
9 people starred this issue and may be notified of changes.

Status: WontFix
Owner: ----
Closed: Sep 2012
Type-Defect
API-YouTube

Add a comment below

Reported by alexey.b...@gmail.com, Sep 9, 2012

```
Name of API affected:
YouTube Data API

Issue summary:
On site working with HTTPS protocol, YouTube videos loaded with IFRAME API in not-secure way - via HTTP instead of HTTPS.

Steps to reproduce issue:
1. Save attached file to secure hosting or open working example https://dl.dropbox.com/u/36706/web/youtube-non-secure-video.html
2. If opening in Google Chrome, you will see notice in console that page displayed insecure content - that is about video file loaded
via HTTP instead of HTTPS.
You can see attached Web inpector's log for requests that video come via HTTP protocol.

Expected output:
Video clip loaded in secure way via HTTPS protocol.

Actual results:
Video clip loaded via HTTP protocol.

Notes:
As I saw in browser requests, https://www.youtube.com/get_video_info returns wrong result with link to the clip.
```

web-inspector.har
59.2 KB View Download

youtube-non-secure-video.html
504 bytes View Download

Figure 18: Google issue tracker for unencrypted YouTube streaming. Marked as "WontFix"

After being alerted by the author of this post to the sale of devices to exploit YouTube users, a representative at Google stated on July 22nd, 2014 that they were accelerating two changes. All users using an extension like HTTPS Everywhere will now receive the full page and video stream over TLS. Additionally, a roll-out of full-TLS YouTube is being carried out for all users, independent of login state.

Microsoft Clear-Text Login

Windows Live presents another attack surface used by Hacking Team's network injection appliance. Unlike some other free webmail providers, some elements of the login page are provided to the user in clear-text, making them observable to a network adversary and consequently easy to tamper with.

As shown in Figure 14 above, a network injection rule exists for the login service for Microsoft's live.com website. When a target loads the login.live.com website, the INJECT-HTML-JAVA payload is deployed. This payload alerts the user of an update to java and installs the RCS agent. It is additionally possible to use an exploit for silent installation.

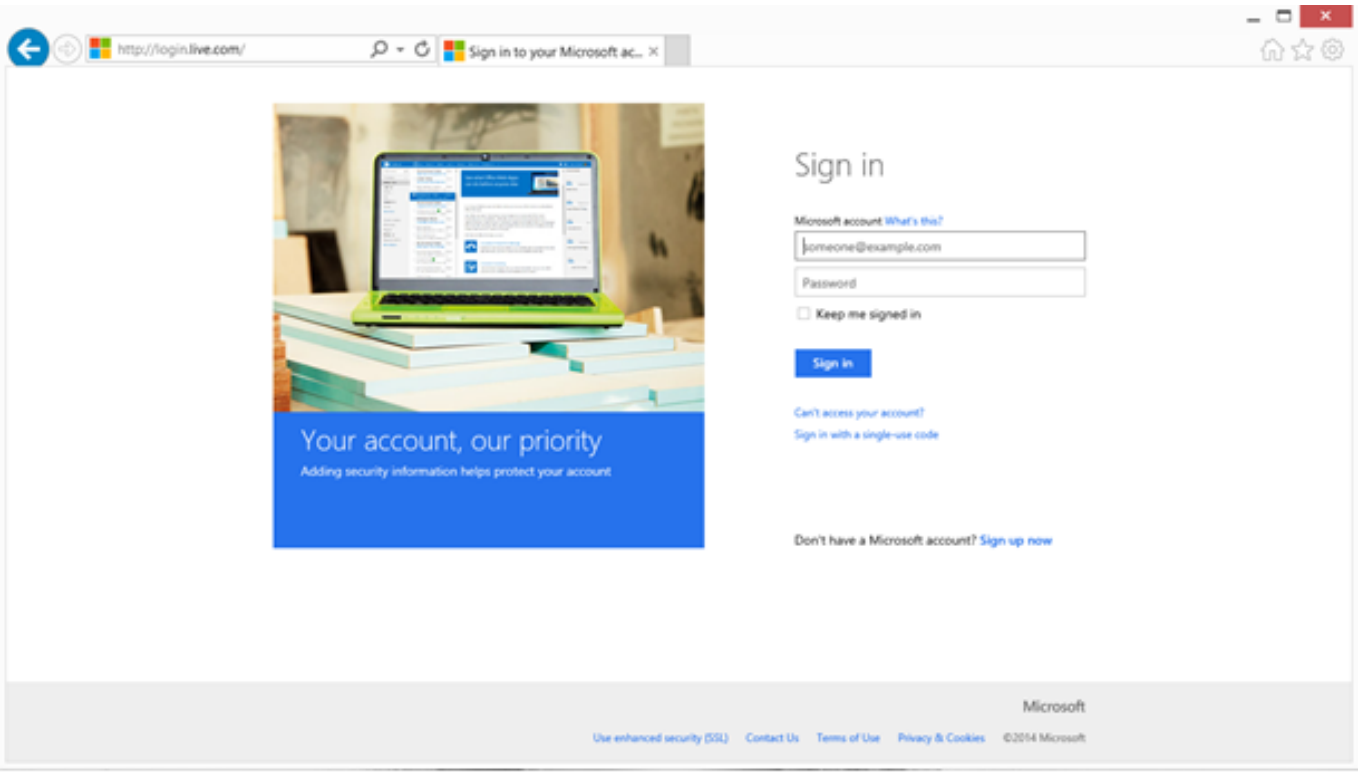

Figure 19: Login page for Microsoft's Live service being served over HTTP

As discussed previously, this type of injection can occur since it is possible to load this page over HTTP.

We alerted Microsoft to this issue and on August 6th, they pushed out a hotfix to automatically force all users to use https://login.live.com.

Mitigation and Prevention Measures

Clear-text is dead

Thus far we have provided two examples of commercial tools that have widely proliferated and that enable purchasers (for a fee) to exploit clear-text traffic in some of the most popular sites on the web.

In order for network injection appliances to function, they rely on the fact that popular websites will not encrypt all of their traffic. In order to mitigate these types of attacks, we suggest that providers serve all content over TLS, and provide end-to-end encryption wherever possible. The use of HSTS and certificate pinning is also strongly recommended.

Historically, it has been considered expensive to run cryptography for major services. This has helped delay the widespread adoption of encryption especially for websites that provide a free service to a large number of users. This is no longer the justification that it once was. In a recent presentation at IETF 90 on HTTP/2, Google's Adam Langley said: "Clear-text is no longer reasonable."

For the average user, no complete solutions to this problem currently exist. The Electronic Frontier Foundation's HTTPS Everywhere has been a good start toward allowing users to request that companies serve them data in an encrypted manner. Even while using this plugin, however, data can still be delivered to the user without HTTPS, including sites where some data is encrypted. There is a plugin currently available, HTTP Nowhere, which claims to allow only encrypted traffic; however, as currently implemented, it might break the functionality of popular websites.

Enabling this feature is an entertaining illustration of how much the user experience of web browsing is still dependent on unencrypted data.

As always, it would be wise to avoid downloading programs from sites that do not use HTTPS and be extremely cautious about sites that prompt you to unexpectedly install software.

CONCLUSION

The proliferation of tools for both tactical and on network injection attacks highlights a vulnerability that has existed since the beginning of the consumer Internet. Until recently, however, it has been challenging to gauge the practical viability of this attack and the number of actors that might have this capability. Hacking Team and FinFisher are probably not unique in packaging and selling these techniques. In terms of surveillance vendors that provide such technology, it seems likely that this is but glimpse into a larger market.

Currently, those residing in or traveling to countries where we and others have identified the presence of these tools have few options for protecting themselves beyond the use of private networks such as VPNs.

This report is not the first to highlight the problem. It is, however, no longer the case that cryptography is so resource intensive that this problem cannot be solved. What is required is a recognition on the part of content and service providers that this falls within the scope of their responsibility to provide secure service to their users. In response to this research, Google and Microsoft have already made statements indicating they are working on the problem. We hope that other providers will take their cues from this and undertake similar measures.

ACKNOWLEDGEMENTS

I would like to thank my colleagues at Citizen Lab for their invaluable assistance with this report. Especially: John Scott-Railton, Sarah McKune, Masashi Nishihata, Adam Senft, and Ron Deibert. Also, Bill Marczak and Claudio Guarnieri for their work in this area over the last two years.

A very special thank you to Willow Brugh for her illustrative skills.

Additionally, I'd like to thank Katie Moussouris and Heather Adkins for support, and the members of the Google Security team and the MSRC for their responsiveness.

My gratitude to the Electronic Frontier Foundation and Privacy International.

FOOTNOTES

[1] http://government-contractors.findthebest.com/l/160067/Cloudshield-Technologies-Inc-in-Sunnyvale-CA
[2] Detailed later in this report.
[3] This assumes fully functioning encryption. Obviously there are potential protocol attacks or algorithm attacks which may allow for decryption of traffic.
[4] Such as the version of FinFly ISP documented in 2011 by Wikileaks in 'The Spy Files'
https://wikileaks.org/spyfiles/docs/gamma/309_remote-monitoring-and-infection-solutions-finfly-isp.html
[5] The open-source penetration-testing tool Evil-Grade was a proof-of-concept tool which used this technique
http://www.infobyte.com.ar/down/isr-evilgrade-Readme.txt
[6] http://www.zdnet.com/top-govt-spyware-company-hacked-gammas-finfisher-leaked-7000032399/
[7] https://twitter.com/GammaGroupPR/status/497086972864000000
[8] Hacking Team, RCS 9: The hacking suite for governmental interception, System Administrator's Guide," 2013