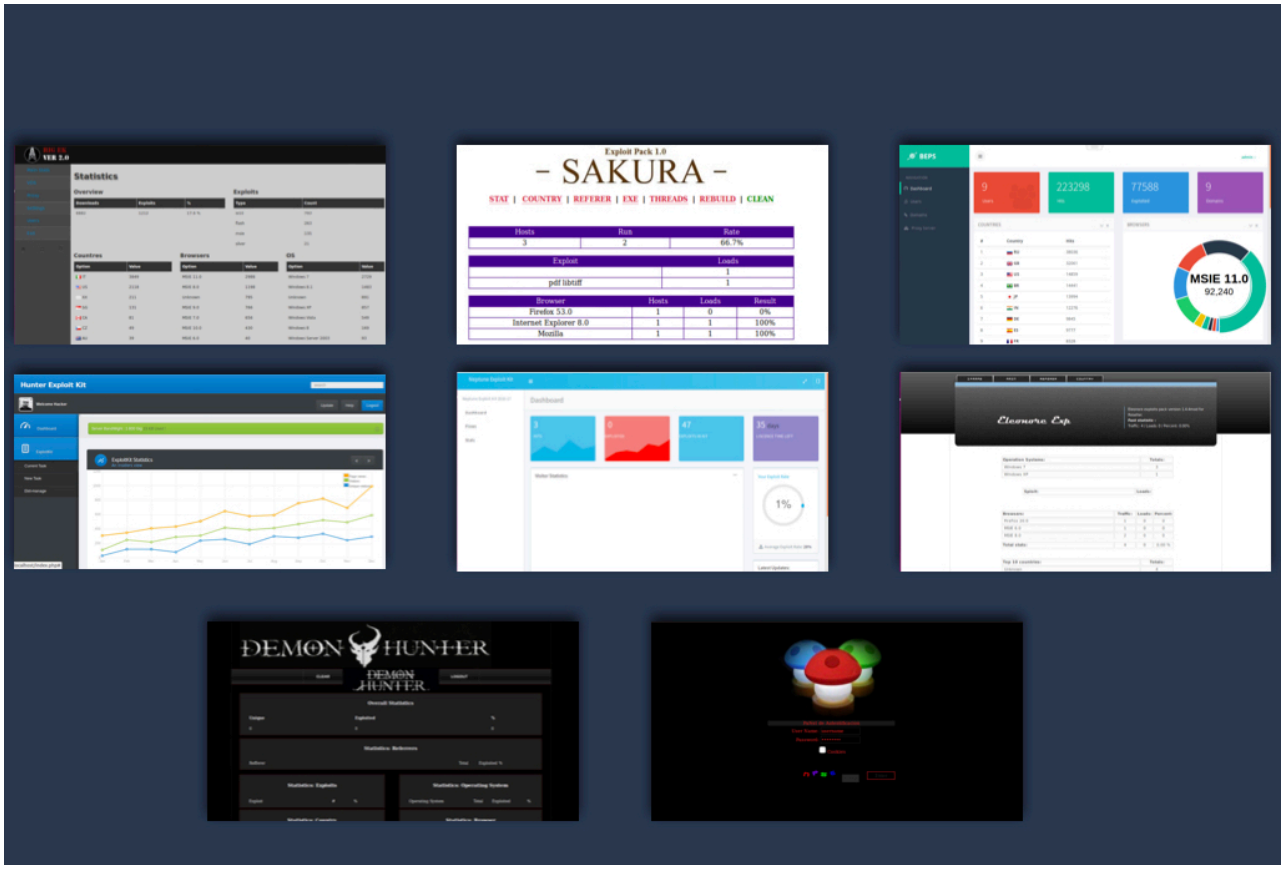
Counter Infiltration

Future Proof Counter Attacks Against Exploit Kit Infrastructure



Yin Minn Pa Pa, Hiroshi Kumagai, Masaki Kamizono, Takahiro Kasama

Black Hat Asia 2018

Table of Contents

List of Figures

List of Tables

Introduction

Recently, operators behind exploit kit as a service offering put more effort into hiding their operational infrastructure while providing better service to their customers. Namely, almost all popular exploit kits nowadays are operated using sophisticated networks of several servers such as proxies or gates, VDS (Virtual Dedicated Server), rotators, up-loaders, panel servers, APIs and more. This complex setup makes it very hard for researchers to analyze the inner workings of these networks, thus limiting the information security community's ability to respond to such threats. However, this customer facing approach also exposes the operators to direct attacks from researchers.

Over the past year, we have replicated several exploit kit infrastructures from leaked sources. This allowed us to gain a deeper understanding of their inner workings, choke points, and weaknesses. We discovered several attacks with the potential to take down an exploit kit that may be performed with nothing but regular customer privileges. We discuss all of these potential attacks in this paper and demonstrate some attacks as a user of the RIG 4.0 exploit kit, which a very recent and currently highly active exploit kit. Our approach let us detect several proxy servers belonging to RIG 4.0, find the actual IP of panel server hiding behind cloud services, and even discover new vulnerabilities revealing who the attackers are, how many attackers are using the RIG 4.0 exploit kit as a service, what kind of exploits they are using and which victims are most likely to be successfully exploited. Furthermore, our curiosity even let us figure out how rich the operators are.

In addition, we also found that code and design-pattern reuse among different exploit kits is frequent, thereby allowing us to use the same attacks against different exploit kits. Thus, it is likely that the same approaches will work for the detection and takedown of future exploit kits as well.

In this paper, we will share our findings, analytical approaches, and recommendations for future engagement with similar offerings. We will also share insights into the customers of these services. The following are the three main takeaways from this paper.

- How exploit kit services work internally, what services they offer to customers, who the customers are, how they hide from detection and what their weaknesses are.
- What actions may take exploit kits down.
- How different exploit kits relate to one another and how this knowledge can be used for taking down future exploit kits.

Chapter 1

Background

Exploit Kit

An Exploit Kit is a suite of web applications for automated attacks. It is used by attackers for drive-by download attack in which, when an innocent victim accesses a malicious website, he or she is redirected through several servers until reaching the landing server, fingerprinted, served with a suitable exploit and finally lead to malware infection. An exploit kit automates all these processes of redirecting, fingerprinting, exploiting and infecting with malware. Malware dropped by an exploit kit - also known as the payload - ranges from cryptocurrency miner malware to ransomware depending on different campaigns setup by attackers.

Exploit Kit Offerings

There are two types of exploit kit offerings: Exploit Kit as a **Service** and Exploit Kit as a **Package**. In exploit kit as a service offering, an attacker pays for a service and he does not need to take care of any server in the attack infrastructure. The attacker does not have control over exploits and only needs to set up which malware he wants to use for a campaign. He contacts the exploit kit operator in an underground market through instant messaging, mostly Jabber, to negotiate a service contract. Transactions are conducted mostly with Bitcoins and the price varies from $80 to $4000. Recent exploit kits are mostly offered as a service to the attacker.

In contrast with this, an attacker may also pay for an exploit kit application package for which servers and attack infrastructure need to be set up according to the manual in the package. The attacker has admin privileges on the panel server and he can update the exploit kit application.

General Attack Infrastructure

In order to protect themselves, recent exploit kits have a sophisticated attack infrastructure including proxy servers, API servers, VDS servers, update servers, etc. A general rule is that the older the exploit kit is, the simpler the infrastructure becomes; in its barest form consisting of only a panel server and landing page.

Live Exploit Kits

The exploit kit landscape has been rocky since 2016 with newer kits constantly replacing the taken down kits. Some active exploit kits in recent years are:

- RIG
- Disdain
- Nebula
- Sundown Pirate
- Neptune

RIG 2.0, one of the most prolific exploit kits, was leaked in February 2015. The recovered version named RIG 3.0 was seen in August 2015 again with an average of 27,000 machines being infected per day. RIG was the dominant exploit kit during 2016 but attacks relating to RIG 3.0 started to decline in April 2017. From August 2017, RIG 4.0 came onto the scene and attacks relating to it seem to increase until the time of this writing in February 2018. RIG 4.0 exploit kit services costs $500 and $1500 for a week and a month respectively.

Disdain was sold on an underground forum in August 2017 and seems to be a copy and paste version of the BEPS/Sundown exploit kit leaked in February 2017. It is available for rent on a daily, weekly, or monthly basis. The prices are $80, $500, and $1,400 respectively.

The Nebula Exploit Kit came onto the scene on February 2017. It is likely to be a variant of BEPs/Sundown whose source code was leaked in February 2017. It has a subscription for 24 hours, one week, one month and prices of $100, $600 and $2000 respectively.

Sundown-Private was uncovered in June 2017. It borrows code from its predecessors the Hunter and Terror exploit kits whose source code was leaked in October 2016. The Hunter exploit kit costs $2500 for a lifetime package.

The Neptune exploit kit was first seen on underground forums in October 2016. In the advertisement, the author claims that it has 17 different exploits. In August 2017, the Neptune exploit kit is used for dropping a cryptocurrency - specifically Monero - miner. Depending on the type of the package, the Neptune exploit kit costs from $2400 to $4000 per month and from $750 to $950 per week.

In fact, all these new exploit kits are updated versions of exploit kits leaked in previous years. Figure 1 shows the results of our initial studies on how new exploit kits are based on leaked kits. Namely, RIG 4.0 is completely based on the leaked RIG 2.0 exploit kit. Disdain and Nebula are based on the previously leaked BEPs/ Sundown. In the same way, Sundown Pirate and Neptune also depend on the leaked kits Hunter and Neptune respectively.

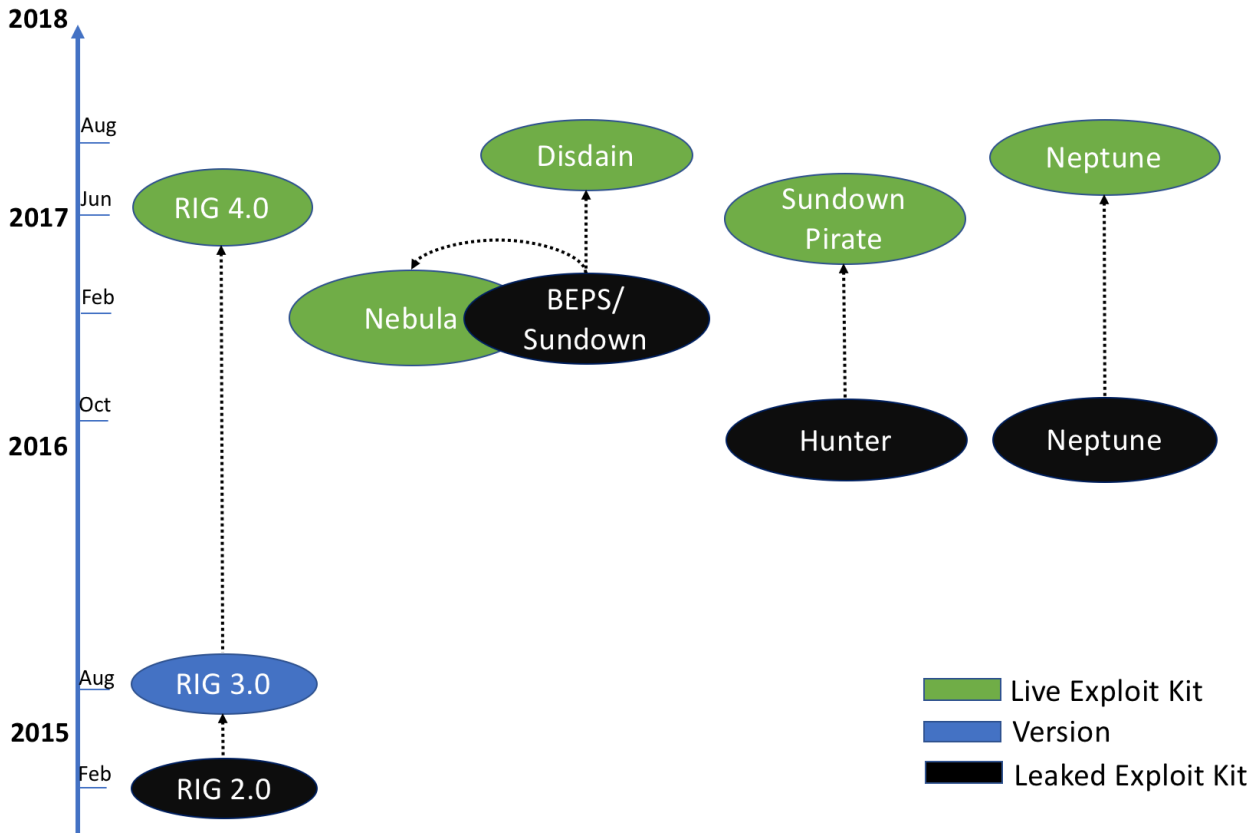


Figure 1 - New Exploit Kits and their predecessors

Chapter 2

Leaked Exploit Kits

We have collected leaked exploit kits from many different available information sources on the Internet such as Cerberus, which is a file sharing service on the dark web, leaked forums, GitHub and Virus Total. We were able to collect 33 different exploit kits and 44 kits in total as some kits have different versions.

We analyzed all the kits to see whether they include exploits, payloads (malware), databases, code for connecting and controlling servers and how many different servers need to be set up to replicate the kits in our lab environment. In general, most exploit kits include database schema, exploits, payloads, and control panel web applications. Some kits have dumped SQL database with more than 400,000 records of the exploit kit's users, referrer URLs, fingerprints of infected victims and exploit details.

In addition to the control panel web application, we notice that some kits have code for proxy servers, landing servers, uploader servers, update servers and SSH servers. Most kits seem to be able to be set up on LAMP (Linux, Apache, MySQL, PHP) while a few need to be set up on an Nginx and Oracle DB environment. Table 1 shows the summary of our analysis results.

Table 1 - Leaked Exploit Kits

NO	Name	Version	Exploit	Payload	Panel Server			Proxy Server		Landing Server		Server Types	Other Servers
					Data in DB	DB Schema	Control Code	Connect Codes	Control Codes	Connect Codes	Control Codes		
1	RIG	1007 1/2	×	✓	✓	✓	✓	×	✓	×	✓	LAMP	VDS Server
2	Sakura	2014	✓	×	×	✓	✓	-	-	-	-	LAMP	Exploit Server
3	BEPS/Sundown	2017	×	✓	✓	✓	✓	✓	✓	×	×	Nginix	Rotator Server
4	Hunter	2015	✓	✓	✓	✓	✓	-	-	-	-	LAMP	Update Server
5	0x88	master	✓	✓	✓	✓	✓	-	-	-	-	LAMP	-
		2.6	×	×	✓	✓	✓	-	-	-	-	LAMP	-
		3.0	×	×	✓	✓	✓	-	-	-	-	LAMP	-
6	Neptune (blaze)	2017	✓	✓	×	✓	✓	-	-	✓	✓	LAMP	Uploader Server SSH Server
7	Siberia	2011	×	×	×	✓	✓	-	-	-	-	LAMP	-
8	Sava	2011	✓	✓	×	✓	✓	-	-	-	-	Oracle	-
9	Elenore	2010/ 1.4.4	✓	×	×	✓	✓	-	-	-	-	LAMP	-
	Elenore Exp	1.2	✓	×	✓	✓	✓	-	-	✓	-	LAMP	-
10	Fragus	2009	✓	×	×	✓	✓					LAMP	-
11	Demon Hunter	01.11.2014	✓	✓	×	✓	✓	-	-	✓	✓	LAMP	-
12	Impassion Frameshit	-	✓	✓	✓	✓	✓	-	-	-	-	LAMP	-
13	adpack-1	1	✓	✓	×	✓	✓	-	-	-	-	LAMP	-

	adpack-2	2	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
14	Armitage	-	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
15	cry217	-	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
16	fiesta	1	✓	×	×	✓	✓	-	-	-	-	LAMP	-
		2	✓	×	×	✓	✓	-	-	-	-	LAMP	-
17	firepack	1	✓	×	×	✓	✓	-	-	-	-	LAMP	-
		2(0.18)	✓	×	×	✓	✓	-	-	-	-	LAMP	-
18	g-pack	-	✓	×	×	✓	✓	-	-	-	-	LAMP	-
19	ice-pack	1	✓	×	×	✓	✓	-	-	-	-	LAMP	-
		2	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
		3	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
20	infector	-	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
21	mpack	none	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
		81	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
		86	×	✓	×	✓	✓	-	-	-	-	LAMP	-
		99	×	✓	×	✓	✓	-	-	-	-	LAMP	-
22	multisploit	none	×	✓	×	✓	✓	-	-	-	-	LAMP	-
		v3	✓	×	✓	✓	✓	-	-	-	-	LAMP	-
23	my-poly-sploit	-	✓	×	×	✓	✓	-	-	-	-	LAMP	-
24	RDS	-	×	×	×	✓	✓	-	-	-	-	LAMP	-
25	SmartPack	-	✓	×	×	✓	✓	-	-	-	-	LAMP	-
26	Target Exploit	-	✓	×	×	✓	✓	-	-	-	-	LAMP	-
27	Tor	-	✓	✓	×	✓	✓	-	-	-	-	LAMP	-
28	Mushroom	2011	✓	✓	×	✓	✓	-	-	✓	✓	LAMP	-
29	Bleeding Life	-	Code cannot be read										
30	Crimepack	-	Code cannot be read										
31	DCpp	-	C++ files										
32	Phoenix	2.5	Old exploit kits based on PHP and needs to set up MySQL server together with SMB server.										
33	Blackhole	100	Code cannot be read										
		102	Code cannot be read										

Chapter 3

Replicating Exploit Kits

Recent and highly active exploit kits such as RIG 4.0, Nebula, Disdain, Sundown Pirate, and Neptune are in fact updated versions of leaked exploit kits such as RIG 2.0, BEPS/Sundown, Hunter and Neptune exploit kits. Thus, in this chapter, we will explain these four main predecessors of currently active exploit kits.

RIG Exploit Kit

RIG exploit kit was first seen in 2014 and it is still active at the time of this writing in February 2018. The current version is RIG 4.0. RIG exploit kit is used for several campaigns to infect victims with different malware ranging from ransomware to cryptocurrency miner malware.

A falling out between developers and one of the sellers of the RIG exploit kit resulted in a partial leak of the kit's source code on a hacker forum in February, 2015. We have downloaded the leaked kit from Github, which is RIG version 2.0, consisting of database files, cache data, and a PHP based web application for controlling servers such as proxy and panel servers. The actual exploits are not included in the leaked kit.

Servers in Attack Infrastructure

The attack infrastructure of the RIG exploit kit is composed of a panel server, TDS (Traffic Direction System) server, VDS (Virtual Dedicated Server), and proxy server.

Panel Server (Admin Account): The panel server is an Apache-based web server. The admin account has four main functions: checking exploit statistics, controlling exploit kit users, setting up cryptographic and token settings and managing URLs for VDS and Proxy servers. A screenshot of the login page to the panel server is depicted in Figure 2.

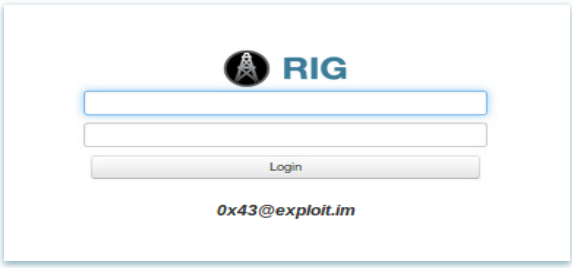


Figure 2 - RIG 2.0 Login Page

After login, admin can check statistics relating to infection rate, exploits, victim information and activities of registered exploit kit users as seen in Figure 3.

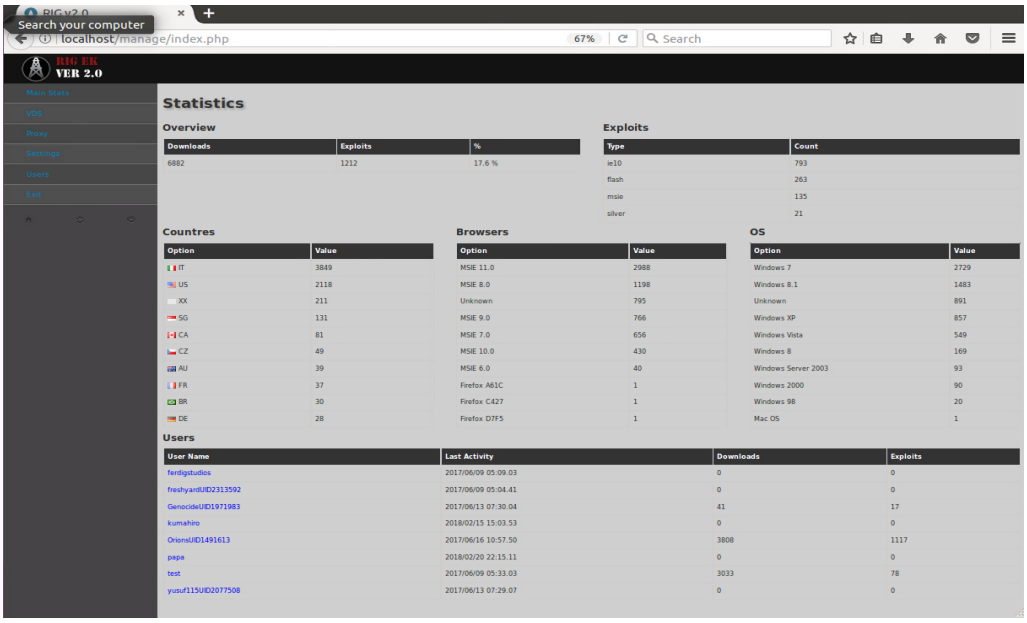


Figure 3 - Statistics

Admin can set up URLs for proxy servers and VDS as shown in Figure 4 and Figure 5. The RIG 2.0 exploit kit uses proxy servers in order to hide its actual landing server (VDS server). In addition,

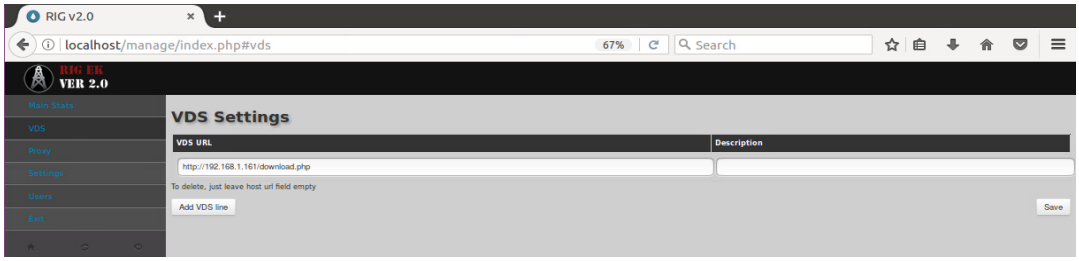


Figure 4 - VDS Setting

these proxy domains are rotated randomly in order to prevent easy takedowns and to confuse security researchers.

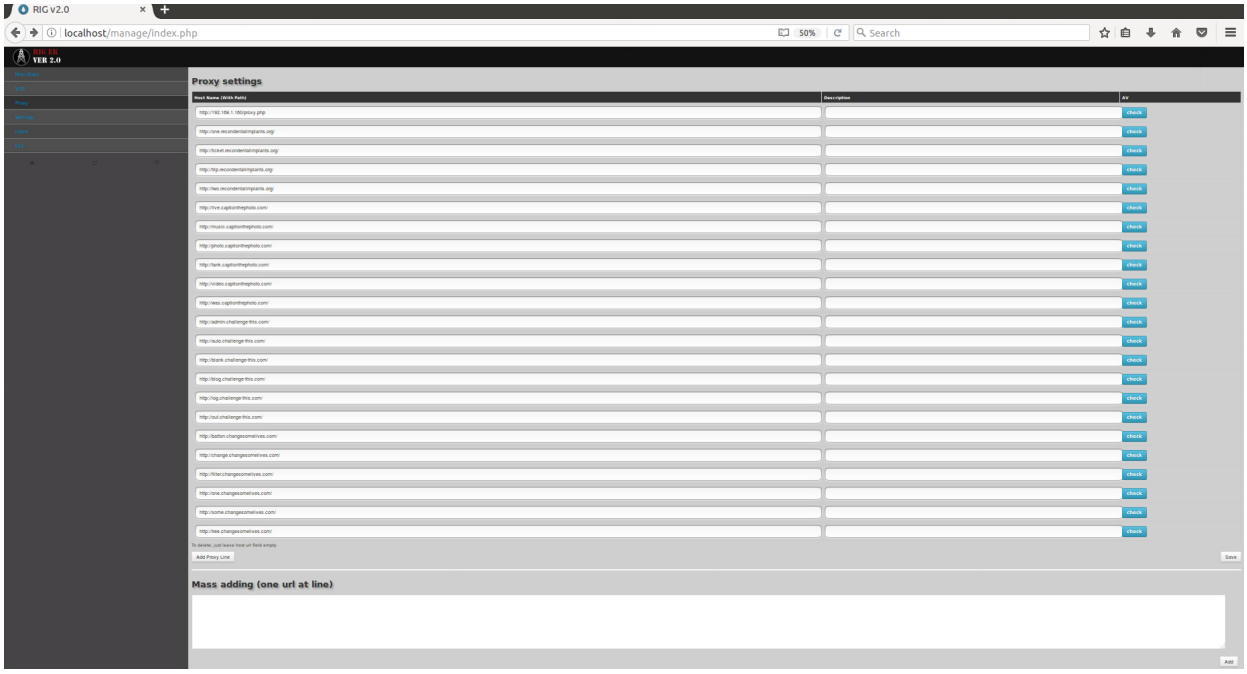


Figure 5 - Proxy Setting

As for the third function, cryptographic keys such as the data XOR key for generating API tokens and the file XOR key for encrypting payloads, TTL for the VDS server, AV warning counts to kill proxies and paths for the web application can be set up in the panel server as shown in Figure 6. It uses the Avdetect service to receive AV warning counts for proxy domain. All settings here are in fact self-protection features of the RIG 2.0 exploit kit.

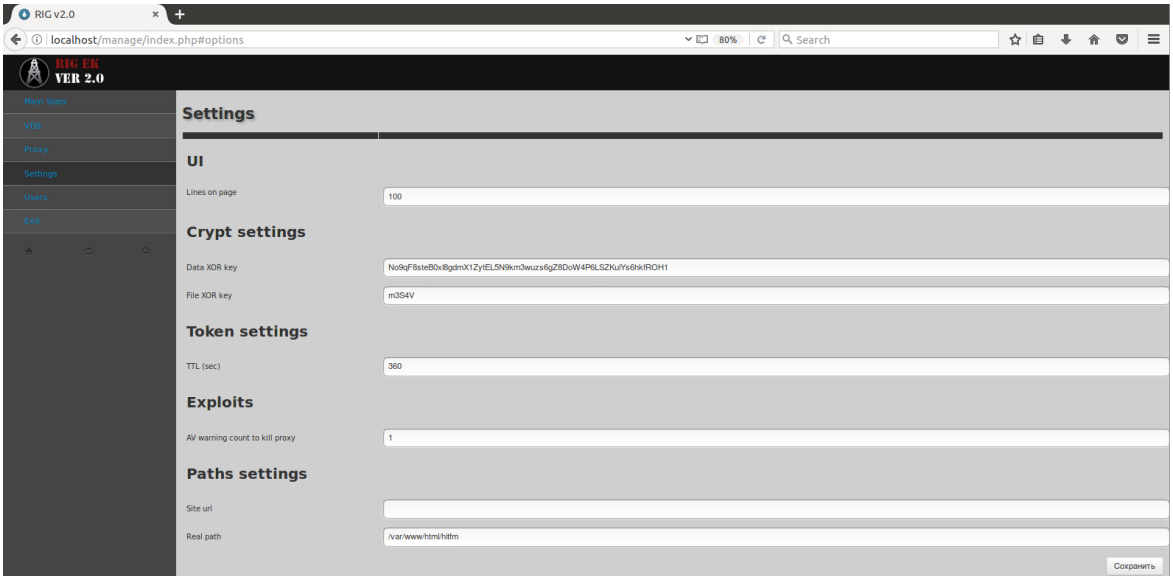


Figure 6 - Setting Page

User control function such as user privileges, passwords and expiry dates of the exploit kit users can be set in the page named “Users” as shown in Figure 7.

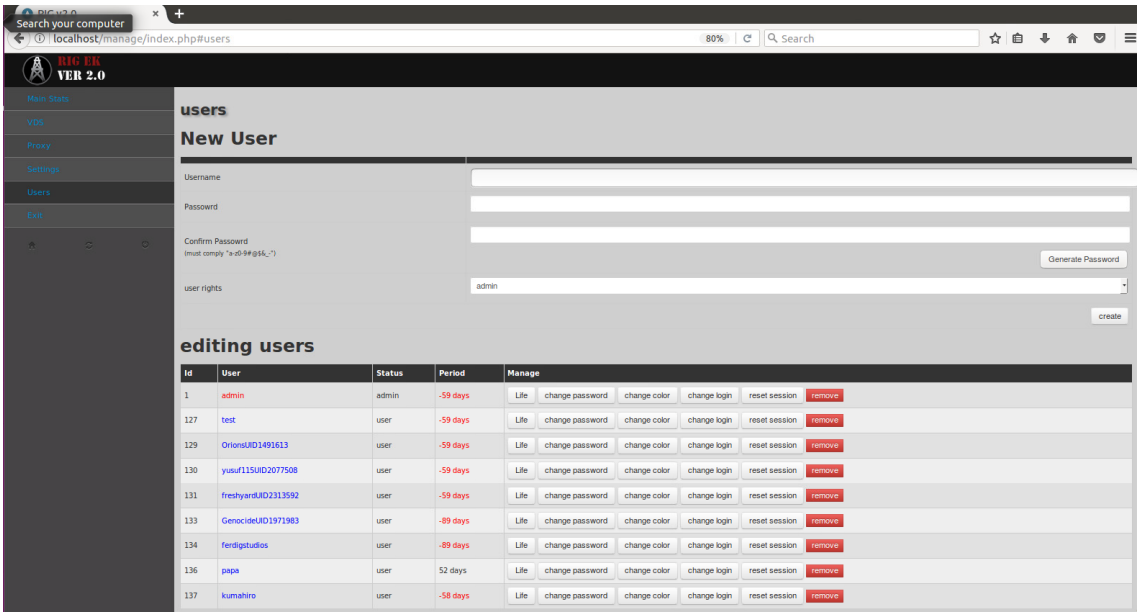


Figure 7 - User Management Settings

Panel Server (User Account): The user interface of a registered user is depicted in Figure 8.

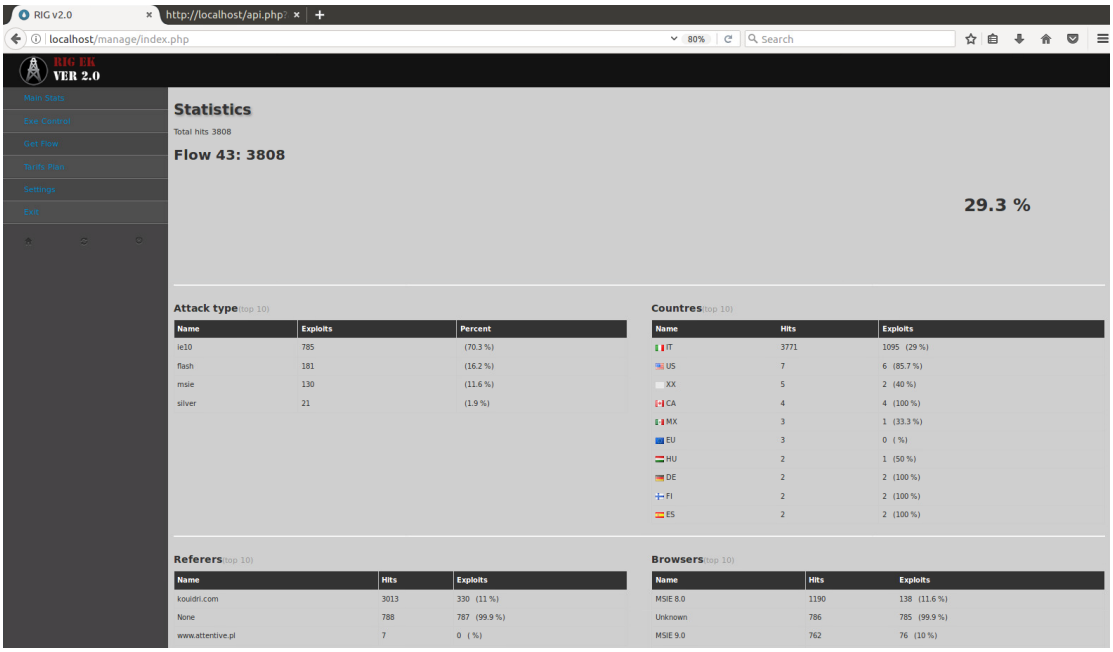


Figure 8 - Statistics (User)

The user can check exploit statistics such as infection rate at the “Main Stats” page and, upload at most two malware files (payloads) on the “Exe Control” pages shown in Figure 9.

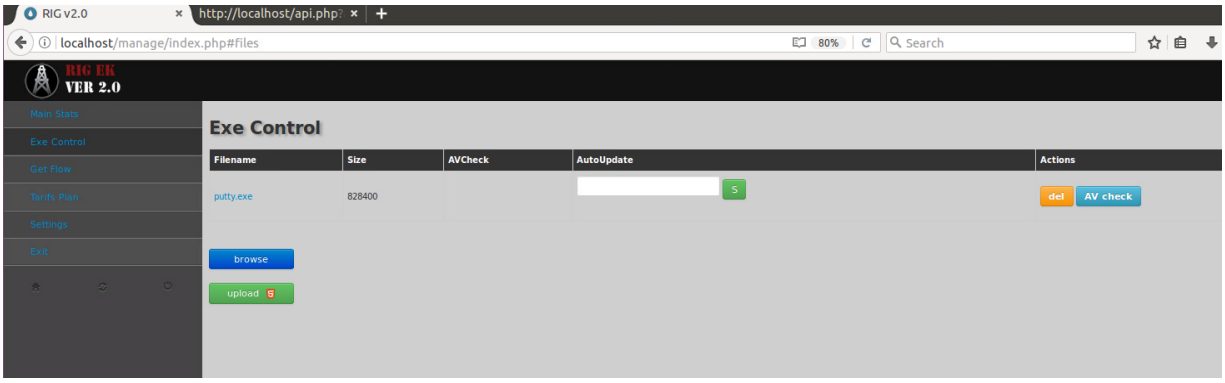


Figure 9 - Payload Control

On the “Get Flow” page depicted in Figure 10, a user can generate API links by clicking the “Get Link” button.

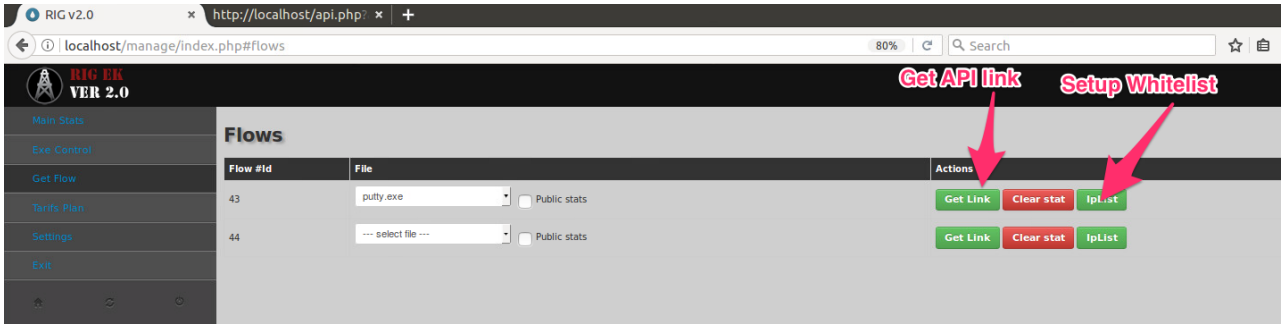


Figure 10 - API Control

The generated API link looks like “http://panel_server_domain/api.php?apitoken= l3SKfPrFJx_ESYjDJunDTaNXPBbaHE3SzYuckOM”. This API link is used for retrieving the proxy URL. The proxy URL consists of the domain of the proxy server and a PHPSSESID. For example, the proxy URL looks like “http://proxydomain/proxy.php?PHPSSESID= **njrMNruDMh7GCJzBKvPcT7tEMU7PSRnMmdLGyvrPVsbu**|ZDA0ZTUyNDA1OWMzN2EwZTEzMTM5ZWZiOGRmNjBhYTk”. The first part of the proxy URL (bolded part of PHPSSESID) consists of the domain of the VDS server (the actual landing server) and the second part is the TTL (time to live) value of VDS server. Clicking the “IpList” button of Figure 10, a user (attacker) can whitelist the IP address of a server. The API is only accessible from the whitelisted servers.

TDS Server: TDS servers are provided by TDS vendors who buy and sell Web traffic. Attackers abuse TDS services and let the TDS redirect traffic to the proxy servers of the RIG 2.0 exploit kit to infect the victim with malware. In order to do so, the TDS needs to know the proxy server URL. As these proxy URLs are rotating and changing dynamically, so the TDS server uses the API link

to update the proxy URL. Thus, we think that an attacker lets the TDS knows his API link and whitelists the TDS IP on panel server in order to prevent API abuse.

Proxy Server: The proxy server handles all the traffic between the victim and the VDS server. In the proxy server, the file named "proxy.php" manages the PHPSSESID sent by a redirected victim and proxies traffic between the victim and the landing server (VDS server). The key for decrypting the PHPSSESID is setup in the "proxy.php" script. Thus, only the proxy server can see the VDS server's domain. We think that this is to hide the IP or domain of the VDS server from victim. The proxy server also handles the ping connection from the panel server.

VDS Server: The VDS server is actually the landing server, hidden behind a proxy server. Please note that the leaked kit does not include the contents of the VDS server. According to the cached data of the panel server we have, we guess that there is a PHP script named "core.php" on the VDS server, which is the actual landing page of RIG exploit kit. It may have functionalities to fingerprint the victim environment, exploit it according to fingerprinted information and send the victim's information to "download.php" on the panel server, which will store that data in the database. Actual exploit codes may also be contained in the VDS server.

Attack Infrastructure

We replicate the attack infrastructure of the RIG 2.0 exploit kit as in Figure 11.

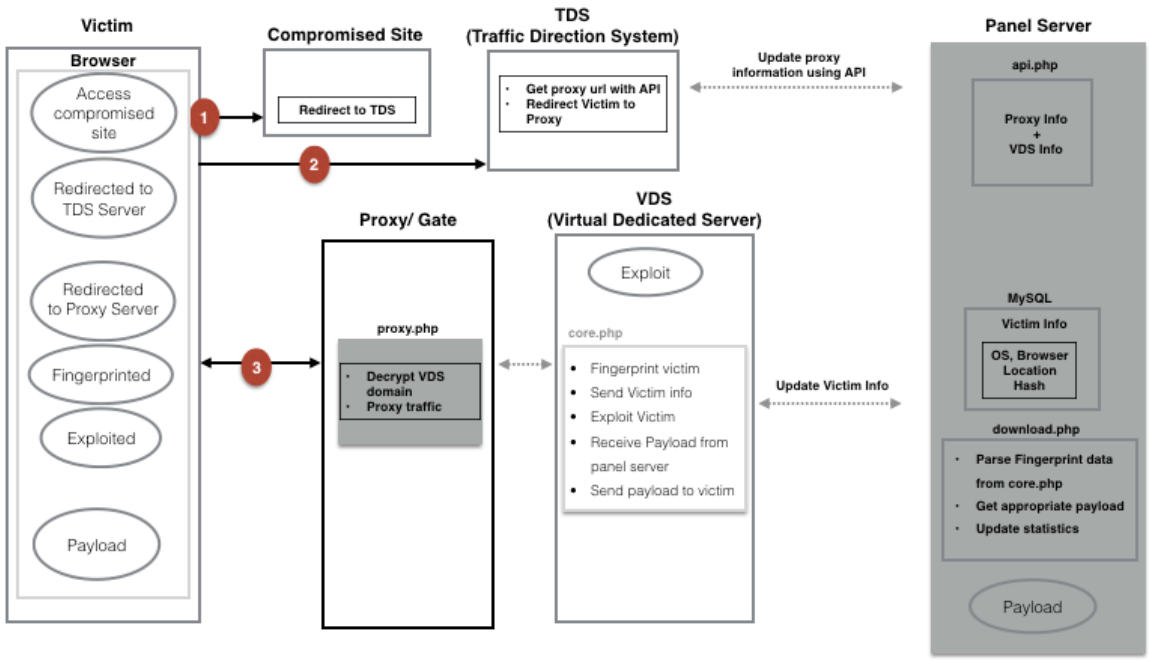


Figure 11 - RIG 2.0 Attack Infrastructure

Red colored numbers in the Figure 11 represents the traffic from the victim's browser and dotted lines show how servers behind the senses are working together to perform the drive-by download attack. Attack flow is as follows:

1. Firstly, the victim accesses to compromised site and is redirected to the TDS server.
2. The TDS server updates the proxy URL using the API. Namely, the TDS server connects to the panel server using the previously assigned API link and redirects the victim to the right proxy server. For example, the TDS connects to the panel server with the link, "http://panel_server_domain/api.php?apitoken=l3SKfPrFJx_ESYjDJunDTaNXPBbaHE3SzYuckOM". As a result, the TDS server receives a proxy URL containing a proxy domain and PHPSSESID. The received proxy URL looks like "http://proxydomain/proxy.php?PHPSSESID=**njrMNnjrMNruDMh7GCJzBKvPcT7tEMU7PSRnMmdLGyvrPVsbu**|ZDA0ZTUyNDA1OWMzN2EwZTEzMTM5ZWZiOGRmNjBhYTk". Using this proxy URL, the TDS redirects the victim to the right proxy server.
3. A PHP script named "proxy.php" on the proxy server decrypts PHPSSESID received from the victim. The first part of PHPSSESID (bolded in 2)) includes the domain of the VDS server and the second part is the TTL of the VDS server. The proxy server handles the connection between the victim and the VDS server where the landing page named "core.php" and exploit codes exit. The script named "core.php" fingerprints the victim's information, passes the data to "download.php" on the panel server, exploits the victim, receives an appropriate payload for the victim and transfers the encrypted payload to the victim via a proxy. The file named "download.php" in the panel server receives data from the "core.php" file, returns the RC4 encrypted payload and updates the statistics of exploited victims in the database of the panel server. Finally, the victim is infected with malware.

Database

The dumped database in the leaked kit contains more than 6,000 records. The name of the database is "baza3". We replicated it on a SQL DB. The analysis results of the DB are shown in Table 2.

Table 2 - Tables in Database

Table name	Table structure	Sample data	No: Rows
exploits	id, name, fault	-	-
files	id, user_id, file, filename, file size, avcheck	exe files	2
flows	id, user_id, file_id, last_token	39,127,2,1496975943	14
options	id, option_name, option_value	2, real_path, /var/www/html/hitfm	7

proxy	id, url, description, last_check	494, http://tree.changesomelives.com,,0	23
tarif	id, user_id, len	400,131,1514753999	62
traff	id, ip, os, br, cc, us, referer, exp, user_id, flow_id, hash	'20756','94.156.115.146','Windows 7','MSIE 11.0','BG','Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko','oxprxt.tk','flash','133','51','390cc1ddfbdf70c5ff79d5d63c565b1b'	6882
userrights	id, name, rights	1, admin, admin	2
users	id, user_login, user_pass, rights, color, first_time, last_time, description, sid	134, ferdigstudios, a3a5823e48cccf107cf1eba5f2cdaa2d, user, 0000FF, 1423277805,1496974143,,a1a6557378ea20856aac56fa4229113	8
vds	id, ip, description	1, http://94.23.207.221/core_hit.php, ,	1

The tables named “exploit” and “files” are empty. The tables named “flows, options, tarff, userrights” are used for the panel server application. Proxy server domains stored in the proxy table are shown in Table 3.

Table 3 - Proxy Domains

Proxy Server Domains	Status of Domain (June 2017)
auto.challenge-this.com	NXDomain
batton.changesomelives.com	46.182.30.163
blank.challenge-this.com	NXDomain
blog.challenge-this.com	NXDomain
change.changesomelives.com	46.182.30.163
filter.changesomelives.com	46.182.30.163
land.recondentalimplants.org	NXDomain
live.captionthephoto.com	NXDomain
log.challenge-this.com	NXDomain
music.captionthephoto.com	NXDomin
one.changesomelives.com	46.182.30.163
one.recondentalimplants.org	NXDomain
out.challenge-this.com	NXDomain
photo.captionthephoto.com	NXDomain
some.changesomelives.com	46.182.30.163
tank.captionthephoto.com	NXDomain
ticket.recondentalimplants.org	NXDomain
tree.changesomelives.com	46.182.30.163
trip.recondentalimplants.org	NXDomain
two.recondentalimplants.org	NXDomain
video.captionthephoto.com	NXDomain
was.captionthephoto.com	NXDomain

While almost all proxy domains are NXDOMAIN (Non-existent domain), others are still resolving to a single IP address, located in Russia, at the time of our analysis in June 2017. Only one record, “http://94.23.207.221/core_hit.php" is included in the VDS table. From the IP, the server is a dedicated server provided OVH dedicated server service from France. Victim information such as IP address, OS, country, browser, the referrer URLs and name of succeeded exploits are stored in the “traff” table. We notice a total of 6,009 victim IP addresses in the table. According to the data

in the “traff” table, a total of 75 countries are targeted; among them Italy, US, and Singapore have infected IP counts of 3849, 2118 and 131 respectively. Windows 7 and Windows 8.1 are the most targeted OS. In term of the browser, IE 11.0 and IE 8.0 are the top browsers out of all targeted browsers. Exploits named ie10 and flash are the most successful exploits out of all exploits. A summary of data in the “traff” table relating to exploits, OS, and browsers is shown in the following tables.

Table 4 - Referrer Domains

Referrer domain	Status of Domain (June 2017)
kouidri.com	217.23.6.139
hitrigenter.com	NXDomain
oxprxt.tk	NXDomain
www.attentive.pl	58.128.170.129
www.freesafeip.com	104.18.46.32, 104.18.47.32
-	104.25.229.53

Table 5 - Type of Exploits

Exploit	Count
unknown	5662
ie10	793
flash	263
msie	135
silver	21

Table 6 - Most Targeted Browsers

Browser	Count
MSIE 11.0	2988
MSIE 8.0	1198
Unknown	795
MSIE 9.0	766
MSIE 7.0	656
MSIE 10.0	430
MSIE 6.0	40
Firefox EB11	90
Firefox D7F5	20

Table 7 - Most Targeted OS

OS	Count
Windows 7	2729
Windows 8.1	1483

Unknown	891
Windows XP	857
Windows Vista	549
Windows 8	169
Windows Server 2003	93
Windows 2000	90
Windows 98	20
Mac OS	1

Self-protection features

In order to protect itself, the RIG exploit kit uses the following features;

- Use proxy servers in order to hide the VDS (landing) server.
- Proxy server domains are rotated to prevent easy takedowns and to confuse security researchers.
- Use an API to update proxy URLs in ral-time counteracting the easy tracking of proxy servers.
- Retrieve the AV warning count from Avdetect to kill detected proxy domains and renew them in real time.
- The VDS server has a TTL in order to prevent duplicate access from counterparties.
- The payload is encrypted to prevent analysis and being abused by rivals.
- API server access is limited whitelisted servers in order to prevent API abuse.

Weak Points

The RIG 2.0 exploit kit also has vulnerabilities that might lead to taking it down.

- The leaked kit has SQL Injection and reflected XSS Vulnerabilities.
- Proxy domains are rotated and a registered customer can collect as many proxy domains as possible by repeatedly using API. Please check Chapter 4 for detailed information.
- Directory listing is not prevented.

BEPS / Sundown Exploit Kit

The BEPS (Browser Exploit Packs) or Sundown exploit kit was the first exploit kit to abuse the CVE-2015-2444 vulnerability in the Internet Explorer in August 2015. Through several updates, BEPS became a significant threat responsible for a large number of infections in 2016. Its source code was leaked in February 2017 consisting of some payloads and source code for the panel server, proxy server, and rotator server although exploits are not included in the leaked kits. We downloaded the leaked kit from a hacking forum.

Servers in Attack Infrastructure

The attack infrastructure of the BEPS exploit kit is composed of a panel server, TDS server, proxy server and VDS server. Details on each server are explained in the following sections.

Panel Server (Admin Account): The admin account on panel server has four main functions 1) to check all exploit statistics for all registered users, 2) to control user registration, 3) to manage proxy domains and 4) to control IP addresses of the proxy server. It is a PHP based web application running on the Nginx web server. A screenshot of the login page to the panel server is depicted in Figure 12.

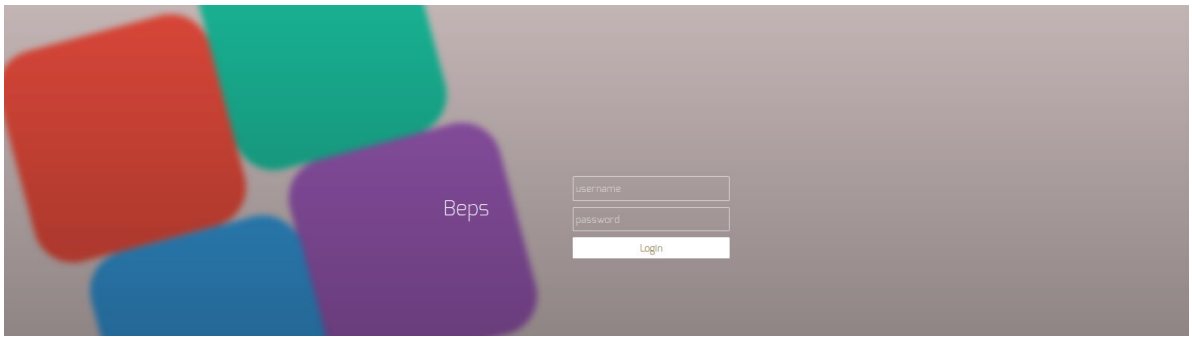


Figure 12 - BEPS login page

After login, the exploit statistic for all the registered users can be seen on a page named “Dashboard” as in Figure 13. Victim information such as countries, cities, browser and the name of the attacker using the BEPS exploit kit, and the referrer domains are shown on the dashboard page. In addition, server status such as CPU usage, RAM usage and disk usage can also be checked there.

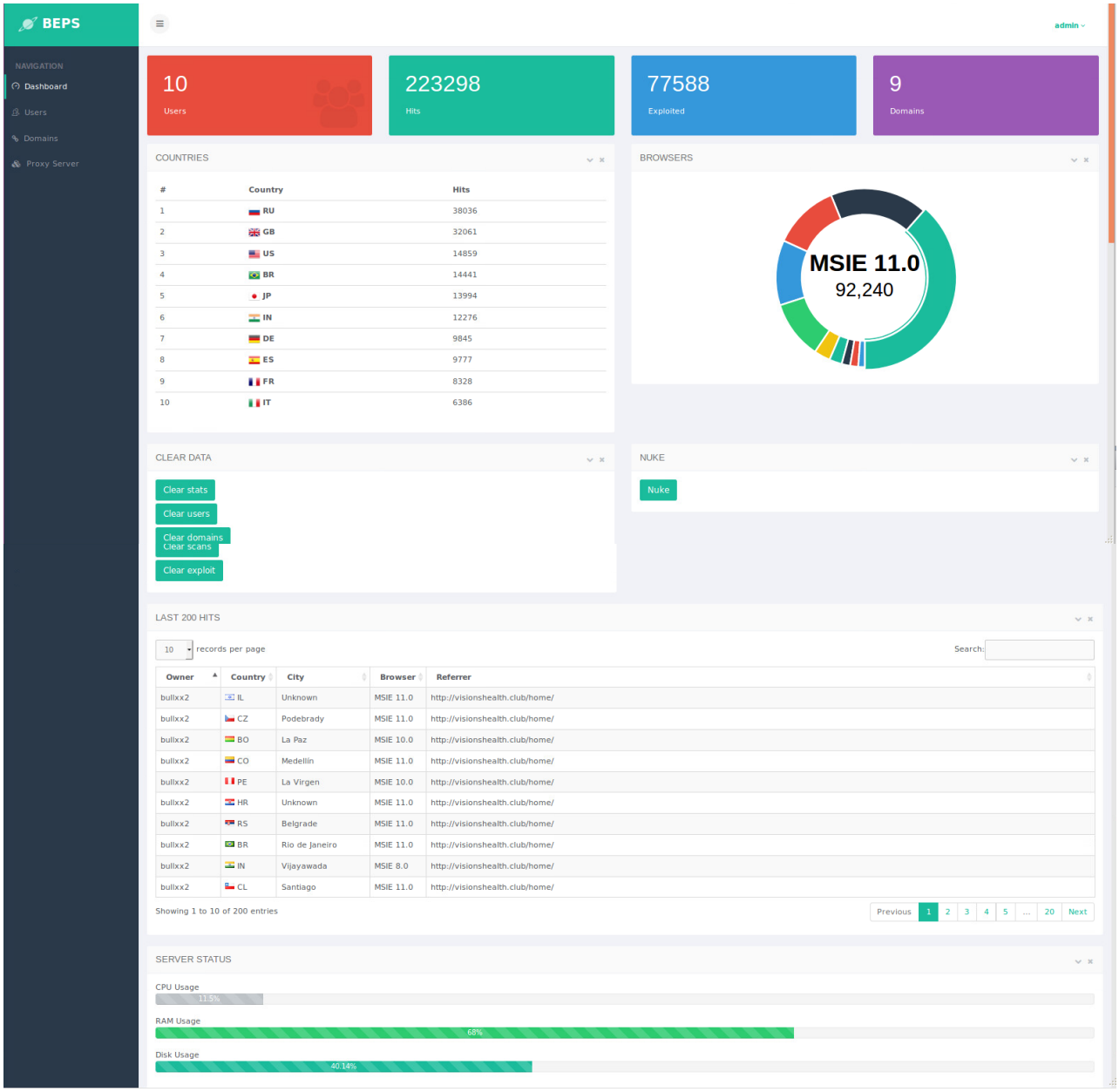


Figure 13 - Dashboard (Admin)

User control functions shown in Figure 14 consist of setting up user ids, passwords, expiration times, and tokens for login and uploading the compiled exploit kit for each user. Admin can upload zipped exploit kit files for the user. We guess that this might be for users who want to resell the BEPS exploit kit. User passwords are salted and encrypted before storing in the DB.

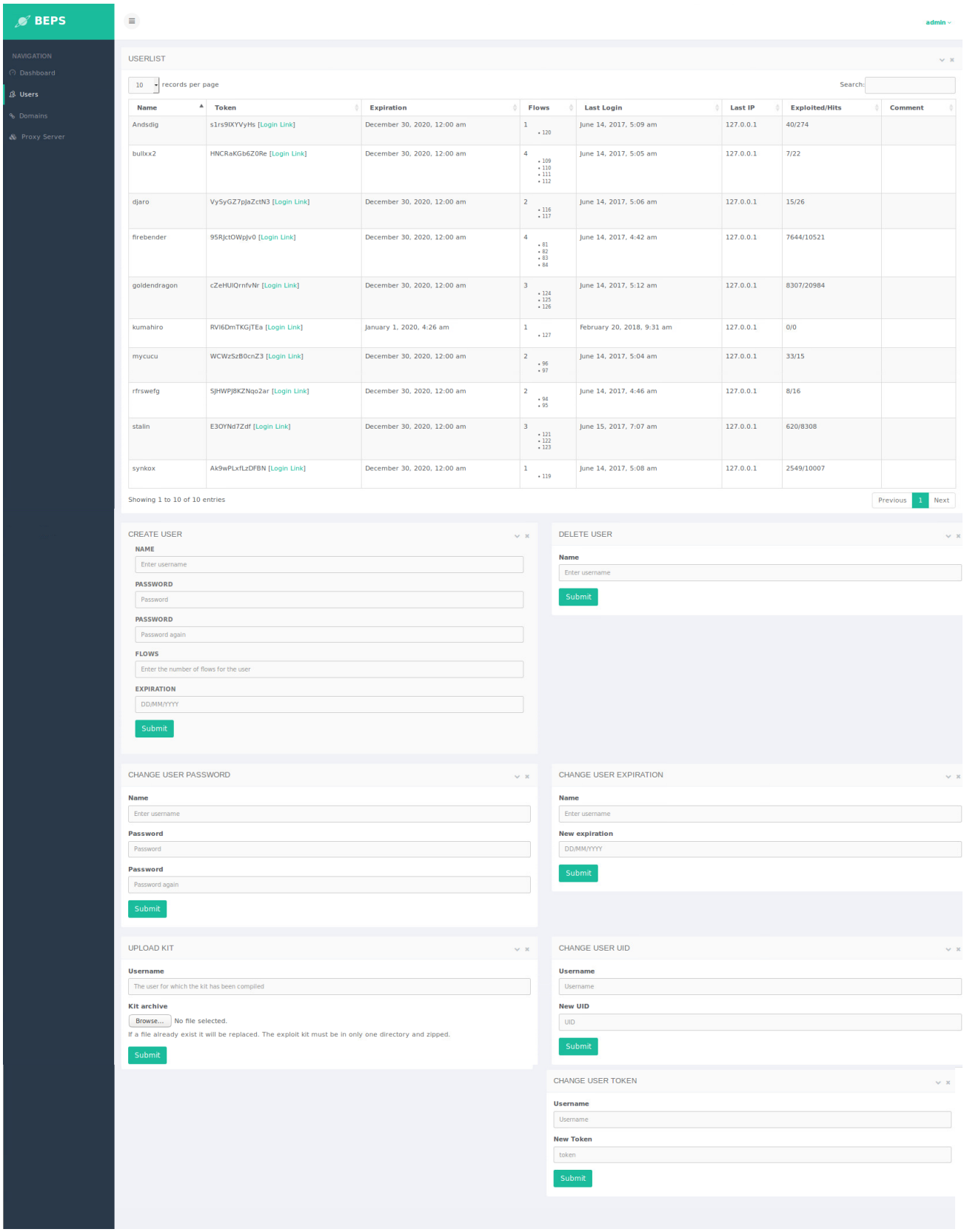


Figure 14 - User Control (Admin)

The proxy control page manages proxy domains as in Figure 15. Proxy domains have three levels including third level domains (hostname) and second level domains also called the master proxy domain. Admin can add proxy domains and master domains one by one or en-masses. Master proxy domains are registered using the “NameCheap” DNS hosting service. Authoritative DNS

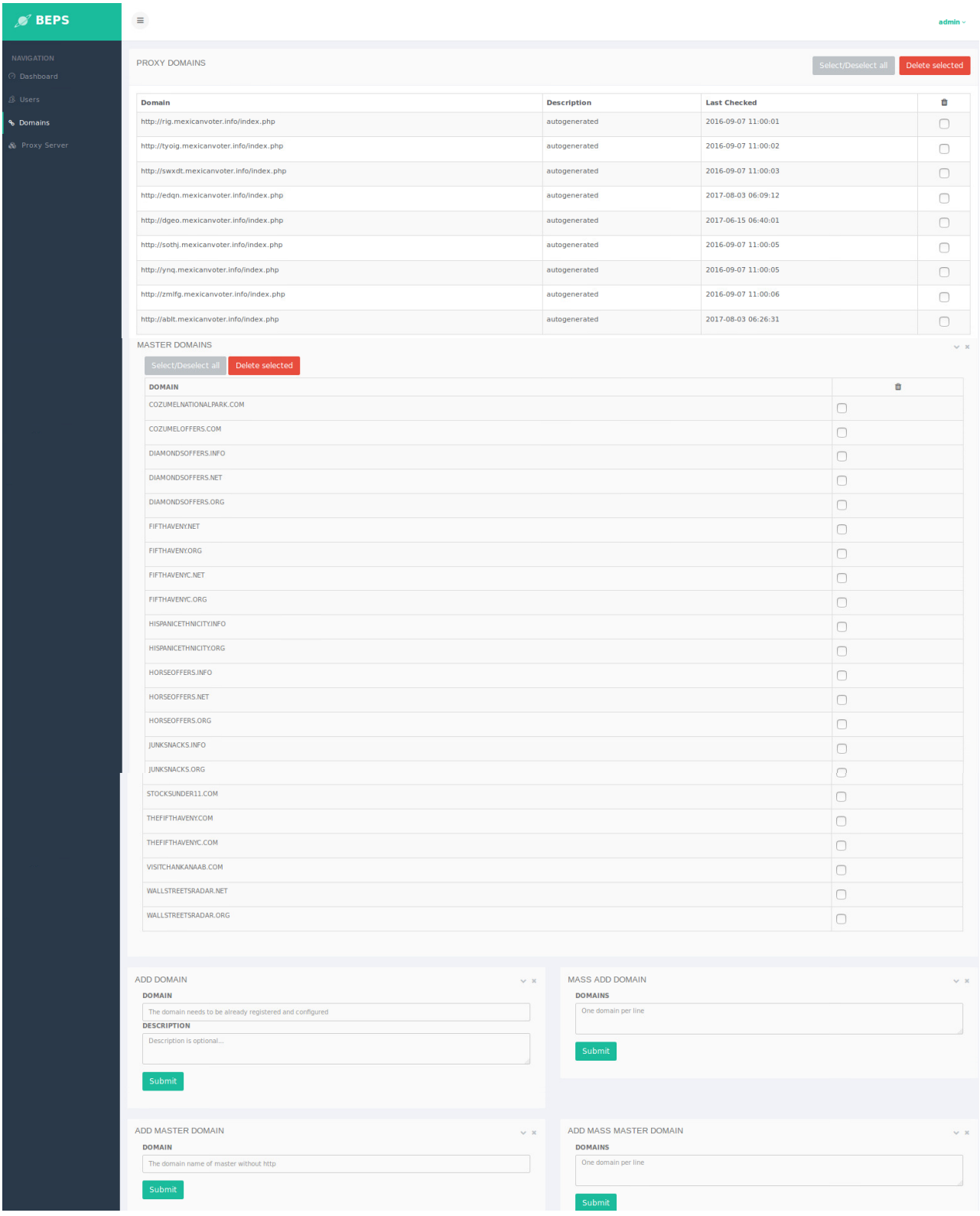


Figure 15 - Proxy Management (Domain)

servers to control third level domains (hostname) of proxy domains are managed by an operator of the BEPS exploit kit using the authoritative name servers, pns25.cloudns.net and pns26.cloudns.net. of clouDNS. We believe that domains are checked (potentially by a cron job) to see whether they are detected as malicious or not using the scan4you service. IP addresses for the proxy server are managed at a page named “Proxy Server” shown in Figure 16.

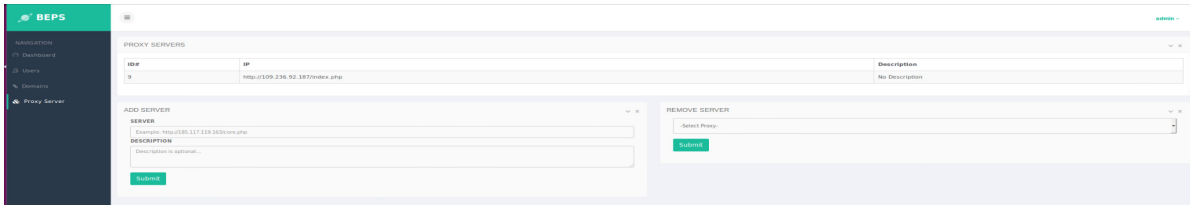


Figure 16 - Proxy Management (IP)

Panel Server (User Account): A registered user (attacker) to the BEPS exploit kit service can set up the payloads, get API links and check exploit statistics in their respective user control panel. On the dashboard, a user can check exploit statistics such as hits (accessed IP to proxy), exploited IPs, threads, exploit ratios, locations, browsers, OSs and referrers as depicted in Figure 17.

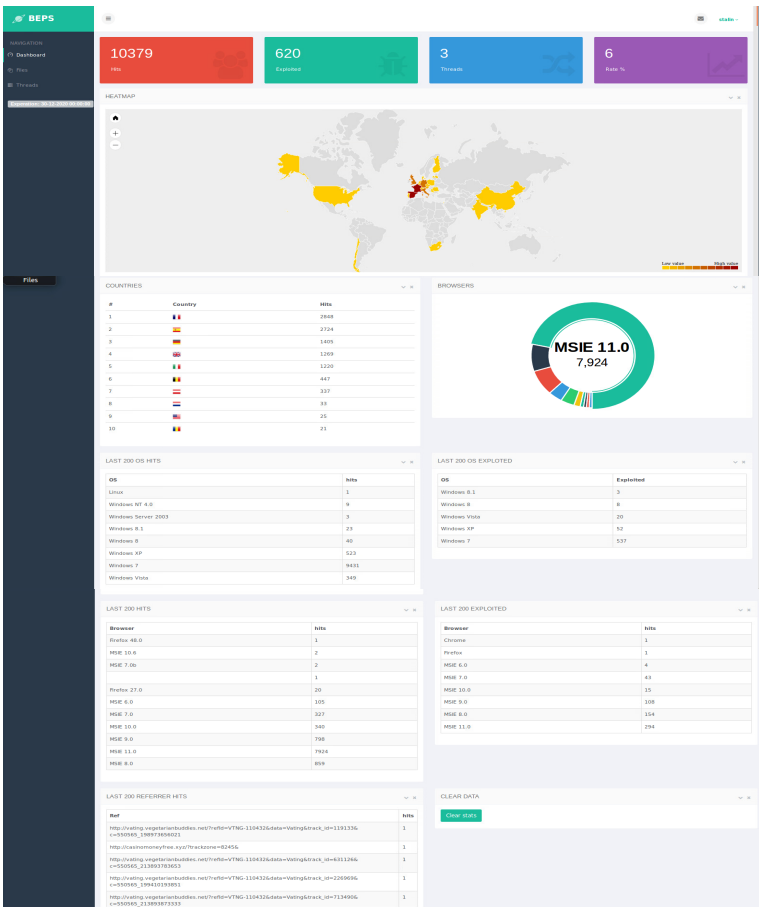


Figure 17 - Dashboard (User)

On the page named “Files” shown in Figure 18, a user can manage payloads such as uploading, scanning, and deleting files.

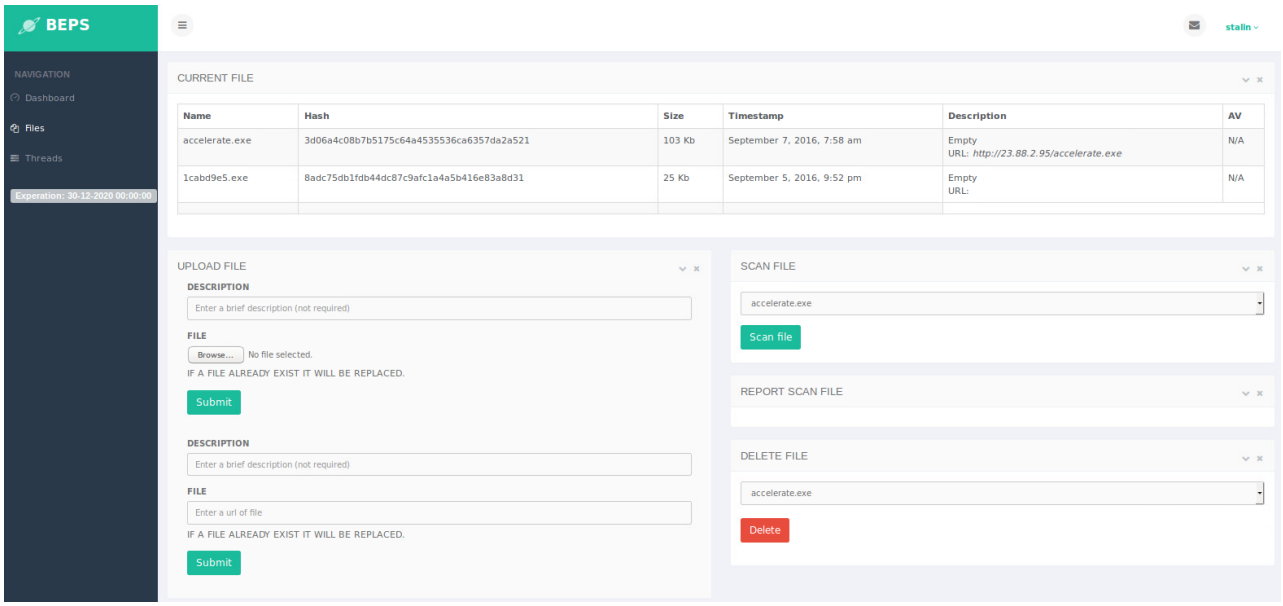


Figure 18 - Payload Management

On the page named “Threads” shown in Figure 19, a user can set up at most three payloads and generate “URL Rotator” link and “Public Stats” link for each payload by clicking the GetURL button. The first URL is an API link to receive the rotating proxy URLs and the second URL is to check exploit statistics without logging into the panel server. The sid value in the API link is an API token generated by encrypting the flow_id, user_id and proxy_host values of a user using RC4. We think that this API link is used by the TDS server as explained in following section.

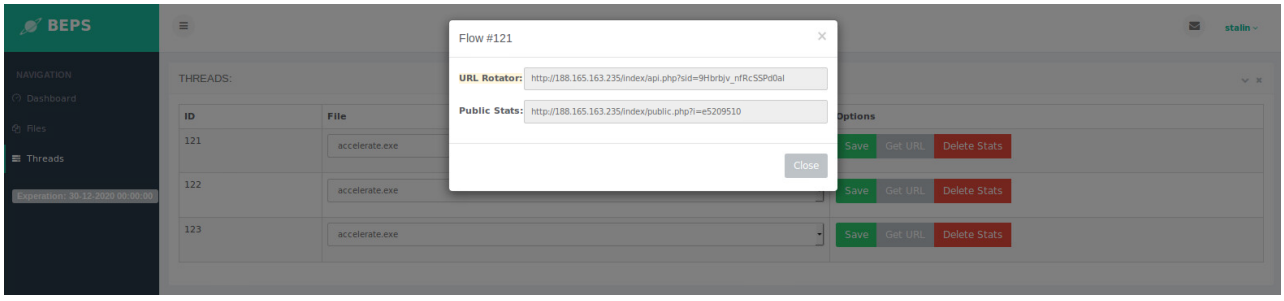


Figure 19 - API Link & Statistics Link

Table 8 shows the summary of exploit statics of all registered users using the BEPS exploit kit before it is leaked.

Table 8 - Actual Attackers and Exploit Ratios

No	User	Hits	Exploited	Threads (exploit type)	Rate of infection
1	admin	223298	77588	-	-
2	stalin	10379	620	3	6%
3	firebender	13066	7644	4	59%
4	rfrswefg	24	8	2	33%
5	mycucu	22	33	2	150%
6	bullxx2	24	7	4	29%
7	djaro	31	15	2	48%
8	synkox	12313	2549	1	21
9	Andsdig	343	40	1	12
10	goldendragon	28294	8307	3	29%

TDS Server: The TDS is server is provided by TDS vendors who buy and sell Web traffic. Attackers abuse TDS services and let TDS redirect traffic to the proxy server of the BEPS exploit kit to infect the victim with malware. In order to do so, TDS needs to know proxy server URL. Since, these proxy URLs are rotating and changing dynamically, TDS server uses an API to update the proxy URL. Please note that the existence of a TDS server is our assumption and there might also be other ways to redirect a victim to the proxy server.

Proxy Server: The “index.php” script on the proxy server fingerprints a visiting victim’s information such as OS, browser, location and updates this information in the “hits” table of the panel server. It then calls the “landing_$flowid.php” script which seems to be the actual script to exploit the victim. Please note that this landing_$flowid.php script is not included in the leaked kit we collected. In any case, we guess that “landing_$flowid.php” exploits the victim together with other exploit scripts existing on the VDS server whose exploit codes are not leaked as well.

On proxy server, another file named “z.php” serves an appropriate payload, fingerprints of exploited victims, and updates a victim’s information in the “hits” table in the panel server. In addition, the proxy server protects itself from being detected by crawlers and the security community by setting blacklisted http-user-agent and browsers as in Figure 20.

Figure 20 - Self Protection

VDS Server: We think that the VDS server might contain actual exploit codes whose functions are called by “landing_$flowid.php” on the proxy server. As the leaked kit does not include these exploit codes, we do not know details on how these codes are functioning together with “landing_$flowid.php” to exploit the victim. We think that as exploit codes are the main components of an exploit kit, exploit kit operators protects VDS server behind proxy servers very well.

Attack Infrastructure

We replicate the attack infrastructure of the BEPS exploit kit in our lab environment as in Figure 21.

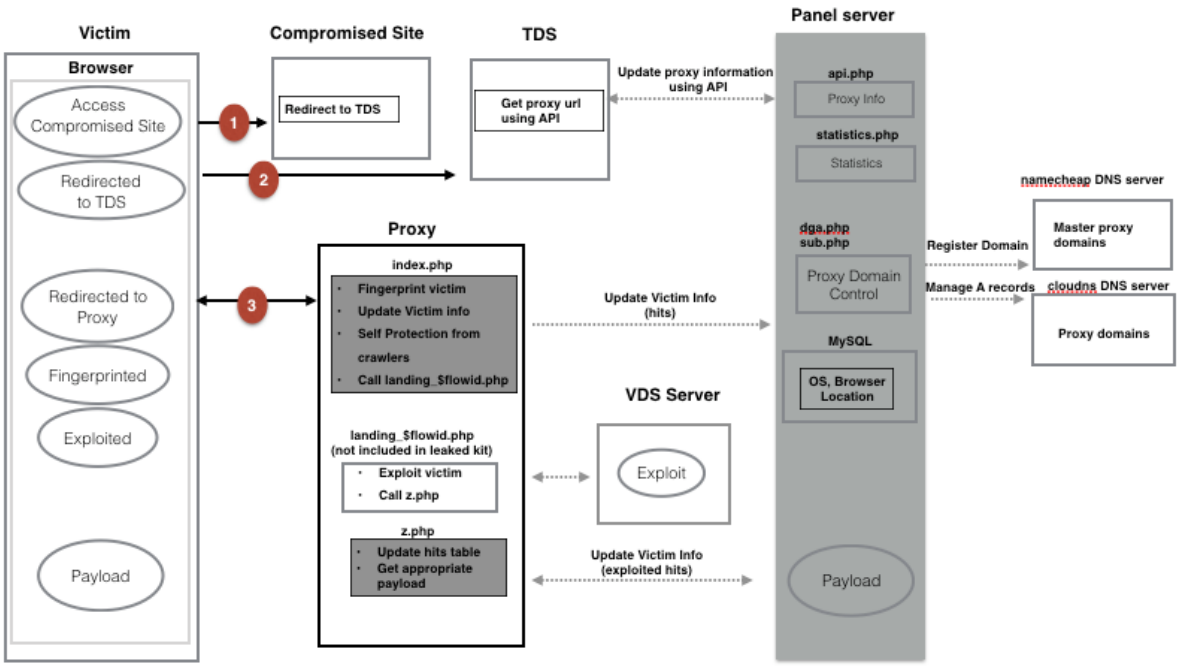


Figure 21 - BEPS Attack Infrastructure

Red colored numbers in Figure 21 represent the traffic from a victim's browser and dotted lines show how servers behind the senses are working together to perform the drive-by download attack. Attack flow is as follows:

1. Firstly, a victim access to the compromised site and is redirected to TDS server.
2. The TDS server updates the proxy URL using the API and redirects the victim to the proxy server. Namely, TDS updates the proxy information using an API link such as "http://panelserver_IP/api.php?sid=9Hbrbjv_nfRcSSPd0al". As result, TDS receives proxy sever URL such as "http://ablt.mexicanvoter.info/index.php?zX3kA02R2cBabnur=tie3YDn12KddRG32N1kce8FmnhMZmrxBhrlf6mlQwcgmmksnik7V3FDJB". Using this link, TDS redirects the victim to the proxy server.
3. The proxy server fingerprints the victim's OS, browser, location and referrer URL, updates this information in the panel server and exploits the victim. We think that "index.php" and "landing_$flowid.php" work together with actual exploit codes on the VDS server in order to exploit the victim. After the victim is successfully exploited, "z.php" on the proxy server fingerprints the exploited victim, updates the "hits" table on the panel server and provides the appropriate payload to the victim. Finally, victim is infected with malware.

Database

The dumped database in the leaked kit contains more than **400,000** records. The name of the database is "panels". We replicate it on a SQL DB. The analysis results of tables in the DB are shown in Table 9.

Table 9 - Tables in Database

Table Name	Table Structure	Sample Data	Rows
domains	id, name	622, wallstreetsradar.org	30
file_scans	id, file, owner, name, hash, rate, result	217,750,59,accelerate.exe,ba3f78935efde883e1c07a890fb71adf5a3ab9a3, 1/35, AVDFree:OK Avast:OK	218
files	id, owner, name, file, hash, description, timestamp, url	676, 60, tihjyuu.exe, exe_file, fa35b9cf029d867ee509a3891a1ce643e38ea22,' ', 1473195774, NULL	24
flows	id, user_id, file_id, last_token	126, 60, 738, 1473246262	126

hits	id, owner, flow, ip, agent, referrer, country, city, browser, exploited, timestamp, os	889961,22,44,'221.40.158.156','Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) likeGecko','http://nikefukuoka.jp/m/banner.php','JP','Unknown','MSIE11.0',0,1465996320,'Windows 8.1'	404,905
proxy	id, url, description, last_check	10880, http://rig.mexicanvoter.info/index.php, autogenerated, 1473246001	9
tokens	token, flow_id, timestamp	5stcclXg49RSo, 126, 1473246262	103
users	id, name, pwd, registered, last_login, last_ip, expiration, uid, comment, token	40, firebender, $2y$10$dJ6IkN4JMxzqX87SNxQ0oe4rnBCzufIjDV1TZFLpYesd8QZkxPrQm, 1469572046, 1473225147, 185.93.185.229, 1473552000, 1a80cc68, ,95RJctOWpJv0	9
vds	id, ip, description	9, http://109.236.92.187/index.php	1

Master domains and proxy domains in the domains table and proxy tables are shown in Table 10 and Table 11. At the time of our analysis in June 2017, all these domains are NXDomains (Non-Existent Domain).

Table 10 - Proxy Domains

No	Domains	Status
1	'http://rig.mexicanvoter.info/index.php'	NXDomain
2	'http://tyoig.mexicanvoter.info/index.php'	NXDomain
3	'http://swxdt.mexicanvoter.info/index.php'	NXDomain
4	'http://edqn.mexicanvoter.info/index.php'	NXDomain
5	'http://dgeo.mexicanvoter.info/index.php'	NXDomain
6	'http://sothj.mexicanvoter.info/index.php'	NXDomain
7	'http://ynq.mexicanvoter.info/index.php'	NXDomain
8	'http://zmlfg.mexicanvoter.info/index.php'	NXDomain
9	'http://ablt.mexicanvoter.info/index.php'	NXDomain

Table 11 - Master Proxy Domains

No	Domains	Status
1	'cozumeloffers.com'	NXDomain

2	'diamondsoffers.info'	NXDomain
3	'diamondsoffers.net'	NXDomain
4	'diamondsoffers.org'	NXDomain
5	'fifthaveny.net'	NXDomain
6	'fifthaveny.org'	NXDomain
7	'fifthavenyc.net'	NXDomain
8	'fifthavenyc.org'	NXDomain
9	'hispanicethnicity.info'	NXDomain
10	'hispanicethnicity.org'	NXDomain
11	'horseoffers.info'	NXDomain
12	'horseoffers.net'	NXDomain
13	'horseoffers.org'	NXDomain
14	'junksnacks.info'	NXDomain
15	'junksnacks.org'	NXDomain
16	'latinoethnicity.info'	NXDomain
17	'latinoethnicity.org'	NXDomain
18	'mexicantequilas.info'	NXDomain
19	'mexicantequilas.org'	NXDomain
20	'mexicanvote.info'	NXDomain
21	'mexicanvoter.info'	NXDomain
22	'retail-price.net'	NXDomain
23	'saintthomasoffers.com'	NXDomain
24	'stocksunder11.com'	NXDomain
25	'thefifthaveny.com'	NXDomain
26	'thefifthavenyc.com'	NXDomain
27	'visitchankanaab.com'	NXDomain
28	'wallstreetsradar.net'	NXDomain
29	'wallstreetsradar.org'	NXDomain

A table named “hits” contains more than 400,000 records of fingerprinted victim information and referrer URLs. The total victim IP count is 224,727 and the total count of referral URLs is 51,826. There are 1,390 unique domains if domains of referral URLs are counted. The analysis of fingerprinted victim information such as OS, browser, locations, and type of exploits of hits table is shown in the following Tables.

Table 12 - Top Targeted Countries More than 5000 Victims

No	Country	Count
1	RU (Russia)	38145
2	GB (United Kingdom)	32083
3	US (United States)	15316

4	BR (Brazil)	14485
5	JP (Japan)	14039
6	IN (India)	12298
7	DE (Germany)	10093
8	ES (Spain)	9778
9	FR (France)	8357
10	IT (Italy)	6389
11	VN (Vietnam)	5290

Table 13 - Top Targeted Browsers

No	Browser	Count
1	MSIE 11.0	92,425
2	MSIE 8.0	42,115
3	MSIE 7.0	28,195
4	MSIE 10.0	27,125
5	MSIE 9.0	24,215
6	Chrome 50.0.2661.102	5,440
7	MSIE 6.0	4,177
8	Firefox 46.0	1,966
9	Chrome 46.0.2486.0	1,790
10	Chrome 49.0.2623.112	1,071

Table 14 - Top Targeted OS

No	OS	Count
1	Windows 7	136,059
2	Windows 8	22,935
3	Windows XP	22,155
4	Windows 8.1	20,443
5	Windows 10	16,862
6	Windows Vista	9,703
7	Unknown	2,628
8	Mac OS	1,591
9	Linux	1,442

Self- Protection Features

In order to protect itself, the BEPs exploit kit uses the following features;

- Proxy server domains are rotated to prevent easy takedown and to confuse security researchers.

- Proxy domains are DGA domains and registered automatically using the Namecheap API. This allows the exploit kit to register new proxy domains in real time if current proxy domains are detected.
- Use of proxy servers in order to hide the VDS (landing) server
- Use of API to update proxy URLs preventing easy tracking of proxy servers
- Payload is encrypted to prevent analysis and being abuse by rivals
- Use of scan4you service to prevent detection on proxy domains
- Check detection ratio of payload (executable files) using scan4you so that payload can be updated
- DNS A records of proxy domains are managed by separate clouDNS servers so that operator can handle host names of proxy domains efficiently.
- Block search engine bots and crawlers from the security community using http-user agent block list.

Weak Points

- TDS servers are not whitelisted and so anyone with access to API information can abuse the API link.
- Proxy domains are rotated and a registered customer can collect as many proxy domains as possible by using API several times. Please look at Chapter 4 for detailed information.
- Directory listing is not prevented.

Hunter Exploit Kit

Hunter exploit kit was first seen in 2015 and its source code was leaked in 2016. Drive-by download attack performed by the Hunter exploit kit mainly targeted banking customers in Brazil. According to the Ranger Exploit group selling hunter kit, the price is $2500 for a lifetime package as shown in Figure 22.

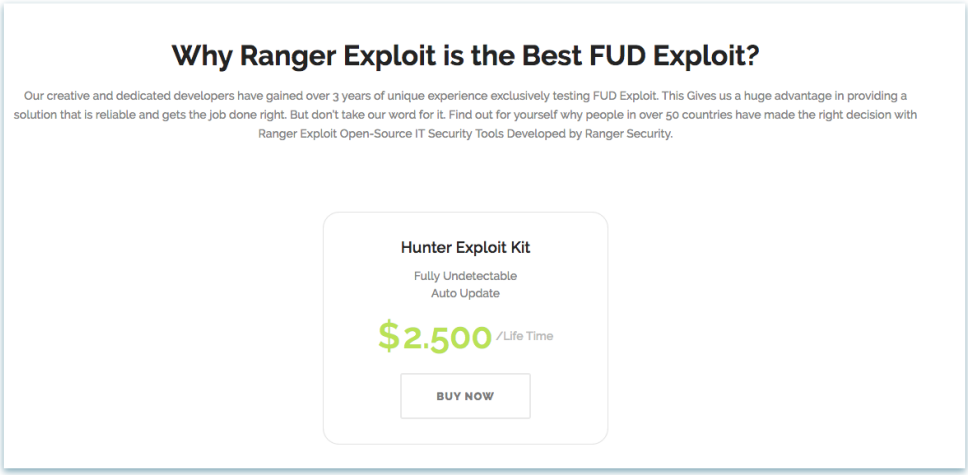


Figure 22 - Sale Page

A group of popular hackers named “peace of mind” have hacked their rival website w0rm.ws.an, a website where hackers can discuss topics and sell knowledge or tools, in October 2016. In addition, “peace of mind” dumped the site’s entire database and leaked online. The leaked data consists of the entire website’s data including files, databases, exploit kits, user data including accounts, passwords, history, PMs, forum posts and other sensitive data. The hunter exploit kit is included in this leaked dataset. We have downloaded it from Crack Pro. The leaked code is Hunter version 1.0.1 and it includes database files, a PHP based web application for controlling panel servers and update server.

Servers in the Attack Infrastructure

The attack infrastructure of the Hunter exploit kit consists of a panel server and update server. The panel server seems to be set up by an attacker. Updates for the web application running on the panel server can be downloaded from the update server.

Panel Server: The panel sever is a PHP based web application running on Apache. It is mainly used to manage the exploitation task, generate landing page URLs and check statistics of the

victim. The login page of the Panel server is shown in Figure 23. After login, a user can check statistics and insider news on the Dashboard page as shown in Figure 24.

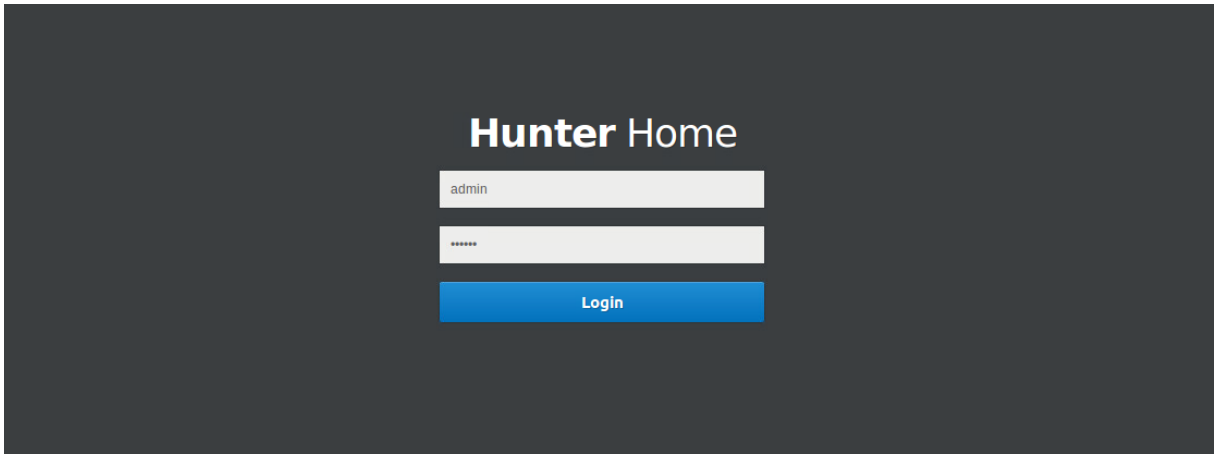


Figure 23 - Hunter Login Page

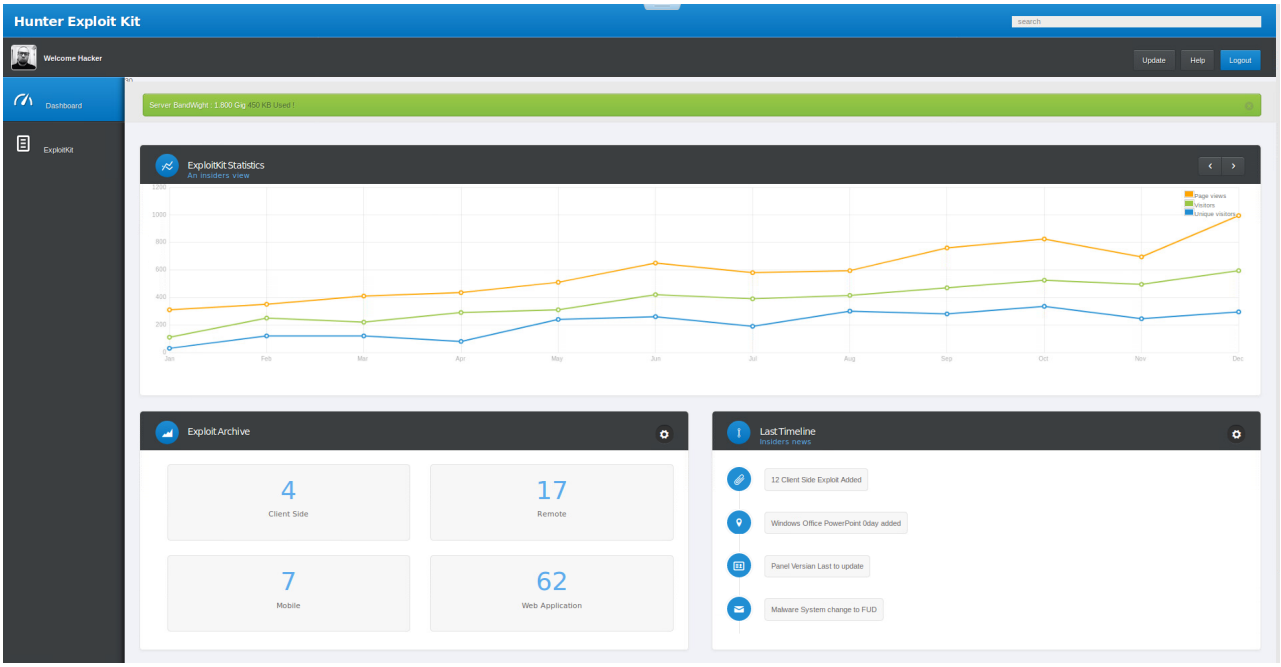


Figure 24 - Dashboard

On the page named Exploit Kit, a user can check current tasks and using the column named Options shown in Figure 25, a user can generate a statistical report relating to the current task, get URLs to the landing page and manage tasks such as start, stop and delete. Here, “task” means a set of chosen exploits and payloads chosen by a user.

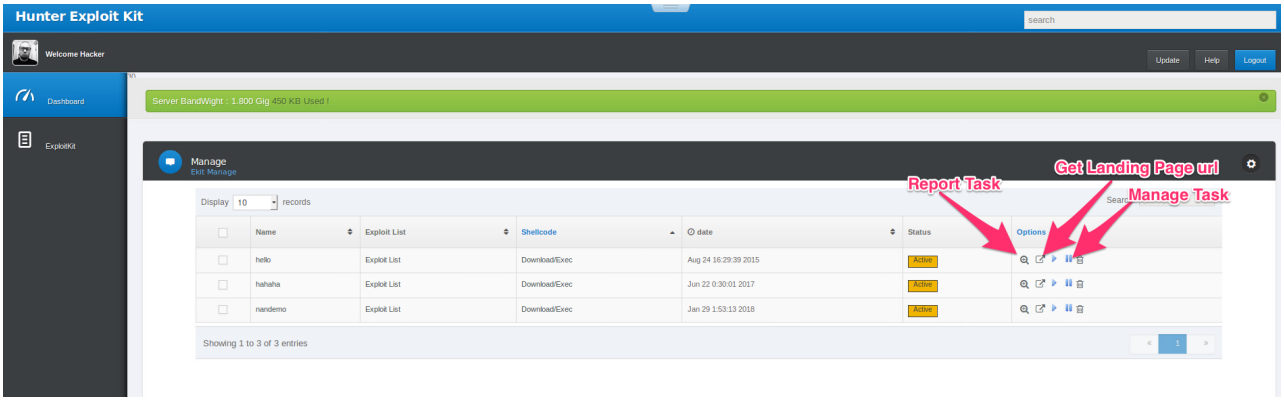


Figure 25 - Manage Exploits

Screenshots of the statistical report relating to the current task and landing page URL are shown in Figure 26 and Figure 27.

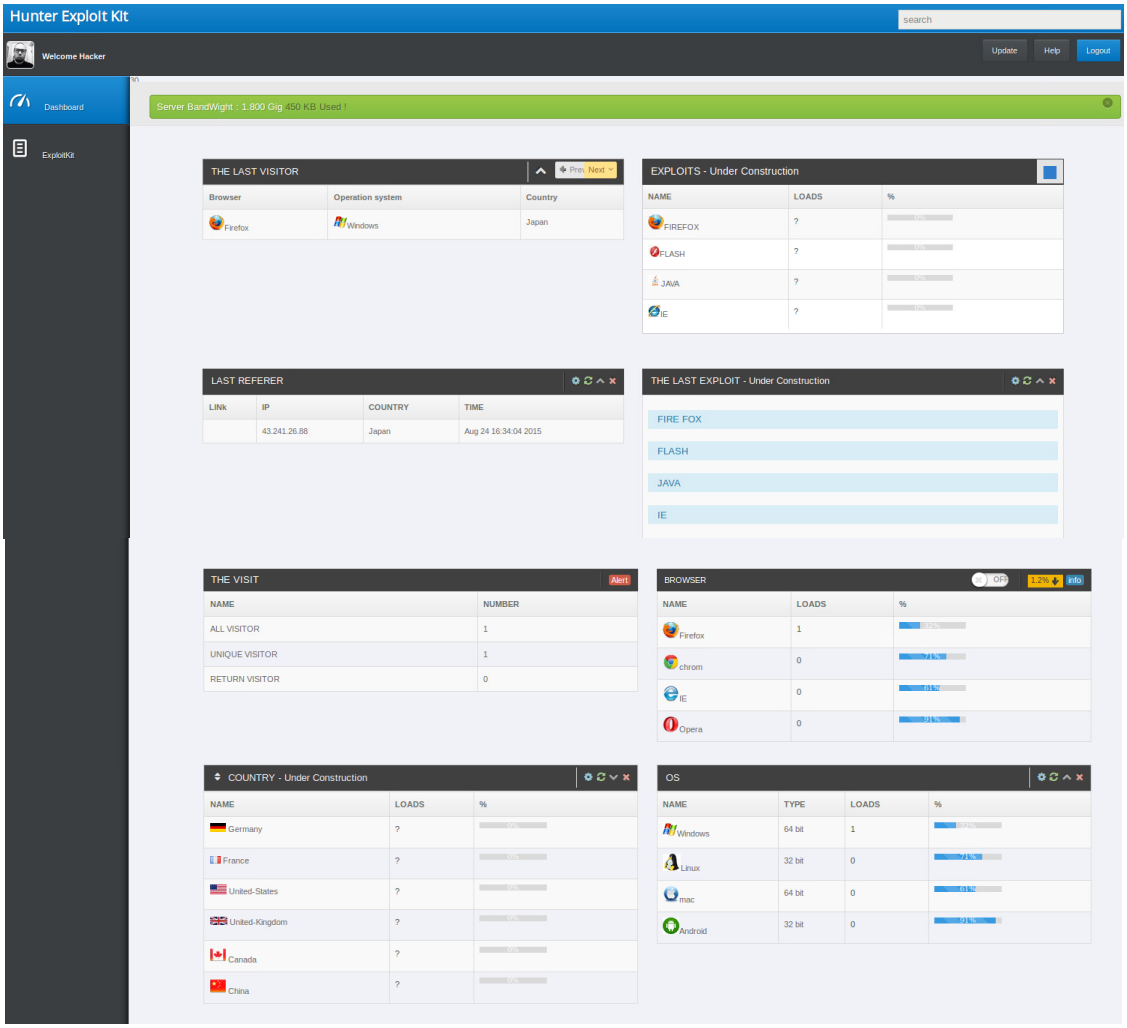


Figure 26 - Example of Report

Figure 27 - Landing Page URLs

In Figure 27, two different types of landing page URLs are generated. The first two URLs are basically the same, one with an iframe tag and the other without it. The same applies for the second two URLs. The first two URLs (first and second URL from above) are for fingerprinting victim information and exploiting a victim whatever the victim environment may be. The second two URLs (third and forth from above) will not exploit victim, rather, it will let the victim download a fake adobe flash player application.

A user can generate new tasks by choosing exploits and payloads as in Figure 28. In contrast with other exploit kits, for each task, a user can customize exploits out of all available exploits. At any given time, only three tasks can be generated. Two landing pages will be generated for each task and the attacker redirects the victim to these landing pages so that the victim can be exploited and infected. The first landing page will do carpet bomb exploitation and the other one will exploit according to the victim's environment.

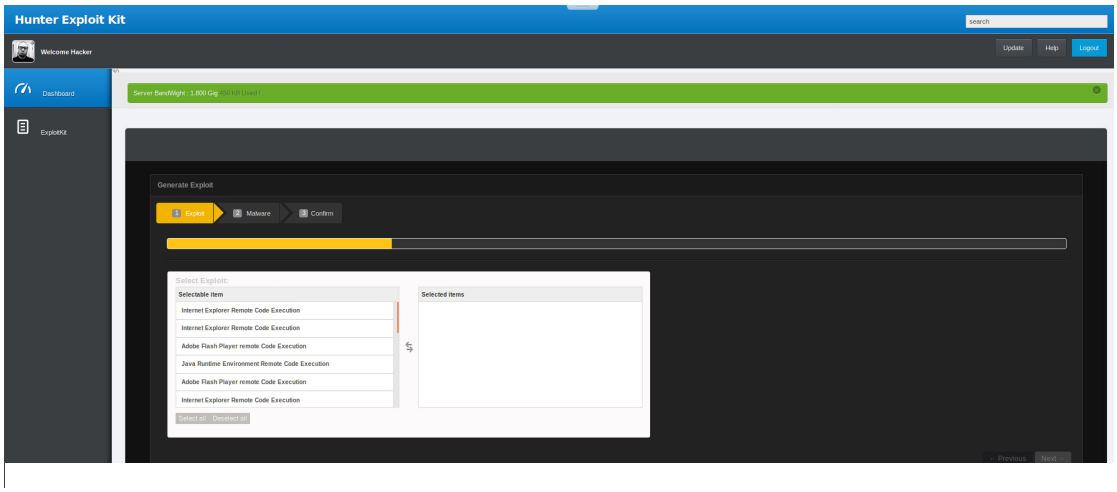


Figure 28 - Manage Exploits

Attack Infrastructure

We replicated the attack infrastructure of the Hunter exploit kit as in Figure 29.

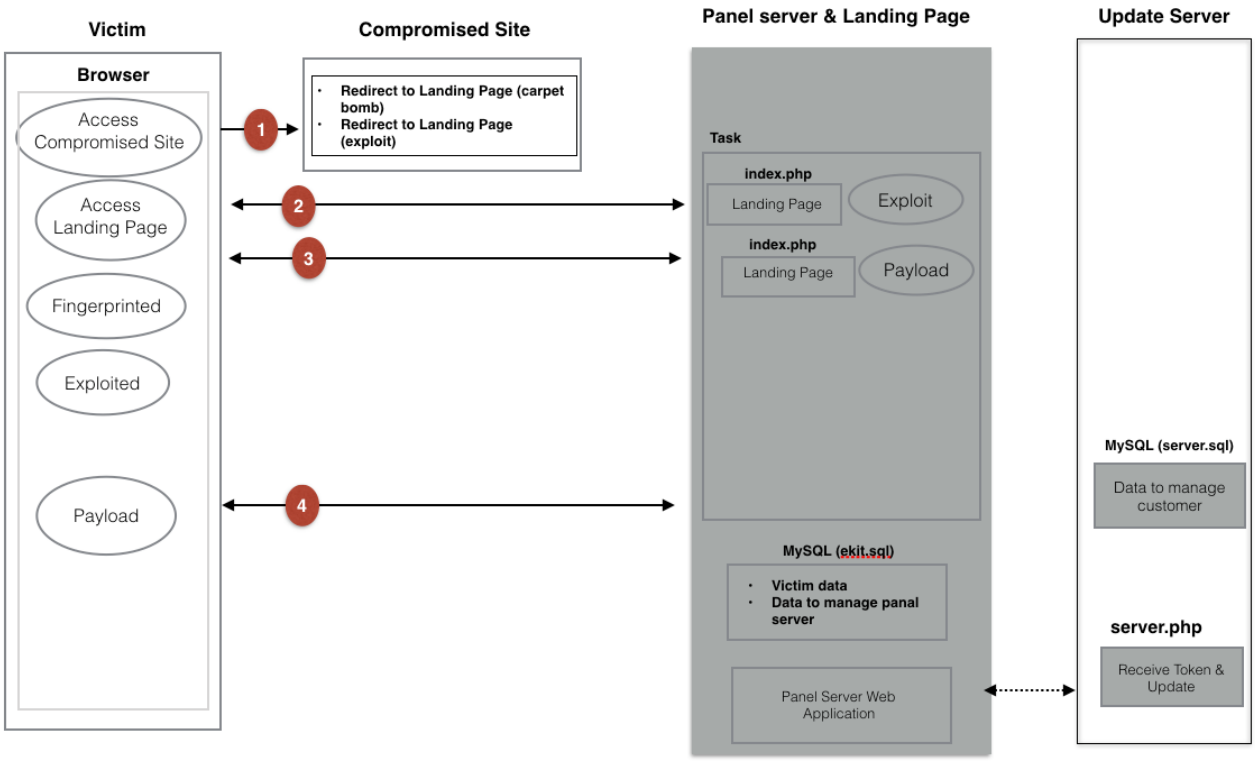


Figure 29 - Hunter Attack Infrastructure

Red colored numbers in the Figure 29 represent the traffic from a victim's browser and dotted lines show how servers behind the senses are working together. Attack flow is as follows:

1. Firstly, a victim accesses the compromised site and is redirected to two landing pages.
2. When a victim accesses the first landing page, the victim's information such as IP, country, browser, OS, and referrer will be recorded. All exploits will be tried regardless of what the victim's environment is. In the jargon, such exploit behavior is called a carpet bomb.
3. When a victim accesses the second landing page, a fake adobe flash player will be downloaded without exploiting the victim. When this file is executed by the victim manually, it will be infected with malware.
4. If the exploit in step 3 succeeds, malware will be downloaded for infection.

Database

The dumped database does not include much data. The name of the database is "kit" and the summary of tables in the database is described in Table 15.

Table 15 - Tables in Database

Table Name	Table Structure	Sample Data	No: Rows
clientside_task	id, taskname, sploitlist, shellcodetype, data, status, taskurl, agenturl, zipass	57,11, Adobe Acrobat Reader Remote Code Execution (6-7-8-9), Download/Exec, May 11 15:07:59 2015, Active, http://81.17.25.3/666f726d20656e6374970653d226d756c746970617274/d07d50a751bc6ddf12bf3af0efee9b45/11/6512bd43d9caa6e02c990b0a82652dca.zip, , 111	1
ekit_clientside	id, sploitname, sploitcode	1,Microsoft Office word Remote Code Execution (2003-1007-2010-2013), e20141876	4
ekit_manage	id, sploitname, dateadd, stable, detail, pbypass, icon	20, Adobe Flash Player remote Code Execution, 2015-08-12, Good, CVE-2015-3090	20
ekit_multiple	id, sploitname, sploitcode	1, Internet Explorer Remote Code Execution, 045423c0415da1d4293522d9ec3a19a7	17
ekit_task	id, taskname, sploitlist, shellcodetype, date, status, taskurl, triggerurl, agenturl, domain, dns1, dns2	201, hello, Mozilla Firefox Remote Code Execution, Downlod/Exec, Aug 24 16:29:39 2015, Active , http://81.17.25.3/666f726d20656e6374970653d226d756c746970617274/task/hello/index.php, http://81.17.25.3/666f726d20656e6374970653d226d756c746970617274/task/hello/c7d08e09a44d2b453e7eeecebf0a8daf/index.php, 81.17.25.3/666f726d20656e63747970653d226d756c746970617274/5128f35c9b4be13788ba41bdb6d1fc1f/5138840586.exe	1
ekit_taks_hello	id, ip, country, browser, os, ostype, referer date	1, 43.241.26.88, Japan, Firefox, Windows XP, 64bit, , Aug 24 16:34:04 2015	1
users	username, password	admin, hash of “hunter”	1

Exploits

There are 14 different types of exploits in the leaked kits. In addition, one fake flash downloader which will be downloaded to the victim whether the exploit succeeded or not is included. The target application and respective CVEs of the exploits are depicted in Table 16.

Table 16 - Exploits

No	Target Application	CVE
1	IE	CVE-2014-6332
2	Flash	CVE-2015-3043
3	Java	CVE-2013-2470
4	Firefox	CVE-2013-1710
5	Firefox	CVE-2014-8636
6	Flash	CVE-2015-5119
7	Flash	CVE-2015-5122
8	IE	CVE-2015-2419
9	Firefox	CVE-2014-1510
10	Flash	CVE-2015-0311
11	-	Unknown CVE
12	-	Unknown CVE
13	-	Unknown CVE
14	-	Unknown CVE
15	Fake Flash downloader	-

Self-protection features

In order to protect itself, directory listing is prevented by the Hunter exploit kit.

Weak Points

- The landing page and panel server seem to be on the same server and thus it is easy to detect them.
- No other functions for self-protection are seen.
- There is a special character called “task” in every iframe generate by the Hunter exploit kit. This might lead to detecting landing page easily.

Neptune (Eris, Blaze, Terror) Exploit Kit

The Neptune exploit kit was first seen in 2016. It was used for drive-by download attacks. In August 2017, the Neptune exploit kit is used for dropping a Monero miner. It is sold as an exploit kit package.

We downloaded Neptune Exploit Kit from VirusTotal. It seems that the leaked kit we downloaded is what the original owner of the Neptune exploit kit (terror) mentions in hacker forums (in October 2016) as shown in Figure 30. The leaked data consists of the web application for the panel server, the database, the source for the uploader server and exploits. The price ranges from $ 750 to $ 4000 according to advertisement about Neptune exploit kit shown in Figure 31.

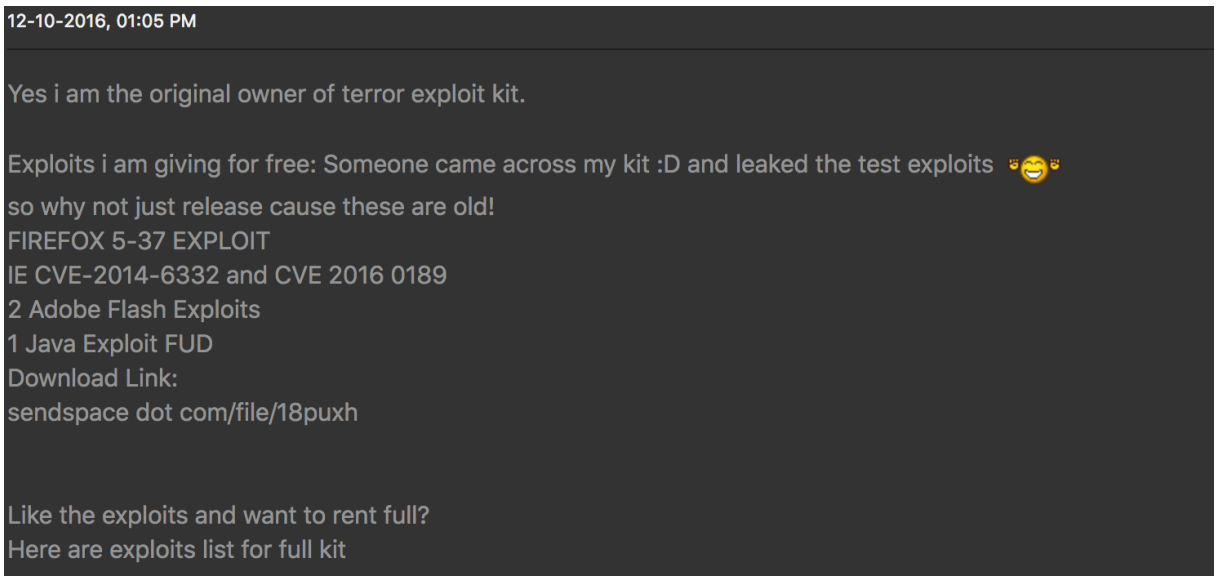


Figure 30 - Post in Hacker Forum

Figure 31 - Neptune Advertisement

Servers in the Attack Infrastructure

The attack infrastructure of the Neptune exploit kit consists of a panel server, an uploader server and a landing server. The panel server is the main server controlling the web application interface for the exploit kit users and the payloads used. The uploader server downloads payload from the panel server, creates the landing page and uploads it to the landing server. The landing server serves the landing page, fingerprints the victim and updates the "hits" table in the database of the uploader server.

Panel Server: The panel sever is a PHP based web application running on Apache. It has functions to manage payloads, generate landing page URLs and check the statistics of the victims.
The login page to Panel server is shown in Figure 32. After login, a user can check statistics on how many victims are exploited with what kind of exploits, hits (visit landing page but not exploited) and license time left as in Figure 33.

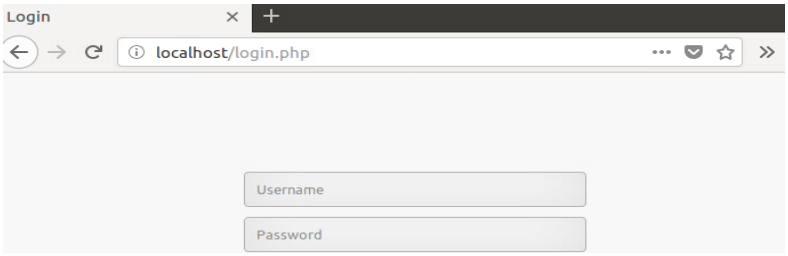


Figure 32 - Neptune Login Page

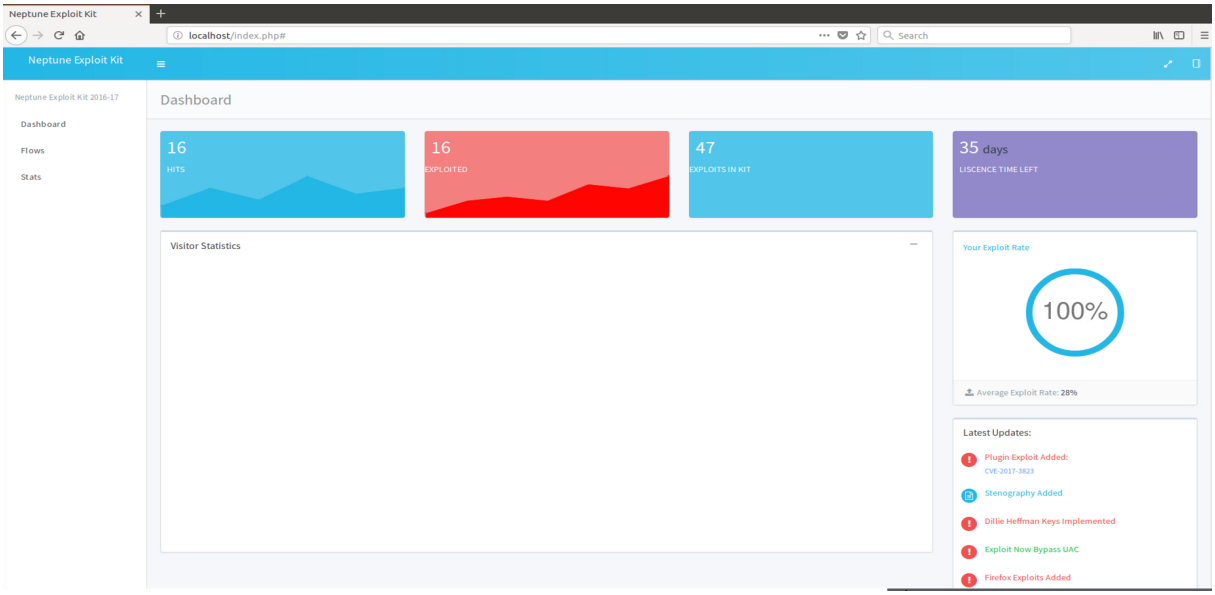


Figure 33 - Dashboard

From the menu on the left, if we click on files, we can setup a flow, which is our payload file. After finishing the setup, the exploit URL (landing page) is automatically generated together with an example of how to redirect victims to the landing server with an iframe as shown in Figure 34.

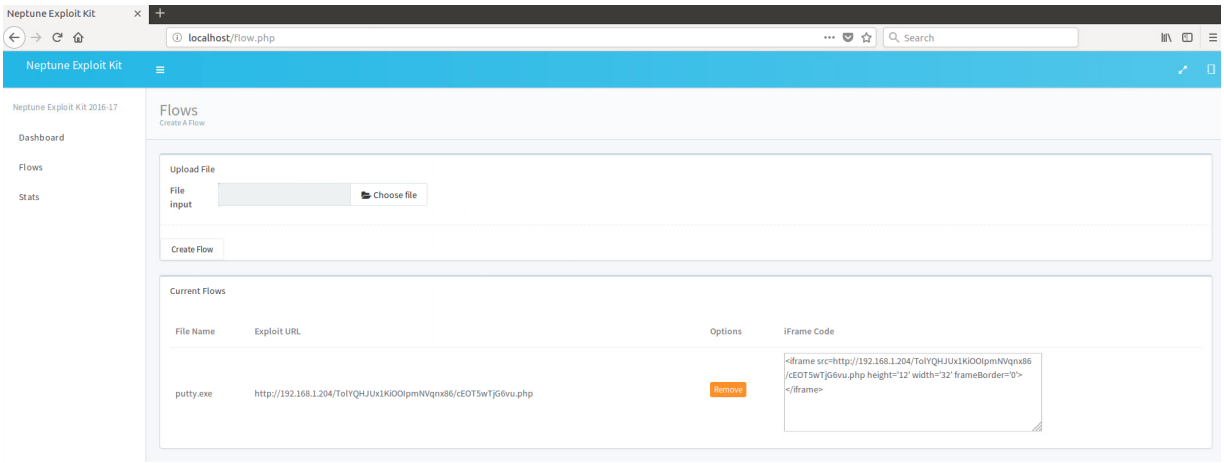


Figure 34 - Manage Payload

On a page named “Stats” shown in Figure 35, a user can check statistics relating to the infected victim such as operating system, browser, country and type of exploits.

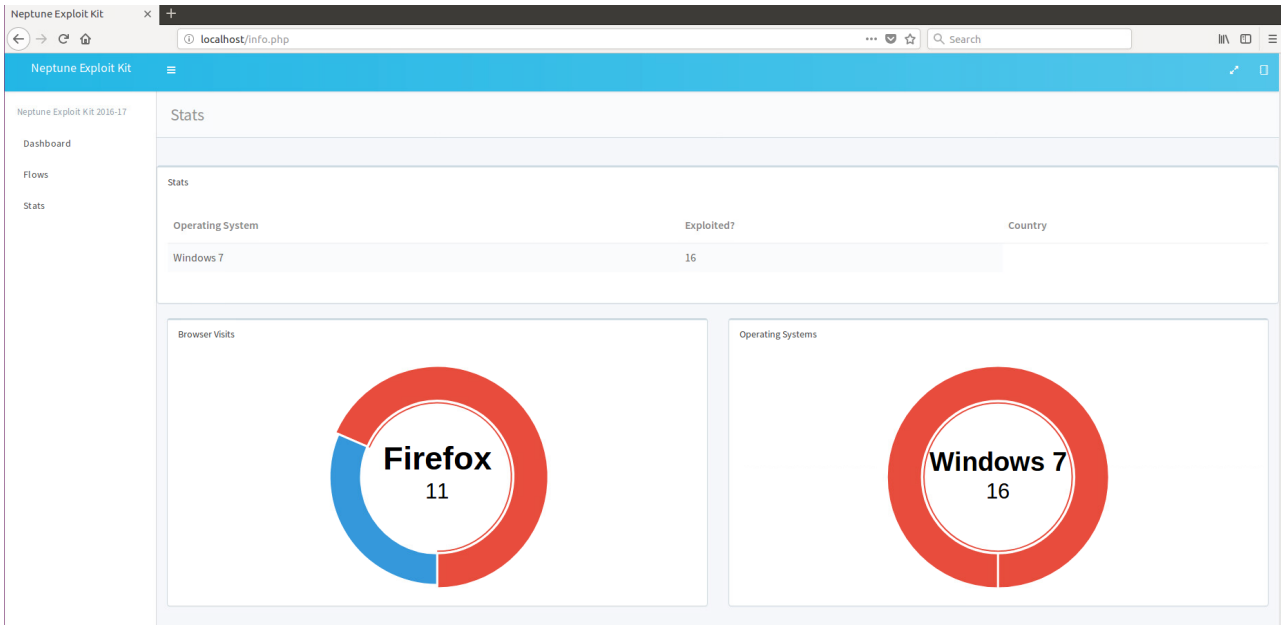
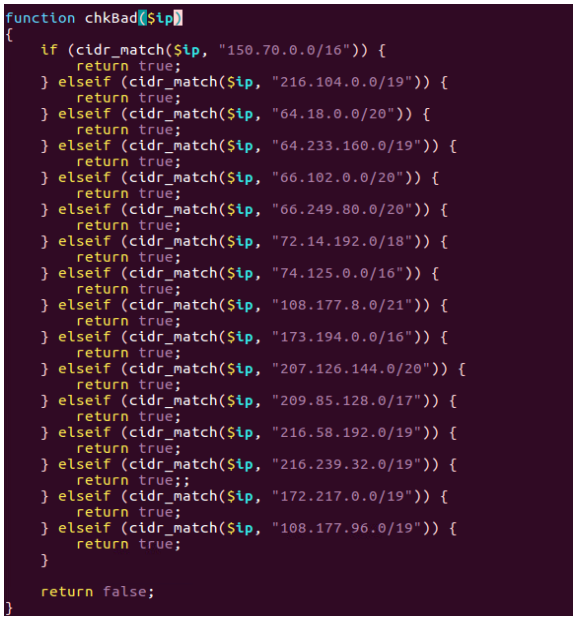


Figure 35 - Statistics

Uploader Server: The uploader sever has two main functions. Firstly, it connects to the panel server using the API and downloads payloads whenever a new flow is set up on the Panel server.

Then, the uploader server generates a folder with a random name which contains, a landing page with randomized name, exploits, payload and configurations files to connect back to the database on the main server. The generated folder is copied to the landing server through as SSH channel. The uploader server connects to panel server one a minute.

Landing Server: The landing server running on Apache hosts the landing page with exploits and connects back to the main server in order to update victim information. When a victim accesses a landing page, it first checks the victim's environment and exploit the victim according to it. In order to protect itself, the landing page blocks search engine robots by filtering http-user-agent and blocks google and trend micro through IP filters as shown in Figure 36 and Figure 37 respectively.



```
function chkBad($ip)
{
    if (cidr_match($ip, "150.70.0.0/16")) {
        return true;
    } elseif (cidr_match($ip, "216.104.0.0/19")) {
        return true;
    } elseif (cidr_match($ip, "64.18.0.0/20")) {
        return true;
    } elseif (cidr_match($ip, "64.233.160.0/19")) {
        return true;
    } elseif (cidr_match($ip, "66.102.0.0/20")) {
        return true;
    } elseif (cidr_match($ip, "66.249.80.0/20")) {
        return true;
    } elseif (cidr_match($ip, "72.14.192.0/18")) {
        return true;
    } elseif (cidr_match($ip, "74.125.0.0/16")) {
        return true;
    } elseif (cidr_match($ip, "108.177.8.0/21")) {
        return true;
    } elseif (cidr_match($ip, "173.194.0.0/16")) {
        return true;
    } elseif (cidr_match($ip, "207.126.144.0/20")) {
        return true;
    } elseif (cidr_match($ip, "209.85.128.0/17")) {
        return true;
    } elseif (cidr_match($ip, "216.58.192.0/19")) {
        return true;
    } elseif (cidr_match($ip, "216.239.32.0/19")) {
        return true;;
    } elseif (cidr_match($ip, "172.217.0.0/19")) {
        return true;
    } elseif (cidr_match($ip, "108.177.96.0/19")) {
        return true;
    }

    return false;
}
```

Figure 36 - Self Protection by IP

```
function bot_detected()
{
    if (isset($_SERVER['HTTP_USER_AGENT']) && preg_match('/bot|crawl|Google|msnbot|Rambler|Yahoo|AbachoBOT|accoona|AcoiRobot|ASPSeek|CrocCrawler|Dumbot|FAST-WebCrawler|GeonaBot|Gigabot|Lycos|MSRBOT|Scooter|AltaVista|IDBot|eStyle|Scrubby|YandexBot|agent|crawler|wget|seek|discovery|baidu|slurp|spider/i', $_SERVER['HTTP_USER_AGENT'])) {
        return TRUE;
    } else {
        return FALSE;
    }
}
```

Figure 37 - Self Protection by User Agent

Attack Infrastructure

We replicated the attack infrastructure of Neptune exploit kit as shown in Figure 38.

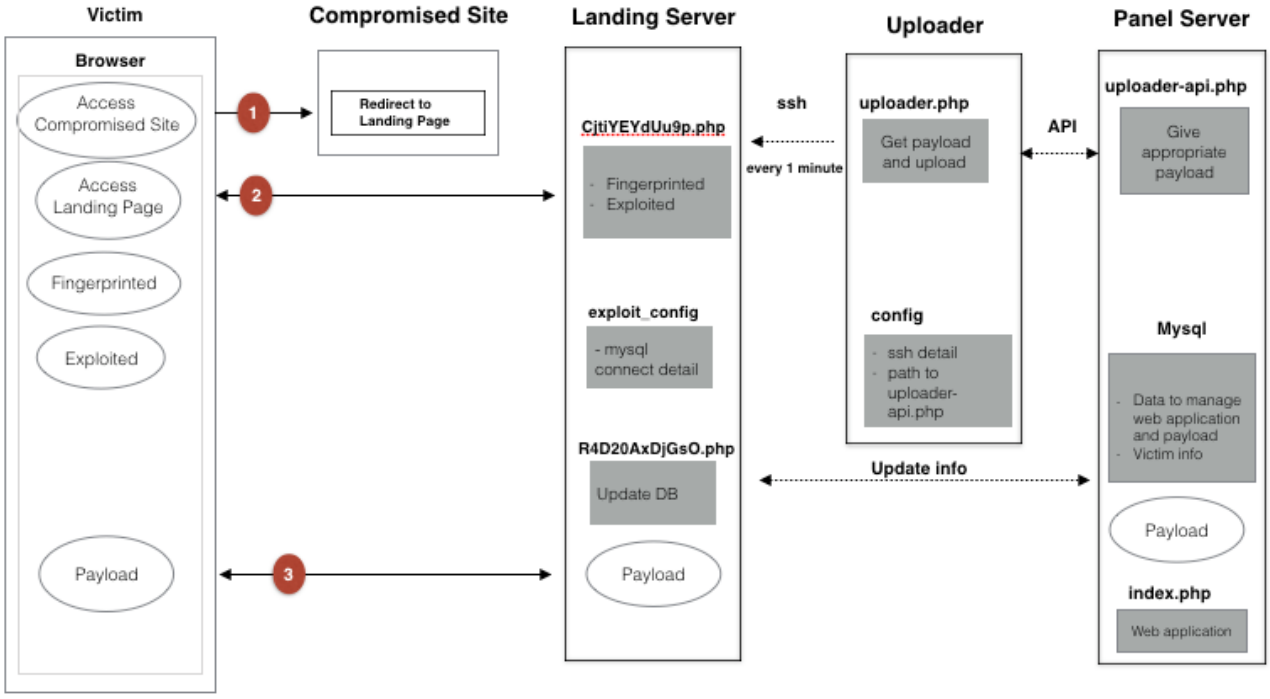


Figure 38 - Neptune Attack Infrastructure

Red colored numbers in Figure 38 represent the traffic from a victim's browser and dotted lines show how servers behind the senses are working together. Attack flow is as follows:

- Firstly, a victim accesses the compromised site and is redirected to the landing page.
- When a victim accesses the landing page, victim information such as IP, country, browser, OS, and referrer will be recorded. Then, the victim will be exploited according to its environment.
- Finally, an exploit is downloaded and the hit data record of DB in panel server will be updated. Now, the victim is owned by the attacker.

Database

The dumped database does not include much data. The name of the database is "blaze" and tables in the database are summarized in Table 17.

Table 17 - Tables in Database

Table name	Table Structure	Sample Data	No: Rows
domains	id, domain	4, www.google.com	3
flows	id, user_id, flow_id, file_url, original_name, status, remote_directory, flow_url, flow_server	41', '1', '1117524043', 'uploads/1117524043.exe', 'messagebox_crypted_02.exe', 'complete', '1sV77pgWNLxl244sTyYogIab', 'http://127.0.0.1:1380/1sV77pgWNLxl244sTyYogIab/VoceCLnEONIQ.php',	1
flows_to_delet e	id, flow_server, remote_directory	empty	0
hits	id, flow , ip, agent, referrer, country, browser, exploited, unixtime, os	2', '1117524043', '192.168.217.2', 'Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko', 'direct', '', 'Internet Explorer', '0', '1488075374',	3
user	id, username, password, active	1,admin, md5ofpassword, 1	1

Exploits

There are 11 different types of exploits in the leaked kits. Although we know the CVE for 8 exploits, we do not know the last 3. Some exploits codes seems to not be completed yet. The target application and respective CVEs of exploits are depicted in Table 18.

Table 18 - Exploits

No	Target Application	CVE
1	IE	CVE-2013-2551
2	Windows	CVE-2014-6332
3	IE	CVE-2015-2419
4	IE	CVE-2016-0189
5	Firefox	CVE-2013-1710
6	Firefox	CVE-2014-1510
7	Firefox	CVE-2014-8636
8	Firefox	CVE-2016-9078
9	-	Unknown CVE
10	-	Unknown CVE
11	-	Unknown CVE

Self-protection features

In order to protect itself, the Neptune exploit kit uses the following features;

- Directory listing attack is prevented.
- Landing page name is randomized.
- There is code for encrypting payloads although the current version does not use it.
- The landing server blocks search engine bots and security vendors such as TrendMicro
- The Jabber message box for buying exploit kits does not accept messages from strangers.
- Blocking search engine bots and crawlers from the security community using IP block lists and http-user agent block lists.

Weak Points

- The panel server does not have whitelist IPs and everyone with API seems to be able to download payload from it.

Chapter 4

Potential Attacks

By replicating the attack infrastructure of exploit kits, we have found weaknesses in their infrastructure, such as the way servers are managed. From this, we believe that there is a potential to counter-attack the exploit kit infrastructure with nothing but customer privileges. In this chapter, we will discuss the weaknesses of each of the leaked exploit kits and potential attacks against them.

In order to confirm our findings of potential attacks, we became an actual customer of the Rig 4.0 exploit kit for one week. Please note that we became a customer only for research purposes as RIG 4.0 is currently highly active compared to other exploit kits. In this chapter, we will also discuss how we became the customer of the RIG 4.0 exploit kit, our analytical approach to current attack infrastructure, and potential methods to take down some servers of the RIG 4.0 exploit kit.

RIG 2.0 Exploit Kit

Attack Infrastructure

The replicated attack infrastructure of RIG 2.0 is depicted in Figure 39.

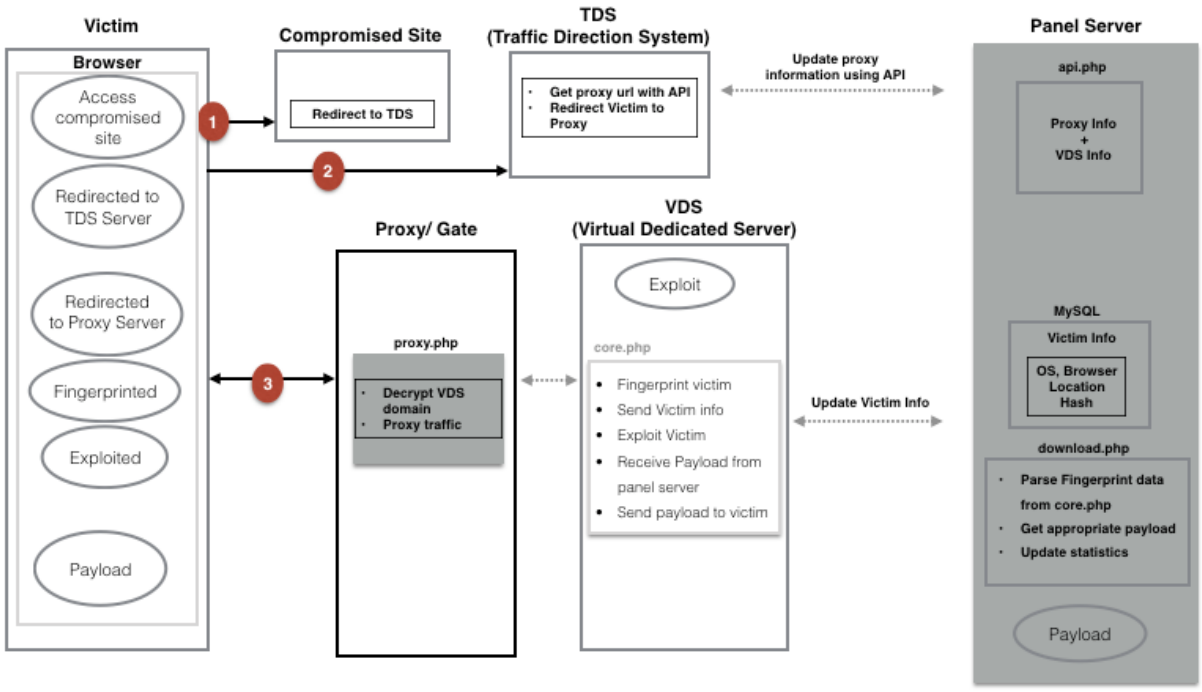


Figure 39 - RIG 2.0 Attack Infrastructure

Players in the Attack Infrastructure

Controlling parties of the RIG exploit kit attack infrastructure includes operators, attackers, and TDS vendors.

Operators: Operators offer exploit kit services to customers.

Attackers: Attackers use exploit kit service offered by operators.

TDS vendors: TDS (Traffic Direction System) vendors buy and sell Web traffic. The server used by them is called the TDS (Traffic Direction System) server.

Firstly, an attacker who would like to launch the campaign needs to register for exploit kit service with operators. In case of the RIG exploit kit, the panel server, VDS server and Proxy/Gate in Figure 39 are managed by operators behind the RIG exploit kit.

Then, in order to infect computers, an attacker needs to buy web traffic from TDS vendors. TDS services are not malicious but attackers abuse them for malware infection. The TDS server in Figure 39 connects to a panel server using API token assigned to the attacker in order to get active proxy server URL. The TDS server needs to have its IP whitelisted on the panel server in order to prevent other servers accessing to the API server and getting proxy URLs. Please refer to Chapter 3 for detailed functions of each server and the attack flow of drive-by download attack.

Potential Attack 1: Proxy Servers

API management: When an attacker registers as a customer of the RIG exploit kit, he or she will receive access to a panel server. Then, the attacker sets up payloads to use for the campaign and receives links to access to API server. An example of the general API link format used to access the API server is “http://panel_server_domain/APIscript.php?APItoken=tokenvalue”. When that API link is accessed by TDS, proxy URL is generated by the API server and TDS uses this proxy URL to redirect a victim to the right proxy server.

Attack Scenario: According to how proxy URLs are generated using the API link discussed above, we notice that a customer can collect as many proxy URLs possible using an API link. As the API server does not appear to enforce any access limits on generating these URLs and as proxy URLs are rotated from time to time, a customer can get as many proxy URLs as possible. We assume that this might lead to eventually exhausting the proxy server domains or IP addresses controlled by operators using only customer privileges. In addition, we also assume that these domains or

IPs of proxy domains might be reused among all attackers registered with the RIG exploit kit. We will prove our potential attack being a real customer of RIG 4.0 in the following sections.

Potential Attack 2: SQL Injection

We found a SQL injection vulnerability in the RIG 2.0 exploit kit. With this vulnerability, it is possible to change data from a certain table in the database or dump the whole database. Figure 41 shows our SQL injection test request using Burp and Figure 40 is the response from the RIG 2.0 panel server.

```
POST /manage/gears/saveVDS.php HTTP/1.1
Host: 192.168.1.175
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Referer: http://192.168.1.175/manage/index.php
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 126
Cookie: dS1G86KwRZ=1b88f059dabdbe9e9d6d8aeddbc4b676
Connection: close

1%5Bid%5D=1&1%5Bip%5D=http%3A%2F%2F192.168.1.161%2Fdownload.php&1%5Bdescription%5D=&2%5Bid%
5D=2&2%5Bip%5D='&2%5Bdescription%5D=
```

Figure 40 - SQL Injection Request

```
<pre style='border:3px dashed red;border-radius:10px;padding:10px;text-transform:none;'>array (
  'Error' => 0,
  'Message' =>
  array (
    0 => 'SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the
manual that corresponds to your MySQL server version for the right syntax to use near \'\'\'\' WHERE `id` = 1\' at line
1',
    1 => 'UPDATE `vds` SET `ip` = \'http://192.168.1.161/download.php\', `description` = \'\'\' WHERE `id` = 1;',
  ),
  'In file' => '/var/www/gears/db.php',
  'On line' => 88,
)</pre>
```

Figure 41 - SQL Injection Response

Potential Attack 3: Reflected XSS Attack

The RIG 2.0 panel server is vulnerable to reflected XSS attacks as well. With this, there is a possibility for session hijacking targeting customers and operators of the RIG 2.0. exploit kit.

Potential Attack: Related Servers on the Internet

From the leaked source code, we extracted some signature words allowing us to find servers relating to the RIG 2.0 exploit kit on Internet. Seller pages and panel server pages found on the Internet are shown in Figure 42 and Figure 43.

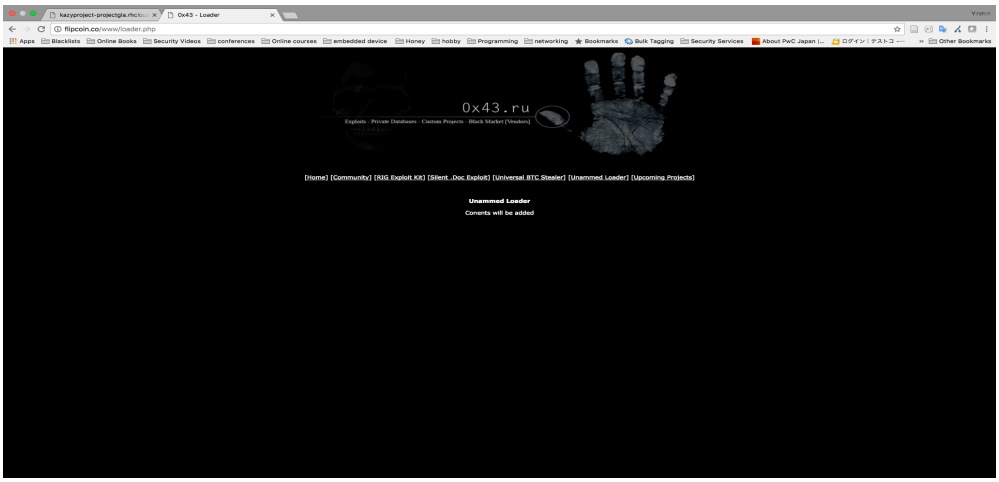
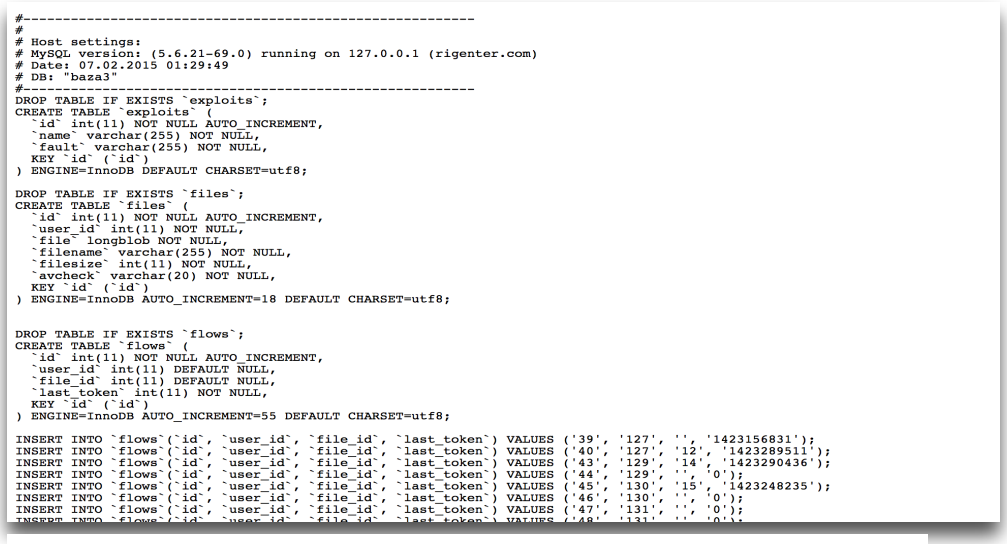


Figure 42 - Seller Page



```
#--------------------------------------------------------
#
# Host settings:
# MySQL version: (5.6.21-69.0) running on 127.0.0.1 (rigenter.com)
# Date: 07.02.2015 01:29:49
# DB: "baza3"
#--------------------------------------------------------
DROP TABLE IF EXISTS `exploits`;
CREATE TABLE `exploits` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `fault` varchar(255) NOT NULL,
  KEY `id` (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

DROP TABLE IF EXISTS `files`;
CREATE TABLE `files` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `user_id` int(11) NOT NULL,
  `file` longblob NOT NULL,
  `filename` varchar(255) NOT NULL,
  `filesize` int(11) NOT NULL,
  `avcheck` varchar(20) NOT NULL,
  KEY `id` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=18 DEFAULT CHARSET=utf8;


DROP TABLE IF EXISTS `flows`;
CREATE TABLE `flows` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `user_id` int(11) DEFAULT NULL,
  `file_id` int(11) DEFAULT NULL,
  `last_token` int(11) NOT NULL,
  KEY `id` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=55 DEFAULT CHARSET=utf8;

INSERT INTO `flows`(`id`, `user_id`, `file_id`, `last_token`) VALUES ('39', '127', '', '1423156831');
INSERT INTO `flows`(`id`, `user_id`, `file_id`, `last_token`) VALUES ('40', '127', '12', '1423289511');
INSERT INTO `flows`(`id`, `user_id`, `file_id`, `last_token`) VALUES ('43', '129', '14', '1423290436');
INSERT INTO `flows`(`id`, `user_id`, `file_id`, `last_token`) VALUES ('44', '129', '', '0');
INSERT INTO `flows`(`id`, `user_id`, `file_id`, `last_token`) VALUES ('45', '130', '15', '1423248235');
INSERT INTO `flows`(`id`, `user_id`, `file_id`, `last_token`) VALUES ('46', '130', '', '0');
INSERT INTO `flows`(`id`, `user_id`, `file_id`, `last_token`) VALUES ('47', '131', '', '0');
```

Figure 43 - Panel Server

RIG 4.0 Exploit Kit

In order to prove our findings of possibilities to detect and take down proxy domains, we became a customer of the RIG 4.0 exploit kit for one week. Our analytical approach of their attack infrastructure, how we became a customer and potential attacks on the RIG 4.0 exploit kit are explained in the following sections. Please note that although we became a customer of the exploit kit as a service offering, we did not buy any traffic from a TDS to redirect real victims. Instead, we setup our own TDS server and all the victim clients came from our lab environment.

Being an Insider

The RIG 4.0 exploit kit started to be active in August 2017. It is used for campaigns aiming to drop cryptocurrency mining payloads. From the forum discussing the RIG 4.0 exploit kit, we noticed the domain of a panel server (www.rigpriv.com) hidden behind the Cloudflare DDoS protection service. The panel server login page is depicted in Figure 44.

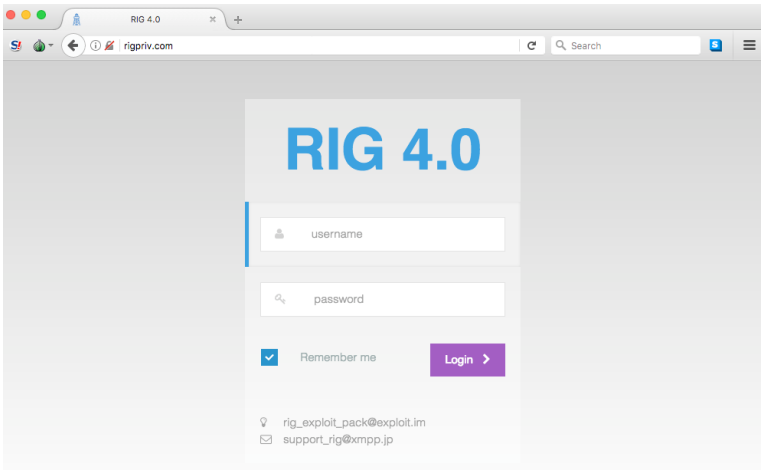


Figure 44 - RIG 4.0 Login Page

We received the Jabber contact (rig_exploit_pack@exploit.im) of a RIG seller from the login page. The contact method is explained on the exploit.im main page in Russian. Original and translated explanations are depicted in Figure 45. Figure 46 shows messages between us and the RIG seller. It seems that there are two different types of licenses; for a week and a month costing $500 US and $1500 US respectively. At the time of our registration, we estimate that there were more than 400 registered users based on our customer ID.

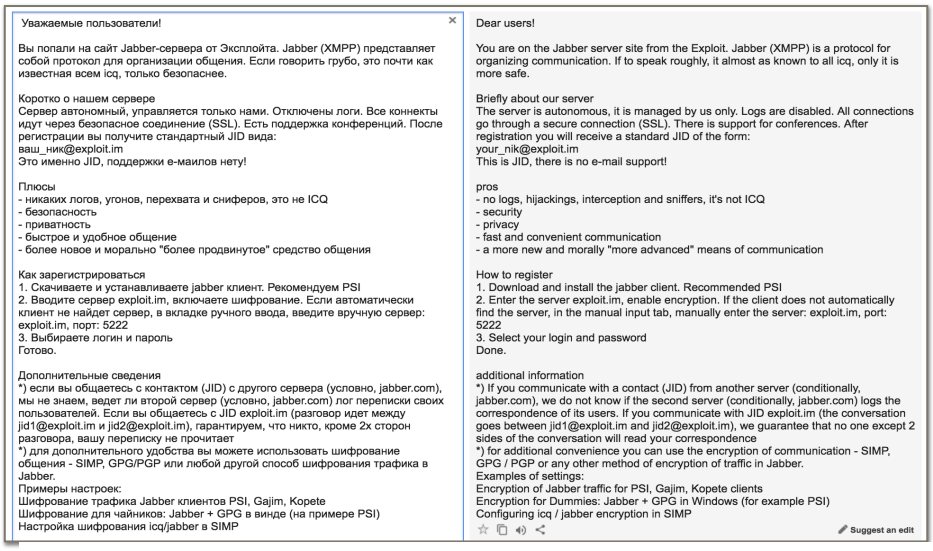


Figure 45 – Hot to Contact to RIG Seller

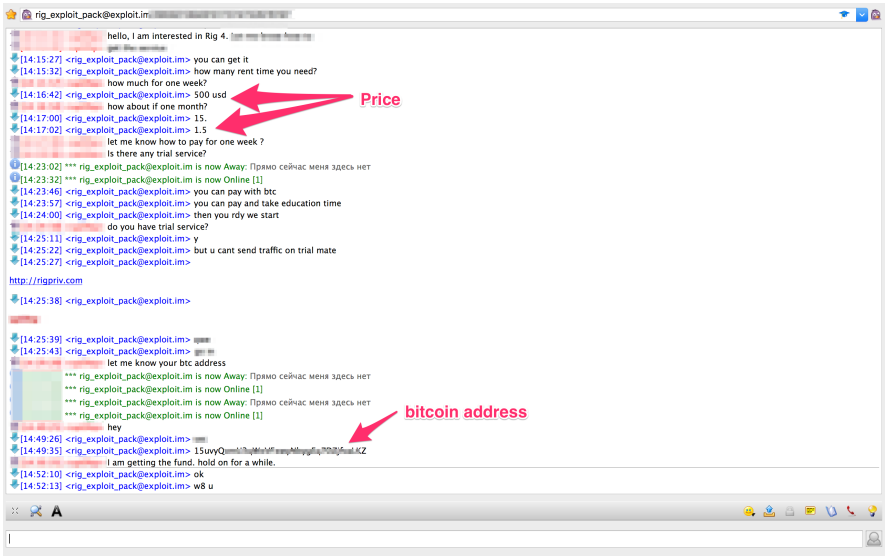


Figure 46 - Message to Seller

Good Income

Our curiosity leads us to check the transitions of the bitcoin address used by the RIG 4.0 operator. From public information, we found that the address started trading from 2014-09-27. At the time of writing, the account received a total of 767.30 bitcoins equivalent to about 7.8 million US dollars. Figure 47 shows the amount of transitions and total received bitcoins. Figure 48 is the amount of bitcoin received from 2014 to 2018. It is interesting to know that the amount of transitions increases right after the new version is released.

Summary		Transactions	
Address	[redacted]	No. Transactions	2518
Hash 160	[redacted]	Total Received	767.30969455 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	0.20494902 BTC

Figure 47 – Bitcoin Transitions

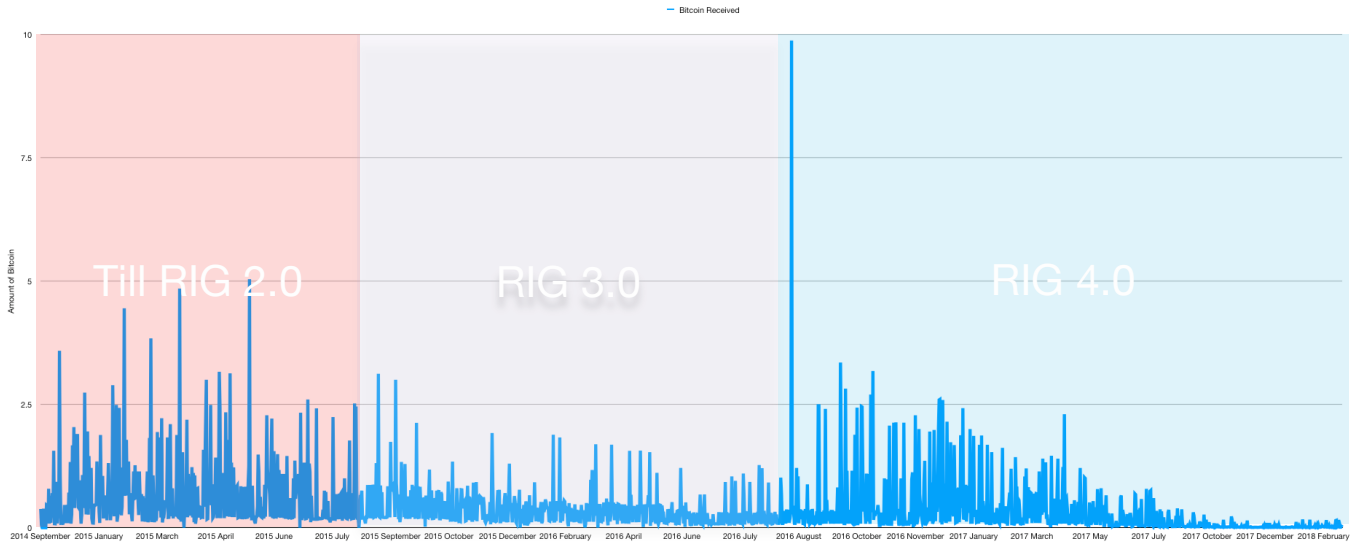


Figure 48 – Received Bitcoins

RIG 4.0 Infrastructure

We depict the attack infrastructure of RIG 4.0 in Figure 49 by analyzing all network traffic visible to us as a customer.

In Figure 49, the gray colored boxes are servers managed by the operators behind the RIG 4.0 exploit kit. Blue colored boxes are servers and clients controlled by us. A white colored box is a server we cannot see as the customer. The straight lines are all network traffic of victims and TDS vendors we are able to capture. Dotted lines are network traffic we cannot see.

The attack infrastructure of the RIG 4.0 exploit kit consists of five different types of servers.

Panel Server: The panel servers is the main server running the web application managing the RIG 4.0 exploit kit. It is hidden behind the Cloudflare DDoS protection service. The domain at the time of this writing is (www.rigpriv.com).

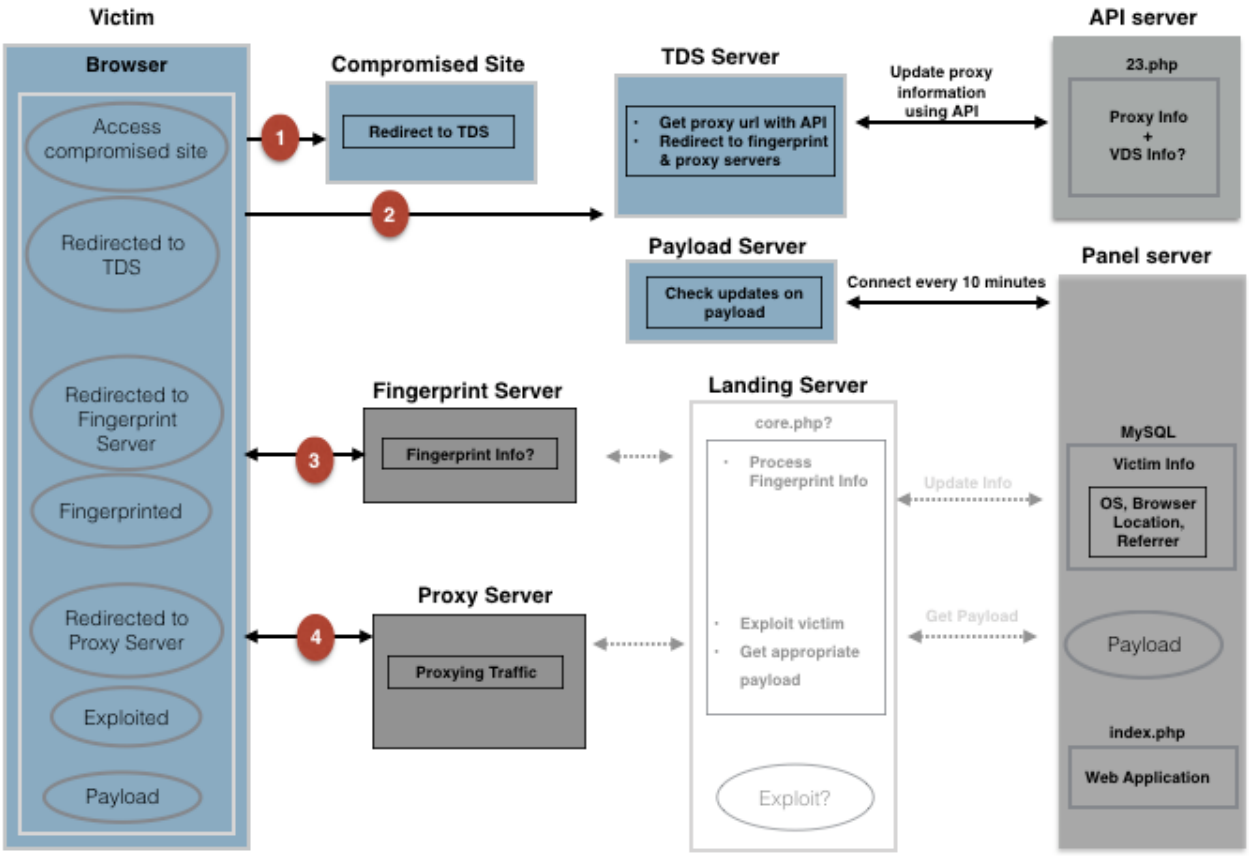


Figure 49 - RIG 4.0 Attack Infrastructure

API Server: The API server returns proxy domains whenever it is accessed by a whitelisted TDS server. In order to get access to the API server, customers need to whitelist the TDS IP as shown in Figure 50 and click the get link button as shown in Figure 51.

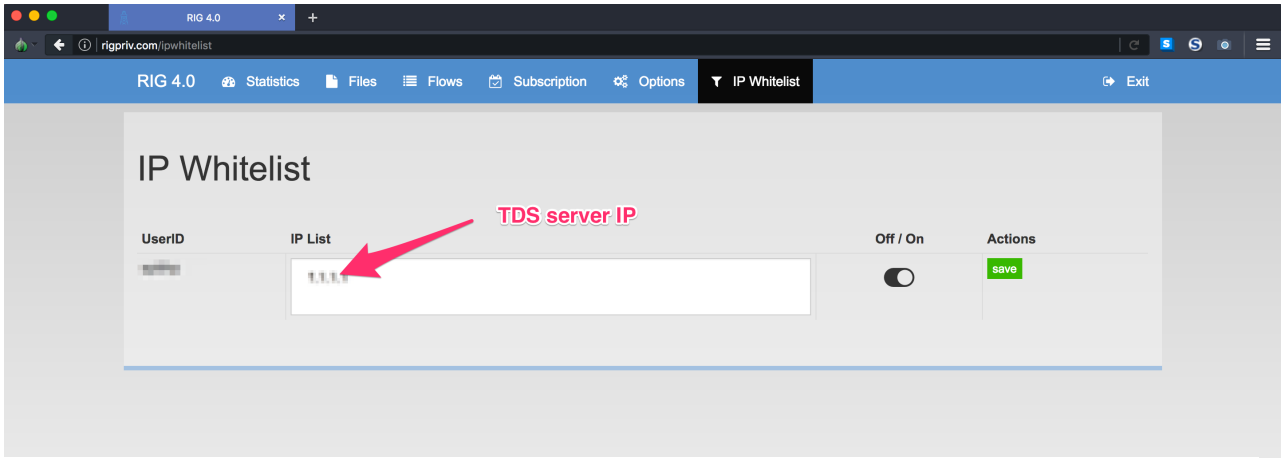


Figure 50 - Whitelist TDS

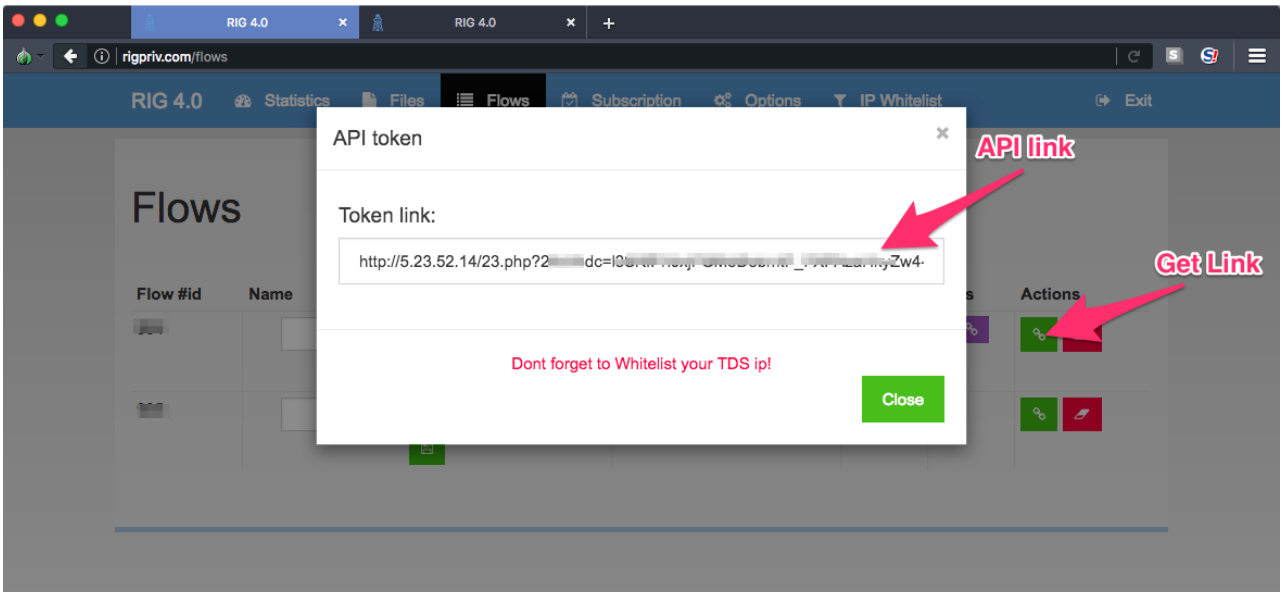


Figure 51 - API Link

Proxy Server: Proxy servers seem to be used to proxy traffic between the victim and VDS servers. Please note that we cannot see VDS servers hidden behind the proxy server. Links to proxy servers can be generated by accessing the API server.

Fingerprint Server: Before a victim is sent to the proxy server, it connects to the fingerprint server and sends some encrypted payload. We think that the victim is sending its environment information to that server.

TDS Server: We set up our own TDS (traffic redirection server) which connects to a panel server with API to get the proxy link and redirect the victim to a proxy server. We think that the VDS server IP and fingerprint server IP is encrypted in the parameters of the proxy link that the TDS receives from the panel Server. An example of a proxy link received from the TDS server is shown in Figure 52 where 188.225.56.143 is the IP address of the proxy server.

```
http://188[.]225[.]56[.]143/?MjI5MjI2&XrbMZkSasnuHx&IzIEBp=Y2FwaXRhbA==&bpPHjfahvu=bG9jYXRlZA==&eabizLZNjmWqf=
bWlsaw==&nRdecvsCs=xHvQMrfYbRnFFYffKPjEUKBEMUrWA0KKwYuZhajVF5ixFDDGpbf1FxnspVidCF6EmvVvdLEHIwah1UHA&DptzGyb=Y2
FwaXRhbA==&audaddCd=SwZjnY1dA1wUpq_7jETVwBDNh5KC9BGEZA9H-ZSQEbVoiVn8zbcXec9yzxDUuGIGzektYl8gpQ5R2ajI&zuNPOmw=Y
2FwaXRhbA==&GTpsYptgP=dGhpbmdz&GHvDVcGFVL=Y2FwaXRhbA==
```

Figure 52 - Proxy URL

Payload Server: A customer can setup a payload server URL in order to update payloads. We setup a payload server listening on TCP port 80. An unknown IP connects to our payload server to check for updates every 10 minutes. Every time, the same IP connects us. When we connect back to this IP, it is hosting the same content as the panel server. From this finding, we conclude that

the IP connecting to our payload server is the actual IP of the RIG panel server hiding behind CloudFlare.

Attack 1: Decoying Proxies

From our analysis of RIG 2.0, we have found that customers can generate as many proxy domains as possible using the API and that this might lead to taking down the proxy server using only customer privileges. This approach has the limitation that if these proxy domains are used only for one customer, even if we are able to take down the proxy it would be meaningless.
To prove our findings, we:

1. Collect as many proxy domains as possible and analyze their behaviors
2. Check whether these proxy domains appear in any other open source reports on the Internet

To collect proxies, our TDS server accesses the API server every 10 minutes. We then analyze all collected proxy URLs and find out that, In RIG 4.0:

1. Rather than domains, proxy servers use IP addresses
2. Proxy IP addresses seem to be rotated randomly
3. Proxy information can be collected even after the registered period as a customer has expired
4. All IP addresses are hosted on the TimeWeb hosting service of Russia
5. All proxy server IP addresses we collected are also used for other customers as there is a 100% match between the proxy IPs we collected and those shared at ektracker.com.

Currently, we are able to collect 108 proxy server IP addresses and this information is shared in the Appendix section.
From these findings, we are able to prove that proxy IPs can be taken down only with customer privileges and that these rotating proxy IP addresses are shared among different users of the current RIG 4.0 exploit kit.

Attack 2: Reveal the Hidden Panel Server IP

Panel server connects to our payload server to check for updated payloads for every 10 minutes. When we connect back to this IP, it is hosting same content as the panel server. From this finding, we conclude that the IP connecting to our payload server is the actual IP of the RIG panel server

hiding behind CloudFlare. The actual panel server IP and contents are shown in Figure 53 and Figure 54.

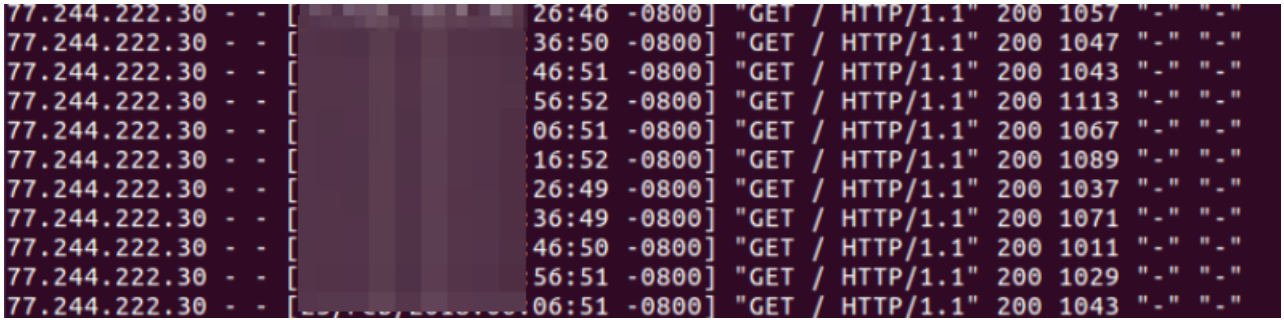


Figure 53 - Connection to Payload Server

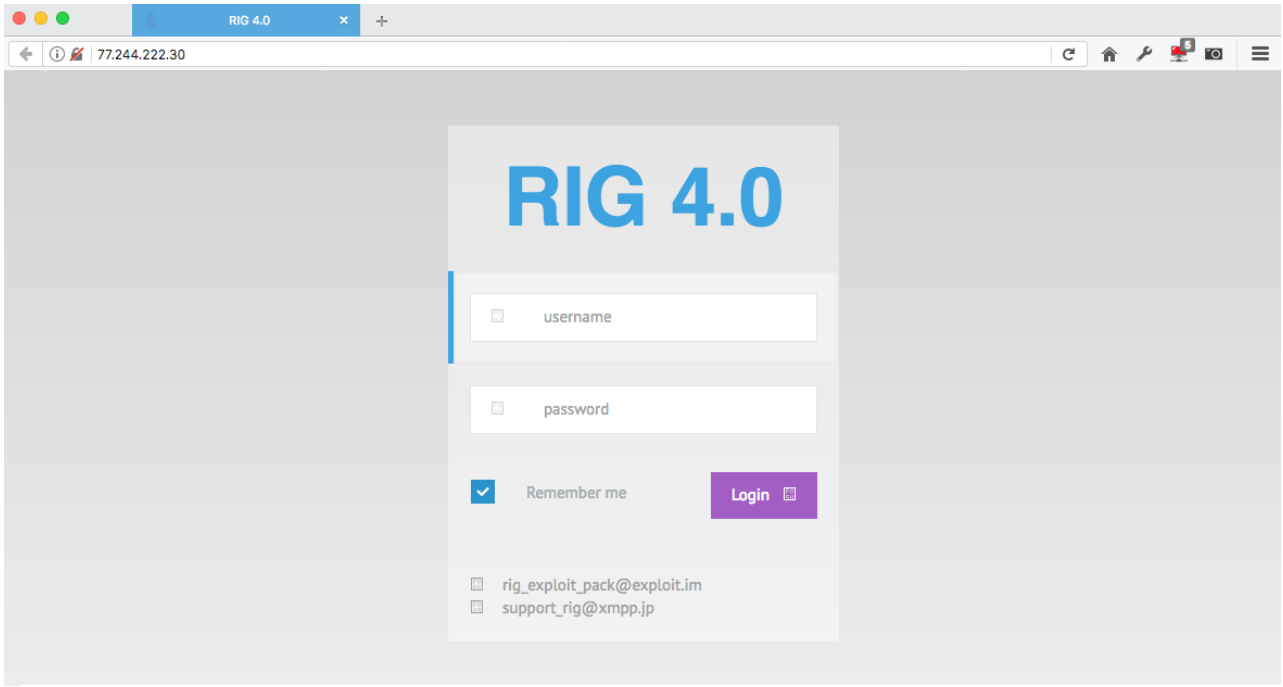


Figure 54 – Actual IP of RIG 4.0 Panel Server

Attack 3: Collecting More and More Proxies

Due to insufficient authentication performed by the API server, even after the registration period has expired, we are able to access the API server and get updated proxy links. We assume that this is due to a weak point in user access management. Using this weak point, we keep on collecting proxy server IP addresses and currently we so far able to collect 108 proxy server IP addresses during our analysis from February 22 to March 5 as shown in Figure 55. All IP addresses are Russian IP addresses hosted at Time Web Hosting service.

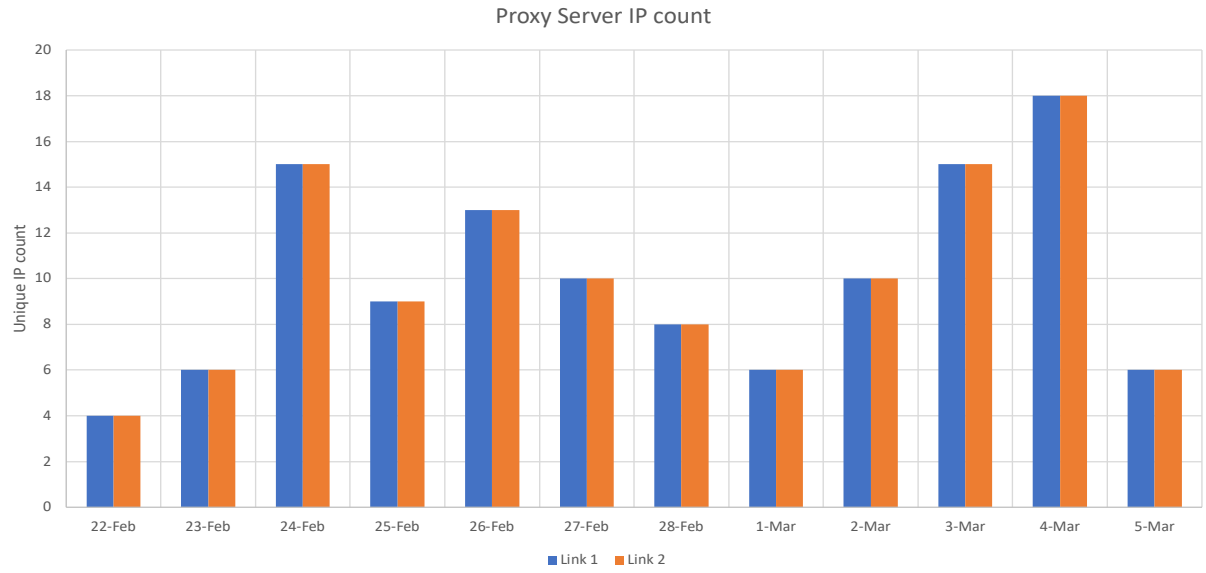


Figure 55 - Collected Proxy Server IP

Attack 4: Directory Listing

Based on our previous knowledge of analyzing the RIG 2.0 exploit kit, we have listed some of the directories and checked the contents. From this, we notice that RIG 4.0 is running on Apache 2.2.22 (Debian) and we are able to access some open directories such as the "/gears/ajax" and "/html" directories shown in Figure 56 and Figure 57. It seems that directory names are almost the same as RIG 2.0. At the time of this writing, the directory "/gears/ajax" is not accessible. It seems that the operators also keep on watching their panel server's security.

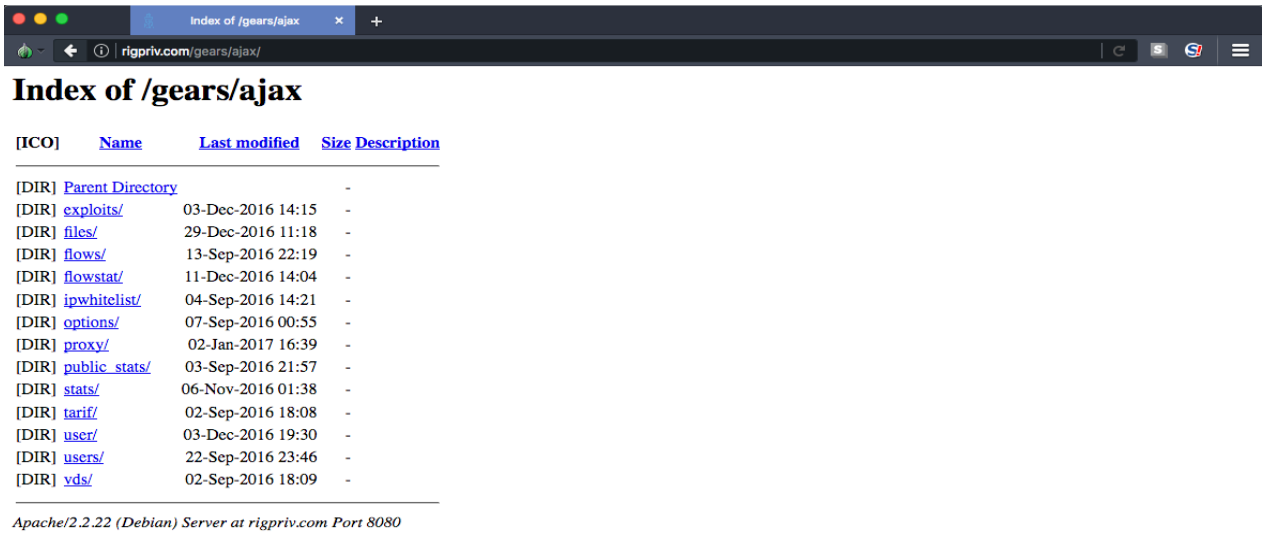


Figure 56 - Directories in Panel Server

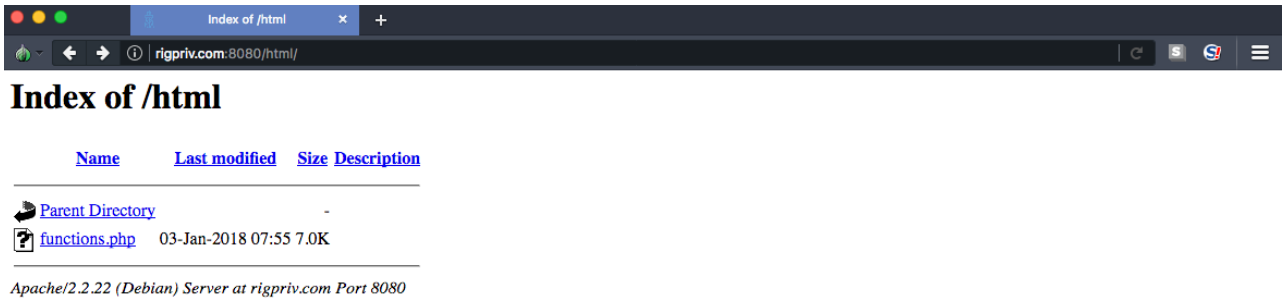


Figure 57 - Directory in Panel Server

Although the content of the folder named "/upload" was visible in RIG 3.0, it is not visible in RIG 4.0. However, we confirmed that the contents we were able to see before are downloadable. The downloaded executable files and their detection ratio on Virus Total is shown in Figure 58.

```
MD5 (A06fdnK6.exe) = 7eea81afdb7ab260064aea5dd5ac6531 (UltraVNC) 48/66
MD5 (B0Pufbvx.exe) = 7d2dc8564359854b9da0a6a83e915185 (Trojan) 52/64
MD5 (CSLu17XX.exe) = 64e0165d8cf21c65d3cb3b8a94718d20 (Trojan) 49/68
MD5 (CeUoJBCb.exe) = cbc23ce5f4b4e4142172808ed3ece105 (Trojan) 49/65
MD5 (LaAET1TP.exe) = a987017ffdee4de5ac20ee15b369e103 (Trojan) 56/65
MD5 (LtKr5sjF.exe) = 4a497fdacf903dc19e9112f007505cf7 (Trojan) 49/68
MD5 (S0jS26J5.exe) = 360f878799f95b9d095676060145252e (Trojan) 29/61
```

Figure 58 - EXE Files in Upload Directory

Attack 5: Peaking Attackers

Due to a lack of access restriction enforcement, we are able to access statistics of other registered users. We tested different flow IDs ranging from 0 to 10 and 840 to 950. From this, we were able to see the exploit rates of 21 users. A summary of our findings is shown in Table 19 . According to Table 19, there are about 111,255 computers being exploited with a total exploitation rate of 12.4 %. In addition, we collected 108 referrer domains which redirect victim traffic to the RIG 4.0 landing page.

Table 19 - Attackers Using RIG 4.0 and Exploit Rates

No	Flow ID	Top Country	Hits	Exploits	%	Top Browser	Top OS	Referrers Domain	Exploit Types
1	874 (mxmxmx)	Mexico	9	2	22.2	MSIE 11.0	Windows 10	1	2
2	975 (mx)	Mexico	5437	378	7	MSIE 11.0	Windows 7	9	6
3	880	Brazil	714451	94351	13.2	MSIE 11.0	Windows 7	10	6
4	884 (TRAFF)	United Kingdom	1	0	0	MSIE 8.0	Windows Vista	0	0
5	887	US	14982	418	2.8	MSIE 11.0	Windows 7	10	5
6	890	United Kingdom	1	0	0	MSIE 11.0	Windows 7	0	0
7	898(col)	US	213	6	2.8	MSIE 11.0	Windows 10	4	2
8	899 (korsaisback)	Netherlands	190	4	2.1	MSIE 11.0	Windows 7	10	2
9	902	Turkey	58560	7874	13.4	MSIE 11.0	Windows 7	10	6
10	906	Turkey	794	96	12.1	MSIE 11.0	Windows 7	1	3
11	907	Mexico	2	0	0	MSIE 11.0	Windows 7	1	0
12	908 (Nutrino)	US	11	0	0	MSIE 11.0	Windows 10	0	0
13	910	US	788	28	3.6	MSIE 11.0	Windows 7	1	5
14	912 (First Server)	US	2860	41	1.4	MSIE 11.0	Windows 7	10	3
15	913 (Second Server)	US	3241	47	1.5	MSIE 11.0	Windows 7	10	3
16	914	Egypt	140	10	7.1	MSIE 11.0	Windows 7	1	2
17	920 (first)	Brazil	83293	7261	8.7	MSIE 11.0	Windows 7	10	6
18	921 (Maaa)	Germany	1	1	100	MSIE 8.0	Windows 7	0	1
19	923 (test)	Taiwan	5530	691	12.5	MSIE 11.0	Windows 7	10	6
20	927 (test)	US	110	32	29.1	MSIE 7.0	Windows XP	10	5
21	929	US	417	15	3.6	MSIE 11.0	Windows 7	0	2
Total			**891031**	**111255**	**12.4**			**108**	**65**

Statistics of some of the high-profile users with more than 10,000 IP hits are shown in Figure 59 and Figure 60. We share the referrer domain list in the Appendix section.

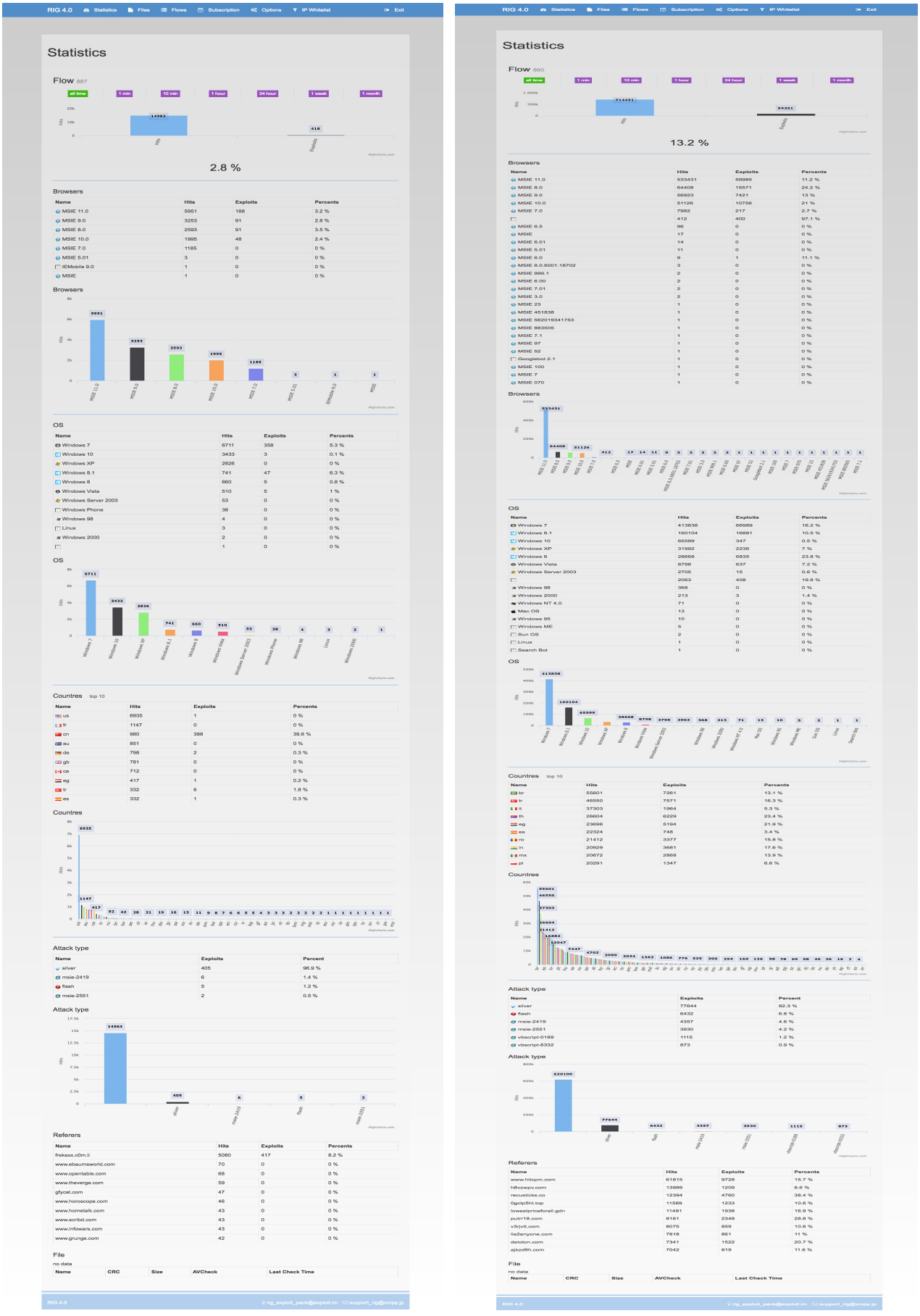


Figure 59 - Flow 887 and Flow 880

Figure 60 - Flow 902 and Flow 920

Attack Infrastructure

The replicated attack infrastructure of the BEPs exploit kit is depicted in Figure 61.

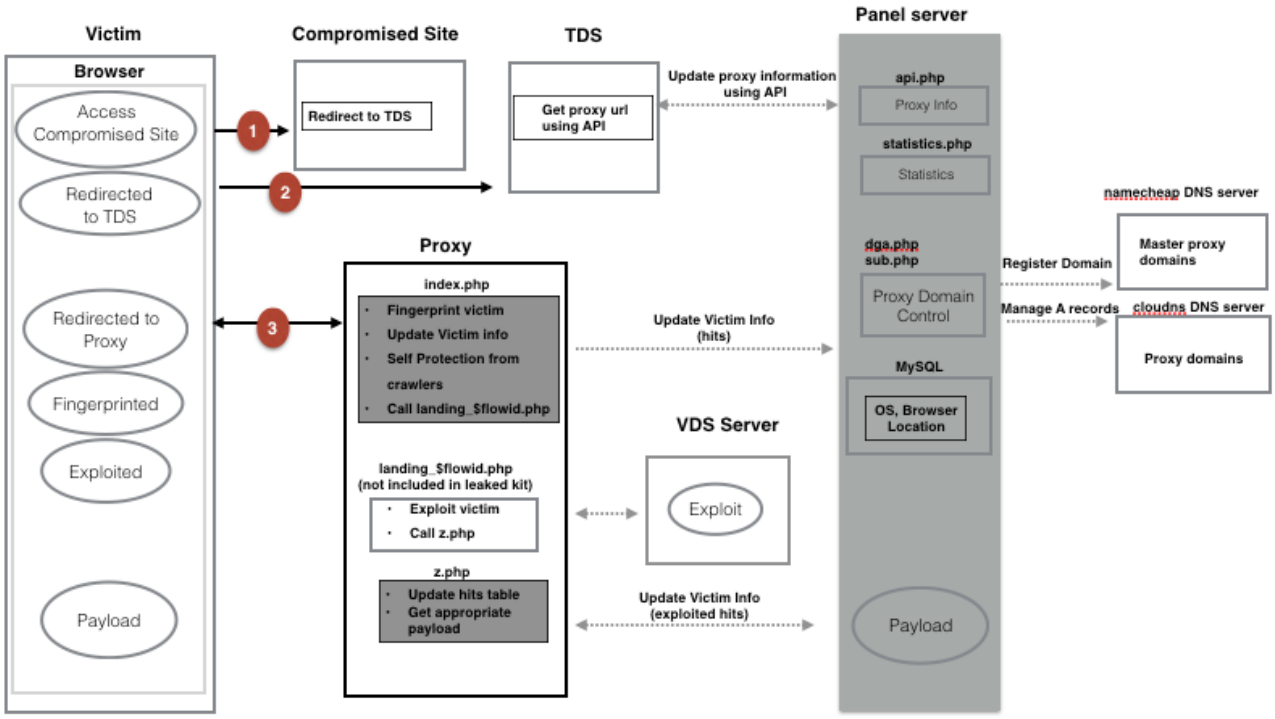


Figure 61 - BEPS Attack Infrastructure

Players in the Attack Infrastructure

Controlling parties of the BEPS/Sundown exploit kit attack infrastructure includes operators, attackers, and TDS vendors.

Operators: Operators offer exploit kit services to customers.

Attackers: Attackers use exploit kit service offered by operators

TDS vendors: TDS (Traffic Direction System) vendors buy and sells Web traffic. The server used by them is called the TDS (Traffic Direction System) server.

Firstly, an attacker who would like to launch the campaign needs to register for exploit kit services with an operator. The panel server and proxy server in Figure 61 are managed by operators behind the BEPS exploit kit.

Then, in order to infect computers, an attacker needs to buy web traffic from TDS vendors. TDS services are not malicious as such attackers abuse them for malware infection. The TDS server connects to panel server using API token assigned to the attacker in order to get active proxy

server URLs. Please refer to Chapter 3 for details on the functions of each server and the attack flow of drive-by download attacks.

Potential Attack 1: Decoying Proxies

API management: When an attacker registers as a customer of the BEPS exploit kit, he or she will receive access to the panel server. Then, attackers setup payloads to use for the campaign and get the link to access the API server using an API link such as http://panelserver_IP/index/api.php?sid=XXX in which XXX is the API token value of the customer.
Attack Scenario: From the analysis on how proxy URLs are generated using the API link discussed above, we notice that a customer can generate proxy URLs using the API. As the API server does not appear to enforce any limits on generating these URLs and as proxy URLs are rotated from time to time, a customer can get as many proxy URLs as desired. We assume that this might lead to exhausting the proxy server domains or IP addresses controlled by operators using only customer privileges.

Potential Attack 2: Fake API Access

IP addresses of TDS servers are not whitelisted on the panel server and so anyone with an API token can access the proxy server. Namely, if we can guess or calculate an API token of a customer, we will be able to get all proxy addresses used by that customer.

Attack Infrastructure

The replicated attack infrastructure of Hunter exploit kit is depicted in Figure 62.

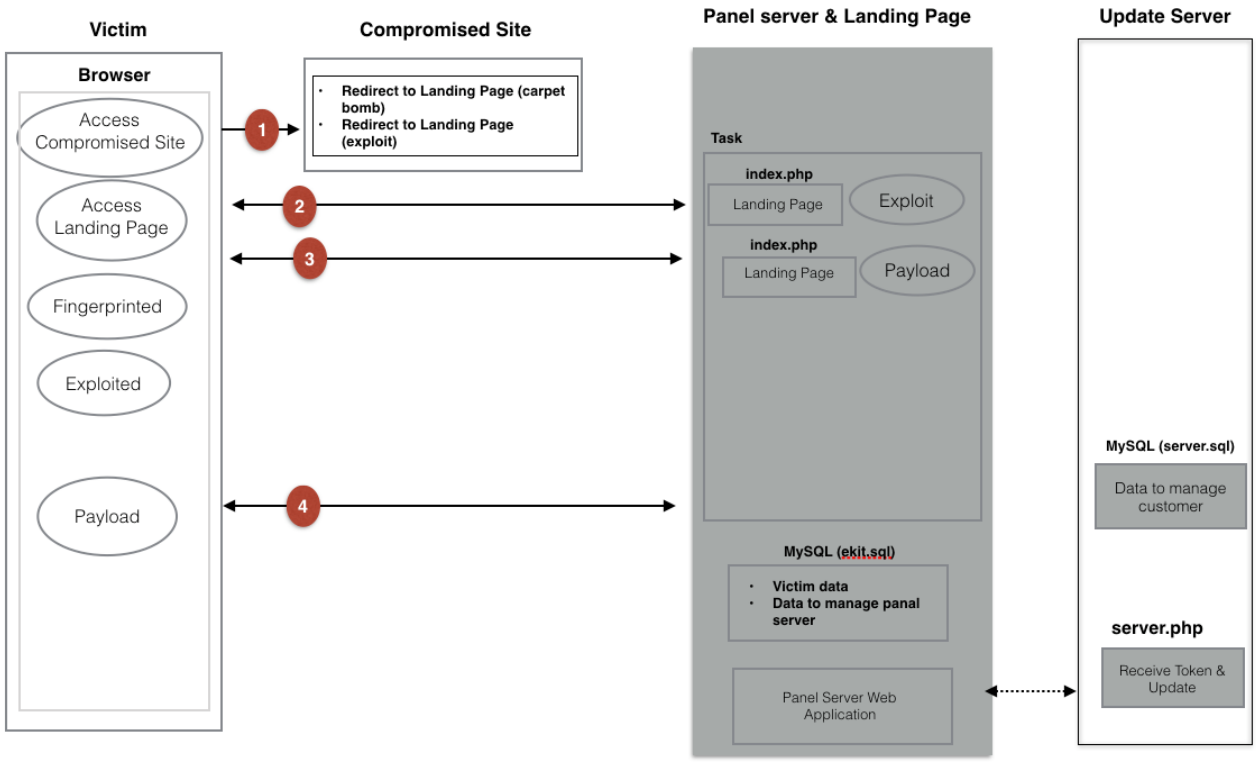


Figure 62 - Hunter Attack Infrastructure

Players in the Attack Infrastructure

Controlling parties of the Hunter exploit kit attack infrastructure include operators and attackers.

Seller: In case of the Hunter Exploit Kit, operators only offer updates of the panel server web application.

Attackers: An attacker buys the exploit kit as a package from the Seller.

Firstly, the attacker who would like to launch the campaign needs to buy the exploit kit web application as a package from the seller. Attackers need to set up the panel server and landing page.

Then, in order to infect computers, the attacker needs to buy web traffic from TDS vendors or use any other way to get victims redirected to his landing page. Please refer to Chapter 3 for details on

the function of each server and the attack flow of drive-by download attacks using the Hunter exploit kit.

Potential Attack 1: Easy to Detect Panel Server

According to the analysis on the leaked code, the landing page and panel server seem to be running on the same server. In addition, we did not find any proxy server functionality. Thus, we think that the panel server can be detected easily.

Potential Attack 2: Easy to Find Landing Page

There is a special character “task” in every iframe generate by the Hunter exploit kit. This might allow to detect landing pages easily.

Potential Attack 3: Related Servers on the Internet

From the leaked source code, we extracted some signature and crawled servers relating to the Hunter exploit kit on the Internet. We are able to detect one panel server page on the Internet as shown in Figure 63.

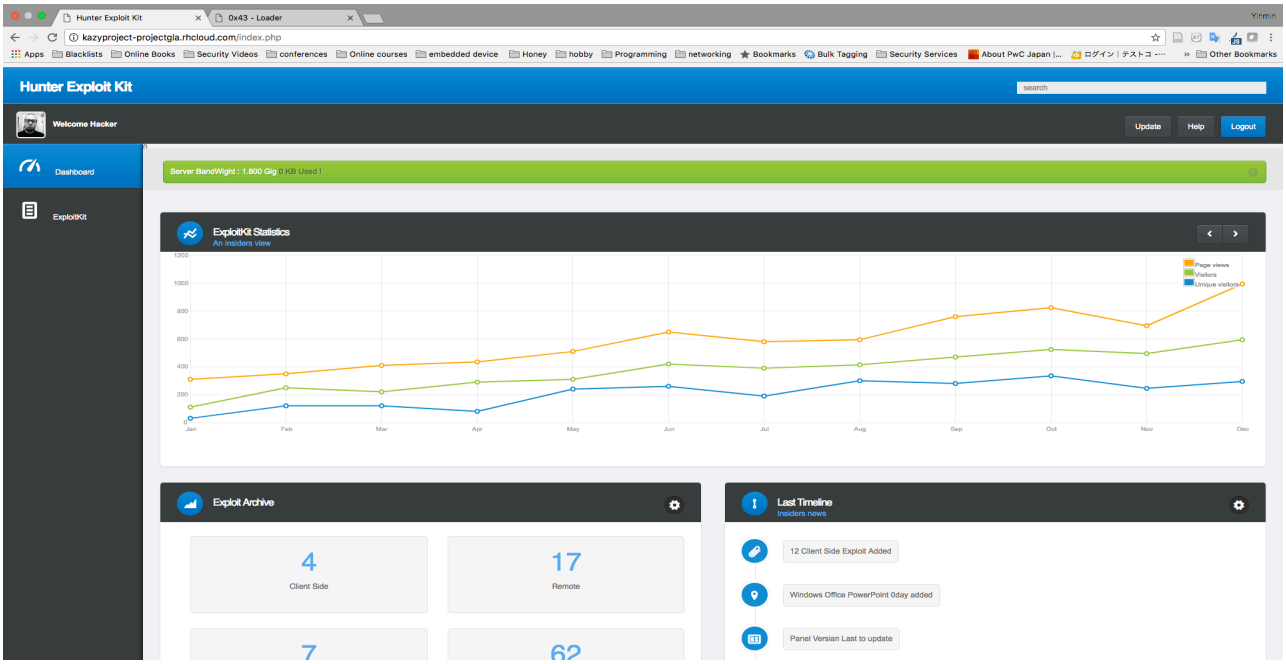


Figure 63 - Hunter Panel Server

Attack Infrastructure

The replicated attack infrastructure of Neptune exploit kit is as shown in Figure 64.

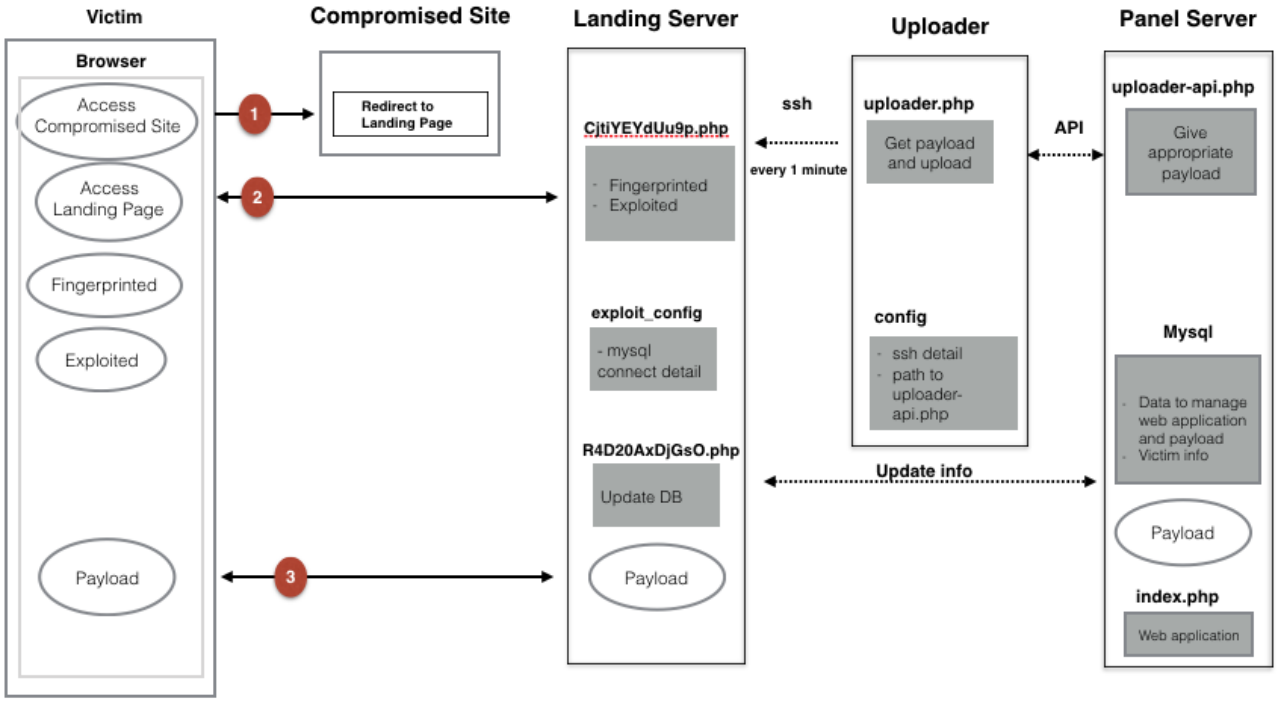


Figure 64 - Neptune Attack Infrastructure

Players in Attack Infrastructure

Controlling parties of the Neptune exploit kit attack infrastructure include sellers and attackers.

Seller: A seller sells code for the panel server, uploader and landing server as a package.

Attackers: An attacker buys the exploit kit as a package.

Firstly, the attacker who would like to launch a campaign needs to buy the exploit kit web application as a package from the seller. Attackers need to set up the panel server, uploader and landing server according to the manual in the package. Then, in order to infect computers, the attacker needs to buy web traffic from a TDS vendor or use any other way to get victims redirected to his landing page. Please refer to Chapter 3 for details on functions of each server and the attack flow of drive-by download attacks using the Neptune exploit kit.

Potential Attack 1: Fake API Access

The panel server does not whitelist IPs and everyone with API access seems to be able to download payloads from it.

Potential Attack 2: Related Servers on Internet

From the leaked source code, we extracted some signature and crawled servers related to the Neptune exploit kit on the Internet. We were able to detect some compromised servers on the Internet as shown in Figure 65.

Figure 65 - Compromised Servers

Chapter 5

Future Possibilities

Upon our analysis of several different leaked exploit kits, we noticed the following two main similarities between them:

- Exploit kits share similar design pattern in their attack infrastructure.
- The code between different exploit kits is similar.

From this, we believe that the attack methods discussed in Chapter 4 are usable not only against leaked kits but also against other unknown kits that share similarities with the leaked ones. In this Chapter, we will discuss similar design patterns and similar code among different exploit kits.

Similar Design Patterns

We analyzed several attack infrastructures of different exploit kits and we were able to group them into two main groups according to similarities in their attack infrastructure.

Group 1: Almost all old exploit kits in this group such as Sakura, Demon Hunter, Mushroom, Elenore Express, etc., share a similar type of attack infrastructure among them. Namely, 1) landing server and panel server exists on the same server, 2) no proxy is set up, 3) landing page URLs have signatures that allow us to detect panel servers easily and 4) several web application vulnerabilities exist.
The similarities in attack infrastructure lead to similarities in vulnerabilities too. Thus, attacks such as detecting panel servers and web applications related to attacks are common among different kits too. Therefore, operators behind exploit kits put more effort into self-defense features such as rotating proxies, TTL of proxies, etc., in new kits.

Group 2: So-call advanced exploit kits common today such as RIG, BEPS/Sundown, etc., use features such as 1) rotating proxies, 2) API to update proxies in their attack infrastructure, 3) VDS servers and 4) hiding behind DDoS protection services, etc. In addition, recent exploit kits give better service to their customers providing one-stop exploit statistic page and updating payloads automatically. These features, in turn, lead to decoying of proxies, abusing APIs and leakage of statistical information of different exploit kit users.
We pointed out some possible attacks relating to these advanced features and we believe that it might be possible to use them for future exploit kits as well.

Code Reuse

Code reuse among different exploit kits we analyzed is quite frequent. We were able to classify 33 leaked exploit kits into 6 groups according to code reuse among them.

Group 1: The first group includes the RIG, Hunter, Neptune and BEPS/Sundown exploit kits sharing. An example of code reuse among them is shown in Figure 66.

Figure 66 - Code Reuse

Group 2: The second group includes the Demon Hunter and Bleeding Life exploit kits. An example of code reuse among them is shown in Figure 67.

Figure 67 - Code Reuse

Group 3: The third group includes the Sakura and Armitage exploit kits. An example of code reuse among them is shown in Figure 68.

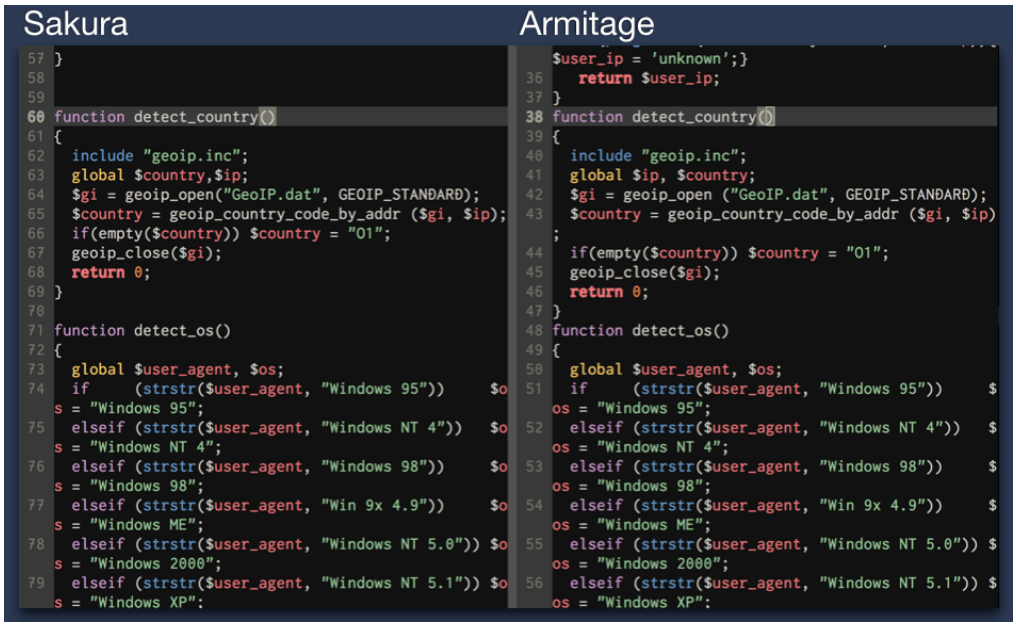


Figure 68 - Code Reuse

Group 4: The fourth group includes the 0x88, multisploit, RDS and Infector exploit kits. An example of code reuse of among them is shown Figure 69.

Figure 69 - Code Reuse

Group 5: The fifth group includes the Sakura and Armitage exploit kits. An example of code reuse of among them is shown Figure 70.

Mushroom

```
function crypt_with_key($orig,$key)
{
  for($l=0;$l<strlen($orig);$l++)
  {
    $symb=$orig[$l];
    $pos_in_key=strpos($key,$symb);
    if($pos_in_key >= -1)
    {
      if($pos_in_key==(strlen($key)-1))
      {
        $pos_in_key =-1;
      }
      $crypt .= $key[$pos_in_key+1];
    }
    else
    {
      $crypt.=$symb;
    }
  }
  return $crypt;
}
////////////////////////////////////////////////
//  <font style="font-size:11px" color="#666666" face="Arial">Infected Name</font>
////////////////////////////////////////////////
function rand_tag_name()
```

Elenore

```
function crypt_with_key($orig,$key)
{

  for($l=0;$l<strlen($orig);$l++)
  {
    $symb=$orig[$l];
    $pos_in_key=strpos($key,$symb);
    if($pos_in_key >= -1)
    {
      if($pos_in_key==(strlen($key)-1))
      {
        $pos_in_key =-1;
      }
      $crypt .= $key[$pos_in_key+1];
    }
    else
    {
      $crypt.=$symb;
    }
  }
  return $crypt;
}
function rand_tag_name() {
  $tag_name = array ('p', 'div', 'b','u','i');
  $count_tag_name = count($tag_name);
  return $tag_name[rand(0, $count_tag_name-1)];
```

Figure 70 - Code Reuse

Group 6: The sixth group includes the rest of exploit kits such as ice-pack, Tor, etc. An example of code reuse among them is shown in Figure 71.

ice-pack

```
6%u14BE%u3828%u74F2%uC108%u0ÐCB%uÐA03%uEB40%u3BEF%u75ÐF%u5EE7%u5E8B%u0324%u66ÐD%u0C8B%u8B4B%u1C5E%uÐD03%u048B%u038B%uC3C5%u7275%u6D6C%u6E6F%u642E%u6C6C%u2e00%u5C2e%u2e7e%u7865%u0065%uC033%u0364%u3040%u0C78%u408B%u8B0C%u1C70%u8BAÐ%u0840%u09EB%u408B%u8Ð34%u7C40%u408B%u953C%u8EBF%u0E4E%uE8EC%uFF84%uFFFF%uEC83%u8304%u242C%uFF3C%u95D0%uBF50%u1A36%u702F%u6FE8%uFFFF%u8BFF%u2454%u8DFC%uBA52%uÐB33%u5353%uEB52%u5324%uÐ0FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF%u83FF%u04EC%u2C83%u6224%uÐ0FF%u7EBF%uE2Ð8%uE873%uFF40%uFFFF%uFF52%uE8Ð0%uFFÐ7%uFFFF".@$escexeurl."';\n";
      echo "var success=0;\n";
      if ( $browers == 1 )
      {
          if ( $config['spl1'] == 'on' && $vers[0] < 7 )
          {
              include( "exploits/x1.php" );
          }
          if ( $config['spl9'] == 'on' )
          {
            include( "exploits/x9.php" );
```

Tor

```
6%u14BE%u3828%u74F2%uC108%u0ÐCB%uÐA03%uEB40%u3BEF%u75ÐF%u5EE7%u5E8B%u0324%u66ÐD%u0C8B%u8B4B%u1C5E%uÐD03%u048B%u038B%uC3C5%u7275%u6D6C%u6E6F%u642E%u6C6C%u2e00%u5C2e%u2e7e%u7865%u0065%uC033%u0364%u3040%u0C78%u408B%u8B0C%u1C70%u8BAÐ%u0840%u09EB%u408B%u8Ð34%u7C40%u408B%u953C%u8EBF%u0E4E%uE8EC%uFF84%uFFFF%uEC83%u8304%u242C%uFF3C%u95D0%uBF50%u1A36%u702F%u6FE8%uFFFF%u8BFF%u2454%u8DFC%uBA52%uÐB33%u5353%uEB52%u5324%uÐ0FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF%u83FF%u04EC%u2C83%u6224%uÐ0FF%u7EBF%uE2Ð8%uE873%uFF40%uFFFF%uFF52%uE8Ð0%uFFÐ7%uFFFF".$escexeurl."';\n";
    echo "var success=0;\n";
    if ( $browser == 1 )
    {
        if ( $x1 && $vers[0] < 7 )
        {
            include( "exploits/x1.php" );
        }
        if ( $x9 )
        {
            include( "exploits/x9.php" );
        }
```

Figure 71 - Code Reuse

Due to this code reuse pattern among several different exploit kits, we believe that vulnerabilities will be similar and this might in turn lead to taking down future exploit kits with the same attack methods we showed in this paper.

Conclusion

In this study, we analyzed many different leaked exploit kits. Most popular exploit kits nowadays are just recovered versions of previously leaked ones. From this, we came up with a detailed understanding of how API servers, panel servers, proxy servers, VDS servers, uploader servers, update servers and fingerprint servers are working together in the exploit kit attack infrastructure. Namely, the attack infrastructure of exploit kits, their self-protection features, and weak-points are revealed in this study explained in Chapter 3.

We will first summarize self-protection features of exploit kits. They are as follows:

1) Use proxy servers in order to hide the actual attack infrastructure.
2) Use rotating domains and IPs for these proxy servers in order to prevent an easy takedown and to confuse security researcher.
3) Domain registration for proxy and VDS servers is automated in order to keep the infrastructure alive even after registered domains are sinkhole.
4) Block search engine bots and crawlers from the security community using IP block list and http-user agent block list.
5) VDS or landing pages have a TTL in order to limit duplicate access from counterparties.
6) The panel server is protected behind DDoS protection services to prevent attacks from rivals and to hide the actual IP of the panel server.
7) API server access is limited to only whitelisted servers in order to prevent API abuse.
8) The landing URL is randomized to prevent detection of landing pages using URL signatures.
9) The payload is encrypted to prevent analysis and abuse by rivals.
10) Detection ratio of proxy domains and payloads is checked in order to update them over time.
11) Directory listings on panel servers and proxy servers are prevented.

Understanding these self-protection features lets us know weak points of exploit kits when such features are not implemented and gives us ideas on how to counter attack them when they are. In addition, the insights on how operators behind exploit kit services give better service to their customers summarized below and a deep understanding on their attack infrastructure gives us ideas on how to counter-attack them using only customer privileges.

Customer services:

1) An API for updating the rotating proxy URL so that customers can update the proxy easily.
2) Public statistic checks so that customer can check infection ratio without logging in to the panel server account.
3) A user can update their payload dynamically by registering a payload server URL at panel server.
4) A service to let users check the detection ratio of his or her payload automatically is provided.

With all these details in mind, we propose potential attacks against each exploit kit in Chapter 4. In addition, we prove some of the proposed attacks by being an insider of today's most profitable exploit kit, RIG 4.0. From this, we prove that RIG 4.0 can be taken down by generating as many proxy IPs as possible using only customer privileges. In addition, we also give insights on other vulnerable points of Rig 4.0 to counter-attack it in Chapter 4.

Finally, we believe that the potential attack methods proposed in this study can be used for future exploit kits as well, due to most exploit kits sharing similar design patterns in their attack infrastructure and the nature of code reuse among different exploit kits as explained in Chapter 5.

References

1) https://blog.trendmicro.com/trendlabs-security-intelligence/promediads-malvertising-sundown-pirate-exploit-kit/
2) https://blog.skyboxsecurity.com/nebula-exploit-kit/
3) https://forum.antichat.ru/threads/prodazha-trafika-android-deskop-vysokogo-kachestva.458691/
4) https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers
5) https://www.hackread.com/hacking-forum-w0rm-ws-hacked-data-leaked/
6) https://www.cyber.nj.gov/threat-profiles/exploit-kit-variants/
7) https://ifud.ws/threads/1-neptune-exploit-kit-17-exploits-in-one-10-30-execution-rate.12471/
8) https://www.jpcert.or.jp/present/2018/JSAC2018_05_ikuse.pdf
9) https://forum.antichat.ru/threads/prodazha-trafika-android-deskop-vysokogo-kachestva.458691/
10) https://www.v3.co.uk/v3-uk/news/2420811/rig-30-exploit-kit-hits-the-hacker-underground-and-infects-millions
11) https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Reloaded---Examining-the-Architecture-of-RIG-Exploit-Kit-3-0/
12) http://malware-traffic-analysis.net/2017/03/02/index.html
13) http://malware.dontneedcoffee.com/2017/03/nebula-exploit-kit.html
14) https://www.cyber.nj.gov/threat-profiles/exploit-kit-variants/sundown

Appendix – 1

RIG 4.0 Proxy IP List

176.57.208.139	188.225.25.118	188.225.26.200	92.53.107.210
176.57.208.145	188.225.25.119	188.225.26.222	92.53.107.215
176.57.208.171	188.225.25.128	188.225.26.238	92.53.107.22
176.57.208.232	188.225.25.129	188.225.27.40	92.53.107.27
176.57.214.105	188.225.25.130	188.225.34.142	92.53.107.28
176.57.215.10	188.225.25.142	188.225.34.41	92.53.107.33
176.57.215.127	188.225.25.143	188.225.38.7	92.53.107.34
176.57.215.137	188.225.25.145	188.225.46.56	92.53.107.35
176.57.215.138	188.225.25.146	188.225.56.149	92.53.107.57
176.57.215.37	188.225.25.147	188.225.57.109	92.53.107.70
176.57.215.78	188.225.25.148	188.225.57.126	92.53.107.73
176.57.215.80	188.225.25.164	188.225.57.130	92.53.107.74
176.57.215.86	188.225.25.165	188.225.57.132	92.53.107.75
176.57.215.87	188.225.25.166	188.225.57.133	92.53.107.80
188.225.10.18	188.225.25.167	188.225.57.236	92.53.107.82
188.225.11.77	188.225.25.168	188.225.57.61	92.53.107.83
188.225.18.102	188.225.25.193	188.225.9.136	92.53.107.84
188.225.18.30	188.225.25.231	188.225.9.147	92.53.107.85
188.225.24.20	188.225.25.232	5.23.48.242	
188.225.24.248	188.225.25.233	5.23.52.74	
188.225.24.249	188.225.25.237	5.23.53.222	
188.225.24.28	188.225.25.238	5.23.55.128	
188.225.24.29	188.225.25.239	92.53.107.121	
188.225.24.39	188.225.25.248	92.53.107.122	
188.225.24.43	188.225.25.249	92.53.107.138	
188.225.25.108	188.225.25.250	92.53.107.170	
188.225.25.109	188.225.25.251	92.53.107.172	
188.225.25.110	188.225.25.252	92.53.107.205	
188.225.25.111	188.225.25.253	92.53.107.206	
188.225.25.117	188.225.25.254	92.53.107.207	

Appendix – 2

RIG 4.0 Referrers

carlosmoles.club	fullmusculo.com
aluminiobalear.club	www.tedigocomosehace.com
fincalaleyenda.club	www.collegemagazine.com
188.225.57.186	superauto.es
188.225.57.189	www.cagliaricontainersagency.com
176.57.214.214	cagliaricontainersagency.com
188.225.57.188	www.canvascamp.us
188.225.57.196	www.clicktripz.com
188.225.33.250	totallythebomb.com
digitaldsp.com	cannabis.com
www.hitcpm.com	aga.grandparents.com
h8vzwpv.com	roomkey.com
recusticks.co	freedomdaily.com
0gctp5ht.top	www.warpedspeed.com
lowestpriceforall.gdn	profitablesoft.top
putrr18.com	earndoublecoin.top
v3rjvtt.com	investingtodayfix.top
lie2anyone.com	mymoneyfixing.top
deloton.com	myearnmoneybin.top
ajkzd9h.com	wowmoney.top
freksxx.c0m.li	link.tl
www.ebaumsworld.com	images.futbolbase.us
www.opentable.com	services.myspservices.com
www.theverge.com	www.imgsky.net
gfycat.com	kstate.ru
www.horoscope.com	sexnn1.c0m.li
www.hometalk.com	185.223.31.126
www.scribd.com	www.makeuseof.com
www.infowars.com	www.nerdwallet.com
www.grunge.com	diseasecalleddebt.com

www.eater.com
www.miamiherald.com
www.mendeley.com
www.arduino.cc
www.google.co.id
popmog.com
185.223.31.126
www.makeuseof.com
www.nerdwallet.com
diseasecalleddebt.com
www.eater.com
findagrave.com
www.google.co.id
www.mendeley.com
www.clickondetroit.com
www.ridgewallet.com
videonabludenn.top
lowestpriceforall.gdn
jebadu.com
newsbusters.org
mktogel008.com
adpays.net
panel.pwrads.com
deloton.com
ah.pe
moradu.com
assets.bro.adca.st
thebloginfolife.blogspot.co.il
thebloginfolife.blogspot.tw
thebloginfolife.blogspot.com.es
thebloginfolife.blogspot.com.tr
thebloginfolife.blogspot.it
thebloginfolife.blogspot.fr
thebloginfolife.blogspot.co.uk
thebloginfolife.blogspot.com.br
thebloginfolife.blogspot.ru
thebloginfolife.blogspot.ro

8teenxxx.mywifibaby.com
bigtitsgalleriesfree.biz
pornoteenxxx.net
www.fresh-galleries.com
ukrainemodels.ru
ateen.space
www.browsebitches.com
firsttimelesbianxxx.com
nudismpage.com
hugeboobsgirl.com