

The path to infection - Eye glance at the first line of "Russian Underground" - focused on Ransomware

Archived: 2026-04-05 21:58:03 UTC

2012-12-05 - Study



One year since I started "active" actions in understanding what is on the other side of malware/mass infection campaign. Will share in one picture how i figure things.

(I hope to have many feedback to fix/adjust my understanding)

I will focus on the Ransomware case but most parts are valid for many other "blind mass attack" (as Ransomware is a specific case of Botnet)

Straight to the visual :



Eye glance at the first line of "Russian Underground"

The path to infection

[Credits](#) for some models used here

Note: New infection vector appeared in early 2013 - RDP compromission then Crypto Ransomware

And now here are basic explanation to read the illustration (even if most of you don't need it :P).

I won't talk about what happen after infection (data/voucher code reselling, money laundering, etc...). It's another story.

(will try to add here a table of content or list of anchor links)

-Poke A Mole Concept

I will first talk about a concept to which i will often refer, the forest hiding the tree, or the "Poke A Mole board". On previous map, most of the steps are represented by a single node but even small groups will hide the real node/bad server behind redirectors/reverse proxies. It's easier to recreate a redirector than rebuild a new server once a node is burnt (read: blacklisted by browser internal protections or antivirus or other filtering tools). The smallest group will have one server and multiple IP, then we'll see some groups with one server and one redirector with multiple IPs, and bigger groups can daily add many redirectors.

This is how you can reach this kind of architecture for a single exploit kit :

or even bigger ([I saw one Blackhole with up to 2400 ips](#) available to reach it...at least 1940 when it was also hosting a Ransomware C&C)

Same goes for Domains. Having hundreds of domain allow bad guy to switch from one to another and escape domain based blacklisting. Managing domain generation/rotation can be manual, "outsourced", built-in the tools or managed by dedicated tools. I'll give more details later.

One other great illustration for both, was back in february/march 2012, the Sinowal/Torpig group hosting its custom Blackhole on infected nodes of its botnet and making it reachable via Fast-Flux && DGA (based on Twitter trends).

-Infection vector :

this is how you get infected (as I focus on *Ransomware*, I won't talk about USB/Network Share etc..

<edit 2013-03-25> Some crypto-ransomware are now deployed after RDP compromission. Bruteforce on windows server and Via Remote Desktop Protocol. </edit>

- Browsing Website :



- Compromised website : one website has been compromised either using a vulnerability (usually on outdated CMS) or using stolen credentials from owner, modified to redirect visitors to the infection.

There are a lot dedicated tools to manage a huge amount of iFrame on website with known credentials or kown vulns

The tools :

[Statistics](#) [Black](#) [Settings](#)

All: 5381 (3289)

- [facebook](#): 30
- [nacha](#): 5351

Today: 3168 (2525)

- [facebook](#): 26
- [nacha](#): 3142

[\[clear visits\]](#) [\[clear downloads\]](#)

A Nacha/Facebook themed spam Tool



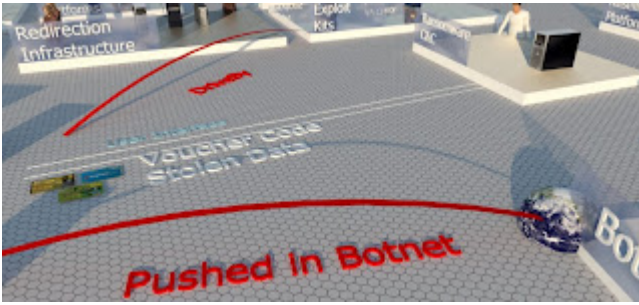
One more mailer

To figure out more about that you can read:

- Manual download

- the victims download the binary by themselves thinking it's something else (a "free" version of a paid game, an indispensable video plugin, a disinfection tool, etc...)

- Push in botnet



Tools : Task option of most Botnet C&C panel

In Upas:

Tasks								
Task	Details	Mode	Seat	Limit	Country	OS	Arch	Status
download and execute	...	Continuous	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ALL	ALL	Active

In Zemra :

Future / Done Tasks (5)

ID	Command	Start Time	Run Until	Selection	Bots
#2	Download (http://[redacted].exe)	03.09.2011 [redacted]	Finished	Global	100/100
#3	Download (http://[redacted].exe)	03.09.2011 [redacted]	Finished	Global	400/400
#5	Download (http://[redacted].exe)	03.09.2011 [redacted]	Finished	Global	1000/1000

In Andromeda :

Menu	#	Type	URL	Countries	Bot ID's	Build ID's	E/F/L*	Enabled	Actions
Bots	1	Update bot	http://[redacted]	*	*	*	#####/unim	True	[edit] [on/off] [delete]
Black list	* - Executed / Failure / Limit								
Tasks	[redacted]								
Service	[redacted]								

etc...

Advertising Platforms

The platform can be legit or not. Clicksor, Plugrush, Adfly are often being victims of these kind of badvertisers. Some platform are built for that dark job. Malekal pointed a fake platform [in this brilliant post](#) about MegoADS

These platforms are used or abused by bad guys to push advertisement that will drive the user to the redirection

infrastructure, often for instance fake porn website (see later).

200	HTTP	delivery.trafficbroker.com	/rd.php?http://datingysa.com/	2
200	HTTP	datingysa.com	/	3
200	HTTP	oskg843.viva-duct.de	/NV7bDHtd6LJ8cxihzX0j6K6zZFjMnX	4
200	HTTP	oskg843.viva-duct.de	/kmwlnyuwpsmpfcalddeacusd.jar	
200	HTTP	oskg843.viva-duct.de	/NV7bDHtd6LJ8cxihzX0j6K6zZFjMnX?s=1	
200	HTTP	wdzxt.ru	/555657555D886BA223AFEF635B46EF031D9CE463DD0E570A1C1B	

Annotations: "Urausy Call home" with arrow pointing to the 5th row; "5" in a circle next to the 5th row.

Malvert redirecting to "Sibhost" EK which is pushing Urausy

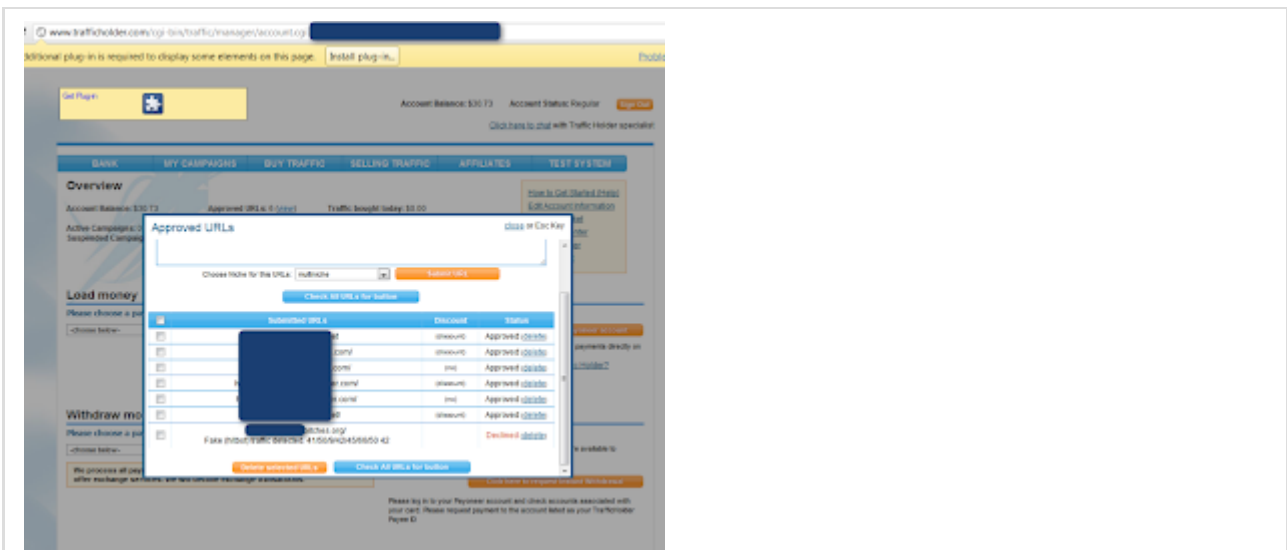
200	HTTP	delivery.trafficbroker.com	/rd.php?http://teen-fuck.com/	209
302	HTTP	teen-fuck.com	/	5
200	HTTP	haztalanhardad.bounceme.net	/JaOqWY?QbJdL=13	1 094
200	HTTP	haztalanhardad.bounceme.net	/kgr3r9BB9nX	17 608
200	HTTP	haztalanhardad.bounceme.net	/kgr3r9BB9nX	17 608
200	HTTP	haztalanhardad.bounceme.net	/PuqaJL?pQIO=12&sQJo=1251	137 216

Cbeplay.P pushed by Sweet Orange via TrafficBroker Malvert

200	HTTP	ads.hooqy.com	/newServing/banner_frame.php?nid=1&pid=249516&si...	3 341
200	HTTP	ads1.progametester.net	/tester_728x90.html	270
200	HTTP	serw.druselod.com	/4f587a91c39d3fb176f15845efe5c2a4	342
200	HTTP	chocolate.trustpulseinventory.com	/links/middle_granting.php	28 349
200	HTTP	chocolate.trustpulseinventory.com	/links/middle_granting.php?ugavrde=38020b0305&vbv...	18 715
200	HTTP	chocolate.trustpulseinventory.com	/links/middle_granting.php?rspvuiqv=38020b0305&xcix...	10 269

BH EK 2.0 landing after tilt on malvert

Tools:



Account on legit platform TrafficHolder

If you want to learn more about malvertising you should follow [Malekal's](#) Job.

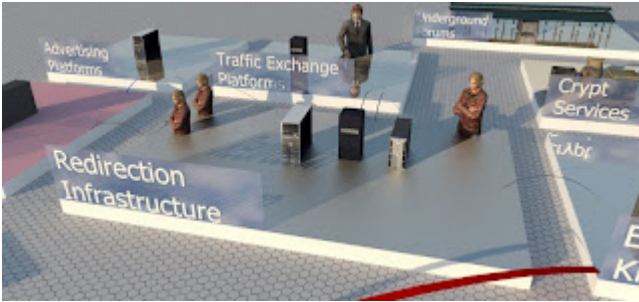
Some readings :

[Malvertising and Dynamic DNS: A Never Ending Story](#) - 2013-02-08 - Abhinav Singh - Symantec

[Finnish Website Attack via Rogue Ad](#) - 2012-12-05 - Sean - F-Secure

[Ads Integrity Alliance: Working together to fight bad ads](#) - 2012-06-14 - Google Official Blog
[Grandclick - a Clicksor Traffic Reseller...](#) - 2014-01-27

Redirection infrastructure :

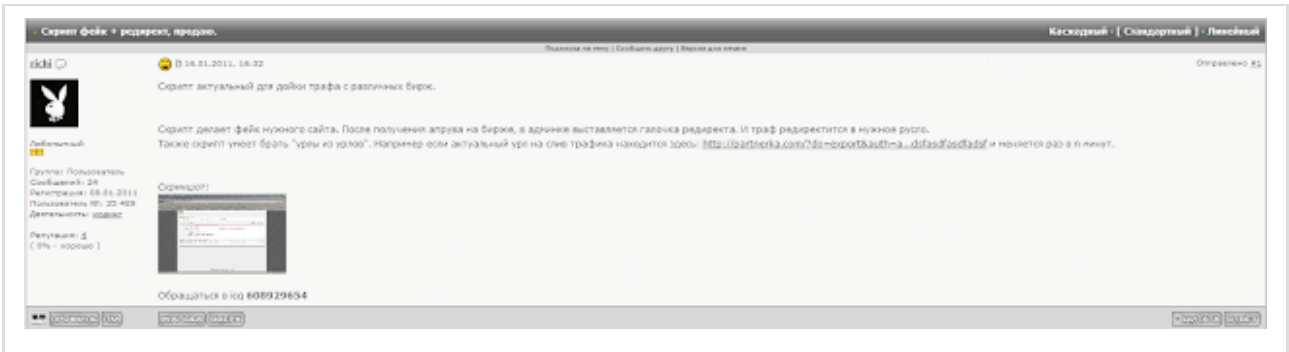


This block cover all the steps between the first redirection to the exploitation. This is the "Traffer Zone". Depending on how many actors are involved/how mature are the groups you can see a huge amount of hops.

The first step after malvertising is TDS or fake website with redirect js

Tools:

When modifying a saved legit page is not enough to build a fake site, there are dedicated tools to do this.



Initial advert for FakeMaker



Fakemaker (one fake website builder)

(more here : <http://kafeine.minus.com/lsInqkPcgjHSY>)

In some case the fake website is used to "prepare" the victim. For instance to increase conversion rate (people paying among infected people) on ransomware some traffer do not hesitate to redirect you to a fake Child porn website (but with real images). Victim shocked before being presented a pseudo law enforcement warning.

Dedicated TDS. Those TDS can be hidden behind forest of redirectors/reverse proxies.

They are redirecting traffic based on country/browser depending on the needs (client requests).

One TDS will often serve different exploit kits depending on the countries/sources of people hitting it.

Sutra,

The screenshot shows the SUTRA v3.6 Traffic Manager interface. At the top, there's a navigation bar with options like 'Схемы', 'Настройки', 'Uptime Bot', etc. Below that is a table with columns for rule names and numbers. The main section is titled 'Схема управления трафиком' (Traffic Management Scheme). It shows a list of rules with columns for 'URL назначения' (Destination URL), 'Сегодня' (Today), 'Страны' (Countries), 'Вес' (Weight), and '%'. Several rules are highlighted in red, indicating they are active or blocked. Blue arrows point from various text labels to specific elements in the interface, such as 'Country based redirection' pointing to the 'Страны' column, and 'SakuraThread' pointing to a rule. At the bottom, there are buttons for 'Создать новое правило', 'Редактировать', and 'Удалить'.

URL назначения	Сегодня	Страны	Вес	%
http://[redacted].php	0	DE	100	
используя frame	0	DE	100	16.7
используя frame	0	CA US AU	100	
remote://[redacted]forum/link.php?id=[redacted]	0	NO SE LU FI	100	16.7
используя frame	0	IR	100	16.7
remote://[redacted]api.php?id=[redacted]&pass=[redacted]	0	FR AT	100	
используя frame	0	DE	100	
remote://[redacted]/api.php?export&query=[redacted]	0	GB	100	
remote://[redacted]/api.php?export&query=[redacted]	0	CH NL	100	16.7
remote://[redacted]/api.php?export&query=[redacted]	0	US	100	16.7
remote://[redacted]/api.php?export&query=[redacted]	0	GB	100	16.7

1 TDS many Exploit Kits (at least 5)

For instance a French landing here will be redirected to the default page.

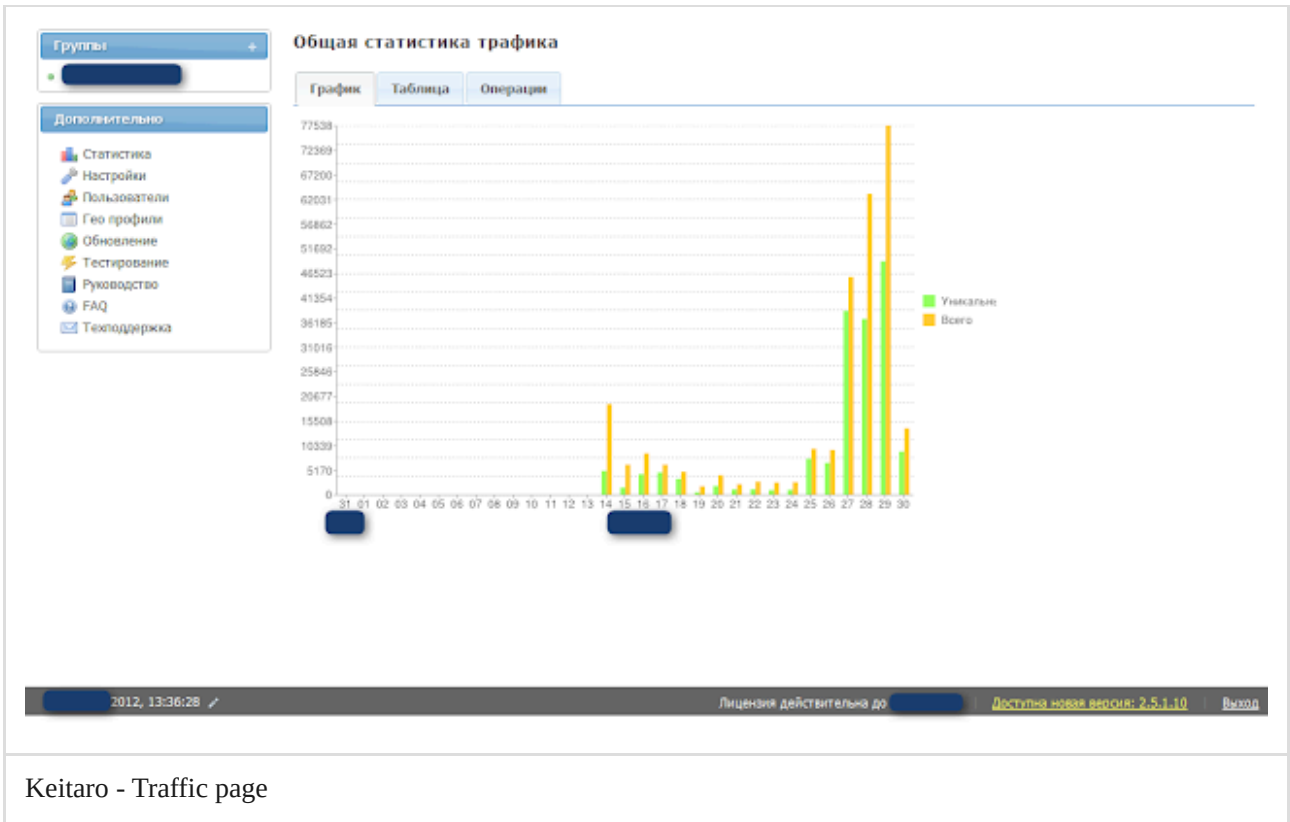
The screenshot shows a browser's developer tools. On the left, the 'Network' tab is open, showing a list of requests from '4.pronatka.com'. The selected request is for '/chrome/'. On the right, the 'Request Headers' tab is open, showing the following information:

```

Request Headers
GET /HTTP/1.1
Client
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Accept-Encoding: gzip,deflate,sdch
Accept-Language: fr-FR,fr;q=0.8,en-US;q=0.6,en;q=0.4
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.95 Safari/537.11
Transport
Connection: keep-alive
Host: 4.pronatka.com
    
```

Sutra driving IT Chrome user to a server faking Chrome Update (the server is in fact also a Blackhole Exploit Kit and Pony C&C redirector)

Keitaro :



Keitaro - Traffic page

SimpleTDS



sTDS 2.0 MOD JackSoft (a simple TDS modification) :

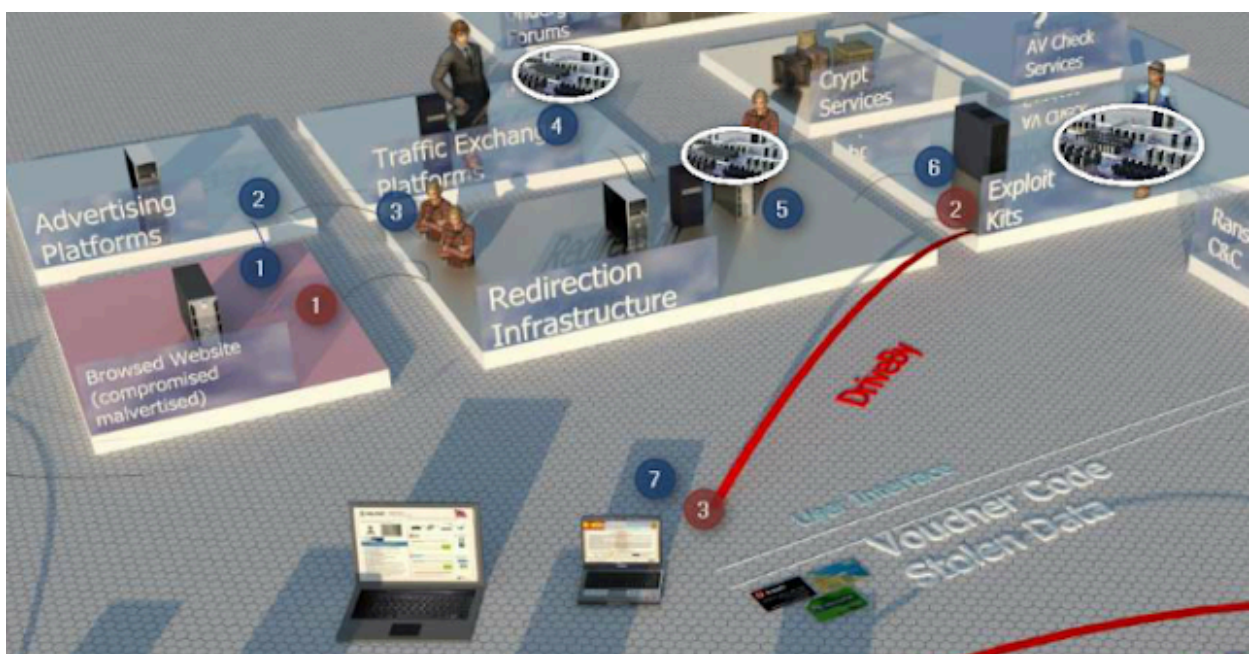


Other tool : Traffic Shop Analyzer the father of Ninja-TDS



Traffic Shop Analyzer v3.2 lite

Illustrating 2 paths :



2 path : a straight simple path (red) vs a more advanced one with multiple node and "poke a mole boards" (i'll add real life illustration at the end)

The RunForestRun campaign that was including DGA was a traffer side work.

The js were redirecting to a TDS who could then redirect to other TDS or to Exploit Kits (We saw at least Blackhole and Redkit).

Want to read more about TDS and Traffic exchange platform ?

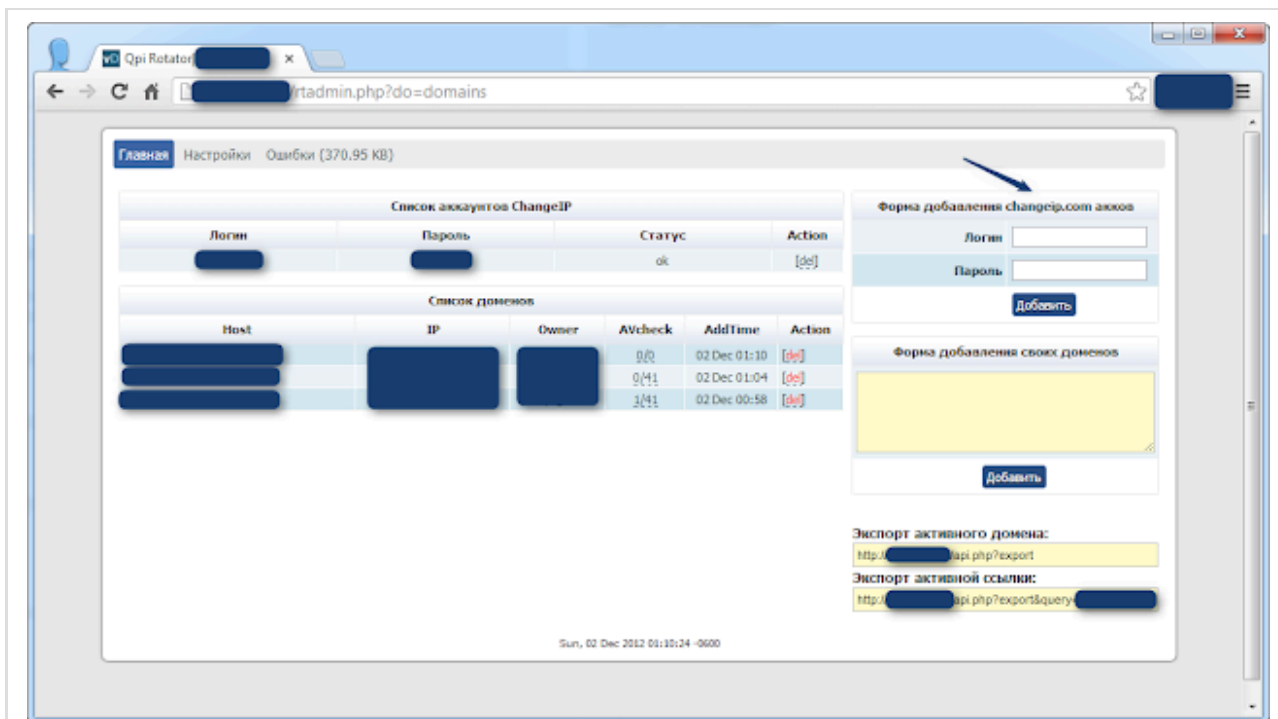
[Using Traffic Direction Systems to simplify fraud... and complicate investigations!](#) - Maxim Goncharov -

This was one of the addition to the version 2.0 of Blackhole Exploit Kit.

This is one of the big feature of Redkit (domain every hours, path every few seconds) , it has also been added to ProPack. The group behind the Cool EK pushing Reveton has also a backend system (I saw at least ten IPs) with an api to serve active hijacked domains to traffers

Tools :

Qpi Rotator



Qpi Rotator

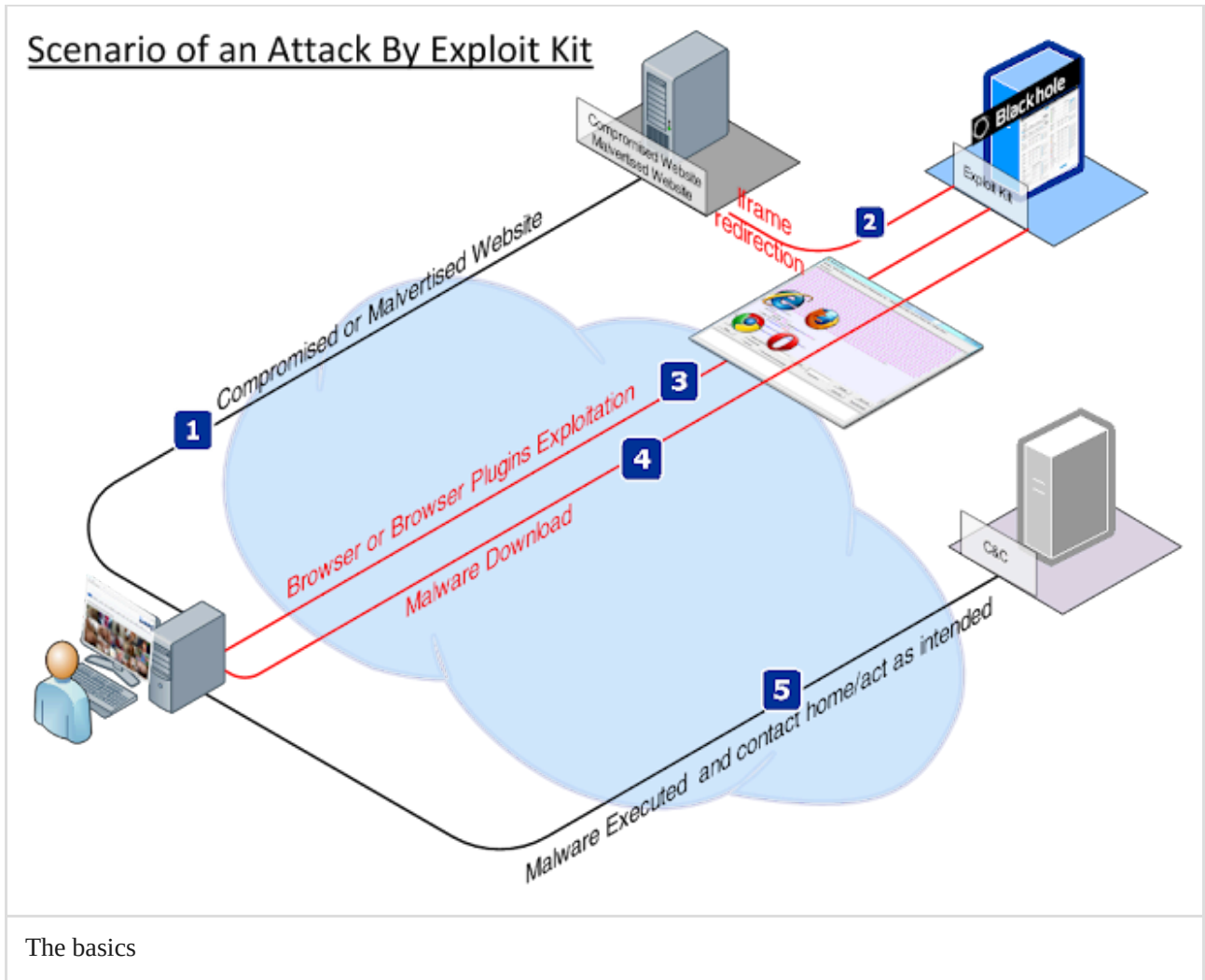


The screenshot displays the 'Основной настройки' (Main Settings) page of the Qpi Rotator. At the top, there are fields for 'Ротация' (Rotation) set to 'По расписанию' (By schedule) and 'Смена' (Shift). Below this is a field for 'IP регистрация домена для чернил' (IP domain registration for blacklists) with a 'Сохранить' (Save) button. The main section is titled 'Настройка BlackList' (BlackList Configuration) and includes a 'Ключ' (Key) field. Below this are several numeric input fields: 'Количество витков' (Number of turns) set to 2, and 'Максимальное кол-во доменов' (Maximum number of domains) set to 1. A large list of blacklist services follows, each with a checkbox: Adware IDB, Adware KBDB, Avast, AVG, AvastDB, CSE, Abound, Conficker by Malwarebytes, DNS BH, DrWeb Black List, Firefox and Chrome Black list, Iphish, IP Black list (SmartScreen Filter), Jigsaw, Kaspersky Black List, Malware Database, Malware Domain List, MalwarePatrol, MalwareURL, PhishBot (Phish Security), NetCrack, NOISI, Norton DNS, Opem, Parabolic (MalwareBlacklist), PhishTank, RUC Ignorant, SORBS, SpamCop, Spamhaus CSS, Spamhaus DBL, Spamhaus PBL, Spamhaus SB, Spamhaus XBL, Spamhaus ZEN, SpyEye Tracker (domain), SpyEye Tracker (ip), Tracit, Yandex, ZnuK Tracker (domain), and ZnuK Tracker (ip). A 'Сохранить' (Save) button is located at the bottom of this list. Below the list is a section for 'Домены чернил с которыми работать' (Domains to work with), which contains a single domain in a yellow box. A final 'Сохранить' (Save) button is at the bottom of the page. The footer shows the date 'Sun, 01 Dec 2012 16:17:44 -0800'.

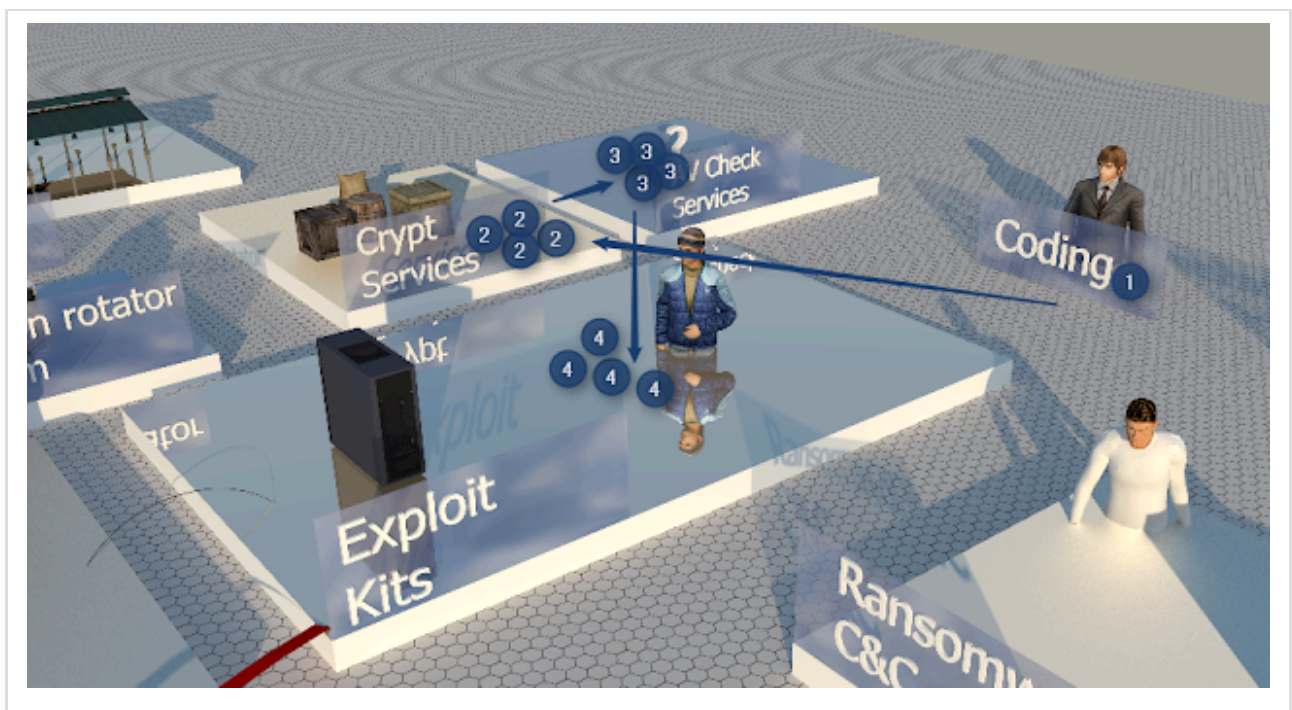
Qpi Rotator Settings allowing domain auto-rotation based blacklisted level

Exploit Kits

Won't spend a lot of time here too as most post in this blog are focused on this part.



A binary life



This to illustrate the Crypt and AV Check Services

Note that most tools on the path are able to check how clean is a binary, exploit pack or domain.

Cool EK check both binary and "sploit pack".

Spoit pack clean: 0/35 ()
File updated: 26.11.2012 13:57 (2/35) [check](#)

Redkit (old capture)

Актуальный IP: **178.162.170.59**
AV-тест IP: **0/32**
URL для обновления IP: **http://88.198.28.38/api.php?action=ip&aid=[redacted]&hash=[redacted]**

Актуальный домен: **pokurilpodelis.tk**
AV-тест домена: **0/32**
URL для обновления домена: **http://88.198.28.38/a?action=domain&aid=[redacted]&hash=[redacted]**

Средний пробив по системе за сегодня: **7.8%**
Средний пробив по системе за прошлый час: **7.7%**
AV-тест связки: **0/37**

Blackhole allow binary check through 2 services

SOFT VERSIONS	SECURITY	PREFERENCES	LOGOUT
----------------------	-----------------	--------------------	---------------

ANTIVIRUS CHECK

Antivirus service

ID Token

Check feature included in Citadel Botnet



In Upas kit :

Upas

The screenshot shows the Upas web interface. On the left is a sidebar menu with the following items: Map, Mots, Statistics, Tools, Logs, Tasks, Download logs, and Settings. The main content area contains a form with the following fields and buttons:

File	<input type="button" value="Choisissez un fichier"/> Aucun fichier choisi	<input type="button" value="Check File"/>
URL	<input type="text" value="http://"/>	<input type="button" value="Check Url"/>
Domain/IP/	<input type="text"/>	<input type="button" value="Check Blacklist/Filter"/>
Exploit Pack	<input type="text" value="http://"/>	<input type="button" value="Check Exploit Pack"/>

Sometimes the crypt provider allow you to add more features than just bypassing Antivirus :



Crypt4u. Note : Bypass UAC, Disable Firewall, etc.....2014-02-17

Underground Forums

This is a key point where all independent actors exchanges service offers and establish contacts. Reading this blog you'll see many screenshots of announcement or services offer. Forum are also often the place where conflict are solved in section often named "Black"/"Blacklist".

If you want an idea on the diversity of services take a look at this advert collection :

<http://kafeine.minus.com/mnrcD1JxAzu2U> (focused on : Traffing, Hosting, Crypting, Virtual Currency Echange, Ransomware affiliates etc...). These advert are found inside services (Forums, Scan, Crypt, Blackhole..etc)

So behind an infection there is a dark economy in turmoil with a lot of specialized individuals/groups. We can spend a lot of time discussing about each hat/job in the path. From the domain registration to the hosting, from the coding to the spreading but it was just an eye glance :)

Feel free to comment / send remarks kafeine at dontneedcoffee dot com.

Reading/resources :

[Malicious Software and its Underground Economy: Two Sides to Every Story](#) Lorenzo Cavallaro - Coursera (1st Session July 2013)

Source: <https://malware.dontneedcoffee.com/2012/12/eyeglanceru.html>