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

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.

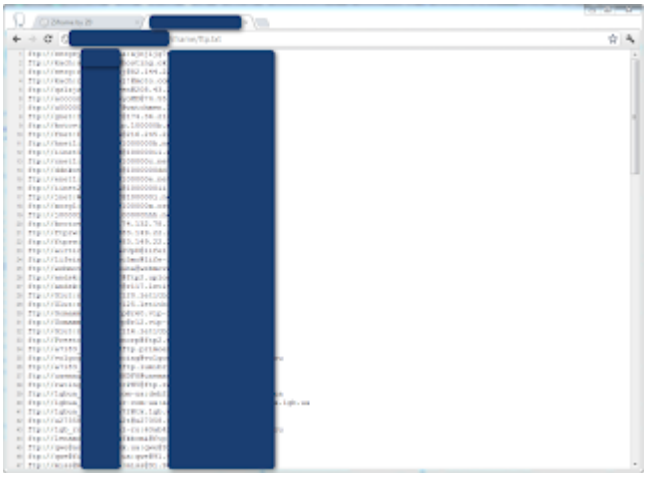
One other great illustration for both, was back in february/march 2012, the Sinowal/Torpig group hosting its custom Blackhole on infected nodes of its botnet and making it reachable via Fast-Flux && DGA (based on Twitter trends).

-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>

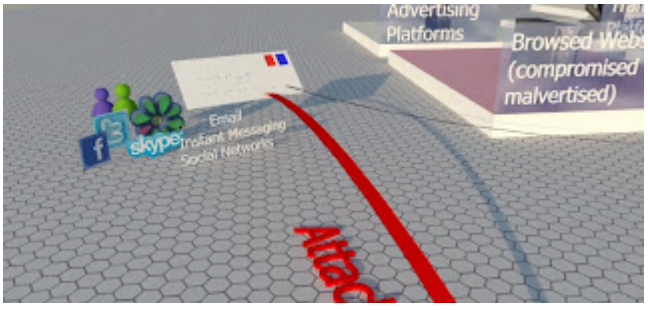
- Browsing Website :

- 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



- Malvertising : same via a malicious fake advert (see advertising platforms)

- Chat/mail



- link to compromised website or exploit kit
- binary as attachement, or document with link to the exploit kit

(Matsnu/Rannoh mainly spread by mail, and skype was used to redirect users to BH EK 2.0 then Ransomware)

The tools :

A Nacha/Facebook themed spam Tool

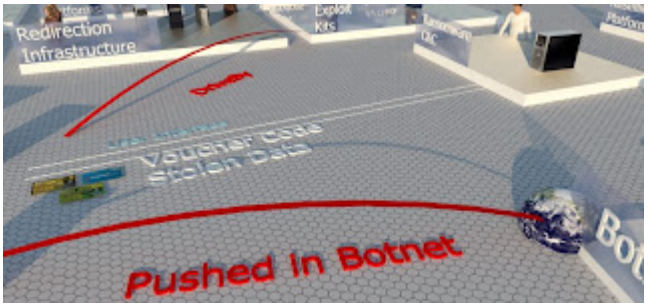
One more mailer

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...)

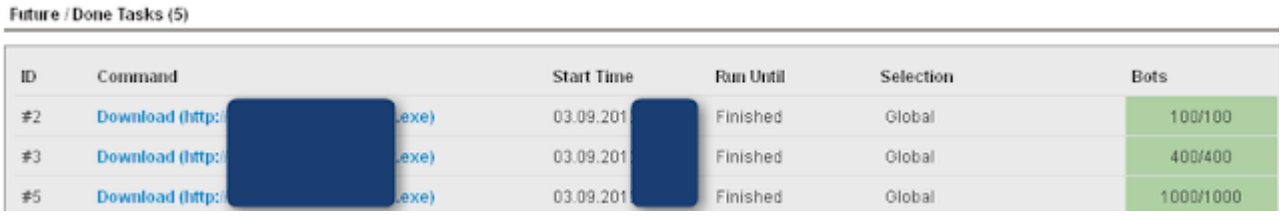
- Push in botnet



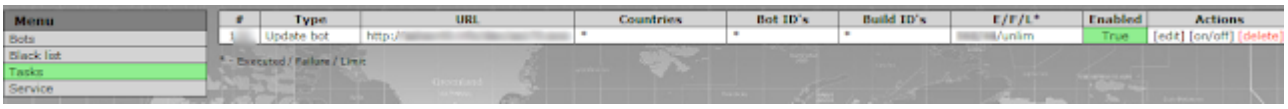
Tools : Task option of most Botnet C&C panel

In Upas:

In Zemra :



In Andromeda :



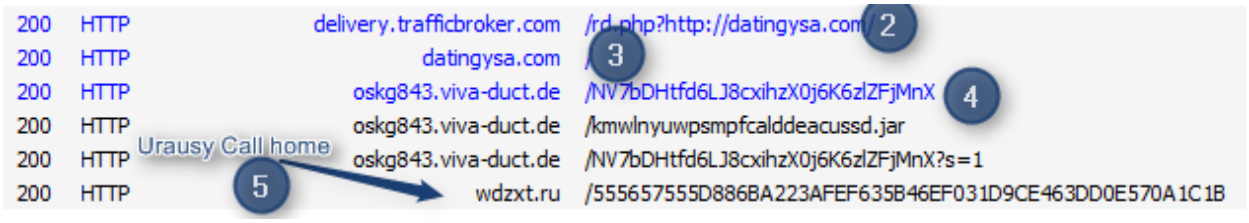
etc...

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).



Malvert redirecting to "Sibhost" EK which is pushing Urausy

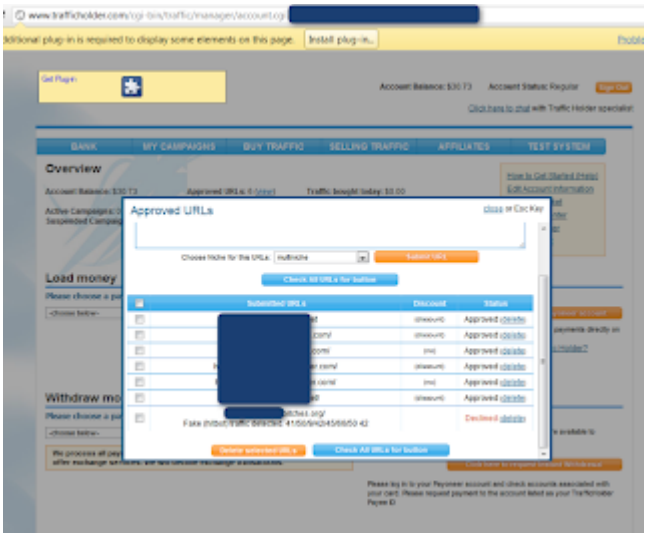
200	HTTP	delivery.trafficbroker.com	/rd.php?http://teen-fuck.com/	209
302	HTTP	teen-fuck.com	/	5
200	HTTP	haztalanhardad.bounceme.net	/JaOqWY?QbJdL=13	1 094
200	HTTP	haztalanhardad.bounceme.net	/kgr3r9BB9nX	17 608
200	HTTP	haztalanhardad.bounceme.net	/kgr3r9BB9nX	17 608
200	HTTP	haztalanhardad.bounceme.net	/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.drunselod.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?rspvuikv=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.

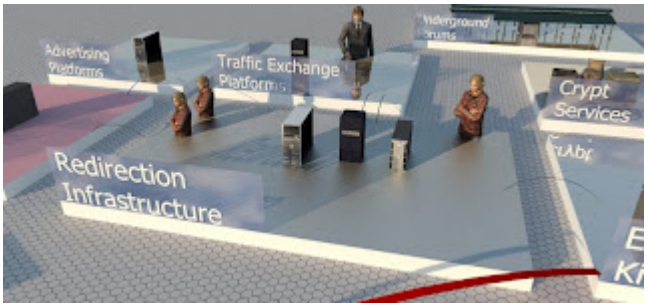
Some readings :

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
Grandclix - a Clicksor Traffic Reseller... - 2014-01-27

Redirection infrastructure :

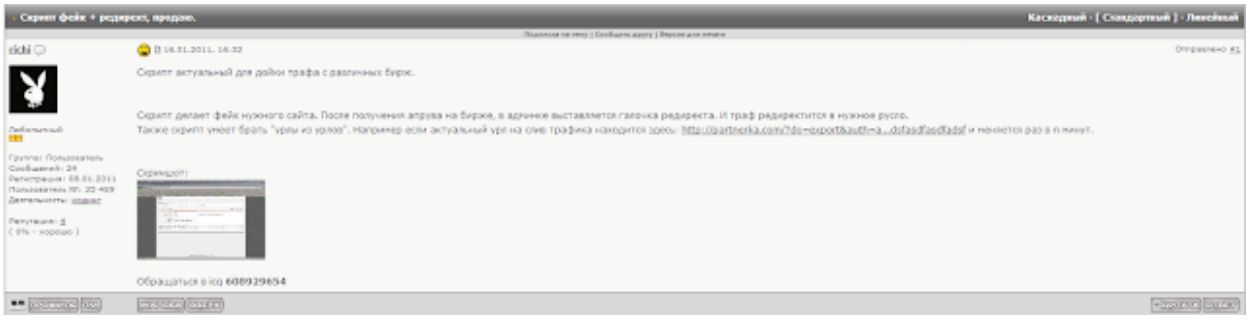


This block cover all the steps between the first redirection to the exploitation. This is the "Traffer Zone". Depending on how many actors are involved/how mature are the groups you can see a huge amount of hops.

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

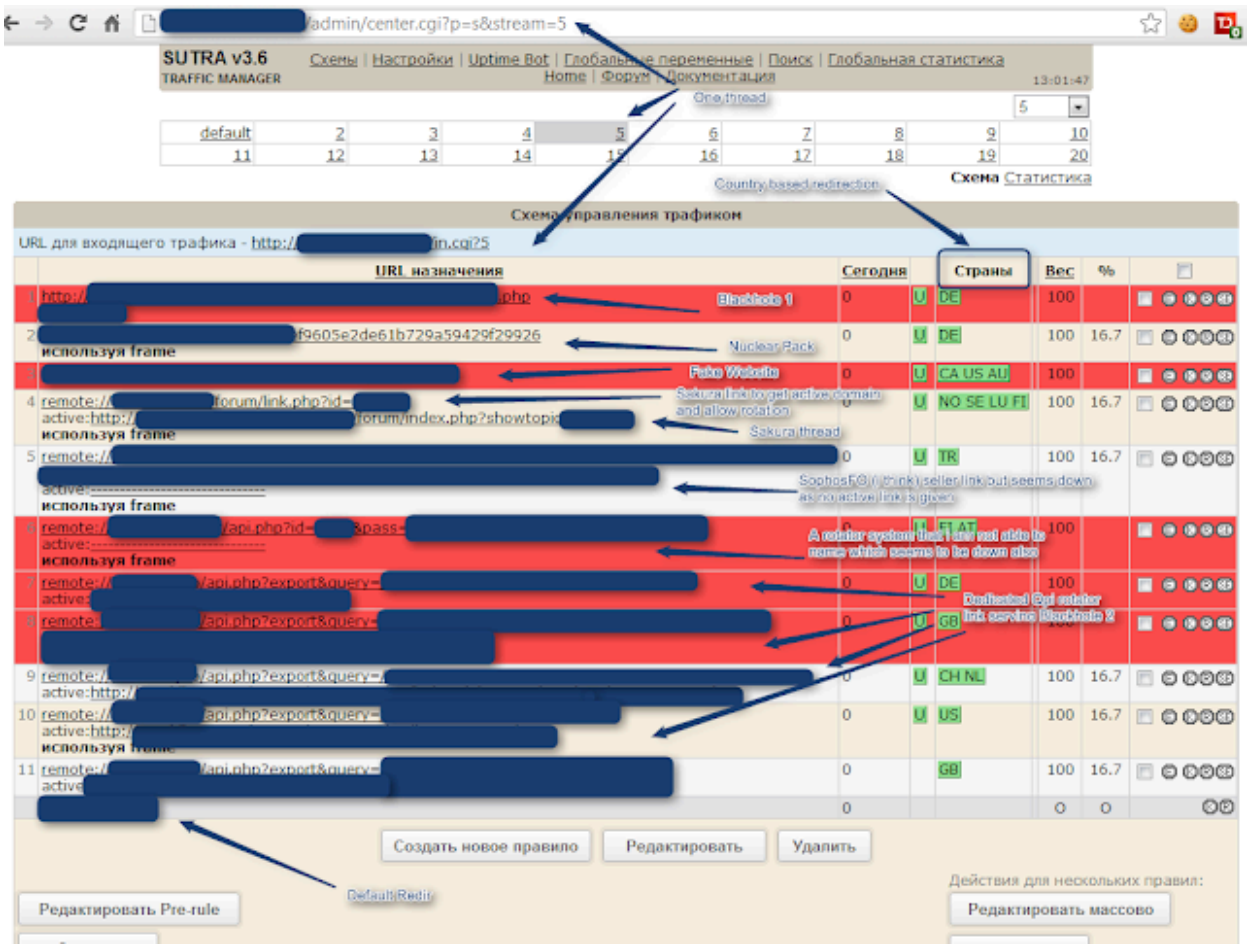
Fakemaker (one fake website builder)

(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.

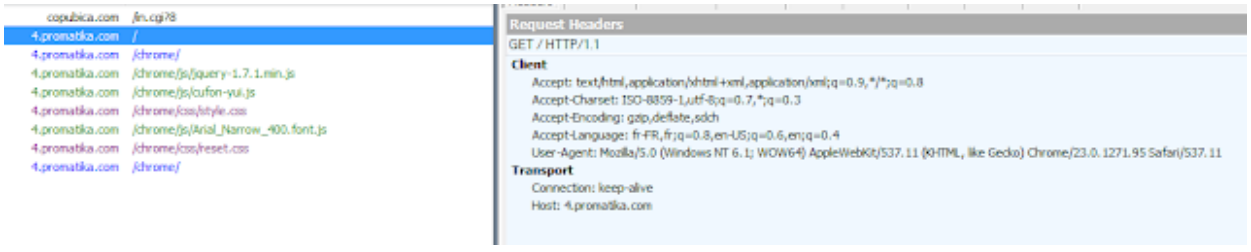
Dedicated TDS. Those TDS can be hidden behind forest of redirectors/reverse proxies.
They are redirecting traffic based on country/browser depending on the needs (client requests).
One TDS will often serve different exploit kits depending on the countries/sources of people hitting it.

Sutra,



1 TDS many Exploit Kits (at least 5)

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



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

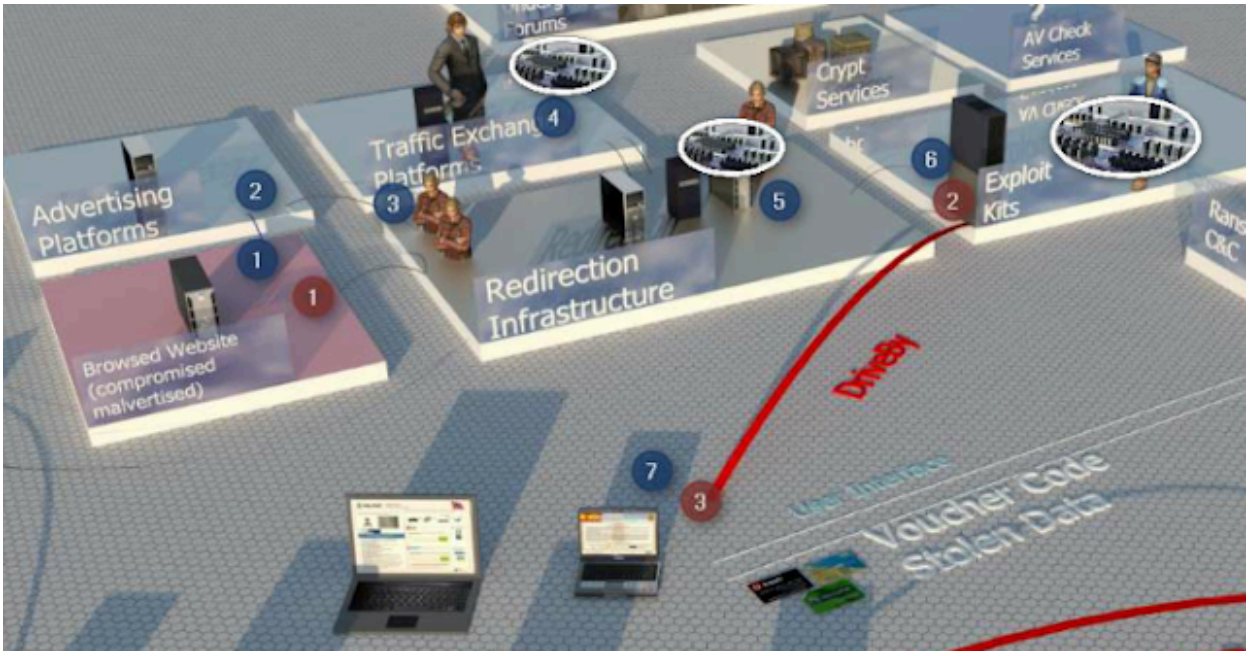
SimpleTDS

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)

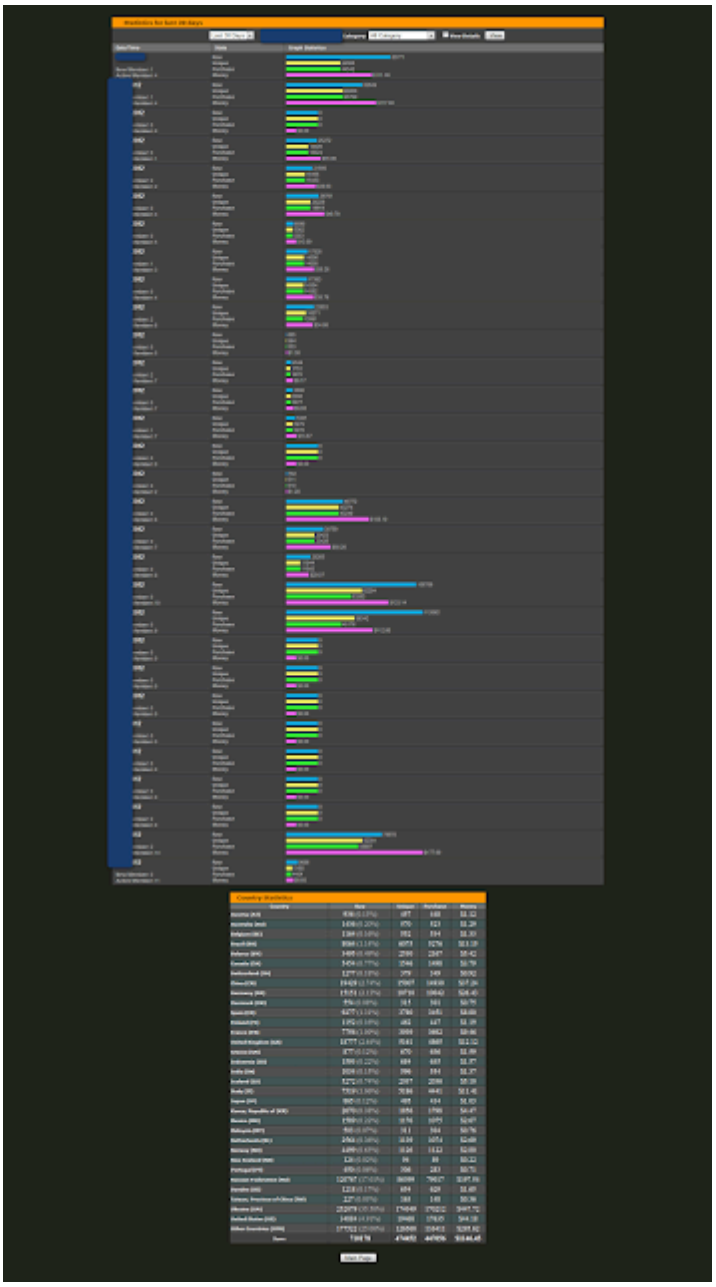
The RunForestRun campaign that was including DGA was a traffer side work.
The js were redirecting to a TDS who could then redirect to other TDS or to Exploit Kits (We saw at least Blackhole and Redkit).

Want to read more about TDS and Traffic exchange platform ?
Using Traffic Direction Systems to simplify fraud... and complicate investigations! - Maxim Goncharov -

Trendmicro for VB2011

Traffic Exchange Platforms

Won't spend a lot of time here. These are places where traffer/EK operators can register and can sell/buy traffic. There are tools to build this kind of platform



Small Traffic Exchange Platform (based on Web-Traffic Shop) stats

Domain rotator sytem

Tools/utility that cover the need for fast/mass domain rotation.

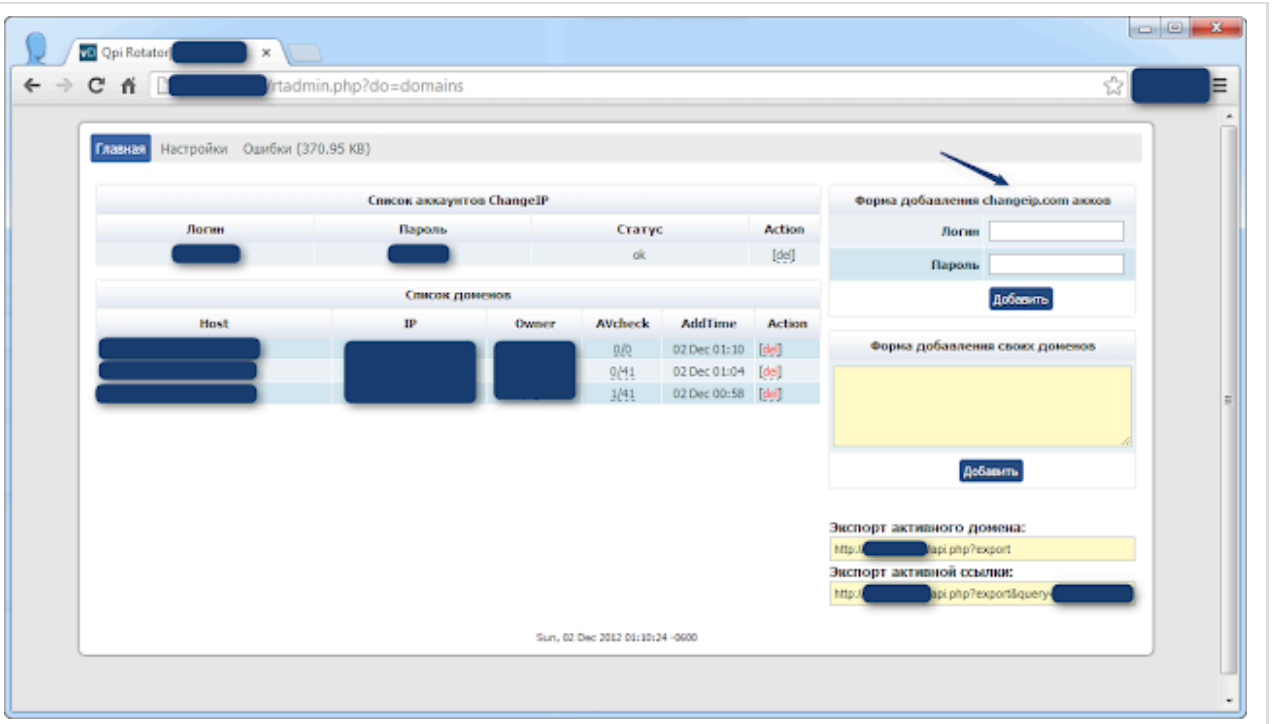
Most exploit kits have built-in features for this.

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

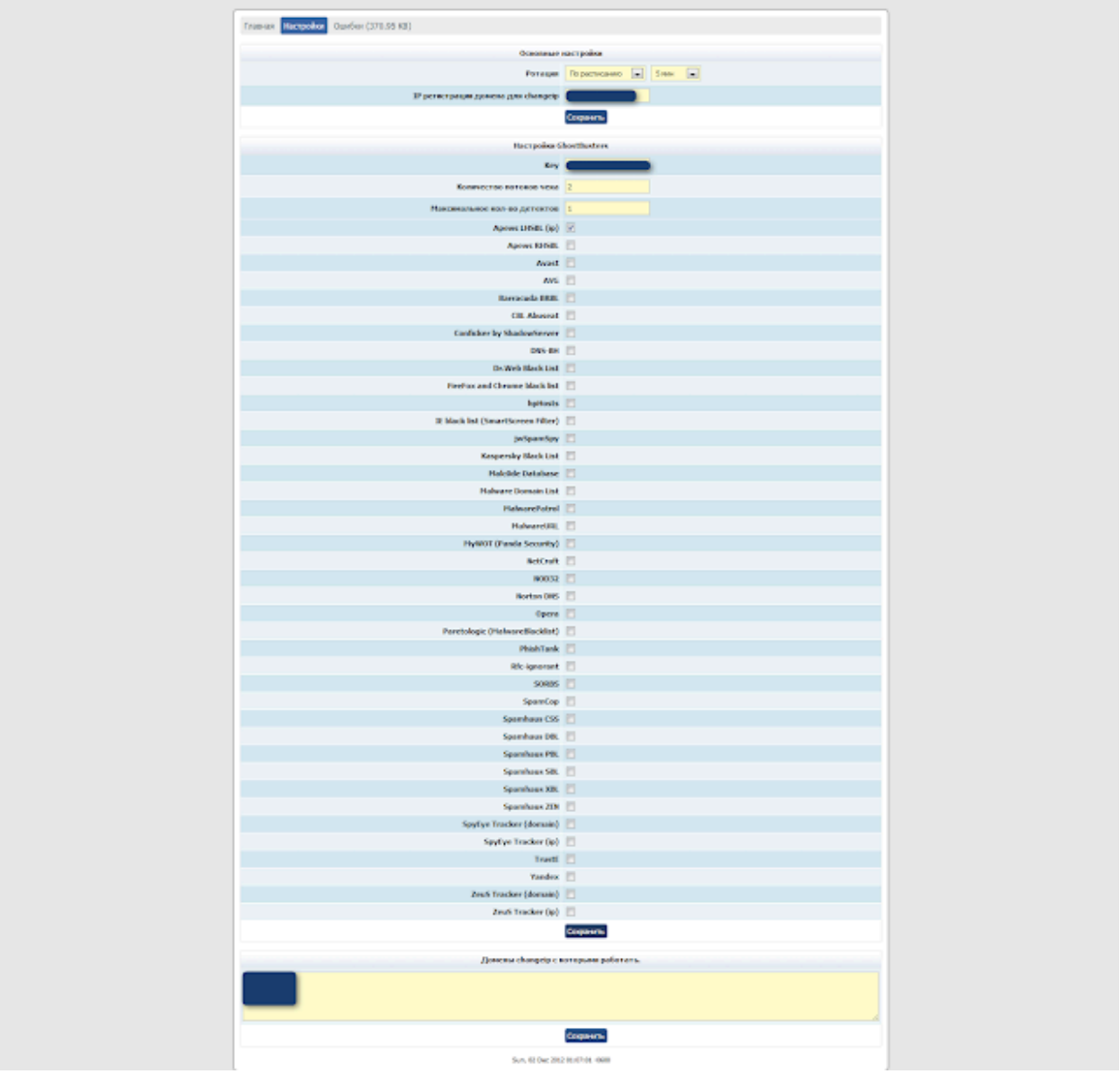
This is one of the big feature of Redkit (domain every hours, path every few seconds) , it has also been added to ProPack. The group behind the Cool EK pushing Reveton has also a backend system (I saw at least ten IPs) with an api to serve active hijacked domains to traffers

Tools :

Qpi Rotator



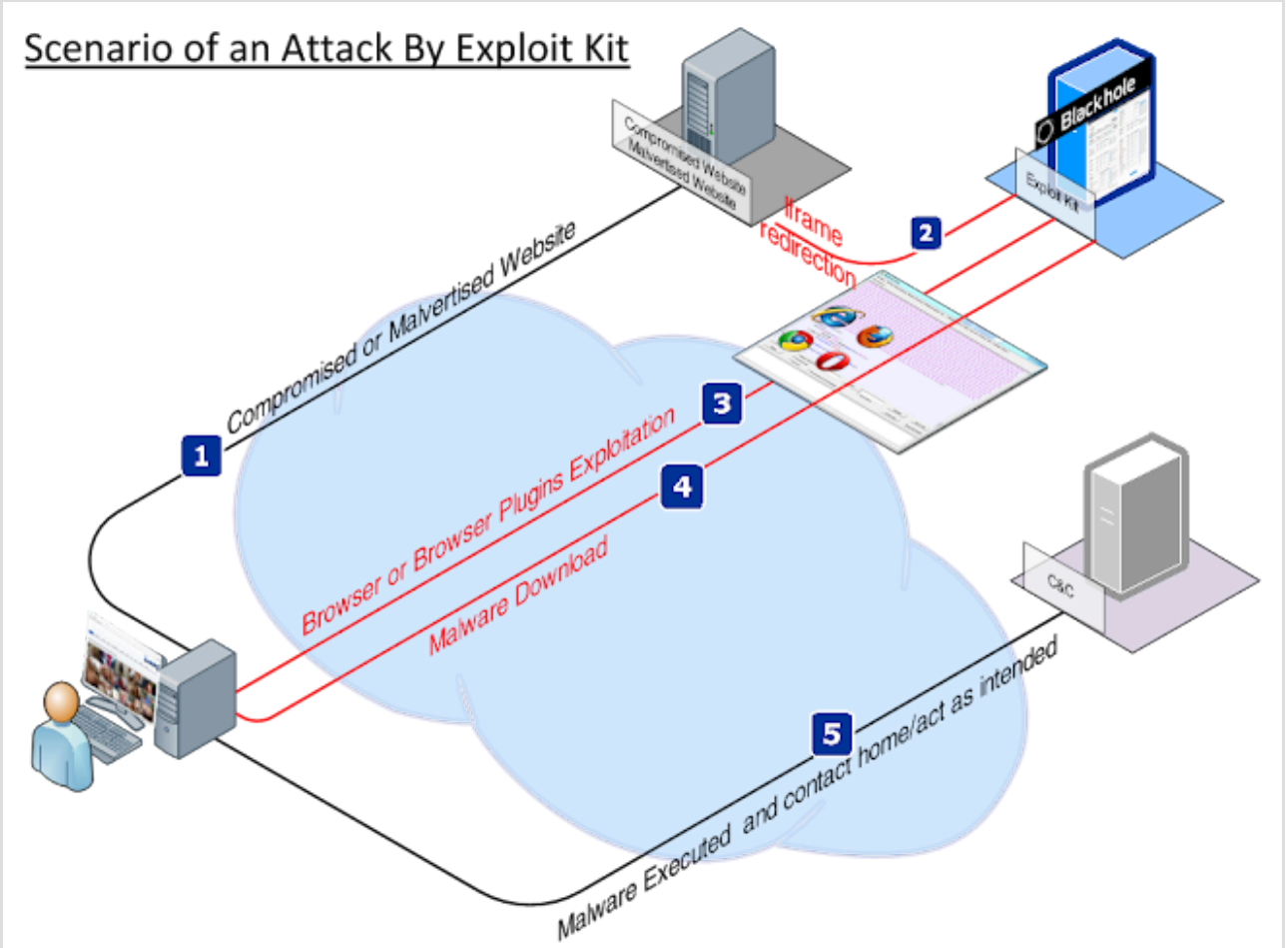
Qpi Rotator



Qpi Rotator Settings allowing domain auto-rotation based blacklisted level

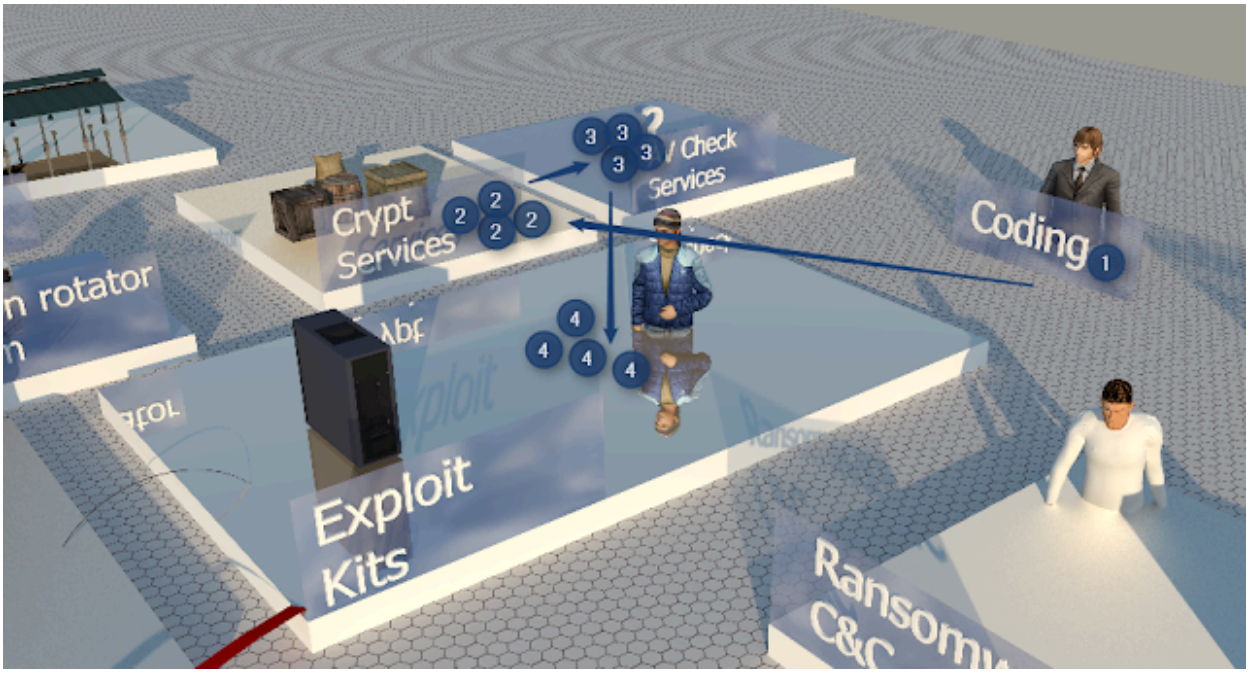
Exploit Kits

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



The basics

A binary life

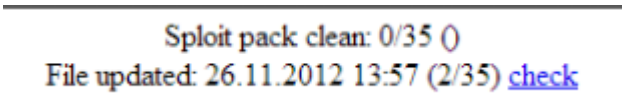


This to illustrate the Crypt and AV Check Services

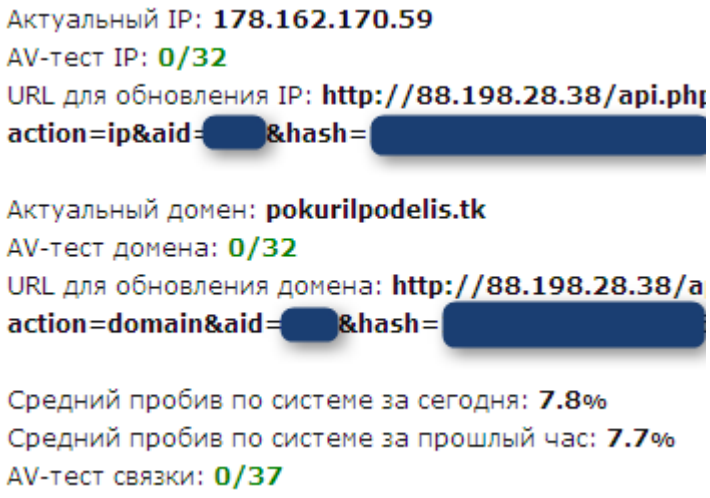
.

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

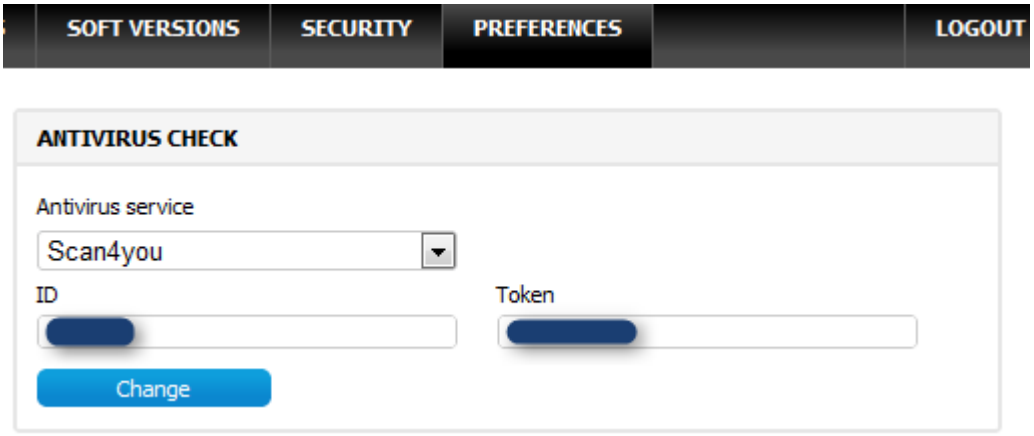
Cool EK check both binary and "sploit pack".



Redkit (old capture)

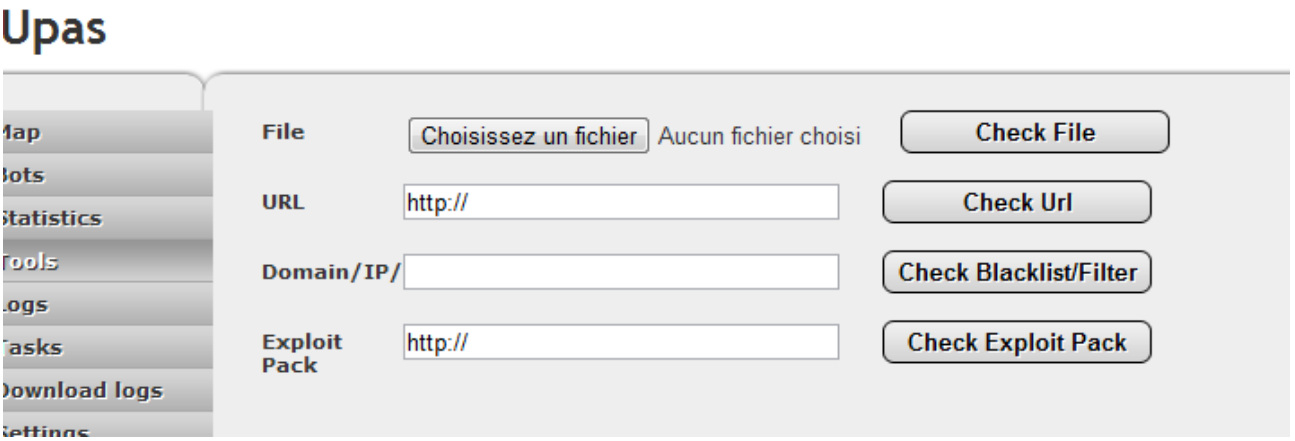


Blackhole allow binary check through 2 services



Check feature included in Citadel Botnet

In Upas kit :



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)
