White Paper

McAfee®
An Intel Company

Operation High Roller Revisited

Ryan Sherstobitoff, McAfee® Labs

Table of Contents

Executive Summary

In our report *Dissecting Operation High Roller*, a joint publication from McAfee Labs and Guardian Analytics, we examined a global fraud ring's efforts to steal money from wealthy businesses and individuals.[1] The complexities of Operation High Roller left many questions unanswered as to the origins and actors responsible for attempting millions of fraudulent transactions. Now we want to revisit the details at a much deeper level to develop a clearer picture of the hidden details and to further map the campaigns and their connections.

These campaigns, like many other attempts at fraud, originated in Eastern Europe, so it is not surprising that the actors had an extensive history of Zeus and SpyEye activity. These fraudsters planned these campaigns for some time and actively participated in other criminal activity long before Operation High Roller was conceived. We have found evidence that ties these actors to early automated transfer systems built to target users. These initial efforts were likely their test ground to gain knowledge of financial systems and their various fraud prevention practices.

These groups have evolved to using more sophisticated techniques, and many of them actively used automated transfer system code against numerous European banks in late 2011.

This analysis attempts to map the domain infrastructure used during Operation High Roller to determine its origins. As with the previous report, we have informed law enforcement of our findings.

Automated Transaction Server

The domain recheckservingbizpacktool.net began its life in Kemerovo on February 7, 2012, and was used as an automated transaction server in Operation High Roller campaigns in March and April. Throughout its two-month lifespan, it moved among multiple hosting providers.

One of these was IP address 70.102.175.218, located in Scottsdale, Arizona, which hosted Ice IX malware previous to the Operation High Roller campaigns.

Event Date	Action	Pre-Action IP	Post-Action IP
2012-02-07	New	-none-	46.180.70.139
2012-02-19	Change	46.180.70.139	209.141.60.202
2012-03-02	Change	209.141.60.202	70.102.175.218
2012-03-14	Change	70.102.175.218	187.62.14.140
2012-03-26	Change	187.62.14.140	37.59.68.20
2012-04-07	Not Resolvable	37.59.68.20	-none-

Figure 1. Hosting history for recheckservingbizpacktool.net. On March 2, it resided in Scottsdale, Arizona. (All IP address tables courtesy of DomainTools.)

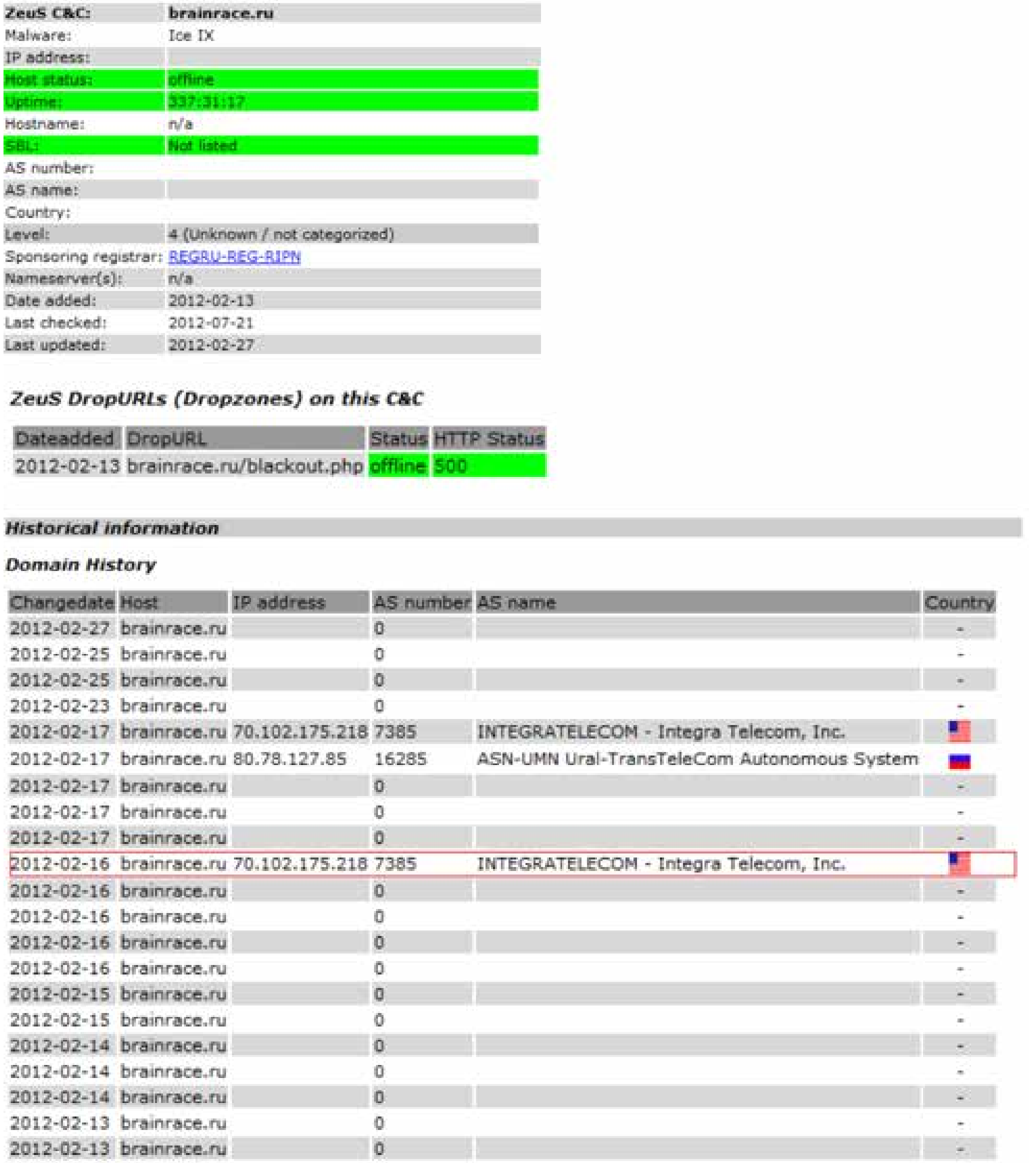
Further investigation into this server in Arizona revealed that it belongs to a legitimate company, Costello-Childs Contemporary of Scottsdale. Our data indicates that the fraudsters likely gained access and hosted the transaction server there for 12 days before moving the domain to a server in Brazil.

```
network:Auth-Area:70.102.0.0/15
network:Class-Name:network
network:ID:70-102-175-216/30-NET
network:Network-Name:70-102-175-216/30-NET
network:IP-Network:70.102.175.216/30
network:Org-Name;I:COSTELLO-CHILDS CONTEMPORARY FINE ARTS RESOURCES
network:Street-Address:2724 N  66TH ST
network:City:SCOTTSDALE
network:State:AZ
network:Postal-Code:85257
network:Country-Code:US
network:Admin-Contact;I:ITIA-ARIN
network:Tech-Contact;I:ITIA-ARIN
network:Updated:2009-01-13
network:Updated-By:bcrawford@integra.net
```

Ice IX and Zeus

Because the automated attacks from the Arizona server were using primarily SpyEye, let’s take a look at the interesting connection to Zeus and Ice IX.

The Arizona server hosted an Ice IX malware drop zone and control server with the domain brainrace.ru. The Ice IX malware was active February 13. The Operation High Roller transaction server did not move to this IP address until March 2. The MD5 hash of the Ice IX malware used in this instance was E661FF3D8AE16AB40B8638B8A74FFF2B and is classified by McAfee as PWS-Zbot.gen.ru.



ZeuS C&C:	**brainrace.ru**
Malware:	Ice IX
IP address:	
Host status:	offline
Uptime:	337:31:17
Hostname:	n/a
SBL:	Not listed
AS number:	
AS name:	
Country:	
Level:	4 (Unknown / not categorized)
Sponsoring registrar:	REGRU-REG-RIPN
Nameserver(s):	n/a
Date added:	2012-02-13
Last checked:	2012-07-21
Last updated:	2012-02-27

ZeuS DropURLs (Dropzones) on this C&C

Dateadded	DropURL	Status	HTTP Status
2012-02-13	brainrace.ru/blackout.php	offline	500

Historical information

Domain History

Changedate	Host	IP address	AS number	AS name	Country
2012-02-27	brainrace.ru		0		-
2012-02-25	brainrace.ru		0		-
2012-02-25	brainrace.ru		0		-
2012-02-23	brainrace.ru		0		-
2012-02-17	brainrace.ru	70.102.175.218	7385	INTEGRATELECOM - Integra Telecom, Inc.	🇺🇸
2012-02-17	brainrace.ru	80.78.127.85	16285	ASN-UMN Ural-TransTeleCom Autonomous System	🇷🇺
2012-02-17	brainrace.ru		0		-
2012-02-17	brainrace.ru		0		-
2012-02-17	brainrace.ru		0		-
2012-02-16	brainrace.ru	70.102.175.218	7385	INTEGRATELECOM - Integra Telecom, Inc.	🇺🇸
2012-02-16	brainrace.ru		0		-
2012-02-16	brainrace.ru		0		-
2012-02-16	brainrace.ru		0		-
2012-02-16	brainrace.ru		0		-
2012-02-15	brainrace.ru		0		-
2012-02-15	brainrace.ru		0		-
2012-02-14	brainrace.ru		0		-
2012-02-14	brainrace.ru		0		-
2012-02-14	brainrace.ru		0		-
2012-02-13	brainrace.ru		0		-
2012-02-13	brainrace.ru		0		-

Figure 2. The first time this malware was seen was approximately 1:16 am UTC on February 15. The malware communicated with http://brainrace.ru/leader.php.

The San Jose Server

As we investigated further, the domain brainrace.ru also had a connection to a server in San Jose, California, at IP address 209.141.60.202, according to DNS records dating back 150 days. The name server ns1.forcraftgoods.com contained "A records" pointing the brainrace.ru domain to several IP addresses, including that of the San Jose server.

These connections were the first indication that this was a "fast-flux" botnet with many levels of complication. The fast-flux technique allows malware to hide itself in an array of compromised servers and increase its lifespan.

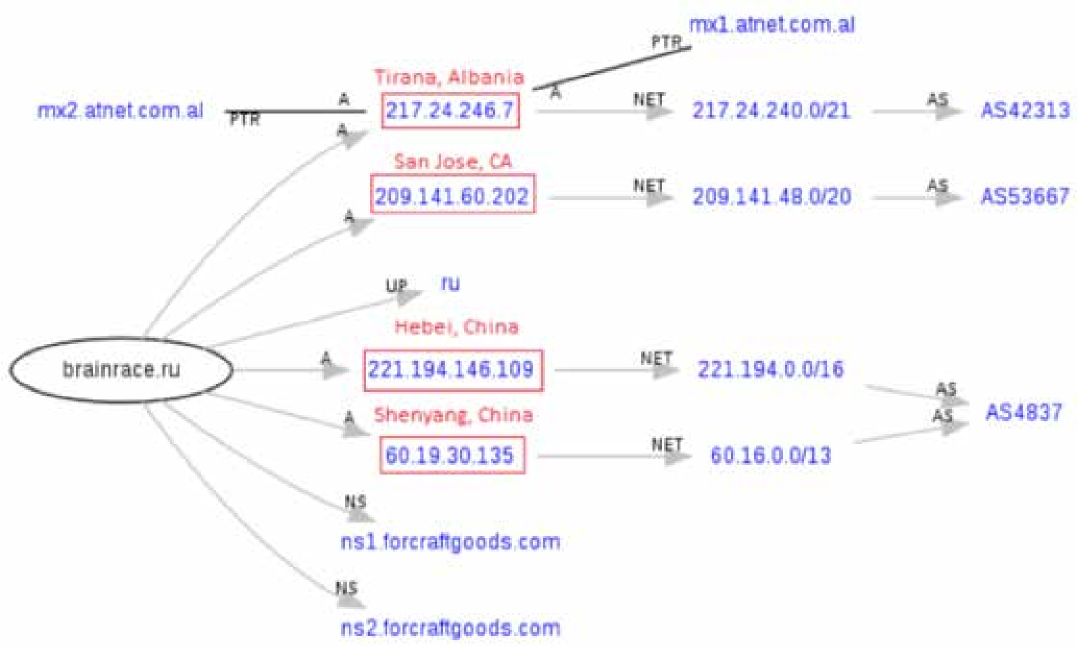
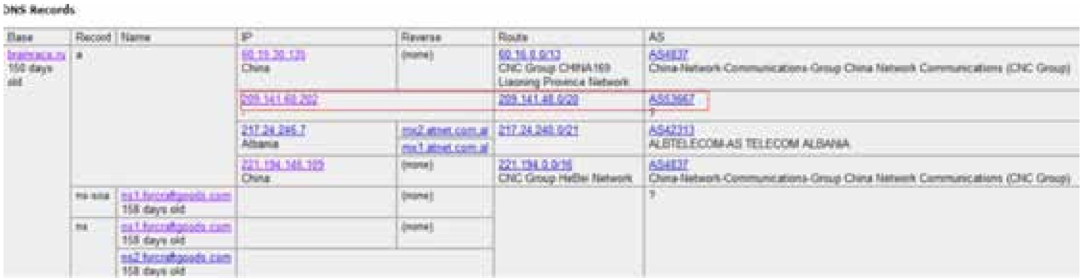


Figure 3. Domain mapping for 209.141.60.202. (All DNS charts and DNS record tables courtesy of Robtex.)



DNS Records

Base	Record	Name	IP	Reverse	Route	AS
brainrace.ru 150 days old	a		60.19.30.135 China	(none)	60.16.0.0/13 CNC Group CHINA169 Liaoning Province Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
			209.141.60.202 ?		209.141.48.0/20	AS53667 ?
			217.24.246.7 Albania	mx2.atnet.com.al mx1.atnet.com.al	217.24.240.0/21	AS42313 ALBTELECOM-AS TELECOM ALBANIA
			221.194.146.109 China	(none)	221.194.0.0/16 CNC Group HeBei Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
	ns-soa	ns1.forcraftgoods.com 158 days old		(none)		?
	ns	ns1.forcraftgoods.com 158 days old		(none)		
		ns2.forcraftgoods.com 158 days old				

Figure 4. Historical DNS records for brainrace.ru.

As we expanded our investigation into the San Jose server, we found that several domains at one point were directed to its IP address, 209.141.60.202. Five of these domains are used in Zeus activity and are documented below.

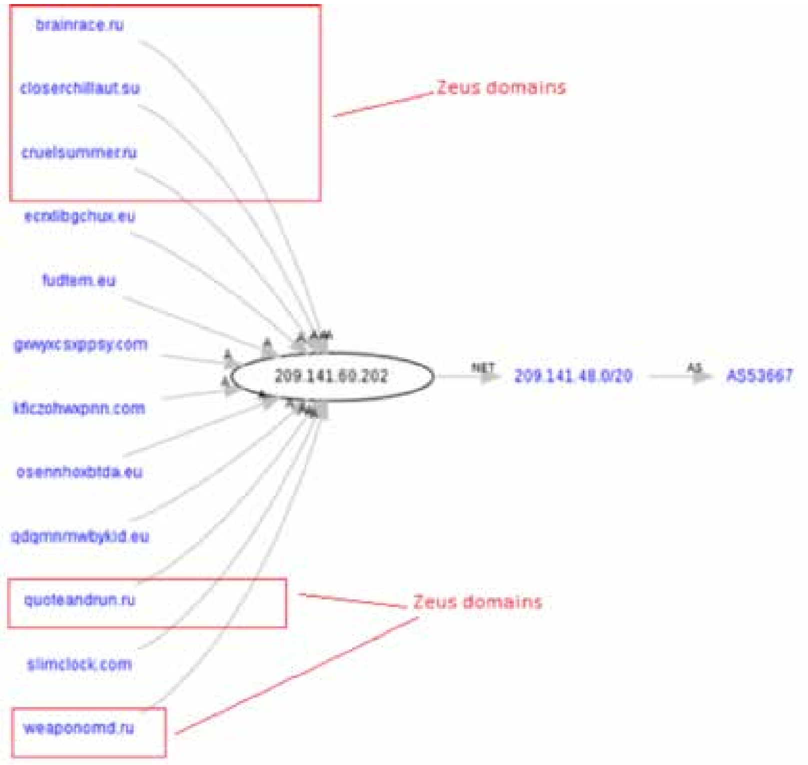
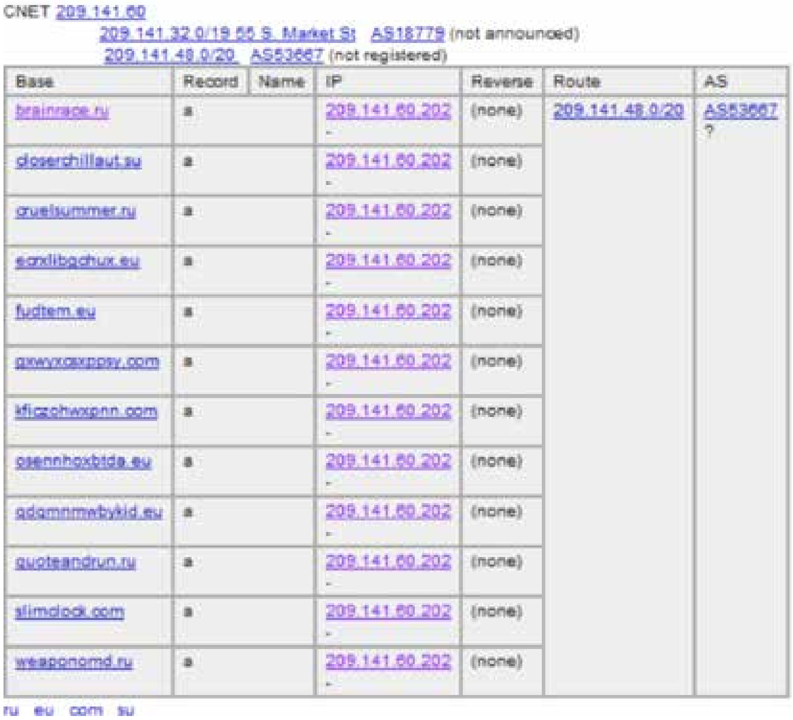


Figure 5. Domain mapping for 209.141.60.202, located in San Jose.



CNET 209.141.60
209.141.32.0/19 55 S. Market St AS18779 (not announced)
209.141.48.0/20 AS53667 (not registered)

Base	Record	Name	IP	Reverse	Route	AS
brainrace.ru	a		209.141.60.202 -	(none)	209.141.48.0/20	AS53667 ?
closerchillaut.su	a		209.141.60.202 -	(none)		
cruelsummer.ru	a		209.141.60.202 -	(none)		
ecnxlibgchux.eu	a		209.141.60.202 -	(none)		
fudtem.eu	a		209.141.60.202 -	(none)		
gxwyxcsxppsy.com	a		209.141.60.202 -	(none)		
kficzohwxpnn.com	a		209.141.60.202 -	(none)		
osennhoxbtda.eu	a		209.141.60.202 -	(none)		
qdqmnmwbykid.eu	a		209.141.60.202 -	(none)		
quoteandrun.ru	a		209.141.60.202 -	(none)		
slimclock.com	a		209.141.60.202 -	(none)		
weaponomd.ru	a		209.141.60.202 -	(none)		

ru eu com su

Figure 6. Historical DNS records for 209.141.60.202.

We discovered 11 additional domains pointing to this IP address; some hosted Zeus-related activity.

All of the domains documented below have a common connection with servers in China.

- **Closerchillaut.su**
  - Added March 20, 2012
  - Hosted a Zeus drop zone at the following URL:
    - closerchillaut.su/deg/dfyhih.php

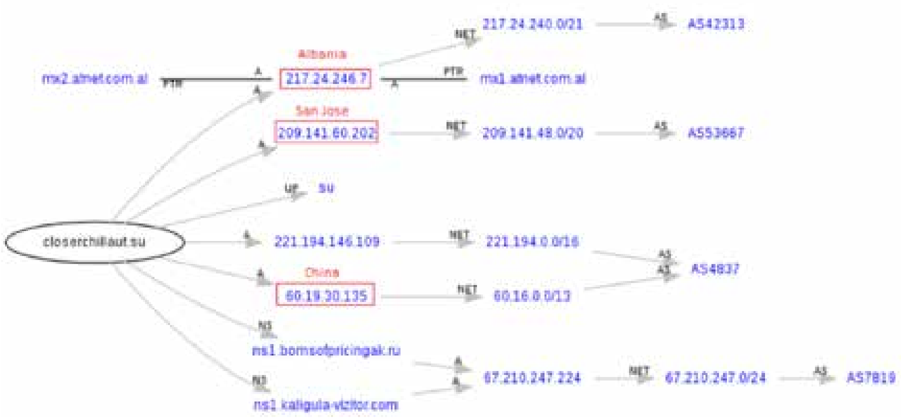
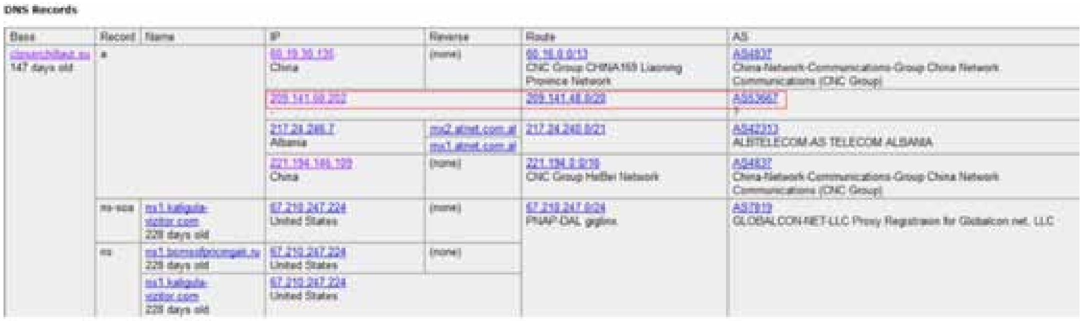


Figure 7. Domain mapping for closerchillaut.su.


DNS Records

Base	Record	Name	IP	Reverse	Route	AS
closerchillaut.su 147 days old	a		60.19.30.135 China	(none)	60.16.0.0/13 CNC Group CHINA169 Liaoning Province Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
			209.141.60.202 -		209.141.48.0/20	AS53667 ?
			217.24.246.7 Albania	mx2.atnet.com.al mx1.atnet.com.al	217.24.240.0/21	AS42313 ALBTELECOM-AS TELECOM ALBANIA
			221.194.146.109 China	(none)	221.194.0.0/16 CNC Group HeBei Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
	ns-soa	ns1.kaligula-vizitor.com 228 days old	67.210.247.224 United States	(none)	67.210.247.0/24 PNAP-DAL giglinx	AS7819 GLOBALCON-NET-LLC Proxy Registration for Globalcon.net, LLC
	ns	ns1.bomsofpricingak.ru 228 days old	67.210.247.224 United States	(none)		
		ns1.kaligula-vizitor.com 228 days old	67.210.247.224 United States			

Figure 8. Historical DNS records for closerchillaut.su.

- **Cruelsummer.ru**
  - Added February 13, 2012
  - Hosted PWS-Zbot.gen.ru with the following MD5s:
    - f387c03c8099d007a25d64df1abbc6f9
    - 0c4cf45b512432aaeb0e0a52697f1e8a
    - 8356fb8f0e9b7d8b6456204ea59f0506
    - fd1819909dd1a9d64c0b58fb90b90636

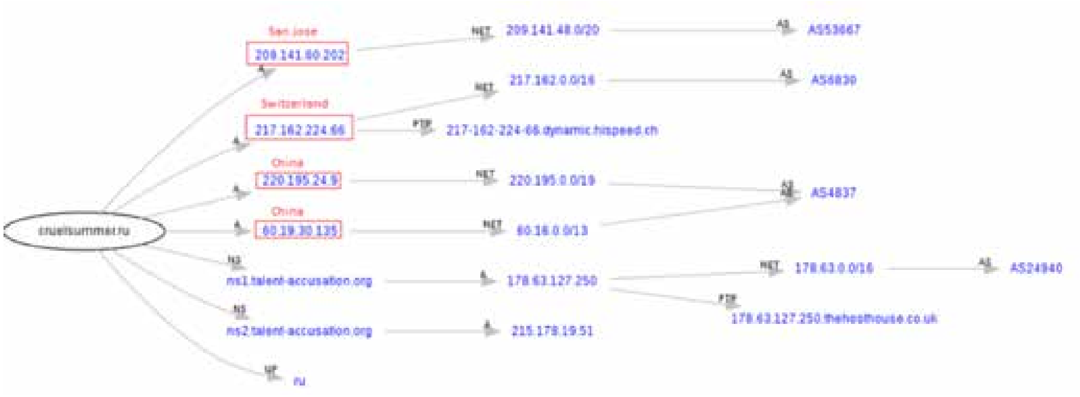
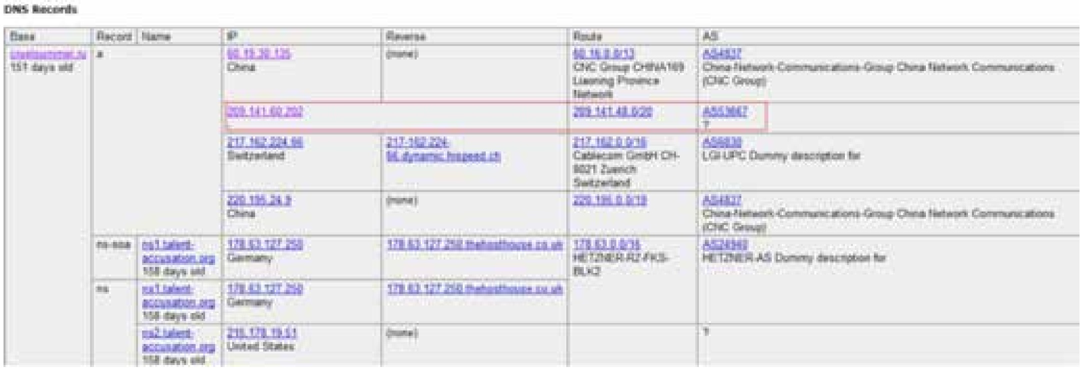


Figure 9. Domain mapping for cruelsummer.ru.



DNS Records

Base	Record	Name	IP	Reverse	Route	AS
cruelsummer.ru 151 days old	a		60.19.30.135 China	(none)	60.16.0.0/13 CNC Group CHINA169 Liaoning Province Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
			209.141.60.202		209.141.48.0/20	AS53667 ?
			217.162.224.66 Switzerland	217-162-224-66.dynamic.hispeed.ch	217.162.0.0/16 Cablecom GmbH CH-8021 Zuerich Switzerland	AS6830 LGI-UPC Dummy description for
			220.195.24.9 China	(none)	220.195.0.0/19	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
	ns-soa	ns1.talent-accusation.org 158 days old	178.63.127.250 Germany	178.63.127.250.thehosthouse.co.uk	178.63.0.0/16 HETZNER-RZ-FKS-BLK2	AS24940 HETZNER-AS Dummy description for
	ns	ns1.talent-accusation.org 158 days old	178.63.127.250 Germany	178.63.127.250.thehosthouse.co.uk		
		ns2.talent-accusation.org 158 days old	215.178.19.51 United States	(none)		?

Figure 10. Historical DNS records for cruelsummer.ru.

- Quoteandrun.ru
  - Added February 20, 2012
  - Hosted PWS-Zbot.gen.ru with MD5:
    - 3654ac937515ec668b4e35277a1c1df

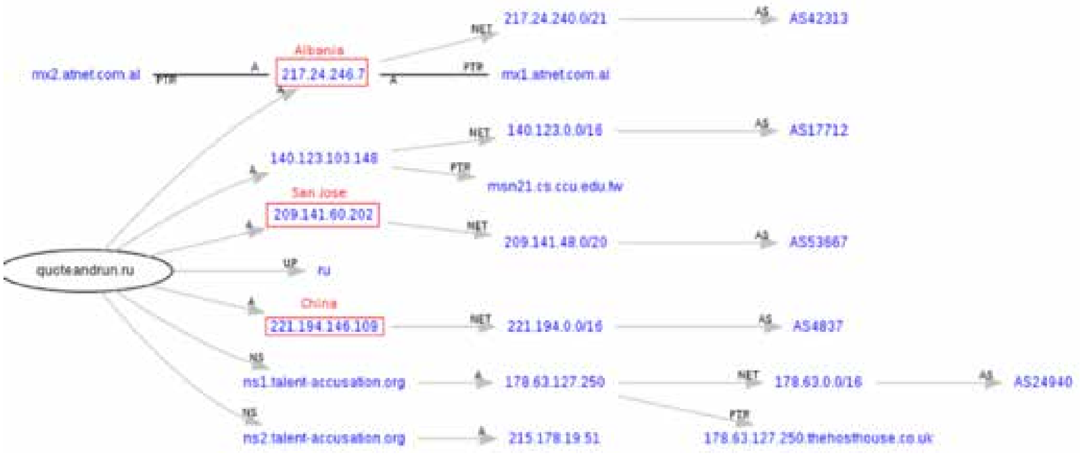
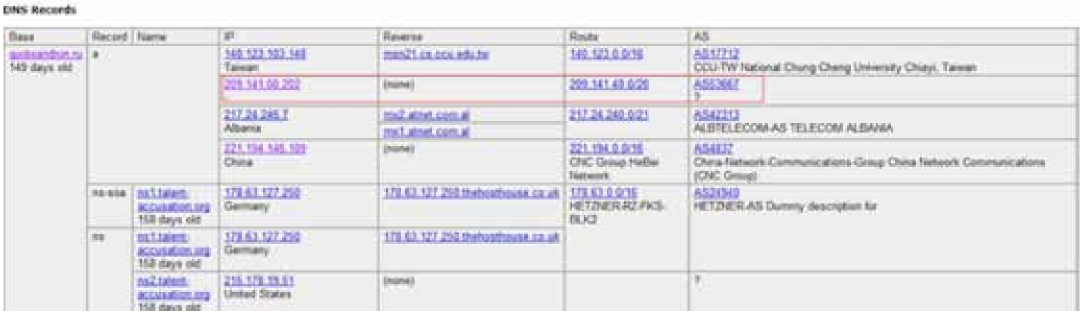


Figure 11. Domain mapping for quoteandrun.ru.



DNS Records

Base	Record	Name	IP	Reverse	Route	AS
quoteandrun.ru 149 days old	a		140.123.103.148 Taiwan	mxn21.cs.ccu.edu.tw	140.123.0.0/16	AS17712 CCU-TW National Chung Cheng University Chiayi, Taiwan
			209.141.60.202	(none)	209.141.48.0/20	AS53667 ?
			217.24.246.7 Albania	mx2.atnet.com.al mx1.atnet.com.al	217.24.240.0/21	AS42313 ALBTELECOM-AS TELECOM ALBANIA
			221.194.145.109 China	(none)	221.194.0.0/16 CNC Group HeBei Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
	ns-soa	ns1.talent-accusation.org 158 days old	178.63.127.250 Germany	178.63.127.250.thehosthouse.co.uk	178.63.0.0/16 HETZNER-RZ-FKS-BLK2	AS24940 HETZNER-AS Dummy description for
	ns	ns1.talent-accusation.org 158 days old	178.63.127.250 Germany	178.63.127.250.thehosthouse.co.uk		
		ns2.talent-accusation.org 158 days old	215.178.19.51 United States	(none)		?

Figure 12. Historical DNS records for quoteandrun.ru.

- Weaponomd.ru
  - Added February 11, 2012
  - Hosted PWS-Zbot.gen.ru with the following MD5s:
    - f387c03c8099d007a25d64df1abbc6f9
    - 8356fb8f0e9b7d8b6456204ea59f0506
    - 0c4cf45b512432aaeb0e0a52697f1e8a
    - fd1819909dd1a9d64c0b58fb90b90636

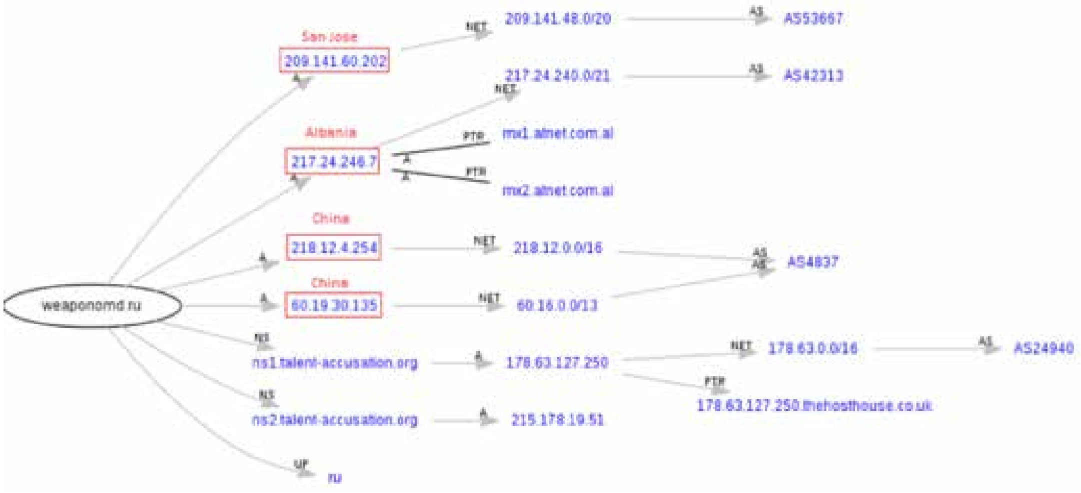
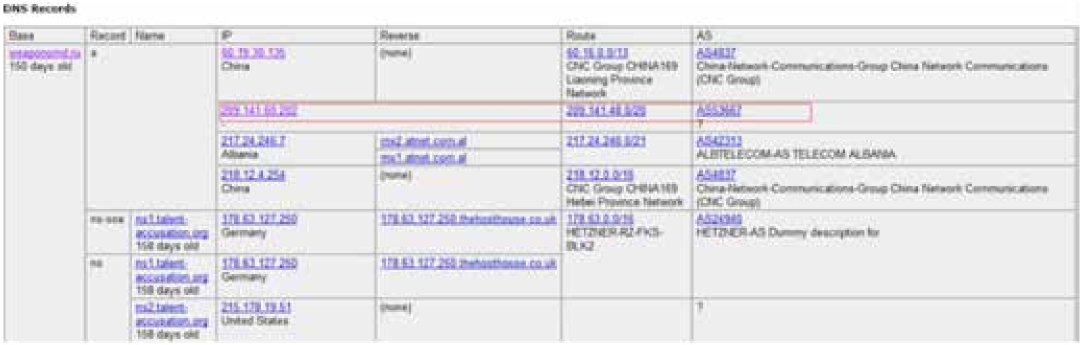


Figure 13. Domain mapping for weaponomd.ru.



DNS Records

Base	Record	Name	IP	Reverse	Route	AS
weaponomd.ru 150 days old	a		60.19.30.135 China	(none)	60.16.0.0/13 CNC Group CHINA169 Liaoning Province Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
			209.141.60.202		209.141.48.0/20	AS53667 ?
			217.24.246.7 Albania	mx2.atnet.com.al mx1.atnet.com.al	217.24.240.0/21	AS42313 ALBTELECOM-AS TELECOM ALBANIA
			218.12.4.254 China	(none)	218.12.0.0/16 CNC Group CHINA169 Hebei Province Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
	ns-soa	ns1.talent-accusation.org 158 days old	178.63.127.250 Germany	178.63.127.250.thehosthouse.co.uk	178.63.0.0/16 HETZNER-RZ-FKS-BLK2	AS24940 HETZNER-AS Dummy description for
	ns	ns1.talent-accusation.org 158 days old	178.63.127.250 Germany	178.63.127.250.thehosthouse.co.uk		
		ns2.talent-accusation.org 158 days old	215.178.19.51 United States	(none)		?

Figure 14. Historical DNS records for weaponomd.ru.

Other malware hosted on the San Jose server

Although the San Jose server seems to be an active location for Zeus-related activity, we also found other malware:

- **Ecrxlibgchux.eu**
  - Hosting Ransom!fd with the following MD5:
    - 988c52c83c3fa6cf2e7001f404a72a6b

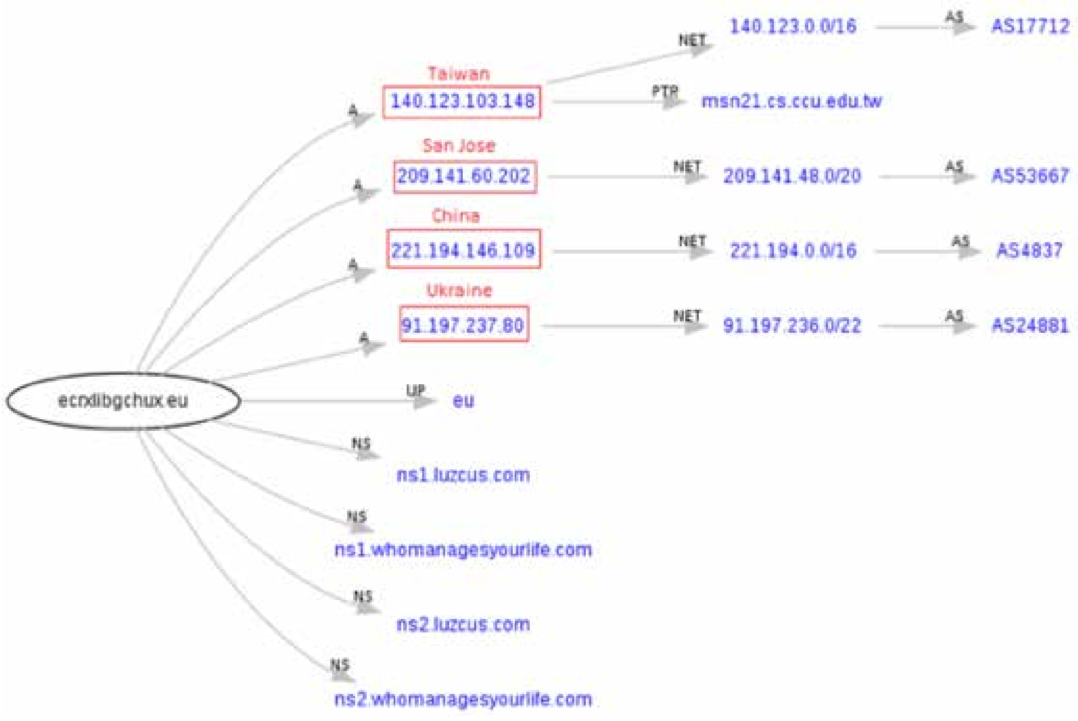
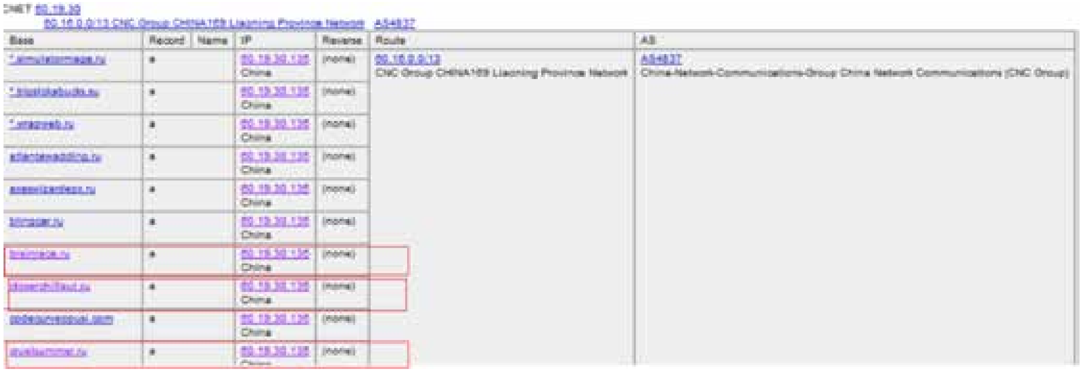


Figure 15. Domain mapping for ecrxlibgchux.eu.

History of Zeus activity

The Ice IX domain brainrace.ru, which pointed to the Arizona and San Jose servers, also used a server in China with the IP address 60.19.30.135. Brainrace.ru pointed to the server as an alternative to the Albania and San Jose servers listed in the DNS history, most likely to dynamically rotate its control among the three locations.

Our analysis is starting to lead to the conclusion that there is a heavy connection to these servers; many of the malicious domains point there.



CNET 60.19.30
60.16.0.0/13 CNC Group CHINA169 Liaoning Province Network AS4837

Base	Record	Name	IP	Reverse	Route	AS
[illegible]	*		60.19.30.135 China	(none)	60.16.0.0/13 CNC Group CHINA169 Liaoning Province Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
[illegible]	*		60.19.30.135 China	(none)		
[illegible]	*		60.19.30.135 China	(none)		
[illegible]	*		60.19.30.135 China	(none)		
[illegible]	*		60.19.30.135 China	(none)		
[illegible]	*		60.19.30.135 China	(none)		
brainrace.ru	*		60.19.30.135 China	(none)		
[illegible]	*		60.19.30.135 China	(none)		
[illegible]	*		60.19.30.135 China	(none)		
[illegible]	*		60.19.30.135	(none)		

Figure 16. Historical DNS records for 60.19.30.135.

Some of the other domains that the Chinese server hosted control Zeus botnets.

- Atlantawadding.ru
  - Added November 27, 2011
  - Hosted a Zeus drop zone at the following URL:
    - atlantawadding.ru/gjk/duals.php
- Axeswizardepx.ru
  - Added February 17, 2012
  - Hosted PWS-Zbot.gen.hb with the following MD5s:
    - 27cf0873515e9d342b7105df9263adfa
    - 63c5ee04d432bd9125e7680af9026628
    - 27cf0873515e9d342b7105df9263adfa

Investigating the Chinese server further reveals a long history of malware activity originating from the IP address that brainrace.ru pointed to at one time. These Zeus variants communicated with different domains, but mapped back to the Chinese IP address—indicating heavy usage of this provider for primarily Zeus activity.

- PWS-Zbot.gen.hv
  - *MD5*: 503f72cc78037a6d1e8cb9d4544c564f
  - *Date*: April 20, 2011
  - *Malware communication (China)*: audionotesbera.su/der/fdsabv.php
  - *Malware communication (Albania)*: 217.24.246.7 (same domain as above)
- PWS-Zbot.gen.hv
  - *MD5*: b8d7d0a773229482bba091e2d3734250
  - *Date*: January 26, 2012
  - *Malware communication (China and Albania)*: historuofgasia.su/wef/ghnfgh.php
- PWS-Zbot.gen.hv
  - *MD5*: 78a2e8a975393a3410e624253094029f
  - *Date*: March 25, 2011
  - *Malware communication (China and Albania)*: neopoliticanso.su/zpl/nbsdus.php
  - Communicates to another Albanian server at IP address 217.24.246.13
- PWS-SpyEye
  - *MD5*: 20826629b8944c83f4c4c83de3499df0
  - *Date*: March 17, 2012
  - *Malware communications to the following domains*:
    - rosefuture.com/login/hi.php?id=A489F54E4E4E41586441&stat=0
    - irishellas.com/res/mtm.exe
    - fuelhit.ru/maps.php
    - herdcave.ru/wings.php
- PWS-Zbot.gen.ab
  - *MD5*: 700b7a81d1460a652e5f9f06fc54dcd6
  - *Date*: March 8, 2012
  - *Malware communication (China)*: wrapweb.ru/wrap.php

- PWS-Zbot.gen.ru
  - *MD5*: f409064f2ff724470bd15fbea2b98573
  - *Date*: March 17, 2011
  - *Malware communication (China and Albania)*: tripslokabucks.su/drh/knmbf.php
- Generic.jb
  - *MD5*: 219906070870505cb68e9292969c3a76
  - *Date*: January 1, 2012
  - *Malware communication (China)*:
    - *kosmovodki.ru/statnl/image.php*
    - *hotelsviluppo.com/wordpress/wp-admin/file.php*
    - *www.speedcash1hour.com/wp-admin/usser.php*
- PWS-Zbot.gen.hb
  - *MD5*: 29c80f68def558ca256b16336f680051
  - *Date*: March 11, 2011
  - *Malware communication (China)*: miniokoyokolia.su/kox/psals.php
- PWS-Zbot.gen.ml
  - *MD5*: 9691fb2da9db2ac6b171ea162e2ca178
  - *Date*: October 31, 2011
  - *Malware communication*
    - *ftwtogether.ru/report.php*
    - *recruitarrowfg.com/zh.exe*
- Artemis!B4F3BCC7F4B4 (Zeus)
  - *MD5*: b4f3bcc7f4b4c009c0df477d4dbd6e05
  - *Date*: March 11, 2011
  - *Malware communication*
    - *rudeink.ru/search/baby2011.php*
    - *fabsnot.ru/search/old02ziu.bin*
- PWS-Spyeye.ci
  - *MD5*: 165d592734418dcfe344fd70eedcf178
  - *Date*: September 30, 2011
  - *Malware communication*
    - *paperrain.net/csv3333c/auto0023.jpg*
- GenericBackDoor.rz
  - *MD5*: 86163faf9f2a2e1048f15badeceabb25
  - *Date*: May 12, 2011
  - *Malware communication*
    - *paperrain.net/csv3333c/auto0023.jpg*
- Artemis!1A3DD65425E8 (Zeus)
  - *MD5*: 1a3dd65425e83a8c72a0430bbcd043a0
  - *Date*: January 13, 2011
  - *Malware communication*
    - *xoophafiel.ru/bin/xxl.bin*

A second Chinese server hosted at the same provider documented earlier also had some common Zeus domains pointing to it.

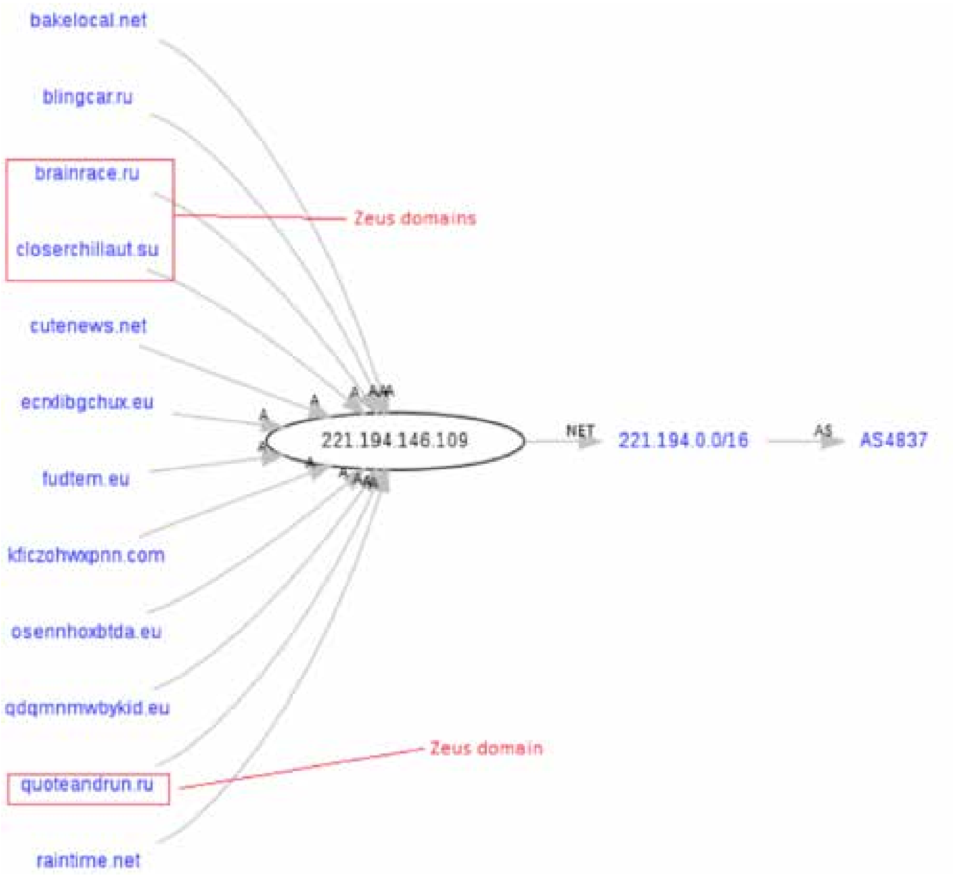


Figure 17. Domain mapping for 221.194.146.109.

Connections to Other Attacks

The campaign that targeted banks in the United States has a strong relationship with earlier server-side automated attacks that operated in a similar manner.

Event Date	Action	Pre-Action IP	Post-Action IP
2011-11-03	New	-none-	217.24.246.7
2011-11-06	Change	217.24.246.7	87.126.200.246
2011-11-18	Change	87.126.200.246	72.167.28.230
2011-11-29	Change	72.167.28.230	66.166.185.2
2011-12-11	Change	66.166.185.2	74.121.183.166
2011-12-22	Change	74.121.183.166	46.180.70.139
2012-01-03	Not Resolvable	46.180.70.139	-none-

Figure 18. Hosting history for securetechicsatcontrol.com.

The attack in 2011 that used SpyEye to conduct server-side automated attacks originated from the Albanian server, which also hosted other Zeus activity. This server was associated with and has commonly been seen as secondary to the San Jose server.

This gang used the Albanian server for three days before moving it.

Event Date	Action	Pre-Action IP	Post-Action IP
2011-02-13	New	-none-	60.206.14.13
2011-02-24	Change	60.206.14.13	205.185.127.222
2011-03-18	Change	205.185.127.222	41.134.93.2
2011-04-10	New	-none-	41.134.93.2
2011-05-03	Change	41.134.93.2	200.74.240.65
2011-05-15	Change	200.74.240.65	66.212.18.79
2011-05-28	Change	66.212.18.79	41.134.93.2
2011-06-09	Change	41.134.93.2	66.212.18.79
2011-07-03	Change	66.212.18.79	41.134.93.2
2011-07-16	Change	41.134.93.2	89.207.255.132
2011-07-28	Change	89.207.255.132	67.226.152.140
2011-08-10	Change	67.226.152.140	62.109.15.218
2011-08-23	Change	62.109.15.218	61.197.232.43
2011-09-05	Change	61.197.232.43	210.125.243.177
2011-10-01	Not Resolvable	210.125.243.177	-none-
2012-02-10	New	-none-	216.218.158.19
2012-03-26	Not Resolvable	216.218.158.19	-none-

Figure 19. Hosting history for touchproofserv.com.

The domain Touchproofserv.com, which was part of a server-side attack in 2011, was hosted at the same provider in San Jose (though with a different IP) as reccheckservingbizpacktool.net.

The Touchproofserv address is 205.185.127.222, and the hosting provider responsible for this IP is Frantech.CA, a legitimate hosting provider at 760 Mission Court, Fremont, California. The attack likely ended on March 18, 2011, as there is no malicious history thereafter.

The Origins: Fast-Flux Botnet with Albanian and Chinese Servers

The transaction server, reccheckservingbizpacktool.net, originated from a Zeus fast-flux botnet connecting to Russian and Chinese servers.

Event Date	Action	Pre-Action IP	Post-Action IP
2012-02-07	New	-none-	46.180.70.139
2012-02-19	Change	46.180.70.139	209.141.60.202
2012-03-02	Change	209.141.60.202	70.102.175.218
2012-03-14	Change	70.102.175.218	187.62.14.140
2012-03-26	Change	187.62.14.140	37.59.68.20
2012-04-07	Not Resolvable	37.59.68.20	-none-

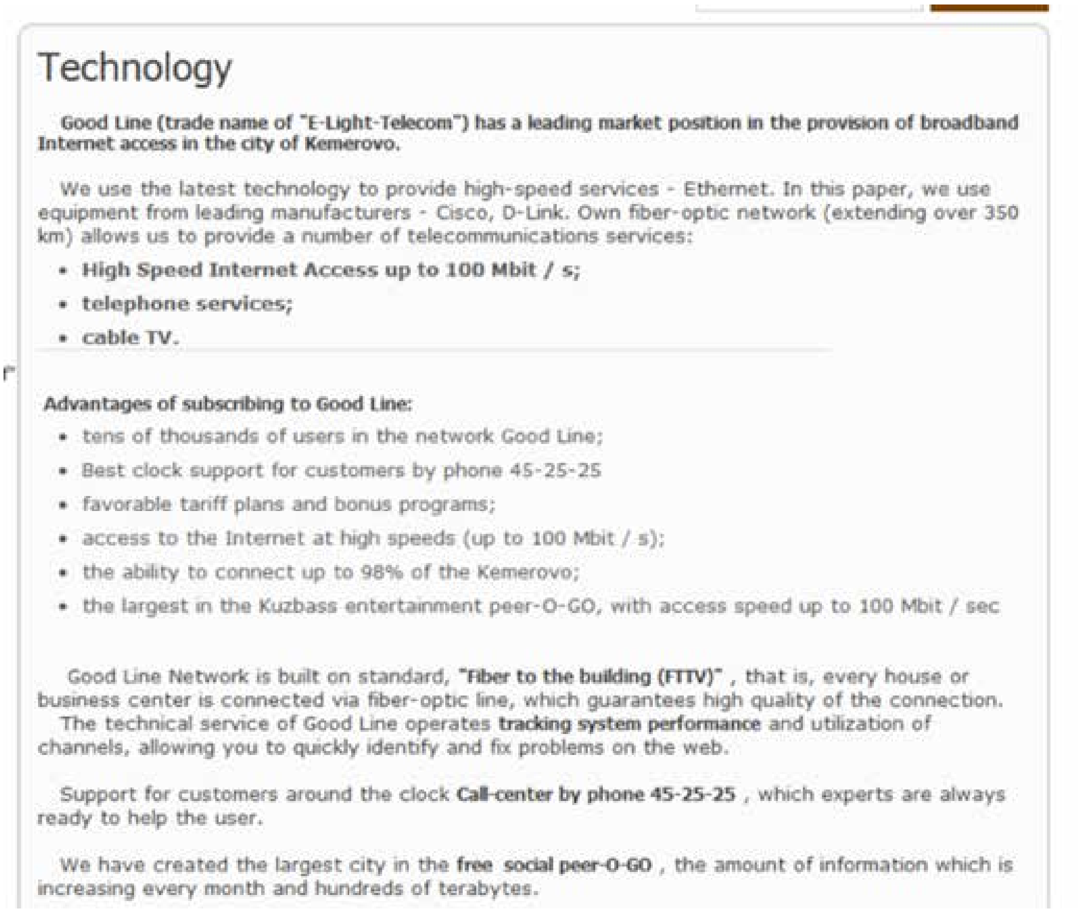
Figure 20. The IP address for reccheckservingbizpacktool.net was 46.180.70.139 and was assigned to a user in Kemerovo, Russia.

```
inetnum:          46.180.0.0 - 46.180.255.255
netname:          GOODLINE-INFO
descr:            E-Light-Telecom
descr:            Russia, Kemerovo, Kuznecky 18
country:          RU
admin-c:          KU5-RIPE
tech-c:           KU5-RIPE
status:           ASSIGNED PA
mnt-by:           ELT-MNT
mnt-lower:        ELT-MNT
mnt-domains:      ELT-MNT
mnt-routes:       ELT-MNT
source:           RIPE # Filtered

person:          Konstantin Usachev
address:         Russian Federation
address:         650099 Kuznetsky 18
address:         Kemerovo
org:             ORG-EA385-RIPE
phone:                       +73842452999
fax-no:          +73842452893
nic-hdl:         KU5-RIPE
mnt-by:          ELT-MNT
source:          RIPE # Filtered

route:           46.180.64.0/20
descr:           Goodline.info
origin:          AS39927
mnt-by:          ELT-MNT
source:          RIPE # Filtered
```

Direct whois information for the IP address.



Technology

Good Line (trade name of "E-Light-Telecom") has a leading market position in the provision of broadband Internet access in the city of Kemerovo.

We use the latest technology to provide high-speed services - Ethernet. In this paper, we use equipment from leading manufacturers - Cisco, D-Link. Own fiber-optic network (extending over 350 km) allows us to provide a number of telecommunications services:

- **High Speed Internet Access up to 100 Mbit / s;**
- **telephone services;**
- **cable TV.**

Advantages of subscribing to Good Line:

- tens of thousands of users in the network Good Line;
- Best clock support for customers by phone 45-25-25
- favorable tariff plans and bonus programs;
- access to the Internet at high speeds (up to 100 Mbit / s);
- the ability to connect up to 98% of the Kemerovo;
- the largest in the Kuzbass entertainment peer-O-GO, with access speed up to 100 Mbit / sec

Good Line Network is built on standard, **"Fiber to the building (FTTV)"** , that is, every house or business center is connected via fiber-optic line, which guarantees high quality of the connection. The technical service of Good Line operates **tracking system performance** and utilization of channels, allowing you to quickly identify and fix problems on the web.

Support for customers around the clock **Call-center by phone 45-25-25** , which experts are always ready to help the user.

We have created the largest city in the **free social peer-O-GO** , the amount of information which is increasing every month and hundreds of terabytes.

Figure 21. Details from Goodline.info translated into English.

McAfee Labs has concluded that the Kemerovo IP address, which originally hosted the transaction server, was part of a Zeus fast-flux botnet because a number of other domains pointed there. According to DNS records, some of these domains—in addition to the domain that was used for the transaction server—were involved in Zeus activity.

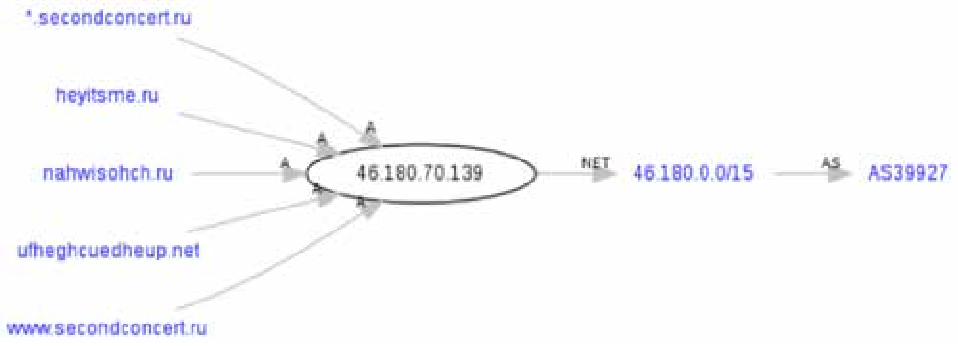
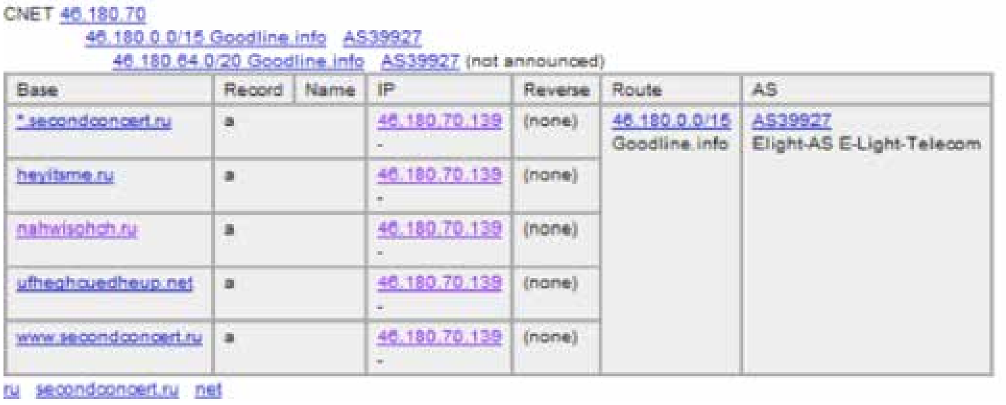


Figure 22. Domain mapping for 46.180.70.139, reccheckservingbizpacktool.net.



CNET 46.180.70
46.180.0.0/15 Goodline.info AS39927
46.180.64.0/20 Goodline.info AS39927 (not announced)

Base	Record	Name	IP	Reverse	Route	AS
*.secondconcert.ru	a		46.180.70.139 -	(none)	46.180.0.0/15 Goodline.info	AS39927 Elight-AS E-Light-Telecom
heyitsme.ru	a		46.180.70.139 -	(none)		
nahwisohgh.ru	a		46.180.70.139 -	(none)		
ufheghouedheup.net	a		46.180.70.139 -	(none)		
www.secondconcert.ru	a		46.180.70.139 -	(none)		

ru secondconcert.ru net

Figure 23. Historical DNS records for 46.180.70.139.

The following domains pointing to 46.180.70.139, reccheckservingbizpacktool.net, are confirmed Zeus domains and are part of the fast-flux botnet operating from this location with connections to Chinese servers. The DNS historical data goes back to December 2011 and when mapped we often find two distinct Chinese servers belonging to the botnet that have been used in different Zeus campaigns.

What we see in common in both domains is the AS4837, an IP address registry that manages the IP address segments used by the fraudsters. A second address belongs to another IP registry in China.

- Heyitsme.ru
  - Hosted a Zeus configuration file on December 14, 2012
    - heyitsme.ru/xx.bin

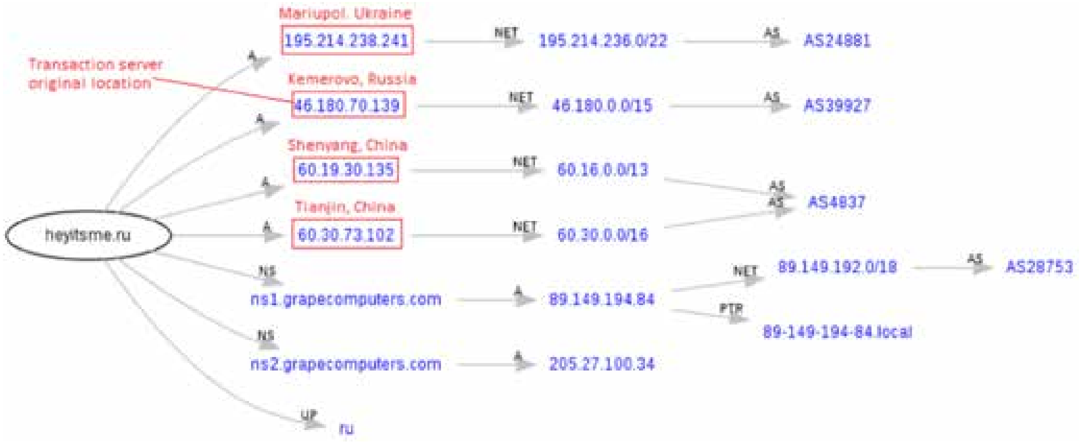
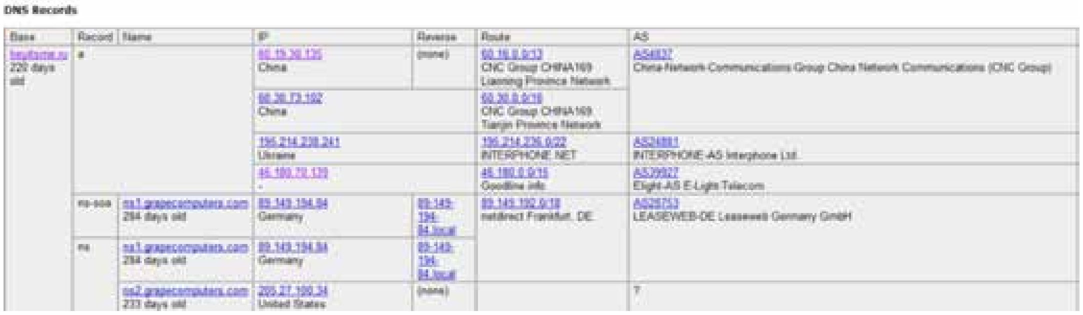


Figure 24. Domain mapping for heyitsme.ru.



DNS Records

Base	Record	Name	IP	Reverse	Route	AS
heyitsme.ru 220 days old	a		60.19.30.135 China	(none)	60.16.0.0/13 CNC Group CHINA169 Liaoning Province Network	AS4837 China Network Communications Group China Network Communications (CNC Group)
			60.30.73.102 China		60.30.0.0/16 CNC Group CHINA169 Tianjin Province Network	
			195.214.238.241 Ukraine		195.214.236.0/22 INTERPHONE NET	AS24881 INTERPHONE-AS Interphone Ltd.
			46.180.70.139 -		46.180.0.0/15 Goodline info	AS39927 Elight-AS E-Light-Telecom
	ns-soa	ns1.grapecomputers.com 284 days old	89.149.194.84 Germany	89-149-194-84.local	89.149.192.0/18 netdirect Frankfurt, DE	AS28753 LEASEWEB-DE Leaseweb Germany GmbH
	ns	ns1.grapecomputers.com 284 days old	89.149.194.84 Germany	89-149-194-84.local		
		ns2.grapecomputers.com 233 days old	205.27.100.34 United States	(none)		?

Figure 25. Historical DNS records for heyitsme.ru as of December 15, 2011.

- Nahwisohch.ru
  - Hosted PWS:Win32/Zbot.gen!Y with the following MD5 on February 17, 2012
    - 816b5164836b18d7778c1307c77df307

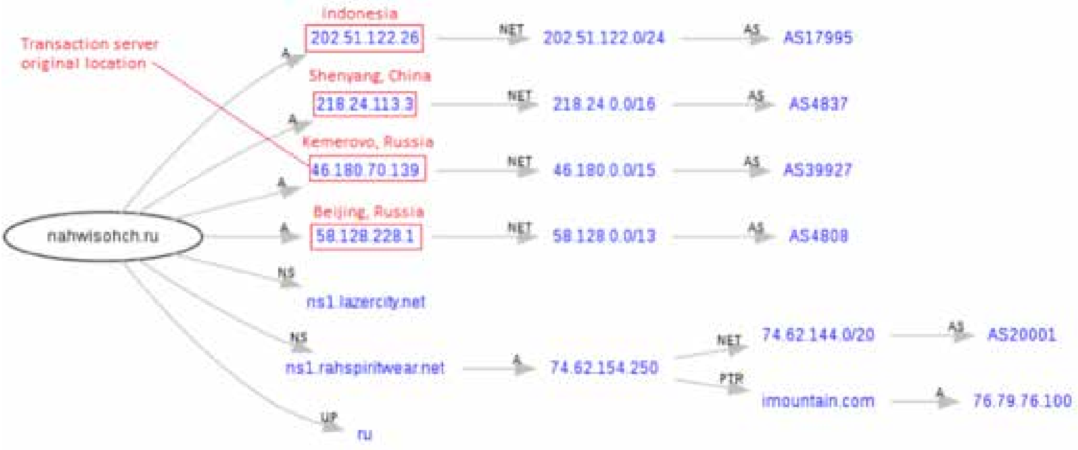
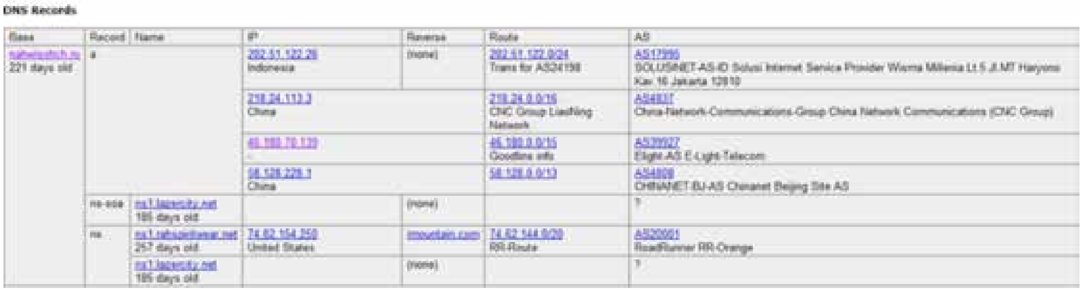


Figure 26. Domain mapping for nahwisohch.ru.



DNS Records

Base	Record	Name	IP	Reverse	Route	AS
nahwisohch.ru 221 days old	a		202.51.122.26 Indonesia	(none)	202.51.122.0/24 Trans for AS24198	AS17995 SOLUSINET-AS-ID Solusi Internet Service Provider Wisma Millenia Lt.5 Jl.MT Haryono Kav 16 Jakarta 12810
			218.24.113.3 China		218.24.0.0/16 CNC Group Liaoning Network	AS4837 China-Network-Communications-Group China Network Communications (CNC Group)
			46.180.70.139 -		46.180.0.0/15 Goodline info	AS39927 Elight-AS E-Light-Telecom
			58.128.228.1 China		58.128.0.0/13	AS4808 CHINANET-BJ-AS Chinanet Beijing Site AS
	ns-soa	ns1.lazercity.net 185 days old		(none)		?
	ns	ns1.rahspiritwear.net 257 days old	74.62.154.250 United States	imountain.com	74.62.144.0/20 RR-Route	AS20001 RoadRunner RR-Orange
		ns1.lazercity.net 185 days old		(none)		?

Figure 27. Historical DNS records for nahwisohch.ru.

Links in the United States

Our investigations revealed connections to US individuals running a legitimate business in Pittsburgh, Pennsylvania. Their domain was originally hosted on one of the Chinese servers hosting other Zeus activity. Their domain is also connected to the fast-flux botnet at IP address 217.116.198.25.

The domain uses the same name servers as the other Operation High Roller domains.

- ns1.mcgarryhome.net
- ns2.mcgarryhome.net

Apparently either the Pittsburgh businessmen’s identities were stolen, or these two got mixed up in a Russian cyberfraud scheme and their shop, a pizza restaurant, is a front. The latter case is certainly possible, given that the fraudsters would need a way to launder the stolen US funds. The timing for the registry and hosting of the domain is right around the time the Operation High Roller attacks happened in the United States.

Targeting Industry Sectors

The groups behind Operation High Roller carefully targeted specific industries in their campaigns. Typically these campaigns have no precise target other than high net worth businesses with significant cash flow; however, we found a common theme.

In the United States, Operation High Roller targeted commercial banking. Fraudsters infected victim companies that belonged to the following industries:

- Manufacturing
- State and local governments
- Import/export

We also found campaigns in Latin America targeted similar industries.

Conclusion

McAfee Labs concludes that the Operation High Roller campaigns of 2012 that targeted the United States and the Netherlands originated from a hosting provider in Kemerovo, Russia, with heavy connections to Albania and China. Throughout the process of mapping the infrastructure, we found that both the starting point in Russia and a hosting provider in San Jose, California, have been involved in other Zeus botnet activity.

Attacks like those documented in Operation High Roller will continue; fraudsters will always develop new and more sophisticated campaigns. We expect that the actors behind Operation High Roller will continue to improve their methods and will look for additional avenues to our money.

In this research, we pointed out how the fraudsters were able to defraud the banks' wire systems via a number of highly complex schemes using several malware families. The likely next move by these actors is to target automated clearing house payment channels using methods similar to those employed in Operation High Roller.

About the Author

Ryan Sherstobitoff is a threats researcher with McAfee Labs. Formerly, he was Chief Security Strategist at Panda Security, where he managed the US strategic response for new and emerging threats. Sherstobitoff is widely recognized as a security and cloud computing expert.

About McAfee Labs

McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence™. The McAfee Labs team of multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

[1] http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com