RBN “Rizing”

ABDALLAH INTERNET HIZMETLERI (AIH)

Version: 1.0.2

Release Date: 29 February 2008

Author: dn1nj4 at shadowserver dot org

Table of Contents

Table of Figures

Russian Business Network

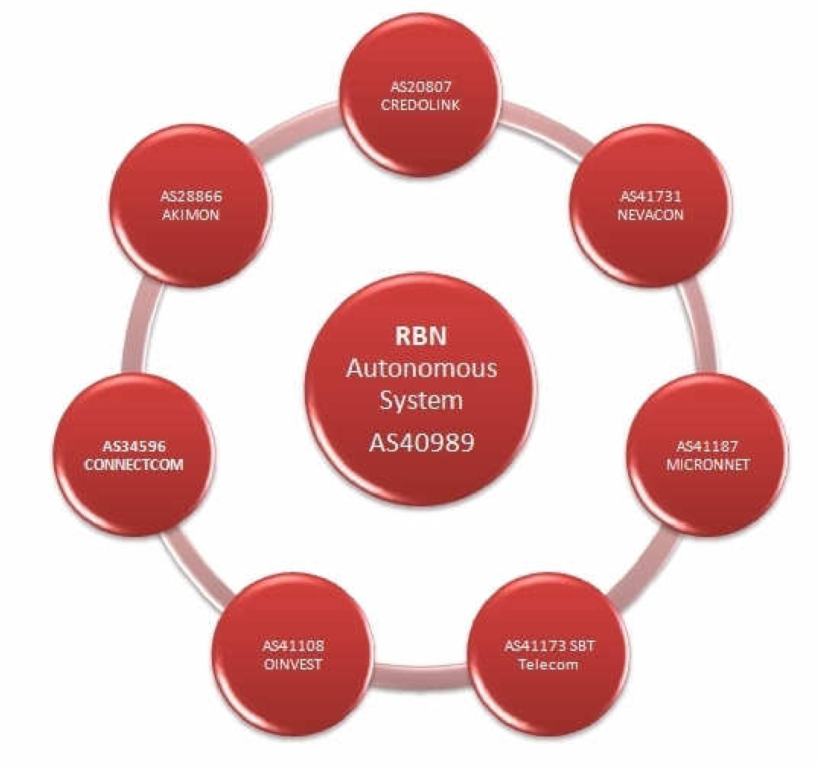

Figure 1: ASNs Associated with RBN

In the last few months, there has been a significant amount of press coverage given to insidious cyber activity associated with the segment of the Internet known as the “Russian Business Network,” or **RBN**. Previous studies have suggested that the RBN has ties to nearly every area of cybercrime, including: phishing, malware, DDOS activity, pornography, botnets, and anonymization.[1] [2]

In November 2007, media reporting indicated that a large portion of the RBN “went dark.” [3] Since that time, the Shadowserver Foundation has been more closely analyzing outlying networks implicated as being associated with RBN. One of these suspected outliers is AS9121, known as TurkTelekom. SecurityZone.org reported in early December 2007 that while not everything in TurkTelekom appears to be malicious, there are some ranges that are “particularly bad[4]” and analysis of Shadowserver Foundation data agrees. Several subranges quickly stand out as being deeply involved in malicious cyber activity: **88.255.90.0/24** and **88.255.94.0/24**. IP registration indicates these ranges are listed under the name “ABDALLAH INTERNET HIZMETLERI” (**AIH**).

Abdallah Internet Hizmetleri (AIH)

In one of the most thorough RBN studies to date, David Bizeul reported that AIH ranges **88.255.90.0/24** and **88.255.94.0/24** - are among the “most used network ranges used by RBN affiliates’ domain names.[5]” The purpose of this paper is to take a deeper look at these two class C ranges of AIH based out of Rize, Turkey[6], available information from the Internet, and statistics collected by the Shadowserver Foundation to provide further insight into the scope and depth of the RBN.

"It is now public knowledge that AbdAllah Internet Hizmetleri is under the control of RBN."[7] ~ Spacequad AntiSpam Services

Shadowserver Malware Repository

A search of the Shadowserver Foundation's 16 million suspect binaries revealed approximately 1,700 samples which connected back to AIH via HTTP. As shown on the timeline in Figure 2 below, after nearly a year with no notable activity AIH malware exploded onto our radar in October 2007. November and December 2007 were fairly quiet, followed by another surge in January 2008. It is unclear exactly what caused the drastic differences.

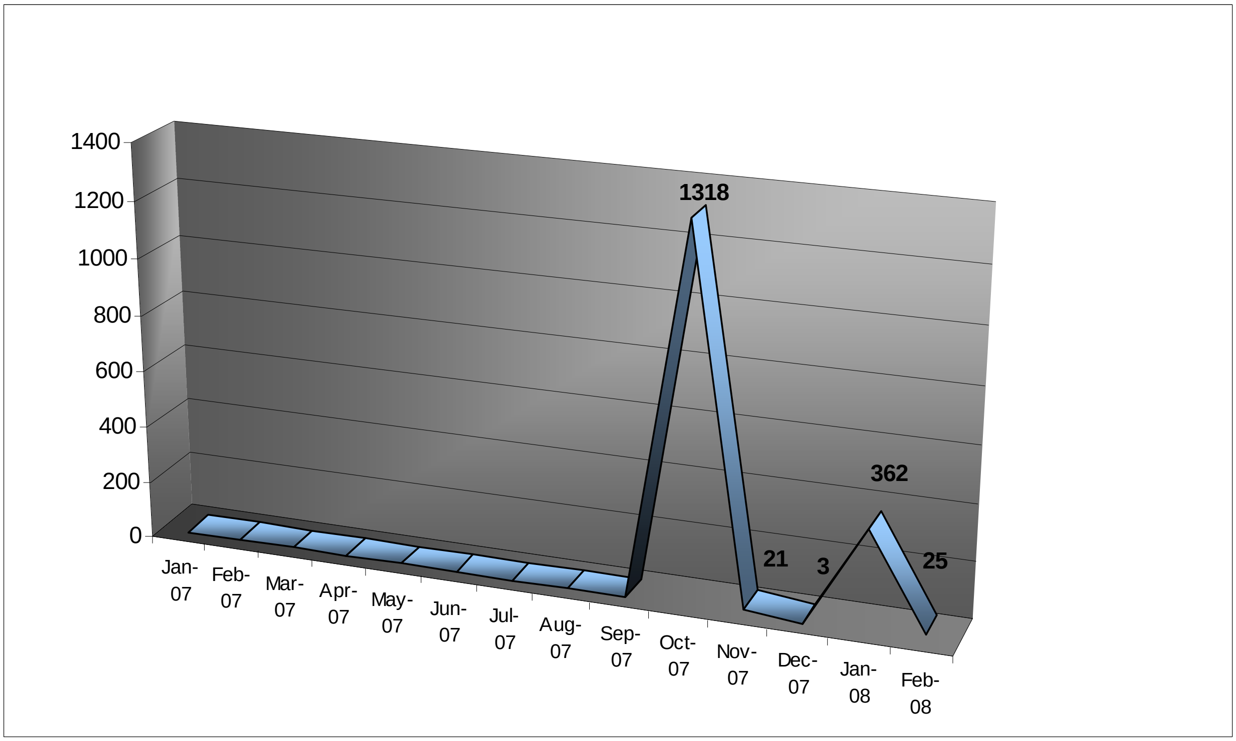

Figure 2: Unique Malware Samples Connecting to AIH Ranges via HTTP

"In recent weeks, moreover, Trend Micro has seen equivalents of RBN pop up in Turkey and Taiwan"[8] ~Trend Micro

Antivirus/Packer Analysis

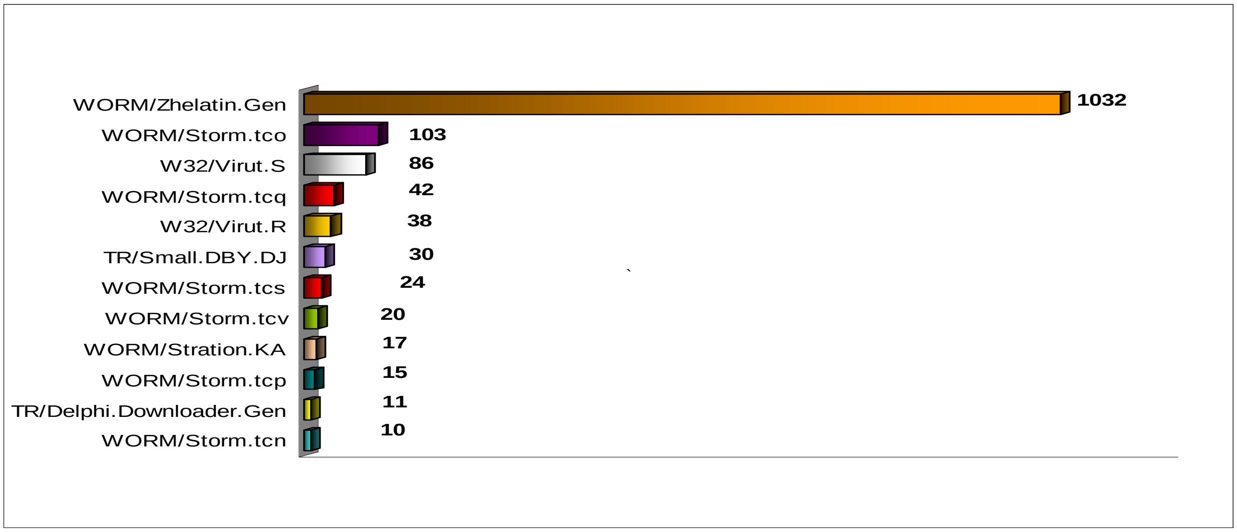

Figure 3: Antivirus Detections with Ten or More Samples[9]

Antivirus scans of the 1,700 samples showed six major groupings of detections, including Zhelatin, Storm, Virut, Stration, and Peed along with various other Trojans, password stealers and proxies. The Shadowserver Foundation's previous analysis of AS40898 identified Tibs and Zhelatin as having a "long and beneficial relationship" with the RBN[10].

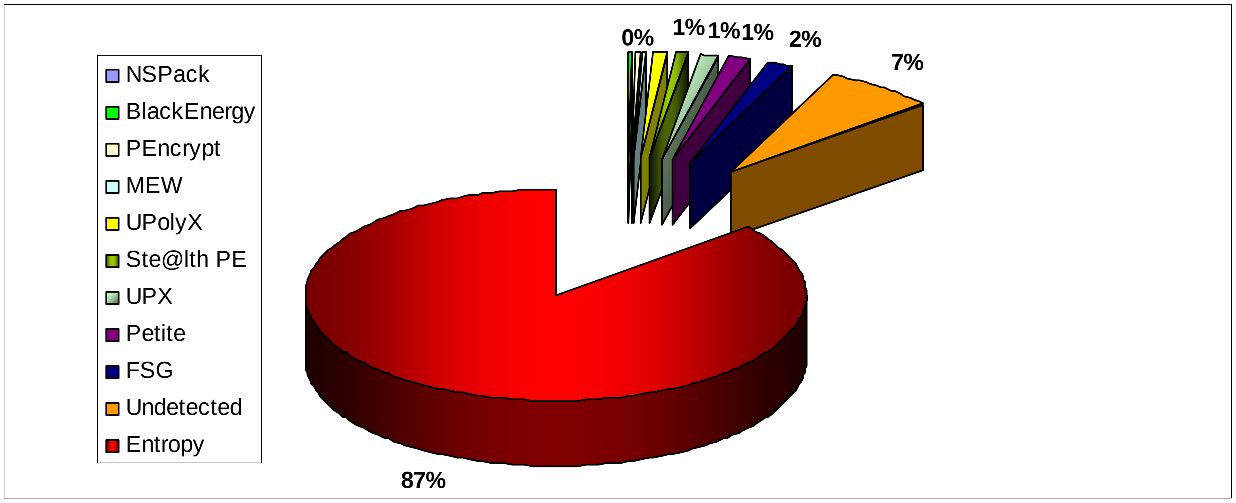

Figure 4: Packer Detection of Samples[11]

Approximately 93% of the samples showed some form of binary compression. While there were a handful that were readily identifiable as commonly seen utilities (such as UPX, FSG, Petite, MEW and NSPack), a majority utilized an unknown compression scheme. *AIH malware in this sample set favors non-standard binary compression.*

Fuzzy Hash Analysis

Using fuzzy hash analysis techniques, it is possible to compare two binary files, A and B, to find the percentage of code in A that is present in B.[12] A scan of the full set of 1,700 binaries revealed a total of 2,944 unique pairs of files sharing some percentage of code. Sample sets which had 5 or more matches sharing over a 50% code similarity are shown in Figure 5, below.

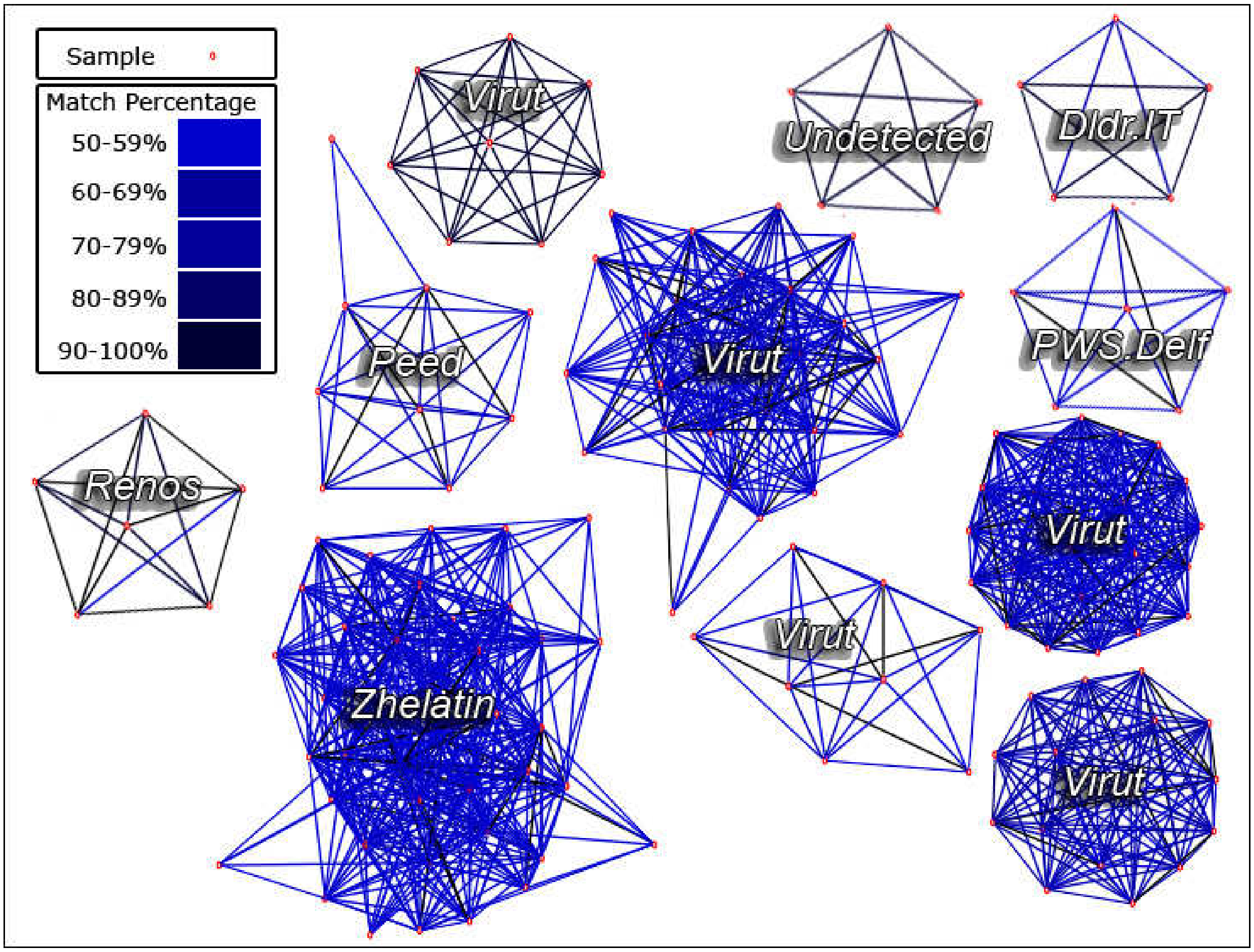

Figure 5: Fuzzy Hash Analysis of AIH Samples

After generation of the matches for Figure 5, an overlay was created with antivirus scan results to give additional meaning to the various clusters. Further research into the cluster labeled "undetected" revealed variants of an AutoIT Downloader.

The direct implication of Figure 5 is that by utilizing fuzzy hashing techniques, there are obvious clusters of samples which can be grouped together without any prior knowledge or hard-coded signatures. Note that fuzzy hashing alone will not indicate a sample's function, but by utilizing these techniques it should be possible to increase the detection and categorization of new samples.

The samples in the selected grouping all had at least half of their code, and in many cases upwards of 99% of their code, present in four or more other samples. With this level of code sharing, it is difficult to discount the possibility that there is either one group of individuals behind the various sets of malware, or one shared code-base amongst multiple groups.

IP Address Callback Analysis

As shown in Figure 6 below, only 21 unique IP addresses were identified as being in use across the 1,700 samples.

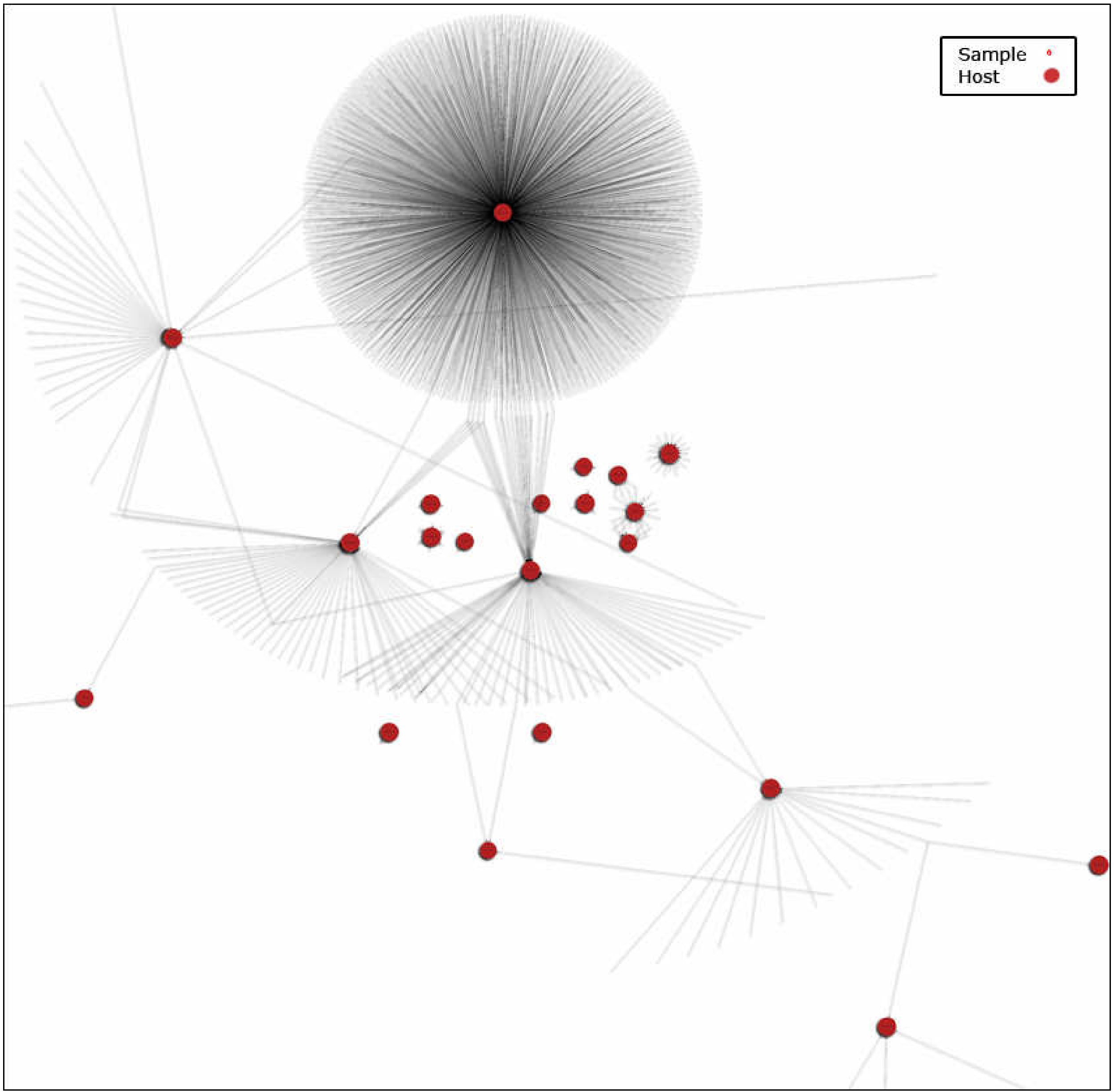

Figure 6: Malware Sample to AIH Host Connections[13]

85% of the callback connections touched AIH IP address 88.255.90.253. This was followed by a distant second with AIH IP address 88.255.90.154 receiving 4% of the connections.

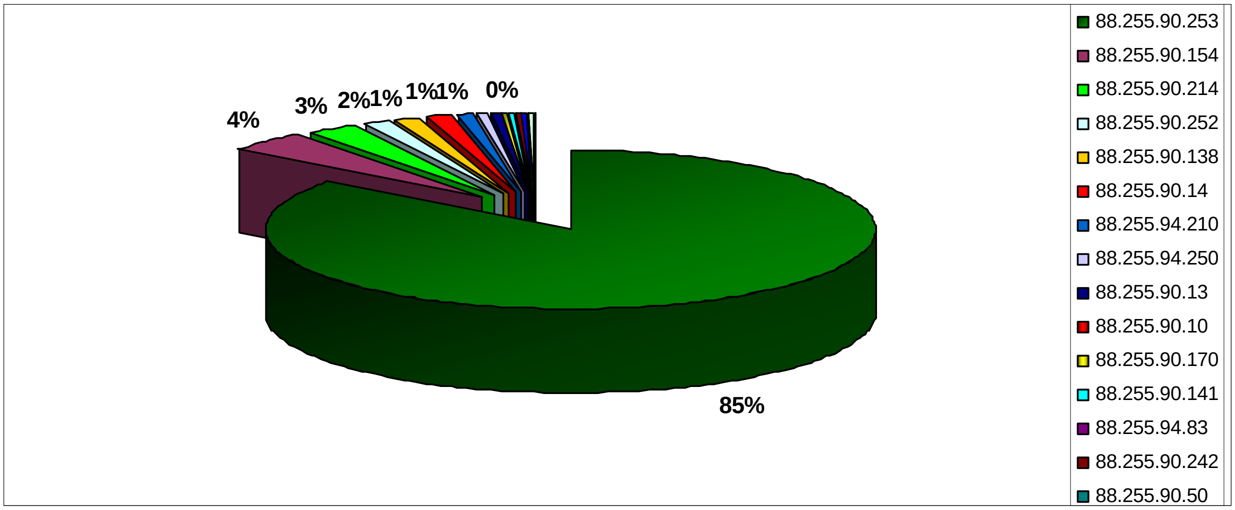

Figure 7: Percentage of Connections By IP Address

Using these 21 unique hosts as a focal point, Internet, passive DNS[14] and graph analysis revealed the following:

Unique IP	Host Information
88.255.90.10	• Listed in the Google Cache on projecthoneynet.org as being possibly spam related. • All malware connecting to this host also connected to 88.255.90.14. • Passive DNS Domains: o c0re.cc o online-scan.com o www.spywaresoftstop.com o ns1.3xvideogalleries.com o vn385.com o www.vn385.cn o ns1.joporvatel.in
88.255.90.13	• All malware connecting to this host also connected to 88.255.90.14. • Passive DNS Domains: o antivirus.online-scan.com o maturecreampieorgies.com o ns2.3xvideogalleries.com o ns2.joporvatel.in o spywaresoftstop.com o spywaresoftstop.org o www.spywaresoftstop.com o www.spywaresoftstop.org
88.255.90.14	• Malware connecting to this IP address often also connected to either 88.255.90.10 or 88.255.90.13

	• Reported as serving malware • Passive DNS Domains: o all1count.net o downloadfilesldr.com o mediacount.net o stat1count.net
88.255.90.26	• Spam Domain: milk0soft.com[15] • Passive DNS Domains: o d34thnation.com o havephun.org o milk0soft.com o plugin.name o www.milk0soft.com
88.255.90.50	• WebAttacker exploitation kit, Viagra Scam, Investment Banking Scams[16] • Passive DNS Domains: o 1941revenge.org o abdulla.cc o a.njnk.net o appolage.org o b.njnk.net o dreamzone.ws o evilrode.org o f-consg.com o f-consgrp.com o gosufootman.info o inn2coming.com o inncoming.com o mail.abdulla.cc o mail.f-consgrp.com o mail.smil3r.info o mail.x-softwares.com o ngc1976.net o ns1.dnsprime.net o olthart.com o pin-l-games.ws o smil3r.info o traff4all.info o verymonkey.com o www.1941revenge.org o www.evilrode.org o www.inn2coming.com o www.inncoming.com o www.ngc1976.net o www.pin-l-games.ws o www.x-softwares.com o www.xsoftwares.com o x-softwares.com o zupacha.info • Spam Domains: [17] o byron-consulting-group.com o dkebooks.ocm o jieod.com

	o midgejs.com o aoejf.com o yseac.com o kaserid.com o jekdoe.com o ujeose.com o masiwer.com o ruesiwe.com o kaoeds.com o iwoser.com o xeirod.com o neusoas.com o geoepd.com o efuyr.com o ziude.com o polsenstanford.com o heyud.com o woqkr.com o seiudr.com o aosier.com o dueor.com o bqgqnfc.cn o wrbhnuw.cn • Progold Investments Criminal Fraud[18]
88.255.90.74	• Storm worm related[19] • Passive DNS Domains: o babla.info o bublgum.net o pirduxa.com o yourtuck.com • One of the two samples connecting to this IP address also connected to 88.255.90.214
88.255.90.138	• Exploit hosting: willposting.com[20] • "Well known, criminal owned" part of Russian Business Network supporting spamvertising and money laundering[21] • Phishing email related.[22] • Hosting suspicious "get paid to read" software.[23] • Passive DNS Domains: o allbusinesinformation.com o alltraffworld.com o artaroundme.com o artsutra.biz o arttraffic.biz o bl0cker.info o bl0cker.org o da-best-place-in-web.net o darkgod.org o ddooss.com o documentu.info o free-porn-movies.info o getsecureaccess.com o greeetthh.com o gwatturar.com

	o hack-off.info o iframe-revenue.com o ilitelist.info o kalabok.info o killload.com o lapanaka.com o lem0n.info o loadscash.com o love-day.net o mail.darkgod.org o mail.greeetthh.com o mail.mjakson.info o mail.my-profitable.biz o mail.tmtraff.com o mail.windowsdefends.com o mail.x-victory.ru o malasha.com o mazafa.com o miron555.org o mjakson.info o musicbox1.cn o my-profitable.biz o ns1.darkgod.org o ns1.srvs4u.biz o ns1.swerjr.ws o ns5.lavlinsky.com o oleniny123.com o online-traffeng.com o parranoik.com o porn--movies.info o scaned.info o sendspam.info o sexrusfuck.com o space-sms.info o statistics-google.org o stopmen.org o takenames.cn o tds.free-porn-movies.info o tds.malasha.com o tds.mazafa.com o td.tmtraff.com o tmtraff.com o toplistsearch.info o traff-market.org.ua o ttt.tmtraff.com o tyc0traf0.com o unicorn-shipping.com o vip-load.net o volkoeb.info o watch77.com o webonlinesecond.com o wellsfargo-usa-uk.com o wellsworldweb.org

	o windowsdefends.com o www.artsutra.biz o www.bismoke.cn o www.free-porn-movies.info o www.gtrrrreee.com o www.scaned.info o www.watch77.com o www.windowsdefends.com o www.x-victory.ru o x-victory.ru o zair32.org • Spam Domains:[24] o europeansmoke.cn o globalsmoke.cn o supersmoke.cn o ultrasmoke.cn o sinlife.cn o sexrusfuck.com o children-europe.nu
88.255.90.141	• Passive DNS Records: o nikitka.org
88.255.90.154	• Downloader contact site.[25] [26] • Adware, spyware or viruses [27] • Fifteen samples connecting to this IP also connected to 88.255.90.214 and/or 88.255.90.253 • One sample connecting to this IP address also connected to 88.255.90.252
88.255.90.170	• Bad mail domain[28] • Known RBN address[29] • Money laundering base for Ukranian/Russian cybercriminal hosting. [30] • Passive DNS Domains: o ns1.showrico.info o ns2.showrico.info
88.255.90.214	• Adware Domains: [31] o worldjackpotcasinoau.com.cn o worldjackpotcasinoav.net.au o worldjackpotcasinoaw.net.au • Domain links in spam email: [32] o clokkl.cn o tockst.net.cn o tocksp.com.cn o cbcxbxv.com o worldjackpotcasinogx.cn o bad-debtzd.com o busloansyr.com.cn o worldjackpotcasinohq.cn o bad-debtyc.net.cn o busloansyr.net.cn • Passive DNS Domains: o 612 domains listed (cut for brevity) • Fifteen samples connecting to this IP also connected to 88.255.90.154 and/or 88.255.90.253

	• Two samples connecting to this IP address also connected to 88.255.90.252
88.255.90.242	• Spam domains:[33] o a9da6.org o 04ccc408.org o bdb7beb6.org • Passive DNS Domains: o 04ccc408.org o a9da6.org o bdb7beb6.org o countq.com o crunet.info o e7da7.biz o e7da7.com o e7da7.name o e7da7.net o e7da7.org o e7da7.ws o ns1.e7da7.com o ns2.e7da7.com o ns3.e7da7.com o ns4.e7da7.com o shiny-stat.com o staticq.com
88.255.90.252	• Passive DNS Domains: o hightstats.net o ns2.cool-cool-websearch.com o ns2.trdns.biz • Three samples connecting to this IP address also connected to 88.255.90.253 • Two samples connecting to this IP address also connected to 88.255.90.214 • One sample connecting to this IP address also connected to 88.255.90.154
88.255.90.253	• Downloader Updates:[34] o stat1count.net o all1count.net o mediacount.net • Domain: softspydelete.com o Tibs malware related [35] o Zhelatin related[36] o Possibly hosting web exploits[37] • Passive DNS Domains: o all1count.net o bestnums.net o blyadsfdg.biz o cool-cool-websearch.com o mediacount.net o prevedtraf.biz o softspydelete.com o stat1count.net o stattrader.biz o www.prevedtraf.biz

	o www.stattrader.biz • Fifteen samples connecting to this IP also connected to 88.255.90.214 and/or 88.255.90.154
88.255.94.22	• Passive DNS Domains: o guestinef.net
88.255.94.83	• Fraud, money laundering and malware sites [38] • Passive DNS Domains: o 60 domains identified (cut for brevity) • Two of the three samples connecting to this IP address also connected to 88.255.90.154.
88.255.94.114	• "Domains to Avoid": [39] o lskdfjlerjvm.com o Cigs4you.info o D101b.com o Estrel-logistics.com o Fethard-best.com o Fresh-film.net o Gp-eurocapital.com o Hack-off.info o Ihos.info o Intway587.com o Media-content.biz o Online-traffeng.com o Pin-l-games.com o Piterseo.com o Prestra.com o Prestra.net o Qadro.net o Qwert285.com o Referatoff.info o Serbitoname.inf o Serd158.com o Trafagon.net o Unistream-shipping.com o Usps-mailcorp.com o Vermont-trust.com o Xolodilnikov.net • Passive DNS Domains: o 88 domains identified (cut for brevity) • The only sample in the Shadowserver malware repository which connected to this IP address also connected to 88.255.90.170 and 88.255.94.210
88.255.94.116	• Passive DNS Domains: o ihos.info
88.255.94.210	• Passive DNS Domains: o 4400hosting.com o 4wap.org o apollohostingcompany.org o baycitysearch.com o bestcashsolution.org o bigtits-revolution.com o board-game-geek.com o bonphire.net

	o carakym.net o car-direct.biz o crutch-field.com o find-fm.net o greatbetcasino.com o hardcore-revolution.com o hi-mobile.biz o hq-pharma.org o inova-comps.com o loads.cc o mail.carakym.net o mail.shaks.cc o mail.traff.cc o mawilliamshomes.net o mobileenterprisemag.net o mp3licensing.biz o mp3mediaworld.biz o ns1.4wap.org o ns1.apollohostingcompany.org o ns1.zaozernoe.com o ns2.rocketcityhosting.net.rocketcityhosting.net o ns2.zaozernoe.com o onlinecatalogworld.com o pharmarcworld.com o rocketcityhosting.net o satellife.info o shaks.cc o traff.cc o travelistic.info o voile212.net o www.apollohostingcompany.org o www.disturbia.cc o www.greens-insurance.com o www.loads.cc o www.shaks.cc o xanaxon.com o zagruzki.name • Two samples connecting to this IP address also connected to 88.255.90.154.
88.255.94.246	• WebAttacker exploitation kit[40]
88.255.94.250	• Under control of the **New Media Malware Gang**[41] • Downloader site[42] • Passive DNS Domains: o ns.imbadns.com o 4uoem.com o bestvalueoemshop.net o bestvalueoemshop.com

Table 1: Sample IP Address Analysis

It is readily apparent based on the above table that many of these 21 IP addresses are linked together. They by no means appear to be innocent bystanders in the propagation of cyber crime. Web research tells a consistent story of malicious code distribution, fraud, money laundering and spam.

While many of these IP addresses have been readily identified to the public as hostile in nature, a number of the IP addresses from this malicious code sample set yielded no cached web results. It is most likely safe to assume that this activity is merely the tip of the iceberg.

User-Agent Callback Analysis

While many of the 1700 samples utilized either the system default browser user-agent settings or forged legitimate-looking user-agent settings, a small subset did not. These user agents can be detected by monitoring Intrusion Detection Systems for outbound HTTP requests containing "User-Agent: <user-agent>".

```
User-Agent: _
User-Agent: 006
User-Agent: C:\12345.exe
User-Agent: clbvbh
User-Agent: gqhe
User-Agent: iDownloadAgent 3.0
User-Agent: Internet Explorer
User-Agent: Machaon
User-Agent: Microsoft Internet Explorer
User-Agent: MS Internet Explorer
User-Agent: WINDOWS_LOADS
```

Table 2: Sample User-Agent Analysis

Domain Name Callback Analysis

The following 80 domain names were utilized by the 1,700 samples. Amplifying information about the resolutions of these domains at the time of this report is provided where it was available.[43] Note that there are a significant number of networks beyond AIH which are associated with this activity.

DOMAIN NAME	***IP ADDRESS***	***Notes***
all1count.net	*n/a*	**Browser Exploits**
a.meza69.com	80.77.85.190	FreeBSD-Apache/1.3.33
bestbsd.info	72.232.247.242	FreeBSD-ngnix/0.6.6
besthotplace.com	216.39.58.206	
bestnums.net	77.91.229.54	**Promoted by spam** FreeBSD-Apache

candy-country.com	*n/a*	
carakym.net	*n/a*	
carrentalhelp.org	72.232.202.162	FreeBSD-Apache
client133.faster-hosting.com	217.20.122.32	
cnc-inc.cn	195.5.116.244	**Phishing or other scams** Linux-ngniz/0.5.33
codecname.com	*n/a*	**Spyware hosting**
codecnice.net	*n/a*	**Spyware hosting**
codecops.net	*n/a*	**Spyware hosting**
codec-scan.com	*n/a*	**Adware, spyware, PUPs Links to malicious domain dvdaccess.net**
command.adservs.com	81.22.35.114	NetWare/MIIxpc/4.7
damndskj.com		**Browser Exploits**
date-porno.net	64.28.181.28	**Adware, spyware, PUPs** Free-BSD-Apache/2.0.59
download.bravesentry.com	69.50.175.181	Linux-ngnix/0.5.35
downloadfilesldr.com		**Adware, spyware, PUPs**
dplog.com	216.195.42.178	Linux-Apache/2.0.52
dvicodec.com	*n/a*	**Adware, spyware, PUPs**
ebalashka.com	*n/a*	**Adware, spyware, PUPs**
f3pj.com	*n/a*	
fklgjslkj.com	58.65.239.114	**Browser Exploits** Linux-Apache/2.2.6
free-porn-movies.info	74.54.43.2	**Adware, spyware, PUPs** Linux-Apache/1.3.39
getxxxmovies.net	*n/a*	
gigacodec.net	*n/a*	**Adware, spyware, PUPs**
guestinef.net	209.85.84.199	Linux-Apache/2.0.52
gwatturar.com	*n/a*	**Adware, spyware, PUPs**
hardcodec.com	*n/a*	**Adware, spyware, PUPs**
hardstream.cn	79.135.181.22	Linux-Apache/2
havephun.org	*n/a*	
hightstats.net	77.91.229.54	**Browser Exploits** FreeBSD-Apache
hqcodec.net	*n/a*	**Adware, spyware, PUPs**
hq-pharma.org	*n/a*	**Links to malicious domain loads.cc**
hyipmanager.org	*n/a*	
i28.a27.wrs.mcboo.com	194.90.224.86	Apache/2.0.63
iframe-revenue.com	*n/a*	
ihos.info	*n/a*	
j27.a27.wrs.mcboo.com	194.90.224.86	**Adware, spyware, PUPs** Apache/2.0.63
key-codec.com	*n/a*	**Adware, spyware, PUPs**
lapanaka.com	*n/a*	

loadbalanse.info	209.123.181.22	Linux-Apache/1.3.39
loads.cc	*n/a*	**Adware, spyware, PUPs**
lotrain.cn	58.65.239.28	ngnix/0.5.33
mail.ru.updatedrivers.cn	195.5.116.244	ngnix/0.5.33
mediacount.net	*n/a*	**Browser Exploits**
megacodec.net	*n/a*	**Links to malicious domain dvdaccess.net** **Adware, spyware, PUPs**
mpegcodec.net	*n/a*	**Adware, spyware, PUPs**
msiesettings.com	*n/a*	**Browser Exploits**
mssystem.info	69.41.164.187	**Adware, spyware, PUPs** Linux-Apache/2.0.52
n26.a27.wrs.mcboo.com	194.90.224.86	**Adware, spyware, PUPs** Apache/2.0.63
nikitka.org	*n/a*	
otlili.cn	202.73.56.150	**Browser Exploits** FreeBSD-ngnix/0.6.25
plus-codec.com	*n/a*	**Adware, spyware, PUPs**
popups.ru	217.16.26.233	**Browser Exploits** Linux-ngnix/0.5.35
porn--movies.info	*n/a*	
prettycodec.com	*n/a*	**Adware, spyware, PUPs**
rezultsd.info	72.232.247.242	FreeBSD-ngnix/0.6.6
service-porn.com	64.28.185.77	**Adware, spyware, PUPs** FreeBSD-Apache/2.0.59
softspydelete.com	209.85.84.167	**Browser Exploits** Linux-Apache/2.0.52
speedofsearching.cn	*n/a*	
spywaresoftstop.com	*n/a*	**Adware, spyware, PUPs**
statofcountry.cn	*n/a*	
tds.free-porn-movies.info	74.54.43.2	**Adware, spyware, PUPs** Linux-Apache/1.3.39
tds.iframe-revenue.com	*n/a*	
thesuperxxx.com	69.50.188.5	**Links to malicious websites vac-soft.com, videowebsoft.com**
traff.cc	*n/a*	
traff.justcount.net	195.93.218.56	**Adware, spyware, PUPs** Linux-Apache/1.3.39
vac-soft.com	*n/a*	**Adware, spyware, PUPs**
vacwebsoft.com	*n/a*	**Adware, spyware, PUPs**
verymonkey.com	*n/a*	
videowebsoft.com	*n/a*	**Adware, spyware, PUPs**
vir-hazard.jino-net.ru	217.107.217.27	Linux-ngnix/0.3.30
www.anti-virus-pro.com	209.8.47.188	Linux-Apache/2.2.3
www.a.serviceupdate.cn	79.135.181.26	Linux/Apache

www.ebalashka.com	*n/a*	
www.porn-party.net	64.28.178.226	FreeBSD-Apache/2.0.59
www.super-figura.com	*n/a*	
www.thefilmsproduction.com	*n/a*	
www.thesuperxxx.com	69.50.188.5	FreeBSD-ngnix/0.6.16
www.uebashka.com	209.160.65.43	Linux-Apache/2
xabmiphabh.cn	85.255.121.195	Linux-Apache/2.2.6
x-victory.ru	203.117.111.106	**Phishing, adware, spyware, PUPs, browser exploits** Linux-Apache/2
yiweuryipeorigwergw4.narod.ru	213.180.199.45	FreeBSD-ZX_Spectrum/1997
ymq.a27.wrs.mcboo.com	194.90.224.86	**Adware, spyware, PUPs**

Table 3: Sample Domain Name Analysis

These domains appeared in the “Host: ” field of the TCP/80 HTTP request. It is therefore possible to detect the samples in question by monitoring Intrusion Detection Systems for “Host: <domain_name>” in outbound HTTP requests.

Affiliated Autonomous System Names (ASN)

Based on the IP address resolved from the above 80 domain names, investigations into activity on the following ASNs may be warranted.[44]

Autonomous System	***Occurrences***	***AS Name***	***Country***
27595	9	INTERCAGE	HK
1680	4	Netvision	IL
13767	3	DataBank Holdings, Ltd.	US
39823	2	COMPIC Ltd.	EE
41947	2	WEBALTA	RU
9121[45]	2	TTNET	TR
21844	2	The Planet	US
36420	2	Everyones Internet	US
44398	1	Buildhouse	UK
18106	1	Viewqwest	SG
4657	1	Starhub Internet	SG
8001	1	Net Access Corporation	US
14361	1	HopOne Internet Corporation	US
3491	1	Beyond the Network, Inc	US
13238	1	Yandex, LLC	RU
6461	1	Metromedia Fiber Network	US
14779	1	Inktomi Corporation	US

8342	1	RTComm.RU	RU
25532	1	Masterhost Autonomous Systems	RU
28753	1	NETDIRECT Frankfurt, DE	DE
33210	1	1-800-HOSTING, Inc.	US
23393	1	ISPrime, Inc	UK
3549	1	Global Crossing, Ltd.	SE

Table 4: Affiliated ASN Analysis

As testimony to David Bizuel’s RBN research, three ASN entries presented in Table 4 also appeared in his top 20 RBN affiliated ranges list.[46] The ASNs appearing in both lists belonged to: HostFresh, Everyones Interent and The Planet.

Final Thoughts and Conclusions

88.255.90.0/24 and **88.255.94.0/24**, registered to Abdallah Internet Hizmetleri in Rize, Turkey have previously been assessed as being affiliated with the Russian Business Network (RBN).[47] Analysis of 1,700 related pieces of malicious code obtained by The Shadowserver Foundation, in conjunction with Internet and passive DNS research implies that at the very least segments of AIH are not an incidental source of cyber crime, but instead act a thriving hub in the cogs of the RBN; propagating many different variants of malicious code, browser exploits, adware, spyware, pornography, spam, fraud and money laundering.

"If you track spam, phishing, malware and other cybercrime then sooner or later you will come across illegal content or activity hosted on [AIH]" [48] *~ Joewein.de LLC*

This 1,700 strong set of malicious code once again demonstrates that cyber criminals have no geographic boundaries. Domain and affiliated AS name analysis presented in this paper offers but a small glimpse into the global web of today's hostile cyber landscape. Suspect domain names in this sample set currently reside in the United Kingdom, United States, Sweden, Germany, Estonia, Singapore, Israel, Hong Kong, Turkey and of course, Russia. As such, it is becoming increasingly difficult to differentiate between the criminals and the victims.

Finally, fuzzy hash testing continues to appear to be a viable method of aggregating large sets of unidentified malicious code into clustered families. While this does not assist in identifying the particular functions of any given cluster, it stands to reason that with higher matching percentages within a given cluster it should be possible to infer the functions of all clustered samples by discerning the functions of a single member. With even larger sample sets of fuzzy hash data, it may also be possible to draw relationships between clusters of malicious code and their particular authors. But such is a topic for another time…

References

[1] Bizuel, David. *“RBN study – before and after”.* http://bizeul.org/files/RBN_study.pdf

[2] Picture from Wikipedia. *“Russian Business Network.” http://en.wikipedia.org/wiki/Russian_Business_Network*

[3] Washington Post. *“Russian Business Network: Down, But Not Out.”*

http://blog.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html?nav=rss_blog

[4] SecurityZone.Org. *“Some TurkTelecom IP Ranges Aren’t Your Friends.”* http://www.securityzone.org/?p=26

[5] Bizuel, David. *See note 1.*

[6] Geographic location provided by http://www.MaxMind.com

[7] Spacequad AntiSpam Services. *“Open letter to ICANN and all the Registrars.”*

http://www.spacequad.com/article.php/open_letter

[8] The Register. “Controversial Russian Business Network Drops Offline”

http://www.theregister.co.uk/2007/11/08/rbn_offline/

[9] Statistics presented represent detections by Avira AntiVir, which was found to have the highest detection percentage against this particular set of malicious code.

[10] The Shadowserver Foundation. *“Clarifying the ‘guesswork’ of criminal activity.”*

http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf

[11] Packer Detection provided by Team Furry’s Sigbuster Utility (http://www.teamfurry.com) and PEiD (http://peid.has.it/)

[12] For more information on fuzzy hash analysis techniques, see “Fuzzy Clarity.”

http://www.shadowserver.org/wiki/uploads/Information/FuzzyHashing.pdf

[13] Graph generated by GraphViz: http://www.graphviz.org/

[14] Passive DNS refers to caching of DNS lookups and is provided by to The Shadowserver Foundation by RUS-CERT (http://cert.uni-stuttgart.de)

[15] Joewein.de LLC. *“AbdAllah Internet Hizmetleri.”* http://www.joewein.net/fraud/host-abdallah-internet.htm.

[16] Dancho Danchev’s Blog. *“Scammy Ecosystem.” http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html*

[17] Joewein.de LLC. *See note 15.*

[18] Bobbear.co.uk. *“Progold Investments Fraud.” http://www.bobbear.co.uk/progoldinvestments.html*

[19] Dancho Danchev’s Blog. *“Possibilty Media’s Malware Fiasco.”*

http://ddanchev.blogspot.com/2007_10_01_archive.html

[20] Google Cache for Malwaredomainlist.com. *“Malware Domain List.”*

http://64.233.169.104/search?q=cache:Q5apaNamlj8J:www.malwaredomainlist.com/mdl.php%3Fsort%3DDomain

%26search%3D%26colsearch%3DAll%26ascordesc%3DASC%26quantity%3D100%26page%3D58+88.255.90.138&hl=en&ct=clnk&cd=4

[21] Bobbear.co.uk. *“Happy Kinds Fraud.”* http://www.bobbear.co.uk/happykids.html

[22] Boardreader.com. *“Phishing Report.”* http://boardreader.com/tp/phishing+report.html

[23] 411Buzz. *“Get Paid Forums.”* http://getpaidforum.com/forums/index.php?s=ddb53504ef8a99239ac88cc59e57d963&showtopic=508560&pid=4899207&st=0&#entry4899207

[24] Joewein.de LLC. See note 15.

[25] Threat Expert. *“ThreatExpert Report – Trojan-Downloader.Win32.Small.cxx”* http://www.threatexpert.com/report.aspx?uid=79a4e97c-fca5-4a0f-ae65-3ea604cf7857

[26] Spywaredetector.net. *“Remove Matcash.”* http://spywaredetector.net/spyware_encyclopedia/Trojan.Matcash.htm

[27] McAfee, Inc. *“spyguardpro.com | Web Safety Rating.”* http://www.siteadvisor.com/sites/spyguardpro.com/postid/?p=546905

[28] NTUA.GR. *“sa-blacklist.”* http://ftp.ntua.gr/sa-blacklist/sa-blacklist.current.at-domains

[29] Google Cache for Autoshun.org. *”Shunlist as of February 19, 2008.”* *http://64.233.167.104/search?q=cache:WlwSGdGOEdoJ:www.autoshun.org/files/shunlist.csv+88.255.90.170&hl=en&ct=clnk&cd=1&gl=us&client=firefox-a*

[30] The Spamhaus Project. *“SBL.”* http://www.spamhaus.org/sbl/sbl.lasso?query=SBL59440

[31] Google Cache for Malwaredomainlist.com. *“Malware Domain List.”* http://64.233.167.104/search?q=cache:Q5apaNamlj8J:www.malwaredomainlist.com/mdl.php%3Fsort%3DDomain%26search%3D%26colsearch%3DAll%26ascordesc%3DASC%26quantity%3D100%26page%3D58+88.255.90.214

[32] Google Cache for AbuseButler. *“AbuseButler – Spamvertised Domains.”* http://64.233.167.104/search?q=cache:G_m_UHtXO1gJ:spamvertised.abusebutler.com/spamvertised.php%3Frep%3Dlasthour+88.255.90.214

[33] Joewein.de LLC. *See note 15.*

[34] Dancho Danchev’s Blog. *See note 16.*

[35] ThreatExpert.com. *“Threat Expert Report: Tibs-Packed.”* *http://www.threatexpert.com/report.aspx?uid=15861464-1259-42cf-bbae-348940c9546a*

[36] ThreatExpert.com. *“Threat Expert Report: Email-Worm.Win32.Zhelatin.ne”* http://www.threatexpert.com/report.aspx?uid=07035b8f-dfdf-4afd-b276-722db6bebca1

[37] Wildeep. *“Potential Hack Attempt.”* http://wordpress.org/support/topic/146440

[38] Bobbear.co.uk. *“Ultragame.”* http://www.bobbear.co.uk/ultragame.html

[39] Patrick Jordan. *"Example of a money transfer scam site." http://sunbeltblog.blogspot.com/2007/11/example-of-money-transfer-scam-site.html*

[40] Dancho Danchev's Blog. *"I See IFRAMEs Everywhere – Part Two." http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html*

[41] Dancho Danchev's Blog. *"The New Media Malware Gang – Part Two."* http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

[42] Dancho Danchev's Blog. *"RBN's Fake Account Suspended Notice."* http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

[43] Results gathered from Netcraft (http://netcraft.com) and McAfee, Inc's SiteAdvisor (http://www.siteadvisor.com)

[44] ASN Information provided by The Shadowserver Foundation (http://www.shadowserver.org) & The CIDR Report (http://cidr-report.org)

[45] AS9121 affiliates represent IP addresses in AS9121 that did not fall into either 88.255.90.0/24 or 88.255.94.0/24.

[46] Bizuel, David. *See note 1.*

[47] Bizuel, David. *See note 1.*

[48] Joewein.de LLC. *See note 15.*