HostExploit's Worldwide Cybercrime Series

Top 50 Bad Hosts and Networks
1st Quarter 2011 - Report

HOST exploit

SITEVET

Table of Contents

Top 50

CyberCrime Series

Bad Hosts and Networks

Backing from

nominet trust

www.nominettrust.org.uk

Edited by

- Jart Armin

Review

- Dr. Bob Bruen
- Raoul Chiesa

Contributors

- Philip Stranger
- James McQuaid
- Steve Burn
- David Glosser
- Brynd Thompson
- Will Rogofsky

Comparative Data

- AA419
- Abuse.CH
- CIDR
- Clean-MX.DE
- Emerging Threats
- Google Safebrowsing
- HostExploit
- hpHosts
- ISC
- KnujOn
- MaliciousNetworks (FiRE)
- MalwareDomains
- MalwareList
- MalwareURL
- RashBL
- Robtex
- Shadowserver
- SiteVet
- Spamhaus
- StopBadware
- SudoSecure
- Sunbelt
- Team Cymru
- UCE Protect

Bad Hosts and Networks

Overview

HostExploit presents the first quarter 2011 report in our ongoing series on the Top 50 Bad Hosts and Networks. This is based on the analysis of the 37,271 currently announced public ASes (Autonomous Systems), exchanging routing information with each other over the Internet, and providing the mainstay for this research.

It has been a busy quarter since the last report in early January. A number of major hacks and intrusions into the corporate world, some using methods that were hitherto considered to be 'low level' intrusion techniques, show a continuing interest in the capturing of data in its many and various forms.

To the HostExploit team, it remains clear that where the source of a crime can be clearly traced – the 'who' of cybercrime – then there can be few arguments against the removal of that source. This is not to say that takedowns alone are sufficient to cleaning up the internet, but when there is no collateral damage, it is a positive step. However, prevention is always preferable to takedowns.

As always we concentrate on the hosts providing the services that cybercriminals make use of in carrying out their operations. By revealing the worst hosts in this respect we hope that steps will be taken by those hosts to actively clean up their servers.

Crime Servers, LizaMoon & 32 Bit ASNs

How many victims of the LizaMoon SQL injection attack have there been? The jury may still be out on that question with estimates varying from thousands of infected websites to hundreds of thousands. What we do know is that a major Command and Control center (C&C) for LizaMoon is no longer active.

A core C&C for the LizaMoon virus was being served from hosting provider AS3.721 (AS197329) ZAMANHOST-AS but HostExploit is very happy to report that this hosting provider is now **offline**. With the cutting off of this core crime server countless potential victims will be prevented from falling for its scareware tactics that encouraged users to install 'anti-virus software' that is not needed.

Google researcher Niels Provos reported in Lizamoon SQL Injection Campaign Compared that the virus appeared to have had a recent resurgence of activity after previously peaking in October.

This is a fairly rare example of a 32-bit ASN serving cybercriminal activity. Traditionally, AS numbers have been 16-bit, giving 2^{16} possibilities; from AS0 to AS65535. Around 80% of these AS numbers (60% public; the remainder private and IANA-reserved) have already been assigned. It is estimated 16-bit ASNs will be exhausted by late 2011. The introduction of 32-bit ASNs increases the supply of AS numbers to over four billion.

So why has so little cybercriminal activity been hosted on 32-bit ASNs to date? The main reason is cost. To run an AS with a 32-bit ASN, all network hardware at the border (routers, switches, hubs etc) have to be 32-bit compatible. A lot of new hardware is still not 32-bit compatible, so this drives up the hardware costs. In addition, all direct upstream ASes must be running 32-bit compatible hardware, and a cybercriminal will usually have no control over this factor.

Cybercrime has become a ruthless business operating on efficient economics and so there is usually no benefit to the extra hardware costs. However, the majority of community blacklisting services are yet to be updated to full 32-bit ASN compatibility. This provides an incentive to cybercriminals to invest extra funds in 32-bit ASN compatible hardware as the lack of community support provides a shield to their activities.

For this reason, we would urge all community services to ensure their services are compatible with 32-bit ASNs as soon as possible.

Spam & Rustock

Fluctuation in levels of spam activity and how this impacts on individual hosting providers is a feature of our reports. Notable events, such as a takedown or efforts to clean up by hosting providers, can have a big impact on figures by showing a sudden decrease in spam detected as being served or vice versa.

Shortly after the release of our last report in January 2011, the #1 Bad Host – the Russian-based web host AS29106 Volgahost, identified for its levels of C&C botnets and other cybercriminal activities – was taken down through a joint community action.

In March 2011, Microsoft Corp, in a month-long joint operation with law enforcement, disrupted the Rustock botnet, decapitating it from its peers and hosting providers.

The tables in Section 6 show the hosting providers with the biggest drops in spam and conversely those with the biggest increases since the previous quarter's report.

The Rustock botnet was responsible for such a large volume of spam that by simply looking at the biggest drops in overall spam, we are able to identify many of the hosts that were involved in the botnet, mainly through zombie servers. This demonstrates the power of using a quantitative numerical index such as our HE Index, as it enables rapid identification of patterns without looking at the content itself.

Of note, with a 96-percent decrease, is a Russian mobile Internet provider AS42115 Bashcell. Of the top 5 most significant drops two are based in Russia, one each in Brazil, Bosnia Herzegovina, and Yemen. Of note, the top 20 biggest drops in spam five are based in the Ukraine.

On the other end of the spectrum, the large increases help to demonstrate that highly-organized spammers are quick to respond to changing situations and move to other hosting providers. The AS50693 Konsing Group in Serbia measured a spam increase of over 15,000 percent, while ironically AS9125 ORIONTELEKOM-AS Drustvo za telekomunikacije also in Serbia was one of the biggest drops. The hosts with the biggest increases simultaneously demonstrate the appearance of a fast-flux and mobile based botnets in parallel to dramatic increases in spam.

Advanced Persistent Threats (APT)

APT is still seen by some as a marketing hype by major security companies, however for research into cyber threat and host activity, this has proved a worthwhile description which we now include within the 'current events' cybercrime analysis section. These have been detected in various forms but perhaps the best described is within the recent Night Dragon Advanced Persistent Threat Report.

These are blended attacks, and Night Dragon targeted energy companies, resulting in the loss of sensitive information from the targeted organizations.

Mobile Malware & Pocket Botnets

With 310 million smartphones shipped in 2010 – of which 38% were Symbian, 23% Android, and 4% Microsoft – we have detected and confirmed over 27 various forms of mobile badware e.g. Android.Pjapps, iKee-B (Apple) and Mitmo (ZeuS smartphone variant).

We have seen the first SMS or mTan (mobile TAN, for Transaction Authentication Number) "Pocket Botnet" as predicted by Mulliner and Seifert at an IEEE International Conference in France last October in their presentation, Rise of the iBots.

This is also being utilized as a DDoS methodology, although in its early stages of usage. Although currently difficult to clarify the specific mobile badness from conventional sources, it is clear this is a major area of concern for Internet security and telecoms/hosts in general.

Although conventional detection methodologies are available, we have determined detection via packet analysis techniques have proved rewarding for locating the origins of an APT as well as determining the true nature of the attacks. This is also a scalable solution that can be applied to almost any existing infrastructure.

Editor's Note

In December 2009, we introduced the HE Index as a numerical representation of the 'badness' of an Autonomous System (AS). Although generally well-received by the community, we have since received many constructive questions, some of which we will attempt to answer here.

Why doesn't the list show absolute badness instead of proportional badness?

A core characteristic of the index is that it is weighted by the size of the allocated address space of the AS, and for this reason it does not represent the total bad activity that takes place on the AS. Statistics of total badness would, undoubtedly, be useful for webmasters and system administrators who want to limit their routing traffic, but the HE Index is intended to highlight security malpractice among many of the world's internet hosting providers, which includes the loose implementation of abuse regulations.

Shouldn't larger organizations be responsible for re-investing profits in better security regulation?

The HE Index gives higher weighting to ASes with smaller address spaces, but this relationship is not linear. We have used an "uncertainty factor" or Bayesian factor, to model this responsibility, which boosts figures for larger address spaces. The critical address size has been increased from 10,000 to 20,000 in this report to further enhance this effect.

If these figures are not aimed at webmasters, at whom are they targeted?

The reports are recommended reading for webmasters wanting to gain a vital understanding of what is happening in the world of information security beyond their daily lives. Our main goal, though, is to raise awareness about the source of security issues. The HE Index quantifies the extent to which organizations allow illegal activities to occur - or rather, fail to prevent it.

Why do these hosts allow this activity?

It is important to state that by publishing these results, HostExploit does not claim that many of the hosting providers listed knowingly consent to the illicit activity carried out on their servers. It is important to consider many hosts are also victims of cybercrime.

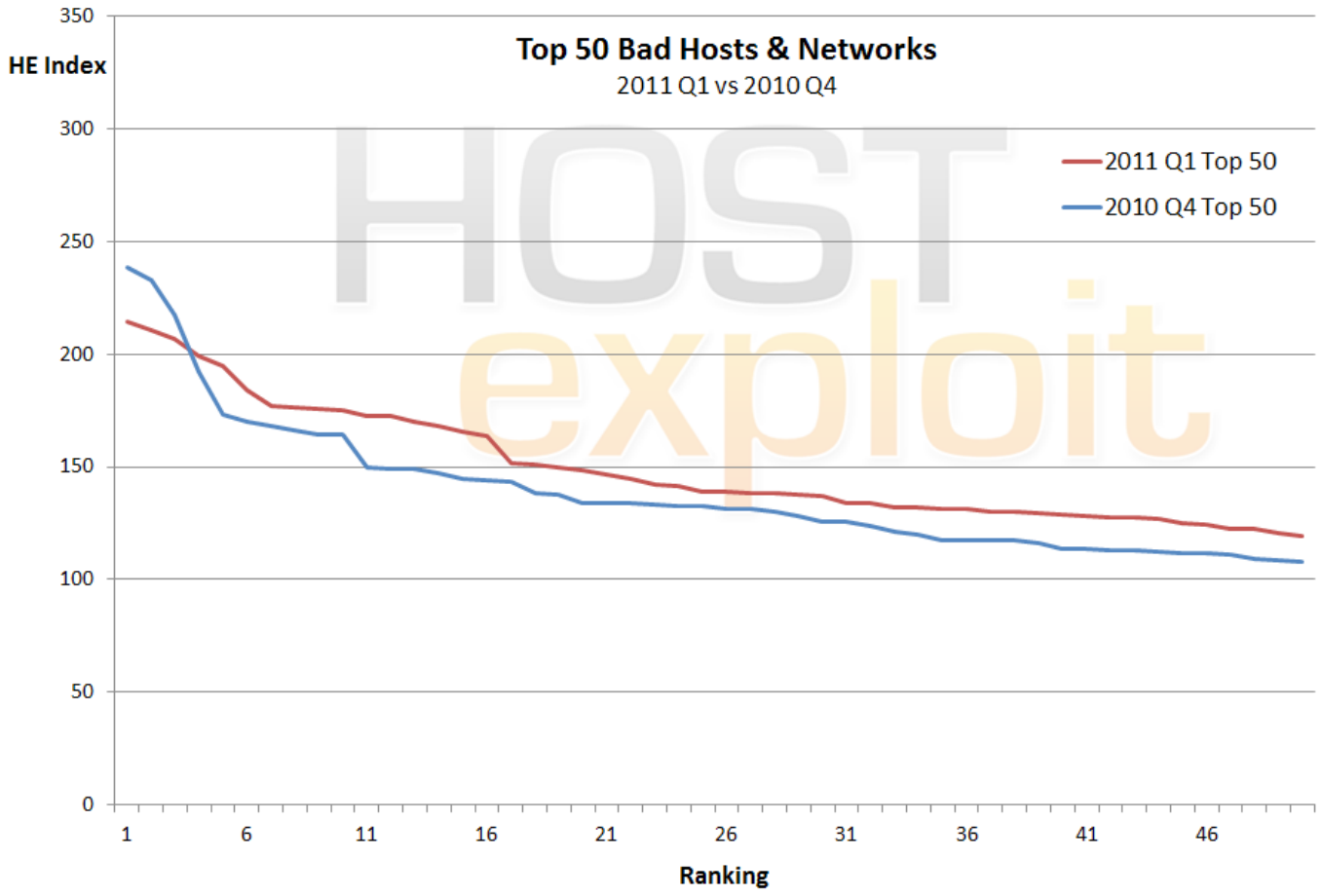
Further feedback is warmly welcomed

admin@hostexploit.com

2. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
1	214.3	41947	WEBALTA-AS OAO Webalta	RU	15,872
2	210.4	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,568
3	207.0	16138	INTERIAPL INTERIA.PL Autonomous System	PL	3,072
4	199.3	10297	ENET-2 - eNET Inc.	US	90,880
5	194.5	39150	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	RU	3,840
6	184.1	36408	ASN-PANTHER Panther Express	US	36,352
7	177.1	6697	BELPAK-AS BELPAK	BY	747,264
8	176.1	29629	INETWORK-AS IEUROP AS	FR	8,192
9	175.6	45899	VNPT-AS-VN VNPT Corp	VN	2,000,128
10	174.9	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	37,632
11	172.4	33626	OVERSEE-DOT-NET - Oversee.net	US	4,096
12	172.3	6851	BKCNET "SIA" IZZI	LV	49,152
13	170.1	9809	NOVANET Nova Network Co.Ltd... Futian District... Shenzhen,China	CN	11,008
14	168.0	21788	CDNETWORKS-GLOBAL unified ASN for CDNetworks...	US	278,528
15	165.5	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,546,752
16	163.8	28753	LEASEWEB-DE Leaseweb Germany GmbH (previously netdirekt...	DE	108,544
17	151.6	24940	HETZNER-AS Hetzner Online AG RZ	DE	437,248
18	150.8	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	109,515,264
19	149.9	16276	OVH OVH	FR	479,744
20	148.2	46844	ST-BGP - SHARKTECH INTERNET SERVICES	US	75,520
21	146.2	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	73,728
22	144.6	32613	IWEB-AS - iWeb Technologies Inc.	CA	218,112
23	142.0	13727	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024
24	141.8	33774	DJAWEB	DZ	91,392
25	139.0	39392	SUPERNETWORK-AS SuperNetwork s.r.o.	CZ	49,664
26	138.9	50693	KONSING-GROUP Konsing group doo	RS	2,048
27	138.4	6849	UKRTELNET JSC UKRTELECOM,	UA	1,526,272
28	138.1	30058	FDCSERVERS - FDCservers.net	US	210,176
29	137.4	13174	MTSNET OJSC "Mobile TeleSystems" Autonomous System	RU	24,064
30	137.1	19318	NJIIX-AS-1 - NEW JERSEY INTERNATIONAL INTERNET EXCHANGE LLC	US	89,856
31	133.9	36057	WEBAIR-AMS Webair Internet Development Inc	US	29,440
32	133.8	49469	SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup SRL	RO	1,792
33	132.2	36752	YAHOO-SP1 - Yahoo	US	109,312
34	131.9	31133	MF-MGSM-AS OJSC MegaFon Network	RU	13,056
35	131.6	29182	ISPSYSTEM-AS ISPsystem Autonomous System	RU	35,328
36	131.5	17974	TELKOMNET-AS2-AP PT Telekomunikasi Indonesia	ID	3,398,656
37	130.2	49981	WORLDSTREAM WORLDSTREAM AS	NL	11,008
38	129.9	32475	SINGLEHOP-INC - SingleHop	US	216,064
39	129.2	36167	NETRIPLEX01 - NETRIPLEX LLC	US	45,568
40	128.8	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	779,008
41	128.3	26496	PAH-INC - GoDaddy.com, Inc.	US	1,111,296
42	127.7	28299	CYBERWEB NETWORKS LTDA	BR	19,968
43	127.6	24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	1,746,944
44	126.6	8560	ONEANDONE-AS 1&1 Internet AG	DE	357,888
45	124.8	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	PK	2,287,616
46	124.1	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	48,640
47	122.7	15169	GOOGLE - Google Inc.	US	284,416
48	122.2	37943	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology...	CN	4,096
49	120.8	32181	ASN-GIGENET - GigeNET	US	42,240
50	119.6	40634	FIRSTLOOK-COM - FirstLook, Inc.	US	512

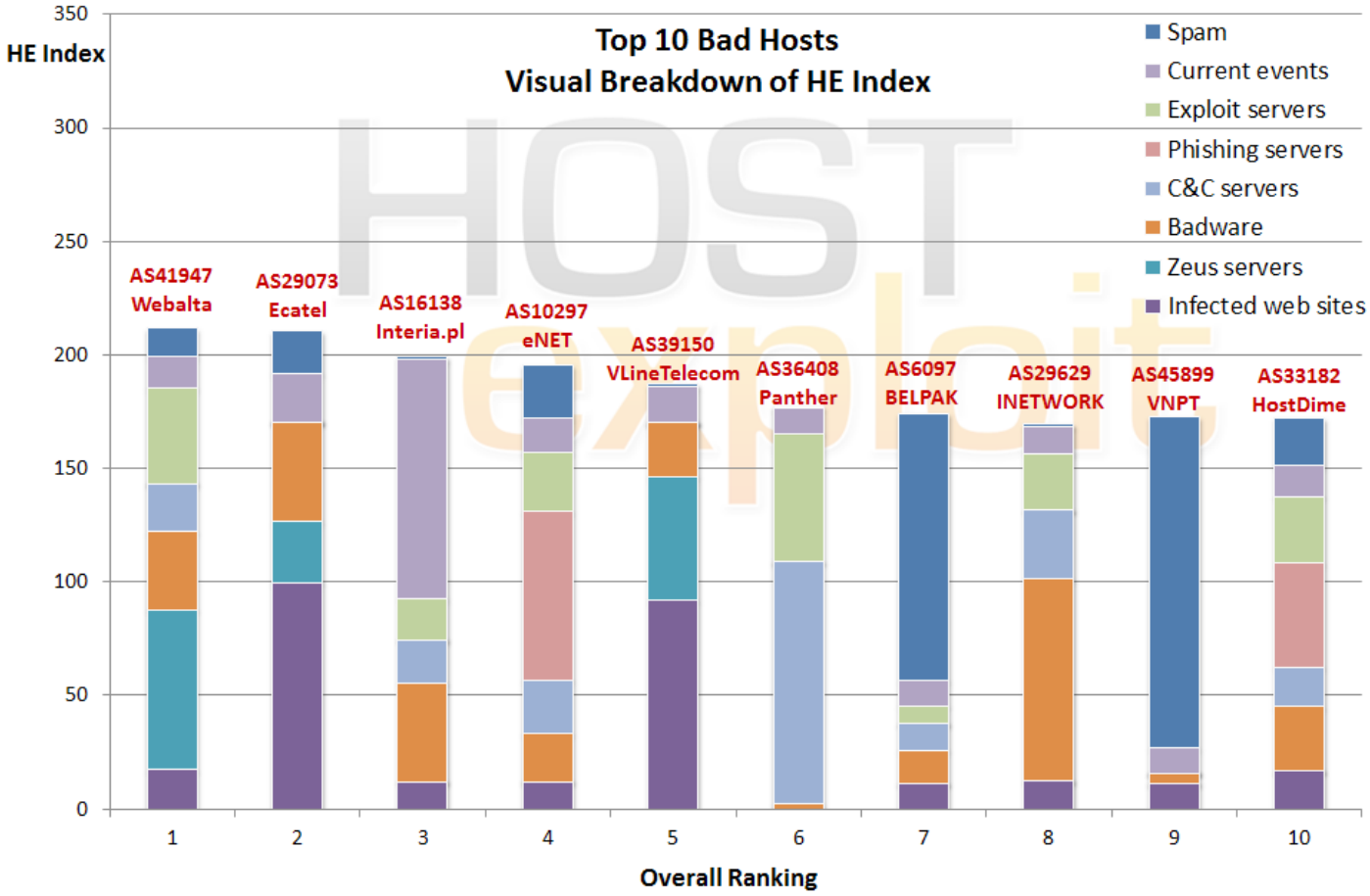
2010 Q4 to 2011 Q1 Comparison



A comparison of the 'Top 50 Bad Hosts' in December 2010 with March 2011.

On the whole, effective levels of badness increased over the quarter for the top 50.

Top 10 Visual Breakdown



The above visual breakdown of the HE Index in the Top 10 Bad Hosts effectively shows two things.

Firstly, that weighting ensures that the make up of the HE Index is a balanced measurement as no particular source of 'badness' dominates among the majority of the hosts.

Secondly, it demonstrates the breakdown of the HE Index for each specific AS in the Top 10, which shows us why it is ranked so highly.

For instance, it can be seen that AS41947 Webalta (RU) is ranked #1 due mainly to its hosting of Zeus servers and exploit servers, as well as smaller concentrations of spam, C&C servers, badware and infected web sites.

AS45899 VNPT (VN) has moved back into the Top 50 almost entirely due to expectionally high concentrations of spam serving.

What's New?

5.1. Overview

	Previous Quarter - Q4 2010			Current Quarter - Q1 2011		
	ASN	Name	Country	ASN	Name	Country
#1	29106	Volgahost	RU	41947	Webalta	RU
#2	29073	Ecatel	NL	29073	Ecatel	NL
#3	21740	eNom / DemandMedia	US	16138	Interia.pl	PL
#1 for Spam	31133	MegaFon	RU	45899	VNPT	VN
#1 for Botnets	36408	CDNETWORKS-GLOBAL	US	36408	Panther Express	US
#1 for Zeus Botnet	20564	Informex	UA	49469	Sa Nova Telecom	RO
#1 for Phishing	10297	ENET-2 - eNET Inc.	US	10297	ENET-2 - eNET Inc.	US
#1 for Exploit Servers	13100	Data Electronics Group	IE	21607	DeployLinux	US
#1 for Badware	21740	eNom / DemandMedia	US	33626	Oversee.net	US
#1 for Infected Sites	6851	BKCNET "SIA" IZZI	LV	6851	BKCNET "SIA" IZZI	LV
#1 for Current Events	16138	Interia.pl	PL	16138	Interia.pl	PL

5.2. Top 10 Newly-Registered Hosts - In Q1 2011

HE Rank	HE Index	AS number	AS name	Country	# of IPs
92	98.3	47306	ISEC-AS The International Scientifical and Educational Centre	UA	256
309	67.4	42741	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	RO	1,280
359	64.0	43134	COMPLIFE-AS CompLife Ltd	MD	512
657	52.9	20228	PACNET-MX - Pacnet, S.A. de C.V.	US	12,288
677	52.2	16109	INCA-AS Informational and Commercial Agency "INCA" LTD	UA	256
827	47.5	8514	INODE UPC Austria GmbH	AT	0
1481	34.1	51786	SATURN-R-GROUP LLC Telecom-Group-Saturn_R	RU	1,536
1779	29.5	55831	AIRCEL-IN Aircel Ltd.	IN	177,152
1854	28.6	51362	BESTISP-AS PE Yastremskiy Leonid Stepanovich	UA	512
1927	27.7	52116	ORIONTELEKOMTIM-AS Orion Telekom Tim d.o.o.Beograd, Nehruova 93A	RS	8,192

Note: by end of Q1 2011 there were **37,271** ASes; an increase of **900** from end of Q4 2010

5.3. Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-50.9%	3	217.4	72	106.6	21740	ENOMAS1 - eNom, Incorporated	US	19,456
-45.4%	78	95.4	678	52.1	13100	Data Electronics Group, Data Exchange...	IE	12,288
-44.2%	20	134.1	222	74.8	18866	ATJEU - Atjeu Publishing LLC	US	13,312
-43.0%	148	80.7	885	46.0	29076	CITYTELECOM-AS Citytelecom.ru	RU	42,496
-38.5%	166	78.2	801	48.1	9120	COHAESIONET Cohaesio A	DK	17,920
-35.4%	123	84.0	627	54.3	45774	SPIDIGO-AS-IN Chandra Net Pvt. Limited...	IN	11,264
-33.0%	52	105.8	258	70.8	47869	NETROUTING-AS Netrouting Data...	NL	16,384
-31.2%	16	143.9	90	99.0	48876	INTERA-AS Takomi Ltd	RU	512
-31.1%	99	88.7	413	61.1	17552	TRUE-AS-AP True Corporation Co.,Ltd.	TH	1,591,040
-30.1%	189	76.1	652	53.2	47142	STEEPHOST-AS SteepHost... Datacentre	UA	2,304

Many forms of badware can be inextricably linked, appearing as an intractable issue to some hosts. However, we applaud the efforts of the ASes in the above table - all have dramatically reduced their badness levels in the three months since our Q4 2010 quarter report was published.

These 10 hosts vary significantly in size, location, area of business and categories of badness improved. This alone shows that is possible under all circumstances to improve the situation with extra effort and some out-of-the-box thinking.

Noteworthy improvements include :

AS21740 eNom – the domain name registrar arm of Demand Media – having previously been ranked as high as #1, is down to #72, with the removal of general badware, malware and Zeus hosts.

AS13100 Data Electronics Group, having been #1 for exploit serving in the previous quarter, is down to #678 overall.

"We've worked very hard on cleaning things up. We implemented a base security measure for orders originating from certain countries, familiar names, manual payment methods etc. It's become more of a daily task now to clean things up."

AS47869 Netrouting - down from #52 to #258.

5.4. Deteriorated Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
12,646.5%	28,462	1.1	26	138.9	50693	KONSING-GROUP Konsing group doo	RS	2,048
175.6%	741	48.5	32	133.8	49469	SA-NOVA-TELECOM-GRUP-SRL Sa	RO	1,792
153.5%	898	44.3	62	112.3	47764	NETBRIDGE-AS... Mail.Ru	RU	16,512
134.6%	763	48.2	59	113.0	9280	CIA-AS connect infobahn australia	AU	8,960
129.1%	994	41.9	98	96.1	51559	NETINTERNET Netinternet Bilgisayar	TR	11,520
128.6%	1,115	39.6	119	90.5	25406	SPLIUS-AS SPLIUS, UAB	LT	53,248
125.4%	1,399	34.6	195	78.0	42363	PHPNET-AS AS for PHPNET	RU	1,024
117.0%	884	44.7	95	97.1	36954	MLTL-AS	NG	28,928
114.8%	1,298	36.4	191	78.1	51699	ANTARKTIDA-PLUS-AS Antarktida	RU	256
106.4%	674	50.7	76	104.7	47781	ANSUA-AS PE Sergey Demin	UA	512

The hosts listed here are the ones with the most increased indexes since the previous quarter. Therefore, this list does not include newly-registered hosts.

Instead, see section 4.2 for newly-registered hosts with the highest badness levels.

The "standout" host this quarter is no doubt AS50693 Konsing Group. From relative anonymity in the previous quarter, it has climbed to #26 this quarter, almost entirely due to a huge rise in spam levels, taking it to the #2 host for spam.

The Serbian-registered AS has a small number of IPs (2,048 = /21 BGP prefix), for which the large increase is particularly worrying.

AS49469 Nova Telecom has arguably gone one "better" by climbing to #1 for Zeus hosting, from #741 overall last quarter. The Romanian-registered AS also has a small IP space, which is typical of most ASes hosting Zeus activity.

Spam & Impact of Rustock Takedown

Q4 2010 Spam Comparison

Fluctuation in levels of spam activity and how this impacts on individual hosting providers is a feature of our reports. Notable events, such as a takedown or efforts to clean up by hosting providers, can have a big impact on figures by showing a sudden decrease in spam detected as being served or vice versa.

Shortly after the release of our last report in January 2011, the #1 Bad Host – the Russian-based web host AS29106 Volgahost, identified for its levels of C&C botnets and other cybercriminal activities – was taken down through a joint community action.

In March 2011, Microsoft Corp, in a month-long joint operation with law enforcement, disrupted the Rustock botnet, decapitating it from its peers and hosting providers.

The tables in Section 6 show the hosting providers with the biggest drops in spam and conversely those with the biggest increases since the previous quarter's report.

The Rustock botnet was responsible for such a large volume of spam that by simply looking at the biggest drops in overall spam, we are able to identify many of the hosts that were involved in the botnet, mainly through zombie servers. This demonstrates the power of using a quantitative numerical index such as our HE Index, as it enables rapid identification of patterns without looking at the content itself.

Of note, with a 96-percent decrease, is a Russian mobile Internet provider AS42115 Bashcell. Of the top 5 most significant drops two are based in Russia, one each in Brazil, Bosnia Herzegovina, and Yemen. Of note, the top 20 biggest drops in spam five are based in the Ukraine.

On the other end of the spectrum, the large increases help to demonstrate that highly-organized spammers are quick to respond to changing situations and move to other hosting providers. The AS50693 Konsing Group in Serbia measured a spam increase of over 15,000 percent, while ironically AS9125 ORIONTELEKOM-AS Drustvo za telekomunikacije also in Serbia was one of the biggest drops. The hosts with the biggest increases simultaneously demonstrate the appearance of a fast-flux and mobile based botnets in parallel to dramatic increases in spam.

Biggest Increases

Spam Index			AS number	AS name	Country	# of IPs
Change	Previous	Current				
15,101.7%	4.0	600.8	50693	KONSING-GROUP Konsing group doo	RS	2,048
7,114.5%	1.8	129.8	8554	ATSAT TAS France	FR	28,416
3,178.8%	3.8	123.8	55386	INET Intercept,Inc.	JP	9,216
1,521.6%	6.7	108.1	50176	PRIZMA-AS Prizma CableTV-ISP	BY	1,536
1,281.0%	8.6	118.9	28769	STTK-AS SibTransTelecom Autonomous System	RU	20,992
811.8%	22.0	200.7	9988	MPT-AP Myanma Posts and Telecommunications	MM	256
788.6%	13.0	115.6	43998	TRKMETRO TRK Metro Ltd.	UA	2,048
370.4%	34.0	160.0	36887	DOPC-AS	NG	9,728
349.1%	24.0	107.8	38771	CYBERPLUS-AS-ID PT Cyberplus Media Pratama	ID	4,096
250.3%	34.7	121.6	42833	TELESWEET-AS Telesweet ISP	UA	49,152

Biggest Drops

Spam Index			AS number	AS name	Country	# of IPs
Change	Previous	Current				
-96.3%	133.3	5.0	42115	BASHCELL-AS Mobile TeleSystems OJSC	RU	2,048
-95.9%	111.7	4.5	53075	Holística Serviços de Telecomunicações e SCM Ltda	BR	4,096
-89.8%	100.8	10.3	51003	SKYLINE-NET Skyline LLC	RU	4,096
-86.3%	105.8	14.5	42450	TELEKABEL Telekabel d.o.o. Zenica	BA	12,288
-86.1%	230.1	32.1	12486	YEMENNET YT - YEMEN NET Autonomous Number	YE	55,552
-82.3%	113.3	20.0	21003	GPTC-AS	LY	361,472
-81.3%	100.3	18.7	48777	SEVNET PE Volodin Yuriy Volodimirovich	UA	2,048
-79.7%	131.2	26.7	42896	ACS-AS TOV "Research and Production Company...	UA	1,792
-75.3%	193.8	47.8	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,568
-73.6%	134.8	35.6	33576	DIGICEL ASN-Digicel	JM	92,160
-71.3%	182.3	52.3	28548	Cablevision, S.A. de C.V.	MX	131,072
-67.5%	119.6	38.9	9125	ORIONTELEKOM-AS Drustvo za telekomunikacije...	RS	90,112
-55.0%	230.7	103.9	30822	MAGEAL-AS Enterprise Mageal	UA	37,120
-54.7%	132.3	60.0	34990	SKYINET-AS SkyInet	UA	2,048
-54.6%	215.8	98.0	17552	TRUE-AS-AP True Corporation Co.,Ltd.	TH	1,591,040
-52.7%	108.4	51.3	51214	VIKS-NET Small Private Enterprise Viks	UA	512
-50.8%	118.8	58.4	43766	MTC-KSA-AS MTC KSA Mobile Telecommunication...	SA	1,536
-49.2%	279.8	142.2	18252	CAT-AS-AP The Communication Authoity of Thailand	TH	28,672
-48.7%	107.6	55.2	29180	O2-ONLINE-AS O2 Online (UK)	UK	61,440
-43.7%	118.8	66.8	35508	FORTE-AS Forte Communications Ltd. AS	BG	1,024

Country Analysis

Hosts in Top 50	Country	Total IPs within Top 50	Total Index	Average Index	Average Indexes by Category							
					Infected web sites	Zeus servers	Badware	C&C servers	Phishing servers	Exploit servers	Current events	Spam
20	UNITED STATES	5,110,016	2,903.4	145.2	151.7	72.3	196.2	187.6	180.3	294.2	134.7	69.1
5	RUSSIAN FED.	92,160	809.7	161.9	292.1	225.4	114.3	70.4	0.2	146.7	80.3	217.6
3	CHINA	109,530,368	443.1	147.7	174.7	46.0	389.6	122.6	44.1	239.4	105.6	57.4
3	GERMANY	903,680	442.0	147.3	230.3	112.3	170.2	153.1	143.2	242.6	120.4	91.1
2	NETHERLANDS	24,576	340.6	170.3	623.9	247.8	250.7	0.2	0.2	0.7	163.4	68.1
2	FRANCE	487,936	326.0	163.0	141.0	71.3	375.2	203.7	130.5	272.7	114.4	56.7
2	CANADA	219,136	286.6	143.3	150.0	0.1	352.2	180.8	224.3	131.3	107.0	49.6
1	POLAND	3,072	207.0	207.0	107.5	0.2	295.2	169.7	0.3	245.4	949.5	4.1
1	BELARUS	747,264	177.1	177.1	100.2	0.0	100.8	104.0	0.0	106.7	100.1	454.0
1	VIETNAM	2,000,128	175.6	175.6	100.1	0.0	31.2	0.0	0.0	0.0	100.1	562.9
1	LATVIA	49,152	172.3	172.3	922.4	0.1	196.8	0.1	0.1	0.3	182.2	68.3
1	ALGERIA	91,392	141.8	141.8	72.4	0.0	62.7	0.1	0.1	0.2	0.0	472.3
1	CZECH REPUBLIC	49,664	139.0	139.0	104.2	0.1	322.9	0.1	461.5	298.0	113.2	36.2
1	SERBIA	2,048	138.9	138.9	0.5	0.2	0.4	0.3	0.3	1.1	0.1	515.0
1	UKRAINE	1,526,272	138.4	138.4	103.3	146.0	103.3	0.0	0.0	109.0	100.8	289.3
1	ROMANIA	1,792	133.8	133.8	170.5	950.0	0.4	0.3	0.3	1.1	27.0	4.3
1	INDONESIA	3,398,656	131.5	131.5	100.1	0.0	100.2	0.0	0.0	0.0	100.1	360.4
1	BRAZIL	19,968	127.7	127.7	103.8	0.1	112.1	222.9	588.4	185.0	102.5	5.4
1	INDIA	1,746,944	127.6	127.6	100.1	0.0	100.1	0.0	0.0	0.0	100.0	345.6
1	PAKISTAN	2,287,616	124.8	124.8	72.1	0.0	31.2	0.0	0.0	0.0	0.0	429.4

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
35,642	0.45	2688	ASATTCA AT&T Global Network Services - LA	US	311,296
35,610	0.49	6203	ISDN-NET - The Nexus Group, Inc.	US	218,368
35,597	0.50	1294	PS-NETPLEX-AS - Perot Systems	US	199,936
35,544	0.56	5605	NETUSE NetUSE AG	DE	140,544
35,474	0.60	17645	NTT-SG-AP ASN - NTT SINGAPORE PTE LTD	SG	115,200
35,421	0.61	23329	AS-OPENACCESS - Open Access Inc.	US	112,384
35,320	0.70	6261	VISINET - NetTelcos	US	75,776
35,251	0.73	5738	SOVER-ASN - SoVerNet, Inc.	US	68,352
35,183	0.77	5109	AS-IDS-NET - Integrated Data Systems, LLC	US	61,440
34,954	0.86	40913	QTS-SJC-1 - Quality Technology Services Santa Clara, LLC	US	46,080

8.1. Why List Examples of Good Hosts?

It would be wrong to give the impression that service providers can only be judged in terms of badness. To give a balanced perspective we have pinpointed the 10 best examples of organizations with minimal levels of service violations. Safe and secure web site hosting environments are perfectly possible to achieve and should be openly acknowledged as an example to others.

Our table of 'good hosts' is testimony to the best practices within the industry and we would like to commend those companies on their effective abuse controls and management.

This is a regular feature of our 'bad hosts' reporting.

8.2. Selection Criteria

We apply the good host selection to ISPs, colocation facilities, or organizations who control at least 10,000 individual IP addresses. Many hosting providers shown elsewhere in this report control less than this number. However, in this context, our research focuses mainly on larger providers which, it could be argued, should have the resources to provide a full range of proactive services, including 24-hour customer support, network monitoring and high levels of technical expertise.

We also only included those ASes that act primarily as public web or internet service providers, although we appreciate that such criteria is subjective.

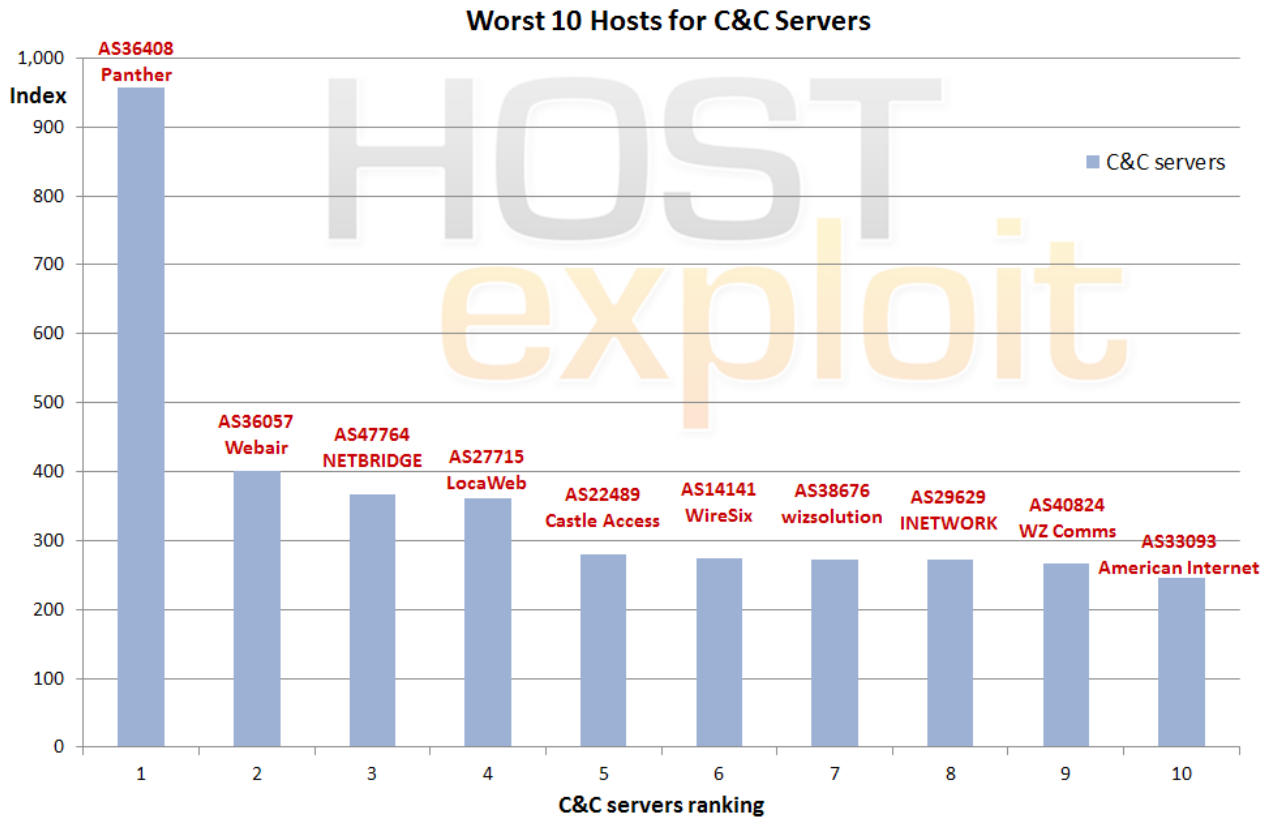
Bad Hosts by Topic

9.1.1. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
6	184.1	**36408**	ASN-PANTHER Panther Express	**US**	36,352	**958.0**
31	133.9	**36057**	WEBAIR-AMS Webair Internet Development Inc	**US**	29,440	**401.1**
62	112.3	**47764**	NETBRIDGE-AS Limited liability company Mail.Ru	**RU**	16,512	**367.6**
53	117.0	**27715**	LocaWeb Ltda	**BR**	58,880	**360.6**
55	115.3	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	45,312	**280.7**
215	75.9	**14141**	WIRESIX - WireSix, Inc.	**US**	7,680	**274.7**
405	61.6	**38676**	AS33005-AS-KR wizsolution co.,Ltd	**KR**	7,936	**273.2**
8	176.1	**29629**	INETWORK-AS IEUROP AS	**FR**	8,192	**271.7**
74	106.0	**40824**	WZCOM-US - WZ Communications Inc.	**US**	8,960	**267.3**
356	64.3	**33093**	AMERICAN-INTERNET-NEVADA - American Internet, Inc.	**US**	2,048	**245.3**

The trend continues from earlier reports with the apprearance of Botnet C&C Servers migrating towards larger hosts. Our own data is combined primarily with data provided by Shadowserver.

The position for the US appears to have deteriorated with 6 out of the top 10 worst hosts for botnet C&Cs . In Q4 2010 the US had only 4.

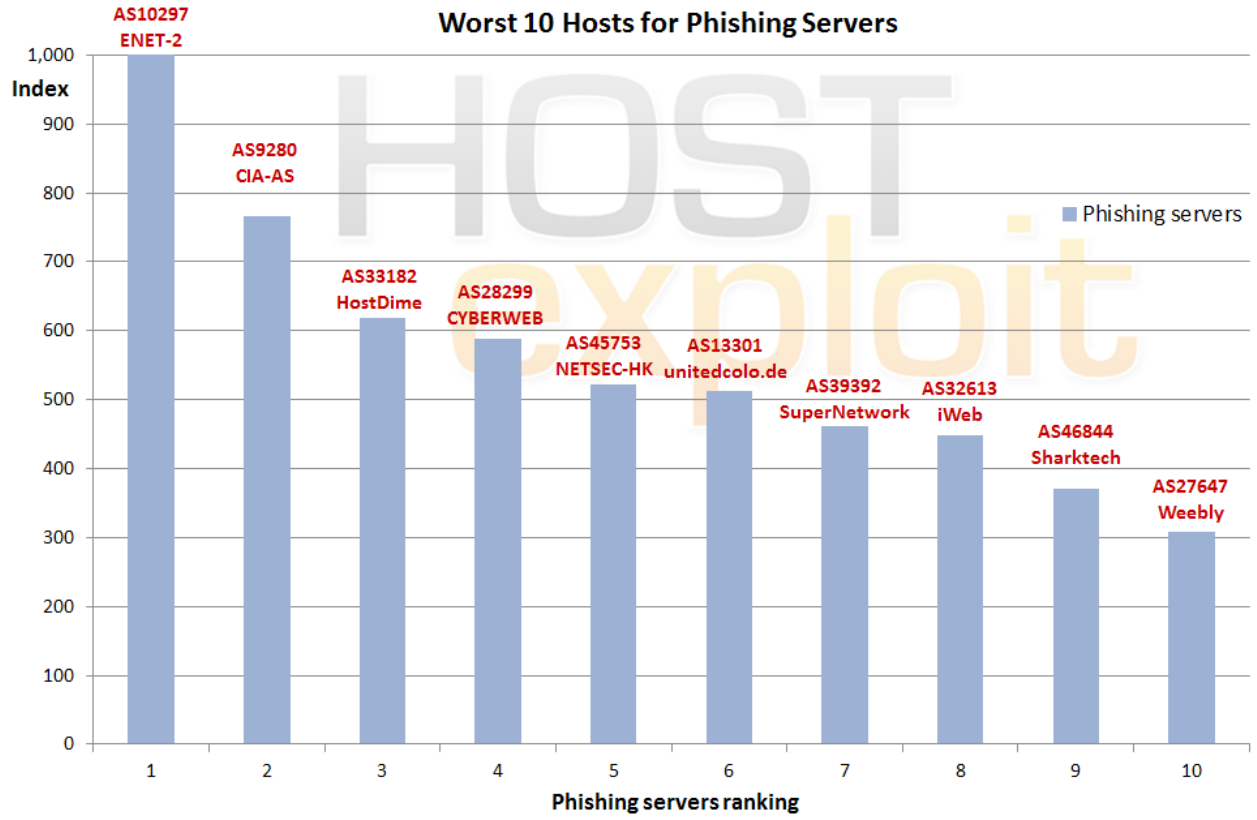


9.1.2. Phishing Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
4	199.3	**10297**	ENET-2 - eNET Inc.	**US**	90,880	**1000.0**
59	113.0	**9280**	CIA-AS connect infobahn australia (CIA)	**AU**	8,960	**766.1**
10	174.9	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	37,632	**617.7**
42	127.7	**28299**	CYBERWEB NETWORKS LTDA	**BR**	19,968	**588.4**
78	103.7	**45753**	NETSEC-HK Unit 1205-1207	**HK**	106,496	**521.7**
81	102.5	**13301**	UNITEDCOLO-AS Autonomous System of unitedcolo.de	**DE**	67,072	**512.2**
25	139.0	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	49,664	**461.5**
22	144.6	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	218,112	**448.2**
20	148.2	**46844**	ST-BGP - SHARKTECH INTERNET SERVICES	**US**	75,520	**370.8**
243	72.4	**27647**	WEEBLY - Weebly, Inc.	**US**	3,072	**307.9**

The proliference of Western countries in the Top 10 list for phishing can be explained by the need to establish false credibility. Phishing continues to be a cause for concern to banks and large corporations alike. Our results show that the top 3 phishing hosts are based in the US and Australia.

The necessary malware can reside on the enterprise's web site, or appears via cross-site scripting or header redirects. It would appear malware located on a server in western countries minimizes the awareness of both customers and target organizations.



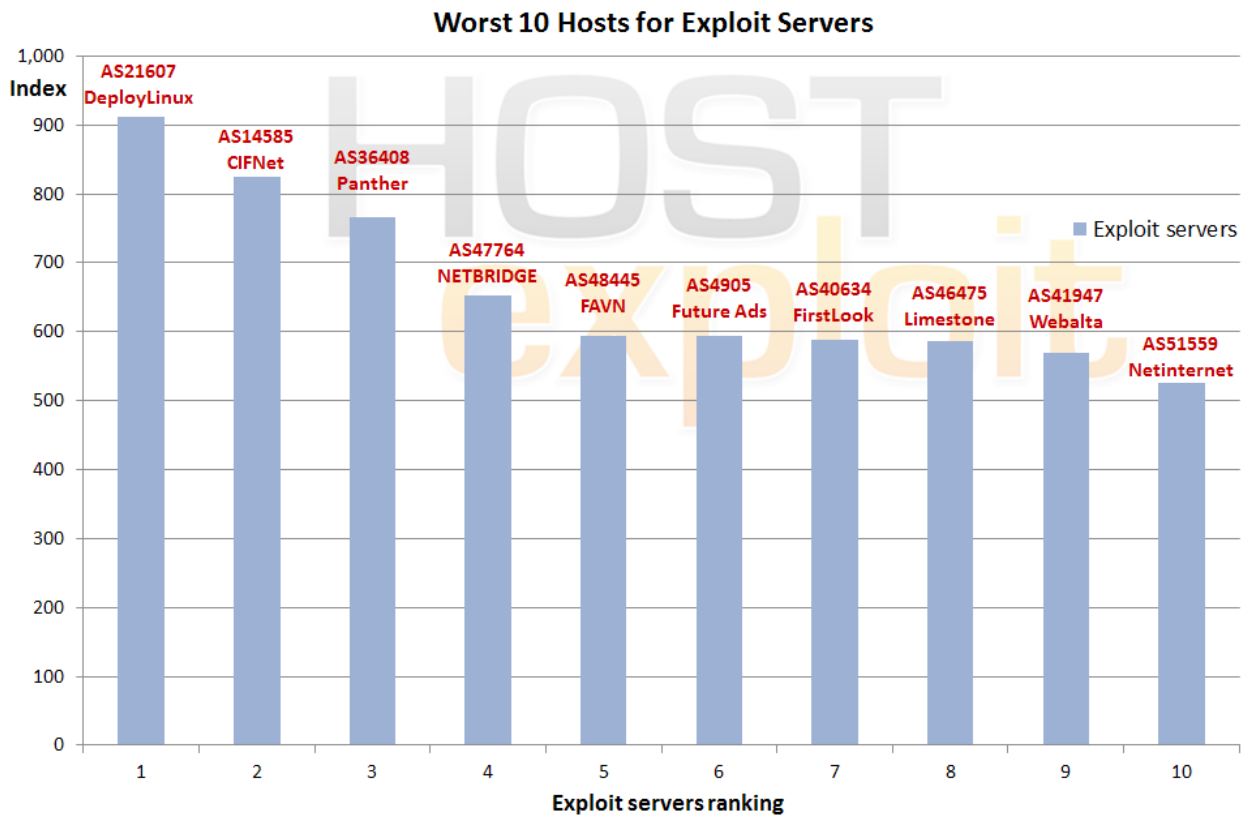
9.1.3. Exploit Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
60	112.7	**21607**	DEPLOYLINUX - DeployLinux Consulting, Inc	**US**	512	**911.9**
103	94.2	**14585**	CIFNET - CIFNet, Inc.	**US**	7,680	**825.5**
6	184.1	**36408**	ASN-PANTHER Panther Express	**US**	36,352	**766.3**
62	112.3	**47764**	NETBRIDGE-AS Limited liability company Mail.Ru	**RU**	16,512	**653.5**
133	87.9	**48445**	FAVN Favorit Network SL	**ES**	256	**593.7**
758	49.3	**4905**	FA-LAX-1 - Future Ads LLC	**US**	256	**593.7**
50	119.6	**40634**	FIRSTLOOK-COM - FirstLook, Inc.	**US**	512	**587.6**
21	146.2	**46475**	LIMESTONENETWORKS - Limestone Networks, Inc.	**US**	73,728	**585.8**
1	214.3	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,872	**569.4**
98	96.1	**51559**	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon...	**TR**	11,520	**526.2**

We consider the category of "Exploit Servers" to be the most important in the analysis of malware, phishing, or badness as a whole. Added weighting is given to this sector. Full detail of our methodology can be viewed in Appendix 2.

Many hosts and corporate servers deliver malware or undertake other malicious activity as a result of having been hacked and compromised. Useful information, victims' identities and other illicitly gained data are then directed back to these Exploit Servers using malware.

In contrast to spam hosts, Exploit Servers have until recently been entirely located in countries subject to lower levels of regulation. However, in this 4th quarter 2010 it should be noted 60% of the top 10 in this sector are located or reported as located in the US.



9.1.4. Botnet Hosting - Zeus

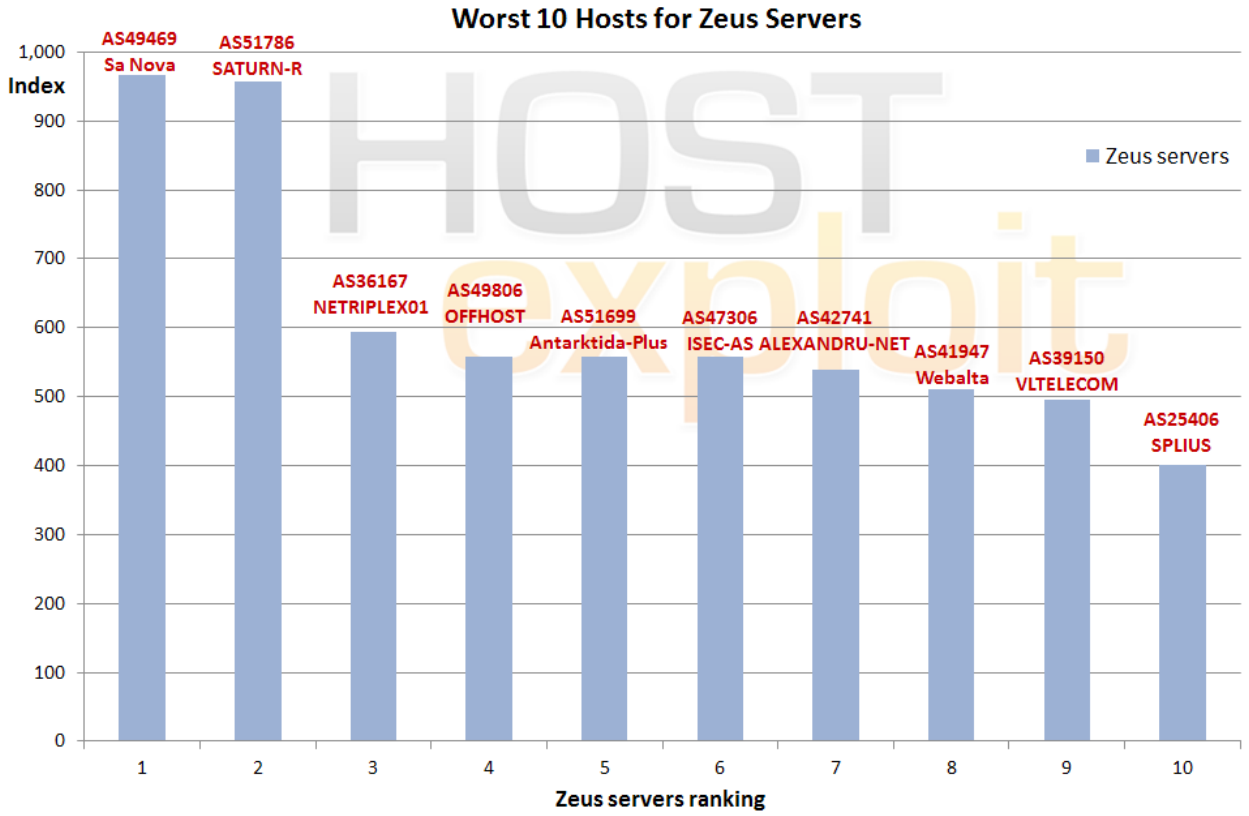
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
32	133.8	**49469**	SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup SRL	**RO**	1,792	**950.0**
92	98.3	**47306**	ISEC-AS The International Scientifical and Educational Centre	**UA**	256	**783.1**
1	214.3	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,872	**636.0**
39	129.2	**36167**	NETRIPLEX01 - NETRIPLEX LLC	**US**	45,568	**573.8**
65	110.2	**49806**	OFFHOST-AS Offshore hosting LTD	**MD**	256	**555.4**
191	78.1	**51699**	ANTARKTIDA-PLUS-AS Antarktida-Plus LLC	**RU**	256	**555.4**
309	67.4	**42741**	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	**RO**	1,280	**534.7**
5	194.5	**39150**	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	**RU**	3,840	**490.7**
119	90.5	**25406**	SPLIUS-AS SPLIUS, UAB	**LT**	53,248	**388.0**
126	89.0	**49017**	TPIC-AS Baltic Center of Innovations TechPromInvest LTD	**RU**	256	**327.8**

Cyber criminals manage networks of infected computers, otherwise known as zombies, to host botnets out of C&C servers. A single C&C server can manage some 250,000, or higher, slave machines. HostExploit focuses here, on the Zeus botnet as it remains the cheapest and most popular on the underground market.

This section should be considered in conjunction with Section 8.5 on Exploit Servers.

Not surprisingly due to the potential monetary reward many cybercrime observers and reserachers will recognize the servers listed in this Top 10.

Zeus Command and Control servers andZeus malicious file hosts data (Zbot) is utilized in conjunction with HostExploit's data from the excellent Zeus Tracker service from abuse.ch.



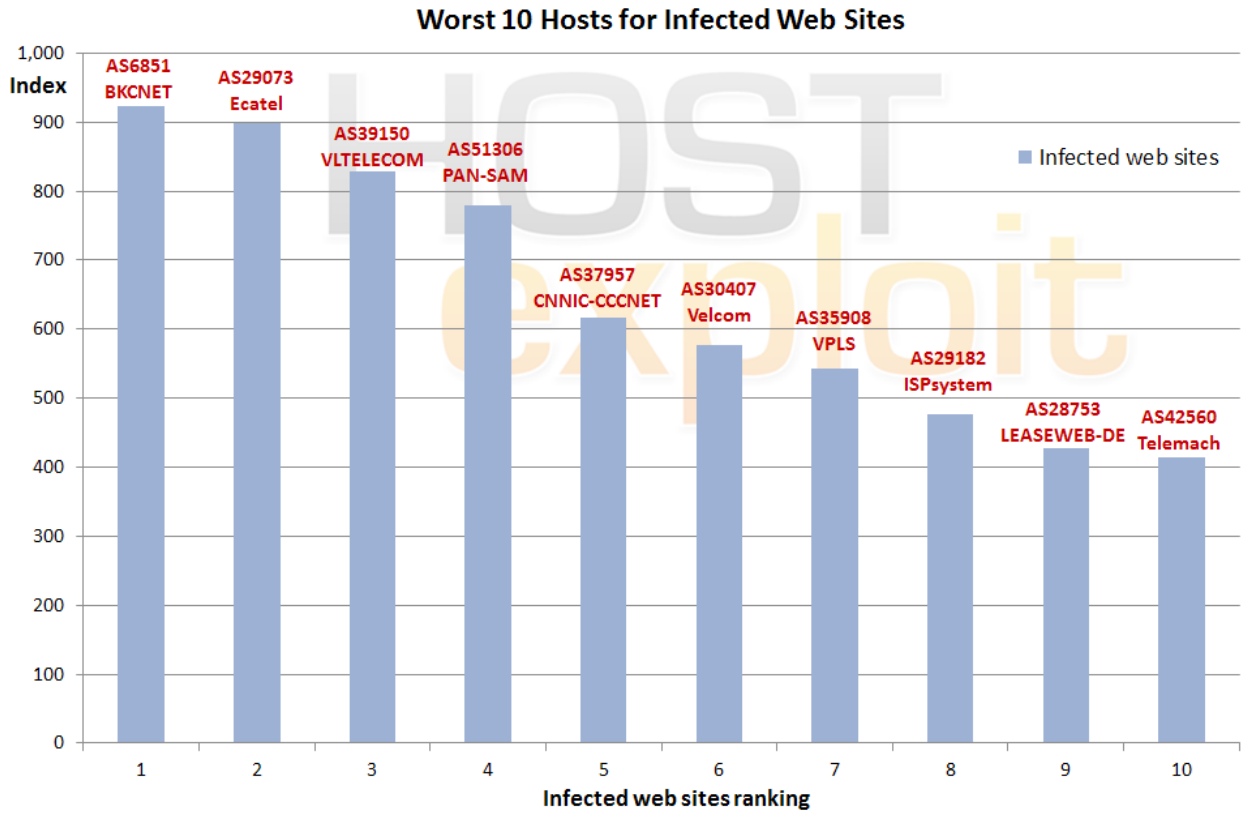
9.2.1. Infected Web Sites

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
12	172.3	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**922.4**
2	210.4	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**898.4**
5	194.5	**39150**	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	**RU**	3,840	**828.0**
64	110.7	**51306**	UAIP-AS PAN-SAM Ltd.	**UA**	2,048	**778.7**
104	94.0	**37957**	CNNIC-CCCNET China Communication Co., Ltd	**CN**	4,096	**617.0**
87	100.5	**30407**	VELCOM - Rcp.net	**CA**	8,192	**576.7**
56	115.0	**35908**	VPLSNET - VPLS Inc. d	**US**	701,952	**542.6**
35	131.6	**29182**	ISPSYSTEM-AS ISPsystem Autonomous System	**RU**	35,328	**476.4**
16	163.8	**28753**	LEASEWEB-DE Leaseweb Germany GmbH (previously netdirekt...	**DE**	108,544	**427.6**
168	80.4	**42560**	BA-TELEMACH-AS Telemach BiH	**BA**	32,768	**413.7**

Infected Web Sites is a general category where simultaneous forms of malicious activity can be present, this may be via knowingly serving malicious content, or via innocent compromise.

Here, our own data, gathered from specific honeypots, is combined with data provided by MalwareURL and hphosts on instances of malicious URLs found on individual ASes. MalwareURL's information is itself an amalgam of a number of community-reported sources.

The results show a mixed outcome with large hosts and a number of smaller, suspected crime servers. 4 of the overall Top 10 are present in this list, suggesting that infected web sites are a mainstay of bad servers.



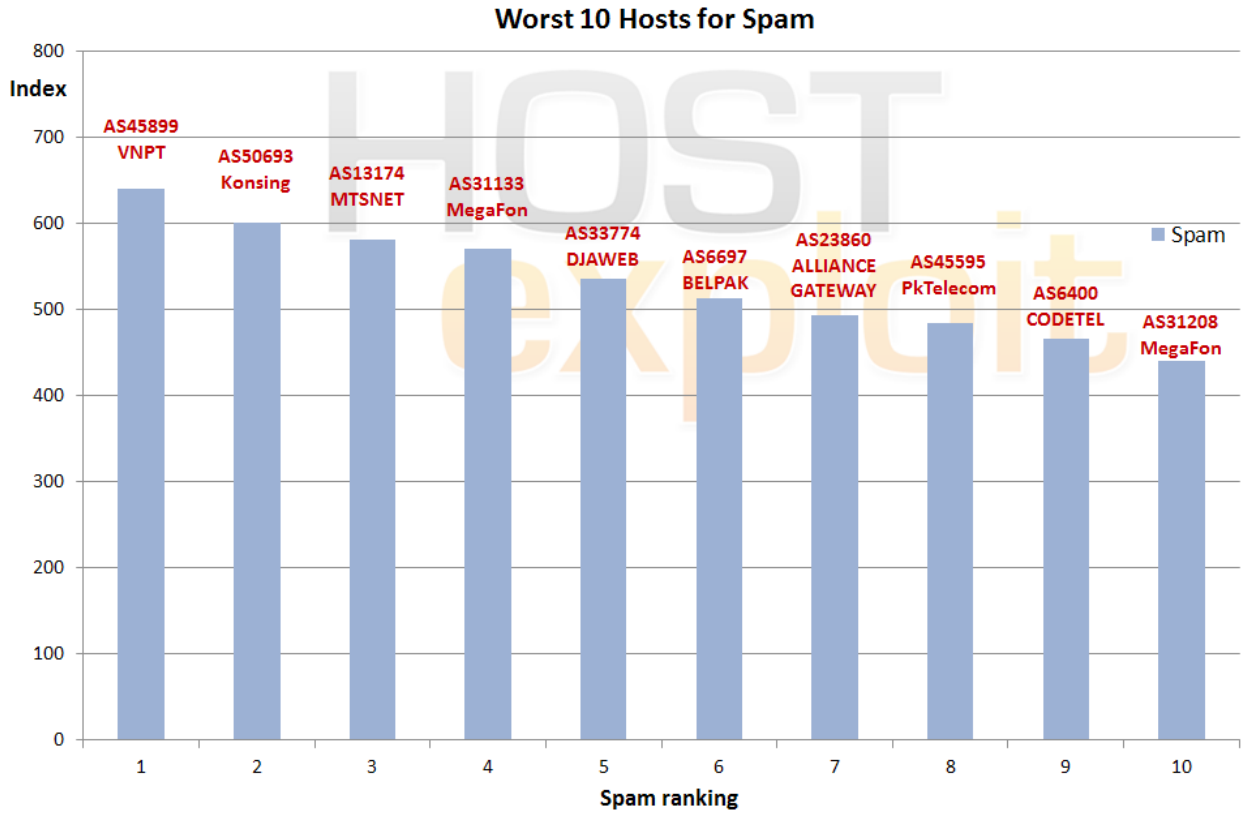
9.2.2. Spam

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
9	175.6	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,000,128	**639.9**
26	138.9	**50693**	KONSING-GROUP Konsing group doo	**RS**	2,048	**600.8**
29	137.4	**13174**	MTSNET OJSC "Mobile TeleSystems" Autonomous System	**RU**	24,064	**581.2**
34	131.9	**31133**	MF-MGSM-AS OJSC MegaFon Network	**RU**	13,056	**570.8**
24	141.8	**33774**	DJAWEB	**DZ**	91,392	**536.2**
7	177.1	**6697**	BELPAK-AS BELPAK	**BY**	747,264	**512.6**
54	116.1	**23860**	ALLIANCE-GATEWAY-AS-AP Alliance Broadband Services...	**IN**	12,288	**493.0**
45	124.8	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	2,287,616	**484.1**
63	110.7	**6400**	CompaÃ±Ãa Dominicana de TelÃ©fonos, C. por A. - CODETEL	**DO**	381,696	**466.2**
83	102.1	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	2,048	**441.0**

Our Top 10 spam results show a consistent pattern for the location of servers used by spammers. Countries with minimal regulation and monitoring enable spammers to use tried-and-tested methods to avoid detection such as fast-flux servers and disposable crime servers. Additionally, they are quick to adapt to current media themes without needing new innovations, unlike other areas of cybercriminal activity.

A single spam server can cause more damage than a whole group of spam servers. Furthermore, a small quantity of spam can be more effective than a large quantity if using targeted techniques. These two properties make this a difficult category to quantitatively measure. For this reason, we combine known spam IPs from a vast range of respected sources – SpamHaus, UCEPROTECT-Network, Malicious Networks (FiRE) and SudoSecure – with our own data. The result is a definitive and current list of spam servers in the world, i.e. those hosting the IP space sending the spam.

Note the three Russian-based servers in this category indicate that Russian servers was particularly utilized for spam activities in Q1. Also, the appearance of AS50693 KONSING-GROUP, straight in at #2 is of note. See section 6 for more information on this mover.



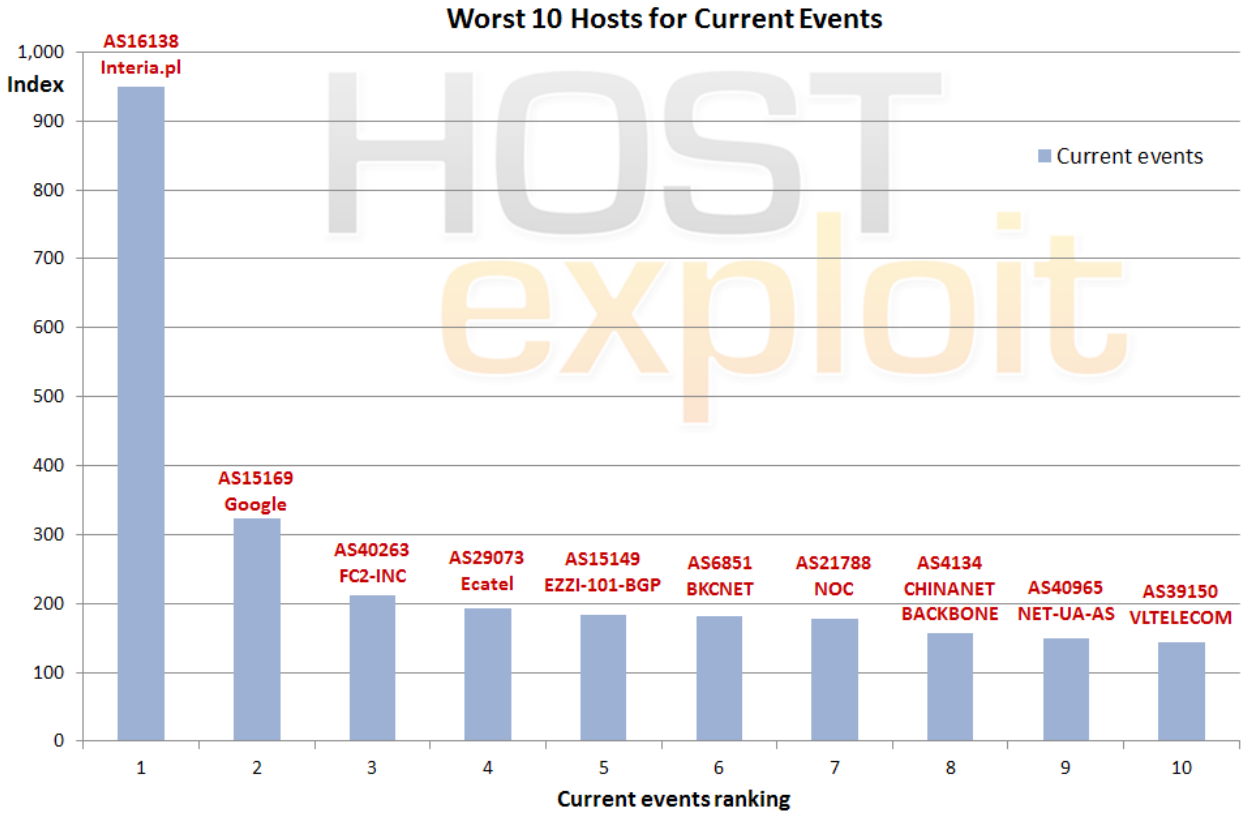
9.2.3. Current Events

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
3	207.0	**16138**	INTERIAPL INTERIA.PL Autonomous System	**PL**	3,072	**949.5**
47	122.7	**15169**	GOOGLE - Google Inc.	**US**	284,416	**322.6**
609	54.9	**40263**	FC2-INC - FC2 INC	**US**	1,024	**211.2**
2	210.4	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**193.3**
314	67.3	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,672	**182.9**
12	172.3	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**182.2**
14	168.0	**21788**	NOC - Network Operations Center Inc.	**US**	278,528	**177.1**
18	150.8	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	109,515,264	**157.7**
759	49.3	**40965**	NET-UA-AS limited corp	**UA**	256	**148.9**
5	194.5	**39150**	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	**RU**	3,840	**144.2**

The most up-to-date and fast-changing of attack exploits and vectors form the category of Current Events.

Here HostsExploit's own processes including examples of MALfi (XSS/RCE/RFI/LFI), XSS attacks, clickjacking, counterfeit pharmas, rogue AV, Zeus (Zbota), Artro, SpyEye, Stuxnet, BlackHat SEO, Koobface, and newly emerged exploit kits form a key component of the data.

The vast array of techniques looked at in this category are reflected in this Top 10 Current Events sector with this list containing some well-known names. Also of note, 40% of the Top 10 here are based in US with 20% being based in Latvia, which appears to be a target for cybercriminal hosting.



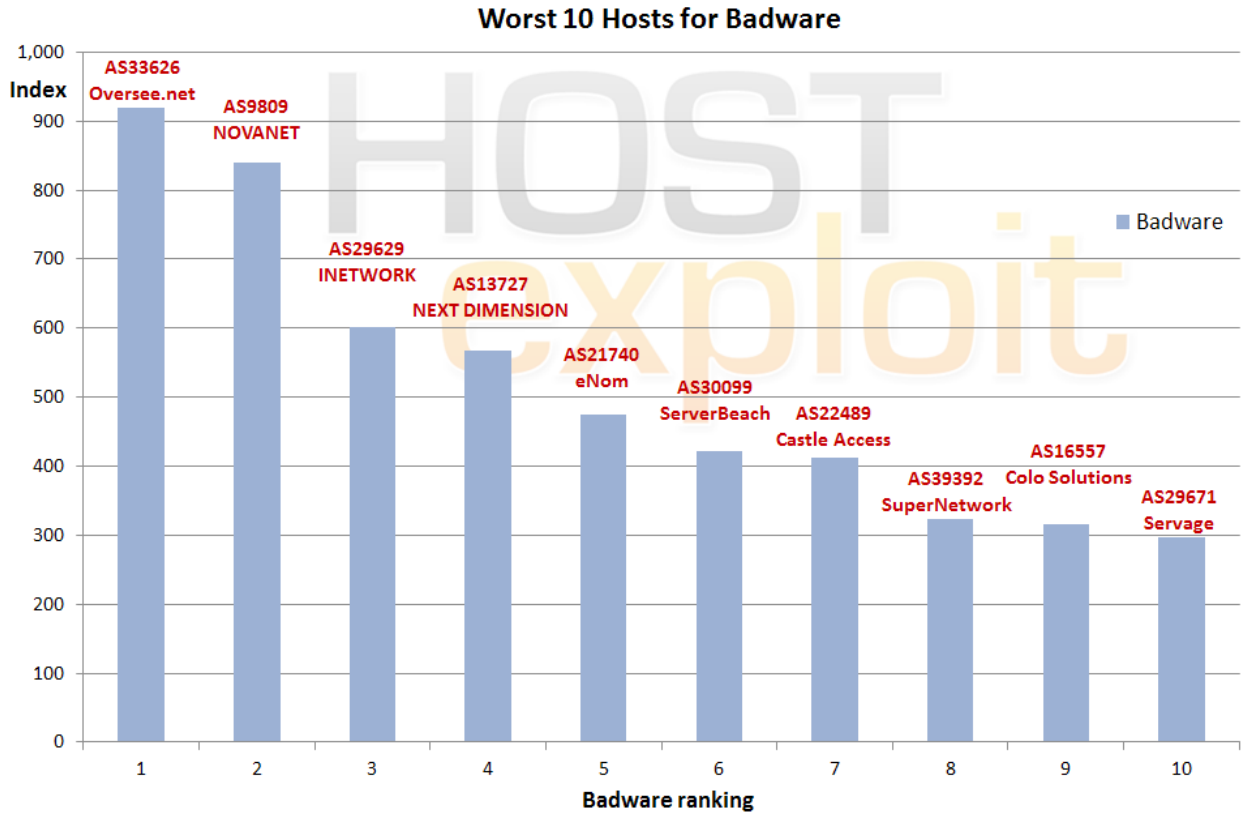
9.2.4. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
11	172.4	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	4,096	**919.7**
13	170.1	**9809**	NOVANET Nova Network Co.Ltd, Futian District... Shenzhen...	**CN**	11,008	**839.7**
8	176.1	**29629**	INETWORK-AS IEUROP AS	**FR**	8,192	**600.9**
23	142.0	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**567.9**
72	106.6	**21740**	ENOMAS1 - eNom, Incorporated	**US**	19,456	**475.5**
52	117.5	**30099**	SB-2 - ServerBeach	**US**	25,088	**422.2**
55	115.3	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	45,312	**412.3**
25	139.0	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	49,664	**322.9**
113	91.5	**16557**	COLOSOLUTIONS - Colo Solutions, Inc.	**DE**	27,392	**315.5**
58	113.4	**29671**	SERVAGE Servage GmbH	**DE**	12,288	**297.3**

Badware fundamentally disregards how users might choose to employ their own computer. Examples of such software include spyware, malware, rogues, and deceptive adware. It commonly appears in the form of free screensavers that surreptitiously generate advertisements, redirects take browsers to unexpected web pages and keylogger programs that transmit personal data to malicious third parties.

In this quarter there has been further analysis on 'false positives' particularly regarding parked domains. These have been found to a limited degree in conjunction with data partners and results are starting to reflect this disparity.

The findings in this category are primarily based on StopBadware's data, which is itself aggregated from Google, Sunbelt Software, and Team Cymru.



Crime Servers

10.1. Background - What Are Crime Servers?

Crime servers are by definition active dedicated accomplices to cybercrime providing a platform for cyber criminals or cells within their own organization to mount cyber attacks. Crime servers cannot be excused on the grounds of being a victim of lax abuse policy enforcement but are active participants in the bad host process sometimes acting as hosting providers or registrars themselves.

Examples of large versions of these have been seen over recent times and shown within earlier HostExploit reports i.e. Atrivo (US), McColo (US), Real Host (LV).

Interestingly the ones discovered within this current analysis and report are considerably smaller than these, numbers of IPs ranging from just 256 to 1,024, while the majority of the top 50 bad hosts appear to be legitimate commercial enterprises.

10.2. Crime Servers or Bad Hosts?

The research contained within this report has been directed at identifying instances of bad hosts around the world to culminate in a league table of the 'Top 50 Worst Hosts', presuming that most of the hosting servers are legitimate internet service providers.

Essentially, the difference between a 'crime server' and a 'bad host' is more acutely seen within the motives of the owners; a crime server's owners can be identified as being actively involved with the criminal activity being carried out on its network whereas a 'bad host' can only be accused of having a poor abuse enforcement policy, lax or non-existent network monitoring, 'turning a blind eye' to web site activity or ignoring complaints about abuses from users.

10.2. Crime Servers - Currently Inactive (Not Announced)

All active at end of Q4 2010; inactive at end of Q1 2011

AS number	Name	IPs	HE Rank
29106	VOLGAHOST-AS PE Bondarenko Dmitriy Vladimirovich	256	N/A
20564	INFORMEX-MNT Informex, E-commerce Service Provider	256	N/A
51554	LYAHOV-AS Lyahovich Maksim	256	N/A
49314	NEVAL PE Nevedomskiy Alexey Alexeevich	256	N/A
197329	ZAMANHOST-AS Rusnak Vasil Viktorvich	256	N/A

10.3. Crime Servers - Examples Currently Active

All active at end of Q1 2011

AS number	Name	IPs	HE Rank
41947	**WEBALTA-AS OAO Webalta**	**15,872**	**1**
16138	**INTERIAPL INTERIA.PL**	**3,072**	**3**
39150	**VLTELECOM-AS VLineTelecom**	**3,840**	**5**
49469	SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup	**1,792**	**32**
21607	**DEPLOYLINUX - DeployLinux**	**512**	**60**
48445	**FAVN Favorit Network SL**	**512**	**133**
4905	**FA-LAX-1 - Future Ads LLC**	**256**	**758**

Conclusions

This report is a further undertaking to highlight the issues which create and allow cyber criminal activity to be hosted and served on the Internet. It should be stressed; HostExploit, the report's authors, sponsors, and the now numerous hosts and volunteers who have helped in establishing this report, do not view the exposure of bad hosting and ISPs as a sole solution to the seemingly ever growing problem of cybercrime. However, providing a comparative and quantitative listing of hosts and ISPs with associated badness clearly contributes to a "who" and a "where" approach to comprehending cybercrime:

• Exposing comparative levels of badness found on Internet hosts, ISPs, and networks in this way highlights the integral part that hosts play in the cycle of cyber criminal activity.

• Such a report and the defined "HE Index" acts as a consumer barometer for each of the **37,271** currently advertised and commercial ASes.

• It provides a definitive and quantitative analysis of the worst hosting and network culprits of failing to prevent cyber criminal activity.

• The release of the Top 50 Bad Hosts reports has delivered a successful outcome with some contacted hosts significantly decreasing levels of abuses by 90%.

•• As shown in earlier reports and only briefly covered within this report, the overall analysis further highlights a relatively small number of dedicated 'Crime Servers', and related 'bullet proof' hosting enterprises.

Action planning for hosts, telecoms and ISPs:

The HE Index, expresses a myriad of different internet malpractices in a comparable format. This report provides disclosure and comparative awareness.

Many hosts and those from the wider Internet community regularly ask HostExploit what can be done. Such queries include:

- What should the providers do to remove, and to better prevent, such badness from happening on their space?
- What did the 'most improved' providers (see section 8) do to 'clean up'?
- How can service providers work with local CERTS and / or law enforcement to investigate and assist in cases of abuse?
- The 'Top Bad Host' reports, SiteVet.com and partners provide community data for the benefit of hosts and ISPs. What relevance does this data have for the wider community?

To answer these and other queries a supplementary paper from HostExploit is underway. This will also include community case studies, advice on good abuse practice, and a wealth of community resources.

Hosts or ASes interested in participating please contact us - **admin@hostexploit.com**

Appendix 1.

Glossary

AS (Autonomous System):

An AS is a unit of router policy, either a single network or a group of networks that is controlled by a common network administrator on behalf of an entity such as a university, a business enterprise, or Internet service provider. An AS is also sometimes referred to as a routing domain. Each autonomous system is assigned a globally unique number called an Autonomous System Number (ASN).

Badware:

Software that fundamentally disregards a user's choice regarding about how his or her computer will be used. Types of badware are spyware, malware, or deceptive adware. Common examples of badware include free screensavers that surreptitiously generate advertisements, malicious web browser toolbars that take your browser to different pages than the ones you expect, and keylogger programs that can transmit your personal data to malicious parties.

Blacklists:

In computing, a blacklist is a basic access control mechanism that allows access much like your ordinary nightclub; everyone is allowed in except people on the blacklist. The opposite of this is a whitelist, equivalent of your VIP nightclub, which means allow nobody, except members of the white list. As a sort of middle ground, a gray list contains entries that are temporarily blocked or temporarily allowed. Gray list items may be reviewed or further tested for inclusion in a blacklist or whitelist. Some communities and webmasters publish their blacklists for the use of the general public, such as Spamhaus and Emerging Threats.

Botnet:

Botnet is a term for a collection of software robots, or bots, that run autonomously and automatically. The term is now mostly associated with malicious software used by cyber criminals, but it can also refer to the network of infected computers using distributed computing software.

CSRF (cross site request forgery):

Also known as a "one click attack" / session riding, which is a link or script in a web page based upon authenticated user tokens.

DNS (Domain Name System):

DNS associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g. www.example.com, into IP addresses, e.g. 208.77.188.166, which networking equipment needs to deliver information. A DNS also stores other information such as the list of mail servers that accept email for a given domain, by providing a worldwide keyword-based redirection service.

DNSBL:

Domain Name System Block List – an optional list of IP address ranges or DNS zone usually applied by Internet Service Providers (ISP) for preventing access to spam or badware. A DNSBL of domain names is often called a URIBL, Uniform Resource Indentifier Block List

Exploit:

An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause irregular behavior to occur on computer software, hardware, or something electronic. This frequently includes such things as violently gaining control of a computer system or allowing privilege escalation or a denial of service attack.

Hosting:

Usually refers to a computer (or a network of servers) that stores the files of a web site which has web server software running on it, connected to the Internet. Your site is then said to be hosted.

IANA (Internet Assigned Numbers Authority)

IANA is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. It coordinates the global IP and AS number space, and allocates these to Regional Internet Registries.

ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN is responsible for managing the Internet Protocol address spaces (IPv4 and IPv6) and assignment of address blocks to regional Internet registries, for maintaining registries of Internet protocol identifiers, and for the management of the top-level domain name space (DNS root zone), which includes the operation of root nameservers.

IP (Internet Protocol):

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering data packets from the source host to the destination host solely based on its address.

IPv4

Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP). Pv4 uses 32-bit (four-byte) addresses, which limits the address space to 4.3 billion possible unique addresses. However, some are reserved for special purposes such as private networks (18 million) or multicast addresses (270 million).

IPv6

Internet Protocol Version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 uses a 128-bit address, IPv6 address space supports about 2^128 addresses

ISP (internet Service Provider):

A company or organization that has the equipment and public access to provide connectivity to the Internet for clients on a fee basis, i.e. emails, web site serving, online storage.

LFI (Local File Inclusion):

Use of a file within a database to exploit server functionality. Also for cracking encrypted functions within a server, e.g. passwords, MD5, etc.

MALfi (Malicious File Inclusion):

A combination of RFI (remote file inclusion), LFI (local file inclusion), XSA (cross server attack), and RCE (remote code execution).

Malicious Links:

These are links which are planted on a site to deliberately send a visitor to a malicious site, e.g. a site with which will plant viruses, spyware or any other type of malware on a computer such as a fake security system. These are not always obvious as they can be planted within a feature of the site or masked to misdirect the visitor.

MX:

A mail server or computer/server rack which holds and can forward e-mail for a client.

NS (Name Server):

Every domain name must have a primary name server (eg. ns1.xyz.com), and at least one secondary name server (ns2.xyz.com etc). This requirement aims to make the domain still reachable even if one name server becomes inaccessible.

Open Source Security:

The term is most commonly applied to the source code of software or data, which is made available to the general public with relaxed or non-existent intellectual property restrictions. For Open Source Security this allows users to create user-generated software content and advice through incremental individual effort or through collaboration.

Pharming:

Pharming is an attack which hackers aim to redirect a website's traffic to another website, like cattle rustlers herding the bovines in the wrong direction. The destination website is usually bogus.

Phishing:

Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information. Phishing is typically carried out using e-mail (where the communication appears to come from a trusted website) or an instant message, although phone contact has been used as well.

Registry:

A registry operator generates the zone files which convert domain names to IP addresses. Domain name registries such as VeriSign, for .com. Afilias for .info. Country code top-level domains (ccTLD) are delegated to national registries such as and Nominet in the United Kingdom, .UK, "Coordination Center for TLD .RU" for .RU and .РФ

Registrars:

A domain name registrar is a company with the authority to register domain names, authorized by ICANN.

Remote File Inclusion (RFI):

A technique often used to attack Internet websites from a remote computer. With malicious intent, it can be combined with the usage of XSA to harm a web server.

Rogue Software:

Rogue security software is software that uses malware (malicious software) or malicious tools to advertise or install its self or to force computer users to pay for removal of nonexistent spyware. Rogue software will often install a trojan horse to download a trial version, or it will execute other unwanted actions.

Rootkit:

A set of software tools used by a third party after gaining access to a computer system in order to conceal the altering of files, or processes being executed by the third party without the user's knowledge.

Sandnet:

A sandnet is closed environment on a physical machine in which malware can be monitored and studied. It emulates the internet in a way which the malware cannot tell it is being monitored. Wonderful for analyzing the way a bit of malware works. A Honeynet is the same sort of concept but more aimed at attackers themselves, monitoring the methods and motives of the attackers.

Spam:

Spam is the term widely used for unsolicited e-mail. . Spam is junk mail on a mass scale and is usually sent indiscriminately to hundreds or even hundreds of thousands of inboxes simultaneously.

Trojans:

Also known as a Trojan horse, this is software that appears to perform or actually performs a desired task for a user while performing a harmful task without the user's knowledge or consent.

Worms:

A malicious software program that can reproduce itself and spread from one computer to another over a network. The difference between a worm and a computer virus is that a computer virus attaches itself to a computer program to spread and requires an action by a user while a worm is self-contained and can send copies of itself across a network.

XSA (Cross Server Attack):

A networking security intrusion method which allows for a malicious client to compromise security over a website or service on a server by using implemented services on the server that may not be secure.

Appendix 2

HE Index Calculation Methodology

April 14, 2011

1 Revision history

Rev.	Date	Notes
1.	December 2009	Methodology introduced.
2.	March 2010	IP significant value raised from 10,000 to 20,000.
3.	June 2010	Sources refined. Double-counting of Google Safebrowsing data through StopBadware eliminated. Source weightings refined.

Table 1: Revision history

2 Motivation

We aim to provide a simple and accurate method of representing the history of badness on an Autonomous System (AS). Badness in this context comprises malicious and suspicious server activities such as hosting or spreading: malware and exploits; spam emails; MALfi attacks (RFI/LFI/XSA/RCE); command & control centers; phishing attacks.

We call this the *HE Index*; a number from 0 (no badness) to 1,000 (maximum badness). Desired properties of the HE Index include:

1. Calculations should be drawn from multiple sources of data, each respresenting different forms of badness, in order to reduce the effect of any data anomalies.
2. Each calculation should take into account some objective size of the AS, so that the index is not unfairly in favor of the smallest ASes.
3. No AS should have an HE Index value of 0, since it cannot be said with certainty that an AS has zero badness, only that none has been detected.
4. Only one AS should be able to hold the maximum HE Index value of 1,000 (if any at all).

3 Data sources

Data is taken from the following 11 sources.

Spam data from UCEPROTECT-Network and ZeuS data from Abuse.ch is cross-referenced with Team Cymru.

Data from StopBadware is itself an amalgam of data from Google, Sunbelt Sofware and NSFOCUS.

Using the data from this wide variety of sources fulfils desired property #1.

Sensitivity testing was carried out, to determine the range of specific weightings that would ensure known bad ASes

#	Source	Data	Weighting
1.	UCEPROTECT-Network	Spam IPs	Very high
2.	MalwareURL	Malicious URLs	High
3.	Abuse.ch	ZeuS servers	High
4.	StopBadware	Badware instances	Very high
5.	SudoSecure	Spam bots	Medium
6.	Malicious Networks	C&C servers	High
7.	Malicious Networks	Phishing servers	Medium
8.	Malicious Networks	Exploit servers	Medium
9.	Malicious Networks	Spam servers	Low
10.	HostExploit	Current events	High
11.	hpHosts	Malware instances	High

Table 2: Data sources

would appear in sensible positions. The exact value of each weighting within its determined range was then chosen at our discretion, based on our researchers' extensive understanding of the implications of each source. This approach ensured that results are as objective as realistically possible, whilst limiting the necessary subjective element to a sensible outcome.

4 Bayesian weighting

How do we fulfil desired property #2? That is, how should the HE Index be calculated in order to fairly reflect the size of the AS? An initial thought is to divide the number of recorded instances by some value which represents the size of the AS. Most obviously, we could use the number of domains on each AN as the value to respresent the size of the AS, but it is possible for a server to carry out malicious activity without a single registered domain, as was the case with McColo. Therefore, it would seem more pragmatic to use the size of the IP range (i.e. number of IP addresses) registered to the AS through the relevant Regional Internet Registry.

However, by calculating the ratio of number of instances per IP address, isolated instances on small servers may produce distorted results. Consider the following example:

Average spam instances in sample set: 50
Average IPs in sample set: 50,000
Average ratio: 50 / 50,000 = 0.001
Example spam instances: 2
Example IPs: 256
Example ratio: 2 / 256 = 0.0078125

In this example, using a simple calculation of number of instances divided by number of IPs, the ratio is almost eight times higher than the average ratio. However, there are only two recorded instances of spam, but the ratio is so high due to the low number of IP addresses on this particular AS. These may well be isolated instances, therefore we need to move the ratio towards the average ratio, moreso the lower the numbers of IPs.

For this purpose, we use the *Bayesian ratio* of number of instances to number of IP addresses. We calculate the Bayesian ratio as:

$$B = (\frac{M}{M+C}) \cdot \frac{N}{M} + (\frac{C}{M+C}) \cdot \frac{N_a}{M_a} \tag{1}$$

where:
B: *Bayesian ratio*
M: *number of IPs allocated to ASN*
M_a: *average number of IPs allocated in sample set*
N: *number of recorded instances*
N_a: *average number of recorded instances in sample set*
C: *IP weighting = 20,000*

The process of moving the ratio towards the average ratio has the effect that no AS will have a Bayesian ratio of zero, due to an uncertainty level based on the number of IPs. This meets the requirements of desired property #3.

5 Calculation

For each data source, three factors are calculated.

To place any particular Bayesian ratio on a scale, we divide it by the maximum Bayesian ratio in the sample set, to give Factor C:

$$F_C = \frac{B}{B_m} \tag{2}$$

where:
B_m: *maximum Bayesian ratio*

Sensitivity tests were run which showed that in a small number of cases, Factor C favors small ASes too strongly. Therefore, it is logical to include a factor that uses the total number of instances, as opposed to the ratio of instances to size. This makes up Factor A:

$$F_A = min\{\frac{N}{N_a}, 1\} \tag{3}$$

This follows the same format as Factor C, and should only have a low contribution to the Index, since it favors small ASes, and is used only as a compensation mechanism for rare cases of Factor C.

If one particular AS has a number of instances significantly higher than for any other AS in the sample, then Factor A would be very small, even for the AS with the second highest number of instances. This is not desired since the value of one AS is distorting the value of Factor A. Therefore, as a compensation mechanism for Factor A (the ratio of the average number of instances) we use Factor B as a ratio of the maximum instances less the average instances:

$$F_B = \frac{N}{N_m - N_a} \tag{4}$$

where:
N_m: *maximum number of instances in sample set*

Factor A is limited to 1; Factors B and C are not limited to 1, since they cannot exceed 1 by definition. Only one AS (if any) can hold maximum values for all three factors, therefore this limits the HE Index to 1,000 as specified in desired property #4.

The index for each data source is then calculated as:

$$I = (F_A \cdot 10\% + F_B \cdot 10\% + F_C \cdot 80\%) \cdot 1000 \tag{5}$$

The Factor A, B & C weightings (10%, 10%, 80% respectively) were chosen based on sensitivity and regression testing. Low starting values for Factor A and Factor B were chosen, since we aim to limit the favoring of small ASes (property #2).

The overall HE Index is then calculated as:

$$H = \frac{\sum_{i=1}^{11} I_i \cdot w_i}{\sum_{i=1}^{11} w_i} \tag{6}$$

where:
w_i: *source weighting (1=low, 2=medium, 3=high, 4=very high)*