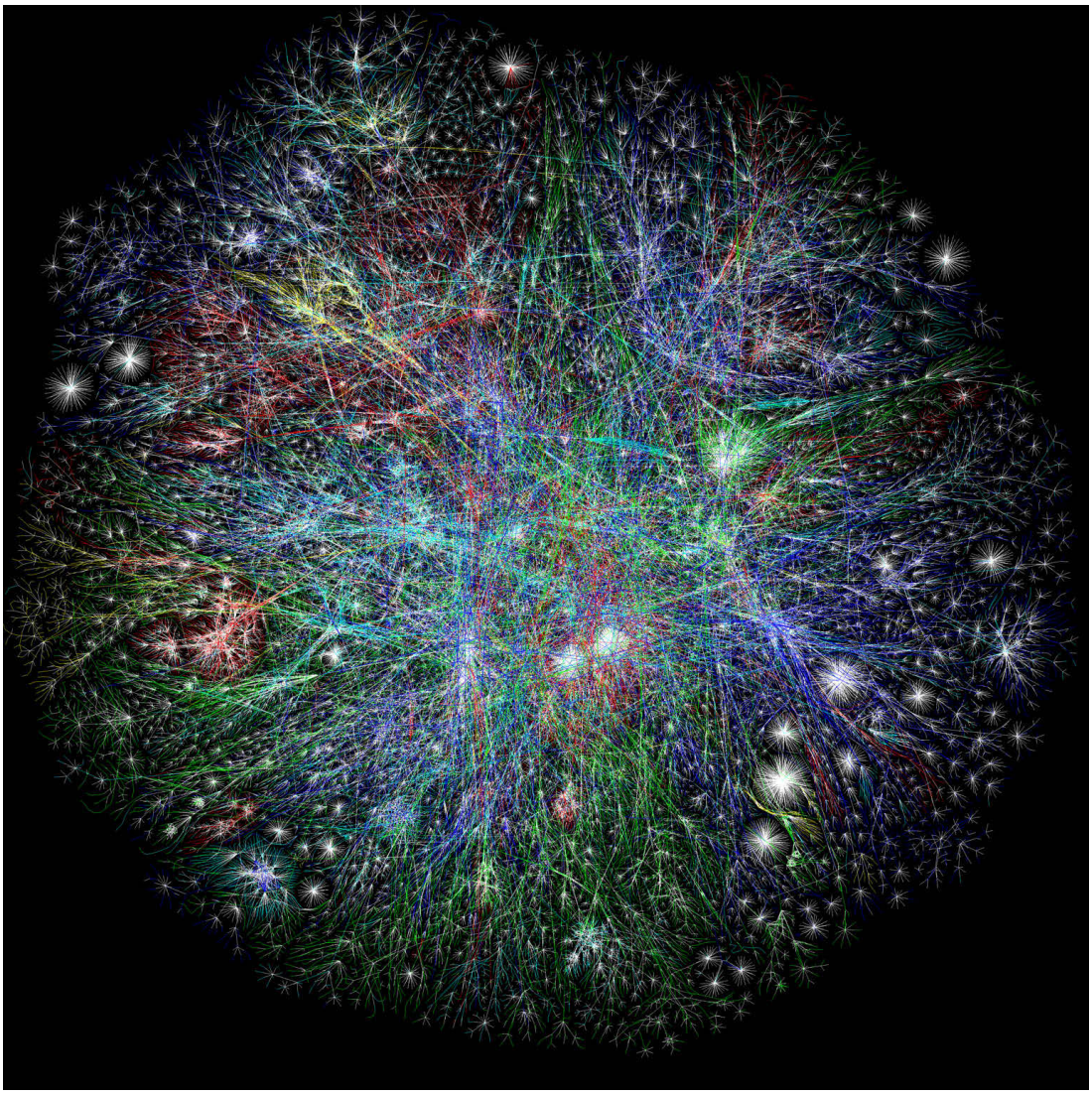
ISBN: 978-0-9836249-0-5

HostExploit's Worldwide Cybercrime Series

Top 50 Bad Hosts and Networks 1st Quarter 2012 - Report



Opte Map of the Internet - CC BY-NC-SA

SITEVET HOST exploit GROUP IB

Table of Contents

1. Introduction Page 4
2. News Roundup Page 5
3. Frequently Asked Questions Page 8
4. The Top 50 - Q1 2012 Page 9
5. Q1 2012 to Q4 2011 Comparison Page 10
6. Top 10 Visual Breakdown Page 11
7. What's New? Page 12
    - 7.1 Overview Page 12
    - 7.2 Top 10 Newly-Registered Hosts Page 13
    - 7.3 Improved Hosts Page 14
    - 7.4 Deteriorated Hosts Page 15
8. The Good Hosts Page 16
9. Bad Hosts by Topic Page 17
    - 9.1 Servers
        - 9.1.1 Botnet C&C Servers Page 17
        - 9.1.2 Phishing Servers Page 18
        - 9.1.3 Exploit Servers Page 19
        - 9.1.4 Zeus Botnet Hosting Page 20
    - 9.2 Activity
        - 9.2.1 Infected Web Sites Page 21
        - 9.2.2 Spam Page 22
        - 9.2.3 HostExploit Current Events Page 23
        - 9.2.4 Badware Page 24
10. Conclusions Page 25

Appendix 1 Glossary Page 26

Appendix 2 Methodology Page 28

Top 50

CyberCrime Series

Bad Hosts and Networks

Supported by

nominet trust

www.nominettrust.org.uk

DEEPEND RESEARCH

Edited by

- Jart Armin

Review

- Dr. Bob Bruen
- Raoul Chiesa
- Andre' DiMino
- Ilya Sachkov

Comparative Data

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

Contributors

- Steve Burn
- Greg Feezel
- David Glosser
- Niels Groeneveld
- Tim Karpinsky
- Bogdan Vovchenko
- Will Rogofsky
- Philip Stranger
- Bryn Thompson
- Yori Kamphuis
- Michel Eppink
- Thorsten Kraft
- DeepEnd Research

Introduction

Introduction

Welcome to HostExploit's 1st Quarter report on the Top 50 Bad Hosts and Networks, published in collaboration with Group-IB.

It has been an interesting quarter for ISPs, hosts and networks worldwide, with an increased recognition by national CERTs and law enforcement of the cross-border actions necessary to bring international cybercriminals to justice.

We have seen recent actions by Microsoft disrupt Zeus and SpyEye botnets alongside significant arrests of cybercriminals. Alongside roundups of these current events, we present our regular lists of the most concentrated areas of malicious activity on the internet.

Watch out for the forthcoming *World Cybercrime Report*, focusing on the geographic distribution of cybercrime, to be released in late April.

Jart Armin

***World Cybercrime Report*:** April 25th 2012

As discussed in previous reports, we've been working towards a more unified method of representing the badness levels in particular countries.

We will be releasing a full report on **April 25th,** showing the results and implications of our latest methodology.

The report will be released with APWG at CeCOS VI in Prague.

In conjunction with the report, we will be launching Global Security Map - an interactive map enabling analysis of the geographic distribution of cybercrime. An early preview can be seen now at http://globalsecuritymap.com/.

Please continue to check out the website for news on the report's release. Alternatively, sign up to our newsletter at HostExploit.com and we'll let you know about release dates.

News Roundup

Disrupting the Botnets via Host Abuse Handling

Interest in botnet takeovers has been high this quarter as seen in coverage of the Microsoft-led disruption of Zeus and SpyEye and the Kaspersky-led dismantling of the second Hlux or Kelihos botnet. (For background information, see HostExploit's coverage.)

Incidents like these raise the debate and serve to intensify points for discussion on several issues. At the center is the question of how best to deal with botnets. On this topic, the security industry divides into two main opinions, which recent events serve to highlight.

Microsoft and partners, for example, refrained from using the word "takedown" in covering events of "Operation b71" - preferring "disrupted" to convey how the botnet's operations were affected. As well, Microsoft expressed their intention as being to "disrupt and undermine" the infrastructure that enables criminal activity and, interestingly, backed up their actions through the existing legal framework in the form of the Racketeer Influenced and Corrupt Organizations Act (RICO).

Kaspersky and partners preferred to use the word "takedown" in their coverage employing similar sinkholing tactics as used previously to disable the targeted Kelihos botnet.

Which course of action, then, is the more effective? Is it enough to cut off one, or several, parts of a hydra, to partially disable but leaving the botnet capable of regeneration? Or should the enablers of the supporting infrastructures be held to account for providing services that criminals can use and abuse?

It is too early to tell in these specific cases what the long-term outcomes will be and, meanwhile, the debate rumbles. The industry itself is pushing for a proactive stance from hosting providers with the publication of a set of voluntary or self-regulating best practices in an effort to staid off government intervention.

The consensus of opinion among HostExploit's researchers remains unchanged. Actions that disrupt, dismantle, take down, and prevent further criminal action, albeit temporarily, are worthwhile, but hosting providers are the enablers; the ones who support, involuntarily or otherwise, the infrastructures that the criminals use.

Responsible hosts, in all honesty, cannot plead ignorance of criminal activity on their servers. Paying close attention to badness levels is conducive to good business and produces loyal customers. Most community sources provide non-intrusive services for free, and the means for hosts to gauge problems are on the rise. So why are they not using them?

Hosts in the News – AS21788 BurstNET and AS53264 Continuum

Two hosting providers, BurstNET Technologies Inc. (AS21788) and Continuum Data Centers (AS53264) – both named in Microsoft's supporting legal documents – received a surprise raid by law enforcement and Microsoft's legal team representatives, as part of the recent coordinated action to seize the command and control servers of Zeus and SpyEye botnets.

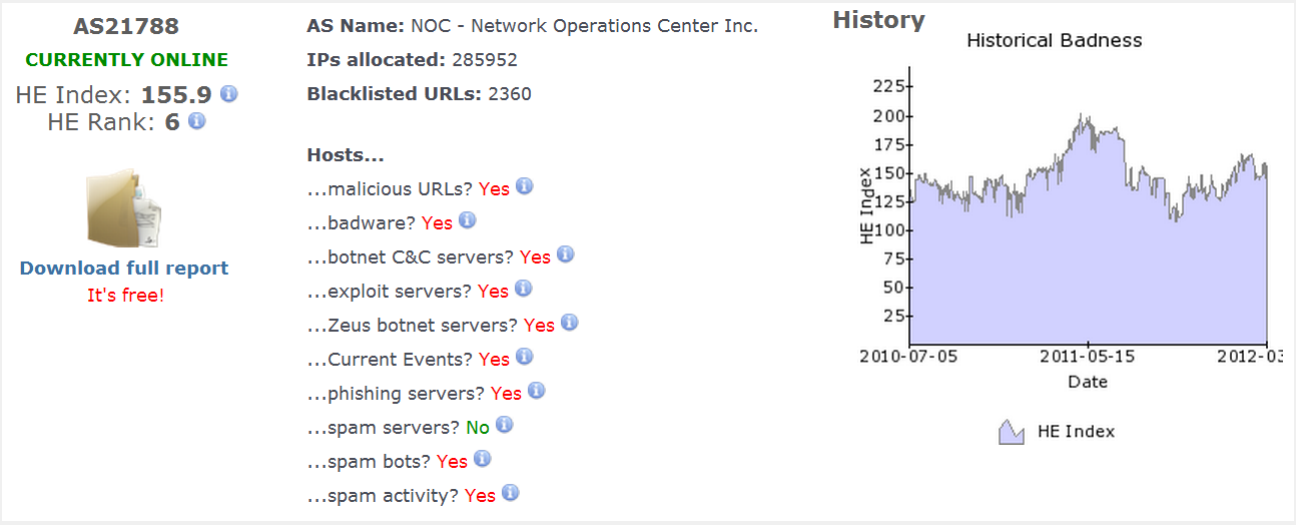
BurstNET's Chief Technology Officer, Joseph Marr, quoted in online news agency "Citizen's Voice", said that the web hosting company had not been implicated in the botnet scheme, nor was it aware of it. The server had been hosted "with one of BurstNET's resellers, or a customer 'who purchases our service with the intent of reselling to other customers.'"

"We do catch a lot of things through our daily activities," Marr said. "But in this case, these guys really knew what they were doing. They were trying to keep things under the radar. They were trying to keep things hidden. Apparently, there were several other servers, but these were the two that were picked off first."

Unfortunately, BurstNET's Network Operation Center is no stranger to the security community and no stranger to HostEploit's

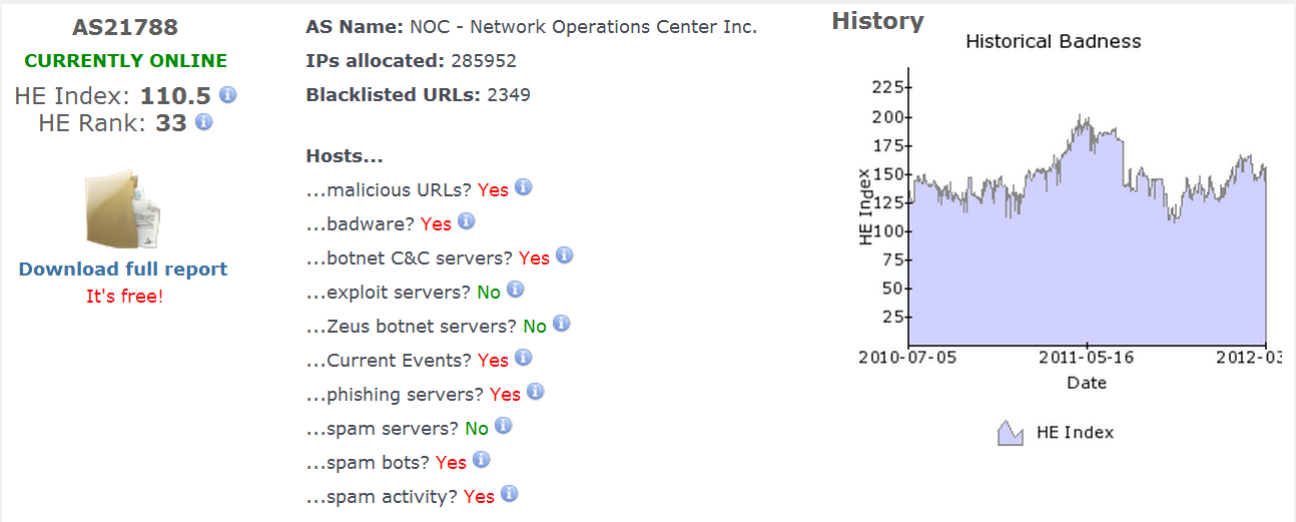
"Top 50 Bad Hosts & Networks" reports. In Q2 2011 it reached as high as #5 for high levels of a wide range of exploits and malware including the presence of Zeus servers. It then dropped to #36 in Q3 2011 and went back up to #18 in Q4 2011.

At the time of the Microsoft raid, BurstNET had returned to an unacceptably high ranking at #6. Note the continued presence of Zeus botnet servers:



AS21788 BurstNET NOC – SiteVet report – Day of Microsoft raid

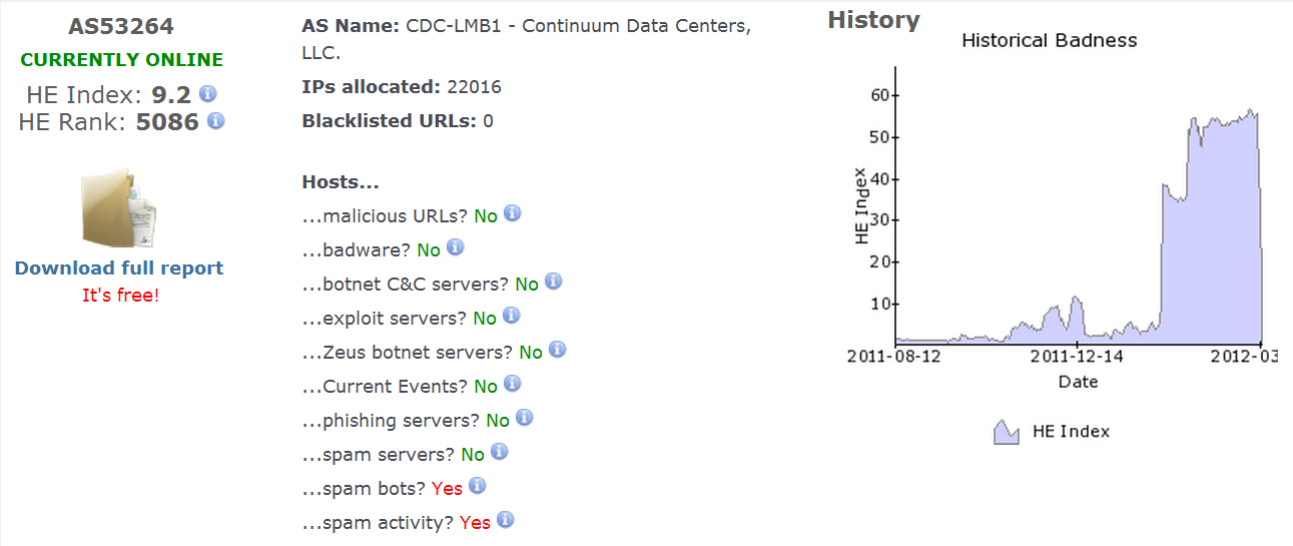
The next day (after the raid), BurstNET's position dropped to #33. Note that there were no Zeus botnets showing at that time:



AS21788 BurstNET NOC – SiteVet report – Day after Microsoft raid

AS53264 Continuum Data Centers has a slightly different history. This web host had been serving low levels of malware until a sudden peak appeared in January 2012 which dropped immediately after Zeus was disrupted:

(Continued on next page...)



AS53264 Continuum – SiteVet report – Day after Microsoft raid

Russian Criminal Gang Arrested In Online Banking Fraud Investigation

A criminal gang of eight who used online banking Trojans to steal large sums of money from banking institutions worldwide over a period of two years were arrested by the Russian Federal Security Service (FSB) and the Ministry of the Interior (MVD), Group-IB announced on March 20 2012.

Group-IB, the first Russian company to provide comprehensive IT security and data breach investigations reported that the gang stole more than 130 million rubles (USD4.4 million, GBP2.8 million, EUR3.4 million) in just the last three months, transferring the stolen money through a complex network of seemingly legitimate business enterprises.

Group-IB and specialist organizations in several countries, including Holland and Canada, cooperated to gather evidence against the cybercriminals. Russian Sberbank provided financial assistance throughout the investigation and Dutch company FOX-IT carried out the forensic analytics.

The cybercriminal gang used malware to infect the computers of unsuspecting visitors to the websites of popular news media and online stores. The gang was able to remotely access the victims' computers to steal the details of online banking log-ins and passwords. They then used fraudulent payment orders to transfer funds from the victims' account to their own specially prepared accounts.

The gang operated as a legitimate data recovery company, complete with a fully operational front office and used normal business services including an accountant, as well as other professionals, to hide evidence of the stolen cash. Money was cashed via company bank cards or fake cards in the name of dummy individuals.

Several hosting providers were used by the gang to enable their web activities and to serve the malicious botnets that defrauded banking customers around the world. These hosting providers can now be revealed as:

- AS51377 BurstNET Limited
- AS21788 BurstNET NOC
- AS47614 Limited Liability Company "Mega-NN"
- AS6367 Embarq Corporation
- AS21844 ThePlanet.com Internet Services, Inc.
- AS51630 SIA BUSINESS AVIATION SERVICES OFFLINE
- AS21793 GOGAX

Security analysts will be familiar with some of these names and many show interesting patterns of cybercriminal activity. (See SiteVet analysis of individual ASes). Note too, the presence of BurstNet and NOC.

Group-IB CEO Ilya Sachkov said, *"Our experts did an enormous amount of work, which resulted in identifying the head of this criminal group, the owner and operator of a specialized banking botnet, identifying the control servers, and identifying the directing of traffic from popular websites in order to spread malware infection. The investigations conducted by our Forensics Lab confirmed the use of the Win32/Carberp and Win32/Rdpdor malware by the criminals in order to carry out theft of funds."*

Frequently Asked Questions

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.

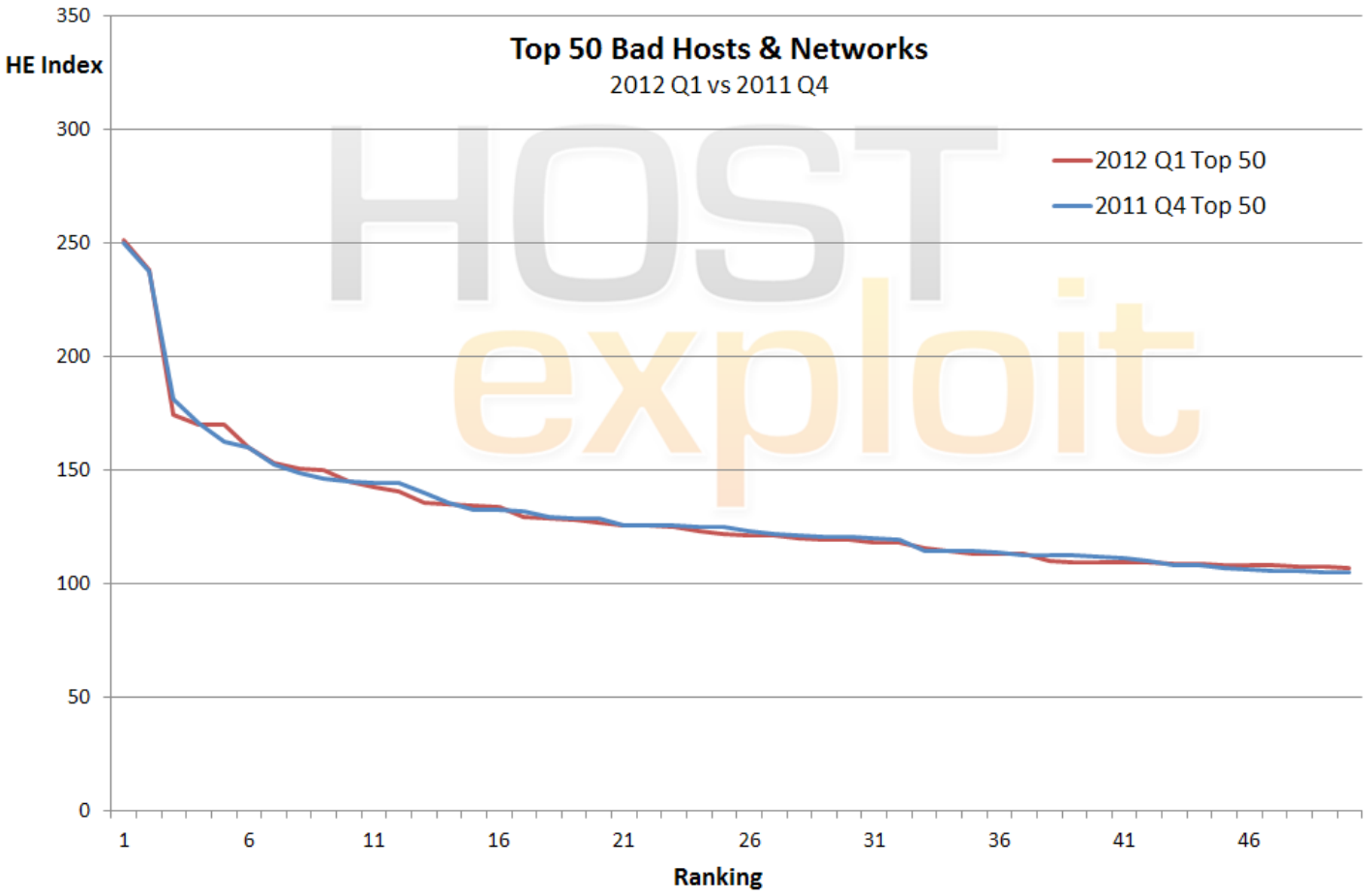
Further feedback is warmly welcomed

contact@hostexploit.com

4. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲ 1	251.64	16138	INTERIAPL INTERIA.PL Sp z.o.o.	PL	4,096
▼ 2	238.20	47583	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	LT	5,376
▼ 3	174.66	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	44,032
▲ 4	170.09	41947	WEBALTA-AS OAO Webalta	RU	15,392
➤ 5	169.92	32475	SINGLEHOP-INC - SingleHop	US	258,816
▲ 6	159.85	40034	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	VG	4,352
▲ 7	152.87	16125	DC-AS UAB Duomenu Centras	LT	5,632
▲ 8	150.82	31133	MF-MGSM-AS OJSC MegaFon	RU	20,224
▲ 9	150.26	16276	OVH OVH Systems	FR	672,000
▲ 10	145.26	29568	COMTEL-AS SYSNET SECURE S.R.L.	RO	17,920
▲ 11	142.60	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	1,098,240
▼ 12	140.76	32613	IWEB-AS - iWeb Technologies Inc.	CA	252,160
▼ 13	135.58	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,536,512
▲ 14	135.12	28753	LEASEWEB-DE Leaseweb Germany GmbH	DE	116,992
▲ 15	134.09	40824	WZCOM-US - WZ Communications Inc.	US	13,056
▲ 16	133.65	24940	HETZNER-AS Hetzner Online AG RZ	DE	504,832
▲ 17	129.36	32181	ASN-GIGENET - GigeNET	US	42,240
▲ 18	128.55	39743	VOXILITY-AS Voxility SRL	RO	17,408
▲ 19	128.35	45899	VNPT-AS-VN VNPT Corp	VN	2,265,600
▲ 20	126.60	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	111,385,888
▼ 21	125.77	10297	ENET-2 - eNET Inc.	US	90,112
▲ 22	125.57	9280	CIA-AS connect infobahn australia (CIA)	AU	8,704
▲ 23	125.17	9891	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	TH	19,456
▼ 24	122.85	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM - CDMA...	IN	245,760
▼ 25	121.87	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,312
▲ 26	121.35	34201	PADICOM PADICOM SOLUTIONS SRL	EU	7,168
▲ 27	121.17	9809	NOVANET Nova Network Co.Ltd... Futian District, Shenzhen, China	CN	10,496
▲ 28	120.05	35415	WEBAZILLA WebaZilla European Network	UA	61,440
▲ 29	119.58	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	86,016
▲ 30	119.50	16265	LEASEWEB LeaseWeb B.V.	NL	305,152
▼ 31	118.19	3595	GNAXNET-AS - Global Net Access, LLC	US	147,200
▼ 32	118.17	9198	KAZTELECOM-AS JSC Kazakhtelecom	KZ	2,189,312
▲ 33	115.46	43637	SOL-AS SOL Ltd	AZ	7,936
▲ 34	114.43	29854	WESTHOST - WestHost, Inc.	US	51,712
▲ 35	113.39	44112	SWEB-AS SpaceWeb JSC	RU	3,072
▼ 36	113.34	21788	NOC - Network Operations Center Inc.	US	285,952
▼ 37	113.00	6697	BELPAK-AS Republican Association BELTELECOM	BY	1,420,544
▲ 38	110.11	43146	AGAVA3 Agava Ltd.	RU	17,920
▲ 39	109.45	30496	COLO4 - Colo4, LLC	US	181,760
▲ 40	109.39	26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC	US	1,336,064
▲ 41	109.34	49505	SELECTEL Selectel Ltd.	RU	11,008
➤ 42	109.10	31034	ARUBA-ASN Aruba S.p.A. - Network	IT	131,840
▼ 43	108.64	22489	CASTLE-ACCESS - Castle Access Inc	US	48,128
▼ 44	108.44	8972	PLUSSERVER-AS intergenia AG	DE	147,456
▼ 45	108.18	26347	DREAMHOST-AS - New Dream Network, LLC	US	284,416
▲ 46	107.93	9120	COHAESIONET Cohaesio A	DK	17,920
▲ 47	107.93	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	PK	3,908,608
▲ 48	107.75	27990	Hosting Panama	PA	5,888
▼ 49	107.36	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
▲ 50	106.66	23352	SERVERCENTRAL - Server Central Network	US	238,336

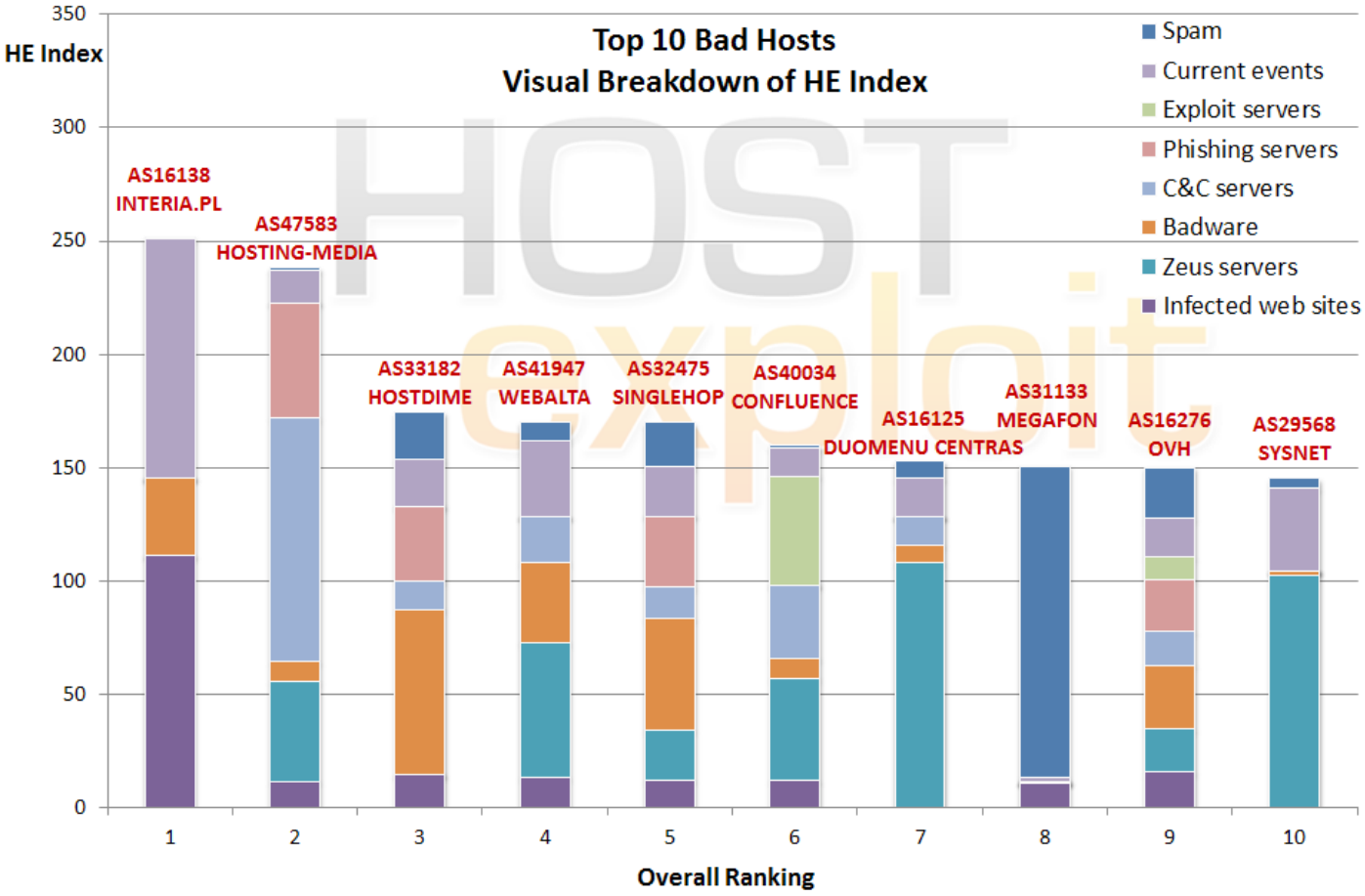
2012 Q1 to 2011 Q4 Comparison



A comparison of the 'Top 50 Bad Hosts' in March 2012 with December 2011.

Despite several large movements of hosts in the Top 50, the overall distribution of concentrations of malicious activity has remained almost identical.

Top 10 Visual Breakdown



The above table gives a visual breakdown of the hosts in the Top 10 according to the HE Index.

It demonstrates the effectiveness of applying weightings to the different categories and ensures that the HE Index is a balanced measurement. This can be seen by the lack of a dominate source of 'badness' among the majority of the hosts.

Further, the visual representation clearly shows why each of the Top 10 ranked ASes is ranked so highly.

For instance, it can be seen that AS16138 INTERIA.PL is ranked #1 due to high concentrations of infected web sites, badware and current events (including XSS and RFI).

AS31133 MEGAFON, on the other hand, is ranked #8 almost entirely due to very large concentrations of spam activity.

What's New?

7.1. Overview

	Previous Quarter - Q4 2011			Current Quarter - Q1 2012		
	ASN	Name	Country	ASN	Name	Country
#1	47583	Hosting Media	LT	16138	Interia.pl	PL
#2	33182	HostDime	US	47583	Hosting Media	LT
#3	10297	eNET	US	33182	HostDime	US
#1 for Spam	55740	TATA Indicom	IN	31133	MegaFon	RU
#1 for Botnets	47583	Hosting Media	LT	47583	Hosting Media	LT
#1 for Zeus Botnet	16125	Duomenu Centras	LT	16125	Duomenu Centras	LT
#1 for Phishing	45634	Sparkstation	SG	9280	Connect Infobahn Australia	AU
#1 for Exploit Servers	36444	Nexcess.net	US	3.537	Infium	CZ
#1 for Badware	33626	Oversee.net	US	9809	Nova Network	CN
#1 for Infected Sites	25795	ARP Networks	US	16138	Interia.pl	PL
#1 for Current Events	16138	Interia.pl	PL	16138	Interia.pl	PL

An analysis of quarterly trends gives an insight into how highly hosting providers rate responsible hosting.

For a responsible host, the shock of finding they are ranked unusually high, or even worse in the #1 position, can be enough to prompt immediate remedial action.

AS47583 Hosting Media and AS16125 Duomenu Centras, however, have both remained at #1 for the presence of botnets and Zeus botnets respectively. This is somewhat intuitive as botnets are persistent and can usually only be resolved through remediation such as takedowns.

Conversely, spam and phishing are faster-paced areas of activity and this quarter we have new #1 ranks in both sectors.

There are no hosts from the United States on top of any particular category for the first time in this series of host reports.

7.2. Top 10 Newly-Registered Hosts - In Q1 2012

By end of Q1 2012 there were **40,678** ASes; an increase of **902** from end of Q4 2011.

Below we show a selection of 10 ASes registered in Q1 2012 with the highest HE Indexes. With significant levels of badness recorded in a short period of time, these hosts are of interest.

Listed below the 10 Q1 ASes are the same findings in the previous two quarterly reports.

As expected, several of the 10 ASes in this quarter's list are very small, with 3 having the smallest possible allocated IP block (/24; 256 IPs). This suggests that they are "disposible" ASes for malicious purposes. All 3 of these ASes are Ukraine-registered.

It is interesting to note that in the last 3 quarterly reports, of the 30 newly-registered ASes we have highlighted as being of interest, 6 of these no longer exist.

Period	HE Rank	HE Index	AS number	AS name	Country	# of IPs
2012 Q1	274	67.0	48031	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	UA	16,640
	653	50.8	12327	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business international	GB	4,608
	906	44.6	49087	PODCEM-AS Open JSC "Podilskiy Tcement"	UA	256
	1,337	35.3	24768	ALMOUROLTEC ALMOUROLTEC SERVICOS DE INFORMATICA E...	PT	2,048
	1,828	27.8	51699	ANTARKTIDA-PLUS-AS Antarktida-Plus LLC	UA	256
	1,875	27.3	49236	RELNET-AS TOV "Leksim"	UA	256
	1,948	26.4	57704	SPEED-CLICK-LTD SpeedClick for Information Technology and...	IL	2,048
	2,053	25.4	31408	ORANGE-PALESTINE Orange Palestine Group Co. for Technological...	PS	1,024
	2,212	24.0	37385	SONITEL	NE	8,960
	2,260	23.7	34109	AS34109 CB3ROB Ltd. & Co. KG	NL	9,216
2011 Q4	740	46.7	21508	COMCAST-21508 - Comcast Cable Communications Holdings, Inc	US	256
	1,356	34.0	4213	VPLSNET-EAST - VPLS Inc. d	US	2,048
	1,644	29.2	27626	AS-JOYTEL - Joytel	US	1,024
	1,986	25.2	57374	GIV-AS Commercial radio-broadcasting company Cable operator...	MK	7,168
	2,063	24.4	47311	ASBRESTRW Transport Republican unitary enterprise...	BY	256
	2,181	23.6	4.459	--No Registry Entry--	BR	256
	2,189	23.5	43463	BST-AS Biuro sprendimu tinklas UAB	LT	3,072
	2,406	21.9	57446	TELEMONT-AS Telemont Service S.R.L.	EU	4,096
	2,596	20.6	28015	MERCO COMUNICACIONES	AR	22,528
	2,905	18.7	3.961	ENERGOMONTAZH-AS ENERGOMONTAZH ltd.	EU	256
2011 Q3	57	98.1	9931	CAT-AP The Communication Authoity of Thailand, CAT	TH	209,920
	160	72.4	9929	CNCNET-CN China Netcom Corp.	CN	1,182,944
	269	64.6	33491	COMCAST-33491 - Comcast Cable Communications, Inc.	US	2,304
	333	61.4	9924	TFN-TW Taiwan Fixed Network, Telco and Network Service Provider.	TW	3,908,352
	364	60.6	7725	COMCAST-7725 - Comcast Cable Communications Holdings, Inc	US	1,536
	452	54.2	33668	CMCS - Comcast Cable Communications, Inc.	US	256
	460	53.9	9919	NCIC-TW New Century InfoComm Tech Co., Ltd.	TW	1,102,848
	542	50.6	33652	CMCS - Comcast Cable Communications, Inc.	US	1,024
	743	44.9	33489	COMCAST-33489 - Comcast Cable Communications, Inc.	US	0
	756	44.6	33490	COMCAST-33490 - Comcast Cable Communications, Inc.	US	1,024

7.3. Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-91.7%	33	114.5	5,023	9.5	25795	ARPNET - ARP NETWORKS, INC.	US	12,288
-72.4%	4	170.8	785	47.2	45634	SPARKSTATION-SG-AP 10 Science Park Road	SG	3,072
-64.5%	49	105.2	1,228	37.3	12260	COLOSTORE - Colostore.com	US	53,248
-55.3%	34	114.1	646	51.1	31147	INLINE-AS Inline Internet Online Dienste GmbH	DE	11,264
-43.4%	26	122.9	247	69.6	36444	NEXCESS-NET - NEXCESS.NET L.L.C.	US	247,040
-41.9%	22	125.8	186	73.1	45538	ODS-AS-VN Online data services	VN	9,472
-41.1%	80	89.8	581	52.9	18059	DTPNET-AS-AP DTPNET NAP	ID	21,248
-38.9%	109	82.2	672	50.2	38676	AS33005-AS-KR wizsolution co.,Ltd	KR	11,136
-38.6%	25	124.9	143	76.6	15149	EZZI-101-BGP - Access Integrated Technologies, Inc.	US	28,928
-38.5%	21	125.9	139	77.4	29873	BIZLAND-SD - The Endurance International Group...	US	96,768

The hosts in the above table have all demonstrated a dramatic reduction in levels of badness in the three months since our Q4 2011 report was published.

Many forms of malicious activity can be inextricably linked, appearing as an intractable issue to some hosts. However, we applaud the efforts of these 10 most improved hosts that vary significantly in size, location, area of business and categories of badness improved. They demonstrate that it is possible under all circumstances to reduce badness levels with some extra effort and out-of-the-box thinking.

Noteworthy improvements include:

- AS45634 Sparkstation, down from #4 to #785. A remarkable reduction, having all but eliminated sources of phishing servers and badware from their network.
- AS25795 ARP Networks, with a large drop of 91.7% in HE Index, bringing it down to #5,023 from #33. Formerly low down in the ranks, ARP had a huge spike in activity in the previous quarter, with large numbers of infected web sites cropping up. Having seemingly addressed the issues immediately, it goes from being the Most Deteriorated host last quarter to the Most Improved host in this.

7.4. Deteriorated Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
1,106.1%	4,228	12.0	10	145.3	29568	COMTEL-AS SYSNET SECURE S.R.L.	RO	17,920
672.1%	3,623	15.0	33	115.5	43637	SOL-AS SOL Ltd	AZ	7,936
619.3%	4,258	12.0	107	86.0	3.537	ASINFIUM Infium Ltd.	CZ	10,496
530.6%	2,823	19.2	26	121.4	34201	PADICOM PADICOM SOLUTIONS SRL	EU	7,168
300.2%	1,822	26.9	48	107.8	27990	Hosting Panama	PA	5,888
266.2%	2,191	23.5	103	86.1	24282	KIR Kagoya Japan CO,LTD	JP	23,552
201.5%	1,640	29.3	93	88.2	15626	ITLAS ITL Company	UA	16,128
130.9%	712	47.4	41	109.3	49505	SELECTEL Selectel Ltd.	RU	11,008
129.7%	474	56.0	18	128.5	39743	VOXILITY-AS Voxility SRL	RO	17,408
111.4%	845	44.5	72	94.1	13174	MTSNET OJSC "Mobile TeleSystems"...	RU	24,320

The hosts listed here display the biggest increases in levels of badness since the last quarter. For these hosts it is advised to undertake a review of recent changes, in order to account for the sudden rise in levels of bad activity. Newly registered hosts are covered in section 7.2.

The "standout" host this quarter is AS29568 Sysnet Secure with a dramatic rise in the rankings from over #4,000 to #10. Over the last quarter, the number of Zeus servers present on Sysnet has steadily increased, coinciding with a sharp rise in the number of malicious URLs being served.

AS43637 SOL has had nearly as sharp a rise in the rankings, due to a large number of XSS instances and malicious URLs, with the former seemingly causing the latter. It's likely that the majority of these instances are due to lax security from innocent victims.

Also of note is AS15626 ITL. Having being praised by HostExploit in the Q2 2010 report as a "good host" due to the lack of recorded malicious activity, the Ukraine-based host has moved up into the Top 100. This is in part due to the appearance of exploit servers on the AS. However, our records show that exploit servers popping up on ITL have been short-lived, and so we expect this rise to be only temporary.

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
36,474	**0.82**	**600**	OARNET-AS - OARnet	**US**	1,549,824
30,276	**1.02**	**8153**	NORTEL-NETWORKS NORTEL NETWORKS SA	**US**	762,624
26,466	**1.06**	**23537**	MICROSOURCEASN - Micro Source, Inc.	**US**	278,784
21,400	**1.09**	**46717**	EVERN-1 - Evernet Hosting	**US**	73,728
11,789	**1.12**	**6423**	EASYSTREET-ONLINE - EasyStreet Online Services, Inc.	**US**	63,744
11,785	**1.13**	**34744**	GVM S.C. GVM SISTEM 2003 S.R.L.	**RO**	668,928
11,748	**1.20**	**10355**	DSCGA - Digital Service Consultants	**US**	84,224
11,043	**1.85**	**3663**	NETNET-NET - NetNet	**US**	106,752
10,809	**1.90**	**20686**	BISPING Bisping & Bisping GmbH & Co. KG	**DE**	86,016
10,758	**1.92**	**9476**	INTRAPOWER-AS-AP IntraPower Pty. Ltd.	**AU**	78,592

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.

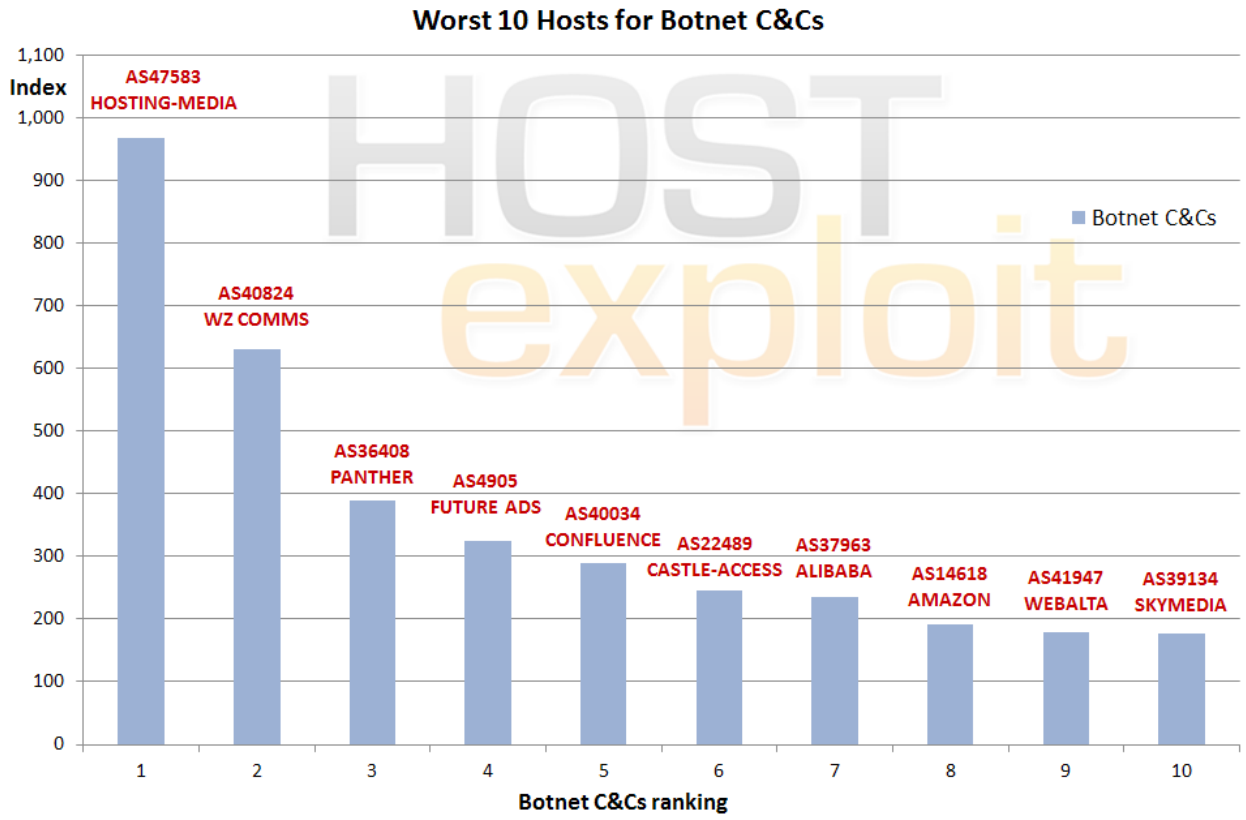
Bad Hosts by Topic

9.1.1. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
2	238.2	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**968.7**
15	134.1	**40824**	WZCOM-US - WZ Communications Inc.	**US**	13,056	**631.1**
243	69.7	**36408**	ASN-PANTHER Panther Express	**US**	45,568	**389.6**
703	49.3	**4905**	FA-LAX-1 - Future Ads LLC	**US**	256	**324.9**
6	159.8	**40034**	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	**VG**	4,352	**289.5**
43	108.6	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	48,128	**244.9**
320	63.3	**37963**	CNNIC-ALIBABA-CN-NET-AP Alibaba (China) Technology Co., Ltd.	**CN**	828,416	**234.9**
57	100.6	**14618**	AMAZON-AES - Amazon.com, Inc.	**US**	954,368	**191.7**
4	170.1	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,392	**179.4**
478	57.6	**39134**	SKYMEDIA United Network LLC	**RU**	16,384	**177.4**

The Botnet C&C Server category shows botnets hosted across a wide range of service provider types. Our own data is combined primarily with data provided by Shadowserver.

Many of the names here are well known and have been persistent members of the Botnet Top 10. Unlike faster-moving sectors such as spam and phishing, botnets require significantly more action to be taken to be shut down.



9.1.2. Phishing Servers

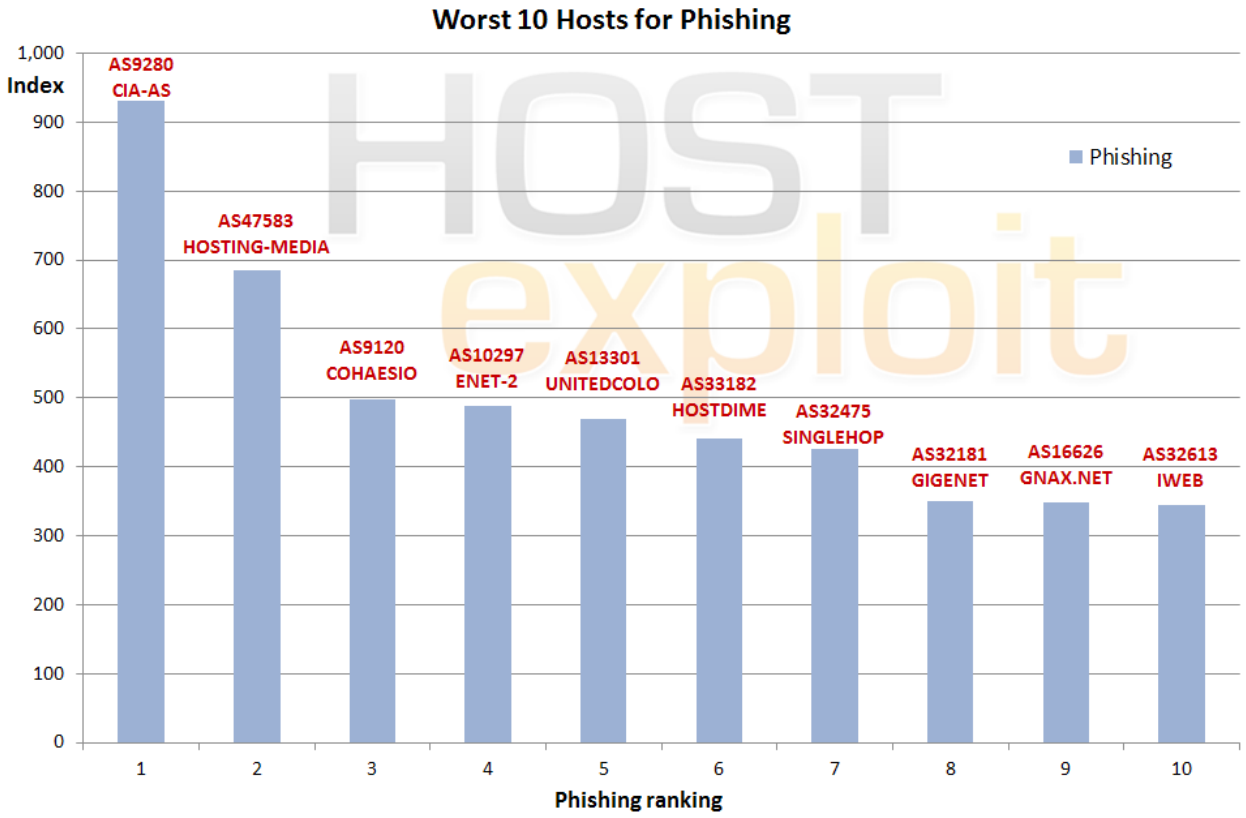
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
22	125.6	**9280**	CIA-AS connect infobahn australia (CIA)	**AU**	8,704	**930.8**
2	238.2	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**684.9**
46	107.9	**9120**	COHAESIONET Cohaesio A	**DK**	17,920	**497.8**
21	125.8	**10297**	ENET-2 - eNET Inc.	**US**	90,112	**488.9**
87	89.9	**13301**	UNITEDCOLO-AS UNITED COLO GmbH	**DE**	66,816	**469.1**
3	174.7	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	44,032	**440.7**
5	169.9	**32475**	SINGLEHOP-INC - SingleHop	**US**	258,816	**425.2**
17	129.4	**32181**	ASN-GIGENET - GigeNET	**US**	42,240	**349.9**
76	92.6	**16626**	GNAXNET-AS - Global Net Access, LLC	**US**	56,832	**347.3**
12	140.8	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	252,160	**344.7**

Phishing and social engineering in general continues to be a cause for concern to banks and corporations of all sizes.

Of note is the fact that the Phishing Top 10 contains ASes which are particularly high up in the overall rankings. This highlights the way in which phishing complements other areas of malicious activity.

Along with spam, phishing is key to directing victims to malicious locations.

In the case of phishing, it is often used in combination with badware - AS47583 Hosting Media and AS32475 SingleHop appearing in the Top 10 of both categories.



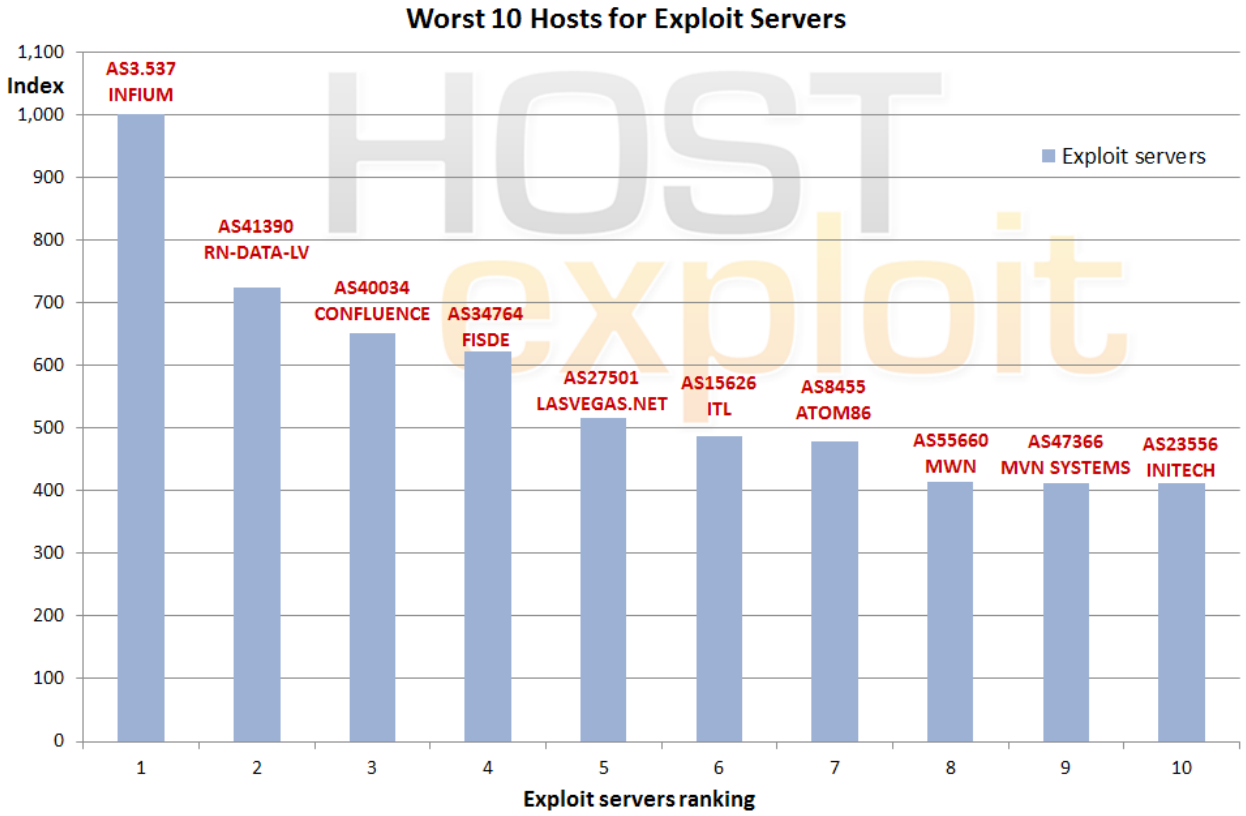
9.1.3. Exploit Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
107	86.0	**3.537**	ASINFIUM Infium Ltd.	**CZ**	10,496	**1,000.0**
81	91.3	**41390**	RN-DATA-LV RN Data, SIA	**LV**	1,280	**723.3**
6	159.8	**40034**	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	**VG**	4,352	**651.0**
48	107.8	**27990**	Hosting Panama	**PA**	5,888	**621.3**
987	42.9	**27501**	LASVEGASNET-AS - LasVegas.Net LLC	**US**	13,312	**516.3**
93	88.2	**15626**	ITLAS ITL Company	**UA**	16,128	**487.7**
145	76.6	**8455**	ATOM86-AS ATOM86 Autonomous System	**NL**	17,152	**478.4**
959	43.6	**55660**	MWN-AS-ID PT Master Web Network	**ID**	1,024	**415.2**
1,375	34.6	**47366**	MVN-AS MVN Systems Ltd	**BG**	1,280	**411.7**
1,563	31.5	**23556**	BANKTOWN-AS-KR INITECH	**KR**	1,280	**411.7**

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. See Appendix 2 for a full methodology.

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

Only one host – AS8455 ATOM86 – has remained in the Top 10 for Exploit Servers since the previous quarter. This is not so much indicative of the rate of change in this category (as is the case with spam and phishing), but as a result of exploits being served from compromised servers.



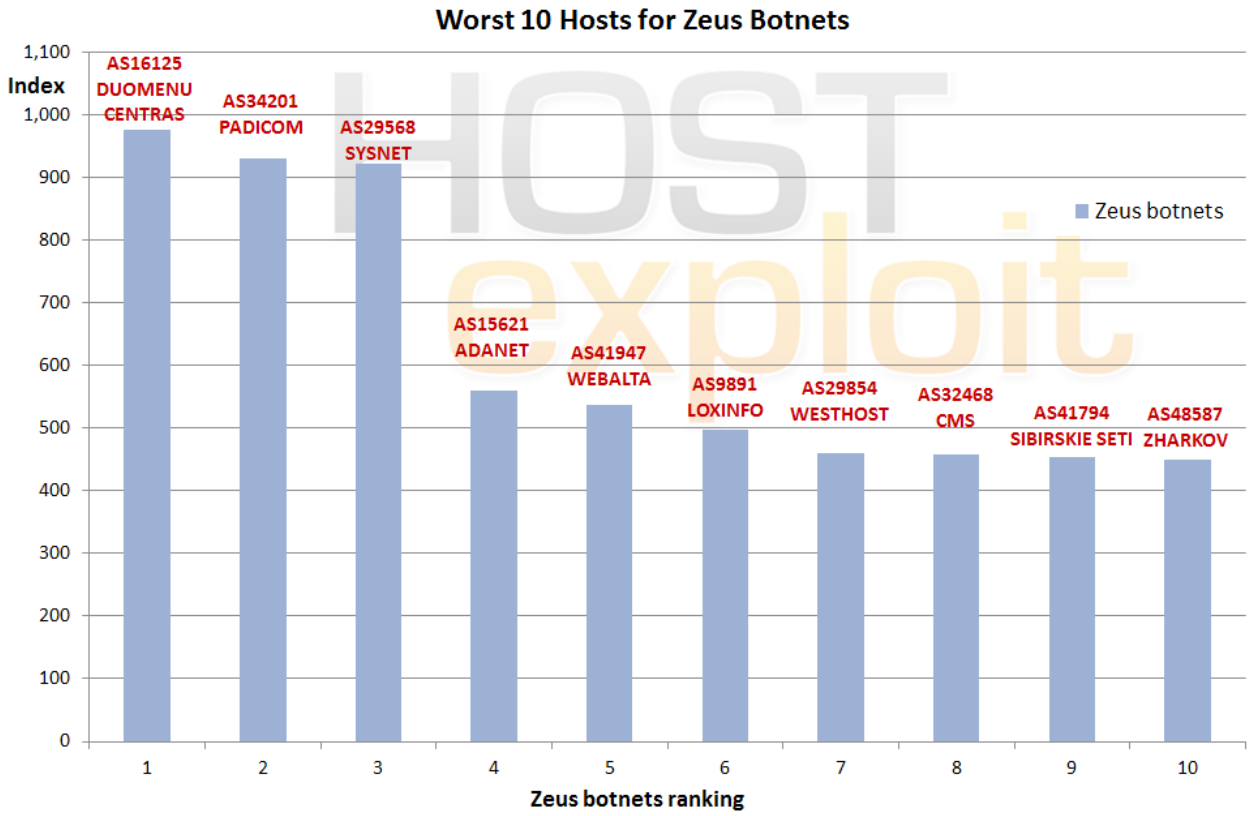
9.1.4. Botnet Hosting - Zeus

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
7	152.9	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,632	**975.1**
26	121.4	**34201**	PADICOM PADICOM SOLUTIONS SRL	**EU**	7,168	**929.8**
10	145.3	**29568**	COMTEL-AS SYSNET SECURE S.R.L.	**RO**	17,920	**921.0**
61	99.6	**15621**	ADANET-AS Azerbaijan Data Network	**RU**	13,312	**560.5**
4	170.1	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,392	**536.3**
23	125.2	**9891**	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	**TH**	19,456	**496.6**
34	114.4	**29854**	WESTHOST - WestHost, Inc.	**US**	51,712	**461.0**
559	54.0	**32468**	CMSSTL - Correctional Medical Services	**US**	512	**458.4**
542	54.6	**41794**	ALTLINE-AS Sibirskie Seti Ltd.	**RU**	768	**454.3**
135	78.5	**48587**	NET-0X2A-AS Private Entrepreneur Zharkov Mukola...	**UA**	1,024	**450.3**

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 upwards of 250,000 slave machines. The Zeus botnet remains the cheapest and most popular botnet on the underground market.

This section should be considered in conjunction with Section 9.1.3 on Exploit Servers.

This list often contains the names of hosts well-known to cybercrime observers and researchers, some of whom are frequent or repeat offenders. Among those names is AS41947 Webalta, which in addition to Zeus botnets, is hosting botnet C&Cs carrying out more typical SSH and IRC attacks.



9.2.1. Infected Web Sites

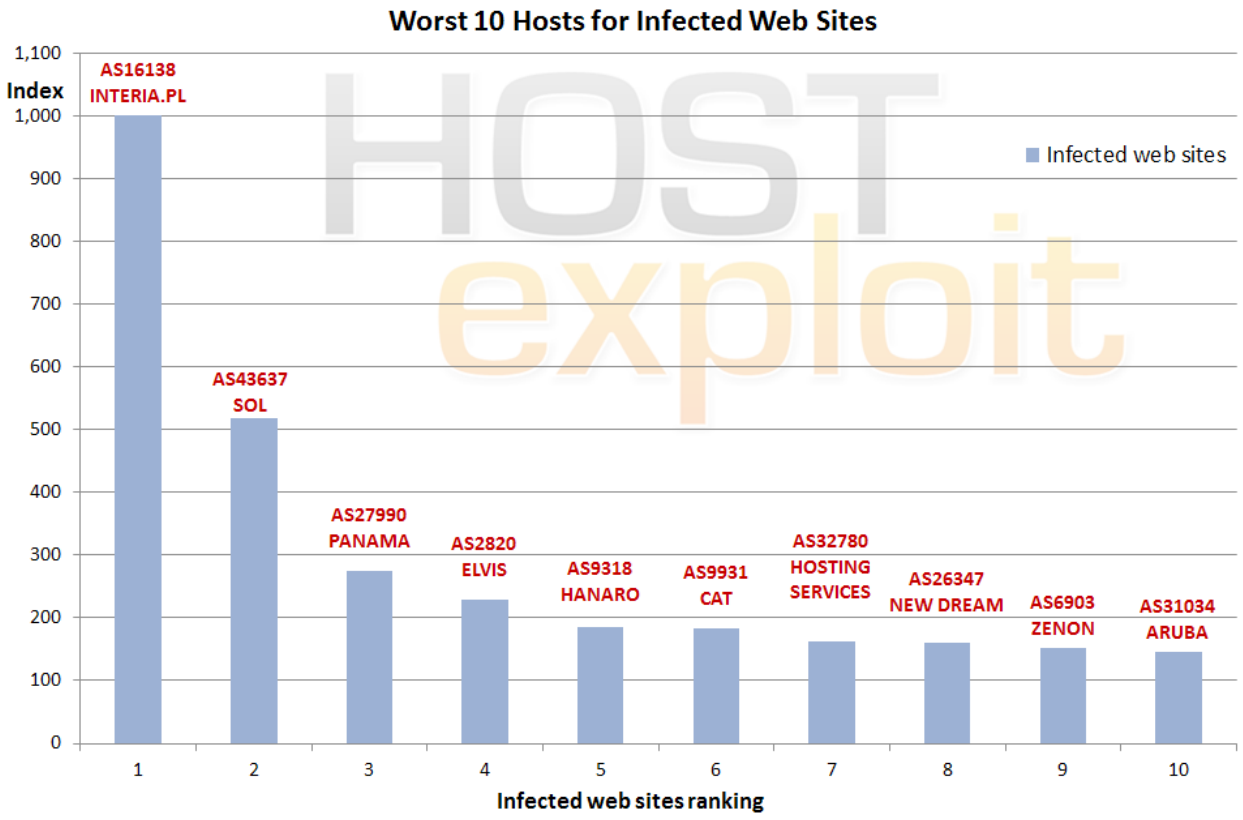
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
1	251.6	**16138**	INTERIAPL INTERIA.PL Sp z.o.o.	**PL**	4,096	**1,000.0**
33	115.5	**43637**	SOL-AS SOL Ltd	**AZ**	7,936	**518.0**
48	107.8	**27990**	Hosting Panama	**PA**	5,888	**275.7**
476	57.7	**2820**	ELVIS-AS ZAO "Elvis-Telecom"	**RU**	51,712	**229.8**
92	88.4	**9318**	HANARO-AS Hanaro Telecom Inc.	**KR**	14,989,312	**186.0**
51	106.2	**9931**	CAT-AP The Communication Authoity of Thailand, CAT	**TH**	209,664	**183.9**
177	73.6	**32780**	HOSTINGSERVICES-INC - Hosting Services, Inc.	**US**	12,288	**162.6**
45	108.2	**26347**	DREAMHOST-AS - New Dream Network, LLC	**US**	284,416	**159.3**
58	100.5	**6903**	ZENON-AS ZENON N.S.P.	**RU**	32,768	**151.6**
42	109.1	**31034**	ARUBA-ASN Aruba S.p.A. - Network	**IT**	131,840	**145.9**

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 Clean-MX and hphosts on instances of malicious URLs found on individual ASes.

The results show a mixed outcome with large hosts and a number of smaller, suspected crime servers.

#1 host for this quarter, AS16138 INTERIA.PL, comes out on top by a distance.



9.2.2. Spam

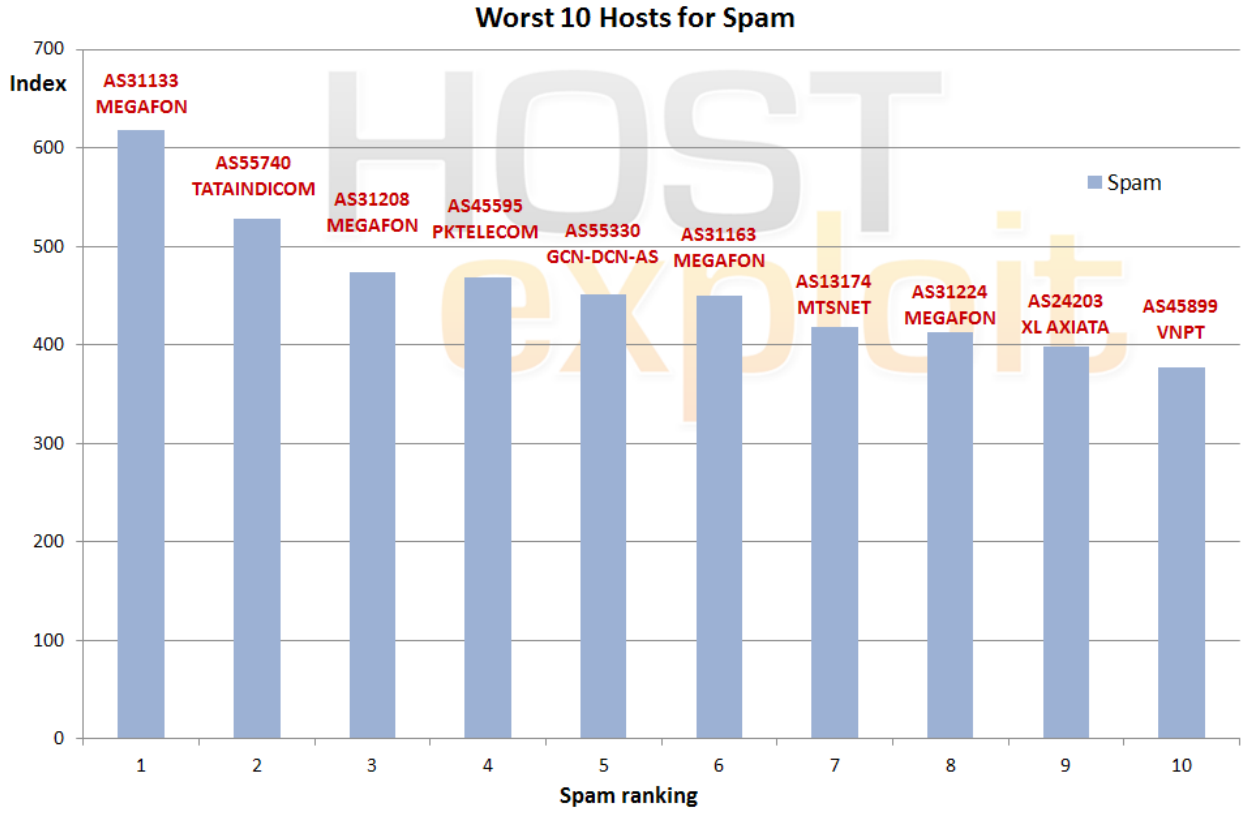
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
8	150.8	**31133**	MF-MGSM-AS OJSC MegaFon	**RU**	20,224	**618.1**
24	122.9	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM...	**IN**	245,760	**528.1**
52	105.4	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	4,096	**473.6**
47	107.9	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	3,908,608	**468.5**
59	100.3	**55330**	GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMMUN...	**AF**	19,712	**450.8**
60	100.1	**31163**	MF-KAVKAZ-AS JSC MegaFon	**RU**	5,120	**449.7**
72	94.1	**13174**	MTSNET OJSC "Mobile TeleSystems" Autonomous System	**RU**	24,320	**418.2**
79	91.8	**31224**	MF-UGSM-AS OJSC MegaFon Network	**RU**	5,120	**412.4**
90	88.7	**24203**	NAPXLNET-AS-ID PT Excelcomindo Pratama (Network Access...	**ID**	22,272	**398.6**
19	128.4	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,265,600	**376.4**

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 without fear of retribution.

This quarter, the position for MegaFon – the Russia-based mobile communications provider – has worsened, with an unprecented 4 ASes located in the Top 10 for spam.

MegaFon has had a long history with the sending of SMS spam, but the situation has become more severe with the rise of mobile malware – in particular the problem of malware from the Android market.

Trojans such as *Trojan-SMS.AndroidOS.Foncy* have transformed the problem from one of illicit advertising to one of more serious malicious activity with a tangible financial cost, by sending SMSes to premium numbers. It's clear that MegaFon is struggling to keep up more than any other provider.



9.2.3. Current Events

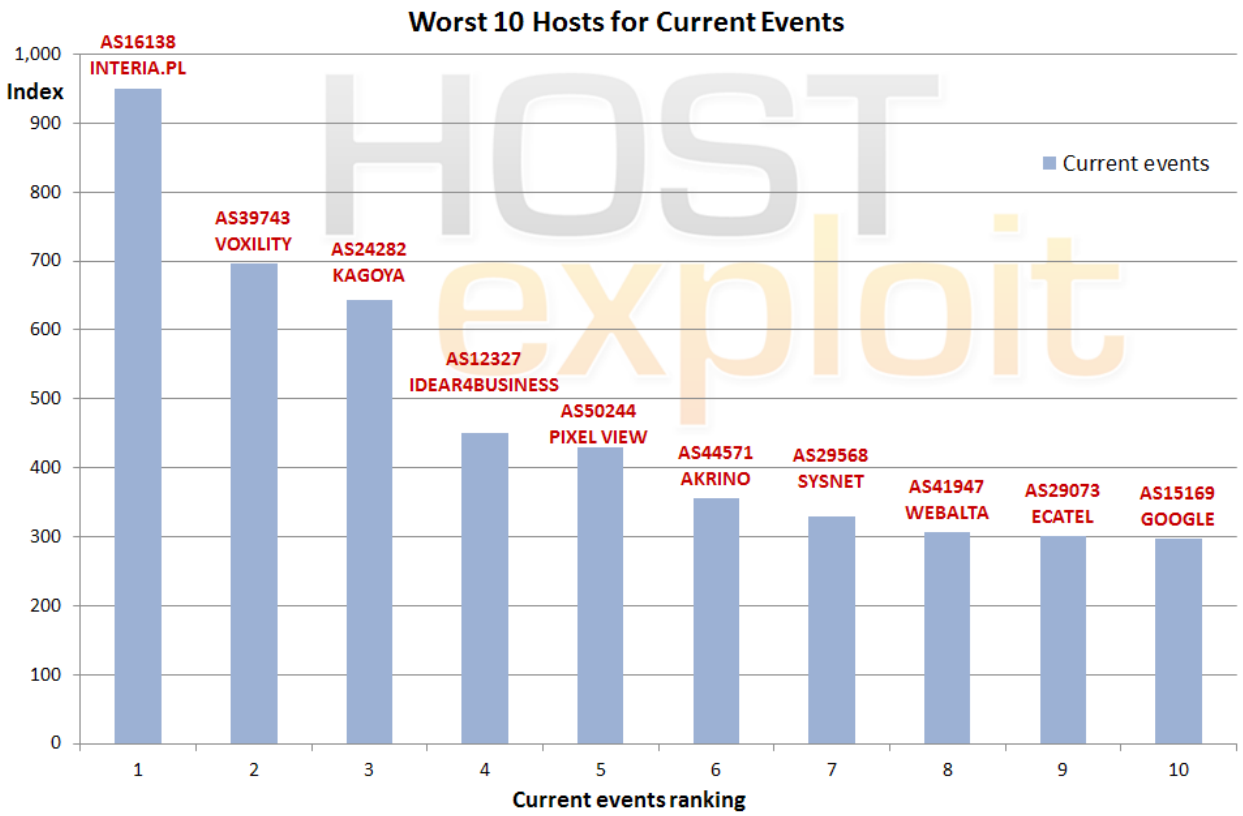
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
1	251.6	**16138**	INTERIAPL INTERIA.PL Sp z.o.o.	**PL**	4,096	**949.2**
18	128.5	**39743**	VOXILITY-AS Voxility SRL	**RO**	17,408	**696.1**
103	86.1	**24282**	KIR Kagoya Japan CO,LTD	**JP**	23,552	**643.9**
653	50.8	**12327**	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business...	**GB**	4,608	**449.6**
459	58.9	**50244**	ITELECOM Pixel View SRL	**RO**	7,936	**429.2**
573	53.4	**44571**	AKRINO-AS Akrino Inc	**RU**	1,024	**355.1**
10	145.3	**29568**	COMTEL-AS SYSNET SECURE S.R.L.	**RO**	17,920	**329.7**
4	170.1	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,392	**305.7**
25	121.9	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,312	**300.7**
62	99.5	**15169**	GOOGLE - Google Inc.	**US**	317,696	**297.1**

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, as well as newly emerged exploit kits which 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.

Having been previously dominated by US-based hosts, this quarter the majority in this Top 10 are located in Eastern Europe.



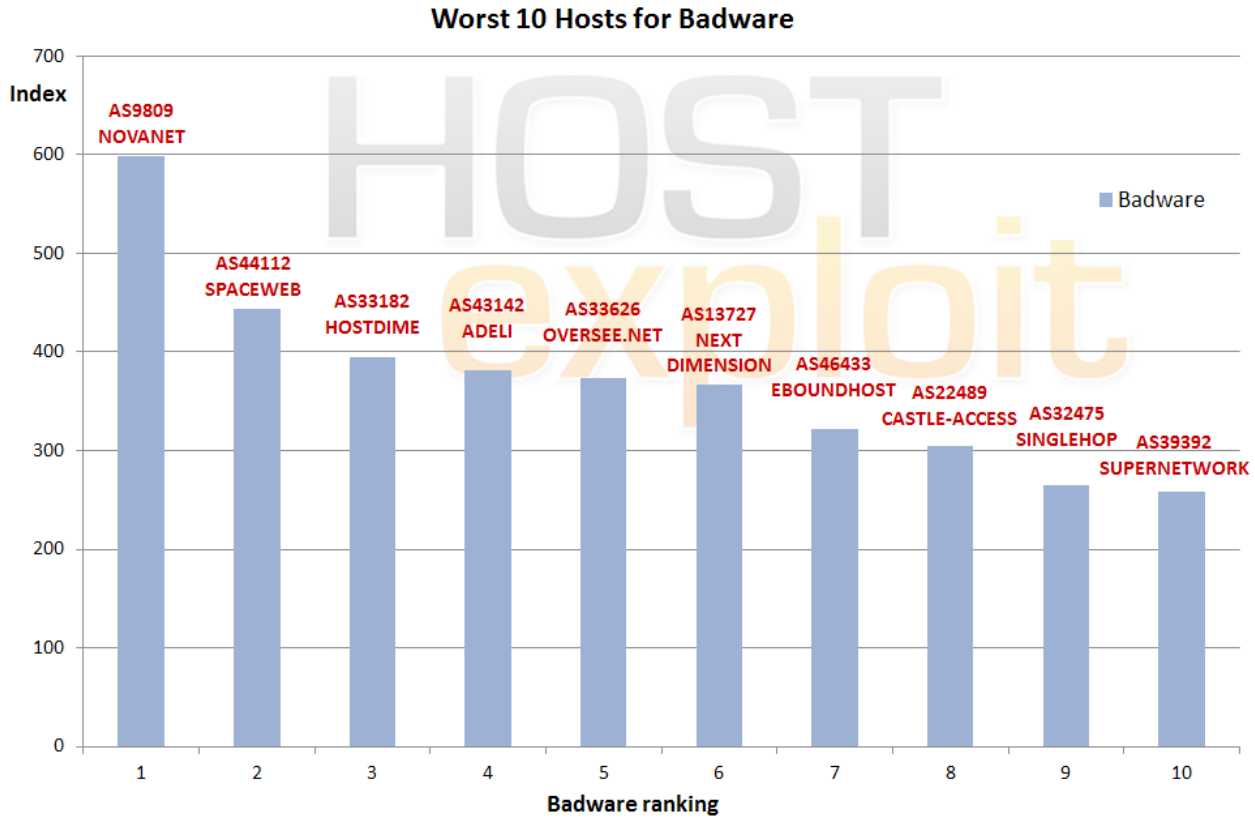
9.2.4. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
27	121.2	**9809**	NOVANET Nova Network Co.Ltd... Futian District, Shenzhen, China	**CN**	10,496	**598.3**
35	113.4	**44112**	SWEB-AS SpaceWeb JSC	**RU**	3,072	**443.4**
3	174.7	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	44,032	**394.6**
218	71.4	**43142**	ADELINOVIUS SARL Adeli	**FR**	5,120	**381.4**
49	107.4	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**373.7**
75	92.9	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**367.4**
112	84.3	**46433**	ADF01 - EBOUNDHOST.com	**US**	7,680	**322.0**
43	108.6	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	48,128	**304.9**
5	169.9	**32475**	SINGLEHOP-INC - SingleHop	**US**	258,816	**265.1**
89	89.3	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	49,664	**258.6**

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 that take browsers to unexpected web pages and keylogger programs that transmit personal data to malicious third parties.

The analysis into 'false positives', particularly regarding parked domains, has continued with our data partners this quarter. The results are starting to reflect this disparity with responsible hosts working in conjunction to further improve this analysis.

The findings in this category are primarily based on data from Google, Sunbelt Software and Team Cymru.



Conclusions

Conclusions

The Top 50 Bad Hosts and Networks report for Q1 2012 should remind us all why a highly visual format contributes to communicating and understanding some aspects from the results of our analysis that may otherwise not be so apparent.

For example, see how the Spam Ranking chart (section 9.2.2) highlights that MegaFon Network has 4 ASes in the Top 10 for this category. Here is evidence that the Android and smartphone malware that many security researchers have warned about for some time is now a huge problem for service providers and users alike. This situation will only worsen if service providers are slow to address the advancing problem of SMS trojans.

Another visual impact is found in the Top 10 chart for Infected Web Sites (section 9.2.1). This category represents a variety of malicious activities that threaten websites, something that AS16138 Interia.pl clearly has more problem controlling than many other hosts. Interia.pl is shown to be serving double the level of activity of the next nearest host in this category.

In fact, AS16138 Interia.pl clearly has a problem controlling many types of cybercriminal activities, including the Current Events category where it is again a clear leader of the pack for high levels of blended attack threats. These unacceptably high levels of badness that Interia are serving has earned it the #1 Bad Host title this quarter, although the former #1, now in #2, AS47583 Hosting Media, is a close second.

AS47583 Hosting Media has not shown any signs of improvement since the last quarter and is still displaying high levels of C&C servers and phishing servers among other exploits.

Elsewhere, HostExploit is proud to announce the arrival of a new tool that we have been working on for some time with our community partners - the Global Security Map. This is to be released in conjunction with the new *World Cybercrime Report* later in April, with APWG at CeCOS VI in Prague.

For now, an early preview is available at http://globalsecuritymap.com/.

Jart Armin

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

October 13, 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.
4.	October 2011	Sources refined. 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.

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

Table 2: Data sources

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

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

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)*