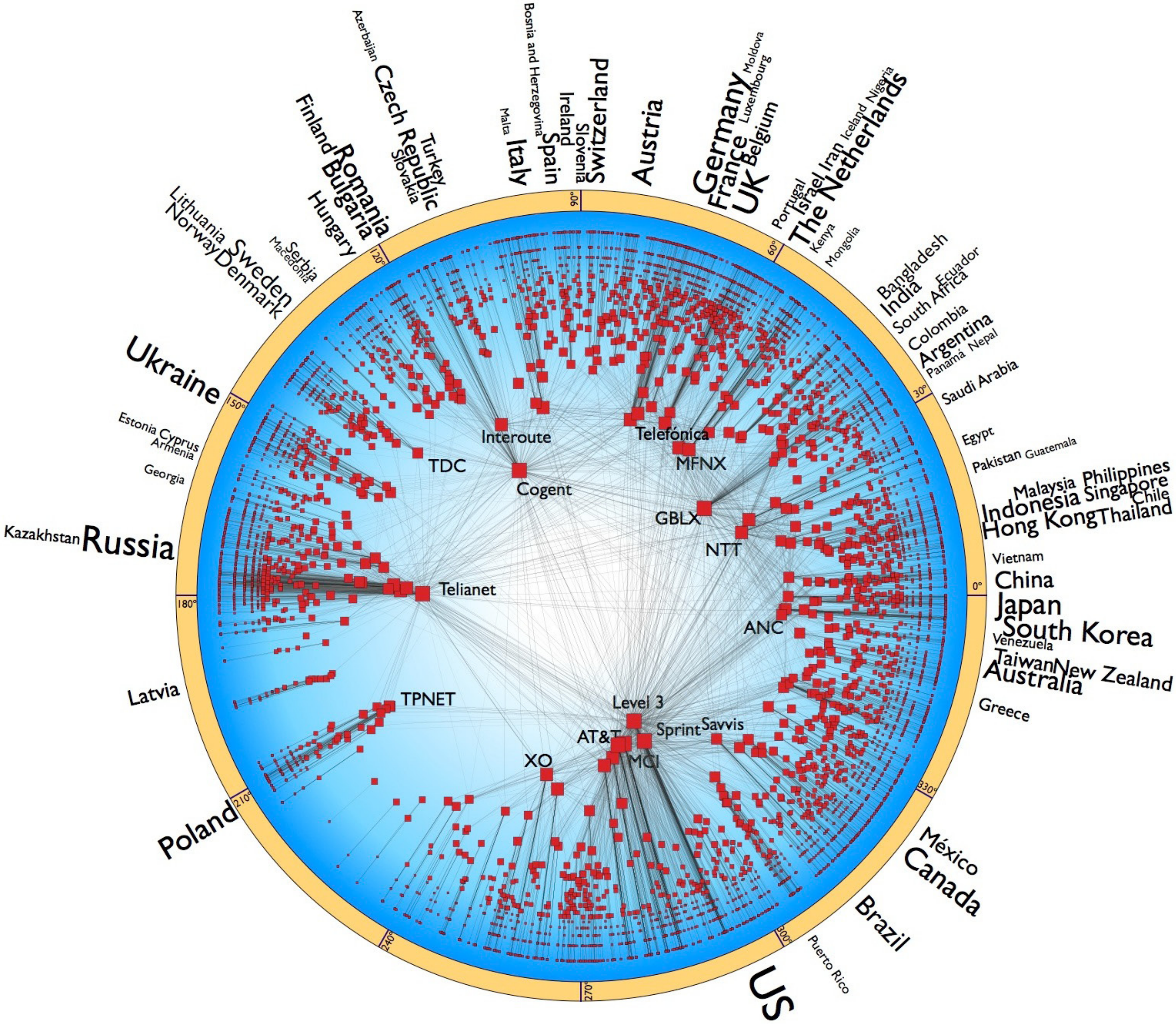
HostExploit - July 2011

HostExploit's Worldwide Cybercrime Series

Top 50 Bad Hosts and Networks 2nd Quarter 2011 - Report



SITEVET

HOST exploit

GROUP IB

Table of Contents

SITEVET HOST exploit GROUP iB

Top 50

CyberCrime Series

Bad Hosts and Networks

Backing from

nominettrust

www.nominettrust.org.uk

Edited by

- Jart Armin

Review

- Dr. Bob Bruen
- Raoul Chiesa
- Alexander Fominenkov
- Bogdan Vovchenko
- Sergey Nikitin
- Alexander Kalinin
- Vesta Matveeva
- Valeriy Baulin

Contributors

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

Comparative Data

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

Front page illustration: Bogu ñ á , M. et al. Sustaining the Internet with hyperbolic mapping. Nat. Commun. 1:62 doi: 10.1038 / ncomms1063 (2010).

Data Exfiltration

The hacking of well-known websites often attributed to or claimed by Anonymous or LulzSec has attracted much of the attention of the world's press recently. However, to put these in context, from April to June 2011 there were approximately 450,000 websites hacked or defaced; in 2010 around 1.5 million.

In the last quarter hackers have made some spectacular data extractions from well-known enterprises such as Sony, Citibank, RSA, and others. So once inside an enterprise, how do hackers exfiltrate all that data in so short a time? And how do they extract it without being detected?

The answer to the first question may surprise a few, because once hackers are in the system (or "own3d" in hacker terminology), weeks and even years of exfiltration may follow. For example, in one study conducted in 2009 on a sample of 218 breaches around the world, Trustwave's SpiderLabs found that on average, 156 days lapsed between an initial breach and its detection.

This is relatively short, in comparison to the discovery by McAfee Inc. (NYSE: MFE) of the "Night Dragon" APT (advanced persistent threat) attack, which hung around for up to four years. And the exfiltration of all the US State Department data for WikiLeaks took place over several months.

Contrary to what many perceive, hackers do not always try to make a quick getaway with their booty, although for some, a quick smash-and-grab is the name of the game. They can, however, lie low to avoid detection, waiting for the best time to make their escape or even extract small bits of data over a long period of time.

Hackers may store the stolen data in temporary password-protected RAR, ZIP, or CAB compressed folders or files, which are common enough to go unnoticed, until the utilized disk space becomes dangerously close to detection levels -- often somewhere around 1 per cent -- before leaving the premises.

In only 38 cases reported by Trustwave was the same remote access application used for entry as well as for exit. Breaches by malware, such as keystroke loggers' data exfiltration, most often used FTP and email capabilities, such a malicious SMTP server directly on the compromised system.

The most covert data extraction method is DNS (domain name server) exfiltration. This method can even be used on systems without a public network connection by resolving domain name queries outside the perimeter of trusted hosts through a series of internal and external nameservers.

While many server operations do observe and record log files from content serving, it is the database server that is often overlooked. More than any other type of query, outgoing DNS requests are permitted access to arbitrary hosts on the Internet. Even when firewalls are set up to prevent a database server from sending data straight to the Internet, hackers can send DNS requests from the internal DNS server using SQL injection.

Hackers also exploit automated time delays between transmitted packets. And they extensively use steganography, which is the exfiltration of data hidden within transmissions -- images, PDFs, or multimedia files. Additionally, spyware – and, if the hacker has physical access, surreptitiously hidden hardware devices -- is commonly used to perform data exfiltration.

Ultimately, hackers use our biggest weakness against us by monitoring "egress," or exit traffic, which receives scant attention in most organizations. Enterprises, in general, do not know enough about the data that they own and the flow of data within their own internal systems, let alone what data is leaving those systems.

Using Conficker & Hijacking the Zombies

The most notable success against cybercrime came from the Security Service of Ukraine releasing details about their part in an international operation, involving 10 countries; to stop the illegal activity of cybercriminals who allegedly used the Conficker virus infected PCs to fraudulently access bank accounts around the world.

The FBI had earlier announced that a criminal gang responsible for a highly sophisticated scareware scheme had been disrupted in a coordinated operation across several countries. The Ukrainian Security Service reports that its officers carried out searches in 19 premises and confiscated more than 74 units of computer equipment, about 300 units of electronic media, documentary materials and cash. It is reported that the cybercriminals stole more than 72 million U.S. dollars by illegally removing funds from bank accounts and transferring them to other bank accounts and international payment systems.

Investigators from the Security Service of Ukraine in Kyiv, Kharkiv and Luhansk interviewed 16 individuals who are believed to have been the organizers and coordinators of the international criminal group that operated under the guise of a legal commercial entity.

Law enforcement agencies in the USA, Great Britain, the Netherlands, France, Germany, Cyprus and Latvia carried out more than 30 searches and two people were arrested in Latvia. The Urainian Security Services reports that more than 40 bank accounts were seized in Latvia and Cyprus.

Securing the IT Supply Chain

Supply chain integrity is designated a Top 5 research priority by the EastWest Institute (EWI) think tank and the European Network and Information Security Agency (ENISA). But the topic is a challenging one to research.

Still, a paper from Chinese sources presented at the recent EWI Cybersecurity Summit in London tackles the subject in an innovative and practical way and proposes a solution.

The authors, Xiaofeng Qiu of Beijing University and Liang Zhao of NSFocus, say existing standards for supply chain soundness fail to properly include vulnerability testing. A weakness at any point of the supply chain could result in the injection of malicious code in hardware or software before components reach their destination. Supply chain integrity is, therefore, essential for IT security.

In this study, the researchers focus in particular on the failure of vulnerability testing to properly detect covert channels, places in a supply chain where information is transferred between processes where that should not be allowed to happen.

SSH Hacks

In May 2011 a major attack was made against a European IX (Internet Exchange).

The hacker(s) exploited a vulnerability in the SSH login procedure, utilizing "ssh_decoder" & "bfssh".

The attack was thwarted due to pro-active server security activity, but in analysis the bullet-proof hosting used as a base for the concerted attacks was via secretsline.biz - a specialist anonymzing VPN Service currently co-hosted via:

- AS24940 HETZNER (DE)
- AS3.135 INTERFRAME (a 32 bit ASN)
- AS35017 SWIFTWAY (NL)

Editor's Note

Data Standardization - A New Approach - Reducing the False Positives

The focus on these reports is generally on quantifying badness levels on the hosts worldwide. However, it's also important to consider the other side of the coin. Blacklists are helpful for hosts and registrars to identify the worst offenders, but this is only a small piece of the puzzle.

By using third-party blacklisting services, there is an inevitable delay in responding to blacklistings. For this reason, we recommend that blacklists are used as a secondary measure to identify patterns of activity that primary abuse processes do not pick up on.

Community blacklists are often operated by small groups of researchers and utilize manual techniques of investigation. This results in a good complement to automated processes such as IPS, IDS and firewalls, and of course good abuse procedures.

Such blacklists have expanded dramatically in the last few years, from a handful of useful services to several hundred in regular use, with most specializing in particular categories of malicious activity. One of the problems caused by such rapid expansion is a lack of cohesion and congruity between different lists. As a result, blacklists tend to compete rather than collaborate. For the most part, this isn't a deliberate strategy, but is borne out of the difficulty of sharing data. There are no real standards for sharing data, but different lists use their own formats (except in cases whereby the list is intended as a firewall or IDS ruleset, but this still doesn't facilitate data sharing as it is an end format).

The above factors are resulting in an increasing number of false positives on various blacklists. Some blacklists have procedures for removing these; some don't. Those that do may take quite some time before "whitelisting" any entries. And because of the lack of data standards, there is no standardized method for whitelisting in bulk.

With such a whitelisting service in place, hosts and registrars would be able to assist the blacklists by reporting data back to their lists. This would increase the quality of the data by removing incorrect entries which cloud the real issues, which ultimately helps both parties. The blacklist receives better data to analyze and use to improve their methodology, while the hosts have a more reliable dataset to clean up from.

A recent example is that of Google's Safe Browsing list. It is an excellent service which helps protect end-users from malicious and suspicious websites by blocking at the browser (used by default in Google Chrome and Mozilla Firefox). Working with Google recently was based on the possibility of false positives we were seeing on its Phishing list - over 80% of the listings of AS21740 eNom were false positives.

Google has now rolled out a process change which should see these false positives eliminated. This will assist hosts and registrars to focus on preventing proven and existing phishing, and malware.

Fortunately, Google has the resources to make such improvements to their methodology, but this isn't always the case for community blacklists. For these reasons we are working on a data standard to help facilitate collaboration between interested parties.

If you are interested in further information about this, or would like to assist in the writing of this standard, please contact us at contact@hostexploit.com.

Jart Armin

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.

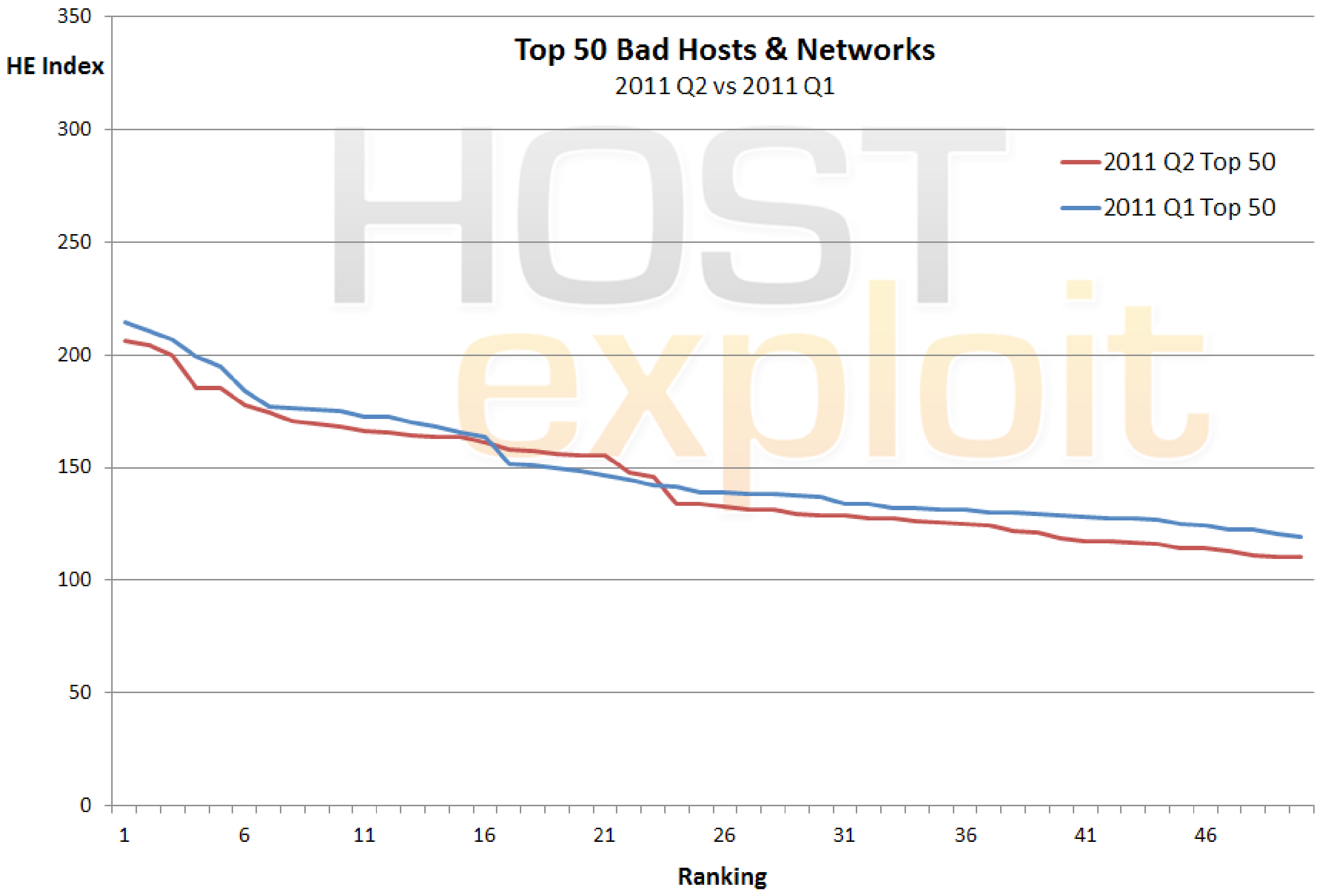
Further feedback is warmly welcomed

contact@hostexploit.com

3. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲ 1	206.0	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	39,680
► 2	204.6	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,568
▲ 3	200.1	10297	ENET-2 - eNET Inc.	US	90,880
▼ 4	185.3	41947	WEBALTA-AS OAO Webalta	RU	16,128
▲ 5	185.2	21788	NOC - Network Operations Center Inc.	US	282,624
► 6	177.8	36408	ASN-PANTHER Panther Express / CDNETWORKS-GLOBAL	US	37,376
▲ 7	174.2	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
▲ 8	170.9	36167	NETRIPLEX01 - NETRIPLEX LLC	US	46,080
▲ 9	169.4	46844	ST-BGP - SHARKTECH INTERNET SERVICES	US	75,520
▲ 10	168.3	9809	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	CN	11,008
▲ 11	166.3	28753	LEASEWEB-DE Leaseweb Germany GmbH (previously netdirekt e. K.)	DE	104,960
▼ 12	165.3	16138	INTERIAPL INTERIA.PL SA	PL	4,096
▼ 13	164.1	45899	VNPT-AS-VN VNPT Corp	VN	2,024,704
▲ 14	163.9	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,548,800
▲ 15	163.7	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	48,640
▼ 16	161.1	6851	BKCNET "SIA" IZZI	LV	49,152
▲ 17	157.8	33774	DJAWEB	DZ	67,840
▼ 18	157.0	24940	HETZNER-AS Hetzner Online AG RZ	DE	502,784
▲ 19	156.1	32475	SINGLEHOP-INC - SingleHop	US	218,624
▲ 20	155.4	36057	WEBAIR-AMS Webair Internet Development Inc	US	25,344
▼ 21	155.3	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	109,796,608
▼ 22	148.0	16276	OVH OVH	FR	546,816
► 23	145.8	13727	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024
▲ 24	133.8	50693	KONSING-GROUP Konsing group doo	SP	2,048
▼ 25	133.6	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	73,728
▲ 26	132.5	22489	CASTLE-ACCESS - Castle Access Inc	US	48,384
▲ 27	131.2	8560	ONEANDONE-AS 1&1 Internet AG	DE	357,888
▲ 28	131.0	26496	PAH-INC - GoDaddy.com, Inc.	US	1,135,616
▼ 29	129.5	6697	BELPAK-AS BELPAK	BY	747,520
▲ 30	128.9	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	887,552
▲ 31	128.5	40824	WZCOM-US - WZ Communications Inc.	US	8,960
▲ 32	127.3	37943	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology	CN	4,096
▲ 33	127.2	39150	TRANSIT-TELECOM-AS Tranzit Telecom LTD	RU	5,376
▲ 34	126.2	6400	CompaÃ±Ãa Dominicana de TelÃ©fonos, C. por A. - CODETEL	DO	390,912
▲ 35	125.6	15169	GOOGLE - Google Inc.	US	284,160
▲ 36	125.0	31147	INLINE-AS Inline Internet Online Dienste GmbH	DE	9,728
▲ 37	124.2	9050	RTD ROMTELECOM S.A	RO	1,645,824
▲ 38	122.0	11798	ACEDATACENTERS-AS-1 - Ace Data Centers, Inc.	US	235,520
▲ 39	121.1	35908	VPLSNET - VPLS Inc. d	US	714,240
▲ 40	118.7	16265	LEASEWEB LEASEWEB AS	NL	276,736
▼ 41	117.2	29182	ISPSYSTEM-AS ISPsystem Autonomous System	RU	35,840
▲ 42	117.2	23650	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone	CN	116,256
▼ 43	116.6	49981	WORLDSTREAM WORLDSTREAM AS	NL	11,520
▼ 44	116.1	30058	FDCSERVERS - FDCservers.net	US	242,432
▼ 45	114.4	24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	1,810,432
▲ 46	113.9	30083	SERVER4YOU - Hosting Solutions International, Inc.	US	20,480
▲ 47	113.2	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San	TR	13,056
▲ 48	111.0	14585	CIFNET - CIFNet, Inc.	US	7,680
▲ 49	110.3	51306	UAIP-AS PAN-SAM Ltd.	UA	2,048
▼ 50	110.2	32181	ASN-GIGENET - GigeNET	US	42,240

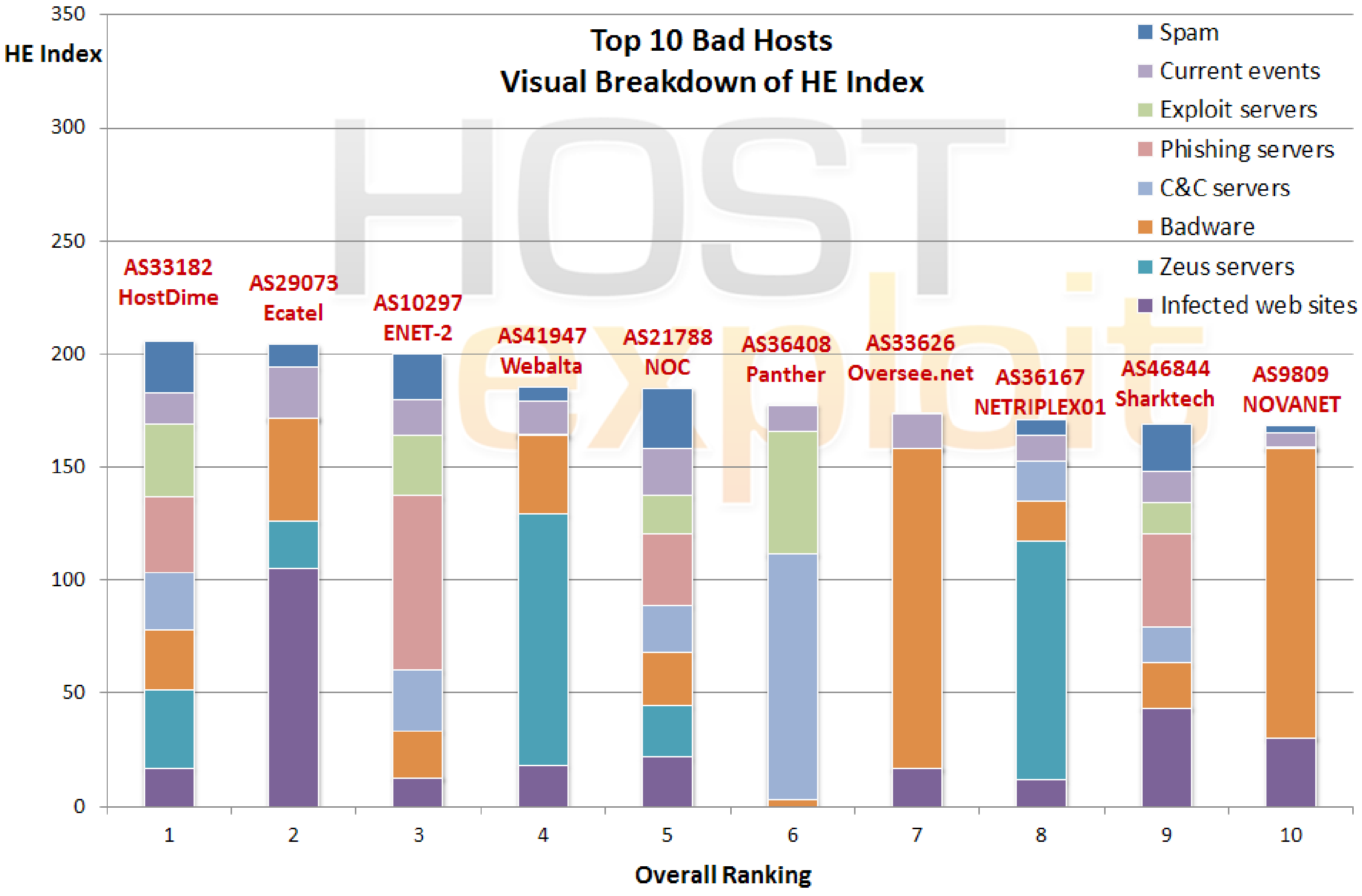
2011 Q1 to 2011 Q2 Comparison



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

On the whole, effective levels of badness remained fairly consistent 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 the weightings across different categories ensure that 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 AS33182 HostDime (US) is ranked #1 due to a wide range of issue, including spam, exploit servers, phishing servers and zeus servers as well as smaller concentrations of C&C servers, badware and infected web sites.

AS41947 Webalta (RU) has moved back down to #4 from #1 in the previous quarter's report.

6.

What’s New?

6.1. Overview

	Previous Quarter - Q1 2011			Current Quarter - Q2 2011		
	ASN	Name	Country	ASN	Name	Country
#1	41947	Webalta	RU	33182	HostDime	US
#2	29073	Ecatel	NL	29073	Ecatel	NL
#3	16138	Interia.pl	PL	10297	eNET	US
#1 for Spam	45899	VNPT	VN	33774	DJAWEB	DZ
#1 for Botnets	36408	Panther Express / CDNetworks	US	36408	Panther Express / CDNetworks	US
#1 for Zeus Botnet	49469	Sa Nova Telecom	RO	41947	Webalta	RU
#1 for Phishing	10297	ENET-2 - eNET Inc.	US	10297	ENET-2 - eNET Inc.	US
#1 for Exploit Servers	21607	DeployLinux	US	14585	CIFNet Inc.	US
#1 for Badware	33626	Oversee.net	US	33626	Oversee.net	US
#1 for Infected Sites	6851	BKCNET "SIA" IZZI	LV	29073	Ecatel	NL
#1 for Current Events	16138	Interia.pl	PL	16138	Interia.pl	PL

6.2. Top 10 Newly-Registered Hosts - In Q2 2011

HE Rank	HE Index	AS number	AS name	Country	# of IPs
146	78.3	33651	CMCS - Comcast Cable Communications, Inc.	US	768
179	73.5	33657	CMCS - Comcast Cable Communications, Inc.	US	256
210	70.4	11380	INTERNETOFFICEPARKS	ZA	0
295	60.6	49093	BIGNESS-GROUP-AS Bigness Group Ltd.	RU	512
572	51.1	3.196	IM-AS Info-Media LTD	RU	256
576	50.9	50073	SOFTNET Software Service Prague s.r.o.	CZ	256
584	50.7	44088	DORINEX-AS SC Dorinex Pord SRL	RO	768
768	45.7	42868	NIOBE Niobe Bilisim Backbone AS	US	4,096
817	44.4	48671	ECSRV-AS Production United Enterprise Econom-Service Ltd	UA	256
818	44.4	49798	SECUREHOST-NET-AS SecureHost LLC	RO	512

Note: by end of Q2 2011 there were **38,030** ASes; an increase of **759** from end of Q1 2011

6.3. Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-84.2%	**62**	112.3	**2,787**	17.8	**47764**	NETBRIDGE-AS... LLC... Mail.Ru	RU	12,032
-64.3%	**59**	113.0	**1,019**	40.4	**9280**	CIA-AS connect infobahn australia (CIA)	AU	8,704
-62.5%	**60**	112.7	**910**	42.3	**21607**	DEPLOYLINUX - DeployLinux Consulting	US	512
-60.4%	**34**	131.9	**539**	52.3	**31133**	MF-MGSM-AS OJSC MegaFon Network	RU	16,128
-57.0%	**81**	102.5	**831**	44.1	**13301**	UNITEDCOLO-AS... unitedcolo.de	DE	67,072
-56.8%	**54**	116.1	**600**	50.2	**23860**	ALLIANCE-GATEWAY-AS-AP...	IN	16,384
-55.2%	**50**	119.6	**514**	53.6	**40634**	FIRSTLOOK-COM - FirstLook, Inc.	US	512
-54.6%	**53**	117.0	**523**	53.1	**27715**	LocaWeb Ltda	BR	83,200
-53.1%	**159**	82.2	**1,094**	38.6	**34449**	MORDOVIA-AS... Mordovian Republic...	RU	63,488
-52.4%	**22**	144.6	**225**	68.8	**32613**	IWEB-AS - iWeb Technologies Inc.	CA	218,624

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 Q1 2011 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 :

AS47764 Netbridge - the AS which hosts the popular mail client Mail.ru is down from #2,787 to #62, with an 84% drop in effective badness levels.

A21607 DeployLinux - having been around the Top 50 for a long time, DeployLinux has made great improvements this quarter with a 62% drop in effective badness levels.

6.4. Deteriorated Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
5,370.4%	**22,632**	1.5	**112**	84.6	**49130**	ARNET-AS SC ArNet Connection SRL	RO	768
4,870.1%	**20,057**	1.5	**159**	76.9	**16125**	DC-AS UAB Duomenu Centras	LT	4,608
540.1%	**3,794**	13.3	**109**	85.2	**50465**	IQHOST IQHost Ltd	RU	1,024
289.8%	**1,978**	27.1	**62**	105.5	**50244**	ITELECOM Pixel View SRL	RO	7,936
125.6%	**1,413**	35.4	**131**	79.9	**42244**	ESERVER eServer.ru - hosting operator	RU	5,120
82.0%	**756**	49.4	**95**	90.0	**48587**	NET-0X2A-AS Zharkov Mukola...	UA	1,024
68.4%	**585**	55.5	**86**	93.6	**44112**	SWEB-AS SpaceWeb JSC	RU	3,072
48.7%	**553**	56.7	**113**	84.3	**8001**	NET-ACCESS-CORP - Net Access Corp...	US	503,040
40.2%	**130**	88.6	**37**	124.2	**9050**	RTD ROMTELECOM S.A	RO	1,645,824
35.9%	**109**	91.9	**36**	125.0	**31147**	INLINE-AS Inline Internet Online...	DE	9,728

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 6.2 for newly-registered hosts with the highest badness levels.

There are two "standout" host this quarter, both with staggering increases in effective badness levels.

Firstly, AS49130 ArNet (RO), which has climbed to #112, with just 768 allocated IP addresses.

Secondly, AS16125 Duomenu Centras (LT), which has climbed to ##159. Both of these hosts have appeared from relative anonymity in the previous quarter.

IQHost, ITelecom, Eserver and SpaceWeb have also had large increase in effective badness levels.

A noticable trend among these ASes is the small number of allocated IP addresses; this is often the case with smaller crime servers.

7.

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
23	UNITED STATES	6,118,400	3,397.0	147.7	167.8	94.5	192.6	215.7	195.0	261.5	130.4	55.2
4	GERMANY	975,360	579.5	144.9	270.3	191.9	149.9	132.4	112.0	188.8	118.7	70.9
4	CHINA	109,927,968	568.0	142.0	166.5	39.0	328.5	217.6	34.4	169.4	105.0	64.4
3	NETHERLANDS	301,824	439.9	146.6	452.8	172.1	218.1	57.1	0.1	53.9	151.5	55.3
3	RUSSIA	57,344	429.8	143.3	450.6	371.3	191.2	0.2	0.1	0.5	125.0	19.5
1	POLAND	4,096	165.3	165.3	107.4	0.2	275.8	0.3	0.2	0.7	949.5	3.2
1	VIETNAM	2,024,704	164.1	164.1	100.1	0.0	35.2	0.0	0.0	0.0	100.1	587.7
1	LATVIA	49,152	161.1	161.1	871.4	0.1	198.8	0.1	0.1	0.2	185.3	36.9
1	ALGERIA	67,840	157.8	157.8	64.3	0.0	53.1	0.1	0.1	0.2	0.0	616.1
1	FRANCE	546,816	148.0	148.0	161.5	140.8	142.1	144.6	262.0	210.6	119.2	106.2
1	CANADA	1,024	145.8	145.8	184.8	230.7	553.2	0.4	0.2	0.8	101.6	3.7
1	SERBIA	2,048	133.8	133.8	0.5	0.2	0.4	0.4	0.2	0.8	0.1	578.8
1	BELARUS	747,520	129.5	129.5	103.0	0.0	100.7	107.4	0.0	115.0	100.1	300.6
1	DOMINICAN REP.	390,912	126.2	126.2	0.0	0.0	0.0	0.0	0.0	0.0	27.3	533.0
1	ROMANIA	1,645,824	124.2	124.2	100.1	0.0	100.3	0.0	0.0	0.0	100.0	371.3
1	INDIA	1,810,432	114.4	114.4	100.2	0.0	100.1	0.0	0.0	0.0	100.0	329.0
1	TURKEY	13,056	113.2	113.2	32.7	0.1	116.2	202.5	0.2	557.6	100.9	59.0
1	UKRAINE	2,048	110.3	110.3	701.4	0.2	103.9	0.4	0.2	0.8	105.2	4.7

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
36,515	0.28	34744	GVM S.C. GVM SISTEM 2003 S.R.L.	RO	482,816
36,488	0.30	5583	ORANGE-BUSINESS-SERVICES-BENELUX Orange...	FR	343,040
36,436	0.34	3764	IA-HOU-AS - Internet America, Inc.	US	201,216
36,353	0.39	19855	ASN-MASERGY-US Masergy US Autonomous System	US	132,096
36,207	0.47	4004	ORANGE-BUSINESS-SERVICES-UK Orange...	US	83,968
36,205	0.47	17229	ATT-CERFNET-BLOCK - AT&T Enhanced Network Services	US	83,456
36,190	0.48	9476	INTRAPOWER-AS-AP IntraPower Pty. Ltd.	AU	78,080
36,154	0.49	41230	ASK4 Ask4 Limited	UK	73,728
36,125	0.51	18705	RIMBLACKBERRY - Research In Motion Limited	CA	67,072
35,977	0.57	3112	OARNET-AS-1 - OARnet	OH	220,160

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.

9.

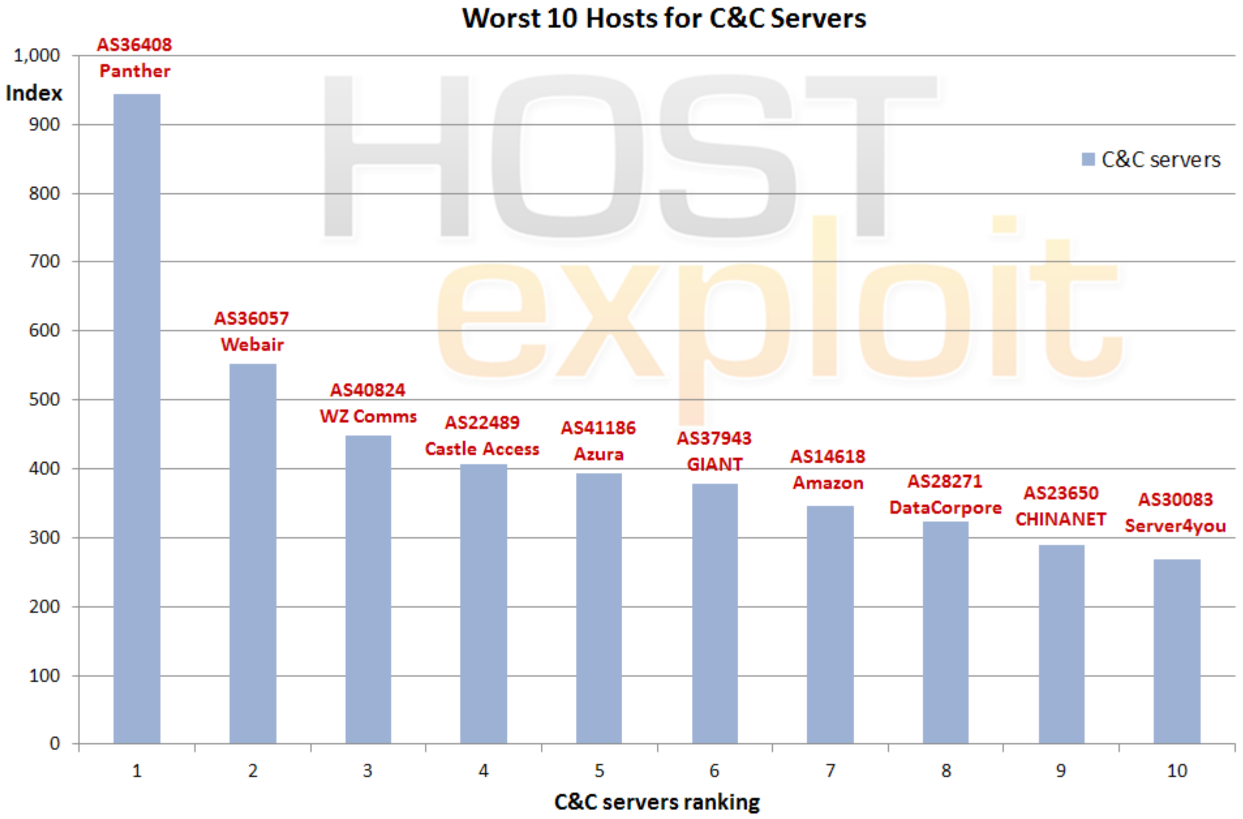
Bad Hosts by Topic

9.1.1. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
6	177.8	**36408**	ASN-PANTHER Panther Express / CDNETWORKS-GLOBAL	US	37,376	**943.8**
20	155.4	**36057**	WEBAIR-AMS Webair Internet Development Inc	US	25,344	**552.7**
31	128.5	**40824**	WZCOM-US - WZ Communications Inc.	US	8,960	**449.2**
26	132.5	**22489**	CASTLE-ACCESS - Castle Access Inc	US	48,384	**406.5**
94	91.3	**41186**	ISPFR-AS AZURA NETWORKS	FR	2,816	**394.0**
32	127.3	**37943**	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology...	CN	4,096	**378.7**
52	110.0	**14618**	AMAZON-AES - Amazon.com, Inc.	US	528,384	**345.8**
72	101.0	**28271**	DataCorpore ServiÃ§os e RepresentaÃ§Ãµes	BR	10,240	**323.3**
42	117.2	**23650**	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province...	CN	116,256	**290.3**
46	113.9	**30083**	SERVER4YOU - Hosting Solutions International, Inc.	US	20,480	**268.4**

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

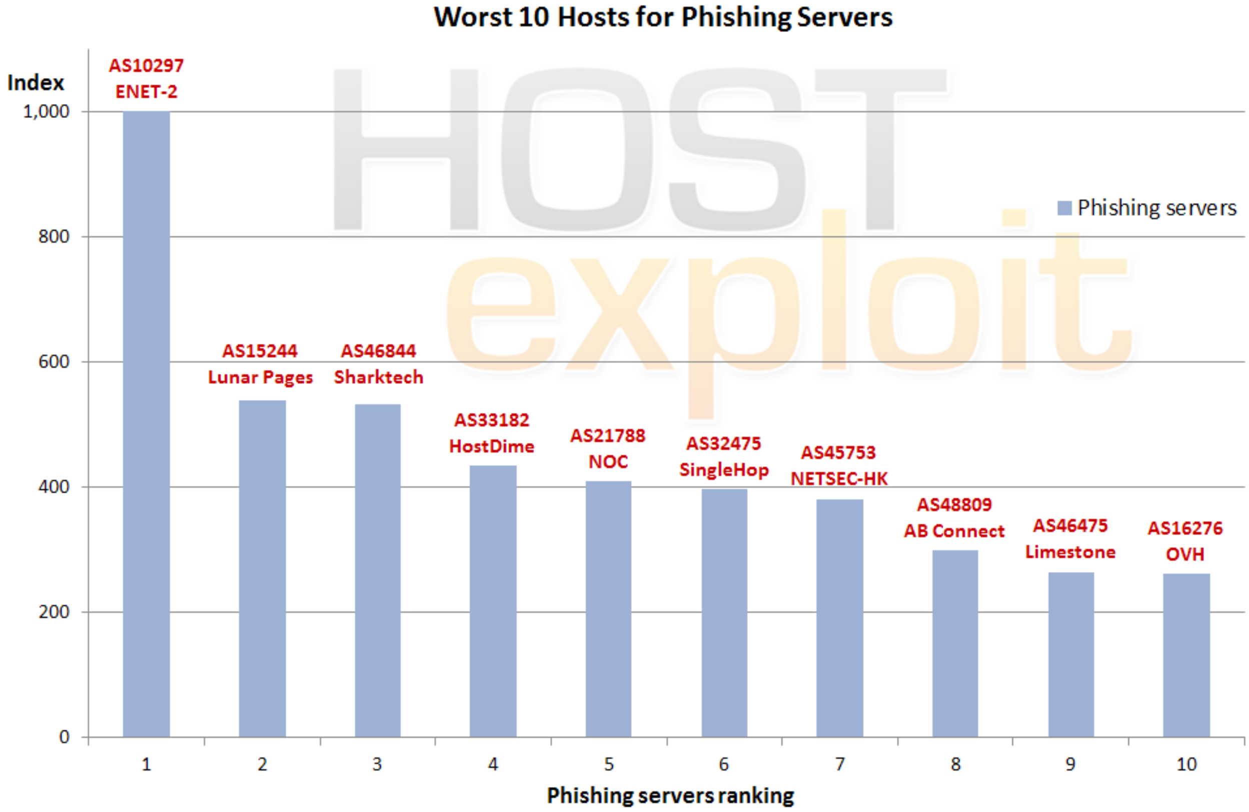
The position for the US appears to have remained consistent, with 6 out of the top 10 worst hosts for botnet C&Cs - the same number as in Q1.



9.1.2. Phishing Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
3	200.1	**10297**	ENET-2 - eNET Inc.	**US**	90,880	**1000.0**
15	163.7	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	**US**	48,640	**539.7**
9	169.4	**46844**	ST-BGP - SHARKTECH INTERNET SERVICES	**US**	75,520	**533.2**
1	206.0	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	39,680	**434.0**
5	185.2	**21788**	NOC - Network Operations Center Inc.	**US**	282,624	**410.4**
19	156.1	**32475**	SINGLEHOP-INC - SingleHop	**US**	218,624	**398.0**
89	93.4	**45753**	--No Registry Entry--	**HK**	113,408	**381.8**
435	56.8	**48809**	ABCONNECT AB CONNECT	**FR**	4,096	**299.2**
25	133.6	**46475**	LIMESTONENETWORKS - Limestone Networks, Inc.	**US**	73,728	**265.3**
22	148.0	**16276**	OVH OVH	**FR**	546,816	**262.0**

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 6 phishing hosts are all based in the US. 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.



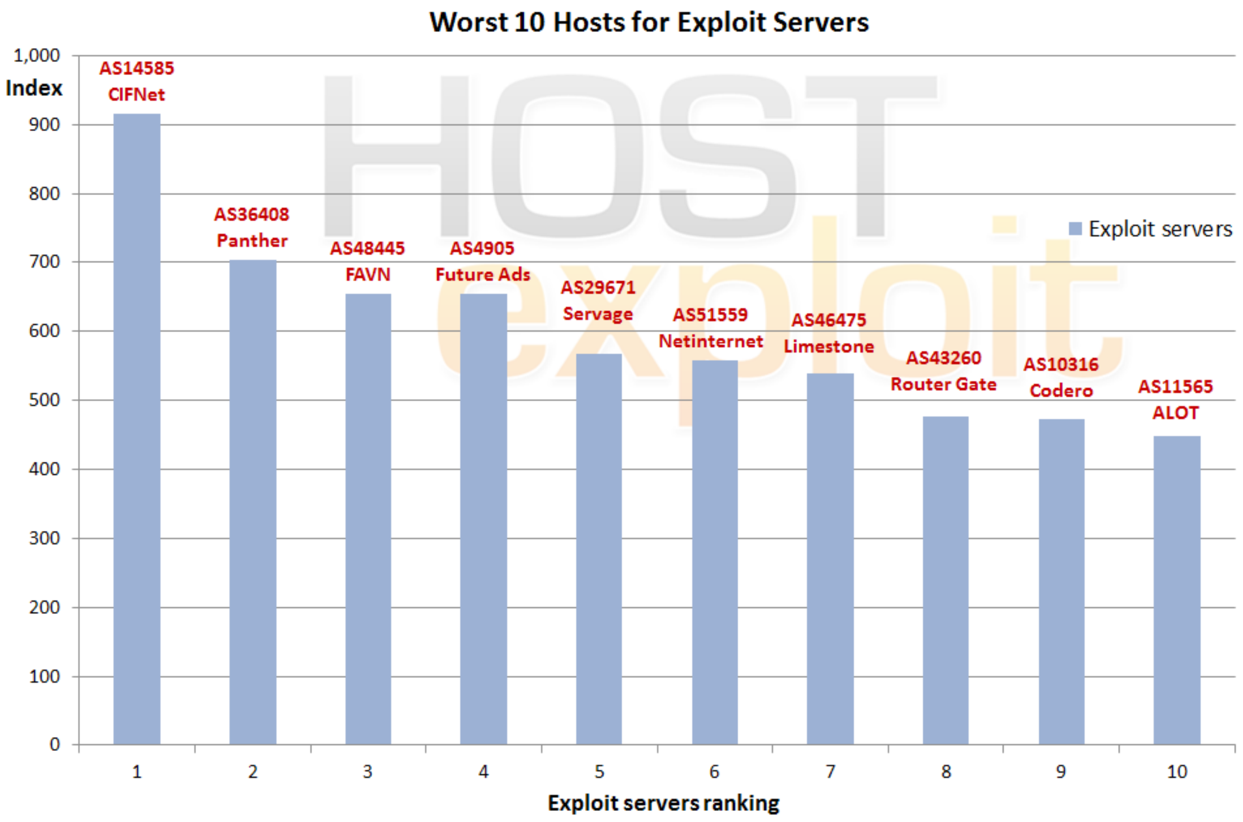
9.1.3. Exploit Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
48	111.0	**14585**	CIFNET - CIFNet, Inc.	**US**	7,680	**916.2**
6	177.8	**36408**	ASN-PANTHER Panther Express / CDNETWORKS-GLOBAL	**US**	37,376	**703.1**
92	92.3	**48445**	FAVN Favorit Network SL	**ES**	256	**655.1**
518	53.4	**4905**	FA-LAX-1 - Future Ads LLC	**US**	256	**655.1**
53	109.7	**29671**	SERVAGE Servage GmbH	**DE**	12,288	**568.2**
47	113.2	**51559**	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon...	**TR**	13,056	**557.6**
64	104.9	**22822**	LLNW - Limelight Networks, Inc.	**US**	119,040	**538.5**
56	108.7	**43260**	ROUTERGATE Router Gate	**TR**	9,984	**477.7**
63	105.2	**10316**	CODERO-AS - Codero	**US**	31,232	**473.8**
611	50.0	**11565**	ASN-ALOT - ALOT, INC.	**US**	1,536	**448.7**

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. 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 Q2 2011 report, it should be noted that 60% of the top 10 in this sector are located or reported as located in the US.



9.1.4. Botnet Hosting - Zeus

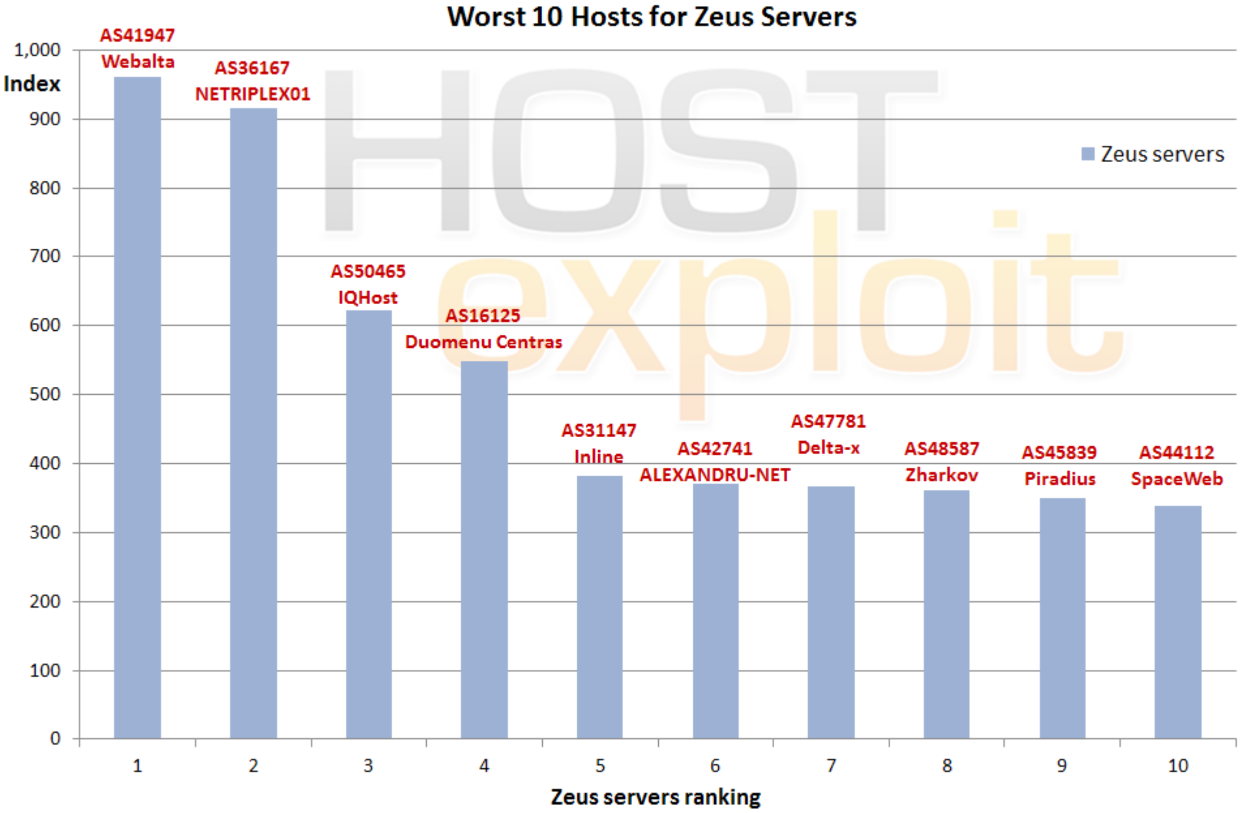
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
4	185.3	**41947**	WEBALTA-AS OAO Webalta	**RU**	16,128	**961.1**
8	170.9	**36167**	NETRIPLEX01 - NETRIPLEX LLC	**US**	46,080	**915.7**
109	85.2	**50465**	IQHOST IQHost Ltd	**RU**	1,024	**622.3**
159	76.9	**16125**	DC-AS UAB Duomenu Centras	**LT**	4,608	**549.4**
36	125.0	**31147**	INLINE-AS Inline Internet Online Dienste GmbH	**DE**	9,728	**381.9**
444	56.4	**42741**	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	**RO**	256	**370.7**
59	106.5	**47781**	ANSUA-AS DELTA-X Ltd	**UA**	512	**367.5**
95	90.0	**48587**	NET-0X2A-AS Private Entrepreneur Zharkov Mukola...	**UA**	1,024	**361.2**
98	88.1	**45839**	PIRADIUS-AS PIRADIUS NET AS45839	**MY**	13,824	**349.8**
86	93.6	**44112**	SWEB-AS SpaceWeb JSC	**RU**	3,072	**339.0**

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



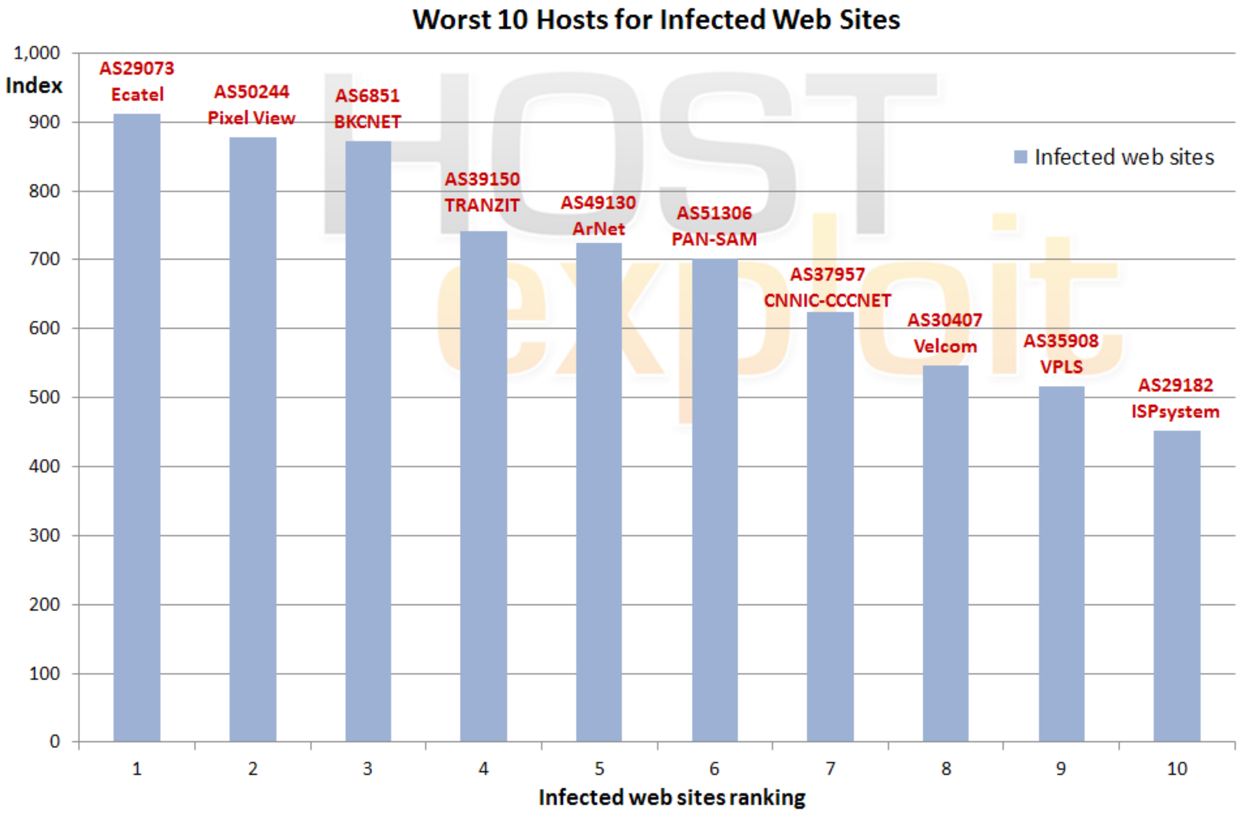
9.2.1. Infected Web Sites

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
2	204.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**911.6**
62	105.5	**50244**	ITELECOM Pixel View SRL	**RO**	7,936	**877.2**
16	161.1	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**871.4**
33	127.2	**39150**	TRANSIT-TELECOM-AS Tranzit Telecom LTD	**RU**	5,376	**741.2**
112	84.6	**49130**	ARNET-AS SC ArNet Connection SRL	**RO**	768	**724.2**
49	110.3	**51306**	UAIP-AS PAN-SAM Ltd.	**UA**	2,048	**701.4**
84	95.1	**37957**	CNNIC-CCCNET China Communication Co., Ltd	**CN**	4,096	**623.6**
82	96.7	**30407**	VELCOM - Rcp.net	**CA**	8,192	**546.7**
39	121.1	**35908**	VPLSNET - VPLS Inc. d	**US**	714,240	**515.6**
41	117.2	**29182**	ISPSYSTEM-AS ISPsystem Autonomous System	**RU**	35,840	**451.4**

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.

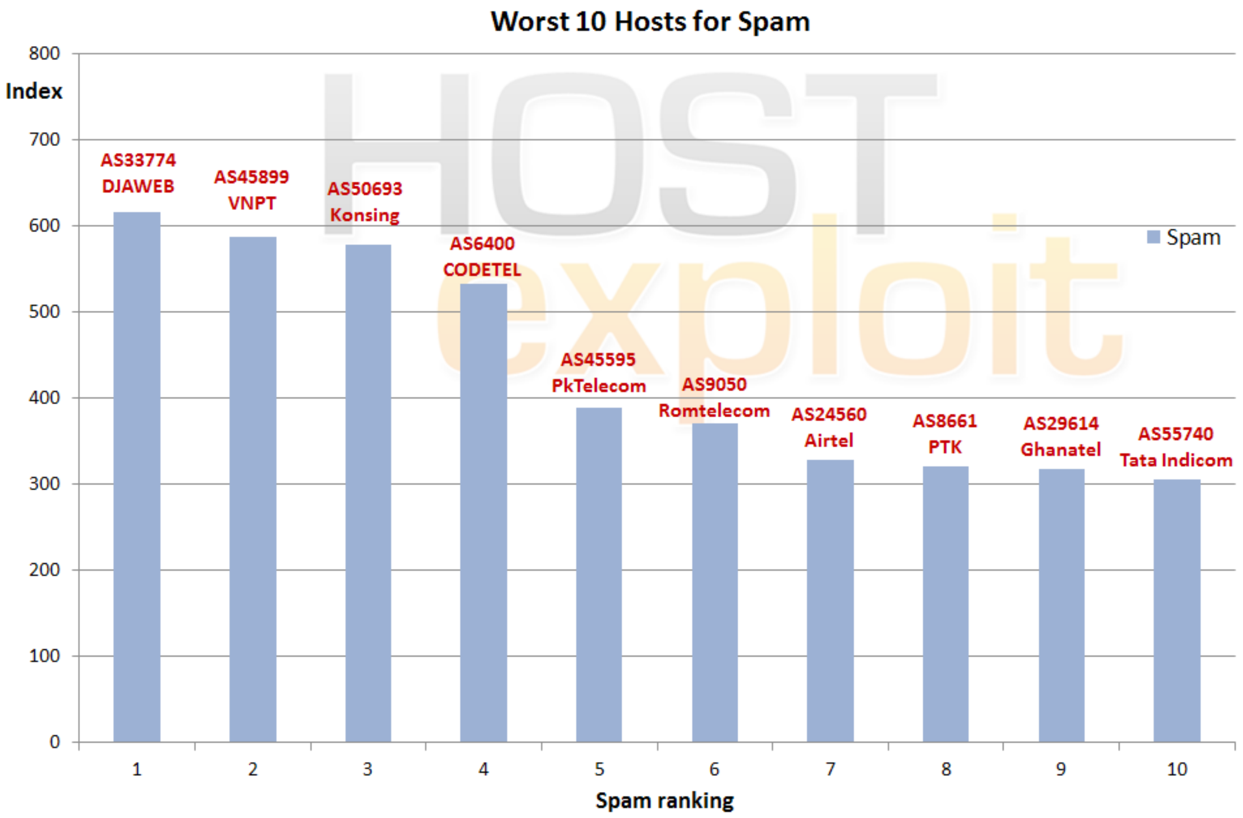


9.2.2. Spam

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
17	157.8	**33774**	DJAWEB	**DZ**	67,840	**616.1**
13	164.1	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,024,704	**587.7**
24	133.8	**50693**	KONSING-GROUP Konsing group doo	**SP**	2,048	**578.8**
34	126.2	**6400**	CompaÃ±Ãa Dominicana de TelÃ©fonos, C. por A. - CODETEL	**DO**	390,912	**533.0**
68	102.4	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	2,321,408	**388.3**
37	124.2	**9050**	RTD ROMTELECOM S.A	**RO**	1,645,824	**371.3**
45	114.4	**24560**	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	**IN**	1,810,432	**329.0**
176	74.2	**8661**	PTK PTK IP	**SP**	57,344	**321.4**
181	73.3	**29614**	GHANATEL-AS	**GH**	100,608	**317.5**
209	70.6	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM...	**IN**	246,784	**305.7**

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.



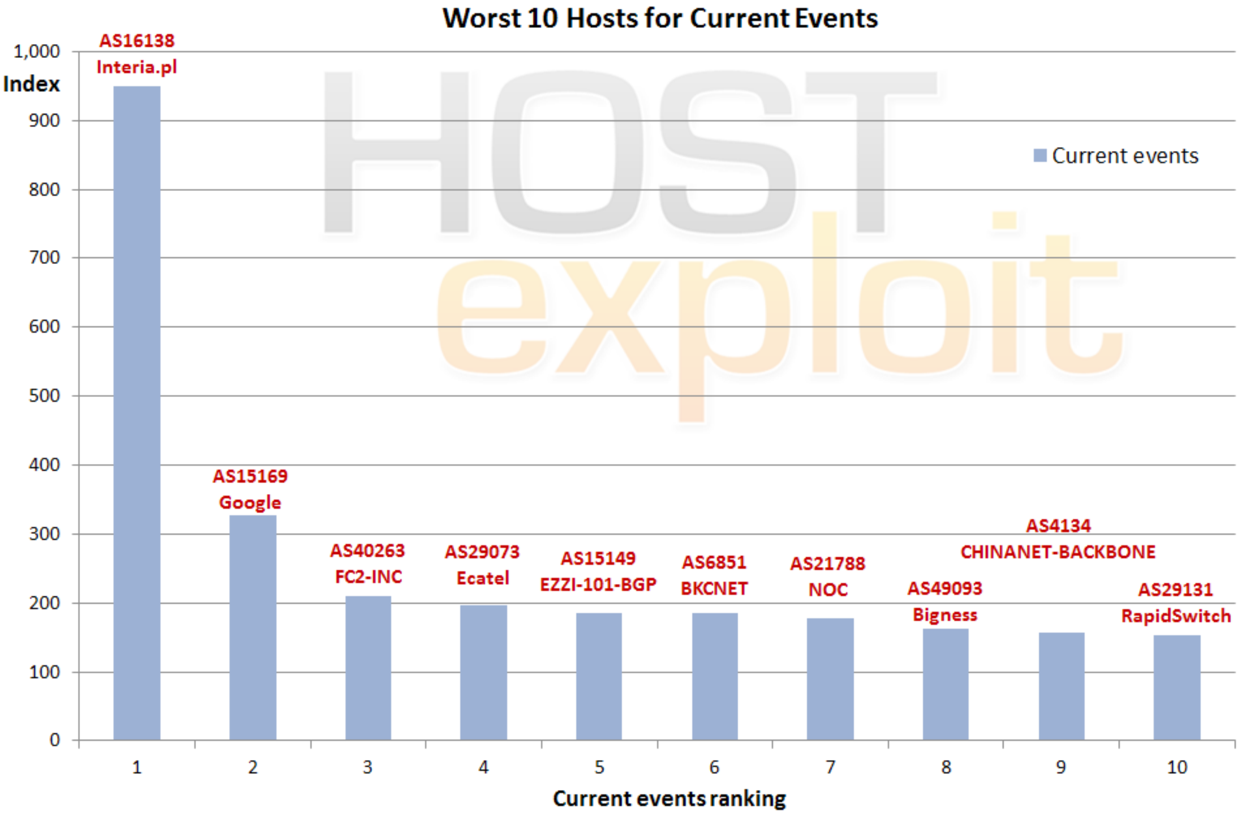
9.2.3. Current Events

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
12	165.3	**16138**	INTERIAPL INTERIA.PL SA	**PL**	4,096	**949.5**
35	125.6	**15169**	GOOGLE - Google Inc.	**US**	284,160	**328.1**
496	54.2	**40263**	FC2-INC - FC2 INC	**US**	2,048	**210.7**
2	204.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**197.1**
233	67.8	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,672	**186.1**
16	161.1	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**185.3**
5	185.2	**21788**	NOC - Network Operations Center Inc.	**US**	282,624	**178.4**
320	60.6	**49093**	BIGNESS-GROUP-AS Bigness Group Ltd.	**RU**	512	**163.5**
21	155.3	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	109,796,608	**157.7**
65	104.7	**29131**	RAPIDSWITCH-AS RapidSwitch	**UK**	0	**152.3**

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.



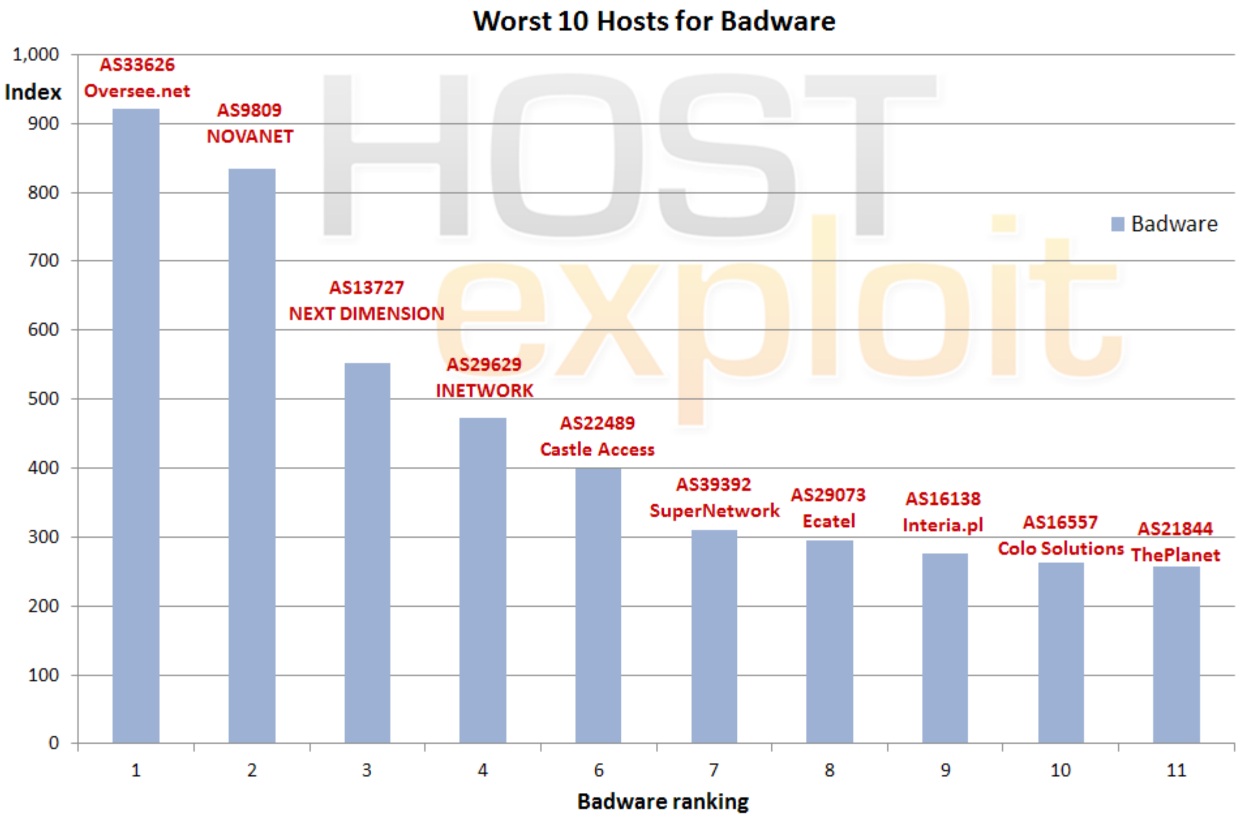
9.2.4. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
7	174.2	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**921.4**
10	168.3	**9809**	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	**CN**	11,008	**833.4**
23	145.8	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**553.2**
75	98.7	**29629**	INETWORK-AS IEUROP AS	**FR**	8,192	**472.0**
26	132.5	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	48,384	**399.1**
79	97.8	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	49,920	**310.6**
2	204.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**294.2**
12	165.3	**16138**	INTERIAPL INTERIA.PL SA	**PL**	4,096	**275.8**
118	82.8	**16557**	COLOSOLUTIONS - Colo Solutions, Inc.	**DE**	27,392	**263.2**
14	163.9	**21844**	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	**US**	1,548,800	**256.8**

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 conjuntion 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.



10.

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.

10.3. Crime Servers - Currently Inactive (Not Announced)

All active at end of Q1 2011; inactive at end of Q2 2011

AS number	Name
49469	SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup
43215	MONYSON GRUP SA
25402	CYBERNET ROMAINA
48709	XISOFT SRL
51699	ANTARKTIDA-PLUS LLC
51362	BESTISP PE Yastremskiy Leonid Stepanovich

10.4. Crime Servers - Examples Currently Active

All active at end of Q2 2011

AS number	Name	IPs	HE Rank
16138	INTERIAPL INTERIA.PL SA	4096	12
13727	ND-CA-ASN - NEXT DIMENSION INC	1024	23
50693	KONSING-GROUP Konsing group doo	2048	24
47781	ANSUA-AS DELTA-X Ltd	512	59
39150	TRANSIT-TELECOM-AS Tranzit Telecom LTD	5376	68
42741	ALEXANDRU-NET-TM-AS	256	84
48445	FAVN Favorit Network SL	256	92
48587	NET-0X2A-AS Zharkov Mukola Mukolayovuch	1024	95
50465	IQHOST IQHost Ltd	1024	109
49130	ARNET-AS SC ArNet Connection SRL	768	112
49093	BIGNESS GROUP LTD	512	295

Conclusions

In a quarter dominated by press stories from self-publicizing hackers such as Anonymous, and LulzSec, matched with DDoS attacks and data exfiltration by others, it is easy to overlook the fact that, worldwide, as an example, there were around 350,000 website defacement hacks in this quarter and 1.5 million in 2010. Additionally, there are currently 800,000 plus web sites hosting malicious exploits and badware.

As for conclusions resulting from our research we have found that there are few changes to the levels of badness being served when comparing the first quarter for 2011 with the last quarter.

Of particular note is the change in the #1 Bad Host position. The title for #1 Bad Host now passes to AS33182 HostDime, a global hosting provider based in the United States. HostDime has climbed to the top of the chart for hosting a wide range of malicious activity from its servers. In fact, it scored in every category we measure – particularly spam, exploit servers, phishing servers and Zeus servers, as well as lower levels of C&C servers, badware and infected websites.

In this quarter, HostDime heads a number of hosts operating out of the United States with significant levels of cybercriminal activity which are being supported by the infrastructure of legitimate organizations. The United States is home to a large proportion of hosts in the Top 50 table of bad hosts, in fact the figure is nearly one half (23) of the total. Cybercriminals are drawn to the hosting providers of those countries where it is relatively easy to obtain hosted website services as well as to those that will give their operation a false credibility.

The Current Events category measure hosts involved in the most up-to-date and fast-changing sectors of malicious internet activity such as clickjacking, counterfeit pharma, new exploit kits, SpyEye, botnets and blended attacks such as MALfi. The #1 bad host in this category is AS16138 Interia.pl.

Hosts and corporate networks do not always host malicious activity with deliberate intent, but can deliver malware by servers added to a network of zombies as a result of having been hacked or compromised. Such networks are used to further the outreach of noxious or virulent material by masking its true origin and, thus, helping to avoid detection. This category is considered by HostExploit to be the most important in the analysis of malware, phishing or general badness. #1 this quarter is AS14585 CIFNet, again hosted in the United States.

However, some well-known names have shown significant improvements in terms of deduction in levels of badness. Most improved is AS47764 Netbridge, host to the popular mail client Mail.ru, which has shown a drop of 84 percent. For overall low levels of malicious activity, the #1 slot has been earned this quarter by AS34744 GVM Sistem, hosted in Romania.

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 **38,030** 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.

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

July 12, 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)*