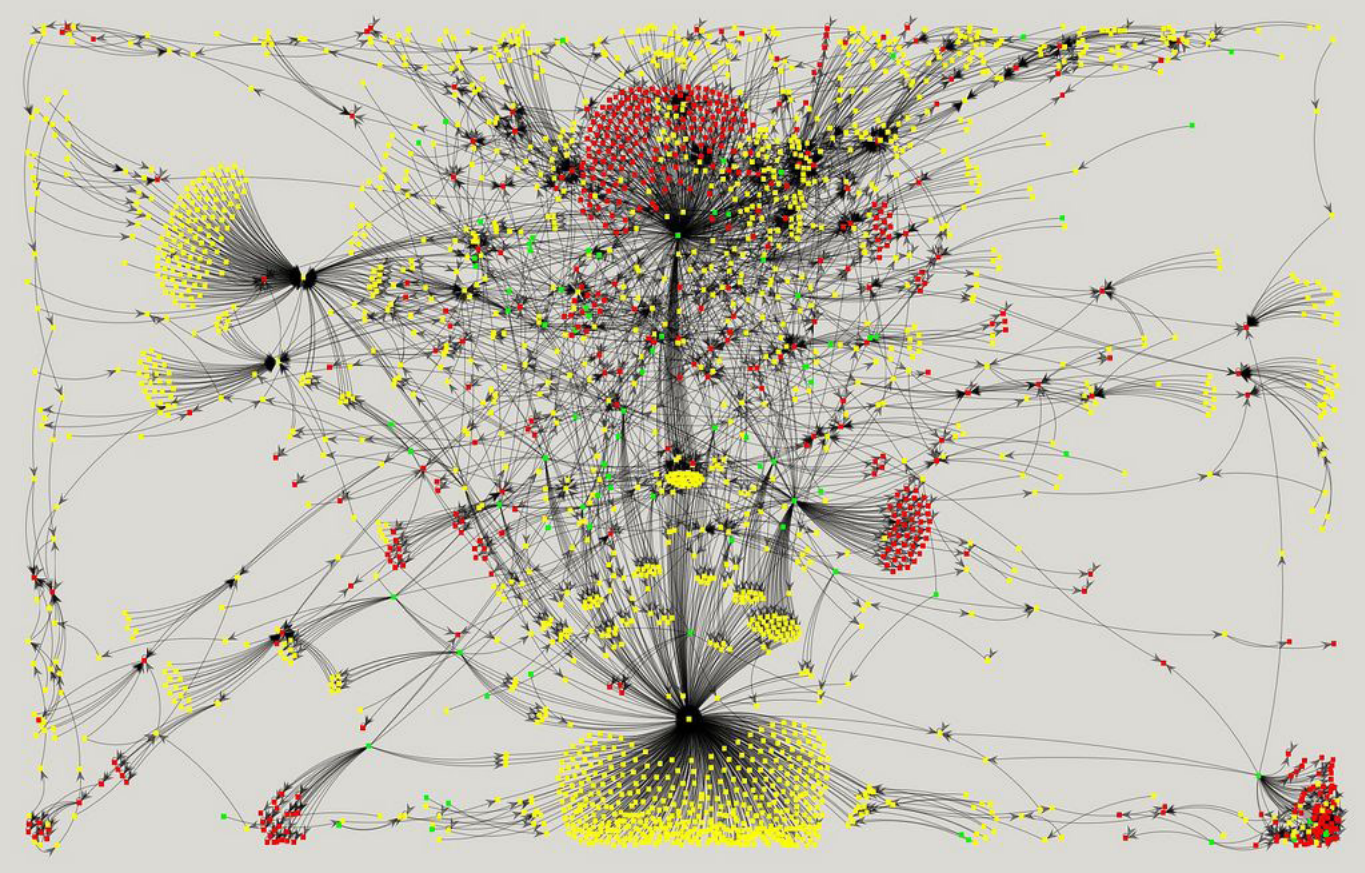
HostExploit's Worldwide Cybercrime Series

Top 50 Bad Hosts and Networks 4th Quarter 2011 - Report



Shnakule - Malware Delivery Network

SITEVET HOST exploit GROUP IB

Table of Contents

Top 50

CyberCrime Series

Bad Hosts and Networks

Supported by

nominet trust

www.nominettrust.org.uk

Edited by

- Jart Armin

Review

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

Contributors

- Steve Burn
- Greg Feezel
- David Glosser
- Niels Groeneveld
- Tim Karpinsky
- Bogdan Vovchenko
- Will Rogofsky
- Philip Stranger
- Bryn Thompson

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

Front page illustration: Shnakule Malware Delivery Network - Courtesy BlueCoat

Introduction

Introduction

In our continuing aim of promoting responsible hosting we present the Q4 2011 Top 50 Bad Hosts report to highlight the hosts that, unintentionally or otherwise, support the malicious activities that threaten and torment Internet users worldwide.

In 2011, lax security by some organizations resulted in truly shocking large scale data breaches with many questions still outstanding on the 'who, where and why.' The most recent example being in late December – the stealing of around 75,000 credit card numbers from strategic forecaster 'Stratfor' together with the posting online of more than 850,000 usernames and passwords.

By refining our country methodology, we hope to help in identifying countries and registries whose standards are lacking, resulting in safe havens for cyber criminals. Rating a country is more complex than an individual web host and so we look forward to continued development in this area. A followup report will be released in February, exploring this topic in further detail.

Attribution continues to be almost impossible in many cases with bad actors hiding behind the lack of cross-border cooperation and international standards relating to the Internet and security. Many also take advantage of the ease with which they can obtain the services that enable their nefarious actions to take place.

By highlighting the hosts that display the greatest amount of malicious activities by using their services we hope to promote responsible hosting without the need for intervention from law enforcement or enforced and often unpopular 'takedowns'. Self-regulation is preferable for most rather than heavy-handed actions as a result of governmental legislation.

Those hosts who consistently fail to act upon the obvious results that are displayed should be avoided by law abiding citizens as using the services of such hosts is, in effect, only supporting further malicious activities. By refusing to 'do business' with these hosts, they will learn that it does not make economic sense to gain a bad reputation.

Jart Armin

News Roundup

The Pocket Botnet

'The Pocket Botnet' focuses on the danger presented by the ever growing popularity of the smartphone with cybercriminals seizing the opportunity to cash in on the lack of security features on the majority of users' phones.

By 2013 it is estimated that the number of smartphones in use will surpass the number of PCs in use (estimate 2 billion) with the smartphone becoming the device of choice by which to access the Internet.

International Data Corporation (IDC) predicted in June 2011 that by the end of 2011 smartphone shipments would reach 450 million units with a further billion estimated by 2015. When including tablet PCs – which mostly run mobile operating systems such as Android and iOS – the numbers are greater still.

Figures from Comscore add support to the prediction that Android handsets will reach a 50 percent market share in 2012 by showing that at the end of November 2011 Android had already attained 46.9 percent of the market. In the same way that the consumer's preferred choice of handset is Android so it is the choice of target for cybercriminals in pursuit of the most profitable route.

Users continue to choose convenience over security and in so doing provide plenty of opportunity for the fraudsters. For example:

- Up to as many as 50 percent of smartphone users connect to banks or financial accounts via their device
- 97 percent connect to either work or personal email accounts
- 87 percent of phones are not supplied by an employer
- One third leave apps/accounts logged in

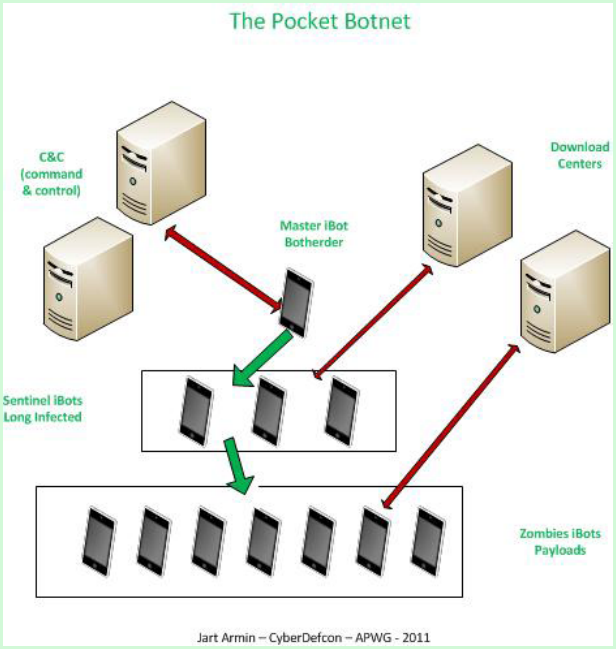
Source: Confident Technologies

Unaware smartphone users continue to make it relatively easy for the array of malware samples in the cybercriminal's arsenal. There is currently an estimated 1,700 smartphone malware samples including Zitmo Android Edition (Zeus for mobile), SpyEye – SMS banking hijacks (mTANs), Premium SMS, root kits, data stealers, click fraud, spyware, DDoS, as well as general malware with more samples found on an almost daily basis.

With the appearance of the first smartphone infections with botnet-like attributes the question is no longer, are mobile botnets possible? The case is now, when will it happen?

Look, for example, at the Android.SmsSend family, which essentially works as fake AV, samples of which increased from 6 to 60 in 2011, Answer.A connects back to a C&C server.

ThemeInstaller.A, infected more than 1 million Symbian smartphones in 1 week in China (CnCert), and has many of the attributes of a zombie including concealment of logs, self-destruction, activity when not in use, defence through an attack on security software, and transmission via other devices through SMS and downloads of new malware from C&C.



With more than 5,700 measurably active botnets in the wild there is plenty of scope for the fraudsters. The bad guys will follow the money and if that means developing new skills and tools, then so be it. Any device that connects either directly or indirectly to the Internet will be targeted. Smartphones provide just such an opportunity and offer the bad guys yet one more avenue through which they can reach just whatever it is they want.

The above is an updated extract from the 'The Pocket Botnet,' presented at the APWG eCrime 2011 conference in San Diego USA, and at UISG in the Kiev Ukraine in December 2011.

DeepEnd Research

Launched in the fall of 2011, DeepEnd Research is an independent information security research group, founded by Andre' M. DiMino, with Mila Parkour, Yuriy Khvyl, Jart Armin, Marnie King, Rosanno Ferraris and Chris Lee.. The name for the group is not without irony as each of the group members can identify at least one occasion when investigating cyber threats has lead them into some very deep and sometimes murky waters!

Andre' M. DiMino said at the launch of the DeepEnd Research website:

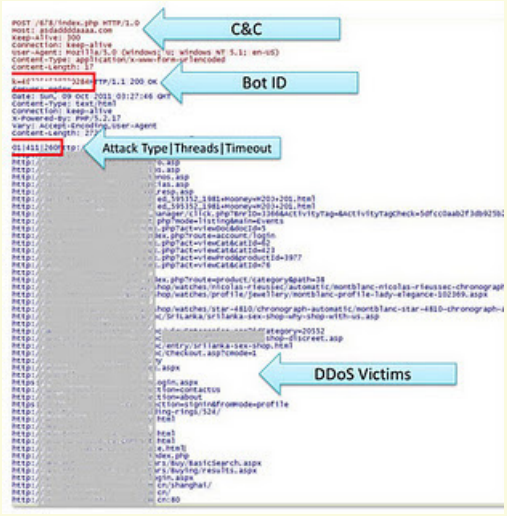
"The primary goal of DeepEnd Research is to foster collaborative research and analysis efforts with other security groups and organizations."

In this way the group can be flexible in its choice of study and in its research methodologies without any of the constraints that can entail from other more 'formal' organizations.

Each of the other group members brings a wealth of expertise and specialization with an emphasis on malware, exploit analysis, botnet tracking, the underground economy and overall cyber threats.

Dirt Jumper DDoS Bot

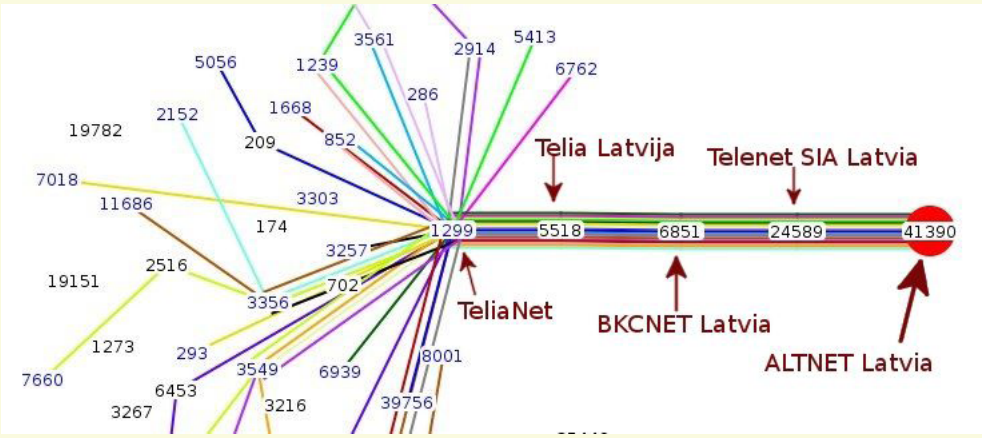
An early analysis by the group began from an encounter with a malware sample that displayed many of the attributes of the Dirt Jumper DDoS bot. Analysis of the Message-Digest Algorithm (MD5) lead back to several Command & Control servers (C&Cs) and victims of Distributed Denial of Service (DDoS) attacks.



It transpired that many antivirus companies detected the Dirt Jumper but used different names for variants of the same bot such as zbot, pinkslipbot, Kryptic among others. Microsoft labeled it as Dishigy.B but armed with this knowledge the researchers were able to gather even more examples and results.

Apart from successfully identifying new variants of the same bot, the research highlighted several weaknesses within the industry that can hinder proper research. A major problem stems from a lack of standardization which analysis of the Dirt Jumper bot neatly highlights in that security companies each use their own terminology in the naming of viruses. In this example, Dirt Jumper has many other names which not only adds confusion but can hinder a proper and thorough analysis of the problem.

The primary source is the SiteVet report on AS41390 RN-DATA / Altnet Latvi



The above is a brief extract taken from the Dirt Jumper analysis and can be found in its entirety, with lots more picture and diagrams, on the DeepEnd research website.

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.

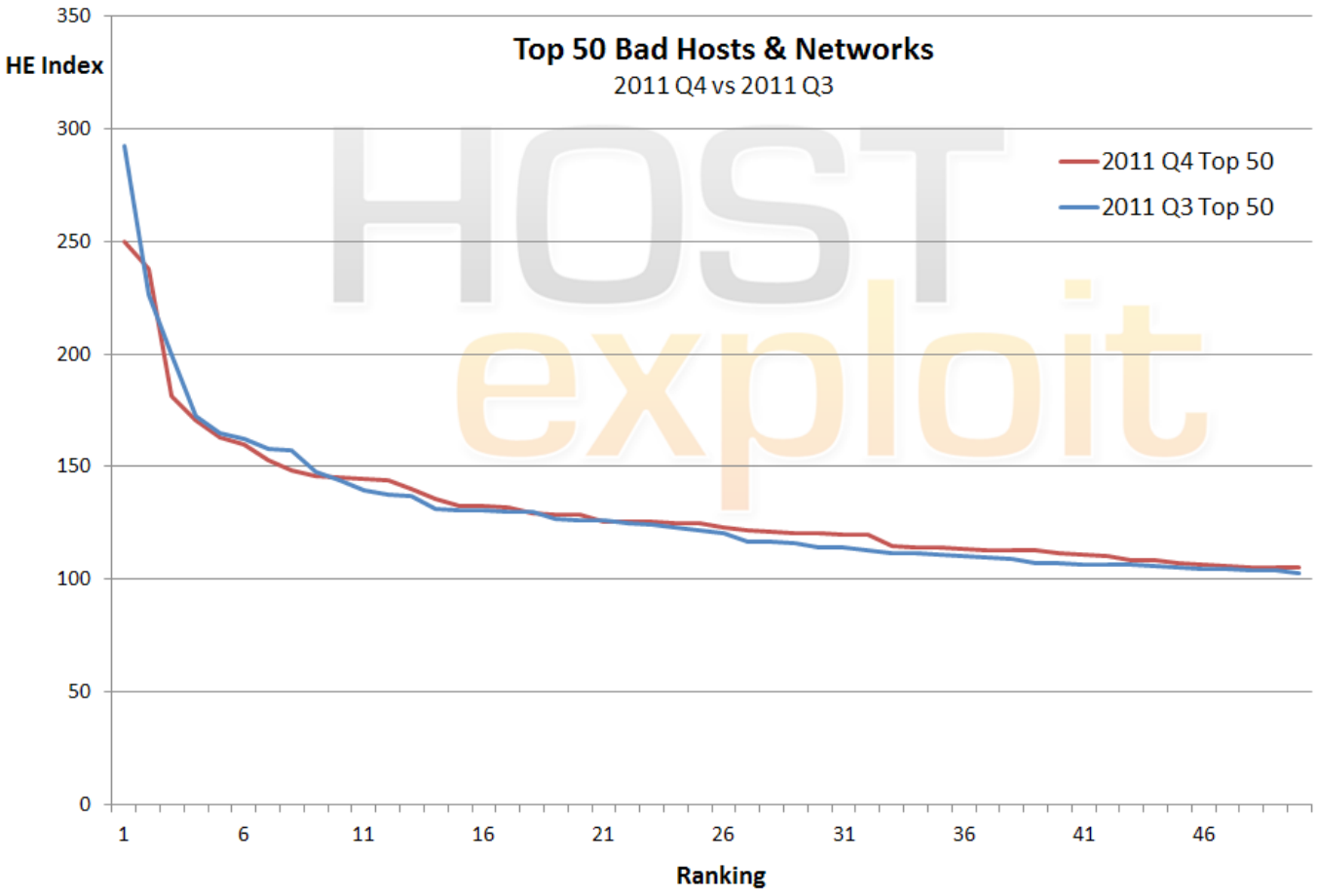
Further feedback is warmly welcomed

contact@hostexploit.com

4. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲ 1	249.90	47583	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	LT	5,376
▲ 2	237.80	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	43,776
▶ 3	181.18	10297	ENET-2 - eNET Inc.	US	90,624
▲ 4	170.85	45634	SPARKSTATION-SG-AP 10 Science Park Road	SG	3,072
▲ 5	162.79	32475	SINGLEHOP-INC - SingleHop	US	248,064
▼ 6	160.09	16138	INTERIAPL INTERIA.PL Sp z.o.o.	PL	4,096
▲ 7	152.61	3595	GNAXNET-AS - Global Net Access, LLC	US	159,232
▲ 8	148.70	32613	IWEB-AS - iWeb Technologies Inc.	CA	235,776
▲ 9	146.10	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,568
▲ 10	144.95	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,541,376
▼ 11	144.64	16276	OVH OVH Systems	FR	583,168
▼ 12	144.19	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
▼ 13	140.11	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	1,011,456
▲ 14	135.54	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM - CDMA	IN	259,072
▲ 15	132.81	26347	DREAMHOST-AS - New Dream Network, LLC	US	329,216
▼ 16	132.40	22489	CASTLE-ACCESS - Castle Access Inc	US	49,408
▲ 17	132.15	24971	MASTER-AS Master Internet s.r.o	CZ	43,520
▲ 18	129.29	21788	NOC - Network Operations Center Inc.	US	281,088
▲ 19	128.67	8972	PLUSSERVER-AS intergenia AG	DE	147,456
▼ 20	128.48	24940	HETZNER-AS Hetzner Online AG RZ	DE	504,832
▲ 21	125.85	29873	BIZLAND-SD - The Endurance International Group, Inc.	US	96,768
▲ 22	125.82	45538	ODS-AS-VN Online data services	VN	9,472
▲ 23	125.35	6697	BELPAK-AS Republican Association BELTELECOM	BY	1,074,432
▼ 24	125.21	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	48,896
▲ 25	124.92	15149	EZZI-101-BGP - Access Integrated Technologies, Inc.	US	28,928
▲ 26	122.93	36444	NEXCESS-NET - NEXCESS.NET L.L.C.	US	115,968
▼ 27	121.97	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	109,571,072
▼ 28	121.32	41947	WEBALTA-AS OAO Webalta	RU	15,872
▲ 29	120.74	9198	KAZTELECOM-AS JSC Kazakhtelecom	KZ	2,079,744
▼ 30	120.41	40824	WZCOM-US - WZ Communications Inc.	US	9,216
▼ 31	120.08	16265	LEASEWEB LeaseWeb B.V.	NL	281,344
▲ 32	119.64	31133	MF-MGSM-AS OJSC MegaFon	RU	19,456
▲ 33	114.46	25795	ARPNET - ARP NETWORKS, INC.	US	12,288
▲ 34	114.12	31147	INLINE-AS Inline Internet Online Dienste GmbH	DE	11,264
▼ 35	114.07	17971	TMVADS-AP TM-VADS Datacenter Management	MY	40,320
▲ 36	113.70	28753	LEASEWEB-DE Leaseweb Germany GmbH (previously netdirekt e. K.)	DE	110,848
▲ 37	112.76	6939	HURRICANE - Hurricane Electric, Inc.	US	649,472
▲ 38	112.65	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	86,016
▲ 39	112.63	47846	SEDO-AS Sedo GmbH	DE	1,280
▲ 40	111.87	9280	CIA-AS connect infobahn australia (CIA)	AU	8,704
▼ 41	111.18	9809	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	CN	10,496
▼ 42	110.17	31034	ARUBA-ASN Aruba S.p.A. - Network	IT	131,840
▼ 43	108.43	15169	GOOGLE - Google Inc.	US	281,344
▼ 44	108.20	16125	DC-AS UAB Duomenu Centras	LT	5,376
▼ 45	107.15	43146	AGAVA3 Agava Ltd.	RU	17,408
▲ 46	106.48	40034	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	VG	3,328
▲ 47	105.62	44112	SWEB-AS SpaceWeb JSC	RU	3,072
▼ 48	105.38	9318	HANARO-AS Hanaro Telecom Inc.	KR	14,991,104
▲ 49	105.23	12260	COLOSTORE - Colostore.com	US	53,248
▲ 50	105.03	55330	GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMMUNICATION	AF	16,384

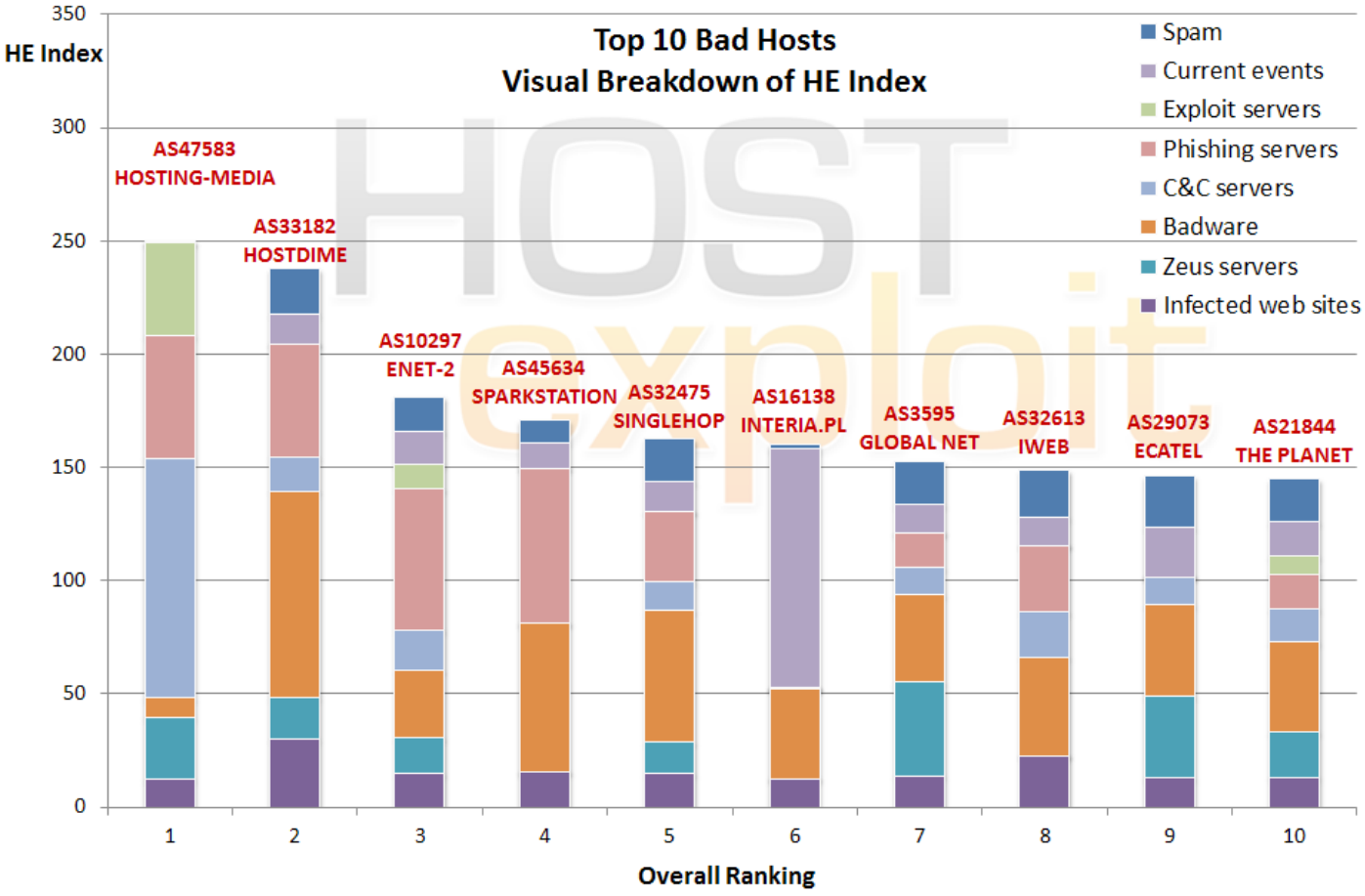
2011 Q4 to 2011 Q3 Comparison



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

Q4 shows few changes to the levels of activity when compared to Q3. Fewer hosts scored distinctly higher in Q4 than in Q3 representing a flatter overall pattern.

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 AS47583 HOSTING-MEDIA is ranked #1 due to a range of cybercriminal activities but primarily to the hosting of C&C servers, phishing servers and Exploit servers, with smaller concentrations of Zeus serving, infected web sites and badware.

At #6 AS16138 INTERIA.PL is serving a large proportion of Current events.

What's New?

7.1. Overview

	Previous Quarter - Q3 2011			Current Quarter - Q4 2011		
	ASN	Name	Country	ASN	Name	Country
#1	33626	Oversee.net	US	47583	Hosting Media	LT
#2	47583	Hosting Media	LT	33182	HostDime	US
#3	10297	eNET	US	10297	eNET	US
#1 for Spam	45899	VNPT Corp	VN	55740	TATA Indicom	IN
#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	10297	eNET	US	45634	Sparkstation	SG
#1 for Exploit Servers	47583	Hosting Media	LT	36444	Nexcess.net	US
#1 for Badware	33626	Oversee.net	US	33626	Oversee.net	US
#1 for Infected Sites	33626	Oversee.net	US	25795	ARP Networks	US
#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.

Take, for example, the Q3 2011 #1 overall Bad Host (#1 for both Badware and Infected sites) AS33626 Oversee.net. This customer orientated reseller swiftly investigated the causes behind its undesired status. The introduction of a clean-up program and new procedures promptly reversed the trend. *(More on this in a future case study.)*

The clean-up for Oversee.net progresses with an added confidence that their high ranking will drop further and take them off the #1 spot for badware.

7.2. Top 10 Newly-Registered Hosts - In Q4 2011

By end of Q4 2011 there were **39,796** ASes; an increase of **1,740** from end of Q3 2011.

Below we show a selection of 10 ASes registered in Q4 2011 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 Q4 ASes are the same findings in the previous two quarterly reports. For Q4 the trend for smaller, and more easily 'disposable' ASes has returned after the unusual activity seen in Q3 when two large ASes in Taiwan, and one in China were newly registered.

Smaller ASes are generally favored for quick 'grab and run' attacks.

Period	HE Rank	HE Index	AS number	AS name	Country	# of IPs
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
2011 Q2	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

7.3. Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-88.8%	90	88.0	4,718	9.8	10922	LIVEJOURNAL - Live Journal Inc.	US	1,536
-68.8%	89	88.2	1,766	27.5	9512	NETLOGISTICS-AU-AP Net Logistics Pty. Ltd.	AU	13,568
-63.2%	33	111.6	1,012	41.1	8660	MATRIX-AS Matrix S.p.A.	IT	8,192
-56.2%	41	106.8	738	46.7	29497	KUBANGSM CJSC Kuban-GSM	RU	22,784
-50.7%	1	292.7	12	144.2	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
-49.2%	51	101.0	590	51.3	39570	LOOPIA Loopia AB	SE	768
-49.2%	100	83.7	944	42.5	6400	Compañía Dominicana de Teléfonos	DO	456,448
-48.7%	45	105.0	524	53.8	8661	PTK PTK IP	RS	97,280
-46.6%	103	83.3	845	44.5	13174	MTSNET OJSC "Mobile TeleSystems"	RU	24,320
-46.3%	38	108.8	435	58.5	24557	AUSSIEHQ-AS-AP AussieHQ Pty Ltd	AU	32,512

The hosts in the above table have all demonstrated a dramatic reduction in levels of badness in the three months since our Q3 2011 report was published.

Many forms of badware 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:

AS10922 Live Journal Inc. down from #90 to #4,718, a drop of 88.8% percent. This social networking site is regularly targeted and used by cybercriminals for a number of reasons including attempts to discredit the provider for allowing Russian activists to blog.

AS33626 Oversee.net improved by 98.5 percent to negligible levels of badness.

7.4. Deteriorated Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
837.2%	3,808	12.2	33	114.5	25795	ARPNET - ARP NETWORKS, INC.	US	12,288
619.3%	3,368	14.8	46	106.5	40034	CONFLUENCE-NETWORK-INC - Confluence Net...	VG	3,328
535.3%	3,440	14.3	79	91.0	50465	IQHOST IQHost Ltd	RU	3,584
301.6%	842	42.5	4	170.8	45634	SPARKSTATION-SG-AP 10 Science Park Road	SG	3,072
176.1%	1,067	38.1	49	105.2	12260	COLOSTORE - Colostore.com	US	53,248
153.2%	620	48.5	26	122.9	36444	NEXCESS-NET - NEXCESS.NET L.L.C.	US	115,968
80.5%	189	69.7	22	125.8	45538	ODS-AS-VN Online data services	VN	9,472
75.2%	438	55.1	66	96.5	18866	ATJEU - atjeu publishing, llc	US	13,312
71.4%	501	52.4	80	89.8	18059	DTPNET-AS-AP DTPNET NAP	ID	16,128
59.1%	517	51.6	109	82.2	38676	AS33005-AS-KR wizsolution co.,Ltd	KR	10,528

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

The 'standout' host this quarter, is AS25795 Arp Networks for greatly increased levels of badness. Formerly lower down the ranking, Arp Networks recently jumped to #33 for overall levels of cybercriminal activity. Arp Networks is #1 for hosting infected web sites.

The second most deteriorated host is AS40034 Confluence Network Inc. Confluence Network scores highly (#4) for hosting botnet C&C servers as well as hosting Zeus botnets (#6). After very low levels of badness detected during the early months of 2011, Confluence Network now moved to #46.

AS45634 Sparkstation SG-AP too has climbed steadly up the rankings. Formerly #842 in Q3 Sparkstation is now #4 in the Top Bad Hosts table. Sparkstation is #1 for hosting phishing servers and #6 in the table for badware.

Country Analysis

As mentioned in previous reports, we have been working on a methodology to more accurately determine the badness levels present on ASes in a particular country. This brings its own set of challenges, such as the impossibility of correctly determining physical server locations in an automated fashion.

However, with certain caveats in place, it is possible to have meaningful results.

Previously, we had been been listing the "worst" countries by crudely summing up the number of hosts appearing from a particular country in the Top 50 and Top 250. Inevitably, this distorted the results towards countries with more hosts. This goes against the philosophy of the Top 50 report which is aimed at reporting on *concentrations* of badness.

So what have we done differently this time around? We are now effectively treating each country as an individual AS, by totalling the number of IPs and badness instances across all ASes registered to that country. We then calculate an index for each country using a similar methodology to that for individual ASes.

The "Country Index" scores a country's badness levels out of 1000, without being driven too strongly by the number of hosts in that country.

The below table shows the resulting Top 10 countries from this methodology:

Country details				Country scoring	
Code	**Name**	**# of ASes**	**Total IPs**	**Rank**	**Index**
LV	LATVIA	189	1,690,880	1	237.66
VG	VIRGIN ISLANDS, BRITISH	3	7,680	2	235.72
LU	LUXEMBOURG	42	1,106,432	3	213.84
MD	MOLDOVA, REPUBLIC OF	32	1,075,648	4	213.70
US	UNITED STATES	13,823	1,253,081,312	5	194.00
LT	LITHUANIA	94	2,463,744	6	182.97
CZ	CZECH REPUBLIC	820	7,887,872	7	177.33
NL	NETHERLANDS	427	17,189,568	8	171.73
RU	RUSSIAN FEDERATION	3,188	45,432,640	9	171.43
BY	BELARUS	68	1,667,328	10	169.60

The results are clearly different to those in previous reports. Most notably, the appearance of the Virgin Islands at #2 shows that the index is taking the "size" of the country (in terms of registered ASes) into consideration and therefore measuring the concentration of badness levels.

A followup report will be released in February, going into more detail on the results of this methodology. Further, the followup report will detail further changes to this methodology in order to improve the accuracy of the results (including a "fairer" representation of where an AS *really* is located).

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
37,296	0.57	721	DNIC-ASBLK-00721-00726 - DoD Network Information Center	US	90,705,408
36,682	0.68	6203	ISDN-NET - The Nexus Group, Inc.	US	185,856
36,506	0.70	21976	NJEDGE-NET - NJEDge.Net, Inc.	US	150,080
36,359	0.71	14985	VEROXITY - Veroxity Technology Partners, Inc.	US	133,632
35,565	0.73	17645	NTT-SG-AP ASN - NTT SINGAPORE PTE LTD	SG	115,200
11,120	1.14	378	MACHBA-AS ILAN	EU	1,160,192
11,047	1.21	50915	ASEVERHOST S.C. Everhost S.R.L.	RO	222,208
9,666	1.70	71	HP-INTERNET-AS Hewlett-Packard Company	US	35,047,424
9,547	1.87	10970	LIGHTEDGE - LightEdge Solutions	US	103,680
9,373	2.06	17229	ATT-CERFNET-BLOCK - AT&T Enhanced Network Services	US	83,712

9.1. 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.

9.2. 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.

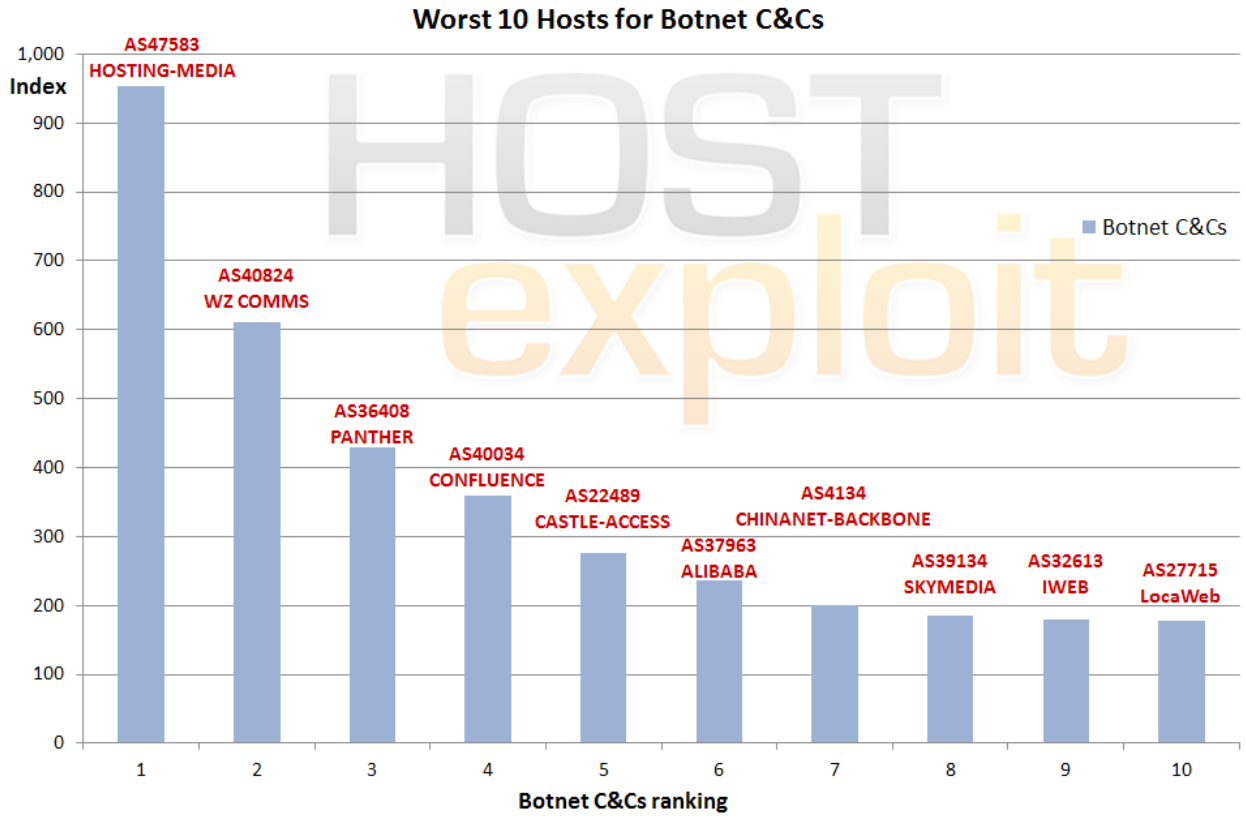
Bad Hosts by Topic

10.1.1. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
1	249.90	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**953.29**
30	120.41	**40824**	WZCOM-US - WZ Communications Inc.	**US**	9,216	**611.92**
135	76.43	**36408**	ASN-PANTHER Panther Express	**US**	79,616	**429.23**
46	106.48	**40034**	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	**VG**	3,328	**359.34**
16	132.40	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,408	**275.95**
226	68.74	**37963**	CNNIC-ALIBABA-CN-NET-AP Alibaba (China) Technology Co., Ltd.	**CN**	828,416	**236.82**
27	121.97	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	109,571,072	**200.35**
263	65.31	**39134**	SKYMEDIA United Network LLC	**RU**	16,384	**185.87**
8	148.70	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	235,776	**179.14**
68	95.16	**27715**	LocaWeb Ltda	**BR**	107,264	**178.42**

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.

The position for the US has improved steadily from Q2 to Q3 and now Q4, with 3 out of the top 10 worst hosts for botnet C&Cs, down from 6.



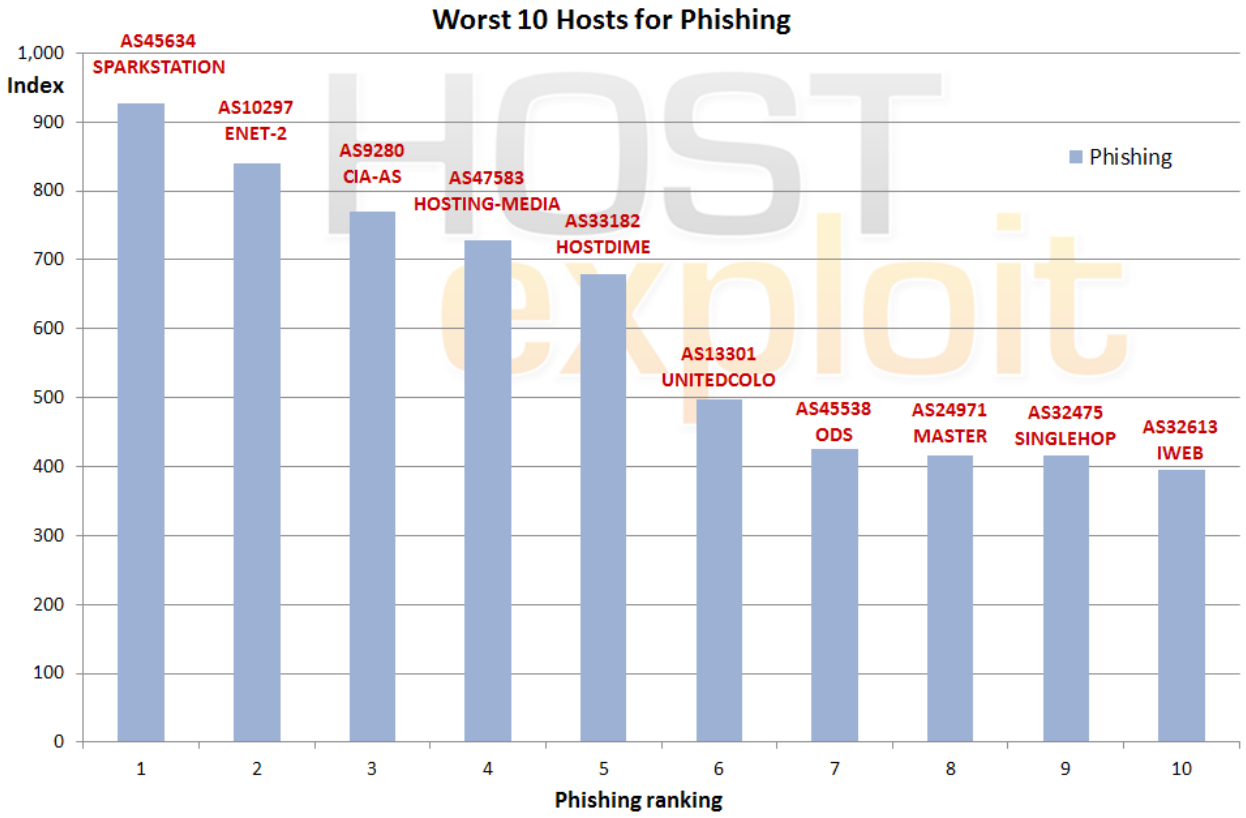
10.1.2. Phishing Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
4	170.85	**45634**	SPARKSTATION-SG-AP 10 Science Park Road	**SG**	3,072	**926.10**
3	181.18	**10297**	ENET-2 - eNET Inc.	**US**	90,624	**839.45**
40	111.87	**9280**	CIA-AS connect infobahn australia (CIA)	**AU**	8,704	**769.13**
1	249.90	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**727.92**
2	237.80	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**678.36**
63	98.88	**13301**	UNITEDCOLO-AS UNITED COLO GmbH	**DE**	66,816	**497.79**
22	125.82	**45538**	ODS-AS-VN Online data services	**VN**	9,472	**426.28**
17	132.15	**24971**	MASTER-AS Master Internet s.r.o	**CZ**	43,520	**416.67**
5	162.79	**32475**	SINGLEHOP-INC - SingleHop	**US**	248,064	**416.45**
8	148.70	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	235,776	**394.73**

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

It is of interest that each of the hosts ranked in the top 5 positions in the overall Top 50 table are present in the Top 10 for hosting phishing servers.

In fact, only one of the hosts in the Top 10 for phishing servers is outside the Top 50 for overall badness.



10.1.3. Exploit Servers

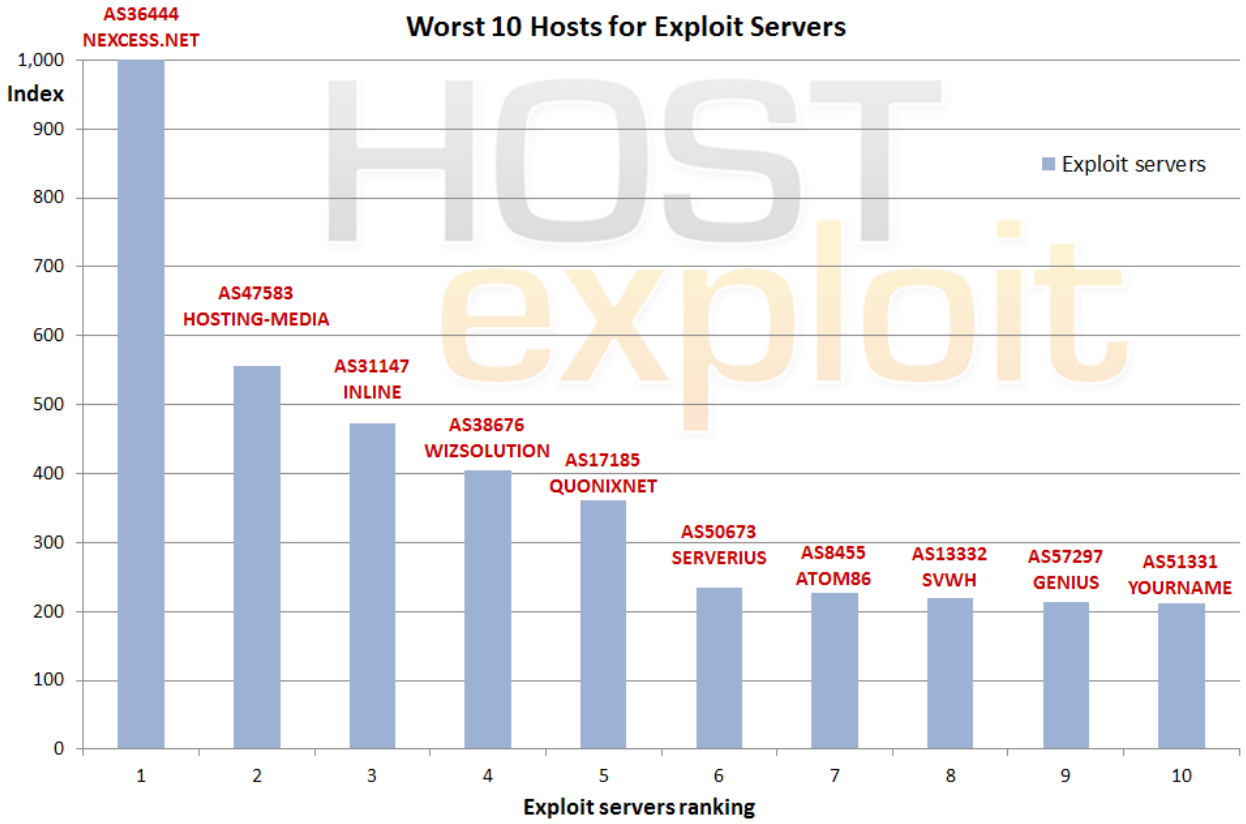
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
26	122.93	**36444**	NEXCESS-NET - NEXCESS.NET L.L.C.	**US**	115,968	**1,000.00**
1	249.90	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	5,376	**557.03**
34	114.12	**31147**	INLINE-AS Inline Internet Online Dienste GmbH	**DE**	11,264	**472.92**
109	82.18	**38676**	AS33005-AS-KR wizsolution co.,Ltd	**KR**	10,528	**405.35**
772	45.99	**17185**	QUONIXNET - Quonix Networks Inc.	**US**	15,872	**361.10**
309	62.51	**50673**	SERVERIUS-AS Serverius Holding B.V.	**NL**	14,848	**234.30**
358	60.41	**8455**	ATOM86-AS ATOM86 Autonomous System	**NL**	17,152	**226.23**
704	47.64	**13332**	SVWH - Silicon Valley Web Hosting, Inc.	**US**	40,192	**219.24**
3,241	16.86	**57297**	GENIUS-AS Genius Investments (Cyprus) Limited	**RU**	256	**214.10**
1,444	32.43	**51331**	YOURNAME Your Name Webhosting	**NL**	768	**211.34**

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.

Four of the hosts present in the Top 10 in Q3 remain in Q4. These hosts should pay urgent attention to the causes as their reputation is being severely damaged.

#1 in this category AS36444 Nexcess has previously had low levels of badness which is indicative of a host that has been compromised or hacked.



10.1.4. Botnet Hosting - Zeus

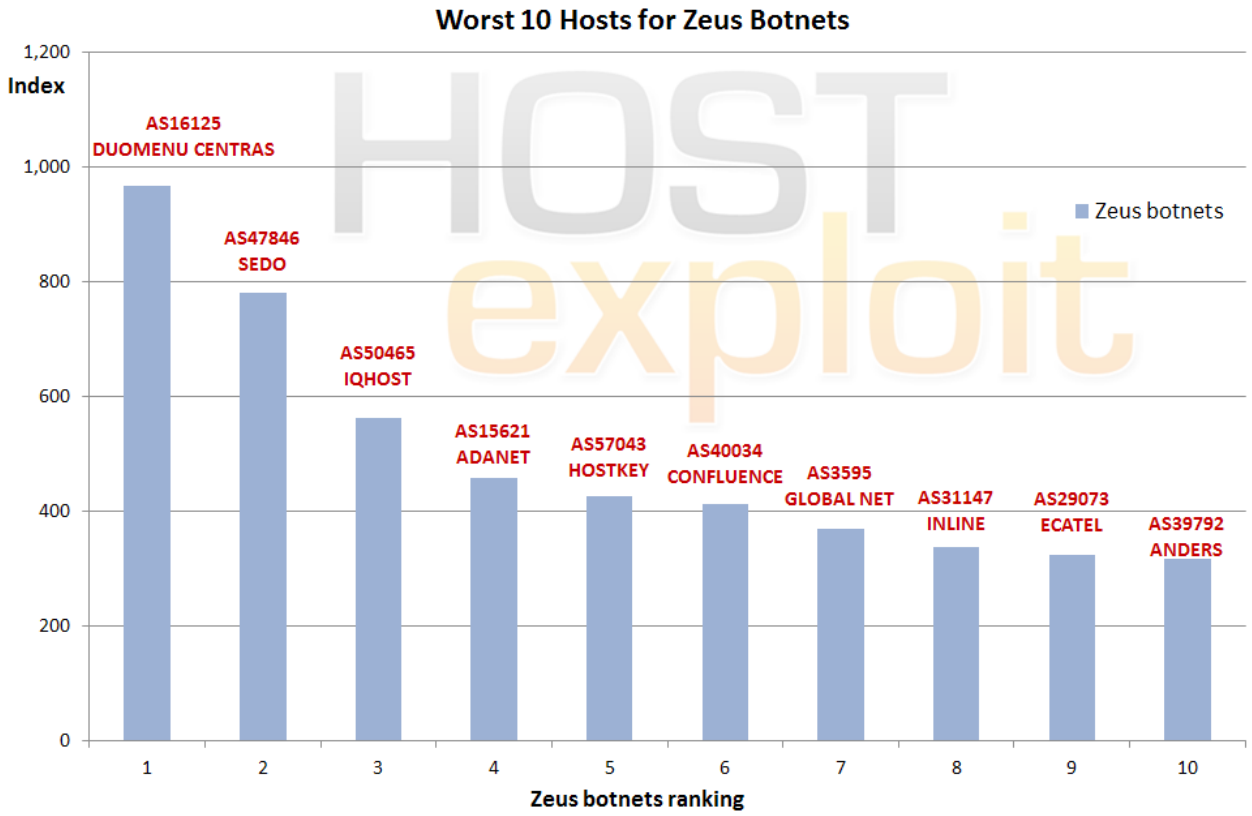
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
44	108.20	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,376	**966.70**
39	112.63	**47846**	SEDO-AS Sedo GmbH	**DE**	1,280	**780.53**
79	91.04	**50465**	IQHOST IQHost Ltd	**RU**	3,584	**563.84**
103	83.74	**15621**	ADANET-AS Azerbaijan Data Network	**RU**	11,264	**458.09**
678	48.20	**57043**	HOSTKEY-AS HOSTKEY B.V.	**NL**	2,304	**425.76**
46	106.48	**40034**	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	**VG**	3,328	**412.43**
7	152.61	**3595**	GNAXNET-AS - Global Net Access, LLC	**US**	159,232	**369.89**
34	114.12	**31147**	INLINE-AS Inline Internet Online Dienste GmbH	**DE**	11,264	**338.77**
9	146.10	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**323.91**
186	71.68	**39792**	ANDERS-AS Anders Telecom Ltd.	**RU**	35,072	**317.70**

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 10.1.3 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 AS29073 Ecatel, previous ranked #1, and back up to #9 for botnet hosting.

Data from the excellent Zeus Tracker service from abuse.ch is used here in conjunction with HE's own data.



10.2.1. Infected Web Sites

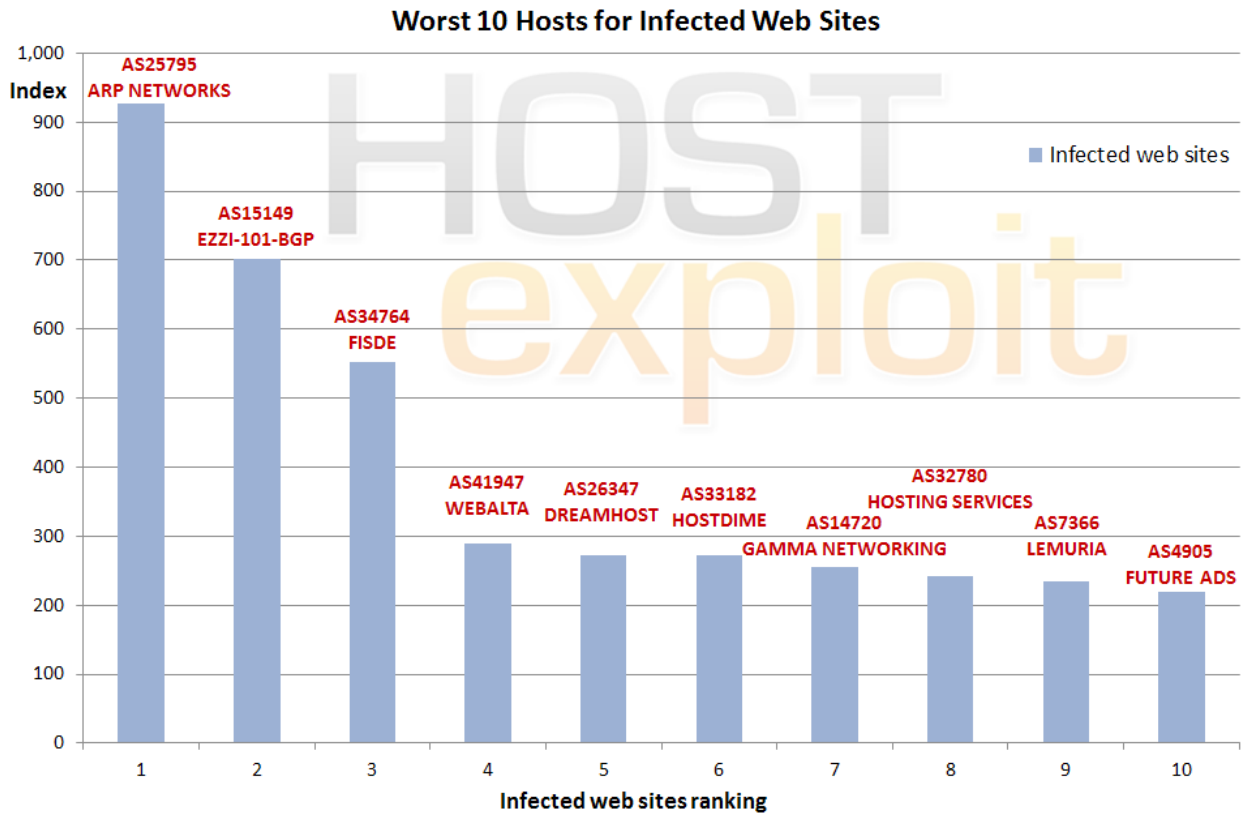
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
33	114.46	**25795**	ARPNET - ARP NETWORKS, INC.	**US**	12,288	**927.26**
25	124.92	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,928	**702.01**
315	62.22	**34764**	FISDE-AS Maurice Funke	**DE**	1,280	**551.73**
28	121.32	**41947**	WEBALTA-AS OAO Webalta	**RU**	15,872	**289.29**
15	132.81	**26347**	DREAMHOST-AS - New Dream Network, LLC	**US**	329,216	**272.73**
2	237.80	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**272.53**
207	70.52	**14720**	GAMMANETWORKING-EAST - Gamma Networking Inc.	**CA**	7,680	**255.52**
108	82.88	**32780**	HOSTINGSERVICES-INC - Hosting Services, Inc.	**US**	12,288	**241.22**
794	45.55	**7366**	LEMURIACO - Lemuria Communications Inc.	**US**	3,072	**235.33**
1,964	25.34	**4905**	FA-LAX-1 - Future Ads LLC	**US**	256	**219.37**

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.

Of note is the cluster of US hosts found within this category.

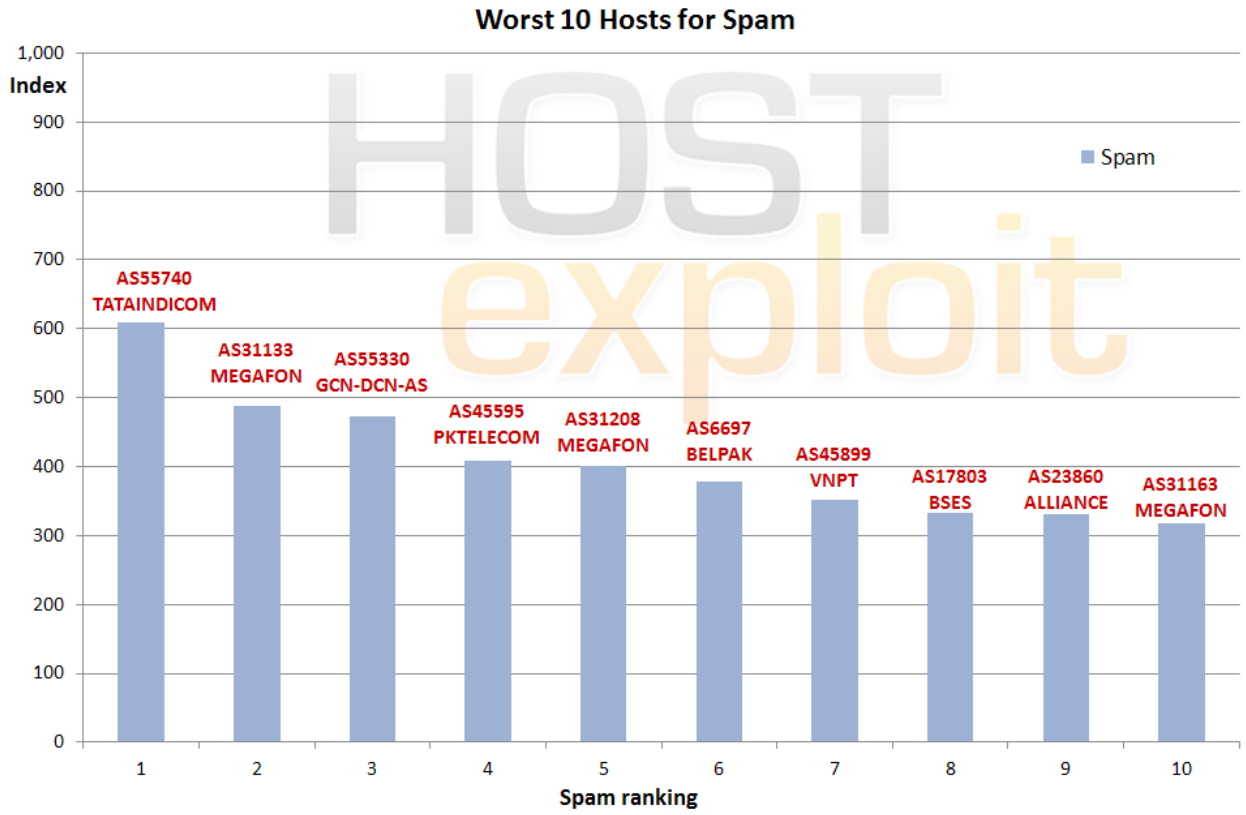


10.2.2. Spam

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
14	135.54	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM	**IN**	259,072	**609.86**
32	119.64	**31133**	MF-MGSM-AS OJSC MegaFon	**RU**	19,456	**487.29**
50	105.03	**55330**	GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMMUN...	**AF**	16,384	**472.08**
71	94.56	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	3,824,384	**408.80**
85	89.48	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	4,096	**401.84**
23	125.35	**6697**	BELPAK-AS Republican Association BELTELECOM	**BY**	1,074,432	**377.65**
57	100.30	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,220,288	**351.93**
114	81.38	**17803**	BSES-AS-AP BSES TeleCom Limited	**IN**	1,034,752	**332.76**
154	73.71	**23860**	ALLIANCE-GATEWAY-AS-AP Alliance Broadband Services...	**IN**	17,408	**331.20**
200	70.93	**31163**	MF-KAVKAZ-AS JSC MegaFon	**RU**	5,120	**318.40**

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 as much damage as 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.



10.2.3. Current Events

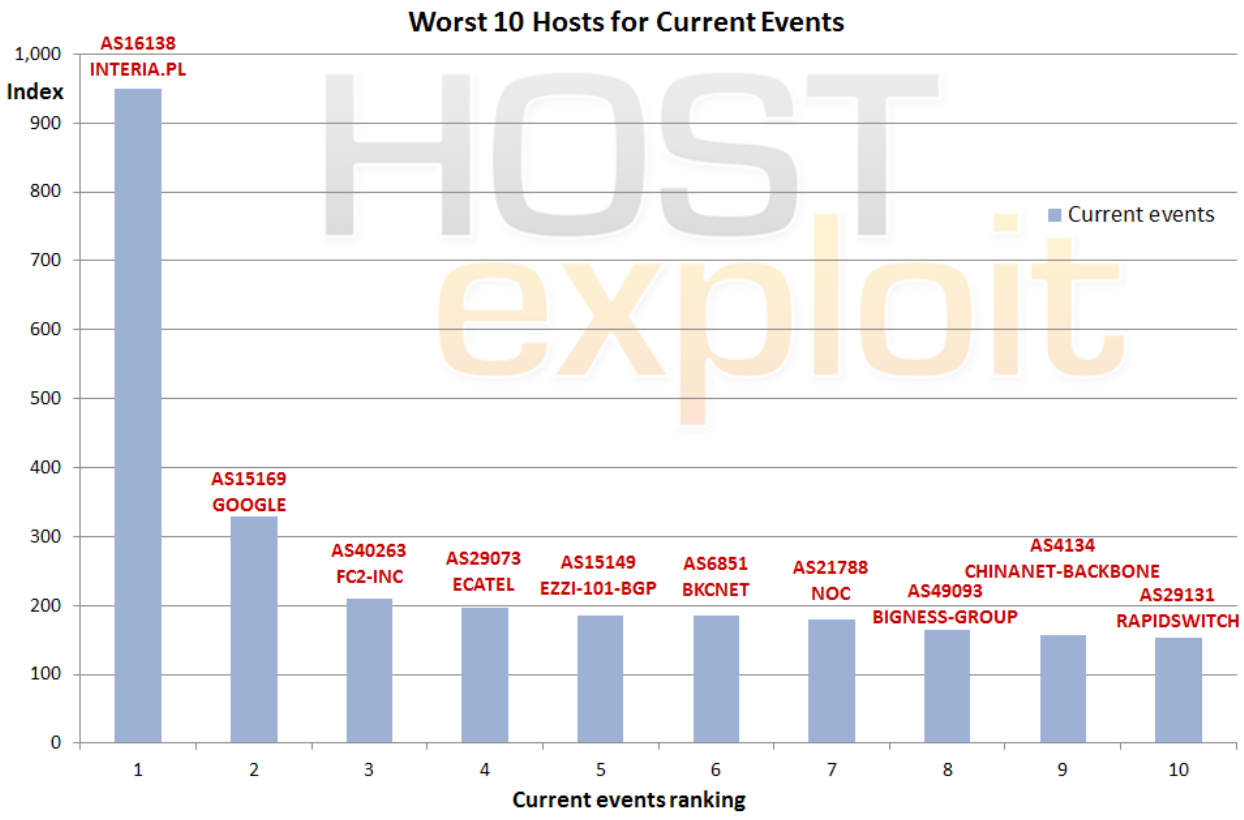
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
6	160.09	**16138**	INTERIAPL INTERIA.PL Sp z.o.o.	**PL**	4,096	**949.48**
43	108.43	**15169**	GOOGLE - Google Inc.	**US**	281,344	**329.30**
446	57.72	**40263**	FC2-INC - FC2 INC	**US**	2,048	**210.73**
9	146.10	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**197.08**
25	124.92	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,928	**185.74**
540	52.94	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**185.32**
18	129.29	**21788**	NOC - Network Operations Center Inc.	**US**	281,088	**178.62**
2,822	19.25	**49093**	BIGNESS-GROUP-AS Bigness Group Ltd.	**RU**	256	**164.28**
27	121.97	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	109,571,072	**157.68**
236	67.72	**29131**	RAPIDSWITCH-AS RapidSwitch	**GB**	0	**152.32**

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.

Unchanged from Q3 is the 40% of the Top 10 that are based in US.



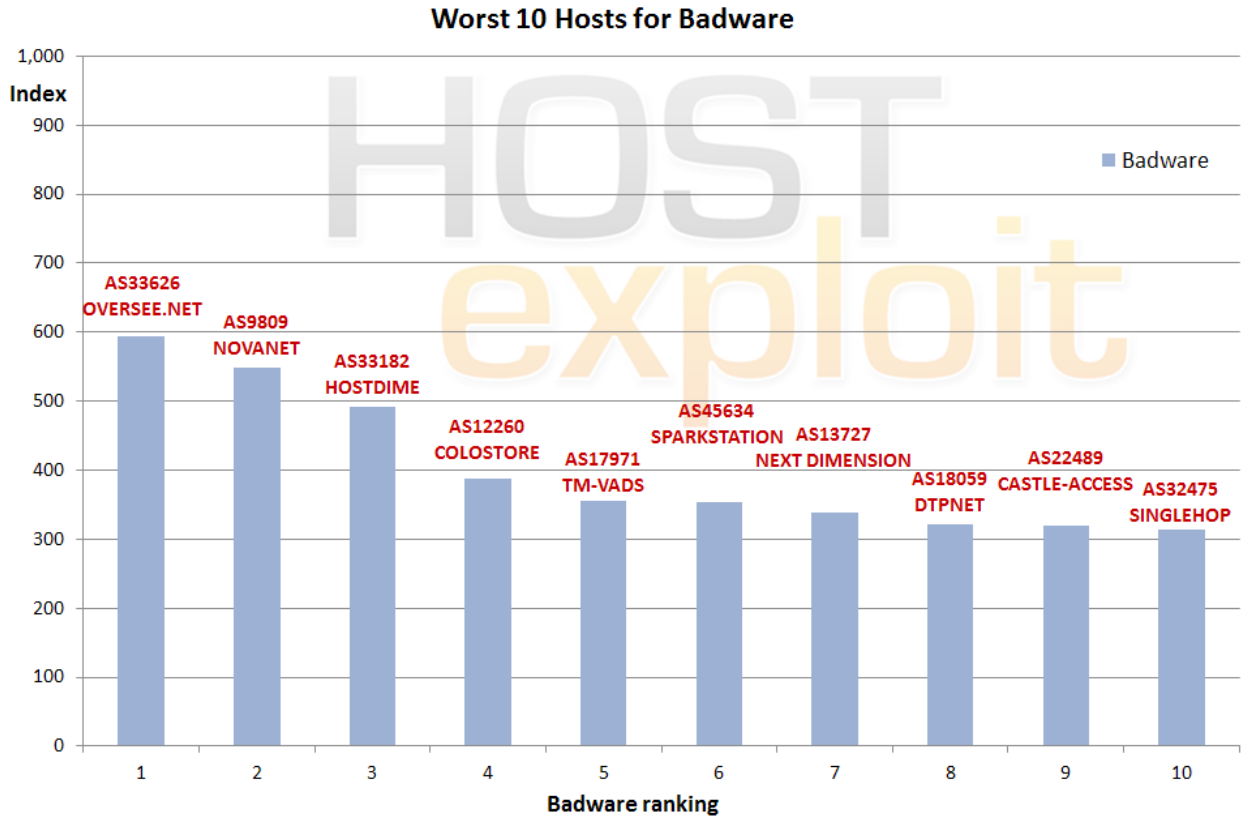
10.2.4. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
12	144.19	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**594.37**
41	111.18	**9809**	NOVANET Nova Network Co.Ltd, Futian District, Shenzhen, China	**CN**	10,496	**548.46**
2	237.80	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**491.96**
49	105.23	**12260**	COLOSTORE - Colostore.com	**US**	53,248	**387.48**
35	114.07	**17971**	TMVADS-AP TM-VADS Datacenter Management	**MY**	40,320	**355.31**
4	170.85	**45634**	SPARKSTATION-SG-AP 10 Science Park Road	**SG**	3,072	**353.87**
81	89.82	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**337.88**
80	89.82	**18059**	DTPNET-AS-AP DTPNET NAP	**ID**	16,128	**320.58**
16	132.40	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,408	**319.03**
5	162.79	**32475**	SINGLEHOP-INC - SingleHop	**US**	248,064	**313.30**

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

This quarter the spotlight on the #1 Bad Host moves out of the US to Lithuania and to the activities of a hosting provider that many researchers will not be surprised to find in that position. AS47583 Hosting Media is supporting some of the worst types of harmful threats including several botnet related activities such as Zeus as well as C&C servers, exploit servers, phishing servers, malware and badware. We hope that highlighting this provider will compel a change for the better as has been the case with other former #1 Bad Hosts.

Success stories include AS33626 Oversee.net, currently in the process of monitoring the cause for their previously high ranking and with expectations of dropping still further down the rankings.

However, one to watch in the coming weeks is AS45634 Sparkstation, up to rank #4, having been in the lower echelons of the Top 1000 for many months beforehand. Located in the Singapore Science Park, the web hosting company is now hosting a wide variety of malicious activity.

And so 2011 finished in the same vein in which it started causing many to label it as 'the year of the security breach' or even the year of chaos with hacks and online revelations of personal data on a colossal scale. Too, there is the rise of the smartphone malware and, in particular, Android emerging as the most targeted platform. Not only that but we are potentially on the verge of the first major 'pocket botnet' with mobile vendors again playing a game of 'catch-up', reminiscent of the early days of desktop viruses.

As 'Bring your own devices' (BYOD) gains momentum within the working environment, employers will face a tough year. Large organizations, we hope, are rising to this challenge but smaller enterprises continue to struggle with the need for security versus costs.

An updated country methodology has produced interesting results which will be further explored in a follow report in February.

On a more positive note 2012 may bring some relief with help coming from more effective cross-border collaboration and cooperation as countries band together in a united front against the 'common enemy'. It serves no country any good to find their economy is being substantially damaged by the nefarious activities of their own citizens or organizations operating from within their borders. So the message for all for 2012, 'unite and collaborate for the good of us all.'

All of us at HostExploit and members of our wider community wish you all a very happy 2012.

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)*