ECYFED

ISBN: 978-0-9836249-3-6

HostExploit's Worldwide Cybercrime Series

World Hosts Report

Q3 2012

GROUP IB

HOST exploit

CSIS

Abstract

Introduction

A change in the top positions sees a new #1 - AS40034 CONFLUENCE-NETWORKS. The Top 10 continues to be mostly populated with familiar names.

Methods

Data of malicious activity, from a dozen community partners, were combined with HostExploit's own data to ensure a balanced dataset as the basis of the report. HostExploit's transparent methodology was used to calculate the *HE Index* of every publicly-routed Autonomous System. The *HE Index* represents detected concentration levels of malicious activity, relative to all other Autonomous Systems.

Results

Global levels of malicious activity have remained consistent with the previous quarter. However, there have been significant movements in the rankings of notable hosts (see *7.3 Improved Hosts* and *7.4 Deteriorated Hosts*).

Discussion

The United States and Russia have by far the most publicly-routed ASes registered (14,221 and 3,892 respectively). With the competitiveness of hosting in these countries, it can be claimed that they will always be likely to host large amounts of malicious content, even in relative terms. In Q2 there was optimism in an improving situation for the United States. Sadly, the improvement appears to have been short-lived with an increase in the number of US hosting providers in the Q3 Top 50 – up to 14 from 12 in Q2.

Conclusion

Both United States and Russia Federation have shown a disappointing set of results in Q3. The overall standing of hosts in both countries has deteriorated since Q2. For individual hosts in these countries , it has been more of a mixed picture with gains and losses.

Table of Contents

CyberCrime Series

World Hosts Report

Supported by

nominet trust

www.nominettrust.org.uk

Edited by

- Jart Armin

Review

- Dr. Bob Bruen
- Raoul Chiesa
- Peter Kruse
- Andre' DiMino
- Thorsten Kraft
- Ilya Sachkov

Comparative Data

- AA419
- Abuse.CH
- Clean-MX.DE
- Cyscon SIRT
- Emerging Threats
- Google Safe Browsing
- Group-IB
- HostExploit
- hpHosts
- ISC
- KnujOn
- MalwareDomains
- MalwareDomainList
- RashBL
- Robtex
- Shadowserver
- SiteVet
- Spamhaus
- SRI International
- StopBadware
- SudoSecure
- Team Cymru
- The Measurement Factory
- UCE Protect

Contributors

- Steve Burn
- Greg Feezel
- Andrew Fields
- David Glosser
- Niels Groeneveld
- Matthias Simonis
- Bogdan Vovchenko
- Will Rogofsky
- Philip Stranger
- Bryn Thompson
- DeepEnd Research

Introduction

Editorial

The #1 Host this quarter is new to the top 100 ranking table – AS40034 Confluence Networks, registered in the Virgin Islands but hosted in the United States.

Historical data, via SiteVet, shows a consistent pattern of rising and falling levels of malicious content on the servers of Confluence Networks. In Q2 this provider of cloud-based products was ranked at #129. Now displaying a significant deterioration Confluence Networks has served an unacceptable amount of Zeus-based malware and hosted C&C servers in the last 90 days. Confluence Networks is advised to take urgent action against abusers of their services, to implement preventative measures and to clean up malware and other malpractices on their networks.

Jart Armin

Want to be Involved?

If you like what we do and would like to be involved, why not become a HostExploit sponsor or partner? We are continually looking to improve on what we do by expanding our outreach. If you think you can be of assistance, we would love to hear from you. Get in touch at contact@hostexploit.com.

Topic for the Quarter

DDoS the World - The Problem with DNS Open & Misconfigured Resolvers

Weaknesses within the DNS (Domain Name System) continue to expose Internet communications to the threat of attack while the fixes remain, largely, a topic for debate.

DNSSEC is beginning to have an impact, although take up is slow, while other DNS problems linger on, failing to attract due attention. Just so is the issue of misconfigured open resolvers, a problem that remains mostly obscured, despite its prominent role in recent DDoS amplification attacks.

Academic papers on this subject date back 10 years or more while security experts have frequently warned about the threat posed from intruders taking advantage of incorrectly configured open resolvers. Once hijacked this resource provides the power to launch a massive DDoS attack.

DDoS floods or attacks can be executed in a variety of ways. Attackers may use multiple computer systems to power a DDoS, via a botnet, or by sheer number of computers. No matter the method of attack the result is invariably the same - a system crash and service interruption.

Here, savvy attackers use open and misconfigured resolvers to good effect.

A small packet query to an open or public DNS server can be used to return multiple responses. Add in a spoofed IP address and the attacker has an effective tool, from few resources, as well as a masked origin.

At the birth of the DNS protocol latency was an issue and speed was often a luxury. Open or public resolvers tended to solve those problems. Improvements and advances since mean that some of the old problems simply no longer exist. What may have once been applicable may no longer be so.

The unrestricted passage of free flowing packets of data via an open resolver that is mis-configured is simply a sitting target for the savvy intruder.

DDoS amplification is used to devasting effect. Not only is the targeted website overwhelmed with the power of the attack, (in excess of 20gps is now commonplace) but to the observer the attack appears to have come via the host. The implications for a host or registrar may be far reaching.

HE continues with its research into this all-important issue and is pleased to announce that future editions of the 'Top 50' will feature outcomes of this study. As a precursor, an initial overview is depicted below.

It should be stressed open recursive nameservers are not a problem in themselves; it is the mis-configuration of a nameserver where the potential problem lays. Additionally, a resolver may be open only due to a misconfiguration, providing the source of yet another vulnerability ripe for exploitation.

The aim here is to raise awareness on this issue and, further, to encourage appropriate remedial and preventative action by hosts and registrars who should check for this type of misconfiguration.

Any advances that can help to achieve a reduction in amplified DDoS attacks due to nameserver misconfiguration is well worth further investigation.

Open resolvers	AS number	AS name	Country	# of IPs	AS rank	AS index
3,219	**7418**	Terra Networks Chile S.A.	**CL**	1,360,640	**735**	**47.2**
2,998	**8167**	TELESC - Telecomunicacoes de Santa Catarina SA	**BR**	6,320,128	**317**	**62.7**
2,464	**3462**	HINET Data Communication Business Group	**TW**	16,813,312	**337**	**61.9**
2,293	**4713**	-Allocated by APNIC-	**JP**	37,320,192	**216**	**67.0**
2,153	**21844**	THEPLANET-AS - THE PLANET	**US**	1,540,096	**119**	**77.9**
1,946	**4766**	KIXS-AS-KR Korea Telecom	**KR**	70,942,304	**120**	**77.7**
1,282	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	131,072	**25**	**113.4**
1,069	**1659**	ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information	**TW**	6,863,616	**300**	**63.3**
961	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	113,836,256	**26**	**113.3**
920	**2516**	JPNIC-ASBLOCK-AP JPNIC	**JP**	18,358,208	**150**	**73.8**

ASes by number of resolvers

The table above shows the 10 ASes with the highest number of open resolvers on their address space. There doesn't appear to be a strong correlation between open resolvers being present on an AS, and the level of malicious activity on that AS, as represented by the AS Index.

The table below shows the 10 ASes with the largest increases in number of open resolvers since the previous quarter. Also shown is the corresponding percent change in the AS Index for each AS. Again, there doesn't appear to be any strong correlation.

What does this tell us?

This reinforces the message that open resolvers themselves aren't a problem. Even misconfigured open resolvers do not appear to cause rises of malicious activity on their own networks. Vulnerable open resolvers are generally used to amplify attacks on other networks, and as such, measuring the impact this causes is very difficult.

% change (open resolvers)	AS number	AS name	Country	# of IPs	% change (index)
341.7%	**12883**	FARLEP-AS Farlep-Internet ISP	**UA**	47,360	**-21.2%**
206.3%	**7381**	SASUSA SunGard Availability Services UK	**US**	432,896	**37.7%**
153.8%	**23724**	CHINANET-IDC-BJ-AP IDC, China Telecommunications...	**CN**	1,414,688	**38.7%**
150.0%	**36024**	COLO4-CO - Colo4Dallas LP	**US**	44,032	**35.4%**
97.4%	**42910**	SADECEHOSTING-COM Sadecehosting-Com	**TR**	68,096	**10.5%**
92.9%	**6400**	VERIZON DOMINICANA	**DO**	443,648	**-14.9%**
89.1%	**20746**	ASN-IDC IT Telecom S.p.A.	**IT**	105,984	**31.6%**
83.3%	**15493**	RUSCOMP-AS Autonomous System for JSC _Russian...	**RU**	14,336	**55.2%**
71.4%	**29614**	GHANATEL-AS	**GH**	108,288	**-23.2%**
66.7%	**34584**	KHBDSV AS for ISP - Khabarovsk Telecommunication Center	**RU**	259,328	**-19.8%**

Frequently Asked Questions

Methodology

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.

Definitions

"# of IPs"

Throughout the report, "# of IPs" refers to the number of number of *originating* IPv4 addresses allocated to the AS. In the context of countries, it is the sum of the "# of IPs" for each AS in that country.

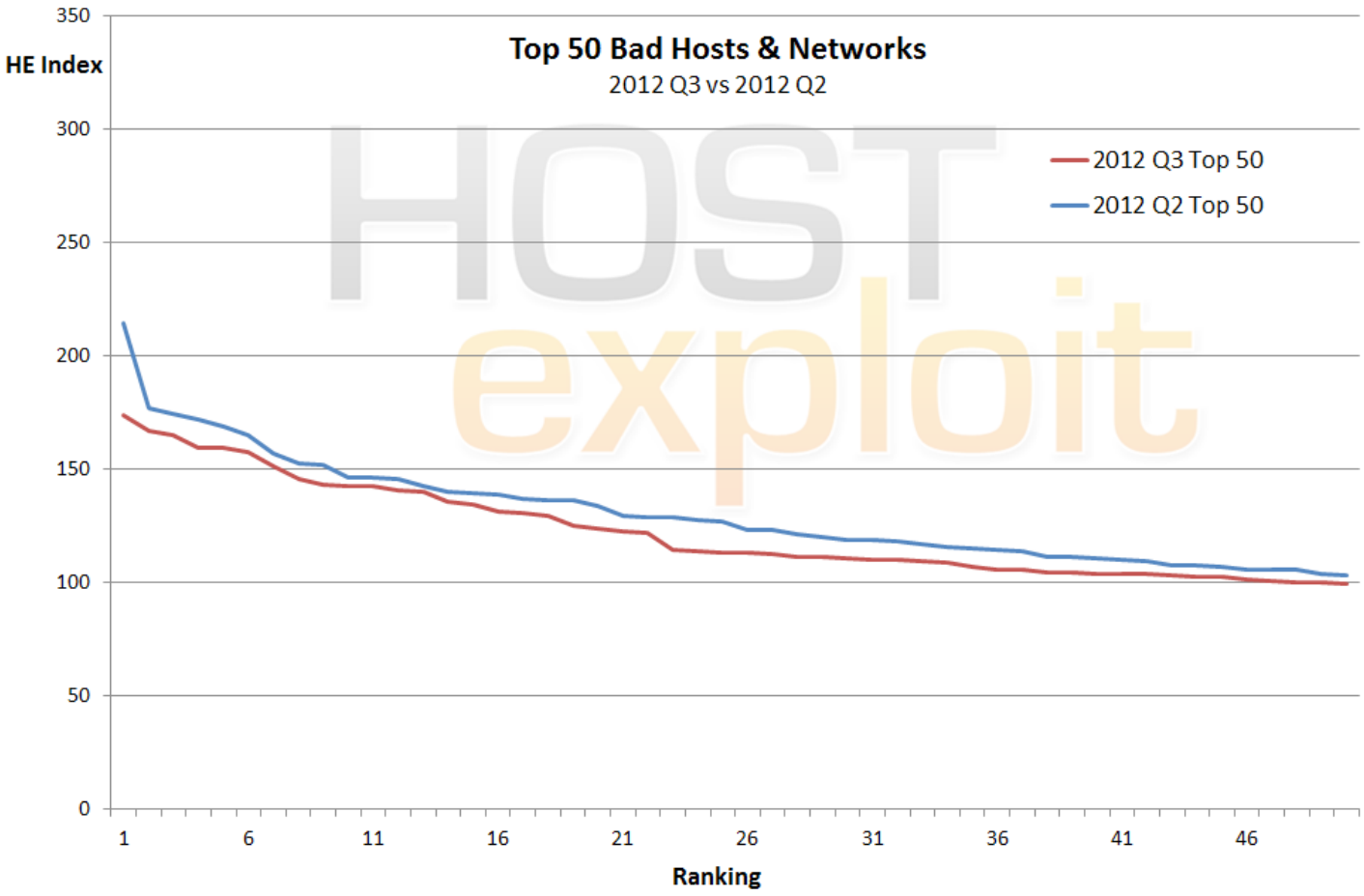
"Country"

Since an AS will usually be physically routed across multiple countries, HostExploit determines the most prominent country of origin for ASes based on their routing locations and registration data.

4. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲ 1	174.03	40034	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	US	6,400
▲ 2	167.07	16138	INTERIAPL INTERIA.PL Sp z.o.o.	PL	4,096
▲ 3	165.03	39743	VOXILITY-AS Voxility S.R.L.	RO	28,672
▲ 4	159.64	16276	OVH OVH Systems	FR	918,016
▲ 5	159.36	58001	IDEALSOLUTION-AS Ideal Solution Ltd	RU	1,536
▲ 6	157.56	9891	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	TH	19,968
▲ 7	151.22	29182	ISPSYSTEM-AS ISPsystem Autonomous System	RU	41,728
▲ 8	145.45	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM - CDMA...	IN	262,144
▲ 9	143.48	11042	LANDIS-HOLDINGS-INC - Landis Holdings Inc	US	28,416
▶ 10	142.78	50465	IQHOST IQHost Ltd	RU	2,304
▼ 11	142.38	41947	WEBALTA-AS OAO Webalta	RU	14,624
▲ 12	140.90	24940	HETZNER-AS Hetzner Online AG RZ	DE	570,624
▲ 13	139.82	16265	LEASEWEB LeaseWeb B.V.	NL	336,384
▲ 14	135.82	32475	SINGLEHOP-INC - SingleHop	US	316,672
▼ 15	134.65	45538	ODS-AS-VN Online data services	VN	9,472
▲ 16	131.41	38731	VTDC-AS-VN Vietel - CHT Compamy Ltd	VN	32,000
▲ 17	130.44	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	1,264,896
▶ 18	129.30	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	86,016
▲ 19	125.33	26105	Telecarrier, Inc	PA	4,736
▲ 20	123.75	33626	OVERSEE-DOT-NET - Oversee.net	US	3,584
▼ 21	122.47	43146	AGAVA3 Agava Ltd.	RU	18,176
▲ 22	121.69	34201	PADICOM PADICOM SOLUTIONS SRL	RO	6,400
▲ 23	114.62	49981	WORLDSTREAM WorldStream	NL	13,312
▼ 24	113.88	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,312
▼ 25	113.43	33182	DIMENOC - HostDime.com, Inc.	US	131,072
▲ 26	113.25	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	113,836,256
▲ 27	112.38	21788	NOC - Network Operations Center Inc.	US	301,568
▲ 28	111.46	26347	DREAMHOST-AS - New Dream Network, LLC	US	283,904
▲ 29	111.21	32613	IWEB-AS - iWeb Technologies Inc.	CA	243,712
▲ 30	110.88	49335	NCONNECT-AS Navitel Rusconnect Ltd	RU	12,544
▼ 31	110.01	15169	GOOGLE - Google Inc.	US	697,600
▲ 32	109.74	24282	KIR Kagoya Japan CO,LTD	JP	23,808
▼ 33	109.54	47781	ANSUA-AS "Delta-X" LTD	UA	1,536
▲ 34	108.60	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	CN	53,461,248
▲ 35	107.23	49467	INETMAR INETMAR Internet Hizmetleri Autonomous System (izmir)	TR	10,240
▼ 36	105.88	44112	SWEB-AS SpaceWeb JSC	RU	3,584
▲ 37	105.80	24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	2,516,736
▲ 38	104.65	29854	WESTHOST - WestHost, Inc.	US	64,000
▲ 39	104.23	53665	BODIS-1 - Bodis, LLC	US	1,024
▲ 40	104.02	8386	KOCNET VODAFONE NET ILETISIM HIZMETLERI A.S	TR	426,496
▲ 41	103.98	26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC	US	1,415,680
▲ 42	103.79	32181	ASN-GIGENET - GigeNET	US	42,240
▲ 43	103.32	35569	PETERHOST-MOSCOW Concorde Ltd.	RU	2,048
▲ 44	102.82	13147	NETINFO NetInfo Ltd.	BG	5,120
▲ 45	102.54	12824	HOMEPL-AS home.pl sp. z o.o.	PL	204,800
▼ 46	101.08	29671	SERVAGE Servage GmbH	EU	12,288
▲ 47	100.46	14618	AMAZON-AES - Amazon.com, Inc.	US	1,087,488
▲ 48	100.32	9198	KAZTELECOM-AS JSC Kazakhtelecom	KZ	2,541,568
▼ 49	99.90	9931	CAT-AP The Communication Authoity of Thailand, CAT	TH	209,664
▲ 50	99.19	9829	BSNL-NIB National Internet Backbone	IN	9,055,488

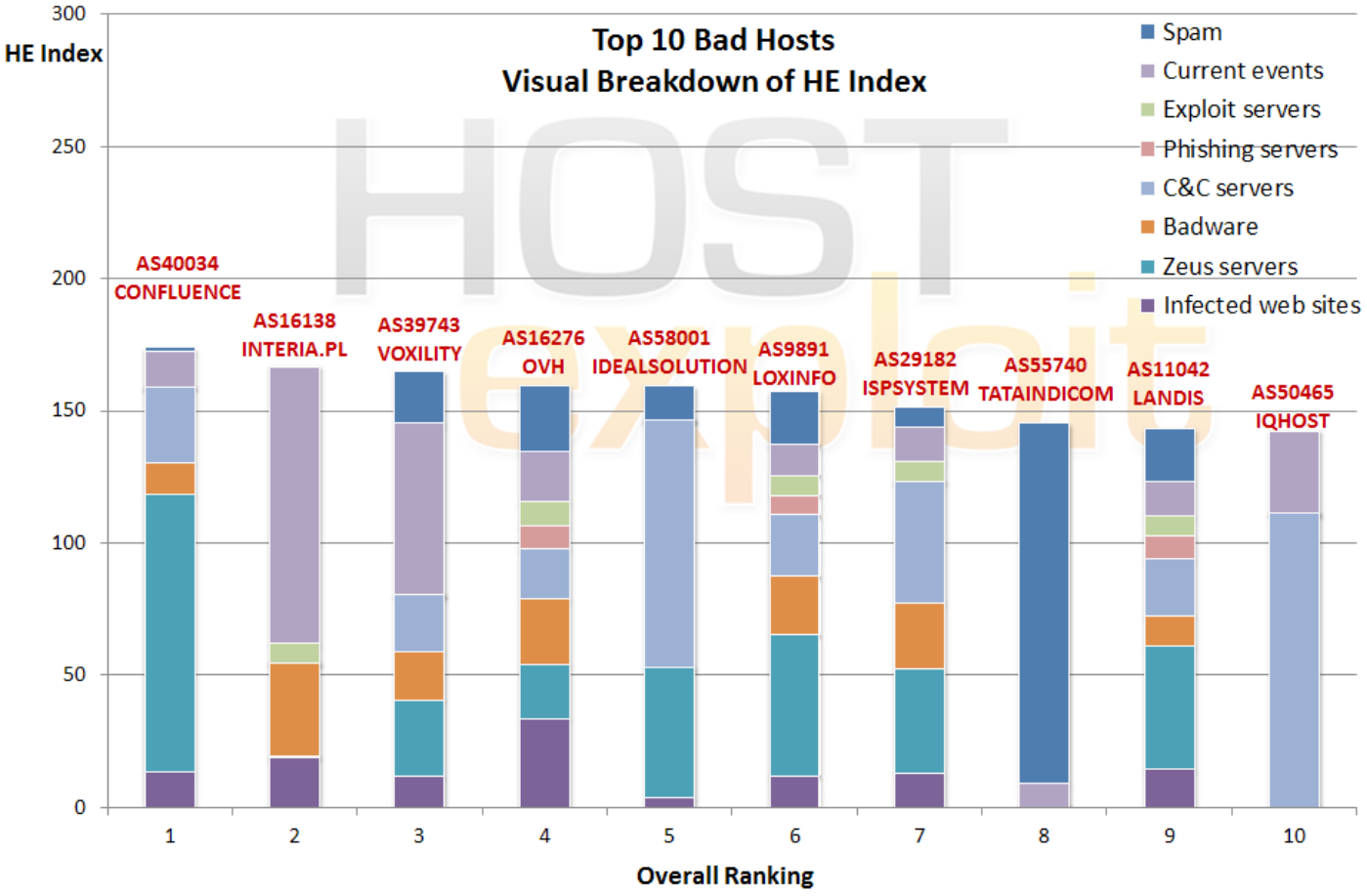
2012 Q3 to 2012 Q2 Comparison



A comparison of the Top 50 hosts in September 2012 with June 2012.

The overall distribution of concentrations of malicious activity has remained almost identical, although the levels of the top 50 overall have dropped slightly.

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 newcomer AS40034 Confluence Networks, holds the #1 position largely due to Zeus servers and other C&C servers.

AS55740 Tata Indicom's presence in the Top 10 almost entirely due to spam.

AS16276 OVH, however, is serving a wide range of malicious activity across all sectors.

What's New?

7.1. Overview

	Previous Quarter - Q2 2012			Current Quarter - Q2 2012		
	ASN	Name	Country	ASN	Name	Country
#1	41947	Webalta	RU	40034	Confluence	US
#2	44112	SWEB	RU	16138	Interia.pl	PL
#3	45538	ODS	VN	39743	Vocility	RO
#1 for Spam	41859	TIC	IR	55740	Tata Indicom	IN
#1 for Botnets	50465	IQHost	RU	50465	IQHost	RU
#1 for Zeus Botnet	34201	Padicom	RO	40034	Confluence Networks	US
#1 for Phishing	43362	Majordomo	RU	53665	Bodis	US
#1 for Exploit Servers	2607	Slovak Academic Network	EU	48614	ITSoft	RU
#1 for Badware	9809	Nova Network	CN	26105	Telecarrier	PA
#1 for Infected Sites	45538	Online data services	VN	41947	Webalta	RU
#1 for Current Events	16138	Interia.pl	PL	16138	Interia.pl	PL

Zeus Botnets – The #1 spot is shared between AS34201 Padicom (#1 in Q2) and the new overall #1 AS40034 Confluence Networks..

The #1 for Badware goes to AS26105 Telecarrier registered in Panama, although last quarter's #1 AS9809 Novanet registered in China has only dropped to #2.

For Botnet C&C's AS50454 IQ Host, registered in the Russian Federation, is sticking resolutely to its #1 position from the last quarter.

There is a new miscreant at the #1 spot for Phishing – AS53665 Bodis registered in China and routed via the United States.

In the Exploit Server Category, AS48614 ITSOFT registered in the Russian Federation has overtaken AS2607 Sanet at #1.

At #1 for current events by a long way is AS16138 Interia.pl. HE considers this to be the category with the worst types of exploits that are currently available.

While AS41947 Webalta registered in the Russian Federation has improved in the overall rankings from #1 in Q2 to #11 in Q3, it has surged to the top position for the number of Infected websites it is currently serving. However, it is important to praise Webalta for its serious effort to clean up some parts of its networks. This is a trend that HE wholeheartedly supports with the hope that this trend will gain momentum over the coming months.

7.2. Top 10 Newly Registered Hosts - In Q3 2012

By end of Q3 2012 there were **42,386** ASes; an increase of **751** from end of Q2 2012.

Below we show a selection of 10 ASes registered in Q3 2012 with the highest HE Indexes. With significant levels of badness recorded in a short period of time, these hosts are of interest.

Listed below the 10 Q3 ASes are the same findings in the previous two quarterly reports.

It is interesting to note that in the last 3 quarterly reports, of the 30 newly-registered ASes we have highlighted as being of interest, several of these no longer exist. This demonstrates the high level of churn among disposable cybercrime hosts.

Period	HE Rank	HE Index	AS number	AS name	Country	# of IPs
2012 Q3	5	159.4	58001	IDEALSOLUTION-AS Ideal Solution Ltd	RU	1,536
	328	62.1	131087	MTS-INDIA-IN 334,Udyog Vihar	IN	403,200
	1,787	26.4	22909	COMCAST-22909 - Comcast Cable Communications, Inc.	US	1,280
	2,162	22.5	58477	ARGON-AS-ID Argon Data Communication	ID	768
	2,207	22.1	50886	NETFIL-AS NETFIL SRL	RO	2,048
	2,395	20.5	50757	KTLNET-AS KTL NET GALATI SRL	RO	1,536
	2,404	20.5	131109	DIGITALNETWORK-IN E-14, Rooprajat Nagar, Tarapur Road	IN	2,560
	2,443	20.2	59458	PURELINE Pure Line Co. For Telecommunications & Internet Ltd.	IQ	5,888
	2,458	20.1	34932	FUZION Fuzion is a Danish Internet Service Provider	DK	512
	2,521	19.7	59443	BAYNUR-AS Baynur and P Ltd.	KZ	2,048
2012 Q2	107	84.5	57668	SANTREX-AS Santrex Internet Services Ltd.	GB	1,280
	1,090	38.2	39365	MICROLINES-AS MICROLINES ISP	LV	8,192
	1,201	35.6	57972	WEBEXXPURTS Deepak Mehta FIE	EE	10,752
	1,485	30.5	132241	SKSATECH1-MY SKSA TECHNOLOGY SDN BHD	MY	1,024
	1,731	26.4	34934	UKFAST UKFast.Net Ltd	GB	27,648
	1,789	25.7	33667	CMCS - Comcast Cable Communications, Inc.	US	0
	1,863	24.8	33659	CMCS - Comcast Cable Communications, Inc.	US	8,192
	2,057	23.0	54444	AVESTA-NETWORKS-LLC - Avesta Networks LLC	US	6,144
	2,338	20.6	132116	ANINETWORK-IN Ani Network Pvt Ltd	IN	1,024
	2,440	20.0	34170	AZTELEKOM Azerbaijan Telecomunication ISP	AZ	36,096
2012 Q1	274	67.0	48031	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	UA	16,640
	653	50.8	12327	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business international	GB	4,608
	906	44.6	49087	PODCEM-AS Open JSC "Podilskiy Tcement"	UA	256
	1,337	35.3	24768	ALMOUROLTEC ALMOUROLTEC SERVICOS DE INFORMATICA E...	PT	2,048
	1,828	27.8	51699	ANTARKTIDA-PLUS-AS Antarktida-Plus LLC	UA	256
	1,875	27.3	49236	RELNET-AS TOV "Leksim"	UA	256
	1,948	26.4	57704	SPEED-CLICK-LTD SpeedClick for Information Technology and...	IL	2,048
	2,053	25.4	31408	ORANGE-PALESTINE Orange Palestine Group Co. for Technological...	PS	1,024
	2,212	24.0	37385	SONITEL	NE	8,960
	2,260	23.7	34109	AS34109 CB3ROB Ltd. & Co. KG	NL	9,216

7.3. Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-81.0%	44	107.2	2,417	20.4	44553	SNS-BG-AS Smart Network Solutions Ltd.	BG	5,376
-79.2%	11	146.2	1,515	30.4	16125	DC-AS UAB Duomenu Centras	LT	9,728
-71.4%	20	133.8	1,115	38.3	48159	TIC-AS Telecommunication Infrastructure Company	IR	177,024
-66.2%	25	127.1	914	42.9	44368	ASDELTAMANAGEMENT DELTA MANAGEMENT AB	SE	3,072
-65.4%	32	118.2	1,020	40.9	48716	PS-AS PS Internet Company Ltd.	KZ	1,024
-65.4%	15	139.2	702	48.2	43362	MAJORDOMO MAJORDOMO LLC	RU	2,560
-63.3%	145	77.5	1,643	28.5	3216	SOVAM-AS OJSC "Vimpelcom"	RU	780,800
-62.0%	76	92.6	1,238	35.2	44557	DRAGONARA Dragonara Alliance Ltd	GB	2,816
-57.4%	116	82.7	1,235	35.2	34941	CYBERCOM-AS CyberCom & YT AB	SE	2,048
-55.3%	31	118.8	557	53.0	6939	HURRICANE - Hurricane Electric, Inc.	US	737,536

The hosts in the above table are all worthy of mention for their improved rankings in the three months since our Q2 2012 report.

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

The most improved host is:

- AS44553 SNS-BG-AS Smart Networks Solutions Ltd (Bulgaria) down from #44 to #2,417.
- Among the hosts in this category the highest placed host last quarter was AS16125 DC-AS UAB Duomenu Centras. (Lithuania), #11, now improved to #1,515.
- All the hosts in this category provide evidence that ranking positions can be improved.

7.4. Deteriorated Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
147.5%	1,233	35.0	86	86.5	51377	BURSTNETLTD BurstNET Limited	GB	2,048
116.9%	129	80.2	1	174.0	40034	CONFLUENCE-NETWORK-INC - Confluence Net...	US	3,840
94.4%	760	46.8	73	90.9	55660	MWN-AS-ID PT Master Web Network	ID	512
91.6%	360	59.8	23	114.6	49981	WORLDSTREAM WorldStream	NL	3,072
80.1%	600	51.4	64	92.6	47583	HOSTING-MEDIA Aurimas Rapalis...	US	28,416
69.9%	301	63.1	35	107.2	49467	INETMAR INETMAR Internet Hizmetleri...	TR	12,288
66.6%	309	62.6	39	104.2	53665	BODIS-1 - Bodis, LLC	US	2,048
64.2%	92	87.4	9	143.5	11042	LANDIS-HOLDINGS-INC - Landis Holdings Inc	US	1,792
45.7%	548	52.7	126	76.8	25761	STAMINUS-COMM - Staminus Communications	US	4,096
44.6%	563	52.3	132	75.7	39134	SKYMEDIA United Network LLC	RU	1,536

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

The most deteriorated host this quarter is AS51377 BurstNet Ltd (United Kingdom) up from #1,233 in Q2 2012 to #86. BurstNet is displaying an unusually high incidence rate for Zeus servers.

AS44553 SNS-BG-AS Smart Network Solutions Ltd has had nearly as sharp a rise in the rankings, due to a large increase in hosting of Botnet C&Cs and spam

Top 10 Countries

Our new methodology more accurately determines 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.

We 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: This table is a small sample of the results available on the Global Security Map website where a full list of countries and rankings can be found.

Country Scoring		Country Details			
Rank	**Index**	**Code**	**Name**	**# of ASes**	**# of IPs**
1	311.4	RU	RUSSIAN FEDERATION	3,972	53,448,864
2	297.2	LV	LATVIA	197	1,764,224
3	233.6	TR	TURKEY	285	21,070,336
4	225.8	LU	LUXEMBOURG	43	1,023,744
5	225.3	UA	UKRAINE	1,663	14,502,144
6	211.8	MD	MOLDOVA, REPUBLIC OF	62	1,450,752
7	211.0	RO	ROMANIA	1,070	14,049,024
8	202.8	FR	FRANCE	733	63,102,016
9	202.5	PL	POLAND	1,495	21,635,904
10	200.8	AZ	AZERBAIJAN	32	738,064

It is disappointing to see that the Russian Federation remains at #1 for the worst levels of malicious activity when using our new method of calculation.

New arrivals are France, Poland and Azerbaijan in at #8, #9 and #10 respectively.

The complete table of country rankings is available on our interaction web tool Global Security Map where filters enable an in-depth analysis of the facts and figures relating to individual countries. This project is in a cycle of continuous development with new features planned for the near future. Please revisit on a regular basis to check out new features or sign up for our newsletter.

Country	Country name		HE Rank	HE Index
RU	**RUSSIAN FEDERATION**		**1**	**311.40**
	Highest sector	**Current events**	1	922.5
	2nd-highest sector	**Badware**	4	409.0
	3rd-highest-sector	**Infected web sites**	5	346.4
LV	**LATVIA**		**2**	**297.23**
	Highest sector	**Badware**	1	912.3
	2nd-highest sector	**Zeus botnets**	2	484.4
	3rd-highest-sector	**Exploit servers**	3	417.6
TR	**TURKEY**		**3**	**233.62**
	Highest sector	**Current events**	5	716.6
	2nd-highest sector	**Botnet C&Cs**	11	375.8
	3rd-highest-sector	**Zeus botnets**	12	224.8
LU	**LUXEMBOURG**		**4**	**225.84**
	Highest sector	**Badware**	2	703.6
	2nd-highest sector	**Zeus botnets**	1	549.9
	3rd-highest-sector	**Infected web sites**	4	430.8
UA	**UKRAINE**		**5**	**225.30**
	Highest sector	**Badware**	3	431.8
	2nd-highest sector	**Current events**	10	348.6
	3rd-highest-sector	**Infected web sites**	8	274.5
MD	**MOLDOVA, REPUBLIC OF**		**6**	**211.84**
	Highest sector	**Infected web sites**	2	865.1
	2nd-highest sector	**Zeus botnets**	5	360.7
	3rd-highest-sector	**Exploit servers**	6	300.1
RO	**ROMANIA**		**7**	**211.02**
	Highest sector	**Exploit servers**	5	331.8
	2nd-highest sector	**Botnet C&Cs**	13	314.1
	3rd-highest-sector	**Infected web sites**	7	279.6
FR	**FRANCE**		**8**	**202.84**
	Highest sector	**Current events**	4	725.8
	2nd-highest sector	**Botnet C&Cs**	16	280.5
	3rd-highest-sector	**Zeus botnets**	20	160.9
PL	**POLAND**		**9**	**202.51**
	Highest sector	**Botnet C&Cs**	5	468.4
	2nd-highest sector	**Current events**	8	362.3
	3rd-highest-sector	**Zeus botnets**	13	210.8
AZ	**AZERBAIJAN**		**10**	**200.76**
	Highest sector	**Infected web sites**	1	904.2
	2nd-highest sector	**Exploit servers**	2	438.0
	3rd-highest-sector	**Current events**	17	267.1

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
37,889	**0.506**	**719**	ELISA-AS Elisa Oyj	**FI**	2,623,616
11,809	**0.880**	**9609**	EACCESS eAccess Ltd.	**JP**	1,105,920
11,804	**0.900**	**226**	LOS-NETTOS-AS - Los Nettos	**US**	445,184
11,799	**0.912**	**34744**	GVM S.C. GVM SISTEM 2003 S.R.L.	**RO**	1,053,696
11,795	**0.913**	**2830**	MCI-DUAL-HOMED-CUSTOMERS Verizon Nederland B.V.	**GB**	314,624
11,785	**0.930**	**206**	CSC-IGN-AMER - Computer Sciences Corporation	**US**	431,616
11,779	**0.938**	**50915**	ASEVERHOST S.C. Everhost S.R.L.	**RO**	340,480
11,768	**0.952**	**9374**	DEODEO DEODEO Corporation	**JP**	165,888
11,755	**0.969**	**19855**	ASN-MASERGY-US Masergy US Autonomous System	**US**	134,400
11,740	**0.972**	**46887**	LIGHTOWER Lightower Fiber Networks (LIGHT-141)	**US**	169,728

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 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.

Hosts by Topic

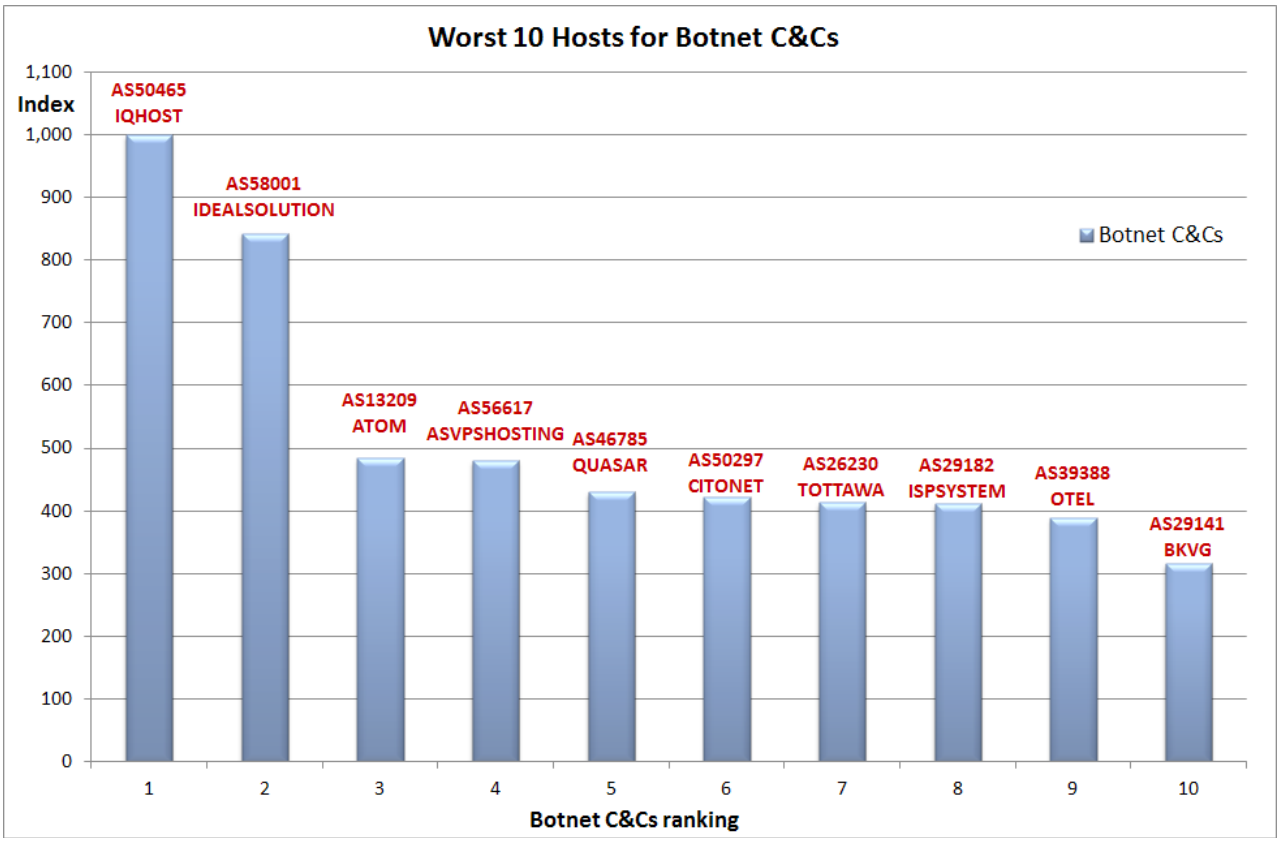
10.1.1. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
10	142.8	**50465**	IQHOST IQHost Ltd	**RU**	2,304	**1,000.0**
5	159.4	**58001**	IDEALSOLUTION-AS Ideal Solution Ltd	**RU**	1,536	**842.9**
124	77.1	**13209**	ATOM-HOSTING Atom Hosting SRL	**RO**	768	**483.8**
364	60.3	**56617**	ASVPSHOSTING SIA "VPS Hosting"	**LV**	1,024	**479.6**
59	94.7	**46785**	QUASAR-DATA-CENTER - QUASAR DATA CENTER, LTD.	**US**	4,608	**430.1**
635	50.1	**50297**	CITONET Centr Informacionnyh Technologii, Ltd.	**UA**	5,376	**421.4**
85	86.8	**26230**	TOTTAWA - Telecom Ottawa Limited	**CA**	22,272	**413.3**
7	151.2	**29182**	ISPSYSTEM-AS ISPsystem Autonomous System	**RU**	41,728	**411.3**
114	79.2	**39388**	OTEL-AS Forcraft Ltd.	**BG**	8,704	**388.7**
163	72.8	**29141**	BKVG-AS Bradler & Krantz GmbH & Co. KG	**DE**	20,736	**315.3**

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 #1 position is the same as in Q1 but now AS50465 IQHOST (Russian Federation) has a compatriot companion at the #2 position AS58001 IDEAL SOLUTION .

There are four new entrants in this catgory meaning that the other six are familiar names presenting little change in the malicious activity being served.

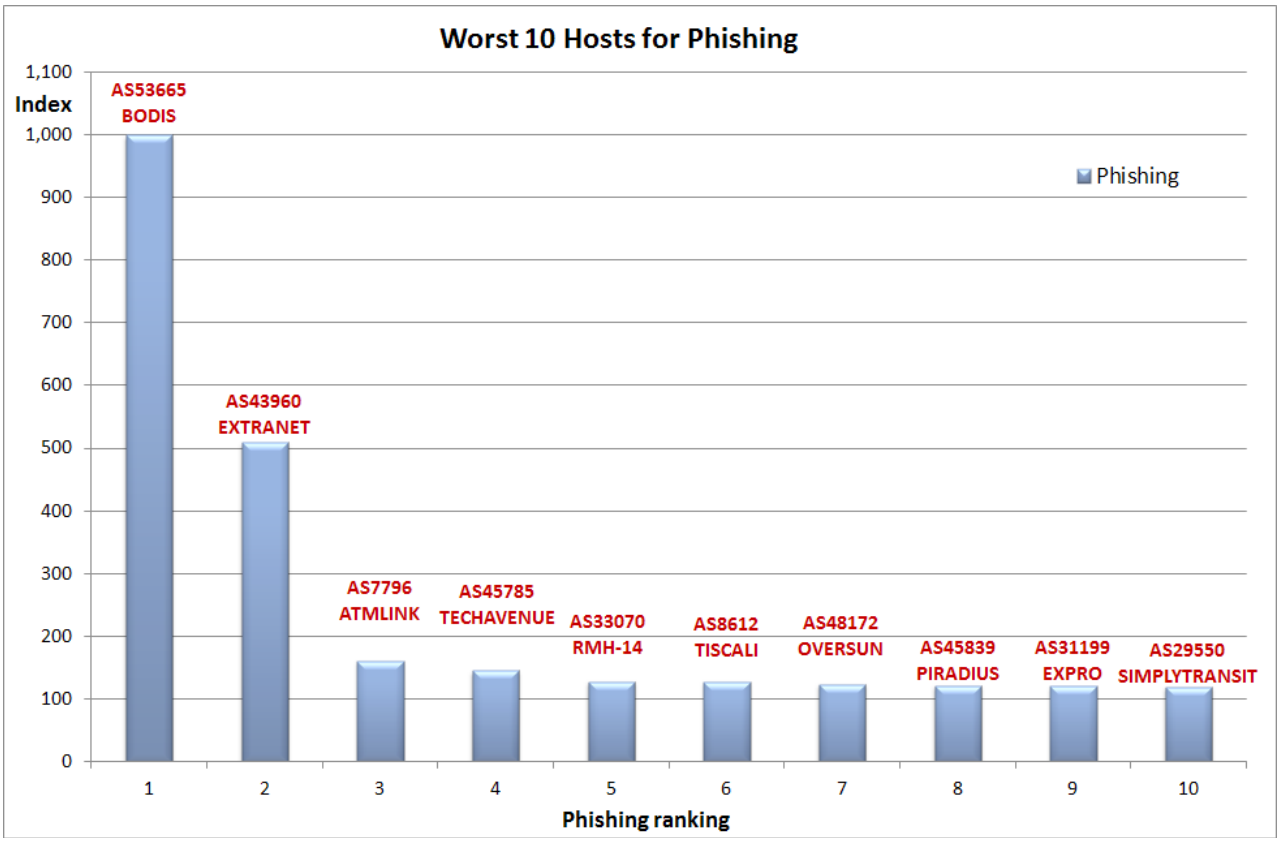


10.1.2. Phishing Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
39	104.2	**53665**	BODIS-1 - Bodis, LLC	**US**	1,024	**1,000.0**
1,113	38.3	**43960**	EXTRANETCTC Consorzio Terrecablate	**IT**	2,048	**508.6**
283	64.0	**7796**	ATMLINK - ATMLINK, INC.	**US**	24,576	**160.1**
741	47.0	**45785**	TECHAVENUE-AP Techavenue Data Center, Global IP Transit, KL...	**MY**	4,352	**145.3**
136	75.4	**33070**	RMH-14 - Rackspace Hosting	**US**	524,800	**127.7**
152	73.6	**8612**	TISCALI-IT Tiscali Italia S.P.A.	**IT**	1,428,736	**127.3**
203	67.7	**48172**	OVERSUN-MERCURY Oversun-Mercury Ltd	**RU**	49,920	**123.4**
279	64.1	**45839**	PIRADIUS-AS PIRADIUS NET AS45839	**MY**	16,384	**120.9**
1,450	31.6	**31199**	EXPRO-AS Expro Sp. z o.o.	**PL**	512	**119.8**
98	83.3	**29550**	SIMPLYTRANSIT Simply Transit Ltd	**GB**	115,456	**119.2**

Phishing and social engineering in general continues to be a cause for concern to banks and corporations of all sizes as cybercriminals endeavour to find new ways of grabbing valuable data or access to 'the money'.

This quarter sees AS43362 MAJORDOMO fall out of the Top 10, with US-based AS53665 Bodis and Italy-based AS43960 EXTRANETCTC moving up to #1 and #2 respectively.



10.1.3. Exploit Servers

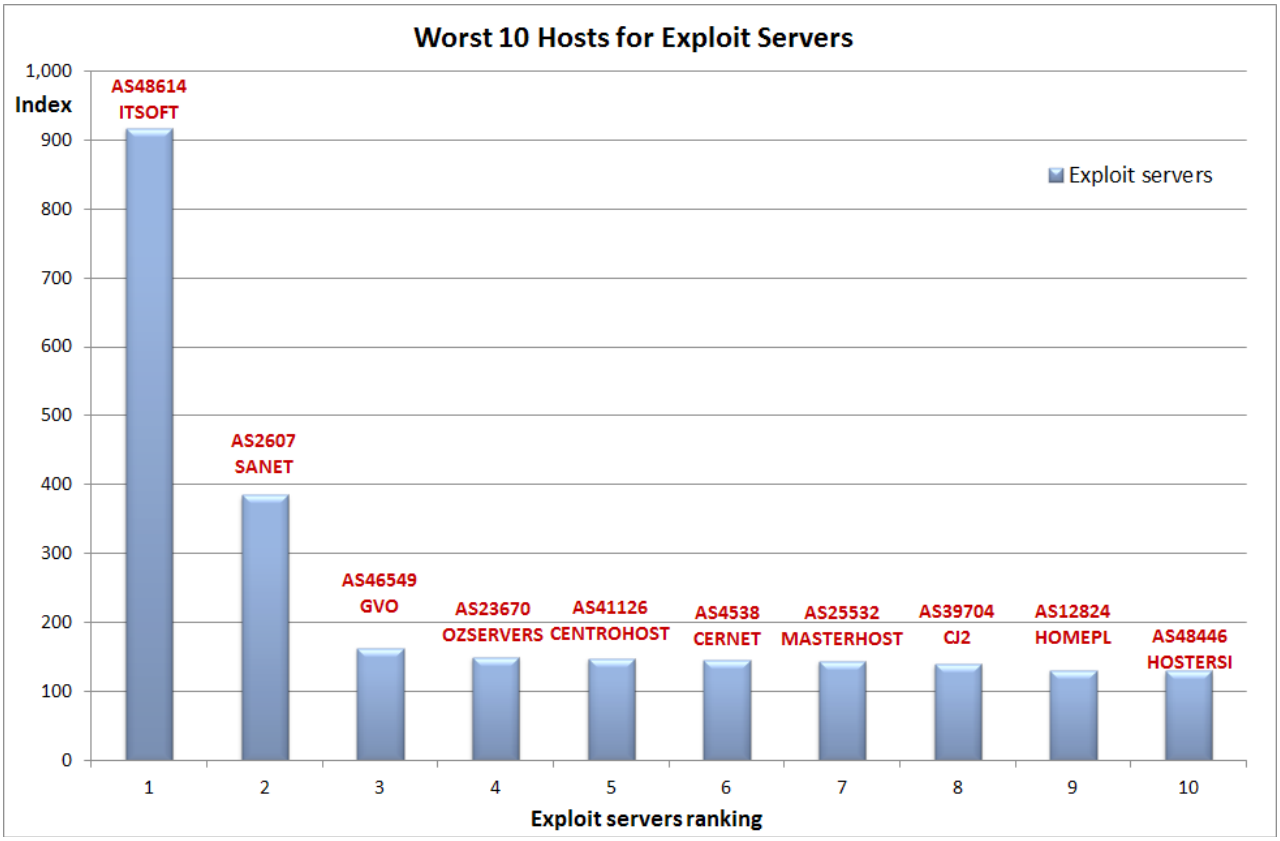
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
54	97.2	**48614**	ITSOFT-AS ITSoft Ltd.	**RU**	2,048	**917.5**
288	63.8	**2607**	SANET Slovak Academic Network	**SK**	526,080	**384.7**
263	64.6	**46549**	GVO - Global Virtual Opportunities	**US**	3,584	**162.7**
556	53.1	**23670**	OZSERVERS-AU Oz Servers, Data Centres, Australia Wide	**AU**	12,288	**149.5**
345	61.3	**41126**	CENTROHOST-AS JSC Centrohost	**RU**	4,096	**148.3**
143	74.4	**4538**	ERX-CERNET-BKB China Education and Research Network Center	**CN**	19,568,384	**145.9**
117	78.3	**25532**	MASTERHOST-AS .masterhost autonomous system	**RU**	77,824	**144.0**
574	52.2	**39704**	CJ2-AS CJ2 Hosting&Development	**NL**	6,400	**140.2**
45	102.5	**12824**	HOMEPL-AS home.pl sp. z o.o.	**PL**	204,800	**130.9**
1,655	28.3	**48446**	HOSTERSI-AS Hostersi Sp. z o.o.	**PL**	1,024	**130.1**

We consider the category of "Exploit Servers" to be one of 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.

Since the previous quarter, AS48614 ITSoft has overtaken the Slovakian AS2607 Sanet to #1.

Unlike the results for Q2, this table presents with several of the same hosts maintaining a high level of poor results to linger in this category.



10.1.4. Botnet Hosting - Zeus

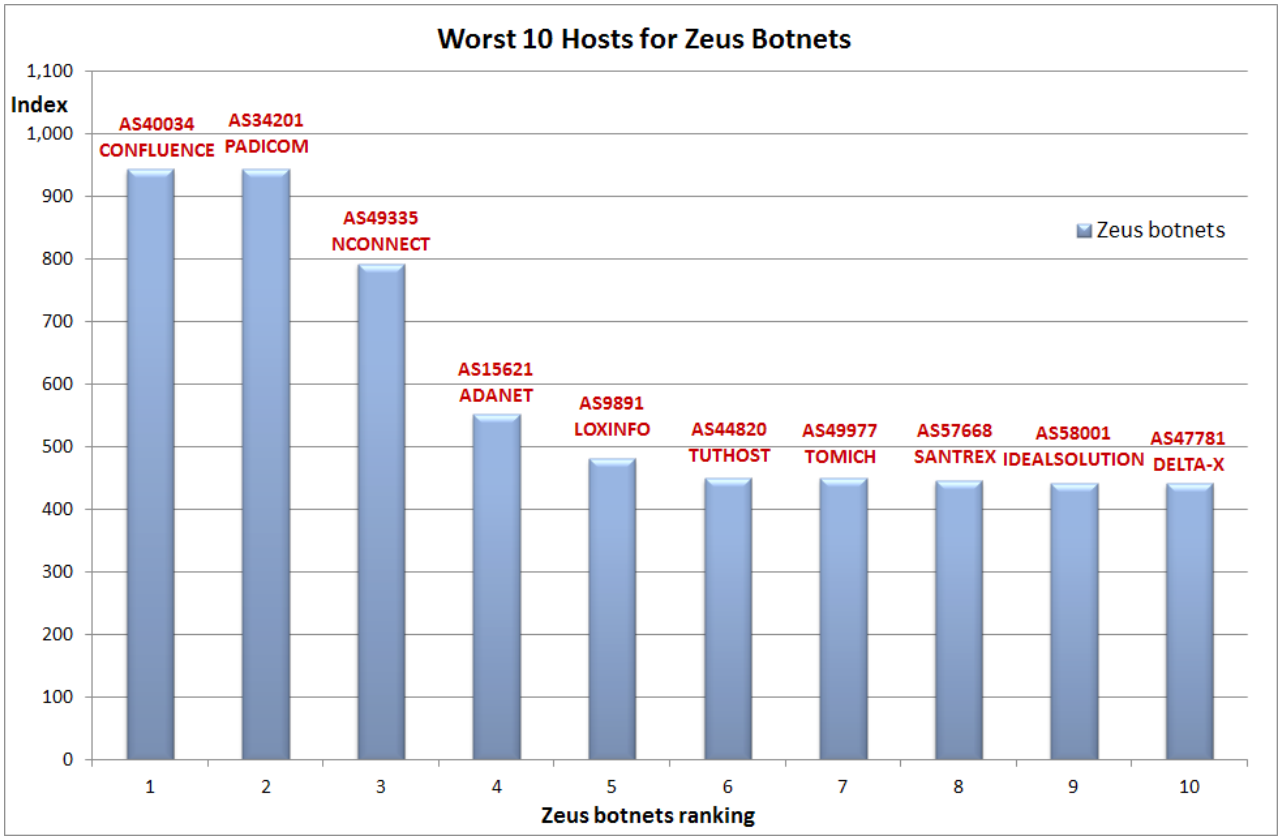
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
1	174.0	**40034**	CONFLUENCE-NETWORK-INC - Confluence Networks Inc	**US**	6,400	**942.9**
22	121.7	**34201**	PADICOM PADICOM SOLUTIONS SRL	**RO**	6,400	**942.9**
30	110.9	**49335**	NCONNECT-AS Navitel Rusconnect Ltd	**RU**	12,544	**791.8**
77	89.9	**15621**	ADANET-AS Azerbaijan Data Network	**AZ**	13,312	**551.3**
6	157.6	**9891**	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	**TH**	19,968	**480.9**
127	76.7	**44820**	TUTHOST Denis Pavlovich Semenyuk	**UA**	1,024	**449.4**
287	63.8	**49977**	TOMICH ZAO "Industrial Financial Corporation "Tomich"	**RU**	1,024	**449.4**
93	83.9	**57668**	SANTREX-AS Santrex Internet Services Ltd.	**RU**	1,280	**445.3**
5	159.4	**58001**	IDEALSOLUTION-AS Ideal Solution Ltd	**RU**	1,536	**441.4**
33	109.5	**47781**	ANSUA-AS "Delta-X" LTD	**UA**	1,536	**441.4**

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.

The stand out feature in this category is the prevalence of service providers registered in Eastern European countries. RU has 4 of the Top 10 in this category.

The #1 spot is now shared between AS34201 Pdicom (#1 in Q2) and the new overall #1 AS40034 Confluence.



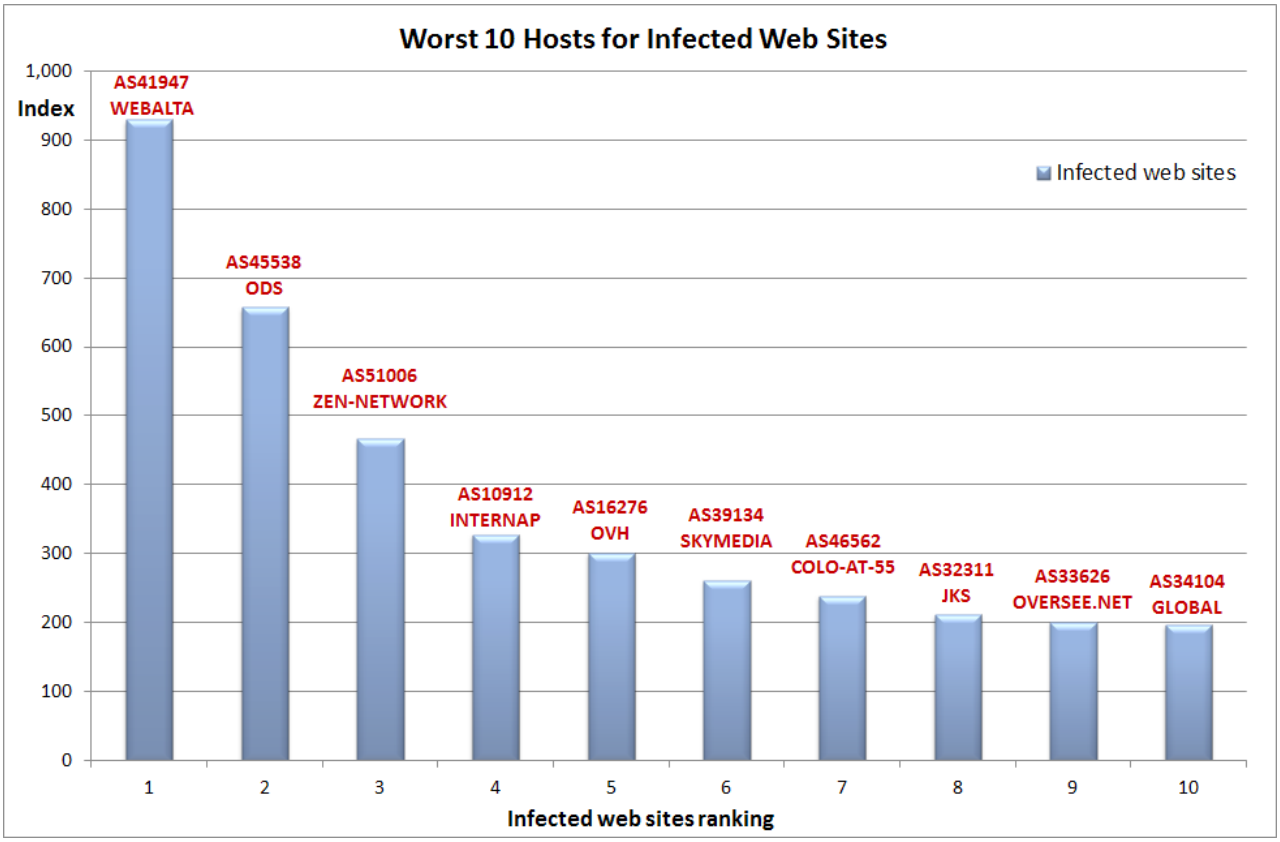
10.2.1. Infected Web Sites

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
11	142.4	**41947**	WEBALTA-AS OAO Webalta	**RU**	14,624	**929.4**
15	134.6	**45538**	ODS-AS-VN Online data services	**VN**	9,472	**657.0**
254	65.2	**51006**	ZEN-NETWORK ZEN Network Technologies Ltd	**GB**	1,280	**466.8**
236	65.9	**10912**	INTERNAP-BLK - Internap Network Services Corporation	**US**	77,056	**327.1**
4	159.6	**16276**	OVH OVH Systems	**FR**	918,016	**300.6**
132	75.7	**39134**	SKYMEDIA United Network LLC	**RU**	19,456	**261.5**
1,966	24.4	**46562**	COLO-AT-55-LLC - Colo at 55, LLC	**US**	27,392	**238.8**
437	56.5	**32311**	JKS-ASN - JKS Media, LLC	**US**	83,712	**210.8**
20	123.7	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,584	**200.4**
97	83.4	**34104**	GLOBAL-AS Global Iletisim Hizmetleri A.S.	**TR**	105,984	**196.9**

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

Here, our own data, gathered from specific honeypots, is combined with data provided by Clean-MX and hphosts on instances of malicious URLs found on individual ASes.

This quarter a number of less familiar names accompany a few well known ones. The #1 position of former AS41947 Webalta, formerly #1 host overall, suggests that counter-measures against infected websites have not been put in place.



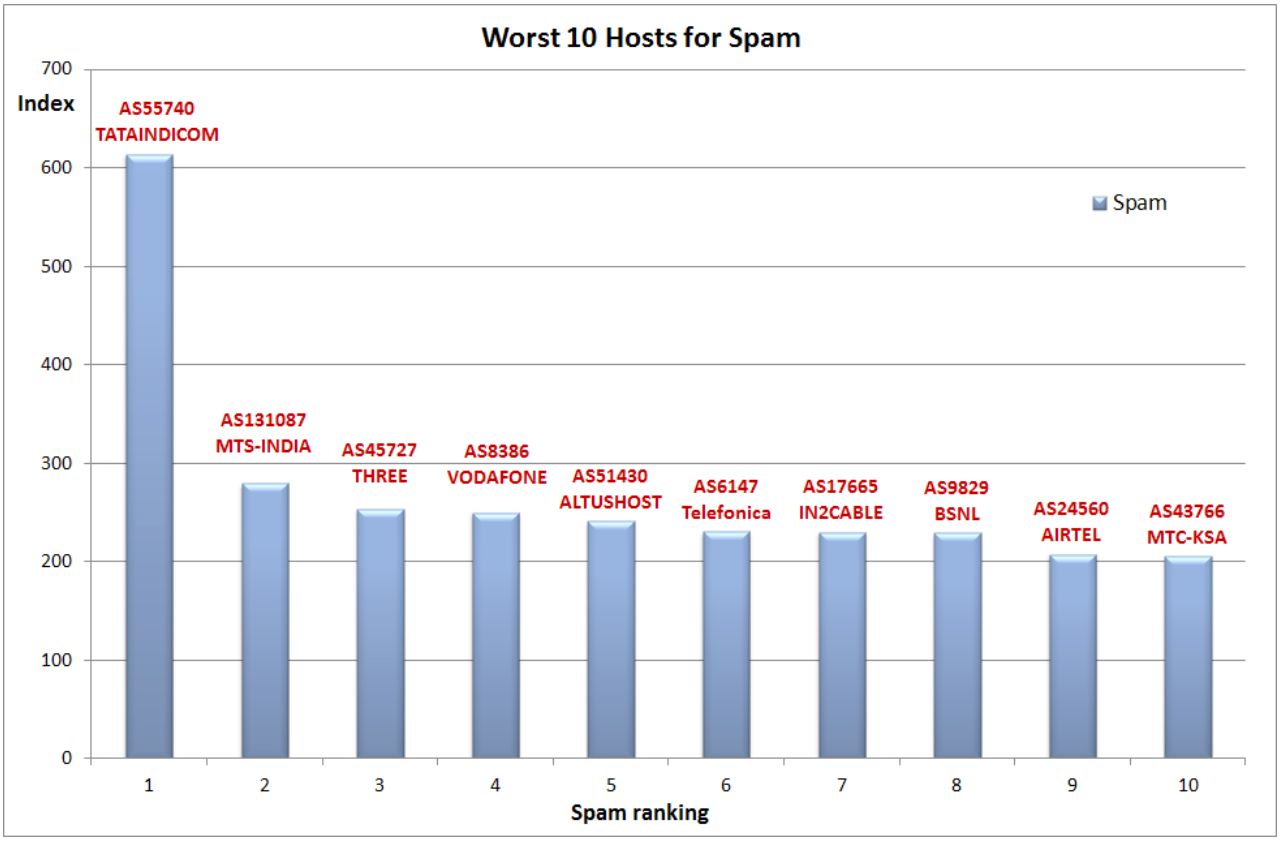
10.2.2. Spam

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
8	145.5	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM...	**IN**	262,144	**614.0**
328	62.1	**131087**	MTS-INDIA-IN 334,Udyog Vihar	**IN**	403,200	**279.6**
442	56.4	**45727**	THREE-AS-ID Hutchison CP Telecommunications, PT	**ID**	3,648	**253.0**
40	104.0	**8386**	KOCNET VODAFONE NET ILETISIM HIZMETLERI A.S	**TR**	426,496	**249.7**
70	91.1	**51430**	ALTUSHOST-NET ALTUSHOST INC.	**NL**	16,384	**240.9**
75	90.0	**6147**	Telefonica del Peru S.A.A.	**PE**	1,943,296	**230.3**
603	51.1	**17665**	IN2CABLE-AP AS Number of In2cable.com (India) Ltd.	**IN**	23,296	**229.5**
50	99.2	**9829**	BSNL-NIB National Internet Backbone	**IN**	9,055,488	**229.2**
37	105.8	**24560**	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	**IN**	2,516,736	**207.4**
789	45.7	**43766**	MTC-KSA-AS MTC KSA Mobile Telecommunication Company	**SA**	1,536	**204.9**

Spammers tend to prefer using servers located in countries with minimal regulation and monitoring as this enables them to operate without fear of retribution.

5 of the 10 ASes are hosted out of India. This is partly due to the lack of regulation in such "safe havens".

It's also worth noting that most of the ASes in the list are primarily for telecommunications. This is explained by the low cost to begin spamming, as well as the disposable nature of spam itself.



10.2.3. Current Events

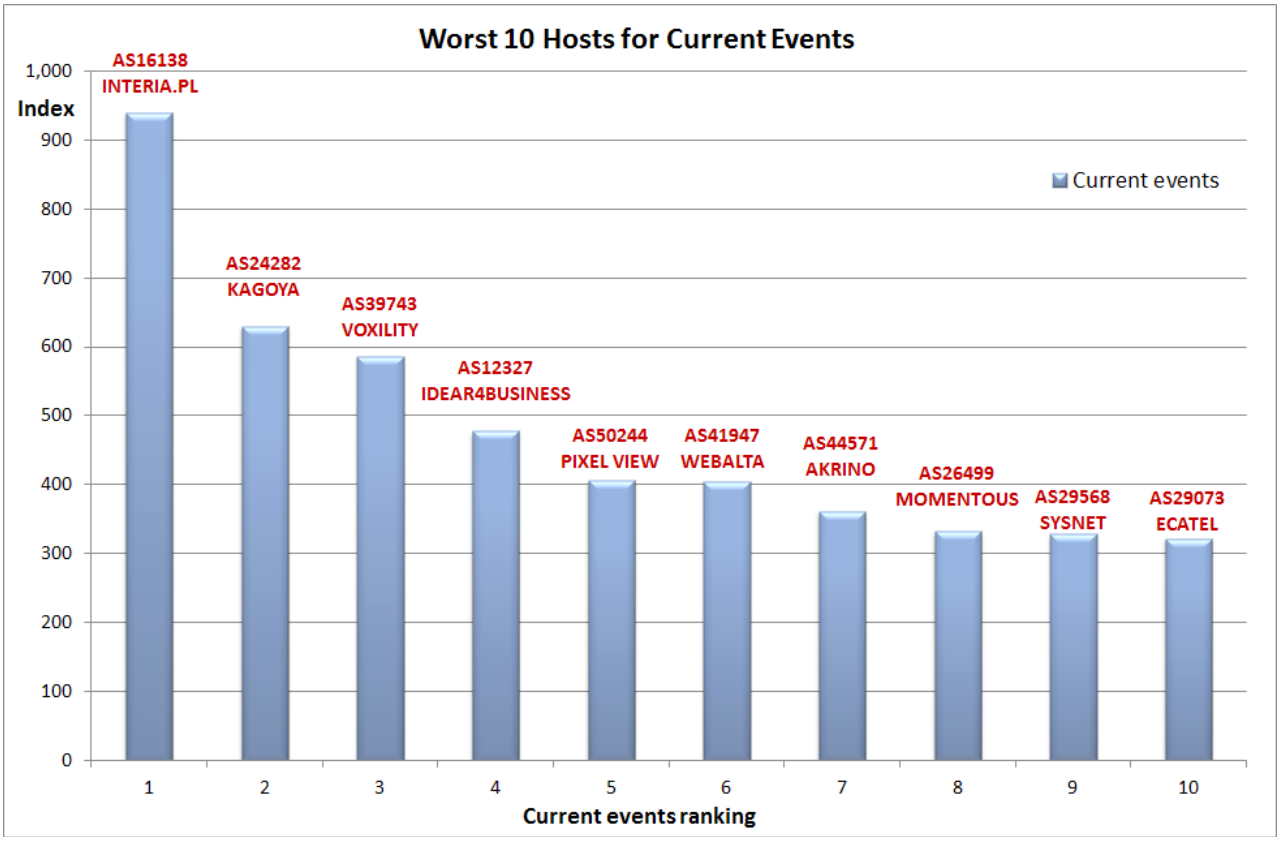
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
2	167.1	**16138**	INTERIAPL INTERIA.PL Sp z.o.o.	**PL**	4,096	**939.8**
32	109.7	**24282**	KIR Kagoya Japan CO,LTD	**JP**	23,808	**630.1**
3	165.0	**39743**	VOXILITY-AS Voxility S.R.L.	**RO**	28,672	**586.2**
237	65.9	**12327**	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business int...	**GB**	2,560	**477.6**
322	62.3	**50244**	ITELECOM Pixel View SRL	**RO**	9,728	**406.2**
11	142.4	**41947**	WEBALTA-AS OAO Webalta	**RU**	14,624	**404.7**
355	60.6	**44571**	AKRINO-AS Akrino Inc	**VG**	1,024	**361.0**
331	62.1	**26499**	MOMENTOUS - MOMENTOUS	**CA**	10,752	**332.1**
1,120	38.2	**29568**	COMTEL-AS SYSNET SECURE S.R.L.	**RO**	17,408	**328.7**
24	113.9	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,312	**322.1**

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

Here HostsExploit's own processes including examples of MALfi (XSS/RCE/RFI/LFI), XSS attacks, clickjacking, counterfeit pharmas, rogue AV, Zeus (Zbota), Artro, SpyEye, Ice9, Stuxnet, DuQu, BlackHat SEO, 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.

This category in earlier reports was previously dominated by US-based hosts. In Q3 2012 the majority in this Top 10 are located in Europe, with 1 in Asia.

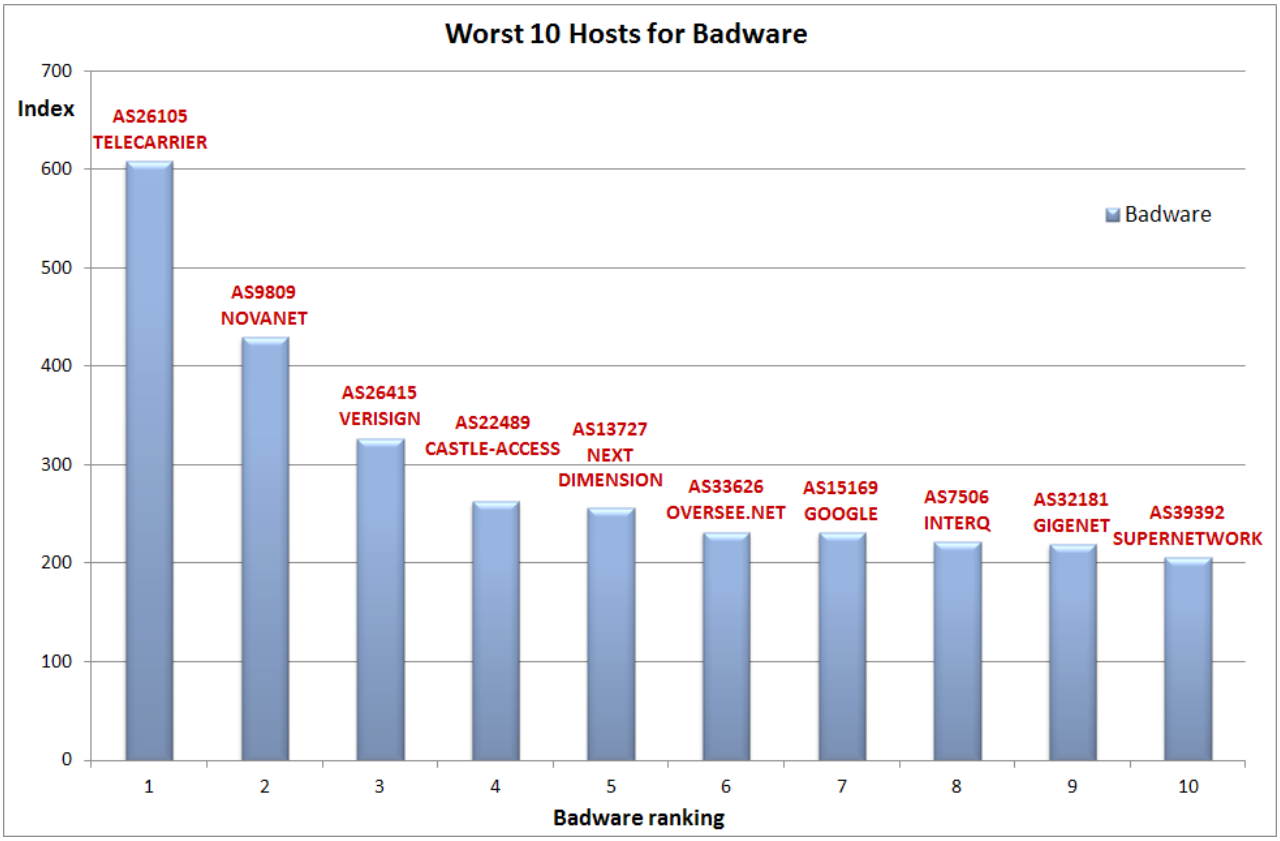


10.2.4. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
19	125.3	**26105**	Telecarrier, Inc	**PA**	4,736	**607.9**
102	81.8	**9809**	NOVANET Nova Network Co.Ltd... Tianan Cyber Park... Shenzhen	**CN**	12,288	**429.6**
148	74.2	**26415**	VERISIGN-INC Verisign	**NL**	11,008	**327.0**
63	93.2	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,152	**262.7**
376	59.5	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**256.7**
20	123.7	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,584	**231.2**
31	110.0	**15169**	GOOGLE - Google Inc.	**US**	697,600	**230.8**
68	91.4	**7506**	INTERQ GMO Internet,Inc	**JP**	102,912	**221.2**
42	103.8	**32181**	ASN-GIGENET - GigeNET	**US**	42,240	**218.8**
240	65.8	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	53,504	**205.3**

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

This quarter many familiar repeat offenders, such as AS9809 NOVANET (China) and AS22489 Castle Access are present, as well as some entries that may be surprising, such as AS26415 Verisign and AS15169 Google.



Conclusion

Conclusion

A stubborn refusal to move down the rankings is a shared characteristic of 7 of the providers in the 'Top 10 Hosts' table for Q3 2012. While it is possible for a responsible host to score badly in the HE Index from time-to-time, as a result of a sudden surge in malicious acivity, this cannot be said of the regular top-place holders. Several consecutive appearances is down to more than simple bad luck. Providers consistently appearing in high positions in any category are failing to implement adequate preventative measures whether it is due to a lack of understanding of the issues involved or, simply, through a a desire to ignore what, or who, is using their networks.

This latter scenario appears to be the case with #2 Host AS16138 Interia.pl, responsible for consistently serving some of the worst types of malicious activity on the web. The vast majority of 'badness' stems from large amounts of 'current events'; the most up-to-date and fast changing of attack exploits and vectors. Offences range from any number of the following including MALfi(XSS/RCE/RFI/LFI), XSS attacks, clickjacking, counterfeit pharmas, rogue AV, Zeus (Zbota), Artro, SpyEye, Ice9, Stuxnet, DuQu, BlackHat SEO as well as newly emerging exploit kits.

Interia.pl (registered in Poland) has been in the 'Top 10' since Q2 2010, (a slight temporary improvement was seen in Q2 2011 when it dropped to #12!). It was #1 in Q1 2012 and frequently in the top 5. So why does Interia remain firmly entrenched at the top of the rankings while others come and go? Just how many computer users have suffered over the past 2 years as a consequence of infected computers and exploits served from Interia hosted systems?

This is a direct message to AS16138 Interia.pl:

> *"Changes to your systems and abuse procedures are long overdue. Please prevent further damage from occurring to the unfortunate and long suffering victims of the individuals or gangs who use your services to carry all manner of Internet malpractices.*
>
> *If you are uncertain where to begin there are a number of agencies who would be willing to help including CERT Poland, CERT-EU , or contact us at: contact@hostexploit.com .*
>
> *In today's competitive environment it does not make business sense to allow your servers to be used for nefarious purposes. Be proactive and instigate a few simple procedures to clean up your networks. Thank you."*

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.

Current Events:

The most up-to-date and fast changing of attack exploits and vectors. Offences within this category include MALfi(XSS/RCE/RFI/LFI), XSS attacks, clickjacking, counterfeit pharmas, rogue AV, Zeus (Zbota), Artro, SpyEye, Ice9, Stuxnet, DuQu, BlackHat SEO as well as newly emerging exploit kits.

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.

DDOS (Distributed Denial of Service):

DDoS attacks or floods can be executed in a variety of ways. The desired effect is to interrupt the normal business of a web service. Attackers use the power of multiple computer systems, via a botnet or by number of users, to cause a system crash. Another method of attack is by amplification using multiple DNS requests via open resolvers.

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.

DNS Security Extensions (DNSSEC):

A set of DNS extensions that authenticate the origin at DNS level and checks the integrity of DNS data. Implementation is required at registry level for the most effective protection.

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

August 6, 2012

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.
4.	July 2012	Sources 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.

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 / C-SIRT	Badware instances	Very high
4.	SudoSecure / HostExploit	Spam bots	Low
5.	Shadowserver / HostExploit / SRI	C&C servers	High
6.	C-SIRT / HostExploit	Phishing servers	Medium
7.	C-SIRT / HostExploit	Exploit servers	Medium
8.	C-SIRT / HostExploit	Spam servers	Low
9.	HostExploit	Current events	High
10.	hpHosts	Malware instances	High
11.	Clean MX / C-SIRT	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:

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

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)*