HostExploit - January 2011

HostExploit's Worldwide Cybercrime Series

Top 50 Bad Hosts and Networks 4th Quarter 2010 - Report

HOST exploit

SITEVET

Table of Contents

HOST exploit

SITEVET

Top 50

CyberCrime Series

Bad Hosts and Networks

Backing from

nominettrust

www.nominettrust.org.uk

Edited by

- Jart Armin

Review

- Andre' M. DiMino
- Dr. Bob Bruen
- Albena Spasova
- Raoul Chiesa

Contributors

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

Comparative Data

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

Top 50

CyberCrime Series

Bad Hosts and Networks

Foreword

In recent years we have witnessed a large upward trend in Internet criminal activity, particularly in the areas of malware distribution, spam, electronic fraud, and botnet related activities. A key data point in addressing this activity comes from the identification and tracking of the network and hosting service providers that facilitate these criminal services. In some cases, it's fairly easy to identify the providers that facilitate these malicious activities, and they are well known within the security community. In other cases, it's not very clear. Criminal gangs now often distribute their operations across multiple providers, thus building in resiliency and a higher availability.

The majority of network and hosting providers are very concerned about their reputation and will respond in rapid fashion when notified of malicious activity. Others are content to let such activities flourish. In any case, it is important to highlight those providers where malicious activity is rampant, and raise general public awareness.

HostExploit's Quarterly Top 50 report is an effort to do just that. This report is especially valuable in that it is not deriving opinion or statistics from few sources with limited visibility into the wide range of criminal activity. It aggregates and correlates the data and findings of many industry partners and researchers who specialize in these areas. The current threat landscape demands more collaboration and coordination among legitimate hosting providers, the security community, and law enforcement. It also demands shining a bright light on those locations that continue to facilitate Internet criminal activity, without public scrutiny.

It is hoped that this latest HostExploit report serves not only to meet these demands, but also to drive greater tracking and accountability of these hosts and networks as well as their own upstream providers.

Andre' M. Di Mino
Co-Founder & Director of The Shadowserver Foundation

Introduction

HostExploit presents the fourth quarter 2010 report in our ongoing series on the **Top 50 Bad Hosts and Networks.**

Analysis of 36,371 public ASes (Autonomous Systems), exchanging routing information with each other over the public Internet, provides the backbone for this research.

The resulting information has been analyzed using a unique combination of formulae and focuses on the worst aspects of cyber-criminal activity in order to create a bespoke 'badness' rating.

This takes into account the size of each network in question, recognizing that larger servers offer greater potential for distributing malware, but also that such larger servers are under more pressure to undertake effective monitoring. The result is an easily understandable measurement of damage caused to internet users by 'bad' activity. We call this measurement the **HE Index**.

For further details about the methodology behind the HE Index, please refer to **Appendix 2**.

The security and wider internet community can play an active role in calling for more stringent enforcement of abuse policies.

The power of community action should not be underestimated, as illustrated in the recent exposure and demise of the malware serving host Troyak.

Credit should be given where it is due, however, and we whole-heartedly support the vast majority of hosting providers who do a good job in keeping cybercriminals at bay. For this reason we also highlight the 'Top 10 Good Hosts', an accolade that I hope the qualifying hosts will appreciate when so much about security is given a negative perspective.

Please note the quantitative analysis of each of the 36,371 ASes can be viewed daily on **SiteVet.com**

Jart Armin

Editor's Note

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

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

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

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

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

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

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

Why do these hosts allow this activity?

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

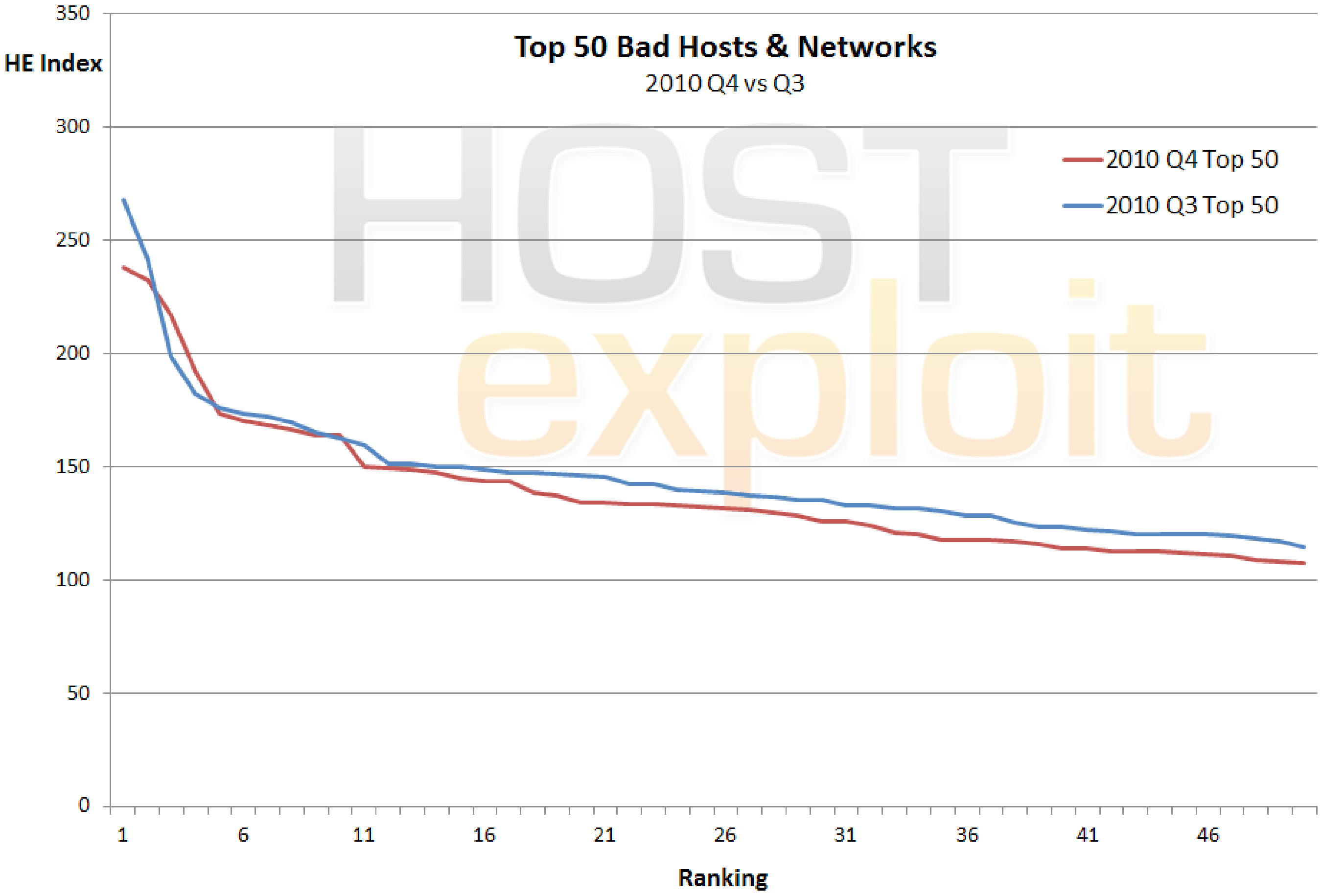
Further feedback is warmly welcomed

admin@hostexploit.com

2. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲1	238.3	29106	VOLGAHOST-AS PE Bondarenko Dmitriy Vladimirovich	RU	256
▼2	232.5	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,056
▲3	217.4	21740	ENOMAS1 - eNom, Incorporated	US	12,288
▲4	192.1	10297	ENET-2 - eNET Inc.	US	90,368
▲5	173.2	6849	UKRTELNET JSC UKRTELECOM,	UA	1,119,744
▼6	170.2	39150	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	RU	5,888
▲7	168.2	6697	BELPAK-AS BELPAK	BY	746,240
▼8	166.2	6851	BKCNET "SIA" IZZI	LV	49,152
▼9	164.1	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,673,728
▼10	164.1	16138	INTERIAPL INTERIA.PL Autonomous System	PL	3,072
▲11	149.8	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	44,544
►12	149.0	16276	OVH OVH	FR	411,392
▲13	148.9	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	106,110,208
▲14	147.4	36408	CDNETWORKS-GLOBAL unified ASN for CDNetworks...	US	35,328
▲15	144.8	28753	NETDIRECT AS NETDIRECT Frankfurt, DE	DE	108,544
▲16	143.9	48876	INTERA-AS Takomi Ltd	RU	512
▲17	143.5	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	57,344
▲18	138.3	24940	HETZNER-AS Hetzner Online AG RZ	DE	445,440
▲19	137.4	32475	SINGLEHOP-INC - SingleHop	US	197,632
▲20	134.1	18866	ATJEU - Atjeu Publishing LLC	US	12,800
▲21	133.9	28299	CYBERWEB NETWORKS LTDA	BR	17,408
▲22	133.7	31133	MF-MGSM-AS OJSC MegaFon Network	RU	14,080
▼23	133.3	29629	INETWORK-AS IEUROP AS	FR	8,192
▲24	132.5	21788	NOC - Network Operations Center Inc.	US	278,528
▲25	132.3	32613	IWEB-AS - iWeb Technologies Inc.	CA	218,112
▼26	131.5	39392	SUPERNETWORK-AS SuperNetwork s.r.o.	CZ	34,048
▲27	131.2	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	658,176
▲28	129.8	15169	GOOGLE - Google Inc.	US	265,984
▲29	128.1	41947	WEBALTA-AS OAO Webalta	RU	13,824
▲30	125.8	9829	BSNL-NIB National Internet Backbone	IN	4,852,224
▲31	125.6	20564	INFORMEX-MNT Informex, E-commerce Service Provider	UA	256
▲32	123.7	49087	TELOS-SOLUTIONS-AS Telos Solutions LTD	LV	256
▲33	121.0	9809	NOVANET Nova Network Co.Ltd...Futian District, Shenzhen ,China	CN	11,008
▲34	120.0	11798	ACEDATACENTERS-AS-1 - Ace Data Centers, Inc.	US	99,328
▲35	117.6	8560	ONEANDONE-AS 1&1 Internet AG	DE	358,912
▼36	117.4	33626	OVERSEE-DOT-NET - Oversee.net	US	4,096
▲37	117.4	26496	PAH-INC - GoDaddy.com, Inc.	US	947,456
▼38	117.3	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	37,632
▼39	115.8	31252	STARNET-AS StarNet Moldova	MD	109,056
▲40	113.6	16265	LEASEWEB LEASEWEB AS	NL	245,760
▼41	113.5	27715	LocaWeb Ltda	BR	58,880
▼42	112.9	36057	WEBAIR-AMS Webair Internet Development Inc	US	28,672
▲43	112.7	46844	ST-BGP - SHARKTECH INTERNET SERVICES	US	75,520
▲44	112.3	6877	AS6877 Utel Mobile Internet Service ASN	US	344,064
▼45	111.7	24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	1,682,688
▲46	111.4	9198	KAZTELECOM-AS JSC Kazakhtelecom	KZ	1,820,672
▲47	110.9	35908	VPLSNET - VPLS Inc. d	US	628,992
▲48	108.8	24965	SPOINT-AS S.Point LTD	US	1,024
▲49	108.2	6939	HURRICANE - Hurricane Electric, Inc.	US	582,144
▲50	107.7	42560	BA-GLOBALNET-AS GlobalNET Bosnia	BA	32,768

2010 Q3 to Q4 Comparison



A comparison of the 'Top 50 Bad Hosts' in September 2010 with December 2010 shows a fairly consistent level of effective badness

4.

What's New?

4.1. Worst Hosts by Sector

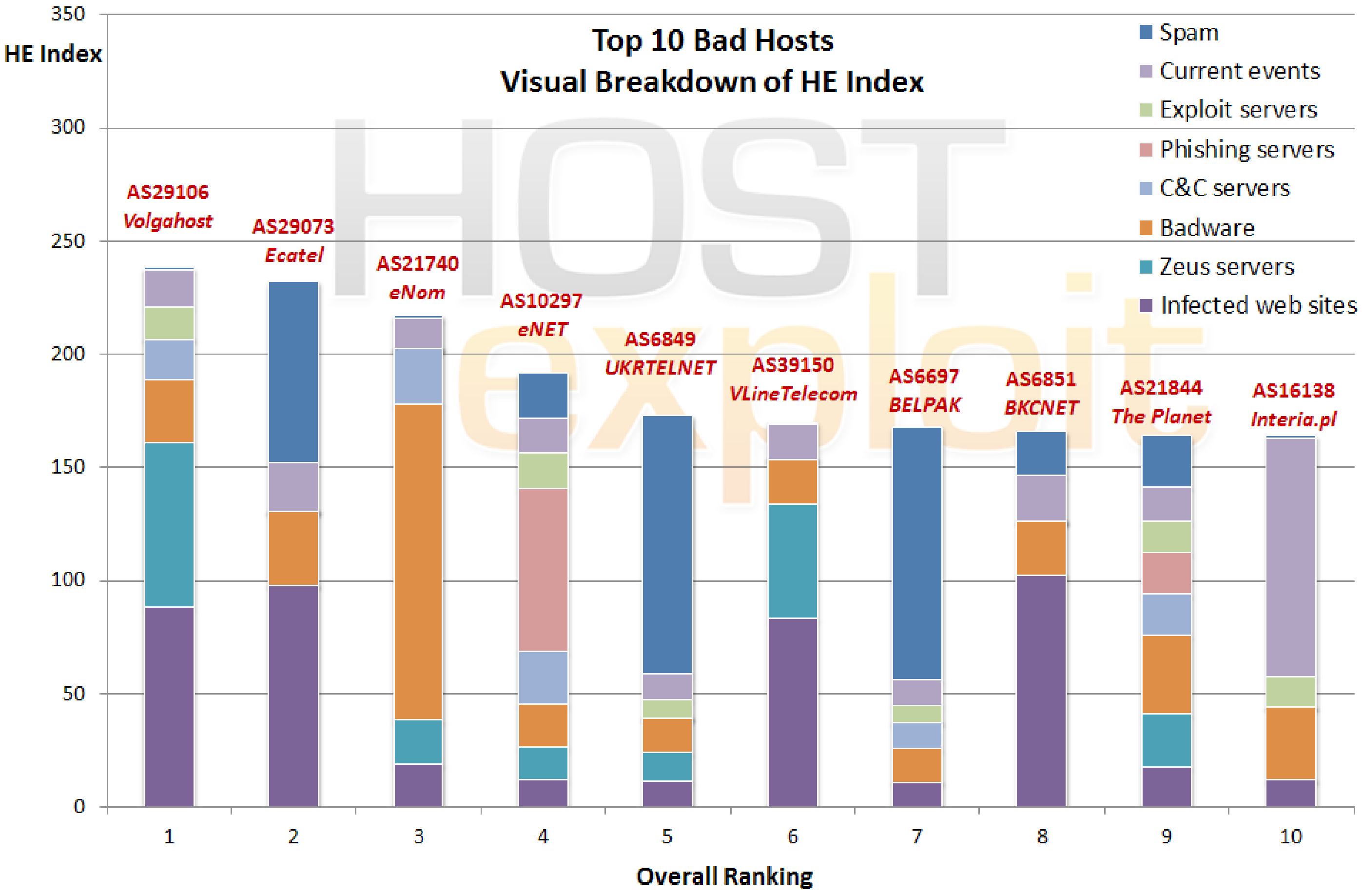
	Previous Quarter - Q3 2010			Current Quarter - Q4 2010		
	ASN	**Name**	**Country**	**ASN**	**Name**	**Country**
#1	**29073**	ECATEL-AS	NL	**29106**	VOLGAHOST-AS	RU
#2	**39150**	VLTELECOM-AS VLineTelecom	RU	**29073**	ECATEL-AS	NL
#3	**29106**	VOLGAHOST-AS	RU	**21740**	eNom / DemandMedia	US
#1 for Spam	**44237**	CTC-CORE	RU	**31133**	MF-MGSM-AS OJSC MegaFon	RU
#1 for Botnets	**36057**	Webair	US	**36408**	CDNETWORKS-GLOBAL	US
#1 for Zeus Botnet	**50134**	Softel Consulting	CZ	**20564**	INFORMEX-MNT Informex	UA
#1 for Phishing	**13301**	UNITEDCOLO-AS	DE	**10297**	ENET-2 - eNET Inc.	US
#1 for Exploit Servers	**13100**	Data Electronics Group	IE	**13100**	Data Electronics Group	IE
#1 for Badware	**21740**	eNom / DemandMedia	US	**21740**	eNom / DemandMedia	US
#1 for Infected Sites	**29073**	ECATEL-AS	NL	**6851**	BKCNET "SIA" IZZI	LV
#1 for Current Events	**16138**	INTERIAPL INTERIA.PL	PL	**16138**	INTERIAPL INTERIA.PL	PL

4.2. Top 10 Newly-registered Hosts - In 4th Quarter 2010

HE Rank	HE Index	AS number	AS name	Country	# of IPs
31	**125.65**	**20564**	INFORMEX-MNT Informex, E-commerce Service Provider	UA	256
83	**94.29**	**51554**	LYAHOV-AS Lyahovich Maksim	RU	256
263	**69.00**	**42872**	GENERALSERVICE-AS General Service LLC	RU	1,024
710	**49.61**	**49536**	DENTA-AS DENTAGLOBAL SYS	CZ	512
994	**41.95**	**51559**	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd.	TR	12,288
1,038	**40.95**	**49873**	TELECOMPO-AS "Telecompo" Ltd.	AG	512
1,298	**36.36**	**51699**	ANTARKTIDA-PLUS-AS Antarktida-Plus LLC	RU	256
1,508	**32.54**	**45349**	TFL-AS-AP Telecom Fiji Ltd	FJ	21,760
1,755	**28.88**	**42533**	DELFANET-AS Delfa Network AS	DK	256
1,959	**26.61**	**51765**	EUHOST-AS Oy Crea Nova Russia LTD	FI	512

Note: by end Q4 2010 there are **36,371 ASes** (hosts) an increase of **858** from end Q3 2010

Top 10 Visual Breakdown



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

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

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

For instance, it can be seen that **AS29106 VolgaHost (RU) is ranked #1** due mainly to its exceptionally high concentrations of infected web sites and spam servers, as well as smaller concentrations or Zeus servers, badware and phishing servers.

AS39150 VLineTelecom (RU), a new entry to the Top 10.

Further, we can see that **AS21740 eNom / Demand Media (US)**, ranked #7 for the previous quarter, has worsened to #3, including Zeus hosting.

6.

Country Analysis

Hosts in Top 50	Country	Total IPs within Top 50	Total Index	Average Index	Average Indexes by Category							
					Infected web sites	Zeus servers	Badware	C&C servers	Phishing servers	Exploit servers	Current events	Spam
21	UNITED STATES	6,075,648	2,817.3	134.2	189.4	103.1	190.5	176.4	168.9	159.6	133.9	56.4
5	RUSSIA	34,560	814.2	162.8	416.7	422.9	103.7	32.7	0.2	126.7	105.9	113.4
3	GERMANY	912,896	400.7	133.6	224.9	42.3	147.6	140.7	225.2	181.5	120.3	88.3
2	NETHERLANDS	258,816	346.1	173.1	506.1	59.4	182.5	79.9	0.1	67.7	159.4	199.0
2	UKRAINE	1,120,000	298.8	149.4	117.8	550.9	51.7	0.2	0.1	57.2	50.5	222.1
2	LATVIA	49,408	289.8	144.9	707.1	105.6	166.6	0.2	0.2	0.4	173.8	40.7
2	FRANCE	419,584	282.3	141.2	136.7	97.5	270.9	206.7	136.8	201.0	115.0	54.9
2	CHINA	106,121,216	269.8	134.9	197.9	77.9	359.2	100.5	66.2	100.7	104.7	61.3
2	BRAZIL	76,288	247.4	123.7	107.2	0.1	120.8	363.8	278.2	163.6	106.5	34.3
2	INDIA	6,534,912	237.5	118.7	100.2	0.0	100.1	0.0	0.0	0.0	100.0	315.0
1	BELARUS	746,240	168.2	168.2	100.2	0.0	100.6	102.9	0.0	104.2	100.1	431.5
1	POLAND	3,072	164.1	164.1	107.2	0.1	217.6	0.3	0.3	182.3	949.5	3.2
1	CANADA	218,112	132.3	132.3	115.5	119.6	124.6	152.0	266.3	205.3	112.4	90.4
1	CZECH REPUBLIC	34,048	131.5	131.5	105.0	0.0	273.9	0.1	526.7	244.0	116.4	35.6
1	MOLDOVA REP	109,056	115.8	115.8	341.5	180.5	131.1	0.1	0.0	0.1	133.5	90.7
1	KAZAKHSTAN	1,820,672	111.4	111.4	100.2	124.4	100.2	0.0	0.0	0.0	100.1	233.1
1	BOSNIA AND HZ	32,768	107.7	107.7	419.7	248.5	112.6	0.1	0.1	0.2	117.9	14.1

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
34,206	0.60	38333	SYMBIO-AS-AU-AP Symbio Networks	AU	131,936
34,153	0.62	23329	AS-OPENACCESS - Open Access Inc.	US	112,384
33,674	0.73	11333	CYBERTRAILS - Cyber Trails	US	65,792
33,641	0.73	37028	FNBCONNECT	ZA	65,536
32,266	0.85	8844	COMMUNITY CI-Net Limited AS	UK	41,472
31,084	0.99	4764	WIDEBAND-AS-AU Wideband Networks Pty Ltd, Transit AS	AU	186,624
29,860	1.01	29384	Qatar Foundation for Education, Science and Community Development	QA	155,136
28,947	1.07	9797	ASIAONLINEAUS-AS-AP Nexon Asia Pacific	AU	110,592
26,829	1.12	33502	VRCT-AUR - SunGard VeriCenter Inc	US	18,176
25,721	1.13	35467	DCF-AS DataCenter Fryslan AS	NL	81,152

7.1. 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 several 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.

That is why we have created a table of 'good hosts' and would like to commend those companies on their effective abuse controls and management.

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

7.2. Selection Criteria

For the good host selection we apply 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.

Most Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-99.1%	29	135.63	27,204	1.16	44237	CTC-CORE-AS ... Telecommunication Company	RU	1792
-60.3%	4	181.96	187	72.19	10292	CWJAM ASN-CWJAMAICA	JM	79104
-58.2%	628	52.01	2,482	21.74	21220	TELEMOBIL Telemobil S.A.	RO	66816
-57.4%	28	136.39	488	58.15	50134	SOFTEL Softel Consulting s.r.o.	CZ	256
-52.7%	21	145.71	234	68.96	27716	Advanced Communication Network, S.A.	PA	22272
-47.1%	17	147.39	140	77.94	14141	WIRESIX - WireSix, Inc.	US	7424
-46.5%	154	78.86	990	42.21	33494	IHNET - IH Networks	US	15104
-45.8%	16	148.68	124	80.62	11305	P1DH-1-ASN - Peer 1 Dedicated Hosting	US	794624
-45.7%	24	139.51	161	75.68	45271	ICLNET-AS-AP 5th Floor, Windsor Building...	IN	185856
-43.4%	234	69.83	1127	39.55	29182	ISPSYSTEM-AS ISPsystem Autonomous System	RU	41984

Many forms of badware can be inextricably linked, appearing as an intractable issue to some hosts. However, we applaud the efforts of the ASes in the above table - all have dramatically reduced their badness levels in the three months since our 3rd quarter report was published.

The most dramatic example is AS44237 CTC-Core (Ru) which showed a 99% drop in badness hosted and served, from a ranking of #29 to #27,204. Similarly, AS10292 CWJAM has moved from #4 in Q3 2010 to #187.

AS28299 CYBERWEB NETWORKS (BR) serves as a good example of the need for constant awareness: having been lauded in the last report for the significant improvement made from 2010 Q2 to Q3, dropping from rank #9 to #228, some of the malicious activity has now resurfaced and it is back up to #21.

Bad Hosts by Topic

9.1. Infected Web Sites

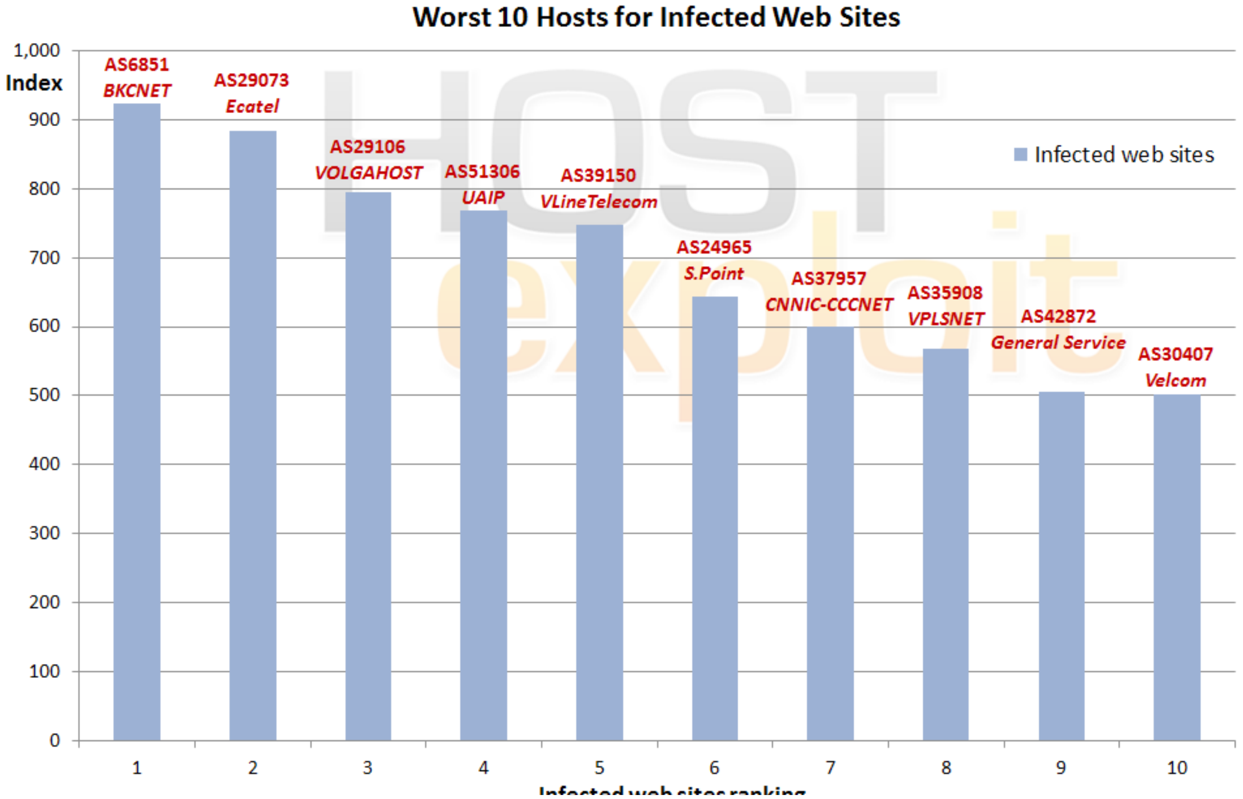
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
8	166.2	**6851**	BKCNET "SIA" IZZI	LV	49,152	**923.2**
2	232.5	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	13,056	**883.2**
1	238.3	**29106**	VOLGAHOST-AS PE Bondarenko Dmitriy Vladimirovich	RU	256	**794.8**
56	104.7	**51306**	UAIP-AS PAN-SAM Ltd.	UA	2,048	**768.3**
6	170.2	**39150**	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	RU	5,888	**748.4**
48	108.8	**24965**	SPOINT-AS S.Point LTD	US	1,024	**643.5**
113	86.0	**37957**	CNNIC-CCCNET China Communication Co., Ltd	CN	4,096	**599.6**
47	110.9	**35908**	VPLSNET - VPLS Inc. d	US	628,992	**567.2**
263	69.0	**42872**	GENERALSERVICE-AS General Service LLC	RU	1,024	**505.5**
108	86.7	**30407**	VELCOM - Rcp.net	CA	10,240	**502.2**

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

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

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

Major countries are 3 Russian and 2 US AS's in this Top 10.



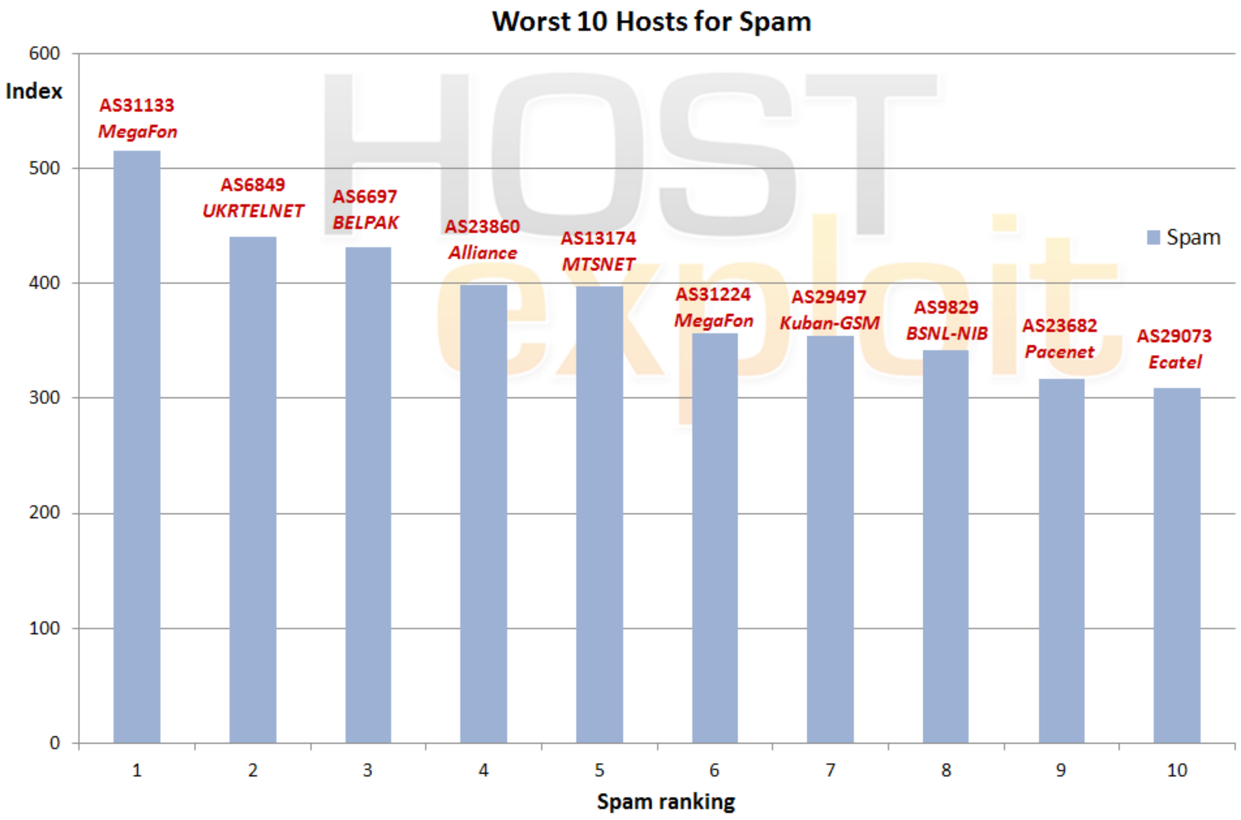
9.2. Spam

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
22	133.7	**31133**	MF-MGSM-AS OJSC MegaFon Network	RU	14,080	**515.2**
5	173.2	**6849**	UKRTELNET JSC UKRTELECOM,	UA	1,119,744	**440.5**
7	168.2	**6697**	BELPAK-AS BELPAK	BY	746,240	**431.5**
53	105.5	**23860**	ALLIANCE-GATEWAY-AS-AP Alliance Broadband Services Pvt. Ltd	IN	16,384	**398.3**
51	105.9	**13174**	MTSNET OJSC "Mobile TeleSystems" Autonomous System	DZ	24,064	**397.1**
87	92.6	**31224**	MF-UGSM-AS OJSC MegaFon Network	IN	3,072	**356.5**
89	92.0	**29497**	KUBANGSM CJSC Kuban-GSM	RU	20,224	**354.3**
30	125.8	**9829**	BSNL-NIB National Internet Backbone	IN	4,852,224	**342.2**
131	82.4	**23682**	PACENET-AS Broadband Pacenet India Limited	PH	27,904	**317.3**
2	232.5	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	13,056	**309.0**

Our Top 10 spam results again indicate that spammers tend to prefer servers located in countries where regulation and monitoring are minimal. Spammers make use of fast-flux servers and disposable crime servers, making ownership difficult to quantify. Spammers use tried and tested methods, and are quick to adapt to current media themes without needing new innovations unlike other areas of cybercriminal activity.

The damage caused by a single spammer can be as great or sometimes greater than a group and is, therefore, a difficult category to measure. For this reason, we used a combination of routing prefixes from respected sources as SpamHaus, UCEPROTECT-Network, spam server information from academic researchers at Malicious Networks (FiRE) and community spam bot data from SudoSecure to provide a wide spread of spam instances. The result is a definitive and current list of spam servers in the world, i.e. those hosting the IP space sending the spam.

Of note is India with 3 entries within the spam Top 10.



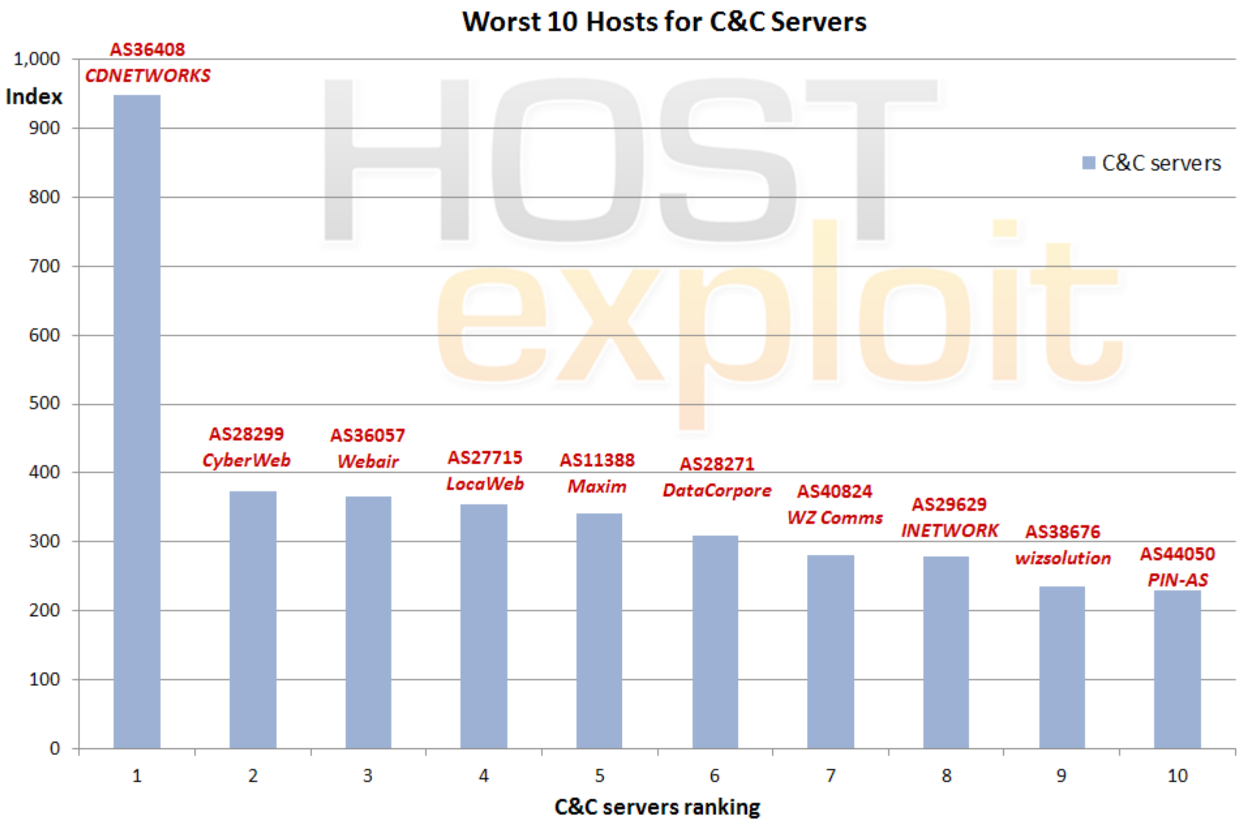
9.3. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
14	147.4	**36408**	CDNETWORKS-GLOBAL unified ASN for CDNetworks...	US	35,328	**948.0**
21	133.9	**28299**	CYBERWEB NETWORKS LTDA	BR	17,408	**373.8**
42	112.9	**36057**	WEBAIR-AMS Webair Internet Development Inc	US	28,672	**366.1**
41	113.5	**27715**	LocaWeb Ltda	BR	58,880	**353.9**
68	98.6	**11388**	MAXIM - Peer 1 Dedicated Hosting	US	135,168	**340.7**
169	78.2	**28271**	DataCorpore ServiÃ§os e RepresentaÃ§Ãµes	BR	10,240	**310.2**
85	93.7	**40824**	WZCOM-US - WZ Communications Inc.	US	7,936	**281.6**
23	133.3	**29629**	INETWORK-AS IEUROP AS	FR	8,192	**280.0**
659	51.2	**38676**	AS33005-AS-KR wizsolution co.,Ltd	KR	7,936	**236.3**
201	74.4	**44050**	PIN-AS Petersburg Internet Network LLC	RU	40,960	**229.1**

The trend continues from earlier reports with the appearance of Botnet C&C Servers migrating towards larger hosts.

Our own data is combined primarily with data provided by Shadowserver.

Here the US leads the table with 4 of the Botnet Top 10 positions, followed next by Brazil with 3



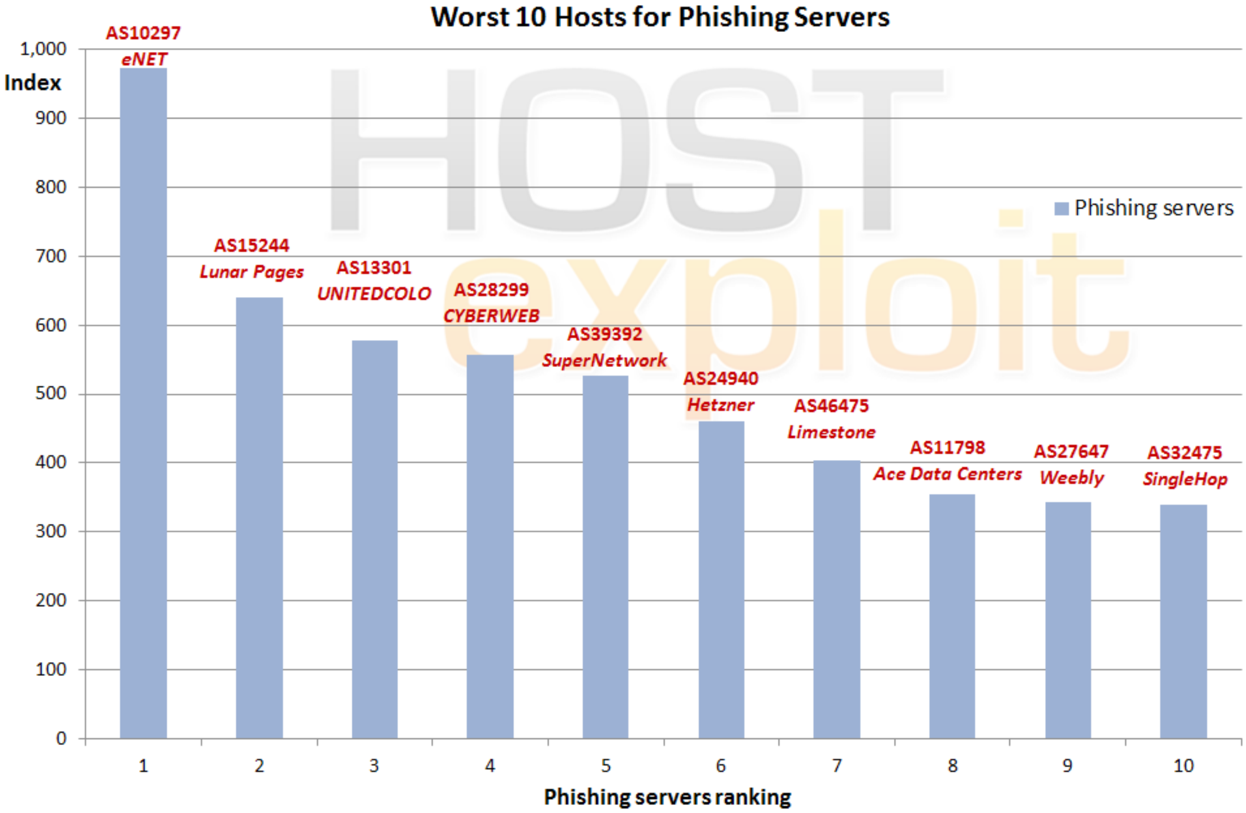
9.4. Phishing

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
4	192.1	**10297**	ENET-2 - eNET Inc.	US	90,368	**972.7**
11	149.8	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	44,544	**640.3**
55	104.8	**13301**	UNITEDCOLO-AS Autonomous System of unitedcolo.de	DE	66,816	**576.8**
21	133.9	**28299**	CYBERWEB NETWORKS LTDA	BR	17,408	**556.3**
26	131.5	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	CZ	34,048	**526.7**
18	138.3	**24940**	HETZNER-AS Hetzner Online AG RZ	DE	445,440	**460.8**
17	143.5	**46475**	LIMESTONENETWORKS - Limestone Networks, Inc.	US	57,344	**403.6**
34	120.0	**11798**	ACEDATACENTERS-AS-1 - Ace Data Centers, Inc.	US	99,328	**354.0**
295	67.2	**27647**	WEEBLY - Weebly, Inc.	US	3,072	**344.0**
19	137.4	**32475**	SINGLEHOP-INC - SingleHop	US	197,632	**339.2**

Phishing continues to be a cause for concern to banks and large corporations alike. The need to establish false credibility explains the dominance of Western countries in the Top 10 list for phishing. In fact our results show that 6 of the top 10 phishing hosts are based in the US and 2 in Germany.

The necessary malware can reside on the enterprise's web site, or appears via cross-site scripting or header redirects.

It would appear Malware located on a server in western countries minimizes the awareness of both customers and target organizational awareness.



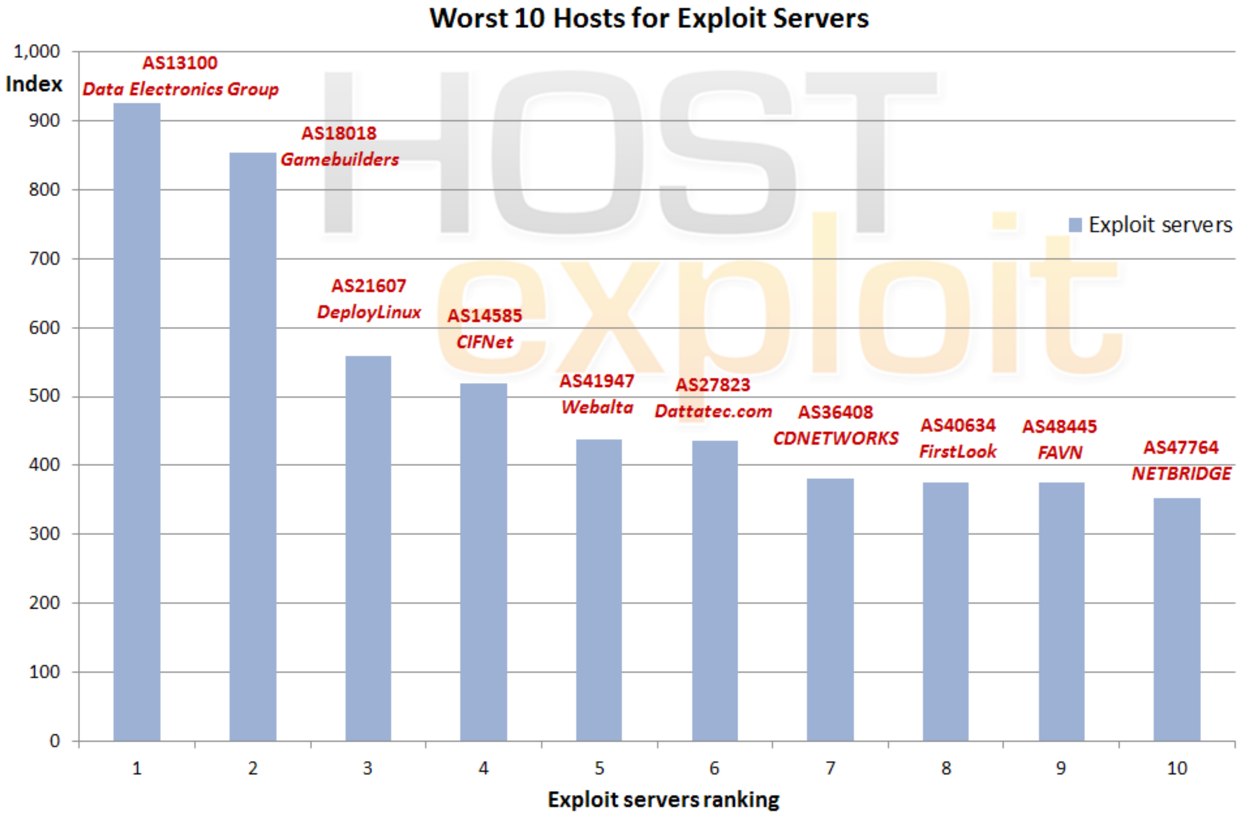
9.5. Exploit Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
78	95.4	**13100**	Data Electronics Group, Data Exchange Centre	IE	12,288	**925.5**
262	69.1	**18018**	GAMEBUILDERS-AS-PH Gamebuilders Inc.	PH	7,680	**853.3**
146	80.7	**21607**	DEPLOYLINUX - DeployLinux Consulting, Inc	US	512	**559.2**
282	67.7	**14585**	CIFNET - CIFNet, Inc.	US	7,168	**518.7**
29	128.1	**41947**	WEBALTA-AS OAO Webalta	RU	13,824	**438.4**
69	97.9	**27823**	Dattatec.com	US	8,192	**436.6**
14	147.4	**36408**	ASN-PANTHER Panther Express	US	35,328	**381.4**
65	99.3	**40634**	FIRSTLOOK-COM - FirstLook, Inc.	US	512	**375.8**
278	68.0	**48445**	FAVN Favorit Network SL	ES	512	**375.8**
898	44.3	**47764**	NETBRIDGE-AS Limited liability company Mail.Ru	US	25,984	**351.8**

It is important to note that "Exploit Servers" is possibly the most important category, to be found in this report, in the analysis of malware, phishing, or badness as a whole . Added weighting was given to this sector.

Many hosts or commercial internet servers that deliver malware or undertake other malicious activity do so because they have been hacked and compromised. Useful information, victim identities and other illicitly gained booty are then directed back to these Exploit Servers using malware.

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



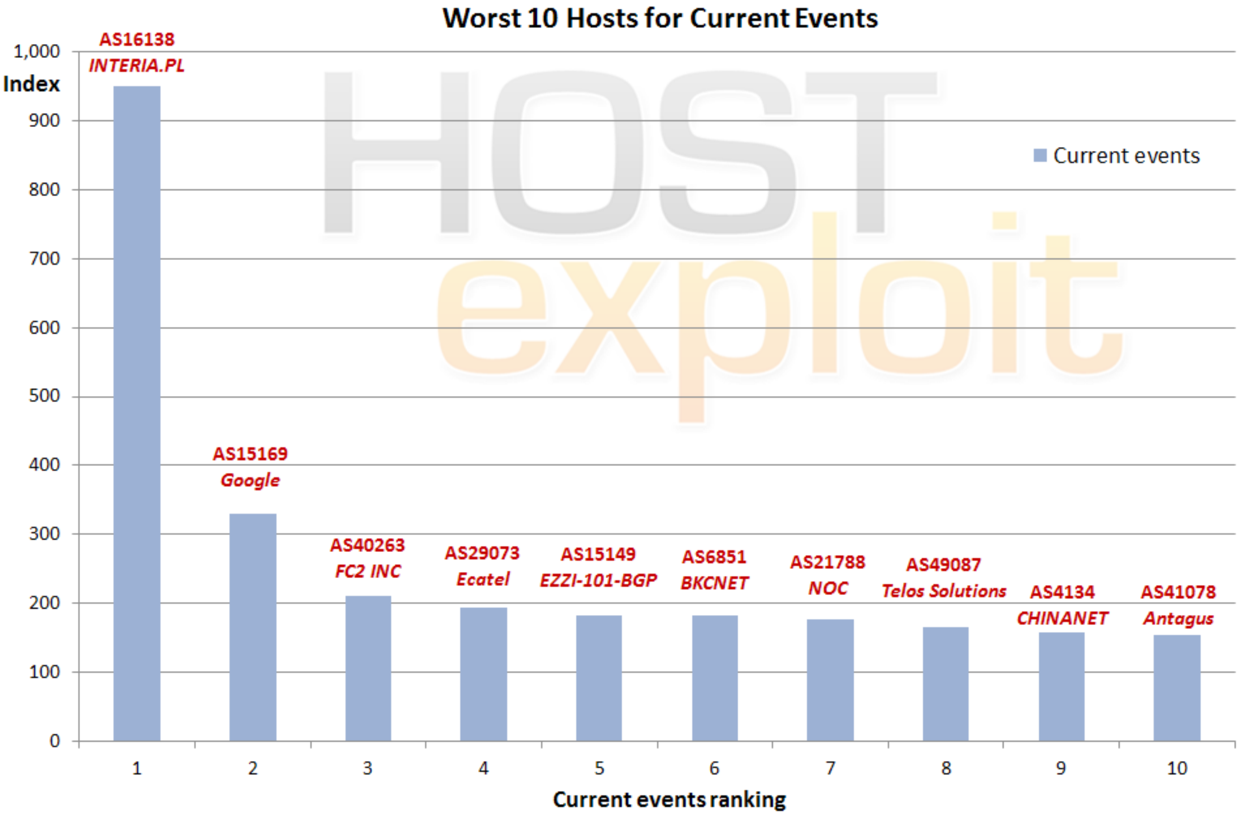
9.6. Current Events

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
10	164.1	**16138**	INTERIAPL INTERIA.PL Autonomous System	PL	3,072	**949.5**
28	129.8	**15169**	GOOGLE - Google Inc.	US	265,984	**330.5**
639	52.1	**40263**	FC2-INC - FC2 INC	US	1,024	**211.2**
2	232.5	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	13,056	**194.6**
334	64.6	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	US	28,672	**182.9**
8	166.2	**6851**	BKCNET "SIA" IZZI	LV	49,152	**182.2**
24	132.5	**21788**	NOC - Network Operations Center Inc.	US	278,528	**177.1**
32	123.7	**49087**	TELOS-SOLUTIONS-AS Telos Solutions LTD	LV	256	**165.3**
13	148.9	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	CN	106,110,208	**157.7**
150	80.4	**41078**	ANTAGUS-AS 1st Antagus Internet GmbH	DE	6,144	**154.9**

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

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

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



9.7. Botnet Hosting - Zeus

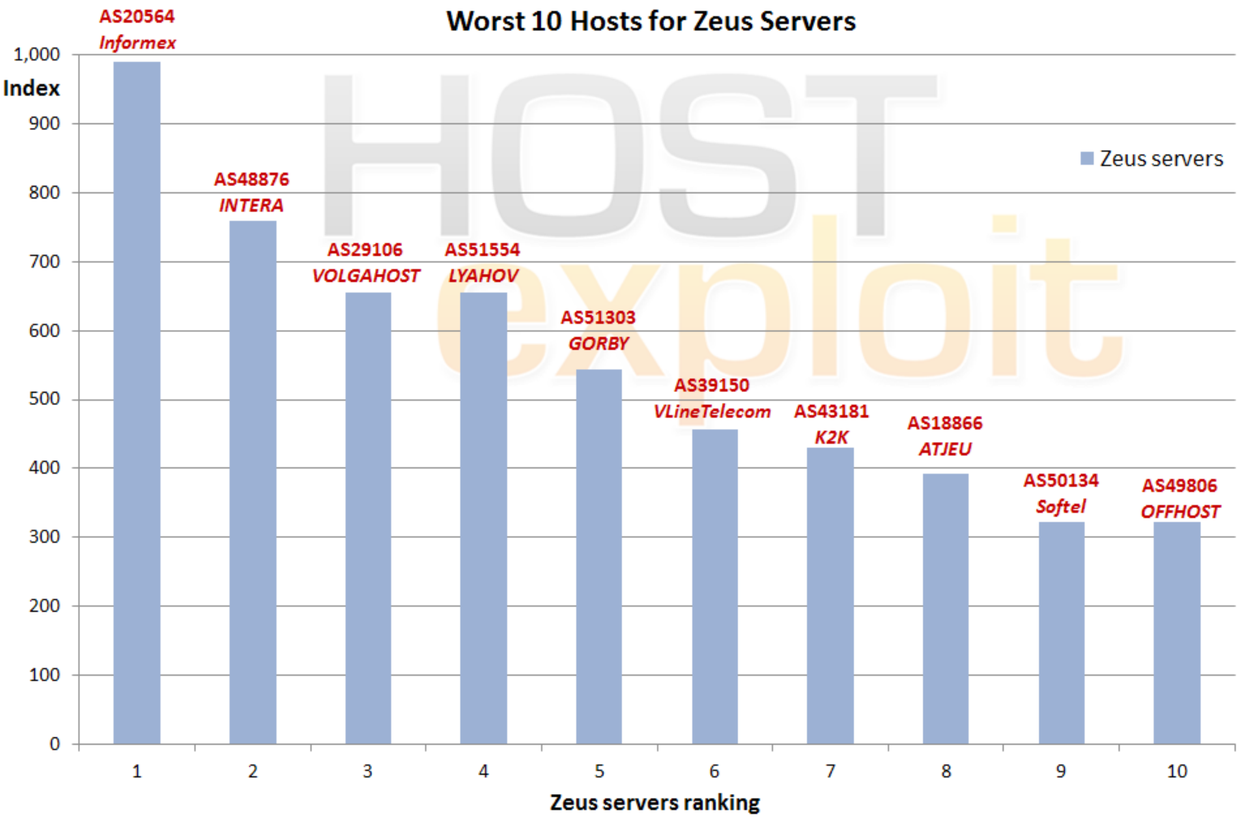
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
31	125.6	**20564**	INFORMEX-MNT Informex, E-commerce Service Provider	UA	256	**988.9**
16	143.9	**48876**	INTERA-AS Takomi Ltd	RU	512	**759.2**
1	238.3	**29106**	VOLGAHOST-AS PE Bondarenko Dmitriy Vladimirovich	RU	256	**655.6**
83	94.3	**51554**	LYAHOV-AS Lyahovich Maksim	UA	256	**655.6**
110	86.0	**51303**	GORBY-AS Alexandr Gorbunov	CZ	256	**544.5**
6	170.2	**39150**	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	RU	5,888	**457.5**
124	83.9	**43181**	K2K-AS Contel 2000 Ltd.	NL	512	**429.7**
20	134.1	**18866**	ATJEU - Atjeu Publishing LLC	US	12,800	**391.5**
170	77.9	**50134**	SOFTEL Softel Consulting s.r.o.	CZ	256	**322.3**
171	77.8	**49806**	OFFHOST-AS Offshore hosting LTD	MD	256	**322.3**

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

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

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

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

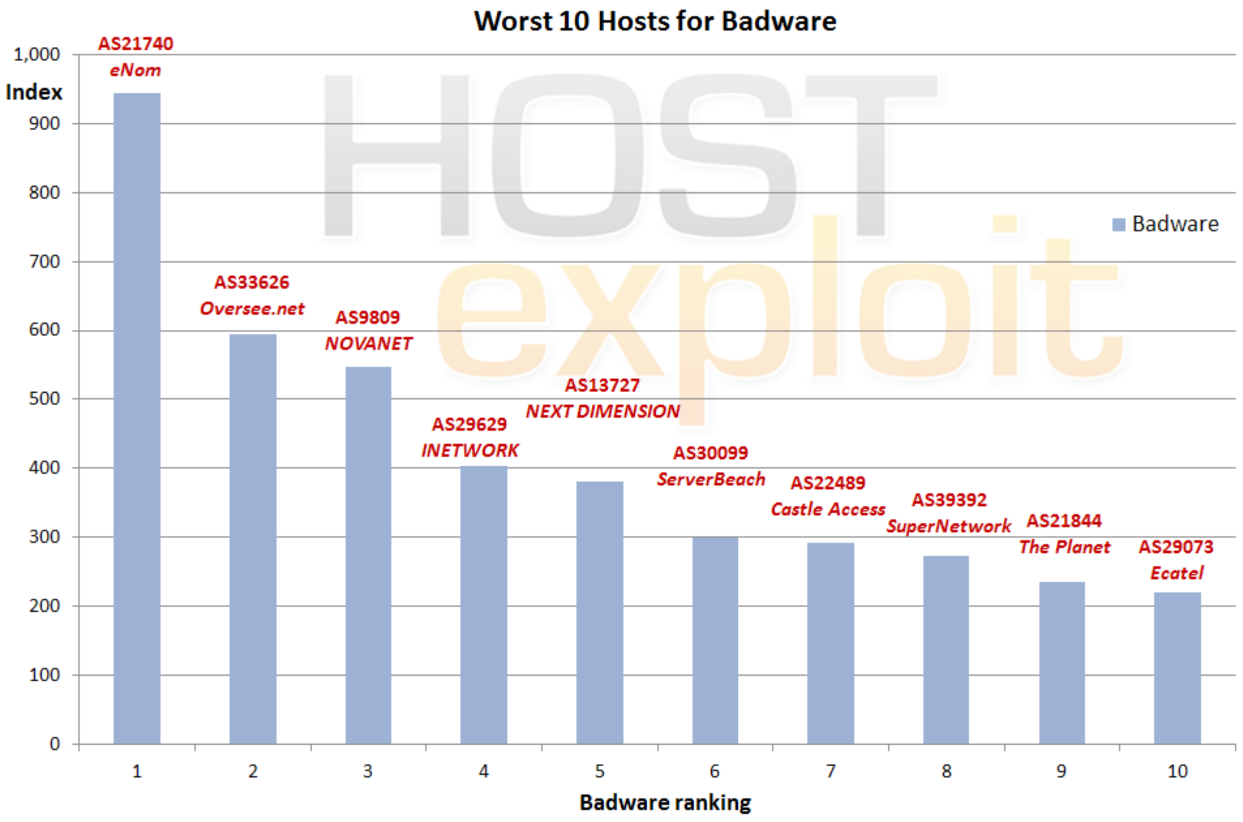


9.8. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
3	217.4	**21740**	ENOMAS1 - eNom, Incorporated	US	12,288	**944.4**
36	117.4	**33626**	OVERSEE-DOT-NET - Oversee.net	US	4,096	**594.0**
33	121.0	**9809**	NOVANET Nova Network Co.Ltd... Shenzhen, China	CN	11,008	**547.8**
23	133.3	**29629**	INETWORK-AS IEUROP AS	FR	8,192	**402.7**
98	88.9	**13727**	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024	**381.5**
94	90.6	**30099**	SB-2 - ServerBeach	US	24,576	**298.9**
326	65.1	**22489**	CASTLE-ACCESS - Castle Access Inc	US	45,824	**291.8**
26	131.5	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	CZ	34,048	**273.9**
9	164.1	**21844**	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,673,728	**234.3**
2	232.5	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	13,056	**219.9**

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

Again it is of concern to see 50% of these are based in US. The findings in this category are primarily based on StopBadware's data, which is itself aggregated from Google, Sunbelt Software, and Team Cymru.



10.

Crime Servers

10.1. Background - What Are Crime Servers?

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

Examples of large versions of these have been seen over recent times and shown within earlier HostExploit reports i.e. Atrivo (US), McColo (US), Real Host (Latvia). Also more recently in the example of Troyak.

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

10.2. Crime Servers or Bad Hosts?

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

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

10.2. Crime Servers - Currently Inactive (Not Announced)

AS number	Name	IPs	HE Rank
12604	CITYGAME-AS Kamushnoy Vladimir Vasulyovich	256	N/A
29371	GAZTRANZITSTROYINFO-AS LLC "Gaztransitstroyinfo"	256	N/A
42229	MARIAM-AS PP Mariam	1,024	N/A
44107	PROMBUDDETAL-AS Prombuddetal LLC	1,024	N/A
47560	VESTEH-NET-AS Vesteh LLC	1,024	N/A
47821	BOGONET-AS PE Syrovatko Igor Mykolayevish	256	N/A
49091	INTERFORUM-AS Interforum LTD	256	N/A
49093	BIGNESS-GROUP-AS Bigness Group Ltd.	512	N/A
49934	VVPN-AS PE Voronov Evgen Sergiyovich	256	N/A
50033	GROUP3-AS GROUP 3 LLC.	256	N/A
50215	TROYAK-AS Starchenko Roman Fedorovich	256	N/A
50369	VISHCLUB-AS Kanyovskiy Andriy Yuriyovich	1,024	N/A
50390	SMILA-AS Pavlenko Tetyana Oleksandrivna	256	N/A
50678	SAINTVPN	256	N/A

10.3. Crime Servers - Examples Currently Active - 12/2010

AS number	Name	IPs	HE Rank
29106	VOLGAHOST-AS PE Bondarenko Dmitriy Vladimirovich	256	1
20564	INFORMEX-MNT Informex, E-commerce Service Provider	256	31
51554	LYAHOV-AS Lyahovich Maksim	256	83
49314	NEVAL PE Nevedomskiy Alexey Alexeevich	256	102

Conclusions

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

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

• Such a report and the defined "HE Index" acts as a consumer barometer for each of the **36,371** currently advertised and commercial ASes.

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

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

• The findings from this report will reinforce the need to demonstrate willingness to 'clean up' systems when bad publicity is seen as harmful to business. The biggest success to date is illustrated by AS30407 Velcom (Canada), which was ranked as the #1 Bad Host in December 2009 report, and has dramatically reduced its badness levels by over 70 per cent over a 12 month period. It is encouraging to see a willingness to begin the process of 'cleaning up' known abuses but as the new report shows there is still much work to be done.

• At ranking #1, **AS29106 VolgaHost (RU)**, which has been in the top 5 throughout 2010, should be classified and termed as a crime server.

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

Action planning for hosts, telecoms and ISPs:

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

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

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

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

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

Appendix 1.

Glossary

AS (Autonomous System):

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

Badware:

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

Blacklists:

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

Botnet:

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

CSRF (cross site request forgery):

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

DNS (Domain Name System):

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

DNSBL:

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

Exploit:

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

Hosting:

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

IANA (Internet Assigned Numbers Authority)

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

ICANN (Internet Corporation for Assigned Names and Numbers)

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

IP (Internet Protocol):

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

IPv4

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

IPv6

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

ISP (internet Service Provider):

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

LFI (Local File Inclusion):

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

MALfi (Malicious File Inclusion):

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

Malicious Links:

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

MX:

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

NS (Name Server):

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

Open Source Security:

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

Pharming:

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

Phishing:

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

Registry:

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

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 4, 2010

1 Revision history

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

Table 1: Revision history

2 Motivation

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

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

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

3 Data sources

Data is taken from the following 11 sources.

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

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

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

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

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

Table 2: Data sources

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

4 Bayesian weighting

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

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

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

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

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

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

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

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

5 Calculation

For each data source, three factors are calculated.

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

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

where:
B$_m$: *maximum Bayesian ratio*

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

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

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

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

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

where:
N$_m$: *maximum number of instances in sample set*

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

The index for each data source is then calculated as:

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

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

The overall HE Index is then calculated as:

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

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

HostExploit - Top 50 Bad Hosts and Networks

4th Quarter 2010