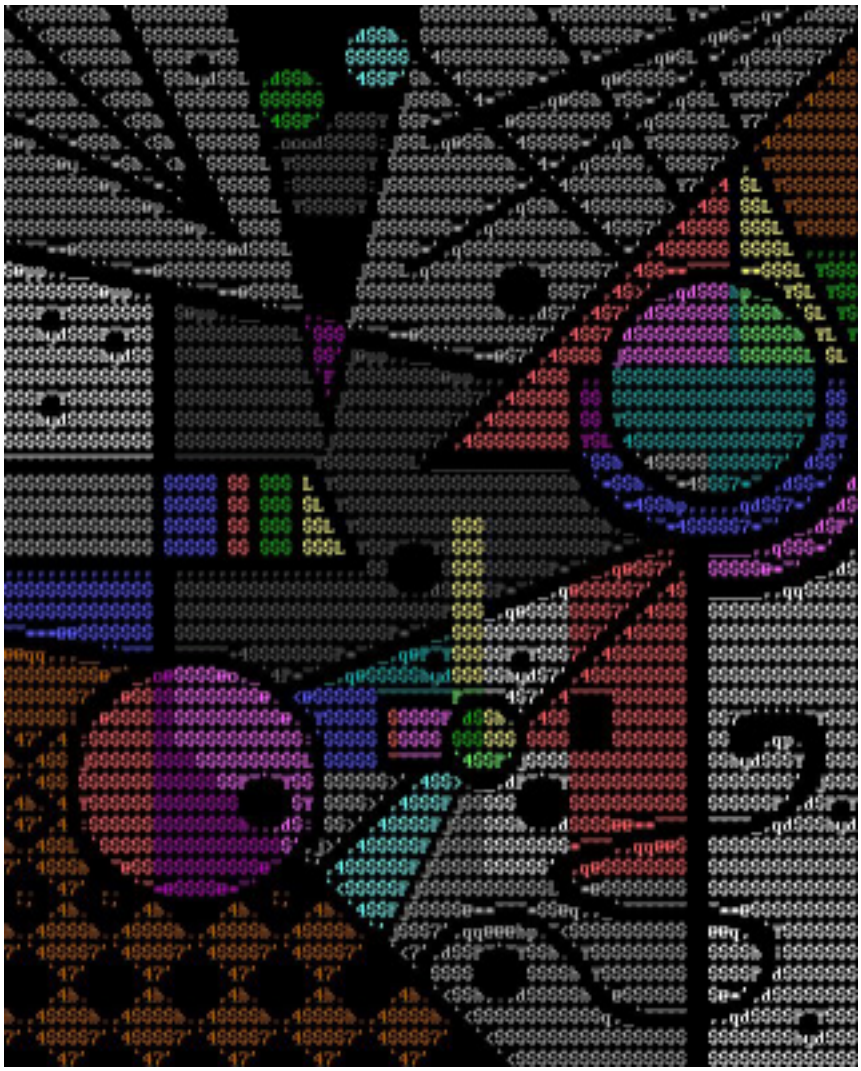
HostExploit's Worldwide Cybercrime Series

Top 50 Bad Hosts and Networks
3rd Quarter 2011 - Report



SITEVET HOST exploit GROUP IB

Table of Contents

Top 50

CyberCrime Series

Bad Hosts and Networks

Supported by

nominet trust

www.nominettrust.org.uk

Edited by

- Jart Armin

Review

- Dr. Bob Bruen
- Raoul Chiesa
- Ilya Sachkov
- Alexander Pisemskiy

Contributors

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

Comparative Data

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

Front page illustration: Juio Sepia - Kandinskii - ASCII art - http://www.juliosepia.com/2010/portafolio/kandinskii/lang/en

Bad Hosts and Networks

DigiNotar and CA Security

As more fascinating details surrounding the major hack of Dutch Web security certificate issuer DigiNotar emerge, the overall consensus is that this was primarily about mass interception of digital communications in Iran, although some recent evidence seems to contradict this view.

This story continues to unfold to reveal an all-too-familiar tale of a slow initial response to what is now obviously a very serious hacker attack and breach. Perhaps "floundering in the dark" is too strong a statement for how DigiNotar dealt with this hack, but at best the incident again exposes the weakness of the CA (certificate authority) technique. At worst, it leaves the issue of dependency on CA and third-party trust in tatters.

Most news stories so far have focused on the issuance of a fake Google certificate for accessing Gmail, but there were 531 fraudulent certificates generated by the hackers, as shown in the Dutch government sponsored and rapidly issued interim report on the incident. Also of note are fraudulent certificates for the following online entities: URLs with .com or .org; Microsoft and Mozilla browsers; Twitter, Wordpress, Equifax, and Torproject (for Tor anonymous browsing nodes); Android apps; Facebook; and -- of special governmental interest -- CIA.gov and sis.gov.uk (MI6).

Fox-IT, a Dutch security company eventually hired by the Dutch government to help draft the interim report, stated that after the hack, 300,000 unique requesting IPs to Google.com were detected (using the fake Google certificate). The certificate was from inside Iran. And around one percent of the requests were from proxy Tor nodes outside of Iran. The report claims that the objective may been to intercept private communications of Internet users in Iran.

The certificate-issuing company DigiNotar BV was bought by Vasco Data Security International Inc. for $12.9 million in January 2011. The hack commenced June 6, 2011, if not before, with the breach not detected until June 19. DigiNotar BV provides digital certificate services, including default SSL Secure Sockets Layer (SSL), qualified certificates, and Dutch government certificates, to a number of CAs.

The hacker(s) gave an altogether different account and appear to be offering advice to Anonymous and LulzSec. The slightly cheery intro to the apparent hacker's message left on PasteBin -- "Hi again! I strike back again, huh?" -- belies the apparent and chilling reason behind this hack. Claimed by ICHSUN (@ICHSUN2 on Twitter), the Comodo hacker from March 2011, the hacker declares it to be a revenge attack for the Dutch government's exchange of Muslim soldiers who were subsequently slaughtered by Serbian rebels during atrocities in the country 16 years ago.

Fox-IT confirms the fingerprints deliberately left on a script are the same used in the Comodo hack by ICHSUN back in March when fake certificates were similarly generated. Other identifying marks had been deleted. The skill of the hacker(s) is assessed as being "amateurish" in parts and "very advanced" in others.

There are perhaps three possibilities related to the DigiNotar attack:

- The lone hacker ICHSUN's account of proceedings does appear to be genuine, as he/she does provide authentic DigiNotar administrative logins and describes the self-taught use of XUDA (Xcert Universal Database API), a software library that is used and incorporated in many CA products from different vendors, such as RSA Security Inc. (Nasdaq: EMC).
- The introduction of the fraudulent Google certificate only in Iran's proxy servers suggests possible interception of encrypted emails by Iranian authorities.
- Of course, this could be another Stuxnet-like "digital black op" against Iran, meant to provide digital confusion. It is interesting to note that Stuxnet also utilized fraudulent certificates against Iran.

Whatever the case, it is clear that an alternative to CA is urgently needed, as "trusted" certificates do not live up to their implied description. As Rik Ferguson of Trend Micro puts it: "Does this event undermine the foundations of trusted communication online? Not entirely, although it certainly highlights a weak link in the chain."

However, this hack, Stuxnet, and similar hacks all provide a blueprint for further trusted third-party attacks and fraudulent certification. The whole community needs to seek a new and more secure solution for data encryption and certification.

Shady Rat Findings

- **Confirmation via the logs of the duration of intrusion.** In reviewing similar log files, we often see similar intrusions ongoing for months or even years, despite some experts hotly arguing that no hackers could be in a victim's servers that long. In the case of Shady RAT and the 72 targets, the average duration of each hack works out at 8.74 months per intrusion.
- **Proof that the APT attack is not just PR hype.** Shady RAT helps to confirm the definition and nature of APT.
- **A hunger for secrets and intellectual property.** This doesn't spell cybercrime, which McAfee labels as serious but more manageable. But the debate rages on as to whether Shady RAT is the work of a state or commercial actor (or actors). Noting many of the familiar trademarks of such attacks over the last ten years, it is still reasonable to assume these are the actions of cybercriminals.
- **Evidence that is not a new attack.** Shady RAT used malware variants that have been around for years .

Shady Rat Questions Raised

- **Evidence of a specific country's involvement.** Many blaring press headlines, such as "China Suspected of Shady RAT Attacks," are uninformed. (This example resulted from an ex-US government lawyer who made the suggestion to the journalist involved.)
- **What is happening to all the hacked data.** It is reasonable to assume that the data gathered by Shady RAT -- possibly petabytes in total -- is being used to gain competitive advantage, which can have a wide-ranging effect on world economy, jobs, and national defense.
- **How many more attacks remain undiscovered or undisclosed.** As this attack is limited to just one command and control center, one could probably surmise there may be similar centers elsewhere. We could be witnessing the tip of the iceberg of this particular hacking spree.
- **When the attack began.** Log files captured only go back as far as 2006, and there is some evidence these particular hacks started even earlier.

Shady Rat Summary

The "Year of the Hackers" would be an appropriate title for 2011, with the added disclosure of Operation Shady RAT. This adds to the growing litany of hacking revelations, and we are only just past half of the year.

The report by McAfee Inc. (NYSE: MFE) is not so focused on the recent spate of data exfiltration hacks, such as those that hit RSA and Sony, or the self-publicized hacks of Lulz or Anonymous. Operation Shady RAT (which stands for Remote Access Tool) is an analysis of discovered log files from a command and control server that date from mid-2006 to mid-2010.

What the log files show is extensive hacking and intrusions into 72 organizations in 14 different countries. The victims include US and UK defense contractors, a Singapore electronics company, Olympic committees, and a Korean steel company.

Dmitri Alperovitch, VP of threat research at McAfee, reasonably concluded: "Although Shady RAT's scope and duration may shock those who have not been as intimately involved in the investigations into these targeted espionage operations as we have been, I would like to caution you that what I have described here has been one specific operation conducted by a single actor/group."

One final positive is the openness of McAfee's approach in publishing many of the facts and figures of this case. For too long such details have often remained a guarded secret. Awareness is part of the solution.

Finally, when it comes to such topics and particularly instant press responses to grab headlines via ill-informed attribution, suggestions have also been made that as China itself was not attacked, it must be the Chinese government that is responsible. If this is the case, why not France, Indonesia, or Greenland, for that matter, as they were not attacked?

As Lord Jeffrey (1773 - 1850), a Scottish lawyer and literary critic, wisely said, *"Beware prejudices. They are like rats, and men's minds are like traps; prejudices get in easily, but it is doubtful if they ever get out."*

The Rise of GHOSTing – Bulletproof Cybercrime Hosting in the Cloud

Increasingly, major cybercriminal bulletproof hosting operations are offering bone fide VPN (virtual private network) / VPS (virtual private servers) to clients who in turn use the services provided to churn out illicit and objectionable badness e.g. malware, botnet C&Cs, phishing and spam operations.

By all intents and purposes this type of operation gives the impression of clean and responsible hosting as no sign of criminal activity is detected on the providers' servers; the actual badness is held at arms' length and hidden away from any investigation of the main hosting provider.

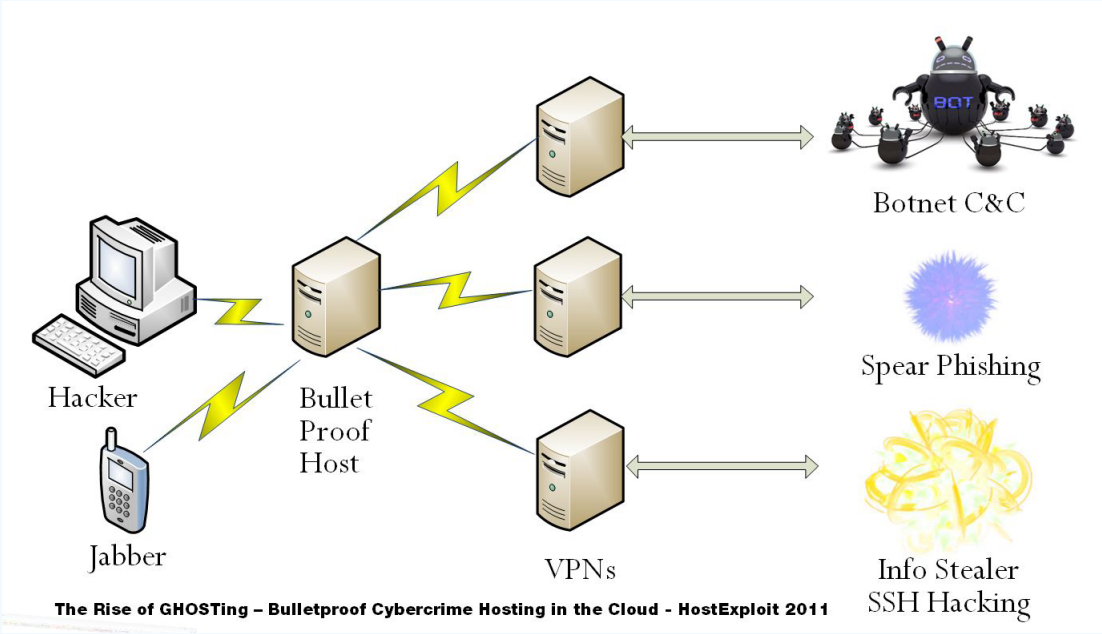


Figure 1 – GHOSTing Bulletproof Host Operations

Used in this way the actual bulletproof host needs only to act as a recipient of the illicit material or stolen data, and can, therefore claim no direct knowledge of any wrong doing. A real example of commercial GHOSTing services on offer from a well-known bullet proof host shows the strict rules on what can and cannot be stored on the hosts' actual server; e.g.

Allowable content:

- Adult
- Botnets
- Results from exploits, loaders
- Drop projects, traffic operation software
- Incoming spam & data

Forbidden content:

- Child pornography
- Terrorism
- Outgoing spam
- No local storage of active exploits or kits, only on VPN/ VPS provided.

Payments are made through the usually preferred routes e.g., LibertyReserve, PerfectMoney, WebMoney, etc. This reduces the risk for the bullet proof hosting operators, and allows their clients to operate on the understanding that the VPN /VPS provided may have a limited life before action by law enforcement agencies require the service to be shut down by the legitimate hosting provider.

Introduction

Introduction

The first half of the year was characterized by frequent reports of hacks and data breaches and Q3 2011 was no different. As of the end of September 2011 there seems little to stem the outward flow of data once unauthorized access has been gained.

The September revelation that the payment card details of Betfair customers had been hacked via AS16096 Betfair the Sporting Exchange Ltd. (UK) was cause for concern but equally was the discovery that the incident had occurred 18 months earlier. None of Betfair's customers were informed of the incident and, further, it was reported that the information was not made public due to an impending stock market flotation.

DigiNotar (NL) provided another example in case with an all-too-familiar tale of slow responses in what turned out to be a very serious hacker attack and breach. 531 fraudulent certificates and an urgent patch from Microsoft to block all DigiNotar certificates proved too much for the certificate issuing company. With its finances and reputation in shatters DigiNotar filed for bankruptcy through the Dutch courts in late September 2011.

Jart Armin

The Kelihos botnet and its Czech Hosting

In keeping with earlier quarters, Q3 provided us with a glimmer of hope in the shape of the news from Microsoft Corp., that the Kelihos botnet (Waledac 2.0) had been taken down. In a first of its kind, Microsoft named a defendant in a civil case complaint alleging that Dominique Alexander Piatti, dotFREE Group S.r.o and 22 John Does were responsible for operating and controlling the Kelihos botnet. The top level domain, cz.cc, used to register other subdomains, and a known repeat offender for hosting several types of badware, was taken offline on 26 September 2011.

The Czech Republic, home to the Kelihos botnet, is no stranger to bad hosts with two consistently prominent players appearing in the top 100 table. AS24971 Master Internet s.r.o. currently hosts C&C servers along with spam bots, malicious URLs and badware. Historical data displayed on SiteVet shows how Master Internet has frequent peaks and troughs in its cybercriminal activity with higher than usual levels noted in late September.

AS39392 SuperNetwork s.r.o., the largest content provider in the Czech Republic, has dropped down the bad host rankings this quarter to #64 but still serves unacceptable levels of spam, malicious URLs, exploits and current events.

In terms of the number of bad hosts the Czech Republic is a small player but the serving of botnets has the potential for a wide outreach depending on the number of computers it can enslave. In the case of Kelihos, 45,000 computers and 4 billion spam messages a day is more than enough to warrant a take down.

Frequently Asked Questions

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

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

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

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

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

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

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

Why do these hosts allow this activity?

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

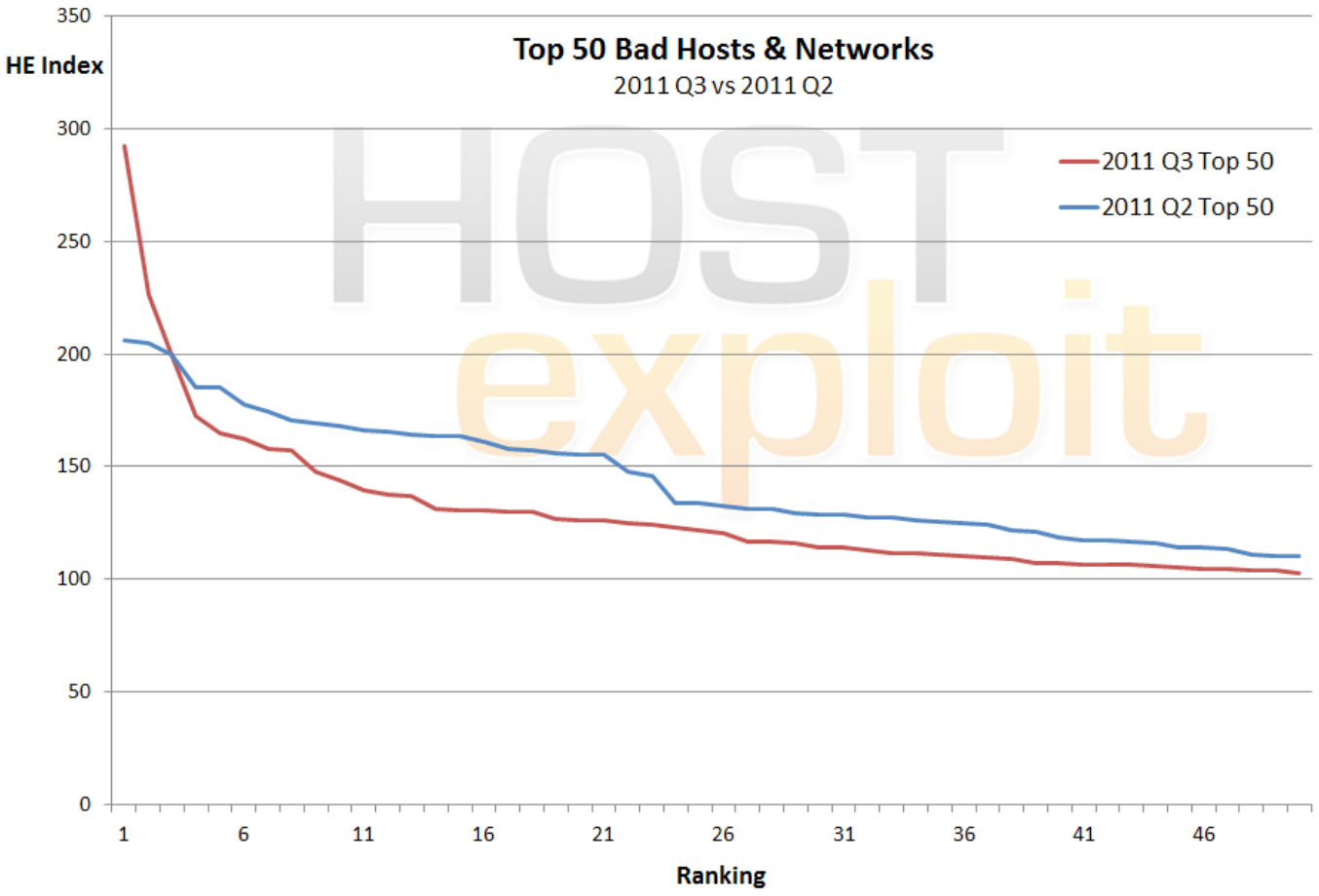
Further feedback is warmly welcomed

contact@hostexploit.com

3. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲ 1	292.7	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840
▲ 2	226.2	47583	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	LT	3,328
▶ 3	200.1	10297	ENET-2 - eNET Inc.	US	90,880
▼ 4	172.8	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	43,776
▲ 5	164.9	16138	INTERIAPL INTERIA.PL SA	PL	4,096
▲ 6	162.6	45899	VNPT-AS-VN VNPT Corp	VN	2,171,136
▲ 7	157.9	32475	SINGLEHOP-INC - SingleHop	US	235,264
▲ 8	157.0	22489	CASTLE-ACCESS - Castle Access Inc	US	49,408
▲ 9	147.8	16276	OVH OVH Systems	FR	548,864
▲ 10	143.9	32613	IWEB-AS - iWeb Technologies Inc.	CA	218,112
▲ 11	139.7	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,548,288
▲ 12	137.8	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	943,104
▲ 13	137.3	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	108,295,136
▲ 14	131.1	13727	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024
▲ 15	130.4	24940	HETZNER-AS Hetzner Online AG RZ	DE	502,784
▼ 16	130.4	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	48,640
▲ 17	130.3	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM - CDMA	IN	254,976
▼ 18	129.8	9809	NOVANET Nova Network Co.LtdRoom 1205... Shenzhen, China	CN	10,240
▼ 19	126.7	41947	WEBALTA-AS OAO Webalta	RU	15,872
▲ 20	126.3	29550	SIMPLYTRANSIT Simply Transit Ltd	GB	106,496
▲ 21	125.9	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve	TR	14,592
▲ 22	124.9	43146	AGAVA3 Agava Ltd.	RU	17,408
▲ 23	124.2	3595	GNAXNET-AS - Global Net Access, LLC	US	155,136
▲ 24	123.3	16265	LEASEWEB LeaseWeb B.V.	NL	279,808
▲ 25	121.6	11798	ACEDATACENTERS-AS-1 - Ace Data Centers, Inc.	US	145,408
▲ 26	120.3	40824	WZCOM-US - WZ Communications Inc.	US	9,216
▲ 27	116.8	6697	BELPAK-AS BELPAK	BY	1,075,200
▲ 28	116.5	6849	UKRTELNET JSC UKRTELECOM,	UA	1,507,840
▲ 29	116.0	19318	NJIIX-AS-1 - NEW JERSEY INTERNATIONAL INTERNET EXCHANGE LLC	US	90,368
▲ 30	114.1	15169	GOOGLE - Google Inc.	US	282,112
▲ 31	114.0	31034	ARUBA-ASN Aruba S.p.A. - Network	IT	129,792
▲ 32	112.7	29873	BIZLAND-SD - The Endurance International Group, Inc.	US	96,768
▲ 33	111.6	8660	MATRIX-AS Matrix S.p.A.	IT	8,192
▲ 34	111.3	17971	TMVADS-AP TM-VADS Datacenter Management	MY	40,576
▲ 35	110.9	25532	MASTERHOST-AS .masterhost autonomous system	RU	78,336
▼ 36	110.2	21788	NOC - Network Operations Center Inc.	US	278,528
▲ 37	109.9	9829	BSNL-NIB National Internet Backbone	IN	7,664,640
▲ 38	108.8	24557	AUSSIEHQ-AS-AP AussieHQ Pty Ltd	AU	32,512
▲ 39	107.2	9318	HANARO-AS Hanaro Telecom Inc.	KR	14,982,912
▲ 40	107.0	15149	EZZI-101-BGP - Access Integrated Technologies, Inc.	US	28,672
▲ 41	106.8	29497	KUBANGSM CJSC Kuban-GSM	RU	21,760
▲ 42	106.5	16125	DC-AS UAB Duomenu Centras	LT	5,376
▲ 43	106.2	12322	PROXAD Free SAS	FR	12,271,616
▼ 44	105.8	9050	RTD ROMTELECOM S.A	RO	1,648,896
▲ 45	105.0	8661	PTK PTK IP	RS	57,344
▲ 46	104.7	8972	PLUSSERVER-AS PlusServer AG, Germany	EU	147,456
▲ 47	104.5	13301	UNITEDCOLO-AS UNITED COLO GmbH	DE	66,816
▲ 48	103.8	6903	ZENON-AS ZENON N.S.P.	RU	32,768
▼ 49	103.7	24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	1,916,160
▲ 50	102.8	13213	UK2NET-AS UK-2 Ltd Autonomous System	EU	54,528

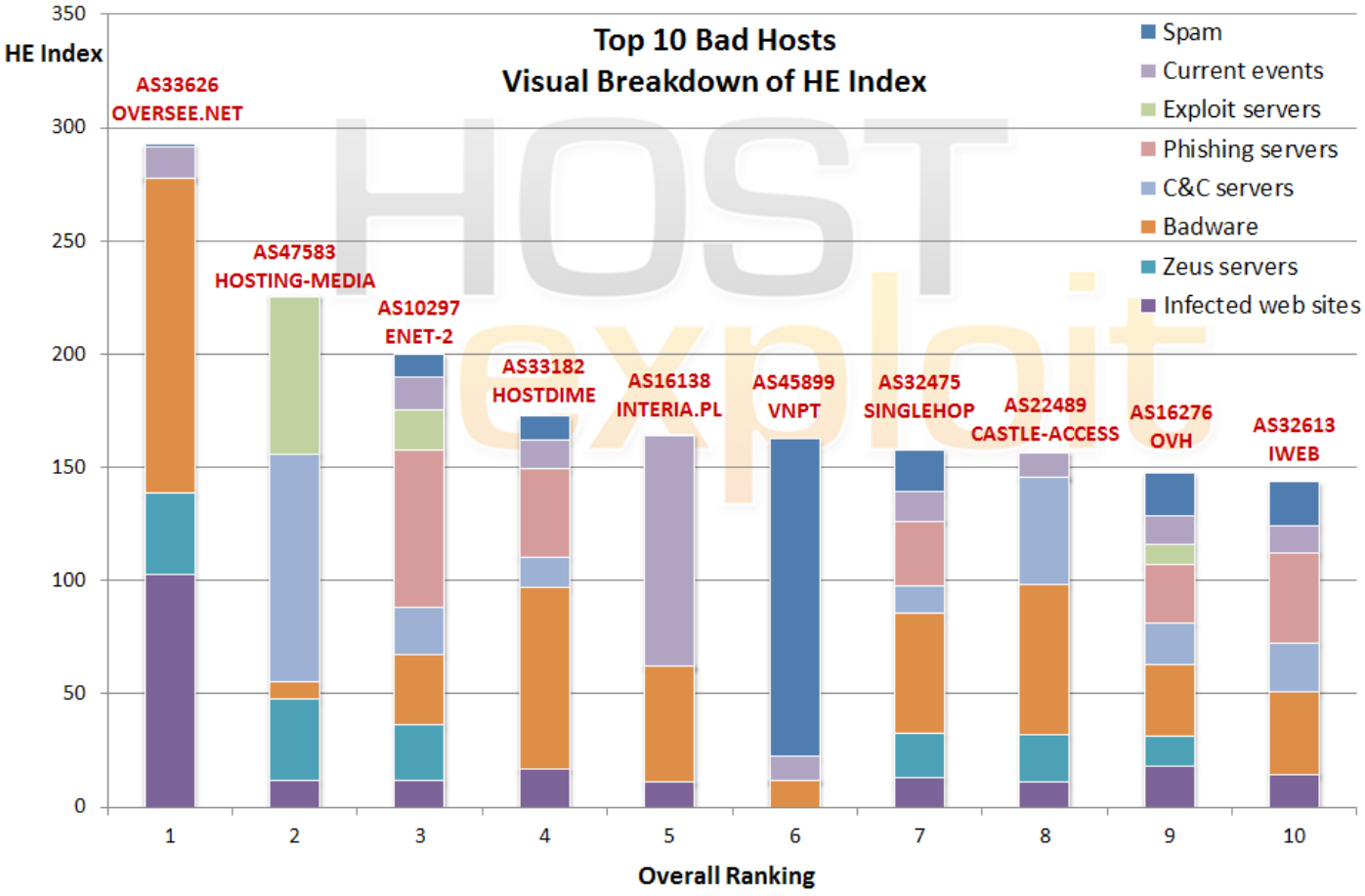
2011 Q3 to 2011 Q2 Comparison



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

Q3 is marked for the concentrated levels of cybercriminal activity found in the servers of some of the worst offenders over the course of the quarter. Overall, levels of activity for the Top 50 Bad Hosts remained approximately the same.

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 AS33626 Oversee.net (US) is ranked #1 due primarily to the hosting of badware and infected web sites, with smaller concentrations of Zeus serving and current events.

AS45899 VNPT (US), on the other hand, is in the Top 10 almost entirely due to its large quantities of spam serving.

What's New?

6.1. Overview

	Previous Quarter - Q2 2011			Current Quarter - Q3 2011		
	ASN	Name	Country	ASN	Name	Country
#1	33182	HostDime	US	33626	Oversee.net	US
#2	29073	Ecatel	NL	47583	Hosting Media	LT
#3	10297	eNET	US	10297	eNET	US
#1 for Spam	33774	DJAWEB	DZ	45899	VNPT Corp	VN
#1 for Botnets	36408	Panther Express / CDNetworks	US	47583	Hosting Media	LT
#1 for Zeus Botnet	41947	Webalta	RU	16125	Duomenu Centras	LT
#1 for Phishing	10297	eNET	US	10297	eNET	US
#1 for Exploit Servers	14585	CIFNet Inc.	US	47583	Hosting Media	LT
#1 for Badware	33626	Oversee.net	US	33626	Oversee.net	US
#1 for Infected Sites	29073	Ecatel	NL	33626	Oversee.net	US
#1 for Current Events	16138	Interia.pl	PL	16138	Interia.pl	PL

This quarter has revealed significant changes for some hosts that have been regular Top 10 high fliers. It is especially pleasing to see that AS29073 Ecatel has completely dropped out of the Top 10 chart and is now placed at #53.

Ecatel had been in the Top 10 since early in 2010. We believe in giving credit when it is due, so well done Ecatel and we hope that your improved position continues its downward trend.

New at #1 is US hosted AS33626 Oversee.net and earns the #1 spot in both badware and infected sites, while AS47583 Hosting Media, new at #2 overall, is #1 for botnets and and exploit servers.

6.2. Top 10 Newly-Registered Hosts - In Q3 2011

By end of Q3 2011 there were **39,056** ASes; an increase of **1,056** from end of Q2 2011.

Below we show a selection of 10 ASes registered in Q3 2011 with the highest HE Indexes. With significant levels of badness recorded in a short period of time, these hosts are of interest.

Listed below the 10 Q3 ASes are the same findings in the previous two quarterly reports. As can be seen, the ASes this quarter are somewhat different - firstly, they are larger in size of address space. Generally it would be expected that newly-registered hosts with significant levels of malicious activity are "disposable" ASes, with the intention of being short-lived. This has previously been the case, until Q3, with two large ASes in Taiwan, and one in China.

Period	HE Rank	HE Index	AS number	AS name	Country	# of IPs
2011 Q3	57	98.1	9931	CAT-AP The Communication Authoity of Thailand, CAT	TH	209,920
	160	72.4	9929	CNCNET-CN China Netcom Corp.	CN	1,182,944
	269	64.6	33491	COMCAST-33491 - Comcast Cable Communications, Inc.	US	2,304
	333	61.4	9924	TFN-TW Taiwan Fixed Network, Telco and Network Service Provider.	TW	3,908,352
	364	60.6	7725	COMCAST-7725 - Comcast Cable Communications Holdings, Inc	US	1,536
	452	54.2	33668	CMCS - Comcast Cable Communications, Inc.	US	256
	460	53.9	9919	NCIC-TW New Century InfoComm Tech Co., Ltd.	TW	1,102,848
	542	50.6	33652	CMCS - Comcast Cable Communications, Inc.	US	1,024
	743	44.9	33489	COMCAST-33489 - Comcast Cable Communications, Inc.	US	0
	756	44.6	33490	COMCAST-33490 - Comcast Cable Communications, Inc.	US	1,024
2011 Q2	146	78.3	33651	CMCS - Comcast Cable Communications, Inc.	US	768
	179	73.5	33657	CMCS - Comcast Cable Communications, Inc.	US	256
	210	70.4	11380	INTERNETOFFICEPARKS	ZA	0
	295	60.6	49093	BIGNESS-GROUP-AS Bigness Group Ltd.	RU	512
	572	51.1	3.196	IM-AS Info-Media LTD	RU	256
	576	50.9	50073	SOFTNET Software Service Prague s.r.o.	CZ	256
	584	50.7	44088	DORINEX-AS SC Dorinex Pord SRL	RO	768
	768	45.7	42868	NIOBE Niobe Bilisim Backbone AS	US	4,096
	817	44.4	48671	ECSRV-AS Production United Enterprise Econom-Service Ltd	UA	256
	818	44.4	49798	SECUREHOST-NET-AS SecureHost LLC	RO	512
2011 Q1	92	98.3	47306	ISEC-AS The International Scientifical and Educational Centre	UA	256
	309	67.4	42741	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	RO	1,280
	359	64.0	43134	COMPLIFE-AS CompLife Ltd	MD	512
	657	52.9	20228	PACNET-MX - Pacnet, S.A. de C.V.	US	12,288
	677	52.2	16109	INCA-AS Informational and Commercial Agency "INCA" LTD	UA	256
	827	47.5	8514	INODE UPC Austria GmbH	AT	0
	1,481	34.1	51786	SATURN-R-GROUP LLC Telecom-Group-Saturn_R	RU	1,536
	1,779	29.5	55831	AIRCEL-IN Aircel Ltd.	IN	177,152
	1,854	28.6	51362	BESTISP-AS PE Yastremskiy Leonid Stepanovich	UA	512
	1,927	27.7	52116	ORIONTELEKOMTIM-AS Orion Telekom Tim d.o.o.Beograd...	RS	8,192

6.3. Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-99.1%	24	133.8	30,277	1.2	50693	KONSING-GROUP Konsing group doo	RS	2,048
-98.5%	112	84.6	11,137	1.3	49130	ARNET-AS SC ArNet Connection SRL	EU	0
-95.2%	62	105.5	6,021	5.0	50244	ITELECOM Pixel View SRL	RO	8,704
-83.2%	109	85.2	3,440	14.3	50465	IQHOST IQHost Ltd	RU	3,584
-80.4%	49	110.3	2,284	21.7	51306	UAIP-AS PAN-SAM Ltd.	UA	2,048
-77.5%	84	95.1	2,337	21.4	37957	CNNIC-CCCNET China Communication	CN	4,096
-69.8%	33	127.2	1,050	38.5	39150	TRANSIT-TELECOM-AS Tranzit Telecom	UA	5,376
-68.1%	17	157.8	555	50.3	33774	DJAWEB	DZ	1,707,776
-65.7%	16	161.1	437	55.2	6851	BKCNET "SIA" IZZI	LV	49,152
-64.8%	48	111.0	1,019	39.0	14585	CIFNET - CIFNet, Inc.	US	7,680

The hosts in the above table have all demonstrated a dramatic reduction in levels of badness in the three months since our Q2 2011 quarter report was published.

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

Noteworthy improvements include:

AS50693 Konsing Group (RS) down from #24 and high levels of badness to #30,277 with insignificant levels of badness, a huge drop of 99.1 percent.

AS49130 Arnet Connection (EU) improved by 98.5 percent to negligible levels of badness.

AS50244 ITelecom (RO) by 95.2 percent, moving out of the Top 100 in the process.

6.4. Deteriorated Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
22,610.1%	31,461	1.0	2	226.2	47583	HOSTING-MEDIA Aurimas Rapalis	LT	3,328
668.9%	3,293	14.5	33	111.6	8660	MATRIX-AS Matrix S.p.A.	IT	8,192
362.6%	2,628	19.0	90	88.0	10922	LIVEJOURNAL - Live Journal Inc.	US	1,024
172.5%	1,330	34.0	78	92.6	55330	GCN-DCN-AS AFGHANTELECOM...	AF	14,592
162.9%	1,536	30.4	115	80.0	20648	RAN-NETWORKS RAN Networks S.L.	ES	8,192
136.9%	831	44.1	47	104.5	13301	UNITEDCOLO-AS UNITED COLO GmbH	DE	66,816
136.4%	1,019	40.4	70	95.5	9280	CIA-AS connect infobahn australia...	AU	8,704
112.8%	691	47.5	51	101.0	39570	LOOPIA Loopia AB	SE	768
109.2%	225	68.8	10	143.9	32613	IWEB-AS - iWeb Technologies Inc.	CA	218,112
101.2%	499	54.1	38	108.8	24557	AUSSIEHQ-AS-AP AussieHQ Pty Ltd	AU	32,512

The hosts listed here display the biggest increases in levels of badness since the last quarter. Newly-registered hosts are covered in a separate section (6.2).

The "standout" host this quarter, is AS47583 Hosting Media for a staggering increase in levels of badness. Formerly low down the ranking Hosting Media has jumped up the ranks to #2 for overall levels of cybercriminal activity. Hosting Media is #1 for hosting botnets and exploit servers.

The second most deteriorated host is AS8660 Matrix S.p.a now at #33. Matrix S.p.a. scores highly for phishing servers (#2 position) as well as hosting malicious URLs, badware, current events and botnets.

AS10922 Live Journal Inc. climbed up the ratings to #90 for hosting high levels of malicious URLs, badware and current events.

All the hosts listed here are advised to review recent changes that may account for the sudden rise in levels of bad activity.

Country Analysis

This quarter we've expanded our table of Bad Hosts by country to 250 ASes in total, up from 50.

The usual countries appear in the list - some with particularly high concentrations of malicious activity, but others appear mainly due to the number of hosts present in the country.

For this reason, we have been working on a unique methodology to more accurately determine the badness levels present in a country. This brings its own set of challenges, such as the impossibility of correctly determining physical server locations in an automated fashion.

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

In effect, this is similar to how the HE Index currently scores a host's badness level, without being driven too strongly by the number of IPs allocated to that host.

This will enable more accurate trend analysis to take place on movement of malicious activity between different countries.

Hosts in Top 250	Country	Total IPs within Top 250	Total Index	Average Index	Average Indexes by Category							
					Infected web sites	Zeus servers	Badware	C&C servers	Phishing servers	Exploit servers	Current events	Spam
60	UNITED STATES	143,109,632	5,712.9	95.2	128.7	59.5	155.4	116.4	85.7	29.8	114.7	40.8
26	RUSSIAN FEDERATION	5,115,328	2,228.1	85.7	82.7	153.9	87.3	52.5	6.1	30.3	82.6	114.7
13	GERMANY	35,424,256	1,156.4	89.0	103.3	105.0	122.1	96.2	70.9	55.3	100.6	48.4
13	CHINA	215,357,856	1,156.3	88.9	89.5	29.5	147.4	112.5	10.5	78.6	103.0	70.8
11	BRAZIL	27,118,080	806.3	73.3	95.3	0.1	101.3	125.7	0.1	29.1	102.5	69.3
10	UNITED KINGDOM	17,348,352	743.5	74.4	105.5	28.1	123.8	86.8	0.1	27.1	109.5	49.1
9	INDIA	11,120,128	788.0	87.6	37.0	0.1	40.7	11.5	0.1	22.0	44.6	313.9
9	UKRAINE	2,242,816	705.2	78.4	80.0	142.6	98.6	74.6	0.2	0.1	105.1	65.8
9	TURKEY	11,368,704	694.5	77.2	96.4	43.1	121.6	51.3	0.1	46.1	102.9	76.2
7	NETHERLANDS	402,688	620.5	88.6	115.6	94.9	125.4	71.2	31.0	101.7	119.8	43.3
6	EUROPE	29,584,896	498.4	83.1	103.6	31.4	117.5	111.5	51.9	0.0	101.0	79.1
5	KOREA, REPUBLIC OF	92,772,032	414.6	82.9	133.9	0.0	93.5	120.7	25.1	99.6	103.7	72.8
4	FRANCE	12,840,960	432.5	108.1	95.7	131.7	188.3	67.5	130.4	58.9	107.9	51.8
4	VIET NAM	6,062,080	393.7	98.4	77.8	0.0	99.8	55.4	0.1	0.0	102.4	241.7
4	CZECH REPUBLIC	391,424	329.6	82.4	111.4	75.3	149.4	83.6	0.1	41.9	105.1	33.4
4	SPAIN	14,407,680	298.9	74.7	105.4	105.2	133.3	25.4	0.1	0.0	101.2	46.7
3	CANADA	373,504	342.7	114.2	78.9	120.5	216.5	103.5	185.1	0.0	105.0	51.0
3	AUSTRALIA	54,784	292.5	97.5	68.1	162.7	97.9	37.2	496.8	0.1	103.4	5.8
3	THAILAND	261,888	233.1	77.7	105.8	117.1	112.3	35.7	0.1	73.8	68.3	62.2

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
37,382	**0.37**	**38333**	SYMBIO-AS-AU-AP Symbio Networks	**AU**	147,296
37,378	**0.38**	**5605**	NETUSE NetUSE AG	**DE**	140,544
37,363	**0.39**	**19855**	ASN-MASERGY-US Masergy US Autonomous System	**US**	131,840
37,356	**0.39**	**2895**	FREE-NET-AS FREEnet	**EU**	131,072
37,324	**0.42**	**23329**	AS-OPENACCESS - Open Access Inc.	**US**	112,384
37,276	**0.46**	**16811**	SPACENET-GTH - Spacenet, Inc.	**US**	913,152
37,246	**0.48**	**2594**	ASN-CSI CSI Piemonte	**EU**	81,920
37,079	**0.53**	**2685**	ASATTCA AT&T Global Network Services - CA	**US**	65,536
37,065	**0.54**	**35776**	TELEOS Teleos	**DE**	62,464
36,815	**0.64**	**71**	HP-INTERNET-AS Hewlett-Packard Company	**US**	35,072,000

8.1. Why List Examples of Good Hosts?

It would be wrong to give the impression that service providers can only be judged in terms of badness. To give a balanced perspective we have pinpointed the 10 best examples of organizations with minimal levels of service violations. Safe and secure web site hosting environments are perfectly possible to achieve and should be openly acknowledged as an example to others.

Our table of 'good hosts' is testimony to the best practices within the industry and we would like to commend those companies on their effective abuse controls and management.

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

8.2. Selection Criteria

We apply the good host selection to ISPs, colocation facilities, or organizations who control at least 10,000 individual IP addresses. Many hosting providers shown elsewhere in this report control less than this number. However, in this context, our research focuses mainly on larger providers which, it could be argued, should have the resources to provide a full range of proactive services, including 24-hour customer support, network monitoring and high levels of technical expertise.

We also only included those ASes that act primarily as public web or internet service providers, although we appreciate that such criteria is subjective.

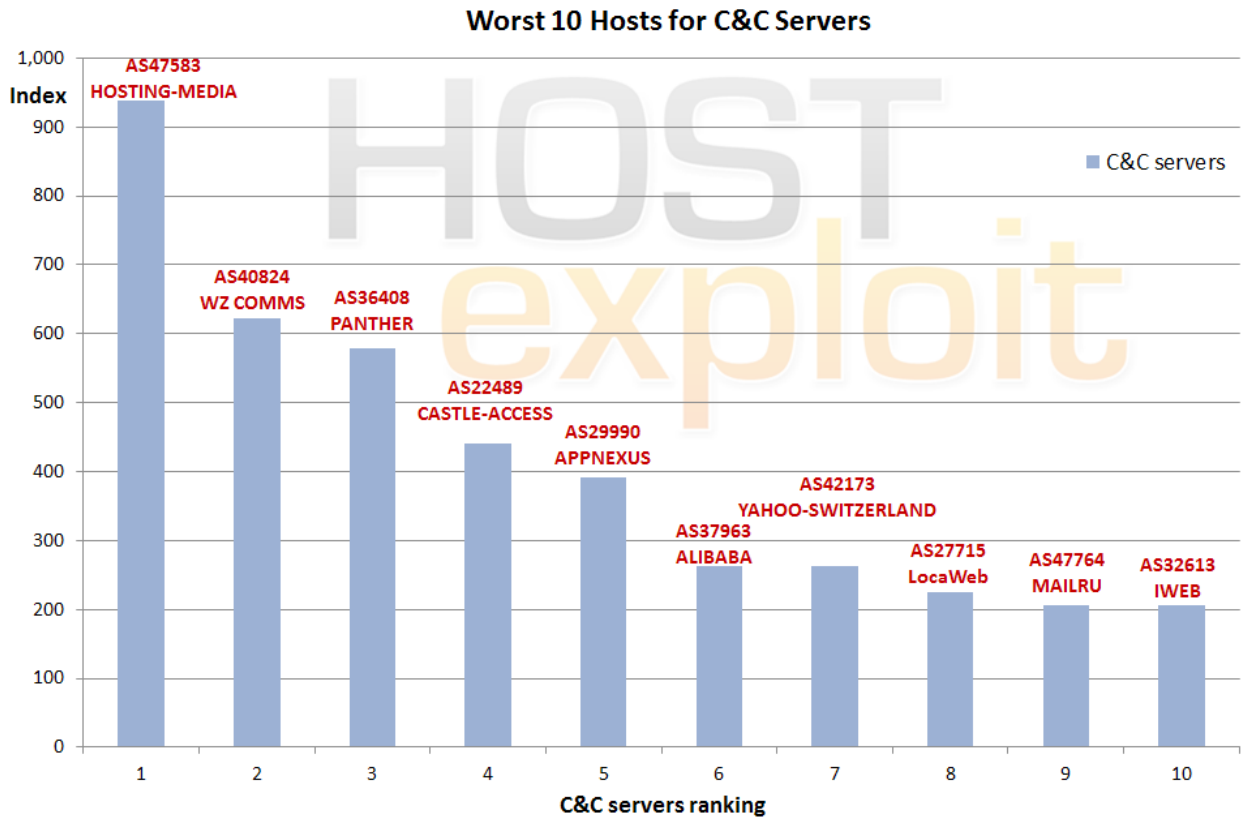
Bad Hosts by Topic

9.1.1. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
2	226.2	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	3,328	**937.6**
26	120.3	**40824**	WZCOM-US - WZ Communications Inc.	**US**	9,216	**621.9**
87	88.6	**36408**	ASN-PANTHER Panther Express	**US**	80,384	**579.0**
8	157.0	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,408	**441.6**
848	42.4	**29990**	ASN-APPNEXUS - AppNexus, Inc	**US**	34,816	**391.7**
747	44.8	**37963**	CNNIC-ALIBABA-CN-NET-AP Alibaba (China) Technology Co., Ltd.	**CN**	762,880	**263.3**
1,376	31.9	**42173**	YAHOO-SWITZERLAND Yahoo! Europe	**GB**	15,104	**262.8**
65	96.2	**27715**	LocaWeb Ltda	**BR**	83,200	**224.9**
515	51.7	**47764**	MAILRU-AS Limited liability company Mail.Ru	**RU**	12,032	**206.5**
10	143.9	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	218,112	**206.1**

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

The position for the US has improved from Q2, with 4 out of the top 10 worst hosts for botnet C&Cs, down from 6.



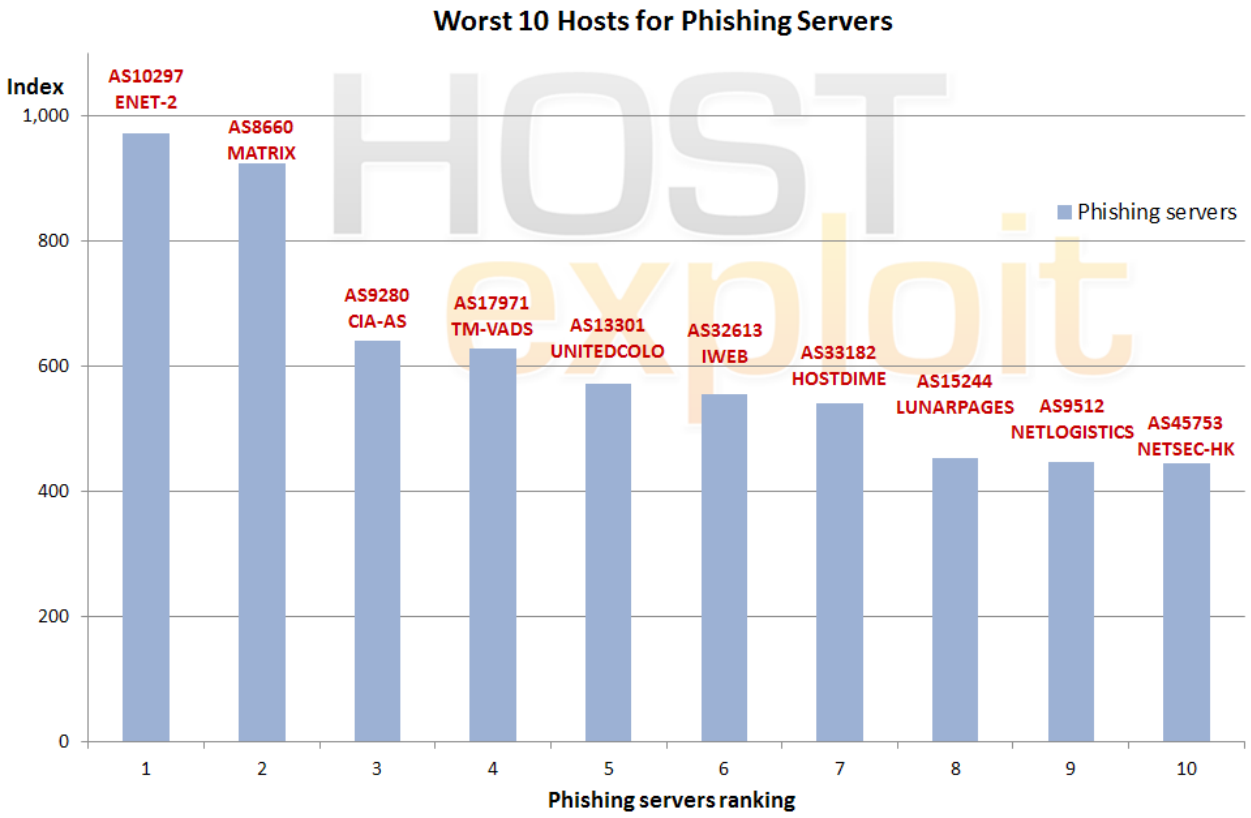
9.1.2. Phishing Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
3	200.1	**10297**	ENET-2 - eNET Inc.	**US**	90,880	**971.6**
33	111.6	**8660**	MATRIX-AS Matrix S.p.A.	**IT**	8,192	**924.0**
70	95.5	**9280**	CIA-AS connect infobahn australia (CIA)	**AU**	8,704	**639.9**
34	111.3	**17971**	TMVADS-AP TM-VADS Datacenter Management	**MY**	40,576	**628.4**
47	104.5	**13301**	UNITEDCOLO-AS UNITED COLO GmbH	**DE**	66,816	**572.9**
10	143.9	**32613**	IWEB-AS - iWeb Technologies Inc.	**CA**	218,112	**555.0**
4	172.8	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**540.6**
16	130.4	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	**US**	48,640	**452.6**
89	88.2	**9512**	NETLOGISTICS-AU-AP Net Logistics Pty. Ltd.	**AU**	13,568	**448.1**
74	94.4	**45753**	NETSEC-HK Unit 1205-1207	**HK**	117,504	**444.7**

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

In the last quarter the top 6 phishing hosts were all based in the US, this has now reduced to 3.

It would appear malware located on servers in Western countries minimizes the awareness of both customers and target organizations and helps to establish false credibility, which is the cornerstone of phishing campaigns.



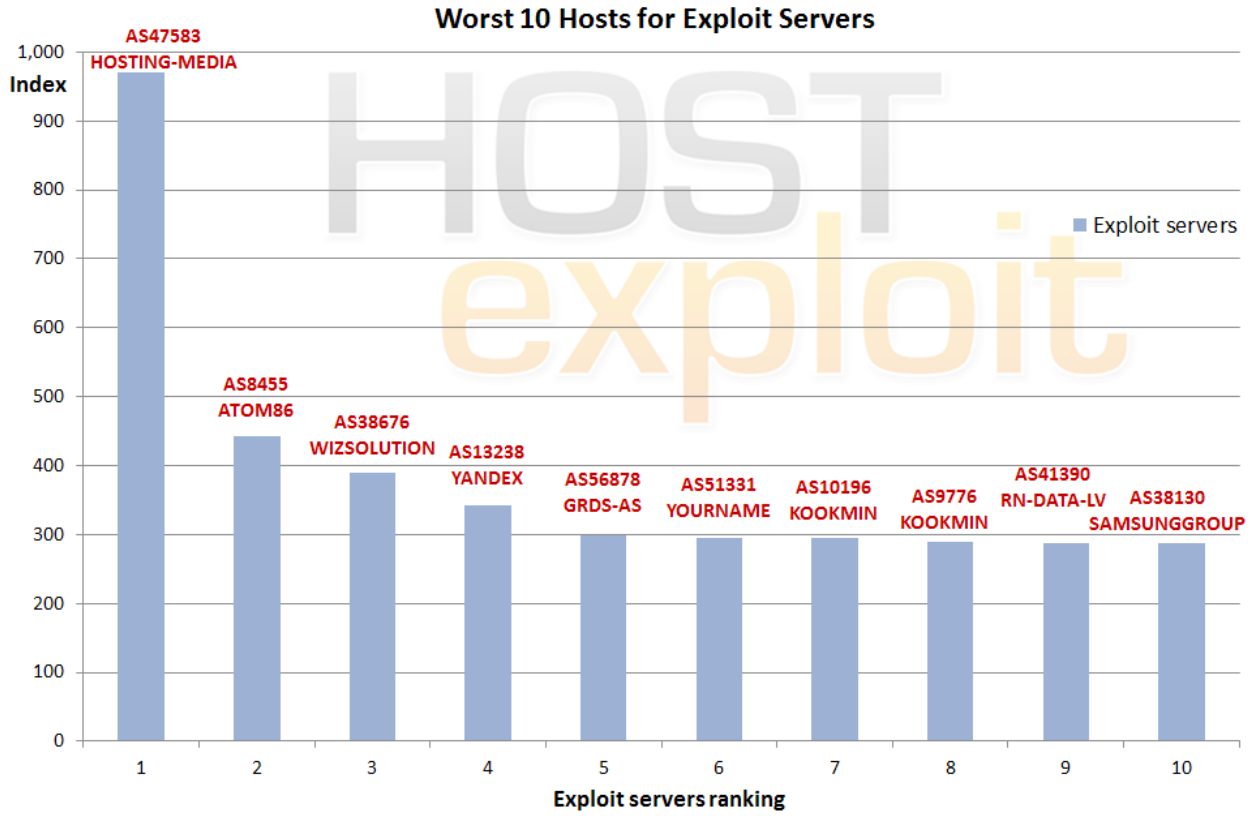
9.1.3. Exploit Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
2	226.2	**47583**	HOSTING-MEDIA Aurimas Rapalis trading as "II Hosting Media"	**LT**	3,328	**971.5**
146	73.8	**8455**	ATOM86-AS ATOM86 Autonomous System	**NL**	17,408	**442.2**
517	51.6	**38676**	AS33005-AS-KR wizsolution co.,Ltd	**KR**	8,704	**388.7**
121	79.0	**13238**	YANDEX Yandex LLC	**RU**	164,480	**341.6**
1,147	36.5	**56878**	GRDS-AS LLC "Inter-Treyd"	**RU**	256	**298.7**
1,271	33.8	**51331**	YOURNAME Your Name Webhosting	**NL**	768	**294.1**
2,214	22.2	**10196**	HNCBWORLD-AS-KR Kookmin Bank	**KR**	768	**294.1**
2,260	21.9	**9776**	KBSTAR Kookmin Bank	**KR**	1,280	**289.8**
270	64.5	**41390**	RN-DATA-LV RN Data, SIA	**LV**	1,536	**287.7**
1,342	32.4	**38130**	SAMSUNGGROUP Samsung Networks Inc.	**KR**	1,664	**286.7**

We consider the category of "Exploit Servers" to be the most important in the analysis of malware, phishing, or badness as a whole. Added weighting is given to this sector. Full detail of our methodology can be viewed in Appendix 2.

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

In contrast to spam hosts, Exploit Servers have until recently been entirely located in countries subject to lower levels of regulation. This is a trend that Q3 2011 returns to after the proliference of US hosts in the top 10 in this sector in Q2.



9.1.4. Botnet Hosting - Zeus

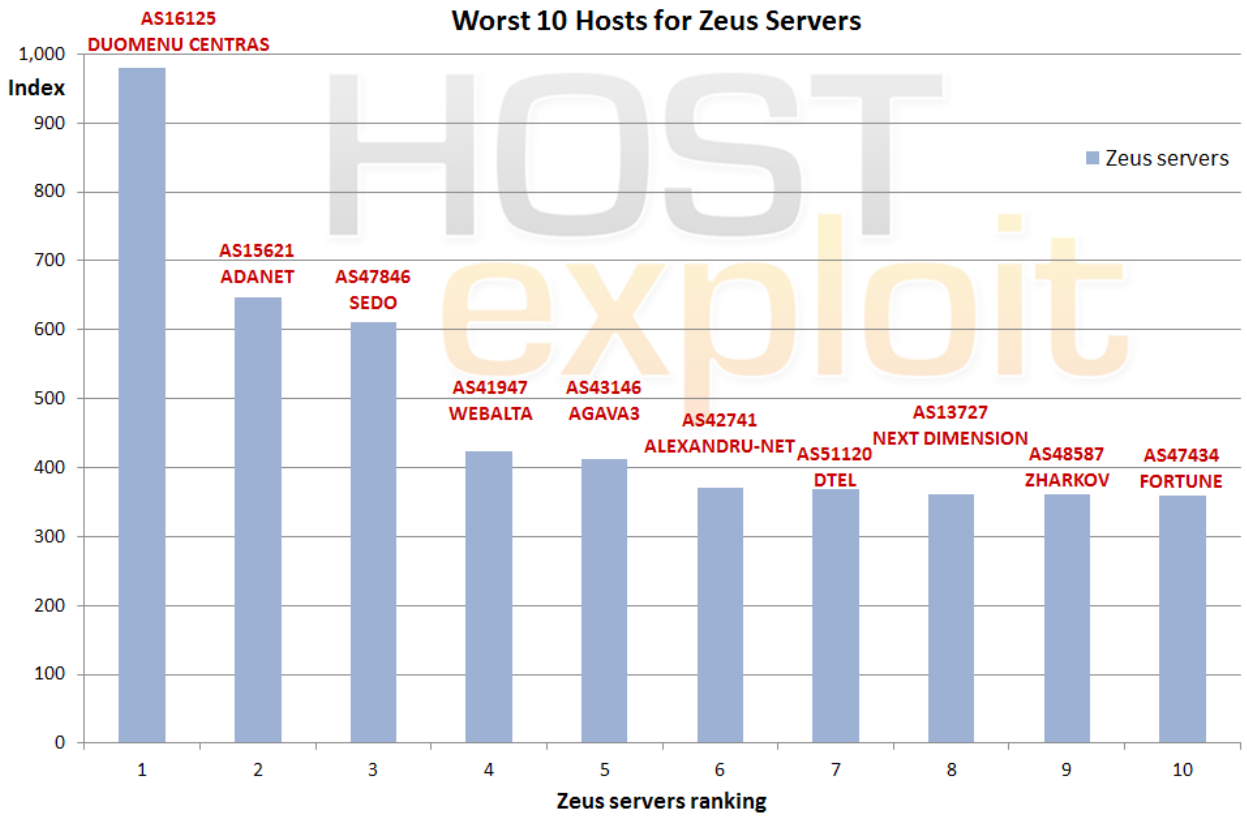
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
42	106.5	**16125**	DC-AS UAB Duomenu Centras	LT	5,376	**980.1**
60	97.3	**15621**	ADANET-AS Azerbaijan Data Network	RU	11,264	**647.1**
71	95.4	**47846**	SEDO-AS Sedo GmbH	DE	1,536	**611.5**
19	126.7	**41947**	WEBALTA-AS OAO Webalta	RU	15,872	**423.1**
22	124.9	**43146**	AGAVA3 Agava Ltd.	RU	17,408	**411.4**
918	41.0	**42741**	ALEXANDRU-NET-TM-AS S.C. ALEXANDRU NET TM S.R.L.	RO	256	**370.7**
923	40.8	**51120**	DTEL-BIZ-AS DTEL Inc.	RU	384	**369.2**
14	131.1	**13727**	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024	**361.6**
185	70.0	**48587**	NET-0X2A-AS Private Entrepreneur Zharkov Mukola...	UA	1,024	**361.6**
113	80.5	**47434**	FORTUNE-AS Fortune Science and Production Company	UA	1,280	**358.7**

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 9.1.3 on Exploit Servers.

This list often contains many names that are familiar to cybercrime observers and researchers, some of whom are known as repeat offenders.

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



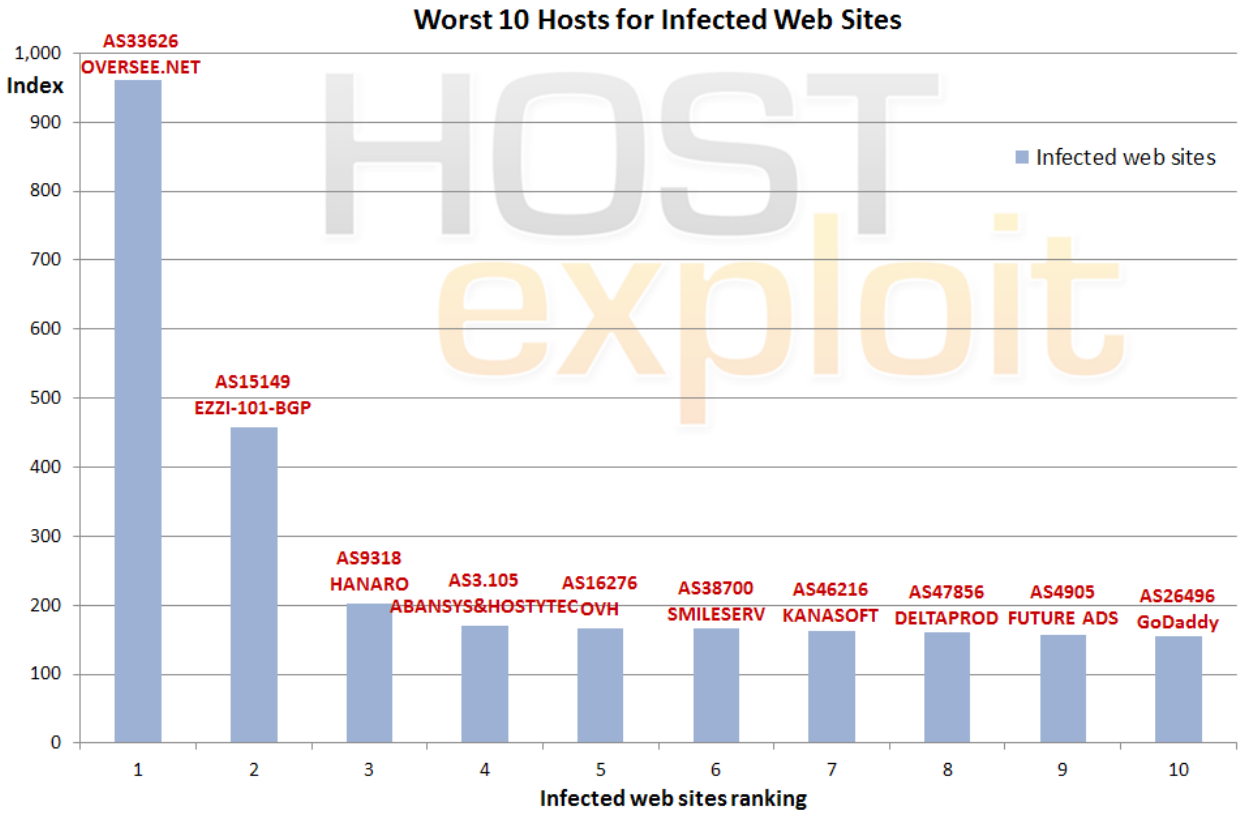
9.2.1. Infected Web Sites

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
1	292.7	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**960.7**
40	107.0	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,672	**457.1**
39	107.2	**9318**	HANARO-AS Hanaro Telecom Inc.	**KR**	14,982,912	**202.1**
1,739	26.9	**3.105**	ABANSYS_AND_HOSTYTEC-AS Abansys & Hostytec, S.L.	**ES**	4,096	**170.5**
9	147.8	**16276**	OVH OVH Systems	**FR**	548,864	**167.0**
366	60.5	**38700**	SMILESERV-AS-KR SMILESERV	**KR**	108,800	**165.7**
1,767	26.7	**46216**	KANASOFT - KANA Software, Inc	**US**	256	**161.6**
2,763	18.5	**47856**	DELTAPROD-AS Delta Productions Ltd	**IM**	512	**160.9**
2,840	18.0	**4905**	FA-LAX-1 - Future Ads LLC	**US**	256	**156.1**
58	98.0	**26496**	PAH-INC - GoDaddy.com, Inc.	**US**	1,287,424	**155.7**

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

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

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

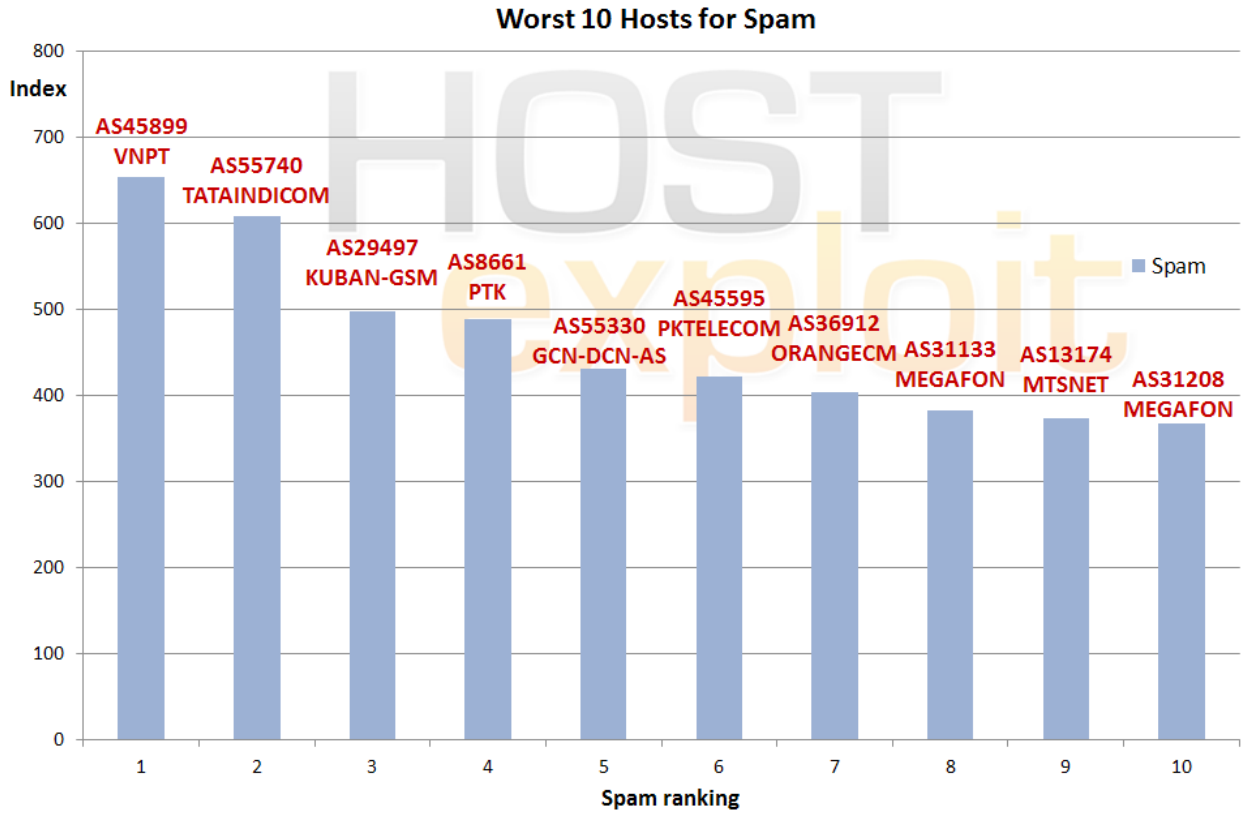


9.2.2. Spam

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
6	162.6	**45899**	VNPT-AS-VN VNPT Corp	**VN**	2,171,136	**653.7**
17	130.3	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM - CDMA	**IN**	254,976	**607.9**
41	106.8	**29497**	KUBANGSM CJSC Kuban-GSM	**RU**	21,760	**498.0**
45	105.0	**8661**	PTK PTK IP	**RS**	57,344	**489.5**
78	92.6	**55330**	GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMM...	**AF**	14,592	**431.5**
73	95.1	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	3,745,536	**422.3**
94	86.7	**36912**	ORANGECM	**CM**	8,192	**403.7**
77	92.9	**31133**	MF-MGSM-AS OJSC MegaFon	**RU**	16,960	**382.5**
103	83.3	**13174**	MTSNET OJSC "Mobile TeleSystems" Autonomous System	**RU**	24,320	**374.5**
122	78.9	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	3,072	**367.5**

Our Top 10 spam results show a consistent pattern for the location of servers used by spammers. Countries with minimal regulation and monitoring enable spammers to use tried-and-tested methods to avoid detection such as fast-flux servers and disposable crime servers. Additionally, they are quick to adapt to current media themes without needing new innovations, unlike other areas of cybercriminal activity.

A single spam server can cause more damage than a whole group of spam servers. Furthermore, a small quantity of spam can be more effective than a large quantity if using targeted techniques. These two properties make this a difficult category to quantitatively measure. For this reason, we combine known spam IPs from a vast range of respected sources – SpamHaus, UCEPROTECT-Network, Malicious Networks (FiRE) and SudoSecure – with our own data. The result is a definitive and current list of spam servers in the world, i.e. those hosting the IP space sending the spam.



9.2.3. Current Events

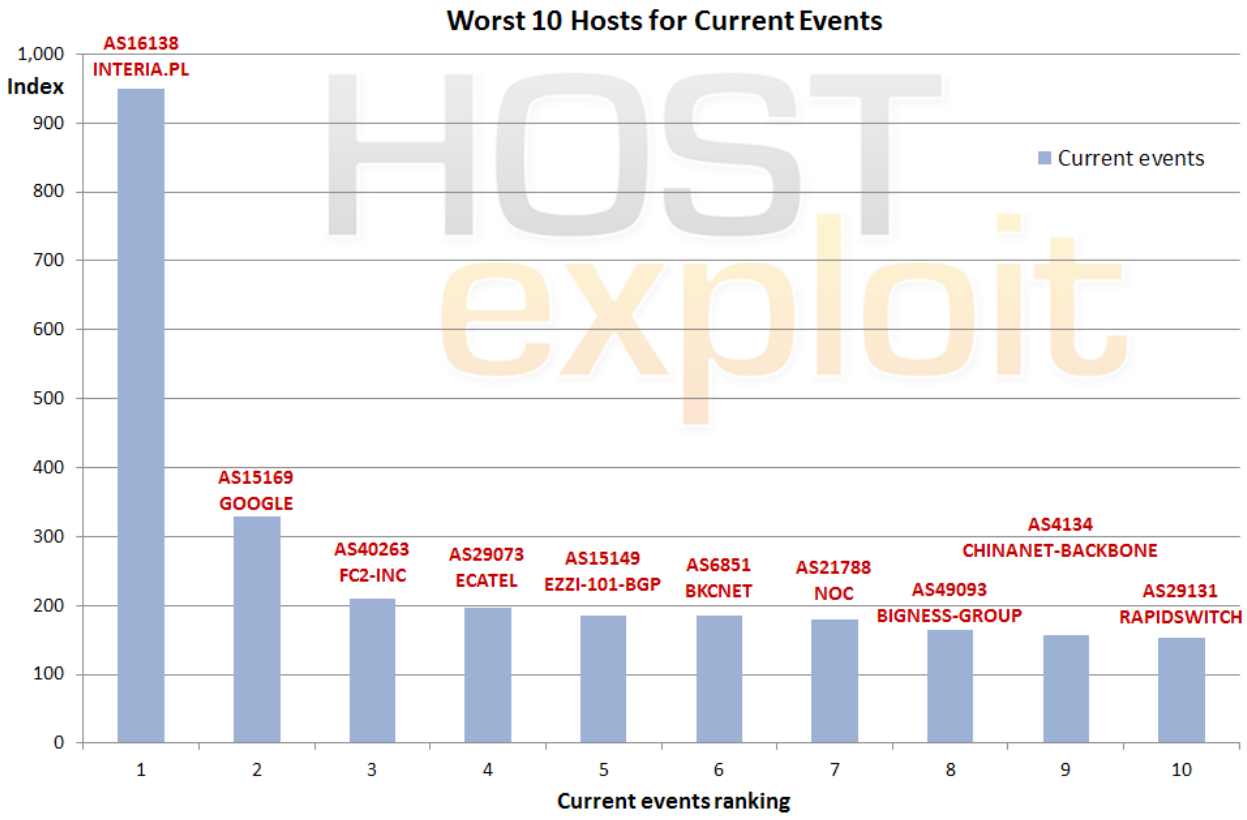
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
5	164.9	**16138**	INTERIAPL INTERIA.PL SA	**PL**	4,096	**949.5**
30	114.1	**15169**	GOOGLE - Google Inc.	**US**	282,112	**329.0**
197	68.9	**40263**	FC2-INC - FC2 INC	**US**	2,048	**210.7**
52	100.6	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,568	**197.1**
40	107.0	**15149**	EZZI-101-BGP - Access Integrated Technologies, Inc.	**US**	28,672	**186.1**
437	55.2	**6851**	BKCNET "SIA" IZZI	**LV**	49,152	**185.3**
36	110.2	**21788**	NOC - Network Operations Center Inc.	**US**	278,528	**179.0**
2,696	18.8	**49093**	BIGNESS-GROUP-AS Bigness Group Ltd.	**RU**	256	**164.3**
13	137.3	**4134**	CHINANET-BACKBONE No.31,Jin-rong Street	**CN**	108,295,136	**157.7**
215	67.6	**29131**	RAPIDSWITCH-AS RapidSwitch	**GB**	0	**152.3**

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

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

The vast array of techniques looked at in this category are reflected in this Top 10 Current Events sector with this list containing some well-known names.

Unchanged from Q2 is the 40% of the Top 10 that are based in US.



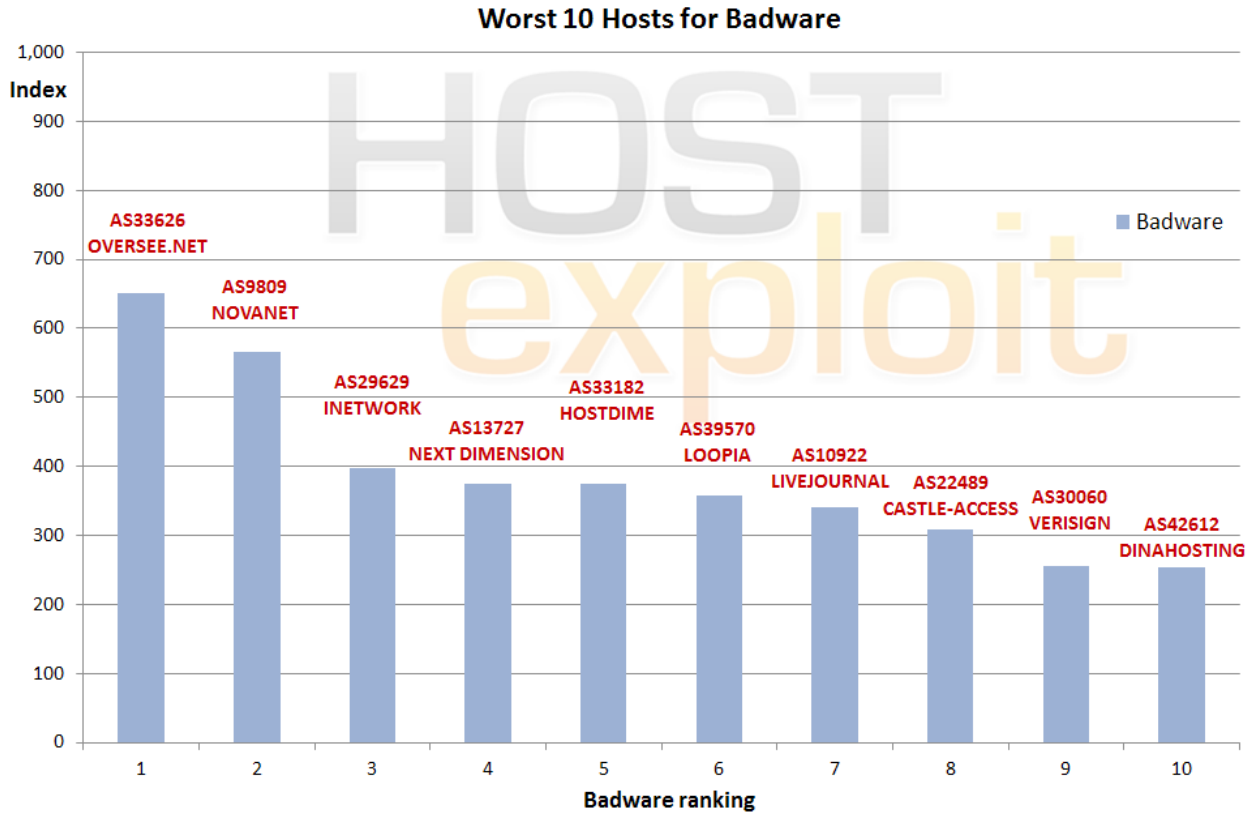
9.2.4. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
1	292.7	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**650.1**
18	129.8	**9809**	NOVANET Nova Network Co.Ltd... Shenzhen, China	**CN**	10,240	**566.6**
59	97.6	**29629**	INETWORK-AS IEUROP AS	**FR**	8,192	**397.2**
14	131.1	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**375.3**
4	172.8	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	43,776	**374.3**
51	101.0	**39570**	LOOPIA Loopia AB	**SE**	768	**357.5**
90	88.0	**10922**	LIVEJOURNAL - Live Journal Inc.	**US**	1,024	**340.9**
8	157.0	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	49,408	**309.3**
236	66.4	**30060**	WILDCARD-VERISIGN - VeriSign Infrastructure & Operations	**US**	5,376	**254.9**
119	79.1	**42612**	DINAHOSTING-AS ASN de Dinahosting SL	**ES**	18,432	**253.9**

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

In this quarter there has been further analysis on 'false positives' particularly regarding parked domains. These have been found to a limited degree in conjuntion with data partners and results are starting to reflect this disparity.

The findings in this category are primarily based on StopBadware's data, which is itself aggregated from Google, Sunbelt Software, and Team Cymru.



Conclusions

Social engineering is now acknowledged as a leading threat to organizations and businesses of all sizes with many the lacking the resources to control a multi-faceted problem. The rise of personal gadgets used within the workplace too brings its own set of problems. Key to countering cybercrime in its many forms and guises is raising awareness and educating users/employees/IT personnel about current threats and the places that they are likely to come from.

Our approach has always been to highlight the hosts that, unintentionally or otherwise, support the continuation of the threats that plague the Internet. We aim to promote the responsible hosting that the vast majority of hosts manage to achieve. However, it takes just a few hosts to tarnish the reputation of the many in the quest to follow the money without much due care and attention to anything else.

As for conclusions from the research for the Q3 2011 report there have been some changes that are worthy of a further mention.

For example, the changes within the Top 10 Bad Hosts this quarter means that it is no longer totally dominated by hosts in the United States, although the US is still the majority holder with 5 of the 10 worst performing service providers. Looking at the Top 50, the US share has now dropped to 16 from a previous high of 23 in Q2, a trend that we hope will continue further. Credit should be given to the relevant hosts who have 'cleaning up' and also to law enforcement for the part that it plays in this process.

Having said that, however, the #1 Bad Host is still a US based service provider, and although no stranger to the Top 10, it is a newcomer to the top position. At #1 now is AS33626 Oversee.net, for its hosting of malicious URLs, badware, Zeus botnet servers and infected sites. Oversee.net monetizes domain names and operates a number of other domain related businesses. According to recent press releases Oversee laid off 13 percent of its workforce in a move to 'realign its work force' as well as being embroiled in law suits from a former employee and a client.

To encourage the hosts who make an effort to 'clean up' their servers the Top 50 reports continue to include a 'Most Improved' section. The best in this category such as AS38333 Symbio Networks and AS5605 Netuse deserve to be congratulated. But of note too is former #1 Bad Host, and a regular in the Top 10 in previous quarters, AS29073 Ecatel now just out of the Top 50 altogether this quarter.

It is perhaps not surprising that a host in the overall position of #2 Bad Host, AS47583 Hosting-Media, should also find itself in the #1 spot in a category which HostExploit considers to be the most important in the analysis of malware, phishing or general badness, 'Exploit Servers.'

Hosts and corporate networks do not always host malicious activity with deliberate intent, but can deliver malware by servers that have been added to a network of zombies as a result of being hacked or compromised. Such networks caught up as 'Exploit Servers' can be used to further the outreach of noxious or virulent material by masking its true origin and, thus, helping to avoid detection.

Appendix 1.

Glossary

AS (Autonomous System):

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

Badware:

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

Blacklists:

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

Botnet:

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

CSRF (cross site request forgery):

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

DNS (Domain Name System):

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

DNSBL:

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

Exploit:

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

Hosting:

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

IANA (Internet Assigned Numbers Authority)

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

ICANN (Internet Corporation for Assigned Names and Numbers)

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

IP (Internet Protocol):

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

IPv4

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

IPv6

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

ISP (internet Service Provider):

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

LFI (Local File Inclusion):

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

MALfi (Malicious File Inclusion):

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

Malicious Links:

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

MX:

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

NS (Name Server):

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

Open Source Security:

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

Pharming:

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

Phishing:

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

Registry:

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

Registrars:

A domain name registrar is a company with the authority to register domain names, authorized by ICANN.

Remote File Inclusion (RFI):

A technique often used to attack Internet websites from a remote computer. With malicious intent, it can be combined with the usage of XSA to harm a web server.

Rogue Software:

Rogue security software is software that uses malware (malicious software) or malicious tools to advertise or install its self or to force computer users to pay for removal of nonexistent spyware. Rogue software will often install a trojan horse to download a trial version, or it will execute other unwanted actions.

Rootkit:

A set of software tools used by a third party after gaining access to a computer system in order to conceal the altering of files, or processes being executed by the third party without the user's knowledge.

Sandnet:

A sandnet is closed environment on a physical machine in which malware can be monitored and studied. It emulates the internet in a way which the malware cannot tell it is being monitored. Wonderful for analyzing the way a bit of malware works. A Honeynet is the same sort of concept but more aimed at attackers themselves, monitoring the methods and motives of the attackers.

Spam:

Spam is the term widely used for unsolicited e-mail. . Spam is junk mail on a mass scale and is usually sent indiscriminately to hundreds or even hundreds of thousands of inboxes simultaneously.

Trojans:

Also known as a Trojan horse, this is software that appears to perform or actually performs a desired task for a user while performing a harmful task without the user's knowledge or consent.

Worms:

A malicious software program that can reproduce itself and spread from one computer to another over a network. The difference between a worm and a computer virus is that a computer virus attaches itself to a computer program to spread and requires an action by a user while a worm is self-contained and can send copies of itself across a network.

XSA (Cross Server Attack):

A networking security intrusion method which allows for a malicious client to compromise security over a website or service on a server by using implemented services on the server that may not be secure.

Appendix 2

HE Index Calculation Methodology

October 13, 2011

1 Revision history

Rev.	Date	Notes
1.	December 2009	Methodology introduced.
2.	March 2010	IP significant value raised from 10,000 to 20,000.
3.	June 2010	Sources refined. Double-counting of Google Safebrowsing data through StopBadware eliminated. Source weightings refined.
4.	October 2011	Sources refined. Source weightings refined.

Table 1: Revision history

2 Motivation

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

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

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

3 Data sources

Data is taken from the following 11 sources.

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

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

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

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

Table 2: Data sources

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

4 Bayesian weighting

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

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

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

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

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

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

where:
B: *Bayesian ratio*
M: *number of IPs allocated to ASN*
M_a: *average number of IPs allocated in sample set*
N: *number of recorded instances*

N_a: *average number of recorded instances in sample set*
C: *IP weighting = 20,000*

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

5 Calculation

For each data source, three factors are calculated.

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

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

where:
B_m: *maximum Bayesian ratio*

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

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

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

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

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

where:
N_m: *maximum number of instances in sample set*

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

The index for each data source is then calculated as:

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

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

The overall HE Index is then calculated as:

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

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