ECYFED

ISBN: 978-0-9836249-2-9

HostExploit's Worldwide Cybercrime Series

Top 50 Bad Hosts and Networks 2nd Quarter 2012 - Report

"Data" - Graffiti Courtesy of cuatropiedos

GROUP IB
HOST exploit
CSIS

Abstract

Introduction

Over the quarter, cross-border collaboration has been successful in operations against long-standing cybercriminals.

Methods

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

Results

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

Discussion

The United States and Russia have by far the most publicly-routed ASes registered (14,178 and 3,760 respectively). With the competitiveness of hosting in these countries, it can be claimed that they will always be likely to host large amounts of malicious content, even in relative terms. The United States, however, has continued to improve and is now at #12 in the country rankings, whereas Russia has climbed to #1 rank. There is no obvious pattern in the deterioration of these Russian hosts.

Conclusion

The standing of Russian hosts in the Top 50 has continued to deteriorate while the situation for the United States has improved - with no hosts topping any category of malicious activity in this quarter.

Table of Contents

Top 50

CyberCrime Series

Bad Hosts and Networks

Supported by nominettrust
www.nominettrust.org.uk

Edited by

- Jart Armin

Review

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

Comparative Data

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

Contributors

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

ECYFED

European Cyber Security Federation

ECYFED - The transcontinental federation for cyber security investigation and threat elimination. CyberDefcon, Group-IB & CSIS.

About CyberDefcon

CyberDefcon is an independent organization dedicated to the pursuit of making the internet a safer place. The focus is on eliminating malicious internet activity at source. CyberDefcon offers a range of customized services and tools to suit individual client needs with an emphasis on applications for hosts and service providers.

About Group-IB

Group-IB is the first company in Russia and the former Soviet Union working professionally and comprehensively in cybercrime investigation, information security breaches, and computer forensics. As part of the company, a computer forensics lab provides independent computer forensic investigations, including for Russian law enforcement agencies. Created on the basis of Group-IB, the CERT-GIB computer emergency response team operates around the clock. Group-IB is part of LETA Group.

About CSIS

Four main principles drive the CSIS team: responsibility, mutual respect, proactive approach, and positive attitude.

This ethos pushes the business both internally and externally, equally with customers and in the way new challenges facing IT-security are tackled. These principles serve as values and help create the framework on which to base decisions and strategies. These form the foundation on which the business has been built.

CSIS was started in Denmark in 2003 and now has about 40 employees, spanning Copenhagen and Skanderborg. Everyone involved with CSIS has an important and indispensable role. Together we create synergy, which enables us to attract and retain leading profiles within the field of IT-security.

DISCLAIMER

Every reasonable effort has been made to assure that the source data for this report was up to date, accurate, complete and comprehensive at the time of the analysis. However, reports are not represented to be error-free and the data we use may be subject to update and correction without notice.

HostExploit or any of its partners including CyberDefcon, Group=IB and CSIS are not responsible for data that is misrepresented, misinterpreted or altered in any way. Derived conclusions and analysis generated from this data are not to be considered attributable to HostExploit or to our community partners.

Introduction

Editorial

Supporters of cross-border cooperation in the security industry have plenty to feel optimistic about this quarter with news of successful operations in several countries against long-standing habitual cybercriminals, each of which involves more than just an element of collaboration.

For too long cybercriminals have easily circumvented current laws bound by national territories. Lacking any vision of real change in international laws, in the near future at least, voluntary partnerships are leading the way in tackling some of the worst offenders in the cyber arena. (See the News Roundup for more on these stories.)

It would be an overstatement to imply that cybercriminals, relying on the vacuum in international laws and a given sense of assurance from virtual safe-harbors, may have had their day. However, the recent trend is certainly bad news for cybercriminals and, obviously, good news for all computer users.

Successes like these ensure that the momentum for voluntary cross-border collaboration continues as the value of information sharing at ground level increasingly proves its worth.

Here, then, is an opportune moment to announce such a venture. We are pleased to report the formation of ECYFED (European Cyber Security Federation) between our partners CyberDefcon, Group-IB and CSIS. Together, the mission is to resolve cyber threats and fight IT criminals as a combined unit of pooled resources. ECYFED is in its early stages of operational planning so keep up to date with our future ventures as more unfolds on the new website.

Jart Armin

Global Security Map

HostExploit ventures continue to expand as we build upon our reputation for supplying trusted and reliable data. If you haven't had a chance to check out the new Global Security Map (GSM), launched in April, then take a look now. The GSM has been well-received with useful feedback from a variety of sources. Plans are underway to expand its capabilities in a continuous cycle of improvements, so be sure to become a regular visitor of the Global Security Map website.

HostExploit Data Partners are Growing

This quarter HostExploit is pleased to the addition of data from new partner, C-SIRT (Cyscon SIRT), a provider of "Security Incident Reporting Service" for malware, phishing and other security related incidents. C-SIRT is widely respected throughout the computer security industry for its detection of suspicious code and will provide added value to HostExploit data and reports.

News Roundup

Transnational Cooperation Defeating Cybercrime

Several gangs and major cybercriminal users of the Carberp virus were apprehended in recent months. This is a major coup for all those involved, not least the central investigator, Group-IB, as well as its various partners in each of the operations.

Carberp, well-known for its capabilities against online banking systems and ecommerce websites, has plagued online financial systems since at least 2009. The criminal enterprises behind the virus have amassed huge earnings, estimated to be as much as several million USD per week. Disrupting these activities became a high priority for Russian financial systems, as the main target of the activities, but banks in several countries were also victims of the Carberp trojan.

The arrest of the first Carberp gang was carried out in March by members of the Russian Interior Ministry (MVD). The criminal gang of eight is reported to have used a combination of Win32/Carberp and Win/32RDPdoor to gain access to personal computers and a large number of online banking systems. This highly organized outfit rented an office under the guise of a legal enterprise and used a number of mules to cash money at various ATMs in Moscow.

In early June came further arrests in connection with Carberp, again as a result of cross-border collaboration with analysts from Group-IB, ESET and others. This time the infamous Hodprot gang, active since 2008 and estimated to be responsible for more than $3.7 million in losses from online bank accounts, were neutralized by specialist forces from the Russian MVD as part of investigations into the theft of funds from Sherbank financial systems.

Later in June, Group-IB reported on the third arrest of Carberp-using criminals. Agents from Department K and MVD raided a residence in Moscow, seizing computers and other evidence of involvement in criminal activity. One of the largest ever botnet operations, said to have been going on for more than three years, had been uncovered. This version of Carberp had been customized to enable vouchers from foreign Facebook users to be stolen.

Known by the online names of Germes and Arashi, the operators created a multimillion banking botnet called Origami in hacker circles. They were the first to use the RDPdoor malware to steal directly from online banking clients and the first to use a version of Carberp with a bootkit as a means of avoiding anti-virus tools. The gang successfully switched from using Blackhole exploits to Nuclear Pack to increase the number of compromised computers to around 6 million in May 2012.

Although this string of successful arrests was brought about in Russia, the operations involved extensive participation with researchers in several countries. Few cybercriminal activities can claim to be exclusive to an individual country when online systems invariably cross virtual borders. Take, for example, the FBI takedown of the international carding operation announced on June 26 where eleven US citizens were arrested in one night with another eleven coordinated arrests in the UK, Bosnia, Bulgaria, Norway and Germany. A number of other countries were involved in the investigations of this truly international operation.

In Bulgaria the police took action against a hacker group known as 'Cyber Warrior Invasion', responsible for more than 500 attacks on websites worldwide including major financial companies, following an investigation lasting several months. The gang used 'zombie' proxy servers to disguise their true location and stole data and credit card information. Raids took place in several locations in Bulgaria and equipment was confiscated. One computer system seized by police held a database of stolen mailboxes and social network user profiles together with passwords. This information had been the subject of attempted blackmail and extortion.

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

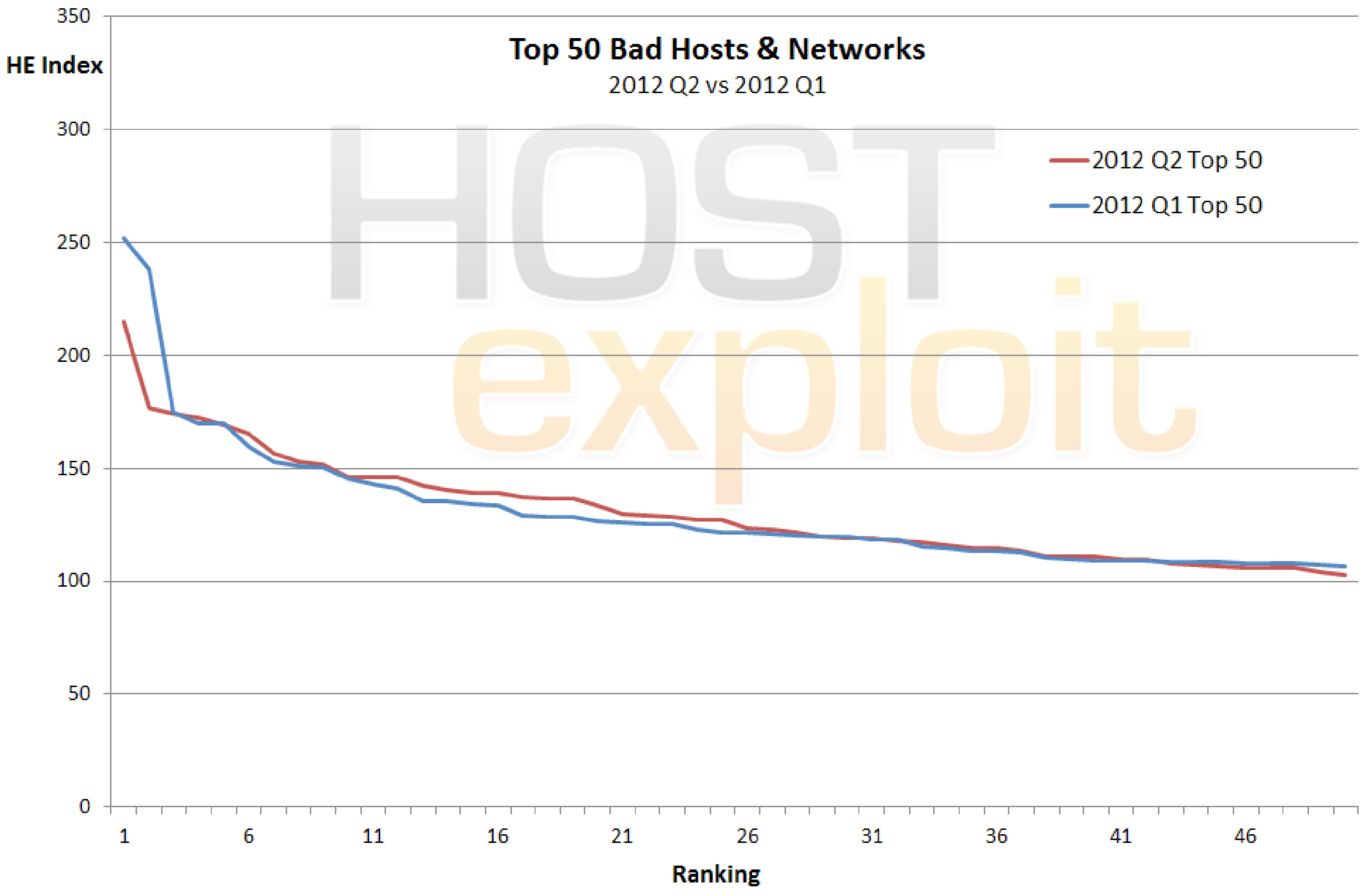
Want to be Involved?

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

4. The Top 50

HE Rank	HE Index	AS number	AS name	Country	# of IPs
▲ 1	214.67	41947	WEBALTA-AS OAO Webalta	RU	14,624
▲ 2	176.84	44112	SWEB-AS SpaceWeb JSC	RU	3,072
▲ 3	174.31	45538	ODS-AS-VN Online data services	VN	9,472
▲ 4	172.17	29073	ECATEL-AS AS29073, Ecatel Network	NL	13,312
▼ 5	168.94	16138	INTERIAPL INTERIA.PL Sp z.o.o.	PL	4,096
▲ 6	165.34	39743	VOXILITY-AS Voxility SRL	RO	21,760
▲ 7	156.84	28753	LEASEWEB-DE Leaseweb Germany GmbH	DE	119,040
▲ 8	152.81	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	50,432
▲ 9	151.70	9891	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	TH	19,456
▲ 10	146.33	50465	IQHOST IQHost Ltd	RU	2,816
▼ 11	146.24	16125	DC-AS UAB Duomenu Centras	LT	5,376
▼ 12	145.81	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	50,432
▲ 13	142.53	48031	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	UA	17,664
▲ 14	140.29	43146	AGAVA3 Agava Ltd.	RU	18,176
▲ 15	139.24	43362	MAJORDOMO MAJORDOMO LLC	RU	2,560
▼ 16	138.95	32475	SINGLEHOP-INC - SingleHop	US	295,168
▲ 17	137.25	47781	ANSUA-AS DELTA-X Ltd	UA	1,536
▲ 18	136.49	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	86,016
▼ 19	136.35	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	1,218,048
▲ 20	133.78	48159	TIC-AS Telecommunication Infrastructure Company	IR	2,048
▲ 21	129.49	35415	WEBAZILLA WebaZilla European Network	CY	63,488
▼ 22	128.95	24940	HETZNER-AS Hetzner Online AG RZ	DE	570,368
▲ 23	128.76	16265	LEASEWEB LeaseWeb B.V.	NL	331,776
▼ 24	127.45	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,539,328
▲ 25	127.07	44368	ASDELTAMANAGEMENT DELTA MANAGEMENT AB	SE	3,072
▶ 26	123.43	34201	PADICOM PADICOM SOLUTIONS SRL	RO	6,400
▲ 27	123.00	15169	GOOGLE - Google Inc.	US	562,688
▲ 28	121.30	38731	VTDC-AS-VN Vietel - CHT Compamy Ltd	VN	33,024
▲ 29	119.99	21788	NOC - Network Operations Center Inc.	US	297,216
▲ 30	119.10	9931	CAT-AP The Communication Authoity of Thailand, CAT	TH	209,408
▲ 31	118.79	6939	HURRICANE - Hurricane Electric, Inc.	US	736,512
▲ 32	118.15	48716	PS-AS PS Internet Company Ltd.	RU	512
▲ 33	117.18	29671	SERVAGE Servage GmbH	DE	12,288
▲ 34	115.85	40676	PSYCHZ - Psychz Networks	US	26,624
▼ 35	114.74	9809	NOVANET Nova Network Co.Ltd... Futian District, Shenzhen, China	CN	10,752
▲ 36	114.57	49335	NCONNECT-AS Navitel Rusconnect Ltd	RU	12,288
▼ 37	113.72	16276	OVH OVH Systems	FR	937,216
▲ 38	111.04	12695	DINET-AS Digital Network JSC	RU	298,624
▼ 39	111.00	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	113,033,184
▲ 40	110.84	57169	EDIS-AS-EU EDIS GmbH	AT	7,936
▼ 41	109.83	32613	IWEB-AS - iWeb Technologies Inc.	CA	235,520
▲ 42	109.72	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	CN	53,795,584
▼ 43	107.54	32181	ASN-GIGENET - GigeNET	US	42,240
▲ 44	107.24	44553	SNS-BG-AS Smart Network Solutions Ltd.	BG	3,840
▲ 45	106.71	29182	ISPSYSTEM-AS ISPsystem Autonomous System	LU	39,168
▲ 46	105.97	35569	PETERHOST-MOSCOW Concorde Ltd.	RU	2,048
▲ 47	105.75	26105	Telecarrier, Inc	PA	44,608
▼ 48	105.70	55740	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM...	IN	262,144
▼ 49	103.89	22489	CASTLE-ACCESS - Castle Access Inc	US	47,872
▼ 50	103.06	33626	OVERSEE-DOT-NET - Oversee.net	US	3,840

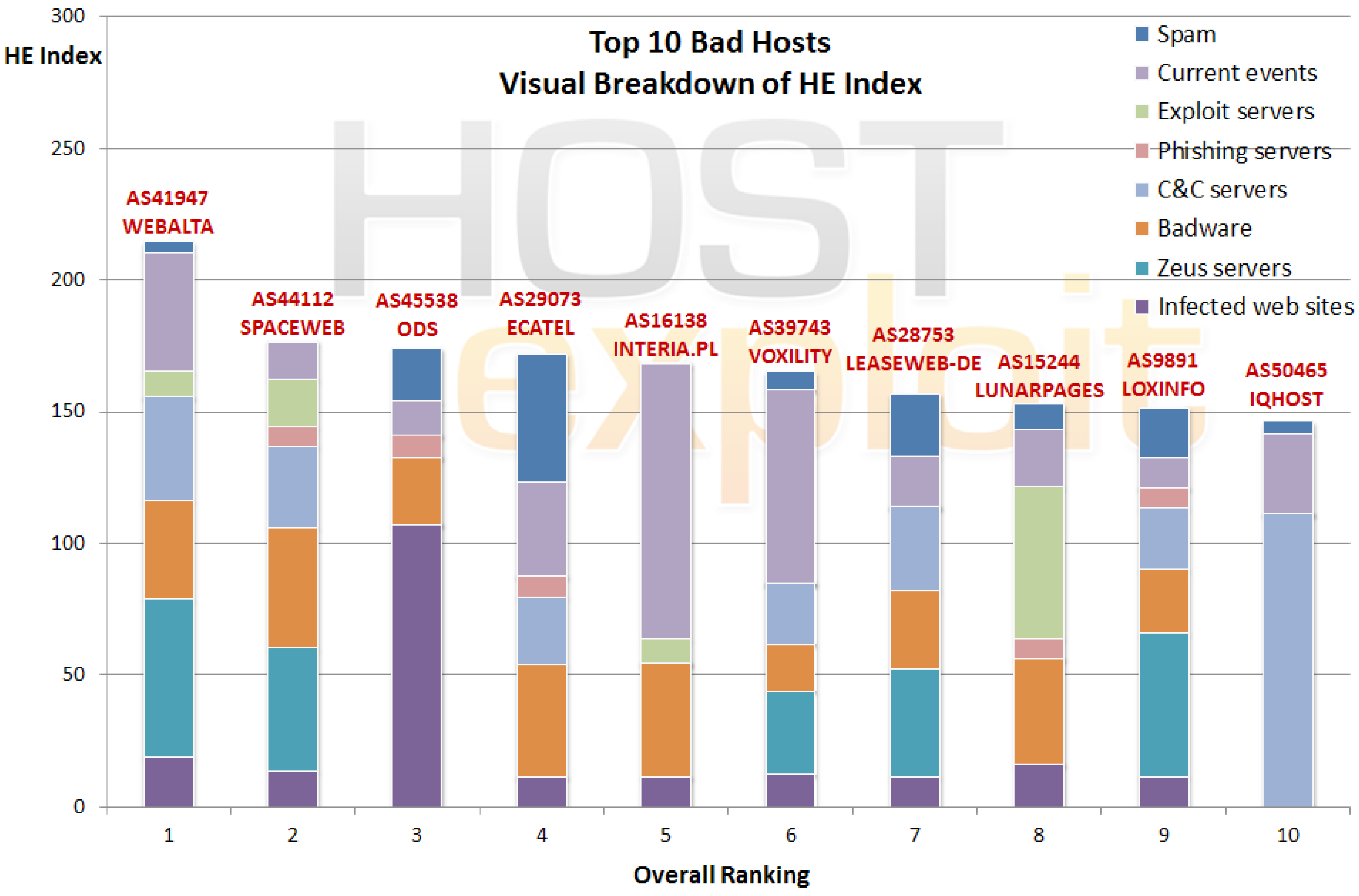
2012 Q2 to 2012 Q1 Comparison



A comparison of the 'Top 50 Bad Hosts' in June 2012 with March 2012.

Despite several large movements of hosts in the Top 50, the overall distribution of concentrations of malicious activity has remained almost identical.

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 AS41947 WEBALTA was ranked # 4 in Q1 2012, now is ranked #1 due to high concentrations of badware and current events (including XSS and RFI).

AS45538 ODS (Vietnam), on the other hand, is now ranked #3 (q1 2012 was #186) almost entirely due to very large concentrations of infected web sites.

7.

What's New?

7.1. Overview

	Previous Quarter - Q1 2012			Current Quarter - Q2 2012		
	ASN	**Name**	**Country**	**ASN**	**Name**	**Country**
#1	**16138**	Interia.pl	PL	**41947**	Webalta	RU
#2	**47583**	Hosting Media	LT	**44112**	SWEB	RU
#3	**33182**	HostDime	US	**45538**	ODS	VN
#1 for Spam	**31133**	MegaFon	RU	**41859**	TIC	IR
#1 for Botnets	**47583**	Hosting Media	LT	**50465**	IQHost	RU
#1 for Zeus Botnet	**16125**	Duomenu Centras	LT	**34201**	Padicom	RO
#1 for Phishing	**9280**	Connect Infobahn Australia	AU	**43362**	Majordomo	RU
#1 for Exploit Servers	**3.537**	Infium	UA	**2607**	Slovak Academic Network	EU
#1 for Badware	**9809**	Nova Network	CN	**9809**	Nova Network	CN
#1 for Infected Sites	**16138**	Interia.pl	PL	**45538**	Online data services	VN
#1 for Current Events	**16138**	Interia.pl	PL	**16138**	Interia.pl	PL

An analysis of quarterly trends gives an insight into how highly hosting providers rate responsible hosting.

For a responsible host, the shock of finding they are ranked unusually high, or even worse in the #1 position, can be enough to prompt immediate remedial action.

It would be comforting to think that responsible hosting is the reason for changes to #1 positions in several individual categories. Sadly, many former #1s have slipped only a few places enabling some less familiar names to achieve the dubious accolade at the top of the table. The new title holders nonetheless deserve their ranks, displaying high concentrations of badness. Meanwhile, AS9809 Novanet and AS16138 Interia are resolutely sticking to their #1 placements for Badware and Current Events respectively.

7.2. Top 10 Newly-Registered Hosts - In Q2 2012

By end of Q2 2012 there were **41,635** ASes; an increase of **957** from end of Q1 2012.

Below we show a selection of 10 ASes registered in Q2 2012 with the highest HE Indexes. With significant levels of badness recorded in a short period of time, these hosts are of interest.

Listed below the 10 Q1 ASes are the same findings in the previous two quarterly reports.

It is interesting to note that in the last 3 quarterly reports, of the 30 newly-registered ASes we have highlighted as being of interest, 6 of these no longer exist.

Period	HE Rank	HE Index	AS number	AS name	Country	# of IPs
2012 Q2	**107**	**84.5**	**57668**	SANTREX-AS Santrex Internet Services Ltd.	**GB**	1,280
	1,090	**38.2**	**39365**	MICROLINES-AS MICROLINES ISP	**LV**	8,192
	1,201	**35.6**	**57972**	WEBEXXPURTS Deepak Mehta FIE	**EE**	10,752
	1,485	**30.5**	**132241**	SKSATECH1-MY SKSA TECHNOLOGY SDN BHD	**MY**	1,024
	1,731	**26.4**	**34934**	UKFAST UKFast.Net Ltd	**GB**	27,648
	1,789	**25.7**	**33667**	CMCS - Comcast Cable Communications, Inc.	**US**	0
	1,863	**24.8**	**33659**	CMCS - Comcast Cable Communications, Inc.	**US**	8,192
	2,057	**23.0**	**54444**	AVESTA-NETWORKS-LLC - Avesta Networks LLC	**US**	6,144
	2,338	**20.6**	**132116**	ANINETWORK-IN Ani Network Pvt Ltd	**IN**	1,024
	2,440	**20.0**	**34170**	AZTELEKOM Azerbaijan Telecomunication ISP	**AZ**	36,096
2012 Q1	**274**	**67.0**	**48031**	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	**UA**	16,640
	653	**50.8**	**12327**	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business international	**GB**	4,608
	906	**44.6**	**49087**	PODCEM-AS Open JSC "Podilskiy Tcement"	**UA**	256
	1,337	**35.3**	**24768**	ALMOUROLTEC ALMOUROLTEC SERVICOS DE INFORMATICA E...	**PT**	2,048
	1,828	**27.8**	**51699**	ANTARKTIDA-PLUS-AS Antarktida-Plus LLC	**UA**	256
	1,875	**27.3**	**49236**	RELNET-AS TOV "Leksim"	**UA**	256
	1,948	**26.4**	**57704**	SPEED-CLICK-LTD SpeedClick for Information Technology and...	**IL**	2,048
	2,053	**25.4**	**31408**	ORANGE-PALESTINE Orange Palestine Group Co. for Technological...	**PS**	1,024
	2,212	**24.0**	**37385**	SONITEL	**NE**	8,960
	2,260	**23.7**	**34109**	AS34109 CB3ROB Ltd. & Co. KG	**NL**	9,216
2011 Q4	**740**	**46.7**	**21508**	COMCAST-21508 - Comcast Cable Communications Holdings, Inc	**US**	256
	1,356	**34.0**	**4213**	VPLSNET-EAST - VPLS Inc. d	**US**	2,048
	1,644	**29.2**	**27626**	AS-JOYTEL - Joytel	**US**	1,024
	1,986	**25.2**	**57374**	GIV-AS Commercial radio-broadcasting company Cable operator...	**MK**	7,168
	2,063	**24.4**	**47311**	ASBRESTRW Transport Republican unitary enterprise...	**BY**	256
	2,181	**23.6**	**4.459**	--No Registry Entry--	**BR**	256
	2,189	**23.5**	**43463**	BST-AS Biuro sprendimu tinklas UAB	**LT**	3,072
	2,406	**21.9**	**57446**	TELEMONT-AS Telemont Service S.R.L.	**EU**	4,096
	2,596	**20.6**	**28015**	MERCO COMUNICACIONES	**AR**	22,528
	2,905	**18.7**	**3.961**	ENERGOMONTAZH-AS ENERGOMONTAZH ltd.	**EU**	256

7.3. Improved Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
-78.4%	**2**	238.2	**600**	51.4	**47583**	HOSTING-MEDIA Aurimas Rapalis "II Hosting Media"	**LT**	4,096
-75.1%	**107**	86.0	**2,239**	21.4	**197145**	ASINFIUM Infium Ltd.	**UA**	9,728
-74.5%	**72**	94.1	**1,933**	24.0	**13174**	MTSNET OJSC "Mobile TeleSystems" Autonomous...	**RU**	26,368
-72.9%	**127**	80.0	**2,208**	21.7	**25159**	SONICDUO-AS AS for MegaFon-Moscow	**RU**	10,240
-66.7%	**135**	78.5	**1,757**	26.1	**48587**	NET-0X2A-AS Private Entrepreneur Zharkov Mukola...	**UA**	1,024
-64.5%	**48**	107.8	**1,091**	38.2	**27990**	Hosting Panama	**PA**	5,632
-63.2%	**90**	88.7	**1,354**	32.6	**24203**	NAPXLNET-AS-ID PT Excelcomindo Pratama...	**ID**	22,528
-63.2%	**115**	82.8	**1,484**	30.5	**27956**	Cyber Cast International, S.A.	**PA**	3,840
-61.5%	**60**	100.1	**1,080**	38.5	**31163**	MF-KAVKAZ-AS JSC MegaFon	**RU**	5,632
-60.7%	**87**	89.9	**1,213**	35.4	**13301**	UNITEDCOLO-AS UNITED COLO GmbH	**DE**	66,816

The hosts in the above table have all demonstrated a dramatic reduction in levels of badness in the three months since our Q1 2012 report was published.

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

Noteworthy improvements include:

- AS47583 HOSTING-MEDIA Aurimas Rapalis "II Hosting Media" (Lithuania) down from #2 to #600. This is a welcome and remarkable reduction, as this host has been within the top 50 bad hosts for many previous reports.
- AS197145 ASINFIUM Infium Ltd. (Ukraine), with a large drop of 75.1% in HE Index, bringing it down to #2,239 from #107. This is due to the elimination of 'exploit servers' for Black Hole Exploit, plus others, however it is still reported as hosting ICE9 Botnet C&Cs

7.4. Deteriorated Hosts

Change	Previous Quarter		Current Quarter		AS number	AS name	Country	# of IPs
	Rank	Index	Rank	Index				
12888.0%	30,182	1.0	20	133.8	48159	Telecommunication Infrastructure Company	IR	2,048
12044.3%	35,872	0.9	44	107.2	44553	SNS-BG-AS Smart Network Solutions Ltd.	BG	3,840
1342.1%	5,445	8.2	32	118.2	48716	PS-AS PS Internet Company Ltd.	RU	512
429.4%	2,216	24.0	25	127.1	44368	ASDELTAMANAGEMENT DELTA MANAGEMENT	SE	3,072
275.6%	2,343	23.3	92	87.4	11042	LANDIS-HOLDINGS-INC - Landis Holdings Inc	US	28,416
244.5%	1,459	33.3	36	114.6	49335	NCONNECT-AS Navitel Rusconnect Ltd	RU	12,288
238.6%	2,167	24.4	116	82.7	34941	CYBERCOM-AS CyberCom & YT AB	SE	2,048
209.7%	2,054	25.4	135	78.8	50939	SPACE-AS Space Ro Srl	RO	1,792
207.4%	1,792	28.3	95	87.1	47894	VERITEKNIK VeriTeknik Bilisim Ltd.	TR	4,096
201.7%	2,086	25.2	153	76.0	47781	ANSUA-AS DELTA-X Ltd	UA	1,536

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

The "standout" host this quarter is AS48159 Telecommunication Infrastructure Company (Iran) with a dramatic rise in the rankings from over #30,182 (of 41,635) to #20. This is solely due to becoming the #1 host for spam worldwide.

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

Top 10 Countries

Our new methodology more accurately determines the badness levels present on ASes in a particular country. This brings its own set of challenges, such as the impossibility of correctly determining physical server locations in an automated fashion.

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

We are now effectively treating each country as an individual AS, by totalling the number of IPs and badness instances across all ASes registered to that country. We then calculate an index for each country using a similar methodology to that for individual ASes.

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

The below table shows the resulting Top 10 countries from this methodology: This table is a small sample of the results available on the Global Security Map website where a full list of countries and rankings can be found.

Country Details			Country Scoring	
Code	**Name**	**Total IPs**	**Rank**	**Index**
RU	RUSSIAN FEDERATION	50,552,160	1	359.3
LU	LUXEMBURG	1,104,128	2	315.6
LV	LATVIA	1,770,752	3	255.8
UA	UKRAINE	14,088,192	4	251.5
VG	VIRGIN ISLANDS, BRITISH	11,264	5	247.1
TH	THAILAND	16,298,225	6	233.9
TR	TURKEY	20,522,752	7	233.7
RO	ROMANIA	12,217,344	8	229.5
MD	MOLDOVA, REPUBLIC OF	1,126,400	9	225.5
NL	NETHERLANDS	23,865,088	10	209.7

9.

The Good Hosts

HE Rank	HE Index	AS number	AS name	Country	# of IPs
36,966	0.520	3300	BT-INFONET-EUROPE BT-Infonet-Europe	SE	700,288
34,085	0.592	38333	SYMBIO-AS-AU-AP Symbio Networks	AU	139,360
31,424	0.610	42362	ALANIA-AS Sevosetinelectrosvyaz	RU	112,640
31,076	0.618	10970	LIGHTEDGE - LightEdge Solutions	US	103,680
31,073	0.619	7821	ZAYO-MN - Onvoy	US	102,912
30,463	0.630	14390	CORENET - Coretel America, Inc.	US	92,672
12,218	0.664	262914	Comision Federal de Electricidad	MX	68,864
12,176	0.670	16360	SATLYNX_GMBH Satlynx GmbH	DE	66,048
11,971	0.671	18268	JANIS Naganoken Kyodou Densan Co.Ltd.	JP	65,536
11,966	0.688	8641	NAUKANET-AS LLC Nauka-Svyaz	RU	57,600

9.1. Why List Examples of Good Hosts?

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

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

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

9.2. Selection Criteria

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

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

10.

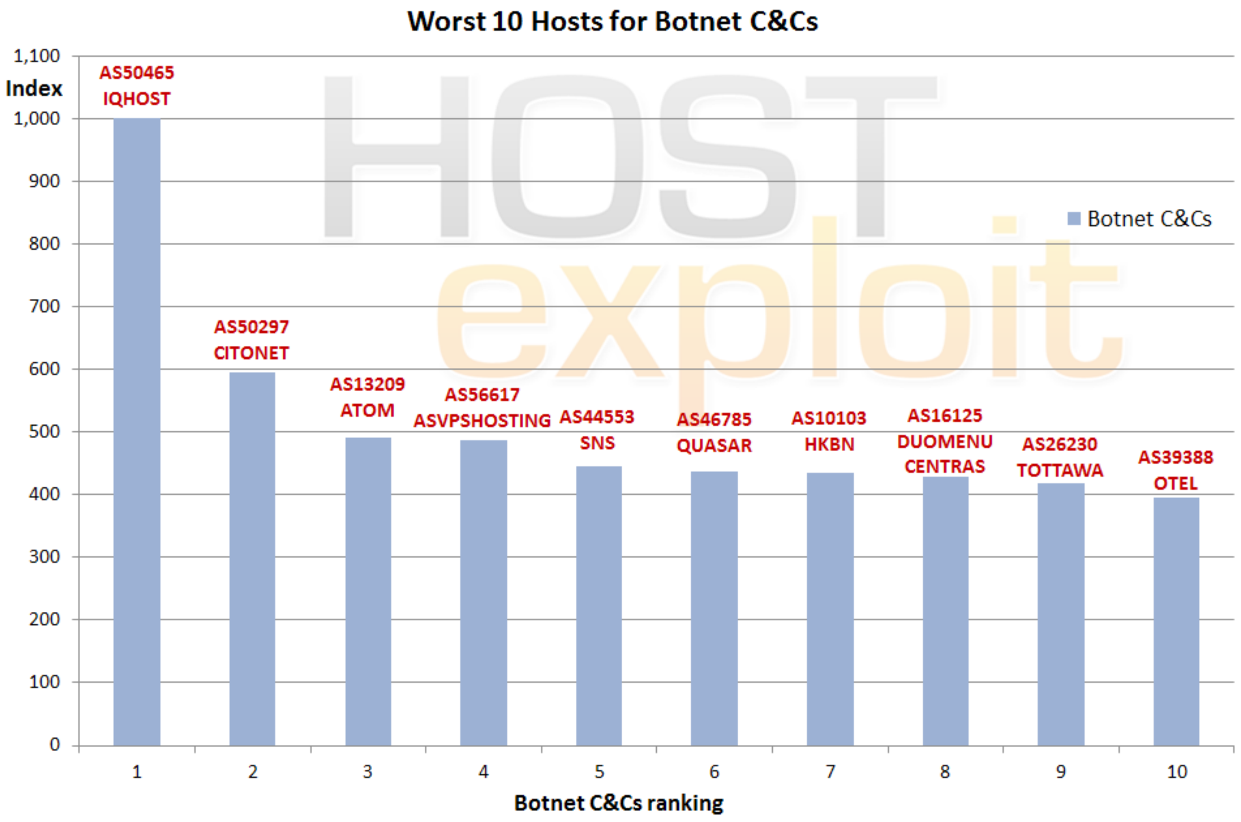
Bad Hosts by Topic

10.1.1. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
10	146.3	**50465**	IQHOST IQHost Ltd	**RU**	2,816	**1,000.0**
190	71.0	**50297**	CITONET Centr Informacionnyh Technologii, Ltd.	**UA**	5,120	**596.1**
250	66.6	**13209**	ATOM-HOSTING Atom Hosting SRL	**RO**	768	**491.7**
434	56.5	**56617**	ASVPSHOSTING SIA "VPS Hosting"	**LV**	1,024	**487.4**
44	107.2	**44553**	SNS-BG-AS Smart Network Solutions Ltd.	**BG**	3,840	**446.4**
160	75.1	**46785**	QUASAR-DATA-CENTER - QUASAR DATA CENTER, LTD.	**US**	4,608	**436.8**
323	61.6	**10103**	HKBN-AS-AP HK Broadband Network Ltd.	**HK**	19,712	**435.9**
11	146.2	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,376	**427.8**
104	84.8	**26230**	TOTTAWA - Telecom Ottawa Limited	**CA**	22,272	**419.2**
153	76.0	**39388**	OTEL-AS Forcraft Ltd.	**BG**	8,704	**394.5**

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.

AS50465 IQHOST (Russian Federation) tops this category for the exceptionally large number of C&C found on its servers. AS44553 SNS Smart Networks Solutions Ltd has jumped up the positions to make it to #5 in this table and #43 in the overall positions. This is a first time in the top 50 and a decline from #35872 in Q1.

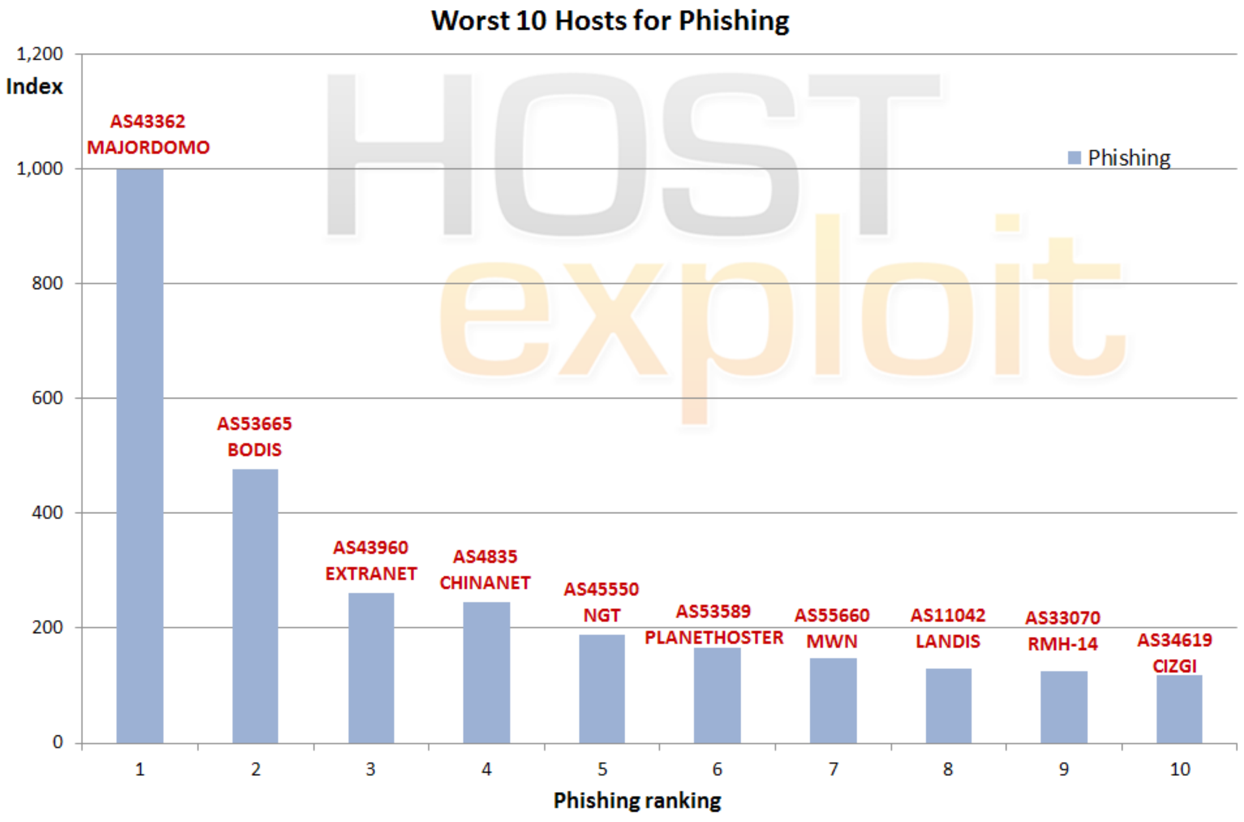


10.1.2. Phishing Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
15	139.2	**43362**	MAJORDOMO MAJORDOMO LLC	**RU**	2,560	**1,000.0**
309	62.6	**53665**	BODIS-1 - Bodis, LLC	**CN**	1,024	**477.3**
2,449	19.9	**43960**	EXTRANETCTC Consorzio Terrecablate	**IT**	2,048	**260.3**
314	62.3	**4835**	CHINANET-IDC-SN China Telecom (Group)	**CN**	103,456	**244.2**
1,453	30.8	**45550**	NGT-AS-VN New Generations Telecommunications Corporation	**VN**	1,280	**188.9**
737	47.6	**53589**	PLANETHOSTER-8 - PlanetHoster	**CA**	3,328	**165.8**
760	46.8	**55660**	MWN-AS-ID PT Master Web Network	**ID**	1,280	**148.6**
92	87.4	**11042**	LANDIS-HOLDINGS-INC - Landis Holdings Inc	**US**	28,416	**128.9**
138	78.6	**33070**	RMH-14 - Rackspace Hosting	**US**	512,768	**125.7**
73	93.3	**34619**	CIZGI Cizgi Telekomunikasyon Hizmetleri Sanayi Ve Ticaret...	**TR**	28,672	**118.0**

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

This quarter it is all change for the top ten in this category with big movements up the table for AS43960 EXTRANETCTC (Italy) for high levels of phishing servers. Note the presence of AS53665 BODIS in the #2 slot, registered in China but routed from the United States. At the #1 spot, AS43362 MAJORDOMO (Russia) has exceptionally high levels of phishing servers.



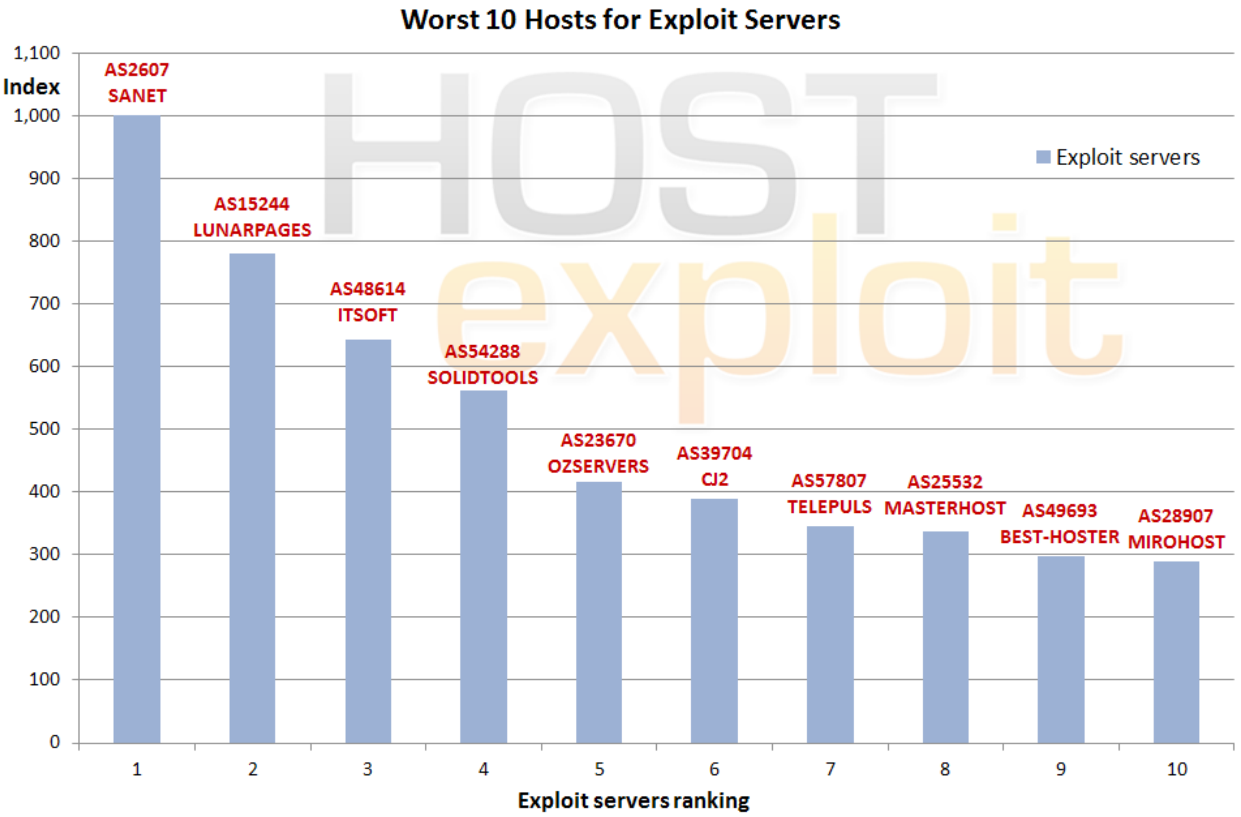
10.1.3. Exploit Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
54	102.6	**2607**	SANET Slovak Academic Network	**EU**	526,080	**1,000.0**
8	152.8	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	**US**	50,432	**780.4**
135	78.8	**48614**	ITSOFT-AS ITSoft Ltd.	**RU**	2,048	**643.9**
486	55.2	**54288**	SOLIDTOOLSINC - SolidTools Technology, Inc.	**US**	16,640	**562.7**
171	73.7	**23670**	OZSERVERS-AU Oz Servers, Data Centres, Australia Wide	**AU**	16,384	**415.7**
198	70.7	**39704**	CJ2-AS CJ2 Hosting&Development	**NL**	6,400	**389.5**
815	45.0	**57807**	TELEPULS-AS Telepuls "Spider" sp. z o.o. S.K.A.	**PL**	6,656	**345.8**
62	97.4	**25532**	MASTERHOST-AS .masterhost autonomous system	**RU**	77,824	**338.0**
122	81.7	**49693**	BEST-HOSTER Best-Hoster Group Co. Ltd	**RU**	2,048	**298.0**
151	76.4	**28907**	MIROHOST Internet Invest Ltd.	**UA**	11,776	**289.3**

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

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

Note that this table consists of a new set of hosting providers from Q1. Large position changes in this category can be as a result of exploits served from compromised servers. AS2607 SANET moved from #940 in Q1 to #52 in Q2 due to a high concentration of exploit servers and the reason for its #1 placing here.



10.1.4. Botnet Hosting - Zeus

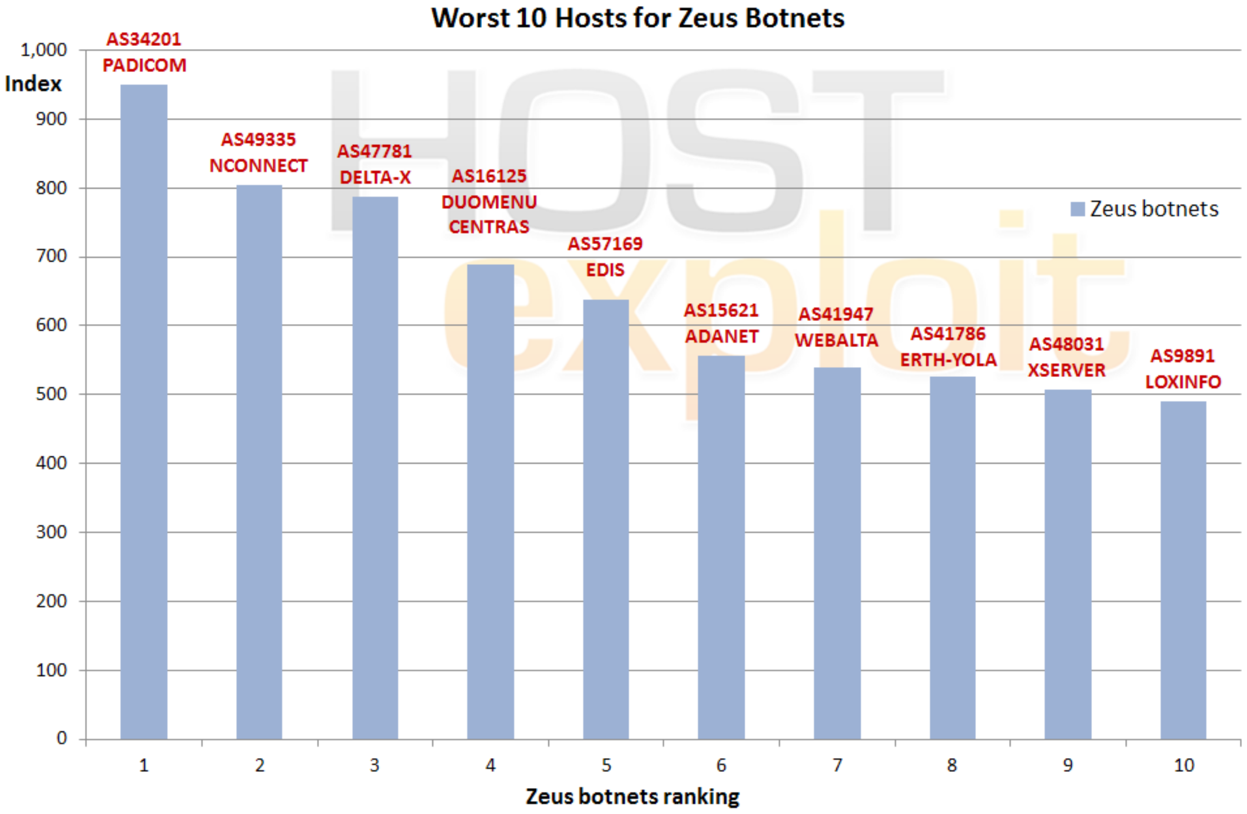
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
26	123.4	**34201**	PADICOM PADICOM SOLUTIONS SRL	**RO**	6,400	**950.0**
36	114.6	**49335**	NCONNECT-AS Navitel Rusconnect Ltd	**RU**	12,288	**804.1**
17	137.2	**47781**	ANSUA-AS DELTA-X Ltd	**UA**	1,536	**787.2**
11	146.2	**16125**	DC-AS UAB Duomenu Centras	**LT**	5,376	**688.3**
40	110.8	**57169**	EDIS-AS-EU EDIS GmbH	**AT**	7,936	**637.4**
64	97.0	**15621**	ADANET-AS Azerbaijan Data Network	**RU**	13,312	**556.1**
1	214.7	**41947**	WEBALTA-AS OAO Webalta	**RU**	14,624	**540.1**
141	78.3	**41786**	ERTH-YOLA-AS CJSC "ER-Telecom Holding"	**RU**	36,096	**526.5**
13	142.5	**48031**	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich	**UA**	17,664	**507.2**
9	151.7	**9891**	CSLOX-IDC-AS-AP CS LOXINFO Public Company Limited.	**TH**	19,456	**490.3**

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 upwards of 250,000 slave machines. The Zeus botnet remains the cheapest and most popular botnet on the underground market.

This section should be considered in conjunction with Section 10.1.3 on Exploit Servers.

The stand out feature in this category is the prevalence of service providers registered in Eastern European countries. Some of the well-known names have shifted a few places in either direction making way for the appearance of Russian registered AS49335 NCONNECT Navitel Rusconnect Ltd.

AS41947 Webalta holds on to a top ten position in this category for the hosting of Zeus and C&Cs.



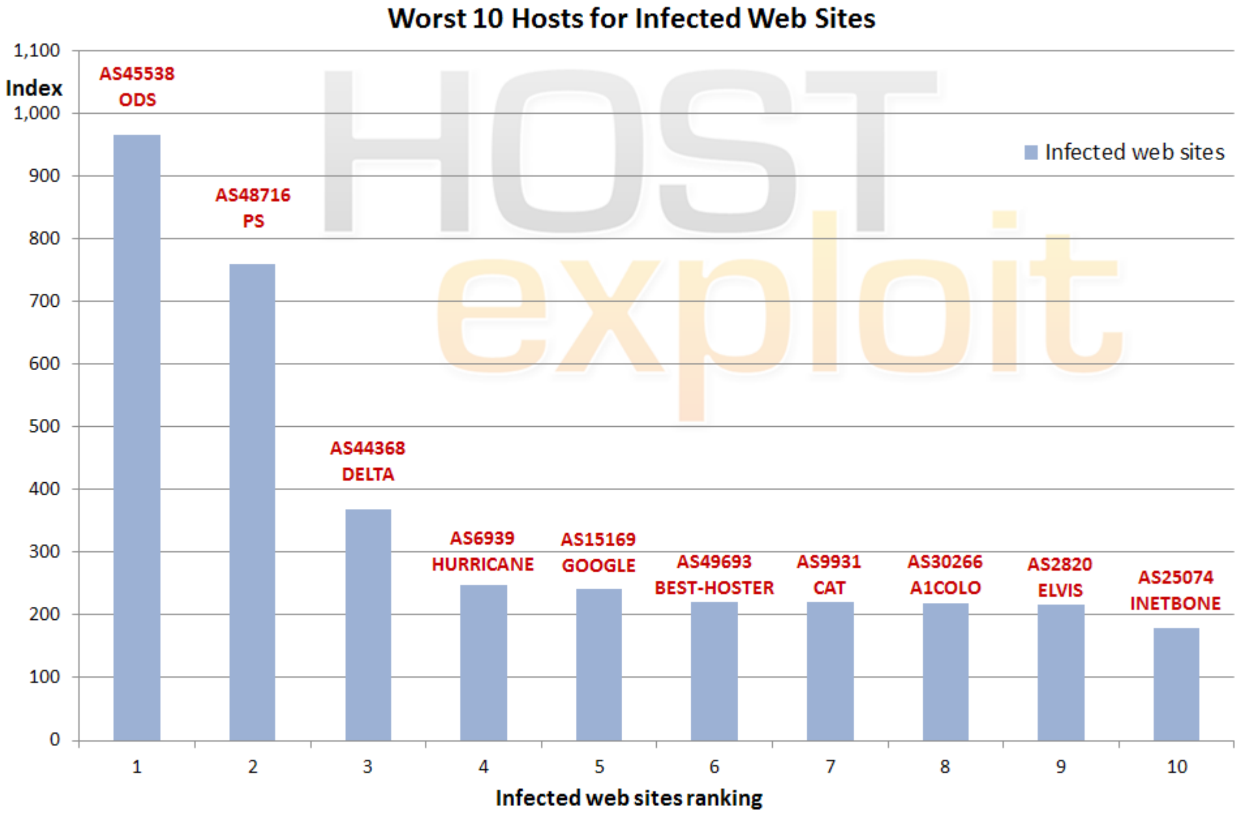
10.2.1. Infected Web Sites

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
3	174.3	**45538**	ODS-AS-VN Online data services	**VN**	9,472	**965.8**
32	118.2	**48716**	PS-AS PS Internet Company Ltd.	**RU**	512	**758.6**
25	127.1	**44368**	ASDELTAMANAGEMENT DELTA MANAGEMENT AB	**SE**	3,072	**368.0**
31	118.8	**6939**	HURRICANE - Hurricane Electric, Inc.	**US**	736,512	**247.4**
27	123.0	**15169**	GOOGLE - Google Inc.	**US**	562,688	**241.1**
122	81.7	**49693**	BEST-HOSTER Best-Hoster Group Co. Ltd	**RU**	2,048	**221.4**
30	119.1	**9931**	CAT-AP The Communication Authoity of Thailand, CAT	**TH**	209,408	**220.3**
303	63.0	**30266**	A1COLO-COM - A1COLO.COM	**US**	8,192	**217.8**
887	43.5	**2820**	ELVIS-AS ZAO "Elvis-Telecom"	**RU**	51,712	**216.4**
58	100.1	**25074**	INETBONE-AS MESH GmbH	**DE**	104,960	**179.1**

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

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

This quarter a number of less familiar names accompany a few well known ones. The #1 position of AS45538 ODS Online Data Services in the Infections table reveals why this provider has shot to #3 in the overall rankings.



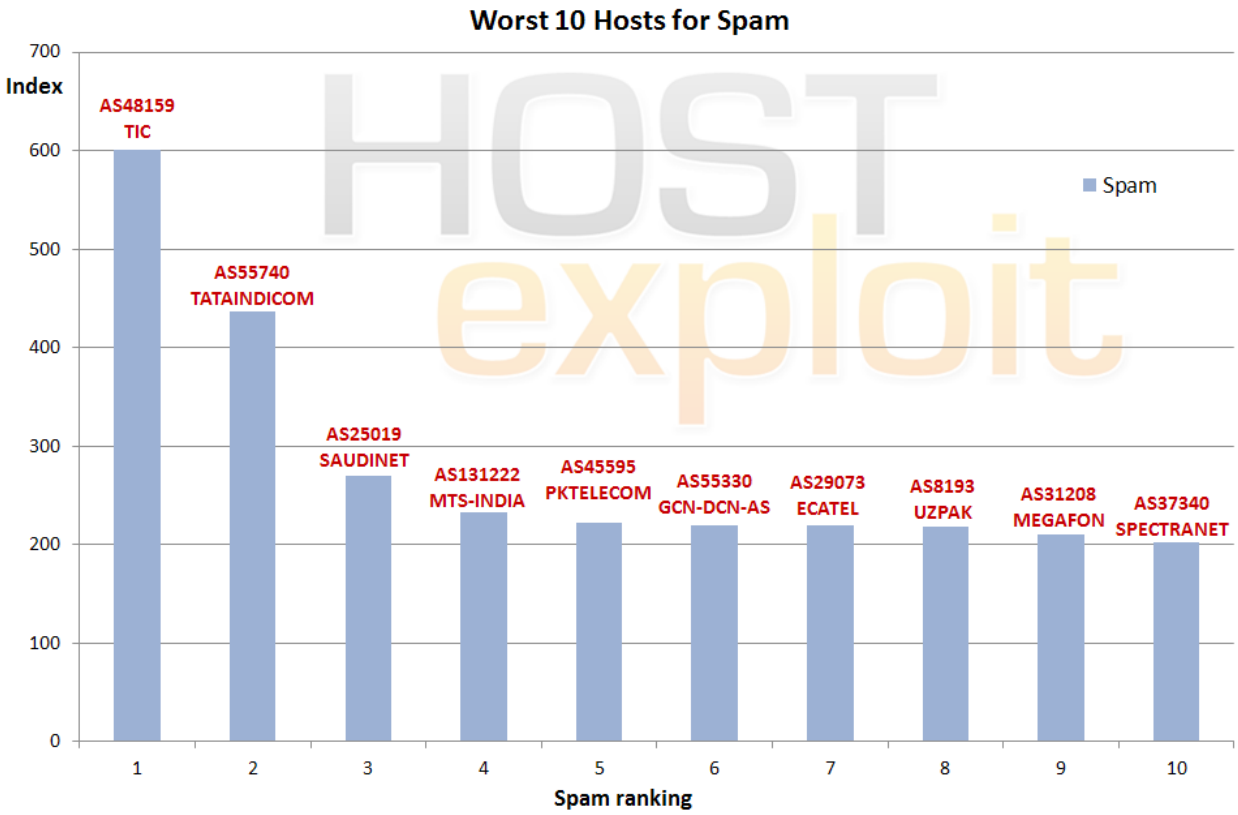
10.2.2. Spam

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
20	133.8	**48159**	TIC-AS Telecommunication Infrastructure Company	**IR**	2,048	**601.1**
48	105.7	**55740**	TATAINDICOM-IN TATA TELESERVICES LTD - TATA INDICOM	**IN**	262,144	**436.6**
119	82.2	**25019**	SAUDINETSTC-AS Autonomus System Number for SaudiNet	**SA**	5,357,056	**269.8**
591	51.6	**131222**	MTS-INDIA-IN 334,Udyog Vihar	**IN**	404,992	**232.3**
419	57.6	**45595**	PKTELECOM-AS-PK Pakistan Telecom Company Limited	**PK**	3,745,024	**222.1**
692	49.0	**55330**	GCN-DCN-AS AFGHANTELECOM GOVERNMENT...	**AF**	19,200	**219.8**
4	172.2	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,312	**219.8**
607	51.3	**8193**	UZPAK Uzpak Net	**UZ**	26,112	**217.5**
754	46.9	**31208**	MF-CENTER-AS OJSC MegaFon Network	**RU**	4,096	**210.0**
808	45.2	**37340**	Spectranet	**NG**	5,120	**202.7**

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

Although this pattern is still repeated, on the whole, in Q2, an interesting situation is presented. The #1 result shows AS48159 TIC as registered in Iran, a country known for its rigid monitoring of network systems. Does this indicate that a 'blind eye' is drawn over such activity or is there some other explanation?

Of note too is the return of AS29073 Ecatel to this Top 10 category.



10.2.3. Current Events

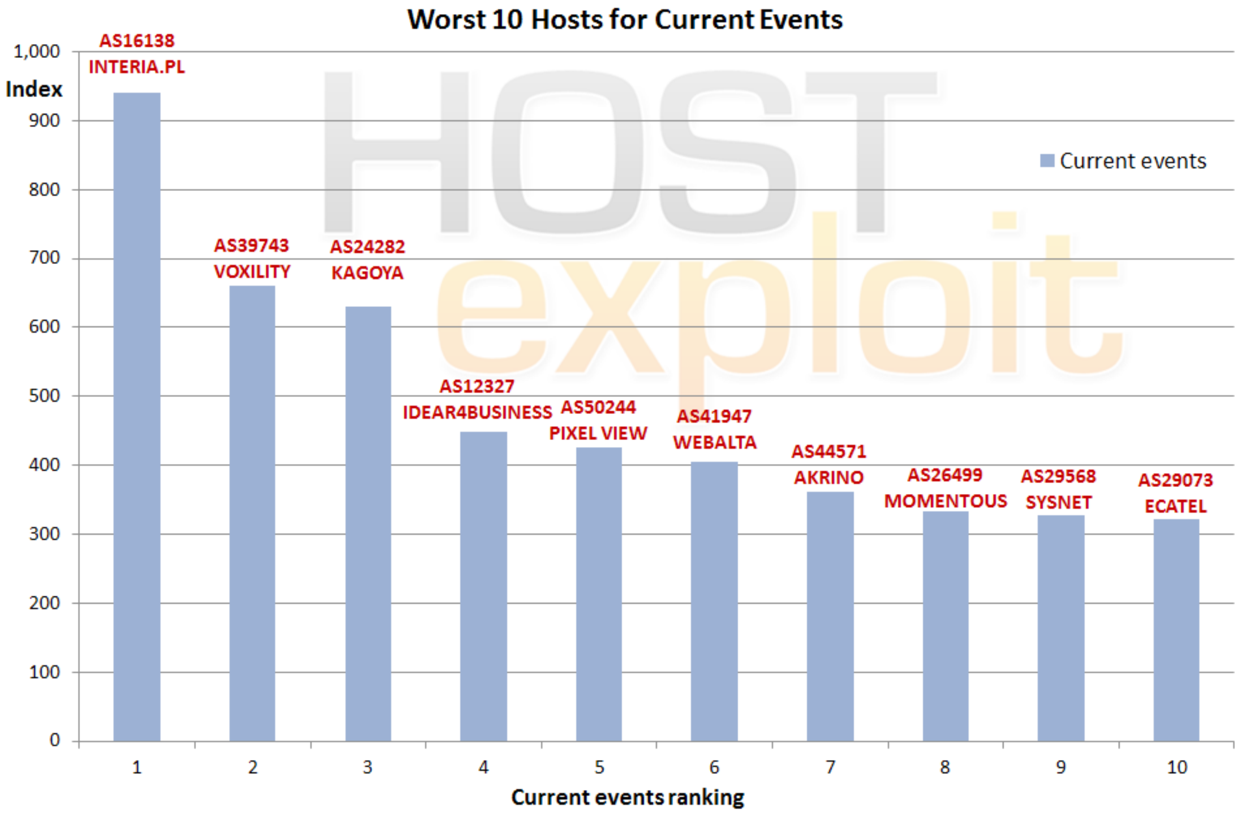
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
5	168.9	**16138**	INTERIAPL INTERIA.PL Sp z.o.o.	**PL**	4,096	**940.1**
6	165.3	**39743**	VOXILITY-AS Voxility SRL	**RO**	21,760	**659.6**
51	102.8	**24282**	KIR Kagoya Japan CO,LTD	**JP**	23,808	**630.4**
648	50.3	**12327**	IDEAR4BUSINESS-INTERNATIONAL-LTD idear4business...	**EU**	4,608	**447.7**
514	54.2	**50244**	ITELECOM Pixel View SRL	**RO**	7,936	**424.8**
1	214.7	**41947**	WEBALTA-AS OAO Webalta	**RU**	14,624	**404.9**
526	53.6	**44571**	AKRINO-AS Akrino Inc	**VG**	1,024	**361.0**
699	48.8	**26499**	MOMENTOUS - MOMENTOUS	**CA**	10,752	**332.2**
180	72.4	**29568**	COMTEL-AS SYSNET SECURE S.R.L.	**RO**	17,664	**327.4**
4	172.2	**29073**	ECATEL-AS AS29073, Ecatel Network	**NL**	13,312	**322.3**

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, Ice9, Stuxnet, DuQu, BlackHat SEO, as well as newly emerged exploit kits which form a key component of the data.

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

This category in earlier reports was previously dominated by US-based hosts. In Q2 2012 the majority in this Top 10 are located in Europe, with 2 in Asia.

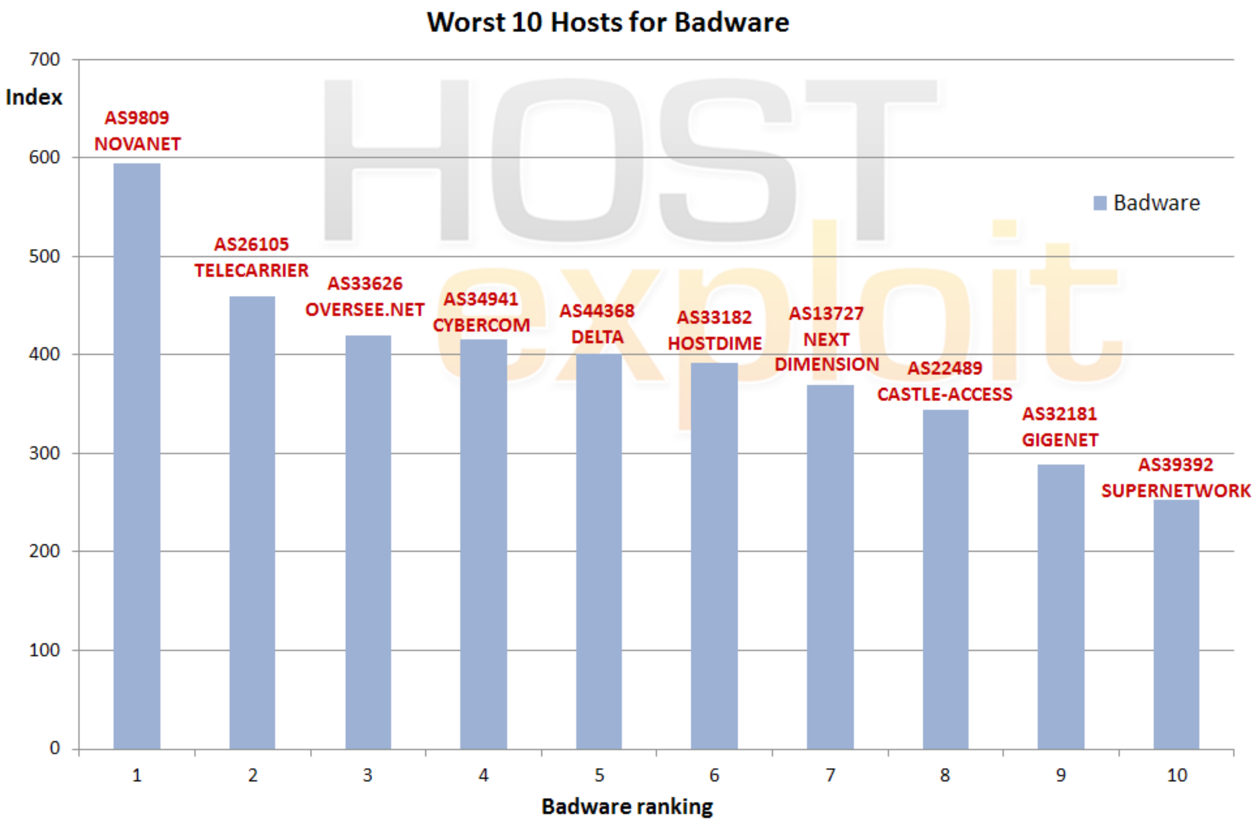


10.2.4. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
35	114.7	**9809**	NOVANET Nova Network Co.Ltd... Futian District, Shenzhen, China	**CN**	10,752	**594.7**
47	105.8	**26105**	Telecarrier, Inc	**PA**	44,608	**459.3**
50	103.1	**33626**	OVERSEE-DOT-NET - Oversee.net	**US**	3,840	**419.5**
116	82.7	**34941**	CYBERCOM-AS CyberCom & YT AB	**SE**	2,048	**415.5**
25	127.1	**44368**	ASDELTAMANAGEMENT DELTA MANAGEMENT AB	**SE**	3,072	**401.9**
12	145.8	**33182**	DIMENOC---HOSTDIME - HostDime.com, Inc.	**US**	50,432	**391.5**
128	80.5	**13727**	ND-CA-ASN - NEXT DIMENSION INC	**CA**	1,024	**370.0**
49	103.9	**22489**	CASTLE-ACCESS - Castle Access Inc	**US**	47,872	**344.4**
43	107.5	**32181**	ASN-GIGENET - GigeNET	**US**	42,240	**288.7**
127	80.5	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	**CZ**	53,504	**253.5**

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

This quarter many familiar repeat offenders, such as AS9809 NOVANET (China) at #1 for the second consecutive term, and AS33626 OVERSEE at #3, are joined by AS26105 TELECARRIER (Panama) at #2 and AS34941 CYBERCOM (Sweden) at #4.



11.

Conclusion

Conclusion

This quarter reflects a mixed bag of successes and failures as far as positions go in the Top 50 Bad Hosts and Networks table.

It is always pleasing when a former #1 drops right out of the top 50 altogether as is the case with AS47583 HOSTING-MEDIA. Sadly, there is always a new #1 deserving of its position, something that AS41947 WEBALTA knows only too well.

Back in Q1 2011 WEBALTA previously topped the table after which it appeared to make good progress in cleaning up its networks, followed by movement down the ranking. It is a great disappointment to see WEBALTA back in the #1 position. Let's hope that finding itself again in this position will prompt renewed action against many of its recent problems displayed through high levels of Current Events and C&C botnets.

The improved placing of service providers registered in the United States is a positive sign. In fact, this quarter, there are no US hosts topping any table. The overall number of US hosts in the Top 50 has fallen from seventeen in Q1 to thirteen in Q2. Obviously, individual US hosts such as AS15222 ADDD2NET - the highest placed at #8 - still have work to do but this is, at least, an encouraging sign.

Not so good is the appearance of hosts registered in Russia taking three of the places in the Top 10, including the #1 and #2 places. Despite the recent successes against the Carberp gang in Russia there is still a heavy workload ahead to clean up networks systems.

On a final note, although not within the timescale of our Q2 report, the recent Grum botnet takedown is worthy of considerable attention. A substantial chunk of spam has been removed as community efforts provide another shining example of a successful collaborative partnership.

Jart Armin

Appendix 1.

Glossary

AS (Autonomous System):

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

Badware:

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

Blacklists:

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

Botnet:

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

CSRF (cross site request forgery):

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

DNS (Domain Name System):

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

DNSBL:

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

Exploit:

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

Hosting:

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

IANA (Internet Assigned Numbers Authority)

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

ICANN (Internet Corporation for Assigned Names and Numbers)

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

IP (Internet Protocol):

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

IPv4

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

IPv6

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

ISP (internet Service Provider):

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

LFI (Local File Inclusion):

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

MALfi (Malicious File Inclusion):

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

Malicious Links:

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

MX:

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

NS (Name Server):

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

Open Source Security:

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

Pharming:

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

Phishing:

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

Registry:

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

Registrars:

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

Remote File Inclusion (RFI):

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

Rogue Software:

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

Rootkit:

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

Sandnet:

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

Spam:

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

Trojans:

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

Worms:

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

XSA (Cross Server Attack):

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

Appendix 2

HE Index Calculation Methodology

August 6, 2012

1 Revision history

Rev.	Date	Notes
1.	December 2009	Methodology introduced.
2.	March 2010	IP significant value raised from 10,000 to 20,000.
3.	June 2010	Sources refined. Double-counting of Google Safebrowsing data through StopBadware eliminated. Source weightings refined.
4.	October 2011	Sources refined. Source weightings refined.
4.	July 2012	Sources refined.

Table 1: Revision history

2 Motivation

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

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

1. Calculations should be drawn from multiple sources of data, each respresenting different forms of badness, in order to reduce the effect of any data anomalies.

2. Each calculation should take into account some objective size of the AS, so that the index is not unfairly in favor of the smallest ASes.

3. No AS should have an HE Index value of 0, since it cannot be said with certainty that an AS has zero badness, only that none has been detected.

4. Only one AS should be able to hold the maximum HE Index value of 1,000 (if any at all).

3 Data sources

Data is taken from the following 11 sources.

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

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

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

Table 2: Data sources

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

4 Bayesian weighting

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

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

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

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

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

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

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)*