HostExploit - CyberCrime Series
March, 2010

Top 50

Bad Hosts and Networks

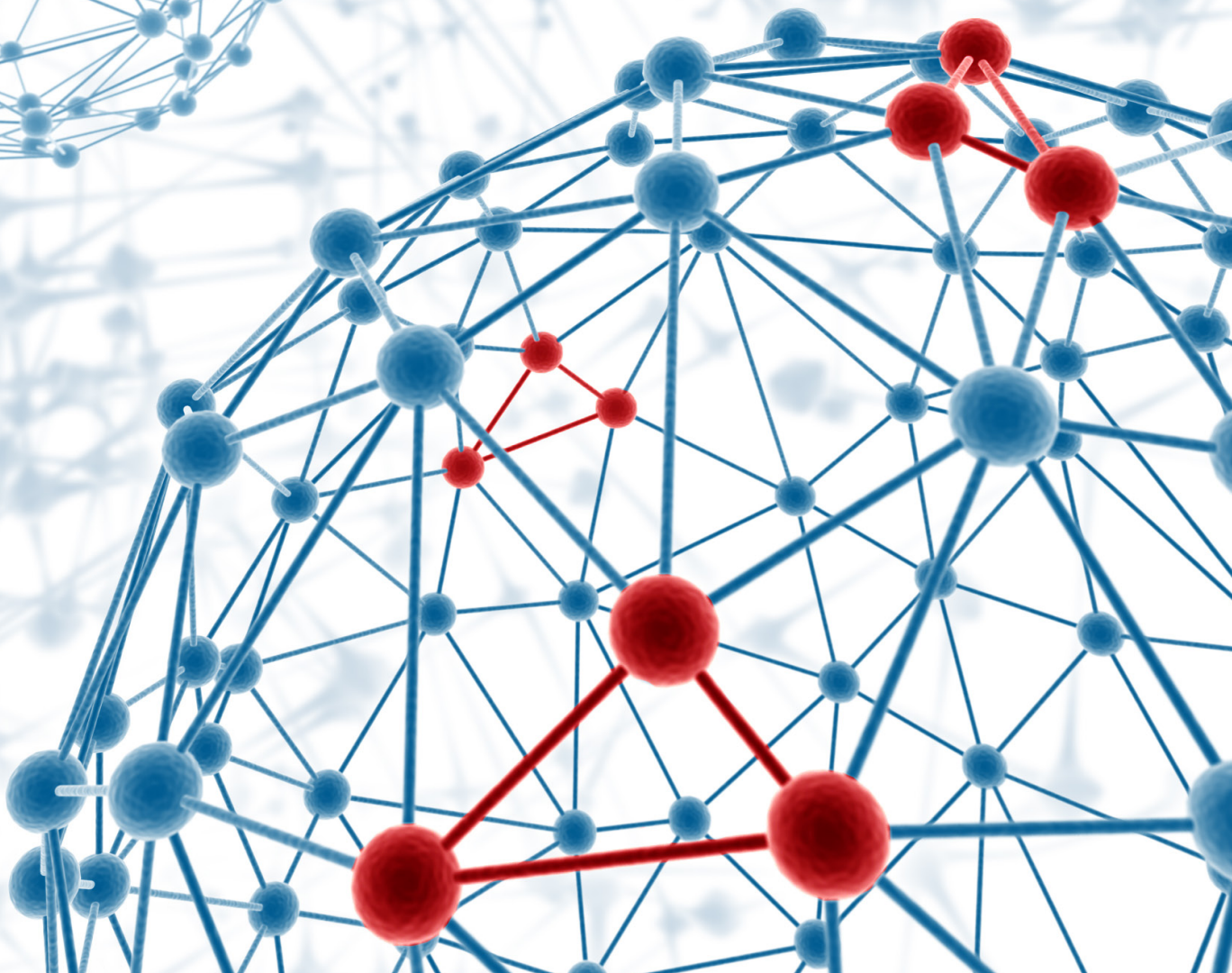


Table of Contents

Top 50

CyberCrime Series

Bad Hosts and Networks

Backing from

nominet trust

www.nominettrust.org.uk

Edited by

- Jart Armin
- Cath Everett

Review

- Dr. Bob Bruen
- Derek Smythe

Contributors

- Philip Stranger
- Scott Logan
- David Glosser
- Max Mockett
- Brynd Thompson
- Will Rogofsky

Comparative Data

- SiteVet
- HostExploit
- RASHbl
- StopBadware
- Google
- MalwareDomains
- MaliciousNetworks
- MalwareURL
- AA419
- SudoSecure
- Sunbelt
- UCE Protect
- Spamhaus
- Abuse.CH
- Emerging Threats
- Knujon
- CIDR
- Robtex
- Team Cymru
- Dancho Danchev

Bad Hosts and Networks

Introduction

HostExploit presents the second report in our ongoing and quarterly series on the Top 50 Bad Hosts and Networks.

HostExploit has used its own sustained research and data gathering together with data from Open Source security sources of: badware, infected web sites, spammers, phishing, malware, botnet C&Cs, ZeuS botnet infections, and exploit serving to compile a list of the worst Internet hosting players around the world.

Such findings are based on data generated by a detailed analysis of **33,410** public ASes (Autonomous Systems) exchanging routing information with each other over the public Internet. 'Bad' activity in this context includes inter related traffic generated by botnets, spam, MALfi, phishing, malware, exploits and the control centers that manage these activities.

The resulting information has been analyzed using a unique combination of actuarially-weighted mathematical equations and focuses on the worst aspects of cyber-criminal activity in order to create a bespoke 'badness' rating. It takes into account the size of each network in question, recognizing that larger servers offer greater potential for distributing malware, but also that such larger servers are under more pressure to undertake effective monitoring. The result is an easily understandable measurement of damage caused to internet users by 'bad' activity. We call this measurement the **HE Index**.

While other network scoring systems do exist, bad hosts have historically been able to avoid exposure on well-known blacklists. McColo, for example, contained few active domains nor did it appear on lists that tracked URLs. For this reason, the HE Index is based on a number of respected data sources of varying significance.

For full details about the methodology of the HE Index, refer to our December 2009 report.

It is important to consider the scale of the findings within the report on a quantitative basis to provide an overview of the state of badness hosted and served across the whole of the Internet:

- An HE Index of 25.0 or lower should be considered a low state of badness - approximately 5% of ASes analyzed exceed this figure.
- From a positive perspective this should be viewed as 95% of the world's commercial ASes, ISPs and servers operating effective abuse procedures with a low tolerance for hosting badness.
- For the Top 50 Bad Hosts, rank #1 has an HE Index of 337.3, and rank #50 has an HE Index of 111.1
- It is clear from a comparison of the Top 50 Bad Hosts reports in December 2009 and March 2010, that the disclosure has been helpful to some hosts. A number of hosts contacted have made progress in resolving badness and abuse issues - in a few demonstrated cases, hosting badness has decreased by up to 90%.
- The underlying research serves as a backbone for further analysis into the growing trend of dedicated "Crime Servers," to be released as a series of supplements to the report. One such supplement will be used to demonstrate recent examples of crime servers - such as Troyak and its peers - and will highlight what action can be taken to combat this issue.

The report also explores the implications of criminal involvement and what such activity means in global security terms. As such, it should act as a benchmark for law enforcement agencies, Internet crime monitoring bodies and the Internet community as a whole.

It likewise endeavors to highlight the urgent need for the more stringent enforcement of abuse policies and the role that the security and wider internet community can play in helping resolve such issues pro actively and effectively.

The power of community action should not be underestimated. The recent exposure and demise of the malware serving host Troyak is an excellent case in example.

The report aims to alert the security industry and the hosts themselves to the danger of system abuses that organized gangs of cybercriminals can take advantage of, which unfortunately is sometimes under the protection of legitimate businesses.

In the interest of providing a balanced perspective and by applying the same techniques as described earlier, the report also briefly looks at the best hosting providers around the world, with the aim of benefiting users, webmasters, web developers and the internet community as a whole.

Please note the quantitative analysis of each of the 33,410 ASNs can be viewed on **SiteVet.com**

Jart Armin

Editor's Note

On The Previous Report...

In our December 2009 report on the Top 50 Bad Hosts & Networks, we introduced the HE Index as a numerical representation of the 'badness' of an Autonomous System (ASN). Although generally well-received by the community, we received many constructive questions, some of which we will attempt to answer here.

Based on feedback, we have amended our use of source data. Notably, we no longer directly use data from the Google Safe Browsing service as this overlaps with data provided by StopBadware.

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 ASN, 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?

Absolutely. Although the HE Index gives higher weighting to ASNs with smaller address spaces, the relationship is not linear. There is a Bayesian factor or "uncertainty factor", which boosts figures for larger address spaces, which we have used to model this responsibility. The critical address size has been increased from 10,000 to 20,000 in the 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 to gain vital understanding of what is happening in the world of information security beyond their daily lives. But our main goal is to raise awareness of the source of security issues by quantifying the extent to which organizations allow illegal activities to occur - or rather, fail to prevent it.

Why do these hosts carry out this activity?

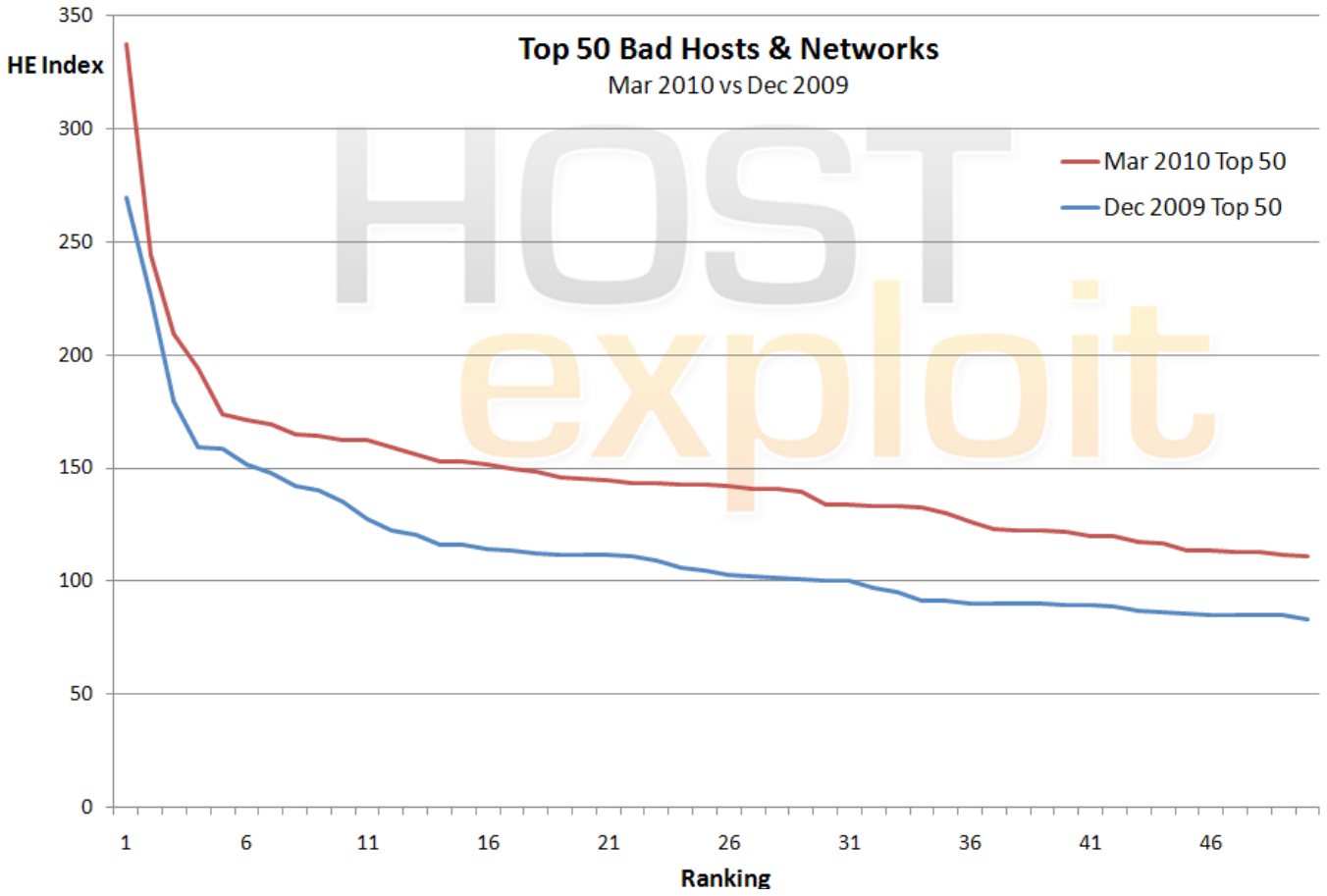
It is important to state that by publishing these results, HostExploit does not claim that the hosting providers listed knowingly consent to the illicit activity carried out on their servers.

Our methodology is a work in progress and so further feedback is warmly welcomed.

2. The Top 50

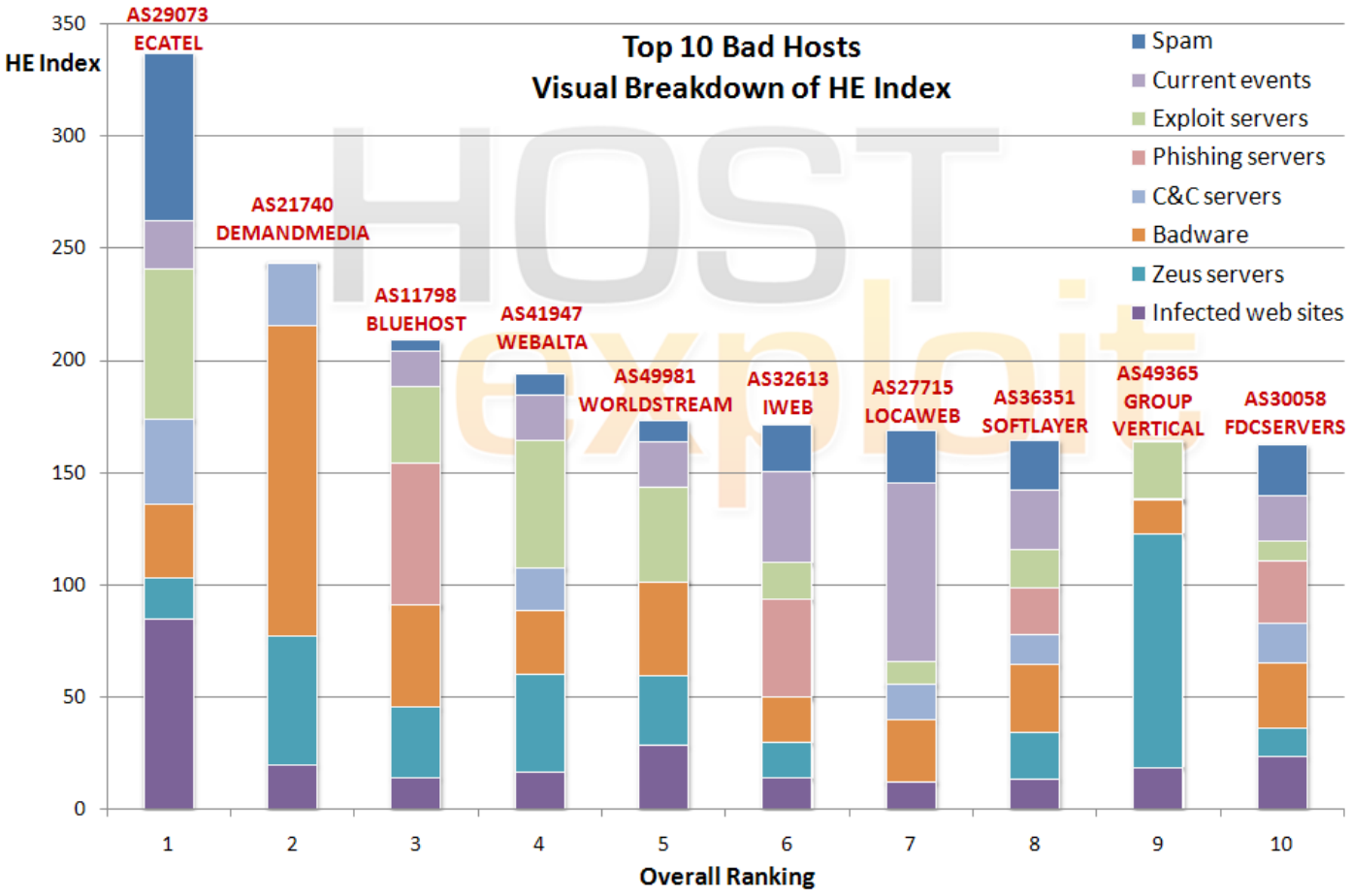
HE Rank	HE Index	AS number	AS name	Country	# of IPs
1	337.3	29073	ECATEL-AS AS29073, Ecatel Network	NL	10,496
2	244.1	21740	DemandMedia AS DemandMedia	US	12,544
3	209.2	11798	BLUEHOST-AS - Bluehost Inc.	US	49,152
4	194.2	41947	WEBALTA-AS Wahome networks	RU	13,312
5	173.5	49981	WORLDSTREAM WorldStream	NL	11,776
6	171.4	32613	IWEB-AS - iWeb Technologies Inc.	CA	152,320
7	169.1	27715	LocaWeb Ltda	BR	41,472
8	164.6	36351	SOFTLAYER - SoftLayer Technologies Inc.	US	478,464
9	164.3	49365	GR-VERTICAL-AS Group Vertical Ltd	RU	256
10	162.5	30058	FDCSERVERS - FDCservers.net	US	146,432
11	162.3	32475	SINGLEHOP-INC - SingleHop	NL	102,528
12	159.4	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.	US	1,534,464
13	156.0	16276	OVH OVH	FR	408,064
14	153.1	23522	IPNAP-ES - Ecomdevel, LLC	US	14,592
15	152.9	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.	US	20,736
16	151.5	31240	OLD-HT-SYSTEMS-AS JSC Hosting Telesystems autonomous system	RU	6,144
17	149.9	3595	GNAXNET-AS - Global Net Access, LLC	US	148,032
18	148.3	10297	COLUMBUSNAP - The Columbus Network Access Point, Inc.	US	81,920
19	145.6	41126	CENTROHOST-AS JSC Centrohost	RU	4,096
20	145.6	4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	93,180,416
21	144.7	35908	VPLSNET - VPLS Inc. d/b/a Krypt Technologies	US	515,584
22	143.6	15244	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	40,448
23	143.2	9680	HINETUSA HiNet Service Center in U.S.A	TW	4,096
24	143.0	31034	ARUBA-ASN Aruba S.p.A. - Network	IT	112,384
25	142.5	28753	NETDIRECT AS NETDIRECT Frankfurt, DE	DE	108,544
26	142.2	8560	ONEANDONE-AS 1&1 Internet AG	DE	380,928
27	141.0	21788	NOC - Network Operations Center Inc.	US	147,456
28	140.7	45899	VNPT-AS-VN VNPT Corp	VN	209,152
29	139.8	32181	ASN-ECOMD-COLOQUEST - Ecomdevel, LLC	US	28,160
30	133.7	29671	SERVAGE Servage GmbH	DE	12,288
31	133.6	5577	ROOT root SA	LU	31,488
32	133.1	49314	NEVAL PE Nevedomskiy Alexey Alexeevich	RU	256
33	133.0	47142	STEEPHOST-AS DC-UA-SteepHost.COM Datacentre Allocation	UA	2,304
34	132.3	24826	KHARKOV-TERMINALS-AS PE Viktor Nastechenko	UA	256
35	130.2	44565	VITAL VITAL TEKNOLOJI	TR	18,432
36	126.5	47781	ANSUA-AS PE Sergey Demin	UA	512
37	123.0	15169	GOOGLE - Google Inc.	US	253,952
38	122.7	49544	INTERACTIVE3D-AS Interactive3D	NL	40,960
39	122.2	46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	57,344
40	121.8	16626	GNAXNET-AS - Global Net Access, LLC	US	58,560
41	120.1	9286	LGH-AS-KR LGHitachi	KR	2,304
42	119.8	32244	LIQUID-WEB-INC - Liquid Web, Inc.	US	163,840
43	117.1	16265	LEASEWEB LEASEWEB AS	NL	285,696
44	116.7	26347	DREAMHOST-AS - New Dream Network, LLC	US	135,168
45	113.4	34305	EUROACCESS Euroaccess Global Autonomous System	RU	38,912
46	113.4	9318	HANARO-AS Hanaro Telecom Inc.	KR	11,912,256
47	112.9	29873	BIZLAND-SD - The Endurance International Group, Inc.	US	51,200
48	112.8	26496	PAH-INC - GoDaddy.com, Inc.	US	811,264
49	111.9	11388	MAXIM - Peer 1 Dedicated Hosting	US	143,360
50	111.1	41075	ATW-AS ATW Internet Kft.	HU	6,912

December 2009 Comparison



From the above graph, it is immediately clear that the Top 50 Bad Hosts show a consistent rise in effective badness from December 2009 to March 2010.

Top 10 Visual Breakdown



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

Firstly, that the sources are weighted in such a way that no particular source dominates the makeup of the HE Index among the majority of the hosts. This ensures that the HE Index is a balanced measurement.

Secondly, it demonstrates the breakdown of the HE Index for each specific AS in the Top 10, so that we can clearly see why it is ranked so highly.

For instance, it is immediately clear that AS29073 Ecatel at rank #1 is top of the list due to a range of issues; particularly spam, exploit servers and infected web sites. However, AS21740 DemandMedia is ranked #2 due to its exceptionally high concentrations of badware, in addition to Zeus and other C&C servers.

Further, we can see that AS49365 Group Vertical is a suspected crime server, due to its very high number of Zeus servers on a small allocated prefix.

Country Analysis

Hosts in Top 50	Country	Total IPs	Total Index	Aver-age Index	Average Indexes by Category							
					Infected web sites	Spam	C&C servers	Phishing servers	Exploit servers	Current events	Zeus servers	Badware
22	UNITED STATES	5,178,368	3,171.3	144.1	169.7	44.1	79.1	211.7	257.2	181.3	152.5	224.4
6	RUSSIAN FEDERATION	62,976	902.1	150.4	182.7	22.5	85.2	0.4	326.9	296.8	330.8	140.3
4	NETHERLANDS, THE	165,760	795.8	199.0	333.3	105.2	85.2	0.2	481.3	282.6	264.6	193.8
3	GERMANY	501,760	418.4	139.5	184.2	45.0	36.8	0.1	230.3	231.4	180.1	273.2
3	UKRAINE	3,072	391.8	130.6	222.0	13.2	177.7	0.5	372.9	74.2	251.5	127.8
2	KOREA, REPUBLIC OF	11,914,560	233.5	116.8	102.0	46.9	0.1	105.8	228.0	394.8	58.8	122.4
1	CANADA	152,320	171.4	171.4	123.5	81.6	0.0	588.0	221.1	364.2	143.9	136.2
1	BRAZIL	41,472	169.1	169.1	107.8	91.5	142.1	0.2	141.1	714.0	0.1	187.8
1	FRANCE	408,064	156.0	156.0	142.1	103.7	0.0	278.9	140.1	405.6	150.3	138.7
1	CHINA	93,180,416	145.6	145.6	115.8	108.1	200.5	138.0	202.7	101.4	162.8	187.6
1	TAIWAN	4,096	143.2	143.2	107.4	130.8	200.3	0.4	1.4	320.6	179.1	131.0
1	ITALY	112,384	143.0	143.0	104.3	63.5	0.0	649.6	158.4	184.5	135.6	131.5
1	VIETNAM	209,152	140.7	140.7	0.0	542.4	0.0	0.0	0.1	0.1	0.0	0.0
1	LUXEMBOURG	31,488	133.6	133.6	549.2	36.2	0.0	0.2	148.9	0.6	217.5	188.4
1	TURKEY	18,432	130.2	130.2	144.0	6.0	0.1	0.3	229.6	170.1	508.2	136.5
1	HUNGARY	6,912	111.1	111.1	101.9	3.3	190.3	0.4	1.2	396.2	0.2	227.1

The Good Hosts

HE Index	HE Rank	AS number	AS name	# of IPs
1.569	8290	8153	ASIAONLINEAUS-AS-AP Nexon Asia Pacific	113,920
1.382	8582	72	SIBERIANET-AS SiberiaNet LLC	6,144
1.355	8623	297	MONTANA-SKY-NETWORKS-INC - Montana Sky Networks, Inc.	13,568
1.328	8652	4010	DATAWEB DataWeb B.V. - The Netherlands	8,192
1.305	8705	5619	PIXELWEB - Pixelweb	4,096
1.237	8870	27065	KURSKTELECOM-AS AS of JSC Kursktelecom	2,048
1.173	9009	109	MANCHESTERMETRONET Manchester Metronet Ltd	16,384
1.159	9123	18676	AHI-AS AlHarbi International for Telecom..	17,408
1.028	9613	1101	METEOMEDIA-AS Meteomedia Deutschland GmbH	256
1.017	9942	3360	KFNETRO KFNET Romania	512

6.1. Why List Examples of Good Hosts?

It is important to give a balanced perspective and would be wrong to give the impression that service providers can only be judged in terms of badness. Safe and secure web site hosting environments are perfectly possible to achieve and, although our research has demonstrated that instances of 'good' providers are few and far between, we have pinpointed several examples of organizations with minimal levels of service violations.

As a result, we have created a table of examples of 'good hosts' and would like to commend those companies as examples of abuse control and management.

It is an accolade that such hosts should be pleased to win and will become a regular feature.

6.2. Selection Criteria

To conform to our definition of AS, ISP or colocation facility, organizations needed to control at least 5,000 individual IP addresses. It should be stressed that several hosting providers in the wider report controlled less than this number, however.

But it means that, 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 took included those ASes that act primarily as public web or internet service providers, although we appreciate that such criteria are subjective.

Most Improved Hosts

Change	Old Index	New Index	AS number	AS name	Country	# of IPs
-99.2%	112.6	0.8	15135	EVERYDNS - EveryDNS, LLC	US	1,024
-98.7%	65.0	0.9	31800	DALNET - DALnet	US	768
-66.1%	90.1	30.5	44042	ROOT root SA	LU	65,536
-61.9%	159.5	60.8	41665	HOSTING-AS National Hosting Provider, Hosting.UA	UA	144,384
-59.4%	269.9	109.6	30407	VELCOM - Rcp.net	CA	11,264
-58.9%	113.6	46.7	48031	NOVIKOV-AS IP Novikov Aleksandr Leonidovich	RU	256
-56.6%	111.6	48.5	15435	KABELFOON CAIW Autonomous System	NL	155,648
-55.2%	100.7	45.1	8206	JUNIK-RIGA-LV JUNIKNET Autonomous System	LV	16,384
-50.7%	142.2	70.2	10929	NETELLIGENT - Netelligent Hosting Services Inc.	CA	38,912
-49.3%	120.3	61.0	48445	FAVN Favorit Network SL	ES	512

Many of these forms of badware are inextricably linked and the problem of tackling the issue can, at time, seem intractable. But the following table shows example of ASNs that have dramatically reduced their badness levels in the three months since our December 2009 report was published.

We were particularly happy to see that AS30407 Velcom, which was ranked as the #1 Bad Host in December's report, has dramatically reduced its badness levels. This would appear to indicate that raising awareness can trigger action and also that it is possible for hosting providers to improve their performance in a relatively short period of time if they put their minds to it.

Two large European ASNs – the Dutch ISP Kabelfoon and Latvian National Hosting Provider – also demonstrated significant falls in badness levels, which is encouraging, particularly from a large AS perspective.

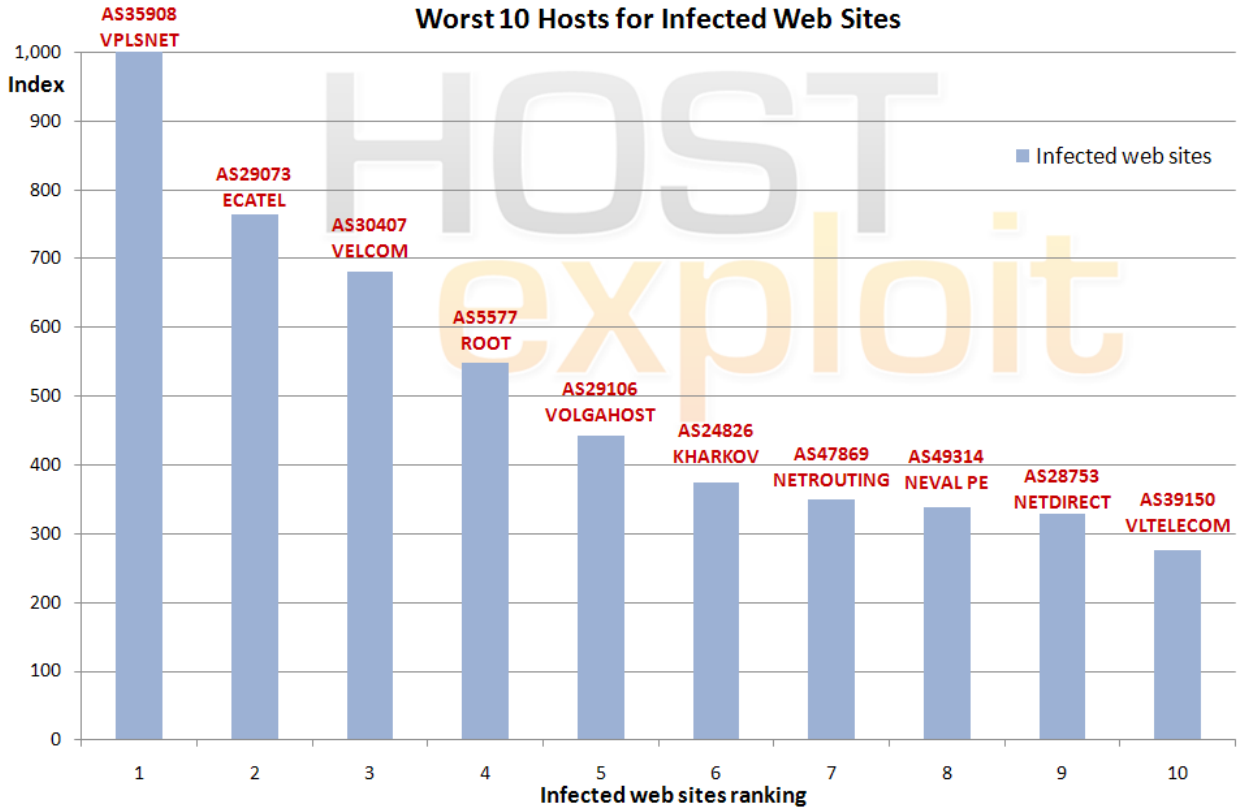
Bad Hosts by Topic

8.1. Infected Web Sites

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
21	144.7	**35908**	VPLSNET - VPLS Inc. d/b/a Krypt Technologies	US	515,584	**1000.0**
1	337.3	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	10,496	**765.0**
51	109.6	**30407**	VELCOM - Rcp.net	CA	11,264	**680.7**
31	133.6	**5577**	ROOT root SA	LU	31,488	**549.2**
53	107.8	**29106**	VOLGAHOST-AS PE Bondarenko Dmitriy Vladimirovich	RU	256	**442.7**
34	132.3	**24826**	KHARKOV-TERMINALS-AS PE Viktor Nastechenko	UA	256	**374.7**
211	70.1	**47869**	NETROUTING-AS Netrouting Data Facilities	NL	6,912	**349.5**
32	133.1	**49314**	NEVAL PE Nevedomskiy Alexey Alexeevich	RU	256	**337.9**
25	142.5	**28753**	NETDIRECT AS NETDIRECT Frankfurt, DE	DE	108,544	**328.2**
54	107.2	**39150**	VLTELECOM-AS VLineTelecom LLC Moscow, Russia	RU	4,352	**276.7**

The category 'Infected Web Sites' is very general because such sites are often subject to multiple simultaneous forms of malicious activity. To understand such activity, however, we combined our own data, gathered from honeypots set up to attract a number of attacks, with data provided by MalwareURL about the number of malicious URLs found on individual ASes. MalwareURL's information is itself an amalgam of a number of community-reported sources.

The results of the analysis were mixed, with infected sites comprising a blend of large hosts and a number of smaller, suspected crime servers. Although there were 3 Russian ASes in the top 10, a US-based hosting provider led the field by some distance.



8.2. Spam

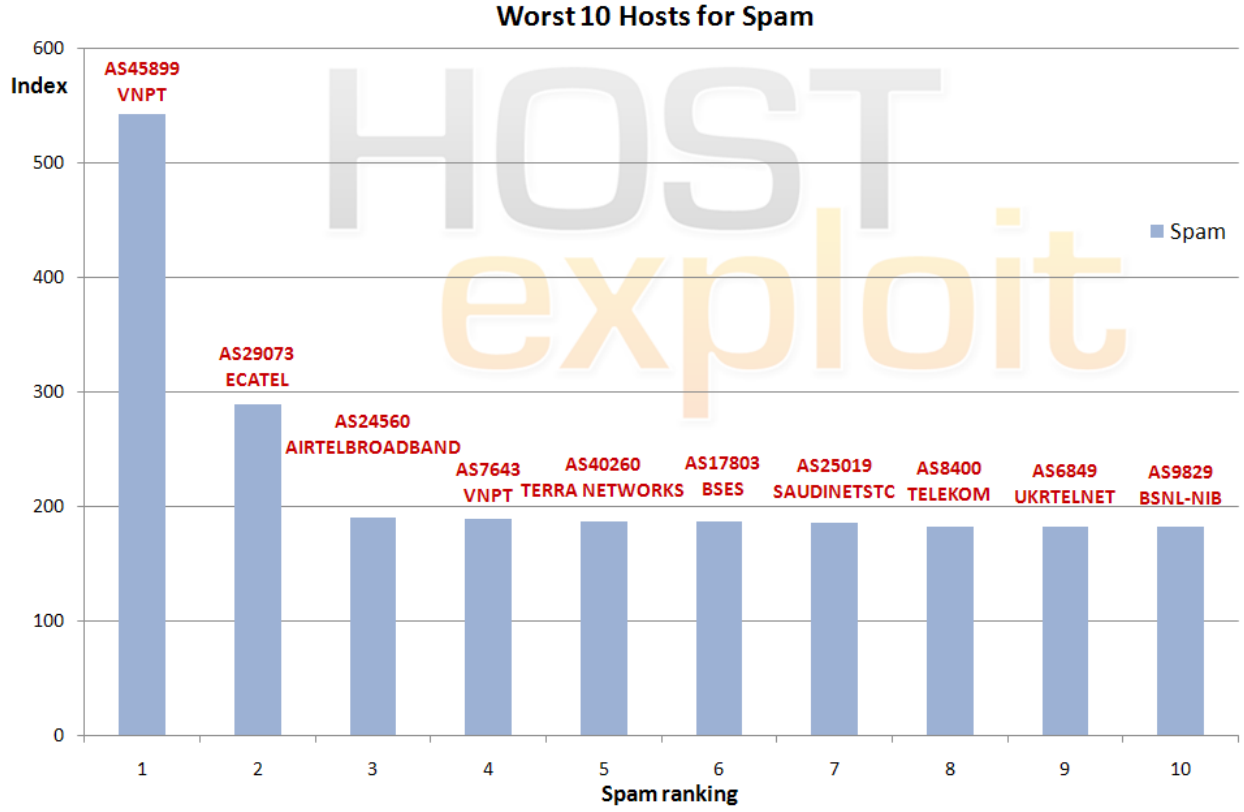
HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
28	140.7	**45899**	VNPT-AS-VN VNPT Corp	VN	209,152	**542.4**
1	337.3	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	10,496	**289.9**
83	94.4	**24560**	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services	IN	1,457,920	**190.6**
115	82.7	**7643**	VNPT-AS-VN Vietnam Posts and Telecommunications (VNPT)	VN	2,475,264	**189.3**
307	64.4	**40260**	TERRA-NETWORKS-MIAMI - Terra Networks Operations Inc.	US	7,168	**187.3**
335	61.5	**17803**	BSES-AS-AP BSES TeleCom Limited	AU	77,312	**187.0**
201	70.7	**25019**	SAUDINETSTC-AS Autonomus System Number for SaudiNet	DE	1,685,504	**186.0**
324	62.5	**8400**	TELEKOM-AS "TELEKOM SRBIJA" a.d.	YU	460,288	**183.1**
87	93.6	**6849**	UKRTELNET JSC UKRTELECOM,	UA	998,656	**182.9**
172	73.4	**9829**	BSNL-NIB National Internet Backbone	NL	5,363,456	**182.7**

Spam is a difficult issue because it is tricky to quantify exactly who is responsible for what. While the number of spammers that use a given server can be employed as a reasonable measure of a machine's spamming badness in some circumstances, in others it cannot. This is because, in some cases, the damage caused by a single spammer can be greater than that by a group.

For this reason, we used a combination of routing prefixes from respected commercial operation UCEPROTECT-Network, spam server information from academic researchers at Malicious Networks (FiRE) and community spam bot data from SudoSecure to provide a wide spread of spam instances. The result was a definitive list of the worst spam havens in the world.

Consistent with our previous findings, these results clearly indicated that spammers prefer servers located in countries that are subject to less regulation and monitoring activity than is typical in the West. Unsurprisingly, therefore, four of the AS's listed in the table below were also present in our Top 10 list of Bad Hosts.

At a time when rapid fast flux servers and "disposable" crime servers are increasingly being employed, this demonstrates that the spam industry has not moved forward at the same pace as other areas of cybercrime. While such a finding may initially seem positive, it may be that loose regulation makes it unnecessary for spammers to spend time and energy on new innovation.



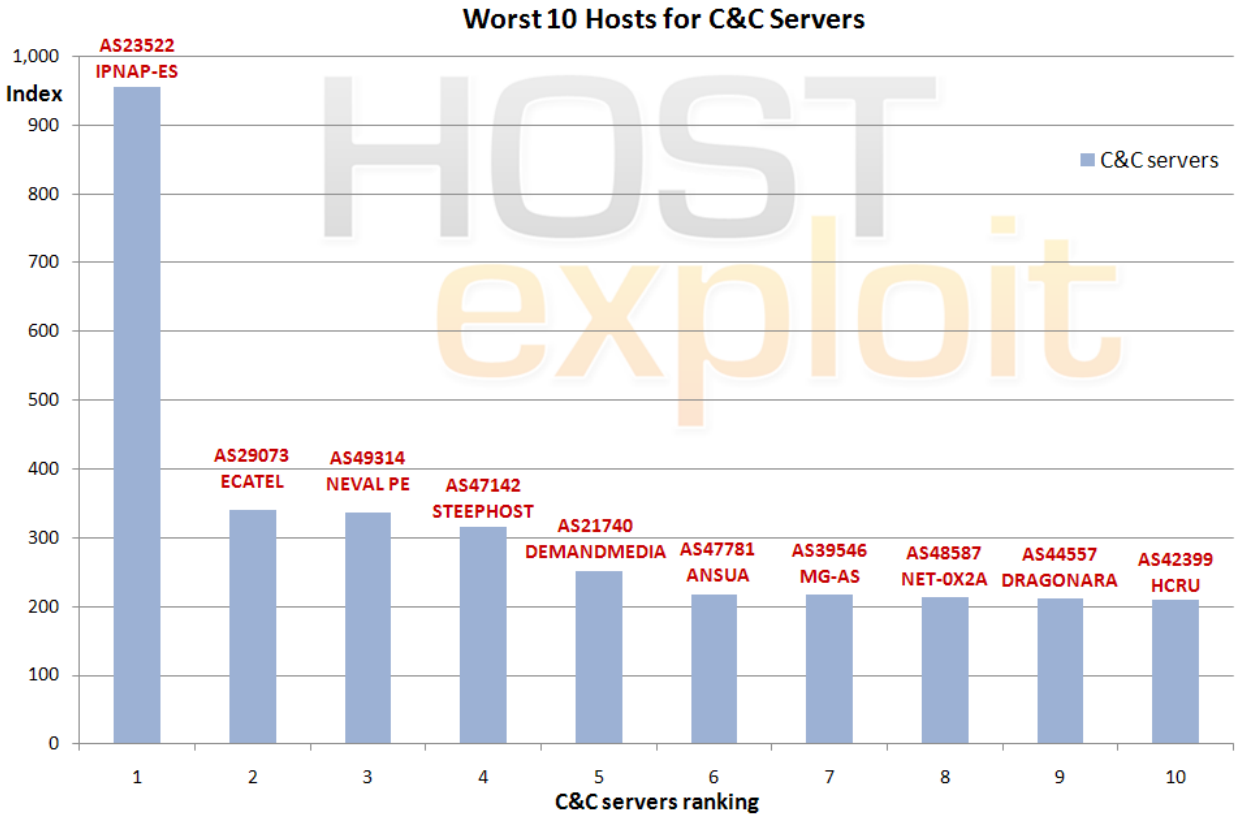
8.3. Botnet C&C Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
14	153.1	**23522**	IPNAP-ES - Ecomdevel, LLC	US	14,592	**954.6**
1	337.3	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	10,496	**340.6**
32	133.1	**49314**	NEVAL PE Nevedomskiy Alexey Alexeevich	RU	256	**336.9**
33	133.0	**47142**	STEEPHOST-AS DC-UA-SteepHost.COM Datacentre Allocation	UA	2,304	**316.0**
2	244.1	**21740**	DemandMedia AS DemandMedia	US	12,544	**250.9**
36	126.5	**47781**	ANSUA-AS PE Sergey Demin	UA	512	**217.1**
1,407	29.7	**39546**	MG-AS ISP MG	UA	512	**217.1**
135	79.5	**48587**	NET-0X2A-AS Private Entrepreneur Zharkov Mukola Mukolayovuch	UA	1,024	**214.3**
90	92.5	**44557**	DRAGONARA Dragonara Alliance Ltd	VG	1,536	**211.7**
953	39.3	**42399**	HCRU-AS Hosting Center	RU	2,048	**209.2**

Because cyber criminals tend to take a "disposable server" approach, Command & Control Servers were most commonly found on smaller ASes.

The exceptions to this rule were DemandMedia (after its acquisition of eNom), Ecatel and Ecomdevel (more commonly known as Gigenet/ Gigeservers).

It was quite surprising to see the polarity between smaller crime servers and such well-known apparently-reputable hosts being used in this fashion, however.



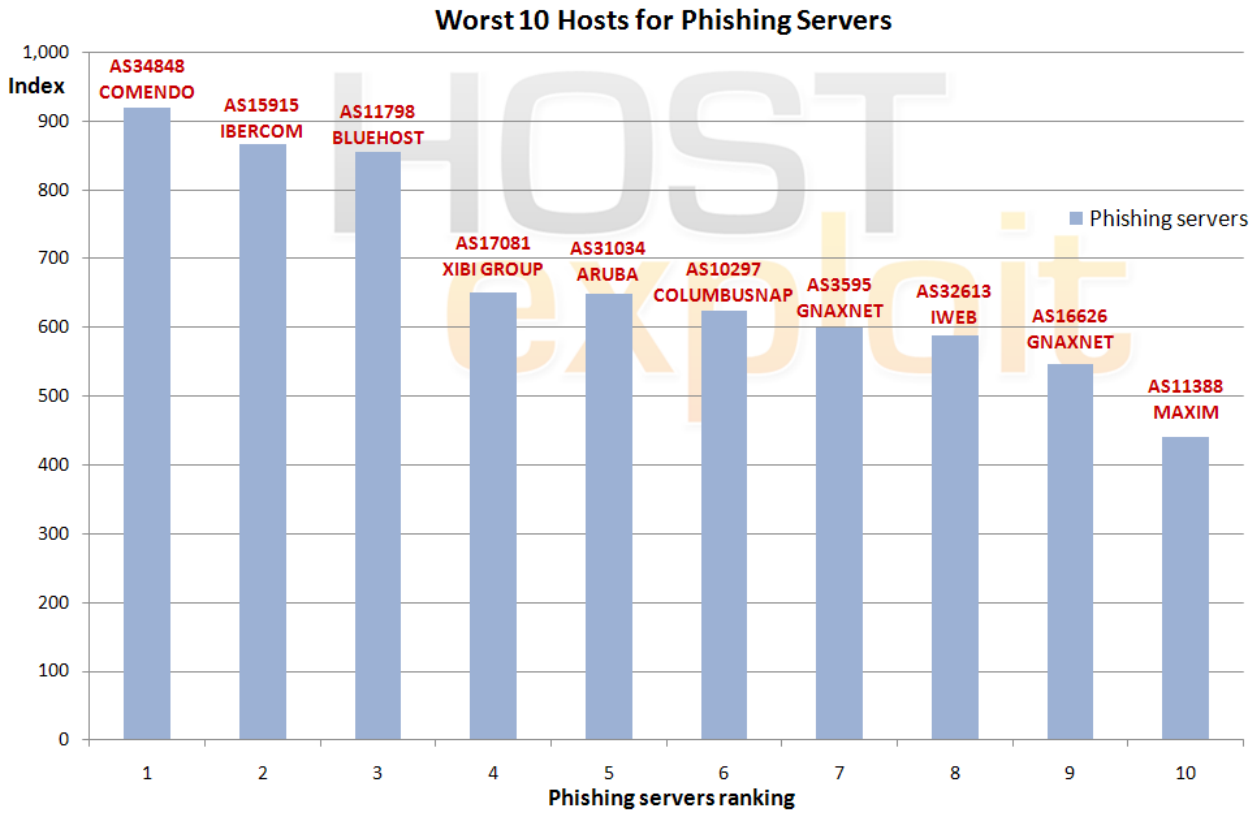
8.4. Phishing

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
167	73.8	**34848**	COMENDO-AS Comendo A/S	DK	11,008	**918.8**
144	78.3	**15915**	IBERCOM WORLD WIDE WEB IBERCOM	ES	24,576	**866.9**
3	209.2	**11798**	BLUEHOST-AS - Bluehost Inc.	US	49,152	**854.8**
213	70.1	**17081**	XIBIG - Xibi Group, Inc.	US	10,752	**650.4**
24	143.0	**31034**	ARUBA-ASN Aruba S.p.A. - Network	IT	112,384	**649.6**
18	148.3	**10297**	COLUMBUSNAP - The Columbus Network Access Point, Inc.	US	81,920	**624.2**
17	149.9	**3595**	GNAXNET-AS - Global Net Access, LLC	US	148,032	**599.0**
6	171.4	**32613**	IWEB-AS - iWeb Technologies Inc.	CA	152,320	**588.0**
40	121.8	**16626**	GNAXNET-AS - Global Net Access, LLC	US	58,560	**546.0**
49	111.9	**11388**	MAXIM - Peer 1 Dedicated Hosting	US	143,360	**441.2**

The top 10 Phishing Servers were located entirely in Western countries, a fact that is unsurprising given that the first goal of phishing is to establish false credibility.

Phishing attacks and scams have significantly increased in sophistication over the last year or so, however, with large corporations and banks in particular now being invariably used as false subjects.

The necessary malware often actually even resides on the enterprise's web site – or appears to via cross-site scripting or header redirects. Therefore, to minimize both customers' and target organizations' suspicion, malware is generally located on a server based in the West.



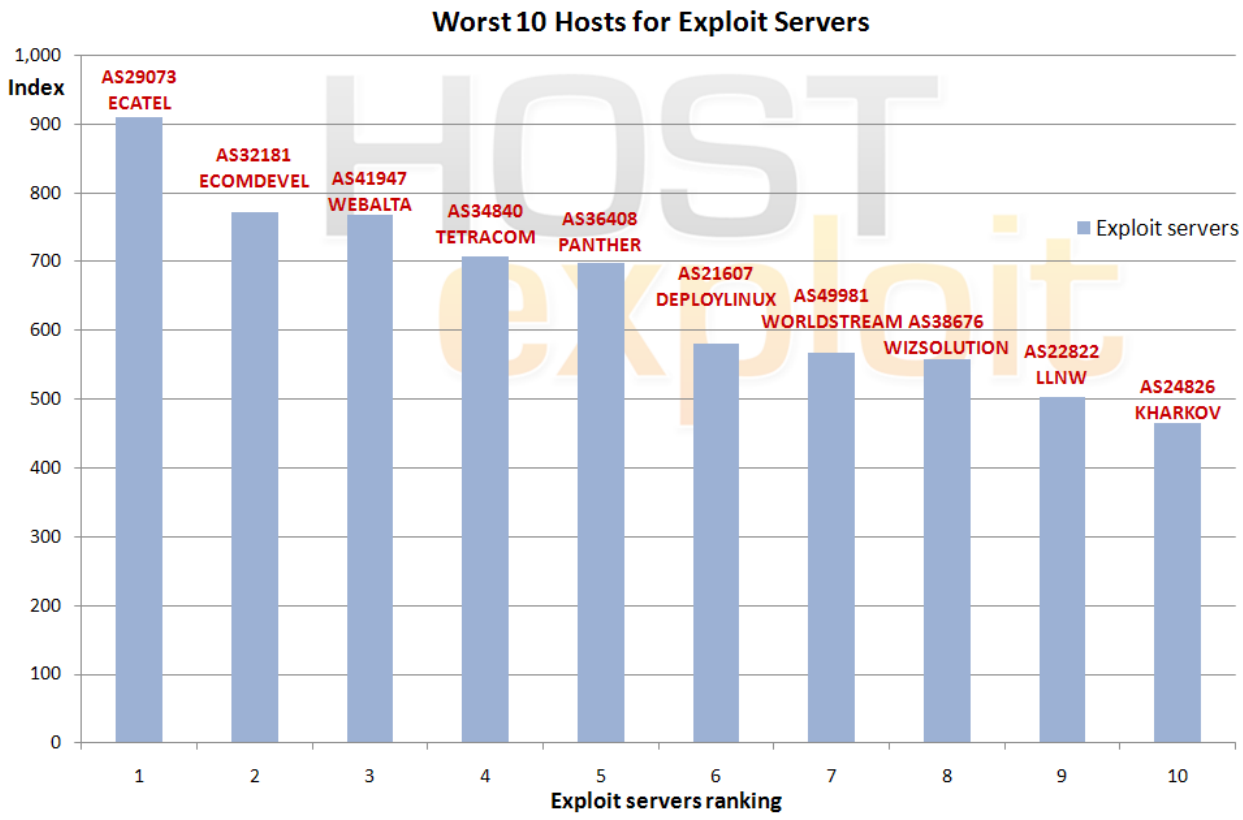
8.5. Exploit Servers

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
1	337.3	**29073**	ECATEL-AS AS29073, Ecatel Network	NL	10,496	**909.7**
29	139.8	**32181**	ASN-ECOMD-COLOQUEST - Ecomdevel, LLC	US	28,160	**771.0**
4	194.2	**41947**	WEBALTA-AS Wahome networks	RU	13,312	**768.0**
57	105.7	**34840**	TETRACOM Tetracom CJSC	RU	256	**707.9**
560	52.3	**36408**	ASN-PANTHER Panther Express	US	13,056	**698.4**
159	75.4	**21607**	DEPLOYLINUX - DeployLinux Consulting, Inc	US	512	**580.6**
5	173.5	**49981**	WORLDSTREAM WorldStream	NL	11,776	**566.9**
790	43.7	**38676**	AS33005-AS-KR wizsolution co.,Ltd	KR	6,912	**558.7**
285	66.5	**22822**	LLNW - Limelight Networks, Inc.	US	100,352	**503.4**
34	132.3	**24826**	KHARKOV-TERMINALS-AS PE Viktor Nastechenko	UA	256	**465.4**

It is important to note that "Exploit Servers" are very important for analyzing malware, phishing, or badness as a whole and, as such, are possibly the most important category to be found in this report.

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

In contrast to spam hosts, Exploit Servers are commonly located in countries subject to higher levels of regulation.

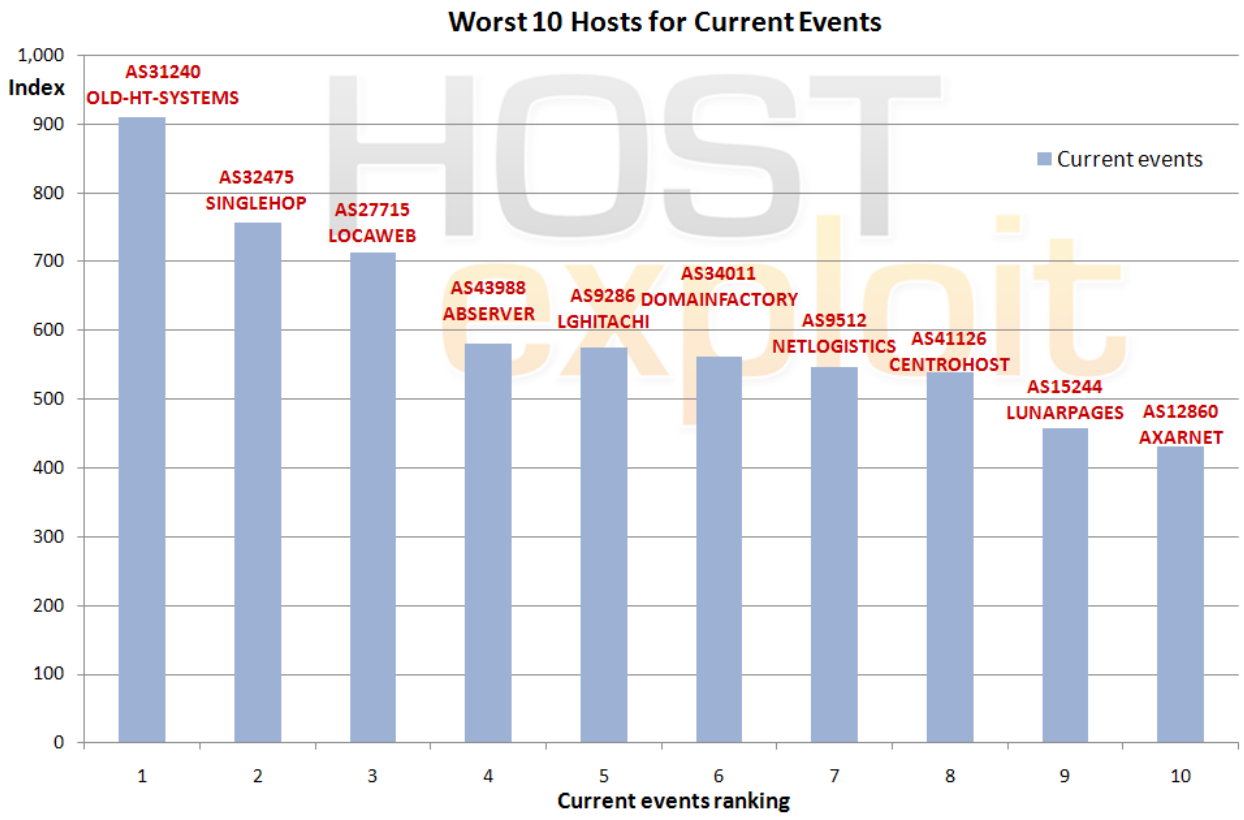


8.6. Current Events

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
16	151.5	**31240**	OLD-HT-SYSTEMS-AS JSC Hosting Telesystems	RU	6,144	**910.8**
11	162.3	**32475**	SINGLEHOP-INC - SingleHop	NL	102,528	**757.4**
7	169.1	**27715**	LocaWeb Ltda	BR	41,472	**714.0**
129	80.6	**43988**	ABSERVER-AS Access Basic Server S.L.	ES	2,048	**580.4**
41	120.1	**9286**	LGH-AS-KR LGHitachi	KR	2,304	**574.9**
56	106.0	**34011**	DOMAINFACTORY domainfactory GmbH	DE	14,592	**561.8**
146	78.2	**9512**	NETLOGISTICS-AU-AP Net Logistics Pty. Ltd.	AU	9,728	**546.9**
19	145.6	**41126**	CENTROHOST-AS JSC Centrohost	RU	4,096	**540.0**
22	143.6	**15244**	ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages	US	40,448	**456.8**
156	76.1	**12860**	AXARNET-NETWORK Red_Axarnet_Madrid	ES	4,096	**430.3**

The fast-changing Current Events field was explored using a range of HostsExploit's own manual and automated processes and focused on the latest and fastest-growing exploits. Such exploits currently include MALfi (XSS/ RCE/RFI/LFI), Zeus and SpyEye.

The vast array of techniques looked at in this category are reflected in the top 10 list below, which covers nine countries.



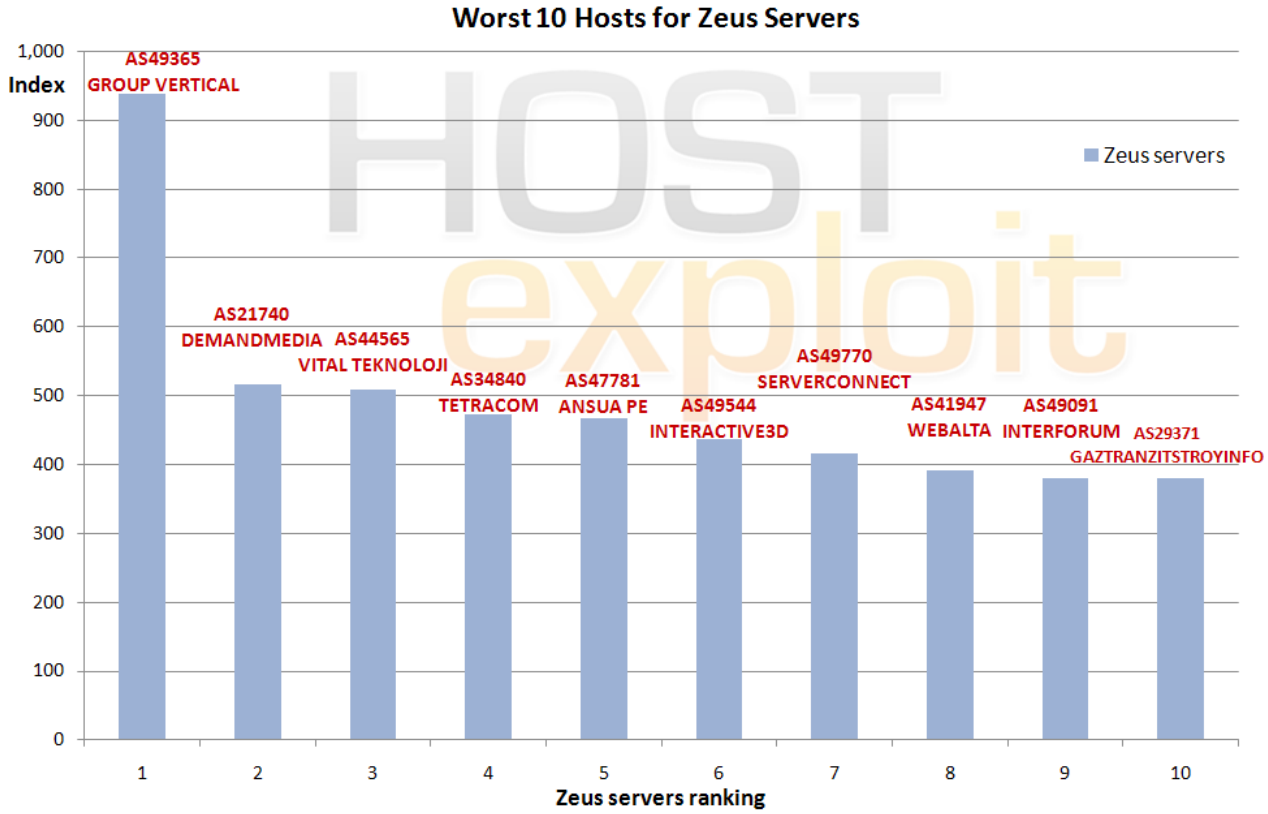
8.7. Botnet Hosting - Zeus

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
9	164.3	**49365**	GR-VERTICAL-AS Group Vertical Ltd	RU	256	**937.5**
2	244.1	**21740**	DemandMedia AS DemandMedia	US	12,544	**516.5**
35	130.2	**44565**	VITAL VITAL TEKNOLOJI	TR	18,432	**508.2**
57	105.7	**34840**	TETRACOM Tetracom CJSC	RU	256	**472.4**
36	126.5	**47781**	ANSUA-AS PE Sergey Demin	UA	512	**468.0**
38	122.7	**49544**	INTERACTIVE3D-AS Interactive3D	NL	40,960	**437.0**
59	105.1	**49770**	SERVERCONNECT-AS ServerConnect Sweden AB	SE	4,096	**415.7**
4	194.2	**41947**	WEBALTA-AS Wahome networks	RU	13,312	**391.2**
52	108.1	**49091**	INTERFORUM-AS Interforum LTD	SP	256	**379.4**
62	102.4	**29371**	GAZTRANZITSTROYINFO-AS LLC "Gaztransitstroyinfo"	LV	256	**379.4**

Our definition of Botnet Hosting relates primarily to Command & Control Servers (C&C) that are used by cyber criminals to manage networks of infected computers, otherwise known as zombies. HostExploit focused on the Zeus botnet as it remains the cheapest and most popular on the underground market. It is common for a single C&C server to manage in the region of 200,000 infected slave machines, often higher.

This section should be considered in conjunction with Section 8.5 on Exploit Servers. In both instances, it is somewhat surprising to see large hosting providers such as DemandMedia and Interactive3D being infected with such high concentrations of C&Cs.

Zeus botnet data is provided by the excellent Zeus Tracker service from abuse.ch.

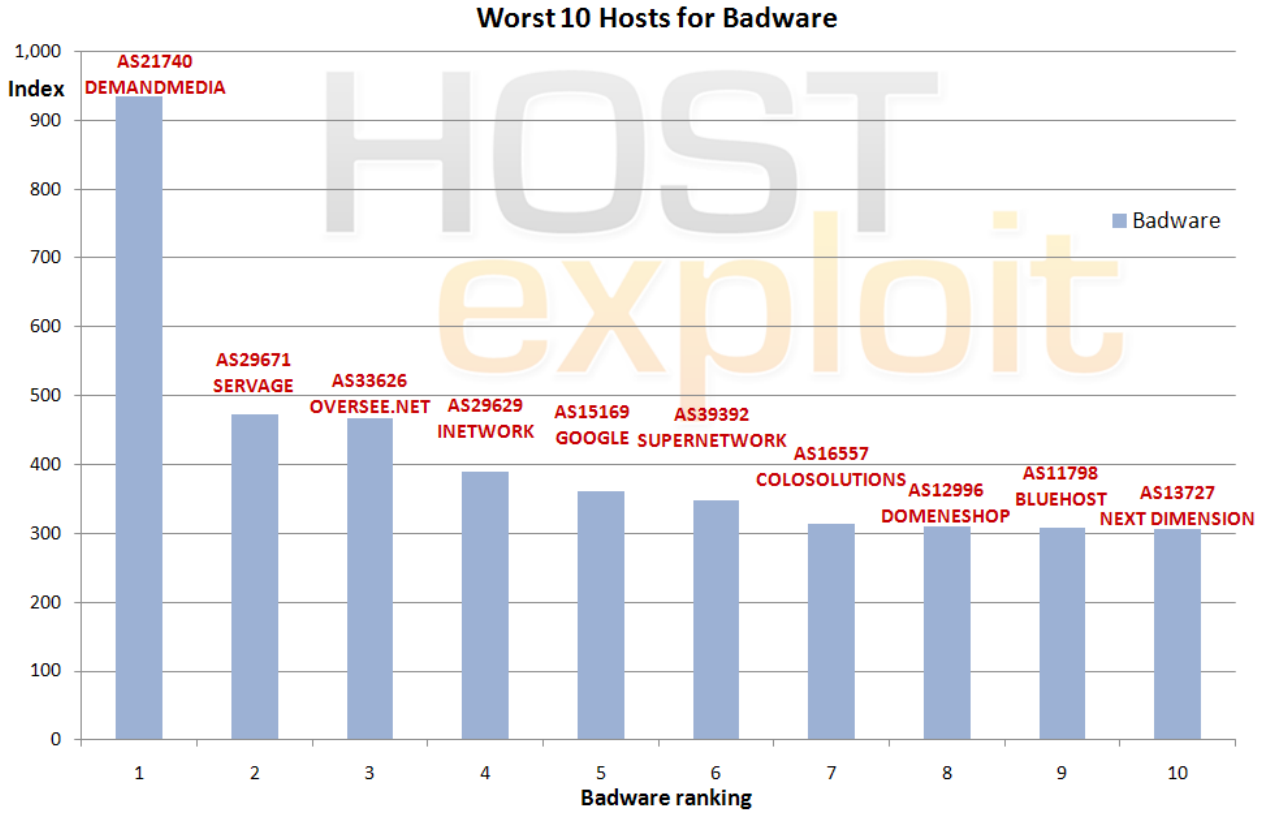


8.8. Badware

HE Rank	HE Index	AS number	AS name, description	Country	# of IPs	Index /1000
2	244.1	**21740**	DemandMedia AS DemandMedia	US	12,544	**934.6**
30	133.7	**29671**	SERVAGE Servage GmbH	DE	12,288	**473.8**
60	104.6	**33626**	OVERSEE-DOT-NET - Oversee.net	US	4,096	**467.7**
110	85.0	**29629**	INETWORK-AS IEUROP AS	FR	8,192	**389.0**
37	123.0	**15169**	GOOGLE - Google Inc.	US	253,952	**360.3**
71	97.5	**39392**	SUPERNETWORK-AS SuperNetwork s.r.o.	CZ	33,536	**348.1**
89	92.6	**16557**	COLOSOLUTIONS - Colo Solutions, Inc.	US	47,360	**313.6**
386	58.4	**12996**	DOMENESHOP Domeneshop AS	NO	3,072	**309.9**
3	209.2	**11798**	BLUEHOST-AS - Bluehost Inc.	US	49,152	**308.8**
142	78.6	**13727**	ND-CA-ASN - NEXT DIMENSION INC	CA	1,024	**305.7**

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

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



Crime Servers

9.1. Background - What Are Crime Servers?

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

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

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

9.2. Crime Servers or Bad Hosts?

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

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

9.2. Crime Servers - Currently Inactive (Not Announced)

ASN	Name	IPs	HE Rank
12604	CITYGAME-AS Kamushnoy Vladimir Vasulyovich	256	4
42229	MARIAM-AS PP Mariam	1,024	19
44107	PROMBUDDETAL-AS Prombuddetal LLC	1,024	5
47560	VESTEH-NET-AS Vesteh LLC	1,024	49
47821	BOGONET-AS PE Syrovatko Igor Mykolayevish	256	183
49093	BIGNESS-GROUP-AS Bigness Group Ltd.	512	36
49934	VVPN-AS PE Voronov Evgen Sergiyovich	256	58
50033	GROUP3-AS GROUP 3 LLC.	256	26
50215	TROYAK-AS Starchenko Roman Fedorovich	256	1214
50369	VISHCLUB-AS Kanyovskiy Andriy Yuriyovich	1,024	68
50390	SMILA-AS Pavlenko Tetyana Oleksandrivna	256	30
50678	SAINTVPN	256	N/A

9.3. Crime Servers - Currently Active

ASN	Name	IPs	HE Rank
34840	TETRACOM Tetracom CJSC	256	N/A
29557	ZONONET PE Anton Kasminin	256	N/A
24826	KHARKOV-TERMINALS-AS PE Viktor Nastechenko	256	35
29106	VOLGAHOST-AS PE Bondarenko Dmitriy Vladimirovich	256	56
29371	GAZTRANZITSTROYINFO-AS LLC "Gaztransitstroyinfo"	256	100
44557	DRAGONARA Dragonara Alliance Ltd	1,536	88
44565	VITAL VITAL TEKNOLOJI	18,432	50
47434	FORTUNE-AS Fortune Science and Production Company	256	154
47781	ANSUA-AS PE Sergey Demin	512	96
49091	INTERFORUM-AS Interforum LTD	256	634
49314	NEVAL PE Nevedomskiy Alexey Alexeevich	256	87
49365	GR-VERTICAL-AS Group Vertical Ltd	256	91

Conclusions

10.1. Conclusions

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

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

- Such a report and the defined "HE Index" acts as a consumer barometer for each of the 33,410 currently advertised and commercial ASes.

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

- The release of the first Top 50 Bad Hosts delivered a successful outcome with some contacted hosts significantly decreasing levels of abuses by up to 90%.

- The findings from this report will reinforce the need to demonstrate willingness to 'clean up' systems when bad publicity is seen as harmful to business. The biggest success to date is illustrated by AS30407 Velcom, which was ranked as the #1 Bad Host in December's report, and has dramatically reduced its badness levels by over 50 per cent.

- It is encouraging to see a willingness to begin the process of 'cleaning up' known abuses but as the new report shows there is still much work to be done.

- At worst host ranking #1 Ecatel AS29083, is carrying a wide range of spam, exploit servers and infected web sites. In at #2, and somewhat surprisingly as a well-known household name, is Demand Media / ENom AS21740, hosting large amounts of badware.

- The, HE Index, therefore, has the ability to express a myriad of different internet malpractices in an easy to understand format. In that way it shows who is hosting the worst of these offences and, following on from disclosure, the first steps towards action against abuses can be taken.

As originally shown in the December report and only touched on within this report, the overall analysis further highlights a relatively small number of dedicated 'Crime Servers', and related 'bullet proofed' hosting enterprises. A further supplementary disclosure of the worst of this type of criminal activity will be released in a new report from HostExploit which is to follow. Examples and results of actions against crime servers, such as Troyak and its peers, will be a feature of one of these supplements.

10.2. Worst Culprits Within Tracked Sectors

Category	HE Rank	ASN	Name	Country
Infected Web Sites	21	**35908**	VPLSNET	US
Spam	28	**45899**	VNPT-AS	VN
Botnet C&C Servers	14	**23522**	IPNAP-ES	US
Phishing	167	**34848**	COMENDO-AS	DK
Exploit Servers	1	**29073**	ECATEL-AS	NL
HE Current Events	16	**31240**	OLD-HT-SYSTEMS-AS	RU
Zeus Botnet C&Cs	9	**49635**	GR-VERTICAL-AS	RU
Badware	2	**21740**	DemandMedia	US

From the figures above we can see the distribution of bad servers to be a global problem and not one which is focused in one area. Through the research conducted for this report we have also found that the attack vector preferred by criminals for different activities depends highly on the nature of their objective. For example the distribution of malware is preferably hosted in the western world for reasons of trust, while spam servers are usually kept in countries with laxer controls on their internet providers for the reason of obvious spikes in server usage.

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 Indicator

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.

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.

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.

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.