HostExploit's

World Hosts Report

September 2013

Abstract

For the first time, hosts registered in a single country – *the United States* – occupy the worst three places in the Top 50 list of hosts and networks.

Examining hosting practices and standards is as relevant as ever in the quest for much needed improvements to a system that has few enforceable restraints.

Quantification through the measurement levels of cybercriminal activity on servers around the world is one way to achieve this aim. Since 2009, HostExploit's World Hosts Report (formerly Top 50 Bad Hosts) has been examining all 44,000+ publicly-routed Autonomous Systems in the world, gathering data on infected websites, botnets, spam and other activity, before combining the research with trusted community sources and to arrive at a reliable analysis of the results.

The report makes suitable reading for service providers, security professionals, webmasters and policymakers alike. For the most part, the reader is left to draw their own conclusions, as numbers speak for themselves. However, it should be stressed that most malicious content is not hosted knowingly – often it is as a result of inaction, and sometimes hosts can be the victims.

However, it remains true that all cybercrime, cyber-attacks, and Internet badness is hosted from someone and from somewhere; i.e. located on and allocated to an ASN. So it makes sense that this is where we should start in the continuing quest for solutions.

- Jart Armin

ISBN 978-0-9836249-6-7

Comparative Data

AA419

Abuse.CH

Clean-MX.DE

Cyscon SIRT

Emerging Threats

Google Safe Browsing

Group-IB

HostExploit

hpHosts

ISC

KnujOn

MalwareDomains

MalwareDomainList

RashBL

Robtex

Shadowserver

SiteVet

Spamhaus

SRI International

StopBadware

SudoSecure

Team Cymru

The Measurement Factory

UCE-Protect

Editor

Jart Armin

Reviewers

Dr. Bob Bruen

Raoul Chiesa

Peter Kruse

Andre' DiMino

Thorsten Kraft

Andrey Komarov

Godert Jan van Manen

Steven Dondorp

Edgardo Montes de Oca

Contributors

Steve Burn

Greg Feezel

Andrew Fields

David Glosser

Niels Groeneveld

Matthias Simonis

Will Rogofsky

Philip Stranger

Bryn Thompson

DeepEnd Research

In association with ECYFED

ECYFED
European Cyber Security Federation

GROUP IB

CSIS

NORTHWAVE

cyscon

SITEVET

montimage

Partner of the ACDC project

ACDC
the Advanced Cyber Defence Centre

Get in touch

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

Editorial

For the first time, hosts registered in a single country – *the United States* – occupy the worst three places in the Top 50 list of hosts and networks.

The top three hosts are AS33182 HostDime.com, AS26347 DreamHost, and AS11042 Landis Holdings. The report, spanning the three months of Q3 2013, ranks hosts by the highest observed concentrations of malicious activity, such as malware, spam and botnets.

This, of course, is not a record to be proud of. Over a long period of time, respected sources have warned of the high levels of malicious activity found in the United States, particularly as relating to phishing[1,2].

What are the causes for this? The main reasons include:

- **Plentiful and cheap hosting.**
- **More integration with anonymity services.** Most domains registrars and web hosts offer 'whois proxy' services, and increased options to purchase via Bitcoin.
- **Enhanced reputation.** Less chance of being blocked by country, and a more reputable look for phishing scams.

However, it is not all bad news for the United States – the Country listings show a downward movement to No. 9 from No. 5. Exceptionally good individual performances from previous high-ranking hosts (including AS21740 eNom, ranking 1150, and AS33626 Oversee, ranking 943) help contribute to this improved status.

So the over-riding good news is: it *is* possible for hosts to clean up. But what incentives are there to do so?

At the moment, legally, there is very little, Cross-border action is notoriously complex and consumer rights vary from country to country, if they exist at all. In the US, for example, ISPs are resisting FCC attempts to introduce industry standards and accountability that could open the door to the imposition of financial penalties for failing to protect consumers.

But even without pecuniary punishments, it just makes good sense for a host to abide by good practices and to make every reasonable effort to remain clean. The benefits are manifold - is better for business, for the economy and for national 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.

1 http://www.zdnet.com/blog/security/how-many-people-fall-victim-to-phishing-attacks/5084

2 http://www.gartner.com/newsroom/id/936913

Methodology

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

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

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

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

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

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

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

Why do these hosts allow this activity?

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

Definitions

IPs

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

Country

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

HE Index

HostExploit's quantitative metric, representing the concentration of malicious activity served from an Autonomous System.

HE Rank

Rank of the Index compared to all 44,556 ASes.

Please see the Glossary for further definitions.

Top 50 Hosts

A list of the 50 ASes with the highest HE Indexes i.e. the highest observed concentrations of malicious activity.

Autonomous System (AS)

A logical collection of Internet routes, controlled by an organization or ISP.

ASN

Unique number assigned to the AS.

HE Index

HostExploit's quantitative metric, representing the concentration of malicious activity served from an Autonomous System.

HE Rank

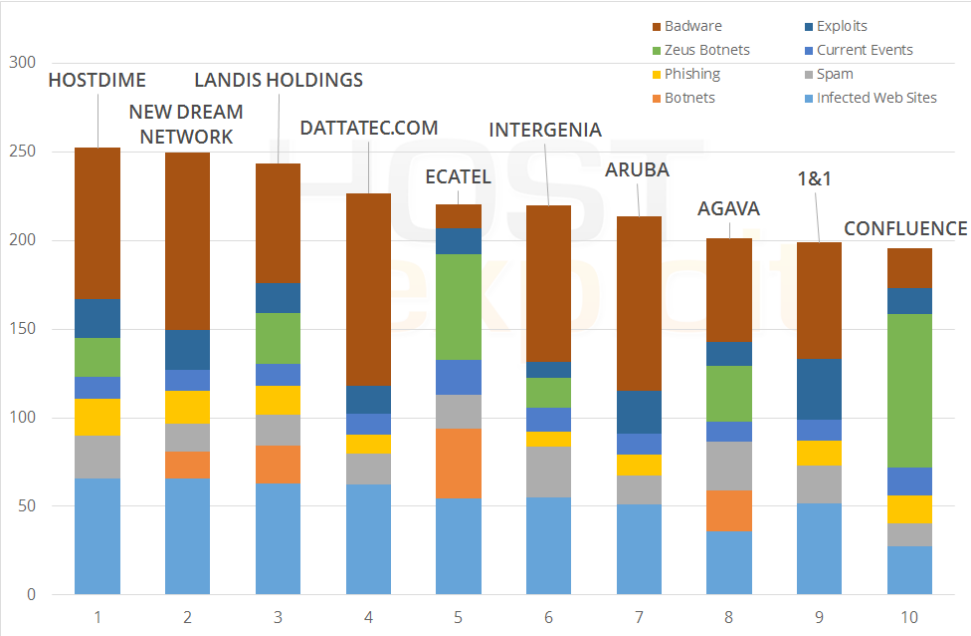
Rank of the Index compared to all 44,556 ASes.

IPs

Number of Internet Protocol addresses assigned to the AS.

HE Rank	HE Index	ASN	Name	Country	IPs
1	252.33	33182	HostDime.com, Inc.	US	63,232
2	249.28	26347	New Dream Network, LLC	US	230,656
3	243.51	11042	Landis Holdings Inc	US	28,416
4	226.75	27823	Dattatec.com	AR	8,192
5	220.57	29073	Ecatel Network	NL	13,312
6	219.59	8972	Intergenia AG	DE	149,760
7	213.56	31034	Aruba S.p.A.	IT	145,664
8	201.20	43146	Agava Ltd.	RU	19,712
9	198.72	8560	1&1 Internet AG	DE	370,176
10	195.66	40034	Confluence Networks Inc	VG	12,288
11	194.54	47583	Hostinger International	US	11,008
12	193.03	25532	Masterhost	RU	77,824
13	191.61	12824	home.pl	PL	204,800
14	184.51	34619	Cizgi Telekomunikasyon	TR	30,208
15	183.00	29182	ISPsystem	RU	44,288
16	178.01	30633	Leaseweb USA	US	14,592
17	174.69	46606	Unified Layer	US	508,416
18	162.44	26496	GoDaddy.com, LLC	US	1,636,352
19	162.05	39743	Voxility S.R.L.	RO	55,808
20	156.79	16276	OVH Systems	FR	1,170,944
21	154.97	44112	SpaceWeb JSC	RU	3,584
22	154.50	50465	IQHost Ltd	RU	2,048
23	150.71	48159	Telecommunication Infrastructure	IR	192,256
24	150.55	16265	LeaseWeb B.V.	NL	365,312
25	149.34	51559	Netinternet	TR	18,432
26	148.55	36351	SoftLayer Technologies Inc.	US	1,401,344
27	141.61	25504	Vautron Rechenzentrum AG	DE	22,784
28	138.73	42612	ASN de Dinahosting SL	ES	18,432
29	137.64	24940	Hetzner Online AG	DE	639,744
30	137.20	4134	Chinanet Backbone	CN	116,932,576
31	132.51	46475	Limestone Networks, Inc.	US	90,112
32	131.42	15626	ITL Company	UA	19,200
33	130.18	41126	JSC Centrohost	RU	4,096
34	130.16	38731	Vietel - CHT Compamy Ltd	VN	28,672
35	126.28	58001	Ideal Solution Ltd	RU	2,560
36	125.61	32475	SingleHop	US	419,584
37	124.85	42244	eServer.ru Ltd.	RU	33,536
38	124.45	57668	Santrex Internet Services	SC	5,632
39	122.56	6147	Telefonica del Peru	PE	2,048,768
40	121.23	21844	ThePlanet.com Internet Services	US	1,509,376
41	120.63	8358	GTS Hungary	HU	30,720
42	120.21	15169	Google Inc.	US	669,696
43	118.32	47869	Netrouting Data Facilities	NL	23,040
44	118.27	9891	CS Loxinfo	TH	23,296
45	118.07	21219	Datagroup	UA	140,544
46	117.55	31815	Media Temple, Inc.	US	113,152
47	116.79	48031	PE Ivanov Vitaliy Sergeevich	UA	15,616
48	116.60	29550	Simply Transit Ltd	GB	116,224
49	115.81	18479	Universo Online S.A.	BR	24,064
50	115.49	41079	SuperHost.pl	PL	4,864

Top 10 Visual Breakdown



What's this?

The chart to the left gives a visual representation of how much of a contribution each sector makes to an AS's Index.

This enables you to see where a host needs to make the most improvement at a quick glance.

Top 10 Newly Registered

The following 10 ASes have the highest Indexes out of the 2,058 ASes registered since the last report. These could potentially be of future interest.

HE Rank	HE Index	ASN	Name	Country	IPs
60	110.1	132524	Tata Institute	IN	512
193	74.1	12860	Axarnet Comunicaciones SL	ES	6,912
464	51.7	60751	Joshua Jameson / ServeByte	IE	1,024
484	50.7	43449	Dimline Ltd.	RU	512
613	45.1	55293	A2 Hosting, Inc.	US	24,576
923	34.5	35042	ISP4P IT Services	DE	26,624
937	34.2	199094	Accord OOD	BG	1,536
1,015	31.7	61036	JSC Dadeh Pardazi Fanava	IR	41,984
1,064	30.6	132497	Smartlink Broadband Services	IN	9,984
1,636	22.2	132527	Department of Posts	IN	1,024

Number of ASes

At March 2013 report
43,454

As of this report
44,556

New ASes
2,058

Removed
956

Net gain
1,102

What's this?

We calculate an index for each country using a similar methodology to that for individual ASes.

The Country Index scores a country's badness levels out of 1,000, without being driven too strongly by the number of hosts in that country.

The table to the right shows the resulting Top 10 countries from this methodology, along with the three sectors with the highest indexes.

Top 10 Countries

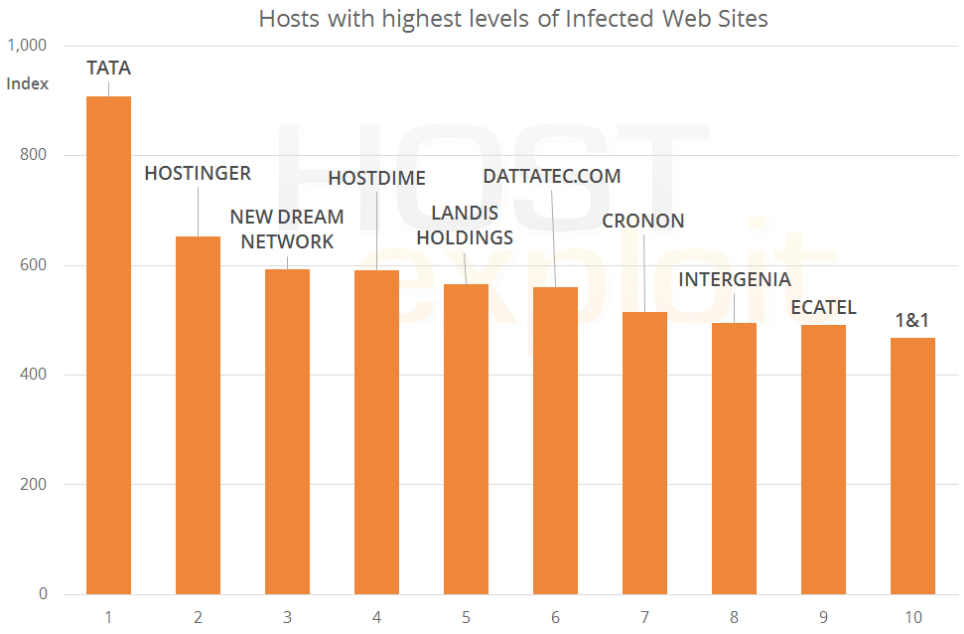
Country	Name	ASes	IPs	Rank	Index
VG	VIRGIN ISLANDS, BRITISH	6	18,688	1	435.5
	Highest sector		Infected web sites	1	905.3
	2nd-highest sector		Botnet C&Cs	1	889.0
	3rd-highest sector		Current events	1	823.9
PL	POLAND	1,590	21,932,032	3	306.7
	Highest sector		Current events	3	666.7
	2nd-highest sector		Phishing	2	648.1
	3rd-highest sector		Zeus botnets	4	431.7
RU	RUSSIAN FEDERATION	4,095	55,361,280	7	249.8
	Highest sector		Badware	3	502.5
	2nd-highest sector		Phishing	7	488.2
	3rd-highest sector		Current events	7	386.9
HU	HUNGARY	173	5,100,544	4	276.9
	Highest sector		Phishing	1	909.0
	2nd-highest sector		Current events	2	718.4
	3rd-highest sector		Zeus botnets	3	437.5
DE	GERMANY	1,294	119,035,296	6	251.3
	Highest sector		Zeus botnets	2	478.0
	2nd-highest sector		Current events	6	390.7
	3rd-highest sector		Phishing	11	261.1
KG	KYRGYZSTAN	27	300,544	8	242.9
	Highest sector		Badware	2	861.2
	2nd-highest sector		Exploit servers	2	465.7
	3rd-highest sector		Infected web sites	6	273.7
TR	TURKEY	304	21,711,872	10	238.7
	Highest sector		Current events	4	508.8
	2nd-highest sector		Zeus botnets	7	326.6
	3rd-highest sector		Botnet C&Cs	8	237.5
SC	SEYCHELLES	7	84,992	18	162.0
	Highest sector		Exploit servers	1	905.5
	2nd-highest sector		Infected web sites	2	840.8
	3rd-highest sector		Current events	171	68.4
US	UNITED STATES	14,573	1,233,079,112	12	218.1
	Highest sector		Current events	11	302.4
	2nd-highest sector		Zeus botnets	10	257.1
	3rd-highest sector		Phishing	13	241.0
UA	UKRAINE	1,666	15,120,384	11	221.1
	Highest sector		Badware	4	394.9
	2nd-highest sector		Phishing	9	284.2
	3rd-highest sector		Current events	13	283.3

Infected Web Sites

Index	ASN	Name	Country	IPs	HE Rank	HE Index
907.2	132524	Tata Institute	IN	512	60	110.1
653.1	47583	Hostinger International	US	11,008	11	194.5
592.0	26347	New Dream Network, LLC	US	230,656	2	249.3
591.2	33182	HostDime.com, Inc.	US	63,232	1	252.3
564.9	11042	Landis Holdings Inc	US	28,416	3	243.5
560.5	27823	Dattatec.com	AR	8,192	4	226.8
515.1	25504	Vautron Rechenzentrum AG	DE	22,784	27	141.6
495.5	8972	Intergenia AG	DE	149,760	6	219.6
490.6	29073	Ecatel Network	NL	13,312	5	220.6
467.3	8560	1&1 Internet AG	DE	370,176	9	198.7

All of the top 3 in the overall HE Index score highly in this category with AS26347 DreamHost at No. 3, AS33182 HostDime at No. 4 and AS11042 Landis at No. 5.

The No.1 host in this category, AS132524 Tata is newly registered in India with a low number of IPs. This could be symptomatic of this host being used for temporary services or a "throwaway ASN".



Did you know?

The top 7 ranked hosts overall all appear in this list.

The numbers

AS132524 Tata has the 8th-lowest number of infected web sites within this Top 10, but is a considerably smaller entity, which pushes it into the top position.

Did you know?

Sotal-Interactive and ISPsystem are both primarily hosted out of Russia, but registered in Ukraine and Luxembourg, respectively.

Botnet C&Cs

Index	ASN	Name	Country	IPs	HE Rank	HE Index
1,000.0	50465	IQHost Ltd	RU	2,048	22	154.5
488.4	61322	Sotal-Interactive ZAO	RU	256	414	55.2
475.7	56617	SIA "VPS Hosting"	LV	1,024	168	76.4
474.4	29182	ISPsystem	RU	44,288	15	183.0
415.0	26230	Telecom Ottawa Limited	CA	21,504	586	46.6
404.8	46785	Quasar Data Center, Ltd.	US	6,656	236	67.6
351.9	29073	Ecatel Network	NL	13,312	5	220.6
318.9	29141	Bradler & Krantz GmbH	DE	19,456	55	113.4
294.3	47900	Art-master LLC	UA	256	950	33.7
292.1	47161	KosmoHost IT Technologies	RU	512	966	33.4

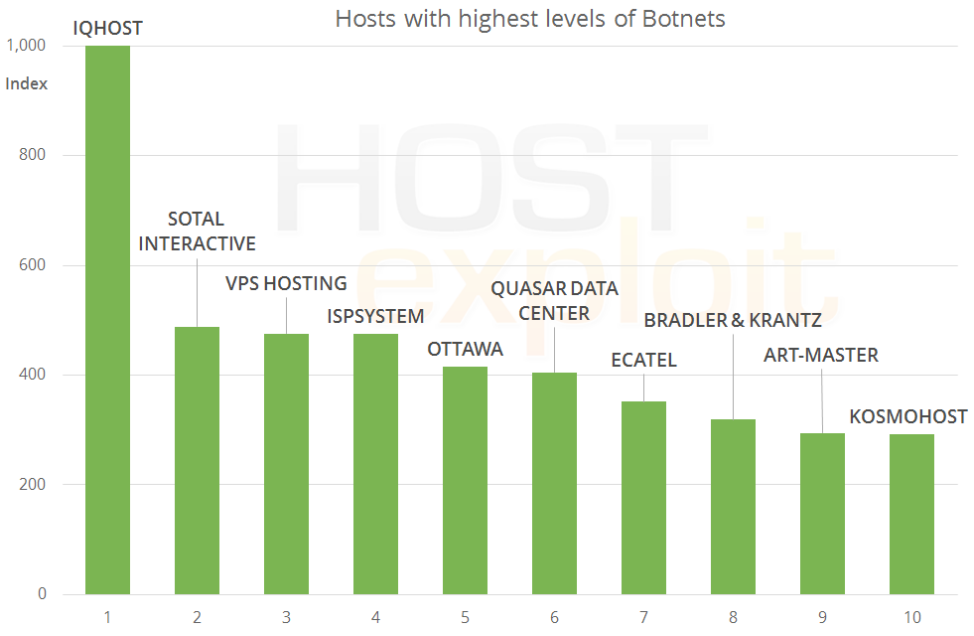
None of the top 4 in this category have changed since the Q1 2013 report.

In fact, AS50465 IQHost has held the top position since Q2 2012. That makes it more than an entire year as the No. 1 host for botnet C&Cs.

The numbers

124 botnet C&Cs were observed in this period, down from 132 in the previous report.

This is lower than the total number of incidences in any other category. The power that each C&C holds, however, underlines their importance from a security perspective.

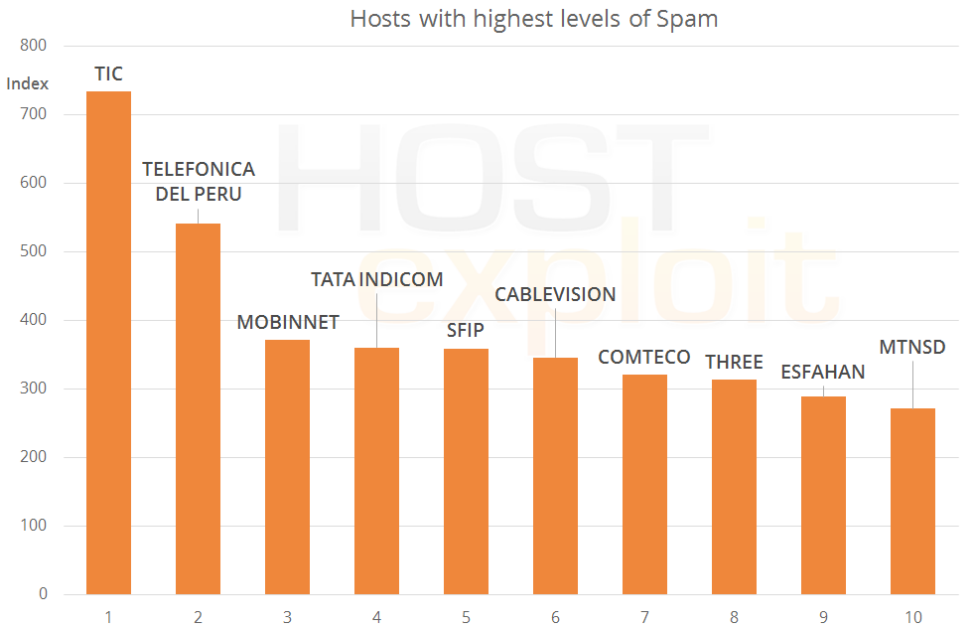


Spam

Index	ASN	Name	Country	IPs	HE Rank	HE Index
733.8	48159	Telecommunication Infr...	IR	192,256	23	150.7
541.4	6147	Telefonica del Peru	PE	2,048,768	39	122.6
371.1	50810	Mobin Net Communication	IR	230,400	228	68.7
360.1	55740	Tata Indicom	IN	262,144	244	66.7
358.9	57879	sfip84	DE	5,120	242	66.8
345.4	28548	Cablevisión, S.A. de C.V.	MX	147,968	274	64.0
320.2	27839	Comteco Ltda	BO	47,616	336	59.4
313.1	45727	Three Hutchison	US	14,400	354	58.2
288.4	58085	Esfahan Telecommunication	IR	131,072	437	53.5
271.0	36972	MTNSD	SD	3,328	488	50.5

The top positions in this category follow the trend seen in previous reports. Spammers continue to prefer countries with the lowest levels of regulations and barriers to AS registration.

Eight of the top 10 hosts fit this description, with Iran, Peru, Mexico, India and Bolivia represented here. The exception are seen in AS57879 SFIP, registered in Germany, and AS45727 Three, which although is registered in Indonesia, is hosted out of the United States.



What do we do?

For this category, we examine traditional spam servers as well as spam bots, crawlers and community-driven IP reputations.

Did you know?

Russian telecoms provider MegaFon has finally moved out of the Top 10, having had a total of *four* ASes simultaneously in the Spam top 10 in 2012.

The numbers

More than 100,000 sources of spam were examined during the reporting period.

Did you know?

Cisco estimated in 2012 that around 100 billion dollars were lost to phishing attacks, from both corporations and consumers.

The numbers

779 unique phishing campaigns were examined during this reporting period.

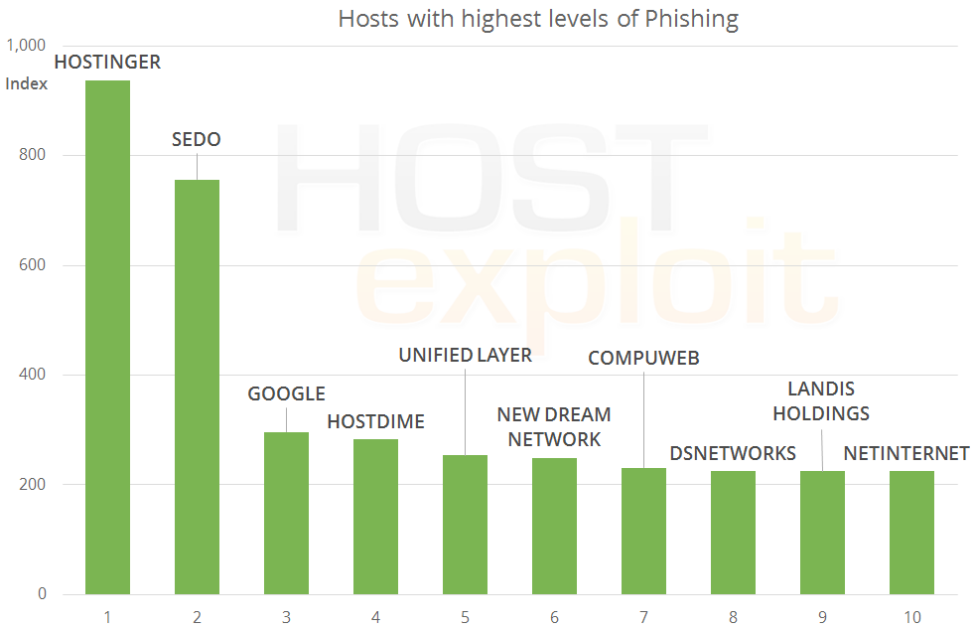
Phishing

Index	ASN	Name	Country	IPs	HE Rank	HE Index
937.3	47583	Hostinger International	US	11,008	11	194.5
756.3	47846	Sedo GmbH	DE	1,280	229	68.1
296.4	15169	Google Inc.	US	669,696	42	120.2
282.9	33182	HostDime.com, Inc.	US	63,232	1	252.3
253.2	46606	Unified Layer	US	508,416	17	174.7
248.7	26347	New Dream Network, LLC	US	230,656	2	249.3
230.9	15510	Compuweb Comms...	GB	6,912	78	102.5
225.2	46816	DirectSpace Networks, LLC.	US	8,192	578	47.0
225.0	11042	Landis Holdings Inc	US	28,416	3	243.5
224.2	51559	Netinternet	TR	18,432	25	149.3

Major web hosting companies in regulated countries dominate the top 10 positions in this category, including all three of our aforementioned 'worst' hosts.

In this fast moving sector, phishers prefer the ease and availability of hosting in established regions. Since phishing sites are short-lived, guarantees of uptime are not needed and so it is not necessary to host from unregulated regions.

The increased apparent legitimacy of a banking or e-commerce site being hosted from the United States or the United Kingdom is, however, beneficial to a phishing scam.

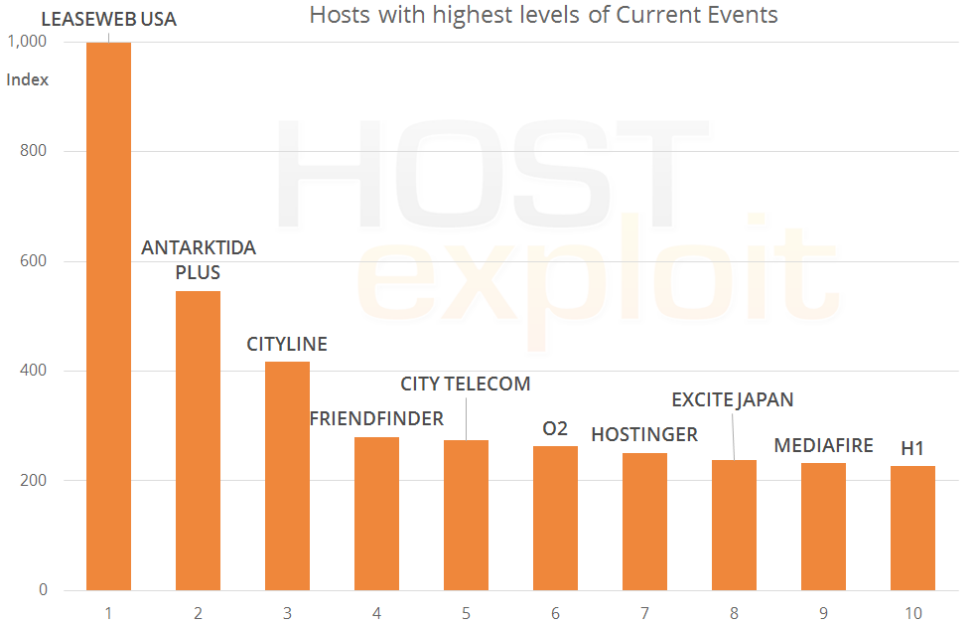


Current Events

Index	ASN	Name	Country	IPs	HE Rank	HE Index
998.6	30633	Leaseweb USA	US	14,592	16	178.0
545.8	51699	Antarktida-Plus	SC	256	305	61.6
417.0	34023	PE Shattah Zia G.Naman	EU	256	283	63.3
280.2	32527	FriendFinder Networks	US	2,560	1,008	32.0
273.9	48271	City Telecom	KG	8,192	51	115.5
262.3	31080	o2 Sp. Z.o.o.	PL	512	311	61.2
251.3	47583	Hostinger International	US	11,008	11	194.5
237.2	45682	Excite Japan Co., Ltd.	JP	2,048	1,267	27.3
231.5	46179	MediaFire, LLC	US	3,072	1,320	26.6
227.0	6870	H1 LLC	RU	5,632	1,383	26.0

Once again AS51699 Antarktida scores highly in this category but the top position for this period is taken by AS30633 Leaseweb USA.

As the name suggests, Currents Events is a fast-changing sector, which results in a variety of hosts being used to host new types of malicious content, and large movements from month to month.



Did you know?

Current Events is HostExploit's own measurement of the most up-to-date and fast-changing attack vectors being utilized worldwide.

These have recently included variants of MALfi attacks (XSS/RCE/RFI/LFI), clickjacking techniques, and large botnets.

The numbers

After a dip in the number of instances observed the previous reporting period, this time the number is back up by 67%.

Did you know?

Zeus, a form of botnet delivered via a trojan payload, remains one of the most popular varieties of botnet, some 6 years after it first gained popularity in the underground cybercriminal scene.

Zeus has been continually improved, with its many variations proving to be adept at bypassing security systems and gathering large networks of zombie machines.

Zeus Botnets

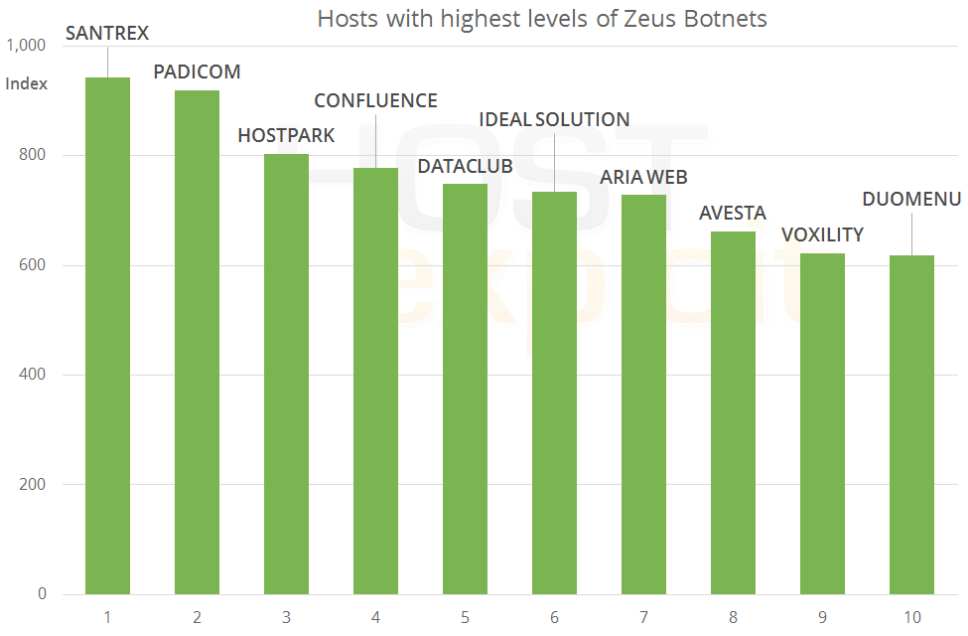
Index	ASN	Name	Country	IPs	HE Rank	HE Index
942.9	57668	Santrex Internet Services	SC	5,632	38	124.4
919.6	34201	Padicom Solutions SRL	RO	6,400	76	102.9
803.6	51743	PE Taran Marina Vasil'evna	UA	256	107	92.2
778.0	40034	Confluence Networks Inc	VG	12,288	10	195.7
748.7	52048	DataClub S.A.	LV	2,048	97	95.4
734.7	58001	Ideal Solution Ltd	RU	2,560	35	126.3
727.9	57230	Aria Web Development LLC	GB	2,816	62	109.6
662.0	54444	Avesta Networks LLC	US	5,632	77	102.9
622.2	39743	Voxility S.R.L.	RO	55,808	19	162.0
618.0	16125	UAB Duomenu Centras	LT	7,936	123	85.8

The top position here, taken by AS57668 Santrex, has a shared commonality with the No. 1 from Q1, as it is routed via the Seychelles.

In the previous report, the top position was held by AS58001 Ideal Solution, now at No. 5, which is registered in the Seychelles but routed via the Russian Federation.

The numbers

The total number of Zeus servers observed has continued to remain nearly constant. This suggests that Zeus continues to be a successful and profitable botnet toolkit of choice.

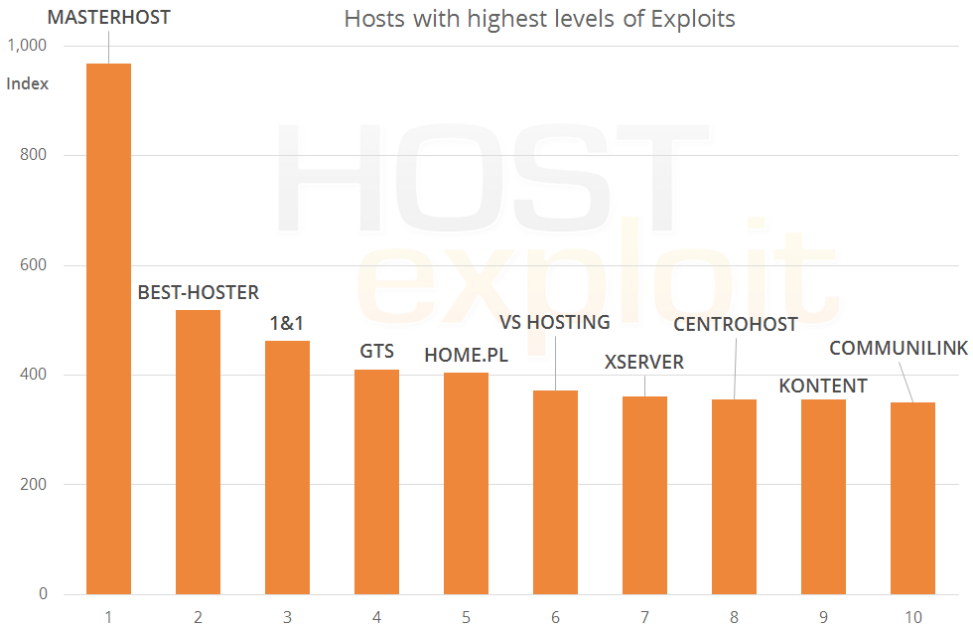


Exploits

Index	ASN	Name	Country	IPs	HE Rank	HE Index
968.4	25532	Masterhost	RU	77,824	12	193.0
517.9	49693	Best-Hoster Group Co. Ltd	RU	2,048	70	105.5
462.1	8560	1&1 Internet AG	DE	370,176	9	198.7
410.1	8358	GTS Hungary	HU	30,720	41	120.6
404.4	12824	home.pl	PL	204,800	13	191.6
371.2	43541	VSHosting s.r.o.	CZ	14,336	155	79.1
361.7	48031	PE Ivanov Vitaliy Sergeevich	UA	15,616	47	116.8
355.5	41126	JSC Centrohost	RU	4,096	33	130.2
355.5	24973	KONTENT GmbH	DE	4,096	196	73.4
350.3	38277	CommuniLink Internet	HK	4,608	230	68.0

This category contains some repeat offenders as both AS25532 Masterhost and AS49693 Best-Hoster have been present here in previous reports.

The majority of hosts here, however, are new entrants in this sector.



Did you know?

Exploits and the web sites that serve them are a key piece of the cybercrime puzzle, as they often provide the first point-of-entrance into a victim's computer.

Exploits take advantage of vulnerabilities in software, which may or may not be publicly-known. The exploit may utilize other code that directly harms the victim's system, or it may only be used by the attacker as a payload to take initial control of the machine.

The numbers

The top 10 ASes in this category account for over 16% of all exploits observed during the reporting period, down from 29% last report.

Did you know?

Badware fundamentally disregards how users might choose to employ their own computer. Examples of such software include spyware, types of 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.

Badware

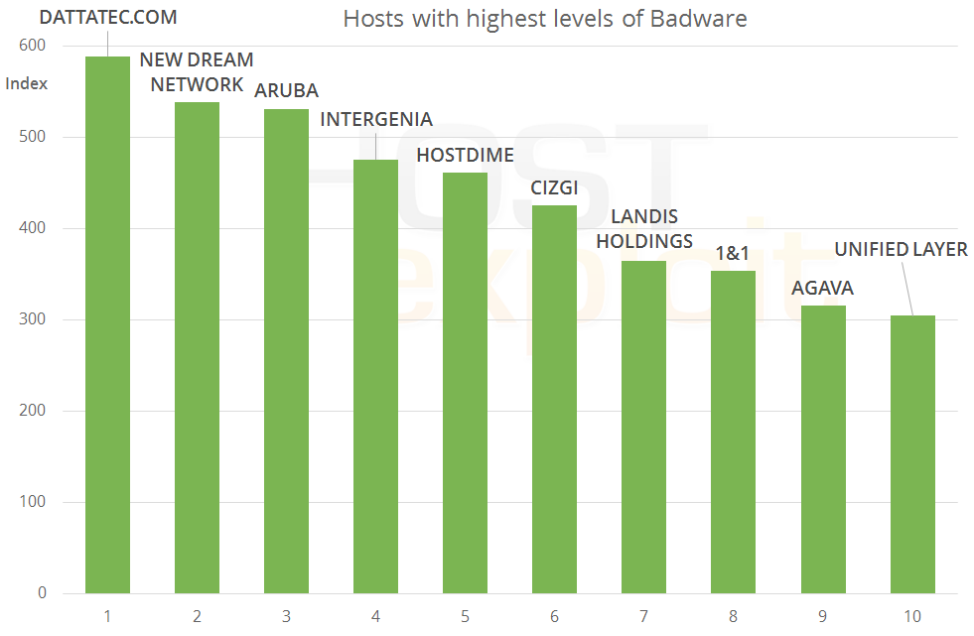
Index	ASN	Name	Country	IPs	HE Rank	HE Index
588.4	27823	Dattatec.com	AR	8,192	4	226.8
538.7	26347	New Dream Network, LLC	US	230,656	2	249.3
531.0	31034	Aruba S.p.A.	IT	145,664	7	213.6
475.6	8972	Intergenia AG	DE	149,760	6	219.6
461.2	33182	HostDime.com, Inc.	US	63,232	1	252.3
425.0	34619	Cizgi Telekomunikasyon	TR	30,208	14	184.5
364.8	11042	Landis Holdings Inc	US	28,416	3	243.5
353.2	8560	1&1 Internet AG	DE	370,176	9	198.7
315.7	43146	Agava Ltd.	RU	19,712	8	201.2
304.5	46606	Unified Layer	US	508,416	17	174.7

In this fast changing sector only two hosts remain the same when compared to Q1, AS31034 Aruba and AS8560 1&1 Internet. Badware is responsive to short-term trends and the hosts in this category will, by necessity, change accordingly.

Our top three 'worst' hosts also feature highly in this category, which taken together with equally high scores for phishing and infected websites, suggest similar requirements of the hosts selected to serve these types of malicious activities.

The numbers

The top 10 hosts in this category account for 23% of the total instances of badware observed.



AS (Autonomous System)

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

Badware

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

Blacklists

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

Botnet

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

Current Events

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

CSRF (cross site request forgery)

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

DDOS (Distributed Denial of Service)

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

DNS (Domain Name System)

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

DNS Security Extensions (DNSSEC)

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

DNSBL

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

Exploit

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

Hosting

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

IANA (Internet Assigned Numbers Authority)

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

ICANN (Internet Corporation for Assigned Names and Numbers)

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

IP (Internet Protocol)

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

IPv4

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

IPv6

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

ISP (Internet Service Provider)

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

LFI (Local File Inclusion)

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

MALfi (Malicious File Inclusion)

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

Malicious Links

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

MX

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

NS (Name Server)

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

Open Source Security

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

Pharming

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

Phishing

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

Registry

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

Registrars

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

Remote File Inclusion (RFI)

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

Rogue Software

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

Rootkit

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

Sandnet

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

Spam

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

Trojans

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

Worms

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

XSA (Cross Server Attack)

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

Appendix 2

HE Index Calculation Methodology

September 25, 2013

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 Safe Browsing data through StopBadware eliminated. Source weightings refined.
4.	October 2011	Sources refined. Source weightings refined.
5.	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 representing 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 represent the size of the AS, but it is possible for a server to carry out malicious activity without a single registered domain, as was the case with McColo. Therefore, it would seem more pragmatic to use the size of the IP range (i.e. number of IP addresses) registered to the AS through the relevant Regional Internet Registry.

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

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

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

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

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

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

C: *IP weighting = 20,000*

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

5 Calculation

For each data source, three factors are calculated.

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

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

where:
B_m: *maximum Bayesian ratio*

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

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

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

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

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

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

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

The index for each data source is then calculated as:

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

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

The overall HE Index is then calculated as:

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

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