HostExploit's

World Hosts Report

March 2013

Abstract

As malware continues to evolve, and cybercriminals continue to learn, one particular fundamental remains constant – almost all malicious threats are physically hosted somewhere. For this reason, it remains as important as ever to examine hosting practices and standards and consider how they can be improved.

One such way is to measure levels of cybercriminal activity on servers around the world, and attempt to quantify the results. Such has been the aim of HostExploit's *World Hosts Report* (formerly *Top 50 Bad Hosts*) since publication began in 2009. The quarterly reports examine all 43,000+ 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 analyzing 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.

This quarter we see the return of Dutch hosting provider Ecatel to the #1 rank, having held the position at various times in the past. Ecatel does not top the rankings for any particular category of activity, but rather for a consistently poor showing across the board.

- Jart Armin

ISBN 978-0-9836249-4-3

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

Contributors

Steve Burn

Greg Feezel

Andrew Fields

David Glosser

Niels Groeneveld

Matthias Simonis

Will Rogofsky

Philip Stranger

Bryn Thompson

DeepEnd Research

Part of ECYFED

ECYFED
European Cyber Security Federation

GROUP IB

CSIS

Northwave

cyscon

SITEVET

Partner of the ACDC project

ACDC
the Advanced Cyber Defence Centre

Introduction 4

Editorial 4

Disclaimer 4

Frequently Asked Questions 5

Methodology 5

Definitions 5

Top 50 Hosts 6

Top 10s 7

Top 10 Visual Breakdown 7

Top 10 Newly Registered 7

Top 10 Countries 8

Hosts by Topic 9

Infected Web Sites 9

Botnet C&Cs 10

Spam 11

Phishing 12

Current Events 13

Zeus Botnets 14

Exploits 15

Badware 16

Appendix 1: Glossary 17

Appendix 2: Methodology 19

Editorial

Some press resources in the Netherlands picked up on a theme Of McAfee's study released in January 2013 showing the global distribution of active botnet control servers[1], calling the Netherlands a 'paradise for cyber criminals'.[2] While we wouldn't go that far, it is clear that there is a persistent problem for the Netherlands in that some hosting providers score consistently high in the HE Index.

HostExploit ranks the Netherlands at #7 in the world. This position is largely the result of two of the country's largest hosting providers appearing in the Top 20 – AS29073 Ecatel at #1 and AS16265 LeaseWeb at #11. It could be argued that both of these providers are victims of the Netherland's excellent internet infrastructure - both at corporate and consumer level - as well as being a major hub for internet traffic.[3]

This quarter sees the return of hosting provider Ecatel to the #1 rank, having held the position at various times in the past. Ecatel does not top the rankings for any particular category of activity, but rather for a consistently poor showing across the board.

While we do not intend to purposely single out an individual hosting provider for criticism our results serve to raise awareness of the issues. If a host consistently fails to perform across a variety of sectors, supported by multiple sources, then the results are hard to dispute.

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.

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://blogs.mcafee.com/mcafee-labs/botnet-control-servers-span-the-globe
[2] http://www.mkbservicedesk.nl/7249/nederland-paradijs-voor-cybercriminelen.htm
[3] http://www.rug.nl/news-and-events/people-perspectives/opinie/2013/05mathieupaapst?lang=en

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 43,454 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

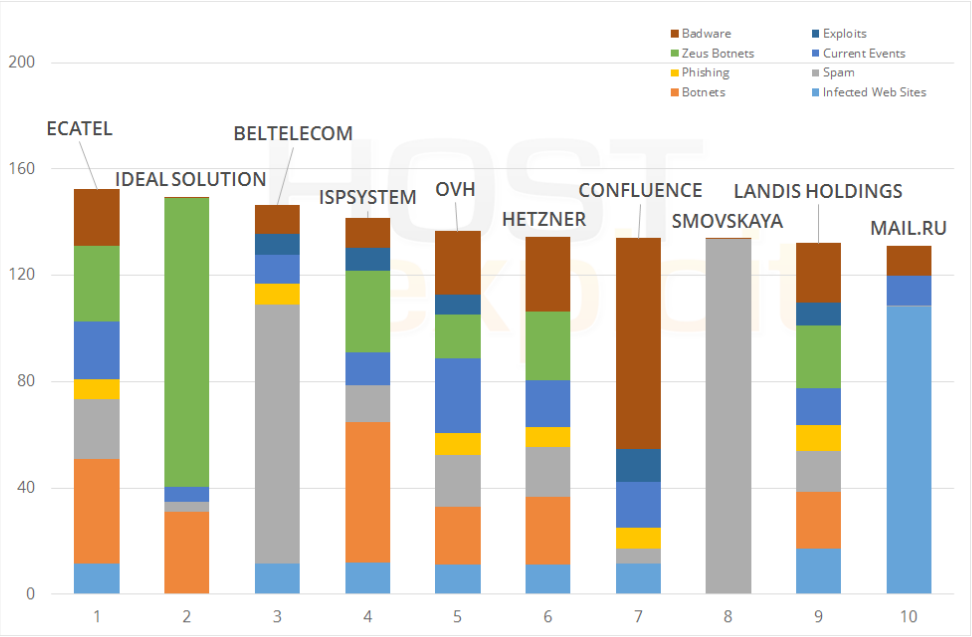
Rank of the Index compared to all 43,454 ASes.

IPs

Number of Internet Protocol addresses assigned to the AS.

HE Rank	HE Index	ASN	Name	Country	IPs
1	152.38	29073	Ecatel Network	NL	13,056
2	149.22	58001	Ideal Solution Ltd	RU	2,304
3	146.69	6697	Beltelecom	BY	1,420,800
4	141.69	29182	ISPsystem	RU	44,800
5	136.65	16276	OVH Systems	FR	1,003,008
6	134.49	24940	Hetzner Online AG	DE	638,208
7	133.96	40034	Confluence Networks Inc	VG	11,776
8	133.83	197774	Smovskaya Valentina Ivanovna	UA	512
9	132.18	11042	Landis Holdings Inc	US	28,416
10	131.11	47764	Mail.Ru LLC	RU	25,088
11	130.72	16265	LeaseWeb B.V.	NL	349,184
12	130.65	51699	Antarktida-Plus	SC	256
13	130.35	47781	"Delta-X" Ltd	UA	1,536
14	129.30	33182	HostDime.com, Inc.	US	55,040
15	128.05	4134	Chinanet Backbone	CN	116,912,864
16	126.03	32475	SingleHop	US	321,024
17	125.66	36351	SoftLayer Technologies Inc.	US	1,329,408
18	125.46	23535	HostRocket	US	13,312
19	124.07	50465	IQHost Ltd	RU	2,304
20	123.64	8560	1&1 Internet AG	DE	370,688
21	120.94	39743	Voxility S.R.L.	RO	29,696
22	119.63	12824	home.pl	PL	204,800
23	116.12	26347	New Dream Network, LLC	US	219,648
24	114.39	31034	Aruba S.p.A.	IT	140,800
25	111.89	38731	Vietel - CHT Compamy Ltd	VN	31,488
26	111.42	198354	SIS Laboratory, LLC	RU	3,328
27	109.94	26496	GoDaddy.com, LLC	US	1,610,496
28	109.47	22489	Castle Access Inc	US	48,384
29	108.73	8342	OJSC RTComm.RU	RU	463,872
30	108.21	9891	CS Loxinfo	TH	20,992
31	106.82	46475	Limestone Networks, Inc.	US	86,016
32	106.69	27823	Dattatec.com	AR	8,192
33	106.17	4837	China169 Backbone	CN	53,791,744
34	104.66	49467	Internet Hizmetleri (izmir)	TR	11,264
35	104.55	21844	ThePlanet.com Internet Services	US	1,509,376
36	100.93	9198	Kazakhtelecom	KZ	2,445,056
37	100.06	44112	SpaceWeb JSC	RU	3,584
38	99.41	51559	Netinternet	TR	17,664
39	98.72	46606	Unified Layer	US	235,520
40	97.61	23352	Server Central Network	US	259,584
41	95.49	13147	NetInfo Ltd.	BG	8,704
42	95.43	9931	The Communication Authoity of Thailand	TH	212,480
43	95.08	34109	CB3ROB Ltd.	DE	9,216
44	94.95	55660	PT Master Web Network	ID	4,096
45	94.29	49335	Navitel Rusconnect Ltd	RU	12,544
46	94.05	32613	iWeb Technologies Inc.	CA	251,904
47	93.80	20773	Host Europe GmbH	DE	220,672
48	93.40	21219	Datagroup	UA	132,864
49	92.22	20454	Secured Servers LLC	US	90,880
50	91.42	12322	PROXAD Free SAS	FR	12,271,616

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 2,195 ASes registered since the last report. These could potentially be of future interest.

HE Rank	HE Index	ASN	Name	Country	IPs
88	76.2	61421	Astra LLC.	RU	256
274	55.0	61322	Sotal-Interactive ZAO	RU	256
343	49.7	56598	KartLand Ltd.	RU	256
447	43.4	22611	InMotion Hosting, Inc.	US	16,128
522	40.9	20785	ISP UCT	UA	256
673	35.2	132322	Good Domain Registry	IN	1,024
740	33.4	33667	Comcast Cable Communications	US	0
1,210	23.7	17589	Gabia Inc.	KR	30,720
1,261	22.8	59684	Hoster kg, Ltd.	KG	1,024
1,351	21.7	61387	Denkers-ICT B.V.	NL	1,536

Number of ASes

At Q3 2013 report
42,386

As of this report
43,454

New ASes
2,195

Removed
1,127

Net gain
1,068

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

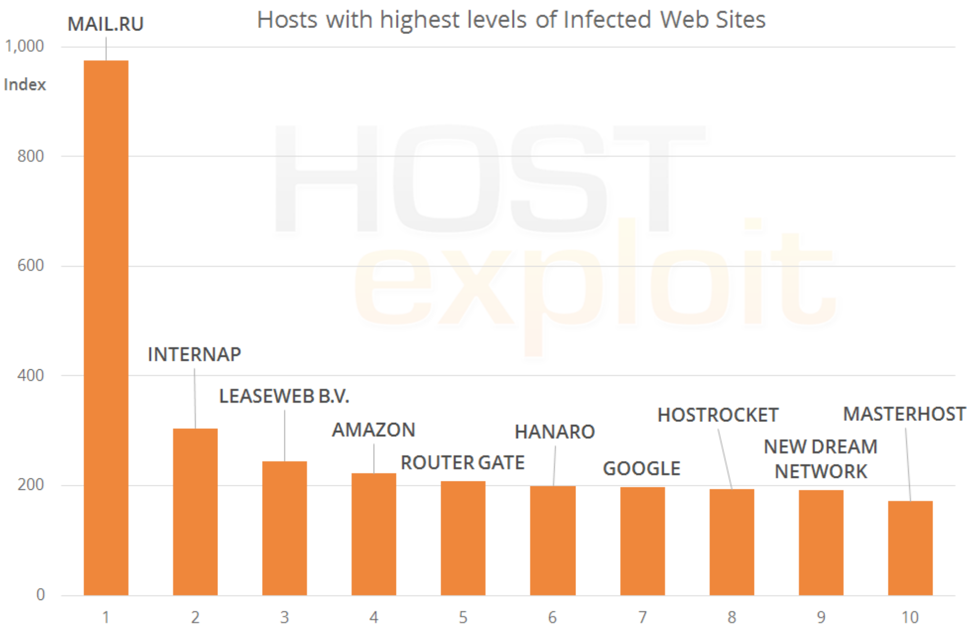
Country	Name	ASes	IPs	Rank	Index
RU	RUSSIAN FEDERATION	4,090	54,994,464	1	391.2
	Highest sector		Infected web sites	1	933.3
	2nd-highest sector		Badware	1	618.8
	3rd-highest sector		Botnet C&Cs	2	445.8
BY	BELARUS	79	2,167,808	2	265.0
	Highest sector		Spam	1	762.8
	2nd-highest sector		Infected web sites	3	475.4
	3rd-highest sector		Phishing	7	148.0
UA	UKRAINE	1,673	15,085,184	3	252.4
	Highest sector		Botnet C&Cs	3	433.2
	2nd-highest sector		Zeus botnets	6	386.5
	3rd-highest sector		Spam	2	359.9
VG	VIRGIN ISLANDS, BRITISH	4	17,152	4	220.8
	Highest sector		Exploits	1	902.7
	2nd-highest sector		Badware	2	417.6
	3rd-highest sector		Infected web sites	9	371.1
US	UNITED STATES	14,632	1,251,674,571	5	217.8
	Highest sector		Infected web sites	11	307.6
	2nd-highest sector		Badware	5	244.4
	3rd-highest sector		Zeus botnets	12	218.3
RO	ROMANIA	1,068	13,610,752	6	215.3
	Highest sector		Infected web sites	4	433.5
	2nd-highest sector		Zeus botnets	7	375.3
	3rd-highest sector		Botnet C&Cs	5	237.6
NL	NETHERLANDS	517	58,569,794	7	202.8
	Highest sector		Infected web sites	2	557.7
	2nd-highest sector		Badware	7	217.0
	3rd-highest sector		Botnet C&Cs	8	192.4
PL	POLAND	1,542	21,701,696	8	194.4
	Highest sector		Infected web sites	8	389.7
	2nd-highest sector		Exploits	4	354.0
	3rd-highest sector		Badware	6	235.9
TR	TURKEY	297	21,354,240	9	189.0
	Highest sector		Infected web sites	7	396.3
	2nd-highest sector		Badware	3	332.4
	3rd-highest sector		Phishing	6	169.6
BG	BULGARIA	449	5,647,872	10	186.0
	Highest sector		Zeus botnets	8	363.0
	2nd-highest sector		Badware	4	312.5
	3rd-highest sector		Botnet C&Cs	4	303.4

Infected Web Sites

Index	ASN	Name	Country	IPs	HE Rank	HE Index
975.7	47764	Mail.Ru LLC	RU	25,088	10	131.1
304.7	14744	Internap Network Services	US	124,928	185	63.3
244.9	16265	LeaseWeb B.V.	NL	349,184	11	130.7
222.2	16509	Amazon.com, Inc.	US	2,125,568	117	71.4
208.3	43260	Router Gate	TR	14,848	128	69.5
199.8	9318	Hanaro Telecom	KR	15,072,512	54	90.3
197.6	15169	Google Inc.	US	667,136	64	84.9
193.6	23535	HostRocket	US	13,312	18	125.5
191.8	26347	New Dream Network, LLC	US	219,648	23	116.1
171.4	25532	Masterhost	RU	77,824	123	69.8

The number of malicious URLs on Mail.ru's servers has risen rapidly over the last quarter, with the vast majority being stored on its file hosting service and download manager. This rise has seen it move into the overall top 10 hosts. Such a sudden increase in malicious files being hosted could either be the result of new features, a change in policy or down to cybercriminals choosing Mail.ru as a temporary hosting service.

HostRocket, on the other hand, has been steadily increasing through the ranks over the past two quarters. Ranking highly in both the Infected Web Sites and Badware categories demonstrates that the problem lies in its hosted content.



Did you know?

At #54 Hanaro Telecom is the highest-ranked Korean AS in the report.

The numbers

Over 59% of malicious URLs recorded in this period were hosted by the top 10 hosts for this category.

Did you know?

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

The numbers

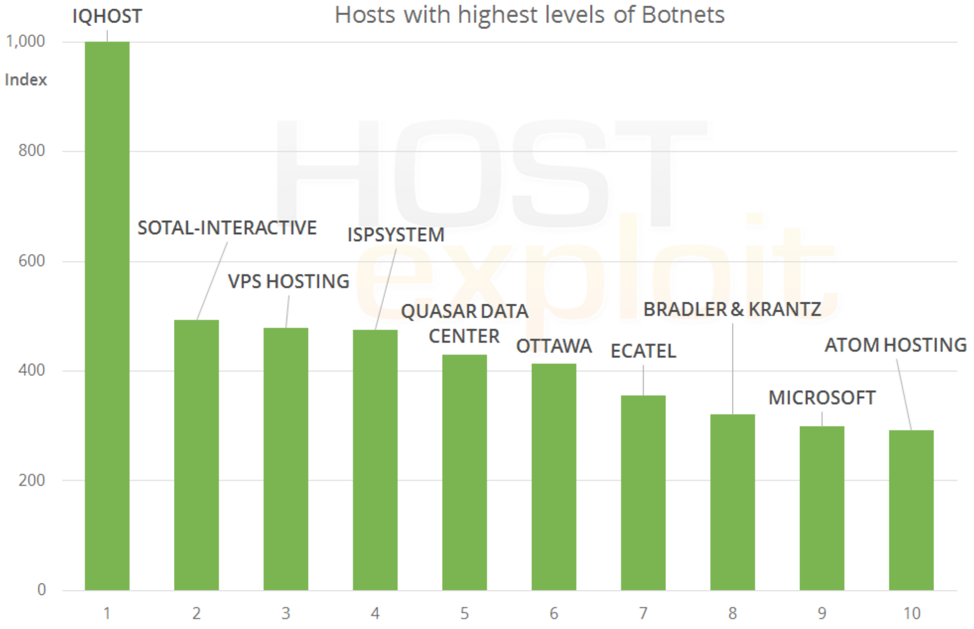
132 botnet C&Cs were observed in this period – lower than the total number of incidences in any other category. The power that each C&C holds, however, underlines their importance from a security perspective.

Botnet C&Cs

Index	ASN	Name	Country	IPs	HE Rank	HE Index
1,000.0	50465	IQHost Ltd	RU	2,304	19	124.1
492.5	61322	Sotal-Interactive ZAO	RU	256	274	55.0
479.6	56617	SIA "VPS Hosting"	LV	1,024	171	64.4
475.4	29182	ISPsystem	RU	44,800	4	141.7
430.1	46785	Quasar Data Center, Ltd.	US	4,608	241	58.2
413.3	26230	Telecom Ottawa Limited	CA	22,272	387	46.9
356.0	29073	Ecatel Network	NL	13,056	1	152.4
321.0	29141	Bradler & Krantz GmbH	DE	19,456	191	62.6
298.6	8069	Microsoft Corp	US	0	350	49.4
292.0	13209	Atom Hosting SRL	RO	768	233	58.9

Most notable in the top 10 for Botnet C&Cs is "Sotal-Interactive", newly registered since the last quarter. With 256 IPs (the minimum for an AS), and the registration being in Ukraine, despite being hosted out of Russia, it appears to fit the profile for an AS set up for a disposable botnet.

Also of interest is the inclusion of one of Microsoft's ASes, despite not having any announced IP blocks. This appears to be due to timing, with the C&C being first detected back in 2012, when a /16 block was allocated to this AS, but the announcement recently being withdrawn.

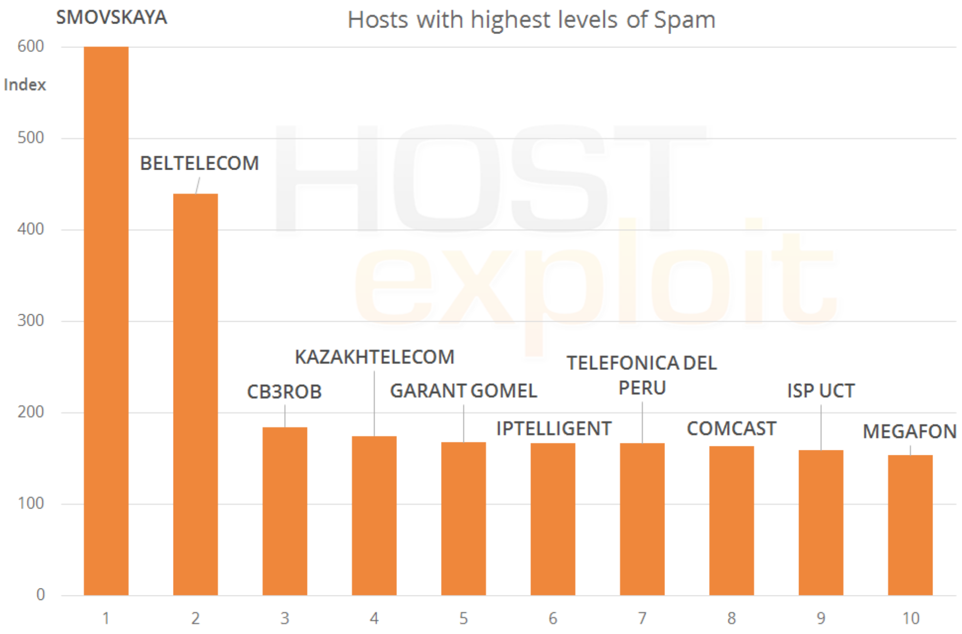


Spam

Index	ASN	Name	Country	IPs	HE Rank	HE Index
601.8	197774	Smovskaya Valentina Ivan...	UA	512	8	133.8
439.3	6697	Beltelecom	BY	1,420,800	3	146.7
184.1	34109	CB3ROB Ltd.	DE	9,216	43	95.1
174.6	9198	Kazakhtelecom	KZ	2,445,056	36	100.9
167.2	42036	Garant Gomel	BY	7,936	613	37.2
167.0	8100	IPTelligent LLC	US	47,104	169	64.8
166.5	6147	Telefonica del Peru	PE	1,976,576	244	57.9
163.7	20214	Comcast Cable	US	256	375	47.3
158.6	20785	ISP UCT	UA	256	522	40.9
153.3	31133	OJSC MegaFon	RU	29,184	110	73.2

In previous reports, the trend has been clear: spammers prefer to send their mail from countries where the level of regulation and barrier to AS registration is low. As such, we've seen hosts in India, Pakistan and Vietnam dominate the top 10 for some time. Last quarter, for example, half of the top 10 were registered in India.

This quarter, however, there are no such Indian hosts in the top 10. Instead, we see a mixture of small, purpose-built spam servers ("Smovskaya" and the newly-registered ISP UCT, both in Ukraine) along with larger telecoms companies that continue to struggle with spam - MegaFon, Beltelecom, Kazakhtelecom and and Telefonica del Peru.



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?

In our Q1 2012 report, MegaFon had a total of 4 ASes in the Spam top 10.

The numbers

More than 100,000 sources of spam were examined during the last quarter.

Did you know?

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

The numbers

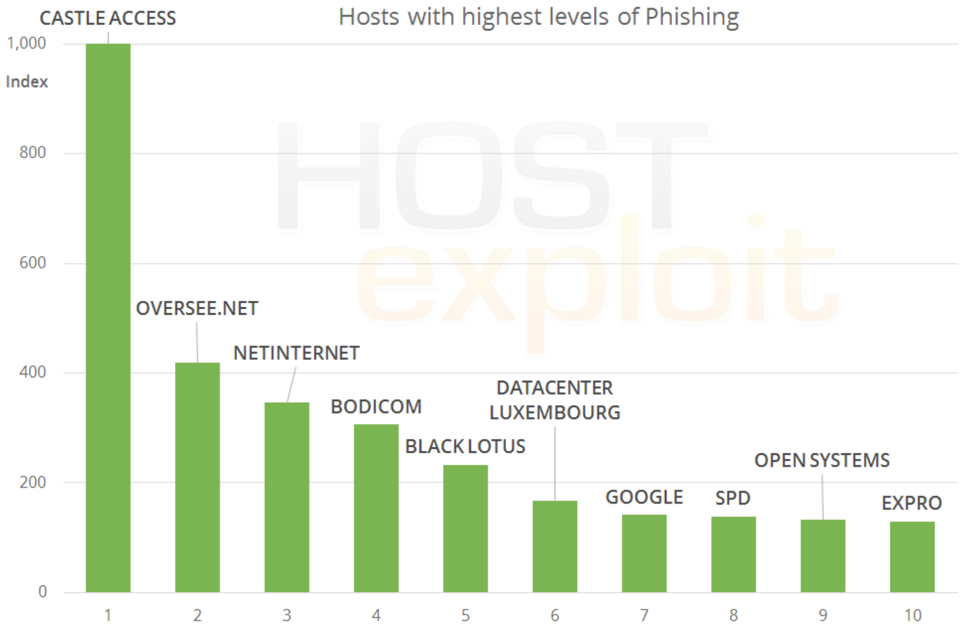
In the previous quarter, a total of 110 instances of phishing were recorded on these particular 10 hosts, compared to a total of 2,461 this quarter.

Phishing

Index	ASN	Name	Country	IPs	HE Rank	HE Index
1,000.0	22489	Castle Access Inc	US	48,384	28	109.5
419.4	33626	Oversee.net	US	3,584	113	72.6
346.2	51559	Netinternet	TR	17,664	38	99.4
305.9	45237	Bodicom ISP Ulaanbaatar	MN	5,120	561	39.1
232.7	32421	Black Lotus Communic...	US	11,264	787	31.6
166.2	24611	Datacenter Luxembourg	LU	8,704	3,168	12.6
141.5	15169	Google Inc.	US	667,136	64	84.9
139.0	40028	Spd Network	CA	17,664	1,196	24.0
132.7	28721	Open Systems S.R.L.	RO	2,560	3,034	13.4
129.8	31199	Expro Sp. z o.o.	PL	512	2,496	15.5

Phishing is a fast-moving sector of cybercrime – this is emphasized by the fact that the majority of phishing sites only remain online for a matter of minutes. For this reason, it's no surprise that only one of the new top 10 was so high up in the last report.

Further, the short-lived nature of these sites is an indication as to why major hosting nations such as the US and Canada are preferred – regulations may be tighter, but when a site is expected to be quickly shut down, the most important asset to the cybercriminal is the ease and availability of hosting.

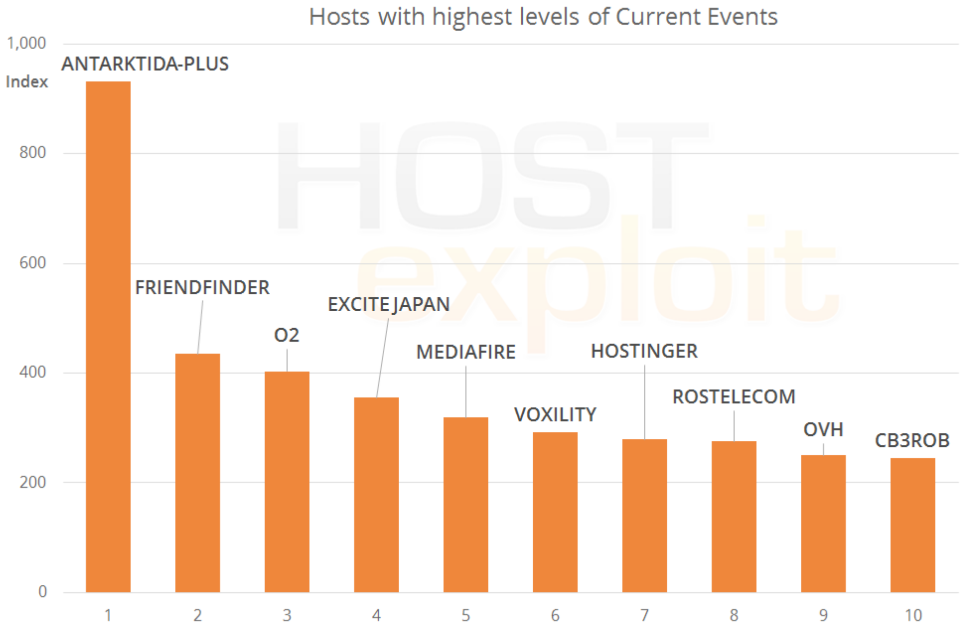


Current Events

Index	ASN	Name	Country	IPs	HE Rank	HE Index
931.6	51699	Antarktida-Plus	SC	256	12	130.7
434.7	32527	FriendFinder Networks	US	2,560	359	48.6
402.7	31080	o2 Sp. Z.o.o.	PL	512	329	50.8
355.0	45682	Excite Japan Co., Ltd.	JP	2,048	549	39.8
318.8	46179	MediaFire, LLC	US	3,072	511	41.1
291.4	39743	Voxility S.R.L.	RO	29,696	21	120.9
279.2	47583	Hostinger International	US	6,144	101	74.8
275.8	35177	Rostelecom	RU	32,768	270	55.2
250.1	16276	OVH Systems	FR	1,003,008	5	136.7
244.5	34109	CB3ROB Ltd.	DE	9,216	43	95.1

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. Only Voxility remains in the top 10 this time around. Major online presences FriendFinder and MediaFire are present, as well as the large French web hosting company, OVH.

Three ASes here were registered in a different country from their hosting location: Antarktida in Russia, Hostinger in Lithuania, and CB3ROB in the Netherlands.



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

The number of Current Events instances observed over the reporting period was less than 17% of the instances during the previous period.

Did you know?

Zeus, a form of botnet delivered via a trojan payload, remains one of the most popular varieties of botnet, some 5 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.

The numbers

The total number of Zeus servers observed has remained near-constant over the previous year. When a Zeus C&C is taken down, it is common for it to appear again from another location.

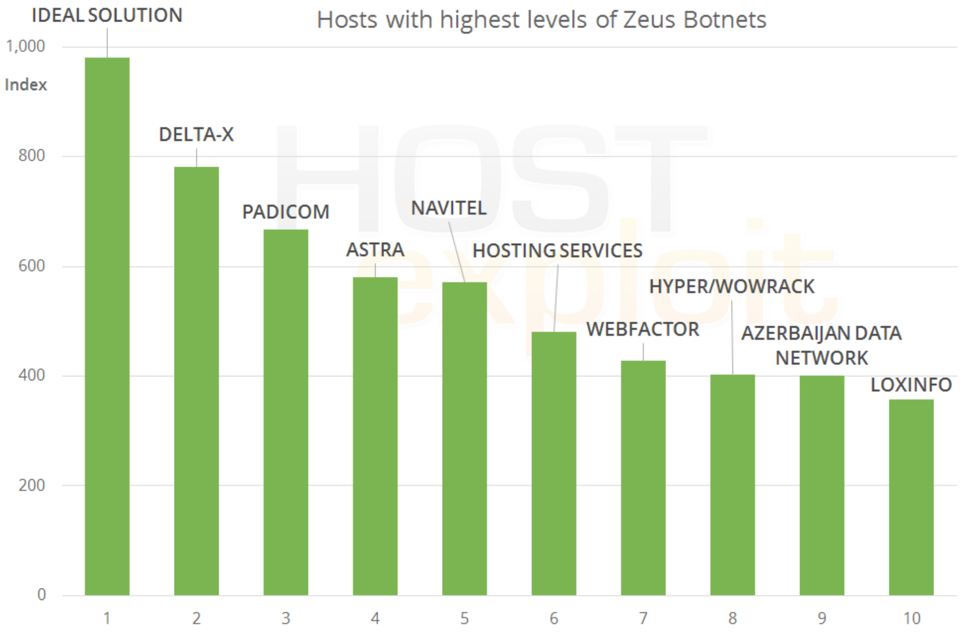
Zeus Botnets

Index	ASN	Name	Country	IPs	HE Rank	HE Index
980.1	58001	Ideal Solution Ltd	RU	2,304	2	149.2
781.5	47781	"Delta-X" Ltd	UA	1,536	13	130.4
667.0	34201	Padicom Solutions SRL	RO	6,400	104	74.4
580.6	61421	Astra LLC.	RU	256	88	76.2
571.3	49335	Navitel Rusconnect Ltd	RU	12,544	45	94.3
481.4	29302	Hosting Services Inc	GB	6,144	83	77.3
427.8	35818	Webfactor SRL	RO	11,008	52	90.8
401.9	23033	Hyper to Wowrack	US	35,328	89	76.2
399.9	15621	Azerbaijan Data Network	AZ	14,336	257	56.6
357.7	9891	CS Loxinfo	TH	20,992	30	108.2

Ideal Solution, registered in the Seychelles, has climbed from #9 to #1 in the Zeus Botnets ranking, with the number of recorded Zeus C&Cs increasing to 4.

Also of note is Astra LLC – the Russian AS is newly-registered and has climbed straight to #4. With just 256 IPs allocated and 2 Zeus C&Cs present, it appears to be a disposable AS.

8 of the 10 ASes are based in Eastern Europe - the same number as in the previous report.

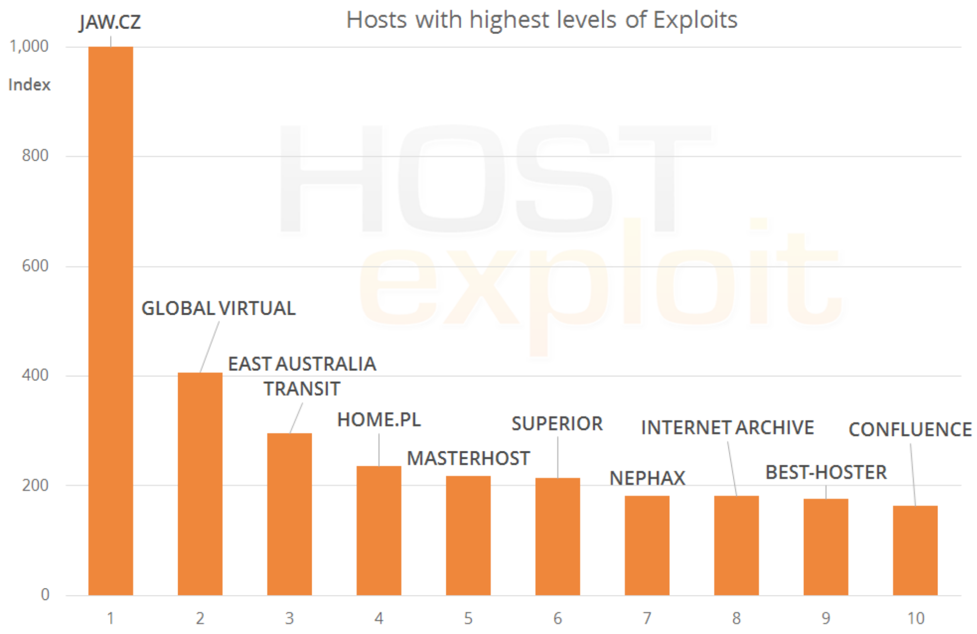


Exploits

Index	ASN	Name	Country	IPs	HE Rank	HE Index
1,000.0	43070	JAW.cz s.r.o.	CZ	3,584	73	81.5
406.9	46549	Global Virtual Opportunities	US	3,584	60	86.7
295.6	45261	East Australia Transit	AU	82,688	712	34.4
235.2	12824	home.pl	PL	204,800	22	119.6
217.6	25532	Masterhost	RU	77,824	123	69.8
213.8	34233	Superior B.V.	NL	4,096	330	50.6
181.5	43333	CIS NEPHAX	PL	17,920	326	50.9
181.0	7941	Internet Archive	US	6,144	449	43.4
175.6	49693	Best-Hoster Group Co. Ltd	RU	1,024	334	50.4
163.1	40034	Confluence Networks Inc	VG	11,776	7	134.0

Despite dropping in overall rank from #2 to #7, Confluence Networks has moved into the top 10 for exploits. The number of exploits observed on JAW.cz has increased rapidly, with the Index increasing from 109.3 to the maximum of 1,000.0. This movement alone has been sufficient for a rise from #4,758 overall to #73.

Home.pl has remained in the exploits top 10, and along with an increase in the levels of phishing and badware has move up the rankings to #22.



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 29% of all exploits observed during the reporting period.

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.

The numbers

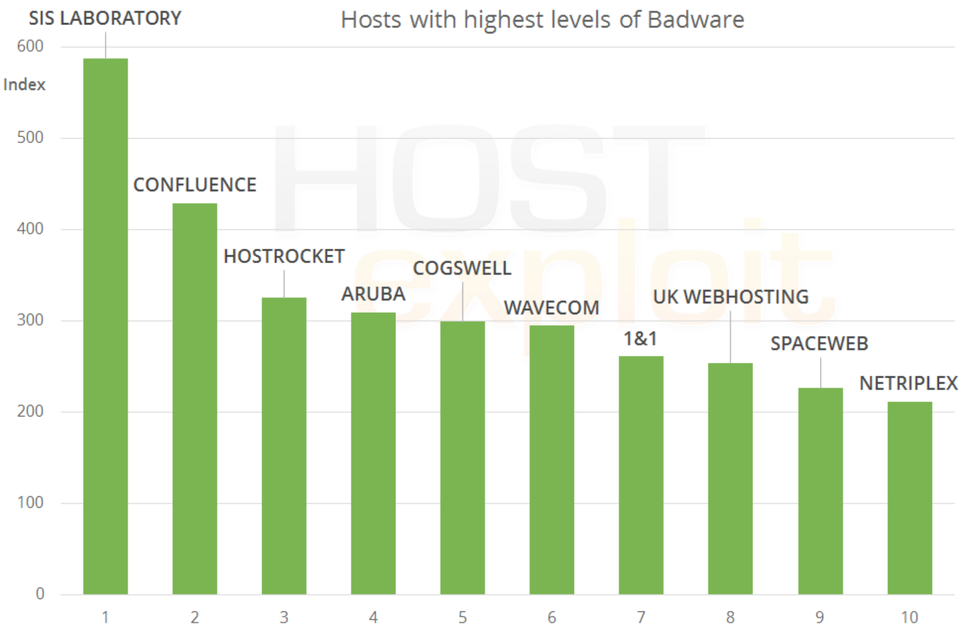
Total observed instances of badware fell by over 65% compared to the previous quarter. This can partly be explained by the holiday season finishing.

Badware

Index	ASN	Name	Country	IPs	HE Rank	HE Index
587.1	198354	SIS Laboratory, LLC	RU	3,328	26	111.4
429.0	40034	Confluence Networks Inc	VG	11,776	7	134.0
325.2	23535	HostRocket	US	13,312	18	125.5
308.6	31034	Aruba S.p.A.	IT	140,800	24	114.4
299.0	19066	Cogswell Enterprises Inc.	US	41,984	53	90.6
294.9	34702	WaveCom AS	EE	9,216	103	74.5
261.2	8560	1&1 Internet AG	DE	370,688	20	123.6
254.1	35732	UK Webhosting Ltd	GB	4,096	58	87.3
226.1	44112	SpaceWeb JSC	RU	3,584	37	100.1
211.9	36167	Netriplex LLC	US	1,536	464	43.1

All top 10 ASes for badware have changed since the previous quarter, which implies that the rate of change is rapid in this sector. Part of the reason for this is that badware can often be campaign-backed, and therefore is susceptible to short-term trends – for example, more activity during the holiday season, when spam is more effective.

Half of the hosts in the top 10 here are also in the top 100 for both phishing and infected web sites – this correlation is due to the similarity of hosting requirements for all 3 sectors.



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

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:

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

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)*