HOST exploit

CyberDefcon

HostExploit's

World Hosts Report

March 2014

Announcement

New Methodology Coming Soon

The HE Index, introduced in December 2009, has become a widely-used metric in the industry for tracking cybercrime and assigning reputations to Autonomous Systems.

HostExploit is pleased to announce that a new methodology is being developed for the next report that will enable greater accuracy of data, higher granularity and many more features.

Alongside the new methodology, the following services will be upgraded:

HostExploit

- New website with easier access to archived reports
- Blocklists and other host tools

SiteVet

- New website with members' features
- Higher granularity, from Country level all the way down to Domains and URLs
- Customisable blocklists and reports
- Email alerts and notifications

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

IntelCrawler™

CSIS

NORTHWAVE

cyscon

SITEVET

montimage

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

In what appears to be a continuing theme, the three worst positions on the HE Index are held by hosts or networks registered in the United States. The HE Index represents concentrations of malicious activity detected on web hosts and networks, in a report spanning three months.

It may not be a surprise to find that the three US-based hosts topping the rankings are the same as in the previous quarter - although this time 1st and 3rd places are reversed. AS11042 Landis Holdings moved to the top of the rankings while AS33182 HostDime.com shifted to third. AS26347 New Dream Network remained anchored in second place.

Closer investigation reveals that a lot more happened than these position changes might, at first, suggest. Looking at the individual categories that collectively form the quantification metrics of the HE Index, exposes the nature of the deterioration in AS11042 Landis Holdings' position. During the reporting period, Zeus botnet activity increased significantly on the servers of AS11042 Landis Holdings.

Similarly, there was increased malicious activity on the servers of AS26347 New Dream Network with more Infected Websites and Exploits but the surge was not sufficient to take the top position from AS11042 Landis Holdings.

Third placed AS33182 HostDime had the fewest changes of the top three which, although nothing to be proud of as very little has been done to clean up their networks, engendered the drop in the table, albeit on the back of increased malicious activity on the servers of two other US-registered hosts.

On a global scale, smaller countries with lower levels of regulations remain the location of choice for professional, cybercriminal servers, with the Virgin Islands, Belrus and Kyrgyzstan all making the Top 10.

Cyprus is not only a new entrant to Top 10 countries list, but has gone straight to top spot for its large concentrations of Current Events, Spam and Zeus botnet activities.

Lastly, despite the appearance of hosts from the United States and Russia in the Top 10, both countries have gone down in the overall country rankings.

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.

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

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

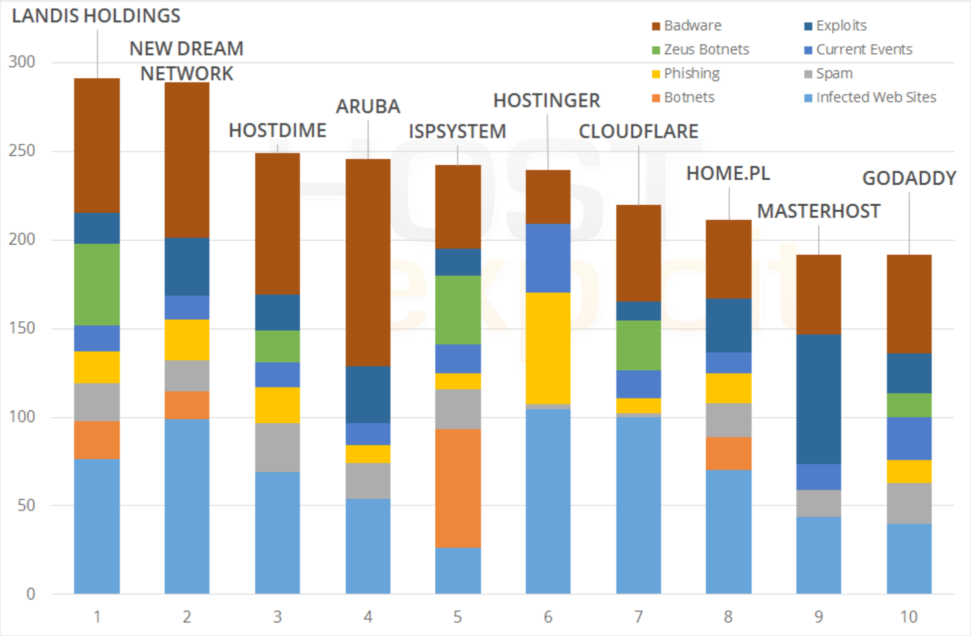
Rank of the Index compared to all 46,022 ASes.

IPs

Number of Internet Protocol addresses assigned to the AS.

HE Rank	HE Index	ASN	Name	Country	IPs
1	291.22	11042	Landis Holdings Inc	US	28,416
2	289.08	26347	New Dream Network, LLC	US	156,928
3	248.71	33182	HostDime.com, Inc.	US	78,848
4	245.64	31034	Aruba S.p.A.	IT	145,664
5	242.00	29182	ISPsystem	RU	44,544
6	239.48	47583	Hostinger International	US	13,568
7	219.72	13335	CloudFlare, Inc.	US	258,560
8	211.48	12824	home.pl	PL	204,800
9	191.78	25532	Masterhost	RU	77,824
10	191.71	26496	GoDaddy.com, LLC	US	1,768,192
11	187.04	8560	1&1 Internet AG	DE	372,224
12	182.24	16276	OVH Systems	FR	1,079,552
13	180.30	34619	Cizgi Telekomunikasyon	TR	30,208
14	179.01	25504	Vautron Rechenzentrum AG	DE	22,784
15	169.96	46606	Unified Layer	US	648,960
16	168.71	27823	Dattatec.com	AR	12,288
17	166.51	38955	World4You Internet Services	AT	6,400
18	163.94	16265	LeaseWeb B.V.	NL	397,824
19	162.89	29073	Ecatel Network	NL	12,800
20	161.04	40034	Confluence Networks Inc	VG	16,128
21	161.00	48159	Telecommunication Infrastructure	IR	385,728
22	160.02	24940	Hetzner Online AG	DE	705,280
23	159.48	43146	Agava Ltd.	RU	20,736
24	157.23	36351	SoftLayer Technologies Inc.	US	1,453,824
25	156.97	50465	IQHost Ltd	RU	2,048
26	151.78	51559	Netinternet	TR	19,200
27	149.34	54444	Avesta Networks LLC	US	5,888
28	147.53	42244	eServer.ru Ltd.	RU	36,352
29	145.19	35415	Webazilla B.V.	NL	77,056
30	143.64	42807	Aerotek Bilisim Taahhut Sanayi	TR	9,984
31	142.84	30633	Leaseweb USA	US	81,152
32	142.22	41079	SuperHost.pl	PL	4,608
33	140.56	41126	JSC Centrohost	RU	4,096
34	138.82	53225	IPGLOBE DATACENTER	BR	11,008
35	135.10	50810	Mobin Net Communication	IR	275,456
36	134.50	15626	ITL Company	UA	31,232
37	134.31	9891	CS Loxinfo	TH	25,344
38	133.07	15169	Google Inc.	US	690,432
39	132.00	31815	Media Temple, Inc.	US	113,152
40	131.10	47869	Netrouting Data Facilities	NL	26,112
41	131.00	44112	SpaceWeb JSC	RU	3,584
42	129.92	18479	Universo Online S.A.	BR	24,064
43	129.67	29076	CITYTELECOM-AS Filanco LTD	RU	45,824
44	129.44	15244	Lunar Pages	US	53,248
45	125.43	34023	PE Shattah Zia G.Naman	EU	256
46	124.88	4134	Chinanet Backbone	CN	118,838,272
47	122.74	29873	The Endurance International Group	US	100,352
48	122.68	4837	China169 Backbone	CN	55,455,232
49	122.14	132524	Tata Institute	IN	1,536
50	121.80	45839	PIRADIUS NET	MY	18,688

Top 10 Visual Breakdown



Top 10 Newly Registered

The following 10 ASes have the highest Indexes out of the 2,699 ASes registered since the last report. These could potentially be of future interest.

HE Rank	HE Index	ASN	Name	Country	IPs
183	82.064	133042	OBEC	TH	2,304
192	80.026	262279	Agencia na Web Sistemas	BR	8,192
261	70.592	8069	Microsoft Corporation	US	0
706	44.945	62605	Brain Host, LLC	US	4,096
960	37.009	262808	Brasilnet Telecomunicaes	BR	8,192
1,371	29.022	12876	ONLINE S.A.S.	FR	180,224
1,471	27.707	60897	IDEAL HOSTING	TR	3,072
1,671	25.307	262701	Brasil Telecomunicacoes	BR	5,120
1,694	25.029	62588	Active Solutions Group	US	1,280
2,004	21.994	22905	SoftCom America Inc.	US	20,992

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.

Number of ASes

At September 2013 report
44,556

As of this report
46,022

New ASes
2,699

Removed
1,233

Net gain
1,466

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

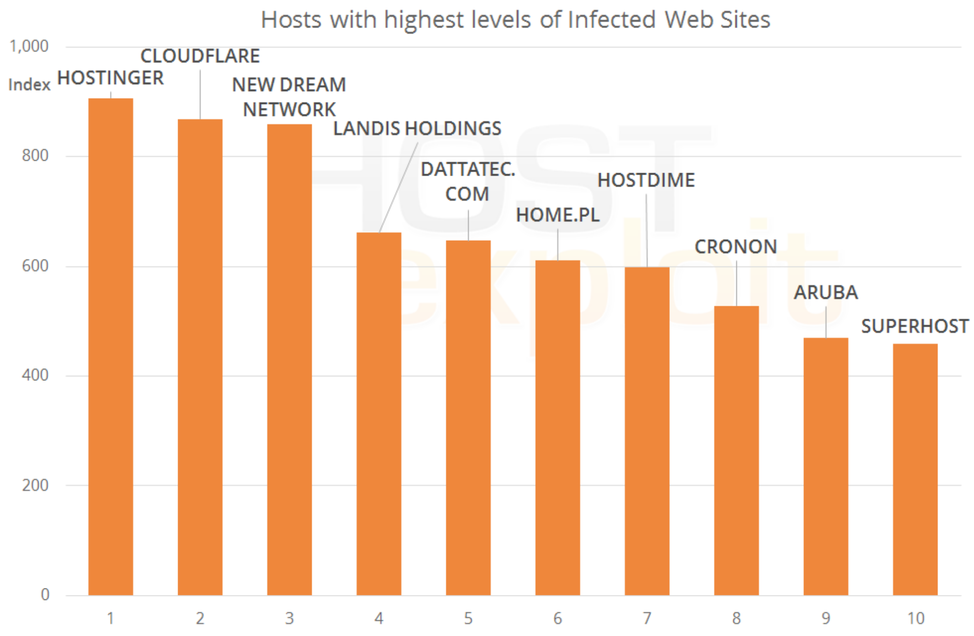
Country	Name	ASes	IPs	Rank	Index
CY	CYPRUS	55	1,944,832	216	18.0
	Highest sector		Zeus botnets	1	512.6
	2nd-highest sector		Current events	21	238.3
	3rd-highest sector		Spam	204	32.1
BY	BELARUS	78	2,130,944	6	287.9
	Highest sector		Spam	3	560.2
	2nd-highest sector		Zeus botnets	2	502.4
	3rd-highest sector		Botnet C&Cs	2	375.1
VG	VIRGIN ISLANDS, BRITISH	7	24,320	2	442.8
	Highest sector		Botnet C&Cs	1	901.1
	2nd-highest sector		Phishing	1	874.1
	3rd-highest sector		Current events	1	821.3
PL	POLAND	1,640	22,498,624	4	323.9
	Highest sector		Current events	2	770.9
	2nd-highest sector		Phishing	4	486.0
	3rd-highest sector		Zeus botnets	4	461.3
TR	TURKEY	309	22,590,976	9	243.1
	Highest sector		Current events	4	481.4
	2nd-highest sector		Zeus botnets	5	344.8
	3rd-highest sector		Botnet C&Cs	6	220.6
HU	HUNGARY	177	4,919,296	13	221.9
	Highest sector		Current events	3	482.2
	2nd-highest sector		Phishing	5	436.2
	3rd-highest sector		Zeus botnets	6	339.2
RU	RUSSIAN FEDERATION	4,247	54,832,928	8	256.5
	Highest sector		Phishing	7	395.9
	2nd-highest sector		Current events	7	392.6
	3rd-highest sector		Badware	4	368.7
CZ	CZECH REPUBLIC	455	9,555,520	11	228.2
	Highest sector		Phishing	2	513.3
	2nd-highest sector		Current events	6	470.9
	3rd-highest sector		Zeus botnets	8	295.6
IT	ITALY	606	49,187,840	19	177.0
	Highest sector		Zeus botnets	9	291.4
	2nd-highest sector		Current events	22	227.6
	3rd-highest sector		Spam	23	213.2
US	UNITED STATES	14,720	1,236,822,624	10	234.7
	Highest sector		Current events	11	323.6
	2nd-highest sector		Zeus botnets	10	280.6
	3rd-highest sector		Phishing	9	231.5

Infected Web Sites

Index	ASN	Name	Country	IPs	HE Rank	HE Index
906.7	47583	Hostinger International	US	13,568	6	239.5
869.0	13335	CloudFlare, Inc.	US	258,560	7	219.7
858.6	26347	New Dream Network, LLC	US	156,928	2	289.1
661.4	11042	Landis Holdings Inc	US	28,416	1	291.2
646.3	27823	Dattatec.com	AR	12,288	16	168.7
610.1	12824	home.pl	PL	204,800	8	211.5
598.2	33182	HostDime.com, Inc.	US	78,848	3	248.7
528.1	25504	Vautron Rechenzentrum AG	DE	22,784	14	179.0
468.8	31034	Aruba S.p.A.	IT	145,664	4	245.6
458.4	41079	SuperHost.pl	PL	4,608	32	142.2

7 of the top 10 ASes in the overall HE Index all feature in the top 10 for Infected Web Sites, as this category is a central component of a variety of cyber threats. In many cases this will be a byproduct of larger hacks and malicious activity, rather than a standalone infection.

Once again, half of the hosts featured are US-based, with ease of registration being key for a quick turnover of infected web sites.



Did you know?

This category features more ASes from the overall top 10 than any other

The numbers

AS27823 Dattatec.com is the highest-ranked South American AS in the overall HE Index, at #16

Botnet C&Cs

Index	ASN	Name	Country	IPs	HE Rank	HE Index
971.5	50465	IQHost Ltd	RU	2,048	25	157.0
828.4	56617	SIA "VPS Hosting"	LV	1,024	51	120.0
665.4	61322	Sotal-Interactive ZAO	RU	256	201	78.2
582.6	29182	ISPsystem	RU	44,544	5	242.0
441.4	57010	IT House Ltd.	RU	2,560	184	82.0
399.5	26230	Telecom Ottawa Limited	CA	21,248	530	52.8
398.5	43355	UPL Telecom s.r.o.	CZ	6,144	420	59.1
301.8	38731	Vietel - CHT Compamy Ltd	VN	20,736	94	101.8
290.8	8069	Microsoft Corp	US	0	261	70.6
288.5	47900	Art-master LLC	UA	256	1,062	34.7

The botnet category continues to be dominated by ASes in Eastern Europe.

The inclusion of a Microsoft AS at #9 is unexpected. As a newly-registered AS, it is likely to be due to configuration issues.

AS50465 IQHost continues to hold the top position, having done so since 2012.

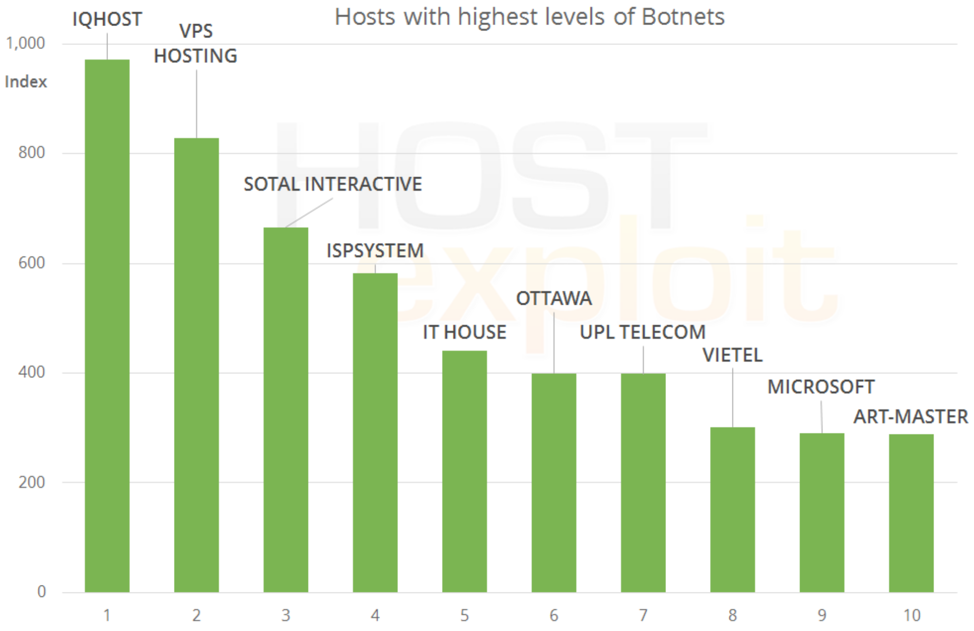
Did you know?

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

The numbers

114 botnet C&Cs were observed in this period, down from 124 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.

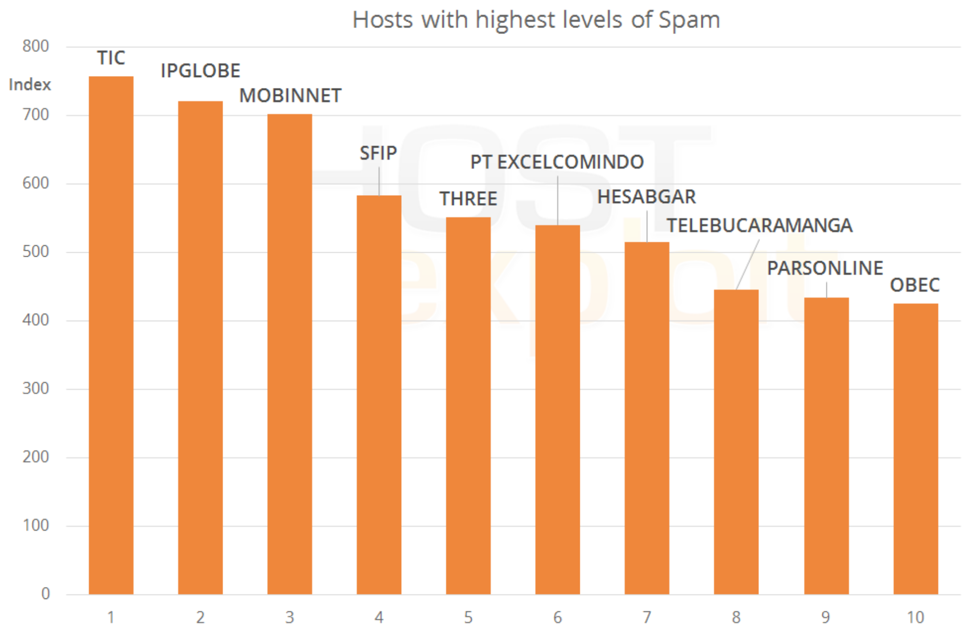


Spam

Index	ASN	Name	Country	IPs	HE Rank	HE Index
757.2	48159	Telecommunication Inf...	IR	385,728	21	161.0
720.3	53225	IPGLOBE DATACENTER	BR	11,008	34	138.8
702.4	50810	Mobin Net Communication	IR	275,456	35	135.1
582.4	57879	sfip84	DE	5,120	65	112.4
551.9	45727	Three Hutchison	US	16,384	84	106.4
539.7	24203	PT Excelcomindo Pratama	ID	8,960	89	104.1
514.4	48359	Hesabgar Pardaz Gharb Co.	IR	7,168	103	99.3
445.8	22368	TELEBUCARAMANGA S.A.	CO	89,344	157	85.8
433.3	16322	PARSONLINE	IR	507,648	112	95.0
424.6	133042	OBEC	TH	2,304	183	82.1

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, Brazil, Indonesia and Thailand represented here.



What do we do?

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

The numbers

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

Phishing

Index	ASN	Name	Country	IPs	HE Rank	HE Index
920.3	47846	Sedo GmbH	DE	1,280	166	83.9
815.8	47583	Hostinger International	US	13,568	6	239.5
318.1	15169	Google Inc.	US	690,432	38	133.1
299.7	26347	New Dream Network, LLC	US	156,928	2	289.1
265.0	33182	HostDime.com, Inc.	US	78,848	3	248.7
248.3	30060	VeriSign Infrastructure	US	5,376	312	66.9
240.5	40034	Confluence Networks Inc	VG	16,128	20	161.0
233.9	46816	DirectSpace Networks, LLC.	US	8,192	450	57.3
232.9	11042	Landis Holdings Inc	US	28,416	1	291.2
230.7	46606	Unified Layer	US	648,960	15	170.0

Did you know?

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

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

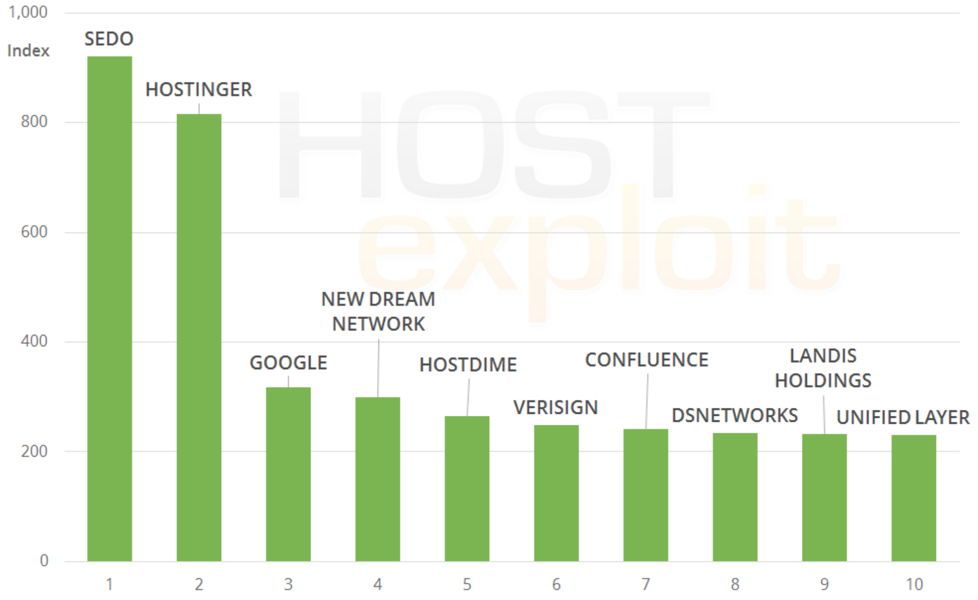
In this fast moving sector, phishers prefer the ease and availability of hosting in established regions. Since phishing sites are short-lived, guarantees of uptime are not needed and so it is not necessary to host from unregulated regions.

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.

The numbers

803 unique phishing campaigns were examined during this reporting period.

Hosts with highest levels of Phishing

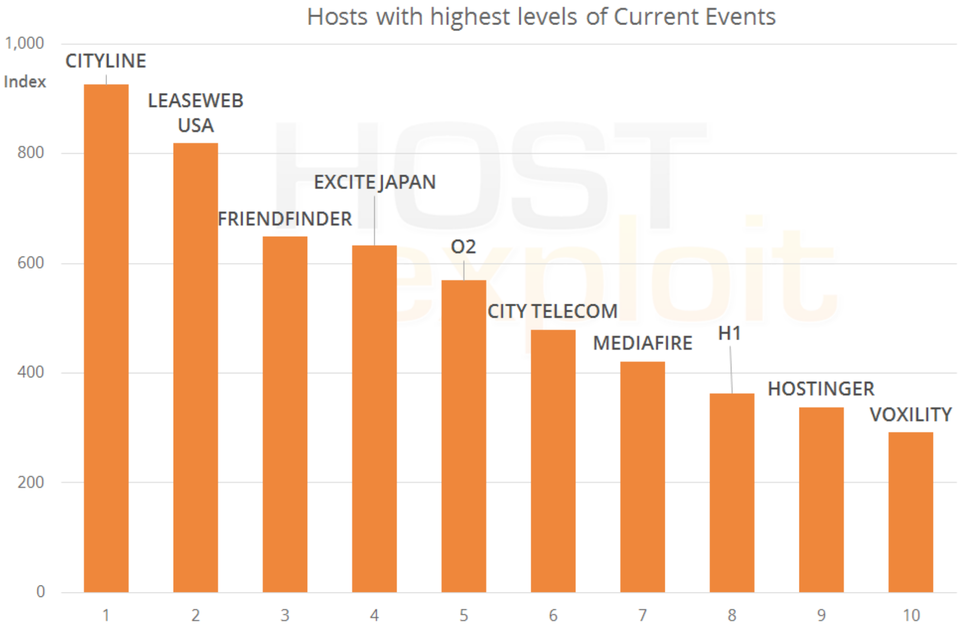


Current Events

Index	ASN	Name	Country	IPs	HE Rank	HE Index
925.8	34023	PE Shattah Zia G.Naman	EU	256	45	125.4
818.6	30633	Leaseweb USA	US	81,152	31	142.8
649.0	32527	FriendFinder Networks	US	2,560	216	76.2
633.3	45682	Excite Japan Co., Ltd.	JP	2,048	228	74.4
568.8	31080	o2 Sp. Z.o.o.	PL	512	168	83.8
479.5	48271	City Telecom	KG	8,192	145	88.2
421.0	46179	MediaFire, LLC	US	3,072	595	49.8
363.4	6870	H1 LLC	RU	7,168	753	43.0
338.1	47583	Hostinger International	US	13,568	6	239.5
291.4	39743	Voxility S.R.L.	RO	47,360	66	112.3

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.

This results in a wide variety of ASes being include, from telecoms (AS31080 o2) to file hosting (AS46179 MediaFire) to web services (AS32527 FriendFinder).



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

Nearly 150,000 current events instances were observed over the reporting period.

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.

The numbers

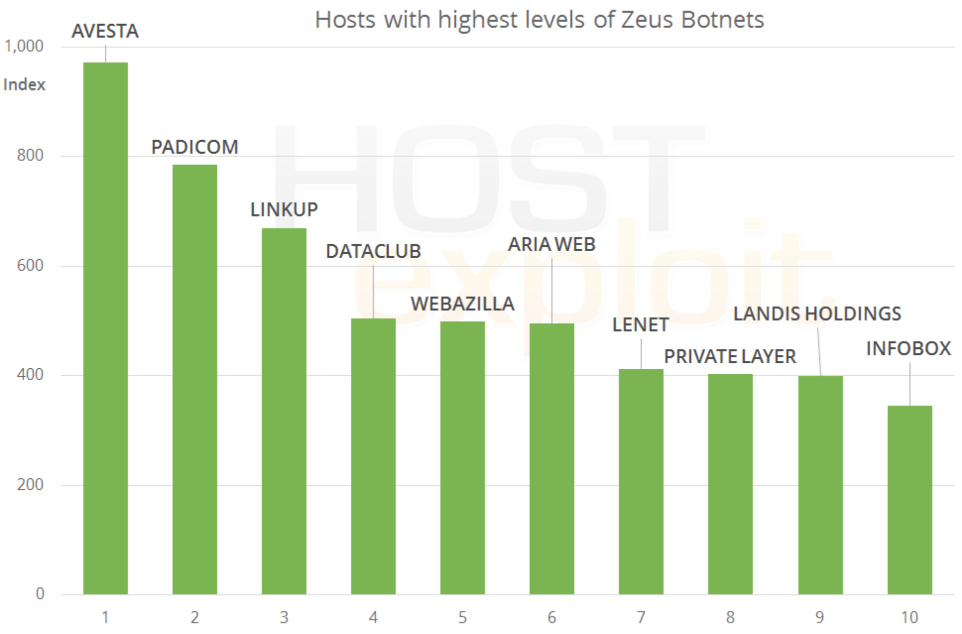
The total number of Zeus servers observed has continued to remain nearly constant. This suggests that Zeus continues to be a successful and profitable botnet toolkit of choice.

Zeus Botnets

Index	ASN	Name	Country	IPs	HE Rank	HE Index
971.5	54444	Avesta Networks LLC	US	5,888	27	149.3
784.8	34201	Padicom Solutions SRL	RO	6,400	127	91.7
669.8	58271	LinkUp Ltd.	UA	3,584	79	106.9
504.4	52048	DataClub S.A.	LV	2,048	246	71.7
498.7	35415	Webazilla B.V.	NL	77,056	29	145.2
495.9	57230	Aria Web Development LLC	GB	2,560	152	87.1
412.2	24607	LENET UAB	LT	9,216	576	50.6
402.3	51852	Private Layer INC	CH	27,904	67	112.3
399.6	11042	Landis Holdings Inc	US	28,416	1	291.2
345.9	30968	Infobox.ru	RU	41,216	121	92.6

The rankings for Zeus Botnets mirrors those of Botnet C&Cs, with many Eastern European ASes represented, and a couple of surprise inclusions (AS57230 Aria Web Development)

The top ranked AS from the previous report, AS57668 Santrex, has dropped out of the top 10 entirely.

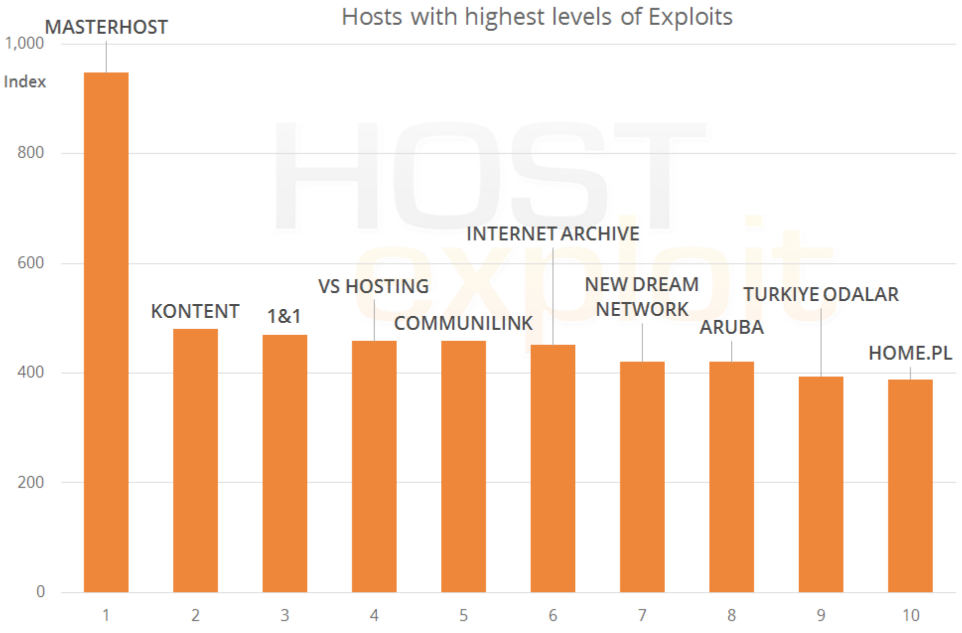


Exploits

Index	ASN	Name	Country	IPs	HE Rank	HE Index
947.3	25532	Masterhost	RU	77,824	9	191.8
480.6	24973	KONTENT GmbH	DE	4,096	154	86.4
470.2	8560	1&1 Internet AG	DE	372,224	11	187.0
458.2	43541	VSHosting s.r.o.	CZ	14,336	100	99.9
458.1	38277	CommuniLink Internet Lim...	HK	5,632	129	90.7
451.2	7941	Internet Archive	US	6,144	69	111.2
420.1	26347	New Dream Network, LLC	US	156,928	2	289.1
419.8	31034	Aruba S.p.A.	IT	145,664	4	245.6
394.0	34755	Turkiye Odalar Borsalar	TR	768	1,210	31.7
389.0	12824	home.pl	PL	204,800	8	211.5

This category continues to include repeat offenders, with AS25532 Masterhost, AS8560 1&1, and AS43541 VSHosting all having been present in the previous report.

In fact, all of the Top 5 here were all present in this same category in the previous quarter. AS25532 Masterhost is proving to be a consistent choice of registrar for Exploits.



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

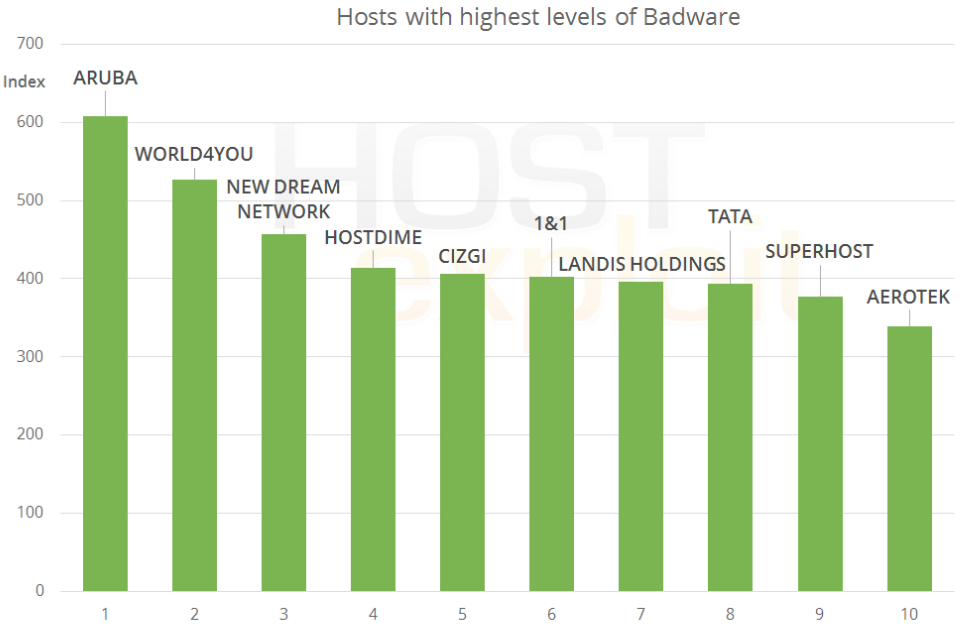
The top 10 ASes in this category account for over 21% of all exploits observed during the reporting period, up from 16% last report.

Badware

Index	ASN	Name	Country	IPs	HE Rank	HE Index
607.5	31034	Aruba S.p.A.	IT	145,664	4	245.6
526.6	38955	World4You Internet Services	AT	6,400	17	166.5
457.6	26347	New Dream Network, LLC	US	156,928	2	289.1
413.5	33182	HostDime.com, Inc.	US	78,848	3	248.7
406.1	34619	Cizgi Telekomunikasyon	TR	30,208	13	180.3
402.4	8560	1&1 Internet AG	DE	372,224	11	187.0
395.6	11042	Landis Holdings Inc	US	28,416	1	291.2
394.0	132524	Tata Institute	IN	1,536	49	122.1
376.7	41079	SuperHost.pl	PL	4,608	32	142.2
339.1	42807	Aerotek Bilisim Taahhut	TR	9,984	30	143.6

Six ASes in this category have remained in the top 10 from the previous report,. This makes it one of the most surprisingly stable sets of listed hosts under this category, since the badware sector is very fast changing. Badware is responsive to short-term trends and the hosts in this category will, by necessity, change accordingly.

Our top four '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.



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

The top 10 hosts in this category account for 12% of the total instances of badware observed, down signifcantly from 23% last report.

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:

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

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

C: *IP weighting = 20,000*

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

5 Calculation

For each data source, three factors are calculated.

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

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

where:
B$_m$: *maximum Bayesian ratio*

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

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

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

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

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

where:
N$_m$: *maximum number of instances in sample set*

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

The index for each data source is then calculated as:

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

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

The overall HE Index is then calculated as:

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

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