ISBN: 978-0-9836249-1-2

HostExploit's Worldwide Cybercrime Series

Global Security Report

May 2012

Inaugural

Table of Contents

HOST exploit

HostExploit's

CyberCrime Series

Global Security Report

GROUP IB

CyberDefcon

CSIS

Supported by

nominettrust

www.nominettrust.org.uk

DEEPEND RESEARCH

Edited by

- Jart Armin

Review

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

Comparative Data

- AA419
- Abuse.CH
- CIDR
- Clean-MX.DE
- Emerging Threats
- Google Safe Browsing
- Group-IB
- HostExploit
- hpHosts
- ISC
- KnujOn
- MaliciousNetworks (FiRE)
- MalwareDomains
- MalwareDomainList
- RashBL
- Robtex
- Shadowserver
- SiteVet
- Spamhaus
- StopBadware
- SudoSecure
- Sunbelt
- Team Cymru
- UCE Protect

Contributors

- Steve Burn
- Niels Groeneveld
- Bogdan Vovchenko
- Will Rogofsky
- Philip Stranger
- Bryn Thompson
- Yori Kamphuis
- Michel Eppink
- Qubis
- DeepEnd Research

Executive Summary

All cybercrime is hosted and served from somewhere.

A simple enough truism and yet little research, or even initiatives, emerge from this area. This report, and the companion website, Global Security Map, aim to provide deeper insights into this domain, as the beating heart of all hosted, or accessible, Internet services, and its potential to yield solutions to a global problem.

Key to understanding a problem is the ability to measure it.

As an industry, Internet security has few standards, with widely varying data formats and too little quantification resulting in a lack of objectivity supporting preventative actions.

HostExploit's new website and tool, the Global Security Map, aims to provide some of the missing links in the field of quantification. As an interactive tool that displays real-time data, the Global Security Map provides the means to gauge and compare levels of malicious activity (badness) served through all the world's hosts, registrars and ISPs, as routed through ASes (autonomous systems). Data is displayed as it relates to individual countries and is compiled into a ranking system of countries according to the rising, or falling, levels of malicious activities served via hosts, registrars, IPSs, etc,.

The HE Index provides an objective, easy-to-understand scoring system.

Issues including malware, trojans, worms, botnets, command & control centers, phishing, spam, rogues, APT are detected and weighted with a number of factors relating to the size, nature and location of the servers. The result is a simple score from 0 to 1000. This methodology, tried and tested thoughout several years of the "Top 50 Bad Hosts and Networks" reports (an invaluable aid to the takedowns of crime servers such as McColo, EstDomains and Atrivo), uses real-time data on the malicious activity served from all 40,000+ ASNs (hosts, registrars and ISPs).

This is the start of a long-term research cycle.

The Global Security Map tool is in a rapid stage of development. While it's results currently apply to high-level views of countries, work is well under way on a fully organic system which is able to drill down seamlessly from world level, to region, to country, to internet exchanges, to ASes and ISPs, and finally to IPs, domains and URLs. This development phase will extend the tool's functionality from one of visualization to one of a research and analysis tool, suitable for hosts, ISPs, governmental bodies, law enforcement and academia to view malicious activity from the top down.

At the time of the report, LITHUANIA ranks at #1 with the highest levels of malicious activities in the world while FINLAND at #219 has the cleanest servers and networks.

With this information in place, the next step is to consider realistic mitigation methods or plans that can help reduce levels of malicious activity. For example, several countries have already set in motion plans for an ISP 'voluntary code of conduct', in the style of the US Federal Communications Commission's recent report 'U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)', and backed by a large consortium of leading U.S. organisations. Voluntary action on the part of ISPs is the preferred course of action but many smaller service providers may not sign up when they can make good money without having to agree to 'binding' codes.

Introduction

2.1. Background

Welcome to HostExploit's inaugural Global Security Report produced in association with Group-IB in Russia and CSIS in Denmark.

If you've followed our Top 50 Bad Hosts & Networks reports, you may be aware of how this new report came about, and aims and reasoning behind it. If not, allow us to fill you in.

Since 2008, we have been publishing quarterly reports on the "Top 50 Bad Hosts & Networks", highlighting hosts with high levels of malicious activity, that we generally label "badness". Not all of those hosts are intentionally "bad" of course - more often that not, it's a case of slack security measures in a fast-growing business, or the host themselves being victim to targeted attacks.

But along the way, some certainly could be labeled as "bad"! Crime servers such as McColo, EstDomains and Atrivo have fallen along the way, in no small part due to the reporting from the community, including ourselves.

As all cybercrime is hosted by someone from somewhere, it made sense to us that measuring such activity as objectively as possible would make for the most efficient means of identifying these instances. By showing the levels of badness served from all of the 40,000+ publicly-routed ASes (Autonomous System), we could give a snapshot of underperforming service providers in terms of cybercriminal activity which could furnish other areas of information such as the locations of cybercriminal hubs and hotspots.

We devised an algorithm called the *HE Index* - a simple scoring system from 0 to 1,000, where 1,000 represents the maximum possible level of badness. This continues to power the reports and the website SiteVet, where daily AS reports can be viewed.

Global Security Map

The next stage of our development of the quantification of internet badness has been with Global Security Map, designed as an interactive tool to enable the visualization and quantification of the geographic distribution of cybercrime.

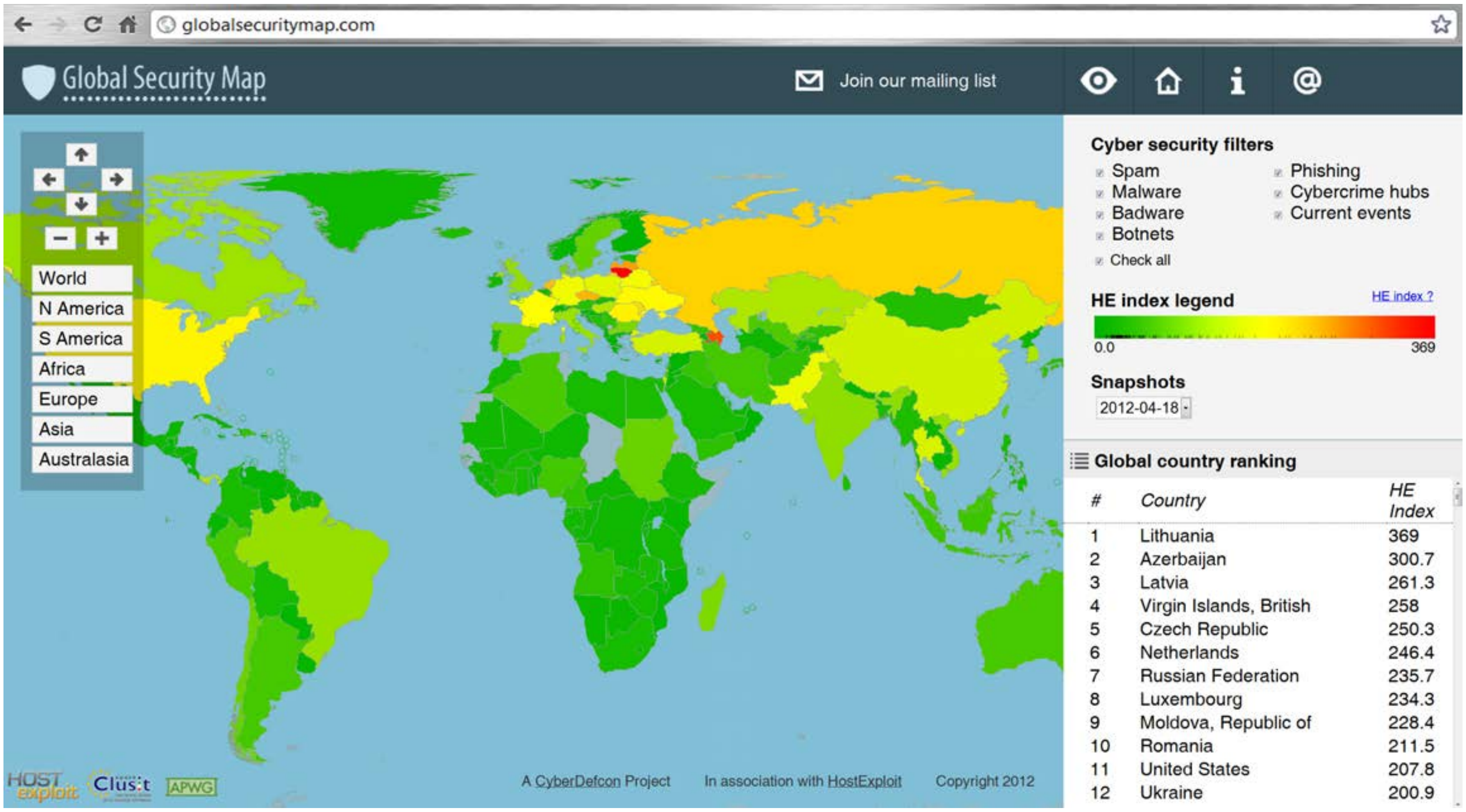
The first stage has been to apply the HE Index concept to countries as a whole. The initial results of this methodology can now be viewed live on globalsecuritymap.com or throughout this report.

Note that the full listings of all 219 countries are not included within this report, but can be viewed on the website.

2.2. What is the Global Security Map?

The Global Security Map is a website that will serve effectively as a frontend for much of the data from our reports.

The following screenshot shows the world view:



Cyber security filters

- ☑ Spam
- ☑ Malware
- ☑ Badware
- ☑ Botnets
- ☑ Phishing
- ☑ Cybercrime hubs
- ☑ Current events
- ☑ Check all

HE index legend

Snapshots

2012-04-18

Global country ranking

#	Country	HE Index
1	Lithuania	369
2	Azerbaijan	300.7
3	Latvia	261.3
4	Virgin Islands, British	258
5	Czech Republic	250.3
6	Netherlands	246.4
7	Russian Federation	235.7
8	Luxembourg	234.3
9	Moldova, Republic of	228.4
10	Romania	211.5
11	United States	207.8
12	Ukraine	200.9

What can it do?

Currently, visitors to globalsecuritymap.com can:

- View the world rankings, updated daily
- View the levels of malicious activity by category within every country in the world
- View numbers of malicious instances by category within every country

Over the coming months, a whole range of features will be rolled out, enabling users to:

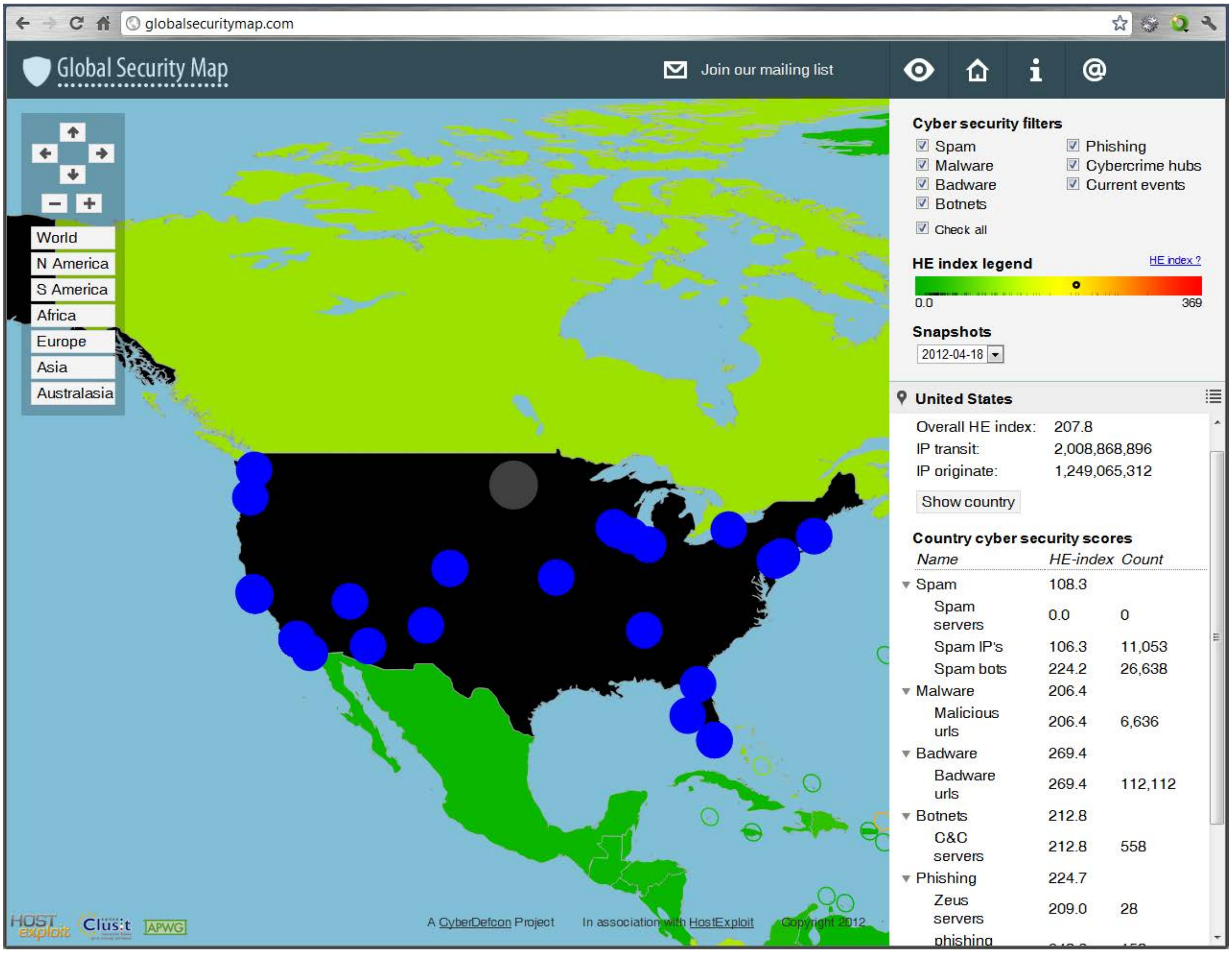
- View global historical records, dating back several years
- Visualize changes in malicious activity over time with customizable animations
- View over 20 ***trillion*** records of malicious instances on individual Autonomous Systems over several years
- Explore and analyze the relationship between countries, registries, internet exchanges, ASes and each of the 20 trillion records of malicious activity
- Automated and customizable reporting and analysis

How’s it going to help?

We believe that Global Security Map is a unique tool. By drilling down from country and world level, right down to specific instances of hacks, spam and malware, it enables an overall gauge on the size and nature of problems caused by cybercrime in all regions.

This combination of detail of and high-level visualization will make the tool of great use to:

- Law enforcement
- The public sector
- Registries and registrars
- Hosts and ISPs
- Financial instutions
- Other corporations targeted financially by cybercrime



Cyber security filters

☑ Spam ☑ Phishing
☑ Malware ☑ Cybercrime hubs
☑ Badware ☑ Current events
☑ Botnets

☑ Check all

HE index legend

0.0 369

Snapshots

2012-04-18

United States

Overall HE index: 207.8
IP transit: 2,008,868,896
IP originate: 1,249,065,312

Country cyber security scores

Name	HE-index	Count
▾ Spam	108.3	
Spam servers	0.0	0
Spam IP's	106.3	11,053
Spam bots	224.2	26,638
▾ Malware	206.4	
Malicious urls	206.4	6,636
▾ Badware	269.4	
Badware urls	269.4	112,112
▾ Botnets	212.8	
C&C servers	212.8	558
▾ Phishing	224.7	
Zeus servers	209.0	28
phishing		

Report Methodology

When calculating levels of badness at country level, the accuracy of identifying the countries serving specific activity is of course critical.

One of the reasons that there has been a lack of research into the geographic distribution of cybercrime is that it is difficult to accurately determine where *anything* is physically hosted on the internet, let alone where *everything* is.

This should **not** be a deterrent to research. Rather, it should encourage more research, as inconsistencies found in data, when publicly released, will put pressure on the relevant internet authorities to enable better methods of quantification. If no one attempts to quantify to begin with, nothing will change.

So how do we define what is hosted in which countries? We primarily use the country of registration for ASes, and sum up the concentration levels of badness for each AS within a country. The country of registration for an AS it not *necessarily* where the AS is physically hosted, and indeed for larger ASes, the infrastructure is often spread across multiple continents.

This does not make it incorrect to use the country of registration, but makes it important to understand the context of the results and what they *mean*. For countries that show high levels of malicious activity in the results, we can conclude that the regional registry responsible for that country is accepting more registrations which end in malicious activity. And usually for extreme cases, of crime servers, the AS will be very small and will not span multiple countries.

In addition, we have run a second methodology which uses our calculated estimation of the *actual* physical location of the infrastructure, based on routing locations. In the few cases where we are not able to draw a strong conclusion on the location, we fall back to the country of registration. The parallels between the two sets of results are very interesting and can be seen in Section 5.

Our methodology continues to evolve - continue to check out globalsecuritymap.com to see the changes being rolled out over the coming weeks and months!

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 is 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.

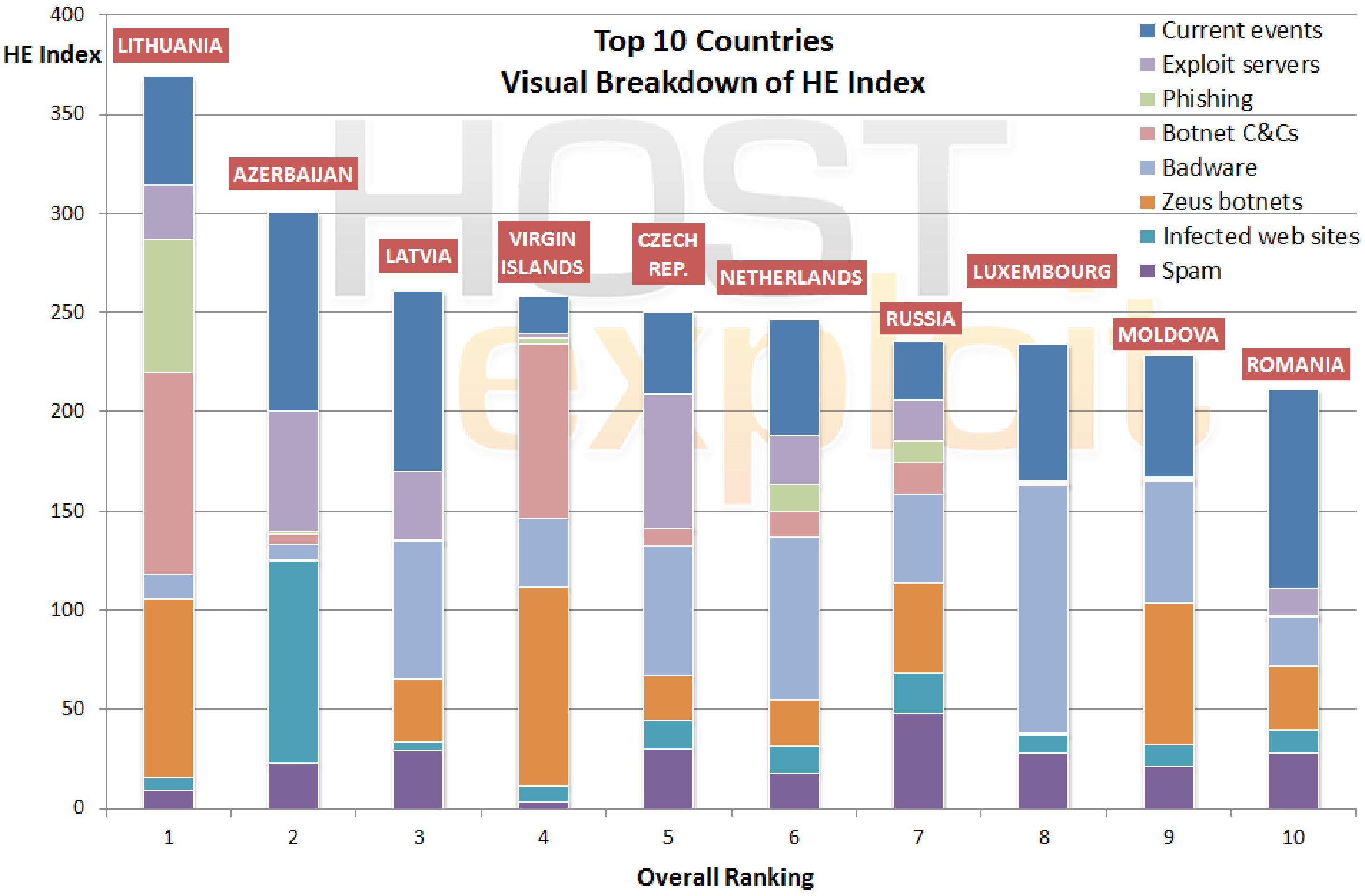
The 'Global Security Map', its related resources and data are not intended as a declaration that any government or country is actively involved in, or a supporter of, cybercriminal activities.

3. The Top 50

HE Rank	HE Index	Country	Country name	ASNs
1	369.02	LT	LITHUANIA	92
2	300.71	AZ	AZERBAIJAN	29
3	261.25	LV	LATVIA	192
4	257.99	VG	VIRGIN ISLANDS, BRITISH	3
5	250.35	CZ	CZECH REPUBLIC	903
6	246.43	NL	NETHERLANDS	439
7	235.66	RU	RUSSIAN FEDERATION	3,276
8	234.32	LU	LUXEMBOURG	43
9	228.39	MD	MOLDOVA, REPUBLIC OF	33
10	211.46	RO	ROMANIA	331
11	207.81	US	UNITED STATES	14,033
12	200.92	UA	UKRAINE	1,436
13	174.43	FR	FRANCE	581
14	160.90	BY	BELARUS	70
15	157.16	DE	GERMANY	1,124
16	152.55	PK	PAKISTAN	59
17	143.72	PL	POLAND	1,411
18	136.97	TH	THAILAND	228
19	135.07	TR	TURKEY	277
20	132.16	CN	CHINA	215
21	124.35	EU	EUROPE	1,323
22	122.54	IL	ISRAEL	201
23	116.39	HU	HUNGARY	168
24	115.14	PA	PANAMA	66
25	113.98	KZ	KAZAKHSTAN	61
26	113.49	KR	KOREA, REPUBLIC OF	693
27	105.97	CA	CANADA	871
28	104.89	IT	ITALY	541
29	103.49	VN	VIET NAM	102
30	103.01	BR	BRAZIL	1,206
31	101.57	GB	UNITED KINGDOM	1,374
32	99.59	IN	INDIA	442
33	98.57	BS	BAHAMAS	3
34	91.06	MG	MADAGASCAR	5
35	90.97	MK	MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	26
36	89.57	BG	BULGARIA	423
37	87.82	DK	DENMARK	172
38	86.57	ES	SPAIN	341
39	82.48	SD	SUDAN	6
40	81.87	CL	CHILE	109
41	80.45	HK	HONG KONG	276
42	79.26	SE	SWEDEN	380
43	70.87	TW	TAIWAN, PROVINCE OF CHINA	116
44	68.69	UZ	UZBEKISTAN	29
45	66.58	DZ	ALGERIA	10
46	66.40	PE	PERU	17
47	65.72	AU	AUSTRALIA	871
48	64.96	MY	MALAYSIA	95
49	63.98	AR	ARGENTINA	222
50	63.93	IR	IRAN, ISLAMIC REPUBLIC OF	193

4.

Top 10 Breakdown



The above chart shows the constituent components of the HE Index for each country in the Top 10. It can be seen that the Virgin Islands and Lithuania dominate both in terms of botnet C&Cs and also Zeus botnet servers specifically.

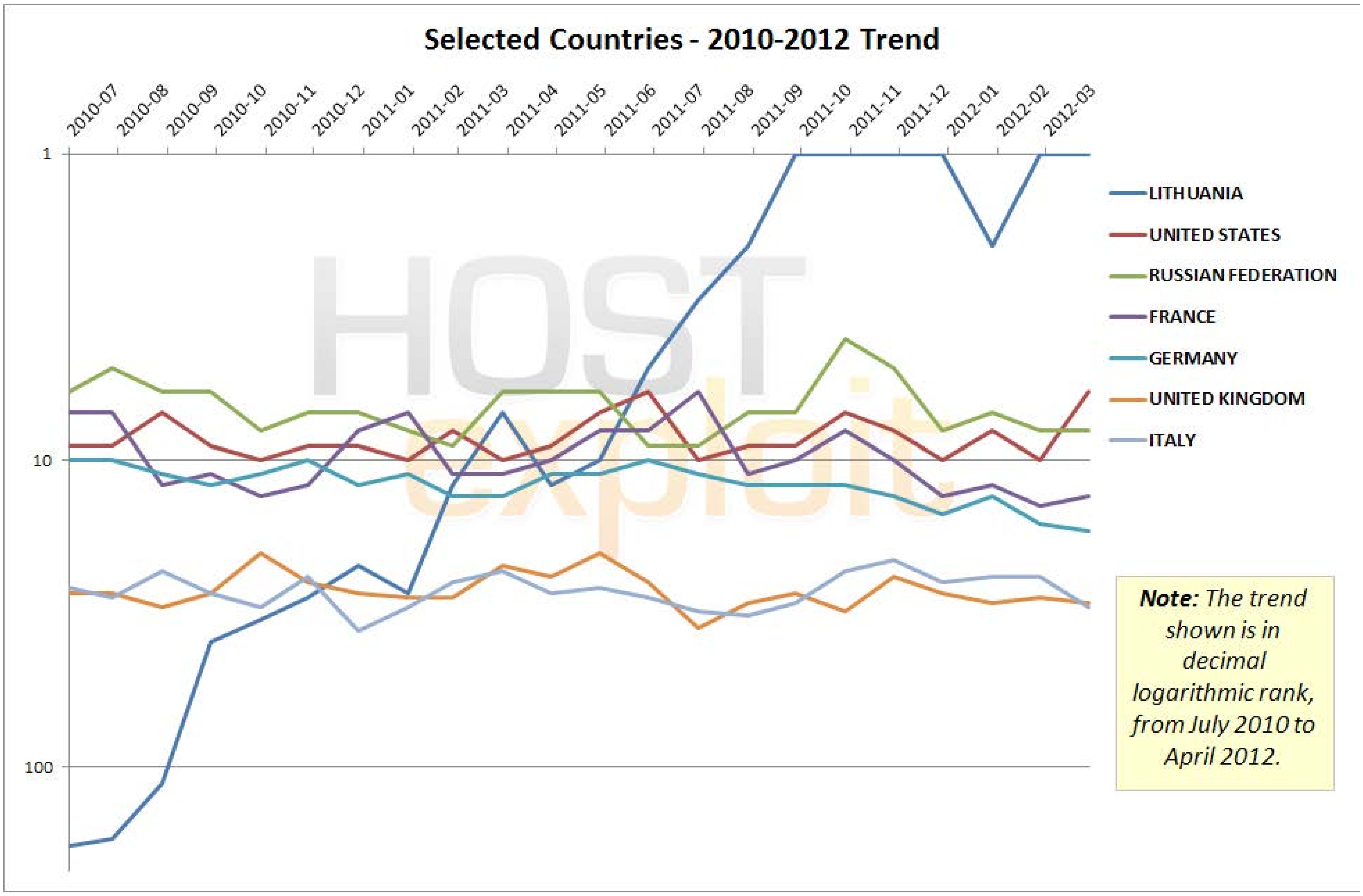
Luxembourg has large concentrations of badware, and Eastern Europe makes up a large proportion of the list.

Current Events and Badware appear to be the most consistent offenders among the Top 10.

4.2. Top 10 Highest Indexed Sectors

Country	Country name		HE Rank	HE Index
LT	**LITHUANIA**		**1**	**369.02**
	Highest sector	**Botnet C&Cs**	1	914.5
	2nd-highest sector	**Phishing**	1	903.8
	3rd-highest-sector	**Zeus botnets**	2	814.5
AZ	**AZERBAIJAN**		**2**	**300.71**
	Highest sector	**Infected web sites**	1	911.2
	2nd-highest sector	**Current events**	2	901.2
	3rd-highest-sector	**Exploit servers**	2	820.6
LV	**LATVIA**		**3**	**261.25**
	Highest sector	**Current events**	3	821.9
	2nd-highest sector	**Exploit servers**	4	462.4
	3rd-highest-sector	**Badware**	3	374.2
VG	**VIRGIN ISLANDS, BRITISH**		**4**	**257.99**
	Highest sector	**Zeus botnets**	1	903.6
	2nd-highest sector	**Botnet C&Cs**	2	792.5
	3rd-highest-sector	**Badware**	19	189.7
CZ	**CZECH REPUBLIC**		**5**	**250.35**
	Highest sector	**Exploit servers**	1	917.5
	2nd-highest sector	**Current events**	8	370.6
	3rd-highest-sector	**Badware**	6	354.5
NL	**NETHERLANDS**		**6**	**246.43**
	Highest sector	**Current events**	6	526.0
	2nd-highest sector	**Badware**	2	442.9
	3rd-highest-sector	**Exploit servers**	6	329.1
RU	**RUSSIAN FEDERATION**		**7**	**235.66**
	Highest sector	**Zeus botnets**	5	411.3
	2nd-highest sector	**Exploit servers**	7	281.7
	3rd-highest-sector	**Current events**	11	268.2
LU	**LUXEMBOURG**		**8**	**234.32**
	Highest sector	**Badware**	1	674.6
	2nd-highest sector	**Current events**	4	624.0
	3rd-highest-sector	**Spam**	34	127.3
MD	**MOLDOVA, REPUBLIC OF**		**9**	**228.39**
	Highest sector	**Zeus botnets**	3	641.2
	2nd-highest sector	**Current events**	5	550.5
	3rd-highest-sector	**Badware**	8	332.7
RO	**ROMANIA**		**10**	**211.46**
	Highest sector	**Current events**	1	904.6
	2nd-highest sector	**Zeus botnets**	6	288.8
	3rd-highest-sector	**Exploit servers**	11	187.9

4.3. Selected Trends



Note: *The trend shown is in decimal logarithmic rank, from July 2010 to April 2012.*

4.4. Cleanest 10 Countries

HE Rank	HE Index	Country	Country name	ASNs
219	**5.25**	38	**FINLAND**	**142**
218	**9.53**	121	**CYPRUS**	**50**
217	**12.25**	384	**PUERTO RICO**	**49**
216	**12.90**	238	**EL SALVADOR**	**11**
215	**13.20**	157	**OMAN**	**3**
214	**13.79**	74	**SYRIAN ARAB REPUBLIC**	**2**
213	**14.05**	1,102	**GREECE**	**105**
212	**15.83**	1,776	**VENEZUELA, BOLIVARIAN REPUBLIC OF**	**37**
211	**16.75**	59	**PARAGUAY**	**15**
210	**17.27**	103	**MACAO**	**3**

Routing Comparison

Summary

As an alternative to basing countries on registration data, we have also based them on routing data. This provides an alternative Rank and Index for each country.

Why is this important? ASes with malicious intent are more likely to use registration data which is false.

Further detail

In the main table of countries, each country is a summation of each of the ASes within that country. This methodology relies on correctly associating each AS with a particular country.

As discussed, the meaning of "where" an AS is located is subjective. Using most definitions, it is still not possible to determine the country with absolute accuracy.

The definition used in the main rankings is the country that the AS is registered to, according to the appropriate internet registry.

It is also useful to look at the countries through which the majority of ASes' allocated IP prefixes are routed. This is also not possible to determine with total accuracy - therefore, we only assert an AS as being in particular country based on its routing data if we are able to assert this with reasonable certainty. If not, we fall back to our traditional definition of the registered country.

Top 10 countries based on routing data

Based on routes		Based on registration		Difference	Country	Country name	ASNs
HE Rank	HE Index	HE Rank	HE Index				
1	397.3	2	300.7	32.1%	AZ	AZERBAIJAN	29
2	263.5	3	261.3	0.9%	LV	LATVIA	192
3	262.7	10	211.5	24.2%	RO	ROMANIA	331
4	243.9	7	235.7	3.5%	RU	RUSSIAN FEDERATION	3,276
5	223.4	9	228.4	-2.2%	MD	MOLDOVA, REPUBLIC OF	33
6	217.3	11	207.8	4.5%	US	UNITED STATES	14,033
7	199.9	1	369.0	-45.8%	LT	LITHUANIA	92
8	199.4	13	174.4	14.3%	FR	FRANCE	581
9	181.4	5	250.3	-27.5%	CZ	CZECH REPUBLIC	903
10	179.6	15	157.2	14.3%	DE	GERMANY	1,124

The above table shows that Azerbaijan, ranked #2 by registration data, comes out on top by routing data. This is largely due to Lithuania dropping down to #7.

None of the upward movements here are particularly large, with all of the Top 10 being in the Top 20 by registration data.

▲ Biggest movers up

Based on routes		Based on registration		Difference	Country	Country name	ASNs
HE Rank	HE Index	HE Rank	HE Index				
33	100.5	155	27.8	261.7%	AL	ALBANIA	23
48	67.6	187	23.7	185.9%	CH	SWITZERLAND	415
121	38.1	205	19.1	99.5%	AN	NETHERLANDS ANTILLES	21
120	38.1	196	20.8	83.5%	DM	DOMINICA	1
11	176.4	33	98.6	79.0%	BS	BAHAMAS	3
57	59.8	81	37.2	61.1%	CO	COLOMBIA	58
211	22.4	213	14.0	59.1%	GR	GREECE	105
24	129.5	37	87.8	47.4%	DK	DENMARK	172
28	117.2	40	81.9	43.1%	CL	CHILE	109
65	54.9	74	39.4	39.2%	SK	SLOVAKIA	84

As can be seen above, some countries have significantly higher Indexes when basing countries on routing data. Albania and Switzerland in particularly show large differences.

These results can be interpreted in a number of ways. One of the more obvious implications is that the registries responsible for these countries do not enforce sufficiently strict regulations when processing AS registrations. Five of the above countries fall under RIPE's jurisdiction; three under LACNIC; and two under ARIN.

With registration data not required to match the location of physical infastructure, it could be interpreted that these 10 countries are where some malicious activity originates from, but is registered elsewhere.

▼ Biggest movers down

Based on routes		Based on registration		Difference	Country	Country name	ASNs
HE Rank	HE Index	HE Rank	HE Index				
72	50.3	21	124.3	-59.5%	EU	EUROPE	1,323
7	199.9	1	369.0	-45.8%	LT	LITHUANIA	92
18	151.4	4	258.0	-41.3%	VG	VIRGIN ISLANDS, BRITISH	3
206	24.1	76	38.7	-37.7%	EG	EGYPT	47
15	164.4	6	246.4	-33.3%	NL	NETHERLANDS	439
168	34.2	67	47.7	-28.2%	IM	ISLE OF MAN	14
9	181.4	5	250.3	-27.5%	CZ	CZECH REPUBLIC	903
14	171.0	8	234.3	-27.0%	LU	LUXEMBOURG	43
46	69.5	36	89.6	-22.4%	BG	BULGARIA	423
51	65.2	42	79.3	-17.7%	SE	SWEDEN	380

Above is the opposite end of the spectrum, with the 10 countries which are most improved based on routing data. Note that Europe is a generic registration category which RIPE allows when a country is not specified.

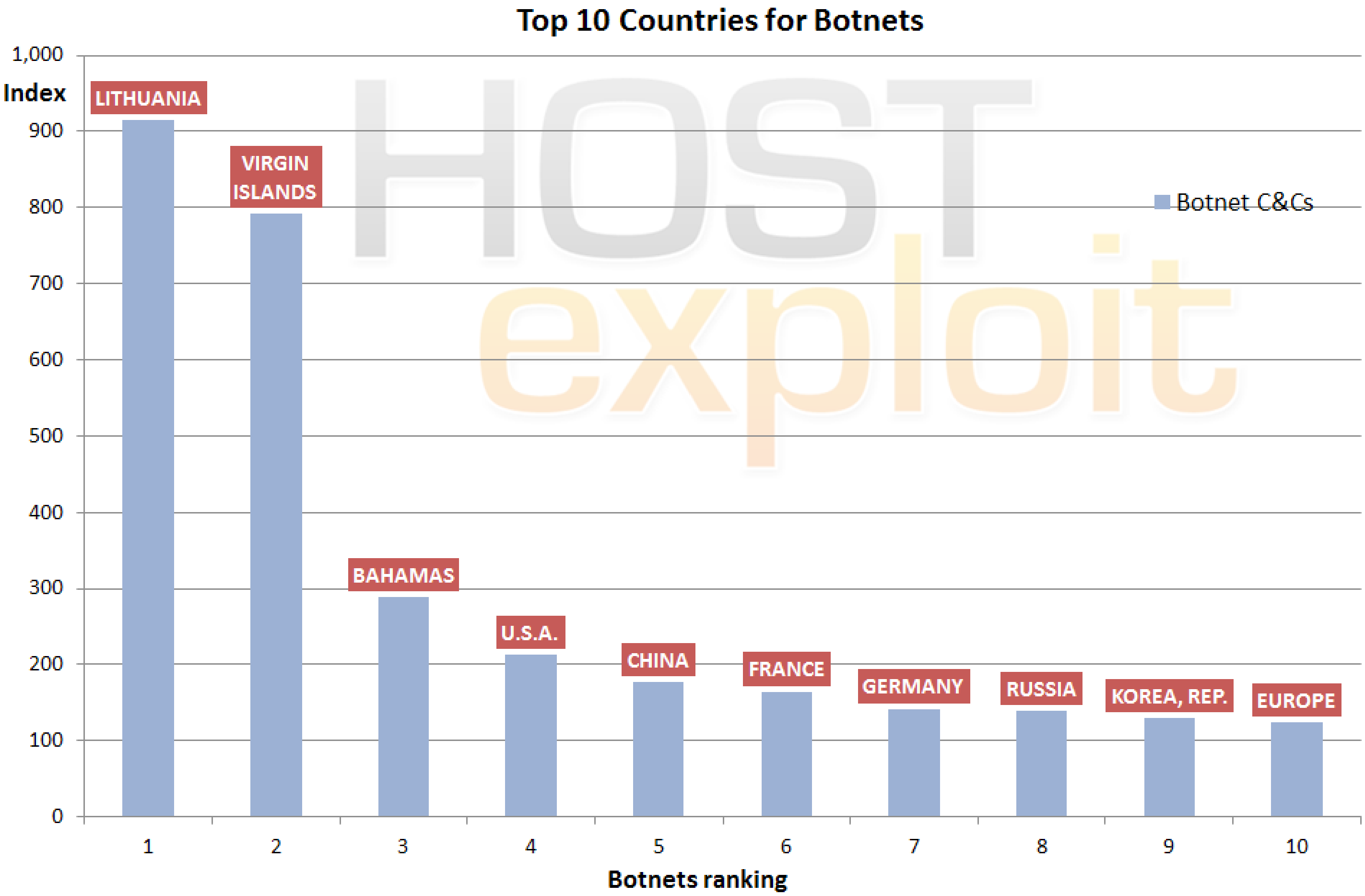
Here, eight countries fall under the jurisdiction of RIPE; one under ARIN; and one under AfriNIC.

It could be interpreted that these are the regions in which ASes are often registered in order to mask the physical location of the source of malicious activity. It would seemingly make sense for a malicious registration to choose the generic "Europe", or countries with low regulation such as the Virgin Islands and the Isle of Man.

6. Countries by Topic

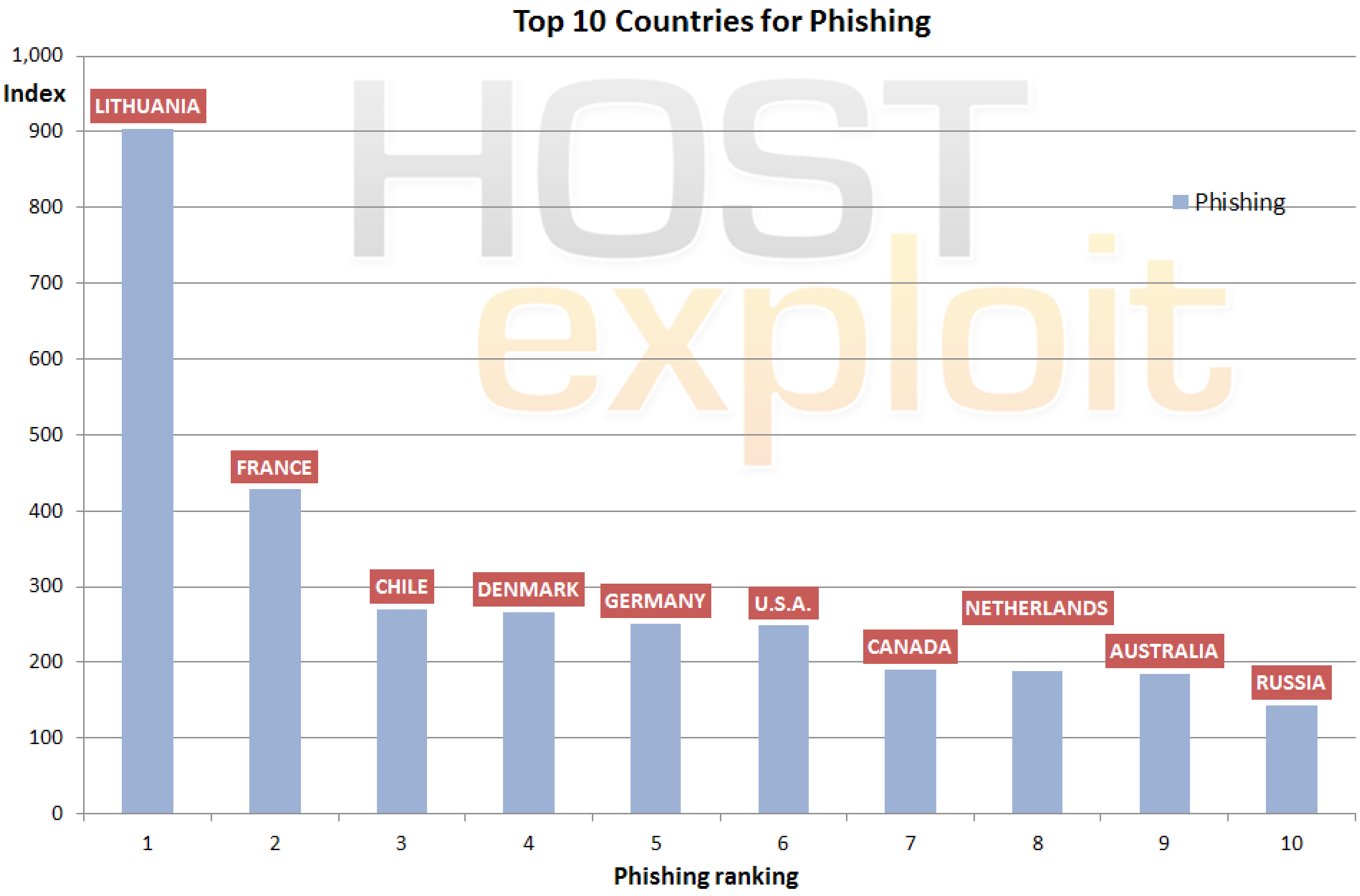
6.1.1. Botnet C&C Servers

HE Rank	HE Index	Country	Country name	ASNs	Botnet Index
1	369.02	LT	LITHUANIA	92	914.5
4	257.99	VG	VIRGIN ISLANDS, BRITISH	3	792.5
33	98.57	BS	BAHAMAS	3	287.9
11	207.81	US	UNITED STATES	14,033	212.8
20	132.16	CN	CHINA	215	176.2
13	174.43	FR	FRANCE	581	164.7
15	157.16	DE	GERMANY	1,124	141.8
7	235.66	RU	RUSSIAN FEDERATION	3,276	139.1
26	113.49	KR	KOREA, REPUBLIC OF	693	129.1
21	124.35	EU	EUROPE	1,323	124.0



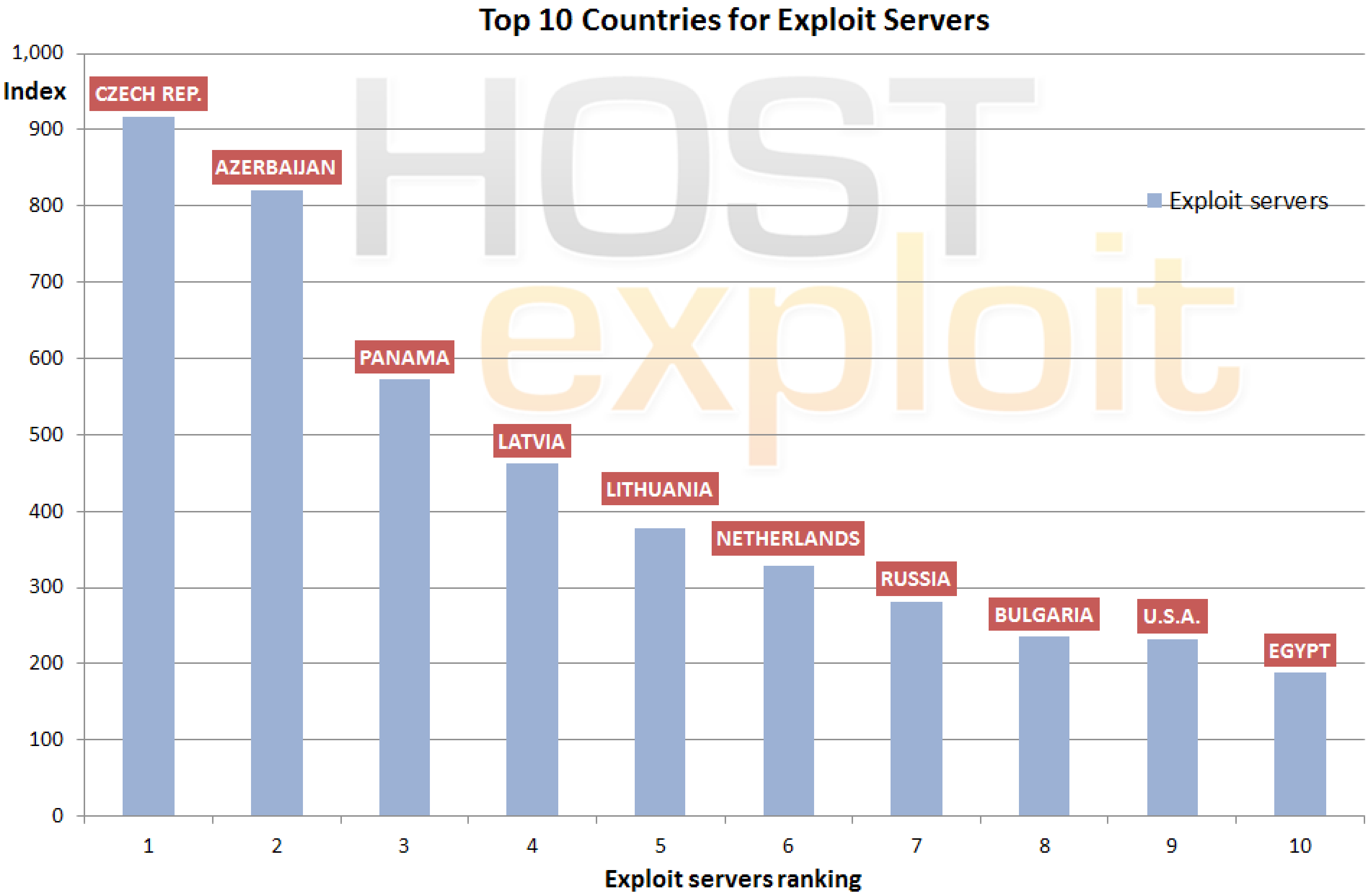
6.1.2. Phishing Servers

HE Rank	HE Index	Country	Country name	ASNs	Phishing Index
1	369.02	LT	LITHUANIA	92	903.8
13	174.43	FR	FRANCE	581	428.5
40	81.87	CL	CHILE	109	270.5
37	87.82	DK	DENMARK	172	266.7
15	157.16	DE	GERMANY	1,124	251.6
11	207.81	US	UNITED STATES	14,033	248.3
27	105.97	CA	CANADA	871	190.9
6	246.43	NL	NETHERLANDS	439	189.2
47	65.72	AU	AUSTRALIA	871	185.5
7	235.66	RU	RUSSIAN FEDERATION	3,276	143.2



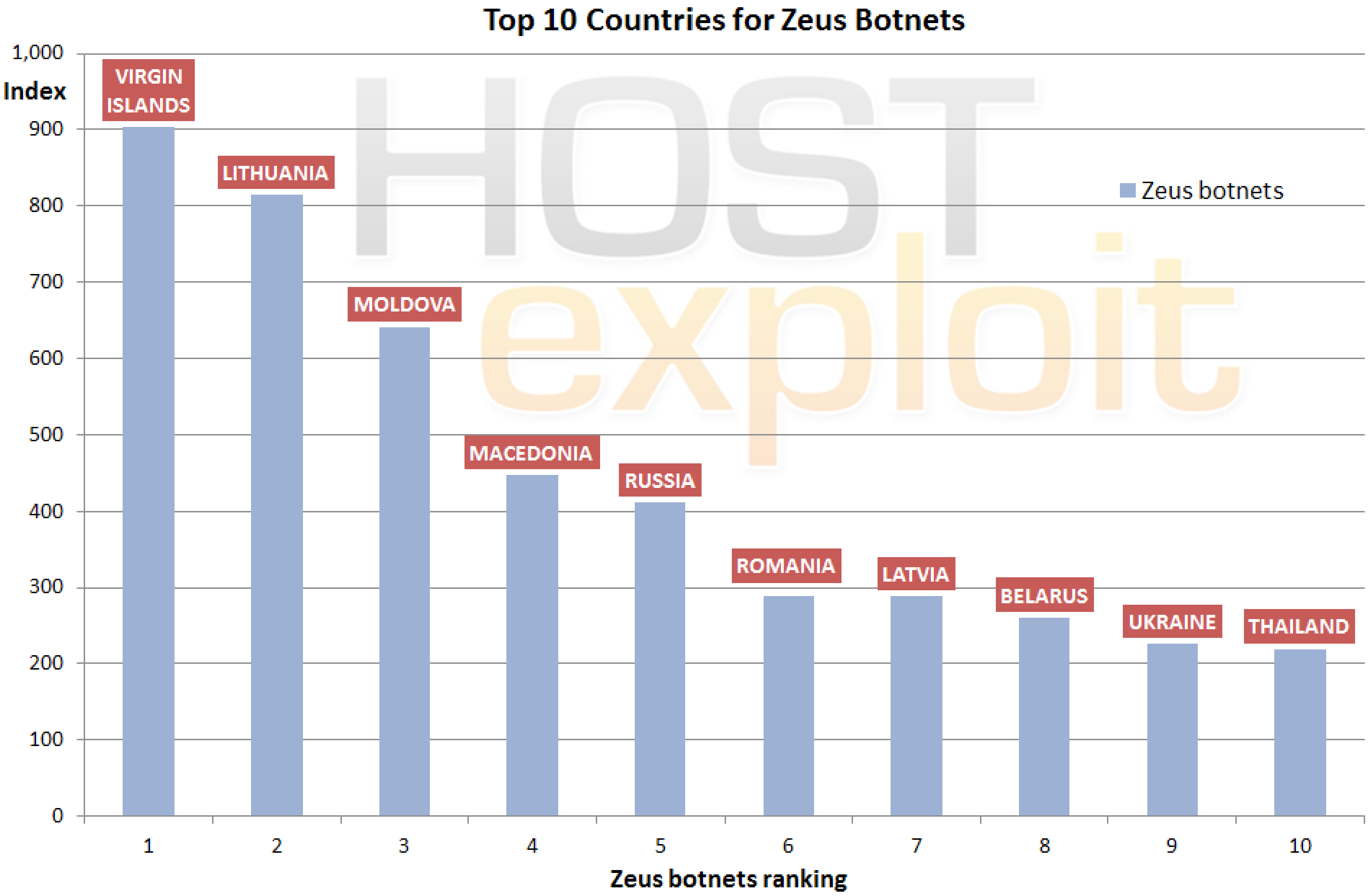
6.1.3. Exploit Servers

HE Rank	HE Index	Country	Country name	ASNs	Exploits Index
5	250.35	CZ	CZECH REPUBLIC	903	917.5
2	300.71	AZ	AZERBAIJAN	29	820.6
24	115.14	PA	PANAMA	66	571.7
3	261.25	LV	LATVIA	192	462.4
1	369.02	LT	LITHUANIA	92	377.2
6	246.43	NL	NETHERLANDS	439	329.1
7	235.66	RU	RUSSIAN FEDERATION	3,276	281.7
36	89.57	BG	BULGARIA	423	235.4
11	207.81	US	UNITED STATES	14,033	232.4
76	38.65	EG	EGYPT	47	188.0



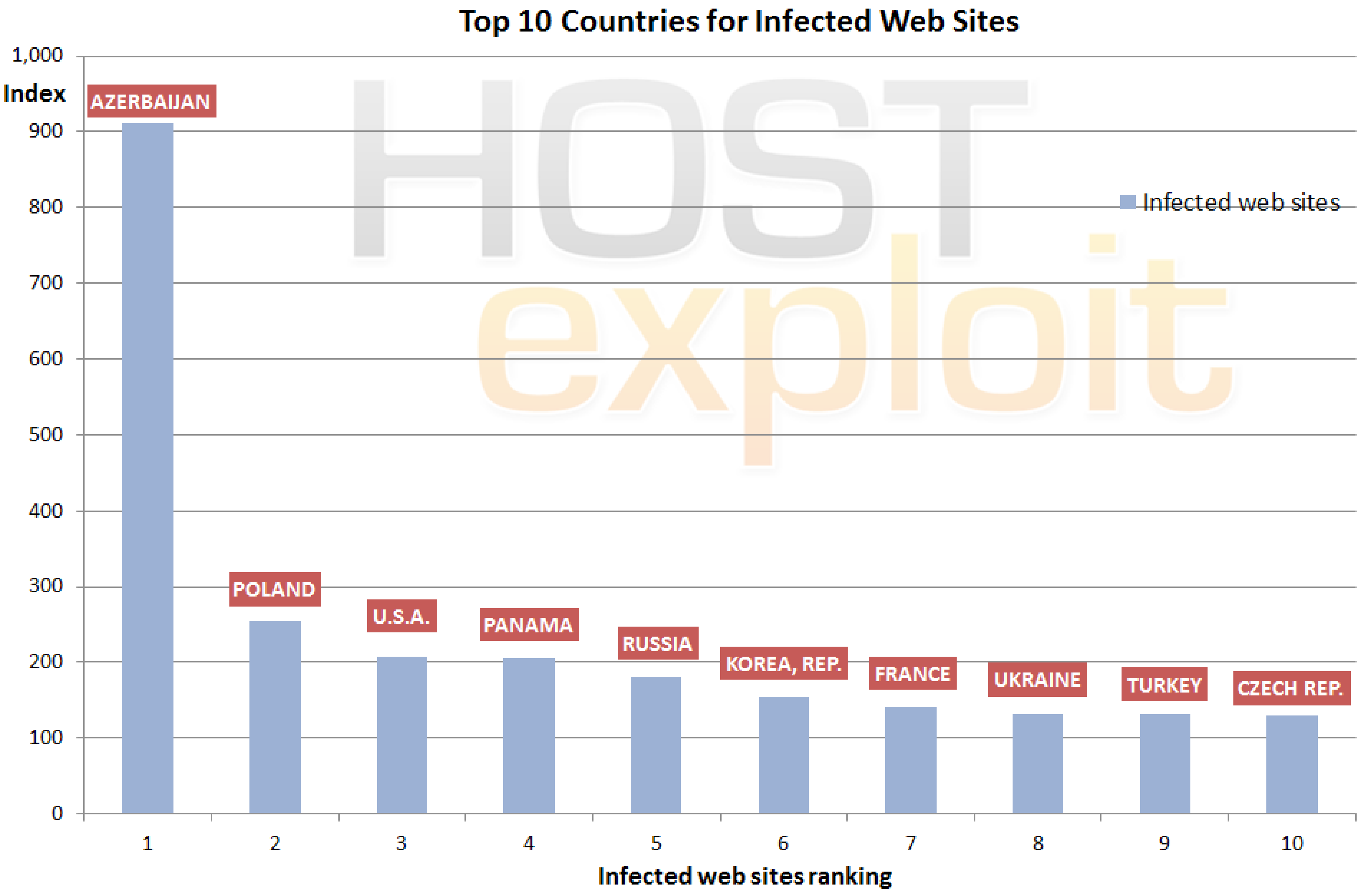
6.1.4. Botnet Hosting - Zeus

HE Rank	HE Index	Country	Country name	ASNs	Zeus Index
4	257.99	VG	VIRGIN ISLANDS, BRITISH	3	903.6
1	369.02	LT	LITHUANIA	92	814.5
9	228.39	MD	MOLDOVA, REPUBLIC OF	33	641.2
35	90.97	MK	MACEDONIA, THE FORMER YUGOSLAV REP.	26	447.4
7	235.66	RU	RUSSIAN FEDERATION	3,276	411.3
10	211.46	RO	ROMANIA	331	288.8
3	261.25	LV	LATVIA	192	288.6
14	160.90	BY	BELARUS	70	260.2
12	200.92	UA	UKRAINE	1,436	225.6
18	136.97	TH	THAILAND	228	219.2



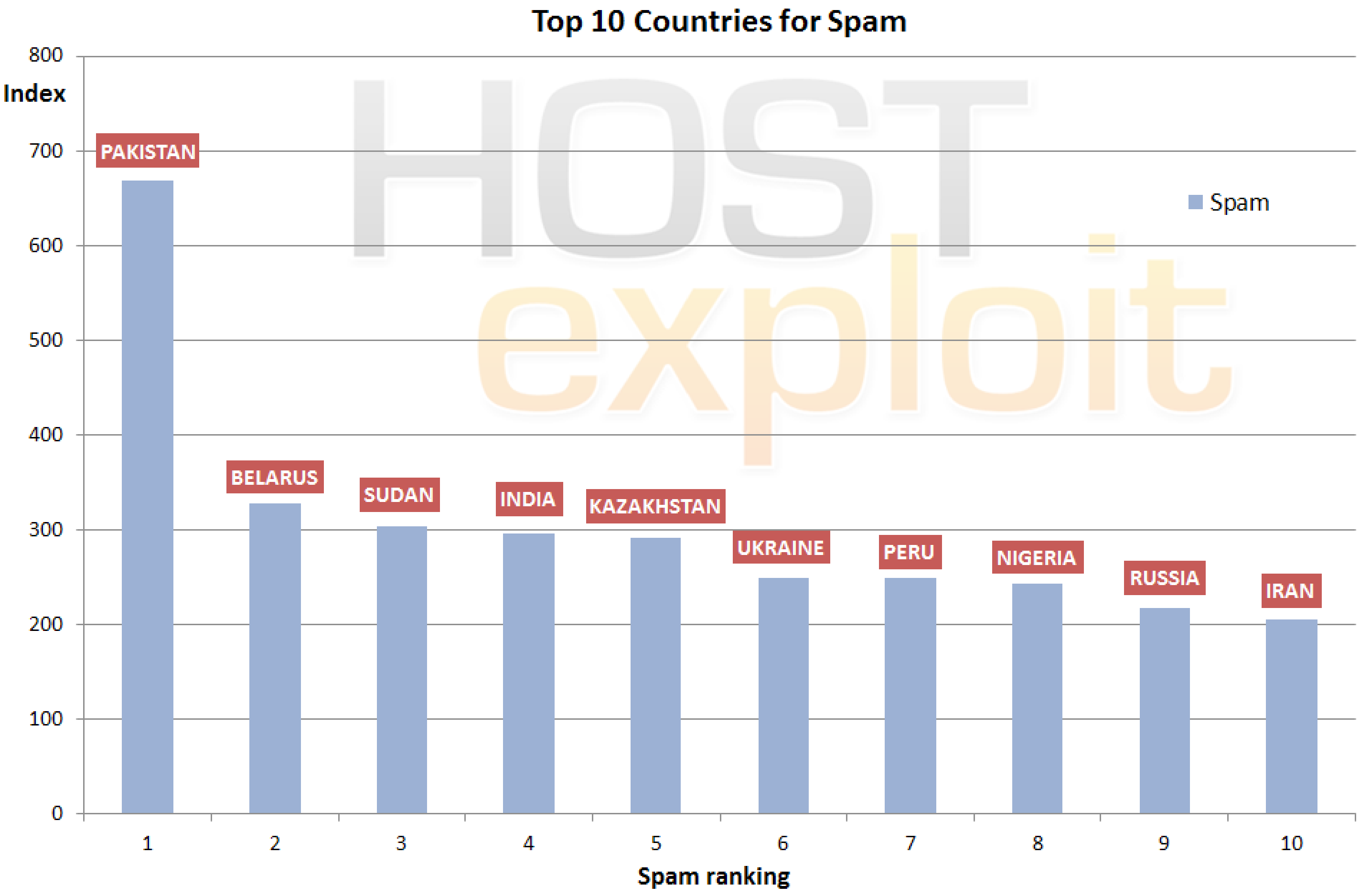
6.2.1. Infected Web Sites

HE Rank	HE Index	Country	Country name	ASNs	Infected Web Sites Index
2	300.71	AZ	AZERBAIJAN	29	911.2
17	143.72	PL	POLAND	1,411	254.2
11	207.81	US	UNITED STATES	14,033	206.4
24	115.14	PA	PANAMA	66	204.6
7	235.66	RU	RUSSIAN FEDERATION	3,276	180.6
26	113.49	KR	KOREA, REPUBLIC OF	693	153.7
13	174.43	FR	FRANCE	581	140.7
12	200.92	UA	UKRAINE	1,436	132.0
19	135.07	TR	TURKEY	277	130.9
5	250.35	CZ	CZECH REPUBLIC	903	130.4



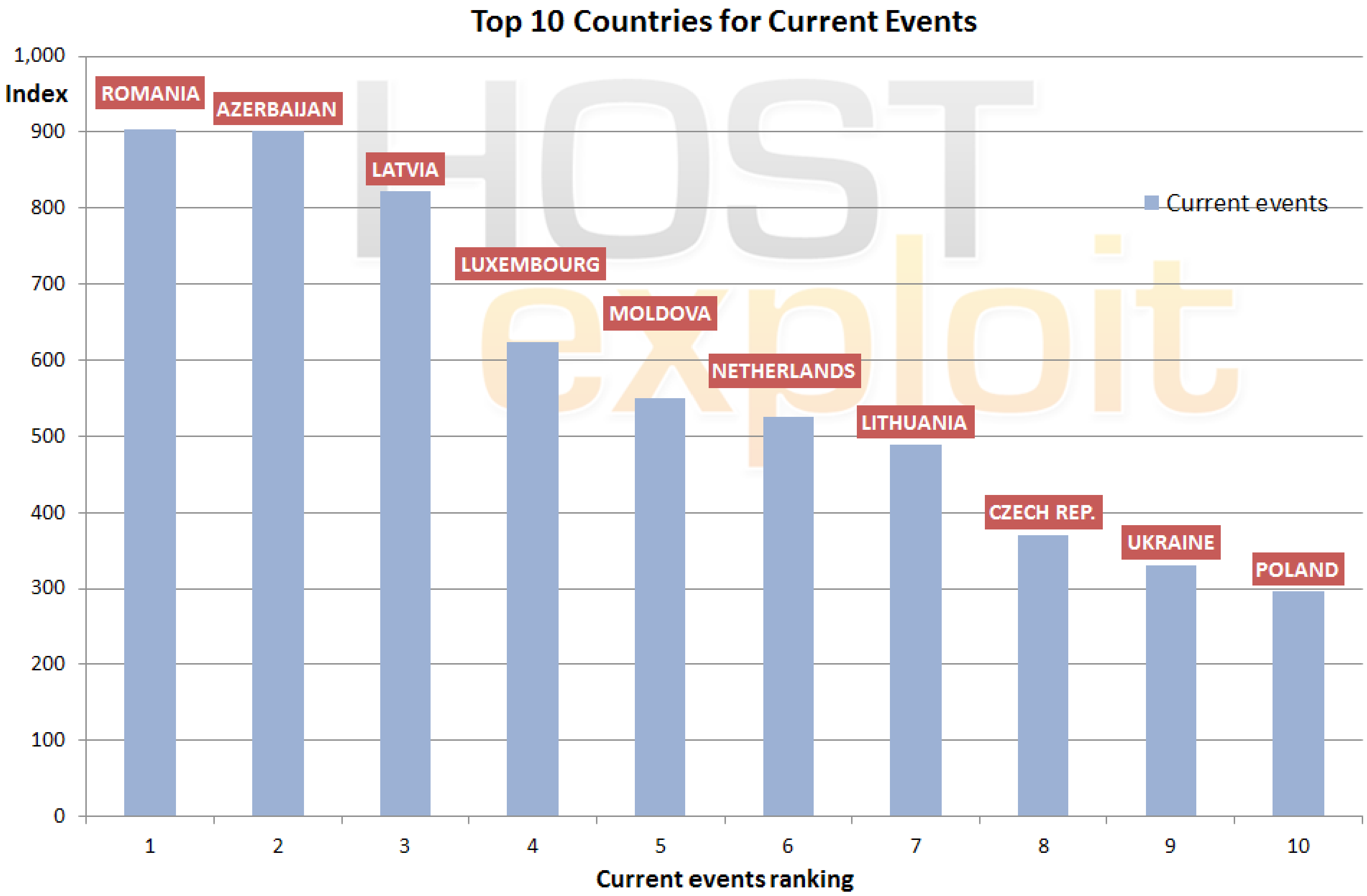
6.2.2. Spam

HE Rank	HE Index	Country	Country name	ASNs	Spam Index
16	152.55	PK	PAKISTAN	59	667.9
14	160.90	BY	BELARUS	70	327.8
39	82.48	SD	SUDAN	6	303.1
32	99.59	IN	INDIA	442	296.3
25	113.98	KZ	KAZAKHSTAN	61	290.9
12	200.92	UA	UKRAINE	1,436	249.5
46	66.40	PE	PERU	17	248.7
51	63.31	NG	NIGERIA	72	242.9
7	235.66	RU	RUSSIAN FEDERATION	3,276	217.5
50	63.93	IR	IRAN, ISLAMIC REPUBLIC OF	193	205.5



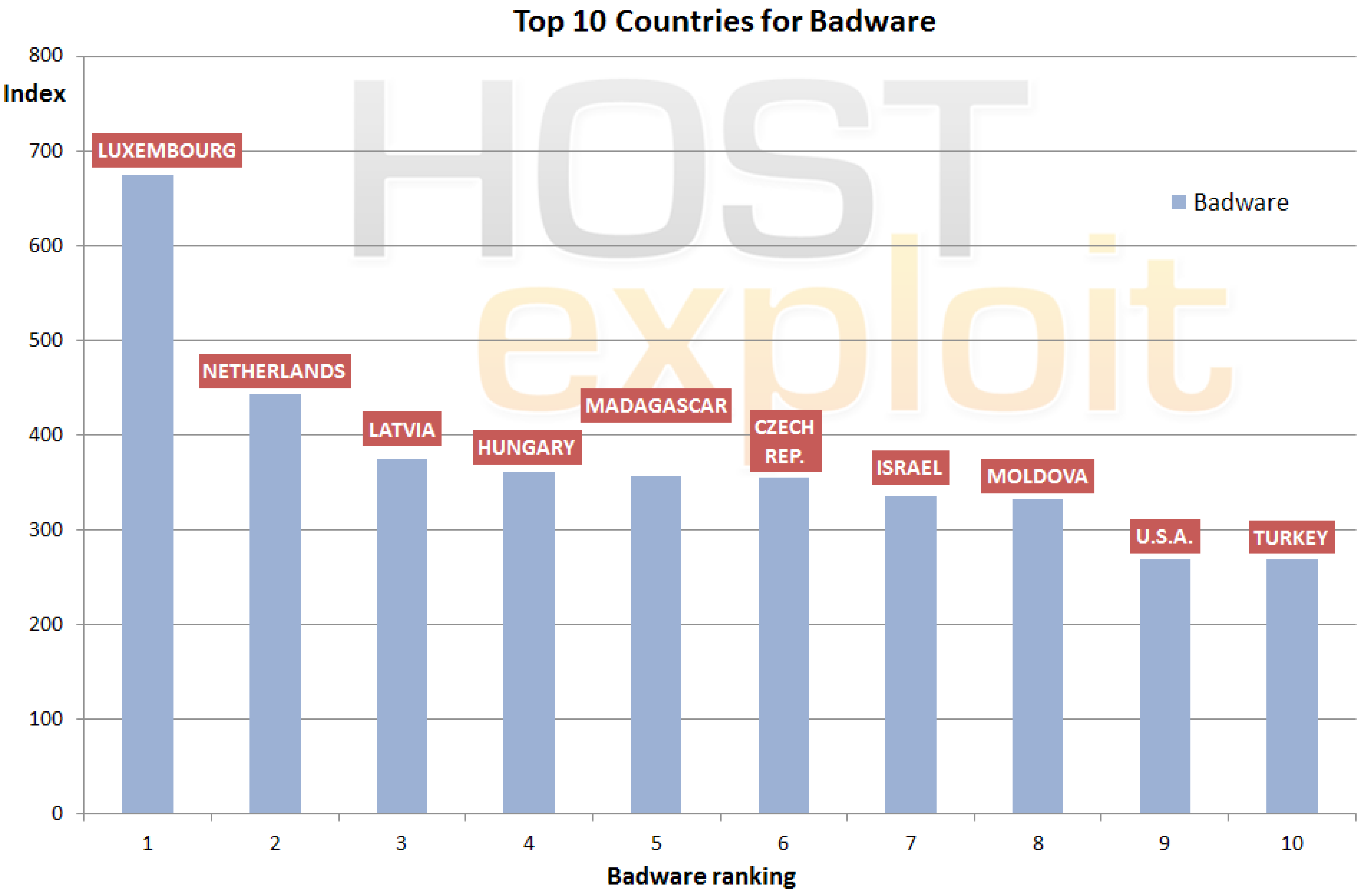
6.2.3. Current Events

HE Rank	HE Index	Country	Country name	ASNs	Current Events Index
10	211.46	RO	ROMANIA	331	904.6
2	300.71	AZ	AZERBAIJAN	29	901.2
3	261.25	LV	LATVIA	192	821.9
8	234.32	LU	LUXEMBOURG	43	624.0
9	228.39	MD	MOLDOVA, REPUBLIC OF	33	550.5
6	246.43	NL	NETHERLANDS	439	526.0
1	369.02	LT	LITHUANIA	92	488.9
5	250.35	CZ	CZECH REPUBLIC	903	370.6
12	200.92	UA	UKRAINE	1,436	331.1
17	143.72	PL	POLAND	1,411	295.3



6.2.4. Badware

HE Rank	HE Index	Country	Country name	ASNs	Badware Index
8	234.32	LU	LUXEMBOURG	43	674.6
6	246.43	NL	NETHERLANDS	439	442.9
3	261.25	LV	LATVIA	192	374.2
23	116.39	HU	HUNGARY	168	360.7
34	91.06	MG	MADAGASCAR	5	356.6
5	250.35	CZ	CZECH REPUBLIC	903	354.5
22	122.54	IL	ISRAEL	201	335.6
9	228.39	MD	MOLDOVA, REPUBLIC OF	33	332.7
11	207.81	US	UNITED STATES	14,033	269.4
19	135.07	TR	TURKEY	277	268.6



Conclusions

Conclusions

So, what makes the difference between the country identified as the "worst", #1 Lithuania, and the "best" #219 Finland? Perhaps some of the answers can be found in a recent Net-Security article by reporter Mirko Zorz who named a Finnish ISP as 'the cleanest ISP in the world'. Certainly Finnish hosts and service providers consistently score low levels of badness according to the HE Index, all of which contributes to the #219 position and the lowest score for 'badness' globally. Even the worst ranked AS in Finland is at #1,060.

When questioned on this subject, Security Manager of TeliaSonera's CSIRT in Finland, Arttu Lehmuskallio put their monitoring and alerting system on the top of the list of reasons for this unrivalled position. Other examples quoted include:

- A better service is provided by acting fast to mitigate the hacking of a customer's box/server
- Using a reversed darknet to detect almost 100% of worms and malware that try to scan the network
- Logging of all outbound traffic when the destination is not found from the routing tables
- Being proactive in searching for badness and informing the client if malware isdetected
- Working closely with FI CERT, researchers and the security community

The mindset of this ISP is to be proactive against every case of abuse of their systems – a zero tolerance policy that reaps returns both morally and economically.

By continuing to evolve our methodology, we hope to encourage hosts and countries into taking the same responsible approach as TeliaSonera. And by enhancing access to data and results through new upcoming features on Global Security Map, we hope to provide a platform on which a variety of professionals can locate cybercrime at any level.

For now, we've begun with a method of visualization which is accessible and understandable to all. Our next report will use an enhanced set of tools, which are able to not only locate countries in a more precise and customizable fashion, but also enable data to be drilled down to specific instances.

Sign up to the mailing list at globalsecuritymap.com to stay in the loop!

Jart Armin

Appendix 1.

Glossary

AS (Autonomous System):

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

Badware:

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

Blacklists:

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

Botnet:

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

CSRF (cross site request forgery):

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

DNS (Domain Name System):

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

DNSBL:

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

Exploit:

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

Hosting:

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

IANA (Internet Assigned Numbers Authority)

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

ICANN (Internet Corporation for Assigned Names and Numbers)

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

IP (Internet Protocol):

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

IPv4

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

IPv6

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

ISP (internet Service Provider):

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

LFI (Local File Inclusion):

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

MALfi (Malicious File Inclusion):

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

Malicious Links:

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

MX:

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

NS (Name Server):

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

Open Source Security:

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

Pharming:

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

Phishing:

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

Registry:

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

Registrars:

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

Remote File Inclusion (RFI):

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

Rogue Software:

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

Rootkit:

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

Sandnet:

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

Spam:

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

Trojans:

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

Worms:

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

XSA (Cross Server Attack):

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