HostExploit's

World Hosts Report

September 2013

Zusammenfassung

Zum ersten Mal überhaupt belegen Hosts aus einem Land, nämlich den USA, die ersten drei Plätze in der Top50-Liste der schädlichsten, registrierten Hosts und Netzwerke. .

Hosting-Praktiken und –Standards zu untersuchen ist wichtig wie eh und je in der Suche nach Verbesserungen in einem System, welches wenige Veränderungen zulässt.

Seit 2009 untersucht HostExploit's World Hosts Report (früher: "Top 50 Bad Hosts") alle 44.000+ weltweiten öffentlichen Autonomen Systeme (ASN) und sammelt dabei Informationen zu infizierten Webseiten, Botnets, Spam und anderen relevanten Aktivitäten. Diese Informationen werden in Zusammenarbeit mit einem Netzwerk aus Experten ausgewertet, um ein realistisches Abbild der Untersuchungsergebnisse sicherzustellen.

Dieser Bericht richtet sich an Service-Provider, Security-Experten, Webmaster und Entscheidungsträger. Im Wesentlichen wird es dem Leser selbst überlassen, seine Schlüsse aus dem Bericht zu ziehen, da die Zahlen für sich selbst sprechen.

Trotzdem gilt es hervorzuheben, dass der überwiegende Teil von schädlichen Inhalten nicht absichtlich gehosted wird. Oft ist dies eine Folge von Passivität und in manchen Fällen können die Hosts sogar selbst das Opfer sein.

Trotz allem bestätigt sich, dass Cyber-Kriminalität, Cyber-Attacken und das Bösartiges im Internet von irgendjemandem irgendwo gehosted werden. Es ist z.B. in einem ASN zu finden und wird von ASN aus verteilt. Aus diesem Grund ist es sinnvoll, dass die Suche nach Lösungen hier beginnt.

- Jart Armin

ISBN 978-0-9836249-6-7

Einbezogene Quellen

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

Herausgeber

Jart Armin

Review

Dr. Bob Bruen

Raoul Chiesa

Peter Kruse

Andre' DiMino

Thorsten Kraft

Andrey Komarov

Godert Jan van Manen

Steven Dondorp

Edgardo Montes de Oca

Unterstützer

Steve Burn

Greg Feezel

Andrew Fields

David Glosser

Niels Groeneveld

Matthias Simonis

Will Rogofsky

Philip Stranger

Bryn Thompson

DeepEnd Research

In Zusammenarbeit mit ECYFED

ECYFED
European Cyber Security Federation

GROUP IB

CSIS

NORTHWAVE

cyscon

SITEVET

montimage

Partner des ACDC Projekts

ACDC
the Advanced Cyber Defence Centre

Sie wollen etwas beitragen?

Sie mögen unsere Arbeit und möchten sie unterstützen? Dann werden Sie Partner oder Sponsor!

Wir arbeiten kontinuierlich daran unsere Arbeit zu verbessern indem wir unsere Reichweite erhöhen.

Wenn Sie uns unterstützen möchten, würden wir uns sehr über eine Nachricht an contact@hostexploit.com freuen.

Editorial

Zum ersten Mal überhaupt belegen Hosts aus einem einzelnen Land, den USA, die ersten drei Plätze in der Top50-Liste der schlimmsten, registrierten Hosts und Netzwerke.

Diese Top3 Hosts sind AS33182 HostDime.com, AS26347 DreamHost, und AS11042 Landis Holdings. The report, spanning the three months of Q3 2013, ranks hosts by the highest observed concentrations of malicious activity, such as malware, spam and botnets.

Dieser Report listet in einer Rangliste die Hosts mit der höchsten beobachteten Konzentration an schadhafter Aktivität, wozu Malware, Spam und Bots zählen, auf. Der untersuchte Zeitraum umfasst die drei Monate des Quartals Q2 2013.

In dieser Rangliste aufzutauchen ist selbstverständlich kein Grund stolz zu sein. Schon seit langer Zeit warnen Experten vor der großen Vielzahl von schadhaften Aktivitäten in den USA, insbesondere im Bereich Phishing[1,2].

Was sind die Ursachen dafür? Die Gründe dafür umfassen:

- **Im Überfluss vorhandene Hosting-Kapazitäten zu niedrigen Preisen.**
- **Stetige Bündelung mit Anonymität.** Viele Registrare und Webhosting–Anbieter ermöglichen anonyme Whois-Registrierungen und die diskrete Möglichkeit, diese Dienstleistung mit Bitcoins zu bezahlen.
- **Eine hohe Reputation.** Die Wahrscheinlichkeit aufgrund seines Standorts gesperrt zu werden ist gering und schafft zudem ein vertrauenswürdiges Umfeld beim Phishing.

Es gibt aber nicht nur schlechte Nachrichten für die USA, denn Sie sind in der Länderliste von Platz 5 auf Platz 9 gefallen. Außerordentlich gute Einzelleistungen von vormals auffälligen Hosts (inklusive AS21740 eNom, Platz 1150, und AS33626 Oversee, Platz 943) halfen dabei, diese Gesamtplatzierung zu verbessern.

Als Zwischenfazit lässt sich sagen: Es ist möglich, das die Hosts bei sich aufräumen. Aber was für Anreize gibt es für sie, dies zu tun?

Derzeit gibt es in diesem Bereich kaum internationale Zusammenarbeit, da diese sich aufgrund rechtlicher Hindernisse sehr schwierig gestaltet. Zudem sind die Verbraucherrechte von Land von Land unterschiedlich oder zum Teil gar nicht vorhanden.

In den USA verweigern sich zudem die ISPs den Versuchen der FCC, allgemeine Standards einzuführen und die Verantwortung an die ISPs zu übertragen. Ursache für diese Verweigerung sind mögliche finanzielle Risiken bei Schadensersatzforderungen, z.B. falls es nicht gelingt, die Verbraucher ausreichend zu schützen.

Auch ohne Bußgelder sollte es für einen ISP einen Anreiz geben, sein Bestes zu geben, um sauber zu bleiben. Die Gründe dafür sind zahlreich – es nutzt dem Handel, der Wirtschaft als auch der nationalen Sicherheit.

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

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

Methodik

Im Dezember 2009 haben wir den HE-Index als zahlenmäßige Repräsentation dafür, wie „schlecht" ein autonomes System ist, vorgestellt. Obwohl er in der Community gut angenommen wurde, haben wir seit dem viele konstruktive Fragen erhalten, von denen wir einige versuchen werden hier zu beantworten.

Warum wird in der Liste nicht die absolute „Schlechte" anstelle einer relativen verwendet?

Ein Kernelement der Charakteristik des Indexes ist die Gewichtung nach der Größe des zugehörigen Adressraums und aus diesem Grund zeigt er nicht die absolute Anzahl schadhafter Aktivitäten in dem AS. Absolute Statistiken wären ohne Zweifel nützlich für Webmaster oder Systemadministratoren, die ihren Routing-Verkehr begrenzen wollen, aber der HE-Index soll die unter den Hosting-Providern weltweit verbreiteten schlechte Umsetzung von Sicherheitsvorkehrungen aufzeigen, zu denen auch die lasche Umsetzung von Maßnahmen zur Missbrauchsbekämpfung gehört.

Sollten größere Organisationen nicht dafür verantwortlich sein ihre Gewinne in bessere Sicherheitsvorkehrungen zu investieren?

Der HE Index gewichtet ASe mit einem kleineren Adressraum höher, aber dies erfolgt nicht linear. Wir verwenden einen „Unschärfe- oder Bayesschen Faktor", um diese Verantwortung abzubilden, wodurch die Zahlen für größere Adressräume verstärkt werden. Die kritische Adressraumgröße wurde dazu in diesem Report von 10.000 auf 20.000 erhöht, um den Effekt weiter zu verstärken.

Wenn diese Zahlen nicht für Webmaster bestimmt sind, für wen sind sie dann?

Webmaster sollten unsere Reports lesen, um ein grundsätzliches Verständnis für die Informationssicherheit jenseits des Alltagsgeschäfts zu bekommen. Unser Hauptziel ist es jedoch, das Bewusstsein für Sicherheitsbelange zu erhöhen. Der HE-Index beziffert das Ausmass in dem Organisationen illegale Aktivitäten zulassen oder vielmehr daran scheitern sie zu verhindern.

Warum wird so etwas überhaupt gehostet?

Es muss betont werden, das HostExploit mit seiner Veröffentlichung nicht aussagt, dass die meisten aufgeführten Hostingprovider der illegalen Nutzung, die von ihren Servern ausgeht, zugestimmt haben. Es ist wichtig in Betracht zu ziehen, dass viele Hosts selbst Opfer cyberkimineller Aktivitäten wurden.

Disclaimer

Wir haben jede angemessene Anstrengung unternommen, um sicherzustellen, dass die Quelldaten für diesen Report zum Analysezeitpunkt aktuell, fehlerfrei, komplett und umfassend waren. Allerdings sind Reports nicht immer fehlerfrei und die Daten, die wir verwenden können aktualisiert oder ohne weitere Ankündigung korrigiert worden sein.

HostExploit oder jeder seine Partner einschließlich CyberDefcon, Group=IB and CSIS sind nicht verantwortlich für Daten, die falsch dargestellt, falsch interpretiert oder in irgendeiner Weise verändert wurden. Abgeleitete Schlussfolgerungen und Analysen auf Basis dieser Daten dürfen nicht HostExploits oder unseren Community-Partnern zugeordnet werden.

Definitionen

IPs

Im gesamten Report bezieht sich das Feld „IPs" auf die Anzahl der einem AS zugeordneten IPv4-Adressen. In Bezug auf die Länder ist es somit die Summe aller „IPs" der ASe in diesem Land.

Land

Da ein AS meist physisch in mehreren Ländern geroutet wird, verwendet HostExploit des herausstechendste Land auf Basis der Routingorte und Registrierungsdaten als Quelle des AS.

HE Index

HostExploit's quantitative Metrik, die die Dichte von schadhaften Aktivitäten, die von einem AS ausgehen, darstellt.

HE Platzierung

Platzierung im Index in Bezug auf alle 44,556 ASe.

Weitere Definitionen finden Sie im Glossar.

Top 50 Hosts

Die 50 ASe mit dem höchsten HE Index, d.h. mit der höchsten Konzentration schadhafter Aktivitäten.

Autonomes System (AS)

Eine Netzverbund mit gemeinsamen Routing, der von einer Organisation oder einem ISP kontrolliert wird.

ASN

Eindeutige Nummer des AS.

HE Index

HostExploits quantitative Metrik, die die Dichte von schadhaften Aktivitäten, die von einem AS ausgehen, darstellt.

HE Platzierung

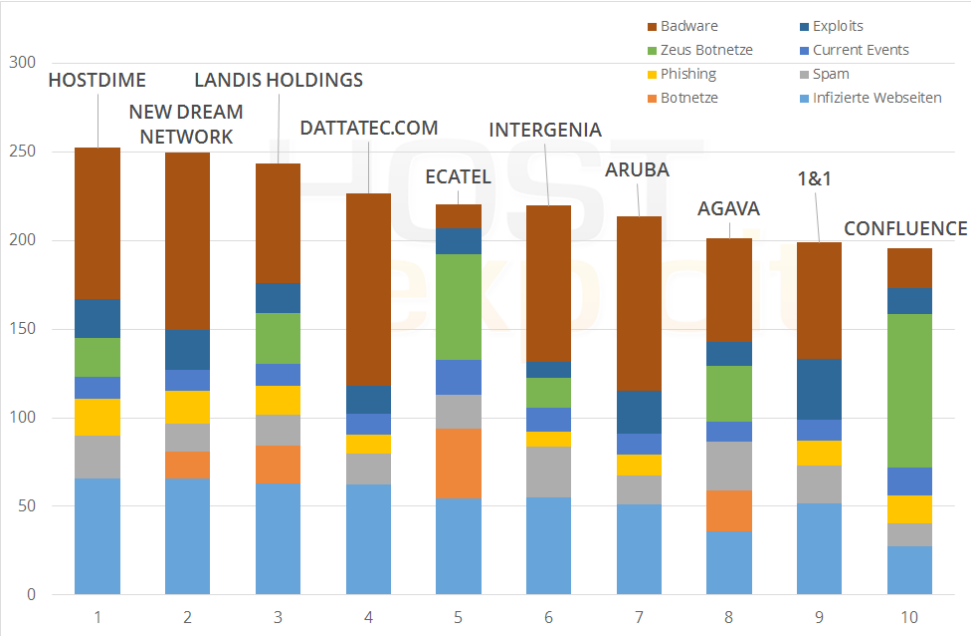
Platzierung im Index in Bezug auf alle 44,556 ASe

IPs

Anzahl der dem AS zugeordneten IP-Adressen

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

Grafische Aufschlüsselung der Top 10



Was ist das?

Das Diagramm auf der linken Seite zeigt den Einfluss der einzelnen Kategorien auf den Gesamtindex des AS.

Dadurch ist sehr einfach erkennbar wo die größten Verbesserungen notwendig sind.

Top 10 der neu registrieren ASe

Die folgenden 10 ASe haben unter den 2.195 seit Erstellung des letzten Reports neu registrierten ASen die höchsten Indizes. Diese ASe könnten zukünftig interessant werden.

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

Nummer der ASes

Im März 2013 Bericht
43,454

AS in diesem Bericht
44,556

New ASes
2,058

Removed
956

Net gain
1,102

Was ist das?

Wir berechnen für jedes Land mit einer ähnlichen Methodik wie für die einzelnen ASe einen Index.

Der Länder-Index zeigt die „Schlechte“ eines Landes auf einer Skala bis 1000 ohne zu stark von der Anzahl der Hosts in dem Land beeinflusst zu werden.

Die Tabelle rechts zeigt die nach dieser Methodik bestimmte Top 10 zusammen mit jeweils den drei Sektoren mit dem höchsten Einzelindex.

Top 10 Länder

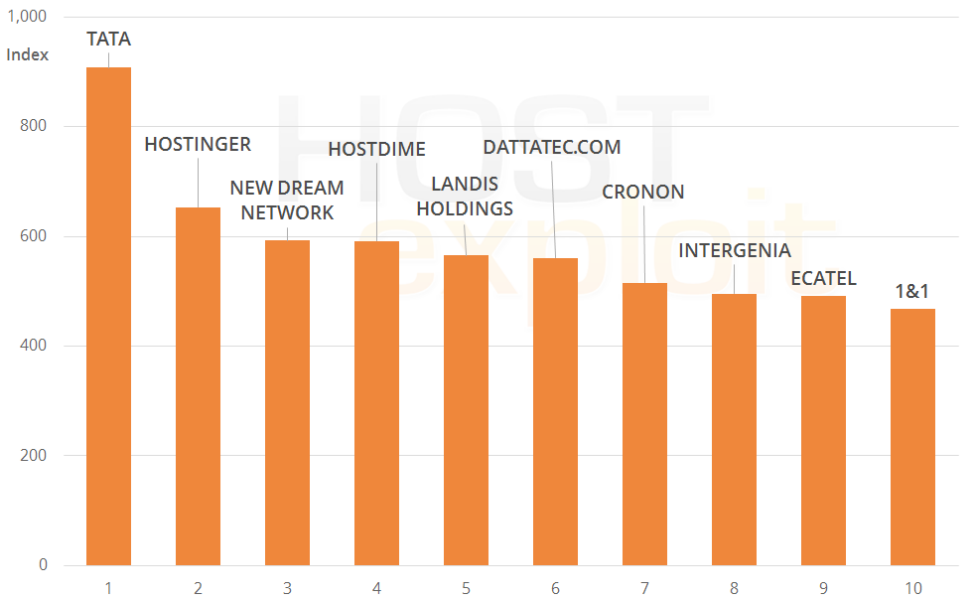
Länderkürzel	Land	ASe	IPs	Platz	Index
VG	VIRGIN ISLANDS, BRITISH	6	18,688	1	435.5
	Highest sector		Infizierte Webseiten	1	905.3
	2nd-highest sector		Botnet C&Cs	1	889.0
	3rd-highest sector		Current events	1	823.9
PL	POLAND	1,590	21,932,032	3	306.7
	Highest sector		Current events	3	666.7
	2nd-highest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

Infizierte Webseiten

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

Alle in den Top3 des Gesamtberichts HE Index Scores gelisteten ASNs ragen in dieser Kategorie hervor, darunter AS26347 DreamHost auf Platz 3, AS33182 HostDime auf Platz 4 und AS11042 Landis auf Platz 5.

Der Spitzenreiter in dieser Kategorie, AS132524 Tata, wurde erst kürzlich in Indien mit einer geringen Anzahl von IPs registriert. Dieser Host könnte bezeichnend für ein temporäre oder „Wegwerf"-ASN stehen.



Wussten Sie schon?

Die Top7 Hosts des Gesamtrankings erscheinen alle in dieser Liste.

Die Zahlen

AS132524 Tata hat den achtniedrigsten Wert an infizierten Webseiten innerhalb dieser Top10, es ist aber ein deutlich kleinerer Anbieter, weshalb er hier auf der Spitzenposition landet.

Wussten Sie schon?

Sotal-Interactive und ISPsystem werden beide vorwiegend aus Russland gehosted, sind aber als Unternehmen in der Ukraine und Luxemburg, registriert.

Botnet C&Cs

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

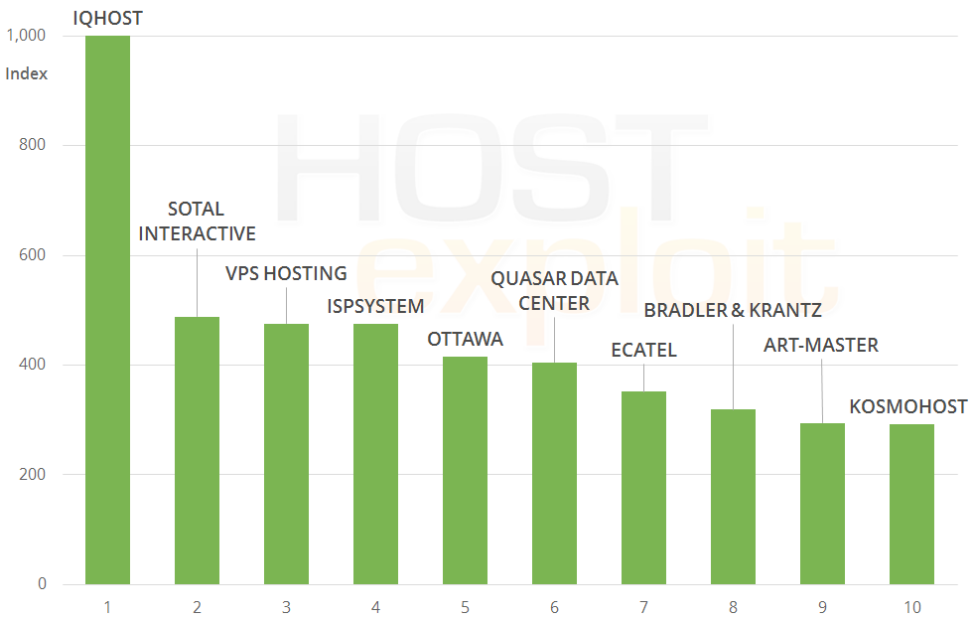
In den Top4 dieser Kategorie gab es keine Veränderung gegenüber dem Report aus Quartal 1 2013.

AS50465 IQHost hält hier die Spitzenposition seit Q2 2012 und ist damit über ein Jahr der Nr.1 Host für Botnet C&Cs.

Die Zahlen

124 Botnet C&Cs wurden in diesem Zeitraum beobachtet, im letzten Bericht waren es 132.

Dies ist geringer als die Gesamtzahl an Vorfällen in jeder anderen Kategorie. Die Macht, welches jedes C&C hält, unterstreicht jedoch ihre Wichtigkeit aus der Sicherheitsperspektive her gesehen.

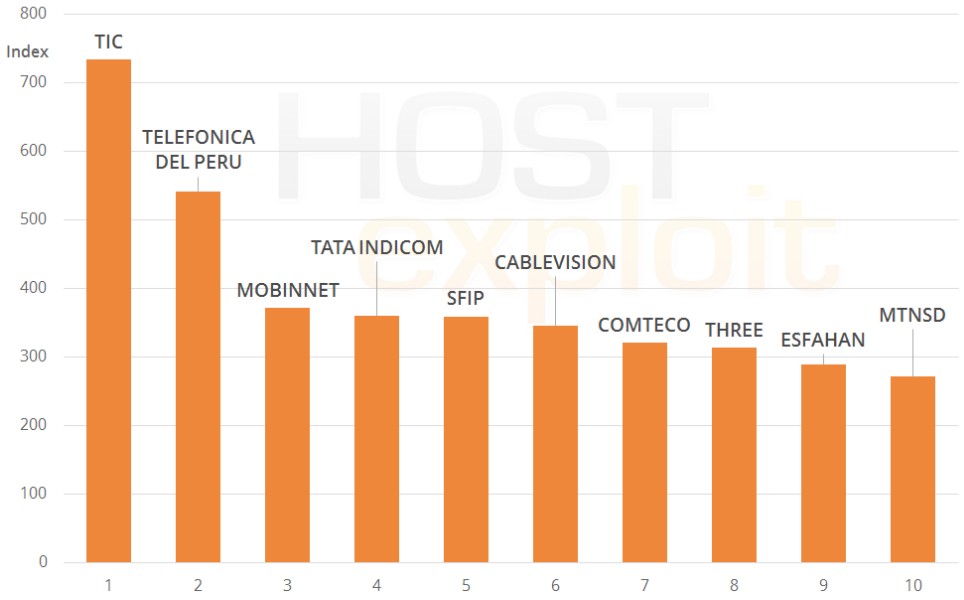


Spam

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

Die Top10 Positionen in dieser Kategorie folgen dem Trend vorheriger Reports. Spammer bevorzugen weiterhin Länder mit dem geringsten Standard an Vorschriften und Hindernissen für AS-Registrierungen.

Acht der Top10 Hosts entsprechen dieser Beschreibung, so sind Iran, Peru, Mexiko, Indien und Bolivien hier vertreten. Als Ausnahmen können AS57879 SFIP, registriert in Deutschland, und AS45727 Three, gesehen werden. Letzterer ist zwar in Indonesien registriert, wird aber aus den USA heraus gehosted.



Was tun wir?

In dieser Kategorie untersuchen wir traditionelle Spam-Server, genauso wie Spam Bots, Crawler und Community-gesteuerte IP Reputationen.

Wussten Sie schon?

Das russische Telekommunikationsunternehmen MegaFon ist endlich aus den Top10 gefallen, nachdem es 2012 zeitgleich sogar vier ASN in den Spam Top10 hatte.

Die Zahlen

Mehr als 100.000 Quellen an Spam wurden für diesen Bericht untersucht.

Wussten Sie schon?

Cisco schätzt, dass im Jahr 2012 sowohl Verbraucher als auch Unternehmen etwa 100 Milliarden Dollar durch Phishing Attacken verloren haben.

Die Zahlen

779 einzelne Phishing-Kampagnen wurden für diesen Report untersucht.

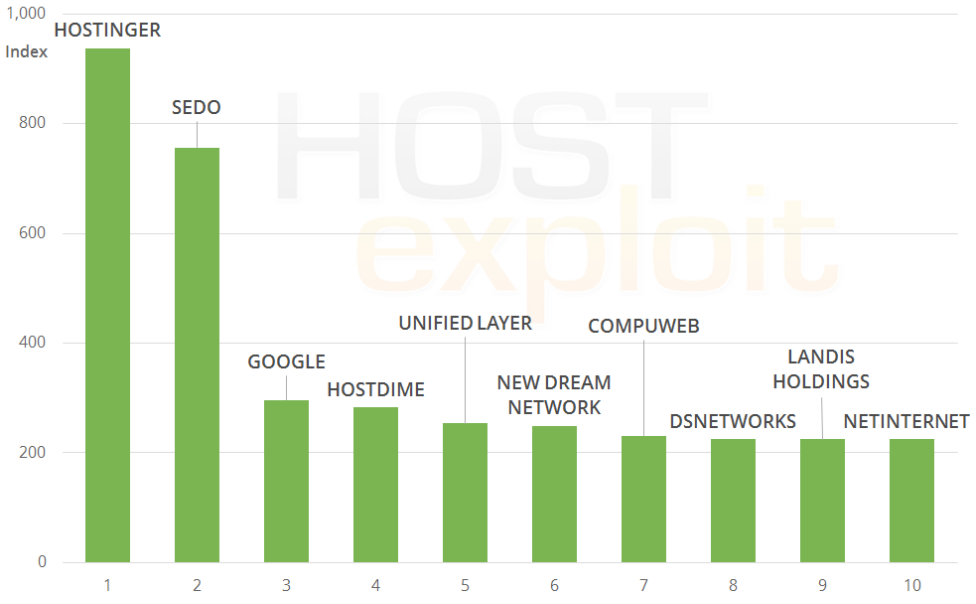
Phishing

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

Große Web Hosting Anbieter aus regulierten Ländern dominieren die Top10 Positionen in dieser Kategorie, inklusive der Top3 bereits erwähnten schädlichsten Hosts.

In diesem sich schnell bewegenden Sektor bevorzugen Phisher die einfache Verfügbarkeit von Hosting-Angeboten in bereits etablierten Regionen. Da Phishing-Seiten nur kurzweilig verfügbar sind, ist eine garantierte Uptime nicht wichtig, und deshalb besteht auch nicht die Notwendigkeit, in unregulierten Regionen gehosted zu werden.

Die scheinbare steigende Legitimität einer Banking oder E-Commerce-Seite in den USA oder Großbritannien gehosted zu sein, ist zudem für Phishing-Betrug von Vorteil.

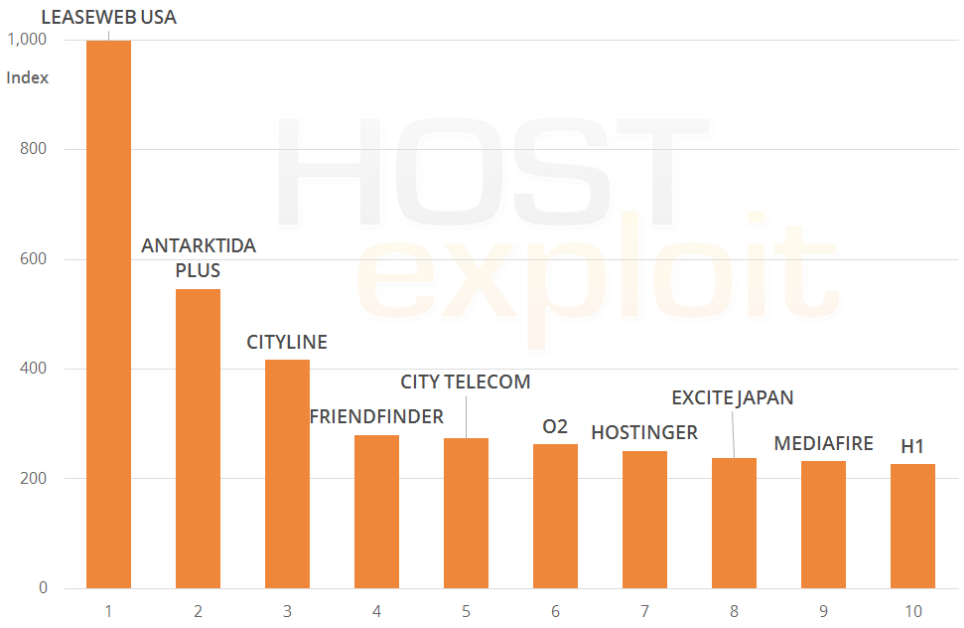


„Currents Events“

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

Erneut hat AS51699 Antarktida einen hohen Wert in dieser Kategorie erhalten, aber die Spitzenposition für diesen Untersuchungszeitraum geht diesmal an AS30633 Leaseweb USA.

Wie der Name schon sagt, ist „Currents Events“ ein schnelllebiger Sektor mit großen monatlichen Schwankungen. Es umfasst eine Vielzahl von Hosts, die für neue Arten von Malware-Inhalten verwendet werden.



Wussten Sie schon?

“Currents Events” ist HostExploit’s eigene Messung von aktuellen und sich schnell ändernden Angriffsbereichen, die weltweit zum Einsatz kommen.

Diese umfassten in letzter Zeit Varianten von MALfi Attacken (XSS/ RCE/RFI/LFI), Clickjacking Techniken, sowie riesiger Botnets.

Die Zahlen

Nachdem in den letzten Reports ein Absinken dieser Zahlen zu verzeichnen war, ist diesmal die Zahl wieder auf 67% gestiegen.

Wussten Sie schon?

Zeus, eine Form von Botnets, welche durch Trojaner verbreitet wird, bleibt weiterhin die populärste Variante eines Botnes, und erfreut sich bereits seit sechs Jahren großer Popularität in der Cybercrimeszene.

Zeus wird ständig verbessert und ist mit seinen zahlreichen Varianten ein Meister im Aushebeln von Sicherheitssystemen, Zeus kommt zudem mit riesigen Netzwerken von Zombie-Maschinen einher.

Die Zahlen

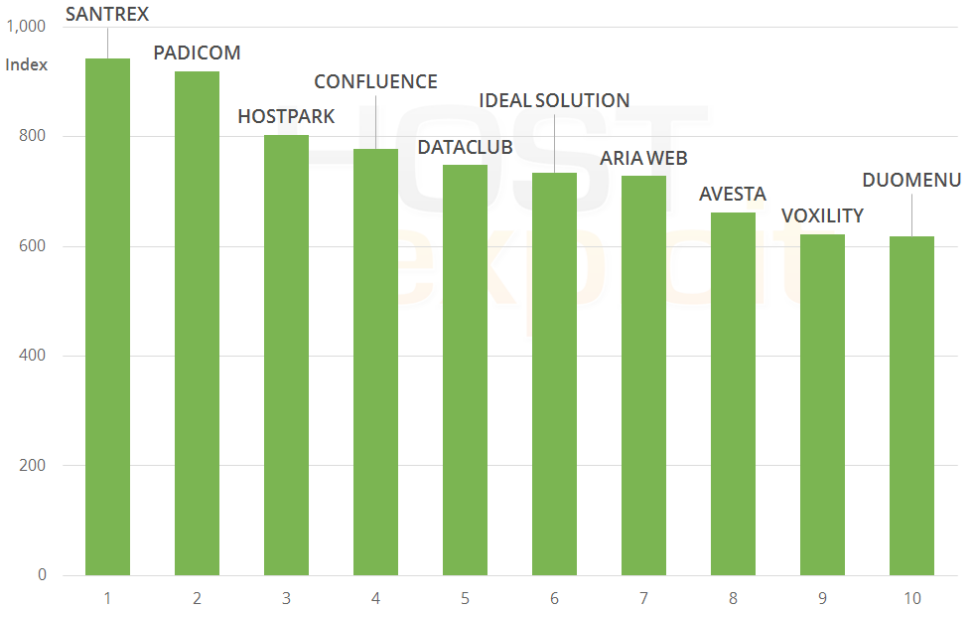
Die Gesamtzahl von beobachteten Zeus-Servern ist nahezu konstant geblieben. Dies könnte bedeuten, dass Zeus weiterhin ein erfolgreiches, profitables und bevorzugtes Botnet Toolkit darstellt.

Zeus Botnets

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

Die Spitzenposition hier halt AS57668 Santrex und hat eine Gemeinsamkeit mit dem Spitzenreiter aus dem vorherigen Quartal, denn auch hier wird das ASN über die Seychellen geroutet.

Im vorherigen Report hatte AS58001 Ideal Solution, jetzt auf Platz 5, die Topposition inne und ist auf den Seychellen registriert, wird jedoch über die Russische Föderation geroutet.

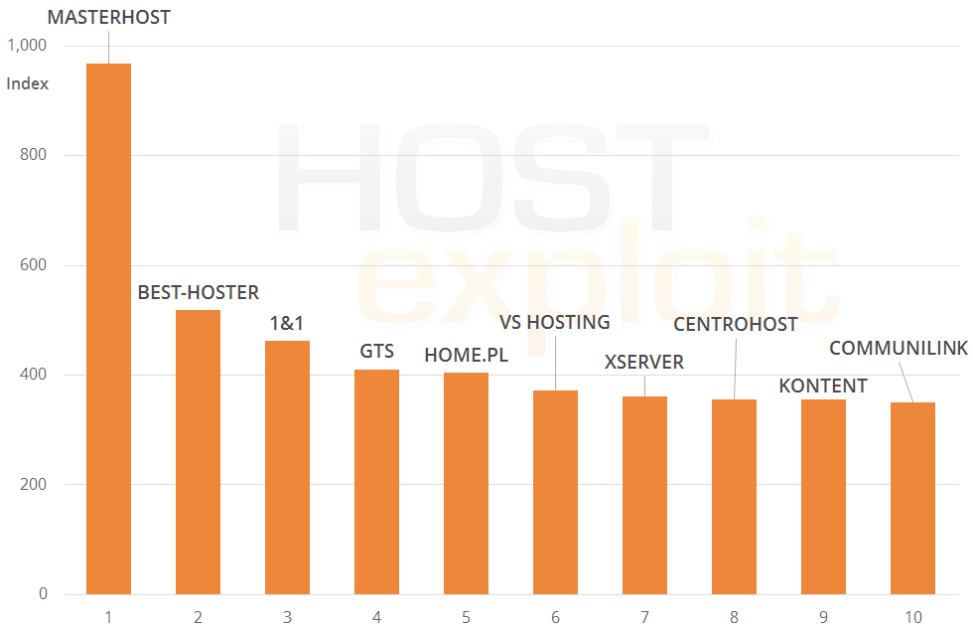


Exploits

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

In dieser Kategorie tauchen erneut die Wiederholungstäter wie AS25532 Masterhost und AS49693 Best-Hoster auf. Beide waren bereits in vorherigen Report hier zu finden.

Die Mehrzahl der Hosts hier sind jedoch Neuzugänge in diesem Sektor.



Wussten Sie schon?

Exploits und die Webseiten, welche diese hosten, sind das Schlüsselstück im Cybercrime Puzzle, da diese meist den ersten Einfallspunkt in den Computer eines Opfers darstellen.

Exploits nutzen den Vorteil von Schwächen in Software, welche zum Teil schon bekannt, aber zum Teil auch noch unentdeckt sind. Der Exploit kann auch anderen Code einschleusen, der dann den Computer des Opfers befällt, des Weiteren kann er auch nur vom Angreifer benutzt werden, um die Kontrolle über einen Rechner zu bekommen.

Die Zahlen

Die Top10 ASN in dieser Kategorie stehen für über 16% aller Exploits, die in diesem Analyse-Zeitraum beobachtet wurden. Dies ist ein Rückgang im Vergleich zu den 29% aus dem letzten Report.

Wussten Sie schon?

Badware ignoriert grundsätzlich, wie Benutzer ihren Computer verwenden. Beispiele für Badware sind Spyware, Arten von Malware, oder betrügerische Arten von Adware. Sie tauchen häufig in der Form von Bildschirmschonern auf, die heimlich Werbung generieren, leiten Browser auf dubiose Webseiten weiter, und verstecken sich als Keylogger, welche private Daten an bösartige Dritte weiterleiten.

Badware

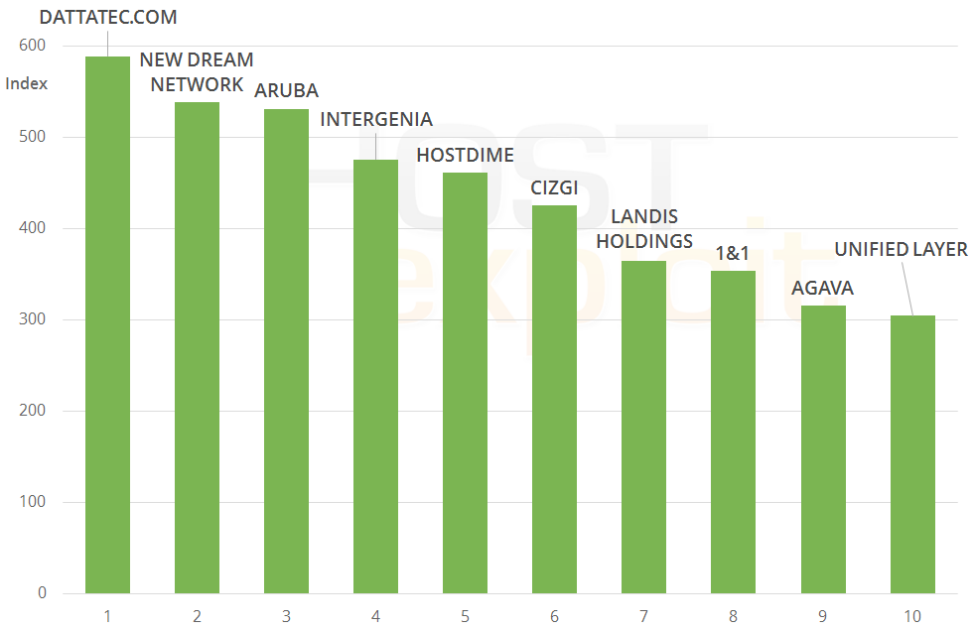
Index	ASN	Name	Land	IPs	Platz	HE Index
588.4	27823	Dattatec.com	AR	8,192	4	226.8
538.7	26347	New Dream Network, LLC	US	230,656	2	249.3
531.0	31034	Aruba S.p.A.	IT	145,664	7	213.6
475.6	8972	Intergenia AG	DE	149,760	6	219.6
461.2	33182	HostDime.com, Inc.	US	63,232	1	252.3
425.0	34619	Cizgi Telekomunikasyon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

In diesem sich schnell verändernden Sektor sind nur zwei Hosts identisch zu Q1, AS31034 Aruba und AS8560 1&1 Internet. Badware reagiert auf kurzfristige Trends und die Hosts in dieser Kategorie ändern sich entsprechend je nach Bedarf.

Unsere Top3 der schädlichsten Hosts sind ebenfalls in dieser Kategorie vertreten. Zusammen mit ihren hohen Ergebnissen im Bereich Phishing und Infizierter Webseiten zeigen sich ähnliche Anforderungen für Hosts, die für diese Art von schadhaften Aktivitäten ausgewählt werden.

Die Zahlen

Die Top10 Hosts in dieser Kategorie umfassen 23% der gesamten Badware-Instanzen, die hier untersucht wurden.



AS (Autonomes System)

Ein AS ist durch einheitliches Routing gekennzeichnet. Es kann sich dabei entweder um ein einzelnes Netz oder eine Gruppe von Netzen, die von einem gemeinsamen Netzworkadministrator für eine Organisation wie eine Universität, ein Unternehmen oder einen Internet Service Provider verwaltet werden, handeln. Als AS wird manchmal auch die Routingdomain bezeichnet. Jedem autonomen System wird seine global eindeutige AS-Nummer zugewiesen (ASN).

Badware

Software, die dem Nutzer grundlegend die Kontrolle darüber entzieht, was sein Computer tut. Dazu zählt Spyware, Malware, Rogueware und fälschende Adware. Üblicherweise taucht sie in Form vom kostenlosen Bildschirmschonern auf, die heimlich Werbung einblenden, Browser zu unerwarteten Webseiten umleiten oder Keylogger enthalten, die persönlichen Daten an bösartigen Dritte übermitteln.

Blacklists:

In der IT ist eine Blacklist ein grundlegender und einfacher Zugriffskontrollmechanismus, der den Zugriff so ähnlich regelt wie ein Nachtclub; jeder darf rein außer die Personen auf der Blacklist. Das Gegenteil davon ist eine Whitelist, entsprechend einem VIP Nachtclub, was bedeutet, dass niemand Zutritt erhält es sei denn er ist ein Mitglieder, das auf der Whitelist steht Eine Mischform davon, eine Graylist enthält Einträge die temporär geblockt oder zugelassen werden. Die Einträge von Graylisten werden getestet bevor sie in Black- oder Whitelisten aufgenommen werden. Einige Communitys und Webmaster veröffentlichen ihre Blacklisten für die Allgemeinheit, wie z.B. Spamhaus oder Emerging Threats.

Botnetz:

Ein Botnetz ist einen Bezeichnung für eine Ansammlung von ferngesteuerten Rechnern (Bots), die unabhängig und automatisch laufen. Der Begriff ist heute meistens mit dem Schadprogramm verknüpft, das Cyberkriminelle verwenden, aber es kann auch für das Netz aus infizierten Rechner mit verteilter Software verwendet werden.

CSRF (cross site request forgery):

Auch bekannt als „Ein-Klick-Angriff/Session Riding" bei dem ein Link oder ein Skript auf einer Webseite mit den Rechten des Nutzers ausgeführt werden.

DNS (Domain Name System):

Das DNS verknüpft Domainnamen mit den unterschiedlichsten Informationen; am wichtigsten ist dabei die Funktion als „Telefonbuch" für das Internet indem es für Menschen einfach lesbare Hostnamen, z.B. www.beispiel.de, in IP-Adressen, z.B. 208.77.188.166, übersetzt, die von Netzkomponenten genutzt werden, um Informationen auszuliefern. Im DNS werden auch andere Informationen wie die Liste der E-Mail-Server, die E-Mails für eine bestimmte Domain annehmen, bereitgestellt.

DNSBL:

Domain Name System Block List – eine Liste von IP-Adressbereichen oder DNS-Zonen, die von Internet Service Providern (ISP) zur Abwehr von Spam oder Badware verwendet wird. Eine DNSBL auf Basis von Domainnamen wir häufig URIBL, Uniform Resource Identifier Block List, genannt.

Exploit:

Ein Exploit ist ein Stück Software oder eine Aneinanderreihung von Daten oder Befehlen, die eine Schwachstelle oder eine Fehler ausnutzen um ein nicht geplantes Verhalten eines Programms, der Hardware oder etwas anderem elektrischen auszulösen. Dies schließt regelmäßig die Übernahme der Kontrolle über den Computer oder das Erlangen von weiteren Zugriffsrechten oder Denial-Of-Service-Angriffen mit ein.

Hosting:

Bezieht sich üblicherweise auf einen Computer (oder ein Netz mit Servern) auf denen die Dateien für eine Webseite gespeichert sind, auf dem die Webserversoftware läuft und der mit dem Internet verbunden ist. Die Seite wird dann als gehosted bezeichnet.

IANA (Internet Assigned Numbers Authority)

Die IANA ist verantwortlich für die weltweite Koordination des DNS, der IP-Adressierung und anderer IP-Ressourcen. Sie koordiniert den globalen Adressraum für IPs und AS-Nummer und weist sie den Regionalen Internet Registrys zu.

ICANN (Internet Corporation for Assigned Names and Numbers)

Die ICANN verwaltet die IP-Adressräume (IPv4 und IPv6) und teilt Adressblöcken den den regionalen Internet-Registrys zu, ist verantwortlich für die Pflege der Registrierung des IP Identifikatoren und für das Management des Top-Level-DNS-Raums. (DNS Root-Zone), was den Betrieb der DNS-Rootserver mit einschließt.

IP (Internet Protocol):

IP ist das primäre Protokoll auf der Internet Schicht der Internet-Protokoll-Familie und sorgt dafür, dass Datenpakete einzig anhand ihrer Adressen von der Quelle zum Ziel gelangen.

IPv4

Das Internet Protocol Version 4 (IPv4) ist die vierte Überarbeitung des Internet Protocol (IP). IPv4 verwendet 32-bit (4 Byte) Adressen, wodurch der Adressraum auf 4.3 Milliarden eindeutiger Adressen beschränkt ist. Allerdings sind zusätzlich einige Adressbereiche bestimmten Zwecken vorbehalten, wie private Netzwerkadressen (18 Millionen) oder Multicasts (270 Millionen).

IPv6

Internet Protocol Version 6 (IPv6) ist eine Version des Internet Protocols, die IPv4 ablösen soll. IPv6 verwendet 128-bit-Adressen, der IPv6 Adressraum umfasst 2^128 Adressen.

ISP (Internet Service Provider):

Ein Unternehmen oder eine Organisation, die die Ausrüstung und einen öffentlichen Zugang bereitstellt, über die zahlende Kunden eine Verbindung zum Internet herstellen können, wie z.B. zum Surfen, für E-Mails oder den Zugriff auf Onlinedatenspeicher.

LFI (Local File Inclusion):

Durch das Einschleusen einer Datei in ein Datenbank wird ein Exploit einer Serverfunktion ausgelöst. Sie kann auch verwendet werden, um verschlüsselte Funktionen innerhalb eines Servers, wie z.B. Passwörter, MD5, usw, zu knacken.

MALfi (Malicious File Inclusion):

Eine Kombination aus RFI (remote file inclusion), LFI (local file inclusion), XSA (cross server attack), und RCE (remote code execution).

Schadhafte Links:

Diese Links werden in Webseiten integriert, um Besucher gezielt auf Webseiten mit schadhaften Inhalt zu führen, z.B. eine Webseite die Viren, Spyware oder jede andere Art von Schadprogramm verteilt. Sie sind nicht immer auf den ersten Blick zu erkennen, da sie verschleichert sind um den Besucher zu täuschen

MX:

Ein E-Mailserver, der E-Mail für die Clients zwischenspeichert und weiterleitet.

NS (Name-Server):

Zu jedem Domainnamen muss ein autorativer Name-Server (z.B. ns1.xyz.com) und mindestens ein nicht-autorativer Name-Server (ns2.xyz.com etc) hinterlegt werden. Durch diese Anforderung ist die Domain auch dann noch erreichbar, wenn einer der Name-Server nicht erreichbar ist.

Open Source Sicherheit:

Dieser Begriff wird am häufigsten für den Quellcode von Programmen oder Daten verwendet, die der allgemeinen Öffentlichkeit zugänglich gemacht wurden und für die es nur geringe oder keine Einschränkungen hinsichtlich des geistigen Eigentums gibt. Open Source Sicherheit erlaubt es Nutzern eigene Software zu erschaffen oder diese durch Zusammenarbeit kontinuierlich zu verbessern.

Pharming:

Pharming ist ein Angriff, bei dem der Verkehr einer Webseite zu einer anderen umgeleitet wird, wie Viehdiebe, die Kühe in die falsche Richtung treiben. Die Zielwebseite ist im Regelfall gefälscht.

Phishing:

Phishing ist eine Art der Verschleierung um wertvolle persönliche Daten wie Kreditkartennummern, Passwörter, Zugangsdaten oder andere Informationen zu stehlen. Phishing wird typischerweise über eine E-Mail gestartet (bei der die Kommunikation von einer vertrauenswürdigen Webseite auszugehen scheint) oder eine Instant Messaging-Nachricht. Auch das Telefon kann zur Kontaktaufnahme verwendet werden.

Registry:

Eine Registry generiert Zonendaten, in denen Domainnamen zu IP-Adressen umgesetzt werden. Domainnamen-Registrys sind VeriSign für .com, Afilias für für .info. Länderbasierte Top-Level-Domains (ccTLD) werden an die nationalen Registrys weitergegeben wie Nominet im Vereinigten Königreich .UK, "Coordination Center for TLD .RU" für .RU und .P?

Registrare:

Ein Domainnamenregistrar ist ein Unternehmen, das Domainnamen registrieren kann und von der ICANN dazu authorisiert wurde.

Remote File Inclusion (RFI):

Eine Methode, die häufig verwendet wird, um Webseiten im Internet von entfernten Rechnern aus anzugreifen. Mit boshafter Absicht kann es mit XSA zusammen verwendet werden, um Schaden auf einem Webserver anzurichten.

Rogue Software:

Rogue-Sicherheitssoftware ist ein Programm, das Malware (schadhafte Software) oder schadhafte Tools verwendet, um sich selbst zu bewerben oder zu installieren oder den Computernutzer für die Beseitigung einer nicht vorhandenen Spyware auf dem Rechner bezahlen zu lassen. Rogue Software installiert häufig ein Trojanische Pferd, um eine Testversion herunterzuladen oder führt andere unerwünschte Operationen aus.

Rootkit:

Eine Sammlung von Softwaretool, die von Dritten eingesetzt wird, um nach dem Zugriff auf einen Computer Änderungen an Dateien oder Prozessen, die ohne das Wissen des Nutzers ausgeführt werden, zu verschleiern.

Sandnet:

Ein Sandnet ist eine abgeschlossene Umgebung auf einer physikalischen Maschine, in der Malware beobachtet und analysiert werden kann. Sie emuliert das Internet so, dass die Malware nicht bemerkt, dass sie beobachtet wird. Sie ist eine gute Möglichkeit um zu analysieren ,wie sich Malware verhält. Ein Honeynet verfolgt das gleiche Konzept, ist aber mehr auf die Angreifer selbst ausgerichtet, um deren Motive und Methoden zu beobachten.

Spam:

Spam ist der allgemein gebräuchliche Begriff für unerwünschte E-Mail. Diese werden massenhaft und walhlos an hunderte oder sogar hunderttausende von E-Mail-Postfächern gleichzeitig versendet.

Trojaner:

Auch als Trojanische Pferde bekannt, erfüllt die Software eine gewünscht Aufgabe oder gibt vor dies zu tun, während sie im Hintergrund Schaden ohne das Wissen oder der Zustimmung des Nutzers anrichtet.

Würmer

Ein Schadprogramm, das sich selbst reproduzieren und von einem zum anderen Computer über ein Netz verbreiten kann. Der Unterschied zwischen einen Wurm und einem Computer-Virus liegt darin, dass sich der Computer-Virus an ein Programm anhängt und eine Nutzeraktion zur Verbreitung notwendig ist, während der Wurm Kopien von sich selbst über das Netz verschicken kann.

XSA (Cross Server Attack):

Eine Angriffsmethode, bei der über einen unsicheren Dienst auf dem Server weitere Dienste angegriffen werden.

Anhang 2

Methodik zur Berechnung des HE-Index

1. August 2012

1 Überarbeitungshistorie

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.

Tabelle 1: Überarbeitungshistorie

2 Motivation

Wir möchten eine einfache und genaue Methode entwickeln, die ein Maß für den Grad an schadhaften Aktivitäten eines Autonomen Systems (AS) in der Vergangenheit ist. Schadhafte Aktivitäten umfasst in diesem Zusammenhang kompromittierte schädliche Server und verdächtige Serveraktivitäten wie das Hosting oder die Verbreitung von Malware und Exploits, Spam-E-Mails, MAL_Angriffen (RFI/LFI/XSA/RCE); Command & Control Centern; Phishing-Angriffen.

Wir nennen dieses den *HE Index*, der eine Wert zwischen 0 (keine schadhaften Aktivitäten) und 1000 (maximale Schadhaftigkeit) annehmen kann. Zu den erwünschten Eigenschaften des HE-Indexes gehören:

1. Die Berechnungen sollen auf mehreren Datenquellen beruhen, von denen jede eine andere Art schadhafter Aktivitäten repräsentiert, um die Auswirkungen von Anomalien in Daten zu verringern.
2. Jede Berechnung soll die objektiv messbare Größe des AS mit berücksichtigen, so das der Index kleinere ASe nicht benachteiligt.
3. Keine AS soll den HE-Index 0 haben, da nicht mit Sicherheit gesagt werden kann, dass in einem AS keine schadhaften Aktivitäten auftreten, sondern nur, dass diese nicht erkannt wurden.
4. Höchstens ein AS kann den maximalen Wert beim HE-Index von 1000 annehmen.

3 Datenquellen

Daten werden aus den folgenden elf Quellen verwendet.

Spamdaten von UCEPROTECT-Network und ZeuS data from Abuse.ch werden kreuzreferenziert mit Team Cymru.

Durch die Verwendung dieser großen Spannbreite an Datenquellen wird die gewünschte Eigenschaft 1 erfüllt.

#	**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

Tabelle 2: Datenquellen

Sorgfältige Test wurden durchgeführt, um den Wertebereich für die spezifische Gewichtung zu bestimmten, die sicherstellen soll, dass als schlecht bekannte ASe an den entsprechenden Positionen auftauchen. Der genaue Wert jeder Gewichtung innerhalb des bestimmten Wertebereichs wird dann vertraulich ermittelt, basierend auf dem tiefgreifenden Verständnis unserer Forschung für die Auswirkungen jeder einzelnen Quelle. Diese Ansatz stellt sicher, dass die Ergebnisse so objektiv und realistisch wie möglich sind, während der notwendige subjektive Einfluss auf das Endergebnis beschränkt wird.

4 Bayessches Gewichtung

Wie erfüllen wir die Anforderung Nummer 2? Damit soll erreicht werden, dass in die Berechnung des HE-Index die Größe des AS gerecht mit einfließt. Der erste Gedanke ist es, die Anzahl der aufgezeichneten Vorfälle durch einen Wert, der die Größe des AS widerspiegelt, zu teilen. Wir könnten dazu die Anzahl der Domains in jedem AS als Wert für die Größe des AS verwenden, allerdings ist es möglich, dass von einem Server schadhafte Aktivitäten ausgehen, ohne dass es eine einzige registrierte Domain gibt, wie es bei McColo der Fall war. Daher ist es pragmatischer die Größe des IP-Adressraums (d.h. die Anzahl der IP-Adressen), die dem AS durch die zuständige regionale Registry zugewiesen wurde, zu verwenden.

Bei der Berechnung des Verhältnisses zwischen der Anzahl der Vorfälle pro IP-Adresse, kommt es allerdings bei einzelnen Vorfälle auf kleinen Servern zu Verzehrungen. Betrachten wir das folgende Beispiel:

Mittlere Anzahl Spam-Vorfälle im Sample: 50
Mittlere Anzahl IPs im Sample: 50,000
Verhältnis: 50 / 50,000 = 0.001
Anzahl Spams: 2
Anzahl IPs: 256
Verhältnis: 2 / 256 = 0.0078125

Bei diesem Beispiel ist bei der Berechnung mit den absoluten Zahlen das Verhältnis fast achtmal so hoch wie bei der Berechnung mit den Durchschnittswerten aus einem größeren Sample. Allerdings widerspricht dem, dass es in Summe nur 2 aufgezeichnete Spams gab. Dies liegt daran, das es in diesem AS nur eine sehr kleine Anzahl IP-Adressen gab. Daher müssen wir das Verhältnis in diesem Fall in Richtung des durchschnittlichen Verhältnisses verschieben – je mehr umso niedriger die Anzahl der IP-Adressen ist.

Um dies zu erreichen, verwenden wir das Bayessche Verhältnis aus der Anzahl der Vorfälle und der Anzahl der IP-Adressen. Dies berechnen wir wie folgt:

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

Mit:
B: *Bayessches Verhältnis*
M: *Anzahl der dem AS zugewiesenen IPs*

M_a: *durchschnittlichen Anzahl zugewiesenen IPs im Sample*
N: *Anzahl der aufgezeichneten Vorfälle*
N_a: *durchschnittliche Anzahl der aufgezeichneten Vorfälle im Sample*
C: *IP -Gewichtung = 20,000*

Durch die Verschiebung des Verhältnis in Richtung des durchschnittlichen Verhältnisses hat kein AS mehr das Bayessche Verhältnis von 0, was aufgrund einer Ungewissheit hinsichtlich der Anzahl der IPs passieren könnte. Damit wird die Anforderung 3 erfüllt.

5 Berechnung

Für jede Datenquelle werden drei Werte berechnet.

Um jedes Bayessches Verhältnis in einem vorgegebenen Wertebereich zu platzieren, wird es durch das maximale Bayessches Verhältnis in dem Sample geteilt und so Faktor C ermittelt:

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

Mit:
B_m: *maximales Bayessches Verhältnis*

Test haben gezeigt, dass in einer kleiner Zahl von Fällen der Faktor C kleinere ASe zu stark begünstigt. Daher ist es logisch einen Faktor hinzuzufügen, der die absoluten Anzahl von Vorfällen repräsentiert und ins Verhältnis gesetzt wird zur mittleren Vorfallsgröße. Dies ist Faktor A:

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

Dies ist analog zum Faktor C und sollte nur einen geringen Einfluss auf den Index haben, da es kleine ASe begünstigt. Es wird nur als Kompensationsmechanismus für die seltenen Fälle von Faktor C verwendet.

Wenn in einem bestimmten AS die Anzahl der Vorfälle signifikant höher als in jedem anderen AS des Samples ist, dann wird Faktor A sehr klein, auch für das AS mit der zweithöchsten Anzahl an Vorfällen. Es ist nicht erwünscht, dass der Wert in einem AS den Wert für den Faktor A verzerrt. Daher wird für den Faktor A (das Verhältnis aus der durchschnittlichen Anzahl der Vorfälle) als Kompensationsmechanismus Faktor B als Verhältnis der maximalen Vorfälle minus der durchschnittlichen Vorfälle verwendet:

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

Mit:
N_m: *Maximum Anzahl der Vorfälle im Sample*

Faktor A kann maximal den Wert 1 annehmen, die Faktoren B und C sind nicht beschränkt, können aber per Definition 1 nicht überschreiten. Höchstens ein AS kann bei allen drei Faktoren das Maximum erreichen, woraus sich der maximale HE-Index von 1000 ergibt (wie in der Anforderung 4 festgelegt)

Der Index wird dann für jede Datenquelle berechnet:

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

Die Gewichtung der Faktoren A, B und C (10Für die Faktoren A und B wurden kleine Werte gewählt, um die Bevorzugung kleinerer ASe zu beschränken (Anforderung 2).

Der gesamt-HE-indes wird dann berechnet durch:

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

Mit:
w_i: *Gewichtung der Quelle (1=niedrig, 2=mittel, 3=hoch, 4=sehr hoch)*