HostExploit's

World Hosts Report

März 2013

Zusammenfassung

Auch wenn Malware immer weiterentwickelt wird und Cyberkriminelle stetig dazulernen, gibt es eine Konstante – fast alles von dem eine Bedrohung ausgeht ist physisch auf Hostingservern zu finden. Aus diesem Grund ist es wichtiger den je, die gelebte Praxis im Hostingumfeld zu beobachten und zu überlegen, wie sie verbessert werden kann.

Eine Ansatz dazu ist es, die Level an cyberkriminellen Aktivitäten auf Servern weltweit zu messen und diese Ergebnisse zueinander in Relation zu setzen. Dies ist das Ziel des seit 2009 erscheinenden World Hosts Report (formals Top 50 Bad Hosts). In dem vierteljährlich veröffentlichten Report werden mehr als 43.000 öffentlich geroutete Autonome System weltweit untersucht, Daten zu infizierten Webseiten, Botnetzen, Spam und anderen schadhafter Aktivitäten erhoben und unter Berücksichtigung vertrauenshafter Quellen aus der Community analysiert.

Der Report richtet sich an ISPs, Sicherheitsexperten, Webmaster und Entscheidungsträger gleichermassen. Zum Großteil bleibt es dem Leser selbst überlassen aus den Daten Schlüsse für sich zu ziehen. Allerdings wird betont, dass die meisten schadhaften Inhalte unwissend gehostet werden – oft als Ergebnis von Nachlässigkeit oder manchmal auch weil der Hoster selbst zum Opfer geworden ist.

In diesem Quartal kehrte der niederländische Hoster Ecatel auf Platz 1 zurück. Bereits in der Vergangenheit hatte er diese Position mehrmals inne. Ecatel führt zwar nicht das Ranking in einer bestimmten Kategorie an, zeigt jedoch schlechte Leistungen quer durch die Bank.

- Jart Armin

ISBN 978-0-9836249-4-3

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

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

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

Verschiedene Presseorgane in den Niederlanden haben die im Januar 2013 veröffentlichte McAfee-Studie aufgegriffen, in der die weltweite Verteilung der aktiven C&C-Server gezeigt und die Niederlande als „Paradies für Cyberkriminelle" dargestellt werden. Wir würden zwar nicht so weit gehen zu behaupten, dass es in den Niederlanden ein dauerhaftes Problem gibt, allerdings haben einige der dort ansässigen Hosting-Provider einen konstant hohen HE Index.

HostExploit's Zahlen ordnen die Niederlande auf Platz 7 weltweit ein. Dies ist vorallem auf zwei der größten Hosting-Provider zurückzuführen, die in den TOP 20 auftauchen – AS29073 Ecatel auf Platz 1 und AS16265 LeaseWeb auf Platz 11. Es könnte argumentiert werden, dass beide Provider das Opfer der hervorragenden Internetinfrastruktur in den Niederladen sind – beide bedienen sowohl den Business- als auch den Consumermarkt – und sie damit ein großer Austauschpunkt für Internetverkehr sind.

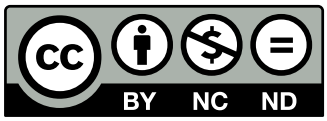
In diesem Quartal kehrte der niederländische Hoster Ecatel auf Platz 1 zurück. Bereits in der Vergangenheit hatte er diese Position mehrmals inne. Ecatel führt zwar nicht das Ranking in einer bestimmten Kategorie an, zeigt jedoch schlechte Leistungen quer durch die Bank.

Unser Ziel ist es nicht bewußt einen einzelne Hostingprovider zu kritisieren, sondern unsere Ergebnisse sollen die gesamte Thematik in das Bewusstsein rücken. Wenn jedoch ein Host in einer Vielzahl von Kategorien schlecht abschneidet und dies durch mehrere Quellen belegt wird, sind die Ergebnisse kaum abzustreiten.

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.



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.

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 43,454 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

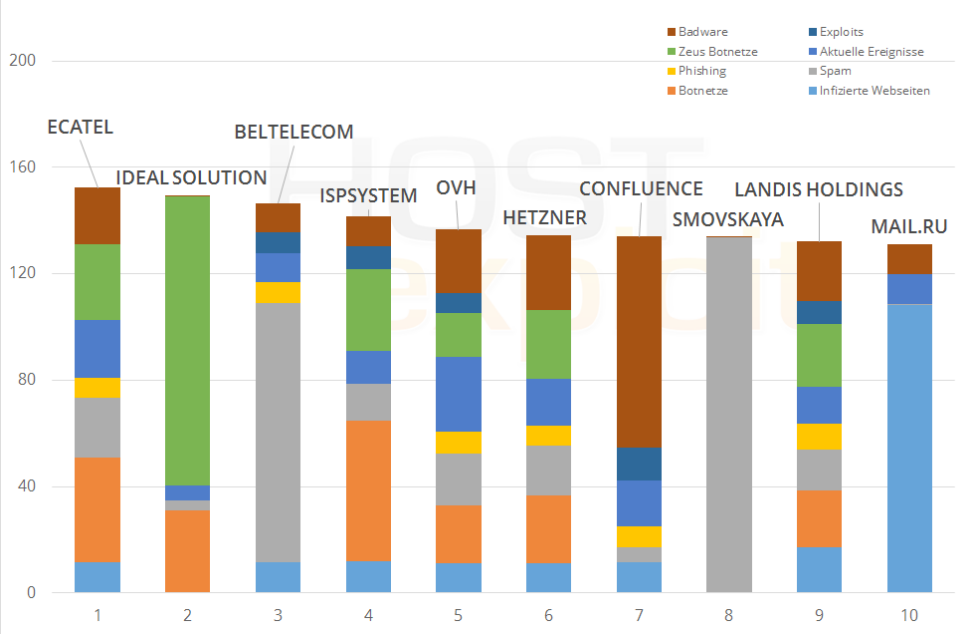
Platzierung im Index in Bezug auf alle 43,454 ASe

IPs

Anzahl der dem AS zugeordneten IP-Adressen

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

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

Anzahl der ASe

Im Report Q3 2012
42,386

ASe in diesem Report
43,454

Neue ASes
2,195

Gelöscht
1,127

Nettozuwachs
1,068

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

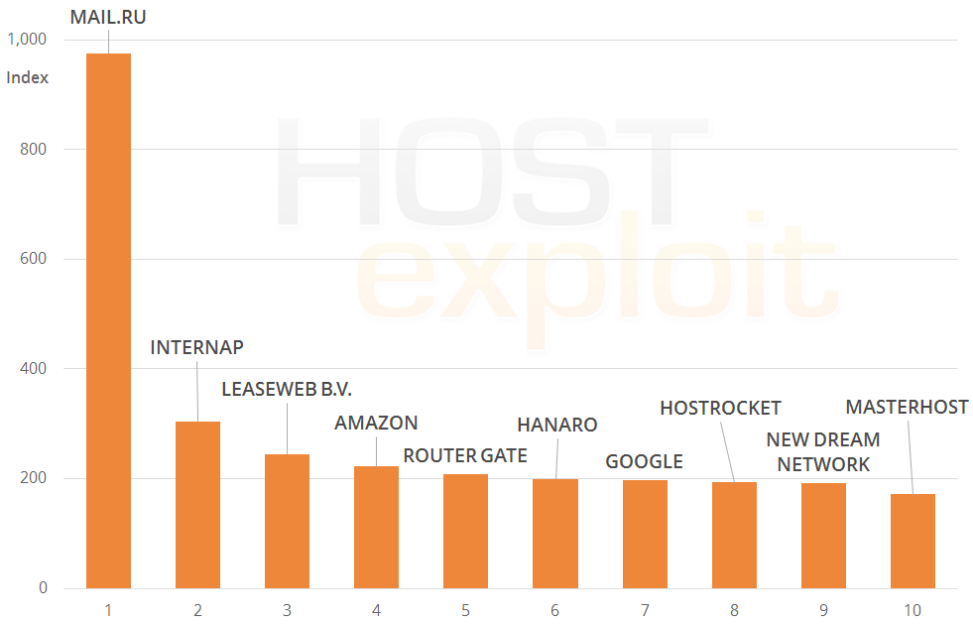
Länderkürzel	Land	ASe	IPs	Platz	Index
RU	RUSSIAN FEDERATION	4,090	54,994,464	1	391.2
	Highest sector		Infected web sites	1	933.3
	2nd-highest sector		Badware	1	618.8
	3rd-highest sector		Botnet C&Cs	2	445.8
BY	BELARUS	79	2,167,808	2	265.0
	Highest sector		Spam	1	762.8
	2nd-highest sector		Infected web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

Infizierte Webseiten

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

Die Anzahl der URL, die zu infizierte Webseiten auf Servern von Mail.ru führen, hat im letzten Quartal drastisch zugenommen, wobei der größte Anteil im Bereich des Dateihostings zu finden ist. Durch diese Zunahme ist Mail.ru in die Gesamt-Top 10 gerutscht. Solch ein plötzlicher Anstieg bei infizierten Dateien, die gehostet werden, könnte entweder das Ergebnis einer neuen Funktion, einem Wechsel der Policy oder durch die Wahl von Mail.ru als temporären Hostingservice durch Cyberkriminelle sein.

HostRocket hingegen zeigt über die vergangenen zwei Quartale einen stetigen Zuwachs. Eine hohe Platzierung sowohl bei den infizierten Webseiten und in der Kategorie Badware zeigt, dass das Problem im Bereich des Contents liegt.



Wußten Sie schon?

An Platz 54 liegt mit Hanaro Telecom das höchstplatzierteste koreanische AS dieses Reports.

In Zahlen

In der Top 10 werden mehr als 59% aller Inhalte gehostet, zu dem in diesem Quartal URLs im Umlauf entdeckt wurden.

Wußten Sie schon?

Sotal-Interactive und ISPsystem werden beide hauptsächlich in Russland gehostet, wurden aber in der Ukraine bzw. in Luxemburg registriert.

In Zahlen

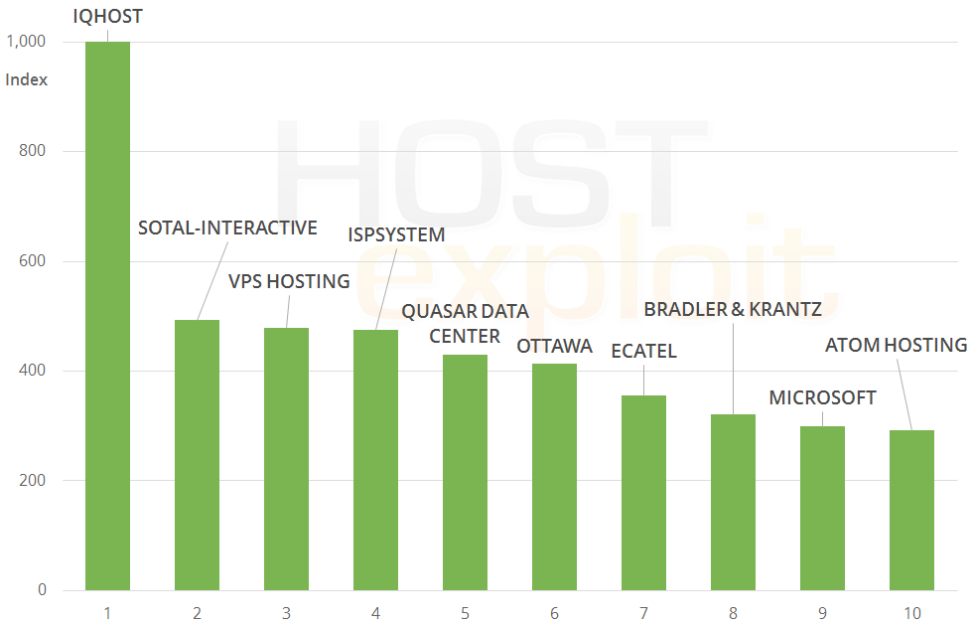
132 Botnetz C&C-Server wurden in diesem Quartal beobachtet und damit weniger absolute Ereignisse als in jeder anderen Kategorie. Die Gefahr, die jedoch von jedem einzelnen C&C-Server ausgeht, unterstreicht die Wichtigkeit der Kategorie aus Sicherheitssicht.

Botnetz C&C-Server

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

Am erwähnenswertesten in der Top 10 der Botnetz C&C-Server ist “Sotal-Interactive”, das im vergangenen Quartal neu registriert wurde. Mit 256 IPs (dem Minimum für ein AS), einer Registrierung in der Ukraine und einen Hosting in Russland, passt es gut in das Profil eines AS, das für ein Wegwerf-Botnetz aufgesetzt wurde.

Auch interessant ist die Auftauchen eines AS von Microsoft, obwohl für dieses keine IP-Blöcke annonciert wurden. Dies scheint im zeitlichen Zusammenhang zu stehen mit der ersten Entdeckung eines C&C-Servers 2012, als ein /16-Block dem AS zugeordnet wurde, dessen Bekanntgabe jedoch kürzlich zurückgezogen wurde.

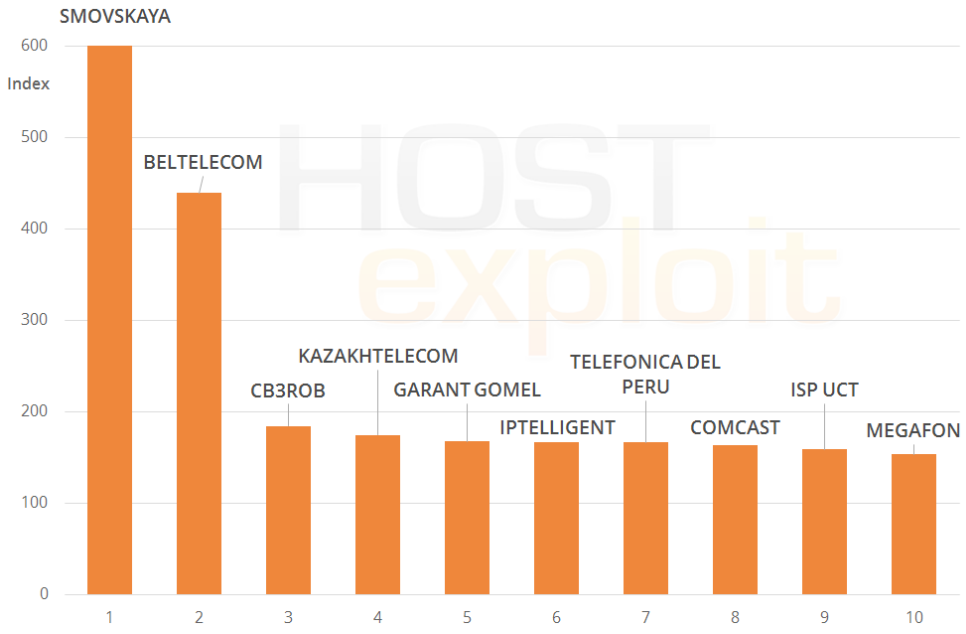


Spam

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

In vorangegangen Reports gab es einen klaren Trend: Spammer bevorzugen für den Versand Länder mit wenig Regulierung und geringen Hürden zur Registrierung neuer ASe. So haben Hosts in Indien, Pakistan und Vietnam die Top 10 für einige Zeit dominiert. Im letzten Quartal war beispielsweise die Hälfte der Top 10 in Indien registriert.

In diesem Quartal gibt es allerdings keine indischen Hosts in der Top 10. Stattdessen sehen wir eine Mischung kleiner extra dafür gebauter Spamserver („Smovskaya“ und den neu registrierten ISP UCT, beide aus der Ukraine) und großer Telekommunikationsunternehmen, die weiterhin mit Spam kämpfen -MegaFon, Beltelecom, Kazakhtelecom und Telefonica del Peru.



Wie gehen wir vor?

In dieser Kategorie untersuchen wir sowohl klassische Spamserver als auch Spambots, Crawler und Listen der Community zur IP Reputation.

Wußten sie schon?

In unserem Report aus dem ersten Quartal 2012 hatte MegaFon 4 ASe in den Spam Top 10

In Zahlen

Mehr als 100.0000 Spamquellen wurden im letzten Quartal ausgewertet.

Wußten Sie schon?

Cisco schätzt, dass 2012 rund 100 Milliarden Dollar an Verlust durch Phishing für Unternehmen und Privatpersonen entstanden ist.

In Zahlen

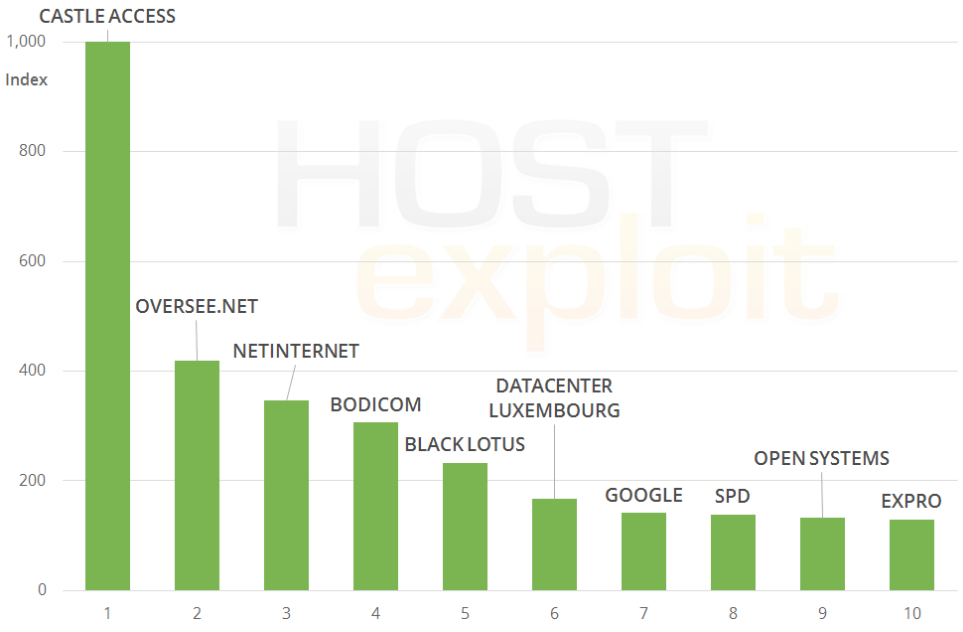
Vergangenes Quartal wurden für die 10 aufgeführten Hosts 110 Phishingvorfälle gemeldet im Vergleich zu 2461 im aktuellen Quartal.

Phishing

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

Phishing ist ein sehr schnell beweglicher Sektor der Cyberkriminalität – dies wird durch die Tatsache, dass die Mehrzahl aller Phishingseiten nur für einige Minuten online bleiben, unterstrichen. Aus diesem Grund ist es keine Überraschung, dass nur ein Kandidat der neuen Top 10 auch im letzten Report eine solch hohe Platzierung hatte.

Weiterhin ist die kurze Lebensdauer solcher Seiten ein Hinweis darauf, wieso als Hosting-Länder die USA und Kanada bevorzugt werden – die Regulierung mag dort härter sein, aber wenn erwartet wird, dass eine Seite schnell offline geschalten wird, ist das wichtigste Kriterium der Cyberkriminellen die Einfachheit und Verfügbarkeit des Hostings.

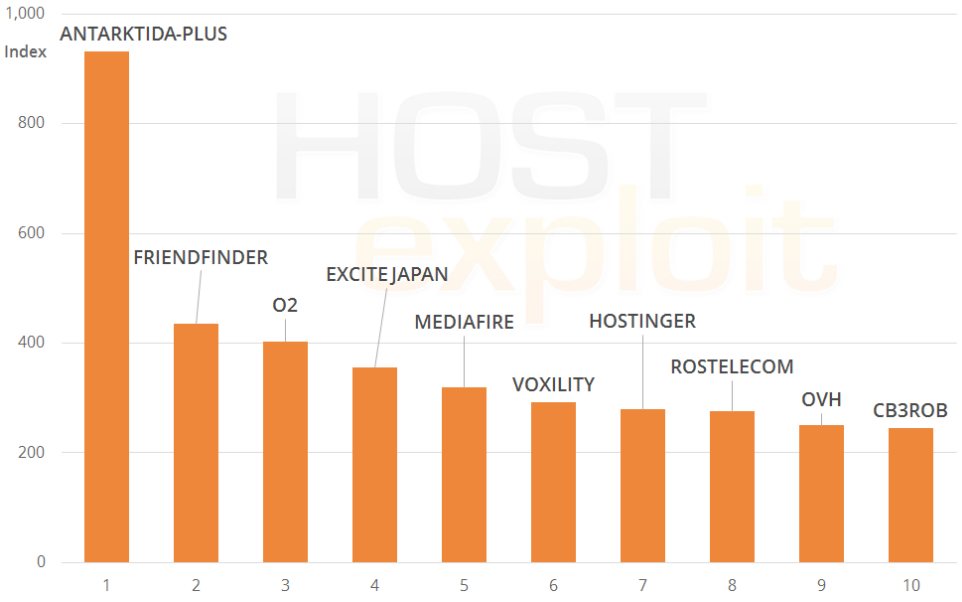


Aktuelle Ereignisse

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

Wie der Name schon verrät ist die Kategorie „Aktuelle Ereignisse“ ein schnelllebiges Feld woraus eine Vielfalt an Hosts resultieren, auf denen neuartiger schadhafter Inhalt gehostet wird. Nur Voxility bleibt in der Top 10 erhalten. Große Onlinepräsenzen wie Friendfinder und MediaFire sind genauso vertreten wie die große französische Hostingfirma OVH.

Drei ASe wurden in anderen Ländern registriert als sie nun gehostet werden: Antarktida in Russland, Hostinger in Litauen, und CB3ROB in den Niederlanden



Wußten Sie schon?

In der Kategorie „Aktuelle Ereignisse spiegelt HostExploits die aktuellsten und sich am schnellsten ändernden Angriffsvektoren weltweit wieder.

Dazu gehören Varianten von MALfi-Angriffen (XSS/RCE/RFI/LFI), Clickjacking und große Botnetze.

In Zahlen

Die Anzahl aktueller Ereignisse ,die in diesem Quartal beobachtet wurden, betrug nur 17% der Ereignisse im vorangegangenen Quartal.

Wußten Sie schon?

Zeus, ein Botnetz, dass sich über Trojaner verbreitet, bleibt eine der populärsten Botnetzvarianten auch 5 Jahre nachdem es erstmals Popularität in der cyberkriminellen Untergrundszene erlangt.

Zeus wurde kontinuierlich weiterentwickelt und angepasst und bietet eine Vielzahl von Varianten um Sicherheitsmechanismen zu umgehen und große Netze mit Zombies aufzubauen.

In Zahlen

Die absolute Zahl von Zeus-Server, die beobachtet wurden, blieb annähernd konstant im vergangenen Jahr. Wenn ein Zeus C&C-Server vom Netz genommen wird, ist es üblich, dass er an einer anderen Stelle ersetzt wird.

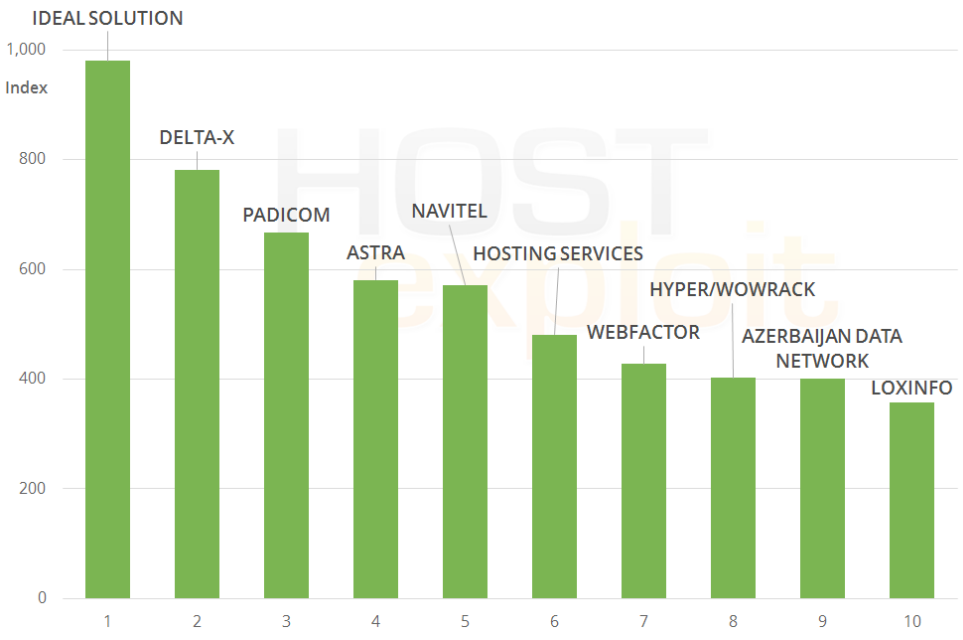
Zeus Botnetze

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

Ideal Solution, registriert auf den Seychellen, ist von Platz 9 auf Platz 1 in dieser Kategorie gewandert und belegt bei der Anzahl der erkannten Zeus C&C-Server Platz 4.

Gleichfalls bemerkenswert ist Astra LLC – das russische AS wurde neu registriert und belegt sogleich Platz 4. Mit nur 256 IP-Adressen und 2 Zeus C&C-Servern, scheint es ein Wegwerf-AS zu sein.

8 von 10 ASen stammen aus Osteuropa – genausoviel wie im vergangenen Report.

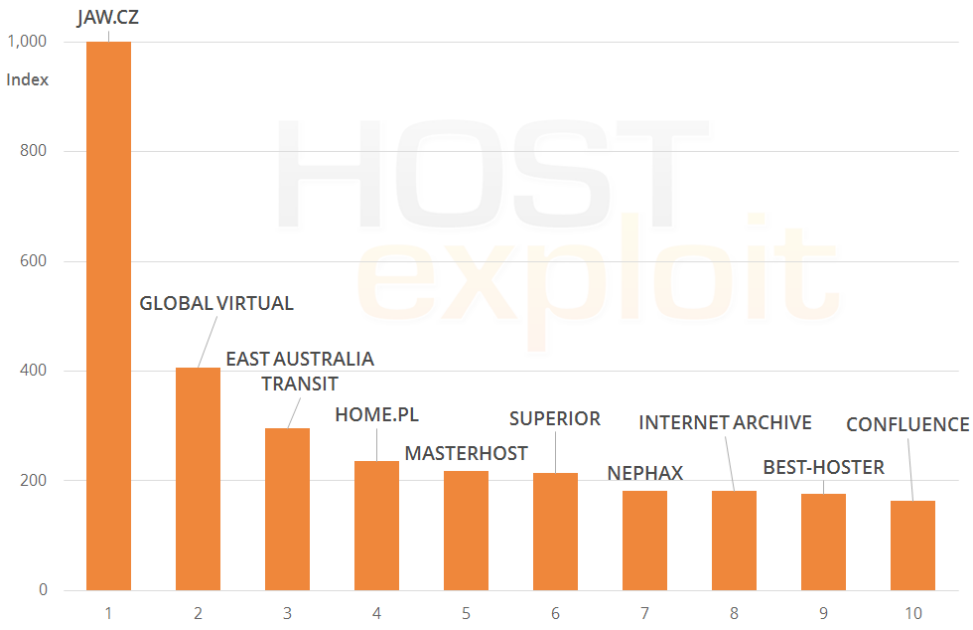


Exploits

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

Trotz eines Rückgangs im Gesamtindex von Platz 2 auf Platz 7, ist Confluence Networks in der Kategorie Exploits in die Top 10 gerutscht. Die Anzahl der auf JAW.cz entdeckten Exploits hat stark zugenommen, wodurch auch der Index von 109.3 auf das Maximum von 1.000 geschnellt ist. Diese Veränderung allein war ausreichend für den Anstieg von Platz 4758 auf Platz 73.

Home.pl bleibt weiterhin in den Top 10 der Exploit-Kategorie und zusammen mit einem Anstieg in den Kategorien Phishing und Badware erreicht es insgesamt Platz 22.



Wußten Sie schon?

Exploits und dazugehörige Webseiten sind das Schlüsselelement der Cyberkriminalität, da sie oftmals den ersten Angriffspunkt zum Eindringen in den Rechner des Opfers bilden.

Exploits nutzen Softwareschwachstellen aus, die nicht unbedingt öffentlich bekannt sind. Der Exploit kann dann anderen Schadcode verwenden, um dem Opfer zu schaden oder die Kontrolle über den Rechner zu übernehmen.

In Zahlen

Die Top 10 dieser Kategorie beinhalten mehr als 29% aller Exploits, die im Berichtszeitraum entdeckt wurden.

Wußten Sie schon?

Badware läßt grundsätzlich außer Acht wie der Nutzer seinen Computer benutzen möchte. In diese Kategorie gehören Spyware, Rogueware und andere Arten betrügerischer Software. Sie tarnt sich häufig als kostenloser Bildschirmschoner, der heimlich Werbung anzeigt, den Browser umleitet und Keylogger installiert, um persönliche Daten zu Dritten weiterzuleiten.

In Zahlen

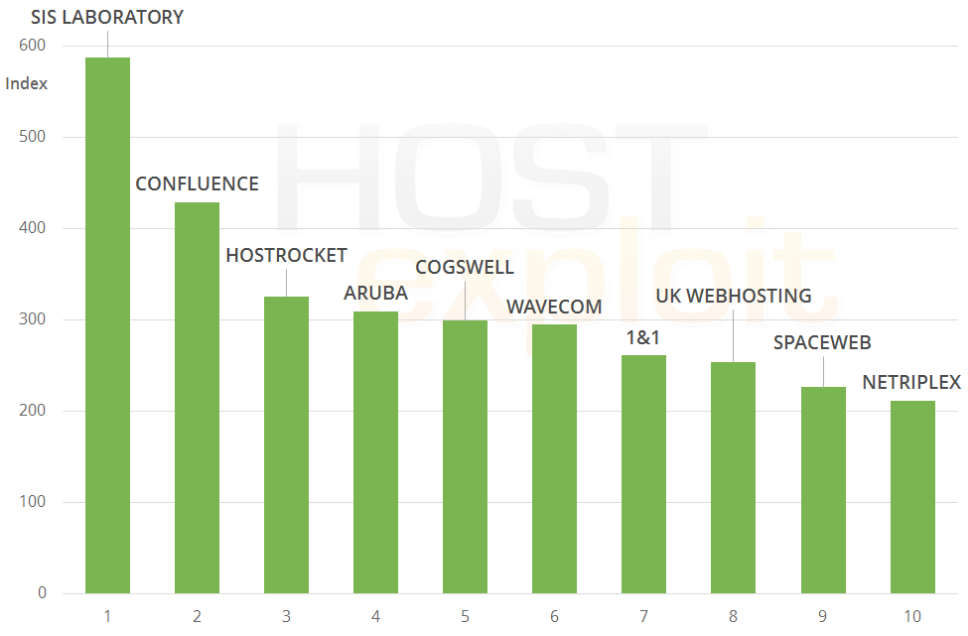
Die absolute Anzahl ging um 65 % im Vergleich zum vorangegangenen Quartal zurück. Dies kann vor allem durch das Ende der Urlaubssaison erklärt werden.

Badware

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

Alle ASe in den Top 10 dieses Quartals sind im Vergleich zum letzten neu, woraus zu schließen ist, dass es auf diesem Gebiet schnelle Veränderungen gibt. Teil der Erklärung ist, das Badware oftmals mit Kampagnen verknüpft wird und es daher anfällig ist für kurzfristige Trends – zum Beispiel während Feiertagen wenn Spam-E-Mails effizienter sind.

Die Hälfte der Hosts in der Top 10 sind auch in der Top 100 für Phishing und infizierte Webseiten vertreten – diese Verknüpfung besteht aufgrund der ähnlichen Anforderungen für all diese Sektoren.



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)*