Septiembre 2013

Informe Mundial sobre los Hosts

de HostExploit

Resumen

Por primera vez, los hosts registrados en un solo país - Estados Unidos - ocupan los tres peores lugares en la lista Top 50 de los hosts y de las redes.

Examinar las prácticas y las normas de hosting es tan relevante como siempre en la búsqueda de mejoras muy necesarias en un sistema que tiene pocas restricciones aplicables.

La cuantificación a través de los niveles de medida de la actividad cibernética criminal en servidores a través del mundo es una forma de lograr este objetivo. Desde 2009, El Informe Hosts Mundial de HostExploit (antes llamado Top 50 Bad Hosts) ha estado examinando todos los 44,000 + Sistemas Autónomos públicos en el mundo, recopilando datos sobre los sitios web infectados, botnets, spam y otras actividades, antes de combinar la investigación con fuentes confiables de la comunidad, para llegar a un análisis fiable de los resultados.

El informe es una lectura altamente interesante para los proveedores de servicios, profesionales de seguridad, webmasters y responsables de las políticas por igual. En su mayor parte, se deja al lector sacar sus propias conclusiones, ya que los números hablan por sí solos. Sin embargo, hay que subrayar que el contenido más dañino no es alojado a sabiendas - a menudo es el resultado de la inacción, y en ocasiones los hosts pueden ser las víctimas.

Sin embargo, sigue siendo cierto que todos los delitos informáticos, ataques cibernéticos, y la maldad de Internet están instalados por alguien y vienen de alguna parte, es decir, se encuentran en un host y son asignados a un ASN. Así que tiene sentido que aquí es donde debemos empezar en la búsqueda continua de soluciones.

- Jart Armin

ISBN 978-0-9836249-6-7

Datos comparativos

AA419

Abuse.CH

Clean-MX.DE

Cyscon SIRT

Emerging Threats

Google Safe Browsing

Group-IB

HostExploit

hpHosts

ISC

KnujOn

MalwareDomains

MalwareDomainList

RashBL

Robtex

Shadowserver

SiteVet

Spamhaus

SRI International

StopBadware

SudoSecure

Team Cymru

The Measurement Factory

UCE-Protect

Editor

Jart Armin

Revisores

Dr. Bob Bruen

Raoul Chiesa

Peter Kruse

Andre' DiMino

Thorsten Kraft

Andrey Komarov

Godert Jan van Manen

Steven Dondorp

Edgardo Montes de Oca

Colaboradores

Steve Burn

Greg Feezel

Andrew Fields

David Glosser

Niels Groeneveld

Matthias Simonis

Will Rogofsky

Philip Stranger

Bryn Thompson

DeepEnd Research

En asociación con ECYFED

ECYFED
European Cyber Security Federation

GROUP IB

CSIS

NORTHWAVE

cyscon

SITEVET

montimage

Socios del proyecto ACDC

ACDC
the Advanced Cyber Defence Centre

Participe!

Si le gusta lo que hacemos y quiere participar, por qué no convertirse en un patrocinador de HostExploit o socio?

Estamos continuamente buscando mejorar lo que hacemos, ampliando nuestro alcance.

Si usted cree que puede ser de ayuda, nos encantaría saber de usted. Póngase en contacto via contact@hostexploit.com

Editorial

Por primera vez, los hosts registrados en un solo país - Estados Unidos - ocupan los tres peores lugares de la lista Top 50 de hosts y redes.

Los tres hosts son AS33182 HostDime.com, AS26347 DreamHost, y AS11042 Landis Holdings. El informe, que abarca el segundo trimestre del 2013, clasifica los hosts por las concentraciones observadas más altas de actividad maliciosa, como malware, spam y botnets.

Esto, por supuesto, no es un record del que se puede estar orgulloso. Durante un largo período de tiempo, las fuentes reconocidas han advertido de los altos niveles de actividad maliciosa que se encuentran en los Estados Unidos, en particular en lo relativo a phishing[1,2].

Cuales son las causas de esto? Las principales razones son:

- Hosting abundante y barato.
- **Más integración con los servicios de anonimato.** La mayoría de los registradores de dominios y los servicios de alojamiento web ofrecen servicios 'whois proxy', y el aumento de las opciones de compra a través de Bitcoin.
- **Reputación mejorada.** Menos probabilidades de ser bloqueados por país, y un aspecto más respetable para las estafas de tipo phishing.

Sin embargo, no todas las noticias son malas para los Estados Unidos – las estadísticas por país muestran una movimiento hacia abajo en el ranking del número 9 al número 5. Excepcionalmente buenas actuaciones individuales de los anteriores hosts de ranking alto (incluyendo AS21740 eNom, de ranking 1150, y AS33626 Oversee, de ranking 943) contribuyen en mejorar el estatus.

Así que la primordial buena noticia es que es posible limpiar los hosts. Pero, ¿qué incentivos existen para hacerlo?

Por el momento, legalmente, hay muy pocos incentivos, la acción transfronteriza es notoriamente compleja y los derechos de los consumidores varían de un país a otro, si es que existen. En los EE.UU., por ejemplo, los ISP están resistiendo a los intentos de la FCC para introducir estándares de la industria y obligaciones que podrían abrir la puerta a la imposición de sanciones financieras cuando no se protegen los consumidores.

Pero incluso sin penas pecuniarias, tiene sentido que un host cumpla con las buenas prácticas y de hacer todo lo posible para mantenerse limpio. Los beneficios son múltiples - es mejor para los negocios, para la economía y para la seguridad nacional.

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

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

Metodología

En diciembre de 2009, se introdujo el índice HE como una representación numérica de la "maldad" de un Sistema Autónomo (AS). Aunque por lo general bien recibido por la comunidad, hemos recibido desde entonces muchas preguntas constructivas, algunas de las cuales vamos a tratar de responder aquí.

¿Por qué la lista no muestra la maldad absoluta en lugar de maldad proporcional?

Una característica central del índice es que se pondera por el tamaño del espacio de direcciones asignado del AS, y por esta razón no representa la mala actividad total que tiene lugar en el AS. Estadísticas de la maldad total sería, sin duda, útil para los webmasters y administradores de sistemas que desean limitar el tráfico de enrutamiento propio. Pero el índice HE pretende destacar la negligencia de seguridad entre muchos de los proveedores de alojamiento de Internet del mundo, que incluye la aplicación no rigorosa de los reguladores de abusos.

¿No son las organizaciones más grandes que deberían encargarse de volver a invertir los beneficios para obtener una mejor regulación de seguridad?

El índice da mayor peso a los sistemas autónomos con pequeños espacios de direcciones, pero esta relación no es lineal. Hemos utilizado un "factor de incertidumbre" o factor bayesiano para modelar esta responsabilidad, lo que aumenta las cifras de los espacios de direcciones mayores. En el presente informe, el tamaño crítico del espacio de direcciones ha aumentado de 10.000 a 20.000 para acentuar aún más este efecto.

Si estas cifras no están destinadas para los webmasters, ¿para quién están destinadas?

Los informes son lectura recomendada para los webmasters que quieren obtener una comprensión fundamental de lo que está sucediendo en el mundo de la seguridad de la información más allá de su vida cotidiana. Nuestro principal objetivo, sin embargo, es de dar a conocer el origen de los problemas de seguridad. El Índice HE cuantifica el grado en que las organizaciones permiten que ocurran actividades ilegales - o, más bien, no hacer lo necesario para impedirlas.

¿Por qué los hosts permiten esta actividad?

Es importante señalar que al publicar de estos resultados, HostExploit no afirma que los proveedores de alojamiento toleran la actividad ilícita llevada a cabo en sus servidores. Es importante tener en cuenta que muchos hosts son también víctimas de la delincuencia informática.

Descargo de responsabilidad

Se han realizado todos los esfuerzos razonables para asegurar que los datos de origen de este informe son actualizados, exactos, completos y exhaustivos en el momento del análisis. Sin embargo, los informes no son presentados como estar libre de errores y los datos que utilizamos pueden ser objeto de actualización y corrección sin previo aviso.

HostExploit o cualquiera de sus socios, incluyendo CyberDefcon, Grupo IB y el CSIS no son responsables de los datos falseados, malinterpretados o alterados de la manera que sea. Conclusiones derivadas y análisis generados a partir de estos datos no son para ser considerado atribuible a HostExploit o para nuestros socios de la comunidad.

Se ruega contactar CyberDefcon para el uso de este informe.

Definiciones

IPs

A lo largo del informe, el campo "IPs" se refiere al número de direcciones IPv4 de origen asignado a la AS. En el contexto de los países, es la suma de los "IPs" para cada AS en ese país.

País

En general, un AS es físicamente rutado a través de múltiples países. En este caso, HostExploit determina el país más importante de origen de los sistemas autónomos basándose en sus lugares de enrutamiento y datos de registro.

Índice HE

La métrica cuantitativa usada por HostExploit representa la concentración de la actividad maliciosa servida a partir de un Sistema Autónomo.

Ranking HE

Ranking con respecto a todo los 44,556 ASes.

Por favor consulte el Glosario para más definiciones.

Top 50 Hosts

Una lista de los 50 ASes con el índice HE más alto, es decir, la más alta concentración de actividad maliciosa.

Sistema Autónomo (AS)

Una colección lógica de rutas Internet controlad por una organización o un ISP.

ASN

Un número único asignado a un AS.

Índice HE

La métrica cuantitativa usada por HostExploit representa la concentración de la actividad maliciosa servida a partir de un Sistema Autónomo.

Ranking HE

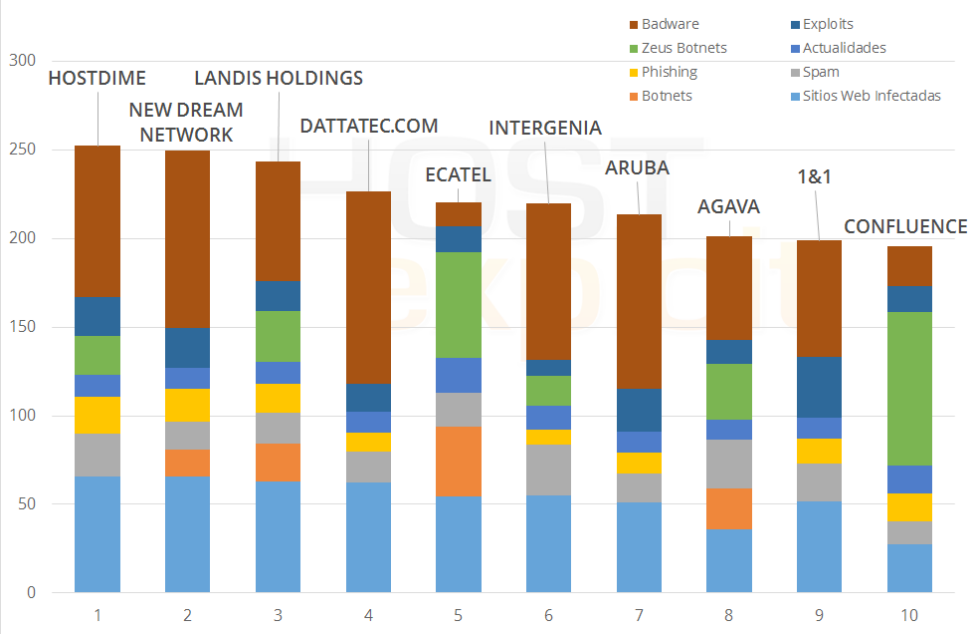
Ranking con respecto a todo los 44,556 ASes.

IPs

El número de direcciones Internet asignadas a un AS.

Ranking	Índice HE	ASN	Nombra	País	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

Top 10 Descomposición Visual



¿Qué es esto?

El gráfico de la izquierda muestra una representación visual del aporte que está haciendo cada sector al índice de un AS.

Este grafico le permite ver rápidamente donde un host debería poner el mayor esfuerzo para mejorarse.

Top 10 Recientemente Registrados

Los 10 ASes que siguen tienen los índices más altos con respecto a los 2,058 ASes registrados desde el último informe. Potencialmente, estos ASes serán interesantes de analizar en el futuro.

Ranking	Índice HE	ASN	Nombra	País	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

El numero de ASes

En el informe de Marzo 2013
43,454

En este informe
44,556

Nuevos ASes
2,058

Eliminados
956

Aumento neto
1,102

¿Qué es esto?

Calculamos el índice de cada país usando los mismos métodos usados para los ASes individualmente.

El Índice por País indica el nivel de maldad sobre 1000, sin considerar demasiado el número de hosts en el país en cuestión.

La tabla a la derecha muestra los 10 principales países que resultan de la aplicación de esta metodología, junto con los tres sectores con los mayores índices.

Top 10 Países

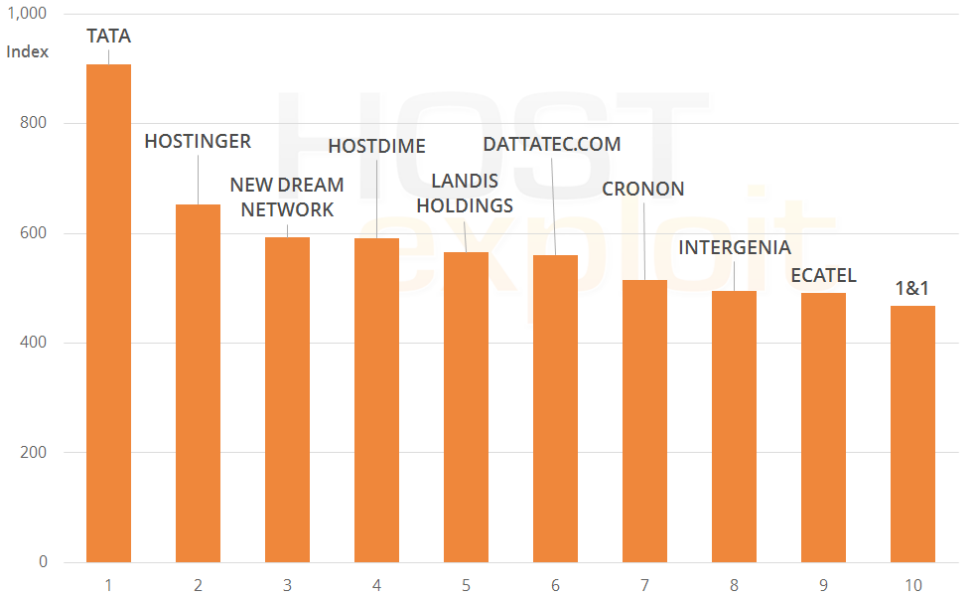
País	Nombra	ASes	IPs	Rank	Índice
VG	VIRGIN ISLANDS, BRITISH	6	18,688	1	435.5
	#1 sector	Sitios Web Infectados		1	905.3
	#2 sector	Botnet C&Cs		1	889.0
	#3 sector	Actualidades		1	823.9
PL	POLAND	1,590	21,932,032	3	306.7
	#1 sector	Actualidades		3	666.7
	#2 sector	Phishing		2	648.1
	#3 sector	Zeus botnets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

Sitios Web Infectados

Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
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

Todos los 3 primeros con índice HE global alto obtienen una puntuación alta en esta categoría con AS26347 DreamHost en posición No. 3, AS33182 HostDime en No. 4 y AS11042 Landis en No. 5.

El Host número 1 en esta categoría, AS132524 Tata fué recientemente registrado en India con un bajo número de IPs. Esto podría querer decir que se utiliza para servicios temporales o que es un "ASN descartable".



¿Sabía usted?

Los top 7 host en la clasificación global aparecen en esta lista.

Los números

AS132524 Tata está en la posición número 8 de los sitios web infectados dentro de este Top 10, pero es una entidad mucho menor, lo que lo empuja a la posición superior.

¿Sabía usted?

Sotal-Interactive y ISPsystem son principalmente alojados en Rusia, pero han registrado respectivamente en Ucrania y Luxemburgo.

Botnet C&Cs

Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
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

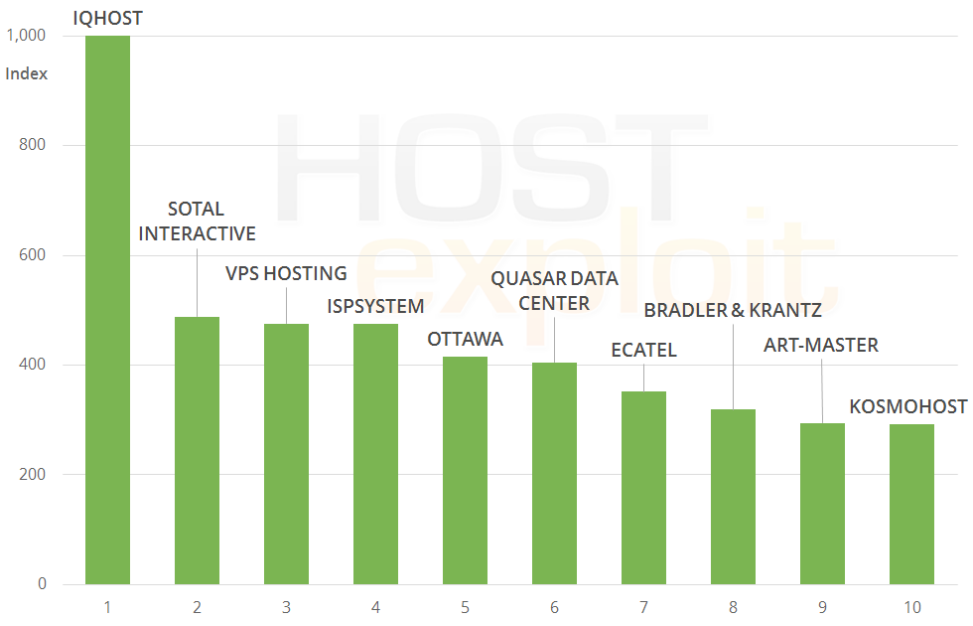
Ninguno de los 4 host con más alto ranking de esta categoría han cambiado desde el informe del primer trimestre de 2013.

De hecho, AS50465 IQHost ha ocupado la primera posición desde el segundo trimestre de 2012. Eso hace que está en posición número 1 desde más de un año como alojador de botnet C&Cs.

Los números

124 botnet C&Cs fueron observados durante este periodo, por debajo de los 132 en el último informe.

Esto es menor que el número total de incidencias en cualquier otra categoría. Sin embargo, el poder de cada uno de los C&C se mantiene y pone en evidencia su importancia desde una perspectiva de seguridad.

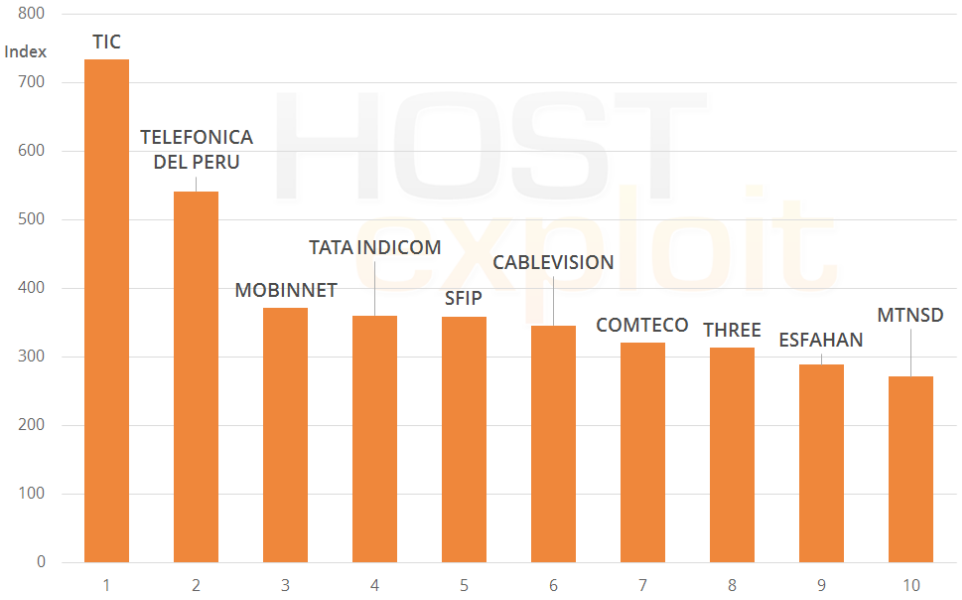


Spam

Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
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

Las primeras posiciones en esta categoría siguen la tendencia observada en los informes anteriores. Los spammers siguen prefiriendo los países con los niveles más bajos de reglamentaciones y barreras para el registro en los AS.

Ocho de los 10 principales hosts se ajustan a esta descripción, con Irán, Perú, México, India y Bolivia representados aquí. Excepciones se observan con AS57879 SFIP, registrado en Alemania, y AS45727 Three, que aunque fue registrado en Indonesia, está actuando desde Estados Unidos.



¿Qué hacemos?

Para esta categoría, se examinan los servidores de spam tradicionales, así como los robots de spam, rastreadores y la reputación IP impulsados por la comunidad.

¿Sabía usted?

Proveedor de telecomunicaciones de Rusia, MegaFon, ha salido del Top 10, después de haber tenido simultáneamente un total de cuatro ASes en el Top 10 Spam en 2012.

Los números

Más de 100,000 fuentes de Spam fueron examinados durante el período.

¿Sabía usted?

Cisco estima que en 2012 unos 100 millones de dólares se perdieron en los ataques de phishing; pérdidas sufridas tanto por las empresas que los consumidores.

Los números

779 campañas de phishing fueron examinadas durante el período de este informe.

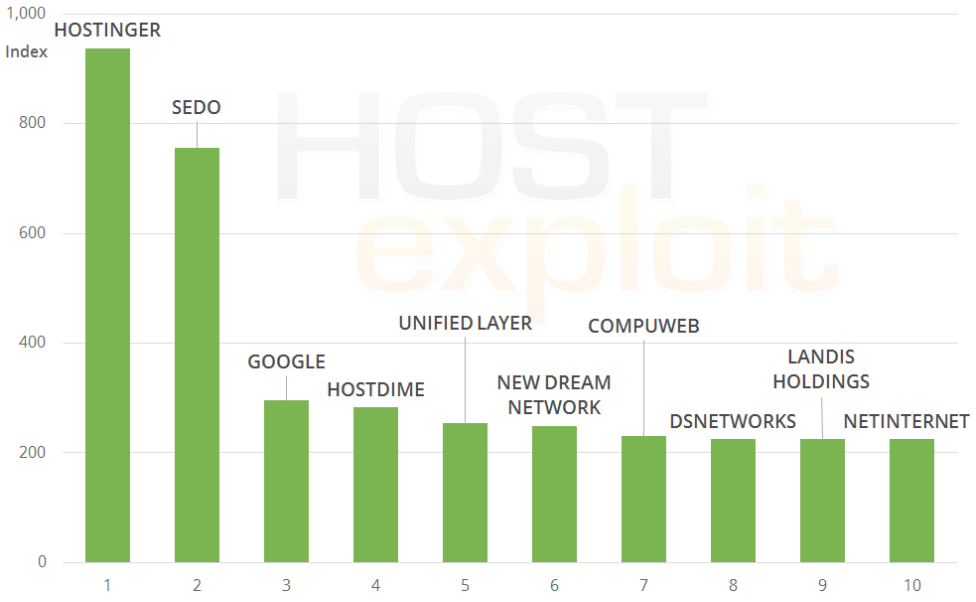
Phishing

Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
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

Las principales empresas de alojamiento web en países con regulaciones más estrictas dominan los 10 primeros puestos de esta categoría, entre ellos los tres hosts identificados como los peores en los últimos informes.

En este sector las cosas cambian rápidamente, phishers prefieren la facilidad y disponibilidad de hospedaje en las regiones establecidas. Dado que los sitios de phishing son de corta duración, no se necesitan garantías de tiempo de actividad y por lo tanto no es necesario alojarse en regiones con menos regulaciones.

Además, la aparente más alta legitimidad de un sitio de un banco o de comercio electrónico alojado desde los Estados Unidos o el Reino Unido es beneficioso para una estafa de tipo phishing.

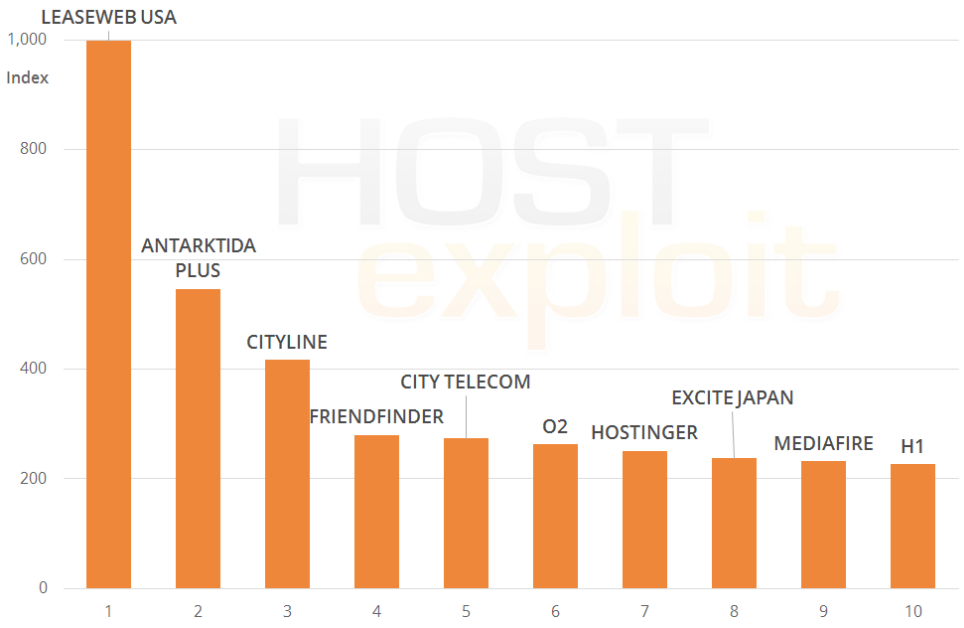


Actualidades

Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
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

Otra vez AS51699 Antarktida obtiene un ranking alto en esta categoria pero la posición número 1 es para AS30633 Leaseweb USA.

Como su nombre indica, Actualidades es un sector en rápida evolución, que se traduce en una gran variedad de hosts que se utilizan para albergar nuevos tipos de contenido malicioso, e implica grandes movimientos de mes a mes.



¿Sabía usted?

Actualidades es una métrica propia de HostExploit que capta los vectores de ataque más actuales y que más cambian al nivel mundial.

Aquí esta incluidos variantes recientes de ataques MALfi (XSS/ RCE/RFI/LFI), técnicas de clickjacking, y grandes botnets.

Los números

Después de una diminución en el número de casos observados en el informe anterior, el número ha subido otra vez al 67%.

¿Sabía usted?

Zeus, un tipo de botnet transmitido a través de una carga útil Troyana. Es una de las variedades más populares de botnet, que hace 6 años ganó popularidad en el ámbito cibernético criminal.

Zeus ha sido continuamente mejorado, hábilmente eludiendo los sistemas de seguridad con sus muchas variaciones y coleccionando grandes redes de máquinas zombis (bots).

Los números

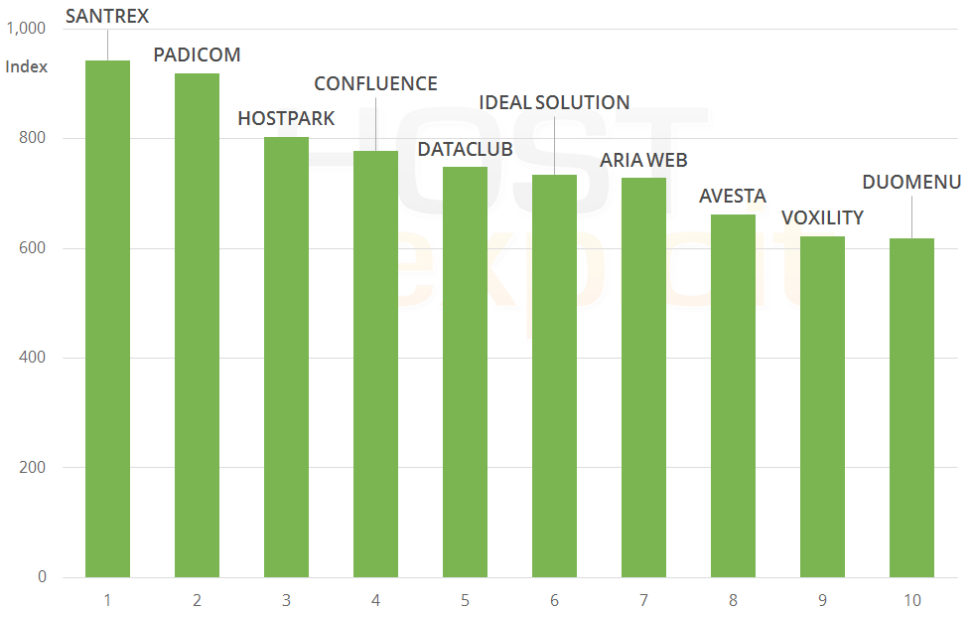
El número total de servidores Zeus observados se ha mantenido casi constante. Esto sugiere que Zeus sigue siendo un exitoso y rentable conjunto de herramientas de redes de bots.

Zeus Botnets

Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
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

La primera posición aquí fue obtenida por AS57668 Santrex. Este resultado está relacionado con la primera posición en el primer trimestre, ya que también se dirige a través de las islas Seychelles.

En el informe anterior, la primera posición fue obtenida por AS58001 Ideal Solution, que ahora es No. 5. Notar que Esta registrada en las Seychelles pero rutada vía la Federación Rusa.

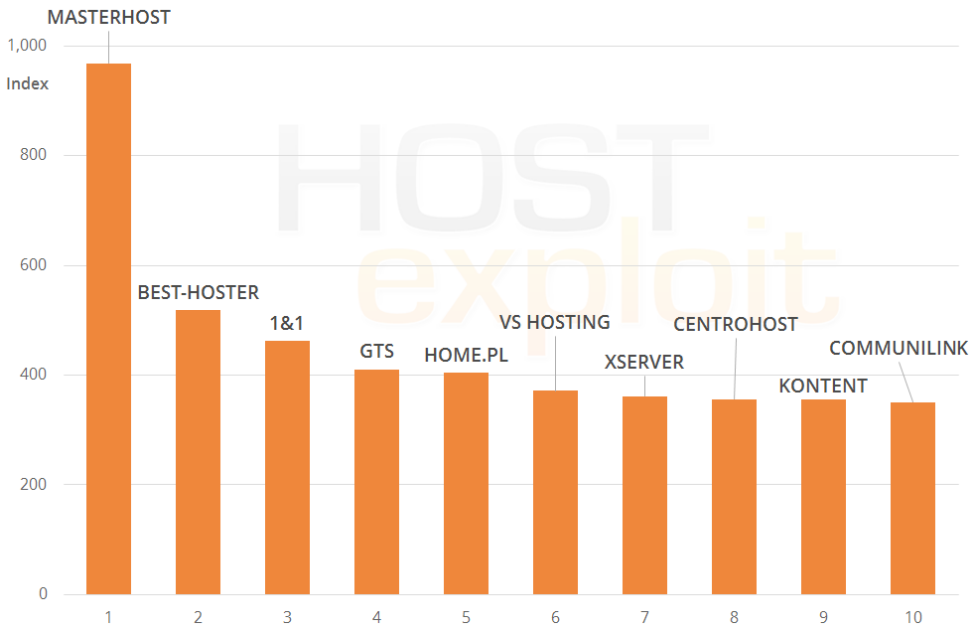


Exploits

Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
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

Esta categoría incluye hosts que ya fueron observados en informes anteriores: AS25532 Masterhost y AS49693 Best-Hoster.

Pero la mayoría de los hosts incluidos aquí son nuevos para el sector.



¿Sabía usted?

Exploits y los sitios web que les sirven son una pieza clave para el cibercrimen, ya que a menudo proporcionan el primer punto de entrada que permite de atacar el ordenador de la víctima.

Exploits aprovechan las vulnerabilidades del software, que puede ser o no ser de conocimiento público. El exploit puede usar otro código que daña directamente el sistema de la víctima, o que sólo es usado por el atacante como una carga útil para tomar el control inicial de una máquina.

Los números

El Top 10 ASes en esta categoría representa más del 16% de todos los exploits observados durante el periodo de este informe. Es una diminución con respecto al 29% del informe anterior.

¿Sabía usted?

Badware fundamentalmente ignora cómo los usuarios se proponen usar su propio equipo. Ejemplos de este tipo de software incluyen software espía, tipos de malware, rougues y adware engañoso. Por lo común, se presenta en forma de protectores de pantalla gratuitos que subrepticiamente generan anuncios, redirecciones a páginas web inesperadas que afectan los navegadores y programas keylogger, que transmiten datos personales a terceros malintencionados.

Badware

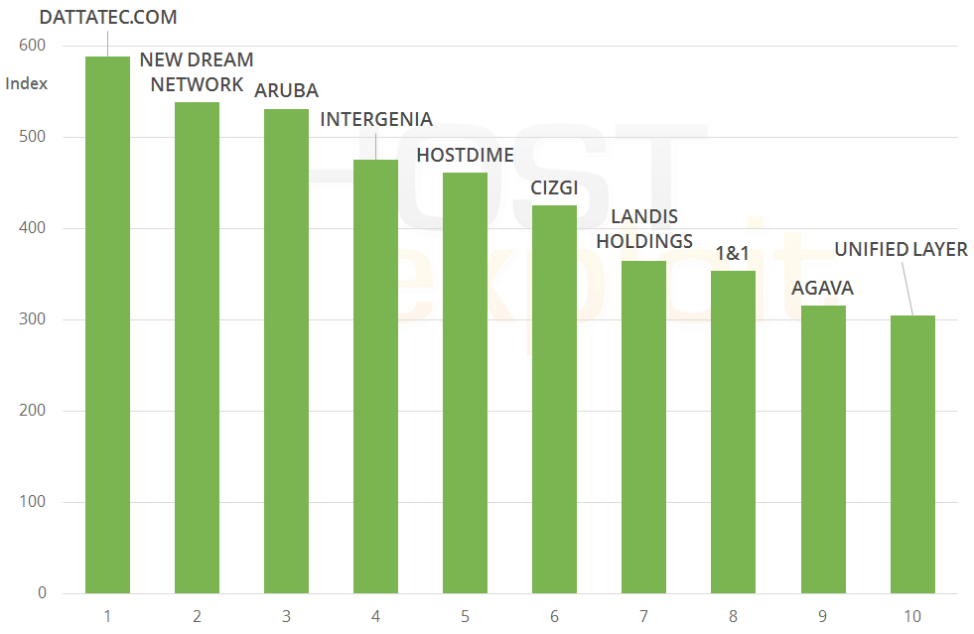
Índice	ASN	Nombra	País	IPs	Ranking	Índice HE
588.4	27823	Dattatec.com	AR	8,192	4	226.8
538.7	26347	New Dream Network, LLC	US	230,656	2	249.3
531.0	31034	Aruba S.p.A.	IT	145,664	7	213.6
475.6	8972	Intergenia AG	DE	149,760	6	219.6
461.2	33182	HostDime.com, Inc.	US	63,232	1	252.3
425.0	34619	Cizgi Telekomunikasyon	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

En este sector que cambia rápidamente, sólo dos hosts siguen siendo los mismos que en el primer trimestre, AS31034 Aruba y AS8560 1&1 Internet. Badware es sensible a las tendencias a corto plazo y los hosts de esta categoría cambian con frecuencia.

Nuestro tres peores hosts en los Top 10 generales también tienen un lugar destacado en esta categoría, que también implica un ranking alto en las categorías de phishing y de los sitios web infectados. Esto sugiere que los hosts responden a requerimientos similares para servir a este tipo de actividades maliciosas.

Los números

Los Top 10 hosts en esta categoría representan un 23% de los casos totales de badware observados.



AS (Sistema Autónomo)

Un AS es una unidad de la política de ruteo, ya sea una sola red o de un grupo de redes que es controlado por un administrador de red común, en nombre de una entidad tal como una universidad, una empresa o proveedor de servicios de Internet. Un AS también se refiere a veces como un dominio de enrutamiento. Cada sistema autónomo se le asigna un número único a nivel mundial llamado un Número de Sistema Autónomo (ASN).

Badware

Badware o Software Maligno es software que actúa sobre un equipo de un usuario de manera no deseada por el. Los tipos de badware son spyware, malware, adware engañoso. Ejemplos comúnmente encontrados de badware incluyen protectores de pantalla gratuitos que subrepticiamente generan anuncios, barras de herramientas maliciosos de navegadores web que lo envían a páginas diferentes que las que uno espera, y programas de keylogger que puede transmitir sus datos personales a terceros malintencionados.

Blacklists

En informática, una blacklist (o lista negra) es un mecanismo de control de acceso básico que permite el acceso salvo a las personas en la lista, similar a lo que suele de hacerse en las discotecas. Por otro lado una whitelist (o lista blanca) es equivalente a la discoteca VIP donde no se permitir la entrada a nadie, excepto a los miembros de la lista. Como una especie de término medio, una graylist (o lista gris) contiene entradas que están bloqueadas temporalmente o permitidas temporalmente. Elementos de la lista gris pueden ser modificados o verificados para su inclusión en una lista negra o lista blanca. Algunas comunidades y webmasters publican sus listas negras para el uso del público en general, como Spamhaus y Emerging Threats.

Botnet

Botnet es un término que identifica un conjunto de robots informáticos o bots, que se gestiona de forma autónoma y automática. El término se asocia sobre todo con software malicioso utilizado por los ciberdelincuentes, pero también puede referirse a la red de ordenadores infectados con software de computación distribuida.

Actualidades

Los más actuales exploits que estan rápidamente cambiando y vectores de ataque. Técnicas delictivas dentro de esta categoría incluyen Malfi (XSS / RCE / RFI / LFI), los ataques XSS, clickjacking, empresas farmacéuticas falsificadas, rogue AV, Zeus (Zbota), Artro, SpyEye, Ice9, Stuxnet, DuQu, BlackHat SEO, así como la los kits de exploit más recientes.

CSRF (cross site request forgery)

Cross Site Request Forgery o falsificación de petición en sitios cruzados, también conocido como "ataques de un click" o "session riding", es un enlace o un script en una página web basada en tokens de usuario autenticados.

DDOS (Distributed Denial of Service)

Ataques de tipo Distributed Denial of Service o Ataque distribuido de denegación de servicio pueden ejecutarse en una variedad de maneras. El efecto deseado es interrumpir la actividad normal de un servicio web. Los atacantes utilizan el poder de múltiples sistemas informáticos, a través de una red de bots, o vía un gran número de usuarios, para provocar una caída de un sistema dado. Otro método de ataque es por amplificación utilizando múltiples peticiones DNS a través de resoluciones abiertas (« open resolvers »).

DNS (Domain Name System)

Domain Name System o Sistema de Nombres de Dominio asocia información variada con nombres de dominio y, más importante todavía, sirve de "guía telefónica" para el Internet mediante la traducción de nombres de host informáticos legibles por humanos, por ejemplo, www.example.com en direcciones IP como 208.77.188.166, que los equipos de red usan para obtener o entregar información. Un DNS también almacena otros datos, como la lista de los servidores de correo que aceptan correo electrónico para un dominio dado, proporcionando un servicio de redirección basada en palabras clave en todo el mundo.

DNS Security Extensions (DNSSEC)

Un conjunto de extensiones DNS que autentican el origen a nivel de DNS y comprueba la integridad de datos DNS. Se requiere la implementación a nivel de registro para la protección más eficaz.

DNSBL

Domain Name System Block List es una lista opcional de los rangos de direcciones IP o zona DNS normalmente aplicados por los proveedores de servicios de Internet (ISP) para impedir el acceso a spam o software maligno. Un DNSBL de nombre de dominios es frecuentemente referido como URIBL, Uniform Resource Indentifier Block List.

Exploit

Un exploit es una pieza de software, un fragmento de datos, o una secuencia de comandos que se aprovechan de un error, fallo o vulnerabilidad con el fin de provocar un comportamiento irregular que se produce en los programas informáticos, hardware, o algún aparato electrónico. Esto incluye con frecuencia cosas como obtener violentamente el control de un sistema informático o permitir la escalada de privilegios o una denegación de servicio.

Hosting

Por lo general, se refiere a un ordenador (o una red de servidores) que almacena los archivos de un sitio web, donde también está instalado software de servidor web que se ejecuta en él y que está conectado a Internet. El sitio entonces se dice que está hosted o alojado.

IANA (Internet Assigned Numbers Authority)

IANA es responsable de la coordinación global del DNS Root, direccionamiento IP y otros recursos de protocolo de Internet. Coordina la IP global y espacio de números AS, asignando éstos a los Registros Regionales de Internet.

ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN es responsable de la gestión de los espacios de direcciones del protocolo de Internet (IPv4 e IPv6) y la asignación de bloques de direcciones a los Registros Regionales de Internet, para el mantenimiento de registros de los identificadores de protocolo de Internet, y para la gestión del primer nivel de nombres de dominio (zona DNS Root) que incluye la operación de servidores de nombres root.

IP (Internet Protocol)

IP es el protocolo principal de la capa de Internet del conjunto de protocolos de Internet y tiene la tarea de entregar paquetes de datos desde el host de origen al host de destino basándose únicamente en su dirección.

IPv4

IP Protocolo del Internet versión 4 (IPv4) es la cuarta revisión en el desarrollo del protocolo. IPV4 utiliza direcciones de 32 bits (cuatro bytes), que limita el espacio de direcciones a 4,3 mil millones de posibles direcciones únicas. Sin embargo, algunos están reservados para usos especiales como redes privadas (18 millones) o las direcciones de multidifusión (270 millones).

IPv6

Protocolo de Internet versión 6 (IPv6)

es una versión del protocolo que está diseñado para tener suceder IPv4. IPv6 utiliza direcciones de 128 bits, o sea que el espacio de direcciones IPv6 soporta alrededor de 2 ^ 128 direcciones.

ISP (Internet Service Provider)

Internet Service Provider o Proveedor de servicios de Internet es una empresa u organización que tiene el equipo y el acceso público para proporcionar conectividad a Internet a los usuarios, es decir, mensajes de correo electrónico, servidores de sitio web, almacenamiento de ficheros accesibles por la red....

LFI (Local File Inclusion)

LFI o Inclusión de Archivos Locales es una vulnerabilidad que permite el uso de un archivo dentro de una base de datos para explotar la funcionalidad del servidor. También para el craqueo de funciones cifrados dentro de un servidor, por ejemplo, contraseñas MD5, etc. LFI es similar a una vulnerabilidad Remote File Inclusion excepto que en lugar de incluir archivos remotos, sólo los archivos locales, es decir los archivos en el servidor actual se pueden incluir.

MALfi (Malicious File Inclusion)

Una combinación de RFI (inclusión de archivos remotos), LFI (inclusión de archivo locales), XSA (ataque al servidor de cruzado), y RCE (ejecución remota de código).

Malicious Links

Malicious Links o Enlaces Maliciosos son enlaces que se plantan en un sitio para enviar deliberadamente a un visitante a un sitio malicioso, por ejemplo, un sitio con el cual se plantará un virus, spyware o cualquier otro tipo de malware en un equipo, como un sistema de seguridad falso. Estos no siempre son evidentes, ya que se pueden esconder en funcionalidades del sitio o ser enmascarados para desorientar al visitante.

MX

Un servidor de correo o un ordenador / servidor en rack que tiene y puede enviar e-mail de un cliente.

NS (Name Server)

Cada nombre de dominio debe tener un servidor de nombres primario (por ejemplo ns1.xyz.com), y al menos un servidor de nombres secundario (ns2.xyz.com, etc.). Este requisito tiene como objetivo hacer que el dominio sigue estando accesible incluso si un servidor de nombres se convierte en inaccesible.

Open Source Security

El término se aplica comúnmente para el código fuente del software o datos, que se pone a disposición del público en general con restricciones de propiedad intelectual relajadas o inexistentes. Por Seguridad del código abierto se refiere a que el código desarrollado por el esfuerzos incremental individuales o mediante la colaboración es frecuentemente mejor testeado, puede fácilmente ser analizado (parque uno tiene acceso al código fuente) y es constantemente corregido para eliminar vulnerabilidades por una comunidad posiblemente importante.

Pharming

Pharming es un ataque donde los hackers pretenden redirigir el tráfico de un sitio web a otro sitio web, como ladrones de ganado que dirijen las vacas hacia una dirección equivocada. El sitio web de destino suele ser falso.

Phishing

El phishing es un tipo de engaño diseñado para robar los datos personales de un usuario, como números de tarjetas de crédito, contraseñas, información de cuentas u otra información. El phishing se realiza típicamente mediante un e-mail (donde la comunicación parece venir de un sitio web de confianza) o un mensaje instantáneo; el contacto telefónico también se utiliza.

Registry

Un operador de registro genera los archivos de zona, que convierten los nombres de dominio en direcciones IP. Registros de nombres de dominio, como VeriSign, para .com., .info. Dominios de nivel superior de código de país (ccTLD) se delegan en los registros nacionales como Nominet en el Reino Unido .uk, "Centro de Coordinación para TLD .ru" para .ru y .рФ.

Registrars

Un registrador de nombres de dominio es una empresa con la autoridad para registrar nombres de dominio, autorizados por la ICANN.

Remote File Inclusion (RFI)

Una técnica a menudo utilizada para atacar sitios web de Internet desde un equipo remoto. Se puede combinar con el uso de XSA para dañar un servidor Web.

Rogue Software

Software de seguridad falso o "rogue" es un software que utiliza el malware (software malicioso) o herramientas maliciosas para hacer publicidad o para obligar a los usuarios de computadoras para pagar por la eliminación de spyware inexistente. Rogue software a menudo instala un troyano para descargar una versión de prueba, o se ejecuta otras acciones no deseadas.

Rootkit

Un conjunto de herramientas de software utilizadas por un atacante que ha obtenido acceso a un sistema informático con el fin de ocultar al usuario la alteración de archivos o procesos.

Sandnet

Un SandNet es un entorno serrado en un equipo físico en el que el malware puede ser monitoreado y estudiado. Emula el Internet de una manera que el malware no puede detectar que se está siendo supervisando. Es una manera maravillosa para analizar como funciona un malware identificado. Una Honeynet es el mismo tipo de concepto, pero más dirigido a los propios atacantes, el seguimiento de los métodos y el estudio de los motivos de los atacantes.

Spam

El Spam es el término utilizado para correo electrónico no solicitado. El spam es correo basura a gran escala y por lo general se envía indiscriminadamente a cientos o incluso cientos de miles de buzones de forma simultánea.

Troyano o caballo de Troya

Es un software que aparece para realizar o de hecho realiza una tarea deseada por un usuario pero que al mismo tiempo realiza tareas dañinas sin el conocimiento o consentimiento del usuario.

Worms

Worm o gusano es un programa de software malicioso que puede reproducirse y propagarse de un ordenador a otro a través de la red. La diferencia entre un gusano y un virus de computadora es que un virus informático se adjunta a un programa de ordenador para difundirse y requiere una acción por parte de un usuario, mientras que un gusano es autónomo y puede enviar copias de sí mismo a través de la red.

XSA (Cross Server Attack)

Un método de intrusión de seguridad de red que permite a una persona malintencionado poner en peligro la seguridad en un sitio web o servicio en el servidor mediante el uso de los servicios implementados en el servidor que pueden no ser seguros.

Apéndice 2

Metodología de Cálculo del Índice HE

25 de septiembre de 2013

1. Historial de revisiones

Rev.	Date	Notes
1.	Diciembre 2009	Introducción de la Metodología.
2.	Marzo 2010	Valor IP significativo aumentado de 10,000 a 20,000.
3.	Junio 2010	Fuentes refinadas. Doble conteo de Google Safebrowsing data vía StopBadware eliminado. Fuentes equilibradas.
4.	Octubre 2011	Fuentes refinadas. Fuentes equilibradas.
5.	Julio 2012	Fuentes refinadas.

Cuadro 1: Historial de Revisiones

2. Motivación

Nuestro objetivo es proporcionar un método simple y preciso de representar la historia de la maldad de un Sistema Autónomo (AS). Maldad en este contexto comprende actividades maliciosas y sospechosas del servidor, como alojamiento o propagación de malware y exploits, correos electrónicos de spam, ataques de Malfi (RFI / LFI / XSA / RCE), centros de mando y control C&C, los ataques de phishing.
A esto le llamamos el *Índice HE*; un número con un valor entre 0 (sin maldad) y 1000 (máximo de maldad). Las propiedades deseadas del Índice HE deberían incluir las siguientes propiedades:

1. Los cálculos deben proceder de múltiples fuentes de datos, cada uno representando diferentes formas de maldad, con el fin de reducir el efecto de las anomalías que pueden existir en los datos.

2. Cada cálculo debe tener en cuenta un cierto tamaño objetivo de la AS, para lo que el índice no favorezca injustamente los sistemas autónomos más pequeños.

3. Ningún AS debe tener un valor de Índice HE igual a 0, ya que no se puede afirmar con certeza que un AS tiene maldad cero, sólo que ninguno ha sido detectado.

4. Sólo un AS debe de ser capaz de tener el máximo índice HE de 1000 (si es que existe realmente uno).

3. Fuentes de Datos

Los datos se obtuvieron de las 11 fuentes que siguen.

Datos de spam de UCEPROTECT-Network y los datos de ZeuS de Abuse.ch se cruza con los de Team Cymru.

Utilizando los datos de esta amplia variedad de fuentes se obtiene la información con la propiedad No 1 deseada.

#	**Fuente**	**Datos**	**Peso**
1.	UCEPROTECT-Network	Spam IPs	Muy alto
2.	Abuse.ch	ZeuS servers	Alto
3.	Google / C-SIRT	Badware instances	Muy alto
4.	SudoSecure / HostExploit	Spam bots	Bajo
5.	Shadowserver / HostExploit / SRI	C&C servers	Alto
6.	C-SIRT / HostExploit	Phishing servers	Medio
7.	C-SIRT / HostExploit	Exploit servers	Medio
8.	C-SIRT / HostExploit	Spam servers	Bajo
9.	HostExploit	Current events	Alto
10.	hpHosts	Malware instances	Alto
11.	Clean MX / C-SIRT	Malicious URLs	Alto
12.	Clean MX	Malicious "portals"	Medio

Cuadro 2: Fuentes de Datos

Pruebas de precisión se llevaron a cabo para determinar que los coeficientes correctores aplicados aseguran que los sistemas autónomos conocidos como malos aparecen en posiciones coherentes. El valor exacto de cada ponderación dentro de un rango determinado se elige entonces siguiendo nuestros criterios, basados en una amplia comprensión de los investigadores de las implicaciones que se pueden derivar de cada fuente. Este enfoque garantiza que los resultados sean lo más objetivos posibles y realistas, limitando el aspecto subjetivo lo más posible.

4. Compensaciones Bayesianas

¿Cómo obtenemos la propiedad deseada No 2? Es decir, cómo se debe calcular el Índice HE con el fin de ponderar correctamente la diferencia de tamaño de las AS? Una idea inicial era de dividir el número de casos registrados por algún valor que represente el tamaño de la AS. El valor más obvio seria de usar el número de dominios de cada AN como el valor de ponderación del tamaño de las ASs. Pero es posible que un servidor que no tiene ningún dominio registrado sirva para llevar a cabo actividad maliciosa, como fue el caso de McColo. Por lo tanto, parece más pragmático usar el tamaño del rango de direcciones IP (es decir el número de direcciones IP) registrados en el AS a través del Registro Regional de Internet correspondiente.

Sin embargo, mediante el cálculo de la proporción entre el número de casos por cada dirección IP, casos aislados de pequeños servidores pueden producir resultados distorsionados. Consideremos el siguiente ejemplo:

Casos de spam en la muestra: 50
IPs en la muestra: 50,000
Resultado: 50 / 50,000 = 0.001
Ejemplo de casos de spam: 2
Ejemplo de IPs: 256
Resultado: 2 / 256 = 0.0078125

En este ejemplo, usando el simple cálculo de número de casos dividido por el número de direcciones IP se obtiene un valor casi ocho veces mayor que para la media. Sin embargo, sólo hay dos casos registrados de spam, pero la proporción es alta debido al bajo número de direcciones IP para este AS. Esto es un caso aislado, pero debemos acercarnos lo más posible al valor medio, más aun cuando el número de IPs es menor.

Para este propósito, utilizamos la *relación Bayesiana* de número de casos con el número de direcciones IP. Calculamos la relación bayesiano como:

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

where:
B: *proporción Bayesiana*
M: *número de IPs asignados al ASN*
M_a: *número medio de IPs asignados en conjunto simple*

N: *número de casos observados*
N_a: *número medio de casos observados en conjunto simple*
C: *ponderación IP = 20,000*

El proceso de traslado de la relación hacia la relación media tiene el efecto de que ningún AS tendrá una relación Bayesiana igual a cero, debido a un nivel de incertidumbre basado en el número de direcciones IPs. Esto cumple con los requisitos de la propiedad deseada No 3.

5. Calculo

Para cada fuente de datos, se calculan tres factores.

Para obtener una relación bayesiana a la buena escala, la dividimos por el coeficiente máximo bayesiano en el conjunto de la muestra, obteniendo el Factor C:

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

where:
B_m: *proporción Bayesiana máxima*

Pruebas de precisión se llevaron a cabo que muestran que en un número reducido de casos, el Factor C favorece demasiado los ASes pequeños. Por lo tanto, es lógico incluir un factor que usa le número de casos totales en vez de la proporción del número de casos sobre el tamaño. Esto resulta en el Factor A:

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

Este Factor es similar en forma al Factor C y debería contribuir solo muy poco en el cálculo del Índice porque favorece los pequeños ASes. Es usado solo como mecanismo de compensación del Factor C en casos particulares solamente.

Si un AS particular tiene un número de casos significativamente mayor que en cualquier otro AS de la muestra, el Factor A resultaría muy pequeño, incluso para el AS con el segundo mayor número de casos. Esto no es deseable ya que el valor de un AS distorsionaría demasiado el valor del Factor A. Por lo tanto, como mecanismo de compensación para el Factor A (la proporción entre el número promedio de casos) usamos el Factor B como proporción de los casos máximos menos los casos medios:

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

donde:
N_m: *número máximo de casos en un conjunto simple*

Factor A esta limitado a 1; Factors B and C no porque lo son por definición. Solo un AS (si lo hay) puede tener un valor máximo para los tres factores, o sea que esto limita el índice HE a 1000 como era deseado en la propiedad No 4.

Entonces el índice para cada fuente de datos es calculada de la maniera siguiente:

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

Los Factores A, B y C pesan respectivamente 10 %, 10 % y 80 % y esto resulta de las pruebas de precisión y los test de regresión. Para comenzar, valores bajos fueron elegidos para los Factores A y Factor B porque es mejor no favorecer demasiado los ASes pequeños (propiedad No 2).

El Índex HE general es calculado usando la fórmula:

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

where:
w_i: *peso de la fuente (1=baja, 2=media, 3=alta, 4=muy alta)*