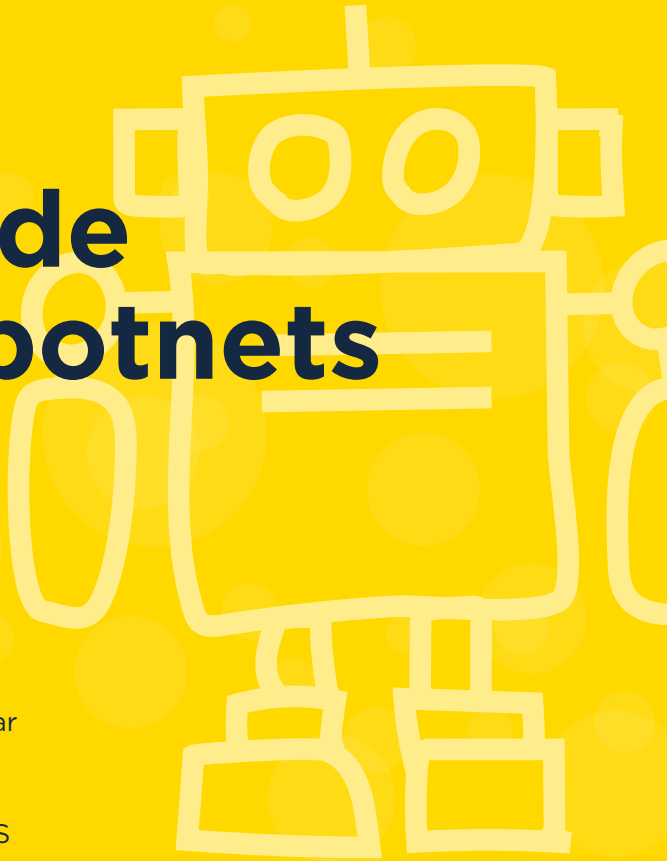
SPAMHAUS



Actualización de amenazas de botnets de Spamhaus

T4 2021

En el T4, se produjo un aumento del 23% en el número de nuevos comando y controladores de botnets (C&C) identificados por nuestro equipo de investigadores. A pesar de este aumento, a nuestros investigadores les resulta imposible rastrear cierta actividad de botnet C&C porque las comunicaciones se realizan mediante DNS sobre HTTPS (DoH). Es algo ciertamente preocupante y que inclina la balanza a favor de los cibercriminales.

Te damos la bienvenida a la Actualización de amenazas de botnets de Spamhaus, T4 de 2021.

Acerca de este informe

Spamhaus rastrea tanto las direcciones de protocolo de Internet (IP) como los nombres de dominio que los individuos malintencionados utilizan para alojar servidores de comando y controladores de botnets (C&C). Estos datos nos permiten identificar los elementos relacionados como la ubicación geográfica de los botnet C&C, el malware relacionado con ellos, los dominios de nivel superior (TLD) utilizados al registrar un dominio para el botnet C&C, así como los registradores colaboradores y la red donde se aloja la infraestructura del botnet C&C.

Este informe proporciona información sobre la cantidad de botnet C&C relacionados con estos elementos, además de una comparación trimestral. Explicamos las tendencias que observamos y destacamos los proveedores de servicios que tienen problemas para controlar la cantidad de operadores de botnet que abusan de sus servicios.

Destacamos

El problema del DNS sobre HTTPS (DoH)

¿Recuerdas los FluBot y TeamBot en el T3?

El último trimestre anunciamos “una explosión del malware de puerta trasera” a causa de FluBot y TeamBot. En el T4, desde la perspectiva de la infraestructura de botnet C&C observada por Spamhaus, esta familia de malware ha desaparecido por completo. No obstante, esto no significa que estuvieran inactivos. En realidad, ocurría lo contrario: ¡estaban activos!

¿Por qué Spamhaus no logra detectarlos?

Este malware no aparece en nuestras listas porque sus malvados creadores han modificado su modo de funcionamiento. En lugar de realizar las comunicaciones de C&C mediante el protocolo HTTPS tradicional, ahora utilizan DNS sobre HTTPS (DoH) y explotan los grandes proveedores de DoH, como Google y Alibaba.

Se hace más difícil evitar el abuso en Internet

A pesar de que DoH se anunció con bombos y platillos como el mejor avance en la seguridad de Internet, algunos profesionales de seguridad (como Spamhaus) suspiramos al comprender que los buenos perderíamos todavía más visibilidad sobre lo que hacen los malos. Al decir “todavía más” nos referimos a otras cuestiones como la pérdida de visibilidad de los datos WHOIS.[1]

(1) www.spamhaus.org/news/article/775/how-has-gdpr-affected-spam

¿Por qué el DoH supone un problema?

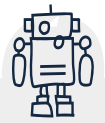
El DoH cifra el tráfico de DNS, convirtiendo en un recurso seguro y privado algo que siempre había sido público antes (no cifrado). Tal vez pienses que es algo bueno, pero, como puedes ver, en este caso nuestros investigadores no tienen visibilidad sobre las peticiones DNS de FluBot y TeamBot. Por ende, es imposible crear listas con las direcciones IP y, por lo tanto, no podemos usar estos datos para proteger a los usuarios. Aunque el objetivo de DoH es proteger a la comunidad de Internet, también está ayudando a los cibercriminales: se trata de un arma de doble filo.

DoH no solo dificulta el rastreo de los delincuentes, sino que también supone que los productos de seguridad basados en la monitorización y el filtrado de DNS resultan menos efectivos, lo que dista mucho de ser ideal. Los problemas de seguridad se acumulan debido a que los principales proveedores de DoH no filtran las resoluciones DNS malignas procedentes de dominios de botnet, phishing o malware.

Cantidad de botnet C&C observados en el T4 de 2021

En el T4 de 2021, Spamhaus identificó 3 271 botnet C&C en comparación con 2 656 en el tercer trimestre de ese mismo año. Un aumento de 23% en el trimestre. El promedio mensual aumentó de 885 botnet C&C al mes en el tercer trimestre a 1090 al mes en el cuarto.

Trimestre	Cant. de botnets	Promedio trimestral	% de cambio
T1	1 660	553	24%
T2	1 462	487	-12%
T3	2 656	885	82%
T4	3 271	1 090	23%



¿Qué son los comando y controladores de botnet?

Un “controlador de botnet”, “botnet C2” o servidor de “botnet Command & Control” comúnmente abreviado como “botnet C&C”. Los estafadores los usan tanto para controlar las máquinas infectadas por malware como para extraer información personal valiosa de las víctimas infectadas.

Los botnet C&C desempeñan un papel vital en las operaciones realizadas por cibercriminales que usan máquinas infectadas para enviar spam o ransomware, lanzar ataques DDoS, cometer fraudes de banca en línea o fraude por clic o para minar criptomonedas como Bitcoin.

Las computadoras de escritorio y los dispositivos móviles, como los smartphones, no son las únicas máquinas que pueden infectarse. Hay una cantidad cada vez mayor de dispositivos conectados a Internet, por ejemplo, los dispositivos del internet de las cosas (IoT) como las cámaras web, el almacenamiento anexado a la red (NAD) y muchos otros. Estos también corren el riesgo de infectarse.

Localización geográfica de botnet C&C, T4 de 2021

Rusia sigue aumentando notablemente

En el trimestre pasado, mencionábamos que el número de botnet C&C en Rusia había aumentado mucho. Pues bien, en este trimestre, el aumento ha sido todavía mayor:

- T1 al T2: aumento de 19%
- T2 al T3: aumento de 64%
- T3 al T4: aumento de 124%

En el T4, casi el 30% de los servidores de botnet C&C estaban alojados en Rusia.

Latinoamérica sigue presente

Varios países latinoamericanos aparecieron por primera vez en las listas en el T3 y continúan entre las 20 primeras posiciones en el T4, como México, República Dominicana, Brasil y Uruguay. Uruguay ha mostrado el mayor incremento porcentual (181%) de todas las ubicaciones en el T4.

Altibajos en Europa

Tras continuos aumentos en varios países europeos, nos alegra informar de que las cifras han descendido en algunos: Países Bajos, Francia, Suecia y Rumanía. Además, Suiza ha abandonado por completo la lista de los 20 puestos principales. Sin embargo, Alemania ha escalado hasta la tercera posición con un aumento de 35% y Gran Bretaña ha experimentado un incremento de 56%.

Nuevas entradas

Ucrania (#12), Bulgaria (#15), Seychelles (#17) y Hong Kong (#18).

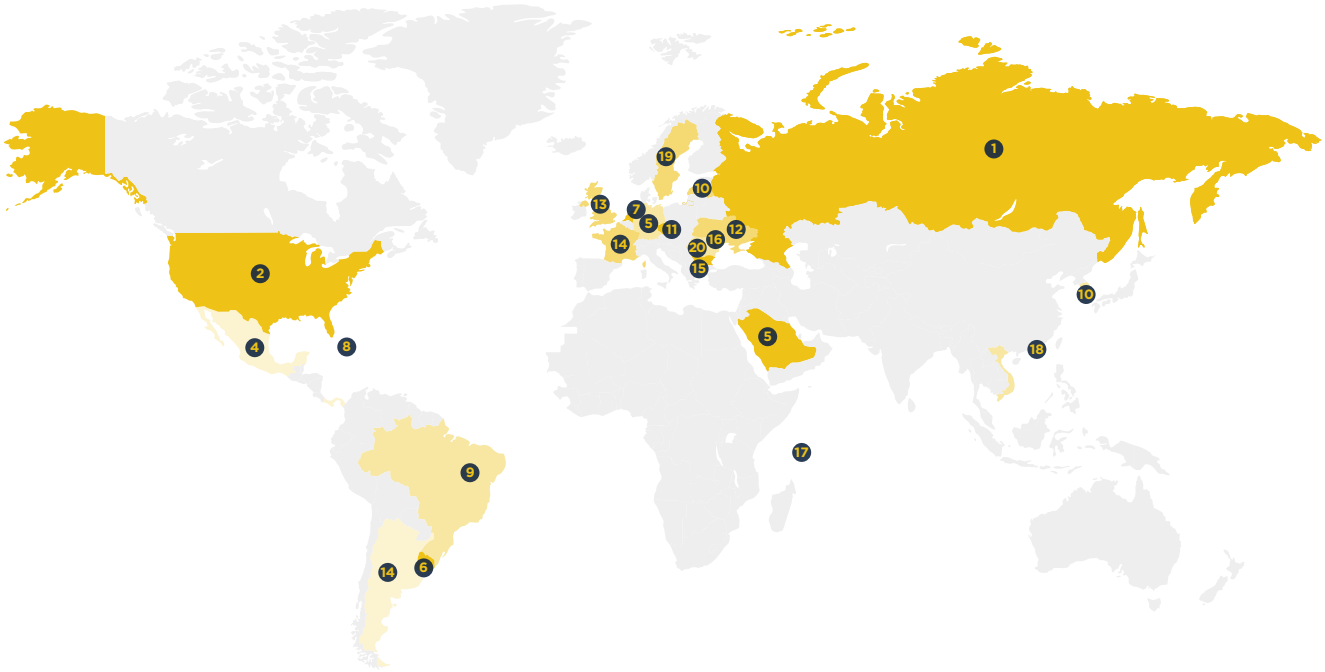
Salidas

Corea, Suiza, Argentina y Vietnam.

Localización geográfica de botnet C&C, T4 de 2021 (continuación)

20 principales localizaciones de botnet C&C

Clasificación	País	T3 2021	T4 2021	% cambio T a T
#1	Rusia	381	854	124%
#2	Estados Unidos	301	384	28%
#3	Alemania	170	230	35%
#4	México	182	186	2%
#5	Arabia Saudita	117	180	54%
#6	Uruguay	63	177	181%
#7	Países Bajos	273	164	-40%
#8	Rep. Dominicana	96	110	15%
#9	Brasil	86	92	7%
#10	Letonia	58	69	19%
#11	Rep. Checa	40	66	65%
#12	Ucrania	-	64	Nueva entrada
#13	Reino Unido	39	61	56%
#14	Francia	123	60	-51%
#15	Bulgaria	-	56	Nueva entrada
#16	Moldavia	49	50	2%
#17	Seychelles	-	34	Nueva entrada
#18	Hong Kong	-	28	Nueva entrada
#19	Suecia	38	26	-32%
#20	Rumanía	33	24	-27%



Malware asociado con botnet C&C, T4 de 2021

En el T4, los ladrones de credenciales fueron el tipo de malware dominante asociado con botnet C&C. No es ninguna sorpresa, ya que los dos primeros malwares en la lista, RedLine y Loki, pertenecen a esta categoría.

Aumento de GCleaner

Hemos observado un aumento considerable en la actividad de GCleaner, que se sitúa ahora en la cuarta posición, a pesar de haber ingresado recientemente a los 20 puestos principales. El *modus operandi* de GCleaner es similar al de Smoke: se utiliza en un modelo de pago por instalación (PPI) e instala otro malware en servidores ya infectados. A pesar de que este malware lleva tiempo en circulación, es la primera vez que GCleaner ingresa a nuestros 20 puestos principales.

Desaparición de FluBot/TeamBot

Como explicábamos en nuestra sección de Destacamos, este malware, que ocupó la primera posición durante el trimestre pasado, ha desaparecido de nuestras listas; sin embargo, continúa estando activo y ahora utiliza DoH.

Nuevas entradas

GCleaner (#4), DCRat (#10), Arkei (#14), TrickBot (#15), Socelars (#16).

Salidas

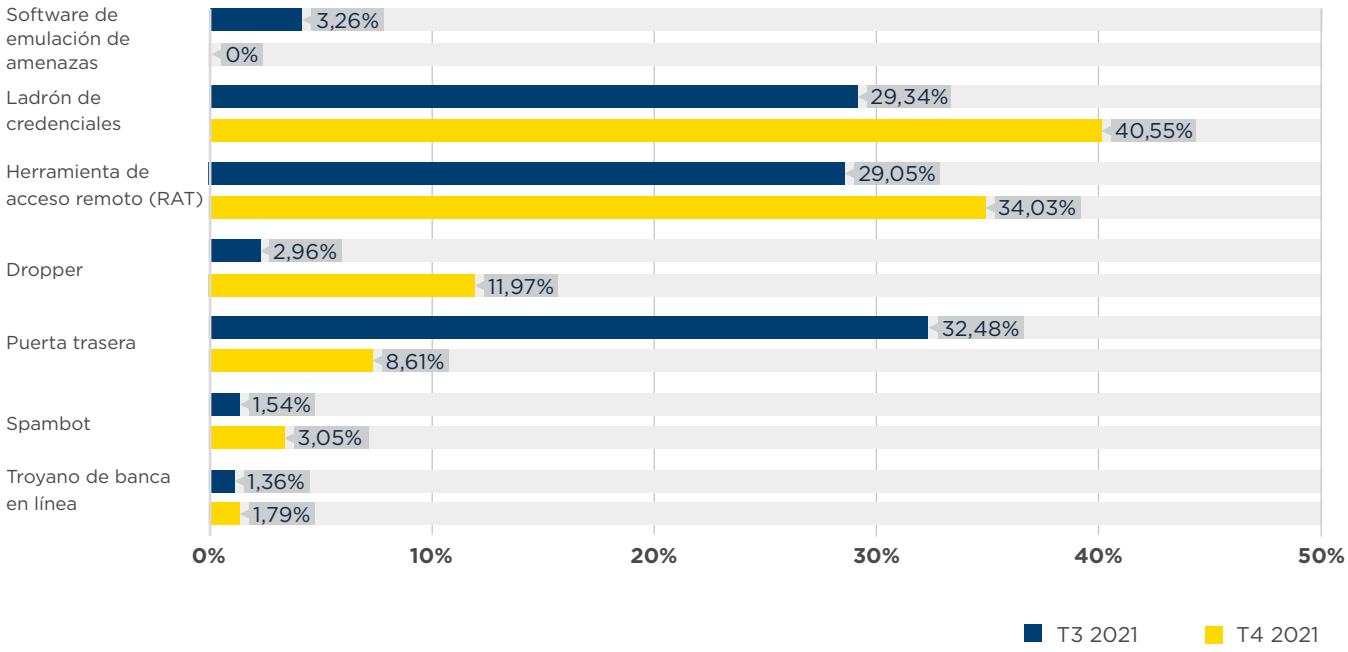
FluBot/TeamBot, AveMaria, ServHelper, QuasarRAT, AgentTesla.

Malware asociado con botnet C&C, T4 de 2021 (continuación)

Familias de malware asociadas con botnet C&C

Clasificación	T3 2021	T4 2021	% de cambio	Familia de malware	Descripción
#1	210	164	-22%	RedLine	Ladrón de credenciales
#2	108	102	-6%	Loki	Ladrón de credenciales
#3	121	91	-25%	AsyncRAT	Herramienta de acceso remoto (RAT)
#4	-	86	Nueva entrada	GCleaner	Dropper
#5	93	75	-19%	Raccoon	Ladrón de credenciales
#6	43	65	51%	Vjw0rm	Herramienta de acceso remoto (RAT)
#7	41	43	5%	CryptBot	Puerta trasera
#8	136	37	-73%	BitRAT	Herramienta de acceso remoto (RAT)
#9	71	36	-49%	NjRAT	Herramienta de acceso remoto (RAT)
#10	-	32	Nueva entrada	DCRat	Herramienta de acceso remoto (RAT)
#11	26	29	12%	Tofsee	Spambot
#11	40	29	-28%	Remocs	Herramienta de acceso remoto (RAT)
#13	50	28	-44%	Smoke Loader	Dropper
#14	-	27	Nueva entrada	Arkei	Ladrón de credenciales
#15	-	21	Nueva entrada	TrickBot	Puerta trasera
#16	-	18	Nueva entrada	Socelars	Ladrón de credenciales
#16	55	18	-67%	CobaltStrike	Puerta trasera
#18	23	17	-26%	Gozi	Troyano de banca en línea
#18	37	17	-54%	NanoCore	Herramienta de acceso remoto (RAT)
#18	30	17	-43%	STRRAT	Herramienta de acceso remoto (RAT)

Comparación de tipos de malware entre el T3 y el T4 de 2021



Dominios de nivel superior (TLD) con mayor abuso, T4 de 2021

Nueva entrada en la cuarta posición

Pocas veces vemos nuevos TLD entre las cinco primeras posiciones de esta lista de los 20 botnet C&C principales; sin embargo, .xxx, un TLD de adultos operado por ICM Registry, aparece en la cuarta posición. Con menos de 10 000 dominios activos pero un total de 223 dominios asociados con actividad de botnet C&C en el cuarto trimestre, podemos asegurar que hay problemas.

Reaparición de .de

El ccTLD .de (Alemania) vuelve a aparecer en nuestra clasificación trimestral en la posición #20, tras haber desaparecido de los 20 puestos principales en el segundo trimestre.

Reducciones y salidas

Nos gustaría felicitar a todos los registros que gestionan TLD que abandonan nuestras listas y a aquellos que han reducido notablemente el número de botnet C&C asociados que utilizan sus TLD, como .buzz y .net, que han experimentado una reducción de 80%.

Error en los datos del T3

Pedimos disculpas a Verisign por un error en nuestras estadísticas del T3 de 2021 para .com. El número de botnet C&C para este TLD estaba equivocado y la cifra correcta fue de 3 730. Este error se debió a varios problemas, pero podemos confirmar que hemos colaborado con Verisign para solucionarlos.

Interpretación de los datos

Los registros con un mayor número de dominios activos están más expuestos a posibles abusos. Por ejemplo, en el T4 de 2021, .net tenía más de 13 millones de dominios activos, de los cuales el 0,00103% estaba asociado con botnet C&C. Mientras que .xxx solo tenía poco más de 9 000 dominios activos, de los cuales el 2,4% estaba asociado con botnet C&C. Ambos aparecen entre los 10 primeros puestos de nuestra lista, pero uno tenía un porcentaje de dominios activos asociados con botnet C&C mucho mayor que el otro.

Dominios de nivel superior (TLD): un breve repaso

Hay varios dominios de nivel superior (TLD) distintos, entre ellos:

TLD genéricos (gTLD): cualquiera puede usarlos.

Dominios territoriales (ccTLD): algunos tienen un uso restringido dentro de un país o región en particular; sin embargo, otros tienen licencias para uso general y ofrecen la misma funcionalidad que los gTLD.

TLD descentralizados (dTLD): dominios de nivel superior (TLD) independientes que no están bajo el control de ICANN.

Colaboramos con el sector para aumentar la seguridad de Internet

Obviamente, preferiríamos que los TLD no tengan botnet C&C que se asocien con ellos, pero tenemos los pies en el suelo y sabemos que siempre se producirán abusos.

Lo fundamental es abordar los abusos con rapidez. Cuando sea necesario, si los nombres de dominio se registran con el único propósito de distribuir malware o alojar botnet C&C, desearíamos que los registros suspendieran estos nombres de dominio. Agradecemos los esfuerzos de muchos registros que colaboran con nosotros para garantizar que se tomen dichas medidas, como .xyz y .top.

Nuevas entradas

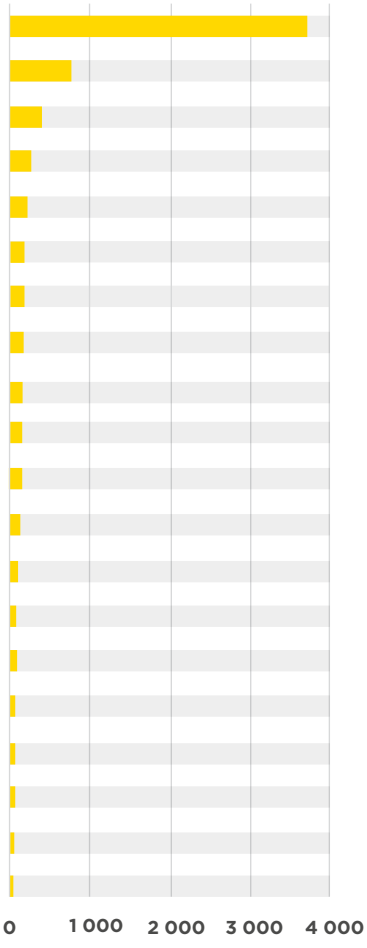
xxx (#4), site (#14), one (#15), gq (#16), sbs (#18), de (#20).

Salidas

cn, su, club, eu, co, monster.

TLD con mayor abuso: cantidad de dominios

Clasificación	T3 2021	T4 2021	% de cambio	TLD	Nota
#1	3 730	3 719	-0,2%	com	gTLD
#2	829	715	-14%	top	gTLD
#3	833	396	-52%	xyz	gTLD
#4	-	223	Nueva entrada	xxx	gTLD
#5	132	143	8%	ga	Originalmente ccTLD, ahora efectivamente gTLD
#6	665	136	-80%	net	gTLD
#7	330	133	-60%	ru	ccTLD
#8	183	122	-33%	tk	Originalmente ccTLD, ahora efectivamente gTLD
#9	265	116	-56%	org	gTLD
#10	538	108	-80%	buzz	gTLD
#11	178	103	-42%	info	gTLD
#12	98	97	-1%	cf	Originalmente ccTLD, ahora efectivamente gTLD
#13	123	87	-29%	ml	Originalmente ccTLD, ahora efectivamente gTLD
#14	-	75	Nueva entrada	site	gTLD
#15	-	70	Nueva entrada	one	gTLD
#16	-	56	Nueva entrada	gq	Originalmente ccTLD, ahora efectivamente gTLD
#17	82	52	-37%	cloud	gTLD
#18	-	51	Nueva entrada	sbs	gTLD
#19	170	45	-74%	br	ccTLD
#20	-	44	Nueva entrada	de	ccTLD



Los registradores de dominios con mayor abuso, T4 de 2021

En términos globales, el registro de dominios fraudulentos descendió en el T4 de 2021, lo que supone buenas noticias. Sin embargo, los registradores de algunos países siguen teniendo problemas.

Registradores en Canadá

Los registradores en Canadá presentaron el mayor número de registros de botnet C&C fraudulentos en el T4, superando a China en relación con el T3.

Registradores en Alemania

Se produjo un aumento considerable (136%) en el número de botnet C&C asociado con registradores que operan desde Alemania. Esto se debió al aumento de 74% de Key Systems y a que 1API regresó a nuestras listas para ocupar la posición #12, tras haber salido de los 20 puestos principales en el T2.

Atak

Este registrador de dominios apareció por primera vez en nuestra clasificación. Atak opera desde Turquía y hasta la fecha no ha respondido a ninguno de nuestros informes de abuso. Por lo tanto, hemos presentado una queja contra Atak ante la ejecución de políticas de la ICANN. Es imprescindible que todas las entidades que forman parte de la ecosfera de Internet trabajen juntas para proteger a los usuarios de Internet.

Nicenic.net (China) y PDR (India)

Estos registradores mostraron aumentos considerables en el número de dominios de botnet C&C registrados con ellos en el T4. Sin embargo, aunque aumentan los registros a través de PDR, sus tiempos de respuesta a los informes de abusos son excelentes.

Gracias a los registradores que han salido de nuestras listas

En el trimestre pasado, destacábamos que CentralNic, West263 y Network Solutions habían mostrado aumentos considerables en el número de nuevos dominios de botnet C&C registrados. En el T4, estos tres registradores, junto con eName, Xin Net, 22net y OVH, salieron de nuestra lista de los 20 lugares principales, por lo que aplaudimos sus esfuerzos para evitar los registros fraudulentos.

Registradores y operadores de botnet C&C

Los cibercriminales necesitan encontrar un registrador colaborador para registrar un nombre de dominio para un botnet C&C. Los registradores no pueden detectar fácilmente todos los registros fraudulentos antes de que estos dominios estén operativos. No obstante, la “vida útil” de los dominios delictivos en un registrador legítimo y bien gestionado suele ser relativamente corta.

Nuevas entradas

1API (#12), Beget (#14), Sav.com (#15), Hostinger (#16), Atak (#18), Naunet (#19), EuroDNS (#20), Mat Bao Corporation (#20).

Salidas

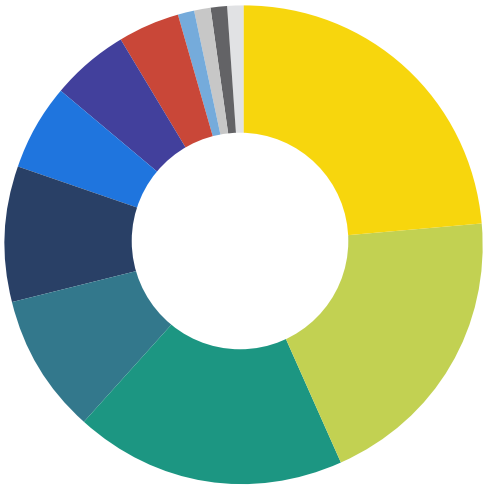
eName, CentralNic, Network Solutions, Xin Net, west263.com, 22net, OVH.

Los registradores de dominios con mayor abuso, T4 de 2021 (continuación)

Los registradores de dominios con mayor abuso: cantidad de dominios

Clasificación	T3 2021	T4 2021	% de cambio	Registrador	País
#1	1 568	988	-37%	NameSilo	Canadá
#2	1 267	718	-43%	Namecheap	Estados Unidos
#3	209	536	156%	nicenic.net	China
#4	169	433	156%	PDR	India
#5	188	328	74%	Key Systems	Alemania
#6	154	272	77%	WebNic.cc	Singapur
#7	1 217	201	-83%	Alibaba	China
#8	165	197	19%	Openprovider	Países Bajos
#9	189	135	-29%	Eranet International	China
#10	403	127	-68%	Tucows	Canadá
#11	475	124	-74%	RegRU	Rusia
#12	-	115	Nueva entrada	1API	Alemania
#13	403	80	-80%	Porkbun	Estados Unidos
#14	-	68	Nueva entrada	Beget LLC	Rusia
#15	-	66	Nueva entrada	Sav.com	Estados Unidos
#16	-	57	Nueva entrada	Hostinger	Lituania
#17	214	54	-75%	dnspod.cn	China
#18	-	51	Nueva entrada	Atak	Turquía
#19	-	49	Nueva entrada	NauNet	Rusia
#20	-	48	Nueva entrada	Mat Bao Corporation	Vietnam
#20	-	48	Nueva entrada	EuroDNS	Luxemburgo

UBICACIÓN DE LOS REGISTRADORES DE DOMINIOS CON MAYOR ABUSO



País	Botnets	%
Canadá	1 115	23,75%
China	926	19,72%
Estados Unidos	864	18,40%
Alemania	443	9,44%
India	433	9,22%
Singapur	272	5,79%
Rusia	241	5,13%
Países Bajos	197	4,20%
Lituania	57	1,21%
Turquía	51	1,09%
Luxemburgo	48	1,02%
Vietnam	48	1,02%
Total	**4 695**	

Redes que alojan los botnet C&C más recientes, T4 de 2021

Como es habitual, hubo muchos cambios en las redes que alojan los botnet C&C más recientes.

¿Esta lista refleja con qué rapidez se gestiona el abuso en las redes?

Si bien esta lista de las 20 posiciones principales indica que pueden existir problemas con los procesos de evaluación de clientes, no muestra la velocidad con la que los operadores gestionan los abusos comunicados. Lee “Redes que alojan los botnet C&C más activos” para ver qué redes no gestionan los abusos con rapidez.

Un poco de todo

Uninet.net.mx (#1), serverion.com (#5) y cloudflare.com (#9) aparecen todos ellos entre las 10 primeras posiciones de nuestras listas, pero hay grandes diferencias entre ellos.

Uninet es una operadora de redes y telecomunicaciones en México. Todos los botnet C&C alojados recientemente en su espacio de IP se debieron a equipos de clientes comprometidos.

Serverion es un proveedor de alojamiento con sede en Países Bajos. Todos los botnet C&C que identificamos en su red en el cuarto trimestre se debieron a registros fraudulentos.

Por último tenemos a Cloudflare, que no aloja ningún contenido, sino que presta servicios de proxy inverso y protección contra DDoS a los botnet C&Cs, ocultando su ubicación real.

Redes y operadores de botnet C&C

Las redes tienen un grado de control razonable sobre los operadores que registran un nuevo servicio de forma fraudulenta.

Se debe realizar un sólido proceso de evaluación y verificación de clientes antes de empezar a operar un servicio.

El hecho de que las redes aparezcan en una posición elevada en la clasificación es indicio de alguno de los siguientes problemas:

1. Las redes no aplican las prácticas recomendadas para los procesos de verificación de clientes.
2. Las redes no se aseguran de que TODOS sus comercializadores apliquen buenas prácticas de verificación de clientes.

En algunos de los peores casos, los empleados o propietarios de las redes se benefician directamente de los registros fraudulentos, es decir, obtienen dinero intencionadamente de los delincuentes por alojar sus botnet C&C; sin embargo, afortunadamente, esto no sucede con frecuencia.

Nuevas entradas

selectel.ru (#10), timeweb.ru (#12), firstbyte.ru (#13), pinvds.com (#15), ihor-hosting.ru (#18), itldc.com (#19), m247.ro (#20).

Salidas

ipjetable.net, pq.hosting, ovh.com, mivocloud.com, telefonica.com.ar, uplus.co.kr, mgnhost.ru.

Redes que alojan los botnet C&C más recientes, T4 de 2021 (continuación)

Botnet C&C descubiertos recientemente por red

Clasificación	T3 2021	T4 2021	% de cambio	Red	País
#1	177	187	6%	uninet.net.mx	México
#2	33	182	452%	alibaba-inc.com	China
#3	63	175	178%	antel.net.uy	Uruguay
#4	105	168	60%	stc.com.sa	Arabia Saudita
#5	115	116	1%	serverion.com	Países Bajos
#6	95	110	16%	claro.com.do	Rep. Dominicana
#7	58	85	47%	telefonica.com.br	Brasil
#8	44	80	82%	baxet.ru	Rusia
#9	68	72	6%	cloudflare.com	Estados Unidos
#10	-	63	Nueva entrada	selectel.ru	Rusia
#11	44	51	16%	nano.lv	Letonia
#12	-	49	Nueva entrada	timeweb.ru	Rusia
#13	-	48	Nueva entrada	firstbyte.ru	Rusia
#13	33	48	45%	hostwinds.com	Estados Unidos
#15	-	47	Nueva entrada	pinvds.com	Rusia
#16	89	39	-56%	privacyfirst.sh	Alemania
#17	51	38	-25%	hetzner.de	Alemania
#18	-	36	Nueva entrada	ihor-hosting.ru	Rusia
#19	-	35	Nueva entrada	itldc.com	Ucrania
#20	-	34	Nueva entrada	m247.ro	Rumanía

Redes que alojan los botnet C&C más activos, T4 de 2021 (continuación)

Finalmente, echemos un vistazo a las redes que alojaban la mayor cantidad de botnet C&C activos al final de 2021. Los proveedores de alojamiento que aparecen en esta clasificación tienen un problema de abuso, no toman las medidas adecuadas cuando reciben los informes de abuso o bien no nos informan cuando han solucionado un problema de abuso.

Nuevas entradas

al.bg (#8), mobily.com.sa (#12), ielo.net (#13), google.com (#16), combahton.net (#16).

Salidas

serverion.com, uplus.co.kr, hostry.com, skbroadband.com, claro.com.co.

Los operadores de red en la región de Latinoamérica abordan los abusos con rapidez

Más del 60% de los botnet C&C activos se encuentran en redes situadas en la región de Latinoamérica. Rogamos a estos operadores que respondan con rapidez a los informes de abusos y colaboren con Spamhaus para reducir el abuso de los botnet C&C en sus redes.

Número total de botnet C&C activos por red (hasta el 31 de diciembre de 2021)

Clasificación	T3 2021	T4 2021	% de cambio	Red	País
#1	185	389	110%	uninet.net.mx	México
#2	119	296	149%	stc.com.sa	Arabia Saudita
#3	68	257	278%	antel.net.uy	Uruguay
#4	97	204	110%	claro.com.do	Rep. Dominicana
#5	63	146	132%	telefonica.com.br	Brasil
#6	79	94	19%	microsoft.com	Estados Unidos
#7	99	91	-8%	ipjetable.net	Francia
#8	-	60	Nueva entrada	a1.bg	Bulgaria
#9	41	41	0%	telefonica.com.ar	Argentina
#10	29	29	0%	tie.cl	Chile
#10	32	29	-9%	vietserver.vn	Vietnam
#12	-	27	Nueva entrada	mobily.com.sa	Arabia Saudita
#13	-	25	Nueva entrada	ielo.net	Francia
#14	21	24	14%	clouvider.net	Reino Unido
#15	24	22	-8%	ovpn.com	Suecia
#16	22	21	-5%	charter.com	Estados Unidos
#16	-	21	Nueva entrada	google.com	Estados Unidos
#16	21	21	0%	algartelecom.com.br	Brasil
#16	21	21	0%	une.net.co	Colombia
#16	-	21	Nueva entrada	combahton.net	Alemania