SPAMHAUS

Actualización de amenazas de botnets de Spamhaus

T2 2021

En este trimestre, los investigadores de Spamhaus observaron una reducción de 12% en los nuevos comandos y controladores (C&C) de botnets identificados, lo cual es buena noticia. Sin embargo, no hay buenas noticias para todos; más de un proveedor líder del sector está sintiendo el peso de los botnet C&C en sus redes.

Te damos la bienvenida a la actualización de amenazas de botnets de Spamhaus T2 2021.

¿Qué son los controladores de botnets?

Un “controlador de botnets”, “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 tienen un papel vital en las operaciones realizadas por cibercriminales que están usando máquinas infectadas para enviar spam o ransomware, lanzar ataques DDoS, cometer fraudes de banca en línea o fraude por clic o para extraer 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 mayor de dispositivos conectados al internet; por ejemplo, los dispositivos del internet de las cosas (IoT) como las cámaras web, el almacenamiento anexado a la red (NAS) y muchos otros. Estos también corren el riesgo de infectarse.

Destacamos

La historia de Emotet continúa

Sí, ya lo sabemos... seguimos hablando de Emotet, a pesar de que su desmantelamiento fue en enero. Y esto se debe a que la narrativa de Emotet no terminó cuando se desmanteló. Lejos de ello.

Como resultado de la proliferación de Emotet, a través del secuestro del hilo, millones de cuentas de correo electrónico quedaron comprometidas y abiertas a mayor explotación por parte de otros malware y ransomware.

Durante este último trimestre, Spamhaus trabajó con el FBI para apoyar con medidas de reparación y llegar a los afectados. Para que te des una idea de la escala de la operación, aquí van algunas cifras:

- 1,3 millones de cuentas de email vulneradas
- 22 000 dominios únicos
- 3000 redes

Nuestro equipo se ha dedicado a contactar a los departamentos relevantes de abuso, departamentos de confianza y seguridad, así como usuarios finales con el fin de ofrecerles datos de remedio e instrucciones para salvaguardar las cuentas hackeadas.

Nos complace informar que ya se aseguraron más del 60% de esos 1,3 millones de cuentas. Esto nos muestra que todos tenemos un papel que desempeñar para hacer que el internet sea un lugar más seguro.

¿Qué es el secuestro del hilo?

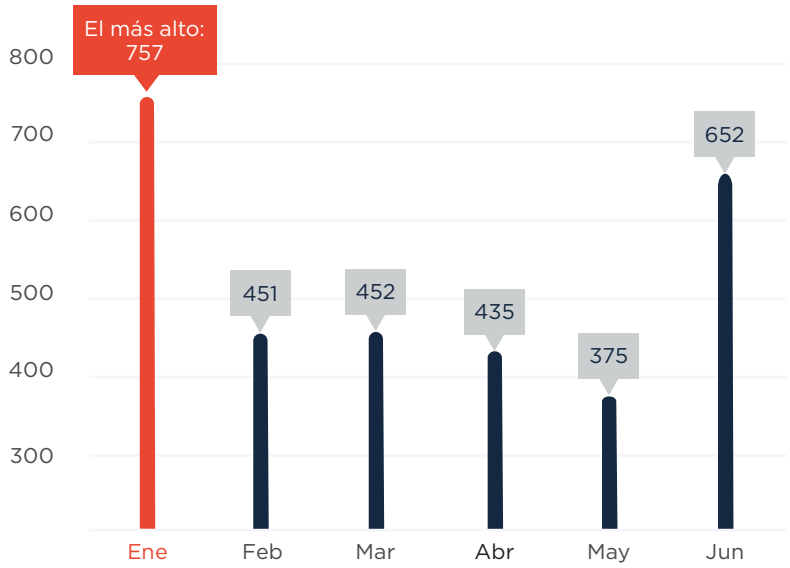
Es donde estos villanos usan las conversaciones de email existentes de sus víctimas (hilo) para difundir y hacer llegar enlaces o archivos adjuntos maliciosos a nuevas víctimas.

Un atacante puede ser mucho más convincente y engañar a más víctimas para que hagan clic en enlaces dañinos o para que descarguen archivos respondiendo a un hilo de email existente.

Cantidad de botnet C&C observados en T2 2021

Aquí te dejamos un resumen de la cantidad de nuevos servidores de comandos y controles de botnet (C&C) en el segundo trimestre de 2021. Spamhaus Malware Labs identificó **1462 botnet C&C** en comparación con 1660 en el primer trimestre de 2021. Una **disminución** del **12%**. El promedio mensual cayó de 553 al mes en el primer trimestre a 487 botnet C&C al mes en el segundo.

Número de nuevos botnet C&C detectados por Spamhaus en 2021:



T1 Promedio mensual: 553

T2 Promedio mensual: 487

Geolocalización de botnet C&C, T2 2021

Observamos varios cambios en la geolocalización que usaron los cibercriminales para establecer nuevos servidores botnet C&C, particularmente en el nivel más bajo de nuestro listado de los 20 principales, donde se produjo un gran número de nuevas entradas.

Disminuciones en América Latina

Se produjo un descenso notable en países latinoamericanos con alojamiento de botnet C&C. Argentina y Colombia quedaron fuera de la lista de los 20 principales y Brasil tuvo una disminución del 40%. La única excepción fue Panamá que se convirtió en el nuevo #13 de la lista.

Incrementos continuos en Europa

Una vez más, presenciamos un aumento en la cantidad de países europeos que se posicionaron en los 20 principales. Entre ellos la República Checa, Polonia y Finlandia. Mientras tanto, Alemania, Francia, Letonia y Reino Unido experimentaron incrementos en botnet C&C.

Nuevas entradas

República Checa (#11), Panamá (#13), Malasia (#15), Polonia (#15), Finlandia (#17), Vietnam (#18).

Salidas

China, Suecia, Hong Kong, Argentina, Colombia, Singapur.

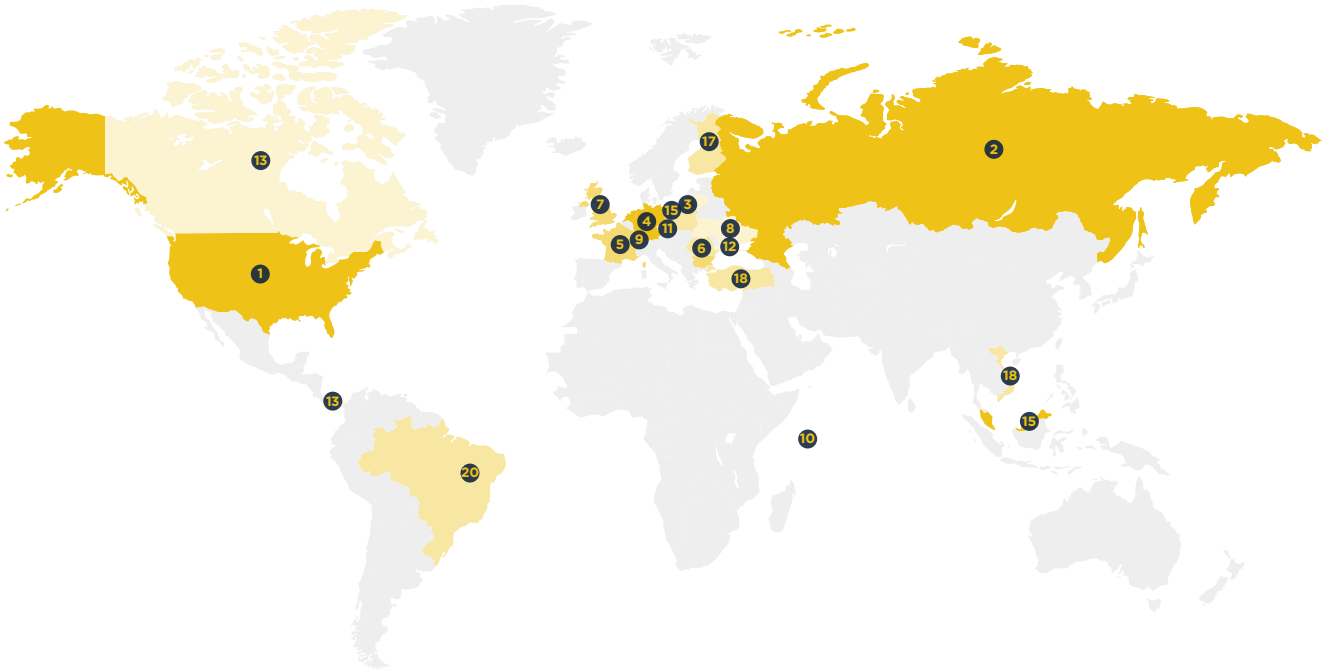
Geolocalización de botnet C&C, T2 2021 (continuación)

20 principales localizaciones de botnet C&C

Clasificación	País	T1 2021	T2 2021	% de cambio de T a T
#1	Estados Unidos	338	281	-17%
#2	Rusia	195	233	19%
#3	Países Bajos	207	168	-19%
#4	Alemania	99	117	18%
#5	Francia	71	92	30%
#6	Letonia	31	84	171%
#7	Reino Unido	49	57	16%
#8	Ucrania	22	44	100%
#9	Suiza	59	41	-31%
#10	Seychelles	29	38	31%

Nueva entrada

Clasificación	País	T1 2021	T2 2021	% de cambio de T a T
#11	República Checa	-	31	Nueva entrada
#12	Moldavia	29	29	0%
#13	Panamá	-	16	Nueva entrada
#13	Canadá	26	16	-38%
#15	Malasia	-	15	Nueva entrada
#15	Polonia	-	15	Nueva entrada
#17	Finlandia	-	14	Nueva entrada
#18	Vietnam	-	13	Nueva entrada
#18	Turquía	25	13	-48%
#20	Brasil	20	12	-40%



Malware asociado con botnet C&C, T2 2021

Empecemos con las buenas noticias. Tras el loable desmantelamiento de la botnet Emotet en el primer trimestre de 2021, nos complace informar que no se ha observado ninguna actividad de Emotet.

Aumento de la popularidad de los droppers

En el segundo trimestre, se produjo un cambio que dejó atrás los ladrones de credenciales y herramientas de acceso remoto (RAT) para pasar a los droppers.

Raccoon alcanza rápidamente el #1

Raccoon hizo su primera aparición en nuestros 20 principales en el último trimestre al ocupar el #8. En el segundo trimestre, escaló la clasificación hasta posicionarse en el primer lugar.

Ladrones de credenciales a la venta

No solo está a la venta en la dark web el ladrón de credenciales antes mencionado, Raccoon, sino que también están RedLine y Oski, que fueron nuevas entradas en nuestras listas de los más populares en este trimestre. Dada la facilidad de acceso, no es de sorprender que la popularidad de este malware vaya en aumento.

¿Qué es un dropper?

Los droppers ocultan el código para que el malware eluda la detección de los escáneres de virus, es decir, dejan caer silenciosamente el malware en el sistema objeto de intervención.

Nuevas entradas

Oski (#7), Tofsee (#11), STRRAT (#15), CryptBot (#16), CobaltStrike (#17), ServHelper (#18), IcedID (#18).

Salidas

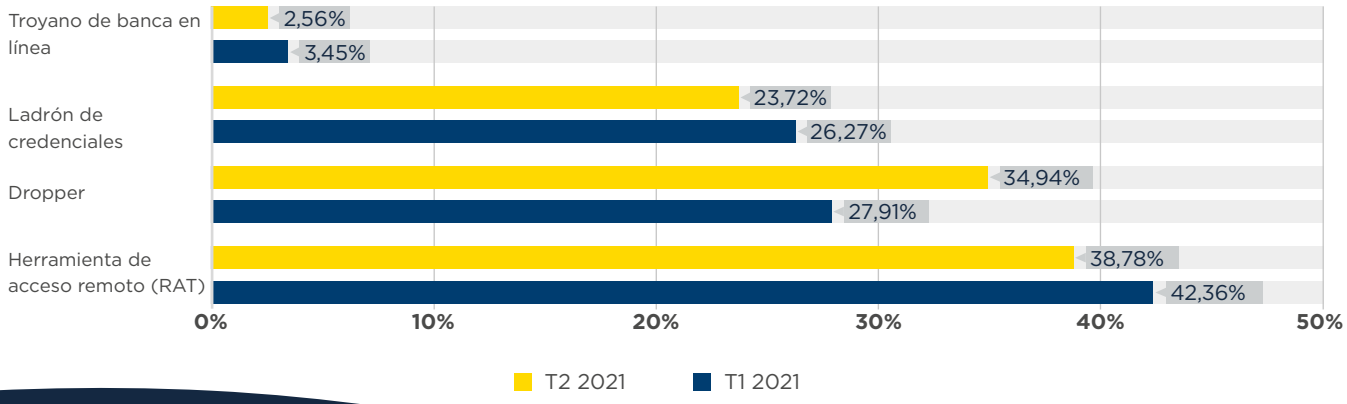
Emotet, NetWire, AveMaria, FickerStealer, AZORult, TriumpLoader, Hancitor

Malware asociado con botnet C&C, T2 2021 (continuación)

Familias de malware asociadas con botnet C&C

Clasificación	T1 2021	T2 2021	% cambio	Familia de malware	Descripción
#1	45	302	571%	Raccoon	Dropper
#2	55	123	124%	RedLine	Herramienta de acceso remoto (RAT)
#3	69	83	20%	AsyncRAT	Ladrón de credenciales
#4	83	66	-20%	Loki	Herramienta de acceso remoto (RAT)
#5	38	43	13%	Gozi	Herramienta de acceso remoto (RAT)
#6	33	42	27%	BitRAT	Ladrón de credenciales
#7	-	28	Nueva entrada	Oski	Herramienta de acceso remoto (RAT)
#8	18	26	44%	Vjw0rm	Ladrón de credenciales
#9	36	24	-33%	NjRAT	Ladrón de credenciales
#9	124	24	-81%	RemcosRAT	Troyano de banca en línea
#11	68	23	-66%	NanoCore	Herramienta de acceso remoto (RAT)
#11	55	23	-58%	AgentTesla	Herramienta de acceso remoto (RAT)
#11	-	23	Nueva entrada	Tofsee	Herramienta de acceso remoto (RAT)
#14	39	19	-51%	Arkei	Herramienta de acceso remoto (RAT)
#15	-	17	Nueva entrada	STRRAT	Ladrón de credenciales
#16	-	16	Nueva entrada	CryptBot	Ladrón de credenciales
#17	-	15	Nueva entrada	CobaltStrike	Herramienta de acceso remoto (RAT)
#18	-	14	Nueva entrada	ServHelper	Ladrón de credenciales
#18	-	14	Nueva entrada	IcedID	Dropper
#20	18	11	-39%	QuasarRAT	Dropper

Comparación de tipos de malware entre T1 y T2 2021



Dominios de nivel superior (TLD) con mayor abuso, T2 2021

.com

Para el segundo trimestre de 2021, gTLD .com volvió a quedar entre los primeros lugares de nuestra clasificación. Además, la cantidad de nuevos dominios registrados de botnet C&C observados en .com incrementó en 166%, ¡pasando de 1549 a 4113!

.xyz

Con un aumento repentino del 114% en este trimestre, no sorprende a nadie que gTLD .xyz haya sustituido a gTLD .top tomando el segundo lugar.

Dominios territoriales

Solo hubo dos nuevos ccTLD en los 20 principales de este trimestre: .br se posiciona en el #5 y .cn en el #12. Mientras tanto, tres ccTLD mejoraron su reputación y abandonaron la lista: .us, .de y .la.

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 un uso general, lo que ofrece la misma funcionalidad que la de los gTLD

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

Nuevas entradas

buzz (#3), br (#5), VIP (#6), cloud (#10), cn (#12), online (#16), live (#17).

Salidas

me, biz, cc, us, la, co, de.

Dominios de nivel superior (TLD) con mayor abuso, T2 2021 (continuación)

TLD con mayor abuso: cantidad de dominios

Clasificación	T1 2021	T2 2021	% cambio	TLD	Nota
#1	1549	4113	166%	com	gTLD
#2	345	739	114%	xyz	gTLD
#3	-	662	Nueva entrada	buzz	gTLD
#4	622	607	-2%	top	gTLD
#5	-	208	Nueva entrada	br	ccTLD
#6	-	175	Nueva entrada	vip	gTLD
#7	83	157	89%	org	gTLD
#8	114	151	32%	ru	ccTLD
#9	72	146	103%	net	gTLD
#10	-	141	Nueva entrada	cloud	gTLD
#11	124	140	13%	tk	Originalmente ccTLD, ahora efectivamente gTLD
#12	-	139	Nueva entrada	cn	ccTLD
#12	108	116	7%	eu	ccTLD
#14	121	106	-12%	ga	Originalmente ccTLD, ahora efectivamente gTLD
#15	106	104	-2%	ml	Originalmente ccTLD, ahora efectivamente gTLD
#16	-	86	Nueva entrada	online	gTLD
#17	-	81	Nueva entrada	live	gTLD
#18	51	80	57%	su	ccTLD
#19	46	78	70%	info	gTLD
#20	82	73	-11%	cf	ccTLD

Los registradores de dominio con mayor abuso, T2 2021

Después de muchos años sin cambios en los primeros puestos de la clasificación de reputación de los registradores, ¡por fin hay movimiento!

NameSilo

Observamos un incremento colosal de 594% en los nuevos registros de dominios de botnet C&C en el registrador de dominios de Estados Unidos, NameSilo, el cual le roba el primer lugar a Namecheap. Esto fue toda una hazaña teniendo en cuenta que NameCheap tuvo un incremento de 52% en relación con los nuevos registros de dominios de botnet C&C. ¡Son cifras gigantescas!

Alemania y China

No solo los registradores estadounidenses vieron incrementos significativos en el segundo trimestre. Los dos registradores alemanes de dominio, Key Systems (56%) y 1API (254%), también experimentaron un crecimiento en la cantidad de dominios de botnet registrados mediante sus servicios, como lo hicieron la mayoría de registradores chinos que se citan a continuación, incluido eName Technology, que se posicionó en nuestros 20 principales en el #3.

Nuevas entradas

eName Technology (#3), Arsys (#5), Xin Net (#10), CentralNic (#11), Network Solutions (#14).

Salidas

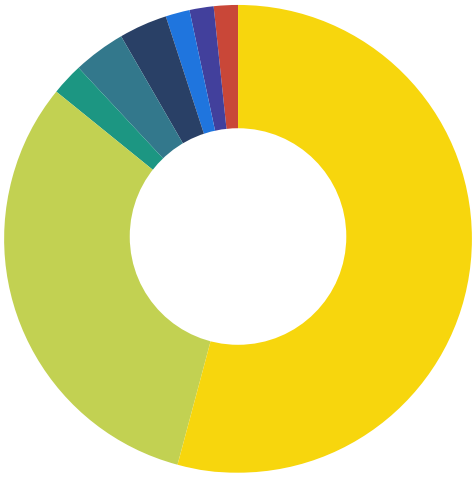
101 Domains, Bizcn, OnlineNIC, OVH, NameBright.

Los registradores de dominio con mayor abuso, T2 2021 (continuación)

Los registradores de dominio con mayor abuso: cantidad de dominios

Clasificación	T1 2021	T2 2021	% cambio	Registrador	País
#1	259	1797	594%	NameSilo	Estados Unidos
#2	628	955	52%	Namecheap	Estados Unidos
#3	-	526	Nueva entrada	eName Technology	China
#4	85	504	493%	Alibaba	China
#5	-	237	Nueva entrada	Arsys	España
#6	384	215	-44%	Eranet International	China
#7	72	188	161%	PDR	India
#8	238	135	-43%	RegRU	Rusia
#9	33	134	306%	HiChina	China
#10	-	125	Nueva entrada	Xin Net	China
#11	-	112	Nueva entrada	CentralNic	Reino Unido
#12	26	110	323%	22net	China
#12	29	110	279%	Tucows	Estados Unidos
#14	-	101	Nueva entrada	Network Solutions	Estados Unidos
#15	28	99	254%	1API	Alemania
#16	59	92	56%	Key Systems	Alemania
#17	56	91	63%	WebNic.cc	Singapur
#18	35	89	154%	Name.com	Estados Unidos
#19	50	80	60%	west263.com	China
#20	116	73	-37%	55hl.com	China

UBICACIÓN DE LOS REGISTRADORES DE DOMINIO CON MAYOR ABUSO



País	Botnets	%
Estados Unidos	3052	52,9%
China	1767	30,6%
España	237	2,3%
Alemania	191	3,3%
India	188	3,3%
Rusia	135	1,6%
Reino Unido	112	1,6%
Singapur	91	1,6%
Total	5773	

Redes que alojan los botnet C&C más recientes, T2 2021

Siempre hay mucho cambio en quienes alojan los botnet C&Cs más recientes. Y este trimestre no fue la excepción.

Operación de alojamiento blindado

En el segundo trimestre, una de las operaciones de alojamiento blindado de mayor envergadura se trasladó de Amazon a DigitalOcean. Como resultado de ello, la cantidad de botnet C&C nuevo en Amazon disminuyó rápidamente. Por el contrario, hubo un incremento repentino en los botnet C&C alojados en DigitalOcean.

Microsoft.com

Vimos a microsoft.com (EE. UU.) entrar en los 20 principales. Observamos que están alojando una cantidad significativa de infraestructura Vjw0rm y BitRAT botnet C&C.

Nuevas entradas

nano.lv (#6), mgnhost.ru (#8), baxet.ru (#10), ipjetable.net (#11), digitalocean.com (#12), internet.it (#14), hostsailor.com (#16), microsoft.com (#17), m247.ro (#8), offshoreracks.com (#19), mivocloud.com (#19).

Salidas

intersec.host, amazon.com, endurance.com, choopa.com, combahton.net, leaseweb.com, linode.com, ispserver.com colocrossing.com, dedipath.com, msk.host.

[2]https://www.spamhaus.org/statistics/networks/

Redes que alojan los botnet C&C más recientes, T2 2021 (continuación)

Botnet C&C recientemente descubierto por red

Clasificación	T1 2021	T2 2021	% cambio	Red	País
#1	35	82	134%	pq.hosting	Rusia
#2	53	74	40%	google.com	Estados Unidos
#3	21	68	224%	serverion.com	Países Bajos
#4	51	56	10%	ovh.com	Francia
#5	23	53	130%	itldc.com	Ucrania
#6	-	49	Nueva entrada	nano.lv	Letonia
#7	131	48	-63%	privacyfirst.sh	Alemania
#8	-	47	Nueva entrada	mgnhost.ru	Rusia
#9	19	46	142%	hetzner.de	Alemania
#10	-	40	Nueva entrada	baxet.ru	Rusia
#11	-	35	Nueva entrada	ipjetable.net	Francia
#12	45	29	-36%	cloudflare.com	Estados Unidos
#12	-	29	Nueva entrada	digitalocean.com	Estados Unidos
#14	-	28	Nueva entrada	Internet.it	Rusia
#15	26	26	0%	alibaba-inc.com	China
#16	-	25	Nueva entrada	hostsailor.com	EAU
#17	-	22	Nueva entrada	microsoft.com	Estados Unidos
#18	-	21	Nueva entrada	m247.ro	Rumanía
#19	-	16	Nueva entrada	offshoreracks.com	Panamá
#19	-	16	Nueva entrada	mivocloud.com	Moldavia

Redes que alojan los botnet C&C más activos, T2 2021

Finalmente, echemos un vistazo a las redes que alojaron una gran cantidad de botnet C&C activos en el segundo trimestre del 2021. Los proveedores de alojamiento que aparecen en esta clasificación tienen un problema de abuso o no toman las medidas adecuadas cuando reciben los informes de abuso.

Nuevas entradas

m247.ro (#12), eliteteam.to (#13), mgnhost.ru (#13), unusinc.com (#17).

Salidas

mail.ru, digitalocean.com, eurobyte.ru, telstra.com.

Eliteteam.to

Esta es una empresa de alojamiento blindado que pretende estar ubicada en las Seychelles. En realidad, lo más probable es que opere desde Rusia.

Microsoft.com y google.com

Es evidente que Microsoft está luchando con la cantidad de abuso generado en su plataforma de nube Azure. De la misma forma, google.com también se ve asediado por informes de abuso.

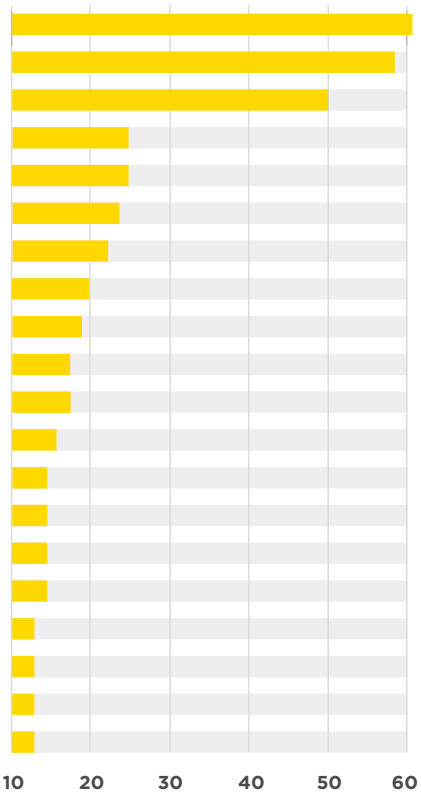
¡Bien por los que se van!

Queremos reconocer a todos los que han dejado de formar parte de esta lista. Es bueno ver que la cantidad de botnet C&C está reduciendo en tu red. ¡Bien hecho!

Redes que alojan los botnet C&C más activos, T2 2021 (continuación)

Cantidad total de botnet C&C activos por red

Clasificación	T4 2020	T1 2021	% cambio	Red	País
#1	33	61	85%	ipjetable.net	Francia
#2	48	58	21%	microsoft.com	Estados Unidos
#3	43	50	16%	google.com	Estados Unidos
#4	23	23	0%	ttnet.com.tr	Turquía
#4	21	23	10%	vietserver.vn	Vietnam
#6	22	21	-5%	charter.com	Estados Unidos
#6	21	21	0%	inmotionhosting.com	Estados Unidos
#8	17	20	18%	ovpn.com	Suecia
#9	18	18	0%	clouvider.net	Reino Unido
#10	12	17	42%	hostry.com	Chipre
#10	17	17	0%	une.net.co	Colombia
#12	-	15	Nueva entrada	m247.ro	Rumanía
#13	17	13	-24%	datawire.ch	Suiza
#13	-	13	Nueva entrada	eliteteam.to	Seychelles
#13	13	13	0%	mtnnigeria.net	Nigeria
#13	-	13	Nueva entrada	mgnhost.ru	Rusia
#17	18	12	-33%	claro.com.co	Colombia
#17	12	12	0%	kornet.net	Corea del sur
#17	14	12	-14%	chinanet-js	China
#17	-	12	Nueva entrada	unusinc.com	Estados Unidos



Y esto es todo por ahora.

¡Cuídate y nos vemos en octubre!