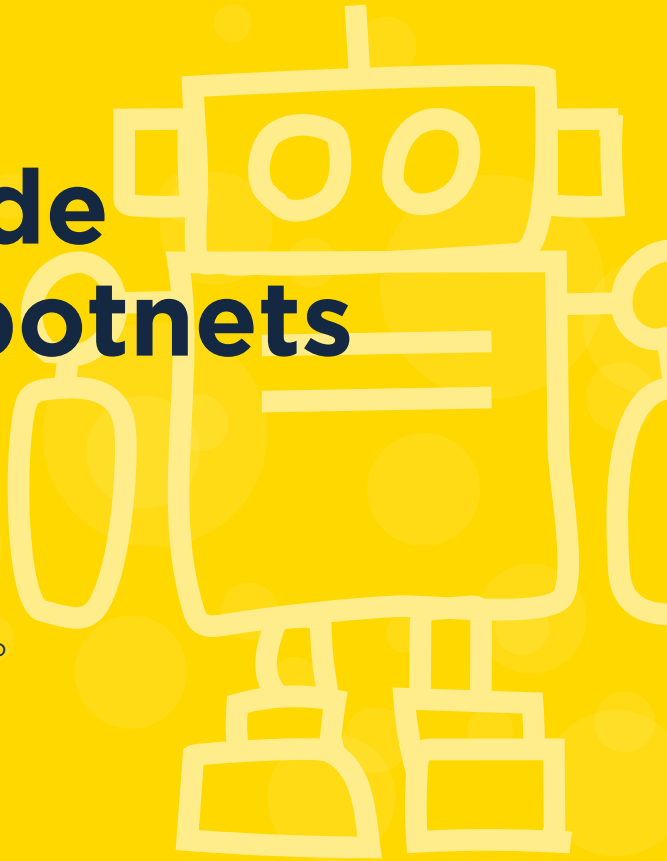
SPAMHAUS

Actualización de amenazas de botnets de Spamhaus



T1 2021

Tras un fin de año 2020 tranquilo, o medio tranquilo, en el mundo de botnets de Spamhaus, el primer trimestre de este año arrancó con toda la actitud. La noticia más importante tuvo que ver con el desmantelamiento de la botnet Emotet en enero. Sin embargo, cuando se erradica un malware, surge otro, como lo muestra el incremento de 24% en la cantidad total de botnet C&C que los investigadores de Spamhaus han observado.

Te damos la bienvenida a la actualización de amenazas de botnets de Spamhaus T1 2021.

¿Qué son los 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 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 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 están en riesgo de infectarse.

Destacamos

Emotet ha desaparecido, pero están emergiendo otras amenazas

En enero de 2021, una coalición internacional que incluía autoridades de diversos países emprendió medidas globales contra la infame botnet Emotet. Los organismos del orden público desactivaron la infraestructura operada por la pandilla Emotet, enviando el tráfico de la botnet Emotet al atolladero.

La operación parece haber sido todo un éxito. No hubo detenciones relacionadas con esta operación, pero la botnet lleva más de dos meses inactiva. No obstante, los expertos en malware de Spamhaus estiman que es muy probable que Emotet vuelva a circular.

En los últimos años, Emotet floreció hasta ser conocida como una de las amenazas de mayor peligro en la red. Los delincuentes la utilizaron para tener un punto de partida en las redes corporativas, permitiéndoles moverse lateralmente dentro de la red de las víctimas, lo que en muchos casos llevó al cifrado con ransomware.

Desafortunadamente, no hay descanso en el mundo de las botnets: en cuanto se extingue una botnet, surge otra para reemplazarla. Rápidamente, otros operadores de botnet se han apresurado para llenar el vacío que dejó Emotet.

Este trimestre, los delincuentes que operan botnets como IcedID, Dridex, Quakbot y TrickBot enviaron grandes volúmenes de correo electrónico de spam con documentos maliciosos. Para la mayoría de estas amenazas, el modus operandi es similar al de Emotet, es decir, entrar en las redes corporativas y cifrarlas con ransomware.

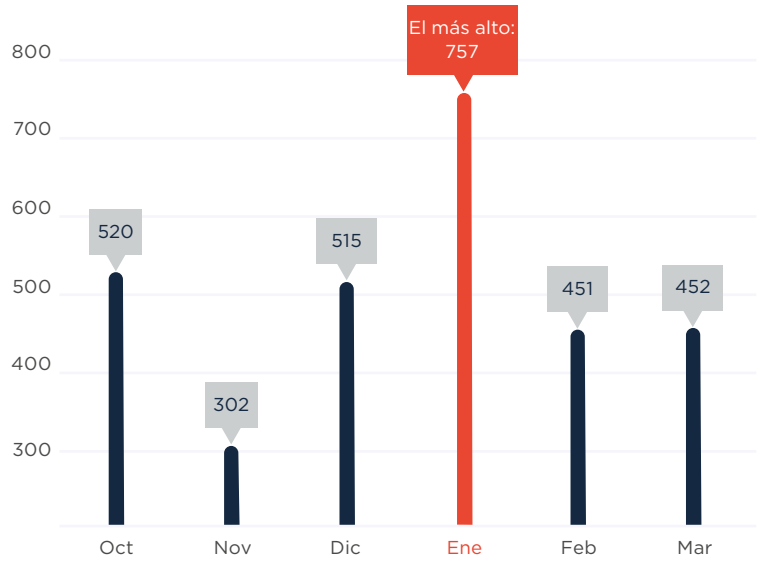
Emotet

Emotet es un antiguo troyano de banca en línea que atacaba a clientes de banca en línea en todo el mundo. En 2018, Emotet cesó sus actividades de fraude de banca en línea y empezó a ofrecer computadoras infectadas mediante un modelo de “Pago por instalación”. Desde el 2019, Emotet se convirtió en una de las botnets más peligrosas.

Cantidad de botnet C&C observados en T1 2021

Primero, veamos la cantidad de nuevos servidores botnet Command & Control (C&C) en el primer trimestre de 2021. En total, Spamhaus Malware Labs identificó 1660 nuevos botnet C&C en comparación con los 1337 del cuarto trimestre del 2020. Esto significa un aumento de 24%, con un promedio de 553 botnet C&C al mes.

Cantidad de nuevos botnet C&C detectados por Spamhaus desde finales del 2020:



T4 Promedio mensual: 445

T1 Promedio mensual: 553

Geolocalización de botnet C&C, T1 2021

En algunos países, hemos visto un incremento de nuevos botnet C&C, mientras que otros países han salido de nuestra lista de los 20 principales.

Estados Unidos sigue en el #1

A pesar de una pequeña disminución de 3% en la cantidad de nuevas botnets observadas, Estados Unidos se mantiene en las primeras posiciones de la clasificación.

Incrementos en Europa

Países Bajos supera Rusia y se posiciona en segundo lugar, con un total de 207 botnets, un incremento de 27% en el cuarto trimestre de 2020.

Otros países europeos han visto incrementos de nuevas infraestructuras de botnet, entre los cuales Alemania (+77%), Francia (+82%), Suiza (+23%) y Reino Unido (+9%).

Nuevas entradas

Moldavia (#11), Hong Kong (#15), Argentina (#18), Colombia (#18).

Salidas

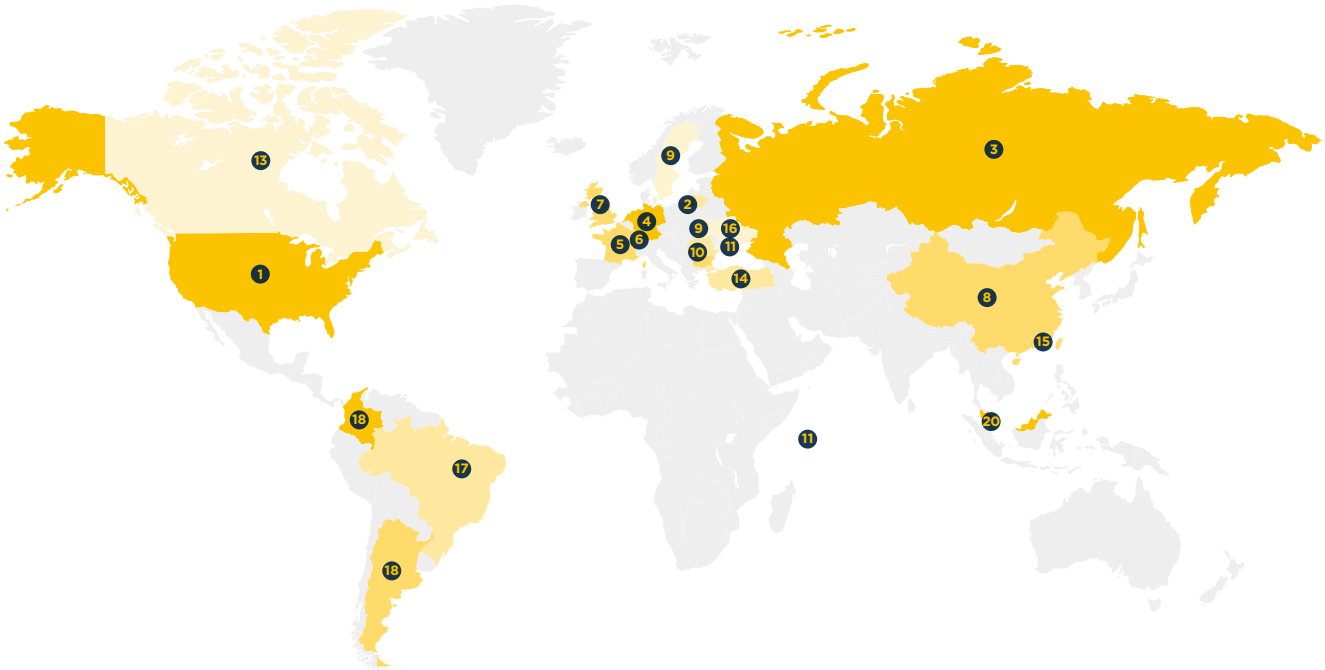
Bulgaria, Hungría, India, Vietnam

Geolocalización de botnet C&C, T1 2021 (continuación)

20 principales localizaciones de botnet C&C

Clasificación	País	T4 2020	T1 2021	% cambio T a T
#1	Estados Unidos	348	338	-3%
#2	Países Bajos	163	207	27%
#3	Rusia	247	195	-21%
#4	Alemania	56	99	77%
#5	Francia	39	71	82%
#6	Suiza	48	59	23%
#7	Reino Unido	45	49	9%
#8	China	32	42	31%
#9	Suecia	34	39	15%
#10	Letonia	24	31	29%

Clasificación	País	T4 2020	T1 2021	% cambio T a T
#11	Seychelles	10	29	190%
#11	Moldavia	-	29	Nueva entrada
#13	Canadá	11	25	136%
#14	Turquía	17	20	47%
#15	Hong Kong	-	24	Nueva entrada
#16	Ucrania	16	22	38%
#17	Brasil	8	20	150%
#18	Argentina	-	18	Nueva entrada
#18	Colombia	-	18	Nueva entrada
#20	Singapur	31	16	-48%



Malware asociado con botnet C&C, T1 2021

Emotet:

En el primer trimestre de 2021, Emotet se posicionó en los primeros lugares de estos 20 principales. No fue ninguna sorpresa dados nuestros esfuerzos por ayudar a los organismos del orden público a desmantelar la infraestructura de la botnet Emotet en enero de 2021.

Raccoon:

Raccoon es un ladrón de credenciales recién llegado. En el primer trimestre de 2021, identificamos 45 botnet C&C asociados con este nuevo malware.

FickerStealer:

Otro ladrón de credenciales visto por primera vez en el primer trimestre de 2021 es FickerStealer con 25 nuevos botnet C&C asociados.

QNodeService:

La primera vez que detectamos este malware fue en 2020. Sin embargo, parece que la actividad de QNodeService desapareció a principios de este año. A la fecha, no hemos observado ningún C&C asociado.

Nuevas entradas

Emotet (#1), Raccoon (#8), Gozi (#10), BitRat (#12), FickerStealer (#15), Vjw0rm (#17), TriumphLoader (#17), Hancitor (#20)

Salidas

Mirai, QNodeService, BazaLoader, ZLoader, CobaltStrike, Smoke Loader, Dridex, RevengeRAT

Malware asociado con botnet C&C, T1 2021 (continuación)

Familias de malware asociadas con botnet C&C

Clasificación	T4 2020	T1 2021	% cambio	Familia de malware	Descripción
#1	-	272	Nueva entrada	Emotet	Dropper
#2	53	124	134%	RemcosRAT	Herramienta de acceso remoto (RAT)
#3	164	83	-49%	Loki	Ladrón de credenciales
#4	29	69	138%	AsyncRAT	Herramienta de acceso remoto (RAT)
#5	71	68	-4%	NanoCore	Herramienta de acceso remoto (RAT)
#6	66	55	-17%	RedLine	Ladrón de credenciales
#6	93	55	-41%	AgentTesla	Herramienta de acceso remoto (RAT)
#8	-	45	Nueva entrada	Raccoon	Ladrón de credenciales
#9	17	39	129%	Arkei	Ladrón de credenciales
#10	-	38	Nueva entrada	Gozi	Troyano de banca en línea
#11	30	36	20%	NjRAT	Herramienta de acceso remoto (RAT)
#12	21	33	57%	NetWire	Herramienta de acceso remoto (RAT)
#12	-	33	Nueva entrada	BitRAT	Herramienta de acceso remoto (RAT)
#14	38	30	-21%	AveMaria	Herramienta de acceso remoto (RAT)
#15	-	25	Nueva entrada	FickerStealer	Ladrón de credenciales
#16	47	24	-49%	AZORult	Ladrón de credenciales
#17	15	18	20%	QuasarRAT	Herramienta de acceso remoto (RAT)
#17	-	18	Nueva entrada	Vjw0rm	Ladrón de credenciales
#17	-	18	Nueva entrada	TriumphLoader	Dropper
#20	-	17	Nueva entrada	Hancitor	Dropper

Dominios de nivel superior con mayor abuso, T1 2021

Durante el primer trimestre de 2021, el gTLD .com se mantiene en los primeros lugares de nuestra clasificación. Una gran mayoría de dominios de botnet C&C que Spamhaus Malware Labs identificó estaban alojados en este TLD. Sin embargo, hemos visto como muchos otros TLD listados mejoraron su reputación con reducciones generalizadas.

.de:

El ccTLD de Alemania volvió a entrar en los 20 principales ocupando el #19. ¡Qué mal! ¿Se debe esto a una política antiabuso débil en DENIC?

.top y .xyz:

Estos dos gTLD tienen una larga historia de abuso, y no sorprende que sigan estando entre los primeros cinco, especialmente dado que .top ha visto un incremento de 90% en la cantidad de botnet C&C alojada durante el primer trimestre de 2021.

Dominios de nivel superior (TLD): un breve repaso

Hay varios dominios de nivel superior 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, ofreciendo la misma funcionalidad que la de los gTLD

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

Nuevas entradas

ru (#6), org (#10), biz (#12), us (#15), info (#18), co (#19), de (#19)

Salidas

casa, br, cyou, kr, ai, ac, gq

Dominios de nivel superior con mayor abuso, T1 2021 (continuación)

Familias de malware asociadas con botnet C&C

Clasificación	T4 2020	T1 2021	% cambio	TLD	Nota
#1	2108	1549	-27%	com	gTLD
#2	328	622	90%	top	gTLD
#3	505	345	-32%	xyz	gTLD
#4	141	124	-12%	tk	Originalmente ccTLD, ahora efectivamente gTLD
#5	185	121	-35%	ga	Originalmente ccTLD, ahora efectivamente gTLD
#6	-	114	Nueva entrada	ru	ccTLD
#7	100	108	8%	eu	ccTLD
#8	133	106	-20%	ml	Originalmente ccTLD, ahora efectivamente gTLD
#9	95	87	-8%	me	gTLD
#10	-	83	Nueva entrada	org	gTLD
#11	94	82	-13%	cf	Originalmente ccTLD, ahora efectivamente gTLD
#12	-	72	Nueva entrada	biz	gTLD
#12	81	72	-11%	net	gTLD
#14	138	66	-52%	cc	gTLD
#15	-	55	Nueva entrada	us	ccTLD
#16	77	51	-34%	su	ccTLD
#17	74	47	-36%	la	ccTLD
#18	-	46	Nueva entrada	info	gTLD
#19	-	36	Nueva entrada	co	ccTLD
#19	-	36	Nueva entrada	de	ccTLD

Los registradores de dominio con mayor abuso, T1 2021

Namecheap (¡otra vez!)

Después de años de estar en el #1 en estos 20 principales, Namecheap (EE. UU.) sigue siendo el registrador de dominios preferido por los delincuentes que registran dominios de botnet C&C.

¿Cuándo cambiará esto? No lo sabemos, pero, dada la larga historia de abuso en Namecheap, no esperamos que sea en un futuro cercano.

Eranet International y RegRU

Con un incremento masivo de 249%, Eranet International (China) desbancó a NameSilo (Estados Unidos) de la posición que ocupaba en segundo lugar. Sin embargo, el aumento más significativo en la cantidad de registros de dominio de botnet C&C le pertenece a RegRU (Rusia), con un enorme incremento de 341%.

Nuevas entradas

OnlineNIC (#13), name.com (#15), HiChina (#16), NameBright (#17)

Salidas

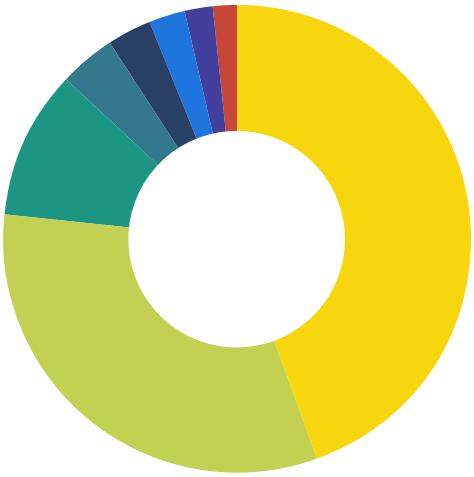
URL Solution, Hosting Concepts

Los registradores de dominio con mayor abuso, T1 2021 (continuación)

Los registradores de dominio con mayor abuso: cantidad de dominios

Clasificación	T4 2020	T1 2021	% cambio	Registrador	País
#1	822	628	-24%	Namecheap	Estados Unidos
#2	110	384	249%	Eranet International	China
#3	444	259	-42%	NameSilo	Estados Unidos
#4	54	238	341%	RegRU	Rusia
#5	115	116	1%	55hl.com	China
#6	101	85	-16%	Alibaba	China
#7	343	72	-79%	PDR	India
#8	367	59	-84%	Key Systems	Alemania
#9	111	56	-50%	WebNic.cc	Singapur
#10	65	50	-23%	west263.com	China
#11	25	44	76%	101Domain	Irlanda
#12	48	42	-13%	Bizcn	China
#13	-	38	Nueva entrada	OnlineNIC	Estados Unidos
#14	32	36	13%	OVH	Francia
#15	-	35	Nueva entrada	name.com	Estados Unidos
#16	-	33	Nueva entrada	HiChina	China
#17	-	30	Nueva entrada	NameBright	Estados Unidos
#18	53	29	-45%	Tucows	Estados Unidos
#19	46	28	-39%	1API	Alemania
#20	29	26	-10%	22net	China

UBICACIÓN DE LOS REGISTRADORES DE DOMINIO CON MAYOR ABUSO



País	Botnets	%
Estados Unidos	1019	44,5%
China	736	32,2%
Rusia	238	10,4%
Alemania	87	3,8%
India	72	3,1%
Singapur	56	2,4%
Irlanda	44	1,9%
Francia	36	1,6%

Redes que alojan los botnet C&C más recientes, T1 2021

En este trimestre, hemos visto una separación entre oriente y occidente, con una reducción en la cantidad de botnet C&C alojados en proveedores de oriente, rápidamente reemplazados por proveedores de servicios en la nube en occidente.

Proveedores de servidores virtuales privados (VPS) rusos

En este trimestre, diversas empresas como invs.ru y selectel.ru salieron de la lista de los 20 principales. Estas son noticias muy buenas, especialmente en lo que respecta a selectel.ru, que formó parte de la lista de los 20 principales durante mucho tiempo.

Proveedores occidentales de VPS

Diversos proveedores ubicados en occidente han ingresado en la lista de los 20 principales en el primer trimestre de 2021, entre ellos google.com, choopa.com, hetzner.de y combahton.net.

Los peores y los que más han mejorado

La red con más abuso es privacyfirst.sh, un proveedor de VPN que opera desde Alemania. En cambio, amazon.com ha reducido 44% la cantidad de nuevos botnet C&C en su red en este último trimestre. ¡Un paso positivo hacia adelante!

Nuevas entradas

Google.com (#2), intersect.host (#6), choopa.com (#12) hetzner.de (#13), combahton.net (#13), linode.com (#16), ispserver.com (#17), colocrossing.com (#17), msk.host (#17)

Salidas

invs.ru, m247.ro, selectel.ru, namecheap.com, digitalocean.com, maxko.org, tencent.com, baxet.ru, belcloud.net

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

Redes que alojan los botnet C&C más recientes, T1 2021 (continuación)

Botnet C&C recientemente descubierto por red

Clasificación	T4 2020	T1 2021	% cambio	Red	País
#1	106	131	24%	privacyfirst.sh	Alemania
#2	-	53	Nueva entrada	google.com	Estados Unidos
#3	33	51	55%	ovh.com	Francia
#4	47	45	-4%	cloudflare.com	Estados Unidos
#5	15	35	133%	pq.hosting	Moldavia
#6	-	32	Nueva entrada	intersect.host	Seychelles
#7	55	31	-44%	amazon.com	Estados Unidos
#8	45	28	-38%	endurance.com	Estados Unidos
#9	26	26	0%	alibaba-inc.com	China
#10	15	23	53%	itldc.com	Ucrania
#11	17	21	24%	serverion.com	Países Bajos
#12	-	20	Nueva entrada	choopa.com	Estados Unidos
#13	-	19	Nueva entrada	hetzner.de	Alemania
#13	-	19	Nueva entrada	combahton.net	Alemania
#13	28	19	-32%	leaseweb.com	Países Bajos
#16	-	18	Nueva entrada	linode.com	Estados Unidos
#17	-	17	Nueva entrada	ispserver.com	Rusia
#17	-	17	Nueva entrada	colocrossing.com	Estados Unidos
#17	25	17	-32%	dedipath.com	Estados Unidos
#17	-	17	Nueva entrada	msk.host	Rusia

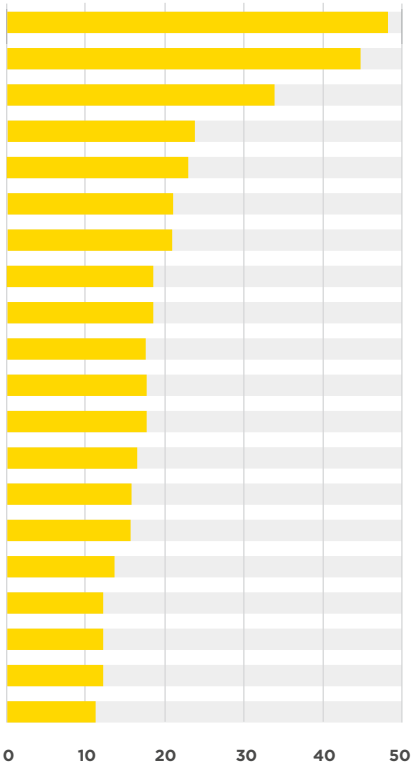
Redes que alojan los botnet C&C más activos, T1 2021

Por último, mas no por ello menos importante, echemos un vistazo a las redes que alojaron sistemáticamente una gran cantidad de botnet C&C activos. Desafortunadamente, Microsoft lidera esta lista de los 20 principales, con 48 botnet C&C activos, seguida por Google con 43 botnet C&C activos.

Las redes que aparecen en este listado tienden a tener una falta de higiene de red y no toman medidas cuando reciben quejas de abuso; un hecho que queda patente al no observarse cambios entre trimestres. ¡Las botnets se mantienen activas durante meses!

Cantidad total de botnet C&C activos por red

Clasificación	T4 2020	T1 2021	% cambio	Red	País
#1	48	48	0%	microsoft.com	Estados Unidos
#2	43	43	0%	google.com	Estados Unidos
#3	33	33	0%	ipjetable.net	Suiza
#4	23	23	0%	ttnet.com.tr	Turquía
#5	22	22	0%	charter.com	Estados Unidos
#6	21	21	0%	inmotionhosting.com	Estados Unidos
#6	21	21	0%	vietserver.vn	Vietnam
#8	18	18	0%	claro.com.co	Colombia
#8	18	18	0%	cloudvider.net	Reino Unido
#10	17	17	0%	ovpn.com	Suecia
#10	17	17	0%	une.net.co	Colombia
#10	17	17	0%	datawire.ch	Suiza
#13	16	16	0%	mail.ru	Rusia
#14	14	14	0%	chinanet-js	China
#14	14	14	0%	digitalocean.com	Estados Unidos
#16	13	13	0%	mtnnigeria.net	Nigeria
#17	12	12	0%	kornet.net	Corea
#17	12	12	0%	hostry.com	Chipre
#19	12	11	-8%	eurobyte.ru	Rusia
#19	11	11	0%	telstra.com	Australia



Dados los eventos relacionados con Emotet durante el primer trimestre de 2021, será muy interesante ver qué sucederá en el próximo trimestre.

Nos vemos el próximo trimestre. Mientras tanto, cuídate.