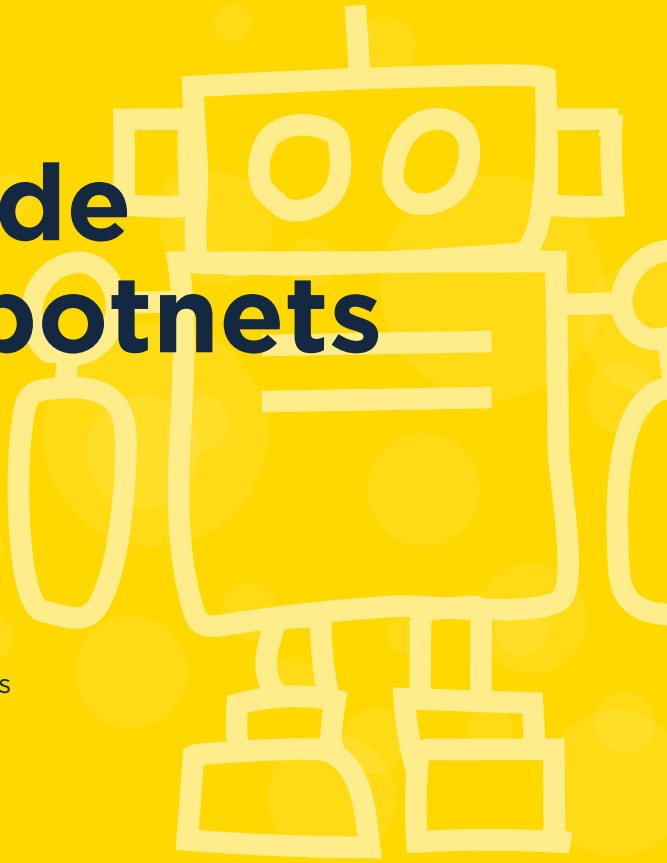
SPAMHAUS

Actualización de amenazas de botnets de Spamhaus



T3 de 2021

En el T3, presenciamos un gran aumento de 82% con respecto a la cantidad de nuevos comando y controladores de botnets (C&C) identificados por nuestro equipo de investigadores, los cuales han observado una explosión en el uso de malware de puerta trasera: los individuos malintencionados utilizan FastFlux para ocultarse, lo que motivó la aparición de varios países y proveedores de servicios nuevos en nuestras listas de los 20 principales.

Te damos la bienvenida a la actualización de amenazas de botnets de Spamhaus, T3 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

FastFlux vuelve a la vida

Después de analizar las estadísticas de este trimestre, es evidente que FastFlux vuelve a cobrar popularidad. Aquí tienes una rápida actualización sobre FastFlux, que incluye información sobre cómo los cibercriminales lo utilizan para impedir el desmantelamiento de su infraestructura.

¿Qué es FastFlux?

FastFlux es una técnica que utilizan los suplantadores de identidad, creadores de malware y operadores de botnet para ocultar la ubicación de su infraestructura tras la red de un servidor comprometido que actúa como proxy y envía el tráfico malicioso al backend auténtico.

¿Por qué FastFlux es tan atractivo para los cibercriminales?

Todas las redes FastFlux que operan actualmente pueden alquilarse como servicio en la web oscura, lo que les facilita la vida a los operadores de botnet. Lo único que necesitan es registrar los dominios necesarios para los botnet C&C y dirigirlos hacia el servicio del operador de FastFlux. FastFlux se encarga de todo lo demás y se asegura de que los registros A cambien con rapidez.

Aquí tienes un ejemplo de dominio para un botnet C&C de FluBot alojado en una botnet de FastFlux:

```
;; APARTADO DE PREGUNTAS:
;gurbngbcxheshsj.ru.      IN   A

;; APARTADO DE RESPUESTAS:
```

Dominio	TTL	Tipo de registro		Dirección IP
gurbngbcxheshsj.ru.	150	IN	A	189.165.94.67
gurbngbcxheshsj.ru.	150	IN	A	124.109.61.160
gurbngbcxheshsj.ru.	150	IN	A	187.190.48.60
gurbngbcxheshsj.ru.	150	IN	A	115.91.217.231
gurbngbcxheshsj.ru.	150	IN	A	175.126.109.15
gurbngbcxheshsj.ru.	150	IN	A	175.119.10.231
gurbngbcxheshsj.ru.	150	IN	A	218.38.155.210
gurbngbcxheshsj.ru.	150	IN	A	179.52.22.168
gurbngbcxheshsj.ru.	150	IN	A	113.11.118.155
gurbngbcxheshsj.ru.	150	IN	A	14.51.96.70

¿Qué es FluBot?

FluBot es un troyano que infecta los dispositivos Android. Roba las credenciales del usuario y se propaga convirtiendo el smartphone infectado en un zombi para enviar spam por SMS.

Como puedes ver, el dominio del botnet C&C utiliza diez registros A concurrentes con un tiempo de vida (TTL) de solo 150 segundos. El monitoreo de estos registros A revela que la botnet de FastFlux subyacente consta de entre 100 y 150 nodos FastFlux activos al día.

Por lo general, estos nodos son dispositivos comprometidos, normalmente equipo local del cliente(CPE) configurado de manera poco segura (p.ej, que utiliza software vulnerable o credenciales de acceso estándares), al que puede accederse directamente desde Internet.

Este tipo de dispositivos son presa fácil para los cibercriminales. Solo tienen que realizar un rastreo en Internet para descubrir estos dispositivos vulnerables y comprometerlos. Todo este proceso puede automatizarse por completo para que se realice de forma rápida, sencilla y eficaz.

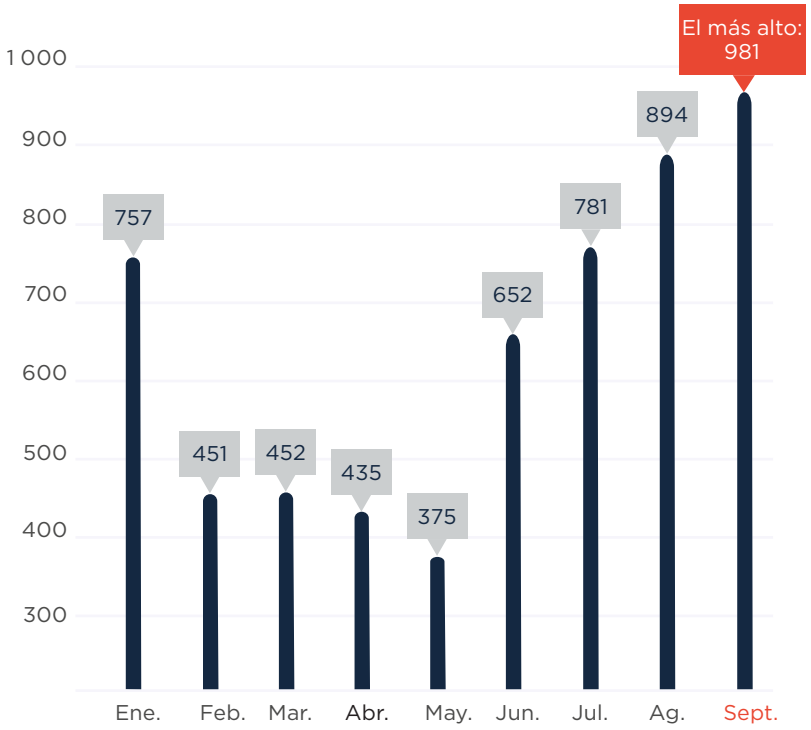
Los operadores de botnets de FastFlux eligen cuidadosamente la ubicación geográfica de los dispositivos que utilizan para el alojamiento de FastFlux. Como observarás al leer este informe, muchos nodos de C&C FastFlux están alojados en lugares que están relativamente bien "digitalizados", es decir, tienen buenas conexiones a Internet, pero no están en una posición tan avanzada en la curva de madurez en cuanto a la ciberseguridad.

Latinoamérica es un objetivo habitual, por ejemplo Brasil, Chile, Argentina y Uruguay, además de países asiáticos como Corea. Esto se refleja en las nuevas entradas en las estadísticas de ubicación geográfica de esta actualización.

Cantidad de botnet C&C observados en el T3 de 2021

En el T3 de 2021, Spamhaus Malware Labs identificó 2 656 botnet C&C en comparación con 1 462 en el T2 de 2021. ¡Un aumento del 82% en el trimestre! El promedio mensual aumentó de 487 por mes en el segundo trimestre a 885 botnet C&C por mes en el tercero.

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



Trimestre	Cantidad de botnets	Promedio trimestral	% de cambio
T1	1 660	553	24%
T2	1 462	487	-12%
T3	2 656	885	82%

¿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 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 corren el riesgo de infectarse.

Localización geográfica de botnet C&C, T3 de 2021

Con la influencia de FastFlux en el último trimestre, no sorprende comprobar que existe un claro patrón entre las nuevas entradas en la lista del T3 de 2021. Muchos de los países que aparecen en las listas alojaron un gran porcentaje de los servidores de botnet C&C de TeamBot y de FluBot —utilizando Fastflux— y encajan en el perfil de países con una amplia cobertura de Internet, pero con un deficiente enfoque en la seguridad.

Nuevas entradas

México (#4), Arabia Saudita (#7), República Dominicana (#8), Corea (#10), Uruguay (#11), Argentina (#14), Suecia (#18) y Rumanía (#20).

Salidas

Ucrania, Seychelles, Panamá, Canadá, Malasia, Polonia, Finlandia y Turquía.

Aumento significativo en Rusia

La cantidad de botnet C&C ubicados en Rusia aumentó notablemente. Se trata de la segunda subida intertrimestral que experimenta Rusia:

- T1 al T2: aumento del 19%
- T2 al T3: aumento del 64%

Por lo tanto, no sorprende que en el T3 Rusia le arrebatara a Estados Unidos el primer lugar.

Incrementos continuos en Europa

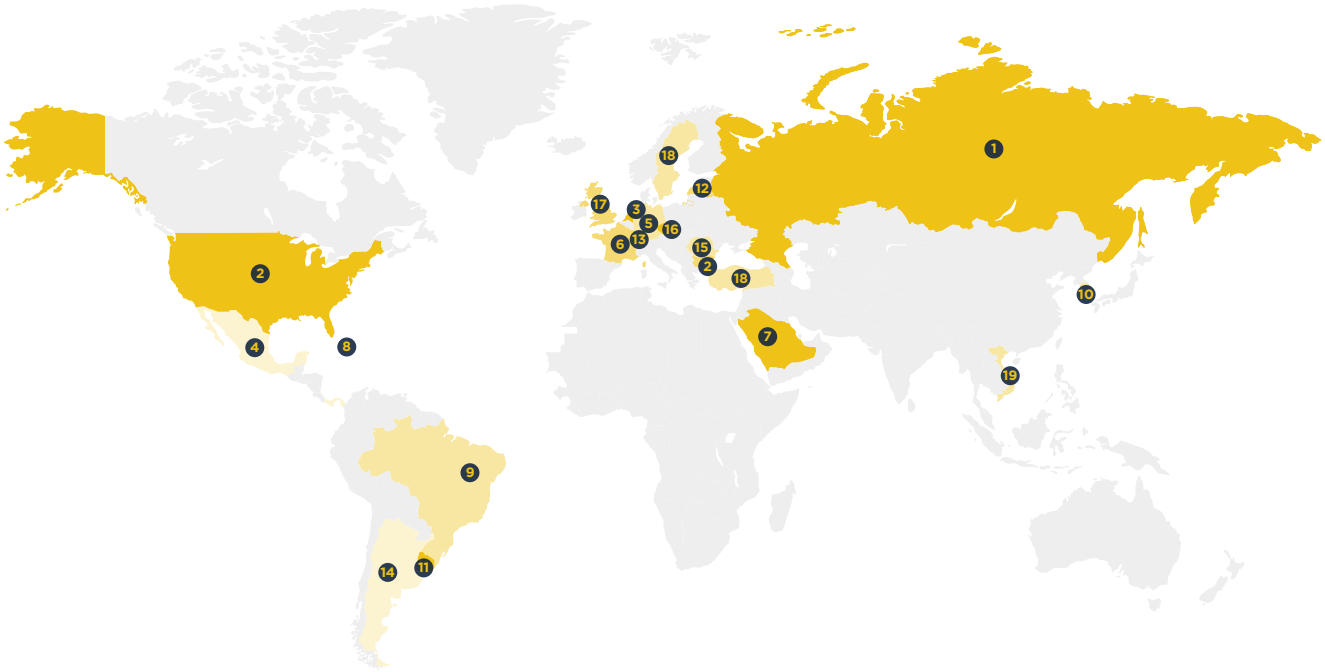
La tendencia iniciada en el T2 continuó en el T3. De nuevo, se produjo un aumento en la cantidad de servidores de botnet C&C alojados en varios países europeos, como Países Bajos (+63%), Alemania (+45%), Francia (+34%) y Suiza (+34%).

Localización geográfica de botnet C&C, T3 de 2021 (continuación)

20 principales localizaciones de botnet C&C

Clasificación	País	T2 2021	T3 2021	% de cambio de T a T
#1	Rusia	233	381	64%
#2	Estados Unidos	281	301	7%
#3	Países Bajos	168	273	63%
#4	México	-	182	Nueva entrada
#5	Alemania	117	170	45%
#6	Francia	92	123	34%
#7	Arabia Saudita	-	117	Nueva entrada
#8	Rep. Dominicana	-	96	Nueva entrada
#9	Brasil	12	86	617%
#10	Corea	-	68	Nueva entrada

Clasificación	País	T2 2021	T3 2021	% de cambio de T a T
#11	Uruguay	-	63	Nueva entrada
#12	Letonia	84	58	-31%
#13	Suiza	41	55	34%
#14	Argentina	-	50	Nueva entrada
#15	Moldavia	29	49	69%
#16	Rep. Checa	31	40	29%
#17	Reino Unido	57	39	-32%
#18	Suecia	-	38	Nueva entrada
#19	Vietnam	13	34	162%
#20	Rumanía	-	33	Nueva entrada



Malware asociado con botnet C&C, T3 de 2021

Estas son las principales familias de malware relacionadas con los botnet C&C más recientes en el T3 de 2021.

Auge de TeamBot y FluBot

¿Habías oído hablar de TeamBot? Probablemente no. Aunque no es nuevo ni constituye una amenaza grave, TeamBot comparte las principales posiciones en las listas con FluBot, ambos son malware de puerta trasera.

Nuestros investigadores de amenazas creen que TeamBot y FluBot utilizan la misma infraestructura de FastFlux, rotando las mismas direcciones IP de los botnet C&C cada pocos minutos, por lo que se incluyen bajo el mismo epígrafe en la tabla.

Este trimestre se produjo una explosión de malware de puerta trasera, que se convirtió en el tipo de malware más habitual asociado con botnet C&C en el T3 de 2021.

RedLine gana, Raccoon pierde

En 2021, presenciamos una pelea por la primera posición entre RedLine y Raccoon, dos ladrones de credenciales que están a la venta en la web oscura. Al tiempo que los servidores de botnet C&C de Raccoon experimentaban un enorme incremento (571%) en el T2 de 2021, el malware RedLine presentó un aumento del 71% en el T3 de 2021 y desplazó a Raccoon de la primera posición.

IcedID desaparece

IcedID permaneció relativamente inactivo este año, con solo una breve aparición en el #18 en el T2 antes de volver a desaparecer este trimestre. Desconocemos los motivos. No obstante, nuestros investigadores no creen que este silencio continuará indefinidamente. IcedID es uno de los troyanos disponibles para grupos de ransomware a la venta en la web oscura. Estos troyanos venden el acceso a redes corporativas, un negocio muy lucrativo.

¿Qué es el malware de puerta trasera?

Este tipo de malware sortea los procedimientos de autenticación y otras medidas de seguridad habituales para obtener acceso de alto nivel a un sistema, red o aplicación.

Nuevas entradas

TeamBot (#1), FluBot (#1) Smoke Loader (#9) y AveMaria (#13).

Salidas

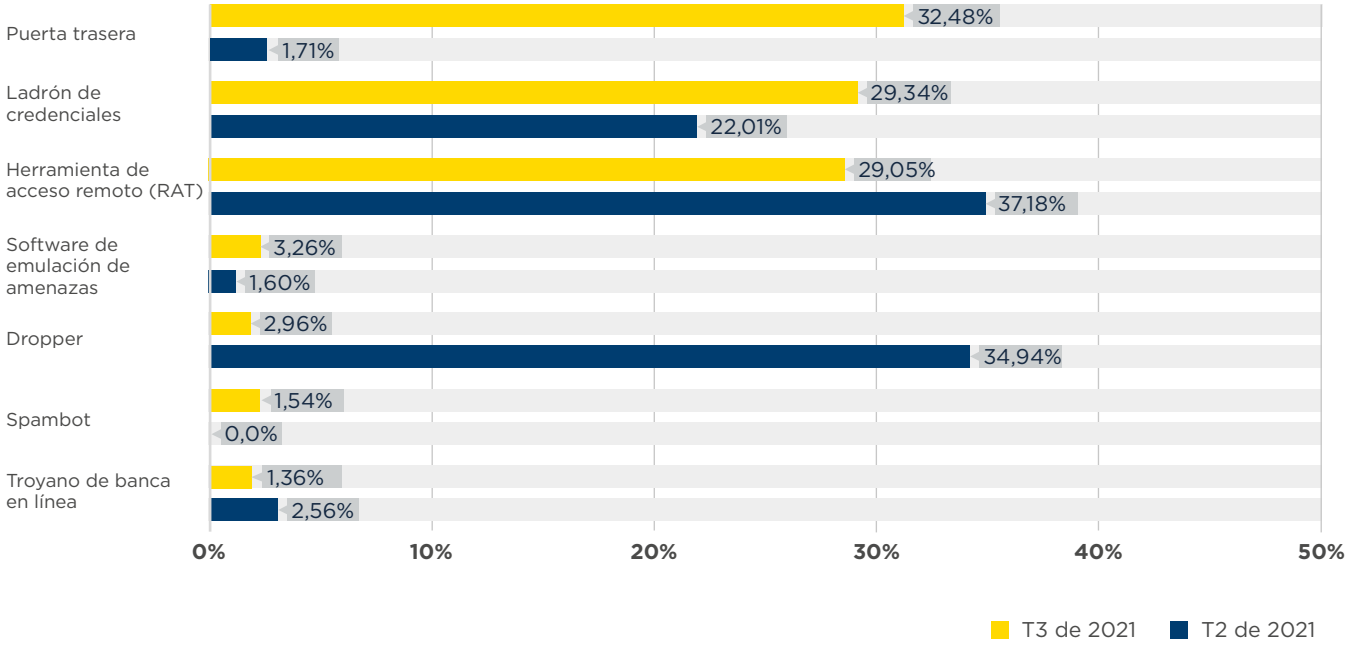
Oski, IcedID y Arkei.

Malware asociado con botnet C&C, T3 de 2021 (continuación)

Familias de malware asociadas con botnet C&C

Clasificación	T2 2021	T3 2021	% de cambio	Familia de malware	Descripción
#1	-	507	Nueva entrada	TeamBot & FluBot	Puerta trasera
#2	123	210	71%	RedLine	Ladrón de credenciales
#3	42	136	224%	BitRAT	Herramienta de acceso remoto (RAT)
#4	83	121	46%	AsyncRAT	Herramienta de acceso remoto (RAT)
#5	66	108	64%	Loki	Ladrón de credenciales
#6	302	93	-69%	Raccoon	Ladrón de credenciales
#7	24	71	196%	NjRAT	Herramienta de acceso remoto (RAT)
#8	15	55	267%	Cobalt Strike	Puerta trasera
#9	-	50	Nueva entrada	Smoke Loader	Dropper
#10	26	43	65%	Vjw0rm	Ladrón de credenciales
#11	16	41	156%	CryptBot	Puerta trasera
#12	24	40	67%	RemcosRAT	Herramienta de acceso remoto (RAT)
#13	-	37	Nueva entrada	AveMaira	Herramienta de acceso remoto (RAT)
#13	23	37	61%	NanoCore	Herramienta de acceso remoto (RAT)
#15	17	30	76%	STRRAT	Herramienta de acceso remoto (RAT)
#16	23	26	13%	Tofsee	Spambot
#17	14	24	71%	ServHelper	Ladrón de credenciales
#18	43	23	-47%	Gozi	Troyano de banca en línea
#19	11	18	64%	QuasarRAT	Herramienta de acceso remoto (RAT)
#20	23	17	-26%	AgentTesla	Ladrón de credenciales

Comparación de tipos de malware entre el T2 y el T3 de 2021



Dominios de nivel superior (TLD) con mayor abuso, T3 de 2021

Sin cambios en las primeras posiciones de la lista

En el T3, .com y .xyz siguieron ocupando las primeras posiciones de nuestra clasificación. La situación se deterioró para estos dos TLD, en particular .com, que experimentó un incremento del 90%. Esperamos que VeriSign y XYZ.COM, los propietarios de estos LTD, tomen todas las medidas necesarias para mejorar la situación y aumentar la reputación de sus TLD.

Tres nuevos TLD

Dos nuevos gTLD y un ccTLD entraron en nuestros 20 principales: .club, .co y .monster. Todos ellos han experimentado un considerable aumento en la cantidad de nuevos dominios de botnet C&C registrados a través de sus servicios.

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.

Nuevas entradas

club (#9), co (#18) y monster (#19).

Salidas

vip, online y live.

Dominios de nivel superior (TLD) con mayor abuso, T3 de 2021 (continuación)

TLD con mayor abuso: cantidad de dominios

Clasificación	T2 2021	T3 2021	% de cambio	TLD	Nota
#1	4 113	7 827	90%	com	gTLD
#2	739	833	13%	xyz	gTLD
#3	607	829	37%	top	gTLD
#4	146	665	355%	net	gTLD
#5	662	538	-19%	buzz	ccTLD
#6	151	330	119%	ru	ccTLD
#7	139	306	120%	cn	ccTLD
#8	157	265	69%	org	gTLD
#9	140	183	31%	tk	Originalmente ccTLD, ahora efectivamente gTLD
#9	80	183	129%	su	ccTLD
#9	-	183	Nueva entrada	club	gTLD
#12	78	178	128%	info	gTLD
#13	208	170	-18%	br	ccTLD
#14	106	132	25%	ga	Originalmente ccTLD, ahora efectivamente gTLD
#15	116	126	9%	eu	ccTLD
#16	104	123	18%	ml	Originalmente ccTLD, ahora efectivamente gTLD
#17	73	98	34%	cf	ccTLD
#18	-	89	Nueva entrada	co	ccTLD
#19	-	82	Nueva entrada	monster	gTLD
#19	141	82	-42%	cloud	gTLD

Los registradores de dominios con mayor abuso, T3 de 2021

Observamos aumentos significativos en la mayoría de los registradores de dominios incluidos en nuestros 20 principales. El mayor porcentaje de registradores de dominios se encuentra en China, seguido de Canadá y Estados Unidos. Si bien el porcentaje de Canadá y la India ha disminuido, el de muchos otros países ha aumentado este trimestre*.

En el T2, se incluía Arsys, que ahora no aparece

Nuestra aprobación para Arsys, una entrada nueva en la quinta posición en el T2. Parecen haber tomado medidas eficaces para asegurarse de que su TLD se mantenga lo más limpio posible y han abandonado los 20 principales en el T3, junto con HiChina, 1API, Name.com y 55hl.com. Todos estos registradores han hecho un trabajo excelente.

Problemas con revendedores

En el T3, observamos los mayores incrementos en dominios de botnet C&C recién registrados en CentralNic (+488%), Tucows (+266%), RegRU (+252%), West263.com (+168%) y Network Solutions (+163%).

La gran mayoría de registros de nombres de dominio fraudulentos procede de revendedores poco fiables y con un proceso de evaluación de clientes inapropiado o inexistente.

Los registradores tienen dificultades para penalizar a estos revendedores por muchas razones, por ejemplo, términos de servicio (ToS) mal redactados. No obstante, también influyen otros factores, como intereses económicos encubiertos o una falta de motivación fundamental para responsabilizarse de estos problemas.

Esperamos que los registradores mejoren su reputación rápidamente mediante la imposición de medidas más estrictas a sus revendedores para asegurarse de que se esfuercen por combatir el registro de nombres de dominio 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

Porkbun (#7), dnspod.cn (#11), nicenic.net (#13), Openprovider (#18) y OVH (#19).

Salidas

Arsys, HiChina, Name.com, 55hl.com y 1API.

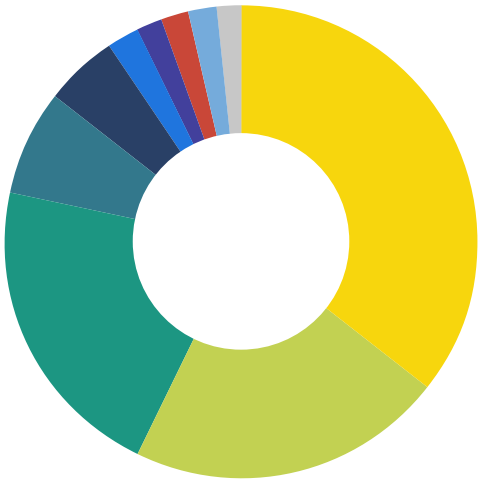
* Actualizado el 15 de octubre de 2021 | Dos registradores (NameSilo y Tucows) se clasificaron como proveedores con sede en Estados Unidos cuando se publicó este informe. Hemos actualizado el texto y los datos para reflejar que tienen su sede en Canadá.

Los registradores de dominios con mayor abuso, T3 de 2021 (continuación)

Los registradores de dominios con mayor abuso: cantidad de dominios

Clasificación	T2 2021	T3 2021	% de cambio	Registrador	País
#1	1 797	1 568	-13%	NameSilo	Canadá*
#2	955	1 267	33%	Namecheap	Estados Unidos
#3	504	1 217	141%	Alibaba	China
#4	526	787	50%	eName Technology	China
#5	112	658	488%	CentralNic	Reino Unido
#6	135	475	252%	RegRU	Rusia
#7	110	403	266%	Tucows	Canadá*
#7	-	403	Nueva entrada	Porkbun	Estados Unidos
#9	101	266	163%	Network Solutions	Estados Unidos
#10	125	255	104%	Xin Net	China
#11	80	214	168%	west263.com	China
#11	-	214	Nueva entrada	dnspod.cn	China
#13	-	209	Nueva entrada	nicenic.net	China
#14	215	189	-12%	Eranet International	China
#15	92	188	104%	Key Systems	Alemania
#16	110	176	60%	22net	China
#17	188	169	-10%	PDR	India
#18	-	165	Nueva entrada	Openprovider	Países Bajos
#19	-	160	Nueva entrada	OVH	Francia
#20	91	154	69%	WebNic.cc	Singapur

UBICACIÓN DE LOS REGISTRADORES DE DOMINIOS CON MAYOR ABUSO



País	Botnets	%
China	3 261	35,7%
Canadá*	1 971	21,57%
Estados Unidos	1 936	21,19%
Reino Unido	658	7,2%
Rusia	475	5,2%
Alemania	188	2,1%
India	169	1,8%
Países Bajos	165	1,8%
Francia	160	1,8%
Singapur	154	1,7%
Total	**9 137**	

* Actualizado el 15 de octubre de 2021 | Dos registradores (NameSilo y Tucows) se clasificaron como proveedores con sede en Estados Unidos cuando se publicó este informe. Hemos actualizado el texto y los datos para reflejar que tienen su sede en Canadá.

Redes que alojan los botnet C&C más recientes, T3 de 2021

Como es habitual, hubo muchos cambios en las redes que alojan los botnet C&C más recientes. En particular, observamos un aumento en las redes que hospedan botnet C&C de FastFlux, usadas por cibercriminales para alojar malware de puerta trasera.

¿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.

serverion.com

Observamos un aumento del 69% en la cantidad de nuevos servidores de botnet C&C instalados en el proveedor holandés de servicios de alojamiento serverion.com. Nuestros investigadores creen que este aumento se debe principalmente a su cliente comercializador des.capital, que suele atraer a operadores de botnet.

Realizar cambios positivos

En la actualización del último trimestre, indicamos que una operación de alojamiento de botnet se había transferido de Amazon a DigitalOcean, provocando que se disparara la clasificación de esta última. Queremos felicitar a DigitalOcean por abandonar nuestra lista de los 20 principales en el T3 de 2021, junto con otras redes, como Google, que ocupaba la segunda posición, HostSailor, Microsoft, M247 y Off Shore Racks.

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/verificación de clientes antes de empezar a operar un servicio.

Cuando las redes aparecen en una posición elevada en la clasificación, esto indica alguno de los problemas siguientes:

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

uninet.net.mx (#1), stc.com.sa (#3), claro.com.do (#4), antel.net.uy (#8), telefonica.com.br (#9), telefonica.com.ar (#16), uplus.co.kr (#17) y hotwinds.com (#18).

Salidas

google.com, itld.com, digitalocean.com, internet-it, hostsailor.com, microsoft.com, m247.ro, offshoreracks.com.

Redes que alojan los botnet C&C más recientes, T3 de 2021 (continuación)

Botnet C&C descubiertos recientemente por red

Clasificación	T2 2021	T3 2021	% de cambio	Red	País
#1	-	177	Nueva entrada	uninet.net.mx	México
#2	68	115	69%	serverion.com	Países Bajos
#3	-	105	Nueva entrada	stc.com.sa	Arabia Saudita
#4	-	95	Nueva entrada	claro.com.do	Rep. Dominicana
#5	48	89	85%	privacyfirst.sh	Alemania
#6	35	69	97%	ipjetable.net	Francia
#7	29	68	134%	cloudflare.com	Estados Unidos
#8	-	63	Nueva entrada	antel.net.uy	Uruguay
#9	-	58	Nueva entrada	telefonica.com.br	Brasil
#10	82	56	-32%	pq.hosting	Rusia
#11	56	52	-7%	ovh.com	Francia
#12	46	51	11%	hetzner.de	Alemania
#13	16	45	181%	mivocloud.com	Moldavia
#14	40	44	10%	baxet.ru	Rusia
#14	49	44	-10%	nano.lv	Letonia
#16	-	43	Nueva entrada	telefonica.com.ar	Argentina
#17	-	41	Nueva entrada	uplus.co.kr	Corea
#18	26	33	27%	alibaba-inc.com	China
#18	-	33	Nueva entrada	hotwinds.com	Estados Unidos
#20	47	32	-32%	mgnhost.ru	Rusia

Redes que alojan los botnet C&C más activos, T3 de 2021

Finalmente, echemos un vistazo a las redes que alojaron una gran cantidad de botnet C&C activos en el tercer trimestre de 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.

Aumento en el abuso de botnet C&C

Por desgracia, la situación en términos de los servidores de botnet C&C activos empeoró para muchos de los ISP incluidos en nuestros 20 principales en el T2. Ipjetable.net (FR), microsoft.com (US), vietserver.vn (VN) y openvpn (SE) tienen todos algo en común: en lugar de tomar medidas apropiadas contra el abuso de su infraestructura, la cantidad de servidores de botnet C&C activos aumentó en estas redes.

uninet.net.mx y stc.com.sa

Estos dos ISP entran por primera vez en nuestros 20 principales este trimestre y ocupan la primera y la segunda posición, debido al gran número de bots de FastFlux alojados en sus redes.

De hecho, la mayoría de las nuevas entradas en esta tabla se deben al alojamiento de bots de FastFlux en sus redes y al hecho de no responder con celeridad a los informes de abusos. Todas estas empresas proporcionan a los operadores de botnet una infraestructura de botnet C&C resistente.

Nuevas entradas

uninet.net.mx (#1), stc.com.sa (#2), claro.com.do (#4), antel.net.uy (#6), telefonica.com.br (#7), telefonica.com.ar (#8), tie.cl (#10), serverion.com (#10), algartelecom.com.br (#14), uplus.co.kr (#17) y skbroadband.com (#19).

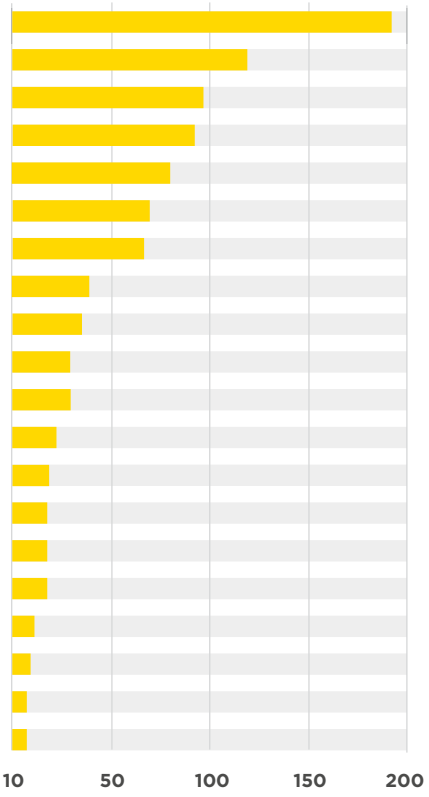
Salidas

google.com, ttnet.com.tr, inmotionhosting.com, m247.ro, datawire.ch, mtnnigeria.net, eliteteam.to, unusinc.com, chinanet-js, kornet.net.

Redes que alojan los botnet C&C más activos, T3 de 2021 (continuación)

Cantidad total de botnet C&C activos por red

Clasificación	T2 2021	T3 2021	% de cambio	Red	País
#1	-	185	Nueva entrada	uninet.net.mx	México
#2	-	119	Nueva entrada	stc.com.sa	Arabia Saudita
#3	61	99	62%	ipjetable.net	Francia
#4	-	97	Nueva entrada	claro.com.do	Rep. Dominicana
#5	58	79	36%	microsoft.com	Estados Unidos
#6	-	68	Nueva entrada	antel.net.uy	Uruguay
#7	-	63	Nueva entrada	telefonica.com.br	Brasil
#8	-	41	Nueva entrada	telefonica.com.ar	Argentina
#9	23	32	39%	vietserver.vn	Vietnam
#10	-	29	Nueva entrada	tie.cl	Chile
#10	-	29	Nueva entrada	serverion.com	Países Bajos
#12	20	24	20%	ovpn.com	Suecia
#13	21	22	5%	charter.com	Estados Unidos
#14	-	21	Nueva entrada	algartelecom.com.br	Brasil
#14	18	21	17%	cloudvider.net	Reino Unido
#14	17	21	24%	une.net.co	Colombia
#17	-	19	Nueva entrada	uplus.co.kr	Corea
#18	17	18	6%	hostry.com	Chipre
#19	-	17	Nueva entrada	skbroadband.com	Corea
#19	12	17	42%	claro.com.co	Colombia



Y esto es todo por ahora.

¡Cuídate y nos vemos en enero!