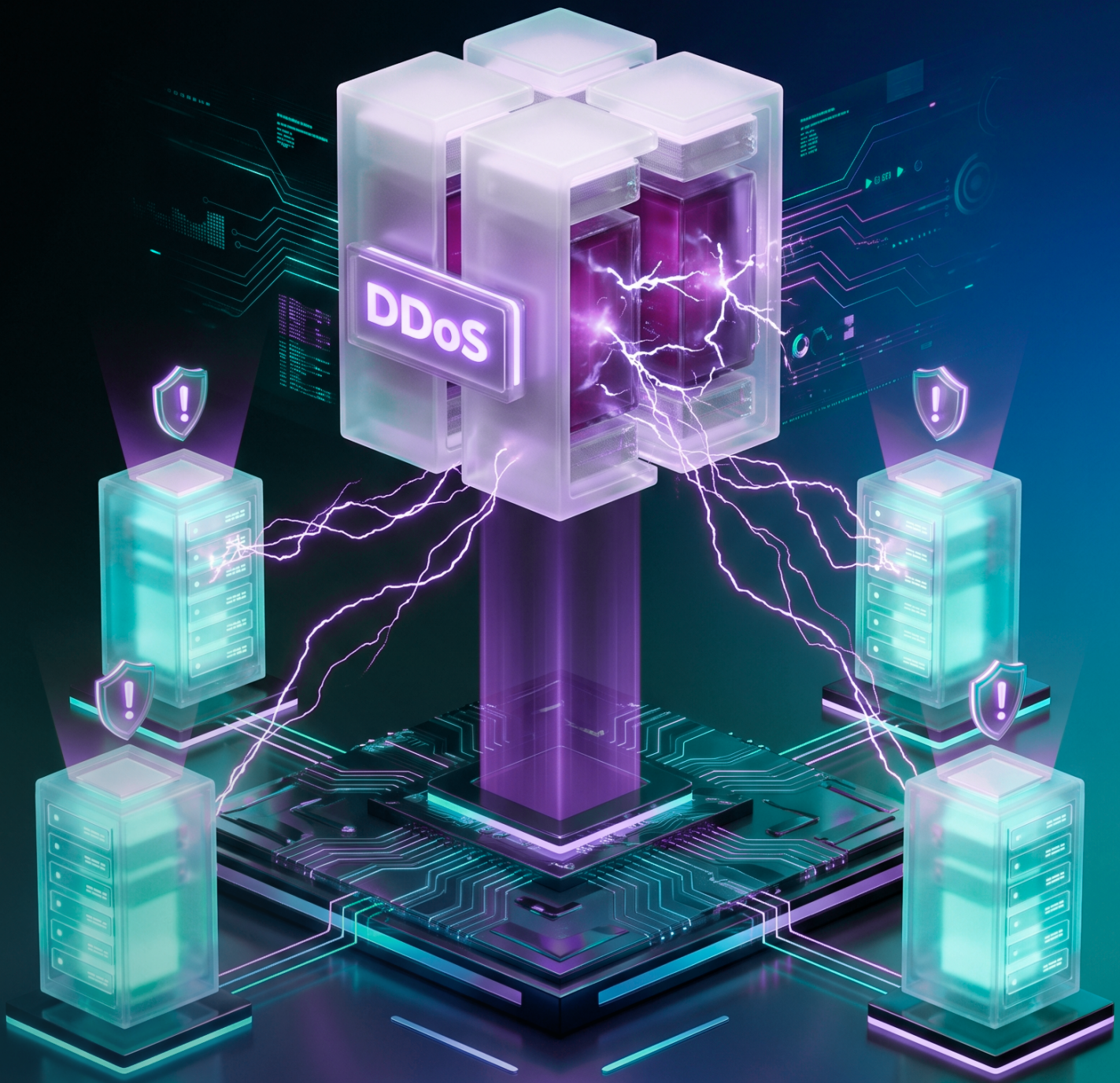
kaspersky cybersecurity true to business



SobreDDoSis

El mercado de provocar inundaciones con fines lucrativos

Introducción

El aumento de los ataques DDoS[1] se volvió una gran inquietud en el sector de la ciberseguridad. Sin embargo, los propios ataques revelan solo una parte del panorama. Detrás de ellos hay un mercado oculto que ofrece capacidades disruptivas como servicio, lo que permite que los ataques selectivos estén disponibles por un precio menor al de un servicio de streaming.

Para examinar este mercado, analizamos más de 256 000 publicaciones en la red oscura y profunda, e identificamos 148 actores DDoS activos desde al menos 2024. Pero la historia más profunda aparece cuando nos remontamos a 2015. En varios años de publicidades, sus playbooks, ofertas e identidades recurrentes, se formó un patrón: no se trataba de una mera colección de servicios de ataque, sino de una economía de la interrupción oculta, persistente, capaz de adaptarse y mucho más organizada de lo que aparentaba a primera vista. En las siguientes páginas, describimos las armas, la presa, los comercios, los precios y la evolución que mantuvieron este mercado con vida.

El informe se desarrolla en tres partes principales:

Armas de interrupción comienza con los ataques: las formas que toman, los objetivos que persiguen y las maneras en que los actores adquieren la capacidad de ejecución.

El precio a pagar trata sobre el lado comercial de la interrupción y analiza cómo se cotizan y venden los diferentes modelos de servicio, y cómo la competencia los determina con el paso del tiempo.

La parte Supervivencia en la industria analiza los actores detrás de estas operaciones: ¿cuánto tiempo permanecen activos?, ¿cómo compiten por la visibilidad?, ¿cómo expanden la capacidad DDoS a servicios adyacentes y cómo adaptan sus ofertas con el tiempo?

Este material se desarrolló para expertos técnicos y estratégicos en ciberseguridad, de analistas de Inteligencia de amenazas a gerentes de Seguridad de la información.

[1] https://blog.cloudflare.com/ddos-threat-report-2025-q4/

Armas de interrupción

Instrumentos de sobrecarga

Al observar cómo los actores describen sus servicios, identificamos dos categorías de ataques amplias: L3/L4 y L7. Junto a ellas, identificamos dos más limitadas: ataques a servidores de juegos y ataques .onion, que aparecen como casos especializados de estos grupos más amplios. De 148 actores de nuestro conjunto de datos, 91 especificaron suficientes detalles en sus publicidades para que podamos determinar la categoría. En 20 de estos 91 casos, el tipo de ataque no se indicó explícitamente, pero se podía inferir de las soluciones anti-DDoS mencionadas u otras pistas contextuales.

L3/L4

Los ataques L3/L4 tienen como fin sobrecargar la capacidad de la red mediante la generación de tráfico de alto volumen.

En nuestro conjunto de datos, los ataques L3 no eran tan comunes como categoría independiente. En la mayoría de los casos, los actores agruparon los ataques L3 y L4, por lo que los tratamos como una única categoría. Solo el 9 % de los actores ofrecieron explícitamente métodos L3 como inundaciones ESP, ICMP o GRE. Los ataques L4 fueron mucho más comunes: el 74 % de los actores mencionaron TCP ACK/SYN, inundaciones UDP, amplificación de DNS u otros métodos de capa de transporte.

10 Gbps-8.2 Tbps

- Intenta sobrecargar el ancho de banda de la red
- Más fácil de ejecutar
- Más fácil de detectar
- Genera grandes picos en el tráfico

Juegos*

Caso especial de L3/L4

>1 Tbps

*Paquetes UDP específicamente diseñados

Un caso destacado es el ataque a servidores de juegos. Técnicamente, pertenece a L4[2], pero los actores suelen tratarlo como algo independiente. En parte, esto se debe a que los servidores de juegos se comportan diferente a la infraestructura de red común. Consumen más memoria, generan picos en el uso de la CPU e impactan en gran medida los discos. Además, los ataques a juegos suelen requerir paquetes específicos para juegos, generalmente a través del UDP. Es por eso que los actores a menudo presentan los ataques a juegos no como otro método de inundación, sino como una capacidad distinta.

[2]Si bien los ataques DDoS a servidores de juegos pueden involucrar tanto técnicas L4 como L7, en las publicidades solo se mencionaron explícitamente los ataques L4 a juegos.

L7

Los ataques L7 funcionan de otra manera. En lugar de intentar sobrecargar el ancho de red o el procesamiento de la conexión, ejercen presión sobre la propia aplicación.

L7 fue la categoría más publicitada de nuestro conjunto de datos: el 92 % de los actores afirmó ofrecerla. Un motivo es que hay muchos métodos L7 de código abierto listos para usar, lo que minimiza los obstáculos para ajustarlo y ofrecerlo para la venta. Otro motivo es la simplicidad relativa de la inicialización del objetivo, ya que para ejecutar el ataque se requiere poco más de un sitio web objetivo.

Los ataques a recursos .onion son un caso específico de ataques L7, dado que los atacantes aprovechan la manera en que Tor gestiona las conexiones en lugar de depender solo del volumen de tráfico. Solo el 3 % de los actores pudo afirmar que implementa esta función.

100 000 rps – 8 500 000 rps

- Intenta de agotar los recursos de la aplicación
- Imita comportamientos legítimos
- Más difícil de detectar
- Requiere conocimiento del objetivo

.onion*

Caso especial de L7

* Requiere comunicación TOR

Cazadores y cazados

Métodos DDoS similares pueden estar impulsados por diferentes motivos, según quién inicia el ataque, qué quiere lograr esa persona y quién se interpone. Aunque siguen diferentes lógicas, los iniciadores de ataque obtienen el mismo resultado: interrupción intencional. Debajo se describen los principales perfiles de atacantes identificados en nuestro conjunto de datos.

Actores económicamente hostiles:

Pérdida financiera mediante la interrupción de la disponibilidad del servicio y daños a la reputación

Provocar daños financieros a través de la reducción del tiempo de actividad, menor posicionamiento en las búsquedas y agotamiento de los presupuestos destinados a la publicidad mediante tráfico ilícito.

Organizaciones que dependen de servicios en línea, rendimiento de SEO y publicidad digital de pago. Entre los sectores más atacados se encuentran las empresas privadas y los servicios de juegos en línea.



Operadores de secuestro de datos:

Forzar un pago al interrumpir los servicios o amenazar con interrupciones continuas.

Beneficio financiero al presionar a las víctimas para que paguen si desean detener o evitar el ataque.

Organizaciones que dependen de una disponibilidad continua del servicio o que están lidiando con ransomware en ese momento. Los sectores comunes incluyen finanzas, fabricación, servicios en línea, telecomunicaciones e infraestructura crítica.



Hacktivistas:

Llamar la atención sobre un evento o "castigar" a organizaciones de una determinada ideología.

Promover opiniones políticas o sociales mediante la interrupción de las operaciones y obtención de visibilidad pública.

Las entidades gubernamentales y financieras, los medios de comunicación, las grandes empresas y la infraestructura crítica se encuentran entre los objetivos más comunes.



Oportunistas:

Utilizan la interrupción como distracción para llevar a cabo otras actividades maliciosas u obtener ventaja.

Beneficio personal o circunstancial.

Las organizaciones con sistemas de supervisión complejos y plataformas de juegos en línea son vulnerables a problemas de sobrecarga o sincronización. Los sectores comunes incluyen grandes empresas, entidades financieras y servicios de juegos en línea.



Compra del arsenal

Si observamos cómo los actores lanzan los ataques, aparecen tres modelos: DDoS intermediado, DDoS como servicio e infraestructura interna. Los primeros dos dependen de proveedores de recursos externos, mientras que el tercero pertenece a actores que pueden desarrollar y mantener una infraestructura de ataque por su cuenta.

Proveedor de recursos: un actor que ya controla la infraestructura requerida para el ataque.

DDoS intermediado



Ataque realizado por otro actor después de una comunicación directa

DDoS como servicio



Acceso a recursos por suscripción

Infraestructura interna

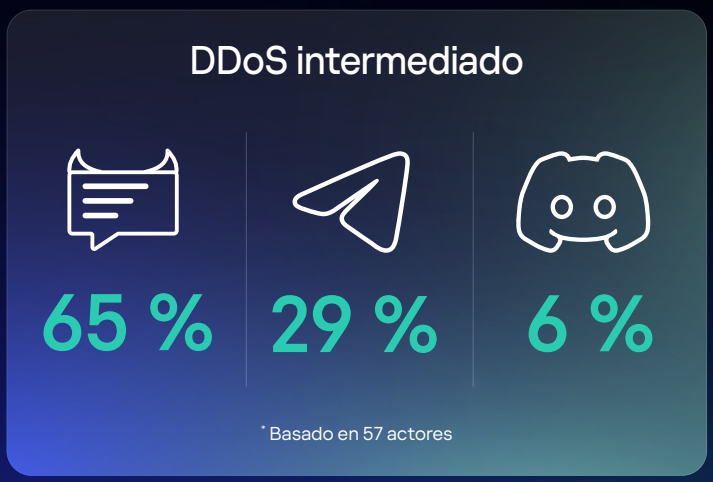


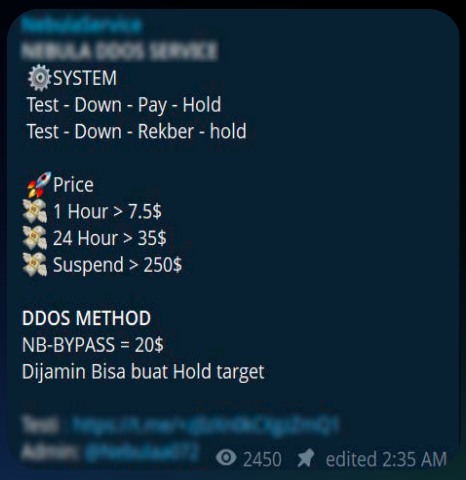
Recursos autosuficientes

DDoS intermediado

El modelo más directo es también el más simple: un iniciador de ataque se comunica con un proveedor de recursos y pide que se lleve a cabo un ataque. De esta manera, los intermediarios DDoS funcionan como proveedores de recursos. El primer contacto sucede en un foro de la red oscura, pero la comunicación luego se traslada a otra plataforma, en la mayoría de los casos Telegram o Discord. En este modelo, el proveedor se encarga de todo lo técnico: qué método usar, cómo moldear el tráfico y cómo abordar la protección anti-DDoS.

Iniciador de ataque: un actor que intenta atacar un sistema, servicio o recurso en línea con un ataque.





Ejemplo de publicidad de DDoS intermediado

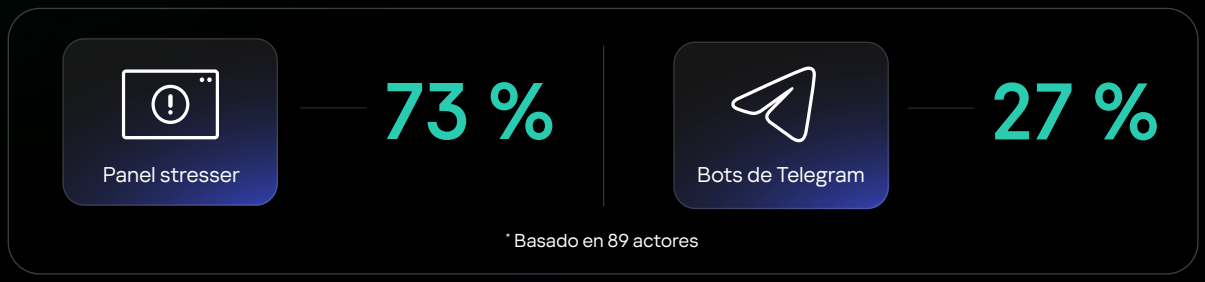
Entre los 57 actores de nuestro conjunto de datos que ofrecían llevar a cabo un DDoS, el 65 % todavía utilizaba foros de ciberdelincuentes como su principal plataforma publicitaria. El resto utilizaba aplicaciones de mensajería, principalmente Telegram y Discord.

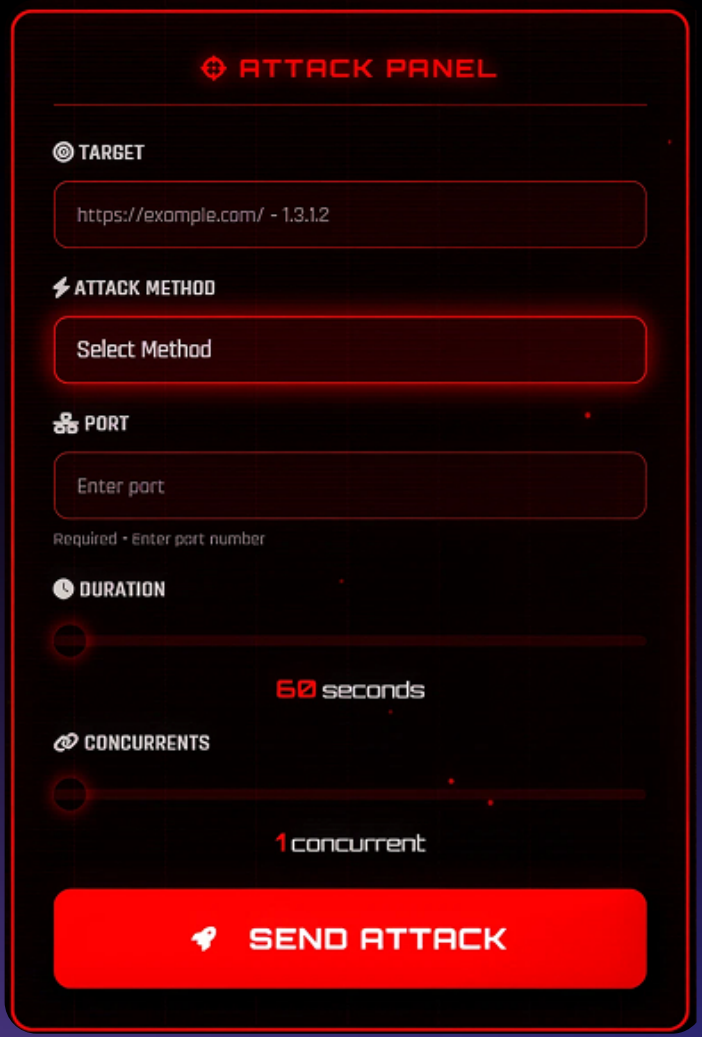
DDoS como servicio

El segundo enfoque elimina las interacciones directas. En lugar de negociar con un proveedor, el iniciador del ataque le compra el acceso a un panel stresser o a un bot de Telegram y lanza el ataque por su cuenta. De esta manera, decide el plan de suscripción, que incluye métodos de ataque particulares, la duración y la cantidad de ataques simultáneos. Algunos servicios van más allá con la simplificación del inicio del ataque. Por ejemplo, un ataque de prueba se puede lanzar de forma gratuita con un simple comando en un chat.

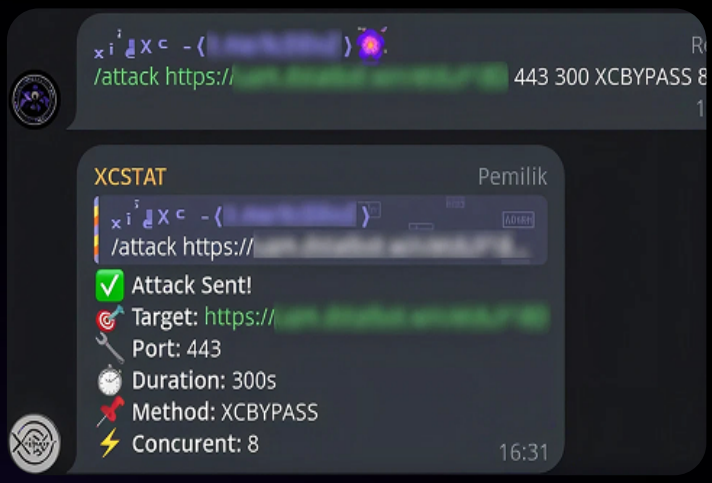
Panel stresser: una interfaz que se utiliza para ejecutar y administrar ataques en DDoS como servicio, controlada por un proveedor de recursos.

Históricamente, este modelo utilizaba paneles stresser. Desde 2022, observamos un fuerte aumento (en comparación con años anteriores) de actores que publicitan bots de Telegram con funcionalidad DDoS exclusiva. Parte del mercado se está moviendo de sitios web a interfaces más simples, rápidas y rápidamente renovables.





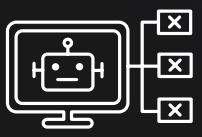
Ejemplo de interfaz de un panel stresser



Ejemplo de iniciación de ataque a través de un bot de Telegram

Infraestructura interna

No todos los iniciadores de ataque utilizan proveedores externos. En cambio, usan su propia infraestructura. En la práctica, esto generalmente significa que ejecutan scripts de ataque mediante la implementación de uno o más métodos, o que desarrollan y mantienen la red de bots completa.



Basado en botnets

La diferencia en parte es técnica y en parte es operativa. Un script puede ser suficiente para una tarea concreta o una campaña breve. Una botnet es diferente: tiene que crearse, mantenerse y preservarse. Es por esto que las capacidades basadas en botnets suelen asociarse con actores con capacidades más técnicas.



Basado en scripts

Desde abril de 2026, identificamos más de 1000 repositorios Github que contienen scripts stresser, junto con 500 más que afirmaban contener código fuente de botnets. Los scripts se pueden conseguir fácilmente de forma gratuita, lo que reduce los obstáculos para los actores que ya cuentan con capacidades técnicas. En contraste, las botnets casi no se distribuyen libremente, sino que suelen estar a la venta.

El precio a pagar

Las diferentes maneras de adquirir la capacidad DDoS tienen diferentes modelos de pago. En DDoS intermediado, los pagos se organizan por solicitud. En DDoS como servicio, los precios se estandarizan por planes de suscripción fija.

DDoS intermediado

En DDoS intermediado, los precios exactos se analizan caso por caso. El iniciador del ataque se comunica con el proveedor, que examina el objetivo antes de decidir el costo del ataque.

Entre los 36 actores de nuestro conjunto de datos que utilizaron este modelo, los precios de ataque variaron de $30 a $2000 según la duración, el objetivo y la capacidad requerida del servicio.

$30 - $2000

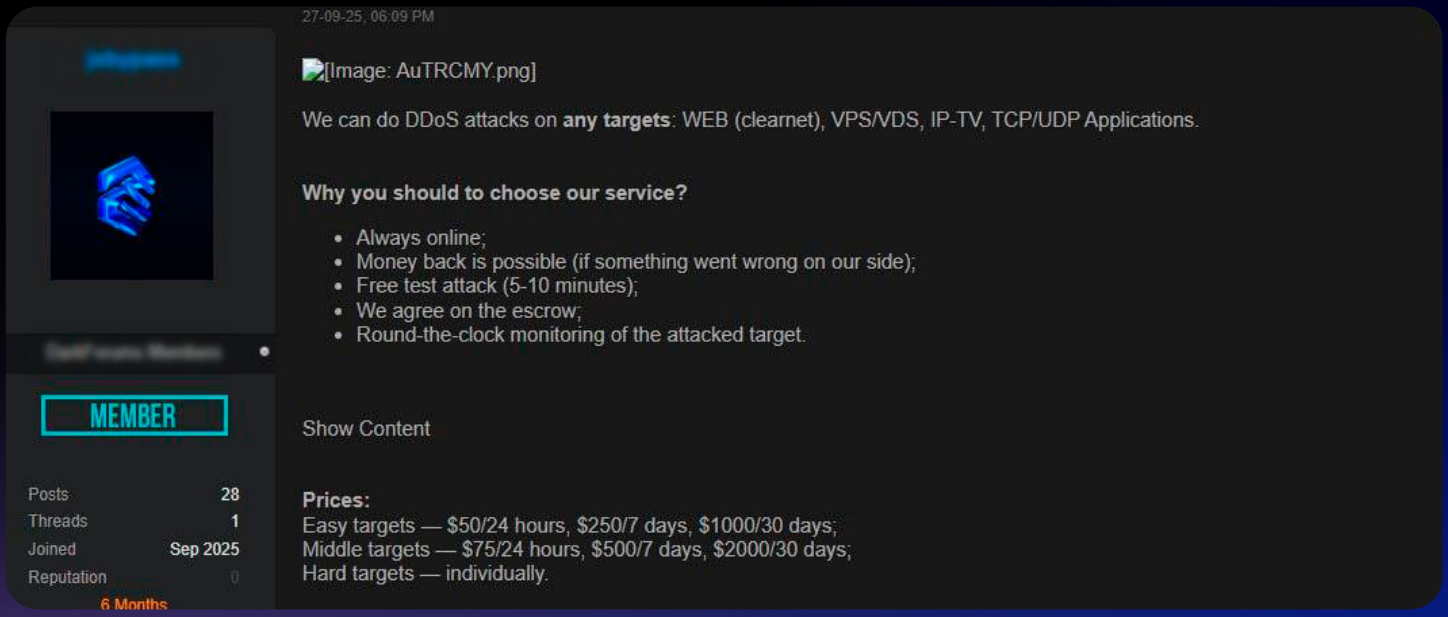
pago a pedido para un solo ataque

*Rango de precios para los ataques de 1 a 30 días de duración

$10	$100	$500	$1250
ataque de prueba	por 1 día	por 7 días	por 30 días

*Precios promedio en base a 36 actores con tipo de pago a pedido

Una oferta típica incluye un ataque de prueba a corto plazo. Algunos actores publicitan pruebas gratuitas, mientras que otros cobran alrededor de $10 para que el iniciador del ataque verifique que el servicio funciona tal como se publicita antes de pagar una campaña más grande.



Ejemplo de anuncio de DDoS intermediado

DDoS como servicio

El modelo de suscripción ofrece un rango más amplio de planes que los DDoS intermediados. En este caso, el iniciador del ataque paga para acceder a la capacidad de ataque en lugar de pagar por un solo ataque solicitado. Una suscripción, que por lo general dura 30 días, define los métodos disponibles, la duración máxima de un ataque individual, la cantidad de ataques simultáneos y el acceso a la API. Los planes de precio de niveles más altos amplían los límites de estos parámetros en lugar de cambiar el modelo en sí.

$1 - $30 000

suscripción a la capacidad de ataque limitada por plan

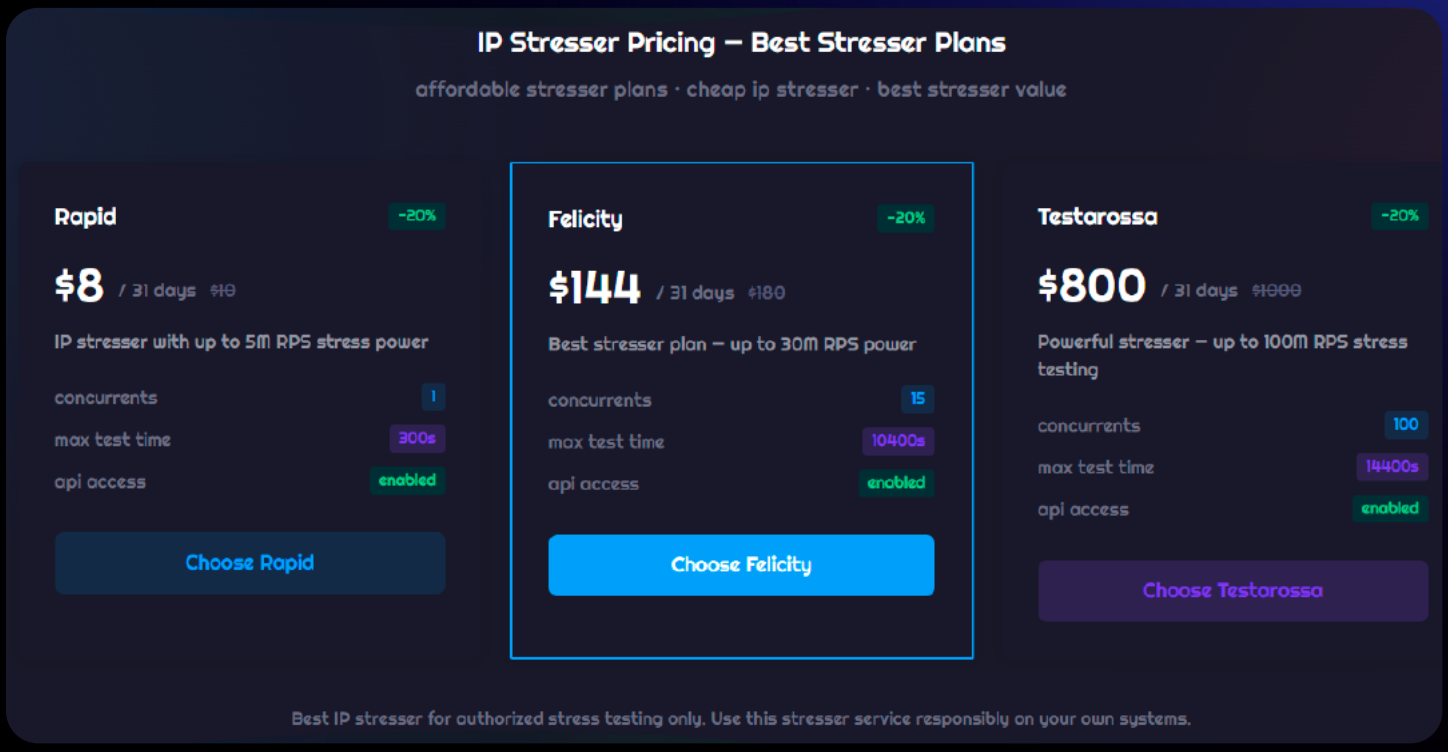
* Para planes de 30 días de duración

En nuestro conjunto de datos, 64 actores publicitaron precios de DDoS como servicio. Para una suscripción de 30 días, los precios variaban de $1 a $30 000. Unos pocos actores también ofrecían una suscripción de 7 días, aunque esto no era tan común. La duración establecida de un ataque individual variaba de 1 minuto a 48 horas.

$20	$191	$2160
de 60 s a 600 s	para 300 s - 3600 s	para más de 3600 s

* Precios promedio para una suscripción de un mes en base a 64 actores

Hubo un detalle que apareció en estos servicios una y otra vez: la duración del ataque se indicaba en segundos, no en minutos ni horas, lo que parece un poco inusual. Según nuestras observaciones, proviene de scripts DoS antiguos, formados por herramientas del estilo Unix/POSIX, en los que los segundos eran la unidad de tiempo predeterminada y los segundos enteros eran el formato más simple para trabajar.



Ejemplo de precios de suscripción al panel stresser

Modelo de servicio	¿Qué se paga?	Esfuerzos del comprador	Duración de ataque individual	Costo relativo
DDoS intermediado	Un ataque solicitado contra un solo objetivo	Relativamente bajos, ya que el proveedor gestiona el ataque	1, 7, 30 días o completamente personalizado	Más rentable para ataques más largos y objetivos complejos
DDoS como servicio	Acceso de 30 días a la capacidad de ataque con límites del plan	El comprador elige el método y la potencia requerida, y es posible que necesite volver a lanzar los ataques	De 1 minuto a 24 horas, según el plan elegido	Más rentable para ataques más cortos y objetivos más simples

Calibre de los ataques

Se encontraron declaraciones acerca de la capacidad de ataque casi exclusivamente en las publicidades de DDoS como servicio. Los intermediarios DDoS rara vez exponen este detalle y los atacantes con capacidad interna deciden por sí mismos, lo que significa que el análisis que se muestra debajo está basado más que nada en servicios realizados a través de paneles stresser.

En esta parte del mercado, la potencia a menudo se vende a través de números: los proveedores prometen una capacidad de entre 15 Gbps y 7000 Gbps, mientras que los precios mencionados varían de $30 a $4500.



Entre los paneles stresser que mencionaron tener capacidad, el 36 % afirmó ofrecer ataques a escala Tbps. Sin embargo, estas cifras deben interpretarse con precaución. La capacidad es algo fácil de publicitar, pero mucho más difícil de verificar. Los paneles comerciales prefieren apuntar a ataques L3/L4 de nivel medio para hacer ganancias rápidas. Los ataques a escala Tbps sin precedentes son lanzados por actores estatales cuyo objetivo es la interrupción, no por modelos de pago por uso.

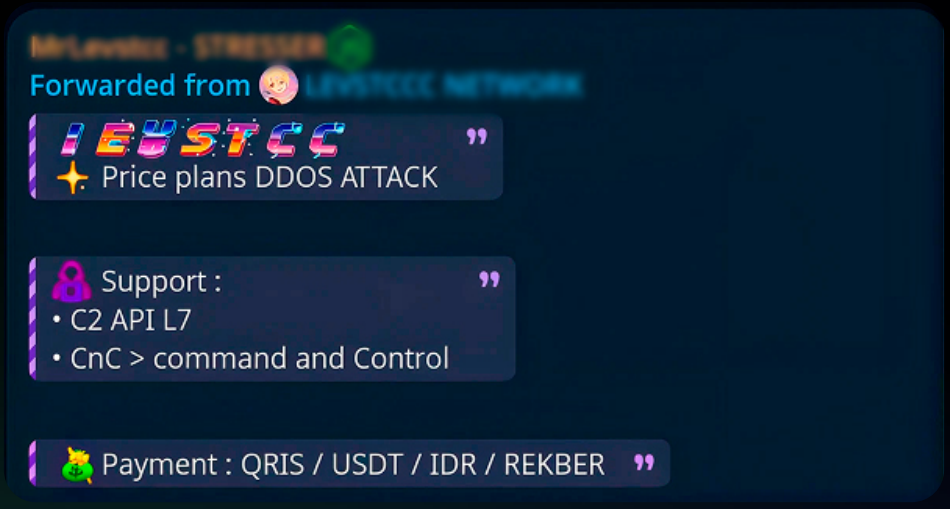
Moneda de intercambio

Se encontró información de pago explícita principalmente en las publicidades de DDoS como servicio, en las que los actores tuvieron que automatizar el acceso a sus servicios. Las ofertas intermediadas tenían muchas menos probabilidades de divulgar dichos detalles de forma pública.

Los servicios de nuestro conjunto de datos aceptaron 25 métodos de pago diferentes. La mayoría de ellos eran criptomonedas. El 92 % de los proveedores aceptaba Bitcoin, mientras que el 60 % aceptaba Ethereum y Litecoin. Los métodos de pago alternativos a las criptomonedas se observaron con mucha menos frecuencia; solo el 7 %, ya que no proporcionan suficiente privacidad.



Al mismo tiempo, los métodos de pago no comunes son útiles para la atribución.



Ejemplo de mensaje con métodos de pago especificados

Infraestructura interna

Los iniciadores de ataque que dependen de su propia infraestructura se enfrentan a costos de otro tipo. No hay un paywall, una suscripción conveniente ni un flujo de compra unificado. En cambio, combinan la capacidad de ataque de diferentes partes: scripts, servidores, infraestructura de control y dispositivos infectados para el caso de botnets. De acuerdo a los playbooks de los atacantes, hay dos modelos generales para crear una infraestructura: una configuración más simple basada en scripts y una configuración más costosa basada en botnets.

Basado en scripts



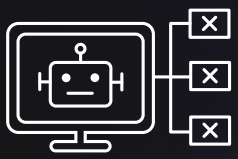
Notas

$0 - $100

Alquiler de VPS

$10 - $30 por mes

Basado en botnets



Código fuente

Más de $2000

Alquiler de C2

$10 - $30 por mes

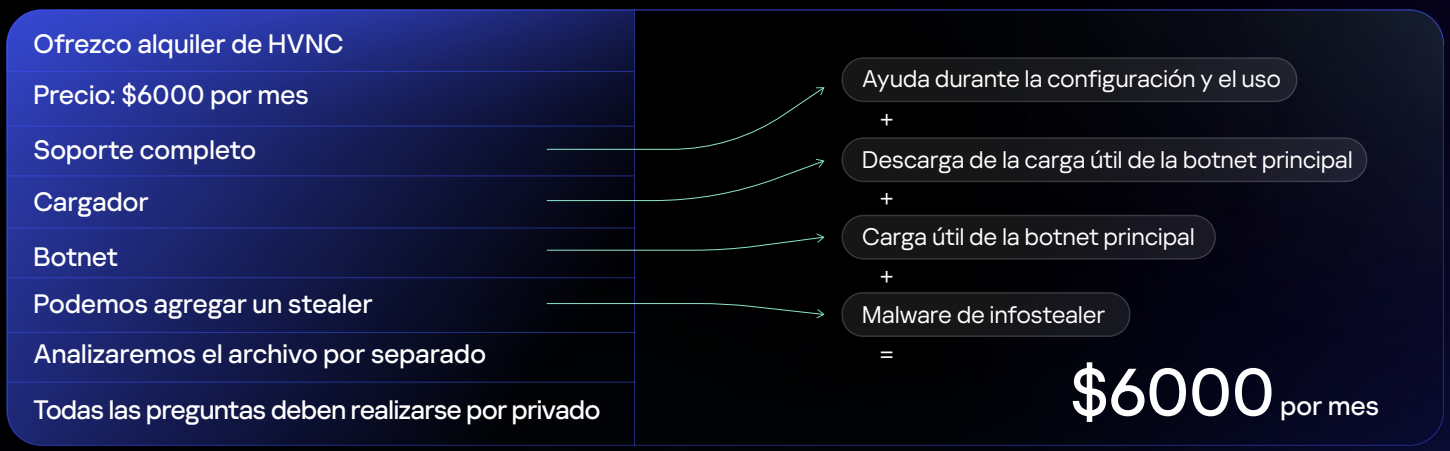
instalaciones, tráfico, mantenimiento

Más de $0.1 por instalación

En el caso más simple, un actor implementa un script de ataque de código abierto o bajo costo en servidores alquilados. El verdadero gasto proviene de la infraestructura subyacente. Los costos de hosting dependen de la cantidad de servidores utilizados, sus características y la tolerancia del proveedor de hosting para los informes de abuso.

Una configuración con botnet requiere invertir en otra liga. Un código fuente arcaico se puede encontrar en Internet, pero una botnet con mayor capacidad suele estar a la venta, en lugar de distribuirse de forma gratuita. Los precios comienzan en alrededor de $2000.

Y eso es solo la punta del iceberg. Ejecutar una botnet también implica pagar servidores C2, instalaciones, tráfico, ofuscación regular para sortear los antivirus y mantenimiento continuo. A diferencia de una configuración basada en scripts, una botnet no solo se ejecuta, debe mantenerse con vida.



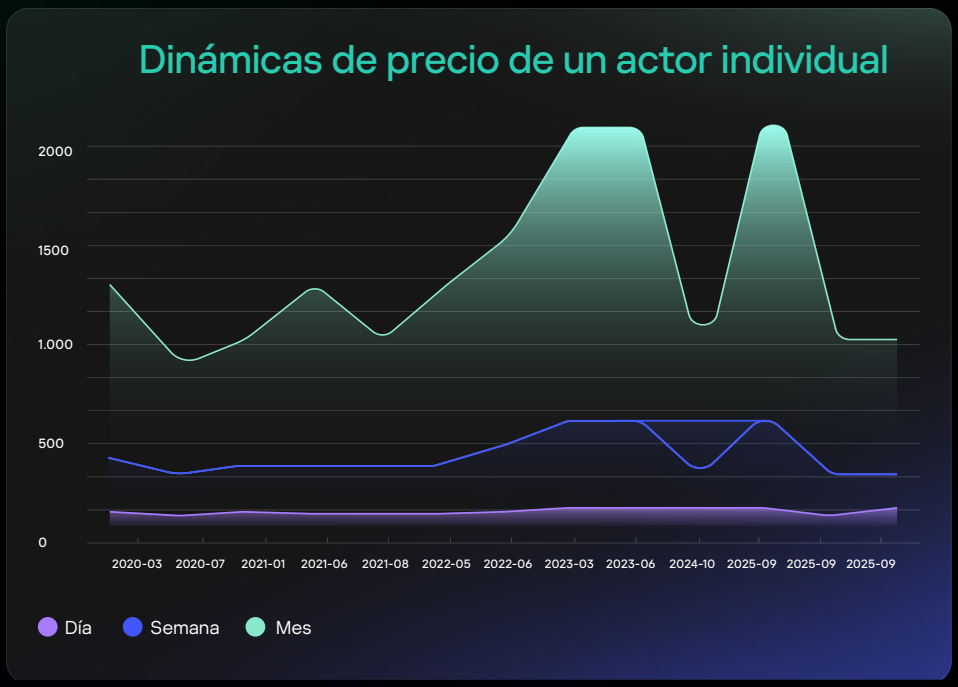
Publicidad de un alquiler de botnet en un foro de la red oscura

Un ejemplo de una publicidad de botnet muestra lo que puede incluir el precio del alquiler. En este caso, un paquete de alquiler de botnet de $6000 por mes incluía no solo el acceso a la botnet, sino también un cargador, soporte del operador y funcionalidad adicional de infostealer. La oferta cubría no solo el código fuente, sino una capacidad de ataque completa mantenida y vendida como un paquete.

La lucha del precio

En un análisis comparativo del precio de DDoS a lo largo del tiempo, se distinguieron dos patrones. Primero, gran parte del mercado parece relativamente coherente: alrededor del 64 % de los servicios de nuestro conjunto de datos mantuvo los mismos precios durante períodos largos; en algunos casos, durante más de una década. Segundo, el 36 % restante mostró fluctuaciones impredecibles. Por ejemplo, descubrimos un actor cuyos precios se redujeron un 50 % en tan solo 20 días.

Desde una perspectiva del mercado, esto es prueba de un sector estable en algunas áreas, pero que está lejos de ser homogéneo.



La estabilidad se debilita cuando cambiamos el enfoque del mercado en general a los diferentes actores. El ejemplo mencionado controla los precios publicitados por un único proveedor para ataques de un día, una semana y un mes. En lugar de un patrón coherente, la figura muestra ascensos y descensos impredecibles. El caso que más llama la atención aparece en octubre de 2024, cuando el mismo actor publicitó dos precios drásticamente diferentes en distintos foros. Más que nada, esto destaca cómo los actores adaptan los precios según el público objetivo.

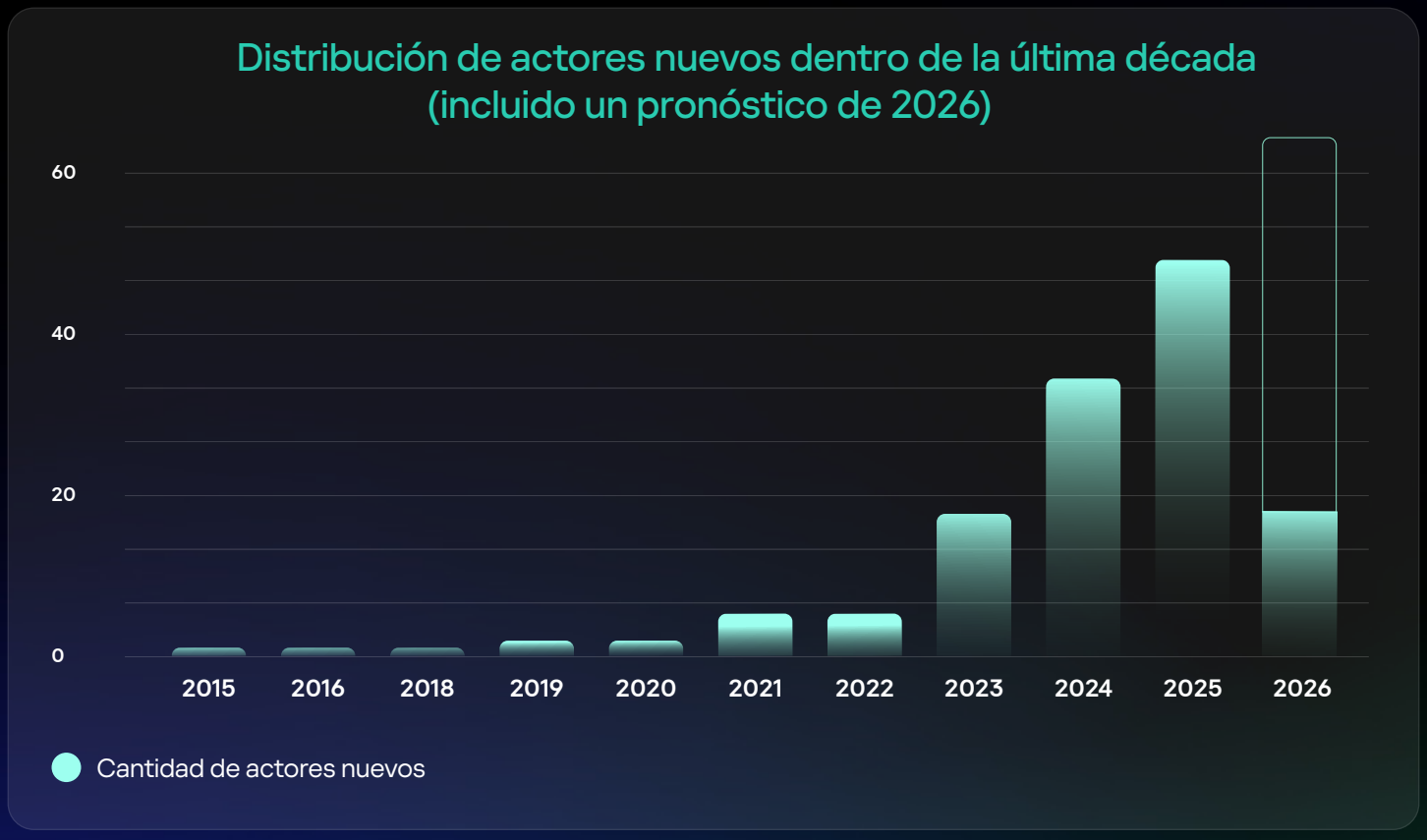
Supervivencia en la industria

Nace, se vende y se va

Entre los 148 actores que estuvieron activos en algún punto del 2024 o antes, la vida útil promedio (tiempo entre la primera y la última publicidad de capacidad DDoS) es de alrededor de 2.5 años, mientras que el proveedor más antiguo que aún está activo cumplió 10 años de operación el año pasado.

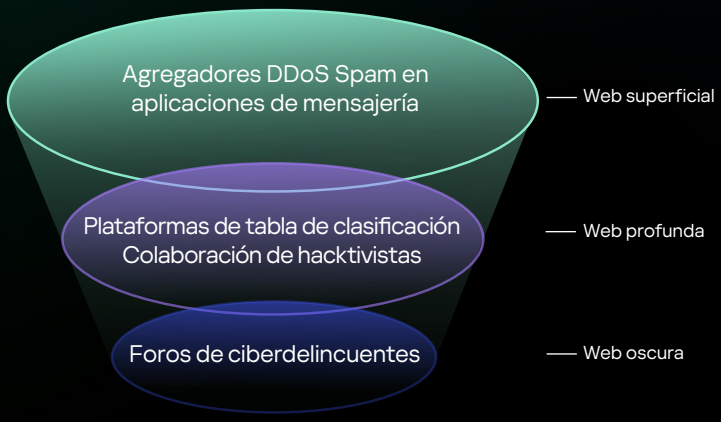
La cantidad de actores nuevos se mantuvo relativamente baja hasta 2022. El primer aumento notable llegó en 2023, y la tendencia continuó en alza desde entonces. Solo en el primer trimestre de 2026, descubrimos 16 actores nuevos. Si la tendencia continúa, la cantidad de actores nuevos en el mercado en 2026 puede superar la cifra de 2025 por al menos el 25 %.

Este crecimiento probablemente refleje varias cosas a la vez. Los ataques DDoS se volvieron más populares en general, especialmente en los últimos años. Las tensiones geopolíticas fomentaron que los grupos de hacktivistas lanzaran campañas más frecuentes, lo que convirtió a DDoS en un tipo más común de ataque. Al mismo tiempo, las herramientas stresser de código abierto bajaron la barrera de entrada.



Batallas por la atención

La visibilidad importa tanto como la capacidad en este mercado. Un proveedor de recursos que no se puede encontrar o recordar tiene pocas chances de adquirir clientes, sin importar los métodos de ataque que afirmen ofrecer. Para mantenerse visibles, los actores DDoS se promocionan en varios niveles de la Web, de agregadores DDoS a foros privados de ciberdelincuentes.

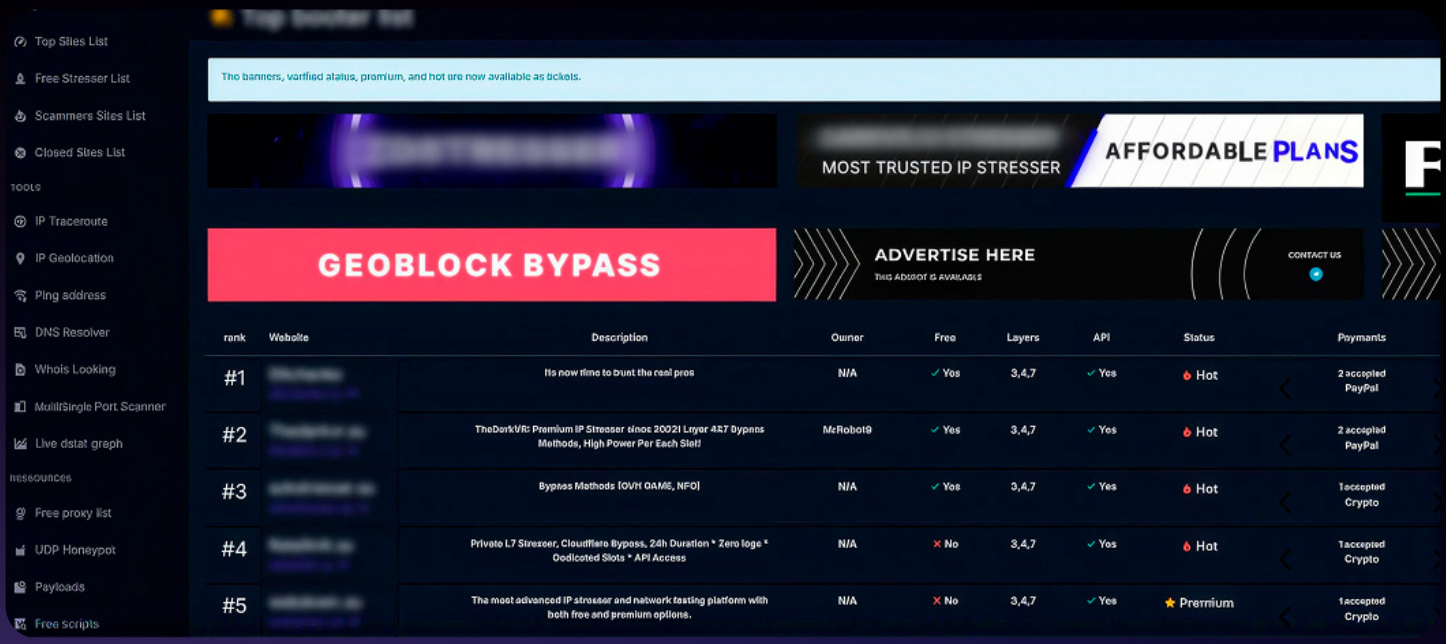


Estas plataformas no tienen el mismo propósito. Algunas están diseñadas para comparar servicios, mientras que otras se basan en spam o reputación. Juntas, forman un panorama de publicidad, en el que los actores compiten por visibilidad.

Junto a estos canales más familiares, identificamos un mecanismo de publicidad más novedoso y distinto: plataformas de tabla de clasificación. Debido a que se diferencian de los canales de promoción normales tanto en forma como en función, se analizan por separado en la sección La tabla de clasificación oscura.

Agregadores DDoS

Son sitios web que recopilan diversos servicios DDoS en un solo lugar. Clasifican a los proveedores por "nivel de confianza", comentarios de los usuarios y niveles de ataque declarados. De esta manera, convierten los servicios clandestinos en catálogos que se pueden buscar.

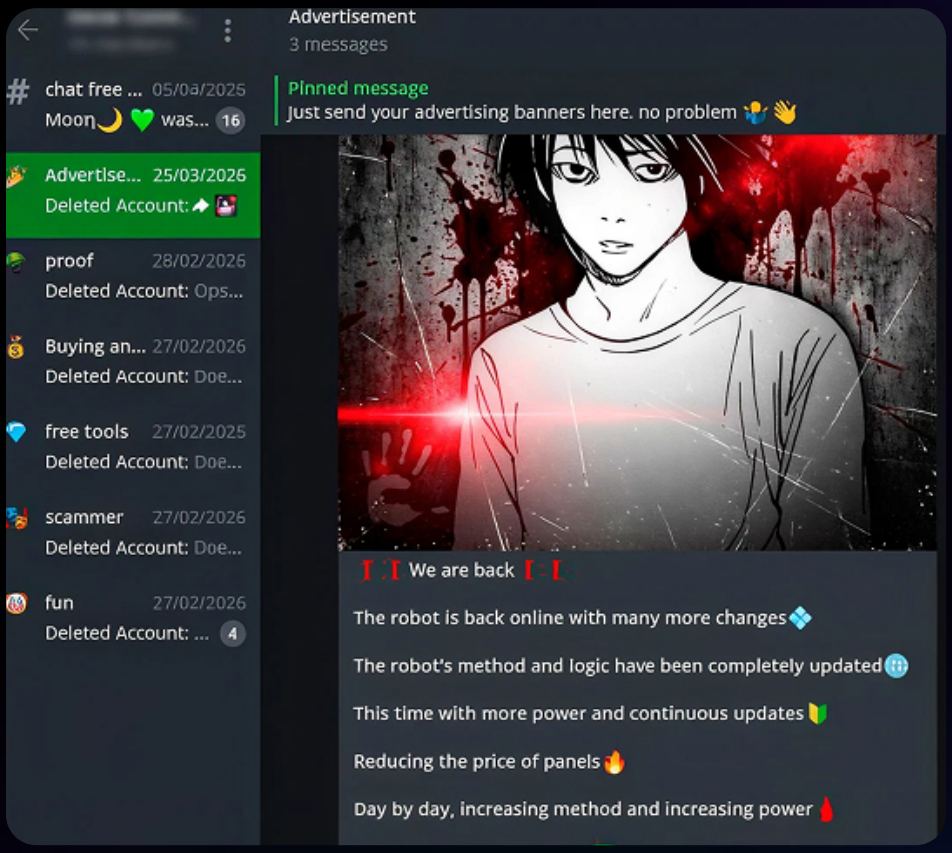


Ejemplo del sitio web de un agregador DDoS

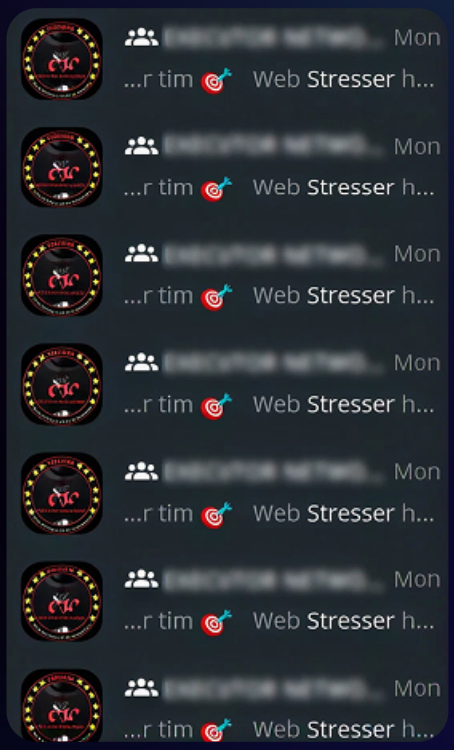
Spam en aplicaciones de mensajería

Otra ruta común es la promoción directa a través de plataformas de mensajería. Aquí, los actores publicitan mediante el envío de mensajes repetidos a uno o varios canales, a menudo intentando llamar la atención por el volumen, en lugar de la credibilidad.

En algunos casos, los administradores de canales crean hilos exclusivos para publicidades a fin de que el spam no interrumpa la conversación general.



Ejemplo de un canal de publicidad exclusivo

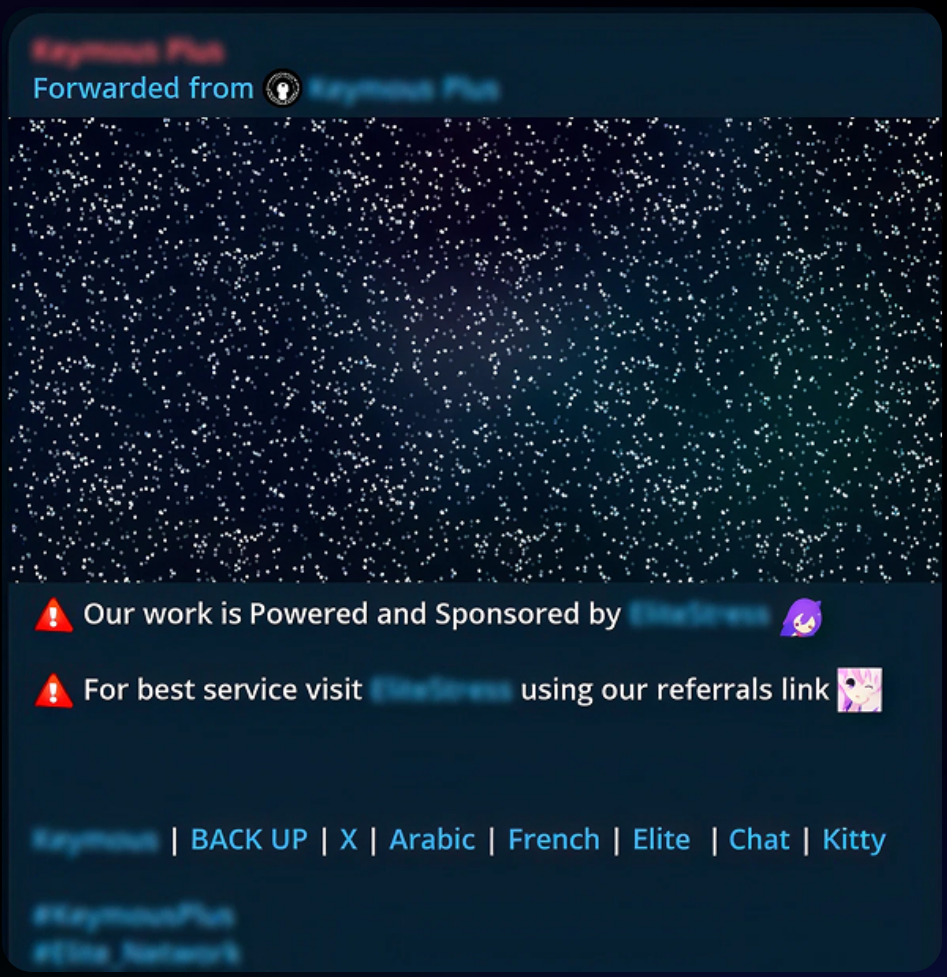


Ejemplo de una publicidad con spam en una aplicación de mensajería

Colaboración de hacktivistas

Los grupos de hacktivistas no solo reclutan personas para realizar ataques motivados por ideologías. En algunos casos, crean alianzas con proveedores de recursos DDoS para sumar capacidad a sus propias campañas. Los grupos con mayores capacidades tienen suficientes recursos para crear su propia infraestructura. Al menos cuatro grupos de hacktivistas activos publicitaron herramientas DDoS propias.

Para los proveedores, estas alianzas también tienen un fin promocional. Los canales de hacktivistas se utilizan como prueba pública de capacidad: los ataques se anuncian, los resultados se comparan y el proveedor obtiene visibilidad a través de la asociación con una campaña activa. En nuestro conjunto de datos, nueve proveedores demostraron una afiliación con hacktivistas.

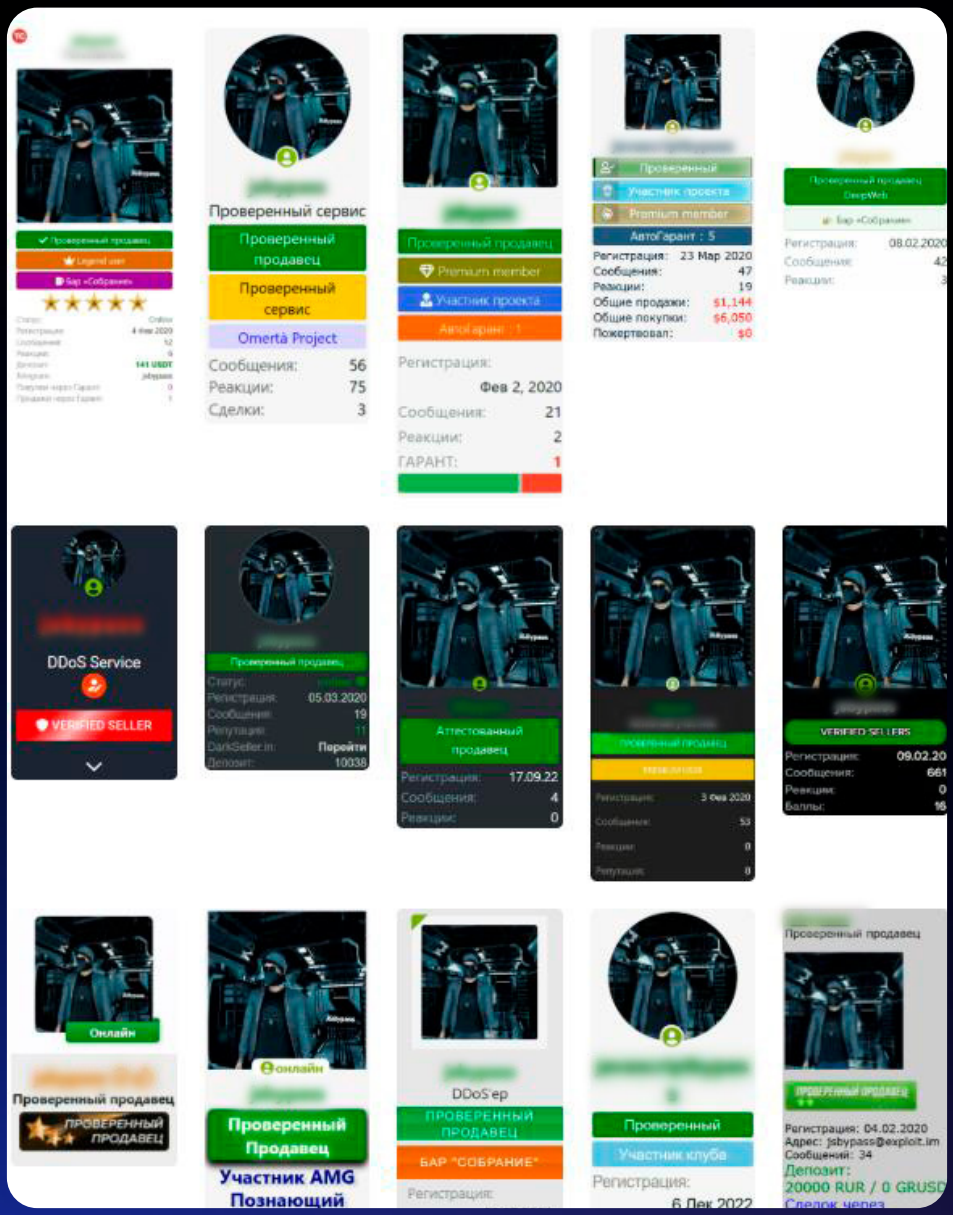


Ejemplo de una declaración de alianza entre hacktivistas y un servicio stresser

Foros de ciberdelincuentes

Los foros de ciberdelincuentes siguen siendo uno de los espacios más consolidados para la promoción de DDoS. Diversos foros especializados se presentan como lugares para analizar las tecnologías de protección DDoS; sin embargo, la evidencia sugiere que también funcionan como espacio de publicidad para los proveedores de ataques. Los foros de ciberdelincuentes más generales, que no se especializan en un único tema, a menudo contienen secciones exclusivas para publicidades relacionadas con DDoS.

En este contexto, un sistema de reputación de foros se vuelve parte de un discurso de venta. Muchos actores publicitan en varios foros a la vez y comparten explícitamente vínculos a otras plataformas para reforzar su reputación o satisfacer las comprobaciones antiestafa de un foro.



Ejemplo del perfil de un actor en diferentes foros



Ejemplo de cuentas de actor en diferentes foros

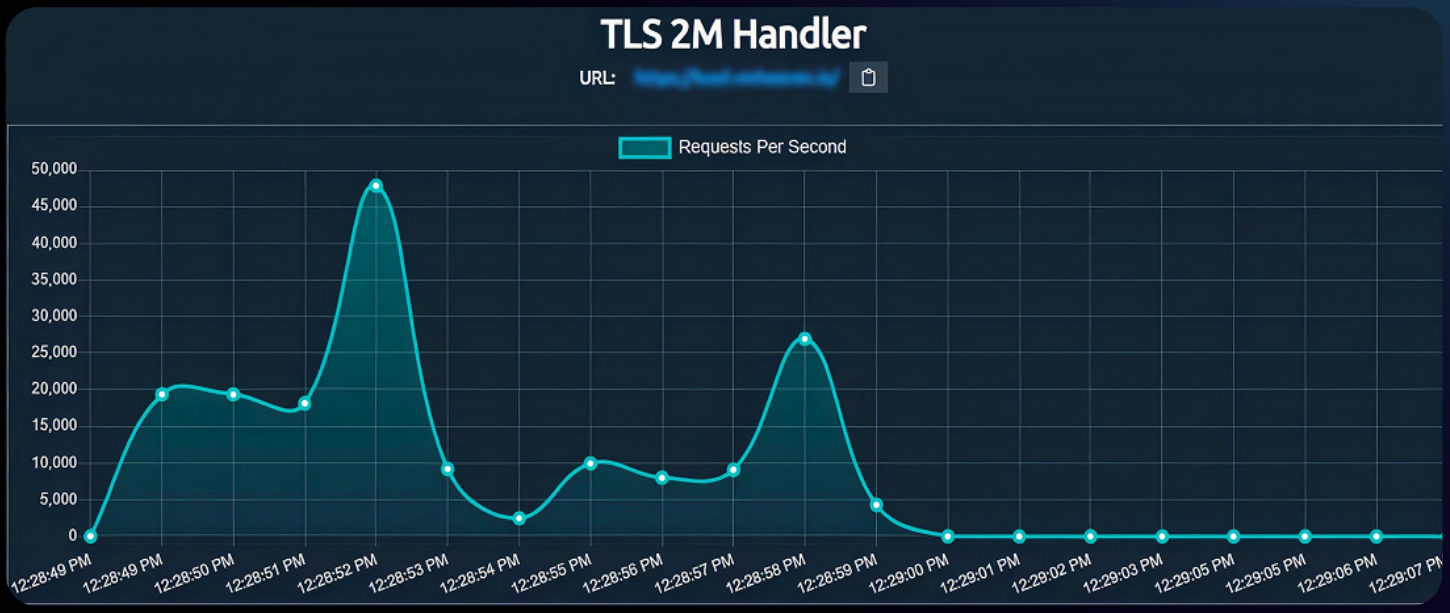
El efecto de la tabla de clasificación

Algunos actores no tienen en cuenta los típicos canales publicitarios en absoluto. En cambio, usan sitios web exclusivos o bots de Telegram para convertir su capacidad de ataque en algo mensurable y tangible. Dichos sistemas a menudo se conocen como DSTAT, que toman el nombre prestado de la herramienta de supervisión del sistema. Esta herramienta se implementa en servidores, la operan proveedores de DDoS o se crean específicamente para actividades de clasificación. Un sitio web o bot de Telegram funciona como una interfaz para la supervisión de ataques y la clasificación de usuarios.

Un participante interactúa con el bot o sitio web, elige los servidores y métodos de ataque, recibe una URL de destino y ejecuta un ataque en ella. Durante el tiempo de cálculo, el bot o sitio web registra las características del tráfico, como solicitudes por segundo o Gbps. Luego, el resultado se agrega a una tabla de clasificación pública bajo el nombre del participante.

	Website	Telegram bot
Nombre típico	dstat.*	*Recuento*
Tabla de ataque en vivo	Sí	No
Selección de nivel de ataque	Sí	Sí
Selección de método	Sí	Sí
Puede utilizarse de forma anónima	Sí	No, de manera predeterminada
Facilidad de acceso	Menor	Mayor

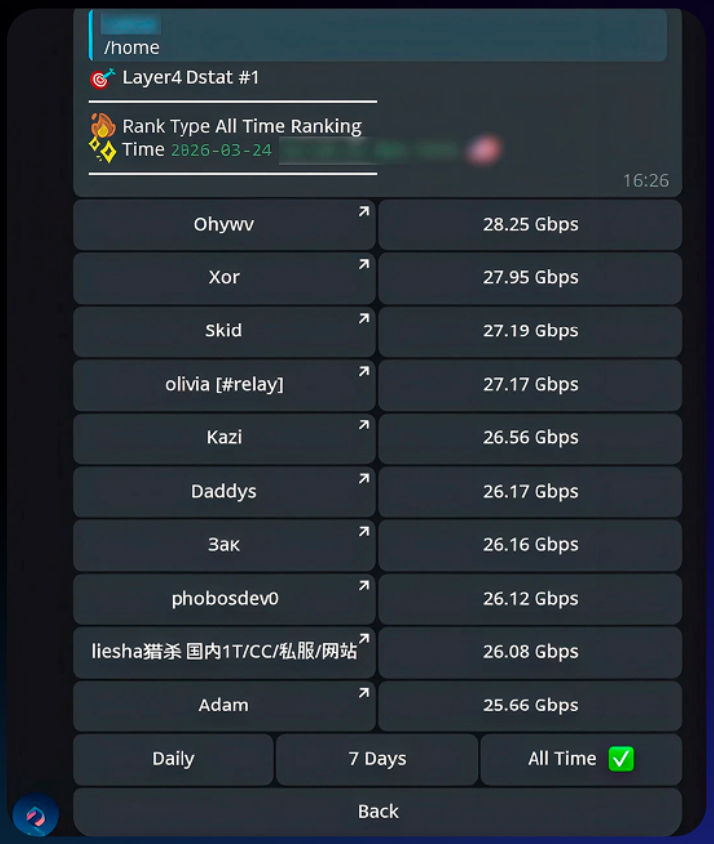
El punto no se limita solo a la medición. Estas tablas de clasificación son de público conocimiento. Les proporcionan a los actores una forma de comparar potencia, competir por visibilidad y publicitar sus servicios en el mismo espacio. En algunos chats, esta lógica se exagera: los grupos lanzan competencias a largo plazo y ofrecen premios a los actores que se mantienen en la primera posición durante seis meses seguidos.



Ejemplo de una lista en un sitio web de tabla de clasificación



Ejemplo de un registro de ataque en un bot de Telegram



Ejemplo de una tabla de clasificación en un bot de Telegram

Más allá del DDoS

La capacidad DDoS rara vez existe aislada. La misma infraestructura utilizada para generar un gran volumen de tráfico y el mismo conocimiento utilizado para eludir protecciones se pueden reutilizar para diferentes actividades maliciosas. En nuestro conjunto de datos, el 43 % de los proveedores de recursos que publicitó en foros de ciberdelincuentes también promocionó servicios secundarios.

Dividimos estos servicios secundarios en dos grupos generales. El primero, la reutilización de activos, incluye infraestructura, malware e instrumentos de ataque readaptados para servicios adyacentes. El segundo, la reutilización de conocimientos, se trata de convertir la experiencia en ofertas de defensa, asesoría y capacitación.

Materiales



Abuso masivo

- Suplantación de identificador de llamadas
- Spam de correo
- Suspensiones de cuentas/ denuncias masivas
- Lista negra de sitios web
- Reclamaciones de eliminación de dominios

33 %



Instrumentos

- Botnets de stealers
- Alquiler de VPS
- ventas de botnets o scripts
- Ventas de exploits DDoS

38 %

Habilidad comercial



- Servicios anti-DDoS
- Capacitación DDoS

19 %

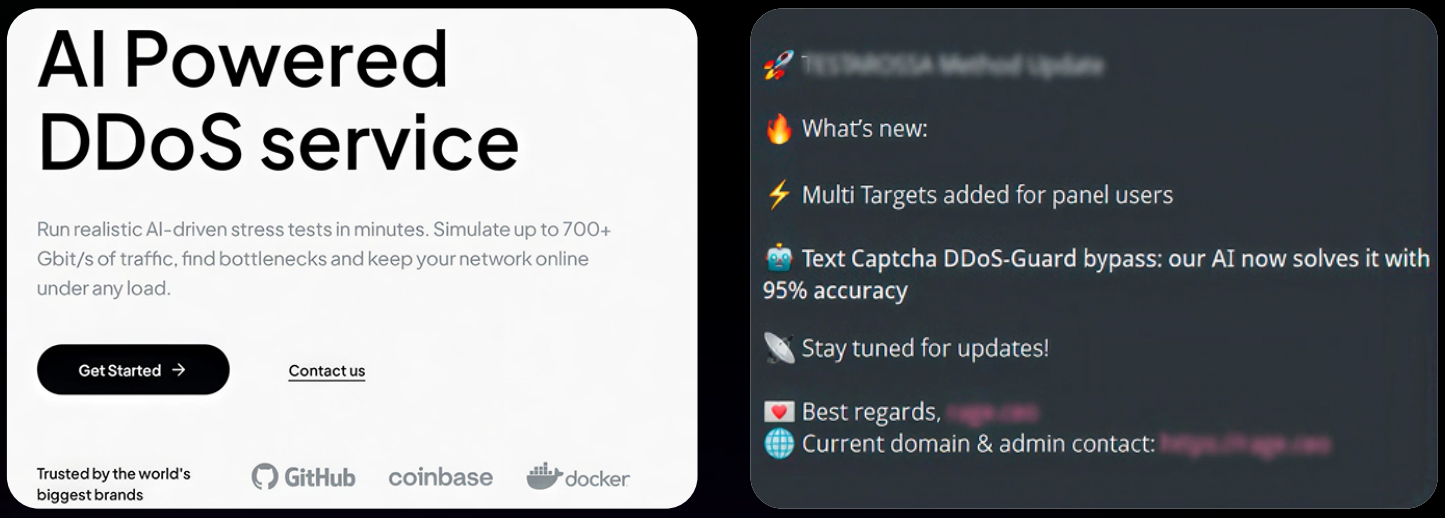
Algunas de estas actividades secundarias son cercanas a DDoS, como las ventas de scripts, el alquiler de VPS o los servicios anti-DDoS. Otras aplican la misma infraestructura o lógica operativa a modelos de abuso adyacentes, desde campañas de spam hasta denuncias masivas o reclamaciones de eliminación.

Potencia en evolución

Para mantenerse competitivos, los proveedores de recursos cambian los ataques que ofrecen. En nuestro conjunto de datos, los atacantes favorecieron sistemáticamente los métodos DDoS patentados por sobre las herramientas públicas. Los scripts de código abierto siguen estando disponibles, pero los actores utilizan soluciones personalizadas para brindar ataques más sólidos y aumentar sus posibilidades de eludir la protección anti-DDoS.

Este desarrollo incluye amplificación de tráfico personalizada, manipulación de solicitudes más avanzada y técnicas de evasión adaptativa diseñadas para hacerse pasar por tráfico legítimo. Algunos actores también indicaron haber explotado debilidades DoS conocidas o imitado comportamientos reales del navegador para pasar los controles defensivos.

La presión competitiva se puede ver en las publicidades; el 33 % de los actores declaró explícitamente la capacidad de eludir protecciones anti-DDoS. En estas declaraciones, identificamos 32 proveedores anti-DDoS que cubrían la protección L4, L7 y de servidores de juegos. Muchos menos actores también mencionaron técnicas impulsadas por IA para eludir los desafíos CAPTCHA.



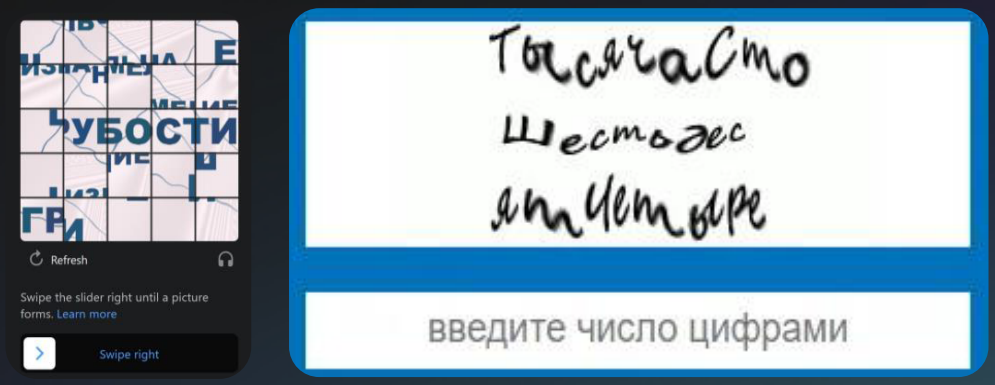
Ejemplos de publicidades con métodos impulsados por IA

Reglas de compromiso

La mayoría de los proveedores de nuestro conjunto de datos no especificó restricciones de objetivos. Sin embargo, un conjunto de datos más pequeño estableció límites claros en cuanto a quién y qué estaban dispuestos a atacar. Estas restricciones por lo general eran técnicas, pero en algunos casos reflejaban preferencias particulares.

Las restricciones observadas recaen en varios grupos:

- Restricciones basadas en TLD: objetivos en dominios *.org, *.gov, *.edu y *.med.
- Objetivos web técnicamente ineficientes: dominios *.r2.web y sitios web estáticos, que requieren tráfico desproporcionadamente alto.
- Protecciones anti-DDoS específicas: objetivos protegidos por CAPTCHA cirílicos que los servicios de IA apenas pueden descifrar.
- Basado en la categoría de servicios: en especial, servidores de juegos y recursos *.onion.
- Función de servicio: por ejemplo, entidades grandes y bancos.



Ejemplos de CAPTCHA cirílico

Estos límites sugieren que incluso en un mercado desarrollado en torno a la interrupción, no todos los objetivos son igualmente deseables. En algunos casos, la opción es más práctica: algunos servicios son más difíciles de atacar o resultan menos rentables.

Al mismo tiempo, la geografía no suele ser una limitación importante. Los proveedores a menudo destacan que pueden atacar sistemas de todo el mundo.



En una publicidad de ejemplo de nuestro conjunto de datos, un actor mencionó explícitamente su alcance global. Se explica por el uso de un conjunto de proxies diverso, que ayuda a eludir las medidas de bloqueo geográfico utilizadas por los proveedores anti-DDoS.

Resumen

DDoS pasó de ser una técnica de ataque independiente a un sector de ciberdelincuencia consolidado.

La accesibilidad sigue siendo uno de los principales factores que impulsan el crecimiento de este mercado, lo que reduce la barrera de entrada tanto para actores de amenaza inexpertos como para actores muy capacitados. En la actualidad, los servicios DDoS se distribuyen a través de operaciones intermediadas, plataformas stresser y una infraestructura basada en Telegram que está ganando popularidad desde 2022.



Bots DDoS de Telegram

- 27 % del mercado de DDoS como servicio
- está pasando de sitios web a interfaces de Telegram

Los DDoS son llevados a cabo por una gama de actores que tienen diferentes fines: de operadores de ransomware y hacktivistas a oportunistas que actúan en beneficio personal.



Los ataques DDoS pueden afectar de pequeñas a grandes empresas de cualquier sector

Rango de precios de servicio

$1 - $30 000

La expansión del mercado se puede observar si analizamos la cantidad de actores nuevos, que sigue creciendo desde 2023. Las posibles causas de este crecimiento son las tensiones geopolíticas que fomentaron a los grupos de hacktivistas a lanzar campañas más frecuentes y la popularidad de las herramientas stresser de código abierto que bajó la barrera de entrada.

La infraestructura DDoS se está expandiendo a operaciones de ciberdelincuentes adyacentes: el 43 % de los proveedores también publicitó servicios secundarios como ventas de exploits DDoS, ventas de scripts y botnets, denuncias masivas y spam, "servicios de protección DDoS" y otros. La presión competitiva está impulsando una rápida adaptación técnica, en especial en capacidades de elusión, métodos de ataque específicamente diseñados y potencia de ataque.

23 % de los actores publicitó la capacidad de atacar juegos con paquetes diseñados específicamente

36 % de los actores afirmó realizar ataques a escala Tbps

33 % de los actores afirmó brindar la funcionalidad de elusión anti-DDoS

Uso emergente de técnicas de elusión de CAPTCHA con IA e imitación de navegador

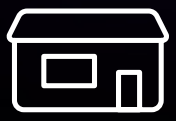
El mercado DDoS desarrolló un ecosistema de ciberdelincuencia consolidado que está respaldado por modelos de suscripción, automatización, accesibilidad global y evolución técnica continua.

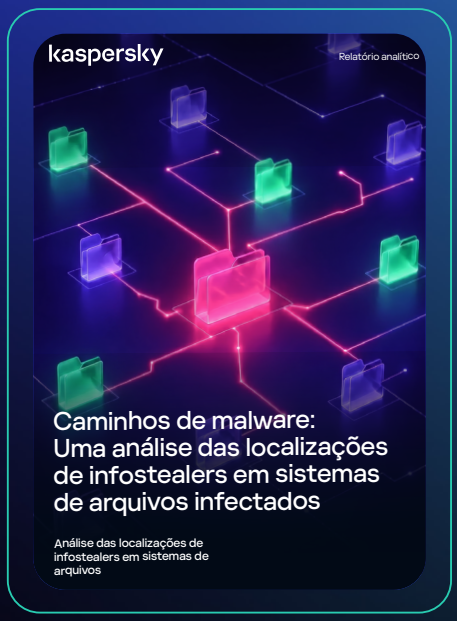
Recomendaciones

Complejidad de la implementación

Ejecutar simulaciones DDoS controladas	Utilizar pruebas de estrés o ingeniería del caos para validar las defensas con regularidad, en especial por el bajo costo y la gran disponibilidad de los servicios DDoS
Implementar protección DDoS multicapa	Los ataques modernos apuntan no solo al ancho de banda en L3/L4, sino también a la CPU y a la memoria a través de solicitudes L7 diseñadas
Controlar la inteligencia de las botnets y enriquecer las detecciones con IoC	Utilizar infraestructura conocida, indicadores e información acerca de los actores para detectar y bloquear actividad maliciosa con mayor rapidez
Implementar detección y respuesta automatizadas	A medida que los ataques DDoS se desarrollan y generan grandes cantidades de telemetría, la automatización es fundamental para una mitigación oportuna
Utilizar una CDN y un proxy inverso	La distribución de tráfico, la protección del origen y la eliminación de puntos de falla individuales son fundamentales para resistir a los ataques DDoS
Separar los servicios importantes y habilitar el autoescalado	Aislar a las funciones críticas del resto de la infraestructura y escalarlas con rapidez cuando aumenta la demanda

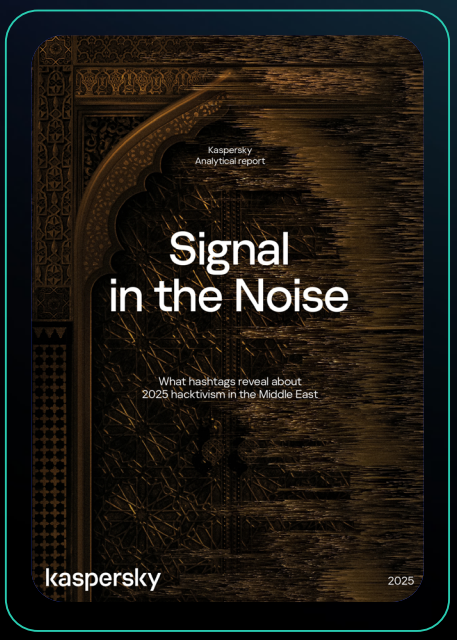


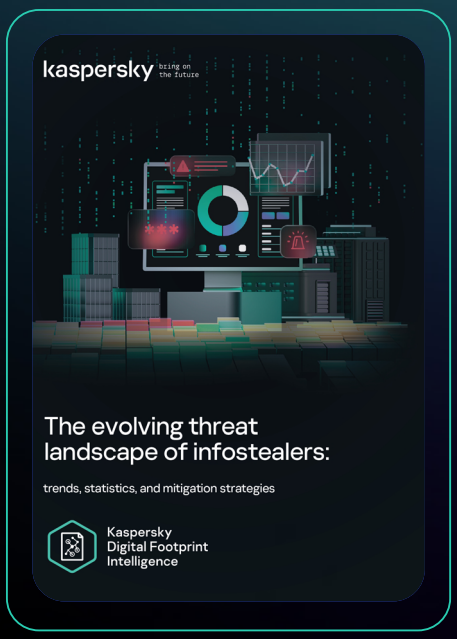












Los demás informes están disponibles en el sitio web

Más información

kaspersky

latam.kaspersky.com