corero

[NETWORK SECURITY]

2025 INFORME DE INTELIGENCIA SOBRE AMENAZAS

Prólogo del Director Técnico

Ashley Stephenson

Director de Tecnología y Productos
Corero Network Security

Cada año, los datos cuentan una historia. No sólo sobre lo que hacen los atacantes, sino sobre lo que están dispuestos a apostar. En 2024, apuestan por la velocidad, la automatización y el acceso. ¿Y por qué no iban a hacerlo? Las herramientas son baratas. La infraestructura está en todas partes. Las barreras son bajas. Lo que antes requería una coordinación sofisticada ahora se puede lograr cada vez más con unos pocos dólares, una red de bots alquilada y algún código de malware reciclado o replicado por IA.

En Corero, llevamos años analizando las tendencias de los ataques DDoS. Y aunque algunas de las tendencias nos resultan familiares–los ataques rápidos y breves siguen dominando–hay matices que exigen atención. La frecuencia ha aumentado. El volumen vuelve a aumentar. El centro del espectro de ataques está reduciendo. Lo que queda es una mezcla de presión oportunista y fuerza bruta estratégica, alimentada por la automatización y la adaptación constante.

Y al igual que evolucionan los atacantes, también lo hace la arquitectura a la que se dirigen. Con el aumento de los entornos de nube híbrida y el cambio hacia la repatriación de las cargas de trabajo críticas a la infraestructura local, la complejidad de la defensa es cada vez mayor. Las rutas de tráfico son menos predecibles. Los puntos de aplicación están más distribuidos. Y para muchas organizaciones, eso significa más puntos ciegos o puertas efectivamente "abiertas".

El informe de este año refleja no sólo lo que vemos en los datos, sino para lo que nos estamos preparando. Las amenazas ya no están limitadas por el ancho de banda o la geografía. Están construyendo infraestructuras más inteligentes, reutilizando continuamente los dispositivos comprometidos y atacando cada vez más la capa de aplicaciones. Como defensores, necesitamos igualar esa adaptabilidad con visibilidad, automatización y velocidad.

Esta complejidad se manifiesta en nuevos retos para la respuesta de los defensores. Según un estudio de Merrill Research, muchos equipos afirman tener dificultades para coordinarse en distintos entornos, seguir el ritmo de las amenazas y actuar con rapidez en la mitigación. El reto no es sólo el volumen de ataques, sino la fricción operativa que ralentiza la defensa.

Nuestra misión en Corero es dar a las organizaciones el poder de ver, detener y evolucionar más rápido que las amenazas a las que se enfrentan. Nuestra misión nunca ha sido más urgente.

Gracias por leer, y por formar parte de la comunidad que defiende lo que importa.

Resumen Ejecutivo

En 2024, los atacantes DDoS no reinventaron su estrategia, sino que la perfeccionaron. Los datos cuentan una historia de ataques implacables y de alta frecuencia llevados a cabo con una eficacia y escala sorprendentes. Los ataques rápidos, cortos y de menos de 10 Gbps siguieron dominando, como lo han hecho durante años, lo que subraya un modelo de amenaza persistente y en evolución en el que la interrupción es barata, accesible y alarmantemente eficaz.

Nuestro análisis de los patrones de tráfico de los clientes muestra que las organizaciones que supervisamos se enfrentaron a una media de 11 ataques DDoS al día en 2024, un 5% más que el año anterior. La mayoría de estos ataques tenían un tamaño inferior a 1 Gbps, capaz de deslizarse por debajo de los umbrales volumétricos tradicionales sin dejar de interrumpir la disponibilidad y el rendimiento. Estos resultados refuerzan una tendencia que hemos observado año tras año: la frecuencia es el arma preferida de los atacantes.

Aunque dominan los ataques pequeños, están aumentando los de mayor escala. Los ataques que superan los 10 Gbps aumentaron hasta el 2,9 % de todos los eventos observados, la cifra más alta desde 2018. Creemos que esto refleja un aumento de la capacidad y automatización de las redes de bots, impulsado por la explotación de dispositivos vulnerables como los routers MikroTik y derivados del malware Mirai que se ejecutan en dispositivos IoT.

Al mismo tiempo, los ataques de tamaño medio, entre 5 Gbps y 10 Gbps, siguen disminuyendo, pasando del 19 % en 2019 a solo el 12,4 % en 2024. El "nivel medio" de DDoS se está desvaneciendo a medida que los atacantes se polarizan: muchos utilizan sondeos ubicuos de bajo volumen para probar las defensas, mientras que otros desencadenan campañas estratégicas de gran volumen para abrumar la infraestructura específicamente dirigida.

El análisis trimestral revela una estacionalidad constante. Los trimestres tercero y cuarto siguen siendo los periodos de mayor actividad de ataques, coincidiendo con las temporadas de mayor tráfico comercial y los periodos en los que el personal puede estar sobrecargado. Curiosamente, en el segundo trimestre de 2024 se produjeron menos ataques en general, pero una mayor proporción de ataques de gran envergadura, lo que podría ser una señal de reconocimiento o de pruebas preparatorias de campañas de mayor envergadura.

Los ataques a la capa de aplicación (capa 7) también están aumentando en todo el sector. Las inundaciones HTTP, los ataques a API y las campañas DDoS específicas de plataforma son cada vez más comunes, ya que los atacantes buscan una interrupción más allá de la simple saturación del ancho de banda. A medida que las defensas de las aplicaciones se convierten en el próximo frente de batalla, las organizaciones deben estar preparadas para defender no sólo la red, sino la propia lógica empresarial.

La conclusión es clara:

El DDoS se está convirtiendo en un estado de constante presión de fondo. Los atacantes confían en la automatización, la asequibilidad y la distribución a escala de infraestructura para mantener a las víctimas en una postura reactiva, enfrentando amenazas que no dejan de aparecer. Lo que siempre ha funcionado sigue funcionando. Hasta que los defensores se pongan al día en velocidad, visibilidad y automatización el DDoS seguirá siendo una de las herramientas más eficaces y persistentes del arsenal del atacante.

DDoS es fácil. La defensa DDoS aún no lo es.

Leer Entre Paquetes

Cada ataque deja un rastro. En 2024, nuestra telemetría global capturó cientos de miles de estos rastros, patrones de frecuencia, volumen, sincronización y tácticas, de ataques reales dirigidos a redes de producción en directo.

Esta sección no es sólo un registro de lo ocurrido. Hemos analizado no sólo el año 2024, sino varios años de datos históricos para sacar a la luz patrones, cambios y estrategias persistentes que configuran el panorama de las amenazas. Es una interpretación de lo que esos patrones significan para los defensores. Porque detrás de cada punto de datos hay una decisión: de un atacante, de un defensor o de un sistema obligado a elegir qué bloquear y qué permitir.

En las páginas desglosamos las tendencias que creemos que definen 2024: qué dicen los datos, por qué importan y qué pueden hacer los defensores en respuesta. Aquí es donde los números se encuentran con el mundo real y donde comienza la verdadera estrategia.

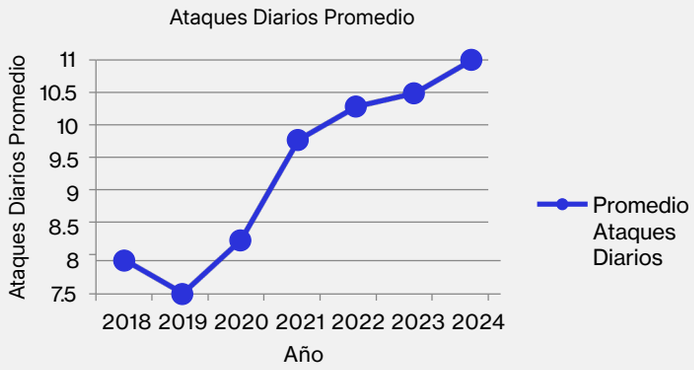
Veamos lo que los atacantes dejaron atrás.

El Pulso de la Presión:
Frecuencia Diaria de Ataques DDoS

LO QUE DICEN LOS DATOS

En 2024, los clientes de Corero experimentaron una media de 11 ataques DDoS al día, frente a 10,48 en 2023. Esto supone un aumento del 5% interanual y forma parte de una tendencia plurianual más amplia. Desde 2018, la media diaria ha aumentado de forma constante, pasando de unos 8 a 11 ataques por cliente y día, lo que supone un incremento del 37,5% en seis años.

Media diaria de ataques DDoS por cliente (2018-2024)



QUE SIGNIFICA

No se trata de un pico, sino de una estrategia. La frecuencia de los ataques no es aleatoria, sino deliberada. A medida que aumenta el número de atacantes, también lo hace la presión de fondo continua, utilizando la automatización y el armamento de infraestructura de menor coste para mantener las defensas activas, abrumadas o insensibilizadas.

Muchos de estos ataques de alta frecuencia son de corta duración y subsaturadores, por lo que es fácil descartarlos como ruido de fondo. Pero cumplen una función clave:

- Detección de puntos débiles
- Medición de los umbrales de mitigación
- Retrasos en la respuesta temporal
- Distraer a los equipos de seguridad de más actividades específicas

En pocas palabras:

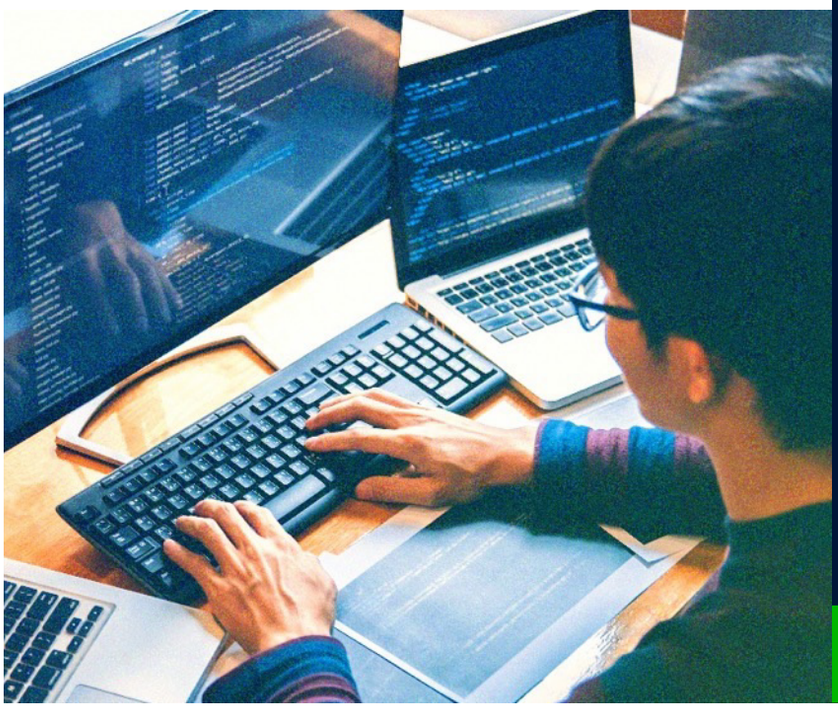
Si defiendes 11 ataques al día, no estás respondiendo a una anomalía...estás operando en un entorno de fuego real.

El Pulso de la Presión

LO QUE PUEDE HACER

Las organizaciones deben tratar los ataques frecuentes como una condición por defecto, no como una excepción. Las acciones clave incluyen:

- Automatice los flujos de trabajo de respuesta para detectar y mitigar sin intervención humana.
- Mejorar la sensibilidad de la detección para identificar anomalías de corta duración y subumbrales.
- Comprenda mejor el comportamiento normal del tráfico, para poder identificar las desviaciones con mayor precisión.
- Refuerce la infraestructura en el perímetro para absorber o desviar ataques de alta frecuencia y bajo volumen sin consumir valiosos recursos internos.



¿Es un Blip o un Ataque DDoS?

¿Cómo saber si estás bajo ataque cuando los indicadores parecen ruido?

Ese es exactamente el problema. La mayoría de los ataques que observamos–especialmente los de menos de 1 Gbps–no causan necesariamente interrupciones obvias. Crean latencia, pérdida de paquetes o interrupciones transitorias que se parecen a cualquier problema común de la red. Muchas organizaciones los tachan de fallos del ISP o del tiempo normal de Internet.

Pero esto es lo que distingue a estos sucesos como atentados:

1. Siguen patrones: quizá la hora del día, características de protocolo similares, o las mismas regiones de origen.
2. Coinciden con campañas de escaneado, sondeo o relleno de credenciales más amplias.
3. Desaparecen o se van rápidamente cuando las defensas se activan–un comportamiento anómalo para cortes reales.
4. Vuelven una y otra vez, a menudo con forma diferente.

Si observa un patrón de interrupciones de corta duración y aparentemente menores, es posible que no se trate de una infraestructura poco fiable.

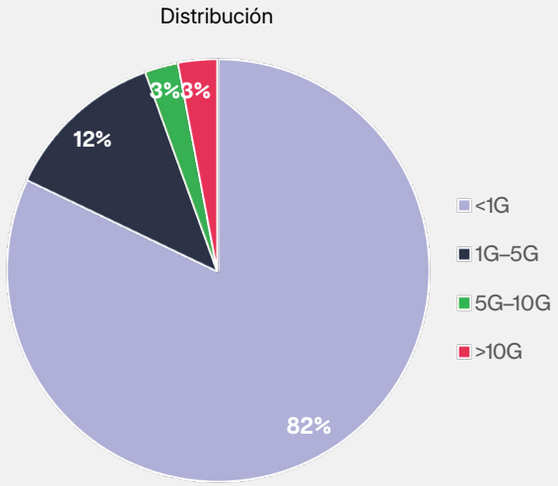
Puede que estés tratando con un atacante que está probando tu límites.

Bajo el Radar, Sobre la Línea: Persistencia de los Ataques por Debajo de 10Gbps

LO QUE DICEN LOS DATOS

Más del 82% de todos los ataques DDoS observados en 2024 inferiores a 1 Gbps. Estos ataques a pequeña escala son, con diferencia, los más comunes. A menudo descartados como ruido de fondo, persisten porque son más fáciles de lanzar, más difíciles de detectar y eficaces para degradar la calidad general del servicio o poner a prueba los límites de una defensa.

Distribución del tamaño de los ataques DDoS - 2024



QUE SIGNIFICA

Ataques pequeños no significan impacto pequeño. Estas campañas de menos de 10 Gbps pueden derribar servicios de aplicaciones frágiles, agotar cortafuegos o desencadenar operaciones de escalado innecesarias y costosas en entornos de nube. Son eficaces y, en muchos casos, precursoras de campañas de mayor envergadura. También es importante tener en cuenta que estas cifras no representan necesariamente ataques discretos y que, sin duda, hay casos en los que un atacante puede haber lanzado varios ataques pequeños que se suman a un ataque total mayor.

Los defensores suelen pasar por alto estos ataques no porque sean intrínsecamente sigilosos, sino operan en una zona gris de detección poco vigilada. Podrían disparar alarmas volumétricas o causar interrupciones inmediatamente identificables. En su lugar, se mueven con ligereza, produciendo huellas débiles: retrasos en la carga de páginas, errores 5xx intermitentes o fallos o contratiempos momentáneos del DNS. Estos efectos pueden pasar desapercibidos fácilmente como ruido aleatorio de Internet, pero si se consideran en su contexto, a menudo indican un sondeo coordinado o una degradación deliberada.

La implicación para los defensores es clara: no se trata de artefactos de fondo, sino de señales válidas de ataques potencialmente más perturbadores. Y la mejor forma de sacarlas a la luz es mediante la supervisión del comportamiento y la correlación en el tiempo y los sistemas. Aquí es donde la visibilidad operativa, y no sólo la defensa del ancho de banda en bruto, se vuelve crítica.

Bajo el Radar, Sobre la Línea

LO QUE PUEDE HACER

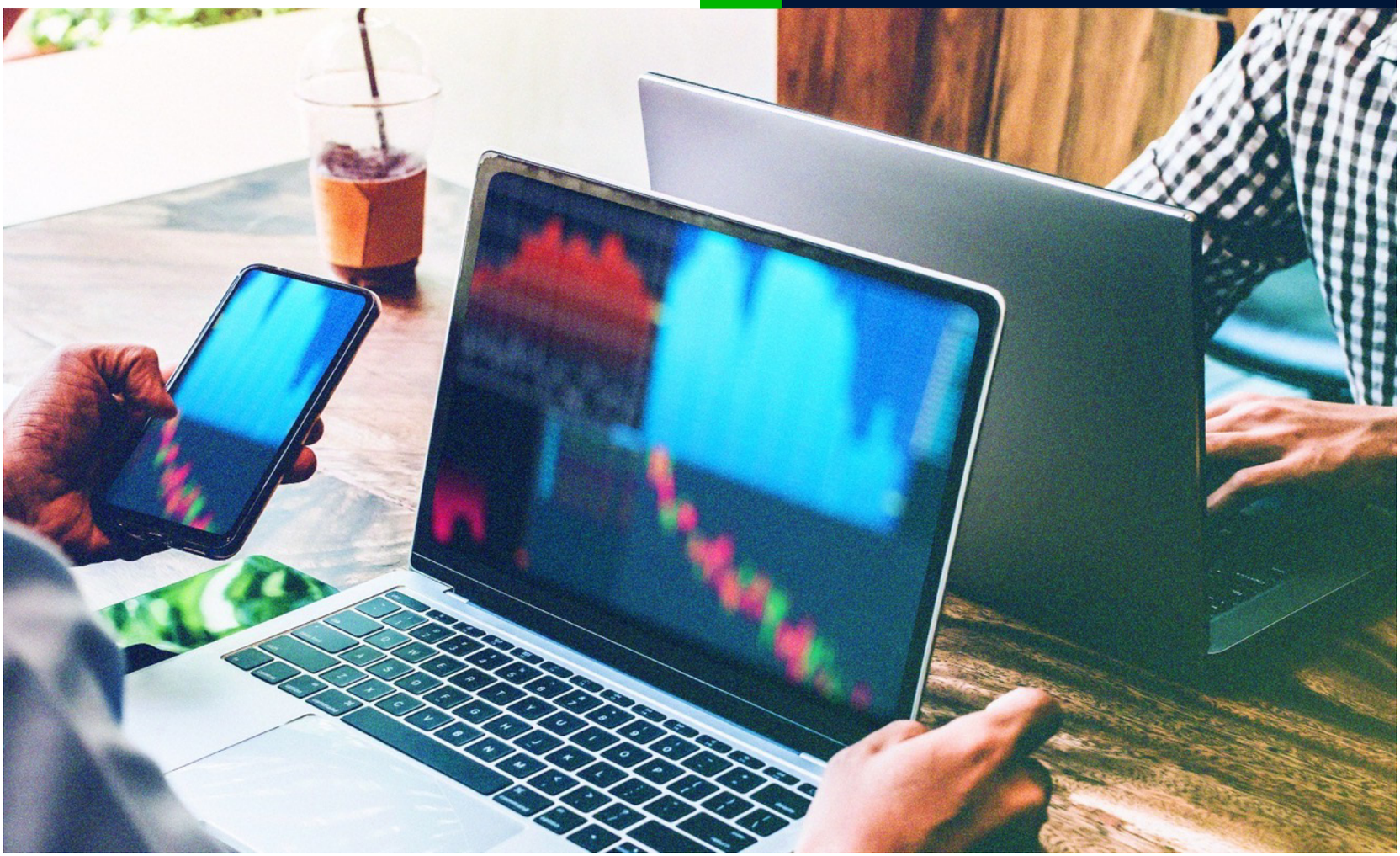
Busque anomalías de rendimiento, como picos de latencia o caídas inexplicables del servicio, como primeros indicadores.

Correlacione eventos en todo su entorno para campañas y de bajo volumen.

Ajuste los umbrales de alerta para captar mejor las perturbaciones pequeñas y persistentes que eluden los activadores volumétricos.

¿Prueba u Objetivo?

Los pequeños ataques no son necesariamente grandes fracasos. Muchos son sondas. Algunos están diseñados para probar umbrales de detección. Otros se dirigen a aplicaciones específicas con la presión suficiente para causar inestabilidad. Conocer la diferencia, prueba frente a objetivo, requiere contexto. Y el contexto proviene de la visibilidad, la telemetría y la investigación.



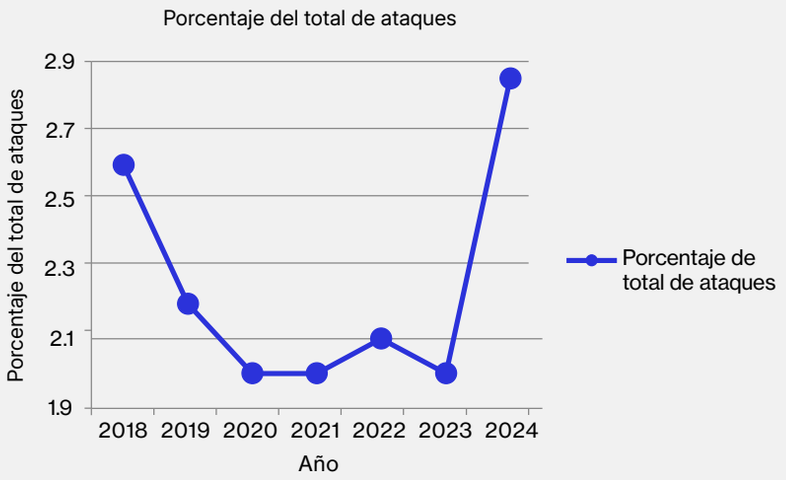
El Regreso de las Redes de Bots más Potentes: Aumento de los Ataques >10Gbps

LO QUE DICEN LOS DATOS

En 2024, el 2,9% de todos los ataques DDoS observados superaron los 10 Gbps de tamaño. Se trata del mayor porcentaje de ataques a gran escala desde 2018, tras varios años de tendencias relativamente planas en estas actividades.

Aunque estos sucesos siguen siendo poco frecuentes en comparación con la categoría dominante de sub-1Gbps, su potencial de perturbación es enorme, y a menudo se dirige a puntos de estrangulamiento de la infraestructura, límites de capacidad de bajada o acuerdos de nivel de servicio.

Crecimiento de los ataques DDoS >10Gbps (2018-2024)



QUE SIGNIFICA

Este crecimiento indica que la potencia de fuego de las redes de bots está aumentando de nuevo, y que los atacantes están accediendo a más botnets. dispositivos u orquestar mejor los que ya controlan.

Entre los factores que pueden contribuir a ello se encuentran:

- Explotación de routers vulnerables y dispostivos IoT, como el hardware MikroTik
- Evolución continua y resurgimiento de malware basado en Mirai.
- Creciente uso de servicios DDoS de alquiler con capacidad de ataque multivectorial.

Estos ataques de mayor envergadura son frecuentes:

- Utilizados como cortinas de humo para los datos exfiltración o movimiento lateral.
- Programado para maximizar la interrupción operativa (por ejemplo, horas punta o durante incidentes).
- Junto con las peticiones de rescate, amenazando ataques repetidos o sostenidos.

El Regreso de las Redes de Bots más Potentes

LO QUE PUEDE HACER

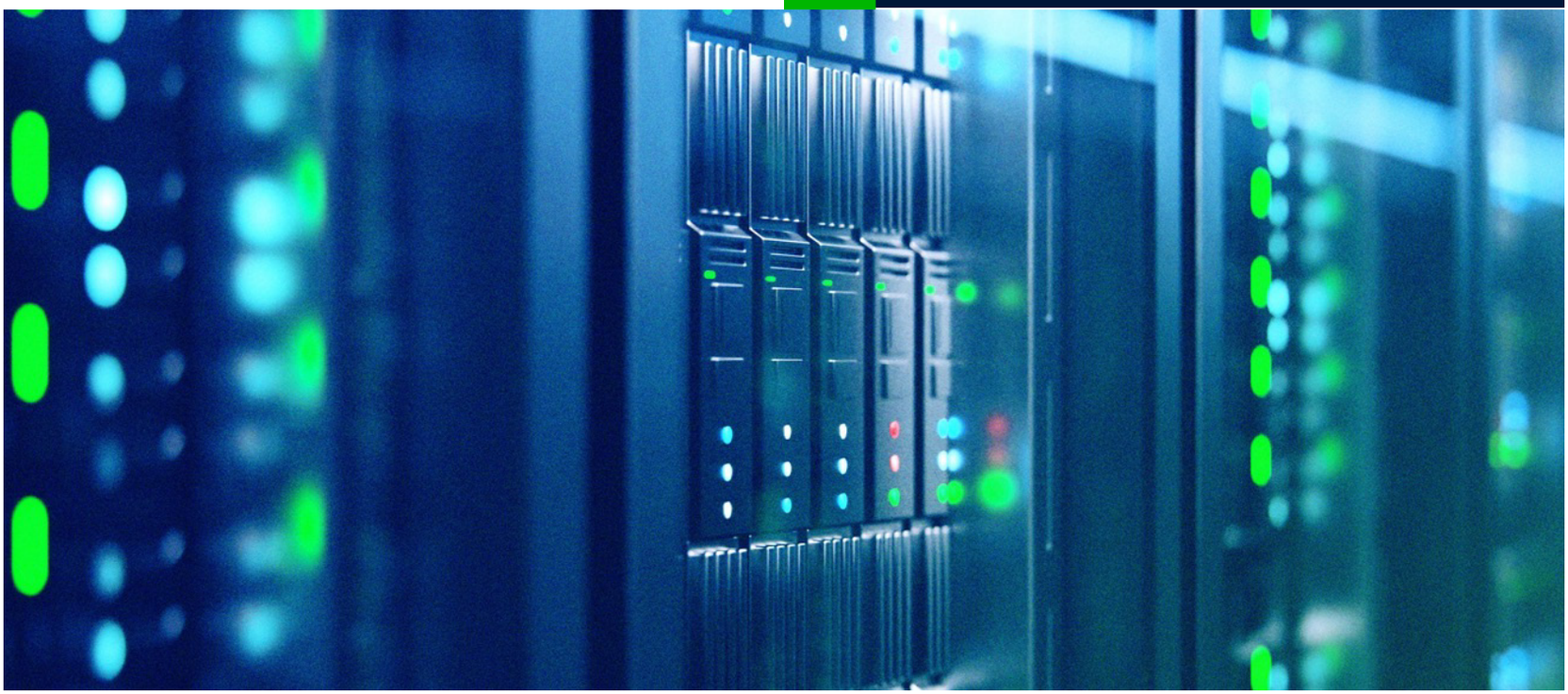
- Conozca sus límites de capacidad. Lo que tu ISP puede absorber ≠ lo que tu infraestructura puede tolerar.
- Colabore con los proveedores de servicios ascendentes para conocer las opciones de redirección de ataques, depuración y conmutación por error.
- Ponga a prueba su respuesta de mitigación ante sucesos simulados a mayor escala (no sólo volumétricos, sino multivectoriales).
- No asuma que la rareza equivale a seguridad. Estos ataques pueden ser menos frecuentes, pero su impacto en los ingresos, las operaciones y la reputación puede ser grave.

Por qué lo grande no siempre es más fuerte

Los ataques a gran escala acaparan titulares, pero no siempre están diseñados para romper Internet. Algunos se utilizan como cortinas de humo para enmascarar intrusiones más sutiles. Otros están programados para generar el máximo estrés operativo: en los cambios de turno, en horas punta o en junto con las demandas ransomware.

Lo que hace que estos ataques sean peligrosos no es sólo su ancho de banda. Es su patrón de selección de objetivos, el momento en que se producen y la perturbación que generan más allá de la red, desde la fatiga de las alertas hasta el pánico ejecutivo.

No confundas rareza con irrelevancia. Los grandes ataques son armas estratégicas, y vuelven al arsenal.



Cuando Llegan las Tormentas: Estacionalidad de DDoS y Sincronización Estratégica

LO QUE DICEN LOS DATOS

Entre 2023 y 2024, Corero observó picos recurrentes en el volumen de ataques durante el 3T y el Q4. En ambos años:

- En el tercer trimestre aumentó la frecuencia total de los ataques, especialmente las ráfagas de menos de 1 Gbps.
- Q4 siguió con una mayor variedad de tamaños de ataque, incluida una mayor concentración de eventos >1Gbps.

En cambio, en el segundo trimestre de 2024 se registró un descenso de la frecuencia, pero una mayor proporción de ataques a gran escala, incluidos los eventos >10Gbps.

Actividad de ataques DDoS por trimestre

2023	75	65	90	95
2024	80	60	88	92

QUE SIGNIFICA

Los atacantes no operan en el vacío—responden a los ritmos empresariales, eventos del calendario y puntos de presión operacionales.

Los patrones estacionales clave pueden incluir:

Q3 La vuelta al cole y las vacaciones (en los sectores del juego, el comercio y la educación).

Q4 Temporada de vacaciones y congelación de los cambios informáticos, que a menudo coinciden con una reducción de personal y un retraso en la respuesta.

Estas tendencias sugieren que la sincronización de los ataques se está volviendo más estratégica, alineándose con los momentos en los que la interrupción hace más daño.

Cuando Llegan las Tormentas

LO QUE PUEDE HACER

Dote a sus defensas de personal teniendo en la estacionalidad. Prevea un aumento de la actividad a finales del tercer y cuarto trimestre.

Aproveche los periodos de bajo volumen, como el primer y el segundo trimestre, para reforzar su infraestructura y probar los flujos de trabajo de mitigación.

Alinee los ejercicios del equipo rojo/equipo azul con los picos de DDoS conocidos para garantizar la cobertura y la confianza.

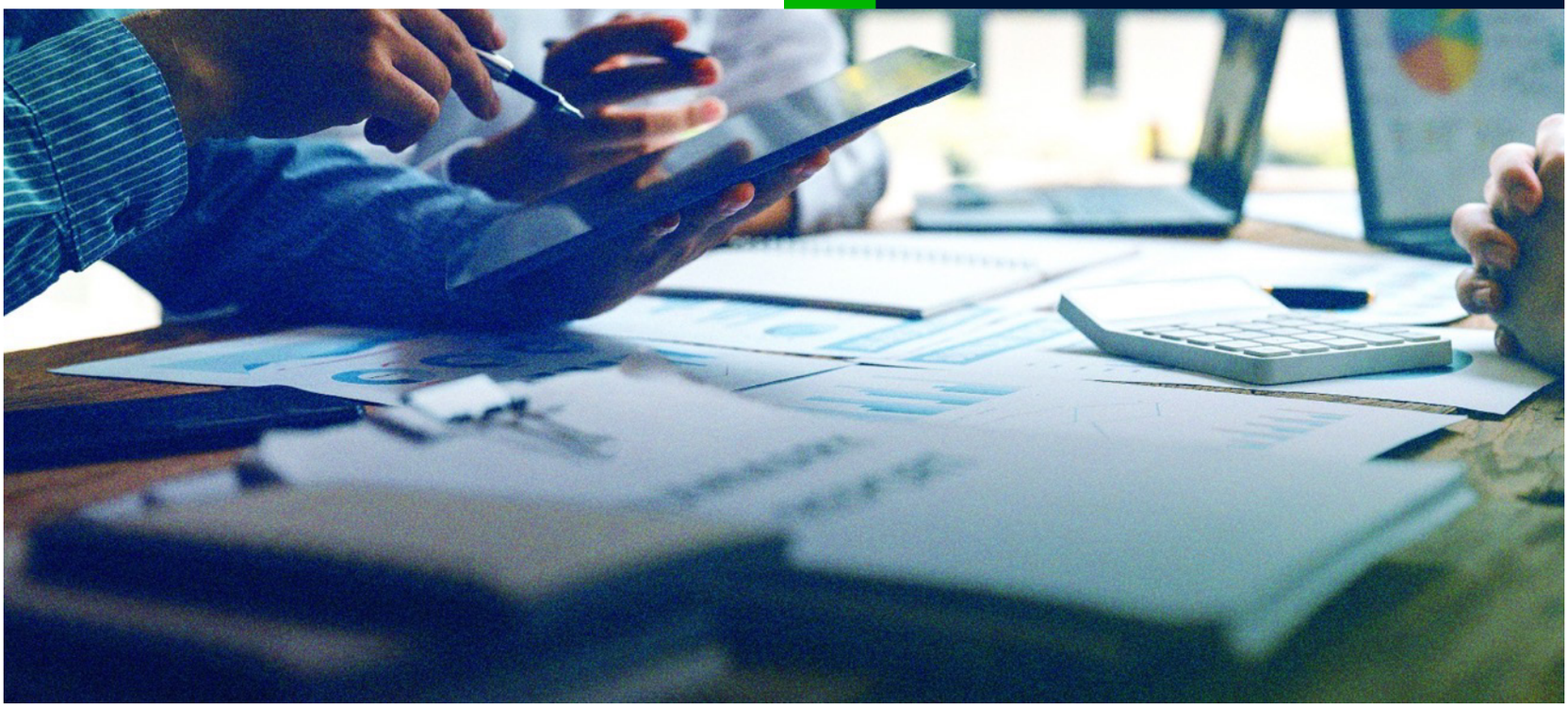
No se fíe sólo de las tendencias medias: fíjese en la estacionalidad histórica para prever las ventanas de presión.

Cuando los Defensores Parpadean

El cuarto trimestre es la estación favorita de los atacantes, no porque haga frío, sino porque los equipos de seguridad no dan abasto. Los presupuestos están congelados. El personal está de vacaciones. Y las ventanas de cambio están limitadas por la tolerancia al riesgo empresarial.

Los atacantes lo saben. Explotan el tiempo tanto como las herramientas, lanzando campañas DDoS cuando el tiempo de respuesta es más lento y la tolerancia a la interrupción es menor.

Si sus defensas dependen de que la gente esté presente, descansada y preparada, entonces la estacionalidad no es sólo un patrón: es una oportunidad para el adversario.



El Medio Misterioso:
El Declive de los Ataques de 1–5Gbps

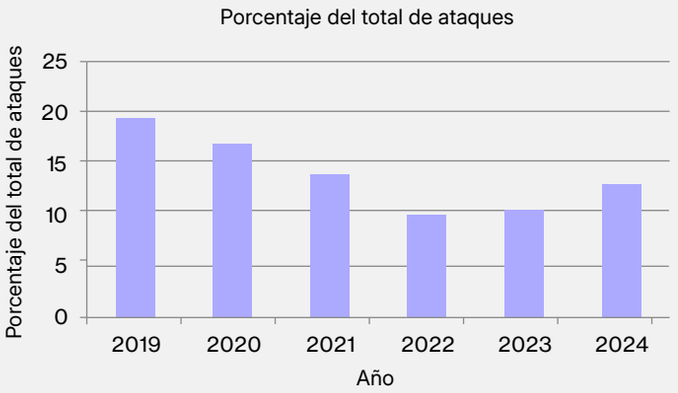
LO QUE DICEN LOS DATOS

En 2019, los ataques en el rango de 1-5Gbps constituyeron casi el 19,4% de todos los eventos DDoS observados. En 2024, esa cifra se había reducido a solo el 12,4 %, un 34 % menos en cinco años.

Aunque se han producido algunos la tendencia a largo plazo de este nivel ha sido a la baja, pasando del 19,4% en 2019 al 12,8% en 2024.

Tal vez sólo está siendo superado por el crecimiento en los ataques de flanco.

Descenso de los ataques DDoS de 1-5Gbps (2019-2024)



QUE SIGNIFICA

Esta tendencia señala una polarización estratégica en el atacante pero el porqué sigue siendo especulativo. Ésta es nuestra opinión:

Muchos atacantes están optando por ataques de bajo volumen y alta frecuencia que evitan la detección y la respuesta de prueba.

Otros pueden estar invirtiendo en inundaciones a gran escala y de gran impacto posibilitadas por botnets e infraestructuras de pago.

¿Se está quedando obsoleto el nivel medio porque es ineficaz? ¿O ya no es eficiente?

La gama de 1-5Gbps:

- Es demasiado pequeño para chocar de lleno con las infraestructuras modernas
- Pero demasiado grande para pasar desapercibido
- Y menos rentable que las alternativas

El alejamiento del centro puede reflejar la evolución de los defensores. Nuestra opinión es que el rango de 1-5 Gbps solía ser un punto ciego para muchos proveedores: lo suficientemente grande como para hacer daño, lo suficientemente pequeño como para colarse. Pero a medida que la protección DDoS maduraba, esa ventana se estrechaba.

Los atacantes se dieron cuenta. Hoy en día, no malgastan ancho de banda donde es probable que se marque y se filtre. Se hacen grandes para abrumar, o pequeños para pasar desapercibidos.

Para los defensores, la red consiste en recalibrar las expectativas. Si su postura de detección y respuesta todavía se centra en la captura de inundaciones de nivel medio, es posible que esté sobrecargado de recursos para lo que ya no es común y poco preparado para los casos extremos.

El Medio Misterioso

LO QUE PUEDE HACER

Vigilar los bordes, no sólo el centro. La lógica de detección debe centrarse en patrones de ráfagas y anomalías, no solo en umbrales fijos.

Evalúe su postura defensiva en ambos extremos del espectro: ¿Puede soportar miles de pequeñas ráfagas? ¿Puede absorber un impacto de 20 Gbps?

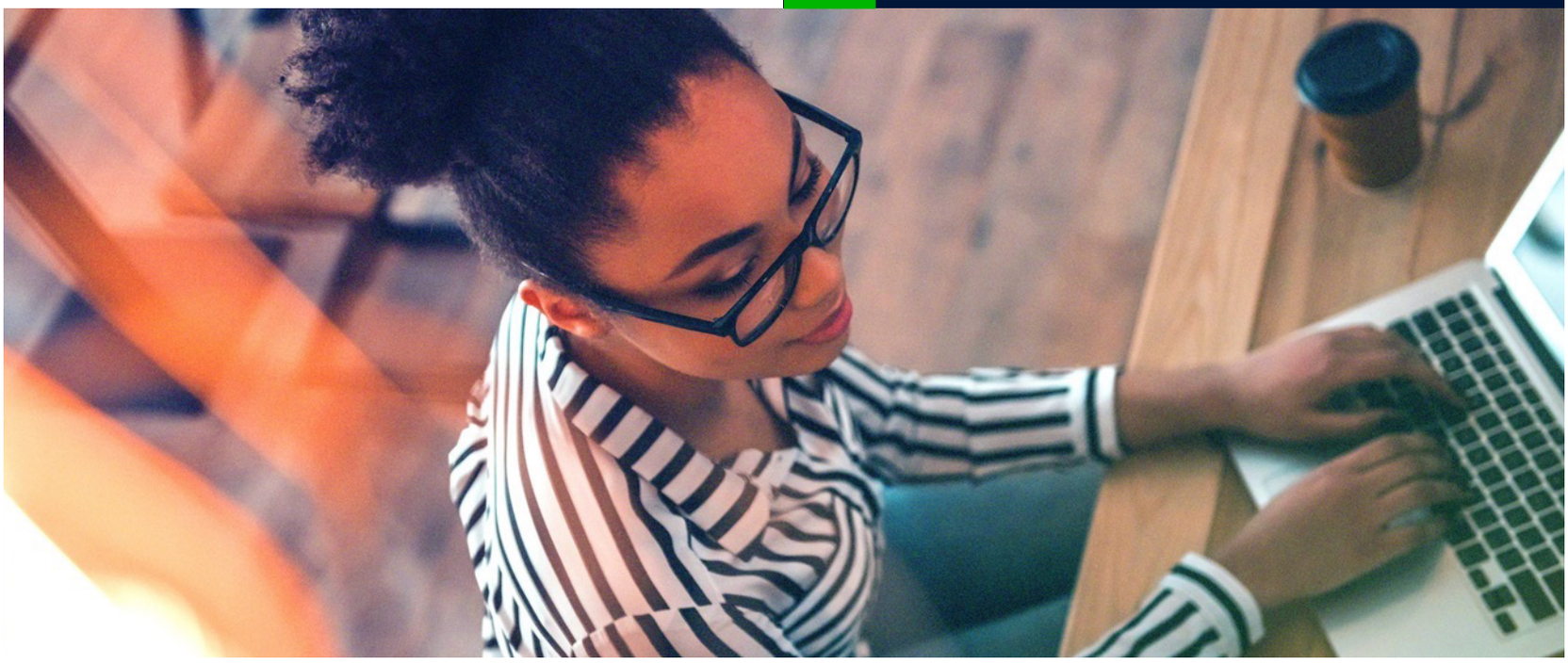
Pruebe el ajuste de mitigación para evitar gastar recursos en exceso en ataques que ya no son frecuentes, pero no elimine la cobertura por completo.

El nivel intermedio de DDoS está desapareciendo

El "nivel intermedio" de los ataques DDoS se está reduciendo como porcentaje de todos los ataques. En el pasado, estos ataques representaban un equilibrio estratégico: lo suficientemente grandes como para afectar al rendimiento, pero lo suficientemente pequeños como para evitar su detección inmediata.

Creemos que los atacantes están optimizando el retorno de la inversión. Los ataques a menos de 1 Gbps son más baratos y más quirúrgicos, mientras que los ataques a más de 10 Gbps son más dramáticos y perturbadores. ¿El rango de 1-5Gbps? Cada vez se deja más atrás.

Esto podría ser una señal de cómo la eficiencia de los atacantes da forma a todo el panorama de amenazas.



Los Ataques Evolucionan: Campañas de DDoS Más Inteligentes y Adaptativas

LO QUE DICEN LOS DATOS

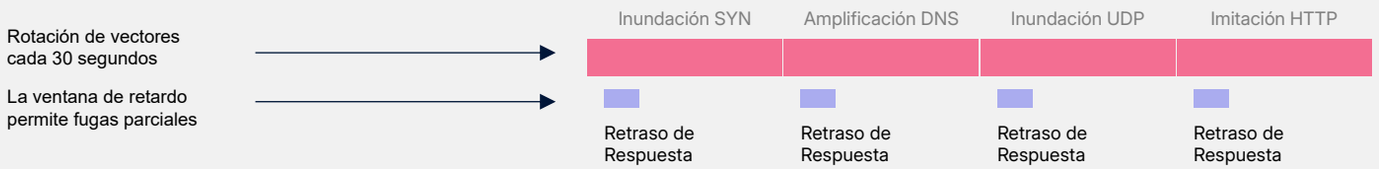
Observamos un patrón creciente de campañas DDoS multivectoriales, secuenciales y evasivas a lo largo de 2024. Aunque el volumen por sí solo ya no es el factor definitorio, el comportamiento de los atacantes es cada vez más sofisticado. En muchos casos, los atacantes lanzaron ataques coordinados dirigidos a diferentes subredes de forma simultánea o en rápida sucesión, a menudo combinando múltiples vectores en ráfagas cortas. Estas campañas no sólo son más difíciles de detectar, sino que también pretenden aprovechar las lagunas de retraso en los sistemas de detección y mitigación.

Este comportamiento incluye:

- Cambio rápido de vectores (por ejemplo, alternando entre inundaciones SYN, amplificación DNS e imitaciones HTTP).
- Probar las defensas sondeando los puntos débiles y modificando las tácticas.
- Lanzamiento de ataques de gran volumen con microrráfagas para eludir los umbrales estáticos.

En varias de las campañas observadas, los atacantes emplearon lo que aquí describimos como "vectores encadenados": ataques de secuencia estricta que cambian rápidamente entre protocolos cada 30-60 segundos. Aunque cada vector por sí solo puede ser manejable, la sincronización y coordinación están diseñadas para explotar incluso breves retrasos en la detección o mitigación, manteniendo las defensas reactivas en lugar de receptivas.

Cronometraje de vectores encadenados y lagunas de respuesta



QUE SIGNIFICA

Esta evolución indica que los ciberdelincuentes ya no se limitan a perturbar el sistema, sino que intentan superar a la automatización. El cambio de la fuerza bruta a la adaptabilidad estratégica desafía incluso a los marcos de mitigación más sensibles.

Las defensas tradicionales suelen estar diseñadas para detectar el volumen, no la velocidad. Cada vez que un atacante cambia de táctica, por ejemplo, pasando de abrir conexiones TCP falsas a activar la amplificación DNS o lanzar inundaciones UDP, la defensa tiene que hacer una pausa, reevaluar y reclasificar. Ese ciclo, por breve que sea, crea repetidos puntos ciegos.

Hemos observado campañas en la naturaleza que rotan los vectores justo cuando se activa la mitigación, creando un efecto de giro que deja a los equipos SOC persiguiendo la cola del ataque. Esto no es ruido. Es diseño. La capacidad de detectar no sólo los paquetes, sino también la intención, se está convirtiendo en algo esencial.

Los Ataques Evolucionan

LO QUE PUEDE HACER

Busque patrones a corto plazo: Utilice la telemetría para identificar cambios rápidos en el tipo de protocolo, la orientación de los puertos o el tamaño de los paquetes. Estos cambios, especialmente si se producen cada 30-60 segundos, pueden indicar un comportamiento vectorial encadenado.

Marque y señale las anomalías en tiempo real: Desarrolle reglas o secuencias de comandos ligeras que etiqueten nuevos perfiles de tráfico a medida que surgen. Esto ayuda a crear bucles de retroalimentación rápidos para su SOC, incluso antes de que se completen los ciclos de detección.

Cree guías SOC en función del comportamiento de los agresores: Utilice patrones de encadenamiento conocidos para informar sus flujos de trabajo de escalada. Establezca expectativas internas sobre cómo es la cadencia de respuesta "normal" y qué podría indicar algo más coordinado.

Por qué funciona la conmutación vectorial

En los entornos de mitigación actuales, el tiempo lo es todo. La mayoría de las defensas DDoS se basan en firmas de detección, umbrales de velocidad y reconocimiento de patrones que tardan en activarse. Incluso las plataformas avanzadas pueden tardar entre 10 y 30 segundos, o más, en analizar el tráfico y comenzar la mitigación.

Los atacantes se aprovechan de ello. Cambiando de vector cada 30-60 segundos, ellos:

- Evadir el filtrado persistente
- Confundir las herramientas de análisis adaptadas a tipos de ataque específicos
- Forzar a las defensas a reiniciar los ciclos de mitigación

El resultado: fugas, agotamiento de recursos y SOC fatiga.

No se trata de abrumar a las defensas, se trata de ir un paso por delante.

Ataques en la Capa de Aplicación: Aumenta el DDoS

LO QUE DICEN LOS DATOS

Nuestras observaciones indican sistemáticamente un aumento de los ataques a la capa de aplicación (capa 7). Estos ataques suelen ser:

- Menor ancho de banda
- Más difícil de detectar debido al cifrado
- Dirigido a API, portales de acceso, carros de la compra, funciones de búsqueda y otros puntos finales que consumen muchos recursos.

Hemos observado indicios, tanto internamente como en todo el sector, de que las interrupciones de las aplicaciones se deben cada vez más a ataques de menor volumen no visibles en los datos volumétricos tradicionales. Los atacantes también están utilizando sondas L3/L4 como reconocimiento para ataques de seguimiento L7, lo que difumina aún más la línea entre las superficies de amenaza de la red y de las aplicaciones.

Comparación entre ataques DDoS L3/L4 y L7				
	Objetivo	Tipo de Ataque	Desafío de Detección	Enfoque del Impacto
L3/L4 DDoS	Infraestructura de Red	Inundaciones Volumétricas	Velocidad y volumen de paquetes	Saturación de Ancho de Banda
L7 DDoS	Aplicaciones y APIs	Imitan Usuarios Legítimos	Comportamiento/Basado en Patrones	Degradación del Servicio

QUE SIGNIFICA

El DDoS en la capa de aplicación no consiste en inundar la tubería, sino en romper la aplicación.

Estos ataques suelen:

Imitar el tráfico legítimo de los usuarios (por ejemplo, Solicitudes HTTPS GET/POST)

Explotar el agotamiento de recurso (CPU/memoria/dinero) en lugar del ancho de banda.

Operar bajo el radar de las herramientas tradicionales de detección volumétrica

El paso a L7 refleja una evolución más amplia: El DDoS ya no se centra sólo en la infraestructura. Se centra en el negocio. Los atacantes de aplicaciones pretenden acabar quirúrgicamente con lo más importante: la experiencia del cliente, el flujo de transacciones o la autenticación.

Esta tendencia también subraya el aumento de los adversarios conscientes de la plataforma, que saben cómo explotar las víctimas específicas. arquitecturas, cargas de trabajo en la nube o lógica de aplicaciones web.

Ataques en la Capa de Aplicación

LO QUE PUEDE HACER

Comience a supervisar la salud de la capa de aplicación junto con el tráfico de red. Tiempos de carga inusuales, errores 5xx o fallos en el inicio de sesión podrían ser señales de DDoS.

Integre las capacidades de defensa de L7 en su pila más amplia de mitigación de DDoS, incluso si aún se encuentran en fases iniciales.

Colabore con los equipos de desarrollo de aplicaciones y plataformas, no sólo con los de operaciones de red, para desarrollar estrategias de respuesta coordinadas.

Considere el modelado del comportamiento del usuario y las estrategias de limitación de velocidad para detectar el abuso de firmas de alta velocidad y bajo volumen.

Cuando el tráfico "normal" se convierte en un ataque

Los ataques DDoS en la capa de aplicación son difíciles de detectar porque a menudo imitan a usuarios reales. Una inundación de inicios de sesión puede parecer un lunes ajetreado. Un ataque a un carrito de la compra puede parecerse al tráfico del Viernes Negro.

La diferencia está en la intención y el patrón. Los ataques L7 son típicamente:

- Muy repetitivo
- Repartidas en IP rotativas
- Diseñado para malgastar los recursos de la aplicación en lugar de los de la red

Defenderse contra esto requiere un análisis del comportamiento y conocimiento de las aplicaciones, no sólo filtrado de paquetes.

Los Defensas aún no se han Puesto al Día

LO QUE DICEN LOS DATOS

Los defensores se enfrentan a retos cada vez mayores para ponerse al día, ya que los patrones de ataque DDoS se han vuelto más automatizados, adaptables y evasivos. Según una investigación encargada por Corero y realizada por Merrill Research, una parte significativa de las organizaciones informan:an:

- Dificultad de coordinación entre los equipos de seguridad, redes y plataformas.
- Incapacidad para mantener una visibilidad clara de todas las rutas de tráfico (especialmente en entornos híbridos y multicloud).
- Retrasos en los flujos de trabajo de detección a mitigación
- Escasez de personal cualificado para gestionar y ajustar las defensas de seguridad

Esto refleja lo que vemos sobre el terreno: los defensores no fracasan por culpa de las herramientas, sino por culpa de la diversidad, la complejidad y el ritmo del cambio.

QUE SIGNIFICA

La postura defensiva está cada vez más distribuida. La adopción de la nube ha superado a la visibilidad. La línea entre los equipos de aplicaciones, infraestructura y seguridad se ha difuminado. Y los manuales tradicionales presuponen un nivel de control que la mayoría de las organizaciones ya no tienen.

Incluso los mejores sistemas de mitigación son sólo tan buenos como:

Las señales que reciben

La automatización que pueden ejecutar

La claridad de la propiedad que los respalda

No se trata sólo de una brecha tecnológica. Es una brecha operativa.

Los Defensas aún no se han Puesto al Día

LO QUE PUEDE HACER

- Lleve a cabo una auditoría de preparación para DDoS: personas, procesos y herramientas.
- Aclare la propiedad de la respuesta: quién hace el triaje, quién actúa y quién ajusta las defensas.
- Cree guías que reflejen su infraestructura real, incluidas las capas híbridas, de CDN y de nube.
- Invierta en automatización, no asuma que es plug-and-play: necesita visibilidad y puesta a punto.
- Convierta los ejercicios DDoS en una actividad periódica para los equipos de seguridad y operaciones.

La respuesta DDoS es un deporte de equipo

La respuesta DDoS ya no se limita a un solo equipo. Afecta a operaciones de red, equipos de aplicaciones, arquitectos de la nube y analistas de SOC. Sin embargo, muchas organizaciones siguen tratándola como una disciplina aislada.

Para ser eficaz, la mitigación debe ser:

- Funciones transversales
- Preautorizado
- Ejercicio continuo

La mejor defensa no siempre es la herramienta más sofisticada, sino las personas que saben cuándo y cómo usarla.

No es la Plataforma. Es la Presión.

Hasta ahora nos hemos centrado en el comportamiento de los atacantes y en las tendencias técnicas. Pero en el centro de cada una de estas perspectivas hay un equipo humano encargado de defenderse de ellos.

Por eso encargamos a Merrill Research que profundizara en el tema. Queríamos entender no solo las amenazas, sino también cómo las viven los profesionales: los profesionales de la seguridad y las redes que viven la respuesta, el estrés y la realidad de la defensa bajo presión.

Estos resultados reflejan las aportaciones de los clientes de Corero como de los que no lo son. El objetivo era sencillo: comprender qué funciona, qué no y qué necesitan realmente los defensores.

La defensa DDoS no es una cuestión de si la tecnología funciona. Es una cuestión de si los equipos pueden trabajar con ella, en todos los ámbitos. funciones, en tiempo real y bajo presión.

Merrill Research ha puesto de manifiesto un patrón consistente: los retos a los que se enfrentan los defensores no tienen que ver con la capacidad sino con coordinación. Incluso con herramientas sólidas, muchos equipos siguen luchando por alinear plataformas, funciones y flujos de trabajo.

Temas clave que surgieron:

Dificultad para demostrar el valor del DDoS protección de las partes interesadas de la empresa

Coordinación limitada entre los equipos de nube, red y aplicaciones

Lagunas en la puesta a punto, guías operativas y estrategias de respuesta integradas

Incertidumbre en torno a la propiedad y la comunicación durante las amenazas activas

El "y qué" es el siguiente: la resiliencia no viene de las herramientas solo. Proviene de la alineación.

Cuando los equipos pueden ver con claridad, actuar con decisión y se comunican con confianza, no sólo reaccionan más rápido, sino que se recuperan con más fuerza.

Los proveedores tienen la responsabilidad de reducir la carga operativa que imponen a sus clientes, con productos que se integren fácilmente en las arquitecturas, los flujos de trabajo y los ecosistemas de herramientas existentes, y en los que ellos mismos puedan integrarse. La buena tecnología debe adaptarse a la forma de trabajar de los equipos, y no al revés.

Lo que nos contaron los defensores

68%

dicen que demostrar el ROI de la protección DDoS es un reto.

51%

citan la falta de coordinación entre equipos como clave vulnerable.

47%

dificultades para adaptar las herramientas existentes a los entornos.

Y más de la mitad afirma que no confía en su capacidad para mitigar los ataques avanzados sin la orientación de un proveedor.

Conclusión: Ver la Señal en el Ruido

El panorama de las amenazas DDoS en 2024 no estaba marcado por el caos. Estaba marcado por la claridad, para aquellos que sabían dónde buscar.

Los ataques cortos y subsaturadores siguieron dominando el panorama, más frecuentes que nunca y tácticamente eficaces. En el otro extremo del espectro, los ataques a gran escala cobraron un nuevo impulso, ayudados por modernas redes de bots y kits de herramientas básicos. Y entre medias, un notable descenso de los ataques de tamaño medio nos indicó algo más: los atacantes se están optimizando.

Eligen sus momentos. Sus métodos. Sus objetivos.

Pero las tendencias técnicas sólo cuentan una parte de la historia. A medida que los datos evolucionaban, también lo hacía la experiencia de defenderse contra ellos. Merrill Research puso de manifiesto lo que muchos ya sienten: el reto no siempre tiene que ver con la capacidad. Se trata de alineación. Visibilidad. Confianza. Y estar preparado cuando el ataque es real, pero aún no evidente.

La defensa contra las campañas DDoS modernas requiere algo más que una mitigación más rápida o filtros más inteligentes. Requiere la integración de herramientas, personas y estrategias. La postura más sólida no se construye a partir de una única plataforma. Se construye a partir de la coordinación, la claridad y el apoyo que se adapta a la velocidad de la amenaza.

DDoS es fácil. La defensa aún no lo es. Pero cuando los defensores están alineados, informados y capacitados, es cuando la ventaja empieza a cambiar.

La señal está ahí. **Y también la solución.**

corero
[NETWORK SECURITY]

ACERCA DE CORERO NETWORK SECURITY

Corero Network Security es un proveedor líder de soluciones de protección contra ataques DDoS, especializado en detección y protección automáticas, con herramientas de visibilidad de red, análisis y generación de informes. La tecnología de Corero protege contra amenazas DDoS externas e internas en entornos complejos de borde y de abonado, garantizando la disponibilidad del servicio de Internet. Con centros operativos en Marlborough, Massachusetts (EE. UU.) y Edimburgo (Reino Unido), Corero tiene su sede central en Londres y cotiza en el mercado AIM de la Bolsa de Londres (ticker: CNS) y en el mercado OTCQX de EE. UU. (OTCQX: DDOSF).

Para más información, visite www.corero.com, y síganos en LinkedIn y Twitter.