SONICWALL®

2024

INFORME DE CIBERAMENAZAS DE SONICWALL

CÓMO HACER FRENTE AL INCESANTE AUMENTO DEL CIBERCRIMEN

sonicwall.com | @sonicwall

INTRODUCCIÓN

MENSAJE DE NUESTRO CEO

Hace casi 18 meses, en SonicWall comenzamos a implementar nuestro enfoque desde fuera hacia dentro en todo lo que hacemos. Para ello, nos centramos en conocer a la perfección las necesidades y los problemas de nuestros partners y clientes y en utilizar ese conocimiento para impulsar la entrega de nuestros productos y servicios.

2023 fue un año importante, en el que se empezaron a apreciar los resultados de ese enfoque. Compramos la empresa Solutions Granted, un Proveedor de servicios de seguridad gestionados (MSSP) que sirve a más de mil Proveedores de servicios gestionados (MSPs) en toda Norteamérica. También reforzamos nuestra plataforma de seguridad en la nube para el personal moderno y remoto con la adquisición de Banyan Security, que incorporó soluciones SSE, incluido el Acceso a la red Zero Trust (ZTNA), al creciente portfolio de SonicWall.

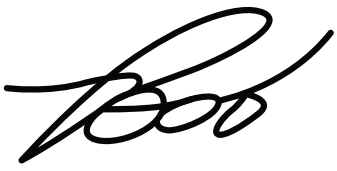
Estas acciones estratégicas permiten a nuestros partners MSP ofrecer a sus clientes una protección 24x7x365 con un equipo de analistas de amenazas y expertos, sin los gastos que implicaría la creación de su propio SOC interno. Asimismo, ampliamos el portfolio de productos y servicios de SonicWall a la nube y proporcionamos a los partners y a sus clientes una mayor flexibilidad, esencial para el desarrollo continuo de la plataforma de ciberseguridad de SonicWall.

A medida que se amplía la plataforma de SonicWall, ofreceremos a nuestros clientes una cantidad cada vez mayor de soluciones de seguridad gestionadas, desde firewalls hasta seguridad en la nube. Sin embargo, tal y como muestra el Informe de Ciberamenazas 2024 de SonicWall, los cibercriminales se muestran implacables: inventan nuevas tácticas y extienden sus tentáculos hasta cada esquina de la creciente superficie de ataque actual.

Dados los aumentos en las intrusiones maliciosas (6 %), el malware (11 %) y el cryptojacking (659 %), la probabilidad de que cualquier organización sea el blanco de un ataque se está disparando.

En este entorno volátil, las defensas de ayer ya no son suficientes: las empresas, independientemente de su tamaño, necesitan soluciones de eficacia probada y estrategias proactivas basadas en la inteligencia de amenazas más actualizada.

Es por ello que SonicWall sigue publicando su Informe de Ciberamenazas: para proporcionar inteligencia de amenazas, no solo con el fin de ofrecer información valiosa accionable, sino también de impulsar nuestra hoja de ruta y crear soluciones que ayuden a nuestros partners. En nombre de nuestra red de partners de confianza y de todo el equipo de SonicWall, incluidos los investigadores de amenazas de Capture Labs, nos complace compartir esta visión exclusiva del cambiante panorama de la ciberseguridad.



Bob VanKirk
Presidente y CEO
SonicWall

Las pequeñas filtraciones pueden causar daños importantes

Los ciberataques acaparan las noticias. Los ataques contra grandes empresas conocidas u oficinas gubernamentales locales ocupan los titulares casi constantemente. Aquellos que siguen la ciberseguridad un poco más de cerca, verán que ocurre algo similar. La cobertura de las principales filtraciones por parte de los medios de comunicación especializados en ciberseguridad está dominada por nombres conocidos, como Mailchimp, MGM, Activision y 23andMe.

A la vista de estas noticias, no sería descabellado suponer que el cibercrimen es un problema mucho mayor para las empresas grandes que para las pequeñas. Sin embargo, nada más lejos de la realidad. En un blog de 2023, CISA afirmó que **las empresas pequeñas tienen una probabilidad tres veces mayor de sufrir un ataque** que las organizaciones más grandes. Además, los ataques perpetrados contra pymes representan miles de millones de dólares en pérdidas cada año.

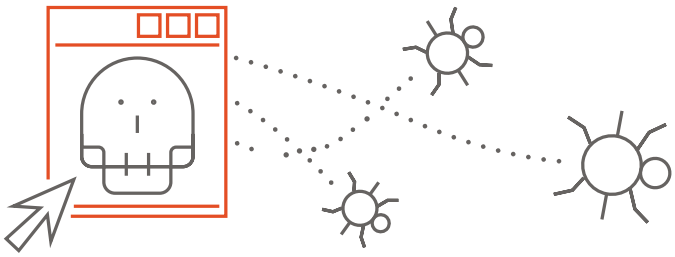
Esta es una de las principales razones por las que en SonicWall estamos tan comprometidos con la investigación y la publicación de la más reciente inteligencia de amenazas. Dado que el 80 % de nuestros usuarios finales son pymes, nuestros datos presentan una visión del panorama de las amenazas diferente a las que encontrará en cualquier otro lugar — menos centrada en los grupos multinacionales, y más en negocios como el suyo.

Principales tendencias de 2023

La aceleración fue posiblemente la mayor tendencia que observamos en 2023. Los investigadores de amenazas de SonicWall Capture Labs notaron un aumento en los volúmenes de ataques prácticamente de todos los tipos y en todas partes. **El malware registró un aumento interanual del 11 %. Las amenazas cifradas crecieron un 117 % y el cryptojacking, un 659 %**. Esta tendencia también se apreció a nivel regional, donde los aumentos del volumen de ataques casi triplicaron la cantidad de descensos.

Tras las constantes idas y venidas causadas por fuerzas externas que hemos observado durante los últimos años, en 2023 los cibercriminales recurrieron a métodos de eficacia probada. Si bien cabría esperar que el aumento de los volúmenes de ataques de malware y los niveles persistentemente altos de phishing vinieran acompañados de altas tasas de malware nuevo, descubrimos justo lo contrario: las detecciones de malware nunca antes visto registraron un descenso interanual del 38 %.

No obstante, esto no significa que los cibercriminales no hayan estado perfeccionando sus técnicas. Los investigadores de SonicWall observaron la aparición de los archivos Microsoft OneNote como vector de amenazas inicial, así como campañas masivas contra vulnerabilidades en WinRAR y MOVEit.



Nuestros datos siguieron reflejando que las vulnerabilidades representan el vector de ransomware más común — y es probable que este siga siendo el caso, ya que las vulnerabilidades siguen aumentando. **En 2023, se publicaron 28.834 CVEs**, una cifra récord que representa un aumento del 15 % con respecto a las cifras de 2022. En diciembre, los investigadores de amenazas de SonicWall **descubrieron y publicaron debidamente la CVE-2023-51467**, una vulnerabilidad que afectaba a ApacheOFBiz. Desde entonces, se ha observado una gran cantidad de intentos de explotación.

Otras campañas mostraron un nivel similar de innovación: se observaron nuevas campañas de phishing que llevan a sus víctimas a páginas muy convincentes de inicio de sesión de Microsoft Outlook y American Express, así como campañas de phishing que utilizan códigos QR para eludir la tecnología de escaneo de archivos. Los cibercriminales aprovecharon la inflación y la incertidumbre económica para lanzar aplicaciones de préstamos fraudulentas llenas de spyware y funciones de robo de credenciales. Además, se utilizaron scripts de Google embebidos en PDFs como armas para cometer robos de criptomonedas, haciendo patente la necesidad de reforzar la vigilancia incluso en entornos aparentemente fiables.

Desde pymes hasta empresas grandes — presente y futuro

Ya podemos vislumbrar un futuro panorama de las amenazas muy diferente al actual, mientras los cibercriminales continúan adoptando ChatGPT y otra tecnología de IA generativa para perfeccionar los intentos de phishing, lanzar ataques de Compromiso del correo electrónico de negocio (BEC) muy convincentes y escribir código malicioso rápidamente.

Sin embargo, la IA también supone una gran promesa para los defensores de las redes. SonicWall adoptó la IA y el AA en una fase temprana, y Capture ATP y RTDMI ya son capaces de detectar muchos de estos tipos de ataques. Sin embargo, será en los próximos años cuando empezaremos a ver el verdadero potencial de la IA como herramienta de defensa.

Mayor cifra desde 2019

En 2023, los investigadores de amenazas de SonicWall Capture Labs registraron 6.060 millones de ataques de malware, cifra que representa un aumento interanual del 11 %. Este es el mayor volumen anual de ataques a nivel global desde 2019, lo cual indica que los niveles de malware han regresado a los valores previos a la pandemia, mientras los cibercriminales siguen aumentando en número, en recursos y en actividad.

No obstante, el aumento global del malware fue el resultado de la combinación de dos tendencias opuestas. En Asia y Europa, el malware *cayó* un 2 %, descenso que, sin embargo, se vio fácilmente compensado por mayores aumentos en Norteamérica (+15 %) y LATAM (+30 %).

Esta divergencia también se aprecia en nuestros datos de sectores específicos. El sector de la Educación, en el que en 2022 se registró el mayor volumen de malware con diferencia, experimentó un descenso del 3 % en 2023. El malware dirigido a los sectores sanitario y minorista, por otra parte, aumentó un 20 %, y los ataques contra agencias gubernamentales se dispararon un 38 %. Sin embargo, las empresas más afectadas fueron las financieras, que vieron cómo se *doblaba* la cantidad de ataques de malware contra ellas. Este aumento fue suficiente para convertir al sector financiero en el más afectado de los que analizamos en 2023 tras haber ocupado el último puesto de la lista en 2021 y una posición central en 2022.

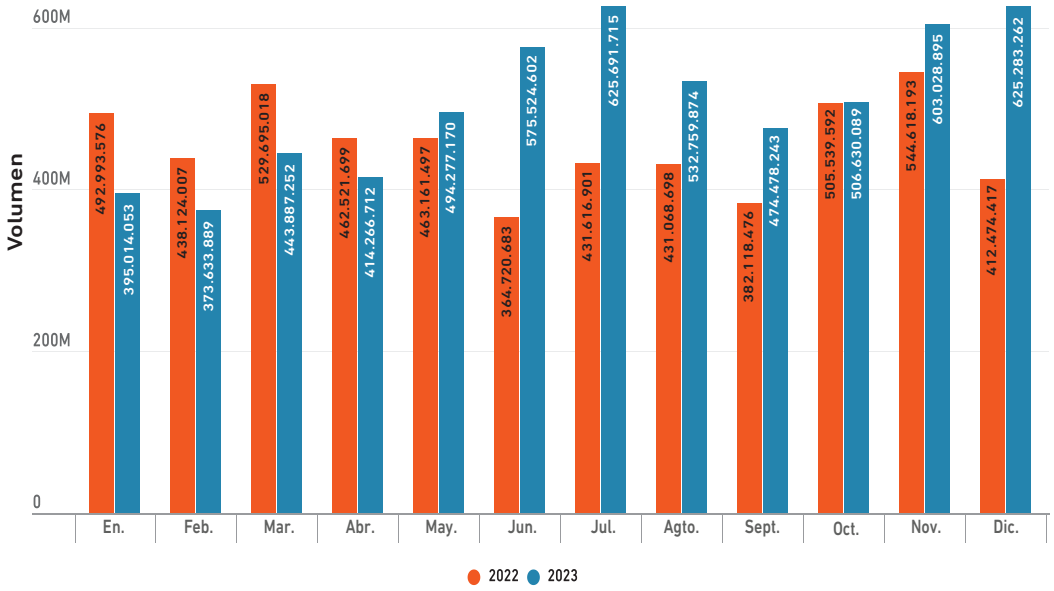
Archivos de OneNote maliciosos

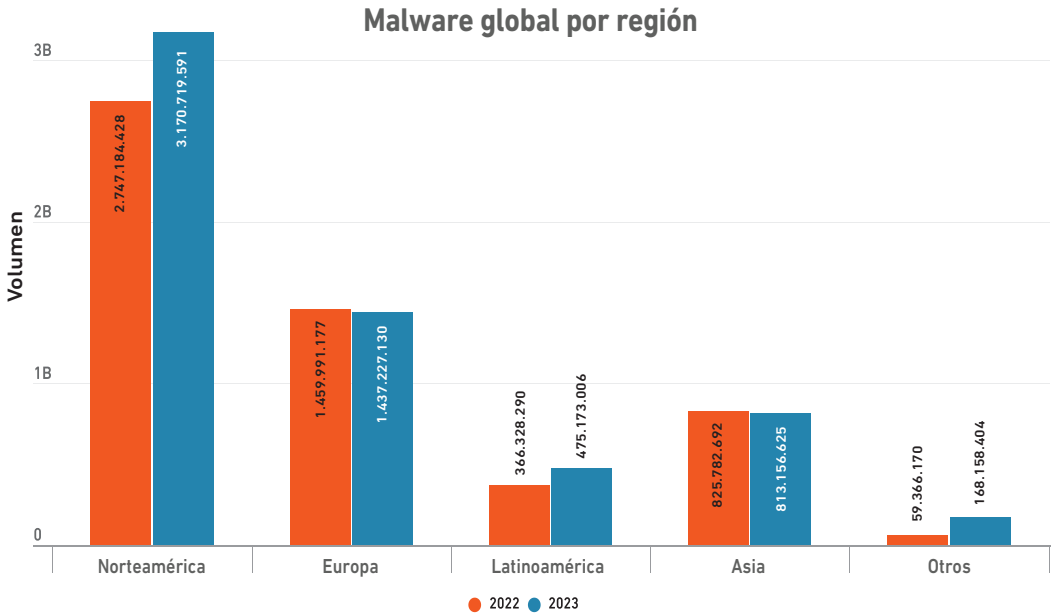
A principios de 2023, los investigadores de SonicWall observaron que los cibercriminales estaban utilizando un nuevo vector inicial para infectar los sistemas: el uso de archivos de Microsoft OneNote. Enviaban estos archivos convertidos en armas por correo electrónico, acompañados de una variedad de técnicas de ingeniería social diseñadas para maximizar la probabilidad de que los archivos adjuntos se abrieran y la víctima hiciera clic en los archivos maliciosos ocultos que incluían, provocando la ejecución de la carga útil.

Sin embargo, cuando rápidamente los proveedores de seguridad se dieron cuenta, empezaron a detectar esos archivos adjuntos con carga útil. Entonces, los cibercriminales pasaron a utilizar una URL que, al hacer clic, llevaba a la víctima a la carga útil. Al mismo tiempo, los perpetradores de ataques empezaron a añadir a su código caracteres nulos repetidos al final de los archivos de OneNote para hacer que el tamaño del archivo superara los 500 MB, con la esperanza de eludir así numerosas soluciones de escaneo antivirus.

En mayo, no obstante, el uso de estos archivos ya había empezado a caer drásticamente, probablemente debido al lanzamiento por parte de Microsoft de una actualización de Office que bloqueaba los archivos embebidos con extensiones peligrosas para impedir que se abrieran en OneNote. Sin embargo, a pesar de la corta duración de esta campaña, se extendió lo suficientemente como para convertir a los archivos de OneNote en el tipo de archivos de Office maliciosos más popular de todo el 2023, siendo utilizados por Qakbot, AsyncRat, AgentTesla, etc. como punto de entrada inicial.

Volumen global de malware





Predominio de los PDFs maliciosos

Hace mucho tiempo que el uso de PDFs maliciosos es una táctica popular entre los cibercriminales. No obstante, su uso aumentó drásticamente en 2023. Pasaron de representar aproximadamente un quinto de todas las detecciones de tipos de archivos maliciosos a casi un tercio, lo cual es un claro indicador de que esta táctica sigue resultando eficaz.

A medida que estos ataques aumentaban, también lo hacía la innovación, lo cual se tradujo en la creación de numerosas variantes importantes. En 2023, SonicWall observó varios casos de PDFs que contenían códigos QR. Uno de ellos amenazaba al usuario con el vencimiento de una contraseña de Microsoft si no escaneaba el código.

Otro PDF incluía una URL maliciosa creada mediante Google Script, con la intención de evadir la detección. Se trataba de una estafa compleja y muy completa. Incluía un registro de transacciones en Bitcoin y una falsa barra de "progreso de minado" con el fin de incitar a las víctimas a introducir información financiera para recibir fondos ficticios.

Como hemos visto en años anteriores, en 2023 los cibercriminales llegaron a extremos para replicar marcas conocidas y fiables, y cada vez se les da mejor. Algunos ejemplos incluyen PDFs maliciosos que aparentan ser comprobantes de iTunes, avisos de múltiples intentos de inicio de sesión en una cuenta de Wells Fargo e incluso la página de inicio de sesión de la plataforma de colaboración RingCentral.

Tácticas más utilizadas por los cibercriminales

Los archivos Portable Executable (PE) son los reyes indiscutibles

Los archivos PE siguen siendo la carga útil final más utilizada debido a la facilidad de entrega, al uso de herramientas extendidas y a la facilidad de ejecución. Sin embargo, en 2023, observamos un aumento del malware basado en archivos PE escrito en .NET. Vimos que actualmente la mayoría del malware basado en archivos PE, incluidas familias de malware conocidas, como RedLine, AgentTesla y AsyncRAT, se está escribiendo en .NET, probablemente a causa de su accesibilidad y de su amplia funcionalidad.

Afortunadamente, los archivos PE hacen saltar las alarmas y se examinan exhaustivamente para descartar intenciones maliciosas. Además, mientras algunos autores de malware utilizan archivos de script como vectores iniciales para otros tipos de malware, o escriben código malicioso completo utilizando JavaScript, VBScript, PowerShell u otros, los clientes de SonicWall están protegidos: la excepcional capacidad de emulación de scripts de RTDMI proporciona excelentes funciones de detección de scripts maliciosos.

WinRAR ofrece a los perpetradores de ataques una forma fácil de lucrarse

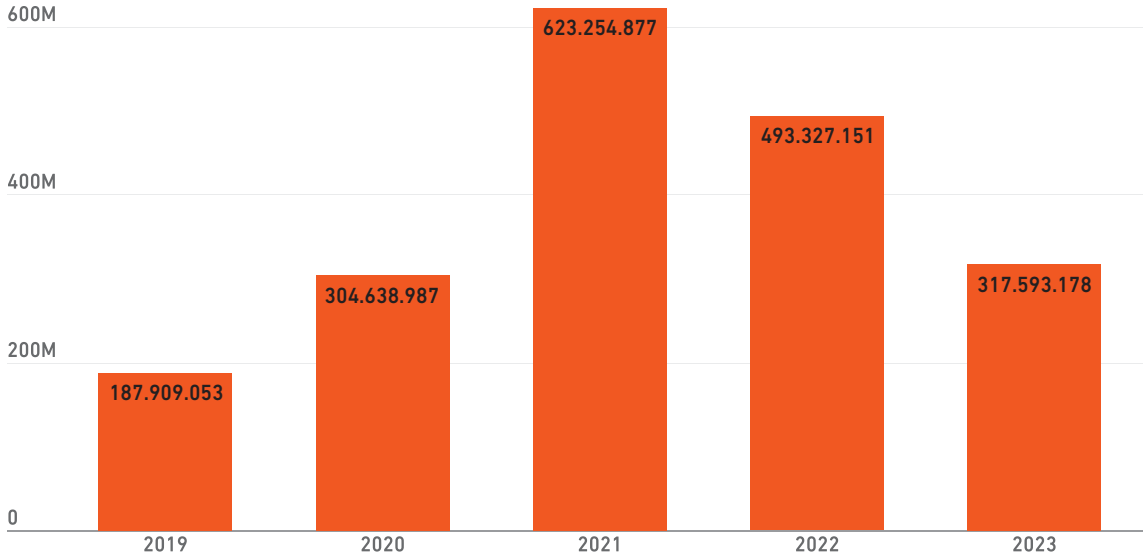
A principios de 2023, los cibercriminales empezaron a explotar una nueva vulnerabilidad en WinRAR, la popular herramienta de gestión y extracción de archivos de Windows. En la segunda mitad del año, múltiples familias de malware dedicadas al robo de información — incluidas AgentTesla, Remcos, Rhadamanthys y Guloader — se vieron implicadas en diversas campañas de explotación de la CVE-2023-38831, que permite a los perpetradores de ataques ejecutar código arbitrario en los archivos zip. Debido al uso generalizado de WinRAR en las empresas grandes, estas campañas proliferaron rápidamente en EE. UU., Oriente Medio y Asia. Ahora, se han vinculado a hackers con patrocinio estatal de Rusia y China, incluidos Sandworm, APT28 y APT 30, entre otros.

Sigue siendo una fuerza a tener en cuenta

En 2023, el panorama de los ataques de ransomware siguió evolucionando. Los investigadores de amenazas de SonicWall Capture Labs registraron 317,6 millones de ataques de ransomware, cifra que supone un descenso interanual del 36 % — pero el tercer total más alto hasta la fecha. Esta tendencia se reflejó en varias regiones: en Norteamérica y Europa el ransomware cayó un tercio, y en LATAM, los ataques disminuyeron un 52 %.

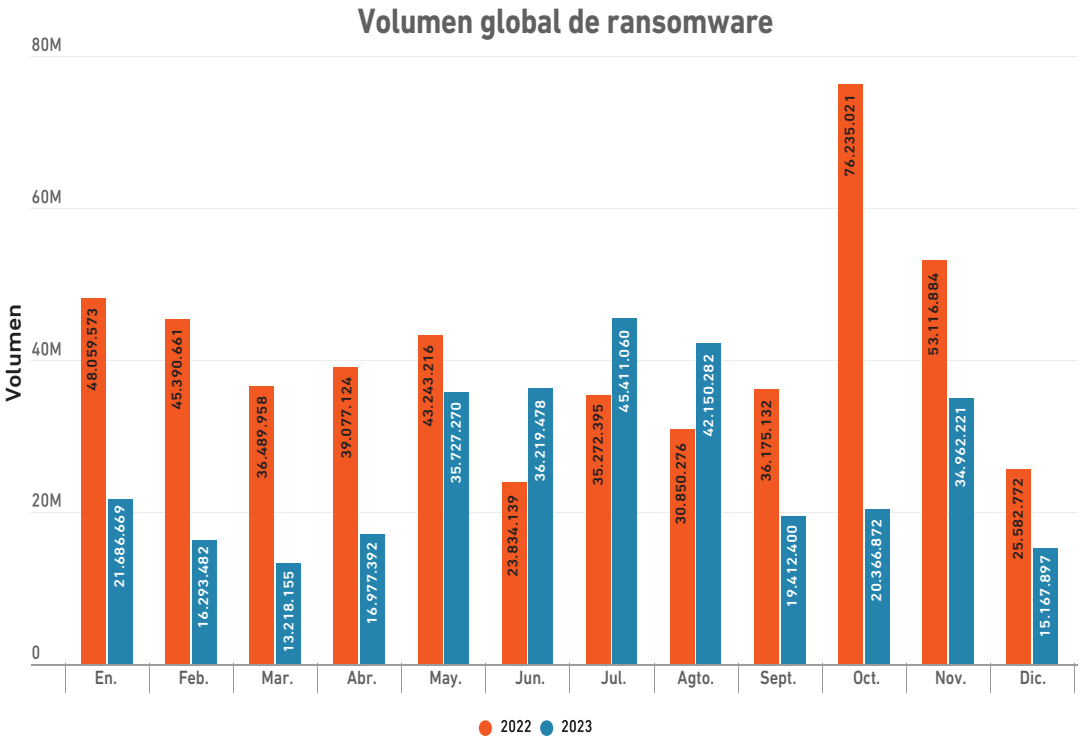
Asia fue la gran excepción. En 2023, los volúmenes de ransomware alcanzaron la cifra récord de 17,5 millones — un aumento del 1.627 % desde 2019. Los ataques contra el sector financiero encabezaron este incremento. En mayo, el grupo de ransomware LockBit robó 15 millones de registros de clientes y 1,5 terabytes de datos internos de Bank Syariah Indonesia. En noviembre, el Industrial and Commercial Bank of China (ICBC), el banco con mayores activos del mundo, también sufrió un ataque de Lockbit. Además, según el informe de IDC publicado en septiembre de 2023, aproximadamente tres cuartos de las empresas de India sufrieron ataques de ransomware en 2022 — cifra que probablemente haya seguido aumentando desde entonces.

Volumen global de ransomware por año



Principales ataques de ransomware en 2023: LockBit

La detención de dos afiliados apenas varió las cifras de LockBit: siguió siendo el grupo de ransomware líder en 2023. Es probable que esto se deba a las continuas innovaciones, como los programas de recompensas por la detección de errores para mejorar la calidad de los "productos," a los esfuerzos de marketing y al lanzamiento regular de versiones actualizadas de kits de herramientas con prestaciones mejoradas. Tras la filtración de LockBit 3.0/ "Black," SonicWall contactó con los cibercriminales, que exigieron un asombroso rescate (Puede ver los detalles aquí.)



Sigue siendo la principal amenaza: por qué es importante actualmente

Suponiendo que no vive en uno de los crecientes focos de ransomware, ¿en qué medida debería preocuparle este tipo de ataques?

En nuestra Encuesta de opinión en materia de amenazas 2023, preguntamos a los clientes qué tipos de ciberataques les preocupaban más. Una vez más, el ransomware ocupó el primer lugar con un 83 %, por delante del phishing, las amenazas cifradas, el malware sin archivos, los ataques de IoT, etc.

A pesar del descenso en el volumen de ataques de ransomware entre nuestros clientes de pymes, creemos que estos encuestados están bien encaminados.

Aquí podría ayudarnos algo de contexto histórico. Un descenso del 36 % suena a mucho, hasta que se tiene en cuenta el crecimiento del ransomware entre 2020 y 2022. Incluso después de esta caída, en el 2023 aún se registraron suficientes ataques de ransomware como para ser el año con la tercera mayor cifra. **Además, con un 27 % más de ransomware en la segunda mitad de 2023 que en la primera, el ransomware va en la dirección equivocada para compensar los enormes picos de 2021 y 2022**.

Cuando proveedores de ciberseguridad como SonicWall miden el ransomware y otras amenazas, solo pueden ver lo que ocurre en su ecosistema. En el mismo periodo en que SonicWall (con la amplia base de clientes de sus partners y MSP) observó un descenso del ransomware en 2023, otros proveedores registraron aumentos. Dado que la mayor actividad de las autoridades hace que cada ataque sea más peligroso, y que las pymes ya no son "presas fáciles" para los cibercriminales que utilizan ataques tipo "spray-and-pray," parece que se está produciendo un cambio de tendencia: ahora los cibercriminales se centran en perpetrar menos ataques, más específicos y con mayores ganancias potenciales.

Sin embargo, esto no significa que no haya presas fáciles. Cada vez es más común que las organizaciones trasladen sus datos y flujos de trabajo a la nube. No obstante, no se están asegurando de que estos datos gocen de la misma protección que los que tienen almacenados en ubicaciones locales. A medida que los cibercriminales siguen perfeccionando sus ataques de ransomware contra soluciones SaaS, no garantizar una seguridad suficiente en la nube podría tener consecuencias desastrosas.

También sigue habiendo gran cantidad de campañas de ransomware activas. Hacia finales de mayo, SonicWall observó la explotación de una vulnerabilidad de día cero de inyección SQL clasificada como crítica en MOVEit Transfer. La popularidad de esta herramienta de transferencia de archivos — y su extendida adopción por parte de las empresas — la convirtieron en un blanco de la banda de ransomware Cl0p. Utilizó la CVE-2023-34362 para perpetrar un ataque contra la cadena de suministro que afectó a alrededor de 2.000 organizaciones de los sectores financiero, asegurador, sanitario, educativo y gubernamental, y mediante el que robó datos de más de 62 millones de personas.

Es importante tener en cuenta que las vulnerabilidades como esta fueron el vector más común observado por SonicWall en los ataques de ransomware en 2023 — y esas campañas contribuyeron a que los pagos por ransomware superaran los 1.000 millones de dólares por primera vez en 2023.

INTRUSIONES

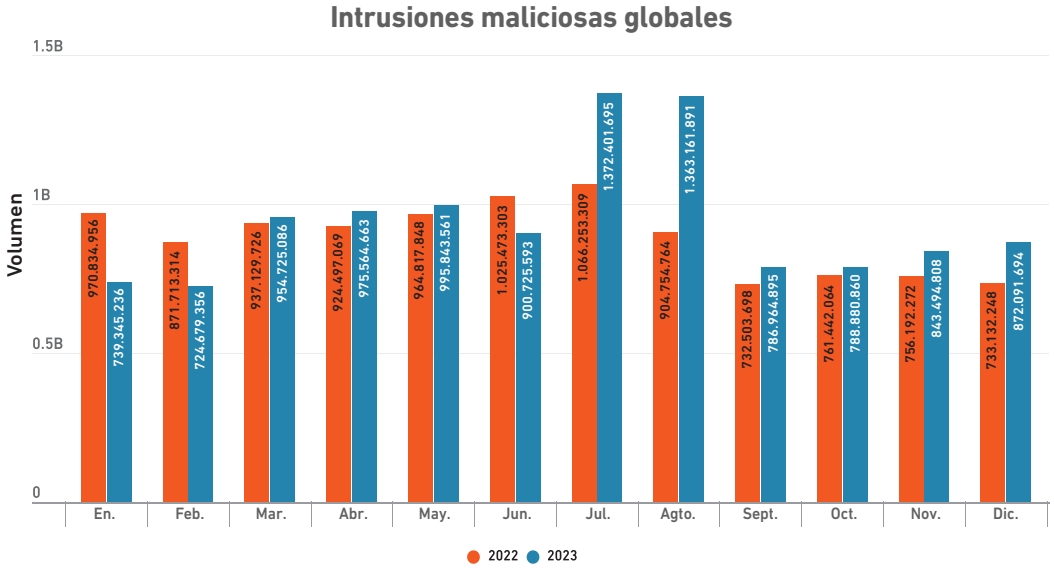
Los intentos aumentan un 20 %

Los intentos de intrusión totales siguieron aumentando en 2023 hasta alcanzar los 7,6 billones, un aumento del 20 % en comparación con el total de 2022. Desde que SonicWall empezó a informar de este parámetro en 2013, la cifra de intentos de intrusión ha aumentado todos los años — y durante la última década, la cantidad de intrusiones ha crecido un 613 %.

Si bien este aumento puede atribuirse en parte a ataques de poca gravedad relacionados con pings y otras acciones típicamente benignas, también se ha observado un repunte de los ataques de gravedad moderada a alta — también conocidos como "intrusiones maliciosas." Estos intentos de intrusión aumentaron hasta alcanzar la cifra de 11.300 millones en 2023, lo cual representa un aumento interanual del 6 %.

Los volúmenes de intrusiones maliciosas también crecieron en todos los sectores analizados. Los ataques de gravedad moderada y alta aumentaron un 19 % para los clientes del sector educativo, un 34 % para los minoristas, un 36 % para el sector sanitario, un 46 % para las agencias gubernamentales y un 47 % para el sector financiero.

Estos intentos disparan alertas que han de ser revisadas por analistas SOC, o por MSPs con analistas SOC, contribuyendo a la fatiga por las alertas y quitando tiempo valioso a otras iniciativas críticas. Además, cuando una intrusión se realiza con éxito, los cibercriminales pueden exfiltrar datos libremente, ejecutar código malicioso, cifrar sistemas, etc. — pudiendo interrumpir las operaciones y costar a las organizaciones miles o millones de dólares en costes de resolución y multas por incumplimiento normativo.



¿Qué es un intento de intrusión?

Un intento de intrusión maliciosa es un evento de seguridad en el que un cibercriminal trata de acceder sin autorización a un sistema o recurso explotando una vulnerabilidad. Aunque la explotación de vulnerabilidades de día cero no publicadas ocupa más titulares, las que más se explotan suelen ser vulnerabilidades conocidas y publicadas como CVE. Sin embargo, puesto que no todo el mundo aplica parches con la misma rapidez, los perpetradores de ataques tienen la oportunidad de utilizar el software o los dispositivos sin parchear como punto de entrada a una red.

Una vez que los cibercriminales están dentro de la red, la explotación de vulnerabilidades continúa, ya que tratan de permanecer en la red y desplazarse lateralmente utilizando otras vulnerabilidades en sistemas sin parchear dentro de la red.

SonicWall hace un seguimiento de la detección y la prevención de exploits procedentes de fuentes tanto externas como internas. Cuando una porción de código que constituye una vulnerabilidad pasa por un firewall con Prevención de intrusiones activada, y el firewall detecta y neutraliza ese código, se cuenta como un intento de intrusión.

AMENAZAS CIFRADAS

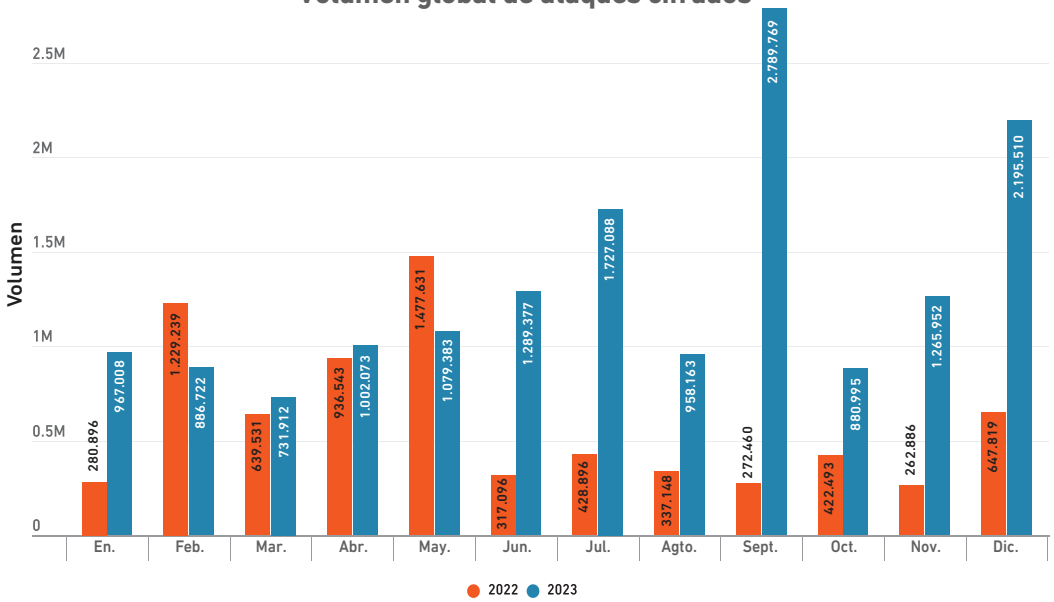
Los ataques cifrados ascienden a más del doble

En 2023, los investigadores de amenazas de SonicWall Capture Labs observaron 15,7 millones de ataques cifrados. Esta cifra es la más alta desde que empezamos a informar de este parámetro y supone un aumento internaual del 117 %.

Mientras que Norteamérica experimentó un aumento más modesto del 30 %, en Europa, Asia y LATAM se registraron ascensos de tres dígitos en los ataques cifrados: 182 %, 462 % y 527 % respectivamente.

En algunos de los sectores analizados se produjeron aumentos aún más bruscos — todos ellos experimentaron picos de tres dígitos. El sector financiero observó el menor aumento: los ataques contra estos clientes "solo" se doblaron. Sin embargo, en el sector sanitario (252 %), el educativo (429 %), el gubernamental (629 %) y el minorista (680 %) las amenazas cifradas se dispararon en 2023.

Volumen global de ataques cifrados



¿Qué son las amenazas cifradas?

La mayoría de las empresas analistas del sector concluyen que actualmente entre el 80 y el 90 por ciento del tráfico de red está cifrado, lo cual hace necesario escanear también el tráfico cifrado. Mientras que TLS (Seguridad de la capa de transporte) proporciona seguridad añadida para las sesiones Web y comunicaciones por Internet, los ciberatacantes cada vez utilizan más este protocolo de cifrado para ocultar ataques de malware, ransomware, de día cero, etc.

Los firewalls antiguos y otros controles de seguridad tradicionales carecen de la capacidad y la potencia de procesamiento necesarias para detectar, inspeccionar y mitigar las amenazas enviadas mediante tráfico HTTPS, convirtiéndolo en una vía de acceso que los perpetradores de ataques pueden utilizar con éxito para implementar y ejecutar sus ataques.

CRYPTOJACKING

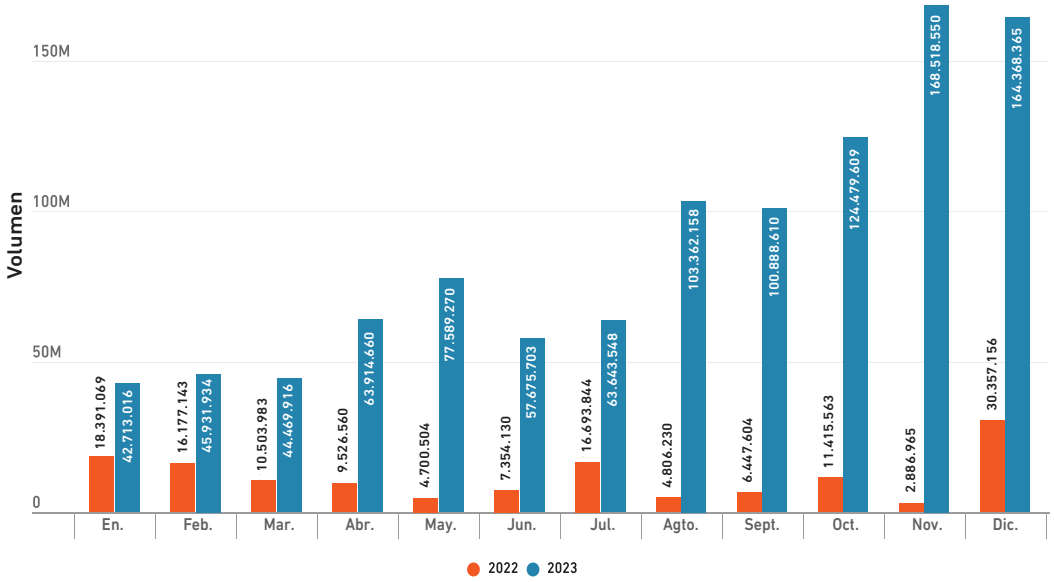
Por qué es peligroso (y por qué está creciendo)

En el informe de amenazas del año pasado, observamos un hito preocupante: la cantidad de ataques de cryptojacking, que se había mantenido bastante baja desde que empezamos nuestro seguimiento en 2018, superó por primera vez los 100.000.

Sin embargo, resultó que el ascenso del cryptojacking no era más que el inicio. A principios de abril de 2023, la cantidad de ataques de cryptojacking había sobrepasado el total anual de 2022, y continuó creciendo. Al final del año, los investigadores de amenazas de SonicWall Capture Labs habían registrado *1.060 millones* de ataques de cryptojacking—un aumento del 659 % con respecto a los totales de 2022. Este total se vio impulsado por volúmenes de ataques sin precedentes en noviembre y diciembre—ambos meses con más ataques de cryptojacking que los registrados en todo el año 2022.

También se observaron grandes aumentos en todas las regiones. En APAC y LATAM, los ataques de cryptojacking aumentaron un 87 % y un 116 % respectivamente. Sin embargo, se registraron ascensos verdaderamente enormes en NOAM (+596 %) y Europa (+1,046 %).

Volumen global de cryptojacking



¿Qué es el cryptojacking?

El cryptojacking es un tipo de ciberataque en el que los cibercriminales secuestran los recursos informáticos de su víctima para minar las criptomonedas sin su consentimiento ni conocimiento. Implica la instalación de malware, a menudo entregado mediante emails de phishing o páginas Web comprometidas, que se ejecuta de forma desapercibida en segundo plano en el ordenador, teléfono inteligente o servidor de una víctima. Este malware utiliza la potencia de procesamiento y la energía del dispositivo para resolver problemas matemáticos complejos ("prueba de trabajo"), generando criptomonedas para el perpetrador del ataque.

El curso actual del cryptojacking

En 2023, XMRig volvió a estar involucrado en la gran mayoría de ataques de cryptojacking. Este software de código abierto es una herramienta legítima fácilmente disponible en Internet que, debido a su facilidad de uso y configuración, a menudo se utiliza con fines maliciosos. Aunque es accesible incluso para cibercriminales novatos, también permite a los usuarios más avanzados modificar código con la intención de evadir la detección y de aumentar los beneficios.

XMRig a menudo se troyaniza, o se introduce de forma desapercibida en otros paquetes de software o adware. Se propaga mediante phishing, anuncios maliciosos, vulnerabilidades, descargas maliciosas, aplicaciones de software crackeadas, etc. Es eficiente y capaz de minar la criptomoneda Monero (también conocida como XMR, y a menudo la criptomoneda preferida por los cibercriminales debido a sus prestaciones de privacidad) a una velocidad relativamente alta sin consumir excesivos recursos de los sistemas. No obstante, sí consume mucha CPU, ya que lleva a cabo su actividad de minería en segundo plano — y lo hace *constantemente*.

Esto al final resulta costoso, tanto desde el punto de vista económico como en términos de productividad, ya que el cryptojacking puede ralentizar considerablemente las actividades no relacionadas con la minería. La víctima no solo paga por el mayor consumo energético, sino que además es posible que deba sustituir dispositivos que se sobrecalientan o que ven reducida su vida útil como consecuencia de estos complejos procesos.

También implica costes medioambientales. Solo en 2020-2021, la minería de Bitcoin tuvo la misma huella de carbono que 190 centrales eléctricas de gas en funcionamiento o la quema de 38.000 millones de kilos de carbón. El gasto total de energía derivado de estas actividades de minería supera el consumo energético de muchos países desarrollados.

La criptominería se ha situado entre los sectores más dañinos para el medio ambiente. Un estudio de Scientific Reports reveló que desde 2016 hasta 2021, cada dólar estadounidense de Bitcoin minado causó 35 céntimos en daños climáticos.

A pesar de su elevado coste, la criptominería no es ilegal, y el cryptojacking pocas veces termina en juicio, aunque es posible que esto esté cambiando. En 2024 ya se ha producido una detención de alto nivel a causa del cryptojacking. Gracias a la colaboración de Europol, las autoridades ucranianas y un proveedor de nube fue posible dar con un sospechoso de haber minado ilegalmente más de 2 millones de dólares en criptomonedas.

Según los datos de SonicWall, en 2023, los ataques de cryptojacking representaron un sexto de todos los ataques de malware. A medida que aumenta la popularidad de la minería ilícita, podemos empezar a ver el mismo tipo de respuestas coordinadas de los sectores público y privado que observamos tras el boom de ransomware del principio de la década de los 2020.

RTDMI detecta más de 1,5 millones de variantes de malware

A pesar de que casi todos los tipos de amenazas han experimentado aumentos, SonicWall Capture Advanced Threat Protection (ATP), con Inspección profunda de memoria en tiempo real (RTDMI), registró considerablemente menos variantes de malware nunca antes vistas en 2023: 387.000, cifra que supone un descenso interanual del 38 %.

Esto, junto con el aumento del malware y los niveles persistentemente altos de phishing, ofrece información valiosa sobre el panorama de las amenazas de 2023. Si bien los cibercriminales no están reduciendo su actividad, de momento, están encontrando variantes eficaces y utilizándolas repetidamente. En diciembre, en particular, se observaron menos variantes nuevas de lo habitual, registrándose la menor cifra desde agosto de 2020.

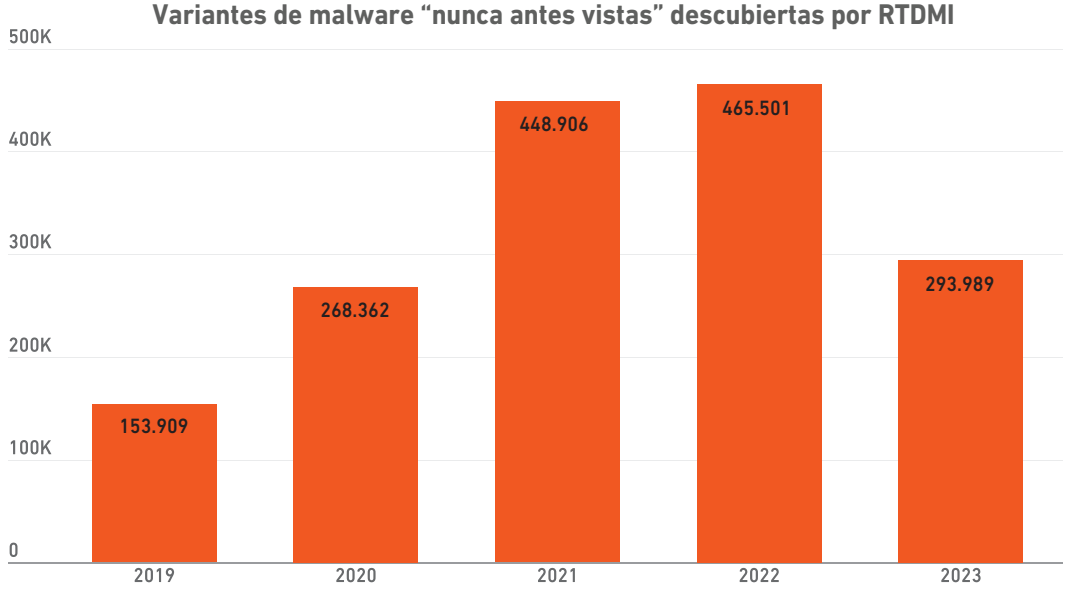
No obstante, todavía se crean muchas variantes de malware nuevas. Tanto es así, que las más de 800 variantes diarias nunca vistas que los clientes registraron de media en 2023 fueron suficientes para superar la marca total de 1,5 millones de detecciones. Sin embargo, parece que se ha ralentizado la innovación, por lo menos de forma temporal.

La RTDMI mejora la seguridad de las credenciales

Mientras que en 2023 los cibercriminales se han decantado por técnicas de eficacia probada, en SonicWall hemos dedicado el año a mejorar nuestros productos y herramientas. Añadimos un nuevo módulo al motor de RTDMI, mejorando enormemente la detección del robo de credenciales vía HTML.

Los ataques de phishing por HTML constituyen uno de los métodos más comunes de robo de credenciales. Las páginas se ofuscan utilizando redireccionamiento mediante iFrame, JavaScript, cargas dinámicas y otros métodos para evitar levantar sospechas. Este nuevo módulo permite detectar estos archivos altamente ofuscados. Entrega contenido HTML de forma segura en un entorno de sandbox y desofusca el estado final, donde la actividad o el intento maliciosos pueden observarse claramente sin poner el peligro la red.

Variantes de malware "nunca antes vistas" descubiertas por RTDMI



Ataques "de día cero" vs. "nunca antes vistos"

El "ataque de día cero" es uno de los conceptos de ciberseguridad más conocidos debido a su conexión con filtraciones de alto nivel. Estos ataques constituyen amenazas completamente nuevas y desconocidas dirigidas contra vulnerabilidades de día cero que no cuentan con ninguna protección (como parches, actualizaciones, etc.) por parte del proveedor o la empresa atacados.

A la inversa, SonicWall hace un seguimiento de la detección y mitigación de "ataques nunca antes vistos," es decir, la primera vez que SonicWall Capture ATP identifica una definición como maliciosa. Estos descubrimientos a menudo se alinean estrechamente con los patrones de los ataques de día cero debido al volumen de ataques analizados por SonicWall.

QUÉ PUEDE HACER USTED

Ante la creciente marea de amenazas descrita en el presente informe, no puede evitar ser el blanco de ataques. Sin embargo, puede tomar medidas para reforzar su enfoque de seguridad en general:

1. **Implementar la autenticación multifactor (MFA)**
   Implementar la MFA mejora significativamente la seguridad de la autenticación. Incluso si alguien consigue acceder a sus contraseñas, no tendrá acceso a sus cuentas ya que el sistema le exige a usted como usuario una segunda autenticación.
2. **Aplicar parches rápidamente**
   Mientras que las vulnerabilidades de día cero acaparan titulares, la mayoría de los intentos de exploit van dirigidos a vulnerabilidades que ya tienen meses o años.
3. **Evaluar la seguridad de forma regular**
   Esto le ayudará a identificar vulnerabilidades, evaluar riesgos y reforzar las defensas de forma proactiva, garantizando una protección sólida contra las cambiantes amenazas.
4. **Ofrecer formación continua en materia de seguridad**
   A medida que avanza la tecnología, también lo hace la ciberseguridad. Al implementar cursos básicos y prácticas rutinarias — como alentar a los empleados a no hacer clic en enlaces maliciosos y enseñarles a identificar e informar de posibles riesgos de seguridad — las empresas pueden disfrutar de un personal más capacitado y atento.
5. **Escanear el tráfico cifrado**
   Los expertos calculan que entre el 80 y el 90 por ciento de todo el tráfico de red actual está cifrado. Sin embargo, muchos firewalls antiguos carecen de la capacidad y la potencia de procesamiento necesarias para detectar, inspeccionar y mitigar los ciberataques enviados a través del tráfico HTTPS, mucho menos si utiliza TLS 1.3, por lo que los hackers utilizan el cifrado de forma rutinaria para implementar y ejecutar su malware. Según datos de SonicWall, desde 2020 hasta 2023, el malware enviado a través de HTTPS registró un espectacular aumento del 117 %. En total, SonicWall registró 15,8 millones de ataques cifrados en 2023, casi tantos como en 2021 y 2022 juntos. El crecimiento del tráfico cifrado y de las amenazas cifradas pone de relieve la necesidad de escanear todo el tráfico.
6. **Ampliar su protección a la nube**
   A medida que las empresas trasladan sus datos y flujos de trabajo a la nube, los enfoques más completos y flexibles que incluyen Security Service Edge (SSE) y la arquitectura de red Zero Trust (ZTNA) se convierten en una necesidad para los entornos de trabajo híbridos.

Si desea obtener inteligencia de amenazas actualizada y novedades del sector, siga el blog de SonicWall.

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

www.sonicwall.com

Acerca de SonicWall

SonicWall es una empresa pionera en ciberseguridad, con más de 30 años de experiencia y un enfoque firmemente centrado en sus partners. Gracias a su capacidad de crear, escalar y gestionar la seguridad en tiempo real en entornos de nube, híbridos y tradicionales, SonicWall puede proporcionar de forma rápida y económica soluciones de seguridad creadas específicamente para respaldar a cualquier organización de cualquier parte del mundo. Basándose en datos de su propio centro de investigación de amenazas, SonicWall ofrece protección sin fisuras contra los ciberataques más evasivos y proporciona inteligencia de amenazas accionable a sus partners, a sus clientes y a la comunidad de la ciberseguridad.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035

SONICWALL®

Como mejor práctica, SonicWall optimiza rutinariamente sus metodologías para la recopilación y el análisis de datos, así como para la elaboración de informes. Esto incluye mejoras en la limpieza de datos, cambios en las fuentes de datos y la consolidación de la información sobre las amenazas. Las cifras publicadas en informes anteriores pueden haber sido ajustadas en diferentes periodos de tiempo, regiones o industrias.