2020

INFORME SOBRE CIBERAMENAZAS DE SONICWALL

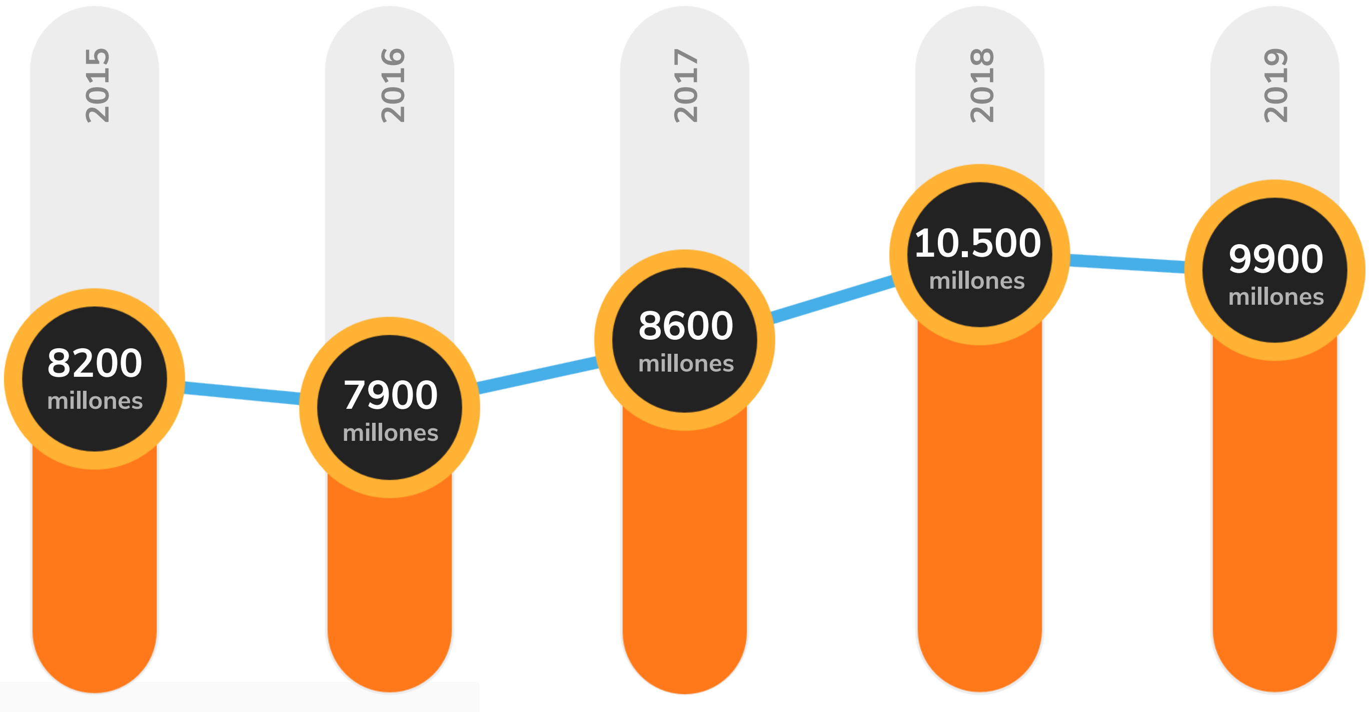
Los límites de su imperio digital son infinitos. Lo que antes era un espacio limitado y defendible es ahora un territorio ilimitado: una enorme y extensa huella de dispositivos, aplicaciones, aparatos, servidores, redes, nubes y usuarios.

Explore la exclusiva inteligencia contra amenazas de SonicWall para comprender mejor cómo piensan los cibercriminales y esté totalmente preparado para saber cuál será su siguiente paso.

MENOS MALWARE, PERO MÁS ORIENTADO Y EVASIVO

9900 millones

fueron los ataques de malware que SonicWall registró* en 2019, con una disminución del 6 %, con respecto al récord de 10.520 millones registrados en 2018.



EL RANSOMWARE ENCONTRÓ UN NUEVO OBJETIVO

187.9 millones

Se está recurriendo al ransomware para atacar con gran precisión a las víctimas más proclives a pagar debido a los datos sensibles que poseen o a los fondos que tienen a su disposición (o ambos).

En 2019, esto significó que muchos de los 187.9 millones de ataques de ransomware fueron contra gobiernos estatales, provinciales y locales, así como sistemas educativos.

DERRUMBE DEL CRYPTOJACKING

El precio del bitcoin y de las criptomonedas complementarias generó una situación insostenible entre el malware de cryptojacking basado en Coinhive y el servicio legítimo de minería de Coinhive.

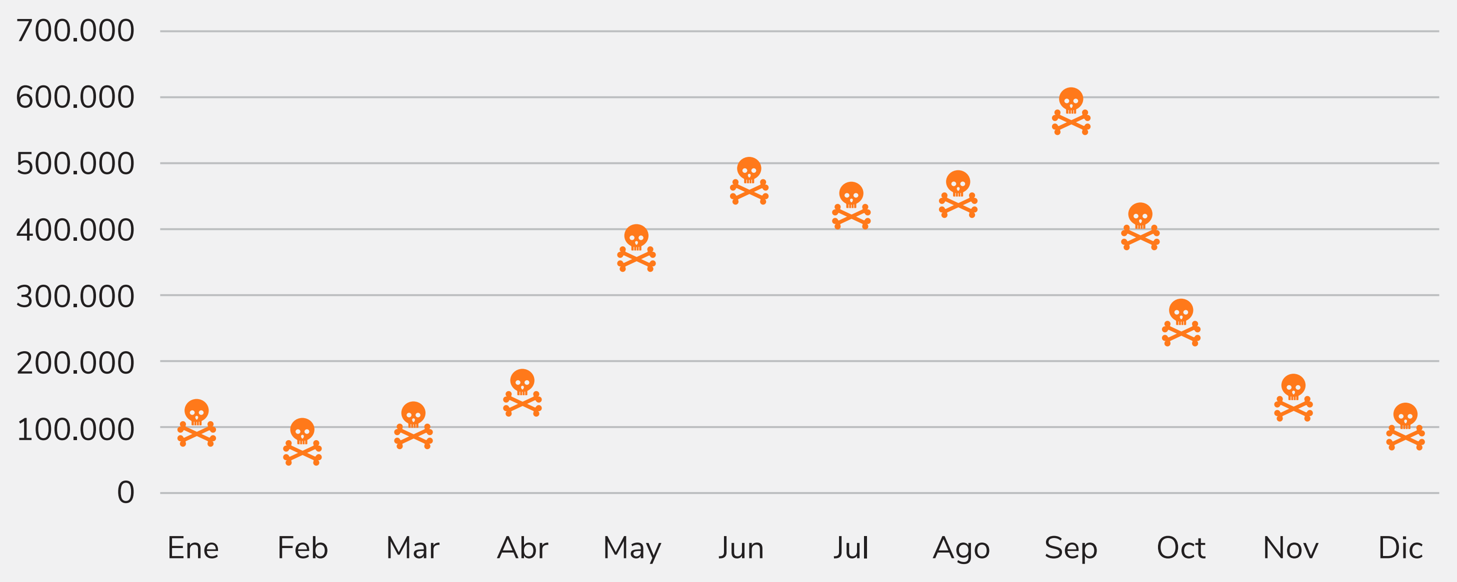
78% ↓

Tras el cierre de Coinhive, el volumen de ataques de cryptojacking cayó un 78% durante la segunda mitad de 2019.

AUMENTA EL MALWARE SIN ARCHIVOS EN EL TERCER TRIMESTRE

El malware sin archivos existe, exclusivamente, como un artefacto basado en memoria y no escribe ninguna parte de su actividad maliciosa en el disco duro de la computadora, lo que lo hace muy resistente a las estrategias forenses. El volumen alcanzó su máximo en el tercer trimestre, con más de 570.000 ataques registrados por SonicWall solo en septiembre de 2019.

Volumen de malware sin archivos en 2019



AMENAZAS CIFRADAS EN CONSTANTE AUMENTO

Los cibercriminales expertos siguen utilizando el cifrado TLS/SSL para ocultar sus ataques de las inspecciones con controles de seguridad tradicionales. En 2019, los investigadores de amenazas de Capture Labs de SonicWall registraron un aumento interanual del 27,3% del malware enviado por tráfico TLS/SSL.

27% ↑

de aumento del malware enviado por tráfico TLS/SSL en 2019.

AUMENTO DEL VOLUMEN DE ATAQUES A LA IOT

En 2019, SonicWall descubrió un aumento del 5 % en el malware de IoT, con un volumen total que alcanzó los 34,3 millones de ataques.

Pero dado el aluvión de nuevos dispositivos de IoT que se conectan cada día, no solo cabe esperar un importante aumento del malware de IoT, sino que también hay que planificar para su llegada.

34,3 MILLONES ↑

PREPÁRESE PARA LO PRÓXIMO

Visite SonicWall.com/ThreatReport para descargar el **Informe sobre amenazas cibernéticas de SonicWall de 2020** completo. Le proporcionará inteligencia fundamental sobre amenazas para ayudarle a comprender mejor cómo piensan los ciberdelincuentes, y para estar totalmente preparado para saber cuál será su siguiente paso.

OBTENGA EL INFORME

SONICWALL®

| SonicWall.com

* Como mejor práctica, SonicWall optimiza de manera rutinaria sus metodologías para la recopilación, el análisis y la generación de informes de datos. Esto incluye ajustes en la limpieza de datos, cambios en las fuentes de datos y una consolidación de la información sobre amenazas. Las cifras publicadas en informes previos pueden haberse ajustado para períodos de tiempo, regiones o industrias diferentes.