2020

INFORME DE CIBERAMENAZAS DE SONICWALL

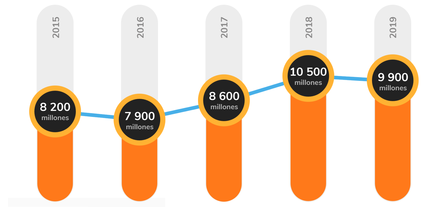
Los límites de su imperio digital son ilimitados. Lo que antes era un espacio finito y defendible ahora es un territorio sin límites: un enorme y extenso espacio ocupado por dispositivos, aplicaciones, aparatos, servidores, redes, nubes y usuarios.

Explore la exclusiva información crítica sobre amenazas de SonicWall para ayudarle a comprender mejor cómo piensan los ciberdelincuentes y estar totalmente preparado para lo que nos depara el futuro.

EL *MALWARE* HA DISMINUIDO, PERO ES MÁS SELECTIVO Y ESQUIVO

9 900 millones

ataques de *malware* fueron registrados* por SonicWall en 2019, una disminución del 6 % con respecto a los 10 520 millones sin precedentes registrados en 2018.



EL *RANSOMWARE* TIENE UN NUEVO OBJETIVO

187,9 millones

El *ransomware* se está utilizando para atacar con gran precisión a las víctimas más proclives a pagar debido a los datos confidenciales que poseen o 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*

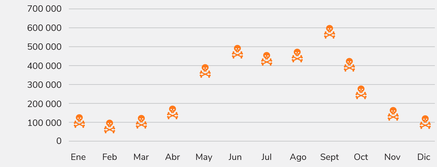
El precio del bitcoin y de las criptomonedas complementarias generó una situación insostenible entre el *malware* de *cryptojacking* basado en Coinhive y el servicio legítimo de minería de Coinhive.

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

EL *MALWARE* SIN ARCHIVOS ALCANZA SU MÁXIMO EN EL 3T

El *malware* sin archivos se ejecuta exclusivamente en la memoria y no registra ninguna parte de su actividad maliciosa en el disco duro del ordenador, con lo que logra eludir 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



LAS AMENAZAS CIFRADAS CONTINÚAN AUMENTANDO DE FORMA CONSTANTE

Los ciberdelincuentes expertos siguen utilizando el cifrado TLS/SSL para ocultar sus ataques de la inspección mediante 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 a través del tráfico TLS/SSL.

27 % aumento del *malware* enviado a través del tráfico TLS/SSL en 2019.

AUMENTO DEL VOLUMEN DE ATAQUES CONTRA 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 alud de nuevos dispositivos IoT que se conectan cada día, solo cabe esperar un importante aumento del malware de IoT, ante el cual hay que estar preparado.

34,3 MILLONES

PREPÁRESE PARA LO PRÓXIMO

Visite SonicWall.com/ThreatReport para descargar el **Informe sobre amenazas cibernéticas de SonicWall 2020** completo. Obtendrá información crítica sobre amenazas para ayudarle a comprender mejor cómo piensan los ciberdelincuentes y a estar totalmente preparado para lo que nos depara el futuro.

OBTENER 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 consolidación de la información sobre amenazas. Las cifras publicadas en informes previos se pueden haber ajustado a través de períodos de tiempo, regiones o industrias diferentes.