Informe de Amenazas Cibernéticas de SonicWall 2019

RESUMEN EJECUTIVO | EDICIÓN MUNDIAL

SonicWall.com

SONICWALL®

CAPTURE LABS

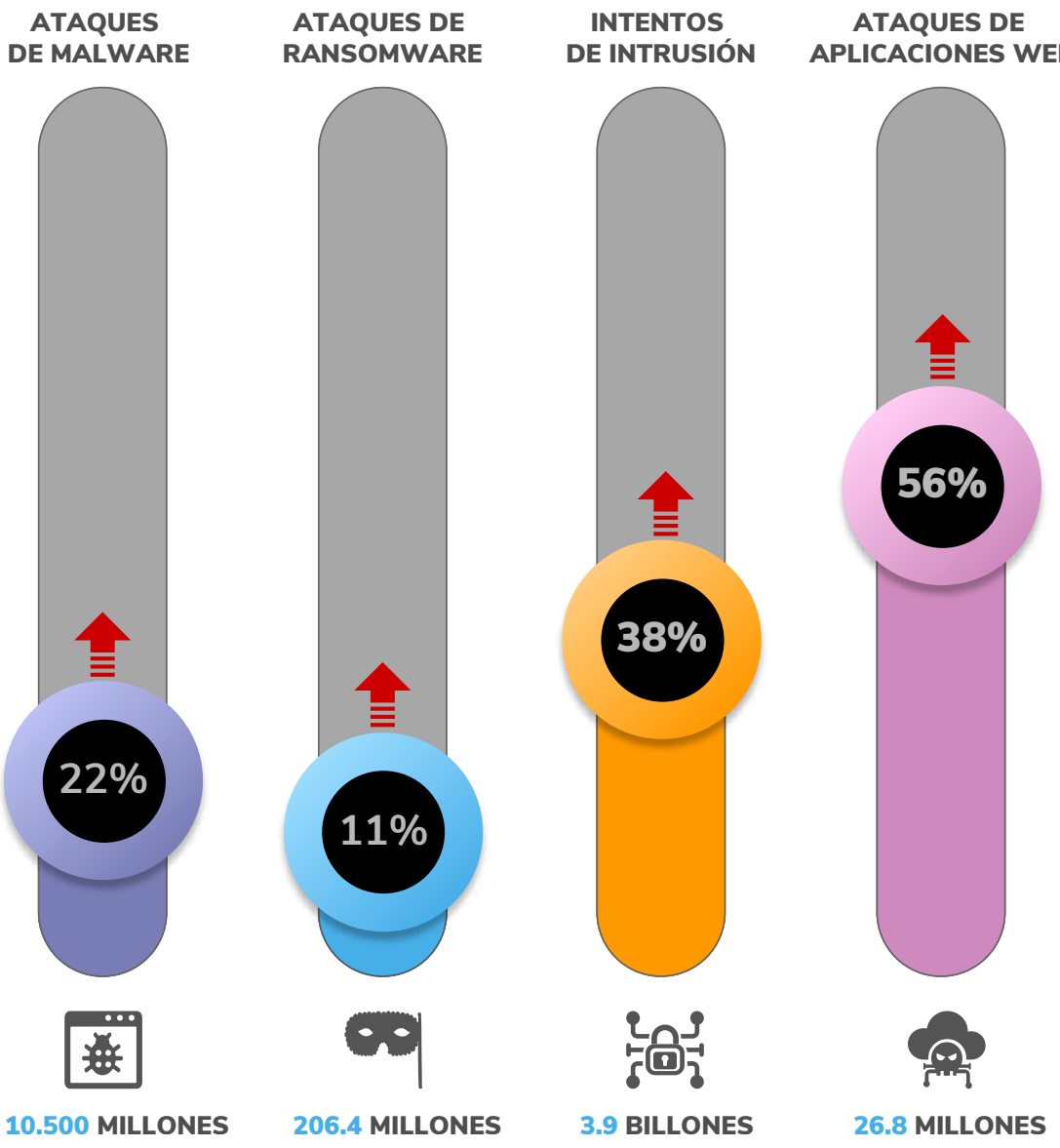
INTRODUCCIÓN: EDICIÓN MUNDIAL

La carrera armamentista cibernética no discrimina ni hace diferenciaciones. Si una red, una identidad, un dispositivo o información tienen valor (en particular la información relacionada con la propiedad intelectual o de uso político, variables financieras, archivos sensibles o infraestructura crítica) los cibercriminales los identificarán, serán sus objetivos y atacarán despiadadamente.

Con el fin de promover una concientización a nivel mundial y facilitar conversaciones importantes, SonicWall permanece firme en su compromiso con investigar, analizar y compartir inteligencia sobre amenazas a través del Informe de amenazas cibernéticas de SonicWall 2019. Como complemento del informe detallado, este resumen ejecutivo brinda una perspectiva de alto nivel acerca de la inteligencia sobre amenazas de parte de los investigadores de amenazas de SonicWall Capture Labs.

DESCUBRIMIENTOS CLAVE DURANTE EL 2018

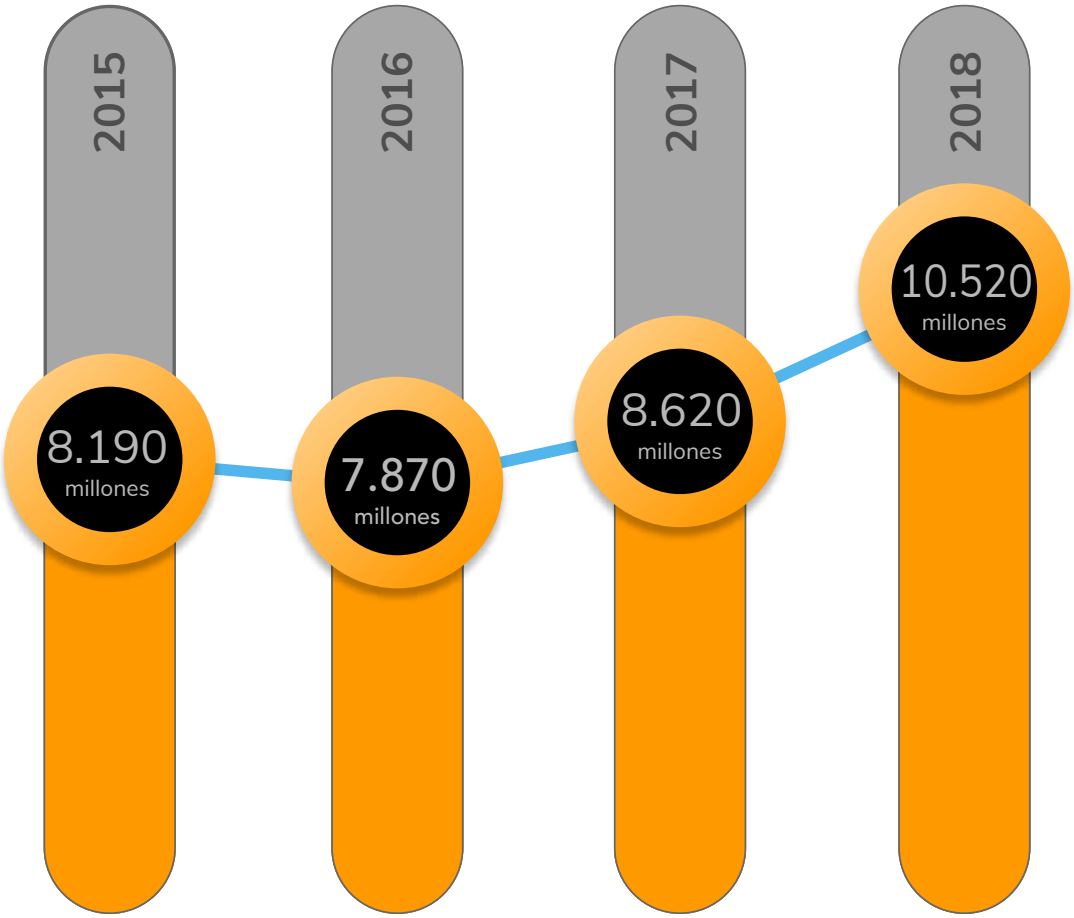
TENDENCIAS DE CIBERATAQUES A NIVEL MUNDIAL DURANTE EL 2018



SONICWALL®

DESCUBRIMIENTOS CLAVE DURANTE EL 2018

En el año 2016, la industria experimentó un descenso en el volumen de malware, lo cual llevó a especulaciones de que el cibercrimen estaba disminuyendo. A partir de entonces, **los ataques de malware se han incrementado un 33,4 por ciento.** A nivel mundial, SonicWall registró 10.520 millones* de ataques de malware durante el 2018, la cantidad más alta registrada.

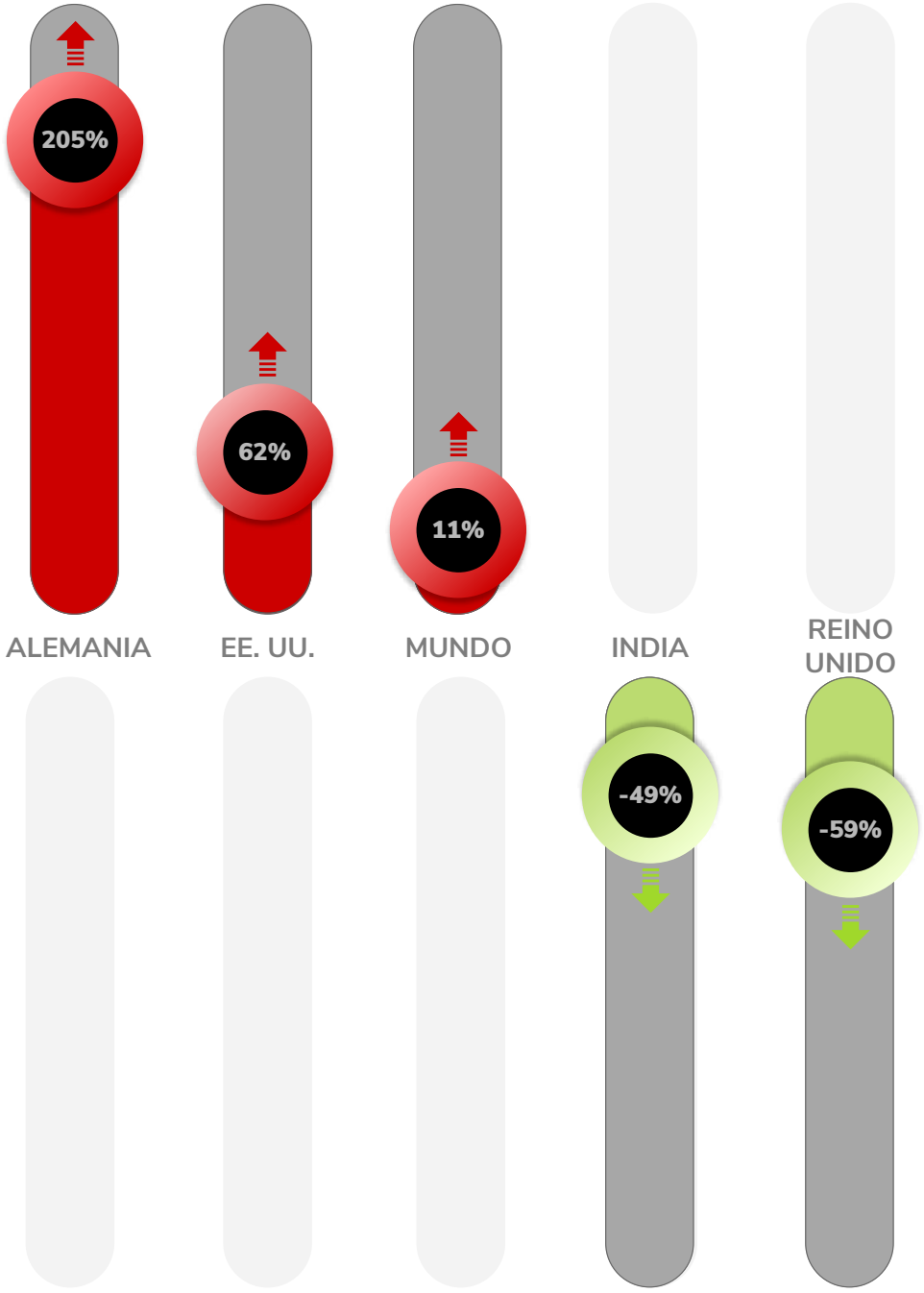


* A modo de práctica recomendada, SonicWall optimiza de manera rutinaria sus metodologías de recolección, análisis e informe de datos. Esto incluye mejoras en la depuración de los datos, cambios en las fuentes de datos y consolidación de los informes sobre amenazas. Las cifras publicadas en informes previos se pueden haber ajustado a través de períodos de tiempo, regiones o industrias diferentes.

EL REINO UNIDO Y LA INDIA, FORTALECIDOS CONTRA EL RANSOMWARE

Luego de que los investigadores de amenazas de SonicWall Capture Labs finalizaron el análisis de la información de amenazas del 2018, se descubrió algo llamativo. El ransomware aumentó en casi todas las regiones geográficas, excepto en dos: el Reino Unido y la India.

Mientras que los países más importantes de América del Norte, Europa y Asia experimentaron un aumento significativo en los ataques de ransomware, **el Reino Unido y la India tuvieron una reducción en el volumen de ransomware del 59 y el 49 por ciento**, respectivamente.



SONICWALL®

ATAQUES DE CANAL LATERAL, PELIGROSAS AMENAZAS A LA MEMORIA, IDENTIFICADOS TEMPRANAMENTE

RTDMI no se limita a detectar los ataques de malware nunca antes vistos. RTDMI también mitiga los peligrosos ataques de canal lateral utilizando una tecnología con patente pendiente. Los canales laterales son el vehículo fundamental utilizado para explotar y exfiltrar datos de vulnerabilidades en los procesadores, como, por ejemplo, Foreshadow, PortSmash, Meltdown y Spectre.

Lamentablemente, las investigaciones actuales indican que **"Spectre llegó para quedarse"** y reconocen que hay diversas vulnerabilidades en los procesadores que no se pueden solucionar con parches, tanto en el software como en el hardware, y que representan una preocupación de seguridad mucho más grave. Por lo tanto, los ataques de canal lateral serán un riesgo continuo en el ámbito informático, y desarrollar tecnología que pueda mitigar estos ataques será una necesidad fundamental.

ATAQUES CIFRADOS EN CONTINUO CRECIMIENTO

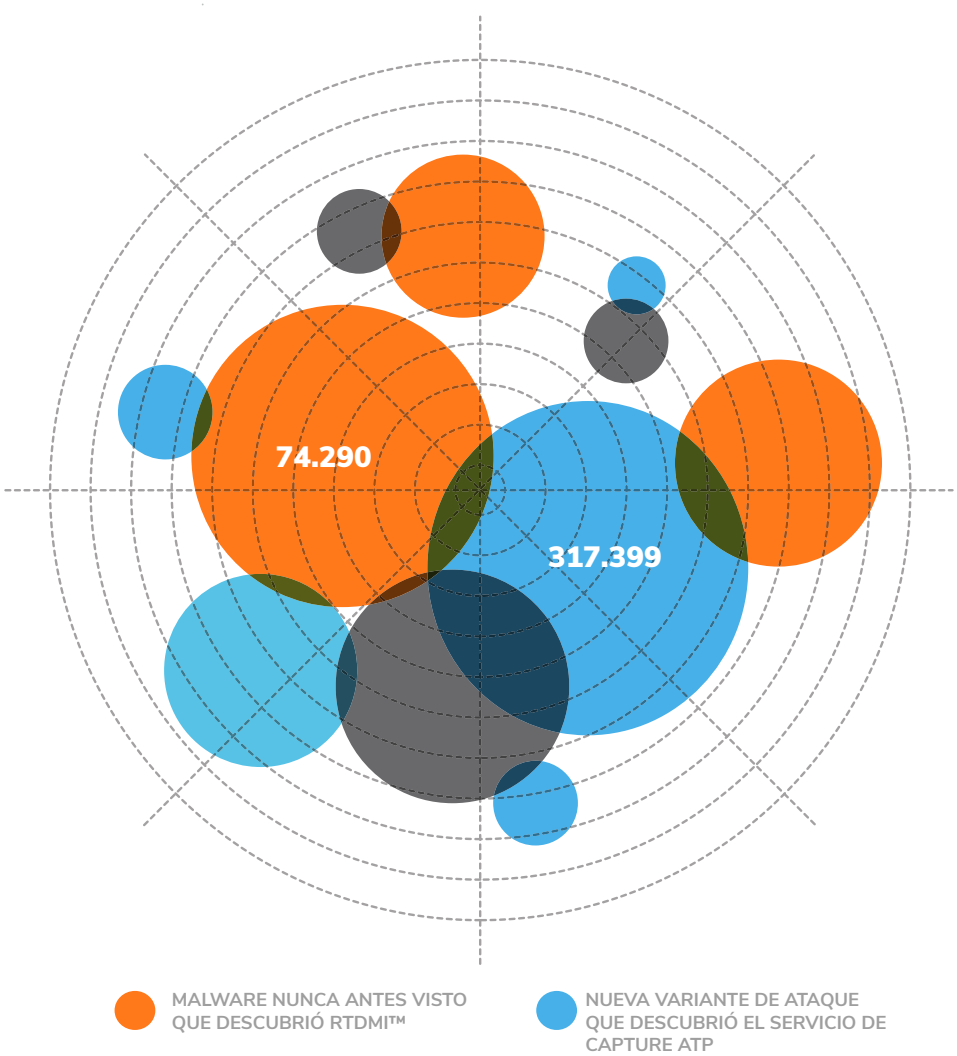
El crecimiento del tráfico cifrado coincide con un aumento de ataques ocultos mediante cifrado TLS/SSL. Durante el 2018, más de **2.8 millones de ataques fueron cifrados,** lo que representó un incremento del 27 por ciento con respecto al 2017.

EVOLUCIÓN DEL APRENDIZAJE AUTOMÁTICO PARA DETENER VARIANTES DE MALWARE NUNCA ANTES VISTAS

El servicio Capture Advanced Threat Protection (ATP) de SonicWall identificó 391.689 variantes nuevas de ataque durante el 2018. Esto da como resultado un promedio de más de **1.072 ataques nuevos que se descubrieron y bloquearon por día.**

El servicio de Capture ATP utiliza un entorno aislado multimotor en la nube en paralelo con la tecnología Real-Time Deep Memory Inspection™ (RTDMI) de SonicWall con patente pendiente. Estas dos capacidades desarrollaron su aprendizaje y mejoramiento automáticos de manera dinámica a lo largo del 2018.

Específicamente, **RTDMI™ identificó 74.290 ataques nunca antes vistos en el 2018.** Estas son variantes de malware tan recientes, únicas o complejas que ningún otro proveedor en el mundo había podido crear ni rastrear firmas en el momento en que SonicWall las descubrió.

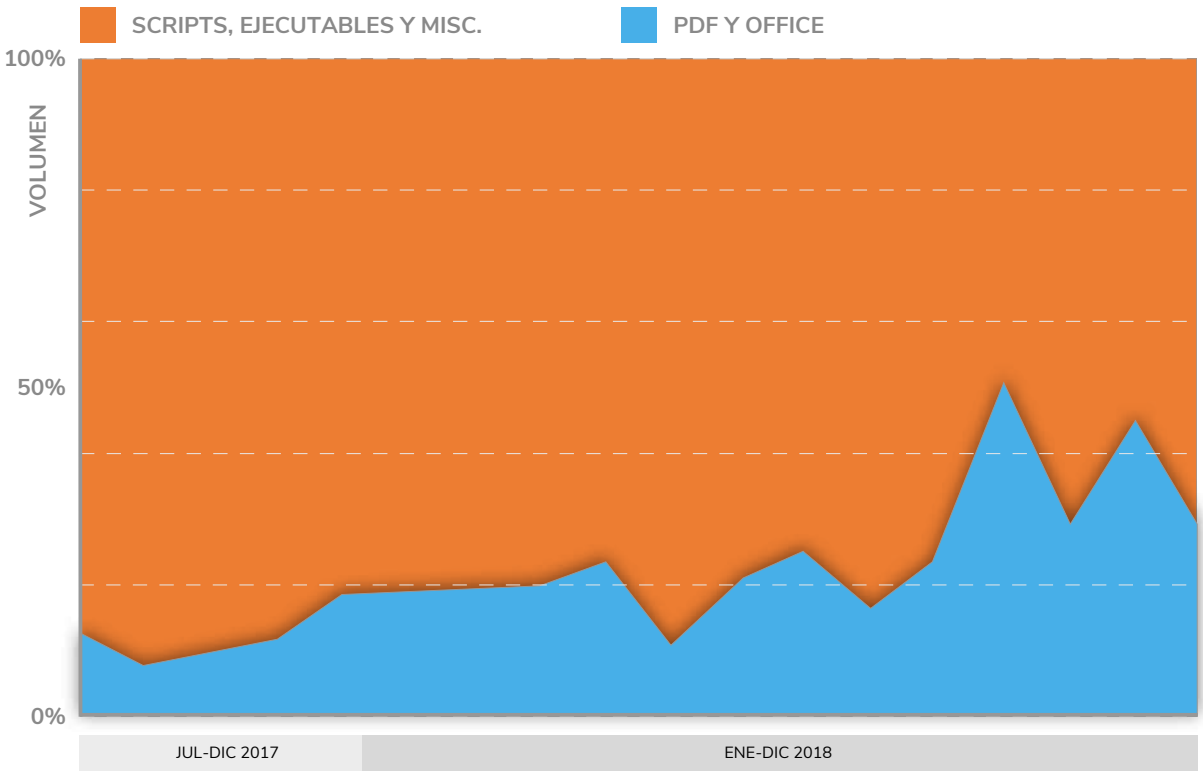


SONICWALL®

CONTROLES DE SEGURIDAD TRADICIONALES SUPERADOS POR ARCHIVOS PDF Y DE MICROSOFT OFFICE MALICIOSOS

Los cibercriminales están utilizando archivos PDF y de Microsoft Office confiables para ayudar al malware a eludir los firewalls tradicionales e incluso los entornos aislados con un solo motor.

INCREMENTO EN LA CANTIDAD DE ARCHIVOS PDF Y DE OFFICE MALICIOSOS

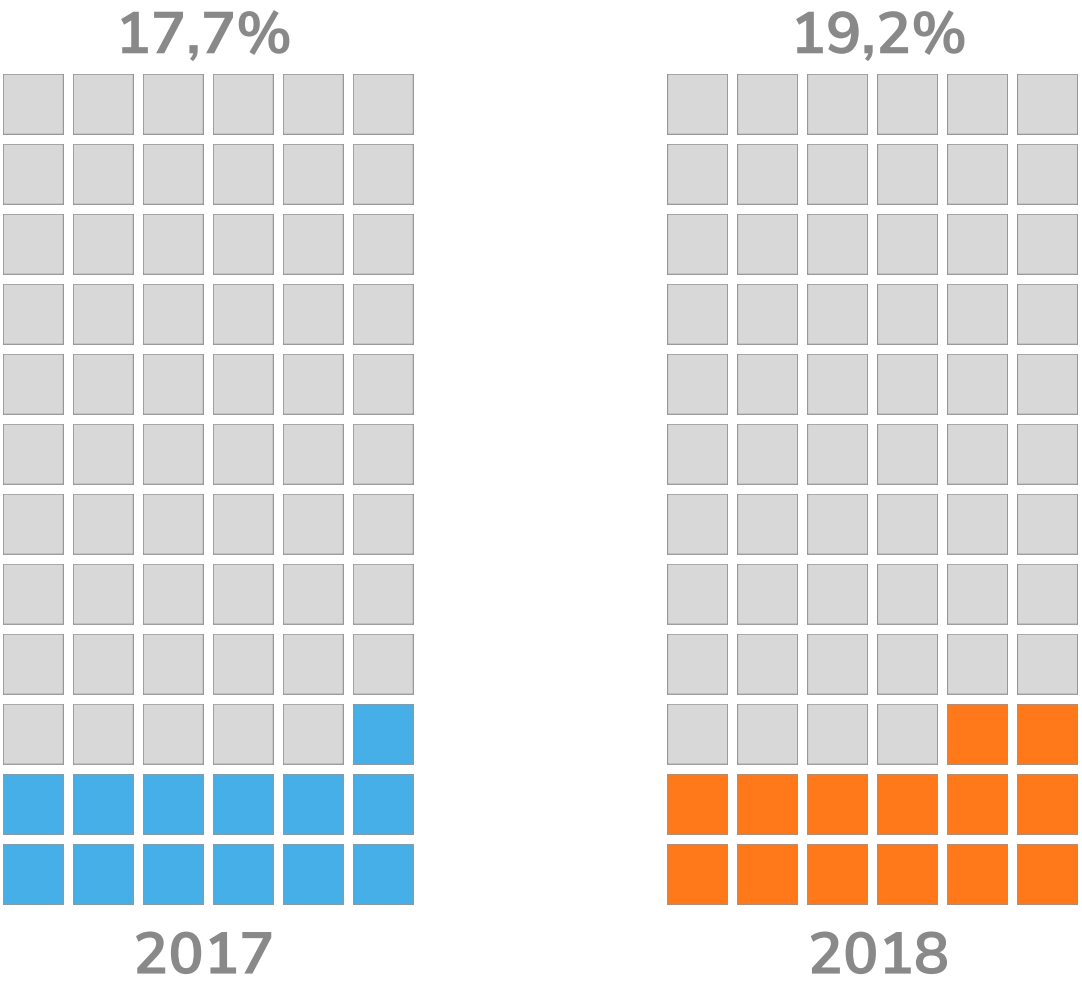


El servicio multimotor de entorno aislado Capture ATP de SonicWall encontró **malware oculto en 47.073 archivos PDF y en 50.817 archivos de Microsoft Office** durante el 2018. Si bien el volumen parece bajo a primera vista, la mayoría de los controles de seguridad no logran identificar y mitigar el malware oculto en estos archivos, lo que aumenta significativamente el éxito de la carga útil.

LOS PUERTOS NO ESTÁNDAR, A MERCED DE EXPLOTACIÓN

Los puertos 80 y 443 son puertos estándar para tráfico web, es por eso que la mayoría de los firewalls se enfocan en protegerlos. Como respuesta a esto, los cibercriminales cambiaron su objetivo a los puertos no estándar para asegurarse de que sus cargas útiles se puedan desplegar sin ser detectadas en un entorno objetivo.

ATAQUES DE MALWARE EN 2018
DIRIGIDOS A PUERTOS NO ESTÁNDAR



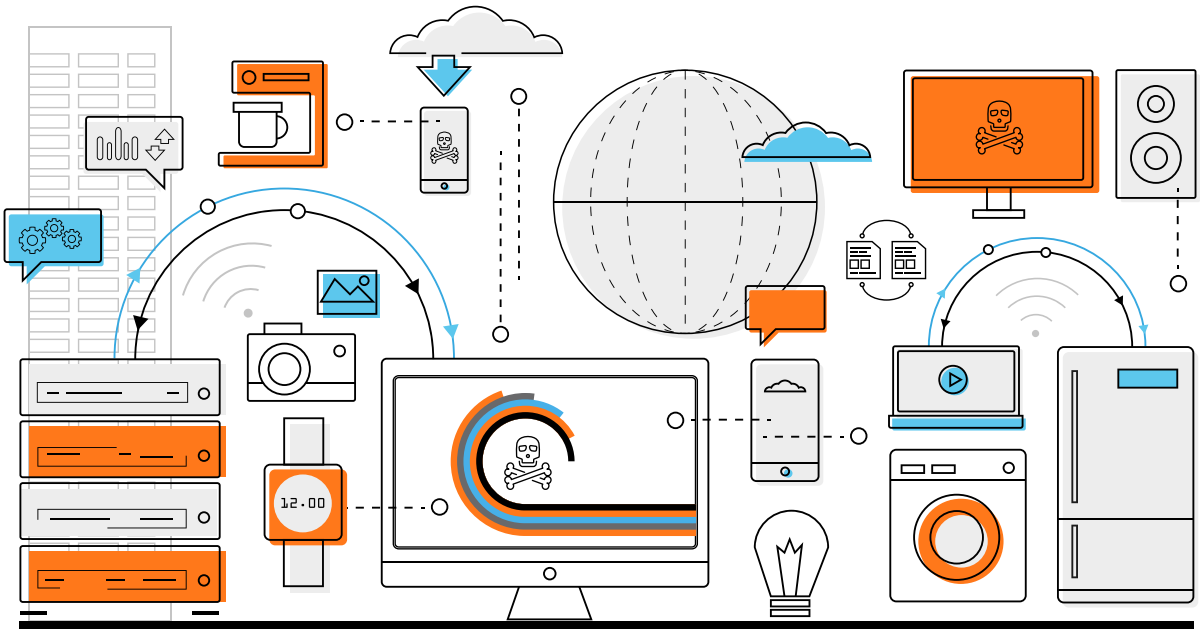
Con base en una muestra de más de 700 millones de ataques de malware, SonicWall descubrió que **el 19,2 por ciento de todos los ataques de malware se realizaron a través de puertos no estándar** en 2018. Debido a que los ataques que se deben monitorear son tantos, los firewalls tradicionales basados en proxy no logran mitigar los ataques contra los puertos no estándar (tanto para el tráfico cifrado como para el no cifrado).

SONICWALL®

ATAQUES AL INTERNET DE LAS COSAS EN AUMENTO

Los consumidores piden cada vez más dispositivos conectados. Pero esta demanda provocó que se apresurara la entrada al mercado de un aluvión de dispositivos de internet de las cosas (IOT) que no contaban con los controles de seguridad adecuados. En muchos casos, los dispositivos de IOT están configurados con ajustes de seguridad predefinidos, lo que los convierte en blancos fáciles de credenciales conocidas o botnets poderosos.

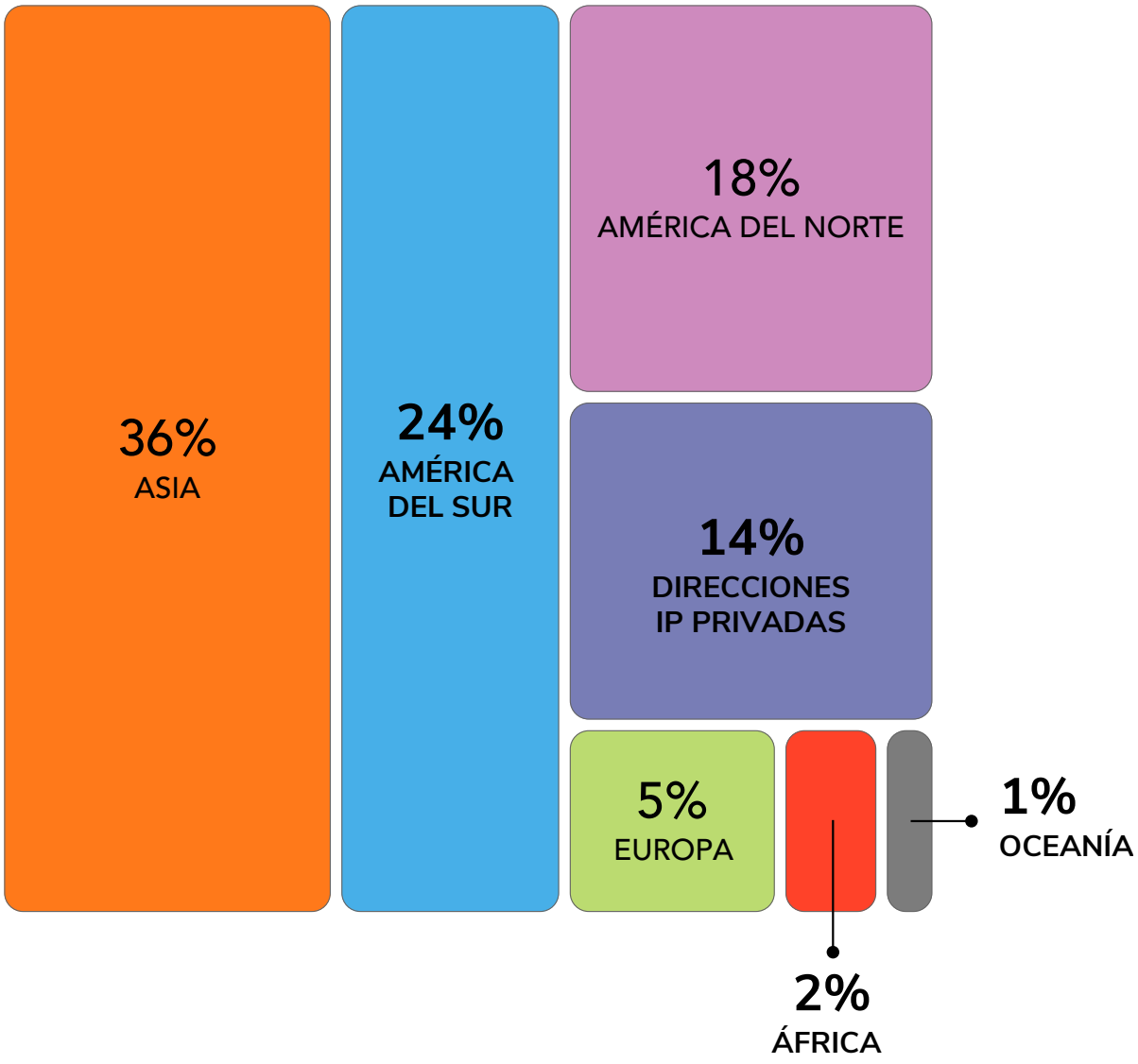
En total, SonicWall registró **32.7 millones de ataques al IOT durante el 2018,** lo que representó un aumento del 217,5 por ciento en comparación con los 10.3 millones de ataques al IOT que la compañía registró en el 2017.



AUGE Y CAÍDA DEL CRYPTOJACKING

En el 2018, el cryptojacking desapareció casi con la misma velocidad con la que apareció. SonicWall registró **57.5 millones de ataques de cryptojacking** a nivel mundial entre abril y diciembre. El volumen alcanzó su pico en septiembre, con 13.1 millones de ataques registrados, pero registró un descenso continuo desde entonces. A pesar de su devaluación, las criptomonedas siguen siendo una mercancía valiosa para los cibercriminales debido a su anonimato.

CRYPTOJACKING POR REGIÓN DURANTE EL 2018



VOLUMEN DE PHISHING GLOBAL EN DESCENSO, ATAQUES MÁS DIRIGIDOS

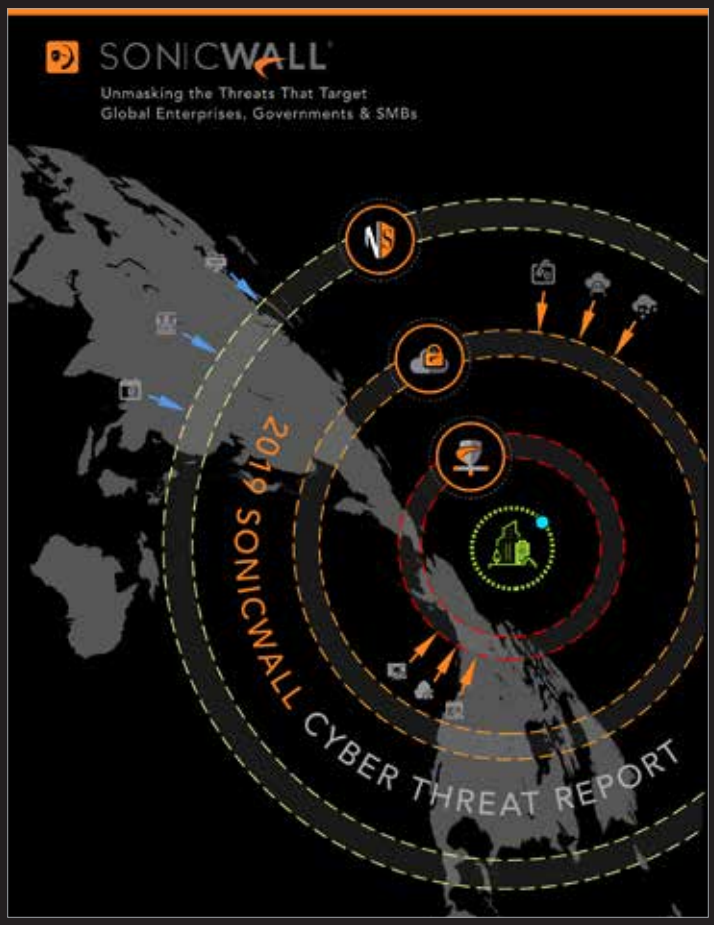
ATAQUES DE PHISHING
EN TODO EL MUNDO **26 MILLONES**

A medida que las empresas mejoran su capacidad de bloqueo de ataques a través de correo electrónico y se aseguran de que sus empleados sean capaces de detectar y eliminar los correos sospechosos, los atacantes cambian sus tácticas. Reducen el volumen de ataque total y lanzan ataques de phishing extremadamente más dirigidos (p. ej., poner en riesgo un correo corporativo, apropiaciones de cuenta, whaling, etc.).

En el 2018, SonicWall registró **26 millones de ataques de phishing en todo el mundo,** lo que representó una disminución del 4,1 por ciento con respecto al 2017. El cliente promedio de SonicWall afrontó 5.488 ataques de phishing durante el 2018.

Información de inteligencia sobre amenazas cibernéticas y análisis exclusivos. Solo con SonicWall Capture Labs.

MÁS INFORMACIÓN



Visite SonicWall.com/ThreatReport para descargar la versión completa del Informe de Amenazas Cibernéticas de SonicWall 2019. Obtendrá un nueva perspectiva sobre las estrategias de ataques cibercriminales y comprenderá cómo defender adecuadamente su organización o negocio de los ciberataques más sofisticados.

* A modo de práctica recomendada, SonicWall optimiza de manera rutinaria sus metodologías de recolección, análisis e informe de datos. Esto incluye mejoras en la depuración de los datos, cambios en las fuentes de datos y consolidación de los informes sobre amenazas. Las cifras publicadas en informes previos se pueden haber ajustado a través de períodos de tiempo, regiones o industrias diferentes.

SONICWALL