MILPITAS, Calif. — OCT. 29, 2020 — Los servicios de Inteligencia y analistas de SonicWall Capture Labs, revelaron las principales amenazas del tercer trimestre del año recopiladas por los más de 1 millón de sensores de seguridad global de la compañía.

Los resultados del año hasta septiembre de 2020 destacan el creciente uso de ransomware por parte de los ciberdelincuentes, las amenazas cifradas y los ataques que aprovechan los puertos no estándar, mientras que el volumen general de malware disminuyó por tercer trimestre consecutivo.

> *"Para la mayoría de nosotros, 2020 ha sido el año en el que las economías casi se detienen, los trayectos diarios al trabajo terminan y las oficinas tradicionales desaparecen"*, dijo Bill Conner, presidente y director ejecutivo de SonicWall. *"Sin embargo, la aparición repentina de fuerzas de trabajo remotas y oficinas virtuales ha proporcionado a los ciberdelincuentes vectores nuevos y atractivos para explotar. Estos hallazgos muestran su incansable búsqueda de obtener lo que no es legítimamente suyo para obtener ganancias, control económico y reconocimiento global «.*

Los principales hallazgos de SonicWall Capture Labs son:

• Disminución del 39% en malware (4.4 mil millones hasta la fecha); continúa a la baja el volumen por tercer trimestre consecutivo
• Aumento del 40% del ransomware global (199.7 millones)
• Incremento del 19% en los intentos de intrusión (3.5 billones)
• Aumento del 30% en el malware de IoT (32.4 millones)
• 3% de crecimiento de amenazas cifradas (3.2 millones)
• Aumento del 2% en criptojacking (57.9 millones)

Disminución del volumen de malware a medida que los ataques están más dirigidos y diversificados

Si bien los autores de ataques de malware y ciberdelincuentes todavía están ocupados trabajando para lanzar sofisticados ataques cibernéticos, la investigación de SonicWall concluye que el volumen global de malware continúa disminuyendo de manera constante en 2020.

En una comparación año tras año hasta el tercer trimestre, los investigadores de SonicWall registraron 4.4 mil millones de ataques, esto representa una caída del 39% en todo el mundo.

Las comparaciones por región muestran que India (-68%) y Alemania (-64%) han experimentado una vez más un porcentaje de disminución considerable, así como Estados Unidos (-33%) y Reino Unido (-44%). Un número menor de malware no significa que vaya a desaparecer por
completo. Más bien, esto es parte de una recesión cíclica que puede corregirse fácilmente en un corto período de tiempo.

El ransomware entra en erupción, Ryuk es responsable de un tercio de todos los ataques

Los ataques de ransomware se reportan diariamente en los medios, ya que causan estragos en empresas, localidades, organizaciones de salud e instituciones educativas. Los investigadores de SonicWall monitorearon un crecimiento agresivo durante cada mes del tercer trimestre, incluido un aumento masivo en septiembre. Mientras que los sensores en la India (-29%), el Reino Unido (-32%) y Alemania (-86%) registraron disminuciones; en Estados Unidos se percibió un asombroso número de 145.2 millones de accesos de ransomware, esto es un aumento interanual del 139%.

En particular, los investigadores de SonicWall observaron un aumento significativo en las

detecciones de ransomware de Ryuk en 2020. Mientras en el tercer trimestre de 2019, SonicWall detectó 5.123 ataques de Ryuk, durante el tercer trimestre de 2020, SonicWall detectó 67.3 millones de ataques Ryuk, lo que una tercera parte (33.7%) de todos los ataques de ransomware de este año.

> *«Lo interesante es que Ryuk es una familia de ransomware relativamente joven que se descubrió en agosto de 2018 y que ha ganado una popularidad significativa en 2020»,* dijo el vicepresidente de arquitectura de plataforma de SonicWall, Dmitriy Ayrapetov. *"El aumento de la fuerza laboral remota y móvil parece haber aumentado su prevalencia, lo que no solo genera pérdidas financieras, sino que también afecta los servicios de salud con ataques a hospitales. Ryuk es especialmente peligroso porque es dirigido, manual y, a menudo, aprovechado a través de un ataque de varias etapas precedido por el malware Emotet y TrickBot. Por lo tanto, si una organización tiene Ryuk, es un buen indicativo de que está infestada de varios tipos de malware»*

En este sentido, la solución de SonicWall Capture Advanced Threat Protection (ATP), con RealTime Deep Memory InspectionTM (RTDMI) pendiente de patente, protege contra todas las variantes de ransomware Emotet, TrickBot y Ryuk, en tiempo real.

La dependencia de IoT crece junto con las amenazas

COVID-19 provocó una avalancha inesperada de dispositivos conectados en las redes, lo que resultó en un aumento de las amenazas potenciales para las empresas que luchan por permanecer operando durante la pandemia. SonicWall Capture Labs detectó un aumento del 30% en los ataques de malware de IoT, un total de 32.4 millones en todo el mundo.

La mayoría de los dispositivos de IoT, incluidos los dispositivos inteligentes activados por voz, así como los timbres de las puertas, cámaras de televisión y los electrodomésticos, no se diseñaron con la seguridad como una prioridad, lo que los hace susceptibles a los ataques y

proporciona a los ciberdelincuentes numerosos puntos de entrada.

> *"A menudo los empleados confiaban en la seguridad de las redes en las oficinas, pero el crecimiento de la fuerza de trabajo remota y móvil ha ampliado las redes distribuidas que sirven tanto en casa como en el home office",* dijo Conner. *"Los consumidores deben detenerse y pensar si dispositivos como controles AC, sistemas de alarma para el hogar o monitores para bebés se han instalado de forma segura. Para una protección óptima, los profesionales que utilizan oficinas virtuales desde casa, especialmente aquellos que operan en la C-suite, deben considerar segmentar las redes domésticas «*

Los datos de la unidad de inteligencia de amenazas de SonicWall también concluyó, que si bien el cryptojacking (57.9 millones), los intentos de intrusión (3.5 billones) y las amenazas de malware de IoT (32.4 millones) son tendencia en los informes de volumen de la primera mitad, siguen
siendo una amenaza y una fuente de oportunidades para ciberdelincuentes.

Acerca de SonicWall Capture Labs

Los investigadores y analistas de amenazas de SonicWall Capture Labs recopilan, analizan y examinan información sobre amenazas entre vectores de la red SonicWall Capture Threat, que consta de dispositivos y recursos globales, incluidos más de 1 millón de sensores de seguridad en casi 215 países y territorios. SonicWall Capture Labs, que fue pionero en el uso de inteligencia artificial para la investigación y protección de amenazas hace más de una década, realiza pruebas y evaluaciones rigurosas de estos datos, establece puntajes de reputación para los remitentes de correo electrónico y el contenido e identifica nuevas amenazas en tiempo real.