MILPITAS, Calif. — Julio 23, 2020 —El equipo de investigación de amenazas de SonicWall Capture Labs publicó hoy la actualización de mitad de año del Reporte de Amenazas Cibernéticas de SonicWall 2020, destacando los aumentos en ransomware, el uso oportunista de la pandemia COVID-19, las debilidades sistémicas y la creciente dependencia de los archivos de Microsoft Office por parte de los ciberdelincuentes.

- *Crecimiento de 20% en ransomware a nivel mundial*
- *México recibió casi 10 millones de ataques de malware en el primer semestre del año; Brasil más de* 69 millones
- *Marzo fue el mes más crítico para México en ataques de malware rebasando los 3 millones de intentos; mientras que en Brasil en junio superó los 16 millones*
- *7% de los ataques de phishing utilizaron la pandemia COVID-19 como señuelo*
- *'Virus' lidera el Top5 de palabras más utilizadas en ataques de phishing*
- *176% de aumento en archivos maliciosos de Microsoft Office*
- *23% de los ataques de malware aprovecharon los puertos no estándar*
- *50% de aumento en ataques de malware IoT*
- *Informe analiza los datos de inteligencia de amenazas recopilados de 1.1 millones de sensores en más de 215 países y territorios*

> *"Los cibercriminales pueden ser ingeniosos y a menudo establecen trampas para aprovechar la bondad de las personas durante un desastre natural, que entrando en pánico a lo largo de la crisis confían demasiado en los sistemas que utilizan en su vida cotidiana»*, dijo el presidente y CEO de SonicWall, Bill Conner. *"Estos últimos datos de amenazas cibernéticas muestran que los cibercriminales continúan transformando sus tácticas para influir en las probabilidades a su favor en tiempos de incertidumbre. Con todo el mundo trabajando más que nunca de forma remota y móvil, las empresas están muy expuestas y la industria cibercriminal es muy consciente de eso. Por lo tanto, es imperativo que las organizaciones se alejen de las estrategias de seguridad improvisadas o tradicionales y se den cuenta que este nuevo normal en los negocios ya no es nuevo «.*

Disminuye malware a nivel global, pero México y Brasil mantienen una fuerte batalla

Durante el primer semestre de 2020, los ataques de malware a nivel global cayeron de 4.8 a 3.2 mil millones (-24%) en comparación con el mismo periodo en 2019. Esta caída es la continuación de una tendencia a la baja que comenzó en noviembre pasado.

Existen diferencias regionales tanto en la cantidad de malware como en el porcentaje de año contra año, lo que deja ver un cambio en los objetivos de los cibercriminales. Por ejemplo, países como Estados Unidos (-24%), Reino Unido (-27%), Alemania (-60%) y la India (-64%), todos experimentaron una reducción en el volumen de malware.

En América Latina, Brasil experimentó una reducción de -56%, mientras que la actividad en México se contrajo en un -3%, cifras que se alinean a la tendencia de disminución a nivel global. Sin embargo, esto no significa que los ciberdelincuentes dejaron de atacar, en el caso de Brasil en la primera mitad de 2020 recibieron 69,583,407 ataques de malware alcanzando en junio el pico más alto con 16,008,648; mientras que México alcanzó la cifra de 9,903,771 ataques de malware obteniendo el punto más crítico durante marzo con 3,944,488 intentos.

Esto hace evidente que menos malware no significa necesariamente un mundo más seguro; de hecho, el ransomware ha venido a complicar la situación ya que durante el mismo periodo de tiempo se ha visto un incremento considerable a nivel global.

Ataques de ransomware suben las apuestas de nuevo

A pesar de la disminución global del volumen de malware, el ransomware sigue siendo la amenaza más preocupante para las corporaciones y la herramienta preferida por los ciberdelincuentes, aumentando un asombroso 20% (121.4 millones) a nivel mundial en el primer semestre de 2020.

En el caso de Latinoamérica, Brasil registró 1,190,092 ataques de ransomware, cifra suficientemente alta como para colocarse en el sexto lugar en el Top10 Global de países con mayor volumen de ataques de este tipo, solo superado por EE. UU., Reino Unido, Malasia, Canadá y los Países Bajos.

Aunque este escenario tiene sus variaciones, tal es el caso de Estados Unidos y Reino Unido. Donde los investigadores de SonicWall Capture Labs detectaron 79.9 millones de ataques de ransomware en EE.UU lo que implica un incremento de 109%, en comparación con los 5.9 millones de ataques de ransomware sufridos por Reino Unido que representan una baja de 6%. Esto significa que las tendencias por país se mueven en función de los comportamientos de las redes cibercriminales.

> *«La fuerza de trabajo remota y móvil se encuentra en un punto de inflexión en el tema de seguridad»*, dijo Chad Sweet, Fundador y CEO The Chertoff Group. *«Nunca ha sido más importante para las empresas y organizaciones priorizar la seguridad en línea, lo que antes podría ser visto como un lujo ahora es una necesidad».*

Emails cargados de malware usaron 5 palabras clave relacionadas con la pandemia

La combinación de la pandemia global y los ciberataques de ingeniería social han demostrado ser una mezcla eficaz para los ciberdelincuentes que utilizan phishing y otras estafas de correo electrónico. Los investigadores de SonicWall detectaron un incremento en la oleada de ataques, estafas y exploits basados específicamente en COVID-19 y notaron un aumento de 7% en los intentos de phishing relacionados con COVID durante los dos primeros trimestres.

En este caso, las palabras clave más utilizadas para ataques de phishing fueron Virus con

42.33%, Corona con 32.92%, Quarantine (Cuarentena) con 9.72%, COVID con 8.77% y Mask (Máscara) con 6.26%.

Como era de esperar, el phishing relacionado con COVID-19 comenzó a despuntar a partir de marzo, viendo los picos más altos los días 24 de marzo, 3 de abril y 19 de junio. Sin embargo, si sacamos COVID de la ecuación, el phishing en general comenzó fuerte en enero y fue bajando ligeramente a nivel mundial (-15%) durante el tiempo en que los intentos de phishing pandémico comenzaron a cobrar fuerza.

Los señuelos de Office continúan siendo básicos

Microsoft Office es una necesidad, que implica a millones de empleados que ahora trabajan de manera remota y son más dependientes de esta suite de aplicaciones de productividad empresarial. Los ciberdelincuentes fueron rápidos para aprovechar este cambio, al respecto los investigadores de amenazas de SonicWall encontraron un aumento de 176% en nuevos ataques de malware disfrazados como archivos de confianza de Microsoft Office.

La solución a este marco es SonicWall CAS (Cloud App Security), que también protege G Suite de Google. Con CAS, el correo electrónico, los mensajes y los archivos generados en Office 365 están protegidos contra ataques, sin importar de dónde acceda el usuario a esta plataforma de Microsoft.

Aprovechando la herramienta SonicWall Capture Advanced Threat Protection (ATP) con la tecnología Real-Time Deep Memory Inspection™ (RTDMI), SonicWall descubrió que el 22% de los archivos de Microsoft Office y el 11% de los archivos PDF representaron el 33% de todo el malware recién identificado en 2020.

La tecnología RTDMI™, pendiente de patente, identificó un récord de 120,910 variantes de malware *«nunca antes vistas»* durante ese tiempo, un aumento del 63% con respecto a los primeros seis meses de 2019. *«Los ciberdelincuentes son demasiado sofisticados para usar variantes de malware conocidas, por lo que están reinventando y reescribiendo malware para derrotar los controles de seguridad como las técnicas tradicionales de sandboxing, y está*

funcionando», dijo Conner.

Los ataques que utilizan Puertos No Estándar están de regreso

Al día de hoy, un promedio del 23% de los ataques tuvieron lugar en puertos no estándar, la marca más alta desde que SonicWall comenzó a rastrear este vector de ataque en 2018.

Mediante el envío de malware a través de puertos no estándar, los asaltantes pueden eludir las tecnologías de firewall tradicionales, lo que garantiza un mayor éxito para las cargas útiles. Un puerto *«no estándar»* es aprovechado por los servicios que se ejecutan en un puerto distinto de su asignación predeterminada (por ejemplo, los puertos 80 y 443 son puertos estándar para el tráfico web).

En esta modalidad se establecieron dos nuevos récords mensuales durante los dos primeros trimestres de 2020. En febrero, los ataques a puertos no estándar alcanzaron el 26% antes de ascender a un 30% en mayo. Durante ese mes, hubo un aumento en muchos ataques específicos, como VBA Trojan Downloader, que pudieron haber contribuido al pico.

IoT continúa entregando amenazas

Los empleados que trabajan desde el hogar o las fuerzas de trabajo remotas pueden presentar muchos riesgos nuevos, incluidos los dispositivos de Internet de las cosas (IoT) como refrigeradores, cámaras para bebés, timbres o consolas de juegos. Los departamentos de TI están siendo asediados con innumerables dispositivos que infestan las redes y puntos finales a medida que la huella de sus empresas se expande más allá del perímetro tradicional.

Los investigadores de SonicWall encontraron un aumento del 50% en los ataques de malware IoT, un número que refleja el número de dispositivos adicionales que están conectados ya sea como individuos o como empresas que funcionan desde casa. Los dispositivos IoT sin

control pueden proporcionar a los ciberdelincuentes una puerta abierta, poniendo en riesgo lo que hasta ahora podría haber sido considerada una organización bien protegida.

Para descargar la actualización completa de mitad de año, visita: www.sonicwall.com/ThreatReport.