Retail, la segunda vertical más atacada por ransomware en 2021: Sophos

- *El año pasado el 77% de las organizaciones minoristas se vieron afectadas por ransomware, frente al 44% en 2020: un aumento del 75%.*

Ciudad de México, 13 de septiembre de 2022.- Sophos, líder mundial en ciberseguridad de última generación, publicó hoy un nuevo informe llamado **"El estado del ransomware en el comercio minorista 2022"**, que descubrió que el retail tuvo la segunda tasa más alta de ataques de ransomware el año pasado de entre todos los sectores encuestados, después de las empresas de medios de comunicación y la industria del entretenimiento.

A nivel mundial, el 77 % de las organizaciones minoristas encuestadas se vieron afectadas, un aumento del 75 % desde 2020. Esto también es un incremento de 11% en cuanto a la tasa promedio global del 66 %.

"Los minoristas continúan sufriendo una de las tasas más altas de ataques de ransomware de cualquier industria; tres de cada cuatro sufrieron un ataque en 2021. Según la experiencia de Sophos, las organizaciones que se defienden con éxito contra estos ataques no sólo usan esquemas de defensa en capas, sino que aumentan la seguridad con especialistas capacitados para monitorear el sistema y cazar activamente las amenazas que eluden el perímetro antes de que puedan convertirse en problemas aún mayores", dijo Chester Wisniewski, científico investigador principal de Sophos.

"La encuesta de este año muestra que solo el 28% de las organizaciones minoristas que fueron objetivo de ransomware pudieron evitar que sus datos se cifraran, lo que sugiere que una gran parte de la industria necesita mejorar su postura de seguridad con las herramientas adecuadas y expertos en seguridad debidamente capacitados para ayudar a administrar sus esfuerzos", añade.

A medida que aumentó el porcentaje de organizaciones minoristas atacadas por ransomware, también aumentó el pago promedio de rescate. En 2021, el pago de rescate promedio fue de USD $226,044, un aumento del 53 % en comparación con 2020 (USD $147,811). Sin embargo, esto representa apenas un tercio del promedio intersectorial (USD $812,000).

"*Es probable que diferentes grupos de amenazas están afectando a diferentes industrias. Algunos de los grupos de ransomware poco calificados piden entre USD $50,000 y uso $200,000 en pagos de rescate, mientras que los atacantes más grandes y sofisticados con mayor visibilidad exigen desde USD $1 millón de dólares en adelante"*, indica Wisniewski.

"Con Initial Access Brokers (IAB) y Ransomware-as-a-Service (RaaS), lamentablemente es fácil para los ciberdelincuentes de nivel inferior comprar acceso a la red y un kit de ransomware para lanzar un ataque sin mucho esfuerzo. Es más probable que las tiendas minoristas

individuales y las cadenas pequeñas sean el objetivo de estos atacantes oportunistas más pequeños", agrega el experto.

- Los hallazgos adicionales del estudio incluyen:

1. Si bien el sector minorista fue la segunda industria más atacada, el aumento percibido en el volumen y la complejidad de los ataques cibernéticos contra la industria estuvo muy ligeramente por debajo del promedio intersectorial (alrededor de 55% en ambos casos)

2. El 92% de las organizaciones minoristas afectadas por el ransomware dijeron que el ataque afectó su capacidad para operar y el 89% dijo que el ataque hizo que su organización perdiera ingresos.

3. En 2021, el costo total para las organizaciones minoristas para remediar un ataque de ransomware fue de USD $1.27 millones, por debajo de los USD $1.97 millones en 2020.

4. En comparación con 2020, la cantidad de datos recuperados después de pagar el rescate disminuyó (del 67% al 62%), al igual que el porcentaje de organizaciones minoristas que recuperaron todos sus datos (del 9% a tan solo 5%).

A la luz de los resultados de la encuesta, los expertos de Sophos recomiendan las siguientes prácticas para todas las organizaciones de todos los sectores:

- Instalar y mantener defensas de alta calidad en todos los puntos del entorno. Revisar los controles de seguridad regularmente y asegurarse de que continúen satisfaciendo las necesidades de la organización.

- Buscar amenazas de manera proactiva para identificar y detener a los adversarios antes de que puedan ejecutar ataques; si el equipo no tiene el tiempo o las habilidades para hacerlo internamente, se debe subcontratar a un equipo de Detección y respuesta administrada (MDR).

- Reforzar el entorno de TI buscando y cerrando brechas de seguridad clave: dispositivos sin parches, máquinas sin protección y puertos RDP abiertos, por ejemplo. Las soluciones de detección y respuesta extendidas (XDR) son ideales para este propósito.

- Prepararse para lo peor y tener un plan actualizado en lugar de un escenario de incidente del peor de los casos.

- Realizar copias de seguridad y practicar su restauración para garantizar una interrupción y un tiempo de recuperación mínimos.

Para obtener más información sobre el estado del ransomware en Retail 2022, consulte el informe completo de Sophos.com.

La encuesta State of Ransomware in Retail 2022 encuestó a 5600 profesionales de TI en organizaciones medianas en 31 países, incluidos 422 encuestados del sector minorista.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/