Sophos lanza servicio para identificar y neutralizar ciberataques activos: Sophos Rapid Response

- *La respuesta a incidentes minimiza el daño de los ataques y reduce el tiempo de recuperación*

CIUDAD DE MÉXICO. 28 de octubre de 2020.- Sophos, la empresa líder en ciberseguridad de última generación, anunció el lanzamiento de Sophos Rapid Response, un servicio remoto de tarifa fija que identifica y neutraliza los ataques de ciberseguridad activos durante el tiempo de contratación de 45 días. Sophos Rapid Response proporciona a la empresa que lo contrata un equipo de ciberseguridad dedicado, 24 horas los 7 días de la semana, para responder ante incidentes, cazar amenazas y analizar las vulnerabilidades de la firma para detener rápidamente ataques, minimizando los costos y reduciendo el tiempo de recuperación para la víctima.

Sophos Rapid Response ha identificado el creciente uso del *dropper* (troyano utilizado para instalar malware) Buer para propagar ransomware. En la investigación llamada *'Hacks for Sale: Inside Buer Loader's Malware-as-a-Service'* elaborada por Sophos Rapid Response y SophosLabs, se detalla cómo Buer compromete las PC con sistema operativo Windows y permite a los atacantes propagar su carga útil. Sophos descubrió esto mientras mitigaba un reciente ataque de ransomware Ryuk, mismo que ha sido notablemente utilizado en los últimos meses y que hace uso de nuevas herramientas, técnicas y procedimientos.

"*Cuando eres víctima de la ciberdelincuencia, el tiempo es esencial. Cada minuto entre el momento en el que eres atacado y la neutralización del incidente cuenta, ya que a medida que las horas pasan, los atacantes tienen más oportunidades de comprometer a tus equipos y tu información*", dijo Joe Levy, CTO de Sophos. "*Los ataques avanzados pueden detener rápidamente las operaciones comerciales de una empresa y los gerentes de sistemas que han experimentado el ransomware de primera mano lo saben y conocen la necesidad de dedicar más tiempo en la respuesta a incidentes y a la prevención de amenazas. Sophos Rapid Response detecta e interrumpe aquellos ataques activos ayudando a las empresas a volver a sus operaciones lo más rápido posible*", añadió.

Las capacidades de Sophos Rapid Response abarcan una amplia gama de incidentes, incluidos distintos tipos de ransomware, ataques de red, entre otros. El equipo de Sophos Rapid Response se puede integrar y empezar a trabajar en cuestión de horas, y la mayoría de los ataques se pueden evaluar en 48 horas.

"*Este año los ataques ransomware se han convertido en una 'mina de oro' para los delincuentes, lo que pone a las empresas de ciberseguridad ante un escenario nunca antes visto. Casi el 85% de los ataques en los que Sophos Rapid Response ha actuado han sido de ransomware, incluyendo Ryuk, REvil y Maze, y puedo decir con confianza que del resto de los ataques que logramos detener, la mayoría habrían resultado también en ransomware si no*

hubiéramos actuado tan rápido", dijo Peter Mackenzie, gerente de Respuesta a Incidentes de Sophos. "*Los criminales están utilizando herramientas que les brindan fácil acceso a los equipos y les permiten obtener altas cantidades de dinero en cuestión de semanas, cifras que muchas otras personas difícilmente conseguirían en toda su vida. Se infiltran en las redes y se mueven sigilosamente antes de lanzar el ransomware, a menudo aprovechando las noches o momentos en los que no hay un monitoreo tan minucioso, para propagar el virus en la mayor cantidad de equipos posible. Sophos Rapid Response toma medidas inmediatas para 'extinguir el incendio', que en casos como el que recientemente atendimos en un hospital atacado por Ryuk significó la diferencia entre la vida y la muerte"*.

Sophos Rapid Response forma parte de Sophos Managed Threat Response (MTR), un equipo global que proporciona servicios de búsqueda, detección y respuesta proactiva de amenazas. Como uno de los servicios de detección y respuesta administrado (MDR) más utilizados en la industria, con más de 1400 clientes, Sophos MTR se distingue por su capacidad para actuar proactivamente y mitigar las amenazas en tiempo real.

Una vez que Sophos Rapid Response neutraliza el ataque, se cambia a un programa de respuesta rápida que emplea un monitoreo continuo de investigación, detección y respuesta inmediata las 24 horas del día hecho por el equipo de Sophos MTR. Un informe de investigación de amenazas detalla los descubrimientos realizados, las acciones tomadas y otras recomendaciones de corrección, lo que ayuda a las organizaciones a comprender el origen del ataque, así como qué activos se vieron comprometidos y los datos a los que se accedió y se extrajeron.

Sophos Rapid Response ya está disponible tanto para los clientes actuales como para los que aún no han contratado producto alguno de Sophos. A diferencia de otros servicios que requieren implementaciones complejas, Sophos Rapid Response ofrece asistencia remota con un modelo de precio fijo, según la cantidad de usuarios y servidores que tenga la organización. También está estructurado para dar protección a empresas de todos los tamaños, incluidas organizaciones pequeñas que no han sido capaces de aprovechar este tipo de servicios ya que su infraestructura y finanzas no se los permitían anteriormente.

¿Qué dicen los socios de canal sobre Sophos Rapid Response?

"*Los ciberataques están evolucionando y son cada vez más sofisticados. Como hemos visto este año, nadie está exento de sufrirlos. Las organizaciones deben prepararse ya que más del 85% de los profesionales en ciberseguridad, encuestados por IDC, indican que han experimentado al menos un incidente que implicó el gasto de recursos adicionales a los que se tenían presupuestados*", dijo Frank Dickson, vicepresidente de Programas de IDC. "Sophos *Rapid Response es un servicio que nadie busca hasta que lo necesita. Las organizaciones, lamentablemente, no están preparadas para combatir un ataque activo y necesitan responder de forma rápida y más agresiva de lo que lo harían si utilizaran únicamente sus recursos. Con*

tarifas fijas y la capacidad de activación el mismo día, Sophos Rapid Response brinda certeza cuando los clientes más lo requieren", agregó.

"*Una organización benéfica que ofrece alojamiento y servicios de apoyo a miles de adultos vulnerables fue atacada por ransomware, lo que detuvo las operaciones en sus más de 40 instalaciones. La organización nos llamó en busca de ayuda y de inmediato utilizamos Sophos Rapid Response"*, cuenta Steve Weeks, presidente de Netcetera. "*En clientes de Netcetera que ya ejecutan las suites de seguridad de última generación de Sophos no hemos visto incidentes de ransomware desde hace varios años. Cuando recibimos una llamada de ayuda de clientes nuevos, confiaremos en Sophos Rapid Response por la capacidad de la solución para sacar a las organizaciones de la zona de peligro"*, añadió.

"Sophos Rapid Response complementa perfectamente nuestros servicios de respuesta a incidentes internos existentes, nos ayuda a realizar planes de respuesta proactivos y brinda apoyo inmediato en el peor de los escenarios. No solo estamos vendiendo una solución, sino que estamos arreglando problemas a largo plazo para evitar que vuelvan a ocurrir", consideró Jeremy Weiss, líder de ciberseguridad en CDW. "*He visto de primera mano cómo el equipo de Sophos Rapid Response puede reducir el tiempo dedicado a neutralizar un ataque en cuestión de horas, y los comentarios al respecto han sido siempre excepcionales*", señaló.

# # #

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de

Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

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