Crónica de un combate ‘mano a mano’ entre Sophos MTR y REvil por 2.5 millones de dólares

CIUDAD DE MÉXICO. 1 de julio de 2021.- Hace algunas semanas, una empresa del sector de la comunicación se vio enfrascada en un combate, en tiempo real, con ciberdelincuentes de REvil, decididos a pedir un rescate millonario por la información robada. El ataque falló, pero la compañía afectada aún no se recupera por completo.

Todo comenzó a principios de junio de 2021 cuando fue detectada en la red de la empresa una intrusión mediante Cobalt Strike, un agente de acceso remoto utilizado como precursor de una gran cantidad de ciberataques. Horas más tarde, alrededor de las 04:00 AM, los ciberdelincuentes lanzaron el *ransomware* y comenzó un combate de cerca de 4 horas entre el equipo de TI del objetivo y Sophos Managed Threat Response (MTR) contra los adversarios que orquestaron el ataque.

Pese a que el ataque falló, los atacantes ya habían conseguido encriptar una serie de datos sensibles de dispositivos desprotegidos, además de que eliminaron las copias de seguridad en línea de dicha información. El rescate exigido era de $2.5 millones y estaba firmado por REvil, también conocido como Sodonikibi.

Se trata de un *ransomware* como servicio (RaaS) al cual los cibercriminales pueden ‘suscribirse’ para propagar un ataque con sus propios recursos. El objetivo en esta ocasión se vio seriamente afectado por la pandemia: al tener que enviar a sus empleados repentinamente a trabajar de forma remota en 2020, no todos los equipos tenían el mismo nivel de protección y fue así como los agentes maliciosos no solo se infiltraron a la red, sino que se movían de dispositivo a dispositivo sin obstáculos.

“*Con la pandemia no es inusual encontrar aplicaciones de acceso remoto instaladas en los dispositivos de los empleados. Fue por eso que cuando vimos Screen Connect en 130 endpoints, pensamos que la empresa los había instalado para que sus empleados trabajaran remotamente. Resultó que la empresa no sabía nada al respecto: los atacantes habían instalado el software para garantizar que pudieran mantener el acceso a la red y los dispositivos comprometidos*”, explica **Paul Jacobs, líder de respuesta a incidentes de Sophos**.

- **El combate**

El equipo de MTR utilizó una función de comportamiento llamada Cryptoguard que se encarga de detectar y bloquear los intentos de cifrado de archivos de toda la red, incluso de aquellos dispositivos remotos desprotegidos. Fue entonces cuando los atacantes supieron que habían sido detectados y comenzaron a intentar de forma repetida violar nuevos equipos con un nivel de protección más alto cifrar nuevos archivos, lanzando ataques desde los *endpoints* que ya tenían en su poder.

Cuando MTR bloqueaba un intento de ataque, el siguiente ya estaba en marcha, lo que desencadenó una batalla sin tregua que culminó cuando estos intentos de cifrado de archivos, al ser fallidos, disminuyeron. Para el amanecer, aún se detectaban algunos intentos intermitentes sin éxito, lo que dejó en claro que el ataque principal había fallado.

La empresa encontró que el daño se había limitado a los dispositivos comprometidos y el dominio de la compañía tuvo que ser reconstruido, además de que las copias de seguridad en línea se habían eliminado. Si bien la empresa no quedó totalmente paralizada y no tuvo que pagar el exorbitante rescate, el regreso al 100% de sus operaciones ha sido lento y aún continúa en curso, al día de la publicación de este texto.

- **Lecciones y recomendaciones**

Este caso nos enseña que cuando las empresas acuden a MTR, el ataque ya tuvo lugar. En esta ocasión, Sophos estuvo ahí para contener a los ciberdelincuentes en la etapa final de la vulneración, por lo que la lección principal es que las empresas deben realizar constantes cambios en su entorno y contar con soluciones proactivas de detección de amenazas para una gestión de riesgos más avanzada.

El segundo aprendizaje radica en la conservación de los datos. Las firmas deben asegurarse de contar con copias de seguridad *offline* y hacer un inventario de sus activos, cuentas y datos sensibles para evitar que los dispositivos desprotegidos y sin parches aumenten el riesgo de crear una situación de peligro.

###

Sobre Sophos

Sophos es la empresa líder mundial en ciberseguridad de última generación, que 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 para la detección 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, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de gestión integral basada en la nube llamada Sophos Central, el eje 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 distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/

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