¿Qué es el *ransomware* Conti y cómo protegerse?

- ***Se trata de un tipo de* ransomware *de 'doble extorsión' operado por humanos, que se ha presentado sobre todo en Estados Unidos y que ya llegó a México.***

CIUDAD DE MÉXICO. 17 de febrero de 2021.- Los ataques cibernéticos operados por humanos representan una amenaza cada vez más grande para las organizaciones alrededor del mundo, comprometiendo información sensible e infiltrándose en las redes de las empresas.

Un ejemplo de ello es **Conti,** un *ransomware* que logra infiltrarse en las redes y obtener acceso a credenciales de administrador en apenas 16 minutos posteriores a la vulneración de un *firewall.* De acuerdo con Sophos, se trata de una acción de "doble extorsión", realizada por humanos, que roba información sensible y amenaza con cifrarla y exponerla a cambio de un rescate.

Peter Mackenzie, gerente general de Sophos Rapid Response, explica que se le denomina de 'doble extorsión' porque **los atacantes obtienen acceso de forma simultánea a dos servidores** para que los equipos de ciberseguridad, al detectar el ataque, deshabiliten únicamente uno de ellos, creyendo que detuvieron la amenaza a tiempo.

En ese momento, los cibercriminales únicamente cambian de servidor y continúan su propagación, en una especie de 'Plan B'. *"Este es un enfoque común en los ataques dirigidos por humanos y un recordatorio de que detectar únicamente una actividad sospechosa en la red no significa que el ataque haya terminado"*, explica.

Conti llega a México

Este tipo de *ransomware* se ha presentado, sobre todo, en Estados Unidos, **pero ya tuvo presencia en México**: de acuerdo con el sitio Conti News, desde 2020 y hasta la fecha se han presentado cerca de 180 casos de Conti a nivel global. Del total, **EE.UU., con 128 ataques, es el país con mayor incidencia**, seguido de Canadá con 14 y Reino Unido con 11 empresas vulneradas. **En nuestro país, hay solo un caso registrado, siendo el único país latinoamericano en el que se ha presentado.**

Una investigación de Sophos revela que los atacantes suelen obstruir el análisis del personal de TI de las empresas mediante **la implementación de balizas Cobalt Strike legítimas en los equipos comprometidos,** para posteriormente cargar el código durante el ataque, sin dejar huellas, esto para que los equipos de defensa no lo encuentren y/o examinen.

Posteriormente, en el caso estudiado, la empresa no tuvo más remedio que cerrar las operaciones. El equipo de Sophos Rapid Response, luego de que la víctima se puso en

contacto, neutralizó el ataque en 45 minutos y la firma pudo recuperar, en un día, la información afectada y reanudar sus operaciones.

"*Este es un ataque muy rápido y potencialmente devastador*", indica Peter Mackenzie. "*Descubrimos que los atacantes lograron comprometer la red del objetivo y obtener acceso a las credenciales de administrador del dominio* ***dentro de los 16 minutos posteriores a la vulneración de una*** **firewall** *y, en cuestión de horas, despliegan la columna vertebral del ataque de* ransomware*"*.

¿Qué hacer ante Conti?

Los primeros pasos a seguir que recomienda Sophos ante este tipo de amenazas son:

- Cerrar el protocolo de escritorio remoto (RDP) orientado para denegar el acceso de los ciberdelincuentes a las redes.
- Si se necesita acceso al RDP, hacerlo mediante una conexión VPN
- Utilizar seguridad en capas para prevenir, proteger y detectar ciberataques, incluidas las capacidades de detección y respuesta de *endpoints* (EDR) y equipos de respuesta administrados, como Sophos Rapid Response, que vigilan las redes las 24/7.
- Disponer de un plan de respuesta a incidentes eficaz y actualizarlo según sea necesario. Si no hay seguridad de que se tengan las habilidades o los recursos al interior de la organización para monitorear amenazas o responder a incidentes, considerar recurrir a especialistas.

La evolución constante de amenazas cibernéticas y el trabajo humano detrás de ellas vuelve cada vez más compleja la labor de defenderse para las organizaciones, razones por las que es indispensable contar con un aliado estratégico en ciberseguridad de última generación.

El robo y/o la vulnerabilidad de la información podría generar un impacto negativo en las operaciones y altos costos económicos para las compañías.

###

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/