¿Qué es el ransomware Maze y cómo se ejecuta?

CIUDAD DE MÉXICO. 22 de septiembre de 2020.- El cifrado de datos, combinado con el robo de información, es una de las tácticas más comunes utilizadas por los ciberdelincuentes en la actualidad. Uno de los primeros ransomware en ejecutar esa forma de secuestro de datos fue Maze, que desde 2019 ha sido una de los más activos.

¿Y cómo se desarrolla ese ataque? Las últimas investigaciones de Sophos indican que los atacantes se inmiscuyen en la red de sus víctimas al menos seis días antes de su primer intento de lanzar la carga útil o *payload*, que es el conjunto de datos mediante el cual se transmite el ransomware. Durante este tiempo, los delincuentes exploran la red, ejecutan herramientas legítimas de terceros, establecen conexiones y extraen datos a un servicio de almacenamiento en la nube preparándose así para el lanzamiento del componente malicioso.

Pero lo que han encontrado los criminales cibernéticos es que las víctimas no suelen pagar por el rescate que exigen en un primer intento y que, posterior a ello, suelen ser rápidamente detectados por las soluciones de ciberseguridad. Es por eso que los atacantes están utilizando una versión reconfigurada de la técnica Ragnar Locker. Este método consiste en instalar en el sistema un archivo en formato .msi que contiene un instalador para las versiones de 32 y 64 bits de VirtualBox 3.0.4, la cual fue lanzada en 2009. De esa forma, el sistema no detecta archivo malicioso alguno, ya que VirtualBox es una aplicación legítima.

Dentro de VirtualBox, el ciberdelincuente genera una 'máquina virtual' basada en una versión anterior del sistema operativo de la máquina, en la que distribuye la carga útil del cifrado de archivos de ransomware.

Lo anterior se hace con el fin de extraer la información que quieren robar mientras que las soluciones de ciberseguridad locales no son capaces de detectar ese proceso, ya que se está ejecutando en la máquina virtual y sobre un sistema operativo antiguo.

Comúnmente la técnica Ragnar Locker genera una máquina virtual con Windows XP, pero en este caso Sophos detectó que los atacantes utilizaron una máquina virtual que ejecutaba Windows 7, por lo que fueron inmediatamente reconocidos y bloqueados.

"*La cadena de ataque descubierta por Sophos destaca la agilidad de los atacantes humanos y su capacidad para sustituir y reconfigurar herramientas rápidamente al verse descubiertos*", dijo Peter Mackenzie, gerente de respuesta a incidentes de Sophos. "*El uso de una técnica de máquina virtual de Ragnar Locker podría reflejar una creciente frustración por parte de los atacantes después de que fallaron sus primeros intentos de cifrar datos*".

Sophos recomienda que para prevenir ciberataques, en particular ransomware, los equipos de seguridad de TI deben actualizar sus sistemas de seguridad en capas basados en la nube, incluida la tecnología anti-ransomware.

Para conocer más sobre este ransomware y saber cómo proteger a tu organización de este tipo de amenazas, consulta la investigación *Atacantes de Maze adoptan la técnica de máquina virtual de Ragnar Locker* de Sophos. El informe detalla cómo los atacantes probaron tres formas diferentes de ejecutar el ransomware Maze durante un solo ataque y exigieron un rescate de 15 millones de dólares.

###

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/