Cifrado intermitente: la nueva técnica que los cibercriminales utilizan para evadir la seguridad

CIUDAD DE MÉXICO. 1 de septiembre de 2021.- Sophos, líder mundial en ciberseguridad de última generación, reveló en una reciente investigación la forma en que los operadores detrás del *ransomware* LockFile cifran los archivos vulnerados en paquetes de 16 bytes, para evadir la detección de amenazas.

Los investigadores de Sophos llamaron a este novedoso enfoque **"cifrado intermitente"**, ya que ayuda al *ransomware* a evitar que se activen las señal de alerta en los equipos de ciberseguridad, esto ya que los archivos cifrados se ve estadísticamente muy similares a su original. Esta es la primera vez que los investigadores de Sophos han visto este enfoque utilizado en *ransomware.*

"*Los operadores de ransomware utilizan generalmente el cifrado parcial para acelerar el proceso de cifrado y hemos visto que BlackMatter, DarkSide y LockBit 2.0 implementan esta técnica",* dijo Mark Loman, director de ingeniería de Sophos. *"Lo que distingue a LockFile es que, a diferencia de los demás, no cifra los primeros bloques. En cambio, cifra los 16 bytes restantes de un documento. Esto significa que un archivo, como un documento de texto, permanece parcialmente legible y se parece estadísticamente al original. Este truco puede tener éxito contra el software de detección de ransomware que se basa en inspeccionar el contenido mediante análisis estadístico para detectar el cifrado*", explica.

El especialista señala que los operadores detrás de LockFile se han mostrado muy ansiosos por utilizar este enfoque para aprovechar las vulnerabilidades recientemente dadas a conocer, como los errores ProxyShell. El mensaje desde Sophos para los defensores es que el panorama de las amenazas cibernéticas nunca se detiene y los adversarios aprovecharán rápidamente todas las oportunidades o herramientas posibles para lanzar un ataque.

Otro hallazgo clave de Sophos es que el ransomware LockFile utiliza un proceso relativamente poco común conocido como "entrada/salida (E/S) mapeada en memoria". Esta técnica permite que el *ransomware* cifre de forma invisible los documentos y los almacena en caché de la memoria de la computadora, sin crear tráfico detectable para las soluciones de ciberseguridad Esta técnica también ha sido utilizada por WastedLocker y Maze

A diferencia de otras amenazas dirigidas por humanos, LockFile no necesita conectarse a un centro de comando y control para comunicarse. Esto le ayuda a mantener la actividad de ataque bajo el radar de detección durante el mayor tiempo posible. Una vez que ha cifrado todos los documentos en la máquina, se borra. Esto significa que, después del ataque, no hay un código binario de *ransomware* que el software de protección de *endpoints* pueda encontrar o limpiar. Adicionalmente, LockFile evita encriptar cerca de 800 archivos diferentes por extensión, lo que vuelve más confuso el trabajo para los equipos de ciberseguridad.

- **¿Qué hacer ante LockFile?**

Sophos recomienda, primero, implementar la protección en capas. Dado que más ataques de *ransomware* también implican extorsión, se debe utilizar la protección en capas para bloquear a los atacantes en tantos puntos como sea posible. También se recomienda combinar el trabajo de expertos humanos y tecnología anti-*ransomware* ya que la tecnología proporciona la escala y la automatización que necesita una estrategia de defensa, mientras que los expertos humanos son los más capaces de detectar las tácticas, técnicas y procedimientos reveladores que indican que un atacante está intentando ingresar al entorno.

Las empresas deben asegurarse de que las herramientas, los procesos y el personal adecuados estén disponibles para supervisar, investigar y responder a las amenazas observadas en el entorno. Los atacantes de ransomware a menudo programan su ataque durante las horas de menor actividad, los fines de semana o durante las vacaciones, asumiendo que poco o ningún personal está mirando.

Se deben establecer contraseñas seguras que sirven como una de las primeras líneas de defensa. También se debe utilizar la autenticación multifactor (MFA), ya que incluso las contraseñas seguras pueden verse comprometidas. Cualquier forma de autenticación multifactor es mejor para asegurar el acceso a recursos críticos como correo electrónico, herramientas de administración remota y activos de red.

Las compañías deben realizar constantes escaneos de su red desde el exterior e identificar los puertos comúnmente utilizados, como las herramientas de acceso remoto. Si una máquina necesita volverse accesible mediante una herramienta de administración remota, esa herramienta debe ser colocada detrás de una VPN o una otra solución segura. También es fundamental que se generen copias de seguridad sin conexión de información y mantenerlas actualizadas.

Hacer un inventario de los activos y cuentas es importante ya que los dispositivos sin parches en la red aumentan el riesgo y crean una situación en la que las actividades maliciosas podrían pasar desapercibidas. Es vital tener un inventario actualizado de todas las computadoras y dispositivos IOT conectados. Utilizar exploraciones de red y comprobaciones físicas para localizarlos y catalogarlos se vuelve crucial. Finalmente se debe mantener todo con los parches actualizados y verificar dos veces que esas protecciones se hayan instalado correctamente.

###

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/

SOPHOS