Una nueva familia de ransomware que surgió el mes pasado cuenta con su propia bolsa de trucos para evitar la protección de ransomware al aprovechar una técnica novedosa llamada *«cifrado intermitente».*

Los operadores del ransomware denominado como LockFile, explotan las fallas recientemente reveladas ProxyShell y PetitPotam, para comprometer los servidores de Windows e implementar malware de cifrado de archivos que codifica solo cada 16 bytes alternativos de un archivo, lo que le da la capacidad de evadir las defensas del ransomware.

> *«Los operadores de ransomware por lo general utilizan el cifrado parcial para acelerar el proceso de cifrado y lo hemos visto implementado por el ransomware BlackMatter, DarkSide y LockBit 2.0. Lo que distingue a LockFile es que, a diferencia de los demás, no cifra los primeros bloques. En cambio, LockFile cifra cada 16 bytes restantes de un documento»,* dijo Mark Loman, director de ingeniería de Sophos.
>
> *«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 protección contra ransomware que se basa en inspeccionar el contenido mediante análisis estadístico para detectar el cifrado»,* agregó.

El análisis de Sophos sobre LockFile proviene de un artefacto que se cargó a VirusTotal el 22 de agosto de 2021.

Una vez depositado, el malware también toma medidas para terminar los procesos críticos asociados con el software de virtualización y las bases de datos a través de la Interfaz de Administración de Windows (WMI), antes de proceder a cifrar los archivos y objetos críticos, y mostrar una nota de ransomware que tiene similitudes estilísticas con la de BitLock 2.0.

La nota de rescate también insta a la víctima a ponerse en contacto con una dirección de

correo electrónico específica «contact@contipauper.com», que Sophos sospecha podría ser una referencia despectiva a un grupo de ransomware competidor llamado Conti.

Además, el ransomware se borra del sistema después del cifrado exitoso de todos los documentos en la máquina, lo que significa que *«no hay binario de ransomware para que los respondedores de incidentes o el software antivirus lo encuentren o limpien».*

> *«El mensaje aquí 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 exitoso»*, dijo Loman.

La divulgación se produce cuando la Oficina Federal de Investigaciones (FBI) de Estados Unidos publicó un informe Flash que detalla las tácticas de un nuevo equipo de Ransomware-as-a-Service (RaaS) conocido como Hive, que consta de varios actores que utilizan múltiples mecanismos para comprometer redes comerciales, exfiltrar datos y cifrar datos en las redes, e intentar cobrar un rescate a cambio de acceso al software de descifrado.