Los actores maliciosos están actualmente intentando explotar una vulnerabilidad de seguridad en Veeam Backup & Replication que ya ha sido corregida, con el fin de desplegar los ransomware Akira y Fog.

La empresa de ciberseguridad Sophos ha informado que ha estado monitoreando una serie de ataques en el último mes que se aprovechan de credenciales VPN comprometidas y de la vulnerabilidad CVE-2024-40711 para crear una cuenta local y lanzar el ransomware.

La vulnerabilidad CVE-2024-40711, con una calificación de 9.8 sobre 10 en la escala CVSS, es una falla crítica que permite la ejecución remota de código sin necesidad de autenticación. Veeam abordó este problema en la versión 12.2 de Backup & Replication a principios de septiembre de 2024.

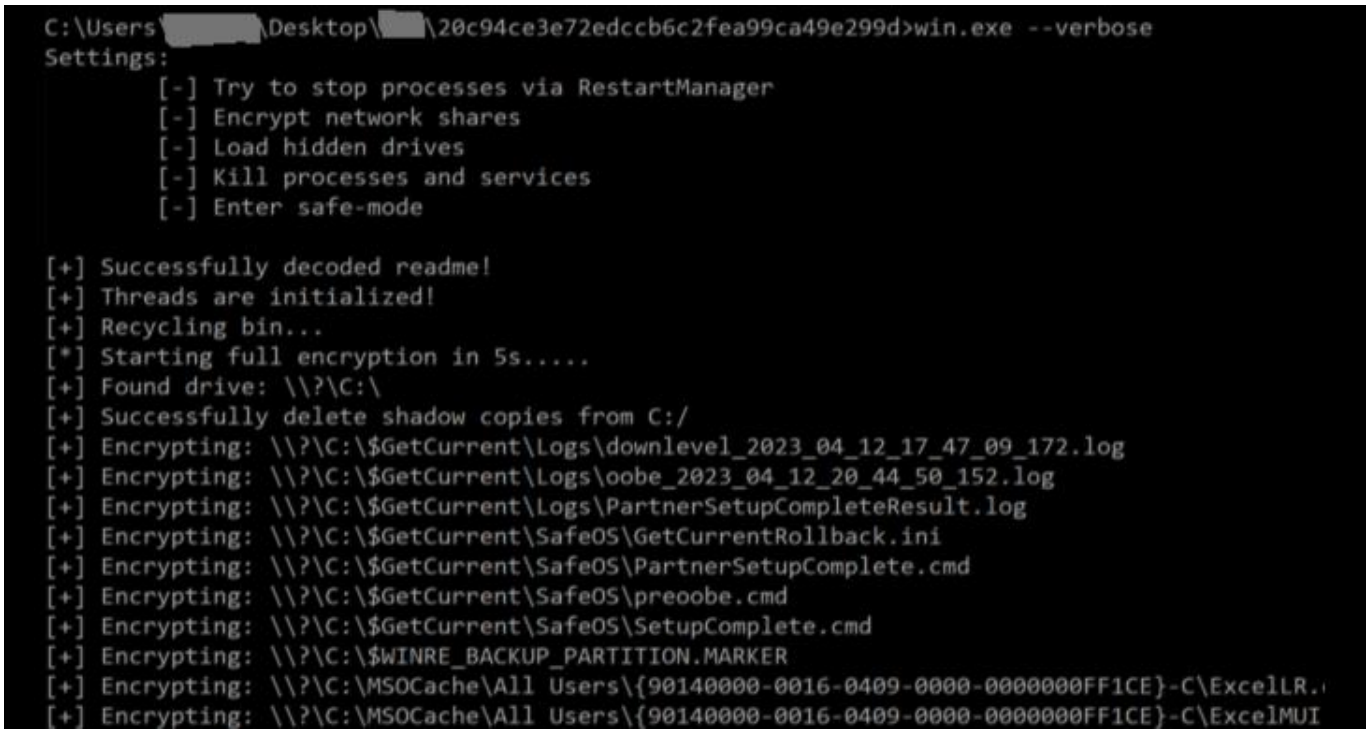
El investigador de seguridad Florian Hauser, de la empresa CODE WHITE, con sede en Alemania, ha sido reconocido por identificar y reportar estas deficiencias de seguridad.

> *«En cada caso, los atacantes accedieron a los sistemas objetivo usando gateways VPN comprometidos que no tenían habilitada la autenticación multifactor. Algunas de estas VPN estaban ejecutando versiones de software que ya no contaban con soporte»*, explicó Sophos.
>
> *«Cada vez, los atacantes explotaron VEEAM a través del URI /trigger en el puerto 8000, activando el archivo Veeam.Backup.MountService.exe para ejecutar net.exe. El exploit crea una cuenta local llamada 'point', la cual se agrega a los grupos de Administradores locales y Usuarios de Escritorio Remoto.»*

En el ataque que resultó en el despliegue del ransomware Fog, los actores maliciosos supuestamente depositaron el ransomware en un servidor Hyper-V no protegido, utilizando la herramienta rclone para exfiltrar datos. Otros intentos de desplegar ransomware no tuvieron éxito.

La explotación activa de la CVE-2024-40711 ha llevado al NHS de Inglaterra a emitir una advertencia, señalando que *«las aplicaciones empresariales de respaldo y recuperación ante desastres son objetivos atractivos para los grupos de amenazas cibernéticas.»*

Este informe coincide con una publicación de Unit 42 de Palo Alto Networks que describe un sucesor del ransomware INC llamado Lynx, que ha estado operando desde julio de 2024 y ha atacado a organizaciones en los sectores de comercio, bienes raíces, arquitectura, servicios financieros y ambientales en EE. UU. y el Reino Unido.



Se cree que el surgimiento de Lynx fue impulsado por la venta del código fuente del ransomware INC en el mercado clandestino criminal en marzo de 2024, lo que permitió a los creadores de malware reempaquetar el ransomware y generar nuevas variantes.

> *«El ransomware Lynx comparte una parte importante de su código con el*

> *ransomware INC. INC surgió en agosto de 2023 y tenía versiones compatibles tanto con Windows como con Linux»,* indicó Unit 42.

Además, el Centro de Coordinación de Ciberseguridad del Sector Salud (HC3) del Departamento de Salud y Servicios Humanos (HHS) de EE. UU. ha advertido que al menos una organización de salud en el país ha sido atacada por el ransomware Trinity, un actor relativamente nuevo en este campo que apareció por primera vez en mayo de 2024 y que se cree es una nueva versión de los ransomware 2023Lock y Venus.

> *«Es un tipo de software malicioso que penetra en los sistemas a través de diferentes vectores de ataque, como correos electrónicos de phishing, sitios web maliciosos y la explotación de vulnerabilidades de software. Una vez dentro, el ransomware Trinity utiliza una estrategia de doble extorsión para presionar a sus víctimas»,* explicó el HC3.

También se han detectado ataques cibernéticos que distribuyen una variante del ransomware MedusaLocker llamada BabyLockerKZ, lanzada por un actor malicioso con motivaciones financieras que ha estado activo desde octubre de 2022, principalmente atacando a objetivos en países de la UE y América del Sur.

> *«Este atacante utiliza varias herramientas públicas conocidas y binarios de tipo 'living-off-the-land' (LoLBins), que son un conjunto de herramientas creadas por el mismo desarrollador (posiblemente el atacante) para facilitar el robo de credenciales y el movimiento lateral en organizaciones comprometidas,»* explicaron los investigadores de Talos.
>
> *«Estas herramientas son principalmente envoltorios de herramientas públicas que incluyen funcionalidades adicionales para agilizar el proceso de ataque y*

> *proporcionar interfaces gráficas o de línea de comandos.»*