Investigadores de seguridad cibernética descubrieron más vínculos entre las familias de ransomware BlackCat (también conocido como AlphaV) y BlackMatter, la primera de las cuales surgió como reemplazo tras el escrutinio internacional el año pasado.

> *«Al menos algunos miembros del nuevo grupo BlackCat tienen vínculos con el grupo BlackMatter, porque modificaron y reutilizaron una herramienta de exfiltración personalizada y que solo se ha observado en la actividad de BlackMatter»*, dijeron los investigadores de Kaspersky.

La herramienta, denominada Fendr, no solo se actualizó para incluir más tipos de archivos, sino que también el grupo la utilizó ampliamente para robar datos de redes corporativas en diciembre de 2021 y enero de 2022 antes del cifrado, en una táctica popular llamada doble extorsión.

Los hallazgos llegan menos de un mes después de que los investigadores de Cisco Talos identificaran superposiciones en las tácticas, técnicas y procedimientos (TTP) entre BlackCat y BlackMatter, describiendo la nueva variante de ransomware como un caso de *«expansión comercial vertical»*.

BlackCat se destaca por dos razones: es un actor afiliado que implementó BlackMatter en el pasado y su malware está escrito en Rust, lo que indica cómo los atacantes están cambiando cada vez más a los lenguajes de programación con capacidades de compilación cruzada.

> *«El grupo proporciona infraestructura, muestras de malware, negociaciones de rescate y probablemente retiros de efectivo. Cualquier que ya tenga acceso a entornos comprometidos puede usar las muestras de BlackCat para infectar un objetivo»,* dijeron los investigadores.

Una vez que se ejecuta, el malware obtiene el MachineGuid del sistema Windows del registro,

una clave única generada durante la instalación del sistema operativo, así como su UUID, antes de pasar por alto el Control de Cuentas de Usuario (UAC), eliminar las copias de seguridad instantáneas e iniciar el proceso de cifrado.

> *«Este uso de un Fendr modificado, también conocido como ExMatter, representa un nuevo punto de datos que conecta a BlackCat con la actividad pasada de BlackMatter»,* dijeron los investigadores.

> *«La modificación de esta herramienta reutilizada demuestra un régimen de planificación y desarrollo más sofisticado para adaptar los requisitos a los entornos objetivo, característico de una empresa criminal madura»,* agregaron.