El equipo de ransomware BlackCat fue visto ajustando su arsenal de malware para pasar desapercibido y expandir su alcance.

> *«Entre algunos de los desarrollos más notables se encuentra el uso de una nueva versión de la herramienta de exfiltración de datos Exmatter y el uso de Eamfo, un malware que roba información y está diseñado para robar las credenciales almacenadas por el software de copia de seguridad de Veeam»,* dijeron los investigadores de Symantec.

BlackCat, también conocido como ALPHV y Norberus, se atribuye a un adversario rastreado como Coreid (también conocido como FIN7, Carbanak o Carbon Spider) y se dice que que es un sucesor renombrado de DarkSide y BlackMatter, los cuales fueron responsables de una serie de ataques de alto perfil, incluido el de Colinal Pipeline.

Se sabe que el atacante, al igual que otros grupos de ransomware notorios, ejecuta una operación de ransomware como servicio (RaaS), que involucra a sus desarrolladores principales que solicitan ayuda de afiliados para realizar los ataques a cambio de una parte del producto ilícito.

ALPHV es también una de las primeras cepas de ransomware que se programan en Rust, una tendencia que desde entonces ha sido adoptada por otra familias como Hive y Luna en los últimos meses para desarrollar y distribuir malware multiplataforma.

La evolución de las tácticas, herramientas y procedimientos (TTP) del grupo se produce más de tres meses después de que se descubriera que la banda de ciberdelincuentes explotaba servidores de Microsoft Exchange sin parches como conducto para implementar ransomware.

Las actualizaciones posteriores de su conjunto de herramientas incorporan nuevas funcionalidades de encriptación que permiten que el malware reinicie las máquinas Windows comprometidas en modo seguro para eludir las protecciones de seguridad.

> *«En una actualización de julio de 2022, el equipo agregó la indexación de datos robados, lo que significa que sus sitios web de fugas de datos se pueden buscar por palabra clave, tipo de archivo y más»,* dijeron los investigadores.

Las últimas mejoras se refieren a Exmatter, una herramienta de exfiltración de datos usada por BlackCat en sus ataques de ransomware. Además de recopilar archivos solo con un conjunto específico de extensiones, la versión renovada genera un informe de todos los archivos procesados procesados e incluso los corrompe.

En el ataque también se implementó un malware de robo de información llamado Eamfo, que está diseñado para desviar las credenciales almacenadas en el software de respaldo de Veeam y facilitar la escalada de privilegios y el movimiento lateral.

Los hallazgos son otra indicación de que los grupos de ransomware son expertos en adaptar y refinar continuamente sus operaciones para seguir siendo efectivos el mayor tiempo posible.

> *«Su desarrollo continuo también subraya el enfoque del grupo en el robo y la extorsión de datos, y la importancia de este elemento de ataques para los actores de ransomware ahora»,* dijeron los investigadores.

También se ha observado recientemente que BlackCat usa el malware Emotet como vector de infección inicial, sin mencionar la presencia de una afluencia de nuevos miembros del ahora desaparecido grupo de ransomware Conti, luego de la retirada de este último del panorama de amenazas este año.

La extinción de Conti también estuvo acompañada por el surgimiento de una nueva familia de ransomware denominada Monti, un grupo *«doppelganger»* que se ha encontrado haciéndose pasar deliberada y descaradamente por los TTP del equipo de Conti y sus herramientas.

La noticia de que BlackCat agregó una lista renovada de herramientas a sus ataques llega cuando un desarrollador asociado con el malware de cifrado de archivos LockBit 3.0 (también conocido como LockBit Black) supuestamente filtró el constructor utilizado para crear versiones personalizadas, lo que generó preocupaciones de que podría conducir a un abuso más generalizado por otros actores menos hábiles.

Pero no es solo LockBit, en los últimos dos años, los grupos de ransomware Babuk y Conti sufrieron infracciones similares, lo que redujo efectivamente la barrera de entrada y permitió que los atacantes lanzaran rápidamente sus propios ataques.