Los operadores del esquema Hive, ransomware-as-a-service (RaaS) revisaron su software de cifrado de archivos para migrar completamente a Rust y adoptar así un método de cifrado más sofisticado.

> *«Con su última variante que incluye varias actualizaciones importantes, Hive también demuestra que es una de las familias de ransomware de más rápida evolución, lo que ejemplifica el ecosistema de ransomware en constante cambio»,* dijo Microsoft Threat Intelligence Center (MSTIC) en un informe.

Hive, que se observó por primera vez en junio de 2021, se ha convertido en uno de los grupos RaaS más prolíficos, con 17 ataques solo en el mes de mayo de 2022, junto con Black Basta y Conti.

El cambio de GoLang a Rust convierte a Hive en la segunda cepa de ransomware después de BlackCat que se escribe en el lenguaje de programación, lo que permite que el malware obtenga beneficios adicionales, como la seguridad de la memoria y un control más profundo sobre los recursos de bajo nivel, así como hacer uso de una amplia gama de librerías criptográficas.

Lo que también ofrece, es la capacidad de hacer que el malware sea resistente a la ingeniería inversa, haciéndolo más evasivo. Por otro lado, cuenta con funciones para detener servicios y procesos asociados con soluciones de seguridad que pueden detenerlo en seco.

Hive no se diferencia de otras familias de ransomware en que elimina las copias de seguridad para evitar la recuperación, pero lo que ha cambiado significativamente en la nueva variante basada en Rust es su enfoque para el cifrado de archivos.

> *«En lugar de incrustar una clave cifrada en cada archivo, genera dos conjuntos de claves en la memoria, las usa para cifrar archivos y luego cifra y escribe los conjuntos en la raíz de la unidad que cifra, ambos con la extensión .key»,* explicó

> MSTIC.

Para determinar cuál de las dos claves se usa para bloquear un archivo específico, se cambia el nombre de un archivo cifrado para incluir el nombre del archivo que contiene la clave, seguido de un guión bajo y una cadena codificada en Base64 que apunta a dos ubicaciones diferentes en el archivo .key correspondiente.

Los hallazgos se producen cuando el atacante detrás del ransomware AstraLocker, menos conocido, cesó sus operaciones y lanzó una herramienta de descifrado como parte de un cambio hacia el cryptojacking, según informó Bleeping Computer.

Pero como una indicación de que el panorama de los ciberdelincuentes está en constante cambio, los investigadores de seguridad cibernética descubrieron una nueva familia de ransomware llamada RedAlert (también conocida como N13V), que es capaz de apuntar a los servidores VMware ESXi de Windows y Linux.