El Departamento de Justicia de los Estados Unidos (DoJ) ha comunicado de manera oficial la interrupción de la actividad del ransomware BlackCat y ha liberado una herramienta de desencriptación que permite a los afectados recuperar sus archivos bloqueados por el programa malicioso.

Documentos judiciales revelan que el FBI de EE. UU. contó con la asistencia de una fuente humana secreta (CHS) para trabajar como colaborador de BlackCat y obtener acceso a una plataforma web utilizada para gestionar las víctimas del grupo delictivo, en un claro caso de contratacar a los delincuentes cibernéticos.

BlackCat, también conocido como ALPHV y Noberus, hizo su aparición inicial en diciembre de 2021 y rápidamente se posicionó como el segundo tipo de ransomware más activo en el mundo, justo después de LockBit. Destaca por ser el primer ransomware desarrollado en el lenguaje Rust que se detecta en entornos reales.

Este avance da por terminadas las especulaciones acerca de una supuesta intervención policial tras la desaparición temporal de su portal en la dark web el 7 de diciembre, reapareciendo cinco días después con solo un único perjudicado.

El FBI informó que colaboró con numerosas víctimas en EE. UU. para instalar la herramienta de desencriptación, evitando pagos de rescate que ascendían a unos 68 millones de dólares. Además, pudo obtener datos sobre la infraestructura del ransomware, logrando recopilar 946 conjuntos de claves para los sitios TOR manejados por el grupo y neutralizarlos.

Al igual que otros grupos de ransomware, BlackCat opera bajo un esquema de servicio, donde hay desarrolladores centrales y colaboradores que distribuyen y ejecutan el malware, enfocándose en objetivos valiosos.

Adicionalmente, implementa una táctica de doble presión, extrayendo información confidencial antes de cifrarla, con el fin de coaccionar a las víctimas para que paguen.

> El DoJ indicó: *«Los colaboradores de BlackCat han logrado ingresar a las infraestructuras de las víctimas mediante diversas técnicas, como el uso de credenciales previamente comprometidas».*

En total, se estima que esta entidad con fines lucrativos ha afectado a más de 1.000 redes alrededor del mundo, obteniendo ganancias ilícitas que superan los cientos de millones de dólares.

Curiosamente, esta intervención ha favorecido indirectamente a grupos rivales como LockBit, que están aprovechando la situación para sumar nuevos colaboradores y ofrecer soluciones a las víctimas.