Un análisis de dos ataques de ransomware identificó superposiciones en las tácticas, técnicas y procedimientos (TTP) entre BlackCat y BlackMatter, lo que indica una fuerte conexión entre los dos grupos.

Aunque es típico que los grupos de ransomware cambien el nombre de sus operaciones en respuesta a una mayor visibilidad de sus ataques, BlackCat (también conocido como Alphv) marca una nueva frontera en el sentido de que el cártel del crimen cibernético se construye a partir de afiliados de otras operaciones de ransomware como servicio (RaaS).

BlackCat surgió por primera vez en noviembre de 2021 y desde entonces se ha dirigido a varias organizaciones en todo el mundo durante los últimos meses. Ha sido llamado por ser parecido a BlackMatter, una familia de ransomware de corta duración que se originó en DarkSide, que atrajo notoriedad por su ataque de alto perfil en Colonial Pipeline en mayo de 2021.

En una entrevista con The Record, de Recorded Future, el mes pasado, un representante de BlackCat descartó los rumores de que se trata de un cambio de marca de BlackMatter, al mismo tiempo que afirmó que está formado por afiliados asociados con otros grupos RaaS.

> *«En parte, todos estamos conectados con gandrevil [GrandCrab/REvil], blackside [BlackMatter/DarkSide], mazegreggor [Maze/Egregor], lockbit, etcétera, porque somos anuncios (también conocidos como afiliados). Tomamos prestadas sus ventajas y eliminamos sus desventajas»*, dijo el representante anónimo.

> *«BlackCat parece ser un caso de expansión comercial vertical. En esencia, una forma de controlar la cadena de suministro ascendente haciendo que un servicio que es clave para su negocio (el operador RaaS) se adapte mejor a sus necesidades y agregando otra fuente de ingresos»,* dijeron los investigadores de Cisco Talos, Tiago Pereira y Caitlin Huey.

Además, la compañía de seguridad cibernética dijo que observó una serie de puntos en común entre un ataque de BlackMatter en septiembre de 2021 y el de un ataque de BlackCat de diciembre de 2021, incluidas las herramientas y los nombres de archivo utilizados, así como un dominio empleado para mantener el acceso persistente a la red objetivo.

Este uso superpuesto de la misma dirección de comando y control planteó la posibilidad de que el afiliado que utilizó BlackMatter haya sido uno de los primeros en adoptar BlackCat, ya que ambos ataques tardaron más de 15 días en llegar a la etapa de cifrado.

> *«Como hemos visto varias veces antes, los servicios RaaS van y vienen. Sin embargo, es probable que sus afiliados simplemente pasen a un nuevo servicio. Y con ellos, es probable que muchos de los TTP persistan»,* dijeron los investigadores.

Los hallazgos se producen cuando BlackBerry detalló una nueva familia de ransomware basada en .NET llamada LokiLocker, que no solo encripta los archivos, sino que también incorpora una función de limpieza opcional que está diseñada para borrar todos los archivos que no son del sistema y sobrescribir el registro de arranque maestro (MBR) en caso de que una víctima se niegue a pagar dentro de un plazo determinado.

> *«LokiLocker funciona como un esquema de ransomware como servicio de acceso limitado que parece venderse a un número relativamente pequeño de afiliados cuidadosamente examinados a puerta cerrada»,* dijeron los investigadores.

Ha estado activo desde al menos agosto de 2021, y la mayoría de las víctimas detectadas hasta ahora se concentran en Europa del Este y Asia.