Microsoft advierte que el equipo de ransomware BlackCat está aprovechando las vulnerabilidades de los servidores de Exchange sin parches, con el fin de obtener acceso a redes específicas.

Al obtener un punto de entrada, los atacantes se movieron rápidamente para recopilar información sobre las máquinas comprometidas, luego llevaron a cabo actividades de robo de credenciales y movimiento lateral, antes de recolectar propiedad intelectual y soltar la carga útil del ransomware.

La secuencia completa de eventos se desarrolló en el transcurso de dos semanas completas, dijo el equipo de inteligencia de amenazas de Microosft 365 Defender en un informe publicado esta semana.

> *«En otro incidente que observamos, descubrimos que un afiliado de ransomware obtuvo acceso inicial al entorno por medio de un servidor de escritorio remoto orientado a Internet usando credenciales comprometidas para iniciar sesión. No hay dos BlackCat 'vivos' o las implementaciones pueden tener el mismo aspecto»,* dijeron los investigadores.

BlackCat, también conocido como ALPHV y Norberus, es un participante relativamente nuevo en el espacio del ransomware hiperactivo. También se sabe que es uno de los primeros ransomware multiplataforma escrito en Rust, lo que ejemplifica una tendencia en la que los actores de amenazas están cambiando a lenguajes de programación poco comunes en un intento de evadir la detección.

El esquema de ransomware como servicio (PaaS), independientemente de los distintos vectores de acceso inicial empleados, culmina en la exfiltración y el cifrado de los datos de destino que luego se retienen como parte de lo que se denomina doble extorsión.

El modelo RaaS ha demostrado ser un lucrativo ecosistema cibercriminal al estilo de la economía de conciertos, que consta de tres jugadores clave diferentes: corredores de acceso (IAB), que comprometen las redes y mantienen la persistencia; operadores, que desarrollan y mantienen las operaciones de ransomware; y afiliados, que compran el acceso a lo sIAB para implementar la carga útil real.

Según una alerta publicada por la Oficina Federal de Investigaciones (FBI) de Estados Unidos, los ataques del ransomware BlackCat han afectado al menos a 60 entidades en todo el mundo hasta marzo de 2022 desde que se detectó por primera vez en noviembre de 2021.

Además, Microsoft dijo que *«dos de los grupos de amenazas afiliados más prolíficos»*, que se han asociado con varias familias de ransomware como Hive, Conti, REvil y LockBit 2.0, ahora están distribuyendo BlackCat.

Esto incluye DEV-0237 (también conocido como FIN12), un actor de amenazas con motivación financiera que se vio por última vez apuntando al sector de la salud en octubre de 2021, y DEV-0504, que ha estado activo desde 2020 y tiene un patrón de cambio de cargas útiles cuando se cierra un programa RaaS.

> *«DEV-0504 fue responsable de implementar el ransomware BlackCat en empresas del sector energético en enero de 2022. Casi al mismo tiempo, DEV-0504 también implementó BlackCat en ataques contra empresas de las industrias de moda, tabaco, TI y manufactura, entre otras»*, dijo Microsoft el mes pasado.