La Oficina Federal de Investigación de los Estados Unidos (FBI) ha emitido una alerta sobre una nueva tendencia de ataques de ransomware que apuntan a las mismas víctimas, al menos desde julio de 2023.

> *«Durante estos incidentes, los actores cibernéticos maliciosos han utilizado dos variantes de ransomware distintas contra empresas afectadas, entre las que se incluyen AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum y Royal. Estas variantes se han empleado en diversas combinaciones»,* señaló el FBI en su comunicado.

Aunque no se tiene información detallada sobre la magnitud de estos ataques, se cree que ocurren en cercanía temporal entre sí, con un intervalo que va desde 48 horas hasta un máximo de 10 días.

Otro cambio destacado en los ataques de ransomware es el aumento en la utilización de herramientas de robo de datos personalizadas, herramientas de borrado y malware para ejercer presión sobre las víctimas y forzar el pago de los rescates.

> *«La utilización de dos variantes de ransomware en estos ataques ha resultado en una combinación de cifrado de datos, extracción de información y pérdidas financieras debidas a los pagos de rescate. Los segundos ataques de ransomware contra sistemas que ya están comprometidos pueden causar un daño significativo a las entidades afectadas»*, subrayó la agencia.

Es importante mencionar que los ataques de ransomware doble no son algo completamente nuevo, ya que se han observado casos desde mayo de 2021.

El año pasado, Sophos dio a conocer que un proveedor de la industria automotriz, no identificado, había sido objeto de un triple ataque de ransomware que involucraba a Lockbit,

Hive y BlackCat durante un período de dos semanas entre abril y mayo de 2022.

Además, a principios de este mes, Symantec detalló un ataque de ransomware a las 3 a. m. que afectó a una víctima no identificada después de un intento fallido de introducir LockBit en la red objetivo.

El cambio en las tácticas se debe a diversos factores, incluyendo la explotación de vulnerabilidades de día cero y la creciente presencia de intermediarios de acceso inicial y afiliados en el panorama del ransomware, quienes pueden revender el acceso a sistemas víctimas y lanzar múltiples cepas de ransomware en rápida sucesión.

Se recomienda a las organizaciones fortalecer sus medidas de seguridad manteniendo copias de respaldo desconectadas de la red, supervisando las conexiones remotas desde el exterior y el uso del protocolo de escritorio remoto (RDP), implementando la autenticación de múltiples factores resistente al phishing, llevando a cabo auditorías de cuentas de usuario y segmentando las redes para evitar la propagación del ransomware.