El actor de amenazas motivado financieramente, identificado como Storm-0501, ha sido observado perfeccionando sus tácticas para realizar filtración de datos y ataques de extorsión dirigidos a entornos en la nube.

"A diferencia del ransomware tradicional en entornos locales, donde los atacantes suelen desplegar un malware para cifrar archivos críticos en los equipos comprometidos y luego negocian una clave de descifrado, el ransomware basado en la nube representa un cambio fundamental," señaló el equipo de Inteligencia de Amenazas de Microsoft en un informe.

"Aprovechando capacidades nativas de la nube, Storm-0501 exfiltra rápidamente grandes volúmenes de información, elimina datos y respaldos dentro del entorno de la víctima y exige un rescate, todo sin depender del despliegue de malware convencional."

Microsoft documentó por primera vez a Storm-0501 hace casi un año, describiendo sus ataques híbridos de ransomware en la nube contra sectores gubernamentales, manufactureros, de transporte y de seguridad pública en EE. UU., donde los atacantes pasaron de entornos locales hacia la nube para realizar robo de credenciales, exfiltración y despliegue de ransomware.

Se estima que el grupo está activo desde 2021 y que ha evolucionado hacia un modelo de ransomware como servicio (RaaS), distribuyendo diversas familias de ransomware a lo largo del tiempo, como Sabbath, Hive, BlackCat (ALPHV), Hunters International, LockBit y Embargo.

"Storm-0501 ha seguido mostrando habilidad para desplazarse entre infraestructuras locales y en la nube, reflejando cómo los actores de amenazas se adaptan conforme crece la adopción de entornos híbridos," indicó la compañía. *"Buscan dispositivos sin gestión y fallos de seguridad en entornos híbridos para evadir la detección, escalar privilegios en la nube y, en ocasiones, atravesar inquilinos en configuraciones multi-tenant para lograr sus objetivos."*

Las cadenas de ataque típicas comienzan con el uso del acceso inicial para escalar privilegios hasta administrador de dominio, seguido de movimientos laterales locales y tareas de reconocimiento que les permiten comprometer el entorno en la nube de la víctima, activando

así una secuencia de varias etapas: persistencia, escalamiento, filtración, cifrado y extorsión.

Según Microsoft, el acceso inicial suele lograrse a través de corredores de acceso como Storm-0249 y Storm-0900, quienes aprovechan credenciales robadas o comprometidas para ingresar a los sistemas, o mediante la explotación de vulnerabilidades conocidas de ejecución remota en servidores públicos sin parches.

En una campaña reciente contra una gran empresa con múltiples filiales, Storm-0501 realizó tareas de reconocimiento antes de moverse lateralmente con Evil-WinRM. También ejecutaron un ataque DCSync para extraer credenciales de Active Directory, simulando el comportamiento de un controlador de dominio.

"Aprovechando su posición en el entorno de Active Directory, se desplazaron entre dominios y finalmente comprometieron un segundo servidor de Entra Connect asociado a otro inquilino de Entra ID y un dominio diferente de Active Directory," explicó Microsoft.

"El actor de amenazas extrajo la cuenta de sincronización de directorios para repetir el proceso de reconocimiento, esta vez enfocado en identidades y recursos del segundo inquilino."

Con estas acciones, Storm-0501 logró identificar una identidad sincronizada no humana con rol de Administrador Global en Microsoft Entra ID dentro de ese inquilino, sin protección de autenticación multifactor (MFA). Esto les permitió restablecer la contraseña del usuario en el entorno local, sincronizándola luego con la identidad en la nube a través del servicio Entra Connect Sync.

Con la cuenta de Administrador Global comprometida, los atacantes accedieron al portal de

Azure, registrando un inquilino de Entra ID controlado por ellos como dominio federado de confianza para crear una puerta trasera, elevar su acceso a recursos críticos de Azure y preparar el terreno para la filtración y posterior extorsión.

"Tras completar la fase de exfiltración, Storm-0501 inició el borrado masivo de los recursos de Azure que contenían la información de la organización víctima, impidiendo que esta pudiera aplicar medidas de recuperación o restaurar los datos," señaló Microsoft.

"Después de exfiltrar y destruir los datos en el entorno de Azure, el atacante dio inicio a la fase de extorsión, contactando a las víctimas mediante Microsoft Teams con una de las cuentas previamente comprometidas, exigiendo el pago del rescate."

La compañía informó que aplicó un cambio en Microsoft Entra ID para evitar que los actores de amenazas abusen de las cuentas de sincronización de directorios para escalar privilegios. Asimismo, liberó actualizaciones para Microsoft Entra Connect (versión 2.5.3.0) que incluyen soporte para Autenticación Moderna, lo que permite configurar autenticación basada en aplicaciones para mayor seguridad.

"También resulta fundamental habilitar el Trusted Platform Module (TPM) en el servidor de Entra Connect Sync para almacenar de forma segura credenciales sensibles y claves criptográficas, mitigando las técnicas de extracción de credenciales utilizadas por Storm-0501," añadió la empresa tecnológica.