El actor de amenazas conocido como Storm-0501 ha dirigido ataques de ransomware contra los sectores gubernamental, de manufactura, transporte y fuerzas del orden en los Estados Unidos.

La campaña de ataques en varias fases está diseñada para comprometer entornos de nube híbrida y realizar movimientos laterales desde infraestructuras locales hacia la nube. Esto culmina en la exfiltración de datos, robo de credenciales, manipulación de sistemas, acceso persistente mediante puertas traseras y la instalación de ransomware, según informó Microsoft.

> *«Storm-0501 es un grupo de ciberdelincuentes motivado por ganancias económicas que emplea herramientas de código abierto y genéricas para llevar a cabo ataques de ransomware»,* según el equipo de inteligencia de amenazas de Microsoft.

Activo desde 2021, este actor de amenazas tiene un historial de ataques a instituciones educativas mediante el ransomware Sabbath (54bb47h). Con el tiempo, evolucionó hasta convertirse en un afiliado del modelo ransomware como servicio (RaaS), utilizando diversas variantes de ransomware, como Hive, BlackCat (ALPHV), Hunters International, LockBit y Embargo.

Uno de los aspectos más notables de los ataques de Storm-0501 es la explotación de credenciales débiles y cuentas con privilegios excesivos para moverse desde los entornos locales hacia la infraestructura en la nube.

Otras técnicas de acceso inicial incluyen aprovechar puntos de acceso establecidos previamente por intermediarios como Storm-0249 y Storm-0900, o aprovechar vulnerabilidades conocidas de ejecución remota de código en servidores expuestos a Internet que no han sido actualizados, como Zoho ManageEngine, Citrix NetScaler y Adobe ColdFusion 2016.

El acceso que estos métodos permiten facilita una amplia operación de reconocimiento,

identificando activos de alto valor, recopilando información de dominios y realizando exploraciones de Active Directory. Después de esta etapa, el atacante despliega herramientas de gestión y monitoreo remoto (RMM), como AnyDesk, para asegurar acceso persistente.

> *«El actor de amenazas aprovechó los privilegios de administrador en los dispositivos locales comprometidos y trató de acceder a más cuentas dentro de la red usando diversas técnicas»,* declaró Microsoft.
>
> *«Principalmente, el actor utilizó el módulo SecretsDump de Impacket, que permite extraer credenciales a través de la red, y lo aplicó en una gran cantidad de dispositivos para obtener más credenciales».*

Las credenciales comprometidas luego son utilizadas para acceder a más dispositivos y extraer más credenciales, mientras el atacante simultáneamente accede a archivos sensibles para extraer secretos de KeePass y lleva a cabo ataques de fuerza bruta para obtener credenciales específicas.

Microsoft detectó que Storm-0501 empleó Cobalt Strike para moverse lateralmente a través de la red utilizando las credenciales comprometidas y emitir comandos adicionales. La exfiltración de datos desde la infraestructura local se lleva a cabo usando Rclone para transferir la información a MegaSync, un servicio público de almacenamiento en la nube.

El actor de amenazas también ha sido observado creando puertas traseras persistentes en la nube y desplegando ransomware en la infraestructura local, sumándose a la lista de actores que apuntan a entornos de nube híbrida, como Octo Tempest y Manatee Tempest.

> *«El actor utilizó las credenciales robadas, específicamente Microsoft Entra ID (anteriormente Azure AD), para moverse lateralmente desde los sistemas locales*

> *hacia la nube, estableciendo un acceso persistente mediante una puerta trasera»*, afirmó Microsoft.

Este movimiento hacia la nube puede realizarse usando una cuenta de usuario comprometida de Microsoft Entra Connect Sync o mediante el secuestro de sesiones en la nube de una cuenta de usuario local con privilegios de administrador en la nube, cuando la autenticación multifactor (MFA) está desactivada.

El ataque concluye con la instalación del ransomware Embargo en la red de la organización víctima, tras haber obtenido control suficiente del sistema, exfiltrar archivos valiosos y realizar movimientos laterales hacia la nube. Embargo es un ransomware escrito en Rust que fue descubierto en mayo de 2024.

> *«Bajo el modelo de RaaS, el grupo detrás de Embargo permite que afiliados como Storm-0501 utilicen su plataforma para ejecutar ataques a cambio de una parte del rescate»,* explicó Microsoft.

> *«Los afiliados de Embargo emplean tácticas de doble extorsión, primero cifrando los archivos de las víctimas y luego amenazando con divulgar los datos robados si no se paga un rescate».*

Esta revelación llega mientras el grupo DragonForce ha estado atacando empresas en los sectores de manufactura, bienes raíces y transporte utilizando una variante del constructor filtrado de LockBit3.0 y una versión modificada de Conti.

Los ataques de DragonForce se caracterizan por el uso del backdoor SystemBC para mantener el acceso persistente, Mimikatz y Cobalt Strike para robar credenciales, y el uso de Cobalt Strike para moverse lateralmente dentro de las redes. Estados Unidos representa más del 50% de las víctimas de estos ataques, seguido por el Reino Unido y Australia.

> *«El grupo utiliza tácticas de doble extorsión, encriptando los datos y amenazando con filtrar la información a menos que se pague un rescate. El programa de afiliados, lanzado el 26 de junio de 2024, ofrece el 80% del rescate a los afiliados, además de herramientas para gestionar y automatizar los ataques»*, indicó Group-IB, con sede en Singapur.