Una vulnerabilidad de seguridad ya solucionada en el software Veeam Backup & Replication está siendo aprovechada por una nueva operación de ransomware conocida como EstateRansomware.

Group-IB, una empresa con sede en Singapur, descubrió al actor de amenazas a principios de abril de 2024 y señaló que el método de operación implicaba la explotación de CVE-2023-27532 (puntuación CVSS: 7.5) para realizar actividades maliciosas.

Se cree que el acceso inicial al entorno objetivo fue facilitado mediante un dispositivo de firewall SSL VPN de Fortinet FortiGate utilizando una cuenta inactiva.

> *«El actor de la amenaza se movió lateralmente desde el firewall FortiGate a través del servicio SSL VPN para acceder al servidor de respaldo,»* explicó el investigador de seguridad Yeo Zi Wei en un análisis publicado hoy.
>
> *«Antes del ataque de ransomware, se detectaron intentos de fuerza bruta de VPN en abril de 2024 usando una cuenta inactiva identificada como 'Acc1'. Días después, se rastreó un inicio de sesión exitoso de VPN con 'Acc1' hasta la dirección IP remota 149.28.106[.]252.»*

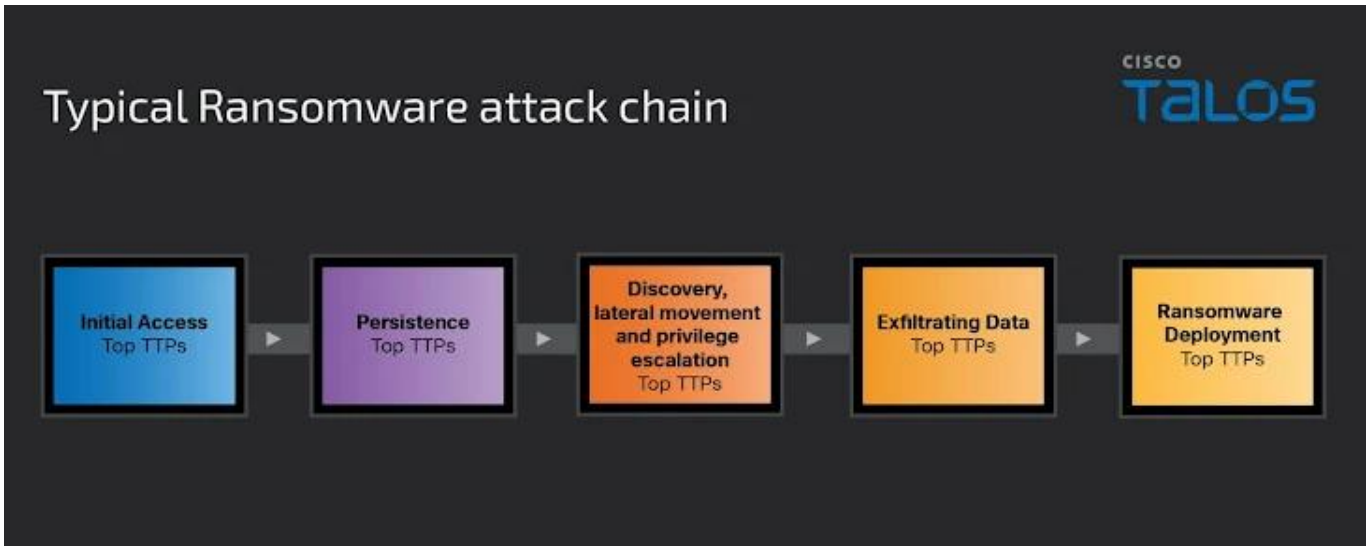
Luego, los atacantes establecieron conexiones RDP desde el firewall al servidor de respaldo, seguido de la instalación de una puerta trasera persistente llamada *«svchost.exe»* que se ejecuta diariamente a través de una tarea programada.

El acceso posterior a la red se logró utilizando la puerta trasera para evitar la detección. La función principal de la puerta trasera es conectarse a un servidor de comando y control (C2) a través de HTTP y ejecutar comandos arbitrarios emitidos por el atacante.

Group-IB indicó que observó al actor explotando la falla de Veeam CVE-2023-27532 con el objetivo de habilitar xp_cmdshell en el servidor de respaldo y crear una cuenta de usuario

falsa llamada «VeeamBkp», además de llevar a cabo actividades de descubrimiento de red, enumeración y recolección de credenciales usando herramientas como NetScan, AdFind y NitSoft con la cuenta recién creada.

> *«Es posible que esta explotación haya involucrado un ataque originado en la carpeta VeeamHax en el servidor de archivos contra la versión vulnerable del software Veeam Backup & Replication instalada en el servidor de respaldo»,* hipotetizó Zi Wei.
>
> *«Esta actividad facilitó la activación del procedimiento almacenado xp_cmdshell y la creación subsecuente de la cuenta 'VeeamBkp'.»*



El ataque concluyó con la implementación del ransomware, pero no antes de tomar medidas para debilitar las defensas y moverse lateralmente desde el servidor de Active Directory a todos los demás servidores y estaciones de trabajo utilizando cuentas de dominio comprometidas.

> *«Windows Defender fue desactivado de forma permanente usando DC.exe [Defender Control], seguido por la implementación y ejecución del ransomware con PsExec.exe,»* informó Group-IB.

La divulgación se produce cuando Cisco Talos reveló que la mayoría de los grupos de ransomware priorizan establecer acceso inicial utilizando vulnerabilidades de seguridad en aplicaciones expuestas al público, archivos adjuntos de phishing o comprometiendo cuentas válidas, y evadiendo defensas en sus cadenas de ataque.

El modelo de doble extorsión, que implica exfiltrar datos antes de cifrar los archivos, ha llevado al desarrollo de herramientas personalizadas por parte de los atacantes (por ejemplo, Exmatter, Exbyte y StealBit) para enviar la información confidencial a una infraestructura controlada por los adversarios.

Esto requiere que estos grupos de ciberdelincuencia establezcan acceso a largo plazo para explorar el entorno con el fin de comprender la estructura de la red, ubicar recursos que puedan apoyar el ataque, elevar sus privilegios o permitirles pasar desapercibidos, e identificar datos valiosos que puedan ser robados.

> *«En el último año, hemos sido testigos de grandes cambios en el ámbito del ransomware con la aparición de múltiples nuevos grupos de ransomware, cada uno mostrando objetivos únicos, estructuras operativas y victimología,»* dijo Talos.

> *«La diversificación resalta un cambio hacia actividades cibercriminales más especializadas, ya que grupos como Hunters International, Cactus y Akira crean nichos específicos, enfocándose en objetivos operativos y elecciones estilísticas distintas para diferenciarse.»*