Investigadores de seguridad cibernética arrojaron luz sobre una nueva cepa de ransomware llamada CACTUS, que se descubrió que aprovecha vulnerabilidades conocidas en los dispositivos VPN para obtener acceso inicial a las redes objetivo.

> *«Una vez dentro de la red, los atacantes de CACTUS intentan enumerar las cuentas de usuario locales y de la red, además de los puntos finales alcanzables antes de crear nuevas cuentas de usuario y aprovechar los scripts personalizados para automatizar la implementación y detonación del cifrador de ransomware por medio de tareas programadas»,* dijo Kroll en un informe.

Se ha observado que el ransomware se dirige a grandes entidades comerciales desde marzo de 2023, con ataques que emplean tácticas de doble extorsión para robar datos confidenciales antes del cifrado. No se ha identificado ningún sitio de fuga de datos hasta ahora.

Después de una explotación exitosa de dispositivos VPN vulnerables, se configura una backdoor SSH para mantener el acceso persistente y se ejecuta una serie de comandos de PowerShell para realizar un escaneo de la red e identificar una lista de máquinas para el cifrado.

Los ataques de CACTUS también usan Cobalt Strike y una herramienta de tunelización conocida como Chisel para comando y control, junto con software de administración y monitoreo remoto (RMM) como AnyDesk para enviar archivos a los hosts infectados.

También se toman medidas para deshabilitar y desinstalar soluciones de seguridad, así como para extraer credenciales de navegadores web y el servicio de subsistema de autoridad de seguridad local (LSASS) para escalar privilegios.

A la escalada de privilegios le sigue el movimiento lateral, la exfiltración de datos y el despliegue de ransomware, el último de los cuales se logra mediante un script de PowerShell que también ha sido usado por Black Basta.

Un aspecto novedoso de CACTUS es el uso de un script por lotes para extraer el binario del ransomware con 7-Zip, seguido de la eliminación del archivo .7z antes de ejecutar la carga útil.

> *«CACTUS esencialmente se encripta a sí mismo, lo que hace más difícil de detectar y lo ayuda a evadir las herramientas antivirus y de monitoreo de red»,* dijo Laurie Lacono, directora general asociada de riesgo cibernético en Kroll.

> *«Esta nueva variante de ransomware bajo el nombre de CACTUS aprovecha una vulnerabilidad en un popular dispositivo VPN, mostrando que los hackers siguen apuntando a los servicios de acceso remoto y vulnerabilidades sin parches para el acceso inicial».*

El desarrollo se produce días después de que Trend Micro arrojara luz sobre otro tipo de ransomware conocido como Rapture, que tiene algunas similitudes con otras familias como Paradise.

«Toda la cadena de infección dura de tres a cinco días como máximo», dijo la compañía, con el reconocimiento inicial seguido por el despliegue de CObalt Strike, que después se usa para eliminar el ransomware basado en .NET.

Se sospecha que la intrusión se facilita por medio de servidores y sitios web públicos vulnerables, por lo que es imperativo que las empresas tomen medidas para mantener los sistemas actualizados y hacer cumplir el principio de privilegio mínimo (PoLP).

> *«Aunque sus operadores usan herramientas y recursos que están fácilmente disponibles, han logrado usarlos de una forma que mejora las capacidades de Rapture, haciéndolo más sigiloso y más difícil de analizar»,* dijo Trend Micro.

CACTUS y Rapture son las últimas incorporaciones a una larga lista de nuevas familias de ransomware que han salido a la luz en las últimas semanas, incluyendo Gazprom, BlackBit, UNIZA, Akira y una variante del ransomware NoCry llamada Kadavro Vector.