Se ha identificado una campaña de ransomware denominada CACTUS que está aprovechando recientemente las vulnerabilidades de seguridad divulgadas en una plataforma de análisis en la nube e inteligencia empresarial conocida como Qlik Sense para ingresar a entornos específicos.

> *«Este episodio marca la primera instancia documentada [...] en la cual los actores de amenazas que implementan el ransomware CACTUS han explotado debilidades en Qlik Sense para lograr un acceso inicial»,* señalan los investigadores de Arctic Wolf, Stefan Hostetler, Markus Neis y Kyle Pagelow.

La empresa de ciberseguridad, que asegura estar respondiendo a *«varias instancias»* de explotación del software, destaca que los ataques probablemente estén aprovechando tres fallos que se han revelado en los últimos tres meses:

- CVE-2023-41265 (puntuación CVSS: 9.9) – Una vulnerabilidad de túneles de solicitud HTTP que permite a un atacante remoto aumentar sus privilegios y enviar solicitudes ejecutadas por el servidor backend que aloja la aplicación del repositorio.
- CVE-2023-41266 (puntuación CVSS: 6.5) – Una vulnerabilidad de travesía de ruta que posibilita a un atacante remoto no autenticado enviar solicitudes HTTP a destinos no autorizados.
- CVE-2023-48365 (puntuación CVSS: 9.9) – Una vulnerabilidad de ejecución remota de código no autenticado que surge debido a la validación incorrecta de encabezados HTTP, permitiendo a un atacante remoto aumentar sus privilegios mediante la tunelización de solicitudes HTTP.

Es relevante señalar que CVE-2023-48365 es el resultado de una corrección incompleta para CVE-2023-41265, el cual, junto con CVE-2023-41266, fue divulgado por Praetorian a finales de agosto de 2023. La solución para CVE-2023-48365 se implementó el 20 de septiembre de 2023.

En los ataques observados por Arctic Wolf, la explotación exitosa de estas vulnerabilidades

es seguida por el mal uso del servicio Qlik Sense Scheduler para generar procesos diseñados para descargar herramientas adicionales con el objetivo de establecer persistencia y configurar el control remoto.

Esto incluye herramientas como ManageEngine Unified Endpoint Management and Security (UEMS), AnyDesk y Plink. También se ha notado que los actores de amenazas desinstalan el software de Sophos, cambian la contraseña de la cuenta de administrador y crean un túnel RDP mediante Plink.

Las secuencias de ataque culminan con la implementación del ransomware CACTUS, y los atacantes utilizan rclone para la extracción de datos.

El panorama del ransomware en constante evolución

Esta revelación se produce en un momento en que el panorama de amenazas de ransomware se ha vuelto más complejo, y la economía subterránea ha evolucionado para facilitar ataques a gran escala mediante una red de intermediarios de acceso inicial y propietarios de botnets que revenden el acceso a sistemas de víctimas a varios actores afiliados.

Según datos recopilados por la empresa de ciberseguridad industrial Dragos, el número de ataques de ransomware que impactan a organizaciones industriales disminuyó de 253 en el segundo trimestre de 2023 a 231 en el tercer trimestre. En contraste, se informaron 318 ataques de ransomware en todos los sectores solo en el mes de octubre de 2023.

A pesar de los esfuerzos continuos de los gobiernos de todo el mundo para abordar el ransomware, el modelo de negocio de ransomware como servicio (RaaS) ha seguido siendo una vía duradera y lucrativa para extorsionar dinero a objetivos.

Black Basta, un grupo prolífico de ransomware que surgió en abril de 2022, se estima que ha obtenido ganancias ilegales de al menos $107 millones en pagos de rescate en Bitcoin de más de 90 víctimas, según una nueva investigación conjunta publicada por Elliptic y Corvus

Insurance.

La mayor parte de estos ingresos se blanquearon a través de Garantex, un intercambio de criptomonedas ruso que fue sancionado por el gobierno de EE. UU. en abril de 2022 por facilitar transacciones con el mercado negro Hydra.

Además, el análisis descubrió pruebas que vinculan a Black Basta con el grupo de ciberdelincuentes ruso Conti, que se disolvió aproximadamente al mismo tiempo que surgió el primero, así como con QakBot, que se utilizó para desplegar el ransomware.

> *«Aproximadamente el 10% del monto del rescate se transfirió a Qakbot, en casos en los que estuvieron involucrados en proporcionar acceso a la víctima. Rastreó Bitcoin por varios millones de dólares desde billeteras vinculadas a Conti hasta aquellas asociadas con el operador de Black Basta»*, señaló Elliptic, agregando que