Se ha observado que varios grupos respaldados por gobiernos de Rusia y China están aprovechando una reciente debilidad de seguridad en la herramienta de compresión WinRAR para Windows como parte de sus operaciones.

La vulnerabilidad en cuestión es la CVE-2023-38831 (con una puntuación CVSS de 7.8), que permite a los atacantes ejecutar código malicioso cuando un usuario intenta abrir un archivo inofensivo dentro de un archivo ZIP. Esta vulnerabilidad ha estado siendo explotada activamente desde al menos abril de 2023.

El Grupo de Análisis de Amenazas de Google (TAG), que detectó estas actividades en las últimas semanas, las ha relacionado con tres grupos diferentes que sigue bajo los nombres FROZENBARENTS (también conocido como Sandworm), FROZENLAKE (también conocido como APT28) e ISLANDDREAMS (también conocido como APT40).

La campaña de phishing relacionada con Sandworm se hizo pasar por una escuela de entrenamiento de drones en Ucrania a principios de septiembre y distribuyó un archivo ZIP malicioso que aprovechaba la CVE-2023-38831 para introducir el malware Rhadamanthys, un programa de robo de datos que se ofrece por $250 como suscripción mensual.

Se informa que APT28, que también tiene vínculos con la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación Rusa (GRU), al igual que Sandworm, lanzó una campaña de correos electrónicos dirigida a organizaciones gubernamentales en Ucrania.

En estos ataques, los usuarios en Ucrania se les instaba a descargar un archivo que contenía una explotación de la CVE-2023-38831, disfrazada como una invitación a un evento del Centro Razumkov, un centro de análisis de políticas públicas en el país.

El resultado es la ejecución de un script de PowerShell llamado IRONJAW que roba datos de inicio de sesión de navegadores y directorios locales y envía la información a una infraestructura controlada por los atacantes en webhook[.]site.

El tercer grupo de amenazas que está aprovechando la vulnerabilidad de WinRAR es APT40,

que lanzó una campaña de phishing dirigida a Papúa Nueva Guinea, en la que los correos electrónicos incluían un enlace de Dropbox a un archivo ZIP que contenía la explotación de CVE-2023-38831.

La secuencia de infección finalmente permitió la instalación de un archivo ejecutable llamado ISLANDSTAGER, que es responsable de cargar BOXRAT, un backdoor .NET que utiliza la API de Dropbox para el control y el comando.

Este informe se basa en descubrimientos recientes de Cluster25, que detalló ataques realizados por el grupo de piratas informáticos APT28 que aprovechaban la debilidad en WinRAR para llevar a cabo operaciones de robo de credenciales.

Además, se ha reportado la participación de otros actores respaldados por gobiernos, como Konni (que comparte similitudes con un grupo norcoreano rastreado como Kimsuky) y Dark Pink (también conocido como Saaiwc Group), según los hallazgos del equipo Knownsec 404 y NSFOCUS.

> *«La explotación generalizada de la vulnerabilidad de WinRAR resalta que los exploits para vulnerabilidades conocidas pueden ser muy efectivos, a pesar de que exista un parche disponible. Incluso los atacantes más sofisticados solo realizarán lo necesario para cumplir sus objetivos»,* señaló Kate Morgan, investigadora de TAG.