I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades

Tipo de incidente: Vulnerabilidades

Nivel de riesgo: Alto

II. ALERTA

WinRAR presentaría una vulnerabilidad que se lanzaría como un PoC falso el cual se encontraría en GitHub con la finalidad de que se pueda infectar a los diferentes usuarios que habría descargado el código que tenía incorporado un malware llamado Venom RAT.

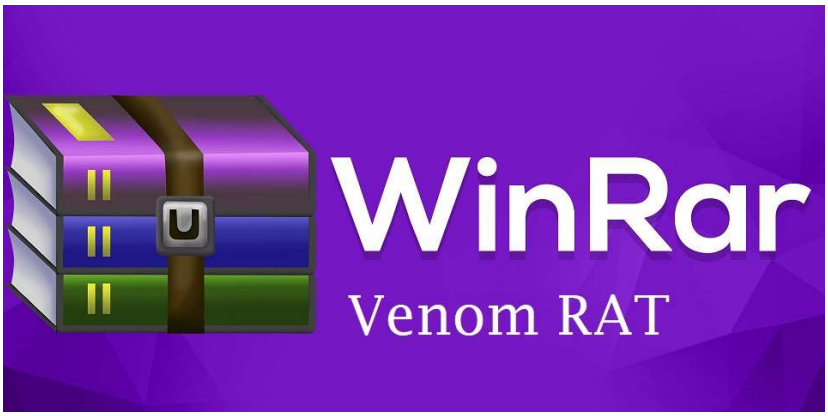

Figura 1.-Ilustración relacionada a WinRAR
Fuente: Elaboración Propia

III. INTRODUCCIÓN

En este caso las vulnerabilidades que se presentan en WinRAR están basadas en un script que se generó principalmente para la explotación de inyección de Sql en una aplicación llamada GeoServer, esto según los investigadores de la Unidad 42 de Palo Alto Network.

Pues bien en el paso de las PoC falsas que ya se han convertido en una de las tácticas ya documentadas para el ataque a la comunidad de investigación, pero firmas de ciberseguridad estarían apostando a que estos ataques lo que generan es una forma de oportunidad a otros delincuentes que estaría tomando como ejemplo estas vulnerabilidades para tenerlas en cuenta en su arsenal.

Este hecho se habría producido el 21 de agosto a tan solo 4 días de que se divulgara públicamente de que existía la vulnerabilidad, la cuenta en la cual se alojaba el repositorio ya no tiene accesibilidad, y con estas vulnerabilidades se podría realizar la toma del RCE (Remote Code Execution) de un ordenador, adjuntamente a esto sea publicado un video en el cual se muestra la manera en la que se logra ejecutar el código el cual atrajo únicamente 121 visitas en total.

Aunque la diferente de la ejecución de este script en es python que este llegaría a un servidor remoto y de esta manera recuperar un ejecutable el cual sería Windows.Gaming.Preview.exe que actuaría como una de las variable del malware Venom Rat ya que este tendría la capacidad de enumerar los diferentes procesos de ejecución los cuales recibirían diferentes comandos controlado por un servidor de actores.

IV. VECTOR DE ATAQUE:

- Toma de control del sistema operativo .

V. IMPACTO:

- Escalabilidad de privilegios.
- Divulgación de información pública.
- Fallas en la ejecución de códigos remotos.

VI. RECOMENDACIONES:

- Verificar las descargas que se realice al equipo.
- Conocer que las PoC que se están yendo a practicar este verificadas y presente la información necesaria.
- Aislar productos que muestren un riesgo para los equipos que nos sea productos actualizados.

VII. REFERENCIAS:

- NIST. CVE-2023-25157. (03 de 03 de 2023). Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2023-25157
- NIST. CVE-2023-38831. (08 de 09 de 2023). Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2023-38831
- Hacker News Fake Researcher Profiles (14 de 06 de 2023). Obtenido de https://thehackernews.com/2023/06/fake-researcher-profiles-spread-malware.html
- Hacker News Winrar Security Flaw Exploited (24 de 08 de 2023). Obtenido de https://thehackernews.com/2023/08/winrar-security-flaw-exploited-in-zero.html