I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades

Tipo de incidente: Vulnerabilidades

Nivel de riesgo: Alto

II. ALERTA

En Windows a sido atacado por una nueva cepa del malware ZenRat el cual está generando una problemática ya que esta incrustado en los paquetes de instalación en uno de los gestores de contraseñas que etaria usando Windows como lo es Bitwarden.

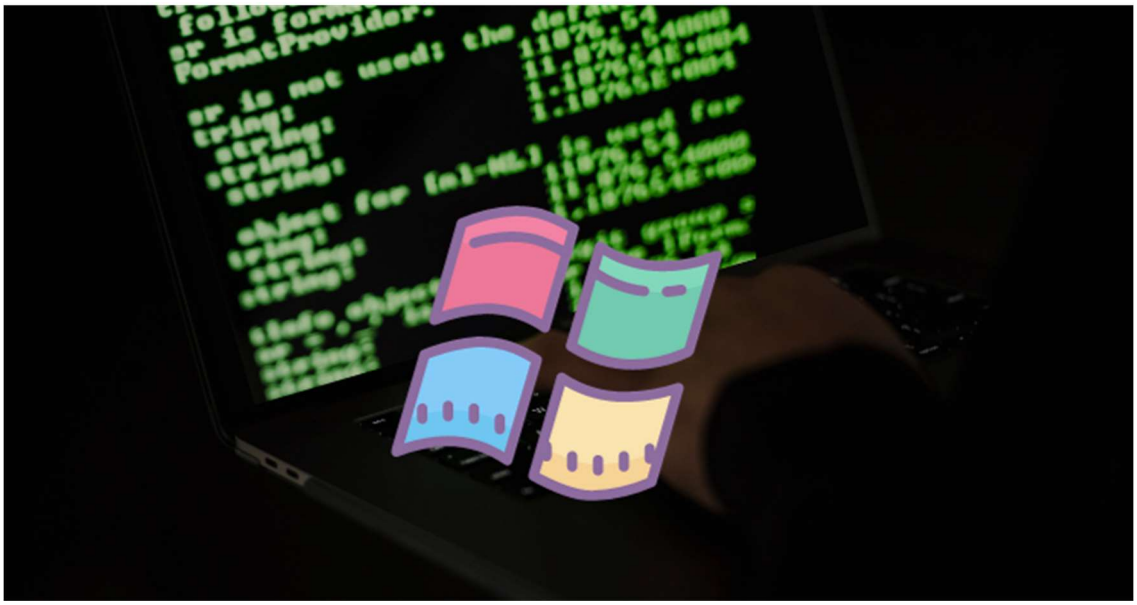

Figura 1.-Ilustración relacionada a Windows y ZenRat
Fuente: https://www.blackhatethicalhacking.com

III. INTRODUCCIÓN

En este momento ha surgido una nueva cepa del malware llamado ZenRat el que estaría enfocado a diferentes usuarios de Windows los cuales al acceder a unas páginas web falsas con un gestor de contraseñas el cual en este caso sea Bitwarden pero aún no se tiene del todo claro de cómo estarían redirigiendo el tráfico de los diferentes dominios.

Para la propagación de este malware que es un troyano modular de acceso remoto el cual generaría brechas en la seguridad del sistema operativo lo que haría que se podría tener un robo de información y la manera en la que se estaría propagando más rápido ese ataque, seria por medio de phishing, publicidad maliciosa, envenenamiento del SEO en el pasado.

Un análisis de los metadatos del instalador revela intentos por parte del actor de amenazas de enmascarar el malware como Speccy de Piriform, una utilidad gratuita de Windows para mostrar información de hardware y software teniendo en cuenta que ZenRat una vez que ya recopila información de detallada sobre el Host en el cual estaría este alojado, como por ejemplo CPU, nombre del GPU y la versión del sistema operativo y software que se esté encargado del tema de la seguridad.

ZenRat también se puede configurar para enviar sus registros en texto plano al servidor, lo que captura una serie de comprobaciones del sistema realizadas por el malware y el estado de ejecución de cada módulo, lo que indica su uso como un "implante modular extensible".

IV. VECTOR DE ATAQUE:

- Robo y propagación de información.

V. IMPACTO:

- Instalación de extensiones y software malicioso.
- Liberación de contraseñas.
- Robo de Información Pública.

VI. RECOMENDACIONES:

- Aislar productos que muestren un riesgo para los equipos que nos sea productos actualizados.
- Informar a usuarios respecto de amenazas provenientes en enlaces remitidos a través de correos electrónicos.
- Restringir la interacción con sitios web respecto de actividades de descarga y ejecución de archivos.

VII. REFERENCIAS:

- Proofpoint. (26 de 09 de 2023). Obtenido de https://www.proofpoint.com/us/blog/threat-insight/zenrat-malware-brings-more-chaos-calm

- BlackHat Malware ZenRat. (28 de 09 de 2023). Obtenido de https://www.blackhatethicalhacking.com/news/zenrat-malware-disguised-as-bitwarden-password-manager-targets-windows-users/

- The Hacker News (27 de 08 de 2023). Obtenido de https://thehackernews.com/2023/09/new-zenrat-malware-targeting-windows.html