I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Remote Access Trojan RAT

Nivel de riesgo: Alto

II. ALERTA

Se ha detectado que el grupo malicioso APT37 conocido como RedEyes, ha desarrollado una nueva herramienta de tipo malware que estaría siendo activamente usada junto a técnicas de estenografía, en campañas de ataque contra activos de información de carácter personal

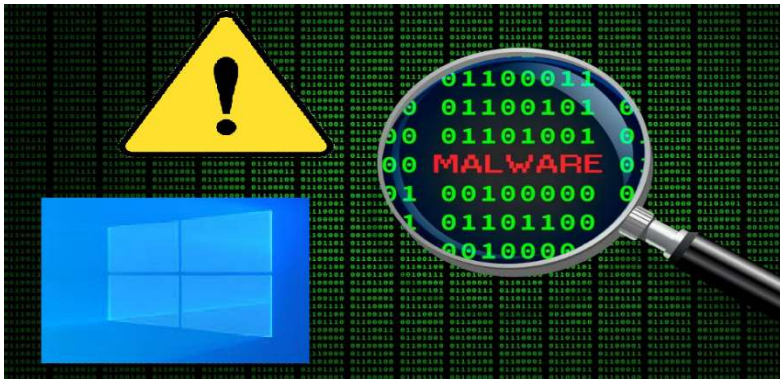

Figura 1.- lustraciones relacionada a detección de malware en Windows
Fuente: Elaboración Propia

III. INTRODUCCIÓN

M2RAT es un programa malicioso (malware) cuya operación se basa en la funcionalidad de un malware de tipo remote Access trojan RAT y sobre este se ejecutan procedimientos de registro y copia de teclas presionadas (keylogging), robo de información, ejecución de comandos y scripts, y captura de pantalla. M2RAT tiene características de diseño enfocadas a dejar pocos rastros de su actividad.

Respecto de las características de la campaña detectada, cabe señalar el interés de los atacantes en obtener información sensible de los usuarios de los sistemas de información comprometidos. M2RAT ejecuta un profundo proceso de recolección de datos para actividades de inteligencia y así determinar los ámbitos sujetos a extorsión, chantaje y robo de identidad.

Uno de los factores técnicos más importantes relacionados a esta campaña maliciosa es la vulnerabilidad existente en la aplicación de procesamiento de texto Hangul, que habilita una Shell la cual a su vez concluye el proceso de descarga de componentes maliciosos para comprometimiento de los sistemas de información.

IV. VECTOR DE ATAQUE:

- Archivos adjuntos a correos electrónicos.
- Ventanas de publicidad maliciosas.
- Ataques de ingeniería social
- Aplicaciones y Programas Informáticos con vulnerabilidades de comprometimiento y ejecución arbitraria de código.

V. IMPACTO:

- Comprometimiento total de sistemas de información vulnerables y ejecución de subsiguientes actividades maliciosas contra otros sistemas de información.
- Chantaje y afectación a la reputación de las personas titulares de información sensible de tipo personal.

VI. INDICADORES DE COMPROMISO

De acuerdo a la información técnica relacionada con la explotación de las vulnerabilidades registradas en CVE-2017-8291 se ha establecido un registro de IOC según el siguiente detalle:

Tipo	Dato
MD5	8b666fc04af6de45c804d973583c76e0 93c66ee424daf4c5590e21182592672e 7bab405fbc6af65680443ae95c30595d 9083c1ff01ad8fabbcd8af1b63b77e66 4488c709970833b5043c0b0ea2ec9fa9 7f5a72be826ea2fe5f11a16da0178e5

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Mantener el sistema operativo Windows actualizado.
- Instalar y mantener actualizado un programa antivirus.
- No abrir y ejecutar los archivos adjuntos en correos electrónicos de fuentes desconocidas.

VIII. DESCARGO DE RESPONSABILIDAD.-

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- Meskauskas, T.PC RISK. How to remove M2RAT malware. (22 de 02 de 2023). Obtenido de https://www.pcrisk.com/removal-guides/26082-m2rat-malware.
- NIST. CVE-2017-8291. (01 de 04 de 2023). Obtenido de https://nvd.nist.gov/vuln/detail/cve-2017-8291
- Toulas, B. Bleepingcomputer.com, RedEyes hackers use new malware to steal data from Windows, phone. (14 de 02 de 2023). Obtenido de https://www.bleepingcomputer.com/news/security/redeyes-hackers-use-new-malware-to-steal-data-from-windows-phones/