I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Infostealer

Nivel de riesgo: Medio

II. ALERTA

Actores maliciosos estarían utilizando mecanismos de Inteligencia Artificial para la generación de videos en Youtube, que a su vez distribuyan una variedad de programas maliciosos malware, especializados en el robo de información.

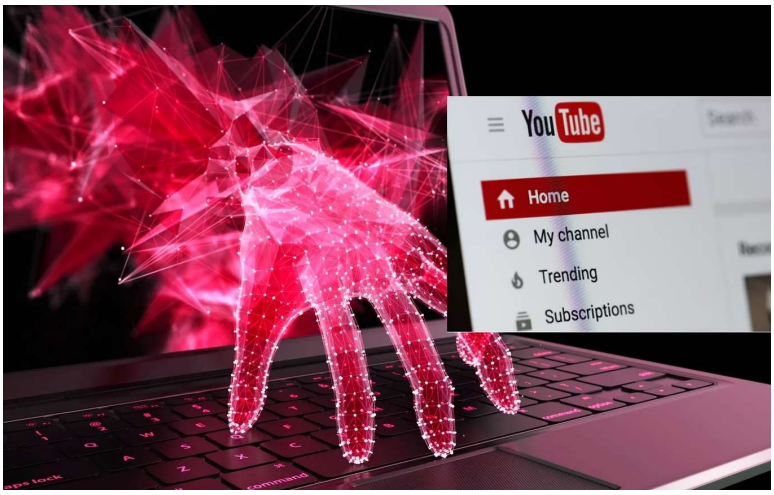

Figura 1.- lustraciones relacionada a detección de malware en Windows
Fuente: Elaboración Propia

III. INTRODUCCIÓN

Los programas maliciosos para la captura y filtración de información (info stealer) son programas diseñados para recolectar información que ingresa, se procesa, y transmite en un sistema de información para fines maliciosos. De manera general, los activos de información más buscados son credenciales de acceso.

Ciber atacantes crean diversos mecanismos para atraer a posibles víctimas. Uno de los medios utilizados es la creación de videos en la plataforma youtube, con temas relacionados como descargar programas y aplicaciones sin necesidad de pagar por el derecho de acceso o instalación. Estos videos están enfocados a aplicaciones populares tales como Photoshop, Autodesk, Microsoft Office, etc.

Dentro de esta campaña de ataque, se han detectado principalmente las variantes SYS01stealer, S1deload, Stealc, Titan, ImBetter, WhiteSnake y Lumma; así como también el sniffer R3NIN.

IV. VECTOR DE ATAQUE:

- Enlaces incluidos en correos electrónicos.
- Vídeos en youtube.

V. IMPACTO:

- Filtración de activos de información.
- Comprometimiento de credenciales de acceso y sistemas de información.

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	01f76140374da14b72a8f1e648cb8f46590419cddd56bc089e67f38cee767735 7f54dc5ddab4de19c5ad7c7b6d4398bd07d97504cdedabc398a6d6db52fe9875 bad4de1c398954b9c381d91fee52607b78e1c65bd9f38c3e82a307e236a76223 2c58bfbf8d274434e3307a76a37720d09387978e8e401780048992ea21fd222b

	c81175d56aa006ad140799e39c800306b439ea98b9efc4491c269eccbfeebd4e c636ed3b0ca558a92687f60f0b37c0e44ff3a6d4f15acd3cfb858fee4b0b0916 833b871f342ba7b0e852363ed123682b99588888f01567e56942889d886bb4b2 daba97a67f219443ef4b0a39e2d051179d20de6a2febb927bec4108dcac1b3a6 5698feaacd122f75d69ed1d9a561ab7210051031e821b934b3022d48a185443b f58b9794f5b973625551333f469878c1df65302733f9a3e9a214e3739cee09bf

VII. RECOMENDACIONES:

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

- Instalar y mantener actualizado un programa antivirus.
- No abrir y ejecutar los enlaces y archivos adjuntos en correos electrónicos de fuentes desconocidas.
- No descargar programas y aplicaciones desde lugares diferentes a los sitios propios de los desarrolladores.

VIII. REFERENCIAS:

- Lakshmanan, R.The Hacker News. Warning: AI-generated Youtube Video Tutorials Spreading Infostealer Malware. (13 de 03 de 2023). Obtenido de https://thehackernews.com/2023/03/warning-ai-generated-youtube-video.html.
- Osipov, A. Morphisec, How SYS01 Stealer will get your sensitive facebook info. (7 de 03 de 2023). Obtenido de https://blog.morphisec.com/sys01stealer-facebook-info-stealer