Los rastreadores de amenazas han desvelado las recientes estratagemas adoptadas por una cepa de malware llamada GuLoader con el objetivo de dificultar el análisis.

> *«Si bien la funcionalidad central de GuLoader no ha experimentado cambios significativos en los últimos años, estas continuas actualizaciones en sus técnicas de ofuscación hacen que analizar GuLoader sea un proceso que requiere mucho tiempo y recursos»*, afirmó Daniel Stepanic, investigador de Elastic Security Labs, en un informe publicado esta semana.

Identificado por primera vez a finales de 2019, GuLoader (también conocido como CloudEyE) es un descargador de malware avanzado basado en shellcode que se emplea para distribuir una variedad de cargas útiles, como robadores de información, y que incorpora un conjunto de sofisticadas técnicas anti-análisis para evadir las soluciones de seguridad tradicionales.

Una serie constante de informes de código abierto sobre el malware en los últimos meses ha revelado que los actores de amenazas detrás de GuLoader han continuado mejorando su capacidad para eludir funciones de seguridad existentes o nuevas, junto con otras características implementadas.

GuLoader suele propagarse mediante campañas de phishing, en las que las víctimas son engañadas para descargar e instalar el malware a través de correos electrónicos que contienen archivos ZIP o enlaces que incluyen un archivo de Visual Basic Script (VBScript).

> En septiembre de 2023, la empresa israelí de ciberseguridad Check Point reveló que *«GuLoader ahora se vende bajo un nuevo nombre en la misma plataforma que Remcos y se promociona de manera implícita como un crypter que hace que su carga útil sea completamente indetectable por los antivirus».*

Uno de los cambios recientes en el malware es una mejora en una técnica anti-análisis

revelada por CrowdStroke en diciembre de 2022 y que se centra en su capacidad de Manejo de Excepciones Vectorizadas (VEH).

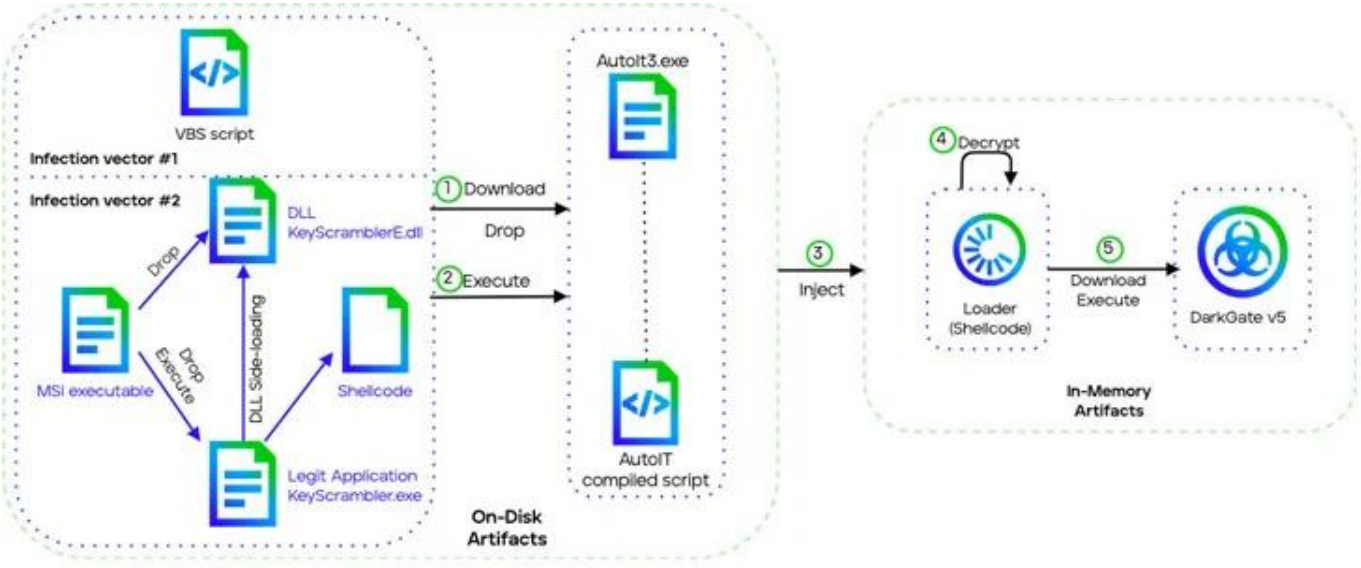
Es relevante señalar que el mecanismo fue detallado anteriormente tanto por McAfee Labs como por Check Point en mayo de 2023, siendo que el primero afirmó que *«GuLoader emplea VEH principalmente para ofuscar el flujo de ejecución y ralentizar el análisis».*

> El método *«consiste en interrumpir el flujo normal de ejecución de código al lanzar deliberadamente un gran número de excepciones y manejarlas en un manejador de excepciones vectorizado que transfiere el control a una dirección calculada dinámicamente»,* según Check Point.

GuLoader está lejos de ser la única familia de malware que recibe actualizaciones constantes. Otro ejemplo destacado es DarkGate, un troyano de acceso remoto (RAT) que permite a los atacantes comprometer completamente los sistemas de las víctimas.

Vendido como malware como servicio (MaaS) por un actor conocido como RastaFarEye en foros clandestinos por una tarifa mensual de $15,000, el malware utiliza correos electrónicos de phishing que contienen enlaces para distribuir el vector de infección inicial: un archivo VBScript o un instalador de software de Microsoft (MSI).

Trellix, que analizó la última versión de DarkGate (5.0.19), indicó que *«introduce una nueva cadena de ejecución que utiliza la carga lateral de DLL y shellcodes y cargadores mejorados»*. Además, viene con una revisión completa de la función de robo de contraseñas de RDP.



> *«El actor de amenazas ha estado monitoreando activamente los informes de amenazas para realizar cambios rápidos, evitando así las detecciones»*, señalaron los investigadores de seguridad Ernesto Fernández Provecho, Pham Duy Phuc, Ciana Driscoll y Vinoo Thomas.

> *«Su capacidad de adaptación, la rapidez con la que itera y la profundidad de sus métodos de evasión atestiguan la sofisticación de las amenazas de malware modernas».*

Este desarrollo se produce en un momento en que troyanos de acceso remoto como Agent Tesla y AsyncRAT han sido observados propagándose mediante nuevas cadenas de infección basadas en correo electrónico que aprovechan la esteganografía y tipos de archivo poco comunes en un intento de eludir las medidas de detección de antivirus.

También sigue a un informe del equipo de inteligencia de amenazas HUMAN Satori sobre cómo una versión actualizada de un motor de obfuscación de malware llamado ScrubCrypt

(también conocido como BatCloak) se utiliza para entregar el malware RedLine Stealer.

> *«La nueva compilación de ScrubCrypt se vendió a actores de amenazas en un pequeño puñado de mercados de la web oscura, incluidos Nulled Forum, Cracked Forum y Hack Forums»*, dijo la empresa.