Investigadores en ciberseguridad han alertado sobre un nuevo y sofisticado malware llamado CoffeeLoader, diseñado para descargar y ejecutar cargas maliciosas secundarias.

Según Zscaler ThreatLabz, este malware comparte similitudes en su comportamiento con otro cargador de malware conocido como SmokeLoader.

> *«El propósito del malware es descargar y ejecutar cargas útiles de segunda etapa mientras evade la detección de productos de seguridad basados en endpoints»,* explicó Brett Stone-Gross, director senior de inteligencia de amenazas en Zscaler, en un análisis técnico publicado esta semana.
>
> *«El malware emplea diversas técnicas para evadir soluciones de seguridad, incluyendo un empaquetador especializado que utiliza la GPU, suplantación de la pila de llamadas (call stack spoofing), ofuscación de tiempos de espera (sleep obfuscation) y el uso de fibras de Windows».*

Características clave de CoffeeLoader

CoffeeLoader, que comenzó a circular en septiembre de 2024, utiliza un algoritmo de generación de dominios (DGA) como mecanismo de respaldo en caso de que sus canales de comando y control (C2) principales sean inaccesibles.

Uno de los elementos centrales del malware es un empaquetador denominado Armoury, que ejecuta código en la GPU del sistema para dificultar su análisis en entornos virtuales. Su nombre proviene del hecho de que se hace pasar por la herramienta legítima Armoury Crate de ASUS.

Proceso de infección

La secuencia de infección comienza con un dropper (cargador inicial) que intenta ejecutar

una carga maliciosa en formato DLL empaquetada por Armoury («ArmouryAIOSDK.dll» o «ArmouryA.dll») con privilegios elevados. Si el dropper no cuenta con los permisos necesarios, primero intentará evadir el Control de Cuentas de Usuario (UAC).

Además, este dropper está diseñado para mantener persistencia en el sistema mediante la creación de una tarea programada que se ejecuta al iniciar sesión del usuario con el nivel de privilegio más alto o cada 10 minutos. Posteriormente, se ejecuta un stager, que a su vez carga el módulo principal del malware.

> *«El módulo principal implementa numerosas técnicas para evadir la detección de antivirus (AV) y soluciones de detección y respuesta en endpoints (EDR), incluyendo la suplantación de la pila de llamadas, la ofuscación de tiempos de espera y el uso de Fibras de Windows«,* afirmó Stone-Gross.

Estos métodos permiten falsificar la pila de llamadas para ocultar el origen de una función maliciosa y ofuscar la carga útil mientras el malware se encuentra en estado de espera, lo que dificulta su detección por parte del software de seguridad.

Objetivo final de CoffeeLoader

El propósito final del malware es contactar un servidor C2 a través de HTTPS para recibir instrucciones y descargar cargas maliciosas adicionales. Entre estas, se encuentra la capacidad de inyectar y ejecutar shellcode de Rhadamanthys.

Zscaler identificó similitudes a nivel del código fuente entre CoffeeLoader y SmokeLoader, lo que sugiere que podría tratarse de una evolución de este último, especialmente después de que las autoridades desmantelaran su infraestructura el año pasado.

> *«Existen notables similitudes entre SmokeLoader y CoffeeLoader. De hecho, se ha observado que el primero está distribuyendo el segundo, aunque la relación exacta*

> *entre ambas familias de malware aún no está clara»*, señaló la compañía.

Campañas de distribución de malware relacionadas

Esta nueva amenaza surge en paralelo con un informe de Seqrite Labs, que detalla una campaña de phishing diseñada para iniciar una cadena de infección en varias etapas, cuyo resultado final es la instalación del malware Snake Keylogger, especializado en el robo de información.

Además, se ha detectado otra campaña maliciosa dirigida a usuarios interesados en el trading de criptomonedas. A través de publicaciones en Reddit, los atacantes promocionan versiones pirateadas de la plataforma TradingView, con el objetivo de engañar a los usuarios y hacer que descarguen stealers como Lumma y Atomic, tanto en sistemas Windows como en macOS.