Un reciente cargador de software malicioso ha sido adoptado por delincuentes cibernéticos para introducir una diversidad de programas ladrones de datos, tales como Lumma Stealer (conocido también como LummaC2), Vidar, RecordBreaker (identificado como Raccoon Stealer V2) y Rescoms.

La empresa de seguridad informática ESET está monitoreando este troyano con la denominación Win/TrojanDownloader.Rugmi.

> *«Esta amenaza es un cargador que consta de tres segmentos: un módulo de descarga que adquiere un paquete cifrado, un cargador primario que inicia el paquete desde fuentes internas y otro cargador secundario que lo ejecuta desde un documento externo en el sistema»,* comentó la entidad en su Informe de Riesgos de la segunda mitad de 2023.

Las estadísticas recolectadas por ESET indican que las alertas por el cargador Rugmi experimentaron un notable incremento en los meses de octubre y noviembre de 2023, ascendiendo de unos pocos casos diarios a varios centenares por jornada.

Los programas maliciosos ladrones se comercializan frecuentemente bajo la modalidad de software como servicio (SaaS) a otros delincuentes informáticos con una suscripción regular. Por ejemplo, Lumma Stealer se ofrece en plataformas clandestinas por una tarifa mensual de $250. El paquete más avanzado tiene un valor de $20,000, pero también concede a los adquirientes el acceso al código original y el permiso para su comercialización.

Existen pruebas que indican que el código base vinculado a los programas Mars, Arkei y Vidar ha sido transformado para desarrollar Lumma.

Adicionalmente, con el objetivo de eludir sistemas de detección, este instrumento preconfigurado se difunde mediante múltiples técnicas, desde anuncios engañosos hasta simulaciones de actualizaciones de navegadores y versiones pirateadas de aplicaciones reconocidas como VLC media player y OpenAI ChatGPT.

Otro enfoque se relaciona con el aprovechamiento de la infraestructura de entrega de contenido (CDN) de Discord para hospedar y difundir el software malicioso, como señaló Trend Micro en octubre de 2023.

Esto implica usar tanto cuentas aleatorias como comprometidas en Discord para enviar mensajes privados a potenciales objetivos, prometiéndoles una suma de $10 o acceso a una membresía Discord Nitro si colaboran en una tarea.

Aquellos que caen en la trampa son dirigidos a descargar un software que se presenta como iMagic Inventory en el CDN de Discord, pero que en verdad aloja el código malicioso de Lumma Stealer.

> *«ESET mencionó que los paquetes de malware listos para usar facilitan la propagación de campañas nocivas, especialmente entre aquellos delincuentes cibernéticos con menos habilidades técnicas,»* afirmaron.

> *«Al ofrecer características adicionales, Lumma Stealer se vuelve aún más atractivo para potenciales compradores.»*

Las noticias emergieron cuando McAfee Labs informó sobre una versión actualizada de NetSupport RAT, derivada del software legítimo NetSupport Manager y ahora en manos de intermediarios que buscan recopilar datos y llevar a cabo operaciones adicionales en individuos específicos.

«Todo comienza con secuencias de código JavaScript codificadas, sirviendo como la primera barrera para la infección», detalló McAfee, señalando las *«estrategias cambiantes utilizadas por los delincuentes digitales».*

Al ejecutarse, el JavaScript prosigue con el ataque, utilizando comandos de PowerShell para

descargar el malware desde un servidor bajo el control de los atacantes. La campaña tiene como principales blancos a Estados Unidos y Canadá.