Los expertos en seguridad cibernética han descubierto múltiples repositorios en GitHub que ofrecen software pirateado, utilizado para desplegar un programa de robo de información conocido como RisePro.

Esta campaña, identificada como gitgub, engloba 17 repositorios asociados con 11 cuentas diferentes, según lo reportado por G DATA. Los repositorios en cuestión han sido retirados por la subsidiaria de Microsoft desde entonces.

> *«Estos repositorios comparten una apariencia similar, mostrando un archivo README.md que promete software pirateado de manera gratuita»,* señaló la compañía de ciberseguridad alemana.
>
> *«En GitHub, los círculos verdes y rojos son comúnmente empleados para indicar el estado de las compilaciones automáticas. Los actores de amenazas de Gitgub agregaron cuatro círculos Unicode verdes en su README.md, simulando un estado junto con la fecha actual para conferir una sensación de autenticidad y actualidad».*

La lista de repositorios es la siguiente, cada uno de ellos vinculado a un enlace de descarga («digitalxnetwork[.]com») que contiene un archivo RAR:

- andreastanaj/AVAST
- andreastanaj/Sound-Booster
- aymenkort1990/fabfilter
- BenWebsite/-IObit-Smart-Defrag-Crack
- Faharnaqvi/VueScan-Crack
- javisolis123/Voicemod
- lolusuary/AOMEI-Backupper
- lolusuary/Daemon-Tools
- lolusuary/EaseUS-Partition-Master
- lolusuary/SOOTHE-2

- mostofakamaljoy/ccleaner
- rik0v/ManyCam
- Roccinhu/Tenorshare-Reiboot
- Roccinhu/Tenorshare-iCareFone
- True-Oblivion/AOMEI-Partition-Assistant
- vaibhavshiledar/droidkit
- vaibhavshiledar/TOON-BOOM-HARMONY

El archivo RAR, al que se accede mediante una contraseña proporcionada en el archivo README.md del repositorio, contiene un archivo instalador que descomprime la carga útil de la siguiente etapa. Este archivo ejecutable, inflado a 699 MB para dificultar el análisis con herramientas como IDA Pro, actúa como un cargador para inyectar RisePro (versión 1.6) en AppLaunch.exe o RegAsm.exe.

RisePro ganó notoriedad a finales de 2022 cuando se distribuyó utilizando un servicio de descarga de malware basado en pago por instalación (PPI) conocido como PrivateLoader.

Escrito en C++, su función es recopilar datos sensibles de sistemas infectados y enviarlos a dos canales de Telegram, que son comúnmente utilizados por agentes de amenazas para obtener información de las víctimas. Curiosamente, investigaciones recientes de Checkmarx han demostrado la posibilidad de infiltrarse y reenviar mensajes desde el bot de un atacante a otra cuenta de Telegram.

Este desarrollo coincide con el detalle de tácticas y técnicas adoptadas por Snake Keylogger por parte de Splunk, quien lo describe como un malware ladrón que *«emplea un enfoque multifacético para la extracción de datos».*

> *«El uso de FTP permite la transferencia segura de archivos, mientras que SMTP posibilita el envío de correos electrónicos con información sensible. Además, la integración con Telegram proporciona una plataforma de comunicación en tiempo real, permitiendo la transmisión inmediata de datos robados»,* explicó Splunk.

Los malware ladrón se están volviendo cada vez más populares, a menudo convirtiéndose en el principal método de ataque para ransomware y otras brechas de datos de gran impacto. Según un informe de Specops publicado recientemente, RedLine, Vidar y Raccoon son los ladrones más ampliamente utilizados, con RedLine siendo responsable del robo de más de 170,3 millones de contraseñas en los últimos seis meses.

> *«El aumento actual de malware de robo de información nos recuerda la constante evolución de las amenazas digitales. Aunque las motivaciones detrás de su uso suelen ser de naturaleza financiera, los ladrones continúan adaptándose y siendo más accesibles y fáciles de usar»,* observó Flashpoint en enero de 2024.