Investigadores de seguridad cibernética revelaron este martes una estafa de gran alcance dirigida a los usuarios de criptomonedas, que comenzó en enero del año pasado a distribuir aplicaciones troyanizadas para instalar una herramienta de acceso remoto no detectada previamente en los sistemas de destino.

Llamado ElectroRAT por Intezer, el RAT se escribe en Golang y fue diseñado para atacar múltiples sistemas operativos como Windows, Linux y MacOS.

Las aplicaciones se desarrollan utilizando el marco de aplicaciones de escritorio multiplataforma de Electron de código abierto.

> *«ElectroRAT es el último ejemplo de atacantes que utilizan Golang para desarrollar malware multiplataforma y evadir la mayoría de los motores antivirus»,* dijeron los investigadores.
>
> *«Es común ver a varios ladrones de información tratando de recopilar claves privadas para acceder a las billeteras de las víctimas. Sin embargo, es raro ver herramientas escritas desde cero y dirigidas a múltiples sistemas operativos para estos fines».*

Tal parece que la campaña, detectada por primera vez en diciembre, ha cobrado más de 6500 víctimas en función del número de visitantes únicos a las páginas de Pastebin utilizadas para localizar los servidores de Comando y Control (C2).

Operation ElectroRAT involucró a los atacantes creando tres aplicaciones contaminadas diferentes, cada una con una versión para Windows, Linux y Mac, dos de las cuales se hacen pasar por aplicaciones de gestión de comercio de criptomonedas con el nombre de «Jam» y «eTrade», mientras que una tercera se llama «DaoPoker», que se hace pasar por una plataforma de póquer de criptomonedas.

Las aplicaciones maliciosas no solo están alojadas en sitios web creados específicamente para esta campaña, sino que los servicios también se anuncian en Twitter, Telegram y foros legítimos relacionados con criptomonedas y cadenas de bloques como «bitcointalk» y «SteemCoinPan», en un intento de atraer a usuarios desprevenidos para descargar las apps contaminadas.

Una vez instalada, la aplicación abre una interfaz de usuario con apariencia inofensiva, pero en realidad, ElectroRAT se ejecuta oculto en segundo plano como «mdworker», que cuenta con capacidades intrusivas para capturar pulsaciones de teclas, tomar capturas de pantalla, cargar archivos desde el disco, descargar archivos arbitrarios y ejecutar comandos maliciosos recibidos del servidor C2 en la máquina de la víctima.

Un análisis de las páginas de Pastebin, que fueron publicadas por un usuario llamado «Execmac» el 8 enero de 2020, encontró servidores C2 usados junto con malware de Windows como Amadey y KPOT, lo que sugiere que los atacantes han pasado de usar troyanos conocidos a un nuevo RAT capaz de atacar múltiples sistemas operativos.

> *«Otro factor de motivación es que se trata de un malware Golang desconocido, que ha permitido que la campaña vuelve por debajo del radar durante un año al evadir todas las detecciones de antivirus»*, agregaron los investigadores.