Investigadores de seguridad cibernética han identificado un paquete malicioso en el registro de paquetes npm que se presenta como una herramienta para identificar fallos en contratos inteligentes de Ethereum. Sin embargo, en realidad, introduce un troyano de acceso remoto (RAT) de código abierto conocido como Quasar RAT en los sistemas de los desarrolladores.

Este paquete, llamado ethereumvulncontracthandler, fue publicado en npm el 18 de diciembre de 2024 por un usuario identificado como *«solidit-dev-416».* Actualmente, sigue estando disponible para su descarga y ha sido descargado 66 veces.

> *«Al instalarse, descarga un script malicioso desde un servidor remoto, ejecutándolo en segundo plano para instalar el RAT en sistemas Windows»,* señaló Kirill Boychenko, analista de seguridad en Socket, en un informe publicado recientemente.

El código malicioso integrado en ethereumvulncontracthandler está protegido con múltiples capas de técnicas de ofuscación, como codificación Base64 y XOR, además de compactación, lo que dificulta su análisis y detección.

El malware también incluye mecanismos para evitar su ejecución en entornos de pruebas virtuales (sandbox) antes de actuar como un descargador que obtiene y ejecuta una segunda carga desde un servidor remoto («jujuju[.]lat»). Este script utiliza comandos de PowerShell para iniciar la ejecución de Quasar RAT.

El troyano asegura su persistencia mediante cambios en el Registro de Windows y se conecta a un servidor de comando y control (C2) en «captchacdn[.]com:7000», desde donde recibe instrucciones adicionales para recopilar y extraer información.

Quasar RAT, lanzado públicamente en GitHub en julio de 2014, ha sido empleado en diversas campañas de ciberdelincuencia y ciberespionaje por actores maliciosos a lo largo de los años.

> *«El atacante también utiliza este servidor C2 para registrar dispositivos infectados y gestionar varios sistemas comprometidos de manera simultánea, lo que sugiere que esta campaña podría formar parte de una red de bots»*, explicó Boychenko.
>
> *«En esta fase, el equipo de la víctima está completamente comprometido y bajo total control y monitoreo del atacante, listo para recibir nuevas instrucciones o actualizaciones».*

El aumento de estrellas falsas en GitHub

Este descubrimiento coincide con un nuevo estudio realizado por Socket junto con académicos de las universidades Carnegie Mellon y Estatal de Carolina del Norte, que reveló un aumento significativo en el uso de «estrellas» falsas para inflar artificialmente la popularidad de repositorios maliciosos en GitHub.

Aunque este problema no es nuevo, la investigación determinó que la mayoría de estas estrellas fraudulentas se utilizan para promocionar repositorios de malware de corta vida que se hacen pasar por software pirata, trucos para videojuegos y bots de criptomonedas.

Repositorios falsos promocionados por vendedores de estrellas de GitHub como Baddhi Shop, BuyGitHub, FollowDeh, R for Rank y Twidium son responsables de hasta 4.5 millones de estrellas falsas generadas por 1.32 millones de cuentas y que abarcan 22,915 repositorios, mostrando la escala del problema.

Baddhi Shop permite a los clientes adquirir 1,000 estrellas por $110. *«Compra seguidores, estrellas, bifurcaciones y observadores en GitHub para aumentar la credibilidad y visibilidad de tu repositorio»*, se lee en una descripción en su sitio web. *«Una mayor interacción real atrae más desarrolladores y colaboradores a tu proyecto».*

> *«Pocos repositorios con campañas de estrellas falsas llegan a publicarse en*

> *registros como npm o PyPI. Y aún menos logran una adopción significativa. Al menos el 60% de las cuentas involucradas en estas campañas muestran patrones de actividad muy limitados»,* dijeron los investigadores.

Mientras los ataques a la cadena de suministro de software de código abierto siguen siendo una amenaza creciente, estos hallazgos subrayan que el conteo de estrellas no es una métrica confiable de calidad o reputación y no debe considerarse sin un análisis más profundo.

En una declaración a *WIRED* en octubre de 2023, GitHub, propiedad de Microsoft, afirmó que conoce este problema desde hace años y que trabaja activamente para eliminar las cuentas involucradas en la generación de estrellas falsas.

> *«La debilidad principal de la métrica de conteo de estrellas es que todas las acciones de los usuarios de GitHub tienen el mismo peso»,* señalaron los investigadores.

> *«Esto hace que sea fácil inflar el número de estrellas usando cuentas automatizadas o usuarios de bajo perfil. Para contrarrestar este abuso, GitHub podría considerar implementar una métrica ponderada que evalúe la popularidad del repositorio basada en factores como la centralidad de red, lo que sería mucho más difícil de manipular».*