Investigadores en ciberseguridad han detectado una nueva campaña en la que actores maliciosos han publicado más de 67 repositorios en GitHub que aparentan contener herramientas de hacking basadas en Python, pero en realidad distribuyen cargas maliciosas camufladas.

Esta actividad, identificada por ReversingLabs con el nombre en clave *Banana Squad*, parece ser una continuación de una operación maliciosa que ya había sido detectada en 2023. En aquella ocasión, se utilizaban paquetes falsos en el repositorio Python Package Index (PyPI), los cuales fueron descargados más de 75,000 veces y estaban diseñados para robar información en sistemas Windows.

Los hallazgos amplían lo reportado previamente por el *Internet Storm Center* del SANS en noviembre de 2024, donde se describía una herramienta falsa llamada *steam-account-checker* alojada en GitHub. Esta herramienta tenía la capacidad de descargar sigilosamente otros scripts en Python para insertar código malicioso en la aplicación de billetera de criptomonedas *Exodus*, y así extraer datos sensibles hacia un servidor externo ("dieserbenni[.]ru").

El análisis más profundo del repositorio y de la infraestructura controlada por los atacantes llevó al descubrimiento de 67 repositorios en GitHub que imitan nombres de proyectos legítimos para engañar a los usuarios.

Hay indicios de que esta campaña apunta a personas que buscan programas como limpiadores de cuentas o trampas para videojuegos, incluyendo herramientas como *Discord account cleaner*, *Fortnite External Cheat*, *TikTok username checker* y *PayPal bulk account checker*. Todos los repositorios detectados han sido eliminados por GitHub.

> *"El uso de puertas traseras y código malicioso en repositorios públicos como los de GitHub está en aumento, y representa un riesgo creciente en la cadena de suministro de software,"* afirmó Robert Simmons, investigador de ReversingLabs.

> *"Para los desarrolladores que dependen de plataformas de código abierto, es fundamental verificar siempre que el repositorio realmente contenga lo que promete."*

GitHub como vector para distribuir malware

Este descubrimiento ocurre en un momento en que GitHub se ha convertido cada vez más en el objetivo de campañas que lo utilizan como canal para distribuir malware. Esta misma semana, Trend Micro informó haber identificado 76 repositorios maliciosos en GitHub operados por un grupo denominado *Water Curse*, utilizados para propagar malware en múltiples etapas.

Estas cargas están diseñadas para robar credenciales, información del navegador y tokens de sesión, además de brindar acceso remoto persistente a los sistemas comprometidos.

Por otro lado, Check Point reveló otra campaña que emplea un servicio criminal conocido como *Stargazers Ghost Network*, el cual apunta a usuarios de Minecraft utilizando malware escrito en Java. *Stargazers Ghost Network* hace referencia a una red de cuentas en GitHub que propagan malware o enlaces dañinos mediante repositorios de phishing.

> *"La red está compuesta por múltiples cuentas que distribuyen enlaces maliciosos y malware, y realizan acciones como marcar con estrellas, bifurcar y suscribirse a repositorios maliciosos para hacerlos parecer legítimos,"* indicó Check Point.

La compañía de ciberseguridad también concluyó que estas *"cuentas fantasma en GitHub son solo una parte del panorama general, con otras cuentas similares operando en diferentes plataformas como parte de un ecosistema mayor de Distribución-como-Servicio."*

Algunos aspectos de esta red fueron expuestos por Checkmarx en abril de 2024, destacando el patrón del grupo atacante de usar estrellas falsas y actualizaciones frecuentes para inflar

artificialmente la visibilidad de los repositorios en los resultados de búsqueda de GitHub.

Estos proyectos maliciosos están hábilmente disfrazados como herramientas legítimas relacionadas con videojuegos populares, trampas, rastreadores de precios de criptomonedas o predictores de multiplicadores en juegos de apuestas.

Estas campañas también coinciden con otra ola de ataques dirigida a cibercriminales novatos que buscan malware y herramientas listas para usar en GitHub, siendo infectados a través de repositorios con puertas traseras.

En un caso reportado este mes por Sophos, se descubrió que el repositorio *Sakura-RAT*, que contenía un troyano, infectaba a quienes compilaban el código en sus sistemas, instalando *stealers* de información y troyanos de acceso remoto (RATs).

Los repositorios identificados contienen hasta cuatro tipos distintos de puertas traseras, integradas en eventos *PreBuild* de Visual Studio, scripts en Python, archivos de salvapantallas y código JavaScript. Estas puertas traseras permiten robar datos, tomar capturas de pantalla, comunicarse por Telegram y descargar más malware como *AsyncRAT*, *Remcos RAT* y *Lumma Stealer*.

En total, Sophos indicó haber detectado al menos 133 repositorios comprometidos como parte de esta campaña, 111 de los cuales contenían la puerta trasera en *PreBuild*, mientras que los demás incluían backdoors en Python, salvapantallas o JavaScript.

Sophos añadió que estas actividades probablemente forman parte de una operación de distribución-como-servicio activa desde agosto de 2022, que ha utilizado miles de cuentas en GitHub para difundir malware incrustado en proyectos relacionados con trampas de videojuegos, exploits y herramientas de ataque.

Aunque no está claro el método exacto de distribución empleado, se sospecha que los actores también están aprovechando servidores de Discord y canales de YouTube para compartir enlaces a los repositorios maliciosos.

> *"No está confirmado si esta campaña está relacionada directamente con otras previamente identificadas, pero el enfoque parece ser efectivo y probablemente continúe bajo otras formas,"* señaló Sophos.
>
> *"En el futuro, es posible que el objetivo se desplace, y los atacantes enfoquen sus esfuerzos en otros grupos además de los cibercriminales inexpertos y jugadores que usan trampas."*

Chet Wisniewski, director y CISO de campo en Sophos, declaró que *"hay similitudes llamativas"* entre esta campaña y *Water Curse*. Estas incluyen:

- Repositorios con nombres casi idénticos
- Uso extensivo de cuentas en GitHub
- Enfoque común en aplicaciones desarrolladas con Electron
- Uso similar de los eventos *PreBuild* en Visual Studio
- Una referencia al correo electrónico "ischhfd83" ("ischhfd83@rambler[.]ru") como autor de los commits en GitHub

> *"Si estas campañas están directamente conectadas o simplemente forman parte de un mismo conjunto de amenazas que comparte código y metodología, es algo que requiere más investigación,"* concluyó Wisniewski.