Investigadores de ciberseguridad han identificado tres módulos maliciosos escritos en Go que contienen código ofuscado diseñado para descargar cargas útiles adicionales que pueden sobrescribir de forma irreversible el disco principal de un sistema Linux, dejándolo inutilizable e incapaz de arrancar.

Los paquetes maliciosos detectados son:

- `github[.]com/truthfulpharm/prototransform`
- `github[.]com/blankloggia/go-mcp`
- `github[.]com/steelpoor/tlsproxy`

A pesar de parecer módulos legítimos, contenían código altamente ofuscado para conectarse a servidores remotos y ejecutar cargas destructivas, explicó Kush Pandya, investigador de Socket.

El código verifica si el sistema operativo es Linux y, en ese caso, descarga un script desde un servidor remoto usando `wget`. Este script malicioso sobrescribe completamente el disco principal (`/dev/sda`) con ceros, lo que impide que el sistema vuelva a arrancar.

> *«Este método destruye los datos de forma permanente, imposibilitando su recuperación incluso con herramientas forenses»*, indicó Pandya.

El ataque puede paralizar por completo servidores Linux o entornos de desarrollo, demostrando el alto riesgo que representan las amenazas en la cadena de suministro, donde código aparentemente confiable puede convertirse en un arma devastadora.

Otras amenazas detectadas en paquetes npm y PyPI

Esta revelación coincide con el hallazgo de varios paquetes maliciosos en el registro de npm, diseñados para robar frases semilla (mnemonic seed phrases) y claves privadas de criptomonedas, así como para exfiltrar información sensible. Estos fueron identificados por

Socket, Sonatype y Fortinet.

- crypto-encrypt-ts
- react-native-scrollpageviewtest
- bankingbundleserv
- buttonfactoryserv-paypal
- tommyboytesting
- compliancereadserv-paypal
- oauth2-paypal
- paymentapiplatformservice-paypal
- userbridge-paypal
- userrelationship-paypal

En el repositorio de PyPI también se descubrieron paquetes con funcionalidades similares, como `web3x` y `herewalletbot`, que han sido descargados más de 6.800 veces desde su publicación en 2024.

Paquetes PyPI que usan servidores de Gmail y WebSockets

Otro grupo de siete paquetes en PyPI utilizaba servidores SMTP de Gmail y conexiones WebSocket para exfiltrar datos y ejecutar comandos de forma remota, evitando así ser detectados. Estos paquetes han sido eliminados, pero usaban credenciales incrustadas de cuentas de Gmail para enviar mensajes que confirmaban la infección y luego establecían una conexión bidireccional con los atacantes.

- cfc-bsb (2,913 downloads)
- coffin2022 (6,571 downloads)
- coffin-codes-2022 (18,126 downloads)
- coffin-codes-net (6,144 downloads)
- coffin-codes-net2 (6,238 downloads)
- coffin-codes-pro (9,012 downloads)
- coffin-grave (6,544 downloads)

Los atacantes se aprovechan de la confianza que las redes corporativas suelen tener en los dominios de Gmail (`smtp.gmail[.]com`), lo que les permite evadir los controles de seguridad tradicionales.

Uno de los paquetes, llamado `cfc-bsb`, no usa Gmail pero sí implementa la lógica de WebSocket para facilitar el acceso remoto.

Recomendaciones de seguridad

Para reducir el riesgo de estas amenazas en la cadena de suministro, se recomienda a los desarrolladores:

- Verificar la autenticidad de los paquetes, revisando el historial del publicador y los enlaces a repositorios en GitHub.
- Auditar regularmente las dependencias del proyecto.
- Restringir el acceso a llaves privadas.
- Supervisar conexiones salientes inusuales, especialmente el tráfico SMTP, ya que puede indicar intento de robo de datos a través de servicios legítimos como Gmail.

> *«El hecho de que un paquete haya existido durante años sin ser eliminado no significa que sea confiable»,* advirtió Olivia Brown, también de Socket.