Investigadores de ciberseguridad han alertado sobre un ataque a la cadena de suministro de software que afecta al ecosistema de Go. Este ataque implica un paquete malicioso diseñado para otorgar a los atacantes acceso remoto a los sistemas comprometidos.

El paquete en cuestión, llamado `github.com/boltdb-go/bolt`, es una imitación del módulo legítimo de la base de datos BoltDB (`github.com/boltdb/bolt`), según el informe de Socket. La versión maliciosa (1.3.1) se subió a GitHub en noviembre de 2021 y, posteriormente, quedó almacenada indefinidamente en la caché del servicio Go Module Mirror.

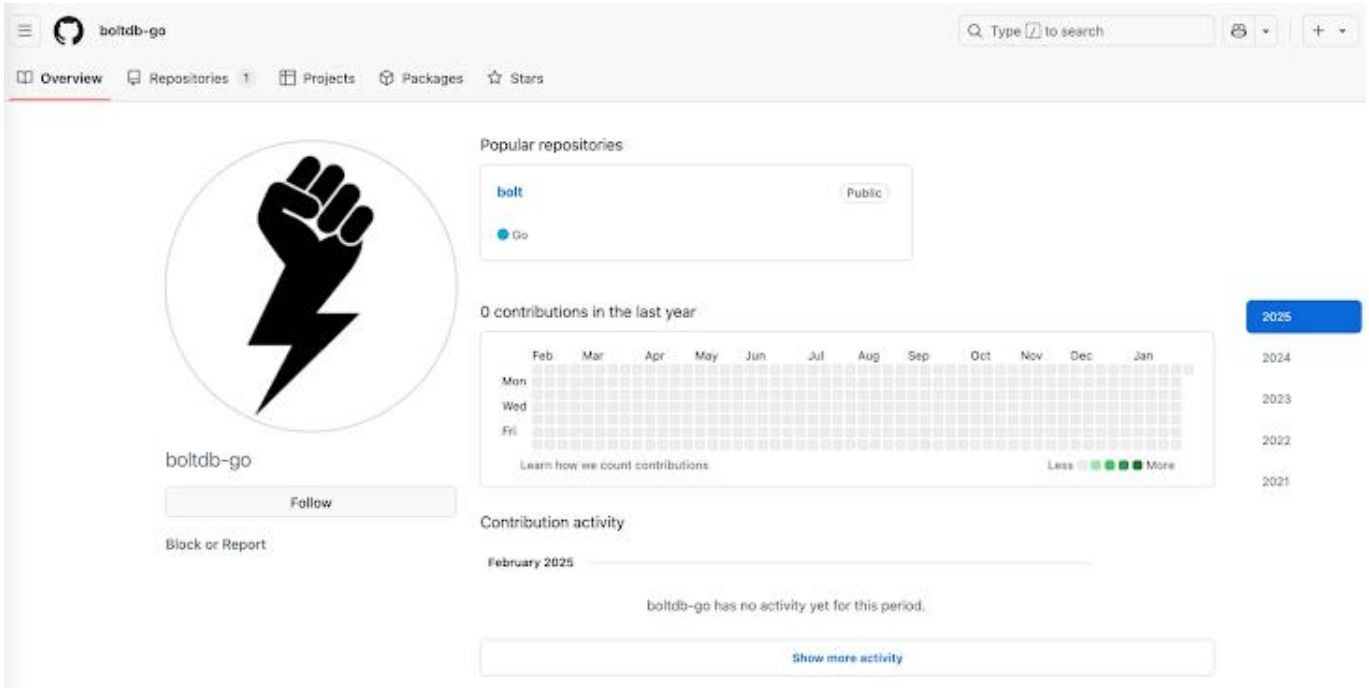
> *«Cuando se instala, este paquete alterado permite a los atacantes controlar el sistema infectado de forma remota y ejecutar comandos arbitrarios»,* explicó el investigador de seguridad Kirill Boychenko en su análisis.

Socket señaló que este incidente representa uno de los primeros casos documentados en los que un actor malicioso ha aprovechado la persistencia del almacenamiento en caché de Go Module Mirror para inducir a error a los desarrolladores y hacer que descarguen software malicioso. Más tarde, el atacante modificó las etiquetas de Git en el repositorio original para que apuntaran a una versión legítima.

Gracias a esta táctica engañosa, una revisión manual del repositorio en GitHub no mostraba ninguna actividad sospechosa. Además, el almacenamiento en caché garantizaba que los desarrolladores que instalaban el paquete a través de la interfaz de línea de comandos de Go continuaran obteniendo la versión infectada.

> *«Cuando una versión de un módulo es almacenada en caché, sigue estando disponible a través del Go Module Proxy, incluso si el código fuente original se modifica después. Aunque este sistema es útil para propósitos legítimos, en este caso fue explotado por el atacante para distribuir código malicioso de manera persistente, a pesar de los cambios posteriores en el repositorio»,* señaló

> Boychenko.



> *«Dado que los módulos inmutables ofrecen tanto ventajas de seguridad como riesgos de abuso, los desarrolladores y equipos de seguridad deben estar atentos a ataques que se aprovechen de versiones almacenadas en caché para evadir la detección».*

Este incidente ocurre mientras la empresa Cycode ha identificado tres paquetes maliciosos en npm – *serve-static-corell*, *openssl-node* y *next-refresh-token* – que contenían código oculto para recopilar información del sistema y ejecutar instrucciones enviadas por un servidor remoto («8.152.163[.]60») en el sistema infectado.