Investigadores en ciberseguridad han revelado detalles sobre un nuevo backdoor desarrollado en Golang que emplea Telegram como medio de comunicación para comando y control (C2).

Netskope Threat Labs, que analizó el funcionamiento del malware, señaló que podría tener origen ruso.

> *"El malware está programado en Golang y, al ejecutarse, opera como un backdoor. Aunque aún parece estar en desarrollo, cuenta con todas las funcionalidades necesarias"*, explicó el investigador de seguridad Leandro Fróes en un informe publicado la semana pasada.

Al activarse, el backdoor verifica si se está ejecutando en una ubicación y con un nombre específicos – «C:\Windows\Temp\svchost.exe» – y, si no es el caso, lee su propio código, lo copia en esa ruta y crea un nuevo proceso para iniciar la versión clonada antes de cerrarse a sí mismo.

Un aspecto distintivo de este malware es que emplea una biblioteca de código abierto que permite la integración de Golang con la API de bots de Telegram para propósitos de C2.

Esto le permite interactuar con la API de Telegram para recibir comandos desde un chat controlado por el atacante. Actualmente, admite cuatro comandos, aunque solo tres están operativos:

- /cmd – Ejecuta órdenes mediante PowerShell
- /persist – Se reinstala en «C:\Windows\Temp\svchost.exe»
- /screenshot – No implementado
- /selfdestruct – Borra el archivo «C:\Windows\Temp\svchost.exe» y se cierra

Los resultados de estos comandos se envían de vuelta al canal de Telegram. Netskope destacó que, aunque la función «/screenshot» no está completamente desarrollada, sigue

enviando el mensaje «Screenshot captured» (Captura de pantalla tomada).

El posible origen ruso del malware se deduce del hecho de que el comando «/cmd» muestra en el chat la frase «Enter the command:» en ruso.

> *"El uso de aplicaciones basadas en la nube representa un desafío complejo para los defensores, y los atacantes lo saben bien. Factores como la facilidad para configurar y comenzar a utilizar la aplicación explican por qué los ciberdelincuentes recurren a estas herramientas en distintas etapas de un ataque",* señaló Fróes.