Un nuevo malware de robo de información basado en Golang denominado Titan Stealer, está siendo anunciado por atacantes a través de su canal de Telegram.

> *«El ladrón es capaz de robar una variedad de información de máquinas Windows infectadas, incluyendo datos de credenciales de navegadores y billeteras criptográficas, detalles del cliente FTP, capturas de pantalla, información del sistema y archivos capturados»,* dijeron los investigadores de seguridad, Uptycs Karthickkumar Kathiresan y Shilpesh Trivedi.

Los detalles del malware fueron documentados primero por el investigador de seguridad cibernética Will Thomas (@BushidoToken) en noviembre de 2022 consultando el motor de búsqueda IoT Shodan.

Tital se ofrece como constructor, lo que permite a los clientes personalizar el binario de malware para incluir funcionalidades específicas y el tipo de información que se filtrará de la máquina de una víctima.

El malware, tras la ejecución, emplea una técnica conocida como proceso de vaciado, que inyecta la carga útil maliciosa en la memoria de un proceso legítimo conocido como AppLaunch.exe, que es de Microsoft .NET.

Algunos de los principales navegadores web dirigidos por Titan Stealer incluyen: Google Chrome, Mozilla Firefox, Microsoft Edge, Yandex, Opera, Brave, Vivaldi, 7 Star Browser, Iridium Browser y otros. Las billeteras criptográficas destacadas son Armería, Armería, Bytecoin, Coinomi, Edge Wallet, Ethereum, Exodus, Guarda, Jaxx Liberty y Zcash.

También es capaz de recopilar la lista de aplicaciones instaladas en el host comprometido y capturar datos asociados con la aplicación de escritorio Telegram.

La información acumulada se transmite posteriormente a un servidor remoto bajo el control del atacante como un archivo codificado en Base64. Además, el malware cuenta con un

panel web que permite a los hackers acceder a los datos robados.

El modus operandi exacto utilizado para la distribución del malware todavía no está claro, pero tradicionalmente los atacantes aprovechan una serie de métodos, como phishing, anuncios maliciosos y software descifrado.

> *«Una de las razones principales por las que los actores de amenazas pueden estar usando Golang para su malware de robo de información es porque les permite crear fácilmente malware multiplataforma que puede ejecutarse en múltiples sistemas operativos, como Windows, Linux y macOS»*, dijo Cyble en su análisis sobre Titan Stealer.

> *«Además, los archivos binarios compilados de Go son de tamaño pequeño, lo que los hace más difíciles de detectar por el software de seguridad».*

El desarrollo lega poco más de dos meses después de que SEKOIA detallara otro malware basado en Go, denominado Aurora Stealer, que está siendo usado por varios hackers en sus campañas.

El malware es típicamente propagado por medio de sitios web similares de software popular, con los mismos dominios actualizados activamente para alojar versiones troyanas de distintas aplicaciones.

También se ha observado aprovechando un método conocido como relleno para inflar artificialmente el tamaño de los ejecutables hasta 260 MB mediante la adición de datos aleatorios para evadir la detección por software antivirus.

Los hallazgos se acercan a una campaña de malware que se ha observado entregando Raccoon y Vidar usando cientos de sitios web falsos disfrazados de software y juegos legítimos.

Team Cymru, en un análisis publicado a inicios de este mes, dijo que *«los operadores de Vidar dividieron su infraestructura en dos partes; una dedicada a sus clientes habituales y la otra para el equipo directiv, y también potencialmente premium/usuarios importantes».*