Expertos en ciberseguridad han descubierto un nuevo grupo de paquetes maliciosos en el registro de paquetes npm que tienen como objetivo robar información delicada de los desarrolladores.

Phylum, una empresa de cadena de suministro de software, fue la primera en identificar estos paquetes *«test»* el 31 de julio de 2023, y afirmó que su funcionalidad y sofisticación aumentaron con el tiempo. Poco después, los paquetes fueron eliminados y subidos nuevamente bajo nombres legítimos y menos sospechosos.

Aunque el propósito exacto de este ataque no está claro, se sospecha que se trata de una campaña dirigida específicamente al sector de las criptomonedas debido a referencias a módulos como *«rocketrefer» y «binarium».*

Todos los paquetes fueron publicados por el usuario malikrukd4732 en npm. Un rasgo común entre todos ellos es su habilidad para ejecutar código JavaScript («index.js») que envía información valiosa a un servidor remoto.

> *«El código index.js se ejecuta en un proceso secundario a través del archivo preinstall.js. Esta acción es desencadenada por el gancho postinstall definido en el archivo package.json, que se activa durante la instalación del paquete»*, explicó el equipo de investigadores de Phylum.

El primer paso consiste en recopilar el nombre de usuario del sistema operativo y el directorio de trabajo actual, después de lo cual se envía una solicitud GET con los datos recolectados a 185.62.57[.]60:8000/http. Aunque la motivación exacta de esta acción no está clara, se cree que la información podría utilizarse para desencadenar *«comportamientos no visibles en el servidor»*.

A continuación, el script avanza para buscar archivos y directorios que coincidan con un conjunto específico de extensiones: .env, .svn, .gitlab, .hg, .idea, .yarn, .docker, .vagrant, .github, .asp, .js, .php, .aspx, .jspx, .jhtml, .py, .rb, .pl, .cfm, .cgi, .ssjs, .shtml, .env, .ini, .conf,

.properties, .yml y .cfg.

Los datos recolectados, que también podrían contener credenciales e información valiosa de propiedad intelectual, son finalmente transmitidos al servidor en forma de un archivo ZIP.

> *«Si bien estos directorios pueden contener información sensible, es más probable que contengan una gran cantidad de archivos de aplicación estándar que no son únicos para el sistema de la víctima y, por lo tanto, menos valiosos para el atacante. Su motivación parece centrarse en extraer código fuente o archivos de configuración específicos del entorno»,* explicó Phylum.

Este desarrollo es el ejemplo más reciente de cómo los repositorios de código abierto se utilizan para propagar código malicioso, con ReversingLabs y Sonatype identificando una campaña en PyPI que emplea paquetes sospechosos de Python, como VMConnect, quantiumbase y ethter, para contactar con un servidor de comando y control (C2) y tratar de descargar una cadena codificada en Base64 con comandos adicionales no especificados.

> *«Como la obtención de comandos se realiza en un ciclo infinito, es posible que el operador del servidor C2 cargue comandos solo después de determinar que la máquina infectada resulta interesante para el actor de amenazas»*, detalló el investigador de seguridad Karlo Zanki.

> *«Además, el servidor C2 podría estar realizando algún tipo de filtrado de solicitudes. Por ejemplo, los atacantes pueden filtrar las solicitudes basándose en la dirección IP de la máquina infectada para evitar infectar objetivos de países específicos».*

A principios de julio de 2023, ReversingLabs también descubrió un conjunto de 13 módulos npm maliciosos que se descargaron en total aproximadamente 1,000 veces como parte de

una nueva campaña llamada Operación Brainleeches.

Lo que resalta en esta actividad es el uso de algunos de estos paquetes para facilitar el robo de credenciales mediante formularios de inicio de sesión falsos de Microsoft 365 que se lanzaban desde un archivo JavaScript adjunto a correos electrónicos. Además, estos paquetes JavaScript también buscaban obtener nuevas cargas útiles desde jsDelivr, una red de entrega de contenido (CDN) utilizada para alojar paquetes en npm.

En otras palabras, los módulos npm publicados desempeñaron un papel como una infraestructura de apoyo para alojar archivos utilizados en ataques de phishing por correo electrónico y también llevar a cabo ataques a la cadena de suministro dirigidos contra desarrolladores.

Este último objetivo se lograba mediante la inclusión de scripts de robo de credenciales en aplicaciones que inadvertidamente incorporaban los paquetes npm fraudulentos. Las bibliotecas fueron publicadas en npm entre el 11 de mayo y el 13 de junio de 2023.

> *«Uno de los aspectos clave de jsDelivr es que ofrece enlaces directos a los archivos: en lugar de utilizar npm para instalar el paquete y hacer referencia a él localmente, puedes enlazar directamente al archivo alojado en el CDN de jsDelivr. Sin embargo, incluso servicios legítimos como el CDN de jsDelivr pueden ser utilizados con fines maliciosos»*, comentó Check Point, que también informó sobre la misma campaña.