Se ha descubierto un nuevo paquete engañoso oculto dentro del registro de paquetes npm, el cual implementa una herramienta de acceso de raíz de código abierto llamada r77, marcando la primera vez que un paquete malicioso incluye funcionalidad de acceso de raíz.

El paquete en cuestión es «node-hide-console-windows«, el cual imita al legítimo paquete npm llamado «node-hide-console-window» en lo que constituye un ejemplo de una campaña de typosquatting. Este paquete fue descargado 704 veces en los últimos dos meses antes de ser retirado.

> ReversingLabs, la cual detectó esta actividad por primera vez en agosto de 2023, informó que el paquete *«descargó un bot de Discord que facilitó la instalación de una herramienta de acceso de raíz de código abierto, r77. Esto sugiere que los proyectos de código abierto podrían ser cada vez más utilizados para distribuir malware».*

El código malicioso, según la empresa de seguridad de la cadena de suministro de software, se encuentra en el archivo index.js del paquete, que al ejecutarse, descarga automáticamente un programa ejecutable.

El programa ejecutable en cuestión es un troyano de código abierto basado en C# conocido como DiscordRAT 2.0, el cual cuenta con funciones para tomar el control de manera remota de un host víctima a través de Discord, utilizando más de 40 comandos que facilitan la recopilación de datos sensibles, al tiempo que desactivan el software de seguridad.

Uno de los comandos es *«!rootkit»,* el cual se utiliza para iniciar el rootkit r77 en el sistema comprometido. r77, el cual es mantenido activamente por bytecode77, es un *«rootkit de anillo 3 sin archivos»* diseñado para ocultar archivos y procesos, y que puede ser incluido con otro software o ejecutado directamente.

Esta no es la primera vez que r77 ha sido utilizado en campañas maliciosas en la naturaleza, ya que actores de amenazas lo han utilizado como parte de cadenas de ataques para

distribuir el troyano SeroXen, así como mineros de criptomonedas.

Además, se ha descubierto que dos versiones diferentes de *«node-hide-console-windows»* descargan una herramienta de robo de información de código abierto llamada Blank-Grabber junto con DiscordRAT 2.0, haciéndola pasar como una *«actualización visual de código».*

Un aspecto destacable de esta campaña es que está completamente basada en componentes que están disponibles de forma gratuita y pública en línea, lo que requiere poco esfuerzo por parte de actores de amenazas para ensamblarla, y abre la *«puerta de ataque a la cadena de suministro»* a actores de amenazas de bajo perfil.

Los hallazgos de esta investigación subrayan la necesidad de que los desarrolladores ejerzan precaución al instalar paquetes de repositorios de código abierto. A principios de esta semana, Fortinet FortiGuard Labs identificó casi tres docenas de módulos con variaciones en estilo de codificación y métodos de ejecución que contenían características de recopilación de datos.

> *«El actor o actores maliciosos hicieron un esfuerzo por hacer que sus paquetes parecieran confiables»,* dijo la investigadora de seguridad Lucija Valentić.

> *«El actor o actores detrás de esta campaña crearon una página de npm que se asemejaba estrechamente a la página del paquete legítimo que estaba siendo objeto de typosquatting, e incluso crearon 10 versiones del paquete malicioso para que coincidieran con el paquete que estaban imitando».*