Los desarrolladores de Roblox están siendo blanco de una campaña persistente que busca comprometer sistemas mediante el uso de paquetes npm falsos, lo que destaca una vez más cómo los actores malintencionados siguen aprovechándose de la confianza en el ecosistema de código abierto para distribuir malware.

> *«Al imitar la popular biblioteca 'noblox.js', los atacantes han lanzado decenas de paquetes diseñados para robar datos sensibles y comprometer sistemas»,* explicó Yehuda Gelb, investigador de Checkmarx, en un informe técnico.

Los detalles de esta actividad fueron documentados por primera vez por ReversingLabs en agosto de 2023, como parte de una campaña que desplegó un malware de robo de información llamado Luna Token Grabber, el cual se describió como una *«repetición de un ataque descubierto hace dos años»* en octubre de 2021.

Desde principios de este año, se han identificado otros dos paquetes llamados noblox.js-proxy-server y noblox-ts como maliciosos, los cuales suplantan la popular biblioteca Node.js para distribuir malware de tipo stealer y un troyano de acceso remoto llamado Quasar RAT.

> *«Los atacantes de esta campaña han empleado técnicas como el secuestro de marcas, combosquatting y starjacking para crear una ilusión convincente de legitimidad en sus paquetes maliciosos»*, señaló Gelb.

Para lograrlo, los paquetes se presentan con nombres como noblox.js-async, noblox.js-thread, noblox.js-threads y noblox.js-api, creando la apariencia de que están relacionados con el paquete legítimo «noblox.js» y engañando así a los desarrolladores desprevenidos.

Las estadísticas de descargas de estos paquetes son las siguientes:

- noblox.js-async (74 descargas)

- noblox.js-thread (117 descargas)
- noblox.js-threads (64 descargas)
- noblox.js-api (64 descargas)

Otra técnica utilizada es el starjacking, en la que los paquetes falsos indican el repositorio fuente como el de la biblioteca noblox.js original, haciendo que parezcan más confiables.

El código malicioso integrado en la última versión funciona como un punto de entrada para desplegar cargas adicionales almacenadas en un repositorio de GitHub. Al mismo tiempo, roba tokens de Discord, modifica la lista de exclusiones de Microsoft Defender Antivirus para evitar ser detectado y asegura su persistencia mediante un cambio en el Registro de Windows.

> *«La efectividad del malware se centra en su método de persistencia, aprovechando la aplicación de Configuración de Windows para mantener el acceso continuo. Como consecuencia, cada vez que un usuario intenta abrir la aplicación de Configuración de Windows, el sistema ejecuta el malware en su lugar, sin que el usuario lo sepa»,* explicó Gelb.

El objetivo final de la cadena de ataques es desplegar Quasar RAT, permitiendo al atacante controlar de manera remota el sistema infectado. La información obtenida se envía al servidor de comando y control (C2) del atacante a través de un webhook de Discord.

Estos hallazgos sugieren que, a pesar de los esfuerzos para eliminar estos paquetes, sigue habiendo un flujo constante de nuevas amenazas, lo que hace crucial que los desarrolladores permanezcan alerta ante este peligro continuo.