Un grupo de hackers publicó nuevamente dos bibliotecas con errores tipográficos en el repositorio oficial de NPM, que imitan un paquete legítimo de Roblox, la compañía de juegos, con el objetivo de distribuir credenciales robadas, instalar troyanos de acceso remoto e infectar los sistemas comprometidos con ransomware.

Se descubrió que los paquetes falsos, llamados *«noblox.js-proxy» y «noblox.js-proxies»,* se hicieron pasar por una biblioteca llamada *«noblox.js«*, un contenedor de API de juegos de Roblox disponible en NPM y que cuenta con casi 20 mil descargas semanales. Con cada una de las bibliotecas infectadas, se descargaron un total de 281 y 106 veces, respectivamente.

Según el investigador de Sonatype, Juan Aguirre, quien descubrió los paquetes maliciosos de NPM, el autor de noblox.js-proxy publicó por primera vez una versión benigna que luego fue manipulada con el texto ofuscado, en realidad, un script de batch (.bat) un archivo JavaScript de instalación.

Dicho script de batch, a su vez, descarga ejecutables maliciosos de Content Delivery Network (CDN) de Discord, que son responsables de deshabilitar los motores anti-malware, lograr la persistencia en el host, desviar las credenciales del navegador e incluso implementar binarios con capacidades de ransomware.

Una investigación reciente de Check Point Research y RiskIQ, propiedad de Microsoft, reveló cómo los actores de amenazas abusan cada vez más de Discord CDN, una plataforma con 150 millones de usuarios, para entregar de forma persistente 27 familias de malware únicas, que van desde puertas traseras y ladrones de contraseñas hasta software espía y troyanos.

Aunque ambas bibliotecas maliciosas de NPM han sido eliminadas y ya no están disponibles, los hallazgos son otra indicación de cómo los registros de códigos populares como NPM, PyPI y RubyGems han surgido como una frontera lucrativa para llevar a cabo una variedad de ataques.

La divulgación también refleja un reciente ataque a la cadena de suministro dirigida a «UAParser.js», una popular biblioteca NPM de JavaScript con más de 6 millones de descargas

semanales, que resultó en el secuestro de la cuenta del desarrollador para corromper el paquete con minería de criptomonedas y malware de robo de credenciales, días después de que otros tres paquetes de minería de cifrado copiados fueran eliminados del registro.