Expertos en seguridad informática han descubierto una nueva serie de paquetes maliciosos que se han publicado en el administrador de paquetes NuGet utilizando un método menos conocido para la distribución de programas maliciosos.

La empresa de seguridad de la cadena de suministro de software, ReversingLabs, ha descrito esta campaña como un esfuerzo coordinado que está en marcha desde el 1 de agosto de 2023. Se ha relacionado con una serie de paquetes falsos de NuGet que se han utilizado para distribuir un troyano de acceso remoto conocido como SeroXen RAT.

> *«Los actores de amenazas detrás de esto están demostrando una tenacidad inquebrantable en su deseo de introducir malware en el repositorio de NuGet y de seguir publicando de manera constante nuevos paquetes maliciosos»,* afirmó Karlo Zanki, ingeniero inverso de ReversingLabs, en un informe.

A continuación, se detallan algunos de los nombres de estos paquetes maliciosos:

- Pathoschild.Stardew.Mod.Build.Config
- KucoinExchange.Net
- Kraken.Exchange
- DiscordsRpc
- SolanaWallet
- Monero
- Modern.Winform.UI
- MinecraftPocket.Server
- IAmRoot
- ZendeskApi.Client.V2
- Betalgo.Open.AI
- Forge.Open.AI
- Pathoschild.Stardew.Mod.BuildConfig
- CData.NetSuite.Net.Framework
- CData.Salesforce.Net.Framework

- CData.Snowflake.API

Estos paquetes, que abarcan varias versiones, imitan paquetes populares y aprovechan la característica de integración MSBuild de NuGet para insertar código malicioso en los sistemas de las víctimas. Utilizan una función conocida como tareas en línea para lograr la ejecución de código.

> *«Este es el primer caso conocido de malware publicado en el repositorio de NuGet que aprovecha esta función de tareas en línea para ejecutar programas maliciosos»,* comentó Zanki.

Los paquetes que han sido retirados ahora muestran características parecidas en el sentido de que los actores de amenazas detrás de la operación intentaron ocultar el código pernicioso mediante el uso de espacios y tabulaciones para sacarlo de la vista del ancho de pantalla estándar.

Como se había mencionado previamente por Phylum, los paquetes también tienen cifras de descargas infladas artificialmente para hacer que parezcan más auténticos. El objetivo último de los paquetes señuelo es funcionar como un conducto para obtener una carga secundaria .NET alojada en un repositorio temporal de GitHub.

> *«El actor de amenazas detrás de esta campaña está mostrando cuidado y atención a los detalles, y está decidido a mantener activa y en marcha esta campaña maliciosa»,* subrayó Zanki.