Se ha descubierto un paquete malicioso en el gestor de paquetes NuGet diseñado para el Framework .NET, el cual transporta un troyano de acceso remoto denominado SeroXen RAT.

Este paquete, bajo el nombre de Pathoschild.Stardew.Mod.Build.Config y publicado por un usuario con el nombre de Disti, constituye una suplantación de un paquete legítimo llamado Pathoschild.Stardew.ModBuildConfig, como lo señala la firma de seguridad de la cadena de suministro de software, Phylum, en su informe más reciente.

A pesar de que el paquete auténtico ha sido descargado casi 79,000 veces hasta la fecha, se ha informado que la variante maliciosa ha inflado artificialmente su cantidad de descargas después de su publicación el 6 de octubre de 2023, superando las 100,000 descargas.

El perfil detrás de este paquete ha publicado otros seis paquetes que han atraído, en total, no menos de 2.1 millones de descargas. Cuatro de estos paquetes se presentan como bibliotecas para varios servicios de criptomoneda, como Kraken, KuCoin, Solana y Monero, pero en realidad están diseñados para desplegar el SeroXen RAT.

La cadena de ataque comienza durante la instalación del paquete a través de un script denominado tools/init.ps1, diseñado para ejecutar código sin activar ninguna advertencia, un comportamiento que JFrog había mencionado previamente en marzo de 2023 como un método explotado para recuperar malware de la siguiente etapa.

> *«A pesar de que se considera obsoleto, el script init.ps1 todavía es reconocido por Visual Studio y se ejecuta sin emitir advertencias al instalar un paquete NuGet. Dentro del archivo .ps1, un atacante puede escribir comandos arbitrarios»,* comentó JFrog en ese momento.

En el paquete analizado por Phylum, el script de PowerShell se emplea para descargar un archivo llamado x.bin desde un servidor remoto, que, en realidad, es un script de Windows Batch altamente ofuscado. Este último es el responsable de construir y ejecutar otro script de PowerShell para finalmente desplegar el SeroXen RAT.

El SeroXen RAT es un software malicioso que se encuentra a la venta por $60 como parte de un paquete de por vida, lo que lo hace accesible para ciberdelincuentes. Se trata de un RAT sin archivos que combina las funcionalidades del Quasar RAT, el rootkit r77 y la herramienta de línea de comandos de Windows conocida como NirCmd.

> *«El descubrimiento del SeroXen RAT en paquetes NuGet subraya cómo los atacantes siguen explotando los ecosistemas de código abierto y a los desarrolladores que los utilizan»,* afirmó Phylum.

Este hallazgo se produce mientras la compañía detectó siete paquetes maliciosos en el repositorio del Índice de Paquetes de Python (PyPI) que se hacen pasar por ofertas legítimas de proveedores de servicios en la nube, como Aliyun, Amazon Web Services (AWS) y Tencent Cloud, con el propósito de transmitir credenciales de manera oculta a una URL remota ofuscada.

A continuación, se presentan los nombres de estos paquetes:

- tencent-cloud-python-sdk
- python-alibabacloud-sdk-core
- alibabacloud-oss2
- python-alibabacloud-tea-openapi
- aws-enumerate-iam
- enumerate-iam-aws
- alisdkcore

> *«En esta campaña, el atacante está explotando la confianza de los desarrolladores, tomando un código base existente y consolidado e insertando un pequeño fragmento de código malicioso con el objetivo de extraer credenciales confidenciales de la nube»,* señaló Phylum.

> *«La sutileza radica en la estrategia del atacante de mantener la funcionalidad original de los paquetes, tratando de pasar desapercibida. El ataque es minimalista y sencillo, pero efectivo».*

Checkmarx, que compartió información adicional sobre la misma campaña, informó que también está dirigida a atacar Telegram a través de un paquete engañoso llamado telethon2, que tiene como objetivo imitar a telethon, una biblioteca de Python para interactuar con la API de Telegram.

La mayoría de las descargas de estas bibliotecas falsificadas provienen de los Estados Unidos, seguidos de China, Singapur, Hong Kong, Rusia y Francia.

> *«En lugar de ejecutar automáticamente, el código malicioso en estos paquetes se ocultó estratégicamente dentro de funciones, diseñadas para activarse solo cuando se llaman estas funciones. Los atacantes utilizaron técnicas de Typosquatting y StarJacking para atraer a los desarrolladores hacia sus paquetes maliciosos»,* explicó la empresa.

A principios de este mes, Checkmarx también expuso una campaña constante y cada vez más sofisticada dirigida a PyPI con el objetivo de infiltrar 271 paquetes maliciosos de Python en la cadena de suministro de software para robar datos confidenciales y criptomonedas de sistemas Windows.

Estos paquetes, que también incluían funciones para desactivar las defensas del sistema, fueron descargados colectivamente aproximadamente 75,000 veces antes de ser retirados.

Actualización

Los otros seis paquetes publicados por Disti, KucoinExchange.net, Kraken.Exchange, SolanaWallet, Modern.Winform.UI, Monero y DiscordsRpc ya no están disponibles en NuGet.