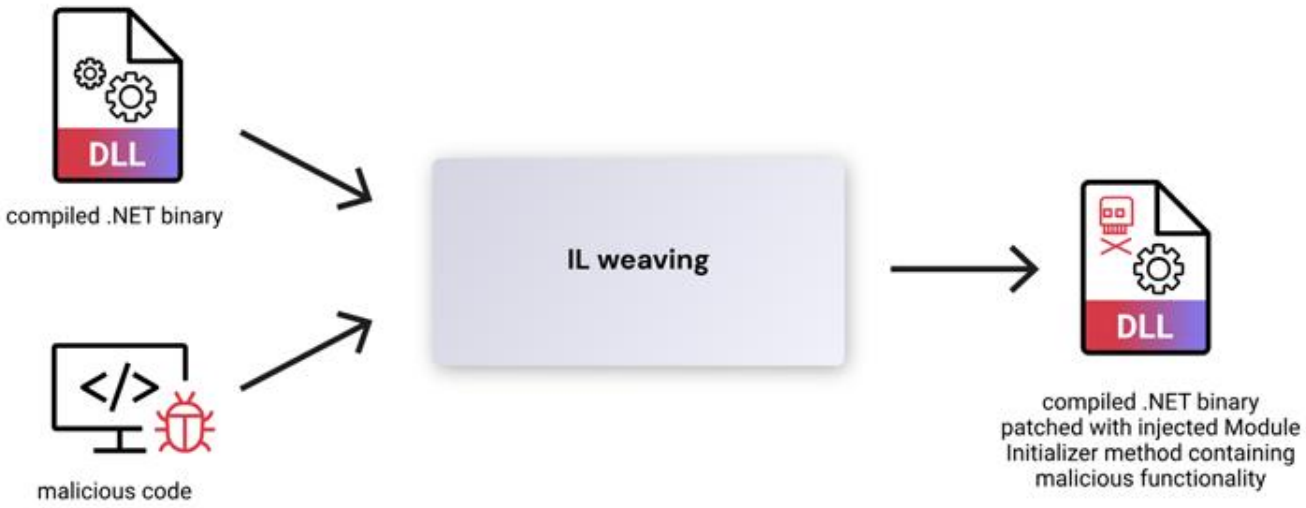
Se ha observado que actores maliciosos están publicando una nueva serie de paquetes maliciosos en el gestor de paquetes NuGet, como parte de una campaña en curso que comenzó en agosto de 2023, añadiendo además una nueva capa de sigilo para evitar ser detectados.

Los nuevos paquetes, aproximadamente 60 en total y con 290 versiones diferentes, muestran un enfoque más sofisticado en comparación con el conjunto anterior revelado en octubre de 2023, según la empresa de seguridad de la cadena de suministro de software, ReversingLabs.

> Los atacantes cambiaron de usar las integraciones de MSBuild de NuGet a *«una estrategia que utiliza descargadores simples y ofuscados que se insertan en archivos binarios PE legítimos mediante el uso de Intermediary Language (IL) Weaving, una técnica de programación .NET para modificar el código de una aplicación después de la compilación»*, explicó el investigador de seguridad Karlo Zanki.

El objetivo final de los paquetes falsificados, tanto los antiguos como los nuevos, es distribuir un troyano de acceso remoto listo para usar llamado SeroXen RAT. Todos los paquetes identificados han sido eliminados desde entonces.




La última serie de paquetes se caracteriza por el uso de una técnica innovadora llamada IL weaving, que permite inyectar funcionalidad maliciosa en un binario PE .NET legítimo tomado de un paquete NuGet legítimo.

Esto incluye tomar paquetes populares de código abierto como Guna.UI2.WinForms y modificarlos con el método mencionado para crear un paquete impostor llamado «Guna.UI3.Winforms,» que utiliza homógrafos para reemplazar las letras «u,» «n,» «i» y «o» por sus equivalentes «u» (\u057D), «n» (\u0578), «i» (\u0456) y «o» (\u0585).

> *«Los actores maliciosos están continuamente evolucionando los métodos y tácticas que usan para comprometer e infectar a sus víctimas con código malicioso que se utiliza para extraer datos sensibles o proporcionar a los atacantes control sobre los activos de TI»,* dijo Zanki.
>
> *«Esta última campaña destaca nuevas formas en las que los actores maliciosos están ideando para engañar a los desarrolladores y a los equipos de seguridad, haciéndoles descargar y usar paquetes maliciosos o alterados de gestores de*

> *paquetes de código abierto populares como NuGet».*