Se ha detectado una reciente campaña de ataques cibernéticos que utiliza archivos de paquetes de aplicaciones MSIX falsos en el entorno de Windows para distribuir un novedoso cargador de malware denominado GHOSTPULSE. Los archivos MSIX falsos se hacen pasar por paquetes de aplicaciones de software popular, como Google Chrome, Microsoft Edge, Brave, Grammarly y Cisco Webex.

> *«MSIX es un formato de paquete de aplicaciones para Windows que los desarrolladores pueden aprovechar para empaquetar, distribuir e instalar sus aplicaciones en los sistemas de Windows»,* comentó Joe Desimone, investigador de Elastic Security Labs, en un informe técnico publicado la semana pasada.

> *«Sin embargo, el uso de MSIX requiere el acceso a certificados de firma de código, ya sean adquiridos legítimamente o robados, lo que los hace atractivos para grupos con recursos por encima de la media».*

Según los instaladores utilizados como señuelos, se sospecha que los posibles objetivos son atraídos para descargar los paquetes MSIX a través de técnicas conocidas, como sitios web comprometidos, manipulación de motores de búsqueda (SEO) o anuncios maliciosos.

Cuando se abre el archivo MSIX, se muestra una ventana de Windows que pide a los usuarios que hagan clic en el botón de instalación. Hacerlo resulta en la descarga sigilosa de GHOSTPULSE en el sistema comprometido desde un servidor remoto (en «manojsinghnegi[.]com») mediante un script de PowerShell.

Este proceso se lleva a cabo en múltiples etapas, siendo la primera carga útil un archivo TAR que contiene un ejecutable que se disfraza como el servicio Oracle VM VirtualBox (VBoxSVC.exe). Sin embargo, en realidad, se trata de un binario legítimo que se encuentra junto a Notepad++ (gup.exe).

Dentro del archivo TAR también se encuentran el archivo handoff.wav y una versión de libcurl.dll modificada para que sea dañina. Esta última se carga para llevar el proceso de infección a la siguiente etapa aprovechando la vulnerabilidad de gup.exe en la carga lateral de DLL.

> *«PowerShell ejecuta el binario VBoxSVC.exe, que cargará desde el directorio actual la DLL maliciosa libcurl.dll. Al minimizar la huella en disco del código malicioso cifrado, el actor de amenazas puede evitar la detección de antivirus y el análisis de aprendizaje automático basados en archivos»,* explicó Desimone.

Posteriormente, el archivo DLL manipulado procede a analizar handoff.wav, que, a su vez, contiene una carga útil cifrada. Esta carga se descifra y ejecuta a través de mshtml.dll, un método conocido como «module stomping», con el fin de cargar finalmente GHOSTPULSE.

GHOSTPULSE actúa como un cargador y utiliza otra técnica llamada *«process doppelgänging»* para iniciar la ejecución del malware final. Este malware incluye SectopRAT, Rhadamanthys, Vidar, Lumma y NetSupport RAT.