Microsoft informó el jueves que está volviendo a desactivar el manejador de protocolo ms-appinstaller de forma predeterminada debido a su explotación por diversos actores maliciosos para propagar software maligno.

> *«Las actividades detectadas de estos actores maliciosos abusan de la configuración actual del manejador ms-appinstaller para introducir malware, lo que podría resultar en la distribución de ransomware»,* mencionó el equipo de Inteligencia de Amenazas de Microsoft.

Agregaron que hay varios delincuentes cibernéticos ofreciendo un paquete de software maligno como servicio, aprovechando el formato de archivo MSIX y el protocolo ms-appinstaller. Estas modificaciones están activas en la versión 1.21.3421.0 o superior de la herramienta App Installer.

Los métodos de ataque consisten en paquetes de aplicaciones MSIX con firmas falsificadas que se diseminan a través de Microsoft Teams o publicidad engañosa de software popular en motores de búsqueda como Google.

Desde mediados de noviembre de 2023, al menos cuatro grupos de ciberdelincuentes con motivaciones económicas han sido detectados usando App Installer para iniciar actividades de ransomware:

- Storm-0569, un intermediario que difunde BATLOADER mediante técnicas de optimización en motores de búsqueda (SEO), presentando páginas que imitan plataformas como Zoom, Tableau y TeamViewer, y luego emplea malware para introducir Cobalt Strike, delegando el control a Storm-0506 para la liberación del ransomware Black Basta.
- Storm-1113, otro intermediario que se vale de instaladores MSIX fraudulentos que se presentan como Zoom para distribuir EugenLoader, una herramienta que facilita la instalación de otros malwares y troyanos de acceso remoto.
- Sangria Tempest (también conocido como Carbon Spider y FIN7), que utiliza

EugenLoader para instalar Carbanak y, posteriormente, implantar Gracewire. Además, este grupo ha utilizado anuncios en Google para incentivar la descarga de paquetes MSIX dañinos desde sitios web maliciosos, distribuyendo POWERTRASH, que luego instala NetSupport RAT y Gracewire.

- Storm-1674, un intermediario que envía páginas engañosas presentándose como Microsoft OneDrive y SharePoint mediante mensajes en Teams, instando a los usuarios a abrir archivos PDF que, al hacerlo, solicitan una actualización de Adobe Acrobat Reader, descargando en realidad un instalador MSIX con cargas maliciosas SectopRAT o DarkGate.

Microsoft identificó a Storm-1113 como una entidad que también ofrece servicios de *«as a service»*, suministrando instaladores y estructuras de páginas web que imitan software legítimo a otros grupos como Sangria Tempest y Storm-1674.

En octubre de 2023, Elastic Security Labs informó sobre otra campaña en la que se usaron archivos MSIX falsos de aplicaciones como Google Chrome y Microsoft Edge para difundir un cargador de malware conocido como GHOSTPULSE.

Esta no es la primera ocasión en que Microsoft toma medidas contra el protocolo ms-appinstaller en Windows. En febrero de 2022, la compañía tomó decisiones similares para prevenir la distribución de amenazas como Emotet y TrickBot.

> *«Es probable que los delincuentes cibernéticos hayan seleccionado el protocolo ms-appinstaller debido a que puede eludir sistemas diseñados para proteger a los usuarios de amenazas, como Microsoft Defender SmartScreen y las alertas integradas del navegador sobre descargas de archivos ejecutables»,* comentó Microsoft.