Microsoft ha revelado detalles sobre una campaña de malvertising a gran escala que, según estimaciones, ha afectado a más de un millón de dispositivos en todo el mundo. La compañía describe este ataque como una ofensiva oportunista diseñada para robar información sensible.

El gigante tecnológico detectó la actividad a principios de diciembre de 2024 y la ha catalogado dentro de la clasificación más amplia de Storm-0408, un nombre asignado a un grupo de actores maliciosos conocidos por distribuir malware de acceso remoto o de robo de información mediante tácticas como phishing, optimización en motores de búsqueda (SEO) o malvertising.

> *«El ataque se originó en sitios web de streaming ilegal que contenían redireccionadores de malvertising, lo que llevaba a los usuarios a un sitio web intermediario antes de ser redirigidos a GitHub y otras dos plataformas»,* señaló el equipo de inteligencia de amenazas de Microsoft.
>
> *«La campaña afectó a una amplia gama de organizaciones e industrias, tanto a nivel de consumidores como de empresas, lo que resalta la naturaleza indiscriminada del ataque».*

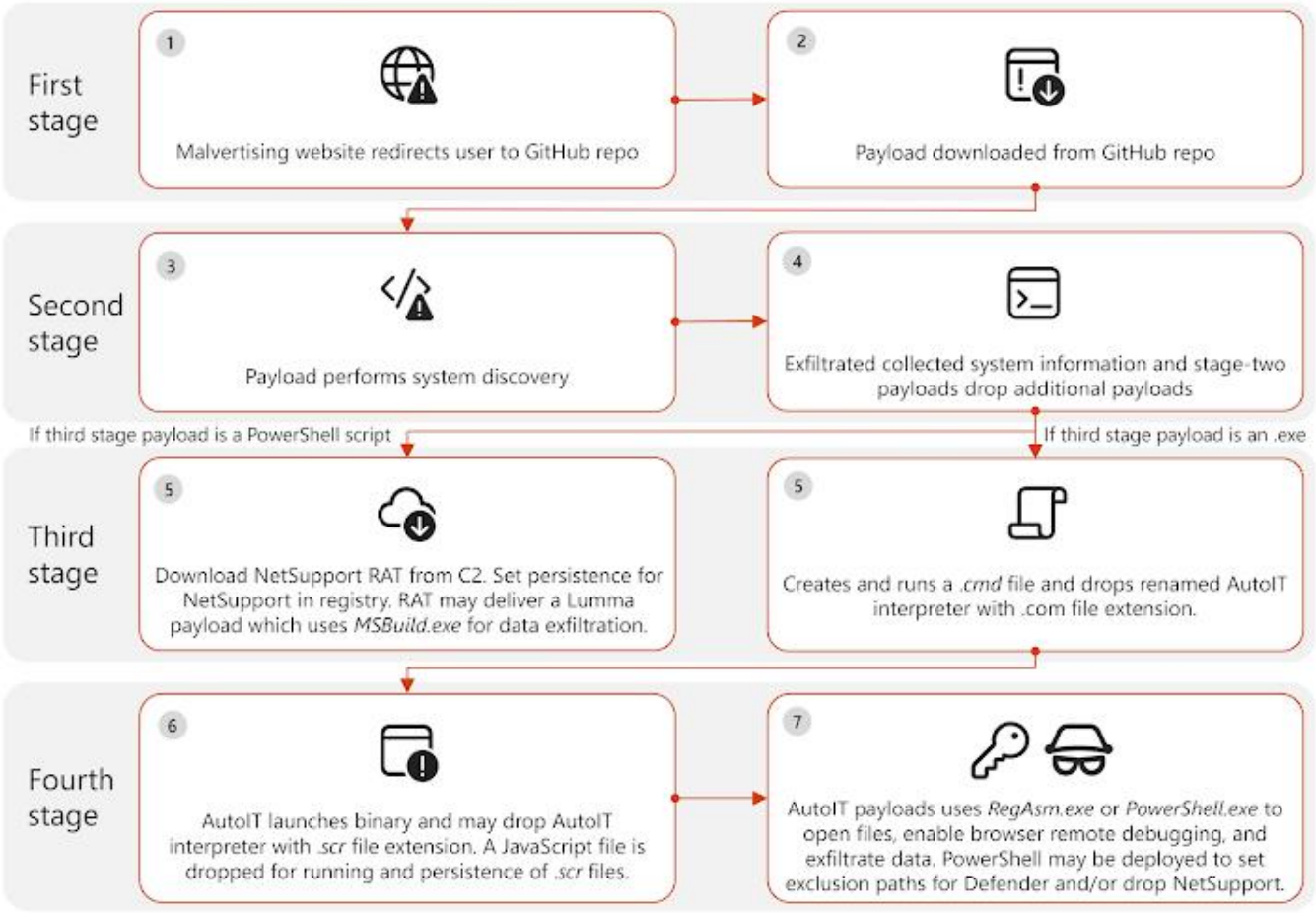
Uno de los aspectos más relevantes de esta operación es el uso de GitHub como plataforma para la distribución de cargas maliciosas iniciales. En al menos dos casos adicionales, se identificó que los archivos maliciosos también estaban alojados en Discord y Dropbox. Los repositorios en GitHub ya han sido eliminados, aunque Microsoft no especificó cuántos fueron retirados.

El servicio de alojamiento de código de Microsoft fue utilizado como una base para dropper malware, el cual ejecutaba otros programas maliciosos, como Lumma Stealer y Doenerium, capaces de recopilar información del sistema.

El ataque empleó una sofisticada cadena de redirección de entre cuatro y cinco capas, comenzando con un redireccionador incrustado en un elemento iframe dentro de sitios de streaming ilegal que ofrecen contenido pirata.

El proceso de infección seguía múltiples etapas:

1. Primera etapa: Establecimiento de presencia en el dispositivo de la víctima.
2. Segunda etapa: Reconocimiento del sistema, recopilación y exfiltración de datos, y entrega de nuevas cargas maliciosas.
3. Tercera etapa: Ejecución de comandos, evasión de medidas de seguridad, persistencia, comunicaciones con servidores de comando y control (C2) y robo de datos.
4. Cuarta etapa: Uso de un script de PowerShell para configurar exclusiones en Microsoft Defender y ejecutar comandos que descargan datos de un servidor remoto.



Otra característica destacada de estos ataques es el uso de diversos scripts de PowerShell para descargar NetSupport RAT, identificar aplicaciones instaladas y detectar software de seguridad, con especial interés en la presencia de billeteras de criptomonedas, lo que sugiere un posible robo de datos financieros.

> *«Además de los programas de robo de información, se ejecutaron scripts de PowerShell, JavaScript, VBScript y AutoIT en los dispositivos afectados. Los actores de amenazas utilizaron archivos binarios y scripts legítimos del sistema (‘Living-off-the-Land Binaries and Scripts’ o LOLBAS), como PowerShell.exe, MSBuild.exe y RegAsm.exe, para establecer comunicaciones C2 y exfiltrar credenciales de usuario*

> *y datos del navegador»,* indicó Microsoft.

Esta revelación surge al mismo tiempo que Kaspersky advirtió sobre el uso de sitios web fraudulentos que se hacen pasar por los chatbots de inteligencia artificial DeepSeek y Grok para engañar a los usuarios y hacerles instalar un ladrón de información basado en Python, previamente desconocido.

Se han identificado sitios falsos con temática de DeepSeek, promocionados por cuentas verificadas en X (como @ColeAddisonTech, @gaurdevang2 y @saduq5), que ejecutan un script de PowerShell con el fin de usar SSH para otorgar acceso remoto a los atacantes.

> *«Los ciberdelincuentes emplean diversas estrategias para atraer a las víctimas a recursos maliciosos. Por lo general, los enlaces a estos sitios se distribuyen a través de mensajería instantánea y redes sociales. Los atacantes también pueden utilizar typosquatting o comprar tráfico publicitario hacia sitios maliciosos mediante numerosos programas de afiliados»,* señaló la empresa de ciberseguridad rusa.