Los usuarios que buscan software popular están siendo objetivo de una campaña de publicidad maliciosa que abusa de Google Ads para ofrecer variantes troyanizadas que implementan malware, como Raccoon Stealer y Vidar.

La actividad hace uso de sitios web aparentemente creíbles con nombres de dominio con errores tipográficos que aparecen en la parte superior de los resultados de búsqueda de Google en forma de anuncios maliciosos mediante el secuestro de búsquedas de palabras clave específicas.

El objetivo final de dichos ataques es engañar a los usuarios desprevenidos para que descarguen programas maliciosos o aplicaciones potenticalmente no deseadas.

En una campaña revelada por Guardio Labs, se observó a los atacantes creando una red de sitios benignos que se promocionan en el motor de búsqueda, que al hacer clic, redirige a los visitantes a una página de phishing que contienen un archivo ZIP troyano alojado en Dropbox o OneDrive.

> *«En el momento en que esos sitios 'disfrazados' son visitados por visitantes específico (aquellos que realmente hacen clic en el resultado de búsqueda promocionado), el servidor los redirige inmediatamente al sitio falso y de allí a la carga maliciosa»,* dijo el investigador Nati Tal.

Entre el software suplantado se incluyen AnyDesk, Dashlane, Grammarly, Malwarebytes, Microsoft Visual Studio, MSI Afterburner, Slack y Zoom, entre otros.

Guardio Labs, que denominó la campaña MasquerAds, atribuye una gran parte de la actividad a un atacante que está rastreado bajo el nombre de Vermux, y dice que el adversario está *«abusando de una amplia lista de marcas y sigue evolucionando».*

La operación Vermux seleccionó principalmente a usuarios en Canadá y Estados Unidos, empleando sitios de masquerAds adaptados a las búsquedas de AnyDesk y MSI Afterburner para proliferar mineros de criptomonedas y ladrones de información de Vidar.

El desarrollo marca el uso continuo de dominios typosquatted que imitan software legítimo para atraer a los usuarios a instalar aplicaciones no autorizadas de Android y Windows.

También está lejos de ser la primera vez que se aprovecha la plataforma de Google Ads para dispensar malware. El mes pasado, Microsoft reveló una campaña de ataque que aprovecha el servicio de publicidad para implementar BATLOADER, que después se usa para eliminar el ransomware Royal.

Aparte de BATLOADER, los atacantes también usan técnicas de publicidad maliciosa para distribuir el malware IceID por medio de páginas web clonadas de aplicaciones conocidas como Adobe, Brave, Discord, LibreOffce, Mozilla Thunderbird y TeamViewer.

> *«IceID es una familia de malware notable que es capaz de entregar otras cargas útiles, incluido Cobalt Strike y otro malware. IceID permite a los atacantes realizar ataques de seguimiento de gran impacto que conducen al compromsio total del sistema, como el robo de datos y el ransomware paralizante»,* dijo Trend Micro la semana pasada.

Los hallazgos también se producen cuando la Oficina Federal de Investigaciones (FBI) de Estados Unidos advirtió que *«los ciberdelincuentes están usando los servicios de publicidad de los motores de búsqueda para hacerse pasar por marcas y dirigir a los usuarios a sitios maliciosos que alojan ransomware y roban credenciales de inicio de sesión y otra información financiera».*