Los perpetradores de amenazas están utilizando resultados de búsqueda manipulados y anuncios falsos en Google para engañar a usuarios que buscan descargar software legítimo, como WinSCP, y lograr que instalen malware en su lugar.

La compañía de ciberseguridad Securonix está monitorizando esta actividad continua bajo el nombre SEO#LURKER.

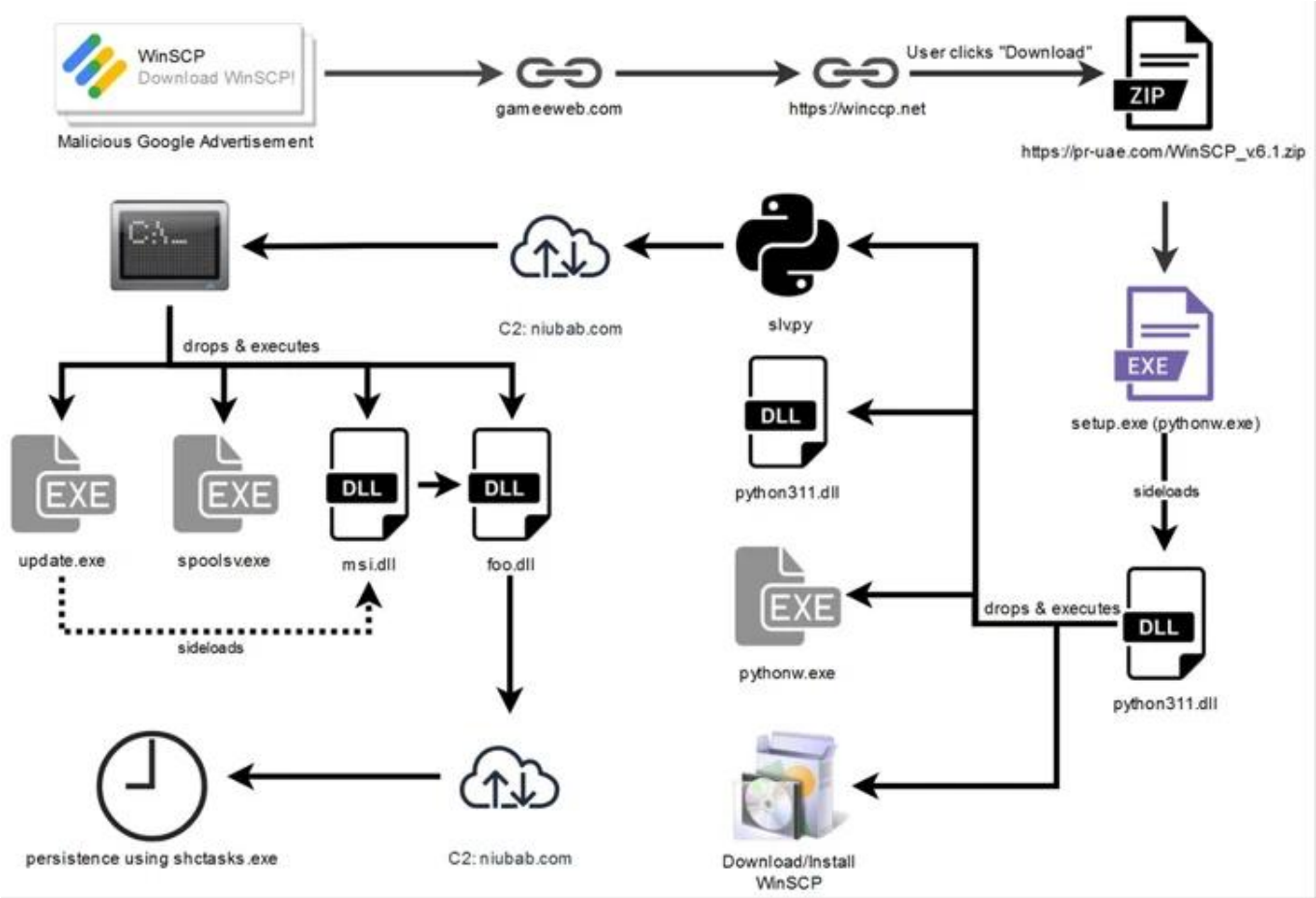
> *«El anuncio malicioso dirige al usuario a un sitio web de WordPress comprometido, gameeweb[.]com, que luego redirige al usuario a un sitio de phishing controlado por el atacante»*, indicaron los investigadores de seguridad Den Iuzvyk, Tim Peck y Oleg Kolesnikov en un informe.

Se cree que los perpetradores de amenazas están aprovechando los Anuncios de Búsqueda Dinámica (DSAs) de Google, que generan anuncios automáticamente basados en el contenido de un sitio para mostrar anuncios maliciosos que llevan a las víctimas al sitio infectado.

El objetivo final de esta cadena de ataques multifásicos es incitar a los usuarios a hacer clic en un sitio web falso y similar a WinSCP, winccp[.]net, y descargar el malware.

> *«El tráfico desde el sitio web gaweeweb[.]com hasta el sitio web falso winsccp[.]net depende de que se establezca correctamente el encabezado de referencia. Si el referente es incorrecto, el usuario es 'Rickrolled' y se le redirige al famoso video de Rick Astley en YouTube»*, explicaron los investigadores.

La carga útil final se presenta como un archivo ZIP («WinSCP_v.6.1.zip») que contiene un ejecutable de configuración. Cuando se ejecuta, utiliza la técnica de carga lateral de DLL para cargar y ejecutar un archivo DLL llamado python311.dll que se encuentra dentro del archivo.



La DLL, a su vez, descarga y ejecuta un instalador legítimo de WinSCP para mantener la apariencia, mientras silenciosamente deja scripts de Python («slv.py» y «wo15.py») en segundo plano para activar el comportamiento malicioso. También se encarga de establecer la persistencia.

Ambos scripts de Python están diseñados para establecer contacto con un servidor controlado por actores remotos para recibir instrucciones adicionales que permitan a los atacantes ejecutar comandos de enumeración en el host.

> *«Dado que los atacantes estaban utilizando anuncios de Google para distribuir*

> *malware, se puede suponer que los objetivos se limitan a aquellos que buscan el software WinSCP»,* señalaron los investigadores.

> *«El bloqueo geográfico utilizado en el sitio que aloja el malware sugiere que los afectados por este ataque están en los Estados Unidos»*.

Esta no es la primera vez que los Anuncios de Búsqueda Dinámica de Google se emplean para distribuir malware. A finales del mes pasado, Malwarebytes reveló una campaña que apunta a usuarios que buscan PyCharm con enlaces a un sitio web hackeado que aloja un instalador falso, facilitando así la instalación de malware que roba información.

El uso de publicidad maliciosa ha ganado popularidad entre los ciberdelincuentes en los últimos años, con numerosas campañas de malware utilizando esta táctica en los últimos meses.

A principios de esta semana, Malwarebytes informó de un aumento en las campañas de skimming de tarjetas de crédito en octubre de 2023 que se estima que han comprometido cientos de sitios web de comercio electrónico con el objetivo de robar información financiera mediante la inyección de páginas de pago falsas convincentes.