Se han desvelado pormenores acerca de una campaña de malvertising que utiliza Google Ads para dirigir a usuarios que buscan software popular hacia páginas de destino ficticias y distribuir cargas útiles en la siguiente fase.

Malwarebytes, que descubrió esta actividad, afirmó que se trata de una estrategia *«singular en su forma de identificar a los usuarios y distribuir cargas sensibles al tiempo».*

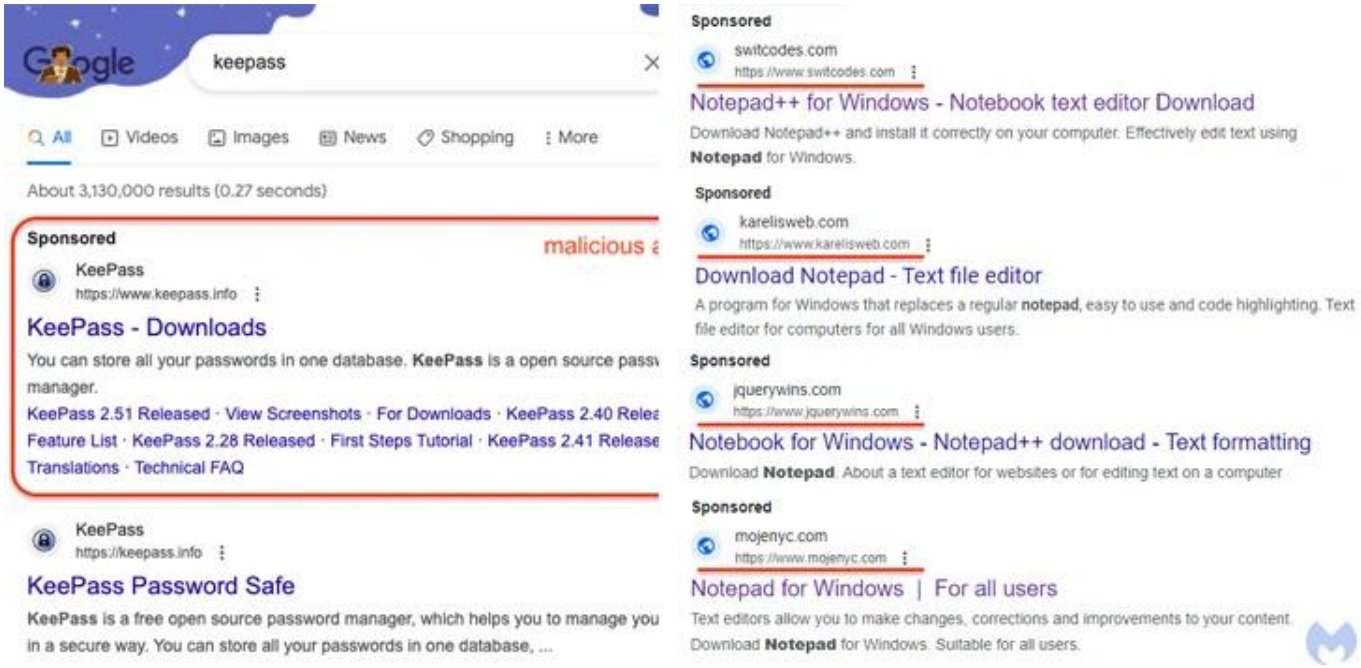
Este ataque se enfoca en usuarios que buscan Notepad++ y convertidores de PDF, mostrando anuncios falsos en la página de resultados de búsqueda de Google. Cuando se hace clic en estos anuncios, se filtran bots y otras direcciones IP no deseadas, mostrando un sitio de señuelo.

Si el visitante es considerado de interés para el actor de amenazas, se le redirige a un sitio web réplica que anuncia el software, mientras se realiza discretamente una huella en el sistema para determinar si la solicitud proviene de una máquina virtual.

Los usuarios que no superan la verificación son redirigidos al sitio legítimo de Notepad++, mientras que un posible objetivo recibe un ID único con fines de *«seguimiento, pero también para que cada descarga sea única y sensible al tiempo».*

El malware en la fase final es una carga útil HTA que establece una conexión con un dominio remoto («mybigeye[.]icu») en un puerto personalizado y sirve como malware complementario.

> *«Los actores de amenazas están aplicando técnicas de evasión con éxito, eludiendo comprobaciones de anuncios y permitiéndoles dirigirse a ciertos tipos de víctimas»,* afirmó Jérôme Segura, director de inteligencia de amenazas.



> *«Con una cadena de suministro confiable de malware en su poder, los actores maliciosos pueden concentrarse en mejorar sus páginas de señuelo y crear cargas personalizadas de malware».*

Esta revelación se superpone con una campaña similar que apunta a usuarios que buscan el gestor de contraseñas KeePass con anuncios maliciosos que redirigen a las víctimas a un dominio que utiliza Punycode (keepass[.]info vs ḳeepass[.]info), una codificación especial que convierte caracteres Unicode a ASCII.

> *«Las personas que hacen clic en el anuncio son redirigidas a través de un servicio de ocultamiento destinado a filtrar entornos de prueba, bots y cualquiera que no se considere una víctima genuina. Los actores de amenazas han configurado un dominio temporal en keepasstacking[.]site que realiza la redirección condicional al destino final»*, señaló Segura.

Los usuarios que llegan al sitio de señuelo son engañados para descargar un instalador malicioso que finalmente conduce a la ejecución de FakeBat (también conocido como EugenLoader), un cargador diseñado para descargar otro código malicioso.

La explotación de Punycode no es del todo nueva, pero combinarla con anuncios falsos de Google es un indicio de que el malvertising a través de motores de búsqueda se está volviendo más sofisticado. Al utilizar Punycode para registrar nombres de dominio similares a sitios legítimos, el objetivo es llevar a cabo un ataque homográfico y atraer a las víctimas para que instalen malware.

> *«Hasta la fecha, aunque el Punycode con nombres de dominio internacionalizados ha sido utilizado durante años por actores de amenazas para pescar a sus víctimas, muestra cuán efectivo sigue siendo en el contexto de la suplantación de marcas a través del malvertising»*, dijo Segura.

Hablando de engaños visuales, se ha observado a varios actores de amenazas, como TA569 (también conocido como SocGholish), RogueRaticate (FakeSG), ZPHP (SmartApeSG), ClearFake y EtherHiding, aprovechar temas relacionados con falsas actualizaciones de navegadores para propagar Cobalt Strike, cargadores, ladrones y troyanos de acceso remoto. Esto indica que estos ataques son una amenaza constante y en constante evolución.

> *«Las falsas actualizaciones de navegadores abusan de la confianza del usuario final con sitios comprometidos y un señuelo personalizado para el navegador del usuario para legitimar la actualización y engañar a los usuarios para que hagan clic»*, dijo el investigador de Proofpoint, Dusty Miller, en un análisis publicado esta semana.

> *«La amenaza solo existe en el navegador y puede iniciarse con un clic desde un correo electrónico legítimo y esperado, un sitio de redes sociales, una consulta en*

> *un motor de búsqueda o incluso simplemente navegando por el sitio comprometido».*