El jueves pasado, Microsoft eliminó una campaña en curso que afecta a los navegadores web populares, y que inyecta de forma sigilosa anuncios infestados de malware en los resultados de búsqueda para ganar dinero a través de publicidad de afiliados.

Adrozek, como lo llama el equipo de investigación de Microsoft 365 Defender, emplea una *«infraestructura de ataques dinámica y expansiva»*, que consta de 159 dominios únicos, cada uno de los cuales alberga un promedio de 17300 URL únicas, que a su vez albergan más de 15300 muestras únicas de malware.

La campaña, que afecta a los navegadores Microsoft Edge, Google Chrome, Yandex Browser y Mozilla Firefox en Windows, tiene como objetivo insertar anuncios adicionales no autorizados en la parte superior de los anuncios legítimos que se muestran en las páginas de resultados de los motores de búsqueda, lo que lleva a los usuarios a hacer clic en dichos anuncios sin darse cuenta.

Microsoft dijo que el malware modificador de navegador persistente se ha observado desde mayo de este año, con más de treinta mil dispositivos afectados todos los días en su punto máximo en agosto.

> *«Los criminales cibernéticos que abusan de los programas de afiliados en el navegador no son nuevos, es uno de los tipos más antiguos de amenazas. Sin embargo, el hecho de que esta campaña utilice una pieza de malware que afecta a múltiples navegadores es una indicación de cómo este tipo de amenaza sigue siendo cada vez más sofisticada. Además, el malware mantiene la persistencia y filtra las credenciales del sitio web, exponiendo los dispositivos afectados a riesgos adicionales»,* dijo Microsoft.

Una vez colocado e instalado en los sistemas de destino a través de descargas no autorizadas, Adrozek procede a realizar múltiples cambios en la configuración del navegador y los controles de seguridad para instalar complementos maliciosos que se hacen pasar por genuinos al reutilizar los ID de las extensiones legítimas.

Aunque los navegadores modernos tienen controles de integridad para evitar la manipulación, el malware deshabilita de forma inteligente la función, lo que permite a los atacantes eludir las defensas de seguridad y explotar las extensiones para obtener scripts adicionales de servidores remotos para inyectar anuncios falsos y obtener ingresos al dirigir el tráfico a estos anuncios fraudulentos.

Además, Adrozek va un paso adelante en Mozilla Firefox para llevar a cabo el robo de credenciales y exfiltrar los datos a servidores controlados por atacantes.

> *«Adrozek muestra que incluso las amenazas que no se consideran urgentes o críticas son cada vez más complejas»,* dijeron los investigadores.
>
> *«Y aunque el objetivo principal del malware es inyectar anuncios y derivar tráfico a determinados sitios web, la cadena de ataque implica un comportamiento sofisticado que permite a los atacantes afianzarse firmemente en un dispositivo. La incorporación del comportamiento de robo de credenciales muestra que los atacantes pueden ampliar sus objetivos para aprovechar el acceso que pueden obtener»*, agregaron.