Una combinación de métodos de propagación, narrativas sofisticadas y técnicas de evasión permitió que la táctica de ingeniería social conocida como ClickFix se expandiera con fuerza durante el último año, según nuevos hallazgos de Guardio Labs.

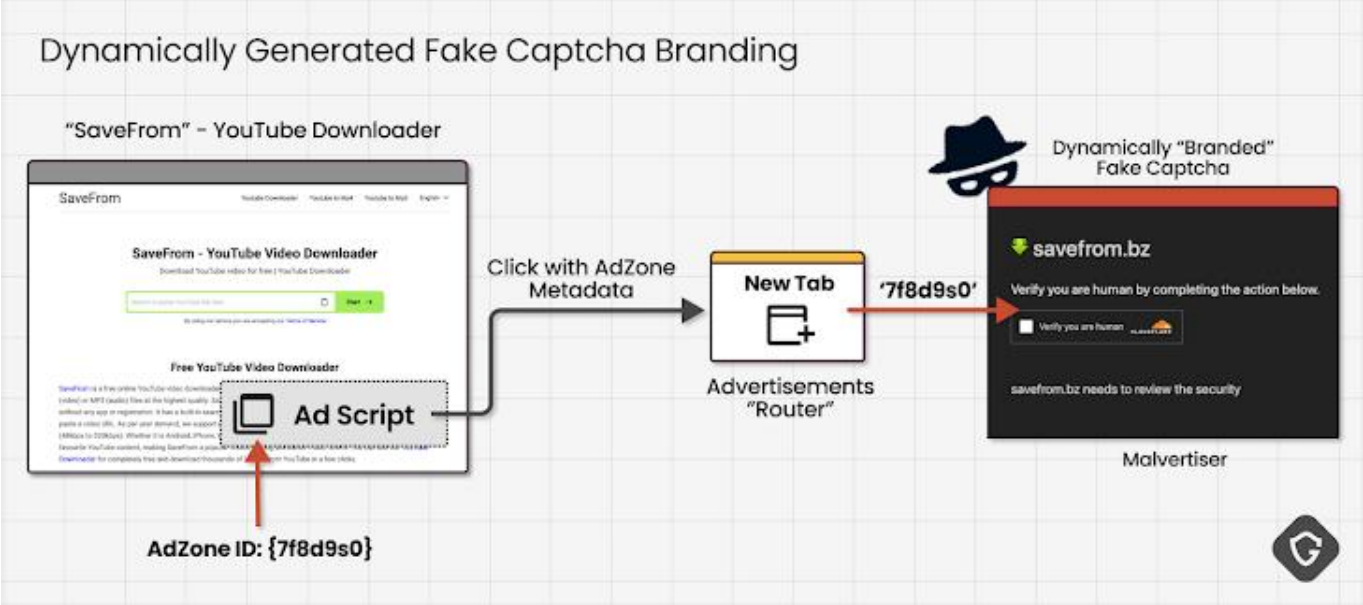
"Al igual que una variante viral en el mundo real, esta nueva cepa llamada 'ClickFix' superó rápidamente y terminó reemplazando por completo la infame estafa de falsas actualizaciones de navegador que dominaba la web el año pasado", señaló el investigador en ciberseguridad Shaked Chen en un informe.

"Lo logró eliminando la necesidad de descargas de archivos, utilizando tácticas de ingeniería social más inteligentes y aprovechando infraestructuras confiables para su distribución. El resultado: una oleada de infecciones que va desde ataques masivos tipo drive-by hasta campañas de spear-phishing altamente dirigidas."

ClickFix es el nombre atribuido a una técnica de engaño en la que las víctimas potenciales son inducidas a infectar sus propios equipos bajo la apariencia de resolver un problema inexistente o verificar un CAPTCHA. Su detección en entornos reales se remonta a principios de 2024.

En estos ataques se utilizan vectores de infección diversos como correos electrónicos de phishing, descargas silenciosas, malvertising y técnicas de envenenamiento SEO para redirigir a los usuarios hacia páginas falsas que muestran mensajes de error.

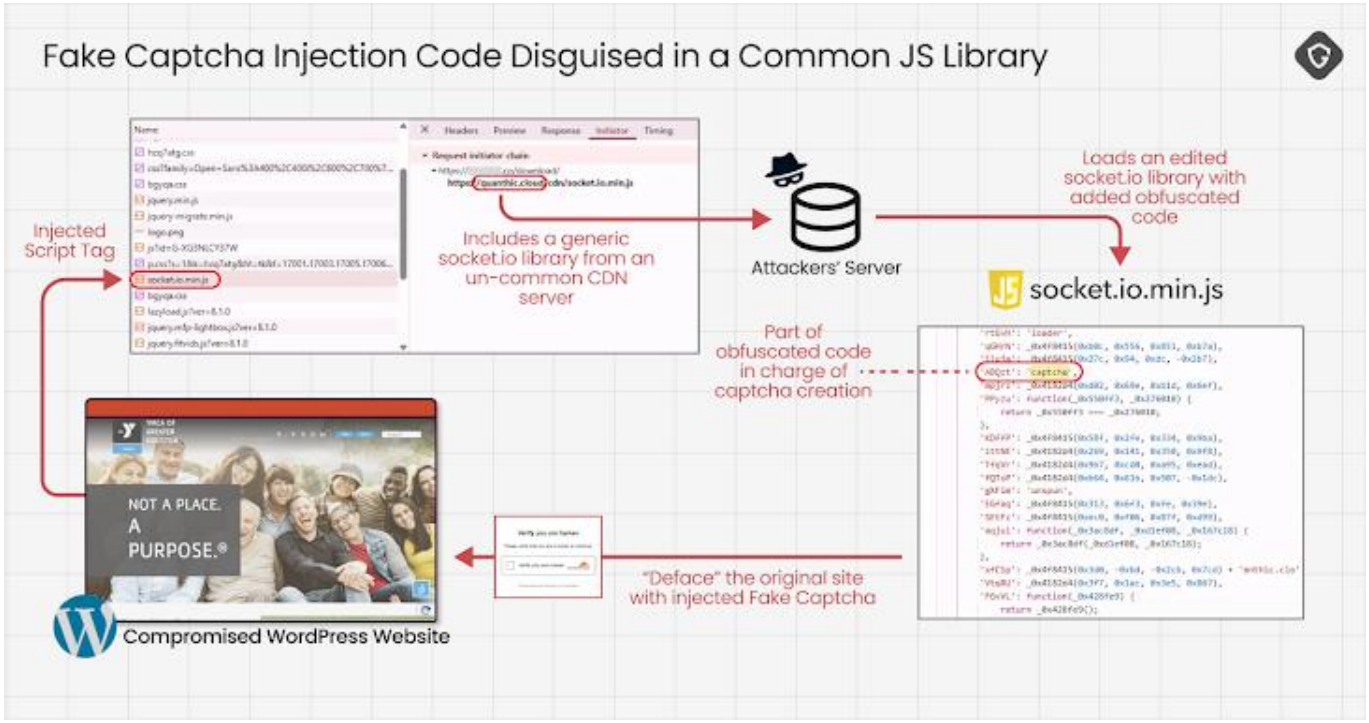
El propósito de estos mensajes es único: guiar a las víctimas a seguir una serie de pasos que terminan ejecutando un comando malicioso que fue copiado subrepticiamente al portapapeles, y que se activa al ser pegado en el cuadro de diálogo "Ejecutar" de Windows o en la app Terminal de macOS.



Este comando malicioso desencadena una cadena de ejecución por etapas, cuyo desenlace es la instalación de distintos tipos de malware como troyanos de acceso remoto (RAT), ladrones de información y cargadores, lo cual evidencia la versatilidad de la amenaza.

La táctica ha resultado tan eficaz y poderosa que ha derivado en lo que Guardio denomina un *CAPTCHAgeddon*, siendo utilizada tanto por cibercriminales como por actores estatales en decenas de campañas en un corto periodo de tiempo.

ClickFix representa una evolución más discreta de ClearFake, un método que se basa en sitios WordPress comprometidos para mostrar falsas actualizaciones de navegador que distribuyen malware tipo stealer. Posteriormente, ClearFake incorporó técnicas avanzadas de ocultamiento como EtherHiding, que utiliza contratos de la Binance Smart Chain (BSC) para esconder la carga maliciosa.



Guardio afirma que el éxito de ClickFix se debe a una mejora constante en sus vectores de propagación, la diversificación de los cebos y mensajes, y las múltiples formas de evadir los mecanismos de detección, al punto de haber reemplazado por completo a ClearFake.

"Los primeros mensajes eran genéricos, pero rápidamente se volvieron más convincentes, añadiendo elementos de urgencia o señales que despertaban sospechas", explicó Chen. *"Estos ajustes aumentaron la tasa de éxito al explotar presiones psicológicas básicas."*

Entre las adaptaciones más notables se encuentra el abuso de Google Scripts para alojar flujos falsos de CAPTCHA, aprovechando la confianza en los dominios de Google, así como la inserción de cargas maliciosas dentro de archivos que aparentan ser legítimos, como *socket.io.min.js*.

"Esta inquietante lista de técnicas – ofuscación, carga dinámica, archivos con apariencia legítima, compatibilidad multiplataforma, entrega de cargas por terceros y uso indebido de

dominios confiables como Google – demuestra cómo los atacantes han evolucionado constantemente para esquivar la detección”, añadió Chen.

“Es un recordatorio contundente de que estos actores no solo perfeccionan sus métodos de engaño, sino que invierten significativamente en técnicas técnicas para que sus ataques se mantengan efectivos y resistentes ante las medidas de seguridad.”