Investigadores en ciberseguridad están alertando sobre una *«campaña a gran escala»* que ha estado comprometiendo sitios web legítimos mediante inyecciones maliciosas de código JavaScript.

De acuerdo con Unit 42 de Palo Alto Networks, estos scripts maliciosos están ofuscados utilizando JSFuck, un *«estilo de programación esotérico y educativo»* que se basa únicamente en un conjunto reducido de caracteres para escribir y ejecutar código.

La empresa de ciberseguridad ha bautizado esta técnica con el nombre alternativo JSFireTruck, debido al lenguaje inapropiado que suele aparecer en su análisis.

> *«Se han detectado múltiples sitios con JavaScript malicioso inyectado que utiliza la ofuscación JSFireTruck, la cual está compuesta principalmente por los símbolos [,], +, $, { y }. La ofuscación del código dificulta entender su verdadero objetivo, lo que complica su análisis»,* explicaron los investigadores de seguridad Hardik Shah, Brad Duncan y Pranay Kumar Chhaparwal.

Un análisis más detallado reveló que el código inyectado tiene como finalidad inspeccionar el campo «document.referrer«, el cual indica la dirección web desde donde se originó la solicitud.

Si el sitio de origen es un motor de búsqueda como Google, Bing, DuckDuckGo, Yahoo! o AOL, el script redirige a los usuarios hacia URLs maliciosas que pueden entregar malware, exploits, monetización de tráfico o publicidad maliciosa.

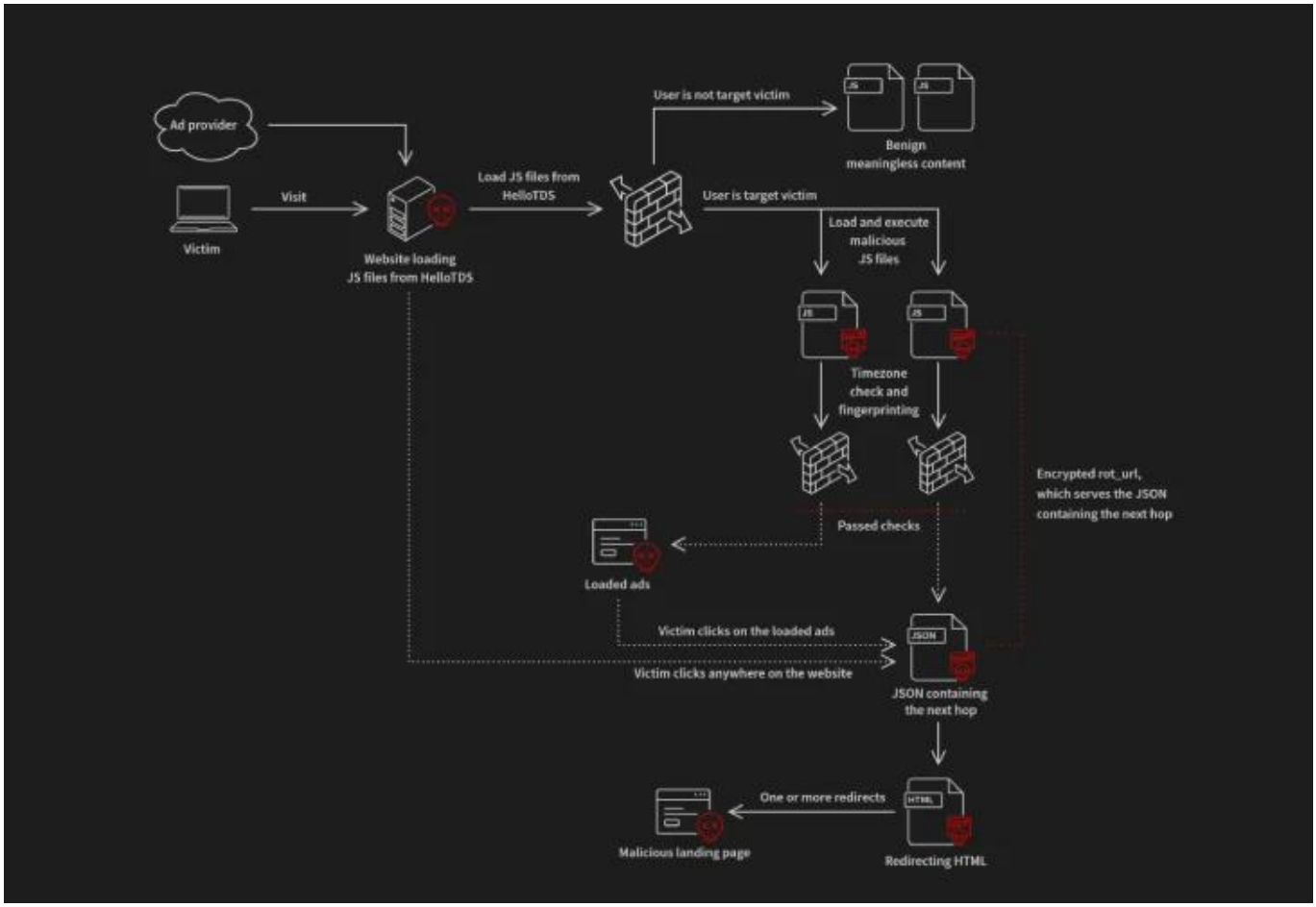
Unit 42 indicó que, según su sistema de monitoreo, se identificaron 269,552 páginas web infectadas con código JavaScript utilizando la técnica JSFireTruck entre el 26 de marzo y el 25 de abril de 2025. El primer gran pico de actividad se detectó el 12 de abril, con más de 50,000 páginas comprometidas en un solo día.

> *«La escala y el sigilo de esta campaña representan una amenaza considerable. La extensión de estas infecciones apunta a un esfuerzo coordinado para vulnerar sitios legítimos y usarlos como vectores para actividades maliciosas adicionales»,* señalaron los investigadores.

Presentamos HelloTDS

Este desarrollo ocurre mientras Gen Digital ha revelado un sofisticado Servicio de Distribución de Tráfico (TDS, por sus siglas en inglés) llamado HelloTDS, diseñado para redirigir selectivamente a los visitantes de un sitio hacia páginas falsas de CAPTCHA, estafas de soporte técnico, actualizaciones de navegador falsas, extensiones no deseadas y fraudes con criptomonedas, a través de código JavaScript alojado de forma remota e insertado en los sitios web.

El propósito principal del TDS es servir como una puerta de entrada que determina el tipo específico de contenido a mostrar a las víctimas tras analizar sus dispositivos. Si el usuario no se considera un objetivo adecuado, es redirigido a una página legítima.



> *«Los puntos de entrada de la campaña son sitios de streaming comprometidos o controlados por atacantes, servicios de intercambio de archivos, así como campañas de publicidad maliciosa»*, señalaron los investigadores Vojtěch Krejsa y Milan Špinka en un informe publicado este mes.
>
> *«Las víctimas son evaluadas con base en su ubicación geográfica, dirección IP y huella del navegador; por ejemplo, las conexiones realizadas mediante VPN o navegadores automatizados son detectadas y bloqueadas.»*

Algunas de estas cadenas de ataque incluyen páginas de CAPTCHA falsas que utilizan la táctica ClickFix para engañar a los usuarios y hacer que ejecuten código malicioso, infectando sus dispositivos con un malware conocido como PEAKLIGHT (también llamado Emmental Loader), el cual está asociado a troyanos de robo de información como Lumma.

Un componente clave de la infraestructura de HelloTDS es el uso de dominios de nivel superior como .top, .shop y .com, los cuales alojan el código JavaScript y activan las redirecciones tras un proceso de huella digital en varias etapas diseñado para recolectar información del navegador y la red.

> *«La infraestructura de HelloTDS utilizada en campañas de CAPTCHA falsos demuestra cómo los atacantes siguen perfeccionando sus tácticas para evadir las defensas tradicionales, evitar ser detectados y seleccionar cuidadosamente a sus objetivos»,* afirmaron los investigadores.
>
> *«Mediante el uso de técnicas avanzadas de fingerprinting, dominios dinámicos y estrategias de engaño (como imitar sitios legítimos o servir contenido inocuo a los analistas), estas campañas logran operar con gran sigilo y alcance.»*