El ataque a la cadena de suministro que afecta la biblioteca JavaScript Polyfill[.]io, ampliamente utilizada, tiene un alcance mayor de lo que se había estimado inicialmente. Nuevos descubrimientos de Censys indican que más de 380,000 hosts están incorporando un script de polyfill que enlaza con el dominio malicioso a partir del 2 de julio de 2024.

Esto incluye referencias a *«https://cdn.polyfill[.]io» o «https://cdn.polyfill[.]com»* en sus respuestas HTTP, según informó la firma de gestión de superficie de ataque.

> *«Aproximadamente 237,700 de estos hosts se encuentran dentro de la red de Hetzner (AS24940), principalmente en Alemania. Esto no es sorprendente, ya que Hetzner es un servicio de alojamiento web muy popular y muchos desarrolladores de sitios web lo utilizan»*, se señaló.

Un análisis adicional de los hosts afectados reveló que hay dominios vinculados a importantes empresas como WarnerBros, Hulu, Mercedes-Benz y Pearson que hacen referencia al endpoint malicioso en cuestión.

Los detalles del ataque se conocieron a finales de junio de 2024 cuando Sansec alertó que el código alojado en el dominio Polyfill había sido modificado para redirigir a los usuarios a sitios web de temática adulta y de juegos de azar. Los cambios en el código se realizaron de manera que las redirecciones solo ocurrían en ciertos momentos del día y solo contra visitantes que cumplían ciertos criterios.

Se informó que el comportamiento malicioso se introdujo después de que el dominio y su repositorio asociado en GitHub fueron vendidos a una empresa china llamada Funnull en febrero de 2024.

Este desarrollo llevó al registrador de dominios Namecheap a suspender el dominio, a redes de entrega de contenido como Cloudflare a reemplazar automáticamente los enlaces de Polyfill con dominios que conducen a sitios espejo alternativos seguros, y a Google a bloquear anuncios para sitios que incrustan el dominio.

Mientras los operadores intentaban reiniciar el servicio bajo un dominio diferente llamado polyfill[.]com, este también fue retirado por Namecheap a partir del 28 de junio de 2024. De los otros dos dominios registrados por ellos desde principios de julio, polyfill[.]site y polyfillcache[.]com, este último sigue activo y funcionando.

Además de esto, se ha descubierto una red más amplia de dominios potencialmente relacionados, que incluye bootcdn[.]net, bootcss[.]com, staticfile[.]net, staticfile[.]org, unionadjs[.]com, xhsbpza[.]com, union.macoms[.]la, newcrbpc[.]com, todos vinculados a los administradores de Polyfill, lo que sugiere que el incidente podría formar parte de una campaña maliciosa más extendida.

«Uno de estos dominios, bootcss[.]com, ha sido visto realizando actividades maliciosas muy parecidas al ataque a polyfill[.]io, con evidencia que se remonta a junio de 2023», destacó Censys, añadiendo que encontraron 1.6 millones de hosts públicamente accesibles que enlazan con estos dominios sospechosos.

> *«No sería descabellado considerar que el mismo actor malicioso responsable del ataque a polyfill.io pueda utilizar estos otros dominios para actividades similares en el futuro.»*

Este desarrollo ocurre mientras la empresa de seguridad de WordPress, Patchstack, alertó sobre los riesgos en cadena causados por el ataque a la cadena de suministro de Polyfill en sitios que utilizan el sistema de gestión de contenido (CMS) a través de numerosos complementos legítimos que enlazan con el dominio fraudulento.