Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUE A LA CADENA DE SUMINISTRO DE POLYFILL.IO AFECTA A MÁS DE 100,000 SITIOS

27 / 06 / 2024

CONTENIDO

INTRODUCCIÓN

El reciente ataque a la cadena de suministro de Polyfill.io ha puesto en jaque a más de 100,000 sitios web, revelando vulnerabilidades críticas en la gestión de dependencias externas. Este incidente, desencadenado por la adquisición del dominio por parte de una empresa china y la posterior inyección de código malicioso, subraya la importancia de la vigilancia constante y la actualización de los recursos de terceros. Con implicaciones que van desde redirecciones no autorizadas hasta la desactivación de anuncios por parte de Google, esta situación ha llevado a actores clave como Cloudflare a intervenir, proporcionando soluciones más seguras para proteger a los usuarios y mantener la integridad de los sitios web afectados.

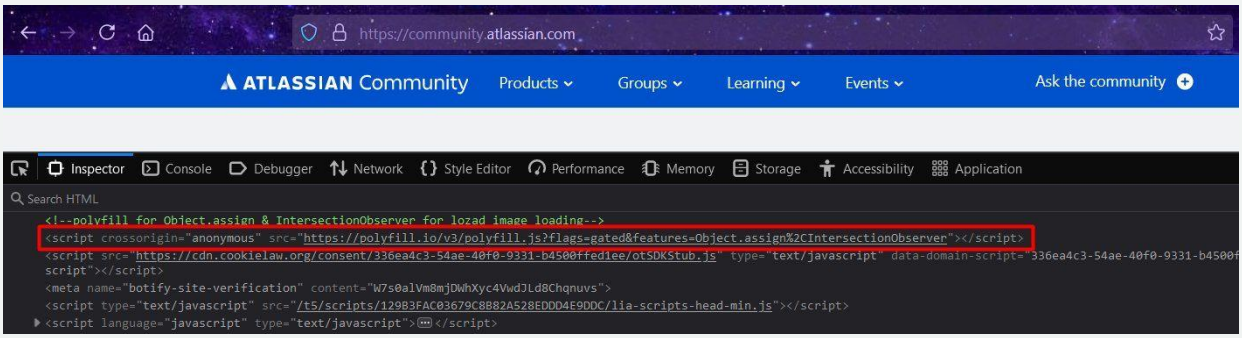
ATAQUE A LA CADENA DE SUMINISTRO DE POLYFILL.IO AFECTA A MÁS DE 100,000 SITIOS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_06_27_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	27/06/2024
Es día cero (0 day):	No

RESUMEN

El 25 de junio de 2024, se reportó que más de 100,000 sitios web fueron afectados por un ataque a la cadena de suministro a través del servicio Polyfill.io. Este incidente se produjo después de que una empresa china adquiriera el dominio y modificara el script para redirigir a los usuarios a sitios maliciosos y de estafa.



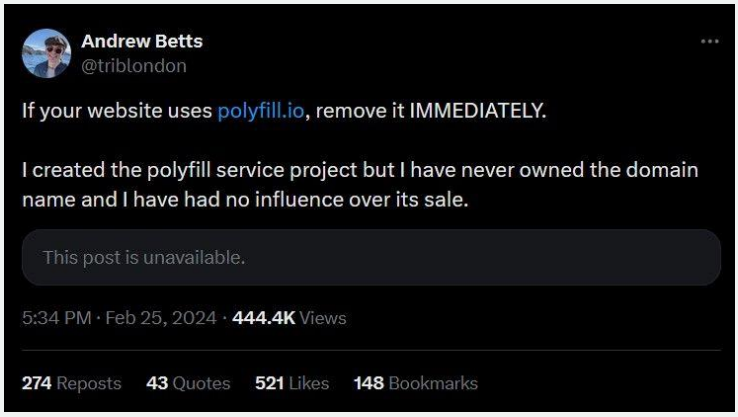
¿QUÉ ES UN POLYFILL?

Un polyfill es un código, como JavaScript, que agrega funcionalidades modernas a navegadores antiguos que normalmente no las soportan. Esto permite que todos los visitantes de un sitio web utilicen la misma base de código, independientemente de las capacidades de sus navegadores.

ADQUISICIÓN Y MODIFICACIÓN DEL SERVICIO POLYFILL.IO

Polyfill.io es utilizado por cientos de miles de sitios para garantizar compatibilidad con navegadores más antiguos. A principios de este año, una empresa china llamada 'Funnull' compró el dominio y la cuenta de GitHub asociada. Desde entonces, el dominio comenzó a inyectar malware en dispositivos móviles a través de cualquier sitio que incorporara el script de cdn.polyfill.io.

En ese momento, el desarrollador original del proyecto Polyfill.io advirtió que nunca fue propietario del sitio polyfill.io y recomendó a todos los sitios web que lo eliminaran de inmediato para reducir el riesgo de un ataque a la cadena de suministro. Servicios como Cloudflare y Fastly crearon espejos confiables del servicio Polyfill.io para que los sitios web pudieran utilizar servicios seguros.



EFECTOS DEL ATAQUE

El script modificado por los nuevos propietarios estaba diseñado para redirigir a los visitantes a sitios no deseados, como sitios falsos de apuestas deportivas. Este comportamiento se logró a través de dominios falsos de Google Analytics (www.googie-anaiytics.com) o redirecciones como kuurza.com/redirect?from=bitget.

```
function isPc() {
  try {
    var _isWin =
        navigator.platform == "Win32" || navigator.platform == "Windows",
      _isMac =
        navigator.platform == "Mac68K" ||
        navigator.platform == "MacPPC" ||
        navigator.platform == "Macintosh" ||
        navigator.platform == "MacIntel";
    if (_isMac || _isWin) {
      return true;
    } else {
      return false;
```

Sansec, mencionó que el script modificado tiene protecciones específicas contra la ingeniería inversa y solo se activa en dispositivos móviles específicos en momentos específicos, además de desactivarse cuando detecta usuarios administradores.

MEDIDAS TOMADAS

Actualmente, el dominio cdn.polyfill.io ha sido redirigido misteriosamente a Cloudflare, aunque los servidores DNS del dominio permanecen sin cambios, lo que permite a los propietarios cambiarlo nuevamente a sus propios dominios en cualquier momento.

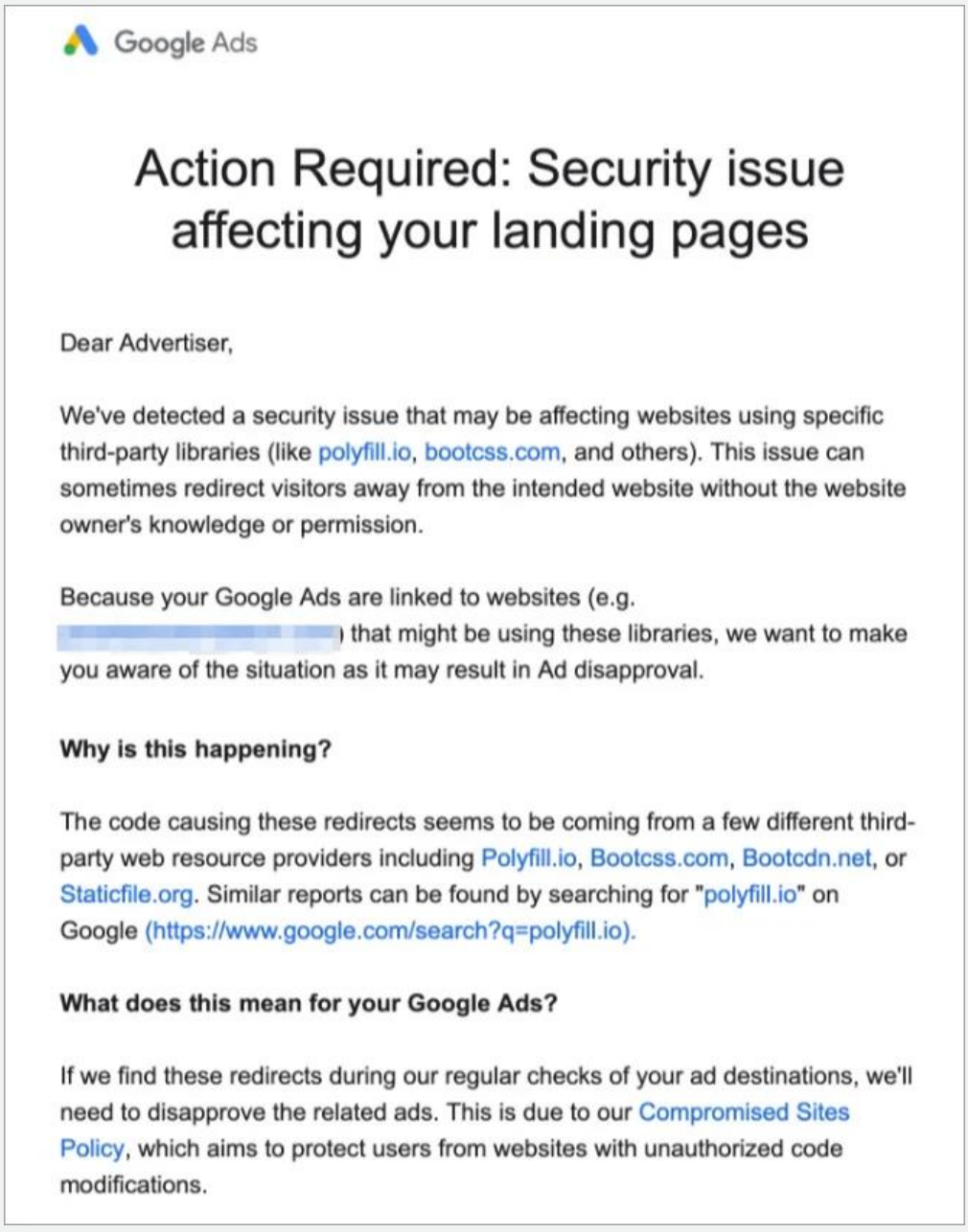
Para ayudar a los desarrolladores web, la empresa de ciberseguridad Leak Signal creó el sitio Polykill.io, que permite buscar sitios que usan cdn.polyfill.io y proporciona información sobre cómo cambiar a alternativas seguras.

ADVERTENCIAS DE GOOGLE

Google ha comenzado a notificar a los anunciantes sobre este ataque, advirtiéndoles que sus páginas de destino incluyen el código malicioso y podrían redirigir a los visitantes sin el conocimiento o permiso del

propietario del sitio. Además, Google advirtió que otros servicios como Bootcss, Bootcdn y Staticfile también están causando redirecciones no deseadas, afectando potencialmente a miles de sitios más.

Google ha informado que, si encuentran estas redirecciones durante las revisiones regulares de los destinos de los anuncios, desaprobarán los anuncios relacionados.



Google Ads

Action Required: Security issue affecting your landing pages

Dear Advertiser,

We've detected a security issue that may be affecting websites using specific third-party libraries (like polyfill.io, bootcss.com, and others). This issue can sometimes redirect visitors away from the intended website without the website owner's knowledge or permission.

Because your Google Ads are linked to websites (e.g.) that might be using these libraries, we want to make you aware of the situation as it may result in Ad disapproval.

Why is this happening?

The code causing these redirects seems to be coming from a few different third-party web resource providers including Polyfill.io, Bootcss.com, Bootcdn.net, or Staticfile.org. Similar reports can be found by searching for "polyfill.io" on Google (https://www.google.com/search?q=polyfill.io).

What does this mean for your Google Ads?

If we find these redirects during our regular checks of your ad destinations, we'll need to disapprove the related ads. This is due to our Compromised Sites Policy, which aims to protect users from websites with unauthorized code modifications.

CONCLUSIÓN

Este incidente subraya la importancia de la vigilancia continua y la gestión proactiva de los servicios y scripts de terceros utilizados en sitios web. Es crucial que las empresas e instituciones revisen y actualicen regularmente sus dependencias para protegerse contra posibles ataques a la cadena de suministro.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240627_Polyfill.io

NOTICIA COMPLETA

https://devel.group/blog/ataque-a-la-cadena-de-suministro-de-polyfill-io-afecta-a-mas-de-100000-sitios/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente