Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

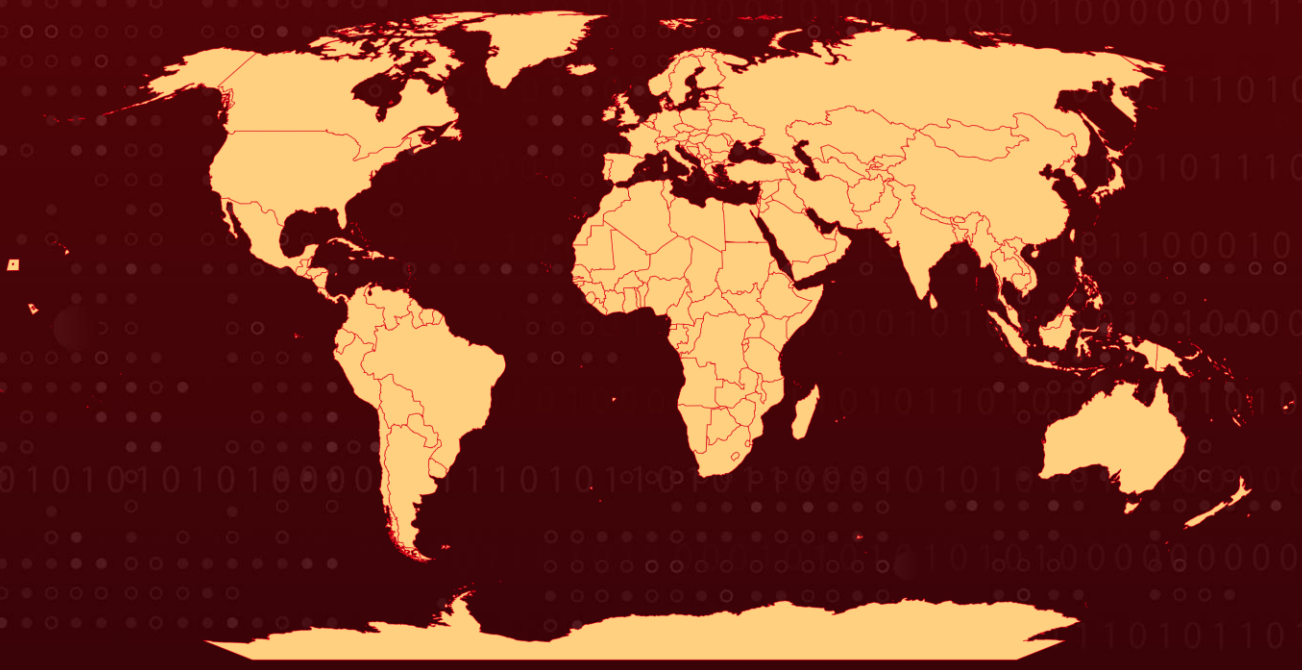
Polyfill.io Supply Chain Attack: Widespread Compromise Affects Over 100,000 Websites

Date of Publication	Admiralty Code	TA Number
July 4, 2024	A1	TA2024258

Summary

First Appearance: June 25, 2024
Targeted Countries: Worldwide
Attack: A significant supply chain attack on the Polyfill.io JavaScript library, affecting over 100,000 websites. A Chinese company acquired the domain in February 2024 and embedded malicious code, redirecting users to harmful sites. Despite mitigation efforts, many websites remain compromised. The incident underscores the need for vigilant security practices in managing third-party dependencies.

Attack Regions



Attack Details

#1 A significant supply chain attack involving the Polyfill.io JavaScript library, which impacted over 100,000 websites. Polyfill.io was a popular JavaScript library that provided compatibility features for older browsers. Many websites embedded scripts from Polyfill.io's CDN (Content Delivery Network) to ensure their functionality across different browsing platforms.

#2 In February 2024, a Chinese company called Funnull acquired Polyfill.io, including its domain and Github account. This raised initial concerns about potential security risks associated with a new owner. These concerns materialized when Funnull modified Polyfill.io's scripts to inject malicious code delivered through their CDN. As a result, any website using scripts from cdn.polyfill.io was unknowingly compromised.

#3 The malicious code primarily targeted mobile devices and redirected users to scam websites, including gambling and pornography. There were also possibilities of phishing attacks to steal sensitive user information or even further malware distribution. Despite the suspension of the domain, the impact remains extensive, with over 384,000 hosts still referencing the compromised script.

#4 Major platforms such as Hulu, Mercedes-Benz, JSTOR, Intuit, and the World Economic Forum were affected. Additionally, the suspected involvement of other CDNs like Bootcss, BootCDN, and Staticfile linked with the polyfill domain operator amplifies the scope of this supply-chain attack. In response, companies like Cloudflare and Namecheap have taken steps to mitigate the risk by taking control of the domain, but the incident underscores the ongoing challenges in securing supply chains in the digital ecosystem.

Recommendations

Remove Polyfill.io References: Immediately audit your website's codebase and remove any references to the compromised Polyfill.io script to prevent further exposure to malicious redirects.

Use Self-Hosted Libraries: Host critical libraries and scripts locally rather than relying on third-party domains. This reduces the risk of supply chain attacks and ensures control over the integrity of the code.

Update Dependencies: Regularly update all third-party libraries and dependencies to the latest versions, ensuring they come from trusted and secure sources.

Content Security Policy (CSP): Implement a robust Content Security Policy (CSP) to control the sources of content that can be loaded on your site, reducing the risk of malicious scripts executing.

Monitor Traffic: Use security monitoring tools to track unusual traffic patterns or redirects, which can help in quickly identifying and responding to malicious activity.

Implement Subresource Integrity (SRI): Use SRI to verify that resources fetched from third-party sources have not been tampered with. This helps in ensuring that the fetched resources are delivered without unexpected modifications.

Regular Security Audits: Conduct regular security audits of your codebase and dependencies to identify and address potential vulnerabilities. This proactive approach helps in early detection and mitigation of risks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0042** Resource Development
T1195 Supply Chain Compromise	**T1195.001** Compromise Software Dependencies and Development Tools	**T1059** Command and Scripting Interpreter	**T1583.001** Domains
T1583 Acquire Infrastructure	**T1059.007** JavaScript		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	Polyfill[.]io bootcdn[.]net, bootcss[.]com, staticfile[.]net, staticfile[.]org, unionadjs[.]com, xhsbpza[.]com, union[.]macoms[.]la, newcrbpc[.]com
URLs	hxxp://kuurza[.]com/redirect?from=bitget, hxxp://www[.]googie-anaiytics[.]com/html/checkcachehw[.]js, hxxp://www[.]googie-anaiytics[.]com/ga[.]js, hxxp://cdn[.]bootcss[.]com/highlight[.]js/9[.]7[.]0/highlight[.]min[.]js, hxxp://union[.]macoms[.]la/jquery[.]min-4[.]0[.]2[.]js, hxxp://newcrbpc[.]com/redirect?from=bscbc

References

https://sansec.io/research/polyfill-supply-chain-attack

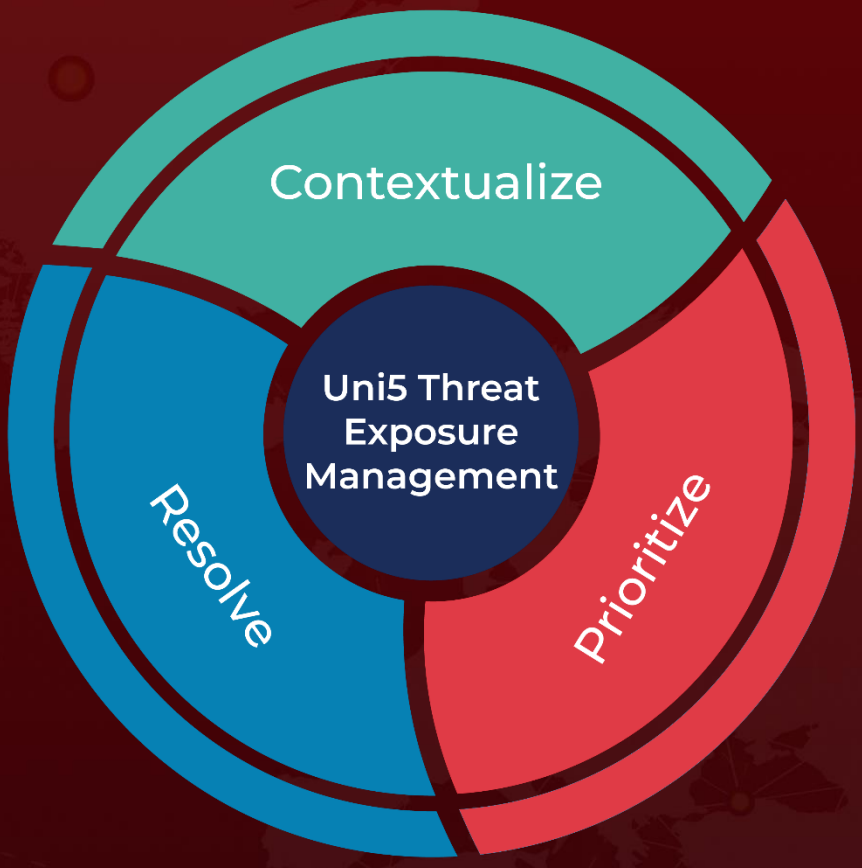
https://x.com/silentpush_labs/status/1806055707642384802

https://x.com/triblondon/status/1761852117579427975

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 4, 2024 • 7:30 AM

More at www.hivepro.com