Tracking the DNS Footprint of the Polyfill Supply Chain Attackers

Table of Contents

Executive Report

Threat actors can often find targeting certain organizations too much of a challenge. So they need to go through what we can consider back channels—suppliers, vendors, or service providers. The Polyfill supply chain attack may fall into this category, as users with vulnerable content delivery network (CDN) service versions ended up with compromised networks courtesy of a malicious JavaScript code.

A polyfill is a piece of JavaScript code that enables older browsers to have modern functionality they do not natively support. A report on the attack revealed the perpetrators obtained popular polyfill open-source projects and infected the code by injecting malicious scripts into them. Users who downloaded compromised polyfills primarily on mobile devices were then redirected to scam sites.

Many cybersecurity researchers looked into the attack and identified indicators of compromise (IoCs). The WhoisXML API research team got hold of a list of six domains identified as such and examined them more closely to identify other potentially connected artifacts. Our IoC list expansion led to the discovery of:

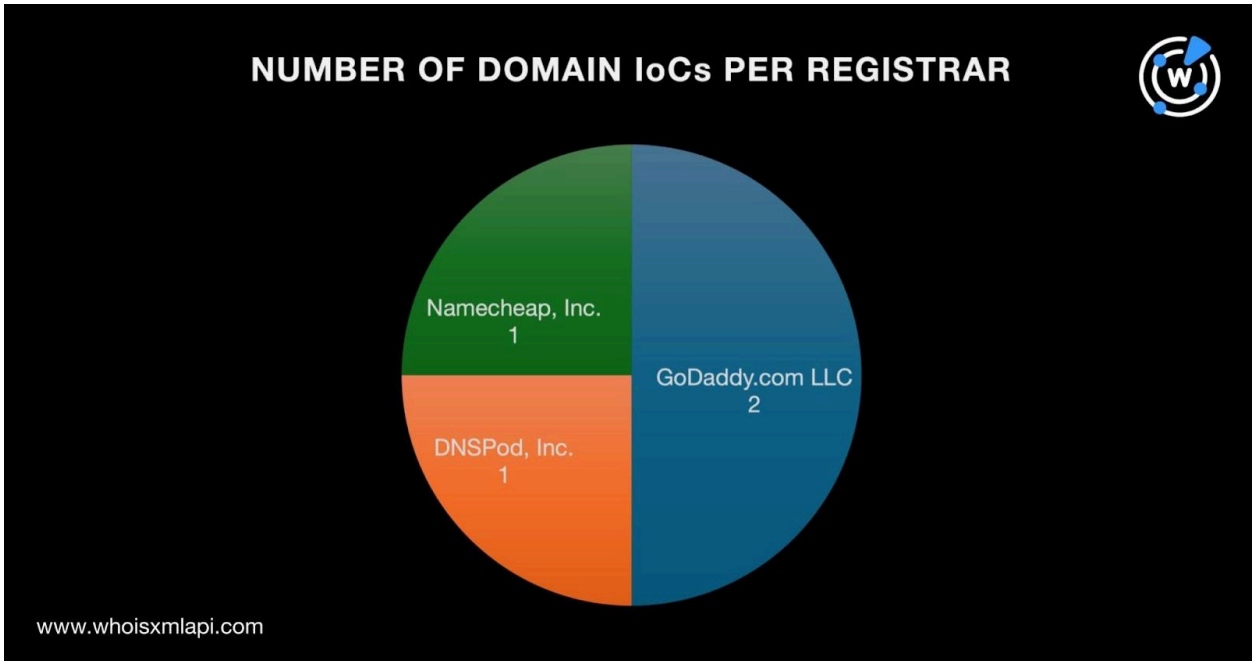
- Six IP addresses, two of which turned out to be malicious
- 104 IP-connected domains
- 94 string-connected domains

More on the Polyfill Attack IoCs

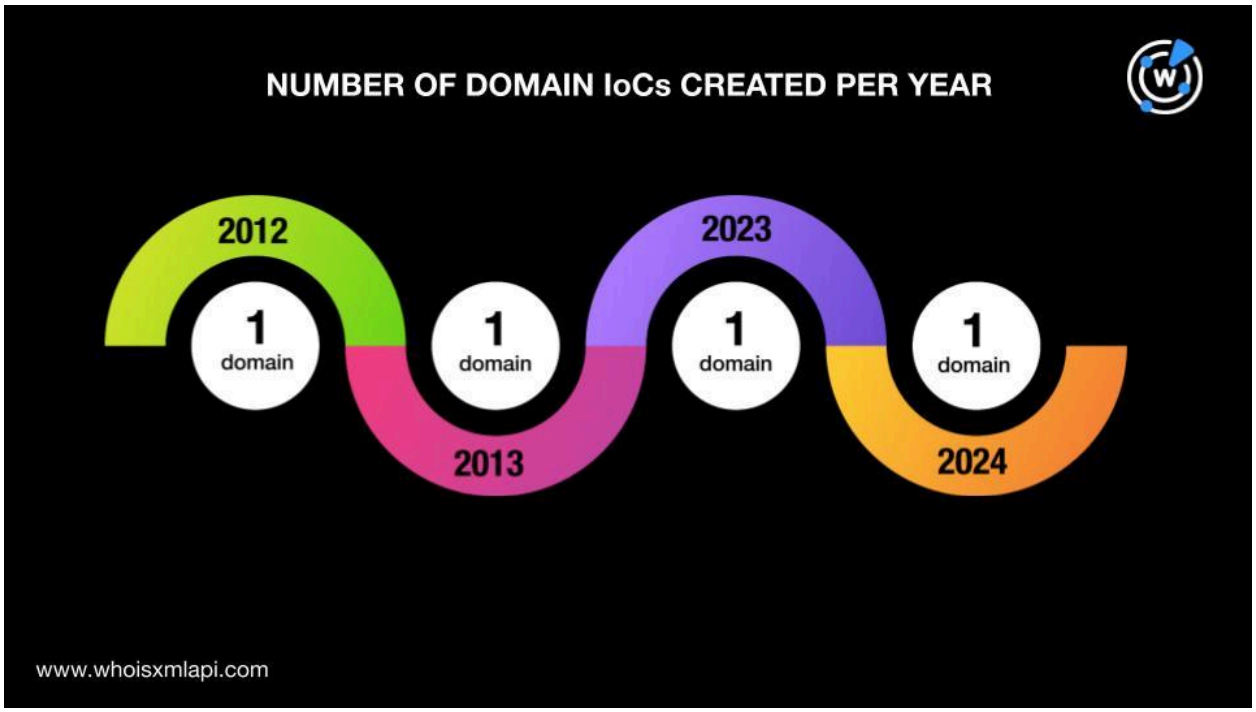
To gain a better understanding of the Polyfill attack infrastructure, we looked closer into the six domains identified as IoCs starting with a bulk WHOIS lookup, which revealed that:

- Only four of the six domains had current WHOIS records.

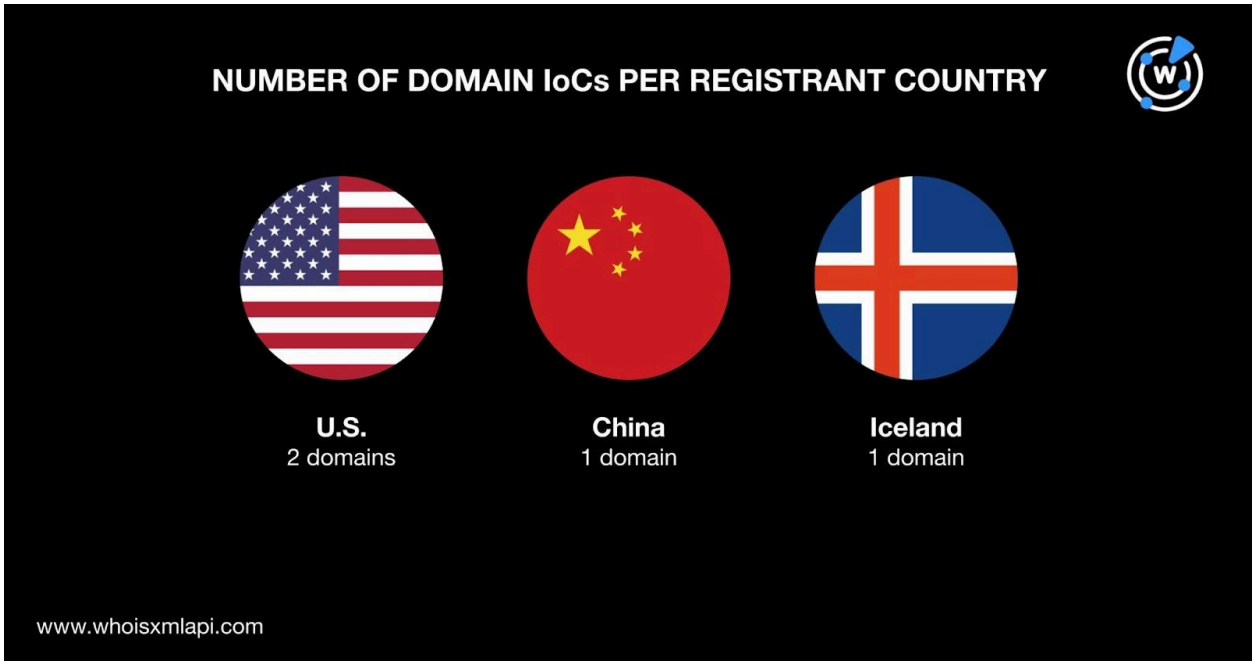
- GoDaddy.com LLC led the pack of registrars, accounting for two domain IoCs. DNSPod, Inc. and Namecheap, Inc. accounted for one domain IoC each.



- The threat actors used a mix of newly registered and aged domains given that the IoCs were created between 2012 and 2024.



- The U.S. was the top registrant country, accounting for two domain IoCs. China and Iceland accounted for one domain IoC each.



Polyfill Attack DNS Traces

If there's one thing all cyber attacks have in common, it's that their perpetrators always leave traces behind. We sought to find such through an IoC expansion analysis for the February 2024 Polyfill supply chain attack.

We began by querying the four domain IoCs on WHOIS History API, which revealed the presence of four email addresses in their historical WHOIS records after duplicates were filtered out. Two of the email addresses were redacted while the other two were public.

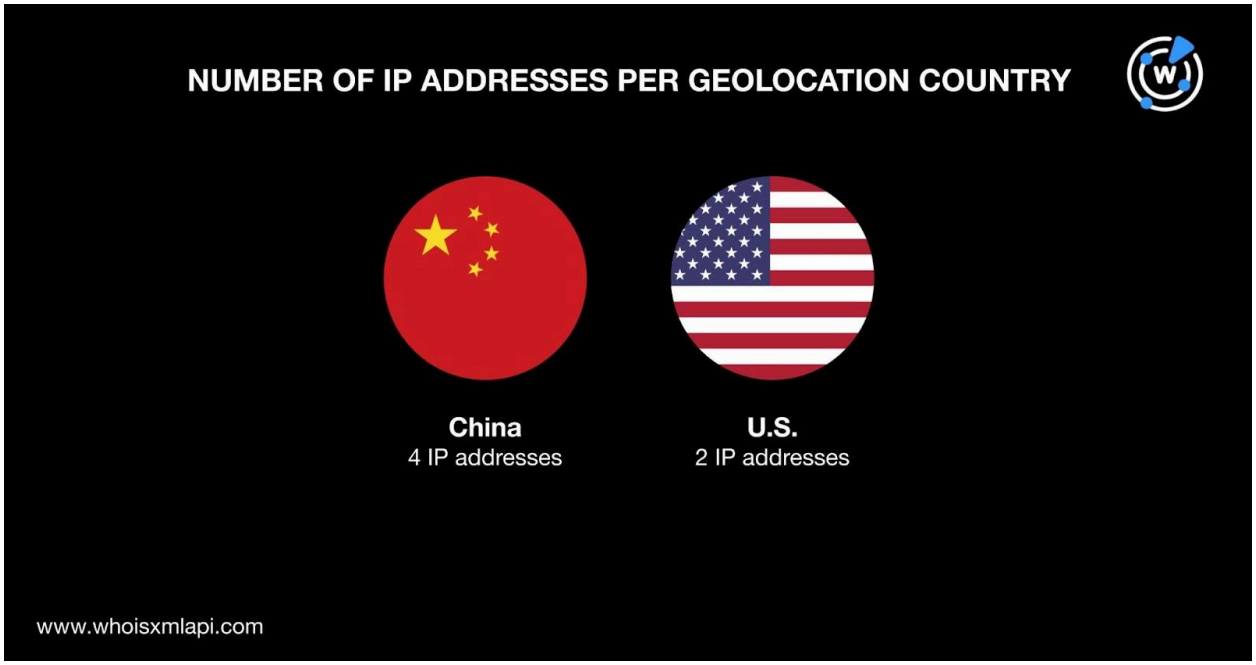
Our Reverse WHOIS API queries for the two public email addresses showed that only one appeared in the current WHOIS records of other domains. However, given that the said public email address turned up in the records more than 10,000 domains, it could belong to a domainer.

Next, we ran DNS lookups for the four domains identified as IoCs and found that they resolved to six IP addresses after duplicates were removed.

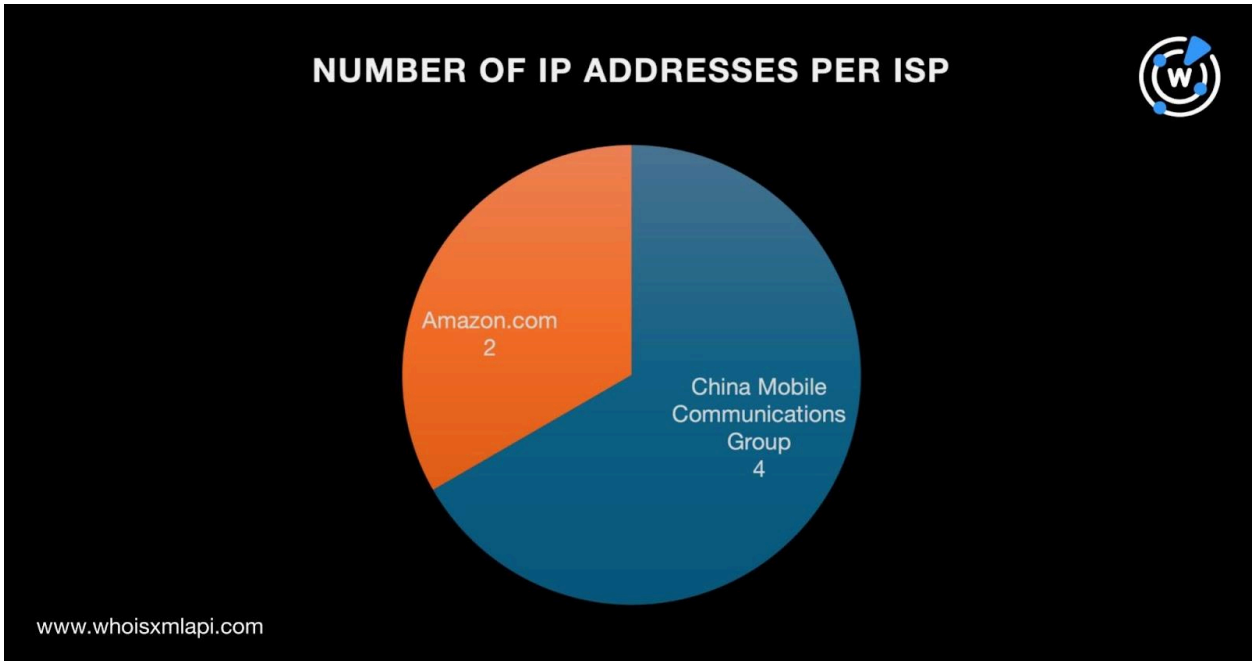
Threat Intelligence Lookup revealed that two of the IP addresses were associated with every kind of threat we track—attacks, command and control (C&C), generic threats, malware infections, phishing, spam campaigns, and suspicious activities.

A bulk IP geolocation lookup for the six IP addresses showed that:

- They were spread across two countries. Four were geolocated in China and the remaining two in the U.S. Note that these two nations also appeared in the list of registrant countries.



- The six IP addresses were also split between two ISPs. Four were administered by the China Mobile Communications Group while two fell under the purview of Amazon.com.



The reverse IP lookups we did earlier also revealed that four of the IP addresses could be dedicated. Altogether, they hosted 104 domains after duplicates and the IoCs were filtered out.

As the last step in our analysis, we looked for domains that resembled the four domain IoCs. We specifically used the **Domains only** and **Starts with** parameters for our Domains & Subdomains Discovery queries for these text strings:

- **bootcss.**
- **googie-anaiytics.**
- **kuurza.**
- **polyfill.**

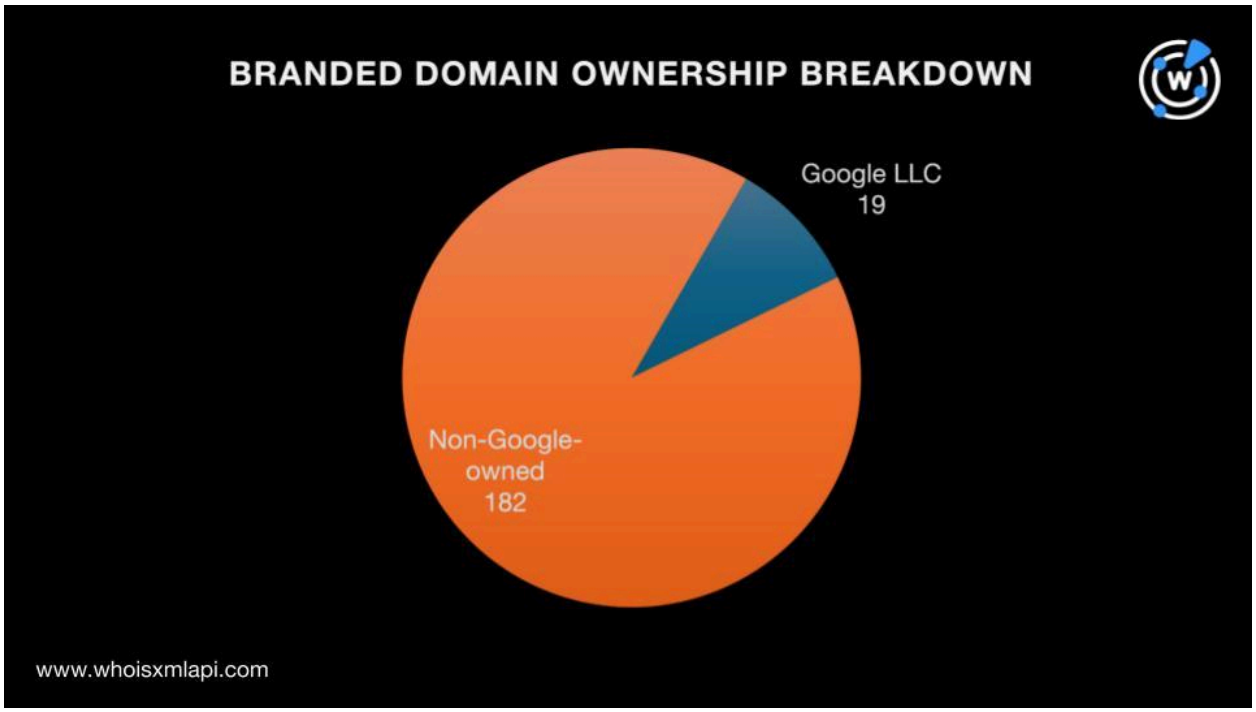
Our searches turned up results for only two of the strings (i.e., **bootcss.** and **polyfill.**). We found 94 string-connected domains.

Signs of Google Analytics Spoofing

One of the domains identified as IoCs—googie-anaiytics[.]com—seem to be taking advantage of the Google Analytics brand. Other attacks could be typosquatting on the brand's popularity as well.

We used the **Domains only** and **Starts with** parameters on Domains & Subdomains Discovery to find other such domains containing the strings **google-analytics** and **googleanalytics**. Our queries turned up 642 branded domains after duplicates and the IoC were removed. However, note that only 201 of the branded domains had current WHOIS records.

WHOIS record comparisons with the Google Analytics subdomain under the Google domain revealed that only 19 of the domains containing the brand name could belong to Google. The remaining 182 could just be typosquatting on the brand's popularity and may be weaponized for future attacks, if they haven't already.



Finally, Threat Intelligence API queries for the 201 branded domains with current WHOIS record details showed that eight were associated with various threats. Here are three examples.

MALICIOUS BRANDED DOMAIN	ASSOCIATED THREAT TYPES
googleanalytics[.]com	Generic
googleanalytics[.]top	Malware
google-analytics[.]icu	Malware

—

Our DNS deep dive into the Polyfill supply chain attack unveiled 204 potentially connected artifacts comprising six IP addresses, 104 IP-connected domains, and 94 string-connected domains after expanding a list of just six IoCs. Two of the web properties we discovered have already been weaponized.

We also looked into domains possibly mimicking Google Analytics akin to one of the attack IoCs and found 622 web properties. A good number of them, 22 to be exact, have already figured in attacks. Note, however, that only 201 of the branded domains had current WHOIS records but only 19 could be publicly attributed to Google.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample IP Addresses

- 120[.]226[.]156[.]189
- 120[.]226[.]156[.]190
- 120[.]226[.]156[.]193

Sample IP-Connected Domains

- 001cq[.]com
- 03ak[.]com
- 100dll[.]com
- 100dll[.]com[.]trpcdn[.]net
- 17fgasddkd2ajnpsqs0na5li4tdihcdlttjcsg85bm8li7785mbvu6t5[.]tt[.]x[.]bsgslb[.]cn
- 268down[.]com
- 268down[.]com[.]trpcdn[.]net
- 512t[.]com
- 512t[.]com[.]trpcdn[.]net
- 66hyz[.]com
- 998youxi[.]com
- 998youxi[.]com[.]trpcdn[.]net
- adsteam[.]cn
- allviedeo[.]xjclass[.]com
- allviedeo[.]xjclass[.]com[.]bsclink[.]cn
- apk101[.]com
- apk101[.]com[.]trpcdn[.]net
- baofeng[.]com
- baofeng[.]com[.]bsclink[.]cn
- bootcss[.]com[.]bsclink[.]cn

Sample String-Connected Domains

- bootcss[.]accountant
- bootcss[.]bid
- bootcss[.]biz
- bootcss[.]cc

- bootcss[.]club
- bootcss[.]cm
- bootcss[.]cn
- bootcss[.]co
- bootcss[.]com[.]cn
- bootcss[.]dev
- polyfill[.]ai
- polyfill[.]app
- polyfill[.]arab
- polyfill[.]at
- polyfill[.]be
- polyfill[.]biz
- polyfill[.]blog
- polyfill[.]ca
- polyfill[.]cc
- polyfill[.]ch

Sample Typosquatting Domains

- google-analytics-4-property[.]com
- google-analytics-cdn33[.]cfd
- google-analytics-cn[.]com
- google-analytics-audits[.]com
- google-analytics-kurs[.]ch
- google-analytics-book[.]com
- google-analytics-newsletter[.]app
- google-analytics-tag-21[.]com
- google-analytics-plus[.]com
- google-analytics-tag-19[.]com
- google-analytics-tanacsadas[.]hu
- google-analytics[.]be
- google-analytics[.]ch
- google-analytics[.]bond
- google-analytics[.]cl
- google-analytics[.]cc
- google-analytics[.]co[.]kr
- google-analytics[.]co[.]uk
- google-analytics[.]co
- google-analytics[.]com[.]cn
- google-analytics[.]cz
- google-analytics[.]com
- google-analytics[.]cn
- google-analytics-training[.]com
- google-analytics-utbildning[.]se
- google-analytics[.]hu
- google-analytics[.]info
- google-analytics[.]io
- google-analytics[.]icu
- google-analytics[.]ie
- google-analytics[.]kr
- google-analytics[.]is
- google-analytics[.]nl
- google-analytics[.]link
- google-analytics[.]org[.]cn
- google-analytics[.]ru
- google-analytics[.]online
- google-analytics[.]me
- google-analytics[.]net
- google-analytics[.]org
- google-analytics[.]tech
- google-analytics[.]pro
- google-analytics[.]top
- google-analytics[.]xyz
- google-analytics[.]zip
- google-analytics4[.]com
- google-analytics101[.]com
- google-analyticss[.]com
- google-analyticsc[.]com
- google-analyticsclc[.]top