Cross-Examining the CAPTCHAgeddon Brought on by ClickFix

Table of Contents

Executive Report

Guardio reported about the ClickFix stealer that is considered an evolved version of fake browser updates. Instead of relying on a file download, it used fake CAPTCHA pages that allowed it to evade detection more effectively. It beat popular anti-bot solutions when users clicked the **Verify** button, which copied a malicious PowerShell command for its execution. As a result, it exfiltrated victims' account credentials and other data from their computers.

The company published their findings in "'CAPTCHAgeddon': Unmasking the Viral Evolution of the ClickFix Browser-Based Threat," naming at least 172 indicators of compromise (IoCs) in the process comprising 156 domains and 16 IP addresses.

WhoisXML API analyzed the IoCs further. Our deep dive led to these discoveries:

- 1,156 unique client IP addresses communicated with 11 unique domain IoCs based on sample DNS traffic data from the Internet Abuse Signal Collective (IASC)
- Two alleged victim IP addresses communicated with three unique IP IoCs based on sample IASC DNS traffic data
- 30 of the domains identified as IoCs were deemed likely to turn malicious 51–209 days before they were dubbed as such

We also expanded the current list of IoCs and uncovered:

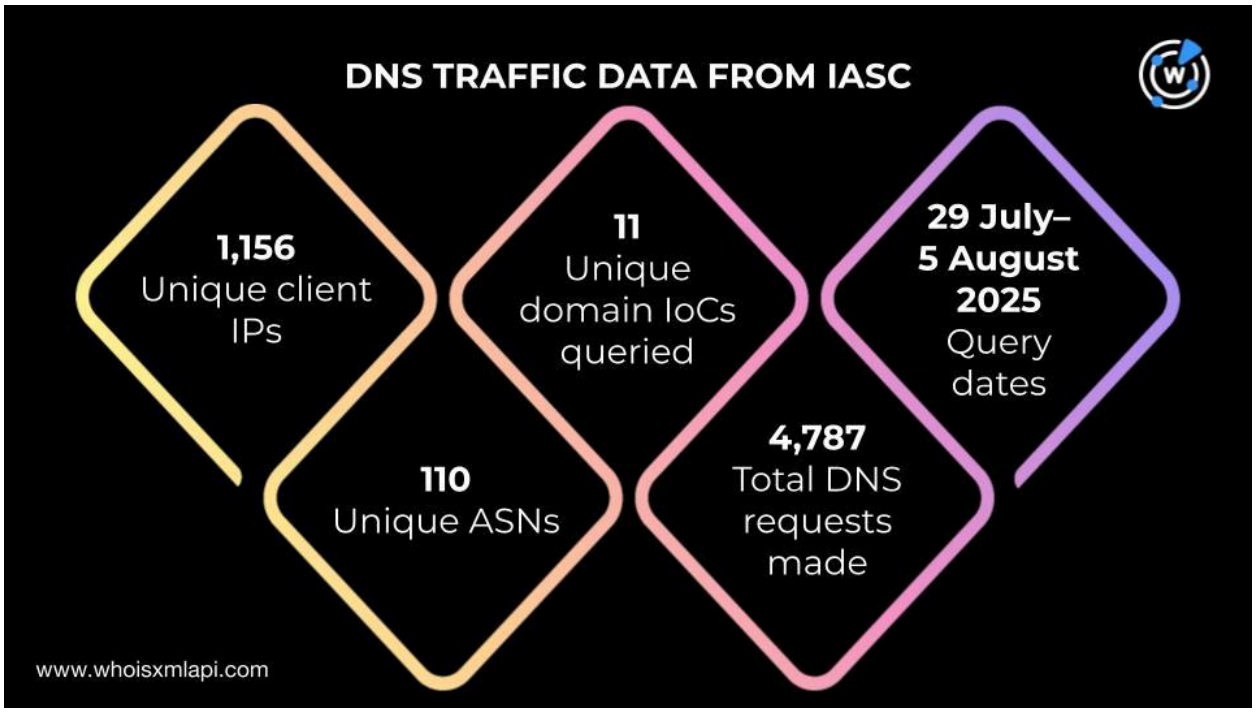
- 289 registrant-connected domains
- 193 email-connected domains, one was malicious
- 133 additional IP addresses, 86 were malicious
- 1,037 IP-connected domains, 28 were malicious
- 3,412 string-connected domains, 30 were malicious

More on the ClickFix IoCs

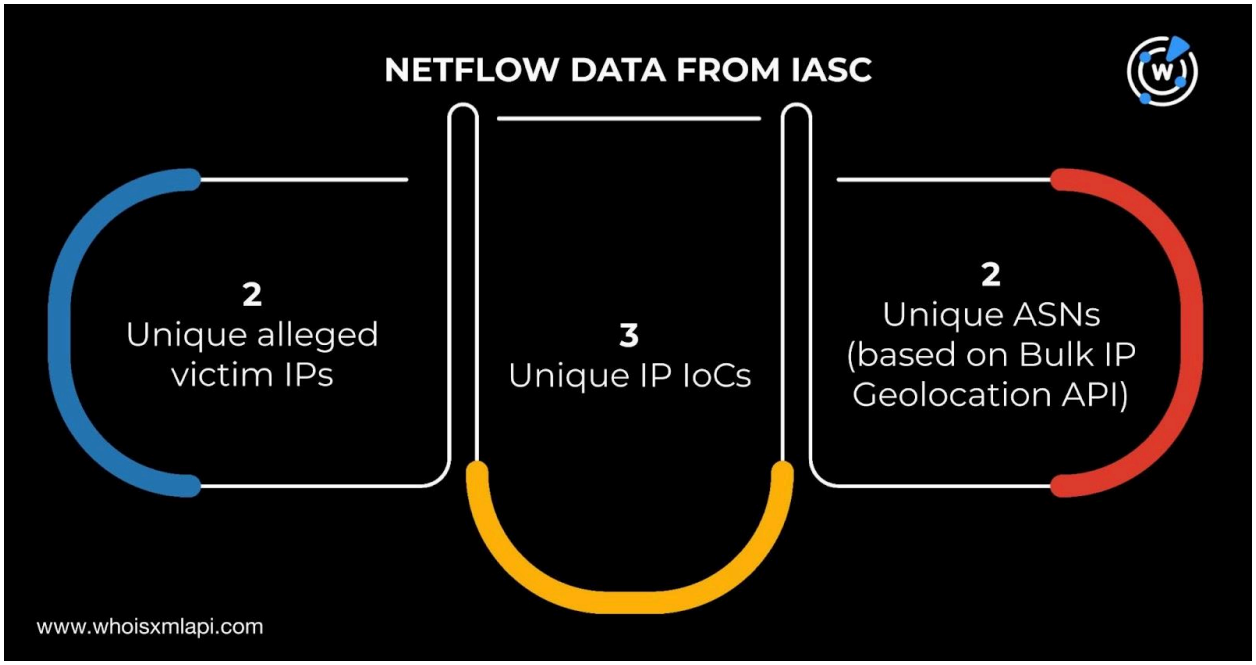
Our deeper dive into the 172 IoCs Guardio identified has two parts. The first delved into insights gleaned from an analysis of the data using sample DNS traffic data from IASC. The second, meanwhile, dove into our findings from our extensive array of intelligence.

Analyzing the IASC Data

Sample DNS traffic data from IASC revealed that 1,156 unique client IP addresses under 110 unique Autonomous System numbers (ASNs) communicated with 11 unique domains identified as IoCs via 4,787 DNS queries made between 29 July 2025 and 5 August 2025.



Another set of IASC data showed that two unique alleged victim IP addresses communicated with three unique IP addresses identified as IoCs under two unique ASNs based on the results of a Bulk IP Geolocation Lookup query.



Diving into WhoisXML API Intelligence

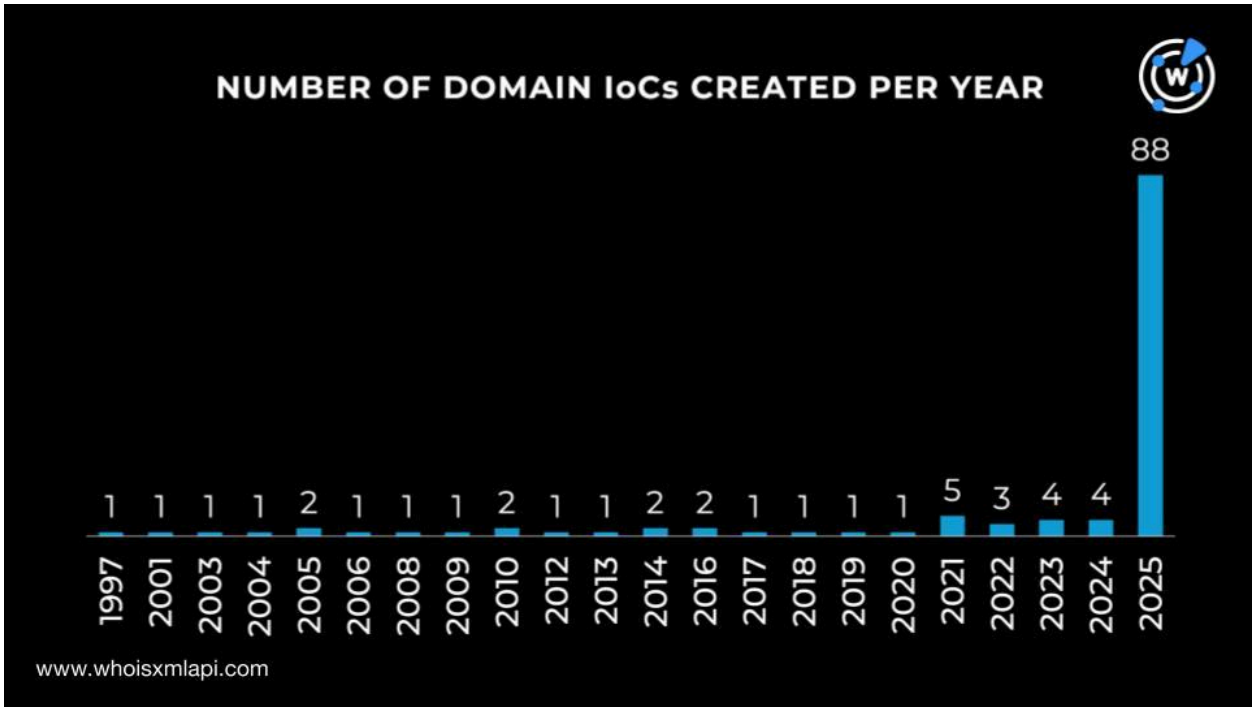
We began our foray by checking which of the 156 domains identified as IoCs appeared on the First Watch Malicious Domains Data Feed. We found out that 30 of the domains were deemed likely to turn malicious 51–209 days before they were dubbed as such on 6 August 2025. Take a look at more details for five of them below.

DOMAIN IoCs	FIRST WATCH ADDITION DATE	NUMBER OF DAYS DEEMED LIKELY TO TURN MALICIOUS BEFORE REPORTING DATE
companystarlink[.]com	9 January 2025	209
companybonuses[.]org	14 January 2025	204
loyalcompany[.]net	15 January 2025	203
usersmanualplatforms19[.]site	14 March 2025	145
candyconverterpdf[.]com	25 March 2025	134

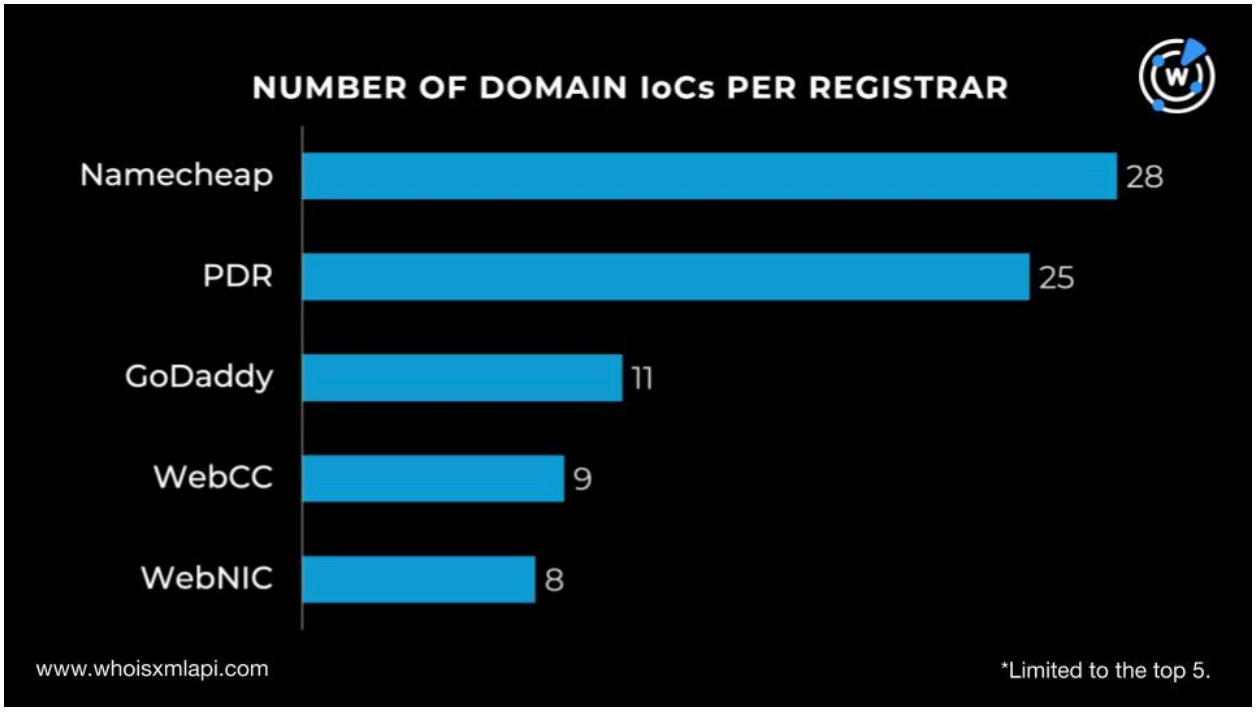
Next, we queried the 156 domains identified as IoCs on Bulk WHOIS API and discovered that:

- Only 125 domains had current WHOIS records.

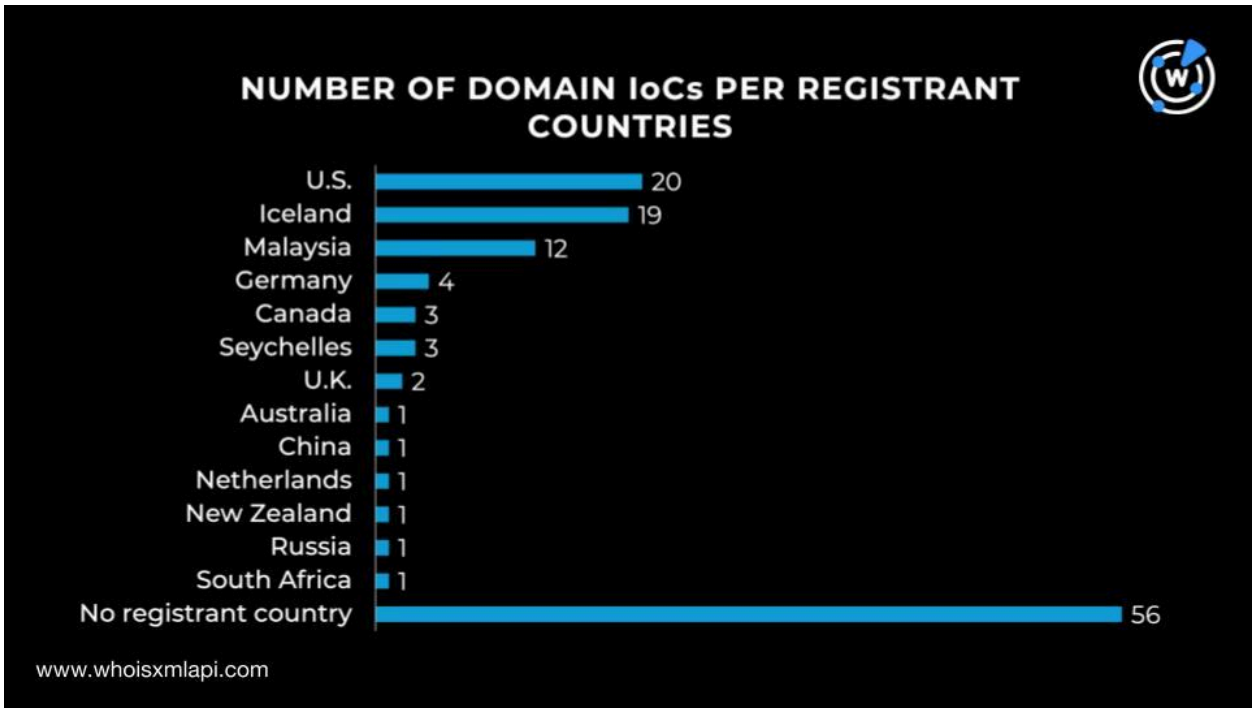
- The 125 domains with current WHOIS records were created between 9 September 1997 and 19 June 2025. A majority, 88 to be exact, were created in 2025, hinting that the threat actors preferred to use newly registered domains (NRDs). In addition, 37 were created between 1997 and 2024.



- The top 5 registrars were Namecheap, which accounted for 28 domains; PDR for 25; GoDaddy for 11; WebCC for nine; and WebNIC for eight. The rest of the 44 domains were spread across 30 other registrars. They comprised OPENPROV-RU (five domains); NameSilo (four domains); NiceNIC (three domains); Bluehost, Global Domain Group, GMO Internet, Porkbun, and Wild West Domains (two domains each); and Amazon, CentralNIC, Cosmotown, Divido, Dreamscape Networks International, Dynadot, eNom, Eranet International, Gostovanje in Domene, Hello Internet, Hosting Concepts, Hostinger Operations, Instra, Internet Domain Service, Isimtescil Bilisim, Prado Ramiro Sebastian, R01-SU, Reg.ru, Squarespace Domains, Tucows, United-Domains, and URL Solutions (one domain each).



- While 56 domains did not have registrant countries on record, 69 were spread out among 13 nations. A total of 20 domains were registered in the U.S.; 19 in Iceland; 12 in Malaysia, four in Germany; three each in Canada and Seychelles; two in the U.K.; and one each in Australia, China, the Netherlands, New Zealand, Russia, and South Africa.



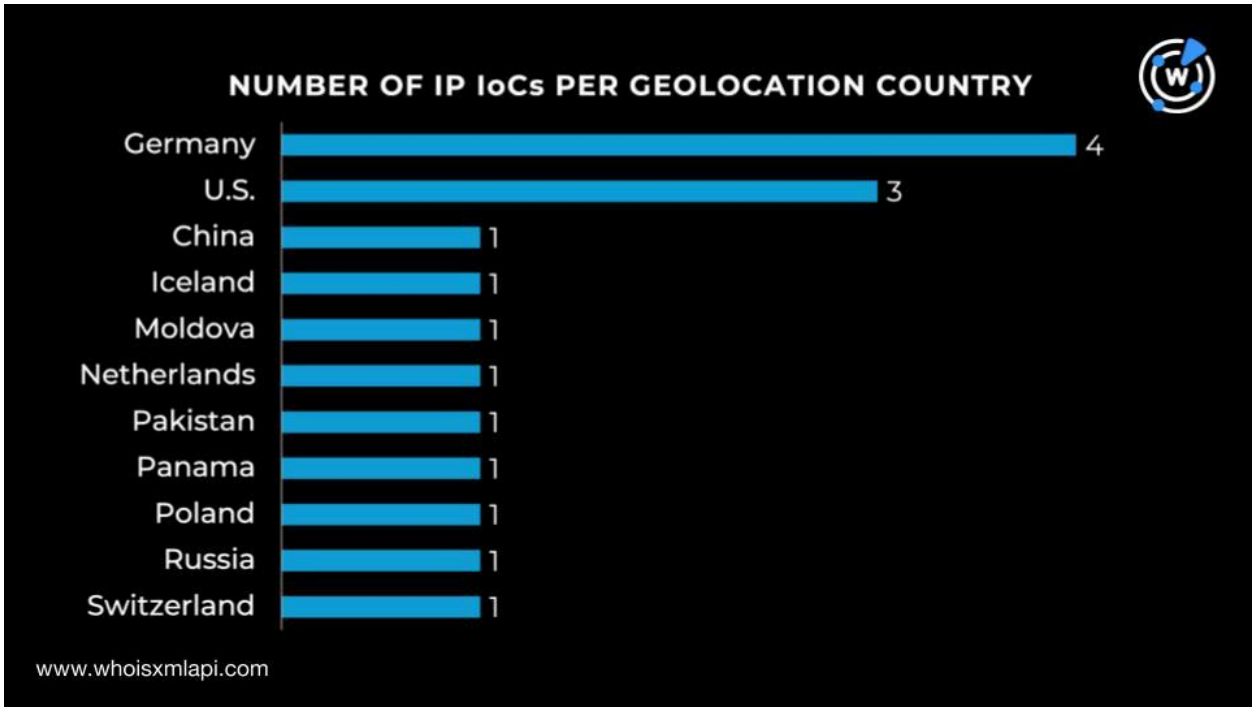
- Eleven domains had 11 unique registrant names on record.

A DNS Chronicle API query for the 156 domains identified as IoCs revealed that 136 had 17,287 historical domain-to-IP resolutions. The domains aasiwins[.]com, appmacosx[.]com, apposx[.]com, attlaw[.]com, autura[.]com, billiboard[.]com, buzzedcompany[.]com, cwbchicago[.]com, and deathtotheworld[.]com recorded the oldest resolutions on 5 February 2017. Take a look at the DNS histories of five domains below.

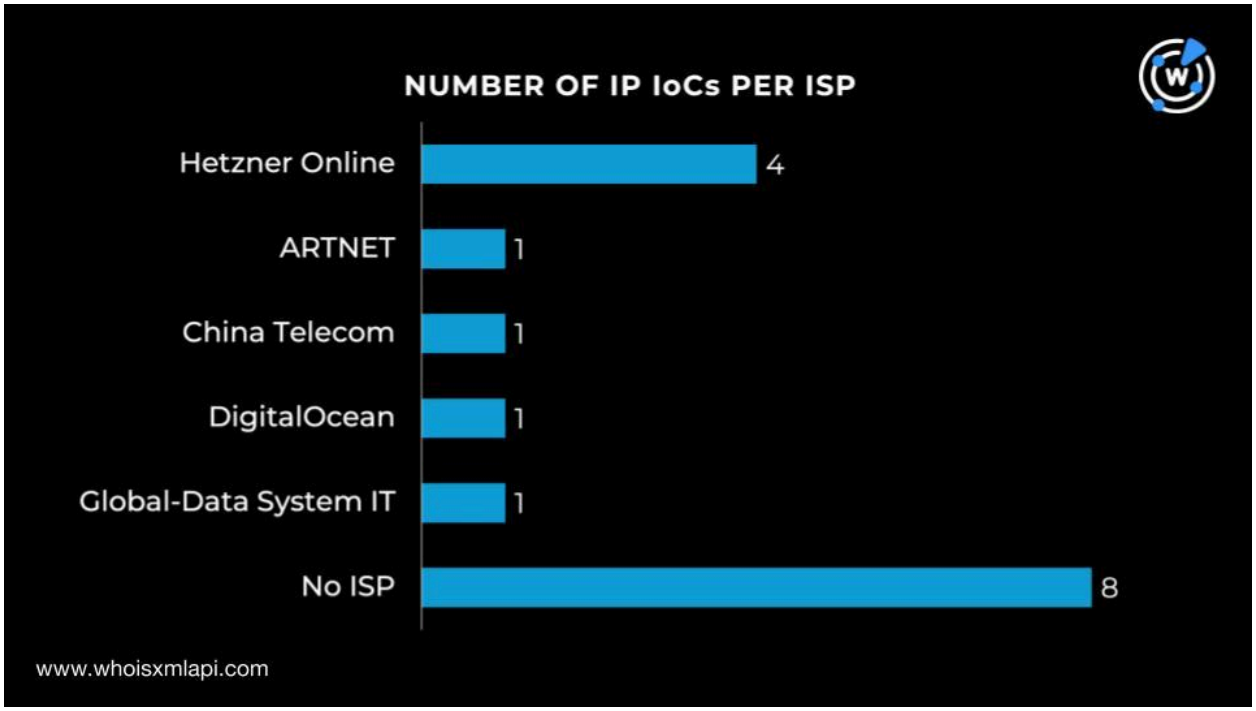
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	FIRST DOMAIN-TO-IP RESOLUTION DATE
aasiwins[.]com	380	5 February 2017
appmacosx[.]com	29	5 February 2017
billiboard[.]com	329	5 February 2017
cwbchicago[.]com	630	5 February 2017
deathtotheworld[.]com	316	5 February 2017

Next, we queried the 16 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in 11 different countries led by Germany, which accounted for four IP addresses. The U.S. placed second with three IP addresses. One IP address each was geolocated in China, Iceland, Moldova, the Netherlands, Pakistan, Panama, Poland, Russia, and Switzerland.



- While eight IP addresses did not have ISPs on record, the rest were distributed among five ISPs. Hetzner Online accounted for four IP addresses while ARTNET, China Telecom, DigitalOcean, and Global-Data System IT accounted for one each.



A DNS Chronicle API query for the 16 IP addresses identified as IoCs uncovered 2,417 IP-to-domain resolutions over time. The IP address 181[.]174[.]164[.]117 posted 260 resolutions since 6 February 2017. Here are historical DNS details for five other IP addresses.

IP ADDRESS IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	FIRST IP-TO-DOMAIN RESOLUTION DATE
88[.]119[.]175[.]52	777	24 August 2019
195[.]201[.]221[.]109	642	26 February 2017
212[.]11[.]64[.]215	240	21 July 2017
159[.]223[.]139[.]207	230	10 December 2021
162[.]55[.]47[.]21	92	23 April 2021

We used the following prompts on the WhoisXML API MCP Server:

- Get the DNS histories of the domains fepez.run, fessoclick.com, figurefaceted.ru, flammablegrunt.site, gbhjj.online, gettsveriff.com, gfddx.run, glsrvc.cloud, gmkkeycap.com, gozog.run, hastilybakeshop.ru, hipercompany.com, homeeick.com, honis.fun, howtocookportuguesestuff.com, and hypertrophyhphied.homes.
- Use IP Netblocks to verify IP ownership of 104.21.16.1, 104.21.32.1, 104.21.48.1, 104.21.64.1, 104.21.80.1, 104.21.96.1, and 104.21.112.1.
- Were there any IP commonalities over time across the domains above?

The results showed that the domains fepez[.]run, gfddx[.]run, and homeeick[.]com all used the Cloudflare IP addresses 104[.]21[.]16[.]1, 104[.]21[.]32[.]1, 104[.]21[.]48[.]1, 104[.]21[.]64[.]1, 104[.]21[.]80[.]1, 104[.]21[.]96[.]1, and 104[.]21[.]112[.]1 in May 2025.

Comprehensive Analysis of IP Addresses 104.21.x.1 Series

Based on the IP netblock verification, I can confirm that **ALL seven IP addresses** you listed are definitively owned and operated by **Cloudflare, Inc.**

Verified Ownership Details:

IP Addresses Analyzed:

- 104.21.16.1
- 104.21.32.1
- 104.21.48.1
- 104.21.64.1
- 104.21.80.1
- 104.21.96.1
- 104.21.112.1

Confirmed Owner Information:

Organization: Cloudflare, Inc. **Network Name:** CLOUDFLARENET **ASN:** 13335
Organization ID: CLOUD14 **Registry:** ARIN (American Registry for Internet Numbers)

Implications:

The fact that domains **fepez.run**, **gfddx.run**, and **homeeick.com** all share this exact same set of seven Cloudflare IP addresses strongly indicates:

1. They're using identical Cloudflare configurations
2. They were likely set up by the same entity or using the same template
3. They're all protected by Cloudflare's proxy service, hiding their actual origin servers

On top of that, eight of the IP addresses, while not necessarily all Cloudflare owned, were first configured or first appeared in May 2025.

Timing Patterns

May 2025 Cluster A significant number of domains first appeared or were configured in May 2025:

- fepez.run (May 10)
- gfddx.run (May 8)
- homeeick.com (May 6)
- gozog.run (May 7)
- hastilybakeshop.ru (May 29)
- gbhjj.online (May 15)
- gettsveriff.com (May 17)
- glsrvc.cloud (May 30)

This temporal clustering in May 2025, combined with the shared Cloudflare IPs for some domains, suggests coordinated registration or setup.

Expanding the Current List of ClickFix IoCs

Earlier, we mentioned that we found 11 unique registrant names for 11 of the 156 domains identified as IoCs. We queried them on Reverse WHOIS API and found out that they appeared in the current WHOIS records of 289 domains after duplicates and those already tagged as IoCs were filtered out.

Next, we queried the 156 domains identified as IoCs on WHOIS History API and uncovered 40 unique email addresses from their historical WHOIS records. Further scrutiny showed that 10 were public email addresses.

While none of them appeared in the current WHOIS records of any other domains based on the results of our Reverse WHOIS API queries, five of the 10 public email addresses were seen in the historical WHOIS records of 193 domains after duplicates, those already identified as IoCs, and the registrant-connected domains were filtered out.

A Threat Intelligence API query for the 193 email-connected domains revealed that one—znm[.]lol—has already been weaponized for malware distribution.

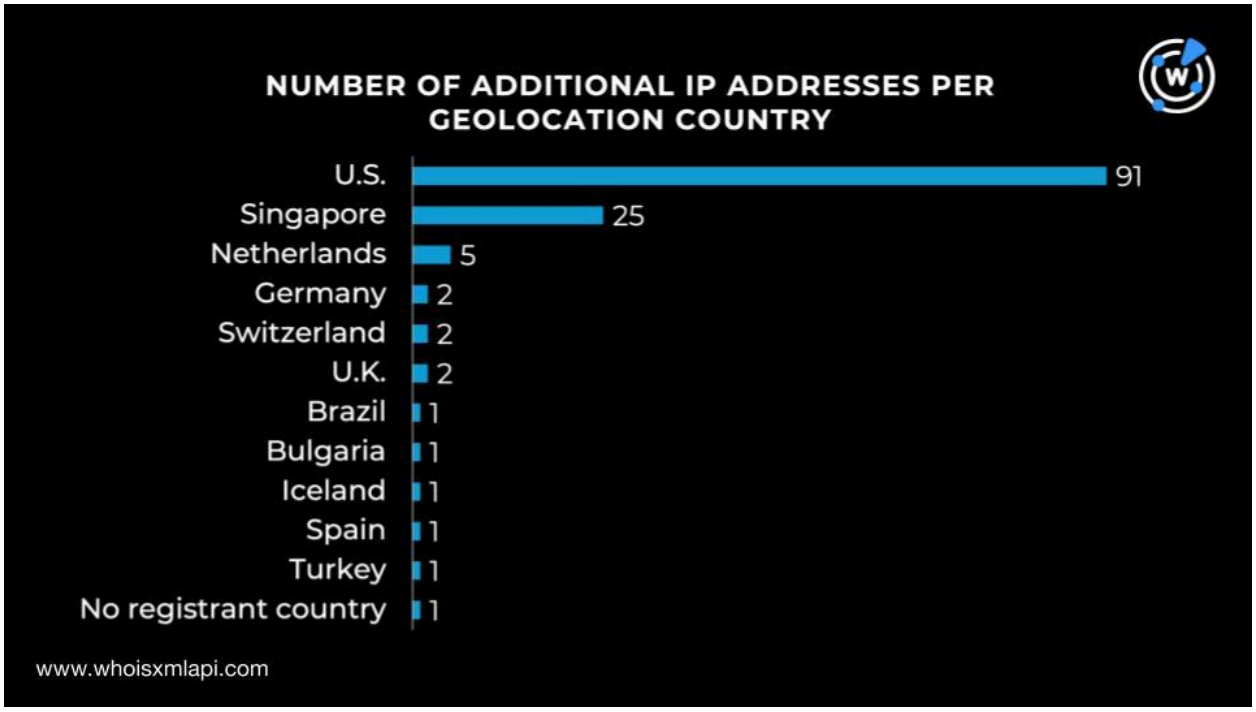
After that, we queried the 156 domains identified as IoCs on DNS Lookup API. We found out that 80 actively resolved to 133 unique IP addresses. None of them were part of the current list of IoCs.

A Threat Intelligence API query for the 133 additional IP addresses showed that 86 have already been weaponized for various attacks. Here are five examples.

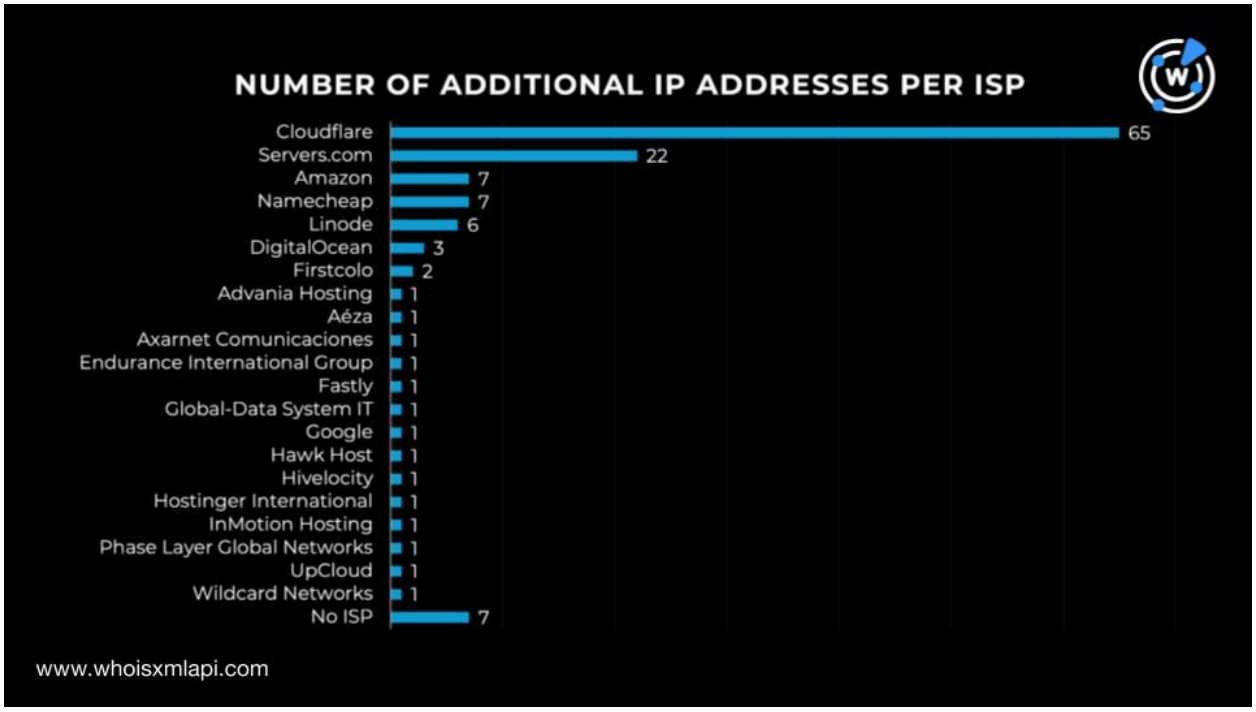
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREATS
104[.]19[.]154[.]92	Phishing Suspicious activity Generic threat
104[.]21[.]112[.]1	Phishing Malware distribution Suspicious activity Generic threat Command and control (C&C Spam campaign
104[.]21[.]16[.]1	Phishing Malware distribution Generic threat Suspicious activity C&C Spam campaign
104[.]21[.]27[.]249	Malware distribution
104[.]21[.]28[.]80	Phishing Malware distribution Generic threat

Next, we queried the 133 additional IP addresses on Bulk IP Geolocation Lookup and discovered that:

- While one did not have a geolocation country on record, the rest were spread across 11 different countries. A total of 91 were geolocated in the U.S.; 25 in Singapore; five in the Netherlands; two each in Germany, Switzerland, and the U.K.; and one each in Brazil, Bulgaria, Iceland, Spain, and Turkey.



- While seven did not have ISPs on record, the rest were spread across 21 ISPs led by Cloudflare, which accounted for 65 IP addresses. Servers.com came in second place with 22 IP addresses. Amazon and Namecheap tied for third place with seven IP addresses each. Linode took the fourth spot with six IP addresses. DigitalOcean had three IP addresses; Firstcolo had two; and Advania Hosting, Aéza, Axarnet Comunicaciones, Endurance International Group, Fastly, Global-Data System IT, Google, Hawk Host, Hivelocity, Hostinger International, InMotion Hosting, Phase Layer Global Networks, UpCloud, and Wildcard Networks had one each.



- The U.S., the Netherlands, Germany, and Iceland appeared in the list of geolocation countries for the IP IoCs and additional IP addresses.
- DigitalOcean and Global-Data System IT appeared in the list of ISPs for the IP IoCs and additional IP addresses.

A Reverse IP API query for the 149 IP addresses (i.e., 16 identified as IoCs and 133 additional) revealed that 47 could be dedicated hosts. Altogether, they hosted 1,037 IP-connected domains after duplicates, those already tagged as IoCs, and the registrant- and email-connected domains were filtered out.

Next, we queried the 1,037 IP-connected domains on Threat Intelligence API and discovered that 28 have already been weaponized for various attacks. Take a look at five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREATS
10x07[.]ink	Malware distribution
73ed366d3137ec936bd60b1184467776[.]com	Malware distribution
908df012d9bb72e6d26b41054588d758[.]com	Malware distribution
bealafulup[.]com	Malware distribution

chaerel[.]com	Malware distribution

A closer look at the 156 domains identified as IoCs allowed us to ascertain they started with 155 unique text strings. Domains & Subdomains Discovery searches revealed that other domains started with exact matches of 100 strings. We named a few of them below.

- 4x4x.
- aasiwins.
- bad-guest-reviewsid77182.
- candlyphoto.
- dashes.
- ee.
- fepez.
- gbhjj.
- hastilybakeshop.
- jupiters.
- kapilarya.
- lacalle.
- macosxappstore.
- nates.
- odyssey1.
- peasplecore.
- qrgen-ai.
- recaptchas.
- s-t-o-r-e-s.
- taken.
- unrimedironize.
- vfr-actevate.
- wgetfiles.
- xgg.
- z98123.

All in all, our search led to the discovery of 3,412 string-connected domains.

Finally, a Threat Intelligence API query for the 3,412 string-connected domains determined that 30 have already been weaponized for various attacks. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREATS
assets-msn[.]live	Malware distribution
betamode[.]click	Generic threat Phishing
bitly[.]best	Malware distribution
bitly[.]bz	Malware distribution
bitly[.]cam	Malware distribution

—

Our in-depth investigation of ClickFix enabled us to determine that 1,156 unique client IP addresses communicated with 11 unique domains identified as IoCs based on sample IASC DNS traffic data. Two alleged victim IP addresses also communicated with three unique IP addresses tagged as IoCs based on sample IASC DNS traffic data. In addition, 30 of the domains identified as IoCs were deemed likely to turn malicious 51–209 days before they were dubbed as such.

We also unearthed 5,064 new artifacts comprising 289 registrant-connected domains, 193 email-connected domains, 133 additional IP addresses, 1,037 IP-connected domains, and 3,412 string-connected domains. Our analysis also revealed that 145 of these artifacts have already figured in various attacks.

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 Registrant-Connected Domains

- 1h-v[.]com
- 7bf55683d14775eeb395c7661cb68f84[.]net
- aafepay[.]com
- aaferpay[.]com
- access-rain[.]com
- adwcbleaner[.]com
- aferppay[.]com
- afrsrinag[.]com
- afsniqa[.]com
- afsnqia[.]com
- aiterpay[.]com
- aktualisieren-paypal[.]com
- alwardaldahabi[.]com
- aml-sec[.]net
- ansfniag[.]com
- api-sendgrid[.]com
- aqfsinag[.]com
- arbitrag-ripple-scanneer[.]com
- arbitrag-ripple-scanner[.]com
- arbitrag-ripple-scanners[.]com
- arbitrage-ripple-scanner[.]com
- arbitrage-ripple-scanners[.]com
- arbitragecomuniade[.]com
- arbitragecrp[.]com
- arbitragemike[.]com
- arbitragx[.]com
- arbtragecomunity[.]com
- arfsinag[.]com
- arsniag[.]com
- asfniqa[.]com
- asqfniag[.]com
- atrsniag[.]com
- baflf168[.]com
- beauttikids[.]com
- bestdancekids[.]com
- betftobet[.]com
- bhbbanx[.]com
- blebnder[.]com
- blender-3d-sotfware[.]com
- blendmer[.]com
- bliulf163[.]com
- bloco6[.]com[.]br
- blulff163[.]com
- bokcenpage[.]com
- bokpagecenter[.]com
- bokpagehelp[.]com
- bookinterpagecen[.]com
- broesrtores[.]com
- buelff[.]com

Sample Email-Connected Domains

- redosiermetrocafe[.]com
- redosiernews[.]com
- redosierroastbeef[.]com
- redosierrochester[.]com
- rereflect[.]com
- rnkenter[.]com
- rosasweddingcreations[.]com
- rpr[.]lol
- rxr[.]lol
- rzr[.]lol
- simpleonlinesite[.]com
- simpleonlinesite[.]net
- sparkysautorepair[.]com
- stytex[.]de
- superbtoysforkids[.]com
- testingthesite[.]net

- texasholdmnow[.]com
- thehdnation[.]com
- thehealthyindianproject[.]com
- thelodgeatbataviacc[.]com
- themotorcyclestoreonline[.]com
- townsend-ny[.]com
- townsendenergy[.]com
- townsendoil[.]net
- tpegbuysbills[.]com
- tpegshouldbuythebills[.]com
- treasurebarn[.]net
- tyy[.]lol
- wnybestenergy[.]com
- wwr[.]lol
- wyy[.]lol
- xpp[.]lol
- xtt[.]lol
- xzz[.]lol
- youriphoneshop[.]com
- zgd[.]help
- zgh[.]help
- zgh[.]lol
- zgj[.]help
- zgk[.]help
- zgl[.]help
- zgp[.]help
- zgq[.]help
- zgr[.]help
- zgr[.]lol
- zgt[.]help
- zgy[.]help
- zgy[.]lol
- znm[.]lol
- zxz[.]lol

Sample Additional IP Addresses

- 100[.]27[.]115[.]166
- 104[.]19[.]154[.]92
- 104[.]21[.]112[.]1
- 104[.]21[.]16[.]1
- 104[.]21[.]27[.]249
- 104[.]21[.]28[.]80
- 104[.]21[.]29[.]34
- 104[.]21[.]3[.]48
- 104[.]21[.]32[.]1
- 104[.]21[.]33[.]139
- 104[.]21[.]37[.]168
- 104[.]21[.]4[.]122
- 104[.]21[.]45[.]223
- 104[.]21[.]48[.]1
- 104[.]21[.]48[.]176
- 104[.]21[.]54[.]135
- 104[.]21[.]57[.]107
- 104[.]21[.]60[.]150
- 104[.]21[.]60[.]166
- 104[.]21[.]61[.]61
- 104[.]21[.]64[.]1
- 104[.]21[.]66[.]137
- 104[.]21[.]7[.]191
- 104[.]21[.]75[.]68
- 104[.]21[.]77[.]218
- 104[.]21[.]8[.]248
- 104[.]21[.]80[.]1
- 104[.]21[.]80[.]114
- 104[.]21[.]84[.]127
- 104[.]21[.]90[.]117
- 104[.]21[.]91[.]178
- 104[.]21[.]96[.]1
- 104[.]21[.]96[.]50
- 104[.]248[.]235[.]211
- 104[.]26[.]10[.]149
- 104[.]26[.]11[.]149
- 108[.]167[.]157[.]184
- 127[.]0[.]0[.]1
- 13[.]216[.]94[.]178
- 141[.]193[.]213[.]10

- 141[.]193[.]213[.]11
- 141[.]193[.]213[.]20
- 141[.]193[.]213[.]21
- 141[.]255[.]166[.]90
- 147[.]79[.]91[.]87
- 15[.]197[.]240[.]20
- 157[.]230[.]52[.]100
- 162[.]0[.]217[.]151
- 162[.]0[.]217[.]215
- 162[.]0[.]217[.]87

Sample IP-Connected Domains

- 012727da-19b3-4f39-8bdc-ac2688d60abe[.]random[.]162-55-47-21[.]plesk[.]page
- 1090ce78-a573-43df-908b-4bc549764a3a[.]random[.]picsee[.]ltd
- 10x07[.]ink
- 157[.]230[.]52[.]100[.]nip[.]io
- 1st2nd[.]cv
- 23[.]109[.]121[.]53[.]sslip[.]io
- 46e10600-9222-4f22-be01-ef2eb1280971[.]random[.]aasiwins[.]com
- 5830c7b4-04d4-4217-8364-25863020f69f[.]random[.]khitmarket[.]com
- 71b002e7-9c3a-45c2-9708-01ddfacca838[.]random[.]picsee[.]ltd
- 73ed366d3137ec936bd60b1184467776[.]com
- 77x44[.]ink
- 80d335e5-cb9b-4010-ad5a-3d92f8525f01[.]random[.]mstsage[.]com
- 866dcae7-a392-4525-87c2-752ed84a67b9[.]random[.]aasiwins[.]com
- 90747612-54da-4563-be53-85b2901fab06[.]random[.]picsee[.]ltd
- 908df012d9bb72e6d26b41054588d758[.]com
- 97c019b3-fb11-43d5-8b42-fafd6b621deb[.]random[.]162-55-47-21[.]plesk[.]page
- a6dc0727-125b-4536-adf6-65c14bbeb90d[.]random[.]mstsage[.]com
- ababa[.]pros[.]is
- abaclieric[.]life
- abodyslaveys[.]world
- account[.]nextbank[.]pros[.]is
- achyliafinders[.]shop
- admin[.]strnetworkasia[.]pros[.]is
- aerosatemeers[.]rest
- affineayenst[.]shop
- aftmostlaen[.]shop
- agadir-today[.]pros[.]is
- agamicwryer[.]help
- agelessyoulook[.]com
- agoniedblotter[.]shop
- aiawongday[.]world
- aikonalitui[.]top
- airbusapport[.]world
- airnsgript[.]shop
- akravaguity[.]click
- alaihihause[.]click
- alationsulafat[.]cfd
- alditolcensure[.]cfd
- algoresdubby[.]click
- alkannaroit[.]world
- allansindle[.]shop
- allworkqasidas[.]cfd
- alopiascimeter[.]shop
- amangdullest[.]digital
- amboferbam[.]click
- ambuliamantuas[.]top
- amicoustubular[.]rest
- andrewrosilla[.]world
- angamisunland[.]shop
- anhingawabble[.]world

Sample String-Connected Domains

- 4x4x[.]app
- 4x4x[.]bio
- 4x4x[.]biz
- 4x4x[.]ca
- 4x4x[.]cc
- 4x4x[.]club
- 4x4x[.]cn
- 4x4x[.]com
- 4x4x[.]com[.]au
- 4x4x[.]ee
- 4x4x[.]fun
- 4x4x[.]hu
- 4x4x[.]icu
- 4x4x[.]in
- 4x4x[.]info
- 4x4x[.]life
- 4x4x[.]net
- 4x4x[.]nl
- 4x4x[.]online
- 4x4x[.]org
- 4x4x[.]org[.]ph
- 4x4x[.]ru
- 4x4x[.]shop
- 4x4x[.]space
- 4x4x[.]store
- 4x4x[.]tech
- 4x4x[.]tk
- 4x4x[.]top
- 4x4x[.]vip
- 4x4x[.]wang
- 4x4x[.]website
- 4x4x[.]xyz
- aasiwins[.]co
- aidetector[.]ac[.]cn
- aidetector[.]ai
- aidetector[.]app
- aidetector[.]be
- aidetector[.]best
- aidetector[.]biz
- aidetector[.]blog
- aidetector[.]ca
- aidetector[.]cc
- aidetector[.]ch
- aidetector[.]chat
- aidetector[.]click
- aidetector[.]cloud
- aidetector[.]club
- aidetector[.]cn
- aidetector[.]co
- aidetector[.]co[.]nz