Profiling a Popular DDoS Booter Service's Ecosystem

Table of Contents

Executive Report

Cybercriminals can launch distributed denial-of-service (DDoS) attacks with relative ease these days by using DDoS booter services, online services that automate the DDoS attack process.

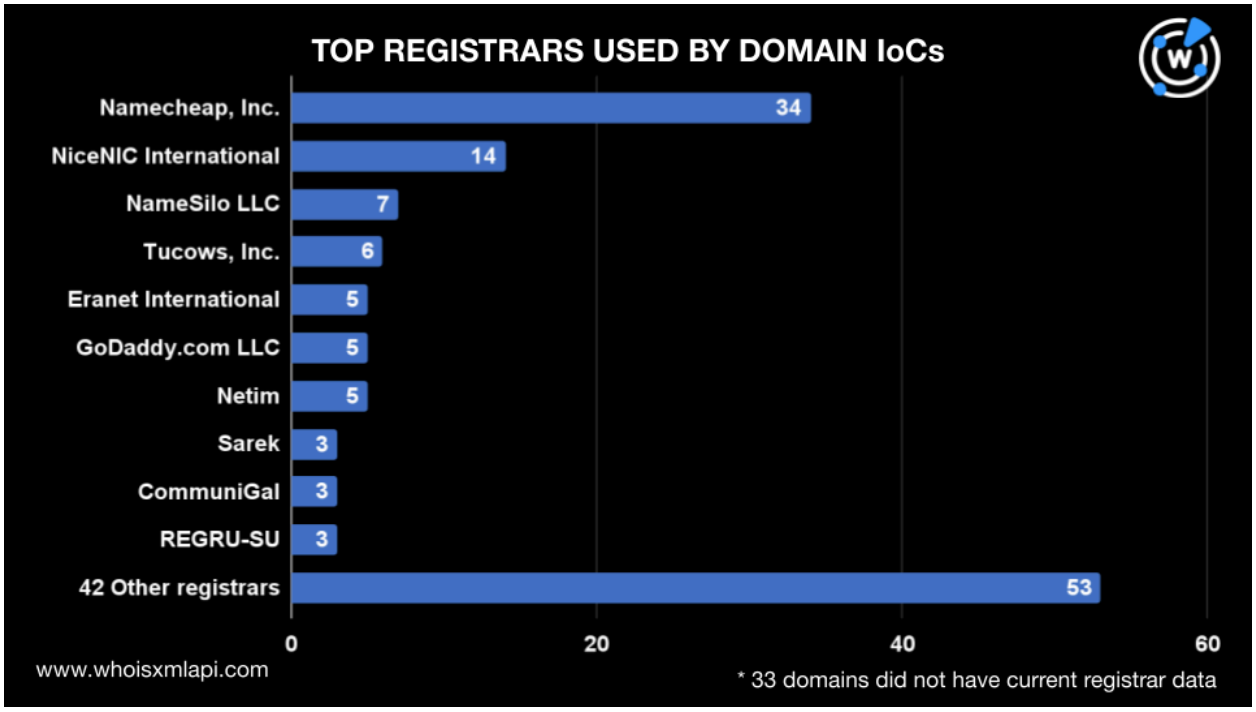
WhoisXML API threat researcher Dancho Danchev recently uncovered a list of the user information for a popular DDoS booter service, which our research team used to create a profile and expand to identify related artifacts. Jumping off a list of 171 domains, 464 IP addresses, and nine email addresses involved in the DDoS booter service operation, we found:

- 20 additional email addresses
- 43 email-connected domains
- 185 additional IP addresses
- 645 IP-connected domains
- 1,303 string-connected domains

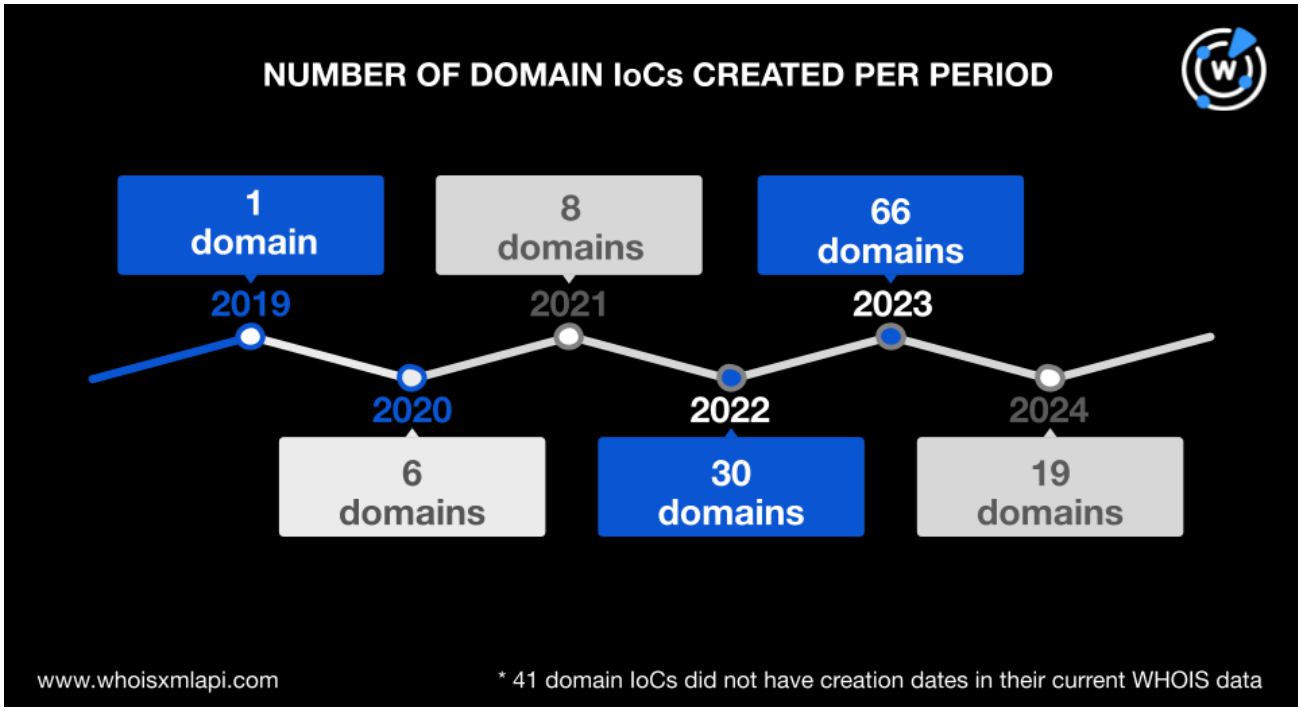
Analysis of the DDoS Booter Service Ecosystem

As a first step, we did a bulk WHOIS lookup for the 171 domains tagged as IoCs to obtain their WHOIS details. We found that:

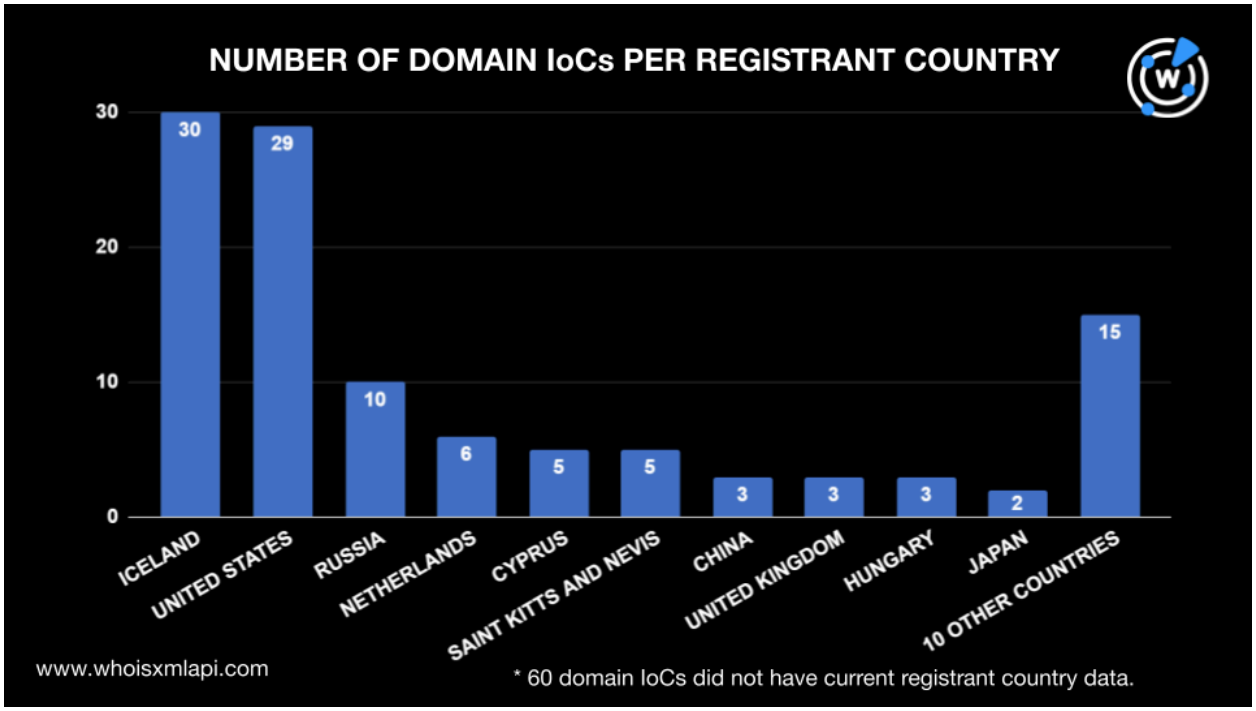
- Fifty-two registrars administered them. The most used registrars were Namecheap (34 domain IoCs); NiceNIC International (14 domain IoCs); NameSilo LLC (7 domain IoCs); Tucows, Inc. (6 domain IoCs); Eranet International, GoDaddy.com LLC, and Netim (5 domain IoCs each); and Sarek, CommuniGal, and REGRU-SU (3 domain IoCs each). The remaining domains, 53 to be exact, were distributed across 42 other registrars, while 33 domains did not have current registrar data.



- The oldest domain was registered in May 2019, while the newest ones were recently created, specifically in May 2024. Most of the domains, 66 to be exact, were created in 2023, six in 2020, eight in 2021, 30 in 2022, and 19 in 2024. Forty-one domain IoCs didn't have creation dates in their current WHOIS records.



- Their registrations were spread across 20 countries. The top 10 registrant countries are shown in the graph below, led by Iceland with 30 domains and the U.S. with 29. Ten domains were registered in Russia; six in the Netherlands; five each in Cyprus and Saint Kitts and Nevis; three each in China, the U.K., and Hungary; and two in Japan. Fifteen domain IoCs were registered across 10 other countries, while 60 did not have current registrant country data.



Some of the domains have already been seized by the Federal Bureau of Investigation (FBI), as revealed by Screenshot API.

stresserusio

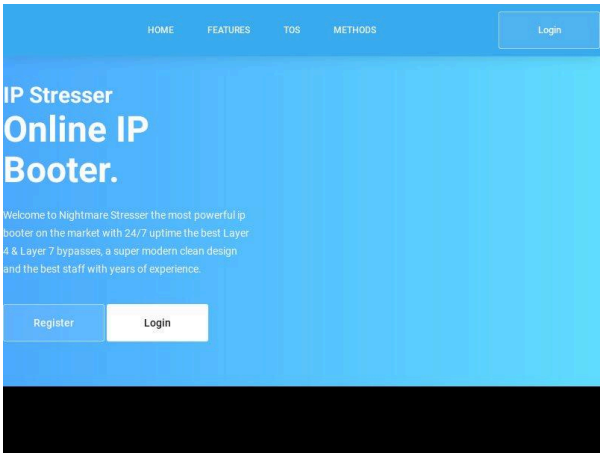
mythicalstressnet

silentto

stresserbestio

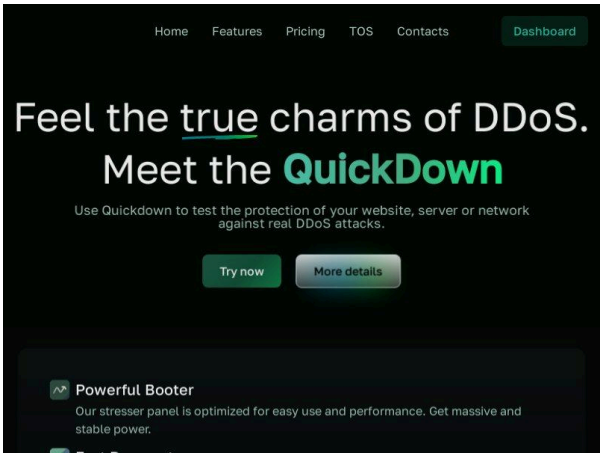
stressertech

Still, some domains continued to host content offering DDoS-related tools. Some of them are shown below.

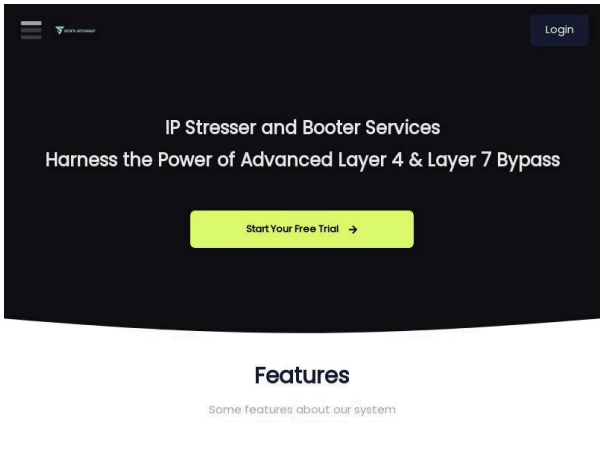


Screenshot of topstresser[.]top

Screenshot of powerstresser[.]pro



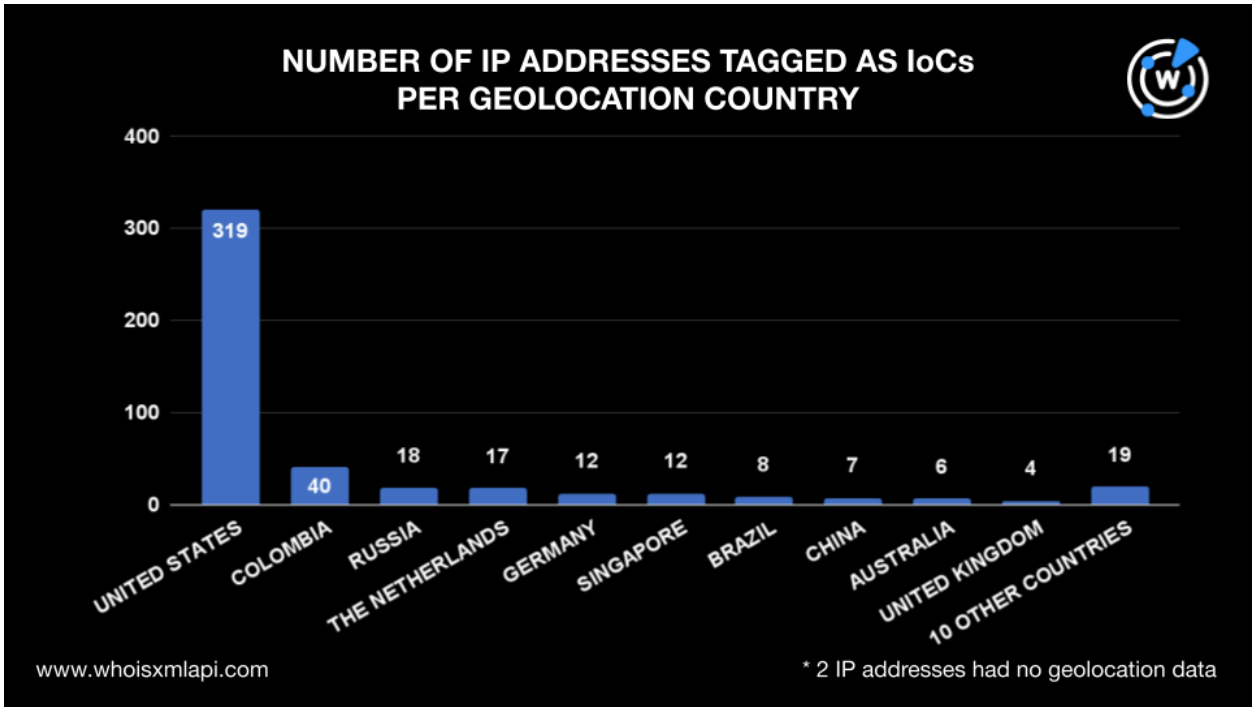
Screenshot of quickdown[.]pro



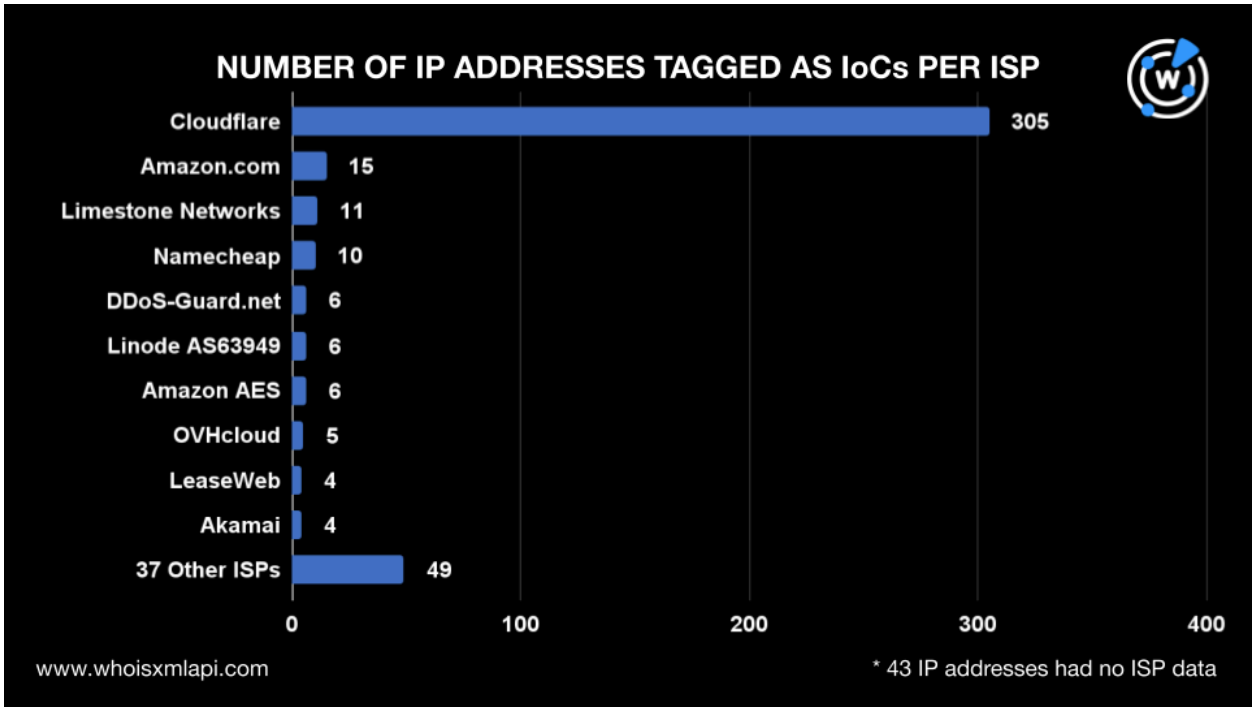
Screenshot of starkstresser[.]net

Next, we subjected the 464 IP addresses to a [bulk IP geolocation lookup](#) and found that:

- They were geolocated across 20 countries, with the U.S. accounting for the highest number of IP resolutions, 319 to be exact. The rest of the top 10 geolocations of the IP addresses tagged as IoCs included Colombia with 40 IP addresses, Russia with 18, the Netherlands with 17, Germany and Singapore with 12 each, Brazil with eight, China with seven, Australia with six, and the U.K. with four. Nineteen IP addresses were geolocated across 10 other countries, while two IP addresses did not have geolocation data.



- The IP addresses were administered by 47 ISPs, with Cloudflare managing 305; Amazon with 15; Limestone Networks with 11; Namecheap with 10; DDoS-Guard.net, Linode AS63949, and Amazon AES with six each; OVHcloud with five; and LeaseWeb and Akamai with four each. 49 IP addresses were administered by other ISPs, while 43 did not have ISP information.



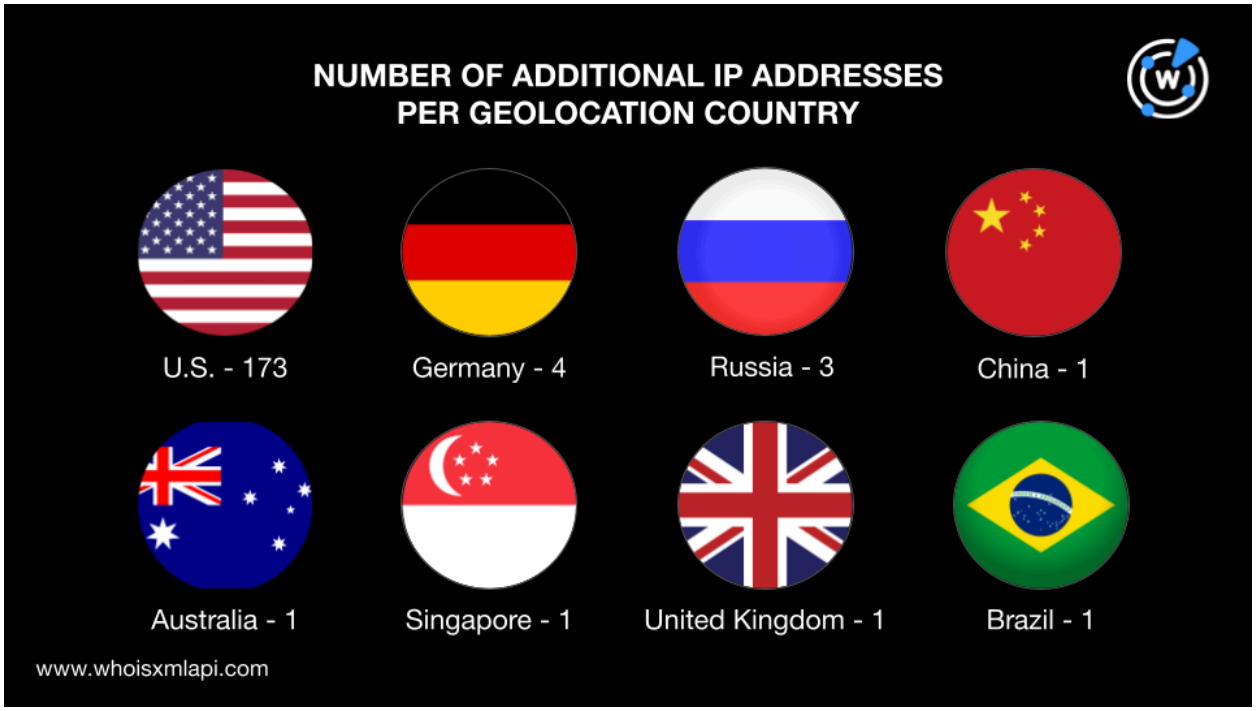
Tracing the DDoS Booter Ecosystem in the DNS

After examining the IoCs, we searched for potential threat artifacts and web properties associated with the DDoS booter.

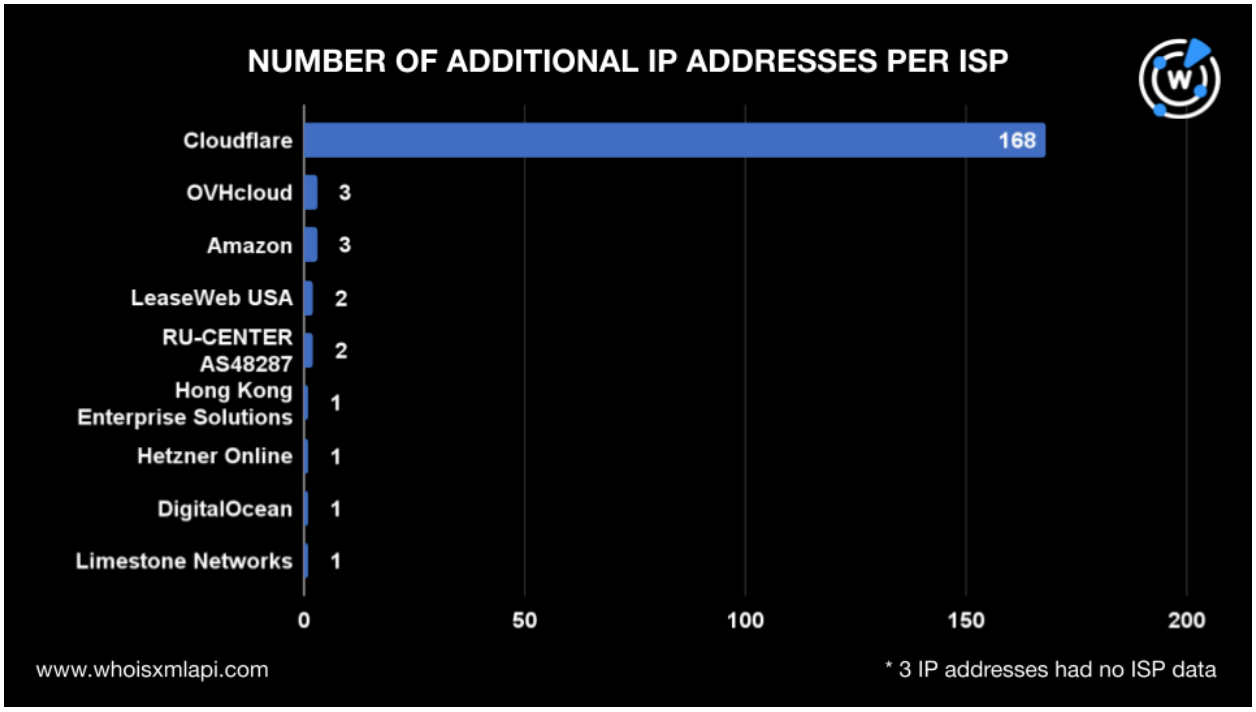
WHOIS History API searches for the domain IoCs led our research team to discover 175 email addresses in their historical WHOIS records, 20 of which were public. We then ran these public email addresses and the nine email addresses tagged as IoCs on Reverse WHOIS API, which revealed that they appeared in the current WHOIS records of more than 15,000 domains. After filtering out the IoCs and domains that may belong to domainers (i.e., email addresses used to register more than 50 domains), we were left with 43 email-connected domains.

We then obtained the IP resolutions of the 171 domains tagged as IoCs by performing DNS lookups, which led to the discovery of 185 additional IP addresses. Running IP geolocation lookups on the IP addresses revealed that:

- They originated from eight countries. A total of 173 IP addresses were geolocated in the U.S.; four in Germany; three in Russia; and one each in China, Australia, Singapore, the U.K., and Brazil.



- Nine ISPs administered them. Cloudflare, Inc. managed 168 IP addresses; OVHcloud and Amazon each managed three; LeaseWeb USA and RU-CENTER AS48287 each managed two; and Hong Kong Enterprise Solutions, Hetzner Online, DigitalOcean, and Limestone Networks each managed one.



We also ran the 185 additional IP addresses on Threat Intelligence API, which revealed that they were all associated with various threats. The table below shows a few examples.

IP ADDRESSES	ASSOCIATED THREAT TYPES
54[.]157[.]24[.]8	Command and control (C&C) Generic Phishing Malware
104[.]21[.]11[.]249	Phishing Malware
172[.]67[.]150[.]206	Phishing Malware
2606:4700:3032::ac43:96ce	Phishing Malware
2606:4700:3032::ac43:911c	Phishing Malware

Next, we subjected the 649 IP addresses in total (i.e., 464 IP addresses tagged as IoCs and 185 additional IP addresses) to reverse IP lookups, which showed that 74 were potentially

dedicated. They led to 645 IP-connected domains after removing duplicates, the IoCs, and the email-connected domains.

Finally, we analyzed the IoCs' string usage and looked for similar-looking domains registered from 1 January 2023 to 19 May 2024. We used text strings that appeared in the 171 domains tagged as IoCs as search strings on Domains & Subdomains Discovery. This led us to 1,303 string-connected domains after removing duplicates, IoCs, and email and IP-connected domains. These domains started with the following text strings:

- **panel.**
- **pluto.**
- **joker**
- **ddos**
- **silent**
- **stresser.**
- **inverse.**
- **stresse.**
- **ddg**
- **alya.**
- **1981.**
- **elitesecurity.**
- **undisclosed**
- **hatter**
- **stressed.**
- **booter**
- **quickdown**
- **stresslab**
- **io9.**
- **ipstresser**
- **packetsto**
- **stressers**
- **tokenview**
- **quez**
- **lkxstress**
- **informants**
- **vacstresser**
- **cfxsecurity**
- **digitalstress**
- **heydos**
- **mythicalstress**
- **cyberstress**
- **webstress.**
- **cryptostresser**
- **downed.**
- **neostresser**
- **stressthem**
- **tresser**
- **ddoser**
- **freestresser**
- **silentstress**
- **mao-stress**
- **redstresser**
- **999stresser**
- **Freeddos**
- **liquidsec**
- **orbitalstress.**
- **sunstresser**
- **xstress.**

Threat Intelligence API revealed that dozens of the string-connected web resources were associated with malware distribution. Examples include the domains that used the same strings as those seized by the FBI, such as:

- mythicalstress[.]su
- mythicalstress[.]com

- stresser[.]org
- stresser[.]top
- stresserus[.]su

—

Our investigation of the DDoS booter service ecosystem began with 171 domains, 464 IP addresses, and nine email addresses. An in-depth analysis of their WHOIS records, IP geolocation, and string usage led us to 2,196 connected artifacts, including 20 additional email addresses, 43 email-connected domains, 185 additional IP addresses, 645 IP-connected domains, and 1,303 string-connected domains.

If you wish to perform a similar investigation or 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 Email-Connected Domains

- flippedscript[.]com
- santabarbaraacupuncturist[.]com
- headsetadapters[.]net
- cloudprinting[.]info
- santacruzhouserentals[.]com
- currencytradingmagazine[.]com
- carpentershoes[.]com
- toyquadcopters[.]com
- suppressed[.]work
- moreno-valley[.]info
- overland-park[.]info
- soquel[.]us
- jiii[.]info
- opmh[.]info
- tvkh[.]info
- sbed[.]info
- teslacoil[.]info
- homeopathics[.]info
- weathermodification[.]xyz
- toydrones[.]info

Sample Additional IP Addresses

- 54[.]157[.]24[.]8
- 104[.]21[.]11[.]249
- 172[.]67[.]150[.]206
- 2606:4700:3032::ac43:96ce
- 2606:4700:3034::6815:bf9
- 172[.]67[.]145[.]28

- 2606:4700:3032::6815:3f5d
- 2606:4700:3032::ac43:911c
- 172[.]67[.]154[.]136
- 104[.]21[.]80[.]227
- 2606:4700:3034::6815:50e3
- 2606:4700:3033::ac43:9a88
- 104[.]21[.]29[.]168
- 2606:4700:3033::ac43:9588
- 2606:4700:3035::6815:1da8
- 104[.]21[.]70[.]181
- 172[.]67[.]138[.]47
- 2606:4700:3031::ac43:8a2f
- 2606:4700:3036::6815:46b5
- 104[.]21[.]57[.]154
- 172[.]67[.]146[.]223
- 2606:4700:3033::ac43:92df
- 2606:4700:3033::6815:399a
- 2606:4700:3033::6815:3334
- 2606:4700:3032::ac43:dd6b
- 172[.]67[.]154[.]10
- 104[.]21[.]4[.]60
- 2606:4700:3035::6815:43c
- 2606:4700:3033::ac43:9a0a
- 172[.]67[.]73[.]27
- 2606:4700:20::ac43:491b
- 2606:4700:20::681a:bc6
- 2606:4700:20::681a:ac6
- 104[.]26[.]0[.]29
- 2606:4700:20::681a:1d
- 2606:4700:20::ac43:46d9
- 2606:4700:20::681a:11d
- 172[.]67[.]196[.]160
- 104[.]21[.]58[.]6
- 2606:4700:3032::6815:3a06
- 2606:4700:3036::ac43:c4a0
- 172[.]67[.]207[.]226
- 104[.]21[.]15[.]220
- 2606:4700:3031::ac43:cfe2
- 2606:4700:3037::6815:fdc
- 2606:4700:3035::ac43:b49f
- 2606:4700:3032::6815:3384
- 172[.]67[.]171[.]142
- 2606:4700:3030::6815:4fda
- 2606:4700:3033::ac43:ab8e

Sample IP-Connected Domains

- agenda-cci79[.]com
- a4j[.]ir
- altoadigebus[.]eu
- bizadulte[.]com
- 4kott[.]life
- 2400[.]ru
- alloksoft[.]com
- best-wallet[.]net
- aevtekg[.]cn
- bitcoin-24[.]pro
- bastonhouseschool[.]org[.]uk
- asiye[.]net
- afestmc[.]ru
- 8v[.]to
- amanecerdeplata[.]es
- arbitrarylogic[.]ai
- bgff163[.]top
- angeleye[.]be
- basilbriance[.]com
- cuisinemorel[.]fr
- dropbollwormscotton[.]com
- ecopowershop[.]at
- ww16[.]bustybri[.]biz
- aim-master[.]pp[.]ua
- bio-art[.]com[.]tr
- astarocentral[.]com
- cyncitytalk[.]com
- hotelcaboblanco[.]com
- imperialmelon[.]cloud
- applymeta[.]com

- aiada[.]net
- clearbridgeadvisors[.]com[.]au
- 30s[.]pl
- mtlenl[.]club
- esocialmed[.]com
- boscocanorowest[.]com
- lansdownevillage[.]ca
- thmzaodo[.]xyz
- maxstresser[.]com
- g3n[.]one
- pulse[.]plus
- emmapage[.]com
- caritas[.]org[.]pl
- canadianvisaexpert[.]com
- carvoz[.]com
- hoheiser[.]com
- doubleuvideo[.]com
- entyre[.]care
- pprotv[.]com
- yckzz[.]com
- chlorolyz[.]com
- fatemeh3dart[.]eu[.]org
- finai[.]com
- ubits[.]club
- terzimario-sa[.]com
- nakheelteam[.]cc
- lewisbrown[.]com
- dealerjobapplication[.]com
- hyperodvoz[.]cz
- sundl[.]shop
- jamuna[.]tv
- agenda-cci79[.]eu
- airwise[.]aero
- antoniolupidesign[.]com[.]au
- bizadulte[.]net
- 4kott[.]site
- ameal[.]sa
- ab[.]ww[.]re[.]guai[.]duckdns[.]org
- art-providers[.]com
- chochox[.]com
- anchorfe[.]hk
- cs-sparta[.]ru
- baywater[.]uk
- babystoresnearme[.]com
- agpsdo[.]edu[.]ru
- app-eigenlayer[.]co
- andresain123[.]xyz
- ashm[.]ca
- buff163[.]top
- bestemischung[.]com
- connerypropertiesl[.]com
- cwacheer[.]com
- graet[.]app
- gadang[.]shop
- fitgirl-repacks[.]ir
- ww16[.]etrogames[.]biz
- e-cui[.]ir
- kermazjo[.]com
- general[.]com[.]au
- collinformations[.]com
- j9customdesigns[.]com
- hoteldanzadelsol[.]com
- mecemecenew[.]com
- moodmeta[.]com
- aiadaconference[.]com
- cooklane[.]nl
- dvnzrt[.]hu
- nlebovic[.]com
- faltexgroup[.]pl
- nationalsecuritylifeandannuity[.]com

Sample String-Connected Domains

- 1981[.]ac[.]jp
- 1981[.]cf
- 1981[.]ru
- 1981[.]zip

- alya[.]com
- alya[.]hu
- alya[.]ma
- anonstress[.]su
- ddg[.]co[.]in
- ddg[.]fr
- 1981[.]au
- 1981[.]bid
- 1981[.]bz
- 1981[.]cn
- 1981[.]co
- 1981[.]co[.]uk
- 1981[.]com
- 1981[.]com[.]au
- 1981[.]country
- 1981[.]credit
- 1981[.]cz
- 1981[.]de
- 1981[.]df[.]gov[.]br
- 1981[.]es
- 1981[.]fi
- 1981[.]fr
- 1981[.]info
- 1981[.]lt
- 1981[.]net
- 1981[.]net[.]ws
- 1981[.]nl
- 1981[.]org
- 1981[.]pics
- 1981[.]pro
- 1981[.]pt
- 1981[.]pw
- 1981[.]se
- 1981[.]today
- 1981[.]us
- 1981[.]xn--j1amh
- 1981[.]xyz
- 999stresser[.]eu
- 999stresser[.]us
- 999stresser[.]xyz
- alya[.]ai
- alya[.]aquila[.]it
- alya[.]au
- alya[.]bid
- alya[.]cc
- alya[.]ch
- alya[.]cl
- alya[.]cn
- alya[.]co[.]uk
- alya[.]com[.]au
- alya[.]de
- alya[.]dk
- alya[.]edu[.]pk
- alya[.]es
- alya[.]fr
- alya[.]gr
- alya[.]info
- alya[.]jp
- alya[.]life
- alya[.]mx
- alya[.]my
- alya[.]my[.]id
- alya[.]net
- alya[.]org
- alya[.]pt
- alya[.]ro
- alya[.]ru
- alya[.]sl
- alya[.]top
- alya[.]us
- alya[.]ventures
- alya[.]web[.]tr
- alya[.]wine
- alya[.]xyz
- anonstress[.]org
- atom-stresser[.]com
- atom-stresser[.]org
- blaststress[.]lol
- blaze-api[.]site
- booter[.]ba

- booter[.]ch
- booter[.]cn
- booter[.]co[.]uk
- booter[.]com
- booter[.]com[.]au
- booter[.]de
- booter[.]df[.]gov[.]br
- booter[.]fr
- booter[.]gg
- booter[.]in
- booter[.]net
- booter[.]network
- booter[.]ninja
- booter[.]nl
- booter[.]org
- booter[.]ru