Silent Night, Deadly Sites: How Christmas Cyber Threats Lurk in the DNS

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

For many across the globe, Christmas represents a joyous time of celebration and giving. But it can also be a time for worry, especially for those unfortunate enough to get scammed while doing their holiday shopping.

This year, we scoured the DNS for domains and subdomains that contained the text string **christmas** to identify potentially harmful properties and other connected artifacts.

Jumping off a list of 22,923 **christmas** domains obtained on 26 November 2024 from First Watch Malicious Domains Data Feed, our in-depth DNS investigation found:

- 1,331 email-connected domains
- 3,229 IP addresses, 2,529 of which turned out to be malicious
- 21,035 IP-connected domains, 96 of which turned out to be malicious
- 1,436 string-connected subdomains

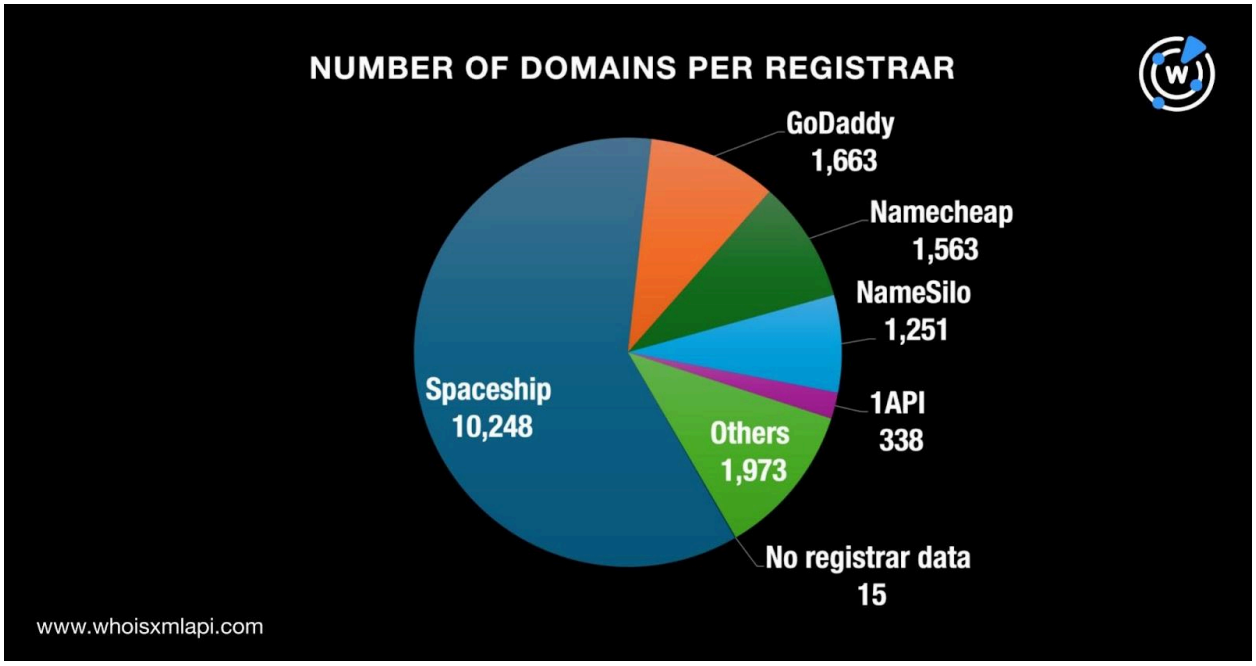
A Look at the *christmas* Domains

As mentioned earlier, we began our foray into the DNS in search of Christmas-themed threats by obtaining 22,923 domains containing the string **christmas** that are either already or likely to turn malicious in the future.

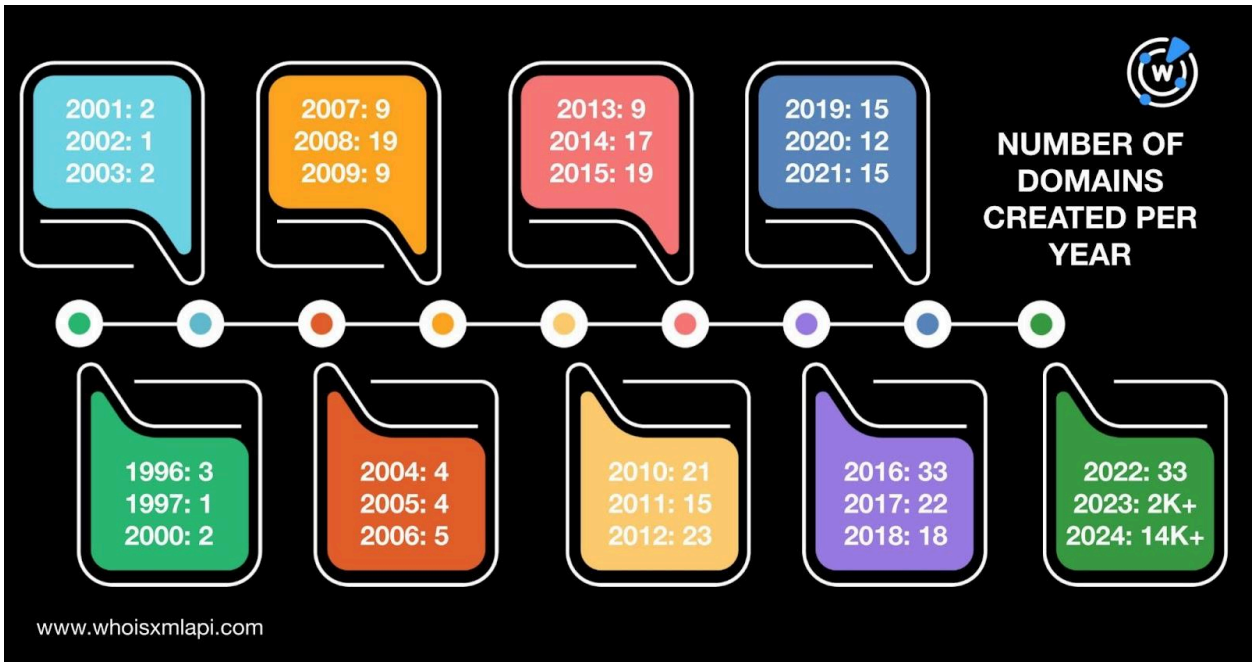
We queried the 22,923 **christmas** domains on Bulk WHOIS Lookup and found that only 17,051 had current WHOIS records. Take a look at our specific findings below.

- They were spread among 172 different registrars led by Spaceship, which accounted for 10,248 domains. GoDaddy with 1,663 domains; Namecheap with 1,563; NameSilo with 1,251; and 1API with 338 completed the top 5. A total of 1,973 domains were

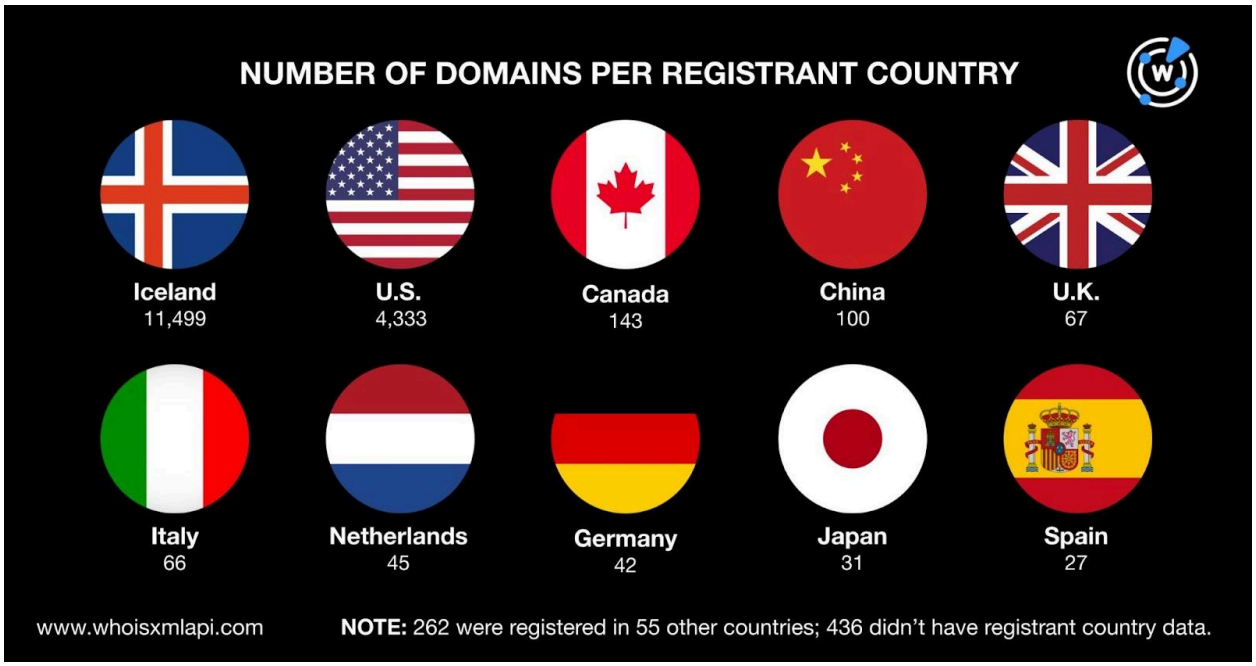
distributed among 167 other registrars, while the remaining 15 didn't have current registrar data.



- They were created between 1996 and 2024. Around 84% of the domains, however, were newly created, just this year.



- They were registered in 65 different countries led by Iceland, which accounted for 11,499 domains. The other top registrant countries were the U.S. with 4,333 domains; Canada with 143; China with 100; the U.K. with 67; Italy with 66; the Netherlands with 45; Germany with 42; Japan with 31; and Spain with 27. A total of 262 domains were registered in 55 other countries, while 436 didn't have current registrant country data.



We then queried the 22,923 **christmas** domains on DNS Chronicle API and found that 17,188 had historical IP resolutions ranging from 1 to 20 per domain. In total, the 17,188 domains had 168,578 recorded events from 4 October 2019 to 8 November 2024. Take a look at five examples below.

DOMAIN	START DATE	LAST DATE	NUMBER OF IP RESOLUTIONS
12daysofchristmas[.]info	29 February 2020	18 November 2024	105
artificialchristmastreesale[.]co[.]uk	11 July 2024	11 November 2024	5
nashvillechristmasbus[.]com	20 February 2020	12 October 2024	71
yourfunny[.]christmas	5 May 2024	13 October 2024	10
zen[.]christmas	25 December 2023	19 November 2024	12

Hunt for *christmas* Domain Connections

After analyzing the sample of 22,923 **christmas** domains, we took a DNS deep dive for potentially connected artifacts.

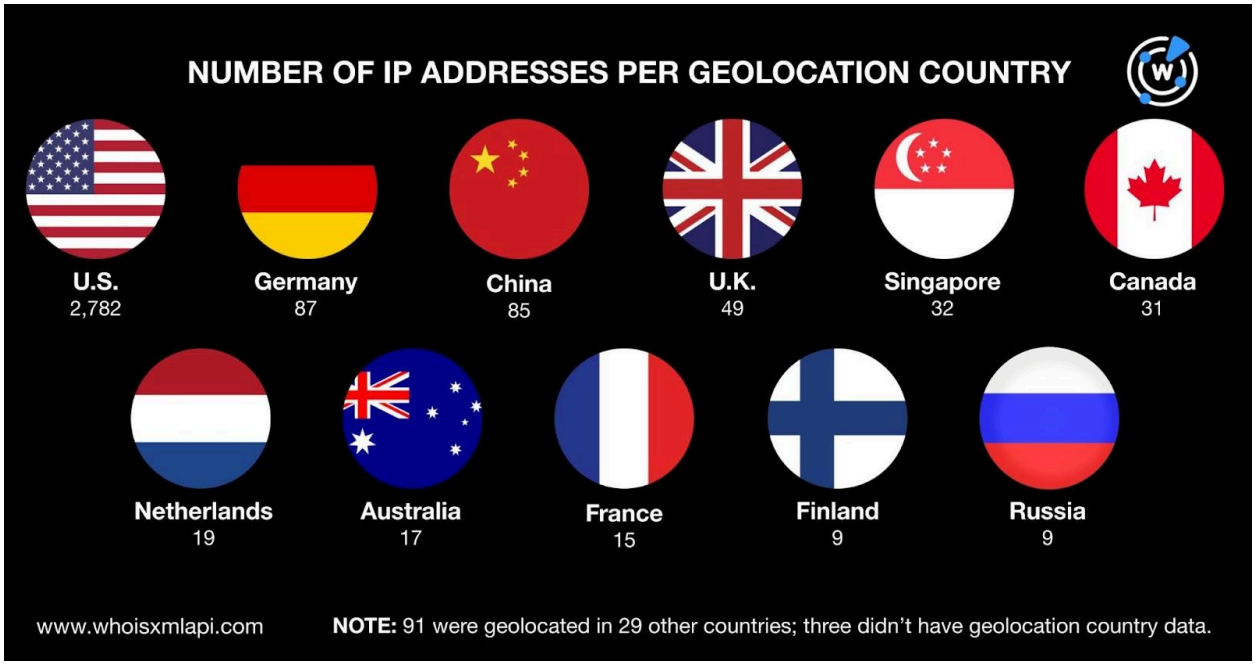
Our bulk WHOIS lookup earlier provided 629 email addresses after duplicates were filtered out, 73 of which turned out to be public addresses. A query for the public email addresses on Reverse WHOIS API yielded 1,331 email-connected domains after duplicates and the original domains from First Watch Malicious Domains Data Feed were removed.

Next, we queried the 22,923 **christmas** domains on DNS Lookup API and found that they actively resolved to 3,229 unique IP addresses. A Threat Intelligence API query for the 3,229 IP addresses revealed that 2,529 of them have already been weaponized. Take a look at five examples below.

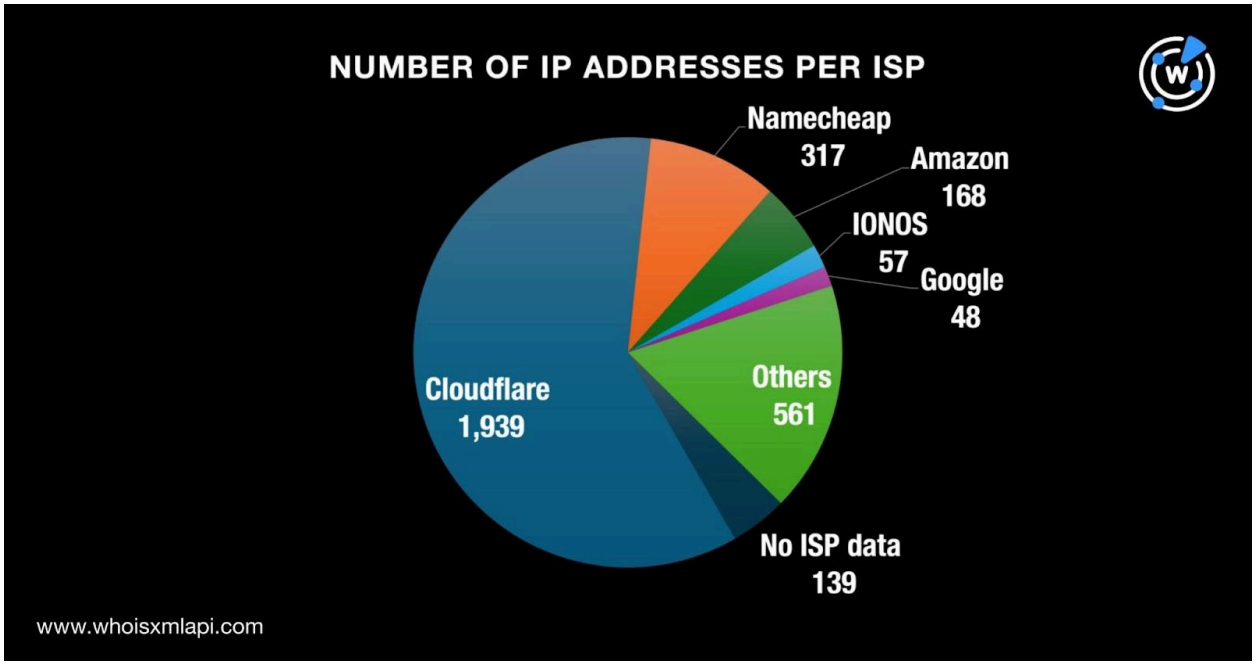
MALICIOUS IP ADDRESS	ASSOCIATED THREATS
100[.]24[.]208[.]97	Attack Generic Malware Phishing Suspicious
207[.]148[.]248[.]143	Attack Command and control (C&C) Generic Malware Phishing Suspicious
3[.]230[.]199[.]117	Generic Malware
44[.]227[.]65[.]245	Attack C&C Generic Malware Phishing Suspicious
5[.]22[.]145[.]155	Generic Malware

We then sought to find out more about the 3,229 IP addresses by querying them on Bulk IP Geolocation Lookup, which revealed that:

- They were geolocated in 40 different countries led by the U.S., which accounted for 2,782 IP addresses. The other top geolocation countries were Germany with 87 IP addresses, China with 85, the U.K. with 49, Singapore with 32, Canada with 31, the Netherlands with 19, Australia with 17, France with 15, and Finland and Russia with nine each. A total of 91 IP addresses were distributed among 29 other countries, while three didn't have geolocation country data.



- They were distributed among 164 different ISPs led by Cloudflare, which accounted for 1,939 IP addresses. The rest of the top ISPs were Namecheap with 317 IP addresses, Amazon with 168, IONOS with 57, and Google with 48. A total of 561 IP addresses were spread across 159 other ISPs, while 139 didn't have ISP data.



After that, we queried the 3,229 IP addresses on Reverse IP API and found that 322 of them could be dedicated hosts. Altogether, they hosted 21,035 IP-connected domains after duplicates, the original domains, and the email-connected domains were filtered out.

A Threat Intelligence API query for the 21,035 IP-connected domains revealed that 96 have already been tagged as malicious. Take a look at five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREATS
answersite[.]com	Generic Malware
bradleys[.]fun	Malware
campsurfmorocco[.]com	Generic Phishing
dragonz[.]shop	Malware
enhances[.]digital	Malware

As our final step, we used Domains & Subdomains Discovery to look for subdomains containing the text string **christmas**. We limited our searches to subdomains only that were added since 1 November 2024 and found 1,436 string-connected subdomains. The strings

photo, **tree**, **game**, **wallpaper**, and **gift** appeared concurrently with **christmas** in many of the subdomains, 436 to be exact.

—

Our in-depth investigation of potential Christmas-themed threat vectors yielded 27,031 connected artifacts comprising 1,331 email-connected domains, 3,229 IP addresses, 21,035 IP-connected domains, and 1,436 **christmas** subdomains. As of this writing, 2,625 of the connected artifacts have already been weaponized and used in various malicious campaigns.

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 *christmas* Domains from First Watch Malicious Domains Data Feed

- 5ph2dd6qd03e[.]christmas
- j40ry893es[.]christmas
- o52tk965tq[.]christmas
- pkyfmhjn3q1g[.]christmas
- ajajchristmaslights[.]com
- 1t75y6ap383g[.]christmas
- z2nn120dc[.]christmas
- a14ff615gr[.]christmas
- e18cv54rc[.]christmas
- j91nh334jg[.]christmas
- kcid05l1xfzk[.]christmas
- q9iq257ig[.]christmas
- r68df786rl[.]christmas
- christmasatccsg[.]com
- 11b5imyxhz[.]christmas
- 2kwwga9mxu[.]christmas
- 2vi4kztb7mry[.]christmas
- 377a4a0[.]christmas
- zc4eeepgta56[.]christmas
- c83jk8zk[.]christmas
- s80ki179sk[.]christmas
- vc7f4i7nr5a[.]christmas
- 1ozwyblyeek[.]christmas
- 3ad0iv89v5e4[.]christmas
- l90sq372tw[.]christmas
- questignitenotification[.]christmas
- xdz5v8cp2lh[.]christmas
- im-looking-for-christmas[.]com
- christmaslightintallersofkentuckiana[.]com
- weinstallingchristmaslights[.]com
- i7qy16qd1fm[.]christmas

- o6s2252yms[.]christmas
- o751j841brl[.]christmas
- v92cm261ro[.]christmas
- vlw84pk5y[.]christmas
- y95xy655mp[.]christmas
- 13rxampi2mva[.]christmas
- 4pyp6i2owcwl[.]christmas
- f70nu877lg[.]christmas
- plhm4ggipw[.]christmas
- yfo5uytpfq[.]christmas
- 830tp63z4ada[.]christmas
- ent617cdeg75[.]christmas
- nsvgr9w2gr47g[.]christmas
- t16mh159ty[.]christmas
- c3a222550456v5cd8[.]christmas
- nk6fskzku[.]christmas
- s6m5vnvtgx[.]christmas
- v1xk724gp[.]christmas

Sample Email-Connected Domains

- 101bianchi[.]com
- 10xbankrate[.]com
- 2024womensworlds5050[.]ca
- 2daysport[.]com
- 310hospitality[.]com
- 4ginternetservice[.]com
- 5050atletico[.]ca
- 5050atleticoottawa[.]ca
- 5050iwk[.]ca
- 5050osegfoundation[.]ca
- 5050ottawa67s[.]ca
- 5050ottawaredblacks[.]ca
- 5050panda[.]ca
- 5050theblackjacks[.]ca
- 5050ymca[.]ca
- 5633814[.]com
- 5dayhyang[.]com
- abetterlansdowne[.]ca
- abitfile[.]com
- abstractxm[.]com
- access5050[.]ca
- actionvest[.]us
- activelinksdirectory[.]com
- ad-archts[.]com
- ad-in[.]net
- ad-nl[.]com
- adirlinc[.]com
- adklandandcamps[.]com
- admaterjewels[.]com
- adoralazaro[.]com
- adultolescents[.]com
- advice16281[.]com
- aegis1000newyear[.]com
- afcjeju[.]com
- affinfinity[.]com
- afreespot[.]com
- afriendinjesus[.]com
- agopunturamilano[.]com
- agosallstar[.]com
- ahotibook[.]com
- aigis1000-newyear[.]com
- aigis1000-r[.]jp
- aigis1000contest9th[.]jp
- albamdollhouse[.]com
- alexndrahospital5050[.]ca
- alibenintersanls[.]ng
- allcreationwaits[.]com
- allcreationwaitsbook[.]com
- allengrey[.]com
- allenzeco[.]com

Sample IP Addresses

- 0[.]0[.]0[.]0
- 1[.]171[.]169[.]182

- 100[.]24[.]208[.]97
- 101[.]44[.]64[.]180
- 102[.]218[.]215[.]124
- 102[.]218[.]215[.]137
- 103[.]169[.]142[.]0
- 103[.]171[.]180[.]169
- 103[.]189[.]234[.]120
- 103[.]207[.]68[.]20
- 103[.]21[.]221[.]33
- 103[.]224[.]182[.]242
- 103[.]224[.]182[.]246
- 103[.]224[.]182[.]250
- 103[.]224[.]182[.]253
- 103[.]224[.]212[.]210
- 103[.]224[.]212[.]211
- 103[.]224[.]212[.]212
- 103[.]224[.]212[.]215
- 103[.]224[.]212[.]216
- 103[.]224[.]212[.]217
- 103[.]42[.]108[.]46
- 103[.]48[.]248[.]164
- 103[.]56[.]114[.]236
- 103[.]56[.]115[.]140
- 103[.]66[.]219[.]147
- 103[.]66[.]57[.]90
- 103[.]97[.]179[.]222
- 104[.]130[.]255[.]68
- 104[.]16[.]100[.]66
- 104[.]16[.]36[.]105
- 104[.]16[.]42[.]105
- 104[.]160[.]190[.]62
- 104[.]160[.]23[.]22
- 104[.]168[.]92[.]174
- 104[.]17[.]157[.]1
- 104[.]17[.]158[.]1
- 104[.]17[.]232[.]29
- 104[.]18[.]11[.]62
- 104[.]18[.]187[.]223
- 104[.]18[.]188[.]223
- 104[.]18[.]73[.]116
- 104[.]18[.]76[.]75
- 104[.]19[.]173[.]68
- 104[.]19[.]174[.]68
- 104[.]19[.]222[.]20
- 104[.]19[.]240[.]93
- 104[.]19[.]241[.]93
- 104[.]21[.]0[.]113
- 104[.]21[.]0[.]122

Sample IP-Connected Domains

- 0check[.]shop
- 1sterr[.]uno
- 1sun[.]buzz
- 2screw[.]shop
- 3ple[.]shop
- 4cast[.]online
- 4more[.]in[.]net
- 5cent[.]shop
- 5lbs[.]fun
- 6bits[.]store
- 6dix[.]shop
- 6sst3f9ti[.]top
- 8great[.]space
- 8mate[.]online
- 9fine[.]shop
- 9line[.]shop
- 9oa2krbd6[.]top
- 9prime[.]store
- aansr4vor[.]top
- adserver[.]smgfiles[.]com
- answersite[.]com
- anthonykvalley[.]com
- artico-x[.]com
- asuszenfone11[.]com
- atucom[.]net
- bradleys[.]fun

- broadtag[.]shop
- campsurfmorocco[.]com
- campustigo[.]com[.]co
- cdn[.]ins[.]hichat[.]buzz
- cosmiccandyclub[.]com
- dbwall[.]com
- drainclogsolutions[.]ca
- enjgom82[.]college
- extrut[.]com[.]au
- fedoroff[.]org
- firstbornreview[.]com
- formulairefibrecanalbox[.]com
- gigglezfoundation[.]org
- globalwork[.]us
- groundnewsletter[.]com
- hardstyle-industry[.]com
- hyfb6z5swt[.]best
- hypewatching[.]com
- intergroup-communications[.]co[.]uk
- inthevalley[.]net
- istezzo1[.]college
- jetpack[.]ad
- jetsuiteexperiences[.]com
- kanawa-logistics[.]com

Sample String-Connected Subdomains

- 12-stacks-of-christmas-2[.]gamesfree[.]me
- 12-stacks-of-christmas-3[.]gamesfree[.]me
- 12daysofchristmas[.]bss[.]design
- 2019christmassocia[.]uwiaafl[.]org
- 2024budweiserchristmas[.]pages[.]dev
- 2024christmasgifts[.]pages[.]dev
- 2024christmasornaments[.]pages[.]dev
- 2024christmaspalette[.]pages[.]dev
- 2024christmasphotomug[.]pages[.]dev
- 2024christmaspresents[.]pages[.]dev
- 2024christmastrees[.]pages[.]dev
- 2024christmasvacationpackages[.]pages[.]dev
- 2024christmaswreathideas[.]pages[.]dev
- 2024gfchristmasgiftideas[.]pages[.]dev
- 2024homechristmasgifts[.]pages[.]dev
- 2024midnightchristmas[.]pages[.]dev
- 2024preceptcolumbuschristmasluncheon[.]eventbritr[.]com
- 2024texaschristmasornament[.]pages[.]dev
- 2024xmchristmaschannels[.]pages[.]dev
- 20diyclaypotchristmasdecorationsthatad[.]yakidee[.]org
- 365-days-of-christmas[.]adriennewoodsbooks[.]com
- 365tochristmas[.]weebly[.]it
- 3d-christmas-fireplace-hd-free[.]ar[.]uptodown[.]com
- 3d-christmas-fireplace-hd-free[.]cn[.]uptodown[.]com
- 3d-christmas-fireplace-hd-free[.]in[.]uptodown[.]com
- 3d-christmas-fireplace-hd-free[.]uptodown[.]com
- 3d-christmas-tree-ii[.]ru[.]uptodown[.]com
- 3d-santa-christmas-live-wallpaper[.]ru[.]uptodown[.]com

- 4k-christmas-wallpapers[.]kr[.]uptodown[.]com
- 651christmaslights[.]trghub[.]com
- a-i-type-christmas-theme[.]en[.]uptodown[.]com
- a[.]christmas[.]story[.]house
- abcchristmasschedule2024[.]pages[.]dev
- achristmascarolm3q0[.]vidilife[.]com
- advice-crisis-christmas[.]pages[.]dev
- ae-christmas[.]pages[.]dev
- ae-christmas[.]studyinglover[.]com
- aldlchristmas[.]pages[.]dev
- ale-ruiz-christmas[.]clarissa-gutierrez[.]com
- alessias-christmas-m[.]babys1ststudio[.]co[.]uk
- alevittownchristmascarol[.]com[.]righteousjolly[.]com
- alex-reshetov-christmas-live-wallpaper[.]in[.]uptodown[.]com
- algharb-christmas-2[.]phazephotography[.]com
- all-i-want-for-christmas-is-you[.]skysound7[.]com
- altools-christmas-wallpapers[.]kr[.]uptodown[.]com
- amanda-christmas[.]alphotographyessex[.]com
- amandas-christmas-mi[.]maisaaphotography[.]com
- amax-lwps-christmas-live-wallpaper[.]th[.]uptodown[.]com
- amax-lwps-christmas-night-live-wallpaper[.]en[.]uptodown[.]com
- amazing-tropical-christmas[.]skysound7[.]com