Malicious Ads Targeting Advertisers in the DNS Spotlight

Table of Contents

Executive Report

Microsoft and Google almost always land on the list of most-phished brands, and that is not surprising given their huge market presence. And phishers are often the most likely threat actors to bank on the brands' popularity for the success of their attacks.

Malwarebytes Labs, in fact, dove deep into a new campaign targeting Microsoft advertisers. The threat actors used malicious Google ads to steal the login information of users of Microsoft's advertising platform.

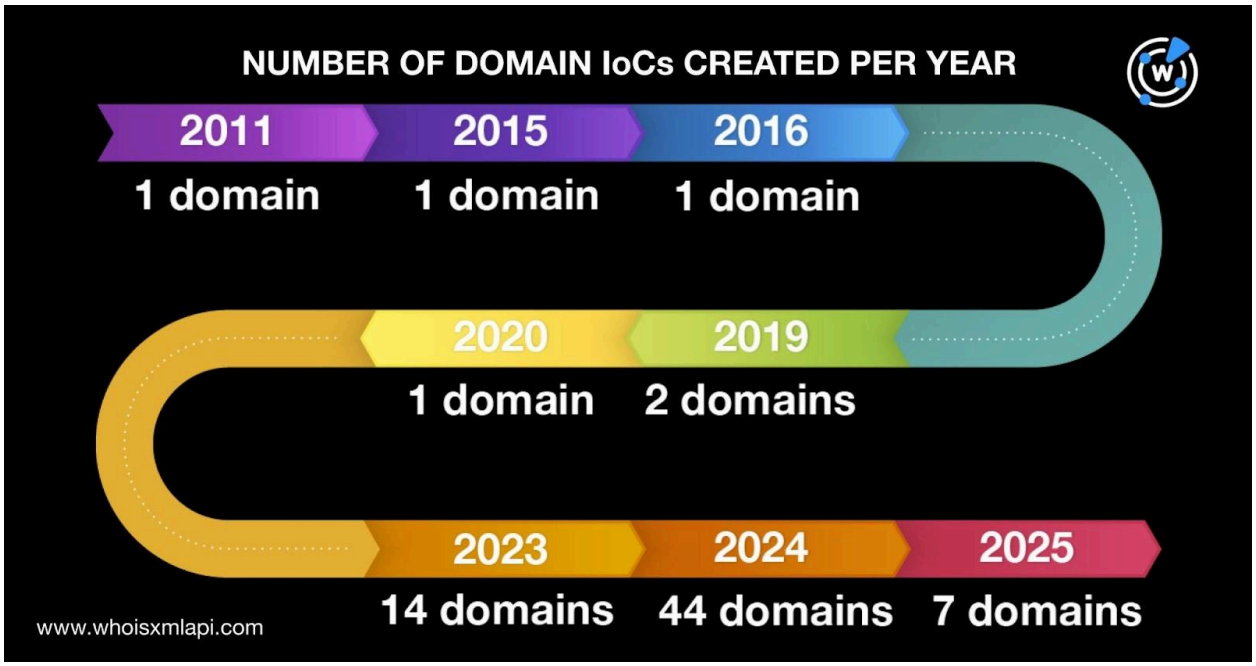
The researchers identified 97 domains as indicators of compromise (IoCs) in their report. WhoisXML API expanded the current IoC list using our extensive collection of DNS intelligence and uncovered additional connected artifacts, namely:

- 204 email-connected domains
- 25 IP addresses, 16 of which turned out to be malicious
- 483 IP-connected domains
- 417 string-connected domains

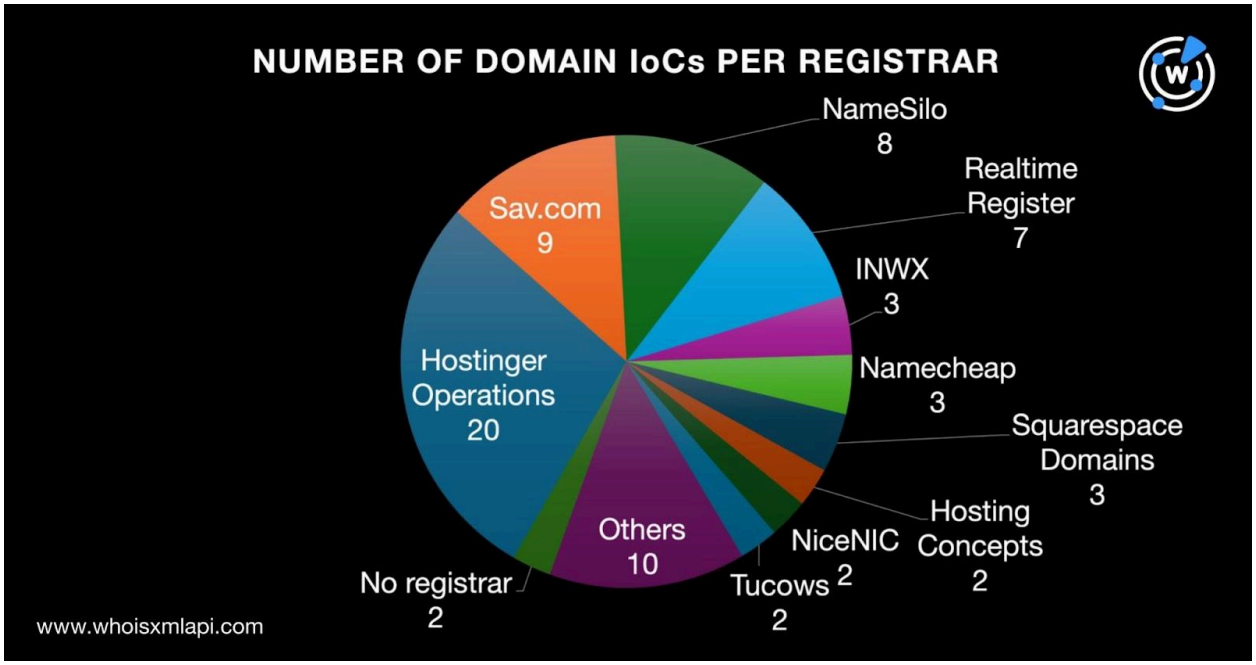
A Closer Look at the IoCs

We began our investigation by querying the 97 domains identified as IoCs on Bulk WHOIS API. The results showed that only 71 of the domains had current WHOIS records. Based on the data we obtained, we found that:

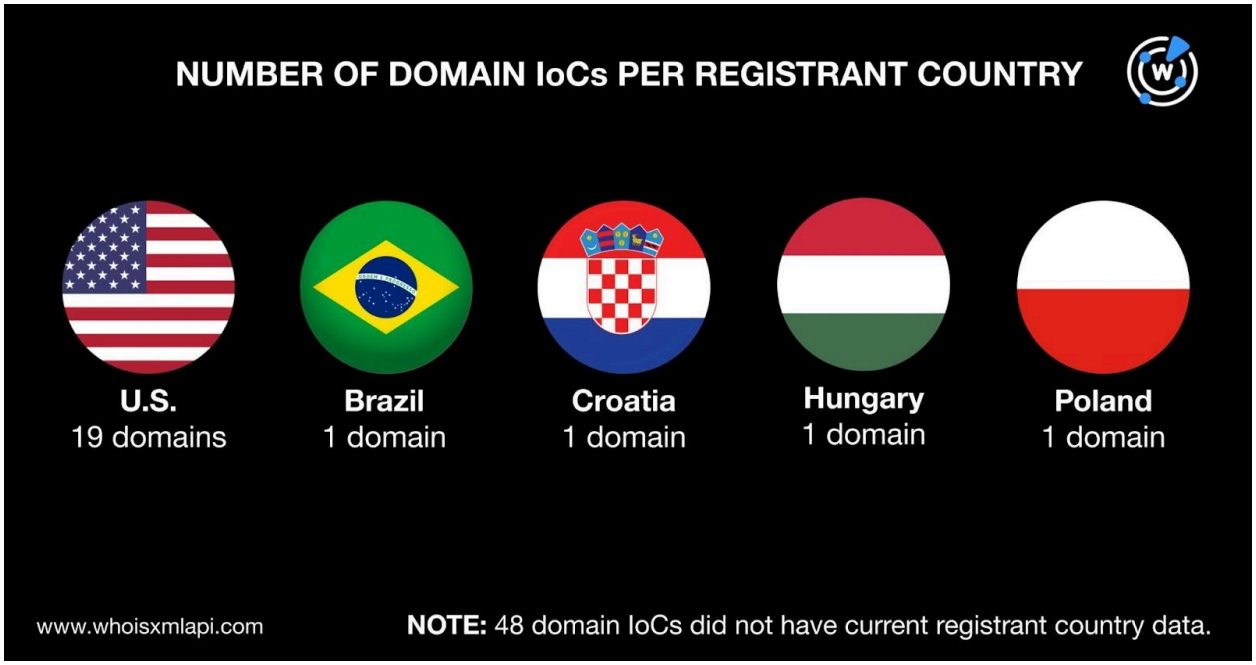
- A majority of the domains, 44 to be exact, were created in 2024. Overall, the IoCs were a mix of both old and new, created between 2011 and 2025. Specifically, 44 domains were created in 2024 as previously mentioned; 14 in 2023; seven in 2025; two in 2019; and one each in 2011, 2015, 2016, and 2020.



- While two of the domains did not have current registrar information, the remaining 69 were spread across 20 different registrars. Hostinger Operations was the top registrar, accounting for 20 IoCs. Sav.com took the second spot with nine domains. NameSilo placed third with eight IoCs. In fourth place was Realtime Register with seven domains. INWX, Namecheap, and Squarespace Domains tied in fifth place with three IoCs each. Hosting Concepts, NiceNIC, and Tucows shared the sixth place with two domains each. Finally, Cloud9, Dynadot, Internet Domain Service, Name SRS, Orbis, PDR, REGTIME-RU, Virtua Drug, Web Commerce, and 阿里云计算有限公司（万网） administered one IoC each.



- The U.S. was the top registrant country, accounting for 19 domains. One IoC each was registered in Brazil, Croatia, Hungary, and Poland. A total of 48 domains, meanwhile, did not have current registrant country information.



We also queried the 97 domains identified as IoCs on DNS Chronicle API and found that 84 of them had DNS histories. Altogether, the 84 domains recorded 1,560 IP resolutions over time.

The IoC euroinvest[.]ge, in particular, posted the oldest first IP resolution date—4 October 2019. Take a look at the DNS histories of five other domains below.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
30yp[.]com	32	29 September 2021
adsadvertising[.]online	2	25 May 2024
blseaccount[.]cloud	16	22 January 2024
krakeri-login[.]com	24	21 May 2024
poezija[.]com[.]hr	109	15 October 2019

IoC List Expansion Analysis Findings

We started our IoC list expansion by querying the 97 domains identified as IoCs on WHOIS History API. We uncovered 59 email addresses from the historical WHOIS records of 32 domains after duplicates were filtered out. Further scrutiny of the 59 email addresses revealed that 26 were public addresses.

A Reverse WHOIS API query for the 26 public email addresses showed that none of them appeared in other domains' current WHOIS records.

So, we dug deeper. We queried the 26 public email addresses and found that 14 appeared in the historical records of 204 email-connected domains after duplicates and those already identified as IoCs were filtered out.

Next, a DNS Lookup API query for the 97 domains identified as IoCs revealed that they actively resolved to 25 IP addresses after duplicates were filtered out.

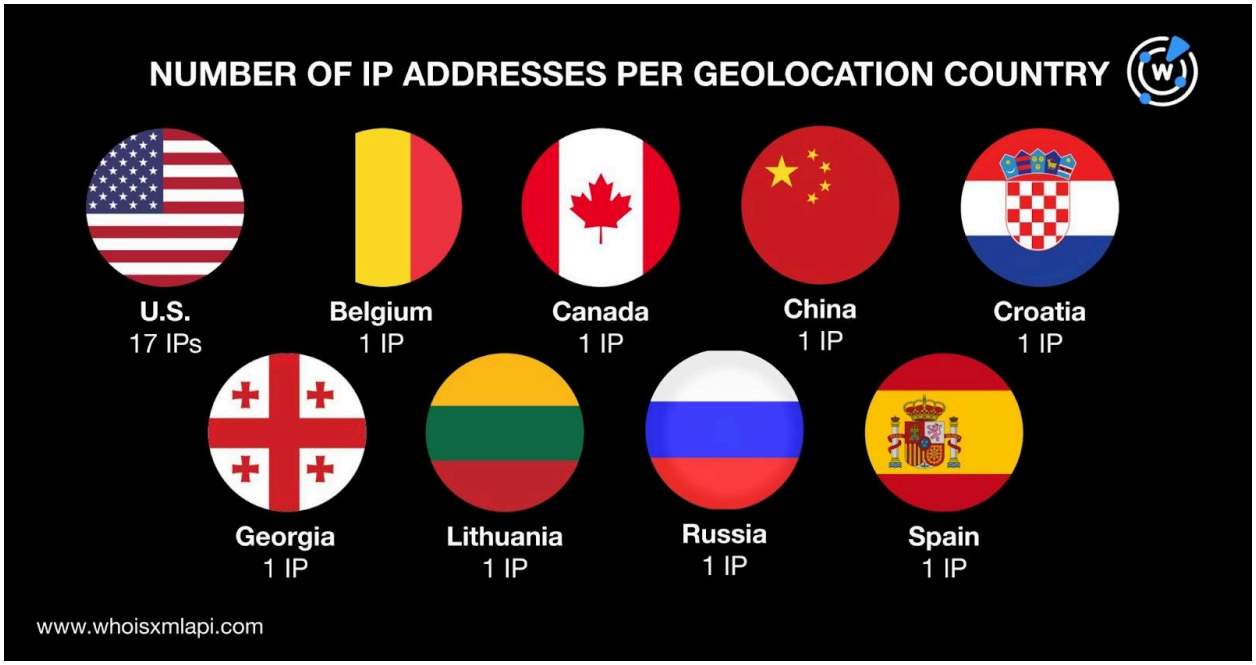
A Threat Intelligence API query for the 25 IP addresses showed that 16 were already considered malicious. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]32[.]1	Attack Command and control (C&C) Generic threat Malware distribution

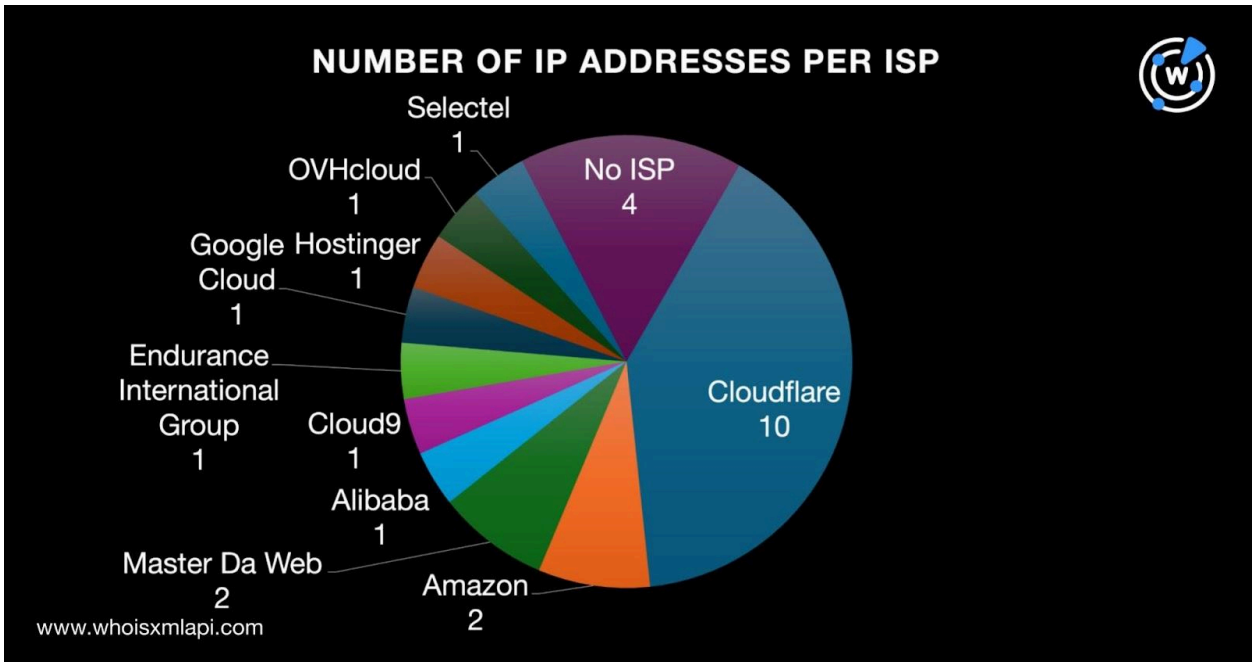
	Phishing Spam campaign Suspicious activity
104[.]21[.]7[.]203	Generic threat Malware distribution Phishing
15[.]197[.]130[.]221	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
172[.]67[.]203[.]159	Attack Malware distribution
34[.]76[.]205[.]124	Attack Generic threat Malware distribution Phishing

We then sought to find more information on the 25 IP addresses starting with a Bulk IP Geolocation Lookup query that led to these findings:

- They were geolocated in nine different countries led by the U.S., which accounted for 17 IP addresses. One IP address each, meanwhile, was geolocated in Belgium, Canada, China, Croatia, Georgia, Lithuania, Russia, and Spain.



- While four IP addresses did not have current ISP information, the remaining 21 were administered by 10 different ISPs led by Cloudflare, which accounted for 10 IoCs. Amazon and Master Da Web administered two IP addresses each. Finally, one IP address each fell under the administration of Alibaba, Cloud9, Endurance International Group, Google Cloud, Hostinger, OVHcloud, and Selectel.



To continue our search for connected artifacts, we queried the 25 IP addresses on Reverse IP API. We discovered that all of them had current domain resolutions. We also found that six could be dedicated IP addresses. Altogether, the six IP addresses hosted 483 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

As our final step, we collated 93 text strings from the 97 domains identified as IoCs. Domains & Subdomains Discovery searches allowed us to find domains that started with these 35 strings:

- 30yp.
- account-microsoft.
- accounts-ads.
- admicrosoft.
- ads-microsoft.
- ads-miicrosoft.
- adsadvertising.
- adsmicrosoft.
- advertising-bing.
- advertising-mlcrosoft.
- bewears.
- bîlkub.
- bing-ads.
- blokchaln.
- ciree.
- côinlíst.
- colnhouse-fr.
- con-webs.
- digitechmedia.
- euroinvest.
- exchangefastex.
- itlinks.
- login-acount.
- microsoft-ads.
- microsoftbingads.
- mlcr0soft.
- mnws.
- mudinhox.
- ndnet.
- phlyd.
- poezija.
- portfoliolkraken.
- smartlabor.
- userads.
- www-bingads.

All in all, we uncovered 417 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

Domains That Could Be Weaponized for Attacks Targeting Google and Microsoft

Given that the threat actors behind the campaign featured in this report trailed their sights on Google and Microsoft based on the inclusion of domains like account-microsoft[.]online and the platform the threat actors abused (i.e., Google). We also noticed that many of the connected domains we uncovered contained brands connected to the two companies. So, we dug deeper into the branded connected artifacts.

We collated 11 connected domains with text strings that could pertain to Google Ads. A Bulk WHOIS API query for them showed none could be publicly attributed to Google.

We also collected 71 connected domains containing text strings that could pertain to Microsoft and Bing. Bulk WHOIS API, however, revealed that only one—bing-ads[.]com[.]au—was publicly attributable to the company.

—

Our IoC list expansion analysis led to the discovery of 1,129 connected artifacts comprising 204 email-connected domains, 25 IP addresses, 483 IP-connected domains, and 417 string-connected domains. Of these, 16 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 Email-Connected Domains

- 001ce[.]cn
- 00qq[.]com
- a88i[.]cn
- ad-words[.]pro
- babakfakhamzadeh[.]com
- babasprojects[.]com
- cjceo[.]cn
- comeandplaywith[.]us
- dailyshit[.]net
- deriveapp[.]net
- encryptonize[.]com
- equidisti[.]me
- f88w[.]cn
- faap[.]com[.]cn
- gamerindex[.]net
- hashhouseharrierssongbook[.]com
- healthenrichpl[.]us
- iamthewalker[.]com
- iamwalkingit[.]com
- jingjiayun[.]cn
- jowu[.]net
- k163[.]net
- khazimula[.]org
- leip[.]com[.]cn
- liuxinkt[.]cn
- malaysiamarketplace[.]online

- mastababa[.]com
- nataliaviana[.]org
- parkroisrl[.]com
- pedaloso[.]com
- qox[.]com[.]cn
- restylinglogo[.]com
- rinnovailtuobusiness[.]com
- salonquiz[.]com
- saunteringverse[.]com
- tecnotexbr[.]com[.]br
- temporari[.]us
- users-blokchain[.]info
- veto[.]org
- villabarbablanca[.]com
- wallet-biockhain[.]com
- wallets--blokchain[.]info
- youyh[.]cn
- yqdzsw[.]cn
- zjydn[.]cn
- zyza[.]cn

Sample IP Addresses

- 104[.]21[.]16[.]1
- 144[.]217[.]140[.]12
- 15[.]197[.]130[.]221
- 172[.]67[.]142[.]131
- 178[.]218[.]163[.]181
- 188[.]93[.]90[.]230
- 192[.]185[.]216[.]95
- 199[.]59[.]243[.]228
- 34[.]76[.]205[.]124
- 45[.]40[.]96[.]193
- 5[.]189[.]231[.]251
- 50[.]116[.]112[.]98
- 63[.]251[.]122[.]121
- 74[.]119[.]239[.]234
- 8[.]141[.]87[.]17
- 84[.]32[.]84[.]33

Sample IP-Connected Domains

- accountraken[.]app
- ads[.]mlcroso[.]fit
- alrdropbeefy[.]cloud
- babyandmom[.]com[.]hr
- bakinecarolije[.]com
- bitbuy-app[.]com
- coinsquare-pro[.]com
- cpanel[.]babyandmom[.]com[.]hr
- cpanel[.]culexalpha[.]com
- dashboardkarken[.]com
- dashboradpro[.]com
- dashlboardpro[.]com
- exploredalmatia[.]com[.]hr
- exploredalmatia[.]eu
- fc001[.]jingjiayun[.]com[.]cn
- fc002[.]jingjiayun[.]com[.]cn
- festivalpozor[.]com
- games[.]gala-alrdropton[.]cloud
- gamesonlinegala[.]top
- geneko[.]hr
- hg001[.]jingjiayun[.]com[.]cn
- hg002[.]jingjiayun[.]com[.]cn
- hg003[.]jingjiayun[.]com[.]cn
- inter-dekor[.]hr
- jamstva[.]com
- jamstvo[.]culexapi[.]eu
- jamstvo[.]net
- kafren-return[.]com
- kaiaka-returne[.]com
- kaika-returne[.]com
- lowrider-tattoo[.]com
- mail[.]babyandmom[.]com[.]hr
- mail[.]culexalpha[.]com
- mail[.]djecjivrticmendula[.]hr

- n10-zagreb[.]com
- nautico[.]hr
- ny001[.]jingjiayun[.]com[.]cn
- osijek031[.]com[.]hr
- painelkraken[.]com
- payglobalretailers[.]com
- phg001[.]jingjiayun[.]com[.]cn
- qc001[.]jingjiayun[.]com[.]cn
- qc002[.]jingjiayun[.]com[.]cn
- qc003[.]jingjiayun[.]com[.]cn
- rewarder-official[.]com
- robineta[.]com
- santos[.]hr
- sdcoffeewinemore[.]com
- sgrney[.]com
- topdigital[.]hr
- trade[.]blsonhome[.]top
- vdsnow[.]ru
- viplimousines[.]com[.]hr
- webdisk[.]babyandmom[.]com[.]hr
- webdisk[.]culexalpha[.]com
- webdisk[.]djecjivrticmendula[.]hr
- x5x[.]host
- x5x[.]ru
- x5x[.]tech
- yl007[.]jingjiayun[.]com[.]cn
- you-hodler[.]com
- youh0dler[.]app
- zlatarna-sardoniks[.]hr

Sample String-Connected Domains

- 30yp[.]cc
- 30yp[.]cn
- account-microsoft[.]cf
- account-microsoft[.]co
- accounts-ads[.]com
- accounts-ads[.]com[.]ua
- admicrosoft[.]xyz
- ads-microsoft[.]cc
- ads-microsoft[.]cloud
- adsadvertising[.]ae
- adsadvertising[.]co[.]in
- adsmicrosoft[.]best
- adsmicrosoft[.]com
- advertising-bing[.]com
- advertising-mlcrosoft[.]com
- bewears[.]nl
- bing-ads[.]cn
- bing-ads[.]co
- blokchaln[.]co
- blokchaln[.]com[.]co
- ciree[.]be
- ciree[.]ca
- colnhouse-fr[.]site
- con-webs[.]online
- digitechmedia[.]biz
- digitechmedia[.]ca
- euroinvest[.]ae
- euroinvest[.]at
- exchangefastex[.]com
- exchangefastex[.]us
- itlinks[.]au
- itlinks[.]be
- login-acount[.]cf
- login-acount[.]com
- microsoft-ads[.]com
- microsoft-ads[.]ga
- microsoftbingads[.]com[.]br
- mlcr0soft[.]cf
- mlcr0soft[.]de
- mnws[.]ac[.]th
- mnws[.]bid
- mudinhox[.]com
- mudinhox[.]com[.]br
- ndnet[.]aichi[.]jp

- ndnet[.]ca
- phlyd[.]cn
- phlyd[.]dk
- poezija[.]ba
- poezija[.]co
- smartlabor[.]ai
- smartlabor[.]ch
- userads[.]com
- userads[.]ga
- www-bingads[.]online
- www-bingads[.]site
- xn--blkub-5sa[.]com
- xn--cinlst-6va6c[.]online
- xn--cinlst-6va6c[.]site