A DNS Deep Dive into Web Hosting Service Provider AWT

Table of Contents

Executive Report

WhoisXML API threat researcher Dancho Danchev recently uncovered that web hosting service provider Advanced Web Tech (AWT) could be involved in several malicious campaigns. His research revealed pertinent information about AWT's potential owner with details including his registrant name and registrant organization (i.e., Advanced Web Tech).

Our research team used Danchev's findings as jump-off points for a DNS deep dive. We expanded a list of 14 domains identified as indicators of compromise (IoCs), namely:

- almanar-tv[.]net
- almanartv[.]news
- app-news[.]org
- awt-lb[.]com
- awt-lb[.]net
- awt-lb[.]org
- awt[.]com[.]lb
- dar-almanar[.]com
- dar-almanar[.]net
- dar-almanar[.]org
- fastpublish[.]net
- lcg-lb[.]com
- manar[.]news
- manartv[.]news

Our IoC expansion analysis aided by WHOIS, DNS, and threat intelligence led to the discovery of close to 2,000 potentially connected artifacts, specifically:

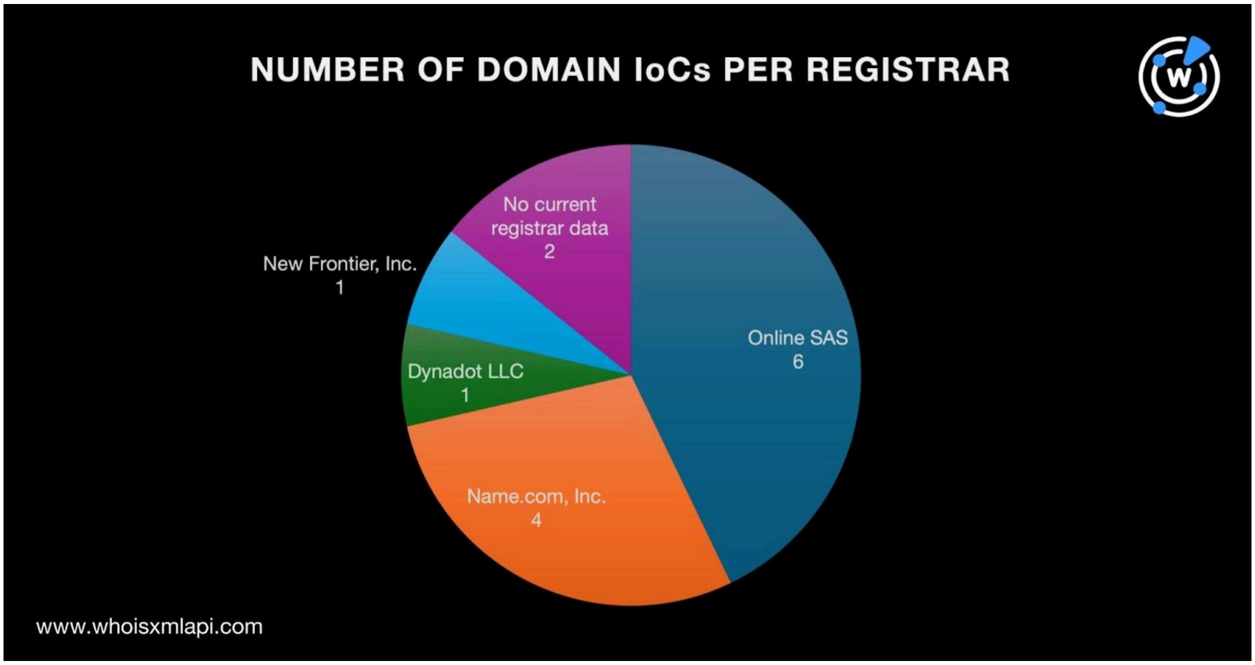
- 456 registrant-connected domains
- Seven email-connected domains
- 14 IP addresses, five of which turned out to be malicious
- 1,055 IP-connected domains, two of which turned out to be malicious
- 377 string-connected domains

A sample of the additional artifacts obtained from our analysis is available for download from our website.

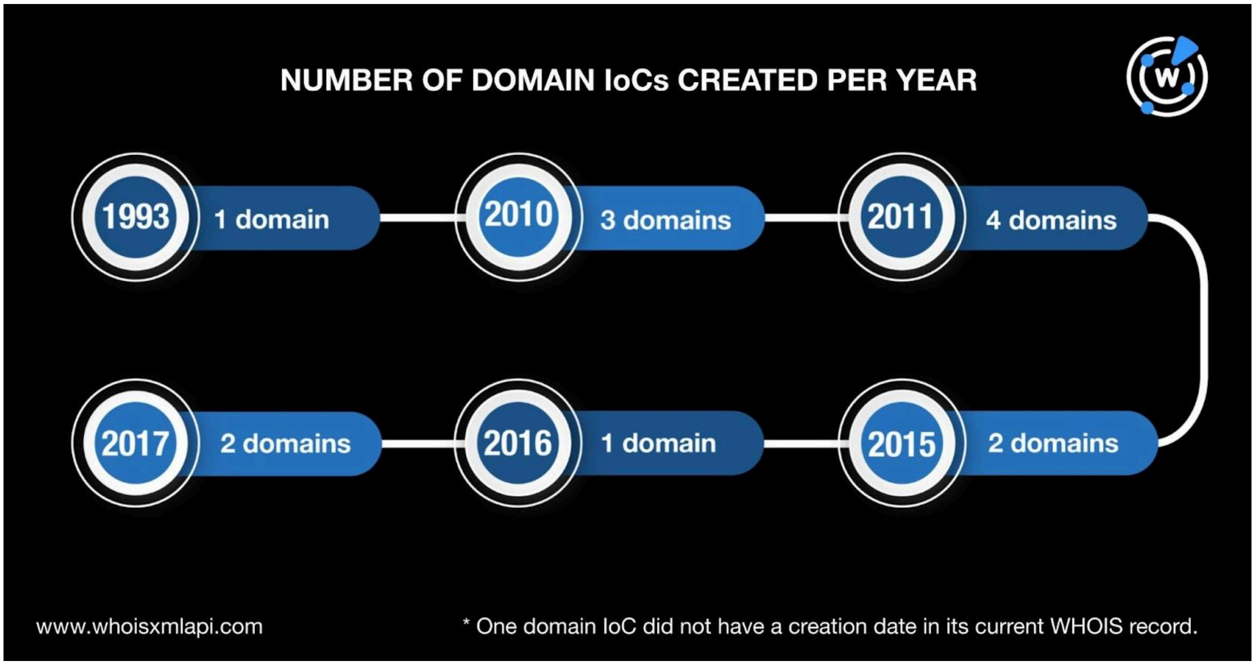
AWT IoC Facts

As is our usual first step, we sought to find out more about the IoCs. We performed a bulk WHOIS lookup for the 14 domains tagged as IoCs, which revealed that:

- Online SAS was the top registrar, accounting for six of the domains named as IoCs. Name.com, Inc. took the second spot with four domain IoCs. Dynadot LLC and New Frontier, Inc., meanwhile, accounted for one domain IoC each. Two domain IoCs did not have registrar data in their current WHOIS records.



- Thirteen of the domains classified as IoCs were created between 1993 and 2017, which could show a threat actor preference for aged domains. Specifically, one domain IoC was created way back in 1993, three in 2010, four in 2011, two in 2015, one in 2016, and two in 2017. One domain IoC did not have a creation date in its current WHOIS record.



NUMBER OF DOMAIN IoCs CREATED PER YEAR

1993 1 domain

2010 3 domains

2011 4 domains

2015 2 domains

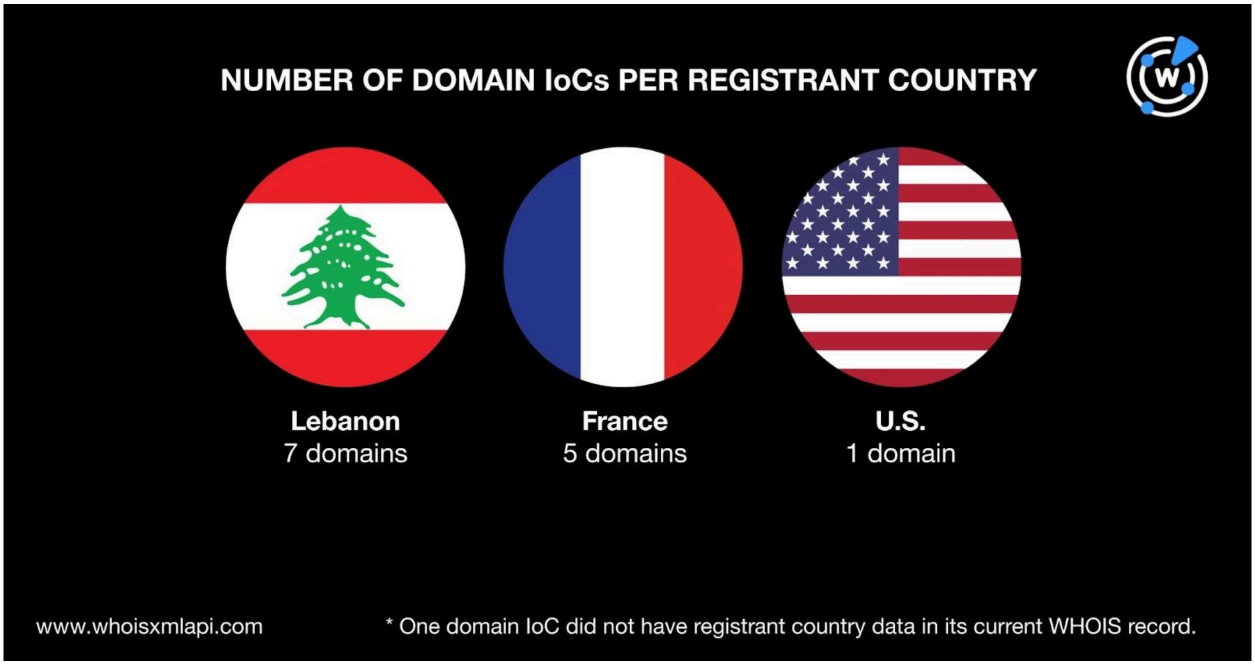
2016 1 domain

2017 2 domains

www.whoisxmlapi.com

* One domain IoC did not have a creation date in its current WHOIS record.

- Lebanon was the top registrant country, accounting for seven of the domains categorized as IoCs. France took second place with five domain IoCs. One domain IoC was registered in the U.S. Finally, one domain IoC did not have registrant country data in its current WHOIS record.



NUMBER OF DOMAIN IoCs PER REGISTRANT COUNTRY

Lebanon
7 domains

France
5 domains

U.S.
1 domain

www.whoisxmlapi.com

* One domain IoC did not have registrant country data in its current WHOIS record.

- Five of the domains identified as IoCs also had public registrant information, particularly two registrant names and one registrant organization (i.e., AWT), in their current WHOIS records that could point to other threat actors or its owner's aliases.

AWT IoC List Expansion Analysis Findings

After obtaining more information on the current list of IoCs, we sought to determine if other web properties could be connected to AWT.

We began by looking for WHOIS records that contained any of the registrant names we found earlier (from the current WHOIS records of five domain IoCs) or registrant organizations (i.e., Advanced Web Tech obtained by Danchev and AWT from the current WHOIS records of five of the domain IoCs).

Historical reverse WHOIS searches for registrant name and organization exact matches gave us 456 registrant-connected domains after duplicates and the domain IoCs were filtered out.

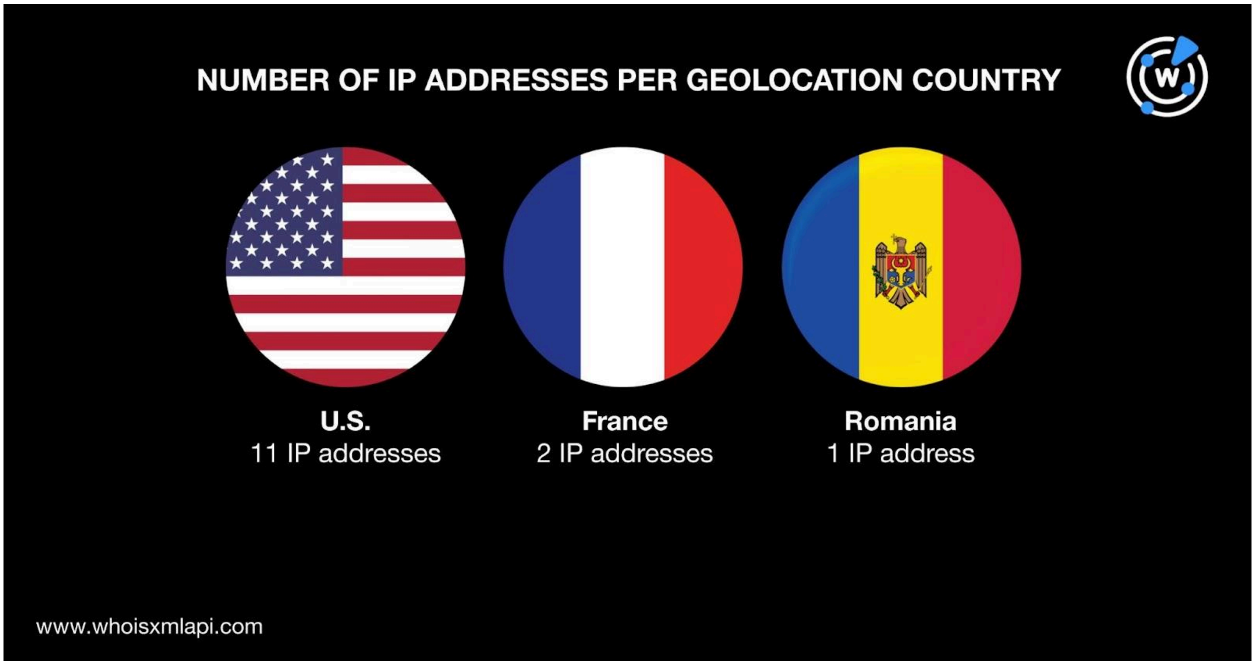
Next, we queried the 14 domains named as IoCs on WHOIS History API and uncovered 10 email addresses in their historical WHOIS records. Two of the email addresses were public.

Reverse WHOIS API queries for the two public email addresses allowed us to identify seven email-connected domains after duplicates, the IoCs, and the registrant-connected domains were removed.

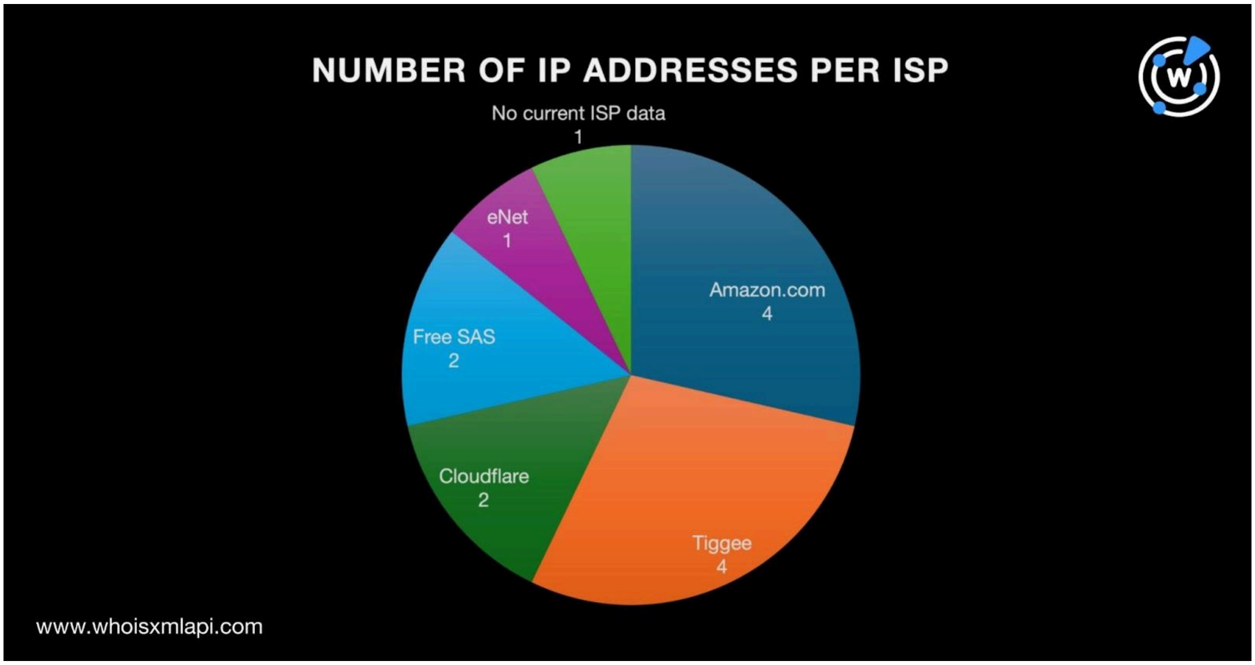
DNS lookups for the 14 domains classified as IoCs showed they resolved to 14 IP addresses after duplicates were filtered out. Threat intelligence lookups for them revealed that five were associated with various threats, including phishing, generic threats, and malware distribution.

A bulk IP geolocation lookup for the 14 IP addresses showed that:

- They were spread across three countries—11 in the U.S., two in France, and one in Romania.



- Amazon.com and Tiggee topped the list of ISPs, accounting for four IP addresses each. Cloudflare and Free SAS administered two IP addresses each and eNet handled one. One IP address did not have ISP information.



Reverse IP/DNS lookups for the 14 IP addresses revealed that six of them could potentially be dedicated. Altogether, they hosted 1,055 domains after duplicates, the IoCs, and the registrant-

and email-connected domains were removed. Threat intelligence lookups also showed two of the IP-connected domains—cdn-ci74[.]actonsoftware[.]com and cdn-forpci74[.]actonsoftware[.]com—were associated with generic threats.

WHOIS record comparisons between the 14 domains tagged as IoCs and the 1,055 IP-connected domains revealed that:

- 20 IP-connected domains shared the IoCs’ registrars.
- 161 IP-connected domains were created in the same years as the IoCs.
- 418 IP-connected domains were registered in the same countries as the IoCs.

To cover all the bases, we then scoured the DNS for other domains containing text strings found among the 14 domains categorized as IoCs. Domains & Subdomains Discovery provided us with 377 domains that started with strings that appeared in some of the IoCs, namely:

- **almanar-tv.**
- **almanartv.**
- **app-news.**
- **awt.**
- **fastpublish.**
- **manar.**
- **manartv.**

WHOIS record comparisons between the 14 domains classified as IoCs and the 377 string-connected domains showed that:

- 10 string-connected domains shared the IoCs’ registrars.
- 51 string-connected domains were created in the same years as some of the IoCs.
- One string-connected domain shared the registrant name of some of the IoCs.
- Three string-connected domains shared the registrant organization of some of the IoCs.
- 48 string-connected domains were registered in the same countries as the IoCs.

—

Our expansion analysis of the 14 domains identified as AWT IoCs led to the discovery of 1,909 potentially connected artifacts comprising nearly 1,900 connected domains and 14 IP addresses. It also allowed us to identify two additional names that could belong to AWT employees or affiliates. Interestingly, seven of the artifacts we uncovered may have already been weaponized for various malicious campaigns.

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 Registrant-Connected Domains

- 47billion[.]com
- a-alqasim[.]com
- abdelqaderalraies[.]com
- abdelqaderalraies[.]net
- abdelqaderalraies[.]org
- abdelwahhab[.]com
- abohaniyeh[.]com
- abudhabi-it[.]com
- acadagive[.]com
- acadagive[.]org
- achintyawebtech[.]com
- adeniny[.]com
- adieu-celibat[.]com
- africawildlifetracking[.]com
- ahlalathar[.]com
- ahlalathar[.]net
- ahmadhammoud[.]info
- airdropworldtoken[.]com
- ais-info[.]net
- akhyworldtrip[.]com
- akhyworldtrip[.]fr
- alajami[.]info
- alalbany[.]biz
- alalbany[.]mobi
- alalbany[.]net
- alalbany[.]online
- alalbany[.]org
- alalbany[.]xyz
- alarabia[.]biz
- alawaysheh[.]com
- alawaysheh[.]net
- albalagh[.]info
- albanymarkaz[.]org
- alfatwah[.]com
- alfatwah[.]info
- alfatwah[.]net
- alfatwah[.]org
- alghazzawihousekeeping[.]com
- alhudaythi[.]com
- alittihad[.]tv
- almahajjah[.]net
- almanarnews[.]org
- almozawwak[.]info
- alothaimeen[.]net
- alotrojjaherbs[.]net
- alraisart[.]com
- alrasibi[.]com
- alsalheen[.]info
- alzoughby[.]com
- anal-destructor[.]com

Sample Email-Connected Domains

- fotoausstellung[.]org
- fotobearbeitungsprogramm[.]org
- hundeausstellung[.]org
- insolvenzverfahren[.]org

Sample IP Addresses

- 13[.]225[.]142[.]3
- 13[.]225[.]142[.]125
- 13[.]225[.]142[.]34
- 13[.]225[.]142[.]104
- 213[.]36[.]252[.]183
- 213[.]36[.]252[.]182
- 89[.]39[.]149[.]251

Sample Malicious IP Addresses

- 213[.]36[.]252[.]183
- 213[.]36[.]252[.]182
- 96[.]45[.]82[.]75

Sample IP-Connected Domains

- 1234br[.]com
- 1hwosv1jov[.]xyz
- 21114[.]bet
- 21114[.]cc
- 23659[.]sistemawbuy[.]com[.]br
- 247[.]gay
- 2651[.]app
- 2651dhw[.]com
- 2651wz[.]com
- 2m1qm49opc[.]xyz
- 2s1r2bausy[.]xyz
- 360cloudsecurity[.]com
- 360cloudsupport[.]com
- 360dmarc[.]com
- 360uptodate[.]com
- 365securescore[.]com
- 3689[.]app
- 3yadx55x60[.]xyz
- 416works[.]com
- 458o[.]com
- 458q[.]com
- 4consent[.]com
- 4mmodel[.]com
- 4real[.]live
- 4real[.]social
- 501g[.]kr
- 55128[.]bet
- 55oicllf60[.]xyz
- 567450[.]com
- 567470[.]com
- 567475[.]com
- 5bbvguxyzh[.]xyz
- 6ixsense[.]co[.]kr
- 716ia1glsn[.]xyz
- 74qzn6d6qyj[.]xyz
- 85118tktz[.]com
- 85118tukutz[.]com
- 85118tz[.]com
- 92rock[.]ae
- a1[.]gg
- a10cdn[.]com
- a1distributorsguernsey[.]com
- aaronwatson[.]store
- abiweekly[.]org
- abm-holdings[.]com
- accruent-insights[.]com
- acousticartanddesign[.]com[.]au
- addedfearinglestpe[.]com
- administephawaii[.]com
- advid[.]com

- afd-stadt-bielefeld[.]de
- ahyun[.]net
- aihastudy[.]com
- aimtcorp[.]com
- akita-murayama-lawoffice[.]com
- albarakah-lb[.]org
- alencon-ouvertures[.]com
- alerfan[.]org
- alfasadwalqadaa[.]info
- all-in[.]drake[.]edu[.]scalefunder-service[.]net
- allcountiescourier[.]com
- alldayon[.]co[.]kr
- alles[.]website
- alliedinvestigativeservices[.]com
- alphabet[.]school
- alwafaabloc[.]org
- alwasat[.]news
- always3patti[.]co
- alzakiya[.]com
- amal-baladi[.]org
- amalbaladi[.]com
- amalbaladi[.]net
- amalbaladi[.]org
- amalbaladi[.]org[.]lb
- amanassociation[.]org
- amankids[.]com
- amarin[.]mozello[.]lv
- ami-usa[.]com
- amway[.]reviews[.]bazaarvoice[.]com
- amydightondesign[.]com
- aneleyporto[.]com[.]ar
- animebanter[.]com
- appliedkinetics[.]com[.]au
- aptone[.]kr
- arabmediagroup[.]ae
- arapsun-turkiye[.]com
- areu[.]co[.]kr
- arnnewscenter[.]ae
- artawardchosun[.]com
- article21corp[.]com
- asankeun[.]com
- ashleavets[.]co[.]uk
- assaggio[.]hk
- assets[.]talkspace[.]com
- assirat[.]com[.]lb
- assirat[.]net
- assistansbolaget[.]nu
- association-alghadir[.]org
- ata-engineering[.]com[.]sg
- atcarpentry[.]com[.]sg

Sample String-Connected Domains

- almanar-tv[.]com
- almanar-tv[.]org
- almanartv[.]com
- almanartv[.]com[.]lb
- almanartv[.]com[.]ph
- almanartv[.]de
- almanartv[.]media
- almanartv[.]net
- almanartv[.]org
- app-news[.]app
- app-news[.]biz
- app-news[.]co
- app-news[.]com
- app-news[.]de
- app-news[.]dev
- app-news[.]ga
- app-news[.]info
- app-news[.]ir
- app-news[.]jp
- app-news[.]link
- app-news[.]mobi
- app-news[.]my[.]id

- app-news[.]net
- app-news[.]online
- app-news[.]ru
- app-news[.]site
- app-news[.]store
- app-news[.]tk
- app-news[.]xyz
- awt[.]ac
- awt[.]ac[.]th
- awt[.]ae
- awt[.]aero
- awt[.]af
- awt[.]ag
- awt[.]agency
- awt[.]ai
- awt[.]airline[.]aero
- awt[.]app
- awt[.]asia
- awt[.]at
- awt[.]au
- awt[.]be
- awt[.]berlin
- awt[.]bet
- awt[.]biz
- awt[.]bj[.]cn
- awt[.]blue
- awt[.]buzz
- awt[.]by