WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A DNS Investigation of SEO Manipulation via Bad Seed BadIIS

Table of Contents

Executive Report

Trend Micro researchers recently uncovered a search engine optimization (SEO) manipulation campaign targeting users of Internet Information Services (IIS) with BadIIS. According to the researchers, the campaign is likely financially motivated since victims were redirected to illegal gambling websites. This campaign has already affected Asian countries like India, Thailand, and Vietnam although its impact can readily extend worldwide.

The in-depth investigation on BadIIS unveiled 51 indicators of compromise (IoCs) comprising 46 domains and five IP addresses. The WhoisXML API research team expanded the current list of IoCs and uncovered additional connected artifacts, including:

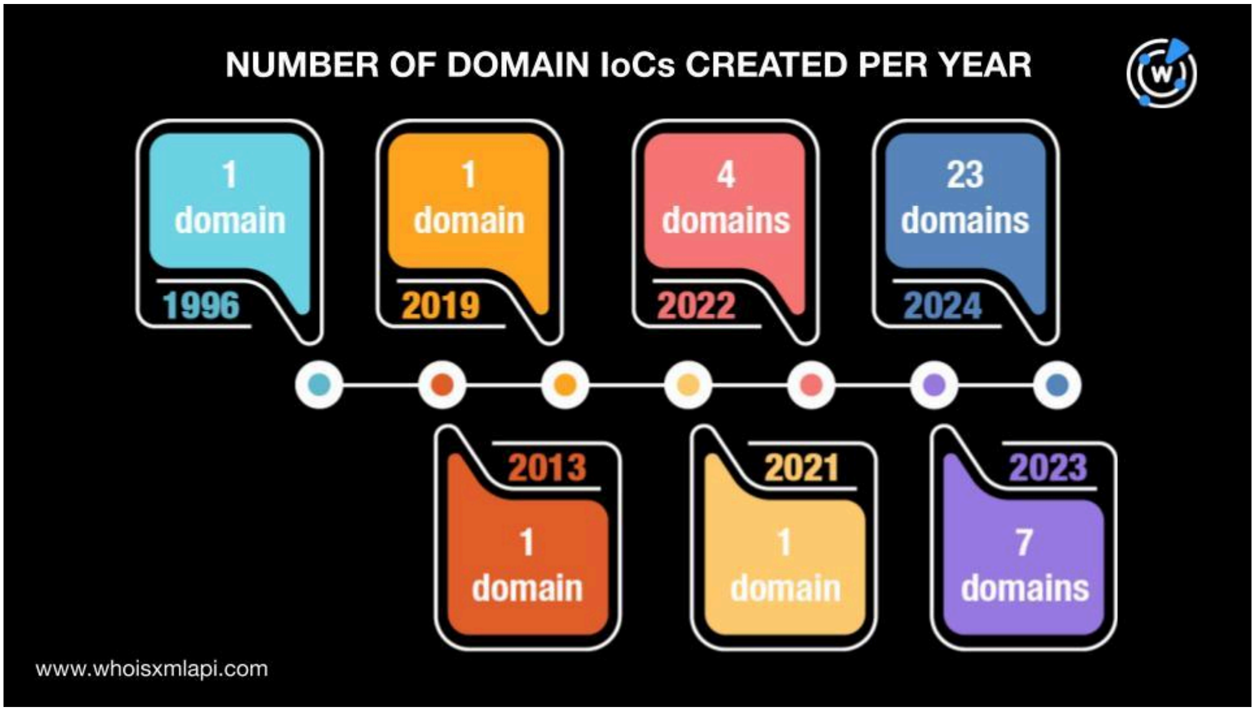
- 738 email-connected domains, two of which turned out to be malicious
- 29 additional IP addresses, 17 of which were associated with various threats
- 335 IP-connected domains
- 1,184 string-connected domains, nine of which have already been weaponized for various campaigns

A Closer Look at the BadIIS IoCs

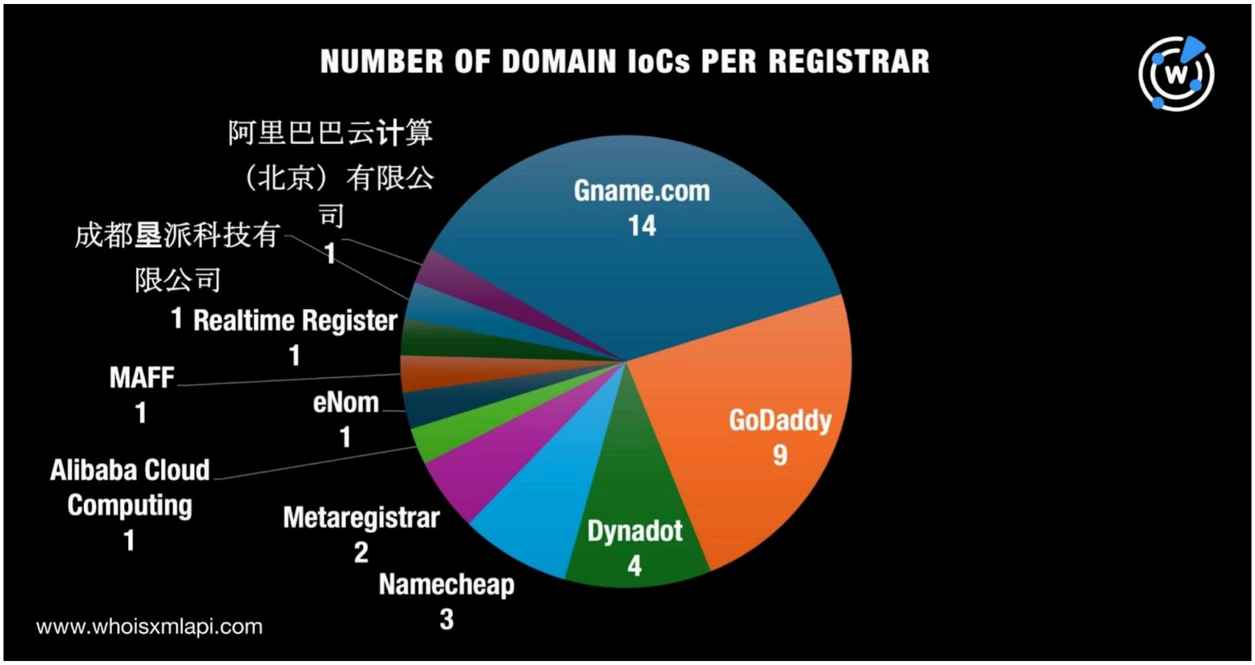
We began our analysis by looking more closely at the 51 BadIIS IoCs.

First, we queried the 46 domains identified as IoCs on Bulk WHOIS API and found that only 38 of them had current WHOIS records. Further scrutiny of these records showed that:

- They were created between 1996 and 2024. Specifically, 23 were created in 2024; seven in 2023; four in 2022; and one each in 1996, 2013, 2019, and 2021.

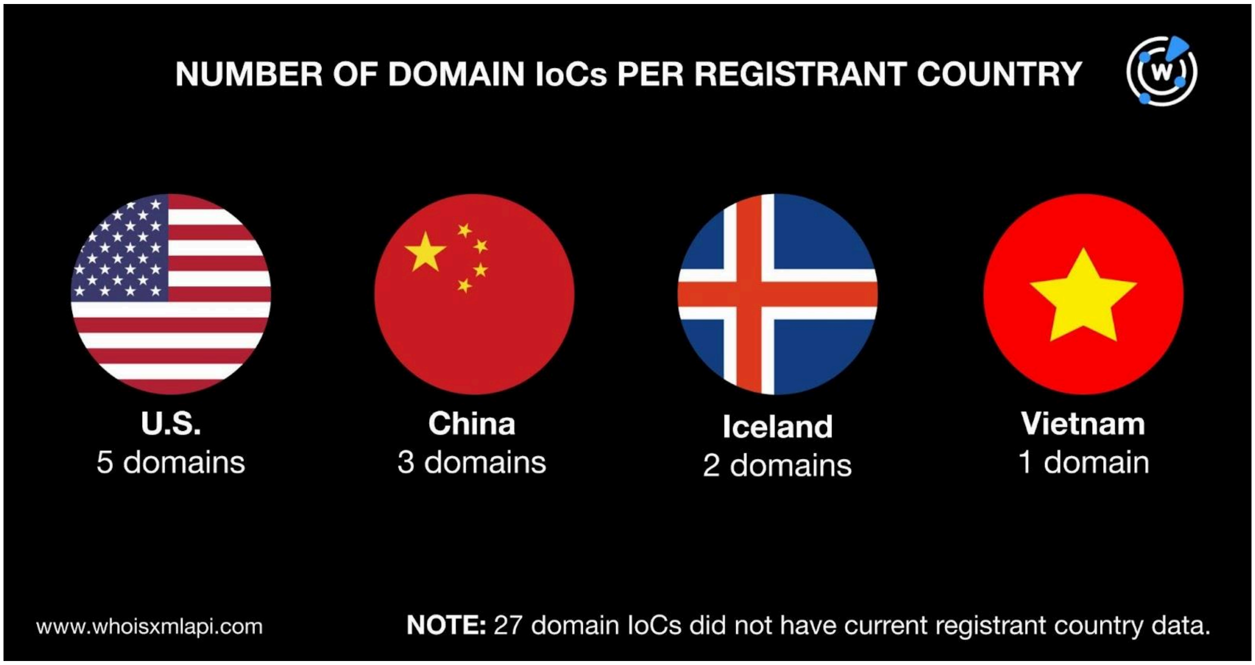


- They were split among 11 registrars led by Gname.com, which accounted for 14 domains. GoDaddy took the second spot with nine domains. Dynadot came in third place with four domains. Namecheap accounted for three domains, followed by Metaregistrar had two. Finally, Alibaba Cloud Computing, eNom, MAFF, Realtime Register, 成都垦派科技有限公司, and 阿里巴巴云计算（北京）有限公司 accounted for one domain each.



NUMBER OF DOMAIN IoCs PER REGISTRAR

- Only 11 of the 38 domains with current WHOIS records had registrant country information. They were registered in four different countries led by the U.S., which accounted for five domains. China took the second spot with three domains. Iceland placed third with two domains. Finally, Vietnam accounted for one domain.



NUMBER OF DOMAIN IoCs PER REGISTRANT COUNTRY

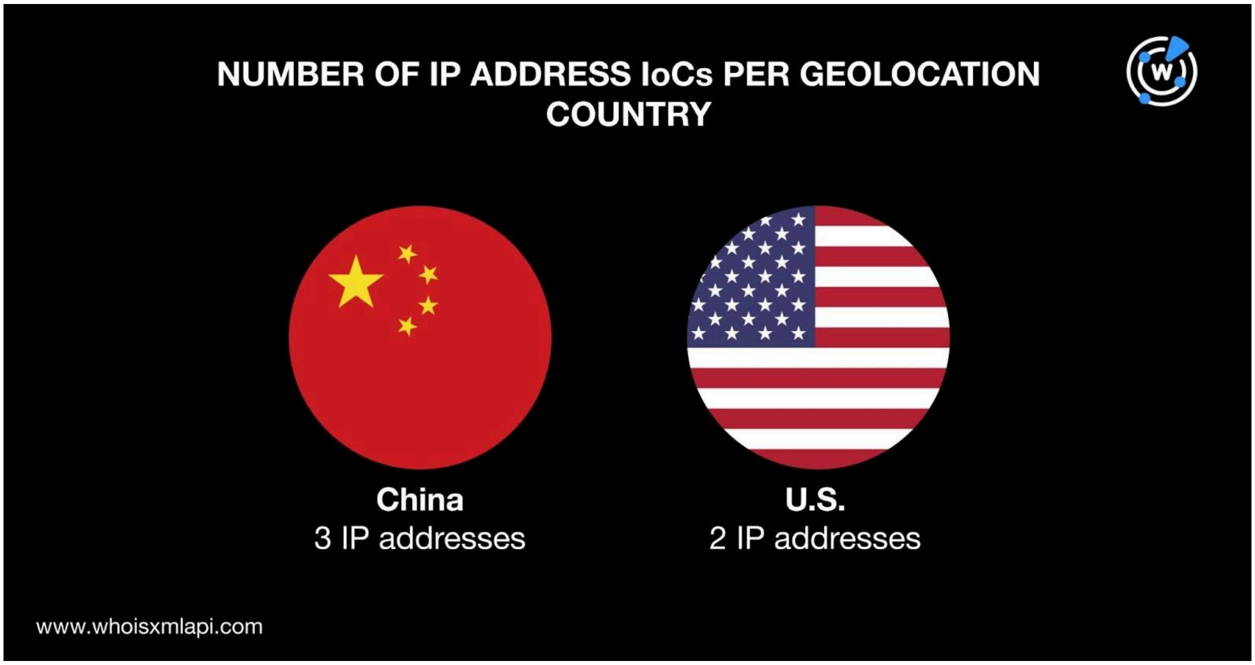
NOTE: 27 domain IoCs did not have current registrant country data.

Next, a DNS Chronicle API query for the 46 domains tagged as IoCs revealed that only 38 of them had historical IP resolutions. In particular, the 38 domains recorded a total of 2,111 IP resolutions over time. The domain xxxx[.]com's first recorded IP resolution occurred on 4 October 2019. The following table shows details about the DNS histories of five other domains.

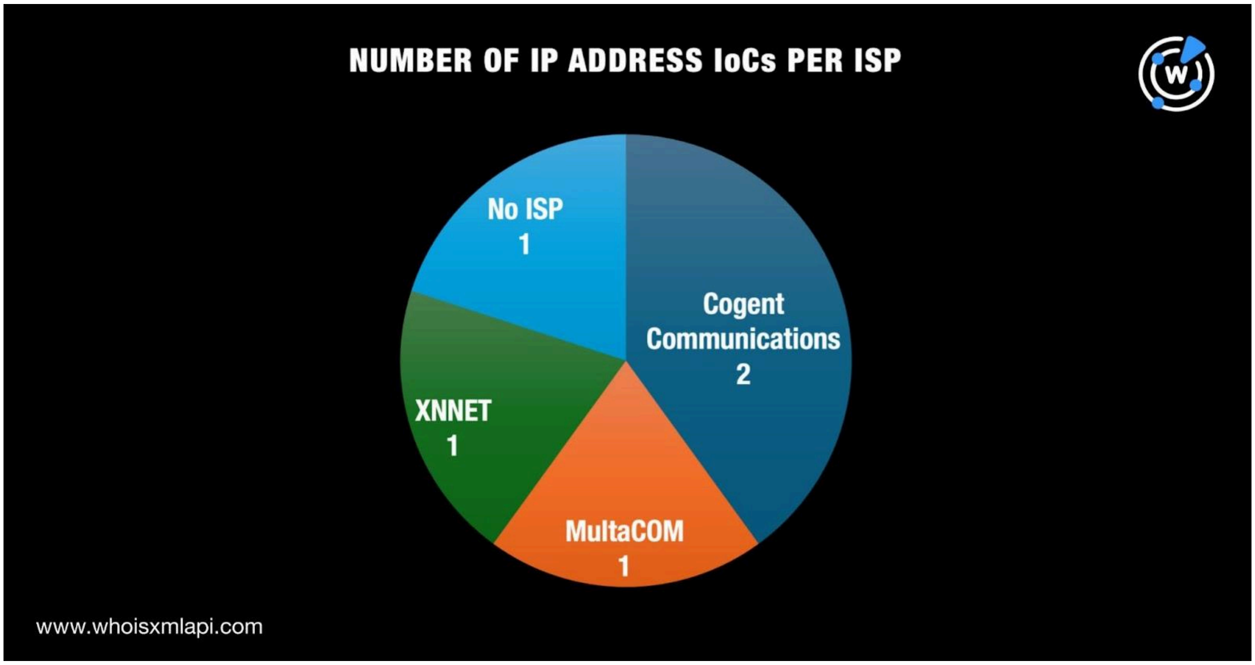
DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
668823[.]com	9	17 September 2021
brcknkblue[.]com	12	2 July 2024
dk8[.]land	77	14 January 2022
jumpiis8[.]com	12	16 January 2024
ruicaisiwang[.]com	35	10 October 2019

We then looked further into the five IP addresses classified as IoCs beginning with a Bulk IP Geolocation Lookup query, which showed that:

- They were geolocated in two countries—three in China and two in the U.S.



- Only four of the five IP addresses had ISP information. They were spread across three ISPs led by Cogent Communications, which administered two IP addresses. MultaCOM and XNNET managed one IP address each.



A DNS Chronicle API query for the five IP addresses identified as IoCs revealed that they all had domain resolutions. Specifically, they posted a total of 512 domain resolutions as of this writing. The IP address 156[.]229[.]134[.]13, for instance, posted the oldest domain resolution date—22 April 2020.

BadIIS IoC List Expansion Analysis

We began our hunt for more connected artifacts with a WHOIS History API query for the 46 domains tagged as IoCs. As it turns out, only 16 of them had email addresses in their historical WHOIS records. Specifically, the 16 domains had 92 email addresses after duplicates were filtered out. Only 28 of them, however, were public email addresses.

Next, we queried the 28 public email addresses on Reverse WHOIS API in a bid to uncover email-connected domains using current WHOIS records. We did not find any, unfortunately. So, we dug deeper and found that nine of them appeared in the historical WHOIS records of 738 email-connected domains after duplicates and those already classified as IoCs were filtered out.

A Threat Intelligence API query for the 738 email-connected domains showed two were already dubbed malicious. The domain gfqfoqz[.]cn, for instance, was associated with malware distribution.

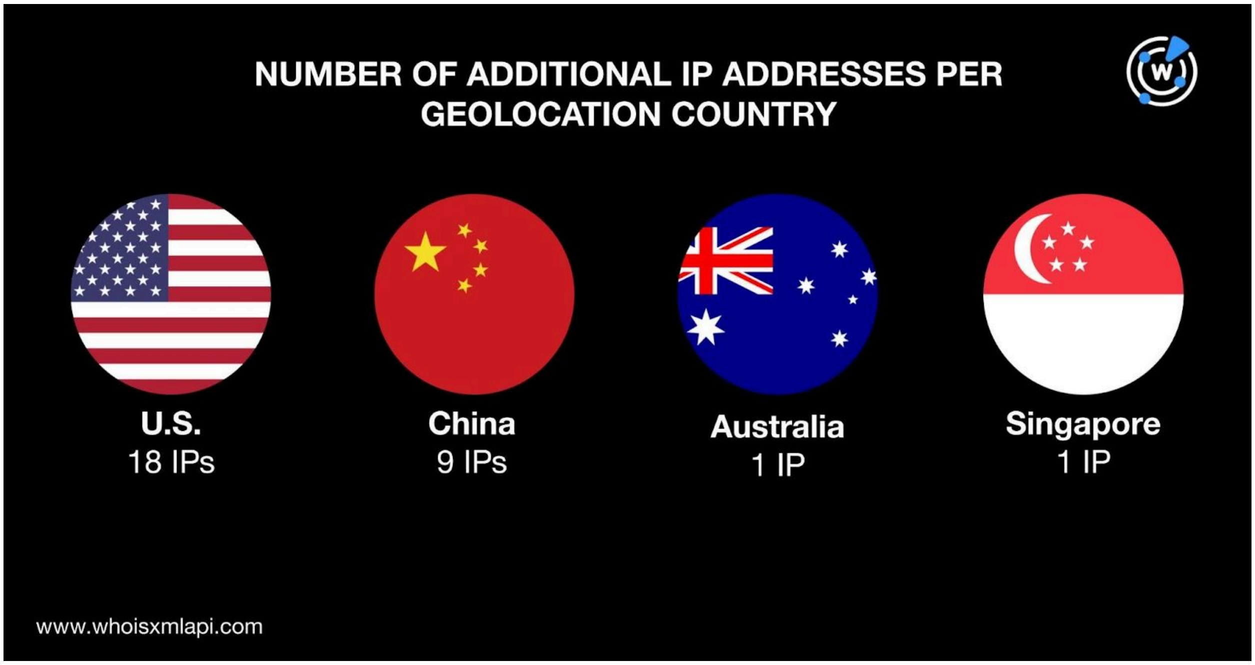
We then queried the 46 domains classified as IoCs on DNS Lookup API and found that 25 of them actively resolved to 29 IP addresses after duplicates and those already identified as IoCs were filtered out.

A Threat Intelligence API query for the 29 additional IP addresses showed that 17 have already figured in malicious campaigns. Take a look at five examples below.

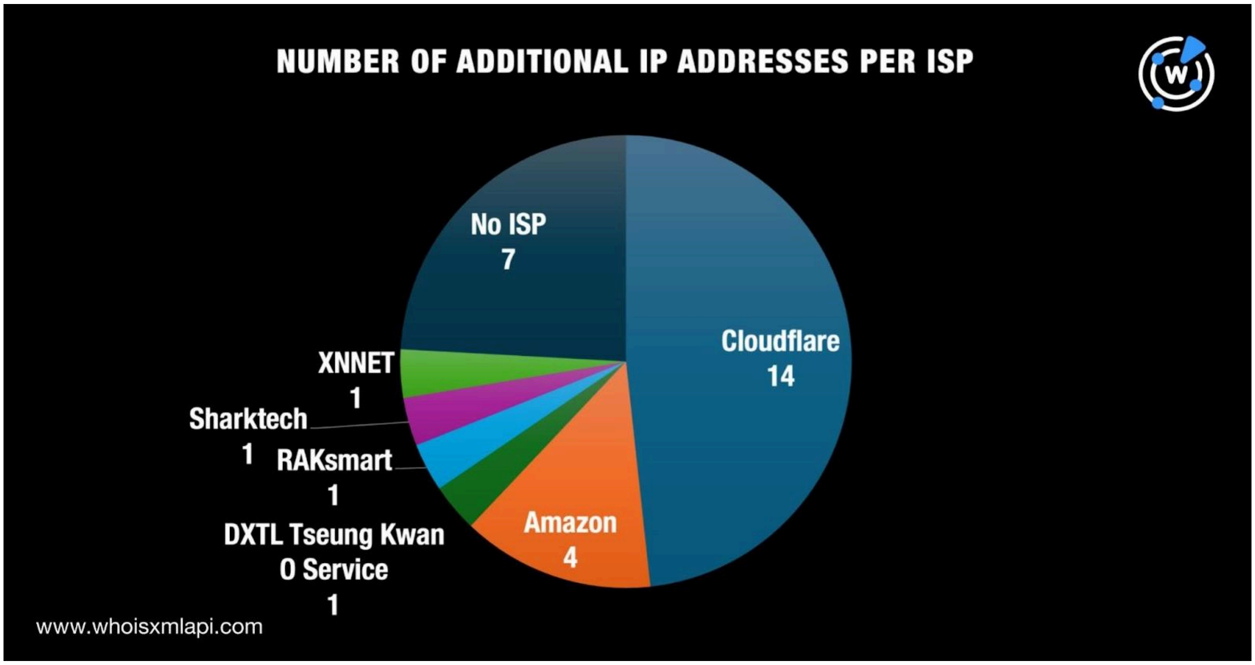
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]12[.]109	Malware distribution Phishing
104[.]21[.]48[.]1	Attack Command and control (C&C) Generic threat Malware distribution Phishing Suspicious activity
104[.]21[.]80[.]1	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
13[.]248[.]169[.]48	Attack C&C Generic threat Malware distribution Phishing Suspicious activity
172[.]67[.]161[.]31	Attack Malware distribution Suspicious activity

Next, a Bulk IP Geolocation Lookup query for the 29 additional IP addresses showed that:

- They were geolocated in four different countries led by the U.S., which accounted for 18 IP addresses. Nine IP addresses were geolocated in China while one each was geolocated in Australia and Singapore.



- Only 22 of them had ISP information. Specifically, Cloudflare administered 14 IP addresses; Amazon handled four; and DXTL Tseung Kwan O Service, RAKsmart, Sharktech, and XNNET managed one each.



We now had a total of 34 IP addresses (i.e., five tagged as IoCs and 29 additional) for further investigation. A Reverse IP API query for them revealed that 33 had current domain resolutions. It also showed that 14 could be dedicated hosts. Altogether, the 14 possibly dedicated IP addresses hosted 335 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

To round up our analysis, we scoured the DNS for domains containing the exact text strings found in those already classified as IoCs. We identified 43 unique strings from the 46 domains identified as IoCs. We checked if the 43 strings from the IoCs were found in other domains via Domains & Subdomains Discovery. Our searches revealed that only these 19 strings appeared in other domains:

- 668823.
- 668th.
- 798love.
- 89vq.
- aafd.
- bet277.
- chem-db.
- cloudflare.
- coronavg99.
- dk8.
- googlecache.
- googleseo.
- ntxx.
- ruicaisiwang.
- s995.
- tz123.
- xxxx.
- zavinac.
- zmdesf.

We uncovered 1,184 string-connected domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out.

A Threat Intelligence API query for the 1,184 string-connected domains showed that nine of them have already been weaponized for various campaigns. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREATS
cloudflare[.]agency	Malware distribution
cloudflare[.]news	Malware distribution
cloudflare[.]site	Malware distribution
dk8[.]io	Generic threat
xxxx[.]claims	Attack

—

Our BadIIS DNS deep dive led to the discovery of 2,286 potentially connected artifacts in all comprising 738 email-connected domains, 29 additional IP addresses, 335 IP-connected domains, and 1,184 string-connected domains. Security teams may wish to pay special attention to 28 of these artifacts since they have already been tagged as malicious to date.

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

- 028cdtravel[.]com
- 0513fuke[.]com
- 0530dh[.]cn
- abbcar[.]com
- adaboost[.]cn
- adjg[.]cn
- baiyi[.]net[.]cn
- banjiudz[.]cn
- basbo[.]cn
- caredowncool[.]com
- cazzg[.]com
- cdyhjc[.]cn
- dagteam[.]cn
- daludaozhusu[.]com
- darunship[.]com
- eaglabs[.]com[.]cn
- eapgfpp[.]cn
- eastypos[.]com
- fangbangshou[.]com
- fangyuanbao[.]com
- fbejclb[.]cn
- gangba[.]net[.]cn
- gaomiwl[.]com
- gesil[.]cn
- h5win[.]cn
- hairbypaabo[.]com
- hairongee[.]com
- i1[.]org[.]cn
- idh87[.]cn
- iewto[.]cn
- j28n3i[.]cn
- jakgnyy[.]cn
- janovic[.]net
- kaiwolaobao[.]com
- kikqlsc[.]cn
- kljmzz[.]com
- l05k1b[.]cn
- l2i09f[.]cn
- lagougou[.]cn
- machaoa[.]cn
- machenshu[.]com
- mahoganymaster[.]com
- n530qd[.]cn
- nantongfilm[.]com
- nao[.]cloud
- o5w69i[.]cn
- ogc168[.]com
- okhlzzo[.]cn
- p2s96a[.]cn
- p88z[.]cn
- paigevr[.]cn
- q700[.]cn
- qddyl[.]cn
- qdfuyong[.]cn
- r601tk[.]cn
- rahwctm[.]cn
- rbzsw[.]cn
- sangally-decor[.]com
- sasp[.]cn
- sc3rx[.]cn
- taoyeba[.]com
- tc521[.]cn
- teamcorp[.]net
- u2r84m[.]cn
- u9x53q[.]cn
- ucbag[.]com
- vcity[.]ink
- viuvxni[.]cn
- vrtrid[.]cn
- wanshangtui[.]cn
- way88[.]cn
- weiweixinniang[.]com[.]cn

- xatcsf[.]cn
- xccy88[.]cn
- xfomstp[.]cn
- yagsolar[.]com
- yajfdc[.]com
- yaozhuanche[.]cn
- zahady[.]net
- zanjiadedian[.]com
- zb110[.]net

Sample Additional IP Addresses

- 104[.]21[.]112[.]1
- 104[.]21[.]12[.]109
- 104[.]21[.]16[.]1
- 208[.]98[.]43[.]131
- 45[.]120[.]80[.]20
- 45[.]194[.]164[.]123
- 54[.]153[.]216[.]130
- 62[.]192[.]190[.]28
- 62[.]192[.]190[.]36
- 62[.]192[.]190[.]50
- 75[.]2[.]18[.]233
- 76[.]223[.]54[.]146

Sample IP-Connected Domains

- 0710wzxc[.]com
- 123phone[.]cn
- 7hbao[.]com
- aiietae[.]com
- b-tysports[.]com
- boomshakal[.]com
- cdn[.]xxxx[.]com
- cdpfjtzwhcmyxgs[.]gdtqyz[.]com
- cotnjyplvaer[.]top
- dakgw[.]com
- dtglttopxpf[.]top
- dvafw[.]com
- ec2-54-153-216-130[.]ap-southeast-2[.]compute[.]amazonaws[.]com
- efhqjrvgzvks[.]top
- frdslolnkfgd[.]top
- ftp[.]aiietae[.]com
- ftp[.]boomshakal[.]com
- gcdzsstqqcxsyxgs[.]7hbao[.]com
- gdtqyz[.]com
- guoba18[.]com
- hcyguanjia[.]cn
- hfqhhzpxsyxgsmcl[.]7hbao[.]com
- hjskeyb[.]com
- i45sjzphysyxgs[.]0710wzxc[.]com
- in42bby43[.]com
- jav[.]xxxx[.]com
- kc7xmdfcgypyxgs[.]0710wzxc[.]com
- kknwmvtupohx[.]top
- lemeseesee[.]com
- lesoursduscorff[.]com
- lkpingan[.]cn
- mail[.]aiietae[.]com
- mail[.]boomshakal[.]com
- mail[.]brcknkblue[.]com
- nhipw[.]com
- nmgkzyhbkjyxgs34w[.]0710wzxc[.]com
- nvyo[.]cn
- officeyes[.]com[.]cn
- pop[.]aiietae[.]com
- pop[.]boomshakal[.]com
- pop[.]brcknkblue[.]com
- qhxyqwlkjyxzrgsgwn[.]7hbao[.]com
- qiande2020[.]com
- qkjxn[.]com
- ryhljyyyxgsttr[.]7hbao[.]com
- s10[.]xxxx[.]com

- scuxyihevsve[.]top
- seeyouiis8[.]com
- test[.]xxxx[.]xxxx[.]com
- uymxv[.]com
- video-mobil[.]com
- w411w87uz7n[.]top
- webdisk[.]aiietae[.]com
- webdisk[.]boomshakal[.]com
- xayjwhcmyxgsfbk[.]zjhee[.]com
- y8jzxszrbllsyxgs[.]zjhee[.]com
- yksjlgcyxgs4xa[.]7hbao[.]com
- z02gzshmxjdfwyxgs[.]gdtqyz[.]com
- zjhee[.]com

Sample String-Connected Domains

- 668823[.]cc
- 668823[.]club
- 668823[.]cn
- 668th[.]cn
- 798love[.]top
- 798love[.]xyz
- 89vq[.]aquila[.]it
- 89vq[.]buzz
- 89vq[.]cn
- aafd[.]arab
- aafd[.]asia
- aafd[.]bid
- bet277[.]cc
- bet277[.]cn
- bet277[.]co
- chem-db[.]net
- chem-db[.]online
- cloudflare[.]ac[.]be
- cloudflare[.]academy
- cloudflare[.]ad
- coronavg99[.]club
- coronavg99[.]cyou
- coronavg99[.]icu
- dk8[.]ac
- dk8[.]academy
- dk8[.]agency
- googlecache[.]com
- googlecache[.]lol
- googlecache[.]nl
- googleseo[.]ac[.]cn
- googleseo[.]ae
- googleseo[.]agency
- ntxx[.]bid
- ntxx[.]biz
- ntxx[.]cc
- ruicaisiwang[.]cn
- s995[.]cc
- s995[.]cn
- s995[.]com
- tz123[.]cc
- tz123[.]cn
- tz123[.]com
- xxxx[.]ac[.]cn
- xxxx[.]actor
- xxxx[.]adult
- zavinac[.]cloud
- zavinac[.]com
- zavinac[.]cz
- zmdesf[.]com
- zmdesf[.]icu