Phishing Group Found Abusing .top Domains

Table of Contents

Executive Report

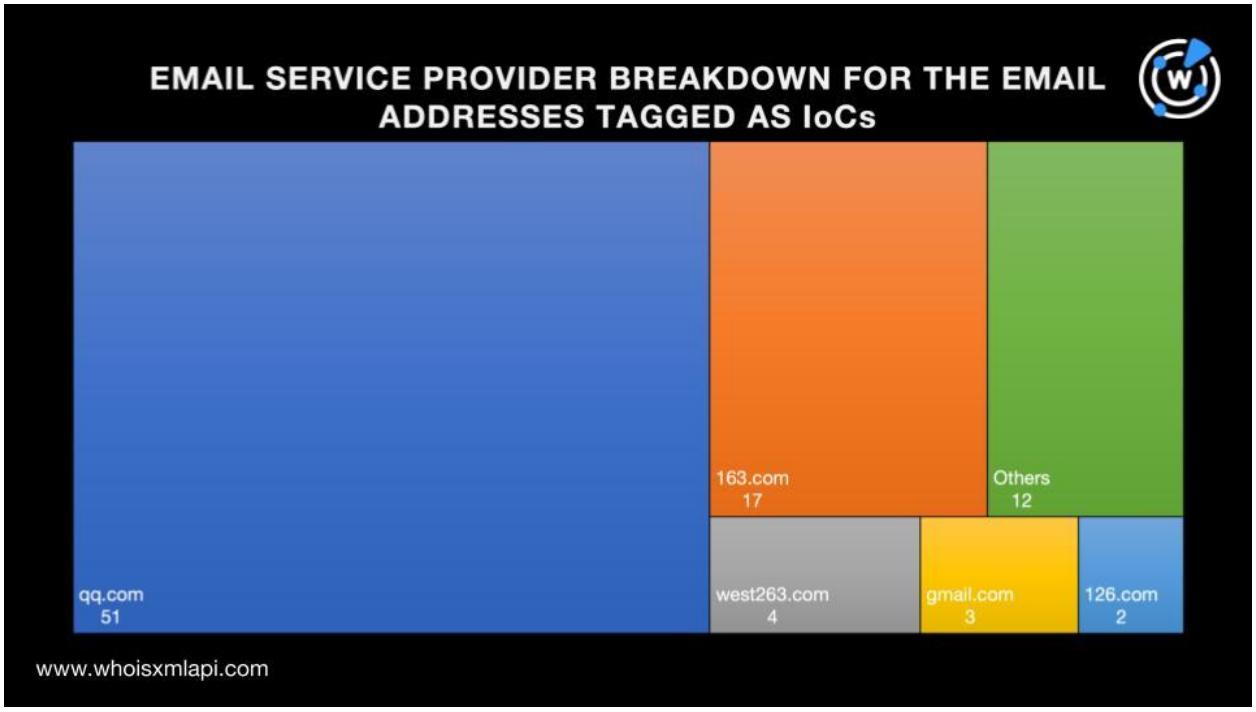
Threat researcher Dancho Danchev recently discovered a phishing operation that seemed to be abusing .top domains for which he collated 89 email addresses that served as indicators of compromise (IoCs). To amass more information and other potentially connected web properties, the WhoisXML API research team took a DNS deep dive that led to the discovery of:

- 4,284 domains that were registered using the email addresses identified as IoCs
- 71 IP addresses that played host to the email-connected domains, two of which turned out to be malicious based on malware checks
- 890 domains hosted on the same IP addresses as the email-connected domains

Facts about the IoCs

We began our analysis by looking closer into the 89 email addresses Danchev identified as IoCs and found that:

- Only 10 of them weren't used to register any domain recently.
- A majority of the email addresses, 51 to be exact, were created via the qq[.]com service. 163[.]com (17), west263[.]com (4), gmail[.]com (3), and 126[.]com (2) rounded out the top 5 email services. The remaining 12 email addresses were spread across 12 different service providers—abc[.]com, domainmanager[.]top, foxmail[.]com, hxmail[.]com, lamartina[.]info, live[.]cn, seobuzz[.]it, sina[.]cn, sina[.]com, somcom[.]com, we[.]top, and yeah[.]net. The chart below shows the email address volume breakdown per service provider.

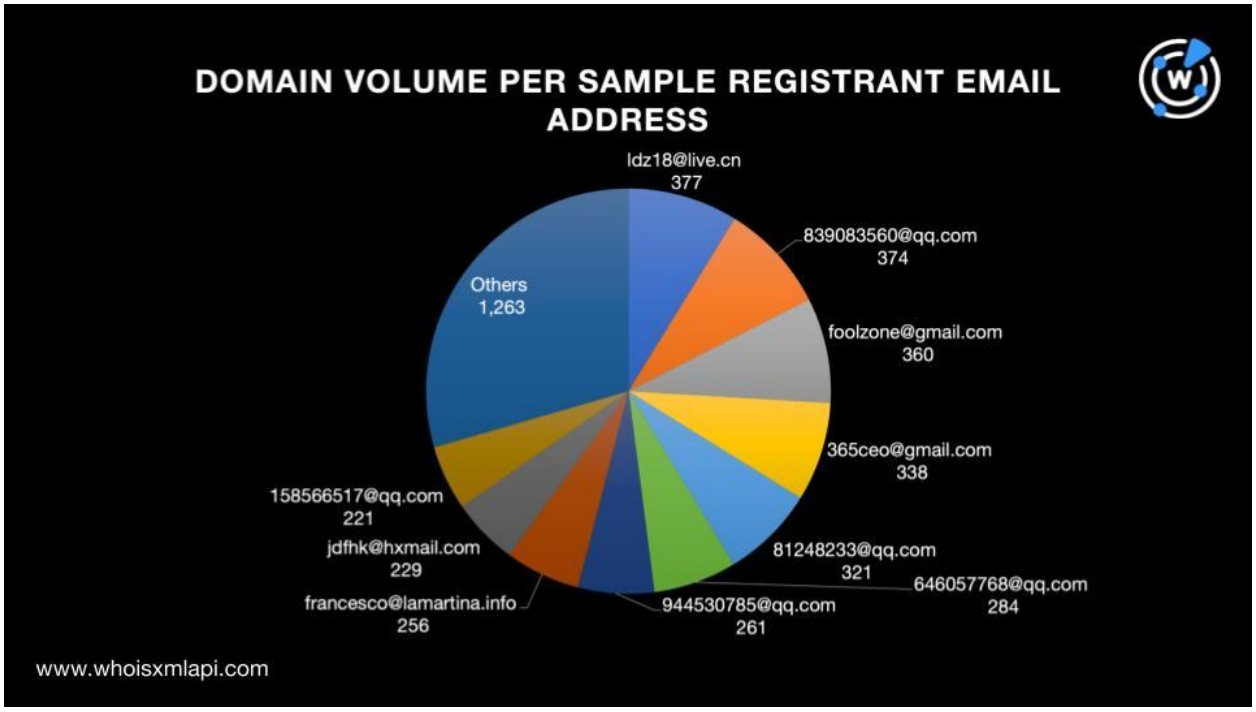


- Each of the 79 email addresses were used to register between one and more than 10,000 domains recently. Altogether, they served as registrant email addresses to 172,654 domains.

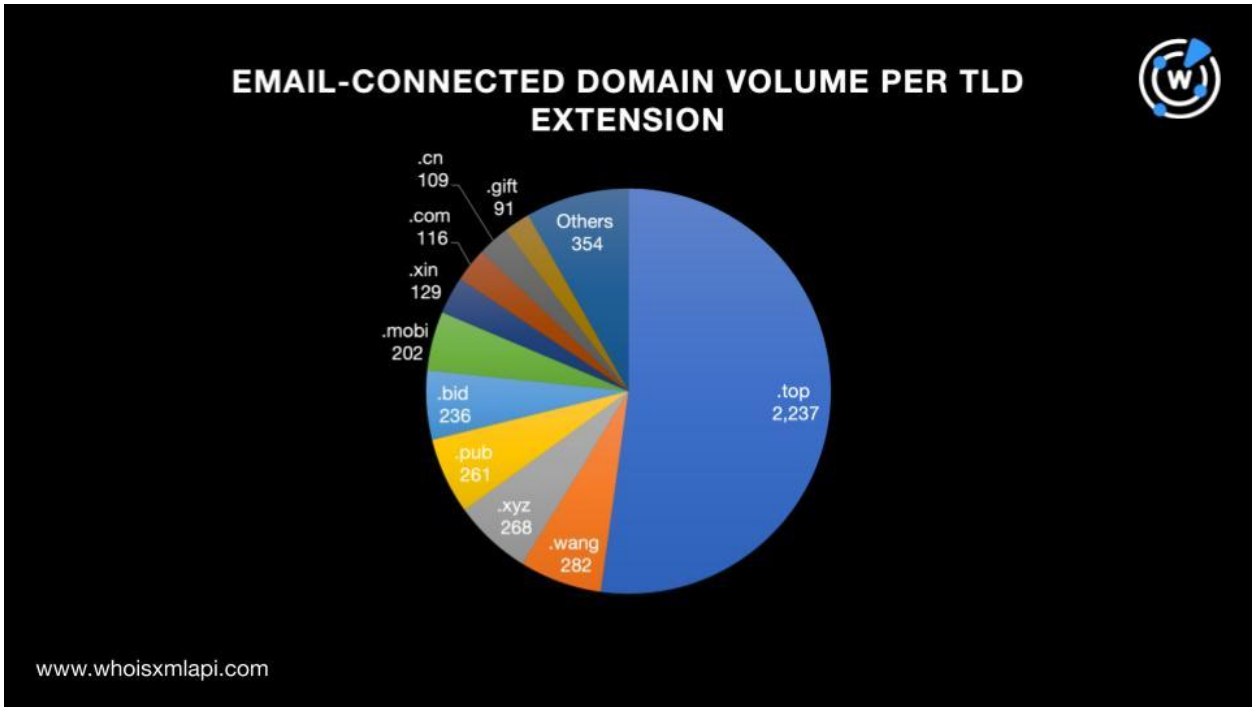
IoC-Related DNS Findings

To begin our hunt for unreported possible connections, we first needed to limit the scope of this study.

We ran reverse WHOIS searches on the 79 email addresses identified as IoCs. We then chose to focus only on those that served as registrant email addresses to 500 or fewer domains registered recently. That left us with a sample of 35 email addresses that were used to register 4,284 potentially connected domains in total. Take a look at the number of domains registered using each email address in the chart below.



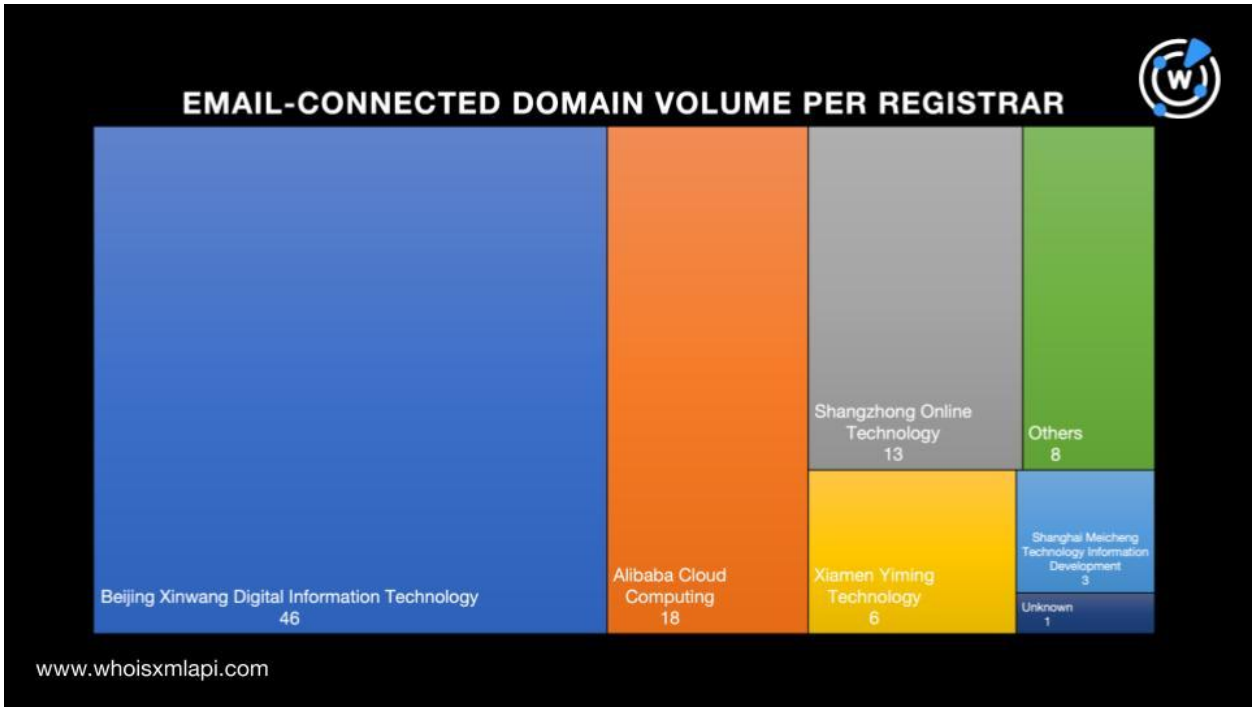
Further scrutiny of the 4,284 domains showed that a majority of them, 2,237 to be exact, sported the .top top-level domain (TLD) extension as Danchev pointed out. The .wang (282), .xyz (268), .pub (261), .bid (236), .mobi (202), .xin (129), .com (116), .cn (109), and .gift (91) TLD extensions completed the top 10. The remaining 354 domains were spread across 27 other TLD extensions. The number of domains per TLD extension is shown in the chart below.



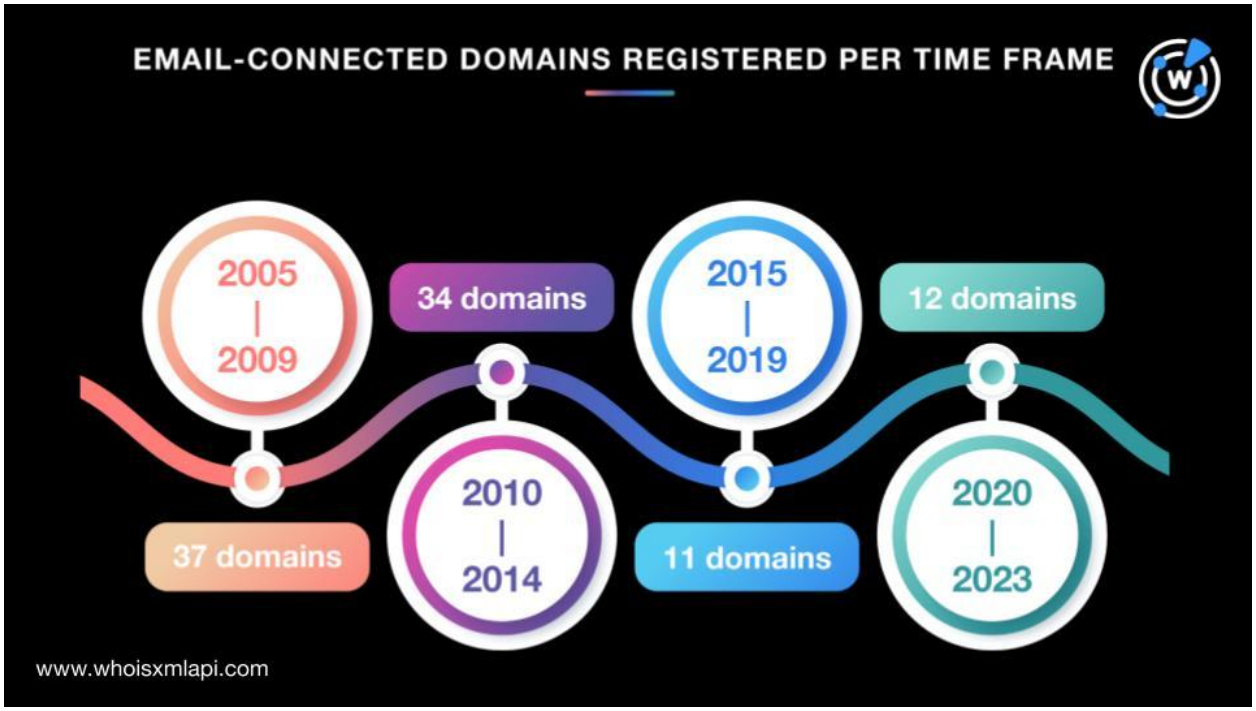
We can thus infer that the phishers mostly favored using domains under gTLD extensions, specifically .top, based on the top 10 list above. That, however, didn't mean they didn't weaponize domains sporting ccTLD extensions, as evidenced by the inclusion of .cn in the top 10, as well.

A bulk WHOIS lookup for the 4,284 email-connected domains revealed that:

- Only 95 had currently active WHOIS records.
- A majority of them, 46 to be exact, were registered with Beijing Xinwang Digital Information Technology. Alibaba Cloud Computing (18), Shangzhong Online Technology (13), Xiamen Yiming Technology (6), and Shanghai Meicheng Technology Information Development (3) completed the top 5 registrars. Eight domains were scattered across eight other registrars while one didn't have publicly available registrar data. The number of domains per registrar is shown in the chart below.



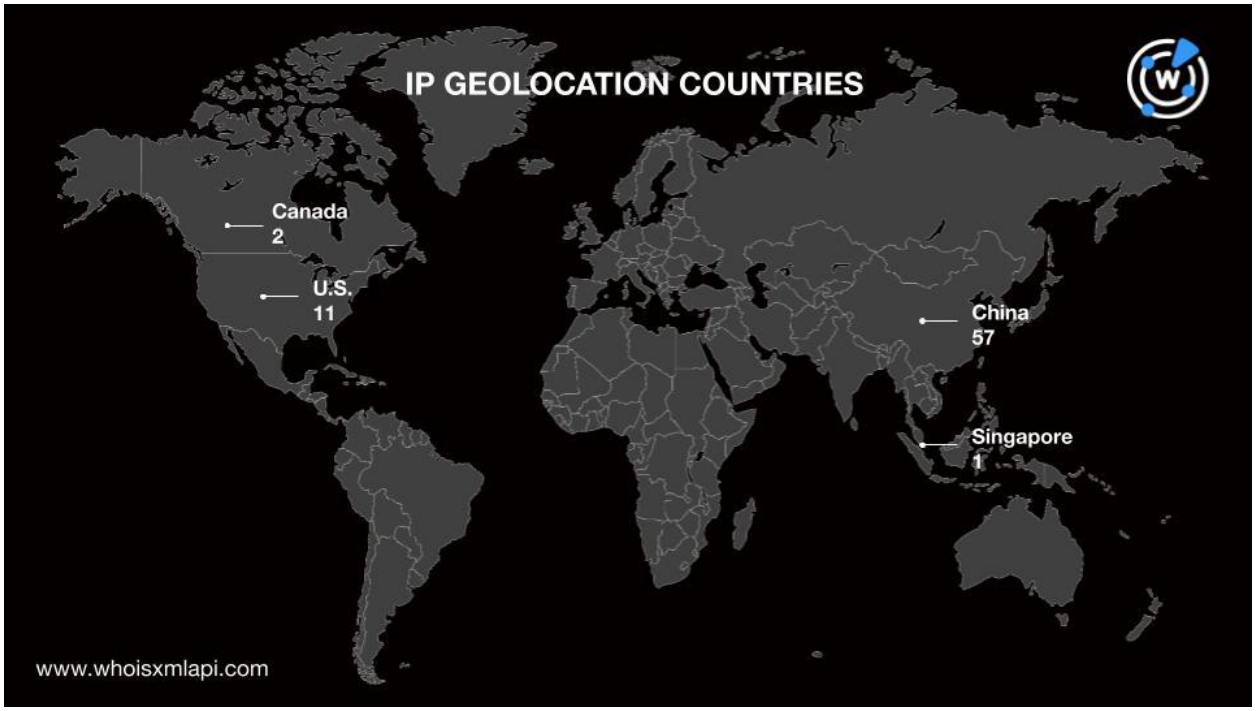
- The highest number of email-connected domains with retrievable WHOIS records, 14 to be exact, were registered in 2021. One didn't have a publicly viewable creation date. Take a look at the domain breakdown by creation period below.



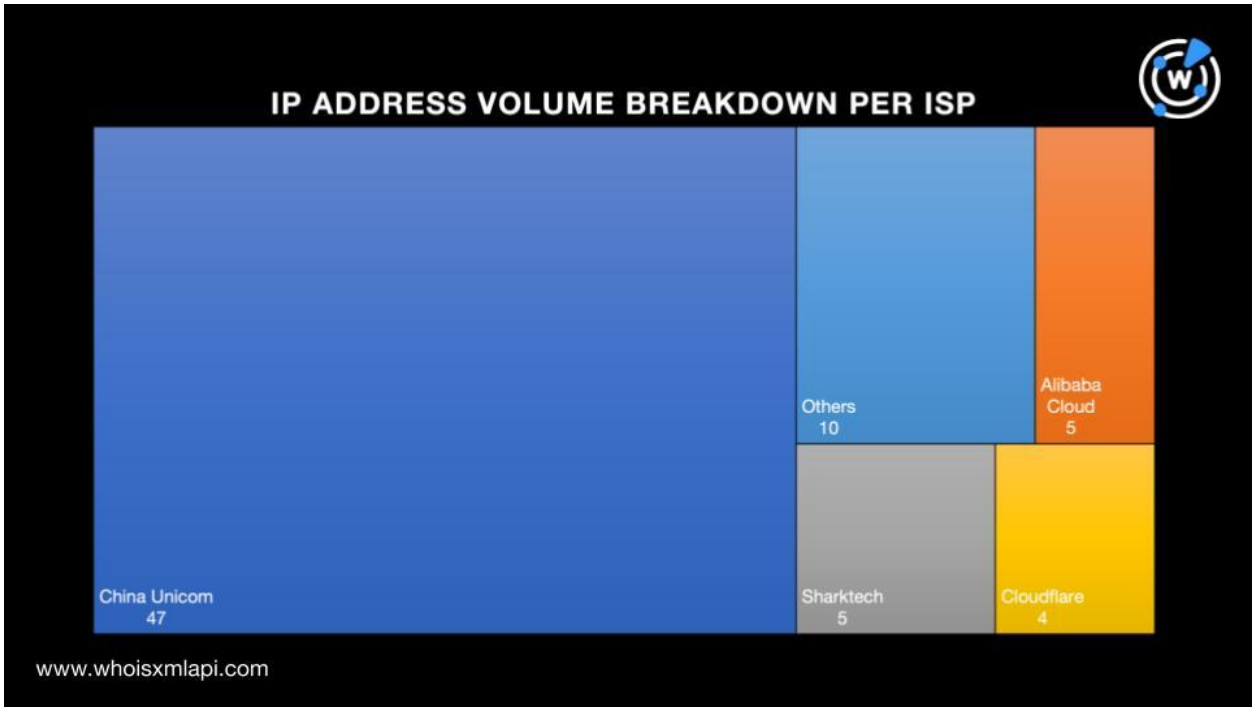
- Only one domain—cnlegaldata[.]com—had a visible registrant country—the U.S.

Next, we subjected the 4,284 email-connected domains to DNS lookups, which revealed that:

- Only 99 of the domains currently resolve to IP addresses.
- They resolved to 71 unique IP addresses, two of which turned out to be malicious based on malware checks.
- A majority of the IP addresses, 57 to be exact, were geolocated in China. The remaining 14 were spread across three other countries—the U.S. (11), Canada (2), and Singapore (1). The chart below sums up our findings.



- China Unicom was the top Internet service provider (ISP), accounting for 47 of the IP addresses. Alibaba Cloud and Sharktech (5 each) and Cloudflare (4) rounded out the top 3 ISPs. The remaining 10 unique IP addresses were distributed among eight other ISPs—Hangzhou Alibaba Advertising and Tencent (2 each) and Zenlayer, China Telecom, Cloudie, Confluence Networks, Hong Kong Communications International, and UCloud Information Technology (HK) (1 each). The chart below shows the number of IP addresses per ISP.



Additional open-source intelligence (OSINT) research on the IP addresses found that one—208[.]91[.]197[.]46—was reported on AbuseIPDB five times as of this writing.

As a final step, we ran reverse IP lookups for the 71 IP addresses in search of IP-connected domains and found that:

- Sixty-six of the IP addresses continued to host domains to date.
- Fifty-seven of them were seemingly dedicated hosts.
- Altogether, the 57 seemingly dedicated IP addresses hosted 890 domains.

While none of the IP-connected domains were dubbed malicious, at least two may be suspicious. Asicskids[.]com and tomfordeyewear[.]com, which bear popular fashion brand names, couldn't be publicly attributed to ASICS and Tom Ford, respectively, based on WHOIS record comparisons with the legitimate companies' official domains.

We also noticed the appearance of the string **bank** in five of the IP-connected domains. While only three seem to be mimicking legitimate banks—grandbank[.]cn, nanjingbank[.]com[.]cn, and ruifengbank[.]com—all five could be weaponized for phishing.

—

Our DNS deep dive into the phishing campaign led to the discovery of 5,245 unreported potentially connected threat artifacts, a majority of which were .top 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 and IoCs

Email Addresses Identified as IoCs

- huangagan@126.com
- 2374066280@qq.com
- 13560062@qq.com
- moocn@163.com
- 382865208@qq.com
- 944530785@qq.com
- 6095@qq.com
- 530968666@qq.com
- smith190000@gmail.com
- 394762617@qq.com
- et4009@163.com
- alibababtc@163[.]com
- jak479@163[.]com
- 523224768@qq[.]com
- 1376693555@qq[.]com
- crc1157@163[.]com
- jdfhk@hxmail[.]com
- 937670066@qq[.]com
- 2074460576@qq[.]com
- loveyou666999111@sina[.]com
- 490722322@qq[.]com
- 758151421@qq[.]com
- 127567@qq[.]com
- yanyuze88@163[.]com
- 646057768@qq[.]com
- beianyuming@yeah[.]net
- 995995588@qq[.]com
- 80150285@qq[.]com
- nczcz@foxmail[.]com
- tiejianwen@163[.]com
- kjzy888@126[.]com
- 1804088@qq[.]com
- 571360507@qq[.]com
- 505301991@qq[.]com
- bahao8899885@163[.]com
- whoisagent@163[.]com
- qiuji20159@163[.]com
- 363959985@qq[.]com
- 2560396608@qq[.]com
- 270642541@qq[.]com
- 5703686@qq[.]com
- 779595468@qq[.]com
- 808882567@qq[.]com
- 63139586@qq[.]com
- pangdada@somcom[.]com
- 278702487@qq[.]com
- qq56e8@163[.]com
- niccolo[.]turchetti@seobuzz[.]it

- 573147430@qq[.]com
- 365ceo@gmail[.]com
- chuxianla@qq[.]com
- 80178039@qq[.]com
- 695795168@qq[.]com
- 987939309@qq[.]com
- francesco@lamartina[.]info
- cyflyy@163[.]com
- 526482873@qq[.]com
- wstmds@qq[.]com
- 254857383@qq[.]com
- 2764659587@qq[.]com
- dai@west263[.]com
- halojean@163[.]com
- klcckkok@west263[.]com
- 282767694@qq[.]com
- info@domainmanager[.]top
- 359577700@qq[.]com
- 839083560@qq[.]com
- bkx856@163[.]com
- 18606717073@163[.]com
- 281647998@qq[.]com
- aaronyeah@sina[.]cn
- whoisagent@west263[.]com
- 158566517@qq[.]com
- abc@abc[.]com
- 283408164@qq[.]com
- ldz18@live[.]cn
- 1936239652@qq[.]com
- 1161160571@qq[.]com
- foolzone@gmail[.]com
- 81248233@qq[.]com
- vvdancom@qq[.]com
- mymail@west263[.]com
- ok358w@qq[.]com
- 804380879@qq[.]com
- 350771@qq[.]com
- hapgoo@163[.]com
- yumingpifa@163[.]com
- 526420409@qq[.]com

Sample Email-Connected Domains

- 19739[.]cn
- stell[.]cn
- 71511[.]cn
- pronunciation[.]vip
- powerprofits[.]vip
- allisontyler[.]vip
- cyberplanet[.]vip
- gasolineras[.]vip
- firstservice[.]vip
- rhfv[.]top
- rhfu[.]top
- tkoe[.]top
- rgyo[.]top
- rgoy[.]top
- rgog[.]top
- rgfv[.]top
- ujai[.]top
- uiur[.]top
- uiuh[.]top
- ugeo[.]top
- uiqe[.]top
- uipv[.]top
- rbvt[.]top
- swvh[.]top
- swvg[.]top
- swor[.]top
- rduk[.]top
- rdui[.]top
- rdug[.]top
- rduf[.]top
- rdud[.]top
- rduc[.]top
- rdsv[.]top
- lrgu[.]top

- lrgi[.]top
- lrfv[.]top
- rglo[.]top
- lrdi[.]top
- rgkv[.]top
- lrcu[.]top
- rgko[.]top
- lrci[.]top
- gvaj[.]top
- rgjv[.]top
- rgju[.]top
- lrbv[.]top
- lrbu[.]top
- lrbo[.]top
- lrbi[.]top
- rgiz[.]top
- rgiu[.]top
- rgir[.]top
- rgiq[.]top
- rgil[.]top
- rgik[.]top
- rgij[.]top
- lrav[.]top
- lrau[.]top
- rgie[.]top
- rgia[.]top
- rghv[.]top
- rghu[.]top
- rhxv[.]top
- rhxu[.]top
- rdiq[.]top
- rdil[.]top
- rdij[.]top
- rgau[.]top
- rfzv[.]top
- rfzu[.]top
- rfyv[.]top
- rfyo[.]top
- rfxu[.]top
- rfxo[.]top
- rfwv[.]top
- rfwo[.]top
- rfvz[.]top
- rfvy[.]top
- rfvt[.]top
- rfvq[.]top
- rfvo[.]top
- rfuo[.]top
- rful[.]top
- rfuj[.]top
- rfui[.]top
- rfug[.]top
- rfuf[.]top
- rfue[.]top
- rfud[.]top
- rfuc[.]top
- rfua[.]top
- rfsv[.]top
- rfru[.]top
- rfro[.]top
- rhkv[.]top
- lqmo[.]top
- rfqu[.]top
- rhko[.]top
- rfqo[.]top
- rhjv[.]top

Sample IP Addresses

- 170[.]106[.]62[.]189
- 170[.]33[.]13[.]246
- 60[.]205[.]142[.]123
- 47[.]108[.]52[.]145
- 67[.]21[.]93[.]230
- 67[.]21[.]93[.]227
- 67[.]21[.]93[.]254
- 64[.]32[.]28[.]230

- 67[.]21[.]93[.]228
- 103[.]231[.]14[.]128
- 121[.]42[.]97[.]194
- 121[.]42[.]101[.]36
- 47[.]90[.]30[.]95
- 206[.]119[.]87[.]32
- 2606:4700:3033::ac43:bbab
- 2606:4700:3031::6815:5442
- 104[.]21[.]84[.]66
- 172[.]67[.]187[.]171
- 208[.]91[.]197[.]46
- 122[.]114[.]118[.]10

Sample Malicious IP Address

- 170[.]33[.]13[.]246

Sample IP-Connected Domains

- a720[.]top
- aeslock[.]com
- agivip[.]com
- ahplm[.]cn
- ai952[.]com
- aikunshiye[.]com
- airseachina[.]com
- airtac-taiwan[.]com
- airway-china[.]cn
- aisense[.]cn
- aixunfuwu[.]com
- ajhrjs[.]com
- alicdn[.]space
- aly669[.]com
- amneodrive[.]com
- anbaiqi[.]cn
- anok[.]cn
- anwo[.]net
- anyangrc[.]cn
- anywherepeople[.]com[.]cn
- aodelong[.]cn
- aoxiangrun[.]com
- apceasy-ups[.]com
- aphaoduo[.]com
- appcliaiton[.]site
- aqbcjx[.]com
- aqdq[.]com
- aqkz[.]com
- asicskids[.]com
- ayawsm[.]cn
- aydsxny[.]com
- aykj[.]site
- b6666[.]com
- bai[.]gs
- baichi[.]cc
- baidugongsi[.]cn
- baifangliang[.]com
- baijiuku[.]com
- baiqiang123[.]top
- banghang17[.]com
- bangyibang[.]cn
- bazhouwtc[.]online
- beifan[.]wang
- beileimaoedu[.]com
- benren[.]ltd
- bevismp[.]com
- bfjmjx[.]com
- bian[.]su
- bianbochina[.]com
- biaoguanwy[.]com
- bjnsti[.]com
- bjss888[.]cn
- bjyljkj[.]com
- bojueshengwu[.]com
- boluomi[.]com[.]cn
- bonuoxcl[.]com

- bosyedu[.]com
- boxman[.]cn
- browser[.]com[.]cn
- bsd56[.]com
- bswlsd56[.]com
- btpglj[.]com
- buding[.]top
- buschvacuum[.]cn
- buuxuu[.]com
- bxcjq[.]com
- c-e-m[.]com
- c6p[.]fun
- caaxaa[.]com
- cafebabe[.]link
- caii[.]cc
- cailang[.]com
- calvatis[.]com[.]cn
- capitbio[.]com
- casinovoxel[.]com
- ccinnetic[.]com
- cctss[.]cn
- ceeb32[.]top
- changgao[.]cn
- changzm[.]top
- chashaorou[.]com
- cheesekid[.]co
- chenqiwen[.]ltd
- china-price[.]cn
- china-transport[.]com
- chinacasket[.]com
- chinadaily[.]wang
- chinaforge[.]cn
- chinajiatuo[.]cn
- chinameeting[.]com[.]cn
- chinapeiyuan[.]com
- chinawood[.]org
- chinayuke[.]com[.]cn
- chinayuke[.]com
- chnc[.]cn
- chunhuadongli[.]com
- ciea[.]cn
- cjwangluo[.]cn
- ckxcp[.]com
- cnlegaldata[.]com