A DNS Examination of the Phishing Campaign Targeting Japanese Brokerage Firms

Table of Contents

Executive Report

Yahoo! News Japan reported cases where securities accounts were hijacked so cybercriminals could sell stocks without their rightful owners' permission. More than 3,500 fraudulent transactions have already been recorded from January to April 2025 alone, amounting to stock owner losses of ¥300+ billion.

A report on the tool that could have been used to phish the Japanese stock owners publicized seven domains as indicators of compromise (IoCs). We used this data, among others from various reports on similar phishing campaigns, to identify more connected artifacts and other pertinent information.

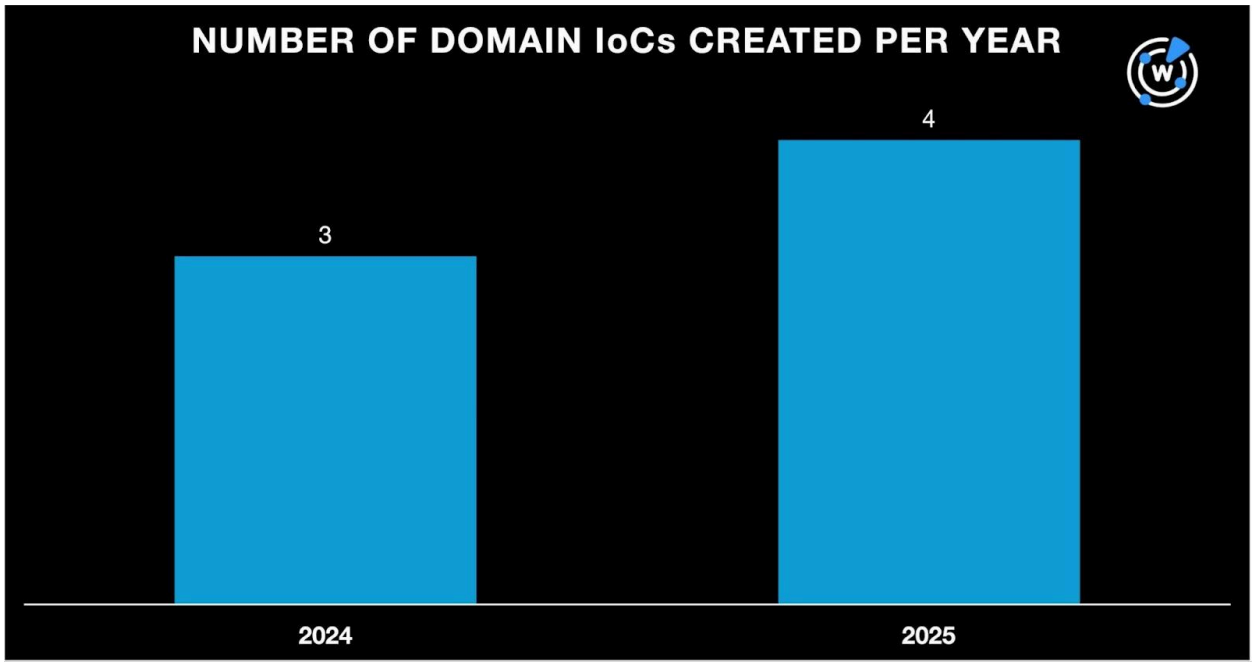
Our in-depth analysis using our expansive repositories of domain and DNS intelligence led to the discovery of:

- 36 registrant-connected domains
- 7,437 email-connected domains, 267 were malicious
- Seven string-connected domains
- 609 look-alike domains found using a similar domain algorithm covering 11 April–22 May 2025
- 47,232 look-alike domains found on First Watch covering January 2024–May 2025

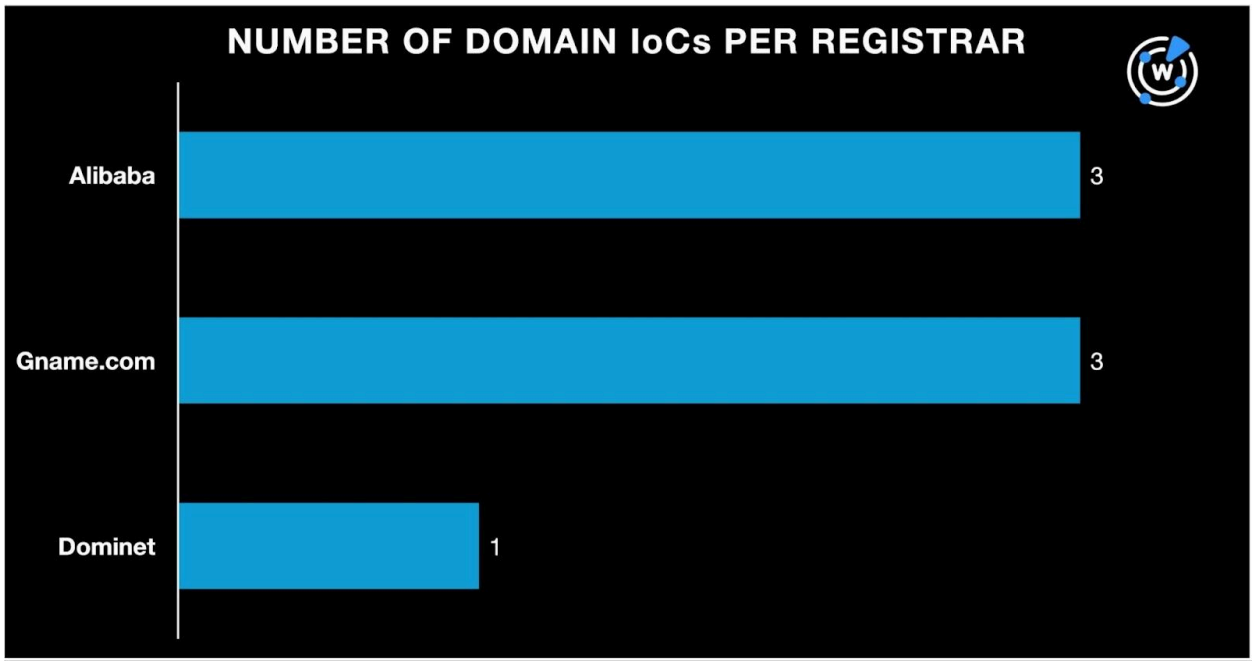
1. Searching for Phishing Kit Connections

We began our search for web properties connected to the phishing kit by querying the seven domains earlier identified as IoCs on Bulk WHOIS API, which revealed that:

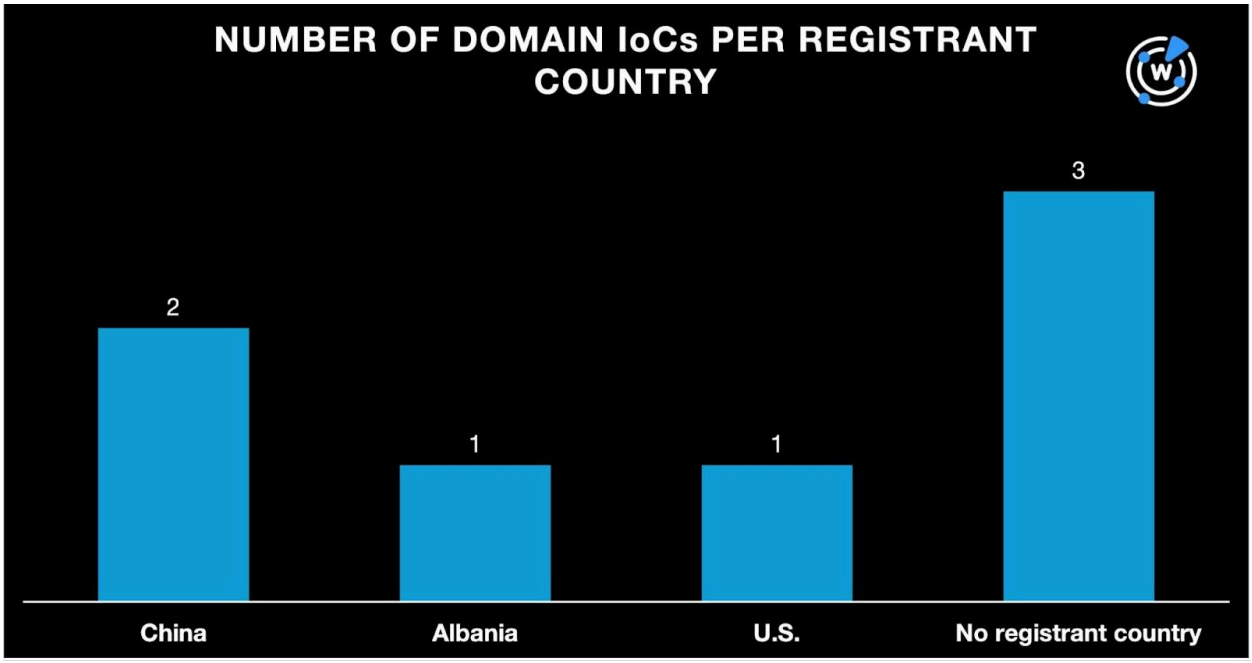
- They were created between 2024 and 2025, making them all relatively newly registered when they were weaponized for attacks.



- They were administered by three registrars led by Alibaba and Gname.com, which accounted for three domains each.



- While three of them did not have registrant countries on record, the remaining four domains were registered in three countries—two in China and one each in Albania and the U.S.



We then queried the seven domains identified as IoCs on DNS Chronicle API and found that four of them had 198 domain-to-IP resolutions over time. The domain evrryday[.]com posted 166 resolutions since 28 April 2017.

Next, we took a closer look at the current WHOIS records of the seven domains identified as IoCs and discovered that two—uhlkg[.]cn and zjkso[.]cn—had the same registrant name. Using this data point as a search term for Reverse WHOIS API, we uncovered 36 registrant-connected domains after filtering out duplicates and those already tagged as IoCs.

After that, we queried the seven domains identified as IoCs on WHOIS History API, which showed that three had email addresses in their historical WHOIS records. We unearthed 10 email addresses in all and upon further scrutiny determined that six were public email addresses.

We queried the six public email addresses on Reverse WHOIS API and discovered that five appeared in the historical WHOIS records of 7,437 email-connected domains. While the remaining public email address also had connections, it could belong to a domainer since it had more than 10,000 connected domains.

A Threat Intelligence API query for the 7,437 email-connected domains revealed that 267 have already figured in various attacks. Take a look at five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREATS
015441[.]cn	Phishing
abivh[.]cn	Phishing
b1wiv[.]cn	Phishing
c4ujvs0b[.]cn	Phishing
dcvlp[.]cn	Phishing

Next, we looked more closely at the seven domains identified as IoCs and determined that they started with seven unique text strings. Only four of the strings, however, appeared in other domains based on our Domains & Subdomains Discovery searches. See the list below.

- etcady.
- evrryday.
- uhlkg.
- zjkso.

Specifically, we uncovered seven string-connected domains.

All in all, we unearthed 7,480 connected domains, 267 of which have already been weaponized for attacks.

2. Searching for Phishing Email Connections

As the next step of this research, we obtained 10 phishing emails possibly related to the same fraud campaign and identified the following 10 email domains that we then analyzed:

- cyoa[.]com
- fsqyqq[.]com
- hzlgx[.]com
- icxw[.]com
- nasture[.]de
- pisw[.]com
- shoken_nikko[.]cn
- tmjs[.]net
- unwwxlf[.]com
- zxno[.]com

Here is a sample phishing email from an email address with the domain tmjs[.]net we received on 19 May 2025.


[redacted]【設定必須】デバイス認証・FIDO認証のご案内（期限：5/31）

SBI証券 認証 <Sbi.aeieindveldcont@tmjs.net>

詳細　2025年05月19日 19:52　返信

認証: このメールの認証情報

宛先：[redacted]

タグ：

【重要】2025年5月31日より認証方式が義務化されます

平素よりSBI証券をご利用いただき誠にありがとうございます。

当社ではお客様の資産と取引の安全性を確保するため、**2025年5月31日（土）以降、ログイン時の多要素認証（デバイス認証・FIDO認証）を義務化**いたします。

現在のご利用環境に関係なく、すべてのお客様に設定をお願いしております。
早期にご対応いただくことで、切替時の混乱を避け、スムーズにサービスをご利用いただけます。

※ 期限を過ぎた場合、ログイン・出金・注文など一部機能がご利用いただけなくなる可能性がございます。

特にスマートフォンからのご利用や、平日・営業時間中のお取引を予定されているお客様は、
余裕をもって事前にご対応くださいますようお願い申し上げます。

■ 設定期限

2025年5月31日（土） 23:59まで

■ 設定はこちら

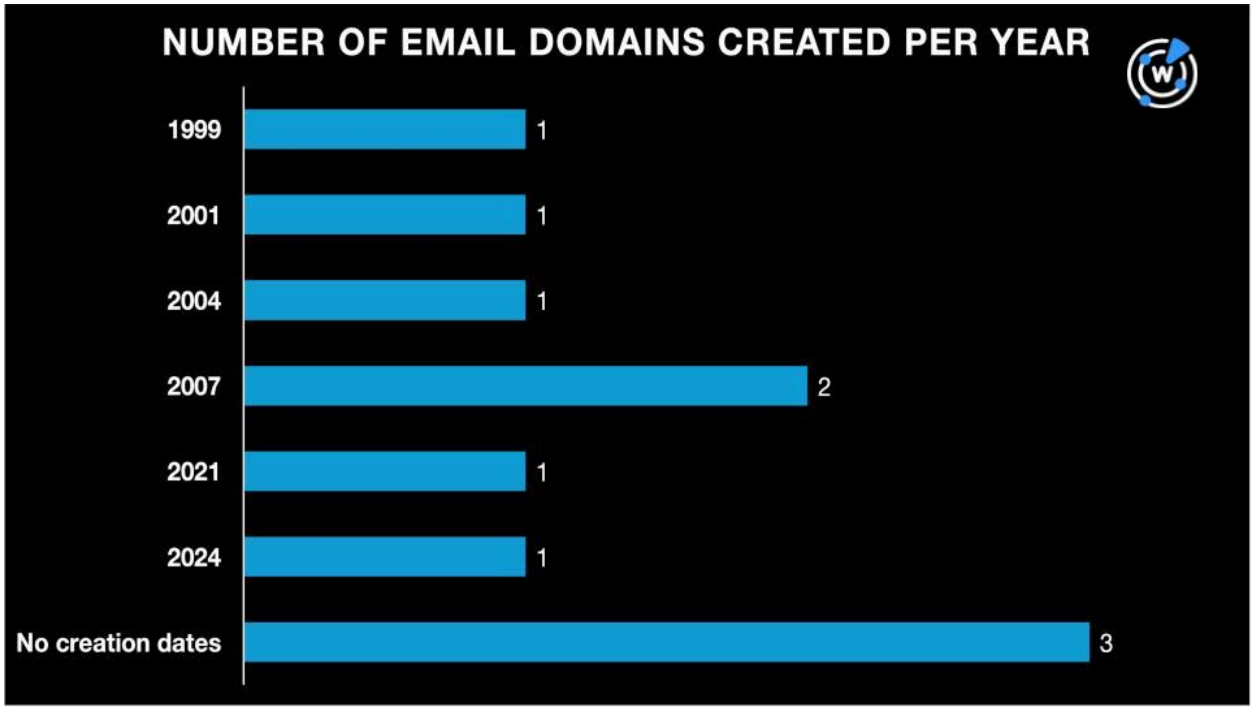
メールアドレス登録および認証方式設定ページへ進む

本通知はSBI証券のシステムより自動送信されています。
ご不明な点は、当社サポート窓口またはヘルプページをご確認ください。

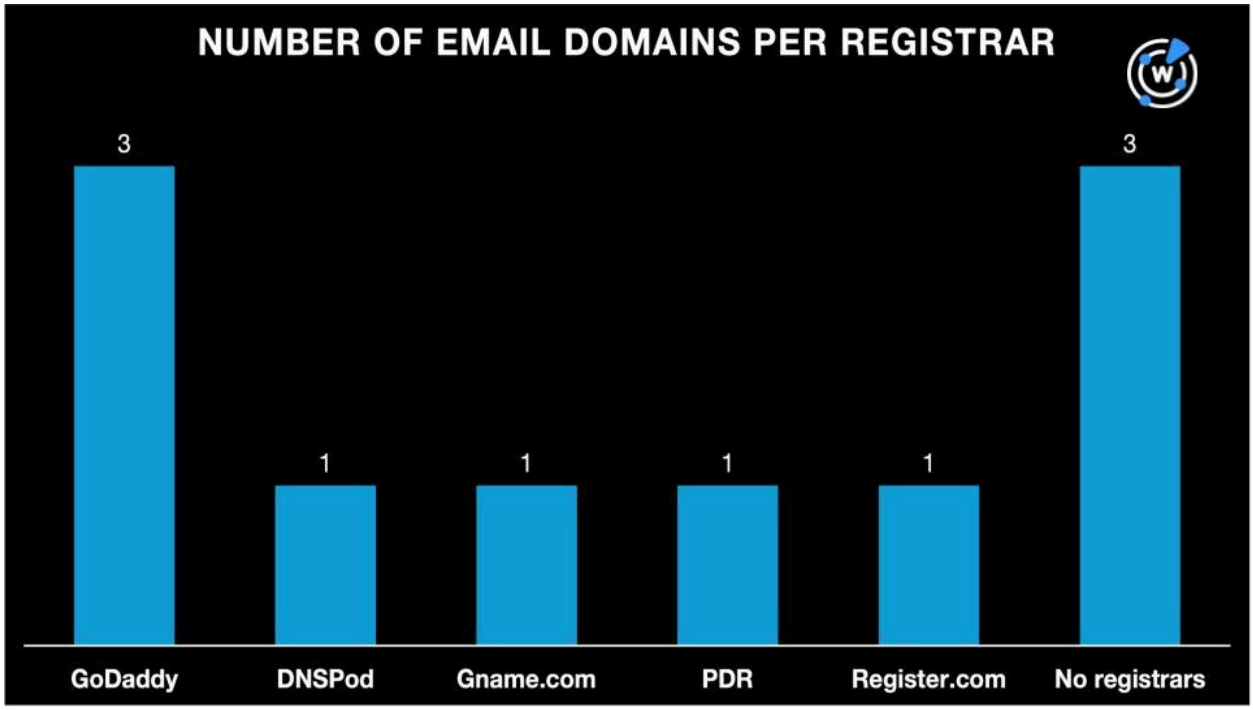
発行元：SBI証券株式会社
〒106-6019 東京都港区六本木1-6-1 泉ガーデンタワー
Copyright © SBI SECURITIES Co., Ltd. All Rights Reserved.

We started by querying the 10 email domains on Bulk WHOIS API and found that:

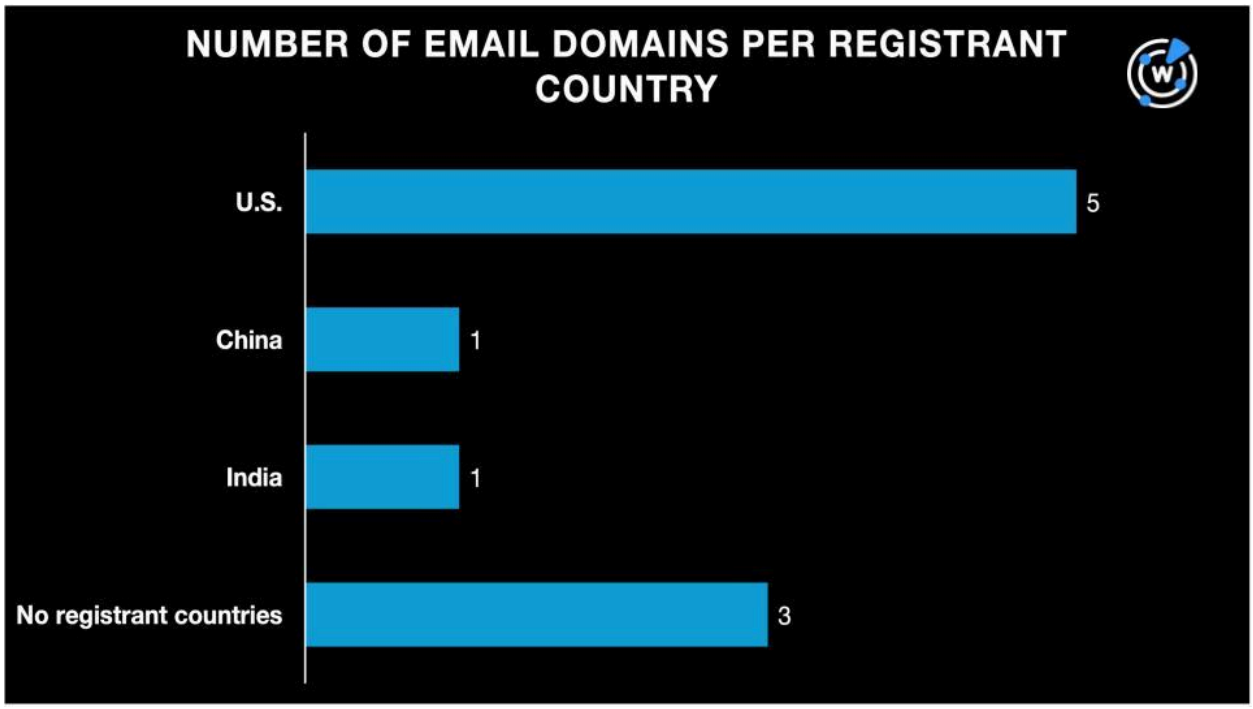
- They were created between 1999 and 2024, inferring that the fraudsters did not discriminate in terms of domain age. Three of the domains did not have creation dates in their current WHOIS records.



- They were administered by five registrars led by GoDaddy, which accounted for three domains. One domain each was administered by DNSPod, Gname.com, PDR, and Register.com. The three remaining domains did not have registrars on record.



- They were registered in three countries topped by the U.S., which accounted for five domains. One domain each was registered in China and India, while three did not have registrant countries on record.



We also analyzed various phishing reports from the Council of Anti-Phishing Japan that contained 44 masked phishing URLs that we looked further into. These were:

- https[:]//****[.]bond/****[.]php
- https[:]//****[.]cyou/****[.]php
- https[:]//****[.]nikkosmbc[.]co[.]jp/****
- https[:]//****[.]tp****[.]com/login/?token=****
- https[:]//acquaaintanceshi[.]hv****[.]com/
- https[:]//biotransformatio[.]bg****[.]com/
- https[:]//chemiluminescenc[.]tq****[.]com/
- https[:]//cs[.]mufg[.]p****[.]sbs/login
- https[:]//dsgr****[.]com/rakuten
- https[:]//fgjfuz****[.]com/
- https[:]//jx****[.]com/
- https[:]//kmm****[.]com/
- https[:]//mehhkapradwwoesi[.]s****[.]com/
- https[:]//mu****[.]cn/rakusec
- https[:]//nomura-****[.]sbs/infojp
- https[:]//nomuragl****[.]sbs/infojp
- https[:]//offeepotech****[.]gc****[.]com/
- https[:]//oingc****[.]com/
- https[:]//pmm****[.]com/
- https[:]//pnasoa****[.]net/
- https[:]//reqi****[.]cn/rakusec
- https[:]//sb-auth****[.]cloud/sup
- https[:]//sbiisec****[.]com/

- https[:]//sbisec-sapony[.]z****[.]com/ETGate/loge/
- https[:]//sdeb****[.]com/
- https[:]//sec-sbi****[.]com/
- https[:]//secure-authen-****[.]club/autolg
- https[:]//sho****[.]com/
- https[:]//sim****[.]com/
- https[:]//szlot****[.]com/
- https[:]//tac****[.]com/
- https[:]//ttd[.]com/95X@pnasoa****[.]net#zemwg
- https[:]//turav****[.]com/web/
- https[:]//ukeiedehuazhuoe[.]a****[.]com/
- https[:]//vasoconstrictio[.]yuleche****[.]com/
- https[:]//wha****[.]top/ufjoeui
- https[:]//wo****[.]com/
- https[:]//www[.]columnistof****[.]com/member/
- https[:]//www[.]duix****[.]com/
- https[:]//www[.]sbl****[.]com/
- https[:]//www[.]tv****[.]cn/
- https[:]//xeroththaamiahl[.]06****[.]com/
- https[:]//yc****[.]com/
- https[:]//zhuanxiuderuuir[.]ki****[.]com/

We used the domains we extracted from the 44 masked URLs above as search terms on First Watch Malicious Domains Data Feed. We discovered 20 domains containing the strings **sb-auth****.cloud**, **sbiisec****.com**, and **sec-sbi**.com** across three groups that could pertain to the actual domains the phishers used. Here are a couple of examples.

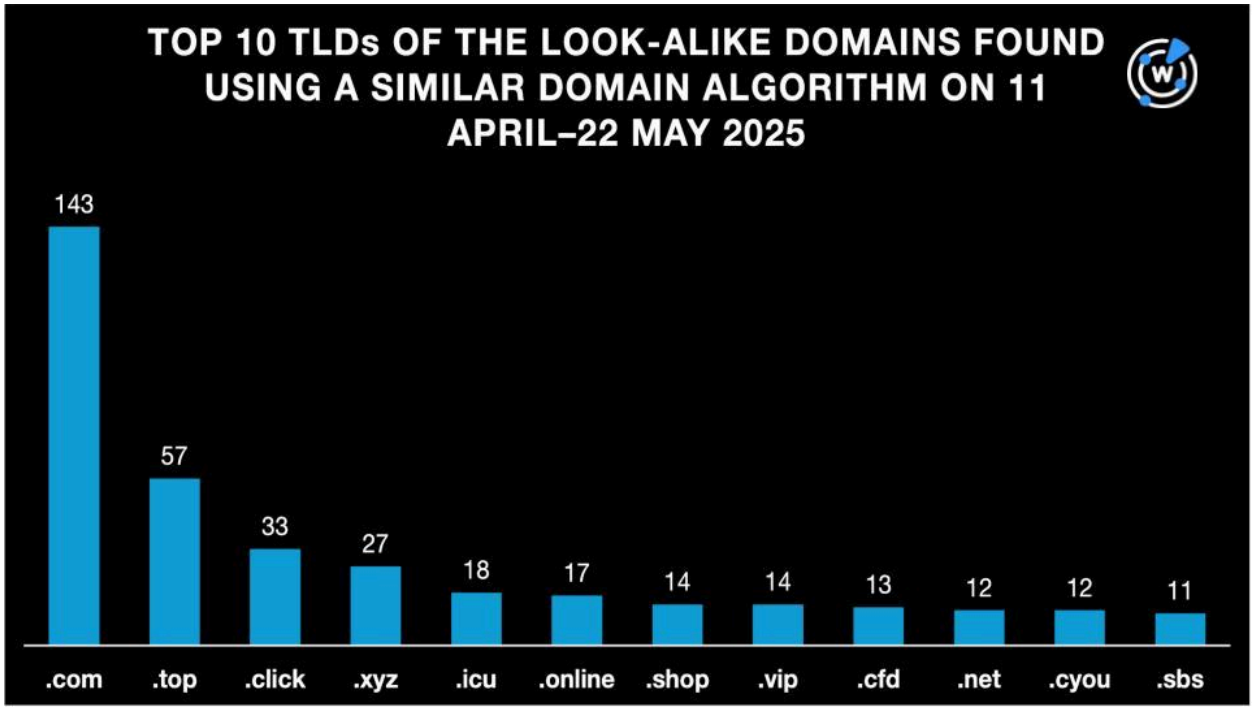
sb-auth****.cloud	sbiisec****.com	sec-sbi**.com
sb-authline[.]cloud	sbiisec06[.]com	sec-sbiloginn06[.]com

3. Hunting for More Connections

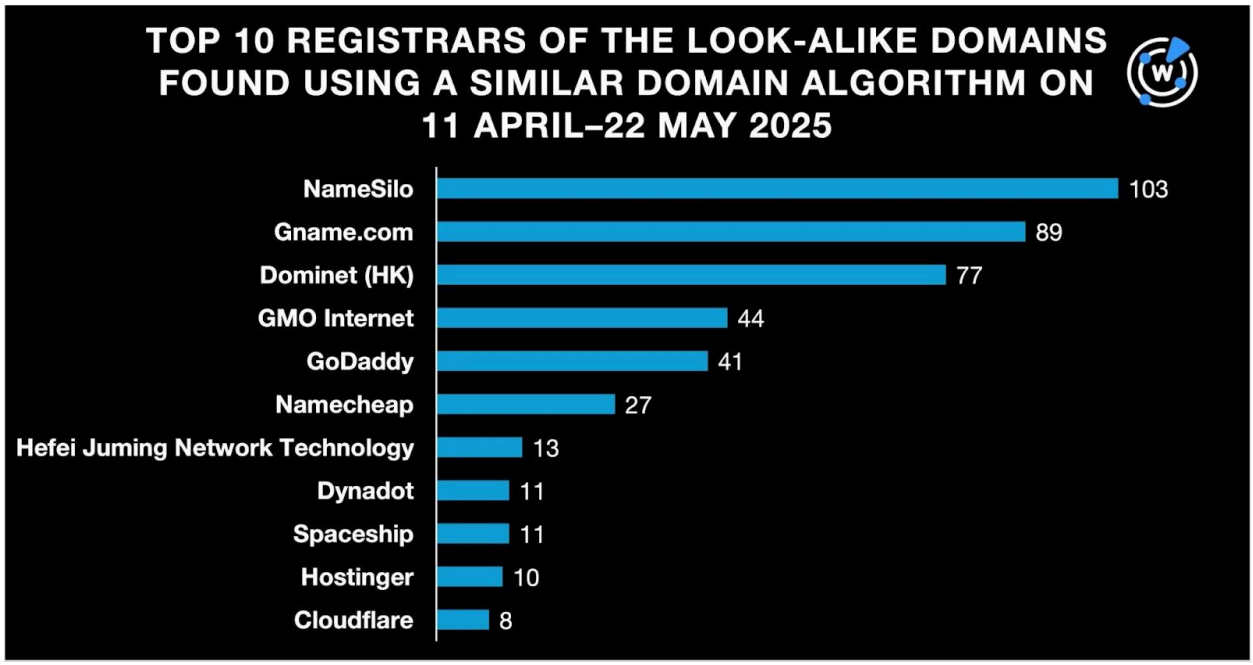
After the more targeted analyses above, we sought broader matches for the 44 phishing URLs cited in the previous section.

First, we used a similar domain algorithm to look for domains that resembled the masked ones in the 44 URLs. We collated 609 domains recorded between 11 April and 22 May 2025. We then looked further into their top-level domain (TLD) extensions, registrars, and registrant countries.

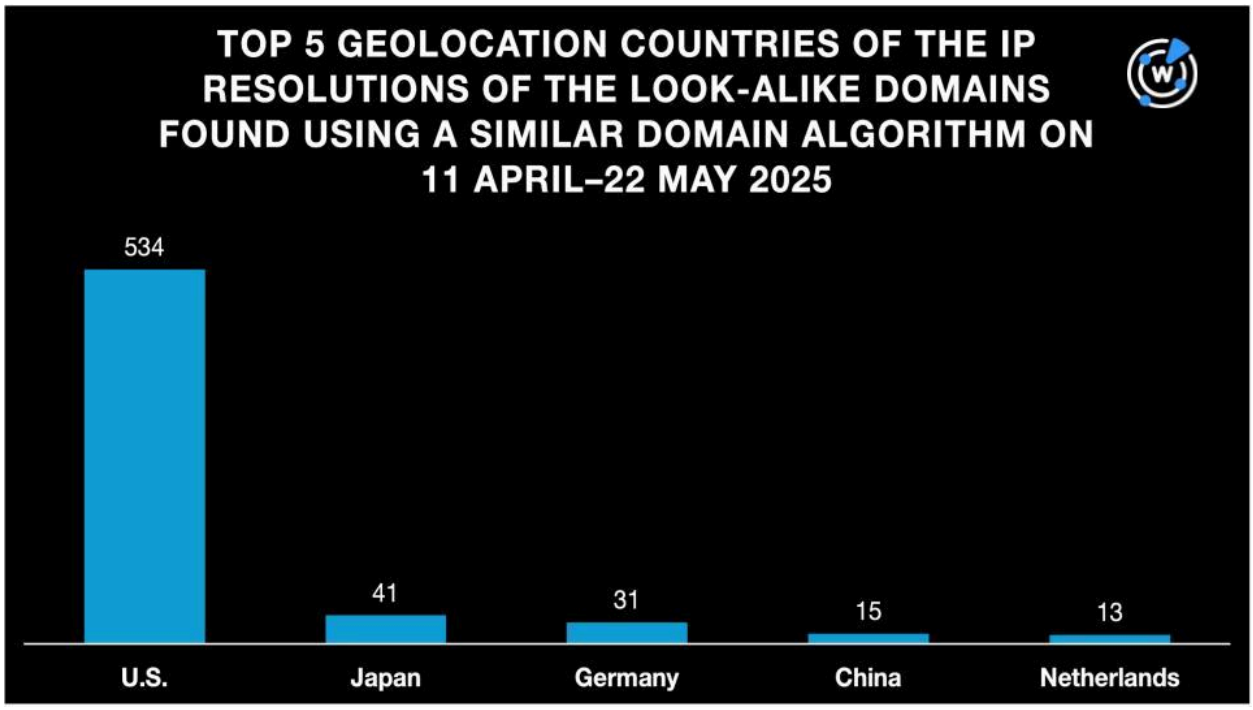
- They sported 122 TLD extensions. A majority of them (23%) had the .com extension. The other chart toppers were .top, .click, .xyz, .icu, .online, .shop, .vip, .cfd, .net, .cyou, and .sbs.



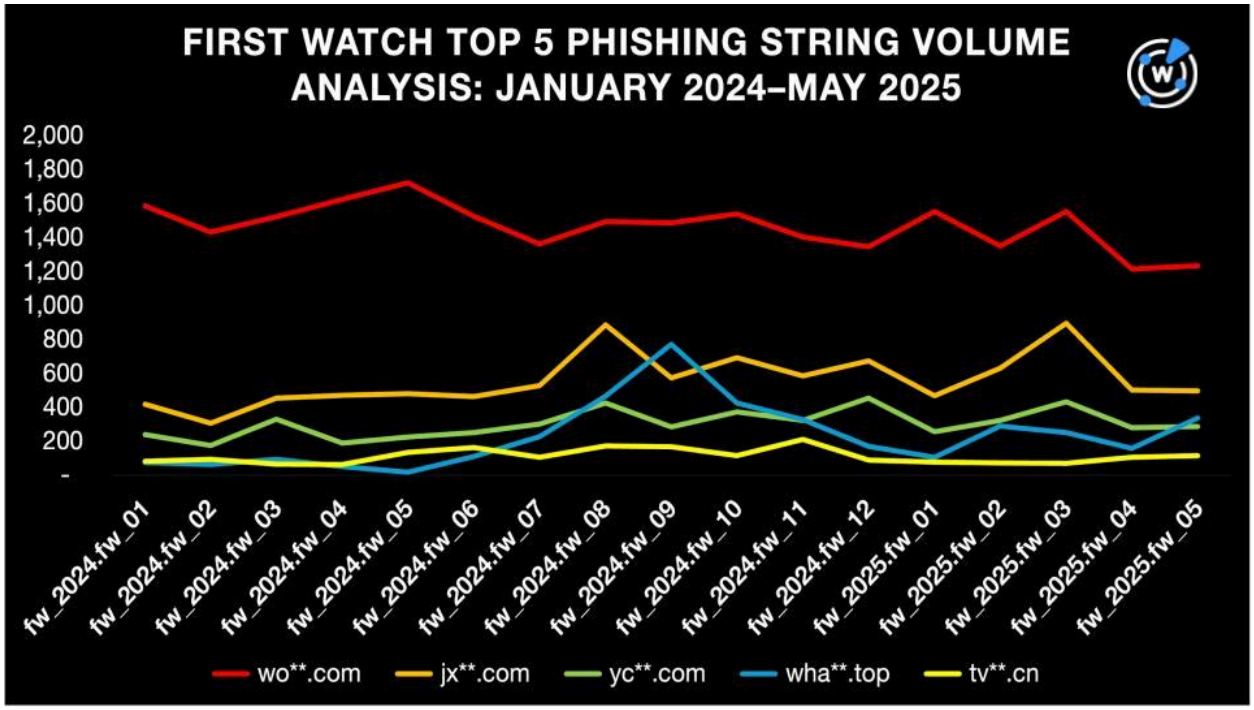
- The top 10 registrars were led by NameSilo, which accounted for 103 domains. Gname.com placed second; Dominet (HK), third; GMO Internet, fourth; GoDaddy, fifth; Namecheap, sixth; Hefei Juming Network Technology, seventh; Dynadot and Spaceship, eighth; Hostinger, ninth; and Cloudflare, tenth.



A DNS Lookup API query for the 609 domains, followed by IP Geolocation API queries, revealed that their resolving IP addresses were geolocated in 26 countries topped by the U.S., which accounted for 534 domains. The other topnotchers were Japan, Germany, China, and the Netherlands.

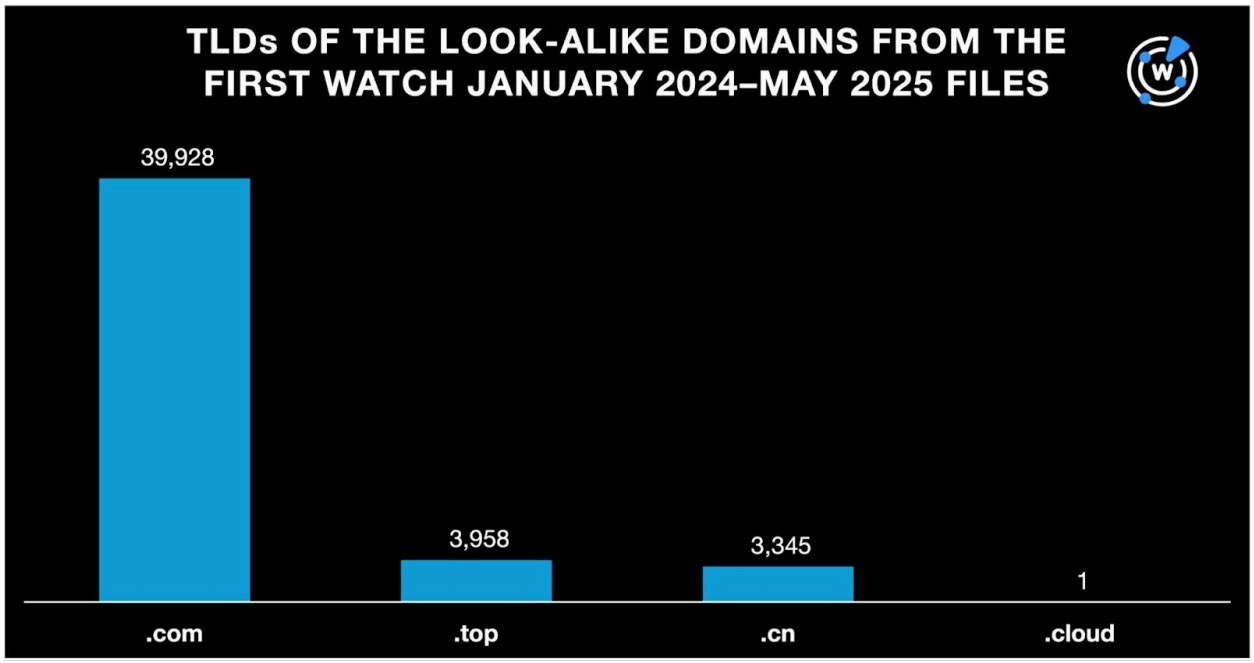


Next, we used First Watch to look for domains that resembled the masked ones in the 44 URLs. We collated data for 13 strings amounting to 47,232 matches in all. The following chart sums up our findings for the five strings that accounted for the highest domain volumes.

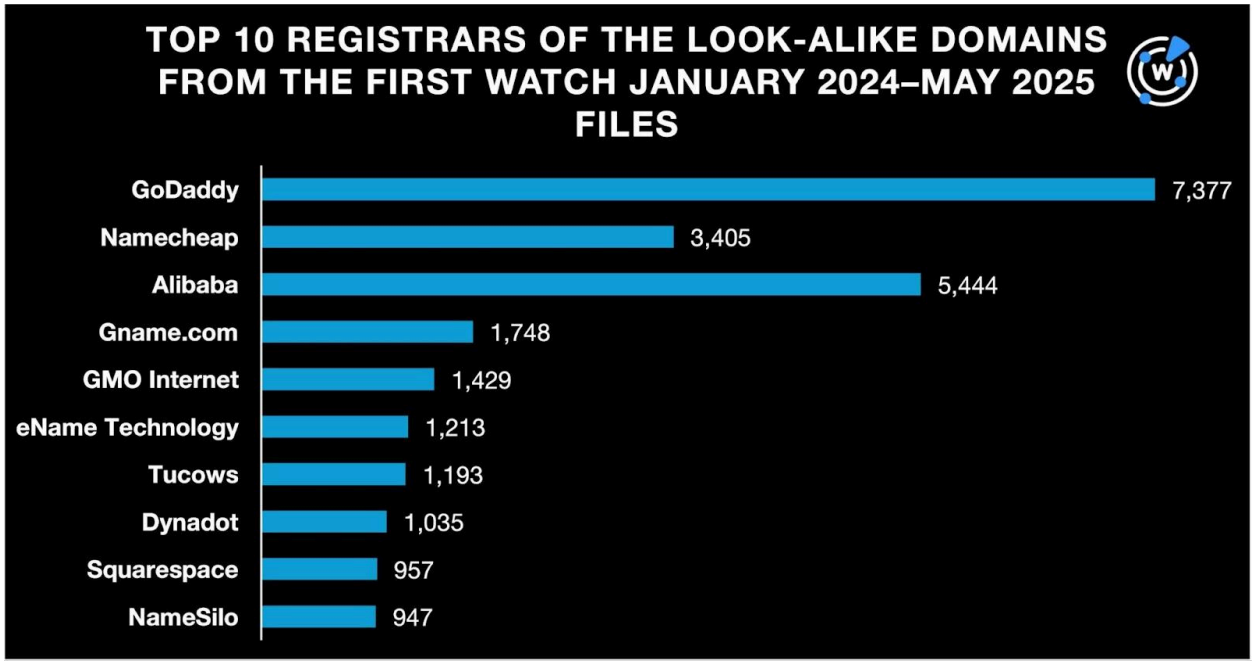


We also used First Watch to uncover look-alikes of the 44 masked domains and uncovered 47,232 domains. We then determined their TLD extensions, registrars, and the geolocation countries of their IP resolutions. Here is a summary of our findings.

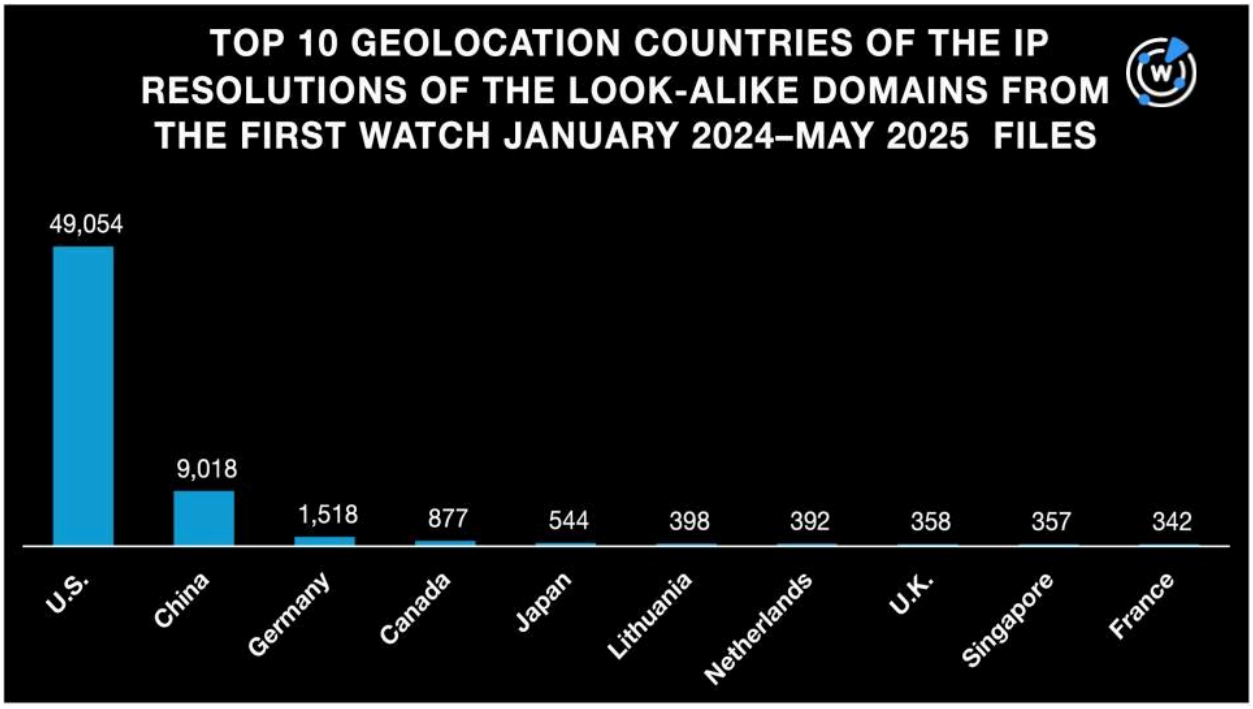
- The 47,232 First Watch domains used four TLD extensions—.com, .top, .cn, and .cloud.



- GoDaddy, Namecheap, Alibaba, Gname.com, GMO Internet, eName Technology, Tucows, Dynadot, Squarespace, and NameSilo were the top 10 registrars.



Using DNS Lookup API, followed by IP Geolocation API queries, we found that while 58 of the IP resolutions did not have geolocation countries on record, the remaining IP addresses were geolocated in 69 countries led by the U.S., which accounted for 49,054.



—

Our analysis of the phishing campaign allowed us to uncover 7,480 connected artifacts comprising 36 registrant-connected domains, 7,437 email-connected domains, and seven string-connected domains. To date, 267 of the connected domains have already figured in various attacks. Our broad-match searches for the 44 masked domains also turned up 609 look-alike domains found using a similar domain algorithm and 47,232 look-alike domains found on First Watch.

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 Registrant-Connected Domains

- 0356f[.]com
- acekameng[.]com
- cccihb[.]com
- dali-flower[.]com
- fengtaijie[.]com
- gjzhpt[.]com
- hqly365[.]net
- jchdsy[.]com
- mazhihong[.]com
- qqyd[.]cc
- sxsima[.]com
- uesgood[.]com
- xn--6rt883abm0aogb[.]com
- yctmms[.]com
- zailuliang[.]com

Sample Email-Connected Domains

- 002b03[.]cn
- 008962[.]cn
- 01302[.]cn
- aaaiang[.]cn
- aab5i[.]cn
- aabmall[.]com
- b1wiv[.]cn
- b406x[.]cn
- b5bb9d[.]cn
- c0893c[.]cn
- c19fd8[.]cn
- c1c9c8[.]cn
- d08a49[.]cn
- d22822[.]com
- d23f82[.]cn
- e-carer[.]com
- e-dana[.]com
- e-tg[.]com
- f07dqj[.]cn
- f2b8fe[.]cn
- f38781[.]cn
- g0ghroiy[.]cn
- g77829[.]cn
- g87jd[.]cn
- h3yx[.]com
- h5idus7h[.]cn
- h74z2v5[.]cn
- ifaac[.]cn
- ifaho[.]cn
- ifcot[.]cn
- jfeip[.]cn
- jffcu[.]cn
- jffhu[.]cn
- kbfei[.]cn
- kbfmh[.]cn
- kbgez[.]cn
- lexsq[.]cn
- lfcuc[.]cn
- lfgjyxj[.]com
- mayut[.]cn
- mazm[.]cn
- mbano[.]cn
- ngshk[.]cn
- ngspa[.]cn
- ngsrr[.]cn
- oopgl[.]cn
- oopqb[.]cn
- oowod[.]cn
- pcsuw[.]cn
- pctrx[.]cn

- pcvjn[.]cn
- qbbbb[.]cn
- qbbhw[.]cn
- qbdia[.]cn
- redjh[.]cn
- redutrip[.]com
- regox[.]cn
- sfrwo[.]cn
- sfslocher[.]com
- sftsp[.]cn
- tagzg[.]cn
- taifp[.]cn
- taigsl[.]cn
- ucgbook[.]com
- ucipa[.]cn
- ucmas[.]cn
- v5204[.]com
- v5205[.]com
- v5206[.]com
- weedb[.]cn
- weemd[.]cn
- weeuq[.]cn
- xewnz[.]cn
- xfdxk[.]cn
- xfgie[.]cn
- ydxkx[.]cn
- ydznf[.]cn
- yeave[.]cn
- zhangzl3[.]com
- zhaorou[.]cn
- zhcca[.]com

Sample String-Connected Domains

- etcady[.]top
- evrryday[.]com[.]au
- uhlkg[.]com
- zjkso[.]com

Sample Look-Alike Domains Found Using a Similar Domain Algorithm

- 1compass[.]net
- abu[.]cash
- abu[.]gg
- abu[.]land
- bakuten-bakuten[.]com
- bakuten[.]online
- bcompass[.]ly
- car-compass[.]pl
- cash-compass[.]de
- cf-compass[.]ru
- daiw[.]top
- daiwa-amjp[.]com
- daiwa-amljp[.]com
- e-ncompass[.]com
- ekabu[.]click
- encompass[.]finance
- f-rakuten[.]cyou
- fas-compass[.]co[.]jp
- fas-compass[.]com
- gene-compass[.]com
- gkabu[.]click
- goal-compass[.]com
- hkabu[.]click
- homura[.]fr
- homura[.]love
- icompass[.]tur[.]br
- idea-compass[.]com
- ikabu[.]click
- jkabu[.]click
- kabu-ito[.]com

- kabu[.]buzz
- kabu[.]earth
- lcompass[.]net
- lkabu[.]click
- loomura[.]shop
- mats[.]com[.]ua
- mats[.]ovh
- mats[.]pl
- namatsu[.]com
- natsumatsu[.]biz
- natsumatsu[.]buzz
- ocompass[.]eu
- okabu[.]click
- omurax[.]info
- pkabu[.]click
- poker-compass[.]com
- poker-compass[.]de
- qkabu[.]click
- raku[.]skin
- rakuraku[.]info
- rakuraku[.]site
- saffron-compass[.]studio
- sbi-sec[.]cfd
- sbi-sec[.]lat
- technomura[.]click
- ten-sec[.]com
- terrace[.]farm
- ukabu[.]click
- ukematsui[.]com
- ux-compass[.]com
- vkabu[.]click
- vkabu[.]com
- wkabu[.]click
- worakutenv[.]vip
- xbisec[.]sbs
- xcompass[.]xyz
- xkabu[.]click
- ykabu[.]click
- yomura[.]es
- zkabu[.]click

Sample Look-Alike Domains from First Watch

- dsgr54[.]com
- dsgr7nyn6-nyv1bf5[.]com
- dsgrandbazaar[.]com
- jx-0z8fxa[.]com
- jx-625-kz2y2[.]com
- jx-aiyouxi[.]com
- mu-ying-hu-li[.]cn
- mu-ying[.]com[.]cn
- mu020yo[.]cn
- reqie[.]cn
- reqie[.]cn
- reqie[.]com[.]cn
- sb-authline[.]cloud
- sbiisec01[.]com
- sbiisec02[.]com
- tv-2i[.]cn
- tv-ages[.]com[.]cn
- tv-beijing[.]com[.]cn
- wha136bx9[.]top
- wha1tsappwe[.]top
- wha455dmoeq[.]top
- yc-35pvzyhgnluiz[.]com
- yc-3mfpn-k-mfpy9-mkb4o[.]com
- yc-53ilhp1jq0vsvu[.]com