日本の証券会社を騙るフィッシングを DNS で分析

目次

要旨

最近、サイバー犯罪者により証券口座が乗っ取られ、株式が正当な口座所有者の許可なく売買される事件が数多く報道されています。2025 年 1 月から 4 月までの間に記録された不正取引は 3,500 件を超え、株式所有者の損失は 3,000 億円あまりにのぼっています。

5 月には、日本の株主などを標的とするフィッシングキットを調査したレポートが Proofpoint により公表され、その中で、セキュリティ侵害インジケーター（IoC）として 7 件のドメイン名が特定されました。当社ではこれを受け、同レポートおよびその他のフィッシングレポートなどをもとに、日本の証券会社になりすますフィッシングに関する調査を独自に実施しました。その結果、さらに多くの関連アーティファクトを特定するとともに、いくつかの重要な情報を得ることができました。

当社の豊富なドメイン名・DNS インテリジェンスを活用して行った今回の調査では、以下を特定することができました。

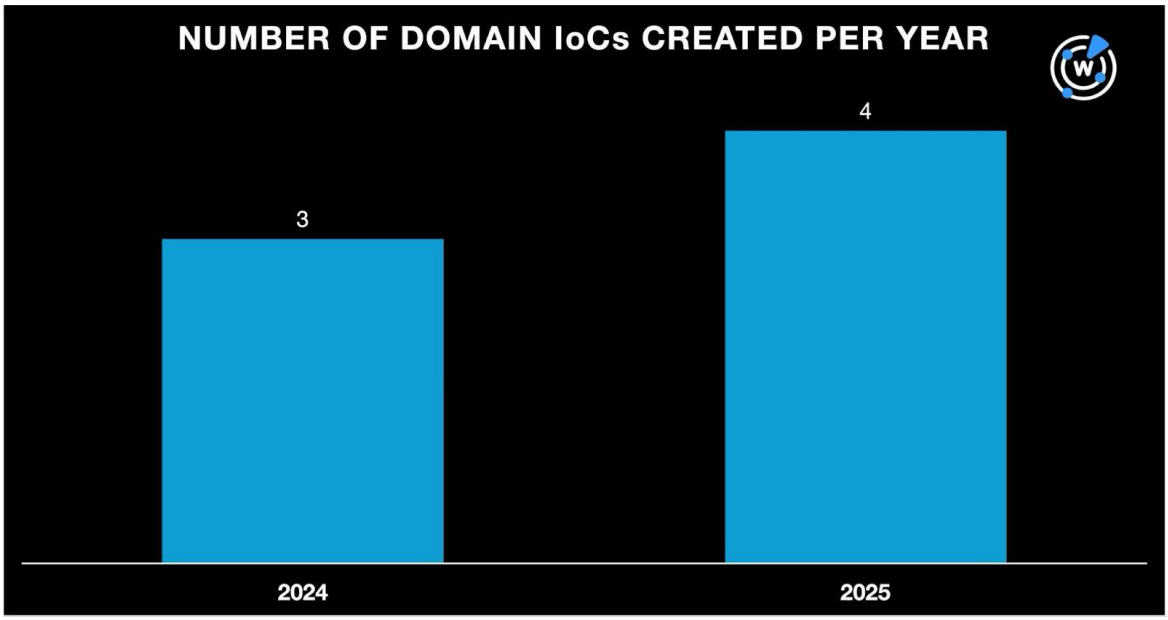
- IoC の登録者が登録していた別のドメイン名 36 件
- IoC の登録メールアドレスを使って登録されていた別のドメイン名 7,437 件
- IoC と同じテキスト文字列を含む別のドメイン名 7 件
- 類似ドメインアルゴリズムによって 2025 年 4 月 11 日～5 月 22 日の記録から検出された類似ドメイン名 609 件
- First Watch によって 2024 年 1 月～2025 年 5 月の記録から検出された類似ドメイン名 47,232 件

この調査で検出したアーティファクトのサンプルは、末尾の付録でご確認いただけます。

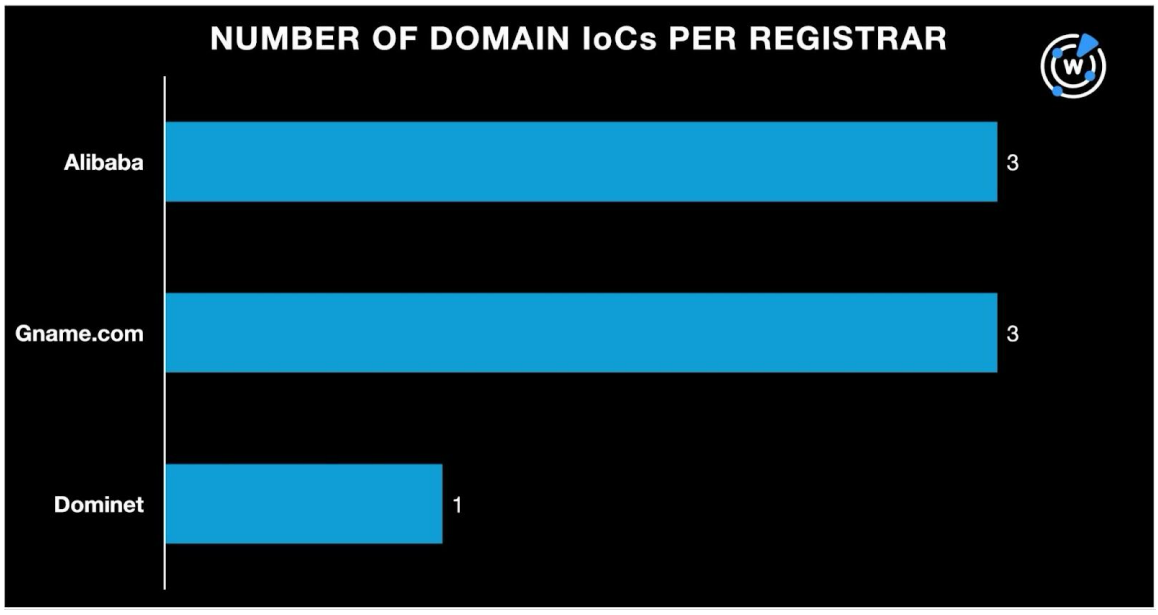
1. フィッシングドメインの特徴

まず、Proofpoint のレポートで IoC として特定された 7 件のドメイン名（以下「ドメイン IoC」）を Bulk WHOIS API で検索しました。その結果、以下のことが明らかになりました。

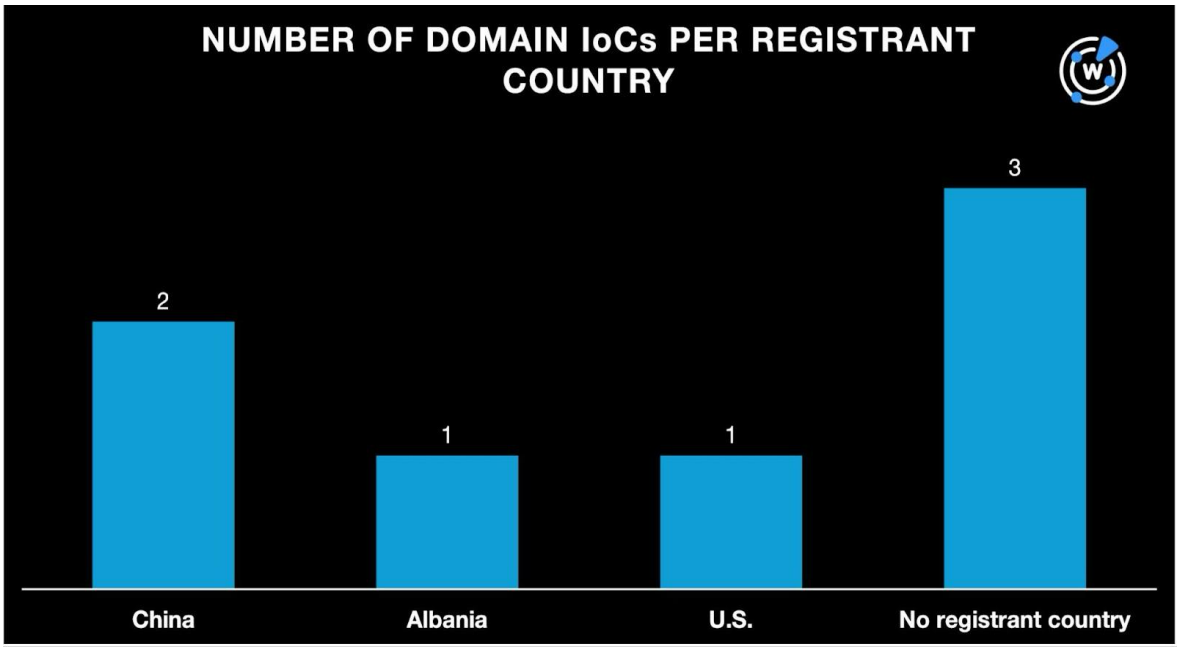
- これらは 2024 年から 2025 年にかけて新規登録されたドメイン名で、攻撃に悪用された時点では比較的新しいドメイン名だったと言うことができます。



- 7 件の IoC を管理していたレジストラは、Alibaba、Gname.com、Dominet という 3 社でした。Alibaba と Gname.com がそれぞれ 3 件、Dominet が 1 件を管理していました。



- 3 件のドメイン IoC については、登録された国が WHOIS に表示されませんでした。残りの 4 件は 3 カ国（中国 2 件、アルバニア 1 件、米国 1 件）で登録されていました。



7 件のドメイン IoC を DNS Chronicle API で照会した結果、4 件については、過去にドメイン名から IP アドレスへの名前解決（A および AAAA レコード）が合計 198 種類設定されていたことがわかりました。特に、evrryday[.]com というドメイン IoC では、2017 年 4 月 28 日以降に設定された名前解決が 166 種類にのぼりました。

次に、7 件の現在の WHOIS レコードを調べたところ、2 件（uhlkg[.]cn と zjkso[.]cn）の登録者名が同一であることがわかりました。さらに、Reverse WHOIS API でこのデータポイントを検索語として検索した結果、その登録者が登録している 36 件のドメイン名を新たに発見しました（重複とすでに IoC として特定されていたものを除く）。

また、WHOIS History API で同様に 7 件のドメイン IoC を検索した結果、3 件については過去の WHOIS レコードにメールアドレスが残っており、合計で 10 件のメールアドレスを特定できました。さらに詳しく調べた結果、そのうち 6 件は公開されているメールアドレスと判明しました。

Reverse WHOIS API を使ってその 6 件の公開メールアドレスを問い合わせたところ、そのうちの 5 件は、7,437 件にのぼるドメイン名の過去の WHOIS レコードにも記録されていました。残り 1 件の公開メールアドレスもドメイン名と紐づいていましたが、紐づいたドメイン名の数が 1 万件を超えていたことから、ドメイナーのものと思われました。

ドメイン IoC の登録に使われていたものと同じメールアドレスが WHOIS に記録されていた 7,437 件のドメイン名を Threat Intelligence API に問い合わせた結果、267 件のドメイン名が攻撃に関与していたことが判明しました。以下はその例です。

ドメイン IoC と同じメールアドレスを使用していた悪意あるドメイン名	関与していた脅威
015441[.]cn	フィッシング
abivh[.]cn	フィッシング
b1wiv[.]cn	フィッシング
c4ujvs0b[.]cn	フィッシング
dcvlp[.]cn	フィッシング

次に、7 件のドメイン IoC が 7 種類の固有のテキスト文字列で始まっていることを確認しました。しかし、その 7 種類を Domains & Subdomains Discovery で検索したところ、他のドメイン名にも含まれていたのは、そのうち以下の 4 種類にとどまりました。

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

4 種類のうちいずれかの文字列を含んだドメイン名は、結局 7 件見つかりました。
上記の調査を通じて、IoC と何らかの関連性を持つドメイン名として、7,480 件が特定されました。そして、そのうち 267 件はすでに攻撃に悪用されていたことがわかりました。

2. フィッシングメールの関連性

調査の次のステップとして、同じ詐欺キャンペーンに関わっている可能性のある 10 件のフィッシングメールをもとに、その送信者メールアドレスから以下のドメイン名を抽出しました。

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

例として、「tmjs[.]net」を含むメールアドレスから 2025 年 5 月 19 日に送信されたフィッシングメールを以下に示します。

【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:

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

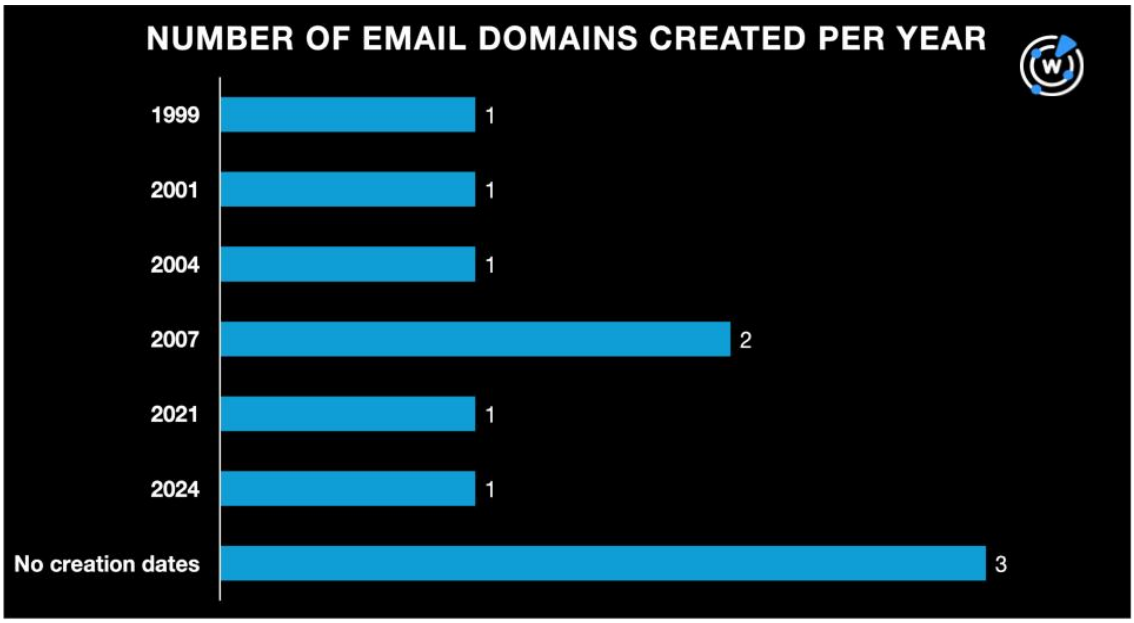
メールアドレス登録および認証方式設定ページへ進む

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。

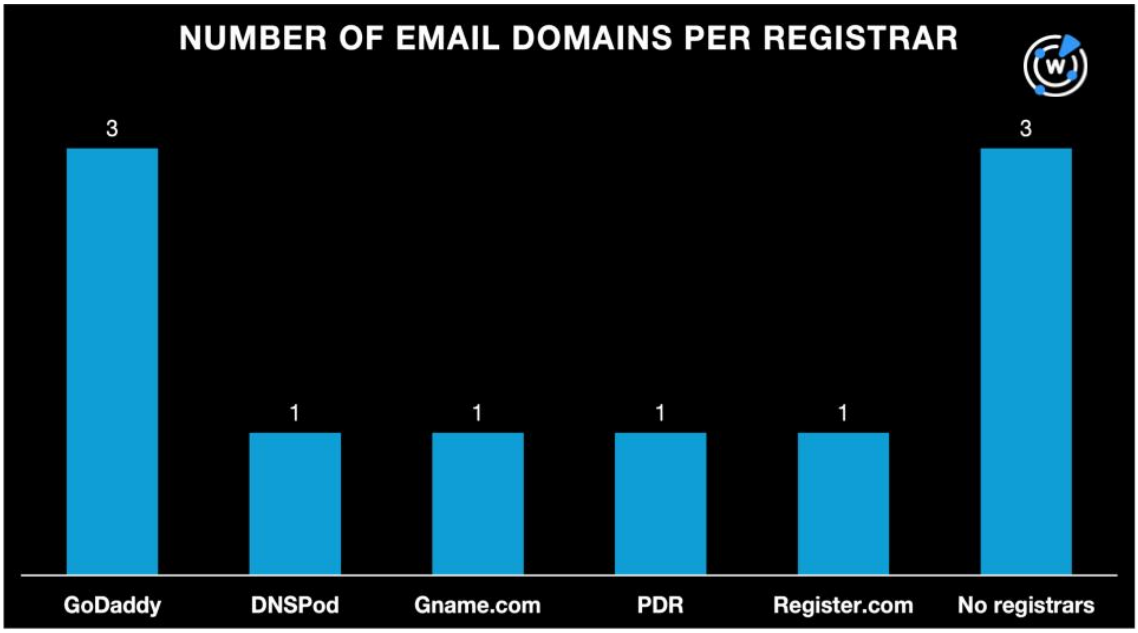
発行元：SBI証券株式会社
〒106-6019 東京都港区六本木1-6-1 泉ガーデンタワー
Copyright © SBI SECURITIES Co., Ltd. All Rights Reserved.

まず、前述の 10 件のメールドメイン名を Bulk WHOIS API で照会したところ、以下のことがわかりました。

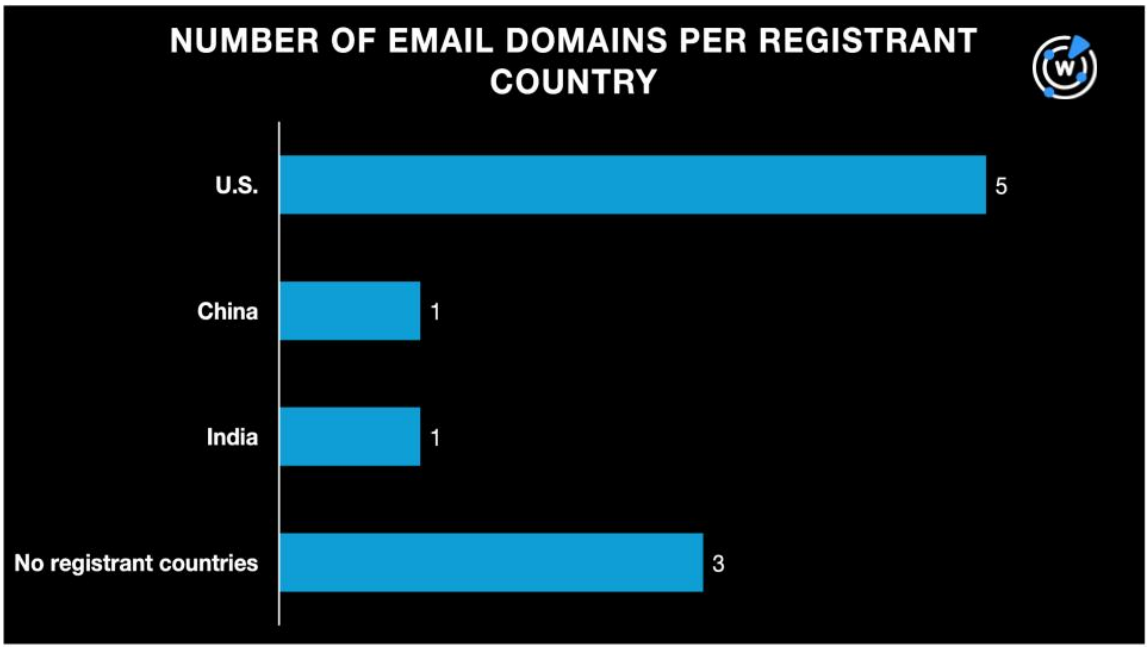
- ドメイン名の登録年は 1999 年から 2024 年にわたって分散していました。このことから、詐欺師たちはドメイン名の登録年数を区別していなかったと推測されます。なお、3 件のドメイン名については、現在の WHOIS レコードに登録年月日がありませんでした。



- メールドメイン名のレジストラとして、5 社が特定されました。GoDaddy が 3 件、DNSPod、Gname.com、PDR、Register.com が 1 件ずつのドメイン名を管理していました。残りの 3 件のドメイン名については、レジストラ名が WHOIS に記録されていませんでした。



- メールドメイン名の登録地として 3 カ国が判明しました。最多は米国で 5 件、次いで中国とインドで 1 件ずつが登録されていました。3 件は登録国が WHOIS に記録されていませんでした。



次に、フィッシング対策協議会の緊急情報から、マスキングされたフィッシング URL を合計 44 件収集できました（本稿執筆時点）。以下の通りです。

- 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/

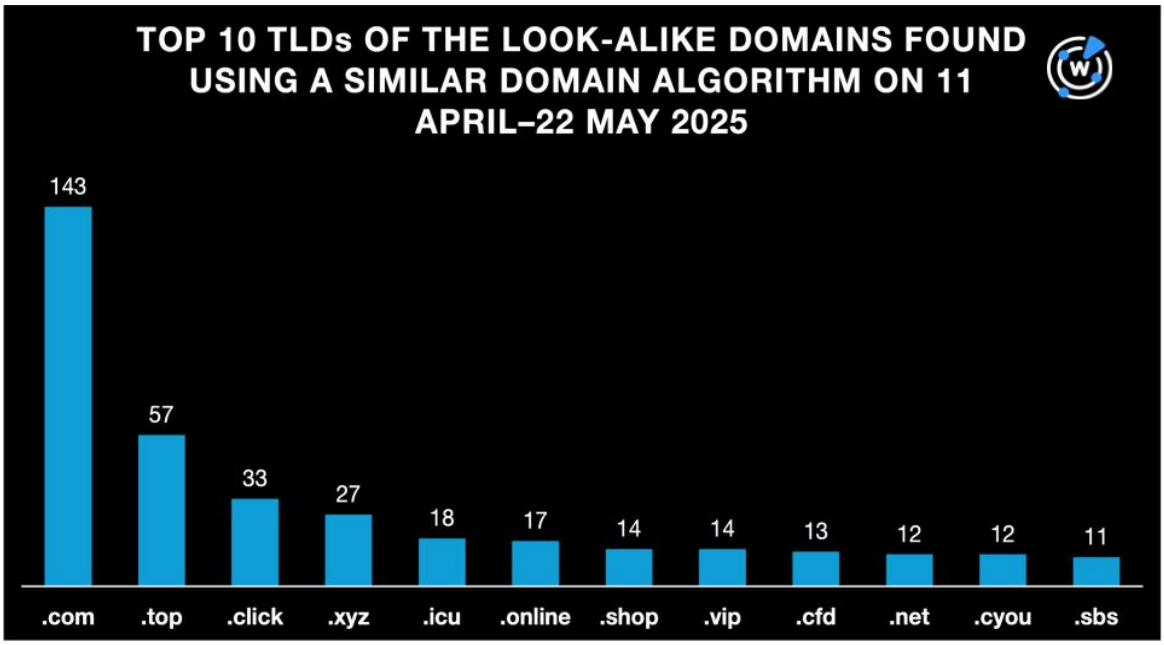
そこでまず、上記の URL から抽出したドメイン名を検索語として、First Watch Malicious Domains Data Feed を実行しました。その結果、3 種類の文字列（**sb-auth****.cloud**、**sbiisec****.com**、**sec-sbi**.com**）のいずれかを含んでいるドメイン名を 20 件検出しました。以下はそのドメイン名の例です。

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

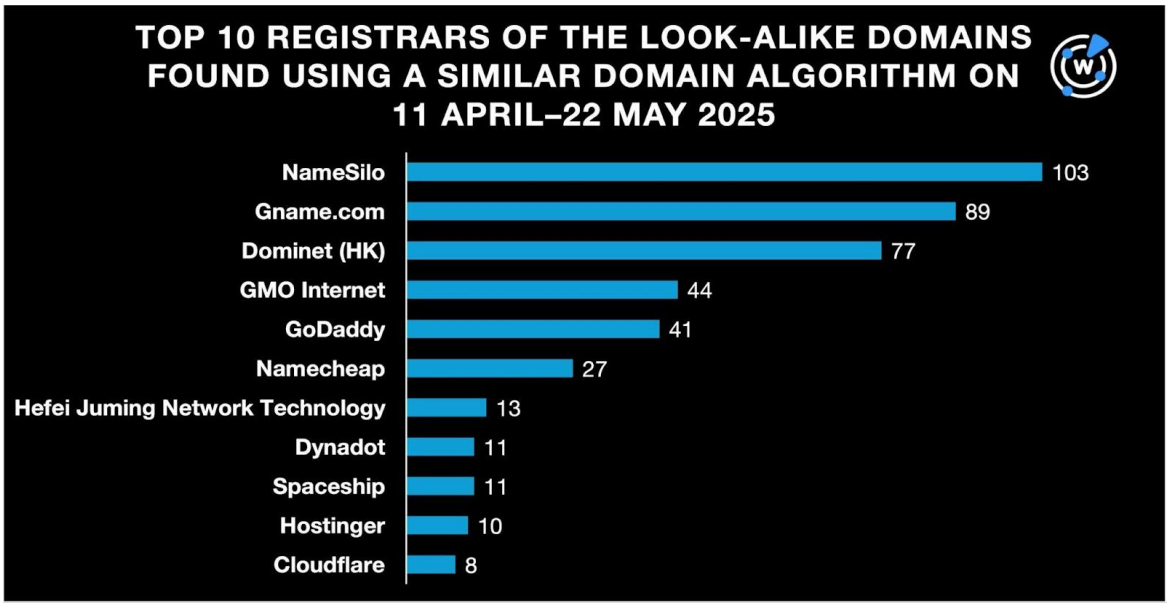
3. さらなる関連性を探る

前述の 44 件のフィッシング URL を使ってより詳細な分析を行うため、類似ドメインアルゴリズムを使い、44 件の URL に含まれているドメイン名と見た目の似ているドメイン名を探しました。その結果、2025 年 4 月 11 日から 5 月 22 日までの記録から 609 件のドメイン名をリストアップできましたので、それらのトップレベルドメイン（TLD）、レジストラおよび登録国についてさらに詳しく見ていきました。

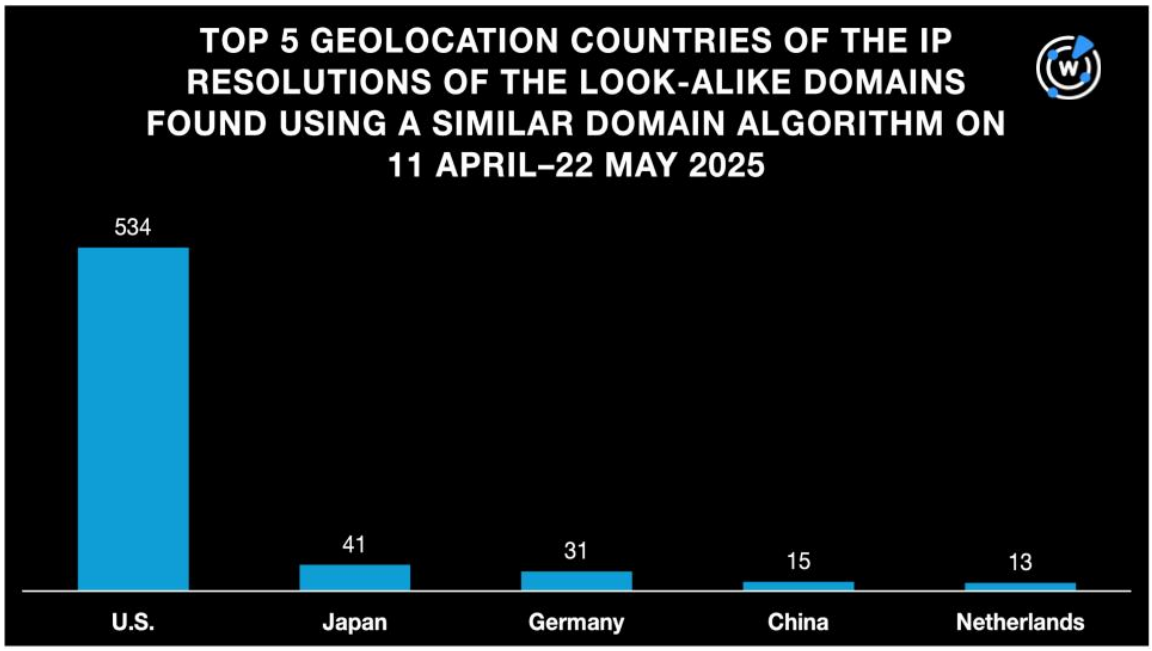
- TLD は 122 種類にのぼりましたが、その大半は.com（23%）でした。次いで多かったのは、.top、.click、.xyz、.icu、.online、.shop、.vip、.cfd、.net、.cyou、.sbs でした。



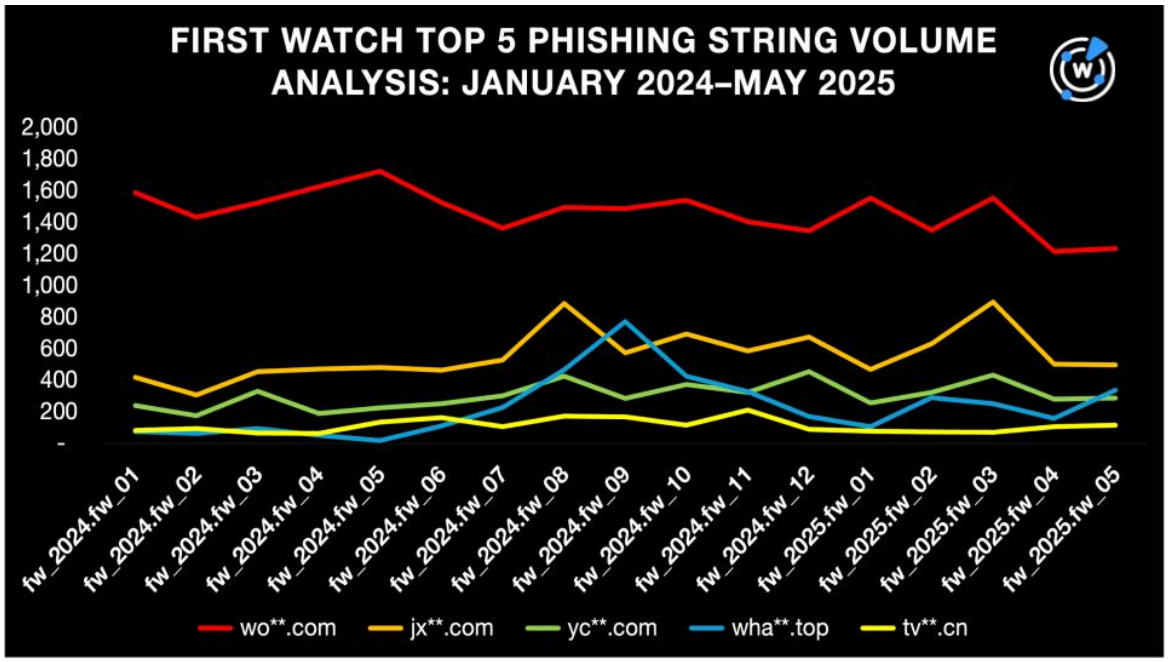
- 管理ドメイン名数が最も多いレジストラは NameSilo で、103 件でした。2 位は Gname.com、3 位は Dominet (HK)、4 位は GMO インターネット、5 位は GoDaddy、6 位は Namecheap、7 位は Hefei Juming Network Technology、8 位は Dynadot と Spaceship、9 位は Hostinger、10 位は Cloudflare でした。



609 件のドメイン名に対して DNS Lookup API を実行し、続いて IP Geolocation API を実行したところ、それらのドメイン名が名前解決する IP アドレスが 26 カ国に分散していることがわかりました。IP アドレスの所在地として最も多かったのは米国で、534 件でした。次に多かったのは、日本、ドイツ、中国、オランダでした。

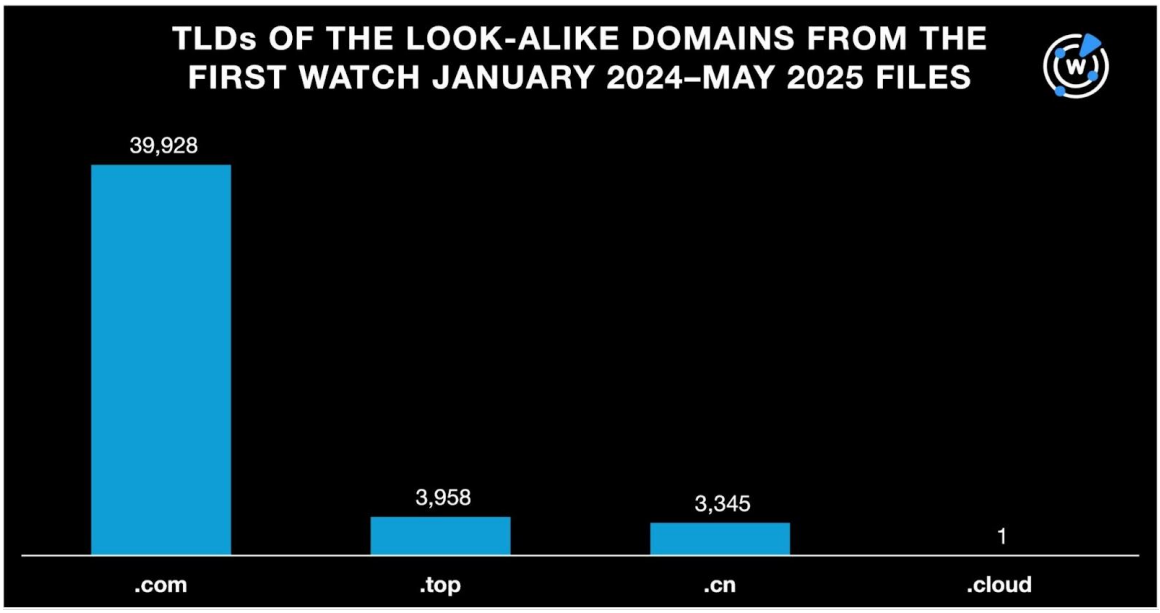


次に、First Watch を使用して、44 件のマスキングされた URL のドメイン名と似ているドメイン名を検索しました。そして、13 種類の文字列に合致するドメイン名を合計 47,232 件検出しました。以下は、ドメイン名数が最も多かった上位 5 種類の文字列に関する調査結果です。

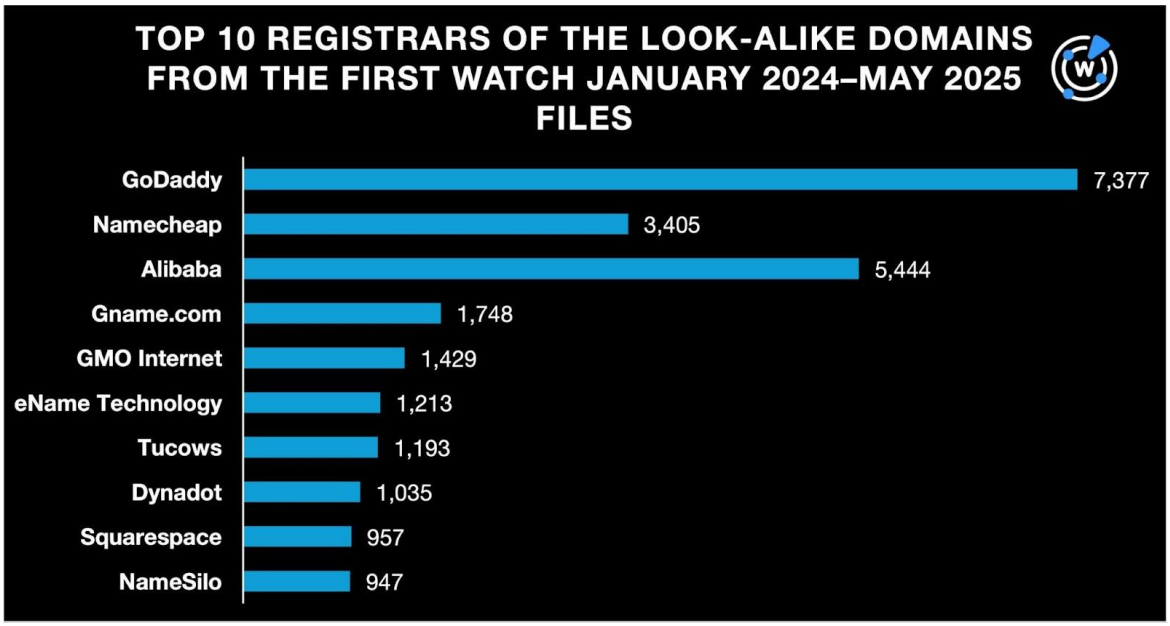


次に、上述の 47,232 件のドメイン名の TLD、レジストラおよび名前解決する IP アドレスの地理的位置を確認し、以下の情報を得ました。

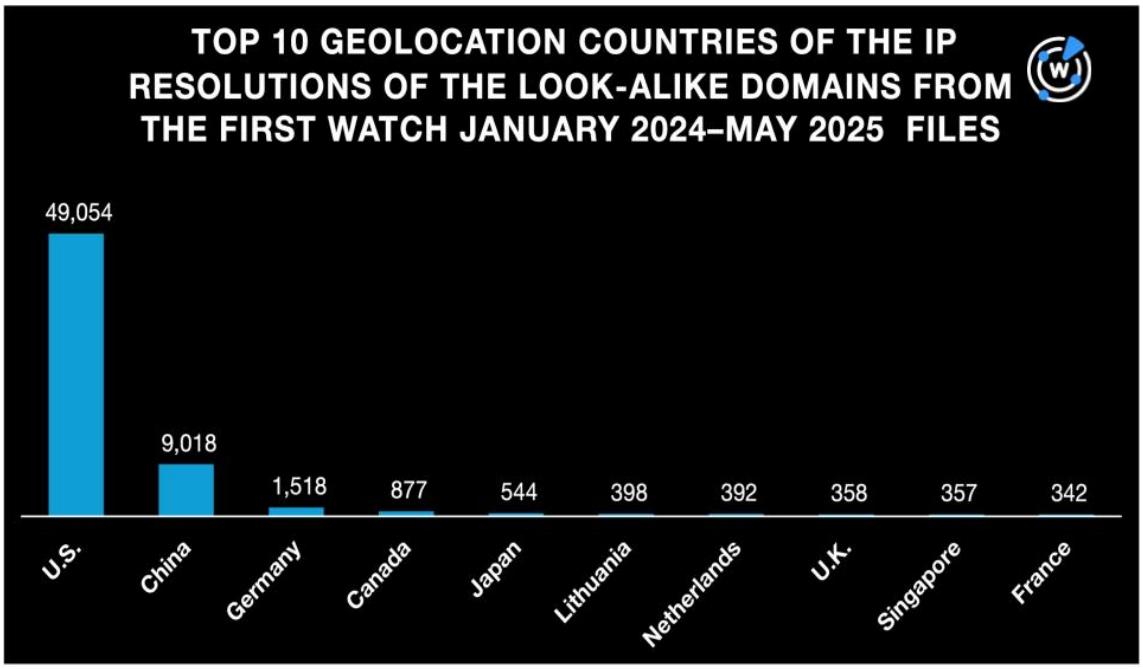
- 47,232 件のドメイン名の TLD は、.com、.top、.cn、.cloud のいずれかでした。



- レジストラの上位 10 社は、多い順に GoDaddy、Namecheap、Alibaba、Gname.com、GMO インターネット、eName Technology、Tucows、Dynadot、Squarespace、NameSilo でした。



DNS Lookup API、続いて IP Geolocation API を使って検索したところ、名前解決した IP アドレスのうち 58 件については、所在している国の情報がありませんでした。残りの IP アドレスは 69 カ国に分布していましたが、最も多く位置していたのは米国で、49,054 件ありました。



—

今回、日本の証券会社を標的としたフィッシングキャンペーンを当社の DNS インテリジェンスで分析した結果、合計 7,480 件の関連アーティファクト（内訳：IoC の登録者が登録していたドメイン名 36 件、IoC の登録メールアドレスを使って登録されていたドメイン名 7,437 件、IoC と同じテキスト文字列を含むドメイン名 7 件）を発見しました。これまでのところ、そのうち 267 件のドメイン名はさまざまな攻撃に関与していることが確認されています。また、マスキングされた 44 件の URL のドメイン名について広範な照合を行い、類似ドメインアルゴリズムを使って 609 件、First Watch を使って 47,232 件の類似ドメイン名を特定しました。

この調査で使用した商品の詳細につきましては、こちらまでお気軽にお問い合わせください。

免責事項： 当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。

付録：アーティファクトの例

IoC の登録者によって登録されていたドメイン名の例

- 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

IoC と同じメールアドレスを使って登録されていたドメイン名の例

- 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

IoC と同じ文字列を含むドメイン名の例

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

類似ドメインアルゴリズムによって検出された類似ドメイン名の例

- 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

First Watch によって検出された類似ドメイン名の例

- 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