.topドメインを悪用するフィッシンググループを発見

目次

要旨

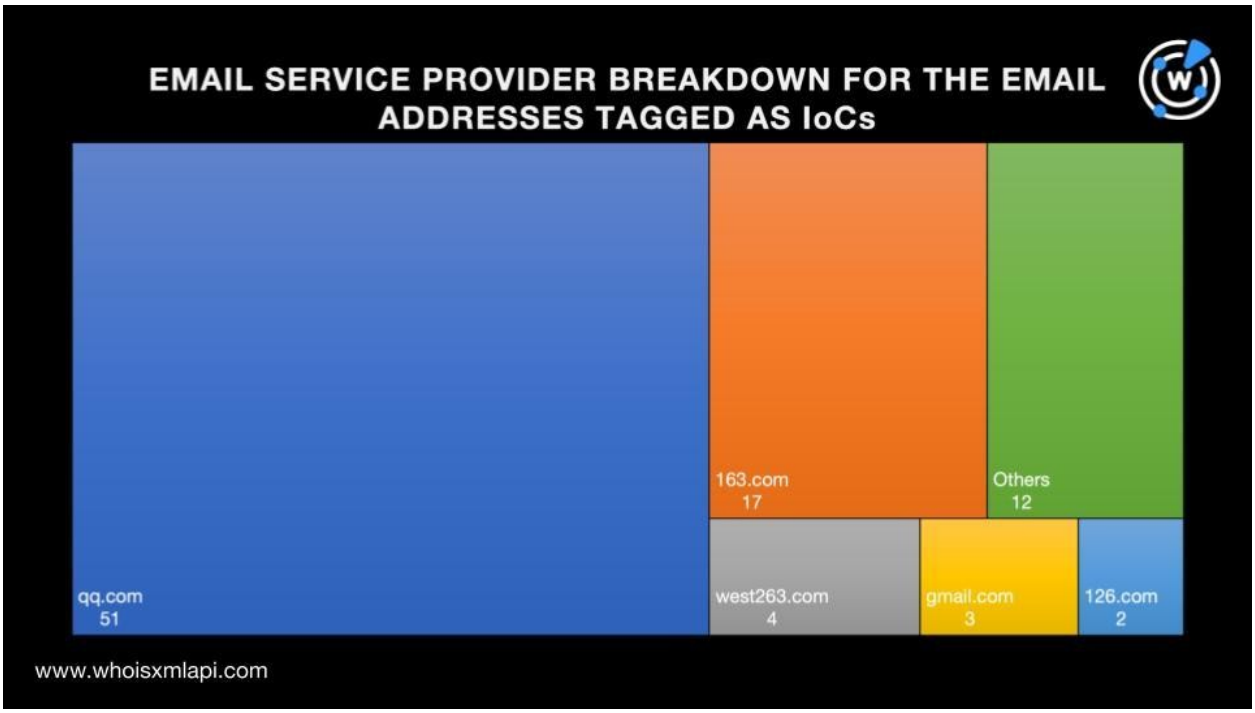
脅威リサーチャーのDancho Danchevは最近、.topドメイン名を悪用したフィッシングを発見し、89個のメールアドレスをセキュリティ侵害インジケーター（IoC）として特定しました。そして、WhoisXML APIの研究チームがこのほど、そのIoCリストをもとに他の関連アーティファクトを見つけるべく、DNSを詳細に調べました。この調査の結果、以下が明らかになりました。

- IoCのメールアドレスを使用して登録された4,284個のドメイン名
- それらのドメイン名の一部をホストしていた71個のIPアドレス。マルウェアチェックにより、そのうち2個には悪意があることを確認
- 上記のIPアドレスの一部がホストしていた890個のドメイン名

IoCに関する事実

まず、DanchevがIoCとして特定した89個のメールアドレスを調べてみると、次のことがわかりました。

- 10個は最近のドメイン名登録に全く使われていない
- 51個はqq[.]comのサービスで作成。次いで多かったメールサービスは、163[.]com（17個）、west263[.]com（4個）、gmail[.]com（3個）、126[.]com（2個）。残りの12個のメールアドレスは、別の12プロバイダー（abc[.]com、domainmanager[.]top、foxmail[.]com、hxmail[.]com、lamartina[.]info、live[.]cn、seobuzz[.]it、sina[.]cn、sina[.]com、somcom[.]com、we[.]top、yeah[.]net）に分散。以下のグラフは、プロバイダーごとのメールアドレス数を示したものです。

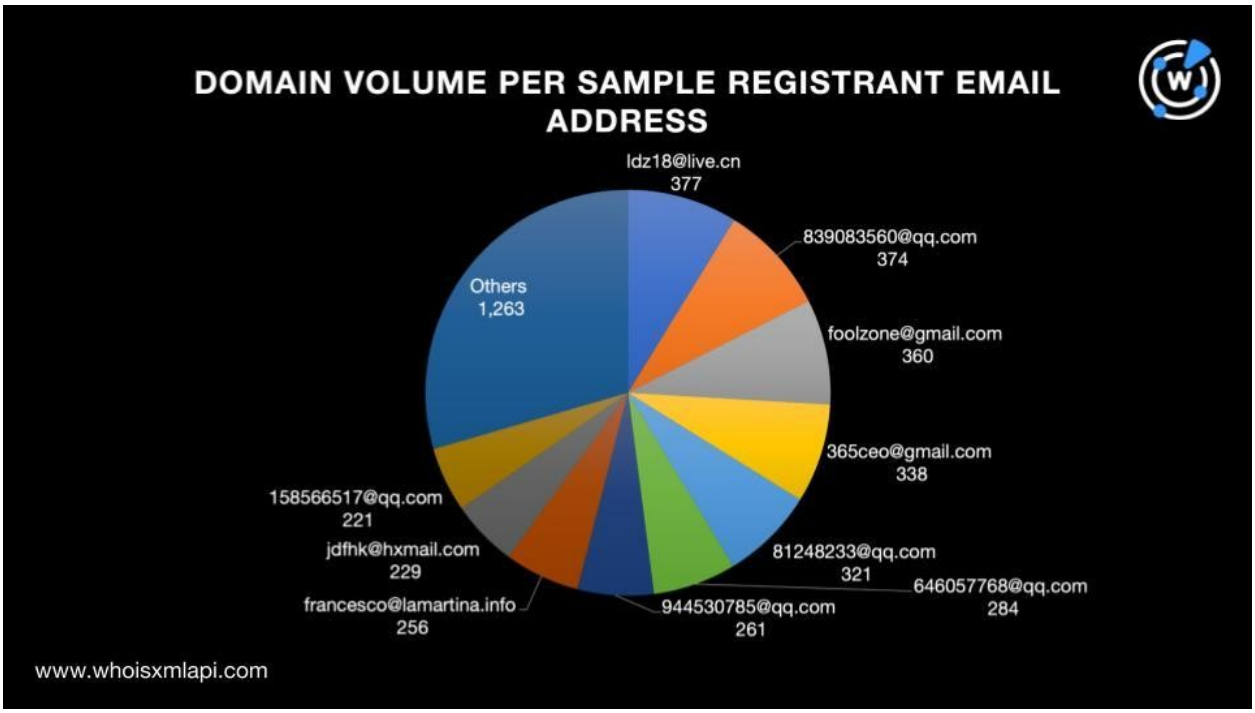


- 79個のメールアドレスはそれぞれ、最近1〜10,000超のドメイン名の登録に使用。合計で172,654個のドメイン名の登録者メールアドレスになっています。

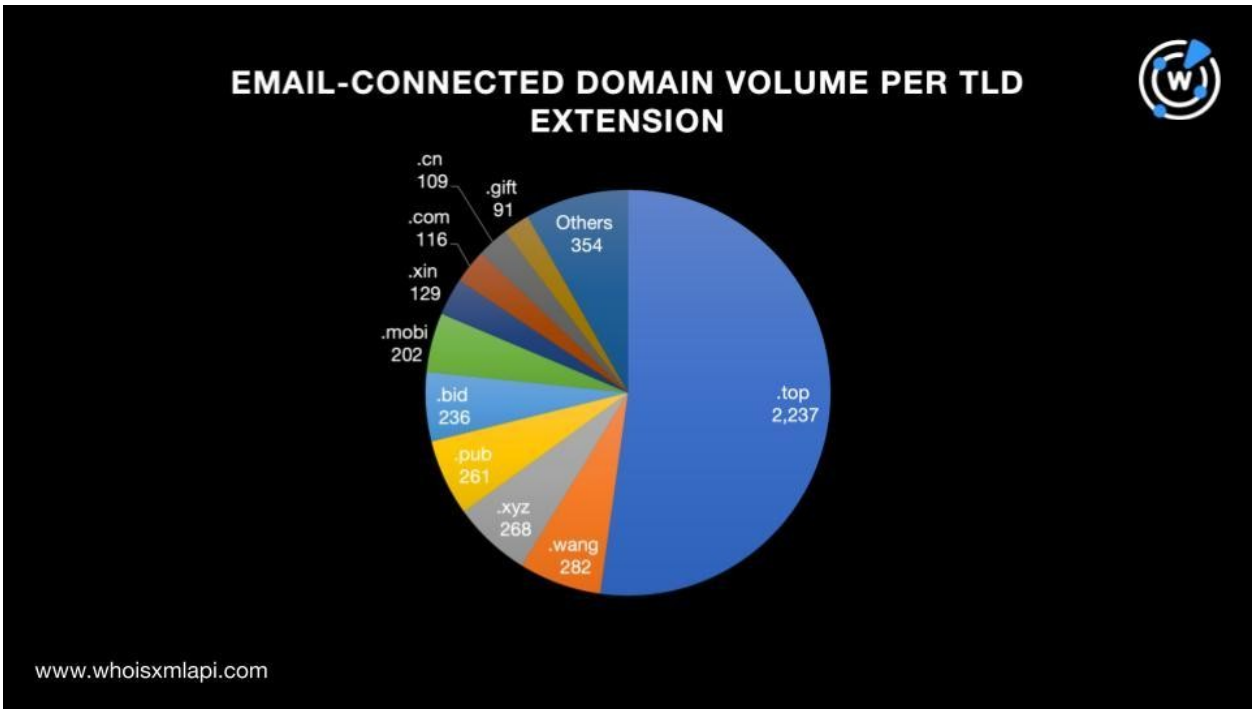
IoC関連のDNS調査結果

WhoisXML APIの研究チームが未報告の関連アーティファクトを探すにあたり、まず調査範囲を絞る必要がありました。

そこで、ドメイン名の登録に使用されたことがあるIoCメールアドレス79個に対してReverse WHOIS Searchを実行し、最近登録された500個以下のドメイン名で登録者メールアドレスとして使用されたものだけを今回の調査対象とすることにしました。その結果、合計4,284個のドメイン名の登録に使用された35個のメールアドレスが残りました。以下の表は、メールアドレスごとの登録ドメイン名数を示しています。



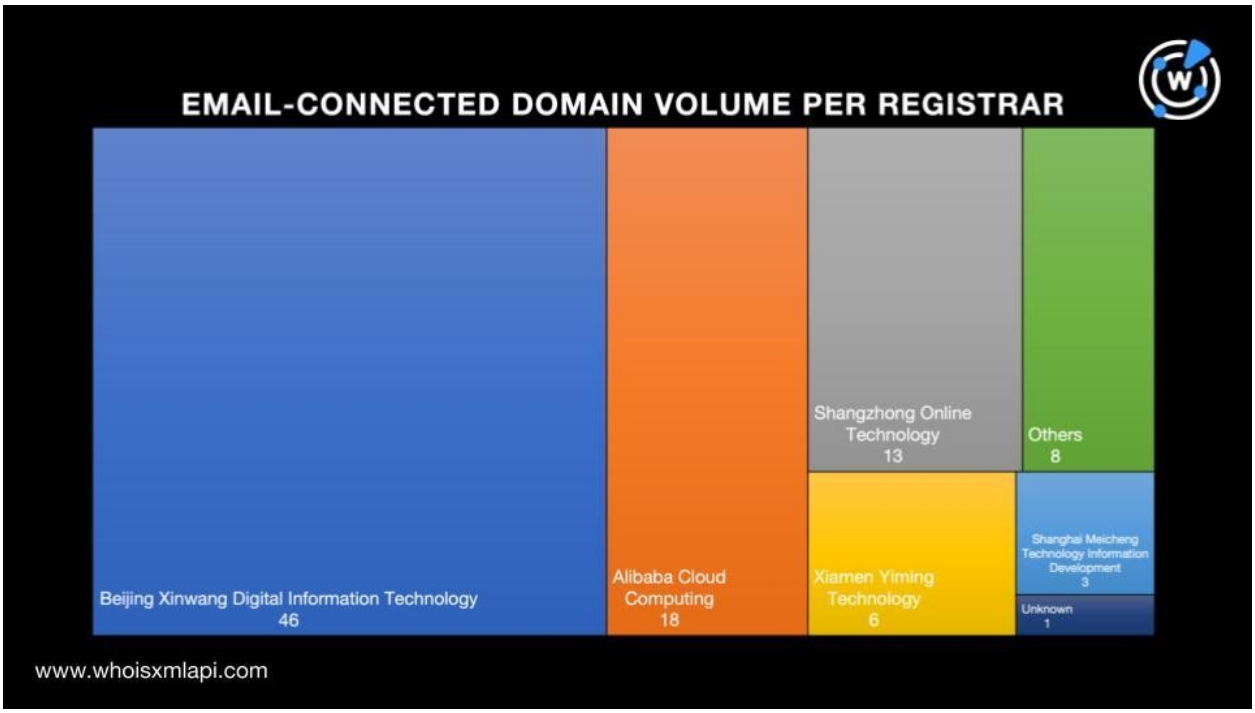
4,284個のドメイン名をさらに精査したところ、大多数の2,237個が、Danchevの指摘通り.topのドメイン名でした。登録ドメイン名数の多いTLDトップ10は、1位の.topに次いで.wang（282個）、.xyz（268個）、.pub（261個）、.bid（236個）、.mobi（202個）、.xin（129個）、.com（116個）、.cn（109個）、.gift（91個）となりました。残りの354個のドメイン名は、別の27のTLDに分散しています。以下はTLDごとのドメイン名数を示したものです。



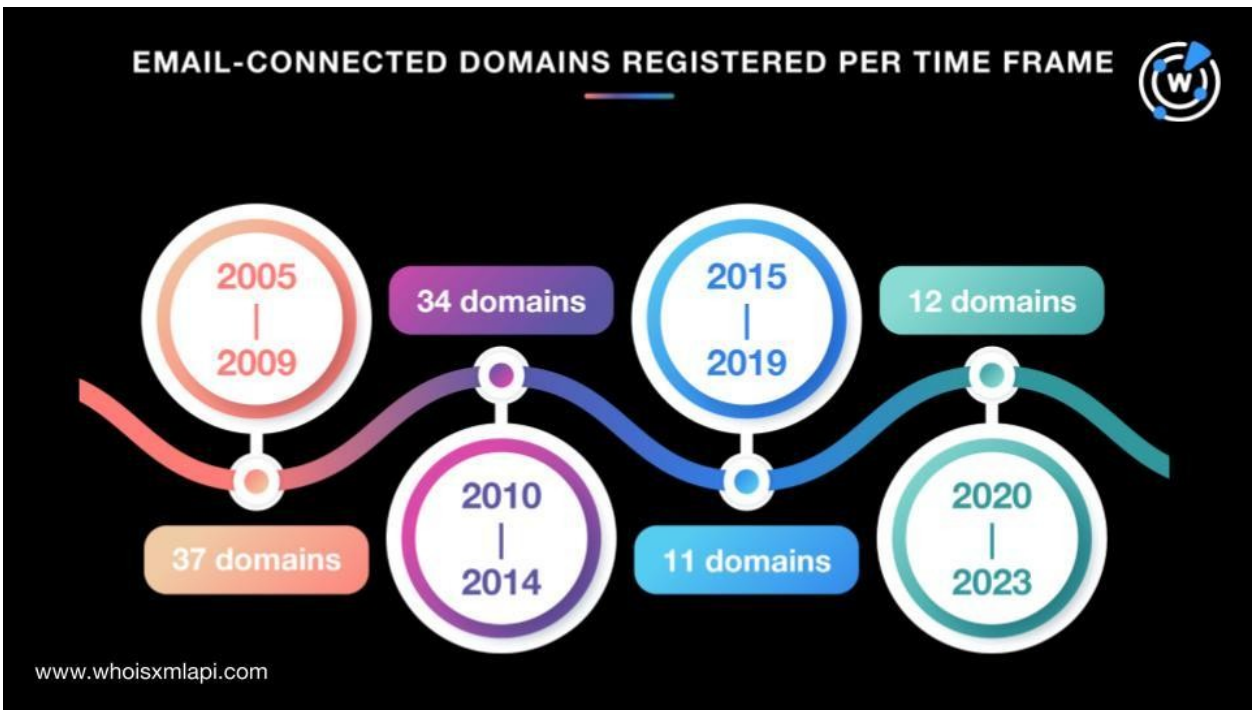
フィッシング詐欺師は、gTLD、特に.topのドメイン名を好んで使用していたことが推測できます。しかし、トップ10に.cnが含まれていることから、ccTLDのドメイン名も悪用していたようです。

また、上述の4,284個のドメイン名についてBulk WHOIS Lookupを実行したところ、以下のことがわかりました。

- その時点でアクティブなWHOISレコードを持っていたドメイン名は95個のみ
- その大部分である46個は、Beijing Xinwang Digital Information Technologyを介して登録。トップ5レジストラの2位以下は、Alibaba Cloud Computing（18個）、Shangzhong Online Technology（13個）、Xiamen Yiming Technology（6個）、Shanghai Meicheng Technology Information Development（3個）。8個のドメイン名は別の8レジストラに分散。1個は公開のレジストラデータなし。以下は、レジストラごとのドメイン名数を示したものです。



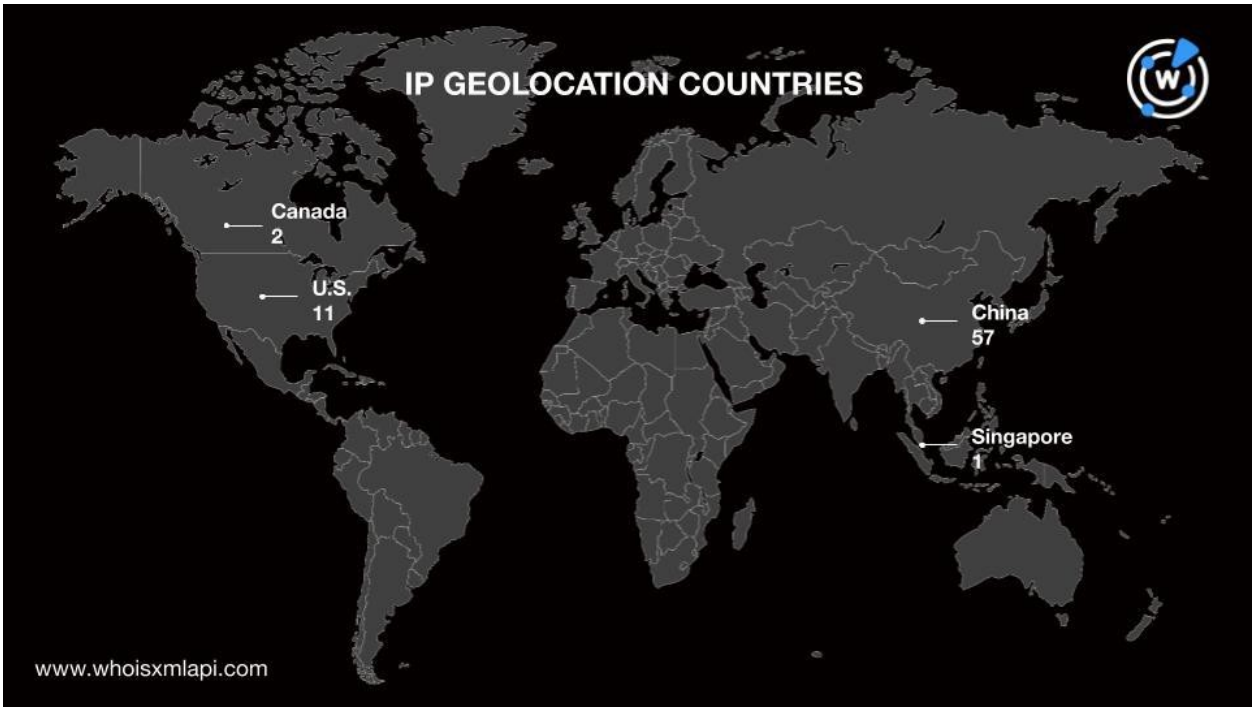
- IoCのメールアドレスを使用して登録され、かつWHOISレコードを取得可能なドメイン名のうち最多の14個は、2021年に登録されたものでした。他方、1個は登録日が公開されていませんでした。以下は、登録時期別のドメイン名数の内訳です。



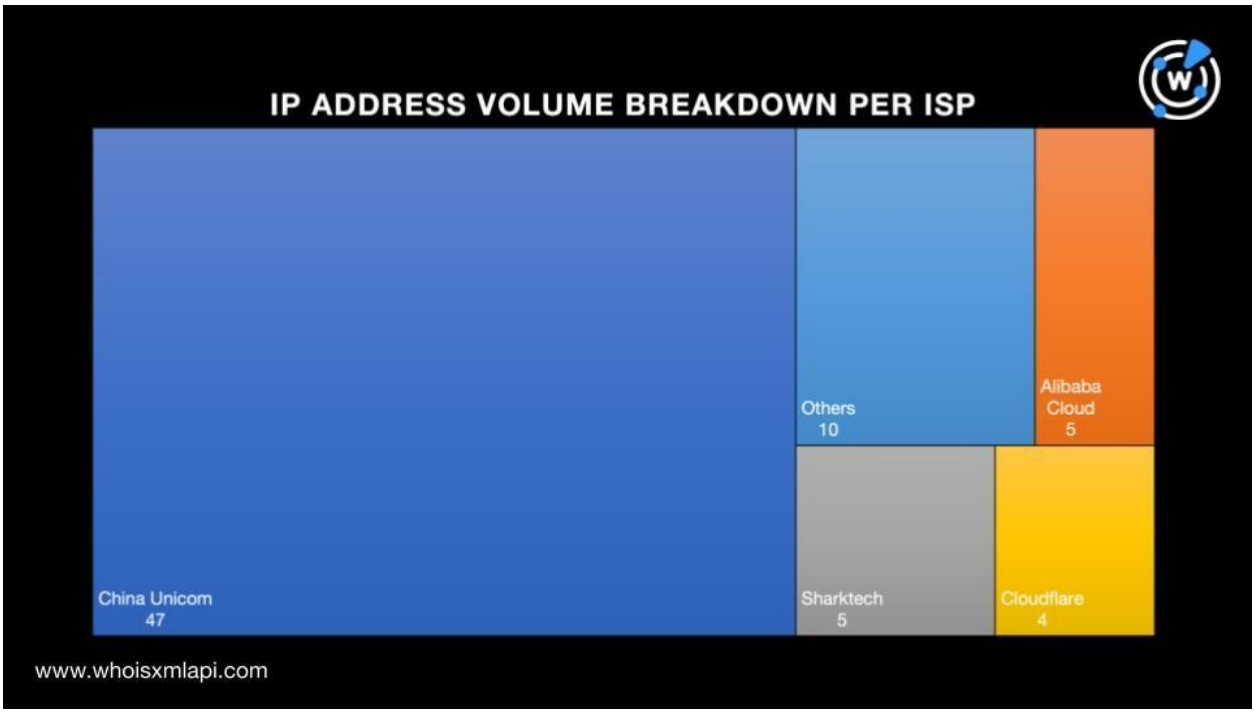
- 登録された国が見える状態になっていたのはcnlegaldata[.]comのみで、米国でした。

次に、4,284個のドメイン名をDNS Lookupにかけたところ、以下のことがわかりました。

- IPアドレスに名前解決したドメイン名は99個のみ
- それらのドメイン名が解決したのは71個のユニークなIPアドレス。そのうち2個はマルウェアチェックの結果悪意があることが判明
- それらのIPアドレスの大半である57個は、中国に位置。残りの14個は、米国（11）、カナダ（2）、シンガポール（1）に分散。以下はこの調査結果をまとめたものです。



- 管理IPアドレスが多いISPのトップ3は、China Unicom（47個）、Alibaba CloudとSharktech（各5個）、Cloudflare（4個）。残りの10個のユニークIPアドレスは、Hangzhou Alibaba AdvertisingとTencent（各2個）、Zenlayer、China Telecom、Cloudie、Confluence Networks、Hong Kong Communications International、UCloud Information Technology (HK)（各1個）に分散。以下は、ISPごとの管理アドレス数を示しています。



これらのIPアドレスについてさらにOSINT調査を進めたところ、本稿執筆時点で、208[.]91[.]197[.]46がAbuseIPDBで5回報告されていることがわかりました。

最後に、71個のIPアドレスを共用しているドメイン名を特定するため、それらのIPアドレスをReverse IP Lookupで検索しました。その結果、以下が明らかになりました。

- 61個のIPアドレスが、現在までドメイン名のホストを継続
- そのうち57個はおそらく専用ホスト
- 合計すると、専用と思われる57個のIPアドレスが890個のドメイン名をホスト

上記の調査で判明したドメイン名のうち悪意があると確認できたものはありませんでしたが、少なくとも2個、すなわちasicskids[.]comとtomfordeyewear[.]comは、疑わしいかもしれません。これらは文字列に人気ファッションブランドの名前を含んでいます。しかし、ASICSとTom Fordの公式ドメイン名のWHOISレコードとそれぞれを比較したところ、上記2ドメイン名のいずれも、ASICSとTom Fordへの帰属を公開のWHOIS情報から確認できませんでした。

また、5個のドメイン名に**bank**という文字列が含まれている点にも注目しました。それらのうち正規の銀行を模倣していると思われたのは3個（grandbank[.]cn、nanjingbank[.]com[.]cn、ruifengbank[.]com）だったものの、5個の全てがフィッシングに悪用される危険性をはらんでいます。

—

今回行ったDNSの徹底調査で、脅威への関連が疑われるアーティファクトが5,245個発見され、その大半が.topドメイン名でした。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、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：アーティファクトとIoCの例

IoCとして特定されたメールアドレス

- 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

IoCのメールアドレスを使用して登録されたドメイン名の例

- 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

IPアドレスの例

- 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

悪意あるIPアドレスの例

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

IPアドレスを共用していたドメイン名の例

- 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