国際的詐欺にWHOISとDNSのスポットライトを当てる

目次

要旨

スキャマーや詐欺師は昔から世界中でユーザーを悩ませてきました。当社のDancho Danchevのような脅威リサーチャーは、悪意あるキャンペーンの可能性を明らかにするために、深く掘り下げた調査に使用できるセキュリティ侵害インジケーター（IoC）を常に収集しています。

Danchevは最近、国際的な詐欺キャンペーンで使われた未編集のメールアドレスを3つ特定しました。そこで、当社でそのIoCをもとに調査を横展開し、以下を含む3,751個のアーティファクトを追加で特定しました。

- それらのメールアドレスを利用して登録した75個のドメイン名。うち5つは悪意あるドメイン名と確認
- それらのメールアドレスを使って登録されたドメイン名をホストしていた9つのIPアドレス。そのうち3つにはマルウェアが仕込まれていることを確認
- IoCのIPホストを共有する1,811個のドメイン名。そのうち6つはマルウェアホストであることを確認
- 共通のメールアドレスまたはIPアドレスを使っているとして当社が特定したドメイン名と同じブランド名を文字列に含む1,856個のドメイン名。そのうち61個は悪意あるドメイン名と確認

WHOISに関連した発見

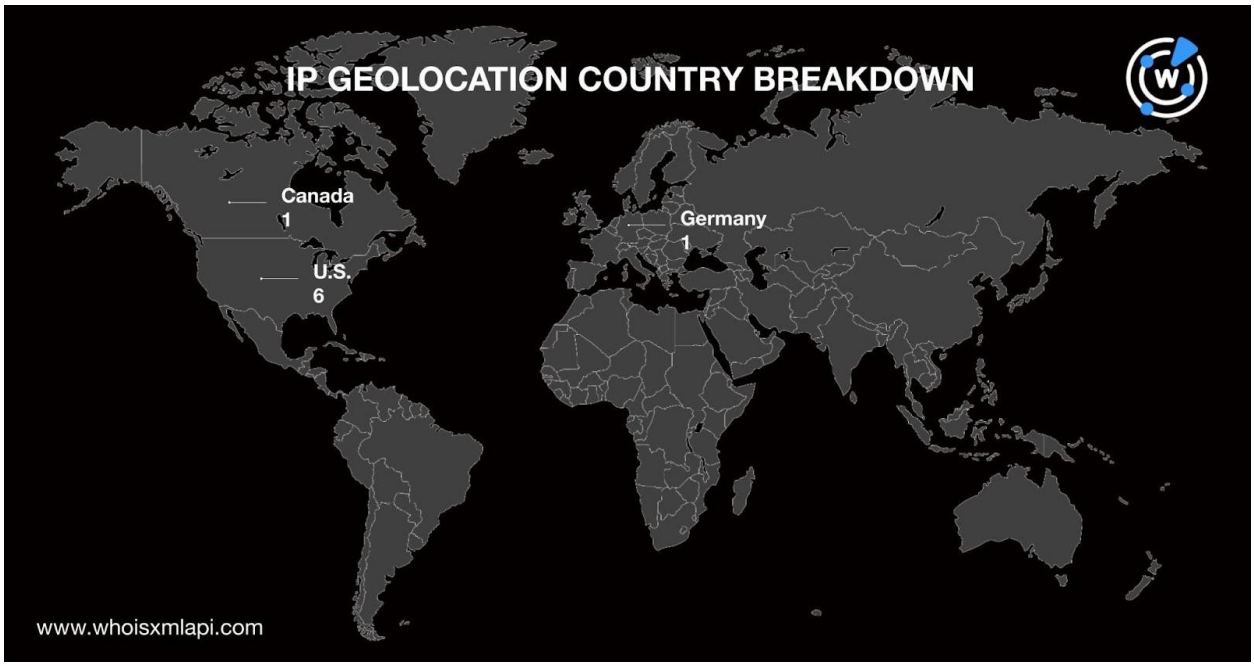
まず、IoCである3つのメールアドレスを使って登録されたドメイン名をReverse WHOIS Searchで探すことから調査を開始しました。その結果、75個のドメインが特定され、そのうち5個が悪意あるドメイン名であることが判明しました。

悪意あるドメイン名のうち2つはアクセス不能になっていましたが、他の2つ（astralair[.]comとsahinler-tr[.]com）は、売りに出ているようでした。残りの1つのドメイン名はパーキングされていたものの、その見た目（usa-irs[.]com）から、米内国歳入庁（IRS）をテーマにした詐欺に関与した可能性があります。

DNSに関連した発見

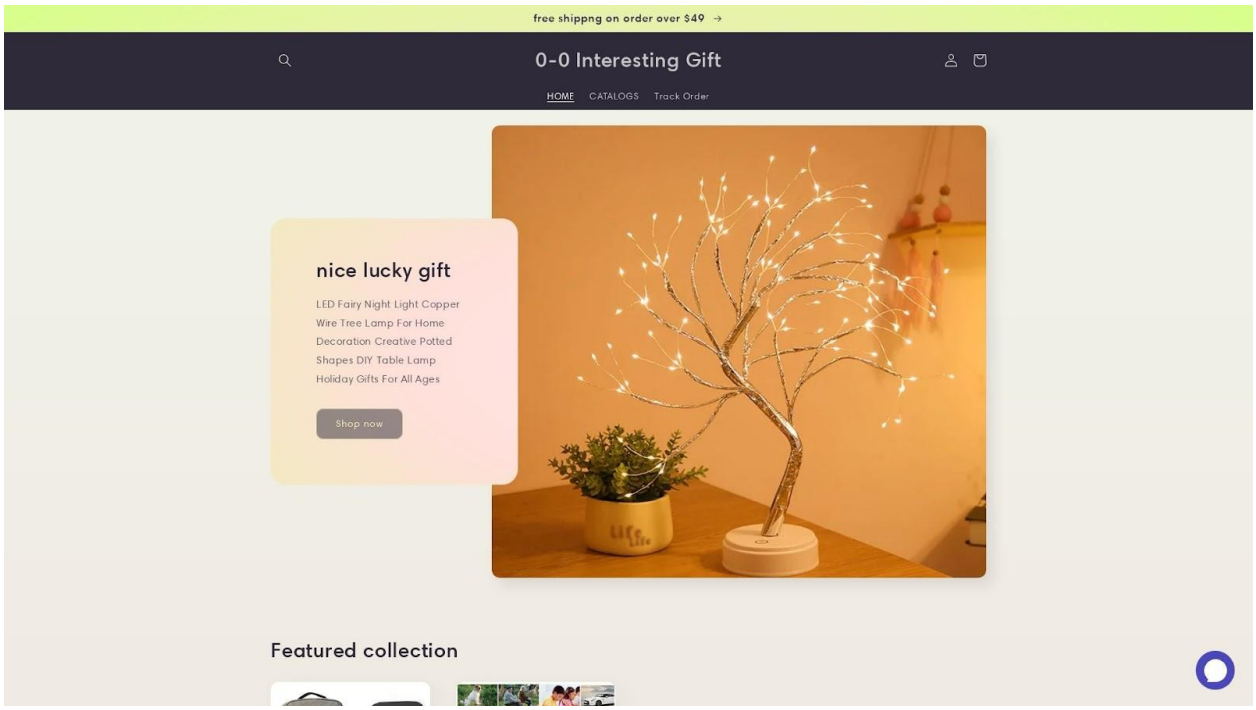
次に、共通のメールアドレスを使っていたドメイン名をDNS lookupsで検索したところ、9個のIPアドレスに名前解決しました。そのうち3個は、マルウェアホストと確認されました。

それらのIPアドレスをIP geolocation lookupsにかけた結果、そのほとんどが北米に位置していることがわかりました。具体的には、米国に6個、カナダに1個、ドイツに1個ありました。また、地理的位置が不明なアドレスが1個ありました。



7個のIPアドレスは300超のドメイン名で共用されていた一方、残りの2個はプライベートアドレスのようでした。104[.]253[.]92[.]243に名前解決したドメイン名が6個、154[.]64[.]232[.]58に名前解決したドメイン名が1個だけありました。

次にそれらのIPアドレスをreverse IP/DNS lookupsで調べた結果、さらに1,811個のドメイン名が見つかり、そのうち6個がマルウェアホストと確認されました。最も興味深かったのは0-0[.]icuというドメイン名で、買い物をした訪問者に無料の景品を配布するコンテンツをホストし続けていました。無料サービスはスキャマーの典型的な手口です。



0-0[.]icuのスクリーンショット

これまでに追加で発見されたアーティファクトを詳しく見てみると、金融サービスプロバイダー（PayPalなど）、銀行（HSBCなど）、郵便サービスプロバイダー（FedExなど）、政府機関（IRSなど）、国際機関・非政府組織（NGO）（国連など）の名前を含むものが多くありました。

今後詐欺に使われ得るアーティファクトをより多く見つけるため、下表の通り、それらのブランド名を含む文字列を検索キーワードとしてDomains & Subdomains Discoveryで調べました。なお、今回は2023年1月1日以降に登録されたドメイン名に限定して検索しました。

ブランド名	検索文字列
PayPal	***paypal***
HSBC	***hsbc***
IRS	***irs + us*** （文字列***first***を含むものなど、明らかな誤検出を除く）
Absa Bank	***absabank***
Zenith Bank	***zenithbank***

Western Union	***westernunion***
FedEx	***fedex***
TD Canada Trust	***canadatrust***
Halifax	***halifax***
FBI	***fbi + us*** （明らかな誤検出を除く）
UN	***unitednations*** （誤検出をできるだけなくすため、文字列***un***は使用せず）
Samsung	***samsung***
First Bank	***firstbank***

その結果、さらに1,856個のアーティファクトが見つかり、うち61個には悪意があることが判明しました。また、***track***、***trace***、***online***、***service***など、ブランド名と共によく使われる文字列は、以下のワードクラウドに示されています。

ブランドを含んだ複数のドメイン名で見つかったこれらの文字列は、詐欺のページやフィッシングサイトを指し示すURLに多く見られます。

—

国際的な詐欺師が使用する3つのメールアドレスを出発点として、当社でそれらのWHOISとDNSレコードを精査した結果、将来に詐欺ページのホストとなり得る3,700個以上のドメイン名が見つかりました。そして、そのうちの72個はすでに悪意あるものとしてタグ付けされていたことがわかりました。

同様の調査をご希望のお客様、またはこの調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

脅威のIoCとして特定されたメールアドレス

- adamsco[REDACTED]@gmail[.]com
- circu[REDACTED]@yahoo[.]fr
- ikecgigo[REDACTED]@gmail[.]com

注：プライバシー保護のため、メールアドレスの一部を編集しています。

同じメールアドレスを使用していたドメイン名の例

- paypalservicecenters[.]com
- bioredox[.]fr
- astralair[.]com
- gmqgroup[.]com
- vatvetd[.]com
- alptekin-tr[.]com
- chnaglong[.]com
- hsbc--bnk[.]com
- usa-irs[.]com
- sahinler-tr[.]com
- onlineuklottery[.]com
- presidentialofficenig[.]com
- roman-py[.]com
- ecobannk[.]com
- absabankk[.]com
- tributariaaes[.]com
- kajariiaceramics[.]com
- zenithbanknig[.]com
- goldsseller[.]com
- westetnunonn[.]com

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の例

- paypalservicecenters[.]com
- astralair[.]com
- gmqgroup[.]com

同じメールアドレスを使用したドメイン名をホストしていたIPアドレスの例

- 217[.]160[.]122[.]44
- 104[.]253[.]92[.]243
- 23[.]227[.]38[.]65
- 162[.]255[.]119[.]7
- 10[.]10[.]10[.]10

悪意あるIPホストの例

- 23[.]227[.]38[.]65
- 165[.]160[.]13[.]20

同じIPアドレスを使用していたドメイン名の例

- a-manlikeme[.]com
- a11ylawyer[.]com
- a1403[.]asia
- a143kl-lc[.]site
- a1cosmetic[.]com
- a1fbg[.]com
- a1sbobet365[.]online
- a2hosst[.]com
- a2zbuyandsell[.]com
- a3-coal[.]com
- a78595172407fad071430bcabea7f0 63bd1792b9[.]unraid[.]net
- a7ong[.]cn
- a7projects[.]tech
- aaa[.]freeddns[.]org
- aaacybershield[.]co
- aaagl[.]shop
- aaainformer[.]com
- aadityasingh[.]live
- aahyjcfghjnc[.]com
- aajiqzt[.]cn
- aalmadan[.]com
- aalsmeermassage[.]com
- aamit[.]co
- aamupotti[.]com
- aandldesigns[.]co[.]uk
- aapn[.]us
- aariakalra[.]com
- aaronhawkey[.]com
- aarubipricecompare[.]com
- aasellers[.]co
- aatom[.]com
- aaveeye[.]com
- aawzxdm[.]cn
- aaxfgbnx[.]com
- aaxlon[.]com
- aazo[.]info
- abaanhouse[.]com
- abalancedone[.]com
- abbeybuilder[.]com
- abbyrohosting[.]com
- abc-konfigurator[.]de
- abcd[.]ad
- abdulhadi[.]us
- abduloseni[.]com
- abernathtree[.]com
- aberracion[.]com
- abgleich-242942342[.]info
- abgqqcashpkv[.]com
- abhiravi[.]com
- abilenetxapartments[.]com
- abilitilab[.]com
- abinterlors[.]com
- abktravel[.]bh
- able-it[.]uk
- abodespace[.]com
- abogadosinmigracion[.]com
- abolandmarketing[.]com
- abolishdoe[.]org
- abolition[.]fyi
- aboplay303[.]com
- aboslot99[.]com
- aboutboxwood[.]com
- aboutitall[.]com
- aboutjameslee[.]com
- aboutnft[.]io

- abp-mail[.]net
- absoluteactiontoys[.]com
- absolutelycleaner[.]pro
- absolutelydarling[.]net
- absorbtive[.]com
- absraihan[.]com
- abstestest[.]com
- abubakar[.]digital
- abundantprivilege[.]com
- abundanttrees[.]com
- abuniverstiy[.]org
- aburghortsociety[.]ca
- abyat[.]healthcare
- acaboysmoving[.]com
- acaciagroves[.]net
- academiadelaplenitud[.]com
- academictec[.]click
- academicwebdesign[.]org
- academy-of[.]life
- academyofunstoppablewomen[.]co
- acaicorp[.]com
- acbadaio[.]xyz
- accelerator[.]guru
- acceliohq[.]com
- accentheatlh[.]com
- accesssellars[.]com
- accesstoloans[.]com
- accolade[.]llc
- accommodatecloud[.]com
- accountantunitedkingdom[.]com
- accountinglessonswithbcv[.]com
- accousticspecialties[.]com
- accudo[.]co
- accuratеracks[.]com
- accurx-co[.]uk

同じIPアドレスを使用していた悪意あるドメイン名の例

- 0-0[.]icu
- 1099[.]healthcare
- 86e50883b9b2159b17a69ab43873b22c[.]xyz

同じメールアドレスを使用していたウェブプロパティのうち、ブランド名を含んだドメイン名の例

- xn--papal-rva[.]vg
- xn--paypa-rnb[.]vg
- xn--ppl-9kal6o[.]ws
- xn--ppl-9kal6o[.]vg
- xn--paypa-rnb[.]ws
- xn--papl-2na8p[.]ph
- xn--aypal-ipb[.]vg
- xn--pypl-0nac[.]ph
- xn--papl-6ra3466b[.]vg
- xn--pypal-rwa[.]ph
- paypals[.]su
- paypall[.]xn--fiqs8s
- cpaypal[.]in
- paypal-x[.]hk
- xn--paypa-we3s[.]arab
- paypalll[.]it
- ampaypal[.]com
- paypalv1[.]com
- paypalcn[.]top
- paypal-iv[.]vg
- hsbcft[.]cn
- hsbcco[.]id
- hsbcbnk[.]in
- hsbcuk[.]cfd
- hsbcsec[.]cn
- hsbcc[.]info
- eohsbch[.]cn
- thsbcyp[.]cn

- hsbcaz[.]com
- hsbcjt[.]net
- hsbcrb[.]com
- hsbc-my[.]co
- 21hsbc[.]org
- xn--sc-cfb4024b[.]com[.]ph
- hsbc-com[.]cn
- hsbcnet[.]xn--ngbrx
- hsbcitl[.]com
- bnphsbc[.]com
- xn--bc-c9a5820a[.]com[.]ph
- hsbcprod[.]ph
- irs-us[.]site
- irsfederal[.]us
- irsusa-tax[.]com
- irsprograms[.]us
- wuw-irsform-usa[.]com
- www-irs-forms-us[.]top
- paymentabsabanks[.]com
- paymentabsabank[.]co[.]za
- zenithbank[.]ltd
- hackzenithbank[.]com
- awesternunion[.]com
- westernunion[.]help
- westernunionpk[.]com
- westernunionpi[.]com
- westernunionfn[.]xyz
- mywesternunion[.]xyz
- bwesternunionvl[.]vip
- fwesternunionvl[.]vip
- awesternunionvl[.]vip
- usawesternunion[.]com
- fedexn[.]us
- fedext[.]cc
- fedexd[.]cc
- fedexb[.]cc
- fedexf[.]cc
- fedexv[.]pw
- fedexp[.]pw
- fedexl[.]pw
- fedexp[.]cc
- fedexl[.]cc
- fedexr[.]cc
- fedexx[.]pw
- ffedex[.]pw
- fedexq[.]pw
- fedexk[.]pw
- fedexs[.]us
- fedexn[.]pw
- fedexo[.]cc
- fedexy[.]pw
- fedexe[.]pw
- canadatrust-td[.]com
- canadatrustedmed[.]com
- Interac100web-canadatrust[.]com
- et-canadatrust-onlinewebca[.]com
- 1001-loginweb-canadatrustca[.]com
- et-interac1001-canadatrustweb[.]com
- halifaxre[.]org
- halifaxfe[.]com
- ucshalifax[.]ca
- gchalifax[.]net
- halifaxre[.]net
- halifaxrx[.]com
- halifaxmt[.]com
- gchalifax[.]com
- halifaxfe[.]org
- halifaxfe[.]net
- halifaxmts[.]com
- halifaxas[.]cyou
- ppshalifax[.]com
- hr-halifax[.]com

共通の文字列を含んだ悪意あるドメイン名の例

- tbpaypal[.]com
- japaypal[.]com

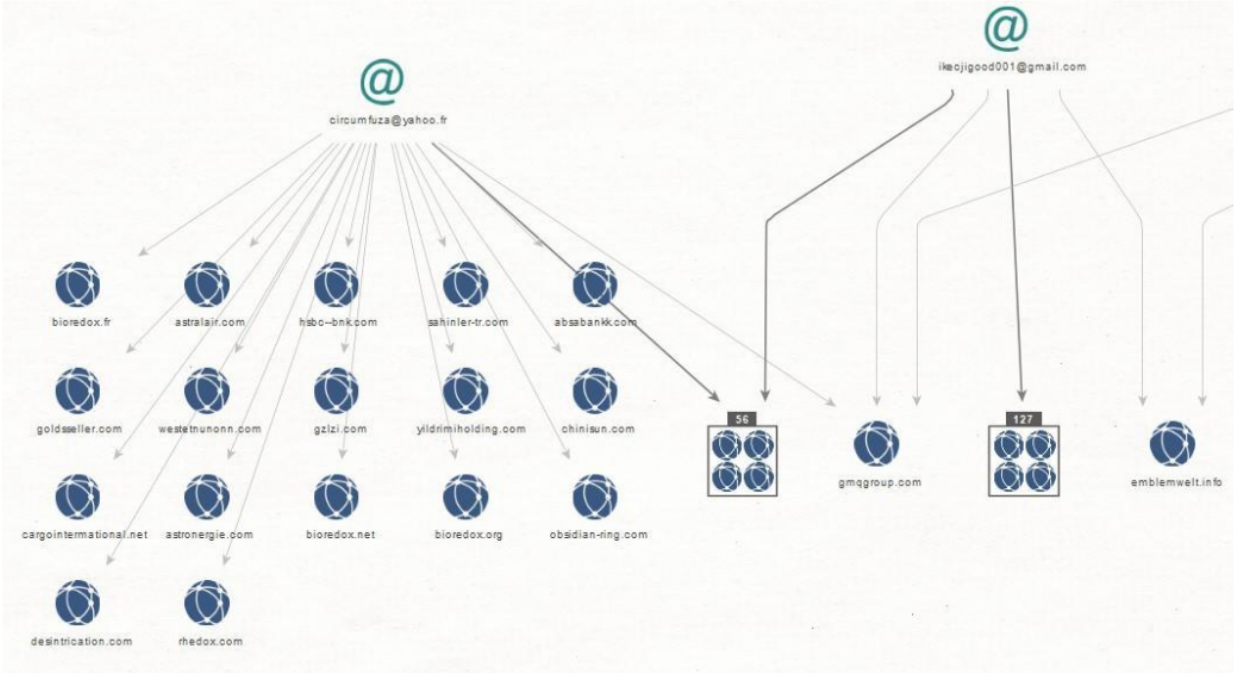
- paypalyydwpww[.]com
- paypal-service[.]top
- mypaypalservice[.]xyz
- paypal-payments[.]xyz
- paypal-security-us[.]com
- assistance-paypal[.]info
- paypall2023validath[.]top
- login2-paypalservice[.]top
- paypalverificationsms[.]com
- helpandsupport-paypal[.]com
- paypalsecure03-account[.]com
- onlinecasinowithpaypal[.]co[.]uk
- paypalverification02account[.]com
- aktualiserungs-service-paypal[.]xyz
- howtouseanotheruserpaypal[.]business
- hsbcltd[.]online
- hsbc-secure[.]live
- hsbc-online[.]live

OSINT分析

悪意あるキャンペーンへの関与が判明しているドメイン名の例

britishimmigrationvisa.co
international-cargo-transporting.com
mail-pay.de
instantbox.info
mail-pay.org
uba-forex.org
whitfieldinspires.com.ng
bsdevelopment.com
nrfcollection.com
gmqgroup.com
aseycon.com
emblemwelt.info
terekilpane.com
mondiaz.com
scotiabankmobiletrinidad.com
vanothuisebv.com
championbluefrenchies.com
allbulldogpuppies.com
nayzeth.com
universalglobalcompany.com
alexramirezlmft.com
standarddeliveryservice.us
depictedme.com
ameriunited.us
highranksearchpros.com
ichaonya.us
senatorcrewing.com
nametest.us
inkbombers.com

end-time-prophecy.info
fojolostrichranch.com
cebuhash.org
6x4.photography
metrobankplc.credit
violetcrew.biz
pragenmetis.com
lucid-is.com.ec
lloydsbank.cam
cfrc.us
atlantia.group
sunlifefsc.us
realtor-department.com
coperatefinance.biz
uskgroup-corp.com
bankofengland.net.in



応答したIPアドレスで、キャンペーンへの関与が判明しているものの例
208.91.197.44
36.86.63.182
185.224.138.195
91.195.241.137

218.93.250.18
103.120.80.144
108.175.2.227
198.54.117.211
192.195.77.237
104.192.6.220
91.195.240.13
162.255.119.116
47.91.107.43
198.54.117.200
23.195.69.108
209.99.40.222
198.54.117.199
198.54.117.197
198.54.117.198
104.152.168.42
23.202.231.168
23.253.126.58
104.239.157.210
23.195.69.112
199.79.63.241
52.4.209.250
199.79.63.239
199.79.63.227
199.79.63.243
199.79.63.110
212.224.112.92
185.181.104.82
209.99.16.240
91.195.240.94
5.187.3.228
91.235.116.180
13.248.196.204
204.11.56.41
208.91.196.34
185.224.137.145
104.18.61.151
104.18.60.151
170.178.168.203
127.0.0.4
68.183.250.107
104.27.132.171
8.5.1.31
208.91.197.46

104.27.133.171
204.11.56.48
209.99.40.223
91.195.240.87
158.255.6.169
108.163.184.66
199.168.189.152
173.212.207.177
173.212.207.183
192.185.4.166
198.54.117.212
173.212.207.184
80.211.196.184
54.208.174.161
35.203.68.147
52.201.19.170
184.168.221.34
34.196.72.62
50.63.202.52
3.140.13.188
185.230.60.161
18.119.154.66
185.230.63.96
185.148.144.161
81.91.170.22
47.88.84.51
54.95.146.233
38.26.155.227
47.91.205.63
154.91.52.182
209.99.64.33
108.179.217.243
146.112.61.107
46.17.101.39
199.59.243.221
199.59.243.201
46.17.101.36
199.59.240.200
199.59.243.211
91.195.240.117
174.138.191.187
131.153.51.122
166.78.101.108
67.227.226.240

104.24.126.85
18.232.40.189
216.58.208.211
107.190.141.194
192.64.119.247
3.91.125.102
149.56.251.98
23.22.216.95
184.72.224.62
54.209.191.40
69.162.115.82
184.154.45.10
66.147.244.166
69.172.201.208
131.153.51.26
173.236.72.116
80.251.18.8
199.168.189.130
173.236.72.115

キャンペーンへの関与が知られている関連ドメイン名の例

ecobannk.com
instantbox.info
roman-py.com
weeknd.info
tributariaaes.com
gardencare.us
absabankk.com
nanobox.us
zenithbanknig.com
kajariiaceramics.com
instantbox.club
westetnunonn.com
goldsseller.com
alptekin-tr.com
fbigovuk.com
vatvetd.com
hsbc--bnk.com
chnaglong.com
sahinler-tr.com
deblobe.com
usa-irs.com
nascartz.com
presidentialofficenig.com

perfectview.us
anwalt-arbeitsrecht-stuttgart.com
onlineuklottery.com
top10party.com
premierleagueaction.com
letstalkpremierleague.com
bnkkofameric.com
bioredox.fr
astralair.com
firstinlndbnk.com
caixiabankk.com
tjmorrisltd.com
milestoneslr.com
brookchems.com
ghmnister.com
marex-commodiities.com
fbiigvus.com
unite-sgp-police.fr
sanntedder.com
ecobnkbb.com
mail-pay.fr
cellmarkk.com
alm-interr.com
aolmall.org
arpas.net
mail-pay.org
llosdybnkgroup.com
mail-pay.de
alinyuns.com
mail-discover.com
fesil-salers.com
intl-pay.de
tainqilithiuim.com
mail-pal.de
taechins.com
santefram.com
sabalanipico.com
emblemwelt.info
shgenerals.com
pidecc.com
sanrdoz.com
pie-tw.com
janus-sersvices.com
albadder-oil.com

amgcorporate.xyz
db-hg.com
alaestur.com
eawmlik.com
priostanbul.com
chinaecece.com
lloydsbnkgrouptsb.com
traffigura.com
petrokishs.com
frontiers-property.com
frontiersfinancialservices.com
nbjeiiju.com
tousdoc.com
astronergie.com
mesphotosenligne.com
hangertionm.com
propertyfrontiers.com
bioredox.org
bioredox.net
frontierswealthmanagement.com
desintrication.com
dan-danielnigenterprisesltd.com
obsidian-ring.com
frontiersfundmanagement.com
frontiersproperty.com
rhedox.com
schwarzwald-erleben.info
samsung-won.com
elitrade-hk.com
swk-tashi.com
faragella.com
ghmnster.com
trasurequest.com
frontiersassetmanagement.com
treasurerquest.com
sanatnader.com
hughesndhughesca.com
samsunguk.co
frontiersinvestmentmanagement.com
firsttbank.com
calespascaul.com
halifx-bank.net
westfiesi.com
jebsen-jessen.net

chocteak.com
ifcnig.org
trafigiura.com
fbi-govvus.com
cocfco.com
halifax-bankplc.com
wplpproducts.com
uniteddnation.org
alphapowerengineerings.com
guarantybondbnk.com
hienzelsales.com
chinametals-tw.com
bernasmy.com
raremetal-jp.com
aggrodif.com
simamarlneafrica.com
imsss-co.com
allacesscreditbank.org
pgpgva.com
cargointermational.net
siantycorp.com
thenigerianpolice.org
orangefieild.com
nationallotery.org
jctc-ceramisc.com
scholarshipsnigeria.org
vantagers.info
nevwenta-ru.com
tdcanada-ttrust.com
uba-forex.org
eacs-corp.com
learnfastbyshelton.com
ethoseneryggroup.com
stadchatteb.com
kkrka.biz
turkagroups.com
ftk-ruls.com
allm-inter.com
medictechsystem.com
allbader-oil.com
ni-zi.com
xn--rs-mja.com
amiitrading.com
fortunemeds.com

tbs-sct.com
chinatarrsglass.com
chinisun.com
mercatorpherma.com
alptekins-tr.com
gzlzi.com
fedexng.com
promofixdistribusion.com
yildrimiholding.com
genexgyroup.com
frieslandcamipina.com
cenbnknig.com
part-unltd.com
gmqgroup.com
end-time-prophecy.info
6x4.photography
uskinteractive.com
uskgroup-corp.com
usk-j.com
jamesnolan1465.com
dongbudaewoelec.com
novarplatik.com
ghminister.com
logisticsweden.com
firstinlanbnk.com
caxiabnk.com
db-frankfurt.com
hallifaxbbank.com
honeywell-flour.com
alma--stores.com
scbankng.com
dandanielnigenterprisesltd.com
sun-trustbnk.com
scbankuk.com
qater-ukraine.com
stilsimdi.com
tclceramic.xyz
scbankonline.org
unitednations-online.com
austalexpressasia.com
acountantgeneralofficeng.com
dbk-hg.com
nrfcollection.com
realtor-department.com

international-cargo-transporting.com
bsdevelopment.com
caixiabnk.com
ecobanknng.com
tdcanadturst.com
commeenpologne.net
satadder.com
imfus.com
zenithnankng.com
caixaibk.com
ecobanknngg.com
hsbcbnkk.com
furukawa-sg.com
sissecam.com
gmgqroup.com
nbjeiju.com
globalfinancesecurities.com
rdiesel-sg.com
novarplastik.com
lacaixiabnkk.com
lacaixabnkk.com
commeenpologne.fr
ecobnkb.com
santerfarm.com
grregpoole.com
sdmeic.com
fbiigovus.com
losalamosconcertassociation.com
le-mat.net
art-transformationnel.org
propertyfrontiersuk.com
studentpropertyinvestments.net
frontiersfoundation.info
salustech.org