A DNS Investigation of the Typhoon 2FA Phishing Kit

Table of Contents

Executive Report

Bleeping Computer recently reported that a phishing-as-a-service (PhaaS) available in cybercriminal forums dubbed "Typhoon 2FA" has the ability to compromise Microsoft 365 and Google accounts even if users have two-factor authentication (2FA) enabled.

Sekoia security analysts uncovered the phishing kit back in October 2023 though they believe it has been active since at least August of that same year. Over time, they have been updating their Typhoon 2FA list of indicators of compromise (IoCs), which to date comprises 55 domains and 48 subdomains.

In a bid to know more about Typhoon 2FA, the WhoisXML API research team expanded the current list of IoCs and found:

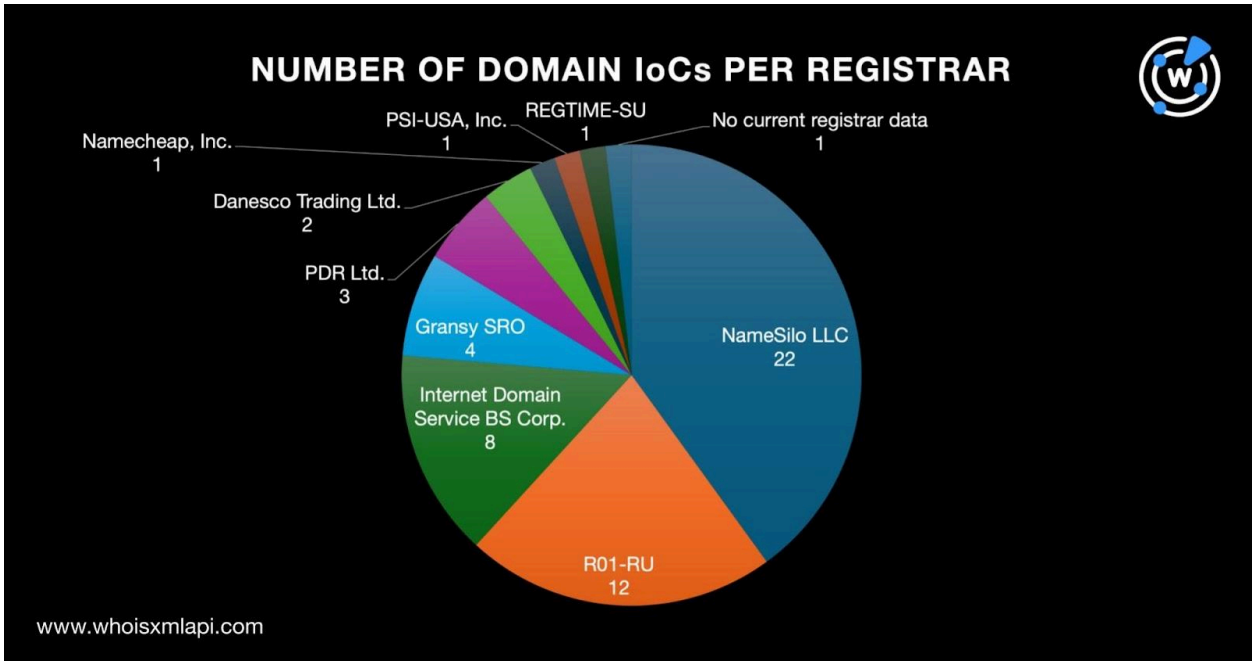
- 288 registrant email address-connected domains
- 110 registrant organization-connected domains
- 262 email-connected domains
- 21 IP addresses, all of which turned out to be malicious
- 137 string-connected domains
- 3,223 string-connected subdomains

A Closer Look at the Typhoon 2FA IoCs

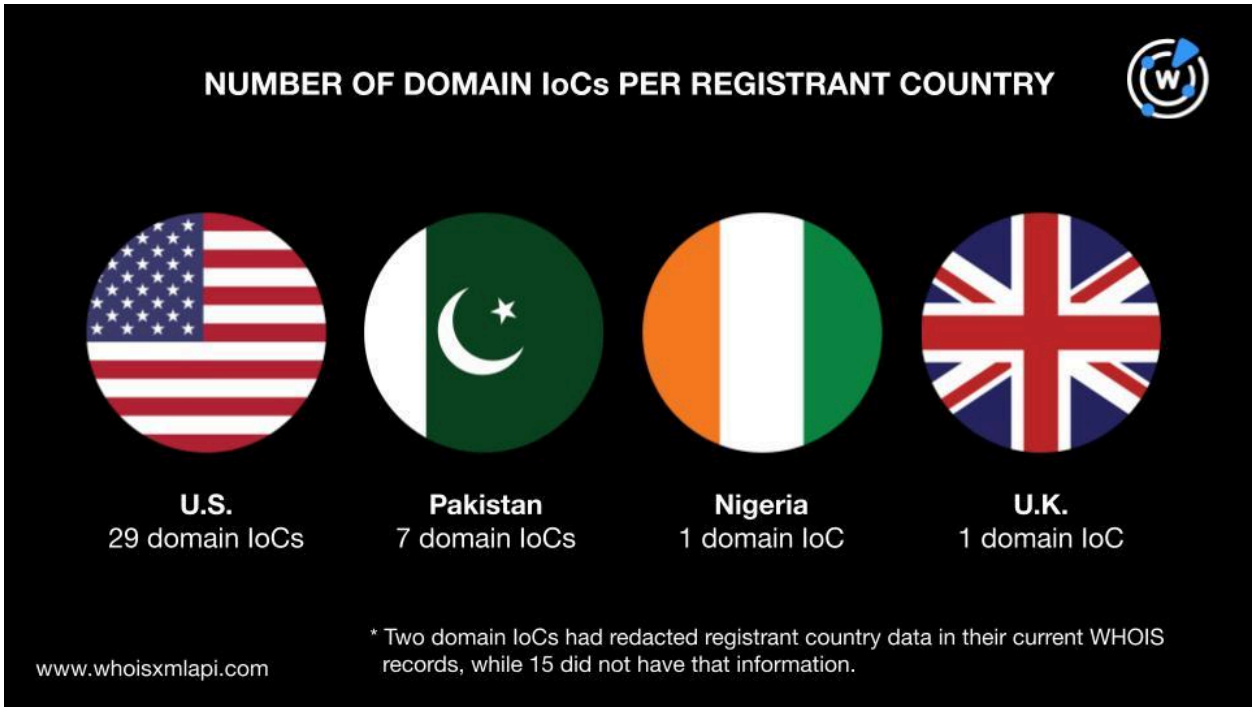
As our usual first step, we subjected the 55 domains identified as IoCs (48 of which were extracted from the subdomain IoCs) to a bulk WHOIS lookup, which revealed that:

- Their top 3 registrars were NameSilo LLC, which administered 22 of the domains tagged as IoCs; R01-RU, which furnished 12; and Internet Domain Service BS Corp., which provided eight. Gransy SRO, accounted for four domains, while Danesco Trading Ltd.

accounted for two. Namecheap, Inc, PSI-USA, Inc., and REGTIME-SU accounted for one domain IoC each. Finally, one domain did not have registrar data in its current WHOIS record.



- The domains classified as IoCs were created between 2023 (18 domains) and 2024 (36 domains), hinting that the Typhoon 2FA operators had a penchant for using newly registered domains (NRDs) in their campaigns. One domain named as an IoC did not have a creation date in its current WHOIS record.
- A majority of the domains categorized as IoCs, 29 to be exact, were registered in the U.S. Seven domains identified as IoCs were registered in Pakistan and one each in Nigeria and the U.K. The registrant countries of two domains tagged as IoCs were redacted. Finally, 15 domains classified as IoCs did not have current registrant country data.



- Four domains named as IoCs had registrant email addresses and names in their current WHOIS records, namely:
    - 3tdx2r[.]com
    - it2ua[.]com
    - lw8opi[.]com
    - tlger-surveillance[.]com
- Eight domains categorized as IoCs had registrant organization names in their current WHOIS records, namely:
    - 3qjpc[.]com
    - 3tdx2r[.]com
    - canweal[.]com
    - it2ua[.]com
    - lw8opi[.]com
    - m1p8z[.]com
    - tlger-surveillance[.]com
    - tnjxb[.]com

A DNS Deep Dive to Find Typhoon 2FA Connected Artifacts

To further investigate possible ties other digital properties may have to Typhoon 2FA, we expanded the current list of IoCs.

First, we looked for domains that shared some of the domain IoCs' registrant information using Reverse WHOIS Search and uncovered:

- 288 registrant email address-connected domains based on their historical WHOIS records
- 110 registrant organization-connected domains based on their historical WHOIS records

We then queried the 55 domains classified as IoCs on WHOIS History API and found 42 email addresses in their historical WHOIS records, 14 of which were public email addresses.

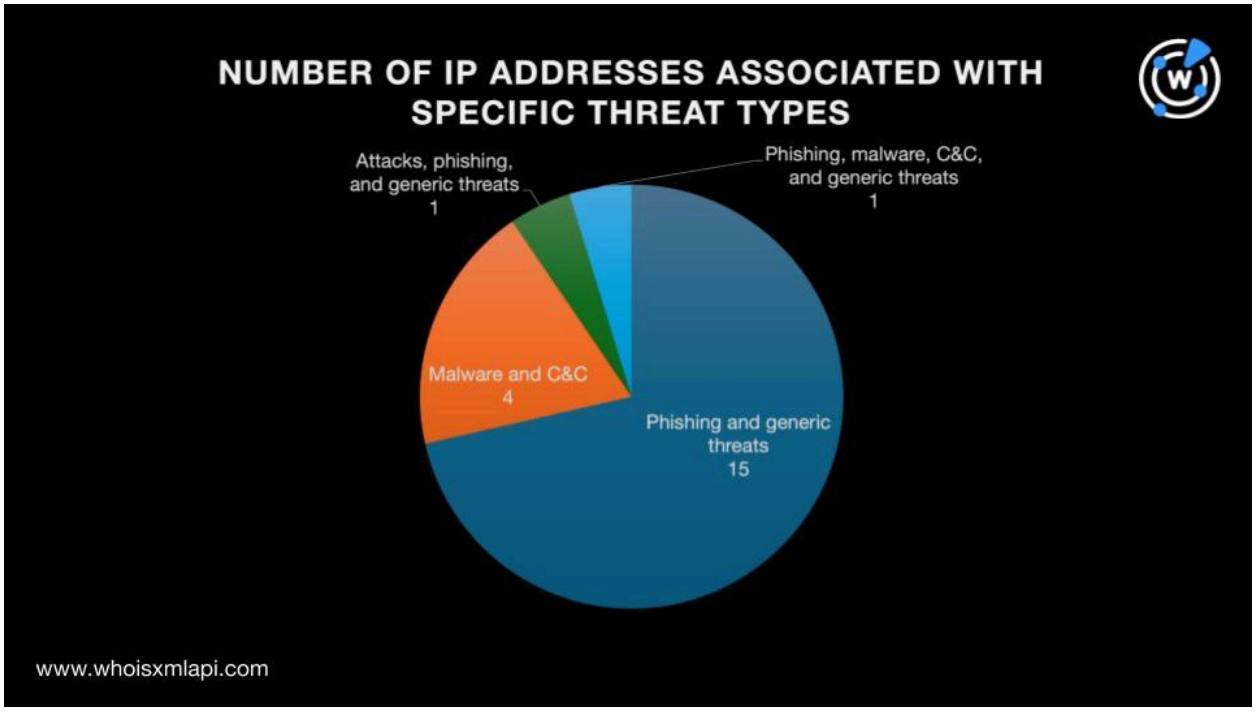
Next, we used the 14 public email addresses as Reverse WHOIS API search terms that led to the discovery of 262 email-connected domains after filtering out duplicates, the IoCs, and the registrant-connected (by email address, name, and organization) domains. A huge chunk of them seem to have been created using domain generation algorithms (DGAs) similar to the IoCs.

After that, we performed DNS lookups on the 55 domains categorized as IoCs that revealed they resolved to 21 unique IP addresses after removing duplicates.

A bulk IP geolocation lookup for the 21 IP addresses showed they were all geolocated in the U.S. A majority of them, 20 to be exact, were administered by Cloudflare, Inc., while one was furnished by Amazon.com, Inc.

Our Threat Intelligence API queries for the 21 IP addresses found that all were associated with various threats. In particular:

- 15 were associated with phishing and generic threats
- Four were connected to malware and command and control (C&C)
- One was related to attacks, phishing, and generic threats
- One was associated with phishing, malware, C&C, and generic threats



Reverse IP/DNS lookups for the 21 IP addresses revealed they were all shared hosts so we could not use any of them to find IP-connected domains.

So, we then trooped to Domains & Subdomains Discovery to uncover string-connected domains and subdomains resembling the IoCs.

- Eleven of the text strings found among the domains named as IoCs appeared in 137 string-connected domains after duplicates, the IoCs, and the registrant- and email-connected domains were filtered out. They were:
    - **7e2r.**
    - **codecrafters.**
    - **codecrafterspro.**
    - **fourth.**
    - **ilert.**
    - **m1p8z.**
    - **rexj.**
    - **sem01.**
    - **tk9u.**
    - **tycoongroup.**
    - **uqin.**
- Eight of the text strings present in the subdomains categorized as IoCs were also seen in 3,223 subdomains. They were:
    - **explore.**
    - **horizon.**
    - **libudi.**
    - **rlpq.**

- **tnyr.**
- **x12y.**
- **xrs.**
- **xrs.**

Interestingly, some of the subdomains contained misspelled variants of popular brands like amazon (explore[.]amazonpi[.]betamazon[.]instructure[.]com), netflix (explore[.]amcway[.]ciostage[.]netfliz[.]ca), apple (explore[.]apjle[.]beta[.]instructure[.]com), gmail (horizon[.]mpk[.]grail[.]com), and salesforce (rlpq[.]j[.]scaleforce[.]net), which could be weaponized should threat actors discover they have been left dangling and insufficiently secured.

—

Our in-depth investigation of the Typhoon 2FA DNS infrastructure through an IoC list expansion analysis enabled us to uncover 4,041 potentially connected artifacts comprising 288 registrant email address-connected domains, 110 registrant organization-connected domains, 262 email-connected domains, 21 IP addresses, 137 string-connected domains, and 3,223 string-connected subdomains. It is also worth noting that all the 21 IP addresses the threat actors used were associated with various threats, specifically, C&C, malware, phishing, attacks, and generic threats.

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

Sample Registrant Email Address-Connected Domains

- 1hu0r[.]com
- 1k4pv8[.]com
- 1ljf0[.]com
- 1nnqn[.]com
- 2ahhl[.]com
- 2f9od[.]com
- 2gawsb[.]com
- 3shaqe[.]com
- 4nriup[.]com
- 52f0v[.]com
- 56l36[.]com
- 5fj4k[.]com
- 5gyw71[.]com
- 5hzoyq[.]com

- 5jbl2j[.]com
- 5pj00t[.]com
- 6gzhs4[.]com
- 6i2x2[.]com
- 6nzjq[.]com
- 6ugt63[.]com
- 8270k7[.]com
- 8wkay[.]com
- 9sbn8[.]com
- a4u7m[.]com
- adamtransprot[.]com
- af5x1[.]com
- ah9v1[.]com
- ahalqosaibi[.]com
- aims-jbaimsmall[.]com
- anrtop[.]com
- art-rul[.]com
- asbapart[.]com
- b09cla[.]com
- b2b-asla[.]com
- b6zmr[.]com
- baffter[.]com
- balconldolcaria[.]com
- bernisworldide[.]com
- bestsourclng[.]net
- boeshringer-ingelheim[.]com
- borlt-intl[.]com
- buasch[.]com
- c38afd[.]com
- c7eqi[.]com
- casalinlsrl[.]com
- cdoinbuction[.]com
- cgc-corq[.]com
- cgzx03[.]com
- charrninghometextiles[.]com
- cheerfuhk[.]net

Sample Registrant Organization-Connected Domains

- 0n2j[.]com
- 0od5e[.]com
- 19hp9[.]com
- 37w8[.]com
- 3kcgw[.]com
- 45hca[.]com
- 4d3zv[.]com
- 4zfql[.]com
- 5xket[.]com
- 70z6[.]com
- 89ena[.]com
- 94zlp[.]com
- 9af4[.]com
- aj3mla[.]com
- alda59[.]com
- an630u[.]com
- awn406[.]com
- b01l9[.]com
- b0t22[.]com
- blaikdriver[.]com
- by1g[.]com
- c0ic4[.]com
- c3ui7[.]com
- cchn1[.]com
- czn345[.]com
- dejmb[.]com
- dt-asia[.]org
- eh5j[.]com
- ew2ff[.]com
- f2ifm[.]com
- faj24[.]com
- familywater[.]com
- fbn3b[.]com
- fca54[.]com
- fiav6[.]com
- fvjc0[.]com
- fy9da[.]com
- g07x2[.]com

- g0z4[.]com
- gej5x[.]com
- gfbs2[.]com
- gtp94[.]com
- h08ux[.]com
- h9m42[.]com
- ht3q8[.]com
- hwq0x[.]com
- hx94b[.]com
- i7u2b[.]com
- idschina[.]org
- ijt2ex[.]com

Sample Email-Connected Domains

- 021nk[.]org
- 021shzhnk[.]com
- 027chanke[.]net
- 0531gongsi[.]com[.]cn
- 079j[.]cn
- 0love0[.]net
- 120shwjfkyy[.]net
- 120sjnk[.]net
- 120xingbing[.]net
- 1860888[.]com[.]cn
- 3d11[.]cn
- 410483[.]com
- 4sqc[.]com[.]cn
- 52261017[.]org
- 65383018[.]com
- 73176kqbdyy[.]com
- 750086[.]com
- achuancai[.]com
- anhysof981[.]com
- anhytfks92[.]com
- audic[.]com[.]cn
- auu[.]asia
- auy[.]asia
- awv[.]asia
- bhv[.]asia
- bij[.]asia
- bjmbjy[.]cn
- bko[.]asia
- blqz[.]com[.]cn
- bvg[.]asia
- bzv[.]asia
- cfv[.]asia
- charmfashion-lauren[.]cn
- dmkstjg[.]com
- door-knockers[.]cn
- dut[.]asia
- easy-buy[.]vip
- egy[.]asia
- eih[.]asia
- ejj[.]asia
- eky[.]asia
- elb[.]asia
- eld[.]asia
- eqg[.]asia
- erj[.]asia
- evw[.]asia
- ewh[.]asia
- exj[.]asia
- ezl[.]asia
- ezs[.]asia

Sample IP Addresses

- 104[.]21[.]25[.]137
- 104[.]21[.]39[.]90
- 104[.]21[.]71[.]7
- 104[.]21[.]73[.]207
- 104[.]21[.]77[.]197
- 172[.]67[.]134[.]71
- 172[.]67[.]141[.]67
- 172[.]67[.]144[.]3

- 172[.]67[.]192[.]39
- 172[.]67[.]211[.]110

* Note that all IP addresses were malicious.

Sample String-Connected Domains

- 7e2r[.]vg
- 7e2r[.]ws
- codecrafters[.]academy
- codecrafters[.]agency
- codecrafters[.]app
- codecrafters[.]art
- codecrafters[.]bar
- codecrafters[.]biz[.]id
- codecrafters[.]boats
- codecrafters[.]cam
- codecrafters[.]cfd
- codecrafters[.]ch
- codecrafters[.]cl
- codecrafters[.]cloud
- codecrafters[.]club
- codecrafters[.]cn
- codecrafters[.]co[.]in
- codecrafters[.]co[.]za
- codecrafters[.]co[.]zw
- codecrafters[.]codes
- codecrafters[.]com[.]ar
- codecrafters[.]com[.]au
- codecrafters[.]com[.]co
- codecrafters[.]com[.]hk
- codecrafters[.]com[.]mx
- codecrafters[.]com[.]ng
- codecrafters[.]com[.]tr
- codecrafters[.]dev[.]br
- codecrafters[.]dk
- codecrafters[.]es
- codecrafters[.]expert
- codecrafters[.]fr
- codecrafters[.]fun
- codecrafters[.]hair
- codecrafters[.]icu
- codecrafters[.]id
- codecrafters[.]ie
- codecrafters[.]info
- codecrafters[.]io
- codecrafters[.]ir
- codecrafters[.]kz
- codecrafters[.]life
- codecrafters[.]live
- codecrafters[.]lk
- codecrafters[.]ltd
- codecrafters[.]lv
- codecrafters[.]my[.]id
- codecrafters[.]net
- codecrafters[.]no
- codecrafters[.]online

Sample String-Connected Subdomains

- explore[.]0[.]yelp[.]com
- explore[.]0nlythebest02[.]mapsense[.]co
- explore[.]1[.]m4ch1n3[.]tech
- explore[.]1[.]sandbox[.]plasma[.]sh
- explore[.]111[.]acuityscheduling[.]com
- explore[.]1blikonline[.]dev[.]atg[.]se
- explore[.]45[.]instructure[.]com
- explore[.]9autodiscover[.]athena[.]bitdefender[.]net
- explore[.]abacus2[.]cyon[.]site
- explore[.]ac22[.]dev[.]atg[.]se

- explore[.]accelschoolsonlineohpi[.]instructure[.]com
- explore[.]acceptatie[.]godo[.]com[.]au
- explore[.]acceptatie[.]lazalogistics[.]ph
- explore[.]acceptatie[.]zalora[.]com[.]ph
- explore[.]account[.]yelp[.]com
- explore[.]ad[.]beta[.]pixocial[.]com
- explore[.]ad[.]pixocial[.]com
- explore[.]adelaidepi[.]instructure[.]com
- explore[.]administrator[.]yelp[.]com
- explore[.]admissions[.]utexas[.]edu
- explore[.]adobe[.]pond5[.]com
- explore[.]affiliatespi[.]instructure[.]com
- explore[.]agsmartit[.]duckdns[.]org
- explore[.]all[.]www[.]50x[.]ch
- explore[.]allidev[.]qa[.]radar[.]epam[.]com
- explore[.]almond[.]calculquebec[.]cloud
- explore[.]alp1[.]ae[.]flow[.]ch
- explore[.]alumclub[.]mit[.]edu
- explore[.]amazonpi[.]betamazon[.]instructure[.]com
- explore[.]amcway-apt[.]ciotest[.]lazalogistics[.]ph
- explore[.]amcway-apt[.]ciotest[.]liebi[.]com
- explore[.]amcway-apt[.]ciotest[.]pop-stage-ext[.]net
- explore[.]amcway-apt[.]ciotest[.]run[.]app
- explore[.]amcway-apt[.]ciotest[.]yellowribbon[.]mil
- explore[.]amcway[.]ciostage[.]netfliz[.]ca
- explore[.]amcway[.]ciostage[.]pulleyapp[.]com
- explore[.]amcway[.]ciostage[.]sex[.]com
- explore[.]amcway[.]ciostage[.]yellowribbon[.]mil
- explore[.]amcway[.]miro[.]com
- explore[.]amd[.]com[.]edgekey[.]net
- explore[.]amia[.]org[.]00d5e0000044eijeae[.]live[.]siteforce[.]com
- explore[.]amira[.]rustwom[.]people[.]amazon[.]dev
- explore[.]analytics[.]yelp[.]com
- explore[.]angloalemani[.]instructure[.]com
- explore[.]antivirus2[.]alditalk-kundenbetreuung[.]de
- explore[.]anvilproject[.]dev[.]cleverca nary[.]com
- explore[.]apaamu[.]beta[.]instructure[.]com
- explore[.]apaccelschools[.]beta[.]instructure[.]com
- explore[.]apacg[.]beta[.]instructure[.]com
- explore[.]apantispam2[.]beta[.]instructure[.]com
- explore[.]apantony[.]beta[.]instructure[.]com
- explore[.]apaugust[.]instructure[.]com
- explore[.]apb99[.]instructure[.]com
- explore[.]apbc[.]beta[.]instructure[.]com
- explore[.]apbcsd[.]instructure[.]com
- explore[.]apbfda[.]instructure[.]com
- explore[.]apbrace[.]beta[.]instructure[.]com
- explore[.]apbravo[.]instructure[.]com

- explore[.]apbrightwood[.]beta[.]instructure[.]com
- explore[.]apcanvas-igo-hr[.]instructure[.]com
- explore[.]apcbet[.]beta[.]instructure[.]com
- explore[.]apccsc[.]beta[.]instructure[.]com
- explore[.]apcluster8[.]instructure[.]com
- explore[.]apcolumbiaschools[.]beta[.]instructure[.]com
- explore[.]apdayspring[.]beta[.]instructure[.]com
- explore[.]apdof[.]instructure[.]com
- explore[.]apdthompson[.]instructure[.]com
- explore[.]apeclass[.]instructure[.]com
- explore[.]apeuropaskolan[.]instructure[.]com
- explore[.]apfarmlabor[.]beta[.]instructure[.]com
- explore[.]apfef[.]instructure[.]com
- explore[.]apgreenbush[.]beta[.]instructure[.]com
- explore[.]apgreenriver[.]beta[.]instructure[.]com
- explore[.]apheadspace[.]instructure[.]com
- explore[.]aphorizon[.]beta[.]instructure[.]com
- explore[.]api[.]30eta[.]instructure[.]com
- explore[.]api[.]ada[.]app
- explore[.]api[.]adobeaemcloud[.]com
- explore[.]api[.]aieta[.]instructure[.]com
- explore[.]api[.]app[.]link
- explore[.]api[.]aureta[.]instructure[.]com
- explore[.]api[.]banyan[.]com
- explore[.]api[.]blue4greenacademy-vanityeta[.]instructure[.]com
- explore[.]api[.]bpo[.]instructure[.]com
- explore[.]api[.]bradfordeta[.]instructure[.]com
- explore[.]api[.]brandeiseta[.]instructure[.]com
- explore[.]api[.]brfeta[.]instructure[.]com
- explore[.]api[.]briantreepayments[.]biz
- explore[.]api[.]carolyneta[.]instructure[.]com
- explore[.]api[.]ccpeta[.]instructure[.]com
- explore[.]api[.]cieta[.]instructure[.]com
- explore[.]api[.]clarksoneta[.]instructure[.]com
- explore[.]api[.]cluster8-fileseta[.]instructure[.]com
- explore[.]api[.]cns-catholiceta[.]instructure[.]com
- explore[.]api[.]cuieta[.]instructure[.]com
- explore[.]api[.]czieta[.]instructure[.]com
- explore[.]api[.]d323eta[.]instructure[.]com
- explore[.]api[.]daneseta[.]instructure[.]com
- explore[.]api[.]devtest5eta[.]instructure[.]com
- explore[.]api[.]dfeeta[.]instructure[.]com