Domain Shadowing IoC Expansion Led to Thousands of Possible Connections

Table of Contents

Executive Report

Palo Alto Networks threat analysts discovered more than 12,000 cases of domain shadowing after scanning the Web from April to June 2022. For this threat, all cybercriminals need to do is create malicious subdomains under legitimate domains, allowing them to host command-and-control (C&C) servers, phishing pages, and other malicious content while riding on the legitimacy of the root domains.

Often, victims cannot detect domain shadowing until it's too late. WhoisXML API researchers built on the indicators of compromise (IoCs) Palo Alto Networks published to obtain possible cases of domain shadowing and expand the list of potentially malicious domains. Our study revealed:

- 2,900+ subdomains starting with trust-evoking strings like "login," "training," and "carrier" added between 1 September and 24 October 2022
- 1,600+ web properties resolving to IP addresses to which the IoCs resolved
- About 4% of the artifacts related to the domain shadowing campaign IoCs were malicious
- Several domains hosting or redirecting to similar Microsoft login pages to which the IoCs redirected

IoC Expansion

What Other Domains Share the Malicious IP Hosts?

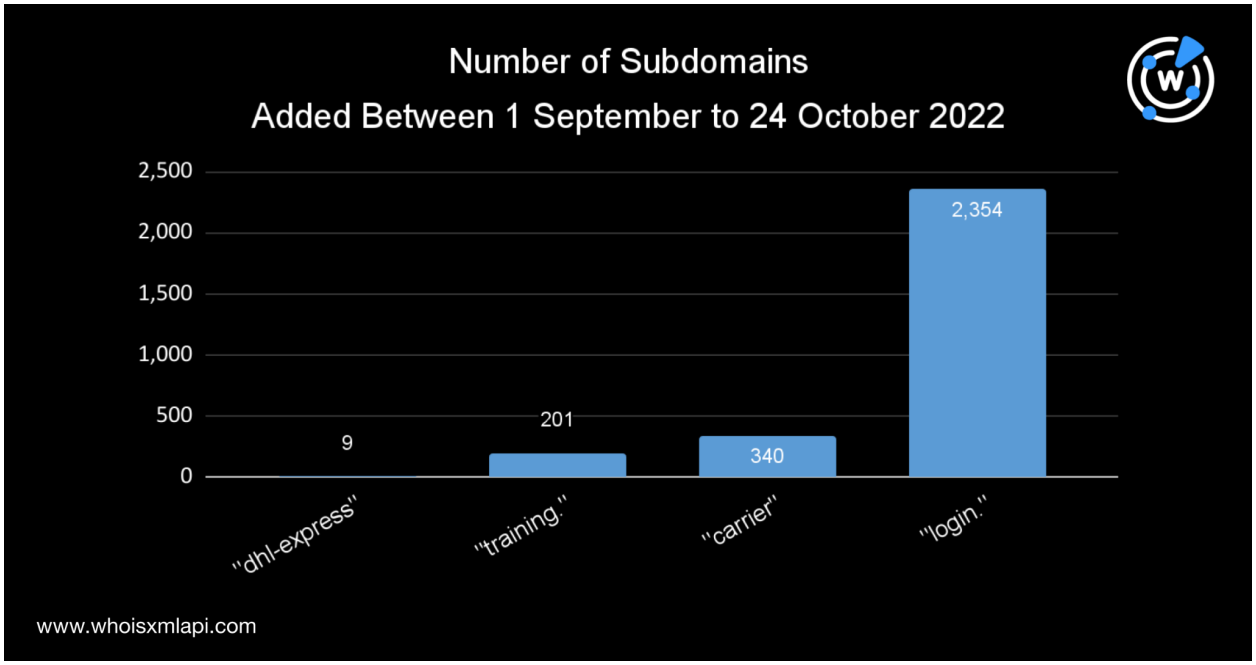
About 14 web properties tagged as IoCs in the domain shadowing campaign were published in the report referenced above. These resources resolved to seven unique IP addresses, also named in the report.

A reverse IP/DNS lookup on the IP addresses revealed 1,675 connected cyber resources, over a dozen of which were flagged as malicious by various malware engines.

What Other Domains Look Similar to the IoCs?

By studying the IoCs, we determined that aside from using random text string combinations for the subdomains, the threat actors also used terms that evoked trust in the average Internet user. Examples include “login” and “training.” We named some of the most common subdomains found under legitimate domains that threat actors may be taking advantage of.

We used these strings as Domains & Subdomains Discovery search terms, along with “dhl-express” and “carrier,” which were also seen in our subdomain lookups for the compromised domains. A total of 2,904 unique subdomains added from 1 September to 24 October 2022 were found. The chart below shows the volume of domains found per search term.

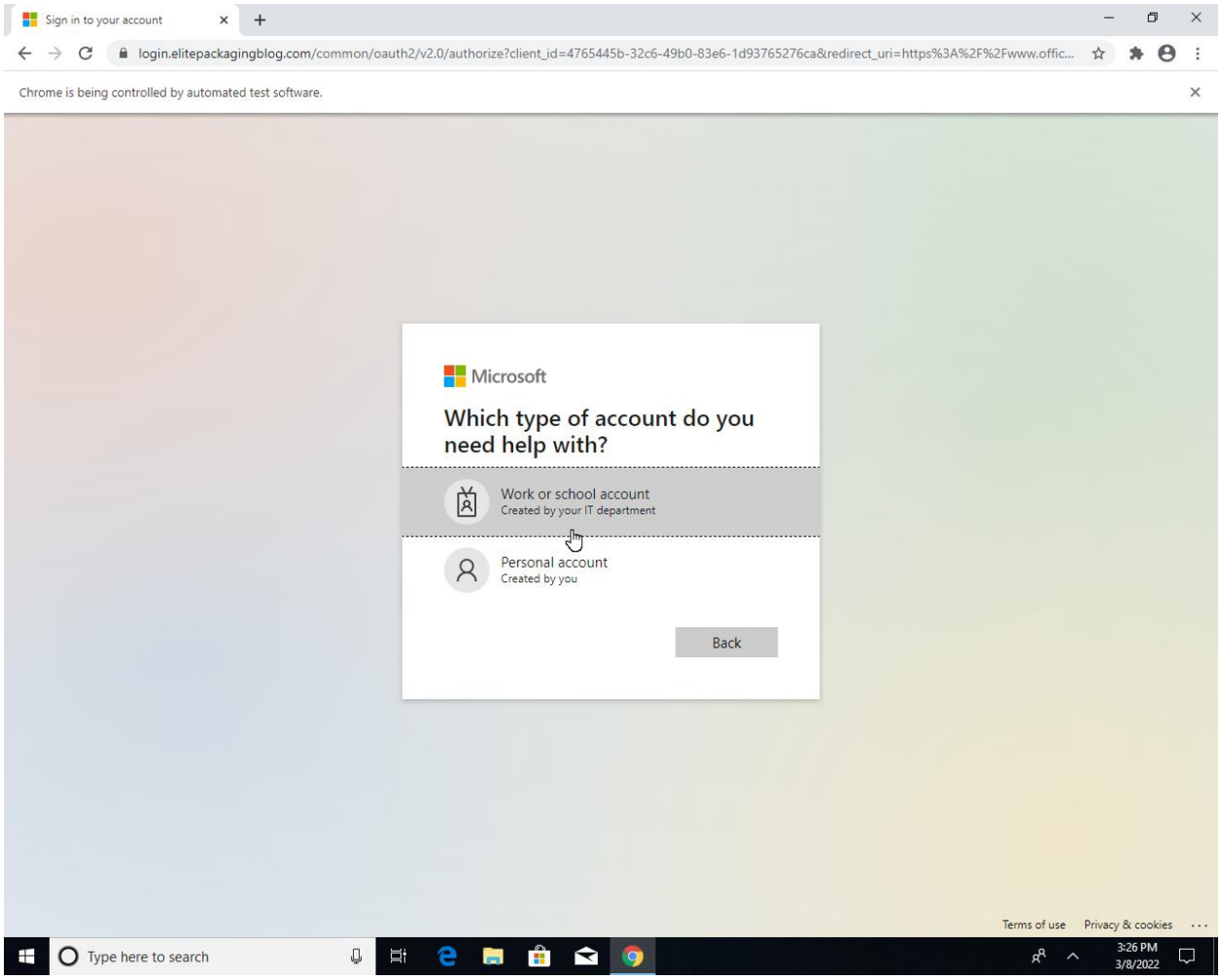


Nearly 4% of these connected properties were found malicious.

Analysis of the Artifacts

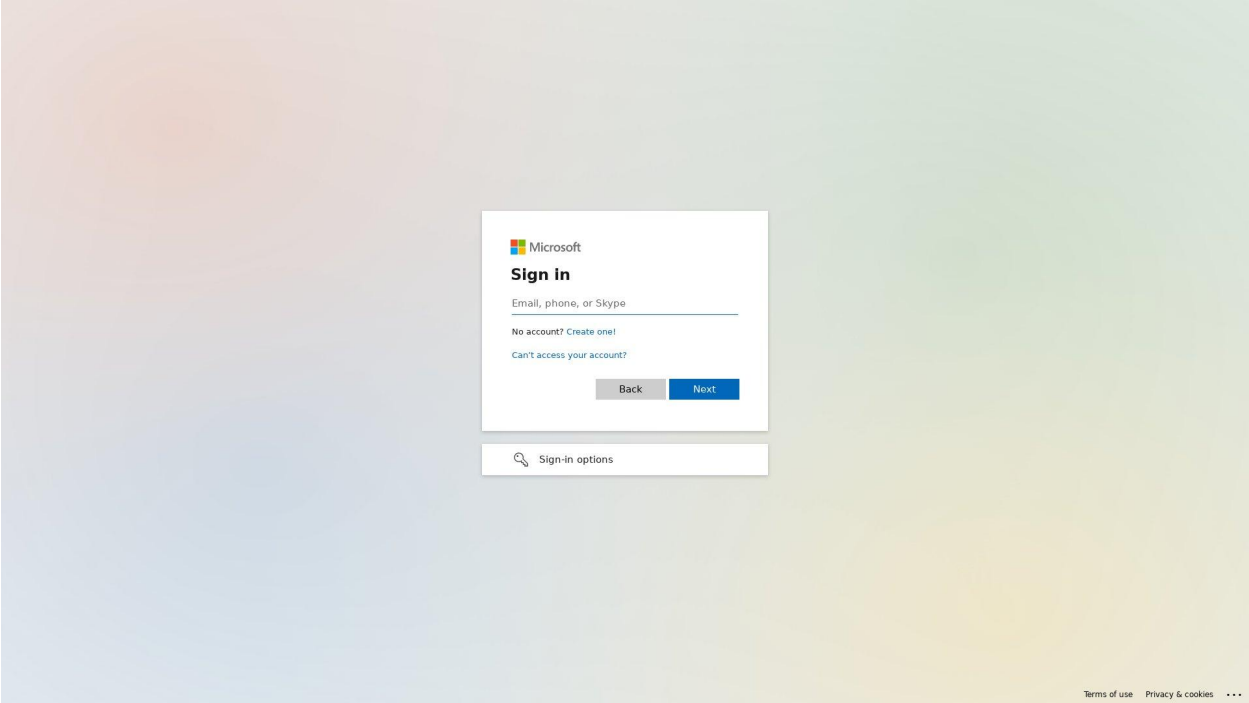
About 81% of the artifacts related to domain shadowing had active IP resolutions. Several subdomains hosted questionable content, according to the screenshot lookup results. Some were login pages, similar to the content the IoCs hosted or redirected to.

The screenshot below shows the page to which users who clicked the IoCs were redirected. The goal of the page could be to steal Microsoft user credentials.



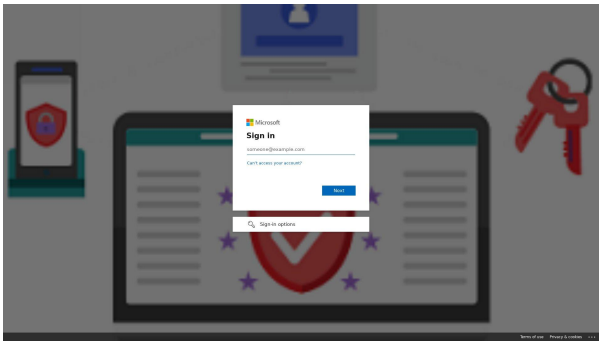
Screenshot of elitepackagingblog[.]com taken from [Palo Alto Networks]

On the other hand, below is a screenshot of one of the connected subdomains we discovered. Like the malicious page above, it also appears to resolve to a Microsoft look-alike login page.

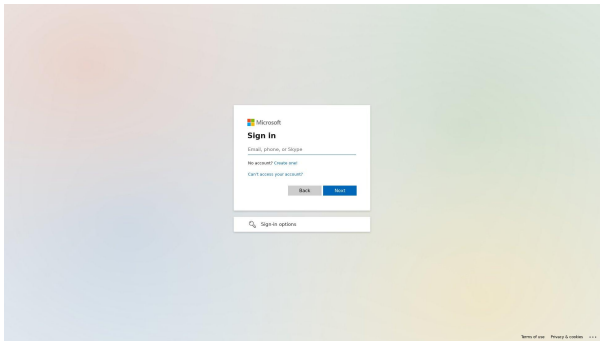


Screenshot of login[.]dev[.]consigli[.]app

Other examples found hosting similar content are shown below.



Screenshot of login[.]springer[.]com[.]eirc[.]remotexs[.]co

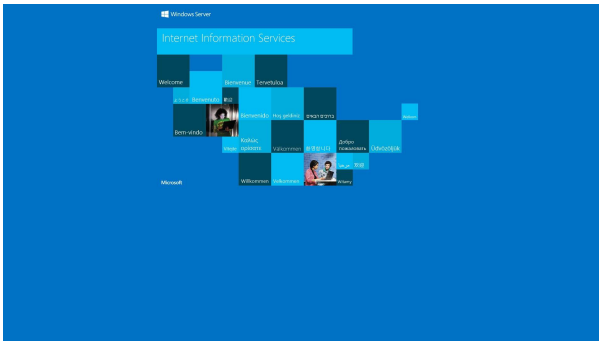


Screenshot of login[.]uat[.]consigli[.]app

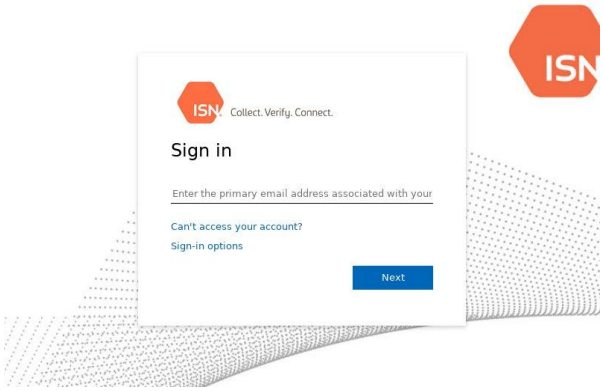
Malicious Subdomains Found

We ran a bulk malware check on the connected properties and found 172 that may have already figured in malicious campaigns, regardless of type—domain shadowing or some other type of cyber attack.

Alarmingly, several still hosted or redirected to suspicious pages, such as those shown below.

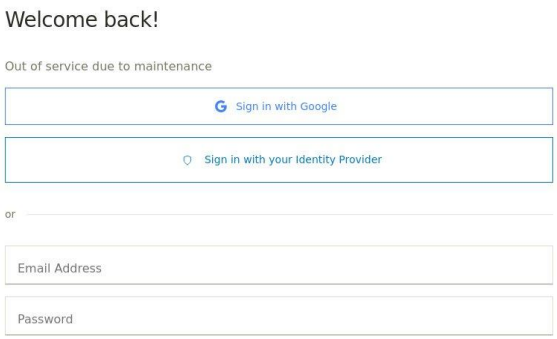


Screenshot of login[.]8923116[.]norseshorestudios[.]com



Screenshot of login[.]isnetworld[.]us[.]com

Screenshot of login[.]raknten[.]jp[.]gdubei[.]top



Screenshot of login[.]ramp[.]com[.]weafricans[.]net

—

Domain shadowing is reminiscent of the Gallium APT Group's modus operandi we studied in the past, where we discovered several malicious subdomains under legitimate root domains. In fact, for this study, some of the malicious properties we found were DuckDNS subdomains.

We found a common theme for both threats—malicious actors hid behind legitimate domains. Compromised pages may, however, be difficult for domain owners to detect until it's too late.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Domains

Sample IoCs from Palo Alto Networks

- halont[.]edu[.]au
- training[.]halont[.]edu[.]au
- ocwdvmjjj78krus[.]halont[.]edu[.]au
- baqrxmgfr39mfpp[.]halont[.]edu[.]au
- barwonbluff[.]com[.]au
- bancobpmmavfhxcc[.]barwonbluff[.]com[.]au
- snaitechbumxzzwt[.]barwonbluff[.]com[.]au
- snaitechbumxzzwt[.]barwonbluff[.]com[.]au/bumxzzwt/xxx[.]yyy@target[.]it
- tomsvprfudhd[.]barwonbluff[.]com[.]au
- brisbanegateway[.]com
- carriernhoousvz[.]brisbanegateway[.]com
- vembanadhouse[.]com
- wiguhllnz43wxvq[.]vembanadhouse[.]com
- login[.]elitepackagingblog[.]com

Sample Subdomains Under Compromised Domains as of 14 October 2022

- cpanel[.]halont[.]edu[.]au
- ak47sender[.]halont[.]edu[.]au
- mail[.]halont[.]edu[.]au
- lieferung-dhl-express-ch-deliver[.]halont[.]edu[.]au
- cpcontacts[.]halont[.]edu[.]au
- www[.]halont[.]edu[.]au
- webdisk[.]halont[.]edu[.]au
- www[.]training[.]halont[.]edu[.]au
- www[.]blog[.]halont[.]edu[.]au
- cpcalendars[.]halont[.]edu[.]au
- www[.]lieferung-dhl-express-ch-deliver[.]halont[.]edu[.]au
- training[.]halont[.]edu[.]au
- autodiscover[.]halont[.]edu[.]au
- webmail[.]halont[.]edu[.]au
- blog[.]halont[.]edu[.]au
- mail[.]barwonbluff[.]com[.]au
- www[.]barwonbluff[.]com[.]au
- mail[.]brisbanegateway[.]com
- www[.]lightshot[.]brisbanegateway[.]com
- lightshot[.]brisbanegateway[.]com
- webdisk[.]vembanadhouse[.]com
- cpcontacts[.]vembanadhouse[.]com
- mail[.]vembanadhouse[.]com
- webmail[.]vembanadhouse[.]com
- cpanel[.]vembanadhouse[.]com
- autodiscover[.]vembanadhouse[.]com
- cpcalendars[.]vembanadhouse[.]com
- www[.]vembanadhouse[.]com

Sample Web Properties Connected to the Domain Shadowing IoCs through Their IP Hosts

- 1recruitintl[.]com
- 2-monkeys[.]com

- 2monkeystours[.]com
- 545baldivis[.]com[.]au
- absolutestripout[.]com[.]au
- acceleratedfs[.]com[.]au
- acemobilelocksmiths[.]com[.]au
- activ8retail[.]co[.]nz
- adelaidehillsdairies[.]com[.]au
- adelaidesigndesign[.]com[.]au
- admiralmotorinn[.]com[.]au
- advancedtimberfinishing[.]com[.]au
- afmc[.]com[.]au
- afsa[.]net[.]au
- agtl[.]com[.]au
- allfloorsqld[.]com[.]au
- alltimberwindows[.]com[.]au
- alt-domains[.]com
- alternatecare[.]com[.]au
- amanastone[.]com[.]au
- amecservices[.]com[.]au
- andrewtelleypsychology[.]com[.]au
- appstarmedia[.]com[.]au
- areras[.]com[.]au
- armadaleconsulting[.]com[.]au
- artisanacademy[.]org[.]au
- ashkagroup[.]com[.]au
- aspect[.]clinic
- aspectclinic[.]com[.]au
- atlasfab[.]com[.]au
- ausidive[.]com[.]au
- austleg[.]com[.]au
- austmadeengineering[.]com[.]au
- autodiscover[.]545baldivis[.]com[.]au
- autodiscover[.]alt-domains[.]com
- autodiscover[.]autodoorservices[.]com[.]au
- autodiscover[.]bachalani[.]com[.]au
- autodiscover[.]balwynpoolfenceinspections[.]com[.]au
- autodiscover[.]blackouttactical[.]com[.]au
- autodiscover[.]byronbayairportshuttle[.]com
- autodiscover[.]globalsourcingtrader[.]com
- autodiscover[.]jac[.]net[.]au
- autodiscover[.]obiwaters[.]com
- autodiscover[.]onlinestorytime[.]org[.]au
- autodiscover[.]profabportlincoln[.]com[.]au
- autodiscover[.]west-global[.]com
- autodiscover[.]wildernessexplorersafrica[.]com
- autodoorservices[.]com[.]au
- autoprojimboomba[.]com[.]au
- availit[.]com[.]au
- b-inked[.]com[.]au
- bachalani[.]com[.]au
- balwynpoolfenceinspections[.]com[.]au
- beckbuilt[.]com[.]au
- bentstems[.]com[.]au
- bestdressdesigns[.]com[.]au
- bestshots[.]com[.]au
- betafinance[.]com[.]au
- betterbricks[.]com[.]au
- bible[.]ucannlearn[.]com
- blackouttactical[.]com[.]au
- blog4u[.]com[.]au
- bluebloods[.]nz
- blurbconsulting[.]com[.]au
- bmwise[.]com[.]au
- brainspine[.]com[.]au
- bramptonfinance[.]com[.]au
- brewdesigns[.]com[.]au
- bridgefieldcorporation[.]com
- brisbanehampers[.]com[.]au
- bu[.]net[.]au
- byronbayairportshuttle[.]com
- c1formworkgroup[.]com

- capebouvardtechnologies[.]com[.]au
- capitalpm[.]com[.]au
- capitalpropertymanagement[.]com[.]au
- capitalpropertymarketing[.]com[.]au
- capitalpropertysettlements[.]com[.]au
- carbonhalo[.]com
- castlerealestate[.]com[.]au
- cbit[.]com[.]au
- cbit[.]net[.]au
- ccmi[.]com[.]au
- ccrefrigeration[.]com[.]au
- ccurb[.]com[.]au
- cehire[.]com[.]au
- celsiusheatingandcooling[.]com[.]au
- chessdata[.]com[.]au
- clermontgroup[.]com[.]au
- cmworks[.]com[.]au
- concreteintegrity[.]com[.]au
- continentalsteel[.]com[.]au
- contrastsigns[.]com[.]au
- cpanel-506-syd[.]hostingww[.]com
- cpanel[.]545baldivis[.]com[.]au
- cpanel[.]alt-domains[.]com
- cpanel[.]autodoorservices[.]com[.]au
- cpanel[.]bachalani[.]com[.]au
- cpanel[.]balwynpoolfenceinspections[.]com[.]au
- cpanel[.]blackouttactical[.]com[.]au
- cpanel[.]byronbayairportshuttle[.]com
- cpanel[.]exactcomputers[.]com[.]au
- cpanel[.]globalsourcingtrader[.]com
- cpanel[.]goldmanbros[.]com[.]au
- cpanel[.]jac[.]net[.]au
- cpanel[.]obiwaters[.]com
- cpanel[.]onlinestorytime[.]org[.]au
- cpanel[.]west-global[.]com
- cpanel[.]wildernessexplorersafrica[.]com
- cpanel[.]youritcrew[.]com[.]au
- cpcalendars[.]545baldivis[.]com[.]au
- cpcalendars[.]alt-domains[.]com
- cpcalendars[.]autodoorservices[.]com[.]au
- cpcalendars[.]bachalani[.]com[.]au
- cpcalendars[.]balwynpoolfenceinspections[.]com[.]au
- cpcalendars[.]blackouttactical[.]com[.]au
- cpcalendars[.]brewdesigns[.]com[.]au
- cpcalendars[.]byronbayairportshuttle[.]com
- cpcalendars[.]darrenglen[.]com
- cpcalendars[.]dev[.]venncap[.]com[.]au
- cpcalendars[.]dreamfeet[.]com[.]au
- cpcalendars[.]esogdc[.]com[.]au
- cpcalendars[.]exactcomputers[.]com[.]au
- cpcalendars[.]gallowaydesigncollective[.]com[.]au
- cpcalendars[.]globalsourcingtrader[.]com
- cpcalendars[.]jac[.]net[.]au
- cpcalendars[.]obiwaters[.]com
- cpcalendars[.]onlinestorytime[.]org[.]au
- cpcalendars[.]west-global[.]com
- cpcalendars[.]wildernessexplorersafrica[.]com
- cpcontacts[.]545baldivis[.]com[.]au
- cpcontacts[.]alt-domains[.]com
- cpcontacts[.]autodoorservices[.]com[.]au
- cpcontacts[.]bachalani[.]com[.]au

- cpcontacts[.]balwynpoolfenceinspections[.]com[.]au
- cpcontacts[.]blackouttactical[.]com[.]au
- cpcontacts[.]brewdesigns[.]com[.]au
- cpcontacts[.]byronbayairportshuttle[.]com
- cpcontacts[.]darrenglen[.]com
- cpcontacts[.]dreamfeet[.]com[.]au
- cpcontacts[.]esogdc[.]com[.]au
- cpcontacts[.]exactcomputers[.]com[.]au
- cpcontacts[.]gallowaydesigncollective[.]com[.]au
- cpcontacts[.]globalsourcingtrader[.]com
- cpcontacts[.]jac[.]net[.]au
- cpcontacts[.]obiwaters[.]com
- cpcontacts[.]onlinestorytime[.]org[.]au
- cpcontacts[.]west-global[.]com
- cpcontacts[.]wildernessexplorersafrica[.]com
- creditms[.]com[.]au
- csspl[.]com[.]au
- ctrl-z[.]net[.]au
- cyberaccountant[.]com[.]au
- cycle-city[.]com[.]au
- cyclecity[.]au
- daptonetball[.]com[.]au
- darrenglen[.]com
- db-a[.]co
- db-x[.]co
- decorativediva[.]com[.]au
- deluxeweb[.]com[.]au
- depositsaviour[.]com[.]au
- dev[.]carbonhalo[.]com
- dev[.]walpol[.]com[.]au
- dev[.]youritcrew[.]com[.]au
- dev2[.]carbonhalo[.]com
- dewkent[.]com[.]au
- digitalbm[.]com[.]au
- dmre[.]net[.]au
- dobie[.]name
- dolcedevelopment[.]com[.]au
- draarchitects[.]com[.]au
- dreamfeet[.]com[.]au
- easterneng[.]com[.]au
- eastonlawyers[.]com[.]au
- easyph[.]com[.]au
- echoadvisory[.]com[.]au
- egbp[.]com[.]au
- electrumproperty[.]com
- elesa[.]com[.]au
- eltaustralia[.]com[.]au
- empirecleaning[.]com[.]au
- empiremanagementservices[.]com[.]au
- endlessrubbish[.]com[.]au
- eplacetv[.]com[.]au
- esogdc[.]com[.]au
- esogroup[.]com[.]au
- explorateurs[.]org[.]au
- eye4design[.]com[.]au
- flatearth[.]net[.]au
- flatstick[.]com[.]au
- flowersuponflowers[.]com[.]au
- fnssa[.]org[.]au
- foxy[.]marketing
- freedomlivingaustralia[.]com[.]au
- frogsontherun[.]com[.]au
- gallowaydesigncollective[.]com[.]au
- garoyda[.]com[.]au
- gaudron[.]com[.]au
- gibsonfreight[.]com
- gibsonfreight[.]com[.]au
- globalsourcingtrader[.]com
- goldcoastfirstaidtraining[.]com[.]au
- grechborg[.]com[.]au
- greenkleenaustralia[.]com[.]au

- halalpoultry[.]com[.]au
- halont[.]edu[.]au
- handybar[.]com[.]au
- harlandeng[.]com[.]au
- harterdental[.]com[.]au
- hawthornbh[.]com[.]au
- hedlandbuslines[.]com[.]au
- hiregearhere[.]com[.]au
- hmservices[.]com[.]au
- hvtinspectionservices[.]com[.]au
- indigotraining[.]com[.]au
- insightintegration[.]com[.]au
- internationalgolfconcepts[.]com
- internationalgolfconcepts[.]com[.]au
- invent-pacific[.]com[.]au
- itqq[.]com[.]au
- jac[.]net[.]au
- jactechnologies[.]com[.]au
- janjorgensen[.]com[.]au
- jayscom[.]net[.]au
- jazzacademy[.]com[.]au
- jdcinfo[.]digitalbm[.]com[.]au
- jetlocksmiths[.]com[.]au
- jimmynet[.]net
- jjgregoire[.]com[.]au
- jodiecicaji[.]com
- jtenvironmental[.]com[.]au
- juicybeanscafe[.]com[.]au
- junkgle[.]com
- kellyfitzgibbon[.]com[.]au
- keswickhouse[.]com[.]au
- keyemployment[.]com[.]au
- kolmark[.]com[.]au
- kurandanc[.]org[.]au
- lansvalesmashrepairs[.]com[.]au
- larklaw[.]com[.]au
- larklaw[.]net[.]au
- larklawyers[.]com[.]au
- loadednet[.]com[.]au
- lpsu[.]com[.]au
- lynwoodunitedfc[.]com
- maccacentral[.]com[.]au
- macedonelegal[.]com[.]au
- macedonia[.]com[.]au
- mail[.]545baldivis[.]com[.]au
- mail[.]agosci[.]org[.]au
- mail[.]alt-domains[.]com
- mail[.]aspect[.]clinic
- mail[.]aspectclinic[.]com[.]au
- mail[.]autodoorservices[.]com[.]au
- mail[.]balwynpoolfenceinspections[.]com[.]au
- mail[.]bodywizefitnesssolutions[.]com[.]au
- mail[.]byronbayairportshuttle[.]com
- mail[.]capebouvardtechnologies[.]com[.]au
- mail[.]darrenglen[.]com
- mail[.]decorativediva[.]com[.]au
- mail[.]depositsaviour[.]com[.]au
- mail[.]divingco[.]com[.]au
- mail[.]dreamfeet[.]com[.]au
- mail[.]esogdc[.]com[.]au
- mail[.]flatstick[.]com[.]au
- mail[.]ftgp[.]com[.]au
- mail[.]globalsourcingtrader[.]com
- mail[.]grechborg[.]com[.]au
- mail[.]halont[.]edu[.]au
- mail[.]harlandeng[.]com[.]au
- mail[.]indigotraining[.]com[.]au
- mail[.]jac[.]net[.]au
- mail[.]jimmynet[.]net
- mail[.]nenwfirstaidtraining[.]au
- mail[.]obiwaters[.]com
- mail[.]onlinestorytime[.]org[.]au
- mail[.]prochill[.]com[.]au
- mail[.]propertybuyersadvocates[.]com[.]au
- mail[.]sotiri[.]com[.]au
- mail[.]studiootto[.]com

- mail[.]sunbustershirts[.]com[.]au
- mail[.]sunrisefitness[.]com[.]au
- mail[.]tamworthsecurityservices[.]au
- mail[.]terofox[.]com[.]au
- mail[.]thebookseat[.]co[.]uk
- mail[.]west-global[.]com
- mail[.]westshockey[.]com
- mail[.]wombolly[.]com
- mailcp[.]anne-saunders[.]com
- mattsvintageguitars[.]com
- mcadams[.]com[.]au
- melbournecranes[.]com[.]au
- melbournemotorcycletowing[.]com[.]au
- messagingonhold[.]com[.]au
- michaelwenzel[.]com[.]au
- milliesykes[.]com
- mmfp[.]com[.]au
- mmointeriors[.]com[.]au
- mosaicartworksbypjohnson[.]com[.]au
- mpmlegal[.]com[.]au
- mrschnitzel[.]com[.]au
- mtgambierdental[.]com[.]au
- music[.]ucannlearn[.]com
- myhomeandgardensupport[.]com[.]au
- nelsonag[.]com[.]au
- nenwfirstaidtraining[.]au
- nenwfirstaidtraining[.]com[.]au
- neurosciences[.]com[.]au
- newagealuminium[.]com[.]au
- nqfitfactory[.]com[.]au
- obiwaters[.]com
- oceansecurities[.]com[.]au
- old[.]carbonhalo[.]com
- onestepconveyancing[.]com[.]au
- onlinestorytime[.]org[.]au
- oxinst[.]com[.]au
- p76clubnsw[.]org
- partyjukebox[.]com[.]au
- paylesstreeservice[.]com[.]au
- pelley[.]com[.]au
- pinnaclebricklaying[.]com[.]au
- please[.]com[.]au
- poetscafe[.]com[.]au
- portmusic[.]com[.]au
- prochill[.]com[.]au
- propertybuyersadvocates[.]com[.]au
- rea-associates[.]com[.]au
- reardon[.]com[.]au
- refinedsurfaces[.]com[.]au
- resultsturningpoint[.]com[.]au
- retailitprojects[.]com[.]au
- rhysholmesconstructions[.]com[.]au
- ridewithskills[.]com[.]au
- rodtech[.]com[.]au
- roycardiology[.]co
- roycardiology[.]com[.]au
- saveyourmoney[.]com[.]au
- sfba[.]com[.]au
- shyamalint[.]com[.]au
- simonejoy[.]com[.]au
- skyebraggdesigns[.]com[.]au
- slimliving[.]com[.]au
- smoothsynergy[.]com[.]au
- smphomecare[.]com[.]au
- solarintegrityaw[.]com[.]au
- solveprojects[.]com[.]au
- spiralflightingsupplies[.]com[.]au
- srbgroup[.]com[.]au
- staging[.]walpol[.]com[.]au
- stanleyenterprise[.]com[.]au
- stanthonysaustral[.]org
- starcommunityservices[.]org[.]au
- stevesdiving[.]com[.]au
- stowawayselfstorage[.]com[.]au
- studioenso[.]com[.]au
- studiootto[.]com
- study[.]ucannlearn[.]com

- sunbustershirts[.]com[.]au
- sunrisefitness[.]com[.]au
- switch-technologies[.]com[.]au
- tamworthsecurityservices[.]au
- tamworthsecurityservices[.]com[.]au
- tasmaniahampers[.]com[.]au
- teardownthewalls[.]net[.]au
- telleypsychology[.]com[.]au
- terofox[.]com[.]au
- terraco[.]com[.]au
- thebusinessofrealestate[.]com[.]au
- thecrystalslipper[.]com[.]au
- thelema[.]com[.]au
- thomaselectricalservices[.]com[.]au
- tiltaction[.]com[.]au
- timeexchange[.]ucannlearn[.]com
- timelessthreads[.]com[.]au
- tonydonald[.]com[.]au
- topcope[.]com[.]au
- trailerhiretas[.]com[.]au
- venncap[.]com[.]au
- walpol[.]com[.]au
- waroonadhs[.]wa[.]edu[.]au
- webdisk[.]545baldivis[.]com[.]au
- webdisk[.]alt-domains[.]com
- webdisk[.]autodoorservices[.]com[.]au
- webdisk[.]bachalani[.]com[.]au
- webdisk[.]balwynpoolfenceinspections[.]com[.]au
- webdisk[.]blackouttactical[.]com[.]au
- webdisk[.]byronbayairportshuttle[.]com
- webdisk[.]exactcomputers[.]com[.]au
- webdisk[.]globalsourcingtrader[.]com
- webdisk[.]jac[.]net[.]au
- webdisk[.]obiwaters[.]com
- webdisk[.]onlinestorytime[.]org[.]au
- webdisk[.]west-global[.]com
- webdisk[.]wildernessexplorersafrica[.]com
- webmail[.]545baldivis[.]com[.]au
- webmail[.]alt-domains[.]com
- webmail[.]autodoorservices[.]com[.]au
- webmail[.]bachalani[.]com[.]au
- webmail[.]balwynpoolfenceinspections[.]com[.]au
- webmail[.]blackouttactical[.]com[.]au
- webmail[.]byronbayairportshuttle[.]com
- webmail[.]globalsourcingtrader[.]com
- webmail[.]jac[.]net[.]au
- webmail[.]obiwaters[.]com
- webmail[.]onlinestorytime[.]org[.]au
- webmail[.]west-global[.]com
- webmail[.]wildernessexplorersafrica[.]com
- webpagefactory[.]com[.]au
- websterndissupport[.]com[.]au
- west-global[.]com
- west-global[.]com[.]westglobal[.]com[.]au
- westglobal[.]com[.]au
- whalebeach[.]sydney
- whm[.]allfloorsqld[.]com[.]au
- whm[.]felixgrossen[.]bridgefieldcorporation[.]com
- whprobus[.]org[.]au
- wildernessexplorersafrica[.]com
- wiskich[.]com[.]au
- wizup[.]com[.]au
- wombolly[.]com
- www[.]alt-domains[.]com
- www[.]aspect[.]clinic
- www[.]aspectclinic[.]com[.]au
- www[.]autodoorservices[.]com[.]au

- www[.]balwynpoolfenceinspections[.]com[.]au
- www[.]bible[.]ucannlearn[.]com
- www[.]blackouttactical[.]com[.]au
- www[.]brewdesigns[.]com[.]au
- www[.]byronbayairportshuttle[.]com
- www[.]carbonhalo[.]com
- www[.]creditms[.]com[.]au
- www[.]darrenglen[.]com
- www[.]dev[.]carbonhalo[.]com
- www[.]dev[.]youritcrew[.]com[.]au
- www[.]dev2[.]carbonhalo[.]com
- www[.]electrumproperty[.]com
- www[.]esogdc[.]com[.]au
- www[.]gallowaydesigncollective[.]com[.]au
- www[.]globalsourcingtrader[.]com
- www[.]jdcinfo[.]digitalbm[.]com[.]au
- www[.]music[.]ucannlearn[.]com
- www[.]nenwfirstaidtraining[.]au
- www[.]obiwaters[.]com
- www[.]old[.]carbonhalo[.]com
- www[.]onlinestorytime[.]org[.]au
- www[.]study[.]ucannlearn[.]com
- www[.]tamworthsecurityservices[.]au
- www[.]timeexchange[.]ucannlearn[.]com
- www[.]west-global[.]com
- www[.]west-global[.]com[.]westglobal[.]com[.]au
- www[.]youritcrew[.]com[.]au
- ycsconstruction[.]com[.]au
- youritcrew[.]com[.]au
- a2zmovingandstorage[.]com[.]au
- a2zmovingandstorage[.]net[.]au
- ablazethefilm[.]com
- actcurious[.]com
- actcuriouseap[.]com[.]au
- actfastpestcontrol[.]com[.]au
- acuitylawpartners[.]com[.]au
- advancedblindscleaning[.]com[.]au
- agqualitypools[.]com[.]au
- aiadstaging[.]com[.]au
- aileenphelancelebrants[.]com[.]au
- alexpavingandlandscaping[.]com[.]au
- alldayandnightelectrical[.]com[.]au
- allsteam[.]com[.]au
- armourflooring[.]com[.]au
- artconcrete[.]com[.]au
- ashleytmarriagecelebrant[.]com[.]au
- astutetiling[.]com[.]au
- australianinternetadvertising[.]com[.]au
- australianpoolheating[.]com[.]au
- azsmartmovers[.]com[.]au
- bacservices[.]com[.]au
- bandcexcavations[.]com[.]au
- barbaracolless[.]com[.]au
- barkerstreetspecialists[.]com[.]au
- barrywrightcelebrant[.]com[.]au
- barwonbluff[.]com[.]au
- bay-built[.]com[.]au
- beardsplumbing[.]com
- beyondpainting[.]com[.]au
- blacktiecleaning[.]net[.]au
- book-now[.]com[.]au
- brake-riteparts[.]com[.]au
- brisbane-shutters[.]com
- byronshirestonemasonry[.]com[.]au
- bystander[.]movingwordsandpictures[.]com[.]au
- caremaxmobilityaus[.]com[.]au
- caringcelebrations[.]com[.]au
- catered4you[.]com[.]au
- cbsnsw[.]com
- celebrate-it[.]com[.]au
- celebrateit[.]com[.]au
- centralwestpm[.]com[.]au

- centralwestsandstone[.]com[.]au
- ceremoniesinadelaide[.]com[.]au
- chimneysweep[.]net[.]au

Sample Subdomains Connected to the Domain Shadowing IoCs through Text Strings

- dhl-express-s[.]blogspot[.]com
- dhl-expressonline[.]sytes[.]net
- dhl-expressvietnam[.]daklaktourist[.]com[.]vn
- mydhl-express-traking[.]erointe[.]com
- www[.]dhl-expressvietnam[.]daklaktourist[.]com[.]vn
- www[.]mydhl-express-traking[.]erointe[.]com
- ondemand-delivery-dhl-express[.]balanzassanchez[.]com
- www[.]ondemand-delivery-dhl-express[.]balanzassanchez[.]com
- frais[.]paiement[.]dhl-express-suivi[.]com[.]lexprdehslaou[.]pw
- training[.]cloud[.]worksoft[.]com
- training[.]aimsnew[.]kerala[.]gov[.]in
- training[.]admin[.]nextgen[.]jendasolutionssandbox[.]com
- training[.]iris-automation[.]dps[.]amazon[.]dev
- training[.]veolia-staging[.]eleo[.]io
- training[.]itsd-8959[.]flowable[.]io
- training[.]prod-sys[.]tcblog[.]net
- training[.]iscoglobal[.]com[.]pages[.]services
- training[.]api[.]apprentice[.]io
- training[.]ka-factory[.]dev1[.]ejaferp[.]com
- training[.]seq-ingestion[.]platform[.]dptsprotrans[.]com
- training[.]bucke533[.]e56ro[.]mcrm[.]iteamhomeinspections[.]com
- training[.]lyh[.]haikuicloud[.]com
- training[.]sio-dock-prod[.]ucsd[.]edu
- training[.]erp[.]almadaralwaad[.]sa
- training[.]bioland[.]cbddev[.]xyz
- training[.]fi[.]uzh[.]ch
- training[.]nginx[.]dev[.]tedlab[.]net
- training[.]od0bm0al[.]poc[.]claroty[.]com
- training[.]advancedipsc[.]tplerp[.]com
- training[.]leocare[.]eleo[.]io
- training[.]mativ[.]eleo[.]io
- training[.]optoro[.]com[.]skilljarapp[.]com
- training[.]opus-qa[.]bmwgroup[.]com
- training[.]api[.]miq[.]cbrecn[.]com
- training[.]ba[.]prd[.]eu[.]bp[.]aws[.]cloud[.]vwgroup[.]com
- training[.]sartorius[.]eleo[.]io
- training[.]orpea[.]eleo[.]io
- training[.]hse-demo-staging[.]eleo[.]io
- training[.]digiclaim[.]suitsolutions[.]eu
- training[.]workflow[.]nasa[.]guycarp[.]com
- training[.]vtretain[.]pitt[.]edu
- training[.]femacms[.]webeoc[.]us
- training[.]demo[.]ejadtech[.]sa
- training[.]lgsc[.]jpd[.]mybluehost[.]me

- training[.]7282-pathway-collaborator[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]order[.]717ink[.]com
- training[.]v3[.]scoda[.]it-corp[.]co
- training[.]bts[.]gov[.]bz
- training[.]eb[.]gzbytech[.]com
- training[.]empower[.]abb[.]com[.]edgekey[.]net
- training[.]7612-success-factors[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]7458-sucess-factors[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]www[.]iup[.]edu
- training[.]preprod-staging[.]eleo[.]io
- training[.]web9[.]disgrafic[.]com
- training[.]v[.]test[.]oleybet[.]link
- training[.]v2-39[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]exbil[.]iinetdev[.]com
- training[.]opus[.]bmwgroup[.]com
- training[.]sandbox[.]grupovizer[.]com
- training[.]hospitality[.]amadeus[.]com
- training[.]kids-room[.]od[.]ua
- training[.]typo3[.]tue-nl[.]flowing-midge[.]maxserv[.]dev
- training[.]test[.]kaiisoft[.]com
- training[.]seq[.]platform[.]dptsprotrans[.]com
- training[.]it[.]aletheiatrust[.]org[.]uk
- training[.]oluwom[.]awsps[.]myinstance[.]com
- training[.]interplast[.]fl3p[.]au
- training[.]training-pierre-fabre[.]eleo[.]io
- training[.]sampling[.]astrazeneca[.]net
- training[.]orrlbpzg[.]jasonleemusic[.]com
- training[.]agilent[.]eleo[.]io
- training[.]zralbtdb[.]poc[.]claroty[.]com
- training[.]ibs[.]asurraa[.]app
- training[.]childrenssociety[.]org[.]uk[.]staging-5em2ouy-hu4zuth6ade6y[.]uk-1[.]platformsh[.]site
- training[.]test[.]devappdirect[.]me
- training[.]leyton[.]eleo[.]io
- training[.]jemeforme-acadnice[.]eleo[.]io
- training[.]us-1[.]intouchccm[.]com
- training[.]web[.]moaby[.]app
- training[.]genuinely-popular-fish[.]explosion[.]cloud
- training[.]safran-aerosystems[.]eleo[.]io
- training[.]training[.]cam[.]ac[.]uk
- training[.]sipermata[.]umum[.]tatausaha8[.]my[.]id
- training[.]dev[.]videnov[.]ro
- training[.]longhorn[.]inxsoftware[.]dev
- training[.]whitesourcesoftware[.]com
dev[.]dev[.]mxb[.]ce-dfw[.]com
- training[.]jhc[.]staging[.]rw1[.]co[.]za
- training[.]www[.]aussiewax[.]com
- training[.]dev[.]umetrics[.]io
- training[.]kpi[.]mx-access[.]com
- training[.]formation-vesa[.]eleo[.]io
- training[.]westus2[.]azurestaticapps[.]net
- training[.]opus-test[.]bmwgroup[.]com
- training[.]itsd-8664[.]flowable[.]io
- training[.]pmd3[.]phishme[.]com
- training[.]jease[.]abdseawarefull[.]wdprapps[.]disney[.]com
- training[.]hkcert22[.]pwnable[.]hk
- training[.]qpulse[.]le[.]ac[.]uk

- training[.]lexisnexisrisk[.]com[.]micros[.]aventri[.]com
- training[.]seq-internal[.]platform[.]dptsprotrans[.]com
- training[.]dev[.]videnov[.]si
- training[.]cmerax[.]com[.]cmerax[.]com
- training[.]order[.]hartadinataabadi[.]co[.]id
- training[.]pnq[.]atpkm[.]com
- training[.]front[.]rapidonkey[.]io
- training[.]nikhad[.]tplerp[.]com
- training[.]7538-sessions-presence-partielle[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]demo-staging[.]eleo[.]io
- training[.]redcap[.]yale[.]edu
- training[.]dhis2[.]mali[.]project[.]urc[.]org
- training[.]veolia[.]eleo[.]io
- training[.]n8n[.]luizeof[.]dev
- training[.]mnestler[.]awsps[.]myinstance[.]com
- training[.]board12[.]glhomes[.]com
- training[.]www[.]roadwayconstructionsolutions[.]com
- training[.]webinar[.]bestworkz[.]com
- training[.]order[.]uteescorporatesales[.]com
- training[.]staging-staging[.]eleo[.]io
- training[.]astoreshop[.]com[.]cdn[.]cloudflare[.]net
- training[.]distributionreport[.]comet[.]wfp[.]org
- training[.]apex[.]hms[.]harvard[.]edu
- training[.]em2[.]sellingplatformconnect[.]amadeus[.]com
- training[.]covid[.]fukuryo[.]id
- training[.]3940-accreditation-lost-alert[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]erp[.]wasdbusiness[.]com
- training[.]sipermata[.]tatausaha8[.]my[.]id
- training[.]neptune[.]schoolbookings[.]co[.]uk
- training[.]formation-hexcel[.]eleo[.]io
- training[.]milleis[.]eleo[.]io
- training[.]typo3[.]web-tue-nl[.]noble-owl[.]maxserv[.]dev
- training[.]cdn[.]dimension[.]hal24k[.]com
- training[.]staging-5em2ouy-hu4zuth6ade6y[.]uk-1[.]platformsh[.]site
- training[.]oasistrial[.]pitt[.]edu
- training[.]empower[.]waf[.]abb
- training[.]itsd-9496[.]flowable[.]io
- training[.]zgr[.]vatptfs[.]com
- training[.]free[.]beeceptor[.]com
- training[.]itsd-9159[.]flowable[.]io
- training[.]velo[.]pl[.]atos[.]net
- training[.]dev[.]videnov[.]mk
- training[.]nextgen[.]jendasolutionssandbox[.]com
- training[.]fra1-de[.]cloudjiffy[.]net
- training[.]opus-int[.]bmwgroup[.]com
- training[.]shops[.]moaby[.]app
- training[.]rpra[.]kzstage[.]com
- training[.]app[.]daylight[.]io
- training[.]lptsi[.]unsoed[.]ac[.]id
- training[.]dev-xyz[.]axiros[.]com
- training[.]typo3[.]tue-nl[.]engaging-griffon[.]maxserv[.]dev
- training[.]2[.]azurestaticapps[.]net
- training[.]cs[.]cert[.]basecamp[.]app
- training[.]referralplatform[.]com[.]00d3k000000vznqea2[.]live[.]siteforce[.]com
- training[.]ips[.]www[.]nadineferont[.]com
- training[.]dev3[.]bluetek[.]co[.]za
- training[.]prod[.]airtrain[.]app

- training[.]safran-university-staging[.]eleo[.]io
- training[.]anhar-alhayat[.]dev1[.]ejaferp[.]com
- training[.]7237-maj-session-longue[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]skyward[.]io[.]skilljarapp[.]com[.]skyward[.]io
- training[.]lynx[.]mythic-beasts[.]com
- training[.]store[.]marjory[.]io
- training[.]clientapi[.]nextgen[.]jjendassolutionssandbox[.]com
- training[.]lemonpoppyseed[.]netkappa[.]work
- training[.]opportunityprospector[.]chartwelldigital[.]com
- training[.]gtwconsortium[.]com[.]gridhosted[.]co[.]uk
- training[.]itsd-9197[.]flowable[.]io
- training[.]accounts[.]hospitality[.]amadeus[.]com
- training[.]lfb[.]eleo[.]io
- training[.]orpea-staging[.]eleo[.]io
- training[.]rwe[.]eleo[.]io
- training[.]qpulseldc[.]le[.]ac[.]uk
- training[.]typo3[.]v11[.]eu-central[.]w3[.]tue[.]nl
- training[.]dev[.]trin[.]net
- training[.]qrm[.]atpkm[.]com
- training[.]online[.]younglife[.]org
- training[.]littleessexacademy[.]com[.]cdn[.]cloudflare[.]net
- training[.]pidashboard[.]harvard[.]edu
- training[.]eng[.]usm[.]my
- training[.]jpd[.]mybluehost[.]me
- training[.]sl[.]eqapt[.]com
- training[.]n[.]client[.]zalon[.]com
- training[.]igpawebsite[.]web[.]illinois[.]edu
- training[.]chechnya[.]gov[.]ru
- training[.]cname[.]360unite[.]com
- training[.]opus-prod[.]aws[.]bmw[.]cloud
- training[.]firearms[.]rcmp[.]gc[.]ca
- training[.]7297-maj-bdp[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]7538-import-historic[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]test-ext[.]engagedmd[.]com
- training[.]range[.]crtcdev[.]net
- training[.]kineis[.]eleo[.]io
- training[.]sit[.]enlivencem[.]com
- training[.]gbfood[.]sigservice-dz[.]com
- training[.]ut[.]umetrics[.]io
- training[.]polypipe[.]monitor[.]softwareimc[.]dev
- training[.]zow83qsq[.]poc[.]claroty[.]com
- training[.]itsd-9171[.]flowable[.]io
- training[.]neumann-mueller[.]elevait[.]io
- training[.]dev[.]videnov[.]gr
- training[.]propeller-uat[.]federato[.]ai
- training[.]miq[.]cbrecn[.]com
- training[.]vantis[.]uas[.]topsky[.]thalesdigital[.]io
- training[.]dev[.]nextpro[.]videnov[.]bg
- training[.]qld[.]rfdsehr[.]io
- training[.]lmspro[.]katimas[.]my
- training[.]mvm-eb-svwinqp[.]mvm[.]ed[.]ac[.]uk
- training[.]swtouch[.]abdseawarefull[.]wdprapps[.]disney[.]com
- training[.]7581-vintage-default[.]ci[.]k8s[.]eleo-dev[.]io
- training[.]ledgebrook-uat[.]federato[.]ai

- carrieris[.]com[.]seattlepsychedelictreatment[.]com
- carrierhvacsmallsolutions[.]smallsolutionsllc[.]com
- carrierwheels[.]tisprojects[.]com
- carrier-one[.]babycarriersi[.]com
- carrierandwholesale[.]stc[.]com[.]sa
- carrieresanpedrone[.]direct[.]quickconnect[.]to
- carrier-411-api-zq65a[.]ondigitalocean[.]app
- carrier-api-pr-403[.]d030[.]aws[.]cldsvc[.]net
- carrier[.]lgtrans24[.]com
- carrier411[.]workers[.]dev
- carrier-invoice-import-qa[.]azurewebsites[.]net
- carrier[.]status[.]polaris[.]synopsys[.]com
- carrier[.]springloadeddivingboard[.]com
- carriersolutionneeds-com[.]mail[.]protection[.]outlook[.]com
- carrier3[.]gk2a[.]in
- carrier[.]2surfablepeninsulas[.]com
- carriere[.]orammdb[.]com
- carrier-api-pr-412[.]d030[.]aws[.]cldsvc[.]net
- carrier-api-pr-435[.]d030[.]aws[.]cldsvc[.]net
- carrierclass-co-nz[.]mail[.]protection[.]outlook[.]com
- carrier-api[.]internal[.]facerack[.]co[.]uk
- carrierip[.]net[.]mx4[.]netcarrier[.]rcimx[.]net
- carrier-api-pr-450[.]d030[.]aws[.]cldsvc[.]net
- carrieragreement[.]demo[.]coyote[.]com[.]cdn[.]cloudflare[.]net
- carrier-api[.]leo[.]internal[.]mistressofmalt[.]com
- carrier-grade-nat-ip-025[.]boaar1[.]cgn[.]fiberby[.]net
- carrier-blackscholes[.]quarantine-pnap[.]web-hosting[.]com
- carrier-api-pr-436[.]d030[.]aws[.]cldsvc[.]net
- carrier[.]frozen-iglooswerebuilt49[.]com
- carrierenas01[.]direct[.]quickconnect[.]to
- carrieres[.]groupeinvestors[.]com
- carriere-nl[.]hoyer-group[.]com
- carrierusps[.]redirectme[.]net
- carriers[.]bc[.]platform[.]sh
- carrier-freedom-api[.]duck[.]dev[.]promos[.]t-mobile[.]com
- carrier42qha009n38qha009n[.]mega-21[.]ru
- carrieresduhainaut-co-uk[.]mail[.]protection[.]outlook[.]com
- carrierrace-com[.]mail[.]protection[.]outlook[.]com
- carrier-api-pr-448[.]d030[.]aws[.]cldsvc[.]net
- carrier-api[.]don[.]internal[.]mistressofmalt[.]com
- carrier[.]prod[.]onrampcard[.]com
- carrier-grade-nat-ip-024[.]vgcar1[.]cgn[.]fiberby[.]net
- carriers-fastway-live[.]azurewebsites[.]net
- carrier[.]egy1[.]online
- carrier1503[.]zendesk[.]com
- carrier24[.]r7tj[.]in
- carrier[.]ghost[.]io
- carriereswitch-nl[.]mail[.]protection[.]outlook[.]com

- carrier-accessories[.]babycarriersi[.]com
- carrier-api-pr-445[.]d030[.]aws[.]cldsvc[.]net
- carrierose[.]cdanjoyner[.]com
- carrieridesign-abbigliamento[.]myshopify[.]com
- carrier-management[.]dev01[.]tk[.]dev
- carrier-api-pr-420[.]d030[.]aws[.]cldsvc[.]net
- carriere[.]folionetwork[.]site
- carrier-api-pr-404[.]d030[.]aws[.]cldsvc[.]net
- carrieres[.]energienb[.]com
- carrier-grade-nat-ip-003[.]vgcar2[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-020[.]vbyar1[.]cgn[.]fiberby[.]net
- carrier[.]okcargo[.]io
- carrier-auctions[.]quarantine-pnap[.]web-hosting[.]com
- carrier-command[.]quarantine-pnap[.]web-hosting[.]com
- carrier-integration[.]internal[.]ie[.]test[.]gelato[.]tech
- carriers-graphql[.]dev[.]freightbox[.]com
- carrier-api-pr-428[.]d030[.]aws[.]cldsvc[.]net
- carrierportal[.]amerigasapps[.]com
- carrieres-malet[.]wildixin[.]com
- carrier[.]hashtechorange[.]com
- carrier-63-175-185[.]connectatelecom[.]cat
- carrier-budget[.]quarantine-pnap[.]web-hosting[.]com
- carrier-grade-nat-ip-026[.]vgcar1[.]cgn[.]fiberby[.]net
- carriersconnectplus-com[.]mail[.]protection[.]outlook[.]com
- carriers-write[.]dev[.]freightbox[.]com
- carriere[.]powidian[.]com
- carrier-ftp[.]oneworldcourier[.]com[.]au
- carriers-borders-live[.]azurewebsites[.]net
- carriers-20210901[.]pod-1[.]braid-inventory[.]com
- carriere[.]meinforum[.]net
- carrier-api-pr-413[.]d030[.]aws[.]cldsvc[.]net
- carrier-woven[.]babycarriersi[.]com
- carrier5-net[.]mxguardian[.]net
- carrieres[.]aca[.]nexia[.]fr
- carrier-world[.]mail[.]protection[.]outlook[.]com
- carrier-grade-nat-ip-013[.]vgcar2[.]cgn[.]fiberby[.]net
- carrier-austrian[.]quarantine-pnap[.]web-hosting[.]com
- carriers[.]ouiris[.]com
- carrieres[.]attitudefraiche[.]stagingsept24[.]com
- carrierwheels[.]axq[.]ozp[.]mybluehostin[.]me
- carrieres-sur-seine[.]innoventure[.]eu
- carriereac-com[.]mail[.]protection[.]outlook[.]com
- carrier-maintenance[.]elrewaad[.]com
- carrier-api-pr-414[.]d030[.]aws[.]cldsvc[.]net
- carrier-api-pr-430[.]d030[.]aws[.]cldsvc[.]net
- carrier99[.]42bootsdancing[.]com
- carriere-gestion-lagence[.]humakare[.]ca

- carriereinutrecht-nl[.]mail[.]protection[.]outlook[.]com
- carrier-schedule[.]cloudintercorpretail[.]pe
- carrierandcouncelling[.]car[.]blog
- carrier-api[.]internal[.]masterofmalt[.]com
- carrierinfo-ca[.]mail[.]protection[.]outlook[.]com
- carrierhub[.]wellbeingzone[.]co[.]uk
- carrier1trucking-com[.]mail[.]protection[.]outlook[.]com
- carriermsportallinux[.]azurewebsites[.]net
- carrier-aid[.]quarantine-pnap[.]web-hosting[.]com
- carrier-grade-nat-ip-016[.]boaar1[.]cgn[.]fiberby[.]net
- carrieritaliasrl[.]smooos[.]com
- carrieres-du[.]mobility-cloud[.]io
- carrierexpressco[.]jpglobalengineering[.]com
- carrieres[.]lfde[.]com
- carriers[.]app[.]render[.]com
- carriertest-328fc1ac20ebb1f92e7f8f44ffec0442-0000[.]us-south[.]stg[.]containers[.]appdomain[.]cloud
- carriers-nightmare-cruz-steering[.]trycloudflare[.]com
- carrierws[.]qa[.]consignor[.]com
- carriereilly-com[.]mail[.]protection[.]outlook[.]com
- carrier6[.]gk2a[.]in
- carrier-grade-nat-ip-011[.]vgcar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-027[.]vgcar1[.]cgn[.]fiberby[.]net
- carrier-basel[.]quarantine-pnap[.]web-hosting[.]com
- carrier[.]alsiyanuh[.]com
- carriergenuistutoral[.]digirises[.]com
- carrier-api-pr-423[.]d030[.]aws[.]cldsvc[.]net
- carrier-corrections[.]favor-cockpit-int[.]azure[.]bmw[.]cloud
- carrier-enrichment[.]pages[.]dev
- carrier-api-pr-444[.]d030[.]aws[.]cldsvc[.]net
- carriere[.]nhc[.]care
- carrier[.]servicecenter-tw[.]com
- carrierintegrationsystem[.]dhl[.]com
- carrier-management[.]app[.]aks[.]prod01[.]tk[.]dev
- carrier-cartel[.]quarantine-pnap[.]web-hosting[.]com
- carrier-grade-nat-ip-007[.]vgcar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-014[.]boaar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-020[.]boaar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-021[.]vbrar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-028[.]vgcar1[.]cgn[.]fiberby[.]net
- carrier-bounded[.]quarantine-pnap[.]web-hosting[.]com
- carrier-prod[.]netlify[.]app
- carrieres[.]psychobunny[.]com
- carrieresducharme-com[.]mail[.]protection[.]outlook[.]com
- carrier-appreciation[.]quarantine-pnap[.]web-hosting[.]com
- carrier-mode[.]tnx[.]co[.]nz
- carriere[.]tempurl[.]host
- carrieressare-fr02c[.]mail[.]protection[.]outlook[.]com
- carrieragreement[.]fast[.]coyote[.]com[.]cdn[.]cloudflare[.]net

- carrier-grade-nat-ip-003[.]vgcar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-032[.]vbrar1[.]cgn[.]fiberby[.]net
- carrier[.]js[.]org
- carrierportalapi[.]amerigasapps[.]com
- carriercentral[.]newegg[.]com
- carrier[.]greensys[.]io
- carriertransitapi-prod[.]azurewebsites[.]net
- carrierchuno-stories-site[.]webstory[.]link
- carriertest[.]us-south[.]stg[.]containers[.]appdomain[.]cloud
- carriers[.]uat[.]trackmatic[.]cloud
- carrier-management[.]prod01[.]tk[.]dev
- carrier-api-pr-427[.]d030[.]aws[.]cldsvc[.]net
- carrier9526[.]zendesk[.]com
- carriere-sante-lagence[.]humakare[.]ca
- carrierip[.]net[.]mx3[.]netcarrier[.]rcimx[.]net
- carriermedia[.]studiosight[.]com
- carriermediaco[.]studiosight[.]com
- carriere[.]montpak[.]ca
- carrier2[.]gk2a[.]in
- carrier-pidgeon[.]staging[.]zonarsystems[.]net
- carrier-grade-nat-ip-030[.]vgcar1[.]cgn[.]fiberby[.]net
- carrier-capitalism[.]quarantine-pnap[.]web-hosting[.]com
- carrier-ceteris[.]quarantine-pnap[.]web-hosting[.]com
- carrierpoint[.]in[.]net
- carrierainbowpsychology-com-au[.]mail[.]protection[.]outlook[.]com
- carrierlubicz-pl01i[.]mail[.]protection[.]outlook[.]com
- carrierecafe[.]tst[.]rb-media[.]nl
- carrierhost[.]com[.]helpingarticles[.]com
- carrier-pidgeon[.]production[.]zonarsystems[.]net
- carrier-grade-nat-ip-009[.]vbyar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-014[.]vgcar2[.]cgn[.]fiberby[.]net
- carrierholdings-com[.]mail[.]protection[.]outlook[.]com
- carrier[.]cloudapps[.]digital
- carrier[.]dev[.]roin[.]co
- carrier-borderos-favor-cockpit-int[.]azure[.]bmw[.]cloud
- carriergeniustutorial[.]in[.]digirises[.]com
- carrierlogicwebsite[.]kinsta[.]cloud
- carrier-line-parcel-official-drop[.]dns-dns[.]com
- carrier[.]dst[.]uz
- carrierrate[.]alphaautotrimltd[.]com
- carriermax5[.]pages[.]dev
- carriers-chartering[.]gr[.]com
- carrierenterprise[.]hosted-by-discourse[.]com
- carrier[.]borovecgroup[.]cz
- carriergud-d5aee7e5d7aa474c8f73fb30ca3a100d-dbserver[.]carriergud-d5aee7e5d7aa474c8f73fb30ca3a100d-dbserverprivate[.]mysql[.]database[.]azure[.]com
- carrier[.]wpenginepowered[.]com
- carrier[.]meritlogistics[.]com
- carrieres[.]jutheau-husson[.]com
- carriere[.]carsat-centreouest[.]fr
- carrierip[.]net[.]mx2[.]netcarrier[.]rcimx[.]net

- carrier[.]usevoyage[.]com
- carrierwheels[.]gridlabstechnologies[.]com
- carrier[.]galapagblog[.]demo[.]staging[.]skinport[.]surf
- carrieres-sur-seine[.]ethereality[.]eu
- carrier[.]keenetic[.]pro
- carrier-api-pr-416[.]d030[.]aws[.]cldsvc[.]net
- carriermax22[.]pages[.]dev
- carrier4291[.]keenetic[.]name
- carrierportal-web[.]lactalis[.]com
- carrier-grade-nat-ip-010[.]boaar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-017[.]vgcar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-018[.]vbrar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-022[.]vbrar1[.]cgn[.]fiberby[.]net
- carrier-api-pr-442[.]d030[.]aws[.]cldsvc[.]net
- carrier[.]fix-devic[.]com
- carrier[.]rag-cloud[.]hosteur[.]com
- carriercheck[.]azurewebsites[.]net
- carrieragreement[.]test[.]coyote[.]com[.]cdn[.]cloudflare[.]net
- carriers-butler-india-tv[.]trycloudflare[.]com
- carriers[.]aramcom[.]com
- carrier-raven[.]vivareal[.]com[.]br
- carrier-management[.]test[.]toolkit[.]co
- carrier[.]tolem[.]asia
- carrier[.]8gymshorts[.]com
- carrier5[.]247work365[.]com
- carrier-grade-nat-ip-021[.]vgcar1[.]cgn[.]fiberby[.]net
- carriereardon[.]sunflowerhomes[.]info
- carrier[.]flying-shadow[.]com
- carrier-api-pr-449[.]d030[.]aws[.]cldsvc[.]net
- carrier-call[.]quarantine-pnap[.]web-hosting[.]com
- carrier40[.]7mirrorreflections[.]com
- carrier-grade-nat-ip-016[.]vbrar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-019[.]vgcar2[.]cgn[.]fiberby[.]net
- carrierhouse-co[.]sop[.]sjj[.]myblueh ost[.]me
- carrieratc-ae01i[.]mail[.]protection[.]outlook[.]com
- carrier-api-pr-406[.]d030[.]aws[.]cldsvc[.]net
- carrier[.]benpao56[.]com
- carrier[.]goalpes[.]ru
- carrier[.]colorfulpinwheel[.]com
- carrier-gw[.]sfr[.]fr
- carrier[.]alealamiy[.]com
- carrier[.]roin[.]co
- carrier-api-pr-426[.]d030[.]aws[.]cldsvc[.]net
- carrier-management[.]app[.]aks[.]dev01[.]tk[.]dev
- carrier[.]amaintenanc[.]com
- carriere-ventes[.]autolemieux[.]com
- carrier-api-pr-395[.]d030[.]aws[.]cldsvc[.]net
- carrier-api-pr-429[.]d030[.]aws[.]cldsvc[.]net
- carrierservices[.]marsh[.]com
- carrier-management[.]toolkit[.]co
- carrier[.]parknowtech[.]net
- carrier[.]forumeg[.]com
- carrieres[.]allen-entrepreneurgeneral[.]com
- carrier-api-pr-446[.]d030[.]aws[.]cldsvc[.]net

- carriergud-d5aee7e5d7aa474c8f73fb30ca3a100d-dbserver[.]mysql[.]database[.]azure[.]com
- carriermax[.]pages[.]dev
- carrierip[.]net[.]mx1[.]netcarrier[.]rcimx[.]net
- carrier-api-pr-391[.]d030[.]aws[.]cldsvc[.]net
- carrier[.]login[.]mailvip[.]co
- carrier-api-pr-402[.]d030[.]aws[.]cldsvc[.]net
- carrier-bonds[.]quarantine-pnap[.]web-hosting[.]com
- carrier[.]gitapp[.]si
- carrier-dev[.]nz[.]netlogixgroup[.]io
- carriermax23[.]pages[.]dev
- carrier[.]login[.]yalroo[.]jp[.]net
- carrier-borderos[.]favor-cockpit-int[.]azure[.]bmw[.]cloud
- carrierapi[.]a-b[.]mn
- carrier-borderos[.]favor-cockpit-int[.]bmwgroup[.]com
- carrieroil--jp[.]j-dns[.]ne[.]jp
- carrier[.]xinix[.]co[.]uk
- carrier[.]xxii-century[.]wezomteam[.]in[.]ua
- carrier[.]upbeattangodancing[.]com
- carriergame-io[.]mail[.]protection[.]outlook[.]com
- carrierportal[.]trimblevisibility[.]com
- carrier[.]15983[.]xyz
- carriera[.]battistolli[.]it
- carrier-schedule[.]cloudintercorpretail-uat[.]pe
- carrier-api-pr-451[.]d030[.]aws[.]cldsvc[.]net
- carriereinspirante[.]bevdev2[.]ca
- carriereduvuache[.]p2[.]mon-site[.]co
- carrier-api-pr-447[.]d030[.]aws[.]cldsvc[.]net
- carriersignal[.]info[.]at
- carrier2[.]coppel[.]com[.]edgekey[.]net
- carrier[.]watch-eagleeye[.]com
- carrier-api-pr-459[.]d030[.]aws[.]cldsvc[.]net
- carrier-grade-nat-ip-006[.]inxar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-012[.]vgcar2[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-026[.]vbrar1[.]cgn[.]fiberby[.]net
- carrier-grade-nat-ip-029[.]vgcar2[.]cgn[.]fiberby[.]net
- carriere[.]amltd[.]net
- carriere[.]adapei-aria[.]com
- carriers-uat[.]comcast[.]com
- carriere[.]newlife-international[.]ca
- carrier-free[.]fastly-terrarium[.]com
- carrier[.]bosphor[.]com
- carrier-api-pr-400[.]d030[.]aws[.]cldsvc[.]net
- carrier[.]touchsms[.]com[.]au

Sample Properties Flagged as Malicious During the Malware Check Dated 24 October 2022

- dhl-express-s[.]blogspot[.]com
- login[.]vpasrnbc[.]jp[.]rpughy[.]top
- login[.]microsoft[.]msoftlog[.]ga
- login[.]microsoft-online[.]sccm[.]info
- login[.]secure2[.]p2p118[.]com
- login[.]hokkokubank[.]logln-microsoftonline[.]com

- login[.]northlane[.]comsecure-rcclusa[.]ygto[.]com
- login[.]4748484747[.]tyfix[.]click
- login[.]outlook[.]corporativo-stone[.]com
- login[.]auth[.]login[.]micrsoftonline[.]net
- login[.]northlane[.]coml-rccl[.]mrbonus[.]com
- login[.]microsoftonline[.]plureaw[.]com
- login[.]live[.]com[.]ragusahomedecor[.]com
- login[.]sso[.]charter[.]net[.]in
- login[.]securibuytherniroscodfyoutbook[.]mefound[.]com
- login[.]login2[.]corporativo-stone[.]com
- login[.]portal[.]corporativo-stone[.]com
- login[.]bankid[.]no[.]i189[.]top
- login[.]anz[.]com[.]internetbanking[.]au-th[.]com
- login[.]shearpointexcel[.]fr[.]mydsomaneger[.]com
- login[.]microsoftonline[.]cpatre[.]com
- login[.]anz[.]com[.]rcd-io[.]co
- login[.]officeshare[.]fr[.]nearcodconsulting[.]com
- login[.]micro-verify[.]wifi-portal[.]me
- login[.]loauh9283793904[.]sinoqlass[.]com
- login[.]account[.]logins-verify[.]tk
- login[.]northlane[.]comwirecard[.]dns04[.]com
- login[.]northlane[.]com2[.]serveuser[.]com
- login[.]vpasrnbc[.]jp[.]vhyyuk[.]top
- login[.]mobile-de-a2[.]gt[.]com[.]bo
- login[.]login[.]outiook-o365[.]live
- login[.]i[.]gefrarn[.]com
- login[.]shopping[.]yahoo[.]ca51r[.]cn
- login[.]i[.]aeon[.]jp[.]ffymkuaiqian001[.]top
- login[.]northlane[.]com[.]dorksid[.]com
- login[.]northlane[.]salarybonus[.]zyns[.]com
- login[.]okta[.]login[.]nexth[.]ink
- afmc[.]com[.]au
- eastonlawyers[.]com[.]au
- barwonbluff[.]com[.]au
- cwsandstone[.]com[.]au
- alphawealthcreation[.]com[.]au
- 2allmobile[.]net
- bsa-dakar[.]com
- jedeconstruction[.]com
- jp[.]bsa-dakar[.]com
- ns1[.]cp-47[.]webhostbox[.]net
- ns2[.]cp-47[.]webhostbox[.]net
- speyerholding[.]com
- toptonog[.]mn