From Counties to Banks: Tracing the Footprint of Ransomware Attack IoCs

Table of Contents

Executive Report

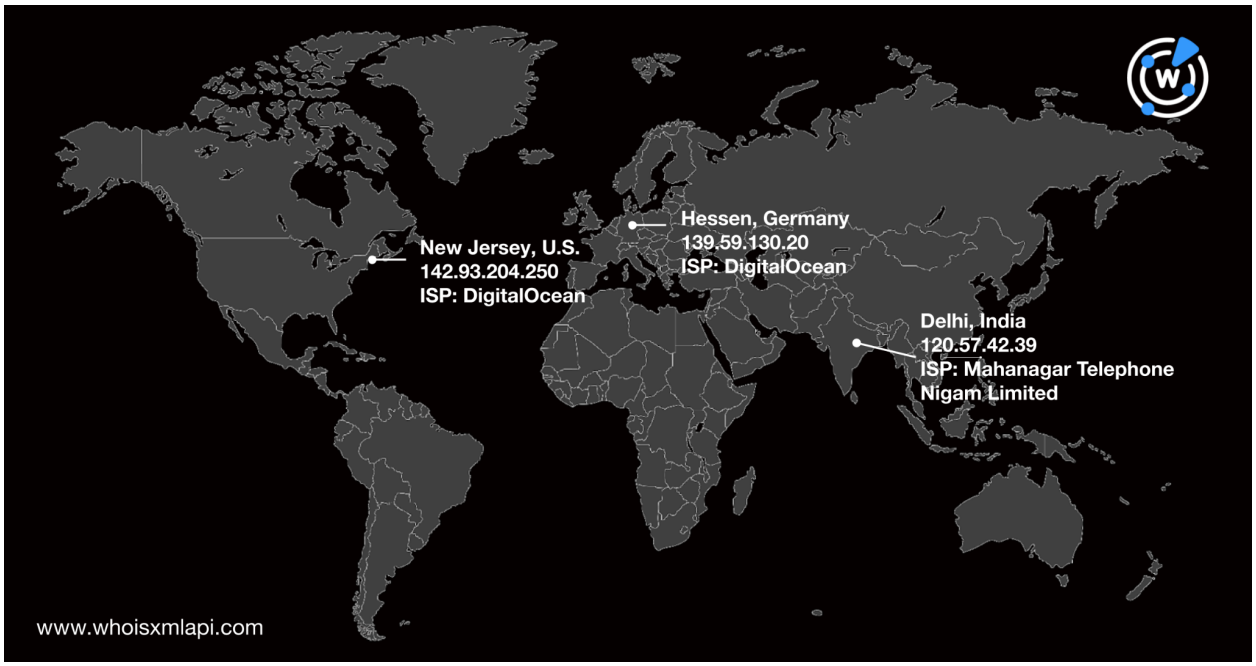
SecurityScorecard published a report on a cyber attack that a U.S. county victim announced on 11 September 2022. With ransomware attacks against local government units increasing in the past few years, WhoisXML API researchers decided to build on the list of IP addresses related to the attacks. Our findings include:

- One of the IP addresses tagged as an indicator of compromise (IoC) resolved to one domain.
- The connected domain's deep WHOIS history pointed us to more than 4,000 additional artifacts, some of which have already figured in malicious campaigns.
- The Cryxos trojan IoCs currently resolving to domains were mostly geolocated in Europe.
- We found more than 390 domains connected to the Cryxos IoCs, several of which were subdomains of legitimate domains.
- Some of the subdomains connected to the Cryxos IoCs were malicious, including bank-related cybersquatting properties. Further expansion led us to hundreds of malicious domains targeting Chase Bank.

What We Know about the Attack

SecurityScorecard's analysis of the network flow revealed three suspicious IP addresses communicating with victims' vulnerable software and open ports. These communications happened in July, leading to a service disruption on 11 September 2022.

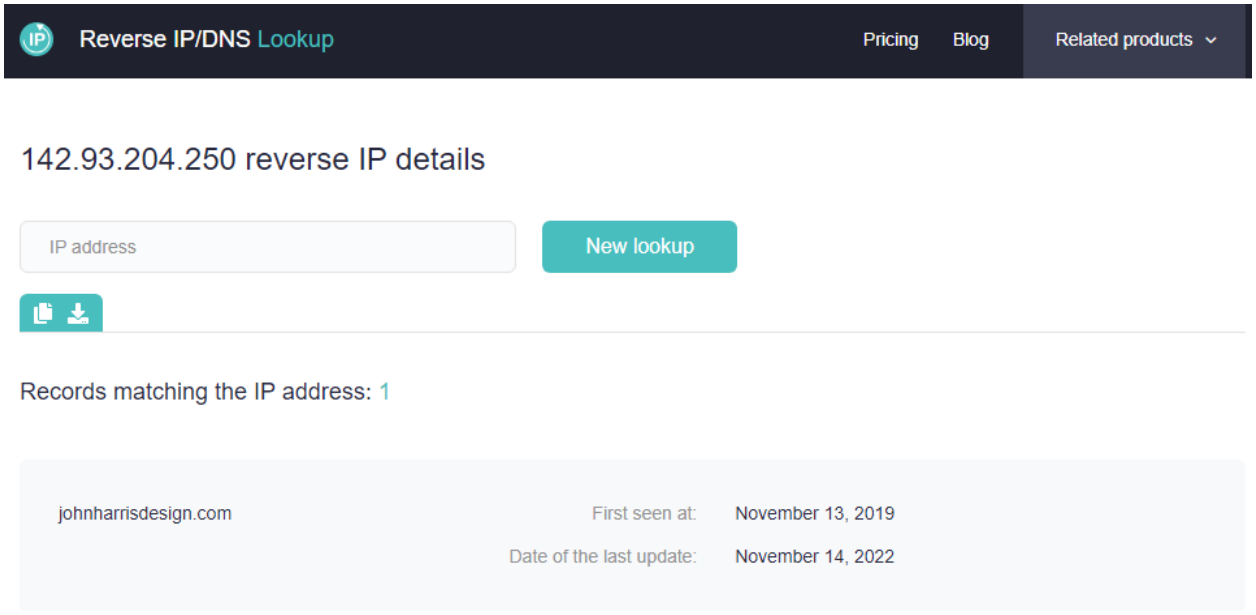
Several security engines flagged a couple of the IP addresses as malicious. Both of these were managed by Digital Ocean and geolocated in Hessen, Germany and New Jersey, U.S. The other IP address was geolocated in India.



IoC Analysis and Expansion

Reverse IP lookups on the IP addresses tagged as IoCs revealed that only 142[.]93[.]204[.]250 resolved to the domain johnharrisdesign[.]com. This IP address has been observed to carry out brute force attacks. SecurityScorecard also reported that the IP address transferred 352.26KB of data to one of the IP addresses.

The IP resolution was first seen in November 2019 and last updated in November 2022, a few weeks after its involvement in an attack. The domain has been associated with the malicious IP address since 2019 and around the time the attack occurred.



We followed the trail to expand the list of IoCs and find more suspicious web properties potentially connected to the actors behind the attack.

Gleaning Insights from WHOIS History

The current WHOIS record of johnharrisdesign[.]com is privacy protected. However, its historical WHOIS records revealed some consistent data., including the same registrant name, state, and country throughout its years-long history.

- **Registrar:** GoDaddy
- **Registrant name:** John Harris
- **Registrant state or region:** Pennsylvania
- **Registrant country:** U.S.

We also discovered a couple of unredacted registrant email addresses prior to WHOIS data redaction.

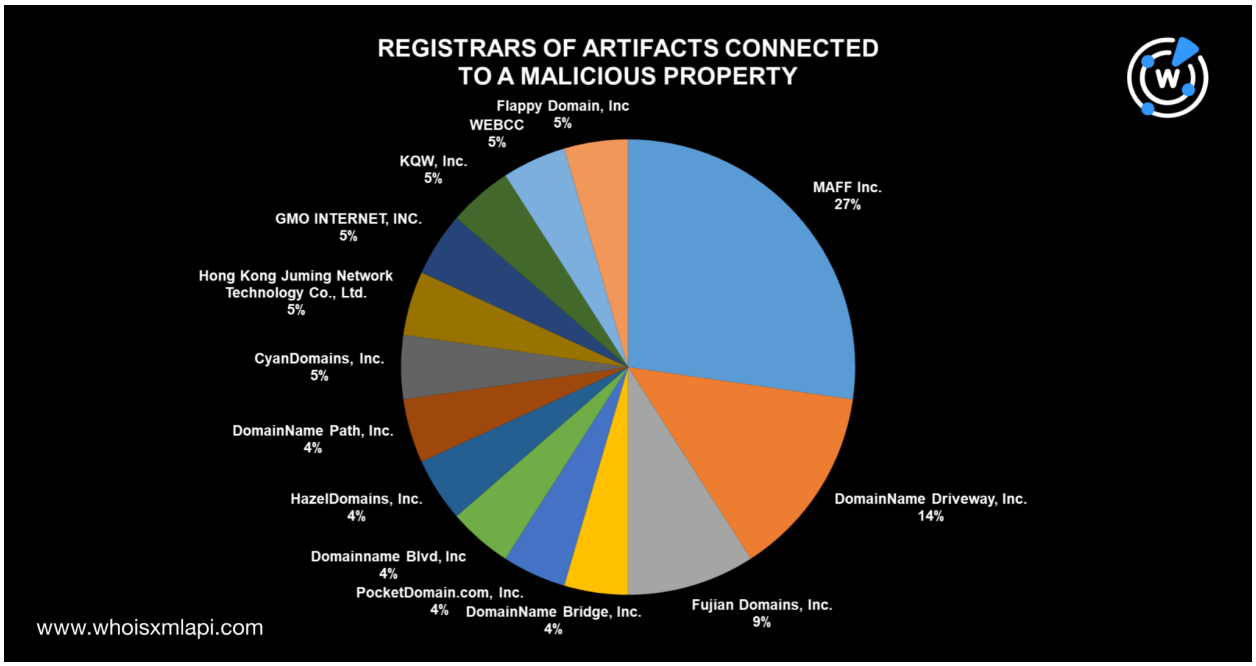
Uncovering Connected Domains

We found more than 4,400 domain names registered by the same entity at one point in time. While some of them may have coincidental connections since the registrant's name is quite common, a bulk malware check on the properties revealed that some of them have already been weaponized.

Most of the malicious artifacts had deep WHOIS histories, allowing us to retrieve four unredacted email addresses. One of them was used to register more than 1,300 domains. It's

wise to pay attention to such artifacts since they are closely related to a confirmed malicious domain.

A bulk WHOIS lookup on the properties revealed that the domains were managed by various registrars despite being owned by the same registrant. The chart below shows their distribution based on registrar.



Beyond the Attack and into the Inner Workings of Cryxos

One way threat actors gain access to victims' systems was via the Cryxos trojan. The malware facilitated callback phishing campaigns by alerting targets about fake malware infections. It then prompted users to call a phone number to fix the problem.

We analyzed the Cryxos IoCs published by several sources. According to IP geolocation lookups, seven of the nine currently resolving properties tagged as IoCs were geolocated in Europe.

Reverse DNS searches for the IoCs pointed us to more than 390 domains that shared their IP hosts. Most of the subdomains resided on dynamic DNS service domains, such as ddns[.]net, bounceme[.]net, and hopto[.]org.

Some of the subdomains were flagged as malicious during our malware check. They included those that appear to have used domain generation algorithms (DGAs). Some also imitated the digital properties of well-known financial institutions, specifically Chase Bank and Glacier Bank.

Expanding the List of Cryxos IoCs

Again, we followed the trail the DNS intelligence presented. Using Domains & Subdomains Discovery, we looked for subdomains bearing the string “chaseauthverify,” which was used in one of the malicious properties. We found 26 subdomains, about one-third of which have already figured in malicious campaigns.

Expanding our search to include web properties containing “chase,” “auth,” and “verify” in any order, we found 1,446 domains. A bulk malware check revealed that 36% of these subdomains or their root domains have already been weaponized.

—

Threat hunting may seem like a wild goose chase at the start, especially since threat actors are often stealth masters. In this investigation, for instance, we started with only three IP addresses

tagged as IoCs in a U.S. county cyber attack. Only one of the IP addresses had a related domain, leading us to several malicious domains connected to the same registrant name.

Our investigation of the Cryxos trojan IoCs led to a similar scenario. Nine resolving IoCs led us to hundreds of malicious digital resources, possibly targeting Chase Bank and its clients.

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 Attack IoCs from SecurityScorecard

- 142[.]93[.]204[.]250
- 120[.]57[.]42[.]39
- 120[.]57[.]42[.]39

Sample Domains Possibly Related to the County Cyber Attack

- teame4e[.]com
- shanahanswines[.]com
- shanahanswines[.]com[.]au
- impress[.]com[.]au
- mclarenvalewineonline[.]com
- barossavalleyshiraz[.]com
- horsepowerautomarketing[.]com
- horsepowerautoservice[.]com
- prosourceagency[.]com
- proinsx[.]com
- widebaydrones[.]com[.]au
- kempservices[.]com[.]au
- titansinkware[.]com
- kentstreetautos[.]com
- racals[.]ac[.]uk
- cleanstartcharlotte[.]com
- peterpanfan[.]com
- barbarianeffeminate[.]com
- beyondthepale[.]com[.]au
- dnart[.]us
- 47stphoto[.]us
- dayzim[.]us
- tiana[.]us
- vnga[.]us
- peachtreechecks[.]us
- psiwebware[.]us
- drosis[.]us
- opteka[.]us
- escapecoachtours[.]com
- elmoblue[.]com
- chuthathaimassage[.]com
- comanchecajun[.]com
- cursecap[.]com
- davis-hendrixfantasyband[.]com
- apostlejohnharris[.]com
- beaconbright[.]com
- boyfellinpond[.]com
- barossavalleywineonline[.]com
- spectrum5[.]com[.]au
- rjharris[.]com[.]au
- wellseys[.]com[.]au
- harrismeadery[.]com
- townandcountryfinance[.]com[.]au
- havrelafitte[.]com

- nchd[.]net
- tandcwa[.]com[.]au
- houseshake[.]dk
- dayzim[.]tw
- robinsoncollege[.]nsw[.]edu[.]au
- townandcountryrealty[.]com[.]au
- worklified[.]dk
- townandcountrywa[.]com[.]au
- roobard[.]com[.]au
- jamesenglund[.]com[.]au
- kosform[.]com[.]au
- nationalcomputerhelpdesk[.]net[.]au
- pkfconstructions[.]net[.]au
- harrisandson[.]com[.]au
- pkfc[.]com[.]au
- cryptonewsnetworktoday[.]com
- harris-furniture[.]com[.]au
- virtualgstore[.]com
- currituckbbq[.]com
- raindropinvestments[.]us
- harbar[.]us
- hychem[.]us
- cseepac[.]us
- harbingermotors[.]us
- driveharbinger[.]us
- lifesatrip[.]us
- thegentlewolf[.]us
- tks-usa[.]us
- dreamjobs[.]us
- bshi[.]net[.]au
- theartboxla[.]com
- danielharrisdesign[.]com[.]au
- vertical-growth-marketing[.]com
- johnharris-design[.]com
- platinumgloballed[.]com
- yinnar[.]vic[.]au
- thegreatnzfilmco[.]com
- escapecoachtours[.]com[.]au
- otherworldlyinvestigations[.]com
- uniseal[.]net[.]au
- linkprojects[.]com[.]au
- milesdavis-tribute-sheetzofsound[.]com
- xanaka[.]com
- blueskyeheavyindustries[.]au
- kempservices[.]net[.]au
- wildlifeexperiences[.]com[.]au
- bowentherapysandywaugh[.]com[.]au
- animalbowenaustralia[.]com[.]au
- thecheesetrap[.]com
- platinumglobalpainting[.]com
- bgsandbox[.]com
- tidetime[.]us
- mjspizzabase[.]com[.]au
- townandcountrylending[.]com[.]au
- caosdj[.]com
- thykingdomcometour[.]com

Sample Cryxos Trojan IoCs

- 134[.]249[.]116[.]78
- 212[.]83[.]46[.]50
- 216[.]58[.]213[.]142
- 216[.]58[.]213[.]174
- 45[.]77[.]226[.]209
- 4750wsh25[.]ddns[.]net
- 5[.]62[.]56[.]255
- 54[.]152[.]33[.]249
- 92[.]63[.]197[.]112
- 92[.]63[.]197[.]60
- aeiziaezieidiebg[.]ru
- aneoeauhiazegfiz[.]ru
- ashihsijaediaehf[.]ru
- booomaahuuoooapl[.]ru

- c1[.]allocal[.]info
- colombiatelecomunicaciones[.]duckdns[.]org
- doomp3[.]net
- eoufaoeuhoauengi[.]ru
- iuefgauiaiduihgs[.]ru
- joshel[.]com
- jquery[.]je
- jquery[.]jp
- maeobnaoefhgoajo[.]ru
- plpanaifheaighai[.]ru
- porkhalal[.]site

Sample Artifacts Related to the Cryxos Trojan

- 0155[.]de
- tokyo-malaw[.]jp
- 032hiddenproxy[.]16-b[.]it
- 01januverznd-maak[.]ddnsking[.]com
- 021mt901inf0[.]myftp[.]org
- 046412647[.]box[.]freepro[.]com
- 02-frgo[.]serveftp[.]com
- 04vb[.]64-b[.]it
- 007dazhanhuangjiaduchangdianying[.]vpndns[.]net
- 002wellsfargo[.]ddns[.]net
- 045640410[.]box[.]freepro[.]com
- 03gw[.]soundcast[.]me
- 02lf[.]mypi[.]co
- portal[.]tokyo-malaw[.]jp
- 02z0[.]dnsup[.]net
- 05secblokchin[.]myvnc[.]com
- 063264822[.]box[.]freepro[.]com
- junichi-tanaka[.]com
- 0[.]z3n[.]nl
- 00e7dc16-1994-4431-b5da-9400a8340022[.]cloudapp[.]net
- 04perfilacesso[.]ddns[.]net
- 05paypal-secure[.]myvnc[.]com
- 007802667[.]box[.]freepro[.]com
- 01tru-secist[.]serveftp[.]com
- 03protectmtb[.]ddns[.]net
- 03hq[.]64-b[.]it
- 003003003[.]com
- 00506004e697[.]ownip[.]net
- 03recovermtb[.]ddns[.]net
- 032procracking[.]16-b[.]it
- 041675009[.]box[.]freepro[.]com
- suzukake-rl[.]jp
- 009s[.]vpndns[.]net
- lifesanmeirecip[.]com
- 05athwebonline-bo[.]servehttp[.]com
- filesendx[.]com
- 0187[.]de
- 0022[.]vpndns[.]net
- 02verfiyusaa[.]ddns[.]net
- nekosenseiblog[.]com
- 0021585jhuttgeedd[.]redirectme[.]net
- 00196900[.]xyz
- 001001001[.]com
- 01xi[.]xyz
- re-menn[.]com
- mandasogo[.]com
- 049535368[.]box[.]freepro[.]com
- 0021wellsid0021use0[.]myftp[.]org
- suzukaen[.]com
- sozoku[.]tokyo-malaw[.]jp
- 0-st[.]16-b[.]it

Sample Properties Flagged as Malicious During the Malware Check Dated 2 December 2022

- dunamisathletics[.]com
- dillo[.]org[.]uk
- emergencyleash[.]org
- chapropertydatabase[.]com
- 010uth-usaa[.]sytes[.]net
- 021252478[.]box[.]freepro[.]com
- 02gla0ciergj07[.]hopto[.]org
- 030358937[.]box[.]freepro[.]com
- 03chaseauthverify[.]hopto[.]org
- 042061052[.]box[.]freepro[.]com
- 04gla0cierbk03[.]hopto[.]org
- secure-07chaseauthverify[.]dns05[.]com
- www[.]secure-07chaseauthverify[.]dns05[.]com
- mail[.]secure-07chaseauthverify[.]dns05[.]com
- cpanel[.]secure-07chaseauthverify[.]dns05[.]com
- webdisk[.]secure-07chaseauthverify[.]dns05[.]com
- webmail[.]secure-07chaseauthverify[.]dns05[.]com
- cpcalendars[.]secure-07chaseauthverify[.]dns05[.]com
- cpcontacts[.]secure-07chaseauthverify[.]dns05[.]com
- chase-verify-auth[.]serveuser[.]com
- verifychaseaccauth[.]sytes[.]net
- cverifychase0b3auth[.]sytes[.]net
- verify12chasewebauth[.]dns04[.]com
- verifying-auth-chase[.]itemdb[.]com
- www[.]chase-verify-auth[.]serveuser[.]com
- mail[.]chase-verify-auth[.]serveuser[.]com
- www[.]verifychaseaccauth[.]sytes[.]net
- authverifychaseaccount[.]dns1[.]us
- chase-secureverifyauth9[.]dns05[.]com
- chase-secureverifyauth7[.]dns05[.]com
- chase3ecure-verifyauth03[.]dns04[.]com
- host-verifymychase-auth[.]dns04[.]com
- chase-secureverifyauth8[.]dns04[.]com
- chase-secureverifyauth0[.]dns05[.]com
- mail[.]verifychaseaccauth[.]sytes[.]net
- mail[.]cverifychase0b3auth[.]sytes[.]net
- chase-secureverifyauth1[.]dns05[.]com
- chase-secureverifyauth4[.]dns05[.]com
- www[.]cverifychase0b3auth[.]sytes[.]net
- host-verifymychase-auth3[.]dns05[.]com
- host-verifymychase-auth6[.]dns04[.]com
- cpanel[.]chase-verify-auth[.]serveuser[.]com
- chase3ecure-verifyauth05[.]dns04[.]com
- www[.]verify12chasewebauth[.]dns04[.]com
- www[.]verifying-auth-chase[.]itemdb[.]com
- webmail[.]chase-verify-auth[.]serveuser[.]com
- sec02-authenchase-verify[.]dynamic-dns[.]net
- chase-secureverifyauth12[.]dns05[.]com

- chase3ecure-verifyauth02[.]dns04[.]com
- host-verifymychase-auth5[.]my03[.]com
- chase3ecure-verifyauth00[.]dns05[.]com
- chase-secureverifyauth13[.]dns04[.]com
- mail[.]verifying-auth-chase[.]itemdb[.]com
- loginauth007b-verifychase[.]dynamic-dns[.]net
- secure05-chaseeauthverify[.]itsaol[.]com
- authverifysecure07b-chase[.]ikwb[.]com
- secured-chase-verify-auth[.]shaddenenterprise[.]com
- ww3ecure-chase-verifyauth[.]dns04[.]com
- mychase-3ecure-verifyauth3[.]my03[.]com
- mail[.]verify12chasewebauth[.]dns04[.]com
- cpanel[.]verifychaseaccauth[.]sytes[.]net
- webdisk[.]chase-verify-auth[.]serveuser[.]com
- authverifysecure077b-chase[.]ikwb[.]com
- cpanel[.]cverifychase0b3auth[.]sytes[.]net
- webdisk[.]verifychaseaccauth[.]sytes[.]net
- ww3ecure-chase-verifyauth6[.]dns04[.]com
- ww3ecure-chase-verifyauth3[.]dns04[.]com
- mychase-3ecure-verifyauth2[.]my03[.]com
- mail[.]authverifychaseaccount[.]dns1[.]us
- webmail[.]verifychaseaccauth[.]sytes[.]net
- www[.]authverifychaseaccount[.]dns1[.]us
- www[.]host-verifymychase-auth6[.]dns04[.]com
- www[.]chase-secureverifyauth8[.]dns04[.]com
- cpanel[.]verify12chasewebauth[.]dns04[.]com
- www[.]chase-secureverifyauth0[.]dns05[.]com
- www[.]host-verifymychase-auth[.]dns04[.]com
- webdisk[.]cverifychase0b3auth[.]sytes[.]net
- mail[.]chase-secureverifyauth0[.]dns05[.]com
- www[.]chase-secureverifyauth7[.]dns05[.]com
- www[.]chase-secureverifyauth9[.]dns05[.]com
- www[.]chase-secureverifyauth4[.]dns05[.]com
- authverifysecure0555a-chase[.]ikwb[.]com
- www[.]chase-secureverifyauth1[.]dns05[.]com
- webmail[.]cverifychase0b3auth[.]sytes[.]net
- cpanel[.]verifying-auth-chase[.]itemdb[.]com
- securemychase-auth0bverify1[.]dns04[.]com
- www[.]host-verifymychase-auth5[.]my03[.]com
- mychase-verify3ecure-auth0b15[.]dns05[.]com

- mychase-verify3ecure-auth0b9[.]dns04[.]com
- webdisk[.]verify12chasewebauth[.]dns04[.]com
- www[.]chase-secureverifyauth12[.]dns05[.]com
- www[.]chase3ecure-verifyauth05[.]dns04[.]com
- www[.]chase3ecure-verifyauth02[.]dns04[.]com
- www[.]chase-secureverifyauth13[.]dns04[.]com
- mychase-verify3ecure-auth0b8[.]dns04[.]com
- www[.]chase3ecure-verifyauth03[.]dns04[.]com
- mychase-verify3ecure-auth0b1[.]dns05[.]com
- securemychase-auth0bverify11[.]dns05[.]com
- mail[.]host-verifymychase-auth[.]dns04[.]com