DNS Deep Diving into Pig Butchering Scams

Table of Contents

Executive Report

New kids on the cybercrime block, pig butchering scams, have been making waves lately, and it is not surprising why. Scammers have been earning tons from them by being able to trick users into investing in seemingly legitimate business ventures but losing their hard-earned cash instead.

Trend Micro recently published an in-depth analysis of pig butchering scams and named eight domains as indicators of compromise (IoCs) in the process. These domains supposedly belonged to investment brokers who were really scammers in disguise.

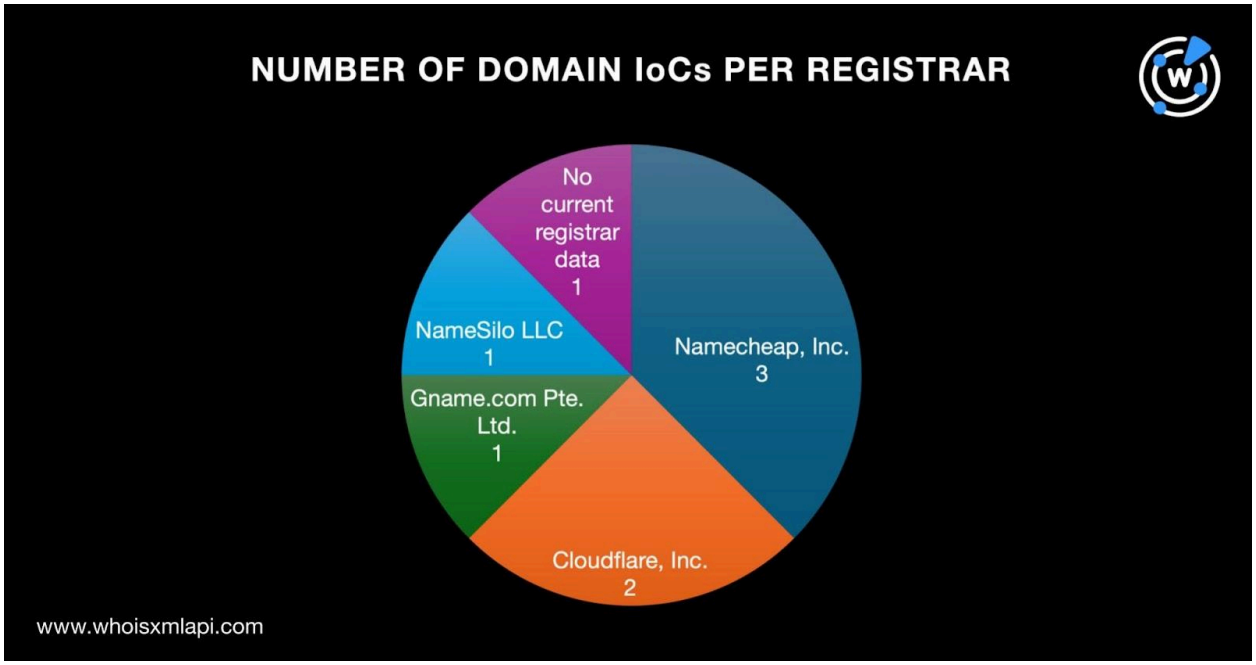
The WhoisXML API research team, in a bid to uncover other unknown threat vectors, expanded the list of pig butchering scam IoCs and found:

- 27 email-connected domains, one of which turned out to be malicious
- Two IP addresses
- 112 string-connected domains

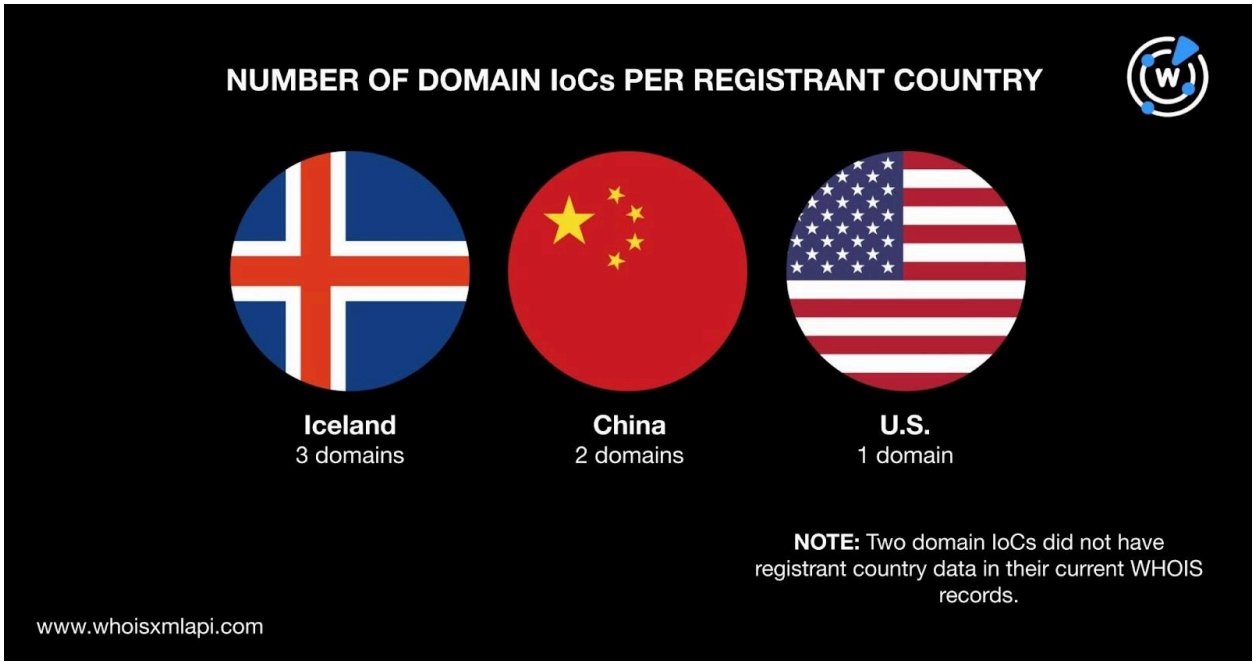
DNS Findings about the Pig Butchering Scam IoCs

As the usual first step in our analysis, we sought to find more information about the eight domains identified as IoCs. A bulk WHOIS lookup for them led to these findings:

- They were administered by four different registrars led by Namecheap, Inc., which accounted for three domain IoCs. Cloudflare, Inc. took the second spot with two domain IoCs. Gname.com Pte. Ltd. and NameSilo LLC accounted for one domain IoC each. One domain IoC did not have registrar data in its current WHOIS record.



- A majority of them, five to be exact, were created in 2023, while two were created in 2022. One domain IoC did not have registrant country information in its current WHOIS record.
- They were registered in three different countries led by Iceland, which accounted for three domain IoCs. Two domain IoCs were registered in China and one in the U.S. Two domain IoCs did not have registrant country data in their current WHOIS records.



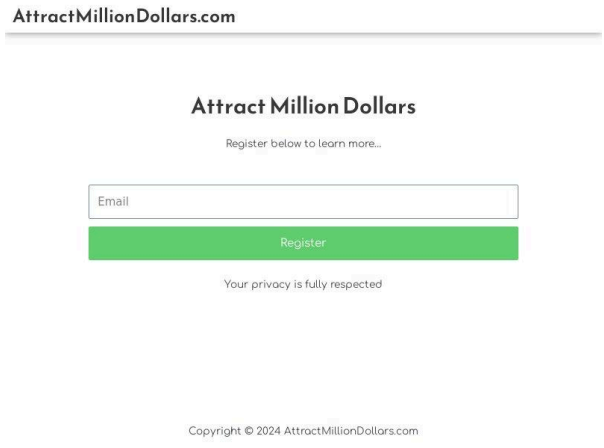
DNS Results from the Pig Butchering Scam IoC List Expansion

To uncover pig butchering scam digital breadcrumbs, we began our expansion analysis with WHOIS History API queries for the eight domains identified as IoCs. They allowed us to gather eight email addresses from the domain IoCs' historical WHOIS records. One of the email addresses was public.

A Reverse WHOIS API query for the public email address led to the discovery of 27 email-connected domains after duplicates and the IoCs were removed.

Threat Intelligence API queries for the email-connected domains showed that one—designalps[.]com—figured in a phishing campaign.

While designalps[.]com was no longer accessible, Screenshot API revealed that 21 of the email-connected domains continued to resolve to live pages. Twelve of them seemingly led to trading-related sites. Take a look at two examples below.



Screenshot of the page hosted on the email-connected domain attractmilliondollars[.]com

Screenshot of the page hosted on the email-connected domain automoneymakers[.]com

Next, we subjected the eight domains tagged as IoCs to DNS lookups and found that two resolved to one unique IP address each.

IP geolocation lookups for the two IP addresses—172[.]234[.]25[.]151 and 45[.]39[.]148[.]106 showed that:

- Both were geolocated in the U.S.

- They were administered by different ISPs—172[.]234[.]25[.]151 by Akamai Technologies, Inc. and 45[.]39[.]148[.]106 by EGIHosting.

Reverse IP lookups for the two IP addresses revealed that both were shared so we decided not to look for IP-connected domains as they would likely be false positives.

Next, we used Domains & Subdomains Discovery to look for other domains that contained text strings that appeared among the domain IoCs. We found 112 string-connected domains after duplicates, the IoCs, and the email-connected domains were filtered out. They all started with the following strings:

- **crmforexs**
- **cronosca**
- **trading-ic**

Forty-eight of the string-connected domains continued to lead to live sites even if more than half of them, 29 to be exact, were parked or led to error or blank pages.

Signs of Finance Site Abuse in the DNS

To succeed, pig butchering scams need to convince potential victims they are making legitimate investments. That is why scammers typically use domains with related text strings, such as **forex**, **coin**, and **trading**, akin to some of these domains identified as IoCs:

- crmforexs[.]com
- filecoinprotocol[.]com
- gcap-forex[.]net
- trading-ic[.]com

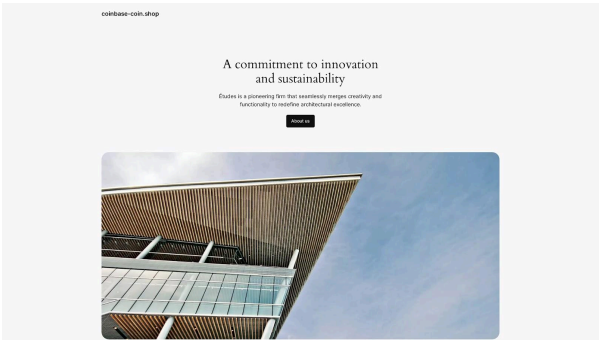
To cover all the bases, therefore, we scoured the DNS for other domains containing the three strings mentioned above that pig butchering scammers could weaponize in future attacks. We used the strings as Domains & Subdomains Discovery search terms and found 11,409 domains in total.

Threat Intelligence API revealed that 13 of the additional string-connected domains were associated with phishing and generic threats. Here are five examples.

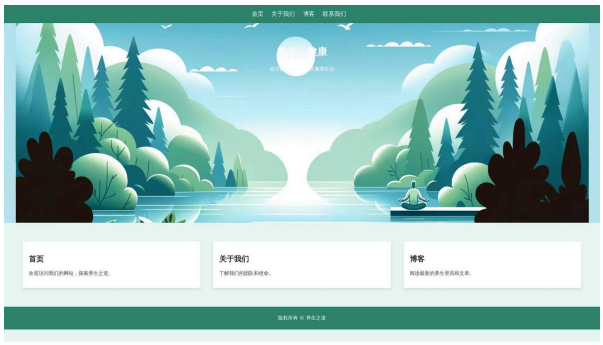
MALICIOUS ADDITIONAL STRING-CONNECTED DOMAIN	ASSOCIATED THREAT TYPE
coinbase-coin[.]shop	Phishing
coinwavepros[.]site	Generic

	Phishing
coinxiazai[.]com	Phishing
hychain[.]trading	Phishing
walletlink-coinbase[.]com	Phishing

Screenshot lookups showed that five of the malicious additional string-connected domains remained accessible—three of them led to blank, error, or under construction pages, while the remaining two led to live sites as shown below.



Screenshot of the page hosted on the malicious additional string-connected domain coinbase-coin[.]shop



Screenshot of the page hosted on the malicious additional string-connected domain coinxiazai[.]com

It is interesting to note that all of the malicious additional string-connected domains contained the text string **coin**. That could be due to the popularity of investing in cryptocurrency at the moment.

—

Our DNS deep dive into pig butchering scams led to the discovery of 141 connected threat artifacts, one of which turned out to be malicious. It also revealed the presence of a number of finance-, cryptocurrency-, and trading-related domains that already figured in or could be weaponized in the future for phishing campaigns, possibly even pig butchering scams.

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 Email-Connected Domains

- artsmyx[.]com
- attractmilliondollars[.]com
- attractmillionsofdollars[.]com
- automoneymakers[.]com
- automoneyprinter[.]com
- binaryoptionsprotocol[.]com
- bitcoinalp[.]com
- bitcoinalps[.]com
- bitcoinapproach[.]com
- brlusd[.]com
- designalp[.]com
- designalps[.]com
- digitalmarketingprotocol[.]com
- filecoinr[.]com
- forexprotocol[.]com
- fourpercent[.]us
- idat[.]us
- mercadocapitales[.]com
- moneyalp[.]com
- moneyalps[.]com

Sample String-Connected Domains

- crmforexsolution[.]com
- crmforexsolutions[.]com
- cronoscadservices[.]com
- cronoscadservices[.]ro
- cronoscadsystems[.]com
- cronoscafe[.]ca
- cronoscafe[.]com
- cronoscal[.]com
- cronoscala[.]com
- cronoscalata[.]com
- cronoscalata[.]it
- cronoscalatacataniaetna[.]com
- cronoscalatacataniaetna[.]it
- cronoscalatacavallo[.]it
- cronoscalatacdf[.]it
- cronoscalatacravetto[.]com
- cronoscalatagiarremilo[.]com
- cronoscalatamariobuti[.]it
- cronoscalatamontecaina[.]it
- cronoscalatamonterice[.]com
- cronoscalatamonterice[.]it
- cronoscalatanevegal[.]com
- cronoscalatanevegal[.]it
- cronoscalatavalledimaddaloni[.]it
- cronoscalate[.]bike
- cronoscalate[.]com
- cronoscalate[.]it
- cronoscalate[.]net
- cronoscalate[.]tv
- cronoscalatemondiali[.]it
- cronoscalatestoriche[.]it
- cronoscalatesud[.]it
- cronoscale[.]io
- cronoscalefaccion[.]com
- cronoscalefaccion[.]com[.]ar
- cronoscalendar[.]com
- cronoscalendar[.]xyz
- cronoscalibracao[.]com[.]br

- cronoscaltd[.]com
- cronoscam[.]com
- cronoscambio[.]com
- cronoscamera[.]com
- cronoscampingsociety[.]com
- cronoscampsociety[.]com
- cronoscampus[.]eu
- cronoscan[.]com
- cronoscan[.]de
- cronoscan[.]dev
- cronoscan[.]io
- cronoscan[.]net

Sample Additional String-Connected Domains

- 0bitcoin[.]cc
- 0coinrobot[.]com
- 0to10trading[.]com
- 0xbitcoin[.]vip
- 1000satscoin[.]com
- 1000spinlinkcoinmaster[.]com
- 1001tradingcommunity[.]com
- 100bitcoiners[.]com
- 100trillioncoin[.]com
- 10safe-trading[.]online
- 11bet[.]forex
- 12985-coinbase[.]com
- 12storeez[.]trading
- 12stories[.]trading
- 13267-coinbase[.]com
- 1485254-coinbase[.]com
- 151234-coinbase[.]com
- 151sydneystreettradinglimited[.]com
- 168985-coinbase[.]com
- 17334522-coinbase[.]com
- 17912-coinbase[.]com
- 1794832-coinbase[.]com
- 17958-coinbase[.]com
- 1800bitcoin[.]ca
- 18276-coinbase[.]com
- 18290185-coinbase[.]com
- 182967-coinbase[.]com
- 1875290-coinbase[.]com
- 18902-coinbase[.]com
- 18forevertrading[.]com
- 1978521-coinbase[.]com
- 1978544-coinbase[.]com
- 1978569-coinbase[.]com
- 199xtrading[.]com
- 19tradinghk[.]com
- 1coin[.]kim
- 1coins[.]com[.]cn
- 1eurocoin[.]nl
- 1eurocoin[.]online
- 1eurocoin[.]store
- 1longcoin[.]com
- 1milliondollarcoin[.]nl
- 1milliondollarcoin[.]online
- 1milliondollarcoin[.]store
- 1milperbitcoin[.]com
- 1stlosstrading[.]com
- 1targettrading[.]com
- 1toncoin[.]com
- 2024coin[.]sbs
- 2024coin2[.]us
- 2030coin[.]site
- 21bitcoin[.]dk
- 21bitcoin[.]es
- 21coin[.]fun
- 21million-bitcoin[.]com
- 21millionbitcoins[.]com[.]au
- 21sisaltrading[.]co[.]tz
- 21stbitcoin[.]com
- 24315347-coinbase[.]com
- 24315350-coinbase[.]com
- 24315679-coinbase[.]com
- 247-global-trading[.]com

- 24bitcoinetf[.]com
- 24bitcoinetfs[.]com
- 24coinpay[.]com
- 2auth-coin-base[.]com
- 2coins[.]top
- 2fa-coin-b-ase[.]com
- 2fas-coinbase[.]com
- 2ndavetrading[.]com
- 2sides2everycoin[.]com
- 2tmcoin[.]com
- 2trading[.]online
- 2u[.]trading
- 30daysofbitcoin[.]com
- 32bitcoins[.]com
- 32bitcoins[.]com[.]au
- 360coinvestpro[.]com
- 360copytrading[.]com
- 365-coincenter[.]com
- 365global-trading[.]com
- 388bet[.]forex
- 388bet[.]trading
- 3kcoinst1ktok[.]ru
- 3kgeneraltrading[.]com
- 420bitcoin[.]com[.]au
- 420bitcoinparty[.]com[.]au
- 438291-coinbase[.]com
- 47630647-coinbase[.]com
- 4bitcoin[.]ai
- 4bitcoin[.]io
- 4coin[.]com[.]cn
- 4coins[.]com[.]cn
- 4coins[.]vip
- 4kcoin[.]online
- 50pagebitcoin[.]com
- 518tradingcards[.]com
- 52coin[.]cc
- 548926-coinbase[.]com
- 5btrading[.]co
- 5coins[.]com[.]cn
- 5duniversetrading[.]com
- 5ftrading[.]com
- 6coins[.]com[.]cn
- 6coins[.]shop
- 70food-tourcoing[.]fr
- 789[.]forex
- 78sixtrading[.]com
- 7coins[.]com[.]cn
- 7seas[.]trading
- 7seastradings[.]com
- 7x-trading[.]com
- 8490coinbase[.]com
- 867483-coinbase[.]com
- 87312-coinbase[.]com
- 88bet[.]trading
- 890170-coinbase[.]com
- 8910-coinbase[.]com
- 8live[.]forex
- 8live[.]trading
- 8rtpcoinmaster[.]xyz
- 9-5trading[.]info
- 9-5trading[.]online
- 916jsgoldcoins[.]in
- 9246-coinbase[.]com
- 948122061-coinbase[.]com
- 999forex[.]mom
- 99coin[.]com[.]cn
- 99coins[.]com[.]cn
- 9coins[.]com[.]br
- 9coinsmedia[.]com
- a-forex[.]top
- a-gtrading[.]biz
- a-trading[.]me
- a-vipcoin[.]com
- a1trading[.]io
- a5generaltrading[.]com
- a5tradings[.]com
- aaaabbbbccccsonounhostfakedolomitienergiatrading-it[.]xn--node
- aaaabbbbccccsonounhostfakedolomitienergiatrading[.]org[.]ph

- aaaabbbbccccsonounhostfakedolomitienergiatrading[.]xn--fiqz9s
- aaaabbbbccccsonounhostfakedolomititrading-it[.]xn--fiqs8s
- aaaabbbbccccsonounhostfakedolomititrading-it[.]xn--mxtq1m
- aaatradingsllc[.]com
- aafxcrypttrading[.]com
- aakgeneraltrading[.]com
- aasthatradinginstitute[.]com
- abacoinnovazione[.]it
- abacoint[.]online
- abargeneraltrading[.]store
- abashiri-trading[.]com
- abcbitcoin[.]au
- abctradingcorporation[.]org
- abd-trading[.]online
- abdtrading[.]biz
- abeliancoin[.]net[.]ws
- abitscoin[.]com
- abnsolutecoinpay[.]com
- aboalrehitrading[.]com
- aboutbitcoin[.]eu
- abrahammckaytrading[.]me
- abuahmedalyarabitrading[.]com
- academia-bitcoin[.]ro
- acceptbitcoinpayment[.]au
- acceptingbitcoin[.]au
- accesstrading[.]in
- accinternationaltradinghk[.]com
- accoingenieria[.]com
- account-coinsbase[.]com
- accountingforbitcoin[.]ca
- accountlogin-coinbase[.]com
- acebitcoin[.]io
- acehotbitcoin[.]com
- acholdingcoinc[.]com
- acidohialuronicoinno[.]com
- acme-coin[.]io
- acmecoins[.]co
- acoin[.]gdn
- acoincheck[.]net
- acoindex[.]net
- across[.]trading
- activetradingbtc[.]com
- acwatchtradingllc[.]com
- adamacoine[.]com
- adaytradingcrypto[.]com
- addcoin[.]site
- addresnames4coins[.]com
- adforexad[.]com
- adiltradingllc[.]com
- adoniscoin[.]xyz
- adoptbitcoin[.]co[.]za
- adoptmetradingserver[.]com
- adrihatrading[.]com
- adtradingcards[.]uk
- advancedeatradingplatform[.]com
- advancedtradingai[.]com
- advisor-coinbase[.]com
- aefetrading[.]com
- aeforex[.]org
- aerocoin[.]shop
- aescoinstruments[.]com
- aetgeneraltrading[.]net
- aezatrading[.]com
- aezatrading[.]ru
- afbcoin[.]vip
- affair-coinbase[.]com
- affcotrading[.]com[.]au
- affiliatekucoin[.]com
- affiliatekucoin[.]store
- affordablecoinpr[.]com
- affordablecoinsandcurrency[.]com
- afoscoinvestmentlimited[.]com[.]ng
- africadeblocktrading[.]com
- africaforexsuccesssummit[.]com
- africatradinginternational[.]com
- africsaveur-trading[.]com
- aftontradingou[.]com

- agab-trading-limited[.]com
- agenciacoinspire[.]com[.]br
- agentbitcoin[.]ai
- agi[.]forex
- agicoin[.]ai
- agix-coin[.]com
- agreen-trading[.]eu
- agrilinktrading[.]com
- agritradinghub[.]com
- agrolife-trading[.]com
- agrotrading[.]sk
- ahafxtrading[.]com
- ahlsntrading[.]com
- ahms-forexports[.]com
- ahoptrading[.]com
- ai-bitcoin[.]com[.]au
- ai4xtrading[.]com
- aiagent[.]trading
- aialtcoin[.]nl
- aialtcoin[.]online
- aiapitrading[.]com[.]ng
- aiareh-trading[.]ir
- aibitcoin[.]ca
- aibitcoin[.]gold
- aibitcoin[.]io
- aibitcoincerts[.]ai
- aibitcoincerts[.]co
- aibitcoinetfs[.]com
- aibitcoininsights[.]com
- aibitcoinsignals[.]com
- aibitcointracker[.]com
- aibitecoin[.]com
- aibittradebitcoin[.]com
- aibtsttrading[.]com
- aibtsttrading[.]in
- aibytecoin[.]com
- aicatcoin[.]com
- aicoin[.]cyou
- aicoin[.]fit
- aicoinada[.]com
- aicoinbank[.]us
- aicoincn[.]co
- aicoinn[.]com
- aicoinnovate[.]com
- aicoinsandcurrency[.]com
- aicoinsbank[.]com
- aicoinscurrency[.]com
- aicoinvestor[.]com
- aicoinw[.]com
- aicryptotrading[.]top
- aicryptotrading24[.]com
- aicryptotradingpro[.]com
- aidottrading[.]com
- aidracoin[.]com
- aidragonitecoin[.]com
- aidrivenforexpicks[.]com
- aienabledbitcoin[.]ie
- aiforexanalysis[.]com
- aiforexinsights[.]com
- aiforexpriceaction[.]com
- aiforextracker[.]com
- aiforextrend[.]com
- aiforexwealthhub[.]com
- aiguotrading[.]com
- aiketradingcolimited[.]com
- aiqforex[.]com
- air-bonkcoin[.]com
- air-metacoin[.]com
- airbiz-circlecoins[.]com
- airbnbcoin[.]es
- airbnbitcoin[.]net
- airciticoin[.]com
- aircoinciti[.]com
- aircoinmemeland[.]xyz
- airdrop-apecoin-tc-8857640[.]com
- airdropcoinglobe[.]gives
- airdropcoinglobe[.]solutions
- airdropdexcoin[.]com
- airextrading[.]com[.]pk
- airline-tradingcards[.]com

- airline-tradingcards[.]ph
- airmemecoinland[.]com
- airmetacoin[.]com
- airmetacoin[.]org
- airobotrading[.]it
- airworld-metacoin[.]com
- aistablecoins[.]com
- aitimtrading[.]com
- aitradingaustralia[.]com
- aitradingdaily[.]com
- aitradingindex[.]com
- aitradingsignal[.]shop
- aiyingtrading[.]com
- ajolotecoin[.]com
- ajtrading[.]store
- ajtradings[.]in
- akaratradingllc[.]com
- akibacoin[.]jp
- akihabaracoin[.]jp
- akiitrading[.]com
- akillicoin[.]com[.]tr
- akinternationaltrading[.]co[.]in
- akirainternationalshipsupplytrading[.]com
- akitacoin[.]live
- akitcoin[.]com
- akrracoin[.]com
- aktifbitcoin[.]com[.]tr
- al-thurayageneraltradingandexport[.]com
- al-trading[.]co[.]uk
- alabeertradingllc[.]com
- aladeeb-trading[.]com
- alaintrading[.]fr
- alajzabtrading[.]net
- alanestrading[.]com
- alarhamtrading[.]site
- alarhamtrading[.]store
- alayyantrading[.]ae
- alayyattrading[.]com
- albertsonscoinc[.]org
- albiladtrading[.]com
- alcoin[.]me
- alcoin[.]us
- alcoinvestments[.]ca
- alemaratforex[.]com
- alertstradingview[.]com[.]ws
- alfa-bitcoin[.]eu
- alfacoin[.]app
- alfanartrading[.]site
- alfatrading[.]finance
- algebra[.]trading
- alghaithtrading[.]ae
- algobullstradingsolutions[.]com
- algorithmtradingfx[.]com
- algos[.]trading
- algotrading[.]au
- algotradingbattles[.]online
- alhabaritrading[.]com
- alhanatrading[.]uk
- alicoins2024[.]com
- alifunicoindia[.]com
- alitashtradingcompany[.]com
- alitrading[.]jp
- alitradingltd[.]com
- aliudtrading[.]eu
- alkatheerytradingestablishment[.]com
- alkestrading[.]com
- alkonadventurestrading[.]ae
- alkuwaitforex[.]com
- all-in-coins[.]com
- allaboutbitcoin[.]io
- allahabadforex[.]in
- allbluetrading[.]com
- allcardtrading[.]com
- allforexblog[.]com
- alliance-coinbase[.]com
- allianceforexit[.]com
- alliektrading[.]com

- allmemecoin[.]xyz
- allocation-bitcoincats[.]world
- allocation-jup[.]trading
- allscrapmetals[.]trading
- allsettrading[.]com
- alltradingcourses[.]com
- alltradingltd-tc-8457471[.]com
- almanarahgeneraltrading[.]com
- almatrading[.]de
- almatrading[.]gmbh
- almazrouitrading[.]com
- almeidajohnsontrading[.]com
- almosli-trading[.]com
- almuhaidebtrading[.]ae
- alnajahatrading[.]com
- alnajmgarmentstrading[.]store
- alocoins[.]ph
- aloktrading[.]co[.]in
- alpa96cartrading[.]com
- alpandagamestrading[.]com
- alphadragonstarcoin[.]com
- alphafundstrading[.]ltd
- alphardtrading[.]com
- alphasmarttrading[.]com
- alphatradingiq[.]com
- alphatradingservice[.]com
- alphatradinguk[.]com
- alphatrendtradingview[.]com
- alphintrading[.]online
- alpinclubtrading[.]com[.]br
- alpsglobaltrading[.]com
- alpynetrading[.]com
- alqatryt-trading[.]com
- alqudstrading[.]com[.]pk
- alsalwatrading[.]com
- alsaqrtrading[.]online
- alshaimafueltrading[.]com
- alshateyfoodsupplementstrading[.]com
- alsintradingpost[.]com
- alsirattrading[.]com
- alsirattrading[.]online
- altadefinizione[.]forex
- altalb-trading-contracting[.]com[.]sy
- altcoinape[.]io
- altcoincomrade[.]xyz
- altcoincryptocasinos[.]com
- altcoinelixir[.]com
- altcoinelixirs[.]com
- altcoinetf[.]org
- altcoinetf[.]xyz
- altcoinetps[.]com
- altcoinfund[.]shop
- altcoingape[.]com
- altcoins[.]cam
- altcoinselixir[.]com
- altcoinselixirs[.]com
- altcoinsera[.]com
- altcoinsetfs[.]com
- altcoinsevolution[.]com
- altcoinsfreedom[.]com
- altcoinsrevolution[.]com
- altcoinsuperapp[.]com
- altcoinswap[.]io
- altcointradeandexchange[.]ca
- altcointradingcenter[.]com
- altcointrusts[.]com
- altercoinspad[.]top
- alteregocoin[.]com
- altlayercoin[.]com
- altrading[.]ee
- alvarestrading[.]com
- alwasadtrading[.]com
- alwaysliveforexperiences[.]com
- alwoodtrading[.]ae
- alyaseentrading[.]com
- amaforexports[.]com
- amaforexports[.]online
- amayatrading[.]net
- ambassadebitcoin[.]ca

- ambattrading[.]com
- ambiente-trading[.]com
- ambition-trading[.]com
- amccoinex[.]com
- amcoins[.]co
- americanbitcoin[.]co
- americanbitcoinexperiment[.]com
- americancoinadvisor[.]com
- americancoins[.]shop
- americancoins24[.]shop
- amgcoin[.]lt
- amgforexbroker[.]com
- amhgoldtrading[.]com
- amintltrading[.]com
- amjctrading[.]com
- amk1grouptrading[.]com
- amrtradings[.]com
- amstrading[.]online
- amtradingclub[.]co
- amustartrading[.]com
- anacoin[.]co
- anacoin[.]tech
- analoscoin[.]com
- analyticoinnovatesphere[.]com
- anantatrading[.]fr
- anantcoin[.]io
- anayratradingandcontracting[.]com
- ancientandrarecoins[.]com
- ancienthistoriccoins[.]co[.]uk
- ancienthistoriccoins[.]com
- andrestradingmarkets[.]online
- anfertradingsolutions[.]com
- anft[.]trading
- anfttrading[.]com
- angelofbitcoin[.]com
- angelsonlinetrading[.]com
- angelspeedtrading[.]com
- angrycoin[.]online
- anikemtrading[.]co[.]ke
- aninternationaltrading[.]com
- anisazglobaltrading[.]com
- anisaztrading[.]com
- anitamaxwynn[.]trading
- anmoltradingco[.]com
- anocoinmarket[.]com
- anonymousttrading[.]io