Cardano Joins the List of Favored Crypto Scam Targets

Table of Contents

Executive Report

Twitter was recently abuzz with news regarding an ongoing Cardano scam via a downloadable phishing app. Posing as a giveaway promo, which is how cybercriminals have frequently been victimzing cryptocurrency owners these days, users who get tricked into downloading the rogue app end up with stolen credentials instead.

We began our investigation into the threat with two indicators of compromise (IoCs) disclosed in a tweet—the malicious domain name airdrop-ada[.]net and the malicious IP address 104[.]21[.]78[.]87. Using these as jump-off points, our deep dive revealed:

- 29 possibly connected domains containing the string combination “airdrop + ada,” akin to the IoC
- 2 possibly connected subdomains containing the string combination “airdrop + ada”
- 300+ connected domains as they shared an IP host of the domain IoC
- 2 of the possibly connected domains and subdomains are malicious
- 1,100+ domains and subdomains containing the string “cardano,” 12 of which are already dubbed “malicious”

Looking for Possible Connections to the IoCs

In our effort to look for other artifacts, we subjected the domain airdrop-ada[.]net to a DNS lookup and found two additional IP addresses, apart from the one identified in the tweet—213[.]226[.]124[.]209 and 172[.]67[.]219[.]16.

We then looked for other potential connections using the string combination “airdrop + ada” on Domains & Subdomains Discovery. The query uncovered 29 possibly connected domains, such as:

- airdrop-diadata[.]org
- adapad-airdrop[.]tech
- trustpadairdrop[.]com
- airdrop-crabada[.]com
- etherpadairdrop[.]org

Using the same string combination, we also discovered two possibly connected subdomains, namely:

- ada-airdrop[.]hwlegnano[.]it
- legit-airdrop-radar[.]myshopify[.]com

Next, we used the IP addresses 213[.]226[.]124[.]209, 172[.]67[.]219[.]16, and 104[.]21[.]78[.]87 as reverse IP lookup search terms and found at least 300 domains that shared 104[.]21[.]78[.]87 as host. Examples include:

- assets[.]ovh
- assumption[.]site
- atdominican[.]com
- atheniamarketing[.]com
- auto-payingsu[.]com

The high number of connected domains and the second-level domain (SLD) string dissimilarity indicate the likely use of shared hosting infrastructure. In addition, a bulk WHOIS lookup for the possibly connected domains showed that only 42 of the 301 possibly connected domains (14%) shared the domain IoC's registrant country, reinforcing our earlier interpretation of the use of a shared hosting infrastructure.

Nevertheless, we subjected all the web properties we found to a bulk malware check on the Threat Intelligence Platform and discovered that two of them—dejob[.]xyz and dispenseoneglint[.]cyou—are considered malicious by various malware engines.

Expanding the Investigation

Cardano has been consistently part of the top 10 cryptocurrencies to invest in and that remains true this year. It's not surprising, therefore, for it to be a favored cybercrime target. We looked

into web properties containing Cardano and the names of other cryptocurrencies, in fact, around the same time last year and found around 30,000 potential threat vehicles.

We sought to discover if new domains and subdomains were registered just this year and found:

- 710 domains registered between 1 January and 18 May 2022 containing the string "cardano," six of which have already been dubbed "malicious" by various malware engines
- 630 subdomains registered on 1January–18 May 2022 containing the string "cardano," five of which turned out to be malicious

Note the growth in web property volume from 677 to more than double at 1,340 domains and subdomains in a span of less than a year. That not only denotes growth in the number of Cardano coin owners but likely also the threats that could target them.

—

All Cardano cryptocurrency owners should heed the call to avoid accessing the domains, subdomains, and IP addresses, especially those deemed "malicious," if they want to avoid the risk of getting scammed or phished. Monitoring the possibly connected domains, particularly those registered in the U.S. and shared other WHOIS details with the domain IoC may also be worth doing.

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 Artifacts and IoCs

Possibly Connected Domains

Contained the String Combination "airdrop + ada"

- airdropada[.]com
- leadairdrop[.]com
- airdrop-ada[.]com
- ada-airdrop[.]com
- ada-airdrop[.]org
- airdropradar[.]de
- airdropradar[.]be
- airdrop-ada[.]net
- airdrop-radar[.]de
- airdrop-radar[.]ru

- airdropradar[.]com
- airdrop-ada[.]live
- ada-airdrop[.]live
- bradairdrops[.]com
- airdropradar[.]net
- airdropburada[.]com
- airdropsradar[.]com
- airdropforada[.]com
- airdropsforada[.]com
- bscpadairdrop[.]tech

Shared the Same IP Host as the Domain IoC

- 0850yetkiliservis[.]com
- 1021d[.]com
- 128bayi[.]com
- 143tycvip[.]com
- 15caoff[.]com
- 30slottica[.]com
- 3501rubindrive[.]com
- 365365k[.]com
- 3darcszobraszat[.]hu
- 4bentcoffee[.]com
- 5ddirectory[.]com
- 884ku[.]com
- 999999[.]wiki
- abasilspasetra[.]tk
- abuhammad-news[.]com
- acalathomcoli[.]ga
- acegac[.]cf
- acnisuri[.]tk
- acnithinneunorty[.]cf
- adfuzingment[.]ga
- adgjl-bp34[.]com
- adinpesoces[.]tk
- afelet[.]ga
- afficofsi[.]cf
- agenciaadvogadoweb[.]com[.]br
- agzy6[.]com
- aheadfurniture[.]com
- ahorronation[.]com
- ahsunyata[.]com
- aiconferences[.]co
- alalgesraluca[.]gq
- albarzonline[.]com
- altair-tours[.]ru
- amextade[.]tk
- amexwayusdt[.]com
- amrrorlecor[.]tk
- andrewveenstra[.]com
- annemettewinther[.]dk
- anonicob[.]tk
- antalyalisesi[.]com
- apkfirefree[.]com
- apkuj5[.]gq
- app10wg[.]space
- appleridgecountryclub[.]com
- archesgui[.]ml
- arcilsocoja[.]tk
- areredultren[.]cf
- arferbirthro[.]gq
- artellux-m[.]website
- artesaniasiquitos[.]com

Contained the String “cardano” Registered on 1 January–18 May 2022

- cardano[.]ng
- cardano[.]ee
- cardano[.]hk
- cardanos[.]de
- cardanos[.]nl
- 2cardano[.]ph

- cardanow[.]io
- 4cardano[.]ws
- cardano[.]day
- 2cardano[.]net
- cardanobi[.]io
- cardano22[.]us
- cardanoh[.]com
- cardano[.]bond
- cardanoq[.]com
- cardano[.]gmbh
- cardano[.]toys
- cardano22[.]io
- 2cardano[.]com
- cardano22[.]ws
- cardano[.]surf
- cardanobet[.]co
- cardanonft[.]ch
- x2cardano[.]org
- buycardano[.]de
- cardanodb[.]com
- cardano2x[.]org
- cardanoo[.]live
- bancardano[.]ws
- cardanoise[.]io
- cardano2x[.]net
- cardanons[.]org
- cardanovs[.]com
- cardanoabu[.]ws
- cardanoada[.]eu
- wecardano[.]com
- tucardano[.]com
- cardanore[.]com
- 22cardano[.]com
- cardanopy[.]net
- cardanotk[.]com
- cardano-de[.]fi
- cardanonft[.]nl
- buycardano[.]us
- cardanoano[.]eu
- cardano[.]study
- cardanola[.]com
- 2xcardano[.]com
- wcardano[.]site
- mvcardano[.]com
- cardanopro[.]io
- cardano888[.]ws
- 22cardano[.]org
- 2xcardano[.]net
- nftcardano[.]co
- cardanoano[.]it
- cardanonft[.]co
- x2cardano[.]net
- cardanogoat[.]io
- cardanogear[.]ws
- cardanodino[.]nl
- cardano-x2[.]org
- cardanowolf[.]io
- frecardano[.]com
- cardanohtx[.]com
- cardanogov[.]org
- cardanolive[.]ws
- cardanoan[.]site
- cardano-2x[.]com
- campcardano[.]ph
- x2-cardano[.]com
- cardano-2x[.]org
- gigacardano[.]nl
- cardano2021[.]io
- cardanolife[.]io
- cardanobees[.]io
- ab-cardano[.]com
- cardanocash[.]ws
- newcardano[.]com
- cardanox2[.]gift
- cardanovids[.]ws
- x2-cardano[.]net
- cardanomass[.]ai
- cardanotext[.]ws
- boxcardano[.]com
- cardanonut[.]com
- cardanopia[.]com
- cardanosada[.]ws
- cardanomart[.]co
- cardano247[.]com

- cardanocard[.]io
- cardanonews[.]io
- cardanofud[.]com
- cardano-x2[.]net
- govcardano[.]com
- cardanobank[.]ca
- cardanobsd[.]org
- cardano-x2[.]com
- 2x-cardano[.]net
- ada-cardano[.]us

Malicious Domains Containing the String “cardano”

- onecardano[.]org
- beincardano[.]com
- 2022-cardano[.]com
- cardanosupport[.]xyz
- cardano-reward[.]com
- cardanovaccines[.]com

Possibly Connected Subdomains

Subdomains Containing the String “cardano” Registered on 1 January–18 May 2022

- www[.]cardanocardano[.]philadelphiaairfare[.]com
- cardano[.]subnote[.]io
- cardano[.]simplisafe[.]com
- cardano[.]vivendo[.]digital
- cardano[.]spb[.]ru
- cardano[.]mhmm[.]io
- cardano[.]soslanx[.]com
- cardano[.]fastmenu[.]ro
- cardano[.]tooling[.]foundation
- cardano[.]compucampus[.]de
- cardano[.]exodus-stage[.]io
- cardano[.]creativedock[.]cloud
- cardano[.]tokenprinters[.]online
- cardano[.]cuongdesign[.]net
- cardano[.]millabs[.]net
- cardano[.]roblyall[.]co[.]uk
- cardano[.]cppay[.]io
- cardano[.]pierrechavez[.]com
- cardano[.]i8coin[.]com
- cardano[.]faucetlig[.]xyz
- cardano[.]glowstake[.]com
- cardano[.]unimi[.]it
- cardano[.]1955digital[.]com
- cardano[.]masonjon[.]es
- cardano[.]carbonweight[.]com
- cardano[.]visuality[.]ge
- cardano[.]markevans[.]work
- cardano[.]coursecleared[.]com
- cardano[.]dreamwave[.]live
- cardano[.]p2p[.]org
- cardano[.]autonio[.]io
- cardano[.]fuixlabs[.]com
- cardano[.]ironstaking[.]space
- cardano[.]decision01[.]cn
- cardano[.]xbglowx[.]com
- cardano[.]pool[.]ovh
- cardano[.]kaz[.]codes
- cardano[.]veo[.]link
- cardano[.]in-aschaffenburg[.]com
- cardano[.]us[.]org
- cardano[.]limas[.]xyz
- cardano[.]liveappsaccess[.]com
- cardano[.]masterupcrypto[.]com
- cardano[.]zendesk[.]com
- cardano[.]fundstrat[.]com
- cardano[.]blackbureau[.]net
- cardano[.]gravn[.]app
- cardano1[.]prodigynet[.]ca
- cardanom[.]kooriwebdesign[.]com

- pycardano[.]readthedocs[.]io
- cardanohl[.]spb[.]ru
- cardano-c[.]cryptomanufaktur[.]net
- cardanobox[.]bakon[.]dev
- cardanomdp[.]github[.]io
- en[.]cardano[.]fixedapps[.]org
- cardanodex[.]micro[.]blog
- en[.]cardano[.]dappsfixed[.]com
- cardanoico[.]biz[.]at
- en[.]cardano[.]liveappsaccess[.]com
- cardanoids[.]biz[.]at
- cardanoptc[.]faucetlig[.]xyz
- adacardano[.]magento2[.]cl
- cardanoorg[.]biz[.]at
- nc-cardano[.]linkriver[.]io
- minecardano[.]biz[.]at
- cardanoiran[.]xn--55qx5d[.]cn
- www[.]cardano[.]mzeetech[.]com
- noticardano[.]linkpc[.]net
- cardano-api[.]visuality[.]ge
- cardanobits[.]github[.]io
- cardanoburn[.]adaburn[.]com
- alancardano[.]xn--55qx5d[.]cn
- cardanohead[.]biz[.]at
- cardanogame[.]promo-miner[.]com
- www[.]cardano[.]connxusdemo[.]com
- www[.]cardano[.]faucetlig[.]xyz
- givecardano[.]biz[.]at
- cardanowood[.]biz[.]at
- lendcardano[.]biz[.]at
- coincardano[.]spb[.]ru
- cardano[.]dev[.]bergmann[.]consulting
- cardano-lab[.]biz[.]at
- www[.]cardano[.]bithub[.]sbs
- cardanothor[.]tradingtent[.]io
- cardanolink[.]altervista[.]org
- cardanofauc[.]promo-miner[.]com
- www[.]cardano[.]markevans[.]work
- cardanodiks[.]buynfts[.]net
- cardanolids[.]biz[.]at
- cardanoboys[.]xn--55qx5d[.]cn
- nc-cardano2[.]linkriver[.]io
- api[.]cardano[.]scantrust[.]io
- cardanonews[.]yivesites[.]com
- cardanom[.]io[.]kooriwebdesign[.]com
- cardanoswap[.]biz[.]at
- cardanosent[.]xn--55qx5d[.]cn
- www[.]cardano[.]carbonweight[.]com
- cardano-app[.]epizy[.]com
- cardanoiran[.]biz[.]at
- cardanocopia[.]derekrankins[.]com

Malicious Subdomains Containing the String “cardano”

- cardano[.]liveappsaccess[.]com
- en[.]cardano[.]fixedapps[.]org
- en[.]cardano[.]liveappsaccess[.]com
- cardanorewards[.]rf[.]gd
- www[.]cardanorewards[.]rf[.]gd