Looking for Traces of Social Media-Based Celebrity Scams in the DNS

Table of Contents

Executive Report

Infoblox, in its Q4 2022 Cyber Threat Report, featured a “Meta” coin scam using fake celebrity endorsements targeting users in the European Union (EU). The analysis revealed several indicators of compromise (IoCs), specifically four domains and one IP address, that could help the public avoid the perils the scams posed. The IoCs identified in the report were:

- 365coinmode[.]com
- 365graphiccoin[.]com
- spartan-trade[.]com
- networkfsi[.]com
- 45[.]63[.]119[.]177

In keeping with WhoisXML API’s mission to make the Internet a transparent and safe place for users, we expanded the list of IoCs in hopes of identifying social media pages that could already be serving or used to serve as fraud vehicles. Our analysis led to the discovery of:

- Three additional IP addresses that played host to the domains identified as IoCs
- 830 domains that shared the IoCs’ IP hosts, 26 of which turned out to be malicious
- 1,657 domains that contained the same strings as those tagged as IoCs, one of which was dubbed a malware host
- 529 Facebook and LinkedIn pages that made their way into the DNS from 1 January 2023 onward, 13 of which were found to be malicious

Expanding the Current List of IoCs

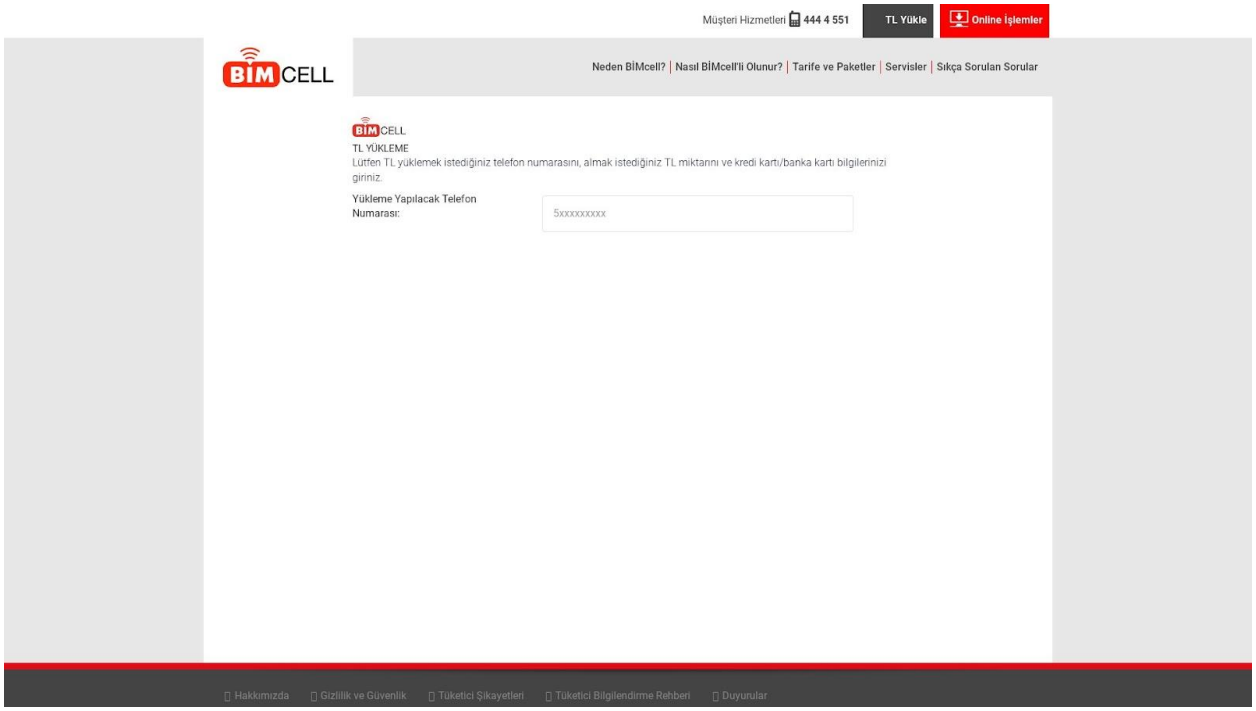
We began our analysis with WHOIS lookups for the domains identified as IoCs that allowed us to draw some similarities among them, namely:

- All four domains were created in 2022 and could thus be considered newly registered when they were used in malicious campaigns.

- Three of the domains—365coinmode[.]com, 365graphiccoin[.]com, and networkfsi[.]com—were registered in Iceland with Namecheap, Inc.
- Two of the domains—365coinmode[.]com and 365graphiccoin[.]com—shared the same IP host—45[.]63[.]119[.]177, which Infoblox also identified as an IoC.

Next, DNS lookups for the four domains provided an additional three IP addresses, bringing the total number of IP hosts to four. We used these as reverse IP lookup search terms, which indicated that three were shared while 45[.]63[.]119[.]177 in the original IoC list was dedicated. Our search uncovered 830 additional domains that shared the IoCs' IP hosts. Of these, 26 turned out to be malware hosts based on a bulk malware check.

Screenshot lookups for the malicious sites revealed that only one—bnzzl[.]net—continued to host live content that looks like a mobile phone directory.



Screenshot of bnzzl[.]net

It was also interesting to note that 11 of the malicious IP-connected domains bore a striking resemblance to two domains tagged as IoCs. Like 365coinmode[.]com and 365graphiccoin[.]com, they contained the strings ***365*** and ***coin***.

- 365coinedition[.]com
- 365coinhtech[.]com
- 365coinlibrary[.]com
- 365coinpromarket[.]com
- 365generatorcoin[.]com
- 365packetcoin[.]com

- 365procentercoin[.]com
- 365profactorycoin[.]com
- 365promotioncoin[.]com
- 365smartcoin[.]com
- 365workspacecoin[.]com

The Infoblox report identified brands and celebrities whose names may have been abused to serve malware through their Facebook and LinkedIn profiles. We named them in the table below and indicated the strings we used on Domains & Subdomains Discovery to search for potentially connected domains. We also included strings found among the IoCs in our search.

Brand/Celebrity Name	Description	Search String
Metacoin	Cryptocurrency used as lure in the scams	***metacoin***
SoulCircuit	DJ duo whose fake profile was used in the scams	***soulcircuit***
Tom Moore	One of SoulCircuit's members	***tommoore***
Dan Timcke	One of SoulCircuit's members	***dantimcke***
Kyriakos Mitsotakis	Greece's Prime Minister whose fake profile was used in the scams	***kyriakosmitsotakis***
Giorgia Meloni	Italy's Prime Minister whose fake profile was used in the scams	***giorgiameloni***
Pedro Sánchez	Spain's Prime Minister whose fake profile was used in the scams	***pedrosanchez***
Rachelle Young	U.S.-based financial analyst whose fake profile was used in the scams	***rachelleyoung***
Mario Draghi	Spanish public official whose fake profile was used in the scams	***mariodraghi***
Dietrich Mateschitz	Austrian businessman whose fake profile was used in the scams	***dietrichmateschitz***

365coinmode[.]com	Domain identified as an IoC	***365coinmode.***
365graphiccoin[.]com	Domain identified as an IoC	***365graphiccoin.***
spartan-trade[.]com	Domain identified as an IoC	***spartan-trade.***
networkfsi[.]com	Domain identified as an IoC	***networkfsi.***

Note that Metacoin is a cryptocurrency owned by Inblock. To date, no such thing as Meta coin, owned by Mark Zuckerberg's Meta, exists.

Using the strings mentioned above, we found 1,657 string-connected domains. No domains containing ***dantimcke***, ***365coinmode.***, and ***365graphiccoin.***, however, were found. Also, only one—walletmetacoin[.]trade—turned out to be a malware host so far. Like two of the original IoCs, it also contained the string ***coin***.

Hunting for Malicious Social Media Pages

According to Infoblox, the cryptocurrency scams targeted Facebook and LinkedIn users. In addition to uncovering other domains that could be part of the threat actors' infrastructure, we also wanted to see if they possibly compromised social media pages apart from those mentioned in the report.

Our search led to the discovery of 529 Facebook and LinkedIn subdomains that began with either ***facebook.com*** or ***linkedin.com*** and were created from 1 January 2023 onward. Thirteen of them were tagged as malicious, all pointing to Facebook pages. Three of the malicious supposedly Facebook pages had the string ***kinderramadan.com***.

—

Apart from identifying 2,490 additional threat artifacts via DNS connections, our analysis also uncovered 13 possibly compromised Facebook pages that could already have figured in scams. That goes to show that IoC expansion is a great addition to any organization's threat discovery toolset.

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

Sample IP Addresses That Played Host to the Domains Identified as IoCs

- 104[.]21[.]41[.]88
- 172[.]67[.]163[.]70

Sample Domains That Shared the IoCs' IP Hosts

- 0-00[.]info
- 0-00[.]online
- 0-097[.]com
- 0-10k[.]online
- 0-231[.]protonet[.]io
- 0-6[.]protonet[.]io
- 0-9j[.]zapto[.]xyz
- 0-d4[.]nid[.]io
- 0-ed[.]nid[.]io
- 0-glacier[.]com
- 166155[.]net
- 365actioncoin[.]com
- 365balancecoin[.]com
- 365bookcoin[.]com
- 365boxcoin[.]com
- 365buildcoin[.]com
- 365centercoin[.]com
- 365centralcoin[.]com
- 365chartcoin[.]com
- 365clientcoin[.]com
- 4p3t9i[.]cyou
- 60yearsnato[.]info
- 6936581[.]com
- 69xx354[.]xyz
- 6hgpj[.]com
- 79811270[.]com
- 7w3highlight[.]shop
- 80sss[.]cc
- 88bm2[.]club
- 911qq[.]net
- a-score-intl-jobs-in-ca[.]fyi
- abacextorpudo[.]tk
- abedreicenmyva[.]ml
- about-drift-casino[.]com
- abowritipicur[.]tk
- achcamo[.]cf
- aclepoluzustio[.]ga
- adamjohnsontherapy[.]com
- adelioproducoes[.]com[.]br
- aderocdistiukelg[.]ga
- b4ke29[.]buzz
- bailiwick[.]com[.]au
- baisaromucec[.]gq
- balikesirdekoronemlak[.]com
- basisdenmark[.]com
- bassinursinghome[.]com
- bateverseward[.]site
- bauspecterealcemi[.]tk
- baweavimanno[.]ga
- bbcmaestro[.]com
- c2dev[.]co[.]nz
- cafciitipdahl[.]cf
- cafe-plein[.]net
- cairogovresults[.]com
- calutguirebolro[.]ga
- cam96vip[.]net
- cardgebestma[.]ml
- carolynaevents[.]com
- carottage-sol[.]fr
- cartoes-de-credito[.]life
- d4n13l3k00[.]ru
- d6print[.]com

- daistabenjetme[.]tk
- dalarangaming[.]com
- dalidendeportres[.]tk
- dan[.]cy
- daniel-dorin-photo[.]de
- dardmetvevernilec[.]ml
- dayweamuchamo[.]tk
- dc-mx[.]5640b2910069[.]bshcl[.]com
- easydog[.]info
- ecoschet[.]ru
- editorone[.]org
- ehdresesbracreta[.]ga
- eichblatt[.]net
- ejttekjo[.]ml
- ekridubilinkhang[.]tk
- elaen[.]com
- elbisivssecorp[.]com
- eleutheranea[.]gr
- fake[.]goubixi6019[.]homes
- fanhaoabc[.]com
- fastblockad[.]com
- fazendadopeixe[.]com
- fciec[.]gq
- fdf[.]ceding-cranial[.]shop
- fenhealhchicareta[.]tk
- ferguson-legal[.]com
- fighpihapnelazdulg[.]gq
- find-private-jets[.]live
- 0-jf[.]protonet[.]io
- 0-jk[.]protonet[.]io
- 0-mnygrestore[.]com
- 0-mtb[.]com
- 0-mtbactive[.]com
- 0-mtbactive09[.]com
- 0-mtbactive3[.]com
- 0-news[.]info
- 0-qt[.]com
- 0-t3[.]protonet[.]io

Sample Malicious IP-Connected Domains

- bl-invest[.]shop
- bnzzl[.]net
- 000363634847372628393836363838[.]xyz
- 365coinedition[.]com
- 365coinhtech[.]com
- 365coinlibrary[.]com
- 365coinpromarket[.]com
- 365generatorcoin[.]com
- 365packetcoin[.]com
- 365procentercoin[.]com
- 365profactorycoin[.]com
- 365promotioncoin[.]com
- 365smartcoin[.]com
- 365workspacecoin[.]com

Sample Domains That Contained Strings Found among the IoCs

- metacoin[.]pl
- metacoin[.]cz
- metacoin[.]co
- metacoin[.]ae
- metacoin[.]cn
- metacoin[.]fr
- metacoin[.]ie
- metacoin[.]ky
- metacoin[.]fi
- metacoin[.]es
- soulcircuit[.]ca
- soulcircuit[.]com
- soulcircuit[.]net
- soulcircuits[.]com
- swsoulcircuit[.]com
- soulcircuitry[.]org

- soulcircuitry[.]com
- thesoulcircuit[.]com
- soulcircuit419[.]com
- soulcircuitry[.]ninja
- tommoore[.]uk
- tommoore[.]us
- tommoore[.]bz
- tommoore[.]co
- tommoore[.]ca
- tommoore[.]io
- tommoore[.]be
- tommoore[.]me
- tommoore[.]eu
- tommoore[.]in
- kyriakosmitsotakis[.]eu
- kyriakosmitsotakis[.]gr
- kyriakosmitsotakis[.]com
- giorgiameloni[.]eu
- giorgiameloni[.]de
- giorgiameloni[.]it
- giorgiameloni[.]es
- giorgiameloni[.]net
- giorgiameloni[.]com
- giorgiameloni[.]one
- pedrosanchez[.]ca
- pedrosanchez[.]tk
- pedrosanchez[.]ph
- pedrosanchez[.]es
- pedrosanchez[.]eu
- pedrosanchez[.]me
- pedrosanchez[.]mx
- pedrosanchez[.]ch
- pedrosanchez[.]us
- pedrosanchez[.]org
- rachelleyoung[.]com
- rachelleyoung[.]info
- rachelleyounglaw[.]com
- mariodraghi[.]co
- mariodraghi[.]it
- mariodraghi[.]eu
- mariodraghi[.]fun
- mariodraghi[.]uno
- mariodraghi[.]org
- mariodraghi[.]com
- dietrichmateschitz[.]xyz
- dietrichmateschitz[.]org
- dietrichmateschitz[.]com
- dietrichmateschitzfoundation[.]org
- thestoryofdietrichmateschitz[.]com
- spartan-trade[.]eu
- spartan-trade[.]co[.]uk
- networkfsi[.]io
- inblock[.]one
- inblock[.]io
- inblock[.]info
- inblock[.]uk
- inblock[.]org
- inblock[.]app
- inblock[.]pl
- inblock[.]net
- inblock[.]online
- inblock[.]co[.]kr
- inblock[.]cz
- inblock[.]eu
- metacoin[.]im
- metacoin[.]sk
- metacoin[.]it
- metacoin[.]ng
- metacoin[.]ph
- metacoin[.]uk
- metacoin[.]nz
- metacoin[.]yt
- metacoin[.]cl
- metacoin[.]st
- metacoin[.]in
- metacoin[.]to
- metacoin[.]cm
- metacoin[.]jp
- metacoin[.]io
- metacoin[.]tk

- metacoin[.]la
- metacoin[.]ws
- metacoin[.]pw
- metacoin[.]lc

Sample Subdomains That Start with facebook.com or linkedin.com Registered from 1 January 2023 Onward

- facebook[.]com-log-in[.]php-wa-ss-ap-directed-to-sign-in-rnd[.]491[.]https[.]facebook[.]irregularcorp[.]com
- facebook[.]com[.]br[.]allposters[.]com
- facebook[.]comiman[.]minibueno[.]com[.]pl
- facebook[.]xn--comlogin-g03d[.]yogurt-slice[.]com[.]pl
- facebook[.]com[.]oladshorten[.]com
- facebook[.]com[.]hightail[.]abccorp[.]officient[.]io
- facebook[.]comyash[.]ferrerogarden[.]pl
- facebook[.]com-vote[.]pour[.]votre[.]amie[.]www[.]server-landing-page[.]web-8[.]hiltonbusinessonline[.]com
- facebook[.]com[.]143445326546245727575247457427[.]rosenberger[.]it
- facebook[.]com[.]giveway[.]waldorfastoriaberlin[.]web-11[.]hiltonbusinessonline[.]com
- facebook[.]com[.]surveymonkey[.]ca
- facebook[.]com[.]apndojo[.]com
- facebook[.]com[.]pagelike[.]fallguys2[.]net
- facebook[.]com[.]fr[.]faceb0ok[.]com[.]fr[.]kinderjoy[.]cz
- facebook[.]com[.]ncontrol[.]de
- facebook[.]comvax[.]com[.]com
- facebook[.]com-log-in[.]php-wa-ss-ap-directed-to-sign-in-rnd[.]491[.]https[.]facebook[.]pcbuildingsim[.]net
- facebook[.]com[.]business[.]kinepolis[.]fr
- facebook[.]com[.]mobile[.]user[.]login[.]matomo[.]cloud
- facebook[.]com[.]ns3[.]kinepolis[.]fr
- facebook[.]com[.]pagelike[.]nutellago[.]com[.]pl
- facebook[.]com[.]security-checkpocust83t-global-do[.]kinepolis[.]fr
- facebook[.]com[.]security-checkpoint-global-do[.]preprod[.]kinepolis[.]fr
- facebook[.]com[.]security-cimmoweltteckpoint-global-do[.]kinepolis[.]fr
- facebook[.]com[.]security-sagepub-global-do[.]kinepolis[.]fr
- facebook[.]com-vote[.]pour[.]votre[.]amie[.]fallguystwo[.]com
- facebook[.]xn--comlogin-g03d[.]fallguysultimateknockout[.]net
- facebook[.]com-vote[.]pour[.]votre[.]amie[.]fallguysuniverse[.]com
- facebook[.]com-vote[.]pour[.]votre[.]amie[.]kinderjoycrazyfriendsroadshow[.]pl
- facebook[.]comwww[.]virnow[.]com
- facebook[.]comiman[.]co-spotka-chlodka[.]pl
- xn--faceboo-uw3c[.]com[.]xn--jga[.]co
- facebook[.]com[.]l[.]helper[.]kindermaxiking[.]pl
- facebook[.]com-----bakutntztn---value[.]greencall[.]us

- facebook[.]com[.]fi[.]cloudplatform[.]fi
- facebook[.]com[.]signe[.]officient[.]io
- facebook[.]com[.]voicestesting[.]com
- facebook[.]com[.]giveway[.]ns30[.]kinderramadan[.]com
- facebook[.]com[.]x[.]yj6e6au11729y6edtel5amrskg2mvqnafrdrnxwmq4tu[.]3232281222[.]tfkc[.]de
- facebook[.]com[.]hbr[.]com
- facebook[.]com[.]g30[.]space
- facebook[.]com[.]l[.]helper[.]ns95[.]kinderramadan[.]com
- facebook[.]com[.]l[.]helper[.]trafficjunky[.]com
- facebook[.]com[.]nera[.]com[.]ph
- facebook[.]com[.]profile[.]fortnite[.]com
- facebook[.]com[.]security-checkpoint-global-acces[.]kinepolis[.]fr
- facebook[.]com[.]security-checkpoint-global-at[.]kinepolis[.]fr
- facebook[.]com[.]b5b86cde58a63b3c9dfbda4652f08c47[.]opalsystems[.]com
- facebook[.]com-update-your-account[.]fallguysultimateknockout[.]com
- facebook[.]com[.]yelptop100[.]com
- facebook[.]com[.]www[.]westloophotel[.]web-6[.]hiltonbusinessonline[.]com
- facebook[.]com[.]watch[.]hmpanel[.]tk
- facebook[.]com[.]pagelike[.]withthegrid[.]com
- facebook[.]com[.]login[.]housepartyfun[.]com
- facebook[.]com[.]fallguys[.]biz
- facebook[.]com[.]profile[.]accounts[.]login[.]userid41d01251163648121s5213[.]ferreroduplo[.]com[.]pl
- facebook[.]com[.]login[.]fallguys-shop[.]com
- facebook[.]com[.]nutella[.]com[.]pl
- facebook[.]com[.]pagelike[.]fallguysultimateknockout[.]net
- facebook[.]com[.]evernote[.]rkscorpsb30[.]dataloader[.]io
- facebook[.]com-vote[.]pour[.]votre[.]amie[.]ns9[.]kinderramadan[.]com
- facebook[.]com[.]servers[.]eurocons umers[.]org
- facebook[.]com[.]security-checkpoint-global-do[.]robocalls[.]ai
- facebook[.]com[.]security-checkpoint-kl-cdn-acc-do[.]kinepolis[.]fr
- facebook[.]com[.]login[.]datahub[.]deliveryhero[.]net
- facebook[.]com[.]venmo[.]com
- facebook[.]com[.]login[.]yogurtslice[.]pl
- facebook[.]com[.]l[.]helper[.]teenidolsroadshow[.]pl
- facebook[.]com[.]pagelike[.]propojse[.]cz
- linkedin[.]com[.]yogurt-slice[.]com[.]pl
- linkedin[.]com[.]portal[.]esonportpw10[.]ph
- linkedin[.]com[.]downloadfallguys[.]com
- linkedin[.]com[.]kinderbuenomini[.]com
- linkedin[.]com[.]dgcement[.]com
- linkedin[.]com[.]kinder[.]com[.]pl
- linkedin[.]com[.]www[.]kinderplussport[.]sk
- linkedin[.]com[.]joghurtschnitte[.]pl

- linkedin[.]com[.]hiltontravelagents[.]web-11[.]hiltonbusinessonline[.]com
- linkedin[.]com[.]xbl[.]spamhause[.]org
- linkedin[.]com[.]zabawanacalegokinder[.]com[.]pl
- linkedin[.]com[.]edgekey[.]net
- linkedin[.]com[.]fallguys3d[.]com
- linkedin[.]com[.]g30[.]space
- linkedin[.]com[.]nexflick[.]ca
- linkedin[.]com[.]fallguys-mobile[.]com
- linkedin[.]com[.]tribalwars2[.]com
- linkedin[.]com[.]fallguysmusic[.]net
- linkedin[.]com[.]kinderchocolatemaxi[.]pl
- linkedin[.]com[.]fallguys[.]biz
- linkedin[.]com[.]fallguystwo[.]com
- linkedin[.]com[.]wixanswers[.]com
- linkedin[.]com[.]tictacliberty[.]com[.]pl
- linkedin[.]com[.]pralinkyferrero[.]cz
- linkedin[.]com[.]fallguys-movie[.]net
- linkedin[.]com[.]animalfriends[.]co[.]uk
- linkedin[.]com[.]art[.]com
- linkedin[.]com[.]irregularcorporation[.]com
- linkedin[.]com[.]kinderjoyroadshowzabawanacalego[.]eu
- linkedin[.]com[.]kinderdelice[.]ch
- linkedin[.]com[.]rondnoir[.]com[.]pl

Sample Malicious String-Connected Subdomains

- facebook[.]com[.]oladshorten[.]com
- facebook[.]com-----bakutntztn---value[.]greencall[.]us
- facebook[.]com[.]giveway[.]ns30[.]kinderramadan[.]com
- facebook[.]com[.]login[.]ns62[.]kinderramadan[.]com
- facebook[.]com[.]athleo[.]net
- facebook[.]com[.]zzzzz[.]get[.]laid[.]at[.]www[.]swingingcommunity[.]com
- facebook[.]com-update-your-account[.]ns79[.]kinderramadan[.]com