ソーシャルメディアを利用したセレブ詐欺の痕跡をDNSで追跡

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

Infobloxは2022年第4四半期のサイバー脅威報告書において、欧州連合（EU）のユーザーを標的に偽の有名人の推薦コメントを用いた「Meta」コイン詐欺を取り上げました。その分析により、詐欺を回避する上で役立つ複数のセキュリティ侵害インジケーター（IoC）、具体的には4つのドメイン名と1つのIPアドレスが明らかになりました。特定されたIoCは以下の通りです。

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

インターネットをユーザーにとって透明で安全な場所にするという使命を果たすべく、WhoisXML APIは今回、上記のIoCリストを拡張し、すでに詐欺に使われている可能性のあるソーシャルメディアのページを特定する調査を行いました。その結果、以下を発見しました。

- IoCと特定されたドメイン名をホストするさらに3つのIPアドレス
- IoCのIPアドレスを共用する830個のドメイン名。うち26個には悪意があることが判明
- IoCとしてタグ付けされたドメイン名と同じ文字列を含む1,657個のドメイン名。そのうち1つはマルウェアホストであることを確認
- 2023年1月1日以降にDNSに登録されたFacebookおよびLinkedInのページ529件、うち13件には悪意があることが判明

現在のIoCリストを拡張

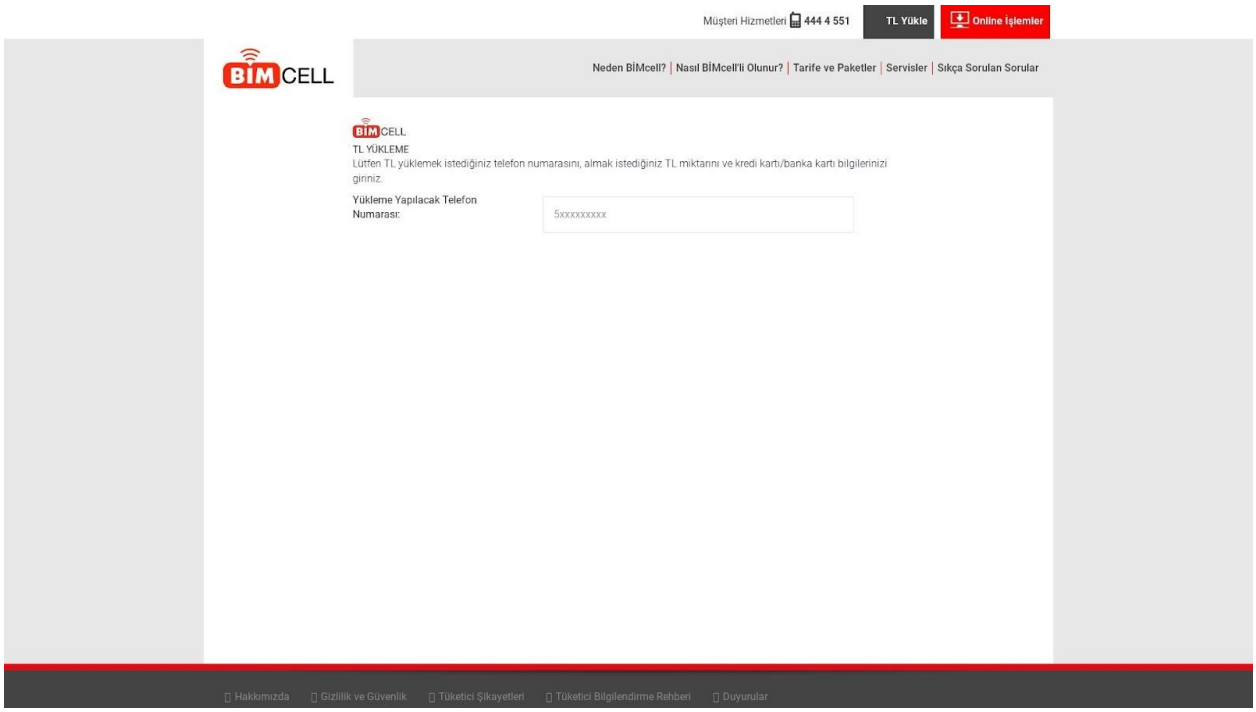
まずIoCと特定されたドメイン名をWHOIS lookupsで検索し、以下の共通点を見出しました。

- 4つのドメイン名はいずれも2022年に作成されたもの。したがって悪意あるキャンペーンに使用される際に新規登録されたドメイン名と考えられる

- 3つのドメイン名、すなわち365coinmode[.]com、365graphiccoin[.]comおよびnetworkfsi[.]comは、Namecheap, Inc.を介してアイスランドで登録されたもの
- 2つのドメイン名、すなわち365coinmode[.]comおよび365graphiccoin[.]comは、InfobloxがIoCと特定したIPアドレス（45[.]63[.]119[.]177）を共用

次に、4つのドメイン名をDNS lookupsで検索してさらに3つのIPアドレスが見つかったため、IPアドレスの総数は4つになりました。これらを検索キーワードとしてreverse IP lookupにかけた結果、3つは共用で、元のIoCリストに含まれていた45[.]63[.]119[.]177が専用アドレスであることがわかりました。そして、この検索により、IoCのIPアドレスを共用するドメイン名がさらに830個発見できました。マルウェアの一括チェックにかけた結果、そのうち26件はマルウェアのホストであることが判明しました。

悪意あるサイトをScreenshot lookupsで検索したところ、bnzzl[.]netは携帯電話の電話帳のように見える生きたコンテンツをホストし続けていたことが判明しました。



bnzzl[.]netの
スクリーンショット

また、興味深いことに、悪意あるIPアドレスを共用しているドメイン名のうち11個が、IoCとされた2つのドメイン名と酷似していました。例えば、365coinmode[.]comと365graphiccoin[.]comは、***365***と***coin***という文字列を含んでいます。

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

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

Infobloxの報告書は、FacebookとLinkedInのプロフィールを介したマルウェア配布のために悪用された可能性のあるブランドおよび有名人の名前を特定しました。以下の通りです。下表はまた、関連している可能性のあるドメイン名を探すためにDomains & Subdomains Discoveryで使用した検索文字列も示しています。それには、当社の調査においてIoCの間に見られた文字列も含めました。

ブランド/有名人の名前	概要	検索文字列
Metacoin	詐欺のルアーとして使われた暗号通過	***metacoin***
SoulCircuit	偽のプロフィールが詐欺に使われた二人組のDJ	***soulcircuit***
Tom Moore	SoulCircuitのメンバーの1人	***tommoore***
Dan Timcke	SoulCircuitのメンバーの1人	***dantimcke***
Kyriakos Mitsotakis	偽プロフィールが詐欺に使われたギリシャの首相	***kyriakosmitsotakis***
Giorgia Meloni	偽プロフィールが詐欺に使われたイタリアの首相	***giorgiameloni***
Pedro Sánchez	偽プロフィールが詐欺に使われたスペインの首相	***pedrosanchez***
Rachelle Young	偽プロフィールが詐欺に使われた米国在住の金融アナリスト	***rachelleyoung***
Mario Draghi	偽プロフィールが詐欺に使われたスペインの公職者	***mariodraghi***
Dietrich Mateschitz	偽プロフィールが詐欺に使われたオーストリアのビジネスマン	***dietrichmateschitz***

365coinmode[.]com	IoCと特定されたドメイン名	***365coinmode.***
365graphiccoin[.]com	IoCと特定されたドメイン名	***365graphiccoin.***
spartan-trade[.]com	IoCと特定されたドメイン名	***spartan-trade.***
networkfsi[.]com	IoCと特定されたドメイン名	***networkfsi.***

なお、MetacoinはInblock社が所有する暗号通貨です。現在のところ、Mark ZuckerbergのMetaが所有するMetaコインというものは存在しません。

上記の文字列をもとに、共通の文字列を含むドメイン名が1,657個見つかりました。しかし、***dantimcke***、***365coinmode***および***365graphiccoin***を含むドメイン名はありませんでした。また、マルウェアのホストであることが判明したのは、今のところwalletmetacoin[.]tradeの1つだけでした。元のIoCのうち2つと同様、このドメイン名にも***coin***という文字列が含まれています。

悪意あるソーシャルメディアのページを追跡

Infobloxによると、この暗号通貨詐欺はFacebookとLinkedInのユーザーを標的としたものでした。そこで、脅威アクターのインフラとなり得る他のドメイン名を発見することに加え、報告書に出ていたもの以外に侵害された可能性のあるソーシャルメディアページがあるかどうかも確認することにしました。

調査の結果、***facebook.com***または***linkedin.com***で始まり、2023年1月1日以降に新規登録されたFacebookおよびLinkedInのサブドメインが529個発見されました。そのうち13個は悪意あるものとしてタグ付けされ、すべてFacebookページを指していました。悪意があるとされたFacebookページのうち3つは、***kinderramadan.com***という文字列を持っていました。

—

今回、DNSの関連性を解明することで脅威となるアーティファクトがさらに2,490個発見できたほか、詐欺に使われた可能性のある13のFacebookページも特定できました。IoCリストの拡張は、あらゆる組織で脅威発見の強力なツールとなります。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

IoCと特定されたドメイン名のホストとなったIPアドレスの例

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

IoCと同じIPアドレスを共用していたドメイン名の例

- 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

共通のIPアドレスを使用していた悪意あるドメイン名の例

- 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

IoCの間で見られた文字列を含むドメイン名の例

- 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

2023年1月1日以降に登録された、facebook.comやlinkedin.comで始まるサブドメインの例

- 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[.]1434453265462457275757247457427[.]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-cimmoweleckpoint-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[.]teenidols roadshow[.]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[.]kinderplusport[.]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

共通の文字列を含む悪意あるサブドメインの例

- 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