DNSのレンズで見るフェイクID市場

目次

要旨

昨今、人々の物理的な国際移動をバーチャルの領域から実現しようとする動きが広がっています。外国への旅行や移住を望む人は多いですが、身分証明書やパスポートなど様々な法的文書が必要となるため、「言うは易く行うは難し」です。

かつては、海外に行くためにリアルの世界でいかがわしい人々と取引し、偽造身分証（以下「フェイクID」）を手に入れようとする人もいました。今ではそうした取引は全てオンラインで済ませられるようになっています。そして、フェイクIDに対する高い需要に目をつけた多くの脅威アクターが、独自のオンライン市場を立ち上げています。

WhoisXML APIの脅威リサーチャーであるDancho Danchevは最近、そのようなフェイクID販売業者のものとされるnoveltypro1@hotmail [.] comというメールアドレスを見つけました。当社の研究チームはこれを受け、その脅威アクターがどの程度広範囲に活動しているかをDNSで調査しました。

今回の分析で、関連する以下のアーティファクトが新たに検出されました：

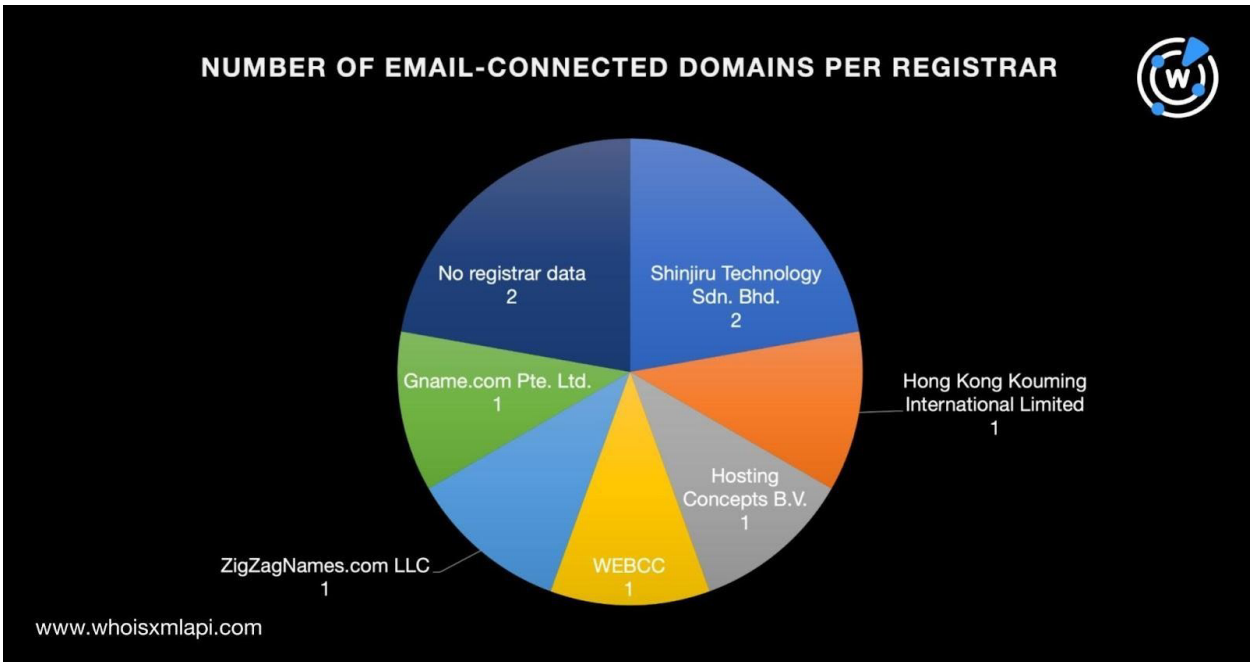
- 同じメールアドレスを使用して登録されていたドメイン名9個
- そのドメイン名をホストしていたIPアドレス7個
- 共通のIPアドレスでホストされていたドメイン名1個
- フェイクID市場に関連した共通の文字列を含むドメイン名231個
- フェイクID市場に関連した共通の文字列を含むサブドメイン777個

DNSでの繋がり

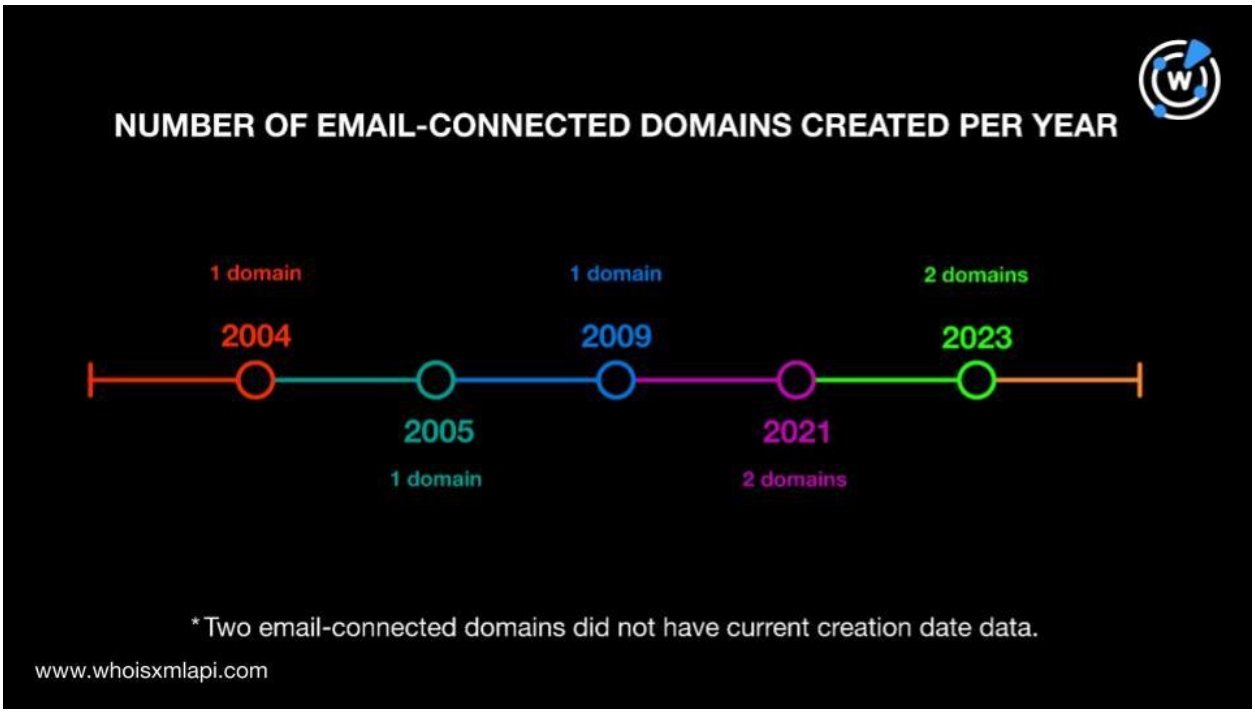
まず、WHOIS History Searchを使い、noveltypro1@hotmail [.] comがWHOISレコードに含まれているドメイン名を探しました。その結果、9個のドメイン名が見つかりました。

その9個のドメイン名をBulk WHOIS Lookupにかけたところ、以下が判明しました：

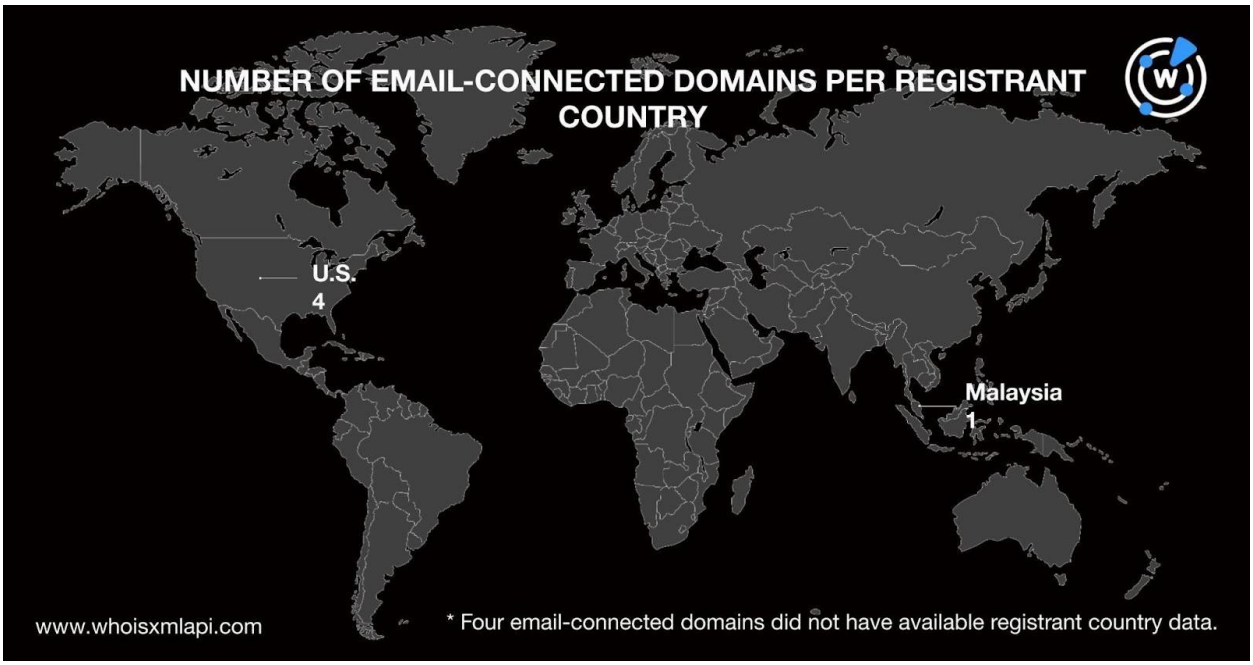
- 9個のうち2個のドメイン名は、Shinjiru Technology Sdn. Bhd.というレジストラによって管理されていました。また、Hong Kong Kouming International Limited、Hosting Concepts B.V.、WEBCC、ZigZagNames.com LLC、Gname.com Pte. Ltd.がそれぞれ1個のドメイン名を管理していました。残りの2個のドメイン名については、現在のレジストラのデータがWHOISで公開されていませんでした。



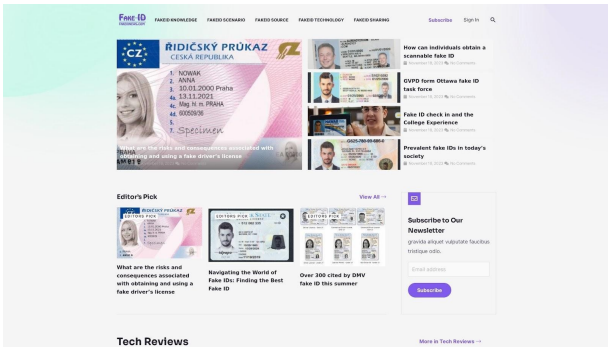
- 2個のドメイン名には新規登録日のデータがありませんでしたが、残りの7個は2004年から2023年の間に新規登録されたものでした。



- 4個は米国で登録されたドメイン名でした。また、マレーシアで登録されたものが1個ありました。残りの4個には登録国のデータがありませんでした。



Screenshot Lookupの結果から、本稿執筆時点で5個のドメイン名はアクセス不能とわかりました。他方、3個は有効なコンテンツをホストし続けており（下図の通り）、残りの1個はエラーページにつながりました。



fakeidnews[.]comのスクリーンショット

fakeidreview[.]comのスクリーンショット

noveltyidsite[.]comのスクリーンショット

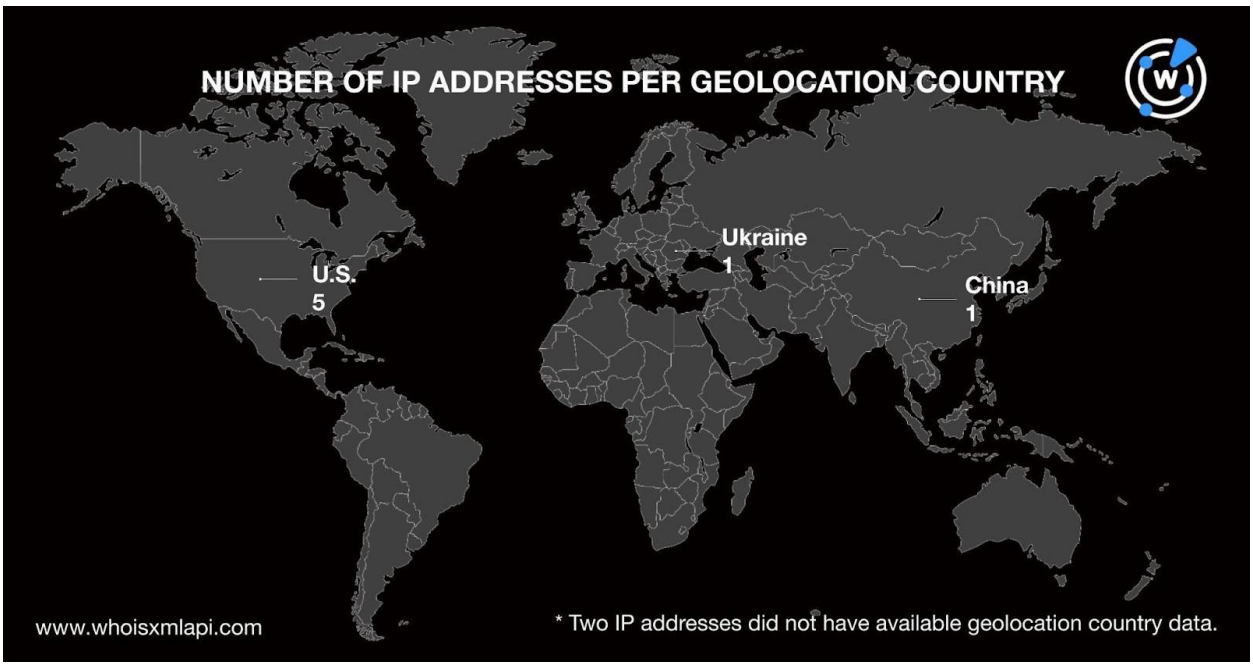
内容からして、上記3つのサイトは、パスポート、免許証、卒業証書といった偽のIDを購入者に提供している可能性があります。

次に、noveltypro1@hotmail [.] comを使用して登録されていたドメイン名をDNS Lookupにかけたところ、7個のユニークなIPアドレスに名前解決しました。そのIPアドレスに対してThreat Intelligence Lookupを実行した結果、下表の通り、5個のIPアドレスに関する興味深い事実が明らかになりました。

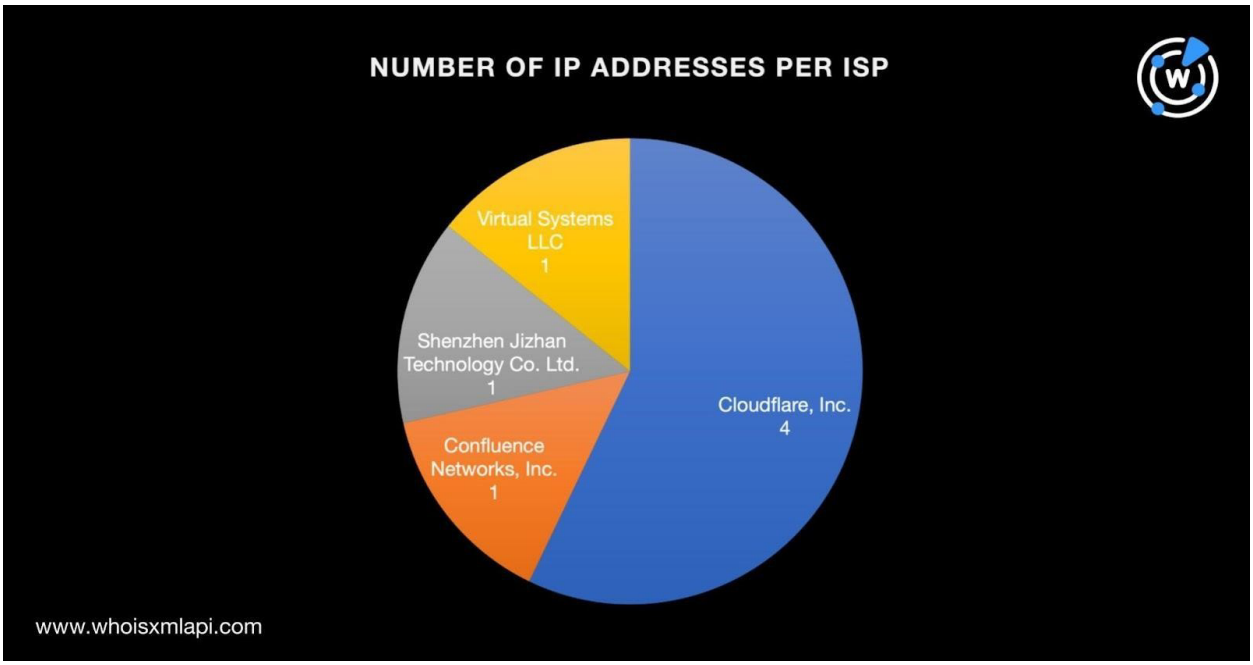
IPアドレス	脅威の種類
172[.]67[.]148[.]80	Generic Phishing
208[.]91[.]197[.]46	Generic Phishing Malware Suspicious C&C
172[.]67[.]132[.]236	Generic Phishing Malware
104[.]21[.]29[.]28	Generic Phishing
104[.]21[.]13[.]182	Generic Phishing Malware

さらに、7個のIPアドレスをBulk IP Geolocation Lookupで検索したところ、以下が判明しました：

- 5個のジオロケーションは米国で、中国とウクライナにそれぞれ1個が位置していました。



- 最も多くのIPアドレスを管理していたISPはCloudflare, Inc.（4個）でした。また、Virtual Systems LLC、Shenzhen Jizhan Technology Co. Ltd.、Confluence Networks, Inc.がそれぞれ1個を管理していました。



7個のIPアドレスをReverse IP Lookupにかけたところ、2個は専用アドレスと思われ、合計で3個のドメイン名をホストしていました。その3個からnoveltypro1@hotmail [.] comを使用しているドメイン名と重複を取り除いた結果、ドメイン名1個（handyman-joes[.]com）が残りました。

noveltypro1@hotmail [.] comを使用していたドメイン名をさらに精査したところ、フェイクID関連のウェブプロパティに含まれている6種類のテキスト文字列が浮上しました。それらをキーワードとしてDomains & Subdomains Discoveryで検索した結果、2023年1月1日以降に作成または追加された別のドメイン名とサブドメインが検出されました。詳細は下表の通りです。なお、ここに示されているドメイン名の数には、すでにnoveltypro1@hotmail [.] comまたは共通のIPアドレスを使っていると特定されたドメイン名も含まれています。

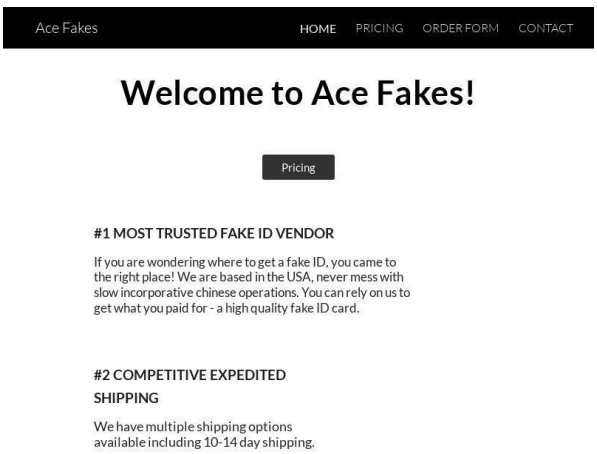
テキスト文字列	その文字列を含むドメイン名の数	その文字列を含むサブドメインの数
cloneid	3	11
fakeid	195	685

fakeidentity	6	0
idclone	10	46
identityclone	0	1
idfake	17	34

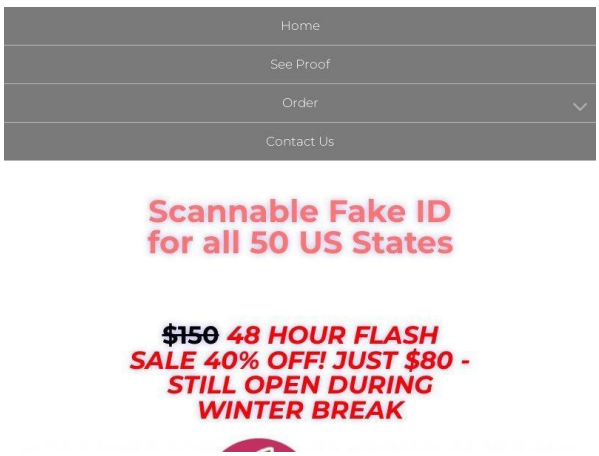
noveltypro1@hotmail [.] comまたは共通のIPアドレスを使っているドメイン名としてすでにタグ付けされていたものと重複を除外した結果、共通の文字列を使っているドメイン名とサブドメインがそれぞれ231個と777個残りました。

そして、そのうち152個のドメイン名と370個のサブドメインが、本稿執筆時点でアクセス可能なままとなっていました。

スクリーンショットから、152個のドメイン名のうち42個はフェイクIDを販売または宣伝するサイトをホストしていることがわかります。以下はその例です。

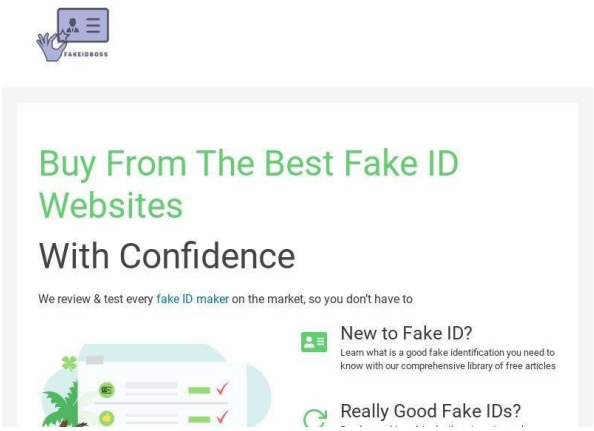


共通の文字列を含むドメイン名 acefakeids[.]laのスクリーンショット



共通の文字列を含むドメイン名 bestfakeids[.]comのスクリーンショット

共通の文字列を含むドメイン名 deluxefakeid[.]comのスクリーンショット

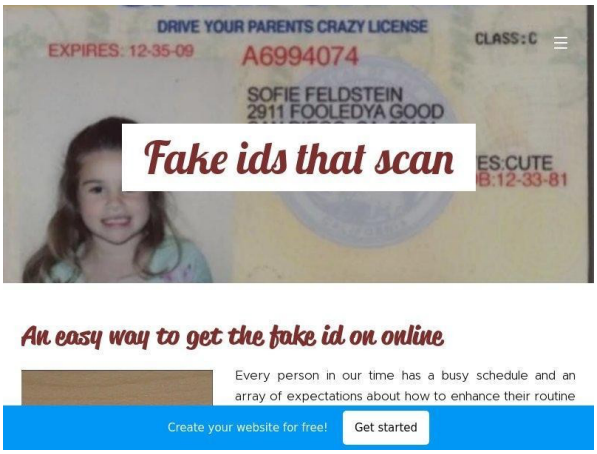


共通の文字列を含むドメイン名 fakeidboss[.]netのスクリーンショット

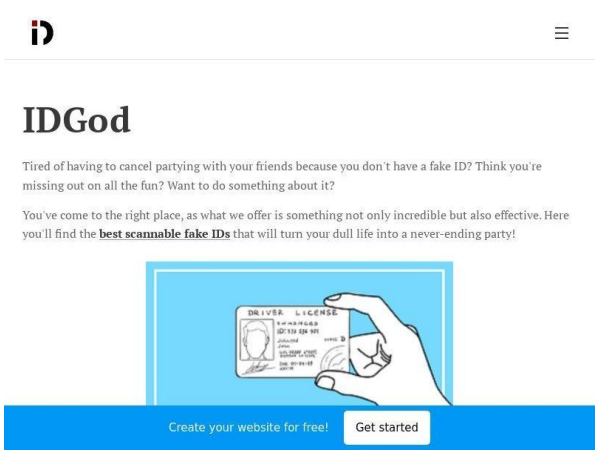
さらに、共通の文字列を含むサブドメインのうち24個は、フェイクIDの利用拡大に関連していると思われるページもホストしていました。その一部は、無料ブログプラットフォームのドメイン名にも該当するようです。以下の4つの例を見てみましょう。

共通の文字列を含むサブドメイン buyirelandfakeid80998[.]xzblogs[.]com のスクリーンショット

共通の文字列を含むサブドメイン delawarefakeid04475[.]bloggerswise[.]com のスクリーンショット



共通の文字列を含むサブドメイン fakeidsthatscan[.]webnode[.]pageのスクリーンショット



共通の文字列を含むサブドメイン scannablefakeid[.]webnode[.]pageのスクリーンショット

—

当社の分析により、フェイクID販売業者のたった1つのメールアドレスから、同じ悪意あるインフラの一部かもしれない17のウェブプロパティ（同じメールアドレスを使用して登録されているドメイン名9個、IPアドレス7個、共通のIPアドレスを使用しているドメイン名1個）が芋づる式に検出されました。また、フェイクID販売業者に属している可能性のある合計522個のドメイン名とサブドメインも見つかりました。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

IoCとして特定されたメールアドレス

- noveltypro1@hotmail[.]com

同じメールアドレスを使って登録されたドメイン名の例

- fakeidnews[.]com
- fakeidreview[.]com

- id-clone[.]com
- identity-solution[.]com
- noveltyidfactory[.]com

IPアドレスの例

- 172[.]67[.]148[.]80
- 91[.]230[.]121[.]48
- 154[.]197[.]253[.]135
- 208[.]91[.]197[.]46

悪意あるIPアドレスの例

- 172[.]67[.]148[.]80
- 208[.]91[.]197[.]46
- 172[.]67[.]132[.]236

共通のIPアドレスを使用していたドメイン名

- handyman-joes[.]com

共通の文字列を含むドメイン名の例

- a3fakeids[.]com
- aaaabbbbccccsonounhostfakeidrotour-com[.]music
- aaaabbbbccccsonounhostfakeidrotour-com[.]xn--fiqs8s
- aaaabbbbccccsonounhostfakeidrotour-com[.]xn--fiqz9s
- aaaabbbbccccsonounhostfakeidrotour-com[.]xn--ngbrx
- aaaabbbbccccsonounhostfakeidrotour-it[.]ph
- aaaabbbbccccsonounhostfakeidrotour-it[.]vg
- aaaabbbbccccsonounhostfakeidrotour-it[.]xn--fiqs8s
- aaaabbbbccccsonounhostfakeidrotour-it[.]xn--node
- aaaabbbbccccsonounhostfakeidrotour[.]aquila[.]it
- aaaabbbbccccsonounhostfakeidrotour[.]arab
- aaaabbbbccccsonounhostfakeidrotour[.]music
- aaaabbbbccccsonounhostfakeidrotour[.]ph
- aaaabbbbccccsonounhostfakeidrotour[.]vg
- aaaabbbbccccsonounhostfakeidrotour[.]ws
- aaaabbbbccccsonounhostfakeidrotour[.]xn--fiqs8s
- aaaabbbbccccsonounhostfakeidrotour[.]xn--node
- aaaabbbbccccsonounhostfakeidrotour[.]ye
- aaaabbbbccccsonounhostfakeidrotourdolomiti-com[.]music
- aaaabbbbccccsonounhostfakeidrotourdolomiti-com[.]vg
- aaaabbbbccccsonounhostfakeidrotourdolomiti-com[.]ws
- aaaabbbbccccsonounhostfakeidrotourdolomiti-com[.]xn--mxtq1m
- aaaabbbbccccsonounhostfakeidrotourdolomiti-it[.]vg

- aaaabbbbccccsonounhostfakeidrotourdolomiti-it[.]ws
- aaaabbbbccccsonounhostfakeidrotourdolomiti-it[.]xn--fiqs8s
- aaaabbbbccccsonounhostfakeidrotourdolomiti-it[.]xn--node
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]arab
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]com[.]ph
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]music
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]ph
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]vg
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]ws
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]xn--fiqz9s
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]xn--mxtq1m
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]xn--node
- acefakeids[.]la
- acidfake[.]online
- aifakeidols[.]com
- amazonfakeid[.]biz
- amazonfakeid[.]club
- amazonfakeid[.]co
- androidfakecallstudio[.]work
- avidfake[.]org
- bestfakeidreview[.]com
- bestfakeids[.]com
- bestfakeidsiteseuropein[.]us
- bestfakeidwebsites[.]us
- beyondcycloneidai[.]org
- bidclone[.]com

共通の文字列を含むサブドメインの例

- 2016-07-01-fakeidentd[.]lb[.]dev[.]atg[.]se
- 2022fakeid21933[.]vidublog[.]com
- 2022fakeid86869[.]oblogation[.]com
- 275a04abf10e[.]fakeidcard[.]marakana[.]com
- 2xfakeidentd[.]merchant-ca[.]dev[.]atg[.]se
- 4bahidfakeip[.]foxycart[.]com
- 4urfakeidlybkyahswydcblxiytvv1678295566[.]darnuid[.]imrworldwide[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]0e[.]vc
- aaaabbbbccccsonounhostfakeidrotour[.]1kapp[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]2ix[.]ch
- aaaabbbbccccsonounhostfakeidrotour[.]adobeaemcloud[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]amscompute[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]atl[.]jelastic[.]vps-host[.]net
- aaaabbbbccccsonounhostfakeidrotour[.]authgear-staging[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]balena-devices[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]bloxcms[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]builtwithdark[.]com

- aaaabbbbccccsonounhostfakeidrotour[.]cafjs[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]cloudcontrolapp[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]co[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]codespot[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]ddnslive[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]de[.]gt
- aaaabbbbccccsonounhostfakeidrotour[.]demo[.]datacenter[.]fi
- aaaabbbbccccsonounhostfakeidrotour[.]deno-staging[.]dev
- aaaabbbbccccsonounhostfakeidrotour[.]discordsays[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]dopaas[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]encoreapi[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]framer[.]app
- aaaabbbbccccsonounhostfakeidrotour[.]framercanvas[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]gr[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]herokuapp[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]heteml[.]net
- aaaabbbbccccsonounhostfakeidrotour[.]hidora[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]hotelwithflight[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]impertrixcdn[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]j[.]scaleforce[.]com[.]cy
- aaaabbbbccccsonounhostfakeidrotour[.]j[.]scaleforce[.]net
- aaaabbbbccccsonounhostfakeidrotour[.]jelastic[.]saveincloud[.]net
- aaaabbbbccccsonounhostfakeidrotour[.]jls-sto1[.]elastx[.]net
- aaaabbbbccccsonounhostfakeidrotour[.]jp[.]ngrok[.]io
- aaaabbbbccccsonounhostfakeidrotour[.]meteorapp[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]myshopblocks[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]myspreadshop[.]at
- aaaabbbbccccsonounhostfakeidrotour[.]myspreadshop[.]com[.]au
- aaaabbbbccccsonounhostfakeidrotour[.]nalchik[.]ru
- aaaabbbbccccsonounhostfakeidrotour[.]ngrok[.]app
- aaaabbbbccccsonounhostfakeidrotour[.]noop[.]app
- aaaabbbbccccsonounhostfakeidrotour[.]onrender[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]orsites[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]outsystemscloud[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]oxa[.]cloud
- aaaabbbbccccsonounhostfakeidrotour[.]pagespeedmobilizer[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]pagexl[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]platter-app[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]pythonanywhere[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]reservd[.]com

- aaaabbbbccccsonounhostfakeidrotour[.]reserve-online[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]simplesite[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]tabitorder[.]co[.]il
- aaaabbbbccccsonounhostfakeidrotour[.]tuva[.]su
- aaaabbbbccccsonounhostfakeidrotour[.]uk[.]reclaim[.]cloud
- aaaabbbbccccsonounhostfakeidrotour[.]vercel[.]app
- aaaabbbbccccsonounhostfakeidrotour[.]weeklylottery[.]org[.]uk
- aaaabbbbccccsonounhostfakeidrotour[.]woltlab-demo[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]wpenginepowered[.]com
- aaaabbbbccccsonounhostfakeidrotour[.]xn--gnstigliefern-wob[.]de
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]123homepage[.]it
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]123paginaweb[.]pt
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]123siteweb[.]fr
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]12hp[.]at
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]12hp[.]de
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]1kapp[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]adobeioruntime[.]net
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]airkitapps-au[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]appspaceusercontent[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]atl[.]jelastic[.]vps-host[.]net
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]au[.]ngrok[.]io
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]authgear-staging[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]balena-devices[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]barsy[.]net
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]bmoattachments[.]org
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]br[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]cafjs[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]canva-apps[.]cn
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]canva-apps[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]carrd[.]co
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]cloudns[.]info
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]cloudns[.]pw
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]co[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]codespot[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]daplie[.]me
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]deno-staging[.]dev
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]discordsays[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]dopaas[.]com

- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]encoreapi[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]fastly-terrarium[.]com
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]faststacks[.]net
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]framer[.]website
- aaaabbbbccccsonounhostfakeidrotourdolomiti[.]googlecode[.]com