WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A Fake ID Marketplace under the DNS Lens

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

The concept of internationalization extends from the virtual to the physical realm. Many people wish to travel or even migrate to other countries at some point in their lives. Unfortunately, that's sometimes easier said than done given the many legal documents, including valid IDs, passports, and others required.

In the past, some wanna-be international travelers met unsavory characters in the real world to obtain fake IDs. Today, all that has become doable online. And due to the demand, many threat actors have put up their own online marketplaces.

WhoisXML API threat researcher Dancho Danchev recently uncovered an email address allegedly belonging to one such proprietor—noveltypro1@hotmail[.]com. Our cybersecurity research team trooped to the DNS to find out how extensive the operation could be.

Our indicator of compromise (IoC) expansion analysis jumping off the malicious email address led to the discovery of:

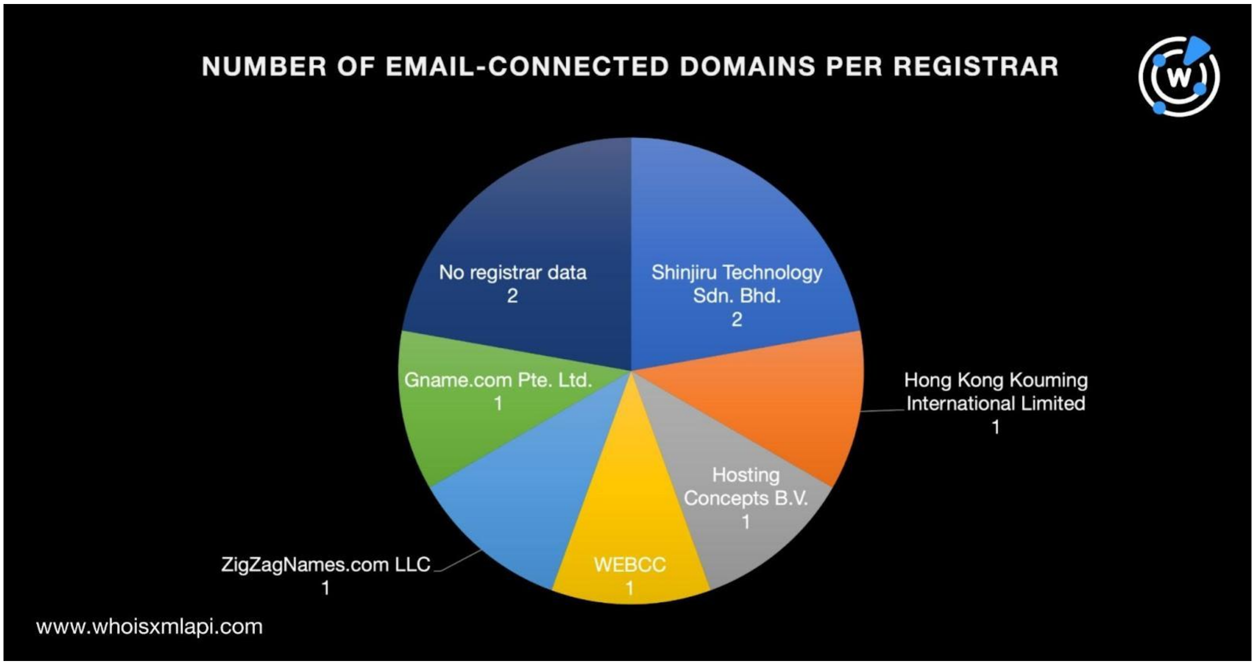
- Nine email-connected domains
- Seven IP addresses that played host to the email-connected domains
- One IP-connected domain
- 231 string-connected domains
- 777 string-connected subdomains

DNS Connections

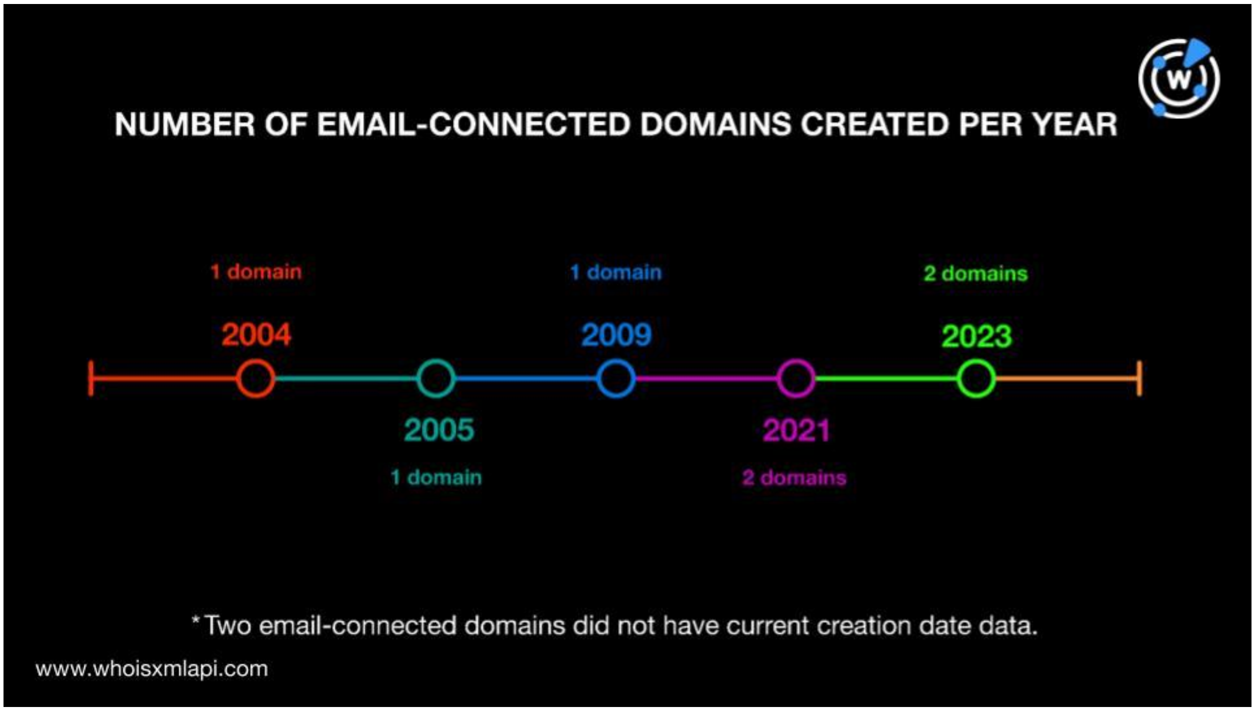
To determine the extent of the fake ID proprietor's network, we performed a WHOIS History Search for domains whose records contained the email address in their records. We uncovered nine such domains.

A bulk WHOIS lookup for the nine email-connected domains showed that:

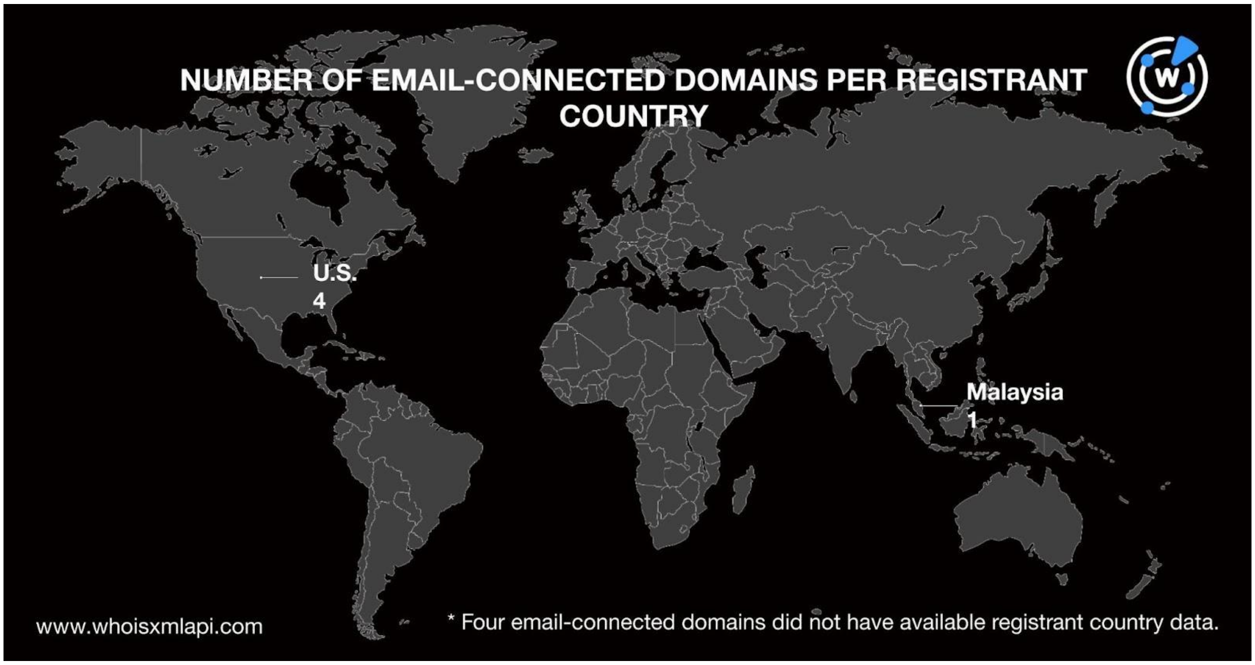
- Shinjiru Technology Sdn. Bhd. was the top registrar, accounting for two of the domains. Hong Kong Kouming International Limited, Hosting Concepts B.V., WEBCC, ZigZagNames.com LLC, and Gname.com Pte. Ltd. administered one domain each. The remaining two email-connected domains did not have public current registrar data.



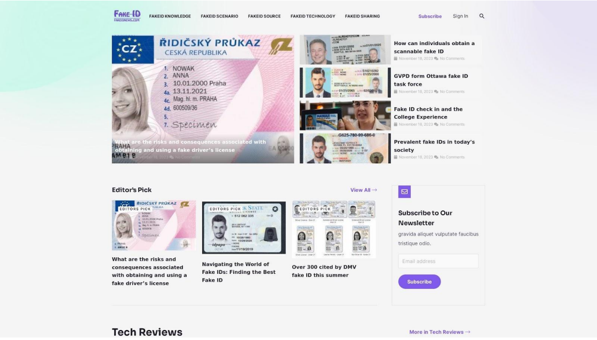
- While two of the email-connected domains did not have current creation dates, the remaining seven were created between 2004 and 2023.



- A majority of the email-connected domains, four to be exact, were registered in the U.S. One was registered in Malaysia. The remaining four did not have available registrant country data.


NUMBER OF EMAIL-CONNECTED DOMAINS PER REGISTRANT COUNTRY
U.S.
4
Malaysia
1
www.whoisxmlapi.com
* Four email-connected domains did not have available registrant country data.

While five of the email-connected domains were unreachable as of this writing based on screenshot lookups, three continued to host live content and one led to an error page.



What are the risks and consequences associated with obtaining and using a fake driver's license

How can individuals obtain a scannable fake ID
November 18, 2023 No Comments

GVPD form Ottawa fake ID task force
November 18, 2023 No Comments

Fake ID check in and the College Experience
November 18, 2023 No Comments

Prevalent fake IDs in today's society
November 18, 2023 No Comments

Editor's Pick

View All →

What are the risks and consequences associated with obtaining and using a fake driver's license

Navigating the World of Fake IDs: Finding the Best Fake ID

Over 300 cited by DMV fake ID this summer

Subscribe to Our Newsletter

gravida aliquet vulputate faucibus tristique odio.

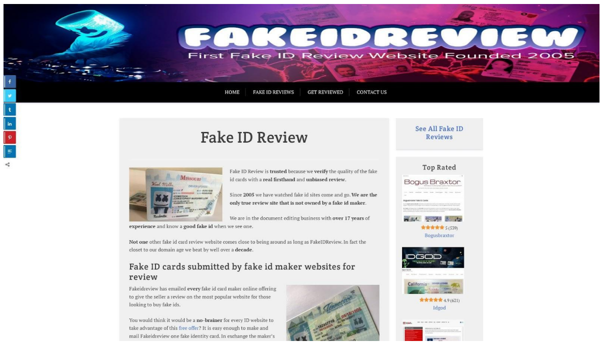
Email address

Subscribe

Tech Reviews

More in Tech Reviews →

Screenshot of email-connected domain fakeidnews[.]com



Fake ID Review

Fake ID Review is **trusted** because we **verify** the quality of the fake id cards with a **real firsthand** and **unbiased review**.

Since **2005** we have watched fake id sites come and go. **We are the only true review site that is not owned by a fake id maker**.

We are in the document editing business with **over 17 years** of **experience** and know a **good fake id** when we see one.

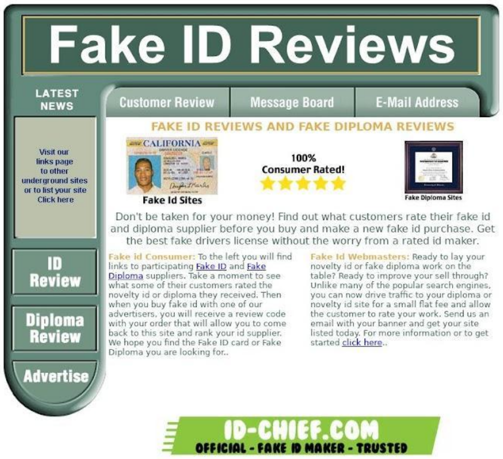
Not one other fake id card review website comes close to being around as long as FakeIDReview. In fact the closet to our domain age we beat by well over a **decade**.

Fake ID cards submitted by fake id maker websites for review

Fakeidreview has emailed **every** fake id card maker online offering to give the seller a review on the most popular website for those looking to buy fake ids.

You would think it would be a **no-brainer** for every ID website to take advantage of this free offer? It is easy enough to make and mail Fakeidreview one fake identity card. In exchange the maker's

Screenshot of email-connected domain fakeidreview[.]com



Visit our links page to other underground sites or to list your site Click here

FAKE ID REVIEWS AND FAKE DIPLOMA REVIEWS

Don't be taken for your money! Find out what customers rate their fake id and diploma supplier before you buy and make a new fake id purchase. Get the best fake drivers license without the worry from a rated id maker.

Fake id Consumer: To the left you will find links to participating Fake ID and Fake Diploma suppliers. Take a moment to see what some of their customers rated the novelty id or diploma they received. Then when you buy fake id with one of our advertisers, you will receive a review code with your order that will allow you to come back to this site and rank your id supplier. We hope you find the Fake ID card or Fake Diploma you are looking for..

Fake Id Webmasters: Ready to lay your novelty id or fake diploma work on the table? Ready to improve your sell through? Unlike many of the popular search engines, you can now drive traffic to your diploma or novelty id site for a small flat fee and allow the customer to rate your work. Send us an email with your banner and get your site listed today. For more information or to get started click here..

Screenshot of email-connected domain noveltyidsite[.]com

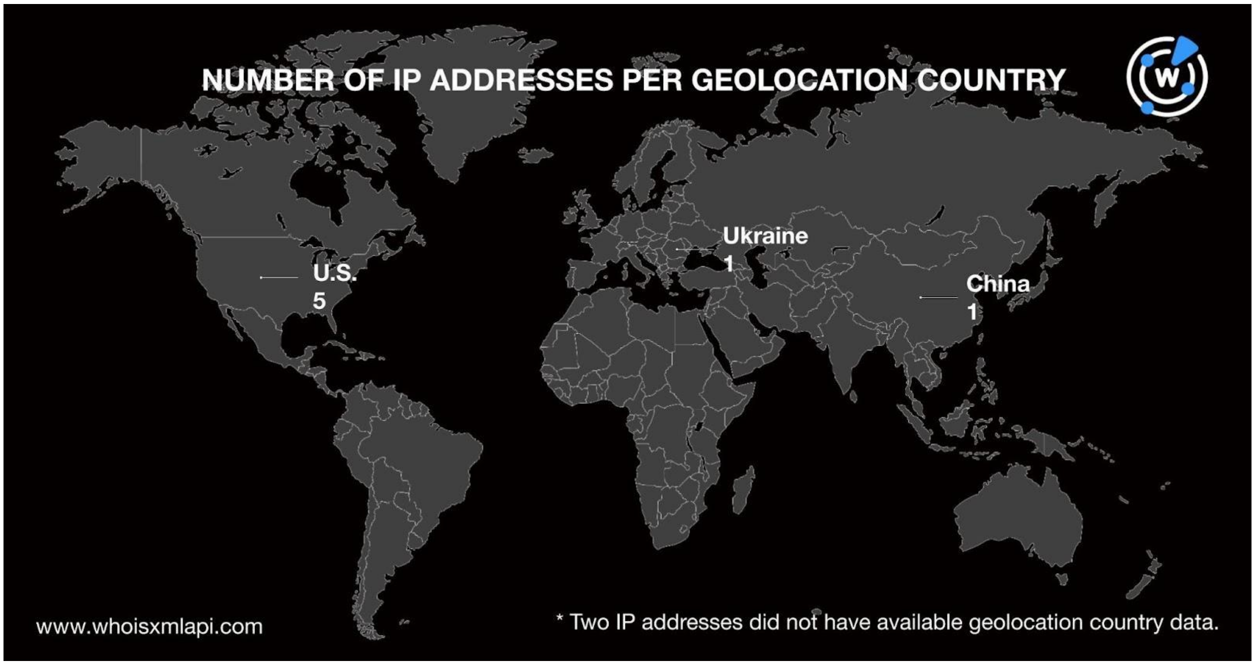
Based on their content, these three sites may offer fake IDs, even passports, licenses, and diplomas, to interested buyers.

Next, we subjected the email-connected domains to DNS lookups, which revealed that they resolved to seven unique IP addresses. Threat intelligence lookups for them yielded interesting findings about five of them. Take a look at the table below.

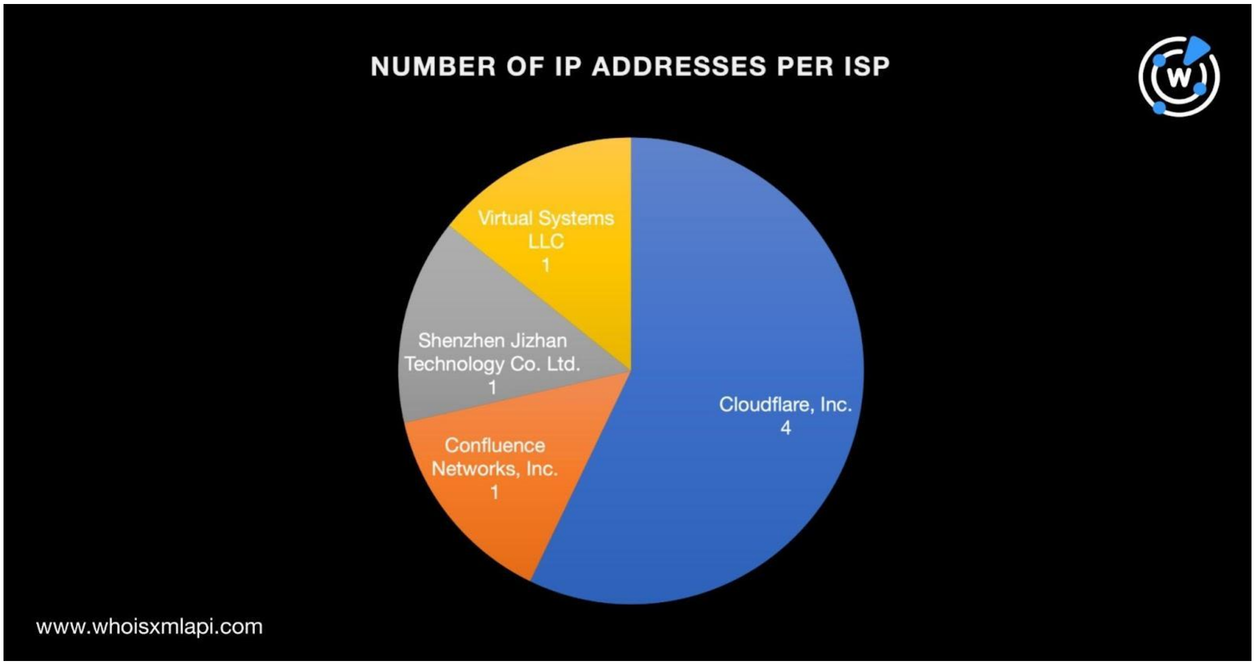
IP ADDRESS	THREAT TYPE CLASSIFICATION
172[.]67[.]148[.]80	Generic Phishing
208[.]91[.]197[.]46	Generic Phishing Malware Suspicious C&C
172[.]67[.]132[.]236	Generic Phishing Malware
104[.]21[.]29[.]28	Generic Phishing
104[.]21[.]13[.]182	Generic Phishing Malware

A bulk IP geolocation lookup for the seven IP addresses showed that:

- They were spread across three countries led by the U.S., which accounted for five IP addresses. One IP address each was geolocated in China and Ukraine.


NUMBER OF IP ADDRESSES PER GEOLOCATION COUNTRY
U.S.
5
Ukraine
1
China
1
www.whoisxmlapi.com
* Two IP addresses did not have available geolocation country data.

- The top Internet service provider (ISP) was Cloudflare, Inc., which accounted for four IP addresses. Virtual Systems LLC; Shenzhen Jizhan Technology Co. Ltd.; and Confluence Networks, Inc. each administered one of the three remaining IP addresses.



We then performed reverse IP lookups on the seven IP addresses and found that two of them were seemingly dedicated. They hosted three domains. After we removed duplicates and the email-connected domains, we were left with one IP-connected domain—handyman-joes[.]com.

Further scrutiny of the email-connected domains allowed us to identify six text strings that are likely to appear in fake ID-related web properties. We used them as Domains & Subdomains Discovery search terms to uncover other domains and subdomains created or added since 1 January 2023. Take a look at the detailed list in the table below. Note that the number of domains indicated still include those that have already been identified as email- and IP-connected.

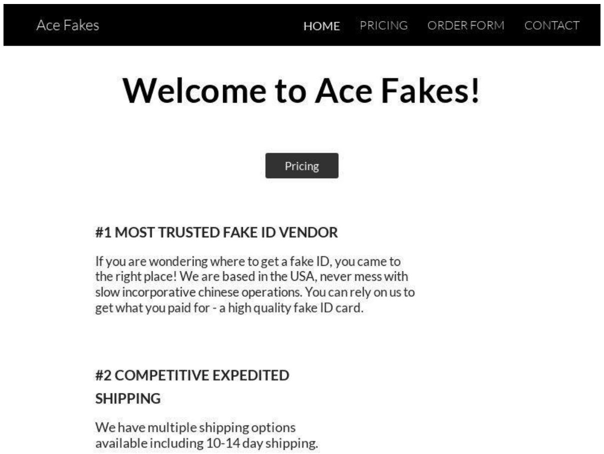
TEXT STRING	NUMBER OF STRING-CONNECTED DOMAINS	NUMBER OF STRING-CONNECTED SUBDOMAINS
cloneid	3	11
fakeid	195	685

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

After filtering the string-connected domain and subdomain lists to exclude duplicates and those that have already been tagged as either email- or IP-connected, we were left with 231 and 777 string-connected domains and subdomains, respectively.

A total of 522 string-connected web properties remained accessible to date—152 domains and 370 subdomains.

Based on their screenshots, 42 of the 152 string-connected domains did host sites that seemingly sold fake IDs or promoted them. Take a look at four examples below.



Welcome to Ace Fakes!

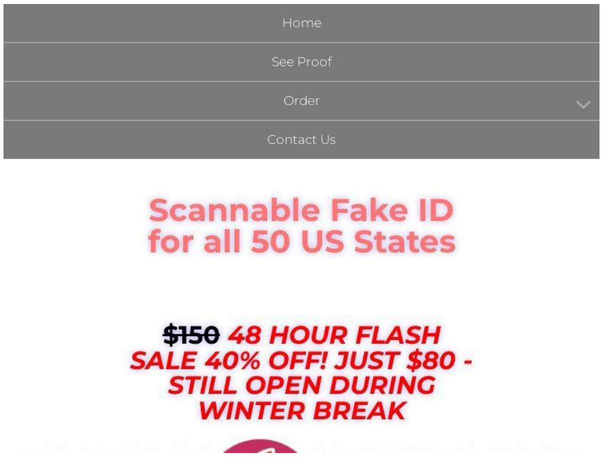
#1 MOST TRUSTED FAKE ID VENDOR

If you are wondering where to get a fake ID, you came to the right place! We are based in the USA, never mess with slow incorporative chinese operations. You can rely on us to get what you paid for - a high quality fake ID card.

#2 COMPETITIVE EXPEDITED SHIPPING

We have multiple shipping options available including 10-14 day shipping.

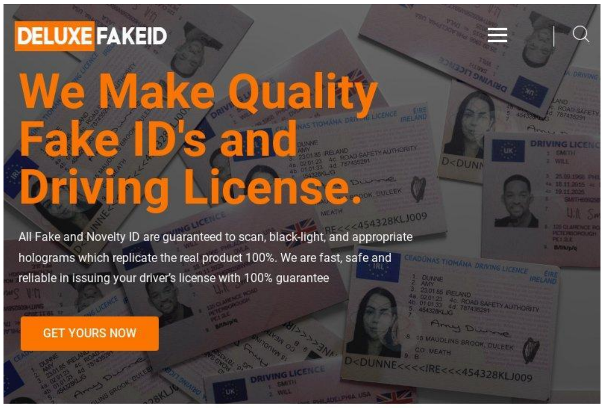
Screenshot of string-connected domain acefakeids[.]la



Scannable Fake ID for all 50 US States

~~$150~~ 48 HOUR FLASH SALE 40% OFF! JUST $80 - STILL OPEN DURING WINTER BREAK

Screenshot of string-connected domain bestfakeids[.]com



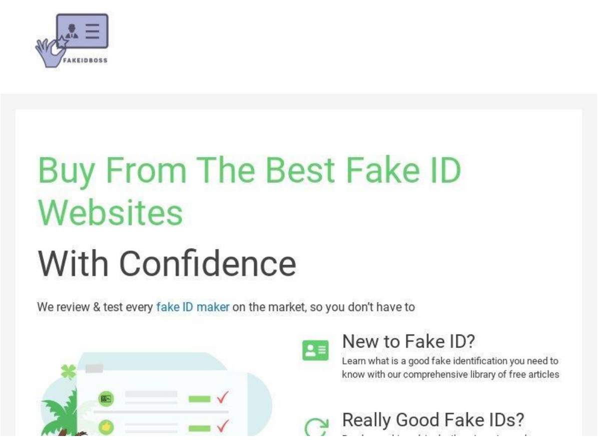
DELUXE FAKEID

We Make Quality Fake ID's and Driving License.

All Fake and Novelty ID are guaranteed to scan, black-light, and appropriate holograms which replicate the real product 100%. We are fast, safe and reliable in issuing your driver's license with 100% guarantee

GET YOURS NOW

Screenshot of string-connected domain deluxefakeid[.]com



FAKEIDBOSS

Buy From The Best Fake ID Websites

With Confidence

We review & test every fake ID maker on the market, so you don't have to

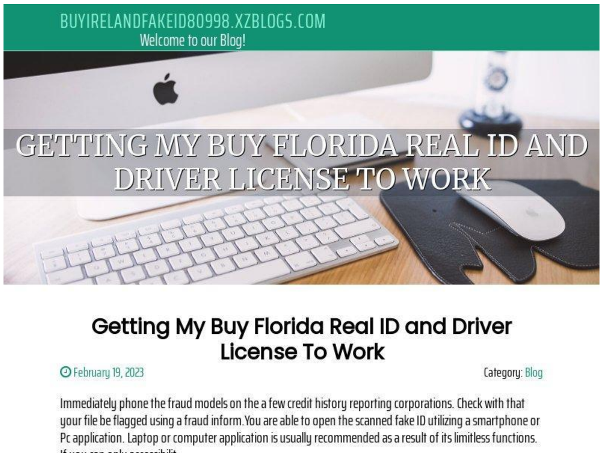
New to Fake ID?

Learn what is a good fake identification you need to know with our comprehensive library of free articles

Really Good Fake IDs?

Screenshot of string-connected domain fakeidboss[.]net

In addition, 24 of the string-connected subdomains also hosted pages that were seemingly related to the proliferation of fake ID usage. Certain of them also appear to fall under free blogging platform domains. Take a look at four examples below.



BUYIRELANDFAKEID80998.XZBLOGS.COM

Welcome to our Blog!

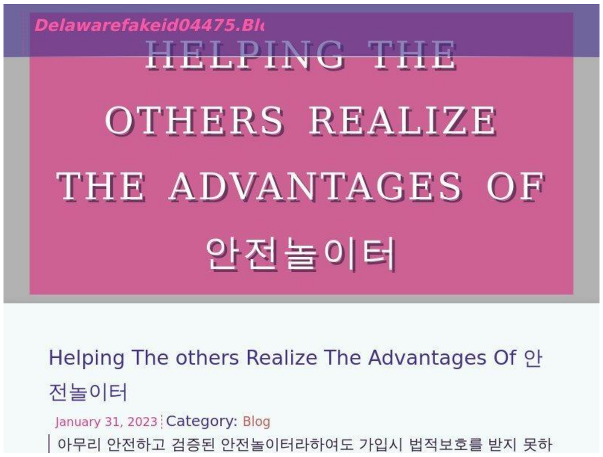
GETTING MY BUY FLORIDA REAL ID AND DRIVER LICENSE TO WORK

Getting My Buy Florida Real ID and Driver License To Work

February 19, 2023 Category: Blog

Immediately phone the fraud models on the a few credit history reporting corporations. Check with that your file be flagged using a fraud inform.You are able to open the scanned fake ID utilizing a smartphone or Pc application. Laptop or computer application is usually recommended as a result of its limitless functions. If you can only accessibilit

Screenshot of string-connected subdomain buyirelandfakeid80998[.]xzblogs[.]com



Delawarefakeid04475.Bl

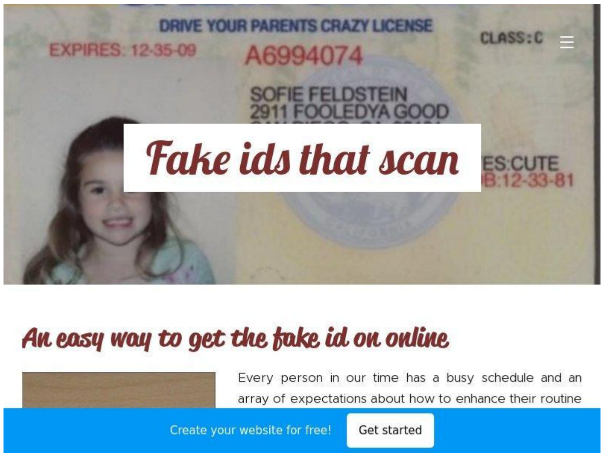
HELPING THE OTHERS REALIZE THE ADVANTAGES OF 안전놀이터

Helping The others Realize The Advantages Of 안전놀이터

January 31, 2023 Category: Blog

아무리 안전하고 검증된 안전놀이터라하여도 가입시 법적보호를 받지 못하

Screenshot of string-connected subdomain delawarefakeid04475[.]bloggerswise[.]com



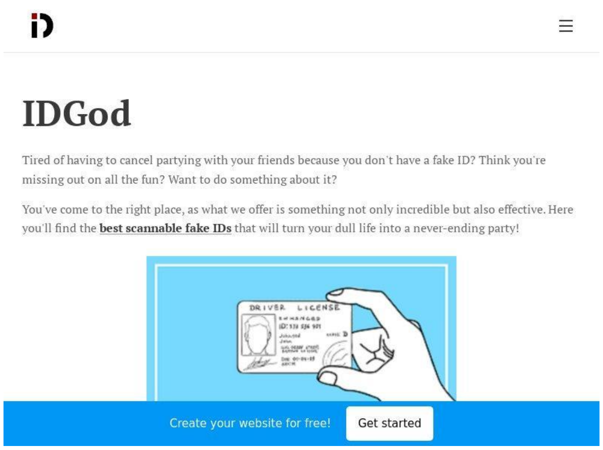
Fake ids that scan

An easy way to get the fake id on online

Every person in our time has a busy schedule and an array of expectations about how to enhance their routine

Create your website for free! Get started

Screenshot of string-connected subdomain fakeidsthatscan[.]webnode[.]page



IDGod

Tired of having to cancel partying with your friends because you don't have a fake ID? Think you're missing out on all the fun? Want to do something about it?

You've come to the right place, as what we offer is something not only incredible but also effective. Here you'll find the **best scannable fake IDs** that will turn your dull life into a never-ending party!

Create your website for free! Get started

Screenshot of string-connected subdomain scannablefakeid[.]webnode[.]page

—

Our in-depth analysis of the sole email address belonging to a fake ID peddler led to the discovery of 17 web properties—nine email-connected domains, seven IP addresses, and one IP-connected domain—that could be part of the same malicious infrastructure. We also found 522 domains and subdomains that could belong to fellow fake ID sellers.

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 and IoCs

Email Address Identified as an IoC

- noveltypro1@hotmail[.]com

Sample Email-Connected Domains

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

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

Sample IP Addresses

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

Sample Malicious IP Addresses

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

IP-Connected Domain

- handyman-joes[.]com

Sample String-Connected Domains

- 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

Sample String-Connected Subdomains

- 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[.]jj[.]scaleforce[.]com[.]cy
- aaaabbbbccccsonounhostfakeidrotour[.]jj[.]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