

# Unmasking Global DNS

Exposing massive badness on the surface

**Ed Gibbs, Field CTO**

BC Membership Meeting

ICANN 77 - June 13, 2023

Washington D.C.



**WhoisXMLAPI**

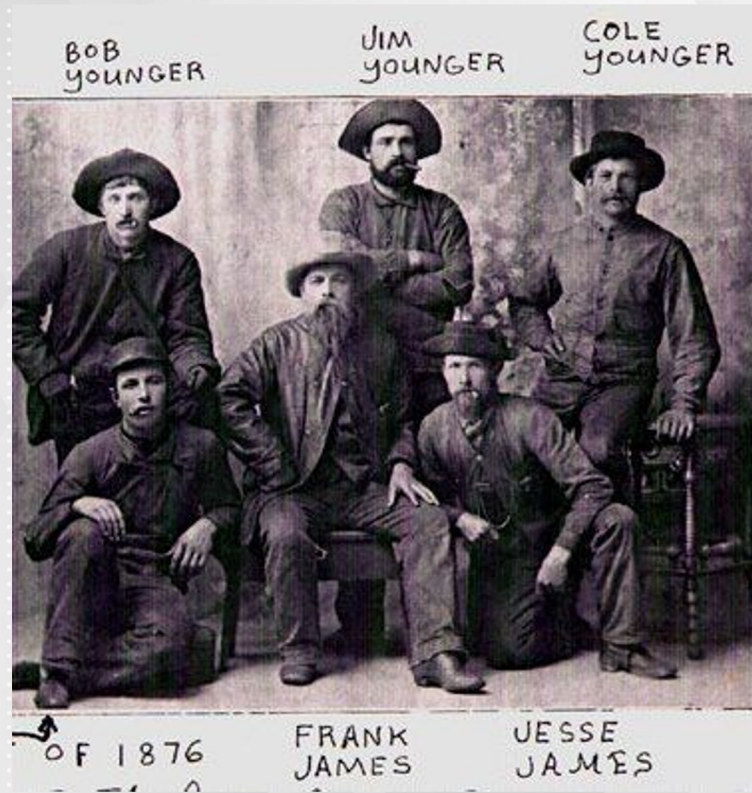
The Who Behind Domain, IP & Cyber Threat Intelligence

# Ed Gibbs Bio

- Current: Field CTO, WHOIS API, Inc. WHOISXMLAPI.COM
- 30+ Years Experience
- Noteworthy:
  - Co-Author: *“Handbook of Computer Crime Investigation”*
  - Volunteer: National Child Protection Task Force (NCPTF)
  - Board Member: Public International Cybercrime Disruption Organization (picdo.org)
  - Closely aligned with various law-enforcement and government agencies

# Agenda

1. Too much DNS freedom to misbehave
2. Techniques to find badness
3. Dig, un-dig, and re-dig
4. Necessity to monitor
5. Bringing it all together



# Too Much Room to Misbehave

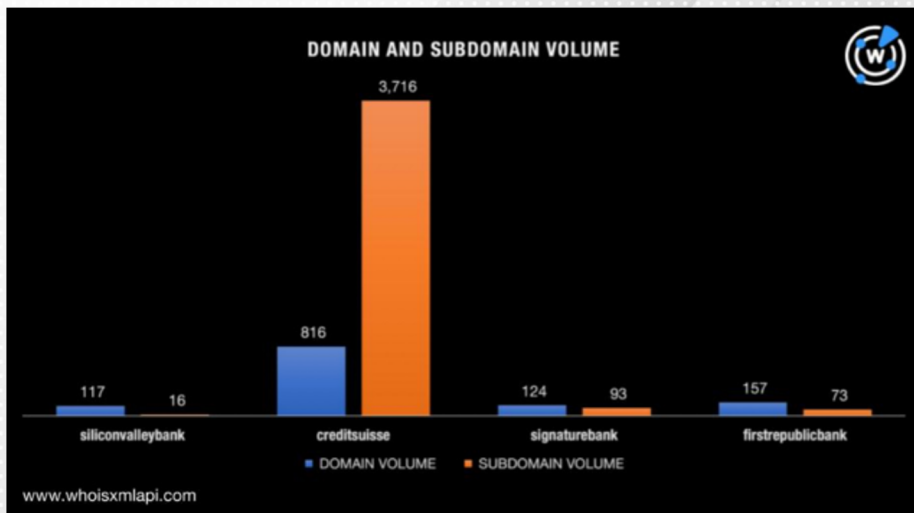
## Child Sexual Abuse Material (CSAM), Pig Butcher Farms are all on the rise in 2023

- CSAM migrating to the left of the root/tld
- PBFs: 10,000 domains registered in one day, identified as an “organized crime” group
  - Commonly used to masquerade, action, or weaponize as Casinos, Banks, Crypto, Crypto-Recovery for example
  - 1000’s of bulk registered domains being detected every month, most go undetected. Security products continue to miss majority.
    - *“15% of the time, it works 100% of the time”*
- Older domains evade reputation system, avoid newly registered domain detection
- Abusive domains often have no MX, AAAA, DNSSEC, very low CNAME and subdomains. Recent study conducted of 250,000 bulk registered domains (>20) in February, 99.7% met this criteria

# Too Much Room to Misbehave

How financial institutions were reflected in DNS after several bank crashes (March 2023)

- A total of 3,902 subdomains contained the bank names
- SVB only owned 21 of the 117 domains names
- Credit Suisse 51 of the 816 domain names
- Signature Bank, 15 of the 124 domains
- Hundreds of derivative names popped up as a result, such as:
  - Bankcollapse
  - Bankalert
  - Bankudpate
  - FDIC + recover
  - Additional Bank Names
- A mass analysis of these domains were privacy shielded, and leveraged CloudFlare
- Current events are indeed reflected in DNS



# Too Much Room to Misbehave

## March 10, 2023 - "International Law Enforcement Takes Down Infamous NetWire Cross-Platform RAT"

```

> worldwiredlabs.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: worldwiredlabs.com
Address: 66.212.148.115

> set type=ns
> worldwiredlabs.com
Server: dns.google
Address: 8.8.8.8

(root)
primary name server = ns1.seizedservers.com
responsible mail addr = hostmaster.seizedservers.com
serial = 8
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 604800 (7 days)
default TTL = 86400 (1 day)
  
```

Basic search    Advanced search

---

Search where

Anywhere ?     In specific WHOIS fields ?

Search term(s)

Name Server    Contains a word ?    **seizedservers.com**     Include

And/Or term ?

**1,537 domain(s)** having your specific search terms in their WHOIS records found

- |                      |                          |                           |
|----------------------|--------------------------|---------------------------|
| ganged.network >     | worldwiredlabs.com >     | cracker.com >             |
| mordematx.com >      | paxforex.com >           | mp3teca.ws >              |
| backpage.ca >        | backpage-insider.com >   | backpage.co.uk >          |
| backpage.net >       | backpage.us >            | viagrageneric.eu >        |
| miami24k.com >       | flowactivo.co >          | corourbanos.com >         |
| beatsbydrekenop.be > | vn1lib.org >             | miami.gift >              |
| blackjob.biz >       | direct-kamagra.eu >      | b-ok.global >             |
| eurodrugstore.eu >   | safepills-pharmacy.com > | alledpills.net >          |
| realtimberland.com > | n1lib.org >              | louisvuittonhandbags.eu > |
| hubertushaz.eu >     | lizardlabs.eu >          | koendearoote.eu >         |



# Too Much Room to Misbehave

Cybersquatting domains and subdomains get launched following major news event or anticipated market releases, often with dubious content

Tech market releases	Strings & connected domains
Valve Steam Deck	steam + deck - 325 domains, 91 subdomains
Rivian R1T	rivian + r1t - 20 domains, 2 subdomains
Meta Quest 3	meta + quest3 - 8 domains
Apple iPhone 14	iphone14 - 690 domains, 234 subdomains
Google Pixel Watch	pixel + watch - 98 domains
Apple AR Glasses	apple + arglasses - 7 domains
Chevy Silverado E	chevy + silveradoe - 7 domains

iphone14promax.pages.dev website screenshot on March 10, 2023

If this site is or  
 This site was built with GroveFunnel

# iPhone 14

Claim Now



iPhone 14  
 Welcome to the iPhone giveaway  
 Claim iPhone >

Source: <https://circleid.com/posts/20221121-the-business-of-cybercrime-does-malicious-campaign-planning-take-as-long-as-legitimate-marketing-campaign-planning>

# Techniques to Find Badness

## CASE STUDY: Fake Fashion

- Research strings were “armani” “burberry” “cartier” “gucci” “hermes” “louisvuitton” “prada” “rolex” and “versace”.
- For those strings, we found 2,504 domains between January 1 - March 27, 2022.
- Looking at bulk registration events in the past 18 months, we found an additional 540 domains broken down into 88 clusters.





# Clusters of Badness

DOMAIN	TOTAL_NO_OF_GRP_MEMBERS	REGISTRANT_COUNTRY
sc72020.icu	9017	CHINA
kyty1154.com	8836	NULL
5852019.icu	8407	CHINA
jq12021.icu	8035	CHINA
yaxin419.vip	3974	UNITED STATES
kycp686.vip	3582	UNITED STATES
zhongo571.vip	3463	UNITED STATES
kyun756.vip	3037	UNITED STATES
zovip750.com	2986	NULL
obet6856.com	2975	UNITED STATES

DOMAIN	TOTAL_NO_OF_GRP_MEMBERS	REGISTRANT_COUNTRY
holiganbet1777.com	988	NULL
2305bobty.com	855	UNITED STATES
1656bobty.com	524	UNITED STATES
moneyeasily-vgf.top	423	UNITED STATES
money-easilyvtu.buzz	400	UNITED STATES
bluenbuss.info	202	UNITED STATES
wujitv115.top	199	PHILIPPINES
wujizhibo65.com	198	UNITED STATES
wutuzhibo51.org	198	UNITED STATES
wututv78.top	197	PHILIPPINES

TOTAL_NO_OF_GRP_MEMBERS	DOMAIN
13358	6222goubo.com
13358	184gobo.com
13358	6366goubo.com
13358	2208goubo.com
13358	4139goubo.com
13358	8679goubo.com
13358	5623goubo.com
13358	9280goubo.com
13358	3470goubo.com
13358	8496goubo.com
13358	4966goubo.com
13358	391gobo.com
13358	7893goubo.com
13358	1758goubo.com
13358	4686goubo.com
13358	1380goubo.com
13358	2185gobo.com
13358	467goubo.vip
13358	1906goubo.com
13358	1731gobo.com
13358	5554goubo.com
13358	7197goubo.com
13358	9361goubo.com
13358	766gobo.com
13358	664gobo.com

# Techniques to Find Badness

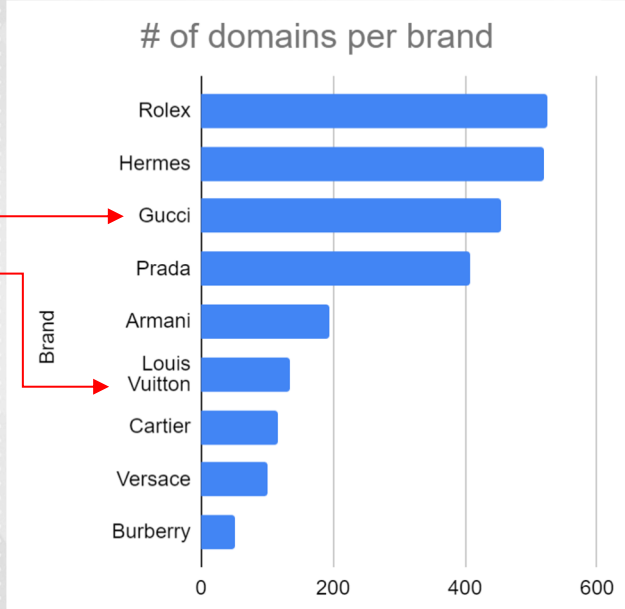
- **CASE STUDY:** Gather domain names for strings of interest.

465 domain(s) having your specific search terms found

gucci-supergucci.com >	gucci2.ws >
guccik.tk >	guccibagsguccishoes.ws >
lvgucci.tw >	guccims.tk >
gucci4.net >	guccivr.co >
guccile.xn--flqs8s >	gucci9.info >
gucci6.info >	guccidev.us >
guccilv.fun >	degucci.net >
gucci.pp.ua >	gucci76.vip >
guccil.live >	lvgucci.vip >
gucci76.com >	gucci3.info >
mrgucci.one >	gucci2.info >
gucci2me.ws >	gucci7.info >
gucci76.net >	migucci.com >
dfs-gucci.cn >	webgucci.com >
guccigirl.ws >	guccibtc.com >
guccisafe.ws >	guccihome.it >

137 domain(s) having your specific search terms found

louisvuittonlouisvuittonl... >	louisvuitton.mk >
louisvuittonvr.co >	louisvuitton9.com >
louisvuittonxw.com >	louisvuittonbag.co >
louisvuitton-p.top >	louisvuittongs.com >
llouisvuitton.site >	louisvuittonuk6.com >
louisvuittondao.com >	louisvuitton-pa.top >
louisvuittonstw.com >	louisvuitton-us.top >

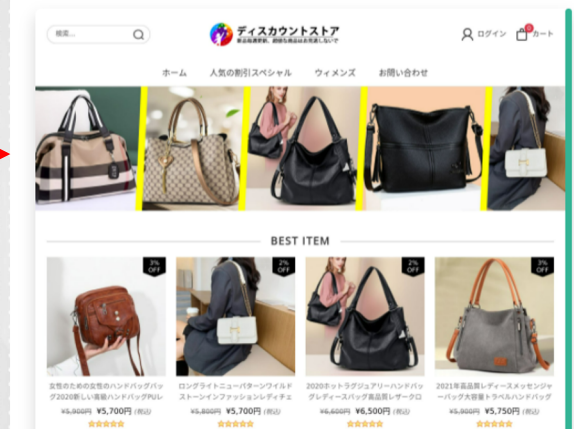


# Techniques to Find Badness

- **CASE STUDY:** Track typosquatting groups and bulk-registered domains with live content.

date	group_number	group_member	total_no_of_grp	domain
2021-05-09	627	1	3	hot-rolex.site
2021-05-09	627	2	3	hot-rolex.shop
2021-05-09	627	3	3	hot-rolex.xyz
2021-05-09	893	1	3	watch-rolex.shop
2021-05-09	893	2	3	watch-rolex.site
2021-05-09	893	3	3	watch-rolex.xyz
2021-05-09	1271	1	4	watches-rolex.xyz
2021-05-09	1271	2	4	watches-rolex.site
2021-05-09	1271	3	4	watches-rolex.shop
2021-05-09	1271	4	4	watches-rolex.top
2021-06-29	130	1	3	tokyolouisvuitton.com
2021-06-29	130	2	3	tokyolouisvuitton.space
2021-06-29	130	3	3	tokyolouisvuitton.xyz

tokyolouisvuitton.com website screenshot



# Dig, Un-dig and Re-Dig

- **CASE STUDY:** Are there major inconsistencies in WHOIS records?

WHOIS record for [prada.com](#)

## Domain age

Created Date: June 9, 1997 04:00:00 UTC  
 Updated Date: June 17, 2020 07:27:43 UTC  
 Expires Date: June 8, 2022 04:00:00 UTC  
 Estimated Domain Age: 9059 day(s)

## Registrar Name

BARBERO & Associates Ltd >

## WHOIS Server

[whois.barbero.co.uk](#) >

## Name Servers

[pete.ns.cloudflare.com](#) >  
[brenda.ns.cloudflare.com](#) >

## Registrant Contact

Registrant Name: Murielle Vincenti >  
 Registrant Organization: PRADA S.A. >  
 Registrant Street1: 23, Rue Aldringen >  
 Registrant City: Luxembourg >  
 Registrant State/Province: LU >  
 Registrant Postal Code: 1118 >  
 Registrant Country: LUXEMBOURG >  
 Registrant Email: [domains@prada.com](mailto:domains@prada.com) >  
 Registrant Phone: 3522626361 >  
 Registrant Fax: 3522622636 >

domainName	registrantName	standardRegCreatedDate	registrant_state	registrant_country
prada-chile.com	ALIBABA.COM SINGAPORE	2022-03-21 12:45:16 UTC	Kuala Lumpur	MALAYSIA
prada-danmark.com	ALIBABA.COM SINGAPORE	2022-03-24 05:04:25 UTC	Kuala Lumpur	MALAYSIA
prada-greece.com	ALIBABA.COM SINGAPORE	2022-03-24 05:17:37 UTC	Kuala Lumpur	MALAYSIA
prada-hungary.com	ALIBABA.COM SINGAPORE	2022-03-24 05:15:02 UTC	Kuala Lumpur	MALAYSIA
prada-portugal.com	ALIBABA.COM SINGAPORE	2022-03-24 04:52:06 UTC	Kuala Lumpur	MALAYSIA
prada-nederland.com	ALIBABA.COM SINGAPORE	2022-03-24 04:59:47 UTC	Kuala Lumpur	MALAYSIA
prada-schweiz.com	ALIBABA.COM SINGAPORE	2022-03-24 02:25:12 UTC	Kuala Lumpur	MALAYSIA
prada-spain.com	ALIBABA.COM SINGAPORE	2022-03-24 02:20:26 UTC	Kuala Lumpur	MALAYSIA
prada-suomi.com	ALIBABA.COM SINGAPORE	2022-03-24 04:41:28 UTC	Kuala Lumpur	MALAYSIA
prada-sverige.com	ALIBABA.COM SINGAPORE	2022-03-24 04:32:53 UTC	Kuala Lumpur	MALAYSIA
prada-turkey.com	ALIBABA.COM SINGAPORE	2022-03-24 04:47:31 UTC	Kuala Lumpur	MALAYSIA
pradaaustraliafactory.com	ALIBABA.COM SINGAPORE	2022-03-17 02:40:09 UTC	Kuala Lumpur	MALAYSIA
pradabelgium.com	ALIBABA.COM SINGAPORE	2022-03-24 04:56:23 UTC	Kuala Lumpur	MALAYSIA
pradacanadafactory.com	ALIBABA.COM SINGAPORE	2022-03-17 02:35:25 UTC	Kuala Lumpur	MALAYSIA
pradagermany.com	ALIBABA.COM SINGAPORE	2022-03-17 04:03:27 UTC	Kuala Lumpur	MALAYSIA
pradaireland.com	ALIBABA.COM SINGAPORE	2022-03-17 02:49:48 UTC	Kuala Lumpur	MALAYSIA
pradaindonesia.com	ALIBABA.COM SINGAPORE	2022-03-17 03:07:33 UTC	Kuala Lumpur	MALAYSIA
pradamalaysiaoutlet.com	ALIBABA.COM SINGAPORE	2022-03-17 02:57:11 UTC	Kuala Lumpur	MALAYSIA
pradaoutletfactoryshop.com	ALIBABA.COM SINGAPORE	2022-03-17 02:27:35 UTC	Kuala Lumpur	MALAYSIA
pradaphilippines.com	ALIBABA.COM SINGAPORE	2022-03-17 03:00:21 UTC	Kuala Lumpur	MALAYSIA
pradanorge.com	ALIBABA.COM SINGAPORE	2022-03-24 05:07:24 UTC	Kuala Lumpur	MALAYSIA
pradasingaporeoutlet.com	ALIBABA.COM SINGAPORE	2022-03-17 02:53:51 UTC	Kuala Lumpur	MALAYSIA
pradauae.com	ALIBABA.COM SINGAPORE	2022-03-17 03:27:06 UTC	Kuala Lumpur	MALAYSIA
pradaukfactory.com	ALIBABA.COM SINGAPORE	2022-03-17 03:39:02 UTC	Kuala Lumpur	MALAYSIA
pradausaonlinestore.com	ALIBABA.COM SINGAPORE	2022-03-17 02:30:20 UTC	Kuala Lumpur	MALAYSIA
tiendapradamexico.com	ALIBABA.COM SINGAPORE	2022-03-21 12:39:58 UTC	Kuala Lumpur	MALAYSIA

# Dig, Un-dig and Re-Dig

- **CASE STUDY:** Are websites live? What contents are hosted there?

pradausaonlinestore.com categories



Categories

- **Tier 1 category:** **Style & Fashion** (ID: IAB-552, Confidence: 0.985)
- **Tier 2 category:** **Women's Accessories** (ID: IAB-561, Confidence: 0.698)
- **Tier 2 category:** **Women's Clothing** (ID: IAB-566, Confidence: 0.667)
- **Tier 2 category:** **Men's Clothing** (ID: IAB-582, Confidence: 0.630)
- **Tier 2 category:** **Women's Shoes and Footwear** (ID: IAB-573, Confidence: 0.630)
- **Tier 2 category:** **Men's Shoes and Footwear** (ID: IAB-589, Confidence: 0.560)

prada.com categories



Categories

- **Tier 1 category:** **Style & Fashion** (ID: IAB-552, Confidence: 0.993)
- **Tier 2 category:** **Women's Clothing** (ID: IAB-566, Confidence: 0.621)
- **Tier 2 category:** **Women's Accessories** (ID: IAB-561, Confidence: 0.617)
- **Tier 2 category:** **Women's Shoes and Footwear** (ID: IAB-573, Confidence: 0.610)
- **Tier 2 category:** **Children's Clothing** (ID: IAB-575, Confidence: 0.598)

# Dig, Un-dig and Re-Dig

- **CASE STUDY:** Hosted or shared DNS / IP infrastructure? What are the links between a target domain and connected domains?

Term	Resolved IP	Domains
prada-chile.com	196.196.38.101	cpanel.eccocanadasale.com, cpcalendar.eccocanadasale.com, cpcontacts.eccocanadasale.com, eccocanadasale.com, hellyhansenchile.com
prada-danmark.com	196.245.152.132	lululemondanmark.com, lululemonnorge.com, occhiali-da-sole-2020.it
prada-greece.com	196.196.38.75	brooksshoesfactoryoutlet.us, inov8italia.it, kedsshoesmy.com, olukai-italia.com, tevasandalsportugal.com
prada-hungary.com	196.245.161.242	conversehungaryoutlet.com
prada-portugal.com	196.196.38.125	eccooutletsklepinternetowy.com, hellyhansenoutletuk.com, inov8ireland.com, lululemonfactoryoutlet.us, vionicsshoesoutletuk.com
prada-nederland.com	196.196.38.76	inov-8jp.com, keds-mexico.com, nintendoswitchsingapore.com, olukaisouthafrica.co.za, sperryonlinestore.com
prada-schweiz.com	196.196.38.69	australianbootsblundstone.com, blundstoneworkboots.com, hostmaster.olukaiukoutlet.com, kedscolombia.com, olukaiukoutlet.com
prada-spain.com	196.245.57.170	botasdemonia.es, lululemonspain.es, tiendademoniashoes.com
prada-suomi.com	196.196.38.113	brooks-hardloopschoenen.com, cpanel.salomonsuomi.com, cpcalendar.salomonsuomi.com, cpcontacts.salomonsuomi.com, inov8shoesaustralia.com
prada-turkey.com	196.196.38.96	ecco-malaysia.com, eccooutletportugal.com, lululemonnz.com, salomonskoooutlet.com, www.ecco-malaysia.com
pradabelgium.com	196.196.38.105	brooksfactoryoutletssydney.com, hellyhansenromania.com, levisfarmerek.com, lululemonmalaysia.com, salomonskleponline.com

# Dig, Un-dig and Re-Dig

- CASE STUDY:** What are the WHOIS History breadcrumbs of counterfeiting sites?

Historical WHOIS record(s) for **guccibelts.com**

2,587 Change(s) detected

9 Different domain owner(s)

4,028 Day(s) of tracking the domain

WHOIS record on **March 28, 2022**

Registrant Name: **Domain Manager** >  
 Registrant Organization: **Guccio Gucci S.p.A.** >  
 Registrant Street: **Via Tornabuoni 73/R** >  
 Registrant City: **Firenze** >  
 Registrant State/Province: **FI** >  
 Registrant Postal Code: **50123** >  
 Registrant Country: **ITALY** >  
 Registrant Email: **gucci@barbero.domains** >  
 Registrant Phone: **39055759221** >

WHOIS record on **January 2, 2018**

Registrant Contact  
 Registrant Name: **Fuze9 Web** >  
 Registrant Organization: **Fuze9 Web** >  
 Registrant Street: **Calle San Lucas, 7** >  
 Registrant City: **Fuengirola** >  
 Registrant State/Province: **Malaga** >  
 Registrant Postal Code: **29640** >  
 Registrant Country: **SPAIN** >  
 Registrant Email: **fuze9web@gmail.com** >  
 Registrant Phone: **34672846895** >

WHOIS record on **March 14, 2017**

Registrant Contact  
 Registrant Name: **JEFF RANDALL** >  
 Registrant Organization: **---**  
 Registrant Street: **CASA 35|CALLE AMELIA DENIS DE ICAZA** >  
 Registrant City: **PANAMA** >  
 Registrant State/Province: **PA** >  
 Registrant Postal Code: **00000** >  
 Registrant Country: **PANAMA** >  
 Registrant Email: **ROCKET@LTDCO.US** >

14 domain(s) having **Fuze9 Web** in their WHOIS records

securicor.net >      canuckiptv.com >  
 magtvboxes.com >      iptvscene.com >

214 domain(s) having **JEFF RANDALL** in their WHOIS records found

sandrospequeros.com >      ratcutlery.com >      gravelroadmusic.com >  
 awaeng.com >      awaengineering.com >      awagreatbasin.com >

# Monitor Clues, Get Evidence

- **CASE STUDY:** Dozens of domains containing luxury fashion brand names are registered daily.

Change(s) by date ↓

Monitor changes on **June 15, 2022** ↑

Date	Domains added	Domains dropped
<b>Jun 15, 2022</b>	<b>19</b>	<b>9</b>
Jun 14, 2022		
Jun 13, 2022		
Jun 12, 2022		
Jun 11, 2022		
Jun 10, 2022		
Jun 09, 2022		
Jun 08, 2022		
Jun 07, 2022		
Jun 06, 2022		

Domains added: 19

- doperolexs.com >
- rollforarolex.com >
- kontrolexpro.store >
- sellmyrolex.shop >
- rolexwatchrepair.shop >
- aerocontrolex.site >
- jamrolexxx.my.id >
- myrolex.vn >
- avfrolexacwin.ga >
- clerolexapfo.gq >

Show more ...

Domains dropped: 9

- rolexlogistics.site >
- rolexustoken.com >
- afrolex.gr >
- verolex.net >
- rolexklockor.se >
- rolexkopiop.se >
- rolexmentorprotege.se >
- rolexshop.co >
- comprolex.com >





**Bringing It All Together**

# Bringing It All Together

## Getting a grasp of the DNS involves asking many questions.

- What domains added within the past hour hints at cybercrime and illegitimate activities?
- What other domains share the same current or historical WHOIS information as suspicious domains?
- What other domains share the same IP address(es)?
- What organization owns the IP range to which the malicious IP address belongs?
- What content do the domains host based on screenshot analyses?
- For domains that don't have content yet, are there WHOIS or DNS data changes indicating they are being mobilized?
- What websites are classified under suspicious categories of the Internet Advertising Bureau (IAB)?
- What mail server did a suspicious email domain use? What other email domains share the MX record?
- Is the suspicious subdomain part of a legitimate company's infrastructure?
- Who issued the malicious websites' SSL certificates? What other clues can you obtain from their SSL certificate chains?



# Bringing It All Together

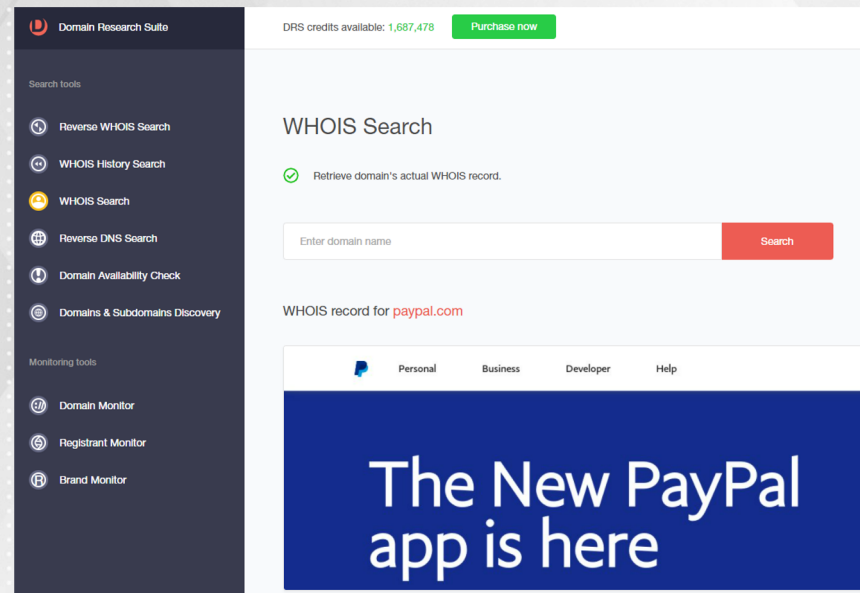
Not everything is visible to traditional badness detection engines

domain	warningDetails (day 1, July 12)	warningDetails (day 2, July 13)	warningDetails (day 4, July 15)	warningDetails (day 13, July 24)
a-stars-best.buzz				
d-stars-best.buzz				
c-stars-best.buzz				
e-stars-best.buzz				
b-stars-best.buzz				
paypal-ticketid158.com	Listed on Google Safe	Listed on Google Safe	Listed on Virus Total	Listed on Google Safe
paypal-ticketid173.com	Listed on Google Safe	Listed on Google Safe	Listed on Virus Total	Listed on Google Safe
paypal-ticketid174.com			Listed on Virus Total	Listed on Virus Total
paypal-ticketid186.com	Listed on Google Safe	Listed on Google Safe	Listed on Google Safe	Listed on Google Safe
paypal-ticketid183.com	→			
paypal-ticketid178.com	→			Listed on Virus Total
paypal-ticketid179.com	→			
paypal-ticketid185.com	Listed on Virus Total	Listed on Google Safe	Listed on Google Safe	Listed on Google Safe
mydormstuff.shop				
mydormstuff.info				

??

# Bringing It All Together

- For more information, contact [ed.gibbs@whoisxmlapi.com](mailto:ed.gibbs@whoisxmlapi.com)
- Free trial available on [www.whoisxmlapi.com](http://www.whoisxmlapi.com)



The screenshot displays the 'Domain Research Suite' interface. On the left is a dark sidebar with navigation options under 'Search tools' (Reverse WHOIS Search, WHOIS History Search, WHOIS Search, Reverse DNS Search, Domain Availability Check, Domains & Subdomains Discovery) and 'Monitoring tools' (Domain Monitor, Registrant Monitor, Brand Monitor). The main content area shows 'DRS credits available: 1,687,478' and a 'Purchase now' button. Below this is the 'WHOIS Search' section with a green checkmark and the text 'Retrieve domain's actual WHOIS record.' A search input field contains 'paypal.com' and a red 'Search' button. The results show the 'WHOIS record for paypal.com' with a navigation bar for 'Personal', 'Business', 'Developer', and 'Help'. A large blue banner at the bottom of the results area reads 'The New PayPal app is here'.



**Thank you.**

**Any questions?**

**[ed.gibbs@whoisxmlapi.com](mailto:ed.gibbs@whoisxmlapi.com)**