Domain Impersonation Vulnerabilities in TLS Ecosystem

Himanshu Goyal, Samina Shiraj Mulani

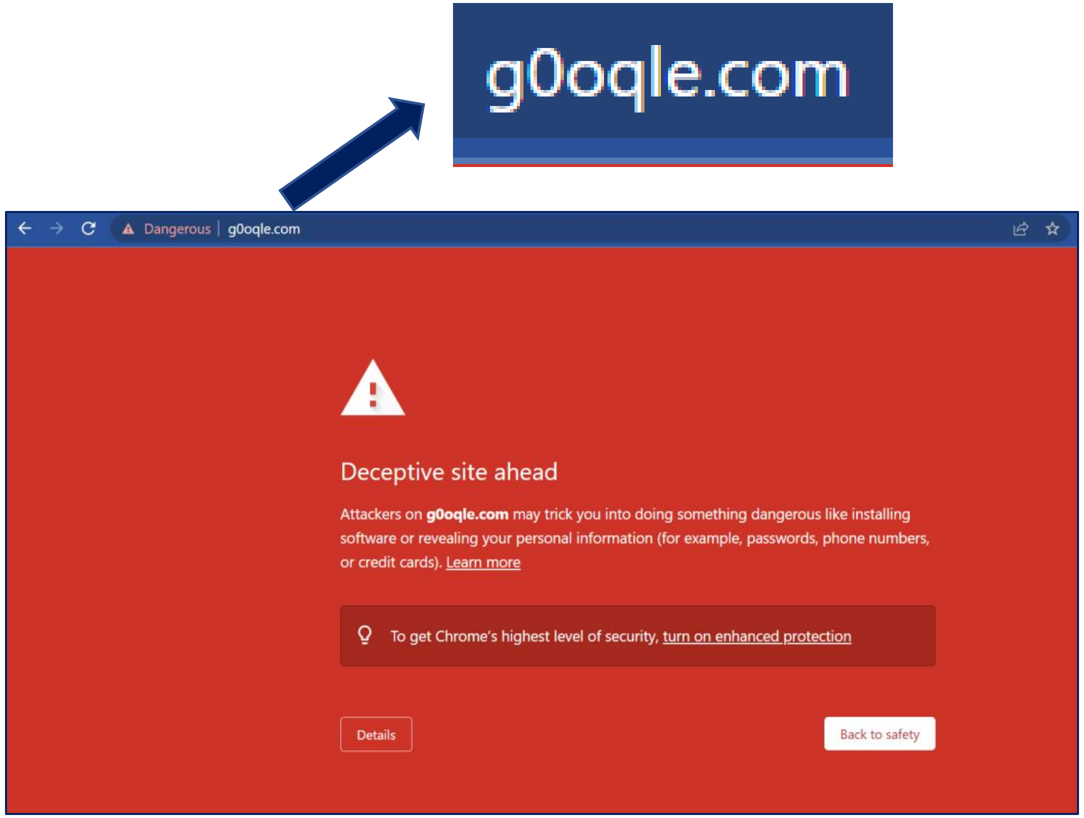
Apr 24, 2023

Contents

- Background/Motivation
- Domain Permutation
- Methodology
- Browser Study
- RPKI and TLS Certificate Study
- Conclusion, Limitations

Background/Motivation

- Look-alike domains are commonly employed in phishing attacks
- Having a secure lock icon (TLS certificate) often fool victims
- Our goals
  - How easy is it to impersonate popular domains?
  - Are browsers a good first line of defense in such attacks?
  - How common is it for such sites to have TLS certificates?
  - To observe patterns/trends in RPKI data and TLS certificates for common sites



Deceptive site ahead

Attackers on **g0oqle.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

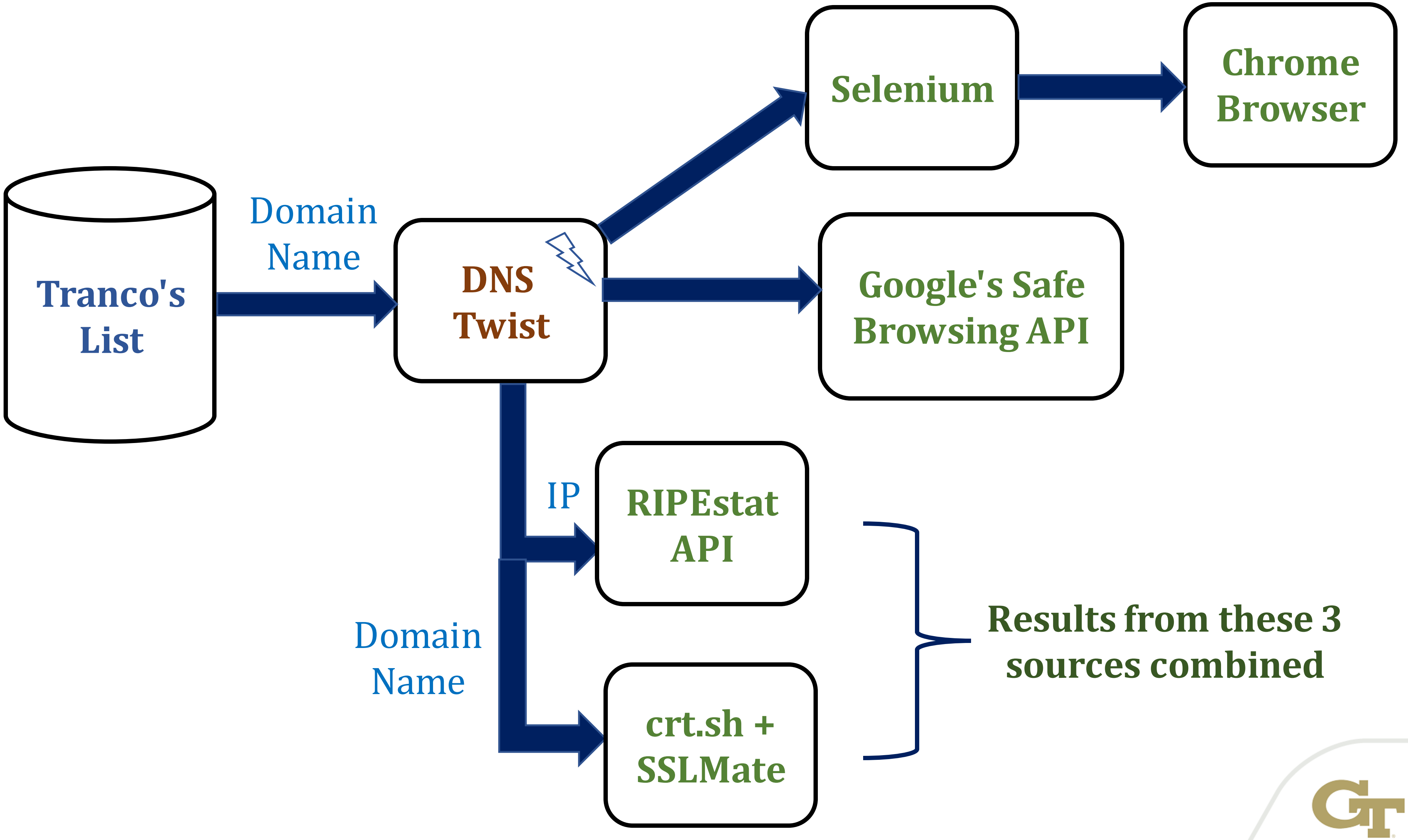
To get Chrome's highest level of security, turn on enhanced protection

Georgia Tech

Domain Twist

- Typo squatting: banrkofamerica.com
- Hyphenation: bankofamerica-signin.com
- Homographs: bànkofamerica.com
- Omission: bankofamrica.com
- Repetition: bankoffamerica.com
- More variations: vowel-swap, subdomain, replacement etc.

Methodology



Tranco's List

Domain Name

DNS Twist

Selenium

Chrome Browser

Google's Safe Browsing API

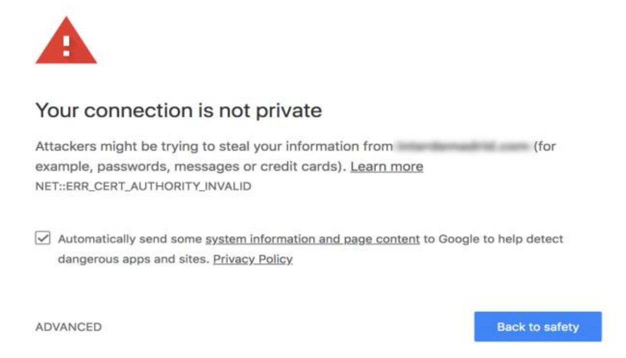
IP

RIPEstat API

Domain Name

crt.sh + SSLMate

Results from these 3 sources combined



Your connection is not private

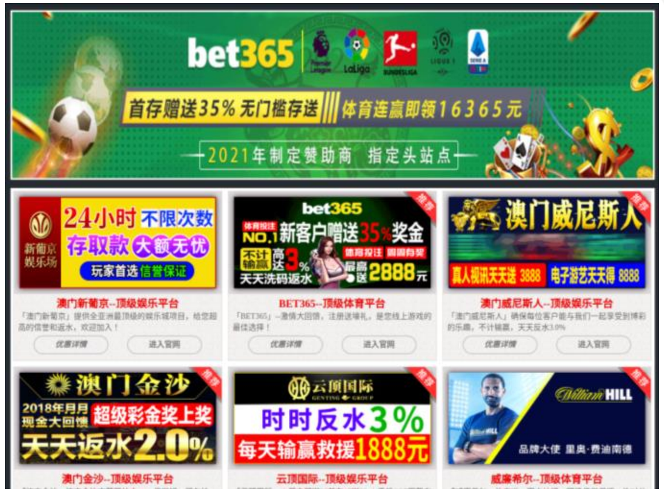
Attackers might be trying to steal your information from [redacted] (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

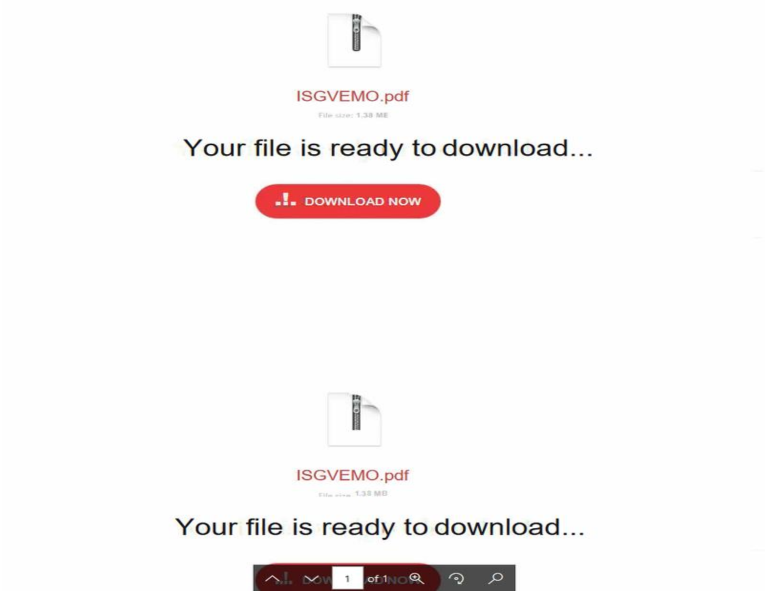
☑ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy Policy

ADVANCED

Back to safety


bet365
首存赠送35% 无门槛存送 体育连赢即领16365元
2021年制定赞助商 指定头站点
24小时不限次数 存取款 大额无忧 玩家首选 信誉保证
澳门新葡京--顶级娱乐平台
bet365 NO.1 新客户赠送35%奖金
BET365--顶级体育平台
澳门威尼斯人
澳门威尼斯人--顶级娱乐平台
澳门金沙
超级彩金奖上奖 天天返水2.0%
澳门金沙--顶级娱乐平台
云顶国际
时时反水3% 每天输赢救援1888元
云顶国际--顶级娱乐平台
William HILL
威廉希尔--顶级体育平台

Google Chrome Browser Study



ISGVEMO.pdf

File size: 1.38 MB

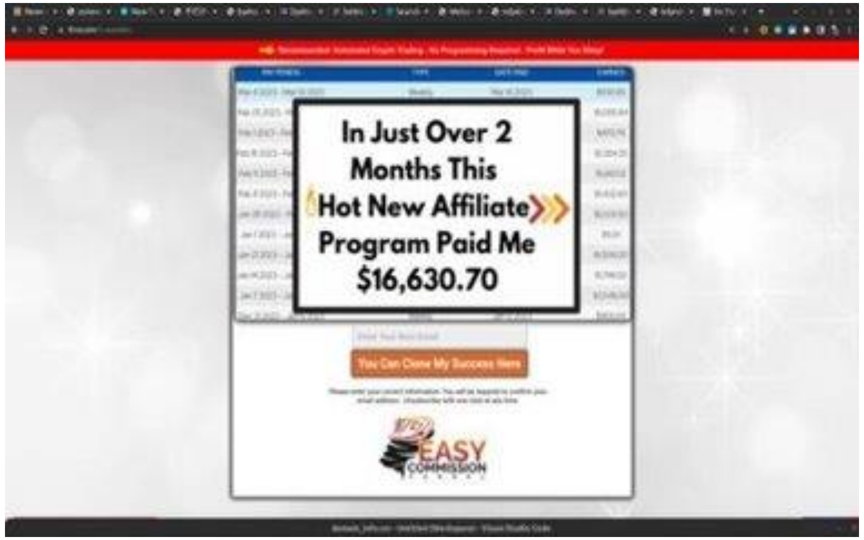
Your file is ready to download...

DOWNLOAD NOW

ISGVEMO.pdf

File size: 1.38 MB

Your file is ready to download...

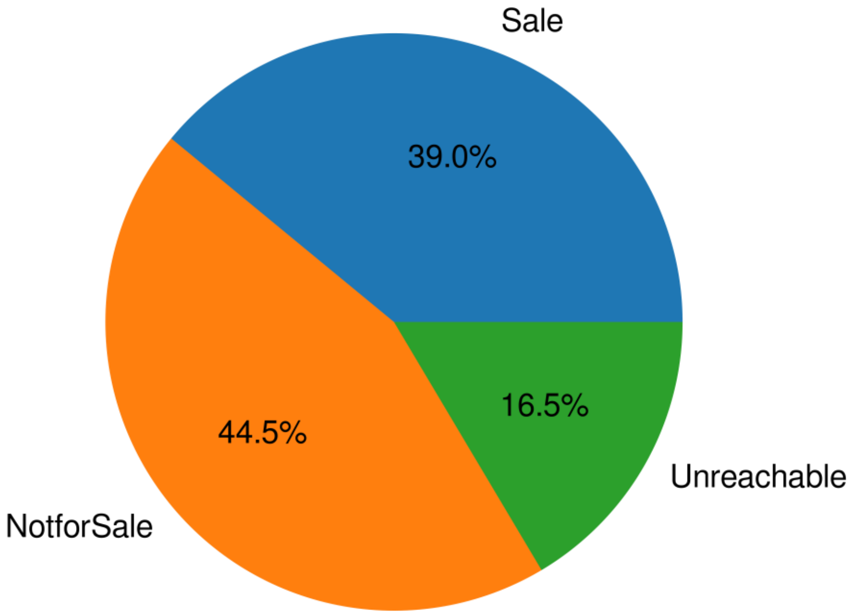


In Just Over 2 Months This Hot New Affiliate Program Paid Me $16,630.70

You Can Clone My Success Here

Chrome Study: Overview

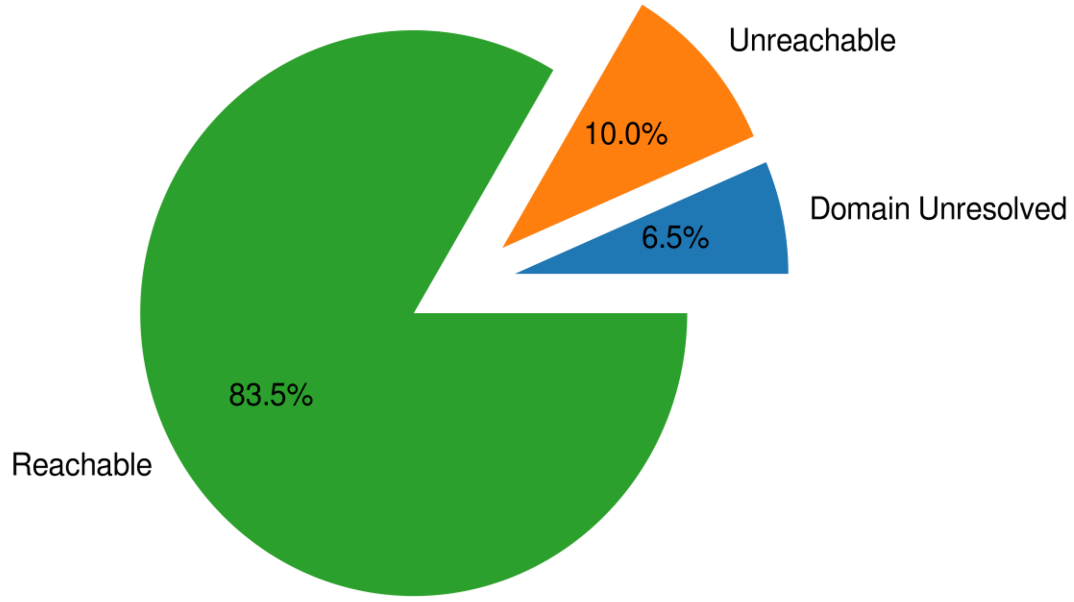
- Took random 150 domains from the top 1500 domains in Tranco's List
- Twisted the domains with minimum edit distance and tried to do the DNS resolution.
- Finally resolved around 3000 domains in total.
- Learning: Launching a phishing website for a renowned domains is not so difficult.



What about domain resolution?

- **Unreachable: HTTP 403/404 Error**

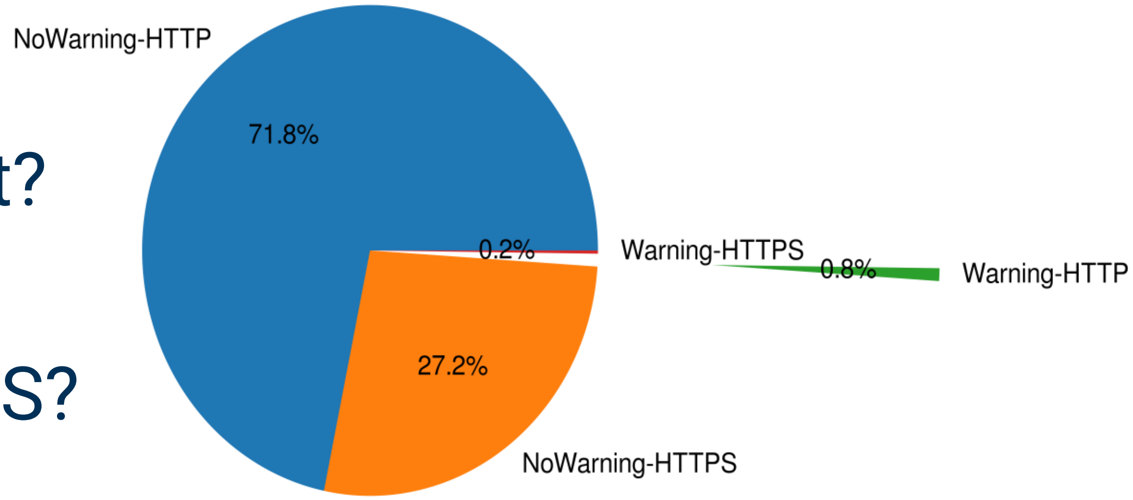
- **Domain Unresolved: Domain doesn't exist or the RIR doesn't support registering those domains**



Chrome Study: Inspection

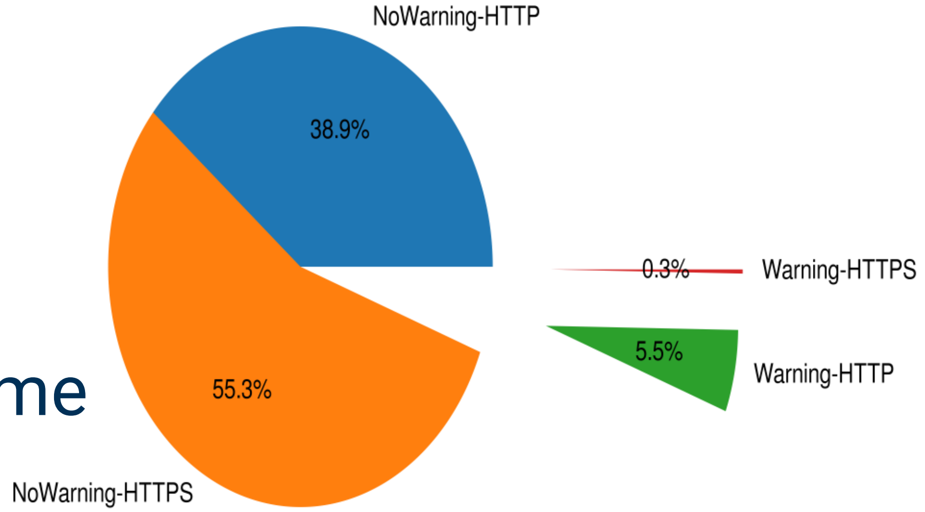
What about the landscape of *available to buy domains*?

- Warning: Chrome shows warning or not?
- HTTP(S): The domain is HTTP or HTTPS?
- For most of the available domains chrome doesn't show warning, and some are securely hosted by domain providers, some aren't.



Chrome Study: Inspection (contd..)

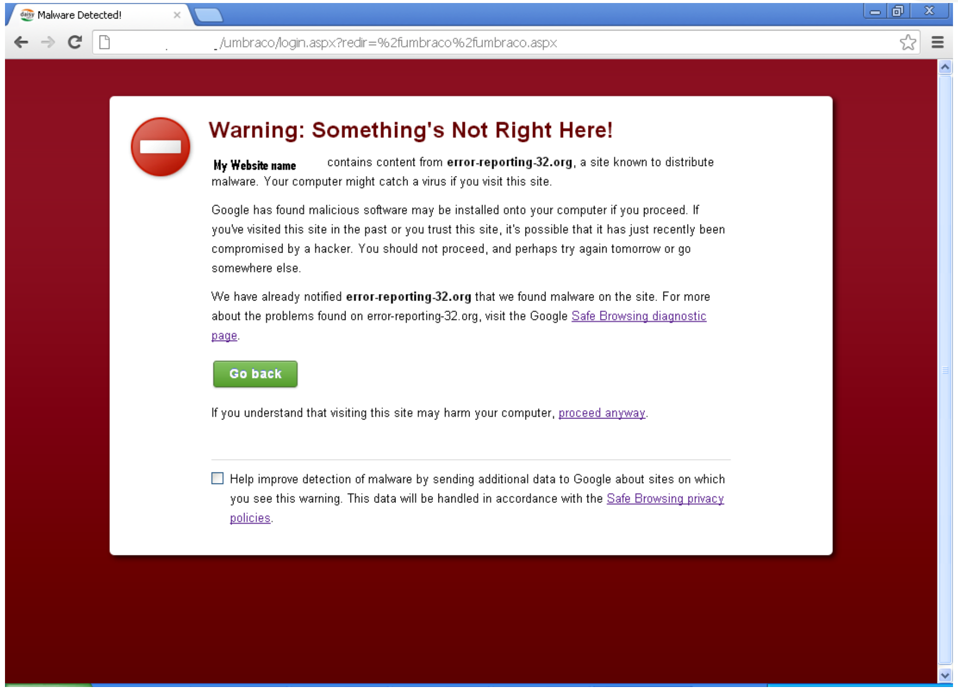
- Domains not-available-to-buy also don't have TLS adoption fully.
- Many legit website(medical, government organizations, universities (*http://vatech.edu/*)) domains rely on HTTP
- Some of the domains do show warning in chrome
- Some HTTPS domains resulted in automatically downloading potentially malicious files



Chrome vs Safe Browsing API

Surprising result:

- Out of nearly 3000 domains, **Chrome** showed warning for around **70** domains,
- However, Safe Browsing API only showed for **6-7** domains.
- Assumption: The open-source safe browsing API doesn't expose updated information.



Warning: Something's Not Right Here!

My Website name contains content from **error-reporting-32.org**, a site known to distribute malware. Your computer might catch a virus if you visit this site.

Google has found malicious software may be installed onto your computer if you proceed. If you've visited this site in the past or you trust this site, it's possible that it has just recently been compromised by a hacker. You should not proceed, and perhaps try again tomorrow or go somewhere else.

We have already notified **error-reporting-32.org** that we found malware on the site. For more about the problems found on error-reporting-32.org, visit the Google Safe Browsing diagnostic page.

Go back

If you understand that visiting this site may harm your computer, proceed anyway.

□ Help improve detection of malware by sending additional data to Google about sites on which you see this warning. This data will be handled in accordance with the Safe Browsing privacy policies.

Google Safe Browsing

RPKI and TLS certificate study

Datasets

- RIPEstat API – for ASN, RPKI status, RIR registration
- Certificate Transparency System – Public, distributed, append-only ledgers of certificates; Supported by Chrome and Safari
    - crt.sh - unstable, limited outdated entries on large domains
    - SSLMate Certificate Search API – up-to-date, expired certificates not shown, rate limited

  (Assumption – correctness of the issuer name in X.509 certificates)

- Now we try to explore patterns in the dataset to see if we can answer what makes it easy to obtain these certificates?
- Certificate info existed for 1519 (53%) of the domains

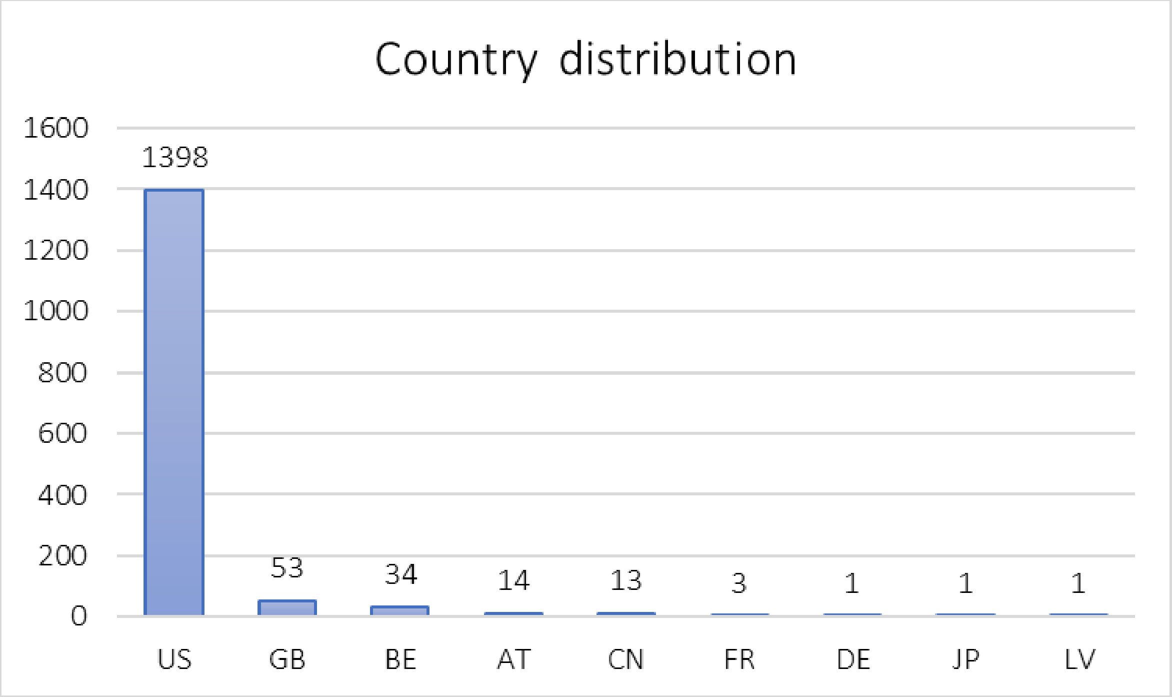
RPKI status and ASN distribution

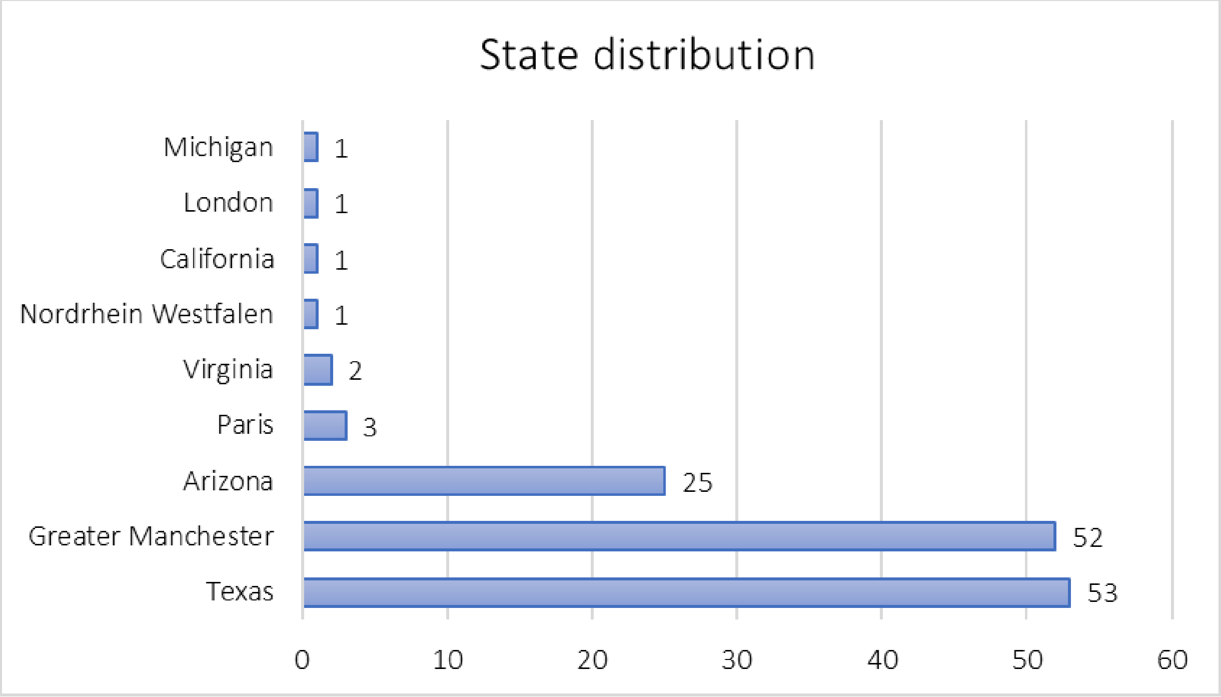
- 1627 valid (57%), 1186 unknown (42%), 4 invalid length
- Addresses with unexpired certificates – 65% valid, 34.7% unknown
- Top ASNs -

ASN	Count	Owner
16509	483	Amazon
6461	226	Zayo Group
206834	172	Team Internet (Germany)
13335	144	Cloudflare
396982	118	Google
133618	108	Trellian Pty. Limited (Australia)
14618	108	Amazon

Geographical distributions

- Country and State wise distributions (RIR data from RIPE shows similar trend wherein 68% prefixes delegated by ARIN)



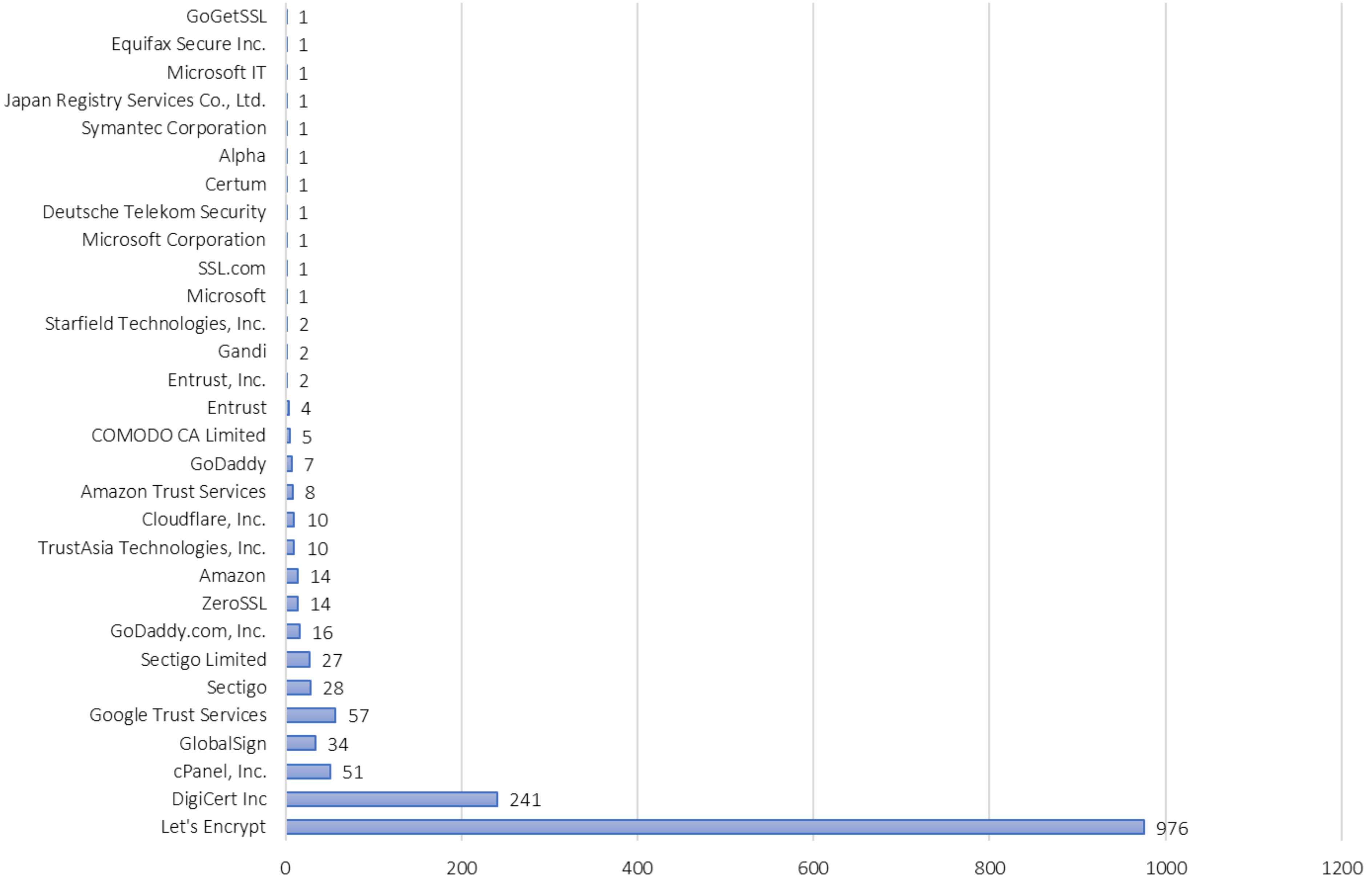


GB – Great Britain, BE – Belgium, AT – Austria, CN – China,

FR – France, DE – Germany, JP – Japan, LV – Latvia

CA distribution

- Let's Encrypt (64%)
- DigiCert (16%)

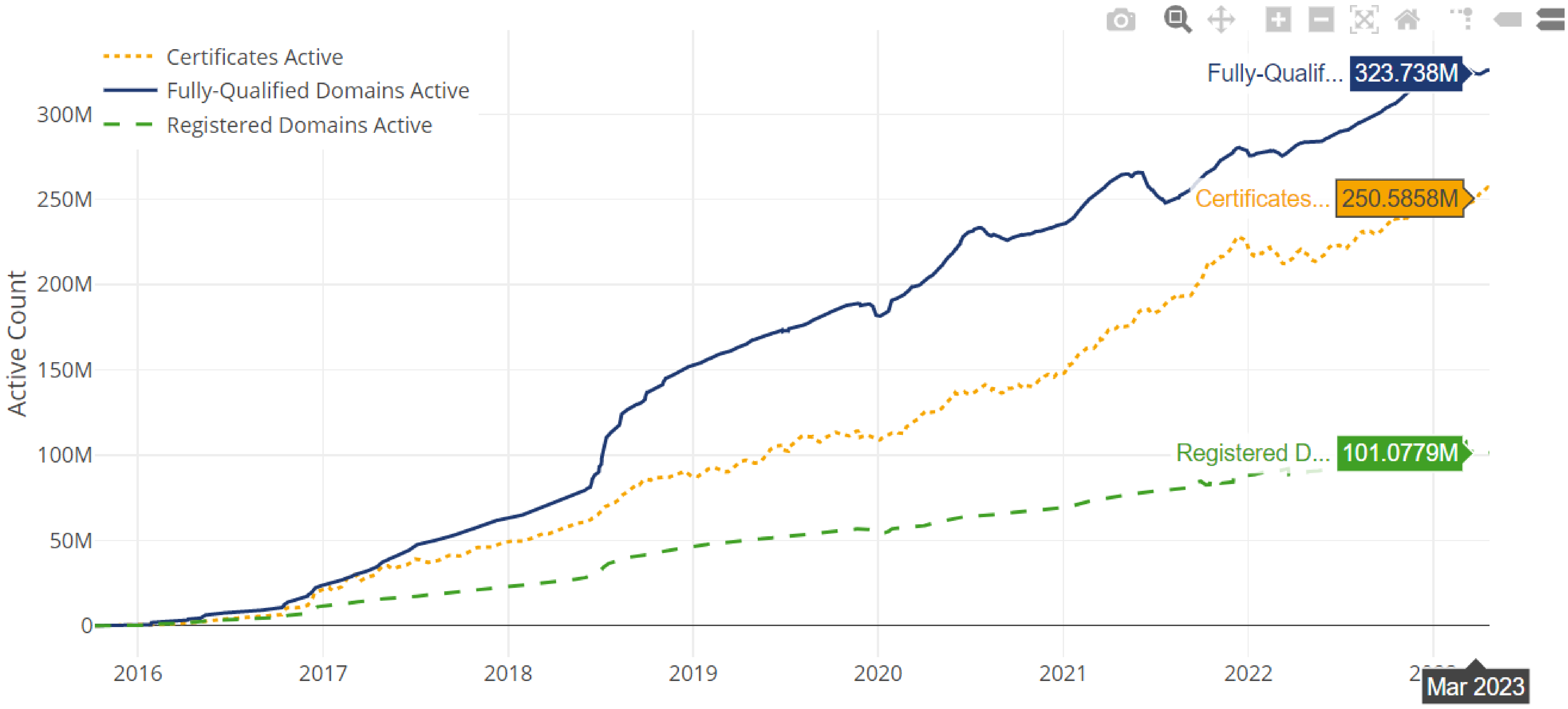


Observations

- Across both expired and unexpired certificates, Let's Encrypt dominates as the issuing CA with a 64% share
- Free, automated and open (ACME protocol for domain validation)

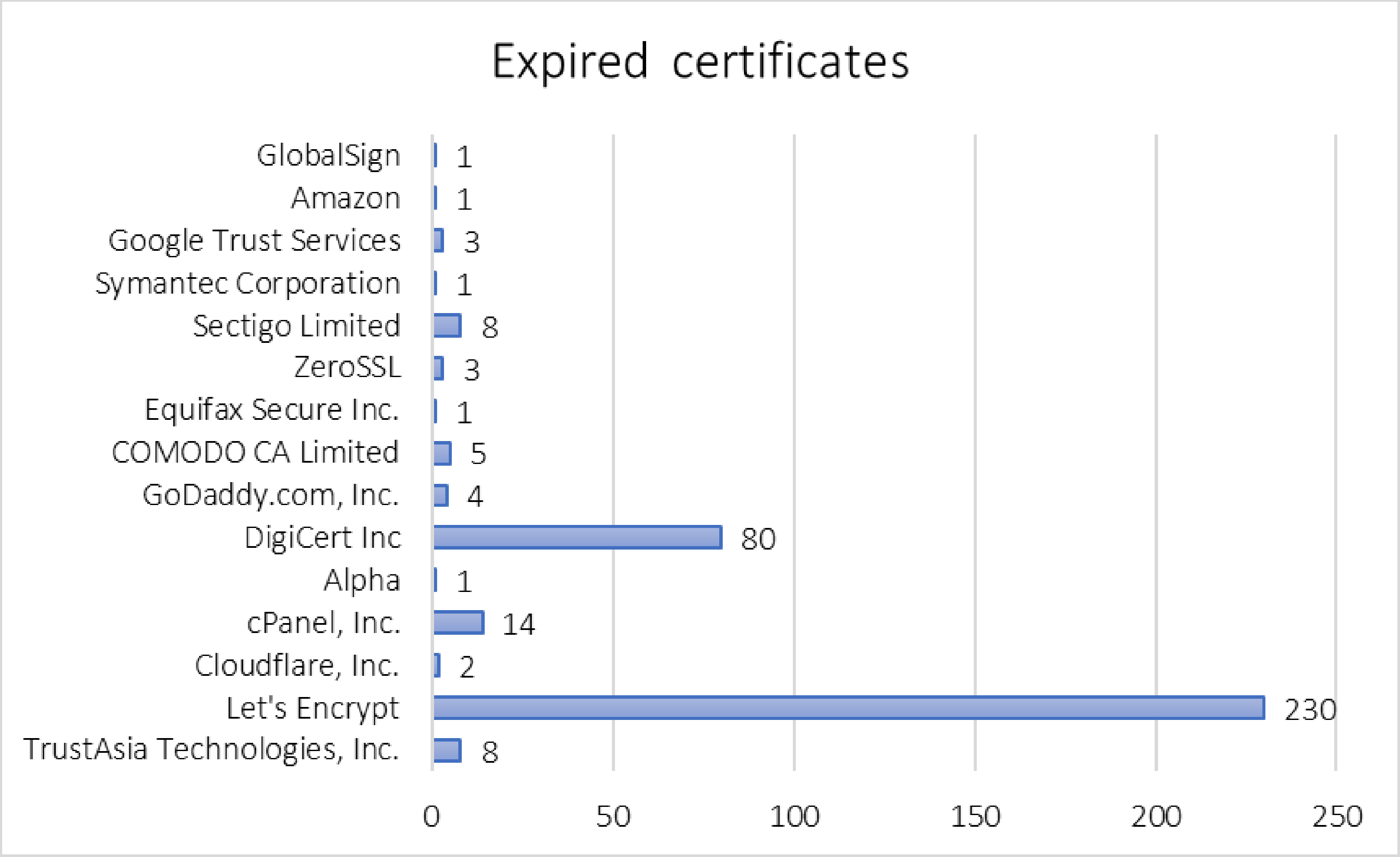
Rank	Issuer	Usage	Market Share	%age seen in our dataset
1	IdenTrust	48.5%	53.6%	0%
2	DigiCert Group	13.1%	14.5%	16%
3	Sectigo (Comodo Cybersecurity)	12.1%	13.4%	0.04%
4	GlobalSign	6.1%	6.7%	0.02%
5	Let's Encrypt	5.8%	6.4%	64.2%
6	GoDaddy Group	4.8%	5.3%	0.015%

Growth of Let's Encrypt over the years



Tech

Expired and Revoked certificates



- Revoked – only 9
- Total (revoked + expired) – only 22%

- Most look-alike domains still have valid certificates (all issued in 2022 or later)

Conclusions and Recommendations

- Google might use multiple sources other than Safe Browsing API
- Obtaining a certificate for look-alike domains is fairly common and easy to do with free certificate granting authorities like Let's Encrypt
- To detect potentially malicious look-alike domains, domain owners can use the combination of tools like DNSTwist and CT Monitors to identify such websites and receive alerts when a new certificate is detected for them

Limitations of our approach

- Usage of a small dataset (150 domains from Tranco's list of a million)

- Restricted to Firefox (Chrome) for the time being

- Usage of 2 datasets (crt.sh and SSLMate) for collecting certificate information might have led to some uncaught inconsistencies (we did not get access to Censys)

- We did not factor in domain reputation (presence in spam filters, blocklists, etc.)

Thank you

Georgia Tech