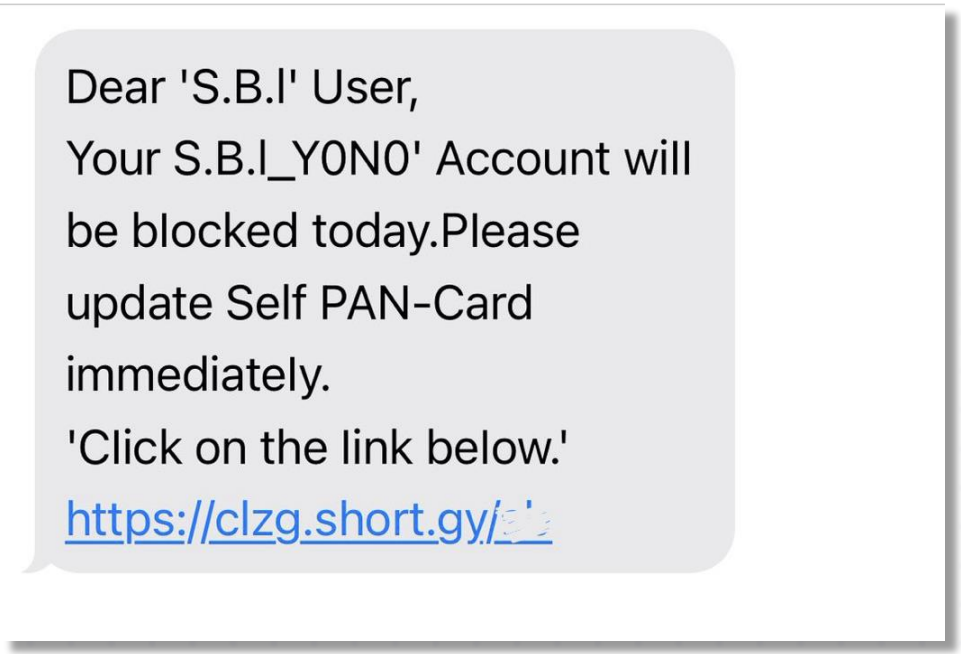
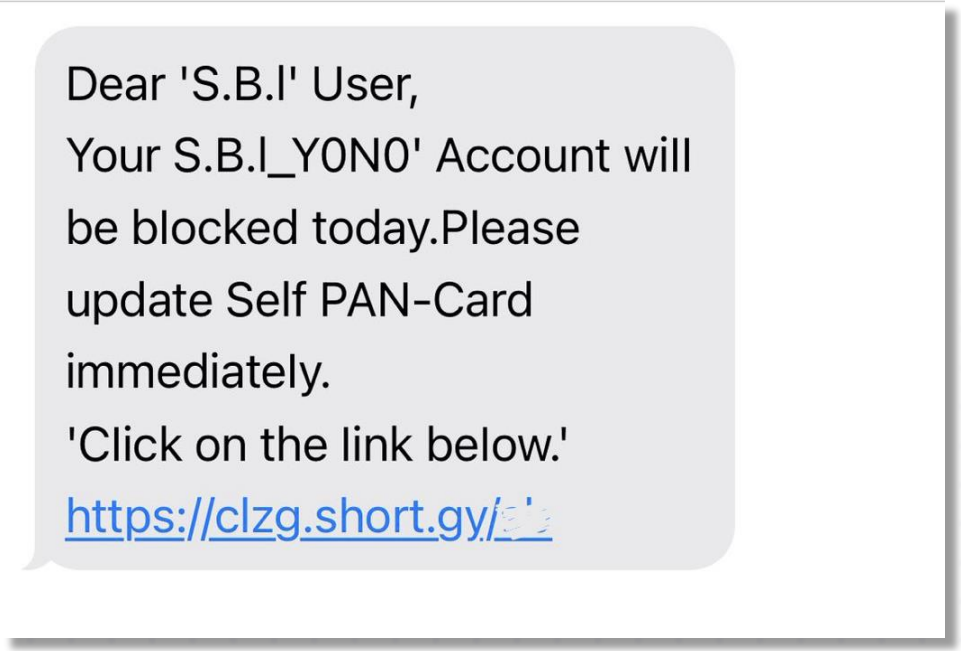
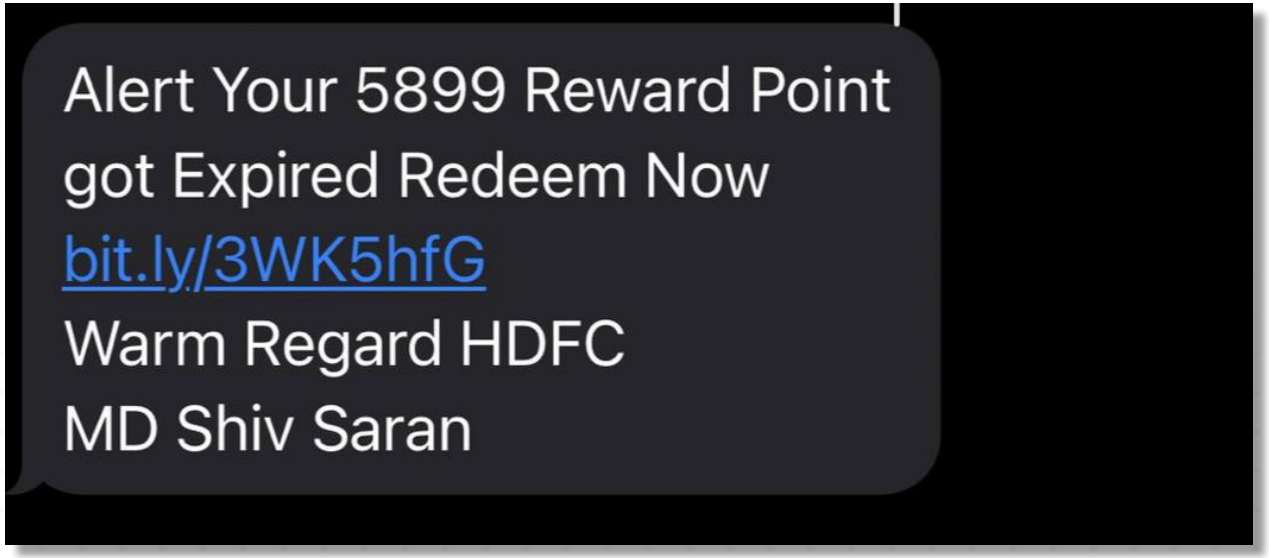
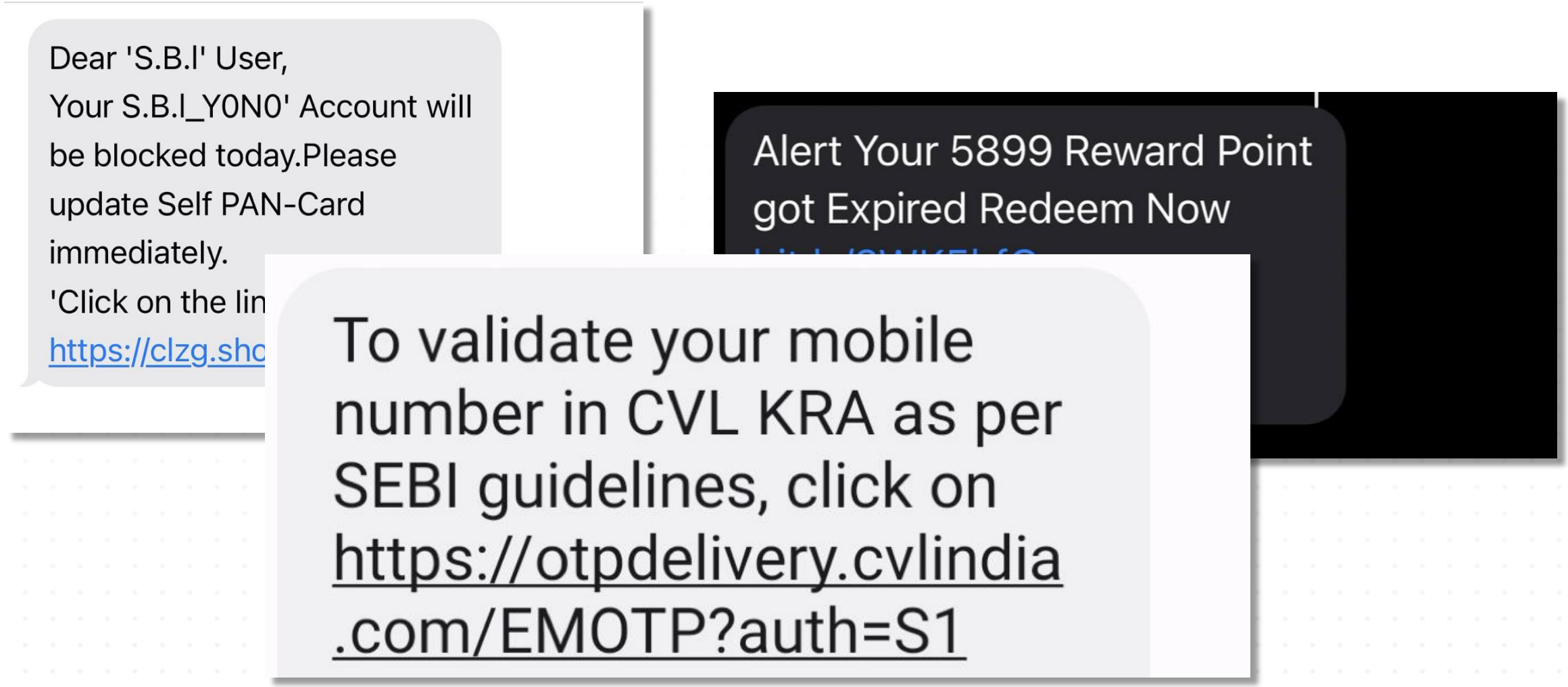
How many of you have received/seen such SMS?

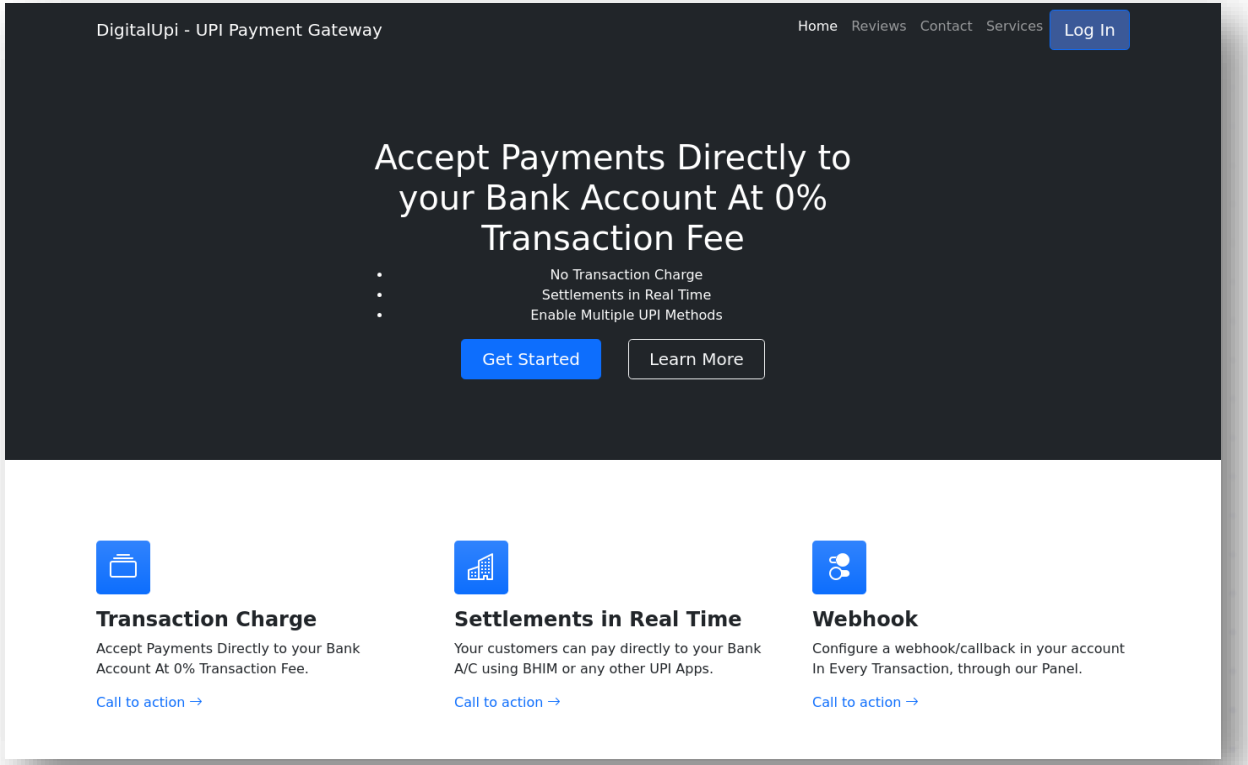

Dear 'S.B.I' User,
Your S.B.I_Y0N0' Account will be blocked today.Please update Self PAN-Card immediately.
'Click on the link below.'
https://clzg.short.gy/

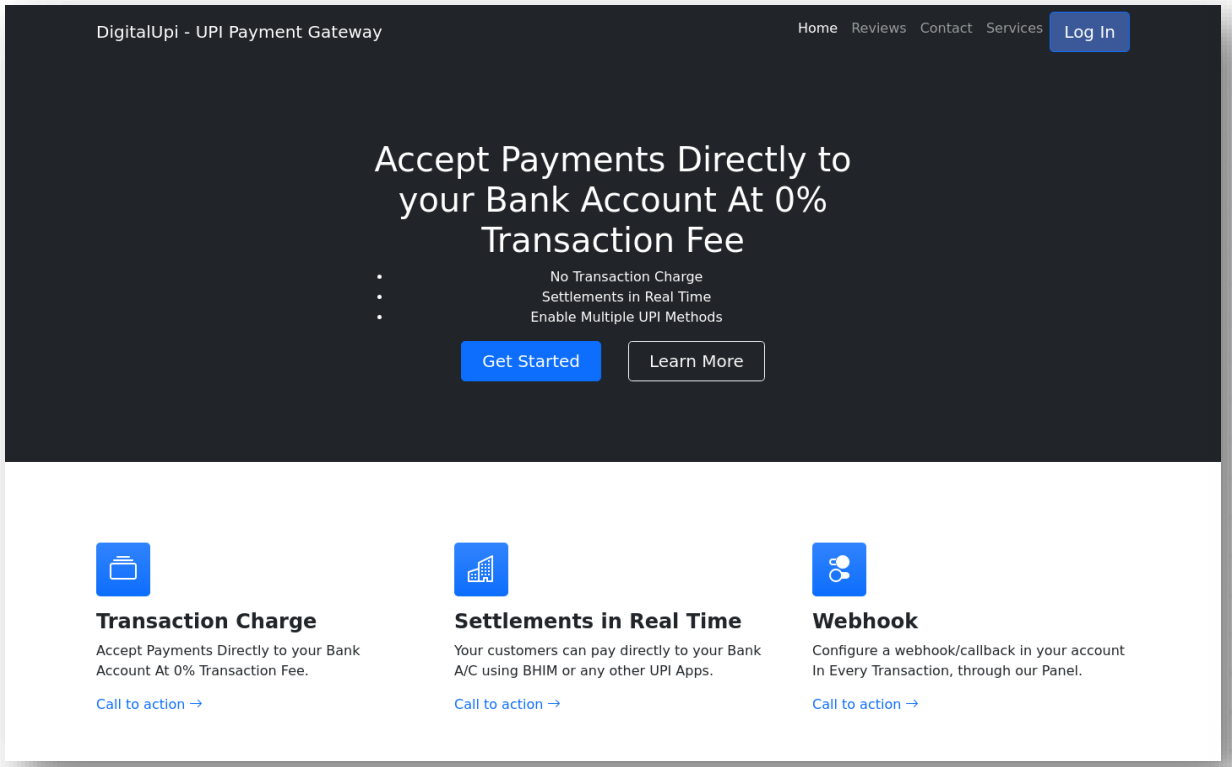

Dear 'S.B.I' User,
Your S.B.I_Y0N0' Account will be blocked today.Please update Self PAN-Card immediately.
'Click on the link below.'
https://clzg.short.gy/


Alert Your 5899 Reward Point got Expired Redeem Now
bit.ly/3WK5hfG
Warm Regard HDFC
MD Shiv Saran

BOLSTER


Dear 'S.B.I' User,
Your S.B.I_Y0N0' Account will be blocked today.Please update Self PAN-Card immediately.
'Click on the lin
https://clzg.sho
Alert Your 5899 Reward Point got Expired Redeem Now
To validate your mobile number in CVL KRA as per SEBI guidelines, click on https://otpdelivery.cvlindia.com/EMOTP?auth=S1


DigitalUpi - UPI Payment Gateway
Home
Reviews
Contact
Services
Log In
Accept Payments Directly to your Bank Account At 0% Transaction Fee
No Transaction Charge
Settlements in Real Time
Enable Multiple UPI Methods
Get Started
Learn More
Transaction Charge
Accept Payments Directly to your Bank Account At 0% Transaction Fee.
Call to action →
Settlements in Real Time
Your customers can pay directly to your Bank A/C using BHIM or any other UPI Apps.
Call to action →
Webhook
Configure a webhook/callback in your account In Every Transaction, through our Panel.
Call to action →


DigitalUpi - UPI Payment Gateway
Home Reviews Contact Services Log In
Accept Payments Directly to your Bank Account At 0% Transaction Fee
No Transaction Charge
Settlements in Real Time
Enable Multiple UPI Methods
Get Started
Learn More
Transaction Charge
Accept Payments Directly to your Bank Account At 0% Transaction Fee.
Call to action →
Settlements in Real Time
Your customers can pay directly to your Bank A/C using BHIM or any other UPI Apps.
Call to action →
Webhook
Configure a webhook/callback in your account In Every Transaction, through our Panel.
Call to action →


PHONEPE GATEWAY
Home Feature Pricing Help Desk Try Demo Free
Login
Register
Paytm
Accept Payments At 0% Transaction Fee
Scan and Pay Feature. Accept All UPI Apps.
No Transaction Charge. Instant Settlements.
Enable Multiple UPI Accounts.
Try for free
SCAN TO PAY
Accepting Payments Made Easy, Simple & FREE!
The logos below are the property of respective trademark owners. All the below apps support BHIM-UPI.
PhonePe
G Pay
amazon pay

DigitalUpi - UPI Payment Gateway

Accep
you

Transaction Charge

Accept Payments Directly to your Bank Account At 0% Transaction Fee.

Call to action →

UPI Gateway

Home Pricing Contact Login

Accept Payments Directly to your Bank Account At 0% Transaction Fee

No Transaction Charge,Settlements in Real Time,Enable Multiple UPI Methods

Get Started →

gin Register Paytm

e & FREE!

BHIM-UPI.

zon pay

BOLSTER

BOLSTER

Outsmarting Scammers: Phishing and Scam Trends in 2023

Anshuman Das | Bolster Research Labs

Get Started →

Agenda

- Some Infamous Trends
- Evolution of the Techniques
- How They are Doing It
- Scams to Watch Out in 2024
- Detecting to Scale

Analysis & Classifications

> 173 Million
Total Analyzed URLs

> 5.69 Million
Suspicious URLs

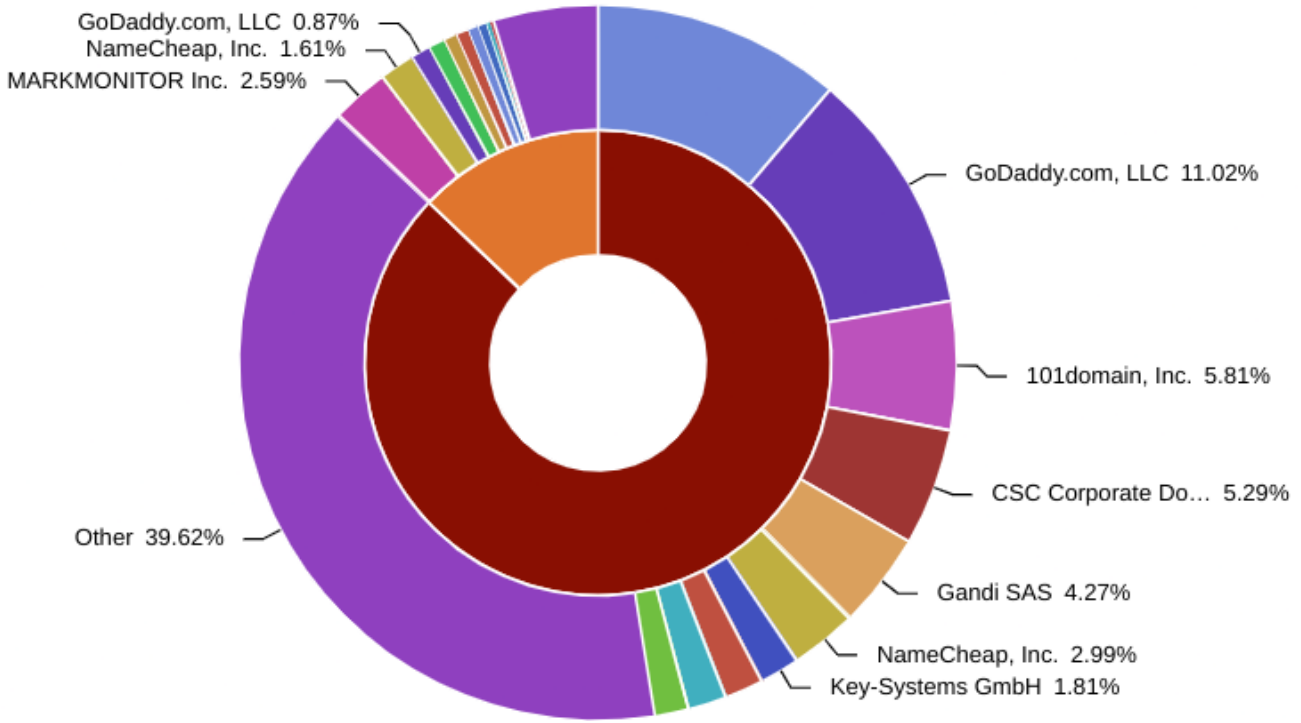
> 7.03 Million
Phishing URLs

> 10.3 Million
Scam URLs

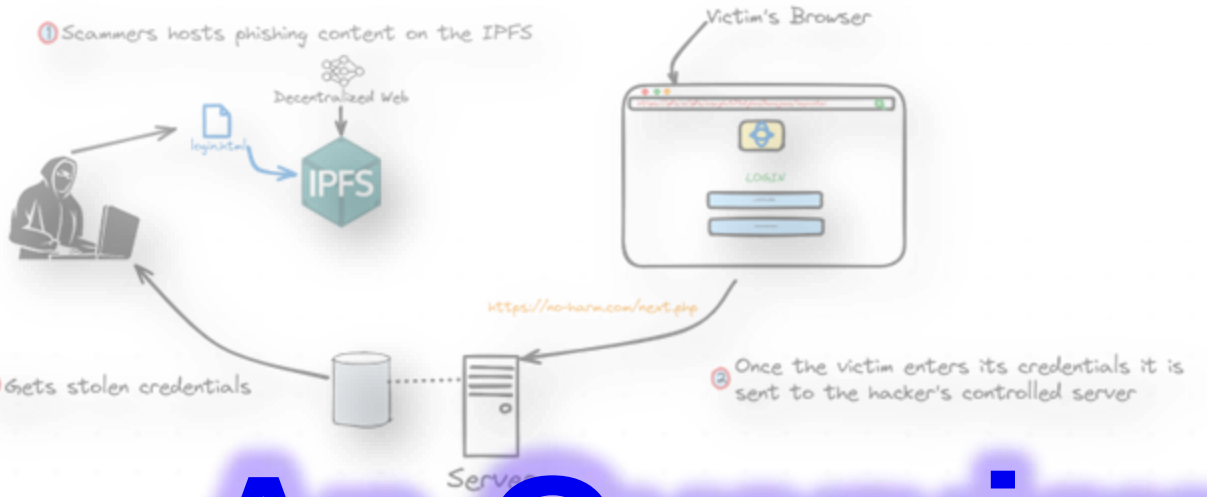
**Source: from the dataset commencing Jan 1,2023*

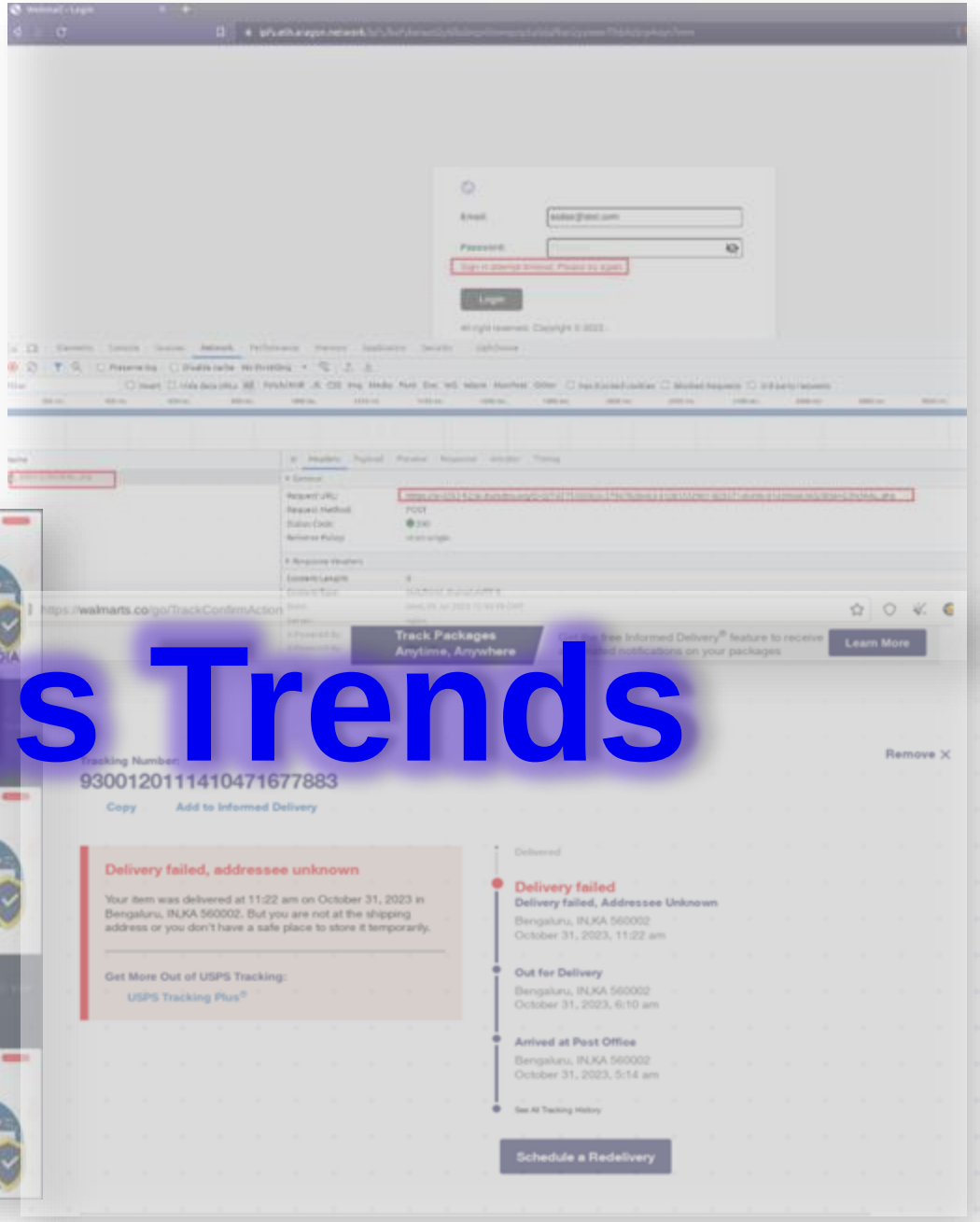
Top Domain Registrar: Scam and Phishing Domains

- GoDaddy.com, LLC
- 101domain, Inc.
- CSC Corporate



BOLSTER



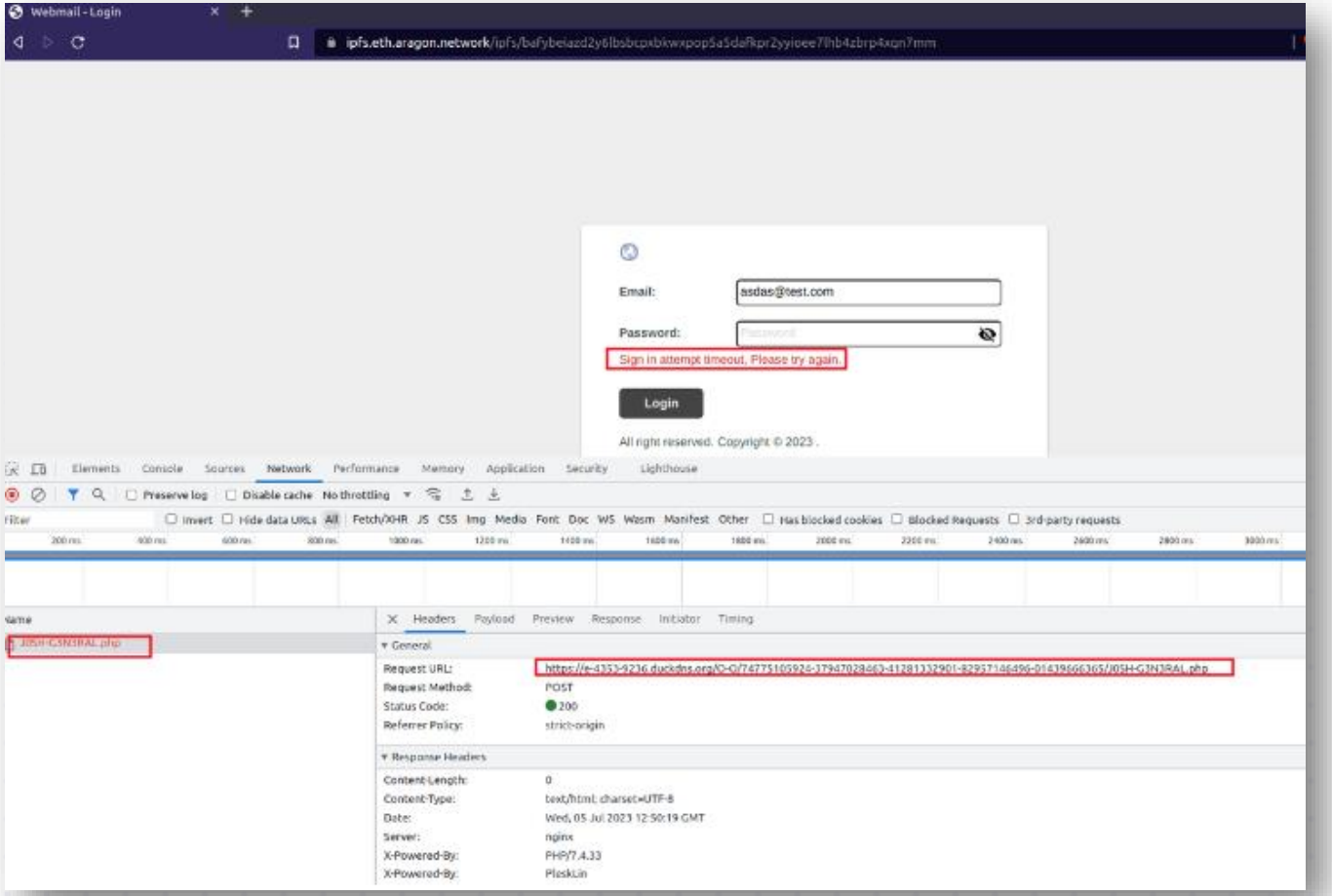


An Overview: Some Infamous Trends

An Overview: Some Infamous Phishing/Scam Campaign

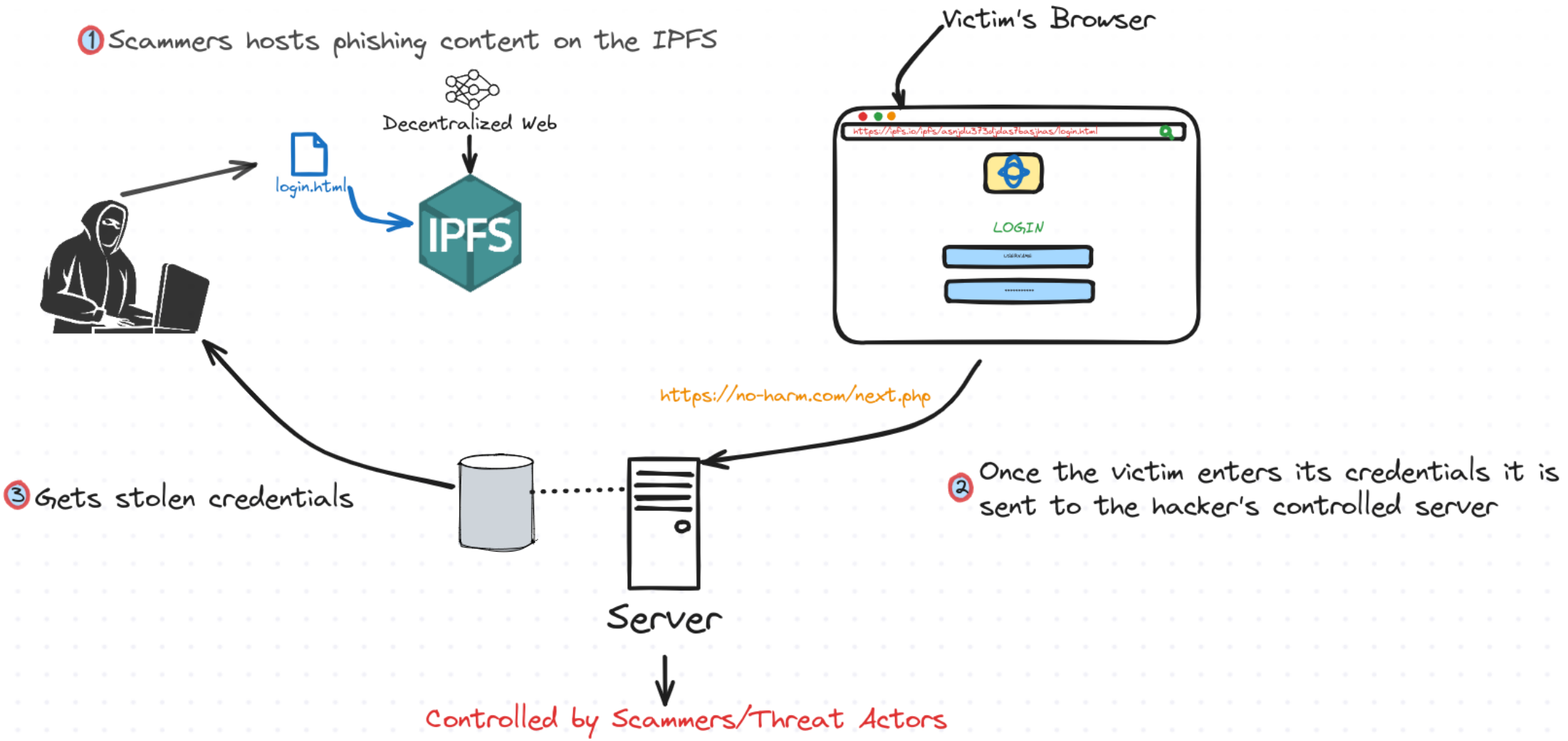
Abusing Decentralized Web

- Blockchain – IPFS
- Free to use
- Less Regulations



BOLSTER

How it works



BOLSTER

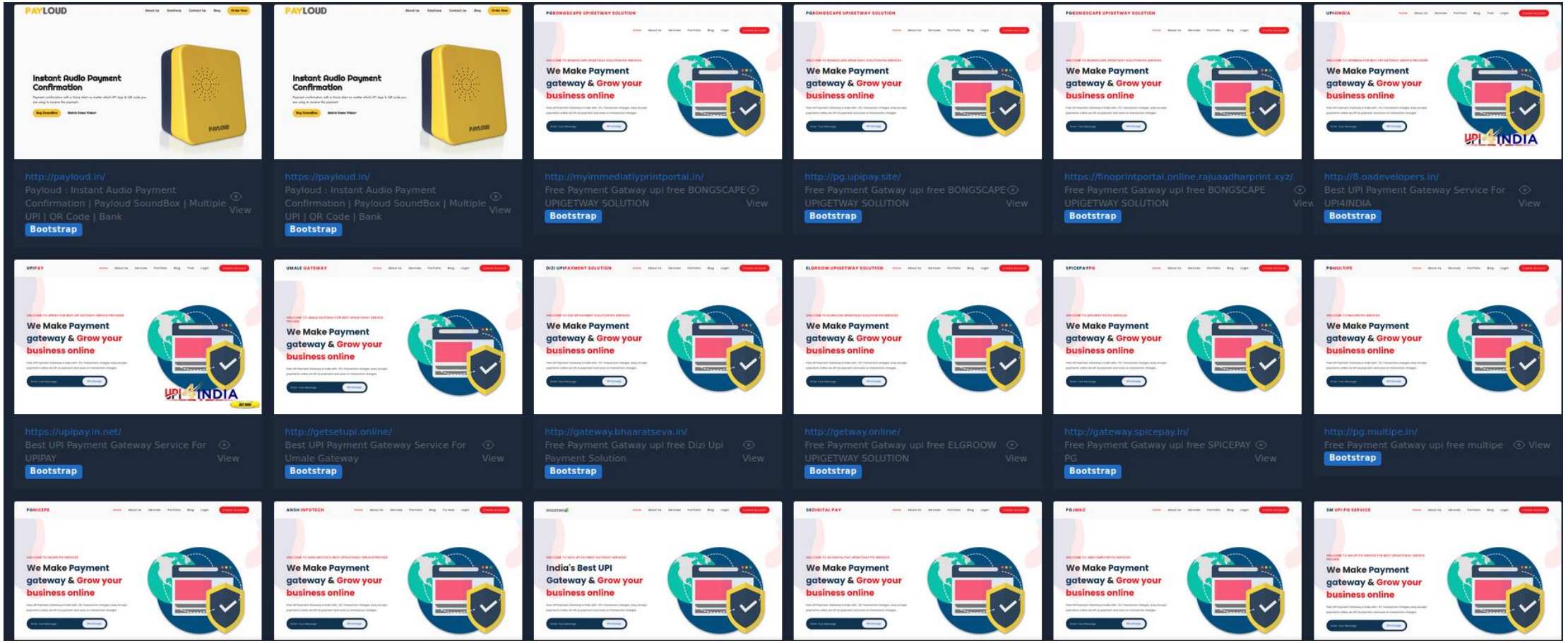
An Overview: Some infamous Phishing/Scam Campaign

Impersonation of Payment Gateways

- Stealing PAN & Aadhaar Number
- Created using phishing-kits
- Masquerades as legit business

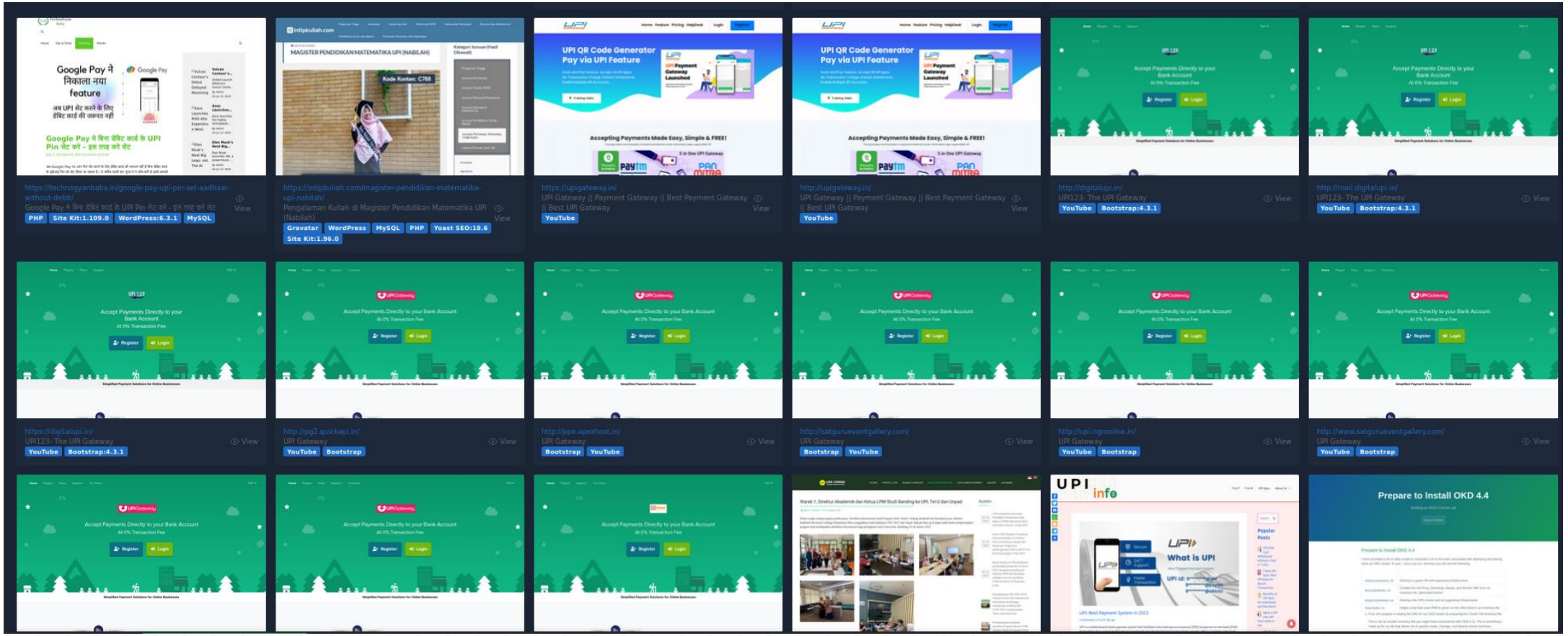
BOLSTER

Similar Looking Phishing Sites !!?

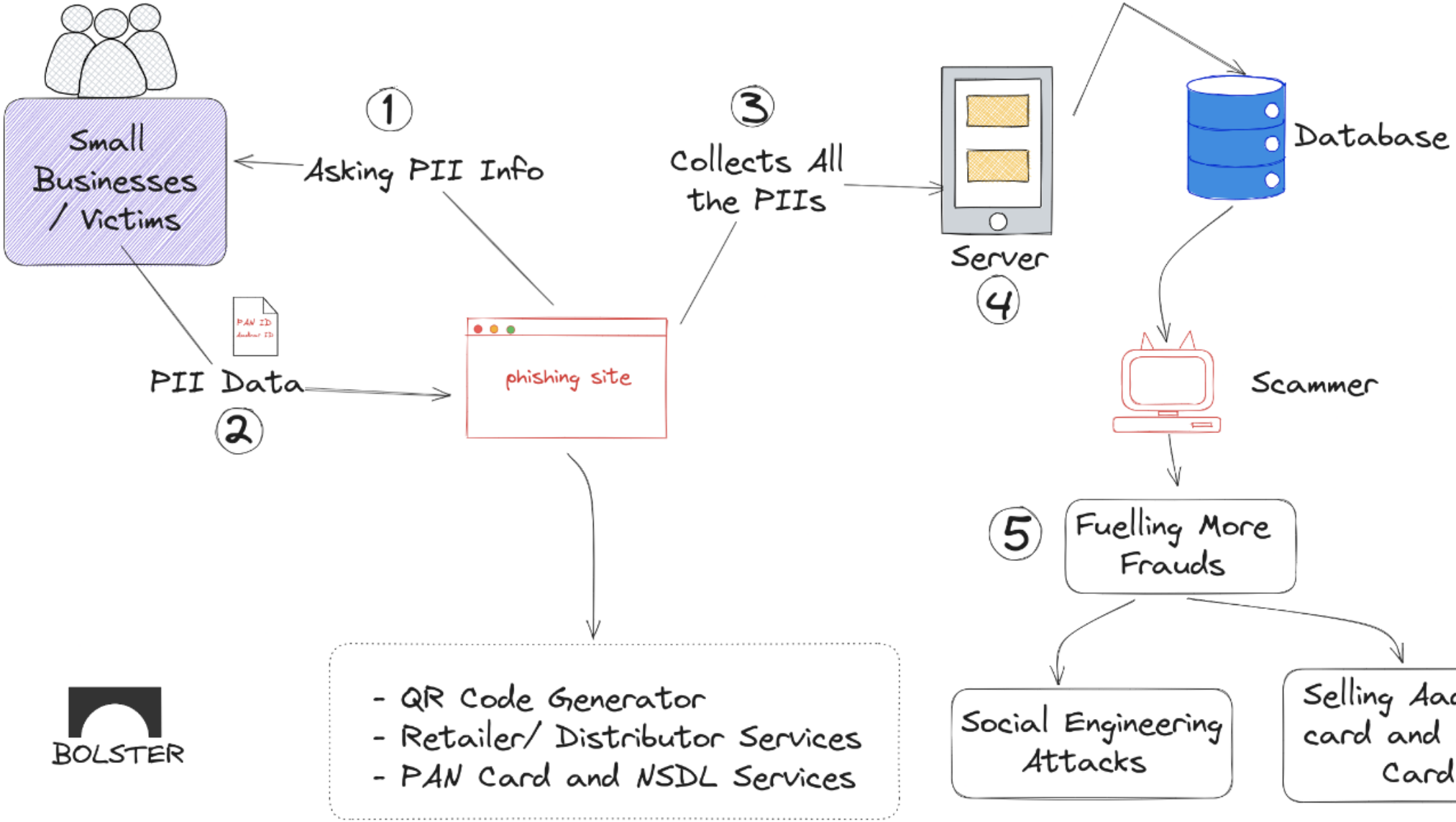


BOLSTER

Some More... 😮



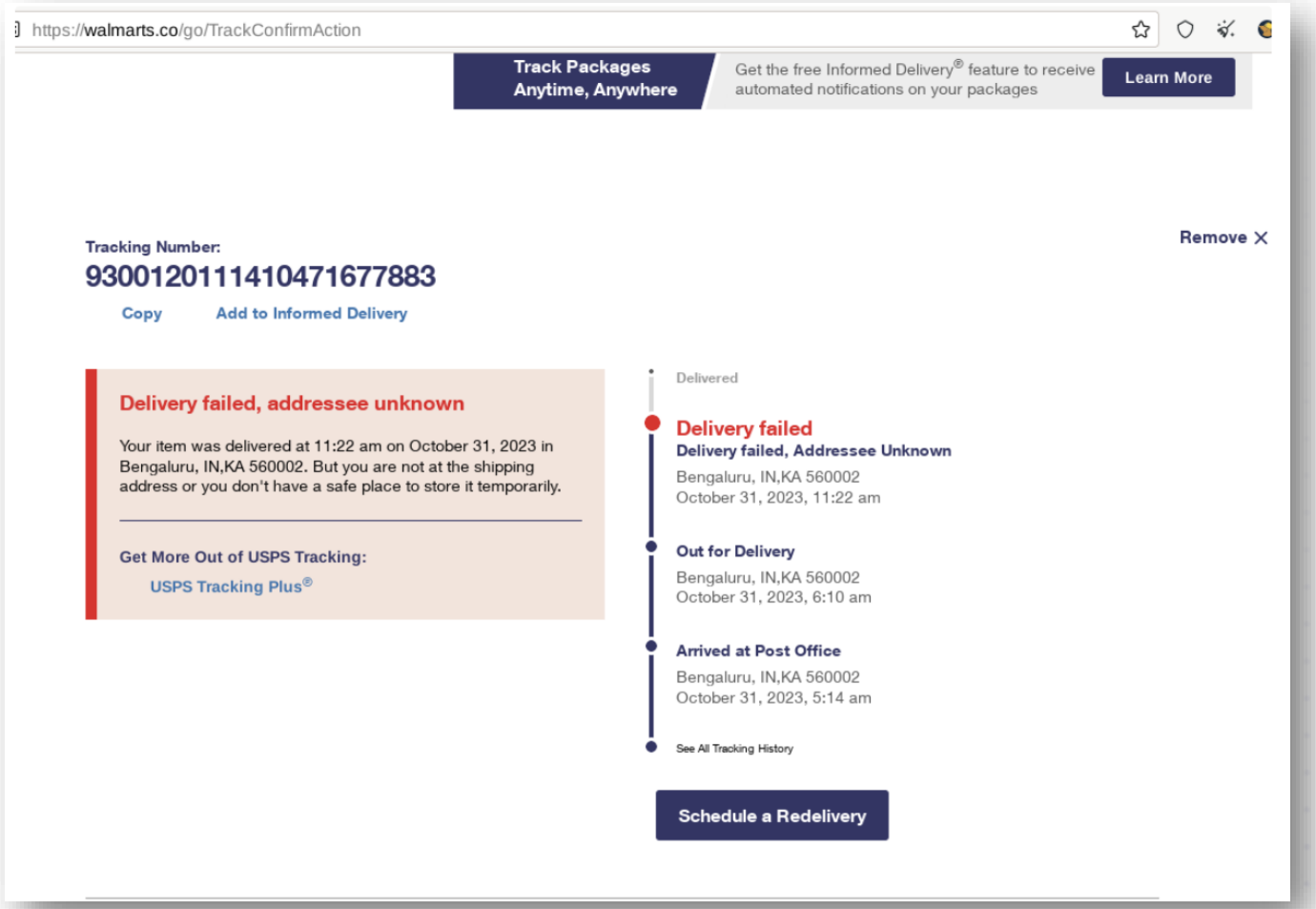
BOLSTER


Small Businesses / Victims
1
Asking PII Info
3
Collects All the PIIs
Server
4
Database
PII Data
2
phishing site
Scammer
5
Fuelling More Frauds
- QR Code Generator
- Retailer/ Distributor Services
- PAN Card and NSDL Services
Social Engineering Attacks
Selling Aadhar card and PAN Card
BOLSTER

An Overview: Some infamous Phishing/Scam Campaign

Shipment Scam Campaigns

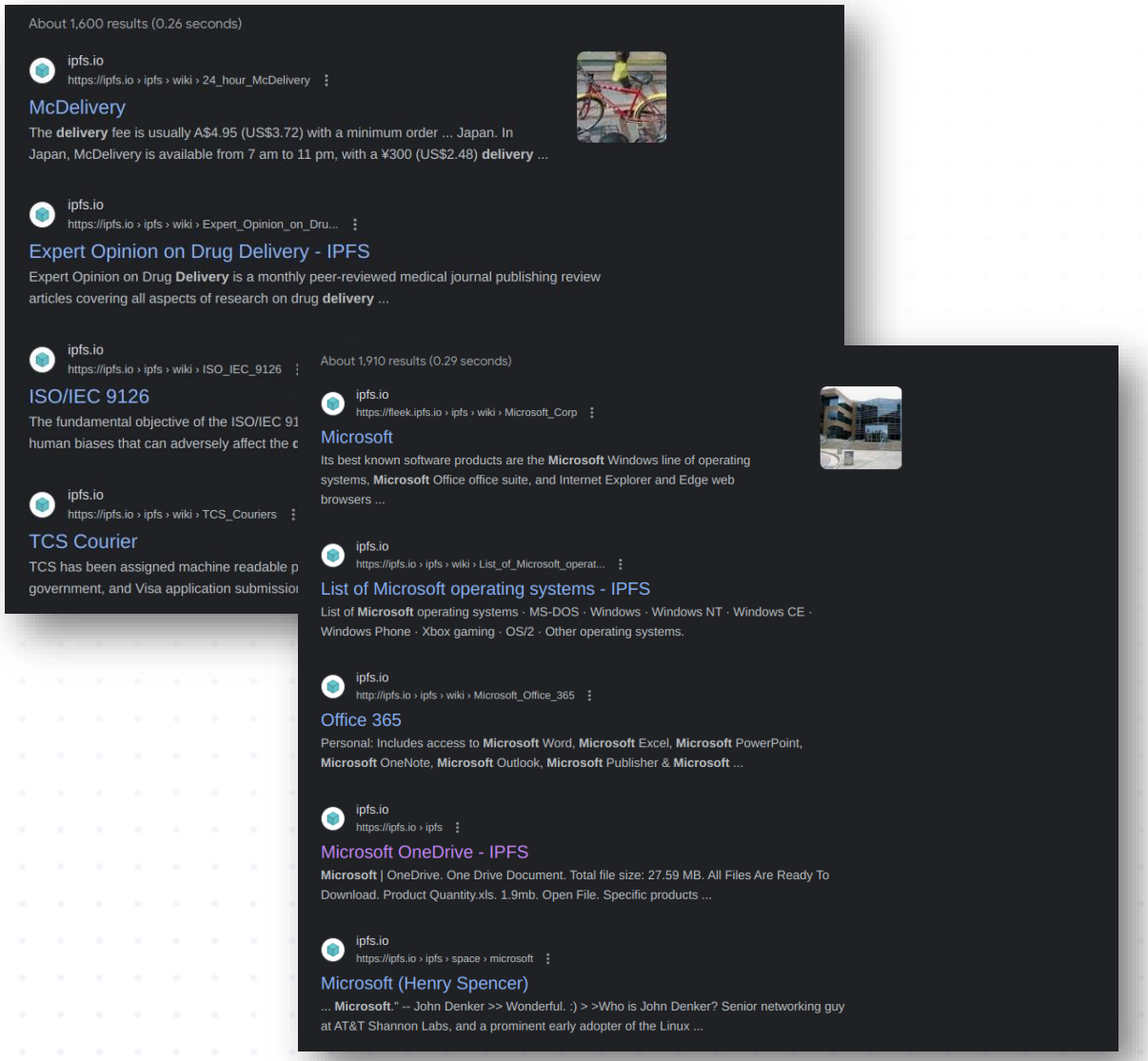
- Usages of Geo-fencing
- Victim's IP location Integration
- Abuse of SaaS & DDNS



BOLSTER

Mediums of Distribution (1)

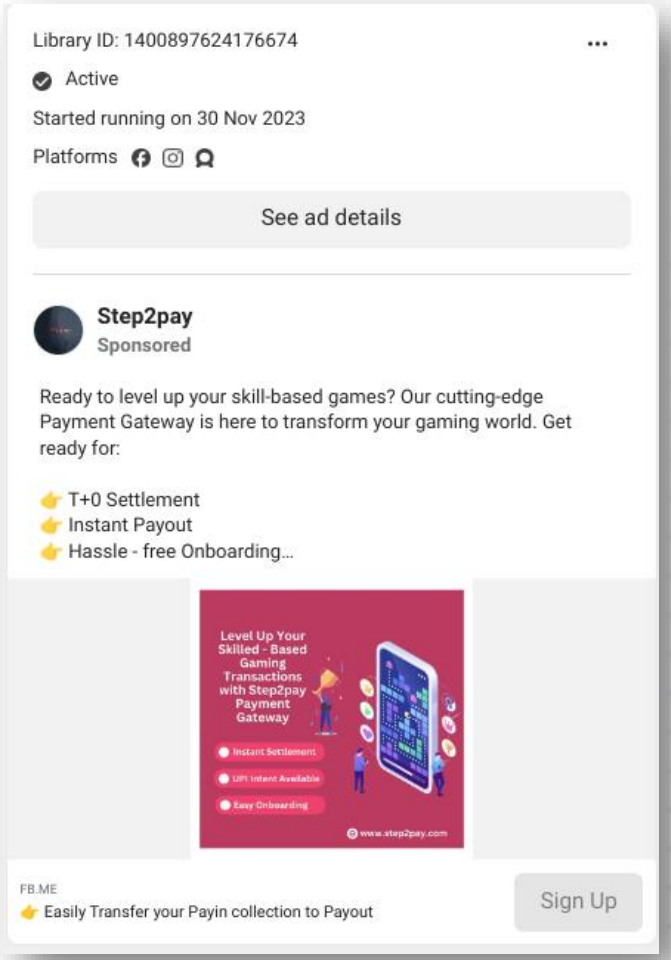
- Google & other search engine ads
- Emails & SMS

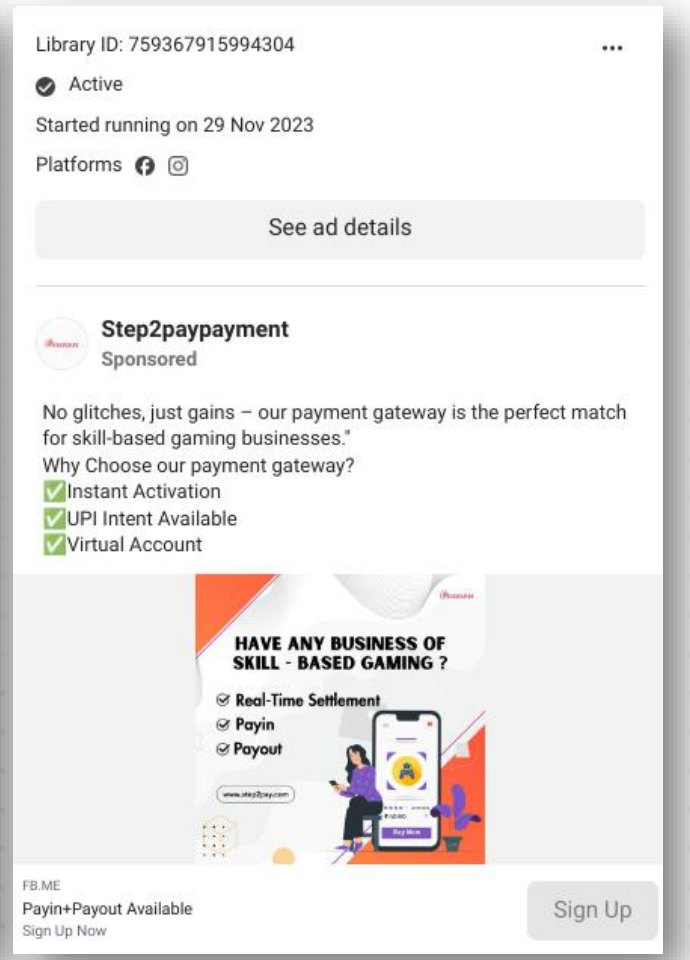


Mediums of Distribution (2)

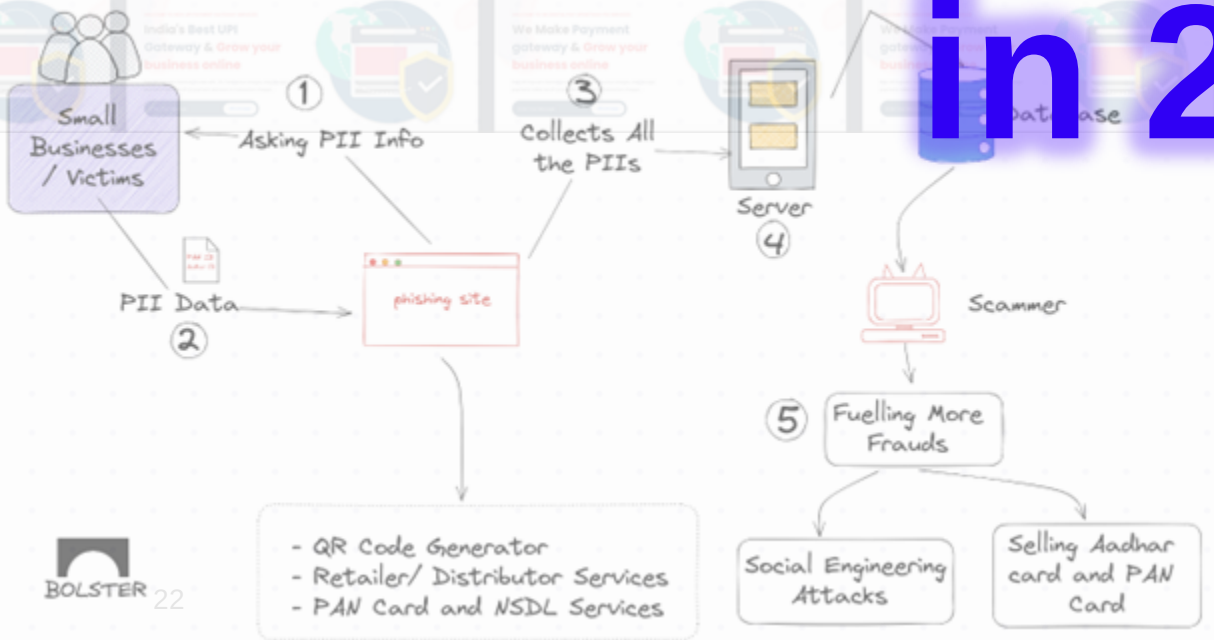
Social media including:

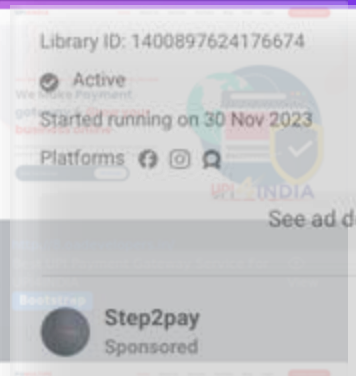
- Facebook/ Facebook Ads
- Instagram
- Twitter
- TikTok
- YouTube

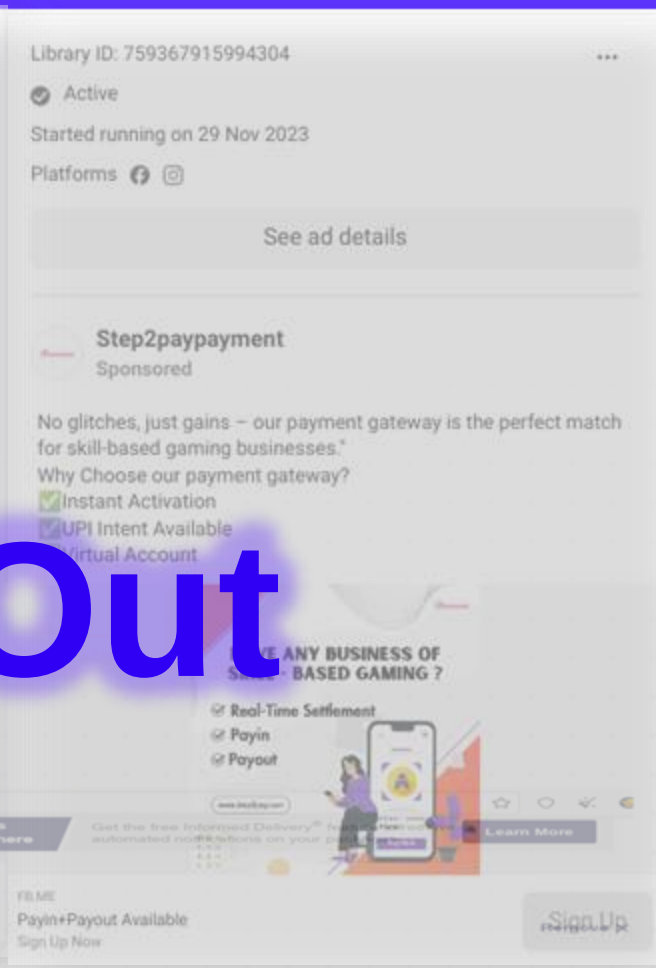


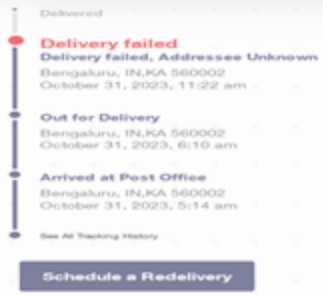


Scams to Watch Out in 2024









Improvised Technique: Usage of Various Freemium SaaS

WHY

- ❑ Less technical complexity
- ❑ Less investment more profit
- ❑ Wide range of deployment of phishing-kits

- repl.co
- glitch.me
- github.io
- gitbook.io
- pantheonsite.io
- webflow.io
- vercel.app
- web.app

Service Providers

Classic Technique: Typosquatting

Source URL	URL Construction	Risk	Live Scan Verdict	Category	IP Address	Name Servers	Mail Servers	MX Records	Registration Date	Registrar	SSL Certificate	Takedown Inquiry
amazoo.org	Scan	3	Suspicious	Unknown	104.21.0.156	dawn.ns.cloudflare.com; igor.ns.cloudflare.com	--	False	17-Jul-2019	Name.com...	--	--
ymazon.com	Scan	3	Suspicious	Unknown	3.33.139.32	ns1.markmonitor.com. ns5.markmonitor.com. ns4.markmonitor.com. ns3.markmonitor.com.	--	False		--	--	--
amazzon.org	Scan	3	Suspicious	Domain ...	162.255.119.185	dns1.registrar-servers.com; dns2.registrar-servers.com	eforward5.registrar-servers.com eforward4.registrar-servers.com eforward1.registrar-servers.com eforward2.registrar-servers.com eforward3.registrar-servers.com	True	29-Mar-20...	NameChe...	--	--
amazonn.xyz	Scan	2	Suspicious	Unknown	15.197.148.33	ns47.domaincontrol.com. ns48.domaincontrol.com.	aspmx.l.google.com alt1.aspmx.l.google.com alt2.aspmx.l.google.com alt3.aspmx.l.google.com alt4.aspmx.l.google.com	True		--	GoDaddy.com, Inc.	--
amazons.xyz	Scan	3	Suspicious	Domain ...	3.64.163.50	NS1.BODIS.COM; NS2.BODIS.COM	--	False	14-Jul-2021	Edomains ...	Let's Encrypt	--
amazonm.net	Scan	3	Suspicious	Unknown	--	NS-CLOUD-D1.GOOGLEDOMAINS.COM; NS-CLOUD-D2.GOOGLEDOMAINS.COM; NS-CLOUD-D3.GOOGLEDOMAINS.COM; NS-CLOUD-D4.GOOGLEDOMAINS.COM	mx01.1and1.com mx00.1and1.com	True	16-Jun-20...	Google LLC	--	--
amazof.com	Scan	3	Suspicious	Unknown	--	NS1.AMZNDNS.CO.UK; NS1.AMZNDNS.COM; NS1.AMZNDNS.NET; NS1.AMZNDNS.ORG; NS2.AMZNDNS.CO.UK; NS2.AMZNDNS.COM; NS2.AMZNDNS.NET; NS2.AMZNDNS.ORG	--	False	13-Apr-20...	MarkMonit...	--	--
amazo.com	Scan	2	Suspicious	Unknown	--	ns-57.awsdns-07.com. ns-1995.awsdns-57.co.uk. ns-1015.awsdns-62.net. ns-1476.awsdns-56.org.	--	False		--	--	--
amazons.io	Scan	3	Clean	Unknown	3.64.163.50	ns1.dan.com. ns2.dan.com.	--	False		--	Let's Encrypt	--
aamzon.com	Scan	1	Clean		15.197.245.13	NS1.AMZNDNS.CO.UK; NS1.AMZNDNS.COM; NS1.AMZNDNS.NET; NS1.AMZNDNS.ORG; NS2.AMZNDNS.CO.UK; NS2.AMZNDNS.COM; NS2.AMZNDNS.NET; NS2.AMZNDNS.ORG	--	False	20-Jul-1998	MarkMonit...	DigiCert Inc	--
amazon.io	Scan	2	Clean	Unknown	3.33.172.98	ns1.amzndns.net. ns1.amzndns.com. ns2.amzndns.co.uk. ns1.amzndns.co.uk. ns2.amzndns.net. ns1.amzndns.org.	--	False		--	Amazon	--

Provider	Count		
	Phish	Scam	Suspicious
repl.co	26011	399	528033
glitch.me	29654	1087	147436
github.io	69548	4727	37616
gitbook.io	21916	64700	145164
pantheonsite.io	3417	2800	33426
webflow.io	3252	4073	43732
vercel.app	13403	4205	135683
web.app	89766	18398	524476

*Source: Classified data from CheckPhish commencing Jan 1,2023

https://abhi-shek1289.gith... Phish Dispute Pivot DOM VIEW WHOIS INFORMATION

Scan Results

Source URL:
https://abhi-shek1289.github.io/Netflix-clone/

Brand:
Netflix

Redirected URL:
https://abhi-shek1289.github.io/Netflix-clone/

IP Address:
185.199.111.153

Hosting Provider:
Fastly

First Seen:
December 7th 2023, 3:18:59 pm

Category:
Streaming

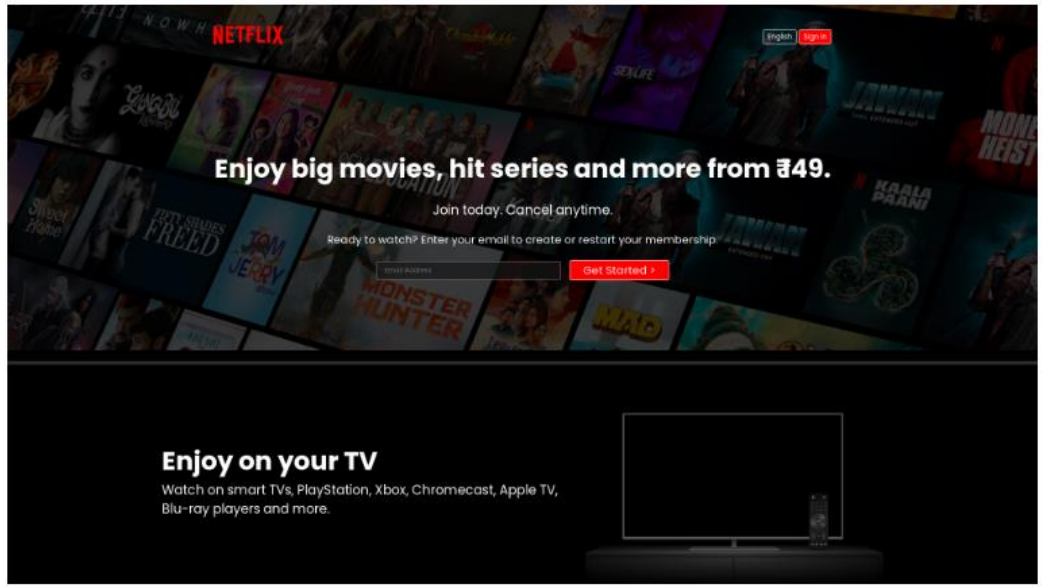
ASN:
54113

Location:
United States

Abuse Contact:
abuse@github.com

Certificate Details:
DigiCert Inc: *.github.io, github.io, *.github.com, github.com, www.github.com, *.githubusercontent.com, gi...

Screenshot



https://dev-doore.pantheo... Phish Dispute

Pivot DOM VIEW WHOIS INFORMATION

Scan Results

Source URL:
https://dev-doore.pantheonsite.io/qqqdayEJKne...

Brand:
Microsoft

Redirected URL:
https://dev-doore.pantheonsite.io/qqqdayEJKnewwt....

IP Address:
23.185.0.2

Hosting Provider:
Fastly

First Seen:
December 13th 2023, 3:52:11 pm

Category:
Unknown

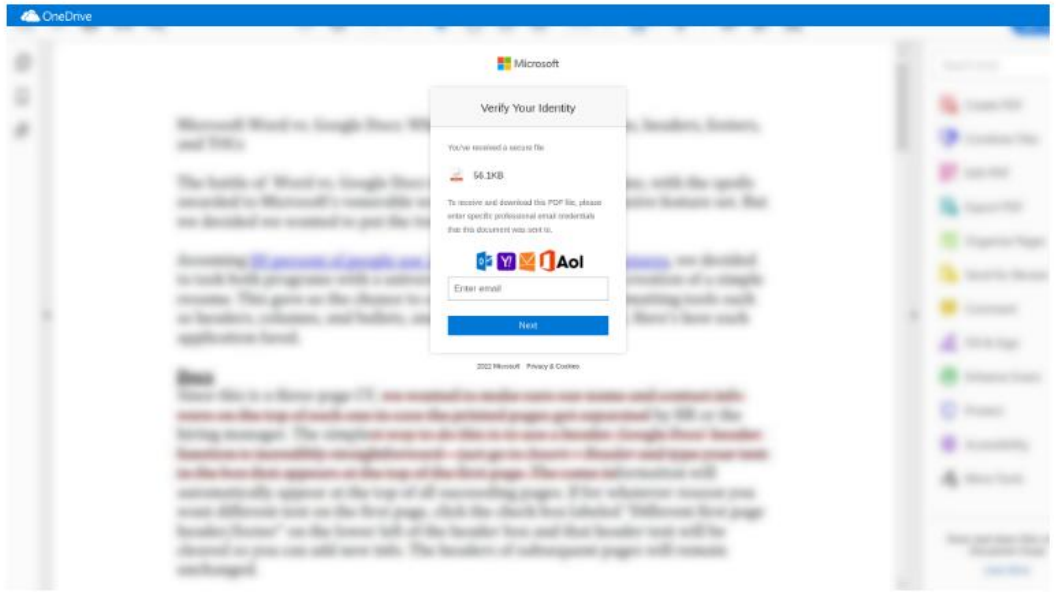
ASN:
54113

Location:
United States

Abuse Contact:
david@davidstrauss.net

Certificate Details:
Sectigo Limited: pantheonsite.io, *.getpantheon.com, *.gotpantheon.com, *.pantheon.io, *.pantheonsite.io, ...

Screenshot

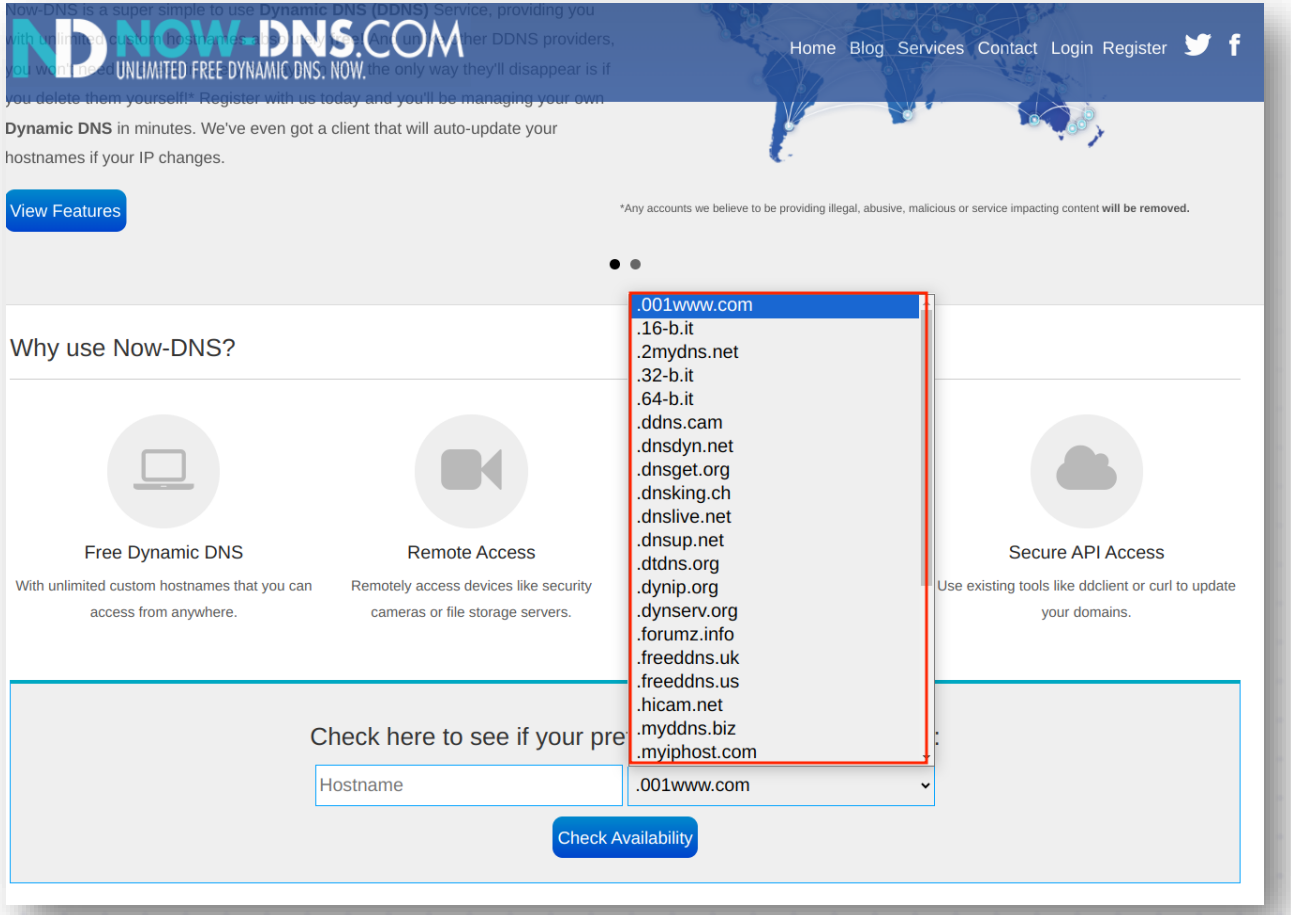


BOLSTER

Improvised Technique: Abuse of Dynamic DNS Services

WHY

- ❑ Simple hosting of content
- ❑ Multiple hostname availability
- ❑ No investment



BOLSTER

Benefits of Now-DNS.com

Free Dynamic DNS

With unlimited custom hostnames that you can access from anywhere.

Remote Access

Remotely access devices like security cameras or file storage servers.

Updater Client

Automatically update your DNS whenever your IP changes.

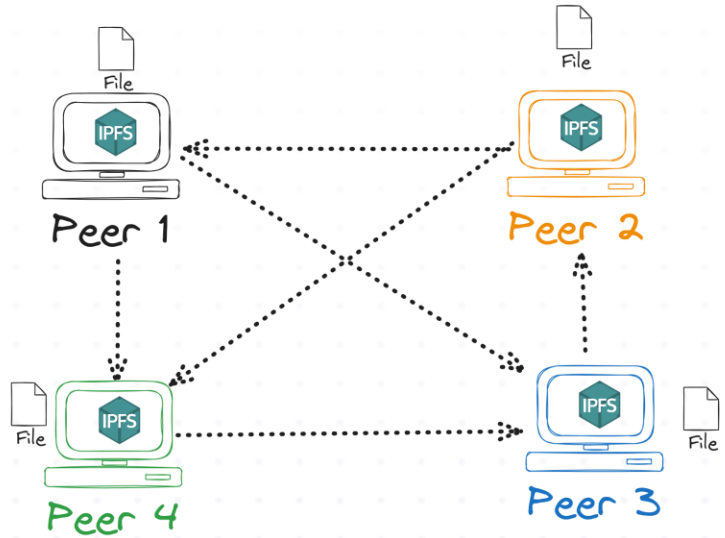
Secure API Access

Use existing tools like ddclient or curl to update your domains.

Improvised Technique: InterPlanetary File System(IPFS)

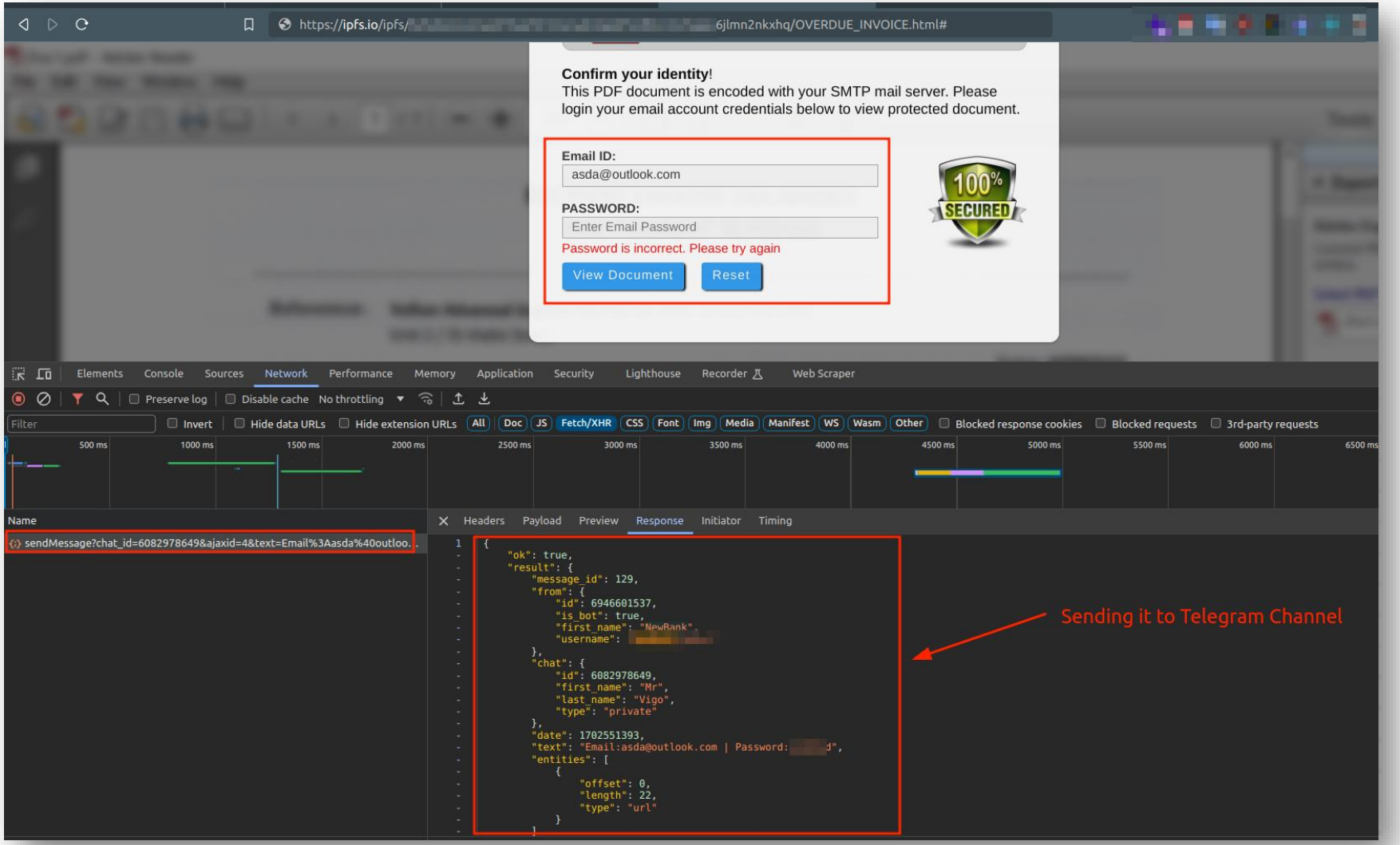
WHY

- ❑ Easy to Set Up
- ❑ Free to Use
- ❑ Less Regulations



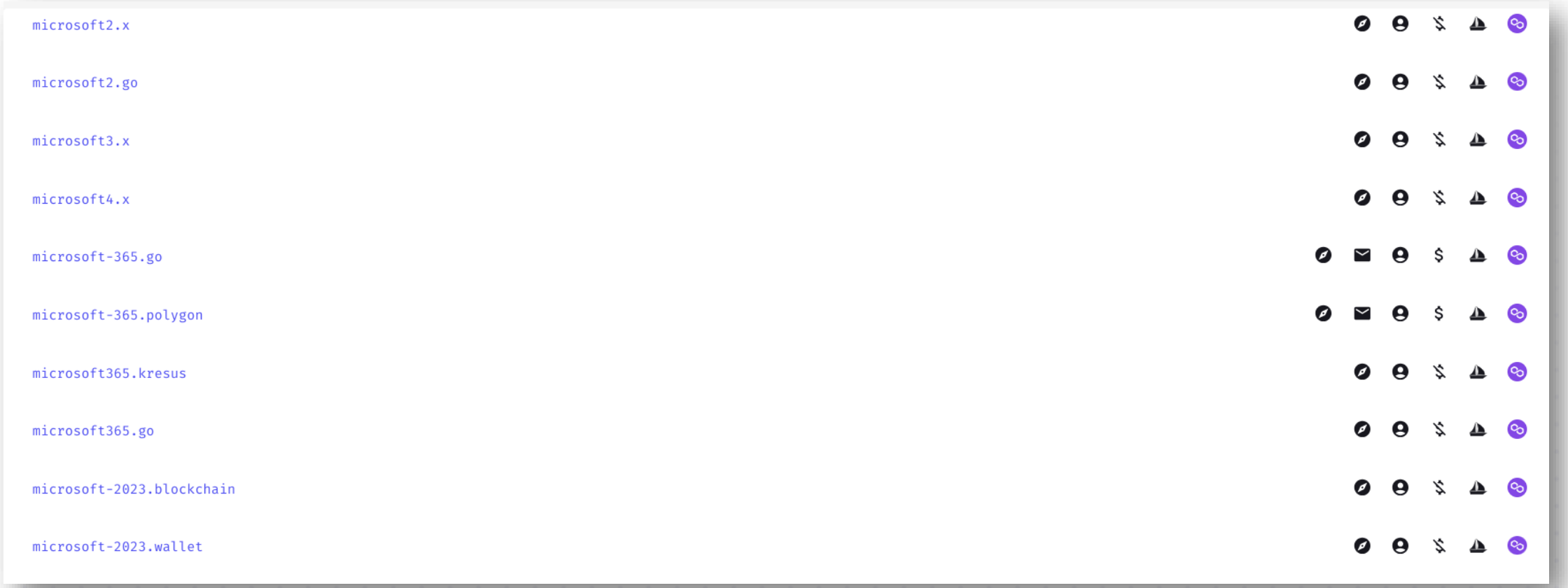
BOLSTER

A Latest Case Study: Data Exfiltration via Telegram Bot



BOLSTER

Improvised Technique: Crypto Domains



BOLSTER

Detecting to Scale

Detecting to Scale: Need for a Machine Learning/ Deep Learning Solution

- **Image-based Signals**
  - Screenshot of the webpage
  - Favicon
  - Logo
- **Text-based Signals**
  - Text on the webpage
  - Copyright
  - Key DOM elements

Criteria

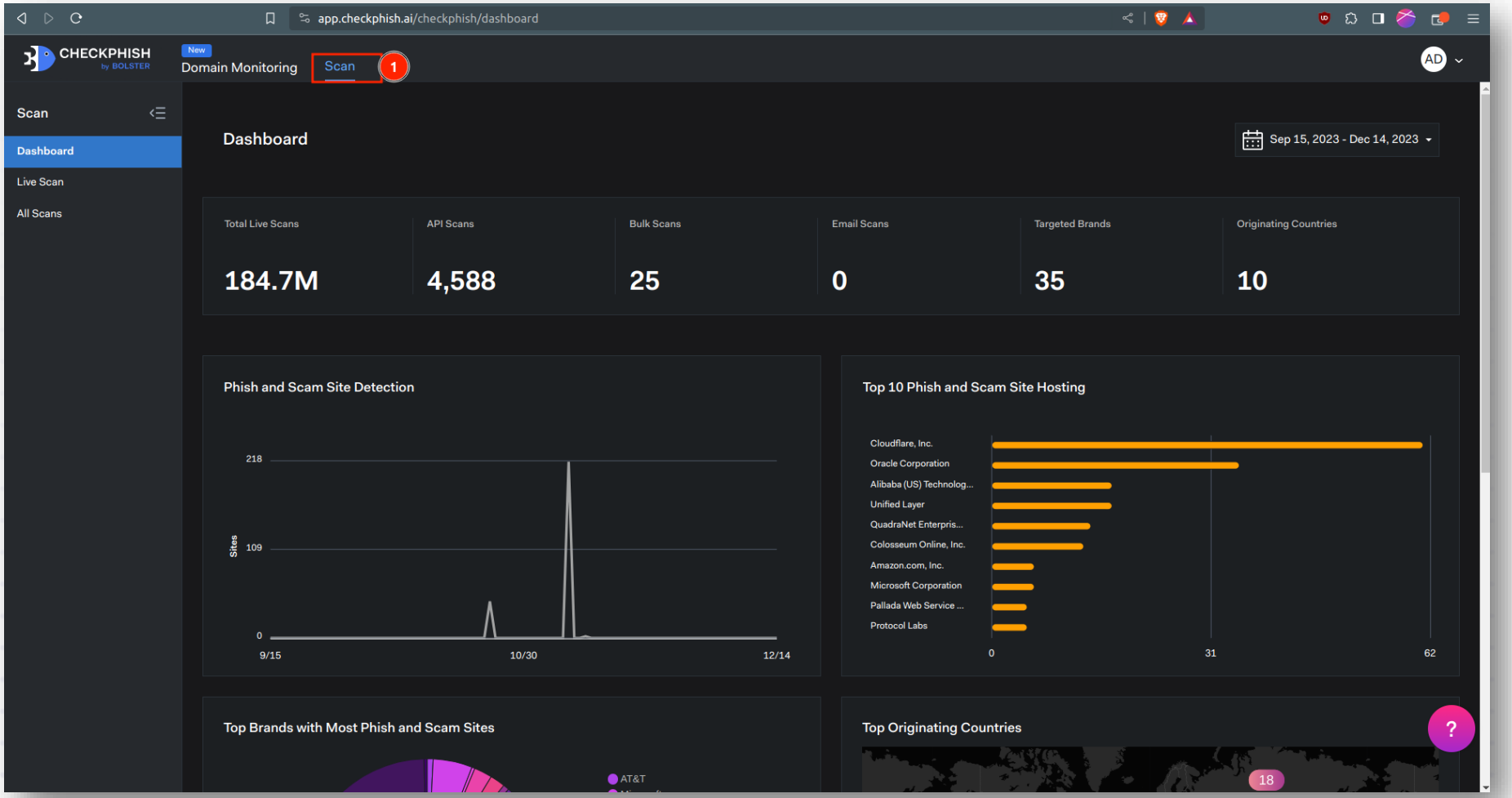
✓ **Speed**
Detection in under 100ms

✓ **False Positive Rate**
Less than 1 in 100,000 are False Positives

✓ **Scalability**
Ability to scale detection to thousands of different types of fraud

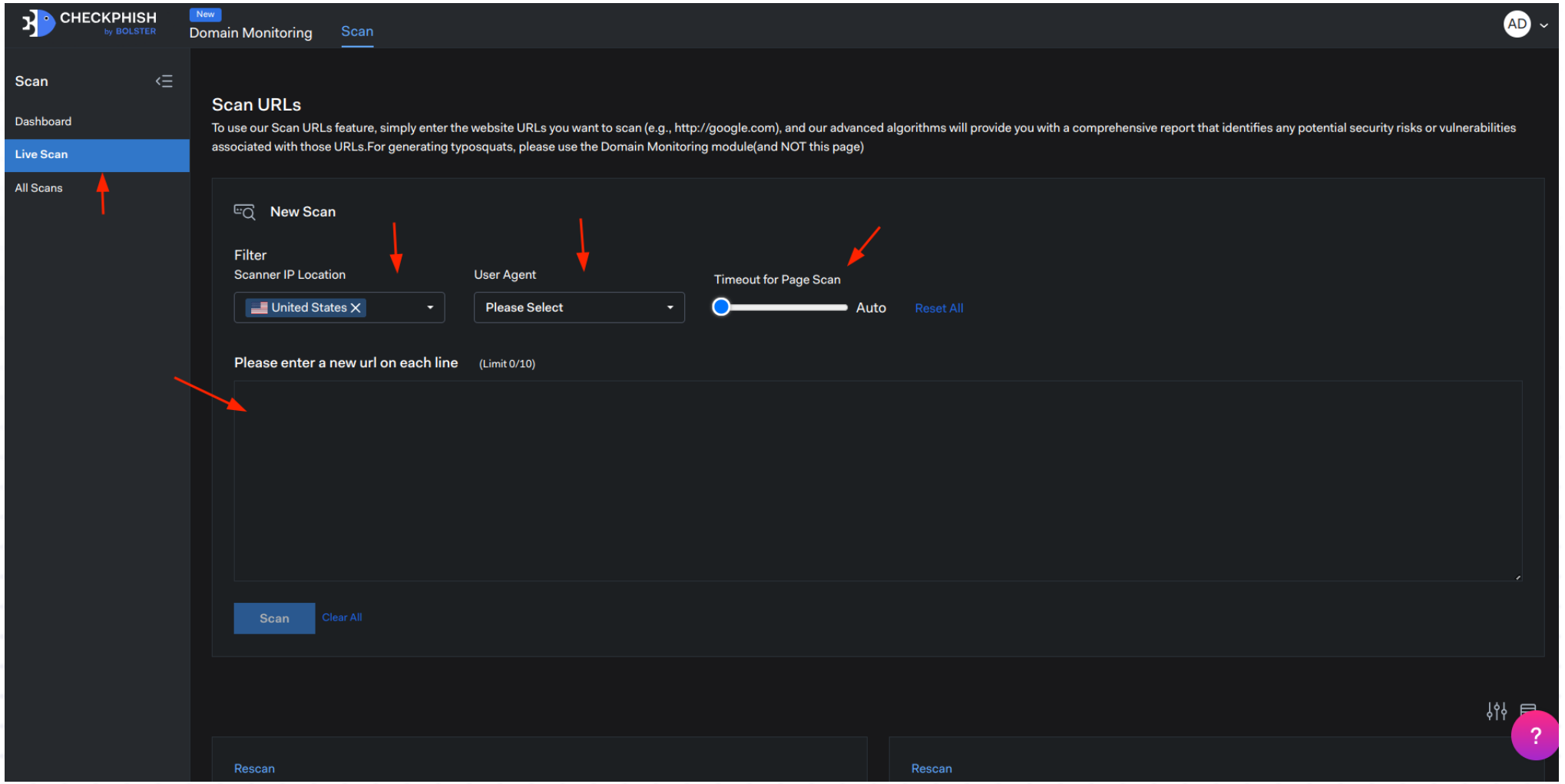
** There are other signals that can be used to train and uncover fraud on the web*

Introducing CheckPhish.ai



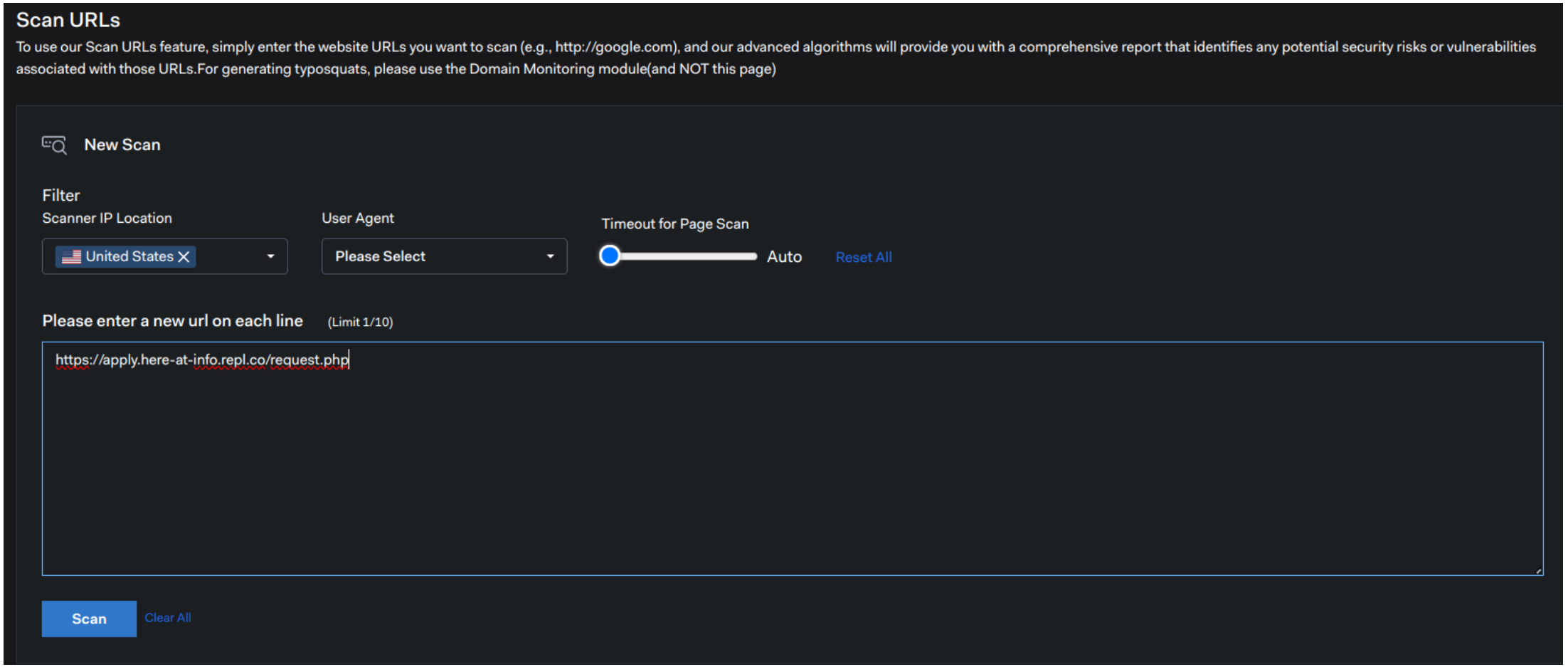
BOLSTER

Performing a Live Scan

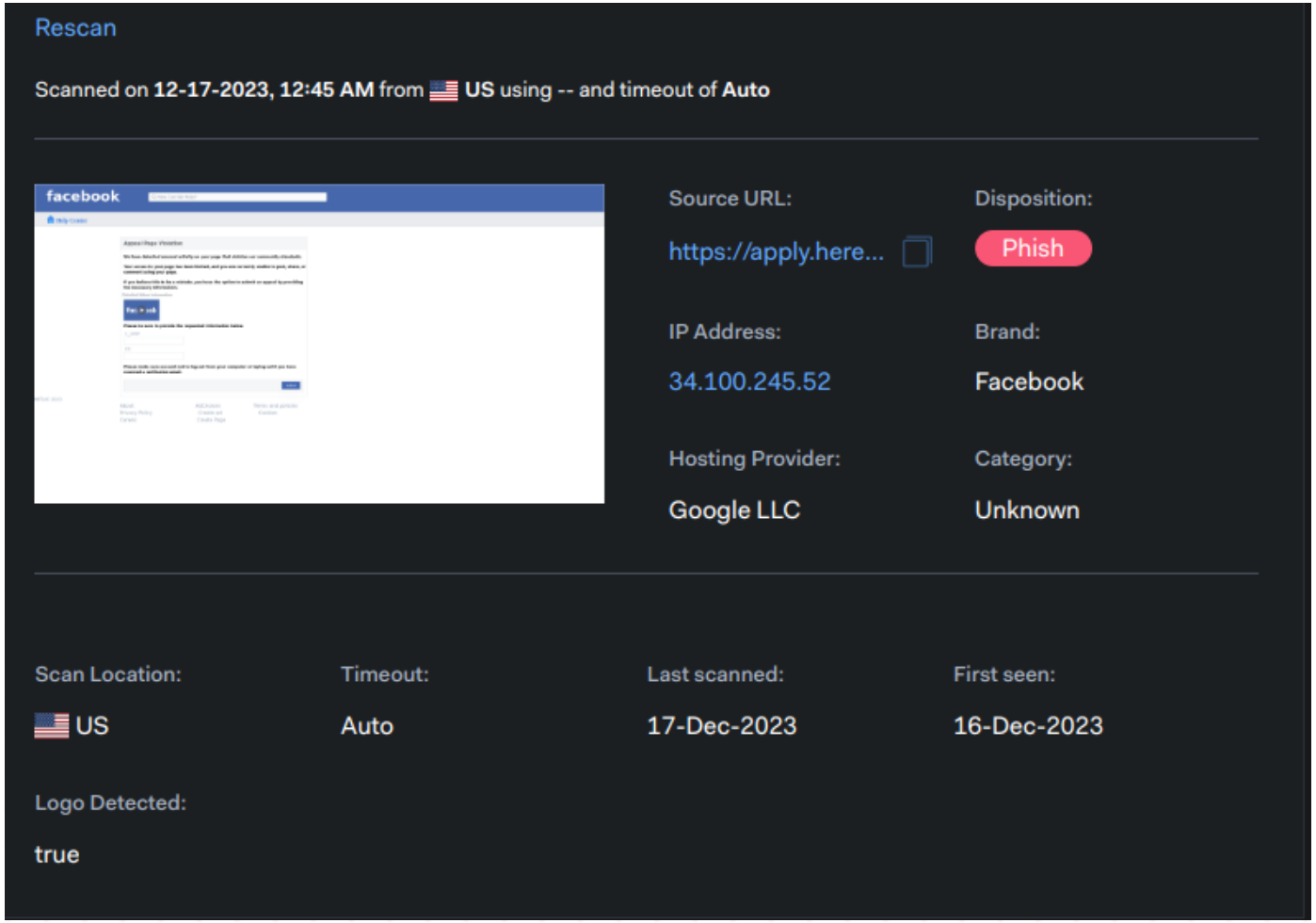


BOLSTER

Performing a Live Scan

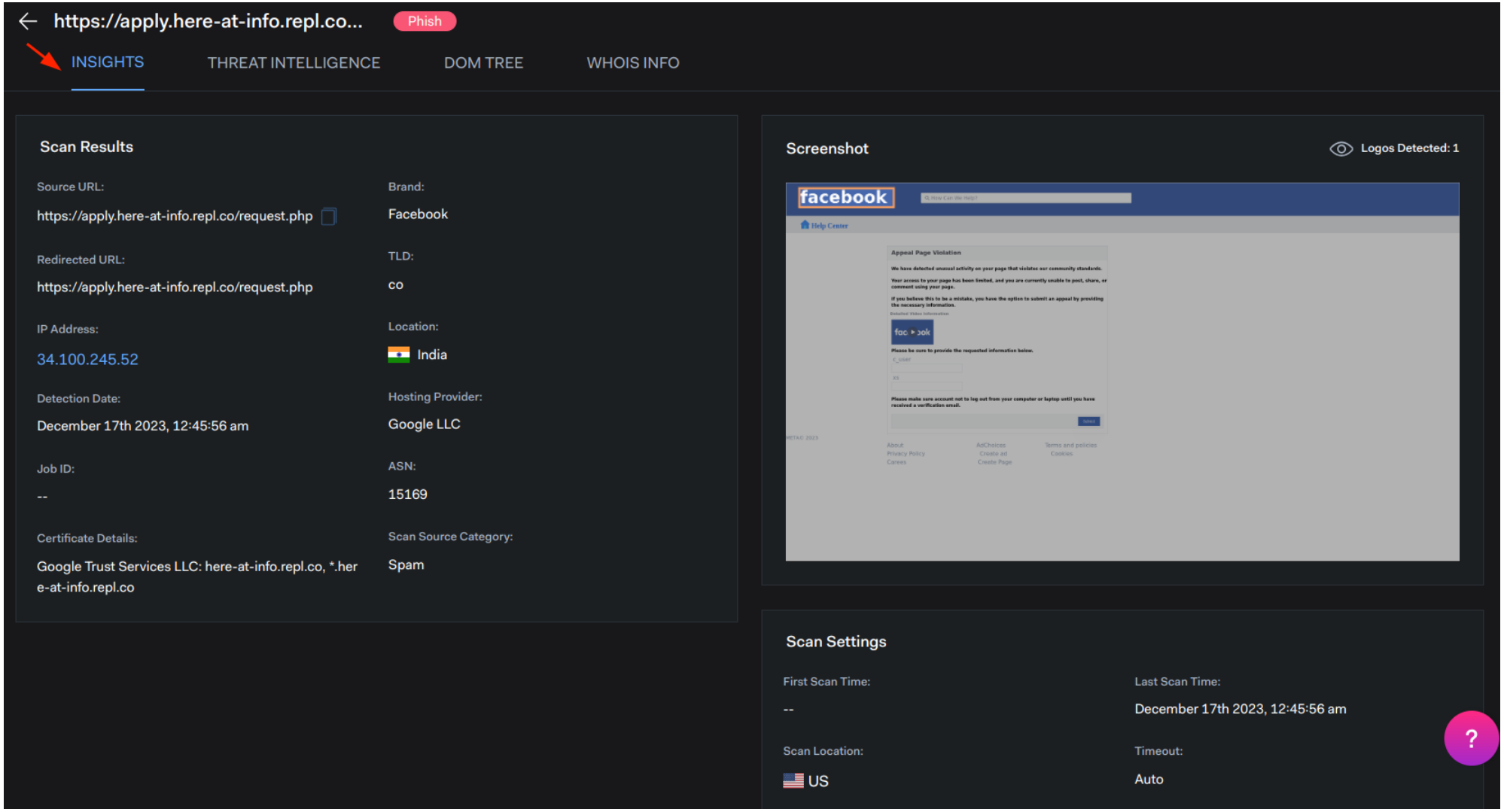


Performing a Live Scan



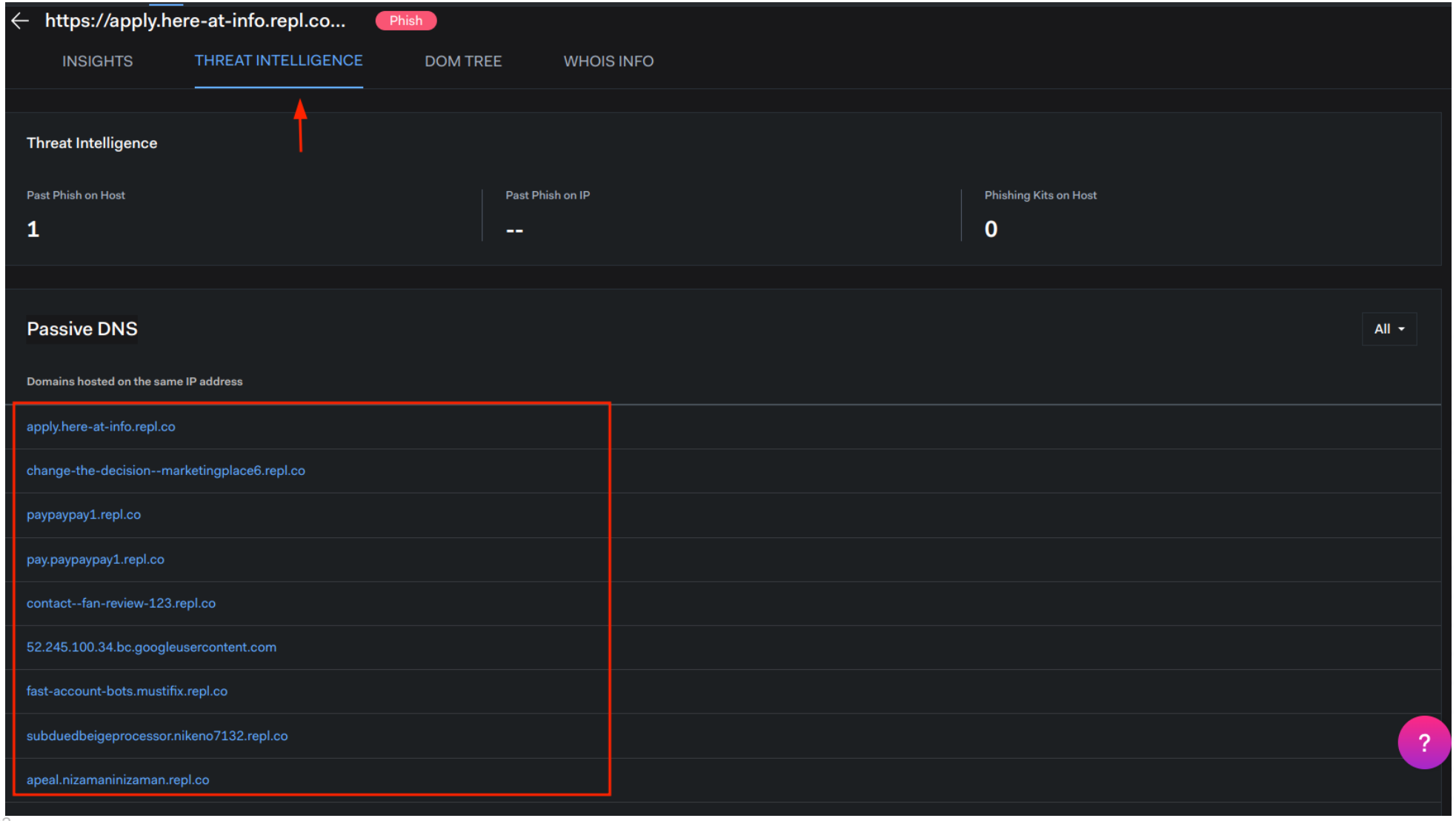
BOLSTER

Performing a Live Scan: Insights



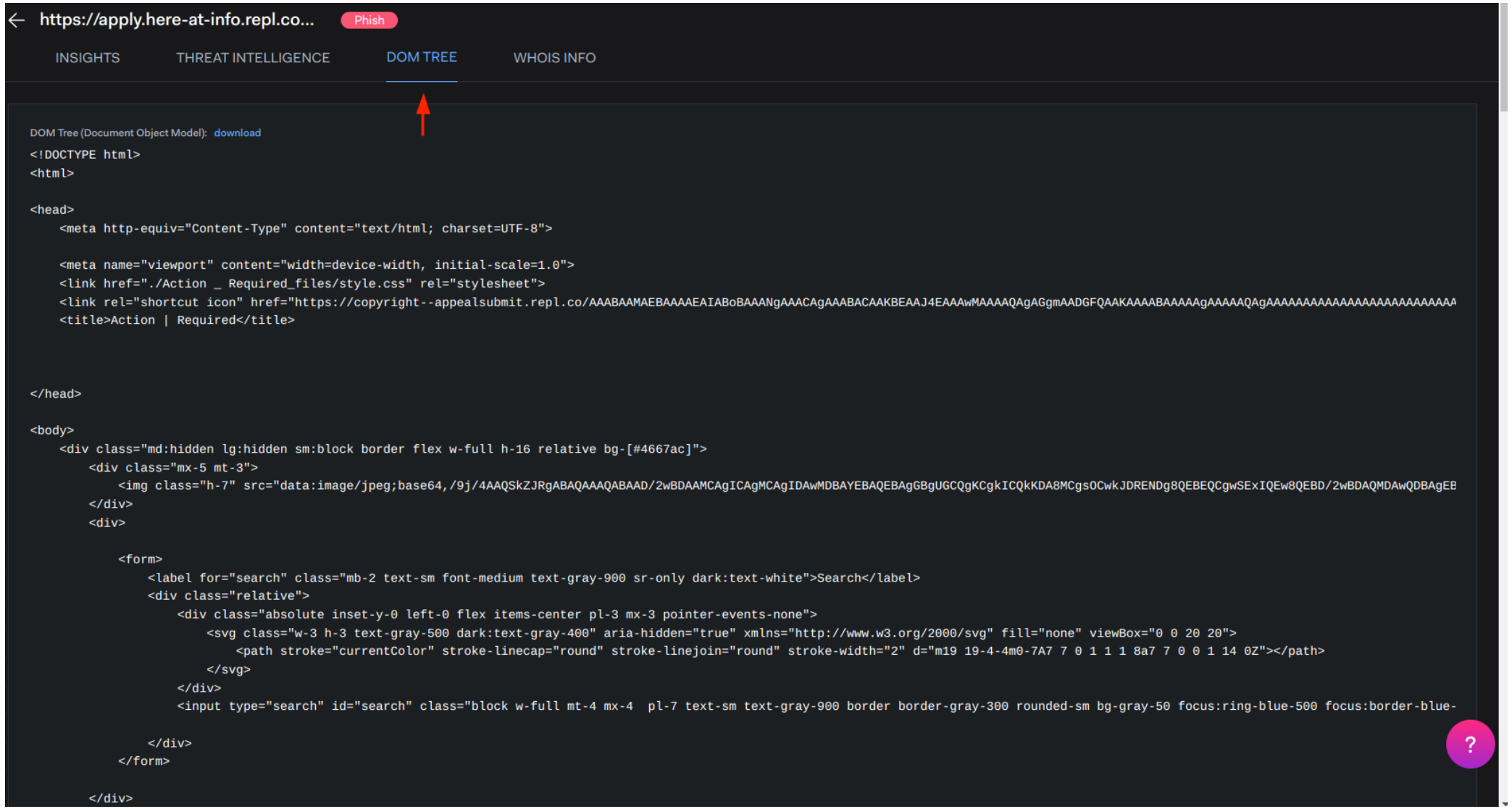
BOLSTER

Performing a Live Scan: Threat Intelligence



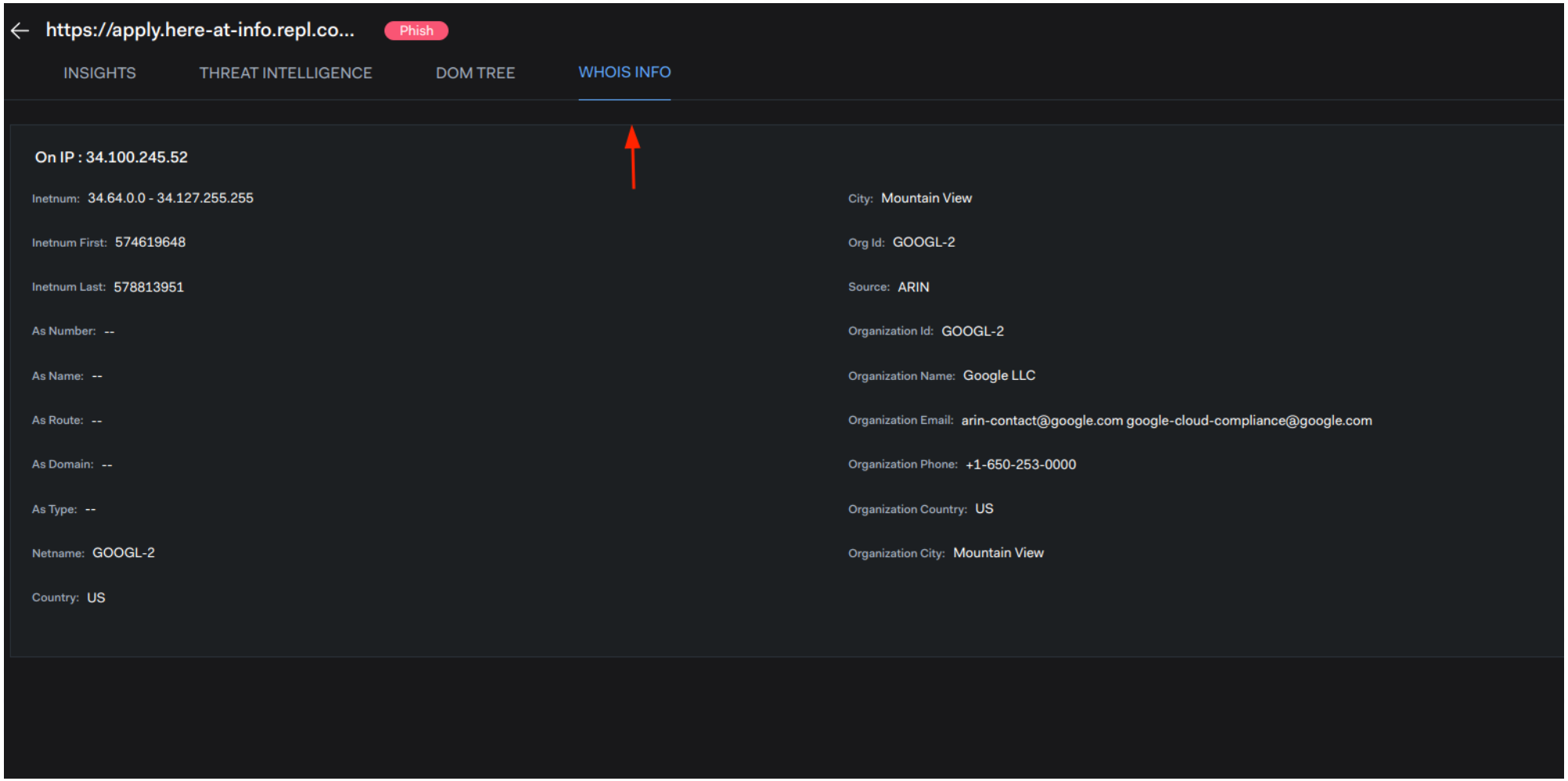
BOLSTER

Performing a Live Scan: DOM Tree

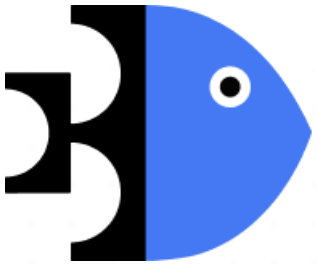


BOLSTER

Performing a Live Scan: WHOIS Info



Wanna be a Threat Hunter for a Day… ??



CHECKPHISH CTF

by BOLSTER

Register at: https://ctf.checkphish.ai
Start Time: 17th December 2023 2PM IST
End Time: 18th December 2023 2PM IST

For Queries/Doubts: Join **DEF CON DELHI GROUP** DC Server[Channel Name: **#checkphish_ctf_2023**

Questions?