

**How many of you have  
received/seen such  
SMS?**

Dear 'S.B.I' User,

Your S.B.I\_YONO' Account will  
be blocked today. Please  
update Self PAN-Card  
immediately.

'Click on the link below.'

<https://clzg.short.gy/5b>

Dear 'S.B.I' User,

Your S.B.I\_YONO' Account will  
be blocked today. Please  
update Self PAN-Card  
immediately.

'Click on the link below.'

<https://clzg.short.gy/5b>

Alert Your 5899 Reward Point  
got Expired Redeem Now

[bit.ly/3WK5hfG](https://bit.ly/3WK5hfG)

Warm Regard HDFC  
MD Shiv Saran

Dear 'S.B.I' User,

Your S.B.I\_YONO' Account will be blocked today. Please update Self PAN-Card immediately.

'Click on the link

<https://clzg.sho>

Alert Your 5899 Reward Point got Expired Redeem Now

[Link To My ECR](#)

To validate your mobile number in CVL KRA as per SEBI guidelines, click on <https://otpdelivery.cvlindia.com/EMOTP?auth=S1>

## 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 →](#)

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

[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](#)



## Accepting Payments Made Easy, Simple & FREE!

The logos below are the property of respective trademark owners. All the below apps support BHIM-UPI.



Accept  
you  
:

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

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

Get Started →



### Transaction Charge

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

Call to action →

UPI Gateway

Home Pricing Contact Login



gin Register Paytm

e & FREE!

BHIM-UPI

Amazon pay

WhatsApp

GetButton



# 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

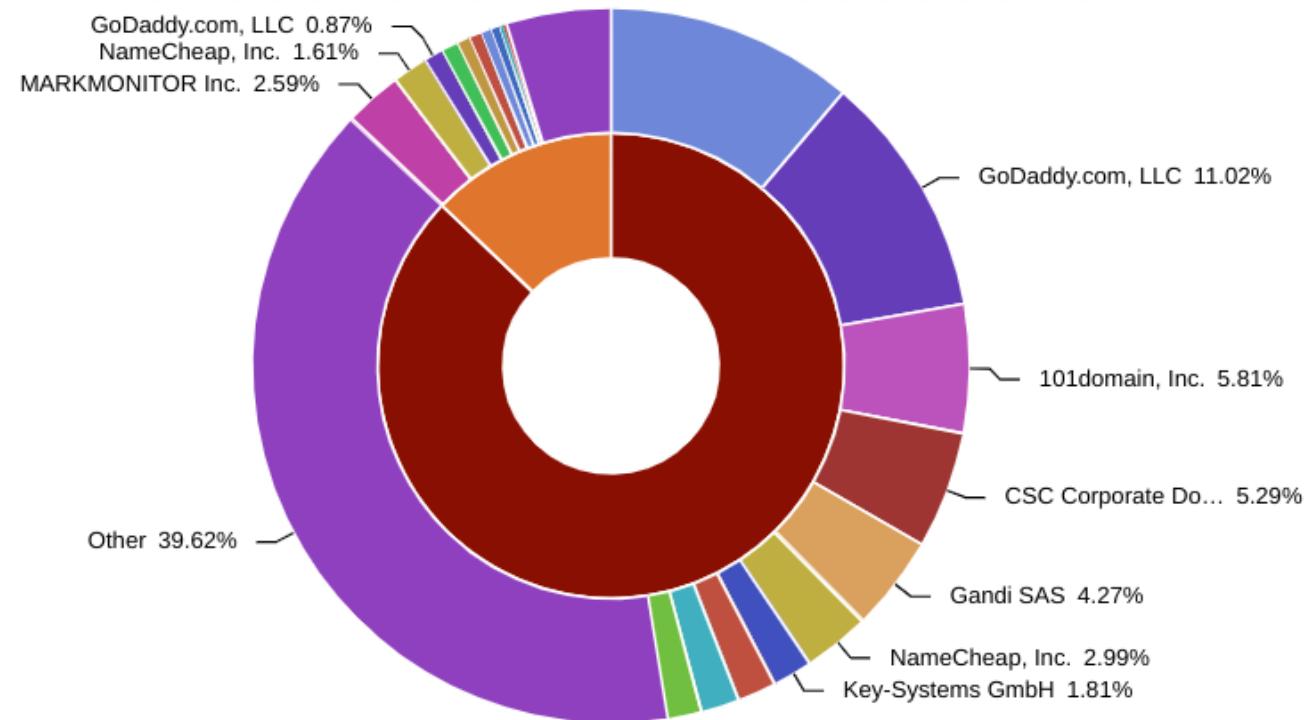
**> 10.3 Million**

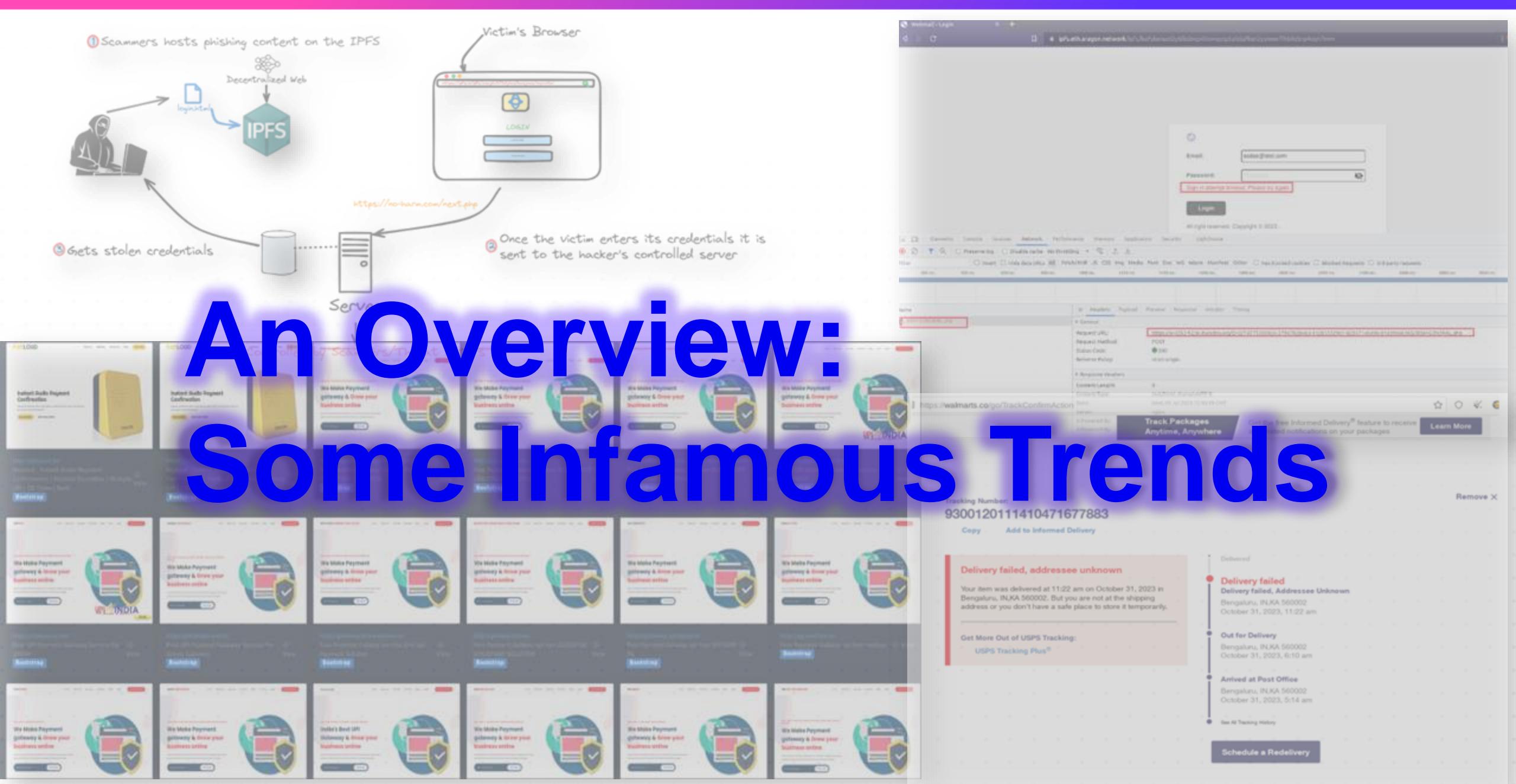
Scam URLs

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

# Top Domain Registrar: Scam and Phishing Domains

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





# An Overview: Some Infamous Phishing/Scam Campaign



## Abusing Decentralized Web

- ❑ Blockchain – IPFS
- ❑ Free to use
- ❑ Less Regulations

Webmail - Login

ipfs.eth.argon.network/index.php?bdfbcbfaz2y6lbbcpbkwxpop5a5defkpr2yyioee7hb4zrp4xon7mm

Email: asdas@test.com

Password:

Sign in attempt timeout. Please try again.

Login

All right reserved. Copyright © 2023.

Network

Name: index.php

Request URL: https://e-332-4216.duckdns.org:0/74731105916-1794202460-41281132901-8395714d49-0143966365/05H-GJN384L.php

Request Method: POST

Status Code: 200

Referrer Policy: strict-origin

Content-Length: 0

Content-Type: text/html; charset=UTF-8

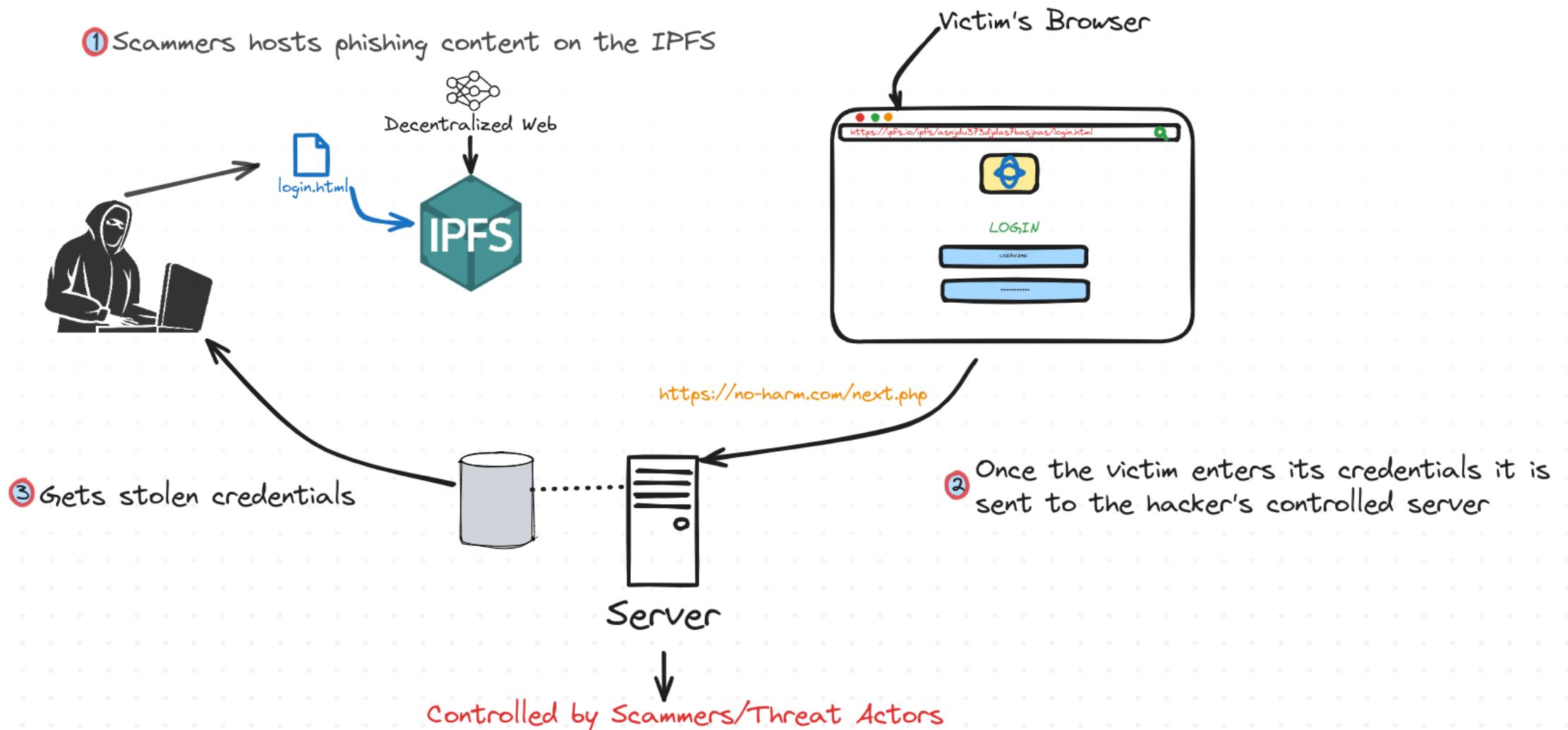
Date: Wed, 05 Jul 2023 12:50:19 GMT

Server: nginx

X-Powered-By: PHP/7.4.33

X-Powered-By: PleskLin

# How it works



# An Overview: Some infamous Phishing/Scam Campaign



## Impersonation of Payment Gateways

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

**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.

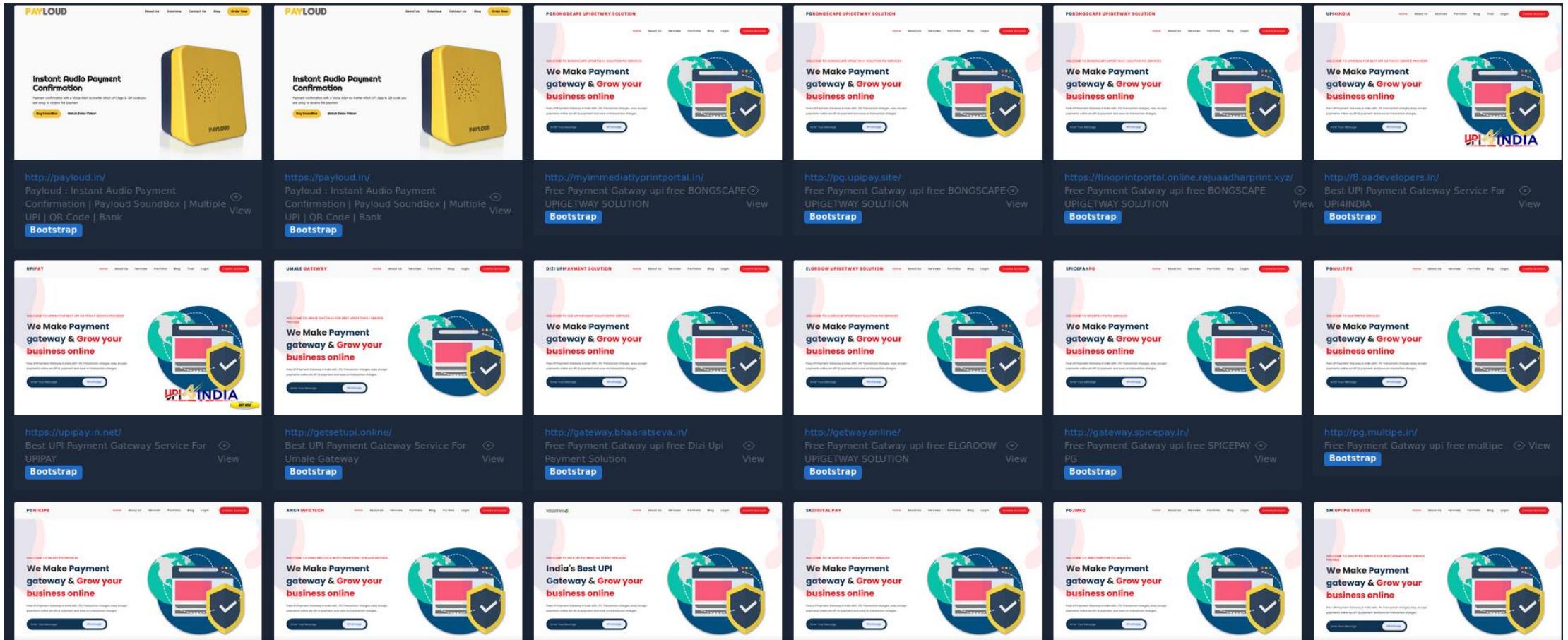
⚡ Try for free

**Accepting Payments Made Easy, Simple & FREE!**

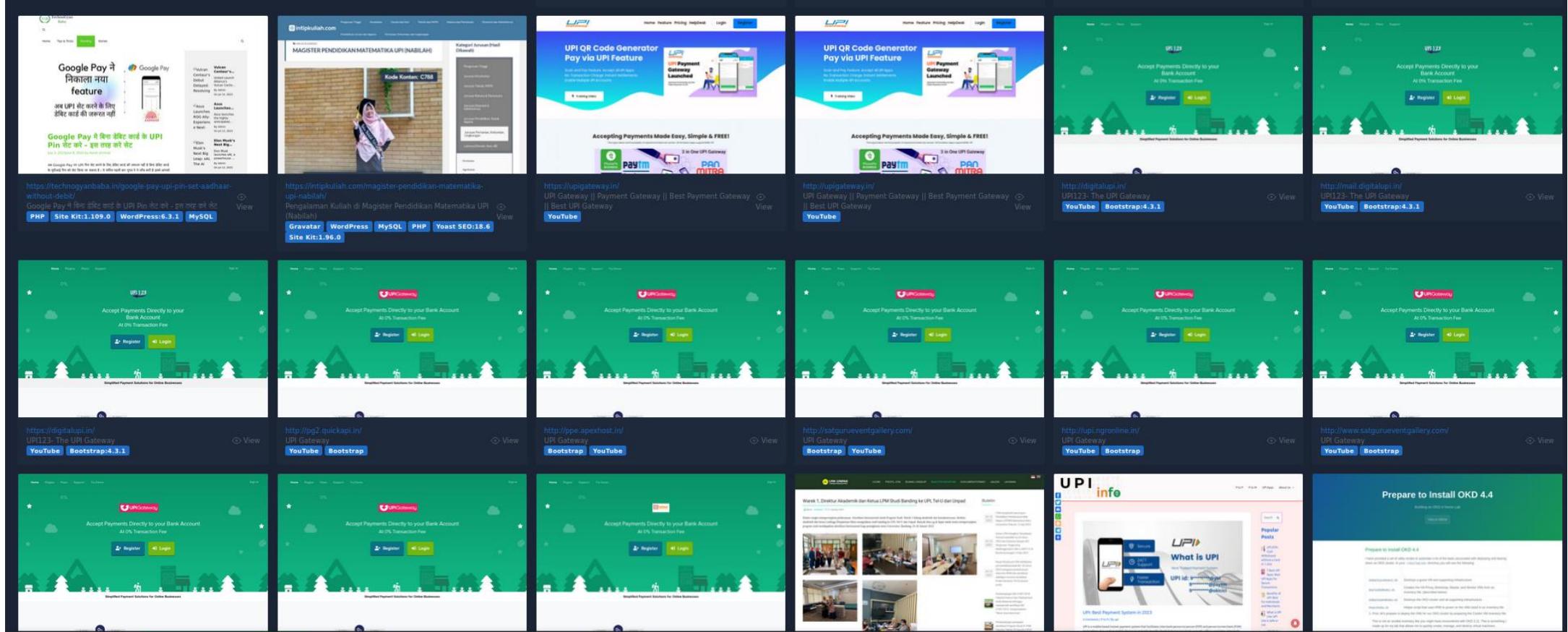
The logos below are the property of respective trademark owners. All the below apps support BHIM-UPI

PhonePe G Pay amazon pay GetButton

# Similar Looking Phishing Sites !!?



# Some More...





②

- QR Code Generator
- Retailer/ Distributor Services
- PAN Card and NSDL Services

③  
Collects All  
the PIIs

④  
Server

Database

Scammer

⑤  
Fuelling More  
Frauds

Social Engineering  
Attacks

Selling Aadhar  
card and PAN  
card

# An Overview: Some infamous Phishing/Scam Campaign



## Shipment Scam Campaigns

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

The screenshot shows a tracking page for a package with tracking number 9300120111410471677883. The page includes a message about a failed delivery due to an unknown addressee. A timeline on the right shows the package was delivered to Bengaluru, India, on October 31, 2023, at 11:22 am, but it failed to reach the intended recipient.

Tracking Number:  
9300120111410471677883

Copy Add to Informed Delivery

**Delivery failed, addressee unknown**

Your item was delivered at 11:22 am on October 31, 2023 in Bengaluru, IN, KA 560002. But you are not at the shipping address or you don't have a safe place to store it temporarily.

Get More Out of USPS Tracking:  
USPS Tracking Plus®

Timeline:

- Delivered
- Delivery failed  
Delivery failed, Addressee Unknown  
Bengaluru, IN, KA 560002  
October 31, 2023, 11:22 am
- Out for Delivery  
Bengaluru, IN, KA 560002  
October 31, 2023, 6:10 am
- Arrived at Post Office  
Bengaluru, IN, KA 560002  
October 31, 2023, 5:14 am

Schedule a Redelivery

# Mediums of Distribution (1)

- Google & other search engine ads
- Emails & SMS

The screenshot shows two separate search results pages from ipfs.io.

**Search Results for "McDelivery":**

- 1. ipfs.io - [https://ipfs.io/ipfs/wiki/24\\_hour\\_McDelivery](https://ipfs.io/ipfs/wiki/24_hour_McDelivery) - **McDelivery**  
The delivery fee is usually A\$4.95 (US\$3.72) with a minimum order ... Japan. In Japan, McDelivery is available from 7 am to 11 pm, with a ¥300 (US\$2.48) delivery ...
- 2. ipfs.io - [https://ipfs.io/ipfs/wiki/Expert\\_Opinion\\_on\\_Dru...](https://ipfs.io/ipfs/wiki/Expert_Opinion_on_Dru...) - **Expert Opinion on Drug Delivery - IPFS**  
Expert Opinion on Drug Delivery is a monthly peer-reviewed medical journal publishing review articles covering all aspects of research on drug delivery ...

**Search Results for "ISO/IEC 9126":**

- 1. ipfs.io - [https://ipfs.io/ipfs/wiki/ISO\\_IEC\\_9126](https://ipfs.io/ipfs/wiki/ISO_IEC_9126) - **ISO/IEC 9126**  
The fundamental objective of the ISO/IEC 9126 standard is to provide a model for evaluating the quality of software products. It identifies six quality characteristics: functionality, reliability, usability, efficiency, maintainability, and portability. The standard also defines a set of human biases that can adversely affect the quality of software products.
- 2. ipfs.io - [https://ipfs.io/ipfs/wiki/TCS\\_Couriers](https://ipfs.io/ipfs/wiki/TCS_Couriers) - **TCS Courier**  
TCS has been assigned machine readable p...  
government, and Visa application submission
- 3. ipfs.io - [https://ipfs.io/ipfs/wiki/List\\_of\\_Microsoft\\_operat...](https://ipfs.io/ipfs/wiki/List_of_Microsoft_operat...) - **List of Microsoft operating systems - IPFS**  
List of Microsoft operating systems - MS-DOS - Windows - Windows NT - Windows CE - Windows Phone - Xbox gaming - OS/2 - Other operating systems.
- 4. ipfs.io - [http://ipfs.io/ipfs/wiki/Microsoft\\_Office\\_365](http://ipfs.io/ipfs/wiki/Microsoft_Office_365) - **Office 365**  
Personal: Includes access to Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft OneNote, Microsoft Outlook, Microsoft Publisher & Microsoft ...
- 5. ipfs.io - <https://ipfs.io/ipfs/> - **Microsoft OneDrive - IPFS**  
Microsoft | OneDrive. One Drive Document. Total file size: 27.59 MB. All Files Are Ready To Download. Product Quantity.xls. 1.9mb. Open File. Specific products ...
- 6. ipfs.io - <https://ipfs.io/ipfs/space/microsoft> - **Microsoft (Henry Spencer)**  
... Microsoft." -- John Denker >> Wonderful. :) > >Who is John Denker? Senior networking guy at AT&T Shannon Labs, and a prominent early adopter of the Linux ...

# Mediums of Distribution (2)

## Social media including:

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

Library ID: 1400897624176674 ...

Active

Started running on 30 Nov 2023

Platforms

[See ad details](#)

Step2pay Sponsored

Ready to level up your skill-based games? Our cutting-edge Payment Gateway is here to transform your gaming world. Get ready for:

- 👉 T+0 Settlement
- 👉 Instant Payout
- 👉 Hassle-free Onboarding...

FB.ME

👉 Easily Transfer your Payin collection to Payout

[Sign Up](#)

Library ID: 759367915994304 ...

Active

Started running on 29 Nov 2023

Platforms

[See ad details](#)

Step2payment Sponsored

No glitches, just gains – our payment gateway is the perfect match for skill-based gaming businesses.\*

Why Choose our payment gateway?

- Instant Activation
- UPI Intent Available
- Virtual Account

FB.ME

Payin+Payout Available

Sign Up Now

[Sign Up](#)

# Scams to Watch Out in 2024



- QR Code Generator
- Retailer/ Distributor Services
- PAN Card and NSDL Services

Social Engineering Attacks

Selling Aadhar card and PAN Card

# 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
<input type="checkbox"/>	amazoo.org	Scan	3	Suspicious	Unknown	104.21.0.156	dawn.ns.cloudflare.com; igor.ns.cloudflare.com	--	False	17-Jul-2019	Name.com...	--	--
<input type="checkbox"/>	ymazon.com	Scan	3	Suspicious	Unknown	3.33.139.32	ns1.markmonitor.com; ns5.markmonitor.com; ns4.markmonitor.com; ns3.markmonitor.com.	--	False	--	--	--	--
<input type="checkbox"/>	amazonz.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...	--	--
<input type="checkbox"/>	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.	--	--
<input type="checkbox"/>	amazons.xyz	Scan	3	Suspicious	Domain ...	3.64.163.50	NS1.BODIS.COM; NS2.BODIS.COM	--	False	14-Jul-2021	Edomains...	Let's Encrypt	--
<input type="checkbox"/>	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	--	--
<input type="checkbox"/>	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...	--	--
<input type="checkbox"/>	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	--	--	--	--
<input type="checkbox"/>	amazons.io	Scan	3	Clean	Unknown	3.64.163.50	ns1.dan.com. ns2.dan.com.	--	False	--	Let's Encrypt	--	--
<input type="checkbox"/>	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	--
<input type="checkbox"/>	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

← https://abhi-shek1289.gith...

Phish Dispute

Pivot ▾ DOM VIEW WHOIS INFORMATION

### Scan Results

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

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

Hosting Provider: Fastly

Category: Streaming

Location: United States

Certificate Details:

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

Brand: Netflix

IP Address: 185.199.111.153

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

ASN: 54113

Abuse Contact: abuse@github.com

### Screenshot

The screenshot shows a dark-themed Netflix clone interface. At the top, there's a banner with the word 'NETFLIX' and several movie posters. Below the banner, a large section displays a grid of movie and TV show thumbnails, including titles like 'FREED', 'TOM & JERRY', 'MONSTER HUNTER', and 'KABLA PAANI'. A red 'Get Started' button is visible at the bottom right of this section. Below the grid, there's a promotional message: 'Enjoy big movies, hit series and more from ₹49.' followed by 'Join today. Cancel anytime.' and 'Ready to watch? Enter your email to create or restart your membership.'

**Enjoy on your TV**  
Watch on smart TVs, PlayStation, Xbox, Chromecast, Apple TV, Blu-ray players and more.

← https://dev-doore.pantheo...

Phish Dispute

Pivot DOM VIEW WHOIS INFORMATION

### Scan Results

Source URL: <https://dev-doore.pantheonsite.io/qqqdayEJKnewwt....>

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

### Screenshot

The screenshot shows a Microsoft OneDrive interface. A modal window titled "Verify Your Identity" is open, prompting the user to enter professional email credentials to download a secure file. The file is described as a PDF document (56.1KB) from Microsoft. Below the modal, there is a large amount of redacted text, likely the original content of the page.

# Improvised Technique: Abuse of Dynamic DNS Services

## WHY

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

The screenshot shows the homepage of Now-DNS.com. At the top, there's a banner with text about their service and a "View Features" button. Below the banner, there's a section titled "Why use Now-DNS?" with two icons: one for "Free Dynamic DNS" (laptop) and one for "Remote Access" (camera). A sidebar lists various custom domain suffixes. At the bottom, there's a search bar with a dropdown menu showing the entered hostname ".001www.com".

Now-DNS is a super simple to use Dynamic DNS (DDNS) Service, providing you with unlimited custom hostnames. No contracts. All you need is another DDNS provider, you won't need UNLIMITED FREE DYNAMIC DNS. NOW, the only way they'll disappear is if you delete them yourself!\* Register with us today and you'll be managing your own Dynamic DNS in minutes. We've even got a client that will auto-update your hostnames if your IP changes.

[View Features](#)

\*Any accounts we believe to be providing illegal, abusive, malicious or service impacting content will be removed.

.001www.com  
.16-bit  
.2mydns.net  
.32-bit  
.64-bit  
.ddns.cam  
.dnsdyn.net  
.dnsget.org  
.dnsking.ch  
.dnslive.net  
.dnsup.net  
.dtdns.org  
.dynip.org  
.dynserv.org  
.forumz.info  
.freeddns.uk  
.freeddns.us  
.hicam.net  
.myddns.biz  
.myiphost.com

Why use Now-DNS?

Free Dynamic DNS      Remote Access

With unlimited custom hostnames that you can access from anywhere.      Remotely access devices like security cameras or file storage servers.

Check here to see if your pre

Hostname: .001www.com

Check Availability

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

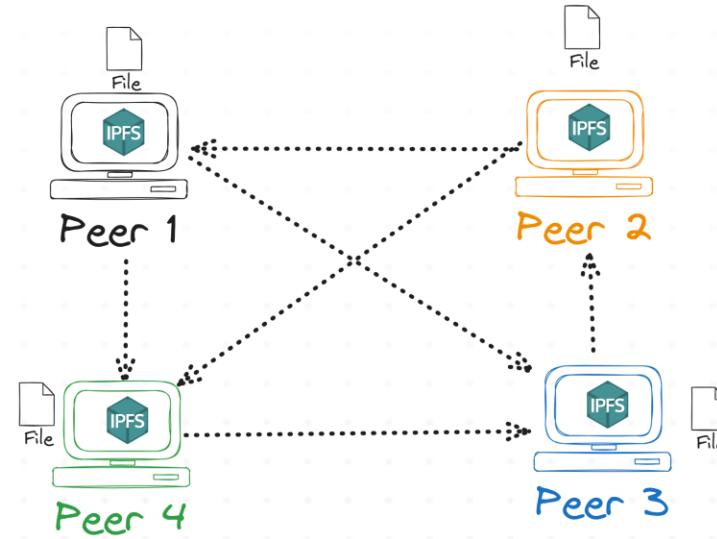


## Secure API Access

# Improvised Technique: InterPlanetary File System(IPFS)

## WHY

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



# A Latest Case Study: Data Exfiltration via Telegram Bot

The screenshot shows a browser window with a PDF document asking for email ID and password. Below it, the browser's developer tools Network tab is open, showing a POST request to a Telegram bot endpoint. The response payload is highlighted with a red box and contains JSON data related to a message being sent to a Telegram channel.

**Confirm your identity!**  
This PDF document is encoded with your SMTP mail server. Please login your email account credentials below to view protected document.

Email ID:  
asda@outlook.com

PASSWORD:  
Enter Email Password

Password is incorrect. Please try again

View Document Reset

100% SECURED

Network Tab Headers:

Name	Headers	Payload	Preview	Response	Initiator	Timing
sendMessage?chat_id=6082978649&ajaxid=4&text=Email%3Asda%40outloo...						

Response Payload (highlighted):

```
1 {  
  "ok": true,  
  "result": {  
    "message_id": 129,  
    "from": {  
      "id": 6946601537,  
      "is_bot": true,  
      "first_name": "NewBank",  
      "username": "██████████"  
    },  
    "chat": {  
      "id": 6082978649,  
      "first_name": "Mr",  
      "last_name": "Vigo",  
      "type": "private"  
    },  
    "date": 1702551393,  
    "text": "Email:asda@outlook.com | Password: ██████████ d",  
    "entities": [  
      {  
        "offset": 0,  
        "length": 22,  
        "type": "url"  
      }  
    ]  
  }  
}
```

Sending it to Telegram Channel

# Improvised Technique: Crypto Domains

microsoft2.x	
microsoft2.go	
microsoft3.x	
microsoft4.x	
microsoft-365.go	
microsoft-365.polygon	
microsoft365.kresus	
microsoft365.go	
microsoft-2023.blockchain	
microsoft-2023.wallet	

# Detecting to Scale

## checkphish

disposition

phishing

analysis

typosquatting

rendered

scam

phish text

takedown

favicon

computer

urls

classification

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

## ● Image-based Signals

- Screenshot of the webpage
- Favicon
- Logo

## ● Text-based Signals

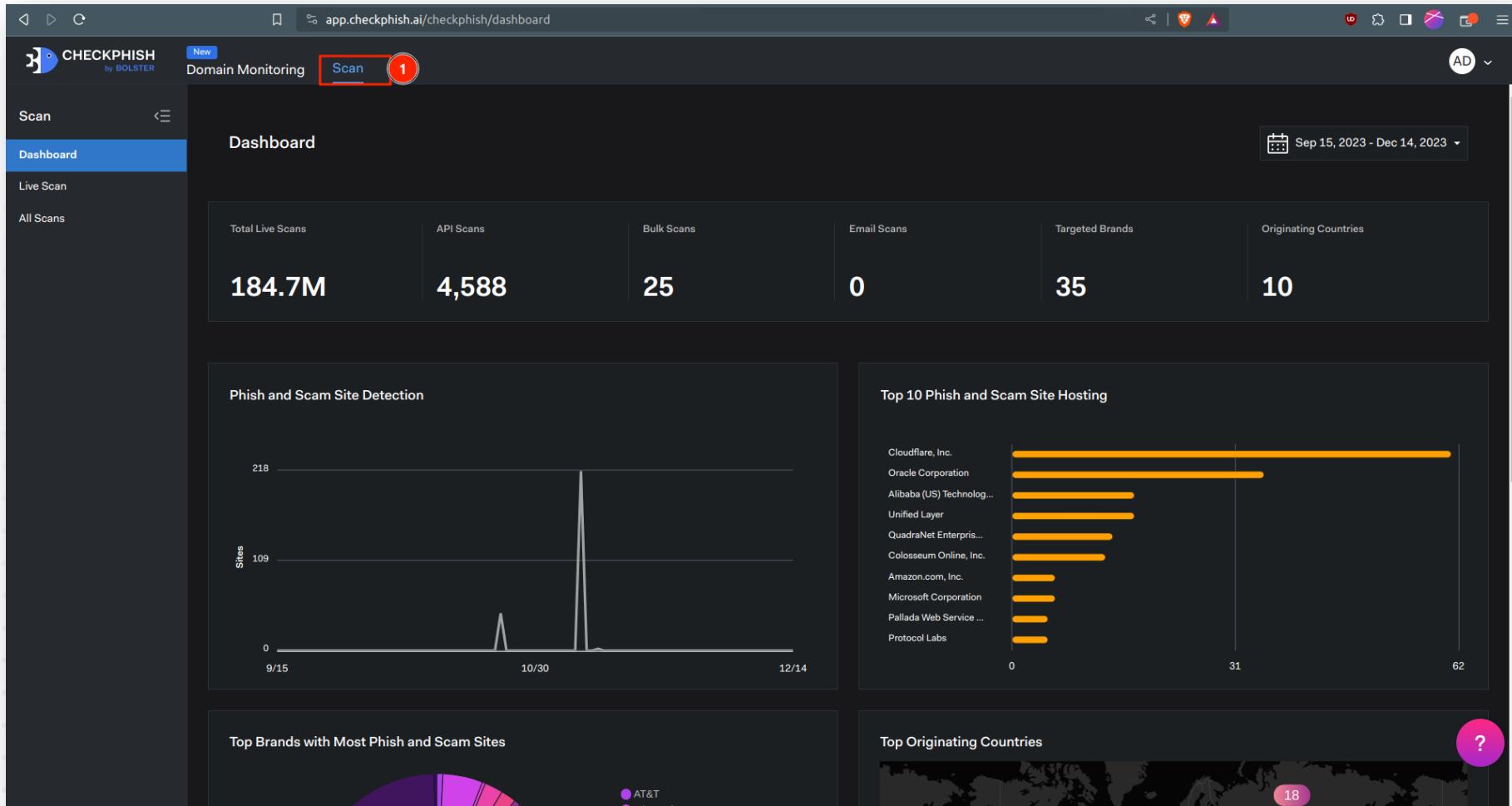
- Text on the webpage
- Copyright
- Key DOM elements

## 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



# Performing a Live Scan

The screenshot shows the CHECKPHISH by BOLSTER web application interface. The top navigation bar includes the logo, 'Domain Monitoring', 'Scan' (selected), and an 'AD' button. The left sidebar has 'Scan', 'Dashboard', and 'Live Scan' (selected). The main content area is titled 'Scan URLs' with a sub-instruction: 'To use our Scan URLs feature, simply enter the website URLs you want to scan (e.g., http://google.com), and our advanced algorithms will provide you with a comprehensive report that identifies any potential security risks or vulnerabilities associated with those URLs. For generating typosquats, please use the Domain Monitoring module (and NOT this page)'. Below this are filter settings: 'Filter Scanner IP Location' (set to 'United States'), 'User Agent' (set to 'Please Select'), and a 'Timeout for Page Scan' slider set to 'Auto'. A large text input field below these says 'Please enter a new url on each line (Limit 0/10)' with a red arrow pointing to it. At the bottom are 'Scan' and 'Clear All' buttons, and a 'Rescan' button at the bottom center.

# Performing a Live Scan

**Scan URLs**

To use our Scan URLs feature, simply enter the website URLs you want to scan (e.g., http://google.com), and our advanced algorithms will provide you with a comprehensive report that identifies any potential security risks or vulnerabilities associated with those URLs. For generating typosquats, please use the Domain Monitoring module (and NOT this page)

 **New Scan**

**Filter**

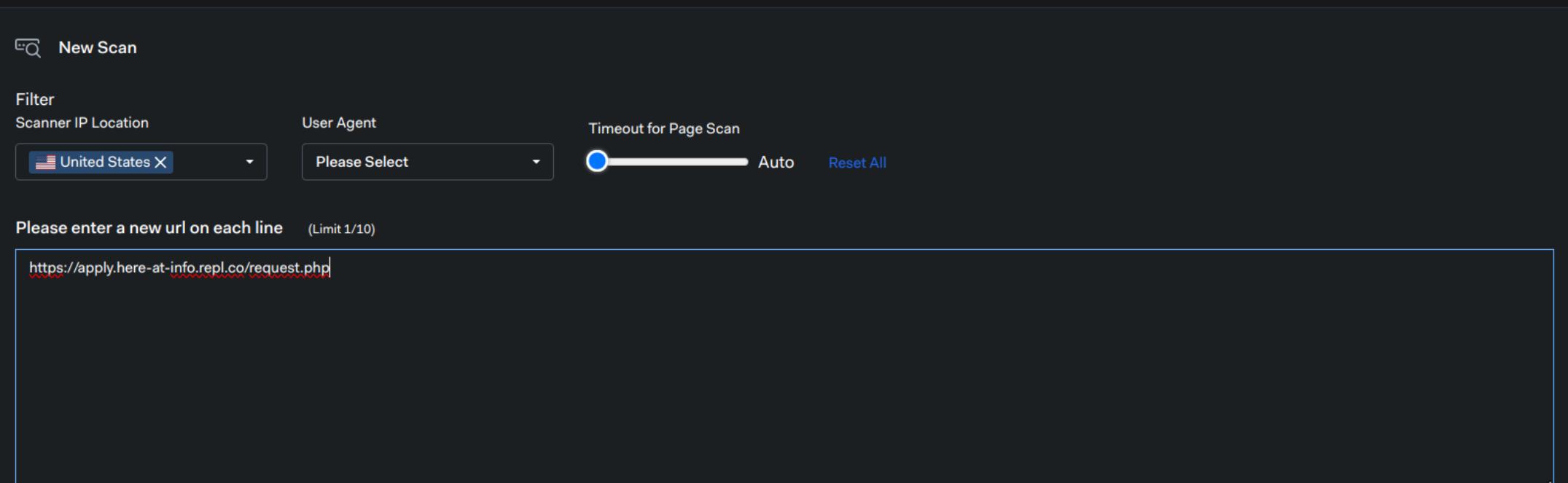
Scanner IP Location      User Agent      Timeout for Page Scan

United States X      Please Select      Auto      Reset All

Please enter a new url on each line (Limit 1/10)

```
https://apply.here-at-info.repl.co/request.php
```

**Scan**      Clear All



# Performing a Live Scan

Rescan

Scanned on 12-17-2023, 12:45 AM from US using -- and timeout of Auto

---

	Source URL: <a href="https://apply.here...">https://apply.here...</a> <input type="checkbox"/>	Disposition: Phish
	IP Address: 34.100.245.52	Brand: Facebook
	Hosting Provider: Google LLC	Category: Unknown

---

Scan Location:	Timeout:	Last scanned:	First seen:
US	Auto	17-Dec-2023	16-Dec-2023

Logo Detected:  
true

# Performing a Live Scan: Insights

← https://apply.here-at-info.repl.co... Phish

**INSIGHTS** **THREAT INTELLIGENCE** **DOM TREE** **WHOIS INFO**

### Scan Results

Source URL: <https://apply.here-at-info.repl.co/request.php>

Brand: Facebook

Redirected URL: <https://apply.here-at-info.repl.co/request.php>

TLD: co

IP Address: 34.100.245.52

Location: India

Detection Date: December 17th 2023, 12:45:56 am

Hosting Provider: Google LLC

Job ID: --

ASN: 15169

Certificate Details: Google Trust Services LLC: here-at-info.repl.co, \*here-at-info.repl.co

Scan Source Category: Spam

### Screenshot

Logos Detected: 1

The screenshot shows a Facebook page with a 'Appeal Page Violation' dialog open. The dialog states: 'We have detected unusual activity on your page that violates our community standards. Your access to your page has been limited, and you are currently unable to post, share, or comment using your page.' It provides an option to submit an appeal by providing necessary information. Below the dialog, there's a message: 'Please make sure account not to log out from your computer or laptop until you have received a verification email.' At the bottom of the page, there are links for 'About', 'Privacy Policy', 'Careers', 'AdChoices', 'Create ad', 'Create Page', 'Terms and policies', and 'Cookies'.

### Scan Settings

First Scan Time: --

Last Scan Time: December 17th 2023, 12:45:56 am

Scan Location: US

Timeout: Auto

# Performing a Live Scan: Threat Intelligence

The screenshot shows a web-based threat intelligence tool interface. At the top, there's a navigation bar with tabs: INSIGHTS, THREAT INTELLIGENCE (which is underlined and highlighted with a red arrow), DOM TREE, and WHOIS INFO. Below the tabs, there's a header "Threat Intelligence".

Under the Threat Intelligence header, there are three sections:

- Past Phish on Host:** Shows 1 past phish on host.
- Past Phish on IP:** Shows -- past phish on IP.
- Phishing Kits on Host:** Shows 0 phishing kits on host.

Below these sections is a "Passive DNS" section with a dropdown menu set to "All". It contains a heading "Domains hosted on the same IP address" and a list of domains:

- apply.here-at-info.repl.co (highlighted with a red box)
- change-the-decision--marketingplace6.repl.co
- paypaypay1.repl.co
- pay.paypaypay1.repl.co
- contact--fan-review-123.repl.co
- 52.245.100.34.bc.googleusercontent.com
- fast-account-bots.mustfix.repl.co
- subduedbeigeprocessor.nikeno7132.repl.co
- apeal.nizamaninizaman.repl.co

A purple circular icon with a question mark is located in the bottom right corner of the list area.

# Performing a Live Scan: DOM Tree

← https://apply.here-at-info.repl.co... Phish

INSIGHTS THREAT INTELLIGENCE DOM TREE WHOIS INFO

DOM Tree (Document Object Model): [download](#)

```
<!DOCTYPE html>
<html>

<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href=". /Action _ Required_files/style.css" rel="stylesheet">
    <link rel="shortcut icon" href="https://copyright--appealsubmit.repl.co/AAABAAMAEBAAAEEAIBoBAAANGAACAgAAABACAAKBEAAJ4EAAAwMAAAAQAgAGgmAADGFQAAKAAAABAAAAgAAAAAQAgAAAAAAAAAAAAA" />
    <title>Action | Required</title>

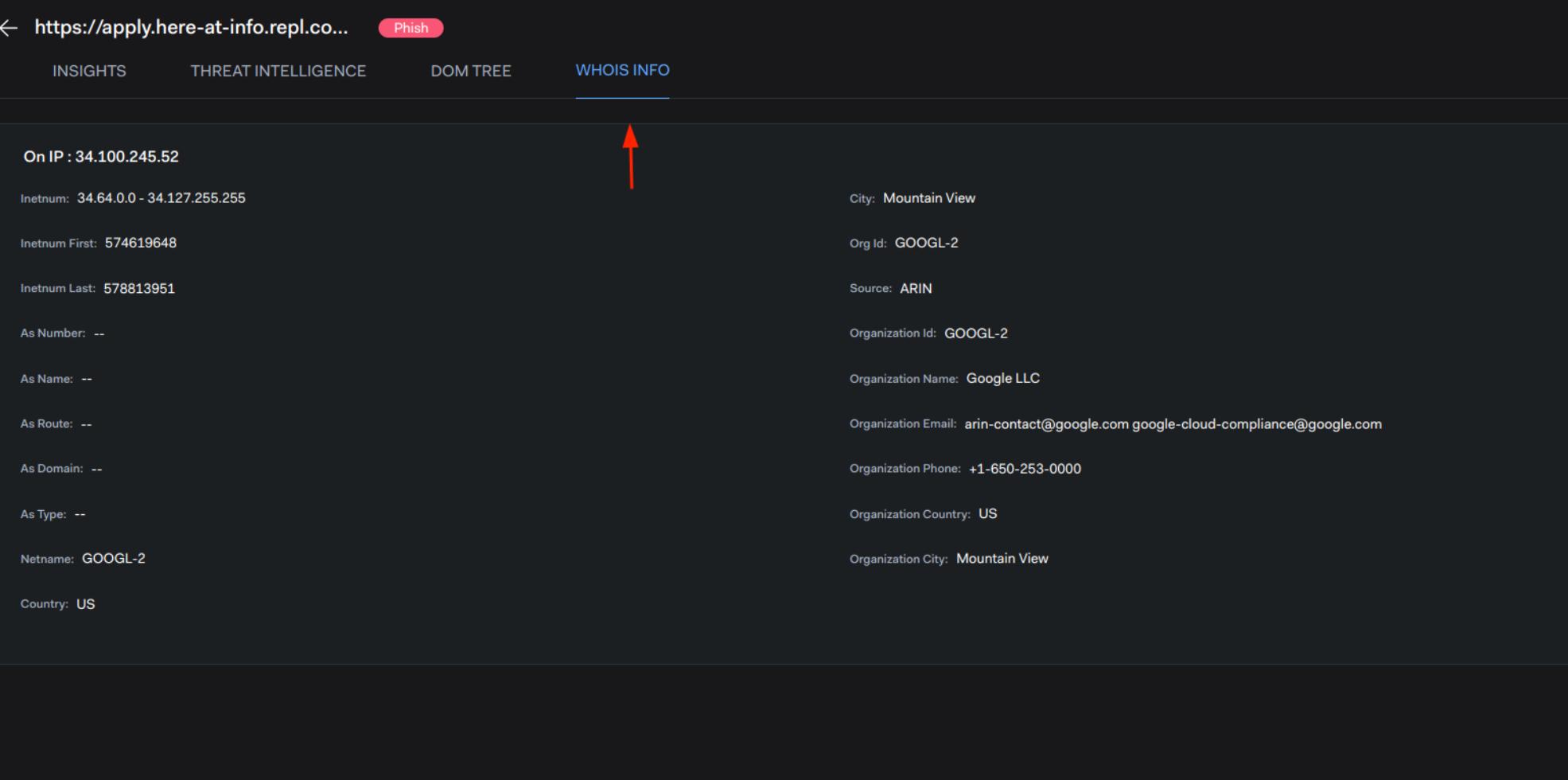
</head>

<body>
    <div class="md:hidden lg:hidden sm:block border flex w-full h-16 relative bg-[#4667ac]">
        <div class="mx-5 mt-3">
            
        </div>
        <div>

            <form>
                <label for="search" class="mb-2 text-sm font-medium text-gray-900 sr-only dark:text-white">Search</label>
                <div class="relative">
                    <div class="absolute inset-y-0 left-0 flex items-center pl-3 mx-3 pointer-events-none">
                        <svg class="w-3 h-3 text-gray-500 dark:text-gray-400" aria-hidden="true" xmlns="http://www.w3.org/2000/svg" fill="none" viewBox="0 0 20 20">
                            <path stroke="currentColor" stroke-linecap="round" stroke-linejoin="round" stroke-width="2" d="m19 19-4-4m0-7a7 7 0 1 1 8a7 7 0 0 1 14 0z"/>
                        </svg>
                    </div>
                    <input type="search" id="search" class="block w-full mt-4 mx-4 pl-7 text-sm text-gray-900 border border-gray-300 rounded-sm bg-gray-50 focus:ring-blue-500 focus:border-blue-500" />
                </div>
            </form>
        </div>
    </div>
</body>
```



# Performing a Live Scan: WHOIS Info



← https://apply.here-at-info.repl.co... Phish

INSIGHTS THREAT INTELLIGENCE DOM TREE WHOIS INFO

On IP : 34.100.245.52

Inetnum: 34.64.0.0 - 34.127.255.255

Inetnum First: 574619648

Inetnum Last: 578813951

As Number: --

As Name: --

As Route: --

As Domain: --

As Type: --

Netname: GOOGL-2

Country: US

City: Mountain View

Org Id: GOOGL-2

Source: ARIN

Organization Id: GOOGL-2

Organization Name: Google LLC

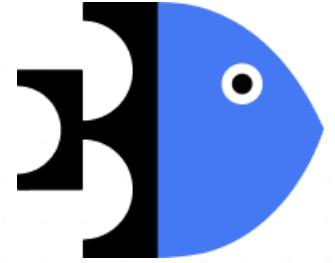
Organization Email: arin-contact@google.com google-cloud-compliance@google.com

Organization Phone: +1-650-253-0000

Organization Country: US

Organization City: Mountain View

**Wanna be a  
Threat Hunter  
for a Day... ??**



# CHECKPHISH CTF

by BOLSTER



Register at: <https://ctf.checkphish.ai>

Start Time: 17<sup>th</sup> December 2023 2PM IST

End Time: 18<sup>th</sup> December 2023 2PM IST

For Queries/Doubts: Join **DEF CON DELHI GROUP** DC Server[Channel Name: **#checkphish\_ctf\_2023**

# Questions?