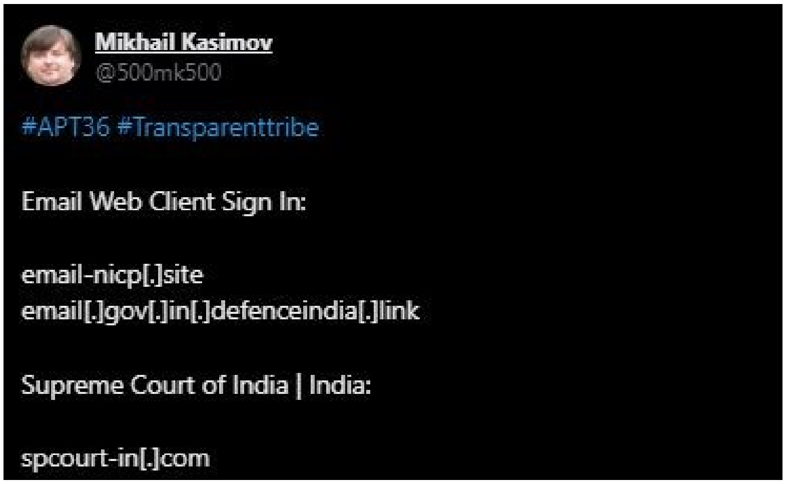
Exposing the Deceit: Phishing Sites Impersonating Government Entities

labs.k7computing.com/index.php/exposing-the-deceit-phishing-sites-impersonating-government-entities/

By Harihara Sudhan February 18, 2025

Threat actors impersonating a Government entity, and using their fake authority and trustworthiness to coerce the victims to divulge their personal or banking details through a Phishing page or an App or a direct voice call is a well-known trend. In India, “Digital Arrest” is the new fad in this trend, and our government is actively working to educate citizens on how to protect themselves.

A particularly alarming aspect of this is when the targets are employees of government institutions and agencies. There have been several instances of advanced persistent threats (APTs) and external parties targeting military personnel, research institutes, and even educational institutions. This targeting is sometimes long-drawn and reuses the tools, framework, and other infra. In this blog, we will present two recent examples of such attacks in which the threat actors masquerade as Government and Judicial entities. We recently came across a tweet, in which was mentioned a few fake Indian government sites.



Mikhail Kasimov
@500mk500

#APT36 #Transparenttribe

Email Web Client Sign In:

email-nicp[.]site
email[.]gov[.]in[.]defenceindia[.]link

Supreme Court of India | India:

spcourt-in[.]com

Figure 1: The tweet

Let’s take a look at the domain **“spcourt-in[.]com.”**. This phishing site is designed to closely resemble the official website of the Supreme Court of India. This fake site collects PII (Personally Identifiable Information), bank account details, etc.

The major difference between the fake and the original site is the presence of those three logos at the bottom right, where the site harvests user data.

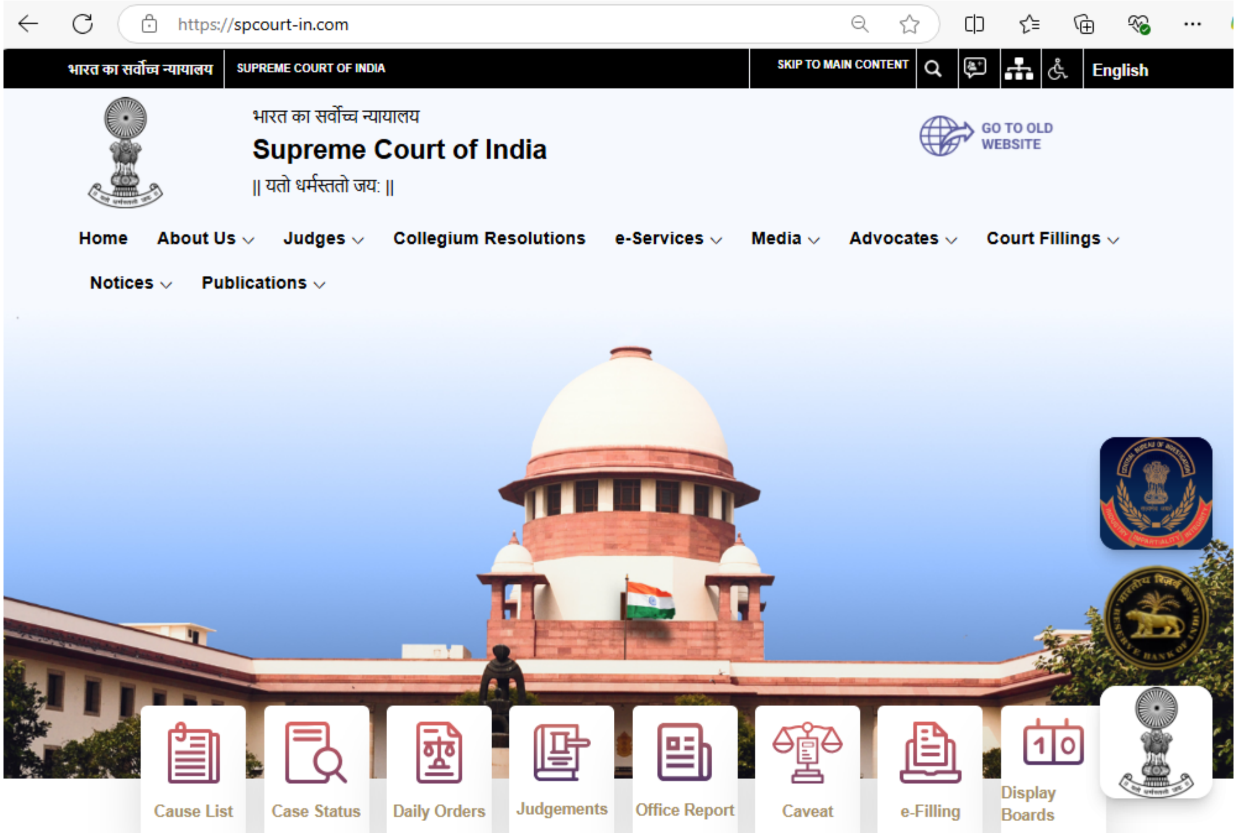


Figure 2: Phishing site posing as The Supreme Court of India website

On the bottom right part of the page, three clickable icons appear to represent official organizations, including the “Central Bureau of Investigation,” “Reserve Bank of India,” and “Supreme Court of India,” just to provide some ‘fake’ authenticity to their site.

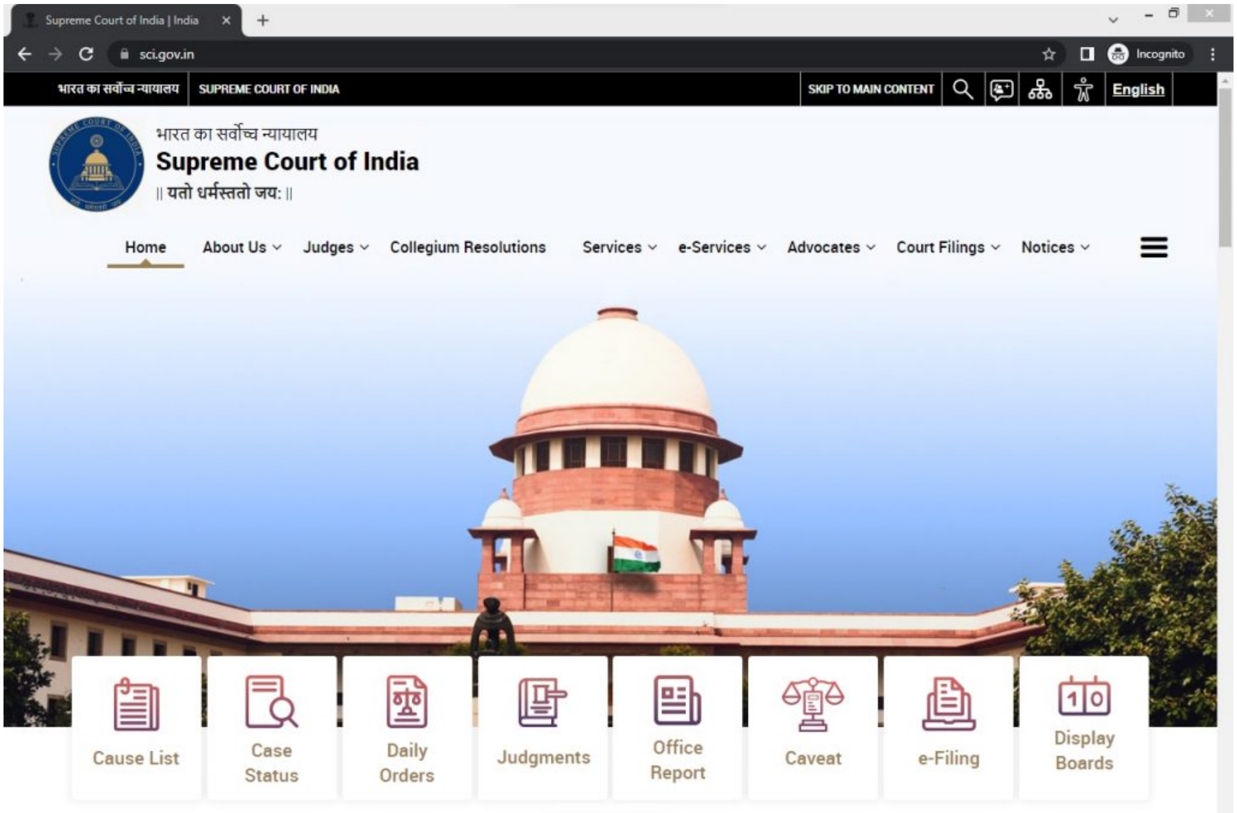
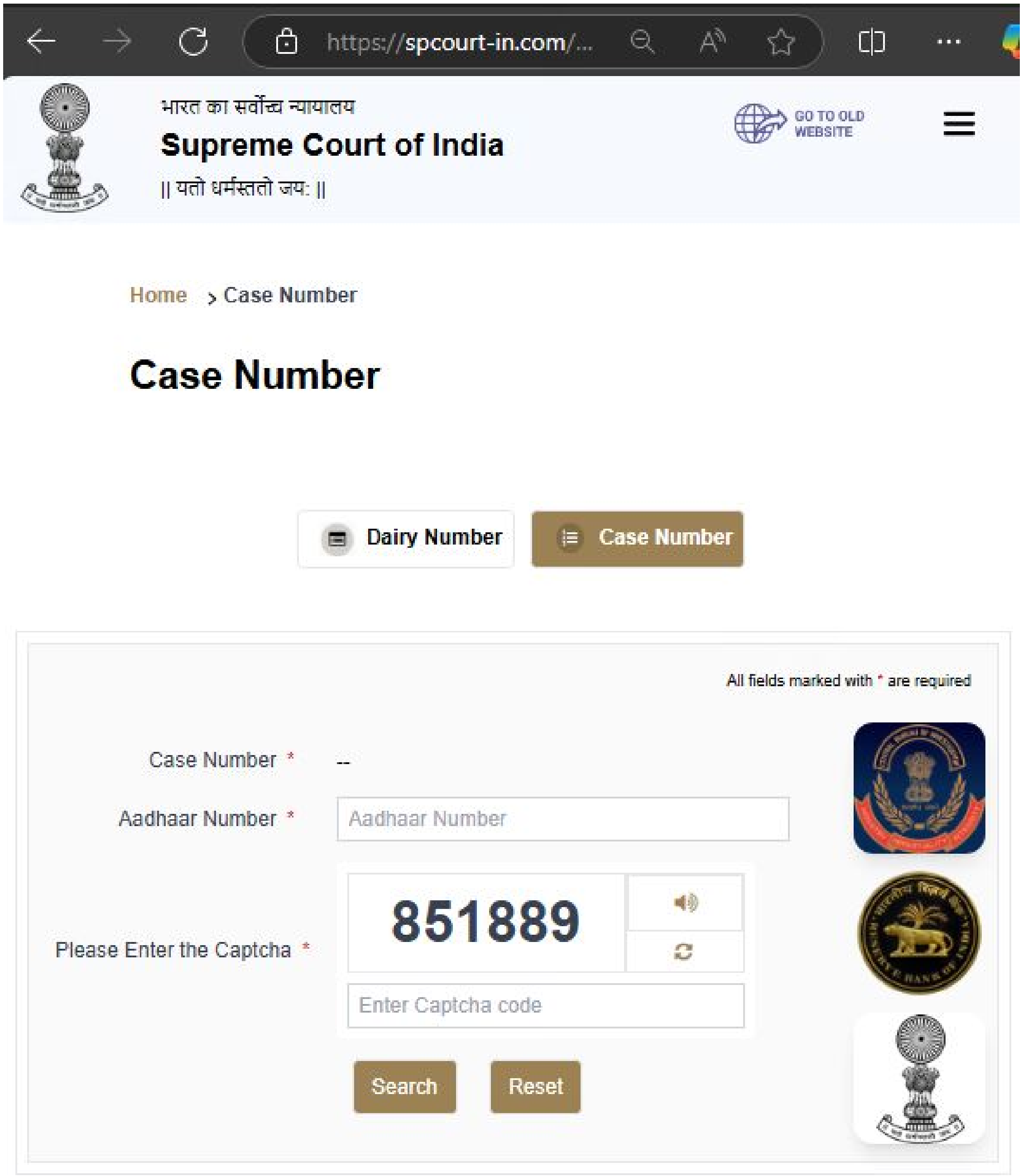


Figure 3: The Original site

Clicking on the CBI logo (the first logo) takes the user to a page where they are prompted to enter details, such as their Aadhar number.



https://spcourt-in.com/...

भारत का सर्वोच्च न्यायालय

Supreme Court of India

|| यतो धर्मस्ततो जय: ||

Home > Case Number

Case Number

All fields marked with * are required

Case Number * --

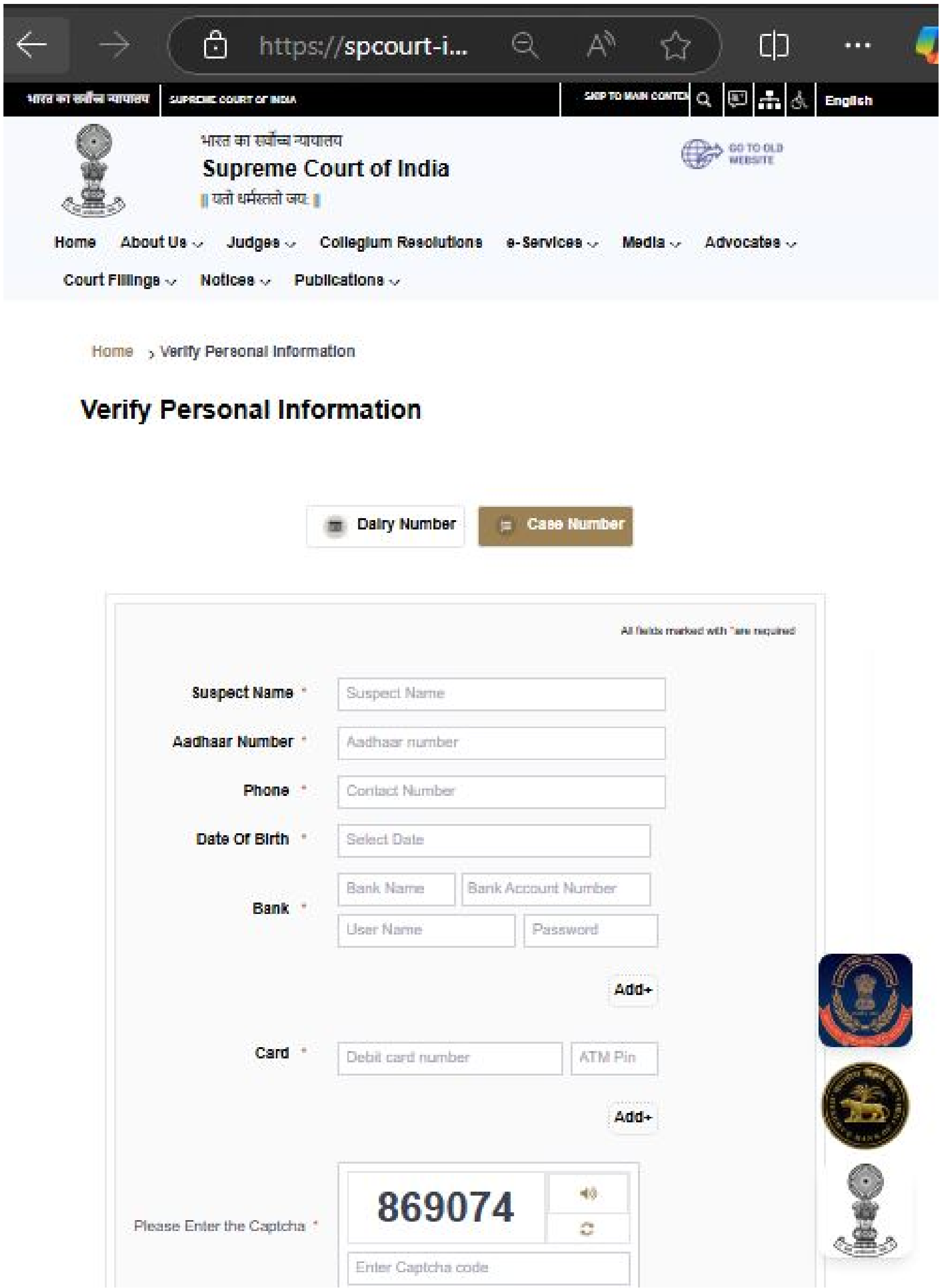
Aadhaar Number * Aadhaar Number

Please Enter the Captcha * 851889

Enter Captcha code

Figure 4: Collecting Aadhar

Clicking on the RBI logo (the second logo) leads the user to a page where they are asked to verify personal information. During this process, the site collects details such as date of birth, Aadhaar number, contact information, and bank account details (including passwords). At a later point in this blog, we will discuss what happens to the data that is being collected via these forms.



https://spcourt-i...

भारत का सर्वोच्च न्यायालय | SUPREME COURT OF INDIA | SKIP TO MAIN CONTENT | English

भारत का सर्वोच्च न्यायालय
Supreme Court of India
|| यतो धर्मस्ततो जयः ||

GO TO OLD WEBSITE

Home | About Us | Judges | Collegium Resolutions | e-Services | Media | Advocates | Court Fillings | Notices | Publications

Home > Verify Personal Information

Verify Personal Information

Diary Number | Case Number

All fields marked with * are required

Suspect Name * : Suspect Name

Aadhaar Number * : Aadhaar number

Phone * : Contact Number

Date Of Birth * : Select Date

Bank * : Bank Name | Bank Account Number | User Name | Password

Add+

Card * : Debit card number | ATM Pin

Add+

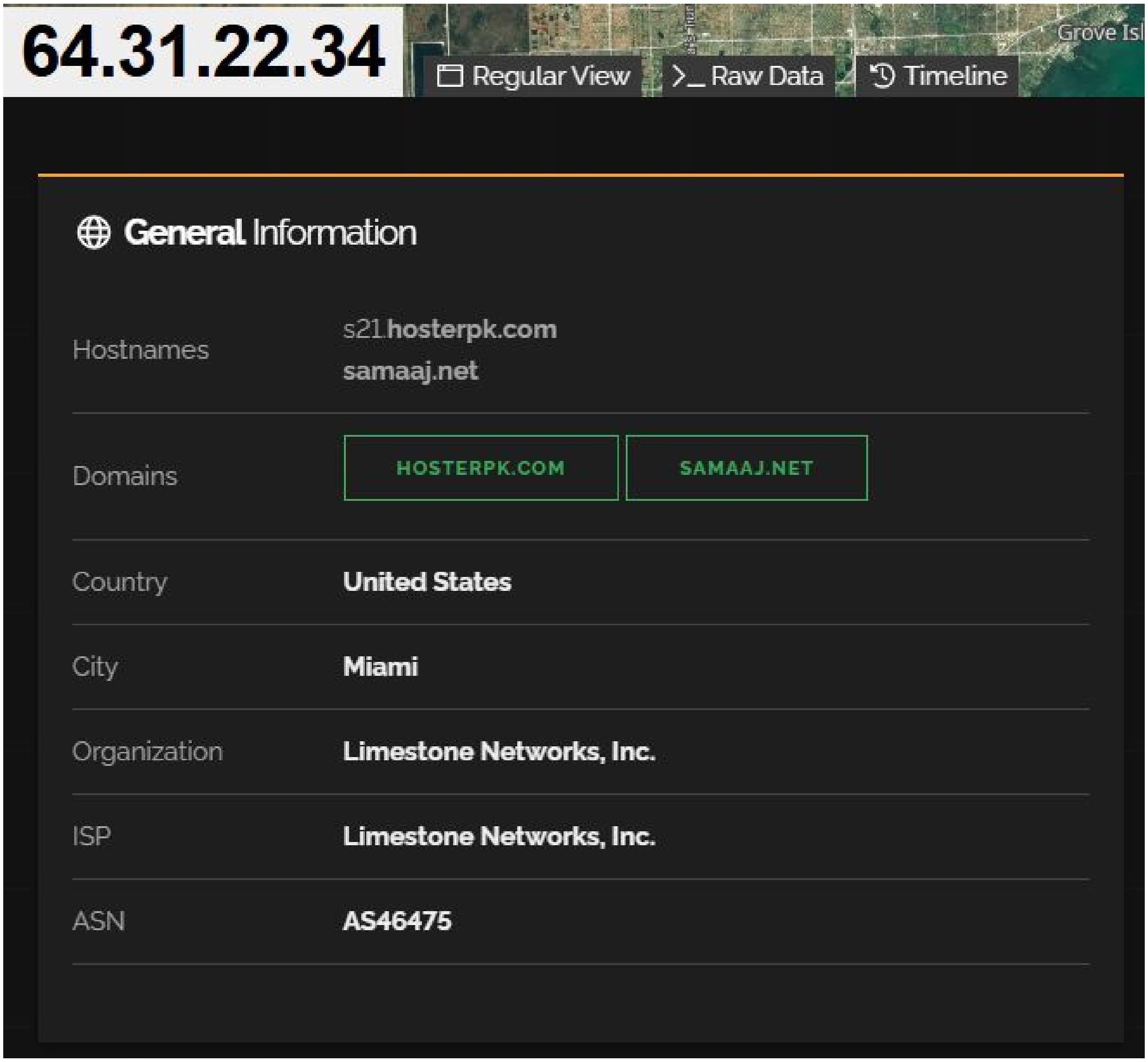
Please Enter the Captcha * : 869074

Enter Captcha code

Figure 5: Collecting Personal & Bank Details

Detailed Analysis on Spcourt-in[.]com

The IP address of the phishing site is “64.31.22.34” was registered on 27-01-2025 and has validity for a year. The website is hosted on servers provided by **Hosterpk[.]com**, a web hosting company based out of **Pakistan**. This information further suggests that the site is likely to be managed from outside India.



64.31.22.34

General Information

Hostnames s21.hosterpk.com
samaaj.net

Domains HOSTERPK.COM SAMAAJ.NET

Country United States

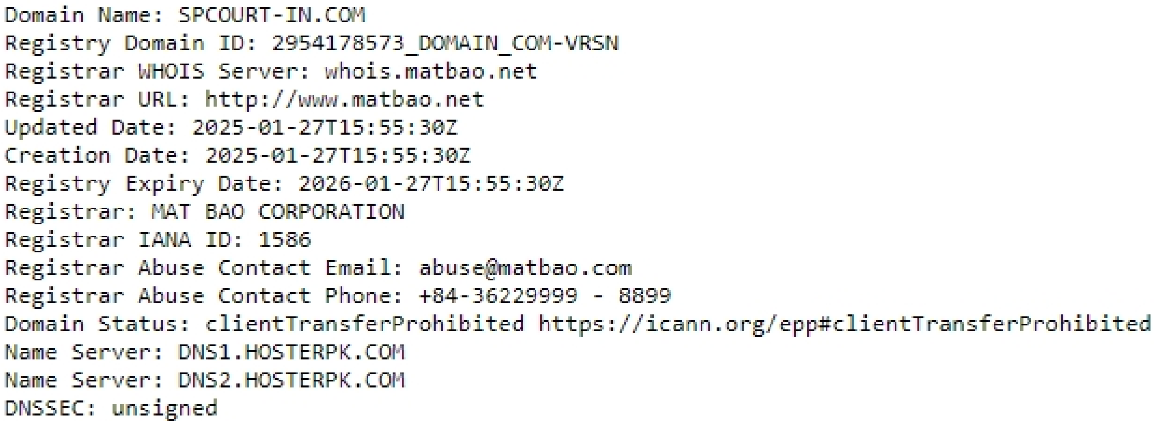
City Miami

Organization Limestone Networks, Inc.

ISP Limestone Networks, Inc.

ASN AS46475

Figure 6: IP-details-I

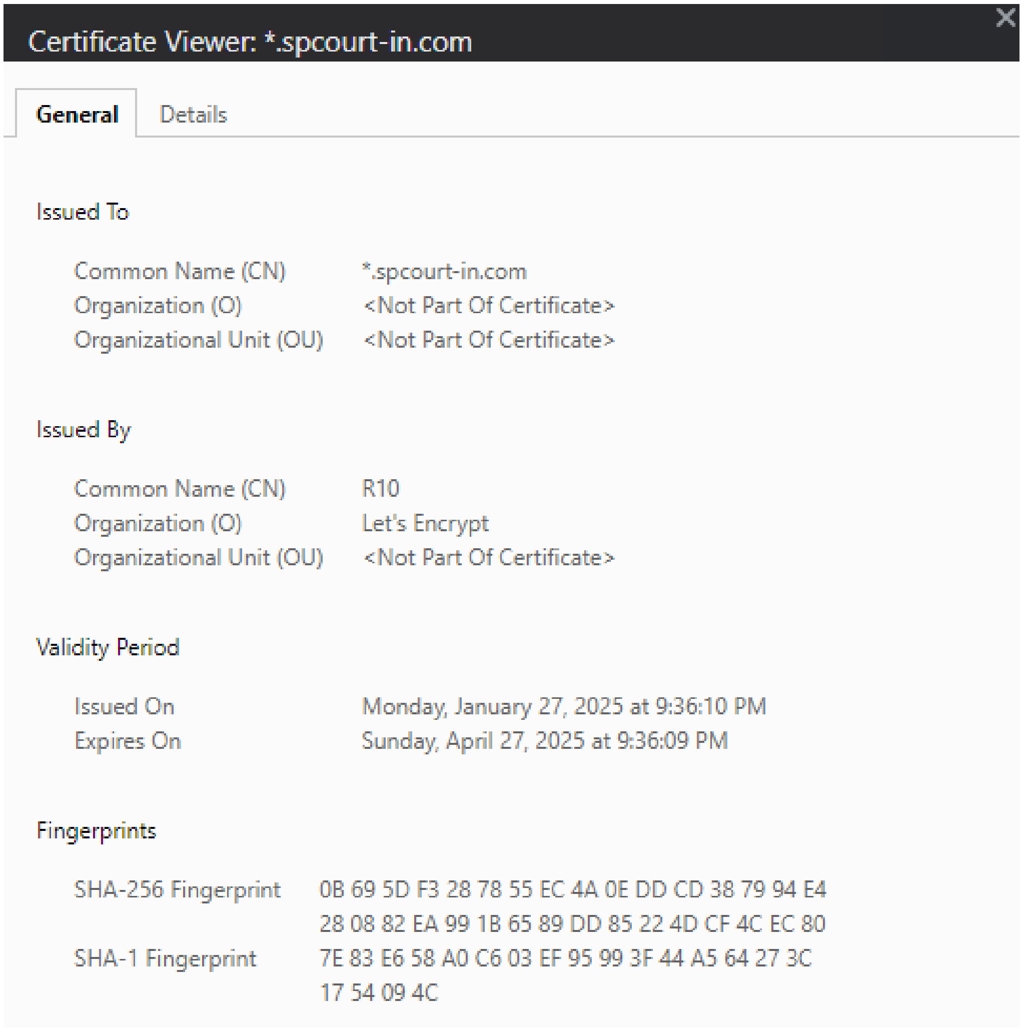


```
Domain Name: SPCOURT-IN.COM
Registry Domain ID: 2954178573_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.matbao.net
Registrar URL: http://www.matbao.net
Updated Date: 2025-01-27T15:55:30Z
Creation Date: 2025-01-27T15:55:30Z
Registry Expiry Date: 2026-01-27T15:55:30Z
Registrar: MAT BAO CORPORATION
Registrar IANA ID: 1586
Registrar Abuse Contact Email: abuse@matbao.com
Registrar Abuse Contact Phone: +84-36229999 - 8899
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.HOSTERPK.COM
Name Server: DNS2.HOSTERPK.COM
DNSSEC: unsigned
```

Figure 7: IP-details-II

TLS details

The certificate is issued by the organization **“Let’s Encrypt”**. While Let’s Encrypt is known for providing free SSL certificates to secure websites, its use here indicates that the attacker is attempting to give the phishing site a legitimate and secure appearance, which could give a false sense of security to users into trusting this site with their PII.



Issued To

Common Name (CN)	*.spcourt-in.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	R10
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

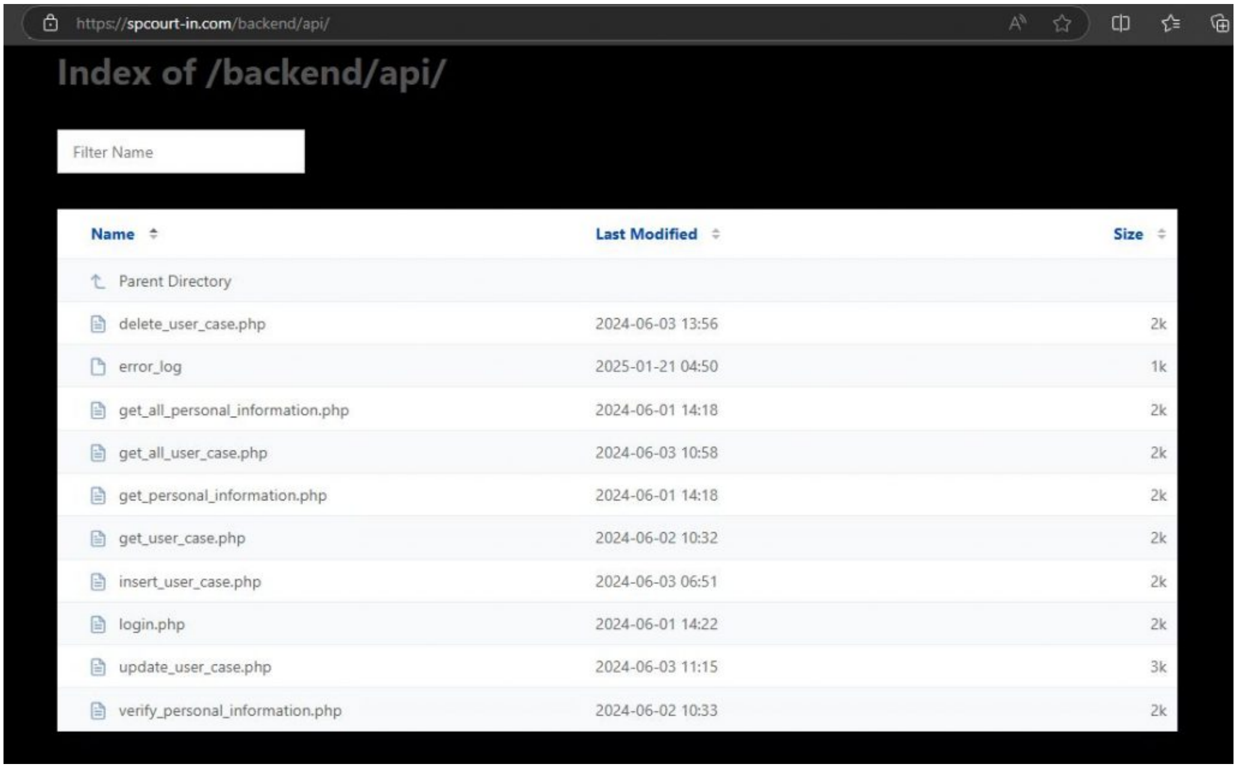
Issued On	Monday, January 27, 2025 at 9:36:10 PM
Expires On	Sunday, April 27, 2025 at 9:36:09 PM

Fingerprints

SHA-256 Fingerprint	0B 69 5D F3 28 78 55 EC 4A 0E DD CD 38 79 94 E4 28 08 82 EA 99 1B 65 89 DD 85 22 4D CF 4C EC 80
SHA-1 Fingerprint	7E 83 E6 58 A0 C6 03 EF 95 99 3F 44 A5 64 27 3C 17 54 09 4C

Figure 8: Certificate Details

The below image shows a list of PHP scripts used for processing the collected data.



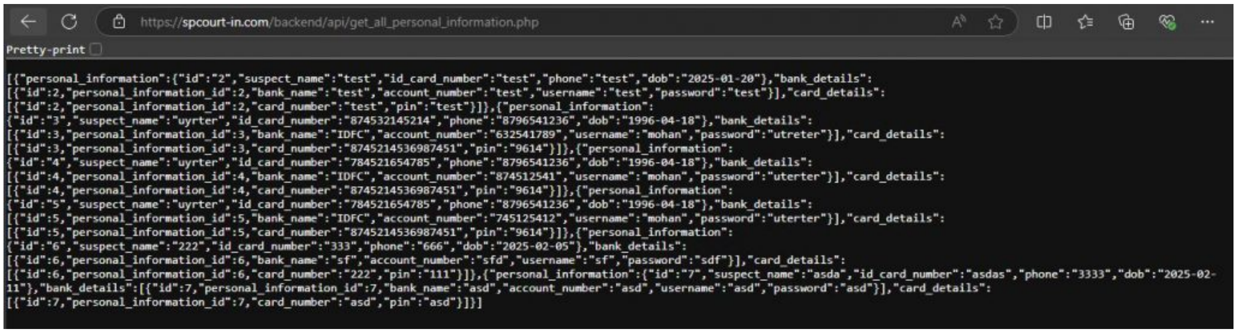
https://spcourt-in.com/backend/api/

Index of /backend/api/

Name	Last Modified	Size
Parent Directory		
delete_user_case.php	2024-06-03 13:56	2k
error_log	2025-01-21 04:50	1k
get_all_personal_information.php	2024-06-01 14:18	2k
get_all_user_case.php	2024-06-03 10:58	2k
get_personal_information.php	2024-06-01 14:18	2k
get_user_case.php	2024-06-02 10:32	2k
insert_user_case.php	2024-06-03 06:51	2k
login.php	2024-06-01 14:22	2k
update_user_case.php	2024-06-03 11:15	3k
verify_personal_information.php	2024-06-02 10:33	2k

Figure 9: backend/api found on the Phishing site

The forms on the site collecting the personal data and bank details are processed through the “get_all_Personal_information.php” and the data submitted are stored in JSON format.

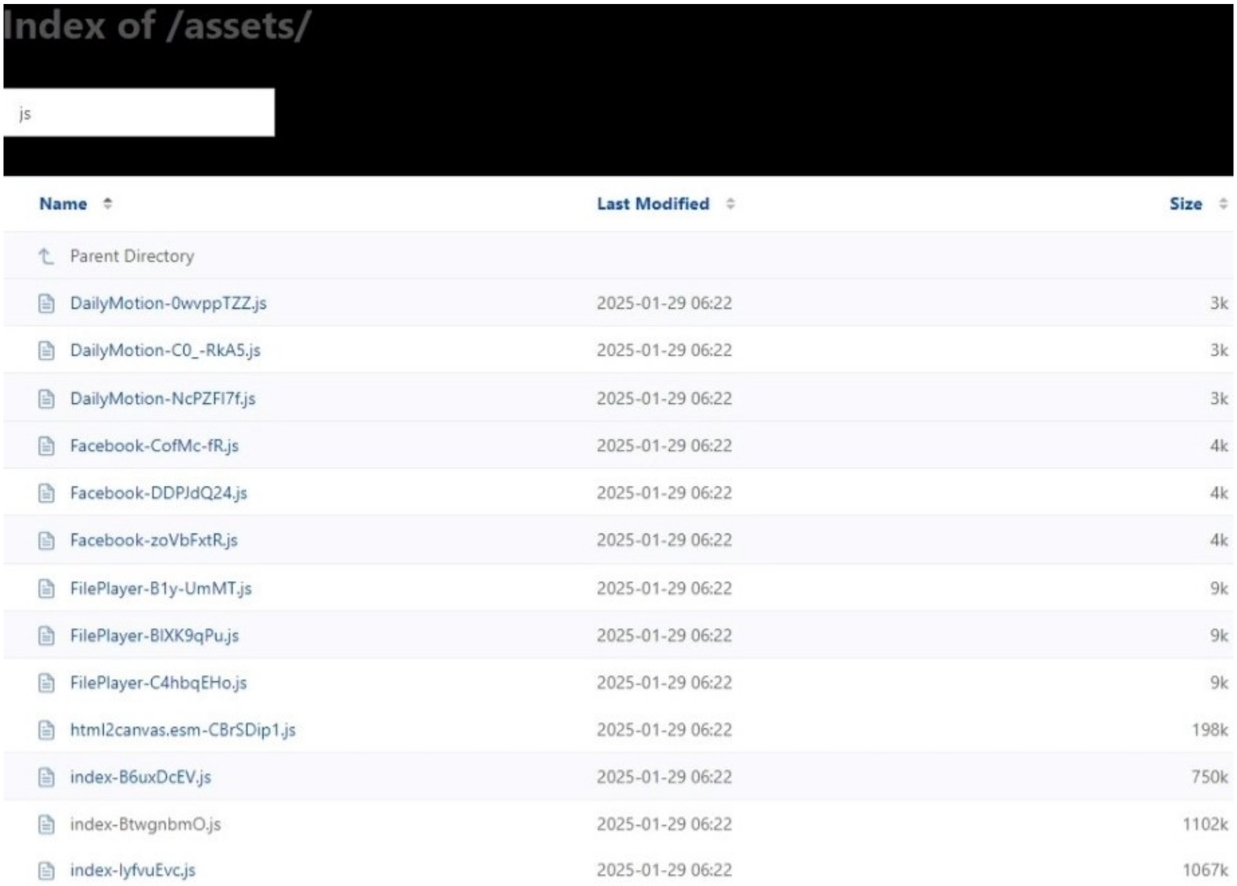


https://spcourt-in.com/backend/api/get_all_personal_information.php

```
[{"personal_information":{"id":"2","suspect_name":"test","id_card_number":"test","phone":"test","dob":"2025-01-20"},"bank_details":
[{"id":2,"personal_information_id":2,"bank_name":"test","account_number":"test","username":"test","password":"test"}],"card_details":
[{"id":2,"personal_information_id":2,"card_number":"test","pin":"test"}]},{"personal_information":
{"id":"3","suspect_name":"uyrter","id_card_number":"874532145214","phone":"8796541236","dob":"1996-04-18"},"bank_details":
[{"id":3,"personal_information_id":3,"bank_name":"IDFC","account_number":"632541789","username":"mohan","password":"utreter"}],"card_details":
[{"id":3,"personal_information_id":3,"card_number":"8745214536987451","pin":"9614"}]},{"personal_information":
{"id":"4","suspect_name":"uyrter","id_card_number":"784521654785","phone":"8796541236","dob":"1996-04-18"},"bank_details":
[{"id":4,"personal_information_id":4,"bank_name":"IDFC","account_number":"874512541","username":"mohan","password":"uterter"}],"card_details":
[{"id":4,"personal_information_id":4,"card_number":"8745214536987451","pin":"9614"}]},{"personal_information":
{"id":"5","suspect_name":"uyrter","id_card_number":"784521654785","phone":"8796541236","dob":"1996-04-18"},"bank_details":
[{"id":5,"personal_information_id":5,"bank_name":"IDFC","account_number":"745125412","username":"mohan","password":"uterter"}],"card_details":
[{"id":5,"personal_information_id":5,"card_number":"8745214536987451","pin":"9614"}]},{"personal_information":
{"id":"6","suspect_name":"222","id_card_number":"333","phone":"666","dob":"2025-02-05"},"bank_details":
[{"id":6,"personal_information_id":6,"bank_name":"sf","account_number":"sfd","username":"sf","password":"sdf"}],"card_details":
[{"id":6,"personal_information_id":6,"card_number":"222","pin":"111"}]},{"personal_information":{"id":"7","suspect_name":"asda","id_card_number":"asdas","phone":"3333","dob":"2025-02-
11"},"bank_details":[{"id":7,"personal_information_id":7,"bank_name":"asd","account_number":"asd","username":"asd","password":"asd"}],"card_details":
[{"id":7,"personal_information_id":7,"card_number":"asd","pin":"asd"}]}]
```

Figure 10: Data we entered in the forms stored in PHP

This domain hosts several JavaScripts as shown below.



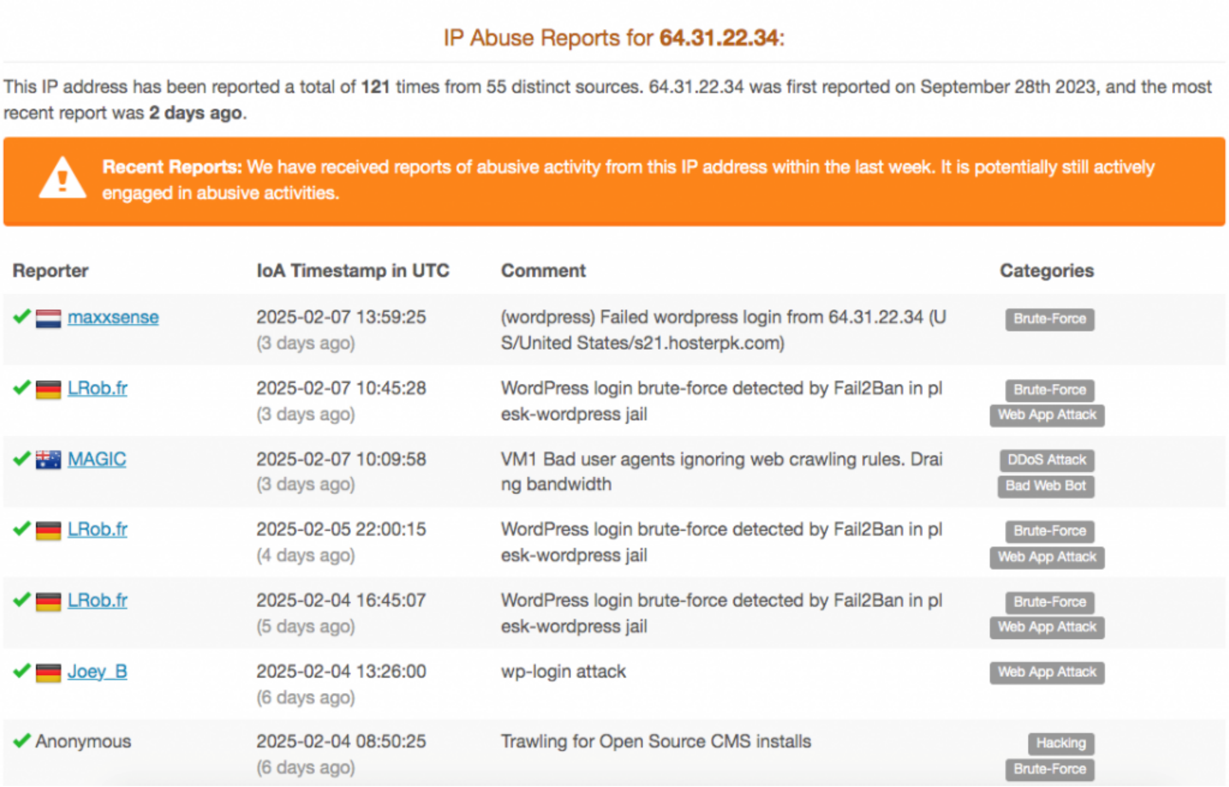
Index of /assets/

js

Name	Last Modified	Size
Parent Directory		
DailyMotion-0wvppTZZ.js	2025-01-29 06:22	3k
DailyMotion-C0_-RkA5.js	2025-01-29 06:22	3k
DailyMotion-NcPZFI7f.js	2025-01-29 06:22	3k
Facebook-CofMc-fR.js	2025-01-29 06:22	4k
Facebook-DDPJdQ24.js	2025-01-29 06:22	4k
Facebook-zoVbFxtR.js	2025-01-29 06:22	4k
FilePlayer-B1y-UmMT.js	2025-01-29 06:22	9k
FilePlayer-BIXK9qPu.js	2025-01-29 06:22	9k
FilePlayer-C4hbqEHo.js	2025-01-29 06:22	9k
html2canvas.esm-CBrSDip1.js	2025-01-29 06:22	198k
index-B6uxDcEV.js	2025-01-29 06:22	750k
index-BtwgnbmO.js	2025-01-29 06:22	1102k
index-lyfvuEvc.js	2025-01-29 06:22	1067k

Figure 11: JavaScripts present in the site

We also checked for signs of any IP abuse and discovered that the IP address associated with the Phishing site had been involved in a **WordPress brute force attack**.



IP Abuse Reports for **64.31.22.34**:

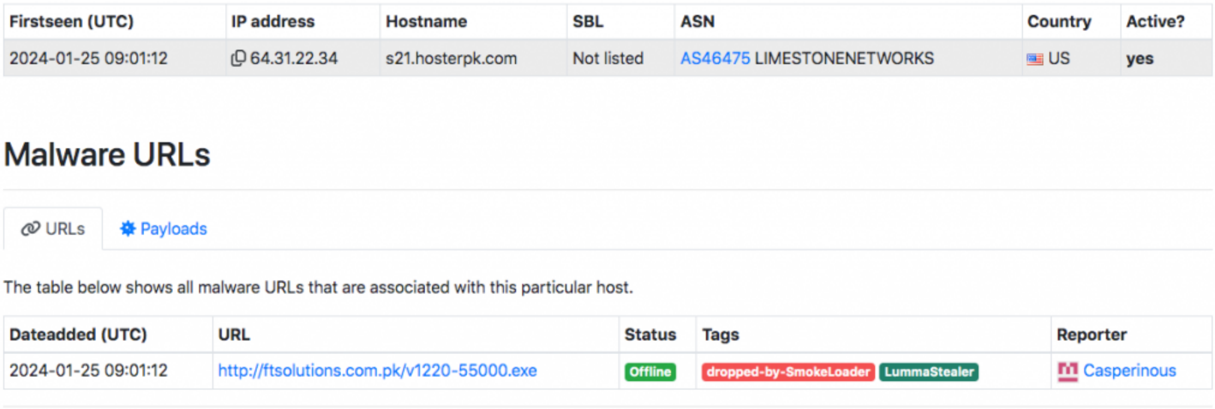
This IP address has been reported a total of **121** times from 55 distinct sources. 64.31.22.34 was first reported on September 28th 2023, and the most recent report was **2 days ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
✓ maxxsense	2025-02-07 13:59:25 (3 days ago)	(wordpress) Failed wordpress login from 64.31.22.34 (US/United States/s21.hosterpk.com)	Brute-Force
✓ LRob.fr	2025-02-07 10:45:28 (3 days ago)	WordPress login brute-force detected by Fail2Ban in plesk-wordpress jail	Brute-Force Web App Attack
✓ MAGIC	2025-02-07 10:09:58 (3 days ago)	VM1 Bad user agents ignoring web crawling rules. Draing bandwidth	DDoS Attack Bad Web Bot
✓ LRob.fr	2025-02-05 22:00:15 (4 days ago)	WordPress login brute-force detected by Fail2Ban in plesk-wordpress jail	Brute-Force Web App Attack
✓ LRob.fr	2025-02-04 16:45:07 (5 days ago)	WordPress login brute-force detected by Fail2Ban in plesk-wordpress jail	Brute-Force Web App Attack
✓ Joey_B	2025-02-04 13:26:00 (6 days ago)	wp-login attack	Web App Attack
✓ Anonymous	2025-02-04 08:50:25 (6 days ago)	Trawling for Open Source CMS installs	Hacking Brute-Force

Figure 12: Abuse Reports from the IP

There is also a history of **Lumma Stealer** being hosted on this site at an earlier point in time.



Firstseen (UTC)	IP address	Hostname	SBL	ASN	Country	Active?
2024-01-25 09:01:12	64.31.22.34	s21.hosterpk.com	Not listed	AS46475 LIMESTONENETWORKS	US	yes

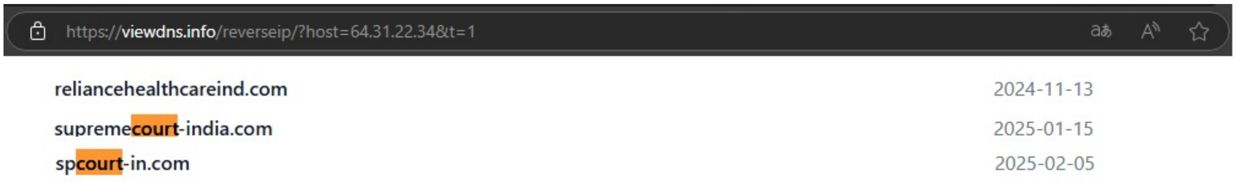
Malware URLs

The table below shows all malware URLs that are associated with this particular host.

Dateadded (UTC)	URL	Status	Tags	Reporter
2024-01-25 09:01:12	http://ftsolutions.com.pk/v1220-55000.exe	Offline	dropped-by-SmokeLoader LummaStealer	Casperinous

Figure 13: Malware history for the IP

While performing a reverse IP lookup for the address **64.31.22.34**, we discovered that another domain, **supremecourt-india[.]com**, was also hosted on the same server. This further suggests that multiple phishing sites may be operating from the same infrastructure, potentially targeting users by impersonating government entities in an attempt to harvest user data.

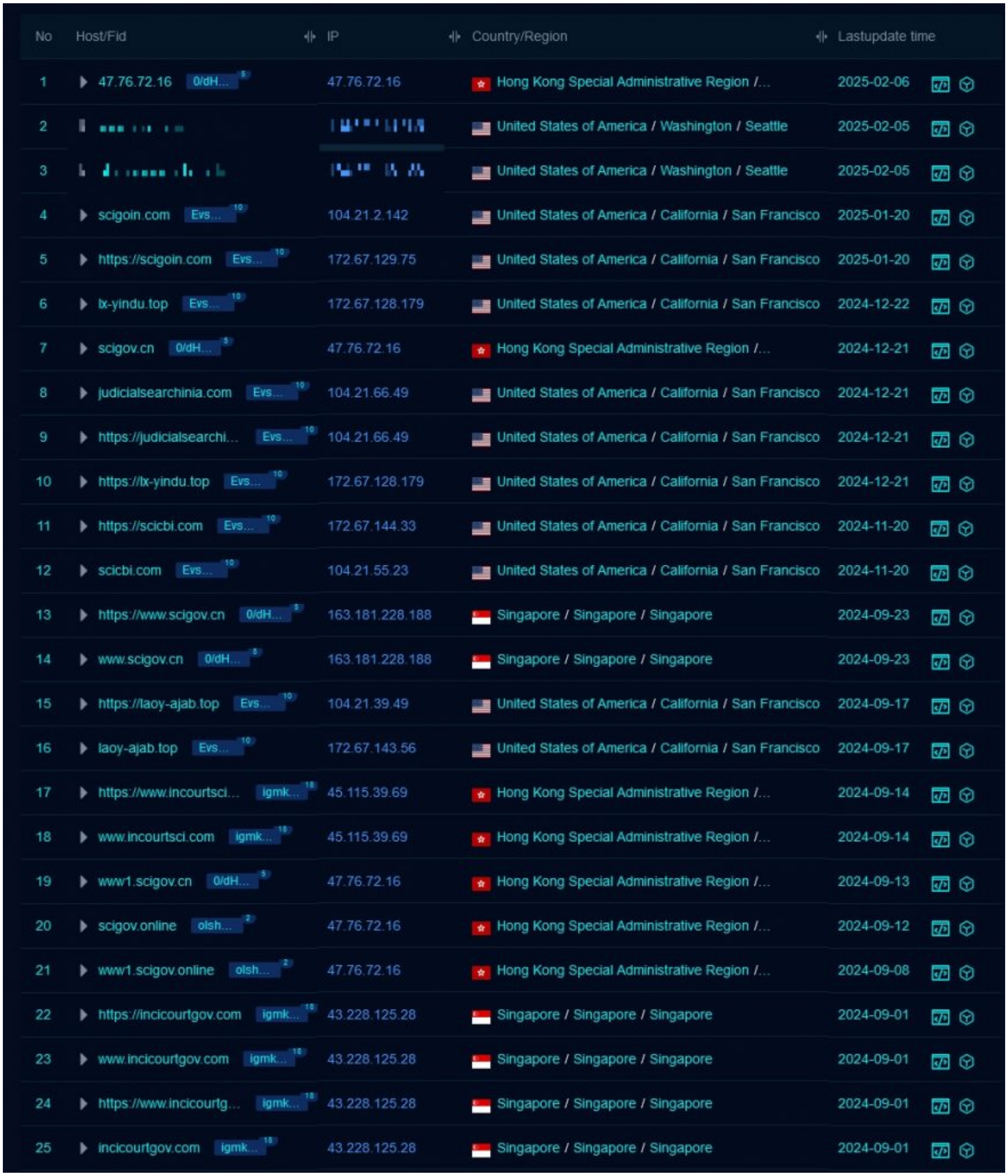


https://viewdns.info/reverseip/?host=64.31.22.34&t=1

reliancehealthcareind.com	2024-11-13
supremecourt-india.com	2025-01-15
spcourt-in.com	2025-02-05

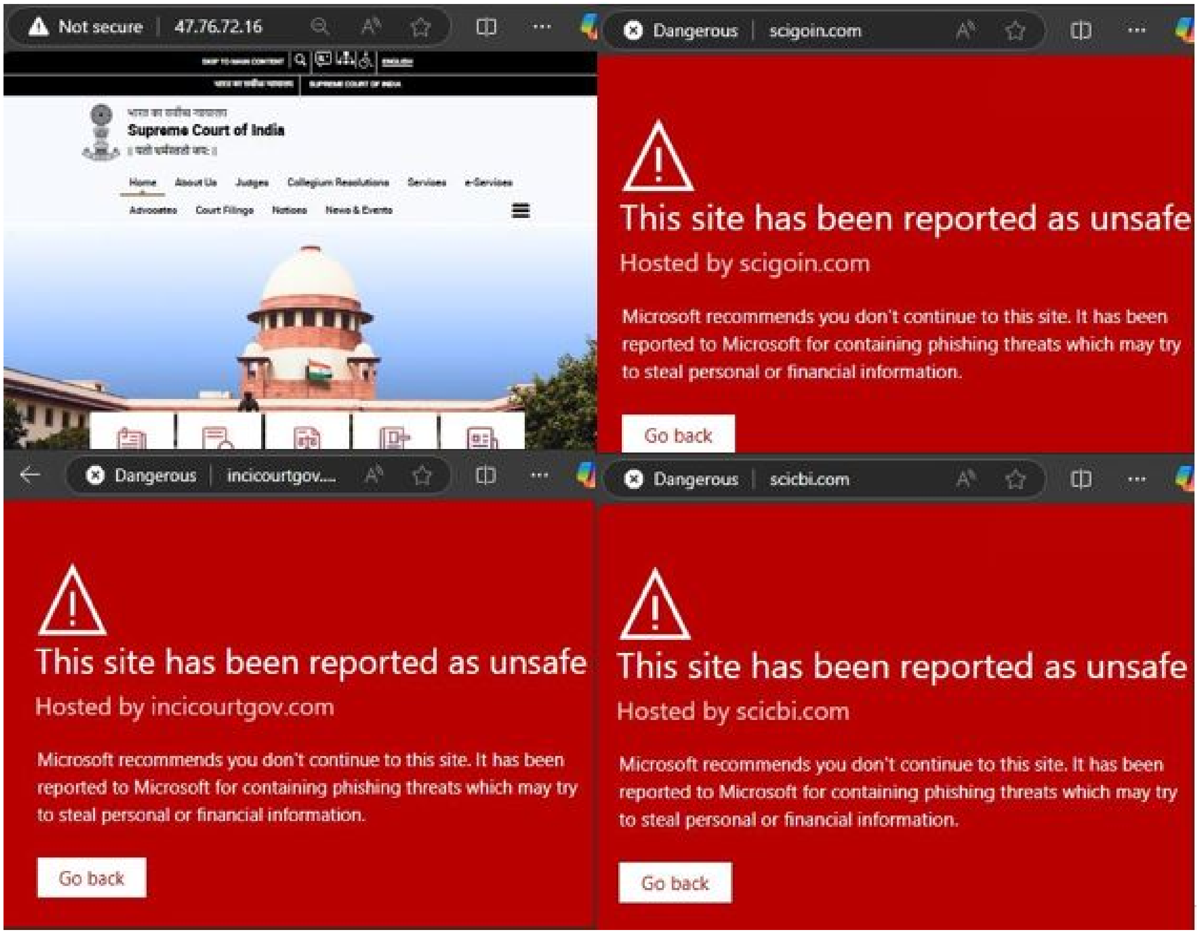
Figure 14: Reverse IP Results

By searching with the filter for the website title **“The Supreme Court of India | India”** and specifying that the hosting country is not India, we obtained several results showing fake sites, some of which were already on the block list as shown in Fig 16. From these findings, it’s clear that these Phishing sites have been active for quite some time, indicating a prolonged campaign. However, the exact **modus operandi** of the attacker remains unclear. Specifically, it is unknown how the attacker plans to approach users and convince them to divulge their PII on these fraudulent sites.



No	Host/Fid	IP	Country/Region	Lastupdate time
1	47.76.72.16 0/dH... 5	47.76.72.16	Hong Kong Special Administrative Region /...	2025-02-06
2	[redacted]	[redacted]	United States of America / Washington / Seattle	2025-02-05
3	[redacted]	[redacted]	United States of America / Washington / Seattle	2025-02-05
4	scigoin.com Evs... 10	104.21.2.142	United States of America / California / San Francisco	2025-01-20
5	https://scigoin.com Evs... 10	172.67.129.75	United States of America / California / San Francisco	2025-01-20
6	lx-yindu.top Evs... 10	172.67.128.179	United States of America / California / San Francisco	2024-12-22
7	scigov.cn 0/dH... 5	47.76.72.16	Hong Kong Special Administrative Region /...	2024-12-21
8	judicialsearchinia.com Evs... 10	104.21.66.49	United States of America / California / San Francisco	2024-12-21
9	https://judicialsearchi... Evs... 10	104.21.66.49	United States of America / California / San Francisco	2024-12-21
10	https://lx-yindu.top Evs... 10	172.67.128.179	United States of America / California / San Francisco	2024-12-21
11	https://scicbi.com Evs... 10	172.67.144.33	United States of America / California / San Francisco	2024-11-20
12	scicbi.com Evs... 10	104.21.55.23	United States of America / California / San Francisco	2024-11-20
13	https://www.scigov.cn 0/dH... 5	163.181.228.188	Singapore / Singapore / Singapore	2024-09-23
14	www.scigov.cn 0/dH... 5	163.181.228.188	Singapore / Singapore / Singapore	2024-09-23
15	https://laoy-ajab.top Evs... 10	104.21.39.49	United States of America / California / San Francisco	2024-09-17
16	laoy-ajab.top Evs... 10	172.67.143.56	United States of America / California / San Francisco	2024-09-17
17	https://www.incourtsci... igmk... 18	45.115.39.69	Hong Kong Special Administrative Region /...	2024-09-14
18	www.incourtsci.com igmk... 18	45.115.39.69	Hong Kong Special Administrative Region /...	2024-09-14
19	www1.scigov.cn 0/dH... 5	47.76.72.16	Hong Kong Special Administrative Region /...	2024-09-13
20	scigov.online olsh... 2	47.76.72.16	Hong Kong Special Administrative Region /...	2024-09-12
21	www1.scigov.online olsh... 2	47.76.72.16	Hong Kong Special Administrative Region /...	2024-09-08
22	https://incicourtgov.com igmk... 18	43.228.125.28	Singapore / Singapore / Singapore	2024-09-01
23	www.incicourtgov.com igmk... 18	43.228.125.28	Singapore / Singapore / Singapore	2024-09-01
24	https://www.incicourtg... igmk... 18	43.228.125.28	Singapore / Singapore / Singapore	2024-09-01
25	incicourtgov.com igmk... 18	43.228.125.28	Singapore / Singapore / Singapore	2024-09-01

Figure 15: FOFA result for the website title



This site has been reported as unsafe

Hosted by scigoin.com

Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing phishing threats which may try to steal personal or financial information.

This site has been reported as unsafe

Hosted by incicourtgov.com

Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing phishing threats which may try to steal personal or financial information.

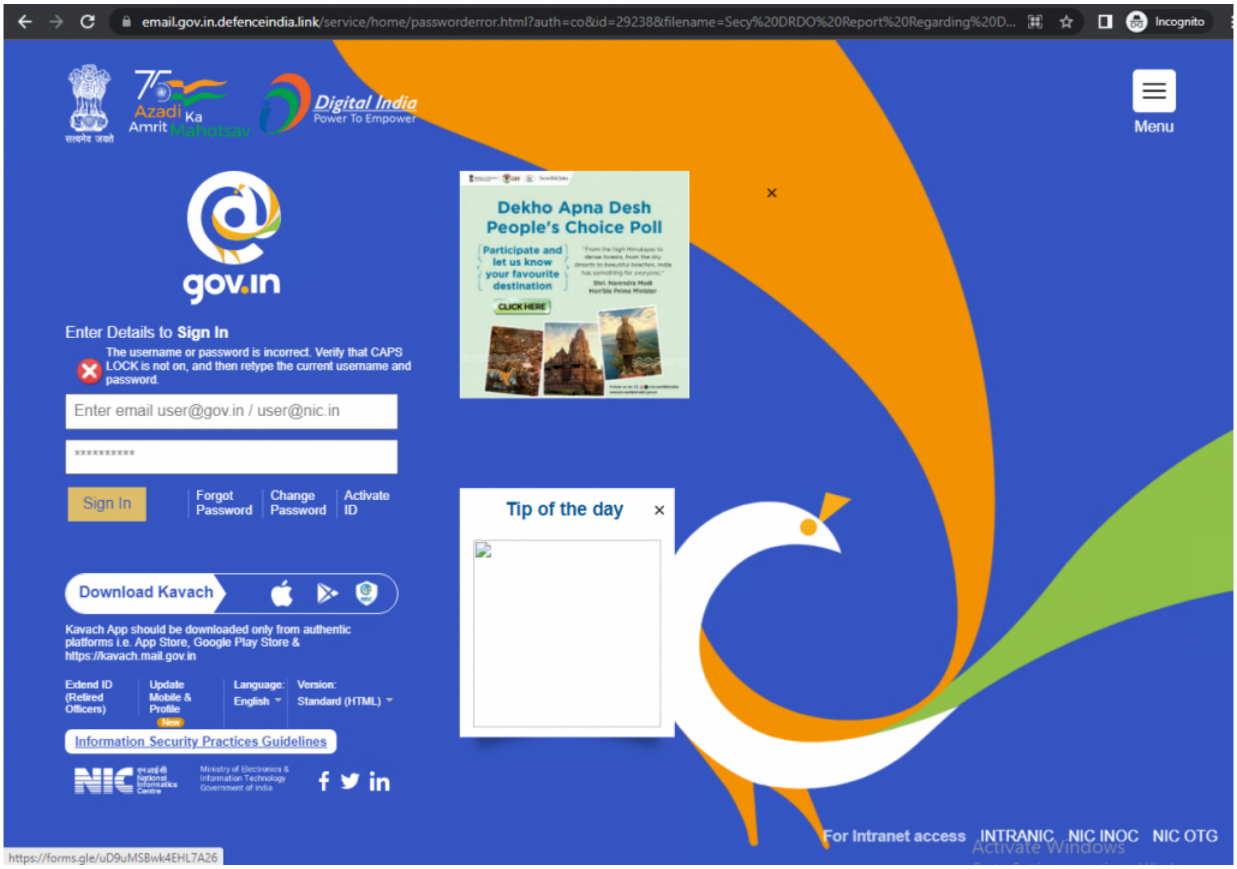
This site has been reported as unsafe

Hosted by scicbi.com

Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing phishing threats which may try to steal personal or financial information.

Figure 16: Screenshots of Supreme Court impersonating sites

Now let’s examine the second site mentioned in the tweet, which is **“email[.]gov[.]in[.]defenceindia[.]link”**. This also is a phishing domain impersonating an official Indian government site.



email.gov.in.defenceindia.link/service/home/passworderror.html?auth=co&id=29238&filename=Secy%20DRDO%20Report%20Regarding%20D...

Enter Details to Sign In

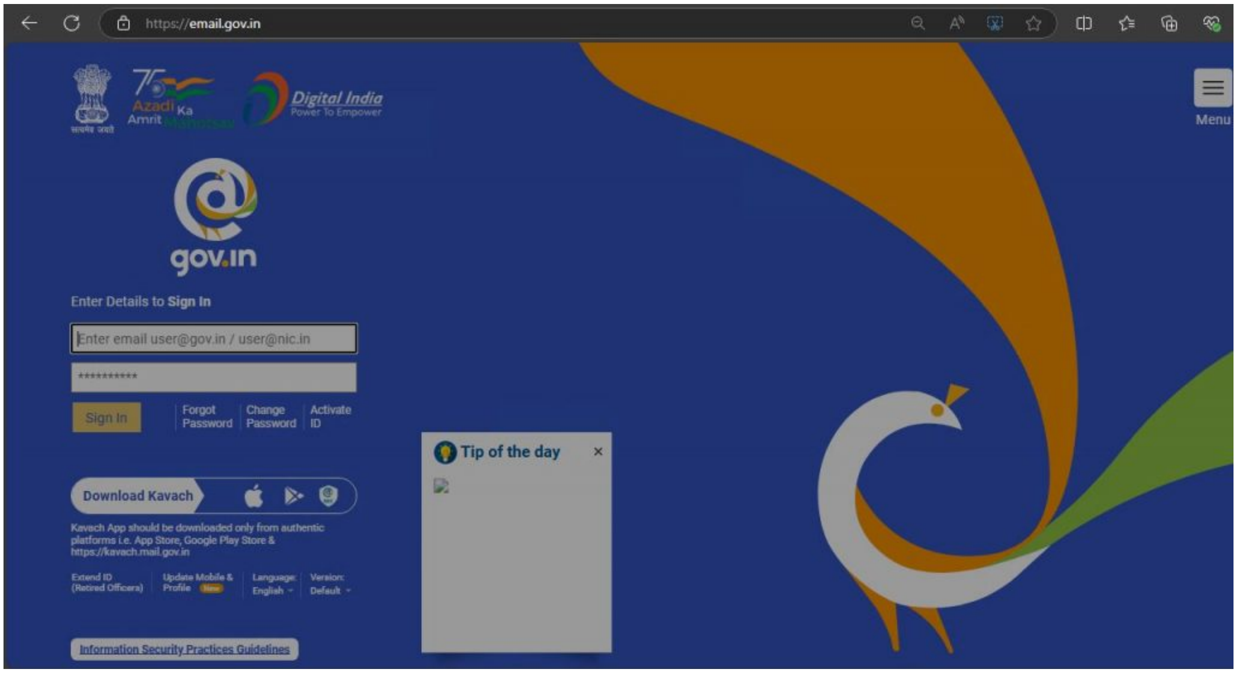
The username or password is incorrect. Verify that CAPS LOCK is not on, and then retype the current username and password.

Enter email user@gov.in / user@nic.in

Kavach App should be downloaded only from authentic platforms i.e. App Store, Google Play Store & https://kavach.mail.gov.in

https://forms.gle/uD9uMSBwk4EHL7A26

Figure 17: Phishing site



https://email.gov.in

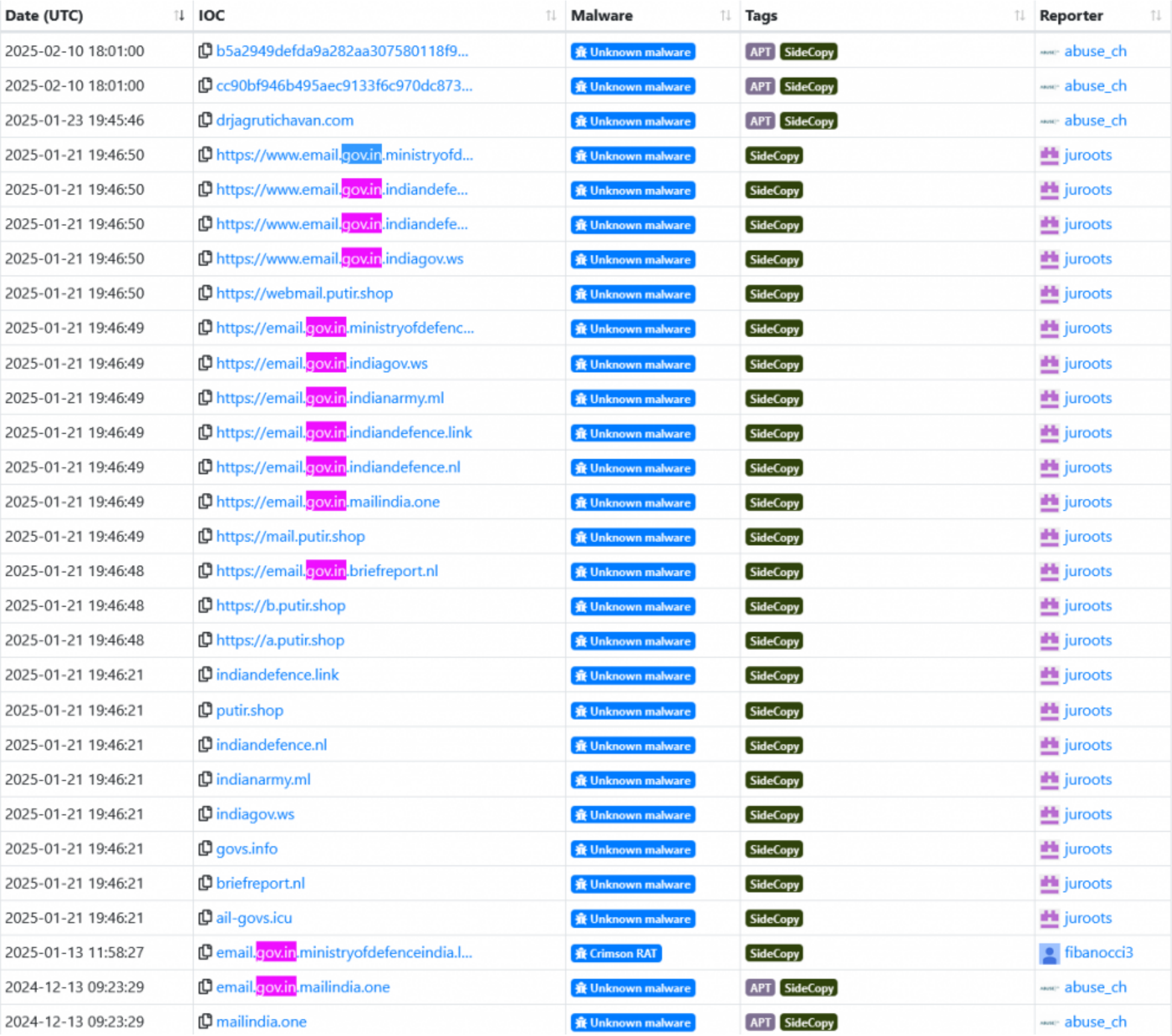
Enter Details to Sign In

Enter email user@gov.in / user@nic.in

Kavach App should be downloaded only from authentic platforms i.e. App Store, Google Play Store & https://kavach.mail.gov.in

Figure 18: Original Site

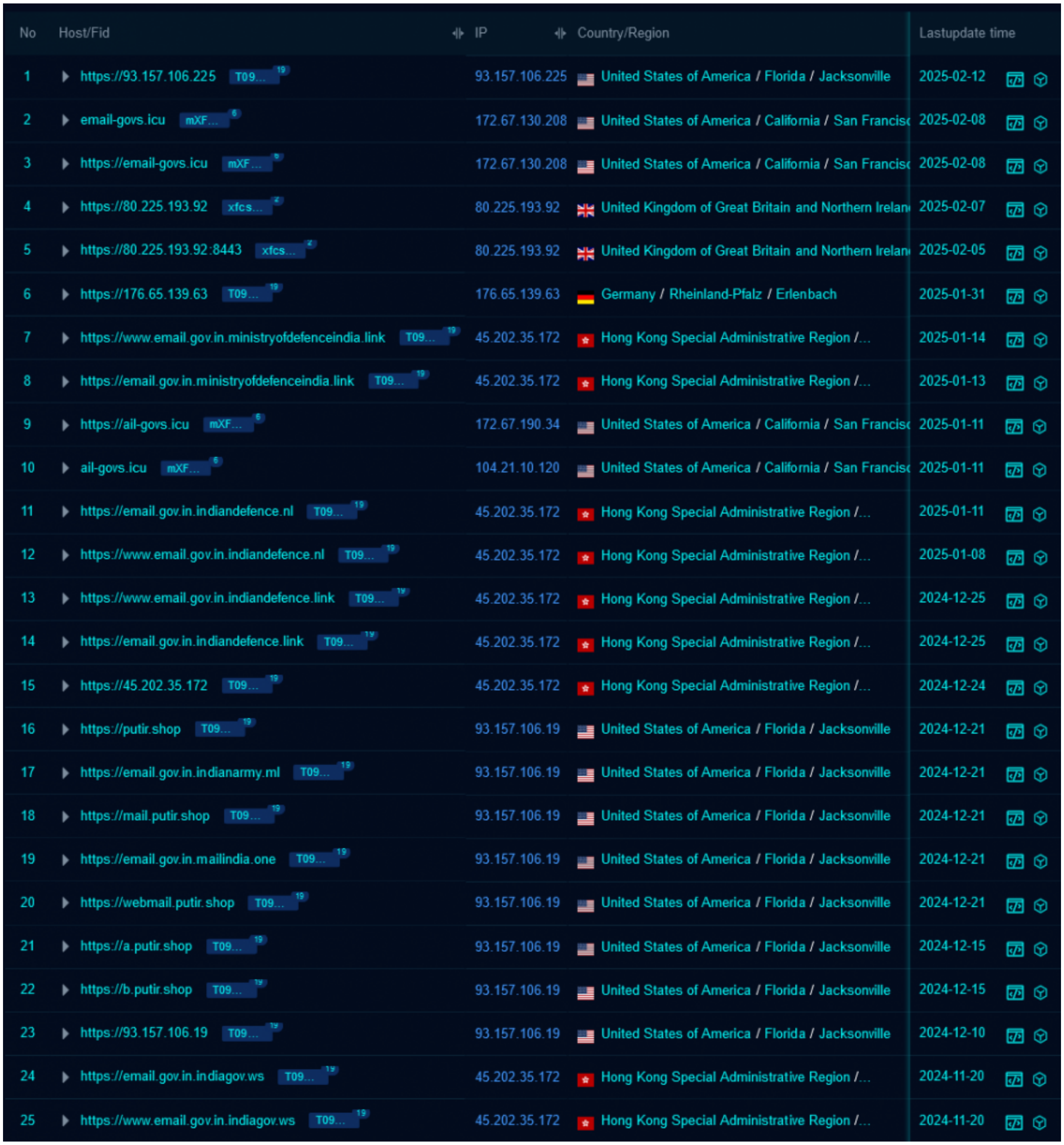
Of late, many impersonators of “email.gov.in” have been seen in the wild, searching on **Malware Bazaar**, we can see tags like Malware and RATs associated with them, all linked to **SideCopy**, a well-known APT operating out of Pakistan.



Date (UTC)	IOC	Malware	Tags	Reporter
2025-02-10 18:01:00	b5a2949defda9a282aa307580118f9...	Unknown malware	APT SideCopy	abuse_ch
2025-02-10 18:01:00	cc90bf946b495aec9133f6c970dc873...	Unknown malware	APT SideCopy	abuse_ch
2025-01-23 19:45:46	drjagrutichavan.com	Unknown malware	APT SideCopy	abuse_ch
2025-01-21 19:46:50	https://www.email.gov.in.ministryofd...	Unknown malware	SideCopy	juroots
2025-01-21 19:46:50	https://www.email.gov.in.indiandefe...	Unknown malware	SideCopy	juroots
2025-01-21 19:46:50	https://www.email.gov.in.indiandefe...	Unknown malware	SideCopy	juroots
2025-01-21 19:46:50	https://www.email.gov.in.indiagov.ws	Unknown malware	SideCopy	juroots
2025-01-21 19:46:50	https://webmail.putir.shop	Unknown malware	SideCopy	juroots
2025-01-21 19:46:49	https://email.gov.in.ministryofdefenc...	Unknown malware	SideCopy	juroots
2025-01-21 19:46:49	https://email.gov.in.indiagov.ws	Unknown malware	SideCopy	juroots
2025-01-21 19:46:49	https://email.gov.in.indianarmy.ml	Unknown malware	SideCopy	juroots
2025-01-21 19:46:49	https://email.gov.in.indiandefence.link	Unknown malware	SideCopy	juroots
2025-01-21 19:46:49	https://email.gov.in.indiandefence.nl	Unknown malware	SideCopy	juroots
2025-01-21 19:46:49	https://email.gov.in.mailindia.one	Unknown malware	SideCopy	juroots
2025-01-21 19:46:49	https://mail.putir.shop	Unknown malware	SideCopy	juroots
2025-01-21 19:46:48	https://email.gov.in.briefreport.nl	Unknown malware	SideCopy	juroots
2025-01-21 19:46:48	https://b.putir.shop	Unknown malware	SideCopy	juroots
2025-01-21 19:46:48	https://a.putir.shop	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	indiandefence.link	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	putir.shop	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	indiandefence.nl	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	indianarmy.ml	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	indiagov.ws	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	govs.info	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	briefreport.nl	Unknown malware	SideCopy	juroots
2025-01-21 19:46:21	ail-govs.icu	Unknown malware	SideCopy	juroots
2025-01-13 11:58:27	email.gov.in.ministryofdefenceindia.l...	Crimson RAT	SideCopy	fibanocci3
2024-12-13 09:23:29	email.gov.in.mailindia.one	Unknown malware	APT SideCopy	abuse_ch
2024-12-13 09:23:29	mailindia.one	Unknown malware	APT SideCopy	abuse_ch

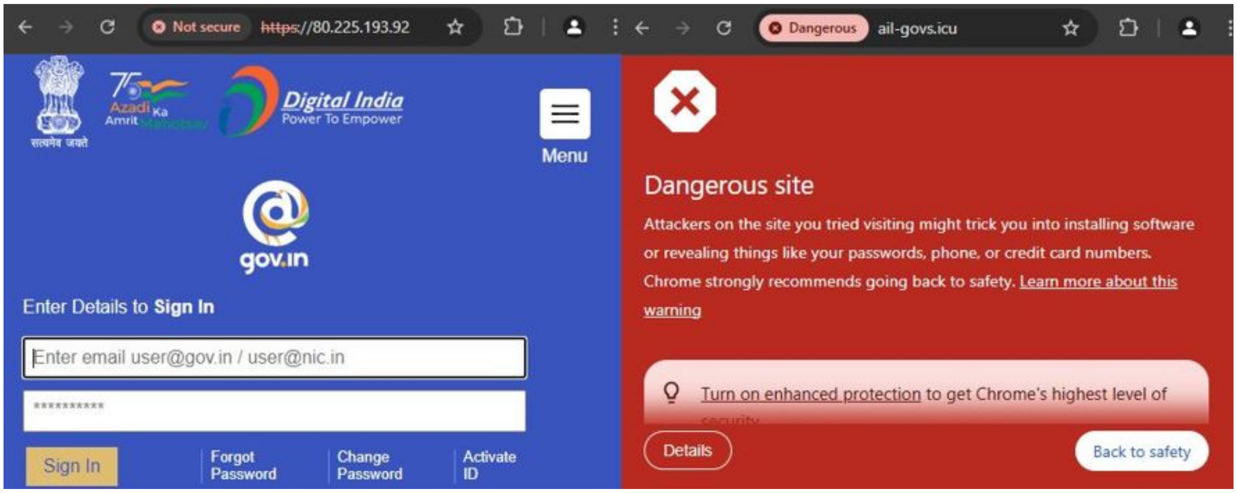
Figure 19: SideCopy IoCs

The data shown in the image below was obtained by applying the filter for the website title "Email Web Client Sign In" with the hosting country, not India.



No	Host/Fid	IP	Country/Region	Lastupdate time
1	https://93.157.106.225 T09... 19	93.157.106.225	United States of America / Florida / Jacksonville	2025-02-12
2	email-govs.icu mXF... 6	172.67.130.208	United States of America / California / San Francisc	2025-02-08
3	https://email-govs.icu mXF... 6	172.67.130.208	United States of America / California / San Francisc	2025-02-08
4	https://80.225.193.92 xfcs... 2	80.225.193.92	United Kingdom of Great Britain and Northern Irelan	2025-02-07
5	https://80.225.193.92:8443 xfcs... 2	80.225.193.92	United Kingdom of Great Britain and Northern Irelan	2025-02-05
6	https://176.65.139.63 T09... 19	176.65.139.63	Germany / Rheinland-Pfalz / Erlenbach	2025-01-31
7	https://www.email.gov.in.ministryofdefenceindia.link T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2025-01-14
8	https://email.gov.in.ministryofdefenceindia.link T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2025-01-13
9	https://ail-govs.icu mXF... 6	172.67.190.34	United States of America / California / San Francisc	2025-01-11
10	ail-govs.icu mXF... 6	104.21.10.120	United States of America / California / San Francisc	2025-01-11
11	https://email.gov.in.indiandefence.nl T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2025-01-11
12	https://www.email.gov.in.indiandefence.nl T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2025-01-08
13	https://www.email.gov.in.indiandefence.link T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2024-12-25
14	https://email.gov.in.indiandefence.link T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2024-12-25
15	https://45.202.35.172 T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2024-12-24
16	https://putir.shop T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-21
17	https://email.gov.in.indianarmy.ml T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-21
18	https://mail.putir.shop T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-21
19	https://email.gov.in.mailindia.one T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-21
20	https://webmail.putir.shop T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-21
21	https://a.putir.shop T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-15
22	https://b.putir.shop T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-15
23	https://93.157.106.19 T09... 19	93.157.106.19	United States of America / Florida / Jacksonville	2024-12-10
24	https://email.gov.in.indiagov.ws T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2024-11-20
25	https://www.email.gov.in.indiagov.ws T09... 19	45.202.35.172	Hong Kong Special Administrative Region /...	2024-11-20

Figure 20: FOFA results for the title client sign-in



Dangerous site

Attackers on the site you tried visiting might trick you into installing software or revealing things like your passwords, phone, or credit card numbers. Chrome strongly recommends going back to safety. Learn more about this warning

Turn on enhanced protection to get Chrome's highest level of security

Figure 21: Screenshots of sites impersonating email.gov.in

Phishing-based traps have become more and more sophisticated of late, making it difficult for users to discern. Netizens should be cautious of the links they are clicking and do some basic checks to make sure they are being redirected to the right channel. They should also be cautious of the data that they are revealing and should discern if such information is definitely needed for their query to be solved. Cybersecurity awareness and having a reputed malicious website blocker such as **"K7 Total Security"** can help users stay protected from such online scams.

References

- https://x.com/500mk500/status/1887282887331901851
- https://x.com/Cyberteam008/status/1881174353376874861
- https://github.com/stamparm/maltrail/blob/master/trails/static/malware/apt_transparenttribe.txt