**Published on June 3, 2025.**

# The weekly trending report of Operation India related Hacktivist groups

*Reported by **Team D4rkn3ttz***

**Effected date: May 22 – May 29, 2025.**

***We mentioned the all date based on those date.*

## Table of Contents

Published on June 3, 2025.

# 1. Executive Summary

We confirmed the coordinated hacktivist activities to targeting Indian institutions spiked significantly. **12 hacktivist groups** operated under the **Operation India**, carrying out attacks including defacements, SQL injection (SQLi), data leaks, and DDoS attacks.

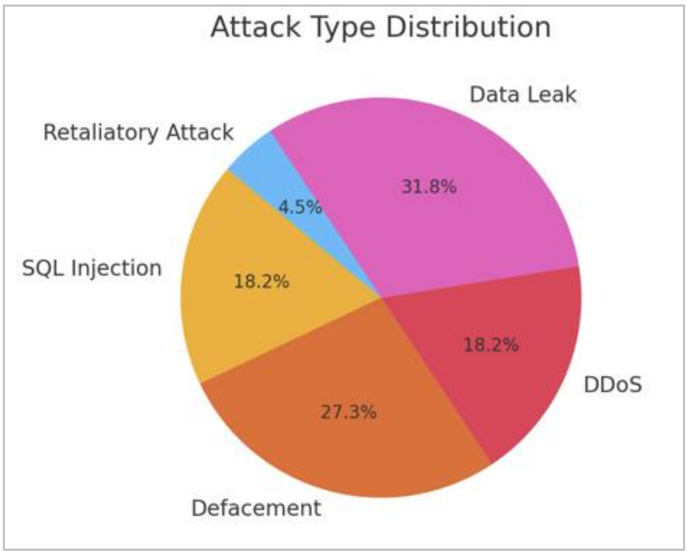
The most attacks were politically or ideologically motivated and intended to provoke symbolic disruption. The groups primarily used **Telegram** for communication and dark forums for sharing stolen data.

# 2. Key Threat Actor Activity

| Group | Tools Used | Attack Types | Victims / Systems | Observed Date |
|---|---|---|---|---|
| ClayOxtymus1337 | sqlmap, Telegram | SQLi, Data Exfiltration | Public schools, edu portals | *2025.05.22.*<br>*2025.05.25.*<br>*2025.05.27.*<br>*2025.05.28.* |
| Cyb3r Drag0nz | Manual tools, ransomware keys | Defacement, Ransomware | Military, gov sites | *2025.05.25.*<br>*2025.05.26.* |
| TengkorakCyberCrew | Manual injection | Defacement | Education, NGO, religion | *2025.05.27.* |
| ZLC.ID | AnonPaste, ZIP | Data Leaks, Reposting | Local gov, officials | *2025.05.26.* |
| Keymous+ | Check-host, botnets | DDoS, Infra disruption | Telecom providers (BSNL etc.) | *2025.05.28.*<br>*2025.05.29.* |

*Table 1. Tactical Overview of Hacktivist Campaigns*

## 2.1. Distribution of attack type



*Graph 1. The pie chart of the attack types*

Based on the current dataset, Data Leak incidents constitute the largest share of observed attack types, accounting for 31.8% of the total. This suggests that adversaries are heavily targeting sensitive information, likely aiming to exploit it for financial gain, espionage, or reputational damage.

**High Incidence of Defacement Attacks**

The second most frequent attack type is Defacement (27.3%), which indicates a significant interest among threat actors in disrupting online presence or spreading ideological messages. Such attacks are often carried out by hacktivist groups or individuals seeking public attention.

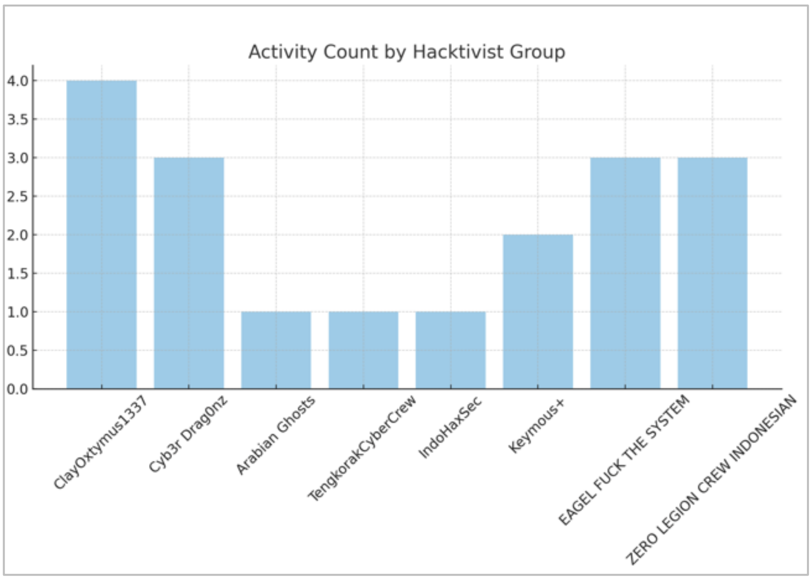
**Technical Exploits and Service Disruption**

SQL Injection and DDoS attacks are equally prevalent, each comprising 18.2% of the incidents. The presence of SQL Injection highlights vulnerabilities in web application security, while DDoS reflects attempts to disrupt service availability, possibly as part of broader campaigns or as retaliation.

**Retaliatory Attacks and Emotional Drivers**

Lastly, Retaliatory Attacks represent a smaller portion (4.5%), but their targeted and emotionally driven nature suggests a different motivation compared to other attack types.

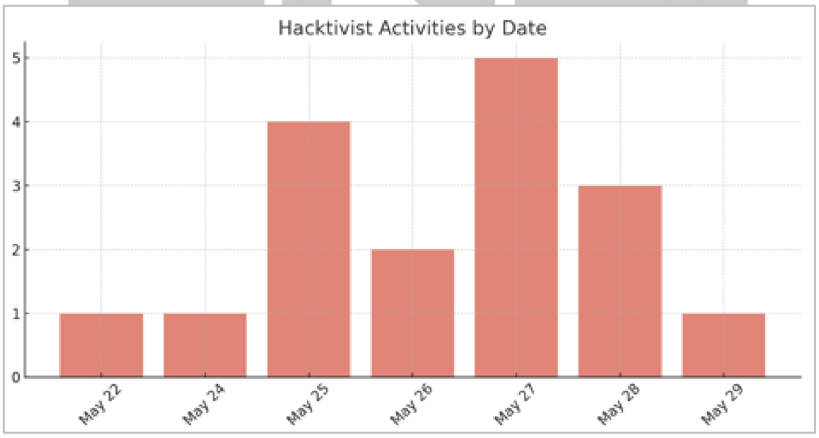
## 2.2. The count of Hacktivist group’s activities



*Graph 2. The count of the activities by groups*

ClayOxtymus1337 and Cyb3r Drag0nz were the most active, followed closely by ZLC.ID, Keymous+, and EAGEL FUCK THE SYSTEM.

## 2.3. The count of Hacktivist group’s effected issues



*Graph 3. The count of the activities by date*

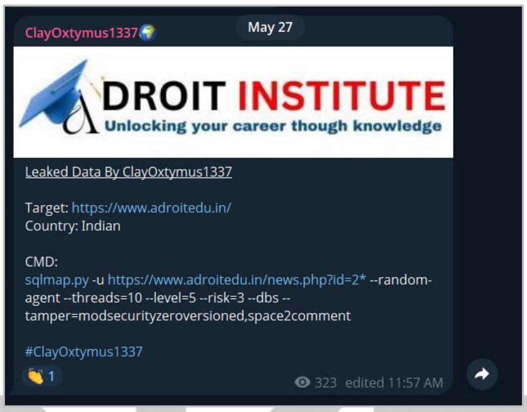
From May 22 to May 29, there was sustained attack activity, with most groups conducting at least one attack during this period. The peak occurred on May 27, when five incidents were reported.

# 3. The analysis of 5 Hacktivist groups

## 3.1. ClayOxtymus1337

### 3.1.1. Attack Behavior

ClayOxtymus1337 exhibits a clear pattern of automated SQL injection attacks using sqlmap.py. In a documented example, they published a command.



ClayOxtymus1337🌍 May 27

Leaked Data By ClayOxtymus1337

Target: https://www.adroitedu.in/
Country: Indian

CMD:
sqlmap.py -u https://www.adroitedu.in/news.php?id=2* --random-agent --threads=10 --level=5 --risk=3 --dbs --tamper=modsecurityzeroversioned,space2comment

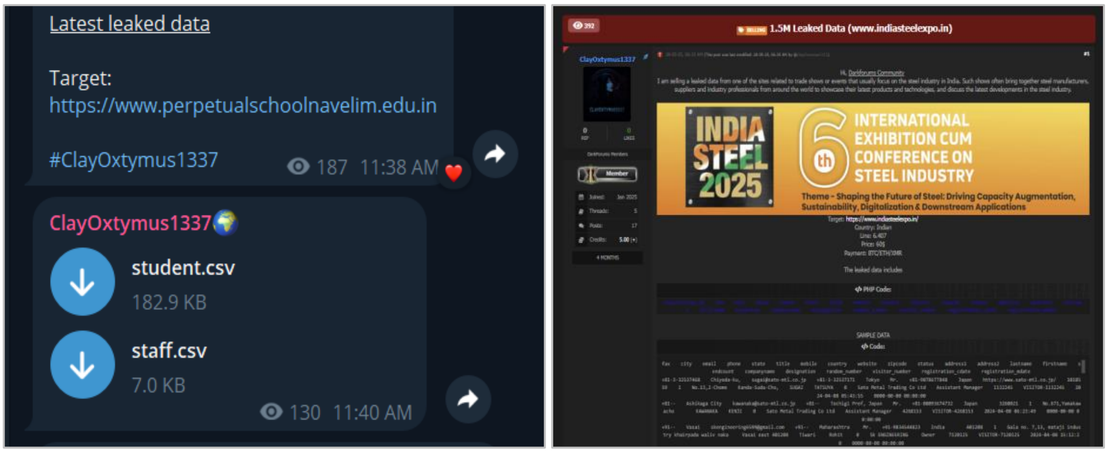
#ClayOxtymus1337
👏 1 323 edited 11:57 AM

*Figure 1. The screenshot of the mentioned SQLi tool by ClayOxtymus1337*

```
sqlmap.py -u https://www.adroitedu.in/news.php?id=2 …
```

This command string reveals the use of --random-agent, multi-threaded brute-force (--threads=10), and tampering modules (e.g., space2comment), indicating automation tuned for evasion and wide probing.

### 3.1.2. Analysis of the leaked files



Latest leaked data

Target:
https://www.perpetualschoolnavelim.edu.in

#ClayOxtymus1337 187 11:38 AM ❤️

ClayOxtymus1337🌍
student.csv 182.9 KB
staff.csv 7.0 KB
130 11:40 AM

392 SELLING 1.5M Leaked Data (www.indiasteelexpo.in)

ClayOxtymus1337
Joined: Jan 2025
Threads: 5
Posts: 17
Credits: 5.00

Hi, Darkforums Community
I am selling a leaked data from one of the sites related to trade shows or events that usually focus on the steel industry in India. Such shows often bring together steel manufacturers, suppliers and industry professionals from around the world to showcase their latest products and technologies, and discuss the latest developments in the steel industry.

INDIA STEEL 2025
6th INTERNATIONAL EXHIBITION CUM CONFERENCE ON STEEL INDUSTRY
Theme - Shaping the Future of Steel: Driving Capacity Augmentation, Sustainability, Digitalization & Downstream Applications

Target: https://www.indiasteelexpo.in/
Country: Indian
Line: 6.407
Price: 60$
Payment: BTC/ETH/XMR

The leaked data includes

PHP Code:

SAMPLE DATA
Code:

*Figure 2. The screenshots of the posts published by ClayOxtymus1337*

Two separate data leak incidents were recently attributed to the threat actor **ClayOxtymus1337**, indicating a continued focus on targeting educational and industrial entities across India.

### Perpetual Succour Convent High School (Goa, India)

On May 27, the threat actor leaked data from the website perpetualschoolnavelim.edu.in, including two CSV files:

- `student.csv` (182.9 KB): Contains personally identifiable information such as student names, registration numbers, prior institutions, admission years, and academic performance.
- `staff.csv` (7.0 KB): Includes departmental assignments and staff employment history.

The exposure of both student and staff data introduces significant **privacy risks** and may lead to **identity misuse or targeted phishing attacks**, particularly against minors.

### India Steel Expo (indiatsteelexpo.in)

A much larger breach was also reported involving over **1.5 million records** related to participants and registrants of the India Steel Expo. The leaked database appears to contain:

- Personally identifiable information (PII)
- Professional affiliations
- Contact details
- IP addresses and other metadata

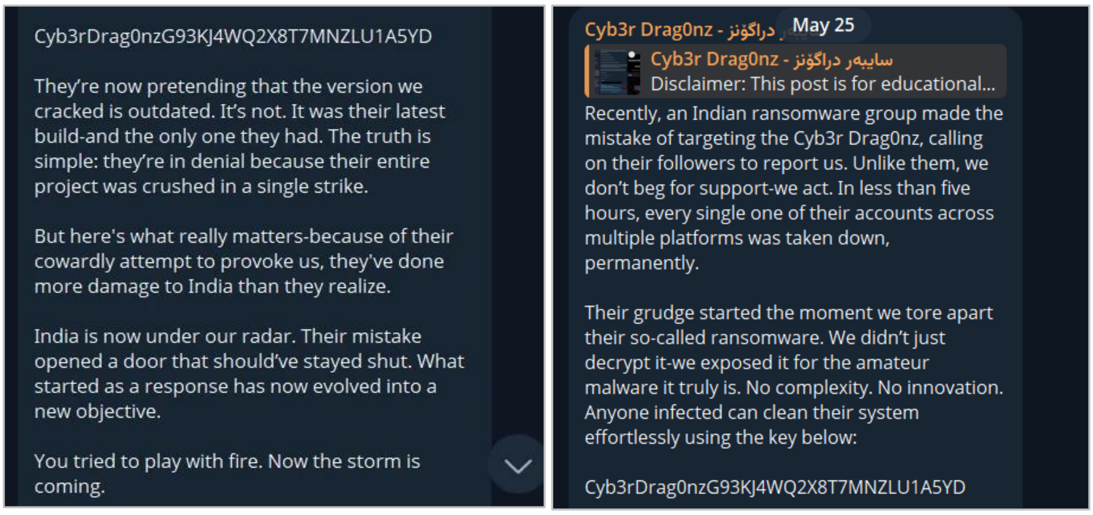
The scale and industrial relevance of this dataset raise concerns about **corporate espionage**, **social engineering**, and potential abuse by nation-state actors or competitors.

Files were shared in formats such as .csv, .xlsx, usually small-sized (under 200KB), suggesting **precision targeting** or limited privilege access during exfiltration.

Their repeated use of public schools and trade fair sites as victims indicates as belows:

- Preference for under-secured, high-visibility targets
- Use of education-sector domains to maximize **symbolic and reputational disruption**

## 3.2. Cyb3r Drag0nz



Cyb3rDrag0nzG93KJ4WQ2X8T7MNZLU1A5YD

They're now pretending that the version we cracked is outdated. It's not. It was their latest build-and the only one they had. The truth is simple: they're in denial because their entire project was crushed in a single strike.

But here's what really matters-because of their cowardly attempt to provoke us, they've done more damage to India than they realize.

India is now under our radar. Their mistake opened a door that should've stayed shut. What started as a response has now evolved into a new objective.

You tried to play with fire. Now the storm is coming.

Cyb3r Drag0nz - دراگونز May 25

Cyb3r Drag0nz - سایبر دراگونز
Disclaimer: This post is for educational...

Recently, an Indian ransomware group made the mistake of targeting the Cyb3r Drag0nz, calling on their followers to report us. Unlike them, we don't beg for support-we act. In less than five hours, every single one of their accounts across multiple platforms was taken down, permanently.

Their grudge started the moment we tore apart their so-called ransomware. We didn't just decrypt it-we exposed it for the amateur malware it truly is. No complexity. No innovation. Anyone infected can clean their system effortlessly using the key below:

Cyb3rDrag0nzG93KJ4WQ2X8T7MNZLU1A5YD

*Figure 3. The screenshots of the mentioned decryption and retaliation by Cyb3r Drag0nz*

### 3.2.1. Attack Behavior

On May 25, the hacktivist group **Cyb3r Drag0nz** issued a retaliatory statement, alleging that their accounts had been flagged by Indian ransomware hunting teams. In response, the group launched a revenge-driven campaign targeting Indian digital assets.

Key elements of the operation included:

- **Decryption key leaks**: The group analyzed and publicly posted decrypted ransomware keys, potentially undermining ongoing remediation efforts.
- **Direct threats**: Messages such as *"Delete all your accounts within 5 hours"* were disseminated to instill urgency and fear.
- **Website defacement**: Several sites were altered to display the **Cyb3r Drag0nz logo** alongside anti-India slogans.
- **Ideologically motivated messaging**: The campaign blended conventional cyber tactics with hostile narratives aimed at India, signaling ideological intent.
- **Narrative justification**: The group cited previous **platform bans and suspensions** as their rationale for the attack.
- **Psychological operations**: Long-term messaging such as *"India is now on our radar"* suggests the group may pursue **persistent psychological pressure** or future campaigns.

The incident reflects the increasing overlap between **cyber retaliation and ideological warfare**, and highlights the potential for hacktivist groups to shift from single-event operations to **multi-stage influence campaigns**.

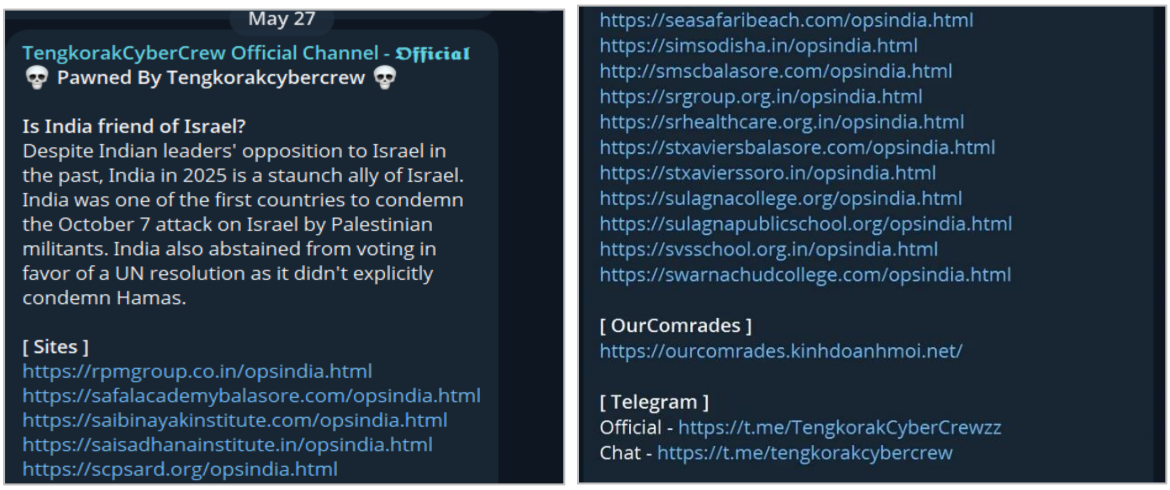
### 3.2.2. Analysis of the leaked files

As part of their escalating campaign, **Cyb3r Drag0nz** extended their operations to include Indian military-related web infrastructure. Notably:

- **Indian Army and Ministry of Defense websites** were observed either **offline** or displaying **altered (defaced) content**, indicating service disruption or unauthorized modification.
- The defaced pages prominently featured **Cyb3r Drag0nz logos** alongside **politically charged messages**, underscoring the group's use of defacement as both a technical and ideological tool.

These activities suggest an intent not only to **embarrass or disrupt official channels**, but also to **amplify anti-India narratives** through visible digital vandalism.

## 3.3. TengkorakCyberCrew



May 27

TengkorakCyberCrew Official Channel - 𝔒𝔣𝔣𝔦𝔠𝔦𝔞𝔩
💀 Pawned By Tengkorakcybercrew 💀

Is India friend of Israel?
Despite Indian leaders' opposition to Israel in the past, India in 2025 is a staunch ally of Israel. India was one of the first countries to condemn the October 7 attack on Israel by Palestinian militants. India also abstained from voting in favor of a UN resolution as it didn't explicitly condemn Hamas.

[ Sites ]
https://rpmgroup.co.in/opsindia.html
https://safalacademybalasore.com/opsindia.html
https://saibinayakinstitute.com/opsindia.html
https://saisadhanainstitute.in/opsindia.html
https://scpsard.org/opsindia.html

https://seasafaribeach.com/opsindia.html
https://simsodisha.in/opsindia.html
http://smscbalasore.com/opsindia.html
https://srgroup.org.in/opsindia.html
https://srhealthcare.org.in/opsindia.html
https://stxaviersbalasore.com/opsindia.html
https://stxavierssoro.in/opsindia.html
https://sulagnacollege.org/opsindia.html
https://sulagnapublicschool.org/opsindia.html
https://svsschool.org.in/opsindia.html
https://swarnachudcollege.com/opsindia.html

[ OurComrades ]
https://ourcomrades.kinhdoanhmoi.net/

[ Telegram ]
Official - https://t.me/TengkorakCyberCrewzz
Chat - https://t.me/tengkorakcybercrew

*Figure 4. The screenshots of the listed defacement targets and campaign message by TengkorakCyberCrew*

### 3.3.1. Attack Behavior

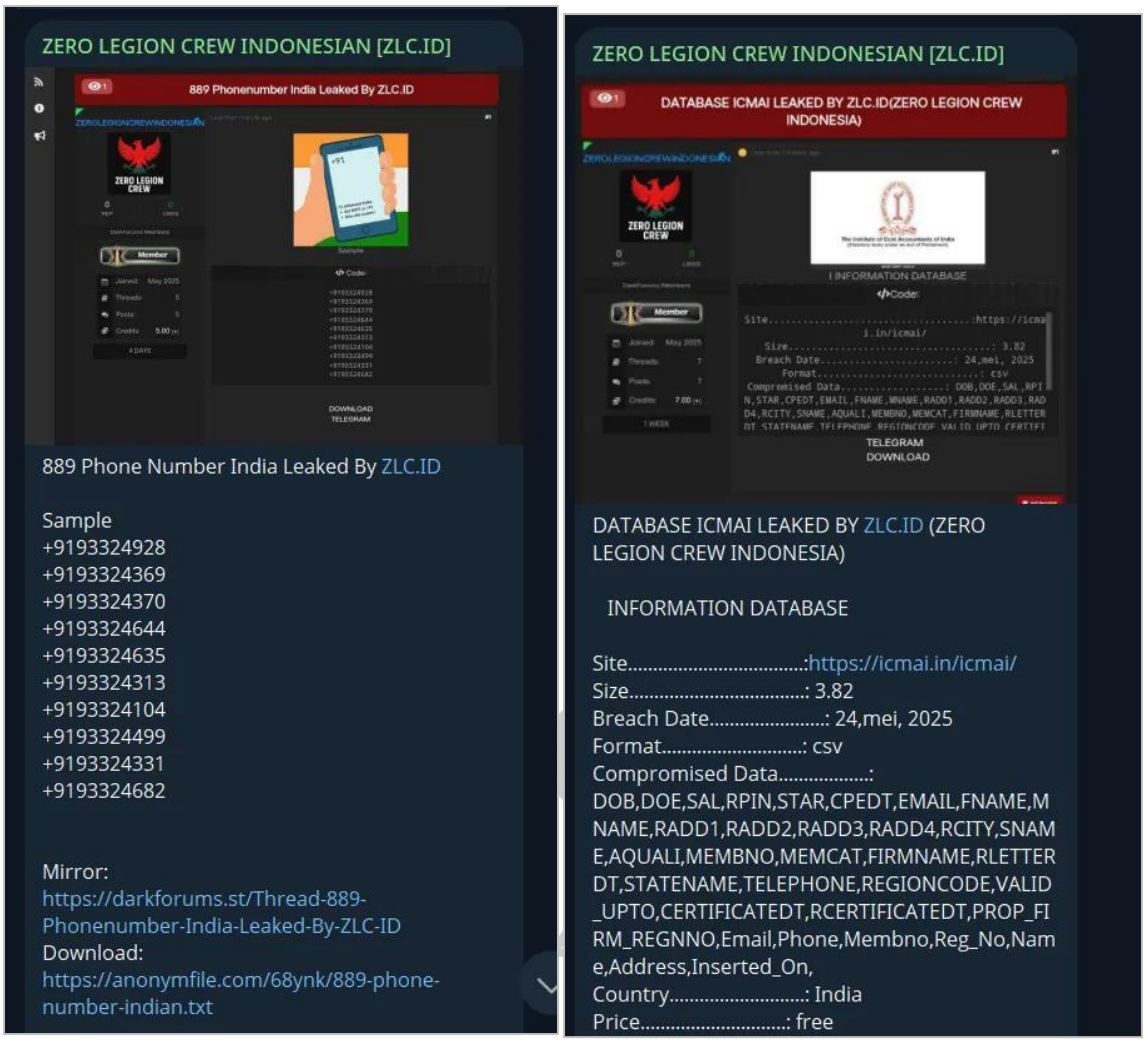
On **May 27**, the pro-Palestinian threat actor group **TengkorakCyberCrew** launched a widespread defacement campaign targeting Indian websites. The defacements featured a **uniform HTML overlay**, focusing on India's foreign policy stance regarding Israel.

Key characteristics of the incident include:

- Prominent use of the headline **"Is India friend of Israel?"**, followed by geopolitical commentary referencing India's **abstention from UN resolutions** and condemnation of Palestinian groups.
- Embedded links directed users to **propaganda resources** and **Tengkorak-affiliated Telegram channels**, signaling an effort to amplify ideological messaging.
- The campaign primarily targeted **educational, religious, and community-facing websites**, likely chosen for their **visibility and weak security posture**.
- Based on the pattern of deployment, the attack appears to have used **mass vulnerability scanning followed by manual exploitation**, rather than automated web-shell injection or scripted bot activity.

This operation exemplifies how threat groups can combine **geo-political narratives** with **low-complexity but high-impact defacements** to maximize both visibility and psychological effect.

## 3.4. ZERO LEGION CREW INDONESIAN (ZLC.ID)



ZERO LEGION CREW INDONESIAN [ZLC.ID]

889 Phonenumber India Leaked By ZLC.ID

889 Phone Number India Leaked By ZLC.ID

Sample
+9193324928
+9193324369
+9193324370
+9193324644
+9193324635
+9193324313
+9193324104
+9193324499
+9193324331
+9193324682

Mirror:
https://darkforums.st/Thread-889-Phonenumber-India-Leaked-By-ZLC-ID
Download:
https://anonymfile.com/68ynk/889-phone-number-indian.txt

ZERO LEGION CREW INDONESIAN [ZLC.ID]

DATABASE ICMAI LEAKED BY ZLC.ID(ZERO LEGION CREW INDONESIA)

I INFORMATION DATABASE

```
Site....................................:https://icmai.in/icmai/
  Size..................................: 3.82
 Breach Date........................: 24,mei, 2025
     Format...............................: csv
 Compromised Data...................: DOB,DOE,SAL,RPIN,STAR,CPEDT,EMAIL,FNAME,MNAME,RADD1,RADD2,RADD3,RADD4,RCITY,SNAME,AQUALI,MEMBNO,MEMCAT,FIRMNAME,RLETTERDT,STATENAME,TELEPHONE,REGIONCODE,VALID_UPTO,CERTIFI
```

TELEGRAM
DOWNLOAD

DATABASE ICMAI LEAKED BY ZLC.ID (ZERO LEGION CREW INDONESIA)

INFORMATION DATABASE

Site.................................:https://icmai.in/icmai/
Size..................................: 3.82
Breach Date......................: 24,mei, 2025
Format...........................: csv
Compromised Data.................: DOB,DOE,SAL,RPIN,STAR,CPEDT,EMAIL,FNAME,MNAME,RADD1,RADD2,RADD3,RADD4,RCITY,SNAME,AQUALI,MEMBNO,MEMCAT,FIRMNAME,RLETTERDT,STATENAME,TELEPHONE,REGIONCODE,VALID_UPTO,CERTIFICATEDT,RCERTIFICATEDT,PROP_FIRM_REGNNO,Email,Phone,Membno,Reg_No,Name,Address,Inserted_On,
Country.........................: India
Price............................: free

*Figure 5. The screenshots of the leaked phone numbers and ICMAI database by ZLC.ID*

### 3.4.1. Attack Behavior

On May 24 and 26, the threat actor group known as Zero Legion Crew Indonesian (ZLC.ID) conducted a series of data breaches targeting Indian organizations and individuals. The group publicly claimed responsibility for two significant leaks:

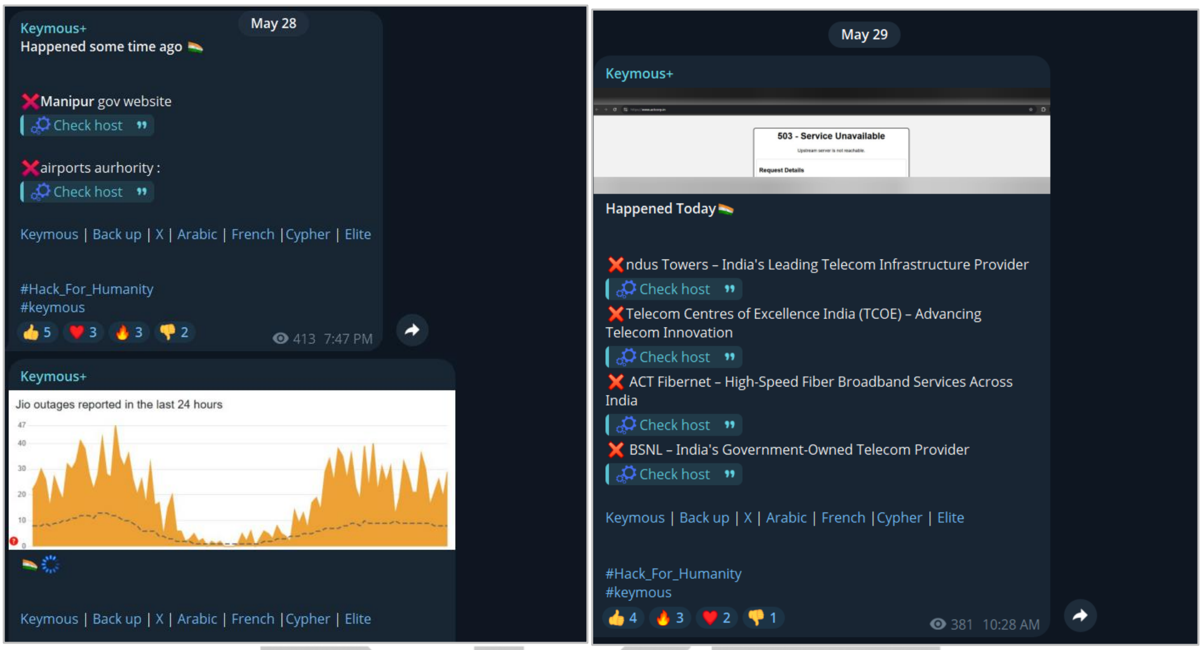
- A dump of 889 Indian phone numbers, posted on multiple forums and mirrored through platforms such as Anonymfile and Darkforums.
- A more extensive data breach involving the Institute of Cost Accountants of India (ICMAI), reportedly exfiltrated on May 24.
- The leaked ICMAI database contained sensitive personally identifiable information (PII) such as full names, contact details, registration numbers, addresses, and academic credentials.

ZLC.ID’s tactics indicate a structured and deliberately publicized campaign. The actor appears to have operated a Telegram-based communication channel, which was previously banned and subsequently re-established under a new alias. Their typical workflow follows a pattern of breach execution, structured formatting of stolen data (commonly in CSV or PDF formats), and redundant publishing via multiple file-sharing platforms.

The group uses provocative taglines such as “SUCCESFUL DATABASE FETCH” and “LEAKD BY ZLC.ID” to amplify visibility and credibility within the cybercriminal ecosystem. While some portions of the leaked data may have been recycled from prior breaches, several entries appear novel, indicating at least partial success in fresh data acquisition.

ZLC.ID’s behavior suggests a combination of opportunistic targeting and symbolic disruption, likely aiming to embarrass Indian institutions while maintaining persistent visibility in underground threat spaces.

## 3.5. Keymous+



May 28

Keymous+
Happened some time ago 🇮🇳

❌Manipur gov website
Check host

❌airports aurhority :
Check host

Keymous | Back up | X | Arabic | French |Cypher | Elite

#Hack_For_Humanity
#keymous

👍 5 ❤️ 3 🔥 3 👎 2 413 7:47 PM

Keymous+

🇮🇳

Keymous | Back up | X | Arabic | French |Cypher | Elite

May 29

Keymous+

503 - Service Unavailable

Request Details

Happened Today🇮🇳

❌ndus Towers – India's Leading Telecom Infrastructure Provider
Check host
❌Telecom Centres of Excellence India (TCOE) – Advancing Telecom Innovation
Check host
❌ ACT Fibernet – High-Speed Fiber Broadband Services Across India
Check host
❌ BSNL – India's Government-Owned Telecom Provider
Check host

Keymous | Back up | X | Arabic | French |Cypher | Elite

#Hack_For_Humanity
#keymous

👍 4 🔥 3 ❤️ 2 👎 1 381 10:28 AM

*Figure 6. The screenshots of the mentioned DDoS Attack by Keymous+*

### 3.5.1. Attack Behavior

Between May 28 and May 29, the threat actor group **Keymous+** reportedly executed a large-scale Distributed Denial of Service (DDoS) attack targeting major telecommunications websites, resulting in widespread 503 service errors. This incident marks the first known occurrence of **Keymous+** conducting such an extensive DDoS operation.

### Tactics and Verification Methods

Indicators suggest that the group focused on disrupting the telecom infrastructure backbone, which aligns with their apparent strategy to undermine communication stability. Verification of the outages was conducted using Check-host URLs, allowing the group to publicly post evidence of the downtime.

### Tools and Motivations

Analysis points to the likely use of public botnets or commercially available booter services to amplify the attack. Messaging associated with the group emphasized “Hack for Humanity,” indicating a possible civil or ideological motivation behind the disruption. This attack demonstrates an evolving capability and intent of Keymous+ to impact critical communication networks, particularly in the context of ideologically motivated cyber operations.

## 4. Trending tools in attacks

| Attacks | Observed Tools | Description |
|---|---|---|
| SQLi Automation | sqlmap | Widely used by ClayOxtymus1337 |
| Defacement | Manual injection | Used by Cyb3r Drag0nz, TengkorakCyberCrew |
| DDoS Indicators | Check-host, 503 pages | Keymous+ infrastructure attacks |
| Data Leaks | CSV/XLS/PDF/ZIP | ZLC.ID, ClayOxtymus1337, EFTS |
| Communication | Telegram + file mirrors | All groups preferred Telegram, plus Mediafire/Anonymfile |

*Table 2. The most tools of the mentioned in attacks*

Several tools and techniques were observed across different threat groups during recent attacks. For SQL injection (SQLi) automation, the tool sqlmap was widely used, particularly by the group ClayOxtymus1337, to exploit vulnerabilities efficiently.

- Defacement attacks were mostly conducted through manual injection methods, employed by groups such as Cyb3r Drag0nz and TengkorakCyberCrew.
- Distributed Denial of Service (DDoS) indicators included the use of services like Check-host and the appearance of 503 error pages, which were linked to infrastructure attacks carried out by Keymous+.
- Data leaks involving various file formats, including CSV, XLS, PDF, and ZIP, were attributed to groups such as ZLC.ID, ClayOxtymus1337, and EFTS.

Regarding communication channels, all groups showed a preference for using Telegram combined with file mirror services like Mediafire and Anonymfile to coordinate activities and distribute data.

**Additionally,** the hacktivist groups primarily used several online platforms to facilitate their activities.

- Telegram served as the main channel for coordination, dissemination of propaganda, and publication of data.
- Dark forums were utilized to propagate leaked data further, often through file-sharing services like Mediafire and Anonymfile.
- X (formerly Twitter) was employed to amplify attack claims and reach a wider public audience.

## 5. Conclusion

The observed increase in automated SQL injection attacks, primarily using tools like sqlmap, alongside the geopolitical motivations behind many incidents—such as references to India's stance on Israel—reflects a growing trend of ideologically driven cyber operations. Repeated breaches of certain Indian websites by multiple threat groups further highlight persistent targeting and underlying infrastructure weaknesses, especially within the telecommunications and educational sectors.

This surge in symbolic, retaliatory, and propaganda-driven hacktivist campaigns demonstrates the normalization of cyberwarfare tactics among ideologically motivated actors. Given their use of platforms like Telegram for coordination and automation tools for exploitation, it is crucial to implement real-time monitoring and strengthen web application defenses. Considering the ongoing regional tensions, attacks associated with Operation India are expected to continue.