Published on July 10, 2025.

The weekly trending report of
Operation India related Hacktivist groups

*Reported by **Team D4rkn3ttz***

Effected date: July 1 – July 7, 2025.

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

Table of Contents

1. Executive Summary

We confirmed the coordinated hacktivist activities targeting Indian institutions spiked significantly. **12 hacktivist groups** operated as part of **Operation India**, carrying out 47 total incidents including defacements, data leaks, DDoS attacks, and ransomware operations.

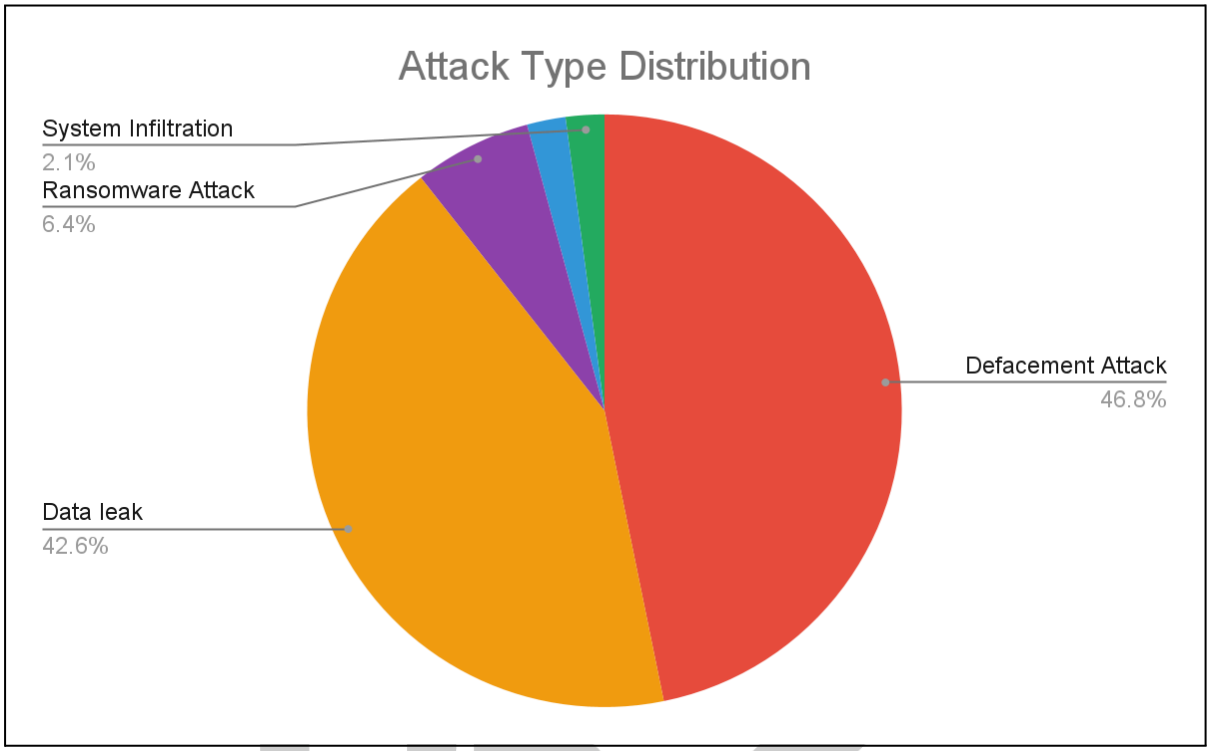
The attacks were primarily politically and religiously motivated, focusing on anti-India sentiment, pro-Palestine messaging, and Kashmir territorial disputes. The groups primarily used **Telegram** for communication and dark forums for sharing stolen data.

2. Key Threat Actor Activity

Group	Tools Used	Attack Types	Victim Industries	Observed Date
TEAM BD CYBER NINJA	Webshell DefacerID(Host archiving Website) HaxorID(Text-file hosting Website)	Defacement Data Leaks	Education Healthcare Hospitality	*2025.07.05.* *2025.07.07.*
GARUDA ERROR SYSTEM	Mediafire(File hosting Website) DefacerMirror(Host archiving website)	Defacement Data Leaks	Education Businesses	*2025.07.02.*
Liwaa Mohammad	Zone-H(Host archiving Website)	Ransomware Defacement	Oil/gas Information Technology	*2025.07.01.* *2025.07.03.*
LulzSec Resistance	Check-host(Host archiving Website)	DDoS Defacement Data Leaks	Engineering Education	*2025.07.02.* *2025.07.03.*
LulzSec Black	-	System Infiltration	Medical	*2025.07.02.* *2025.07.06.*

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, Defacement attacks constitute the largest share of observed attack types, accounting for 46.8%, while Data Leak incidents represent 42.6%. This indicates that threat actors are primarily focused on website vandalism and stealing sensitive information.

High Incidence of Website Defacement

Defacement attacks represent the most visible form of hacktivist operations (46.8%), indicating significant interest among threat actors in disrupting online presence and spreading ideological messages. Such attacks are often carried out by politically motivated groups seeking public attention and symbolic victory over their targets.

Systematic Data Exploitation

Data Leak incidents comprise 42.6% of the total attacks, suggesting adversaries are heavily targeting sensitive information repositories. The focus on educational databases, medical records, and corporate data shows that attackers are choosing valuable targets for financial gain and reputational

damage.

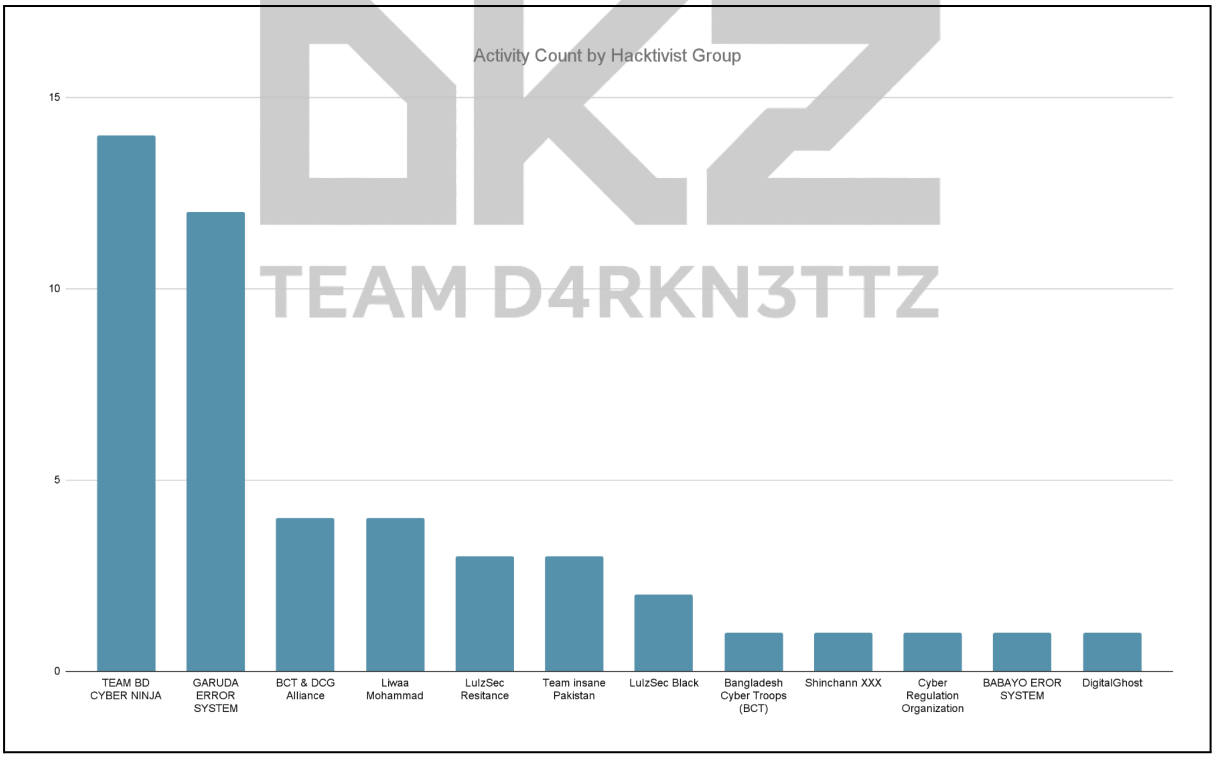
Ransomware and Service Disruption

Ransomware attacks represent 6.4% (3 incidents) but demonstrate high technical sophistication, involving data theft followed by complete system encryption. DDoS attacks account for 2.1% (1 incident), reflecting attempts to disrupt service availability as part of broader psychological warfare campaigns.

Advanced Persistent Infrastructure Penetration

System Infiltration represents the smallest portion at 2.1% (1 incident), but its targeted and technically advanced nature suggests sophisticated APT-level capabilities. The successful direct system access demonstrates abilities for infrastructure compromise beyond web application vulnerabilities.

2.2. The count of Hacktivist group's activities

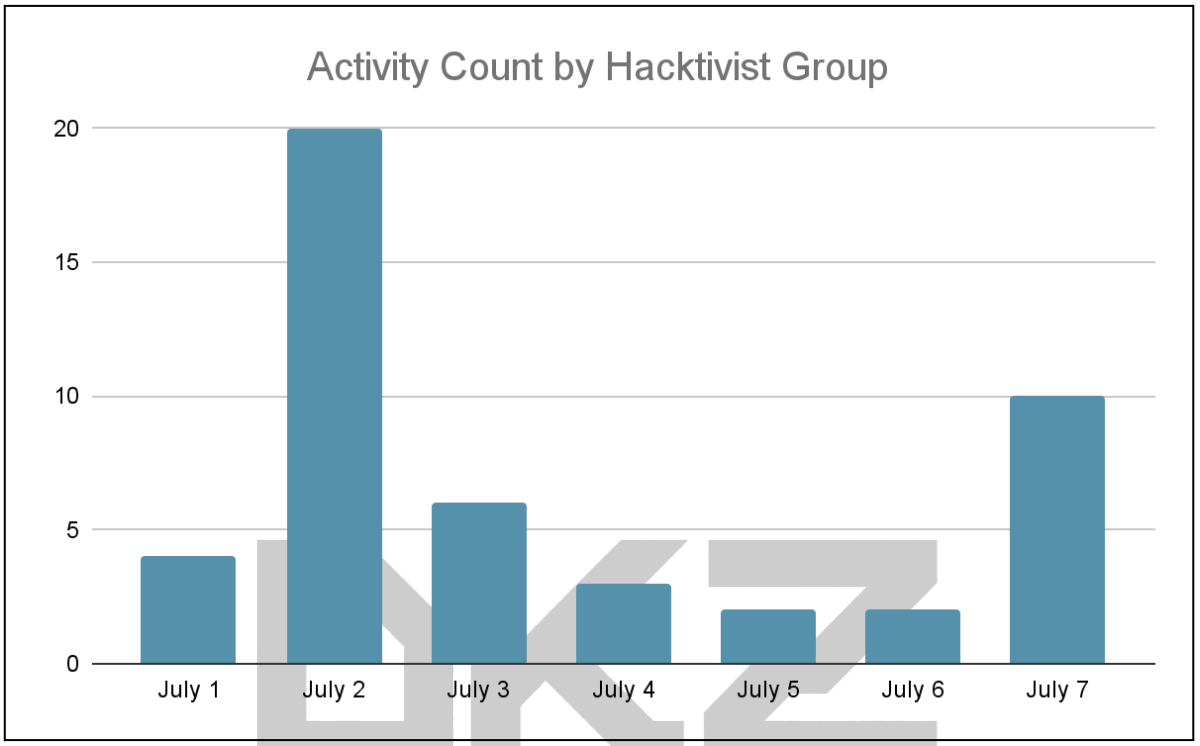


Graph 2. The count of the activities by groups

TEAM BD CYBER NINJA and GARUDA ERROR SYSTEM were the most active, followed closely by

Liwaa Mohammad, BCT & DCG alliance, LulzSec Resitance, and Team Insane Pakistan.

2.3. The count of Hacktivist group's effected issues



Graph 3. The count of the activities by date

From July 1 to July 7, there was sustained attack activity across multiple sectors. July 2 showed the highest concentration of attacks, with multiple groups conducting simultaneous operations.

3. The analysis of 5 Hacktivist groups

3.1. TEAM BD CYBER NINJA

3.1.1. Summary of the activities

TEAM BD CYBER NINJA conducted the most extensive campaign during the observation period, with 14 attacks including sophisticated multi-stage operations. The group demonstrated particular focus on Indian educational institutions and government-affiliated organizations, beginning with website defacement and escalating to comprehensive data exfiltration.

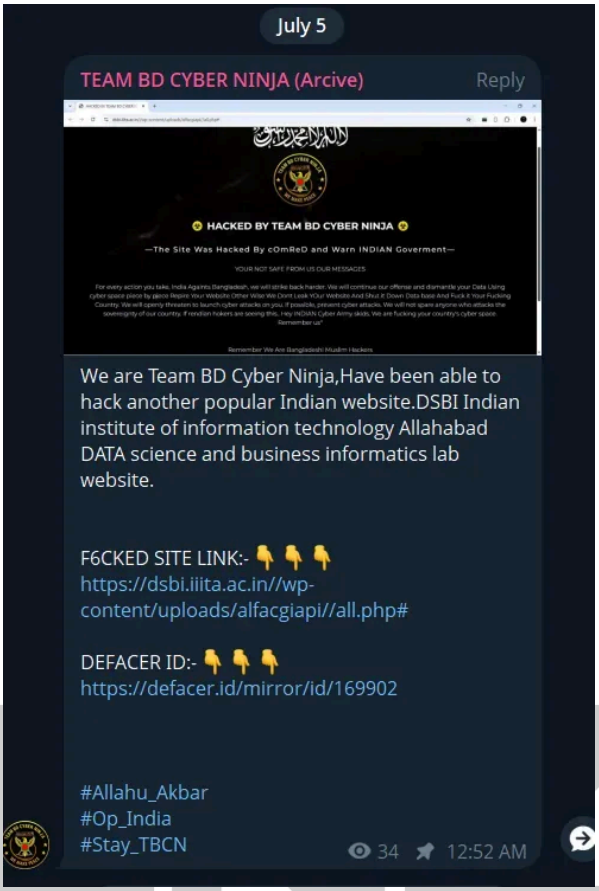


Figure 1. The screenshot of the Wordpress file upload vulnerability exploitation by TEAM BD CYBER NINJA

3.1.2. Analysis of the leaked files

DSBI (Indian Institute of Information Technology Allahabad) Breach

The group successfully exploited WordPress file upload vulnerabilities, uploading PHP files to the uploads directory. The compromised URL structure reveals bypass of file extension filtering and successful execution of malicious code, indicating weak input validation and insufficient file type verification on the target system.

https://dsbi.iiita.ac.in/wp-content/uploads/alfacigapi/all.php#

The compromised URL structure shows successful exploitation of WordPress file upload mechanisms, where the attacker bypassed file extension filtering to upload a PHP webshell (all.php) into the uploads directory, demonstrating weak input validation and insufficient file type verification on

the target system.

Multi-target Defacement Campaign

Figure 2. Website defacement showing TEAM BD CYBER NINJA's ideological messaging and attack signature

The threat actor conducted coordinated attacks against 14 websites across multiple sectors:

- Educational institutions and government-affiliated organizations in India
- Private sector companies including medical clinics and hospitality services
- International targets, notably a Korean solar energy company in Kenya

Cross-sector targeting demonstrates opportunistic selection based on vulnerability rather than strategic significance.

Operation Black Storm

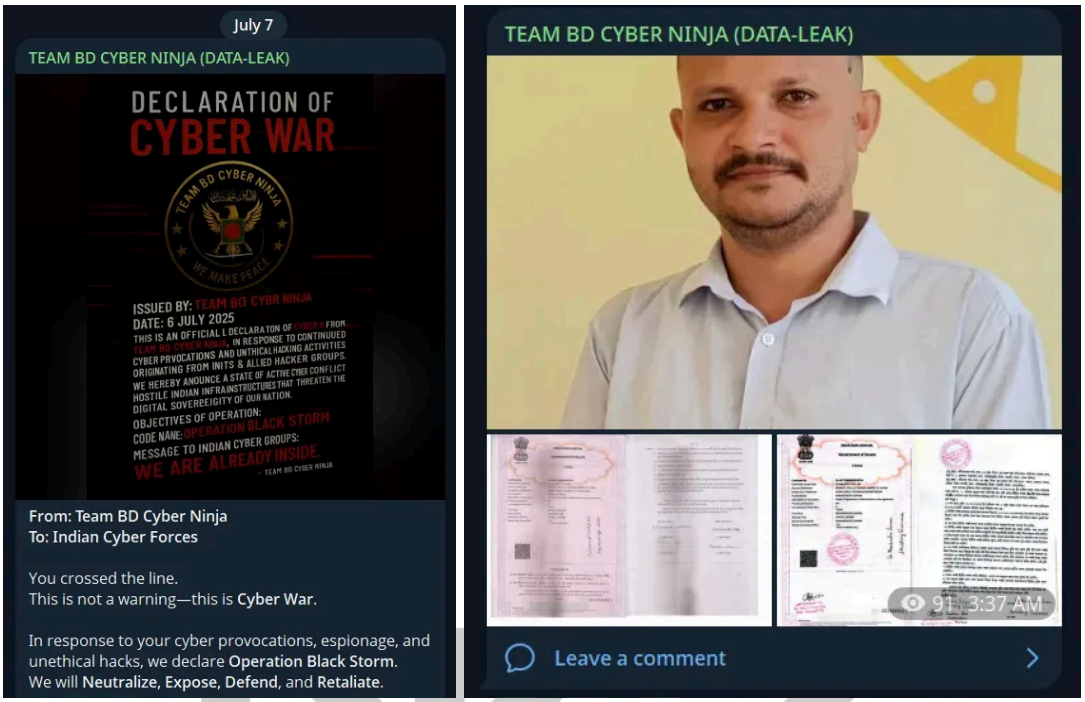


Figure 3. The screenshots of Operation Black Storm declaration and leaked government documents by TEAM BD CYBER NINJA

The group initiated a new phase by officially declaring cyber warfare against Indian Cyber Forces, citing retaliation for alleged unethical hacking activities. The operation included:

- Comprehensive data exfiltration from educational institutions
- Publication of sensitive student records and administrative documents
- E-stamp and notarized legal document theft
- Systematic targeting of Indian digital infrastructure as symbolic retaliation

Their repeated targeting of educational databases containing student personal information indicates preference for high-visibility targets with significant civilian impact potential.

Reported by Team D4rkn3ttz

3.2. GARUDA ERROR SYSTEM

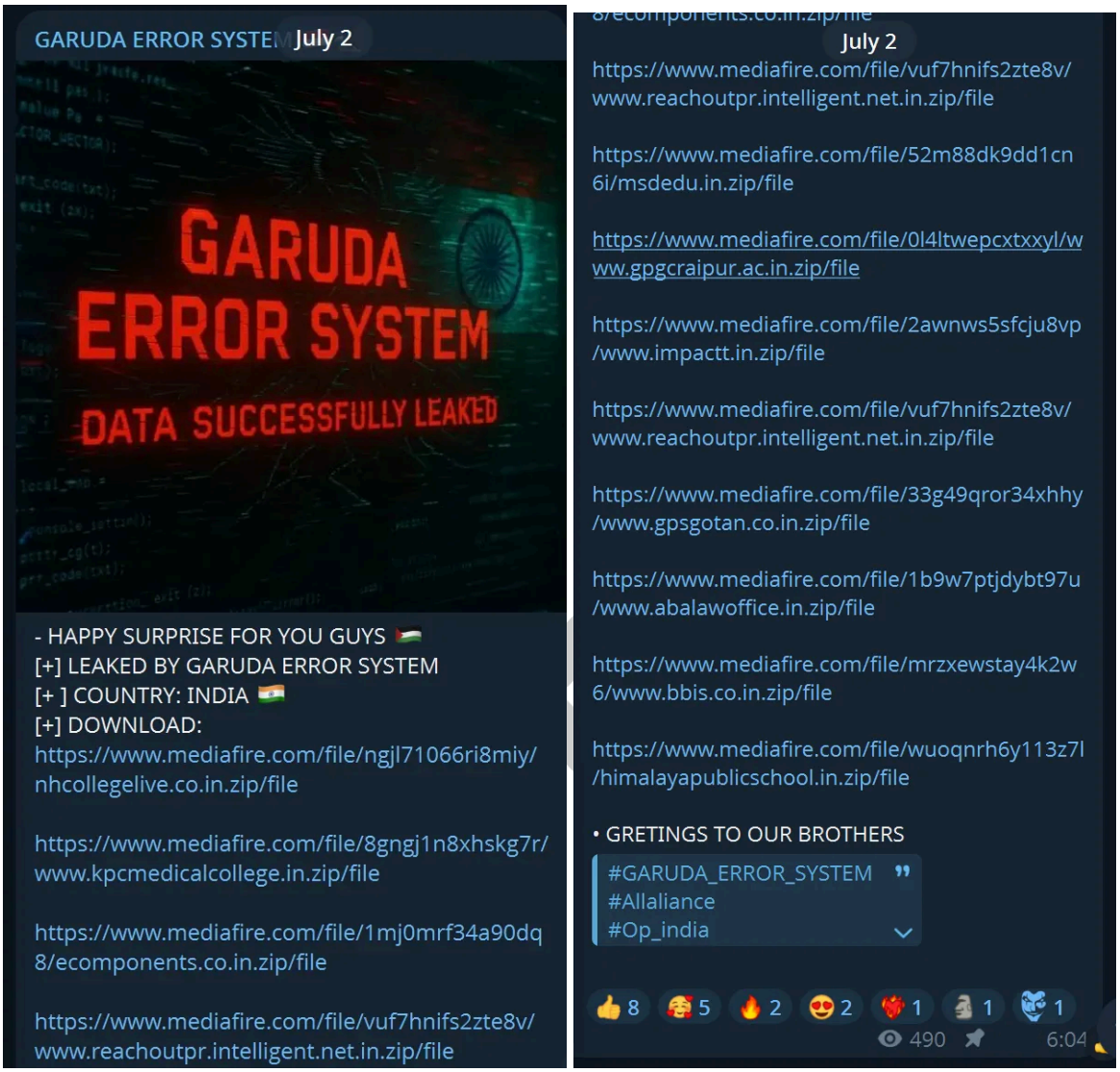


Figure 4. The screenshots of the mass data leak distribution via Mediafire by GARUDA ERROR SYSTEM

3.2.1. Summary of the activities

GARUDA ERROR SYSTEM conducted extensive campaigns during the observation period, with 12 attacks primarily targeting educational institutions across India. The group demonstrated sophisticated data distribution mechanisms using Mediafire links and systematic approach to educational database exploitation.

3.2.2. Analysis of the leaked files

Himalaya Public School Comprehensive Breach

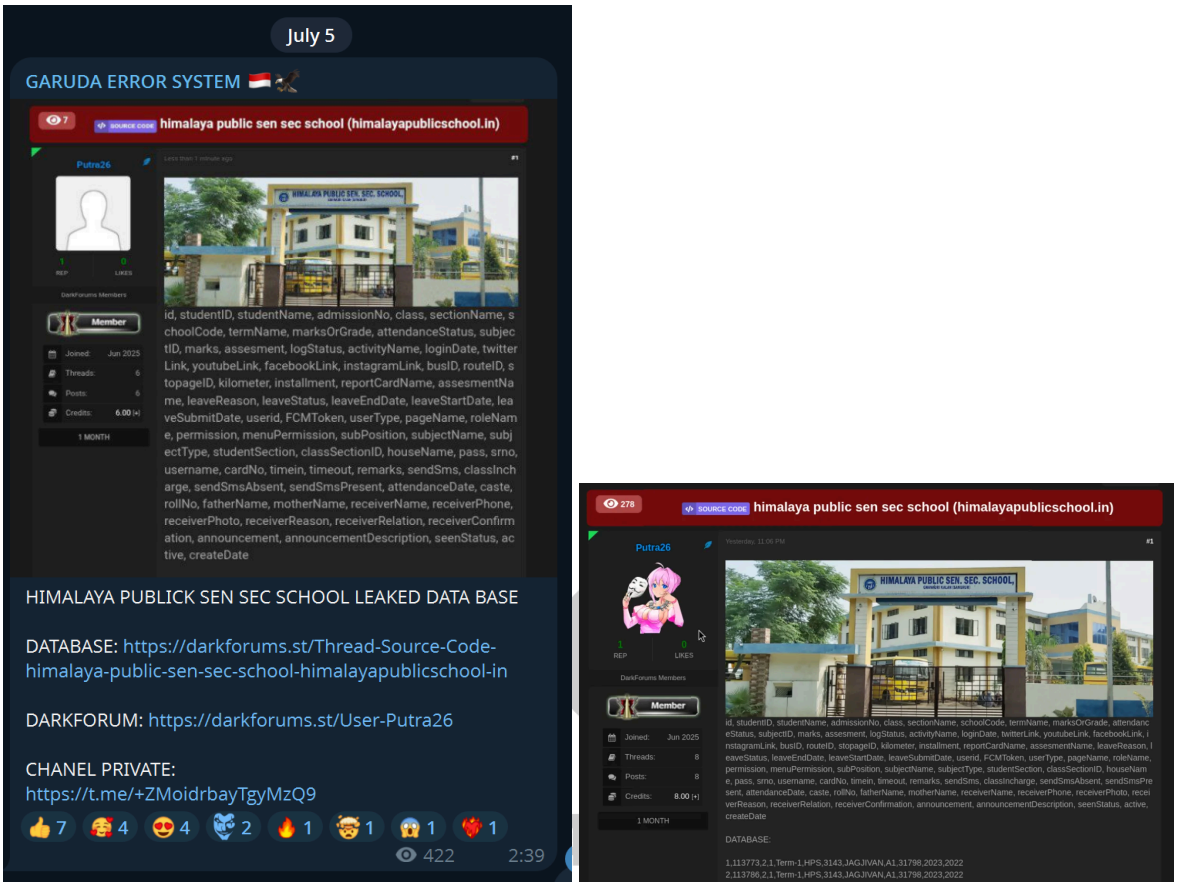


Figure 5. Th The screenshots of Himalaya Public School database breach by GARUDA ERROR SYSTEM

The group successfully penetrated the school's database infrastructure, exfiltrating a comprehensive dataset containing **2,720 individual records**. The breach exposed sensitive educational data including student enrollment information, academic performance records, and family contact details. Additionally, the attackers accessed internal communication systems, obtaining SMS logs between school administration and parents.

Systematic Educational Sector Targeting

GARUDA ERROR SYSTEM demonstrated strategic selection of educational targets, focusing on institutions with weak security postures and high-value databases. The campaign encompassed diverse educational entities ranging from private medical colleges to government universities,

indicating opportunistic targeting based on vulnerability assessment rather than specific institutional significance.

The group's systematic approach to data categorization and distribution through established file-sharing platforms suggests operational maturity and intent for maximum data exposure. Their consistent focus on educational databases containing minor student information represents a concerning trend toward targeting civilian infrastructure for ideological impact.

3.3. Liwaa Mohammad

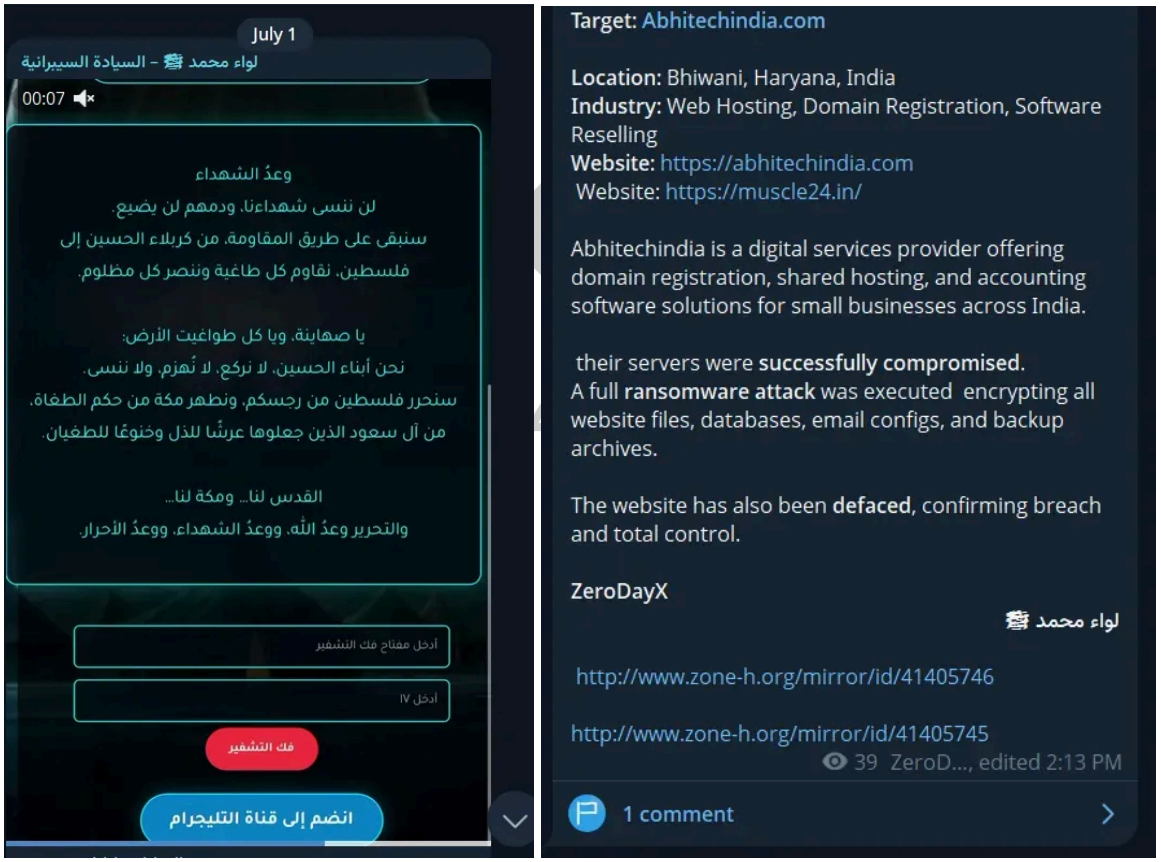


Figure 6. The screenshots of the ransomware attack and defacement by Liwaa Mohammad

3.3.1. Summary of the activities

Liwaa Mohammad(لواء محمد – السيادة السيبرانية) conducted the most sophisticated ransomware operations during the observation period, demonstrating advanced persistent threat capabilities with focus on critical infrastructure and IT service providers.

3.3.2. Analysis of the leaked files

Kiri Oilfield Services Pvt. Ltd. Ransomware Attack

The threat actor demonstrated sophisticated capabilities by targeting critical energy sector infrastructure with a comprehensive ransomware deployment. The attack involved gaining system administrator privileges on production servers, followed by systematic encryption of both operational systems and backup infrastructure. The threat actor executed encryption commands at root level, indicating advanced persistent access and deep system compromise capabilities.

CodeCrew Infotech Pvt. Ltd. Breach

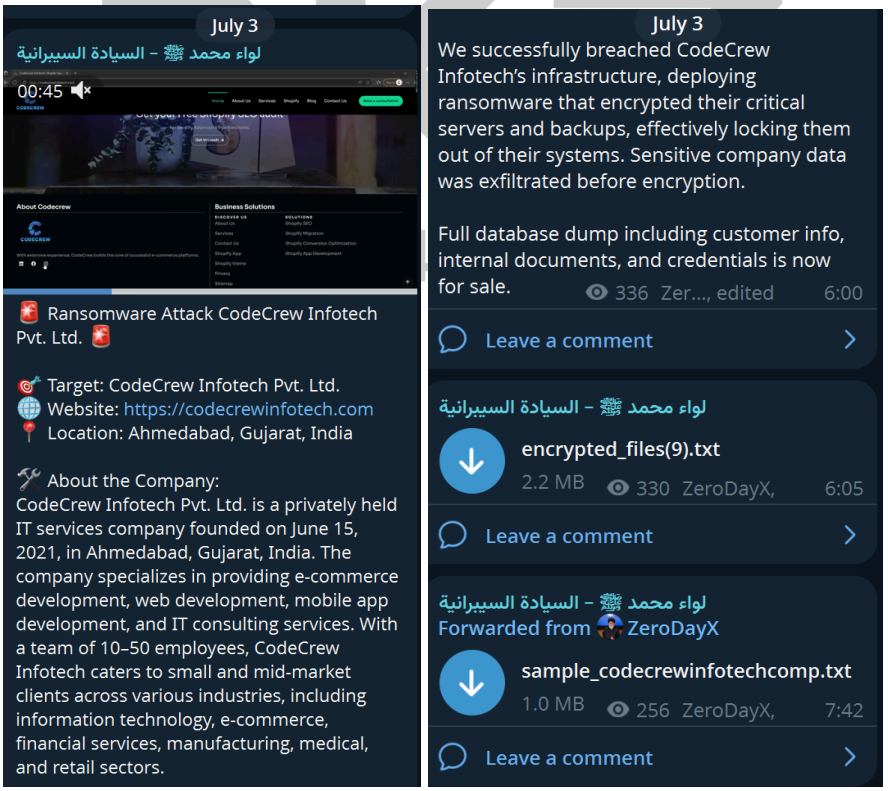


Figure 7. The screenshots of CodeCrew Infotech ransomware attack and data sale announcement by Liwaa Mohammad

Reported by Team D4rkn3ttz

The group conducted a methodical breach of the private IT service provider, deploying ransomware across operational servers while simultaneously exfiltrating sensitive corporate data. Technical evidence indicates the attackers achieved complete database access, extracting a full MySQL dump containing customer management systems, user credentials, and business-critical operational data. The comprehensive file system compromise, spanning WordPress core files and administrative interfaces, demonstrates advanced persistent access capabilities beyond typical ransomware operations. Prior to encryption, the attackers systematically harvested customer databases, internal documentation, and authentication credentials. The stolen data was subsequently monetized through underground forum sales, demonstrating the group's integration of ransomware tactics with traditional cybercriminal revenue models.

Abhitech India Combined Attack

This attack exemplified the group's dual motivation structure, combining financial extortion with ideological messaging. The operation involved comprehensive server encryption alongside website defacement featuring anti-Zionist propaganda and Palestinian liberation themes. The simultaneous deployment of ransomware and ideological content indicates the group's evolution beyond purely financial motivations toward politically-driven cyber operations with revenue generation components.

3.4. LulzSec Resitance

Figure 8. The screenshots of SB Engineers administrative dashboard breach by LulzSec Resitance

3.4.1. Summary of the activities

LulzSec Resitance demonstrated a pattern of escalating attacks, beginning with website defacement and progressing to data exfiltration and DDoS operations. The group targeted **Sai Computer School** on July 2, followed by a more sophisticated attack against **SB Engineers** on July 3.

3.4.2. Analysis of the leaked files

SB Engineers (sbindia.in) Breach

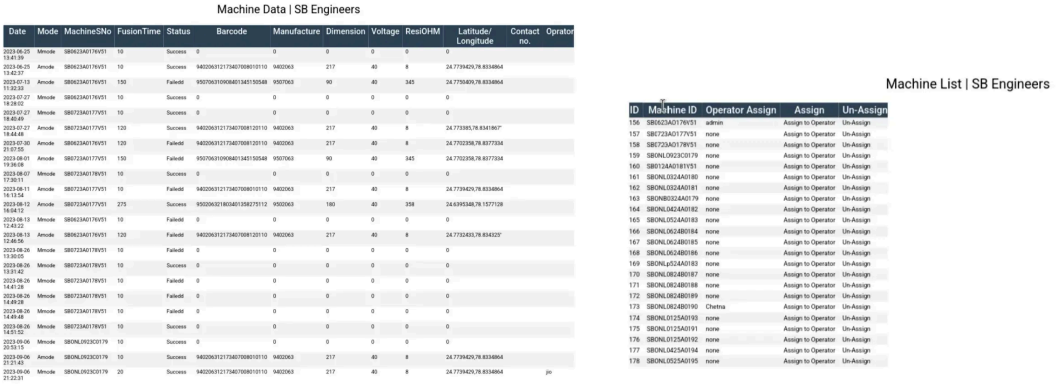


Figure 9. The screenshots of exfiltrated Machine Data and Machine List databases from SB Engineers

The group successfully penetrated SB Engineers' administrative dashboard, gaining access to comprehensive industrial equipment databases. The exfiltrated data revealed detailed operational intelligence including:

- Machine Data: Complete equipment inventory with operational status, manufacturer specifications, and maintenance records
- Machine List: Operator assignments, equipment allocation, and personnel contact information
- Operational Intelligence: Real-time equipment status, assignment details, and operational workflow data

The leaked databases expose critical infrastructure information that could facilitate targeted attacks against specific industrial equipment or personnel. The systematic nature of the data extraction suggests advanced persistent access to internal management systems.

3.5. LulzSec Black

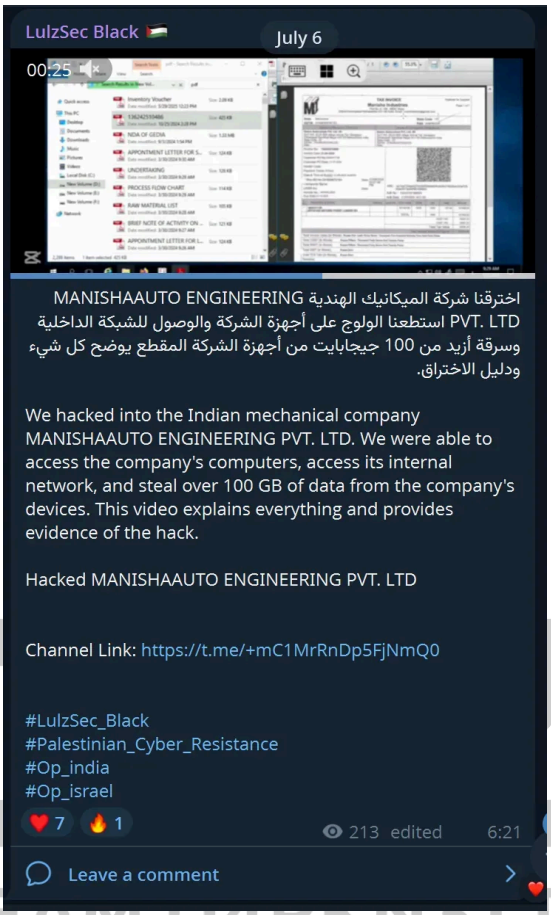


Figure 10. The screenshots of the mentioned DDoS Attack by Keymous+

3.5.1. Summary of the activities

LulzSec Black conducted highly sophisticated operations targeting both medical technology and automotive manufacturing sectors, demonstrating advanced persistent access capabilities and large-scale data harvesting techniques across diverse industries.

3.5.2. Analysis of the leaked files

MAP FILTRES INDIA Comprehensive Breach

- Successfully penetrated internal network infrastructure of medical technology solutions company
- Exfiltrated 1.4TB of sensitive corporate data

- Leaked hospital equipment and system design blueprints
- HVAC system quotations and pricing proposals
- Customer company and hospital-related information
- IVF center design documents and technical specifications

Manisha Auto Engineering System Infiltration

- Successfully infiltrated internal network infrastructure of Indian automotive parts manufacturing company
- Gained direct access to company computers and internal network systems
- Exfiltrated over 100GB of sensitive corporate data
- Accessed appointment documents, invoices, and tax calculation sheets
- Obtained internal business correspondence and operational documents
- Demonstrated GUI-based system access indicating advanced remote access methods

The dual-sector targeting demonstrates LulzSec Black's versatility in attacking both web-based infrastructure and direct system infiltration, with capabilities spanning medical technology intellectual property theft and manufacturing sector operational intelligence gathering.

4. Additional Notable Activities

System Infiltration Operations

- Liwaa Mohammad conducted direct system infiltration against Manisha Auto Engineering, an Indian automotive parts manufacturing company
- Successfully gained direct access to internal systems, evidenced by GUI environment manipulation and overlay button controls suggesting remote desktop access
- Exfiltrated over **100GB** of internal corporate data including appointment documents, invoices, and tax calculation sheets

Cross-Border Alliance Operations

- **Bangladesh Cyber Troops (BCT) & Dark Cyber Gang (DCG)** demonstrated sophisticated international coordination
- Targeted systems in Eswatini (National Cooperative Federation) alongside Indian institutions
- Conducted joint operations with shared messaging and coordinated timing

Reported by Team D4rkn3ttz

Published on July 10, 2025.

Reported by Team D4rkn3ttz

5. Trending tools in attacks

Attacks	Observed Tools	Description
File Upload Exploits	Webshell	TEAM BD CYBER NINJA PHP webshell deployment
Defacement	DefacerMirror(Host archiving Website) Zone-H(Host archiving website) DefacerID(Host archiving Website) HexorID(Host archiving Website)	Used by GARUDA ERROR SYSTEM, TEAM BD CYBER NINJA, TEAM insane Pakistan, BCT & DCG Aliance
DDoS Indicators	Check-host(Host archiving Website)	LulzSec Resitance infrastructure attacks
Data Leaks	Mediafire(File hosting website)	GARUDA ERROR SYSTEM, LulzSec Black, Shinchan XXX
Communication	Telegram	All groups preferred Telegram

Table 2. Most Commonly Used Tools in Documented Attacks

Several tools and techniques were consistently observed across different threat groups during the first week of July 2025. WordPress file upload vulnerabilities were exploited by TEAM BD CYBER NINJA for webshell deployment, demonstrating the prevalence of web application security weaknesses in target organizations.

Communication and Distribution Infrastructure:

- Telegram was utilized as the primary platform for operational coordination for all observed groups
- Mediafire and file mirror services were the preferred methods for data leak distribution
- Check-host services were utilized for DDoS attack verification and proof-of-concept demonstrations

Data Formats and Storage:

- CSV, XLS, PDF, and ZIP files were the standard formats for leaked data distribution
- Groups demonstrated consistent preference for structured data formats that facilitate easy sharing and analysis

The hacktivist groups demonstrated preference for readily available tools and platforms rather than sophisticated custom malware, indicating a focus on accessibility and operational security through commonly used services.

6. Conclusion

The first week of July 2025 demonstrated a significant escalation in coordinated hacktivist activities targeting Indian institutions. The observed campaigns show clear patterns of ideological motivation, with many attacks explicitly referencing geopolitical tensions related to Kashmir, Palestine, and regional conflicts.

The repeated targeting of educational institutions, particularly those containing sensitive student and family information, represents a concerning trend toward attacks on civilian infrastructure. The technical sophistication varied significantly between groups, with some demonstrating advanced persistent access capabilities while others relied on basic web application vulnerabilities.

Given the sustained nature of these campaigns and their explicit ideological motivations, continued monitoring and enhanced security measures for educational and government institutions are strongly recommended. The use of mainstream communication platforms like Telegram for coordination suggests these groups prioritize operational security and broad reach over technical sophistication.