

17-05-2025

CERTMH_CTI_2025_23



DIGITAL CROSSFIRE: INDIA-PAKISTAN CYBER TENSION



**CYBER ATTACK
ON INDIA**



EXECUTIVE SUMMARY



India's digital borders are under siege. In the wake of the Pahalgam terror attack, the country is facing a wave of cyber aggression unlike anything seen before.

In the aftermath of the Pahalgam terror attack, India has witnessed an unprecedented surge in cyber intrusions orchestrated by hostile hacker groups from Pakistan, Bangladesh, Indonesia, and parts of the Middle East. Maharashtra Cyber over has revealed surge in cyberattacks were launched targeting Indian websites and digital infrastructure in a coordinated and politically motivated campaign.

This offensive is being driven by more than 40 hacktivist groups—most notably Keymous+ and AnonSec—which are actively targeting Indian government entities and critical infrastructure. Their tactics include website defacement, distributed denial-of-service (DDoS) attacks, and data exfiltration, with several successful breaches already reported.

Future threats outlined by these groups involve high-value targets such as the Indian Army, Air Force, Navy, and the Ministry of Defence. The ongoing campaign is a strategic attempt to disrupt national operations, weaken public morale, and erode trust in digital systems



HACKTIVIST ORIGIN, MOTIVE, AND ESCALATION



Pro-Pakistan hacktivist communities have a long-standing history of politically motivated campaigns targeting Indian digital assets. These groups often leverage geopolitical events to justify their actions and amplify their ideological narratives. Following India's recent military operations, these actors have escalated their efforts, claiming responsibility for a series of retaliatory cyberattacks.

Their current campaigns have targeted government portals, municipal systems, aviation infrastructure, and other critical sectors aiming to disrupt essential services and erode public trust. In recent communications, several prominent groups have announced their intent to target high-value defense organizations, including the Indian Army, Air Force, Navy, and the Ministry of Defence.

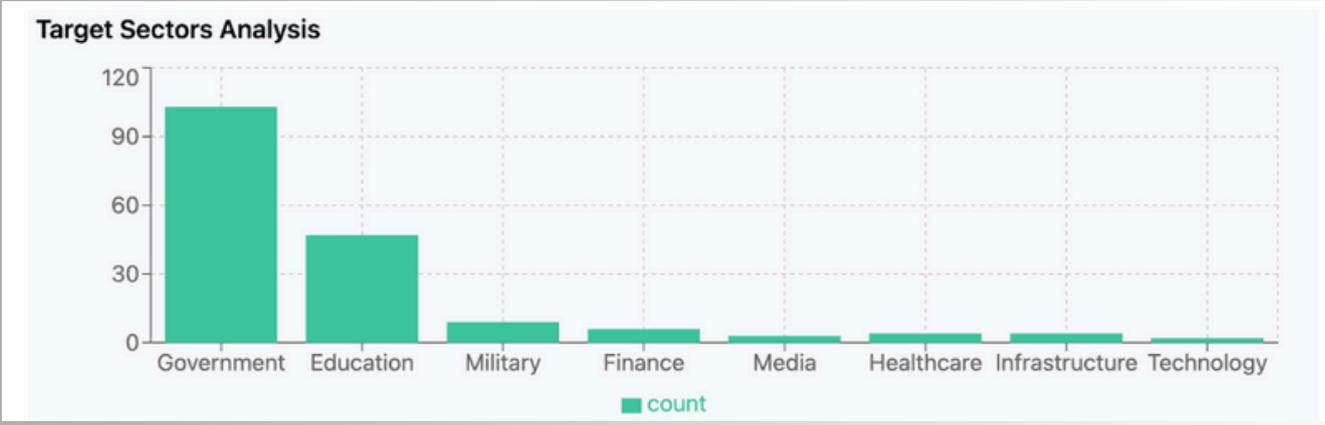
India recently faced a coordinated cyber onslaught that unfolded in five strategic phases, indicating a deliberate and well-orchestrated campaign. The operation began with target identification and surveillance, where attackers mapped vulnerable digital assets across critical sectors. This led to the infiltration phase, marked by spear-phishing and exploitation of weak points in public systems.

Once inside, attackers moved laterally within networks, escalating privileges and establishing persistence. In the disruption stage, they launched DDoS attacks and website defacements, aiming to destabilize operations and push ideological messaging. The final phase focused on information warfare—publicizing stolen data and propaganda across social platforms and underground channels to intensify psychological pressure and shape public perception. This phased execution underscores the evolving nature of geopolitical cyber warfare against Indian interests.

These claims form part of a broader psychological and information warfare strategy designed to instill fear, provoke reaction, and influence public perception. The use of website defacements, data exfiltration, and distributed denial-of-service (DDoS) attacks suggests a coordinated attempt to not only breach but also broadcast their ideological objectives. Their messaging is often amplified through Telegram channels, dark web forums, and social media, further increasing their reach and perceived impact.



SECTOR IMPACTED



GOVERNMENT



EDUCATION



DEFENCE

Advanced Persistent Threat (APT) groups and Pro-Pakistan hacktivist collectives have claimed responsibility for a series of cyberattacks targeting Indian government entities. According to their statements across various forums, the campaign focused on compromising central and state-level administrative systems, disrupting digital public services, and affecting platforms related to governance, law enforcement, and the judiciary.

Additionally, claims include attacks on the education sector, critical infrastructure, and financial systems highlighting a broad, politically motivated operation aimed at weakening national capabilities and public trust.



THREAT ACTORS AND THEIR CLAIMS

ISLAMIC HACKER ARMY

The Islamic Hacker Army has claimed responsibility for cyberattacks on key Indian digital assets, including mod.gov.in, mib.gov.in, and the School of Haryana website.



Their campaigns often feature website defacements and ideological messaging amplified via Telegram and dark web forums. Their operations were observed alongside other pro-Palestinian and anti-India hacktivist groups during the post-Pahalgam cyber offensive.



#Ransomware

#OP_UAE #OP_india

We will launch a massive cyberattack, hitting hundreds of Emirati and Indian companies and institutions with our new ransomware.

The UAE and India are the two countries that support Israel most.

This will be the first of its kind... coming soon ... ✨

سنشن هجوماً إلكترونيًا ضخمًا، نستهدف من خلاله مئات الشركات والمؤسسات الإماراتية والهندية ببرنامج الفدية الجديد.

الإمارات والهند هما الدولتان الأكثر دعمًا لإسرائيل.

هذا سيكون الأول من نوعه... قريبًا ... ✨

#Islamic_Hacker_Army

<https://mod.gov.in> ✖

#Islamic_Hacker_Army

4 👍 1 ❤️ 1

725 👁 ALKnsOle edited 02:18 AM

Leave a comment >

#OP_india ...

<https://mib.gov.in> ✨

<https://check-host.net/check-report/25c9aca5kf4> ✨

#Islamic_Hacker_Army

1 👍

441 👁 ALKnsOle 02:48 AM

3 comments >

#OP_india ...

<https://schooleducationharyana.gov.in> ✖

#Islamic_Hacker_Army

385 👁 ALKnsOle 05:46 PM

Leave a comment >

#OP_india

<https://uppwd.gov.in> 📍

<https://check-host.net/check-report/25d09334k605> ✨



DIENET

DieNet is a politically motivated hacktivist group that surfaced in March 2025, conducting widespread DDoS attacks against critical infrastructure across multiple nations. Recently, the group has extended its focus toward South Asian targets, including India, aligning its attacks with pro-Palestinian and anti-Western narratives.

The group has claimed responsibility for disabling ten significant Iraqi websites, framing the action as support for their affiliates in the “Shiite Harvest.” Their operations suggest motivations rooted in sectarian dynamics, with a coordinated effort indicated by the use of hashtags like #DieNet and #Shiite_Harvest.

DieNet's operations have been promoted by other Pro-Palestinian hacktivist groups, including Mr Hamza, LazaGrad Hack, and Sylhet Gang-SG, indicating possible alliances.



NOTABLE ATTACKS

Sanitation.zip
Source : h[redacted].gov.in
168 Ko/s - 2,6 Mo sur 422 Go, 30 jours restants

NIC एनआईसी
National Informatics Centre

We have hacked into the Some National Informatics Centre, Government of India Servers. We have extracted over 247 GB of data. This will be published on this channel as time goes on. As India goes beyond its limits, we will publish more sensitive information.

0:02 Proof of proposed marriage Document

DIENET

We hacked the official website of the Rupashree Perkalpa Scheme, a marriage planning initiative in India. (Belongs to the Indian Government)

We were able to access a massive database of information (bank account information, personal details, ID photos, and more).

Our capabilities include not only powerful DDoS, and we will show you this over time... This is a warning to India and all hostile nations.

We will publish part of the data as a warning to India... We are Dienet.

http://nta.ac.in

Ce site est inaccessible

La connexion a été réinitialisée.

Voici quelques conseils :

- Vérifier la connexion
- Vérifier le proxy et le pare-feu
- Exécutez les diagnostics réseau de Windows

ERR_CONNECTION_RESET

DIENET

Actualiser

The Indian National Testing Agency official Webste is Down by DieNet

503 Backend fetch failed

radioindia.in

Error 503 Backend fetch failed

Backend fetch failed

Guru Medi on.

XID: 6632279

DIENET

Flush cache server

Currently we have taken down radio service in India and caused a total outage of online audio streaming from radioindia servers

Proofs: " "

<https://check-host.net/check-report/25ec3f01k9e6> " "

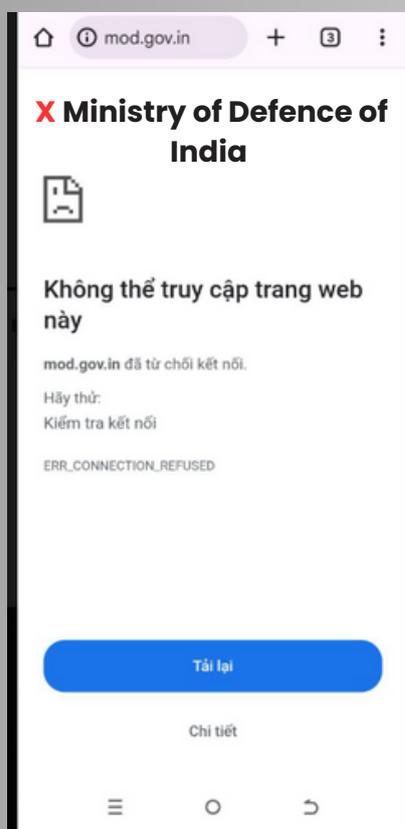


VULTURE

- Indian government websites and educational institutions were the main focus of this group's claimed activities.
- Claims included attacks on the Minister of Defence portal, the official website of the President of India, and the Prime Minister's Office (PMO) website. Vulture was frequently mentioned in joint operation claims, indicating collaboration with other hacktivist entities.



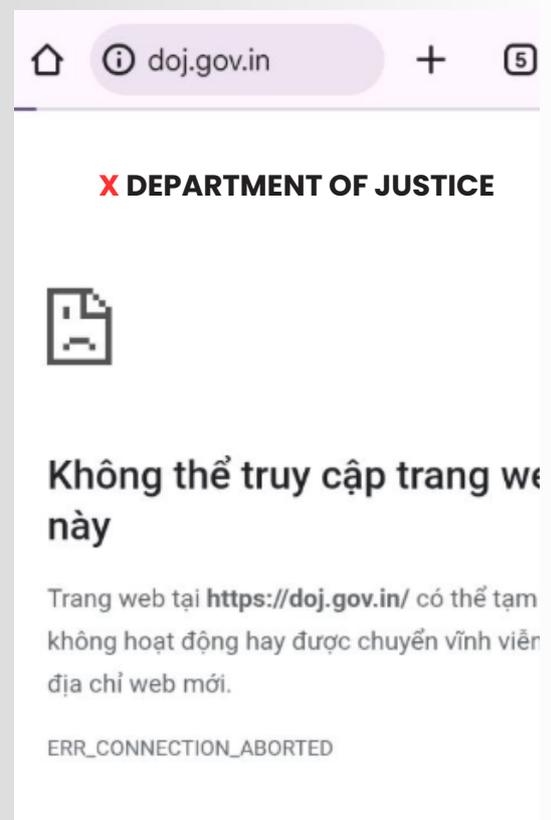
NOTABLE ATTACKS



<https://check-host.net/check-report/25d279c7k106>



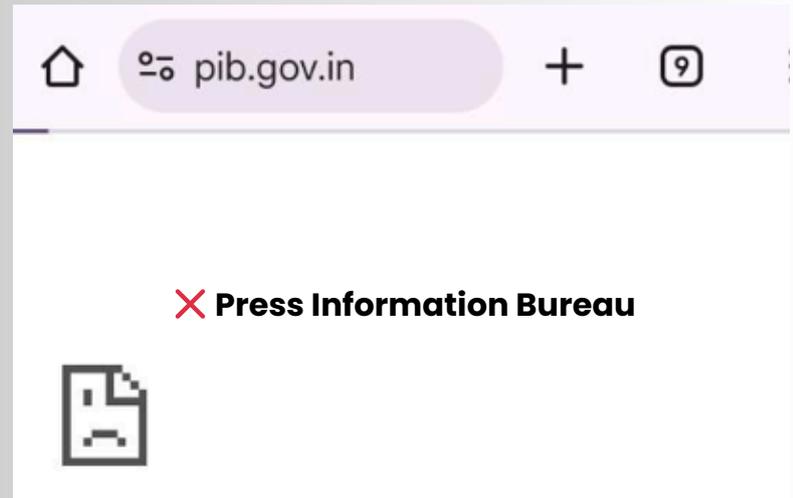
<https://check-host.net/check-report/25d27cb0k58c>



<https://check-host.net/check-report/25d27e%C3%A83kd08>



<https://check-host.net/check-report/25da7990k760>



<https://check-host.net/check-report/25da70c9kd79>



Lực Lượng Đặc Biệt Quân Đội Điện (Electronic Army Special Forces)

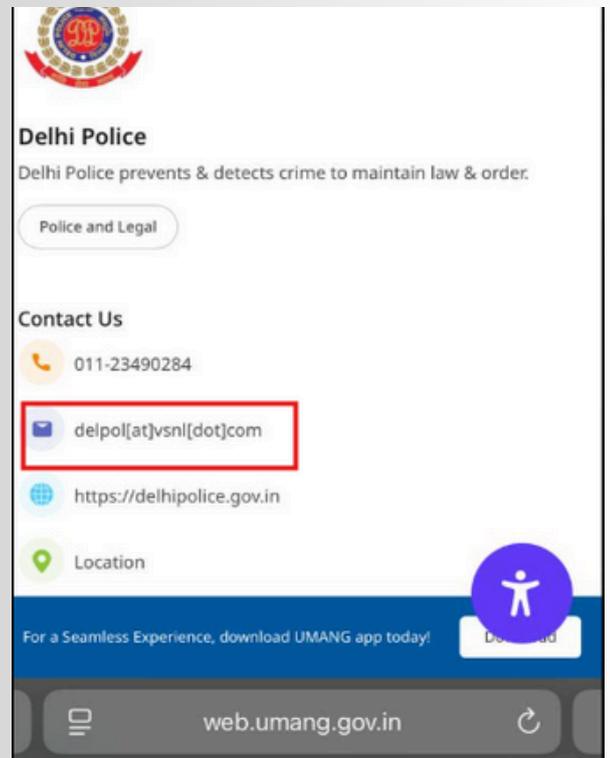
- The group known as Lực Lượng Đặc Biệt Quân Đội Điện Tử (Electronic Army Special Forces) and its affiliates have concentrated their efforts on India's Judicial infrastructure and Government digital assets.
- Their campaign has reportedly targeted court systems ranging from district to high courts as well as various central and state-level government portals and law enforcement platforms, signaling a strategic focus on disrupting administrative and legal operations.



NOTABLE ATTACKS



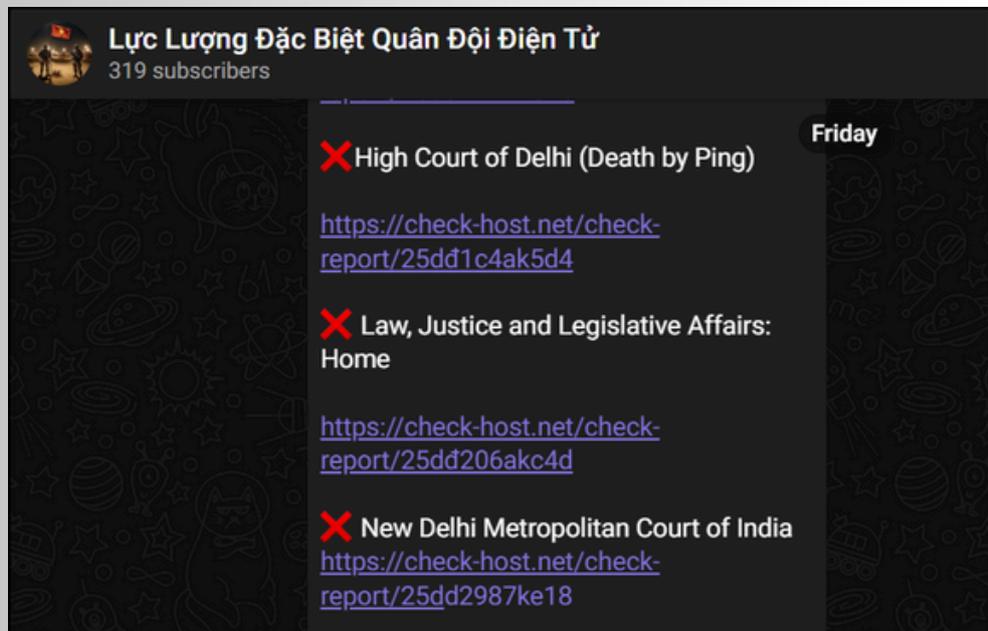
<https://check-host.net/check-report/25dccd3cka1>



<https://check-host.net/check-report/25dce19fk742>



<https://check-host.net/check-report/25d349d7k597>



Attacker claimed multiple DDOS attack on Judicial courts of India



KEYMOUS+



Keymous+ is a North African hacktivist group known for its politically motivated cyber activities. The group primarily targets governmental, financial, and media institutions, leveraging a mix of traditional cyberattack techniques to promote political causes and disrupt critical infrastructure. Their operations often reflect regional political tensions.

NOTABLE ATTACKS

Keymous+
420 subscribers

Pinned message
De la beauté et du charme On pense qu'on mérite pas les cieux

- ✗ CtrlS - Asia's Largest Rated 4 Data Center & Managed Service Provider
[Check host](#)
- ✗ National Cloud | National Informatics Centre | India
[Check host](#)
- ✗ Municipal Corporation of Mumbai
[Check host](#)
- ✗ official portal for Bharat Broadband Network Limited
[Check host](#)
- ✗ National Internet Exchange of India
[Check host](#)
- ✗ Department of Telecommunications
[Check host](#)

[Keymous](#) | [Back up](#) | [X](#) | [Arabic](#) | [French](#) | [Cypher](#) | [Elite](#)

Keymous +
@KeymousTeam

Just for fun !
Hacked Access :
Kerala Farmers' Welfare Fund Board – Official Portal for Farmer Registration, Pension & Benefits

1	gfm:	Other
	flg:	Thiruv
	roqgaf:	Mahadgarum
	rdgaf:	Kozhik
	mlkba's email:	11
	mlkba's mobile:	
	pdgaf:	BENJALAKTA
	mlkaf's email:	3 1
	agfgr:	28
	rdgaf's mobile:	rdgaf.
	rdgaf's mobile:	rdgaf.
2	gfm:	Other

Keymous+
432 subscribers

- ✗ K. K. Wagh Institute of Engineering Education and Research
- ✗ indian booking service
- ✗ IndianBank

Screenshots available on X : Follow us

Thank you , Next ...

[Keymous](#) | [Back up](#) | [X](#) | [Arabic](#) | [French](#) | [Cypher](#) | [Elite](#)

#Hack_For_Humanity
#Holy_League
#Keymous

👍 3 ❤️ 3 🔥 1

198 👁 07:07 PM

Keymous+
432 subscribers

10/17

- ✗ Power Grid Corporation of India
[Check host](#)
- ✗ National Commission for Women (NCW)
[Check host](#)
- ✗ Kalpataru Power Transmission
[Check host](#)
- ✗ Delhi Police
[Check host](#)
- ✗ NHPC Limited
[Check host](#)

Keymous+
432 subscribers

As we said before , it was possible ! 🌈 **Sunday**

Happened in late time 🕒

- ✗ CERT-In (Indian Computer Emergency Response Team)
[Check host](#)
- ✗ NCIIPC (National Critical Information Infrastructure Protection Centre)
[Check host](#)
- ✗ C-DAC (Centre for Development of Advanced Computing)
[Check host](#)
- ✗ IPS (Indian Police Service)
[Check host](#)



ANONSEC



AnonSec is a decentralized hacktivist collective that emerged from the Anonymous movement. Known for its cyber activism, the group primarily targets organizations and governments to protest against perceived injustices and to promote transparency. AnonSec has claimed responsibility for various high-profile cyber attacks, often emphasizing social and political causes.

AnonSec employs a variety of attack techniques, including but not limited to:

- 1. Distributed Denial of Service (DDoS) Attacks:** Overwhelming a target's server with traffic to render it inaccessible.
- 2. Website Defacement:** Modifying the content of a website to convey political messages or discredit the target.
- 3. Data Breaches:** Gaining unauthorized access to sensitive information and leaking it publicly to expose wrongdoing
- 4. Social Engineering:** Manipulating individuals to divulge

NOTABLE ATTACKS

- India's Airport Sites and Portals Have Gone Offline...
 - Rajiv Gandhi International Airport (Hyderabad) Official Website. — India.
Check Host : <https://check-host.net/check-report/25e47e17k442>
 - Chennai International Airport — India.
Check Host : <https://check-host.net/check-report/25e48220ke99>
 - Rajahmundry Airport India Official Website.
Check Host : <https://check-host.net/check-report/25e4728akc03>
 - Devi Ahilyabai Holkar Airport (Indore) Official Website.
Check Host : <https://check-host.net/check-report/25e47a07k7e0>
 - Sardar Vallabhbhai Patel International Airport — India.
Check Host : <https://check-host.net/check-report/25e44af1k623>

Is Newdelhiairport.in down? May 8

It's not just you! newdelhiairport.in is down.

Last updated: May 8, 2025, 7:03 AM (1 second ago)

Check website: <https://newdelhiairport.in/>

Location	Status	Time	Code	# of visitors
Abu Dhabi, United Arab Emirates	Server error	6:59 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:57 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:55 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:53 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:51 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:49 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:47 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:45 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:43 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:41 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:39 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:37 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:35 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:33 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:31 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:29 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:27 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:25 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:23 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:21 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:19 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:17 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:15 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:13 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:11 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:09 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:07 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:05 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:03 AM	500 (Internal Server Error)	20,204,244
Abu Dhabi, United Arab Emirates	Server error	6:01 AM	500 (Internal Server Error)	20,204,244

The official website of Indira Gandhi International Airport [Delhi].

- Rajiv Gandhi International Airport (Hyderabad) Official Website. — India.
Check Host : <https://check-host.net/check-report/25e47e17k442>
- Chennai International Airport — India.
Check Host : <https://check-host.net/check-report/25e48220ke99>
- Rajahmundry Airport India Official Website.
Check Host : <https://check-host.net/check-report/25e4728akc03>
- Devi Ahilyabai Holkar Airport (Indore) Official Website.
Check Host : <https://check-host.net/check-report/25e47a07k7e0>
- Sardar Vallabhbhai Patel International Airport — India.
Check Host : <https://check-host.net/check-report/25e44af1k623>

AnonSec claims to have targeted the website of BSNL India.

NB: Site is down at the moment.

Is Bsnl.co.in down?

It's not just you! bsnl.co.in is down.

Last updated: Apr 23, 2025, 11:58 PM (1 second ago)

- BSNL - One of the Biggest Telecommunications company Of India.
- Proofs :
 - <https://check-host.net/check-report/2542adfak21>
 - <https://check-host.net/check-report/2542afa8k2f4>



THREAT ACTORS & THEIR ALLIANCES

Following the Pahalgam terror attack and India's retaliatory strikes against Pakistani targets, the cyber threat landscape has seen a sharp escalation. Multiple ideologically aligned hacktivist groups have begun forming publicly declared alliances aimed at disrupting India's digital infrastructure. These developments underscore a coordinated geopolitical agenda, moving beyond isolated hacktivism into campaign-based cyber offensives.

Name of the Threat Actor: **Electronic Army Special Forces**



Alliances of Electronic Army Special Forces

FalconFeeds.io @FalconFeedsio

Alert: New Hacktivist Alliance

Garuda Error System and Electronic Army Special Forces have officially announced a new alliance. They have recently been targeting India, Thailand, Israel, Egypt, Philippines, Vietnam, and Cambodia.



NEW ALLIANCE
HACKTIVIST ALLIANCE
2025

OFFICIAL SPECIAL ANNOUNCEMENT

R3V0XAn0nymous proudly announces a new strategic alliance with ELECTRONIC ARMY SPECIAL FORCES.

GARUDA ERROR SYSTEM

Forwarded from **Anonymous Guys**

ALLIANCE



ALIANCE MUSLIM CYBER TEAM

We officially announced a new alliance with the Cyber Army Special Forces to strengthen cyber security, help each other if one of us is attacked, and jointly carry out DDOS attacks and website hacks.

We Declare Our Official **Alliance** With "Electronic Army Special Forces".



Name of the Threat Actor: VULTURE

Alliances of VULTURE



Forwarded from GARUDA ERROR SYSTEM



OFFICIAL ALLIANCE ANNOUNCEMENT
We are proud to announce our official Alliance with Vulture, This collaboration will strengthen our efforts to expand our reach, and bring new opportunities.

er alliance with vulture to enhance
acks against injustice and spread t
the way we know how.



Name of the Threat Actor: Keymous+

Alliances of Keymous+

NEW ALLIANCE
HACKTIVIST ALLIANCE

📢 OFFICIAL ANNOUNCEMENT 📢

We are proud to announce that Keymous, the New Hacktivist Alliance, has officially formed an alliance with R3VOXAnOonymous

➔ Forwarded from GARUDA ERROR SYSTEM

NEW ALIANCE

📢 OFFICIAL **ALLIANCE** ANNOUNCEMENT 📢

We are proud to announce our official **Alliance** with Keymous, This collaboration will strengthen our efforts, expand our reach, and bring new opportunities.



Alliances of AnonSec



Dark Storm X AnonSec

United In Cyber Resistance

OFFICIAL ANNOUNCEMENT

We are proud to announce our official Alliance with DARK STORM! , This collaboration will strengthen our efforts, expand



Sumatra Utara Cyber Team X AnonSec

United In Cyber Resistance

OFFICIAL ANNOUNCEMENT

We are proud to announce our official Alliance with Sumatra Utara Cyber Team, This collaboration will strengthen our



Garuda Error System X AnonSec

United In Cyber Resistance

OFFICIAL ANNOUNCEMENT

We are proud to announce our official Alliance with GARUDA ERROR SYSTEM, This collaboration will strengthen our effort expand our reach, and bring new opportunities.



RipperSec X AnonSec

United In Cyber Resistance

OFFICIAL ANNOUNCEMENT

We are proud to announce our official Alliance with RipperSec, This collaboration will strengthen our efforts, expand our reach, and bring new opportunities.



PRIMARY ATTACK METHODS

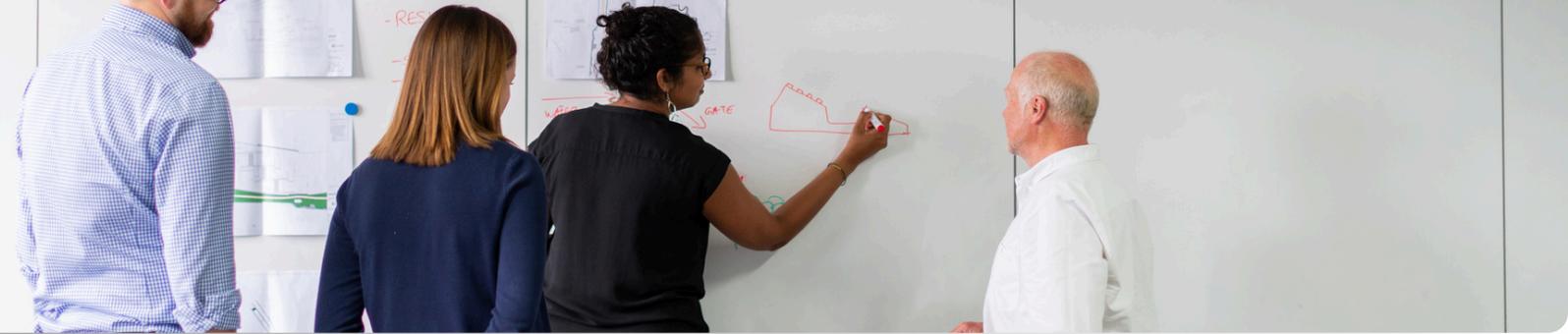


1. DDoS (Distributed Denial-of-Service Attacks):

- **DNS Reflection/Amplification Attack:** Exploits vulnerable DNS servers to amplify rogue requests, flooding the target with massive DNS response traffic.
- **TCP Flood (Layer 4 Attack):** Abuses the TCP three-way handshake by sending numerous connection requests without completing them, causing resource exhaustion via half-open connections.
- **HTTP Flood (Layer 7 Attack):** Overloads web servers with a high volume of seemingly legitimate HTTP requests, depleting resources and denying service to genuine users.
- **RUDY (R-U-Dead-Yet) Attack (Layer 7):** Sends slow HTTP POST requests one byte at a time, holding connections open to drain server memory and processing power.
- **Other Reflection & Amplification Attacks (Layer 3/4):** Use spoofed IP addresses to exploit UDP-based services (e.g., NTP, Memcached, Chargen, SSDP) for amplifying traffic and hiding attacker identity.

2. Web Defacement

- **Target Vector:** Hacktivists exploit vulnerabilities in PHP file upload plugins, particularly using the "Alone injector.php" tool.
- **Attack Method:** A PHP code injection technique is used to upload and execute malicious scripts on the target server.
- **Exploitation Technique:** The injected PHP scripts often contain functions that allow execution of system-level commands, enabling attackers to take control of the web application or server.
- **Impact:** Once access is gained, attackers alter the website's content, replacing legitimate pages with hacktivist slogans, images, or political messages.



TECHNICAL RECOMMENDATIONS AND COUNTER MEASURES BY MH-CERT

• IO- Based Defence (Multi-Layered Application)

- o **Firewall / IPS / Perimeter Devices:** Block malicious IP addresses, C2 domains, and URL patterns through perimeter firewalls, UTM, or NGFW with threat feeds.
- o Endpoint Detection and Response (EDR/XDR): Block and monitor execution of malicious hashes (MD5/SHA256), file paths, and process behaviours.
- o Web Proxy / Secure Web Gateway (SWG): Apply domain-based IOC filtering to block malicious or typosquatted domains and suspicious URLs used in phishing lures or redirections.
- o Email Security Gateway: Filter attachments, URLs, and sender domains associated with malicious campaigns. Use IOC-based allow/block lists to filter at MTA level.

• Endpoint Protection & EDR Hardening:

- o Implement EDR rules to block execution based on file extensions commonly used in malicious campaigns (e.g., .bat, .sh, .vbs, .js, .ps1).
- o Disable PowerShell access for non-administrative users to limit post-exploitation lateral movement.
- o Block USB storage devices and memory card slots at the OS level unless explicitly required. Use device control features of EDR.
- o Ensure SMBv3 or later is used with signing enforced to secure file-sharing protocols.
- o Disable NTLM authentication or enforce NTLMv2 at minimum; prefer Kerberos wherever possible.

• Email and Supply Chain Threat Protection

- o Harden email gateway policies to block high-risk file types (.bat, .js, .vbs, .sh, .exe, .lnk) from untrusted sources.
- o Implement advanced anti-phishing and anti-spoofing controls (SPF, DKIM, DMARC) and enhanced sandboxing for external attachments.
- o Enable aggressive spam and scam heuristics for all inbound messages from non-whitelisted domains.
- o Review third-party and supply chain communication flows—enable domain-based trust validation and enforce communication only through vetted channels.
- o Segment and audit supplier access and establish fallback plans for critical dependencies during heightened threat periods.

• Network Security and Proxy Layer

- o Review secure web gateway and proxy configurations to enforce domain filtering, SSL inspection, and malware scanning.
- o Deploy next-gen firewalls with threat intel integration to detect known APT infrastructure.
- o Implement Anti-APT appliances or sandboxes at critical egress/ingress points for zero-day and behavioral detection.
- o Deploy SSL inspection and TLS 1.3 proxying where legally and technically feasible.

Backup & Recovery Controls

- o Ensure immutable backups stored across different geo-locations, with at least one copy in a non-seismic and non-network-accessible environment.
- o Test disaster recovery and data restoration procedures regularly for ransomware scenarios.
- o Isolate backup systems from production domains using logical or physical segregation.

• DDoS and Critical Infrastructure Readiness

- o Engage with ISPs to implement Clean Pipe / DDoS scrubbing services, especially for public-facing applications.
- o Run DDoS readiness tests and simulate failovers to alternate geo-redundant routes.
- o Update incident response playbooks to include high-scale volumetric and application-layer DDoS events.
- o Ensure your cloud volumetric DDoS monitoring thresholds are properly configured to detect unusual traffic spikes in the above-mentioned protocols/services.
- o In the case of on-premise/inline DDoS protection solutions, make sure to enable on-demand HTTP authentication controls in case of abnormal HTTP requests.
- o Ensure directory listing is disabled to prevent attackers from viewing sensitive files.
- o If using a CMS (e.g., WordPress, Joomla), ensure it is properly configured and secured.
- o Use security plugins/modules designed to detect and block malicious activity
- o Regularly change default admin passwords and usernames.

• Authentication and Access Control

- o Enforce Multi-Factor Authentication (MFA) for all privileged and remote access.
- o Apply the Principle of Least Privilege (PoLP) to all users and service accounts.
- o Continuously review and revoke unused privileges in critical systems.
- o Implement Windows security policies to restrict access to vssadmin, wmic, and PowerShell for regular users.

• Active Directory and Privileged Access Management

- o Conduct Active Directory security reviews including group memberships, admin roles, and GPO policies.
- o Deploy tiered admin access model (Tier 0, 1, 2) to segregate domain controllers and sensitive systems.
- o Perform regular tests of your Disaster Recovery Plan (DRP) and Domain Controllers (DCs) for failover reliability.
- o Log, Monitor and alert on suspicious AD changes and privilege escalations.
- o Use EDR solutions that detect and alert on bulk shadow copy deletions

• Mobile Device Security

- o Implement Mobile Device Management (MDM) on smartphones.
- o Limit app installations to authorized stores only and disable the "Install from Unknown Sources" option.
- o Continuously monitor Android devices for signs of CapraRAT and other mobile Remote Access Trojans (RATs).

• Awareness & Governance

- o Conduct frequent cybersecurity awareness sessions focusing on phishing, USB hygiene, and reporting procedures.
- o Conduct Table Top – Incident Response Testing for CSIRT teams and Table Top Cyber Crisis Management Testing for Executive Leadership.