India-Pakistan Cyber Frontlines: The Invisible Battlefield

MH CERT

Advisory ID: CERTMH_CTI_2025_21

Date: 10th May 2025

Contents

OVERVIEW

In the wake of the tragic Pahalgam terror attack targeting Indian tourists, Indo-Pakistani tensions have escalated dramatically, pushing both nations into heightened military and strategic readiness. As conventional forces conduct large-scale drills including India's most extensive civilian war preparedness exercise since 1971, scheduled for May 7 2025, the digital domain has simultaneously emerged as a silent yet potent battleground.

In 2025, warfare transcends physical borders. The battlefield now includes cyberspace, where threat actors deploy malware, exploit vulnerabilities, and exfiltrate sensitive data long before the first bullet is fired. Recent reports of Pakistani cyber groups targeting Indian defence establishments underscore a coordinated effort to weaken national security and sow psychological disruption ahead of any kinetic confrontation.

Following the Pahalgam terror incident, MH-CERT has found a dramatic surge in hostile cyber activity originating from Pakistan and its ideological allies. According to telemetry from multiple threat monitoring systems, over 10 million intrusion attempts were recorded within days of the attack a mix of **DDoS floods, website**

defacements, phishing campaigns, and exploit attempts targeting public, critical infrastructure and defence portals.

CERT-Maharashtra (MH-CERT) indicate that Pakistani actors are not operating in isolation. Indicators suggest collaboration with actors from multiple Islamist cyber groups across regions forming what appears to be a loosely aligned cyber coalition targeting Indian critical infrastructure, defence think tanks, and public-facing assets. Their aim appears to be twofold: destabilization of internal systems and information warfare to fuel panic and erode public trust.

Key Points

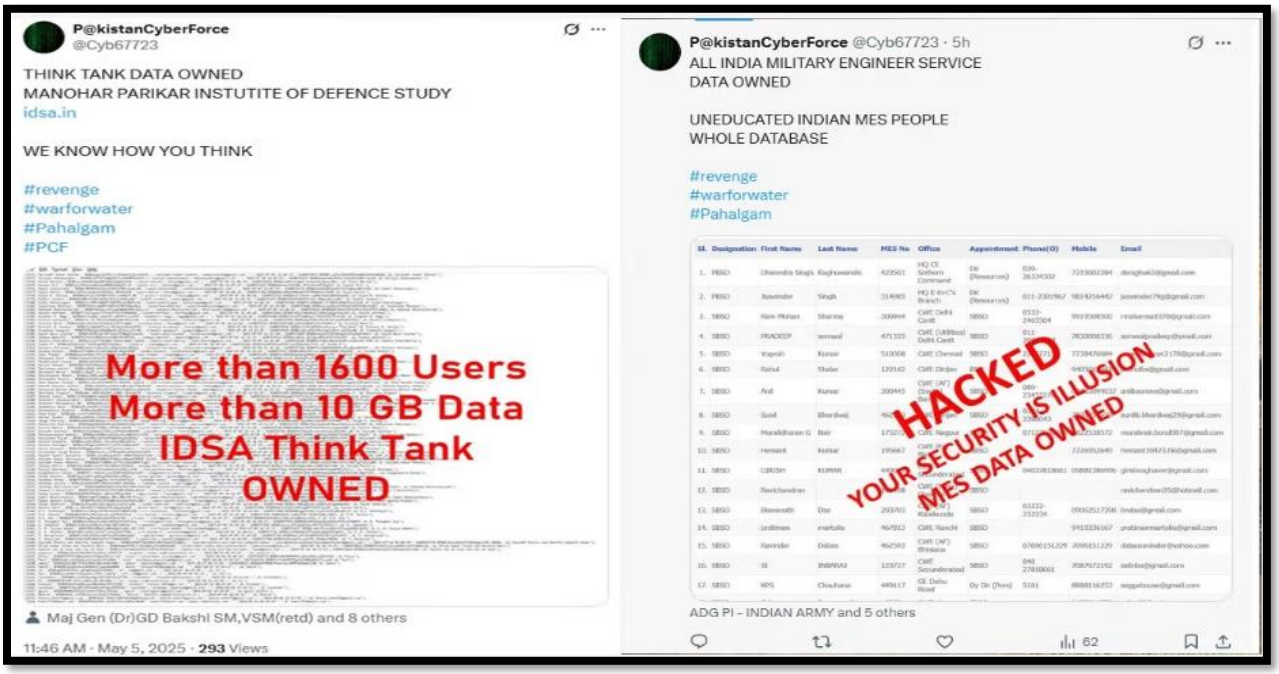
- **Key Targets:** Government portals, financial institutions, and educational institutions.
- **Tactical Escalation:** Activities are evolving from basic website defacements to advanced intrusions involving data exfiltration and disruption of critical infrastructure.
- **Ongoing Multi-Vector Operations:** Multiple simultaneous campaigns such as #OpIndia, #FreeKashmir, Operation Cyber_Wrath, and other pro-Pakistan hacktivist operations—are actively targeting Indian digital assets.

Pakistan Cyber Force's Claims

On **May 5, 2025**, a hacker group identifying itself as the “Pakistan Cyber Force” publicly claimed to have gained unauthorized access to data from the **Military Engineering Services (MES)** and the **Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA)**, a government-affiliated strategic think tank. The group asserted that they had obtained login credentials and other sensitive information associated with personnel from these institutions.

In addition to this data breach, the hacker group also defaced the official website of defence PSU **Armoured Vehicles Nigam Limited (AVNL)** with images of the Pakistan flag and the Al Khalid tank.

Pic 1: Pakistan Cyber Force claimed they have hacked AVNL limited posted on X (formerly known as twitter)



Pic 2: Pakistan Cyber Force hacked MP-IDSA and MES posted on X (formerly known as twitter)

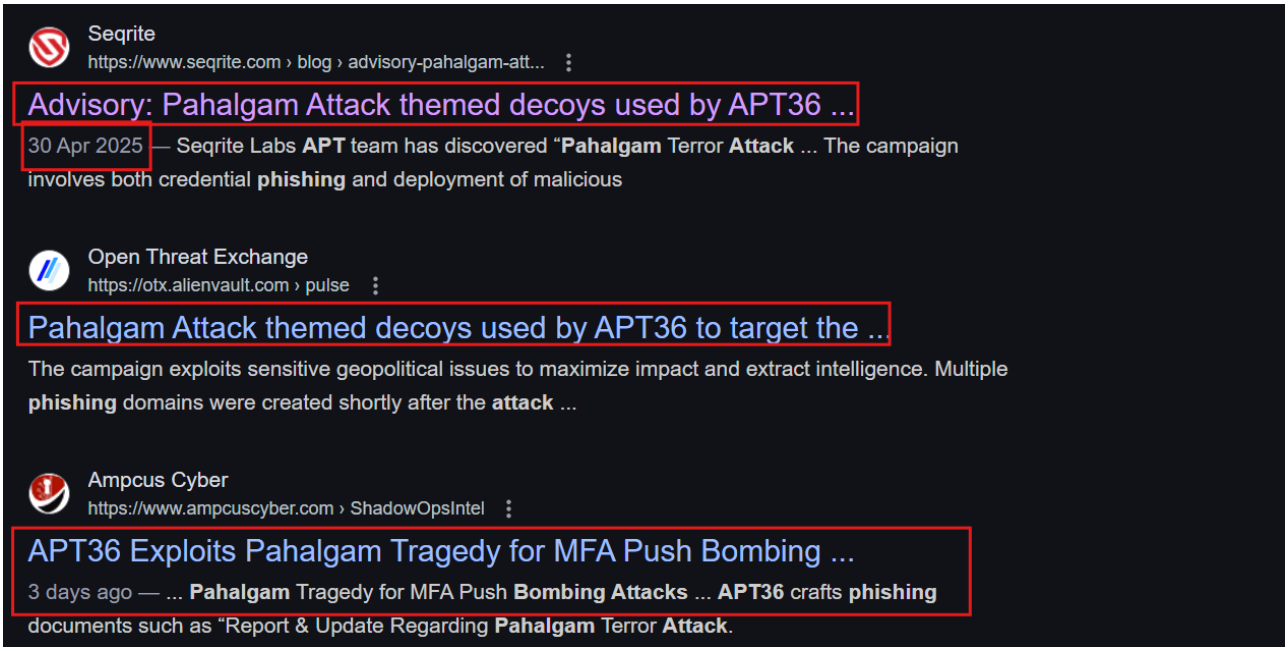
APT 36 Claim

Transparent Tribe, also known as APT36, is a Pakistan-based advanced persistent threat (APT) group that primarily targets Indian diplomatic, military, Defence, and aerospace sectors. Transparent Tribe has been observed using modern techniques such as clickjacking to trick users into unintentionally interacting with malicious content. Their operations commonly involve spearphishing emails, remote access Trojans (RATs), and data exfiltration mechanism

Aliases: Transparent Tribe, APT36, Mythic Leopard, ProjectM, C-Major
***Origin*:** Pakistan (state-sponsored)
Active Since: since 2013
Motivation: Espionage, primarily targeting India's defence, government, and educational sectors.
Target Sectors: Military, government institutions, education, research organizations, and defence contractors.

Notable Attack by APT36

Pic 3: APT36's March 2025 campaign using fake India Post site and malicious APK to target Indian users



Pic 4: APT36's April 2025 Pahalgam attack-themed lure Indian citizen

Malware families used by APT36

Malware	Description
Crimson RAT	Custom-built Remote Access Trojan. Used for surveillance, keylogging, data exfiltration.
ObliqueRAT	Used in attacks with malicious documents and image-based loaders. Delivered via phishing.
ObliqueRAT	Used in attacks with malicious documents and image-based loaders. Delivered via phishing
CapraRAT	Android spyware used against mobile devices. Can record audio/video, track location.
Peppy RAT / Remote Access Tools	Deployed via spear-phishing, often using .NET-based payloads.
JaskaGO	A lesser-known info-stealer/trojan linked to later stages of infection.

Sidecopy

The Pakistan-linked Advanced Persistent Threat (APT) group SideCopy has expanded its targeting scope since December 2024, now including sectors like railways, oil & gas, and external affairs ministries in India. APT team has been instrumental in uncovering SideCopy's evolving tactics, which now involve impersonating government officials and using Microsoft Installer (MSI) packages for payload delivery, shifting from HTML Application (HTA) files. The group has repurposed open-source tools such as Xeno RAT and Spark RAT, aligning them with Async RAT to enhance their espionage capabilities.

SideCopy's operations involve phishing campaigns using compromised and fake domains registered through GoDaddy.com, LLC, and they employ advanced techniques like reflective loading and AES/RC4 decryption to deploy custom RATs, highlighting the need for improved cybersecurity measures in targeted sectors.
Aliases: SideCopy only
Country of Origin: Pakistan
Active Since: At least 2019
Primary Targets: Indian defence and government sectors; occasional targeting of Afghanistan and Bangladesh
Targeted Sectors: Indian Armed Forces and Defense Research Organizations (e.g., DRDO), Government Ministries and Officials, Think Tanks and Policy Institutes, Educational Institutions (e.g., NCERT, universities), Diplomatic Entities.

Notable Attack by SideCopy

Pic5: SideCopy APT uses ReverseRAT backdoor to target DRDO in 2023 (source cyble)

Malware families used by SideCopy

Malware Name	Type	Description
ActionRAT	Custom RAT	Executes commands, downloads/upload files, takes screenshots. Widely used.
CetaRAT	Custom RAT	NET-based; designed for data exfiltration and command execution.
DetaRAT	Custom RAT	Used for remote desktop control and credential theft.
MargulasRAT	Custom RAT	Executes system surveillance tasks and steals documents.
AresRAT	Custom RAT	Includes Windows and Linux versions; used in recent multi-platform campaigns.
ReverseRAT	Custom RAT	Highly stealthy RAT focused on lateral movement and persistence.
AllaKore RAT	Commodity RAT	Lightweight remote-control tool; used for spying and data theft.
njRAT	Commodity RAT	Common RAT; supports keylogging, webcam control, credential theft.

The Anonymous 71

Anonymous 71 is a Bangladeshi hacktivist group operating under the broader Anonymous ideology. While its branding aligns with the global Anonymous collective, the group is primarily motivated by religious and regional grievances, often targeting Indian digital infrastructure. Their campaigns frequently use Bangladesh's national symbols, and group members explicitly associate themselves with Bangladeshi identity and causes, including anti-India narratives.

- **Aliases:** Anonymous 71
- **Country of Origin:** Bangladesh
- **Active Since:** Reportedly active since early 2020
- **Primary Targets:** Government websites and portals in India, Law enforcement and defense-linked web infrastructure.
- **Tactics and Methods:** DDoS (Distributed Denial of Service) attacks targeting public-facing services.

Pic 6: Based on the actor's claim about hacking 30+ Indian websites on Telegram channel

🔗 Alliance with Web-Sec

The below image confirms the formal **merger of Anonymous 71 with Web-Sec**, a Gaza-origin cyber group. The announcement, accompanied by jihadi imagery and messaging, signals a strategic cyber alliance intended to increase the scope, sophistication, and regional alignment of their operations. Their stated objective: to "work together for the benefit of the Muslim Ummah" implying a shared ideological motivation and coordination for broader impact.

Pic 7: Actor Anonymous 72 and web-sec declared merger on telegram

The group has publicly claimed responsibility for numerous **DDoS attacks** and **website defacements**, asserting these acts are retaliation against India's geopolitical stance.

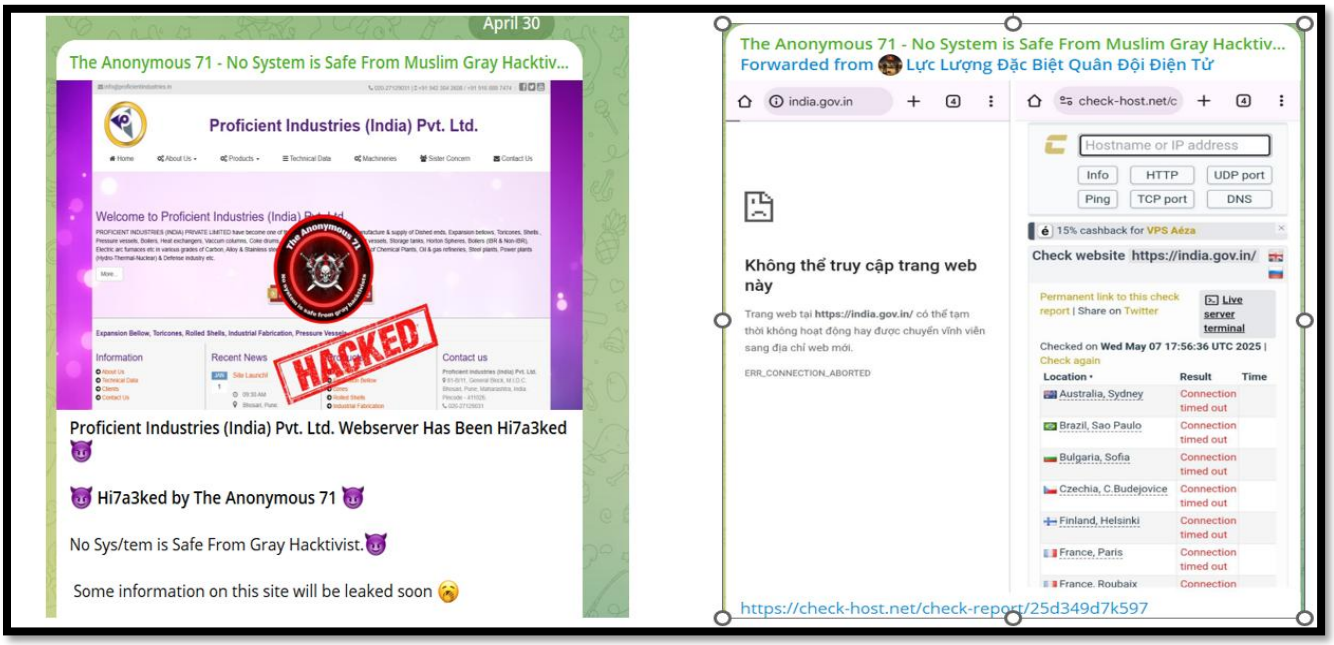
Through Telegram and other social platforms, Anonymous 71 has posted **screenshots and lists of compromised domains**, showcasing successful intrusions into various Indian web assets, including:

- Government-affiliated portals,
- Educational institutions,
- E-commerce and cosmetic platforms,
- Local tourism and travel websites.

Notable Attacks by Anonymous 71

These claims have been substantiated by visual evidence shared online (see screenshots below), where the group boasts of overwhelming Indian domains with traffic or leaving defaced political messages on compromised pages.

In above pictures on 28th April 2025, Actor claimed on Telegram that they hacked India's famous civil and defense aviation systems and the National Academy of Agricultural Science.



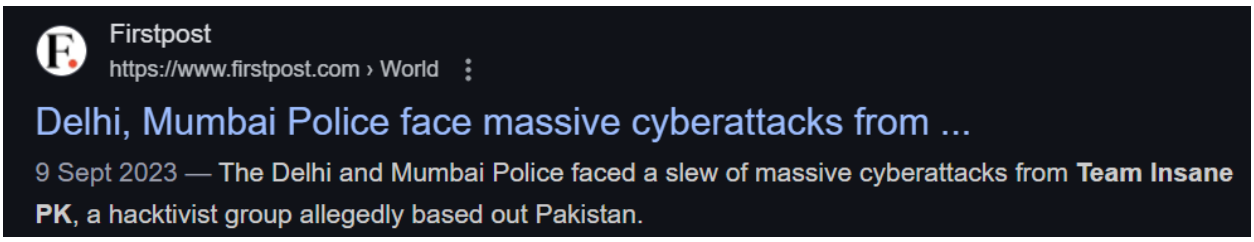
The Anonymous 71" also claimed to have breached the website of Proficient Industries (India) Pvt. Ltd., displaying a defacement page with their logo and the message "No Sys/tem is Safe from Gray Hacktivist" The image shows both the compromised corporate website with a "HACKED" stamp and monitoring results suggesting connection timeouts for india.gov.in from multiple global locations, potentially indicating a DDoS attack.

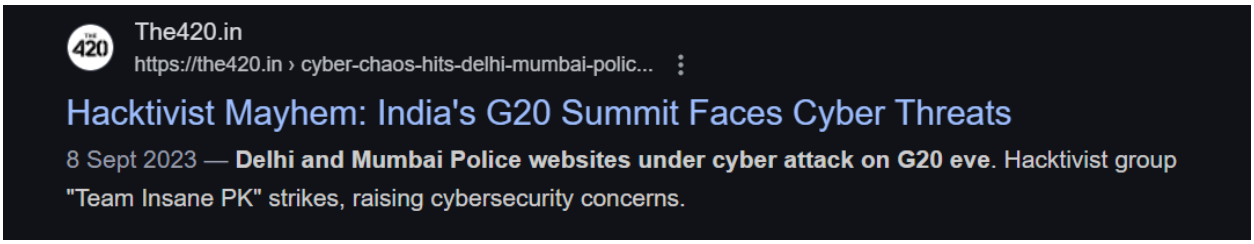
Team Insane PK

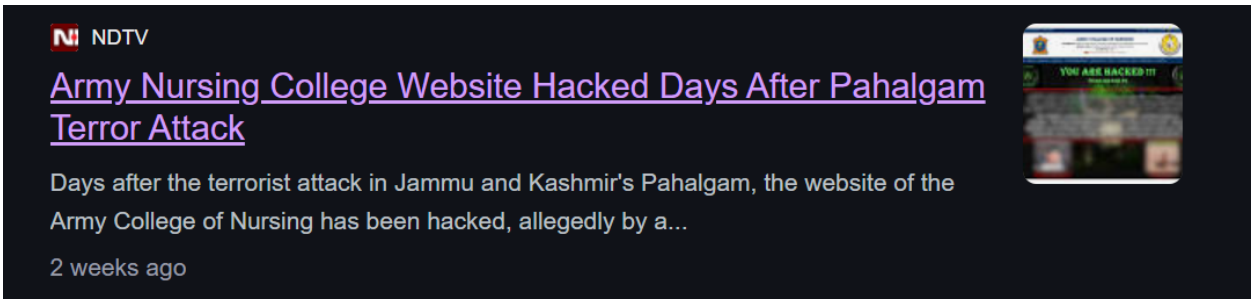
Team Insane PK is a group known for its activities in the realm of religious hacktivism. This group, allegedly based out of Pakistan, has been involved in numerous cyberattacks targeting Indian businesses and government websites. Their operations often involve the use of Distributed Denial of Service (DDoS) attacks, a common tactic in cyber warfare that overwhelms a network with traffic, rendering it inaccessible.

- **Aliases:** Team Insane PK
- **Type:** Religious/political hacktivist collective
- **Country of Origin:** Pakistan
- **Active Since:** At least February 2023
- **Primary Targets:** Police departments (e.g., Delhi and Mumbai Police), Ministry of Defence

Notable Attack by Team Insane PK







Attack Methods Observed

- **Fake Domain Registrations:** Malicious domains mimicking official ones (e.g., @gov[.]in, @nic[.]in, and jkpolice[.]gov[.]in[.]kashmirattack[.]exposed) were used in phishing campaigns.

- **Phishing & Social Engineering:** Distribution of spoofed government documents portraying Pakistan in a favorable light.

- **DDoS and Trojan Deployments:** Remote Access Trojans used for persistent attacks and intelligence gathering.

Modes of Attack

- **Website Defacement:** Most common tactic, primarily targeting educational institutions and small-scale websites to spread propaganda and create public visibility.

- **Distributed Denial of Service (DDoS) Attacks:** Directed at government portals and critical infrastructure, aiming to disrupt service availability and undermine trust.

- **Data Breaches:** Increasingly sophisticated intrusions focused on extracting personal and financial data from targeted database.

MH-CERT Recommendations

1. Endpoint Protection & EDR Hardening

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

2. Email and Supply Chain Threat Protection

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

3. Network Security and Proxy Layer

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

4. DDoS and Critical Infrastructure Readiness

- Engage with ISPs to implement Clean Pipe / DDoS scrubbing services, especially for public-facing applications.
- Run DDoS readiness tests and simulate failovers to alternate geo-redundant routes.
- Update incident response playbooks to include high-scale volumetric and application-layer DDoS events.

5. Backup & Recovery Controls

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

6. Authentication and Access Control

- Enforce Multi-Factor Authentication (MFA) for all privileged and remote access.
- Apply the Principle of Least Privilege (PoLP) to all users and service accounts.
- Continuously review and revoke unused privileges in critical systems.

7. Active Directory and Privileged Access Management

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

8. Awareness & Governance

- Conduct frequent cybersecurity awareness sessions focusing on phishing, USB hygiene, and reporting procedures.
- Regularly audit firewall ACLs and DMZ configurations to ensure least-exposure principles are enforced.

SAVE THESE 24x7 HELPLINE NUMBERS & REPORT

- **1945 & 1930**
- **https://mhcyber.gov.in/ (MAHARASHTRA CYBER CRIME PORTAL)**