Three Recent Malware Incidents

By Aravind Radhakrishnan

This report focuses exclusively on significant malware incidents in India during 2025. Each case includes a summary, timeline, technical analysis of attack methods, mitigation and resolution steps, and lessons learned. Where details are still under investigation, the most likely vectors are identified based on public reporting and common TTPs in similar attacks.

1) Delhi Hospitals Hack (Sant Parmanand & NKS Super Speciality) — June 2025

Summary

On the night of June 10–11, 2025, two North Delhi hospitals reported server compromises that caused operational disruption. Investigations determined the event to be a deliberate cyberattack, likely involving ransomware or similar malware impacting core systems. OPD and IPD services were affected, and the facilities shifted to manual workflows to maintain patient care while the incident was contained.

Timeline (Key Dates)

- June 10–11: Servers at two Delhi hospitals are compromised; services disrupted.
- June 11–12: Initial triage treats the issue as a technical glitch; later confirmed as a cyberattack.
- Mid-June: FIR registered under the IT Act; cybersecurity experts engaged; manual contingency processes enabled.

Attack Method (Technical Breakdown)

While full forensic details have not been publicly disclosed, indicators point to a ransomware-style intrusion. Common initial access vectors in such cases include phishing emails carrying malicious attachments or links, exposed remote services (e.g., RDP/VPN) with weak credentials, or exploitation of unpatched vulnerabilities in internet-facing systems. Post-compromise actions often include lateral movement, privilege escalation, data exfiltration, and encryption of critical servers.

Mitigation & Resolution

- Immediate containment: Isolated affected servers and networks; shifted clinical operations to paper/manual workflows to sustain patient care.
- Forensics & law enforcement: FIR registered; cyber forensics teams engaged to identify the intrusion vector and scope the compromise.
- Recovery: Systems rebuilt and restored from backups where possible; staged reintroduction of digital services after validation.
- Hardening: Enforced MFA on remote access, patched internet-facing assets, implemented EDR with 24/7 monitoring, and reviewed backup/DR readiness.

Lessons Learned

- Healthcare-specific resilience: Maintain and routinely exercise downtime procedures for OPD/IPD and labs.
- Least privilege and segmentation: Limit blast radius by segmenting clinical, admin, and guest networks.

- Backups: Keep offline/immutable backups with regular restore drills; prioritize EMR/LIS systems.
- Early detection: Deploy EDR/NDR and monitor for anomalous encryption, mass file renames, and privilege escalations.

2) Lucknow Advertising Firm Ransomware — July 2025

Summary

A Lucknow-based advertising firm suffered a ransomware attack that encrypted key servers and disrupted business operations. The company filed a police complaint and engaged external security teams. Some systems were formatted and data restored from backups, though this unfortunately removed potential forensic artifacts required for deeper analysis.

Timeline (Key Dates)

- Early July: Attackers encrypt servers and demand ransom; operations impacted.
- Mid-July: FIR lodged; external AV/security team attempts data recovery; internal IT formats systems and restores from backups.
- Late July: Cyber investigation teams analyze probable initial access and affected infrastructure.

Attack Method (Technical Breakdown)

The attack aligns with common ransomware TTPs: initial phishing or exploitation of exposed services, followed by credential theft, lateral movement, and rapid encryption of file servers and endpoints. Data exfiltration cannot be ruled out, given prevalent double-extortion models.

Mitigation & Resolution

- Containment: Affected endpoints isolated; known-malicious processes terminated; network shares disabled.
- Recovery: Reimaged/clean-built systems; restoration from verified backups; staged service resumption with integrity checks.
- Forensics & reporting: Law enforcement engaged; logs preserved where possible; external responders assist with IOCs and eradication.
- Hardening: MFA enabled; privileged access reviewed; patch hygiene improved; continuous monitoring added.

Lessons Learned

- Preserve evidence: Avoid blanket formatting before forensic imaging; maintain chain of custody.
- Zero-trust basics: Restrict administrative rights; enforce strong authentication; monitor anomalous SMB/WinRM use.
- User awareness: Phishing-resistant authentication and continuous training reduce initial footholds.

3) State Cyber Crime Wing Data Centre Disruption — West Bengal (July 2025)

Summary

West Bengal's State Cyber Crime Wing (CCW) reported a major disruption at its data centre on July 28, 2025. The private vendor managing the centre cited a ransomware attack, but police suspect internal sabotage, given that the

vendor retained exclusive remote access and had not handed over administrative control. Critical platforms, including VoIP analysis tools, were affected.

Timeline (Key Dates)

- July 28: Disruption reported at the CCW data centre; vendor alleges ransomware.
- Late July: Police initiate investigation citing potential conspiracy and breach of trust; multiple staff questioned.
- August: Administrative control and access reviews undertaken; restoration and security audit efforts continue.

Attack Method (Technical Breakdown)

Attribution remains under investigation. Two competing hypotheses exist: (1) external ransomware intrusion, or (2) insider-enabled sabotage. Both scenarios would involve privilege abuse and control over remote administration tools. For ransomware, typical stages include payload delivery, lateral movement, and encryption with data theft. For sabotage, actions could include deliberate service disruption, configuration tampering, and data wiping.

Mitigation & Resolution

- Access remediation: Revoked exclusive remote access; instituted multi-admin control with logging and approvals.
- Incident response: Forensic acquisition of servers and admin consoles; law enforcement proceedings under the IT Act and relevant penal codes.
- Service recovery: Rebuild of affected services from known-good images and backups; validation of forensics tools before redeployment.
- Governance: Tightened vendor SLAs, key escrow, and administrative handover procedures; continuous monitoring and segmentation.

Lessons Learned

- Third-party governance: Never allow single-vendor exclusive remote/admin access; enforce dual control and audit trails.
- Credential and key management: Implement key escrow and break-glass procedures governed by policy.
- Segmentation and monitoring: Separate critical investigative platforms from general IT; instrument for tamper-evident logs.

References

Times of India — 'Servers of two city hospitals hacked; police register FIR' (June 2025): https://timesofindia.indiatimes.com/city/delhi/servers-of-two-city-hospitals-hacked-police-register-fir/articleshow/121836219.cms

Times of India — 'FIR after ransomware corrupts ad firm data' (July 2025): https://timesofindia.indiatimes.com/city/lucknow/fir-after-ransomware-corrupts-ad-firm-data/articleshow/122147266.cms

Times of India — 'State police cyber crime wing faces data breach, cops suspect sabotage' (Aug 2025): https://timesofindia.indiatimes.com/city/kolkata/state-police-cyber-crime-wing-faces-data-breach-cops-suspect-sabotage/articleshow/123047377.cms