Three Recent Malware Incidents

By Akshai S

This report explores three major malware incidents in India during 2025, highlighting how attackers used fake apps, phishing links, and system intrusions to steal data and money. These methods caused both financial losses for individuals and operational risks for organizations, showing how deeply malware now affects India's digital ecosystem. By analyzing the attacks, their impact, and responses, the report underlines the urgent need for stronger defenses and public awareness.

1) Tata Group's Indian Hotels Company (IHCL) Malware Incident

Summary

In February 2025, the Tata Group–owned Indian Hotels Company Limited (IHCL) disclosed a malware incident affecting some of its IT systems. While core hotel operations continued, the admission highlighted increasing cyber risks in India's hospitality industry.

Timeline

- **Feb 16, 2025** – IHCL publicly confirms malware detected in its IT systems.
- **Feb 17, 2025** – Affected servers isolated to contain the attack.
- **Feb 18, 2025** – Company notifies relevant regulators and law enforcement.
- **Late February 2025** – Forensic investigation and monitoring expanded across all networks.

Attack Analysis

- **Possible Vectors:** Phishing emails, exploitation of unpatched servers, or lateral movement after credential compromise.
- **Likely Goals:** Exfiltration of guest data, disruption of payment/reservation systems, or ransomware encryption.

Impact

- Potential exposure of guest records and payment card information.
- Operational disruption risk, though hotels continued functioning.
- Reputation risks for a luxury brand.

Response & Resolution

- Isolation of infected systems and forensic review.
- Regulatory notifications filed promptly.
- Hardening of endpoints, stronger patching, and improved monitoring.

Key Takeaways

- Even elite corporations are vulnerable to malware attacks.
- Transparency and swift disclosure help retain trust.
- Proactive monitoring and patching reduce damage.

2) Tamil Nadu e-Challan Malware Scam

Summary

In August 2025, Tamil Nadu cybercrime authorities warned of a WhatsApp-driven scam where victims received fake traffic challan alerts. The messages instructed users to download a counterfeit “mParivahan” APK app, which was actually malware.

Timeline

- **Mid-August 2025** – Victims begin reporting suspicious WhatsApp challan messages.
- **Aug 18–20, 2025** – Investigations confirm malicious APK distribution.
- **Aug 21, 2025** – Tamil Nadu cybercrime wing issues statewide alert.
- **Late August 2025** – Awareness drives launched, fake APK links reported for takedown.

Attack Analysis

- **Delivery:** Fake government-themed WhatsApp messages.
- **Execution:** Malicious APK requests excessive permissions (SMS, contacts, notifications).
- **Core Trick:** Intercepted OTPs and banking SMS to bypass 2FA and drain accounts.

Impact

- Citizens risked financial theft and privacy loss.
- The government’s brand was abused for credibility.
- Fear spread among drivers about legitimate challans.

Response & Resolution

- Publicly clarified that traffic fines are *never* sent on WhatsApp.
- Guidance: use only official Parivahan website/app.
- Warnings in local media to boost citizen awareness.

Key Takeaways

- Social engineering via government impersonation is highly effective.
- APK sideloading remains India’s weakest security gap.
- Education in regional languages is vital to reach vulnerable groups.

3) Jamnagar WhatsApp Malware Fraud

Summary

In March 2025, police in Jamnagar arrested two individuals after a farmer and his father lost ₹6.4 lakh to a WhatsApp-distributed malware called **RTO.APK**. The malware hijacked phones, intercepted OTPs, and enabled fraudulent bank transfers.

Timeline

- **Mar 5, 2025** – Victims receive WhatsApp link to download fake RTO.APK.
- **Mar 6–7, 2025** – Fraudulent UPI withdrawals of ₹2 lakh and ₹4.4 lakh occur.
- **Mar 8, 2025** – Police trace fraud, arrest two suspects in Jamnagar.
- **Mid-March 2025** – Investigation expands to track mastermind in Jharkhand.

Attack Analysis

- **Distribution:** WhatsApp link delivering a fake government app.
- **Execution:** APK abused SMS, UPI, and contact permissions.
- **Fraud Chain:** Stolen OTPs enabled attackers to bypass authentication and transfer funds.

Impact

- Direct loss of ₹6.4 lakh to victims.
- Psychological stress for the farmer's family.
- Highlighted how malware scams penetrate rural India.

Response & Resolution

- Arrests of two local perpetrators.
- Funds traced through rented bank accounts.
- Hunt for larger network and "Anwar," the mastermind, still ongoing.

Key Takeaways

- WhatsApp is India's #1 malware delivery channel.
- Rural citizens are increasingly vulnerable.
- Multi-factor authentication beyond SMS OTP is critical.

Conclusion

These three incidents show how malware in India during 2025 has **multiple faces**:

- Corporate system compromise (IHCL).
- Government-impersonation fraud (e-Challan scam).
- Grassroots-level WhatsApp malware fraud (Jamnagar).

The common threads are **malicious APKs, weak awareness, and misuse of trust**. Solutions lie in **corporate resilience, public education, and better authentication standards.**

References

- Economic Times – IHCLdent
- Times of India – Tamil Nadu e-challan malware scam
- Times of India – Jamnagar WhatsApp fraud