Cyber Espionage Against Critical Infrastructure: A Case Study of Targeted Attacks on Indian State Load Dispatch Centres (SLDCs)

Riya Malpani[1]
Computer Science & Engineering (First Year)
Jawaharlal Nehru Engineering College, MGM University
Chh. Sambhajinagar,India
Email- riyamalpani56@gmail.com

Aneesh Pande2
Computer Science & Engineering (First Year)
Jawaharlal Nehru Engineering College, MGM University
Chh. Sambhajinagar,India
Email
pandeaneesh0304@gmail.com

Ms.Sushama Deshmukh3
Asst.Professor Computer Science & Engineering Jawaharlal Nehru Engineering College,
MGM University
Chh. Sambhajinagar, India
Email-
sushamadeshmukh2020@gmail.com

Abstract—With rapid digitalization, India has witnessed an exponential rise in cybercrime, necessitating robust cyber security measures and advanced cyber forensic techniques. While cybersecurity seeks to prevent attacks, Cyber forensics, also known as digital forensics, is a critical discipline within the broader field of cybersecurity that involves the identification, preservation, analysis, and presentation of digital evidence. As cybercrimes continue to evolve in complexity and scale, cyber forensics plays a vital role in investigating incidents such as data breaches, cyber terrorism, and financial fraud.Also, India's critical infrastructure is facing an unprecedented rise in cyber threats, with electrical grid systems being a prime target.This paper explores the interplay between cyber security and cyber forensics in India through a case study approach of real-life case investigating a targeted cyber espionage campaign against at least seven State Load Dispatch Centres (SLDCs), responsible for grid control via Supervisory Control and Data Acquisition (SCADA) systems, highlighting systemic strengths and weaknesses and assessing the legal and technological responses to cybercrime.

Keywords—Cybersecurity & Cyber forensics, Digital evidence, SCADA systems,Critical infrastructure attacks, Cyber espionage campaign, PLA-linked threat actors, Data breaches, Indian power grid cybersecurity, Forensic analysis, Cyber laws and policy response.

I. INTRODUCTION

The increasing convergence of operational technology (OT) and information technology (IT) has exposed national infrastructure to advanced cyber threats. India's SLDCs, which form the nerve center of the state electrical grids, are vulnerable due to reliance on legacy SCADA systems. Between 2021 and 2024, researchers reported targeted attacks on these centres, likely tied to geopolitical tensions with China.

So what is a SCADA System?

SCADA (Supervisory Control and Data Acquisition) is a type of industrial control system used to monitor and control critical infrastructure and industrial processes remotely. It is a combination of hardware and software that enables industrial process automation by capturing Operational Technology (OT) real-time data. It connects sensors that monitor equipment like motors, pumps, and valves to an onsite or remote server, ensuring seamless communication and control.These systems are invaluable in industries where real-time monitoring and data acquisition are crucial.

II. IMPORTANCE OF SLDC'S AND SCADA SYSTEMS

The SLDC is the Apex body to ensure integrated operation of the Power System in a State. The State Load Despatch Centre shall be responsible for:-

- Scheduling and despatch of electricity
- Carrying out real time operation for control of grid and ensuring reliability
- Exercising the supervision and control over the intra state transmission system
- Monitoring Grid Operations
- Keeping account of the electricity transmitted through the Grid
- Coordinating with Western Region Load Despatch Centre.
- Grid load balancing
- Frequency and voltage management
- Scheduling and dispatch of electricity

A SCADA system is a combination of hardware and software that enables industrial process automation by capturing Operational Technology (OT) real-time data. It connects sensors that monitor equipment like motors, pumps, and valves to an onsite or remote server, ensuring seamless communication and control.

-Data Acquisition: The collection of SCADA data frequently involves some kind of analog to digital conversion. -

Networked Data Communication: The collected data is transmitted either spontaneously or in response to a request for data to some kind of upstream consolidator ormaster. -

Data Presentation: The collected data is processed, organized and presented for system operators to make appropriate response and control decisions.

-Control: If control decisions are warranted and the system supports output, appropriate commands can be dispatched to affect specific operational or configuration changes. Most control actions are performed by RTUs and PLCs.

III. CYBER SECURITY LANDSCAPE IN INDIA

India's digital growth through initiatives like Digital India has led to increased cyber threats, including phishing, ransomware, and identity theft. Key institutions like CERT-In (Computer Emergency Response Team - India) monitor and respond to incidents, while the IT Act 2000 provides legal recourse.

A. Rise in Cyber Threats

The digital era has heightened vulnerabilities – making cybersecurity paramount. India is facing a whole spectrum of cyberthreats, from financial fraud and data breaches to advanced cyber-espionage campaigns.

B. Diverse Attack Techniques

With its vast population, India is a hotspot for cybercriminals employing phishing, ransomware, and social engineering tactics.

C. Targeted Sectors

Financial institutions, e-commerce platforms, and government entities are prime targets due to their sensitive data.

D. Ransomware Surge

A dramatic increase in ransomware incidents has led to significant business disruptions ranging from a few days to a few weeks.

IV. TIMELINE OF THE ATTACK

- **Late 2021:** Initial access likely gained via vulnerable VPN appliances(Pulse Secure/Cisco VPNs).
- **Mid 2022:** ShadowPad malware detected on SLDC networks; lateral movement observed.
- **2023-24:** Persistent activity linked to ChineseAPT groups; CERT-In and Recorded Future issue public alerts.

Date/Period	Incident/Action
Q4 2021	Initial network scanning and vulnerability exploitation.
Q1 2022	Access gained via outdated VPN servers.
Q3 2022	Malware (ShadowPad) deployed in at least 7 SLDCs.
2023–2024	C2 communications observed, suggesting ongoing surveillance rather than sabotage.

V. THREAT ACTOR PROFILE

Attribution:

The attack has been attributed to a PLA-affiliated threat actor, likely APT41 or a closely related group, Strongly linked to Chinese state sponsored group (likely APT 41 or RedEcho) based on:

* Use of ShadowPad(ShadowPad malware-a modular backdoor associated with PLA-linked groups)backdoor (previously linked to China).

*Infrastructure overlap with known Chinese C2 networks.

* Geopolitical timing aligned with Indo-China border tensions.

Objective: Long-term intelligence gathering and possibly pre-positioning for future grid disruptions

VI. TECHNICAL ANALYSIS OF THE INTRUSION

Stage | Activity
Reconnaissance | External scanning of SLDC systems, including exposed VPNs
Initial Access | Exploitation of CVE-2021-22937 (Pulse Secure VPN)
Payload Deployment | Side-loading of ShadowPad DLL files
Persistence | Scheduled tasks, registry modifications
C2 Communication | DNS tunneling to servers located in China.

Phase	Description
1.Reconnaissance	Scanning of SLDC IP ranges,identifying vulnerable VPN ports and legacy.
2.Initial Access	Exploitation of unpatched VPN gateway vulnerabilities(e.g.,CVE-2021-22937).
3.Malware Deployment	Installation of ShadowPad via DLL side-loading techniques.
4.Lateral Movement	Movement within internal SLDC networks, targeting SCADA communication modules.
5.Persistence & Exfiltration	Scheduled tasks and registry persistence; periodic communication with external C2 severs.

VII. CYBER FORENSIC INVESTIGATION

At the moment, there is no publicly available and exhaustive cyber forensic investigation report released by Indian National Technical Research Organization (NTRO) or Indian National Critical Information Infrastructure

Protection Centre (NCIIPC) in relation to the cyberattacks on Indian State Load Dispatch Centres (SLDC).

In early 2022, cybersecurity firm Recorded Future reported that a Chinese state-sponsored group, identified as TAG-38, targeted at least seven Indian SLDCs. These centres are responsible for real-time operations of the electrical grid, including Supervisory Control and Data Acquisition (SCADA) systems. The attackers employed ShadowPad malware, a modular backdoor linked to Chinese threat actors, to infiltrate these systems.

The attacks were characterized as espionage activities, aiming to gather information rather than cause immediate disruption. The focus on SLDCs, especially those near the disputed border with China, suggests a strategic intent to monitor critical infrastructure.

Methods Used:
- Packet Analysis (Wireshark) revealed encrypted traffic to known malicious IPs.
- Memory Forensics (Volatility) detected obfuscated malware payloads.
- Log Correlation across firewall, VPN, and endpoint systems confirmed timeline.

Indicators of Compromise (IOCs):
- Registry keys for persistence
- DLLs with altered hash values
- Reused C2 domains linked to earlier attacks on telecom and defense sectors

VIII.RESPONSE FROM INDIAN AUTHORITIES

In response to cyberattacks targeting SLDCs:

- The Indian Computer Emergency Response Team (CERT-In) has been engaged in tracking and responding to such threats, although actual details of their response here have not been made public. As well as they issued red alerts and mitigation advisories.

- The Ministry of Power mandated cyber audits and infrastructure segmentation.

- The National Critical Information Infrastructure Protection Centre (NCIIPC), tasked with protecting India's critical information infrastructure, has been proactive in enhancing cybersecurity across the power sector. Their initiatives were as follows:

~ Security Guidelines and Advisories

~ Threat Monitoring

~ Incident Response Coordination

~ Risk Management Frameworks

~ Technology Implementation

~ Security Audits

- Specific details about National Technical Research Organisation's (NTRO) actions concerning the SLDC cyberattacks are not publicly disclosed, the organization plays a crucial role in India's cyber defense strategy. The NTRO carries out technology intelligence duties and possesses the ability to take cyber defense steps, such as monitoring and analyzing cyber threats that arise as a danger to national security.

- NTRO and NCIIPC also conducted joint assessments.
- Enhanced monitoring of north India's critical SLDCs near the LAC (Line of Actual Control).

IX. STRATEGIC AND GEOPOLITICAL IMPLICATIONS

- Geopolitical: Likely tied to Indo-China tensions in border areas, the attack suggests China is using cyber espionage as a tool to monitor or prepare for potential conflict escalation, especially near the Ladakh border.
- Tactical: Demonstrates China's use of cyber tools for reconnaissance and signaling, Raises questions on India's readiness to protect Critical Information Infrastructure (CII).
- Risk: Prepositioned malware could be triggered in the future, risking blackouts or grid instability,Highlights asymmetry in offensive cyber capabilities between India and rival nations.

X. CHALLENGES AND GAPS

- Legacy and Vulnerable SCADA Systems
Many software development life cycles incorporate obsolete Supervisory Control and Data Acquisition (SCADA) software with poor authentication and patching.

-Lack of Network Segmentation
Operational Technology (OT) networks were sometimes not well-segregated from Information Technology (IT) networks.

- Low inter-agency threat sharing between DISCOMs and national security agencies

- Skill Gaps and Awareness
Staff at SLDCs often lacked specialized training in cybersecurity.

- Limited Detection Capabilities
There was a lack of real-time tracking or intrusion detection systems to detect threats at an early stage.

- Weak Threat Intelligence Sharing
There were some restrictions on the communication between national and central cybersecurity organizations such as CERT-In and NCIIPC and subnational security actors

XI. RECOMMENDATIONS

- Immediate isolation and security audits of all SLDC SCADA networks
- Mandating Zero Trust Architecture and frequent red team assessments
- Development of indigenous, secure SCADA alternatives
-Upgrade legacy SCADA systems with secure-by-design alternatives.
-Regular red-teaming exercises for critical utilities.
-Strengthen international cyber threat intelligence sharing.
-Establish a Cyber Warfare Command under the Defence Cyber Agency with specific focus on CII protection.

Lessons:

- Creation of a centralized Critical Infrastructure Cyber Operations Center (CICOC)
- Even non-kinetic cyber attacks can weaken national morale and expose systemic vulnerabilities.
- SLDCs and similar utilities often rely on outdated hardware/ software.
- Attribution is challenging but critical to inform diplomatic response.

XII. CONCLUSION

This case underscores the intersection of cyber warfare, national security, and critical infrastructure. The SLDC intrusions were not just IT incidents, this case shows the strategic leverage that cyber actors can gain through sustained reconnaissance and malware implantation in power infrastructure.The landscape of cybersecurity in India and the APAC region presents a complex mix of challenges and evolving threats. The adoption of advanced technologies like AI and ML, the increasing importance of cloud security, and the ever-present human factor, all underline the need for robust, proactive cybersecurity strategies. Organizations must stay ahead of these trends and continuously evolve their cybersecurity posture to safeguard their assets and maintain the trust of their stakeholders.The targeted cyber intrusions into Indian SLDCs mark a dangerous precedent in the militarization of cyberspace. India must now prioritize resilience and cyber deterrence to secure its national critical systems.India must now prioritize resilience and cyber deterrence to secure its national critical systems, must integrate cyber forensics, policy reform, and technological modernization to defend its digital borders.

XIII. REFERENCES

1. Recorded Future (2022–24). Targeting India's Power Sector.
2. CERT-In (2022–24). Advisories on APT Activity Targeting Power Grids.
3. FireEye Threat Intelligence Reports.
4. NCIIPC Guidelines for Critical Information Infrastructure and Energy Sector.
5. Media coverage: The Hindu, Economic Times, The Wire (Cybersecurity desk).
6. Ministry of Power Press Releases.
7. Kaspersky & FireEye Malware Analysis on ShadowPad
8.https://www.plctechnician.com/news-blog/scada-system-what-it-and-how-it-works
9.https://therecord.media/suspected-china-backed-hackers-target-7-indian-electricity-grid-centers
10.https://mperc.in/uploads/regulation_document/bb6c63d4fc113555437087fd2b84d173.pdf
11.https://www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html
12.https://www.sldcorissa.org.in/function.aspx
13.https://www.dpstele.com/scada/how-systems-work.php
14.https://economictimes.indiatimes.com/industry/energy/power/chinese-hackers-target-indian-power-grid-assets-in-ladakh/articleshow/90950986.cms?utm_source=chatgpt.com&from=mdr
15.https://www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html
16.https://www.kaspersky.co.in/blog/cybersecurity-landscape-india-2024/26836/
17.https://www.cybersecuritydive.com/news/china-backed-hackers-continue-cyberattacks-on-telecom-companies/740066/
18.https://therecord.media/suspected-china-backed-hackers-target-7-indian-electricity-grid-centers
19.https://www.upguard.com/blog/nciipc-explained?utm_source=chatgpt.com
20.https://www.recordedfuture.com/research/continued-targeting-of-indian-power-grid-assets?utm_source=chatgpt.com
21.https://therecord.media/suspected-china-backed-hackers-target-7-indian-electricity-grid-centers