TATA COMMUNICATIONS

TATA

QUARTERLY EXECUTIVE THREAT REPORT

APR - JUN' 25

TATA COMMUNICATIONS

Executive summary

April to June of 2025 saw a sharp escalation in cyber threats, marked by a rise in double extortion ransomware, zero-day exploitation, and state-sponsored espionage campaigns targeting critical infrastructure and cloud ecosystems. High-impact vulnerabilities in Microsoft, SAP, and SonicWall were actively weaponised, while geopolitical tensions fuelled targeted APT activity across Asia. Regulatory developments in India, the UK, and the US signal growing global pressure for cybersecurity accountability. Executives should prioritise behavioural threat detection, Zero Trust architecture, and proactive patch management to navigate this intensifying threat landscape.

A landscape of new threats - Quarterly highlights

"In April-June 2025, cyber-attacks per organisation increased by 47%, reaching an average of 1,925 weekly attacks, when compared to the previous quarter[1]"

As 2025 begins to unfold further, enterprises encountered a rapidly evolving cyber threat landscape marked by intensified ransomware campaigns, memory-resident malware, and geopolitically-driven espionage. Attacks by threat groups such as Agenda, Sarcoma, and IndoHaxSec demonstrated how both sophisticated actors and low-complexity hacktivists can disrupt operations across healthcare, education, government, and infrastructure sectors. Meanwhile, high-profile incidents like the Microsoft zero-day exploit wave and SAP NetWeaver compromise exposed critical weaknesses in enterprise software ecosystems, raising alarm over patching delays and major supply chain risks.

The increasing use of in-memory loaders, evasive backdoors, and credential theft underscores the need for real-time behavioural detection and cloud-native visibility. Nation-state operations-such as those conducted by SideCopy and Earth Ammit - further emphasised the urgency for Zero Trust policies and cross-sector threat intelligence sharing, particularly in today's tense global landscape and multiple global conflict zones across the world. As enterprises prepare for what lies ahead in 2025, building cyber resilience through adaptive defence, employee awareness, and strategic patch prioritisation is more essential than ever before.

What executives will find in this report:

1.	Top 10 threats and how to mitigate them
2.	State-sponsored espionage and geopolitical risks
3.	Ransomware trends: Double, triple & multi-extortion attacks
4.	Key government and regulatory developments
5.	Strategic guidance for executive decision-making
6.	Our top 5 cybersecurity recommendations

TATA COMMUNICATIONS

Adapting to an evolving threat ecosystem- Top ten threats of April-June 2025

Based on the insights gained from our threat intelligence research, some of the key threats identified in April-June 2025 are:

Transparent Tribe (APT36) cyber activities against India

Over the past quarter, Transparent Tribe (APT36), a Pakistan-linked APT group, has intensified cyber espionage against India's defense, government, and critical infrastructure. They use a new Golang-based DISGOMOJI malware, delivered via Google Drive, leveraging Google Cloud Platform for C2. This malware deploys CrimsonRAT, MeshAgent, and browser plugins, achieving persistence through .bashrc and systemd tampering. The group also exploits geopolitical themes and job recruitment for malware distribution via fake government websites and HTA payloads, demonstrating strong social engineering. Recent threat intelligence reveals APT36's expanding toolkit, including CapraRAT, Ares Python RAT, and Android spyware.

These campaigns highlight the urgent need for proactive monitoring, secure software practices, and heightened cyber vigilance across Indian government and military networks. To counter this, Indian organisations must adopt a nation-state-level cybersecurity posture, ideally through strict adherence to the policies of the Digital Personal Data Protection Act (DPDP Act) with aggressive network segmentation, EDR, and behavioural analytics. Security teams should deploy threat intelligence feeds tuned to TTPs, reinforce identity management, limit administrative access, and conduct red team exercises. Information sharing between sectors and CERT-IN is crucial.

Industries Impacted:	Oil & Gas, Railways, Defence, Government
Business Impact:	Espionage could lead to data compromise, geopolitical disruption, and reduced confidence in national infrastructure operations.
Severity:	High

IndoHaxSec: The rising Indonesian hacking collective targeting global organisations

A new hacking group, IndoHaxSec, emerged as a growing cyber threat, leveraging low-complexity attacks to breach organisations worldwide[2]. According to the latest threat intelligence, the Indonesia-based collective has claimed responsibility for multiple high-profile intrusions, including attacks on Australian universities, Indonesian government agencies, and a US-based cybersecurity firm. Unlike sophisticated state-sponsored actors, IndoHaxSec relies on exploiting known vulnerabilities, credential stuffing, and social engineering, tactics that highlight the risks of poor cyber hygiene. The group often boasts about its exploits on social media, suggesting a focus on notoriety rather than financial gain.

Security experts warn that IndoHaxSec's activities signal a broader trend of regional hacktivist groups gaining traction. Organisations are urged to patch vulnerabilities, enforce multi-factor authentication (MFA), and monitor for credential leaks to mitigate risks. As cyber threats evolve, proactive defence measures remain critical in countering emerging collectives like IndoHaxSec.

Industries Impacted:	Education, Government, Logistics
Business Impact:	Could lead to reputational damage, loss of public trust, and service disruption in academic and public-sector institutions.
Severity:	Medium

Escalation of hacktivist activity against Indian digital infrastructure

Between late April and June 2025, India experienced a significant surge in hacktivist cyber operations. Groups like Nation of Saviors and Dark Storm Team launched coordinated DDoS attacks, data breaches, and website defacements across telecom, government, education, healthcare, finance, and defence sectors. Post-Pahalgam terror attack, defacements intensified with symbolic messaging, and DDoS attacks targeted government and critical infrastructure. Dark Storm Team led high-impact, ideologically driven DDoS campaigns, demonstrating hacktivism's decentralised nature. Sustained incidents highlight Indian digital infrastructure vulnerabilities. To mitigate future disruptions, strengthening sector-specific cyber defences, improving public-private coordination, and enhancing monitoring of ideological threat actors are essential.

CERT-In recommends executives regularly update systems, patch vulnerabilities, and enforce strong MFA. Deploy WAFs, IDS, and log monitoring for early detection. Restrict user inputs, limit privileges, disable unused services, and maintain secure, tested backups for quick recovery against hacktivist-related attacks.

Industries Impacted:	Defence, Government, BFSI, Manufacturing, Telecom, Education, Healthcare
Business Impact:	Elevated risk of service outages, reputational harm, and exploitation of sector-specific vulnerabilities across critical Indian digital infrastructure.
Severity:	High

DarkWatchman and Sheriff Malware hit Russia and Ukraine

A large-scale phishing campaign has targeted Russian organisations across the financial, transportation, energy, and retail sectors, delivering DarkWatchman – an advanced, stealthy malware linked to the Hive0117 group[3]. DarkWatchman operates in memory, making detection difficult, and enables long-term espionage and credential harvesting. Meanwhile, in Ukraine, researchers uncovered "Sheriff," a modular backdoor with reconnaissance, persistence, and command-execution capabilities, underscoring growing cyber instability in the region.

To counter these threats, executives should leverage behaviour-based detection tools capable of identifying in-memory execution and post-exploitation tactics. Email security should include phishing-resistant authentication, attachment sandboxing, and link inspection. SOC teams should monitor for indicators of compromise, such as unusual registry changes, scheduled tasks, and persistence scripts. System hardening, including restricted PowerShell usage and logging, can help reduce risks. In high-risk regions, real-time threat intelligence and geo-fencing can help proactively block malicious infrastructure linked to ongoing campaigns.

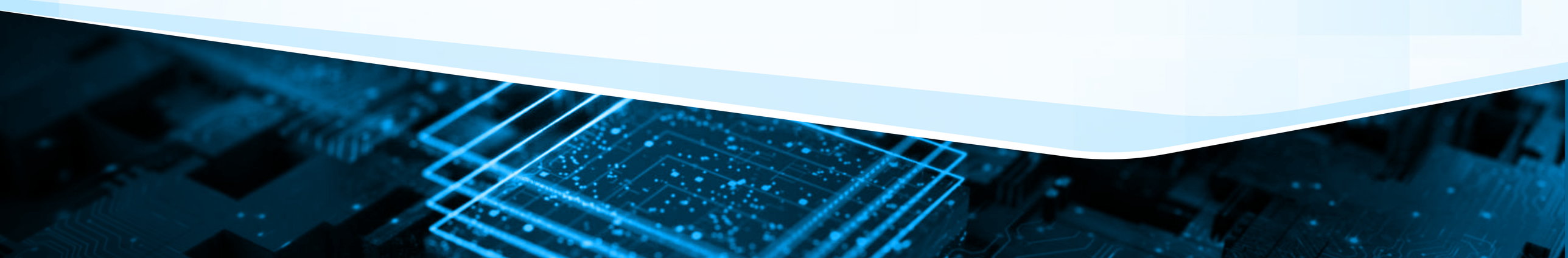
Industries Impacted:	Finance, Energy, Retail, Transportation
Business Impact:	Prolonged data theft or surveillance could result in operational disruption, exposure of sensitive assets, and potential financial compliance violations.
Severity:	High

Hacktivist activity surge in UAE

Between early May and June 1, 2025, ideologically driven hacktivist activity surged against UAE organisations. Coordinated DDoS attacks and website defacement campaigns targeted government, media, tourism, space, healthcare, advertising, and automotive sectors. DDoS attacks used botnets and proxy services, leveraging volumetric and application-layer techniques for maximum disruption, though short-lived. Defacement incidents exploited outdated web infrastructure and weak credentials to display political or religious messages, causing reputational harm without deeper compromise.

Executives must ensure they strengthen cyber defences with layered DDoS protection (WAF, rate limiting, cloud mitigation) and website security (patch management, MFA, vulnerability scanning, file integrity monitoring). Revisiting incident response protocols and public communication plans is essential. This highlights a tactical shift towards high-visibility disruption, underscoring preparedness needs in symbolically important sectors.

Industries Impacted:	Government, Defence, Military, Media, Tourism, Manufacturing
Business Impact:	Moderate to high risk of service disruption, reputational damage, and operational downtime across public-facing and symbolically significant sectors.
Severity:	High



Agenda ransomware evolves with NETXLOADER and SmokeLoader

The Agenda ransomware group has ramped up its operations with the introduction of SmokeLoader and a new, stealthy .NET-based loader called NETXLOADER[4]. These tools enable highly obfuscated, in-memory malware execution, making detection difficult and prolonging dwell time within networks. Targeting industries across India, Brazil, the US, and beyond, Agenda's campaigns focus on healthcare, finance, telecommunications, and IT sectors. Their evolving toolset reflects increasing sophistication and intent to evade even advanced security defences.

Executives should implement advanced behavioural analysis tools capable of detecting reflective DLL loading and in-memory execution. EDR/XDR platforms with script-blocking and real-time telemetry are essential. Network defenders should analyse lateral movement patterns, credential abuse, and unusual process trees. Blocking outbound connections to known malicious IPs and C2 infrastructure can help stop data exfiltration. Patch hygiene, strict access policies, and multi-factor authentication (MFA) reduce the initial attack surface. Backup systems must be segmented, versioned, and tested regularly for ransomware resilience. Businesses should also include agenda-specific IOCs in their threat-hunting activities.

Industries Impacted:	Healthcare, Finance, Telecommunications, IT
Business Impact:	Could lead to severe downtime, financial loss, and data exposure - particularly damaging in regulated and patient-facing industries.
Severity:	High

DragonForce ransomware cartel targets UK retail sector with a strategic shift toward high-impact victims

DragonForce, a Malaysia-linked RaaS cartel, escalated activities in Q2 2025, targeting major UK retailers. Attacks used social engineering and credential theft to infiltrate networks, exfiltrate data, and deploy ransomware, causing widespread outages. Their decentralised infrastructure enabled affiliates to target critical business systems, leading to payment, payroll, and inventory disruptions. Prolonged access to Active Directory allowed extensive lateral movement. Encryptors, based on LockBit/Conti code, crippled infrastructure, including VMware ESXi. DragonForce's multi-extortion model forced high-pressure ransom negotiations. This marks a strategic pivot to large, public-facing entities with low disruption tolerance.

Executives in the retail sector must adopt proactive, layered defenses. Strengthen identity controls with phishing-resistant MFA and privilege audits. Harden remote access via zero-trust gateways and strong authentication. Secure Active Directory with LSASS protection and EDR tools. Fortify endpoint defenses against unsigned drivers and suspicious processes. Ensure robust, immutable, offline backups and test recovery plans frequently. Segment networks to limit lateral movement and isolate critical systems.

Industries Impacted:	Retail
Business Impact:	High potential for operational paralysis, data leakage, and financial loss in large commercial enterprises due to prolonged infiltration and multi-extortion ransomware tactics.
Severity:	High

Sarcoma Group ransomware is an evolving new threat

Sarcoma Group ransomware is a highly disruptive threat that uses strong encryption to lock files and employs double extortion tactics by stealing sensitive data before demanding a ransom[5]. This approach increases pressure on victims by threatening public leaks. The malware typically infiltrates through phishing emails, unpatched software vulnerabilities, and poorly secured Remote Desktop Protocol (RDP) setups. Its broad targeting of organisations globally raises alarm for sectors that rely heavily on uninterrupted data access, such as healthcare, logistics, and education.

To defend against Sarcoma Group ransomware, organisations should implement a layered security approach. Strong email security gateways and user training are critical to reducing phishing success rates. RDP should be disabled if not essential or protected using VPNs and multi-factor authentication. Backup strategies must prioritise redundancy and isolation to avoid simultaneous encryption or deletion. Security teams should use ransomware-specific detection rules, monitor for suspicious data exfiltration, and develop response playbooks that include legal and PR considerations due to the data leak risk.

Industries Impacted:	Healthcare, Logistics, Education
Business Impact:	High potential for operational shutdown, regulatory fines for data breaches, and brand damage due to leaked sensitive records.
Severity:	High

Earth Ammit APT group targets East Asia's critical infrastructure

Earth Ammit, a Chinese-speaking APT group, has executed two interconnected campaigns - VENOM and TIDRONE - against critical infrastructure in Taiwan and South Korea[6]. The VENOM campaign used open-source tools to infiltrate upstream IT providers, while TIDRONE employed custom malware (CXCLNT and CLNTEND) for surveillance and data theft in the drone and military supply chain sectors. These long-term campaigns reflect advanced cyber-espionage tradecraft, including strategic targeting, layered persistence, and infrastructure manipulation.

To mitigate APT threats like Earth Ammit, critical infrastructure operators should implement zero-trust architecture and enforce network segmentation between supplier access points and operational technology (OT) systems. Email security, sandboxed attachment scanning, and DNS filtering can help disrupt initial infection attempts. Detection rules should be tuned to spot the use of dual-use tools and behaviour matching Earth Ammit's malware. Threat intelligence collaboration with national cybersecurity agencies is critical, especially when state-linked groups may be involved. Regular red-teaming exercises and audits of third-party integrations will further reduce supply chain risks.

Industries Impacted:	Aerospace & Defence, Government, IT Services
Business Impact:	Could result in intellectual property theft, disrupted R&D operations, and heightened geopolitical risk for supply chain-dependent firms.
Severity:	High

BianLian and RansomExx exploit SAP NetWeaver with PipeMagic Trojan

Multiple threat actors, including BianLian, RansomExx, and Chinese APTs, are exploiting CVE-2025-31324, a critical SAP NetWeaver vulnerability[7]. The attacks involve the deployment of sophisticated malware like PipeMagic and Brute Ratel, with some also chaining CVE-2025-42999. These attacks seize full system access, enabling data theft, lateral movement, and extortion through ransomware payloads. SAP environments are increasingly attractive to cybercriminals and nation-state actors alike due to their deep integration into enterprise operations.

Immediate patching of CVE-2025-31324 and the related vulnerabilities is essential. Organisations must apply vendor updates across SAP NetWeaver and closely monitor for signs of exploitation using SAP Enterprise Threat Detection (ETD) or SIEM integration. EDR and XDR tools should be configured to detect PipeMagic behaviour, DLL sideloading, and Brute Ratel signatures. Limiting administrative access, segmenting ERP systems, and deploying database activity monitoring will help limit exposure. Regular SAP security audits and threat hunting for persistence mechanisms can help detect existing compromises. Given the actors involved, enterprises should treat these threats as high-impact incidents with possible geopolitical implications.

Industries Impacted:	Manufacturing, Energy, Finance, Logistics
Business Impact:	High potential for financial disruption, operational downtime, and data integrity loss in core business systems.
Severity:	High

State-sponsored espionage fuelled by geopolitical conflict

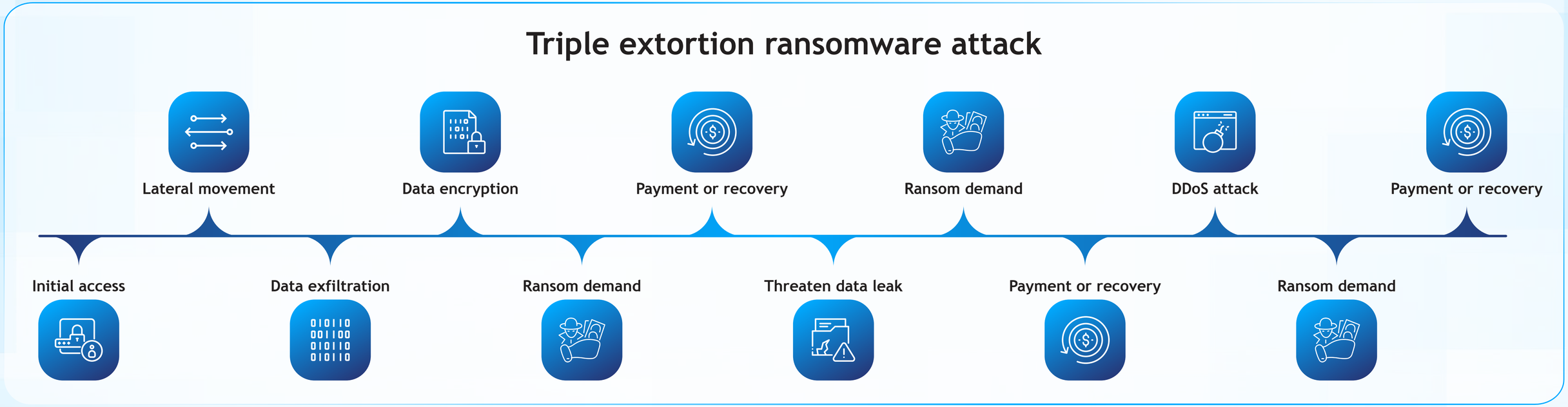
The April-June quarter of 2025 also saw a sharp escalation in state-sponsored cyber operations, driven by intensifying global tensions and ongoing geopolitical conflicts. APT groups such as SideCopy (linked to Pakistan) and Earth Ammit (linked to China) launched coordinated espionage campaigns targeting government agencies, defence supply chains, and critical civilian infrastructure in regions like India, Taiwan, and South Korea. These attacks were often aligned with military or diplomatic events, using cyber as a force multiplier to gather intelligence, sow instability, or signal political pressure. One major example of this is how, following Operation Sindoor in early May 2025, India faced massive cyberattacks from Pakistani and other allied state-sponsored hacktivists. Reports further indicate that **75% of all the claimed DDoS attacks** were directed at government organisations, with education (8.3%), finance (7.4%), manufacturing (6.5%), and telecom (6.5%) being the most prominent targets[8].

These actors used sophisticated tactics such as DLL sideloading, PowerShell-based decryption, spoofed infrastructure, and open-source tool abuse to evade detection and achieve long-term persistence. Campaigns like VENOM and TIDRONE infiltrated not just government networks, but also upstream IT providers and military-adjacent private sector organisations, demonstrating how the line between civilian and strategic infrastructure is becoming increasingly blurred. As conflicts in Asia and other hotspots persist, cyber warfare will remain a preferred theatre of engagement. To counter this, enterprises and governments must adopt Zero Trust frameworks, enhance supply chain security, and actively collaborate with national CERTs and intelligence partners to detect, attribute, and mitigate threats originating from adversarial states.

Ransomware trends: The rise of double, triple, and multi-extortion attacks

Ransomware threats have advanced significantly beyond traditional file encryption. From Q1 to Q2 of FY 2025, a clear shift toward multi-extortion tactics has emerged, with double and triple extortion now becoming standard operating models for leading ransomware groups. First emerging as a trend in 2019, this attack method is unfortunately the norm in today's digital ecosystem. In fact, research has found that in **96% of recent ransomware incident response cases,** attackers have also exfiltrated data to apply pressure to extort payment[9].

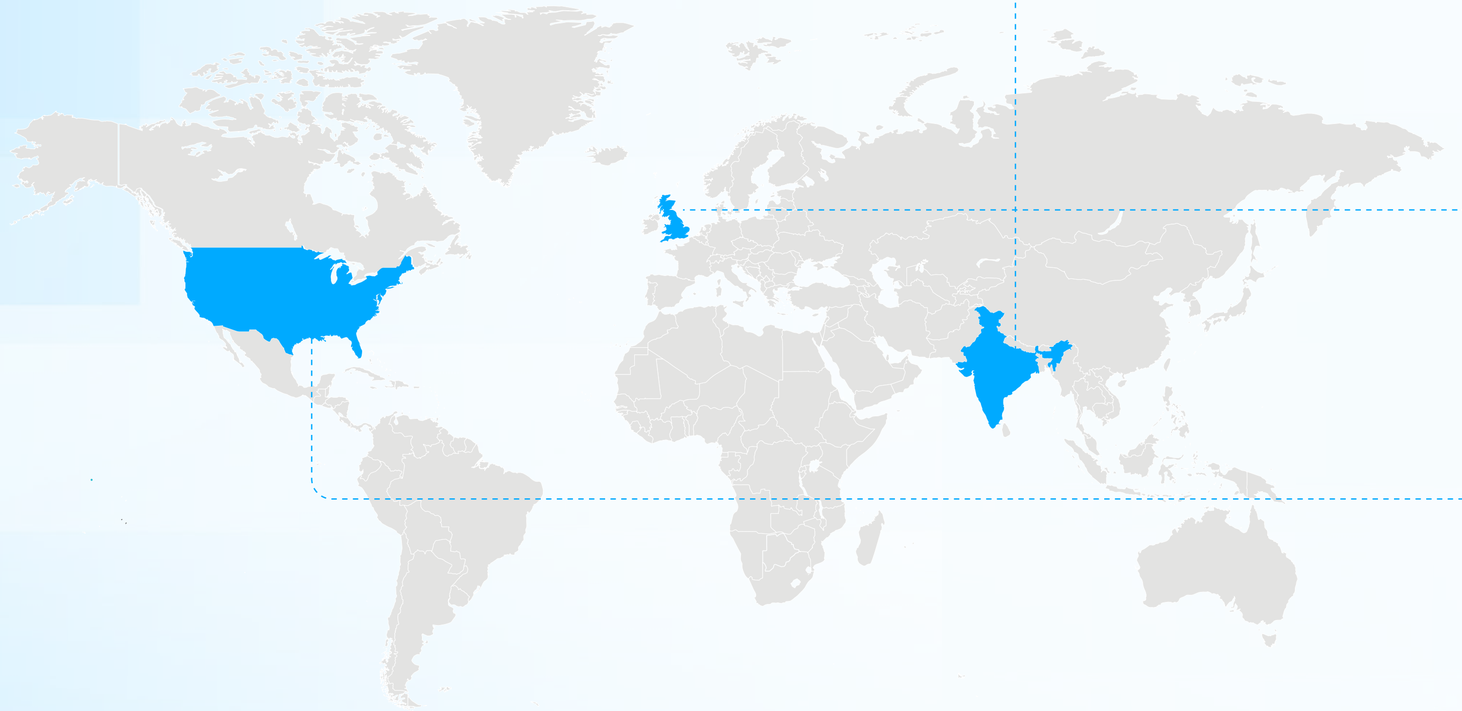
Double extortion, in particular, has overtaken simple encryption-based attacks. In this method, threat actors not only lock critical systems but also exfiltrate sensitive data, threatening public leaks or regulatory consequences if victims refuse to pay. This dual pressure significantly increases the stakes—enterprises face not only operational downtime but also reputational and legal fallout from data exposure. Some groups have even moved away from encryption entirely, using data theft alone as extortion leverage.



Building on this, triple extortion adds further complexity by introducing additional attack vectors—most notably DDoS attacks and third-party targeting. In such cases, attackers simultaneously disrupt online services while threatening to expose or contact clients, partners, or patients of the victim organisation. More aggressive multi-extortion campaigns can also involve tactics like short-selling threats against publicly traded companies or regulatory pressure simulations. These layered extortion strategies are designed to create maximum disruption and compel faster ransom payments. As threat actors increasingly adopt this playbook, executives must strengthen cyber hygiene, ensure robust backup and recovery plans, and implement coordinated defence strategies that include third-party risk management and communication protocols.

TATA COMMUNICATIONS

Important government cybersecurity advisories



INDIA

INDIA : On April 30, The Securities and Exchange Board of India (SEBI) has issued a critical update to its Cybersecurity and Cyber Resilience Framework (CSCRF) via circular SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2025/60[10]. This circular redefines cybersecurity compliance for SEBI-regulated entities (REs) based on risk, size, and operational exposure.

Executive Implication: May significantly impact compliance budgets and cybersecurity staffing requirements for BFSI firms in India.

UK

UK: Published on April 1, 2025, this bill outlines expanded regulations under the Network and Information Systems (NIS) directive, targeting improved security and resilience across critical sectors[11]. The bill sets legislative scope for combating ransomware and strengthening public service cyber defences.

Executive Implication: Public utilities, telecom, and healthcare operators should expect increased regulatory oversight and mandatory investment in resilience technologies.

USA

USA: As of April 2025, multiple states began their 2025 legislative sessions by introducing hundreds of new AI bills[12]. These bills include over a dozen regulations that have been passed and will seek to address algorithmic discrimination, AI-generated CSAM, intimate imagery, election-related content, generative AI chatbots, and digital replicas among other areas of concern.

Executive Implication: May increase legal exposure and compliance obligations for firms deploying AI tools in advertising, media, and fintech sectors.

TATA COMMUNICATIONS

TATA

Lessons from April-June 2025: 10 key takeaways for future resilience

Prioritise cyber hygiene to counter low-skill threat actors:

Even unsophisticated threat groups can cause major damage by exploiting weak credentials and unpatched systems. Organisations must enforce multi-factor authentication (MFA), conduct regular patching, and monitor for credential reuse. Establishing strong baseline cyber hygiene is essential to defend against rising hacktivism and opportunistic attackers.

Strengthen ransomware defences with in-memory threat visibility:

In-memory ransomware loaders require advanced telemetry and behavioural analytics. Organisations must implement script-blocking, reflective DLL detection, and lateral movement monitoring. Effective segmented backups and a tested ransomware playbook are critical to resilience and recovery.

Establish double extortion readiness plans:

With ransomware actors threatening to leak data, organisations must enforce robust email security, RDP hardening, and data exfiltration monitoring. Immutable, offline backups and legal/public relations response plans must be included in incident response strategies to manage extortion-based coercion.

Deploy behaviour-based detection for in-memory threats:

Stealthy, memory-resident malware bypasses signature-based antivirus. Enterprises should invest in EDR/XDR solutions capable of detecting post-exploitation behaviours, like PowerShell abuse and DLL tampering. In high-risk regions, geo-fencing and real-time threat intelligence help prevent advanced persistence mechanisms.

Secure network edge devices with strict patch governance:

Perimeter appliances are prime entry points. Enterprises must establish firmware patching protocols, restrict access to management interfaces, and regularly audit logs for anomalies. Tracking CISA's KEV catalogue ensures that vulnerability response is timely and prioritised.

Simulate nation-state APT campaigns with red teaming:

Persistent threat actors exploit human error and trust. Critical infrastructure operators must conduct red teaming, identity access management audits, and PowerShell usage controls. Coordination with CERT-IN and use of SideCopy-specific threat intelligence can boost sector-wide readiness.

Secure cloud infrastructure against supply chain exploits:

Cloud services must be treated as high-risk assets. Implement zero-trust models, multi-factor authentication for all cloud interfaces, and cloud workload protection platforms (CWPPs) to identify misuse. Organisations should rotate credentials regularly and monitor for known malicious IPs.

Secure ERP systems and monitor for advanced persistence:

ERP platforms like SAP are high-value targets. Apply SAP-specific threat detection (e.g., SAP ETD), monitor for PipeMagic and Brute Ratel signatures, and restrict administrative access. Database activity monitoring, segmentation, and frequent SAP security audits can prevent deep compromise.

Enforce OT-IT segmentation in critical infrastructure:

Cyber-espionage campaigns demand strategic defences. Operators must segment operational technology (OT) from supplier and IT systems, deploy sandboxed email scanning, and monitor for dual-use tool misuse. Red-teaming and third-party risk audits are essential in supply chain-heavy ecosystems.

Accelerate patch management for widely exploited vulnerabilities:

Patching must be proactive, not reactive. Enterprises need automated patch management systems, regular update audits, and prioritisation based on exploitability. Use sandboxing, application whitelisting, and Microsoft Defender ATP to block phishing and macro-based exploits targeting Office and Windows components.

Our top 5 recommendations

The dynamic nature of cybersecurity threats and their innovative vulnerabilities underscore the importance of a holistic approach to threat mitigation. By implementing these frameworks, enterprises can establish a robust, adaptive, and comprehensive cybersecurity framework to address current and emerging threats effectively. Tata Communications is committed to this all-encompassing approach to cybersecurity, and with the insights gained from April-June 2025's major cybersecurity incidents, they recommend five key recommendations that enterprises can imbibe:

Build threat visibility with behaviour-based detection and response:

Traditional antivirus solutions are no longer sufficient to counter modern threats like DarkWatchman, Sheriff, and Agenda ransomware, which operate in memory and use evasive tactics. Enterprises must deploy endpoint and extended detection and response (EDR/XDR) platforms that leverage behavioural analytics to identify suspicious activities such as script-based malware, credential theft, and lateral movement. Integrating telemetry from across endpoints, cloud, and network into a centralised SOC enhances threat visibility and enables rapid response.

Prioritise patch management and vulnerability intelligence:

With threat actors actively exploiting flaws in Microsoft, SonicWall, and SAP systems, enterprises must prioritise timely patching based on criticality and exploitability. Leveraging CISA's Known Exploited Vulnerabilities (KEV) list and maintaining accurate asset inventories are crucial to identifying and remediating high-risk systems. Automated patch management and frequent vulnerability scans ensure enterprises stay ahead of exploitation attempts in dynamic environments.

Foster cyber awareness, red teaming, and information sharing:

The rise of low-sophistication yet disruptive groups like IndoHaxSec proves that human factors remain a critical vulnerability. Enterprises should invest in continuous phishing awareness programs, simulate real-world attacks through red teaming, and assess employee and system readiness regularly. Active participation in threat intelligence sharing platforms, such as ISACs and national CERTs, promotes collective defence and early threat detection.

Secure identity, access, and cloud infrastructure:

State-sponsored campaigns like those by SideCopy and Earth Ammit, along with the Commvault Azure breach, highlight the growing threat posed by weak identity controls and cloud misconfigurations. Organisations must adopt Zero Trust Architecture, enforce multi-factor authentication across all accounts, and continuously monitor identity behaviours for anomalies. To strengthen resilience in hybrid environments, cloud workload protection platforms (CWPPs) should be deployed to enhance visibility and secure privileged access.

Harden ransomware resilience and backup strategies:

Ransomware groups such as Sarcoma and Agenda continue to evolve, using double extortion tactics and in-memory loaders to bypass traditional defences. Organisations must maintain segmented, immutable backups, test restoration procedures regularly, and ensure ransomware-specific detection rules are in place. Blocking outbound C2 communications and disabling unnecessary services like RDP further reduce the likelihood of successful ransomware deployment and data loss.

Sources: Tata Communications Threat Intelligence and Research
1.Checkpoint, 2.Arctic Wolf, 3.Habr, 4.Trend Micro, 5.The Medium, 6.Security Online, 7.The Hacker News, 8.Times of India, 9.Arctic Wolf, 10.Tax Management India, 11.National Cybersecurity Center , 12.Inside Global Tech