TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 21, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As April 2026 draws to a close, the cyber threat landscape is escalating, driven by increasingly sophisticated hostile activities. Traditional defence models are proving inadequate as adversaries exploit structural weaknesses across deeply interconnected digital ecosystems. To preserve resilience and strategic advantage, organisations must strengthen core security foundations, implement layered defences, and integrate anticipatory intelligence across their architectures.

In this high-stakes environment, the Tata Communications Cyber Threat Intelligence report becomes indispensable. Published weekly, the report delivers incisive analysis of emerging attack campaigns, evolving adversary tactics, and sector-specific exposures. By converting intelligence into immediate defensive action, security teams can anticipate, prepare for, and neutralise threats proactively to protect critical operations globally before disruption.

TATA COMMUNICATIONS

APT actors compromise OT communication ports via insecure internet exposure

Threat intelligence agencies have reported ongoing activity by Iranian-affiliated APT actors targeting internet-exposed operational technology environments, particularly Rockwell Automation and Allen-Bradley programmable logic controllers. The campaign focuses on critical infrastructure networks, where attackers exploit insecure configurations and direct internet connectivity to gain initial access using legitimate engineering software and commonly exposed OT communication ports.

Once inside, threat actors manipulate controller project files and alter HMI and SCADA data to disrupt industrial processes and degrade operational visibility. Observed techniques include the deployment of SSH tools for persistent remote access and lateral movement. The activity underscores systemic weaknesses in OT security postures, increasing the risk of operational disruption, financial loss, and potential safety impacts.

ATTACK TYPE	Cyber espionage	**SECTOR**	Waste disposal, Government, Energy
REGION	United States	**APPLICATION**	Siemens Simatic PLC, Siemens, Rockwell Automation

Source - https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

TATA COMMUNICATIONS

Emerging Space Bears deploys double extortion against mid-market enterprise targets

Space Bears is an emerging ransomware and data-extortion group first observed in April 2024, with links to the Phobos ransomware-as-a-service ecosystem. The group targets organisations by stealing sensitive data, encrypting systems, and demanding payment under threat of public disclosure via dark web leak sites, reinforcing a growing shift towards double-extortion-driven cybercrime models.

Despite relying on relatively unsophisticated techniques, Space Bears achieves impact through reputational pressure and strategic data exposure. Its corporate-styled leak platform amplifies coercion while targeting mid-sized organisations across sectors such as technology, healthcare, and manufacturing. This approach highlights how threat actors increasingly prioritise psychological leverage and operational scale over advanced malware development.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, IT, Transportation, Logistics
REGION	Singapore, Canada, Germany, Italy, Morocco, Norway, Spain, the United States	**APPLICATION**	Windows

Source - https://www.tripwire.com/state-of-security/space-bears-ransomware-what-you-need-know

TATA COMMUNICATIONS

LockBit-derived Brain Cipher integrates advanced stealth and propagation capabilities

Brain Cipher, a LockBit 3.0-derived ransomware strain active since mid-2024, continues to intensify global cyber extortion risks through double-extortion tactics combining data theft and file encryption. Derived from leaked builder code and showing overlap with BlackMatter tradecraft, it employs API hashing, anti-debugging, obfuscation, and lateral movement via GPO and PsExec to maximise operational disruption.

In a parallel phishing campaign, researchers have identified Cifrat, a newly discovered Android malware distributed through fake Booking.com update links. Victims are lured into installing a malicious APK that initiates a multi-stage infection chain, deploying an accessibility-enabled remote access trojan over WebSocket command channels for credential theft, SMS interception, screen surveillance, and full remote device control.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, IT, Government, Education, Telecommunications
REGION	Indonesia, Israel, Philippines, Portugal, South Africa, Thailand	**APPLICATION**	Windows

Source - https://www.group-ib.com/blog/brain-cipher-ransomware/

TATA COMMUNICATIONS

FortiGate flaw enables authentication bypass for persistence and lateral movement

Active exploitation of CVE-2025-59718 in FortiGate appliances has enabled attackers to bypass FortiCloud SSO authentication through crafted SAML responses, granting unauthorised administrative access to exposed systems. Investigations indicate adversaries rapidly accessed configuration files containing sensitive data, facilitating credential exposure and enabling further compromise of additional edge devices within targeted environments.

Following initial access, threat actors maintained persistence by creating rogue administrative accounts and modifying configurations, often enabling remote services to sustain access. Using valid credentials, they conducted internal reconnaissance, lateral movement, and credential harvesting, with activity frequently remaining undetected due to limited telemetry from edge devices, complicating incident response and delaying containment efforts.

ATTACK TYPE	Vulnerability, Breaches	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail, Telecommunications
REGION	Global	**APPLICATION**	Fortinet FortiGate, FortiSwitch Manager, FortiOS, FortiGate Firewall, Fortinet FortiGate SSL VPN, Fortinet FortiGate SSO Authentication

Source - https://www.rapid7.com/blog/post/ve-fortigate-cve-2025-59718-exploitation-incident-response-ir-findings/

TATA COMMUNICATIONS

RaaS KRYBIT ransomware targets Windows ESXi and NAS systems simultaneously

KRYBIT emerged as a ransomware-as-a-service group in 2026, reflecting the broader expansion of affiliate-driven cybercrime models that combine encryption with data exfiltration for double extortion. Such operations increasingly rely on Tor-based leak sites to amplify pressure on victims, particularly mid-sized organisations lacking mature detection and response capabilities.

The group gains initial access through phishing, compromised credentials and exposed services, before deploying cross-platform crypto-ransomware across Windows, ESXi and NAS environments. Leveraging tools such as data-stealing modules, attackers exfiltrate sensitive information prior to encryption, using leak site exposure and ransom demands to maximise coercion and sustain operational impact.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Education, Business
REGION	Japan, Austria, Botswana, Brazil, Mexico, Hong Kong	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://www.redpacketsecurity.com/krybit-ransomware-victim-bj-grupo/

Fileless STX RAT employs cryptographic C2 protocols for system compromise

Security researchers have identified STX RAT, a highly sophisticated remote access trojan engineered for stealth through fileless execution and multi-stage delivery chains. It deploys payloads directly in memory using scripted loaders and privilege escalation techniques, avoiding traditional detection.

The malware features a modular architecture supporting credential theft, remote control, and secondary payload delivery, alongside advanced encrypted command-and-control communications. It employs custom API resolution using hashed values to evade static analysis and reverse engineering, while strong cryptographic protocols ensure secure data exchange, reinforcing its resilience and operational persistence in compromised environments.

ATTACK TYPE	Malware	**SECTOR**	Financial services
REGION	Global	**APPLICATION**	Microsoft Edge, Mozilla Firefox, Windows, Google Chrome, FileZilla

Source - https://www.esentire.com/blog/stx-rat-a-new-rat-in-2026-with-infostealer-capabilities

TATA COMMUNICATIONS

Zero-Day (CVE-2026-34621) PDF attacks bypass Adobe Reader security features

Researchers have identified a sophisticated PDF-based exploit targeting Adobe Reader users, leveraging the zero-day vulnerability CVE-2026-34621 to execute malicious code upon opening specially crafted files. The flaw, actively exploited in the wild, enables attackers to trigger arbitrary code execution and conduct system fingerprinting, significantly increasing the risk of targeted compromise and data exposure.

The exploit facilitates communication with attacker-controlled command-and-control infrastructure to retrieve additional payloads, supporting multi-stage intrusion workflows. By dynamically profiling victims, threat actors can escalate attacks towards remote code execution and potential sandbox evasion, allowing deeper system access. Security advisories emphasise urgent patching, as no effective mitigations exist beyond updating affected Adobe Acrobat and Reader versions.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail, Telecommunications
REGION	Global	**APPLICATION**	Adobe Acrobat, Adobe Acrobat Reader

Source - https://www.hkcert.org/security-bulletin/adobe-acrobat-remote-code-execution-vulnerability_20260413

TATA COMMUNICATIONS

Critical Axios library flaw enables remote code execution and AWS credential theft

A critical vulnerability, CVE-2026-40175, has been identified in the widely used Axios HTTP client, exposing applications to a chained exploitation path stemming from prototype pollution in dependent libraries. The flaw enables attackers to inject malicious HTTP headers during request construction, facilitating request smuggling and server-side request forgery, thereby compromising internal services and cloud metadata endpoints.

The vulnerability arises from improper header sanitisation and unsafe configuration merging, allowing polluted properties to be inherited into outbound requests. This enables potential AWS IMDSv2 bypass, credential theft, and remote code execution under specific conditions. While patches have been released, the issue highlights systemic risks within software supply chains and the amplification of seemingly low-level flaws.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, Manufacturing, IT, Government, Transportation, Business, Aviation, Retail, Telecommunications
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, Axios

Source - https://securityonline.info/axios-vulnerability-cve-2026-40175-cloud-takeover-rce/

TATA COMMUNICATIONS

GlassWorm campaign uses Zig dropper to infect multiple developer IDE ecosystem

The GlassWorm campaign has evolved into a sophisticated supply chain threat, leveraging a trojanised OpenVSX extension masquerading as a legitimate developer tool to infiltrate environments. The extension deploys a Zig-compiled native binary that operates outside JavaScript sandbox restrictions, enabling full system-level access and silently initiating compromise across multiple integrated development environments on infected machines.

Once executed, the dropper scans for compatible IDEs and propagates malicious extensions across each instance, ensuring widespread persistence. A secondary payload is then deployed, enabling credential theft, remote access, and data exfiltration while communicating via blockchain-based command-and-control channels. This multi-stage, cross-IDE propagation significantly amplifies risks across developer ecosystems and software supply chains.

ATTACK TYPE	Vulnerability	**SECTOR**	IT
REGION	Global	**APPLICATION**	Microsoft Visual Studio, Windows, VS Code, GitHub

Source - https://www.aikido.dev/blog/glassworm-zig-dropper-infects-every-ide-on-your-machine

TATA COMMUNICATIONS

Unauthenticated attackers exploit React flaw to cause high-impact DoS attacks

A high-severity vulnerability, CVE-2026-23869, has been identified in React Server Components, enabling unauthenticated attackers to trigger denial-of-service (DoS) conditions through specially crafted HTTP requests. The flaw exploits unsafe deserialisation and uncontrolled resource consumption, allowing malicious payloads to exhaust CPU resources for extended periods, significantly degrading application performance and availability in affected environments.

The vulnerability impacts multiple server-side React packages and can be exploited remotely without authentication, increasing risk exposure for production deployments using server components. By targeting Server Function endpoints, attackers can repeatedly trigger resource exhaustion, potentially causing sustained service disruption. Security experts recommend immediate patching, strengthened input validation, and rate-limiting controls to mitigate exploitation risks.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, IT, Government, Transportation, BFSI, Business, Aviation, Manufacturing, Retail, Telecommunications
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, React

Source - https://cybersecuritynews.com/react-server-components-vulnerability-2/

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today's cyber threat landscape.

Book your visit