TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 5, 2026

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As May 2026 begins, the cyber threat landscape continues to intensify, driven by increasingly advanced and coordinated adversarial activities. Conventional defence models are struggling to keep pace with threat actors that exploit systemic vulnerabilities across highly interconnected digital environments. Sustaining resilience and competitive advantage now requires organisations to reinforce foundational security, adopt layered defence strategies, and embed forward-looking intelligence into their operational frameworks.

In this high-risk environment, the Tata Communications Cyber Threat Intelligence report serves as a critical resource. Issued weekly, it delivers incisive analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into actionable defence measures, security teams are better equipped to anticipate, respond to, and mitigate threats, ensuring continuity of critical operations at scale.

TATA COMMUNICATIONS

Harvester APT expands GoGra Linux backdoor via Microsoft Graph API for evasion

The Harvester APT group has expanded its espionage toolkit with a new Linux variant of the GoGra backdoor, marking a shift from earlier Windows-focused campaigns. The malware is delivered through socially engineered decoy files, often disguised as legitimate documents, and establishes persistence using systemd services and XDG autostart mechanisms to maintain long-term access within compromised environments.

A key feature of the malware is its abuse of Microsoft Graph API and Outlook mailboxes as covert command-and-control channels, allowing communications to blend with legitimate cloud traffic and evade detection. By leveraging trusted infrastructure and automated mailbox polling for instructions, the campaign demonstrates a growing trend of cloud-enabled espionage techniques designed for stealth, resilience, and cross-platform targeting.

ATTACK TYPE	Social engineering, Malware, Cyber-espionage, APT	**SECTOR**	Government
REGION	India, Afghanistan	**APPLICATION**	Microsoft Outlook, Linux, Microsoft Graph

Source - https://www.security.com/threat-intelligence/harvester-new-linux-backdoor-gogra

TATA COMMUNICATIONS

Pre-authentication SQL injection LiteLLM flaw exploited after public disclosure

A critical vulnerability, CVE-2026-42208, has been identified in LiteLLM, exposing its authentication workflow to pre-authentication SQL injection attacks. The flaw stems from improper handling of the Authorization header during API key verification, allowing unauthenticated attackers to execute arbitrary SQL queries against backend databases and access sensitive credentials without prior authentication.

Security researchers observed exploitation attempts within 36 hours of public disclosure, with attackers using targeted payloads to enumerate database structures and extract API keys, provider credentials, and configuration data. The vulnerability significantly elevates risk for exposed LiteLLM gateways, prompting urgent patching, credential rotation, and strengthened access controls to mitigate potential compromise and downstream cloud service abuse.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail, Telecommunications
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Lite LLM

Source - https://securityonline.info/litellm-sql-injection-exploited-in-the-wild-cve-2026-42208/

TATA COMMUNICATIONS

Android KYCShadow malware impersonates KYC processes to intercept financial data

KYCShadow is an advanced Android banking malware campaign delivered via WhatsApp messages masquerading as KYC verification requests, exploiting user trust in financial compliance processes. It functions as a multi-stage dropper, deploying a concealed payload that enables SMS interception, call monitoring, USSD execution, and WebView-based phishing to harvest sensitive financial credentials from infected devices.

The malware leverages Firebase-based command-and-control infrastructure alongside VPN-driven traffic interception and native code obfuscation to evade detection and maintain persistence. Stolen data, including OTPs, PINs, and card details, is encrypted before exfiltration. Researchers warn that its modular design and social engineering approach significantly increase success rates and pose sustained risks to mobile banking ecosystems.

ATTACK TYPE	Malware, Mobile	**SECTOR**	BFSI
REGION	India	**APPLICATION**	Android

Source - https://www.cyfirma.com/research/kycshadow-an-android-banking-malware-exploiting-fake-kyc-workflows-for-credential-and-otp-theft/

INTRODUCTION | GOGRA BACKDOOR TARGETS LINUX SYSTEMS THROUGH MICROSOFT GRAPH API ABUSE | CRITICAL SQL INJECTION VULNERABILITY IN LITELLM GATEWAY UNDER ACTIVE EXPLOITATION | FAKE KYC WORKFLOWS DEPLOY MALWARE, ENABLING SMS INTERCEPTION AND PHISHING | KYBER RANSOMWARE TARGETS ESXI AND WINDOWS SYSTEMS IN CROSS-PLATFORM THREATS | TRIGONA OPERATORS DEPLOY PURPOSE-BUILT TOOL FOR SELECTIVE DATA THEFT | LOTUSLITE BACKDOOR VARIANT EXPANDS TARGETING ACROSS FINANCIAL SECTORS | ORACLE ADDRESSES SECURITY RISKS ACROSS DATABASES AND MIDDLEWARE PLATFORMS | UAT-4356 FLAWS EXPLOITED TO DEPLOY FIRESTARTER BACKDOOR ON FIREWALL DEVICES | CROWDSTRIKE PATH TRAVERSAL FLAW PERMITS UNAUTHORISED SERVER FILE RETRIEVAL | ATTACKERS WEAPONISE GITHUB CI/CD WORKFLOWS TO DISTRIBUTE NPM PACKAGES

TATA COMMUNICATIONS

Kyber ransomware deploys coordinated attacks across Windows and ESXi platforms

Kyber is an emerging cross-platform ransomware threat targeting both Windows and VMware ESXi environments through coordinated dual-payload deployment. Identified during a March 2026 incident response, the malware leverages native administrative tools to encrypt data, terminate virtual machines, and disable recovery mechanisms, significantly increasing the risk of widespread operational disruption across enterprise infrastructure.

Technical analysis reveals distinct encryption approaches across platforms, with ESXi variants using ChaCha8 with RSA-based key wrapping, while Windows samples deploy AES-CTR combined with Kyber1024 encryption. Both variants share Tor-based command infrastructure and campaign identifiers, confirming unified operations. With over 900 ransomware incidents reported, researchers warn of escalating risks from coordinated, enterprise-wide attack strategies.

ATTACK TYPE	Ransomware	**SECTOR**	IT
REGION	Global	**APPLICATION**	VMware ESXi, Windows, Microsoft Hypervisor

Source - https://www.rapid7.com/blog/post/tr-kyber-ransomware-double-trouble-windows-esxi-attacks-explained/

TATA COMMUNICATIONS

Trigona ransomware affiliates deploy custom exfiltration tool for data theft

Recent threat intelligence indicates that Trigona ransomware affiliates have introduced a custom-built data exfiltration tool, marking a shift away from widely used utilities such as Rclone and MegaSync. Observed in March 2026 campaigns, the proprietary tool enables attackers to conduct faster and more controlled data theft while maintaining a lower detection profile during critical intrusion stages.

The tool supports parallel data transfers, TCP connection rotation, and selective file exfiltration, allowing attackers to optimise speed and evade network monitoring. Preceded by defence impairment through BYOVD techniques and credential harvesting tools such as Mimikatz, the activity highlights increasing attacker investment in customised tooling to enhance stealth, persistence, and operational efficiency in ransomware campaigns.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail, Telecommunications
REGION	Global	**APPLICATION**	AnyDesk, Windows

Source - https://www.security.com/threat-intelligence/trigona-exfiltration-custom

TATA COMMUNICATIONS

Mustang Panda deploys LOTUSLITE backdoor targeting financial and banking sector

A new variant of the LOTUSLITE backdoor, attributed with moderate confidence to Mustang Panda, is targeting banking and policy-focused entities through spear-phishing campaigns. Delivered via malicious CHM files and executed using DLL sideloading with a legitimate Microsoft-signed binary, the malware establishes covert persistence and communicates with dynamic, DNS-based command-and-control infrastructure over HTTPS.

Technical analysis indicates the implant retains core espionage functions, including remote shell access, file manipulation, and session control, while introducing enhanced evasion techniques and modular execution. Researchers note updated command structures, network signatures, and infrastructure reuse, highlighting ongoing development. The campaign reflects an expansion in targeting scope and a continued emphasis on stealth-driven, intelligence-gathering operations.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	Government, BFSI
REGION	India, Asia, South Korea, United States	**APPLICATION**	Windows

Source - https://www.acronis.com/en/tru/posts/same-packet-different-magic-mustang-panda-hits-indias-banking-sector-and-korea-geopolitics/

TATA COMMUNICATIONS

Oracle releases emergency CPU patches for authentication bypass flaws

Oracle's April 2026 Critical Patch Update introduces 481 security patches addressing 241 unique CVEs across 28 product families, including 34 critical vulnerabilities. A substantial number of these flaws are remotely exploitable without authentication, significantly increasing exposure risk across enterprise systems, particularly within Oracle Communications, middleware, and business application environments.

The update spans a wide range of enterprise technologies, including databases, ERP platforms, cloud services, and Java components, highlighting the breadth of potential attack surfaces. Security experts emphasise that delayed patch adoption could leave organisations vulnerable to exploitation, reinforcing the need for immediate remediation, robust vulnerability management, and continuous monitoring across Oracle-dependent infrastructures.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, BFSI, Construction, IT, Government, Transportation, Education, Business, Aviation, Automobile, Retail, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Oracle products

Source - https://www.oracle.com/security-alerts/cpuapr2026.html

INTRODUCTION | GOGRA BACKDOOR TARGETS LINUX SYSTEMS THROUGH MICROSOFT GRAPH API ABUSE | CRITICAL SQL INJECTION VULNERABILITY IN LITELLM GATEWAY UNDER ACTIVE EXPLOITATION | FAKE KYC WORKFLOWS DEPLOY MALWARE, ENABLING SMS INTERCEPTION AND PHISHING | KYBER RANSOMWARE TARGETS ESXI AND WINDOWS SYSTEMS IN CROSS-PLATFORM THREATS | TRIGONA OPERATORS DEPLOY PURPOSE-BUILT TOOL FOR SELECTIVE DATA THEFT | LOTUSLITE BACKDOOR VARIANT EXPANDS TARGETING ACROSS FINANCIAL SECTORS | ORACLE ADDRESSES SECURITY RISKS ACROSS DATABASES AND MIDDLEWARE PLATFORMS | UAT-4356 FLAWS EXPLOITED TO DEPLOY FIRESTARTER BACKDOOR ON FIREWALL DEVICES | CROWDSTRIKE PATH TRAVERSAL FLAW PERMITS UNAUTHORISED SERVER FILE RETRIEVAL | ATTACKERS WEAPONISE GITHUB CI/CD WORKFLOWS TO DISTRIBUTE NPM PACKAGES

TATA COMMUNICATIONS

FIRESTARTER backdoor targets Cisco Firepower FXOS through UAT-4356 exploitation

Ongoing activity attributed to UAT-4356 has been observed targeting Cisco Firepower devices, exploiting n-day vulnerabilities CVE-2025-20333 and CVE-2025-20362 to gain unauthorised access and deploy the FIRESTARTER backdoor. The malware enables remote control of compromised systems and is designed to persist even after patching or firmware updates, significantly increasing long-term intrusion risks.

Post-exploitation activity involves injecting shellcode into the LINA process and executing attacker-controlled payloads via crafted XML requests, demonstrating advanced tradecraft aligned with earlier ArcaneDoor campaigns. Researchers note that compromised devices may remain infected despite remediation efforts, requiring deeper forensic analysis and full system reimaging to effectively eradicate the threat and restore secure operations.

ATTACK TYPE	APT	**SECTOR**	IT, Government, Telecommunications
REGION	Global	**APPLICATION**	Cisco Adaptive Security Appliance (ASA), Cisco Firepower, Cisco FXOS

Source - https://blog.talosintelligence.com/uat-4356-firestarter/

TATA COMMUNICATIONS

Critical CrowdStrike LogScale flaw enables unauthenticated file access on servers

A critical vulnerability, CVE-2026-40050, has been identified in CrowdStrike LogScale, enabling unauthenticated attackers to exploit a path traversal flaw and read arbitrary files from affected servers. The issue resides in a cluster API endpoint and stems from missing authentication and improper path validation, exposing sensitive data such as configuration files, logs, and credentials.

The vulnerability affects specific self-hosted LogScale versions, while SaaS deployments have been mitigated through network-layer protections. Although no active exploitation has been observed, the ease of remote exploitation significantly elevates risk. Security experts strongly recommend immediate patching, restricting exposed endpoints, and strengthening access controls to prevent potential data exposure and compromise.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, BFSI, IT, Government, Business, Aviation, Automobile, Broadcast Media Production, Retail, Telecommunications, Logistics, Cryptocurrency
REGION	Global	**APPLICATION**	CrowdStrike

Source - https://cybersecuritynews.com/crowdstrike-logscale-vulnerability/

TATA COMMUNICATIONS

GitHub exploited to distribute compromised Bitwarden and Checkmarx packages

The Bitwarden CLI version 2026.4.0 was compromised as part of a broader supply chain attack linked to the Checkmarx campaign, where attackers tampered with a GitHub Actions workflow to inject malicious code into the npm distribution. The compromised package included a rogue file, enabling execution of a credential-stealing payload during installation without user interaction.

The payload targeted developer environments, harvesting sensitive data such as API tokens, cloud credentials, and CI/CD secrets, while enabling lateral propagation across repositories and automation pipelines. Researchers note the attack mirrors earlier incidents leveraging compromised build systems, underscoring systemic risks in software supply chains and the growing exposure of trusted development and deployment infrastructure.

ATTACK TYPE	Supply Chain	**SECTOR**	IT Services and Consulting
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, VS Code, Node Packager Manager (npm)

Source - https://socket.dev/blog/bitwarden-cli-compromised , https://socket.dev/blog/checkmarx-supply-chain-compromise

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