TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: NOVEMBER 25, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

The final quarter of 2025 has arrived, and with it, the most aggressive threat landscape enterprises have faced. Attacks are evolving at unprecedented scale and sophistication, exploiting systemic vulnerabilities across interconnected digital ecosystems and rendering conventional defences increasingly obsolete.

Tata Communications' weekly Cyber Threat Intelligence report delivers incisive analysis of emerging campaigns, evolving adversarial tactics, and sector-specific risks. By transforming intelligence into actionable defence, it empowers security teams to anticipate, prepare for, and neutralise threats proactively — safeguarding critical operations before disruption occurs.

SimpleHelp RMM flaws enable Medusa and DragonForce supply chain attacks

In early 2025, cyber investigations revealed that the ransomware groups Medusa and DragonForce exploited three critical vulnerabilities — CVE-2024-57726, CVE-2024-57727 and CVE-2024-57728 — in the SimpleHelp Remote Monitoring & Management (RMM) platform to infiltrate MSPs and their downstream clients. By gaining SYSTEM-level access via compromised third-party RMM servers, attackers deployed discovery tools, disabled defences and gained full network control.

Once inside the environment, the threat actors exfiltrated data using tools such as RClone (in the Medusa campaign) and Restic (in the DragonForce campaign) before encrypting systems en masse. These attacks highlight the severe risks presented by supply-chain dependencies and underline the urgency for MSPs and enterprises to ensure prompt patching, robust RMM hardening and rigorous vendor oversight to prevent similar intrusions.

ATTACK TYPE	Vulnerability, Ransomware	**SECTOR**	IT
REGION	UK	**APPLICATION**	Windows, SimpleHelp RMM

Source - https://zensec.co.uk/blog/how-rmm-abuse-fuelled-medusa-dragonforce-attacks/

TATA COMMUNICATIONS

Emerging ransomware BlackShrantac prioritises large-scale exfiltration for data theft

BlackShrantac, active since September 2025, is a data-extortion, double-extortion ransomware operation targeting mid-sized and enterprise organisations. The group gains access via phishing, supply-chain compromise, exposed RDP/VPN services and unpatched vulnerabilities, then uses PowerShell- and shell-based execution to steal large volumes of data before encryption. It pressures victims via Tor leak sites; unusually large outbound data transfers are a key indicator of compromise.

Organisations should prioritise rapid detection and response: monitor egress for abnormal transfers, segment networks, enforce multi-factor authentication for RDP/VPN, harden supply-chain security, and apply timely patches. Incident responders must preserve evidence of exfiltration and consider legal and regulatory obligations. Refer to CERT-In advisories for tailored mitigation and reporting procedures to manage data-extortion incidents effectively and notify stakeholders, including CISOs and boards.

ATTACK TYPE	Ransomware	**SECTOR**	Financial services, Manufacturing, IT, Government, Business
REGION	India, Mexico, Turkey, United Arab Emirates, United States	**APPLICATION**	Windows

Source - CERT-In

TATA COMMUNICATIONS

HelloKitty successor Kraken ransomware threatens Windows, Linux ESXi systems

Researchers have detected a marked uptick in big-game-hunting and double-extortion campaigns orchestrated by the Russian-speaking ransomware collective Kraken, believed to have emerged from the remnants of the HelloKitty cartel. In one case analysed by Cisco Talos, the group exploited exposed SMB vulnerabilities for initial access, then leveraged tools such as Cloudflared for persistent access and SSHFS to mount remote directories for extraction of sensitive data — all ahead of deployment of a bespoke encryptor across Windows, Linux and VMware ESXi platforms.

Once inside victim environments, Kraken conducts system-performance benchmarking to optimise encryption speed and evade detection, distinguishing itself from many traditional ransomware operations. Victim sets span multiple geographies—including the UK, US, Canada, Denmark, Kuwait and Panama—and ransom demands have reached approximately US $1 million paid in cryptocurrency.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Government
REGION	Canada, UK, Denmark, Kuwait, Panama, United States	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - CERT-In

TATA COMMUNICATIONS

Threat actor UNC6485 exploits Triofox flaw for global system compromise

Threat analysts have confirmed that the vulnerability CVE-2025-12480 in Triofox (versions before 16.7.10368.56560) enabled unauthenticated attackers to bypass access controls, reach initial setup pages and create new administrator accounts. The exploit chain involved manipulation of the HTTP Host header in the function CanRunCriticalPage(), labelled as improper access control and assigned a CVSS score of 9.1.

In one active campaign, threat actor UNC6485 exploited this gap from 24 August 2025 onwards to deploy remote-access tools via the built-in anti-virus feature. The attacker shifted from admin creation to arbitrary code execution, installing tunnelling utilities (SSH/Plink/Putty) and remote-desktop access. Organisations are urged to patch to version 16.7.10368.56560 and audit anti-virus paths, admin accounts and SSH traffic.

ATTACK TYPE	Vulnerability, Malware, Cyberespionage	**SECTOR**	IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	Generic, Gladinet

Source - https://cloud.google.com/blog/topics/threat-intelligence/triofox-vulnerability-cve-2025-12480/

TATA COMMUNICATIONS

Active exploitation of FortiWeb path traversal flaw enables stealth admin takeover

A critical path traversal vulnerability (CVE-2025-64446, CVSS 9.1) in Fortinet FortiWeb devices is being actively exploited by threat actors to create unauthorised administrator accounts on internet-exposed systems. Researchers observed crafted HTTP POST requests targeting the /api/v2.0/cmdb/system/admin%3f/../../../../../cgi-bin/fwbcgi endpoint, allowing malicious users to provision local privileged accounts without authentication.

The attacks have escalated globally, prompting Fortinet to issue a patch in FortiWeb 8.0.2 and urge organisations to update immediately if running version 8.0.1 or earlier. In parallel, security teams are advised to check for suspicious usernames (“Testpoint”, “trader1”, “trader”), review logs for fwbcgi path access, and monitor for activity originating from malicious IP ranges such as 107.152.41.19 and 185.192.70.0/24.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Finance, Manufacturing, IT, Government, Transportation, Education, E-Commerce, BFSI, Retail, Telecommunication
REGION	Global	**APPLICATION**	Fortinet FortiWeb WAF

Source - https://www.bleepingcomputer.com/news/security/fortiweb-flaw-with-public-poc-actively-exploited-to-create-admin-users/

TATA COMMUNICATIONS

Sophisticated UNK_SmudgedSerpent mimics think tanks to compromise experts

Between June and August 2025, threat researchers uncovered a previously unidentified espionage cluster dubbed UNK_SmudgedSerpent, which specifically targeted academics and foreign-policy experts. The actor leveraged seemingly harmless emails on themes such as Iran's domestic political reform and IRGC militarisation, spoofed think-tank figures, and used OnlyOffice and Microsoft Teams-style phishing to harvest credentials.

Once initial access was achieved, the group delivered a ZIP archive containing an MSI payload, which installed legitimate Remote Monitoring & Management (RMM) tools — PDQConnect and ISL Online — to maintain persistence. Although UNK_SmudgedSerpent's tactics overlap significantly with Iranian threat actors TA453 (Charming Kitten), TA455 (Smoke Sandstorm) and TA450 (MuddyWater), Proofpoint emphasises that firm attribution remains inconclusive.

ATTACK TYPE	Social engineering, Malware, Cyberespionage	**SECTOR**	Education
REGION	Iran, United States, South Asia, East Asia	**APPLICATION**	Microsoft Office 365, Microsoft Teams

Source - https://www.proofpoint.com/us/blog/threat-insight/crossed-wires-case-study-iranian-espionage-and-attribution

TATA COMMUNICATIONS

CHAMELEON#NET malware delivers FormBook RAT targeting enterprise systems

Researchers have uncovered a sophisticated multi-stage .NET malware campaign named CHAMELEON#NET, spread via malspam that delivers the DarkTortilla loader to eventually deploy the FormBook RAT. Initial access is gained through phishing emails directing victims to download a .BZ2 archive containing a heavily obfuscated JavaScript dropper, which unpacks further scripts and a VB.NET loader.

The VB.NET loader decrypts an embedded DLL using a custom index-based XOR cypher and then employs reflective loading, so the payload executes entirely in memory, avoiding any disk traces. The final FormBook RAT payload establishes persistence via registry keys and a startup folder, disables security defences, implements stealthy keylogging, and communicates with its command-and-control server through a DuckDNS domain.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Global	**APPLICATION**	Microsoft .NET Framework, Windows

Source - https://www.securonix.com/blog/chameleonnet-a-deep-dive-into-multi-stage-net-malware-leveraging-reflective-loading-and-custom-decryption-for-stealthy-operations/

MaaS Android RAT Fantasy Hub targets fake play pages and SMS handler

Security researchers have uncovered Fantasy Hub, a new Android Remote Access Trojan (RAT) sold as Malware-as-a-Service (MaaS) on Russian-language Telegram and crime-forum channels. The malware enables deep device compromise: it steals SMS messages, contacts, call logs, photos and videos, while also intercepting, responding to, and deleting incoming notifications to maintain stealth.

Delivered via a subscription bot, Fantasy Hub comes with builder/dropper tools and detailed malicious documentation — including video tutorials and guides to create fake Google Play pages and phishing overlays for Russian banking apps such as Alfa, PSB, T-Bank and Sberbank. It exploits Android's default SMS handler role to bypass MFA and uses native dropper techniques and WebRTC for live audio/video streaming, posing a serious risk to BYOD environments and mobile-first organisations.

ATTACK TYPE	Malware, Mobile	**SECTOR**	Financial services, BFSI
REGION	Global	**APPLICATION**	Android

Source - https://zimperium.com/blog/fantasy-hub-another-russian-based-rat-as-m-a-a-s

Kimsuky’s JavaScript espionage campaign targets financial institutions

Researchers have uncovered a new espionage campaign by the North Korean threat actor Kimsuky, employing a multi-stage JavaScript malware chain beginning with a loader named Themes.js. This initial script, which is not obfuscated, connects to a hostile server to retrieve further JavaScript payloads that gather system information, running processes, and files under the user directory.

In later stages, the malware establishes persistence by writing Themes.js into the %APPDATA%\Microsoft\Windows\Themes directory and registering a scheduled task named Windows Theme Manager to execute it every minute. The campaign also delivers a benign-looking Word document — likely a decoy — underlining Kimsuky’s sustained emphasis on stealthy intelligence gathering.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Government, Education
REGION	APAC	**APPLICATION**	Windows

Source - https://blog.pulsedive.com/dissecting-the-infection-chain-technical-analysis-of-the-kimsuky-javascript-dropper/

MastaStealer exploits LNK shortcuts for stealthy credential theft cartel

The recent campaign involving MastaStealer has been observed using spear-phishing emails that carry weaponised Windows LNK files, which then fetch a rogue MSI installer from a typosquatting domain. Researchers report that once executed, the installer drops a file masquerading as dwm.exe in a hidden directory and registers it as a command-and-control beacon. The campaign also modifies Windows Defender exclusions to evade detection and uses randomised domains for stealthy communication.

The infection enables credential theft, persistent endpoint compromise and financial fraud by harvesting sensitive data across systems, posing an elevated risk to enterprise networks. Indicators of compromise include MSI installation failures under non-privileged accounts (Event ID 11708) and unexpected Defender exclusion entries created via PowerShell. Security teams should monitor for these signs, restrict execution of LNK attachments and block downloads from suspicious domains to mitigate this evolving threat.

ATTACK TYPE	Malware	**SECTOR**	IT, Financial Services, Business
REGION	Global	**APPLICATION**	Microsoft SharePoint Server, Windows

Source - https://www.linkedin.com/feed/update/urn:li:activity:7394160502563590144/ , CERT-In

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