TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: November 4, 2025

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Organisations have witnessed an extraordinary rise in AI-driven social engineering campaigns, strategically orchestrated supply chain infiltrations, and increasingly advanced ransomware variants throughout FY25. As conventional security frameworks are demonstrably inadequate in the closing months of 2025, cyber adversaries continue their sophisticated operations with unwavering persistence. For organisations, maintaining cyber resilience means reinforcing the foundational security architecture while implementing holistic, intelligence-driven protection mechanisms that can predict and mitigate emerging risks.

Tata Communications' weekly threat intelligence briefings are purposefully designed to provide your security teams with the strategic advantage they need. Each bulletin delivers current threat assessments and practical guidance, empowering you to identify, triage, and address vulnerabilities before they can compromise your business continuity.

Threat actor TransparentTribe impersonates government services to harvest credential

TransparentTribe, a Pakistan-linked APT36, has launched a targeted spear-phishing campaign impersonating India’s NIC eMail Services, using typo-squatted lookalike domains and counterfeit login portals to harvest credentials from government recipients. Malicious messages deliver weaponised Office macros or archived payloads that unpack loaders masquerading as legitimate documents, increasing click-through risk among busy officials and enabling follow-on compromise of internal systems.

Analysis shows the operation deploys a Golang-built backdoor dubbed StealthServer with Windows and Linux variants, delivered via macro-laced Office files and .desktop loaders. The implant supports multiple C2 channels (TCP, HTTP, and WebSocket), implements anti-analysis obfuscation and persistence routines, and enables credential theft, remote command execution, and sustained data exfiltration from compromised hosts, raising significant espionage and long-term access concerns.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Healthcare, Manufacturing, Government, Defence Industry
REGION	India	APPLICATION	Windows, Linux, Microsoft Office 365

Source - https://gbhackers.com/nic-eemail-services/ | https://blog.xlab.qianxin.com/apt-stealthserver-cn/

APT36 revamps Linux tooling with DeskRAT targeting defence infrastructure

In a newly uncovered campaign, TransparentTribe (APT36) has launched a targeted phishing operation against Indian government and defence organisations, exploiting unrest linked to national protests. The attackers send ZIP archives masked as official communications, containing malicious DESKTOP files. When opened, these execute a Bash one-liner that downloads and decodes a Golang-based Remote Access Trojan (RAT) dubbed DeskRAT, while concurrently displaying a decoy PDF to the unsuspecting user.

Once deployed, DeskRAT connects to WebSocket-based command-and-control (C2) servers masquerading as “Advanced Client Monitoring & Management” tools, enabling real-time interaction with compromised hosts. The malware is tailored for BOSS Linux, a distribution used by Indian government entities, and employs multiple persistence mechanisms — including systemd services, cron jobs, autostart files, and .bashrc scripts. Intriguingly, the RAT’s code suggests LLM-assisted development, with uniform function names for evasion routines and dummy computations.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Government, Defence Industry
REGION	India	APPLICATION	Linux

Source - https://blog.sekoia.io/transparenttribe-targets-indian-military-organisations-with-deskrat/

INTRODUCTION

MULTI-PROTOCOL TRANSPARENTTRIBE DEPLOYED AGAINST OFFICIAL NETWORK SYSTEMS

GOVERNMENT DEFENCE NETWORKS FACE TARGETED TRANSPARENTTRIBE MALWARE CAMPAIGN

CROSS-PLATFORM QILIN RANSOMWARE CAMPAIGN EXPLOITS REMOTE MANAGEMENT TOOLS

MATURE INC RANSOMWARE OPERATION DEPLOYS CROSS-PLATFORM ENCRYPTION TOOLS

CWE-502 WINDOWS SERVER VULNERABILITY ENABLES REMOTE EXPLOITATION

ENTERPRISE SOFTWARE VENDOR FIXES CVE-2025 REMOTE UNAUTHENTICATED ATTACK VECTORS

CRITICAL TOOLSHELL ZERO-DAY VULNERABILITY ENABLES TELECOM ESPIONAGE OPERATIONS

LEETAGENT SPYWARE DEPLOYED THROUGH CHROME VULNERABILITY IN OPERATION FORUMTROLL

BANKING TROJAN GHOSTGRAB EXECUTES CREDENTIAL THEFT FOR CRYPTOCURRENCY MINING

ADVANCED ESPIONAGE CAMPAIGN DREAMJOB TARGETS AEROSPACE TECHNOLOGY SECRETS

Agenda ransomware evolves with Linux deployment and BYOVD techniques

The Qilin ransomware-as-a-service (RAS) operation (also known as Agenda) has developed a strikingly advanced hybrid attack approach: it now deploys a Linux-compiled payload on Windows hosts by exploiting legitimate remote management and file-transfer tools such as WinSCP and Splashtop Remote. Attackers also employ Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques to disable endpoint defences, harvest credentials from backup infrastructures such as Veeam Backup & Replication, and bypass traditional Windows-centric detection mechanisms.

Since January 2025, the group has hit 700-plus organisations in more than 60 countries, targeting high-value sectors such as manufacturing, technology, financial services, and healthcare. The attack chain typically begins with fake CAPTCHA-like lures hosted on cloud storage, proceeds via credential theft and lateral movement using built-in remote-management tools, then culminates in deployment of the Linux payload on Windows systems, enabling full encryption plus data exfiltration.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT Services
REGION	Global	**APPLICATION**	AnyDesk, VMWare ESXi, Windows, Linux, WinSCP, Veeam, AnyDesk, Veeam Backup Enterprise Manager

Source - https://www.trendmicro.com/en_us/research/25/j/agenda-ransomware-deploys-linux-variant-on-windows-systems.html
https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/

Sophisticated INC RaaS targeting healthcare with double extortion tactics

The mature ransomware-as-a-service operation driven by INC Ransomware continues to pose a serious threat to organisations in 2025. Having ranked among the most active groups, it leverages common but highly effective entry paths such as unpatched network appliances, exposed remote services, and weak credentials. Affiliates exploit these vulnerabilities in sectors with limited security resilience, particularly healthcare, and then move swiftly to infiltrate internal systems.

Once inside, INC's affiliates exploit proof-of-concept attacks, credential theft, and lateral movement tools to deploy multi-threaded Linux and Windows lockers. Victims face rapid file encryption and exfiltration followed by double extortion via a dedicated portal and public leak site. Ransom negotiations are formalised through a victim-specific portal, combining pressure and professionalism to maximise payment chances.

ATTACK TYPE	Ransomware	SECTOR	Healthcare, Financial services, Manufacturing, Government, BFSI
REGION	Russia, Armenia, Azerbaijan, Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Ukraine, Uzbekistan	APPLICATION	Citrix Access Gateway, Citrix NetScaler, Fortinet FortiClient SSL VPN, Fortinet FortiGate, Windows, Linux, FortiGate EMS/SPP

Source - https://www.morado.io/blog-posts/preventable-paths-how-inc-ransomware-continues-to-thrive

Critical WSUS RCE deserialisation flaw allows CVE remote code execution

The Cybersecurity and Infrastructure Security Agency (CISA) has formally added CVE-2025-59287, a critical remote-code-execution vulnerability in Windows Server Update Services (WSUS), to its Known Exploited Vulnerabilities (KEV) catalogue following reports of active exploitation. The flaw resides in the unsafe deserialisation of untrusted data (CWE-502) and enables unauthenticated attackers to execute arbitrary code with SYSTEM privileges on servers where the WSUS role is enabled.

With multiple proofs-of-concept released and evidence of attacks emerging, the urgency is clear. Microsoft Corporation issued an out-of-band (OOB) security update on 23 October 2025 to comprehensively address the vulnerability, after the initial October Patch Tuesday release proved incomplete. Organisations are urged to patch immediately or, if unable to do so promptly, disable the WSUS Server role or block inbound traffic on ports 8530/8531 as temporary countermeasures.

ATTACK TYPE	Vulnerability	SECTOR	Healthcare, Financial services, Manufacturing, IT, Government, Transportation, Education, Energy, E-Commerce, BFSI, Retailer and Distributor, Telecommunications
REGION	Global	APPLICATION	Windows, Windows Server Update Services (WSUS)

Source - https://www.bleepingcomputer.com/news/security/hackers-now-exploiting-critical-windows-server-wsus-flaw-in-attacks/
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Oracle October 2025 security update fixes multiple flaws across core products

The latest Oracle Critical Patch Update for October 2025 addresses 374 new vulnerabilities across a broad range of its product families, including Database, Fusion Middleware, Java SE, MySQL, PeopleSoft, Siebel, Retail, and more. Among the most serious are remote-exploitable, unauthenticated flaws such as CVE-2025-6965 (CVSS 9.8), CVE-2025-61757 (9.8), CVE-2024-52577 (9.8), and CVE-2024-52046 (9.8).

Within this update, Oracle highlights that multiple critical vulnerabilities allow attackers to gain remote access without authentication, often via HTTP or network vectors, and many stem from third-party components such as Apache Commons FileUpload. The advisory emphasises that customers should apply patches immediately and ensure they operate on supported product versions to reduce the risk of successful exploitation.

ATTACK TYPE	Vulnerability	SECTOR	Healthcare, Hospitality, Financial services, Manufacturing, IT, Government, Education, Energy, Defence Industry, E-Commerce, BFSI, Aviation, Retailer and Distributor, Telecommunications
REGION	Global	APPLICATION	Oracle

Source - https://www.oracle.com/security-alerts/cpuoct2025.html

State-sponsored group breaches Telecom networks via ToolShell flaw globally

Shortly after its public disclosure and patch in July 2025, the zero-day vulnerability CVE-2025-53770 — commonly referred to as "ToolShell"— was leveraged by China-based threat actors to breach a telecom company in the Middle East. Their campaign then spread quickly, compromising government departments in Africa and academic networks across South America and the U.S., with the attackers deploying advanced malware for persistence and espionage.

The threat actors deployed the backdoor Zingdoor via sideloaded legitimate binaries, alongside the RAT ShadowPad and loader KrustyLoader — techniques consistently attributed to Chinese-nexus groups such as Glowworm and UNC5221. The breadth of victim geography and tools used indicates a broad espionage objective, rather than a financially motivated campaign.

ATTACK TYPE	Vulnerability, Malware	SECTOR	Financial services, Government, Education, Telecommunications
REGION	USA, Middle East, Africa	APPLICATION	Microsoft SharePoint Server, Windows

Source - https://www.security.com/threat-intelligence/toolshell-china-zingdoor

Commercial LeetAgent spyware deployed via sandbox-escape flaw exploitation

In early 2025, cybersecurity researchers identified a sophisticated phishing campaign named Operation ForumTroll that exploited a previously unknown Chrome sandbox-escape vulnerability, CVE-2025-2783. The campaign relied on personalised spear-phishing links, which, once clicked, triggered the exploit in Chrome and allowed attackers to bypass sandbox protections and deploy espionage-grade malware. The targets spanned media, government, and academic organisations in Russia and Belarus, underscoring the operation’s geopolitical focus.

Further analysis revealed the malware toolkit at play included LeetAgent spyware — capable of key-logging, file-theft, and remote execution — and uncovered the presence of a hidden commercial spyware platform named Dante developed by Memento Labs (formerly Hacking Team). The linkage between the APT threat actor and this advanced surveillance toolkit highlights both the quality of the attack chain and the troubling evolution of commercial spyware use in state-aligned campaigns.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Financial services, Government, Education, Broadcast Media Production and Distribution
REGION	Russia, Belarus	APPLICATION	Google Chrome OS, Windows, Google Chrome

Source - https://securelist.com/forumtroll-apt-hacking-team-dante-spyware/117851/

GhostGrab Android malware executes financial fraud and resource exploitation

The Android malware family GhostGrab merges covert cryptocurrency mining with active financial data theft, according to a detailed analysis. It systematically harvests banking credentials, debit-card details, and one-time passwords via SMS interception, while simultaneously exploiting device resources to mine Monero in the background.

GhostGrab's sophisticated architecture leverages a Firebase-based command-and-control infrastructure alongside WebView-based phishing workflows to mimic legitimate banking interfaces. It hides its presence using persistent background services, hides the app icon, and requests high-risk permissions to ensure long-term operation and clandestine control. Security teams are urged to monitor domains such as kychelp[.]live and uasecurity[.]org and enforce stricter app-installation policies.

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

Source - https://www.cyfirma.com/research/ghostgrab-android-malware/

Cyber espionage group Lazarus compromises defence industry organisations

The campaign, branded by ESET as a fresh surge of the Operation DreamJob offensive, sees the North Korea-linked Lazarus Group targeting European defence and aerospace firms engaged in unmanned aerial vehicle (UAV) manufacture. Among several incidents in 2025, three companies in Central and Southeastern Europe were infiltrated using elaborate job-offer styled social-engineering baits, followed by trojanised open-source tools and payloads such as ScoringMathTea — a remote access tool (RAT) customised for persistent espionage.

The attackers' use of modules referenced internally as "DroneEXEHijackingLoader.dll" strongly signals UAV-themed intent. With at least one targeted firm contributing components to drones deployed in Ukraine, analysts infer that the Lazarus campaign was designed to extract manufacturing know-how and design data for UAVs — aligning with North Korea's growing investment in drone capabilities and its ambition to produce attack and reconnaissance platforms at scale.

ATTACK TYPE	Malware	**SECTOR**	Manufacturing, Aerospace, Defence Industry
REGION	Europe	**APPLICATION**	Notepad++, Windows

Source - https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/

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

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.