TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 19, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As May 2026 progresses, the cyber threat landscape continues to intensify, driven by increasingly advanced and coordinated adversarial activity. Conventional defence models are struggling to keep pace as threat actors 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

Iranian-nexus campaign exposes Omani government data via Open C2 server

Researchers uncovered an Iranian-linked cyberespionage operation targeting Oman's government after attackers accidentally exposed an open directory on a UAE-hosted VPS server. The intrusion affected at least 12 ministries, including the Ministry of Justice, where more than 26,000 citizen and judicial records were reportedly exfiltrated. Investigators identified exploitation of ProxyShell and DotNetNuke vulnerabilities alongside extensive credential harvesting activity.

Threat actors deployed ASPX webshells, privilege-escalation utilities, tunnelling frameworks, and multi-stage Python-based tooling to maintain persistent access across compromised environments. Analysis of the exposed infrastructure revealed command-and-control components, exploitation scripts, and stolen registry data, highlighting significant operational sophistication. Researchers warned that the campaign demonstrates continued targeting of government infrastructure through legacy vulnerabilities, stealth persistence, and coordinated espionage-focused intrusion techniques.

ATTACK TYPE	Cyber-espionage, APT	**SECTOR**	Legal services, Government
REGION	The Middle East, Europe, Asia, the United States	**APPLICATION**	Microsoft Exchange Server, Oracle Application Server, Fortinet, Spring Boot

Source - https://hunt.io/blog/iranian-nexus-oman-government-intrusion#Indicators_of_Compromise

TATA COMMUNICATIONS

CloudZ RAT exploits Microsoft phone link via Pheno plugin to intercept OTPs

Researchers have identified an active intrusion campaign involving the CloudZ remote access trojan and a newly discovered Pheno plugin that abuses Microsoft Phone Link to intercept synchronised mobile data from compromised Windows systems. Active since January 2026, the malware monitors Phone Link sessions and accesses locally stored SQLite database files containing SMS messages, call logs, and authentication notifications.

The campaign deploys CloudZ via a Rust-based loader, followed by a .NET payload that establishes encrypted command-and-control communications and enables modular plugin delivery. Researchers observed extensive evasion capabilities, including in-memory execution, sandbox detection, rotating user-agent strings, and anti-analysis checks. By targeting trusted PC-to-phone synchronisation channels, attackers can capture credentials and OTPs without compromising mobile devices directly.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Windows

Source - https://blog.talosintelligence.com/cloudz-pheno-infostealer/

TATA COMMUNICATIONS

Deceptive OpenClaw skill spreads GhostLoader and Remcos via AI pipelines

A malicious campaign identified in March 2026 weaponised the OpenClaw AI framework through a deceptive “DeepSeek-Claw” skill targeting autonomous AI agent workflows and developer environments. Researchers observed manipulated installation instructions triggering hidden payload execution, enabling attackers to abuse trusted binaries and sideload malicious components while bypassing conventional user interaction and signature-based security controls.

On Windows systems, the campaign deployed Remcos RAT via MSI-based DLL sideloading using a legitimate GoToMeeting executable, while Linux and macOS environments received GhostLoader through heavily obfuscated Node.js scripts. The malware employed ETW and AMSI patching, encrypted payload execution, credential harvesting, and covert persistence mechanisms to exfiltrate sensitive developer, cloud, and authentication data from compromised environments.

ATTACK TYPE	Supply Chain	**SECTOR**	IT
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Node.js, OpenClaw

Source - https://www.zscaler.com/blogs/security-research/malicious-openclaw-skill-distributes-remcos-rat-and-ghostloader

TATA COMMUNICATIONS

Analysts uncover MuddyWater intrusion disguised as Chaos ransomware attack

Researchers have identified a sophisticated intrusion campaign masquerading as a Chaos ransomware operation but assessed with moderate confidence to be linked to MuddyWater. The attackers used Microsoft Teams-based social engineering to impersonate IT support personnel, manipulate multi-factor authentication settings, and gain remote access through legitimate tools, including AnyDesk and DWAgent.

Rather than prioritising file encryption, the campaign focused on persistence, credential harvesting, and covert data exfiltration using a custom remote access trojan named Game.exe alongside remote management utilities. Investigators observed extensive abuse of trusted collaboration platforms and interactive screen-sharing sessions, reflecting a growing convergence between state-sponsored espionage activity and ransomware-style operational deception techniques.

ATTACK TYPE	Supply Chain	**SECTOR**	Manufacturing, Construction, Business
REGION	the Middle East, the United Arab Emirates, the United States	**APPLICATION**	AnyDesk, Windows, Microsoft Teams

Source - https://www.rapid7.com/blog/post/tr-muddying-tracks-state-sponsored-shadow-behind-chaos-ransomware/

TATA COMMUNICATIONS

Spear-phishing Silent Rotor operation compromises Eurasian unmanned aviation sector

Operation Silent Rotor is a highly targeted spear-phishing campaign directed at professionals within the Eurasian unmanned aviation sector, leveraging aviation-themed business documents linked to the “Unmanned Aviation 2026” forum to deliver a Rust-based malicious executable. The malware displays convincing decoy documents while silently fingerprinting compromised systems, collecting host, user, and network information for profiling and operational targeting.

Researchers observed the malware communicating with attacker-controlled infrastructure over encrypted HTTPS channels, exfiltrating collected data in JSON format before downloading and executing a second-stage payload. The campaign also employs obfuscation, staged payload delivery, and short-lived command-and-control infrastructure to reduce detection opportunities, reflecting increasingly stealth-focused tradecraft targeting aviation and aeronautical information ecosystems across multiple regions.

ATTACK TYPE	Phishing, Cyber-espionage	**SECTOR**	Aviation
REGION	Global	**APPLICATION**	Windows, Microsoft Office Documents, HTTPS, Rust Executable Files

Source - https://www.seqrite.com/blog/operation-silent-rotor-rust-malware-unmanned-aviation-sector/

TATA COMMUNICATIONS

GriefLure operation deploys modular RAT against Asian telecom and healthcare

Researchers have identified Operation GriefLure, a sophisticated spear-phishing campaign targeting organisations within the military telecommunications and healthcare sectors. Threat actors distributed malicious LNK files through nested archive attachments containing authentic legal and whistleblower-themed documents, increasing credibility and user interaction. The infection chain abused Windows ftp.exe utilities and DLL sideloading techniques to execute polymorphic payloads while evading conventional security monitoring.

The modular remote access trojan enabled credential theft, screenshot capture, process injection, and targeted file exfiltration from compromised environments. Researchers observed encrypted HTTPS-based command-and-control communications alongside persistence and stealth mechanisms designed to hinder forensic analysis. The campaign reflects increasing use of Living-off-the-Land techniques and socially engineered lures to support covert espionage, long-term access, and operational intelligence collection.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Military, Law, Telecommunications
REGION	Asia, Philippines, Vietnam	**APPLICATION**	ChromeOS, Windows, Google Chrome

Source - https://www.seqrite.com/blog/operation-grieflure-dissecting-an-apt-campaign-targeting-vietnams-military-telecom-philippine-healthcare/

TATA COMMUNICATIONS

Fake Claude AI delivers Donut loader and Beagle backdoor through DLL sideloading

Researchers have uncovered a sophisticated malvertising campaign leveraging a fake Claude AI website to distribute malware through DLL sideloading and a newly identified backdoor named Beagle. Victims downloading a trojanised MSI installer unknowingly execute a signed G DATA executable alongside a malicious DLL and encrypted payload files, enabling in-memory execution while maintaining the appearance of a legitimate installation process.

Analysis indicates the attack chain deploys Donut shellcode through AES-encrypted payload staging and establishes command-and-control communications over TCP and UDP protocols. Researchers observed infrastructure overlaps with PlugX-style delivery operations and AdaptixC2-related activity, highlighting increasingly sophisticated use of trusted software branding, stealth persistence, and evasive malware delivery techniques targeting developers and enterprise environments.

ATTACK TYPE	Phishing, Malware	**SECTOR**	Government, IT Services and Consulting
REGION	Russia	**APPLICATION**	Microsoft Windows Defender, Windows, Anthropic Claude Code

Source - https://www.seqrite.com/blog/operation-silent-rotor-rust-malware-unmanned-aviation-sector/

TATA COMMUNICATIONS

Android fixes wireless ADB authentication bypass, allowing remote code execution

A high-severity Android vulnerability, CVE-2026-0073, affects the wireless ADB authentication mechanism, enabling attackers on adjacent networks to bypass mutual TLS verification and execute arbitrary code without user interaction. The flaw stems from improper certificate validation within the adbd TLS authentication workflow, exposing devices where wireless debugging is enabled to stealthy remote compromise and persistent unauthorised access.

Security researchers warn that the vulnerability impacts multiple Android versions and significantly increases enterprise mobile exposure, particularly within development and testing environments relying on wireless ADB connectivity. Successful exploitation grants shell-level execution privileges, allowing attackers to deploy payloads, manipulate device functions, and potentially pivot across connected networks. Immediate patching and disabling unnecessary wireless debugging services are strongly recommended.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, BFSI, IT, Government, ONGC, Energy, Defence, Business, Aviation, Automobile, Retail, Telecommunications
REGION	Global	**APPLICATION**	Android

Source - https://www.hkcert.org/security-bulletin/android-remote-code-execution-vulnerability_20260505

TATA COMMUNICATIONS

Lazarus Group abuses Git pre-commit scripts to deliver InvisibleFerret malware

The Lazarus Group has expanded its Contagious Interview and TaskJacker operations by embedding malicious second-stage loaders within Git pre-commit hooks distributed through fake coding assessment repositories. Once developers clone the repositories, the hooks silently execute before commits occur, retrieving platform-specific payloads from attacker-controlled infrastructure and bypassing conventional detection through abuse of legitimate development workflows.

The campaign fingerprints operating systems to selectively deploy InvisibleFerret and BeaverTail malware variants capable of credential theft, cryptocurrency wallet compromise, and persistent remote access. Researchers observed the operation evolving beyond earlier npm and VS Code task abuse techniques, reflecting increasingly sophisticated supply chain tradecraft targeting software developers, cryptocurrency organisations, and enterprise development environments through highly convincing recruitment-themed social engineering activity.

ATTACK TYPE	Social engineering, Malware, Supply Chain	**SECTOR**	IT, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Apple macOS, Windows, GitHub

Source - https://opensourcemalware.com/blog/dprk-git-hooks-malware

TATA COMMUNICATIONS

Critical PAN-OS buffer overflow flaw actively exploited on internet-facing firewalls

A critical remote code execution vulnerability, CVE-2026-0300, has been identified in Palo Alto Networks PAN-OS, affecting the User-ID Authentication Portal service on PA-Series and VM-Series firewalls. The flaw stems from a buffer overflow condition that allows unauthenticated attackers to execute arbitrary code with root privileges through specially crafted network packets, without requiring user interaction or valid credentials.

Security researchers and vendor advisories confirm active exploitation targeting internet-exposed authentication portals, significantly elevating risk for organisations operating externally accessible PAN-OS environments. Successful exploitation enables complete firewall compromise, policy manipulation, and potential lateral movement across enterprise networks. Palo Alto Networks has urged immediate mitigation through portal restriction, trusted IP enforcement, and accelerated patch deployment to reduce exposure and prevent large-scale compromise.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, IT, Government, Military, Business, BFSI, Aviation, Automobile, Retail, Telecommunications
REGION	Global	**APPLICATION**	Palo Alto Networks GlobalProtect, Palo Alto Networks PAN-OS, Palo Alto

Source - https://www.hkcert.org/security-bulletin/palo-alto-pan-os-remote-code-execution-vulnerability_20260506

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