TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 28, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As April 2026 approaches its end, the cyber threat landscape continues to intensify, shaped by increasingly advanced and coordinated adversarial activities. 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 provides sharp analysis of emerging threat campaigns, shifting 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

Trojanised application disguised as AI upgrade delivers covert backdoor access

A malicious campaign has emerged leveraging a fake website impersonating Anthropic's Claude, distributing a trojanised "Pro" installer that appears legitimate to users. The installer deploys a PlugX remote access trojan using DLL sideloading via a signed G DATA executable, while simultaneously running the genuine application to avoid suspicion and maintain stealth.

The attack infrastructure demonstrates active management, including rotational email delivery systems and convincingly mimicked installation paths, enhancing credibility and persistence. Malware is deployed via startup folder entries, enabling continuous execution and rapid command-and-control communication. The campaign highlights growing risks associated with downloading AI tools from unverified sources and evolving social engineering techniques targeting developer ecosystems.

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

Source - https://www.malwarebytes.com/blog/scams/2026/04/fake-claude-site-installs-malware-that-gives-attackers-access-to-your-computer

TATA COMMUNICATIONS

Coordinated campaign combines credential abuse with destructive wiper deployment

CERT-In and threat intelligence reporting indicate that the Ababil of Minab campaign combines data exfiltration with destructive actions, with actors claiming access to enterprise and operational systems, alongside large-scale data theft and wiping capabilities. The operation demonstrates coordinated intrusion into virtualised infrastructure, web services, and potentially operational technology environments, amplifying risks beyond traditional IT compromise.

The campaign leverages Living-off-the-Land techniques, credential abuse, and lateral movement to evade detection while targeting critical systems including, CI/CD pipelines and recovery environments. By disrupting backup mechanisms and executing wiper activity post-exfiltration, attackers maximise operational impact and hinder remediation, reflecting an evolution towards hybrid campaigns combining espionage, disruption, and destructive cyber capabilities.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Healthcare, BFSI, IT, Government, Business
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux

Source - CERT-In Research

TATA COMMUNICATIONS

macOS infostealer campaign Phantom Claude leverages fake AI app for distribution

Operation Phantom Claude is an active macOS-focused infostealer campaign that impersonates Anthropic's Claude AI platform to deceive users into downloading malicious payloads. Threat actors employ fake domains, Cloudflare-backed infrastructure, and staged delivery mechanisms, including AppleScript loaders, to execute multi-stage infections while evading traditional security controls and maintaining persistence across compromised systems.

The campaign deploys stealer variants resembling Atomic and Poseidon families, targeting credentials, cryptocurrency wallets, and sensitive data from macOS devices. Its infrastructure supports encrypted command-and-control communication and dynamic payload delivery, reflecting a mature operational design. The activity highlights growing abuse of trusted AI ecosystems in social engineering campaigns to increase infection success rates and data exfiltration efficiency.

ATTACK TYPE	Malware	**SECTOR**	IT and Software Development
REGION	Global	**APPLICATION**	Apple macOS

Source - https://falconfeeds.io/blogs/operation-phantom-claude-macos-infostealer-anthropic-impersonation-campaign/

TATA COMMUNICATIONS

CISA flags actively exploited Microsoft vulnerabilities requiring immediate remediation

CISA has added two actively exploited vulnerabilities to its Known Exploited Vulnerabilities catalogue, signalling heightened risk for enterprise environments. The SharePoint Server flaw, CVE-2026-32201, stems from improper input validation and enables network-based spoofing, allowing attackers to impersonate trusted systems and potentially compromise authentication workflows.

Also included is CVE-2009-0238, a legacy Microsoft Excel vulnerability enabling remote code execution through crafted files, which continues to be exploited in unpatched or outdated systems. Its inclusion highlights persistent risks from legacy software, reinforcing the need for timely patching, asset visibility, and prioritised remediation aligned with actively exploited threats.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, Legal, Manufacturing, Entertainment, IT, Government, Education, Business, Aviation, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Microsoft Excel, Microsoft SharePoint Server, Windows, Microsoft Office 365

Source - https://www.cisa.gov/news-events/alerts/2026/04/14/cisa-adds-two-known-exploited-vulnerabilities-catalog

TATA COMMUNICATIONS

Microsoft releases patches for 169 vulnerabilities, including exploited zero-day

Microsoft's April 2026 Patch Tuesday release addresses approximately 167–169 vulnerabilities across its product ecosystem, including Windows, Office, Edge, Azure, SQL Server and Hyper-V. The update includes two zero-day flaws, one actively exploited and another publicly disclosed, underscoring heightened risk exposure and the urgency for organisations to prioritise remediation efforts.

The vulnerabilities span critical categories such as remote code execution, privilege escalation and security bypass, potentially enabling full system compromise, data manipulation and unauthorised access. Security experts highlight that several flaws affect widely deployed enterprise components, increasing the potential attack surface. Immediate patching, alongside continuous monitoring and vulnerability management, remains essential to mitigate exploitation risks effectively.

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

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2026-patch-tuesday-fixes-167-flaws-2-zero-days/

TATA COMMUNICATIONS

JanaWare Campaign leverages Adwind RAT targeting users via phishing lures

A cyber threat campaign leveraging a customised Adwind Java RAT has been identified delivering JanaWare ransomware through phishing emails containing malicious JAR files. The malware employs advanced obfuscation and polymorphic techniques to evade detection, while geofencing mechanisms restrict execution based on system locale and IP address, limiting visibility and targeting specific regional users.

Once executed, the RAT establishes remote access, enabling attackers to deploy the ransomware payload selectively after profiling victims. JanaWare encrypts files and communicates via Tor-based infrastructure, demanding relatively low ransom payments in a high-volume model. The campaign primarily impacts individuals and small to medium-sized businesses, reflecting a sustained, targeted and evasive threat operation.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Business
REGION	Turkey	**APPLICATION**	Microsoft Outlook, Java, Google Chrome, Google Drive

Source - https://www.acronis.com/en/tru/posts/new-janaware-ransomware-targets-turkey-via-adwind-rat/

TATA COMMUNICATIONS

ShadowByt3$ ransomware targets Linux and Windows with cross-platform encryption

ShadowByt3$ is an emerging ransomware-as-a-service operation that has gained attention despite relatively immature tradecraft and limited operational success. Active since late 2025, the group employs polymorphic ransomware builders alongside strong encryption standards, including AES-256-GCM/RSA-2048 on Linux systems, and ChaCha20 with ECIES on Windows, enabling payload variation and significantly reducing antivirus detection rates.

Analysis indicates that while the group has struggled with execution inconsistencies and low ransom conversions, its technical foundation remains credible. Ongoing affiliate recruitment efforts and exposed infrastructure suggest attempts to scale operations rapidly. Security researchers caution that continued refinement could enable ShadowByt3$ to evolve into a more coordinated and disruptive ransomware threat across enterprise environments.

ATTACK TYPE	Ransomware	**SECTOR**	Services, Education, Retail and Distribution
REGION	Global	**APPLICATION**	Windows, Linux

Source - https://barricadecyber.com/cti-report-shadowbyt3-ransomware-group/

TATA COMMUNICATIONS

RedSun POC release increases attack risks for unpatched Microsoft Defender systems

A proof-of-concept exploit dubbed “RedSun” has been publicly released for CVE-2026-33825, a high-severity privilege escalation vulnerability in Microsoft Defender. The flaw enables attackers to gain SYSTEM-level access by abusing Defender’s privileged operations, significantly elevating impact once initial access is achieved and increasing enterprise exposure following public disclosure.

The exploit’s release outside coordinated disclosure channels has accelerated potential weaponisation timelines, with security researchers warning of rapid adoption by threat actors. Additional exploit developments, including potential remote code execution variants, have been signalled, heightening urgency for immediate patching, continuous monitoring, and strengthened endpoint protection strategies to mitigate evolving attack scenarios.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, Pharmaceuticals, Construction, IT, Government, Education, E-Commerce, BFSI, Aviation, Automobile, Logistics
REGION	Global	**APPLICATION**	Microsoft Windows Defender

Source - https://gbhackers.com/poc-microsoft-defender-0-day-flaw/

TATA COMMUNICATIONS

Payouts King ransomware uses vishing and spam bombing tactics for active evasion

Payouts King ransomware, attributed to former BlackBasta affiliates, has emerged as a highly adaptive threat leveraging established social engineering techniques, including spam bombing, vishing, and abuse of legitimate tools such as Microsoft Teams and Quick Assist to gain initial access. These methods enable attackers to impersonate IT personnel and deploy malware while evading user suspicion.

Once deployed, the malware employs strong RSA-4096 and AES-256 encryption alongside advanced obfuscation, direct system calls, and process termination to bypass endpoint defences. It establishes persistence through scheduled tasks and selectively encrypts files to maximise impact while accelerating execution, reflecting a shift towards efficient, stealth-driven ransomware operations focused on data theft and disruption.

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

Source - https://www.zscaler.com/blogs/security-research/payouts-king-takes-aim-ransomware-throne

TATA COMMUNICATIONS

ZionSiphon malware targets water infrastructure with ICS sabotage capabilities

ZionSiphon is an emerging operational technology malware targeting water treatment and desalination systems, combining traditional intrusion techniques with ICS-specific sabotage logic. It employs privilege escalation, persistence, and USB-based propagation, while scanning industrial networks for protocols such as Modbus and S7comm to identify control systems and manipulate operational parameters.

Designed to alter chlorine dosing and hydraulic pressure, the malware demonstrates a clear intent to cause physical disruption. Although a logic flaw currently prevents execution, researchers warn that its modular architecture could enable future functional variants, signalling an escalation towards cyber-physical threats where digital compromise directly impacts critical infrastructure operations and public safety.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Manufacturing, Energy, Renewable Energy
REGION	Israel	**APPLICATION**	Windows

Source - https://www.bleepingcomputer.com/news/security/zionsiphon-malware-designed-to-sabotage-water-treatment-systems/

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