TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 7, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As July 2026 begins, the cyber threat landscape shows no sign of easing, as threat actors deploy ever more sophisticated and coordinated tactics across highly interconnected digital environments. Traditional defence models are being tested as adversaries exploit systemic weaknesses at scale. To sustain resilience and competitive advantage, organisations must strengthen foundational security controls, adopt layered defence strategies, and embed forward-looking intelligence throughout their operational frameworks.

Against this backdrop, the Tata Communications Cyber Threat Intelligence report remains an essential resource for security practitioners. Issued weekly, it offers incisive analysis of emerging threat campaigns, shifting attacker methodologies, and sector-specific risk exposures. Turning intelligence into actionable defence guidance enables security teams to anticipate, respond to, and mitigate threats effectively, safeguarding the continuity of critical operations at scale.

TATA COMMUNICATIONS

Tax-themed DragonReturn campaign deploys multi-stage DcRAT to target taxpayers

First observed on 18 May 2026 and still active in mid-June, the campaign exploits the AY2026-27 filing season by cloning a legitimate government utility filename, making the malicious file exceptionally difficult to distinguish from the genuine one. The lure impersonates an official memorandum, citing real sections of the Income Tax Act and a fabricated reference number to lend credibility.

The attack chain conceals a secondary payload within an image file named background.jpg, from which encrypted DcRAT components are extracted. The malware disables AMSI scanning, loads a .NET assembly directly into memory for fileless execution, and establishes persistence via a Windows service disguised as a Mixed Reality component, communicating over encrypted TLS channels throughout.

ATTACK TYPE	Malware	**SECTOR**	Government, BFSI
REGION	India	**APPLICATION**	Windows

Source - https://www.seqrite.com/blog/operation-dragonreturn-china-nexus-cyber-espionage-campaign-targeting-govt-of-india-mof-tax-infrastructure-via-multi-stage-dcrat-deployment/

TATA COMMUNICATIONS

Microsoft disrupts StealC and Amadey malware driving credential theft and intrusions

Microsoft's Digital Crimes Unit, working with Europol and industry partners, announced a coordinated disruption resulting in the takedown, suspension, and blocking of domains and command-and-control servers underpinning StealC and Amadey infrastructure. In total, the unit identified over 200 malicious Amadey and StealC command-and-control domains and IP addresses, moving to shut them down through court orders and seizures.

StealC operates as a malware-as-a-service infostealer, collecting sensitive data from browsers, cryptocurrency wallets, messaging applications, email clients, and gaming platforms via a centralised web panel. Amadey functions as a loader used to deliver StealC and other malware. These modular, pay-as-you-go models allow threat actors to escalate a single initial infection into multiple downstream threats.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Manufacturing, Education, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Edge, Microsoft Outlook, Mozilla Firefox, Mozilla Thunderbird, Windows

Source - https://www.microsoft.com/en-us/security/blog/2026/06/24/stealc-and-amadey-breaking-down-infostealers-and-the-cybercrime-services-that-deliver-them/

TATA COMMUNICATIONS

Fraudulent tax notice weaponises government branding to deploy stealthy RAT malware

The fraudulent portal closely mimics official government communications, using legal references, financial penalties, and compliance instructions to create a sense of urgency. Victims who interact with the notice are prompted to download a ZIP archive disguised as official assessment documentation, which reveals a disk image file functioning as a container for the actual malicious payload.

Tax_Assessment.exe operates as a loader, invoking libsvcs.dll via .NET reflection to transfer execution dynamically, whilst both binaries are obfuscated with ConfuserEx to complicate analysis. The DLL carries full RAT capabilities, including startup registration, scheduled task creation, system reconnaissance, and encrypted communication, with behaviour closely matching the XWorm family favoured by financially motivated actors.

ATTACK TYPE	Phishing, Malware	**SECTOR**	Financial services, Government
REGION	India	**APPLICATION**	Windows

Source - https://www.cyfirma.com/research/an-income-tax-assessment-notice-phishing-campaign-delivering-malware/

TATA COMMUNICATIONS

WhatsApp VBScript campaign uses fake business documents to seize victim systems

The attacks begin with messages sent from compromised accounts containing nothing but a heavily obfuscated VBScript file, disguised as financial reports, billing statements, or account notices to draw the target's attention. Filenames are localised in multiple languages, confirming the campaign's global reach across markets including India, the UK, Brazil, Singapore, Spain, and Australia.

Once the victim opens the file on Windows, the VBScript fetches two additional scripts that disable User Account Control protections through Registry modifications, then downloads a ZIP archive containing ManageEngine Endpoint Central. The software installs silently in the background, configured to connect to attacker-controlled servers and grant them remote administrative access to the compromised machine.

ATTACK TYPE	Malware	**SECTOR**	Financial services
REGION	Australia, Singapore, Russia, India, UK, Brazil, Malaysia, Mexico, Spain, Taiwan, Vietnam	**APPLICATION**	Windows, Zoho ManageEngine, WhatsApp

Source - https://www.bleepingcomputer.com/news/security/whatsapp-phishing-attack-uses-fake-business-docs-to-hack-pcs/

TATA COMMUNICATIONS

Payouts King ransomware affiliate deploys Edgecution through fake Outlook updates

The intrusion chain begins with targeted social engineering, typically via Microsoft Teams messages impersonating corporate IT personnel and directing victims to a convincingly forged Outlook Updates Management Console. That lure offers multiple deployment vectors, including an obfuscated AutoHotkey script, encrypted archive downloads, and clipboard-pasted batch or PowerShell scripts, which schedule a hidden, headless Edge instance loading the malicious extension.

Edgecution comprises two primary components: a browser extension that beacons to a command-and-control server over WebSockets, and a Python backdoor acting as the native host. By abusing the Chrome native messaging protocol, the extension relays privileged commands the browser cannot execute, enabling system information collection, arbitrary Python execution, file writing, process launching, and PowerShell.

ATTACK TYPE	Ransomware	**SECTOR**	IT Services and Consulting
REGION	Global	**APPLICATION**	Microsoft Edge, Microsoft Outlook, Python, Microsoft Office 365, Microsoft Teams, PowerShell

Source - https://gbhackers.com/payouts-king-initial-access-broker/

TATA COMMUNICATIONS

Coinbase Cartel emerges as a rebranded extortion group leveraging access broker networks

Intrinsec assesses with high confidence that Coinbase Cartel is a rebrand of a short-lived operation named DataVault, which claimed a modus operandi of stealing data using valid access acquired through strategic partnerships. The group may not directly perform technical intrusions, instead seeking to monetise data stolen by other threat actors and to buy valid accesses in bulk.

The threat actor g77 was the main user promoting Coinbase Cartel inside cybercrime forums, and is known to collaborate with others to buy valid access, test malware, and send phishing. Few discriminant indicators were identified, consistent with an operation that performs no encryption and steals data purely within a simple extortion scheme.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, IT, Transportation, Real Estate, Retail and Distribution, Software Development, Logistics and Shipping
REGION	France, Peru, United Arab Emirates, United States	**APPLICATION**	Apple macOS, Windows, Linux

Source - https://www.intrinsec.com/coinbase-cartel-behind-the-noise-of-a-prolific-leak-operation/

TATA COMMUNICATIONS

Actively exploited Cisco Unified CM flaw added to the federal known-flaws catalogue

Cisco announced patches for CVE-2026-20230 on 3 June, warning that an unauthenticated remote attacker could conduct SSRF attacks, write arbitrary files to the underlying operating system, and escalate privileges to root. Exploitation requires the WebDialer service, which is disabled by default; organisations running exposed appliances with the service enabled should assume potential exposure and prioritise immediate remediation.

Threat intelligence firm Defused observed exploitation over the weekend of 21 to 22 June, with attacks originating from a single source using properly constructed file-write payloads landing on decoy systems. Subsequent campaigns featured highly automated mass scanning routed through Tor exit nodes, deploying webshells against internet-exposed appliances before CISA mandated federal remediation by 28 June.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Cisco Unified Call Manager, Cisco Web Manager, Cisco Unified Communications Manager

Source - https://securityonline.info/cisco-unified-cm-rce-cve-2026-20230/

TATA COMMUNICATIONS

Backdoor.Mistic grants access brokers durable covert footholds for ransomware affiliates

Mistic was side-loaded through MpExtMs.exe, a legitimate file, and loaded from a DLL named EndpointDlp.dll, a name associated with Microsoft endpoint-security tooling, helping the backdoor blend in with trusted software. It runs payloads in memory with no file written to disk and includes a kill switch enabling self-deletion, features consistent with an operator pursuing long-term, low-visibility access.

Woodgnat functions primarily as an initial access broker, aiming not to deliver the final payload but to establish durable remote access and sell it to ransomware affiliates for a fee. The broker has been publicly linked to Qilin, Interlock, Rhysida, Akira, 8Base, and Black Basta, underscoring the growing role of custom malware in monetising enterprise intrusions.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	Education, BFSI, IT Services and Consulting
REGION	Global	**APPLICATION**	Python, Windows

Source - https://www.security.com/threat-intelligence/new-mistic-backdoor-modelorat

TATA COMMUNICATIONS

Severe Amazon Q flaw exposed AWS credentials allowing silent code execution in IDEs

The root cause lay in how Amazon Q handled Model Context Protocol server configurations, automatically loading them from a hidden .amazonq/mcp.json file inside workspace directories without prompting for consent or verifying workspace trust. Because these spawned processes inherited the victim's complete environment, they gained immediate access to AWS credentials, session tokens, API keys, and SSH agent sockets.

Exploitation required minimal interaction: an attacker simply planted a malicious configuration file inside a repository and waited for a developer to clone and open the folder in an IDE with Amazon Q active. Successful exploitation could allow attackers to backdoor IAM users, establish cloud persistence, or pivot into internal production systems using inherited contexts.

ATTACK TYPE	Vulnerability	**SECTOR**	IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	Microsoft Visual Studio, VS Code, Amazon Web Services, AWS

Source - https://gbhackers.com/amazon-q-developer-vulnerability/

TATA COMMUNICATIONS

LokiBot campaign steals credentials through a layered JScript and PowerShell chain

The attack begins with a malspam campaign carrying a malicious JScript attachment that, once executed, runs highly obfuscated code interleaving decryption routines with decoy functions. This initial script decodes a Base64-encoded PowerShell payload, saves it to the temporary folder, and executes it, whilst a cleanup function deletes evidence if an execution timeout is reached.

The PowerShell script functions as a .NET assembly loader, performing XOR decryption to reveal an assembly reflectively loaded into memory, which hands control to a third-stage injector protected by ConfuserEx. Notably, this variant features a broken persistence mechanism, writing an incorrect registry path that causes it to fail upon system reboot.

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

Source - https://cyberpress.org/lokibot-uses-obfuscated-loaders/

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