TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 26, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As May 2026 draws to a close, the cyber threat landscape shows no sign of abating, with threat actors deploying increasingly sophisticated and coordinated tactics across highly interconnected digital environments. Conventional defence models continue to be tested as adversaries exploit systemic vulnerabilities at scale. Organisations must reinforce foundational security controls, adopt layered defence strategies, and embed forward-looking intelligence into operational frameworks to sustain resilience and competitive advantage.

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

TATA COMMUNICATIONS

Linux kernel Dirty Frag flaw actively exploited across majority of QNAP NAS products

QNAP has issued a security advisory (QSA-26-17) confirming that the "Dirty Frag" vulnerability, tracked as CVE-2026-43284 with a CVSS score of 8.8, affects the majority of its NAS product lines. Confirmed affected devices include all QNAP x86-based NAS models, all ARM64-based NAS models, all QuTS hero NAS models, and all QuTScloud NAS instances. The flaw was publicly disclosed on 7 May 2026 and stems from a vulnerability in the Linux kernel's ESP handling logic. Only specific ARM-based models running Linux Kernel 4.2 are not affected.

A working proof-of-concept exploit was published on the same day as disclosure, ahead of any patched kernels being made available from distributions. QNAP confirms no official patch is currently available and urges organisations to apply interim mitigations immediately. Recommended measures include restricting SSH and Telnet access for non-administrator accounts, avoiding privileged container modes, disabling unused services, and ensuring NAS devices are not directly exposed to the internet. Users should monitor QNAP's security advisories closely for patch availability.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Linux, QNAP NAS, QuTS hero, QuTScloud, QuTS Hero OS

Source - https://www.hkcert.org/security-bulletin/qnap-nas-elevation-of-privilege-vulnerability_20260512

TATA COMMUNICATIONS

Microsoft May update tackles 138 flaws spanning Windows and cloud services

Microsoft released patches for 138 security vulnerabilities spanning its product portfolio on 13 May 2026, with none listed as known or under active exploitation. Of the 138 flaws, 30 are rated Critical, 104 Important, three Moderate, and one Low in severity. Affected products include Windows and components, Office, SharePoint, Azure, Dynamics 365, SQL Server, Hyper-V, Visual Studio Code, GitHub Copilot, DNS Client, and TCP/IP services.

The vulnerability breakdown comprises 61 privilege escalation bugs, 32 remote code execution flaws, 15 information disclosure issues, 14 spoofing vulnerabilities, eight denial-of-service weaknesses, six security feature bypass flaws, and two tampering vulnerabilities. Security experts recommend prioritising fixes for the Windows DNS Client, Netlogon, Dynamics 365, and Microsoft Word flaws, given their high impact and low user-interaction requirements, whilst applying remaining updates through standard patch cycles without delay.

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

Source - https://msrc.microsoft.com/update-guide/releaseNote/2026-May

TATA COMMUNICATIONS

Iran-linked Seedworm launches global espionage campaign across nine countries

Researchers have uncovered a wide-ranging espionage campaign attributed to Seedworm — also known as MuddyWater — an Iran-linked group believed to operate under the Iranian Ministry of Intelligence and Security. Active in early 2026, the campaign compromised at least nine organisations across four continents, spanning electronics manufacturing, industrial firms, government bodies, financial services, education, and professional services sectors.

The attackers deployed legitimately signed Fortemedia and SentinelOne binaries to execute malicious DLLs through sideloading, orchestrated by Node.js-driven PowerShell implants. Credential theft was conducted via SAM hive extraction and Kerberos ticket abuse, whilst stolen data was exfiltrated through sendit.sh, a public file-transfer service, enabling the group to blend malicious traffic with legitimate consumer web activity and evade network-based detection.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	BFSI, Manufacturing, Government, Education, Aviation
REGION	Middle East, South Korea, South Asia, Latin America	**APPLICATION**	Chromium, Windows, Node.js, PowerShell

Source - https://www.security.com/threat-intelligence/iran-seedworm-electronics

TATA COMMUNICATIONS

TeamPCP targets npm and PyPI in renewed Mini Shai-Hulud supply chain campaign

On 11 May 2026, the threat actor group TeamPCP launched a coordinated supply chain attack targeting the npm and PyPI ecosystems, compromising packages across multiple namespaces simultaneously. Researchers attributed the campaign to a renewed "Mini Shai-Hulud" operation, noting strong continuity with prior TeamPCP intrusions. Impacted packages included TanStack's widely used React routing library, UiPath's enterprise automation tooling, and the official Mistral AI TypeScript client.

The TanStack compromise exploited a chain of vulnerabilities in GitHub Actions workflows, whereby attackers poisoned the Actions cache and extracted OIDC tokens directly from the runner process memory to publish malicious package versions without stealing npm credentials. Once active, the payload functioned as a self-propagating worm, stealing CI/CD and cloud credentials, installing a persistent daemon, and deploying a destructive home-directory wipe capability against affected developer environments.

ATTACK TYPE	Malware	**SECTOR**	Software Development
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Node Packager Manager (npm), GitHub, AnyDesk, Microsoft Teams

Source - https://www.wiz.io/blog/mini-shai-hulud-strikes-again-tanstack-more-npm-packages-compromised

INTRODUCTION | QNAP NAS DEVICES AFFECTED BY ACTIVELY EXPLOITED DIRTY FRAG LINUX KERNEL FLAW | MICROSOFT'S MAY PATCH CYCLE CLOSES 138 SECURITY GAPS ACROSS ITS PRODUCT SUITE | SEEDWORM ABUSES SIGNED SECURITY BINARIES TO CONDUCT GLOBAL ESPIONAGE ATTACKS | SUPPLY CHAIN ATTACKERS EXPLOIT GITHUB ACTIONS TO POISON NPM AND PYPI PACKAGES | CERT-IN FLAGS SUPPLY CHAIN ATTACK SPREADING BIRDCALL ACROSS WINDOWS AND ANDROID | FAKE IPL TICKET PORTALS AND MALICIOUS STREAMING SITES DEFRAUD MILLIONS OF FANS | FIRESCALE HELPS TEAMPCP SURVIVE COMMAND-AND-CONTROL SERVER TAKEDOWN | WINDOWS CLOUD FILTER DRIVER FLAW RE-EMERGES, GRANTING FULL SYSTEM PRIVILEGES | MICROSOFT EXCHANGE SERVER ZERO-DAY CVE-2026-42897 ADDED TO CISA FLAWS LIST | BACKEND DATABASE LEAK EXPOSES THE GENTLEMEN RANSOMWARE OPERATION IN DETAIL

TATA COMMUNICATIONS

ScarCruft embeds BirdCall spyware in gaming software targeting Windows and Android

CERT-In has issued a high-severity advisory warning of an active supply-chain campaign orchestrated by a North Korea-linked threat group, ScarCruft, also tracked as APT37. The attackers compromised sqgame.net, a gaming platform serving ethnic Korean communities, deploying the BirdCall backdoor through trojanised Windows installers and repackaged Android APK files. The malicious Windows update had been active since at least November 2024, initially delivering the RokRAT backdoor before dropping the BirdCall backdoor.

The Android variant of BirdCall — a new addition to ScarCruft's toolkit — harvests contacts, SMS messages, call logs, documents, media files and private keys, and can also capture screenshots and record surrounding audio. Both Windows and Android variants leverage legitimate cloud storage services, including Dropbox, pCloud, Yandex Disk and Zoho WorkDrive, for command-and-control communications, effectively blending malicious traffic with routine network activity.

ATTACK TYPE	Malware, Mobile, Cyber-espionage, Supply Chain, APT	**SECTOR**	Gaming industry
REGION	Global	**APPLICATION**	Android, Windows

Source - CERT-IN Advisory

TATA COMMUNICATIONS

IPL scam campaign exploits fake ticket booking and malicious streaming platforms

The ongoing IPL 2026 season has given rise to a large-scale cybercrime ecosystem targeting cricket fans across India. Threat actors have deployed over 600 fraudulent ticketing domains that convincingly impersonate legitimate platforms, replicating their logos, colour schemes and user interfaces to disarm suspicion. Victims are funnelled to these sites via Meta advertisements, SEO-poisoned search results and social media reels, ultimately losing money through UPI payments before receiving fabricated PDF tickets that are rejected at stadium gates.

Beyond ticketing fraud, researchers identified over 400 malicious free-streaming websites engineered to deliver multi-stage malware to unsuspecting fans. These platforms use user-agent detection scripts to serve OS-specific payloads, routing macOS users through ClickFix-style infection chains that deploy SHub Stealer — a full-featured infostealer capable of harvesting browser credentials, cryptocurrency wallet seed phrases, Telegram sessions and iCloud data, whilst installing a persistent remote access backdoor disguised as a Google Update service.

ATTACK TYPE	Cybercrime, Phishing, Malware	**SECTOR**	Entertainment, Gaming industry, BFSI, Telecommunications, Social Media, Cryptocurrency
REGION	India	**APPLICATION**	Apple macOS, Microsoft Edge, Mozilla Firefox, Opera Browser, Windows, Google Chrome, Telegram

Source - https://www.cloudsek.com/blog/hit-wicket-inside-the-expansive-web-of-scams-targeting-millions-of-ipl-fans-this-season

TATA COMMUNICATIONS

TeamPCP Python toolkit deploys three-tier exfiltration in developer supply chain attack

Researchers at Hunt.io have published a detailed analysis of the 13-module Python toolkit deployed by TeamPCP as the second-stage payload in the Mini Shai-Hulud supply chain campaign. The toolkit targets Linux developer environments, evading sandboxes through three sequential checks — Linux platform, Russian locale, and CPU core count — before executing. It harvests credentials from over 90 sources spanning cloud CLIs, password managers, AI coding tools and container environments.

The malware employs a three-tier exfiltration chain: a hardcoded primary command-and-control server, a FIRESCALE GitHub dead-drop mechanism using cryptographically signed commit messages, and the victim's own GitHub account as a final fallback. Notably, the AWS collection module explicitly targets US GovCloud partitions, whilst machines in Israel or Iran face a geopolitical wiper that plays audio at maximum volume before deleting all accessible files. Russian-locale machines exit without executing any payload.

ATTACK TYPE	Malware	**SECTOR**	IT, Government, Defence Industry
REGION	Global	**APPLICATION**	Docker, Kubernetes, Linux, VS Code, GitHub CLI, Cursor IDE, Anthropic Claude, Bitwarden

Source - https://hunt.io/blog/teampcp-python-toolkit-firescale-github-c2-takedown

TATA COMMUNICATIONS

MiniPlasma Windows Zero-Day grants SYSTEM access on fully patched systems

Security researcher Nightmare-Eclipse released the MiniPlasma exploit on GitHub on 13 May 2026, targeting the cldflt.sys Cloud Filter driver's HsmOsBlockPlaceholderAccess routine. The flaw was originally reported to Microsoft by Google Project Zero's James Forshaw in September 2020 and was believed to have been patched as CVE-2020-17103 in December that year. However, Chaotic Eclipse confirmed the same issue remains present and unpatched, suggesting Microsoft either never fully remediated it or the fix was silently rolled back.

Confirmed affected versions include Windows 11 and Windows Server 2022 and 2025. The exploit is a race condition, meaning success rates may vary, though researchers confirmed it works reliably on fully patched Windows 11 environments. No official patch is currently available, and the publicly weaponised exploit is expected to be rapidly adopted by threat actors, making immediate detection and mitigation steps strongly advisable for organisations.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, Government, Business, Telecommunications
REGION	Global	**APPLICATION**	Windows, Windows Server 2022, Microsoft Windows Server 2025

Source - https://securityonline.info/miniplasma-zero-day-poc-exploit-code-and-vulnerability-details-publicly-disclosed-for-windows-11/

TATA COMMUNICATIONS

Microsoft Exchange Server zero-day under active exploitation prompts CISA KEV listing

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2026-42897 to its Known Exploited Vulnerabilities catalogue, as Microsoft confirmed active exploitation of the Exchange Server zero-day in the wild. Carrying a CVSS score of 8.1, the flaw is classified as an improper neutralisation of input vulnerability, enabling cross-site scripting, which allows unauthorised attackers to perform spoofing over a network.

The vulnerability specifically targets Outlook Web Access, where attackers can exploit it by delivering a specially crafted email that executes malicious JavaScript upon opening. The flaw emerged two days after Microsoft's May 2026 Patch Tuesday, which addressed 138 separate vulnerabilities. With no permanent patch yet available, Microsoft has deployed temporary mitigations via the Exchange Emergency Mitigation Service and urged administrators to apply them immediately.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, Construction, IT, Government, Transportation, Education, Defence, Business, Aviation, Automobile, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Microsoft Exchange Server, Microsoft Outlook, Windows

Source - https://securityaffairs.com/192204/security/cve-2026-42897-microsoft-confirms-active-exploitation-of-exchange-server-zero-day.html

TATA COMMUNICATIONS

Gentlemen RaaS leak uncovers administrator identity, affiliate roles and extortion tactics

Researchers at Check Point Research uncovered the leak of The Gentlemen's internal Rocket database on 4 May 2026, exposing nine accounts, including administrator zeta88, also identified as hastalamuerte, who built the locker, managed the RaaS panel, and oversaw payouts. The partial leak, briefly posted on an underground forum before removal, contained internal channel conversations across INFO, general, TOOLS, and PODBOR, offering a rare end-to-end view of the operation's coordination, toolsets, and victim management.

The group has listed approximately 332 victims in the first five months of 2026, positioning it as the second most productive RaaS operation publicly listing victims during that period. Leaked negotiation screenshots revealed a successful ransom settlement of 190,000 USD, down from an initial demand of 250,000 USD. In a notable cross-border operation, data exfiltrated from a UK software consultancy was subsequently reused during an attack against a Turkish firm, with the consultancy falsely credited as the access broker to amplify pressure on the Turkish victim.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Tourism, BFSI, Manufacturing, IT, Transportation, Education, Defence, Business, Aviation, Renewable Energy, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Microsoft Active Directory Services, Cisco Identity Services Engine (ISE), Cisco IOS, Fortinet FortiGate, VMWare ESXi, Windows, Linux, Veeam, Veeam Backup Enterprise Manager

Source - https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/

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