TATA COMMUNICATIONS

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 11, 2026

TATA COMMUNICATIONS

# THREAT INTELLIGENCE ADVISORY REPORT

As August progresses towards its third week, the cyber threat landscape shows no sign of relenting. Threat actors are mounting increasingly sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Conventional defence models are being pushed to their limits as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now hinges on organisations reinforcing foundational security controls, adopting layered defence strategies, and weaving forward-looking intelligence into every layer of their operational frameworks.

In this fast-shifting environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Published weekly, it offers sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By turning intelligence into practical defence guidance, it enables security teams to anticipate, counter, and contain threats with confidence — safeguarding the continuity of critical operations at scale.

TATA COMMUNICATIONS

# Mirage Kitten unleashes backdoor and tunnelers to hijack high-value corporate networks

Mirage Kitten, an advanced persistent threat group also tracked as UNC1549, Smoke Sandstorm and Nimbus Manticore, has broadened its cyber-espionage operations across the Middle East and Africa. The campaign targets aerospace, aviation, defence, telecommunications, government, financial and small-business organisations. Researchers at Kaspersky have identified a previously undocumented malware toolkit developed and deployed by the group to sustain covert, long-term access.

The toolkit comprises NightLedger, a Windows backdoor supporting reconnaissance, command execution, file operations and screenshot capture, alongside two WebSocket-based tunnellers, ArcBridge and BridgeHead. The tunnellers turn compromised machines into covert relay nodes, funnelling operator traffic through victim networks to evade detection. Organisations in the affected sectors are urged to remain vigilant and hunt for the published indicators of compromise.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Cyber-espionage, APT | **SECTOR** | BFSI, Government, Aerospace, Defence, Business, Telecommunications |
| **REGION** | Middle East, Africa, Burkina Faso, Egypt, Ethiopia, Jordan, Pakistan, Tanzania | **APPLICATION** | Windows |

Source - https://securelist.com/mirage-kitten-new-tools/120811/

TATA COMMUNICATIONS

# Triple X group signals a decisive shift away from traditional ransomware encryption

Triple X is an emerging data extortion group that reflects a broader shift within the ransomware ecosystem, moving away from traditional encryption towards data theft and leak-driven extortion. Active since May 2026, the group operates the Triple X WebBlog leak site and primarily targets organisations holding large volumes of sensitive financial, legal and customer information.

The group gains unauthorised access through compromised credentials and exposed internet-facing systems, including brute-force attacks against remote desktop services, before exfiltrating substantial volumes of data. Public disclosure on its leak site is then used as leverage to pressure victims into payment. Organisations are advised to enforce strong authentication, secure external-facing services and monitor for suspicious access.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Ransomware, Emerging Threats | **SECTOR** | Legal services, BFSI, IT Services and Consulting |
| **REGION** | India, Indonesia, United States | **APPLICATION** | Apple macOS, Windows, Linux |

**Source** - CTI Team Internal Research

TATA COMMUNICATIONS

# Cisco firewall manager flaw added to federal catalogue of exploited vulnerabilities

CISA has added a Cisco Secure Firewall Management Center vulnerability, CVE-2026-20316, to its Known Exploited Vulnerabilities Catalogue after confirming active exploitation. The hard-coded password flaw, carrying a CVSS base score of 5.3, allows an unauthenticated remote attacker to authenticate using built-in low-privileged credentials and access sensitive information held on affected appliances, including configurations, policies and event logs.

Although rated medium in severity, Cisco assigned the flaw a High Security Impact Rating, warning that it may be chained with other vulnerabilities to escalate privileges. No configuration workaround exists, so administrators must apply the released hot-fix packages. Federal agencies were given until 1 August 2026 to remediate, and all organisations are urged to patch without delay.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Vulnerability | **SECTOR** | IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications |
| **REGION** | Global | **APPLICATION** | Cisco Secure Firewall, Cisco FMC |

Source - https://securityonline.info/cisco-fmc-cve-2026-20316/

TATA COMMUNICATIONS

# Helpdesk hijackers abuse Teams vishing and GoGRPC Backdoor for corporate breach

An active intrusion campaign tracked since January 2026 sees a threat actor, believed to operate as an initial access broker, target enterprises through Microsoft Teams voice phishing. Impersonating IT helpdesk staff, the attackers pressure employees into launching Quick Assist remote sessions, then use PowerShell-based staging to profile the host and deploy further payloads onto compromised machines.

Attackers then install the GoGRPC backdoor, which uses the gRPC protocol over HTTP/2 to blend command-and-control traffic with legitimate enterprise streams. Alongside multiple proxy and data-theft tools, it enables reconnaissance, persistence and remote command execution, ultimately preparing networks for potential ransomware. Organisations are urged to restrict Quick Assist, verify support requests and monitor for anomalous PowerShell activity.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Phishing, Malware | **SECTOR** | IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Telecommunications |
| **REGION** | Global | **APPLICATION** | Windows, Microsoft Teams, AWS S3 |

Source - https://securityonline.info/gogrpc-backdoor-teams-vishing/

TATA COMMUNICATIONS

# ENCFORGE ransomware strain targets AI model files, training data, and vector databases

ENCFORGE is a newly identified Go-based ransomware purpose-built to target AI and machine-learning environments. Deployed by the agentic threat actor JADEPUFFER, it encrypts model weights, vector indexes, training datasets and other critical AI artefacts using AES-256-CTR encryption protected by RSA-2048 keys. Encrypted files are renamed with a .locked extension, and ransom notes are dropped to facilitate extortion.

The campaign gains initial access by exploiting CVE-2025-3248, a critical unauthenticated remote code execution flaw in the Langflow AI framework, then abuses an exposed Docker socket to escape the container and execute ENCFORGE on the underlying host. Organisations are urged to upgrade Langflow to version 1.3.0 or later, restrict Docker socket access and maintain immutable model backups.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Ransomware, Emerging Threats | **SECTOR** | IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications |
| **REGION** | Global | **APPLICATION** | Linux, Langflow |

Source - https://thehackernews.com/2026/07/new-encforge-ransomware-targets-ai.html

TATA COMMUNICATIONS

# Scammer turned CRPx0 ransomware offers extortion service across Windows and macOS

CRPx0 is a financially motivated ransomware and extortion group that emerged in early July 2026, listing more than thirty victims within its first month. The operation runs a ransomware-as-a-service ecosystem supported by an affiliate programme, ClickFix social-engineering lures and a multi-stage, Python-based malware framework targeting Windows and, to a lesser extent, macOS systems. Healthcare organisations feature prominently among victims.

Researchers link the group to earlier cryptocurrency scam operations, notably a Flash Token money-laundering service sharing the same contact identifiers. Once executed, the malware unhooks endpoint defences, downloads a portable Python runtime, disables security services and establishes persistence via a scheduled task. Organisations are urged to raise awareness of ClickFix prompts and block the published indicators of compromise.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Ransomware, Emerging Threats | **SECTOR** | Healthcare, BFSI, Aviation, Broadcast Media Production and Distribution, IT Services and Consulting |
| **REGION** | North America, Australia, Europe, UK, China, Netherlands, Qatar, Turkey, United States | **APPLICATION** | Apple macOS, Python, Windows |

Source - https://theravenfile.com/2026/08/03/crpx0-scammer-turned-ransomware-operator/

TATA COMMUNICATIONS

# DPRK-backed hackers linked to a year-long series of AWS-linked npm supply chain attacks

Amazon Threat Intelligence has attributed a series of high-profile npm supply chain compromises to a single DPRK-linked threat actor tracked as SAPPHIRE SLEET, also known as BlueNoroff and Stardust Chollima. The campaign spans the typo-crypto package in early 2025, the widely used debug and chalk libraries in September 2025, and the hugely popular axios package in March 2026.

The group compromised trusted maintainers through social engineering, then published trojanised updates that reached an estimated one in ten cloud environments within two hours. Amazon also observed evolving tradecraft, including fragmented malware delivery, externalised payloads, advanced encryption and sandbox evasion. AI-enabled techniques such as slopsquatting and prompt injection increasingly help attackers generate code, documentation and convincing maintainer identities.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware, Supply Chain | **SECTOR** | BFSI, IT Services and Consulting |
| **REGION** | Global | **APPLICATION** | Apple macOS, Windows, Linux, Node Package Manager (NPM), Axios |

Source - https://www.bleepingcomputer.com/news/security/amazon-links-debug-chalk-npm-supply-chain-attacks-to-north-korean-hackers/

TATA COMMUNICATIONS

# FakeAgent campaign abuses Claude AI platform to spread powerful SectopRAT malware

A large-scale malvertising campaign dubbed FakeAgent targeted users searching for the Claude Desktop application, compromising at least 29 organisations between 21 and 22 July 2026. Attackers purchased Bing search ads that pointed to a malicious public Claude Artifact hosted on the legitimate claude.ai domain, which impersonated the official download page and redirected victims to attacker-controlled infrastructure serving SectopRAT.

The fake ClaudeDesktop.exe used DLL sideloading, VMProtect packing, anti-virtualisation checks and GPU-assisted decryption to evade analysis, while concealing its command-and-control addresses within blockchain transactions via the EtherHiding technique. SectopRAT harvests passwords, browser cookies, payment card data and files. Anthropic removed the malicious Claude Artifact after roughly 7,100 views; affected hosts should be treated as fully compromised.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | IT Services and Consulting, Software Development |
| **REGION** | Global | **APPLICATION** | Microsoft Edge, Google Chrome OS, Windows, Google Chrome, Anthropic Claude |

Source - https://www.bleepingcomputer.com/news/security/fake-claude-app-promoted-by-bing-ads-pushes-sectoprat-malware/

TATA COMMUNICATIONS

# BlueNoroff hackers hijack trusted contacts to spread ClickFix through fake video meetings

BlueNoroff, a financially motivated North Korean threat group linked to the Lazarus ecosystem, is targeting Web3 and cryptocurrency organisations through an elaborate social engineering operation. The attackers hijack trusted Telegram accounts to distribute fake Zoom and Microsoft Teams meeting invites, profiling victims' cryptocurrency wallets before delivering any payload. Malicious ClickFix prompts then trick targets into executing the attackers' code.

Researchers report the kit deploys PowerShell, VBScript and macOS malware to steal credentials and drain wallets, while disabling security defences to evade detection. Crucially, stolen Telegram sessions are reused to propagate attacks through fresh trusted relationships, creating a self-sustaining chain. Organisations are advised to verify meeting invitations via a second channel and never paste unfamiliar commands into their systems.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Social engineering, Phishing, Malware, APT | **SECTOR** | BFSI, IT Services and Consulting, Investment Management, Software Development, Cryptocurrency |
| **REGION** | Global | **APPLICATION** | Microsoft Windows Defender, Apple macOS, Microsoft Edge, Chromium, Mozilla Firefox, Opera Browser, Windows, Microsoft Teams, Google Chrome, Telegram, Zoom Workplace |

Source - https://cyberpress.org/bluenoroffs-telegram-meeting-trap/

TATA COMMUNICATIONS

# TAG-195 Maas group expands TinyEgg with modular implants for browser session theft

Researchers have identified four new malware families within the TAG-195 ecosystem, the malware-as-a-service operation also known as Golden Chickens or Venom Spider. Named TinyEgg, ChonkyChicken, a modularised ChonkyChicken variant and ChromEggscalator, the tools mark a clear architectural shift toward scalable, operator-driven capabilities delivered through ClickFix-style social engineering campaigns using fake security verification pages.

TinyEgg acts as a lightweight initial-access backdoor, while ChonkyChicken adds browser credential theft, session hijacking, reconnaissance and surveillance. The modularised variant introduces a controller-and-plugin architecture, loading discrete capability modules on demand to minimise its detection footprint. ChromEggscalator, meanwhile, bypasses Chrome's App-Bound Encryption. Organisations are advised to strengthen endpoint monitoring and educate users against ClickFix-style verification lures.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | BFSI |
| **REGION** | Global | **APPLICATION** | Microsoft Edge, Windows, Google Chrome |

Source - https://thehackernews.com/2026/07/golden-chickens-resurfaces-with-four.html

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*