TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 7, 2026

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As we enter April 2026, the cyber threat landscape is intensifying due to increasingly sophisticated hostile activities. Traditional defence models are failing as adversaries exploit structural weaknesses across interconnected digital ecosystems. To preserve resilience and strategic advantage, organisations must strengthen core security foundations, implement layered defences, and integrate anticipatory intelligence into their architectures.

In this high-stakes environment, the Tata Communications Cyber Threat Intelligence report becomes indispensable. Published weekly, it delivers incisive analysis of emerging attack campaigns, evolving adversary tactics, and sector-specific exposures. By converting intelligence into immediate defensive action, security teams can anticipate, prepare for, and neutralise threats proactively to protect critical operations globally before disruption occurs.

TATA COMMUNICATIONS

TeamPCP Enhances CanisterWorm with Kubernetes Wiper Capability

A new TeamPCP campaign has upgraded the CanisterWorm malware to include a destructive wiper targeting Kubernetes environments. The malware uses an ICP canister for command-and-control, consistent with previous campaigns. It performs environment fingerprinting by checking the time zone and locale settings. On Kubernetes clusters, it deploys privileged DaemonSets with hostPath mounts to either wipe systems or install a backdoor disguised as PostgreSQL tooling like pglog and pg_state. The wiper container is named Kamikaze, and it deletes all files before forcing a reboot. Standalone systems are destroyed using root-level deletion commands. The latest variant adds lateral movement through SSH key theft and exploitation of exposed Docker APIs on port 2375, enabling rapid propagation across cloud-native environments.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	IT
REGION	Iran	**APPLICATION**	Docker, PostgreSQL, Kubernetes, Linux

Source - https://www.aikido.dev/blog/teampcp-stage-payload-canisterworm-iran

TeamPCP Targets litellm PyPI Package in Supply Chain Attack

Researchers identified that litellm versions 1.82.7 and 1.82.8 on PyPI were backdoored with malicious code absent from the upstream GitHub repository, impacting a library with over 95 million monthly downloads. The payload executes on import and, in version 1.82.8, on any Python startup via a .pth file. The malware performs credential harvesting across over 15 categories of sensitive files, including SSH keys, cloud provider configs, and Kubernetes tokens. On AWS hosts, it queries IMDS for IAM role credentials. In Kubernetes environments, it dumps secrets across all namespaces and deploys privileged pods to every node. A persistent systemd service polls a C2 domain every 50 minutes, feeding AdaptixC2 and Havoc frameworks for ongoing access. Activity is attributed to TeamPCP, extending a multi-ecosystem campaign targeting security tools.

ATTACK TYPE	Malware	**SECTOR**	IT, Cryptocurrency
REGION	Global	**APPLICATION**	Apple Mac OS, Python, Kubernetes, Windows, Linux, Microsoft Azure, Amazon Web Services, Node Packager Manager (NPM)

Source - https://hunt.io/blog/33k-exposed-litellm-teampcp-c2-supply-chain-attack

TATA COMMUNICATIONS

The Ramadan Coupon Lure Leverages AWS-based Exfiltration to Deliver Stealth RAT

Researchers identified a multi-stage malware campaign targeting Middle East users through Ramadan-themed coupon lures impersonating AlCoupon and major retailers like Carrefour and Hyper One. The attack delivers a Remote Access Trojan via weaponised Word documents containing VBA macros that generate and compile obfuscated C# payloads using legitimate .NET tools like csc.exe and ilasm.exe. The malware executes through rundll32, enabling persistent access, system profiling, and data exfiltration. Stolen data is routed via AWS S3 presigned URLs, bypassing conventional C2 detection. The RAT operates under the namespace Ftu4You and communicates with a dedicated C2 panel at article-learning[.]com. It supports remote shell access, screenshot capture, and file browsing. The campaign combines social engineering, living-off-the-land techniques, and cloud abuse to enhance stealth.

ATTACK TYPE	Phishing, Malware	**SECTOR**	E-commerce, Retail and Distribution
REGION	Middle East	**APPLICATION**	Microsoft Word, Windows, AWS S3

Source - https://cdn.cloudsek.com/pdfs/threat_Actors_using_Ramadan+Coupon_as_a_lure_in_middle_east.pdf

Nasir Security Group Targets Energy Sector via Supply Chain Attacks

Nasir Security, a pro-Iranian cyber group, is targeting Middle East energy firms through supply chain compromises and disinformation campaigns. The group leverages business email compromise, spear phishing, impersonation, and exploitation of public-facing applications to exfiltrate data from third-party vendors, such as contractors in engineering and safety, rather than primary targets. Stolen documents are authentic but originate from third parties, leading to exaggerated claims of breach impact. The group's activity resurged in March 2026 after a pause since October 2025, aligning with the regional conflict. Resecurity assessed that the group has not directly hacked major energy companies like Dubai Petroleum and CC Energy Development. Instead, it targets vendors to fuel propaganda and psychological operations with limited direct operational impact.

ATTACK TYPE	Social engineering, Phishing, Cyber Espionage, Supply Chain	**SECTOR**	Construction, Oil and gas, Logistics and Shipping
REGION	Middle East, Iraq, Saudi Arabia, United Arab Emirates	**APPLICATION**	Apple Mac OS, Windows, Linux

Source - https://www.resecurity.com/blog/article/pro-iranian-nasir-security-is-targeting-the-energy-sector-in-the-middle-east

Red Menshen Group Targets Telecom Backbone with Stealth BPFdoor

Researchers uncovered a long-term espionage campaign by a China-nexus threat actor tracked as Red Menshen leveraging BPFdoor, a stealth Linux backdoor, to implant covert "sleeper cells" within global telecommunications networks. Operating at the kernel level, BPFdoor uses passive packet filtering and encrypted triggers to evade detection while enabling persistent access. The implant installs a Berkeley Packet Filter inside the kernel that inspects incoming traffic for a specific pattern, activating only when it receives a crafted "magic packet." Newer variants introduce HTTPS-based activation where triggers are embedded within encrypted web traffic, ICMP control channels for communication between compromised hosts, and telecom protocol awareness, including SCTP inspection. This enables deep surveillance, subscriber tracking, and long-term intelligence collection across critical infrastructure. The malware masquerades as legitimate hardware management services like HPE ProLiant daemons to blend into operational environments.

ATTACK TYPE	Malware	**SECTOR**	Government, Telecommunications
REGION	Global	**APPLICATION**	Linux

Source - https://www.rapid7.com/blog/post/tr-bpfdoor-telecom-networks-sleeper-cells-threat-research-report/

TATA COMMUNICATIONS

CrySome RAT: Advanced, Persistent, .NET Trojan with Reset Survival and AV Evasion

CrySome RAT is a sophisticated, .NET-based, remote-access trojan designed for persistent command and control over TCP. It combines full-spectrum capabilities such as remote execution, credential theft, HVNC stealth control, and network pivoting with advanced persistence mechanisms including scheduled tasks, Windows services, watchdog processes, redundant binary placement, and recovery partition abuse. Its AVKiller module systematically disables security tools by terminating processes, blocking services, poisoning the hosts file to prevent updates, and using IFEO hijacking to block execution of cybersecurity products. Offline registry modification ensures execution even after a system reset, making the malware highly resilient. Additional features include keylogging, screen capture, webcam and audio access, and SOCKS proxy support for lateral movement.

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

Source - https://www.cyfirma.com/research/crysome-rat-an-advanced-persistent-net-remote-access-trojan/

TATA COMMUNICATIONS

CISA Adds F5 BIG-IP APM RCE to KEV Catalogue amid Active Exploitation

CISA has added a critical vulnerability in F5 BIG-IP to its Known Exploited Vulnerabilities catalogue. The flaw, tracked as CVE-2025-53521 with a CVSS score of 9.3, is actively exploited and allows unauthenticated remote code execution via malicious traffic targeting Access Policy Manager configurations. Exploitation leverages improper resource handling within APM policy processing, enabling attackers to trigger uncontrolled execution paths on exposed virtual servers. This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise. CISA strongly urges all organisations to prioritise remediation of this vulnerability as part of their vulnerability management practices.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, Financial Services, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	F5 BIG-IP

Source - https://www.cisa.gov/news-events/alerts/2026/03/27/cisa-adds-one-known-exploited-vulnerability-catalog

TATA COMMUNICATIONS

AI-driven GitHub Malware Campaign Abuses OpenClaw Lures to Deliver LuaJIT Infostealer

A large-scale malware campaign is leveraging GitHub repositories to distribute a LuaJIT-based trojan. Masquerading as developer tools, gaming cheats, and utility software like OpenClaw Docker deployers, phone tracking tools, and Fishing Planet game enhancements, it uses AI-generated lure names drawn from obscure biological taxonomy and medical terminology to bypass detection. The malware employs a dual-component payload design: a renamed LuaJIT interpreter paired with an encrypted script that remains inert when analysed separately. Once executed, it performs five anti-analysis checks, including debugger detection and RAM inspection, then sleeps for approximately 29,000 years to evade sandbox analysis. It captures desktop screenshots and communicates with Frankfurt-based C2 infrastructure across eight load-balanced servers, indicating large-scale credential theft activity.

ATTACK TYPE	Mobile	**SECTOR**	IT, Gaming, Cryptocurrency
REGION	Global	**APPLICATION**	Windows, GitHub

Source - https://www.netskope.com/blog/openclaw-trap-ai-assisted-lure-factory-targets-developers-gamers

TATA COMMUNICATIONS

Pawn Storm Deploys PRISMEX Malware Targeting Defence Supply Chain via Zero-Day Exploits

Pawn Storm, the Russia-aligned group also known as APT28, has launched a sophisticated campaign targeting Ukraine's defence supply chain and allied infrastructure across Central and Eastern Europe using a modular malware suite named PRISMEX. The operation leverages spear-phishing emails with malicious RTF documents exploiting CVE-2026-21509, an OLE security feature bypass, alongside zero-day CVE-2026-21513 in the MSHTML Framework, exploited at least 11 days before patching. The attack chain enables fileless execution through steganographic PNG images using a unique "Bit Plane Round Robin" algorithm, COM hijacking for persistence, and abuse of Filen.io cloud storage for command-and-control. The malware includes PrismexSheet, PrismexDrop, PrismexLoader, and Covenant Grunt implants, with observed wiper commands indicating dual espionage and sabotage objectives.

ATTACK TYPE	Cyber Espionage	**SECTOR**	Government, Transportation, Defence, Mining, Logistics and Shipping
REGION	Czech Republic, Poland, Romania, Slovakia, Slovenia, Turkey, Ukraine	**APPLICATION**	Windows

Source - https://www.trendmicro.com/en_us/research/26/c/pawn-storm-targets-govt-infra.html

NICKEL ALLEY Targets Developers with Fake Jobs and PyLangGhost RAT

NICKEL ALLEY, a North Korea-aligned threat group, is conducting ongoing Contagious Interview campaigns targeting technology professionals through fake job offers, LinkedIn personas, and GitHub repositories. The operation delivers PyLangGhost RAT via ClickFix techniques, where victims are tricked into running malicious commands through fake error pages, as well as through malicious npm packages and Visual Studio Code task abuse. The malware, a Python-based remote access trojan ported from an earlier GoLang version, enables credential theft, command execution, and targeting of cryptocurrency wallet browser extensions. Infrastructure is rapidly rotated using Vercel hosting and deceptive domains mimicking legitimate recruitment organisations. The group creates fake company websites and GitHub accounts masquerading as blockchain development firms to build credibility. Broader objectives include cryptocurrency theft, espionage, and potential supply chain compromise.

ATTACK TYPE	Malware, APT	**SECTOR**	IT, Cryptocurrency
REGION	North Korea	**APPLICATION**	Apple Mac OS, Microsoft Visual Studio, Google Chrome OS, Windows, Linux, VS Code, Node.js, Node JS, Google Chrome, GitHub

Source - https://www.sophos.com/en-gb/blog/nickel-alley-strategy-fake-it-til-you-make-it

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