TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: March 24, 2026

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As March 2026 progressed, we saw advanced hostile activities intensify cyber threats globally. Traditional security approaches are proving to be insufficient, as attackers are taking advantage of the vulnerabilities existing deep within the digital ecosystems. Organisations need to reinforce their security foundations, establish multi-layered defences, and leverage predictive intelligence to stay resilient and maintain a competitive edge.

To attain such a security posture, the Tata Communications Cyber Threat Intelligence report is an essential resource for CISOs. The report offers sharp insights into emerging threats, adversaries, and industry-specific vulnerabilities every week. By turning intelligence into swift defensive measures, security teams can predict and counter threats, preventing disruption of critical operations around the world.

TATA COMMUNICATIONS

MOIS-linked cyber threat entities evolve tactics in ongoing campaigns across strategic sectors

Boggy Serpens, also known as MuddyWater, an Iranian APT linked to the Ministry of Intelligence and Security (MOIS), has conducted sustained cyberespionage campaigns targeting diplomatic, energy, maritime, and financial sectors globally.

The hackers shifted from noisy phishing to stealthy, multi-wave intrusions using trusted account hijacking, AI-assisted malware, and Rust-based implants. Their operations feature tailored lures, macro-based delivery, and custom backdoors including BlackBeard, LampoRAT, UDPGangster, and Nuso. Advanced C2 methods like Telegram APIs, HTTP status codes, and UDP channels enable persistence, while coordinated infrastructure and repeated targeting suggest strategic intent toward long-term regional infiltration.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	BFSI, Government, Transportation, Energy, Aviation, Telecommunications
REGION	The Middle East, Europe, The United States, Central Asia	**APPLICATION**	Windows

Source - https://unit42.paloaltonetworks.com/boggy-serpens-threat-assessment/

TATA COMMUNICATIONS

AI-generated ‘Slopoly’ malware deployed by Hive0163 in interlock ransomware campaign

Security researchers have identified a suspected AI-generated malware framework called Slopoly during a ransomware attack attributed to the threat group Hive0163. The malware functions as a PowerShell-based command-and-control persistence client deployed in the later stages of the intrusion to maintain sustained access to compromised systems.

The attack chain began with a ClickFix social engineering technique, which enabled the deployment of NodeSnake, followed by InterlockRAT, and eventually the Interlock ransomware. This incident highlights how threat actors are increasingly using LLM-generated malware to accelerate development and streamline their ransomware operations, marking another example of AI's growing role in cyberattacks.

ATTACK TYPE	Social engineering	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail, Telecommunications
REGION	Global	**APPLICATION**	Windows, Node.js, PowerShell

Source - https://www.ibm.com/think/x-force/slopoly-start-ai-enhanced-ransomware-attacks

TATA COMMUNICATIONS

GlassWorm attack targets Open VSX extensions, MCP servers, and React npm packages

Researchers have identified a major evolution of the GlassWorm supply chain campaign targeting developers through Open VSX extensions, npm packages, MCP servers, and compromised GitHub repositories. The latest wave distributes malware through transitive extension dependencies, typosquatted extensions, and malicious npm preinstall scripts that enable staged JavaScript execution and in-memory payload delivery.

The operation leverages Solana transaction memos, Google Calendar links, and rotating command-and-control infrastructure to retrieve payloads and evade detection. This multi-layered approach allows attackers to steal credentials, cryptocurrency wallets, and developer secrets from compromised systems, posing significant risks to software supply chains.

ATTACK TYPE	Cyberespionage	**SECTOR**	IT, Cryptocurrency
REGION	Global	**APPLICATION**	VS Code, Node Packager Manager (NPM), GitHub, React

Source - https://socket.dev/blog/open-vsx-transitive-glassworm-campaign | https://www.koi.ai/blog/glassworm-hits-mcp-5th-wave-with-new-delivery-techniques
https://www.aikido.dev/blog/glassworm-strikes-react-packages-phone-numbers

China-linked cyberattacks use PlugX and Cobalt Strike to target countries

Following the recent escalation in the Middle East, researchers observed increased cyber-espionage activity by China-linked threat actors targeting Qatar. The Camaro Dragon APT rapidly launched campaigns using conflict-themed lures referencing missile strikes and attacks on regional oil infrastructure to deceive victims.

These operations delivered PlugX malware and Cobalt Strike through complex infection chains involving LNK files, DLL hijacking, and Rust-based loaders. The campaigns highlight how threat actors quickly adapt to geopolitical events and demonstrate ongoing intelligence-collection efforts against Gulf entities, reflecting the strategic importance of the region amid heightened tensions.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Government, Oil & Gas, Energy, Defence, Telecommunications
REGION	The Middle East, Qatar	**APPLICATION**	Windows

Source - https://blog.checkpoint.com/research/china-nexus-activity-against-qatar-observed-amid-expanding-regional-tensions/

TATA COMMUNICATIONS

Iranian APT group Charming Kitten and its allies attack amidst the war in the Middle East

Charming Kitten, an IRGC-linked Iranian APT also tracked as APT35, Phosphorus, Mint Sandstorm, and NewsBeef, specialises in human-targeted cyber espionage through advanced social engineering, credential harvesting, and targeted malware deployment. Active since 2014, the group focuses on journalists, researchers, policymakers, nuclear scientists, and diaspora activists operating both within and outside Iran.

Their campaigns leverage browser impersonation infrastructure, malicious browser extensions, and a diverse malware arsenal including POWERSTAR, HYPERSCRAPE, BellaCiao, MELLONA, and RATMILAD. Amid escalating Iran-Israel tensions and recent US-Israeli military strikes, analysts expect Iranian cyber retaliation through state-linked proxies, hacktivist groups, and semi-autonomous APT elements targeting regional adversaries and their allies.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Healthcare, Government, Energy, Aerospace, Defence
REGION	The Middle East, Europe, Israel, The US	**APPLICATION**	Apple Mac OS, Mozilla Firefox, Windows, Microsoft Office 365, Google Chrome, Gmail

Source - https://falconfeeds.io/blogs/charming-kitten-in-the-iran-israel-cyber-war

TATA COMMUNICATIONS

Critical FreeScout vulnerability enables unauthenticated remote code execution via email

A critical vulnerability tracked as CVE-2026-28289 with a CVSS score of 10 has been discovered in the FreeScout helpdesk platform. The flaw allows unauthenticated zero-click remote code execution when a crafted email attachment is sent to a mailbox configured in the system.

The vulnerability bypasses a previous fix for CVE-2026-27636 by exploiting a filename validation weakness using a Zero-Width Space character to evade security checks. The malicious attachment is stored in a predictable server directory and later executed through the web interface. FreeScout versions up to 1.8.206 are affected, with the issue patched in version 1.8.207. Successful exploitation could lead to full system compromise, data exfiltration, and lateral movement within affected networks.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, IT, Government, Media
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, FreeScout

Source - https://www.bleepingcomputer.com/news/security/mail2shell-zero-click-attack-lets-hackers-hijack-freescout-mail-servers/

BlackSanta malware targets recruitment processes with EDR-killer payload

Threat analysts have uncovered a stealthy malware campaign targeting HR and recruitment teams using resume-themed lures that deliver an ISO file containing malicious scripts. When opened, the ISO triggers a multi-stage infection chain that executes PowerShell commands, extracts hidden payloads through steganography, and deploys a malicious DLL that performs reconnaissance and anti-analysis checks.

A key component called BlackSanta acts as an EDR-killer using bring-your-own-vulnerable-driver techniques with vulnerable drivers to disable security protections. After neutralising defences, attackers establish encrypted command-and-control communications, maintain persistence on compromised systems, and enable data theft and further network compromise.

ATTACK TYPE	Malware	**SECTOR**	Staffing
REGION	Global	**APPLICATION**	Windows

Source - https://www.aryaka.com/docs/reports/blacksanta-edr-killer-threat-report.pdf

TATA COMMUNICATIONS

MOIS-linked Handala Hack conducts destructive campaigns targeting global enterprises

Handala Hack, an online persona operated by the MOIS-linked threat actor Void Manticore, also known as Red Sandstorm and Banished Kitten, conducts destructive cyber operations combining wiper attacks with hack-and-leak campaigns. The group has targeted Israel, Albania, and recently the US enterprises, including Stryker.

The attackers rely on compromised VPN credentials, brute-force access, and supply-chain targeting of IT providers to gain initial entry. Intrusions involve hands-on activity, lateral movement via RDP and tunnelling using NetBird. During the destructive phase, multiple wiping techniques are deployed simultaneously, including custom wipers, PowerShell scripts, manual deletion, and disk encryption using VeraCrypt to maximise operational impact on compromised networks.

ATTACK TYPE	Cyberespionage, APT	**SECTOR**	Healthcare, Government, IT, Telecommunications
REGION	Albania, Israel, The US	**APPLICATION**	Windows

Source - https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/

TATA COMMUNICATIONS

New infostealer MicroStealer uses Electron and Java payload for identity theft

MicroStealer is a rapidly spreading infostealer observed in more than 40 sandbox sessions within a month despite maintaining low antivirus detection rates. The malware uses a layered delivery chain consisting of an NSIS installer, Electron loader, and Java-based stealer module to complicate analysis and delay detection.

It steals browser credentials, session cookies, screenshots, and cryptocurrency wallet data while exfiltrating collected information to Discord webhooks and attacker-controlled infrastructure. Obfuscation techniques, sandbox evasion mechanisms, and scheduled task persistence allow MicroStealer to maintain prolonged access and conduct large-scale credential theft across compromised systems.

ATTACK TYPE	Malware	**SECTOR**	Education, Telecommunications
REGION	Germany, The US	**APPLICATION**	Windows

Source - https://any.run/cybersecurity-blog/microstealer-technical-analysis/

Play ransomware abused RustDesk, PSExec, and native Windows utilities

CERT-In has observed evolving tactics associated with Play ransomware operations involving credential harvesting, remote monitoring tools, and stealthy persistence mechanisms. Threat actors leverage legitimate utilities such as RustDesk, PSExec, PowerShell, and esentutl.exe to evade detection while maintaining elevated access within compromised networks.

Registry hive extraction, firewall modifications and RDP enablement facilitate lateral movement and privilege abuse across affected systems. Malicious DLL execution and additional remote access tools expand attacker control before ransomware deployment, when files are encrypted with the .PLAY extension and ransom notes are dropped on compromised machines.

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

Source - https://cybelangel.com/blog/play-ransomware-double-extortion-gang/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a[

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