TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 14, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

The first week of April 2026 witnessed cyber threats growing more intense and complex. Hostile actors continue to take advantage of weak points in connected digital systems, causing traditional security methods to fail. To stay resilient and aware of persistent and new risks, organisations need to strengthen their core security, build layered defences, and add predictive intelligence to their systems.

In such a high-risk environment, the weekly Tata Communications Cyber Threat Intelligence report plays a critical role in enabling organisations to stay aware and prepared. It provides a clear analysis of new attack campaigns, changing attacker methods, and risks specific to different sectors. Security teams can use this intelligence to anticipate and prepare for threats and take immediate action to stop them before any disruption occurs.

TATA COMMUNICATIONS

FortiClient EMS Critical Security Flaw Actively Exploited

Fortinet has released emergency patches for a serious vulnerability called CVE-2026-35616. This flaw affects FortiClient EMS and has a CVSS score of 9.1. It is a pre-authentication API access control issue that allows unauthenticated attackers to bypass authentication by sending purpose-crafted API requests. This allows them to run arbitrary commands and escalate privileges. The affected versions are 7.4.5 and 7.4.6. The company first observed exploitation in the wild on March 31, 2026. Attackers are using weak access controls to exploit the flaw. The researchers Simo Kohonen from Defused Cyber and Nguyen Duc Anh discovered and reported it. Fortinet strongly urges all users to deploy the hotfix immediately. A full fix will also be included in the upcoming version 7.4.7.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, Manufacturing, Construction, IT, Government, Education, E-commerce, BFSI, Aviation, Automobile, Retail, Energy, Telecom, Logistics
REGION	Global	**APPLICATION**	Firewall Forticlient, Forticlient EMS, FortiClient

Source - https://thehackernews.com/2026/04/fortinet-patches-actively-exploited-cve.html

TATA COMMUNICATIONS

Claude Code Leak Weaponised to Spread Vidar and GhostSocks Malware via GitHub

Anthropic accidentally exposed its internal Claude Code source code through an npm package. Within 24 hours, they set up fake GitHub repositories disguised as the leaked tools to distribute Vidar stealer and GhostSocks proxy malware. The malicious files were hidden inside Trojanised archive files. This campaign is part of a larger operation. Since February 2026, the same attackers have been using fake software lures. They have impersonated more than 25 different brands. They abuse trusted platforms like GitHub Releases to deliver malware. The attackers rely on social engineering and trust abuse. This incident shows that security risks often come from human and organisational gaps, not just software bugs.

ATTACK TYPE	Social Engineering, Malware	**SECTOR**	IT, Financial Services, Gaming, Cryptocurrency
REGION	Global	**APPLICATION**	Windows, Anthropic Claude Code

Source - https://www.trendmicro.com/en_us/research/26/d/weaponizing-trust-claude-code-lures-and-github-release-payloads.html

TATA COMMUNICATIONS

CERT Polska Identifies Cifrat Android RAT Using Multi-Stage Loader and Accessibility Abuse

CERT Polska has analysed a new Android malware called Cifrat. The malware is delivered through a phishing campaign that impersonates Booking.com. Victims receive a phishing email with a malicious link that redirects them through a Google share link and then to a fake Booking.com update page. It offers a fake APK file, which loads a native library and decrypts a second APK, which then extracts a hidden file named FH.svg. After decryption, the final RAT payload is deployed to abuse Android accessibility services. It can steal credentials, monitor the screen, intercept SMS messages, and remotely control the device. The RAT communicates with its command-and-control server using WebSocket channels over ports 8443 and 8444.

ATTACK TYPE	Malware, Mobile	**SECTOR**	Tourism, Hospitality
REGION	Global	**APPLICATION**	Android

Source - https://cert.pl/en/posts/2026/04/cifrat-analysis/

TATA COMMUNICATIONS

Persistent Espionage Campaigns Linked to Stately Taurus and Related Clusters

Researchers have uncovered a coordinated cyberespionage operation targeting a government in Southeast Asia. The campaign involves three distinct but overlapping clusters. These are Stately Taurus, CL-STA-1048, and CL-STA-1049. The attackers used USB-propagated malware, multiple remote access Trojans (RATs), loaders, and information stealers. Their goal was to gain persistent access and steal sensitive data. Stately Taurus deployed the USBFect worm and the PUBLOAD backdoor. CL-STA-1048 used tools like the EggStremeFuel backdoor, Masol RAT, EggStreme Loader, Gorem RAT, and the TrackBak stealer. CL-STA-1049 used the Hypnosis loader to deliver the FluffyGh0st RAT. Overlaps in tools and tactics suggest these are China-aligned actors working in parallel.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Government
REGION	South Asia, East Asia	**APPLICATION**	Windows

Source - https://unit42.paloaltonetworks.com/espionage-campaigns-target-se-asian-government-org/

TATA COMMUNICATIONS

Qilin Ransomware Uses Advanced EDR Killer to Disable Over 300 Security Tools

Researchers have uncovered a complex, multi-stage infection chain used by the Qilin ransomware. The attack starts with a malicious DLL file named “msimg32.dll” that deploys an advanced EDR killer. A loader prepares the environment before decrypting and running the EDR killer in memory. The EDR killer loads two helper drivers named “rwdrv.sys” and “hlpdrv.sys” to disable security tools. The malware uses SEH and VEH-based control flow obfuscation, syscall recovery, and in-memory payload execution. These methods help the malware bypass detection. The malware also abuses legitimate signed drivers to gain kernel-level access. It disables telemetry, unregisters security callbacks, and terminates over 300 different EDR solutions from almost every vendor.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Financial Services, IT, Government, Education, Defence, Broadcast Media Production & Distribution, Retail & Distribution, Logistics & Shipping
REGION	Global	**APPLICATION**	Windows

Source - https://blog.talosintelligence.com/qilin-edr-killer/

Pay2Key Ransomware Can Now Target Linux Enterprise Infrastructure

Researchers have discovered a Linux version of the Pay2Key ransomware. The malware uses a configuration-driven execution model that needs root privileges to run. Once it has system-level access, it disables defences, stops critical services, and encrypts via mounted filesystems. The ransomware uses the ChaCha20 encryption algorithm and supports both full-file encryption and partial or sampled encryption modes. This gives the operators flexibility between speed and impact. The ransomware also tries to disable SELinux and AppArmor. It kills processes and sets up a cron entry to survive reboots. Notably, this Linux variant does not have active command-and-control communication. This means it works as a standalone encryptor.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Government, Defence, BFSI
REGION	Global	**APPLICATION**	Linux

Source - https://www.morphisec.com/blog/inside-pay2key-technical-analysis-of-a-linux-ransomware-variant/

TATA COMMUNICATIONS

Operation TrueChaos Uses Zero-Day TrueConf Exploit to Deploy Havoc

Operation TrueChaos is a targeted cyberespionage campaign that exploits a zero-day vulnerability in the TrueConf client update mechanism. The flaw is CVE-2026-3502 with a CVSS score of 7.8 and was added to the CISA KEV catalogue. Attackers compromised an on-premises TrueConf server and replaced the legitimate update with malicious poweriso.exe and 7z-x64.dll. The server distributed the fake update to all connected clients, enabling remote execution across multiple government endpoints. The attackers used DLL sideloading and then deployed a Havoc implant. Researchers attribute the campaign to a Chinese-nexus threat actor. The targets were Southeast Asian government entities.

ATTACK TYPE	Cyber-espionage	**SECTOR**	Government
REGION	South Asia	**APPLICATION**	Windows, TrueConf Windows Client

Source - https://research.checkpoint.com/2026/operation-truechaos-0-day-exploitation-against-southeast-asian-government-targets/

TATA COMMUNICATIONS

CrystalX RAT MaaS Trojan Spreads Spyware, Stealer, and Prankware Threat via GitHub

A large-scale malware campaign is using GitHub repositories to distribute a LuaJIT-based trojan called CrystalX RAT. It is offered in the form of a malware as a service (MaaS) with three subscription tiers. The malware masquerades as developer tools, gaming cheats, and utility software and uses AI-generated lure names and a dual-component payload to bypass detection. Once executed, it performs anti-analysis checks and captures desktop screenshots. It also includes a credential stealer, a keylogger, a clipper for crypto wallets, and prankware features like screen rotation and fake BSOD. The malware communicates with Frankfurt-based C2 infrastructure, indicating large-scale credential theft activity.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, Financial Services, Manufacturing, Government, Transportation, Education, Energy, Retail & Distribution, Telecom
REGION	Russia, Global	**APPLICATION**	Chromium, Windows, Telegram, DISCORD

Source - https://securelist.com/crystalx-rat-with-prankware-features/119283/

TATA COMMUNICATIONS

Operation NoVoice Enables Persistent, Full-Device Compromise on Android

Operation NoVoice, a sophisticated Android rootkit campaign, targets users through malicious apps distributed on Google Play. The malware exploits legacy vulnerabilities from 2016 to 2021 to gain root access and inject code into all applications on the device. The rootkit maintains persistence even after a factory reset and can be removed only by re-flashing the firmware. The rootkit replaces core system libraries and uses a watchdog daemon to self-heal if removed. The malware has an active command and control infrastructure, operates using a modular plugin-based architecture, and was found stealing sensitive data, including WhatsApp session credentials. Over 50 malicious apps were identified – with at least 2.3 million downloads – and removed by Google after responsible disclosure.

ATTACK TYPE	Malware, Mobile	**SECTOR**	IT, Healthcare, Financial Services, Manufacturing, Government, Transportation, Education, Energy, Retail & Distribution, Telecom
REGION	India, Algeria, Ethiopia, Kenya, Nigeria	**APPLICATION**	Android, WhatsApp

Source - https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-research-operation-novoice-rootkit-malware-android/

TATA COMMUNICATIONS

OilRig Uses Stolen EV Certificate to Sign Karkoff Backdoor Targeting the Energy Sector

Analysts uncovered previously unreported activity by the Iranian threat group OilRig, also tracked as APT34. The group used a stolen Entrust Extended Validation (EV) code signing certificate issued to MOSCII Corporation, a legitimate Thai IT vendor. OilRig used it to sign the Karkoff backdoor and additional low-detection payloads. The signed sample had an internal filename of egatdmtools.exe, apparently for targeting the Electricity Generating Authority of Thailand (EGAT) supply chain. As MOSCII has business relationships with EGAT, OilRig probably first compromised MOSCII to steal the certificate. This allowed the group to disguise malware as trusted vendor tools. The operation demonstrates advanced evasion through abuse of trusted certificates and stealth-focused tactics.

ATTACK TYPE	Supply Chain, APT	**SECTOR**	Government, Energy & Power
REGION	Thailand, South Asia	**APPLICATION**	Windows

Source - https://blog.polyswarm.io/polykg-discovers-previously-unreported-oilrig-samples-using-stolen-cert

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