TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: November 17, 2026



TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

With November 2026 well under way, the cyber threat landscape shows no sign of easing, as threat actors engineer increasingly sophisticated and well-coordinated campaigns across deeply interconnected digital environments. Traditional defence models are struggling to keep pace as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now depends on organisations reinforcing foundational security controls, adopting layered defence strategies, and embedding forward-looking intelligence throughout their operational frameworks.

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

INTRODUCTION

BUGGY HYFLOCK RANSOMWARE ENCRYPTS ONLY PART OF LARGE FILES, LEAVING DATA READABLE

SLIPPYNUNCHUCKS ABUSES SOGOU INPUT METHOD TO DISTRIBUTE DARKVIGIL MALWARE

DATABASE SERVERS HIT BY ANUBIS RANSOMWARE USING A PREVIOUSLY UNDOCUMENTED BACKDOOR AND VULNERABLE DRIVERS

ANDROID MR ROBOT MAAS RENTS BANKING TROJANS THAT INTERCEPT OTPS AND REROUTE CALLS

C3RB3R EXPLOITS A LONG-PATCHED SYNOLOGY FLAW TO ENCRYPT FILES ON OUTDATED NAS DEVICES

APT29 POISONS WEB ANALYTICS SERVICE TO COMPROMISE IOS AND ANDROID DEVICES

PARTISAN ZMIY HIDES VASILEK BACKDOOR INSIDE VMWARE TOOLS TO SPY ON NETWORKS

CWPDOOR LINUX BACKDOOR HIDES INSIDE A TROJANISED WEB HOSTING PANEL BINARY

LONE BOSSAI OPERATOR SCALES ATTACKS ACROSS 11 COUNTRIES USING A MESH OF 12 AI AGENTS

FAKE AI DESKTOP APPS ON GITHUB ABUSE SIGNED BINARIES TO MINE CRYPTOCURRENCY

TATA COMMUNICATIONS

HYFLOCK switches programming languages and loaders, and an encryption flaw allows partial file recovery

Researchers have analysed HYFLOCK, a Windows ransomware operation that has iterated rapidly through 2026. Beginning with a Rust-based encryptor in April, it introduced a separate loader in July, adopted a Go-based carrier in early October, then reverted to a standalone Rust executable disguised as a software update on 17 October. Each build encrypts files and inhibits recovery.

Implementation flaws undermine HYFLOCK's own encryption. The 17 October build locked only the first four kilobytes of larger files, letting researchers recover internal document components without a key, while an earlier build could permanently discard data. Unverified victim claims span manufacturing and government. Organisations should preserve encrypted artefacts, identify the exact build, and maintain offline backups before attempting recovery.

ATTACK TYPE	Ransomware, Emerging Threats	**SECTOR**	Manufacturing, Government, Business, Retail and Distribution, Telecommunications
REGION	Canada, India, Brazil, Ecuador, Nigeria, Saudi Arabia, Turkey, United States, Vietnam	**APPLICATION**	Windows

Source - https://gbhackers.com/hyflock-ransomware/

TATA COMMUNICATIONS

SlippyNunchucks abuses Sogou app traffic to plant DarkVigil malware via DNS hijacking

Researchers have uncovered a DNS hijacking operation by the China-aligned threat actor SlippyNunchucks, which abuses insecure HTTP communications in the Windows version of Sogou Input Method, a popular Chinese-language input method editor developed by Tencent. By redirecting the application's unencrypted configuration requests to attacker-controlled servers, the group serves a malicious configuration that hijacks Sogou's legitimate brand-promotion and component-loading mechanisms.

The malicious configuration instructs the legitimate SGTool.exe component to download and sideload a malicious library, ultimately executing the modular DarkVigil backdoor (also known as FDMTP) for espionage, surveillance, and data exfiltration. ESET observed victims across Asia and Europe. Tencent has since patched the flaw, tracked as CVE-2026-120422, and users should update Sogou Input Method to version 16.10 or later immediately.

ATTACK TYPE	Vulnerability, Malware, Cyberespionage, Supply Chain, APT	**SECTOR**	Gambling
REGION	Russia, Japan, UK, Global, Austria, Denmark, Oman, Philippines, Sri Lanka, Thailand, Vietnam, South Asia, East Asia, Hong Kong, Dubai	**APPLICATION**	Windows

Source - https://www.welivesecurity.com/en/eset-research/slippynunchucks-hijacks-sogou-input-methods-brand-promotion-mechanism-to-distribute-malware/

TATA COMMUNICATIONS

Anubis ransomware deploys custom backdoor to abuse Microsoft SQL Server systems

Symantec has detailed an Anubis ransomware intrusion against a US organisation in October 2026, attributed to a group it tracks as Hawkmoth, which operates Anubis as a ransomware-as-a-service platform. The attackers deployed a previously undocumented custom backdoor, named Lindnor, on two Microsoft SQL Server hosts, where it masqueraded as legitimate Chrome and VMware components and ran as a Windows service.

Alongside the backdoor, the group used Bring Your Own Vulnerable Driver techniques, dropping signed but flawed drivers to gain kernel-level access and disable endpoint defences, supported by numerous security-disabling tools. Anubis typically conducts double-extortion attacks, appending the .anubis extension to encrypted files. Although this incident was blocked before encryption, organisations with similar infrastructure should closely monitor their database servers.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	IT, Healthcare, Government, Transportation, Oil and Gas, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	United States	**APPLICATION**	Microsoft SQL Server, Windows

Source - https://securityonline.info/lindnor-backdoor-anubis-ransomware-byovd/

TATA COMMUNICATIONS

Rented MR ROBOT Android banking trojans steal OTPs and silently reroute verification calls

Researchers have uncovered MR ROBOT, a previously unreported Android malware-as-a-service operation targeting customers of Indian banks. Fraudsters rent customised trojans disguised as banking, utility and government applications, including fake Aadhaar and KYC updaters. Once installed, the malware intercepts SMS messages and OTPs and harvests financial credentials through convincing phishing overlays.

A standout capability is covert unconditional call forwarding, which quietly reroutes incoming bank calls to defeat phone-based verification. To evade scanners, the malware lies dormant for at least 48 hours before activation, exfiltrating stolen data through Firebase and Telegram. One affiliate alone intercepted 5,407 SMS messages across 153 devices. Customers should avoid sideloaded APKs and migrate away from SMS-based authentication.

ATTACK TYPE	Malware, Mobile	**SECTOR**	Government, Energy, Power, BFSI, Telecommunications
REGION	India	**APPLICATION**	Android

Source - https://www.cloudsek.com/blog/inside-mr-robot-malware-as-a-service-targeting-indian-bank-customers

TATA COMMUNICATIONS

C3RB3R ransomware targets vulnerable Synology NAS data via outdated DSM versions

Synology has warned that threat actors are exploiting a DiskStation Manager (DSM) vulnerability, originally patched in December 2024, to deploy C3RB3R ransomware against network-attached storage devices running outdated software. A variant of the Cerber family, the ransomware scans accessible folders and encrypts stored data, appending a .L0CK3D extension and dropping a read-me3.txt ransom note into each affected directory.

Successful attacks can disrupt storage operations, cause data loss, and inflict considerable financial and operational damage. With researchers tracking hundreds of thousands of internet-exposed Synology devices, the potential attack surface is large. Synology has not published a decryptor, urging customers instead to update DSM immediately, enable automatic updates, and block internet access to the management web interface.

ATTACK TYPE	Ransomware, Emerging Threats	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Education, Telecommunications
REGION	Global	**APPLICATION**	macOS, Windows, Linux, Synology

Source - https://securityonline.info/synology-nas-ransomware-attacks/

TATA COMMUNICATIONS

APT29 poisoned website attacks exploit n-day flaws in unpatched iOS and Android

Researchers have detailed a large-scale watering hole campaign, assessed with moderate-to-high confidence as the work of APT29, targeting iOS and Android users. The operation combined three delivery vectors: compromised legitimate websites, lookalike domains impersonating high-profile sites, and a supply-chain compromise of the Ukrainian Plerdy analytics service, whose tracker script was poisoned between late August and early September 2026.

A malicious JavaScript loader fingerprinted each visitor's device before serving a platform-specific n-day exploit chain. On iOS, the DarkSword kit harvested cookies and full device data; on Android, AndroSnitch stole Chrome cookies, credentials, and Wi-Fi passwords. Fully patched devices were unaffected, and the malware left no persistence. Users should update promptly, rotate credentials, and revoke active sessions.

ATTACK TYPE	Malware, Mobile, Cyberespionage, Supply Chain, APT	**SECTOR**	Healthcare, Government, Military, Energy, Defence Industry, Chemical Manufacturing, Hospitality
REGION	Australia, UK, Global, Bulgaria, Czech Republic, Ukraine, United States	**APPLICATION**	Android, Apple iOS, Apple iCloud, Apple Safari, Google Chrome, Telegram, WhatsApp

Source - https://www.sekoia.com/blog/poisoned-source-apt29-watering-holes-targets-mobile-devices-with-n-day-exploits

TATA COMMUNICATIONS

Partisan Zmiy replaces VMware Tools to plant stealthy Telegram-controlled Vasilek backdoor

Researchers have detailed a prolonged intrusion by the Partisan Zmiy group, also known as the Cyber Partisans, which maintained covert access to a medical organisation's infrastructure from early 2024. To blend in, the attackers replaced the legitimate VMware Tools DLL with a malicious version carrying the Vasilek backdoor, establishing persistence through DLL hijacking and rogue Windows services.

A custom scheduler loader, masquerading as a VMware service, orchestrated the payloads, while command and control ran through DNS tunnelling, the Telegram Bot API, GOST, and 3proxy to evade monitoring. The campaign granted prolonged access to sensitive medical data and interconnected healthcare environments, with no destructive activity reported. Organisations should verify VMware Tools binary integrity and monitor unusual outbound traffic.

ATTACK TYPE	Hacktivism, Malware, Cyberespionage	**SECTOR**	Healthcare
REGION	Global	**APPLICATION**	Windows, VMware Tools, Telegram

Source - https://cybersecuritynews.com/hackers-hide-vasilek-backdoor/

TATA COMMUNICATIONS

Stealthy CWPdoor Linux backdoor executes encrypted commands via HTTP request headers

Researchers have uncovered CWPdoor, a passive Linux backdoor distributed through a trojanised version of cwpsrv, the web server behind the Control Web Panel hosting tool. First captured in June 2026 via a fake updater script, it replaces the legitimate binary and lies dormant, executing encrypted commands only when triggered by specially crafted HTTP request headers.

To evade detection, CWPdoor suppresses access logs, verifies signed commands, and uses AES-256 encryption. With more than 340,000 Control Web Panel instances exposed online, the potential attack surface is substantial. The malware was found alongside artefacts linked to the long-running Ebury operation, though researchers have not confirmed a relationship. Administrators should inspect the cwpsrv binary and rotate all credentials

ATTACK TYPE	Malware, Emerging Threats	**SECTOR**	IT, Healthcare, Government, Transportation, Military, Oil and Gas, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	CentOS, Linux

Source - https://www.bleepingcomputer.com/news/security/hackers-backdoor-linux-servers-using-trojanized-cwp-web-server/

TATA COMMUNICATIONS

Lone operator BOSSAI wields a mesh of 12 AI agents to attack critical infrastructure

Researchers at the Acronis Threat Research Unit have detailed BOSSAI, an operation in which a single operator coordinated a mesh of twelve AI agents to automate reconnaissance, vulnerability scanning, and exploitation. Targeting organisations across Taiwan, Mexico, and Thailand, amongst 11 countries in total, the campaign exposed medical, educational, financial, and personal data across government, healthcare, and BFSI sectors.

The agents were divided into roles spanning infrastructure management, scanning, and active exploitation, with the operator manually relaying results amongst them. Notably, commercial AI models repeatedly refused malicious instructions despite jailbreak attempts, and the agents succeeded mainly where basic defences were weak, exploiting SQL injection and default credentials. Organisations should enforce strong authentication, patch known flaws, and harden internet-facing systems.

ATTACK TYPE	Cyber Crime, Emerging Threats	**SECTOR**	Healthcare, Government, Education, BFSI
REGION	Honduras, Mexico, Taiwan, Thailand	**APPLICATION**	Oracle, WordPress, Hikvision

Source - https://www.acronis.com/en/tru/posts/bossai-inside-the-ai-attack-mesh-that-targeted-taiwans-emergency-services/

TATA COMMUNICATIONS

Yoba malware abuses signed AI applications for DLL sideloading and cryptocurrency mining

Check Point Research has uncovered Yoba, a malware campaign exploiting surging interest in AI tools through fraudulent GitHub repositories impersonating ChatGPT and Claude desktop applications. Promoted via suspected SEO poisoning, the fake projects bundle legitimate, digitally signed OpenAI and Anthropic executables alongside a malicious DLL, which the trusted binary loads through DLL sideloading, a technique designed to bypass security protections.

The chain deploys YobaDropper and YobaLoader on Windows systems, employing prolonged execution delays, regional language filtering, and scheduled-task persistence to evade analysis and maintain access. The final payload observed was the XMRig cryptocurrency miner, though the loader can deliver other executables or PowerShell scripts. Organisations should source AI applications only from official vendors and monitor for unauthorised scheduled tasks.

ATTACK TYPE	Malware	**SECTOR**	IT Services and Consulting, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Windows, PowerShell, ChatGPT, Anthropic Claude

Source - https://gbhackers.com/yobaloader-malware/

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

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.

© 2026 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Private Limited.