TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: November 10, 2026



TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As November 2026 gets under way, the cyber threat landscape remains as unrelenting as ever, with threat actors devising increasingly sophisticated and coordinated campaigns across interconnected digital environments. Conventional defence models are being outpaced as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now hinges on organisations strengthening foundational security controls, adopting layered defence strategies, and weaving forward-looking intelligence throughout their operational frameworks.

In this rapidly shifting environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Issued weekly, it offers sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating 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.

INTRODUCTION

CYBERDAKAIT TROJAN TARGETS BANKING CUSTOMERS THROUGH PHISHING AND FAKE APPS

UNATTRIBUTED NETAMLOADER TARGETS A WINDOWS BUILD RESERVED FOR GOVERNMENT USE

OPEN-SOURCE AGENTIC AI FRAMEWORKS WEAPONISED TO AUTOMATE CYBER INTRUSIONS

TRUST#GRAFT HIJACKS WORDPRESS ADMIN SESSIONS TO INSTALL HIDDEN PHP BACKDOORS

CHINA- NEXUS STORM-2603 DEPLOYS WARLOCK RANSOMWARE AGAINST CRITICAL INFRASTRUCTURE

NEW BRONZE SANDCASTLE PLANTS IN-MEMORY BACKDOORS THROUGH DLL SIDELOADING

AOKIGAHARA HUNTS AI SESSION TOKENS TO UNLOCK REPOSITORIES, CLOUD ACCOUNTS, AND PIPELINES

SIRIUS BACKDOOR TARGETS WINDOWS VIA PHISHING EMAILS AND FILELESS CODE EXECUTION

MALICIOUS CODING EXTENSION ON A TRUSTED MARKETPLACE PLANTS AN SSH BACKDOOR ON DEVELOPERS' MACHINES

NEW DARKCORE RAT REUSES STOLEN SESSIONS TO IMPERSONATE VICTIMS ONLINE

TATA COMMUNICATIONS

CyberDakait malware drains banking users through malicious apps and SMS interception

Researchers have exposed CyberDakait, a financially motivated Android malware operation that has targeted Indian banking customers since July 2025. Using seven distinct trojan families, the campaign has compromised at least 17,960 devices and intercepted more than 7.6 million SMS messages. Attackers impersonate banks through fraudulent calls and messages, directing victims to phishing sites and malicious applications.

Once installed, the malware harvests banking credentials, card details, and identity information through convincing phishing screens, while intercepting OTPs to defeat two-factor authentication. Additional capabilities include call forwarding, remote command execution, and covert cryptocurrency mining, managed through a dedicated controller. The campaign poses serious financial and privacy risks. Users should never install banking apps shared via SMS or messaging links.

ATTACK TYPE	Phishing, Malware, Mobile, Emerging Threats	**SECTOR**	BFSI
REGION	India	**APPLICATION**	Android

Source - https://gbhackers.com/indian-banking-users-targeted/

INTRODUCTION | CYBERDAKAIT TROJAN TARGETS BANKING CUSTOMERS THROUGH PHISHING AND FAKE APPS | UNATTRIBUTED NETAMLOADER TARGETS A WINDOWS BUILD RESERVED FOR GOVERNMENT USE | OPEN-SOURCE AGENTIC AI FRAMEWORKS WEAPONISED TO AUTOMATE CYBER INTRUSIONS | TRUST#GRAFT HIJACKS WORDPRESS ADMIN SESSIONS TO INSTALL HIDDEN PHP BACKDOORS | CHINA- NEXUS STORM-2603 DEPLOYS WARLOCK RANSOMWARE AGAINST CRITICAL INFRASTRUCTURE | NEW BRONZE SANDCASTLE PLANTS IN-MEMORY BACKDOORS THROUGH DLL SIDELOADING | AOKIGAHARA HUNTS AI SESSION TOKENS TO UNLOCK REPOSITORIES, CLOUD ACCOUNTS, AND PIPELINES | SIRIUS BACKDOOR TARGETS WINDOWS VIA PHISHING EMAILS AND FILELESS CODE EXECUTION | MALICIOUS CODING EXTENSION ON A TRUSTED MARKETPLACE PLANTS AN SSH BACKDOOR ON DEVELOPERS' MACHINES | NEW DARKCORE RAT REUSES STOLEN SESSIONS TO IMPERSONATE VICTIMS ONLINE

TATA COMMUNICATIONS

Stealthy NetamLoader targets a government Windows build through software supply-chain attack

Researchers have uncovered NetamLoader, a previously unknown .NET and XAML-based loading framework used against a customised Windows 10 build reserved for government use in Asia. The malware was found inside a CAB archive within the Windows update folder, abusing a legitimate, signed patch-management component through AppDomainManager injection to trigger a deserialisation flaw and launch its chain.

The infection executes layered, encrypted XAML payloads, injecting into dllhost.exe before a final plugin polls a Cloudflare-hosted command server. To evade detection, NetamLoader bypasses AMSI scanning, disables .NET event tracing and deletes staging files, logs, and Prefetch artifacts. Kaspersky identified a single victim in Asia and could not attribute it to a known APT group. Organisations should monitor update directories.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Asia	**APPLICATION**	Windows

Source - https://securelist.com/netamloader/121676/

TATA COMMUNICATIONS

ARTEX and other agentic AI frameworks automate cyber attacks at unprecedented scale

Multiple threat actors are now abusing agentic AI frameworks to automate intrusions at unprecedented scale. According to CrowdStrike, the China-nexus group VAPOR PANDA used the open-source ARTEX framework, run on DeepSeek and a commercial large language model, to target more than 200 organisations across at least 14 countries, deploying the BLOODALCHEMY backdoor for espionage and credential theft at confirmed victims.

Separately, a financially motivated actor tracked as CRAFTY FALCON reportedly combined CyberStrikeAI, ARTEX derivatives, and the Cairn framework to target financial institutions, exploit cloud infrastructure, and compromise payment applications and cryptocurrency assets. Related frameworks, including PentAGI and Hexstrike, have surfaced in further campaigns. Organisations should monitor for agentic tooling on their networks and tighten egress controls to AI services.

ATTACK TYPE	Malware, Cyberespionage, Emerging Threats	**SECTOR**	Pharmaceuticals, Government, Aerospace, BFSI, Defence and Space Manufacturing, Telecommunications
REGION	Middle East, Europe, Asia, Global, United States, Latin America	**APPLICATION**	Windows, Microsoft Azure, AWS

Source - https://www.crowdstrike.com/en-us/blog/vapor-panda-uses-artex-to-scale-global-campaign/

TATA COMMUNICATIONS

WordPress administrator session abused to deploy the TRUST#GRAFT PHP backdoor

Researchers have identified TRUST#GRAFT, a JavaScript-to-WordPress attack chain that abuses an already authenticated administrator's browser to deploy a persistent PHP backdoor. No authentication vulnerability is exploited. Malicious JavaScript, often masked behind a fake Cloudflare-style verification screen, checks whether the visitor is a logged-in administrator before quietly reusing that trusted session to install a plugin.

The script extracts the WordPress nonce, uploads a staged archive, and activates a plugin disguised as Web Media Optimizer, which is in fact a backdoor. It copies itself into the must-use plugins directory for persistence, grants token-gated administrator access, and hides from plugin management views. The initial delivery route remains unconfirmed. Administrators should use a dedicated wp-admin browser profile.

ATTACK TYPE	Social Engineering, Cyber Crime	**SECTOR**	IT, Healthcare, Government, Transportation, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	WordPress

Source - https://www.securonix.com/blog/trust-graft-wordpress-admin-php-backdoor/

TATA COMMUNICATIONS

China-nexus Storm-2603 group exploits SharePoint flaws to deploy Warlock ransomware

Researchers have detailed a campaign by Longlegs, a China-nexus group also tracked as Storm-2603, deploying Warlock ransomware against critical infrastructure, government, and education targets. Over two months, the group struck four organisations, including a water utility and a telecommunications provider, across Portuguese and Spanish-speaking countries in Europe, Africa, and Latin America, by exploiting unpatched on-premises SharePoint servers.

After planting a web shell, the attackers spent around nine days moving through the network before deploying a signed but vulnerable driver to disable security software on roughly 40 hosts within hours. Warlock was then distributed through the domain's SYSVOL share and encrypted at least 33 machines. Organisations should patch SharePoint promptly, restrict vulnerable drivers, and monitor domain replication paths.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Government, Education, Telecommunications
REGION	Europe, Africa, Latin America	**APPLICATION**	Microsoft SharePoint Server

Source - https://blog.polyswarm.io/china-linked-warlock-ransomware-campaign-targets-critical-infrastructure

TATA COMMUNICATIONS

BRONZE SANDCASTLE deploys Meterpreter backdoors through stealthy DLL sideloading

Researchers have identified BRONZE SANDCASTLE, a suspected China-based espionage group active between August 2025 and August 2026. The group targeted organisations across Asia and Africa, with confirmed victims in the Philippines, Taiwan, Afghanistan, Namibia, and likely South Korea. Its signature technique is Sandboxie DLL sideloading, abusing a legitimate executable to load a malicious library.

Once the trusted application runs, the malicious DLL decodes an encrypted config.ini and executes a modified Meterpreter-based backdoor in memory, minimising static detection. The group also sideloads through Java, Krita, NVDA, and Sysinternals utilities to steal credentials and sensitive data. Organisations should monitor for anomalous DLL loading, inspect memory-resident activity, and apply the published indicators of compromise promptly.

ATTACK TYPE	Cyberespionage, APT, Emerging Threats	**SECTOR**	IT, Healthcare, Government, Transportation, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Afghanistan, Namibia, Philippines, South Korea, Taiwan	**APPLICATION**	Windows

Source - https://www.sophos.com/en-us/blog/bronze-sandcastle-deploys-modified-meterpreter-shells

TATA COMMUNICATIONS

Aokigahara malware targets AI assistant sessions, SSH keys, and cloud credentials together

Researchers have detailed Aokigahara, also tracked as Aoki, a Windows infostealer that has expanded well beyond browsers and cryptocurrency wallets. A dedicated collection module harvests local authentication files, session data, and settings from AI assistants including ChatGPT Desktop, Claude, Codex, Cursor, and GitHub Copilot, alongside tokens that could grant attackers access to victims' paid AI accounts.

A separate handler seeks out Git credentials, SSH private keys and AWS, Azure, and Google Cloud configuration files, exfiltrating the data over encrypted channels. Because AI tokens and developer secrets are stolen together, a single infection can cascade into compromised repositories, cloud resources, and deployment pipelines. Organisations should revoke exposed AI, Git, and cloud sessions and adopt short-lived credentials.

ATTACK TYPE	Cyber Crime, Malware, Emerging Threats	**SECTOR**	IT, Healthcare, Government, Transportation, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Azure, Windows, AWS, ChatGPT, CoPilot, GitHub, Cursor IDE, Gemini, Claude

Source - https://cybersecuritynews.com/aokigahara-malware/

TATA COMMUNICATIONS

Sirius backdoor blinds security tools and hijacks cryptocurrency transfers on Windows

Researchers have detailed a previously undocumented variant of the Sirius backdoor, delivered through spear-phishing emails impersonating FedEx billing notifications. A weaponised PDF triggers a multi-stage, largely fileless chain that loads the payload directly into memory. Using Early Bird APC injection and process hollowing, the malware conceals itself inside legitimate Windows processes such as msbuild.exe and svchost.exe.

Once active, Sirius establishes covert remote access with hidden desktop control and SOCKS5 pivoting, harvests Chromium browser credentials, captures webcam and microphone feeds, and swaps cryptocurrency wallet addresses in the clipboard. It patches Event Tracing for Windows to blind security monitoring and, notably, and survives a full operating system reset. Defenders should focus detection on the initial document trigger.

ATTACK TYPE	Phishing, Malware	**SECTOR**	BFSI, Transportation, Business, Logistics
REGION	Australia, Canada, Global, Europe, South Korea, United States	**APPLICATION**	Adobe Acrobat Reader, Chromium, Microsoft Defender, PowerShell, Windows

Source - https://gbhackers.com/sirius-backdoor-variant/

INTRODUCTION | CYBERDAKAIT TROJAN TARGETS BANKING CUSTOMERS THROUGH PHISHING AND FAKE APPS | UNATTRIBUTED NETAMLOADER TARGETS A WINDOWS BUILD RESERVED FOR GOVERNMENT USE | OPEN-SOURCE AGENTIC AI FRAMEWORKS WEAPONISED TO AUTOMATE CYBER INTRUSIONS | TRUST#GRAFT HIJACKS WORDPRESS ADMIN SESSIONS TO INSTALL HIDDEN PHP BACKDOORS | CHINA- NEXUS STORM-2603 DEPLOYS WARLOCK RANSOMWARE AGAINST CRITICAL INFRASTRUCTURE | NEW BRONZE SANDCASTLE PLANTS IN-MEMORY BACKDOORS THROUGH DLL SIDELOADING | AOKIGAHARA HUNTS AI SESSION TOKENS TO UNLOCK REPOSITORIES, CLOUD ACCOUNTS, AND PIPELINES | SIRIUS BACKDOOR TARGETS WINDOWS VIA PHISHING EMAILS AND FILELESS CODE EXECUTION | MALICIOUS CODING EXTENSION ON A TRUSTED MARKETPLACE PLANTS AN SSH BACKDOOR ON DEVELOPERS' MACHINES | NEW DARKCORE RAT REUSES STOLEN SESSIONS TO IMPERSONATE VICTIMS ONLINE

TATA COMMUNICATIONS

Trojanised Claude Code extension smuggles SSH backdoor via a trusted official marketplace

On 29 October 2026, a maliciously modified build of the Claude Code extension (version 2.1.313) was distributed through the Cursor Marketplace. Its JavaScript bundle carried a loader inserted ahead of the legitimate code, which collected system information, planted an unauthorised SSH key labelled svc-telemetry, attempted to enable the SSH service, and established a persistent reverse SSH tunnel to attacker infrastructure.

The loader also transmitted host reconnaissance data over unencrypted HTTP beacons to an attacker-controlled server. Cursor removed the package, which was live for roughly 11 hours, and reported up to 5,000 affected users. Uninstalling the extension does not remove the backdoor. Affected developers should delete the planted SSH key, terminate tunnel processes, and consider rebuilding compromised machines.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	IT and Software Development
REGION	Global	**APPLICATION**	Claude, Cursor IDE, Linux, macOS, OpenSSH, Windows

Source - https://opensourcemalware.com/blog/trojanized-claude-code-extension-plants-persistent-ssh-backdoor

TATA COMMUNICATIONS

DarkCore RAT hijacks browser sessions to access accounts and may bypass MFA

Researchers have uncovered DarkCore, a Windows-based remote access trojan advertised on cybercrime forums since August 2026. Written in native C++, it combines credential theft, hidden desktop access, file transfers, and reverse-proxy functionality. Its standout feature is a dedicated browser that reuses stolen session cookies to access services such as Gmail, WhatsApp, YouTube, and MediaFire as the victim.

By routing this activity through the victim's own IP address, DarkCore can make account access appear legitimate and potentially bypass repeated authentication and MFA prompts. Delivery uses a PDF-themed shortcut that opens a decoy report while downloading a separate executable. Researchers also recovered its configuration and direct TCP command-and-control endpoint. Organisations should prioritise session-token protection and endpoint monitoring.

ATTACK TYPE	Cyber Crime, Malware	**SECTOR**	BFSI, Government, IT, Social Media, Telecommunications
REGION	Global	**APPLICATION**	Chrome, Gmail, WhatsApp, Windows

Source - https://cybersecuritynews.com/new-darkcore-rat/

INTRODUCTION | CYBERDAKAIT TROJAN TARGETS BANKING CUSTOMERS THROUGH PHISHING AND FAKE APPS | UNATTRIBUTED NETAMLOADER TARGETS A WINDOWS BUILD RESERVED FOR GOVERNMENT USE | OPEN-SOURCE AGENTIC AI FRAMEWORKS WEAPONISED TO AUTOMATE CYBER INTRUSIONS | TRUST#GRAFT HIJACKS WORDPRESS ADMIN SESSIONS TO INSTALL HIDDEN PHP BACKDOORS | CHINA- NEXUS STORM-2603 DEPLOYS WARLOCK RANSOMWARE AGAINST CRITICAL INFRASTRUCTURE | NEW BRONZE SANDCASTLE PLANTS IN-MEMORY BACKDOORS THROUGH DLL SIDELOADING | AOKIGAHARA HUNTS AI SESSION TOKENS TO UNLOCK REPOSITORIES, CLOUD ACCOUNTS, AND PIPELINES | SIRIUS BACKDOOR TARGETS WINDOWS VIA PHISHING EMAILS AND FILELESS CODE EXECUTION | MALICIOUS CODING EXTENSION ON A TRUSTED MARKETPLACE PLANTS AN SSH BACKDOOR ON DEVELOPERS' MACHINES | NEW DARKCORE RAT REUSES STOLEN SESSIONS TO IMPERSONATE VICTIMS ONLINE

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.