TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: November 03, 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 tightly coordinated campaigns across deeply 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

FAST-GROWING N0N GROUP PRESSURES VICTIMS BY PUBLISHING STOLEN CORPORATE DATA ONLINE

CRITICAL PHP CORE FLAWS AND DUPLICATOR INJECTION BUG DEMAND URGENT PATCHING

BLACKLOTUS BOOTKIT EXPLOITS CVE-2022-21894 TO TARGET GOVERNMENT AGENCIES

MASS EXPLOITATION OF FIREWALL AND VPN FLAWS YIELDS OVER 70,000 STOLEN CREDENTIALS

HIRUDO MALWARE PERSUADES VICTIMS TO SWAP GENUINE BANKING APPS FOR TROJANISED VERSIONS

YUANKONG ANDROID RAT STEALS BANKING PINS BY ABUSING ACCESSIBILITY AND WIRELESS DEBUGGING

NEEDYMANTIS BACKDOOR HELPS ATTACKERS MAINTAIN ACCESS INSIDE BREACHED NETWORKS

GHOSTACTION CAMPAIGN HIJACKS DEVELOPER ACCOUNTS TO STEAL SECRETS AT MASSIVE SCALE

OPERATION FLASHHOLE ABUSES FINANCIAL SECURITY SOFTWARE TO FUEL ESPIONAGE CAMPAIGN

STEALC INFOSTEALER RETURNS AS NEW STADIA RAT MALWARE AFTER TAKEDOWN

TATA COMMUNICATIONS

N0n data extortion group names 38 maritime and logistics organisations globally

A newly emerged data-extortion group known as N0n, first observed posting victims on its Tor leak site on 18 September 2026, has rapidly expanded operations across multiple industries. In a single batch on 12 October, it named 38 maritime, port, and logistics organisations spanning 18 countries and territories, more than doubling its previously recorded victim count almost overnight.

Unlike traditional ransomware, N0n has not deployed a publicly confirmed file encryptor. It threatens to publish allegedly stolen data unless victims pay. Its leak site has recorded 76 entries representing roughly 64 to 66 distinct entities, functioning as a public pressure scoreboard. The activity raises concerns over commercial information exposure, third-party supply-chain risk, and secondary fraud against affected organisations.

ATTACK TYPE	Ransomware, Emerging Threats	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Construction, Government, ISP, E-Commerce, Retail and Distribution, Logistics
REGION	Argentina, Australia, Luxembourg, South Korea, United States, Venezuela, Vietnam	**APPLICATION**	Windows

Source - https://www.provendata.com/blog/n0n-ransomware

INTRODUCTION
FAST-GROWING N0N GROUP PRESSURES VICTIMS BY PUBLISHING STOLEN CORPORATE DATA ONLINE
CRITICAL PHP CORE FLAWS AND DUPLICATOR INJECTION BUG DEMAND URGENT PATCHING
BLACKLOTUS BOOTKIT EXPLOITS CVE-2022-21894 TO TARGET GOVERNMENT AGENCIES
MASS EXPLOITATION OF FIREWALL AND VPN FLAWS YIELDS OVER 70,000 STOLEN CREDENTIALS
HIRUDO MALWARE PERSUADES VICTIMS TO SWAP GENUINE BANKING APPS FOR TROJANISED VERSIONS
YUANKONG ANDROID RAT STEALS BANKING PINS BY ABUSING ACCESSIBILITY AND WIRELESS DEBUGGING
NEEDYMANTIS BACKDOOR HELPS ATTACKERS MAINTAIN ACCESS INSIDE BREACHED NETWORKS
GHOSTACTION CAMPAIGN HIJACKS DEVELOPER ACCOUNTS TO STEAL SECRETS AT MASSIVE SCALE
OPERATION FLASHHOLE ABUSES FINANCIAL SECURITY SOFTWARE TO FUEL ESPIONAGE CAMPAIGN
STEALC INFOSTEALER RETURNS AS NEW STADIA RAT MALWARE AFTER TAKEDOWN

TATA COMMUNICATIONS

PHP2Shell and Duplicator flaws enable unauthenticated RCE and PHP object injection

Two critical PHP core vulnerabilities, CVE-2026-109618 and CVE-2026-109619 (CVSS v4.0: 9.2), collectively dubbed PHP2Shell, enable unauthenticated remote code execution and were patched in an emergency release on 21 October 2026. The flaws stem from out-of-memory corruption and stale request-owned global state, and affect virtually all PHP installations serving web requests, including PHP-FPM, Apache mod_php, and LiteSpeed deployments.

Separately, CVE-2026-82814 is a high-severity PHP object injection flaw in the Duplicator Free and Pro plugins for WordPress, while CVE-2026-115560 affects PHP session handling under specific configurations. Compounding the risk, public proof-of-concept exploits and advanced attack chains, targeting PHP2Shell, have emerged, alongside suspected DPRK-linked activity and reported attempts to deploy the Mirai-derived Potassium botnet. Immediate patching is essential.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Government, Transportation, Military, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Palo Alto Networks PAN-OS, WordPress, PHP, Okta

Source - https://cybersecuritynews.com/php-early-exploitation-attempts/

TATA COMMUNICATIONS

APT41 BlackX UEFI bootkit exploits unpatched Baton Drop flaw to defeat Secure Boot

Researchers have identified BlackX, a UEFI bootkit used in an early-2026 espionage campaign against diplomatic agencies in Tajikistan, Turkmenistan, and Uzbekistan. A derivative of the notorious BlackLotus, it exploits the Baton Drop vulnerability (CVE-2022-21894) to bypass Windows Secure Boot. Although Microsoft patched the flaw in 2022, the fix required manual revocation steps that many organisations never applied.

After gaining administrator access, attackers enrol attacker-controlled keys to load the bootkit, which injects a signed malicious driver into the Windows kernel to disable security monitoring. It then deploys espionage payloads, including a remote access trojan, exfiltrating data through cloud services such as Google Drive and OneDrive. Attributed to APT41 with medium confidence, the campaign underlines firmware-level risks.

ATTACK TYPE	Vulnerability, Malware, Cyberespionage, APT	**SECTOR**	Government
REGION	Tajikistan, Turkmenistan, Uzbekistan, Central Asia	**APPLICATION**	Windows, Microsoft OneDrive, Google Drive

Source - https://securelist.com/uefi-bootkit-blackx/121539/

TATA COMMUNICATIONS

k0t exploits FortiWeb and GlobalProtect flaws to harvest more than 70,000 credentials

A joint investigation has exposed a large-scale campaign by a threat actor tracked as k0t, targeting internet-facing Fortinet FortiGate and FortiWeb appliances and Palo Alto Networks GlobalProtect gateways. Combining vulnerability exploitation with brute-force attacks, the operation harvested more than 70,000 exposed credentials and related records, including LDAP and Active Directory details, from organisations worldwide.

Observed activity included credential theft, persistent remote access, and data exfiltration, with victims concentrated across Asia-Pacific and Latin America. Group-IB assesses that k0t may operate as an initial access broker. Although victim overlap with the Qilin and The Gentlemen ransomware groups was noted, no direct affiliation is confirmed. Organisations should enforce multi-factor authentication and patch edge devices promptly.

ATTACK TYPE	Vulnerability, Cyber Crime, Breaches	**SECTOR**	Healthcare, Manufacturing, Government, Education, ISP, Energy, BFSI, IT Services and Consulting, Telecommunications
REGION	North America, Europe, APAC, Latin America	**APPLICATION**	Fortinet FortiGate, Palo Alto Networks GlobalProtect, Palo Alto Networks PAN-OS, Fortinet FortiWeb WAF, Sonicwall SMA, Cisco ISE

Source - https://securityonline.info/k0t-fortigate-globalprotect-attacks/

TATA COMMUNICATIONS

Hirudo Android RAT targets banking users through trojanised application replacements

Researchers have identified Hirudo, an Android banking trojan and remote access tool that steals credentials and enables live device control. Distributed through lure apps disguised as shopping, adult-video, and short-drama services, it uses fake update prompts to persuade victims to uninstall genuine banking apps and install patched replacements that disable the banks' own security checks from within.

An internal hooking engine blinds signature, Accessibility, and Play Integrity checks, aided by a publicly leaked attestation keybox whose certificates already appear on Google's revocation list. Purpose-built replacements target eight Indonesian banking apps, while credential theft spans several further countries. An exposed backend analysed in August 2026 held thousands of records. Users should install apps only from official stores.

ATTACK TYPE	Malware, Mobile, Emerging Threats	**SECTOR**	BFSI
REGION	India, China, Indonesia, Mexico, Morocco, Thailand	**APPLICATION**	Android

Source- https://securityonline.info/hirudo-banking-trojan-android-apps/

TATA COMMUNICATIONS

YuanKong RAT abuses accessibility features to steal banking PINs and control phones

Researchers at STAR Labs have identified YuanKong, an Android remote access trojan that abuses the platform's Accessibility features to steal banking credentials and seize control of infected devices. It reads on-screen content and the accessibility tree to capture passwords and payment PINs, without requesting access to SMS or contacts.

Distinct operator identifiers embedded in each build point to a shared service used by multiple operators. Beyond screen capture and remote control, YuanKong abuses Wireless Debugging to self-pair with the device's own ADB service, gaining a shell-level session that strengthens persistence and resists removal. Users should avoid sideloading apps and revoke accessibility permissions from any untrusted application immediately.

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

Source - https://cybersecuritynews.com/new-yuankong-android-rat/

TATA COMMUNICATIONS

Stealthy NeedyMantis uses DLL sideloading to sustain covert access in targeted intrusions

Microsoft Threat Intelligence has detailed NeedyMantis, a modular post-compromise malware family deployed in targeted intrusions since at least October 2025. It is installed once attackers are already inside a network, maintaining long-term, covert control. Observed victims span telecommunications providers, universities, intergovernmental organisations, medical non-profits, and government contractors, indicating a focus on high-value targets.

Microsoft uncovered the family while pivoting from indicators tied to the DAEMON Tools supply-chain compromise, linking at least one operator, Storm-3069, to its use. NeedyMantis relies on DLL sideloading through legitimate signed applications, obfuscated loaders, and modular command-and-control over encrypted channels. Its stealth and anti-analysis features hamper detection. Organisations should hunt for the published indicators and strengthen endpoint monitoring.

ATTACK TYPE	Malware, Cyberespionage, Supply Chain	**SECTOR**	Healthcare, Government, Education, International Trade and Development, Telecommunications
REGION	Global	**APPLICATION**	7-Zip, Windows, NVIDIA, Intel

Source - https://www.microsoft.com/en-us/security/blog/2026/09/28/needymantis-unpacking-a-post-compromise-malware-family-used-in-targeted-operations/

TATA COMMUNICATIONS

GhostAction escalates theft of CI/CD secrets and cloud credentials from repositories

GhostAction is a supply-chain campaign that compromises GitHub accounts to steal CI/CD secrets and cloud credentials. Using stolen personal access tokens, often harvested from infostealer logs, attackers inject a malicious workflow disguised as a security audit into repositories, including Uber's athenadriver. Newer variants scan both active files and entire Git histories, exposing API keys, SSH credentials, and package-registry tokens.

The campaign escalated sharply in October 2026, with researchers reporting around 1,900 compromised accounts targeting more than 30,000 repositories in a matter of days. Although GitHub began blocking the malicious workflow on 9 October, exposed secrets remain a serious risk, enabling unauthorised access and operational disruption. Organisations should rotate all potentially exposed credentials and audit their repository histories without delay.

ATTACK TYPE	Cyber Crime, Phishing, Malware, Supply Chain	**SECTOR**	IT and Software Development
REGION	Global	**APPLICATION**	GitLab Community Edition (CE), VS Code, Python Package Index (PyPI), GitHub

Source - https://cyberpress.org/ghostaction-targets-github-secrets/

TATA COMMUNICATIONS

Lazarus Group turns trusted security software into a covert malware delivery channel

Researchers at Kaspersky have attributed Operation FlashHole, a cyberespionage campaign running since July 2025, to the North Korea-linked Lazarus Group. The operation has targeted South Korean organisations across the software, construction, and manufacturing sectors. Using spear-phishing emails and fake résumé and portfolio websites, the attackers are believed to have abused mandatory INISAFE CrossWeb EX software to trigger in-memory malware execution.

The campaign deployed a modular malware framework comprising TechHub, TouchHub, ClientHub, Cubridge, and the long-running LPEClient, chaining downloaders, loaders, and profiling tools largely in memory. For command-and-control, the operators abused GitHub, compromised websites, and Dropbox to blend into trusted traffic. Notably, LPEClient employed post-quantum encryption to conceal its payloads. Organisations should patch CrossWeb EX and monitor for anomalous process behaviour.

ATTACK TYPE	Phishing, Malware, Cyberespionage	**SECTOR**	Manufacturing, Construction, Software Development
REGION	South Korea	**APPLICATION**	Microsoft Active Directory Services, Microsoft Edge, Windows, Google Chrome, GitHub

Source - https://cybersecuritynews.com/north-korean-hackers/

TATA COMMUNICATIONS

Disrupted StealC infostealer returns as Stadia RAT with expanded control capabilities

Researchers at Varonis Threat Labs have detailed Stadia, a Windows-based remote access trojan that repackages the disrupted StealC infostealer into a far broader intrusion platform. Advertised on 16 October 2026, roughly four months after Europol's Operation Endgame dismantled StealC's infrastructure, Stadia reuses StealC version 3.5 code byte for byte, including an identical Chromium App-Bound Encryption helper confirming the lineage.

Sold via subscription, Stadia offers six modules: the original stealer plus hidden desktop access, a remote command shell, a loader, a file explorer, and process manager. It harvests browser credentials, cryptocurrency wallets, and messaging data, communicating with its servers over disguised, encrypted traffic and persisting through hidden scheduled tasks. Organisations should strengthen endpoint detection and monitor for the published indicators.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Africa, South Asia, Latin America	**APPLICATION**	Microsoft Outlook, Mozilla Thunderbird, OpenVPN, Windows, Google Chrome, Telegram, Discord

Source - https://www.varonis.com/blog/stealc-returns

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.