TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 23, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

The cyber threat landscape is evolving as 2025 draws to a close, driven by increasingly sophisticated hostile activities. Traditional defence models are proving inadequate as threats exploit the structural vulnerabilities of highly interconnected digital ecosystems. To maintain resilience and strategic advantage, organisations must strengthen foundational security frameworks, deploy multi-layered defences, and embed anticipatory intelligence throughout their architectures.

In this high-stakes environment, Tata Communications' Cyber Threat Intelligence report becomes indispensable. Published weekly, the report delivers an incisive analysis of emerging attack campaigns, evolving adversarial tactics, and sector-specific exposures. By translating intelligence into immediate defensive action, security teams can anticipate, prepare for, and neutralise threats proactively — safeguarding critical operations before disruption takes hold.

TATA COMMUNICATIONS

Emerging Tengu ransomware uses double extortion and credential abuse techniques

Tengu is a newly observed Ransomware-as-a-Service (RaaS) operation first detected in October 2025, notable for hands-on keyboard intrusions and a classic double-extortion methodology. Operators abuse valid credentials and exposed remote access, leverage LOLBins and living-off-the-land techniques for stealth, and conduct credential theft, lateral movement and discovery. Post-compromise steps include shadow copy deletion and log tampering to hinder recovery and forensic analysis.

Once inside a network, Tengu stages and compresses sensitive data before bulk exfiltration via tools such as Rclone and WinSCP over encrypted channels. Following data theft, it deploys a .NET encryptor, directs victims to Tor-based negotiation portals, and threatens public leakage on dedicated sites if ransoms remain unpaid. The group has been linked to attacks against entities in multiple sectors.

ATTACK TYPE	Ransomware	**SECTOR**	Manufacturing, Education, Energy, Food and Beverage Service
REGION	Brazil, Iran, Morocco, Spain, United Arab Emirates	**APPLICATION**	Windows

Source - https://www.redpiranha.net/news/threat-intelligence-report-october-21-october-27-2025 , https://www.shenouda.nl/new-threat-actor-tengu/

Coinbase Cartel uses staged leaks to pressure cloud vulnerabilities globally

Emerging in September 2025, Coinbase Cartel is a sophisticated data-extortion group formed by affiliates of ShinyHunters and Lapsus$, distinguished by its departure from traditional ransomware encryption. Instead, it prioritises covert data theft through insider bribery, vishing, OAuth abuse and cloud-focused exfiltration scripts before publicly threatening staged leaks. The group's advanced evasion and collaboration tactics are amplifying pressure on victims across sectors globally, reshaping extortion dynamics.

Intelligence indicates Coinbase Cartel leverages social engineering, credential abuse and cloud misconfiguration to penetrate targets, often mimicking legitimate tools for stealthy extraction without encryption activity. Its evolving techniques include ESXi-targeting loaders and long-lived OAuth tokens to maintain persistence and disrupt recovery. As leak sites and partnerships proliferate, organisations must strengthen defences against this rising extortion threat.

ATTACK TYPE	Ransomware	**SECTOR**	Legal services, Manufacturing, IT, BFSI, Broadcast Media Production and Distribution, Telecommunications, Logistics
REGION	Europe, Canada, India, Japan, Israel, South Korea, United Arab Emirates, United States	**APPLICATION**	VMWare ESXi, Windows, Salesforce

Source - https://izoologic.com/region/uk/coinbase-cartel-a-newly-emerged-ransomware-group-redefinisng-data-extortion/ , https://www.linkedin.com/pulse/new-threat-actor-coinbase-cartel-joe-shenouda-m2lue/

TATA COMMUNICATIONS

Hacktivist groups escalate cyber disruptions targeting regional critical infrastructure

Over the past fortnight, threat activity across the Middle East intensified, with the UAE and Saudi Arabia most affected. Incidents ranged from data breaches and initial-access brokerage to DDoS campaigns, website defacements and ransomware. Activity levels indicate coordinated, financially motivated operations alongside opportunistic disruption, increasing pressure on organisations' perimeter security, identity controls and incident response readiness.

A notable development is the rapid escalation of Coinbase Cartel operations, a newer cluster showing overlaps with scattered LAPSUS$ hunters. The group has focused aggressively on UAE-based real estate, financial services and business-services firms. Concurrent hacktivist actions and ransomware intrusions continue to broaden exposure across government, BFSI, logistics, education and contracting sectors within the region.

ATTACK TYPE	Ransomware, Hacktivism, Breaches, DDOS	**SECTOR**	Healthcare, Hospitality, Manufacturing, IT, Government, Education, Business, BFSI, Aviation, Broadcast Media, Retailer, Telecommunications
REGION	Middle East, Oman, Saudi Arabia, United Arab Emirates	**APPLICATION**	Generic

Source - Cyber Threat Intel Team-Internal Research

TATA COMMUNICATIONS

Coordinated hacktivist and DDOS operations target government and education sectors

Cyber activity targeting India intensified in recent months, with hacktivist collectives conducting widespread website defacements and sustained DDoS campaigns that disrupted government portals, educational institutions and small-to-medium enterprises. Industry trackers and national reports note a marked rise in such low-cost, high-visibility attacks that amplify operational disruption and increase exposure for under-resourced organisations, and compromise public trust.

Concurrent ransomware campaigns impacted Indian IT, industrial, legal and service enterprises, with emergent families such as Kill Security, TENGU, Kairos and Sinobi implicated in extortion and selective data theft. Public leak sites, access listings and unverified disclosures have multiplied risk vectors, complicating incident response and escalating potential operational and regulatory fallout across critical digital ecosystems.

ATTACK TYPE	Ransomware, Hacktivism, Breaches, DDOS, Cyberespionage	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Government, Education, Media Production, Retailer, Telecommunications
REGION	India	**APPLICATION**	Generic

Source - Cyber Threat Intel Team-Internal Research

Shanya tool provides ransomware groups with sophisticated payload obfuscation

Shanya is a new packer-as-a-service rapidly gaining traction in the ransomware ecosystem, effectively succeeding tools such as HeartCrypt by offering advanced obfuscation and evasion techniques. It provides obfuscated loaders, Windows AMSI bypass, anti-VM/sandbox checks, API hashing and stealthy portable executable replacement. These capabilities enable attackers to evade endpoint detection and response (EDR) and inject payloads via DLL side-loading.

Security researchers note Shanya's adoption by multiple ransomware operations, including Akira, Qilin, Crytox, Medusa and CastleRAT campaigns across various regions. The service can facilitate EDR-killer drivers to disable security software before execution, broadening access to sophisticated attack chains for lower-skill actors. Its rise underscores an ongoing shift towards commoditised, stealth-focused malware tooling in today's threat landscape.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	Business, Hospitality
REGION	China, Costa Rica, Nigeria, Pakistan, Tunisia, United Arab Emirates	**APPLICATION**	Windows

Source - https://news.sophos.com/en-us/2025/12/06/inside-shanya-a-packer-as-a-service-fueling-modern-attacks/

TATA COMMUNICATIONS

Rust-based 01flip ransomware uses Sliver framework for lateral network movement

Security researchers have identified a new Rust-based ransomware family designated 01flip, observed in limited attacks across the Asia-Pacific region and linked to activity cluster CL-CRI-1036. 01flip targets both Windows and Linux systems, leveraging post-exploitation tooling such as Sliver for reconnaissance, credential access and lateral movement before deploying its encryption routines.

Once executed, 01flip conducts structured encryption using AES-128-CBC and RSA-2048 cyphers, appending a .01flip extension to affected files, dropping ransom notes and then self-deleting to hinder analysis. Early victims include organisations responsible for critical infrastructure, and Unit 42 researchers have observed alleged dark-web data sale activity linked to the campaign, underscoring evolving threats posed by Rust-compiled malware.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, IT, Government, Defence Industry, BFSI, Aviation, Retailer, Telecommunications
REGION	Philippines, Taiwan, South Asia, East Asia, APAC	**APPLICATION**	Windows, Linux, Zimbra Collaboration, Zimbra desktop client

Source - https://unit42.paloaltonetworks.com/new-ransomware-01flip-written-in-rust/

TATA COMMUNICATIONS

DeadLock attackers disable security defence through kernel-level driver vulnerability

Researchers have identified a financially motivated threat actor employing a novel BYOVD loader to deploy DeadLock ransomware by exploiting a vulnerability in a Baidu Antivirus driver (CVE-2024-51324). The actor used the compromised driver to terminate endpoint detection and response tools at the kernel level, before executing a UAC-bypassing PowerShell script that disables Windows Defender and deletes shadow copies.

Following initial defence evasion, the adversary leveraged valid credentials to enable RDP and install AnyDesk for remote access, carried out system reconnaissance, and finally executed a bespoke time-seeded stream-cypher encryptor that selectively targets files while employing anti-forensics measures to hinder recovery. Talos noted the sophisticated encryptor and preparatory script significantly complicate forensic analysis and restoration efforts in affected Windows environments.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Hospitality, Manufacturing, IT, Government, Energy, Business, BFSI, Aviation, Retailer, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Windows

Source - https://blog.talosintelligence.com/byovd-loader-deadlock-ransomware/

TATA COMMUNICATIONS

Fraud APK Using VPN harvests credentials through fraudulent payment workflows

A sophisticated fraudulent “RTO Challan/e-Challan” Android APK has been identified spreading via WhatsApp, masquerading as an official traffic fine alert. The malicious app uses a two-stage dropper and heavy code obfuscation to install stealthily, creates a custom VPN tunnel to evade detection, and harvests personal, device, SIM, SMS, OTP and banking data. It also presents a fake payment interface to steal financial credentials.

Analysis reveals the malware exfiltrates data to Base64-encoded command-and-control domains such as jsonserv[.]xyz/biz, enables SMS/OTP interception and call manipulation, and deceives users into entering sensitive information under the guise of a ₹1 challan payment verification. This coordinated campaign poses severe risks of identity theft and financial fraud, underscoring the need for heightened detection, user awareness and mitigation efforts.

ATTACK TYPE	Phishing, Malware	**SECTOR**	Financial services, BFSI, Retailer and Distributor, Telecommunications
REGION	India	**APPLICATION**	Android, WhatsApp

Source - https://www.cyfirma.com/research/rto-challan-fraud-a-technical-report-on-apk-based-financial-and-identity-theft/

TATA COMMUNICATIONS

ZnDoor malware deployed via React2Shell targets React and Next.js environments

Since December 2025, Japanese cybersecurity teams have reported multiple incidents exploiting the critical React2Shell vulnerability (CVE-2025-55182) to deploy a previously unidentified malware now designated ZnDoor. Observed primarily in vulnerable React and Next.js environments, attackers leverage remote code execution to install the malware, which subsequently initiates persistent communication with its command-and-control infrastructure, highlighting the rapid weaponisation of this flaw in real-world attacks.

Analysis indicates that ZnDoor functions as a full-featured remote access trojan, providing SOCKS5 proxying, remote command execution, file operations and evasion techniques to maintain persistence on compromised systems. The malware's deployment underscores the urgent need for organisations to patch affected frameworks and monitor for indicators of compromise, as exploitation of the React2Shell flaw continues to facilitate sophisticated unauthorised access.

ATTACK TYPE	Malware, Vulnerability	**SECTOR**	IT
REGION	Japan	**APPLICATION**	Linux, Next.js, React

Source - https://jp.security.ntt/insights_resources/tech_blog/react2shell_malware_zndoor/

TATA COMMUNICATIONS

Active exploitation of CVE-2025-55182 delivers multi-stage Linux malware

Following the public disclosure of CVE-2025-55182, also known as React2Shell, on 3 December 2025, threat actors rapidly began exploiting this critical unauthenticated remote code execution vulnerability in React Server Components. Google Threat Intelligence Group has reported diverse campaigns deploying tunnelling tools, downloaders and backdoors, underscoring the significant risk to unpatched React and Next.js workloads in internet-facing environments.

Observed payloads include MINOCAT, SNOWLIGHT, HISONIC, COMPOOD, ANGRYREBEL.LINUX, and illicit cryptocurrency mining via XMRIG, illustrating extensive post-compromise abuse. These activities are attributed to both China-nexus espionage groups and financially motivated actors, emphasising the urgency for organisations to patch affected React Server Components and strengthen detection and mitigation controls to counter this widespread exploitation.

ATTACK TYPE	Malware, APT, Vulnerability	**SECTOR**	Healthcare, Manufacturing, IT, Government, Defence Industry, BFSI, Aviation, Retailer, Telecommunications
REGION	Global	**APPLICATION**	Windows, Linux, MacOS, React

Source - https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-exploit-react2shell-cve-2025-55182/

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