TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 20, 2025

THREAT INTELLIGENCE ADVISORY REPORT

In today's fast-changing digital landscape, organisations must adopt proactive cybersecurity measures to combat rising threats. Our weekly Cyber Threat Intelligence (CTI) reports provide critical insights into emerging risks, vulnerabilities, and attack trends, empowering businesses to fortify defences and stay ahead of cyber adversaries.

Through expert analysis and actionable strategies, we help clients anticipate, detect, and neutralise threats before they escalate. This proactive approach not only protects critical assets, but also ensures business continuity and strengthens stakeholder confidence. With our CTI insights, organisations can build long-term cyber resilience, navigating the digital world with greater security and assurance.

Hacktivist cyberattacks against India continue into May

Hacktivist groups such as Nation of Saviors, AnonSec, Sylhet Gang-SG, and Islamic Hacker Army have escalated cyberattacks against the Indian government, as well as the defence and education sectors, in May 2025. These campaigns, driven by political motives, are focused on Distributed Denial of Service (DDoS) attacks and website defacements. Attackers aim to disrupt operations and push ideological narratives through visible, high-impact disruptions. Their coordinated efforts highlight the growing influence of hacktivist collectives and the vulnerabilities in public-sector digital infrastructure.

Organisations targeted by these attacks must prioritise hardening internet-facing services and deploying Web Application Firewalls (WAFs) to protect public portals. DDoS mitigation tools, such as content delivery networks (CDNs) with rate-limiting and traffic scrubbing, are essential. Security Information and Event Management (SIEM) systems should be configured to detect defacement indicators and abnormal traffic surges. Regular website backups and secure recovery plans will aid in restoring services swiftly after the attacks. Collaborations with national CERTs, proactive monitoring, and public communication strategies can help mitigate reputational damage and operational impact.

ATTACK TYPE	Hacktivist	**SECTOR**	Government, Military, and Defence Industry
REGION	India	**APPLICATION**	Generic

Source - Tata Communications Threat Intel

INTRODUCTION | HACKTIVIST STORM CONTINUES TO TARGET INDIA DURING INTENSIFIED INDO-PAK TENSIONS | ANARCHYRANSOM PLAYS MIND GAMES WITH VICTIMS | LAMPION MALWARE CLICKFIXES ITS WAY INTO PORTUGUESE NETWORKS | BPFDOOR: LINUX BACKDOOR THAT DODGES DETECTION | PAKISTAN-ALIGNED APTS RAMP UP INDIAN ESPIONAGE AMID RECENT CROSS-BORDER CONFLICT | AGENDA RANSOMWARE DEPLOYS NEW LOADER FOR STEALTH ATTACKS | DOGE BIG BALLS: RIDICULOUS NAME, SERIOUS THREAT | JAVA RAT SNEAKS INTO SOUTHERN EUROPE WITH GEOFENCED INVOICES | FAKE AI VIDEO SITES SPREAD NOODLOPHILE MALWARE | OTTERCOOKIE EXPANDS TO MACOS FOR GLOBAL FINANCIAL ESPIONAGE

AnarchyRansom uses fear and deception to wreak havoc

AnarchyRansom is a ransomware strain that encrypts victims' data, appending a ".ENCRYPTED" extension and demanding payment for file recovery. Its ransom notes often promise a "free trial" decryption to build trust, but cybersecurity experts warn that payments rarely result in full data restoration. The malware is spread primarily through phishing and malicious downloads, targeting a wide range of Windows-based systems globally. Its psychological manipulation tactics increase urgency and pressure on victims.

Organisations must combat AnarchyRansom through a multi-layered cybersecurity strategy. Email filtering, anti-phishing training, and application allow-listing are key to blocking initial infection vectors. Reliable, versioned backups stored offline are critical for restoring data without negotiating with attackers. Incident response teams should prepare ransomware-specific playbooks, including protocols for containment, evidence collection, and legal coordination. EDR solutions that detect file encryption patterns and lateral movement can help stop infections early. Sharing threat indicators through ISACs or threat intel platforms ensures improved awareness and coordinated defence across sectors.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyclonis.com/remove-anarchyransom-ransomware/

Lampion Infostealer uses ClickFix trick to target Portugal

A new malware campaign in Portugal is delivering the Lampion infostealer through a deceptive “ClickFix” method that tricks users into executing malicious PowerShell under the guise of system repair. The campaign targets government, financial, and transportation sectors using obfuscated multi-stage payloads, task scheduling, and loaders to evade detection. Lampion collects sensitive credentials and data, posing a severe threat to institutional security.

Organisations should educate users about social engineering lures disguised as IT fixes or “cleaners”. Application Control and PowerShell execution restrictions can prevent unauthorised script activity. Advanced EDR tools should monitor task scheduler abuse, command-line anomalies, and behaviour consistent with infostealers. Email security solutions must detect and quarantine suspicious attachments and URLs. Regular system auditing and credential hygiene are also important, particularly in high-trust environments like finance and government. Threat intelligence feeds should include detection rules for Lampion’s known patterns and infrastructure to enable proactive blocking.

ATTACK TYPE	Malware	SECTOR	Government, Transportation and BFSI
REGION	Global	APPLICATION	Windows

Source - https://unit42.paloaltonetworks.com/lampion-malware-clickfix-lures/

BPFDoor: Stealthy Linux malware evades detection

BPFDoor is a Linux-based backdoor malware used by China-linked APT group Earth Bluecrow. It exploits the Berkeley Packet Filter (BPF) system to create covert network channels and maintain persistent access across TCP, UDP, and ICMP protocols. BPFDoor employs anti-forensic techniques such as process name spoofing, custom “magic bytes” in packets, and encrypted reverse shells. Its advanced evasion capabilities make it extremely difficult to detect using traditional Linux defences.

To defend against BPFDoor, telecom and critical infrastructure organisations must implement behaviour-based monitoring and endpoint telemetry collection for Linux systems. Security teams should inspect BPF filters, review kernel-level activity, and deploy tailored YARA rules to catch anomalies in process names and network behaviour. Firewalls should be configured to flag suspicious ICMP or UDP traffic. Since BPFDoor operates covertly for extended periods, regular forensic reviews and log audits are essential. Enterprises should also monitor for unusual persistence mechanisms and maintain up-to-date Linux threat detection signatures.

ATTACK TYPE	Malware	**SECTOR**	Telecommunications
REGION	South Korea	**APPLICATION**	Linux

Source - https://medium.com/s2wblog/detailed-analysis-of-bpfdoor-targeting-south-korean-company-328171880a98

Pakistan-backed APTs escalate targeting of Indian infrastructure

Several Pakistan-aligned APT groups such as APT36 (Transparent Tribe), SideCopy, Cosmic Leopard, and Gorgon Group continue to target Indian defence, education, and infrastructure sectors. These operations leverage geopolitical tensions and use spear-phishing, malicious documents, and backdoors to infiltrate and maintain access to critical systems. Emerging threats include ransomware-as-a-cover operations and opportunistic malware implants used for long-term espionage.

Defending against these threats requires robust email filtering, user awareness training, and monitoring of endpoints for signs of compromise. Organisations should deploy EDR tools with memory scanning, behaviour-based anomaly detection, and sandboxing for document attachments. Network segmentation and privileged access controls help contain potential breaches. Indian government agencies and private infrastructure providers must share threat intelligence and coordinate defensive strategies with CERT-IN and allied partners. Simulated red-team exercises and risk-based asset prioritisation should also be used to test resilience against APT campaigns that target national interests.

ATTACK TYPE	Malware	SECTOR	Government, Education, Military, Defence and Space Manufacturing
REGION	India	APPLICATION	Windows, Linux

Source - https://medium.com/@DarkKnightt/threat-actor-profiling-pakistan-cyber-threat-actors-targeting-india-3aee5ab55e8e

Agenda ransomware evolves with NETXLOADER and SmokeLoader

The Agenda ransomware group has ramped up its operations with the introduction of SmokeLoader and a new, stealthy .NET-based loader called NETXLOADER. These tools enable highly obfuscated, in-memory malware execution, making detection difficult and prolonging dwell time within networks. Targeting industries across India, Brazil, the U.S., and beyond, Agenda's campaigns focus on healthcare, finance, telecommunications, and IT sectors. Their evolving toolset reflects increasing sophistication and intent to evade even advanced security defences.

Organisations must respond with advanced behavioural analysis tools capable of detecting reflective DLL loading and in-memory execution. EDR/XDR platforms with script-blocking and real-time telemetry are essential. Network defenders should analyse lateral movement patterns, credential abuse, and unusual process trees. Blocking outbound connections to known malicious IPs and C2 infrastructure can help stop data exfiltration. Patch hygiene, strict access policies, and multi-factor authentication (MFA) reduce the initial attack surface. Backup systems must be segmented, versioned, and tested regularly for ransomware resilience. Businesses should also include agenda-specific IOCs in their threat-hunting activities.

ATTACK TYPE	Ransomware	SECTOR	Information technology, Healthcare/hospitals, BFSI and Telecommunications
REGION	India, Brazil, Netherlands, Philippines and United States	APPLICATION	Windows

Source - https://www.trendmicro.com/en_us/research/25/e/agenda-ransomware-group-adds-smokeloader-and-netxloader-to-their.html

INTRODUCTION
HACKTIVIST STORM CONTINUES TO TARGET INDIA DURING INTENSIFIED INDO-PAK TENSIONS
ANARCHYRANSOM PLAYS MIND GAMES WITH VICTIMS
LAMPION MALWARE CLICKFIXES ITS WAY INTO PORTUGUESE NETWORKS
BPFDOOR: LINUX BACKDOOR THAT DODGES DETECTION
PAKISTAN-ALIGNED APTS RAMP UP INDIAN ESPIONAGE AMID RECENT CROSS-BORDER CONFLICT
AGENDA RANSOMWARE DEPLOYS NEW LOADER FOR STEALTH ATTACKS
DOGE BIG BALLS: RIDICULOUS NAME, SERIOUS THREAT
JAVA RAT SNEAKS INTO SOUTHERN EUROPE WITH GEOFENCED INVOICES
FAKE AI VIDEO SITES SPREAD NOODLOPHILE MALWARE
OTTERCOOKIE EXPANDS TO MACOS FOR GLOBAL FINANCIAL ESPIONAGE

DOGE Big Balls ransomware chain blends humour with harm

Despite its provocative name, DOGE Big Balls ransomware is a serious multi-stage threat. It uses custom PowerShell scripts, Mimikatz for credential dumping, Rubeus for Kerberos abuse, and vulnerable drivers for kernel access. It incorporates cryptojacking capabilities and hosts payloads on platforms like Netlify, allowing rapid updates and distribution. The campaign's sophistication lies in its ability to combine open-source tools and evasive techniques to escalate privileges, steal data, and mine cryptocurrency.

Organisations should harden defences against lateral movement and privilege escalation. This includes disabling unnecessary administrative tools, implementing Group Policy to restrict script execution, and applying driver blocklists through Microsoft Defender. Regular EDR tuning should flag anomalous use of credential theft tools. Web filtering should block known malicious hosting services, and asset management systems should track third-party software use across environments. As this campaign abuses legitimate utilities, security teams must adopt behaviour-based detection and regularly review logs for signs of unusual PowerShell activity and cryptojacking attempts.

ATTACK TYPE	Ransomware	SECTOR	Global
REGION	All	APPLICATION	Windows

Source - https://www.netskope.com/blog/new-doge-big-balls-ransomware-tools-in-the-wild

INTRODUCTION

HACKTIVIST STORM CONTINUES TO TARGET INDIA DURING INTENSIFIED INDO-PAK TENSIONS

ANARCHYRANSOM PLAYS MIND GAMES WITH VICTIMS

LAMPION MALWARE CLICKFIXES ITS WAY INTO PORTUGUESE NETWORKS

BPFDOOR: LINUX BACKDOOR THAT DODGES DETECTION

PAKISTAN-ALIGNED APTS RAMP UP INDIAN ESPIONAGE AMID RECENT CROSS-BORDER CONFLICT

AGENDA RANSOMWARE DEPLOYS NEW LOADER FOR STEALTH ATTACKS

DOGE BIG BALLS: RIDICULOUS NAME, SERIOUS THREAT

JAVA RAT SNEAKS INTO SOUTHERN EUROPE WITH GEOFENCED INVOICES

FAKE AI VIDEO SITES SPREAD NOODLOPHILE MALWARE

OTTERCOOKIE EXPANDS TO MACOS FOR GLOBAL FINANCIAL ESPIONAGE

Java RAT malware targets Southern Europe via fake invoices

A highly targeted email campaign is delivering a Java-based Remote Access Trojan (RAT) to victims in Spain, Italy, and Portugal. Threat actors use social engineering tactics like fake invoices and CAPTCHA pages to lure users into downloading malware hosted on Dropbox, MediaFire, and Ngrok. The campaign uses geofencing, SPF-aligned domains, and benign-looking attachments to bypass filters. Once installed, the RAT gives attackers full control, enabling data theft and surveillance.

To counter this threat, organisations must strengthen email defences using advanced threat protection (ATP), attachment sandboxing, and sender verification tools like DMARC. Employees should receive regular training on phishing indicators, especially financial-themed lures. Organisations should monitor outbound connections to cloud storage services and anonymising networks like Ngrok. Endpoint monitoring tools should detect new Java processes and unexpected network connections. Blocking risky file types in email (e.g., JAR files) and enforcing the use of signed applications can significantly reduce exposure.

ATTACK TYPE	Malware	SECTOR	All
REGION	Italy, Portugal, Spain	APPLICATION	Apple Mac OS, Windows, Linux

Source - https://www.fortinet.com/blog/threat-research/multilayered-email-attack-how-a-pdf-invoice-and-geofencing-led-to-rat-malware

Noodlophile Stealer masquerades as AI video software

Noodlophile is an info-stealing malware distributed via fake AI video generation sites, advertised through malicious Facebook ads. The malware is disguised as an MP4 video file and installs a multi-stage stealer that harvests browser credentials, session cookies, and cryptocurrency wallet data. Exfiltrated data is sent via Telegram bots, and in some cases, the malware is bundled with XWorm RAT for remote access. This campaign exemplifies the use of trending AI themes to lure unsuspecting users.

Businesses should restrict access to social media-advertised downloads and monitor for suspicious downloads from lesser-known domains. Users must be educated about malicious content disguised as AI tools or media files. DNS filtering and browser isolation can prevent access to malicious platforms. Endpoint protections should detect unusual file types masquerading as videos, and security teams should inspect for Telegram-based exfiltration channels. SOCs must remain alert to emerging lures tied to AI or deepfake technologies, as cybercriminals exploit their growing popularity for high-conversion malware campaigns.

ATTACK TYPE	Malware	SECTOR	Other
REGION	Global	APPLICATION	Windows

Source - https://www.morphisec.com/blog/new-noodlophile-stealer-fake-ai-video-generation-platforms/

OtterCookie Stealer evolves for global espionage

OtterCookie, attributed to North Korea’s WaterPlum group, is a modular infostealer that is now targeting both Windows and macOS systems, particularly in Japan’s financial and cryptocurrency sectors. Initially a basic file grabber, the latest versions support credential harvesting, virtual machine evasion, and multi-channel data exfiltration. Distributed through fake job recruitment messages, the malware reflects a significant evolution toward state-backed cyber-espionage and strategic financial targeting.

To defend against OtterCookie, financial institutions must implement identity protection, strict email filtering, and sandboxing for document-based lures. Behavioural monitoring can help detect atypical data access or unexpected connections from macOS endpoints, which are often overlooked in enterprise environments. User awareness training should include warnings about fake job offers and recruitment scams. EDR solutions with macOS support are critical for early detection. Additionally, organisations should monitor DNS activity for signs of encrypted data tunnelling and apply threat intelligence feeds to block WaterPlum-associated infrastructure.

ATTACK TYPE	Malware	SECTOR	Financial services
REGION	Japan	APPLICATION	Apple Mac OS, Windows

Source - https://jp.security.ntt/tech_blog/en-waterplum-ottercookie

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.