TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 1, 2025

TATA COMMUNICATIONS

TATA

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.

CISA adds high-profile Linux, Apple, TP-Link flaws to KEV list

CISA has added critical vulnerabilities affecting Linux Kernel (CVE-2023-0386), Apple devices (CVE-2025-43200), and TP-Link routers (CVE-2023-33538) to its Known Exploited Vulnerabilities (KEV) catalogue. The Linux flaw allows privilege escalation via OverlayFS, making it a significant risk for server environments. Apple users face threats from malicious iCloud-shared media, which could lead to system compromise. TP-Link routers contain command injection flaws, exposing home and enterprise networks to remote takeover. These vulnerabilities are actively exploited, with unknown ransomware groups already leveraging them in the wild.

CISA has mandated all federal agencies to apply vendor-recommended patches or mitigate these flaws by July 2025. Private organisations are strongly advised to follow suit, ensuring updates are applied across affected devices. Where patches aren't feasible, discontinuation or isolation of vulnerable products is critical. Additionally, monitoring for exploitation attempts and hardening network perimeters will help mitigate potential attacks stemming from these flaws.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Apple Mac OS, Apple IOS, Linux, TP-Link

Source - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Veeam backup flaws under exploitation by ransomware gangs

Veeam has released critical patches for its Backup & Replication (VBR) and Agent for Windows products to address multiple vulnerabilities, including CVE-2025-23121, a remote code execution flaw in domain-joined environments. This vulnerability allows authenticated domain users to execute arbitrary code on backup servers, posing a significant threat to data integrity. Two additional flaws, CVE-2025-24286 and CVE-2025-24287, enable job manipulation and privilege escalation. Active exploitation by ransomware groups like Akira and Fog has been observed, with attackers targeting backups to disable recovery options before deploying ransomware.

All Veeam users must urgently apply patches provided in VBR 12.3.2 and Agent for Windows 6.3.2. Organisations should isolate backup infrastructure from production environments, enforce strict access controls, and monitor for abnormal activities within backup servers. Implementing immutable backups and offline copies can help ensure data recovery even if backups are targeted.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Veeam, Veeam Backup Enterprise Manager

Source - https://thehackernews.com/2025/06/veeam-patches-cve-2025-23121-critical.html

Indian infrastructure faces intensifying hacktivist attacks

Hacktivist groups, including Nation of Saviors, Keymous+, Anonymous_SVN, and GARUDA ERROR SYSTEM, have ramped up attacks on Indian telecom, government, education, and healthcare sectors. The campaign involves DDoS attacks, website defacements, and data breaches, exploiting sector-specific vulnerabilities. Educational institutions and private companies are frequent defacement targets, while government portals face sustained DDoS activity. These attacks illustrate the global, decentralised nature of hacktivism, where politically or ideologically motivated groups exploit technical gaps to cause disruption.

Targeted sectors must enhance DDoS mitigation capabilities, regularly patch public-facing assets, and conduct web application security assessments. Incident response plans should account for defacements and data leaks. Collaborating with national CERTs and telecom providers to monitor threat activity can help organisations stay ahead of evolving hacktivist campaigns.

ATTACK TYPE	Hacktivism	**SECTOR**	Healthcare/hospitals, Government, Education, Defence Industry, BFSI, Broadcast Media Production and Distribution, Telecommunications
REGION	India	**APPLICATION**	Generic

Source - Cert-in

TATA COMMUNICATIONS

Infostealer malware hides behind copyright fraud emails

An infostealer malware campaign is spreading across South Korea, Japan, Thailand, and parts of Europe, disguised as legal copyright infringement notifications. Victims receive emails prompting them to download malicious documents that exploit DLL side-loading or double-extension file tricks to bypass detection. The primary malware identified is Rhadamanthys, which steals sensitive data, including email and banking credentials. Attackers prey on recipients' psychological response to legal threats, increasing infection success rates.

Organisations, particularly in legal and financial sectors, must implement email security filters capable of detecting double-extension files and known malware indicators. User awareness training should emphasise caution with unsolicited legal notices. Security teams should monitor for signs of Rhadamanthys activity and ensure endpoint defences can detect stealthy malware behaviours.

ATTACK TYPE	Malware	**SECTOR**	Financial services, Legal services
REGION	Japan, Greece, Hungary, North Korea, South Korea, Portugal, Thailand	**APPLICATION**	Windows

Source - https://asec.ahnlab.com/en/88544/

AMERILIFE ransomware encrypts files with “.ameriwasted” extension

AMERILIFE ransomware is a dangerous threat targeting Windows systems by encrypting files and appending a “.ameriwasted” extension. The ransomware is distributed through phishing campaigns, malicious downloads, and infected USB drives. Victims receive ransom demands offering decryption keys, but paying does not guarantee file recovery. Like many ransomware families, AMERILIFE disrupts businesses by targeting critical files and backups.

The most effective defence is prevention — regular offline backups, strong endpoint protection, and phishing awareness training are essential. Organisations should implement anti-ransomware tools that leverage behaviour analysis to detect early-stage infections. Backup systems must be tested regularly for recovery capabilities, and segmentation should be applied to prevent ransomware from spreading laterally.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

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

DarkHack ransomware emerges with file encryption threat

DarkHack is a newly discovered ransomware variant encrypting files and appending a unique ID and ".darkhack" extension. It spreads through phishing, malicious downloads, and exploitation of unpatched software vulnerabilities. Once infected, victims face ransom demands accompanied by strict instructions and intimidation tactics to prevent seeking outside help. Like most ransomware, paying the ransom is discouraged, as it does not guarantee data restoration.

Organisations should prioritise regular, tested backups and ensure all systems are up to date with the latest security patches. Email filtering and endpoint detection tools should be configured to block ransomware delivery methods. Incident response teams should develop ransomware-specific playbooks and educate users on phishing prevention.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

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

TaxOff exploits Google Chrome zero-Day with Trinper backdoor

The TaxOff group has exploited a zero-day vulnerability in Google Chrome (CVE-2025-2783) to deliver a custom C++ backdoor named Trinper. Distributed via phishing campaigns, Trinper provides attackers with remote control, keylogging, multithreading, and data exfiltration capabilities. Links to Team46 suggest a shared cyber-espionage infrastructure, with operations targeting both individuals and organisations globally. This campaign highlights the persistent targeting of browsers as initial access vectors.

Immediate patching of Google Chrome to the latest version is essential. Organisations should enforce browser update policies, implement EDR solutions that detect backdoor behaviour, and monitor for unauthorised outbound communications. Users must be trained to recognise phishing attempts, especially those prompting browser-based downloads.

ATTACK TYPE	Malware	**SECTOR**	Global
REGION	All	**APPLICATION**	Google Chrome OS, Google Chrome

Source - https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/team46-and-taxoff-two-sides-of-the-same-coin

Qilin emerges as dominant Ransomware-as-a-Service provider

With established ransomware groups like LockBit and RansomHub collapsing due to infighting and law enforcement actions, Qilin has seized the opportunity to rise as a dominant player in the ransomware landscape. Qilin offers a sophisticated Ransomware-as-a-Service (RaaS) model, providing affiliates with advanced technical capabilities, legal guidance, and full-service cybercrime infrastructure. Its organised approach reflects a disturbing trend towards industrialised cyber extortion.

Enterprises must assume ransomware will continue to evolve. Comprehensive in-depth defence strategies are critical, including patch management, endpoint protection, email security, and strong identity access controls. Regular tabletop exercises simulating ransomware attacks will improve response readiness. Engaging in threat intelligence sharing can help enterprises track and defend against Qilin-related activity.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows, Linux

Source - https://www.cybereason.com/blog/threat-alert-qilin-seizes-control

North Korean APT uses fake Zoom extension to target macOS

APT group TA444, linked to North Korea, has launched a targeted macOS campaign using a fake Zoom browser extension to deliver advanced malware implants. The malware includes keyloggers, infostealers, and tools for process injection, aimed at stealing cryptocurrency assets and sensitive data. This sophisticated intrusion demonstrates the growing interest of state-sponsored groups in macOS environments, traditionally considered lower-risk.

Organisations with macOS fleets should deploy enterprise-grade endpoint security solutions tailored for macOS. Strict controls on browser extensions and user privileges can limit infection vectors. Employee awareness programs must cover targeted social engineering tactics, particularly those exploiting popular collaboration platforms like Zoom.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Apple Mac OS, Windows

Source - https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis

Amatera Stealer advances as powerful MaaS data theft tool

Amatera Stealer, a rebranded and enhanced version of ACR Stealer, has surfaced as a leading malware-as-a-service (MaaS) threat. It features advanced evasion techniques, including stealth C2 channels using NTSockets and WoW64 Syscalls, allowing it to bypass security tools. Distributed via campaigns like ClearFake, it primarily targets browsers, cryptocurrency wallets, and messaging apps to steal credentials and sensitive information. The stealer also facilitates delivery of additional payloads, amplifying its impact.

Enterprises should adopt robust endpoint detection and response (EDR) tools capable of identifying stealthy malware behaviour. Users should be educated about social engineering lures like ClickFix used to propagate Amatera. Regular system updates, application allowlisting, and strict browser security settings will help reduce exposure to this evolving threat.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://www.proofpoint.com/us/blog/threat-insight/amatera-stealer-rebranded-acr-stealer-improved-evasion-sophistication

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