TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 10, 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.

StarFire ransomware: Cosmic branding, cataclysmic damage

StarFire is a newly identified ransomware strain that encrypts files using AES and RSA encryption and appends a ".Celestial" extension. It demands a $3,000 ransom in Bitcoin and spreads via phishing emails, fake software updates, and compromised websites. The malware alters system settings and deletes shadow copies, leaving victims with little recourse. StarFire's branding may seem whimsical, but its impact is severe — targeting businesses and individuals across Windows platforms with no known decryptor available.

To defend against StarFire, organisations should deploy comprehensive email filtering to block phishing attempts and train staff to identify suspicious links and attachments. System administrators should disable macros and restrict software execution from temporary directories. Regular, offline backups — ideally immutable — are critical to rapid recovery. Endpoint Detection and Response (EDR) tools must be configured to detect file encryption and unauthorised registry modifications. Patch management should also be prioritised to close vulnerabilities exploited by fake update mechanisms. Paying the ransom is strongly discouraged, as it does not guarantee data recovery.

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

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

DEVMAN ransomware: Double trouble with encryption and data theft

DEVMAN is a double-extortion ransomware that encrypts files with the ".yAGRTb" extension and simultaneously exfiltrates sensitive data. Victims are threatened with both file loss and public exposure if they fail to pay the ransom. The malware spreads via phishing emails, cracked software, and fake updates. DEVMAN uses obfuscated scripts and persistence techniques to maintain a foothold in compromised systems.

Organisations must strengthen phishing defences and discourage the use of unauthorised or pirated software. Endpoint security solutions should be tuned to detect signs of data exfiltration and suspicious scripting behaviour. Backups should be tested regularly and kept offline to prevent encryption or tampering. Network segmentation can contain lateral movement, and monitoring tools should alert on anomalies in outbound traffic. Security teams should also implement Data Loss Prevention (DLP) policies to monitor and block unauthorised data transfers. Incident response playbooks must include steps for data breach notification and legal consultation, especially under privacy regulations.

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

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

Chrome 137 and Firefox 139 patch multiple high-severity flaws

On May 29, 2025, Google and Mozilla released security updates for Chrome (v137) and Firefox (v139), addressing 21 vulnerabilities combined—including three classified as high severity. Chrome's update patched memory safety issues, while Firefox fixed a critical double-free bug in libvpx. Thunderbird and Extended Support Releases (ESR) also received important security patches. These flaws could allow remote code execution or browser crashes if left unpatched.

Organisations must enforce browser patching through centralised management tools like GPO, Intune, or Jamf. Vulnerability management platforms should verify that Chrome and Firefox are up to date across all devices. Secure browser configurations should disable unnecessary features like legacy plug-ins, and sandboxing should be enforced for risky content. Administrators should monitor usage of outdated or non-standard browsers and apply content filtering to block known exploit-hosting domains. Given the speed of browser-based attacks, timely patching is critical, especially in environments with high browser usage or public-facing web access.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Mozilla Firefox , Mozilla Thunderbird , Google Chrome

Source - https://www.securityweek.com/chrome-137-firefox-139-patch-high-severity-vulnerabilities/

TATA COMMUNICATIONS

Everest ransomware shifts toward data-leak extortion and insider recruitment

The Everest ransomware group, active since 2020, is evolving its tactics. Once focused on encrypting systems, it now increasingly relies on data exfiltration, threatening leaks to extort victims without encryption. Everest also offers initial access for sale on dark web forums and is known to recruit insiders at targeted companies. Sectors like healthcare, financial services, legal, and manufacturing are prime targets. Their recent campaigns span Apple macOS, Windows, and Linux.

To defend against Everest, organisations must implement robust identity and access management controls, including MFA, privileged access restrictions, and user activity monitoring. EDR and XDR tools should monitor for credential theft, unusual file access, and data exfiltration attempts. Insider threat detection platforms can flag suspicious employee behaviour. Data should be encrypted in transit and at rest, and DLP tools must be in place to block unauthorised transfers. Companies should also conduct periodic threat hunting and red teaming to simulate Everest-style attacks and validate detection capabilities.

ATTACK TYPE	Ransomware	**SECTOR**	Information technology, Healthcare/hospitals, Financial services, Legal services, Manufacturing, Construction, Government, BFSI, Retailer and Distributor
REGION	Global	**APPLICATION**	Apple Mac OS , Windows , Linux

Source - https://socradar.io/dark-web-profile-everest-ransomware/

TATA COMMUNICATIONS

Asulo ransomware: Low-cost threat, High-risk impact

Asulo is a Xorist-family ransomware variant that appends the ".asulo" extension to encrypted files and demands a modest $500 ransom via email or Telegram. Despite the relatively low ransom, the malware disables recovery options and establishes persistence through registry modifications. It spreads through phishing emails and infected executables and currently has no free decryption tool available, making recovery difficult without proper backups.

Organisations must ensure strong email protection, especially for executable attachments or archive files from unknown sources. Anti-ransomware tools should detect registry changes and unauthorised encryption processes. Offline or cloud-based backups must be maintained and tested regularly for reliability. Users should be educated about risks related to unknown email senders and downloading suspicious software. Application allowlisting can prevent unauthorised programmes from executing, while routine vulnerability scans can uncover weak points in the environment. Asulo's simplicity belies its potential impact—early containment and backup hygiene are key to resilience.

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

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

Smile ransomware leaves users far from satisfied

Smile ransomware encrypts user files using AES and RSA encryption and appends a .SM$LE extension. Victims are prompted to pay $3,000 in Bitcoin within 72 hours through a TOR-based platform, or risk permanent data loss. Furthermore, it propagates via phishing, malicious downloads, and unpatched systems.

To counter such threats, organisations must combine real-time monitoring with strong endpoint security solutions. Network access controls and multi-factor authentication (MFA) can prevent the initial compromise. Applying regular software patches and monitoring dark web channels for threat intelligence indicators can pre-empt targeted attacks. Legal and communication teams should be looped into incident planning to manage extortion scenarios effectively, ensuring both compliance and crisis management are aligned.

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

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

Hacktivist DDoS barrage hits UAE sectors

From May to June 2025, UAE-based sectors — particularly government, media, and tourism — faced a wave of DDoS and website defacement attacks by hacktivist groups. These attacks aim for disruption and reputational damage rather than financial gain or data theft. The attackers exploit poorly secured web infrastructure and public-facing services.

To mitigate such threats, organisations are investing in DDoS mitigation services, WAFs (Web Application Firewalls), and redundant DNS solutions. Threat intelligence feeds can help anticipate attacks aligned with geopolitical events. Regular penetration tests and hardened hosting environments reduce exposure to defacements. Proactive public communication strategies can limit the impact of successful attacks and ensure transparency with stakeholders.

ATTACK TYPE	Hacktivism , DDOS	**SECTOR**	Tourism/Hospitality , Government , Aerospace , Automobile / Manufacturing , Broadcast Media Production and Distribution , Food and Beverage Service , Retailer and Distributor
REGION	United Arab Emirates	**APPLICATION**	Generic

Source - CTI Team

TATA COMMUNICATIONS

Interlock ransomware’s NodeSnake RAT slithers into UK academia

The Interlock ransomware group has deployed NodeSnake, a JavaScript-based remote access trojan (RAT), against UK universities. Delivered via Cloudflare Tunnels, NodeSnake variants B and C exhibit improved obfuscation, encryption, and multi-payload capabilities. The malware facilitates remote access, persistence, and data theft, often preceding ransomware deployment.

Higher education institutions should embrace zero-trust principles, enforcing network segmentation and identity verification. EDR and next-gen antivirus solutions can detect unusual behaviour associated with Node.js-based threats. Cloud access security broker (CASB) tools and monitoring of DNS tunnelling or anomalous outbound traffic are essential. Incident response drills tailored to academic IT systems, often decentralised and BYOD-heavy, can enhance preparedness across faculty and administrative units.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	Education
REGION	UK	**APPLICATION**	Windows , Node JS

Source - https://www.bleepingcomputer.com/news/security/interlock-ransomware-gang-deploys-new-nodesnake-rat-on-universities/

Lyrix ransomware is a Python-based stealth attacker

Lyrix is a Python-based ransomware identified in April 2025, targeting Windows environments. It uses AES-256 encryption, deletes system backups, disables recovery, and appends a unique extension to victim files. Known for its anti-analysis capabilities, it evades traditional detection methods. Ransom demands are accompanied by threats of public data exposure.

Organisations should implement deep packet inspection and deploy honeypots to trap polymorphic malware like Lyrix. Restricting script execution privileges and using app isolation can neutralise Python-based threats. Cybersecurity frameworks like MITRE ATT&CK help map Lyrix behaviours for proactive detection. Enhanced log analysis and threat sharing across industry alliances can help improve collective defence and early detection of such malware variants.

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

Source - https://www.cyfirma.com/research/lyrix-ransomware/

PumaBot Botnet targets Linux-based IoT devices

PumaBot is a Linux-based botnet written in Go, designed to compromise IoT devices through SSH brute-force attacks. Instead of random scanning, it pulls targets from a command-and-control (C2) server. It deploys malware like jierui, ddaemon, and networkxm, and manipulates SSH keys and systemd services to ensure persistence.

Enterprises must treat IoT security as an enterprise-level concern. Network segmentation for IoT environments, default credential changes, and firmware updates are baseline defences. Behavioural detection can identify unusual outbound traffic patterns from compromised devices. Some organisations are now using IoT-specific security platforms and inventory discovery tools to identify and isolate vulnerable endpoints. Regulatory compliance for IoT device integrity is also gaining prominence in risk management strategies.

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

Source - https://www.darktrace.com/blog/pumabot-novel-botnet-targeting-iot-surveillance-devices

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