TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 11, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

In today's rapidly evolving digital environment, proactive cybersecurity is essential for organisations across all industries. Our weekly Cyber Threat Intelligence (CTI) reports deliver crucial insights into emerging threats, vulnerabilities, and attack patterns, enabling businesses to fortify their defences and stay ahead of evolving risks. By blending expert analysis with actionable recommendations, we empower clients to anticipate, detect, and neutralise potential threats before they escalate.

This forward-thinking approach not only safeguards critical digital assets but also ensures uninterrupted operations and strengthens stakeholder confidence. With our CTI reports, organisations can build enduring cyber resilience, fostering long-term security and trust in an increasingly uncertain digital landscape.

TATA COMMUNICATIONS

CISA expands the KEV Catalog to strengthen national cybersecurity

The Cybersecurity and Infrastructure Security Agency (CISA) has updated its Known Exploited Vulnerabilities (KEV) Catalog, adding new vulnerabilities actively exploited by cyber adversaries. This move aims to bolster national cybersecurity by providing organisations with critical insights to prioritise and address security gaps. The catalogue, mandated under Binding Operational Directive (BOD) 22-01, serves as a vital resource for federal agencies and private entities to mitigate risks posed by these vulnerabilities.

CISA emphasises the urgency of patching identified vulnerabilities, as they are frequently targeted by malicious actors to compromise systems and steal sensitive data. The updated catalogue includes vulnerabilities across a range of software and hardware, underscoring the need for proactive defence measures. By leveraging the KEV Catalog, organisations can enhance their cyber resilience, reduce attack surfaces, and safeguard critical infrastructure. CISA continues to urge all stakeholders to adopt a proactive approach to vulnerability management in the face of evolving cyber threats.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows, Zimbra Collaboration

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

TATA COMMUNICATIONS

CERT-In warns of critical vulnerabilities in major network products

The Indian Computer Emergency Response Team (CERT-In) has issued a high-severity alert regarding critical vulnerabilities in products from F5, Cisco, Citrix NetScaler, and Palo Alto Networks. These flaws, including risks like denial of service (DoS), privilege escalation, session hijacking, and email filter bypass, could allow attackers to execute arbitrary commands, bypass security protocols, or disrupt systems, compromising data confidentiality, integrity, and availability.

CERT-In emphasises the urgent need for organisations to apply patches and updates to affected systems to mitigate potential exploitation. The vulnerabilities pose significant threats to network security, with attackers potentially gaining unauthorised access or causing widespread outages. The advisory underscores the importance of proactive vulnerability management in safeguarding critical infrastructure. Organisations using these products are urged to act swiftly to secure their systems and prevent potential cyberattacks.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Citrix NetScaler, F5 BIG-IP, Cisco Secure Email, PAN-OS, Palo Alto Cortex XDR

Source - https://www.cert-in.org.in/

TATA COMMUNICATIONS

LightSpy spyware grows capabilities, now poses greater threat to mobile users

In a concerning development, the advanced iOS spyware LightSpy has significantly expanded its capabilities, now supporting over 100 commands to infiltrate and monitor mobile devices. Originally targeting Asian users, LightSpy has evolved into a sophisticated surveillance tool capable of extracting sensitive data, including location, contacts, messages, and even browser history. Security researchers warn that the spyware operates through malicious websites and phishing campaigns, exploiting vulnerabilities to gain unauthorised access. Its expanded command set allows attackers to execute complex operations, such as recording audio, capturing screenshots, and monitoring real-time activities, posing a severe threat to user privacy.

Experts urge mobile users to avoid clicking on suspicious links, update devices regularly, and employ robust security solutions. As LightSpy continues to evolve, its growing sophistication highlights the escalating risks of mobile spyware and the need for heightened vigilance in the digital age.

ATTACK TYPE	Spyware	**SECTOR**	All
REGION	Global	**APPLICATION**	macOS, Android, Windows, Linux

Source - https://thehackernews.com/2025/02/lightspy-expands-to-100-commands.html

New macOS malware targets the crypto sector with stealthy attacks

Cybersecurity researchers have uncovered a sophisticated macOS malware campaign specifically targeting the cryptocurrency sector. Dubbed CryptoStealer, the malware infiltrates systems through malicious software downloads and phishing schemes, aiming to steal sensitive data such as wallet credentials, private keys, and transaction details. The malware employs advanced evasion techniques, including masquerading as legitimate software and bypassing security protocols, making it difficult to detect. Once installed, it can monitor clipboard activity, hijack cryptocurrency transactions, and exfiltrate data to remote servers controlled by attackers.

Researchers warn that the crypto sector's high-value assets make it a prime target for such attacks. They urge macOS users to exercise caution when downloading software, enable robust security measures, and regularly update systems to mitigate risks. This discovery highlights the growing sophistication of macOS malware and underscores the need for heightened vigilance in the cryptocurrency community to safeguard digital assets.

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

Source - https://unit42.paloaltonetworks.com/macos-malware-targets-crypto-sector/

TATA COMMUNICATIONS

GitLab urges immediate patching for critical vulnerabilities exposing systems to high risk

GitLab has issued an urgent warning to users regarding two critical vulnerabilities – CVE-2025-0475 and CVE-2025-0555 – which could allow attackers to execute arbitrary code, bypass authentication, and gain unauthorised access to sensitive data. These high-risk flaws affect multiple versions of GitLab's Community and Enterprise Editions, posing significant threats to organisations relying on the platform for version control and collaboration. CVE-2025-0475 enables privilege escalation, while CVE-2025-0555 allows remote code execution, potentially leading to full system compromise. Exploiting these vulnerabilities could result in data breaches, service disruptions, and unauthorised changes to code repositories.

GitLab has released patches for both issues and strongly urges users to update their installations immediately. Cybersecurity experts emphasise the importance of timely patching to mitigate risks, as unpatched systems remain highly vulnerable to exploitation. This alert underscores the critical need for proactive vulnerability management in safeguarding software development environments.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	GitLab Community Edition (CE), GitLab Enterprise Edition (EE)

Source - https://securityonline.info/cve-2025-0475-cve-2025-0555-gitlabs-high-risk-patch-now/

TATA COMMUNICATIONS

DragonForce ransomware group intensifies attacks on Saudi Arabian organisations

The notorious DragonForce ransomware group has escalated its cyberattacks, specifically targeting Saudi Arabia's critical infrastructure and enterprises. Known for its double-extortion tactics, the group steals sensitive data before encrypting systems, demanding hefty ransoms to prevent leaks and restore access. Recent attacks have disrupted operations in healthcare, energy, and government sectors, raising alarms about national cybersecurity resilience. DragonForce leverages sophisticated phishing campaigns and exploits unpatched vulnerabilities to infiltrate networks, leaving organisations vulnerable to data breaches and financial losses.

Cybersecurity experts warn that the group's operations are becoming more aggressive, with tailored attacks aimed at maximising disruption. Authorities urge organisations to strengthen defences, implement robust backup strategies, and educate employees on phishing risks. As Saudi Arabia accelerates its digital transformation, the surge in ransomware attacks underscores the urgent need for enhanced cybersecurity measures to protect critical assets and maintain operational continuity in the face of evolving threats.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, energy, real estate
REGION	Saudi Arabia	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://www.resecurity.com/blog/article/dragonforce-ransomware-group-is-targeting-saudi-arabia

TATA COMMUNICATIONS

Critical vulnerability in Sliver C2 framework exposes systems to remote exploitation

A high-severity vulnerability has been discovered in Sliver, a popular command-and-control (C2) framework used by cybersecurity professionals and threat actors alike. Tracked as CVE-2025-1234, the flaw allows attackers to execute arbitrary code remotely, potentially compromising entire systems and exfiltrating sensitive data. Sliver, often employed for penetration testing and red teaming, is now a potential entry point for malicious exploitation if left unpatched. The vulnerability stems from improper input validation in the framework's server component, enabling unauthorised access and control over affected systems.

Security researchers urge users to update to the latest version of Sliver immediately to mitigate risks. Organisations leveraging the framework are advised to review their configurations and monitor for suspicious activity. This discovery highlights the dual-edged nature of security tools, emphasising the need for continuous updates and vigilance to prevent their misuse in cyberattacks.

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

Source - https://cybersecuritynews.com/sliver-c2-server-vulnerability/

TATA COMMUNICATIONS

Security intelligence highlights rising cyber threats and emerging attack trends

A recent cybersecurity report reveals a surge in sophisticated cyberattacks targeting global organisations. Key findings include a rise in ransomware campaigns, state-sponsored espionage, and exploitation of zero-day vulnerabilities. Threat actors are increasingly leveraging AI-driven tools to enhance attack precision and evade detection. The report highlights a notable spike in attacks on critical infrastructure, particularly in the energy and healthcare sectors, with attackers exploiting weak supply chain security. Additionally, phishing campaigns have become more targeted, using social engineering tactics to bypass traditional defences.

The report emphasises the importance of proactive threat intelligence and robust cybersecurity measures to counter these evolving risks. Organisations are urged to adopt advanced detection tools, conduct regular security audits, and educate employees on emerging threats. As cybercriminals grow more sophisticated, the report underscores the need for global collaboration and innovation in cybersecurity to stay ahead of adversaries and protect critical assets.

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

Source - https://www.cyfirma.com/news/weekly-intelligence-report-28-feb-2025/

Squidoor backdoor threatens global networks with stealthy espionage

Cybersecurity analysts have uncovered Squidoor, a highly sophisticated backdoor malware targeting organisations worldwide. Designed for stealthy espionage, Squidoor infiltrates systems via spear-phishing emails and malicious documents, enabling attackers to gain persistent access, exfiltrate sensitive data, and execute commands remotely. The malware employs advanced evasion techniques, including encrypted communications and modular architecture, making detection and analysis challenging. It primarily targets government, defence, and technology sectors, aiming to steal intellectual property and classified information.

Researchers warn that Squidoor's capabilities indicate state-sponsored origins, with its complexity rivalling notorious threats like APT28. Organisations are urged to enhance email security, deploy endpoint detection tools, and conduct regular threat hunting to mitigate risks. The discovery of Squidoor underscores the growing sophistication of cyber espionage tools and the need for heightened vigilance to protect critical assets from advanced persistent threats.

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

Source - https://unit42.paloaltonetworks.com/advanced-backdoor-squidoor/

Loches ransomware targets users with data encryption

A new ransomware strain, Loches has been identified, posing a significant threat to individuals and businesses alike. Loches infiltrates systems through malicious email attachments and software cracks, encrypting files and demanding ransom payments in cryptocurrency for decryption. Unlike typical ransomware, it also threatens to leak stolen data if demands are not met. Cybersecurity experts warn that Loches employs strong encryption algorithms, making file recovery without the decryption key nearly impossible. Victims are advised against paying ransoms, as there is no guarantee of data restoration, and it fuels further criminal activity.

To mitigate risks, users are urged to avoid suspicious emails, download software only from trusted sources, and maintain regular backups. Anti-malware tools can help detect and remove Loches, but prevention remains the best defence. The rise of Loches underscores the importance of cybersecurity awareness and proactive measures to combat evolving ransomware threats.

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

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

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