TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 4, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

In today’s fast-paced digital landscape, proactive cybersecurity measures are vital for organisations across all sectors. Our weekly Cyber Threat Intelligence (CTI) reports provide critical insights into emerging threats, vulnerabilities, and attack trends, equipping businesses to strengthen their defences and stay ahead of evolving risks. By combining expert analysis with actionable recommendations, we empower clients to anticipate, detect, and mitigate potential threats before they escalate.

This proactive strategy not only protects essential digital assets but also ensures operational continuity and boosts stakeholder trust. With our CTI reports, organisations can cultivate robust cyber resilience, fostering long-term security and confidence in an increasingly unpredictable digital world.

Websites at risk due to critical Jupiter X Core RCE vulnerability

A critical Remote Code Execution (RCE) vulnerability, identified as CVE-2025-0366, has been discovered in the Jupiter X Core theme, putting over 90,000 websites at risk. This high-severity flaw allows attackers to execute arbitrary code remotely, potentially compromising sensitive data, hijacking websites, or deploying malicious payloads. The vulnerability stems from improper input validation within the theme's core functionality, making it exploitable without requiring authentication.

Security experts warn that unpatched websites are highly susceptible to attacks, urging administrators to apply the latest updates immediately. The Jupiter X Core theme, widely used for WordPress websites, is a popular target due to its extensive user base. Cybersecurity firms have released patches to mitigate the risk, but many sites remain vulnerable due to delayed updates. Organisations are advised to prioritise patching, conduct security audits, and monitor for suspicious activity to safeguard their digital assets from potential exploitation.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	WordPress

Source - https://securityonline.info/90000-sites-at-risk-jupiter-x-core-rce-vulnerability-cve-2025-0366/

Highly obfuscated .NET Sectoprat malware emerges as a stealthy threat

A new and highly sophisticated malware, dubbed Sectoprat, has been identified by cybersecurity researchers. This .NET-based threat employs advanced obfuscation techniques to evade detection, making it a significant challenge for traditional security tools. Sectoprat is designed to steal sensitive information, including credentials, browser data, and cryptocurrency wallets, while maintaining a low profile on infected systems. The malware utilises multiple layers of encryption and anti-analysis methods to bypass security defences, enabling it to operate undetected for extended periods. Once installed, it establishes persistence and communicates with command-and-control (C2) servers to exfiltrate stolen data.

Sectoprat's emergence highlights the growing trend of attackers leveraging obfuscation to enhance malware effectiveness. Cybersecurity experts urge organisations to adopt advanced threat detection solutions, regularly update systems, and educate employees on phishing tactics to mitigate risks. Vigilance and proactive measures are essential to combat this evolving threat.

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

Source - https://cybersecuritynews.com/highly-obfuscated-net-sectoprat/

TATA COMMUNICATIONS

Spectrum Stealer malware threatens user data through sophisticated methods

Cybersecurity experts have issued warnings about Spectrum Stealer, a dangerous malware targeting sensitive user data, including login credentials, browser information, and cryptocurrency wallets. This stealthy threat infiltrates systems through phishing emails, malicious downloads, or compromised websites, operating discreetly to avoid detection. Spectrum Stealer is designed to harvest critical information, such as saved passwords, cookies, and financial data, which it then exfiltrates to remote servers controlled by attackers. Its ability to evade traditional antivirus solutions makes it particularly concerning for individuals and businesses alike.

To combat this threat, users are advised to employ robust antivirus software, avoid suspicious links, and regularly update their systems. Removal tools and detailed guides are available to help infected users eliminate the malware and secure their data. Cybersecurity professionals emphasise the importance of vigilance and proactive measures to mitigate risks posed by evolving threats like Spectrum Stealer.

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

Source - https://www.cyclonis.com/remove-spectrum-stealer/

TATA COMMUNICATIONS

Fake DeepSeek malware disguised as AI tool threatens user security

Cybersecurity experts have uncovered a new malware threat, Fake DeepSeek, masquerading as a legitimate AI-powered tool. This malicious software lures users with promises of advanced AI capabilities but instead infiltrates systems to steal sensitive data, including personal information, login credentials, and financial details. Fake DeepSeek is distributed through fake websites, phishing emails, and malicious ads, exploiting the growing interest in AI technologies. Once installed, it operates covertly, harvesting data and exfiltrating it to remote servers controlled by cybercriminals. Its sophisticated design allows it to evade detection by traditional security tools, making it a significant risk for individuals and businesses.

To protect against this threat, users are advised to download software only from trusted sources, avoid clicking on suspicious links, and use reputable antivirus programs. Cybersecurity professionals recommend regular system scans and immediate removal of Fake DeepSeek if detected. Vigilance and caution are crucial to safeguarding against such deceptive malware.

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

Source - https://www.cyclonis.com/remove-fake-deepseek-malware/

TATA COMMUNICATIONS

Critical vulnerability in NetScaler Console exposes Citrix systems

A severe security flaw, identified as CVE-2024-12284, has been discovered in the NetScaler Console, potentially exposing systems to unauthorised command execution. This high-severity vulnerability allows attackers to bypass authentication and execute arbitrary commands on affected systems, compromising sensitive data and network integrity. The flaw stems from improper access controls within the console, enabling malicious actors to exploit it remotely. Organisations using unpatched versions of NetScaler are at significant risk of cyberattacks, including data breaches and system hijacking.

Citrix, the vendor behind NetScaler, has released patches to address the vulnerability and urges users to update their systems immediately. Cybersecurity experts recommend implementing additional security measures, such as network segmentation and monitoring, to mitigate risks. This discovery underscores the importance of timely software updates and robust security practices to protect against evolving threats. Organisations are advised to act swiftly to safeguard their infrastructure from potential exploitation.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Citrix NetScaler

Source - https://securityonline.info/cve-2024-12284-in-netscaler-console-exposes-systems-to-unauthorized-command-execution/

TATA COMMUNICATIONS

SocGholish GhostWeaver backdoor threatens enterprise security

Cybersecurity researchers have uncovered a sophisticated backdoor, dubbed GhostWeaver, linked to the SocGholish malware campaign. This advanced threat targets enterprise networks, enabling attackers to gain persistent access, exfiltrate sensitive data, and deploy additional payloads. GhostWeaver operates by exploiting compromised websites to deliver malicious JavaScript, often disguised as fake browser updates. Once installed, the backdoor establishes communication with C2 servers, allowing attackers to execute commands remotely. Its stealthy nature and ability to evade detection make it a significant risk for organisations. SocGholish campaigns have historically targeted industries like healthcare, finance, and government, emphasising the need for heightened vigilance.

Security experts recommend implementing robust endpoint protection, monitoring network traffic for anomalies, and educating employees about phishing tactics. Regular software updates and patching are also critical to mitigating risks. As SocGholish continues to evolve, organisations must adopt proactive measures to safeguard their networks against this persistent and evolving threat.

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

Source - https://trac-labs.com/dont-ghost-the-socgholish-ghostweaver-backdoor-574154dd9983

TATA COMMUNICATIONS

Zhong Stealer malware emerges as a growing threat to sensitive data security

Cybersecurity analysts have identified a new data-stealing malware, Zhong Stealer, designed to harvest sensitive information from infected systems. This malicious tool targets credentials, browser data, cryptocurrency wallets, and other personal information, posing a significant risk to individuals and organisations alike. Zhong Stealer operates by infiltrating systems through phishing campaigns, malicious downloads, or compromised software. Once installed, it collects and exfiltrates data to remote servers controlled by attackers. Its lightweight design and ability to evade detection make it a formidable threat.

Researchers highlight its use of advanced techniques, such as anti-analysis methods and encryption, to bypass security defences. The malware's emergence underscores the growing sophistication of cybercriminals and the need for robust cybersecurity measures. To mitigate risks, experts recommend using reputable antivirus software, avoiding suspicious links, and keeping systems updated. Vigilance and proactive security practices are essential to combat evolving threats like Zhong Stealer and protect sensitive data from exploitation.

ATTACK TYPE	Phishing, malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://any.run/cybersecurity-blog/zhong-stealer-malware-analysis/

TATA COMMUNICATIONS

CISA and FBI warn of Ghost ransomware breaching enterprise cybersecurity

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have issued a joint alert warning about the widespread impact of Ghost ransomware, which has breached organisations in over 70 countries. This sophisticated ransomware variant encrypts critical data and demands payment for decryption, causing significant operational disruptions. Ghost ransomware operators exploit vulnerabilities in remote desktop protocols (RDP) and phishing campaigns to infiltrate networks. Once inside, they deploy the ransomware, exfiltrate sensitive data, and threaten to leak it unless ransom demands are met. The attackers' global reach and aggressive tactics have made them a formidable threat to businesses, healthcare providers, and government agencies.

CISA and FBI urge organisations to strengthen cybersecurity defences by enabling multi-factor authentication (MFA), patching vulnerabilities, and regularly backing up data. They also recommend monitoring network traffic for unusual activity and educating employees about phishing risks. Proactive measures are essential to mitigate the growing threat of Ghost ransomware.

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

Source - https://www.bleepingcomputer.com/news/security/cisa-and-fbi-ghost-ransomware-breached-orgs-in-70-countries/

TATA COMMUNICATIONS

Palo Alto Networks warns of exploited firewall vulnerability

Palo Alto Networks has flagged a critical vulnerability in its firewall software, now actively exploited in cyberattacks. Tracked as CVE-2024-3400, the flaw allows attackers to execute arbitrary code on affected devices, potentially gaining unauthorised access to networks and sensitive data. The vulnerability impacts specific versions of PAN-OS, the operating system used in Palo Alto firewalls. Exploits have been observed in the wild, targeting organisations to deploy malware, exfiltrate data, or disrupt operations. The company has released patches to address the issue and urges customers to update their systems immediately.

Cybersecurity experts emphasise the importance of applying patches promptly, as unpatched firewalls remain highly vulnerable to exploitation. Organisations are also advised to monitor network traffic for unusual activity and implement additional security measures, such as intrusion detection systems. This incident highlights the critical need for timely software updates and robust cybersecurity practices to protect against evolving threats and safeguard network infrastructure.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	PAN-OS, Palo Alto Firewall

Source - https://www.bleepingcomputer.com/news/security/palo-alto-networks-tags-new-firewall-bug-as-exploited-in-attacks/

TATA COMMUNICATIONS

Stately Taurus deploys Bookworm malware in targeted attacks

Researchers have uncovered a cyberespionage campaign by the Stately Taurus group, leveraging a new malware strain called Bookworm. This advanced threat actor, linked to Chinese state-sponsored operations, targets government, defence, and technology sectors to steal sensitive information. The Bookworm malware is delivered through spear-phishing emails containing malicious Word documents. Once executed, it establishes persistence, exfiltrates data, and communicates with C2 servers. The malware's modular design allows it to adapt to various environments, making detection and mitigation challenging.

Stately Taurus employs sophisticated tactics, including social engineering and zero-day exploits, to infiltrate high-value targets. The group's activities highlight the growing threat of state-sponsored cyberespionage and the need for robust defences. Organisations are urged to implement advanced threat detection, employee training, and regular system updates to counter such threats. Proactive cybersecurity measures are essential to safeguard sensitive data and mitigate risks posed by groups like Stately Taurus.

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

Source - https://unit42.paloaltonetworks.com/stately-taurus-uses-bookworm-malware/

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