TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 14, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today's rapidly evolving cybersecurity landscape, safeguarding critical systems and data is vital for individuals, businesses, and governments. Cyber threats pose risks of financial losses, reputational harm, and operational disruptions.

Our weekly Cyber Threat Intelligence (CTI) report offers actionable insights into global threats, equipping organisations with proactive strategies to mitigate risks. Backed by expert advisory services, this intelligence-driven approach addresses vulnerabilities, strengthens defences, and builds resilience against emerging challenges. Stay ahead in the cybersecurity race with the tools and knowledge to secure a robust digital future.

LummaStealer emerges as a new threat to digital security

Cybersecurity researchers have uncovered the emergence of LummaStealer, a sophisticated infostealer targeting Windows systems. Distributed through phishing emails and malicious attachments, LummaStealer harvests credentials, cryptocurrency wallets, and other sensitive data. Its modular design enables seamless adaptation, making it particularly dangerous for individuals and businesses.

The malware uses advanced obfuscation techniques to evade detection and establishes communication with command-and-control (C2) servers for data exfiltration. Its rapid deployment through underground forums has heightened concerns about its widespread adoption among cybercriminals. Experts stress the need for robust email security, user education, and endpoint monitoring to mitigate this evolving threat.

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

Source - https://www.cybereason.com/blog/threat-analysis-rise-of-lummastealer

TATA COMMUNICATIONS

QuasarRAT found disguised as NPM package, threatens developers with malware

Researchers have discovered a malicious campaign involving QuasarRAT, a potent remote access trojan, camouflaged as an NPM package. This sophisticated attack targets developers by embedding the malware within libraries that seem legitimate, leveraging the trust placed in open-source repositories. Upon installation, QuasarRAT enables attackers to gain full remote access to compromised systems, allowing them to exfiltrate sensitive information, execute commands, and monitor activities. The malware's functionality poses significant risks to developers and their organisations, including data theft and potential compromise of broader software ecosystems.

The attack underscores a growing trend of supply chain threats, where adversaries target developers by injecting malicious code into widely used platforms like NPM. Security experts recommend stringent measures, such as verifying package sources, monitoring dependencies, and employing advanced security tools to detect and mitigate these threats.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Node Package Manager (NPM)

Source - https://socket.dev/blog/quasar-rat-disguised-as-an-npm-package

Rise of memory-based attacks causing stealthy cybersecurity challenge

Memory-based attacks, an increasingly sophisticated cybersecurity threat, are on the rise. These stealthy tactics exploit system memory, bypassing traditional file-based detection measures to inject malicious code, launch malware, or execute ransomware. Techniques like reflective DLL injection and process hollowing allow attackers to avoid leaving disk traces, complicating threat detection. These attacks typically target organisations with high-value data, using vulnerabilities in software or exploiting unpatched systems to gain access. Once inside, the malware operates directly within the system's memory, enabling attackers to exfiltrate sensitive data, disrupt operations, or escalate privileges without triggering standard antivirus mechanisms.

Security experts stress the importance of proactive defences, such as real-time memory integrity monitoring, advanced endpoint protection, and regular system patching, to combat these evolving threats. Awareness and investment in next-generation cybersecurity tools are crucial for organisations to safeguard against this advanced attack vector.

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

Source - https://cybersecuritynews.com/memory-based-attacks/

Rising threat of post-holiday shopping scams and phishing attacks

As post-holiday sales attract eager shoppers, cybercriminals exploit the surge in online transactions with scams and phishing schemes. Researchers highlight increased activity targeting platforms like Amazon and eBay, deploying fake advertisements, fraudulent websites, and deceptive phishing emails. These scams often lure victims with unrealistically low prices or urgent offers. Phishing campaigns use cloned websites and malicious links to harvest user credentials and payment details. Fake delivery notifications are also common, tricking users into clicking malware-laden links. Additionally, malicious browser extensions and apps pose significant risks, capable of siphoning personal and financial data.

Experts advise caution during post-holiday shopping, emphasising the importance of verifying website legitimacy, avoiding suspicious links, and enabling multi-factor authentication. Robust cybersecurity practices are crucial to mitigating risks in this high-threat period.

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

Source - https://www.cloudsek.com/blog/high-potential-for-online-shopping-scams-and-phishing-attacks-targeting-post-holiday-sales#

Noneuclid RAT targets organisations in sophisticated cybercampaign

Cybersecurity experts have uncovered a new threat, Noneuclid RAT, a remote access trojan used in advanced cybercampaigns targeting global organisations. Distributed through phishing emails and malicious documents, the trojan enables attackers to infiltrate systems, exfiltrate sensitive data, and execute arbitrary commands. Noneuclid RAT employs obfuscation techniques to evade detection and maintains persistence on compromised networks. Its capabilities include keylogging, system reconnaissance, and the ability to download additional payloads.

Researchers warn that this evolving malware represents a significant risk, particularly to enterprises with inadequate defences. Proactive measures such as email filtering, employee training, and robust endpoint protection are critical to mitigating this emerging threat.

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

Source - https://www.cyfirma.com/research/noneclid-rat/

Watering hole attacks target academic and government sites in Japan

Cybersecurity experts have highlighted two recent instances of watering hole attacks targeting users from Japanese academic institutions. In these attacks, attackers exploited a university research laboratory website, infecting visitors with malware after displaying a fake Adobe Flash Player update screen. The malware, once downloaded, injected malicious code into systems, enabling attackers to control infected machines and exfiltrate sensitive data.

Researchers discovered the malware's sophisticated techniques, including Cobalt Strike Beacon, to maintain long-term persistence and avoid detection. This type of attack highlights the evolving nature of cyber threats and the need for enhanced security measures against increasingly targeted exploits.

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

Source - https://blogs.jpcert.or.jp/en/2024/12/watering_hole_attack_part2.html , https://blogs.jpcert.or.jp/en/2024/12/watering_hole_attack_part1.html

New scam uses fake game sites to spread information stealers

A rising cyber threat involves scammers enticing users with fake game beta testing invitations. Victims receive direct messages from attackers, offering a download link to test a new game. However, the downloaded files are actually information-stealing trojans like Nova Stealer and Hexon Stealer. These malicious programs target browser credentials, cryptocurrency wallets, and Discord tokens, potentially allowing further exploitation through compromised accounts.

Hosted on unresponsive platforms like Dropbox and Blogspot, the trojans spread via archives and MSI installers. To avoid falling victim, users should verify downloads from trusted sources and maintain up-to-date anti-malware solutions.

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

Source - https://www.malwarebytes.com/blog/news/2025/01/can-you-try-a-game-i-made-fake-game-sites-lead-to-information-stealers

Malicious NPM packages leverage OAST techniques for data theft

Cybersecurity researchers have uncovered a growing threat where attackers exploit Out-of-Band Application Security Testing (OAST) techniques to weaponise malicious packages in NPM, PyPI, and RubyGems ecosystems. These malicious packages use OAST services, such as oastify.com and interact.sh, originally developed for ethical penetration testing, to exfiltrate sensitive data from compromised systems. Through these packages, threat actors can bypass traditional detection systems by exfiltrating data and establishing communication channels for further exploitation. Using these advanced tactics, attackers can remotely probe developer environments, access sensitive project data, and launch multi-stage attacks. These tools are rapidly being misused to steal valuable data, making them a significant concern for the security of the software supply chain.

Socket's threat research highlights the growing misuse of ethical security tools, emphasising the need for heightened vigilance and more robust security practices across development platforms. As this trend continues, both developers and organisations must adopt advanced monitoring and defence mechanisms to protect their codebases from being hijacked by such covert operations.

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

Source - https://socket.dev/blog/weaponizing-oast-how-malicious-packages-exploit-npm-pypi-and-rubygems

TATA COMMUNICATIONS

Butcher Shop phishing campaign targets legal, government, and construction firms

Cybersecurity researchers have uncovered the Butcher Shop phishing campaign, which primarily targets Microsoft 365 accounts within legal, government, and construction sectors. This advanced attack uses a combination of email redirects and open redirect vulnerabilities, making it difficult for traditional phishing defences to block. The campaign, which has seen over 200 malicious domains, involves phishing links embedded in emails and compromised WordPress sites. Once a user is redirected to a malicious site, attackers harvest sensitive credentials. Using legitimate services like Cloudflare to evade detection, the campaign makes traditional URL blocking ineffective.

The inclusion of custom scripts and random meat-themed text adds further obfuscation to its deceptive tactics. This ongoing campaign highlights the need for heightened vigilance against phishing, especially in sectors handling critical data.

ATTACK TYPE	Malware	**SECTOR**	Construction, government
REGION	Global	**APPLICATION**	Microsoft Office 365

Source - https://www.obsidiansecurity.com/blog/butcher-shop-phishing-campaign-targets-organizations/

TATA COMMUNICATIONS

Critical GoCD vulnerability patches released to prevent privilege escalation

GoCD has urgently patched a critical vulnerability, CVE-2024-56320, found in versions prior to 24.5.0. This flaw, stemming from improper access controls on the admin “Configuration XML” UI, allowed authenticated users to escalate their privileges to that of a GoCD administrator. Attackers could exploit this to gain unauthorised access to sensitive system information and control over GoCD environments. The vulnerability, which requires prior authentication to be exploited, poses a significant risk, especially for malicious insiders.

GoCD users are strongly urged to update to version 24.5.0 immediately. For those unable to upgrade promptly, the GoCD project recommends temporary mitigations, including blocking vulnerable paths and reducing user access. The patch addresses the security hole, but organisations must act swiftly to secure their CI/CD pipelines from potential exploitation.

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

Source - https://securityonline.info/gocd-patches-critical-vulnerability-allowing-user-privilege-escalation/

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