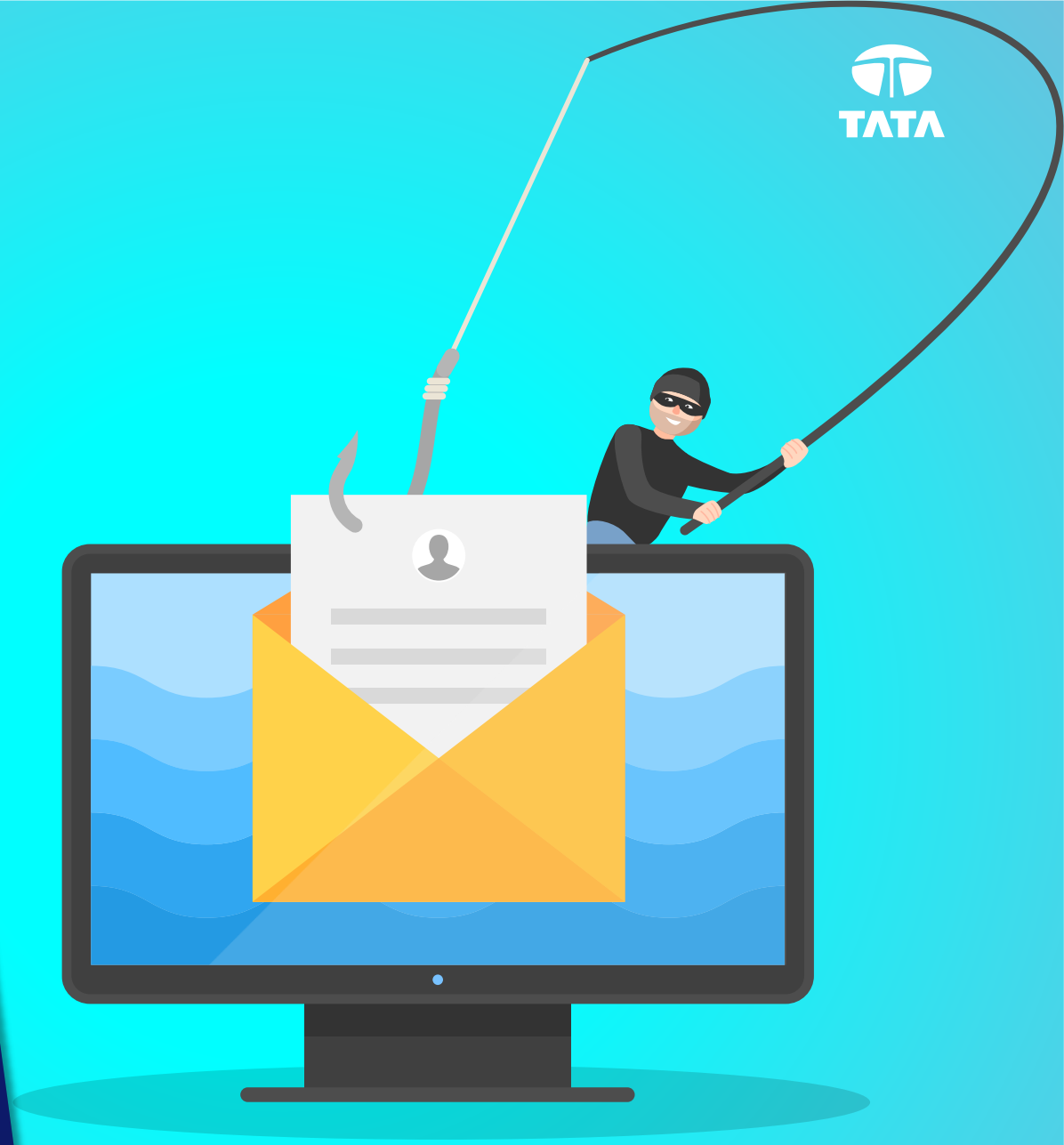
TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 31, 2024



TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the ever-evolving realm of cybersecurity, safeguarding critical systems and data is paramount for individuals, businesses, and governments. Cyber threats can inflict financial losses, reputational harm, and disrupt operational security.

Our weekly Cyber Threat Intelligence (CTI) report delivers actionable insights into emerging global threats, empowering organisations with proactive strategies to combat growing risks. Supported by expert advisory services, this intelligence-driven approach strengthens security postures, mitigates persistent risks, and fortifies resilience against dynamic challenges. Equip your organisation with the knowledge and tools to navigate the complex cybersecurity landscape and ensure a secure, robust future.

Tax-themed FluxConsole malware exploits Windows Management Console

Researchers have uncovered a campaign leveraging FluxConsole, a malware-delivering backdoor targeting the Windows Management Console via tax-themed phishing lures. Threat actors use malicious links and attachments disguised as legitimate tax documents to trick victims into executing backdoor payloads.

Once installed, FluxConsole enables attackers to exfiltrate data and establish persistent access. The campaign underscores a growing trend of exploiting native Windows tools to bypass defences and evade detection. Organisations are urged to bolster email security and educate users about phishing tactics to mitigate such risks.

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

Source - https://www.securonix.com/blog/analyzing-fluxconsole-using-tax-themed-lures-threat-actors-exploit-windows-management-console-to-deliver-backdoor-payloads/

Critical vulnerability in Hitachi systems enables remote exploits

Researchers have identified a severe authentication bypass vulnerability, CVE-2024-10205, in Hitachi's Infrastructure Analytics Advisor and Ops Center Analyzer. Rated 9.4 on the CVSS scale, this flaw allows attackers to bypass authentication, potentially leading to data theft, system compromise, and service disruptions. The vulnerability impacts specific versions of Hitachi software running on Linux (x64) platforms. Exploitation requires no prior authentication, enabling remote access to critical systems. Hitachi has released updates to mitigate the issue and urges affected users to upgrade immediately, as no workarounds are available.

This discovery highlights the importance of maintaining updated software and monitoring security advisories to protect against emerging threats. Organisations using these Hitachi solutions are strongly advised to apply patches or consult Hitachi support to safeguard their infrastructure against attacks.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Hitachi Infrastructure Analytics Advisor, Hitachi Ops Center Analyzer

Source - https://gbhackers.com/hitachi-authentication-bypass-vulnerability/

New ransomware NotLockBit emerges and causes disruptions

Analysts have identified NotLockBit, a ransomware variant mimicking LockBit but operating independently. This malware employs unique encryption tactics and extortion methods, targeting diverse organisations. Delivered via phishing or malicious downloads, NotLockBit encrypts files and demands ransom for decryption keys. Its use of unconventional code highlights a distinct approach compared to its namesake.

Cybersecurity experts emphasise heightened vigilance and urge organisations to deploy robust defences against ransomware, including timely updates and network monitoring. The emergence of NotLockBit underscores the evolving landscape of cyber threats demanding proactive security measures.

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

Source - https://blog.qualys.com/vulnerabilities-threat-research/2024/12/18/notlockbit-a-deep-dive-into-the-new-ransomware-threat

LummApp campaign uses browser extensions to steal credentials

Experts have uncovered LummApp, a malicious campaign leveraging fake browser extensions to steal credentials. Disguised as legitimate add-ons, these extensions exploit users by targeting Chromium-based browsers like Chrome and Edge. The malware infiltrates via phishing emails or compromised websites, aiming to harvest sensitive login details and session cookies.

LummApp bypasses traditional security measures by embedding itself into users' browsers, enabling attackers to gain unauthorised access to accounts. Its advanced techniques underline the growing threat posed by infostealers. Researchers recommend heightened awareness, regular browser updates, and avoiding unverified extensions to mitigate risks.

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

Source - https://www.hunters.security/en/blog/lummapp-infostealer-browser-extensions-credential-theft

Skuld infostealer resurfaces on NPM, causing a threat to developers

Security researchers have detected the return of the Skuld infostealer to the Node Package Manager (NPM) ecosystem, targeting developers by infiltrating JavaScript packages. Skuld is designed to steal sensitive data, including credentials, tokens, and configuration files, from compromised development environments.

The malware masquerades as legitimate or popular packages, tricking users into downloading it. Once installed, it exfiltrates data to command-and-control (C2) servers, posing significant risks to projects and infrastructure. Developers are urged to validate package sources and adopt strict dependency monitoring to protect against such threats.

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

Source - https://socket.dev/blog/skuld-infostealer-returns-to-npm

RockStar phishing platform evolves amid security concerns

Cybersecurity specialists have highlighted the resurgence of RockStar, a sophisticated phishing platform capable of bypassing two-factor authentication (2FA). RockStar lures victims into credential theft through convincing phishing pages that mimic trusted services. Adding to the threat, Flowerstorm, a new malware delivery method, targets users compromised by RockStar. This duo exemplifies the growing sophistication of phishing-as-a-service operations.

Organisations must fortify their defences against phishing by implementing robust email security, employee training, and multi-layered authentication (MFA) strategies to mitigate risks from evolving cyber threats.

ATTACK TYPE	Phishing	**SECTOR**	All
REGION	The US, the UK, Canada, Australia, New Zealand, Singapore, India, Israel, Italy, the UAE	**APPLICATION**	Generic

Source - https://news.sophos.com/en-us/2024/12/19/phishing-platform-rockstar-2fa-trips-and-flowerstorm-picks-up-the-pieces/

TATA COMMUNICATIONS

Advanced cyberattack playbook exposes organisations to a new threat landscape

Researchers have uncovered a sophisticated playbook for advanced cyberattacks targeting critical sectors globally. The stealthy tactics involve precise reconnaissance, lateral network movement, and tailored payloads designed to evade detection. This advanced approach reflects an escalating threat landscape where attackers prioritise persistence and data theft.

The playbook showcases advanced infiltration methods, including zero-day vulnerabilities, credential harvesting, and malware deployment through phishing and social engineering. Experts emphasise the urgency of proactive defence strategies, including threat intelligence, real-time monitoring, and incident response readiness to mitigate such evolving threats.

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

Source - https://cyble.com/blog/a-stealthy-playbook-for-advanced-cyber-attacks/

CleverS0ar campaign exploits WinOS4.0 module for cyberespionage

Cybersecurity researchers have identified WinOS4.0, a sophisticated online staging module, as a critical component in the CleverS0ar cyberespionage campaign. This campaign targets global entities across finance, defence, and government sectors, leveraging advanced tools to exfiltrate sensitive data.

WinOS4.0's modular framework enables attackers to deploy tailored payloads, enhancing stealth and efficiency. The malware uses encrypted communication channels to evade detection and maintain persistence on compromised networks. Researchers emphasise the urgency of robust cybersecurity measures, including endpoint detection and network monitoring, to counter these sophisticated threats.

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

Source - https://www.esentire.com/blog/winos4-0-online-module-staging-component-used-in-cleversoar-campaign

A new cyber threat variant emerges in the form of BellaCpp malware

Experts have identified BellaCpp, a C++ adaptation of the infamous BellaCiao malware, signalling an evolution in targeted cyberattacks. This malware variant is designed for cross-platform deployment and showcases enhanced evasion techniques. BellaCpp is being used in advanced espionage campaigns to infiltrate organisations globally, targeting sensitive data.

Leveraging robust modularity and compatibility with various operating systems, BellaCpp demonstrates a focus on stealth and persistence. Researchers emphasise the critical need for comprehensive threat detection and response strategies to counter this escalating cyber threat effectively.

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

Source - https://securelist.com/bellacpp-cpp-version-of-bellaciao/115087/

Earth Koshchei hackers target RDP systems with red team tools

Researchers have uncovered a sophisticated campaign by the Earth Koshchei group, which is exploiting Remote Desktop Protocol (RDP) vulnerabilities using advanced red team tools. This threat actor leverages legitimate penetration testing software to infiltrate systems, facilitating unauthorised access and exfiltration of sensitive data. The attack methods mimic real-world adversary techniques, making it harder for detection systems to identify the malicious activities.

Earth Koshchei's use of trusted tools allows them to bypass traditional security defences, leading to targeted data theft and system compromise. Organisations are urged to enhance RDP security, implement strong authentication protocols, and monitor for abnormal behaviours to mitigate the risks posed by these advanced tactics.

ATTACK TYPE	Phishing, malware	**SECTOR**	IT, government, military, energy, BFSI, telecommunications
REGION	Australia, the UK, Estonia, Germany, the Netherlands, Portugal, Ukraine, the US	**APPLICATION**	Teams

Source - https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html

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