TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: FEBRUARY 04, 2025

THREAT INTELLIGENCE ADVISORY REPORT

In today’s evolving cyber landscape, safeguarding critical systems is vital for individuals, businesses, and governments. Cyber threats can cause financial loss, reputational harm, and operational disruptions.

Our weekly Cyber Threat Intelligence (CTI) report offers actionable insights on emerging threats, helping organisations enhance security, mitigate risks, and build cyber resilience. Supported by expert advisory services, this intelligence-driven approach identifies vulnerabilities and strengthens defence strategies. Stay ahead of cyber risks with the latest knowledge and tools to protect your digital assets and ensure a secure future.

Nnice ransomware hits systems globally, encrypting data with extension

The Nnice ransomware is a newly discovered strain targeting Windows systems. This malware encrypts files and appends the .xdddd extension, rendering critical data inaccessible. Victims receive a ransom note on infected devices, coercing them into paying for decryption. Spreading primarily through phishing emails and malicious downloads, Nnice represents a significant risk to organisations without strong cybersecurity defences. Security experts recommend implementing proactive measures such as endpoint protection, regular data backups, and advanced email filtering to mitigate the threat.

Since ransomware operators continuously refine their attack methods, businesses must remain vigilant and enforce strict security policies to prevent infections. Furthermore, educating employees on phishing tactics can reduce the risk of initial infiltration. If infected, organisations should avoid paying the ransom and instead seek assistance from cybersecurity professionals. The rise of Nnice highlights the evolving ransomware landscape and the ongoing need for robust cybersecurity strategies.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

LucKY_Gh0$t ransomware strikes with advanced evasion tactics

LucKY_Gh0$t, a newly identified ransomware from the Chaos family, poses a significant threat to Windows systems. This variant encrypts files, renames them using random extensions, and changes desktop wallpapers to display ransom demands. Attackers deliver their ransom note through the Session messaging platform, further complicating mitigation efforts. Advanced evasion tactics make detection difficult, as the malware deletes Volume Shadow Copies and manipulates Windows Registry settings to establish persistence.

Cybersecurity professionals emphasise the importance of regular backups, robust endpoint security, and user awareness training to counter such threats. The use of sophisticated encryption mechanisms and aggressive data deletion methods make recovery particularly challenging. Organisations should adopt a zero-trust approach, restrict administrative privileges, and ensure timely software updates to reduce exposure. As ransomware actors continue evolving, businesses must enhance cybersecurity resilience by implementing multi-layered security defences.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.broadcom.com/20240124-lucky-gh0-t-ransomware

Black Basta and FIN7 target Microsoft Teams calls for remote access

Cybercriminals are exploiting Microsoft Teams as an attack vector, using advanced social engineering tactics to deploy ransomware. Groups like Black Basta and FIN7 have been observed leveraging email bombing and impersonation techniques via Teams calls to trick employees into granting remote access. Attackers exploit Teams' default configurations, using phishing lures to convince users to install malicious software. These campaigns often lead to ransomware deployment, data exfiltration, and financial extortion.

Organisations are urged to enhance Teams security by blocking external communication, disabling Quick Assist, and enforcing multi-factor authentication. Employee awareness training is critical to identifying social engineering attacks before they succeed. IT administrators should also audit Teams access policies and enforce stringent security controls to mitigate risks. This growing trend highlights the need for continuous monitoring and proactive defences to counter increasingly sophisticated ransomware tactics targeting enterprise communication platforms.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	MS Teams

Source - https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

Contacto ransomware stealthily uses multi-threaded encryption for maximum damage

Contacto is a newly discovered ransomware strain that employs advanced evasion techniques to avoid detection. It leverages stealthy execution, privilege escalation, and multi-threaded encryption to maximise its impact. Unlike traditional ransomware variants, Contacto manipulates Windows console functions to operate in a low-profile manner, making it difficult for standard security tools to detect. The ransomware uses flexible encryption modes and a sophisticated key generation process, further complicating decryption efforts. Additionally, it establishes persistence via fake scheduled tasks and erases traces by self-deleting post-encryption.

Security researchers advise organisations to adopt robust cybersecurity measures, including endpoint protection, strict access controls, and frequent system audits, to detect and neutralise threats like Contacto before they cause significant damage. Keeping software up to date and employing behavioural-based detection tools can further mitigate the risk of infection.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://cybersecuritynews.com/new-contacto-ransomware-evades-av-detection/

Dharma ransomware evolves with a new variant that disables recovery

A new variant of the notorious Dharma ransomware has been identified, appending the .nqix extension to encrypted files. Like its predecessors, this variant disables system recovery features such as Volume Shadow Copies, making data restoration difficult without external backups. While the new strain does not exhibit advanced lateral movement capabilities, it remains highly effective in disrupting business operations through rapid file encryption. Dharma primarily spreads via phishing emails and malicious attachments, highlighting the continued importance of email security.

Organisations are advised to implement proactive defence strategies, including offline backups, user awareness training, and endpoint security solutions. Given Dharma’s persistence in the ransomware landscape, enterprises should adopt a zero-trust approach and enforce strict access control policies to limit exposure. If infected, organisations should refrain from paying the ransom and seek assistance from cybersecurity experts to explore alternative recovery options.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://cymulate.com/blog/immediate-threat-analysis-new-dharma-ransomware/

GamaCopy mimics Gamaredon to deploy advanced spyware

GamaCopy, a newly identified cyberespionage group, is actively targeting Russian defence and infrastructure sectors using tactics reminiscent of the Gamaredon APT. The group employs military-themed phishing lures, embedding malicious payloads within 7z SFX archives to evade detection. Once executed, the payload deploys UltraVNC, a remote access tool, allowing attackers to establish persistent access to compromised systems. GamaCopy's techniques include obfuscation, encrypted communication over port 443, and false-flag operations to misattribute attacks. The choice of Russian-language documents and region-specific attack vectors suggests a deliberate focus on Russian-speaking targets.

Organisations in critical sectors should enhance monitoring for unauthorised remote access, enforce strict endpoint security policies, and conduct security awareness training to prevent phishing-based intrusions. Given the group's evolving tactics, proactive threat intelligence and incident response planning are essential to mitigate future attacks.

ATTACK TYPE	Cyberespionage	SECTOR	Defence
REGION	Russia	APPLICATION	UltraVNC Viewer, Generic

Source - https://securityonline.info/gamacopy-a-new-cyber-espionage-group-imitating-gamaredon-to-target-russia/

Bashe ransomware exploits high-value financial targets with double extortion

The Bashe ransomware group, also known as APT73, has intensified its attacks on financial institutions using double extortion tactics. First observed in 2024, Bashe encrypts sensitive data while also stealing and threatening to leak it unless a ransom is paid. The group primarily targets large financial entities, aiming to exploit transactional records and client data for maximum financial leverage. Their TOR-based Data Leak Site mimics the operational structure of LockBit, emphasising their sophistication and intent to maximise financial damage. Recent attacks indicate an expansion into industries such as healthcare, manufacturing, and telecommunications.

Organisations must bolster cybersecurity defences by implementing real-time monitoring, network segmentation, and zero-trust architecture to minimise exposure. Enhanced backup strategies and strict data access policies can mitigate the impact of Bashe's evolving threat landscape. Given the growing risk to financial institutions, proactive security measures are critical to prevent disruption.

ATTACK TYPE	Ransomware	SECTOR	IT, healthcare, manufacturing, construction, transportation, BSFI, telecommunications
REGION	India, the UK, Austria, Brazil, France, Poland, the US	APPLICATION	Windows

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

Clop gang automates ransomware deployment via Cleo CVEs

The Clop ransomware group has been exploiting critical vulnerabilities CVE-2024-50623 and CVE-2024-55956 in Cleo software to execute unauthorised file operations and exfiltrate sensitive data. These vulnerabilities allow attackers to automate ransomware deployment, primarily targeting finance and government sectors. Clop has previously leveraged zero-day vulnerabilities in enterprise applications, underscoring the importance of timely patch management.

Organisations using Cleo software must immediately apply security updates, review access controls, and monitor network activity for potential exploitation attempts. Given Clop’s history of orchestrating high-profile data theft campaigns, cybersecurity professionals recommend proactive threat hunting, intrusion detection, and real-time endpoint monitoring to mitigate risks. The continued exploitation of software vulnerabilities highlights the need for regular vulnerability assessments and adherence to best security practices to defend against evolving ransomware tactics.

ATTACK TYPE	Ransomware	SECTOR	BFSI, government
REGION	Australia, the US	APPLICATION	Generic, Cleo software

Source - https://www.imperva.com/blog/imperva-protects-against-the-exploited-cves-in-the-cleo-data-theft-attacks/

CISA warns of active attacks exploiting unpatched jQuery systems

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued a warning regarding CVE-2020-11023, a five-year-old cross-site scripting (XSS) vulnerability in jQuery that is now actively exploited in cyberattacks. Despite being patched in jQuery v3.5.0, many organisations continue using outdated versions, leaving them vulnerable to arbitrary code execution. Attackers exploit this flaw to inject malicious scripts, steal credentials, and compromise web applications. Federal agencies have been instructed to patch affected systems by February 13, 2025, but organisations across industries should prioritise updates immediately.

Security experts recommend conducting code audits, applying Content Security Policies (CSPs), and monitoring web applications for suspicious activity to mitigate risks. The continued exploitation of older vulnerabilities underscores the importance of aggressive patching policies and regular security assessments to protect against evolving threats.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	jQuery

Source - https://thehackernews.com/2025/01/cisa-adds-five-year-old-jquery-xss-flaw.html

PANdora’s Box exploits could-enabled remote code execution

A security evaluation of three Palo Alto Networks firewalls (PA-3260, PA-1410, PA-415) has revealed multiple critical vulnerabilities, collectively named PANdora’s Box. These flaws include BootHole (CVE-2020-10713) and firmware issues that could allow attackers to bypass Secure Boot and execute malicious code. If exploited, these vulnerabilities could enable persistent access, remote code execution, and privilege escalation.

While Palo Alto Networks has stated that up-to-date devices following best security practices are not affected, organisations should review their firewall configurations, apply security patches, and enforce strict access controls. Cybersecurity teams are advised to conduct regular penetration tests and implement zero-trust network segmentation to mitigate risks. The discovery of PANdora’s Box highlights the critical role of firmware security in enterprise defence strategies.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Palo Alto

Source - https://thehackernews.com/2025/01/palo-alto-firewalls-found-vulnerable-to.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

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.