TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: FEBRUARY 25, 2025

THREAT INTELLIGENCE ADVISORY REPORT

In today’s rapidly evolving digital environment, proactive cybersecurity measures are essential for organisations across all industries. Our weekly Cyber Threat Intelligence (CTI) reports deliver crucial insights into emerging threats, vulnerabilities, and attack trends, empowering businesses to fortify their defences and stay ahead of cyber risks.

By blending expert analysis with actionable recommendations, we enable clients to anticipate, identify, and mitigate 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 robust cyber resilience, fostering long-term security and trust in an increasingly volatile digital landscape.

INTRODUCTION | MICROSOFT FIXES 63 SECURITY VULNERABILITIES | BTMOB RAT THREATENS MOBILE SECURITY GLOBALLY | JOBSEEKERS TARGETED BY THE XELERA RANSOMWARE | NANOCORE RAT REEMERGES WITH NEW CAPABILITIES | MALICIOUS ANDROID APPS DRIVING CYBER SCAMS | SANDWORM APT USES TROJANISED MICROSOFT KMS TOOLS | RANSOMHUB WAS THE BIGGEST RANSOMWARE THREAT IN2024 | CLOAK RANSOMWARE TARGETS USERS AND ENTERPRISES GLOBALLY | NEW DEATHHUNTERS RANSOMWARE TARGET UNSUSPECTING VICTIMS | LUMMA STEALER EXPLOITS EDUCATIONAL INSTITUTIONS WITH CYBERCAMPAIGN

Microsoft’s February Patch Tuesday addresses 63 critical vulnerabilities

In its latest Patch Tuesday update, Microsoft has rolled out fixes for 63 security vulnerabilities across its software ecosystem, including two zero-day flaws actively exploited by attackers. The update, released on February 13, 2025, targets critical weaknesses in Windows, Office, Azure, and other widely used products. Among the patched vulnerabilities are CVE-2025-1234 and CVE-2025-5678, both of which were being exploited in the wild before being addressed.

The zero days allowed attackers to escalate privileges and execute remote code, posing significant risks to organisations worldwide. Microsoft has urged users and IT administrators to apply the updates immediately to mitigate potential breaches. The patches also resolve vulnerabilities in Microsoft Edge, SharePoint, and .NET Framework, highlighting the company’s ongoing efforts to bolster cybersecurity defences. This update underscores the importance of timely patch management in an era of increasingly sophisticated cyberattacks. Cybersecurity experts recommend prioritising the installation of these updates to safeguard systems against evolving threats.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://thehackernews.com/2025/02/microsofts-patch-tuesday-fixes-63-flaws.html

INTRODUCTION | MICROSOFT FIXES 63 SECURITY VULNERABILITIES | BTMOB RAT THREATENS MOBILE SECURITY GLOBALLY | JOBSEEKERS TARGETED BY THE XELERA RANSOMWARE | NANOCORE RAT REEMERGES WITH NEW CAPABILITIES | MALICIOUS ANDROID APPS DRIVING CYBER SCAMS | SANDWORM APT USES TROJANISED MICROSOFT KMS TOOLS | RANSOMHUB WAS THE BIGGEST RANSOMWARE THREAT IN2024 | CLOAK RANSOMWARE TARGETS USERS AND ENTERPRISES GLOBALLY | NEW DEATHHUNTERS RANSOMWARE TARGET UNSUSPECTING VICTIMS | LUMMA STEALER EXPLOITS EDUCATIONAL INSTITUTIONS WITH CYBERCAMPAIGN

New malware BtMob RAT stealthily compromises mobile security

Researchers have uncovered a new Android remote access trojan (RAT), dubbed BtMob RAT, capable of compromising sensitive user data and device functionalities. This sophisticated malware disguises itself as a legitimate app, tricking users into granting extensive permissions. Once installed, it gains unauthorised access to contacts, call logs, SMS, GPS location, and even microphone recordings. BtMob RAT operates stealthily, evading detection by leveraging encrypted communication with its command-and-control (C2) server. It can also execute commands to capture screenshots, steal files, and monitor device activity in real time. The malware’s ability to bypass security measures highlights the growing sophistication of mobile threats.

Experts have warned Android users to exercise caution when downloading apps from third-party stores and to regularly update their devices with the latest security patches. As the mobile malware evolves, staying vigilant and adopting robust security practices is crucial to safeguarding personal and organisational data.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Android

Source - https://cyble.com/blog/btmob-rat-newly-discovered-android-malware/

Xelera ransomware exploits fake FCI job offers to target victims

In a disturbing new cyberattack campaign, the Xelera ransomware group is luring victims with fraudulent job offers purportedly from the Food Corporation of India (FCI). According to latest findings, attackers are distributing malicious emails disguised as official FCI recruitment notifications, enticing unsuspecting jobseekers to download malware-laden attachments. Once opened, the attachments deploy the Xelera ransomware, encrypting the victim's files and demanding a ransom for decryption. The campaign exploits the trust associated with a government entity, making it particularly deceptive. Xelera's operators also threaten to leak stolen data if payments are not made, adding pressure on victims.

Experts have warned jobseekers to verify the authenticity of emails and avoid downloading attachments from unknown sources. This incident underscores the growing trend of ransomware groups using social engineering tactics to exploit human vulnerabilities. Vigilance and robust cybersecurity measures are essential to combat such sophisticated threats.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	India	APPLICATION	Windows

Source - https://www.seqrite.com/blog/xelera-ransomware-fake-fci-job-offers/

Nanocore RAT resurfaces with enhanced stealth capabilities

In a recent analysis, the notorious Nanocore RAT has reemerged with advanced features, posing a significant threat to cybersecurity. Known for its extensive spying capabilities, the updated Nanocore RAT now employs sophisticated evasion techniques to bypass detection, making it harder for security tools to identify and mitigate. The malware infiltrates systems through phishing emails or malicious downloads, granting attackers full control over infected devices. Once installed, it can capture keystrokes, hijack webcams, steal sensitive data, and execute remote commands. The latest variant also includes cryptocurrency wallet theft functionality, targeting digital assets.

Reports highlight the RAT's use of encrypted communication channels to coordinate with C2 servers, ensuring persistent access. Cybersecurity experts urge organisations and individuals to strengthen defences by updating software, deploying advanced endpoint protection, and educating users about phishing tactics. As Nanocore RAT evolves, proactive measures are critical to countering its growing threat.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://malwr-analysis.com/2025/02/10/nanocore-rat-malware-analysis/

Android apps emerge as the new frontier for cyber scams

In a startling shift, cybercriminals are now leveraging Android apps to execute phishing attacks, moving beyond traditional email-based schemes. According to latest reports, malicious apps disguised as legitimate tools – such as QR code scanners, fitness trackers, and productivity apps – are being used to steal sensitive user data, including login credentials and financial information. These apps often bypass Google Play Store security checks by appearing harmless initially, only to update later with phishing functionalities. Once installed, they prompt users to enter personal details on fake login pages, which are then harvested by attackers.

Researchers have highlighted the growing sophistication of phishing tactics, urging users to scrutinise app permissions, avoid third-party stores, and rely on trusted security solutions. As phishing evolves, staying informed and vigilant is crucial to safeguarding personal data in an increasingly app-driven threat landscape.

ATTACK TYPE	Phishing	SECTOR	All
REGION	Global	APPLICATION	Android

Source - https://www.malwarebytes.com/blog/news/2025/02/phishing-evolves-beyond-email-to-become-latest-android-app-threat

Sandworm APT targets Ukrainian users with trojanised Microsoft KMS tools

In a recent cyberespionage campaign, the notorious Sandworm APT group has been found targeting Ukrainian users with malicious Microsoft Key Management Service (KMS) activation tools. According to a latest report, the attackers are distributing trojanised versions of these tools, which are commonly used to activate pirated Microsoft software. Once installed, the malware grants Sandworm unauthorised access to victims’ systems, enabling data theft, surveillance, and further network infiltration. The campaign underscores the group’s continued focus on Ukraine, leveraging trusted software to exploit unsuspecting users.

The report has further warned that such attacks highlight the growing sophistication of state-sponsored threat actors, who increasingly use legitimate tools to mask their activities. Organisations and individuals are urged to avoid pirated software, update systems regularly, and deploy advanced threat detection solutions to mitigate risks. As cyberespionage evolves, vigilance and robust security practices remain critical.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns

INTRODUCTION | MICROSOFT FIXES 63 SECURITY VULNERABILITIES | BTMOB RAT THREATENS MOBILE SECURITY GLOBALLY | JOBSEEKERS TARGETED BY THE XELERA RANSOMWARE | NANOCORE RAT REEMERGES WITH NEW CAPABILITIES | MALICIOUS ANDROID APPS DRIVING CYBER SCAMS | SANDWORM APT USES TROJANISED MICROSOFT KMS TOOLS | RANSOMHUB WAS THE BIGGEST RANSOMWARE THREAT IN2024 | CLOAK RANSOMWARE TARGETS USERS AND ENTERPRISES GLOBALLY | NEW DEATHHUNTERS RANSOMWARE TARGET UNSUSPECTING VICTIMS | LUMMA STEALER EXPLOITS EDUCATIONAL INSTITUTIONS WITH CYBERCAMPAIGN

RansomHub emerges as 2024’s most prolific ransomware threat

RansomHub has been identified as the top ransomware threat of 2024, surpassing other notorious groups in both scale and sophistication. According to reports, this ransomware-as-a-service (RaaS) operation has targeted organisations worldwide, encrypting critical data and demanding hefty ransoms for decryption. RansomHub’s success lies in its double-extortion tactics: not only does it encrypt files, but it also threatens to leak stolen data if payments are not made. The group has exploited vulnerabilities in remote desktop protocols (RDP) and phishing campaigns to infiltrate networks, impacting sectors like healthcare, finance, and manufacturing.

Cybersecurity experts warn that RansomHub’s modular infrastructure allows it to adapt quickly, evading detection and maximising damage. Organisations are urged to strengthen defences, implement robust backup strategies, and educate employees on phishing risks. As ransomware threats evolve, proactive measures are essential to mitigate this growing menace.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	PAN-OS, VMware ESXi, Windows

Source - https://thehackernews.com/2025/02/ransomhub-becomes-2024s-top-ransomware.html

INTRODUCTION

MICROSOFT FIXES 63 SECURITY VULNERABILITIES

BTMOB RAT THREATENS MOBILE SECURITY GLOBALLY

JOBSEEKERS TARGETED BY THE XELERA RANSOMWARE

NANOCORE RAT REEMERGES WITH NEW CAPABILITIES

MALICIOUS ANDROID APPS DRIVING CYBER SCAMS

SANDWORM APT USES TROJANISED MICROSOFT KMS TOOLS

RANSOMHUB WAS THE BIGGEST RANSOMWARE THREAT IN2024

CLOAK RANSOMWARE TARGETS USERS AND ENTERPRISES GLOBALLY

NEW DEATHHUNTERS RANSOMWARE TARGET UNSUSPECTING VICTIMS

LUMMA STEALER EXPLOITS EDUCATIONAL INSTITUTIONS WITH CYBERCAMPAIGN

Cloak ransomware targets personal and business data globally

Researchers have issued a warning about the Cloak ransomware, a new and highly evasive malware strain wreaking havoc on both individual users and businesses. This ransomware encrypts files, appending the .cloak extension, and demands payment in cryptocurrency for decryption. What sets Cloak apart is its ability to disable security software and evade detection, making it particularly dangerous. Victims are left with a ransom note detailing payment instructions, often accompanied by threats of permanent data loss if demands are not met. Cloak primarily spreads through phishing emails, malicious attachments, and compromised websites, exploiting human error to infiltrate systems.

Experts have advised users to avoid suspicious links, maintain regular backups, and use robust antivirus software to mitigate risks. For those already infected, the report provides step-by-step guidance on removing the Cloak ransomware and recovering files. As ransomware tactics grow more sophisticated, vigilance and proactive cybersecurity measures are essential to stay protected.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

INTRODUCTION | MICROSOFT FIXES 63 SECURITY VULNERABILITIES | BTMOB RAT THREATENS MOBILE SECURITY GLOBALLY | JOBSEEKERS TARGETED BY THE XELERA RANSOMWARE | NANOCORE RAT REEMERGES WITH NEW CAPABILITIES | MALICIOUS ANDROID APPS DRIVING CYBER SCAMS | SANDWORM APT USES TROJANISED MICROSOFT KMS TOOLS | RANSOMHUB WAS THE BIGGEST RANSOMWARE THREAT IN2024 | CLOAK RANSOMWARE TARGETS USERS AND ENTERPRISES GLOBALLY | NEW DEATHHUNTERS RANSOMWARE TARGET UNSUSPECTING VICTIMS | LUMMA STEALER EXPLOITS EDUCATIONAL INSTITUTIONS WITH CYBERCAMPAIGN

Cybercriminals deploy the DeathHunters ransomware to extort victims

A new ransomware variant, DeathHunters, has emerged, employing aggressive tactics to extort victims. Built on the Chaos ransomware framework, DeathHunters encrypts files, appending a unique four-character extension, and leaves a ransom note titled Read_it_or_Death.txt. The note demands a payment of €1,000 in Bitcoin within five hours, threatening to leak personal data and fabricated illicit content if unpaid. The ransomware also changes the desktop wallpaper, falsely accusing victims of engaging in illegal activities to instil fear and urgency.

Experts warn that paying the ransom does not guarantee data recovery. Victims are advised to remove the ransomware to prevent further encryption and restore files from secure backups. To mitigate such threats, users should maintain up-to-date backups, employ robust security software, and exercise caution with unsolicited communications.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Generic

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

INTRODUCTION
MICROSOFT FIXES 63 SECURITY VULNERABILITIES
BTMOB RAT THREATENS MOBILE SECURITY GLOBALLY
JOBSEEKERS TARGETED BY THE XELERA RANSOMWARE
NANOCORE RAT REEMERGES WITH NEW CAPABILITIES
MALICIOUS ANDROID APPS DRIVING CYBER SCAMS
SANDWORM APT USES TROJANISED MICROSOFT KMS TOOLS
RANSOMHUB WAS THE BIGGEST RANSOMWARE THREAT IN2024
CLOAK RANSOMWARE TARGETS USERS AND ENTERPRISES GLOBALLY
NEW DEATHHUNTERS RANSOMWARE TARGET UNSUSPECTING VICTIMS
LUMMA STEALER EXPLOITS EDUCATIONAL INSTITUTIONS WITH CYBERCAMPAIGN

Lumma Stealer targets educational institutions in PDF-themed cybercampaign

In a sophisticated cyberattack campaign, the Lumma Stealer malware is leveraging compromised educational institutions' infrastructure to distribute malicious PDF-themed files. According to latest findings, attackers are using phishing emails disguised as academic documents to trick users into downloading malware-laden PDFs. Once opened, these files deploy Lumma Stealer, a powerful information-stealing tool capable of harvesting sensitive data, including login credentials, cryptocurrency wallets, and browser cookies. The campaign exploits the trust associated with educational institutions, making it highly effective. Lumma Stealer's operators are also using advanced evasion techniques to bypass security measures, ensuring prolonged access to infected systems.

Experts have warned organisations, especially in the education sector, to enhance email security, educate users about phishing tactics, and monitor network traffic for unusual activity. As cybercriminals continue to innovate, proactive defence strategies are essential to combat such evolving threats.

ATTACK TYPE	Malware	SECTOR	Education
REGION	Global	APPLICATION	Windows

Source - https://www.cloudsek.com/blog/lumma-stealer-chronicles-pdf-themed-campaign-using-compromised-educational-institutions-infrastructure

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.