TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: APRIL 1, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

In today’s fast-changing digital landscape, organisations must adopt proactive cybersecurity measures to combat rising threats. Our weekly Cyber Threat Intelligence (CTI) reports provide critical insights into emerging risks, vulnerabilities, and attack trends, empowering businesses to fortify defences and stay ahead of cyber adversaries.

Through expert analysis and actionable strategies, we help clients anticipate, detect, and neutralise threats before they escalate. This proactive approach not only protects critical assets but also ensures business continuity and strengthens stakeholder confidence. With our CTI insights, organisations can build long-term cyber resilience, navigating the digital world with greater security and assurance.

TATA COMMUNICATIONS

IndoHaxSec: The rising Indonesian hacking collective targeting global organisations

A new hacking group, IndoHaxSec, has emerged as a growing cyber threat, leveraging low-complexity attacks to breach organisations worldwide. According to latest threat intelligence, the Indonesia-based collective has claimed responsibility for multiple high-profile intrusions, including attacks on Australian universities, Indonesian government agencies, and a US-based cybersecurity firm. Unlike sophisticated state-sponsored actors, IndoHaxSec relies on exploiting known vulnerabilities, credential stuffing, and social engineering – tactics that highlight the risks of poor cyber hygiene. The group often boasts about its exploits on social media, suggesting a focus on notoriety rather than financial gain.

Security experts warn that IndoHaxSec's activities signal a broader trend of regional hacktivist groups gaining traction. Organisations are urged to patch vulnerabilities, enforce multi-factor authentication (MFA), and monitor for credential leaks to mitigate risks. As cyber threats evolve, proactive defence measures remain critical in countering emerging collectives like IndoHaxSec.

ATTACK TYPE	Hacktivism, DDoS	**SECTOR**	All
REGION	Indonesia, Malaysia, Australia, US	**APPLICATION**	Generic

Source - https://arcticwolf.com/resources/blog/indohaxsec-emerging-indonesian-hacking-collective/

TATA COMMUNICATIONS

Stealthy steganography attack spreads malware through disguised image files

A sophisticated new malware campaign is using steganography – the art of hiding data within image files – to bypass security defences and infect systems. Discovered by threat researchers, this attack embeds malicious codes inside seemingly harmless BMP image files distributed via phishing emails or compromised websites. Once opened, these images secretly execute scripts that download additional payloads, including remote access trojans (RATs), info-stealers, and ransomware. The technique allows attackers to evade traditional detection methods, making it a growing threat to businesses and individuals.

Key targets include financial, healthcare, and government sectors, where stolen data holds high value. Experts advise organisations to deploy advanced threat detection capable of analysing file anomalies, train employees to spot phishing attempts, and block suspicious macros and scripts. As cybercriminals refine covert delivery methods, experts warn that steganographic attacks may surge this year.

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

Source - https://www.seqrite.com/blog/steganographic-campaign-distributing-malware/

CISA raises alarm about hackers exploiting Fortinet and GitHub flaws

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has urgently added two critical vulnerabilities to its Known Exploited Vulnerabilities catalogue, warning of active attacks targeting Fortinet FortiOS (CVE-2022-42475) – a severe heap-based buffer overflow flaw enabling remote code execution – and GitHub Actions (CVE-2024-37051) – a high-severity privilege escalation vulnerability. Federal agencies must patch these flaws, though all organisations are strongly advised to take immediate action. These vulnerabilities are being actively weaponised, with Fortinet's flaw particularly dangerous as it requires no authentication for exploitation.

Security experts emphasise prioritising patching systems immediately, monitoring network traffic for exploitation attempts, and implementing additional access controls where patching isn't immediately possible. This alert follows a pattern of threat actors increasingly targeting IT infrastructure and developer tools to gain persistent access.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Fortinet, GitHub

Source - https://securityonline.info/cybersecurity-alert-cisa-adds-fortinet-and-github-action-vulnerabilities-to-exploited-list/

Operation Akairyu: MirrorFace targets Europe with revived Anel backdoor

Researchers have uncovered Operation Akairyu, a sophisticated cyberespionage campaign by the China-linked MirrorFace APT group, targeting organisations involved in Europe's Expo 2025 preparations. The attackers have revived the Anel backdoor, previously used in Japanese political cyberattacks, demonstrating evolving tactics. The key findings are:

- Spear-phishing emails impersonate Japanese government entities
- Malicious documents deliver the Anel backdoor, enabling remote system control
- Targets include diplomatic, academic, and research institutions

MirrorFace's reuse of older malware suggests resourcefulness in repurposing tools while maintaining operational security. The campaign highlights growing threats to international events and diplomatic networks. Here are some security recommendations:

- Verify sender authenticity for unsolicited documents
- Update endpoint protection to detect Anel variants
- Monitor for suspicious macro-enabled file activity

As global tensions rise, experts warn of increased APT activity targeting high-profile events.

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

Source - https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

Mass exploitation of PHP vulnerability puts Windows servers at critical risk

Security researchers have issued an urgent warning about widespread exploitation of CVE-2024-4577, a critical PHP vulnerability affecting Windows servers. This flaw allows attackers to execute arbitrary code through argument injection attacks, particularly dangerous for servers running Chinese and Japanese language packs and legacy PHP-CGI implementations. This vulnerability has been actively exploited since June 2024 with attackers deploying web shells and cryptocurrency miners. Over 1,000 vulnerable servers have already been compromised.

The vulnerability stems from improper Unicode conversion in PHP's Windows implementation, enabling attackers to bypass previous security fixes (CVE-2012-1823). Experts report seeing automated scanning and mass exploitation attempts within hours of the vulnerability's disclosure. They recommend immediate updating to PHP versions 8.3.8, 8.2.20, or 8.1.29, disabling PHP-CGI if not essential, and monitoring logs for suspicious .php requests.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Asia	**APPLICATION**	PHP

Source - https://www.bitdefender.com/en-us/blog/businessinsights/technical-advisory-update-mass-exploitation-cve-2024-4577

Sophisticated Cactus ransomware threatens corporate networks

The Indian Computer Emergency Response Team (CERT-In) has issued a critical warning about Cactus ransomware, a highly adaptable malware targeting Windows, ESXi, and Hyper-V environments across corporate networks. The ransomware employs multiple infiltration methods, including exploitation of software vulnerabilities, abuse of administrative tools, and phishing campaigns. Once inside, Cactus encrypts critical data, causing severe financial losses and operational disruptions. CERT-In highlights that organisations in finance, healthcare, and critical infrastructure are particularly vulnerable.

Key mitigation strategies include network segmentation to limit lateral movement, immediate patching of known vulnerabilities, endpoint detection and response (EDR) solutions, comprehensive employee training against phishing, and tested incident response plans. With ransomware attacks escalating globally, CERT-In stresses that proactive defence measures are no longer optional but essential for business continuity. Organisations are urged to audit their cybersecurity posture immediately to prevent devastating breaches.

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

Source - CERT-In

CISA identifies three critical vulnerabilities under active exploitation

CISA has issued an urgent warning about three actively exploited vulnerabilities posing severe risks to organisations worldwide. These flaws affect:

- **IoT devices:** Remote code execution in popular industrial control systems
- **Backup solutions:** Authentication bypass in enterprise backup software
- **Business applications:** Privilege escalation in widely used enterprise platforms

According to CISA's advisory, nation-state actors and cybercriminals are already weaponising these vulnerabilities to gain initial network access, move laterally across systems, and deploy ransomware or steal sensitive data. Organisations are advised to patch affected systems immediately, isolate vulnerable devices from critical networks, monitor for unusual authentication attempts, and implement multi-factor authentication (MFA). With exploitation activity increasing daily, CISA emphasises that delaying remediation could lead to catastrophic breaches.

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

Source - https://securityonline.info/cisa-warns-of-three-actively-exploited-security-vulnerabilities-in-iot-backup-and-enterprise-systems/

TATA COMMUNICATIONS

New ransomware strain D1v35h emerges as growing threat to global enterprises

CERT-In has issued a critical alert about D1v35h, a sophisticated new ransomware strain targeting organisations worldwide. This advanced malware employs double extortion tactics, both encrypting files and stealing sensitive data to pressure victims into paying ransoms. It uses AES-256 encryption with unique keys per victim, targets Windows and Linux systems, spreads through phishing emails and RDP vulnerabilities, and threatens to leak data on dark web portals. Healthcare organisations, financial institutions, and critical infrastructure providers are particularly at risk.

Organisations are advised to ensure immediate patching of RDP and email servers, network segmentation to limit spread, multi-factor authentication (MFA) for all remote access, and regular offline backups. CERT-In warns that D1v35h operators are actively evolving their tactics, making early detection crucial. Organisations are urged to update endpoint protection and train staff on phishing recognition immediately.

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

Source - https://www.linkedin.com/posts/d1v35h_ransomware-cybersecurity-threatintel-activity-7308132663142297604-CxtV/

TATA COMMUNICATIONS

VanHelsing ransomware emerges as new cybersecurity threat to global enterprises

Cybersecurity researchers have uncovered VanHelsing, a sophisticated new ransomware strain wreaking havoc on corporate networks worldwide. This advanced malware employs triple extortion tactics, combining file encryption, data theft, and threats of DDoS attacks to pressure victims into paying ransoms. The ransomware uses RSA-4096 and AES-256 encryption for maximum security bypass, targets both Windows and Linux systems, spreads via phishing campaigns and software vulnerabilities, and threatens to leak stolen data on dark web portals.

Organisations are advised to immediately patch known vulnerabilities, implement network segmentation to limit spread, deploy advanced endpoint detection systems, and conduct regular security audits. With ransomware attacks increasing 47% year-over-year, experts warn VanHelsing represents a dangerous evolution in cyber threats. Organisations are urged to update defences immediately as this ransomware variant continues to spread globally.

ATTACK TYPE	Ransomware	**SECTOR**	Pharmaceuticals, manufacturing, government
REGION	Global	**APPLICATION**	Windows

Source - https://www.cyfirma.com/research/vanhelsing-ransomware/

RansomHub emerges as new cyber threat, leveraging Betrüger backdoor

Security researchers have uncovered RansomHub, a dangerous new ransomware operation using the Betrüger backdoor to infiltrate corporate networks undetected. The malware-as-a-service (MaaS) platform is being offered to cybercriminals, enabling widespread attacks with advanced evasion techniques. It deploys Betrüger backdoor for persistent access, uses living-off-the-land tactics to avoid detection, deploys double extortion scheme, and targets Windows and Linux systems. The ransomware gains initial access via phishing or exploits, installs the backdoor stealthily, does a network reconnaissance, and exfiltrates and encrypts data.

Healthcare, financial services, and critical infrastructure organisations are particularly at risk. They are advised to patch known vulnerabilities immediately, implement multi-factor authentication (MFA), monitor for unusual RDP/VPN activity, and deploy behaviour-based threat detection. With ransomware attacks fast increasing, organisations must act now to protect against this emerging threat.

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

Source - https://www.security.com/threat-intelligence/ransomhub-betruger-backdoor

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