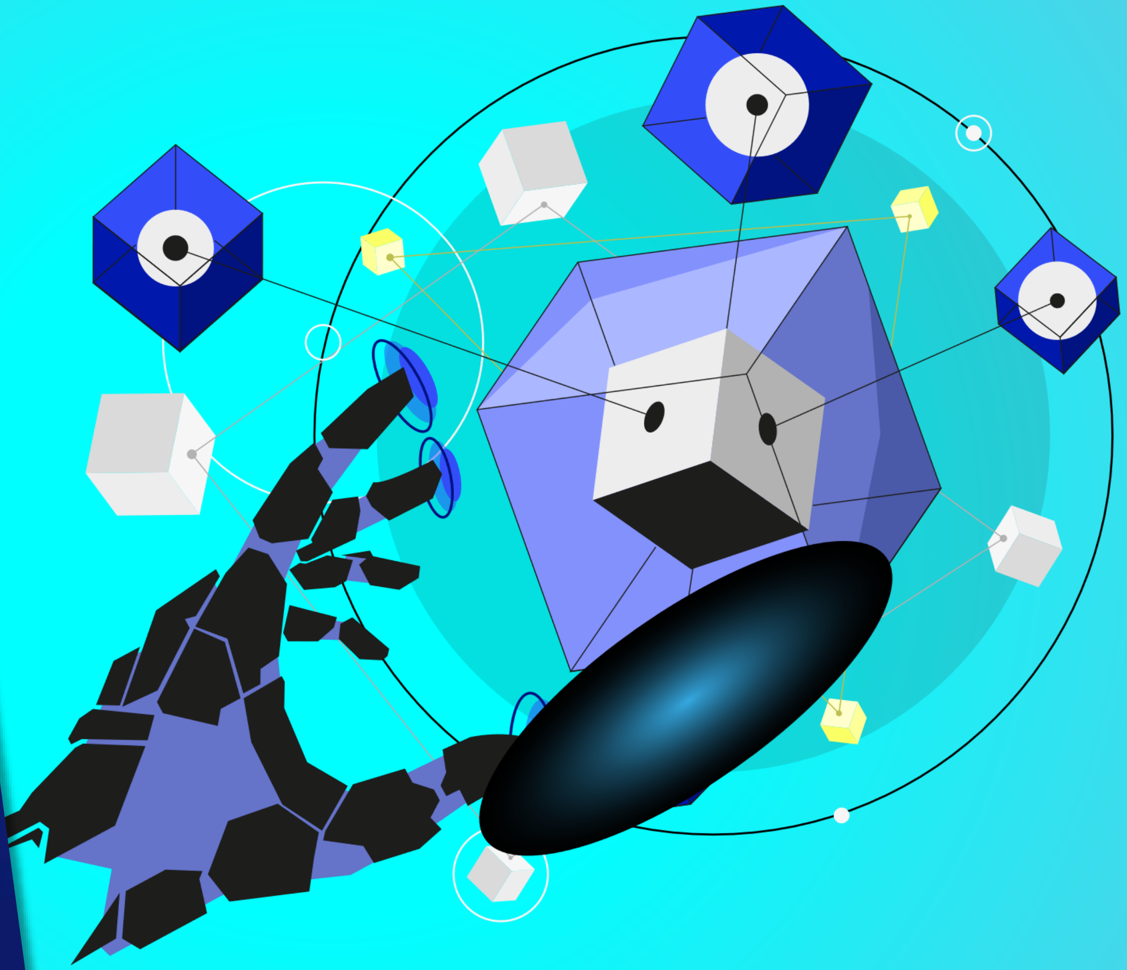
TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MAY 27, 2025



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.

SAP May 2025 patch fixes zero-day exploited in the wild

SAP's May 2025 Patch Day addressed 16 newly discovered vulnerabilities and updated 2 previously known issues. Most notably, the critical zero-day CVE-2025-31324 in SAP NetWeaver is confirmed to be under active exploitation. The patch release also includes fixes for SAP S/4HANA and Supplier Relationship Management (SRM) modules. Vulnerabilities affect remote code execution, authentication bypass, and privilege escalation, —posing serious risks for enterprises relying on SAP to manage core business processes.

Businesses must prioritise immediate patching across all SAP systems, especially NetWeaver deployments. Given the complexity of enterprise SAP environments, patch management should be coordinated with rigorous regression testing. Security teams should actively monitor SAP logs and network traffic for indicators of compromise, particularly unauthorised administrative access, or anomalous queries. SAP-specific security tools, such as SAP Enterprise Threat Detection (ETD), can assist in detecting abuse. Backup strategies must be validated, and business continuity plans updated to handle potential disruptions.

ATTACK TYPE	Vulnerability	SECTOR	Global
REGION	All	APPLICATION	SAP

Source - https://securityonline.info/sap-security-alert-may-2025-patch-day-exposes-critical-threats/

Chihuahua Stealer deploys stealthy, multi-stage data theft

Chihuahua Stealer is a .NET-based malware that employs advanced evasion tactics to steal browser data, session cookies, and cryptocurrency wallet credentials. It spreads via heavily obfuscated PowerShell scripts and maintains persistence using scheduled tasks and custom file markers. The malware avoids detection through in-memory payload execution and AES-GCM encryption, packaging stolen data in encrypted archives before exfiltration. Its stealth-focused delivery chain marks it as one of the more advanced info-stealers seen this year.

To protect against threats like Chihuahua Stealer, organisations should disable or restrict PowerShell usage where possible and enable script block logging for better visibility. Endpoint Detection and Response (EDR) tools must be tuned to detect memory-based threats and persistence mechanisms. User behaviour analytics (UBA) can help spot credential misuse or abnormal access to crypto-related assets. Regular audits of browser extension permissions and the implementation of zero-trust access policies will further limit the attack surface. Employee education should include red flags for social engineering and “fix-it” script lures that commonly deliver such malware.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.gdatasoftware.com/blog/2025/05/38199-chihuahua-infostealer

INTRODUCTION | ZERO-DAY IN SAP NETWEAVER DEMANDS IMMEDIATE ACTION | CHIHUAHUA STEALER: SMALL STATURE, BIG DATA THEFT | MICROSOFT FIXES 5 ZERO-DAYS IN MAY PATCH BLITZ | EARTH AMMIT APT TARGETS DRONE SUPPLY CHAINS | HORABOT MALWARE PHISHES LATIN AMERICA WITH FAKE INVOICES | DARKCLOUD RETURNS WITH AUTOIT AND IN-MEMORY PAYLOADS | INTERLOCK RANSOMWARE HITS U.S. DEFENCE FIRM WITH ESPIONAGE INTENT | BIANLIAN, RANSOMEXX EXPLOIT SAP NETWEAVER WITH PIPEMAGIC | J GROUP RANSOMWARE: RUST-BUILT AND GLOBALLY DEPLOYED | BERT RANSOMWARE ENCRYPTS AND EXTORTS VIA SESSION APP

Microsoft May 2025 patch fixes 5 actively exploited zero-days

Microsoft's May 2025 security update resolves 82 vulnerabilities, including 75 newly reported CVEs and 12 critical flaws. Among these are five zero-days actively exploited in the wild, —particularly CVE-2025-30397, a memory corruption vulnerability in the Windows scripting engine. The updates cover Windows OS, Microsoft Office, .NET Framework, Azure, and developer tools. Many of the vulnerabilities enable remote code execution, privilege escalation, and security bypass, —particularly within Office and scripting components.

Organisations must immediately deploy the latest patches across all Microsoft ecosystems, including client and server environments. Prioritisation should be based on exploitability, criticality, and business exposure. Vulnerability scanners and patch management systems (e.g., WSUS, SCCM, Intune) should be audited to ensure updates apply successfully. SOC teams must look for anomalous scripting engine behaviour, especially in Office documents and browser contexts. Application whitelisting, sandboxing email attachments, and leveraging Microsoft Defender ATP are all essential components of a layered defence. The sheer volume and repeated targeting of Office-related components suggest a need for greater vigilance against phishing and macro-based malware campaigns.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2025-patch-tuesday-fixes-5-exploited-zero-days-72-flaws/

INTRODUCTION | ZERO-DAY IN SAP NETWEAVER DEMANDS IMMEDIATE ACTION | CHIHUAHUA STEALER: SMALL STATURE, BIG DATA THEFT | MICROSOFT FIXES 5 ZERO-DAYS IN MAY PATCH BLITZ | EARTH AMMIT APT TARGETS DRONE SUPPLY CHAINS | HORABOT MALWARE PHISHES LATIN AMERICA WITH FAKE INVOICES | DARKCLOUD RETURNS WITH AUTOIT AND IN-MEMORY PAYLOADS | INTERLOCK RANSOMWARE HITS U.S. DEFENCE FIRM WITH ESPIONAGE INTENT | BIANLIAN, RANSOMEXX EXPLOIT SAP NETWEAVER WITH PIPEMAGIC | J GROUP RANSOMWARE: RUST-BUILT AND GLOBALLY DEPLOYED | BERT RANSOMWARE ENCRYPTS AND EXTORTS VIA SESSION APP

Earth Ammit APT group targets East Asia’s critical infrastructure

Earth Ammit, a Chinese-speaking APT group, has executed two interconnected campaigns — VENOM and TIDRONE — against critical infrastructure in Taiwan and South Korea. The VENOM campaign used open-source tools to infiltrate upstream IT providers, while TIDRONE employed custom malware (CXCLNT and CLNTEND) for surveillance and data theft in the drone and military supply chain sectors. These long-term campaigns reflect advanced cyber-espionage tradecraft, including strategic targeting, layered persistence, and infrastructure manipulation.

To mitigate APT threats like Earth Ammit, critical infrastructure operators should implement zero-trust architecture and enforce network segmentation between supplier access points and operational technology (OT) systems. Email security, sandboxed attachment scanning, and DNS filtering can help disrupt initial infection attempts. Detection rules should be tuned to spot the use of dual-use tools and behaviour matching Earth Ammit’s malware. Threat intelligence collaboration with national cybersecurity agencies is critical, especially when state-linked groups may be involved. Regular red-teaming exercises and audits of third-party integrations will further reduce supply chain risks.

ATTACK TYPE	Malware	SECTOR	Healthcare/hospitals , IT , Military , Broadcast Media Production and Distribution
REGION	South Korea , Taiwan	APPLICATION	Windows

Source - https://securityonline.info/earth-ammit-strikes-drone-supply-chains-venom-and-tidrone-campaigns-expose-east-asias-critical-infrastructure/

Horabot malware phishing targets Latin America with layered scripts

Horabot is a multi-layered phishing malware targeting Spanish-speaking users in Latin America. Disguised as fake invoice emails, the malware chain uses VBScript, AutoIt, and PowerShell to evade defences, steal credentials, and propagate via Outlook contact lists. It collects browser and system data before deleting traces to hinder forensic analysis. The campaign emphasises business email compromise (BEC) risks and highlights the evolving sophistication of Latin American threat actors.

Enterprises should bolster defences with layered email protection that includes SPF, DKIM, and DMARC enforcement, combined with real-time link inspection and sandboxing. AutoIt and PowerShell execution policies must be restricted on user endpoints, especially for non-IT users. SOC teams should review outbound Outlook activities and look for indicators of lateral phishing within the organisation. Continuous employee training focused on invoice-based phishing and email hygiene can reduce attacks’ success. Where possible, monitoring outbound connections and data exfiltration attempts will improve visibility into stealthy malware campaigns like Horabot.

ATTACK TYPE	Malware	SECTOR	All
REGION	Latin America	APPLICATION	Windows

Source - https://securityonline.info/horabot-malware-targets-latin-america-with-sophisticated-phishing/

DarkCloud Stealer returns with AutoIt-powered persistence

DarkCloud Stealer, seen for the first time in 2022, has resurfaced with a more advanced version, leveraging AutoIt scripting and multi-stage payloads that operate almost entirely in memory. The latest variant targets the government, telecom, financial, and media sectors, particularly in regions like Poland, Brazil, and the U.S. DarkCloud's delivery relies heavily on phishing emails with encrypted attachments and uses anti-analysis and obfuscation tactics to remain undetected. Once active, it steals credentials and browser data, using encrypted channels to exfiltrate the information.

To combat DarkCloud, organisations must implement EDR solutions with strong memory-scanning and script-monitoring capabilities. Email security gateways should quarantine encrypted attachments by default, and user education should emphasise caution when dealing with suspicious file formats. Threat detection teams must monitor for AutoIt and PowerShell execution anomalies, while SOCs should maintain up-to-date IOCs (Indicators of Compromise) for known variants. Log analysis and network anomaly detection will be crucial for identifying stealthy, post-compromise behaviour. The proactive use of threat intelligence and information sharing among industry peers can enable early detection.

ATTACK TYPE	Malware	SECTOR	Financial Services, Manufacturing, IT, Government, Broadcast Media Production and Distribution
REGION	Brazil, Hungary, Netherlands, Peru, Turkey, United States	APPLICATION	Windows

Source - https://unit42.paloaltonetworks.com/darkcloud-stealer-and-obfuscated-autoit-scripting/

INTRODUCTION | ZERO-DAY IN SAP NETWEAVER DEMANDS IMMEDIATE ACTION | CHIHUAHUA STEALER: SMALL STATURE, BIG DATA THEFT | MICROSOFT FIXES 5 ZERO-DAYS IN MAY PATCH BLITZ | EARTH AMMIT APT TARGETS DRONE SUPPLY CHAINS | HORABOT MALWARE PHISHES LATIN AMERICA WITH FAKE INVOICES | DARKCLOUD RETURNS WITH AUTOIT AND IN-MEMORY PAYLOADS | INTERLOCK RANSOMWARE HITS U.S. DEFENCE FIRM WITH ESPIONAGE INTENT | BIANLIAN, RANSOMEXX EXPLOIT SAP NETWEAVER WITH PIPEMAGIC | J GROUP RANSOMWARE: RUST-BUILT AND GLOBALLY DEPLOYED | BERT RANSOMWARE ENCRYPTS AND EXTORTS VIA SESSION APP

Interlock ransomware targets AMTEC with espionage motives

Interlock ransomware has been used in a high-impact attack on AMTEC, a U.S. defence manufacturer and subsidiary of National Defense Corporation. The breach exposed sensitive logistics and contractual data with major global defence partners. While ransomware is typically financially motivated, the specificity of this breach points to geopolitical espionage. Data exfiltration, network reconnaissance, and possible nation-state affiliations make this more than just a standard extortion case.

Organisations in the defence and aerospace sectors must consider ransomware as a potential espionage tool, not just a financial threat. Advanced network segmentation, least-privilege access, and continuous monitoring of sensitive systems are essential. Data loss prevention (DLP) tools and endpoint forensics should be used to track unusual transfers and file access patterns. Regular backup validation and offline storage reduce ransom leverage. Security teams should prepare incident response plans that factor in geopolitical risks and include coordination with national cyber defence agencies. The Interlock case reinforces the convergence of cybercrime and state-sponsored tactics in targeting critical industries.

ATTACK TYPE	Ransomware	SECTOR	United States
REGION	Defence Industry, Defence and Space Manufacturing	APPLICATION	Windows

Source - https://www.resecurity.com/blog/article/how-interlock-ransomware-affects-the-defense-industrial-base-supply-chain

INTRODUCTION | ZERO-DAY IN SAP NETWEAVER DEMANDS IMMEDIATE ACTION | CHIHUAHUA STEALER: SMALL STATURE, BIG DATA THEFT | MICROSOFT FIXES 5 ZERO-DAYS IN MAY PATCH BLITZ | EARTH AMMIT APT TARGETS DRONE SUPPLY CHAINS | HORABOT MALWARE PHISHES LATIN AMERICA WITH FAKE INVOICES | DARKCLOUD RETURNS WITH AUTOIT AND IN-MEMORY PAYLOADS | INTERLOCK RANSOMWARE HITS U.S. DEFENCE FIRM WITH ESPIONAGE INTENT | BIANLIAN, RANSOMEXX EXPLOIT SAP NETWEAVER WITH PIPEMAGIC | J GROUP RANSOMWARE: RUST-BUILT AND GLOBALLY DEPLOYED | BERT RANSOMWARE ENCRYPTS AND EXTORTS VIA SESSION APP

BianLian and RansomExx exploit SAP NetWeaver with PipeMagic Trojan

Multiple threat actors, including BianLian, RansomExx, and Chinese APTs, are exploiting CVE-2025-31324, a critical SAP NetWeaver vulnerability. The attacks involve the deployment of sophisticated malware like PipeMagic and Brute Ratel, with some also chaining CVE-2025-42999. These attacks seize full system access, enabling data theft, lateral movement, and extortion through ransomware payloads. SAP environments are increasingly attractive to cybercriminals and nation-state actors alike due to their deep integration into enterprise operations.

Immediate patching of CVE-2025-31324 and the related vulnerabilities is essential. Organisations must apply vendor updates across SAP NetWeaver and closely monitor for signs of exploitation using SAP Enterprise Threat Detection (ETD) or SIEM integration. EDR and XDR tools should be configured to detect PipeMagic behaviour, DLL sideloading, and Brute Ratel signatures. Limiting administrative access, segmenting ERP systems, and deploying database activity monitoring will help limit exposure. Regular SAP security audits and threat hunting for persistence mechanisms can help detect existing compromises. Given the actors involved, enterprises should treat these threats as high-impact incidents with possible geopolitical implications.

ATTACK TYPE	Vulnerability, Ransomware	SECTOR	All
REGION	Global	APPLICATION	SAP

Source - https://thehackernews.com/2025/05/bianlian-and-ransomexx-exploit-sap.html

J Group ransomware emerges as cross-platform threat

J Group is a new ransomware operator that has quickly gained notoriety with attacks across 14 countries, targeting both Windows and Linux environments. Its ransomware binaries, compiled in Rust, mimic the structure of Akira ransomware and show code-level similarities to Babuk. Infrastructure is hosted on nginx servers, and the payloads are optimised for fast encryption and stealth. J Group's global reach and rapid development mark it as an emerging major threat.

Organisations must prepare for J Group's cross-platform approach by ensuring both Windows and Linux systems are covered under their security policies. Backup systems must be isolated and tested regularly for full restoration capabilities. SOC teams should monitor for unusual process behaviours and lateral movement patterns, particularly those involving newly compiled binaries or unsigned executables. Linux servers should be hardened, and SSH access restricted using key-based authentication. Threat intelligence teams should track emerging indicators related to Rust-compiled payloads and nginx-hosted infrastructure. Given the group's potential, early containment and rapid response are key to minimising damage.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Australia, India, Argentina, Brazil, China, France, Germany, Luxembourg, Spain, United States, Vietnam	APPLICATION	Windows, Linux

Source - https://www.linkedin.com/posts/ctiacademy_new-ransomware-group-alert-j-ransomware-activity-7324407966718214144-zHw8/

Bert ransomware uses PowerShell and Session App for double extortion

Bert ransomware is a newly observed variant targeting Windows environments in the healthcare, finance, and manufacturing sectors. It encrypts files with the “.encryptedbybert” extension and drops ransom notes via the Session messaging app. It uses PowerShell-based loaders, anti-debugging techniques, and registry modifications for persistence. Bert also engages in data exfiltration, applying double extortion tactics to increase pressure on victims. Its stealth and agility make it a rising concern in ransomware operations.

Enterprises should implement PowerShell logging and block risky script execution through Group Policy. Anti-ransomware solutions must monitor for file encryption behaviour and unauthorised registry changes. Detecting Session app-based communication or its unique network signatures can help in identifying infected hosts. Backups should be immutable, encrypted, and segmented to avoid simultaneous compromise. User awareness training must emphasise the dangers of opening unsolicited attachments and the importance of reporting suspicious behaviour immediately. The Bert campaign demonstrates that emerging ransomware groups are adopting advanced techniques quickly, requiring continuous vigilance and defence adaptation.

ATTACK TYPE	Ransomware	SECTOR	Healthcare/hospitals, Business, Software Development
REGION	Taiwan, Turkey, United States	APPLICATION	Windows

Source - https://www.broadcom.com/support/security-center/protection-bulletin/bert-ransomware

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.