TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 22, 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.

Android zero-day exploits addressed in Google security update

On April 8, 2025, Google rolled out a critical Android security update patching 62 vulnerabilities, including two actively exploited zero-day flaws. Of particular concern is CVE-2024-53197, used by Serbian authorities with Cellebrite forensic tools to unlock confiscated devices. This vulnerability, paired with other high-severity privilege escalation flaws and kernel information leaks, underscores the persistent risk to Android users globally. These zero-days allowed threat actors—and even law enforcement agencies—to bypass traditional device security, posing a severe threat to data confidentiality and device integrity.

Organisations with mobile workforces or bring-your-own-device (BYOD) environments should urgently assess device patch compliance. Mobile Device Management (MDM) solutions should be configured to enforce timely updates and flag devices running outdated OS versions. Additionally, threat hunting teams should monitor for unusual access patterns and lateral movement stemming from potentially compromised Android endpoints. Google's ongoing patching efforts are crucial, but businesses must implement layered defences—including endpoint protection and strong mobile access controls—to stay ahead of such rapidly exploited vulnerabilities.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Android

Source - https://www.bleepingcomputer.com/news/security/google-fixes-android-zero-days-exploited-in-attacks-60-other-flaws/

INTRODUCTION | Android zero-day exploits addressed in Google security update | Nanocrypt: An evolving threat in the ransomware landscape | Craxsrat ransomware is an emerging threat targeting global organisations | Vidar Stealer's updated tactics make it more menacing than ever before | Windows CLFS zero-day vulnerability exploited by ransomware group | SideCopy APT escalates India-focused cyber campaigns | SAP releases April 2025 patch that protects against critical risks | Sarcoma Group ransomware is an evolving new threat | SKUNK: A hacktivist façade with classic ransomware tactics | Microsoft patches one zero-day and 134 other vulnerabilities

Nanocrypt: An evolving threat in the ransomware landscape

Nanocrypt is an aggressive ransomware variant that encrypts victims' data using RSA and AES algorithms, appending the ".ncrypt" extension and demanding a $50 Bitcoin ransom. Despite the low monetary demand, victims often remain permanently locked out of their files, making the true cost of infection much higher. Nanocrypt propagates through phishing emails, cracked software, and malicious advertising (malvertising), allowing it to rapidly spread across devices and networks. Once embedded, it establishes persistence, potentially allowing reinfection even after removal.

Organisations must treat Nanocrypt as a serious threat regardless of the ransom size. Proactive defences should include email filtering, endpoint detection and response (EDR), and strict web content filtering to block malvertising. Regular employee training is essential to reduce susceptibility to phishing. Furthermore, maintaining encrypted and segmented backups—tested regularly for integrity—can minimise downtime and avoid data loss. Infected systems should be isolated immediately to prevent lateral movement and given Nanocrypt's deceptive tactics and destructive behaviour, businesses should also prioritise in-depth strategies combined with a swift incident response plan.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

Craxsrat ransomware is an emerging threat targeting global organisations

Craxsrat is a fast-acting ransomware variant that has recently emerged on the global stage, targeting Windows systems by encrypting data and appending the “.craxsrat” extension. Victims are instructed to pay a $50 ransom in Bitcoin to regain access. While the ransom demand appears minor, the real danger lies in Craxsrat’s rapid propagation and ability to evade basic defences. It spreads via phishing, trojanised downloads, and malicious links, threatening data availability and business continuity.

Despite its small ransom, organisations should not underestimate Craxsrat. Early detection is key, which means investing in behaviour-based endpoint protection and continuous monitoring of file activity and encryption patterns. Network segmentation, strong access control, and timely patching of vulnerabilities are crucial to limiting the blast radius of an infection. Since Craxsrat may be used as a testbed for future, more sophisticated variants, companies should view it as an early warning and strengthen their ransomware readiness plans, including offline backups and simulation-based incident response training.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

Vidar Stealer's updated tactics make it more menacing than ever before

Vidar Stealer has returned with new tactics that make it harder to detect, embedding itself in a trojanised version of Microsoft’s BGInfo utility. It cleverly uses an expired but seemingly legitimate digital signature and mimics metadata to appear trustworthy. This allows the malware to bypass many security filters, launching its payload to extract sensitive information such as browser credentials, crypto wallets, and system details. Its stealth and targeting of trusted software illustrate a growing trend in malware delivery.

Organisations should take this case as a warning to scrutinise even widely-used tools—especially those downloaded from unofficial sources or shared internally. Application whitelisting, code-signature verification, and robust file integrity monitoring can help flag tampered software. IT teams should regularly audit installed applications and remove unauthorised software from corporate devices. Additionally, user awareness programs should also strongly emphasise caution when downloading tools.

ATTACK TYPE	Malware	SECTOR	Healthcare, IT, government, real estate, retail and distribution
REGION	Global	APPLICATION	Windows

Source - https://www.gdatasoftware.com/blog/2025/04/38169-vidar-stealer

Windows CLFS zero-day vulnerability exploited by ransomware group

CVE-2025-29824, a zero-day vulnerability in the Windows Common Log File System (CLFS), has been exploited in the wild by the ransomware group Storm-2460. This flaw enables attackers to escalate privileges to SYSTEM level – one of the most dangerous permissions on Windows systems – allowing them to deploy ransomware payloads with devastating impact. In parallel, CVE-2025-30406 in Gladinet CentreStack also poses remote code execution risks. Both vulnerabilities have global implications and require urgent attention.

Organisations should prioritise patching all Windows endpoints and CentreStack instances, especially those exposed to the internet. Endpoint protection tools should be configured to monitor and alert on unusual privilege escalation or file access behaviour. Security teams should also validate that system hardening guidelines are enforced, including disabling unnecessary services and accounts. Implementing strong identity and access management (IAM) policies – such as least privilege and multi-factor authentication – further reduces the attack surface. Rapid vulnerability management processes and patch orchestration are essential to stay resilient against fast-moving zero-day exploits like this one.

ATTACK TYPE	Ransomware, vulnerability	SECTOR	Global
REGION	All	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/security/microsoft-windows-clfs-zero-day-exploited-by-ransomware-gang/

SideCopy APT escalates attacks on India's critical infrastructure

The Pakistan-linked SideCopy APT group has significantly intensified its cyber espionage campaign against India, now targeting critical sectors such as oil and gas, railways, and foreign affairs. The group transitioned from HTA-based to MSI-based malware delivery, employing sophisticated techniques including DLL side-loading, reflective loading, and PowerShell-based AES decryption. Its toolkit includes modified versions of open-source RATs, notably CurlBack RAT, and utilises spoofed domains for phishing and payload deployment.

To counter such persistent threats, Indian infrastructure organisations must embrace a nation-state-level cybersecurity posture. This includes aggressive network segmentation, endpoint detection and response (EDR), and behavioural analytics to detect lateral movement and stealthy malware. Security teams should deploy threat intelligence feeds tuned to SideCopy’s tactics, techniques, and procedures (TTPs). Organisations must also reinforce identity management systems, limit administrative access, and conduct red team exercises to simulate targeted APT attacks. Information sharing between sectors and CERT-IN is critical to mitigating coordinated APT campaigns.

ATTACK TYPE	Malware	SECTOR	Government, oil and gas, defence
REGION	India	APPLICATION	Windows

Source - https://www.seqrite.com/blog/goodbye-hta-hello-msi-new-ttps-and-clusters-of-an-apt-driven-by-multi-platform-attacks/

SAP releases April 2025 patch that protects against critical code injection risks

SAP's April 2025 Patch Day addressed 18 new and 2 updated vulnerabilities, many of which carry critical severity scores. Among the most pressing are code injection flaws within SAP S/4HANA and SAP Landscape Transformation (SLT), which could permit attackers to fully compromise systems. An authentication bypass vulnerability in SAP Financial Consolidation was also patched, adding to the urgency. Given SAP's integral role in business operations—ranging from supply chain management to financial reporting—these flaws could enable system-wide disruption or data breaches if left unpatched.

Organisations relying on SAP systems should immediately assess their exposure and apply the latest patches. IT and security teams must coordinate closely to minimise downtime during updates while ensuring thorough testing in staging environments. Additionally, implementing strict access controls, input validation, and logging around SAP interfaces helps reduce the risk of code injection and unauthorised access. Regular vulnerability assessments and real-time security monitoring of SAP environments are vital for defending against increasingly sophisticated exploitation attempts, especially in ERP systems that handle critical business data.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	SAP

Source - https://securityonline.info/sap-april-2025-patch-day-critical-code-injection-risks/

Sarcoma Group ransomware is an evolving new threat

Sarcoma Group ransomware is a highly disruptive threat that uses strong encryption to lock files and employs double extortion tactics by stealing sensitive data before demanding a ransom. This approach increases pressure on victims by threatening public leaks. The malware typically infiltrates through phishing emails, unpatched software vulnerabilities, and poorly secured Remote Desktop Protocol (RDP) setups. Its broad targeting of organisations globally raises alarm for sectors that rely heavily on uninterrupted data access, such as healthcare, logistics, and education.

To defend against Sarcoma Group ransomware, organisations should implement a layered security approach. Strong email security gateways and user training are critical to reducing phishing success rates. RDP should be disabled if not essential or protected using VPNs and multi-factor authentication. Backup strategies must prioritise redundancy and isolation to avoid simultaneous encryption or deletion. Security teams should use ransomware-specific detection rules, monitor for suspicious data exfiltration, and develop response playbooks that include legal and PR considerations due to the data leak risk.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyclonis.com/remove-sarcoma-group-ransomware/

SKUNK: A hacktivist façade with classic ransomware tactics

SKUNK ransomware presents an unusual case – it encrypts files and alters system settings but doesn’t demand a ransom. Instead, it adopts the appearance of a political or hacktivist protest, appending the “.SKUNK” extension and claiming responsibility in a manifesto-like note. Despite the absence of monetary motivation, the result is the same: business disruption, lost access to critical data, and potential reputational harm. The malware claims the ability to spread laterally across networks, though this behaviour is still under analysis.

Organisations must treat SKUNK as seriously as financially motivated ransomware. While there may be no ransom, the risk to operations, compliance, and public trust remains. Incident response teams should prioritise containment and forensic analysis to determine whether it is a genuine protest, cover for data theft, or a test deployment for future attacks. Strong segmentation, regular vulnerability patching, and disabling unnecessary file-sharing protocols can help reduce risk. It's also important to integrate threat intelligence about non-financially motivated actors into organisational security planning, as hacktivist-style ransomware may become more common in politically tense environments.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

Microsoft patches one zero-day and 134 other vulnerabilities in April update

Microsoft's April 2025 Patch Tuesday addressed a total of 134 vulnerabilities, including 11 marked as critical and one actively exploited zero-day – CVE-2025-29824. This specific flaw affects the Windows CLFS driver, enabling privilege escalation and has been linked to the RansomEXX ransomware group. Given the breadth of vulnerabilities across multiple Microsoft products, including Office and Azure, this update is crucial for maintaining enterprise security posture.

Organisations should immediately deploy the April updates through automated patch management tools while ensuring critical systems are tested for compatibility. Since CVE-2025-29824 has been exploited in the wild, IT teams should investigate whether indicators of compromise (IOCs) tied to RansomEXX are present in logs. In parallel, least-privilege policies should be reviewed, and user behaviour analytics deployed to detect abuse of elevated access. To keep pace with the increasing volume of monthly patches, organisations should also refine their vulnerability management lifecycle – prioritising threats based on exploitability and business impact.

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

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2025-patch-tuesday-fixes-exploited-zero-day-134-flaws/

INTRODUCTION

Android zero-day exploits addressed in Google security update

Nanocrypt: An evolving threat in the ransomware landscape

Craxsrat ransomware is an emerging threat targeting global organisations

Vidar Stealer's updated tactics make it more menacing than ever before

Windows CLFS zero-day vulnerability exploited by ransomware group

SideCopy APT escalates India-focused cyber campaigns

SAP releases April 2025 patch that protects against critical risks

Sarcoma Group ransomware is an evolving new threat

SKUNK: A hacktivist façade with classic ransomware tactics

Microsoft patches one zero-day and 134 other vulnerabilities

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.