TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 29, 2025

TATA

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.

DarkMystic ransomware: A rising threat from the BlackBit family

DarkMystic, a recently detected ransomware variant stemming from the BlackBit ransomware family, is designed to encrypt victims’ data and demand Bitcoin payments under heavy threats of data destruction or public exposure. It spreads rapidly through phishing emails, malicious downloads, and lateral movement within compromised networks. The ransomware uses robust encryption methods, making file recovery without decryption keys nearly impossible. Victims without secured offline backups are especially vulnerable to permanent data loss.

Organisations must adopt a proactive and layered defence strategy to mitigate DarkMystic. This includes deploying advanced endpoint protection, filtering phishing attempts, and training employees on safe email handling. Also, network segmentation can prevent widespread lateral movement post-compromise. Most critically, IT departments must enforce a regular backup policy with offsite or immutable backup options and test recovery procedures frequently. As paying the ransom doesn't guarantee file recovery, containment and rapid incident response remain paramount. Adopting a zero-trust framework and conducting regular security assessments can further reduce ransomware exposure.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

Jackalock ransomware is MedusaLocker’s data-leaking descendant

Jackalock is a new ransomware variant believed to descend from the MedusaLocker family. Like its predecessor, it encrypts victims’ data and appends a “.jackalock” extension while threatening to leak stolen data if the ransom demand is not met. The malware targets Windows systems across sectors and spreads through phishing, malicious attachments, and exploitation of unpatched software vulnerabilities. Recovery without backups is rarely possible due to its use of strong encryption and potential for double extortion.

To protect against Jackalock, organisations should invest in vulnerability management and endpoint protection solutions capable of detecting ransomware behaviours. Maintaining up-to-date software and enforcing strict patch management policies are essential. Email security solutions, combined with phishing simulation and user awareness training, reduce the likelihood of successful entry. Also, secure and segmented backup solutions are key for recovery. Additionally, incident response teams should prepare containment protocols and monitor for signs of data exfiltration to prevent public exposure. Transparency and coordination with legal and compliance teams are also critical during ransomware incidents.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

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

INTRODUCTION | DARKMYSTIC RANSOMWARE EMERGES WITH A VENGEANCE | JACKALOCK RANSOMWARE THREATENS STOLEN DATA LEAK | CHROME UPDATE BLOCKS CRITICAL CODE EXECUTION FLAWS | APPLE RUSHES IOS PATCH FOR ACTIVE ZERO-DAY EXPLOITS | FIREFOX RACE CONDITION BUG FIXED IN LATEST UPDATE | INTERLOCK RANSOMWARE USES FAKE UPDATES AND PHISHING LURES | SONICWALL SMA100 VULNERABILITY ACTIVELY EXPLOITED | AKIRA RANSOMWARE LINKED TO MAJOR CYBERCRIME GROUPS | XORDDOS MALWARE UPGRADES FOR LARGE-SCALE LINUX ATTACKS | FOG RANSOMWARE EXPLOITS FAKE GOVERNMENT MESSAGING

Chrome zero-days patched with major fixes for CVE-2025-3619 and CVE-2025-3620

Google has released Chrome version 135.0.7049.95/.96 to patch two major security vulnerabilities—CVE-2025-3619, a critical heap buffer overflow, and CVE-2025-3620, a high-severity use-after-free bug. These vulnerabilities could allow remote attackers to execute arbitrary code and compromise entire systems via malicious web content. Google is withholding full technical details until most users apply the patch, underscoring the urgency of updating.

Enterprises should ensure that Chrome browsers across all endpoints are updated immediately, especially in environments where browser-based applications are widely used. Browser configuration policies should enforce auto-updates and restrict the installation of untrusted extensions. In enterprise settings, vulnerability scanners should be used to confirm patch deployment. Organisations should also consider browser isolation technologies to reduce the risk of exploitation via drive-by attacks. User behaviour monitoring, threat intelligence integration, and DNS filtering are additional layers that can help thwart web-based attacks leveraging browser vulnerabilities.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Chrome

Source - https://securityonline.info/critical-chrome-security-update-patch-cve-2025-3619-cve-2025-3620-now/

INTRODUCTION | DARKMYSTIC RANSOMWARE EMERGES WITH A VENGEANCE | JACKALOCK RANSOMWARE THREATENS STOLEN DATA LEAK | CHROME UPDATE BLOCKS CRITICAL CODE EXECUTION FLAWS | APPLE RUSHES IOS PATCH FOR ACTIVE ZERO-DAY EXPLOITS | FIREFOX RACE CONDITION BUG FIXED IN LATEST UPDATE | INTERLOCK RANSOMWARE USES FAKE UPDATES AND PHISHING LURES | SONICWALL SMA100 VULNERABILITY ACTIVELY EXPLOITED | AKIRA RANSOMWARE LINKED TO MAJOR CYBERCRIME GROUPS | XORDDOS MALWARE UPGRADES FOR LARGE-SCALE LINUX ATTACKS | FOG RANSOMWARE EXPLOITS FAKE GOVERNMENT MESSAGING

Apple addresses two exploited zero-days with iOS emergency patch

Apple has issued an urgent security update to address two actively exploited zero-day vulnerabilities—CVE-2025-31200 and CVE-2025-31201—affecting CoreAudio and RPAC components. These flaws allow arbitrary code execution and bypass iOS security mechanisms, posing major surveillance and espionage risks. Discovered in collaboration with Google's TAG, the vulnerabilities are known to have been used in targeted attacks on high-risk users.

Organisations, especially those handling sensitive or government-related data, must ensure immediate iOS patch compliance, particularly for executives and employees in high-profile or high-risk roles. Mobile Device Management (MDM) platforms should enforce patch deployment and restrict access from outdated or jailbroken devices. Security teams should also monitor device telemetry for signs of compromise and consider enabling iOS lockdown mode for users at higher risk. Regular security reviews of mobile usage policies and data access permissions can minimise potential damage from mobile threats.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Apple IOS

Source - https://securityonline.info/urgent-apple-security-patch-zero-day-exploits-target-iphones/

Firefox vulnerability CVE-2025-3608 raises a significant memory corruption alert

Mozilla has patched CVE-2025-3608, a high-severity vulnerability in the Firefox browser's nsHttpTransaction component. This flaw, stemming from a race condition, could allow remote code execution through memory corruption without requiring user privileges or interaction. The vulnerability was discovered through Mozilla's fuzz testing efforts, and while no exploitation has been reported yet, the risk of future abuse remains high.

Enterprises relying on Firefox for internal or web-based systems should ensure all Firefox browsers are updated to version 137.0.2 immediately and patch compliance is validated using configuration management tools. Web content filtering and behaviour analytics can help detect malicious web payloads designed to exploit such flaws. Firefox's open-source nature makes it more transparent but also more targetable, so companies should monitor vulnerability disclosures and incorporate browser security updates into broader patch management cycles. Least privilege principles should be applied to browser-based processes to reduce attack surfaces.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Mozilla Firefox

Source - https://cybersecuritynews.com/firefox-high-severity-vulnerability/

Interlock ransomware is moving under-the-radar but evolving rapidly into a more sinister threat

The Interlock ransomware group, active since late 2024, has emerged as a stealthy and dangerous player in the cybercrime landscape. Although, its attacks have not been as prolific as other major ransomware gangs. Interlock leverages advanced techniques such as fake software updaters, PowerShell backdoors, and credential-stealing malware. Notably, it also employs social engineering tactics like "ClickFix" to lure users into executing malicious payloads. Its targets span North America and Europe, with a focus on big-game hunting and double extortion.

Organisations should remain vigilant against lesser-known but highly capable threat actors like Interlock. Endpoint protection platforms should detect behavioural anomalies associated with PowerShell misuse and credential theft. IT teams must educate employees on the risks of fake updates and social engineering schemes and adopt stringent application listing to prevent unauthorised execution. Network segmentation and robust privilege access controls can also limit lateral movement. Given Interlock’s adaptability, threat intelligence sharing and simulated ransomware drills will help prepare teams for unexpected and emerging tactics.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	North America, Europe	APPLICATION	Windows

Source - https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/

SonicWall SMA100 exploited as CISA flags CVE-2021-20035

CISA has added CVE-2021-20035 to its Known Exploited Vulnerabilities (KEV) catalogue, confirming in-the-wild exploitation of this OS command injection flaw affecting SonicWall SMA100 series appliances. Exploiting this vulnerability can lead to full system compromise, making it critical for network edge devices. SonicWall has released patches, and federal agencies are required to implement mitigations by May 7, 2025.

Enterprises using SonicWall appliances should immediately apply the latest firmware updates and ensure proper segmentation of remote access systems. If patching is delayed, temporary mitigations such as disabling affected services must be deployed. Device logs should be reviewed for signs of compromise, including suspicious administrative access or abnormal configuration changes. As edge devices are prime targets for initial access brokers and ransomware gangs, regular vulnerability scanning and strict access controls for management interfaces are crucial. Cybersecurity teams should also track CISA's KEV catalogue as part of their vulnerability prioritisation workflow.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Sonicwall SMA

Source - https://securityonline.info/cisa-alert-actively-exploited-sonicwall-sma100-vulnerability/

Akira ransomware is a persistent threat backed by notorious groups

Akira is a double-extortion ransomware operation linked to known cybercriminal groups like PUNK SPIDER and GOLD SAHARA. Since its emergence in 2023, Akira has impacted over 250 organisations across finance, healthcare, education, and manufacturing sectors in North America, Europe, and Australia. Victims face the threats of both data encryption and public exposure. Akira targets vulnerabilities in Cisco FirePOWER, ASA devices, and Windows systems, leveraging known exploits and RDP exposure.

To counter Akira, organisations must adopt a multi-layered defence strategy. Network and endpoint defences should be tuned to detect lateral movement and data exfiltration. Devices exposed to the internet—especially Cisco appliances—must be patched and monitored. Segmented backups and incident response playbooks should also be tested regularly. Additionally, MFA, secure RDP configurations, and zero-trust architecture are essential in defending against Akira's access techniques. Threat hunting should focus on early indicators such as failed login attempts, credential dumping, and unusual outbound traffic.

ATTACK TYPE	Ransomware	SECTOR	Healthcare/hospitals, Financial services, Manufacturing, Education, Business, Consultancy, Retailer and Distributor
REGION	North America, Australia, Europe, UK	APPLICATION	Cisco FirePOWER , Windows , Cisco FirePOWER Threat Protection , Cisco ASA

Source - https://darkatlas.io/blog/akira-ransomware-road-to-glory

XorDDoS malware resurfaces with “VIP” variant

XorDDoS, a Linux-based malware family active for nearly a decade, has resurfaced with new infrastructure and a “VIP” variant, signalling a more professionalised approach to distributed denial-of-service (DDoS) attacks. This malware primarily spreads via SSH brute-force attacks and establishes long-term persistence through rootkits and custom cron jobs. Cisco Talos reports that over 70% of its recent infections have targeted U.S.-based systems. The malware’s control servers and botnet infrastructure have become more centralised and resilient, suggesting renewed focus by Chinese-speaking actors.

With XorDDoS’s evolution, proactive Linux threat monitoring is more important than ever. Organisations running Linux systems must ensure SSH configurations are hardened by disabling password-based logins, enforcing key-based authentication, and limiting root access. Security teams should monitor for brute-force attempts, unusual traffic patterns, and persistence mechanisms such as modified crontabs. DDoS mitigation strategies—including rate-limiting, geo-IP blocking, and upstream filtering—are vital, especially for high-availability services. Admins should also audit servers for unauthorised services or user accounts.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Linux

Source - https://blog.talosintelligence.com/unmasking-the-new-xorddos-controller-and-infrastructure/

FOG ransomware campaign exploits government trust

FOG ransomware has returned with a campaign that abuses trust in government communications. Masquerading as content related to a U.S. government initiative (DOGE), attackers distribute ZIP and LNK files through phishing emails. Once executed, multi-stage PowerShell scripts deploy the ransomware alongside credential harvesting and sandbox evasion techniques. Over 100 organisations across IT, education, healthcare, and transportation sectors have been affected since early 2024, demonstrating the campaign's broad scope and evolving sophistication.

To defend against FOG, enterprises must implement layered phishing protection and sandboxing for email attachments. Security awareness training should emphasise the danger of ZIP/LNK files and fake government messages. Disabling macros and script execution in email-handling systems can help reduce risk. Endpoint Detection and Response (EDR) solutions should also monitor for suspicious PowerShell activity and lateral movement. Regular backups and incident playbooks that include data exfiltration scenarios are vital. As FOG evolves, threat intelligence collaboration and simulated phishing tests can help businesses remain resilient.

ATTACK TYPE	Ransomware	SECTOR	Information technology, Healthcare/hospitals, Manufacturing, Transportation, Education, Business, Retailer and Distributor
REGION	United States	APPLICATION	Windows

Source - https://www.trendmicro.com/en_us/research/25/d/fog-ransomware-concealed-within-binary-loaders-linking-themselve.html

INTRODUCTION | DARKMYSTIC RANSOMWARE EMERGES WITH A VENGEANCE | JACKALOCK RANSOMWARE THREATENS STOLEN DATA LEAK | CHROME UPDATE BLOCKS CRITICAL CODE EXECUTION FLAWS | APPLE RUSHES IOS PATCH FOR ACTIVE ZERO-DAY EXPLOITS | FIREFOX RACE CONDITION BUG FIXED IN LATEST UPDATE | INTERLOCK RANSOMWARE USES FAKE UPDATES AND PHISHING LURES | SONICWALL SMA100 VULNERABILITY ACTIVELY EXPLOITED | AKIRA RANSOMWARE LINKED TO MAJOR CYBERCRIME GROUPS | XORDDOS MALWARE UPGRADES FOR LARGE-SCALE LINUX ATTACKS | FOG RANSOMWARE EXPLOITS FAKE GOVERNMENT MESSAGING

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.

© 2025 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Private Limited.