TATA COMMUNICATIONS

TATA

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JUNE 3, 2025

TATA COMMUNICATIONS

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.

TATA COMMUNICATIONS

# More_Eggs malware targets HR Teams with malicious job files

Venom Spider's More_Eggs malware is actively targeting HR departments via fake job application emails. The latest campaign includes a zip file (“Sebastian Hall.zip”) containing a decoy image and a malicious LNK shortcut. This shortcut triggers obfuscated commands that deploy an .inf file and abuse the Windows utility ieuinit.exe to execute a JavaScript backdoor. Once installed, More_Eggs harvests system information and contacts command-and-control (C2) servers for further instructions. It employs variable fragmentation and server-side polymorphism to avoid detection, making it highly evasive.

Organisations should block LNK files from untrusted sources and monitor for suspicious use of ieuinit.exe and unexpected Word launches from the %Temp% directory. Security awareness training should emphasise caution when handling unsolicited job applications. EDR solutions must be configured to detect behavioural anomalies such as script-based process launches and C2 communication attempts. Email filters should scan attachments for uncommon file types, and network firewalls must monitor for outbound connections to known malicious IPs or domains. Given its stealth and persistence, More_Eggs represents a significant threat, particularly to businesses managing recruitment workflows.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | Information technology, Financial services, Hospitality, Retailer and Distributor, Telecommunications |
| **REGION** | All | **APPLICATION** | Atlassian Confluence, Elasticsearch, Microsoft Office 365 |

Source - https://securityonline.info/more_eggs-malware-deep-dive-abusing-ieuinit-exe-and-polymorphic-javascript/

TATA COMMUNICATIONS

# Muddled Libra: Scattered Spider affiliate shifts to social engineering & AI spoofing

Muddled Libra, a threat actor now tied to the broader Scattered Spider collective, has evolved from smishing campaigns into highly targeted attacks on IT helpdesks and enterprise personnel. Leveraging AI-based voice spoofing and insider tactics, the group impersonates executives or users to manipulate helpdesk staff into resetting credentials or granting privileged access. Muddled Libra has demonstrated a deep understanding of corporate workflows, Active Directory configurations, and multi-factor authentication (MFA) mechanisms, making its campaigns particularly effective across sectors.

Organisations must enhance helpdesk authentication protocols to require identity validation beyond voice or user claims — such as callback verification, user-specific security questions, or token-based confirmation. Cybersecurity awareness training should include exercises on social engineering threats targeting support teams. Logging of all privilege escalation requests and system changes is critical for post-incident analysis. Organisations should deploy identity threat detection and response (ITDR) tools to monitor for irregular access requests or changes in authentication flows. As AI-driven impersonation grows more convincing, layered defences and internal control validation are key to preventing social engineering-based breaches.

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

Source - https://unit42.paloaltonetworks.com/muddled-libra/

# Steganography malware hides in .NET Bitmaps to evade detection

A new wave of targeted malware campaigns is leveraging steganography within 32-bit .NET applications to bypass traditional detection methods. Attackers embed malicious payloads in bitmap image resources, allowing them to deliver multi-stage malware like Agent Tesla while avoiding scrutiny from antivirus engines. These campaigns have primarily targeted the financial and logistics sectors across Asia and Turkey. Because payloads are concealed in image files and decoded at runtime, typical static analysis and signature-based tools are often ineffective.

Organisations should deploy endpoint solutions with memory analysis and sandboxing to detect runtime behaviours, such as fileless execution or abnormal DLL loading. Developers and IT security teams should audit .NET binaries for unusual embedded resources, particularly large or non-standard bitmap files. Email and web filters must be configured to flag suspicious attachments, especially those disguised as business files with embedded images. Regular employee training on phishing risks and malicious file indicators can further reduce exposure. Forensic teams should leverage steganalysis tools to uncover hidden content and understand attack chains, especially in malware affecting critical business sectors.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | Financial services, Logistics & Shipping |
| **REGION** | Asia, Turkey | **APPLICATION** | Windows |

Source - https://securityonline.info/high-risk-flaw-in-python-web-framework-reflex-could-lead-to-account-takeover/

# Desolator ransomware delivers swift damage with 48-hour countdown

Desolator ransomware is a severe and fast-acting strain that encrypts user files, appending a. desolated extension and dropping a ransom note with a 48-hour deadline. The malware spreads via phishing emails, malicious attachments, and compromised software downloads. Once inside, Desolator alters system settings to establish persistence and deliver its payload, leaving most victims without recovery options unless offline backups are available. Its use of anonymous communication channels makes tracking and negotiation difficult.

Organisations must deploy multi-layered ransomware defences, starting with email filtering to block malicious attachments and URLs. Regular patching and application control prevent attackers from exploiting known vulnerabilities. Backups should be stored offline or in immutable storage and tested regularly. EDR platforms must monitor for signs of file encryption, privilege escalation, and system modifications. Security teams should implement isolation protocols to quickly contain infected devices and prepare playbooks for ransomware response. Since Desolator employs both speed and stealth, early detection and rapid containment are critical for minimising damage.

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

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

# Fake Kling AI sites push infostealers via Facebook ads

In a deceptive campaign exploiting the rising popularity of Kling AI, attackers created fake websites and Facebook ads to lure users into downloading malware. The executable payload masqueraded as an AI video generator but instead dropped a remote access trojan (RAT) via a stealthy loader. Once installed, the malware harvested browser credentials, crypto wallet data, and system information. Linguistic markers and tactics point to a Vietnamese threat group behind the operation.

To counter threats like this, organisations must implement web filtering to block newly registered and deceptive domains. Social media-linked domains should be scrutinised, and endpoint protections must flag unauthorised executables and abnormal data access patterns. Users should be warned against downloading software from ads or unfamiliar platforms, particularly if tied to trending technologies like AI. DNS monitoring, sandbox analysis of downloads, and traffic inspection can help identify early-stage malware delivery. This campaign underscores the importance of vigilance against social engineering tactics exploiting current tech trends.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | All |
| **REGION** | Asia | **APPLICATION** | Windows |

Source - https://securityonline.info/ai-scam-alert-fake-kling-ai-sites-deploy-infostealer-hide-executables/

TATA COMMUNICATIONS

# Chinese APT uses MarsSnake backdoor in espionage attack on Saudi organisation

A Chinese-linked APT group, dubbed UnsolicitedBooker, deployed a sophisticated backdoor named MarsSnake in a targeted phishing campaign against a Saudi-based international organisation. Disguised as flight booking confirmations, the emails contained malicious links that led to the deployment of MarsSnake — a modular backdoor used for surveillance and remote control. This campaign is part of a broader uptick in Chinese cyber-espionage activity across the Middle East, Asia, and Africa, often involving groups like DigitalRecyclers and PerplexedGoblin.

To defend against such attacks, organisations — particularly in government, healthcare, and critical infrastructure — must implement phishing-resistant authentication mechanisms, including hardware-based MFA and conditional access policies. Email gateways should be configured to inspect and detonate links and attachments in secure sandboxes. Detection teams should monitor for known MarsSnake indicators and anomalous DNS or C2 traffic. Security awareness training should include targeted spear-phishing scenarios, especially those impersonating travel or finance services. Strategic partnerships with national CERTs and sectoral ISACs will improve visibility into geopolitical threats and support coordinated defence responses.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | Information technology, Healthcare/hospitals, Legal services, Manufacturing, Government, Transportation, BFSI, Hospitality, Telecommunications |
| **REGION** | Middle East, Africa, Asia | **APPLICATION** | Generic |

Source - https://thehackernews.com/2025/05/chinese-hackers-deploy-marssnake.html

TATA COMMUNICATIONS

# Node.js Multer flaws open door to DoS and memory attacks

Recent research has revealed critical vulnerabilities in the Multer middleware for Node.js, commonly used to handle file uploads. These flaws, if exploited, could allow remote attackers to launch Denial-of-Service (DoS) or memory exhaustion attacks, potentially crashing applications and rendering services unavailable. Given the widespread use of Multer in production environments, the risk extends across thousands of applications handling user-submitted files.

Enterprises using Node.js should urgently update their Multer dependency to a secure version and review upload validation logic. Input sanitisation and file size limits must be strictly enforced to prevent oversized or malformed payloads from overwhelming memory. Application-layer firewalls should throttle upload requests and log anomalies. Developers should also implement rate limiting and buffer management, especially for APIs exposed to the public. Vulnerability scanners and dependency management tools like Snyk or npm audit can help ensure that libraries are up to date. As attackers increasingly exploit open-source ecosystems, secure development practices and regular code audits are essential to maintaining application resilience.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Vulnerability | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | Node JS |

Source - https://securityonline.info/high-dos-risk-multer-flaws-threaten-millions-of-node-js-apps/

# Medusa ransomware group continues global extortion campaign

Medusa ransomware, active since 2021, has now surpassed 430 confirmed incidents globally, affecting industries ranging from education and manufacturing to legal and BFSI. Operating as a ransomware-as-a-service (RaaS) model, Medusa uses phishing, credential theft, lateral movement, and data exfiltration to gain leverage over its victims. The group often uses built-in system tools ("living off the land") and known software vulnerabilities to maintain persistence and avoid detection.

To counter Medusa, organisations must adopt a zero-trust security model and implement network segmentation to isolate critical assets. Email gateways and endpoint protection platforms must detect phishing attempts and lateral movement. Identity protection strategies — including MFA, just-in-time access, and role-based access controls — can minimise privilege abuse. Data Loss Prevention (DLP) tools and encryption should be applied to sensitive data, both at rest and in transit. Backup systems must be immutable and regularly tested. Due to Medusa's reliance on stealth and insider techniques, continuous threat hunting and behavioural anomaly detection are vital for early identification and containment.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Ransomware | **SECTOR** | Legal services, Manufacturing, Education, BFSI |
| **REGION** | Global | **APPLICATION** | Windows |

Source - https://www.bridewell.com/insights/blogs/detail/who-are-medusa-ransomware-group

# FBI and CISA disrupt Lumma Stealer's Malware-as-a-Service network

In a coordinated global operation, the FBI and CISA helped disrupt Lumma Stealer's infrastructure, one of the most active info-stealer malware services in 2025. Lumma was sold under a Malware-as-a-Service (MaaS) model and used phishing and fake CAPTCHA pages to infect systems. It exfiltrated credentials, session cookies, and crypto wallet information using evasive encryption and injection techniques. Despite the infrastructure takedown, variants remain active in the wild.

Organisations should strengthen phishing protections and ensure anti-malware solutions are updated with the latest Lumma indicators of compromise (IOCs). Email and browser security policies should detect fake CAPTCHA or login pages, and telemetry should be monitored for data theft behaviours, particularly in browser and crypto-related directories. Employee education on credential phishing and rogue downloads is essential. Threat intelligence teams should track Lumma derivatives and prepare for re-emergence, as cybercrime MaaS services often regenerate under new branding. Participation in industry information-sharing initiatives can also enhance awareness of active campaigns.

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

Source - https://www.welivesecurity.com/en/eset-research/eset-takes-part-global-operation-disrupt-lumma-stealer/ ; https://www.trellix.com/blogs/research/a-deep-dive-into-the-latest-version-of-lumma-infostealer/

# Midnight ransomware targets global enterprises with stealth and speed

Midnight ransomware is an emerging threat targeting Windows-based systems across sectors, including healthcare, manufacturing, and finance. It encrypts files using strong algorithms and issues ransom notes through anonymous communication platforms. Midnight uses anti-debugging techniques, registry-based persistence, and PowerShell loaders to remain hidden. Like many modern ransomware strains, it also exfiltrates sensitive data to support double-extortion tactics.

Organisations must defend against Midnight by enabling PowerShell logging, disabling macros in Office documents, and applying script control policies through Group Policy or endpoint protection suites. SOC teams should monitor for signs of registry tampering, new scheduled tasks, and unusual outbound connections. Immutable backups should be isolated from the network and tested regularly. Legal, compliance, and incident response teams should coordinate ransomware playbooks that account for both operational and reputational risks. With Midnight's rapid spread and stealth-focused tactics, proactive preparation is essential for minimising impact.

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

Source - https://www.cyclonis.com/remove-midnight-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.

© 2024 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Private Limited.