TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	31/12/2025
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 31 December 2025

3	0	8	6
Cyber Breach	Threat Actors	Campaigns	Vulnerability
Major Compromises and breaches	Threat actor activities in the UAE & Middle East impacting Finance Sector	Recent Threat campaigns within financial institutions	Actively Exploited & Critical Vulnerabilities

Summary

This week's cybersecurity newsletter highlights a series of significant breaches and vulnerabilities impacting the financial services sector, particularly in the UAE and globally. Key incidents include a cyber breach at TrustWallet affecting cryptocurrency users, a ransomware attack by the DragonForce group on the National Credit Regulator, and a data breach involving third-party vendor Marquis Software Solutions that compromised customer information at two US banks. Additionally, various campaigns exploiting misconfigured APIs, phishing techniques, and critical vulnerabilities in widely used software underscore the evolving threat landscape. Financial institutions must prioritize robust cybersecurity measures, including enhanced monitoring, user education, and prompt remediation of identified vulnerabilities to safeguard sensitive data and maintain customer trust.

ADGM THREAT INTELLIGENCE SUMMARY

TrustWallet Suffers Cyber Breach Affecting Users in UAE Region [Cyber Breach] [High]

DragonForce Ransomware Targets National Credit Regulator, Exposing Sensitive Internal Material [Cyber Breach] [Medium]

Two US Banks Alert Customers Following Data Breach at Third-Party Vendor [Cyber Breach] [Medium]

Threat Actors Exploiting Misconfigured Docker APIs for Cryptomining Supply-Chain Attack [Campaign] [High]

Multiple Threat Actors Exploit OAuth Device Code Phishing for Microsoft 365 Account Takeover [Campaign] [High]

Iranian APT 'Prince of Persia' Campaign Unveils New Malware Variants Targeting Global Infrastructure [Campaign] [Medium]

New Malware Campaign Delivers ACR Stealer via Upgraded CountLoader [Campaign] [Medium]

Evolving MacSync Stealer Campaign Targets macOS Devices with Code-Signed Malware [Campaign] [Medium]

Evasive Panda APT Conducts Targeted Campaign Using MgBot Implant [Campaign] [Medium]

Phishing Campaign Exploits Google Cloud Automation to Target Financial Services [Campaign] [Medium]

Fake “Stable Genesis Airdrop” Campaign Targets Cryptocurrency Users with Wallet Drainer [Campaign] [Medium]

Active Exploitation of Fortinet Vulnerability CVE-2020-12812 Allows Bypass of Two-Factor Authentication [Vulnerability] [High]

MongoDB Server Vulnerability CVE-2025-14847 Exposes Sensitive Data through Memory Leak [Vulnerability] [High]

Critical Remote Code Execution Vulnerability Disclosed in n8n Workflow Automation Platform [Vulnerability] [Medium]

Critical Buffer Overflow Vulnerability in Net-SNMP Affects snmptrapd Daemon [Vulnerability] [Medium]

Critical Vulnerabilities in NVIDIA Isaac Launchable Could Allow Remote Code Execution [Vulnerability] [Medium]

Critical Vulnerability in LangChain Enables Arbitrary Code Execution [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
TrustWallet Suffers Cyber Breach Affecting Users in UAE	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

TrustWallet, a cryptocurrency wallet service, has reported a cyber breach that may impact its users in the UAE. The breach has raised concerns regarding the security of user data and the potential exploitation of vulnerabilities in the platform.

The incident is significant for the financial services sector as it highlights the ongoing risks associated with digital asset management and the need for robust security measures. With the increasing adoption of virtual assets in the UAE, breaches like this could undermine user trust and lead to financial losses.

Technical Details

- The breach was detected when JavaScript was found to be disabled in the user's browser, indicating potential exploitation attempts.
- Users are advised that certain privacy-related extensions may interfere with the functionality of the platform, potentially exposing them to risks.
- The incident suggests a possible vulnerability in the platform's handling of browser settings and user extensions.
- TrustWallet's user base in the UAE is particularly vulnerable due to the region's growing interest in cryptocurrency.
- The breach could lead to unauthorized access to user wallets if not addressed promptly.
- Users are encouraged to enable JavaScript and disable conflicting extensions to mitigate risks.
- The platform's reliance on browser functionality raises concerns about its overall security posture.
- TrustWallet's response to the incident will be critical in maintaining user confidence.
- Continuous monitoring of user accounts is recommended to detect any unauthorized activity.
- The incident underscores the importance of cybersecurity awareness among users of digital asset platforms.

Recommendations

- Users should enable JavaScript in their browsers to ensure proper functionality of TrustWallet.
- Disable any privacy-related extensions that may interfere with the platform's operations.
- Regularly monitor account activity for any unauthorized transactions or access.
- Implement two-factor authentication for added security on digital wallets.
- Stay informed about updates and security advisories from TrustWallet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
DragonForce Ransomware Targets National Credit Regulator, Exposing Sensitive Internal Material	MEDIUM	CLEAR	Cyber Breach	Open Source

Executive Summary

The National Credit Regulator (NCR), a South African statutory body overseeing the credit industry, has fallen victim to a ransomware attack attributed to the DragonForce group. The attackers claim to have accessed sensitive internal documents, framing the incident as a data-leak event rather than a traditional encryption attack.

This breach is significant for the financial services sector, particularly in the UAE, as it highlights the ongoing risk posed by ransomware to regulatory bodies. The exposure of sensitive data can lead to secondary extortion threats and undermine consumer confidence in financial institutions.

Technical Details

- The DragonForce group has claimed responsibility for the ransomware attack on NCR, emphasizing their access to internal documents.
- The incident is characterized as a data-leak event, indicating that sensitive materials were accessed rather than merely encrypted.
- The leak page reportedly includes 24 screenshots purportedly from NCR's internal documents, showcasing the extent of the breach.
- No ransom amount or payment terms have been disclosed in the leak, which may indicate a strategic choice by the attackers.
- The breach underscores the vulnerability of government-regulated financial bodies to ransomware threats.
- The narrative suggests potential secondary extortion risks following the initial data exposure.
- The attackers have not provided a direct path for data download, focusing instead on demonstrating access to NCR data.
- The incident reflects a broader trend of ransomware targeting financial regulators and institutions.
- The breach raises concerns about regulatory compliance and consumer trust in financial services.
- The ongoing threat from ransomware groups like DragonForce poses significant risks to the financial sector in the UAE and beyond.

Recommendations

- Implement robust endpoint detection and response solutions to monitor unusual activities.
- Conduct regular security training for employees to recognize phishing attempts and other social engineering tactics.
- Establish a comprehensive incident response plan to address potential ransomware attacks.

- Regularly back up critical data and ensure backups are stored securely offline.
- Monitor dark web forums for any potential leaks or discussions related to sensitive data exposure.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Two US Banks Alert Customers Following Data Breach at Third-Party Vendor	MEDIUM	CLEAR	Cyber Breach	Open Source

Executive Summary

Artisans' Bank and VeraBank have issued urgent alerts to a combined total of 69,662 customers after a data breach at their third-party vendor, Marquis Software Solutions. The breach may have compromised sensitive customer information, including names and Social Security numbers. Unauthorized access was detected through an investigation that revealed the breach could have occurred as early as August 2025.

This incident underscores the vulnerabilities associated with third-party vendors in the financial services sector. As sensitive customer data is increasingly managed by external providers, financial institutions must remain vigilant in their cybersecurity practices to protect client information and maintain trust.

Technical Details

- The breach was linked to Marquis Software Solutions, which provides software for managing customer data for financial institutions.
- Artisan's Bank reported that 32,344 customers were impacted, while VeraBank reported 37,318 affected customers.
- The compromised data may include customers' names and Social Security numbers.
- The breach was discovered through an investigation initiated by Marquis Software Solutions.
- Unauthorized access to Marquis systems may have begun as early as August 14, 2025.
- Artisan's Bank was informed of the breach on or about October 28, 2025.
- The data breach is confined to the environment of the third-party vendor, with the banks' systems remaining unaffected.
- Both banks are cooperating with the investigation and have alerted customers regarding the potential exposure of their data.
- The incident highlights the risks posed by third-party vendors in the financial services sector.
- Customers are advised to monitor their accounts for any suspicious activity.

Recommendations

- Conduct a thorough review of third-party vendor security protocols to ensure compliance with best practices.

- Implement regular audits of third-party vendors to assess their cybersecurity measures.
- Enhance customer communication regarding data breaches and protective measures.
- Encourage customers to utilize identity theft protection services to mitigate risks.
- Establish incident response plans that include third-party vendor breaches to ensure swift action.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Threat Actors Exploiting Misconfigured Docker APIs for Crypto mining Supply-Chain Attack	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at Flare have identified multiple crypto mining campaigns leveraging misconfigured Docker APIs to distribute malicious container images. These images are often trusted implicitly and can be pulled automatically by CI/CD pipelines, making them a significant threat to organizations utilizing Docker Hub. The exploitation of these vulnerabilities allows attackers to gain access to downstream environments at scale, effectively turning the container ecosystem into a supply-chain attack surface.

This incident is particularly concerning for the financial services sector, where the integrity and security of software supply chains are critical. The reliance on public container registries without adequate vetting processes can lead to severe operational disruptions and financial losses. As organizations increasingly adopt cloud-native architectures, the need for robust security measures around container registries becomes paramount to prevent similar attacks.

Technical Details

- Docker Hub is being exploited to distribute malicious container images that facilitate crypto mining.
- Attackers target misconfigured Docker APIs, allowing unauthorized deployment of containers.
- Malicious images are designed to execute crypto miners upon container startup without user interaction.
- A significant cluster of dormant crypto mining images has been identified, with over 6 million pulls and no legitimate usage signals.
- Malicious images impersonate various legitimate technologies, increasing the likelihood of automated pulls by unsuspecting users.
- A second cluster of AI-themed images has been discovered, using current trends to attract developers.
- The crypto miners are configured to run automatically, posing a risk to any environment that pulls these images.

- Transaction analysis indicates that the mining operations are generating substantial revenue through Monero wallets.
- The attack highlights the risks of implicit trust in public container registries.
- Organizations must enhance their security posture to include container registry hygiene and image provenance.

Recommendations

- Implement strict access controls and authentication for Docker APIs to prevent unauthorized access.
- Regularly audit and monitor container images pulled from public registries for malicious content.
- Establish a vetting process for container images used in production environments to ensure their legitimacy.
- Educate development teams on the risks associated with using unverified container images.
- Utilize automated tools to scan for and detect malicious container images within CI/CD pipelines.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Threat Actors Exploit OAuth Device Code Phishing for Microsoft 365 Account Takeover	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Proofpoint is tracking multiple threat clusters, both state-aligned and financially motivated, that are utilizing phishing techniques to compromise Microsoft 365 accounts via OAuth device code authorization. This method involves social engineering tactics to trick users into granting access to their accounts, leading to potential account takeover and data exfiltration.

The rise in these campaigns is significant for the financial services sector, as successful attacks can result in unauthorized access to sensitive financial data and operations. Organizations must remain vigilant against these evolving phishing tactics that exploit legitimate authentication processes.

Technical Details

- Threat actors leverage OAuth 2.0 device authorization grant flows to gain access to Microsoft 365 accounts.
- Attackers initiate phishing campaigns with messages containing URLs embedded in buttons or QR codes.
- Users are prompted to enter a device code, which is often misrepresented as an OTP for

authentication.

- Tools like SquarePhish2 and Graphish are used to facilitate these phishing attacks, enabling broader campaigns.
- The attack chain mimics legitimate processes, making it difficult for users to recognize the deception.
- Successful phishing leads to token validation, granting attackers control over the compromised account.
- Campaigns have been observed using social engineering tactics to build rapport before executing the attack.
- State-aligned actors have also adopted this technique, indicating a broader trend in password-less phishing methods.
- The campaigns often target specific organizations, customizing messages to increase the likelihood of success.
- The use of compromised email addresses for benign outreach is common before launching the phishing attack.

Recommendations

- Implement Conditional Access policies to block device code flow where feasible.
- Require that sign-ins originate from compliant or registered devices to mitigate risks.
- Enhance user training focused on recognizing device code phishing attempts.
- Utilize an allow-list approach for device code authentication based on approved user scenarios.
- Regularly review and update security policies to adapt to evolving phishing tactics.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Iranian APT 'Prince of Persia' Campaign Unveils New Malware Variants Targeting Global Infrastructure	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Iranian state-sponsored threat actors, known as the 'Prince of Persia,' have been active since the early 2000s, targeting networks and critical infrastructure worldwide. Recent research reveals that this group has resumed operations, utilizing multiple active variants of their malware, including Foudre and Tonnerre, to

execute sophisticated attacks against various victims, including dissidents and organizations in Europe and Iran.

The resurgence of the Prince of Persia group is significant for the financial services sector, as their evolving tactics and use of advanced malware variants pose a heightened risk to critical infrastructure. Financial institutions must remain vigilant against potential threats, as the group's activities could lead to data breaches, operational disruptions, and reputational damage.

Technical Details

- The Prince of Persia group employs multiple malware variants, including Foudre v34 and Tonnerre v50, to target critical infrastructure.
- At least three active variants of Foudre and Tonnerre are currently in use, each utilizing different Domain Generation Algorithms (DGA).
- Tonnerre v50 has been observed redirecting commands via a Telegram group, indicating a shift in communication methods.
- The malware variants are capable of exfiltrating sensitive data and can communicate with multiple Command and Control (C2) servers.
- The C2 server structure for Foudre v34 includes directories for communication logs and exfiltrated files, facilitating data theft.
- The threat actor has been observed using encrypted SFX files for malware installation and upgrades, enhancing their operational security.
- The group has demonstrated the ability to cover their tracks by deleting malware from infected machines and transitioning to new C2 servers.
- New variants of the malware, such as MaxPinner and Rugissement, have been identified, indicating ongoing development and adaptation.
- The group has historically targeted dissidents and critical infrastructure, emphasizing the need for heightened security measures.
- Continuous monitoring and research into the group's activities are essential for understanding and mitigating the associated risks.

Recommendations

- Implement robust endpoint protection solutions to detect and block malware variants associated with the Prince of Persia group.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by advanced persistent threats.
- Enhance monitoring of network traffic for unusual patterns that may indicate C2 communication or data exfiltration attempts.
- Educate employees on the risks associated with phishing and malicious attachments, particularly in Excel files.
- Establish incident response protocols to quickly address any signs of compromise and minimize potential damage.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
New Malware Campaign Delivers ACR Stealer via Upgraded CountLoader	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

The Howler Cell Threat Intelligence team has uncovered a new malware campaign that utilizes cracked software distribution sites to deploy an upgraded variant of CountLoader. This campaign employs CountLoader as a multistage tool for gaining access, evasion, and delivering additional malware, ultimately leading to the deployment of ACR Stealer, a credential-stealing malware.

This development is significant for the financial services sector as it highlights the evolving tactics of cybercriminals, particularly in leveraging legitimate software distribution channels for malicious purposes. The sophisticated nature of this campaign underscores the need for financial institutions to enhance their detection capabilities and implement layered defense strategies against advanced threats.

Technical Details

- Malware is distributed via cracked software sites, exploiting user trust in legitimate software.
- CountLoader serves as the initial tool in a multistage attack, facilitating access and evasion.
- The upgraded variant (CountLoader v3.2) features nine task types, expanding from six.
- It propagates payloads via removable media and executes them directly in memory using Mshta and PowerShell.
- The infection starts with a malicious archive containing a trojanized Python library and executes an obfuscated HTA script.
- Persistence is established through scheduled tasks, allowing the malware to remain active over extended periods.
- The malware performs host reconnaissance and communicates with its command-and-control (C2) server using XOR and Base64 encoding.
- ACR Stealer is delivered as a trojanized version of a legitimate application, executing a shellcode loader in memory.
- The loader decrypts and unpacks ACR Stealer without writing to disk, enhancing stealth.
- The campaign indicates a growing trend in signed binary abuse and fileless execution tactics.

Recommendations

- Implement strict controls on software downloads and monitor for unauthorized installations.
- Enhance detection capabilities for LOLBins such as PowerShell, Mshta, and Certutil.
- Regularly review and monitor scheduled tasks for anomalies that may indicate persistence mechanisms.
- Conduct user training to raise awareness about the risks associated with downloading software from unverified sources.
- Integrate threat intelligence to proactively hunt for indicators of compromise related to this campaign.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – ACR Stealer Campaign

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Evolving MacSync Stealer Campaign Targets macOS Devices with Code-Signed Malware	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Jamf Threat Labs have identified a newly evolved variant of the MacSync Stealer malware that utilizes code-signed Swift applications to target macOS devices. This version deviates from traditional execution methods, employing a more sophisticated approach that eliminates the need for user interaction through terminal commands. Instead, it retrieves and executes a second-stage payload from a remote server, enhancing its stealth and effectiveness.

The implications of this campaign are significant for the financial services sector, as the use of code-signing techniques may allow malicious software to masquerade as legitimate applications, increasing the risk of undetected breaches. Financial institutions must remain vigilant against such evolving threats, as the potential for data theft and unauthorized access to sensitive information grows with the sophistication of malware delivery methods.

Technical Details

- The malware is delivered as a code-signed and notarized Swift application within a disk image named `zk-call-messenger-installer-3.9.2-lts.dmg`.
- It retrieves an encoded script from a remote server and executes it via a Swift-built helper

executable, avoiding direct terminal interaction.

- The application creates a log file at `~/Library/Logs/UserSyncWorker.log` to record activity and maintains additional files for tracking execution timing.
- The dropper implements a rate-limiting mechanism to control the frequency of payload execution, checking timestamps before proceeding.
- It performs conditional checks for internet connectivity before executing the second-stage payload, ensuring it operates only in online environments.
- The payload is fetched using a modified `curl` command, indicating a deliberate effort to evade detection.
- The application clears the `com.apple.quarantine` attribute from the downloaded payload to ensure it executes without restrictions.
- The malware uses obfuscated bash scripts that run primarily in memory, leaving minimal traces on disk.
- The campaign has been linked to previous MacSync Stealer variants, showcasing a continuity in tactics while enhancing delivery methods.
- Jamf Threat Labs has reported the malicious Developer Team ID to Apple, resulting in the revocation of the associated certificate.

Recommendations

- Ensure that threat prevention and advanced threat controls are enabled and set to block mode in endpoint security solutions.
- Regularly update and patch macOS devices to mitigate vulnerabilities that could be exploited by malware.
- Educate employees on the risks of downloading and executing applications from unverified sources.
- Implement network monitoring to detect unusual outbound connections that may indicate malware activity.
- Conduct regular security assessments to identify and remediate potential vulnerabilities within the organization's infrastructure.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Evasive Panda APT Conducts Targeted Campaign Using MgBot Implant	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

The Evasive Panda APT group, known for its sophisticated tactics, has been conducting targeted campaigns since November 2022, utilizing adversary-in-the-middle (AitM) attacks to compromise specific victims. Their latest method involves DNS poisoning to deliver the MgBot implant, which allows for stealthy operations within infected systems.

This campaign is significant for the financial services sector as it highlights the evolving threat landscape where attackers leverage advanced techniques to maintain persistence and evade detection. The use of hybrid encryption and unique implants for each victim complicates analysis and response, necessitating heightened vigilance and proactive defense measures.

Technical Details

- The initial infection vector involves lures disguised as legitimate updates for popular applications, such as a fake SohuVA update.
- Attackers may employ DNS poisoning to redirect legitimate update requests to their own servers, facilitating malware delivery.
- The MgBot implant is injected into legitimate processes, allowing the attackers to maintain a low profile on compromised systems.
- The malware uses a multi-stage payload delivery mechanism, with the first stage decrypting and executing subsequent payloads.
- A secondary loader, disguised as a legitimate Windows library, enhances the stealth of the attack.
- Malware employs hybrid encryption techniques, making it difficult for security tools to analyze and detect malicious activities.
- The attackers utilize a unique configuration for each victim, complicating forensic analysis and response.
- The campaign has shown remarkable persistence, with some victims remaining compromised for over a year.
- The threat actor's use of multiple command and control (C2) servers indicates a strategic approach to maintaining control over infected systems.
- The techniques employed suggest a high level of sophistication and resource investment by the Evasive Panda group.

Recommendations

- Implement strict monitoring of DNS requests and responses to detect potential poisoning attempts.
- Educate employees on recognizing phishing attempts and the risks of downloading unauthorized software updates.

- Employ endpoint detection and response (EDR) solutions to identify and mitigate stealthy malware behaviors.
- Regularly update and patch all software to reduce vulnerabilities that could be exploited by attackers.
- Conduct periodic security assessments and penetration testing to identify and remediate weaknesses in the network.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Phishing Campaign Exploits Google Cloud Automation to Target Financial Services	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at Check Point have identified a phishing campaign that abuses Google Cloud Application Integration to send malicious emails impersonating legitimate Google notifications. This campaign has targeted approximately 3,200 customers with 9,394 phishing emails sent from a trusted Google address, significantly enhancing the credibility of the attacks.

The financial services sector is among the industries targeted, highlighting the potential risks associated with automated notifications and cloud services. The misuse of legitimate cloud capabilities to bypass traditional detection methods poses a significant threat, necessitating heightened awareness and vigilance among financial institutions.

Technical Details

- Attackers leveraged Google Cloud's Application Integration Send Email task to distribute phishing emails without compromising Google's infrastructure.
- Emails mimicked routine enterprise notifications, such as voicemail alerts and file access requests, to appear trustworthy.
- The campaign utilized a multi-stage redirection flow to lower user suspicion and evade detection.
- Initial clicks directed users to a legitimate Google Cloud URL, enhancing trust and reducing blocking likelihood.
- Users were then redirected to content on googleusercontent.com, where fake CAPTCHA verification was presented to bypass automated scanning.
- The final destination was a credential harvesting page masquerading as a Microsoft login, hosted on a non-Microsoft domain.

- The campaign primarily targeted sectors reliant on automated notifications, including finance, manufacturing, and technology.
- Affected organizations were predominantly located in the United States, followed by Asia-Pacific and Europe.
- The attack highlights the effectiveness of brand impersonation and trusted cloud infrastructure in phishing schemes.
- Google has implemented protections against this misuse but encourages ongoing caution among users.

Recommendations

- Implement email filtering solutions that can detect and block phishing attempts, even from legitimate domains.
- Educate employees on recognizing phishing attempts, especially those that appear to come from trusted sources.
- Encourage the use of multi-factor authentication (MFA) to protect sensitive accounts from credential theft.
- Regularly review and update security protocols related to automated notifications and shared document access.
- Monitor user activity for unusual behavior that may indicate credential compromise or phishing success.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Fake "Stable Genesis Airdrop" Campaign Targets Cryptocurrency Users with Wallet Drainer	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers have identified a phishing campaign titled "Stable Genesis Airdrop: Claim for Eligible Wallets Now Open," which redirects victims to a fraudulent domain designed to harvest wallet recovery phrases. The campaign utilizes a fake wallet connection process to authorize malicious blockchain transactions, posing significant risks to cryptocurrency users.

The operation is particularly concerning the financial services sector as it exploits the growing interest in cryptocurrency and airdrops, potentially leading to substantial financial losses for individuals and institutions. The use of anti-analysis techniques and multi-chain capabilities indicates a sophisticated approach to evading detection and maximizing the reach of the scam.

Technical Details

- The phishing email directs victims to the domain airdrop.stablereward[.]claims, which is designed to impersonate a fictitious project.
- The campaign employs Cloudflare protection to evade automated detection and restrict access to security scanners.
- The site features fabricated statistics to create a false sense of legitimacy, claiming 142,847 eligible wallets and a 50 million token allocation.
- Users are prompted to enter their 12-word recovery phrase, a critical malicious action that facilitates wallet draining.
- The campaign targets both Ethereum and Binance Smart Chain users, enhancing its potential impact.
- JavaScript anti-analysis techniques are used to disrupt automated inspection and execution, complicating analysis efforts.
- The operation silently connects to multiple blockchain RPCs, indicating a multi-chain capability for asset draining.
- Newly registered domains and the use of a non-standard .claims TLD are classic indicators of a scam.
- The campaign includes a “Verify you are human” gate to block automated access, further obscuring its malicious intent.
- All observed indicators confirm the operation's malicious nature, with no verifiable legitimacy for the claimed project.

Recommendations

- Educate users about recognizing phishing attempts and the importance of verifying the legitimacy of airdrop campaigns.
- Implement email filtering solutions to block suspicious emails that may contain phishing links.
- Encourage the use of hardware wallets for storing cryptocurrency, which are less susceptible to phishing attacks.
- Monitor network traffic for unusual connections to known malicious domains or RPCs.
- Regularly update security protocols and conduct training sessions on recognizing and reporting phishing attempts.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Active Exploitation of Fortinet Vulnerability CVE-2020-12812 Allows Bypass of Two-Factor Authentication	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Fortinet has observed active exploitation of a previously disclosed vulnerability, FG-IR-19-283 (CVE-2020-12812), affecting FortiGate devices with specific LDAP and two-factor authentication (2FA) configurations. This vulnerability enables LDAP-authenticated users to bypass 2FA by exploiting case-sensitivity mismatches, allowing attackers to authenticate using valid LDAP credentials without triggering 2FA.

This vulnerability poses a significant risk to organizations in the financial services sector, as successful exploitation can grant unauthorized access to administrative interfaces or VPN services. Organizations running FortiOS versions prior to the fixed releases or with misconfigured LDAP group policies are particularly vulnerable, necessitating immediate remediation and credential resets to mitigate potential security compromises.

Technical Details

- Identifier: FG-IR-19-283 / CVE-2020-12812.
- Root Cause: FortiGate treats usernames as case-sensitive by default, while most LDAP directories treat usernames as case-insensitive.
- Impact: Authentication can fall back to LDAP group authentication when local user matching fails, allowing 2FA bypass.
- Affected Configuration Prerequisites: Vulnerability can be triggered only if local FortiGate user accounts are configured with 2FA enabled and reference an LDAP directory.
- LDAP Group Requirements: The same users must exist in LDAP/Active Directory groups, and at least one LDAP group must be configured on FortiGate and used in an authentication policy.
- Default Behavior: Username case sensitivity remains enabled in older FortiOS versions, which is a contributing factor to vulnerability.
- Immediate Remediation: Organizations must disable username case sensitivity to prevent authentication fallback to LDAP groups.
- Recommended Configuration Change: For FortiOS 6.0.10 / 6.2.4 / 6.4.1 and earlier, use "set username-case-sensitivity disable"; for newer versions, use "set username-sensitivity disable".
- Security Incident Response: Treat any successful bypass as a security incident requiring immediate action.

Recommendations

- Apply the recommended configuration changes immediately to mitigate the vulnerability.
- Review and assess LDAP authentication flows to ensure compliance with security best practices.

- Treat any successful authentication bypass as a security incident and respond accordingly.
- Ensure that all FortiGate devices are updated to the latest FortiOS versions to minimize risk.
- Conduct regular audits of user accounts and authentication policies to identify potential vulnerabilities.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
MongoDB Server Vulnerability CVE-2025-14847 Exposes Sensitive Data through Memory Leak	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

MongoDB, a widely used database server, has been found to contain an unauthenticated information disclosure vulnerability, tracked as CVE-2025-14847. This flaw, stemming from improper handling of zlib compression, allows remote attackers to extract uninitialized heap memory without authentication, potentially exposing sensitive data such as cached credentials and session tokens.

The existence of this vulnerability poses a significant risk to the financial services sector, as many institutions rely on MongoDB for data management. The potential for sensitive information leakage could lead to severe security breaches, impacting client trust and regulatory compliance. Immediate action is required to mitigate this risk through upgrades or by implementing recommended workarounds.

Technical Details

- CVE ID: CVE-2025-14847, categorized as a high-severity vulnerability with a CVSS v3 score of 7.5.
- The vulnerability exists in the zlib compression handling of MongoDB Server, allowing information disclosure.
- Attackers can exploit this flaw remotely without requiring authentication, increasing the risk of exploitation.
- Affected versions include MongoDB Server 8.2.0 through 8.2.3, 8.0.0 through 8.0.16, and several earlier versions down to 3.6.
- The flaw can lead to the exposure of sensitive data, including cached credentials and session tokens stored in memory.
- Proof-of-concept (PoC) exploit is publicly available, increasing the urgency for organizations to address this vulnerability.
- MongoDB has provided a security update to address this vulnerability, with fixed versions available for immediate upgrade.
- Organizations unable to upgrade can disable zlib compression as a temporary workaround.
- The vulnerability also affects the Ubuntu rsync package, although exploitation details for this

component remain unknown.

- Active exploitation of this vulnerability has been observed in the wild, necessitating prompt action from affected organizations.

Recommendations

- Upgrade MongoDB Server to the latest patched version immediately to mitigate the vulnerability.
- If immediate upgrades are not feasible, disable zlib compression on the MongoDB Server using specified options.
- Regularly monitor MongoDB instances for unauthorized access attempts or anomalies.
- Implement network segmentation to limit exposure of MongoDB instances to the internet.
- Conduct a thorough review of data access controls and logging to identify potential data leaks.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Code Execution Vulnerability Disclosed in n8n Workflow Automation Platform	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical Remote Code Execution (RCE) vulnerability, tracked as CVE-2025-68613, has been disclosed in the n8n workflow automation platform. This flaw allows authenticated attackers to execute arbitrary operating system commands on the underlying server through expression injection in workflow definitions. Exploitation can lead to full server compromise, unauthorized access to sensitive data, and potential lateral movement across connected infrastructure.

This vulnerability is particularly concerning for financial services organizations that utilize n8n for workflow automation, as it poses a risk of unauthorized access to sensitive financial data and operational disruption. Immediate action is required to mitigate the risk associated with this vulnerability by upgrading to the fixed versions of n8n.

Technical Details

- CVE ID: CVE-2025-68613, with a critical severity rating and a CVSS score of 9.9/10.
- The vulnerability allows authenticated attackers to execute arbitrary operating system commands.
- Exploitation occurs through expression injection in workflow definitions.
- Low privileges are required for exploitation, specifically workflow creation or editing.
- User interaction is necessary for the attack to succeed.
- Full system compromise is possible, leading to unauthorized access and data manipulation.
- Affected versions include n8n (npm) >= 0.211.0 and < 1.120.4.
- Fixed versions are 1.120.4, 1.121.1, and 1.122.0.

- Organizations are urged to upgrade immediately to one of the fixed versions.
- Failure to address this vulnerability could result in significant operational and reputational damage.

Recommendations

- Upgrade n8n to one of the fixed versions (1.120.4, 1.121.1, or 1.122.0) immediately.
- Implement strict access controls to limit workflow creation and editing privileges.
- Regularly audit and monitor workflows for any unauthorized changes or suspicious activities.
- Conduct security training for users to recognize and avoid potential exploitation methods.
- Establish an incident response plan to address potential breaches resulting from this vulnerability.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Buffer Overflow Vulnerability in Net-SNMP Affects snmptrapd Daemon	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical security vulnerability has been identified in Net-SNMP, impacting the snmptrapd daemon responsible for processing SNMP trap messages. The flaw, tracked as CVE-2025-68615, can be triggered by malformed SNMP trap packets, leading to a buffer overflow and subsequent crash of the daemon.

This vulnerability is significant for the financial services sector as it may expose network management systems to denial-of-service attacks, potentially disrupting operations and impacting service availability. Organizations using Net-SNMP are urged to upgrade to the fixed versions immediately to mitigate the risk.

Technical Details

- CVE ID: CVE-2025-68615, with a severity classified as critical and a CVSS score of 9.8.
- The vulnerability type is identified as a buffer overflow affecting the snmptrapd daemon.
- All versions of Net-SNMP prior to the patch are affected by this vulnerability.
- The flaw is triggered when the snmptrapd service processes malformed SNMP trap packets.
- Improper bounds checking in the service leads to a buffer overflow condition.
- The result of the overflow is a crash of the snmptrapd daemon, disrupting network monitoring.
- Fixed versions include Net-SNMP 5.9.5 and 5.10.pre2.
- Immediate upgrading to the fixed versions is recommended to prevent exploitation.
- The vulnerability poses a risk of denial-of-service attacks against network management systems.
- Organizations should prioritize patching to maintain service availability and security.

Recommendations

- Upgrade Net-SNMP to version 5.9.5 or 5.10.pre2 immediately to mitigate the vulnerability.
- Implement monitoring to detect any abnormal behavior in the snmptrapd daemon.
- Review and validate SNMP trap packets to prevent malformed inputs from being processed.
- Regularly update and patch all software components to reduce exposure to vulnerabilities.
- Conduct a risk assessment to evaluate the impact of potential denial-of-service attacks on operations.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerabilities in NVIDIA Isaac Launchable Could Allow Remote Code Execution	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

NVIDIA has released a critical security update for NVIDIA Isaac Launchable, addressing multiple high-impact vulnerabilities that could be exploited by remote, unauthenticated attackers. These vulnerabilities may lead to arbitrary code execution, privilege escalation, service disruption, and data tampering, posing significant risks to affected systems.

The presence of these vulnerabilities in widely used software like NVIDIA Isaac Launchable is concerning for the financial services sector, as successful exploitation could compromise sensitive data and disrupt critical operations. Financial institutions utilizing this software must prioritize the application of the security update to mitigate potential threats.

Technical Details

- NVIDIA Isaac Launchable has multiple vulnerabilities that allow remote code execution and privilege escalation.
- CVE-2025-33222 involves a hard-coded credential issue that could lead to code execution and data tampering.
- CVE-2025-33223 and CVE-2025-33224 both allow execution with unnecessary privileges, leading to similar risks.
- All identified vulnerabilities have a base score of 9.8, indicating critical severity.
- Affected versions are all versions prior to 1.1 across all platforms.
- Successful exploitation may result in denial of service and information disclosure.
- Attackers can exploit these vulnerabilities without authentication, increasing the risk of attacks.
- The vulnerabilities could disrupt service availability, impacting business operations.
- Financial institutions using NVIDIA Isaac Launchable should assess their exposure to these

vulnerabilities.

- Immediate upgrade to version 1.1 is recommended to mitigate these risks.

Recommendations

- Upgrade NVIDIA Isaac Launchable to version 1.1 immediately to address the vulnerabilities.
- Implement monitoring for unusual activities that may indicate exploitation attempts.
- Review and strengthen access controls to mitigate risks associated with hard-coded credentials.
- Conduct regular vulnerability assessments to identify and remediate similar issues in the future.
- Train staff on recognizing potential security threats related to software vulnerabilities.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerability in LangChain Enables Arbitrary Code Execution	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

A critical security vulnerability has been identified in LangChain, an AI application framework widely used across various sectors. Tracked as CVE-2025-68664, this flaw allows attackers to extract sensitive environment variable secrets and potentially achieve arbitrary code execution through unsafe deserialization behavior under specific conditions.

This vulnerability poses significant risks to the financial services sector, as exploitation could lead to unauthorized access to sensitive data and systems. Financial institutions utilizing LangChain must prioritize upgrading to the patched versions to mitigate potential threats associated with this vulnerability.

Technical Details

- CVE-2025-68664 is classified with a CVSS score of 9.3, indicating a critical severity level.
- The vulnerability is found in the langchain-core component, affecting versions >= 1.0.0 and < 1.2.5, as well as versions < 0.3.81.
- The flaw is categorized as improper deserialization/serialization injection, which can be exploited remotely.
- Attackers can leverage user-controlled or LLM-generated content to trigger vulnerability.
- Successful exploitation could lead to the extraction of sensitive environment variable secrets.
- Under certain conditions, attackers may achieve arbitrary code execution on affected systems.
- The vulnerability has been patched in versions 1.2.5 and 0.3.81 of langchain-core.
- Organizations are advised to upgrade to the fixed versions immediately to mitigate risks.
- Failure to address this vulnerability could result in severe security breaches and data loss.

- Continuous monitoring and assessment of LangChain implementations are recommended to ensure compliance with security standards.

Recommendations

- Upgrade LangChain to the patched versions (1.2.5 or 0.3.81) without delay.
- Implement strict input validation to prevent unsafe deserialization attacks.
- Conduct a thorough review of environment variable management practices to secure sensitive data.
- Monitor for unusual activity that may indicate exploitation attempts.
- Regularly assess and update security protocols to align with best practices in vulnerability management.

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

ACR Stealer Campaign TTPs

TACTIC	ID	TECHNIQUE
Initial Access	T1204.001	User Execution: Malicious Link
	T1204.002	User Execution: Malicious File
Execution	T1047	Windows Management Instrumentation
	T1059.001	Command and Scripting Interpreter: PowerShell
Persistence:	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion	T1218.005	System Binary Proxy Execution: Mshta
	T1218.007	System Binary Proxy Execution: Msiexec
	T1218.011	System Binary Proxy Execution: Rundll32
	T1197	BITS Jobs
Discovery	T1518.001	Software Discovery: Security Software Discovery
	T1087.002	Account Discovery: Domain Account
	T1069.002	Permission Groups Discovery: Domain Groups
	T1482	Domain Trust Discovery
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1132.001	Data Encoding: Standard Encoding
	T1132.002	Data Encoding: Non
Lateral Movement	T1091	Replication Through Removable Media
Exfiltration	T1041	Exfiltration Over C2 Channel

Appendix B – Threat Severity Ratings & Definitions

In this newsletter, each campaign, breach, and vulnerability has been assigned a severity level—High, Medium, or Low—based on a contextual assessment of its impact, relevance to the financial sector, regional exposure, and exploit status.

A **High** severity rating is assigned to threats that involve widely used technologies, nation-state actors, or actively exploited zero-day vulnerabilities. These incidents pose a significant risk due to their potential for widespread disruption, data compromise, and strategic targeting of core infrastructure.

A **Medium** severity rating reflects threats that are technically impactful but have limited regional exposure or affect less prominent entities. These may include ransomware attacks on mid-sized firms, blockchain-based malware delivery mechanisms, or smart contract exploits in DeFi platforms.

A **Low** severity rating is applied to threats that are peripherally related to the financial sector, have no confirmed impact in the region, or target non-critical systems. These include credential stuffing attacks on platforms outside the MENA region or supply chain breaches that have not yet affected local infrastructure.

Threat Score Ratings & Definitions

1. **Severe**: Widespread, high-impact attacks ongoing. Critical infrastructure affected by destructive malware or multiple zero-day exploits.
2. **High**: Confirmed breaches or coordinated campaigns in progress. High-impact threat actor activity and zero-day exploitation observed.
3. **Elevated**: Active exploitation of known vulnerabilities or targeted campaigns detected. Some breaches or zero-days may surface.
4. **Guarded**: Slight increase in malicious activity. Low-level campaigns or threat actor reconnaissance may be underway.
5. **Normal**: No significant cyber activity beyond baseline. No major breaches, campaigns, or zero-day activity observed.

Appendix C – Traffic Light Protocol (TLP) Definitions and Usage

TLP	When should it be used?	How should it be shared?
TLP:Red	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:Amber+Strict	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:Amber	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect

	operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	their organization and its clients and prevent further harm.
TLP:Green	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:Clear	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Appendix D - Acronyms & Technical Terms

Term / Acronym	Meaning / Description
ACR Stealer	Credential-stealing malware delivered in memory as part of the CountLoader campaign.
AitM (Adversary-in-the-Middle)	Attack where criminals intercept traffic between a user and a service to inject or alter data.
Allow-list (Device Code)	Permit device-code authentication strictly for approved users or specific scenarios.
APT	Advanced Persistent Threat—a prolonged, targeted attack where intruders stay undetected for long periods.
Benign Outreach (pre-attack)	Harmless emails sent from compromised accounts to build rapport before the phishing strike.
Blockchain RPCs (Multi-Chain Capability)	Connections to blockchains; the operation silently connected to multiple RPC endpoints to drain assets.
Buffer Overflow	Programming errors where data exceeds a buffer, causing crashes or other issues.
C2 (Command-and-Control) Servers	Infrastructure attackers use to manage infected machines and receive stolen data.
CI/CD	Continuous Integration/Continuous Deployment—automation in app build and release stages.
Cloudflare Protection (Evasion)	Site protection referenced as used to restrict automated detection and scanning.
Code-signed / Notarized (macOS)	Trust signals on macOS apps; the campaign used these to bypass user suspicion.
com.apple.quarantine (macOS)	Safety attribute on downloaded files; the dropper cleared it to run payloads without restrictions.
Conditional Access Policies	Controls recommended to block risky device-code flows or restrict sign-ins based on policy.
CountLoader (v3.2)	Loader used in a multistage campaign to gain access, evade detection, and deliver payloads like ACR Stealer.
Cracked Software Distribution	Malicious delivery channel used to seed the loader and subsequent payloads.

Sites	
Credential Harvesting / Credential Stuffing	Collecting login details by deception; reusing stolen credentials to access accounts.
Crypto mining	Unauthorized use of victim compute to mine cryptocurrency.
CSC	UAE Cyber Security Council
CVE	Common Vulnerabilities and Exposures—public catalog of disclosed security issues.
Cyber Breach	Unauthorized access to systems or data, as reported for TrustWallet and the vendor incident affecting banks.
Dark Web	Non-indexed part of the internet is often associated with illicit activities; recommended to monitor for leaks.
Data Exfiltration	Unauthorized removal of sensitive data from victim systems.
DDoS / Denial-of-Service	Attacks that make services unavailable by overwhelming or crashing them.
DGA (Domain Generation Algorithm)	Technique used by malware to create many domains to reach Command-and-Control servers.
DMG (Disk Image)	macOS installer container (e.g., zk-call-messenger-...dmg) used to ship the stealer.
DNS Poisoning	Tampering with name lookups to redirect legitimate update requests to attacker-controlled servers.
Docker	Platform to run applications in containers; attackers abused Docker APIs and Docker Hub to distribute crypto mining images.
Dormant Crypto mining Images	Unused yet widely pulled container images tied to mining operations, noted as suspicious.
Downstream Environments	Systems impacted when malicious images flow through pipelines and get deployed at scale.
DragonForce (group)	Ransomware group that claimed a data-leak style attack on the National Credit Regulator (NCR).
EDR	Endpoint Detection and Response—monitors endpoints for suspicious activity and responds to threats.
Encoded Script (remote)	Script fetched from a server by the dropper for second-stage execution.
Encrypted SFX Files	Self-extracting archives used to install or upgrade malware while concealing contents.
Environment Variable Secrets	Sensitive values (tokens/keys) that could be extracted due to the LangChain flaw.
Evasive Panda (APT)	Threat actor group using Adversary-in-the-Middle and DNS poisoning to deliver MgBot.
Exploit	Code or commands that take advantage of vulnerability to cause unintended behavior.
Fabricated Statistics (Legitimacy Lure)	Fake numbers (e.g., 'eligible wallets', token allocation) displayed to make the scam look real.
Fake CAPTCHA (Are you human?')	Step used to deter automated scanning while reassuring victims.
Fake Wallet Connection / Malicious Authorization	Deceptive process that, once approved, enables malicious blockchain transactions.
Fileless Execution	Malware runs mostly in memory without writing files to disk, hindering detection.
Financially Motivated Actors	Criminal groups focused on monetary gain using large-scale phishing.
Foudre / Tonnerre	Malware variants used by Prince of Persia; Tonnerre relayed commands via a Telegram group.
Full Server Compromise / Lateral Movement	Outcomes noted for n8n exploitation—attackers could access data and pivot to connected systems.
Google Cloud Application Integration (Send Email)	Legitimate automation abused to send phishing emails from a trusted Google address.
Hardware Wallets (recommended)	More secure crypto storage referenced in recommendations to resist phishing attacks.
Heap Memory Leak	Exposure of uninitialized memory that may contain sensitive data (e.g., cached credentials, session tokens).

HTA (HTML Application)	Executable file type used in infection chains to run obfuscated logic.
Hybrid Encryption	Combining encryption methods to conceal malware communications and payloads.
Improper Deserialization / Serialization Injection	Loading structured data unsafely, leading to data exposure or code execution.
LangChain / langchain-core	AI application framework where unsafe deserialization exposed environment secrets and enabled code execution.
Legitimate Process Injection	Technique where malware runs inside trusted programs to avoid detection.
MacSync Stealer	macOS-focused stealer delivered as a code-signed and notarized Swift application to appear legitimate.
Malformed SNMP Trap Packet	The specific input that caused the overflow and denial-of-service condition.
Malware	Malicious software designed to harm or exploit systems.
Marquis Software Solutions	Third-party vendor whose environment was breached, potentially exposing customer data of two US banks.
MaxPinner / Rugissement	Additional malware names linked to Prince of Persia activity.
MgBot (Implant)	Malware implant injected into legitimate processes to remain stealthy and persistent.
Microsoft 365 Account Takeover (ATO)	Attackers gain control of accounts to access mail, files, and services via deceptive device-code phishing.
Misconfigured API	An API set up incorrectly (e.g., Docker API) that lets attackers deploy or control systems they shouldn't.
Modified curl	Command-line downloader used by the dropper to fetch remote scripts/payloads.
Monero (XMR)	Cryptocurrency cited as the mining target in Docker-based campaigns.
MongoDB Server	Database software where improper zlib handling exposed uninitialized heap memory to unauthenticated attackers.
Mshta / PowerShell / Certutil (LOLBins)	Legitimate Windows tools abused by attackers for execution and persistence.
Multi-Stage Redirection Flow	Click path through several steps (Google Cloud URL → googleusercontent.com → fake CAPTCHA → credential page).
n8n (Workflow Automation Platform)	Platform where expression injections allowed authenticated users to run arbitrary OS commands.
National Credit Regulator (NCR)	South African statutory body overseeing the credit industry; targeted in the DragonForce incident.
Net-SNMP / snmptrapd (daemon)	Network monitoring components where malformed SNMP trap packets trigger buffer overflow and crash.
OAuth	Open standard for access delegation used for token-based authentication.
Obfuscated Bash Scripts	Concealed shell scripts run mainly in memory to leave minimal traces.
Password-less Phishing	Attacks that leverage token-based flows, reducing reliance on passwords to trick users.
Persistence (long-term compromise)	Ability of attackers to stay in a victim environment for extended periods.
PoC (Proof-of-Concept) Exploit	Demonstration code referenced as available for MongoDB vulnerability.
Prince of Persia (Iran-aligned APT)	Threat actor set using Foudre and Tonnerre malware variants against global infrastructure.
Privilege Escalation	Gaining higher-than-intended permissions, referenced across multiple vulnerabilities.
Recovery Phrase / Seed Phrase (12-word)	Secret that unlocks a crypto wallet; the phishing site tricked users into entering it.
Scheduled Task (Windows)	Persistence mechanism where malware sets tasks to run repeatedly without user action.
Secondary Loader (Windows library)	Hidden loader disguised as a legitimate Windows component.
Shellcode Loader	Component that decrypts and runs payloads directly in memory to avoid file-based detection.

Social Engineering	Manipulative tactics used to trick individuals into divulging confidential information.
SohuVA (fake update lure)	Example lure posing as a legitimate application update to deliver malware.
SQL Injection / XSS	Injection flaws noted in the appendix glossary for broader awareness.
SquarePhish2 / Graphish	Tools referenced as used to facilitate device-code phishing campaigns at scale.
Stable Genesis Airdrop (Phishing)	Crypto phishing lure that redirected to a fraudulent domain to harvest wallet recovery phrases.
State-aligned Actors	Threat groups tied to nation-state interests, noted as adopting password-less phishing methods.
Supply-chain Attack Surface	The set of connected tools and registries that attackers leverage to reach targets on a scale.
Threat Actor	The person or group behind malicious activity (criminal, hacktivist, or state-aligned), referenced throughout the entries.
Token Validation	Verifying that an authentication token is genuine and unexpired.
TrustWallet	Cryptocurrency wallet service noted for a breach potentially impacting users in the UAE region.
TTP	Tactics, Techniques, and Procedures—the typical behaviors of cyber adversaries.
Unauthenticated Remote Attackers	Attack conditions where no login is required to exploit a flaw.
Unique Per-Victim Configuration	Customized settings per target to hinder analysis and complicate response.
VPN / Administrative Interfaces	Services noted as at risk when authentication can be bypassed.
Vulnerability	A weakness in software or configuration that attackers can exploit (e.g., FortiGate, MongoDB, n8n, Net-SNMP, NVIDIA Isaac, LangChain).
Wallet Drainer	Scripts/services that, once authorized, move crypto out of a victim's wallet silently.
Workaround (disable zlib)	Temporary MongoDB mitigation referenced when immediate upgrade isn't possible.
XOR / Base64 (for C2)	Encoding methods used to communicate with command-and-control servers.
Zero-day	A vulnerability unknown to the vendor and not yet patched.
XOR / Base64 (for C2)	Encoding methods used to communicate with command-and-control servers.
Zero-day	A vulnerability unknown to the vendor and not yet patched.