TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	2/4/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 2 April 2026

11	6	0	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Finance Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a series of sophisticated phishing campaigns and critical vulnerabilities. Notable threats include a phishing campaign exploiting Microsoft's Device Code OAuth flow, which captures OAuth tokens to gain unauthorized access to accounts, and a campaign using Windows Toast Notifications to harvest credentials. Additionally, researchers have identified critical vulnerabilities in platforms such as n8n and Langflow, allowing for remote code execution, which could lead to significant data breaches and operational disruptions. These threats are particularly relevant to financial institutions, as they highlight the ongoing risk of credential theft, unauthorized access, and potential supply chain compromises. The exploitation of vulnerabilities in widely used software and platforms underscores the urgency for financial organizations to prioritize patching and monitoring efforts. As these campaigns evolve, financial institutions should remain vigilant against similar tactics and ensure robust security measures are in place to protect sensitive data and maintain operational integrity in the coming week.

ADGM THREAT INTELLIGENCE SUMMARY

Abuse of Microsoft Device Code OAuth Flow in Sophisticated Phishing Campaign [Campaign] [High]

Threat Actors Exploit Windows Toast Notifications for Credential Harvesting [Campaign] [High]

macOS ClickFix Campaign Using Fake "Claude Code Docs" to Deliver AMOS Stealer [Campaign] [High]

High-Severity WebLogic Vulnerabilities Observed on a High-Interaction Oracle Honeypot [Campaign] [High]

DPRK-Linked Nickel Alley exploits fake jobs and developer toolchains to deliver PyLangGhost [Campaign] [High]

Kinsing Campaign Exploits Multiple CVEs Using Shared Infrastructure [Campaign] [High]

China-Nexus Red Menshen Deploys BPFdoor Backdoors [Campaign] [Medium]

TeamPCP Threat Actor Compromises LiteLLM as Part of a Supply Chain Campaign [Campaign] [Medium]

Multi-Vector Malware Campaign Exploits VBS and Open Infrastructure [Campaign] [Medium]

Kamasers Botnet Launches Multi-Vector DDoS Attacks Targeting Organizations Worldwide [Campaign] [Medium]

Critical Supply Chain Compromise in Aqua Security Trivy Ecosystem [Campaign] [Medium]

Critical RCE Vulnerabilities in n8n Workflow Automation Platform [Vulnerability] [High]

Citrix Addresses Critical and High Severity Flaws in Multiple Products – Active Reconnaissance Observed [Vulnerability] [High]

Critical Remote Code Execution Vulnerability in Langflow Exposes Systems to Attacks [Vulnerability] [High]

Active Exploitation of Critical flaws in Ivanti EPMM to Deploy Multi-Stage Malware [Vulnerability] [High]

Google Chrome Security Update Addresses Eight High-Severity Vulnerabilities [Vulnerability] [Medium]

Multiple Vulnerabilities Discovered in F5 NGINX [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Abuse of Microsoft Device Code OAuth Flow in Sophisticated Phishing Campaign	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at PaloAltoNetworks have identified an active phishing campaign that impersonates a well-known cloud-based file storage service and two electronic signature platforms. This campaign leverages Microsoft's Device Code OAuth flow, tricking victims into entering a verification code on a legitimate Microsoft login page, while the attacker's server captures the resulting OAuth tokens in the background. These tokens provide attackers with long-term access to victims' accounts, including email and files.

This campaign may impact organizations in the financial services sector, particularly those utilizing cloud-based services for document management and communication. Financial institutions should be aware of the sophisticated techniques employed, such as obfuscated payloads and anti-bot measures, which could allow similar attacks to bypass traditional security measures.

Technical Details

- Phishing links are embedded in emails, specifically tailored to target individual customers.
- The attacker serves an obfuscated HTML page containing an encrypted payload with a decryption key.
- The victim's browser decrypts the payload in-browser, replacing the visible shell with legitimate branding.
- A "start session" request is sent to the attacker's server, initiating the Microsoft Device Code flow.
- The attacker relays the user code back to the victim's browser, instructing them to visit microsoft[.]com/devicelogin.
- Upon pasting the user code and signing in, the attacker’s server polls Microsoft for the access token.
- The access token is stored by the attacker, granting immediate access to the victim's Microsoft account.
- The browser is redirected to a legitimate brand page, misleading the victim into believing they completed a valid verification step.
- Advanced evasion techniques include disabling developer tools and obfuscating URLs to avoid detection.
- The campaign has multiple variants targeting different services, showcasing its adaptability.

Recommendations

- Implement multi-factor authentication (MFA) for all user accounts to add an additional layer of security.
- Educate employees about phishing tactics, emphasizing the importance of verifying URLs before entering credentials.
- Monitor for unusual login attempts and access token requests from unfamiliar locations or devices.

- Regularly update and patch systems to protect against known vulnerabilities.
- Utilize advanced email filtering solutions to detect and block phishing emails before they reach users.

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
Threat Actors Exploit Windows Toast Notifications for Credential Harvesting	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a campaign leveraging Windows Toast Notifications to manipulate users into performing actions that may lead to credential harvesting. This technique utilizes the Application User Model ID (AUMID) to create seemingly legitimate notifications that can trick users into clicking malicious links or providing sensitive information. The campaign has been facilitated by tools like "ToastNotify," which can generate custom notifications.

This campaign may impact organizations in the financial services sector, as threat actors could exploit the trust users place in system notifications. Financial institutions should be aware that such social engineering tactics can lead to unauthorized access and lateral movement within their networks, potentially compromising sensitive financial data.

Technical Details

- The campaign uses Windows Toast Notifications, which are legitimate system alerts, to deceive users.
- Attackers can enumerate AUMIDs using PowerShell scripts to identify applications capable of sending notifications.
- A PowerShell script called "Invoke-CredentialPhisher" was previously used to create deceptive notifications, although it may not work on newer Windows versions.
- The "ToastNotify" assembly allows for in-memory execution of notifications, enhancing the attack's stealth.
- Notifications can prompt users to click on links or provide credentials, appearing to come from trusted applications.
- The campaign can utilize Microsoft Teams AUMIDs to impersonate users and request sensitive actions, such as joining calls.
- The success of this campaign relies on the attackers' ability to establish a channel with the endpoint before executing the notification.

Recommendations

- Implement group policies to restrict or manage Toast Notifications across all systems and login portals.
- Develop detection rules for processes attempting to load notification-related DLLs, focusing on unusual behaviors.
- Educate employees about the risks associated with clicking on notifications and the importance of verifying their legitimacy.
- Regularly review and monitor the Notifications registry hive for abnormal activities or unexpected changes.
- Ensure that all critical business systems have endpoint protection measures in place to detect and respond to suspicious activities.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
macOS ClickFix Campaign Using Fake "Claude Code Docs" to Deliver AMOS Stealer	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a campaign targeting users of Claude Code, Grok, n8n, NotebookLM, Gemini CLI, OpenClaw, and Cursor with the AMOS Stealer malware. The attack employs a redirect from Google ads to a fake documentation page, where a ClickFix flow is used to deliver the malicious payload. This payload downloads an encoded script that installs AMOS Stealer, which collects sensitive data and deploys a backdoor for persistent access.

This campaign may impact organizations in the financial services sector, particularly those utilizing macOS in their environments. As macOS adoption grows, the exploitation of visibility gaps makes early detection challenging, potentially leading to credential theft and data exfiltration, which could affect sensitive financial information.

Technical Details

- Attackers redirect users from Google ads to a counterfeit Claude Code documentation page to initiate the attack.
- A ClickFix flow is utilized to deliver the payload, which is an encoded script.
- The script installs AMOS Stealer, which collects browser data, credentials, Keychain contents, and sensitive files.
- The malware deploys a backdoor module located at "~/.mainhelper" for persistent access.

- The backdoor has evolved from its original version, which supported limited commands via HTTP polling.
- The updated backdoor introduces a fully interactive reverse shell over WebSocket with PTY support.
- This evolution allows attackers real-time control over the infected macOS system.
- Multi-stage delivery and obfuscated scripts hinder detection and visibility into the attack.
- Legitimate macOS components are abused, complicating the identification of malicious activity.
- The complexity of the attack slows down triage and escalation decisions, increasing the risk of data theft.

Recommendations

- Implement robust endpoint detection and response solutions to monitor for unusual script executions.
- Educate employees about the risks of clicking on suspicious ads or links, especially those claiming to be documentation.
- Regularly review and update security policies to address the evolving threat landscape for macOS environments.
- Employ multi-factor authentication (MFA) to protect sensitive accounts and data from unauthorized access.
- Conduct regular security assessments and penetration testing to identify vulnerabilities in macOS systems.

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

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
High-Severity WebLogic Vulnerabilities Observed on a High-Interaction Oracle Honeypot	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at CloudSEK have analyzed attack data from a high-interaction honeypot simulating a vulnerable Oracle WebLogic Server. The study revealed a surge in automated exploitation attempts targeting the recently disclosed CVE-2026-21962, a critical unauthenticated Remote Code Execution (RCE) vulnerability, immediately after public exploit code was released. This highlights the speed at which attackers can weaponize newly disclosed vulnerabilities.

This campaign may impact organizations in the financial services sector that utilize Oracle WebLogic Server. The rapid adoption of these exploits underscores the need for immediate patching and robust security measures to mitigate the risk of unauthorized access and potential data breaches.

Technical Details

- The honeypot emulated an unpatched Oracle WebLogic Server (v14.1.1.0.0) over a 12-day period, capturing extensive attack data.
- Attackers exploited CVE-2026-21962, which allows unauthenticated RCE via specially crafted HTTP requests.
- Other targeted vulnerabilities included CVE-2020-14882/14883, CVE-2020-2551, and CVE-2017-10271, all of which also permit RCE.
- Attackers predominantly used rented Virtual Private Servers (VPS) from providers like DigitalOcean and HOSTGLOBAL PLUS.
- High-volume automated scanning was observed, with tools such as libredtail-http and Nmap Scripting Engine being frequently utilized.
- Attack patterns indicated a "spray and pray" approach, with attempts to exploit various non-WebLogic vulnerabilities as well.
- The logs revealed a significant number of reconnaissance requests, indicating broad scanning for vulnerabilities.
- Specific attack vectors included HTTP GET and POST requests targeting WebLogic console endpoints and other critical paths.
- The data collection setup included a reverse Nginx proxy for logging all requests, enhancing visibility into attack attempts.

Recommendations

- Immediately apply the latest Oracle Critical Patch Updates (CPUs) to all WebLogic components.
- Restrict access to the WebLogic administrative console by using firewalls and VPNs to limit exposure.
- Deploy a Web Application Firewall (WAF) to filter and block malicious traffic targeting known vulnerabilities.
- Enhance logging and monitoring for WebLogic components to detect unusual activity and rapid access attempts.
- Implement the principle of least privilege by running the WebLogic Server with minimal operating system privileges.

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
DPRK-Linked Nickel Alley exploits fake jobs and developer toolchains to deliver PyLangGhost	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have uncovered a sustained social-engineering campaign by the North Korea–linked group NICKEL ALLEY, which fabricates job opportunities and developer toolchains to deliver the PyLangGhost RAT. This campaign employs tactics such as fake interviews and developer-centric lures to gain trust and ultimately execute malware aimed at stealing cryptocurrency and other sensitive data.

The implications of this campaign may affect organizations in the financial services sector, particularly those with technology firms, blockchain startups, and developer teams. The methods used by NICKEL ALLEY highlight the risk of credential theft and potential supply-chain exposure, especially if developers execute unvetted code on enterprise systems. Financial institutions should be aware of these tactics to safeguard against potential data theft and espionage.

Technical Details

- NICKEL ALLEY fabricates companies and job opportunities to gain trust and deliver malware.
- The campaign utilizes the ClickFix tactic to push the Python-based PyLangGhost RAT.
- Fake interview workflows are employed to lure victims into executing malicious code.
- Developers are coerced into cloning repositories that fetch payloads like BeaverTail and OtterCookie.
- The group rotates infrastructure to align with their lures and evade detection.
- PyLangGhost supports file exfiltration, arbitrary command execution, and credential harvesting.
- The actors abuse cloud hosting and developer tooling to stage and execute payloads.
- ClickFix involves victims running commands that retrieve and execute malware from local environments.
- The campaign reflects a disciplined operation blending social engineering with developer workflow abuse.

Recommendations

- Harden developer workflows by requiring isolated sandboxes for evaluating external repositories.
- Constrain script interpreters and tooling with application control and alerting on unusual process chains.
- Detect ClickFix-style flows by monitoring command execution initiated from browser interactions.
- Secure recruitment channels by establishing verified contact procedures and training staff on unsolicited requests.
- Instrument IDEs and CI/CD by disabling autorun features and logging network calls from IDEs.

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
Kinsing Campaign Exploits Multiple CVEs Using Shared Infrastructure	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Canary Intelligence have identified a resurgence of the Kinsing malware campaign, which is exploiting vulnerabilities CVE-2023-46604, CVE-2023-38646, and CVE-2025-55182. The exploitation activities are linked to a shared infrastructure, with the attacker node 212.113.98.30 observed initiating attacks on March 12, 2026. This marks the first association of Kinsing with CVE-2025-55182 in their monitoring systems.

This campaign may impact organizations in the financial services sector as Kinsing continues to leverage known vulnerabilities to infiltrate systems. Financial institutions should be aware that the Kinsing malware is capable of evading detection and maintaining persistence through stealth techniques, which could lead to unauthorized access and data compromise.

Technical Details

- The Kinsing malware campaign is exploiting CVE-2023-46604 (ActiveMQ) and CVE-2023-38646 (Metabase) as well as the newly associated CVE-2025-55182 (React2Shell).
- The exploitation of CVE-2023-38646 involves sending a POST request to trigger command execution via a crafted JSON payload.
- The payload retrieves and executes a script from the staging host, which downloads core Kinsing components.
- The script "mt[.]sh" includes commands to kill processes and overwrite crontab entries, indicative of Kinsing's persistence mechanisms.
- Kinsing installs "libsystem[.]so" to hide its activities within normal user-space processes, enhancing its stealth capabilities.
- The campaign utilizes the JavaScript execution primitive of CVE-2025-55182 to run a bash stager that fetches additional payloads.
- The stager uses bash's /dev/tcp to retrieve scripts directly from the staging infrastructure, bypassing traditional utilities like curl or wget.
- The Kinsing campaign demonstrates that older malware can remain effective by leveraging new vulnerabilities without needing significant changes to its core components.
- Canary Intelligence's analysis highlights the clustering of these CVEs around the same infrastructure, indicating a coordinated exploitation effort.

Recommendations

- Implement robust monitoring on all systems and login portals to detect unusual activity associated with known vulnerabilities.
- Ensure that all software is updated to mitigate the risks associated with CVE-2023-46604, CVE-2023-38646, and CVE-2025-55182.
- Employ network segmentation to limit the potential spread of malware within organizational infrastructure.
- Conduct regular security training for staff to recognize and respond to phishing attempts that may lead to exploitation.
- Review and enhance incident response plans to address potential Kinsing-related incidents effectively.

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
China-Nexus Red Menshen Deploys BPFdoor Backdoors	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Rapid7 Labs have identified a campaign by the China-nexus threat actor, Red Menshen, which involves embedding stealthy digital sleeper cells within telecommunications networks. This campaign aims to facilitate high-level espionage, potentially impacting government communications and critical infrastructure on a global scale. The BPFdoor backdoor, a key component of this operation, operates within the Linux kernel, making it exceptionally difficult to detect and remove.

The implications of this campaign may affect organizations in the financial services sector, particularly those involved in telecommunications or reliant on these networks for operations. As these networks are integral to the digital economy, the presence of such advanced persistent threats could lead to unauthorized access to sensitive communications and data, raising concerns about the security of financial transactions and customer information.

Technical Details

- BPFdoor operates within the Linux kernel, utilizing Berkeley Packet Filter (BPF) functionality to inspect network traffic without exposing traditional command-and-control channels.
- The backdoor activates only upon receiving a specifically crafted trigger packet, allowing it to remain dormant and undetected until needed.
- Initial access to telecom environments is often achieved through exploitation of public-facing applications and abuse of valid accounts on devices like VPN appliances and firewalls.

- The campaign employs tools such as CrossC2, a Linux-compatible beacon framework, and TinyShell, a passive backdoor framework, for lateral movement and persistence.
- BPFdoor variants have evolved to use encrypted HTTPS traffic for command delivery, complicating detection efforts.
- The implant can masquerade as legitimate system processes, further obfuscating its presence within the network.
- Attackers leverage ICMP packets as a lightweight communication mechanism between compromised hosts, allowing for covert command propagation.
- The backdoor's architecture supports long-term intelligence collection and monitoring of sensitive communications, raising national security concerns.

Recommendations

- Implement enhanced monitoring of kernel-level operations and network traffic to detect unusual behavior indicative of BPFdoor activity.
- Regularly update and patch public-facing applications and devices to mitigate initial access points for attackers.
- Employ multi-factor authentication for all remote access systems to reduce the risk of credential abuse.
- Conduct regular security assessments and penetration testing to identify vulnerabilities within telecom infrastructure.
- Share intelligence and collaborate with national CERTs and industry partners to stay informed about emerging threats and mitigation strategies.

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
TeamPCP Threat Actor Compromises LiteLLM as Part of a Supply Chain Campaign	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at Endor Labs have identified that two backdoored versions of the LiteLLM library (1.82.7 and 1.82.8) were published on PyPI, containing malicious code that enables credential harvesting and lateral movement within Kubernetes environments. The malicious payload activates upon importing the library, executing a sophisticated three-stage attack that compromises sensitive credentials and establishes a persistent backdoor.

This campaign may impact organizations in the financial services sector that utilize LiteLLM or similar libraries in their development processes. The targeted nature of this attack, focusing on security-adjacent tools,

indicates that financial institutions should be vigilant about the integrity of their software supply chains and the potential for similar exploitation of other widely used libraries.

Technical Details

- The malicious code is injected into "litellm/proxy/proxy_server[.]py", executing upon import and enabling credential harvesting.
- Version 1.82.8 includes a ".pth" file that runs the payload on any Python invocation, increasing the attack surface.
- The payload conducts a three-stage attack: credential harvesting, Kubernetes lateral movement, and installation of a persistent backdoor.
- Credentials harvested include SSH keys, cloud tokens, Kubernetes secrets, and cryptocurrency wallets.
- The attacker deploys privileged pods across Kubernetes clusters, gaining extensive access to the environment.
- The persistence mechanism is established through a systemd service that periodically polls for additional payloads.
- Exfiltrated data is encrypted and sent to attacker-controlled domains, complicating detection efforts.
- The campaign is attributed to TeamPCP, known for targeting security-related software.
- The attack exploits the trust placed in security tools, allowing for broad access once compromised.
- The campaign has already affected multiple ecosystems, indicating a coordinated and ongoing effort.

Recommendations

- Verify that no backdoored versions of LiteLLM (1.82.7 or 1.82.8) are installed in your environments.
- Audit CI/CD pipelines for usage of compromised tools during the attack window and rotate all accessible credentials.
- Implement dependency pinning and integrity checks against upstream repositories to prevent similar compromises.
- Monitor for unexpected changes in dependencies and employ automated diff reviews.
- Educate development teams on secure coding practices and the risks associated with using third-party libraries.

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
Multi-Vector Malware Campaign Exploits VBS and Open Infrastructure	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at LevelBlue SpiderLabs have identified a multi-stage malware delivery campaign that began with a suspicious Visual Basic Script (VBS) file. Although endpoint protection mechanisms successfully prevented the execution of the file, further analysis revealed a sophisticated malware framework utilizing fileless loaders, obfuscation techniques, and various payload delivery methods. The campaign includes multiple obfuscated VBS files leading to different malware payloads, such as XWorm and Remcos RAT, and a secondary infection vector involving weaponized documents.

This campaign may impact organizations in the financial services sector as it demonstrates advanced evasion techniques that could bypass traditional security measures. The use of open directories for malware staging and delivery increases the potential for widespread exploitation, indicating that financial institutions should be vigilant against similar multi-vector attacks leveraging reusable malware frameworks.

Technical Details

- The campaign was initiated by a suspicious VBS file named "Name_File[.]vbs" detected in the "\Users\Public\Downloads\" directory.
- The VBS file acted as an obfuscated launcher, decoding, and executing a secondary PowerShell payload rather than containing malicious logic directly.
- The PowerShell command retrieved a PNG file from a remote server, which contained a Base64-encoded .NET assembly, enabling execution without writing to disk.
- The embedded .NET assembly, known as PhantomVAI, facilitated the loading of additional malware payloads and persistence mechanisms.
- The attacker utilized open directories on the domain news4me[.]xyz to host multiple VBS files and malware payloads, indicating a modular delivery model.
- A secondary infection vector involved a weaponized "PDF" and batch script, which redirected users to attacker-controlled domains for further payload retrieval.
- The batch script executed in a hidden context and established outbound connections to external URLs hosting additional malicious files.
- The campaign's infrastructure allows for rapid modification and expansion of available payloads without altering the initial delivery mechanism.
- The presence of Python-based tooling introduces an additional execution layer capable of handling post-compromise activities.
- The use of non-traditional file formats and scripting languages enhances the campaign's evasion capabilities against signature-based defenses.

Recommendations

- Restrict execution of high-risk script types such as ".vbs" and ".bat" from user-writable directories to reduce initial access risks.
- Monitor and constrain PowerShell usage, particularly focusing on in-memory execution techniques to limit attacker flexibility.
- Implement network controls to block or tightly regulate WebDAV traffic to disrupt Internet Shortcut-based delivery methods.
- Consider TLD-based filtering to restrict access to commonly abused domains, such as those ending in ".xyz".
- Conduct deeper analysis beyond initial alerts to identify supporting infrastructure and alternate delivery paths, enhancing overall threat detection capabilities.

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
Kamasers Botnet Launches Multi-Vector DDoS Attacks Targeting Organizations Worldwide	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified the Kamasers botnet, a sophisticated DDoS attack platform capable of executing both application-layer and transport-layer attacks. This botnet employs resilient command-and-control mechanisms, utilizing legitimate public services to maintain its operations and evade detection. The malware can also function as a loader, increasing the risk of further compromise and data theft.

The Kamasers botnet may impact organizations in the financial services sector by turning compromised systems into operational liabilities. If corporate infrastructure is exploited for DDoS attacks, it could lead to reputational damage and regulatory scrutiny. Financial institutions should be aware of the risks associated with such botnets, as they can create vulnerabilities that extend beyond immediate DDoS threats.

Technical Details

- Kamasers supports various DDoS attack vectors, including HTTP, TLS, UDP, TCP, and GraphQL-based flooding.
- The botnet can act as a loader, downloading and executing additional payloads, which raises the risk of data theft and ransomware deployment.

- Its command-and-control (C2) infrastructure utilizes a Dead Drop Resolver (DDR) mechanism through legitimate services like GitHub Gist, Telegram, and Dropbox.
- The botnet was observed distributing through established malware delivery chains, specifically GCleaner and Amadey.
- The botnet can turn infected enterprise systems into attack infrastructure, posing reputational and legal risks.
- It employs advanced techniques such as IP spoofing and connection-holding methods to enhance attack efficacy.
- The bot retrieves commands from C2 servers, executing DDoS attacks based on specified parameters.
- Kamasers has been linked to Railnet ASN, which has a history of malicious activity across various malware families.
- The botnet's use of public services for C2 discovery complicates detection and response efforts.

Recommendations

- Monitor all outbound connections for suspicious activity and unusual patterns indicative of botnet behavior.
- Implement robust incident response plans to address potential DDoS attacks and associated risks.
- Utilize threat intelligence feeds to gain visibility into emerging threats and malicious infrastructure.
- Conduct regular security assessments to identify vulnerabilities that could be exploited by botnets like Kamasers.
- Educate employees on recognizing signs of malware infections and the importance of reporting suspicious activities.

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
Critical Supply Chain Compromise in Aqua Security Trivy Ecosystem	**MEDIUM**	**CLEAR**	**Campaign**	**CSC**

Executive Summary

A significant software supply chain attack has impacted the Aqua Security Trivy ecosystem, where threat actors exploited compromised credentials to distribute malicious versions of Trivy binaries, GitHub Actions, and container images. This attack was facilitated by incomplete credential rotation following an earlier breach, allowing attackers to maintain persistence and introduce credential-stealing malware into widely used CI/CD components.

This campaign may impact organizations in the financial services sector that utilize CI/CD pipelines relying on the affected Trivy versions. The potential for full CI/CD pipeline compromise and exposure of sensitive secrets, such as API keys and cloud credentials, could affect the integrity and security of development processes within financial institutions.

Technical Details

- The threat actor used compromised credentials and tokens to initiate the attack.
- Exploited a credential rotation window that lasted several days after the initial breach.
- Inserted credential-stealing malware into GitHub Actions, CLI binaries, and container images.
- Conducted force-push attacks on version tags, undermining trust in versioning.
- Replaced legitimate code with credential harvesting logic, posing a risk to CI/CD pipelines.
- Created suspicious repositories, indicating successful exfiltration fallback.
- Abused mutable version tags instead of immutable commit SHAs, increasing vulnerability.
- The attack has been classified under CVE-2026-33634, with a CVSS score of 9.4 (Critical).
- Organizations using affected versions may face lateral movement into production environments.
- The attack could lead to downstream supply chain compromises affecting various stakeholders.

Recommendations

- Identify exposure by checking for usage of Trivy versions 0.69.4, 0.69.5, and 0.69.6 distributed via Docker Hub.
- Update to known-safe versions of Trivy to mitigate risks.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical RCE Vulnerabilities in n8n Workflow Automation Platform	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

The n8n Workflow Automation Platform has been identified with critical remote code execution (RCE) vulnerabilities, specifically CVE-2026-33660 and CVE-2026-33696. These vulnerabilities allow authenticated users with workflow permissions to execute malicious SQL queries and inject harmful properties, potentially leading to full system compromise.

This vulnerability may affect organizations in the financial services sector that utilize the n8n platform for workflow automation. Financial institutions should be aware that these vulnerabilities could enable attackers to execute arbitrary code and manipulate application logic, posing significant risks to data integrity and security.

Technical Details

- CVE-2026-33660 allows RCE through the Merge node when configured in “Combine by SQL” mode, leveraging the AlaSQL library.
- Insufficient sandboxing permits authenticated users to execute malicious SQL queries on the host system.
- The impact includes reading arbitrary local files and executing arbitrary code, leading to full system compromise.
- CVE-2026-33696 enables prototype pollution in the GSuiteAdmin node, allowing attackers to inject malicious properties into the global Object.prototype.
- This vulnerability can lead to arbitrary code execution and bypass security controls.
- Both vulnerabilities have a critical severity rating with a CVSS score of 9.4.
- All versions of n8n prior to the patched releases are affected.

Recommendations

- Update to the latest versions of n8n: 2.14.1 or later, 2.13.3 or later, or 1.123.27 or later.

Detailed Vulnerability Details and Affected Products can be found *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Citrix Addresses Critical and High Severity Flaws in Multiple Products – Active Reconnaissance Observed	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Citrix has addressed critical and high-severity vulnerabilities in its NetScaler ADC and NetScaler Gateway products, specifically CVE-2026-3055 and CVE-2026-4368. CVE-2026-3055 allows unauthenticated remote attackers to extract sensitive data, including session tokens and administrative credentials, while CVE-2026-4368 can lead to unauthorized visibility within another user's session context. Both vulnerabilities pose significant risks to organizations using these products, as they can bypass authentication measures and facilitate unauthorized access.

This situation may impact organizations in the financial services sector that utilize Citrix products for secure transactions and data management. The observed active reconnaissance suggests that threat actors are preparing for potential exploitation, highlighting the urgency for financial institutions to patch their systems and monitor for unusual activity. Organizations should prioritize immediate remediation to mitigate risks associated with these vulnerabilities.

Technical Details

- CVE-2026-3055 is a critical vulnerability with a CVSS score of 9.3, allowing attackers to perform an out-of-bounds read and extract sensitive data from memory.
- CVE-2026-4368 has a CVSS score of 7.7 and involves a race condition that can lead to user session mix-ups, granting unauthorized access to another user's session.
- Successful exploitation of these vulnerabilities can bypass authentication and multi-factor authentication (MFA) measures.
- Attackers can extract active session tokens, administrative credentials, and SSL private keys from vulnerable appliances configured as SAML Identity Providers (IdP).
- Active reconnaissance has been observed, with attackers probing the endpoint "/cgi/GetAuthMethods" to fingerprint authentication methods.
- Vulnerable versions include NetScaler ADC and NetScaler Gateway 14.1 (before 14.1-66.59), 13.1 (before 13.1-62.23), and FIPS/NDcPP (before 13.1-37.262).
- The reconnaissance phase typically precedes automated exploitation, indicating an urgent need for patching.

Recommendations

- Immediately upgrade to the fixed builds for NetScaler ADC and Gateway as specified in the advisory.
- Audit all configurations for the identified strings to ensure no vulnerable setups remain.
- Monitor logs for any anomalous requests to the "/cgi/GetAuthMethods" endpoint or unusual session behaviors.
- Terminate all active and persistent sessions after applying patches to prevent token misuse.
- Utilize built-in CVE detection and remediation workflows available in the NetScaler Console/Service for ongoing security management.

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

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Code Execution Vulnerability in Langflow Exposes Systems to Attacks	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical vulnerability, tracked as CVE-2026-33017, has been discovered in Langflow, allowing unauthenticated remote code execution (RCE) through the "/api/v1/build_public_tmp/{flow_id}/flow"

endpoint. This flaw permits attackers to execute arbitrary code without authentication, leading to potential full system compromise, including command execution and data exfiltration.

Organizations in the financial services sector should be aware that this vulnerability may affect their systems if they utilize Langflow versions 1.8.1 or earlier. Given the nature of the vulnerability, it could lead to severe consequences, including unauthorized access to sensitive data and lateral movement within networks, making immediate action essential.

Technical Details

- The vulnerability is tracked as CVE-2026-33017 and has a CVSS v4 score of 9.3, indicating critical severity.
- It allows unauthenticated remote code execution via the "/api/v1/build_public_tmp/{flow_id}/flow" endpoint.
- The flaw arises from improper handling of attacker-controlled input executed through Python's exec() function.
- Attackers can exploit this vulnerability without requiring credentials or user interaction.
- Successful exploitation can lead to full system compromise, including command execution and data exfiltration.
- Affected versions of Langflow are those up to and including 1.8.1.
- The vulnerability has been patched in version 1.9.0 and later.
- The attack vector for this vulnerability is network-based, allowing remote exploitation.

Recommendations

- Organizations using Langflow should prioritize applying the patch available in version 1.9.0 or later.

Detailed Vulnerability Details and Affected Products can be found *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Active Exploitation of Critical flaws in Ivanti EPMM to Deploy Multi-Stage Malware	**HIGH**	**CLEAR**	**Vulnerability**	**Open Source**

Executive Summary

Researchers at WithSecure have identified active exploitation attempts targeting critical vulnerabilities in Ivanti's Endpoint Manager Mobile (EPMM), tracked as CVE-2026-1281 and CVE-2026-1340. These flaws allow threat actors to achieve unauthenticated remote code execution, potentially leading to data exfiltration and persistent access to compromised systems. The exploitation attempts have varied in success, with some failing due to URL-encoding errors, while others have resulted in confirmed data breaches.

This vulnerability may affect organizations in the financial services sector that utilize Ivanti EPMM for mobile device management. Successful exploitation could allow attackers to access sensitive information, including

administrator credentials and device identifiers. Financial institutions should be aware of the risks associated with these vulnerabilities and take immediate action to mitigate potential impacts.

Technical Details

- The vulnerabilities CVE-2026-1281 and CVE-2026-1340 have a CVSS score of 9.8, indicating critical severity.
- Exploitation allows unauthenticated remote code execution on the EPMM appliance.
- Attackers can access sensitive information, including usernames, email addresses, and device identifiers.
- Multiple threat actors have been observed exploiting these vulnerabilities simultaneously.
- Some exploitation attempts have failed due to URL-encoding errors, while others succeeded.
- In one confirmed case, data exfiltration occurred through a fully automated operation.
- The AntSword offensive framework has been leveraged by attackers, indicating a lower barrier for exploitation.
- There are indicators of tooling reuse associated with other threat actors, suggesting shared resources.
- A publicly available Proof-of-Concept (POC) exploit exists for these vulnerabilities.

Recommendations

- Organizations using Ivanti EPMM should apply the latest patches, RPM 12.x.0.x or RPM 12.x.1.x, based on their specific version.
- Ensure that all systems running Ivanti EPMM are updated to the latest version to mitigate risks.
- Monitor for unusual activity or unauthorized access attempts on mobile device management systems.
- Implement network segmentation to limit access to critical systems and reduce potential damage from exploitation.

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

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Google Chrome Security Update Addresses Eight High-Severity Vulnerabilities	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Google has released a security update for the Google Chrome desktop browser, addressing eight high-severity vulnerabilities related to memory safety issues, including use-after-free, heap buffer overflows, integer overflows, and out-of-bounds reads. These vulnerabilities could allow attackers to execute arbitrary code, cause browser crashes, or compromise system integrity.

This vulnerability may affect organizations in the financial services sector that rely on Google Chrome for secure browsing. Financial institutions should be aware that unpatched vulnerabilities in widely used software can lead to exploitation attempts, potentially compromising sensitive data and systems.

Technical Details

- CVE-2026-4673: A heap buffer overflow vulnerability in WebAudio could allow attackers to execute arbitrary code.
- CVE-2026-4674: An out-of-bounds read in CSS may lead to browser crashes or unexpected behavior.
- CVE-2026-4675: A heap buffer overflow in WebGL could be exploited to execute malicious code.
- CVE-2026-4676: A use-after-free vulnerability in Dawn may allow attackers to manipulate memory.
- CVE-2026-4677: An out-of-bounds read in WebAudio could compromise system integrity.
- CVE-2026-4678: A use-after-free vulnerability in WebGPU may lead to arbitrary code execution.
- CVE-2026-4679: An integer overflow in Fonts could be exploited to cause crashes or execute code.
- CVE-2026-4680: A use-after-free vulnerability in FedCM may allow attackers to gain control over the browser.
- The update is available in Chrome version 146.0.7680.164 for Linux and 146.0.7680.164/165 for Windows and Mac.

Recommendations

- Update Google Chrome to the latest version to ensure all vulnerabilities are patched.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities Discovered in F5 NGINX	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

F5 NGINX has been found to have multiple high-severity vulnerabilities, including buffer overflow and memory corruption issues that could lead to denial-of-service conditions. These vulnerabilities affect both NGINX Plus and Open-Source versions, potentially allowing attackers to crash worker processes or execute arbitrary code.

Organizations in the financial services sector should be aware that these vulnerabilities may affect their systems if they utilize any versions of NGINX listed as vulnerable. The potential for denial-of-service attacks could disrupt services, making it crucial for financial institutions to monitor their NGINX deployments and apply the necessary mitigations provided by F5.

Technical Details

- CVE-2026-27654: A buffer overflow vulnerability in the ngx_http_dav_module could allow an attacker to crash the NGINX worker process or manipulate file paths outside the document root.
- CVE-2026-27784: A buffer over-read/overwrite vulnerability in the ngx_http_mp4_module affects 32-bit NGINX Open-Source systems, potentially leading to memory corruption and denial-of-service conditions.
- CVE-2026-32647: This vulnerability in the MP4 module may allow attackers to perform buffer over-read or overwrite operations, causing worker process termination or enabling arbitrary code execution.
- CVE-2026-27651: A flaw in the ngx_mail_auth_http_module can allow unauthenticated attackers to crash worker processes repeatedly when CRAM-MD5 or APOP authentication is enabled, leading to denial-of-service.
- Affected Products: NGINX Plus versions R32 – R36 and NGINX Open-Source versions 1.0.0 – 1.29.6, including legacy versions 0.5.13 – 0.9.7.
- The vulnerabilities can be triggered by specific actions, such as using MOVE or COPY methods in combination with alias directives.
- Exploitation of these vulnerabilities could lead to significant service disruptions for organizations using affected NGINX versions.

Recommendations

- Review and update all NGINX installations to ensure they are running the latest patched versions.
- Implement the mitigation or workaround provided by F5 to protect against these vulnerabilities.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

macOS ClickFix Campaign Using Fake "Claude Code Docs" to Deliver AMOS Stealer

TACTIC	TECHNIQUE	DESCRIPTION
Execution	T1059.002 Command and Scripting Interpreter: AppleScript	Use of osascript for persistence loop and user credential validation via dscl.
Persistence	(Unmapped in source)	Wrapper script runs infinite osascript loop to launch ~/.mainhelper.
Defense Evasion	T1497.001 Virtualization/Sandbox Evasion: System Checks	Anti-VM checks via system_profiler.
Credential Access	T1555.001 Credentials from Password Stores: Keychain	Keychain credential collection attempts observed.
Credential Access	T1555.003 Credentials from Web Browsers	Targeting of browser-stored credentials, cryptocurrency wallet extension IDs detected in osascript.
Collection	T1074.001 Local Data Staging	Staging of stolen data into out[.]zip (e.g., cookies.sqlite, NoteStore.sqlite, Web Data) prior to exfiltration.

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 operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect 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
.pth file (LiteLLM 1.82.8)	File that executes payloads on any Python invocation, broadening attack reach.
/cgi/GetAuthMethods	Endpoint probed during active reconnaissance to fingerprint authentication methods.
/dev/tcp (bash)	Bash feature abused to fetch scripts directly from staging servers without curl/wget.
~/.mainhelper (backdoor module)	Location of the macOS backdoor component providing persistence for AMOS Stealer.
AlaSQL (library)	SQL engine used in n8n context that, without strict sandboxing, enabled RCE.
AMOS Stealer	macOS malware that collects browser data, credentials, Keychain contents, and files, then drops a persistent backdoor.
Anti-bot measures	Evasion techniques (e.g., disabling developer tools, URL obfuscation) used to avoid automated detection.
AntSword (tooling)	Offensive framework leveraged in successful Ivanti exploitation chains.
Application-layer vs transport-layer DDoS	Attack types targeting web/application protocols or network transport protocols, respectively.
Aqua Security Trivy (ecosystem)	Security tooling compromised via credentials to distribute malicious binaries, Actions, and images.
AUMID (Application User Model ID)	Identifier used to impersonate trusted apps in fake toast notifications for credential harvesting.
Automated scanning / reconnaissance	High-volume probing of exposed services using tools and VPS infrastructure to find exploitable targets.
Backdoor	Hidden access mechanism (e.g., BPFdoor, LiteLLM persistence) enabling remote control.
Base64-encoded .NET assembly	Payload hidden inside an image to enable execution without touching disk.
BeaverTail / OtterCookie	Payloads retrieved via coerced developer workflows in the NICKEL ALLEY operation.
Berkeley Packet Filter (BPF)	Kernel functionality enabling traffic inspection without typical C2 channels, aiding stealth.
Botnet	Network of compromised systems used for DDoS and to load additional malware.
BPFdoor	Linux backdoor operating via Berkeley Packet Filter, activating on a specific trigger packet to stay covert.
C2 (Command and Control)	Attacker infrastructure to receive commands and exfiltrate data; discovered via DDR in Kamasers.
Citrix NetScaler ADC / Gateway	Appliances with critical/high flaws enabling data extraction and unauthorized session access.
ClickFix (developer lures)	Technique where victims run suggested commands that actually fetch and execute malware locally.
Credential harvesting	Stealing passwords/tokens via deceptive prompts or compromised tools/libraries.
Credential rotation window	Gap after an earlier breach that allowed attackers to maintain persistence.
crontab overwrite	Technique to maintain control by scheduling recurring malicious tasks.
CrossC2 / TinyShell	Tools used for lateral movement and passive backdoor capabilities in compromised Linux environments.
CSC	UAE Cyber Security Council
CVE-2023-38646 (Metabase)	Flaw exploited via crafted JSON to trigger command execution in Metabase.
CVE-2023-46604 (ActiveMQ)	Vulnerability leveraged by Kinsing as one of several entry points.
CVE-2025-55182 (React2Shell)	JavaScript execution primitive used by Kinsing to run bash stagers and pull payloads.
CVE-2026-1281 / CVE-2026-1340 (EPMM)	Flaws enabling remote code execution and access to sensitive information.
CVE-2026-21962	Critical unauthenticated RCE in WebLogic abused via crafted HTTP requests; quickly weaponized after public exploit.

CVE-2026-3055 (NetScaler)	Critical out-of-bounds read enabling extraction of session tokens, admin credentials, and SSL keys.
CVE-2026-33017 (Langflow)	Critical RCE via /api/v1/build_public_tmp/{flow_id}/flow allowing arbitrary code without authentication.
CVE-2026-33634 (Trivy)	Identifier assigned to the Trivy supply chain incident with critical severity.
CVE-2026-33660 (n8n)	RCE via Merge node in 'Combine by SQL' mode using AlaSQL with insufficient sandboxing.
CVE-2026-33696 (n8n)	Prototype pollution in GSuiteAdmin node enabling arbitrary code execution and control bypass.
CVE-2026-4368 (NetScaler)	Race condition causing user session mix-ups and unauthorized visibility.
CVSS	Common scoring system used to express vulnerability severity in several entries.
Data exfiltration	Automated or encrypted theft of sensitive information from victim systems.
Dead Drop Resolver (DDR)	C2 discovery mechanism using public services (GitHub Gist, Telegram, Dropbox) to locate controllers.
Device Code OAuth flow	Authentication method misused in phishing; victims enter a code at a legitimate Microsoft page while attackers capture tokens for long-term account access.
DigitalOcean / HOSTGLOBAL PLUS	Examples of VPS providers observed in exploit traffic against WebLogic.
DLL (notification-related)	Dynamic link libraries whose unusual loading can signal attempts to craft deceptive toast notifications.
Docker Hub (affected versions)	Distribution channel from which compromised Trivy versions were obtained.
DoS (Denial-of-Service)	Outcome where services are disrupted due to crashes or overload, noted in NGINX and botnet scenarios.
Exfiltration (encrypted)	Outbound transfer of stolen data to attacker domains using encryption to hinder detection.
F5 NGINX (Plus & Open Source)	Web server platforms with multiple high-severity flaws causing crashes or possible code execution.
Fileless execution	Running payloads from memory (e.g., Base64 assemblies in PNG) to avoid disk artifacts.
Fileless loader (PowerShell)	Technique retrieving a PNG with embedded Base64 .NET assembly for in-memory execution.
Force-push / mutable tags	Overwriting version tags, undermining trust compared to immutable commit SHAs.
Google Chrome (security update)	Desktop browser release addressing eight high-severity memory safety bugs.
GraphQL-based flooding	Botnet attack vector that overwhelms GraphQL endpoints.
Hidden execution (batch)	Running scripts without visible windows to avoid user suspicion.
HTTP GET/POST	Web request methods seen in exploit attempts against administrative endpoints.
ICMP (lightweight comms)	Packet type leveraged as a covert communication mechanism between compromised hosts.
IDE / CI/CD instrumentation	Hardening recommendation to disable autorun features and log network calls in developer environments.
Internet Shortcut / WebDAV	Alternate delivery mechanisms abused to fetch and run additional files.
Invoke-CredentialPhisher	PowerShell script previously used to fabricate credential-harvesting notifications (not effective on newer Windows).
IP spoofing / connection-holding	Techniques used to enhance DDoS effectiveness and evade filters.
Ivanti EPMM	Mobile device management platform with actively exploited critical unauthenticated RCEs.
JSON payload (Metabase)	Crafted POST body used to trigger command execution and stage Kinsing components.
Kamasers botnet	DDoS platform capable of HTTP/TLS/UDP/TCP/GraphQL floods and acting as a loader for further compromise.
Keychain (macOS)	macOS secure store targeted for credential theft by AMOS Stealer.

Kinsing	Malware campaign exploiting multiple CVEs (ActiveMQ, Metabase, React2Shell) with stealthy persistence and shared infrastructure.
Kubernetes privileged pods	High-privilege workloads deployed to gain extensive access across clusters.
Kubernetes secrets / cloud tokens / SSH keys	Sensitive credentials targeted for theft during supply-chain abuse.
Langflow	Platform with a critical unauthenticated RCE via a public build endpoint, fixed in 1.9.0+.
Lateral movement	Attacker expansion within environments (e.g., via Kubernetes credentials).
Least privilege (WebLogic)	Operational hardening to run services with minimal OS permissions to reduce impact.
libredtail-http	Scanning tool observed in automated exploitation attempts against a WebLogic honeypot.
libsystem.so (disguise)	Installed component used to hide Kinsing activity within normal user-space processes.
LiteLLM (backdoored PyPI releases)	Library versions 1.82.7/1.82.8 contained code that runs on import, enabling theft and persistence.
macOS ClickFix	Malvertising flow from fake documentation pages that walks users through steps that actually install malware.
Malvertising	Use of paid ads to redirect users to fake pages delivering malware.
Merge node 'Combine by SQL'	n8n configuration that, with AlaSQL, allowed malicious queries and arbitrary code execution.
microsoft[.]com/devicelogin	Legitimate Microsoft verification page abused in the device code phishing flow to make attacks appear authentic.
mt.sh	Downloaded script that kills processes and overwrites crontab entries for persistence.
Multi-stage malware framework (VBS)	Campaign using obfuscated VBS launchers, fileless loaders, and diverse payloads like XWorm/Remcos.
n8n	Workflow automation platform with critical issues enabling SQL-based RCE and prototype pollution.
NetScaler Console/Service CVE workflows	Built-in detection/remediation features referenced for ongoing management.
ngx_http_dav_module (MOVE/COPY + alias)	Buffer overflow allowing worker crashes or path manipulation outside document root.
ngx_http_mp4_module (32-bit)	Buffer over-read/overwrite on 32-bit systems leading to memory corruption/DoS.
ngx_mail_auth_http_module (CRAM-MD5/APOP)	Flaw enabling unauthenticated attackers to repeatedly crash worker processes.
NICKEL ALLEY	DPRK-linked threat group running fake jobs and developer lures to deliver PyLangGhost for credential and crypto theft.
Nmap Scripting Engine	Recon/exploitation component seen in attack traffic targeting vulnerable services.
Notifications registry hive	Windows registry area whose abnormal changes may indicate manipulation of notification behavior.
OAuth access token	Credential issued after sign-in that grants access (e.g., email, files); attackers can reuse tokens to maintain access.
Obfuscated HTML payload	Encrypted or hidden code delivered in phishing pages that the browser decrypts in-memory to mask malicious actions.
Obfuscation	Encoding/hiding of scripts (VBS, PowerShell) and URLs to evade detection.
Open directories	Public folders used to host multiple staged scripts and malware variants.
Oracle Critical Patch Update (CPU)	Vendor patch bundle recommended for immediate application to WebLogic components.
Oracle WebLogic Server	Application server heavily probed and exploited for RCE (e.g., CVE-2026-21962) shortly after exploit release.
Persistence	Techniques (e.g., backdoors, crontab changes, systemd services) to maintain long-term access.
PhantomVAI	Embedded .NET component facilitating loader behavior and persistence.
Phishing (brand impersonation)	Emails linking to fake pages that mimic cloud storage/e-signature providers to kick off device code abuse.

Prototype pollution / Object.prototype	Injection of properties into JavaScript's global object leading to code execution paths.
PTY	Pseudo-terminal support that allows interactive command sessions on a compromised system.
PyLangGhost RAT	Python-based remote access tool enabling file exfiltration, command execution, and credential harvesting.
PyPI	Python Package Index used as distribution channel for the backdoored library.
Python exec() (Langflow)	Improper handling of attacker input executed through exec(), enabling full compromise.
Railnet ASN	Network provider designation associated with malicious activity in this context.
RAT (Remote Access Trojan)	Type of malware providing remote control over infected systems (e.g., Remcos, PyLangGhost).
RCE (Remote Code Execution)	Vulnerability class allowing attackers to run arbitrary code on a target system, often leading to full compromise.
Red Menshen	China-nexus threat actor embedding stealth 'sleeper cells' in telecom networks and deploying BPFdoor implants.
Remcos RAT	Remote access trojan payload observed in the multi-vector campaign.
Reverse Nginx proxy (logging)	Setup used in the honeypot to capture all inbound requests for detailed attack visibility.
Reverse shell	Remote command channel established from victim to attacker; here enabled via WebSocket and PTY.
Reverse shell over WebSocket with PTY	Upgraded backdoor capability enabling real-time, interactive control of infected macOS systems.
RPM 12.x (Ivanti patches)	Recommended patch lines for affected EPMM versions.
SaaS	Cloud-hosted applications referenced in identity and OAuth monitoring recommendations.
SAML	Authentication standard referenced in NetScaler IdP configurations.
SAML Identity Provider (IdP)	Configuration where attackers could extract sensitive keys/tokens from vulnerable appliances.
Secrets (API keys, cloud creds)	Sensitive values at risk of exposure during CI/CD compromise.
SQL	Query language leveraged in n8n 'Combine by SQL' RCE scenario.
Staging host	Attacker-controlled server hosting scripts and payloads for subsequent download.
Supply chain attack (Trivy)	Compromise of upstream components leading to credential-stealing malware in CI/CD pipelines.
systemd service (persistence)	Mechanism used to periodically poll and load additional payloads, maintaining access.
TeamPCP	Threat actor that published backdoored LiteLLM versions to harvest credentials and move laterally in Kubernetes.
Terminate sessions (post-patch)	Action recommended after patching to prevent reuse of stolen tokens.
Three-stage attack (LiteLLM)	Sequence: credential harvesting → Kubernetes lateral movement → persistent backdoor installation.
TLD-based filtering ('.xyz')	Control to restrict access to commonly abused domains such as .xyz in this campaign.
ToastNotify	Assembly used to generate in-memory toast notifications, increasing stealth of social engineering.
Trigger packet	Special network packet that activates dormant BPFdoor functionality.
TTPs	Attacker tactics, techniques, and procedures referenced across campaigns.
URL-encoding errors (exploit)	Observed failure mode in some exploitation attempts; others resulted in confirmed exfiltration.
Use-after-free / heap buffer overflow / integer overflow / out-of-bounds read	Memory issues fixed that could allow code execution or crashes.

VBS (Visual Basic Script)	Initial launcher script that decodes and runs secondary PowerShell without storing to disk.
Version 146.0.7680.164/165	Patched Chrome versions for Linux/Windows/Mac noted in the update.
VPN	Remote-access device type cited as an initial access vector in telecom environments.
VPS (Virtual Private Server)	Rented servers commonly used as attacker infrastructure during exploitation and scanning.
WAF (Web Application Firewall)	Filter used to block malicious traffic targeting known web vulnerabilities.
Weaponized 'PDF' + batch	Secondary vector redirecting users to attacker domains, executing in hidden context to fetch more payloads.
WebAudio / CSS / WebGL / WebGPU / Dawn / FedCM / Fonts	Chrome components cited as affected by the vulnerabilities.
WebSocket	A web protocol that enables persistent, two-way communication; used here to control infected hosts interactively.
Windows Toast Notifications	Legitimate Windows alerts crafted by attackers to prompt clicks or credential entry through deceptive pop-ups.
Worker process (NGINX)	Process targeted by the cited flaws; repeated crashes lead to denial-of-service.
XWorm	Malware payload referenced in the multi-vector campaign.