TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	5/2/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 5 February 2026

9	8	1	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Financial	Actively Exploited & Critical Vulnerabilities	Major Compromises and breaches	Threat actor activities in the UAE & Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a sustained surge in socially engineered intrusions and rapidly weaponized vulnerabilities targeting enterprise users and infrastructure. Phishing remains the primary entry point using tender/RFP lures, contractor-domain credential harvesting against Gmail/Microsoft 365, and cloud-hosted email abuse via AWS WorkMail alongside vishing that targets SaaS access and a malicious VS Code extension delivering remote control capability. In parallel, multiple actively exploited or critical weaknesses across widely used products (including WinRAR, Fortinet SSO, Microsoft Office, Ivanti EPMM, OpenSSL, GNU telnetd, n8n, and vm2) raise the likelihood of unauthorized access and system compromise, while the Crunchbase breach reinforces ongoing data-theft and extortion pressure. For financial services, these developments materially increase the risk of account takeover, sensitive data exposure, and operational disruption through compromised identities, endpoints, and internet-facing services.

ADGM THREAT INTELLIGENCE SUMMARY

Critical Sandbox Escape Vulnerability in vm2 Allows Arbitrary Code Execution [Vulnerability] [Medium]

Crunchbase Confirms Data Breach Exposing Over 2 Million Records [Cyber Breach] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Tender-Themed Phishing Campaign Targets Financial Services with JavaScript Dropper	HIGH	CLEAR	Campaign	CPX-TIC

Executive Summary

CPX-TIC has analyzed a tender-themed phishing campaign that exploits procurement and RFP lures to redirect recipients to malicious content, ultimately delivering a JavaScript-based dropper. The emails originate from a suspicious sender infrastructure flagged by multiple security engines, and the hosted content mimics tender document directories to enhance credibility and increase click-through rates.

This campaign poses significant risks to the Financial Services sector based on observed activity in the region. This campaign employs a multi-stage infection chain associated with remote access tools and information-stealing malware. Once executed, the dropper not only enables persistence but also facilitates command-and-control operations, making it a critical threat to organizations handling sensitive financial data and transactions.

Technical Details

- The attack begins with targeted phishing emails containing links to ‘tender invitations’ or ‘RFPs’, leading to JavaScript droppers hosted on a cloud-based service.
- Victims who click the embedded link are redirected to a file cloud service prompting the download of a RAR file related to tender documents.
- Upon downloading, the RAR file deploys a JavaScript dropper that executes via Windows scripting, utilizing a legitimate LuaJIT interpreter to run malicious code.
- The malware employs signed-binary abuse techniques to evade signature-based defenses while focusing on credential theft from major browsers.
- Persistence is achieved through a scheduled task that triggers frequently, along with modifications to common autorun mechanisms.
- The malware retrieves and launches a remote access payload that communicates with preconfigured command-and-control endpoints.
- The sender domain, lookfang[.]com, has been flagged as suspicious and is linked to the phishing emails, with its mail infrastructure used to relay messages.
- The domain was created in 2013 but recently updated, indicating potential configuration changes for phishing operations.

- The malicious RAR file contains a JavaScript dropper associated with Remcos and Redline Stealer malware families.
- The malware targets sensitive data from web browsers, specifically Chrome, Edge, and Firefox, harvesting credentials stored in various files.

Recommendations

- Implement phishing-resistant MFA (such as FIDO2 or Passkeys) to prevent credential theft even if users are tricked into entering their passwords.
- Enable advanced link-protection and sandbox detonation in email security tools to automatically block malicious redirect chains and anti-analysis environments.
- Restrict access to newly registered or suspicious domains through secure web gateways to prevent users from reaching attacker-controlled infrastructure.
- Strengthen email authentication (DMARC, DKIM, SPF) and continuously monitor partner or supplier accounts to reduce the risk of compromised-sender phishing.
- Conduct regular user awareness training using realistic malware dropper phishing simulations to improve user recognition.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Diverse Threat Actors Exploit Critical WinRAR Vulnerability CVE-2025-8088	HIGH	CLEAR	Campaign	Open Source

Executive Summary

The Google Threat Intelligence Group has identified widespread exploitation of the critical WinRAR vulnerability CVE-2025-8088, affecting various organizations including those in the financial sector. This vulnerability allows attackers to establish initial access and deliver diverse payloads by exploiting a path traversal flaw that enables files to be dropped into the Windows Startup folder for persistence.

The significance of this vulnerability to the financial services sector lies in the potential for attackers to deploy malware and steal sensitive information from commercial targets. The ongoing exploitation by both government-backed and financially motivated threat actors highlights the urgent need for enhanced application security and user awareness to mitigate these risks.

Technical Details

- The Google Threat Intelligence Group has identified ongoing in-the-wild exploitation of WinRAR vulnerability CVE-2025-8088, rated critical.
- CVE-2025-8088 is a high-severity path traversal vulnerability in WinRAR, allowing attackers to exploit Alternate Data Streams (ADS).

- Attackers can craft malicious RAR archives that write files to arbitrary locations on the system when opened by a vulnerable version of WinRAR.
- The exploit often conceals malicious files within the ADS of a decoy file, misleading users into opening seemingly harmless documents.
- Malicious payloads are typically written to the Windows Startup folder, ensuring execution upon user login.
- The exploit utilizes directory traversal characters in conjunction with the ADS feature to achieve persistence.
- Government-backed actors have targeted military, government, and technology sectors using this vulnerability.
- Financially motivated actors have also leveraged this exploit to deploy commodity RATs and information stealers against commercial entities.

Recommendations

- Immediately apply patches for WinRAR to mitigate the risk associated with CVE-2025-8088.
- Educate employees on the dangers of opening unknown or suspicious files, especially RAR archives.
- Implement endpoint monitoring to detect unusual file behavior, particularly in the Windows Startup folder.
- Utilize advanced threat detection solutions to identify and respond to potential exploitation attempts.
- Regularly review and update security policies to address emerging threats and vulnerabilities.

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
Tycoon 2FA Campaign Targets Gmail and Microsoft 365 Users via Contractors Domains	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers have identified a campaign known as Tycoon 2FA that exploits domains ending in *.contractors to harvest credentials from Gmail and Microsoft 365 users. The campaign utilizes social engineering tactics to deceive users into providing their login information through fraudulent interfaces.

This campaign poses a significant threat to the financial services sector, as the compromised credentials can lead to unauthorized access to sensitive financial data and systems. The use of two-factor authentication (2FA) adds a layer of complexity, making it crucial for organizations to be vigilant against such targeted phishing attempts.

Technical Details

- The Tycoon 2FA campaign specifically targets users of Gmail and Microsoft 365 services.
- It employs social engineering techniques to lure victims into entering their credentials on fake login pages.
- The campaign leverages domains that end with *[.]contractors to create a sense of legitimacy.
- The fraudulent pages are designed to closely mimic the legitimate login interfaces of the targeted services.
- Observed behaviors of the phishing page include:
    - Accurate UI and branding replication
    - Email address prefilled or dynamically referenced.
    - Transition into multi-step authentication flows
    - MFA approval interception and credential capture
- Once credentials are harvested, attackers gain unauthorized access to user accounts.
- The campaign highlights the risks associated with 2FA, as attackers may attempt to bypass this security measure.

Recommendations

- Implement multi-factor authentication (MFA) beyond just 2FA to enhance security.
- Regularly monitor for suspicious login attempts and unusual account activity.
- Block known malicious domains and employ email filtering to reduce phishing attempts.
- Conduct regular security awareness training to keep staff informed about evolving threats.

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
Ongoing Campaign Exploits FreePBX Vulnerability to Deploy EncystPHP Web Shell	MEDIUM	CLEAR	Campaign	CSC

Executive Summary

FortiGuard Labs has identified an active attack campaign exploiting CVE-2025-64328, a high-severity command injection vulnerability in FreePBX Endpoint Manager versions 17.0.2.36 to 17.0.3. Threat actors are deploying the EncystPHP web shell, which allows for persistent remote access and full system compromise.

The implications for the financial services sector are significant, as organizations utilizing FreePBX systems may face unauthorized access, data exfiltration, and potential abuse of communication resources. The stealthy nature of the EncystPHP web shell complicates detection and remediation efforts, increasing the risk of long-term operational control by attackers.

Technical Details

- The attack exploits CVE-2025-64328 via the FreePBX administrative interface, allowing arbitrary command execution.
- EncystPHP is a sophisticated PHP-based web shell that enables persistent remote access and privilege escalation.
- The malware is delivered in Base64-encoded form and masquerades as legitimate FreePBX files to evade detection.
- Key capabilities include MD5-hash-based authentication and an interactive command execution interface.
- EncystPHP employs cron-based persistence, executing droppers at 1-3 minutes interval.
- It creates a root-level user (newfpbx) with UID/GID 0 for sustained access.
- The malware injects attacker controlled SSH public keys to maintain access via port 22.
- Multiple web shells are deployed across common FreePBX-accessible paths, with .htaccess rules redirecting traffic to malicious handlers.
- Anti-forensics techniques include log tampering and timestamp forgery to hinder detection.
- The attack patterns align with the threat actor group INJ3CTOR3, known for previous vulnerabilities.

Recommendations

- Patch immediately by upgrading FreePBX Endpoint Manager to a version that addresses CVE-2025-64328.
- Proactively review and hunt for known Indicators of Compromise (IOCs) associated with EncystPHP and INJ3CTOR3 activity.
- Monitor network traffic, system users, cron jobs, web directories, and FreePBX configuration files for signs of compromise.
- If a compromise is suspected, isolate affected systems, and perform a full system wipe, rebuilding from trusted backups.
- Implement robust security measures to detect and respond to unauthorized access attempts.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – EncystPHP Web Shell

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Threat Actors Exploit AWS WorkMail in Phishing Campaign	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Rapid7 has identified a phishing campaign where threat actors exploited compromised AWS credentials to deploy phishing infrastructure using AWS WorkMail. By bypassing traditional anti-abuse controls of AWS Simple Email Service (SES), attackers leveraged Amazon's infrastructure to send emails that appeared legitimate, complicating detection efforts for the organizations.

This incident is particularly concerning for financial services, as it highlights the potential for attackers to exploit cloud services to conduct phishing operations with minimal risk of detection. Organizations with exposed AWS credentials and inadequate monitoring are at heightened risk, emphasizing the need for robust security practices to safeguard sensitive information and maintain trust with clients.

Technical Details

- Initial access was gained through exposed long-term AWS access keys, with the use of the TruffleHog tool indicating credential validation.
- The attackers performed reconnaissance using AWS APIs, leading to the discovery of limited permissions and subsequent privilege escalation through compromised IAM users.
- They executed API calls to assess Amazon SES configurations, indicating early intent to abuse email-sending capabilities.
- The attackers created new IAM users with broader permissions and established a login profile for full AWS Management Console access.
- To circumvent SES restrictions, they pivoted to AWS WorkMail, creating multiple organizations and verifying domains for phishing operations.
- WorkMail allows immediate email sending to external recipients, bypassing SES's sandbox limitations.
- Emails sent via WorkMail may obscure the attacker's true IP address, complicating attribution and detection efforts.
- The attackers utilized both the WorkMail web interface and SMTP access for sending emails, with the latter generating no CloudTrail events.

Recommendations

- Implement AWS Organizations Service Control Policies (SCPs) to block the use of AWS WorkMail where not required.
- Enforce strict least-privilege IAM policies for WorkMail and SES administration to minimize potential abuse.
- Monitor and approve any changes to WorkMail and SES configurations to detect unauthorized activities.
- Conduct regular secret scanning and key rotation to reduce the risk of credential leakage.

- Educate staff on secure development practices to prevent exposure of AWS credentials.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Threat Actors Exploit AWS WorkMail

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
ShinyHunters Campaign Expands with Vishing and Credential Theft Targeting SaaS Platforms	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Mandiant has identified an increase in threat activity associated with ShinyHunters, utilizing voice phishing (vishing) and credential harvesting tactics to gain access to corporate environments. The campaign primarily targets cloud-based software-as-a-service (SaaS) applications, aiming to exfiltrate sensitive data and internal communications for extortion purposes.

The implications for the financial services sector are significant, as the threat actors are not exploiting security vulnerabilities but rather leveraging social engineering techniques. This underscores the critical need for organizations to adopt phishing-resistant multi-factor authentication methods to mitigate the risks associated with such campaigns.

Technical Details

- The campaign employs vishing tactics where threat actors impersonate IT staff to manipulate employees into providing SSO credentials and MFA codes.
- Credential harvesting sites are branded to resemble legitimate company portals, often using formats like {company name}sso[.]com or {company name}internal[.]com.
- Threat actors gain access to Okta customer accounts, exploiting identity providers and targeting SaaS platforms for data exfiltration.
- After initial access, the actors move laterally within the victim's environment to extract data from various SaaS applications.
- Specific searches are conducted for sensitive documents and personally identifiable information (PII) within cloud applications.
- The actors enable tools such as the ToogleBox Recall for the victim's Workspace account.
- Subsequent phishing emails has been observed to be sent to contacts at cryptocurrency firms using compromised accounts to further exploit the situation.

- Extortion activities are attributed to a separate cluster, UNC6240, which has been linked to ransom demands and threats of DDoS attacks against victims.
- A new data leak site associated with ShinyHunters lists alleged victims and provides contact information for negotiations.
- The campaign represents an evolution in tactics, expanding the range of targeted platforms and increasing the sophistication of extortion methods.

Recommendations

- Implement phishing-resistant multi-factor authentication methods, such as FIDO2 security keys, to reduce the risk of credential theft.
- Conduct regular security awareness training for employees to recognize and respond to vishing attempts and social engineering tactics.
- Monitor for unusual access patterns and lateral movement within corporate environments to detect potential intrusions early.
- Establish incident response protocols for handling data breaches and extortion attempts, including communication strategies with affected parties.
- Regularly review and update security measures for SaaS applications to ensure they are resilient against credential harvesting attacks.

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
Fake Clawdbot VS Code Extension Installs ScreenConnect RAT	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Aikido Security have identified a malicious VS Code extension named "ClawdBot Agent," which masquerades as a legitimate AI coding assistant while secretly deploying malware on Windows systems upon startup. The extension exploits the popularity of the Clawdbot brand, which has not officially released any VS Code extensions, allowing attackers to impersonate it effectively.

This incident is significant for the financial services sector as it highlights the growing trend of brand impersonation in malware campaigns. The use of trusted software like VS Code to deliver remote access tools can lead to severe security breaches, particularly in environments handling sensitive financial data. Organizations must remain vigilant against such threats that leverage trusted applications to bypass security measures.

Technical Details

- The extension activates automatically on VS Code startup, requiring no user interaction to execute.
- It fetches configuration data from a command-and-control (C2) server to download and run malicious payloads.
- The primary payload, Code.exe, is a weaponized version of the legitimate ScreenConnect software, allowing remote access to infected machines.
- The malware employs a redundant delivery mechanism via a Rust-based DLL, DWrite[.]dll, which can fetch payloads from alternative sources if the primary C2 fails.
- The attack leverages a technique known as "Bring Your Own ScreenConnect," utilizing trusted IT support tools for malicious purposes.
- The malicious extension is designed to evade detection by using legitimate software signatures and disguising its activities.
- The attackers have implemented multiple fallback mechanisms to ensure payload delivery, including hardcoded URLs and batch scripts.
- The infrastructure behind the attack includes domains hosted offshore, complicating attribution and takedown efforts.
- The malware can establish remote access sessions with the attacker's infrastructure, posing a significant risk to organizational security.
- The attackers have built in anti-analysis techniques to hinder detection by security tools.

Recommendations

- Immediately uninstall the "ClawdBot Agent" extension from VS Code if installed.
- Check for and remove any ScreenConnect installations from the system.
- Monitor for any unexpected processes related to Code[.]exe or ScreenConnect in the Task Manager.
- Block the identified malicious domains and IP addresses at the firewall level.

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-Aligned Threat Groups Utilize PeckBirdy Framework for Targeted Attacks	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Trend Micro have identified PeckBirdy, a sophisticated JScript-based command-and-control (C&C) framework employed by China-aligned APT groups since 2023. This framework is designed to exploit

living off the land binaries (LOLBins) across various environments, allowing attackers to deliver advanced backdoors to targeted sectors. The framework is linked to multiple campaigns, notably SHADOW-VOID-044 and SHADOW-EARTH-045, which demonstrate its versatility and effectiveness in executing attacks.

The significance of PeckBirdy to the financial services sector lies in its ability to exploit vulnerabilities in widely used systems, potentially impacting organizations involved in online transactions and sensitive data management. The framework's use of malicious scripts to inject backdoors into legitimate websites poses a serious threat, as it can lead to credential harvesting and unauthorized access to critical systems, making it essential for financial institutions to remain vigilant against such sophisticated threats.

Technical Details

- PeckBirdy is a JScript-based C&C framework that has been active since 2023, allowing for flexible deployment across multiple environments.
- The framework includes two modular backdoors, HOLODONUT and MKDOOR, enhancing its attack capabilities beyond its core functions.
- The SHADOW-VOID-044 campaign injects malicious scripts that, upon user interaction, download and deploy the PeckBirdy framework.
- The SHADOW-EARTH-045 campaign focuses on Asian government entities, using script injections to harvest credentials from government websites.
- PeckBirdy can operate in various environments, including browsers, MSHTA, WScript, Classic ASP, Node JS, and .NET.
- The framework utilizes APIs to download landing scripts, which are tailored based on the execution environment.
- During execution, PeckBirdy generates a victim ID based on the environment, which can include hardware information or a random string.
- The framework employs a combination of JScript and ECMAScript 5 functions to ensure compatibility across different execution contexts.
- PeckBirdy maintains persistence through various communication protocols and can execute multiple actions depending on the environment.
- The framework's design allows it to serve as a watering-hole control server and a reverse shell server during different phases of an attack.

Recommendations

- Implement robust web application firewalls to detect and block malicious script injections on websites.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by frameworks like PeckBirdy.
- Conduct thorough security assessments of online platforms, particularly those handling sensitive financial transactions.
- Educate employees on recognizing phishing attempts and the risks associated with downloading software from untrusted sources.

- Monitor network traffic for unusual patterns that may indicate the presence of malicious scripts or unauthorized access 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
HoneyMyte APT Group Enhances CoolClient Backdoor with New Stealers and Features	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified that the HoneyMyte APT group has updated its CoolClient backdoor, deploying multiple variants of browser login data stealers and various scripts for data theft. The updated CoolClient has been observed in campaigns targeting government entities across Southeast Asia and Europe. This malware utilizes sophisticated techniques including DLL sideloading and new functionalities such as clipboard monitoring and HTTP proxy credential sniffing.

The implications for the financial services sector are significant, as the capabilities of this malware extend beyond traditional espionage, focusing on active surveillance and data exfiltration. Financial institutions should be aware of the potential for targeted attacks utilizing these advanced tools, which can compromise sensitive data and lead to severe reputational and financial damage.

Technical Details

- CoolClient backdoor has been enhanced with new features including clipboard monitoring and HTTP proxy credential sniffing.
- The malware employs DLL sideloading to execute malicious code using legitimate signed executables.
- It collects detailed system information, including user credentials, network details, and installed software.
- New variants of browser login data stealers target Chrome and Microsoft Edge, capable of exfiltrating saved credentials.
- The malware uses a command and control (C2) infrastructure that supports both TCP and UDP communication.
- It includes plugins for remote shell access, file management, and service management, expanding its operational capabilities.
- The malware can perform keylogging, file uploads, and process injection, enhancing its stealth and persistence.
- HoneyMyte's campaigns have been observed in multiple countries, indicating a broad operational scope.

- The malware utilizes public file-sharing services for data exfiltration, complicating detection and response efforts.
- HoneyMyte has a history of targeting government entities, raising concerns about similar tactics being employed against financial institutions.

Recommendations

- Implement strict access controls and monitor for unauthorized use of signed executables.
- Utilize endpoint detection and response (EDR) solutions to identify and mitigate suspicious activities.
- Conduct regular security awareness training for employees to recognize phishing attempts and suspicious downloads.
- Ensure robust logging and monitoring of network traffic to detect potential data exfiltration attempts.
- Regularly update and patch systems to defend against known vulnerabilities that could be exploited by such malware.

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 Authentication Bypass Vulnerability in Fortinet Products Actively Exploited	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Fortinet has disclosed a critical authentication bypass vulnerability affecting multiple products when FortiCloud Single Sign-On (SSO) is enabled. This vulnerability allows attackers with any FortiCloud account to authenticate as administrators on other devices registered to different accounts, leading to unauthorized access and potential data exfiltration.

The vulnerability, identified as CVE-2026-24858, is significant for the financial services sector as it enables full administrative compromise of affected devices. With the potential for threat actors to gain persistent access and exfiltrate sensitive configuration data, immediate action is required to mitigate risks associated with this vulnerability.

Technical Details

- The vulnerability allows an attacker with a FortiCloud account with a registered device to authenticate as an administrator on other Fortinet devices registered to different FortiCloud accounts.
- It stems from improper access control in FortiCloud SSO authentication paths (CWE-288).
- Active exploitation has been observed, enabling unauthorized administrative access.

- Attackers can exfiltrate configuration data and establish persistent access through local admin accounts.
- Malicious local admin account names include 'audit', 'backup', 'remoteadmin' and others.
- The vulnerability has a CVSS v3 score of 9.4, indicating a critical severity level.
- Fortinet has temporarily disabled FortiCloud SSO on the backend and re-enabled it only for patched device versions.
- Affected products include FortiAnalyzer, FortiManager, FortiOS, FortiProxy
- Ongoing investigations include FortiWeb and FortiSwitch Manager for potential vulnerabilities.

Recommendations

- Upgrade all affected Fortinet products immediately to the specified fixed versions.
- Conduct an audit of all administrative accounts for unauthorized or suspicious entries.
- Review authentication logs for any unusual FortiCloud SSO login activity.
- Rotate credentials for all administrative users to enhance security.
- Implement monitoring for new admin account creations and FortiCloud SSO login events.

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

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Zero-Day Vulnerability in Microsoft Office Actively Exploited	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Microsoft has released emergency out-of-band security updates to address a high-severity security feature bypass vulnerability, CVE-2026-21509, in Microsoft Office that is currently being exploited. This vulnerability allows attackers to bypass OLE mitigations designed to protect users from unsafe COM and OLE controls in malicious documents, requiring user interaction to exploit.

This incident is particularly significant for the Financial Services sector, as the exploitation of this vulnerability could lead to severe impacts on confidentiality, integrity, and availability of sensitive financial data. Organizations must prioritize patching affected Microsoft Office versions to mitigate risks associated with this actively exploited flaw.

Technical Details

- CVE-2026-21509 is a high-severity security feature bypass vulnerability in Microsoft Office with CVSS score of 7.8.
- The vulnerability is actively exploited in the wild.

- The vulnerability allows attackers to bypass OLE mitigations, exposing users to unsafe COM and OLE controls.
- Exploitation requires user interaction, specifically opening a crafted malicious Office document.
- The attack complexity is low, making it easier for attackers to exploit the vulnerability.
- Affected products include Microsoft Office 2016, 2019, LTSC 2021, LTSC 2024, and Microsoft 365 Apps for Enterprise.
- The flaw highlights ongoing risks from legacy COM/OLE components and social engineering tactics.

Recommendations

- Immediately apply Microsoft security updates for all affected Office versions.
- Restart Office applications to activate service-side protections.
- For systems unable to patch promptly, implement the interim registry-based workaround.
- Educate users about the risks of opening unsolicited Office documents.
- Regularly review and update security policies regarding the handling of Office files.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerabilities in Ivanti Endpoint Manager Mobile Allow Remote Code Execution	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Ivanti has released urgent security updates addressing two critical vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) that are being actively exploited. These vulnerabilities allow unauthenticated remote attackers to execute arbitrary code on affected systems, posing a significant risk to organizations using the product.

The financial services sector should prioritize these updates due to the potential for unauthorized access and control over sensitive data. The exploitation of these vulnerabilities could lead to severe operational disruptions and data breaches, making immediate mitigation essential for affected entities.

Technical Details

- Ivanti has confirmed that a limited number of customers were actively exploited at the time of disclosure, significantly increasing the risk profile.
- CVE-2026-1281 is a code injection vulnerability allowing unauthenticated remote code execution (RCE) with a CVSS score of 9.8 (Critical).
- CVE-2026-1340 is another code injection vulnerability allowing unauthenticated RCE, also with a CVSS score of 9.8 (Critical).

- Both vulnerabilities share the same CWE designation: CWE-94 (Improper Control of Code Generation).
- Affected versions include Ivanti Endpoint Manager Mobile (EPMM) 12.5.0.x and earlier, 12.6.0.x and earlier, 12.7.0.x and earlier, 12.5.1.0 and earlier, and 12.6.1.0 and earlier.
- The vulnerabilities allow attackers to gain significant control over the affected systems, which could lead to further exploitation.

Recommendations

- Identify EPMM version and apply the appropriate RPM patch immediately.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Authentication Bypass Vulnerability in GNU Inetutils telnetd Actively Exploited	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical authentication bypass vulnerability has been disclosed in the GNU Inetutils telnetd daemon, allowing remote attackers to gain unauthorized access without valid credentials. This vulnerability is actively exploited in the wild, posing a significant risk to systems utilizing the affected software.

This vulnerability is concerning to the financial services sector, as it enables unauthorized access to systems, potentially leading to data breaches and operational disruptions. The nature of the vulnerability highlights the importance of securing remote access protocols to prevent exploitation by malicious actors.

Technical Details

- A critical authentication bypass vulnerability, tracked as CVE-2026-24061, affects the telnetd daemon in GNU Inetutils (versions from 1.9.3 through 2.7).
- This flaw allows unauthenticated remote attackers to bypass login authentication and gain root-level access by injecting the "-f root" flag via the USER environment variable during Telnet session negotiation.
- The vulnerability has been assigned a CVSS v3.1 score of 9.8 (Critical), indicating its severity.
- The vulnerability enables direct remote code execution as root with no credentials required.
- The root cause is improper sanitization of user-controlled environment variables during the Telnet authentication process.
- Specifically, telnetd improperly processes the USER environment variable, allowing attackers to inject arguments.
- The vulnerability is categorized under CWE-88 – Improper Neutralization of Argument Delimiters in a Command (Argument Injection).

Recommendations

- Apply vendor patches or updated packages as soon as they become available.
- If no patch is available, remove GNU InetUtils telnetd entirely.
- Replace Telnet with SSH or other encrypted remote-access protocols.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerability in OpenSSL Enables Remote Code Execution	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

The OpenSSL Project has released a security update addressing multiple vulnerabilities across supported OpenSSL versions. The most severe issue, CVE-2025-15467, is a high-severity, pre-authentication stack buffer overflow that may allow remote code execution or denial of service. This vulnerability can be exploited without valid credentials, putting internet-facing systems at significant risk.

The financial services sector, which relies on OpenSSL for secure communications and cryptographic services, must prioritize immediate upgrades to mitigate potential exploitation. Failure to address these vulnerabilities could lead to severe operational disruptions and compromise sensitive data.

Technical Details

- CVE-2025-15467 is a high-severity stack buffer overflow that may lead to remote code execution or denial of service.
- The vulnerability can be triggered without valid credentials, increasing the risk for internet-facing systems.
- Additional vulnerabilities include a moderate severity flaw in PKCS#12 MAC verification (CVE-2025-11187).
- Low-severity vulnerabilities(CVE-2025-15469, CVE-2025-66199, CVE-2025-15468) include data truncation in openssl dgst and TLS 1.3 memory exhaustion.
- Affected OpenSSL versions include 3.6.x, 3.5.x, 3.4.x, 3.3.x, 3.0.x, and legacy versions 1.1.1 and 1.0.2.
- The patched versions include OpenSSL 3.6.1, 3.5.5, 3.4.4, 3.3.6, and 3.0.19.
- Organizations using OpenSSL for TLS, certificate handling, or cryptographic services must act swiftly.

Recommendations

- Upgrade OpenSSL immediately on all affected systems.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities in n8n Workflow Automation Platform Enable Remote Code Execution	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Multiple vulnerabilities have been identified in the n8n workflow automation platform that may lead to sandbox bypass and remote code execution on affected systems. Successful exploitation could allow full compromise of an n8n instance and exposure of sensitive enterprise data, credentials, and connected services.

The presence of these vulnerabilities is particularly concerning for financial services organizations that utilize automation platforms, as it could lead to unauthorized access to sensitive data and critical operational disruptions. Ensuring that these vulnerabilities are addressed is essential to maintaining the integrity and security of financial operations.

Technical Details

- Multiple vulnerabilities in the n8n workflow automation platform could allow authenticated attackers to bypass sandbox protections and achieve remote code execution (RCE).
- Successful exploitation may lead to full compromise of an n8n instance, exposing sensitive enterprise data, credentials, and connected services.
- CVE-2026-1470 has a CVSS Score of 9.9 (Critical) and allows authenticated users to execute arbitrary code with the privileges of the n8n process.
- Exploitation of CVE-2026-1470 may result in unauthorized access to sensitive data, workflow manipulation, and execution of system-level operations.
- CVE-2026-0863 has a CVSS Score of 8.5 (High) and enables authenticated users to bypass restrictions using string formatting and exception handling.
- In internal execution mode, CVE-2026-0863 allows for full n8n instance takeover and operating system-level code execution.
- In external execution mode, code execution is confined to a Sidecar container, which reduces the impact.
- All deployments running vulnerable versions of the n8n workflow automation platform are affected.
- Fixed versions include 1.123.17, 2.4.5, and 2.5.1 or later.

Recommendations

- Update the n8n workflow automation platform to fixed or latest versions to mitigate these vulnerabilities.

Detailed Vulnerability Details and Affected Products can be found here: *Source1* and *Source2*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Mozilla Releases Security Updates Addressing Multiple Vulnerabilities in Firefox and Thunderbird	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Multiple vulnerabilities have been identified in the n8n workflow automation platform that may lead to sandbox bypass and remote code execution on affected systems. Successful exploitation could allow full compromise of an n8n instance and exposure of sensitive enterprise data, credentials, and connected services.

The presence of these vulnerabilities is particularly concerning for financial services organizations that utilize automation platforms, as it could lead to unauthorized access to sensitive data and critical operational disruptions. Ensuring that these vulnerabilities are addressed is essential to maintaining the integrity and security of financial operations.

Technical Details

- CVE-2026-24869 is a high-severity use-after-free vulnerability in the Layout: Scrolling and Overflow component, potentially leading to arbitrary code execution or application crashes.
- CVE-2026-24868 is a moderate-severity mitigation bypass in the Privacy: Anti-Tracking component, which may allow tracking protections to be circumvented.
- CVE-2026-0818 is a moderate-severity CSS-based exfiltration vulnerability that allows partial disclosure of content from partially encrypted emails when remote content is enabled.
- The vulnerabilities affect both Firefox and Thunderbird, which are widely used applications.
- Attackers could exploit these vulnerabilities under certain conditions, emphasizing the need for timely updates.
- The vulnerabilities could have significant implications for user data security and privacy.

Recommendations

- Apply the latest updates released by Mozilla for Firefox and Thunderbird.

Detailed Vulnerability Details and Affected Products can be found here: *Source1*, *Source2*, and *Source3*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Sandbox Escape Vulnerability in vm2 Allows Arbitrary Code Execution	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

A critical security vulnerability has been identified in vm2, a widely used Node.js sandbox library, which allows attackers to bypass sandbox restrictions and execute arbitrary code on the host system. This vulnerability, tracked as CVE-2026-22709, has a CVSS score of 9.8, indicating its severity and potential impact on systems utilizing this library.

The financial services sector, which often relies on secure execution environments for untrusted code, must be vigilant regarding this vulnerability. Successful exploitation could lead to unauthorized access to sensitive data and compromise of system integrity, posing significant risks to organizations that utilize vm2 in their applications.

Technical Details

- The vulnerability is tracked as CVE-2026-22709 and has a CVSS score of 9.8, categorizing it as critical.
- It arises from incomplete sanitization of JavaScript Promise callbacks within the vm2 sandbox environment.
- Local Promise callbacks are sanitized, but global Promise object callbacks are not, leading to potential exploitation.
- An attacker can leverage this flaw through an async function to access unsanitized Promise methods.
- This access allows traversal of the prototype chain and execution of arbitrary code outside the sandbox.
- Successful exploitation can lead to a full sandbox escape, enabling remote code execution.
- Attackers could execute arbitrary system commands with the privileges of the host application.
- Compromised systems may allow access to sensitive data and facilitate lateral movement within the environment.

Recommendations

- Update to vm2 to latest or fixed version to mitigate the vulnerability.
- Conduct a thorough review of all applications utilizing the vm2 library to assess exposure.
- Implement monitoring for unusual activity that may indicate exploitation attempts.
- Educate development teams on secure coding practices to prevent similar vulnerabilities.
- Regularly review and update dependencies to ensure all components are secure.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Crunchbase Confirms Data Breach Exposing Over 2 million Records	MEDIUM	CLEAR	Cyber Breach	Open Source

Executive Summary

Crunchbase, a market intelligence firm, has confirmed a data breach after hackers from the ShinyHunters group published files allegedly stolen from its systems. The breach reportedly involves over 2 million records containing personal information, with the hackers making more than 400 MB of compressed files available for download after a ransom demand was refused.

The incident is significant for the financial services sector as it highlights the ongoing threat posed by cybercriminal groups targeting sensitive data. The exposure of personal information can lead to identity theft and fraud, impacting both individuals and organizations within the financial ecosystem.

Technical Details

- The ShinyHunters group claims to have stolen more than 2 million records from Crunchbase's systems.
- The hackers published over 400 MB of compressed files for download on their website.
- Crunchbase detected the cybersecurity incident and confirmed the exfiltration of certain documents.
- The company stated that no business operations were disrupted because of the breach.
- Crunchbase has contained the incident and secured its systems.
- The data breach raises concerns about the protection of personal information in the financial services sector.
- The incident underscores the risks associated with ransom demands and the potential for public data exposure.
- The breach reflects the increasing sophistication of cybercriminal groups like ShinyHunters.

Recommendations

- Implement robust data protection measures to safeguard sensitive information.
- Regularly conduct security assessments and penetration testing to identify vulnerabilities.
- Educate employees on recognizing phishing attempts and other social engineering tactics.
- Establish an incident response plan to quickly address potential data breaches.
- Monitor for unusual activity and potential data leaks on the dark web.

Reference to the Source

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Ongoing Campaign Exploits FreePBX Vulnerability to Deploy EncystPHP Web Shell

Tactic	Technique
Initial Access	Exploit Public-Facing Application: T1190
Execution	Command and Scripting Interpreter: Unix Shell: T1059.004
Persistence	Scheduled: Task/Job: Cron: T1053.003
Persistence	Server Software Component: Web Shell: T1505.003
Privilege Escalation	Exploitation for Privilege Escalation: T1068
Privilege Escalation	Create Account: Local Account: T1136.001
Credential Access	OS Credential Dumping: T1003
Defense Evasion	Indicator Removal on Host: File Deletion: T1070.004
Defense Evasion	File and Directory Permissions Modification: Linux: T1222.002
Defense Evasion	Masquerading: Match Legitimate Name or Location: T1036.005
Defense Evasion	Impair Defenses: Disable or Modify: Tools: T1562.001
Lateral Movement	Remote Services: SSH: T1021.004
Command and Control	Ingress: Tool: Transfer: T1105
Command and Control	Application Layer Protocol: Web Protocols: T1071.001
Impact	Resource Hijacking: T1496

Threat Actors Exploit AWS WorkMail in a Phishing Campaign

Tactic	Technique
Initial Access	Valid Accounts: Cloud Accounts (T1078.004)
Persistence	Create Account: Cloud Account (T1136.003)
Privilege Escalation	Account Manipulation: Additional Cloud Roles (T1098.003)
Discovery	Cloud Infrastructure Discovery (T1580)
Impact	Resource Hijacking: Cloud Service Hijacking (T1496.004)

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
2FA	Two-Factor Authentication; targeted by phishing flows that attempt to intercept approvals/codes.
Account takeover	Unauthorized access to user accounts after credential theft, enabling broader access to systems and data.
Advanced link protection	Email security feature recommended to block malicious redirect chains used in phishing.
Aikido Security	The organization cited as identifying the malicious VS Code extension ("ClawdBot Agent").
Amazon SES	Email sending service referenced for anti-abuse controls that attackers attempted to bypass.
Anti-analysis	Malware behaviours designed to hinder investigation or automated detection.
APT	Advanced Persistent Threat; used for sophisticated, often state-linked groups conducting targeted attacks.
Attribution	Determining who is behind an attack; described as complicated by infrastructure choices.
Authentication bypass	Weakness allowing access without proper verification (Fortinet and telnetd cases).
AWS	Cloud platform referenced as being abused to build and send phishing infrastructure.
AWS API	Interface used by attackers for reconnaissance and configuration discovery.
AWS Management Console	Web administration portal for AWS; referenced as accessed by attackers after escalation.
AWS WorkMail	AWS email service abused to send phishing emails while bypassing certain SES controls.
Bring Your Own ScreenConnect	Technique described where attackers misuse trusted IT tools for malicious remote access.
Browser credential theft	Stealing saved credentials from browsers (Chrome/Edge/Firefox) as described in multiple entries.
China-aligned threat groups	State-linked groups described as using PeckBirdy for targeted attacks since 2023.
Click-through rate	The likelihood that recipients will click a link; attackers improve this by mimicking real tender directories.
CloudTrail	AWS activity logging service; referenced as not capturing certain SMTP actions.
COM	Component model referenced alongside OLE controls as part of the Office security bypass context.
Command-and-Control (C2/C&C)	Attacker infrastructure used to control compromised systems and deliver instructions/payloads.
CPX-TIC	CPX Threat Intelligence Centre
Credential theft / harvesting	Stealing usernames/passwords (and sometimes MFA approvals) via fake pages, calls, or deception.

Cron	Linux/Unix scheduler abused for persistence (e.g., running droppers every 1–3 minutes).
Crunchbase	Organization referenced as confirming a breach with over 2 million records and published files.
CSC	UAE Cyber Security Council
CVE	Common Vulnerabilities and Exposures identifier used to track specific vulnerabilities.
CVSS	Common Vulnerability Scoring System; indicates severity and helps prioritize remediation.
CWE	Common Weakness Enumeration; classification system for software weakness types.
Data breach	Confirmed exposure of records/documents due to unauthorized access (Crunchbase case).
Data exfiltration	Unauthorized removal of data from systems; referenced across campaigns and breach reporting.
Data leak site	Attacker site referenced as listing victims and providing contact details for negotiations.
DKIM	Email signature mechanism recommended to help verify message authenticity and integrity.
DLL	Windows library format used as part of the malware delivery mechanism (e.g., DWrite.dll).
DMARC	Email authentication control recommended to reduce spoofing and increase confidence in sender legitimacy.
DoS	Denial of Service; disruption of system availability referenced as a potential outcome of the OpenSSL flaw.
Dropper	Initial malware stage that installs or fetches additional malware (e.g., RATs/stealers).
EDR	Endpoint Detection and Response; security tooling recommended to detect suspicious endpoint behaviour.
EncystPHP	PHP-based web shell described as enabling persistent access, privilege escalation, and anti-forensics.
Extortion	Pressure tactic involving ransom demands and/or threats (e.g., data leak site, DDoS threats).
Fallback mechanism	Redundant delivery approach (hardcoded URLs/scripts) to ensure malware delivery if one path fails.
FIDO2	A phishing-resistant authentication approach explicitly recommended.
Financially motivated actors	Criminal threat actors described as exploiting WinRAR to deploy commodity RATs and stealers for commercial gain.
Firefox	Mozilla browser referenced as receiving security updates addressing multiple vulnerabilities.
FortiAnalyzer	Fortinet product listed as affected by the FortiCloud SSO authentication bypass.
FortiCloud SSO	Cloud single sign-on feature referenced as the affected authentication path in the Fortinet issue.
FortiGuard Labs	The research team cited as identifying the FreePBX exploitation campaign and EncystPHP deployment.
FortiManager	Fortinet product listed as affected by the FortiCloud SSO authentication bypass.
Fortinet	Vendor referenced as disclosing a critical FortiCloud SSO authentication bypass under active exploitation.
FortiOS	Fortinet product listed as affected by the FortiCloud SSO authentication bypass.
FortiProxy	Fortinet product listed as affected by the FortiCloud SSO authentication bypass.
FortiSwitch Manager	Fortinet product mentioned as under investigation for potential related issues.
FortiWeb	Fortinet product mentioned as under investigation for potential related issues.
GNU Inetutils telnetd	Telnet daemon referenced as vulnerable to an authentication bypass enabling root-level access.
Google Threat Intelligence Group	The group cited as identifying in-the-wild exploitation of the WinRAR vulnerability.
Government-backed actors	Threat actors described as leveraging WinRAR exploitation to target multiple sectors.

HOLODONUT	A modular backdoor referenced as part of the PeckBirdy framework toolkit.
HoneyMyte	An APT group described as enhancing the CoolClient backdoor with new stealers and features.
IAM	Cloud identity/permissions system; attackers escalated access via compromised IAM users.
Indicators of Compromise (IOCs)	Artifacts (domains, files, behaviors) recommended for proactive hunting/detection.
INJ3CTOR3	Threat actor group referenced in relation to the FreePBX campaign patterns and prior vulnerability exploitation.
Ivanti EPMM	Ivanti Endpoint Manager Mobile; referenced as having two critical vulnerabilities under active exploitation.
JavaScript dropper	Script-based dropper used to initiate execution and fetch additional payloads.
Key rotation	Recommended practice to regularly change keys/credentials to limit impact of exposure.
Lateral movement	Expansion from one compromised account/system to others after initial access.
Least privilege	Security principle recommended to minimize permissions and reduce blast radius if accounts are compromised.
Log tampering / Timestamp forgery	Anti-forensics methods used to obscure attacker actions and delay detection.
Login profile	Configuration enabling console login access; created by attackers for AWS Management Console access.
LOLBIN	Living off the land binaries; legitimate tools abused to support malicious activity.
Malicious extension ("ClawdBot Agent")	A fake extension that impersonates an AI coding assistant and deploys malware automatically.
Mandiant	The organization cited as reporting expanded ShinyHunters activity using vishing and SaaS credential theft.
MFA	Multi-Factor Authentication; recommended to reduce the impact of stolen passwords.
Microsoft 365	Cloud productivity platform referenced as a phishing target and part of the affected Office ecosystem.
Mitigation bypass	Circumventing protective controls (referenced in Firefox anti-tracking and Office OLE protections).
MKDOOR	A modular backdoor referenced as part of the PeckBirdy framework toolkit.
n8n	Workflow automation platform referenced as vulnerable to sandbox bypass and RCE.
Node.js	Platform referenced as part of vm2 usage and PeckBirdy execution environment coverage.
Offshore hosting	Infrastructure placement referenced as complicating attribution and takedown efforts.
Okta	Identity platform referenced as being targeted via compromised customer accounts for access to SaaS environments.
OLE	Office technology referenced in the security bypass vulnerability (mitigation bypass for unsafe controls).
OpenSSL	Cryptographic library referenced as having a high-severity flaw that may enable RCE/DoS.
Out-of-band update	Emergency security update released outside routine cycles (Microsoft Office case).
Passkeys	A phishing-resistant login method explicitly recommended to reduce credential-theft risk.
Payload	The malware delivered to achieve attacker goals (remote control, theft, persistence).
PeckBirdy	JScript-based command-and-control framework used across multiple campaigns for targeted access.
Persistence	Techniques used to maintain access (Startup folder, scheduled task, cron jobs, user creation, SSH keys).
Phishing	Deceptive messages designed to trick users into clicking malicious links or revealing credentials.
Phishing-resistant MFA	MFA methods (e.g., FIDO2/passkeys) recommended to prevent reuse of stolen credentials and approvals.

PII	Personally Identifiable Information, sensitive personal data referenced as a target for searches and exfiltration.
Privilege escalation	Gaining higher permissions (e.g., root/admin) after initial access, enabling full compromise.
Procurement	Business purchasing process used as a theme to make phishing emails look legitimate.
Ransom demand	Payment demand referenced in the Crunchbase breach scenario prior to public file release.
Rapid7	The organization cited as identifying AWS WorkMail abuse for phishing infrastructure.
RAT	Remote Access Trojan/Tool; mentioned as a common payload type delivered after exploitation.
RCE	Remote Code Execution: ability for attackers to run code on a target system remotely.
Reconnaissance	Attacker discovery actions to understand permissions, services, and pathways for escalation.
Redirect chain	Multiple hops used to route victims to malicious downloads while evading detection.
Redline Stealer	Information-stealing malware family referenced as associated with the dropper campaign.
Registry workaround	Interim mitigation mentioned for Office where patching cannot be completed immediately.
Remcos	Malware family referenced as associated with the malicious JavaScript dropper campaign.
Remote access tool / Remote control	Tools enabling attackers to operate systems remotely, often leading to data theft and lateral movement.
Reverse shell	Remote command channel referenced as a possible role served by the PeckBirdy design.
Root-level access	Highest privilege level on Unix/Linux systems; mentioned as achievable in the telnetd issue.
Rust-based DLL	Delivery component referenced as a redundant/fallback mechanism for payload retrieval.
SaaS	Cloud-delivered business applications targeted for data exfiltration and extortion.
Sandbox	Restricted execution environment intended to contain untrusted code; multiple entries discuss bypass/escape.
Sandbox detonation	Security approach recommended for safely opening/detonating suspicious links/files to observe malicious behaviour.
Scheduled task	Windows feature abused to run malware frequently and maintain persistence.
SCP (Service Control Policy)	AWS Organizations control recommended to block/limit WorkMail usage if not required.
ScreenConnect	Legitimate remote support tool referenced as weaponized for unauthorized remote control.
Secret scanning	Recommended practice to detect exposed long-term access keys and other secrets.
Secure web gateway	Web control recommended to restrict access to suspicious/newly registered domains used in campaigns.
SHADOW-EARTH-045	Campaign name referenced as linked to PeckBirdy framework usage.
SHADOW-VOID-044	Campaign name referenced as linked to PeckBirdy framework usage.
ShinyHunters	A threat actor group referenced in both SaaS/vishing activity and the Crunchbase breach with data publication.
Sidecar container	Isolated component referenced in n8n external execution mode that can reduce impact.
Signed-binary abuse	Evasion approach where attackers leverage trusted/signed executables to reduce detection.
SMTP	Email protocol: noted because SMTP sending may generate no CloudTrail events in this scenario.
Social engineering	Manipulation of people (not systems) to gain access, approvals, or sensitive information.

SPF	Email sender authorization control recommended to reduce fraudulent sending from look-alike domains.
SSH keys	Attacker-added keys used to maintain remote access via SSH (port 22 referenced).
SSO	Single Sign-On; a central login method targeted in vishing to unlock broad SaaS access.
Telnet	Legacy remote access protocol referenced as high risk; replacement with SSH is recommended.
Tender/RFP lures	Business-themed bait (procurement/tender invitations) used to trick recipients into opening malicious content.
Thunderbird	Mozilla email client referenced as receiving security updates addressing multiple vulnerabilities.
TLS	Transport Layer Security; referenced as part of OpenSSL's role in protecting communications.
Trend Micro	The organization cited as reporting the PeckBirdy framework used by China-aligned groups.
Tycoon 2FA	Named phishing campaign targeting Gmail and Microsoft 365 users to harvest credentials through fake login flows.
UNC6240	A cluster linked to extortion activity, ransom demands, and DDoS threats.
Use-after-free	Vulnerability class referenced in Firefox updates that may enable arbitrary code execution.
Vishing	Voice-based phishing where attackers impersonate IT staff to obtain SSO credentials and MFA codes.
vm2	Node.js sandbox library referenced as vulnerable to a critical sandbox escape.
VS Code	Developer tool targeted via a malicious extension that executes on startup.
Watering-hole	Attack approach where legitimate sites are injected with malicious scripts to infect visitors.
Web shell	Server-side backdoor script that provides persistent remote access (e.g., EncystPHP).
Windows Startup folder	Windows location abused to auto-run malicious files at user login (persistence).
Zero-day	A vulnerability being exploited before typical patching cycles; referenced for Microsoft Office active exploitation.