TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	18/6/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 18 June 2026

9	8	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 UAE & Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights social engineering, trusted-platform abuse, and rapid exploitation of new vulnerabilities. Campaigns used phishing sites, AI-themed lures, fake logins, malicious VS Code extensions, ClickFix prompts, and MaaS tools to steal credentials, hijack sessions, and deploy malware. It also tracked critical flaws affecting Chrome, PAN-OS, Remote Access VPN, Oracle PeopleSoft, Apache ActiveMQ, Linux 'nf_tables', VMware Cloud Foundation Operations, and Microsoft's June 2026 updates. From a financial sector perspective, these issues may affect remote access, browser-based authentication, developer environments, Windows and Linux endpoints, and critical management platforms. The risk includes unauthorized VPN access, credential theft, session abuse, remote code execution, privilege escalation, and operational disruption especially where systems are internet-facing or high-trust workflows lack strong controls. Priority actions include faster patching, reducing exposed legacy services, improving VPN and endpoint monitoring, and strengthening awareness of phishing, ClickFix prompts, AI-themed lures, and untrusted software or extensions.

ADGM THREAT INTELLIGENCE SUMMARY

NFCShare Expands Through Phishing Pages and GitHub-Hosted Android APKs [Campaign] [High]

UNK_DeadDrop Developer Phishing Campaign Targets Cryptocurrency Ecosystem [Campaign] [High]

MENA-Focused Social Engineering and Monetization Through SniperDz PhaaS [Campaign] [High]

Sophisticated Browser-in-the-Browser (BitB) Phishing Campaign Targets OAuth Credentials [Campaign] [High]

DPRK-Linked Malicious VS Code Extension Deploys Covert Multi-Stage Backdoor [Campaign] [Medium]

MLTBackdoor Delivered Through a Multi-Stage ClickFix Campaign [Campaign] [Medium]

SilabRAT MaaS Enables Covert Browser Session Abuse and Financially Motivated Theft [Campaign] [Medium]

Golang-Based BLUERABBIT Malware with Encryption, Remote Access and Wiping Features [Campaign] [Medium]

AI Themed Lures Deliver AsyncRAT Through Multi-Stage Malware Chains [Campaign] [Medium]

ShinyHunters Campaign Leveraging Oracle PeopleSoft Weaknesses [Vulnerability] [High]

China-Nexus SLIME88 Leveraging ActiveMQ Remote Code Execution Chains [Vulnerability] [High]

Google Chrome Zero-Day Patched in Stable Channel Update [Vulnerability] [High]

Authentication Bypass in Remote Access VPN Under Active Exploitation [Vulnerability] [High]

PAN-OS Authentication Bypass Actively Exploited Against GlobalProtect [Vulnerability] [High]

Microsoft June 2026 Updates Address Zero-Days, Defender Exploitation, and Broad RCE Exposure [Vulnerability] [High]

Linux Kernel nf_tables Flaw Allows Local Root Escalation [Vulnerability] [High]

Flaws in VMware Cloud Foundation Operations Could Enable Unauthorized Admin Actions [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
NFCShare Expands Through Phishing Pages and GitHub-Hosted Android APKs	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an updated NFCShare campaign targeting users through bank-themed mobile phishing pages and malicious Android application packages. The attack begins with a spoofed banking portal that captures login details, then pushes the victim to install a fake app update, which uses a card-verification screen to prompt the user to tap a payment card to the phone, capture card data over NFC (Near-Field Communication), collect a PIN, and send the information to attacker-controlled infrastructure.

The campaign could affect organizations with exposure to mobile banking workflows because it combines credential theft, fraudulent application updates, and payment-card data capture into a single social-engineering chain. The newer wave also shows more frequent APK (Android Package Kit) rebuilds, rotating banking lures, and packaging changes intended to hinder basic analysis and slow defensive response.

Technical Details

- The campaign starts with a phishing website designed to look like a legitimate banking portal, where victims first submit their online banking credentials.
- After credential entry, the victim is told that the banking application must be updated, creating a believable reason to install a malicious Android package.
- The delivery chain then moves through a shortened link and ends with a malicious APK hosted in a public repository disguised as a harmless project.
- Once installed, the app opens a local WebView-based interface that imitates a card-verification process and keeps the victim engaged step by step.
- The malware asks the victim to place a payment card near the device, then uses Android NFC functions and EMV (Europay, Mastercard, and Visa) parsing to read card data.
- It then prompts for a 4-digit PIN and packages that value with previously collected card information for transmission.
- The newer samples keep the same core NFC reading and exfiltration logic seen in earlier versions, showing continuity in the fraud workflow.
- The main changes are operational: more frequent APK rebuilds, broader brand rotation, and updated command-and-control configuration.
- Recent versions also increased the DEX (Decentralized Exchange) count and introduced malformed ZIP paths that can break simple extractors and disrupt automated analysis pipelines.
- These packaging changes do not alter the malware's objective, but they make triage and family matching more difficult for defenders.

Recommendations

- Monitor for phishing workflows that combine credential capture with prompts to install a mobile banking "update."
- Restrict or closely review APK sideloading on Android devices used for sensitive financial activity.
- Flag mobile applications that combine WebView-based banking verification screens with NFC card-reading behavior.
- Treat APK extraction failures and malformed archive structures as suspicious, especially in newly observed Android banking samples.
- Prioritize detections based on the combined behavior of credential theft, NFC card reading, PIN capture, and repeated APK rebuild patterns.

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
UNK_DeadDrop Developer Phishing Campaign Targets Cryptocurrency Ecosystem	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified UNK_DeadDrop, a phishing campaign that targeted individuals in nearly 100 organizations across finance, cryptocurrency, technology, education, and other sectors. The activity used developer recruitment, code review, Foundry testing, and AI payments project themes to lure targets into cloning attacker-controlled repositories and opening them in code editors, which silently triggered malware execution through preconfigured tasks and a malicious editor extension.

The campaign may impact organizations with developer teams working on cryptocurrency, blockchain, and related engineering workflows because it combines convincing project lures with low-interaction execution and credential theft. Organizations in the financial sector should be aware that the activity was designed to steal browser wallet data, decrypted credentials, and desktop wallet information while also removing artifacts from the cloned repository to hinder investigation.

Technical Details

- The campaign began with phishing emails that posed as job offers, code review requests, testing tasks, or project opportunities aimed at software developers and security-focused users.
- Those emails directed targets to attacker-controlled repositories that appeared legitimate, with realistic project structures, working scripts, and references to real blockchain and development standards.
- Victims were instructed to clone the repository and open it in editors such as VS Code or Cursor, making the malicious workflow appear like a normal development task.

- A hidden task configuration was set to run automatically when the folder was opened, which launched platform-specific scripts with little or no visible user interaction.
- The initial scripts installed a malicious editor extension and then triggered the next stage of the infection chain based on the victim's operating system.
- On Linux and macOS, the campaign used native Go-based malware that maintained a persistent connection, performed system reconnaissance, and enabled remote command execution.
- On Windows, the activity ran inside the editor process using a Node[.]js-based workflow, staged encrypted components, and executed credential and wallet theft functions without dropping a traditional binary.
- Across platforms, the malware collected browser wallet extensions, standalone wallet data, browser credentials, and other locally stored authentication material before sending it to attacker-controlled infrastructure.
- The campaign also used anti-forensic cleanup by deleting malicious files and directories from the cloned repository after execution, while keeping access through the installed extension where supported.
- Multiple repository themes and repeated builds showed continued development, suggesting the operators were actively refining both delivery and post-compromise tradecraft.

Recommendations

- Review and restrict automatic task execution in development editors, especially when repositories are opened from untrusted external sources.
- Enforce strict controls for cloning external code repositories on systems used for financial, blockchain, or virtual asset development.
- Monitor developer endpoints for suspicious editor extension installations, unusual script execution, and access to browser wallet or credential stores.
- Train developers to treat unsolicited job offers, code review requests, and testing tasks involving external repositories as high-risk.
- Prioritize detection for activity that combines repository-based initial access, editor task abuse, credential theft, wallet collection, and post-execution cleanup.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – UNK_DeadDrop Developer Phishing Campaign Targets Cryptocurrency Ecosystem

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
MENA-Focused Social Engineering and Monetization Through SniperDz PhaaS	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Group-IB has identified SniperDz as a centralized PhaaS (Phishing as a Service) and PNaaS (Private Network as a Service) ecosystem driving MENA-focused social engineering campaigns. The operation uses fraudulent social media accounts, trusted link-aggregation services, localized lure pages, and deceptive browser notification prompts to move victims into phishing and monetization flows.

This campaign may impact organizations in the financial sector because it uses investment-themed lures, harvests personal data, and redirects users into fraud schemes based on device, location, and carrier. Financial services organizations in the region should be aware of how trusted brands and localized themes are abused to drive user engagement.

Technical Details

- Threat actors used fraudulent Facebook accounts to impersonate politicians, public figures, telecom providers, and trusted organizations. These accounts promoted fake offers such as free mobile data, financial compensation, and subsidy programs.
- Victims who clicked the posts were not taken directly to a phishing page. Instead, they were first routed through trusted link-aggregation services such as Linkbio and Linktree to hide the real destination.
- The intermediate pages looked like legitimate promotions and used localized Arabic content to increase trust. Although victims saw multiple buttons and choices, every option led to the same attacker-controlled tracking infrastructure.
- After leaving the link-aggregation page, victims were sent to a final landing page designed to obtain browser notification permissions. The page used a simple message instructing users to click “Allow”, making the request appear like a normal verification step.
- If the victim accepted the prompt, the site created a push-notification subscription and sent the subscription token and related tracking data back to the operators. This gave the attackers a persistent way to push unwanted content to the victim later.
- Researchers found the same VAPID (Voluntary Application Server Identification) public key across multiple campaigns, including telecom-themed and investment-related scams. This shared key linked different lures and brands back to the same underlying notification ecosystem.
- The pages also used browser manipulation to keep victims trapped in the scam flow. This included adding fake browser history entries and using tab-under redirects to move the victim back into attacker-controlled pages.
- Once victims were inside the ecosystem, the traffic distribution system evaluated factors such as device type, location, and mobile carrier. Based on that profile, users were redirected to premium-rate calls, premium SMS subscriptions, or fake investment pages.

- In the investment-related flows, victims were asked to submit personal information such as name, email address, and phone number. That data could then be used for follow-on fraud, lead generation, or shared with affiliated operators.
- Researchers also linked the activity to a wider hosting and domain cluster associated with more than 900 suspicious domains. This indicates the campaign is part of a broad and centralized fraud and monetization ecosystem.

Recommendations

- Verify promotions and investment offers only through official websites or confirmed social media accounts.
- Treat multi-stage redirects through link-aggregation services and unrelated domains as suspicious.
- Block or closely monitor unexpected browser notification prompts delivered through web-based promotions.
- Review and remove suspicious browser notification permissions on user systems regularly.
- Monitor for unauthorized premium SMS charges, premium-rate calls, and suspicious lead-capture pages tied to investment themes.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – MENA-Focused Social Engineering and Monetization Through SniperDz PhaaS

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
Sophisticated Browser-in-the-Browser (BitB) Phishing Campaign Targets OAuth Credentials	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers have identified a browser-in-the-browser phishing campaign involving at least 10 unique domains that uses a fake browser pop-up within a webpage to steal credentials. The pop-up presents a login form and a crafted address bar designed to resemble a legitimate OAuth authorization URL, making the sign-in prompt appear authentic to the victim.

Organizations in the financial sector should be aware that this technique could affect environments that rely on OAuth-based sign-in workflows, as the fake window is tailored to match the victim's operating system and browser while using multiple evasion methods to reduce visibility. The combination of realistic interface

design, anti-analysis features, and separated payload delivery may make the activity harder to detect during routine web use.

Technical Details

- The attack relied on a browser-in-the-browser technique, where a webpage displayed a fake browser pop-up instead of opening a real browser window.
- Inside the fake window, the victim was shown a login form intended to capture credentials.
- The pop-up also contained a fake browser address bar with text carefully crafted to look like a legitimate OAuth authorization URL.
- To make the page appear more convincing, the fake window was draggable and included refresh, minimize, back, and close buttons like a normal browser.
- The code checked whether the victim was using Windows, macOS, or Linux, and also identified the browser in use, then applied matching styling so the fake window looked native.
- The spoofed address bar content was specifically designed to imitate a real OAuth sign-in flow.
- The page used anti-debugging methods by overriding common console functions, making browser-based analysis more difficult.
- Visible text was broken up with empty HTML tags and random class names to defeat simple string-based detections.
- If bot detection was triggered, the victim was redirected to a legitimate help page, while the actual credential-harvesting content was loaded in a sandboxed iframe separate from the fake browser shell.

Recommendations

- Train users to treat login prompts displayed inside a webpage as suspicious and to verify that authentication opens in a real browser window.
- Monitor authentication-themed pages for fake browser controls, draggable pop-ups, and address bars rendered as webpage content.
- Review detections for scripts that override console methods or use anti-analysis techniques to hide browser-based phishing activity.
- Inspect suspicious pages for fragmented visible text and heavy interface styling that may be used to bypass text-based security checks.
- Investigate web content that uses sandboxed iframes to separate a realistic outer interface from a hidden credential collection page.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Sophisticated Browser-in-the-Browser (BitB) Phishing Campaign Targets OAuth Credentials

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 Malicious VS Code Extension Deploys Covert Multi-Stage Backdoor	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a malicious VS Code extension campaign in which Jupyter-themed and other developer utility packages appeared legitimate in the VS Code Marketplace but silently delivered a multi-stage backdoor after installation. The extension used a JavaScript control layer to communicate through Graph API and SharePoint, then deployed platform-specific agents for Windows, Linux, and macOS that enabled code execution, file access, and data movement on the compromised system.

Organizations in the financial sector should be aware that this activity may impact development environments that rely on trusted extensions and standard cloud services as part of normal workflows. The use of encrypted communications, cloud-hosted proxy brokers disguised as financial APIs, and cross-platform tooling could affect visibility by making malicious traffic appear similar to routine developer and collaboration activity.

Technical Details

- The campaign involved multiple VS Code Marketplace extensions that looked like normal developer tools but contained hidden backdoor functionality.
- One highlighted sample was a Jupyter-themed extension, which helped the package blend into common development workflows.
- After installation, a JavaScript layer managed command-and-control traffic and acted as the main control point for the malware.
- That control layer communicated through Graph API and SharePoint instead of using a more obvious attacker-controlled channel.
- The malware then deployed different agents based on the operating system, using an executable for Windows and Python scripts for Linux and macOS.
- A SharePoint site functioned as the command queue, victim registry, and exfiltration channel for the operation.
- Access to the backend was routed through Azure-hosted proxy brokers that were disguised as financial APIs.
- Once active, the backdoor supported arbitrary file read, write, exfiltration, and code execution on infected systems.
- The source states that all inter-process and command-and-control traffic was protected with AES-256-CBC (Cipher Block Chaining) encryption.
- The Windows binary also used evasion measures, including a forged compilation timestamp set to 2040, and the research described three related extensions under different publisher names.

Recommendations

- Restrict installation of VS Code extensions to approved packages and review new developer tools before use in enterprise environments.
- Monitor developer systems for unusual Graph API and SharePoint activity tied to extension installation or execution.
- Investigate extensions that bundle executables or cross-platform script components when the package claims to be a lightweight productivity tool.
- Review network traffic that appears to use financial API themes but originates from developer tooling.
- Prioritize detection of encrypted extension-related traffic that coincides with unexpected file access, exfiltration, or code execution.

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
MLTBackdoor Delivered Through a Multi-Stage ClickFix Campaign	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified MLTBackdoor, a newly observed malware family delivered through a multi-stage ClickFix infection chain that begins with a lure on an automotive-related webpage and the attack tricks victim into copying, pasting, and running harmful code. Once triggered, the chain downloads a compressed archive, uses a DLL to decrypt an RC4-encrypted second-stage payload, and then sideloads the backdoor through a legitimate signed security component to continue execution.

Organizations in the financial sector should be aware that this activity may impact environments where social engineering can be used to trigger follow-on malware execution and establish a foothold for later movement. The combination of heavy obfuscation, fallback command-and-control logic, and modular post-compromise capability could affect visibility and make analysis more difficult once the malware is active.

Technical Details

- The infection chain started with a ClickFix lure hosted on an automotive-related webpage.
- The victim had to copy, paste, and run the displayed content, making user interaction a required step in the attack.
- That action downloaded a compressed archive containing a DLL and an encrypted data file.
- The DLL then decrypted the RC4-encrypted file, which contained the second-stage payload.
- The decrypted payload was MLTBackdoor, which performed a self-update before continuing execution.

- The malware then reused the DLL filename and was sideloaded through a legitimate signed component to help execution blend in.
- MLTBackdoor supported file-related commands, including downloading and uploading files from the victim system.
- One of its stronger capabilities was a Beacon Object File loader, which allowed operators to extend functionality after deployment.
- The malware used Mixed Boolean-Arithmetic and Control Flow Flattening to make static and dynamic analysis harder.
- It also used a domain generation algorithm so it could continue reaching command-and-control infrastructure if hardcoded domains became unavailable.

Recommendations

- Train users to treat ClickFix-style prompts that ask them to copy and execute content as suspicious.
- Monitor for unusual archive downloads followed by DLL execution and rapid second-stage payload loading.
- Review endpoint activity for signs of sideloading through legitimate signed components.
- Prioritize detection of heavily obfuscated binaries that also perform file operations after execution.
- Watch for malware families that use fallback domain generation logic to maintain contact with remote infrastructure.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
SilabRAT MaaS Enables Covert Browser Session Abuse and Financially Motivated Theft	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified SilabRAT, a Malware-as-a-Service (MaaS) remote access trojan that has been sold on dark web forums since at least September 2025 and used in real-world email spam and ClickFix campaigns. In the observed infection chain, victims were socially engineered into interacting with ClickFix content delivered through phishing, malicious advertisements, or compromised websites, after which the malware provided operators with credential theft, browser session abuse, remote control, and follow-on payload delivery capabilities.

Organizations in the financial sector should be aware that this activity may impact environments where authenticated browser sessions, stored credentials, and cryptocurrency-related assets are present on user endpoints. Its combination of hidden remote access, browser profile cloning, wallet-focused credential

recovery, and session abuse could affect efforts to detect fraud when attacker activity originates from the victim's own device and network context.

Technical Details

- SilabRAT has been offered as a subscription-based MaaS, where buyers run their own command-and-control servers while the developer handles updates and service support.
- In observed activity, operators delivered the malware through email spam and ClickFix campaigns, although the infection chain can vary between customers.
- Once active, the malware connects to an operator-hosted web panel that gives attackers a live view of infected machines, hardware details, active windows, and running software.
- The panel allows operators to launch hidden remote sessions, trigger a stealer, execute additional payloads, and monitor keystrokes and clipboard activity.
- SilabRAT is built to steal credentials and wallet data, and it can also use passwords taken from browser data to try to unlock encrypted cryptocurrency wallets automatically.
- For browser session abuse, it can steal cookies and also clone the victim's browser profile to help bypass protections tied to device fingerprints or IP address checks.
- Its hidden remote access uses a separate component that redirects browser file operations to a cloned profile, allowing attackers to use the victim's browser session without visible on-screen activity.
- The malware also includes bypasses for browser app-bound protection, basic AMSI interference, privilege elevation through a COM-based UAC bypass, and persistence through Run keys or scheduled tasks.

Recommendations

- Treat ClickFix-style prompts that ask users to copy, paste, or execute content as suspicious and investigate them quickly.
- Strengthen email and web filtering to reduce exposure to phishing, malicious advertisements, and compromised sites used to deliver remote access malware.
- Enforce MFA across critical services, while also monitoring for browser session abuse that may bypass password-based controls.
- Prioritize patching of operating systems, browsers, and related software so current security protections remain effective against credential and session theft techniques.
- Monitor endpoints for hidden remote control behavior, unexpected browser profile access, keylogging, clipboard monitoring, and follow-on payload delivery.

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
Golang-Based BLUERABBIT Malware with Encryption, Remote Access and Wiping Features	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified BLUERABBIT, a Golang-based backdoor that, once executed on a Windows system, checks for prior execution, establishes persistence through a scheduled task and then registers with remote infrastructure using RabbitMQ instead of a more typical web-based command channel. The malware receives numeric task IDs over AMQP (Advanced Message Queuing Protocol), maps them to built-in modules, and supports a full intrusion flow that includes reconnaissance, file staging, exfiltration, file encryption, and destructive disk wiping.

Organizations in the financial sector should be aware that this activity may impact Windows environments where message-broker or cloud-style traffic could blend into normal operations. The combination of remote access, system profiling, data exfiltration, encryption, and anti-recovery actions could affect response efforts, particularly if the malware reaches its later destructive stages.

Technical Details

- After execution, the malware checks a registry location associated with OneDrive environment settings to determine whether it has already run on the system.
- It then establishes persistence by creating a scheduled task named “OneDrive Update” that triggers at startup and repeats every 60 seconds.
- For command-and-control, BLUERABBIT connects to RabbitMQ over AMQP and declares a queue named after the victim device.
- The malware uses a modular tasking model, where numeric task IDs are received over AMQP and mapped to more than a dozen built-in functions.
- Early tasking includes reconnaissance of the operating system, hardware, network settings, installed software, security products, BitLocker status, drivers, and domain details.
- Files selected for theft are staged in GUID-named directories before being exfiltrated to attacker-controlled MinIO infrastructure.
- State management is handled through Redis, allowing the malware to separate tasking, operational state, and data movement across different services.
- Remote access features include VNC-style control with keyboard and mouse input, shell command execution, screenshot capture, and service or process management.
- The malware can encrypt files across logical drives using a “.candy” extension and can also launch two separate disk-wiping routines designed to render systems unrecoverable.
- Before destructive actions, it disables recovery-related functions and takes ownership of critical boot files to reduce the chance of system recovery.

Recommendations

- Monitor Windows endpoints for unexpected scheduled tasks that imitate legitimate update activity and execute at short recurring intervals.
- Review workstation traffic for unusual RabbitMQ, Redis, or MinIO communications that do not align with approved business applications.
- Investigate systems that begin collecting detailed host, software, security product, or BitLocker information alongside file staging activity.
- Prioritize detections for VNC-style remote control, shell execution, screenshot capture, and process or service manipulation on user systems.
- Prepare response playbooks for malware that combines exfiltration, encryption, and anti-recovery behavior so containment can occur before destructive modules are triggered.

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
AI Themed Lures Deliver AsyncRAT Through Multi-Stage Malware Chains	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a campaign that uses AI-themed learning resources as lures to deliver a multi-stage malware chain on Windows systems, including files presented as AI Related guides. In the observed flow, a compressed archive appears harmless, but when the victim opens a shortcut file inside it, native Windows tools are used to extract hidden content from disguised PDF files, launch staged scripts, and ultimately deploy AutoHotkey-based loaders that reflectively inject a ".NET" remote access trojan and AsyncRAT into memory.

Organizations in the financial sector should be aware that this activity could affect users who open AI-themed documents or reference material from untrusted sources, especially when the content arrives as archived files containing shortcuts. The layered use of hidden files, built-in Windows components, in-memory loading, and carefully staged script execution may impact visibility by reducing obvious signs of malware delivery during the early phases of compromise.

Technical Details

- The campaign used AI-related document themes to make the files appear relevant and trustworthy to users seeking technical or marketing resources.
- Delivery started through a compressed archive that showed a shortcut file as visible content while two additional files were present with a hidden attribute.

- When the victim opened the shortcut, it ran an obfuscated command sequence built from native Windows components such as cmd[.]exe, more, type, and findstr.
- One hidden file was not treated as a document, but as a data container from which only specific line ranges were extracted and executed.
- The first extracted content was only a staging step, which again read from the same file and passed another selected block into PowerShell.
- The PowerShell stage was launched with hidden-window and execution-bypass options to reduce visibility and avoid normal script restrictions.
- The overall chain was described as highly staged, with each phase existing mainly to reveal the next rather than dropping a single obvious payload.
- The final stages used AutoHotkey-based loaders to reflectively inject both a ".NET" remote access trojan and AsyncRAT into memory for command-and-control and follow-on execution.
- The source also noted that several intermediate scripts used Simplified Chinese variable names and a structured coding style.

Recommendations

- Treat AI-themed guides or technical resources delivered as compressed archives with caution, especially when they contain shortcut files instead of normal documents.
- Monitor for shortcut-initiated execution chains that call native Windows tools to read hidden content from files that appear to be documents.
- Review PowerShell activity for hidden-window execution and script-bypass patterns tied to staged content extraction.
- Investigate unexpected AutoHotkey-based loading behavior, particularly when it is followed by in-memory injection rather than normal application use.
- Reinforce user awareness around AI-themed lures that are presented as learning materials but rely on nonstandard file structures or execution steps.

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 Leveraging Oracle PeopleSoft Weaknesses	HIGH	CLEAR	Vulnerability	Open Source

Executive Summary

Oracle has published a security alert for CVE-2026-35273 in Oracle PeopleSoft PeopleTools, noting that PeopleSoft Enterprise Applications customers may also be affected and that the issue is remotely exploitable without authentication and may lead to remote code execution. The accessible source content also states that observed activity was consistent with exploitation of the Environment Management component, where attackers targeted exposed PeopleSoft application infrastructure and used the weakness to gain initial access before staging follow-on actions.

Organizations in the financial sector should be aware that this vulnerability may impact internet-exposed PeopleSoft environments, particularly where the affected management functionality remains reachable from external networks. The observed exploitation preceding Oracle's June 10, 2026, advisory suggests defenders could face limited warning time when similar weaknesses are abused in active intrusion and extortion activity.

Technical Details

- Oracle's alert states that CVE-2026-35273 affects PeopleSoft PeopleTools 8.61 and 8.62, and that some PeopleSoft Enterprise Applications customers may also be exposed.
- Oracle describes the issue as remotely exploitable without authentication, with successful exploitation potentially resulting in remote code execution.
- The observed campaign took place between May 27, 2026, and June 9, 2026, and was linked to exploitation of the vulnerable Environment Management component.
- The available reporting states that the activity predated Oracle's June 10, 2026 advisory, indicating the flaw was exploited as a zero-day.
- The targeting directly aligned with exposed Environment Management Hub endpoints in Oracle PeopleSoft infrastructure.
- Researchers reported notifying more than 100 global organizations whose IP addresses correlated with potentially vulnerable endpoints.
- The accessible excerpt states that 68% of those organizations were in the higher education sector, showing focused opportunistic targeting of exposed environments.
- The attacker staging environment reportedly hosted customized remote management agents that were used to run administrative command queries and deploy a custom lateral movement and defacement script.

Recommendations

- Apply Oracle's released patches and mitigations immediately and prioritize upgrades to supported PeopleTools versions where required.

- Review perimeter and application logging for external requests targeting PeopleSoft management and integration functions.

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

Vulnerability and affected product details can be found *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
China-Nexus SLIME88 Leveraging ActiveMQ Remote Code Execution Chains	HIGH	CLEAR	Vulnerability	Open Source

Executive Summary

Apache has disclosed CVE-2026-34197, a remote code execution vulnerability in Apache ActiveMQ and Apache ActiveMQ Broker that affects vulnerable versions where the Jolokia JMX-HTTP ((Java Management Extensions) bridge permits exec operations on ActiveMQ MBeans. In the described attack path, an authenticated actor sends a crafted HTTP request to the Jolokia endpoint, uses a crafted discovery URI to force the broker to load a remote Spring XML application context, and achieves code execution on the broker's JVM before configuration validation completes.

This vulnerability may impact organizations with exposed ActiveMQ environments, particularly where default credentials remain in use or where older weaknesses can assist with authentication bypass on some versions. The activity also states that threat actors, including SLIME88, actively exploited the issue shortly after disclosure and used the resulting access to deploy follow-on malware on Linux systems.

Technical Details

- The flaw affects Apache ActiveMQ Broker and Apache ActiveMQ versions before 5.19.4 and 6.0.0 before 6.2.3.
- The vulnerable component is the Jolokia JMX-HTTP bridge exposed at "/api/jolokia/" on the web console.
- The default Jolokia access policy allows exec operations on ActiveMQ MBeans, including methods that can add connectors.
- An attacker can invoke those operations with a crafted discovery URI that causes the broker to load a remote Spring XML application context.
- Code execution occurs because singleton beans are instantiated before the broker validates the configuration.
- The accessible reporting states that exploitation used a crafted HTTP request and a malicious XML payload fetched from attacker infrastructure.
- Although the issue requires authentication, the reporting notes that default credentials are common in many cases.

- The same reporting also states that, on some versions, actors can use CVE-2024-32114 to bypass authentication.

Recommendations

- Upgrade affected deployments to 5.19.4 or 6.2.3 as recommended in the vendor advisory.
- Review whether the Jolokia endpoint is externally reachable and restrict access where possible.
- Remove or change default credentials on exposed ActiveMQ systems.

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

Vulnerability and affected product details can be found *here*, *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Google Chrome Zero-Day Patched in Stable Channel Update	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Google has released Chrome Stable Channel version 149.0.7827.102/.103 for Windows and macOS and 149.0.7827.102 for Linux, addressing 74 security issues including 17 Critical and 57 High/Medium severity vulnerabilities. Among them is CVE-2026-11645, a High-severity out-of-bounds memory access flaw in the V8 JavaScript engine that has been confirmed as actively exploited in the wild, where a remote attacker could use a crafted HTML page to trigger out-of-bounds read and write conditions and execute arbitrary code inside the browser sandbox.

Organizations in the financial sector should be aware that this update may impact environments where Chrome is widely used to access sensitive internal or external services, particularly because the patched release also includes numerous Critical memory corruption issues across core browser components. The combination of an actively exploited V8 flaw and multiple additional high-risk browser vulnerabilities could affect exposure management if enterprise browsers are not updated quickly across user endpoints.

Technical Details

- Google released updated Chrome Stable Channel builds for Windows/macOS.
- The release addresses 74 vulnerabilities in total, including 17 Critical and 57 High/Medium severity issues.
- CVE-2026-11645 is the actively exploited vulnerability highlighted in the update. It is a High-severity out-of-bounds read and write issue in V8.
- According to the provided content, a remote attacker could exploit CVE-2026-11645 using a crafted HTML page to achieve arbitrary code execution inside a sandbox.
- The Critical issues include multiple use-after-free flaws across core components such as Ozone, File Input, Aura, TabStrip, Bluetooth, Gamepad, Autofill, Views, Printing, Compositing, Web Apps, and Proxy.

- The update also fixes CVE-2026-11640, a Critical integer overflow in libyuv that may lead to memory corruption and possible code execution.
- Additional High-severity issues were addressed in V8, Bindings, WebRTC, GPU, libyuv, Media, and Bluetooth, including memory corruption, information disclosure, and code execution risks.

Recommendations

- Update Google Chrome to the latest stable version immediately.
- Enable automatic browser updates across enterprise environments.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Authentication Bypass in Remote Access VPN Under Active Exploitation	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Check Point has disclosed CVE-2026-50751, a high-severity authentication bypass vulnerability affecting Remote Access VPN and Mobile Access VPN on Gaia and Gaia Embedded systems when specific legacy settings are enabled. In the described attack path, a remote attacker can exploit a logic flow weakness in VPN certificate validation during authentication to establish a VPN connection without a valid user password, provided IKEv1, legacy client support, and non-mandatory machine certificate checks are in place.

Organizations in the financial sector should be aware that this issue may impact environments where legacy remote access settings remain enabled, as successful exploitation could allow unauthorized entry into internal networks. The fact that the vulnerability is actively exploited in the wild could affect remote access security posture, especially where unsupported versions, weak configuration controls, or limited VPN session monitoring remain in use.

Technical Details

- CVE-2026-50751 is a high-severity authentication bypass vulnerability affecting Remote Access VPN and Mobile Access VPN deployments on Gaia and Gaia Embedded platforms.
- The weakness is network-exploitable and does not require a valid user password when the vulnerable configuration is present.
- The root cause is described as a logic flow weakness in VPN certificate validation during authentication.
- Exploitation requires Remote Access VPN or Mobile Access VPN to be enabled on the gateway.
- The vulnerable path also requires IKEv1 to be enabled for remote access and legacy VPN clients to be accepted.
- A further condition is that the gateway does not require a machine certificate for connections.

- Successful exploitation can allow an attacker to bypass user authentication controls and establish unauthorized VPN connections.
- Once connected, the attacker may gain remote access to internal corporate networks, which can support lateral movement, access to sensitive systems, privilege escalation, and further compromise.
- A successful exploit attempt is indicated by completion of a VPN Quick Mode negotiation resulting in a "Key Install" event in logs.
- The affected versions include multiple gateway and firewall releases, including supported hotfix branches and several end-of-support versions.

Recommendations

- Apply the latest available Jumbo Hotfix Accumulator or supported vendor hotfixes for affected releases as soon as possible.
- Upgrade all unsupported end-of-support versions immediately to supported versions.
- Review VPN settings and disable IKEv1 and legacy client support where operationally possible.
- Confirm whether machine certificate authentication is enforced for remote access connections.
- Review VPN logs for Quick Mode negotiations, "Key Install" events, unusual remote access sessions, and unexpected connection activity, and validate MFA deployment for remote access users.

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

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
PAN-OS Authentication Bypass Actively Exploited Against GlobalProtect	HIGH	CLEAR	Vulnerability	Open Source

Executive Summary

Palo Alto Networks has disclosed active exploitation of CVE-2026-0257, an authentication bypass vulnerability in the portal and gateway components of vulnerable PAN-OS versions that can be used to target GlobalProtect. In the observed activity, an unidentified threat actor attempted to access GlobalProtect by abusing the flaw to bypass security controls and initiate VPN connections without following the normal authentication path.

Organizations in the financial sector should be aware that this issue may impact internet-facing remote access infrastructure where vulnerable PAN-OS deployments remain exposed. The accessible reporting states that only a small portion of probed devices progressed to successful VPN sessions, but confirmed gateway-connected events could affect incident handling because they indicate the attacker moved beyond probing into active connection establishment.

Technical Details

- The activity involved CVE-2026-0257, which the source describes as an authentication bypass issue in vulnerable PAN-OS software.
- The vulnerable area is the portal and gateway components, which are directly tied to GlobalProtect remote access functionality.
- The attack goal observed in the report was to access GlobalProtect by circumventing normal security controls.
- Successful exploitation could allow an unauthorized attacker to initiate VPN connections through the affected components.
- The observed activity included probing of exposed devices, but only a small portion of those devices actually established VPN sessions.
- Where exploitation was successful, the result was the appearance of gateway-connected events in GlobalProtect logging.
- At the time of reporting, the source noted no identified post-access behavior or lateral movement, suggesting visibility was strongest around the access stage.
- The report also highlights that defenders should search GlobalProtect logs for successful gateway-connected events linked to suspicious activity patterns.

Recommendations

- Review the official security advisory and apply the available workarounds, mitigations, or fixed PAN-OS version upgrades without delay.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft June 2026 Updates Address Zero-Days, Defender Exploitation, and Broad RCE Exposure	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Microsoft has released its June 2026 Patch Tuesday updates addressing 206 vulnerabilities across Windows, Microsoft Office, Outlook, Hyper-V, Remote Desktop Client, BitLocker, HTTP[.]sys, Microsoft Defender, and other core components. The release includes three publicly disclosed zero-day vulnerabilities and an actively exploited Microsoft Defender elevation of privilege flaw, alongside multiple remote code execution paths that could be triggered through exposed services, crafted content, or vulnerable local system components depending on the affected product.

Organizations in the financial sector should be aware that these issues may impact internet-facing systems, remote access infrastructure, domain-joined endpoints, privileged workstations, and systems running Remote Desktop Client. The concentration of remote code execution, elevation of privilege, security feature bypass, and denial-of-service issues could affect patching priorities where critical services, sensitive data, or administrative access paths rely on the affected Microsoft technologies.

Technical Details

- The June 2026 release addresses 206 vulnerabilities across a wide range of Microsoft products and core platform components.
- The update includes 3 publicly disclosed zero-day vulnerabilities, 37 Critical vulnerabilities, and 166 Important/Moderate vulnerabilities.
- The publicly disclosed zero-days are CVE-2026-50507 affecting Windows BitLocker, CVE-2026-49160 affecting HTTP[.]sys, and CVE-2026-45586 affecting the Windows Collaborative Translation Framework (CTFMON).
- CVE-2026-41091 is a Microsoft Defender Elevation of Privilege vulnerability that has been actively exploited in the wild.
- Several Microsoft Office vulnerabilities are included, such as CVE-2026-45461, CVE-2026-45463, CVE-2026-45472, and CVE-2026-45474, all identified as remote code execution issues.
- Additional Office-related exposure includes Outlook and Word remote code execution vulnerabilities, including CVE-2026-45456, CVE-2026-47635, and CVE-2026-45458.
- The release also addresses Windows Hyper-V remote code execution vulnerabilities, including CVE-2026-45607, CVE-2026-47652, and CVE-2026-45641.
- Multiple Remote Desktop Client remote code execution vulnerabilities are included, alongside Active Directory Domain Services, Kerberos KDC, DHCP Client Service, Windows Deployment Services, and HTTP[.]sys issues.
- The release further includes BitLocker security feature bypass, Microsoft Cryptographic Services elevation of privilege, Azure Kubernetes Service remote code execution, and Windows Graphics Component vulnerabilities.

Recommendations

- Apply the June 2026 Microsoft security updates as a priority across all affected systems.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Linux Kernel nf_tables Flaw Allows Local Root Escalation	HIGH	CLEAR	Vulnerability	Open Source

Executive Summary

Linux kernel maintainers have addressed CVE-2026-23111, a use-after-free vulnerability in the 'nf_tables' subsystem that can be abused by a local unprivileged user to escalate privileges to root. The accessible source material shows that the flaw stems from an inverted activity check in the abort phase for catchall map elements, allowing a failed transaction path to mishandle object state and eventually free a chain that is still referenced, creating a usable use-after-free condition.

Organizations in the financial sector should be aware that this issue may impact Linux systems where 'nf_tables' is enabled and unprivileged users can reach the vulnerable code path, particularly on platforms that allow user namespaces. The availability of public technical analysis and reproduction material could affect patch urgency because it lowers the barrier for additional actors to study and adapt the vulnerability for local privilege escalation.

Technical Details

- The core issue is an inverted condition in the catchall element handling logic during the abort phase of 'nf_tables' transactions.
- In the vulnerable flow, the code skips inactive elements and processes active ones, which is the opposite of the required logic.
- When a 'DELSET' operation is aborted, the expected reactivation path is not completed for the catchall element.
- For 'NFT_GOTO' verdict elements, this means the reference count for the target chain is not properly restored.
- Each abort cycle reduces chain->use, and once that count reaches zero, 'DELCHAIN' can free the chain while verdict elements still point to it.
- That stale reference results in a use-after-free, which the public analysis shows can be turned into local privilege escalation from an unprivileged user to root.
- The technical write-ups state that exploitation was demonstrated on Debian Bookworm, Debian Trixie, Ubuntu 22.04 LTS, and Ubuntu 24.04 LTS, and is relevant where 'CONFIG_USER_NS' and 'CONFIG_NF_TABLES' are enabled.

Recommendations

- Apply kernel updates that include the fix for CVE-2026-23111 as a priority.
- Prioritize Linux systems where 'nf_tables' are in use and user namespaces are enabled, as those conditions are specifically tied to exploitability in the accessible reporting.

Vulnerability and affected product details can be found *here*, *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Flaws in VMware Cloud Foundation Operations Could Enable Unauthorized Admin Actions	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities, tracked as CVE-2026-41722, CVE-2026-41723, and CVE-2026-41724, each rated High with a CVSS v3.1 score of 8.0. In the described attack path, an authenticated attacker with privileges to create policies, views, or text widgets can inject malicious scripts into the application, which are then executed in the application context when rendered, potentially enabling unauthorized actions by abusing trusted user sessions and administrative workflows.

Organizations in the financial sector should be aware that these flaws may impact environments using affected VMware Cloud Foundation Operations and related products where privileged users can create or modify application content. The ability to execute malicious scripts within the application context could affect administrative integrity by enabling session compromise, content manipulation, and unauthorized actions within management interfaces.

Technical Details

- The flaws are stored cross-site scripting vulnerabilities, meaning malicious content can be saved within the application and executed later when viewed.
- Exploitation requires an authenticated attacker who already has privileges to create policies, views, or text widgets.
- The attacker can use those features to inject malicious scripts into the application.
- When the injected content is rendered, the script executes within the application context rather than as a separate external payload.
- Successful exploitation may result in unauthorized administrative actions inside the affected environment.
- The provided impact also includes potential session compromise and manipulation of application content.
- Affected products include VMware Cloud Foundation Operations, VMware Aria Operations, and related bundled deployments across multiple supported versions.

Recommendations

- Update affected products to the fixed or latest versions released by Broadcom.

Vulnerability and affected product details can be found *here*.

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

UNK_DeadDrop Developer Phishing Campaign Targets Cryptocurrency Ecosystem

Tactics	Techniques	Observed Activity
Initial Access	Spearphishing Link T1566.002	Phishing emails used recruitment, code review, and testing themes to direct developers to attacker-controlled code repositories.
Execution	User Execution T1204	The victim had to clone or open the malicious project in a development environment, after which execution was triggered.
Execution	Command and Scripting Interpreter T1059	The campaign used shell, command-line, JavaScript, and Python-based execution paths depending on platform and stage.
Persistence	Event Triggered Execution T1546	A malicious editor extension was installed and, on some platforms, reactivated when the development tool was opened again.
Credential Access	Credentials from Password Stores T1555	The malware accessed browser-stored credentials and local secret stores, including operating system-managed credential material.
Credential Access	Input Capture T1056	On macOS and Linux, deceptive password prompts were used to obtain user credentials.
Collection	Data from Local System T1005	The operators collected browser profile data, wallet-related information, cookies, and standalone wallet artifacts from local systems.
Collection	Archive Collected Data T1560	Stolen material was packaged into archive files before upload.
Command and Control	Application Layer Protocol T1071	The campaign used web-based communications, including persistent connections on some platforms and web requests for data upload.
Exfiltration	Exfiltration Over C2 Channel T1041	The collected credential and wallet data was uploaded through the same command-and-control path used during the intrusion.
Defense Evasion	File and Directory Removal T1070.004	The malware deleted malicious payloads and directories from the cloned project to reduce forensic evidence after execution.

MENA-Focused Social Engineering and Monetization Through SniperDz PhaaS

Tactics	Techniques	Observed Activity
Resource Development	T1585.001 – Establish Accounts: Social Media Accounts	Threat actors used fraudulent Facebook accounts to impersonate politicians, public figures, and trusted organizations as the initial delivery channel for the campaign.
Defense Evasion	T1036 – Masquerading	The operation impersonated trusted public figures, politicians, telecommunications providers, and well-known brands to make fraudulent content appear legitimate.
Initial Access	T1566.002 – Phishing: Spearphishing Link	Victims were encouraged to click embedded links in fake social media offers in order to claim advertised benefits.
Resource Development	T1583.006 – Acquire Infrastructure: Web Services	The campaign abused high-reputation link-aggregation services to conceal malicious destinations and support traffic redirection.
Defense Evasion	T1071 / Trusted Web Redirection Abuse	Intermediary websites and trusted services were used in a redirect chain to obscure the final malicious destination and evade automated security controls

Sophisticated Browser-in-the-Browser (BitB) Phishing Campaign Targets OAuth Credentials

Tactics	Techniques	Observed Activity
Initial Access	Phishing (T1566)	Fake browser pop-up mimicking OAuth login to trick users into entering credentials
Credential Access	Input Capture (T1056)	Credential harvesting via embedded login form within fake window
Defense Evasion	Obfuscated Files or Information (T1027)	Text fragmentation and dynamic string splitting to evade detection
Defense Evasion	Disable or Modify Tools (T1562)	Console method hijacking to prevent debugging and analysis
Discovery	System Information Discovery (T1082)	Detection of operating system and browser to tailor attack appearance
Defense Evasion	Virtualization/Sandbox Evasion (T1497)	Redirecting bots/scanners to benign pages to evade automated analysis
Execution	JavaScript (T1059.007)	Use of client-side scripts to render fake interface and execute attack logic

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
ActiveMQ	An open-source message broker used in enterprise environments to move data between systems and applications. In the newsletter, a vulnerability in ActiveMQ could allow attackers to run code remotely.
Administrative Actions	Changes or operations performed with elevated privileges inside a system or application. Unauthorized administrative actions can let attackers alter settings, create access, or disrupt operations.
Affiliate / Affiliates	Individuals or groups that use another actor's tools or services to run their own attacks. In cybercrime, affiliates often license malware or phishing infrastructure from operators.
AI-Themed Lures	Fake files, documents, or messages designed to look related to artificial intelligence topics in order to attract victims and encourage them to open malicious content.
AMQP	Advanced Message Queuing Protocol. A communication method used by message brokers such as RabbitMQ; in the newsletter, malware used it as a command channel to blend into normal traffic.
Apache ActiveMQ	An enterprise message broker platform. The newsletter covered a vulnerability in this product that could lead to remote code execution.
API	Application Programming Interface. A method software uses to communicate with other software or services. Attackers often abuse trusted APIs to hide malicious operations inside normal-looking traffic.
APK	Android Application Package. The file format used to install Android apps. Malicious APKs were used in the newsletter to impersonate banking applications.
Application Context	The active environment in which a program or web application runs. If an attacker can run code in the application context, they may act with that application's permissions.

Arbitrary Code Execution	The ability for an attacker to make a system run commands or software of their choosing. This is one of the most serious outcomes of a vulnerability.
AsynRAT / AsyncRAT	A remote access trojan included in one of the campaigns in the newsletter. It gives attackers ongoing control over infected systems.
Attack Chain	The sequence of steps used by an attacker from initial entry to final impact. This can include phishing, malware delivery, persistence, remote control, and data theft.
Attack Surface	All the systems, applications, services, and exposed points an attacker could potentially target. A larger attack surface generally creates more opportunities for compromise.
Authentication Bypass	A flaw that allows attackers to get past login or identity checks without proper credentials. This can lead to unauthorized access to internal systems or services.
AutoHotkey	A Windows scripting and automation tool. In the newsletter, attackers used AutoHotkey-based loaders to help deliver malware into memory.
BitB	Browser-in-the-Browser. A phishing method where a web page creates a fake browser pop-up to trick users into entering credentials into a fake login prompt.
BitLocker	A Windows security feature used to protect data on disks. The newsletter covered vulnerabilities that could weaken or bypass this protection.
BLUERABBIT	A Golang-based backdoor described in the newsletter. It supports remote access, data theft, encryption, and destructive wiping functions.
BOF	Beacon Object File. A modular payload format that attackers can load after compromise to add new capabilities without deploying a full new malware package.
Bot / Bot Management Interface	A compromised machine under attacker control is often called a bot. A bot management interface is the control panel attackers use to view and manage infected systems.
Browser Profile Cloning	A technique that copies a victim's browser environment so an attacker can reuse a session and appear more like the legitimate user. This helps bypass some fraud and session protections.
Browser Session Abuse	Misuse of an already authenticated web session, often to access accounts or services without needing a password again.
C2 / Command and Control	Systems or channels used by attackers to communicate with infected devices, issue instructions, and receive stolen data or results.
Certificate Validation	A check used to verify the legitimacy of a certificate during secure communication. Weaknesses in this process can lead to authentication bypass or impersonation.
Chrome V8	The JavaScript engine inside Google Chrome. The newsletter referenced an actively exploited flaw in V8 that could allow code execution through crafted web content.
ClickFix	A social engineering technique that tricks a user into copying, pasting, or running commands that trigger malware infection.
Cloud Foundation Operations	A VMware management product covered in the newsletter. Stored XSS issues in this platform could allow malicious scripts to run inside the application context.
Cloud Storage Exfiltration	The theft of data by uploading it to cloud-based storage services controlled by attackers. This can help conceal data movement within normal-looking network traffic.
Credential Theft	The theft of usernames, passwords, tokens, cookies, or other access data. This is often used to gain unauthorized access without needing to exploit a system directly.
Critical Vulnerability	A severe flaw with high potential impact, often including remote code execution, authentication bypass, or complete compromise of a system.
Cross-Site Scripting (XSS)	A vulnerability that lets attackers inject malicious script into a trusted web application. When another user views the content, the script can run in their browser.
CSC	UAE Cyber Security Counsil
CTFMON	Collaborative Translation Framework Monitor. A Windows component referenced in a publicly disclosed elevation of privilege vulnerability in the Microsoft update summary.

CVE	Common Vulnerabilities and Exposures. The standard naming system used to identify publicly known security flaws.
Data Exfiltration	The unauthorized copying or transfer of data out of a network or system. It is often a precursor to extortion, fraud, or further compromise.
Data Exposure	The unauthorized access, viewing, or leakage of sensitive information. This can result from theft, misconfiguration, account compromise, or extortion activity.
Defacement	The unauthorized modification of content, often on websites or web applications. It is typically used to signal compromise or disrupt normal operations.
Developer Environment	Systems and tools used by software developers to write, test, or deploy code. These are increasingly targeted because they often hold elevated access, secrets, or production pathways.
Disk Wiping	The deliberate destruction of data on a drive by overwriting it. This can make systems unusable and recovery difficult or impossible.
Domain-Joined Endpoint	A workstation or server connected to a corporate identity domain. These devices often have access to central resources and are higher-value targets if compromised.
DPRK	Short for Democratic People's Republic of Korea. In the newsletter, some activity was described as DPRK-linked, meaning it was assessed to overlap with North Korea-aligned tradecraft.
Elevation of Privilege (EoP)	A weakness or technique that allows an attacker to gain higher permissions than they were supposed to have, such as moving from a regular user account to administrator or root.
EMHub	Environment Management Hub. A PeopleSoft component referenced in the Oracle exploitation activity described in the newsletter.
Endpoint	Any device such as a laptop, workstation, server, or mobile device that connects to a network and can be targeted or monitored.
Enterprise Messaging Traffic	Business application traffic used internally for communication between systems, such as message brokers. Attackers may use similar traffic patterns to hide malicious communications.
Exploit / Exploitation	The act of taking advantage of a vulnerability or weakness to gain unauthorized access, run code, or achieve another malicious goal.
Exploit Chain	A sequence of weaknesses, tricks, or actions combined together to move from limited access to broader compromise.
Extortion	A tactic where attackers threaten to publish, sell, destroy, or continue abusing stolen data unless a payment or other demand is met.
Firewall Rule	A configuration that controls what network communications are allowed or blocked. Attackers may create or abuse firewall rules to maintain access or disguise activity.
Gaia / Gaia Embedded	Operating platforms referenced in the VPN vulnerability entry. The disclosed authentication bypass affected systems running these platforms under vulnerable configurations.
GitHub-Hosted Payload	Malicious code or files stored on a GitHub repository to make delivery appear more legitimate or blend into trusted traffic patterns.
GlobalProtect	A remote access VPN service. The newsletter described exploitation attempts against GlobalProtect through a PAN-OS authentication bypass.
Golang	A programming language also known as Go. Several malware families in threat reporting are developed in Golang because it supports cross-platform and self-contained binaries.
Graph API	A Microsoft interface used to access data and services in the Microsoft cloud ecosystem. In the newsletter, malicious code used it as part of command-and-control.
Hidden Attribute	A file setting that makes a file less visible to normal users. Attackers use hidden files to disguise malware components inside seemingly harmless archives or directories.
High-Severity Vulnerability	A serious flaw with the potential to cause meaningful security impact, though not always as severe as a Critical-rated vulnerability.

Host Profiling / System Profiling	The collection of information about a device, such as operating system, hardware, network settings, software, and security tools. Attackers use profiling to decide what actions to take next.
HTTP.sys	A Windows component that handles HTTP protocol processing. The newsletter included both denial-of-service and remote code execution issues affecting it.
HVNC	Hidden Virtual Network Computing. A covert remote control method that lets attackers interact with a victim system without obvious user-visible signs like mouse movement or open windows.
Hyper-V	Microsoft's virtualization technology. The June 2026 updates included multiple Hyper-V remote code execution vulnerabilities.
Identity Provider	A system that manages user login and authentication for applications and services. Attackers often imitate trusted identity providers in phishing campaigns.
IKEv1	Internet Key Exchange version 1. A legacy VPN key exchange method. In the newsletter, it was one of the required conditions for a Check Point authentication bypass.
Incident Response	The process an organization follows to investigate, contain, and recover from a security incident.
Indicator of Compromise (IOC)	A sign that a system may have been attacked, such as suspicious IP addresses, unusual log events, or malicious file hashes.
Initial Access	The first successful entry point an attacker gains into an environment, such as through phishing, stolen credentials, or exploitation of an internet-facing system.
In-Memory Injection	A technique where malicious code is loaded directly into memory instead of written to disk. This can reduce obvious file-based traces and complicate detection.
Internet-Facing System	A system that is reachable directly from the internet. These are often prioritized for patching because attackers can target them remotely.
Investigative / Telemetry Signals	Observations from logs, network flows, process activity, or security tools that help defenders identify suspicious behavior.
JMX	Java Management Extensions. A management framework for Java applications. If exposed or misused, it can give attackers a path to sensitive operations.
Jolokia	A JMX-over-HTTP bridge used by ActiveMQ. The vulnerability described in the newsletter was triggered through this exposed interface.
Jumbo Hotfix Accumulator	A cumulative hotfix package used in some products. Applying the latest accumulator was part of the remediation guidance in the VPN vulnerability entry.
KDC	Key Distribution Center. A core Kerberos service used for authentication in Windows environments. The newsletter listed a remote code execution issue affecting this component.
KEV	Known Exploited Vulnerability. A catalog of vulnerabilities that have already been observed being used in real attacks.
Key Install Event	A VPN log event noted as an indicator of successful exploit activity in the VPN authentication bypass entry.
Lateral Movement	The movement of an attacker from one compromised system to others inside the same environment. This is often done after initial access to reach sensitive systems or accounts.
Legacy Client Support	Continued support for older software or connection methods. While useful for compatibility, it can increase risk when attackers abuse outdated protocols or behaviors.
Linux Kernel	The core component of the Linux operating system. Vulnerabilities in the kernel can have serious impact because they affect the most privileged part of the system.
Loader	Malware or a malicious component whose job is to deliver, decrypt, unpack, or launch another payload.
Local Privilege Escalation	A technique where someone with limited access on a machine gains higher privileges, such as administrator or root.

Malware-as-a-Service (MaaS)	A criminal service model where malware is rented or sold to other operators, often with updates and support included.
Memory Corruption	Damage or unintended changes to computer memory caused by a flaw. Many serious vulnerabilities begin as memory corruption issues because they can lead to crashes or code execution.
MeshCentral Agent	A remote management component referenced in the Oracle PeopleSoft exploitation reporting. It was described as being customized and used as part of attacker operations.
Microsoft Defender	Microsoft's security product suite for endpoint protection. The newsletter included an actively exploited elevation of privilege vulnerability affecting Defender.
MinIO	An S3-compatible object storage platform. In the newsletter, it was used by malware to exfiltrate stolen data to attacker-controlled storage.
Mobile Access VPN	A remote access service that allows users to connect to internal networks from outside the organization. It was one of the affected components in the Check Point vulnerability.
Multi-Stage Infection Chain	An attack flow where one script, file, or action reveals or launches the next stage instead of deploying the final malware immediately.
nf_tables	A Linux kernel subsystem used for network packet filtering and firewall rules. The newsletter described a flaw in this subsystem that could allow local root access.
NFC	Near Field Communication. A short-range wireless communication method used by payment cards and devices. In the newsletter, malware abused NFC functions to harvest card-related data.
NFCShare	An Android banking fraud malware family described in the newsletter. It was used in phishing flows that tricked victims into installing fake banking app updates.
OAuth	A common framework used to authorize access and support modern sign-in flows. Attackers often imitate OAuth login prompts to steal credentials.
Oracle PeopleSoft	An enterprise application platform used for business operations. The newsletter described exploitation activity involving a PeopleSoft Environment Management weakness.
Out-of-Bounds Read / Write	A type of memory safety flaw where software reads from or writes to memory outside its intended range. This can lead to crashes, data leaks, or code execution.
PAN-OS	The operating software for certain firewall and security appliances. The newsletter described active exploitation of a PAN-OS authentication bypass affecting remote access functions.
Patch Tuesday	Microsoft's regular monthly release cycle for security updates. The newsletter summarized the June 2026 Patch Tuesday release.
Payload	The main malicious code or capability delivered by an attack. A payload may steal data, provide remote access, encrypt files, or perform other harmful actions.
PeopleTools	A technical framework used by Oracle PeopleSoft. The Oracle vulnerability in the newsletter affected PeopleTools versions.
Persistence	Techniques attackers use to stay on a system after the initial compromise, such as scheduled tasks, registry changes, or startup triggers.
Phishing	A fraudulent technique used to trick people into revealing information, opening malicious content, or taking unsafe actions.
Phishing-as-a-Service (PhaaS)	A criminal service model that provides ready-made phishing kits, templates, infrastructure, or hosting for other attackers to use.
PoC / Proof of Concept	A test or demonstration showing that a vulnerability can be exploited. Public release of a PoC can increase the risk of wider abuse.
Privilege Escalation	Another term for elevation of privilege. It refers to gaining more access rights than originally granted.
Quick Mode	A stage in VPN negotiation referenced in the authentication bypass entry. Successful Quick Mode activity was noted as part of exploit detection.

RabbitMQ	A message broker platform. BLUERABBIT used RabbitMQ over AMQP as a tasking channel to disguise its control traffic as normal enterprise messaging.
Ransomware	Malware that encrypts files or disrupts systems to pressure victims into paying a ransom. Some modern operations also steal data first to increase extortion pressure.
RAT	Remote Access Trojan. Malware that allows attackers to remotely control a compromised device, often while also spying, stealing data, or installing additional payloads.
RCE	Remote Code Execution. A highly serious vulnerability impact allowing an attacker to run code on a target system from a remote location.
Reconnaissance	Information gathering performed by attackers on a target system or organization to understand what to target next.
Redis	A data platform used in BLUERABBIT for operational state handling. It helped separate control and result tracking from other attacker functions.
Remote Access VPN	A service that lets users connect into internal corporate systems from outside the organization. Weaknesses in this area can have major business risk because they expose internal networks.
Remote Desktop Client	A Microsoft client used to connect to remote systems. The June 2026 update included multiple vulnerabilities affecting this component.
Remote Management Agent	Software used to administer systems remotely. Attackers may abuse legitimate or modified remote management tools after exploitation.
Root	The highest privilege level on Linux and Unix-like systems. If an attacker gets root access, they typically gain full control of the device.
Sandbox / Sandboxed iframe	A controlled or restricted execution environment. Attackers may still abuse sandboxed structures to separate visible decoys from hidden malicious logic.
Scheduled Task	A system feature used to run programs automatically at set times or events. Attackers often abuse scheduled tasks to maintain persistence.
Session Hijacking	Taking over an already authenticated session so an attacker can act as the legitimate user without logging in normally.
Session Protection	Controls that make it harder to reuse or steal an authenticated session, such as device checks, IP checks, or tied browser attributes.
SharePoint	A Microsoft collaboration platform. In the VS Code extension campaign, it was used as part of the attacker's command-and-control and data handling design.
ShinyHunters	The name associated with the extortion activity linked to Oracle PeopleSoft exploitation in the newsletter.
SilabRAT	A subscription-based remote access trojan described in the newsletter. It focuses on credential theft, browser session abuse, wallet-related theft, and hidden remote control.
SLIME88	The China-nexus threat actor name referenced in the Apache ActiveMQ exploitation reporting in the newsletter.
SniperDz	The name of the phishing and push-notification service ecosystem discussed in the newsletter. It supported phishing, browser notification abuse, and other monetization methods.
Social Engineering	Manipulating people into taking unsafe actions, such as clicking links, entering credentials, or executing content that leads to compromise.
SoxAgent	The malware referenced in the ActiveMQ exploitation reporting as a follow-on payload deployed after successful exploitation.
Stored XSS	Stored Cross-Site Scripting. Malicious script is saved inside an application and runs later when viewed by users, especially those with higher privileges.
Supply Chain Risk	Security risk that comes through software, services, tools, or third-party components an organization trusts. Malicious extensions and compromised developer tooling are examples.

Threat Actor	An individual, criminal group, or state-linked group carrying out malicious cyber activity.
Threat Group / Campaign Name	A label used in reporting to track a specific threat actor or cluster of related activity over time.
Trusted Platform Abuse	The misuse of trusted software, cloud tools, repositories, or business services to make malicious activity appear legitimate.
UAF / Use-After-Free	A software flaw where memory is accessed after it has already been released. This can lead to crashes, privilege escalation, or code execution.
Unauthorized Administrative Actions	Actions carried out with privileged application or system rights without legitimate approval. This can include changing settings, creating access, or manipulating content.
Unauthorized VPN Connection	A VPN session established without valid or intended authentication. This gives attackers remote access to internal environments.
UNK_DeadDrop	The threat cluster name used in the newsletter for a phishing campaign targeting developers through fake recruitment and repository-based lures.
V8	Google Chrome's JavaScript engine. A high-severity out-of-bounds memory access issue in V8 was confirmed as actively exploited in the wild.
Views / Text Widgets / Policies	Application features referenced in the VMware stored XSS vulnerabilities. Privileged users could abuse these features to save malicious content in the management interface.
Virtual Private Network (VPN)	A technology that gives remote users or systems secure access into internal networks. Because it reaches internal environments directly, VPN compromise is especially serious.
VMware Aria Operations	A management and operations platform referenced in the stored XSS vulnerability entry.
VMware Cloud Foundation	A VMware platform for managing infrastructure and operations. The newsletter covered stored XSS flaws in related operations components.
VNC	Virtual Network Computing. A remote desktop-style control method. Some malware in the newsletter used VNC-like or hidden remote access capabilities.
VS Code	Visual Studio Code. A widely used developer tool that was abused in multiple newsletter entries through malicious repositories and extensions.
VSIX	The package format used for Visual Studio Code extensions. Malicious VSIX files were used to hide backdoor functionality inside trusted-looking developer tools.
WebSocket	A persistent communication method used by web applications or software. In the newsletter, one campaign used it to send stolen card data to a remote endpoint.
Windows Sandbox / Browser Sandbox	A restricted security boundary designed to limit what code can do if exploited. Some vulnerabilities in the newsletter allowed code execution inside the sandbox, which can still be dangerous.
Zero-Day	A vulnerability that is exploited or disclosed before defenders have broadly applied a fix. These issues often require urgent response because attackers may already be using them.