TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	26/3/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 26 March 2026

9	4	0	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Finance Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a series of high-risk campaigns and vulnerabilities that pose significant threats to the financial services sector. Additionally, the Interlock ransomware campaign exploited a critical vulnerability in Cisco's firewall software, while the Contagious Trader campaign from North Korea targeted cryptocurrency users through malicious trading bots. These campaigns employed sophisticated techniques such as social engineering, malware deployment via trusted platforms, and exploitation of zero-day vulnerabilities. The relevance of these threats to financial institutions cannot be overstated, as they expose organizations to risks of operational disruption, data theft, and reputational damage. The targeting of critical infrastructure and financial entities indicates a broader trend of cyber espionage and ransomware tactics that could disrupt financial flows and relationships in the region. As these campaigns evolve, financial institutions must remain vigilant and proactive in their cybersecurity measures, particularly as they navigate an increasingly complex threat landscape.

ADGM THREAT INTELLIGENCE SUMMARY

MuddyWater Campaign Continues [Campaign] [High]

Cyber Actors Leverage Telegram for Malware Deployment [Campaign] [High]

Interlock Ransomware Campaign Exploits Critical Cisco Firewall Vulnerability [Campaign] [High]

Boggy Serpens Campaign Targets Critical Sectors with Advanced Cyber Espionage Techniques [Campaign] [High]

North Korean Campaign "Contagious Trader" Targets Cryptocurrency Users with Malicious Trading Bots [Campaign] [High]

GhostClaw Campaign Leverages GitHub Repositories to Deliver macOS Infostealer [Campaign] [Medium]

Multi-Stage Stealer Campaign Utilizes Fake CAPTCHA Mechanism [Campaign] [Medium]

RoadK1ll Campaign Leverages WebSocket-Based Implant for Network Pivoting [Campaign] [Medium]

Claude Fraud Campaign Targets Developers with Malicious AI Tools [Campaign] [Medium]

Critical Remote Code Execution Vulnerability in Microsoft SharePoint Actively Exploited [Vulnerability] [High]

Multiple High-Severity Vulnerabilities in Apple Products Exploited by Threat Actors [Vulnerability] [High]

Apple Addresses WebKit Vulnerability Affecting iPhones, iPads, and Macs [Vulnerability] [Medium]

Oracle Addresses Critical Severity Flaw in Multiple Products [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
MuddyWater Campaign Continues	HIGH	CLEAR	Campaign	Open Source

Executive Summary

In early February 2026, the cyber espionage group MuddyWater conducted a coordinated intrusion campaign. This campaign utilized two malware families, Dindoor and Fakeset, to establish persistent access and facilitate data exfiltration.

This campaign may impact organizations in the financial services sector. The targeting of a financial institution, among other critical sectors, highlights the potential for intelligence gathering and operational leverage that could affect financial flows and relationships in the region. Financial institutions should remain vigilant as this campaign reflects a broader trend of using legitimate cloud services to obscure malicious activities.

Technical Details

- The campaign leveraged Dindoor, a backdoor utilizing the Deno runtime, allowing operators to bypass traditional detection controls.
- Fakeset, a Python-based implant, was also deployed, maintaining a lineage with previous MuddyWater malware families through reused code-signing certificates.
- The operators established persistent access through legitimate cloud infrastructure, reducing overt indicators of compromise.
- Data exfiltration was attempted using Rclone, directing information to a Wasabi cloud storage bucket, complicating detection efforts.
- The campaign reflects a shift towards low-signature, behavior-driven intrusion techniques, minimizing reliance on traditional command-and-control infrastructure.
- Each target was selected based on its strategic value, providing insights into financial flows and potential disruption opportunities.
- The use of legitimate cloud platforms allowed the adversaries to blend malicious traffic with routine enterprise network activity.
- The absence of detailed atomic indicators suggests a high-tier intelligence operation, with an emphasis on maintaining operational security.
- MuddyWater has historically targeted sectors such as government, telecommunications, and finance, indicating a sustained interest in critical infrastructure.

Recommendations

- Financial institutions should enhance monitoring of cloud service usage to detect anomalous activities.
- Implement multi-factor authentication (MFA) across all access points to reduce the risk of unauthorized access.
- Conduct regular security assessments to identify and mitigate vulnerabilities in cloud infrastructure.
- Train employees on recognizing phishing attempts and other social engineering tactics commonly used in cyber espionage.
- Collaborate with threat intelligence sharing platforms to stay informed about emerging threats and tactics used by adversaries.

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
Cyber Actors Leverage Telegram for Malware Deployment	HIGH	CLEAR	Campaign	Open Source

Executive Summary

The cyber actors utilize Telegram as a command-and-control (C2) infrastructure to deploy malware, leading to intelligence collection, data leaks, and reputational harm against targets.

The use of Telegram for C2 increases the risk of compromise for those engaged in sensitive communications. Organizations in the region should be aware of the potential for reputational damage and intelligence breaches, necessitating immediate attention from network defenders.

Technical Details

- Cyber actors deploy multiple versions of malware targeting Windows operating systems.
- The malware campaign features a multi-stage payload that enables remote access to infected devices.
- The first stage of the malware masquerades as commonly used applications to deceive victims.
- The second stage connects the infected machine to Telegram command and control bots for data exfiltration.

- The attack chain begins with social engineering tactics via messaging applications, posing as known contacts.
- Victims are convinced to accept file transfers containing the masquerading stage 1 malware.
- Once executed, the malware installs a persistent implant (stage 2) for ongoing access and further downloads.
- The malware employs defensive evasion techniques and modifies the Windows registry for autorun capabilities.
- Various samples are used for data exfiltration, including screen recordings and audio captures.

Recommendations

- Ensure devices are updated with the latest operating system and install software updates regularly.
- Only download software from trusted sources, such as official app stores or vendor websites.
- Enable antivirus or anti-malware software on devices and run scans regularly.
- Use strong, unique passwords and enable multi-factor authentication.
- Remain vigilant against social engineering tactics employed by potential threat actors.

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
Interlock Ransomware Campaign Exploits Critical Cisco Firewall Vulnerability	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Amazon threat intelligence has identified an active Interlock ransomware campaign exploiting CVE-2026-20131, a critical vulnerability in Cisco Secure Firewall Management Center Software. This vulnerability allows unauthenticated, remote attackers to execute arbitrary Java code as root on affected devices, with exploitation beginning 36 days prior to the public disclosure of the vulnerability.

This campaign may impact organizations in the financial services sector that utilize Cisco Secure Firewall Management Center. As attackers leverage zero-day vulnerabilities to gain initial access, organizations should be aware of the potential for operational disruption and financial loss, particularly in sectors where ransomware operators typically exert maximum pressure for payment.

Technical Details

- The campaign exploits CVE-2026-20131, allowing remote code execution on Cisco Secure Firewall Management Center.
- Interlock began exploiting this vulnerability 36 days before its public disclosure, indicating a zero-day exploit.
- A misconfigured infrastructure server exposed Interlock's operational toolkit, revealing their multi-stage attack chain.
- The attack involves custom remote access trojans (RATs) and reconnaissance scripts for mapping victim networks.
- Command-and-control communication is conducted over encrypted WebSocket connections, complicating detection efforts.
- Interlock uses legitimate tools like ConnectWise ScreenConnect alongside custom malware for redundancy.
- The operational toolkit includes a PowerShell script for systematic Windows environment enumeration post-compromise.
- A memory-resident webshell is utilized to evade traditional file-based detection methods.
- The campaign has historically targeted sectors such as education, healthcare, and government for maximum disruption.

Recommendations

- Organizations should immediately apply Cisco's security patches for the affected firewall software.
- Conduct thorough reviews of logs for indicators of compromise related to this campaign.
- Implement continuous threat monitoring and hunting capabilities to detect unusual network activity.
- Educate security teams on the tactics, techniques, and procedures employed by Interlock.
- Regularly test incident response procedures to prepare for potential ransomware scenarios.

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
Boggy Serpens Campaign Targets Critical Sectors with Advanced Cyber Espionage Techniques	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at Palo Alto Networks have been tracking ongoing cyberespionage campaigns by the threat

group Boggy Serpens. This group consistently targets critical infrastructure across the Middle East. Their operational strategy has evolved to focus on trusted relationship compromises and multi-wave targeting of key organizations.

This campaign may impact various sectors, including financial services.

Technical Details

- Boggy Serpens employs hijacked accounts to initiate attacks, targeting high-profile victims such as diplomats and IT vendors.
- The group utilizes social engineering techniques alongside advanced malware, including AI-enhanced implants designed for long-term persistence.
- Recent campaigns against a national marine and energy company demonstrate the group's commitment to infiltrating regional critical infrastructure.
- The attackers have refined their operational approach, leveraging AI-generated code and Rust-based tools like the BlackBeard backdoor for rapid deployment.
- Command and control (C2) mechanisms include standard HTTP status codes and customized UDP-based traffic.
- The group has shifted from high-volume, low-sophistication tactics to more stealthy and persistent methods, enhancing their defense evasion capabilities.
- Boggy Serpens is now targeting more than just government entities and has begun focusing on key economic sectors.
- The group's recent activities indicate a significant increase in resource allocation and cross-unit coordination.
- Their phishing campaigns have become more tailored, utilizing specialized toolkits for mass email distribution and account exploitation.

Recommendations

- Financial institutions should implement multi-factor authentication (MFA) to protect against account hijacking.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by advanced malware.
- Conduct employee training on recognizing social engineering tactics to reduce the risk of successful phishing attempts.
- Monitor network traffic for unusual patterns that may indicate command and control activity.
- Establish incident response protocols to quickly address any suspected compromises or breaches.

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
North Korean Campaign "Contagious Trader" Targets Cryptocurrency Users with Malicious Trading Bots	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a sophisticated malware campaign named "Contagious Trader," attributed with high confidence to North Korea's Lazarus Group. This campaign leverages malicious cryptocurrency trading bot projects on GitHub, which are designed to exfiltrate sensitive files and private keys from users. The campaign is highly active and utilizes various techniques, including malicious npm dependencies, to achieve its objectives.

The potential impact of the Contagious Trader campaign on the financial services sector is notable, particularly for organizations involved in cryptocurrency and digital asset management. The use of enticing trading bot themes may attract unsuspecting users, leading to unauthorized access to sensitive information. Financial institutions should be aware of the evolving tactics employed by threat actors in this space and consider the implications for their security posture.

Technical Details

- The campaign utilizes malicious cryptocurrency trading bot projects hosted on GitHub, designed to lure cryptocurrency users.
- Several of the GitHub projects are created to exfiltrate sensitive files and private keys through various methods.
- Malicious npm packages are employed as part of the infection chain, consistent with tactics used by North Korean threat actors.
- The campaign has a significant footprint on GitHub, with numerous repositories and npm packages identified as malicious.
- Direct exfiltration methods include sending data to actor-controlled HTTP endpoints and databases.
- The campaign features a variety of infection points, including poisoned GitHub projects and transitive npm dependencies.
- The use of Base64-encoded exfiltration endpoints is a common technique observed in the campaign.
- Some repositories have been observed to contain hardcoded database connection strings for direct data exfiltration.
- The trading bot theme is a consistent element across all identified malicious repositories, suggesting organized operations.
- The campaign is linked to the FAMOUS CHOLLIMA group, which is part of North Korea's offensive cyber capabilities.

Recommendations

- Financial institutions should implement strict monitoring of GitHub repositories related to cryptocurrency trading bots.
- Organizations should educate users about the risks associated with downloading and using third-party trading bots.
- Employ endpoint protection solutions that can detect and block malicious npm packages.
- Regularly audit and review access to sensitive information and private keys within cryptocurrency platforms.
- Consider implementing multi-factor authentication (MFA) to enhance security for accounts associated with cryptocurrency trading.

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
GhostClaw Campaign Leverages GitHub Repositories to Deliver macOS Infostealer	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Jamf Threat Labs have identified the GhostClaw malware campaign, which utilizes GitHub repositories and AI-assisted development workflows to distribute credential-stealing payloads targeting macOS systems. This campaign expands beyond traditional npm-based delivery methods, allowing attackers to reach a broader audience, including users executing commands from online sources.

This campaign may impact organizations in the financial services sector, as the malware is designed to harvest sensitive credentials. Financial institutions should be aware of the potential risks associated with executing code from unverified sources, particularly as attackers increasingly exploit trusted platforms and workflows to deliver malicious payloads.

Technical Details

- The campaign employs malicious GitHub repositories that impersonate legitimate tools, increasing their perceived credibility among users.
- Initial access is gained through README files that provide installation commands, encouraging users to execute shell commands that retrieve and run remote scripts.
- A variant of the campaign targets AI-assisted development workflows, where automated agents install external "skills" from GitHub, allowing malware execution with minimal user interaction.
- The infection chain begins with a bootstrapper script called "install[.]sh", which performs legitimate setup tasks while retrieving malicious payloads.

- The script uses the "-k" flag with curl to disable TLS certificate verification, reducing transport security during downloads.
- Credential theft is facilitated by a heavily obfuscated JavaScript file named "setup[.]js", which mimics legitimate installation processes to deceive users.
- The malware prompts users for credentials through fake terminal prompts and AppleScript dialogs, designed to resemble macOS security prompts.
- Once credentials are captured, the malware communicates with a command-and-control (C2) server to retrieve additional payloads.
- The campaign utilizes a consistent C2 infrastructure across multiple repositories, with unique identifiers for tracking interactions.
- Post-execution scripts are employed to obscure earlier activities and establish persistence within user-controlled directories.

Recommendations

- Financial institutions should implement strict code review processes for any scripts or commands sourced from online repositories.
- Educate employees about the risks of executing installation commands from unverified sources, particularly on GitHub.
- Utilize endpoint protection solutions that can detect and block suspicious script execution and credential theft attempts.
- Regularly monitor and audit command-and-control communications to identify potential malware activity.
- Encourage the use of multi-factor authentication to mitigate the impact of credential theft.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multi-Stage Stealer Campaign Utilizes Fake CAPTCHA Mechanism	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at LevelBlue have identified a multi-stage malware campaign that leverages a network of compromised legitimate websites to redirect victims to fake CAPTCHA verification pages. These pages deliver credential-stealing payloads through a ClickFix social engineering method, showcasing a broad operational scope with at least six distinct malware families observed. The campaign has been active for a confirmed operational window of at least six months, indicating a sustained threat landscape.

This campaign may impact organizations in the financial services sector as it utilizes compromised websites across various industries, including finance. The use of fake CAPTCHA pages to harvest credentials and deliver malware poses risks to sensitive data and operational integrity, necessitating vigilance from financial institutions to mitigate potential exploitation of their users.

Technical Details

- The campaign employs a ClickFix social engineering method, prompting users to execute malicious commands via a fake browser security alert.
- More than two dozen legitimate websites have been compromised to redirect users to fake CAPTCHA domains, indicating widespread opportunistic targeting.
- The infrastructure includes domains masquerading as cryptocurrency exchanges, enhancing the legitimacy of the attack.
- A defensive mechanism is implemented to hinder analysis by freezing the page when Developer Tools are opened.
- The clipboard hijacking script replaces the user's clipboard content with a malicious PowerShell command after user interaction with a fake verification checkbox.
- The PowerShell command retrieves and executes scripts entirely in memory, avoiding the creation of persistent file artifacts.
- The first-stage server delivers a script that maintains user engagement while the second stage is fetched in the background.
- The second script allocates executable memory to run shellcode, ensuring stealth during execution.
- The payload is executed from memory, further complicating detection efforts by security solutions.
- The campaign's geographic reach spans multiple countries and targets various sectors, including finance.

Recommendations

- Implement robust web filtering solutions to block access to known malicious domains associated with this campaign.
- Educate employees about the risks of social engineering tactics, particularly regarding fake security prompts.
- Employ endpoint detection and response (EDR) solutions to monitor for suspicious PowerShell activity and clipboard manipulation.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by similar campaigns.
- Encourage the use of multi-factor authentication (MFA) to protect sensitive accounts from credential theft.

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
RoadK1ll Campaign Leverages WebSocket-Based Implant for Network Pivoting	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Blackpoint Response Operations Center (BROC) have identified a NodeJS-based implant named RoadK1ll, designed to maintain reliable access to internal networks after an initial compromise. This implant establishes outbound WebSocket connections to attacker-controlled infrastructure, enabling TCP traffic brokering without requiring inbound listeners on the victim host.

This campaign may impact organizations in the financial services sector as it allows attackers to utilize a compromised machine as a relay point for accessing internal systems and services. The stealthy nature of RoadK1ll, which blends into normal network traffic, could pose risks to sensitive financial data and operations, making it essential for organizations to remain vigilant against such threats.

Technical Details

- RoadK1ll operates as a reverse tunneling implant, establishing outbound WebSocket connections to facilitate TCP traffic management.
- It uses a custom protocol that carries multiple streams of traffic over a single WebSocket connection, improving flexibility.
- The implant imports NodeJS modules "net" for TCP socket handling and "ws" for WebSocket communication, bridging two operational environments.
- Connection settings include parameters like VPS_HOST, VPS_WS_PORT, and TUNNEL_SECRET for authentication and reconnection management.
- RoadK1ll defines a message structure with a 4-byte channel identifier and a 1-byte message type, allowing for efficient communication.
- The implant can manage multiple concurrent connections, enabling lateral movement within the compromised network.
- It employs a reconnect mechanism to restore the WebSocket tunnel automatically if the connection drops, ensuring persistent access.
- The implant's design avoids traditional persistence methods, relying instead on maintaining an active process for access.
- RoadK1ll's functionality allows operators to dynamically create connections to internal systems, bypassing perimeter defenses.
- The implant's traffic forwarding capabilities facilitate bidirectional communication between the attacker and internal systems.

Recommendations

- Implement strict network segmentation to limit lateral movement opportunities for potential intruders.

- Monitor outbound WebSocket traffic for unusual patterns that may indicate the presence of implants like RoadK1ll.
- Employ endpoint detection and response (EDR) solutions to identify and mitigate unauthorized access attempts.
- Regularly update and patch systems to reduce vulnerabilities that could be exploited for initial compromise.
- Conduct security awareness training for employees to recognize and report suspicious activities.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Claude Fraud Campaign Targets Developers with Malicious AI Tools	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at 7AI have identified a sophisticated malware campaign named Claude Fraud, which exploits the Claude[.]ai and VS Code brands to target developers and security professionals. The campaign utilizes Google Ads and fake landing pages to deliver the MacSync Infostealer on macOS and employs a trojanized VS Code extension to execute PowerShell silently on Windows. Over 15,600 victims have been documented publicly, highlighting the campaign's significant scale.

This campaign may impact organizations in the financial services sector, particularly those utilizing AI coding tools and developer environments. The deliberate targeting of technically sophisticated users and newer AI enthusiasts raises concerns about the exploitation of trust in legitimate platforms, making it essential for security teams to remain vigilant against such threats.

Technical Details

- The campaign operates through two confirmed attack vectors: malvertising via Google Ads and a malicious VS Code extension.
- On macOS, users are tricked into executing a terminal command that downloads the MacSync Infostealer via a base64-encoded string.
- The MacSync malware establishes command-and-control communication and targets macOS Keychain credentials, browser-stored login data, and cryptocurrency wallet private keys.
- On Windows, the malicious VS Code extension executes PowerShell commands to modify Windows Defender settings and download payloads.
- The execution chain observed includes "Code[.]exe" → "powershell[.]exe" → "mshta[.]exe", allowing for silent execution of malicious commands.
- The attackers leveraged compromised advertising accounts to run sponsored placements, enhancing the credibility of their malicious content.

- The campaign is actively maintained, with operators quickly adapting their infrastructure after takedowns of previous vectors.
- Detection signals include unusual process behavior and command chains that deviate from normal development workflows.
- The campaign exploits the growing adoption of AI coding tools, creating a new attack surface for threat actors.

Recommendations

- Hunt for the process chain "Code[.]exe" → "powershell[.]exe" → "mshta[.]exe" across Windows endpoints where VS Code is installed.
- Conduct audits of VS Code extensions on developer machines, focusing on recently installed extensions that invoke shell commands.
- Train users to treat sponsored search results advertising developer tools as potential phishing vectors.
- Implement ad-blocking controls via MDM or browser policy to reduce exposure to malicious advertisements.

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 Remote Code Execution Vulnerability in Microsoft SharePoint Actively Exploited	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

A critical remote code execution (RCE) vulnerability, identified as CVE-2026-20963, has been discovered in Microsoft SharePoint, allowing attackers to run malicious code remotely without authentication. This vulnerability arises from the insecure deserialization of untrusted data and is currently being actively exploited, posing a significant risk to affected systems.

Organizations in the financial services sector should be aware that this vulnerability may affect their operations, particularly if they utilize Microsoft SharePoint Server in their infrastructure. Given the high CVSS score of 9.8, immediate action is recommended to mitigate potential risks associated with ongoing exploitation.

Technical Details

- CVE ID: CVE-2026-20963 is a critical vulnerability with a CVSS score of 9.8.
- The vulnerability affects Microsoft SharePoint Server, including Subscription Edition, 2019, and Enterprise Server 2016.

- It is categorized as a Remote Code Execution (RCE) vulnerability, allowing attackers to execute arbitrary code.
- The vulnerability is actively exploited (listed in CISA's KEV), but no specific threat actor has been identified.

Recommendations

- Apply Microsoft security updates without delay across all affected SharePoint systems.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple High-Severity Vulnerabilities in Apple Products Exploited by Threat Actors	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Multiple high-severity vulnerabilities have been identified in Apple products, including iOS, macOS, and Safari. These flaws are actively exploited through maliciously crafted web content, often associated with sophisticated "watering hole" attacks. The vulnerabilities are part of the DarkSword exploit kit, which is utilized by various threat actors to deploy advanced malware capable of extensive data theft and remote code execution.

This situation may affect organizations in the financial services sector, particularly those utilizing Apple products for operations. Financial institutions should be aware that these vulnerabilities could lead to unauthorized access and data compromise, emphasizing the need for immediate action to mitigate potential risks.

Technical Details

- CVE-2025-31277 is a memory corruption vulnerability in WebKit, potentially triggered by malicious web content, allowing arbitrary code execution within the browser context.
- CVE-2025-43510 is a memory corruption flaw in the kernel, enabling a malicious application to manipulate shared memory, which may lead to privilege escalation or system compromise.
- CVE-2025-43520 is another kernel memory corruption vulnerability that could result in unexpected system termination or unauthorized writing to kernel memory, allowing elevated privileges or arbitrary code execution.
- These vulnerabilities affect various Apple products, including watchOS, iOS, iPadOS, macOS, visionOS, and tvOS.
- The exploitation of these vulnerabilities is linked to the DarkSword exploit kit, which has been leveraged by multiple threat actors.

- Attackers can deploy advanced malware families capable of extensive data theft and persistence through these vulnerabilities.
- The vulnerabilities are actively being exploited, highlighting the urgency for organizations to address them.
- Maliciously crafted web content is a common vector for these attacks, necessitating increased caution among users.
- The sophistication of the attacks may complicate detection and response efforts for affected organizations.

Recommendations

- Apply Updates Immediately: Ensure all Apple devices are updated to the latest available versions.
- Enable Automatic Updates: To reduce exposure to future vulnerabilities.
- Exercise Caution with Web Content: Avoid clicking on suspicious links or visiting untrusted websites.
- Monitor Systems: Watch for indicators of compromise, especially unusual data access or system instability.
- Deploy Security Controls: Implement network monitoring, endpoint protection, and threat detection solutions.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Apple Addresses WebKit Vulnerability Affecting iPhones, iPads, and Macs	**Medium**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Apple has released a Background Security Improvements update to address a WebKit vulnerability (CVE-2026-20643) that affects iPhones, iPads, and Macs. This flaw allows malicious web content to bypass browser security controls, potentially leading to unauthorized access to sensitive data and session hijacking.

This vulnerability may affect organizations in the financial services sector that utilize Apple devices, as successful exploitation could enable unauthorized access to sensitive data across different web domains. Financial institutions should be aware of this vulnerability and ensure that their systems are updated to mitigate potential risks.

Technical Details

- CVE-2026-20643 is a cross-origin policy bypass issue in WebKit with a high severity CVSS score of 8.8.
- The vulnerability exists in the Navigation API due to insufficient input validation, allowing crafted malicious web content to bypass the Same Origin Policy (SOP).

- Successful exploitation could enable unauthorized access to sensitive data across different web domains.
- Attackers could potentially hijack sessions or exfiltrate data from affected devices.
- The flaw allows execution of unintended actions in the context of trusted sites, increasing the risk of exploitation.
- Affected versions include iOS 26.3.1, iPadOS 26.3.1, macOS 26.3.1, and macOS 26.3.2.

Recommendations

- Ensure all Apple devices are updated to the latest versions released by Apple.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Oracle Addresses Critical Severity Flaw in Multiple Products	MEDIUM	CLEAR	Vulnerability	Open Source

Executive Summary

Oracle has issued a security alert regarding vulnerability CVE-2026-21992 affecting Oracle Identity Manager and Oracle Web Services Manager. This vulnerability is remotely exploitable without authentication, potentially allowing attackers to execute arbitrary code on affected systems if successfully exploited.

This vulnerability may affect organizations in the financial services sector that utilize Oracle's products, as it poses a risk of unauthorized access and control over critical systems. Financial institutions should remain vigilant and ensure they apply the necessary updates or mitigations as recommended by Oracle to safeguard their environments.

Technical Details

- The vulnerability CVE-2026-21992 is present in Oracle Identity Manager and Oracle Web Services Manager.
- It is remotely exploitable without requiring authentication, increasing the risk of exploitation.
- Successful exploitation may lead to remote code execution, allowing attackers to execute arbitrary commands.
- The vulnerability affects product versions under Premier Support or Extended Support phases.
- Earlier versions of affected releases are likely also vulnerable, necessitating upgrades to supported versions.

Recommendations

- Apply the latest security patches and updates provided by Oracle immediately.

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

back to top

Appendix A – 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 B – 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 C - Acronyms & Technical Terms

Term / Acronym	Meaning / Description
AI-enhanced implants	Malware that uses artificial intelligence techniques to improve its effectiveness and evasion capabilities.
APT	Advanced Persistent Threat: A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period.
Boggy Serpens	A cyber espionage group that targets critical infrastructure in the Middle East.
C2	Command-and-Control: A method used by cyber attackers to maintain communication with compromised systems to control them remotely.
ClickFix	A social engineering method used to trick users into executing malicious commands through fake security alerts.
Contagious Trader	A malware campaign attributed to North Korea's Lazarus Group that targets cryptocurrency users through malicious trading bots.
credential theft	The unauthorized acquisition of user credentials, often leading to account takeovers and data breaches.
CSC	UAE Cyber Security Council

CVE	Common Vulnerabilities and Exposures: A list of publicly disclosed cybersecurity vulnerabilities and exposures.
CVE-2025-31277	A memory corruption vulnerability in WebKit that can be exploited to execute arbitrary code within the browser context.
CVE-2025-43510	A kernel memory corruption flaw that may lead to privilege escalation or system compromise.
CVE-2025-43520	Another kernel memory corruption vulnerability that could result in unauthorized writing to kernel memory.
CVE-2026-20643	A WebKit vulnerability that allows malicious web content to bypass browser security controls, potentially leading to unauthorized access.
CVE-2026-20963	A critical remote code execution vulnerability in Microsoft SharePoint that allows unauthenticated attackers to execute arbitrary code.
CVE-2026-21992	A vulnerability in Oracle Identity Manager and Oracle Web Services Manager that is remotely exploitable without authentication.
CVSS	Common Vulnerability Scoring System: A standardized scoring system that rates the severity of vulnerabilities on a scale from 0 to 10.
DarkSword	An exploit kit used by various threat actors to deploy advanced malware capable of extensive data theft and remote code execution.
data exfiltration	The unauthorized transfer of data from a system, often by cybercriminals seeking sensitive information.
Dindoor	A backdoor malware used by the MuddyWater campaign to establish persistent access to compromised systems.
EDR	Endpoint Detection and Response: Security solutions that monitor endpoints for suspicious activities and respond to potential threats.
Fakeset	A Python-based implant used in the MuddyWater campaign to facilitate data exfiltration.
financial flows	The movement of money and financial transactions within and between organizations, which can be disrupted by cyber threats.
GhostClaw	A malware campaign that targets macOS systems to steal credentials using GitHub repositories for distribution.
Interlock	A ransomware campaign exploiting vulnerabilities in Cisco Secure Firewall Management Center, allowing remote code execution.
MacSync	An Infostealer malware used in the Claude Fraud campaign to target macOS Keychain credentials and other sensitive data.
malware	Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
MFA	Multi-Factor Authentication: A security process that requires two or more verification methods to gain access to a resource, enhancing security.
MuddyWater	Cyber espionage group.
operational disruption	Interruptions to normal business operations caused by cyber incidents, often resulting in financial losses.
operational security	Measures taken to protect sensitive information from being accessed by unauthorized individuals.
phishing	A cyber-attack that involves tricking individuals into providing sensitive information by masquerading as a trustworthy entity.
phishing	A cyber-attack that involves tricking individuals into providing sensitive information by masquerading as a trustworthy entity.
ransomware	A type of malware that encrypts a victim's files, demanding payment for the decryption key.
RAT	Remote Access Trojan: A type of malware that allows an attacker to control a system remotely, often used for data theft or espionage.
RCE	Remote Code Execution: A vulnerability that allows an attacker to execute arbitrary code on a remote system, often leading to full system compromise.
RoadK1ll	A NodeJS-based implant that establishes outbound WebSocket connections for maintaining access to internal networks.
social engineering	Manipulative tactics used by attackers to deceive individuals into divulging confidential information.

Telegram	A messaging application.
TTP	Tactics, Techniques, and Procedures: The behaviour or modus operandi of threat actors, used to describe how they conduct attacks.
zero-day vulnerability	A security flaw that is exploited by attackers before the vendor has released a fix, making it particularly dangerous.