ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	7/1/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 7 January 2026

1	0	7	2
Cyber Breach	Threat Actors	Campaigns	Vulnerability
Major Compromises and breaches	Threat actor activities in the UAE & Middle East impacting Finance Sector	Recent Threat campaigns within financial institutions	Actively Exploited & Critical Vulnerabilities

Summary

This week's cybersecurity newsletter highlights a series of significant threats and vulnerabilities impacting the financial services sector, particularly in the UAE and MENA region. Key incidents include a $3.9 million loss due to a multisig hijack at Unleash Protocol, the distribution of malicious software through a deceptive campaign targeting the Cardano community, and the identification of a critical Remote Code Execution vulnerability in MariaDB. Additionally, the emergence of advanced malware strains and exploitation techniques, such as the EDR-Freeze method and the HoneyMyte APT's use of kernel-mode rootkits, underscore the evolving threat landscape. Financial institutions are urged to enhance their security measures, conduct regular audits, and educate users on the risks associated with emerging threats to safeguard sensitive data and maintain operational integrity.

ADGM THREAT INTELLIGENCE SUMMARY

Unleash Protocol Suffers $3.9M Loss Due to Multisig Hijack [Cyber Breach] [Medium]

Suspicious "Eternl Desktop" Campaign Distributes LogMeIn Resolve via MSI Installer [Campaign] [High]

DarkSpectre Campaign Compromises Over 8.8 million Users through Browser Extensions [Campaign] [Medium]

Researchers Identify 'EDR-Freeze' Technique Targeting Endpoint Security in Financial Services [Campaign] [Medium]

RondoDoX Botnet Campaign Targets Web Apps and IoT Devices with React2Shell Exploitation [Campaign] [Medium]

New Strain of Shai Hulud Malware Detected in npm Package [Campaign] [Medium]

HoneyMyte APT Utilizes Kernel-Mode Rootkit and ToneShell Backdoor in Cyberespionage Campaign [Campaign] [Medium]

GlassWorm Campaign Targets macOS with Evolving Malware Techniques [Campaign] [Medium]

Critical Remote Code Execution Vulnerability in MariaDB Affects Backup Operations [Vulnerability] [High]

Critical Authentication Bypass Vulnerability in IBM API Connect [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Unleash Protocol Suffers $3.9M Loss Due to Multisig Hijack	MEDIUM	CLEAR	Cyber Breach	Open Source

Executive Summary

Unleash Protocol, a decentralized intellectual property platform, has lost approximately $3.9 million in cryptocurrency following an unauthorized contract upgrade that enabled asset withdrawals. The attacker gained administrative control over the multisig governance system, allowing them to execute this exploit without the approval of the Unleash team.

This incident is significant for the financial services sector as it highlights vulnerabilities in decentralized finance (DeFi) systems, particularly those utilizing multisig governance. The breach not only results in substantial financial losses but also raises concerns regarding the security of asset management protocols and the potential for similar attacks across the blockchain ecosystem.

Technical Details

- An unauthorized contract upgrade was executed, allowing asset withdrawals without approval.
- The attacker gained administrative control via Unleash’s multisig governance system.
- Stolen assets included WIP (wrapped IP), USDC, WETH (wrapped Ether), stIP (staked IP), and vIP (voting-escrowed IP).
- The unauthorized drain resulted in losses estimated at $3.9 million.
- The attacker used third-party infrastructure to bridge the assets to external addresses, enhancing obfuscation.
- Stolen funds were deposited into the Tornado Cash mixing service to obscure their origin.
- Tornado Cash has been previously sanctioned for facilitating money laundering activities.
- Unleash Protocol has paused all operations and initiated an investigation with external security experts.
- Users are advised against interacting with Unleash Protocol contracts until further notice.
- The incident underscores the need for robust security measures in DeFi platforms.

Recommendations

- Implement stricter access controls and monitoring for multisig governance systems.
- Regularly audit smart contracts to identify and mitigate vulnerabilities.
- Educate users on the risks associated with interacting with DeFi platforms.
- Establish incident response protocols to quickly address breaches and vulnerabilities.
- Collaborate with blockchain security experts to enhance overall platform security.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Suspicious "Eternl Desktop" Campaign Distributes LogMeIn Resolve via MSI Installer	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

A campaign targeting the Cardano community is distributing a suspicious MSI installer named "Eternl Desktop," which drops LogMeIn Resolve. The email promoting this software appears legitimate but raises significant concerns upon closer inspection of its download mechanism and installer behavior. The campaign employs social engineering tactics to create a sense of urgency and trust among users, leveraging references to Cardano's governance and token rewards.

The implications for the financial services sector are serious, as this campaign exemplifies how threat actors exploit crypto governance narratives to distribute covert access tools disguised as legitimate software. The use of Remote Monitoring and Management (RMM) tools within a wallet installer poses a high risk, as these tools can facilitate persistent access and potential credential harvesting on compromised systems.

Technical Details

- The campaign uses a professionally crafted email to promote the "Eternl Desktop" software, creating a false sense of legitimacy.
- The download URL is newly registered and lacks historical reputation, raising immediate concerns about its authenticity.
- The MSI installer is distributed without publicly available checksums or digital signatures, preventing users from verifying its integrity.
- The installer drops an executable named "unattended-updater.exe," which is associated with LogMeIn Resolve.
- The extracted executable attempts to connect to multiple domains, indicating potential command and control behavior.
- The software enables unattended access, allowing remote connections without user presence, which is a significant security risk.
- The campaign is flagged as potentially unwanted application (PUA) and exhibits behaviors consistent with remote management agents.
- The combination of a newly registered domain, MSI installer, and RMM tool indicates a high-risk scenario for users.
- The campaign is characterized by overlapping indicators consistent with supply-chain abuse and trojanized wallet distribution.
- It suggests preparation for follow-on activities, including credential harvesting or cryptocurrency wallet compromise.

Recommendations

- Financial institutions should educate users about the risks of unsolicited emails and software downloads, particularly in the crypto space.

- Implement strict email filtering to detect and block suspicious communications related to cryptocurrency.
- Monitor for unusual network traffic to newly registered domains associated with wallet software.
- Conduct regular security assessments to identify and mitigate risks associated with remote management tools.
- Encourage the use of multi-factor authentication (MFA) to protect sensitive accounts and assets.

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
DarkSpectre Campaign Compromises Over 8.8 million Users through Browser Extensions	MEDIUM	CLEAR	Campaign	CSC

Executive Summary

A sophisticated threat campaign attributed to the DarkSpectre actor has been identified, compromising over 8.8 million users globally through more than 300 malicious browser extensions. This campaign has been active for over seven years, utilizing delayed activation and remote payload delivery to evade detection and maintain a facade of legitimacy.

The implications for the financial services sector are significant, as the Zoom Stealer campaign exemplifies a shift towards corporate espionage, harvesting sensitive information such as meeting links and credentials in real time. This represents a serious risk to corporate security and confidentiality, particularly for institutions engaged in high-stakes financial transactions and negotiations.

Technical Details

- DarkSpectre exploits the browser extension trust model by publishing legitimate extensions that later activate malicious behavior.
- The campaign employs time-delayed logic bombs, with malicious execution triggering 48-72 hours post-installation to evade detection.
- Extensions download encoded JavaScript payloads disguised as image files, allowing for unrestricted remote code execution.
- Overprivileged permissions are exploited, with extensions requesting access to multiple video conferencing platforms unrelated to their advertised functionality.
- Real-time data exfiltration occurs through persistent WebSocket connections, enabling

unauthorized access to confidential meetings.

- The campaign includes dormant "sleeper" extensions that appear benign but can be weaponized later through updates or remote configuration changes.
- Security scanners fail to detect malicious activity due to the legitimate appearance of extensions during the review process.
- The use of obfuscated code and steganography enhances the stealth of the malicious payloads.
- Malicious behavior is triggered only after the marketplace review is completed, resulting in prolonged undetected threats.
- The campaign poses a risk of impersonation, spear-phishing, and corporate espionage, particularly affecting financial institutions.

Recommendations

- Conduct a full audit of installed browser extensions to identify potential threats.
- Remove extensions that have excessive or unrelated permission or come from unknown publishers.
- Rotate compromised meeting links and credentials regularly to mitigate risks.
- Block known malicious infrastructure and domains associated with the DarkSpectre campaign.
- Implement robust monitoring for unusual browser activity and unauthorized access attempts.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Researchers Identify 'EDR-Freeze' Technique Targeting Endpoint Security in Financial Services	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers uncovered a proof-of-concept technique known as ‘EDR-Freeze’, which temporarily suspends endpoint security processes by exploiting legitimate Windows Error Reporting behavior. This technique creates a monitoring blind spot, allowing threat actors to conduct hostile actions with reduced telemetry during the suspension period.

The implications for the financial services sector are significant, as organizations heavily rely on endpoint detection and response mechanisms. The EDR-Freeze technique can lead to critical visibility gaps, making it essential for financial institutions in the UAE to assess their exposure to such user-mode process suspension tactics and strengthen their detection capabilities.

Technical Details

- The EDR-Freeze technique operates entirely in user mode, avoiding kernel-level methods while leveraging race conditions.
- It temporarily suspends security processes by timing the suspension of the dump helper, creating a reversible “coma” state.
- The attack begins with a diagnostic dump workflow against the security process via Windows Error Reporting.
- All threads of the target process are placed into a suspended state during the dump preparation phase.
- The attacker races to suspend the helper component at the moment the target is paused, preventing the dump from completing.
- This technique preserves a non-telemetry-producing security process for a configurable interval before normal activity resumes.
- Forensic examination reveals high-privilege handle access and controlled thread suspension, indicating explicit targeting.
- Detection opportunities arise from command-line parameters that specify process identifiers and individual threads.
- Memory-forensics tooling can correlate helper-thread activity timing with the target’s suspended threads to substantiate the manipulation.
- The technique highlights the need for defenders to focus on abnormal dump workflows and privilege patterns rather than just process existence checks.

Recommendations

- Harden against dump-workflow abuse by monitoring Windows Error Reporting invocations with explicit targeting parameters.
- Detect user-mode processes that gain broad suspend/resume privileges over protected security services or their threads.
- Instrument thread-state telemetry to baseline normal states and alert on sudden multi-thread suspension patterns.
- Strengthen self-protection by enabling endpoint control features that resist or report thread suspension attempts.
- Prepare memory-forensics workflows to validate suspected freeze events using handle mapping and thread-state timelines.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
RondoDoX Botnet Campaign Targets Web Apps and IoT Devices with React2Shell Exploitation	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

CloudSEK has identified a persistent nine-month campaign by the RondoDoX botnet, which is exploiting vulnerabilities in web applications and IoT devices. The threat actors have recently begun weaponizing a critical Next.js vulnerability, deploying malicious payloads such as "React2Shell" and cryptominers, indicating an evolution in their attack strategies.

This campaign poses significant risks to the financial services sector, as organizations with internet-facing applications and IoT devices are likely to be targeted. The exploitation of Next.js vulnerabilities can lead to severe server compromises, while the botnet's activities may facilitate DDoS attacks and unauthorized crypto mining, impacting operational integrity and customer trust.

Technical Details

- The RondoDoX botnet campaign has been ongoing for nine months, with a focus on IoT devices and web applications.
- Recent shifts in tactics include the exploitation of a Next.js vulnerability, allowing for remote code execution.
- Attack patterns have evolved through three distinct phases: reconnaissance, web application exploitation, and IoT botnet deployment.
- The campaign has seen at least six confirmed command and control (C2) servers with overlapping operational periods.
- Automated exploitation attempts have increased, with over 80 attempts recorded on a single day in April 2025.
- The botnet deploys multiple malware variants, including cryptominers and web shells, to maintain persistence and control.
- Credential harvesting and lateral movement tactics are employed to pivot from web application exploitation to IoT infrastructure.
- The botnet targets diverse architectures, ensuring payload delivery across various environments, including cloud instances and embedded systems.
- Continuous monitoring of attack vectors has led to alerts for organizations with overlapping technology stacks.
- The campaign indicates a high frequency of exploitation attempts, particularly against Next.js applications, with hourly attacks observed.

Recommendations

- Conduct immediate audits of all Next.js applications to ensure they are patched and secure against known vulnerabilities.

- Isolate IoT devices into dedicated VLANs and apply strict security measures, including disabling remote management interfaces.
- Implement Web Application Firewalls (WAF) to block command injection patterns and enforce strict input validation.
- Block identified C2 infrastructure at perimeter firewalls and deploy intrusion detection signatures for known attack patterns.
- Establish a Zero Trust architecture for administrative interfaces, requiring VPN access and multi-factor authentication.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
New Strain of Shai Hulud Malware Detected in npm Package	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Aikido Security have identified a new strain of the Shai Hulud malware, recently uploaded to the npm package repository under the name @vietmoney/react-big-calendar. This strain appears to be in the testing phase, with no significant spread or infections reported at this time. The code exhibits obfuscation techniques that suggest the attackers had access to the original source code, indicating a sophisticated approach to malware development.

The emergence of this new malware strain is concerning for the financial services sector, as it highlights the ongoing threat posed by advanced malware targeting software supply chains. Financial institutions must remain vigilant against such threats, as attackers increasingly exploit vulnerabilities in widely used software packages to gain unauthorized access and potentially compromise sensitive financial data.

Technical Details

- The new strain is uploaded to npm under the package name @vietmoney/react-big-calendar, indicating a potential supply chain attack.
- The malware exhibits obfuscation, suggesting it was developed by someone with access to the original source code.
- A notable coding error was identified where the malware attempts to fetch a file named c0nt3nts.json but saves it as c9nt3nts.json.
- The initial file is renamed to bun_installer.js, while the main payload is now called

environment_source.js.

- The GitHub repository description has been altered to "Goldox-T3chs: Only Happy Girl," indicating a change in the attacker's branding.
- New leaked file names include 3nvir0nm3nt.json, cl0vd.json, and pigS3cr3ts.json, suggesting a focus on exfiltrating sensitive data.
- The dead man switch feature appears to be removed, potentially reducing the malware's self-destruct capabilities.
- Improved error handling has been implemented for the malware's execution, indicating ongoing development and refinement.
- The malware now accommodates version-dependent package publishing, enhancing its compatibility across different operating systems.
- The order of data collection and saving has been modified, suggesting a strategic change in how the malware operates.

Recommendations

- Monitor npm packages for any unauthorized or suspicious uploads, particularly those related to financial services.
- Implement strict controls and validation for third-party software dependencies to mitigate supply chain risks.
- Educate development teams on secure coding practices to minimize the risk of introducing vulnerabilities.
- Employ advanced threat detection solutions to identify and respond to potential malware infections promptly.
- Regularly review and update incident response plans to address emerging threats like the Shai Hulud malware.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
HoneyMyte APT Utilizes Kernel-Mode Rootkit and ToneShell Backdoor in Cyberespionage Campaign	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Kaspersky have identified a sophisticated cyberespionage campaign attributed to the HoneyMyte APT, which employs a kernel-mode rootkit to deliver the ToneShell backdoor. The malicious driver, signed with a stolen digital certificate, injects the backdoor into system processes, enabling remote access and control for the attackers. This campaign primarily targets government organizations in Southeast and East Asia, with notable activity in Myanmar and Thailand.

The implications for the financial services sector are significant, as the techniques used in this campaign demonstrate an evolution in threat actor capabilities, particularly in the use of kernel-mode injectors to enhance stealth and resilience. Financial institutions must be vigilant, as similar tactics could be employed against them, potentially leading to unauthorized access to sensitive financial data and systems.

Technical Details

- The malicious driver file is named `ProjectConfiguration.sys` and registers as a mini-filter driver on infected systems.
- It is signed with a digital certificate from Guangzhou Kingteller Technology Co., Ltd., which was valid until 2015.
- The driver injects the ToneShell backdoor, allowing the attacker to establish a reverse shell and execute commands remotely.
- The driver employs dynamic resolution of API addresses to obfuscate its behavior and evade detection.
- It protects itself from removal by monitoring specific file operations and denying access to security tools attempting to quarantine it.
- The malware maintains a list of protected registry keys and processes, preventing legitimate operations from affecting its functionality.
- The ToneShell backdoor communicates with two command-and-control servers over TCP on port 443, disguising its traffic with fake TLS headers.
- The backdoor supports various remote operations, including file uploads/downloads and remote shell access.
- Memory forensics is crucial for detecting the injected shellcode, as it executes entirely in memory.
- The campaign shows a notable evolution in HoneyMyte's tactics, emphasizing the need for advanced detection and response measures.

Recommendations

- Implement robust network security measures, including firewalls and intrusion detection systems, to monitor unusual traffic patterns.
- Utilize advanced endpoint detection and response (EDR) solutions to identify and mitigate threats in real-time.
- Conduct regular security awareness training for employees to recognize potential phishing attempts and other social engineering tactics.
- Perform routine security audits and vulnerability assessments to identify and remediate weaknesses in systems.
- Consider deploying a security information and event management (SIEM) system to enhance monitoring and analysis of security-related data.

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
GlassWorm Campaign Targets macOS with Evolving Malware Techniques	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Koi Security have identified a new wave of the GlassWorm campaign, which has shifted its focus from Windows to macOS. This latest iteration employs AES-256-CBC encrypted payloads embedded in compiled JavaScript, targeting developers in the crypto and web3 sectors. The malware is designed to replace legitimate hardware wallet applications with trojanized versions, posing significant risks to cryptocurrency users.

The evolution of the GlassWorm threat actor highlights their adaptability and persistence. With the introduction of platform-specific techniques and a new command-and-control (C2) infrastructure leveraging the Solana blockchain, this campaign represents a serious threat to the financial services sector, particularly for organizations involved in cryptocurrency and digital asset management.

Technical Details

- The GlassWorm campaign has transitioned to targeting macOS exclusively, marking a significant shift from its previous Windows focus.
- The malware uses AES-256-CBC encryption for its payloads, which are embedded in compiled JavaScript, enhancing its stealth capabilities.
- A 15-minute delay is implemented before executing the malicious payload, evading detection by automated sandbox environments.
- The campaign utilizes a new Solana wallet for C2 communication, indicating an evolution in its operational infrastructure.
- The malware attempts to replace hardware wallet applications, such as Ledger Live and Trezor Suite, with trojanized versions.
- The attack incorporates platform-specific techniques, including AppleScript for stealth execution and LaunchAgents for persistence.
- The malware targets over 50 browser extension wallets and various desktop wallets, aiming to steal sensitive cryptocurrency information.
- Exfiltration of stolen data is staged in a temporary directory and sent to a designated exfiltration server.
- The threat actor has demonstrated a pattern of adapting their techniques in response to security

research findings.

- The shared infrastructure across multiple waves confirms the continuity of the threat actor's operations.

Recommendations

- Implement continuous behavioral analysis across software supply chains to detect evolving threats.
- Educate developers on the risks associated with installing extensions from unverified sources.
- Enforce strict access controls and monitoring for sensitive cryptocurrency applications.
- Utilize endpoint protection solutions that can detect encrypted payloads and anomalous behavior.
- Regularly review and update security policies to address emerging threats in the cryptocurrency space.

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 MariaDB Affects Backup Operations	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

A critical Remote Code Execution (RCE) vulnerability has been identified in the MariaDB mariadb-dump utility, tracked as CVE-2025-13699. This vulnerability arises from improper validation and encoding of user-supplied table and view names when using the --tab (-T) option, allowing for directory traversal and arbitrary file write operations that could lead to system compromise.

This vulnerability is particularly concerning for organizations in the financial services sector that utilize MariaDB for automated backup and administrative workflows. Exploitation could result in arbitrary code execution in the context of the MariaDB client user, highlighting the need for immediate action to mitigate potential risks associated with database management and backup processes.

Technical Details

- The vulnerability is tracked as CVE-2025-13699 and has a CVSS v3.1 score of 7.0, indicating a high severity level.
- It affects the mariadb-dump client utility specifically when the --tab (-T) option is used to export tables or views to filesystem paths.
- The flaw allows for directory traversal and arbitrary file write operations, which could lead to remote code execution.

- Attack vectors may involve remote manipulation of database objects processed by privileged dump operations.
- Affected versions include MariaDB 10.6, 10.11, 11.4, and 11.8.
- The vulnerability is classified as critical priority, necessitating prompt action from affected organizations.
- Fixed versions are available: 10.6.24, 10.11.15, 11.4.9, and 11.8.4.
- Organizations should review their backup and export practices to mitigate risks associated with this vulnerability.
- Interaction with the mariadb-dump utility is required for exploitation, emphasizing the importance of secure database management.
- Immediate upgrading of affected versions is recommended to prevent potential exploitation.

Recommendations

- Upgrade to the fixed versions of MariaDB (10.6.24, 10.11.15, 11.4.9, 11.8.4) as soon as possible.
- Review and enhance backup and export practices to minimize exposure to this vulnerability.
- Implement strict access controls to limit interaction with the mariadb-dump utility.
- Monitor for any unusual activity related to database operations that may indicate exploitation attempts.
- Conduct regular security assessments of database configurations and practices to ensure ongoing protection.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Authentication Bypass Vulnerability in IBM API Connect	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

IBM has disclosed a critical authentication bypass vulnerability affecting IBM API Connect, tracked as CVE-2025-13915. This flaw allows unauthenticated remote attackers to bypass login controls entirely, gaining unauthorized access to affected systems. The vulnerability poses a severe risk to enterprise API infrastructures, potentially leading to data exposure, service manipulation, and further compromise of backend systems.

The financial services sector should be particularly vigilant, as the exploitation of this vulnerability could result in significant data breaches and operational disruptions. IBM has released interim fixes for all affected versions and strongly urges immediate remediation to mitigate the risks associated with this critical vulnerability.

Technical Details

- The vulnerability is tracked as CVE-2025-13915, with a CVSS v3.1 base score of 9.8, indicating a critical severity level.

- It allows unauthenticated remote attackers to bypass login controls, gaining unauthorized access to systems.
- The CVSS vector is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H), highlighting the potential impact on confidentiality, integrity, and availability.
- Affected products include IBM API Connect versions 10.0.8-10.0.8.0 to 10.0.8.5 and version 10.0-10.0.11.0.
- IBM has released official interim fixes (iFixes) for all impacted versions to address vulnerability.
- Organizations unable to apply fixes immediately are advised to disable self-service sign-up on the Developer Portal as a temporary mitigation.
- The flaw poses risks of data exposure, service manipulation, and backend system compromise.
- Immediate remediation is strongly urged to prevent exploitation.
- The vulnerability affects enterprise API infrastructures, which are critical in financial services operations.
- Organizations should prioritize patching to maintain security and operational integrity.

Recommendations

- Identify all IBM API Connect deployments within your environment and apply the appropriate iFix immediately based on the deployed version.
- Disable self-service sign-up on the Developer Portal if it is enabled, as a temporary mitigation measure.
- Regularly review and update security policies to include vulnerability management for API infrastructures.
- Conduct security assessments to identify potential exposure points related to vulnerability.
- Stay informed about updates from IBM regarding further patches or security advisories.

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	Recipients may share TLP:AMBER+STRICT

	information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	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
Advanced Persistent Threat (APT)	Highly skilled threat group conducting long-term targeted attacks.
API Management Platform	Enterprise system used to publish and manage application programming interfaces.
AppleScript	macOS scripting language leveraged for stealth execution.
Authentication Bypass	Flaw that allows access without proper login or credentials.
Backdoor	Hidden access mechanism allowing persistent remote control.
Botnet	Network of compromised devices controlled by threat actors.
Browser Extension Abuse	Attack technique exploiting trusted browser add-ons for malicious purposes.
Code Obfuscation	Methods used to deliberately make code difficult to analyze.
Command and Control (C2)	Infrastructure attackers manage compromised systems remotely.
Cryptocurrency Mixing Service	Service used to obscure the origin of digital asset transactions.
CSC	UAE Cyber Security Council
Database Backup Utility	Command-line tool used to export database content.
DeFi	Decentralized Finance systems operating on blockchain platforms without centralized intermediaries.
Directory Traversal	Exploitation techniques allowing access to unintended filesystem locations.

EDR-Freeze	Technique that temporarily suspends endpoint security processes to reduce visibility.
Encrypted Payload	Malicious code protected by encryption to evade detection.
Endpoint Detection and Response (EDR)	Security technology that monitors and responds to endpoint threats.
Exfiltration	Unauthorized transfer of data from a compromised system.
Interim Fix (iFix)	Temporary vendor patch addressing a critical security issue.
Internet of Things (IoT)	Network-connected devices often targeted for large-scale compromise.
Kernel-Mode Rootkit	Malware operates at the operating system kernel level for stealth.
Logic Bomb	Malicious code designed to activate after a certain delay or condition.
Memory Forensics	Analysis of volatile memory to detect in-memory attacks.
MSI Installer	Microsoft Installer package format used to distribute software.
Multisig (Multisignature)	Governance mechanism requiring multiple approvals to authorize actions or transactions.
Persistence Mechanism	Technique used by malware to survive reboots and maintain access.
PUA (Potentially Unwanted Application)	Software flagged for risky or undesirable behavior.
Race Condition	Timing flaw that can be exploited when operations overlap unexpectedly.
Remote Code Execution	Ability for an attacker to run arbitrary commands on a remote system.
Reverse Shell	Technique where the victim system initiates a connection to the attacker.
RMM (Remote Monitoring and Management)	Tools that enable remote administration and monitoring of systems.
Smart Contract	Self-executing blockchain code that automatically enforces transaction rules.
Stablecoin	Cryptocurrency designed to maintain a stable value, typically pegged to fiat currency.
Steganography	Technique of hiding malicious code within seemingly benign files.
Supply Chain Attack	Attack targeting trusted software dependencies or distribution channels.
TLP:CLEAR	Traffic Light Protocol classification indicating the information may be freely distributed.
Web Application Firewall (WAF)	Security control that filters and blocks malicious web traffic.
WebSocket	Persistent communication channel enabling real-time data exchange.
Windows Error Reporting	System diagnostic service abused to suspend security processes.
Wrapped Token	A tokenized representation of an underlying digital asset used for compatibility.
Zero Trust Architecture	Security model that assumes no implicit trust and continuously verifies access.