TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	26/2/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 26 February 2026

8	5	2	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 AI enabled intrusions, state linked campaigns, critical zero days, and high impact breaches impacting blockchain infrastructure. Key events include UNC1069 targeting FinTech with deepfake social engineering, ClickFix execution, and multiple macOS malware families, an AI assisted compromise of more than 600 FortiGate devices, and malware that hides command and control behind web-based AI services. The roundup includes exploitation of Dell RecoverPoint CVE-2026-22769 by UNC6201, OpenClaw delivery of Atomic macOS Stealer, a driver based crypto miner, a ClickFix chain that installs MIMICRAT, and MuddyWater activity under Operation Olalampo. Other items include high risk issues in Ivanti EPMM, Mozilla products, Windows Admin Center, and Google Chrome, plus the IoTeX ioTube bridge breach and the FICOBA registry exposure. For the financial sector the risk centers on credential theft, movement into identity and virtualized platforms, covert AI proxied traffic, and third-party dependencies. Near term actions are to patch RecoverPoint and Ivanti EPMM, update Chrome and Firefox and Windows Admin Center, restrict internet facing admin access with MFA and segmentation, elevate EDR for PowerShell and kernel signals, and limit untrusted AI services.

ADGM THREAT INTELLIGENCE SUMMARY

UNC1069 Targets FinTech Entities with Sophisticated Multi-Stage Malware Campaign [Campaign] [High]

AI-Augmented Threat Actor Compromises Over 600 FortiGate Devices Globally [Campaign] [High]

AI-Driven Malware Campaign Exploits Web-Based AI Services as Command-and-Control Proxies [Campaign] [High]

UNC6201 Campaign Exploits Dell RecoverPoint Zero-Day Vulnerability [Campaign] [Medium]

Malicious OpenClaw Skills Distribute Evolved Atomic MacOS Stealer [Campaign] [Medium]

Sophisticated Monero Mining Campaign Leverages Social Engineering and Kernel Exploits [Campaign] [Medium]

Adversaries Abuse Compromised Websites with ClickFix Technique to Distribute MIMICRAT [Campaign] [Medium]

MuddyWater Campaign 'Operation Olalampo' Targets Organizations with New Malware Variants [Campaign] [Medium]

Critical Zero-Day Vulnerability in Dell RecoverPoint for Virtual Machines Enables Remote Exploitation [Vulnerability] [High]

Critical Vulnerabilities in Ivanti EPMM Enable Remote Code Execution [Vulnerability] [High]

Multiple High-Severity Vulnerabilities in Mozilla Products [Vulnerability] [Medium]

Microsoft Discloses Vulnerability in Windows Admin Center Allowing Privilege Escalation [Vulnerability] [Medium]

Google Chrome Vulnerabilities Could Allow Remote Code Execution [Vulnerability] [Medium]

IoTeX Suffers Security Breach Affecting ioTube Multi-Chain Bridge [Cyber Breach] [High]

Data Breach at French Bank Registry Exposes 1.2 million Accounts [Cyber Breach] [High]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
UNC1069 Targets FinTech Entities with Sophisticated Multi-Stage Malware Campaign	HIGH	CLEAR	Campaign	Open Source

Executive Summary

A targeted intrusion into a FinTech entity was attributed to UNC1069, a North Korea-nexus financially motivated threat actor. The operation deployed seven unique malware families on a macOS host through sophisticated social engineering involving a compromised Telegram account, a spoofed Zoom meeting, a reported deepfake video, and a ClickFix technique to initiate infection.

This campaign is significant for the financial services sector as it highlights the evolving tactics of state-sponsored threat actors, particularly in the cryptocurrency domain. The use of advanced social engineering techniques and multiple malware families underscores the need for enhanced security measures to protect sensitive financial data and assets from theft.

Technical Details

- UNC1069 employed a multi-stage infection chain beginning with social engineering through a hijacked Telegram account and a fake Zoom meeting.
- The attack utilized ClickFix commands to execute initial payloads on macOS systems, indicating a sophisticated approach to infection.
- The campaign leveraged new malware families (SILENCELIFT, DEEPBREATH, CHROMEPUSH) alongside the existing SUGARLOADER downloader.
- The operation aimed to harvest credentials, browser data, session tokens, Keychain items, and Apple Notes content to facilitate cryptocurrency theft.
- Persistence was maintained via a manually configured launch daemon for SUGARLOADER, allowing continued access to the compromised system.
- The malware included WAVESHAPER, a packed C++ backdoor, and HYPERCALL, a Go-language downloader that loads dynamic libraries from C2 servers.
- DEEPBREATH bypassed macOS TCC protections, enabling unauthorized access to sensitive data stored in the Keychain and browser artifacts.
- CHROMEPUSH was disguised as a Google Docs offline extension, targeting Chromium browsers to log keystrokes and capture credentials.
- The campaign reflects UNC1069's shift towards targeting Web3 entities, including cryptocurrency exchanges and venture capital personnel.

Recommendations

- Implement multi-factor authentication (MFA) for all sensitive accounts to enhance security against credential theft.
- Conduct regular security awareness training for employees to recognize and respond to social engineering attacks.
- Monitor and analyze behavioral logs for any anomalies that may indicate unauthorized access or malware activity.
- Employ endpoint detection and response (EDR) solutions to improve visibility and response capabilities against advanced threats.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by malware.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
AI-Augmented Threat Actor Compromises Over 600 FortiGate Devices Globally	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Amazon Threat Intelligence has identified a campaign involving a Russian-speaking financially motivated threat actor who compromised over 600 FortiGate devices across more than 55 countries. This campaign exploited exposed management ports and weak credentials, leveraging commercial AI services to enhance their operational scale without requiring advanced technical skills.

This activity is particularly relevant to the financial services sector as it highlights the growing trend of AI-augmented cyber threats. Organizations should be aware that such campaigns may lead to significant operational disruptions, especially if attackers gain access to sensitive internal networks and backup infrastructures, potentially paving the way for ransomware deployment.

Technical Details

- The campaign utilized credential-based access to FortiGate management interfaces exposed to the internet, targeting ports 443, 8443, 10443, and 4443.
- The threat actor employed AI-assisted Python scripts to parse, and decrypt stolen FortiGate configuration files, which contained high-value credentials and network topology information.
- Compromised FortiGate devices provided access to internal networks, facilitating Active Directory compromise and credential harvesting.
- The threat actor's reconnaissance tool, developed with AI assistance, automated the process of network discovery and vulnerability scanning.

- Post-exploitation activities included the use of Meterpreter and mimikatz for DCSync attacks against domain controllers to extract NTLM password hashes.
- The attacker demonstrated opportunistic targeting, with clusters of compromised devices observed across various global regions, including South Asia and Northern Europe.
- The operational security of the threat actor was inadequate, revealing methodologies and AI usage through publicly accessible infrastructure.
- The campaign's success was attributed to exploiting fundamental security gaps rather than advanced technical capabilities.
- The threat actor exhibited a pattern of moving to softer targets when encountering robust defenses, indicating a reliance on AI for efficiency.

Recommendations

- Implement strong credential hygiene practices, including the use of multi-factor authentication and regular password updates.
- Ensure management interfaces for critical devices are not exposed to the internet or are secured with robust access controls.
- Regularly update and patch FortiGate devices to mitigate potential vulnerabilities.
- Conduct thorough network segmentation to limit lateral movement within internal networks.
- Enhance detection capabilities for post-exploitation indicators to identify and respond to potential breaches promptly.

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-Driven Malware Campaign Exploits Web-Based AI Services as Command-and-Control Proxies	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Check Point Research has identified a campaign that leverages web-based AI services, such as Grok and Microsoft Copilot, as covert command-and-control (C2) proxies. This technique allows attackers to blend malicious traffic with legitimate enterprise communications, facilitating the exfiltration of data and the delivery of commands without detection. The campaign demonstrates how AI can be integrated into malware operations, enhancing its adaptability and stealth.

The implications of this campaign may impact organizations in the financial services sector, as the use of AI-driven malware could lead to more sophisticated and unpredictable attacks. Financial institutions should be

aware that the evolving landscape of AI technology can be exploited by threat actors, increasing detection' complexities, and response efforts.

Technical Details

- Attackers can exploit AI assistants with web browsing capabilities to serve as covert C2 relays, blending malicious traffic with legitimate communications.
- The campaign utilizes platforms like Grok and Microsoft Copilot, which allow for anonymous web access and URL fetching.
- AI-driven malware can autonomously adapt its behavior based on environmental feedback, shifting from static logic to dynamic decision-making.
- The malware can collect host context, such as user roles and installed software, to prioritize targets and adjust tactics in real-time.
- This approach enables attackers to execute more complex operations with less-skilled actors, reducing the time and cost of malware development.
- AI models can influence which capabilities are activated and how aggressive the malware should be during an attack.
- The use of AI services as a transport layer allows for stealthy communication without traditional API keys, complicating mitigation efforts.
- The integration of AI into malware enhances its ability to evade detection by reducing predictable patterns that defenders rely on.
- Attackers can initiate commands and exfiltrate data through AI agents without the need for user accounts or API keys, increasing operational stealth.
- This campaign marks a significant evolution in malware development, with AI becoming a core component of the malware's runtime decision-making process.

Recommendations

- Financial institutions should implement strict monitoring of AI service usage within their networks to detect potential misuse.
- Organizations should consider blocking access to untrusted AI platforms to mitigate the risk of exploitation.
- Employ endpoint detection and response (EDR) solutions to identify anomalous behavior indicative of AI-driven malware.
- Regularly update security protocols to address the evolving tactics employed by threat actors leveraging AI technologies.
- Conduct employee training to raise awareness about the risks associated with AI services and the potential for exploitation.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
UNC6201 Campaign Exploits Dell RecoverPoint Zero-Day Vulnerability	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Mandiant and Google Threat Intelligence Group have identified the exploitation of a zero-day vulnerability in Dell RecoverPoint for Virtual Machines, tracked as CVE-2026-22769. This vulnerability has been leveraged by the threat actor group UNC6201 to gain unauthorized access, maintain persistence, and deploy various malware including SLAYSTYLE and GRIMBOLT. The initial access vector remains unconfirmed, but the group is known to target edge appliances for entry.

The exploitation of this vulnerability may impact organizations in the financial services sector that utilize **"**Dell RecoverPoint"***** for Virtual Machines. As the threat actor employs sophisticated techniques to pivot into VMware infrastructures, financial institutions should be aware of the potential risks associated with this campaign and consider implementing robust security measures to mitigate exposure.

Technical Details

- The vulnerability CVE-2026-22769 has a CVSSv3.1 score of 10.0, indicating a critical risk.
- UNC6201 has exploited this flaw since at least mid-2024, using it to move laterally within victim environments.
- The group has replaced older BRICKSTORM binaries with a new malware variant called GRIMBOLT, enhancing their operational capabilities.
- GRIMBOLT is designed using C# and compiled with native ahead-of-time (AOT) compilation, complicating static analysis.
- The threat actor modifies a legitimate shell script named "convert_hosts[.]sh" to establish persistence on compromised appliances.
- Exploitation involves authenticating to the Dell RecoverPoint Tomcat Manager using hard-coded default credentials.
- A malicious WAR file containing a SLAYSTYLE web shell is deployed to facilitate further exploitation.
- UNC6201 has been observed creating "Ghost NICs" for stealthy network pivoting within VMware environments.
- The actor uses iptables for Single Packet Authorization, allowing selective traffic redirection.

Recommendations

- Organizations should ensure that all Dell RecoverPoint for Virtual Machines are updated with the latest security patches.
- Implement strong access controls and change default credentials for all administrative interfaces.
- Monitor web logs for suspicious requests to the Tomcat Manager and investigate any unauthorized deployments.

- Employ network segmentation to limit lateral movement within virtual infrastructures.
- Conduct regular security audits and incident response drills to prepare for potential exploitation scenarios.

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

Note: Please refer to the Glossary of Keywords for asterisk(*) marked keywords.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Malicious OpenClaw Skills Distribute Evolved Atomic MacOS Stealer	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

TrendAI™ Research has identified a campaign leveraging malicious OpenClaw skills to distribute a new variant of the Atomic MacOS Stealer (AMOS). This campaign manipulates AI workflows to trick users into installing malware that can steal extensive personal data. The attack utilizes deceptive instructions hidden within "SKILL[.]md" files to exploit AI agents as trusted intermediaries, leading to user credential theft and data exfiltration.

The implications of this campaign may impact organizations in the financial services sector, particularly those who have integrated OpenClaw and rely on macOS endpoints. As the malware targets sensitive information such as credentials and keychain items, financial institutions should be aware of the potential risks associated with this evolving threat landscape and take necessary precautions to safeguard their data.

Technical Details

- The campaign utilizes malicious OpenClaw skills to deliver AMOS, shifting from traditional software distribution methods to supply chain attacks.
- Malicious instructions are embedded in "SKILL[.]md" files, tricking AI agents into presenting fake installation requirements to users.
- A deceptive dialogue box prompts users to enter their passwords, facilitating the malware infection.
- The campaign has been observed across multiple repositories, with hundreds of malicious skills uploaded to ClawHub and SkillsMP.
- The AMOS variant collects sensitive data including credentials, browser data, and files from common folders, but lacks system persistence.
- Initial access is gained through a seemingly benign "SKILL[.]md" file that instructs users to install a prerequisite tool.
- The malware is delivered as a Mach-O universal binary, compatible with both Intel and Apple Silicon Macs.

- The binary is signed with an ad-hoc signature, lacking the security assurances of a proper code-signing certificate.
- Data exfiltration occurs via a command-and-control server, uploading compressed files containing stolen information.
- The malware avoids exfiltrating ".env" files, which typically store sensitive API keys.

Recommendations

- Implement robust endpoint protection solutions to detect and block malicious binaries.
- Educate employees on the risks of installing software from unverified sources, particularly through AI-driven platforms.
- Regularly monitor and audit installed applications and permissions granted to ensure no unauthorized software is present.
- Employ multi-factor authentication (MFA) to enhance security for sensitive accounts and 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
Sophisticated Monero Mining Campaign Leverages Social Engineering and Kernel Exploits	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Trellix have identified a sophisticated cryptocurrency mining campaign that utilizes advanced techniques for persistence and lateral movement. The campaign employs social engineering tactics, specifically offering pirated software as a lure, to initiate the infection and deploy a Monero mining payload that destabilizes victim systems.

This campaign may impact organizations in the financial services sector as it highlights the evolving nature of crypto jacking threats. Financial institutions should be aware of the potential for similar tactics to be employed against them, especially given the campaign's use of legitimate software masquerades and kernel-level exploitation to evade detection.

Technical Details

- The campaign uses a social engineering tactic by promising free premium software, distributing pirated software bundles as the entry point.
- The primary orchestration node is a binary named "Explorer[.]exe," which operates as a persistent state machine, managing the infection lifecycle.
- The malware exhibits worm-like capabilities, allowing it to spread across external storage devices and enabling lateral movement in air-gapped environments.

- To avoid antivirus detection, the mining process is disguised as "Microsoft Compatbility Telemetry[.]exe"*, a name similar to a legitimate Windows process.
- The malware employs DLL sideloading techniques to load the actual mining payload, using a fake DLL named "kernel32 [.]dll" with a space in its name.
- The campaign utilizes the Bring Your Own Vulnerable Driver (BYOVD) technique to execute code with Kernel (Ring 0) privileges, bypassing OS security.
- A critical vulnerability (CVE-2020-14979) in the dropped driver "WinRing0x64.sys" allows any user to control low-level CPU configurations.
- The malware creates a service pointing to the vulnerable driver and uses IOCTL codes to communicate with it, facilitating the mining operation.
- The campaign is currently utilizing the Kryptex mining pool for monetization, which is popular among entry-level cybercriminals for its ease of use.
- The threat actor is in the testing phase, refining the infection chain and persistence mechanisms before wider distribution.

Recommendations

- Implement strict endpoint protection measures to detect and block unauthorized software installations.
- Educate employees about the risks of downloading pirated software and the tactics used in social engineering attacks.
- Regularly update and patch systems to mitigate vulnerabilities, particularly those associated with drivers.
- Monitor for unusual system behavior indicative of crypto jacking, such as unexpected CPU usage spikes.
- Employ application whitelisting to prevent the execution of unauthorized binaries, especially those masquerading as legitimate processes.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Sophisticated Monero Mining Campaign

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

Note: Please refer to the Glossary of Keywords for asterisk(*) marked keywords.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Adversaries Abuse Compromised Websites with ClickFix Technique to Distribute MIMICRAT	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Elastic Security Labs have identified an active ClickFix campaign that compromises multiple legitimate websites to deliver a sophisticated malware chain culminating in MIMICRAT, a custom remote access trojan (RAT). This campaign employs a five-stage attack process, leveraging compromised sites to distribute malicious scripts that execute commands directly on victims' machines without downloading files.

The implications of this campaign may impact organizations within the financial services sector, particularly those that rely on web-based services for customer interactions. Using compromised legitimate websites as delivery vectors increases the risk of evading traditional security controls, underscoring the need for financial institutions to stay vigilant against evolving threats.

Technical Details

- The campaign employs a five-stage malware delivery chain, starting with compromised legitimate websites.
- Victims are lured via a fake Cloudflare verification page that instructs them to execute a malicious PowerShell command.
- The initial command is obfuscated and designed to avoid detection by security tools, minimizing the window for intervention.
- A Lua-based loader is used to execute shellcode entirely in memory, enhancing stealth.
- MIMICRAT features malleable command and control (C2) profiles, allowing for flexible communication with the attacker.
- The malware is capable of token theft and utilizes SOCKS5 tunneling for network communication.
- The campaign supports localization in 17 languages, broadening its reach to diverse victim demographics.
- Detection evasion techniques include bypassing Event Tracing for Windows (ETW) and Anti-Malware Scan Interface (AMSI).
- The infrastructure relies on compromised sites, such as bincheck[.]io and investonline[.]in, to deliver the malicious payload.
- The campaign remains active, with ongoing monitoring and analysis by security researchers.

Recommendations

- Implement robust web application firewalls to detect and block malicious scripts from compromised sites.

- Educate employees about the risks of executing commands from untrusted sources, especially via clipboard.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by such campaigns.
- Employ endpoint detection and response (EDR) solutions to monitor for suspicious PowerShell activity.
- Conduct regular security assessments and penetration testing to identify potential weaknesses in web applications.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Adversaries Abuse Compromised Websites with ClickFix Technique

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
MuddyWater Campaign 'Operation Olalampo' Targets Organizations with New Malware Variants	MEDIUM	CLEAR	Campaign	CSC

Executive Summary

Researchers at Group-IB have uncovered a new cyber campaign designated as 'Operation Olalampo', attributed with high confidence to the Iranian-linked threat actor 'MuddyWater'. This campaign involves the deployment of several newly identified malware variants and utilizes a Telegram-based command-and-control mechanism, reflecting tactical continuity with previous operations by the group.

The implications of this campaign may impact organizations within the financial services sector, particularly those operating in the MENA region. The evolving tactics and tools employed by MuddyWater highlight the need for organizations to remain vigilant and proactive in their cybersecurity measures, as the threat actor continues to refine its capabilities and operational sophistication.

Technical Details

- The campaign introduced four new malware variants, including a Rust-based backdoor and multiple downloader families.
- An advanced backdoor was identified, showing overlap with earlier MuddyWater toolsets, indicating infrastructure reuse.
- A Telegram bot was used as the primary command-and-control channel, allowing visibility into operator actions and tool deployment.

- Activity logs revealed both recent and older interactions, suggesting a persistent infrastructure rather than isolated campaigns.
- Researchers found a custom Python-based command server linked to one of the downloader families in victim environments.
- The operational workflow began with initial compromise, leading to malware deployment and subsequent data collection methods.
- The campaign reflects the threat actor's evolving post-exploitation behavior and operational sophistication.
- Signs of possible AI-assisted development were noted within the custom-built tools used in the campaign.
- The campaign underscores MuddyWater's commitment to enhancing its offensive capabilities through new malware development.
- Historical alignment with previous MuddyWater campaigns was observed, indicating tactical and technical consistencies.

Recommendations

- Enhance Endpoint Monitoring: Implement robust endpoint detection capable of identifying anomalous behavior related to custom backdoors and novel downloader activity.
- Strengthen Communications Oversight: Monitor for unauthorized use of encrypted or unconventional messaging platforms that may serve as command-and-control channels.
- Improve Access Control Measures: Apply stricter authentication, logging, and privilege restrictions to detect and mitigate unauthorized post-exploitation activity.
- Conduct Targeted Threat Hunting: Regularly search for behavioral patterns and infrastructure elements associated with MuddyWater's historically reused operational methods.
- Integrate Regional Threat Intelligence: Continuously update defensive strategies with current intelligence on evolving threat actor tactics within the MENA region.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Zero-Day Vulnerability in Dell RecoverPoint for Virtual Machines Enables Remote Exploitation	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical zero-day vulnerability, CVE-2026-22769, has been identified in Dell RecoverPoint for Virtual Machines, allowing unauthenticated remote attackers to gain root-level access. This vulnerability, attributed

to a hardcoded credential flaw, affects versions prior to 6.0.3.1 HF1 and has been actively exploited in the wild, with threat activity linked to the group UNC6201.

The implications of this vulnerability may impact organizations within the financial services sector that utilize Dell RecoverPoint for Virtual Machines for backup and disaster recovery. Financial institutions should be aware of the potential for exploitation, which could lead to unauthorized access, deployment of custom malware, and lateral movement within their networks.

Technical Details

- CVE-2026-22769 has a CVSS score of 10.0, indicating a critical severity level.
- The vulnerability is present in Dell RecoverPoint for Virtual Machines prior to version 6.0.3.1 HF1.
- Exploitation allows unauthenticated remote attackers to gain root-level access to the affected appliances.
- Threat activity associated with this vulnerability has been linked to the threat actor group UNC6201.
- Exploitation has been observed since mid-2024, indicating ongoing threat activity.
- Post-exploitation activities include the deployment of custom malware families, specifically BRICKSTORM and GRIMBOLT.
- Attackers have been observed implanting web shells, known as SLAYSTYLE, on compromised systems.
- The "Ghost NIC" technique has been utilized for lateral movement within VMware ESXi environments.
- Persistence mechanisms are employed by attackers to maintain access to compromised systems.
- There is potential for SaaS pivoting, allowing attackers to extend their reach within cloud environments.

Recommendations

- Immediately apply the latest security updates for Dell RecoverPoint for Virtual Machines to mitigate this vulnerability.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerabilities in Ivanti EPMM Enable Remote Code Execution	**HIGH**	**CLEAR**	**Vulnerability**	**Open Source**

Executive Summary

Two critical zero-day vulnerabilities, CVE-2026-1281 and CVE-2026-1340, affecting Ivanti Endpoint Manager Mobile (EPMM) are currently being exploited in the wild. These vulnerabilities allow

unauthenticated attackers to remotely execute arbitrary code on target servers, providing full control over mobile device management infrastructure without requiring user interaction or credentials.

The widespread exploitation of these vulnerabilities poses a potential risk to organizations in the financial services sector, as they may impact enterprise mobile fleets and corporate networks. Financial institutions should be aware of the possibility of attackers establishing reverse shells, installing web shells, and conducting reconnaissance, which could lead to further malicious activities within their networks.

Technical Details

- CVE-2026-1281 and CVE-2026-1340 are critical remote code execution vulnerabilities with a CVSS score of 9.8, affecting Ivanti EPMM.
- The vulnerabilities exploit legacy bash scripts used by the Apache web server for URL rewriting, allowing attackers to execute arbitrary commands.
- Attackers can manipulate input through HTTP GET requests to specific endpoints, triggering the vulnerabilities without authentication.
- The exploitation process involves variable manipulation, payload injection, and command execution via bash arithmetic expansion.
- Attackers have been observed establishing reverse shells and installing web shells to maintain control over compromised servers.
- Reconnaissance activities include issuing sleep commands to test server vulnerabilities, indicating successful exploitation.
- The vulnerabilities have been added to the U.S. Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog due to their severity.

Recommendations

- Apply the recommended patches from Ivanti immediately to mitigate the vulnerabilities.

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

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple High-Severity Vulnerabilities in Mozilla Products	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Mozilla has released security updates addressing multiple high-severity vulnerabilities, including a heap buffer overflow in libvpx and a website spoofing flaw in Firefox for iOS. These vulnerabilities affect products such as Firefox, Thunderbird, and Firefox ESR, which are widely used across various sectors, including financial services.

The presence of these vulnerabilities may impact organizations in the financial sector that utilize Mozilla products for their operations. It is crucial for these organizations to apply the latest updates to mitigate potential risks associated with these vulnerabilities, as they could be exploited by threat actors to compromise sensitive information or disrupt services.

Technical Details

- CVE-2026-2447 is a high-severity heap buffer overflow vulnerability in libvpx, affecting Firefox, Firefox ESR, and Thunderbird.
- CVE-2026-2032 involves website spoofing via interrupted page loads specifically in Firefox for iOS, also rated as high severity.
- Both vulnerabilities could allow attackers to execute arbitrary code or mislead users into interacting with malicious sites.
- The vulnerabilities are fixed in the latest versions of the affected products, which include Firefox 147.0.4 and Thunderbird 147.0.2.

Recommendations

- Apply the latest security updates released by Mozilla to all affected products immediately.

Detailed Vulnerability Details and Affected Products can be found here: 1, 2, 3.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft Discloses Vulnerability in Windows Admin Center Allowing Privilege Escalation	**MEDIUM**	**CLEAR**	**Vulnerability**	**Open Source**

Executive Summary

Microsoft has disclosed a vulnerability in its Windows Admin Center product, tracked as CVE-2026-26119, which allows an authorized attacker to exploit the flaw over a network. This vulnerability, rated 8.8 on the CVSS scale, enables attackers to elevate their privileges to match those of the user running the application.

This vulnerability may impact organizations in the financial services sector that utilize Windows Admin Center for administrative tasks. The potential for privilege escalation could lead to unauthorized access to sensitive data and systems, making it crucial for affected entities to apply the recommended patch and upgrade to version 2.6.4 to mitigate the risk.

Technical Details

- The vulnerability is classified as 'Improper Authentication' in Windows Admin Center, allowing for unauthorized privilege escalation.
- An attacker with authorized access can exploit this flaw over a network, gaining elevated permissions.

- The flaw affects Windows Admin Center versions up to 2.6.3, making these versions particularly vulnerable.
- Successful exploitation grants the attacker the same permissions and access rights as the user running the application.
- The vulnerability has been assigned CVE-2026-26119 and carries a CVSS score of 8.8 according to Microsoft's rating.

Recommendations

- Upgrade Windows Admin Center to version 2.6.4 immediately to mitigate the vulnerability.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Google Chrome Vulnerabilities Could Allow Remote Code Execution	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Google has released a security update for the Chrome browser addressing multiple vulnerabilities that affect both desktop and mobile platforms. Successful exploitation could allow remote attackers to execute arbitrary code or compromise system stability by enticing users to visit specially crafted webpages. High-severity flaws involving heap buffer and integer overflows may lead to full browser compromise under specific conditions.

Organizations in the financial services sector should be aware that these vulnerabilities could impact their operations, particularly if employees use the Chrome browser for online transactions or sensitive communications. Keeping browsers updated is essential to mitigate potential risks associated with these vulnerabilities.

Technical Details

- Google Chrome has released multiple vulnerabilities that could lead to remote code execution, affecting both desktop and mobile versions.
- CVE-2026-2648 is a high-severity heap buffer overflow vulnerability in PDFium that could be exploited by attackers.
- CVE-2026-2649 involves an integer overflow in the V8 engine, which may also allow for arbitrary code execution.
- CVE-2026-2650 is a medium-severity heap buffer overflow in Media, potentially impacting browser stability.
- Exploitation of these vulnerabilities may cause application crashes or trigger memory corruption.
- Attackers could persuade users to visit specially crafted webpages to exploit these vulnerabilities.

- The vulnerabilities affect various versions of Chrome across different operating systems, including Windows, Mac, Linux, and Android.

Recommendations

- Ensure that all users update Google Chrome to the latest version immediately.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
IoTeX Suffers Security Breach Affecting ioTube Multi-Chain Bridge	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

IoTeX, a modular blockchain platform, has reported a security breach affecting the ioTube multi-chain bridge, specifically targeting the Ethereum-side. The breach involved a sophisticated four-step attack that compromised the Validator contract, allowing the attacker to mint 410 million CIOTX and drain approximately $4.4 million in various tokens from the bridge reserves. Immediate actions have been taken by the IoTeX team to secure the assets and trace the stolen funds.

The incident is significant for the financial services sector as it highlights vulnerabilities in decentralized finance (DeFi) infrastructure. The attack's professional execution and potential links to previous high-profile exploits underscore the need for enhanced security measures and continuous monitoring in the rapidly evolving landscape of blockchain and virtual assets.

Technical Details

- The attack began with the compromise of the Validator contract owner account on Ethereum, granting administrative control to the attacker.
- A malicious upgrade of the Validator contract was executed, bypassing all signature and validation checks.
- The compromised validator layer allowed the attacker to take control of the MintPool and TokenSafe, facilitating asset drainage.
- The attacker minted 410 million CIOTX tokens and drained approximately $4.4 million in various tokens from the bridge reserves.
- Over 86% of the minted tokens have been locked or are in the process of being frozen through rapid response protocols.
- The attacker has been traced to 29 addresses on the IoTeX chain, with efforts underway to blacklist them via a chain-level patch.
- Approximately 2,183 ETH was converted from stolen reserve tokens, with a significant portion bridged to Bitcoin via THORChain.

- Four Bitcoin addresses holding a total of 66.78 BTC have been identified and are under continuous monitoring by IoTeX team.

Recommendations

- Implement rigorous access controls and regular audits of smart contracts to prevent unauthorized access.
- Enhance monitoring of blockchain transactions to quickly identify and respond to suspicious activities.
- Collaborate with exchanges and trading partners to freeze any potentially stolen assets immediately.
- Educate users on security best practices to minimize risks associated with DeFi platforms.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Data Breach at French Bank Registry Exposes 1.2 million Accounts	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

The French Ministry of Finance has disclosed a cybersecurity incident affecting data linked to 1.2 million user accounts. Hackers gained access to the national bank account registry (FICOBA) by exploiting stolen credentials from a civil servant, allowing them to access sensitive information stored in the database.

The breach is significant for the financial services sector as it exposes critical personal and banking information, including account details and identity data. The incident highlights vulnerabilities in access controls and the importance of safeguarding sensitive information against unauthorized access, which could have broader implications for trust in financial institutions.

Technical Details

- Hackers accessed the FICOBA database using credentials stolen from a civil servant with interministerial access.
- The compromised database contains sensitive information, including bank account details and account holder identities.
- Data exposed includes RIBs/IBANs, physical addresses, and taxpayer identification numbers in some cases.
- The breach has disrupted FICOBA's operations, prompting immediate security enhancements.
- The French Ministry of Finance took swift action to restrict the threat actor's access upon detection of the incident.
- The breach underscores the risks associated with centralized databases of sensitive financial information.

Recommendations

- Implement strict access controls and regularly review user permissions to minimize insider threats.
- Conduct regular cybersecurity training for employees to recognize phishing and social engineering attacks.
- Establish a robust incident response plan to quickly address breaches and mitigate damage.
- Consider adopting multi-factor authentication for sensitive systems to further secure access.

Reference to the Source

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Sophisticated Monero Mining Campaign Leverages Social Engineering and Kernel Exploits

TACTIC	TECHNIQUE
Initial Access	T1204.002 User Execution: Malicious File
Execution	T1059.003
	Command and Scripting Interpreter: Windows Command Shell
Persistence	T1543.003 Create or Modify System Process: Windows Service
	T1574.002 Hijack Execution Flow: DLL Side-Loading
	T1546 Event Triggered Execution: Trap
Privilege Escalation	T1134 Access Token Manipulation
	T1068 Exploitation for Privilege Escalation
Defense Evasion	T1036.003 Masquerading: Rename System Utilities
	T1036.006 Masquerading: Space after Filename
	T1564.001 Hide Artifacts: Hidden Files and Directories
	T1112 Modify Registry
	T1070.004 File Deletion
Discovery	T1057 Process Discovery
	T1124 System Time Discovery
	T1120 Peripheral Device Discovery
Impact	T1496 Resource Hijacking
	T1489 Service Stop

Adversaries Abuse Compromised Websites with ClickFix Technique to Distribute MIMICRAT

TACTIC	TECHNIQUE
Initial Access	T1566.003 – Phishing: Spearphishing via Service
Execution	T1204.001 – User Execution: Malicious Link
	T1059.001 – Command and Scripting Interpreter: PowerShell
Defense Evasion	T1027 – Obfuscated Files or Information

	T1562.001 – Impair Defenses: Disable or Modify Tools
	T1562.002 – Impair Defenses: Disable Windows Event Logging
	T1620 – Reflective Code Loading
Persistence	T1053.005 – Scheduled Task/Job: Scheduled Task
Privilege Escalation	T1134.001 – Access Token Manipulation: Token Impersonation/Theft
Defense Evasion	T1055 – Process Injection
Discovery	T1057 – Process Discovery
	T1083 – File and Directory Discovery
Exfiltration	T1041 – Exfiltration Over C2 Channel
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols
	T1090 – Proxy

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
.env files	Secret files that the observed AMOS variant explicitly avoided exfiltrating.
Active Directory	Identity infrastructure targeted after FortiGate compromise, where the actor performed DCSync to obtain NTLM password hashes.
Ad hoc signature	Signing state for code that lacks a proper certificate, noted for the AMOS binary.
AI augmented threat actor	Actor who used commercial AI services and scripts to scale compromise of more than 600 FortiGate devices by parsing and decrypting configs and automating recon.
AI driven C2 proxies	Use of web-based AI assistants such as Grok and Microsoft Copilot as covert relays for command and control that blend with normal enterprise traffic.
Air gapped environments	Networks without direct connectivity where the malware could still spread through external storage devices.
AMOS	Atomic macOS Stealer variant delivered via OpenClaw skills that collected credentials, browser data, and files and did not persist in the observed campaign.
AMSI	Anti Malware Scan Interface that the campaign attempted to bypass.
Apple Notes content	User content that UNC1069 aimed to collect as part of data theft objectives.
Blacklisting addresses	Response step where identified attacker addresses on the IoTeX chain were to be blacklisted via a chain level patch.
BRICKSTORM	Older malware family replaced by GRIMBOLT in the UNC6201 campaign.
Browser spoofing	Issue noted in Firefox for iOS where interrupted page loads could enable website spoofing under CVE-2026-2032.
Browser updates	Action recommended for Firefox, Thunderbird, and Chrome to mitigate listed vulnerabilities.
BYOVD	Bring Your Own Vulnerable Driver tactic that enabled kernel level code execution and bypassed operating system defences in the mining campaign.
C# AOT compilation	Build approach used for GRIMBOLT that complicates static analysis by compiling ahead of time.
C2	Command and control channels used by attackers to issue commands and move data, including malleable profiles and AI proxied transport.
CHROMEPUSH	Malware disguised as a Google Docs offline extension that targeted Chromium browsers to log keystrokes and capture credentials.
Chromium browsers	Browsers targeted by CHROMEPUSH while posing as a Google Docs offline extension to log keys and capture credentials.
CIOTX	Token that the attacker minted in the IoTeX bridge incident, totalling 410 million units.
CISA KEV	Known Exploited Vulnerabilities catalog to which the Ivanti EPMM flaws were added due to severity and active exploitation.
ClickFix	Technique that convinces users to run attacker supplied commands from compromised or fake pages, starting infection chains such as those that lead to MIMICRAT.
Compromised legitimate websites	Trusted sites abused to host and deliver the multistage chain that led to MIMICRAT.
CSC	UAE Cyber Security Council
CVE-2026-1281	Critical Ivanti EPMM flaw exploited in the wild that allowed command execution through legacy bash rewrite scripts.
CVE-2026-1340	Critical Ivanti EPMM flaw exploited in the wild that enabled attackers to execute commands without authentication.
CVE-2026-22769	Critical flaw in Dell RecoverPoint for Virtual Machines with CVSS 10 that enabled unauthenticated remote root access and was exploited in the wild.
CVE-2026-26119	Windows Admin Center vulnerability with CVSS 8.8 that allowed an authorized attacker to elevate privileges over the network.
CVSS score	Severity rating cited for multiple vulnerabilities, including 10.0 for CVE-2026-22769 and 8.8 for CVE-2026-26119.
DCSync	Technique for requesting account data from a domain controller that yields NTLM password hashes when successful.

DEEPBREATH	Malware used by UNC1069 that bypassed macOS TCC privacy controls to access sensitive items such as Keychain and browser artifacts.
Deepfake video	Deceptive media reported as part of the UNC1069 social engineering tactics to increase credibility.
Default credentials	Weak configuration described in the RecoverPoint exploitation where Tomcat Manager accepted hard coded defaults.
DeFi	Decentralized finance context highlighted by the IoTeX bridge breach and its impact on digital assets.
Dell RecoverPoint for VMs	Backup and recovery product affected by CVE-2026-22769 that allowed remote root access and was used as a pivot point into VMware environments.
Downloader families	New downloaders observed in the MuddyWater campaign, including one tied to a custom Python command server in victim environments.
Edge appliances	Systems at the network boundary referenced as common initial access targets for the actors.
EDR	Endpoint Detection and Response recommended to spot anomalies such as PowerShell abuse, cryptomining signals, and AI driven malware.
ETW	Event Tracing for Windows that the ClickFix to MIMICRAT campaign attempted to bypass.
Explorer[.]exe	Primary orchestration node binary that managed the infection lifecycle in the cryptomining campaign.
Fake Cloudflare verification page	Phishing style page that instructed victims to execute a malicious PowerShell command to begin the infection.
FICOBA	French national bank account registry that was accessed with stolen civil servant credentials, impacting about 1.2 million accounts.
Firefox	Mozilla browser referenced as affected by multiple vulnerabilities that were patched in current releases.
Firefox 147.0.4 and Thunderbird 147.0.2	Releases referenced as including fixes for noted Mozilla vulnerabilities.
Firefox ESR	Mozilla browser release channel referenced as affected in the advisory along with Firefox and Thunderbird.
FortiGate	Network security devices whose exposed management interfaces and weak credentials were abused to access internal networks and enable Active Directory compromise.
Ghost NIC	Stealth network configuration created by the actor for pivoting within VMware ESXi environments.
Google Chrome vulnerabilities	Issues that could enable remote code execution and instability with examples including PDFium heap overflow CVE-2026-2648 and V8 integer overflow CVE-2026-2649.
GRIMBOLT	New malware written in C# and compiled ahead of time that replaced BRICKSTORM in UNC6201 operations and complicates static analysis.
Grok	Web based AI service referenced as a covert relay for command and control in an AI driven malware campaign.
Grok and Copilot URL fetching	Capability cited as enabling anonymous web access and relay for C2 without traditional API keys.
Heap buffer overflow	Memory issue noted in both Mozilla and Chrome advisories, including libvpx and PDFium.
Host context collection	Capability where malware gathers user roles and installed software to prioritize targets and adjust behavior in real time.
HYPERCALL	Go based downloader used by UNC1069 that loads dynamic libraries from command-and-control servers.
IBAN	Bank account identifier noted among the exposed data in the FICOBA breach.
Improper Authentication	Classification assigned to the Windows Admin Center vulnerability that enabled privilege escalation.
Integer overflow	Issue noted in the Chrome V8 engine under CVE-2026-2649.
Interministerial access	Level of access of the compromised civil servant account that was used to reach the FICOBA database.
IOCTL codes	Control messages the malware used to communicate with the vulnerable driver service.
IoTeX	Modular blockchain platform that reported a breach of the ioTube bridge on the Ethereum side.

ioTube bridge	Multi chain bridge where the Validator contract owner account was compromised, enabling a malicious upgrade and token minting.
iptables	Utility the actor configured to implement Single Packet Authorization and selective traffic redirection on compromised appliances.
Ivanti EPMM	Mobile device management platform affected by CVE-2026-1281 and CVE-2026-1340 that allowed unauthenticated remote code execution.
kernel32[.]dll	Fake DLL with a space in its name that was sideloaded to load the mining payload.
Keychain items	Sensitive credentials and secrets harvested during the UNC1069 intrusion.
Kryptex	Mining pool named in the crypto mining campaign as the chosen monetization route.
Kryptex mining pool	Pool used by the crypto mining operation for monetization.
Lateral movement	Attacker behaviour to move from one system to another, seen after RecoverPoint and FortiGate compromises.
Launch daemon	Mechanism used on macOS to keep SUGARLOADER persistent on compromised hosts.
libvpx	Component referenced in Mozilla advisories where a heap buffer overflow was fixed under CVE-2026-2447.
Localization	Support for multiple languages noted in the MIMICRAT campaign which included 17 languages.
Lua based loader	In memory loader used in the ClickFix chain to execute shellcode without dropping files.
Mach-O universal binary	Binary format compatible with Intel and Apple Silicon used to deliver AMOS with an ad hoc signature.
macOS TCC	macOS privacy control that was bypassed by DEEPBREATH to access protected data such as Keychain and browser artifacts.
Meterpreter	Post exploitation tool observed in activity following FortiGate compromises.
MFA	Multi Factor Authentication repeatedly recommended to reduce credential theft and unauthorized access.
Microsoft Compatbility Telemetry.exe	Process name used by the miner to disguise activity on victim systems.
Microsoft Copilot	Web based AI service referenced as a covert relay for command and control in an AI driven malware campaign.
MIMICRAT	Custom remote access trojan delivered through a staged chain that supports malleable C2, token theft, SOCKS5 tunnelling, and bypass of ETW and AMSI.
mimikatz	Tool used to execute DCSync attacks against domain controllers to extract NTLM password hashes.
MintPool	Component of the validator layer that was taken over during the IoTeX breach to facilitate asset drainage.
Monero mining campaign	Crypto jacking operation that used pirated software lures, worm like spread, and kernel level techniques to keep mining activity running.
Mozilla vulnerabilities	High severity issues that included a libvpx heap buffer overflow CVE-2026-2447 and a website spoofing issue CVE-2026-2032 in Firefox for iOS.
MuddyWater	Iranian linked group running Operation Olalampo with new malware variants and Telegram based command and control, showing infrastructure reuse and evolving post exploitation behaviour.
Network segmentation	Defensive measure repeatedly recommended to limit lateral movement inside networks.
NTLM password hashes	Credential material taken from Active Directory via DCSync during the FortiGate campaign.
OpenClaw	AI workflow platform where malicious skills steered users into installing AMOS using deceptive SKILL.md instructions.
Operation Olalampo	Campaign attributed to MuddyWater that used new downloaders and a Rust based backdoor, plus a Telegram bot for C2 and a custom Python command server.
PDFium	Component referenced in Chrome advisories where a high severity heap buffer overflow was noted as CVE-2026-2648.
Ports 443 8443 10443 4443	Management ports noted as targeted when FortiGate interfaces were exposed to the internet.

PowerShell	Scripting environment abused in the ClickFix chain that instructed users to run a command copied from a fake verification page.
Privilege escalation	Outcome where an attacker gained the same permissions as the user running Windows Admin Center after exploiting the flaw.
Privilege escalation	Outcome noted for Windows Admin Center where attackers could gain the same permissions as the running user.
Reconnaissance	Activity observed in multiple campaigns including network discovery and the use of sleep commands during Ivanti probing.
Remote code execution	Outcome possible in several entries including Ivanti EPMM and Chrome where attackers could run arbitrary code.
Reverse engineering resistance	Effect of GRIMBOLT being compiled with AOT which complicates static analysis efforts.
Reverse shell	Access mechanism established by attackers during Ivanti EPMM exploitation as part of post exploitation control.
RIB	Bank account identifier noted among the exposed data in the FICOBA breach.
Rust based backdoor	New backdoor written in Rust and used by MuddyWater as part of the campaign toolset.
SaaS pivoting	Post exploitation potential noted in the Dell RecoverPoint entry where attackers could extend reach into cloud environments.
SILENCELIFT	Malware family used by UNC1069 as part of the macOS intrusion sequence.
Single Packet Authorization	Access control approach that allows selective service access after receipt of a specific packet, as configured by the actor.
SKILL.md	Instruction file inside OpenClaw skills that tricked users into entering passwords and installing malware.
SLAYSTYLE	Web shell implanted on compromised RecoverPoint systems via a malicious WAR file.
Sleep commands	Simple commands used by attackers against Ivanti servers to test if exploitation paths were working.
SOCKS5 tunneling	Network tunneling method used by MIMICRAT for communications.
SUGARLOADER	Downloader that maintained persistence on macOS via a manually configured launch daemon in the UNC1069 campaign.
Taxpayer identification numbers	Identity data noted as exposed in some cases in the FICOBA incident.
Telegram	Messaging platform used in multiple contexts including social engineering in UNC1069 and C2 in MuddyWater activity.
Telegram bot C2	Primary command channel used in MuddyWater activity that revealed operator actions and tool deployment.
THORChain	Route used to bridge a portion of converted ETH to Bitcoin after the IoTeX breach.
Thunderbird	Mozilla email client referenced as affected by the libvpx issue and addressed in current updates.
TokenSafe	Component of the validator layer that was taken over during the IoTeX breach to facilitate asset drainage.
Tomcat Manager	Administrative interface that was abused, including use of default credentials, to deploy a malicious WAR containing the SLAYSTYLE web shell.
UNC1069	North Korea nexus threat actor that targeted a FinTech entity with multistage macOS malware delivered through deepfakes, Telegram and Zoom lures, and ClickFix to steal credentials and crypto assets.
UNC6201	Threat actor that exploited Dell RecoverPoint for Virtual Machines via CVE-2026-22769 to gain access, persist, pivot into VMware, and deploy malware including GRIMBOLT and the SLAYSTYLE web shell.
V8	Component referenced in Chrome advisories where an integer overflow was noted as CVE-2026-2649.
Validator contract	Contract that the attacker maliciously upgraded to bypass signature and validation checks and take control of MintPool and TokenSafe.

WAR file	Web application archive used by UNC6201 to deploy the SLAYSTYLE web shell.
WAVESHAPER	Packed C++ backdoor used by UNC1069 to maintain access to compromised systems.
Web shell	Persistent access mechanism installed by attackers on Ivanti EPMM servers following successful exploitation.
Web3	Area that UNC1069 shifted toward which included cryptocurrency exchanges and venture capital personnel.
Windows Admin Center	Administrative product with CVE-2026-26119 that allowed network-based privilege escalation due to Improper Authentication.
WinRing0x64[.]sys	Vulnerable driver tracked as CVE-2020-14979 that granted low level CPU control and was used by the miner for privilege escalation.
Zero-day vulnerability	Vulnerability described in the entries as being exploited in the wild before widespread fixes, including the Dell RecoverPoint issue.