TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	21/1/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 21 January 2026

3	0	11	13
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 surge in diverse and high-impact threats from large-scale data breaches and advanced malware campaigns to critical zero-day vulnerabilities across widely used platforms. The entries collectively reveal increasing exploitation of social engineering, cloud abuse, remote-access tool misuse, sophisticated RAT and ransomware ecosystems, blockchain-based C2 channels, and widespread exploitation of critical enterprise software vulnerabilities. Threat actors continue leveraging living-off-the-land techniques, obfuscation, impersonation fraud, supply-chain access pathways, and long-term stealth frameworks targeting cloud, mobile, browser, and containerized environments.

For the financial sector, these developments underscore escalating risks to investor data, payment ecosystems, trading infrastructure, cloud workloads, privileged identities, and customer-facing platforms. Institutions should prioritize rapid patching cycles, strict control over RMM tools, enhanced monitoring of cloud and mobile channels, stronger identity protections, and proactive threat-hunting for data-theft-only operations, impersonation scams, and sophisticated multi-stage malware. Strengthening resilience across third-party integrations, developer pipelines, and remote-access infrastructure remains essential to mitigating financial fraud, service disruptions, and systemic operational compromise.

ADGM THREAT INTELLIGENCE SUMMARY

Name	Threat Severity Rating	TLP	Attribution	Originating Source
CIRO Data Breach Exposes Sensitive Information of 750,000 Canadian Investors	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

CIRO, a Canadian financial self-regulatory body, confirmed that a cyber breach last year exposed personal information belonging to approximately 750,000 investors. The incident was first detected on August 11 and led to the shutdown of certain non-critical systems while an extensive forensic investigation proceeded.

This exposure is relevant to financial institutions due to the sensitivity of the compromised data, including income details and investment account information, which poses heightened risks for sectors managing regulated investor data and financial profiles.

Technical Details

- CIRO identified a cybersecurity threat on August 11, prompting the shutdown of selected non-critical systems and the launch of a forensic investigation completed January 14.
- Approximately 750,000 investors were impacted, representing a portion of CIRO's current and former members with regulated data held by the organization.
- Compromised information may include dates of birth, phone numbers, annual income, social insurance numbers, government-issued ID numbers, investment account numbers, and account statements.
- CIRO confirmed that login credentials, passwords, or account security questions were not affected, as such data is not stored in its systems.
- Investigative efforts spanned over 9,000 hours, with no evidence found that the stolen data has been misused or published on the dark web.
- Preliminary findings earlier had shown exfiltration of some personal information from member firms and their registered employees.
- The breach involved exfiltration of regulated information that CIRO collects during oversight of investment dealers, mutual fund dealers, and trading activity.
- Upon detecting the threat, CIRO immediately isolated affected systems and launched an in-depth forensic review.
- Impacted individuals will receive direct communication with instructions on how to enroll in the offered protection services.
- The breach was noted among significant cybersecurity incidents in Canada during the period referenced.

Recommendations

- Strengthen monitoring and access controls around systems storing regulated investor and account-level data.
- Enforce phishing-resilience measures, focusing on rapid detection of credential-harvesting attempts.

- Review and limit the scope of sensitive personal and financial data retained within operational systems.
- Enhance endpoint visibility and logging around compliance and regulatory data repositories.
- Implement workflows to detect and respond to misuse or anomalies involving investor identity information.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Betterment Confirms Data Breach Following Social Engineering Attack	**HIGH**	**CLEAR**	**Cyber Breach**	**Open Source**

Executive Summary

Betterment, a fintech investment platform, confirmed that hackers accessed some of its systems through a social engineering attack on January 9, compromising personal information of an undisclosed number of customers. The attackers used access gained through third-party platforms to send fraudulent crypto-related notifications urging users to send $10,000 to a malicious wallet.

This incident is significant for financial services due to the exposure of personal customer data and the successful misuse of trusted communication channels, increasing risks of social engineering and fraud across fintech and wealth-management platforms.

Technical Details

- Hackers broke into certain Betterment systems on January 9 via a social engineering attack that exploited “third-party platforms” the company uses for marketing and operations, enabling unauthorized access to internal communication capabilities.
- Compromised data included customer names, email addresses, postal addresses, phone numbers, and dates of birth, which attackers obtained during the breach.
- Using this access, attackers sent fraudulent notifications claiming users could triple their cryptocurrency by sending $10,000 to a wallet controlled by the threat actor, as noted in the TechCrunch report.
- Betterment detected the attack the same day, immediately revoked the unauthorized access, and initiated a comprehensive investigation with support from a cybersecurity firm.
- The company stated that no customer accounts, passwords, or other login credentials were accessed or compromised during the incident.
- Betterment published a notice on its website acknowledging the breach but did not disclose how many customers were targeted or how many had their personal data viewed or stolen.
- The fraudulent notification impersonated official communication channels, increasing the likelihood of user trust and engagement.

- Betterment directly reached out to affected customers advising them to disregard the fraudulent crypto message sent by attackers.
- Representatives did not respond to additional requests for comment at the time, and the organization's incident webpage used a "noindex" tag, limiting search engine visibility of the disclosure.
- The breach illustrates how access to third-party operational or marketing systems can enable downstream compromise of user-facing messaging infrastructure.

Recommendations

- Review and restrict access permissions across all third-party marketing and operational platforms integrated into financial communication workflows.
- Implement enhanced employee training to improve resistance against social engineering attacks targeting operational accounts.
- Increase monitoring for anomalous use of communication channels, including unexpected outbound notifications or mass-messaging activity.
- Strengthen validation measures for customer-facing messages to ensure users can authenticate legitimacy before acting on unexpected offers.
- Conduct immediate internal reviews of third-party system configurations and ensure rapid revocation workflows for any suspicious activity.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Impersonation-Driven Crypto Fraud Surges to Record $17B in Losses	**MEDIUM**	**CLEAR**	**Cyber Breach**	**Open Source**

Executive Summary

Chainalysis has identified that impersonation-based fraud contributed significantly to an estimated $17B in crypto scam losses in 2025, with impersonation tactics growing by 1400% year-over-year. The findings highlight increasingly industrialized scam operations leveraging AI-enabled tools, phishing-as-a-service kits, and layered laundering networks across East and Southeast Asia.

For financial institutions, especially those in fintech, virtual assets, and wealth management, the rise in impersonation fraud underscores the expanding risk of socially engineered attacks, cross-border laundering networks, and industrial-scale scam infrastructures that can exploit customer trust and digital-asset workflows.

Technical Details

- Impersonation scams grew by over 1400% YoY, becoming a primary driver of crypto scam losses, with average payments per scam increasing from $782 in 2024 to $2,764 in 2025, a 253% increase.
- AI-enabled scams proved 4.5 times more profitable than traditional variants, extracting on average $3.2M per operation compared to $719K for non-AI scams, supported by deepfakes, face-swap tools, and synthetic messaging.
- Scam infrastructure became industrialized, supported by phishing-as-a-service kits, stolen-data brokers, large spamming operations, and specialized laundering services that facilitate high-volume multistage transactions.
- A Chinese-speaking group known as "Darcula" (Smishing Triad) conducted large-scale government-impersonation scams, such as E-ZPass phishing campaigns reaching up to 330,000 SMS messages daily and generating $1B over three years.
- Criminal marketplaces like Lighthouse provided phishing kits, templates, domain services, update packages, and evasion tools, with kits reportedly costing under $500 and receiving over 7,000 deposits totaling $1.5M in cryptocurrency.
- Private-sector impersonation attacks included a major case involving fraudulent outreach posing as Coinbase customer service, defrauding victims of nearly $16M through social engineering and insider-enabled data theft affecting 70,000 customers.
- Impersonation scams increasingly use DeFi ecosystems for laundering, with 2024–2025 laundering patterns shifting between smart contracts, cross-chain bridges, and decentralized exchanges.
- Chinese-language criminal networks, CMLNs, and forced-labor scam compounds in Southeast Asia formed key operational hubs for pig-butchering, investment scams, and high-volume laundering.
- Malware-laced phishing operations (e.g., stealer malware, RATs) are used to drain victims' accounts through single-click compromise, bypassing relationship-building scams.
- Large law-enforcement actions included the UK seizure of 61,000 BTC tied to a multibillion-dollar fraud and U.S.-led actions against Prince Group, resulting in over $15B in seized illicit proceeds.

Recommendations

- Implement AI-driven real-time fraud detection, especially for impersonation patterns involving unsolicited account-security claims or transfer-verification prompts.
- Strengthen controls on third-party communications, SMS channels, and customer-facing messaging to prevent spoofing of institutional identities.
- Enhance monitoring of interactions with crypto ecosystems, including bridges, DEX patterns, and unusual payment escalations tied to impersonation behaviors.
- Establish cross-border intelligence sharing within the financial ecosystem to identify laundering flows linked to CMLNs and scam-compound infrastructures.
- Advance customer-awareness programs specifically addressing impersonation threats, fake support communications, and AI-generated social-engineering lures.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Long-Running Global Magecart Campaign Targets Six Major Card Networks	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Silent Push have identified a long-term global Magecart web-skimming campaign active since at least early 2022. The operation uses malicious JavaScript to steal cardholder data by targeting American Express, Diners Club, Discover, JCB, Mastercard, and UnionPay across compromised e-commerce checkout pages.

This activity is relevant to financial institutions as it impacts payment ecosystems at scale, enabling the theft of sensitive card data that can facilitate fraud, identity theft, and monetization via underground markets.

Technical Details

- Silent Push uncovered a vast network of domains tied to a multi-year web-skimming campaign using highly obfuscated scripts targeting six major payment networks.
- The campaign injects malicious JavaScript into legitimate checkout pages, enabling interception of payment, personal, and shipping details during the final payment process.
- Scripts identified include obfuscated loader files delivered from domains such as cdn-cookie[.]com/recorder.js that activated client-side skimming routines.
- The skimmer verifies the checkout page is fully loaded before creating a malicious iframe that mimics payment forms, replacing legitimate interfaces to harvest card data transparently.
- Victims unknowingly submit their payment information into the fake form; the skimmer then forwards the stolen data to attacker-controlled servers before restoring the original checkout flow.
- Silent Push identified that compromised infrastructure was linked to PQ.Hosting/Stark Industries, a bulletproof hosting entity previously associated with malicious campaigns.
- Some infections date back to early 2022, demonstrating long-term operational resilience and indicating repeated reinfection or widespread distribution techniques.
- Web skimmers executed entirely client-side, making detection difficult for site owners and causing users to remain unaware that their payment data was intercepted.
- The malicious code employs obfuscation layers such as string concatenation and function-splitting to avoid detection and forensic analysis, evidencing a mature development pipeline.
- The campaign primarily impacts e-commerce merchants and global payment processors, increasing exposure to identity theft, unauthorized transactions, and downstream fraud.

Recommendations

- Enforce Content Security Policies (CSP) to restrict unauthorized external JavaScript execution across e-commerce and payment environments.

- Conduct regular integrity monitoring and client-side script inspection to detect injected or modified checkout-page code.
- Ensure PCI DSS compliance, including secure handling of cardholder-data environments and full auditing of third-party scripts or integrations.
- Implement continuous scanning for suspicious domains, obfuscated JavaScript loaders, and anomalous iframe behavior in checkout flows.
- Educate e-commerce operators on long-term Magecart threats and prioritize proactive monitoring of payment portals.

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
deVixor Android Banking RAT Expands to Ransomware in Targeted Campaign Against Iranian Users	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Cyble have identified an evolving Android malware campaign known as deVixor, which targets Iranian users through phishing websites impersonating automotive businesses. The malware is distributed as malicious APK files and has advanced from simple SMS harvesting to a fully featured Remote Access Trojan (RAT).

The campaign poses significant risk to financial services due to its ability to steal banking credentials, intercept OTPs, execute banking fraud, and deploy ransomware—all of which directly affect mobile-based financial transactions across targeted institutions.

Technical Details

- The campaign distributes malicious APKs via phishing domains impersonating automotive retailers, luring victims with discounted vehicle offers to install the deVixor malware.
- Active since October 2025, over 700 variants have been observed, showing rapid evolution from basic SMS harvesting to overlay attacks, keylogging, and ransomware capabilities.
- The malware leverages Telegram-based administrative infrastructure and assigns each infected device a unique Bot ID stored in port.json, enabling real-time command execution and continuous updates.
- deVixor relies on dual-server architecture—Firebase for receiving commands and a decrypted C2 server for exfiltrating stolen information—to maintain resilience and operational security.

- The RAT conducts large-scale SMS-based financial data harvesting, extracting OTPs, account balances, card numbers, and banking or crypto-exchange messages using regex-based parsing.
- WebView-based JavaScript injection is used to load legitimate banking pages while capturing credentials through injected scripts after users interact with fake notifications.
- Its ransomware module activates via the RANSOMWARE command, locking devices and demanding TRON cryptocurrency payments using ransom metadata stored in LockTouch.json.
- Additional capabilities include preventing uninstallation, hiding app presence, keylogging, taking screenshots, harvesting contacts, capturing notifications, sending SMS at scale, and impersonating system apps.
- Targeting indicators—linguistic artifacts, Persian UI overlays, and exclusive focus on Iranian banks and exchanges—highlight a regionally specialized operation.
- The malware supports a wide command set across v1 and v2 (e.g., GET_BANK_BALANCE, GET_CARD_NUMBER, SEND_SMS_TO_ALL, KEYLOGGER, TAKE_SCREENSHOT, REMOVE_RANSOMWARE), reflecting a modular and extensible threat platform.

Recommendations

- Install mobile applications only from official stores and avoid APKs from phishing sites or unsolicited links.
- Scrutinize app permission requests, especially for SMS, Accessibility Service, and notification access.
- Implement MFA across banking and financial applications to mitigate credential theft risks.
- Monitor for phishing overlays and suspicious banking notifications that may redirect users into WebView-based credential harvesting.
- Encourage users to report suspicious device activity promptly and perform device resets if infection is suspected.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – deVixor: An Evolving Android Banking RAT

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
Gootloader Campaign Uses Malformed ZIP Archives to Evade Detection	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Expel have identified that Gootloader malware is distributed through deliberately malformed ZIP archives designed to evade analysis and bypass many unarchiving tools. The ZIP files, constructed with anti-analysis features such as truncated structures and randomized metadata, enable victims to extract and execute embedded JScript payloads while impeding security workflows.

This matters to financial services because Gootloader has long served as an initial-access vector for ransomware operations, allowing threat actors to infiltrate systems, establish persistence, and hand off access to secondary operators who may execute high-impact ransomware or data theft attacks.

Technical Details

- Gootloader is delivered as a JScript file packaged inside a malformed ZIP archive created to bypass analysis by corrupting ZIP structures while remaining extractable by Windows' default unarchiver.
- The ZIP archive consists of 500–1,000 concatenated ZIP files, generated uniquely at download time through an XOR-encoded blob that expands client-side, preventing network-based detection.
- The "End of Central Directory" field is truncated with two missing bytes, causing parsing errors in typical unarchiving tools while remaining functional for victims.
- Randomization of non-critical metadata fields (e.g., Disk Number, Number of Disks) creates "hashbusting," ensuring every archive is unique and resistant to signature-based detection.
- Mismatched metadata between the Local File Header and Central Directory appears consistently, including discrepancies in CRC32, file sizes, timestamps, and filenames.
- Multiple instances—often hundreds—of Local File Header and End of Central Directory structures appear within each archive, reflecting the concatenated ZIP construction method.
- When victims open the ZIP, the embedded JScript executes from a temporary directory under Windows Script Host (WScript), initiating the infection chain.
- Execution spawns CScript and ultimately PowerShell, establishing persistence via LNK files placed within the Startup directory, referencing secondary JScript payloads stored in random locations.
- NTFS shortnames are used when executing JScript files, providing defenders with unique behavioral detection opportunities.
- Gootloader developers embed malicious code inside large benign-looking JScript files, hiding fewer than 100 malicious lines within a 10,000-line script.

Recommendations

- Reassociate .js and .jse file extensions to open with Notepad via Group Policy, preventing automatic execution of malicious scripts.

- Restrict or block execution of wscript.exe and cscript.exe where operationally feasible to reduce exposure to script-based initial access vectors.
- Monitor for wscript.exe executing JScript files from AppData\Local\Temp, which commonly indicates ZIP-based execution.
- Detect creation of .LNK files within Startup folders pointing to scripts located in unusual, non-standard directories.
- Alert on process chains where cscript.exe executes JScript files using NTFS shortnames or subsequently spawns powershell.exe, as these behaviors align with Gootloader's first-stage execution.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
DeadLock Ransomware Leveraging Polygon Smart Contracts for Stealthy Infrastructure Control	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Group-IB have identified that the DeadLock ransomware family, first discovered in July 2025, is abusing Polygon smart contracts to rotate and distribute proxy server addresses. This technique is poorly documented, under-reported, and significantly enhances the malware's ability to evade traditional infrastructure-based detection.

This matters to financial organizations and related sectors because decentralized smart-contract-powered infrastructure provides threat actors with resilient, takedown-resistant communication channels that complicate incident response and reduce visibility during ransomware activity.

Technical Details

- DeadLock is a ransomware family with no affiliate program and no data leak site, contributing to low public visibility despite active operations since July 2025.
- Group-IB identified DeadLock's innovative use of Polygon smart contracts to store and rotate proxy server addresses, providing decentralized C2 infrastructure.
- The technique mirrors similar blockchain abuse observed in other campaigns, such as EtherHiding, where malicious content is stored or referenced on public blockchain ledgers.
- Smart contract usage allows threat actors to update proxy information without centralized infrastructure, increasing operational stealth and bypassing domain/IP blocking.

- Analysis noted that AnyDesk has been observed as the primary remote monitoring and management tool within DeadLock's operational toolkit.
- At least three DeadLock ransomware variants have been identified, suggesting continuous development and tactical refinement.
- Infections result in file encryption with the ".dlock" extension and victims receive a ransom note; newer variants threaten the sale of stolen data.
- The malware creates an HTML file containing an embedded Session messenger wrapper, enabling direct encrypted communication between victims and operators.
- Group-IB analysts highlight that the abuse of blockchain smart contracts for malicious purposes is emerging as a trend with wide potential variation.
- The findings emphasize that decentralized smart-contract-based infrastructure is difficult to dismantle, posing long-term detection and response challenges.

Recommendations

- Monitor for anomalous C2 activity patterns, especially blockchain-based communication channels that do not rely on traditional DNS/IP infrastructure.
- Enhance monitoring for remote administration tools like AnyDesk to detect unauthorized lateral movement associated with ransomware staging activity.
- Implement strict access controls and review endpoint logging for unusual HTML-based communication components dropped post-infection.
- Integrate blockchain-aware telemetry into threat-hunting workflows to identify smart-contract-based C2 mechanisms.
- Strengthen backup and recovery processes to mitigate impacts from encryption-only ransomware strains lacking data-leak sites.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – DeadLock ransomware uses blockchain for evasion

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
Ransomware Extortion Tactics Expand as Encryptionless Attacks Surge	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers outline a significant rise in cyber-extortion activity driven by actors adopting encryptionless

data-theft tactics, enabling rapid victimization even in well-defended environments. These tactics leverage zero-day vulnerabilities and supply-chain weaknesses to exfiltrate data before organizations can respond.

This evolution matters to financial services and adjacent sectors as it broadens extortion pathways, increases exposure to data-theft-only attacks, and accelerates the pace at which adversaries can monetize stolen information.

Technical Details

- Extortion attacks reached record levels in 2025, driven by a new class of actors who rely solely on data theft rather than encryption, using zero-day vulnerabilities and supply-chain weaknesses to infiltrate networks.
- Attacks involving encryption remain steady at more than 4,700 annually, despite disruptions to major operators such as LockBit and RansomHub.
- Growth in extortion was marked by 6,182 attacks in 2025, a 23% increase from 2024 when encryptionless attacks are included.
- Snakefly (Cl0p) pioneered large-scale, zero-day-driven exfiltration campaigns, including an October 2025 operation exploiting CVE-2025-61882 in Oracle E-Business Suite.
- ShinyHunters expanded this model by targeting Salesforce environments across multiple corporations to exfiltrate sensitive data.
- Newer ransomware operators—including Akira, Qilin, Safepay, and DragonForce—have grown rapidly, capturing affiliates previously aligned with LockBit and RansomHub.
- Analysis shows 4,737 ransomware attacks claimed on leak sites in 2025, the highest recorded total.
- Living-off-the-land tools remain central to attacker tradecraft: PowerShell appeared in 25% of investigated attacks and PsExec in 22%.
- Dual-use software is heavily leveraged, including NetScan (19%), Rclone (10%), and remote-access tools such as AnyDesk (13%), ScreenConnect (4%), PDQ (3%), and Splashtop (2%).
- Attackers prioritize minimal malware use until late-stage deployment and increasingly rely on legitimate software to evade detection and maintain persistence.

Recommendations

- Strengthen controls around remote-access and administrative tools, including continuous monitoring and allow-listing.
- Enhance detection for living-off-the-land activity, especially PowerShell and PsExec-based lateral movement.
- Reinforce supply-chain security with rigorous patching, vendor risk assessments, and continuous monitoring for zero-day exploitation indicators.
- Implement robust data-exfiltration monitoring and anomaly detection to identify theft-only extortion operations.
- Conduct regular tabletop exercises addressing data-theft extortion scenarios alongside traditional ransomware recovery planning.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Hackers Use Fake PayPal Notices to Steal Credentials, Deploy RMMs	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at CyberProof have identified a multi-stage campaign in which threat actors abuse Remote Monitoring and Management (RMM) tools, leveraging fake PayPal alerts to initiate credential theft and escalate into corporate environments.

This matters to financial services organizations because threat actors are increasingly bypassing EDR controls using legitimate remote-access tools, enabling footholds that can transition from personal accounts to corporate compromise.

Technical Details

- Campaigns begin with phishing emails impersonating PayPal notifications, shifting away from seasonal lures to high-urgency financial themes that prompt immediate action.
- Initial compromise is achieved through fake PayPal alerts that socially engineer victims into engaging with attackers via phone and installing remote access tools.
- Attackers deploy legitimate RMM tools such as LogMeIn Rescue and subsequently AnyDesk, creating redundancy and reducing detection risk.
- CyberProof observed this pattern across six incidents, including one where the attacker pivoted from a personal PayPal account to corporate access.
- Threat actors successfully bypass EDR solutions by using legitimate RMM utilities rather than custom malware, allowing remote control and credential harvesting.
- Persistence is established through scheduled tasks and shortcut files disguised with Gmail-style naming conventions.
- Investigators identified multiple LogMeIn Rescue binaries and evidence of active remote sessions during analysis.
- The campaign reflects a broader trend of attackers using one RMM tool to install another, a redundancy tactic previously highlighted in other research referenced by CyberProof.
- The attack chain is multi-layered: phishing → social engineering → RMM installation → persistence → unauthorized access escalation.
- CyberProof notes the long-term risk that access obtained through RMM backdoors could be monetized or sold to other threat actors for deeper compromise.

Recommendations

- Restrict or tightly control the installation and execution of RMM tools, ensuring only approved remote-access solutions are permitted.
- Implement enhanced phishing-resilience measures, focusing on financial-themed lures and voice-based social engineering vectors.
- Monitor for unexpected LogMeIn Rescue or AnyDesk installations and investigate any RMM activity originating from unusual user workflows.
- Detect and alert on creation of suspicious scheduled tasks and startup shortcuts mimicking email or cloud-service naming conventions.
- Strengthen endpoint monitoring for unauthorized remote sessions and enforce MFA on all payment-related or financial-service accounts.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multi-Stage AsyncRAT Campaign Abuses Cloudflare and Python Environments	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Trend Micro have identified a multi-stage AsyncRAT campaign that exploits Cloudflare's free-tier infrastructure and TryCloudflare tunneling domains to mask malicious WebDAV servers. The campaign leverages phishing emails distributed via Dropbox links to deliver deceptive double-extension files, enabling attackers to establish a foothold with minimal detection.

This matters to financial services organizations as the use of trusted cloud services and legitimate Python environments enables attackers to bypass traditional defenses, execute advanced code injection, and maintain persistence across systems.

Technical Details

- Threat actors exploited Cloudflare's free-tier services and TryCloudflare tunneling domains to host WebDAV servers, concealing malicious activity behind trusted infrastructure.
- Initial access began via phishing emails that used Dropbox links and double-extension files (.pdf.url) to trick users into opening malicious content while displaying legitimate PDFs during execution.
- Attackers deployed legitimate Python downloads from official sources to establish a full Python environment on victim systems, facilitating code injection targeting explorer.exe processes.
- The initial payload utilized Windows Script Host (WSH) to download and execute additional scripts hosted on the malicious WebDAV server, automating multi-stage infection.

- Persistence was achieved through startup folder scripts (e.g., ahke.bat, olsm.bat), WebDAV mounting, and "living-off-the-land" techniques using Windows Script Host, PowerShell, and system utilities.
- The campaign demonstrated reliance on legitimate infrastructure to evade detection and ensure reliable delivery of subsequent payloads.
- AsyncRAT's modular Python-based architecture facilitated remote command execution, keylogging, and screen capture, enabling full attacker control.
- Earlier stages involved batch files and additional payloads retrieved from WebDAV directories, ensuring seamless execution flow.
- The campaign's infection chain combined phishing, cloud abuse, legitimate tooling, and code injection, reflecting increasingly sophisticated evasion tactics.

Recommendations

- Block or scrutinize access to free-tier cloud tunneling domains such as TryCloudflare and monitor for unusual WebDAV mount activity.
- Implement enhanced phishing controls targeting Dropbox-based deliveries and double-extension file lures.
- Restrict unauthorized Python installations and monitor for unexpected Python environment setups on endpoints.
- Detect and alert on activity involving WSH, PowerShell, and unusual script execution from startup directories.
- Enforce endpoint behavioral monitoring capable of identifying code injection into explorer.exe and similar processes.

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
Threat Actors Distribute RMM Tools Masquerading as Video Files	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at ASEC have identified an attack campaign distributing malicious PDF files that redirect users to spoofed Google Drive pages, ultimately delivering Remote Monitoring and Management (RMM) tools such as Syncro, SuperOps, NinjaOne, and ScreenConnect. The attackers leverage signed installers and deceptive file-naming to trick users into executing remote-access utilities.

This activity is significant for financial sector organizations as RMM abuse enables persistent unauthorized access, credential theft, and lateral movement without relying on conventional malware—making detection difficult across enterprise environments.

Technical Details

- Attackers distributed PDF files with names referencing invoices, product orders, payments, and defective products, likely sent as phishing email attachments to entice victims to open them.
- The PDFs cannot be previewed and instead prompt users to click links to pages impersonating Google Drive or Adobe, pushing them toward downloading a file disguised as "Video_recorded_on_iPhone17.mp4".
- The downloaded file masquerades as a video but actually installs RMM tools from a deceptive dissemination page, using social engineering to hide malicious intent.
- Syncro RMM was deployed through installers created with Advanced Installer and signed with certificates—now revoked—indicating sustained activity dating back to at least October 2025.
- Syncro installers include parameters such as "key" and "customerid", which appear to uniquely identify the attacker's environment; multiple identical Syncro builds were distributed in late 2025.
- Additional malicious installers signed with the same certificate deployed ScreenConnect, which has been abused by various threat groups in prior incidents.
- NinjaOne and SuperOps RMM tools were also delivered, both of which provide remote access, patching, software deployment, monitoring, and asset-management capabilities useful for malicious control.
- The campaign also used NSIS-based downloader components containing embedded commands to fetch additional payloads, including prior NinjaOne distributions.
- Multiple RMM installers and downloaders were distributed under a unified signing certificate, suggesting a single threat actor orchestrating all observed activity.
- Korean-language strings and mutexes indicate a targeting focus on South Korean users, and obfuscation in loaders complicates detection by traditional security tools.

Recommendations

- Block and monitor execution of unapproved RMM tools, including Syncro, NinjaOne, SuperOps, and ScreenConnect, across all endpoints.
- Conduct phishing-resilience training emphasizing invoice- and payment-themed attachments and PDF files that prompt external downloads.
- Monitor for unusual installer activity, including Advanced Installer or NSIS packages deploying remote-access utilities.
- Enforce application-allowlisting to prevent installation of unauthorized remote-management software.
- Ensure OS and security solutions are fully updated and conduct periodic integrity checks for persistent RMM-based access mechanisms.

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
VoidLink Malware Framework Targets Linux Cloud Servers	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Check Point uncovered VoidLink, an advanced cloud-first Linux malware framework composed of custom loaders, implants, rootkits, and modular plugins designed for long-term persistence in modern cloud and container environments.

This emerging threat poses a risk to financial services organizations as it targets cloud infrastructure and developer ecosystems, harvesting cloud and source-code credentials that could enable supply-chain compromise or unauthorized access to critical workloads.

Technical Details

- VoidLink is built as an advanced, modular malware framework containing custom loaders, implants, rootkits, and more than 30 modular plugins available by default.
- The framework is engineered to operate reliably across cloud environments and container systems, including Kubernetes and Docker, automatically adapting its behavior based on detected infrastructure.
- A custom Plugin API—reminiscent of Cobalt Strike's Beacon Object Files—allows operators to extend capabilities dynamically and tailor functionality per target.
- VoidLink employs multiple OPSEC mechanisms, including runtime code encryption, self-deletion upon tampering, and diverse user-mode and kernel-level rootkits.
- The malware appears to be under active development, with binaries containing debug symbols and development artifacts, suggesting ongoing refinement toward broader real-world use.
- The framework harvests credentials associated with cloud providers and source-code version control systems like Git—indicating potential targeting of developers and CI/CD pipelines.
- VoidLink can profile a system extensively, detecting cloud environments such as AWS, Azure, GCP, Alibaba, and Tencent, then adjusting evasion strategies automatically.
- Its architecture is written in Zig and demonstrates high technical proficiency across multiple languages including Go, C, and modern frameworks like React.
- Indicators suggest Chinese-affiliated developers, and the design and documentation imply an intention for commercial use or specialized client deployment.
- Stealth mechanisms include integrity-checking, anti-analysis routines, and automated evasion selection based on environmental risk scoring.

Recommendations

- Strengthen monitoring and detection around cloud workloads, focusing on anomalous behavior in Kubernetes, Docker, and virtualized compute environments.
- Implement strict controls for access to cloud-provider metadata services and enforce least-privilege permissions for cloud and developer accounts.
- Monitor for unauthorized credential harvesting activity, particularly involving Git repositories or cloud IAM environments.
- Deploy behavioral analytics to identify rootkit-style stealth techniques, runtime code masking, or unusual plugin-like execution patterns.
- Conduct regular audits of cloud infrastructure posture to detect early signs of long-term persistence mechanisms tailored to container or virtualization environments.

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
SHADOW#REACTOR Multi-Stage Campaign Uses Text-Only Staging to Deploy Remcos RAT	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Securonix have analyzed SHADOW#REACTOR, a multi-stage Windows malware campaign that relies on obfuscated scripts, text-based payload staging, and in-memory loaders to covertly deploy the Remcos RAT.

This campaign is significant for financial organizations because its fileless execution path, use of trusted Windows components, and multi-stage obfuscation tactics reduce detection visibility, increasing the risk of persistent unauthorized access.

Technical Details

- The infection chain begins with an obfuscated VBS launcher executed via wscript.exe, responsible only for invoking the next stage without performing direct malicious actions.
- The VBS script launches a PowerShell downloader that retrieves fragmented, text-based payloads from a remote host.
- These text files contain Base64-encoded and further obfuscated binary payload fragments transported purely as plain text to evade static detection engines.

- PowerShell implements a resilient download loop, repeatedly fetching content until it meets a minimum size threshold to ensure integrity before execution.
- Retrieved payload fragments are reconstructed into encoded loaders and decoded fully in memory by a .NET Reactor–protected assembly designed to resist reverse-engineering and sandboxing.
- The .NET loader uses reflective loading to orchestrate subsequent stages, manage cleanup, and decode the Remcos configuration data — all without writing artifacts to disk.
- The final stage is executed via MSBuild.exe, a trusted Microsoft-signed living-off-the-land binary (LOLBin), enabling stealthy deployment of the Remcos backdoor.
- The ultimate payload is Remcos RAT, a commercial remote administration tool widely repurposed for malicious use, providing full remote control and persistent access to the compromised system.
- The use of reflective loading, text-only intermediates, and LOLBin escalation forms a highly evasive chain designed to undermine static detection and sandbox analysis.
- Securonix assesses the campaign as modular and actively maintained, though unattributed, with evidence suggesting broad opportunistic targeting rather than a specific vertical.

Recommendations

- Monitor for unusual script-based execution paths such as wscript.exe spawning PowerShell with long encoded command strings.
- Implement behavioral detection for repeated outbound HTTP requests from PowerShell to untrusted infrastructure.
- Detect MSBuild.exe misuse by monitoring for unexpected build-task execution initiated outside development workflows.
- Harden EDR to capture reflective .NET loading behaviors and text-based staging patterns.
- Enforce user awareness training regarding execution of downloaded scripts or document-linked files that launch VBS or PowerShell components.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – SHADOW#REACTOR Multi-Stage Campaign Uses Text-Only Staging to Deploy Remcos RAT

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
RedVDS Infrastructure Enables Global Cybercriminal Operations Through Disposable Windows VDS Environments	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Microsoft observed that RedVDS, a virtual dedicated server (VDS) provider, became a significant enabler of financially motivated threat actors conducting business email compromise (BEC), mass phishing, account takeover, and financial fraud across multiple sectors and countries.

This campaign has major implications for financial services due to the abuse of low-cost, administrator-level Windows VDS instances that allow scalable credential theft, automated fraud, and global phishing operations using a single cloned Windows host image.

Technical Details

- RedVDS operated as a criminal marketplace offering inexpensive, unlicensed Windows-based Remote Desktop Protocol (RDP) servers with full administrator control and no usage limits, making them attractive to cybercriminals.
- Microsoft's investigation revealed that all RedVDS instances were generated from a single cloned Windows Server 2022 image, sharing the identical hostname WIN-BUNS25TD77J, which created a unique detectable fingerprint across campaigns.
- The threat actor behind RedVDS, tracked as Storm-2470, reused the same computer ID and Windows license to replicate hosts, allowing rapid provisioning at scale using QEMU virtualization and VirtIO drivers.
- Multiple threat actors—including Storm-0259, Storm-2227, Storm-1575, Storm-1747, and operators of the RacoonO365 phishing service—leveraged RedVDS infrastructure for BEC, credential theft, and large-scale phishing.
- RedVDS-enabled attacks targeted legal, construction, manufacturing, real estate, healthcare, and education sectors across the US, Canada, UK, France, Germany, Australia, and regions with major banking infrastructure.
- The platform accepted cryptocurrency payments—including Bitcoin, Litecoin, Monero, Binance Coin, Avalanche, Dogecoin, and TRON—to obscure financial trails and support anonymous access.
- Microsoft observed thousands of stolen credentials, invoice theft, phishing infrastructure, and mass-mailer tools deployed on RedVDS systems, indicative of broad cybercriminal adoption.
- RedVDS systems rented from hosting providers across the US, UK, France, Canada, Netherlands, and Germany enabled attackers to obtain geographically aligned IP addresses to bypass location-based filters.
- Reported US-based financial fraud associated with RedVDS-enabled operations totaled approximately $40 million since March 2025.

- The service facilitated infrastructure for mass phishing, account takeovers, and fraud schemes, with widespread use by cybercriminals for credential harvesting and target reconnaissance.

Recommendations

- Enforce conditional access policies and monitor for sign-ins originating from anomalous or previously unseen Windows RDP environments.
- Detect and block traffic associated with known RedVDS domains and infrastructure fingerprints, especially repeated hostnames such as WIN-BUNS25TD77J.
- Implement strong MFA on all accounts, especially those involved in financial workflows or email operations susceptible to BEC.
- Monitor for sudden spikes in phishing attempts or credential validation activity originating from external VDS-hosted IP addresses.
- Enhance email authentication controls (DMARC, DKIM, SPF) to reduce exposure to mass-phishing campaigns supported by criminal VDS ecosystems.

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
Active RCE Exploitation via Symbolic-Link Bypass in Gogs	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Gogs has disclosed CVE-2025-8110, a high-severity vulnerability allowing authenticated users to achieve remote code execution by abusing symbolic links to bypass a previous patch. The flaw reopens an attack path linked to CVE-2024-55947 and is being exploited at scale, with more than 700 publicly exposed instances already compromised.

This vulnerability matters to financial services because compromised Git servers expose source code, credentials, and internal workflows, creating direct risks to fintech development, virtual asset platforms, investment systems, and broader software supply-chain integrity.

Technical Details

- CVE-2025-8110 is rated CVSS-BT 8.7 (High) and enables authenticated remote code execution through a symbolic-link bypass of an earlier file-write vulnerability, allowing attackers to place files outside intended repository paths.
- The flaw originated from the fix for CVE-2024-55947, where input validation blocked path traversal but failed to account for symbolic links residing inside repositories used for redirecting writes.
- Exploitation has been active since July 10, 2025, with attackers creating random 8-character repository and owner names immediately before malware execution.

- The observed attack patterns show automated, large-scale exploitation, rapidly creating repositories and deploying malicious payloads without manual operator involvement.
- Approximately 1,400 Gogs instances are publicly exposed, and 700+ have already been confirmed compromised, indicating widespread operational impact.
- Previously exposed internet-facing Gogs servers, especially those with open registration, are assessed as likely compromised and require immediate forensic review.
- Attackers leverage symbolic links to access sensitive configuration files such as .git/config, enabling unauthorized modifications including injected SSH commands.
- Repositories containing unexpected or externally referenced symbolic links represent high-risk indicators of compromise requiring urgent validation and cleanup.
- Compromise may extend to SSH keys, access tokens, and service accounts, as attackers can manipulate file paths to capture or alter authentication material.
- Without immediate patching, any authenticated user—including attacker-created accounts—can escalate to remote code execution and full system takeover.

Recommendations

- All organizations running affected versions of Gogs should apply the available patch immediately to mitigate the risk of active exploitation.
- Gogs instances that were previously exposed to the internet, particularly those with open registration enabled, should be treated as potentially compromised and subjected to a full security and forensic review.
- Administrators should audit all repositories for the presence of suspicious or unexpected symbolic links, especially those referencing paths outside the repository directory.
- The .git/config file and other sensitive configuration files should be reviewed for unauthorized modifications, including injected sshCommand entries.
- Credentials associated with the Gogs service, including SSH keys, access tokens, and service accounts, should be rotated following patch deployment.
- Until patching is completed, repository creation privileges should be restricted to trusted users only.
- Network exposure should be reduced by placing Gogs behind a VPN, reverse proxy, or IP allow-list where possible.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft Released Jan 2026 Security updates	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Microsoft has disclosed multiple vulnerabilities as part of its January 2026 Patch Tuesday, addressing 112–115 flaws across Windows, Office, and related components, including eight rated critical and three

zero-days. One of the zero-days, CVE-2026-20805, is confirmed to be actively exploited in the wild and poses immediate risk to unpatched systems.

This disclosure is highly relevant to financial services institutions relying on Windows-based infrastructure, as exploitation paths affecting privilege escalation, secure boot integrity, and Office-based attack vectors can be leveraged to compromise endpoints, steal credentials, or facilitate targeted financial fraud operations.

Technical Details

- CVE-2026-20805, an actively exploited Desktop Window Manager information disclosure flaw, allows local exposure of user-mode memory through an ALPC port and is rated Important with CVSS 5.5.
- Additional zero-days include CVE-2023-31096, an elevation-of-privilege issue in the Agere Soft Modem driver enabling SYSTEM-level compromise, and CVE-2026-21265, a Secure Boot certificate expiration bypass due to legacy 2011 certificates.
- Eight critical vulnerabilities span Windows Graphics, VBS enclaves, LSASS, Microsoft Word, Office, and Excel, enabling elevation-of-privilege or remote code execution under specific conditions.
- CVE-2026-20822 is a use-after-free flaw in Windows Graphics permitting authenticated attackers to escalate to SYSTEM privileges by winning a race condition.
- CVE-2026-20876 affects the VBS enclave with a heap-based buffer overflow granting VTL2 privileges, resulting in deep system compromise potential.
- LSASS RCE (CVE-2026-20854) is a network-based exploitation path without elevated privileges, posing high impact due to LSASS' role in credential management.
- Multiple Office-based vulnerabilities (CVE-2026-20944, -20952, -20953, -20955, -20957) rely on malicious documents to trigger memory corruption or pointer manipulation.
- A series of Important-severity vulnerabilities—including those affecting Windows Installer, WER, CLFS, NTFS, RRAS, Ancillary Function Driver, and DWM—have been designated more likely to be exploited.
- The vulnerability mix includes risks enabling remote execution, privilege escalation, and boot-process bypasses, collectively impacting endpoint resilience and identity integrity.
- The patch set covers both kernel-mode and user-mode components, reflecting broad attack surface exposure across Windows environments.

Recommendations

- Deploy January 2026 cumulative updates across all Windows and Office systems.
- Prioritize remediation of CVE-2026-20805.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity XXE Vulnerability in Apache Struts	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Apache Struts has disclosed CVE-2025-68493, a high-severity XML External Entity (XXE) injection vulnerability affecting the XWork component due to improper validation during XML configuration parsing. The flaw affects multiple legacy and current Struts versions, enabling adversaries to abuse XML parsing logic to compromise confidentiality, availability, or internal network access.

This vulnerability poses notable risk to financial services operators using Java-based applications, as exploitation could expose sensitive internal resources, enable SSRF-driven lateral movement, or disrupt critical application workflows supporting payments, virtual asset platforms, and customer-facing web services.

Technical Details

- CVE-2025-68493 is rated Base Score 8.1 (High) and exists in the XWork core component due to insufficient validation during XML configuration processing, enabling XXE injection.
- Successful exploitation allows attackers to read sensitive local files, access internal resources, cause denial-of-service conditions, or trigger server-side request forgery (SSRF) via crafted XML payloads.
- Affected versions include Struts 2.0.0–2.3.37 (EOL), 2.5.0–2.5.33 (EOL), and 6.0.0–6.1.0, representing a wide deployment footprint across Java-based enterprise applications.
- The vulnerability stems from XML parser behavior that incorrectly processes external entities, enabling unauthorized expansion or outbound requests from the host system.
- The issue impacts both legacy and maintained branches, reflecting systemic exposure within older XWork implementations that continue to underpin business applications.
- Attackers could chain XXE exploitation with internal resource enumeration to escalate into larger compromise scenarios, including internal service probing.
- Misconfigured or internet-exposed Struts deployments face higher exploitation likelihood due to historical attacker interest in Struts-based attack surfaces.
- The flaw's impact spans confidentiality, availability, and network integrity, particularly affecting applications that rely heavily on XML-based workflows.
- Remediation is provided in Struts 6.1.1, the only version containing the official fix addressing improper XML handling.
- Organizations unable to upgrade immediately must implement interim mitigations to restrict entity resolution paths and reduce external entity expansion risk.

Recommendations

- Upgrade Apache Struts to fixed version or later.
- Apply temporary Mitigations (If Upgrade Is Not Immediately Possible).

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Critical and High-Severity Vulnerabilities Affect Key Fortinet Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Fortinet has disclosed several critical and high-severity vulnerabilities affecting FortiSIEM, FortiFone, FortiOS, FortiSwitchManager, and FortiSASE, including unauthenticated remote command execution, configuration exposure, and heap-based buffer overflow conditions. These flaws allow attackers to execute arbitrary commands, extract sensitive data, or gain unauthorized control of systems, depending on the product affected.

This disclosure is highly relevant to financial services organizations due to the widespread use of Fortinet appliances across network security, operations, and infrastructure segmentation—making exploitation a potential avenue for lateral movement, service disruption, or compromise of sensitive financial processing environments.

Technical Details

- CVE-2025-64155 is a critical unauthenticated remote command injection flaw in FortiSIEM Super and Worker nodes, caused by improper sanitization of OS command input received via crafted TCP requests, allowing full remote execution without authentication.
- This FortiSIEM vulnerability impacts versions 6.7.0 through 7.4.0, excluding FortiSIEM Cloud and version 7.5, and requires upgrading to the relevant fixed versions or restricting access to TCP port 7900 as a temporary measure.
- CVE-2025-47855 affects FortiFone web portals, enabling unauthenticated disclosure of configuration information due to improper access control, with impacted versions across the 7.0.x and 3.0.x branches.
- The FortiFone flaw exposes sensitive device configuration data to unauthenticated users and requires upgrading to version 7.0.2+ or 3.0.24+.
- CVE-2025-25249 is a high-severity heap-based buffer overflow in the cw_acd daemon affecting FortiOS, FortiSwitchManager, and FortiSASE, enabling remote unauthenticated arbitrary code execution.
- Affected FortiOS branches include 6.4.x through 7.6.x, requiring upgrades to patched releases across all supported major versions, with some fixes pending availability for specific older branches.
- FortiSwitchManager versions 7.0.x and 7.2.x are also vulnerable and require upgrading to their respective fixed versions.
- FortiSASE versions 25.1.a.2 and 25.2.b are impacted, with remediation available in version 25.2.c or through migration to fixed builds.

- The vulnerabilities span multiple architectural components, including OS command parsing, access control validation, and memory handling routines.
- Exploitation could provide attackers with unauthorized control, exposure of configuration data, or execution of arbitrary code across network-critical devices used in enterprise and financial environments.

Recommendations

- Upgrade all affected systems to the vendor-recommended fixed versions.
- Use Fortinet's Upgrade Tool to ensure correct upgrade paths.
- Prioritize internet-facing and fabric-enabled interfaces.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Google Chrome Released Security Updates for Jan 2026	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Google has published a security update for the Chrome browser addressing 10 vulnerabilities, including three high-severity issues in the V8 JavaScript engine and Blink rendering engine that could enable remote code execution when users visit malicious websites. These flaws impact multiple Chrome platforms including Windows, macOS, Linux, Android, and iOS.

This update is important for financial services institutions due to Chrome's widespread use across trading platforms, payment portals, and internal web applications. Exploitation could expose users to arbitrary code execution, UI manipulation, or browser-based compromise, affecting confidentiality and operational integrity.

Technical Details

- Three high-severity vulnerabilities—CVE-2026-0899, CVE-2026-0900, and CVE-2026-0901—impact V8 and Blink, involving out-of-bounds access and inappropriate implementations that can be triggered via malicious web content.
- Medium-severity issues include inappropriate implementation in V8, insufficient input validation in Downloads, incorrect security UI in Digital Credentials, and insufficient policy enforcement in Network, affecting user trust and browser policy controls.
- Three low-severity vulnerabilities involve incorrect security UI, a UI flaw in Split View, and a use-after-free in ANGLE, potentially enabling user deception or stability issues.
- Successful exploitation may allow attackers to execute arbitrary code within the browser context, bypass browser security controls, or mislead users through manipulated security indicators.
- Some vulnerabilities, particularly those affecting V8 and Blink, may be chainable for enhanced exploitation paths, increasing the risk of deeper compromise.

- Fixes have been released across Chrome desktop and mobile platforms, including Windows, macOS, Linux, Android, and iOS.
- Desktop releases include Chrome 144.0.7559.59/60 for Windows and macOS, and 144.0.7559.59 for Linux.
- Android users receive Chrome 144.0.7559.59, while iOS users are updated to Chrome 144 (144.0.7559.85).
- These vulnerabilities affect components involved in JavaScript execution, rendering logic, downloads, and underlying GPU abstraction layers.

Recommendations

- Update Chrome on all platforms—Windows, macOS, Linux, Android, and iOS—to the latest fixed versions (Chrome 144 branches).
- Enable automatic browser updates across managed enterprise environments to ensure timely patch deployment.
- Monitor for user reports of abnormal browser behavior, unexpected UI changes, or unexplained redirects that could signal attempted exploitation.
- Enforce browser isolation or sandboxing policies for high-risk browsing activities within financial environments.
- Review security controls for web-facing applications accessed via Chrome to ensure compatibility with updated browser security mechanism.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
SAP Jan 2026 Security Updates	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

SAP has released its January 2026 security patch package containing 17 security notes that fix critical vulnerabilities across SAP S/4HANA, SAP HANA database, SAP NetWeaver, SAP Wily Introscope, and several application components. The update includes four HotNews vulnerabilities with CVSS scores up to 9.9 and multiple high-severity issues impacting core enterprise workflows.

These vulnerabilities pose notable risk to financial institutions due to the central role SAP systems play in financial processing, general ledger operations, intercompany reconciliation, and backend business services that support payments, treasury operations, and asset management functions.

Technical Details

- Four Critical-severity vulnerabilities (CVSS 9.0–10.0) include CVE-2026-0501, a SQL injection flaw in SAP S/4HANA General Ledger components affecting versions S4CORE 102–109 with a CVSS score of 9.9.

- CVE-2026-0500 enables remote code execution in SAP Wily Introscope Enterprise Manager WorkStation (version 10.8), carrying a critical CVSS rating of 9.6.
- Code injection vulnerabilities CVE-2026-0498 (affecting S/4HANA Private Cloud & On-Premise) and CVE-2026-0491 (affecting SAP Landscape Transformation DMIS versions) both carry CVSS 9.1 ratings.
- Four High-severity vulnerabilities include CVE-2026-0492, a privilege escalation flaw in SAP HANA Database (HDB 2.00) with CVSS 8.8.
- CVE-2026-0507 is an OS command injection issue in SAP Application Server ABAP / NetWeaver RFCSDK impacting kernels 7.53–9.16 and NWRFCSDK 7.50, rated CVSS 8.4.
- Multiple vulnerabilities (CVE-2026-0511 / 0496 / 0495) affect the SAP Fiori Intercompany Balance Reconciliation App, impacting UIAPFI70 versions 500–902 and S4CORE 102–108, with CVSS 8.1.
- CVE-2026-0506 involves a missing authorization check in SAP NetWeaver AS ABAP / ABAP Platform across SAP_BASIS versions 700–816, rated CVSS 8.1.
- Seven Medium-severity and two Low-severity vulnerabilities cover additional components across SAP environments but still require remediation within regular maintenance cycles.
- Affected SAP modules include financials, transformation services, database engines, reconciliation workflows, and ABAP application servers—key systems supporting financial sector operations.
- Vulnerabilities range from remote code execution and SQL injection to privilege escalation and missing authorization checks, increasing risk of data compromise or unauthorized system activity.

Recommendations

- Prioritize patching of all Critical and High-severity SAP Notes.
- Apply Medium-severity patches during scheduled maintenance windows.
- Review role-based access controls (RBAC) for affected SAP modules.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Adobe January 2026 Patch Bundle Fixes 25 Vulnerabilities	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Adobe has released its January 2026 Patch Tuesday updates addressing 25 vulnerabilities across 11 products, including several critical arbitrary code execution flaws. The highest-severity issue, CVE-2025-66516 (CVSS 10.0), impacts ColdFusion through a vulnerable Apache Tika dependency and allows remote code execution via malicious PDF/XFA input.

These vulnerabilities pose elevated risk to financial services institutions relying on Adobe platforms for document workflows, reporting, customer communications, and internal content production, where RCE or memory corruption can jeopardize confidentiality, operational continuity, and trust.

Technical Details

- ColdFusion contains CVE-2025-66516 (CVSS 10.0), an XXE vulnerability through Apache Tika enabling remote code execution, SSRF, information disclosure, and denial-of-service, affecting ColdFusion 2025 Update 5 and earlier, and ColdFusion 2023 Update 17 and earlier.
- ColdFusion is rated Priority 1 due to the severity of the RCE vector, with fixes available in ColdFusion 2025 Update 6 and ColdFusion 2023 Update 18.
- Dreamweaver (APSB26-01) patches multiple critical vulnerabilities—CVE-2026-21267, 21268, 21271, 21272, and 21274—spanning OS command injection, inadequate validation, arbitrary file write, and authorization bypass, with fixes in version 21.7.
- InDesign (APSB26-02) resolves issues involving uninitialized pointers, heap buffer overflows, and out-of-bounds reads (CVE-2026-21275, 21276, 21277, 21304, 21278), enabling remote code execution or memory exposure, fixed in versions ID21.1 and ID20.5.1.
- Illustrator (APSB26-03) addresses critical and important vulnerabilities including untrusted search path RCE and NULL pointer dereference (CVE-2026-21280, 21288), with fixes in versions 29.8.4+ and 30.1+.
- InCopy (APSB26-04) patches CVE-2026-21281, a heap buffer overflow leading to remote code execution, with fixes in versions 21.1 and 20.5.1.
- Bridge (APSB26-07) fixes CVE-2026-21283, a critical heap buffer overflow enabling RCE, with remediations in versions 15.1.3 (LTS) and 16.0.1.
- Substance 3D Modeler addresses multiple RCE, DoS, and memory exposure flaws (CVE-2026-21298 through 21303), including out-of-bounds writes and NULL dereferences.
- Substance 3D Stager patches CVE-2026-21287, a use-after-free leading to RCE, while Substance 3D Painter fixes CVE-2026-21305, an out-of-bounds write enabling RCE.
- Substance 3D Sampler resolves CVE-2026-21306, a critical RCE vulnerability, with Substance 3D Designer addressing CVE-2026-21308, an out-of-bounds read causing memory leak.
- These vulnerabilities span input validation flaws, memory corruption, pointer errors, and insecure file handling, affecting a broad set of Adobe product families used in enterprise environments.

Recommendations

- Apply all Adobe January 2026 security updates without exception.
- Prioritize remediation in the following order:

  o ColdFusion (Priority 1)

  o All Critical RCE client-side products

  o Remaining high/medium severity products.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical and High-Severity Vulnerabilities in ManageEngine Identity and Privileged Access Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

ManageEngine has released fixes for multiple vulnerabilities affecting its identity management and privileged access solutions, including ADSelfService Plus, PAM360, Password Manager Pro, and Access Manager Plus. The most severe flaw, CVE-2025-11250, impacts ADSelfService Plus and could allow compromise of the application and underlying identity services.

These vulnerabilities directly affect financial institutions relying on ManageEngine for identity workflows and privileged access governance, creating potential pathways for unauthorized access to critical systems, sensitive financial data, and infrastructure components.

Technical Details

- CVE-2025-11250 is a critical vulnerability in ADSelfService Plus affecting builds 6518 and earlier, where exploitation could compromise the application and identity services, with remediation available in build 6519.
- The flaw may enable attackers to interfere with authentication, user self-service operations, or identity-linked backend components, depending on deployment architecture.
- CVE-2025-11669 is a high-severity unauthorized access vulnerability impacting multiple privileged access products—PAM360, Password Manager Pro, and Access Manager Plus.
- PAM360 is vulnerable up to build 8201, Password Manager Pro up to build 13220, and Access Manager Plus up to build 4400, with fixes provided in builds 8202, 13221, and 4401 respectively.
- Exploitation of CVE-2025-11669 requires managed resources to be network-accessible from the product server, enabling unauthorized access paths if network segmentation is weak.
- These issues affect privileged credential vaulting, administrative session brokering, and remote resource access workflows central to enterprise security.
- Improper isolation of managed resources could allow attackers to pivot from the affected ManageEngine product to connected devices.
- Vulnerabilities span both identity self-service platforms and privileged access management controls, increasing overall risk if left unpatched.
- Successful exploitation could result in elevated access, unauthorized resource interactions, or compromise of sensitive administrative functions.
- The vendor has issued fixed builds for all impacted products, with patching required to restore secure operation.

Recommendations

- Immediately upgrade ADSelfService Plus, PAM360, Password Manager Pro, and Access Manager Plus to their latest fixed versions to remediate the identified critical and high-severity vulnerabilities.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Privilege Escalation in ServiceNow AI Platform	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

ServiceNow has addressed a critical privilege escalation vulnerability, tracked as CVE-2025-12420, affecting its AI Platform. The flaw allowed unauthenticated attackers to impersonate legitimate users by exploiting weaknesses in account-linking and authentication logic, potentially bypassing MFA and SSO protections.

This vulnerability is particularly relevant to financial institutions leveraging ServiceNow for workflow automation and AI-assisted operations, as unauthorized privilege escalation could expose sensitive data, compromise service processes, or enable fraudulent system-level activity.

Technical Details

- CVE-2025-12420 carries a critical severity rating with a CVSS score of 9.8 and is classified as Execution with Unnecessary Privileges (CWE-250), enabling privilege escalation without authentication.
- The vulnerability resided within the authentication and account-linking mechanisms of the ServiceNow AI Platform, allowing attackers to assume identities of valid users.
- Exploitation could bypass multi-factor authentication (MFA) and single sign-on (SSO) controls, granting access to privileged actions normally restricted to authorized personnel.
- Affected components include the Now Assist AI Agents and Virtual Agent API, both foundational elements in automated and AI-driven workflows.
- Now Assist AI Agents were impacted prior to versions 5.1.18 and 5.2.19, which contain the security fix.
- The Virtual Agent API was vulnerable before versions 3.15.2 and 4.0.4, which include the required remediation.
- The flaw could facilitate impersonation attacks, enabling unauthorized actions across workflows dependent on AI-based task execution.
- Its impact spans identity integrity, operational workflow security, and potential exposure of sensitive business functions.
- No exploitation details were provided, but the privilege escalation risk makes unpatched environments vulnerable to unauthorized activity.

- Immediate verification and upgrade of affected modules is required to restore secure authentication behavior.

Recommendations

- Verify deployed versions of Now Assist AI Agents and Virtual Agent API and Apply updates immediately if running vulnerable versions.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Command Injection Vulnerability in NVIDIA Nsight Graphics for Linux	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

NVIDIA has released a security update addressing CVE-2025-33206, a high-severity command injection vulnerability in Nsight Graphics on Linux systems. The flaw arises from improper neutralization of OS command elements, enabling attackers to execute arbitrary commands.

This vulnerability is relevant to financial institutions operating Linux-based development, analytics, or GPU-accelerated workflows, where exploitation could lead to unauthorized code execution, system compromise, and disruption of critical research or application environments.

Technical Details

- CVE-2025-33206 is rated CVSS 7.8 (High) and categorized under CWE-78, indicating improper neutralization of special elements used in OS commands, resulting in command injection risk.
- The vulnerability affects NVIDIA Nsight Graphics for Linux, allowing attackers to craft malicious input triggering execution of arbitrary system commands.
- Under certain conditions, successful exploitation can escalate into remote code execution, depending on deployment context and user privileges.
- Potential impacts include arbitrary code execution, privilege escalation, unauthorized data modification, and denial-of-service conditions.
- All versions of Nsight Graphics prior to 2025.5 are affected, exposing Linux-based GPU analysis and debugging environments to manipulation.
- The flaw could enable attackers to interfere with profiling or debugging workflows tied to GPU-accelerated applications.
- NVIDIA has released version 2025.5 as the fixed build containing the required security correction.
- The vulnerability stems from improper handling of command-line input that allows OS command injection through crafted payloads.
- Attack success may depend on how Nsight Graphics interacts with external tools and user-initiated workflows.

- This issue underscores the risks associated with unvalidated OS command execution paths within development and analysis tools.

Recommendations

- Update NVIDIA Nsight Graphics for Linux to version 2025.5 or later immediately across all environments.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerability in Palo Alto Networks Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Palo Alto Networks has disclosed a high-severity denial-of-service vulnerability (CVE-2026-0227) impacting PAN-OS firewalls and Prisma Access deployments where GlobalProtect Gateway or Portal is enabled. An unauthenticated attacker can repeatedly trigger the flaw to force devices into maintenance mode, causing complete service disruption.

This issue presents material risk to financial institutions relying on GlobalProtect for secure remote access, network segmentation, and user authentication. Exploitation could interrupt secure connectivity for trading desks, payment systems, and core financial operations.

Technical Details

- CVE-2026-0227 is rated CVSS 8.7 (High) and allows an unauthenticated remote attacker to repeatedly trigger a condition that forces the firewall into maintenance mode, resulting in a full denial-of-service.
- The vulnerability affects only deployments with GlobalProtect Gateway or Portal enabled, increasing risk for organizations dependent on remote access infrastructure.
- Impacted PAN-OS versions include: 12.1 (earlier than 12.1.3-h3 and 12.1.4), 11.2 (earlier than 11.2.4-h15, 11.2.7-h8, and 11.2.10-h2), 11.1 (earlier than 11.1.4-h27, 11.1.6-h23, 11.1.10-h9, and 11.1.13), 10.2 (earlier than 10.2.7-h32, 10.2.10-h30, 10.2.13-h18, 10.2.16-h6, and 10.2.18-h1), and 10.1 (earlier than 10.1.14-h20).
- Prisma Access versions affected include 11.2 (earlier than 11.2.7-h8*) and 10.2 (earlier than 10.2.10-h29*), where the issue can similarly result in GlobalProtect-triggered device failure.
- Exploitation can be repeated at will, enabling sustained service interruption if unpatched devices are exposed or reachable externally.
- The vulnerability directly impacts firewall availability, tunnel establishment, and secure remote-user workflows.
- Attackers do not require credentials, increasing exposure for internet-facing gateways.
- Devices entering maintenance mode become inoperable until manually restored, prolonging disruption.

- All unsupported older PAN-OS versions remain vulnerable and require upgrading to supported, fixed releases.
- The fix has been included in later hotfixes and major versions across all affected PAN-OS and Prisma Access release trains.

Recommendations

- Upgrade immediately to the fixed versions: PAN-OS 12.1.4+, 11.2.10-h2+ / 11.2.7-h8+ / 11.2.4-h15+, 11.1.13+, 10.2.18-h1+, and 10.1.14-h20+.
- For Prisma Access, upgrade to 11.2.7-h8+ or 10.2.10-h29+ to eliminate the DoS condition.
- Prioritize patching for all GlobalProtect-enabled, internet-facing nodes supporting remote access into financial systems.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Unauthenticated Privilege Escalation in Modular DS WordPress Plugin	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

The Modular DS WordPress plugin has been found to contain a critical unauthenticated privilege escalation vulnerability, tracked as CVE-2026-23550, affecting versions 2.5.1 and below. The flaw allows remote attackers to gain full administrative (wp-admin) access without authentication.

This issue is highly relevant to financial sector organizations operating public-facing WordPress sites, as successful exploitation enables complete site takeover, unauthorized content manipulation, credential theft, and long-term persistence that can be weaponized for fraud or supply-chain attacks.

Technical Details

- CVE-2026-23550 is rated CVSS 10.0 (Critical) and stems from multiple chained design and implementation weaknesses within the Modular DS plugin.
- The vulnerability enables remote, unauthenticated adversaries to bypass authentication and directly obtain administrative privileges on affected WordPress instances.
- Root causes include flawed request-authentication logic, attacker-controlled routing decisions, and an insecure auto-login fallback mechanism embedded within the plugin.
- Exploitation has been confirmed in the wild, with attackers logging in as administrators and creating malicious persistent admin accounts.
- The affected install base includes 40,000+ WordPress sites, significantly expanding the potential attack surface.
- Versions ≤ 2.5.1 of Modular DS are vulnerable, enabling attackers to escalate privileges without credentials.

- Patched versions begin at 2.5.2, which corrects the insecure authentication pathways.
- Attackers can leverage administrative access to modify site configurations, inject malicious code, or pivot into environments linked to the WordPress instance.
- Financial institutions relying on WordPress for public-facing portals are at heightened risk of reputational and operational impact.
- This vulnerability allows full wp-admin takeover, supporting long-term persistence and automated malware deployment.

Recommendations

- Upgrade Modular DS plugin to fixed version immediately.
- Review WordPress admin user list: Remove unauthorized or suspicious accounts.

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 Patched in Mozilla Firefox and Thunderbird	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Mozilla has released security updates for Firefox and Thunderbird addressing multiple high-severity vulnerabilities across browser and messaging components. These flaws could allow attackers to bypass security restrictions, escape sandboxes, or execute arbitrary code.

This update is particularly relevant to financial sector organizations where browser integrity is critical for accessing trading systems, digital banking portals, payment platforms, and customer communication tools.

Technical Details

- CVE-2026-0877 is a mitigation bypass issue in the DOM Security component, allowing attackers to circumvent built-in protections.
- CVE-2026-0878 involves incorrect boundary conditions in the Graphics: CanvasWebGL component, enabling sandbox escape scenarios.
- CVE-2026-0879 affects Graphics boundary handling, similarly allowing sandbox breakout under crafted conditions.
- CVE-2026-0880 is an integer overflow within Graphics that can be abused for sandbox escape and subsequent privilege misuse.
- CVE-2026-0881 impacts the Messaging System component, supporting sandbox escape through manipulated messaging workflows.

- CVE-2026-0882 is a use-after-free vulnerability in the IPC component, posing risk of memory corruption and potential code execution.
- CVE-2026-0891 encompasses memory safety bugs addressed in Firefox ESR 140.7, Thunderbird ESR 140.7, Firefox 147, and Thunderbird 147.
- Collectively, these vulnerabilities allow remote code execution, sandbox escape, mitigation bypass, and memory corruption.
- Successful exploitation could lead to application crashes or compromise of sensitive browser-handled data.
- The issues affect multiple ESR and mainstream release channels, expanding the scope of potential exposure across enterprise environments.

Recommendations

- Update all instances of Firefox and Thunderbird to the latest fixed versions: Firefox 147, Firefox ESR 115.32, Firefox ESR 140.7, Thunderbird 147, and Thunderbird 140.7.
- Prioritize updates on systems handling financial transactions, corporate authentication workflows, and sensitive customer information.
- Enforce browser update controls and automated patching across managed endpoints to reduce exposure windows.

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

deVixor: An Evolving Android Banking RAT with Ransomware Capabilities Targeting Iran

Tactic	Technique ID	Procedure
Initial Access (TA0027)	Phishing (T1660)	Malware is distributed via a phishing site
Persistence (TA0028)	Event Triggered Execution: Broadcast Receivers(T1624.001)	deVixor registered the BOOT_COMPLETED broadcast receiver to activate on device startup
Persistence (TA0028)	Foreground Persistence (T1541)	deVixor uses foreground services by showing a notification
Defense Evasion (TA0030)	Hide Artifacts: Suppress Application Icon (T1628.001)	deVixor hides icon
Defense Evasion (TA0030)	Impair Defenses: Prevent Application Removal (T1629.001)	Prevent uninstallation
Defense Evasion (TA0030)	Impair Defenses: Disable or Modify Tools (T1629.003)	deVixor can disable Google Play Protect
Defense Evasion (TA0030)	Masquerading: Match Legitimate Name or Location (T1655.001)	Masquerade as a YouTube app
Defense Evasion (TA0030)	Obfuscated Files or Information (T1406)	deVixor uses an encrypted C&C server URL
Credential Access (TA0031)	Access Notifications (T1517)	deVixor collects device notifications
Credential Access (TA0031)	Input Capture: Keylogging (T1417.001)	deVixor collects keylogged data
Credential Access (TA0031)	Input Capture: GUI Input Capture (T1417.002)	deVixor collects entered banking credentials
Discovery (TA0032)	Software Discovery (T1418)	deVixor collects the installed application list
Discovery (TA0032)	System Information Discovery (T1426)	deVixor collects the device information
Collection (TA0035)	Archive Collected Data (T1532)	deVixor compressing collected data and saving to a .zip file
Collection (TA0035)	Data from Local System (T1533)	deVixor collects media from the gallery
Collection (TA0035)	Protected User Data: Contact List (T1636.003)	Collects contact data
Collection (TA0035)	Protected User Data: SMS Messages (T1636.004)	Collects SMS data
Collection (TA0035)	Protected User Data: Accounts (T1636.005)	deVixor collects Accounts data
Collection (TA0035)	Screen Capture (T1513)	deVixor can take Screenshots
Command and Control (TA0037)	Application Layer Protocol: Web Protocols (T1437.001)	Malware uses HTTPs protocol
Exfiltration (TA0036)	Exfiltration Over C2 Channel (T1646)	deVixor sends collected data to the C&C server
Impact (TA0034)	SMS Control (T1582)	deVixor can send SMSs from the infected device

DeadLock ransomware uses blockchain for evasion

MITRE Tactic	Technique ID	Technique Name	Behavior/Procedure
Command & Control	T1102.003	Web Protocols: Web APIs / Blockchain-based C2 channels	Use of Polygon smart contracts to rotate and store proxy server (C2) addresses
Command & Control	T1102	Web Service	Retrieval of proxy URLs via JavaScript interacting with Polygon RPC endpoints
Command & Control	T1105	Ingress Tool Transfer	Dropping an HTML file that serves as a wrapper for the Session encrypted messenger
Command & Control	T1568.002	Dynamic Resolution: Application-layer protocol	Use of Session decentralized messenger for attackerâ€“victim communication
Lateral Movement / Command & Control	T1219	Remote Access Software	Use of AnyDesk for remote monitoring and lateral movement
Impact	T1490	Inhibit System Recovery	Deletion of shadow copies to prevent recovery
Defense Evasion	T1562.001	Impair Defenses: Disable Security Tools	Deletion of services or disabling system protection
Defense Evasion	T1027	Obfuscated/Encrypted Infrastructure	Use of blockchain-based infrastructure to avoid takedowns and provide resiliency
Command & Control	T1008	Fallback Channels / Rotating Infrastructure	Use of infinite proxy variants via smart contract updates

SHADOW#REACTOR Multi-Stage Campaign Uses Text-Only Staging to Deploy Remcos RAT

Tactics	Techniques
Initial Access	T1204: User Execution
Execution	T1059.005: Visual Basic
	T1059.001: PowerShell
	T1620: Reflective Code Loading
	T1047: MSBuild Abuse / Signed Binary Proxy Execution
Persistence	T1060: Startup Folder / Shortcut
Defense Evasion	T1027: Obfuscated/Encrypted Payloads
	T1112 / T1116: Execution Policy Bypass and LOLBAS Abuse
Command and Control	T1105: Ingress Tool Transfer
	T1219: Remote Access Tools

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
.NET Reactor	Code protection tool used to obscure malware loaders.
ABAP	SAP application server and programming language.
AnyDesk	Remote access tool frequently abused by threat actors.
APK	Android Package file used to install applications on Android devices.
AsyncRAT	Remote administration malware enabling keylogging and remote commands.
Base64	Encoding format used to hide payloads.
BEC	Business Email Compromise fraud operations.
Blink	Chrome rendering engine targeted by exploits.
C2	Command and Control infrastructure used by attackers to manage compromised systems.
CIRO	Canadian Investment Regulatory Organization; a financial self regulatory body whose systems were breached.
Cloudflare	Cloud service abused to hide malicious infrastructure.
CRC32	Checksum used to verify file integrity; manipulated for evasion.
CSC	UAE Cyber Security Council
CVE	Common Vulnerabilities and Exposures identifier.
CVSS	Vulnerability severity scoring system.
CWE78	Improper neutralization of OS commands classification.
Data Exfiltration	Unauthorized transfer of data out of an organization.
Docker	Container platform supporting cloud applications, targeted by malware.
Fintech	Financial technology platforms offering digital financial services.
Git	Version control system exposed via Gogs vulnerability.
GlobalProtect	Palo Alto Networks VPN platform with DoS vulnerability.
Heap Buffer Overflow	Memory corruption flaw enabling RCE.
HotNews	SAP s highest severity patch category.
IPC	Inter Process Communication targeted by vulnerabilities.
JScript	Microsoft scripting language often used to deliver malware.
Kubernetes	Container orchestration platform targeted by cloud native malware.
Living Off the Land	Use of legitimate tools like PowerShell for malicious activity.

LogMeIn Rescue	Legitimate RMM tool misused for unauthorized access.
LSASS	Windows authentication process targeted for credential theft.
MFA	Multi Factor Authentication security control.
MSBuild.exe	Legitimate Windows build tool abused as a LOLBin for malware.
NSIS	Installer system used to package payload downloaders.
NTFS	Windows file system; used for shortname execution in attacks.
OTP	One Time Password used for authentication, frequently targeted in fraud.
Polygon	Blockchain platform abused by DeadLock ransomware for C2.
PowerShell	Windows automation tool widely abused for lateral movement.
PsExec	Remote execution tool abused for privilege escalation.
RAT	Remote Access Trojan enabling full remote control of infected systems.
RCE	Remote Code Execution vulnerability.
RDP	Remote Desktop Protocol used for remote access and abuse.
Reflective Loading	In memory execution technique avoiding file system writes.
Regex	Pattern matching syntax used for text extraction.
Remcos RAT	Commercial RAT abused for remote control.
RMM	Remote Monitoring & Management tools leveraged for stealthy access.
Rootkit	Stealth mechanism enabling deep system persistence.
Sandbox Escape	Breaking isolation boundaries in browsers/applications.
Secure Boot	System integrity mechanism vulnerable to bypass.
Smart Contract	Blockchain based code used to store rotating ransomware infrastructure.
Social Engineering	Psychological manipulation used to trick individuals into revealing information or performing harmful actions.
SSO	Single Sign On authentication system.
SSRF	Server Side Request Forgery allowing unauthorized internal access.
Tika	Apache library implicated in ColdFusion RCE.
V8 Engine	Chrome JavaScript engine affected by vulnerabilities.
VBS	Visual Basic Script used for staged malware launchers.
VDS	Virtual Dedicated Server used for criminal infrastructure.
WebDAV	Web based file sharing protocol used to host malware payloads.
WebView	Android component that displays web content inside apps, abused for credential harvesting.
Wp admin	Administrative interface of WordPress vulnerable to takeover.
XOR	Simple obfuscation technique used by attackers.
XXE	XML External Entity attack using malicious XML parsing.
Zero Day	Previously unknown vulnerability exploited before a patch exists.