TLP:CLEAR

ADGM

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	17/12/2025
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 17 December 2025

1	0	14	8
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 Zero-day vulnerabilities

Summary

This week's cybersecurity newsletter highlights a surge in advanced threats and critical vulnerabilities impacting global organizations, with direct implications for financial services. Key observations include sophisticated campaigns such as EtherRAT leveraging blockchain-based C2, GrayBravo's CastleLoader malware-as-a-service ecosystem, and vishing attacks abusing Microsoft Teams and Quick Assist for fileless .NET malware delivery. Other notable campaigns involve Phantom Stealer distributed via ISO-mounted executables, JSCEAL targeting cryptocurrency users, and supply-chain exposure in Notepad++ updates.

On the vulnerability front, actively exploited zero-days in Microsoft, Google Chrome, and Apple products underscore the urgency of patching, alongside critical flaws in SAP, Ivanti Endpoint Manager, and Fortinet devices that could enable remote code execution and administrative compromise. These developments highlight the growing sophistication of adversaries and the expanding attack surface across enterprise and cloud ecosystems. Financial institutions should prioritize timely patching, enforce strict access controls, monitor for anomalous behaviors, and strengthen user awareness to mitigate these evolving risks.

ADGM THREAT INTELLIGENCE SUMMARY

ThinkMarkets Suffers Ransomware Breach Exposing 512GB of Sensitive Data [Cyber Breach] [HIGH]

DPRK Deploys EtherRAT Implant via React2Shell Exploits Using Ethereum-Based C2 [Campaign] [HIGH]

Spiderman Phishing Kit Enables Large-Scale Attacks on European Banks and Crypto Platforms [Campaign] [HIGH]

Malicious VSCode Extensions Deploy Infostealers via DLL Hijacking [Campaign] [HIGH]

Ashen Lepus Deploys AshTag Backdoor in Espionage Campaign Targeting Middle East [Campaign] [HIGH]

Storm-0249 Evolves from Mass Phishing to EDR Exploitation via DLL Sideloading [Campaign] [MEDIUM]

Vishing Campaign Exploits Microsoft Teams and Quick Assist for Fileless .NET Malware Deployment [Campaign] [MEDIUM]

JS#SMUGGLER Uses Compromised Sites and HTA/PowerShell Chain to Install NetSupport RAT [Campaign] [MEDIUM]

Akira Ransomware Targets Hyper-V and ESXi to Encrypt VMs at Scale via Hypervisor Exploitation [Campaign] [MEDIUM]

GrayBravo Uses ClickFix Technique to Deliver CastleLoader Malware Across Multiple Industries [Campaign] [MEDIUM]

NANOREMOTE Backdoor Exploits Google Drive API for Covert Control on Windows Systems [Campaign] [MEDIUM]

ConsentFix Attack Hijacks Microsoft Accounts via Azure CLI OAuth in Browser-Only Flow [Campaign] [MEDIUM]

Adversary-in-the-Middle Phishing Campaign Targets Microsoft 365 and Okta SSO Users [Campaign] [MEDIUM]

JSCEAL Infostealer Adopts Hardened C2 and Anti-Analysis Tactics to Target Crypto Users [Campaign] [MEDIUM]

Operation MoneyMount-ISO Delivers Phantom Stealer via ISO-Mounted Executables [Campaign] [MEDIUM]

Microsoft Zero-Day Vulnerabilities Enable Privilege Escalation and Remote Code Execution [Vulnerability] [HIGH]

Actively Exploited Zero-Day in Google Chrome Requires Immediate Patch [Vulnerability] [HIGH]

Apple Patches Actively Exploited WebKit Zero-Days Across iOS, macOS, and Safari [Vulnerability] [HIGH]

Multiple High-Severity Flaws in Firefox and Thunderbird [Vulnerability] [HIGH]

SAP December 2025 Security Updates Address Critical Code Injection and Deserialization Flaws [Vulnerability] [MEDIUM]

Ivanti Endpoint Manager Update Fixes Critical XSS and High-Severity File Manipulation Flaws [Vulnerability] [MEDIUM]

Fortinet December 2025 Security Updates Address Critical FortiCloud SSO Authentication Bypass [Vulnerability] [MEDIUM]

Supply-Chain Exposure in Notepad++ Updater Enables Malware Delivery via Manipulated Network Traffic [Vulnerability] [MEDIUM]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
ThinkMarkets Suffers Ransomware Breach Exposing 512GB of Sensitive Data	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

ThinkMarkets, a global online trading broker with operations in the UAE, has reportedly suffered a significant data breach after being targeted by the Chaos ransomware group. The attackers claim to have exfiltrated 512 GB of sensitive data, including HR records, legal documents, trading information, and KYC details of clients.

This incident is critical for the financial services sector as it exposes sensitive customer and operational data, potentially impacting trust, compliance, and regulatory obligations. The breach highlights the growing ransomware threat to brokers and trading platforms operating in high-value markets like MENA.

Technical Details

- The Chaos ransomware group listed ThinkMarkets on its dark web extortion site on December 8, claiming responsibility for the breach.
- Attackers allege theft of 512 GB of data, including HR files, customer dispute records, legal advice, company policies, and trading-related information.
- Observed leaked data includes passport scans of employees and KYC documentation of clients, indicating exposure of personally identifiable information (PII).
- Chaos ransomware supports multiple platforms, including Windows, ESXi, Linux, and NAS systems, enabling broad attack surface coverage.
- The malware uses individual file encryption keys and rapid encryption speeds, combined with network resource scanning for lateral movement.
- The group operates an automated panel for managing victims and ransom negotiations, requiring a paid entry fee for affiliates.
- Chaos emphasizes high-speed encryption and robust security measures, making recovery challenging without backups.
- The group actively promotes its ransomware on Russian-language forums and recruits affiliates for distribution.
- Chaos claims to avoid targeting BRICS/CIS countries, hospitals, and government entities, focusing instead on commercial organizations.
- ThinkMarkets have a global footprint, including offices in the Middle East, increasing regional exposure risk.

Recommendations

- Immediately review and strengthen endpoint protection and EDR solutions to detect ransomware behaviors.

- Implement strict network segmentation and disable unnecessary services to limit lateral movement opportunities.
- Enforce multi-factor authentication (MFA) across all critical systems, especially remote access points.
- Regularly back up critical data offline and test restoration procedures to ensure resilience against encryption attacks.
- Monitor for leaked data on dark web sources and initiate incident response for regulatory compliance and client notification.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
DPRK Deploys EtherRAT Implant via React2Shell Exploits Using Ethereum-Based C2	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified EtherRAT, a novel implant deployed through React2Shell exploitation just days after CVE-2025-55182 disclosure. This advanced malware leverages Ethereum smart contracts for command-and-control, employs multiple persistence techniques, and downloads its own Node.js runtime for stealthy operations.

This campaign poses a significant risk to financial services as it targets widely used frameworks like React and Next.js, enabling attackers to gain persistent access to web applications that may handle sensitive financial transactions and client data.

Technical Details

- EtherRAT exploits CVE-2025-55182, an unsafe deserialization vulnerability in React Server Components, allowing unauthenticated remote code execution.
- The attack chain consists of four stages: shell dropper, Node.js deployment, encrypted loader, and persistent implant.
- Initial access is achieved via a base64-encoded shell command that downloads and executes a malicious script.
- EtherRAT downloads a legitimate Node.js runtime from nodejs.org to reduce detection risk and execute its payload.
- The implant uses AES-256-CBC encryption for payload decryption, enhancing obfuscation and evasion.
- Command-and-control is resolved through Ethereum smart contracts, avoiding static infrastructure and complicating takedown efforts.

- C2 polling occurs every 500 milliseconds, executing JavaScript commands received from the server.
- Five Linux persistence mechanisms are deployed: systemd user service, XDG autostart, cron job, bashrc injection, and profile injection.
- EtherRAT includes a self-update feature, sending its source code to a remote endpoint and replacing itself with re-obfuscated code.
- Overlap with DPRK-affiliated tooling suggests nation-state involvement or advanced tool-sharing among threat actors.

Recommendations

- Patch immediately: Upgrade React to 19.2.1+ and Next.js to patched versions; rebuild and redeploy applications.
- Hunt for persistence: Inspect systems for unauthorized services, cron jobs, and shell configuration changes.
- Monitor Ethereum RPC traffic: Investigate unusual outbound connections from application servers.
- Deploy runtime detection: Use behavioral monitoring to detect implants that dynamically modify code.
- Review application logs: Identify suspicious POST requests to RSC endpoints and rotate exposed credentials promptly.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Spiderman Phishing Kit Enables Large-Scale Attacks on European Banks and Crypto Platforms	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have uncovered Spiderman, a sophisticated phishing kit designed to replicate login portals of dozens of European banks and financial services providers. The kit offers attackers an automated interface to launch phishing campaigns, intercept credentials, and manage victim sessions in real time.

This campaign is highly relevant to financial institutions as it demonstrates the growing ease of executing cross-border fraud, including hybrid banking and cryptocurrency theft. Its advanced evasion and OTP interception capabilities pose significant risks to payment service providers and wealth management platforms.

Technical Details

- Spiderman is a full-stack phishing framework that clones login pages of major European banks, government portals, and crypto wallet providers.
- Targets include Deutsche Bank, Commerzbank, ING, CaixaBank, and cryptocurrency platforms such as Ledger, Metamask, and Exodus.
- The kit's modular design allows attackers to add new banks and authentication flows, ensuring long-term adaptability.
- Operators can launch attacks with minimal effort—select a bank, generate a phishing page, and send pre-built lures.
- Real-time session monitoring enables attackers to capture credentials, OTP codes, and credit card details during the phishing workflow.
- Advanced anti-analysis features include country whitelisting, ISP/ASN filtering, device-type restrictions, and custom redirects to evade detection.
- OTP interception modules (PhotoTAN) allow attackers to bypass multi-factor authentication used by European banks.
- Captured data includes usernames, passwords, full identity details, credit card information, and device metadata for account takeover and fraud.
- The kit's operator dashboard supports credential export and session tracking, streamlining large-scale phishing operations.
- A Signal group linked to the kit's seller has ~750 members, indicating active distribution and widespread adoption.

Recommendations

- Implement advanced phishing detection and takedown services to monitor cloned banking portals.
- Enforce strong multi-factor authentication methods resistant to real-time interception, such as hardware tokens.
- Educate customers on phishing risks and encourage verification of URLs before entering credentials.
- Monitor for suspicious traffic patterns, including geo-specific anomalies and repeated failed login attempts.
- Collaborate with financial sector ISACs and law enforcement to share intelligence on emerging phishing kits.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Malicious VSCode Extensions Deploy Infostealers via DLL Hijacking	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have uncovered a campaign leveraging Visual Studio Code extensions to deliver advanced infostealers. Two extensions—Bitcoin Black and Codo AI—masquerade as a theme and an AI coding assistant but execute malicious payloads that capture screenshots, steal credentials, and hijack browser sessions.

This campaign is highly relevant to financial institutions as compromised developer environments can expose sensitive code, credentials, and session tokens, creating downstream risks for payment systems, fintech platforms, and trading applications.

Technical Details

- Bitcoin Black, marketed as a premium dark theme, includes activation events and PowerShell execution—behavior not typical for VSCode themes.
- Codo AI provides real AI functionality but embeds malicious code before legitimate features, reducing detection likelihood.
- Both extensions deliver the Lightshot screenshot tool bundled with a malicious DLL, exploiting DLL hijacking (MITRE T1574.001).
- The malicious DLL executes an infostealer that harvests clipboard data, WiFi credentials, installed programs, and system details.
- The malware captures full desktop screenshots, exposing sensitive information such as code, emails, and chat sessions.
- Browser hijacking is performed by launching Chrome and Edge in headless mode with flags for cookies and session theft.
- The DLL uses the mutex COOL_SCREENSHOT_MUTEX_YARRR, derived from legitimate Lightshot code, complicating behavioral detection.
- Payload staging occurs in %APPDATA%\Local\Evelyn, where stolen data is aggregated before exfiltration.
- The attacker employs A/B testing with two lures—crypto-themed and AI productivity—to target different developer demographics.
- At least one malicious extension remains live on the VSCode marketplace, indicating ongoing exposure risk.

Recommendations

- Audit installed VSCode extensions and remove any unverified or suspicious packages immediately.
- Implement application whitelisting and restrict developer environments from executing unauthorized scripts.

- Monitor for DLL hijacking indicators and unusual process trees involving legitimate binaries like Lightshot.exe.
- Deploy endpoint detection solutions capable of identifying credential theft and browser session hijacking behaviors.
- Educate developers on supply chain risks and enforce strict extension vetting policies before installation.

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
Ashen Lepus Deploys AshTag Backdoor in Espionage Campaign Targeting Middle East	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have analyzed a long-running espionage campaign by Ashen Lepus, a Hamas-linked threat actor, targeting governmental and diplomatic entities across the Middle East. The group has introduced AshTag, a modular .NET malware suite, alongside enhanced operational security measures to evade detection.

This campaign is significant for financial and governmental sectors in the region as it demonstrates advanced persistence and data exfiltration capabilities, posing risks to sensitive communications and strategic assets.

Technical Details

- Ashen Lepus has been active since 2018, focusing on Arabic-speaking government entities and expanding to Oman, Morocco, and other nations.
- Infection begins with a benign PDF lure leading to a RAR archive containing a binary, a malicious loader, and a decoy PDF.
- The binary side-loads a DLL (AshenLoader), which opens the decoy PDF while executing malicious code in the background.
- AshenLoader retrieves AshenStager, which downloads and executes the AshTag payload and sets persistence via scheduled tasks.
- AshTag is a modular .NET toolset supporting file exfiltration, command execution, and in-memory module loading.
- Payload encryption and infrastructure obfuscation using legitimate subdomains enhance evasion.
- Secondary payloads are embedded within HTML tags on benign-looking pages, complicating detection.

- C2 servers perform geolocation and User-Agent checks to avoid sandbox analysis and ensure delivery only to intended victims.
- The campaign uses DLL side-loading and in-memory execution to minimize forensic artifacts.
- Lure themes remain geopolitical, with recent focus on Turkey and Palestinian affairs.

Recommendations

- Monitor for suspicious DLL side-loading activity and scheduled task creation on endpoints.
- Implement network monitoring for anomalous subdomain requests and HTML-based payload delivery.
- Deploy behavioral detection for in-memory execution and modular malware patterns.
- Educate staff on spear-phishing risks and verify document sources before opening archives.
- Apply strict access controls and regularly audit systems for unauthorized persistence 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
Storm-0249 Evolves from Mass Phishing to EDR Exploitation via DLL Sideloading	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have observed Storm-0249, a seasoned initial access broker, shifting from large-scale phishing to precision exploitation of trusted EDR processes. The group now leverages DLL sideloading, fileless execution, and domain spoofing to blend malicious activity into legitimate operations, enabling stealthy ransomware delivery.

This evolution poses a significant threat to financial institutions and other high-value sectors, as attackers exploit trusted security software to maintain persistence and evade detection, accelerating ransomware attack timelines.

Technical Details

- Storm-0249 operates within the ransomware-as-a-service ecosystem, selling pre-built access to affiliates for rapid attack deployment.
- The campaign begins with ClickFix social engineering, tricking users into executing malicious commands via the Windows Run dialog.
- Attackers abuse curl.exe to download payloads, piping them directly into PowerShell for fileless execution in memory.

- Malicious scripts are hosted on spoofed Microsoft-like domains (e.g., sgcipl[.]com/us.microsoft.com/) to bypass user scrutiny and security filters.
- MSI packages downloaded from phishing URLs execute with SYSTEM privileges, enabling attackers to place files in protected directories.
- DLL sideloading targets SentinelOne's SentinelAgentWorker.exe, leveraging trust in signed security binaries to conceal malicious code.
- The trojanized DLL is dropped alongside legitimate SentinelOne executables in AppData, a location often excluded from strict monitoring.
- Attackers use domain spoofing and encrypted C2 traffic to disguise reconnaissance and persistence activities.
- Techniques observed include Living-off-the-Land binaries (LOLBins), fileless execution, and abuse of legitimate processes for stealth.
- These methods allow Storm-0249 to maintain undetected access, prolong dwell time, and facilitate ransomware deployment.

Recommendations

- Monitor trusted processes for anomalies such as DLL sideloading and unexpected outbound connections.
- Restrict execution of legitimate tools like curl.exe and PowerShell to prevent abuse for payload delivery.
- Enforce strict MSI installation policies and validate sources before execution.
- Strengthen DNS monitoring and block spoofed domains mimicking legitimate vendors.
- Deploy behavioral analytics and automated incident responses to detect evasion tactics and isolate compromised endpoints.

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

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Storm-0249

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Vishing Campaign Exploits Microsoft Teams and Quick Assist for Fileless .NET Malware Deployment	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have uncovered a sophisticated vishing campaign that combines social engineering with legitimate Microsoft tools to deliver multi-stage .NET malware. Attackers impersonate IT staff via Microsoft Teams calls, coerce victims into launching Quick Assist, and pivot to fileless execution using reflection-based in-memory loading.

This campaign poses a significant risk to financial institutions and other UAE organizations that rely on Microsoft 365 collaboration and remote assistance workflows. Abuse of trusted applications reduces user suspicion and bypasses traditional defenses, enabling rapid privilege escalation and stealthy persistence.

Technical Details

- Attack begins with spoofed Microsoft Teams calls impersonating senior IT staff to establish trust.
- Victims are instructed to launch Windows Quick Assist, granting attackers remote access under the guise of troubleshooting.
- Within ~10 minutes, victims are redirected to a malicious webpage (ciscocyber[.]com/verify.php) for payload delivery.
- A trojanized updater.exe executes as a .NET Core wrapper embedding loader.dll for fileless execution.
- loader.dll retrieves encryption keys from jysync[.]info, then downloads an encrypted payload from the same infrastructure.
- Payload is decrypted using AES-CBC combined with XOR obfuscation, complicating static analysis.
- Final stage uses .NET reflection to load the assembly directly into memory—no disk artifacts—evading signature-based detection.
- Execution occurs under the privileges of the user initiating Quick Assist, enabling lateral movement.
- Dual-layer cryptography and separated key management hinder forensic analysis and detection.
- Campaign demonstrates convergence of social engineering, abuse of legitimate tools, and advanced memory-resident techniques.

Recommendations

- Require out-of-band verification before granting remote access; disable unsolicited Quick Assist sessions by policy.
- Restrict and monitor Quick Assist usage, log session initiator identity and duration for anomaly detection.
- Enable EDR telemetry for .NET reflection, in-memory assembly loads, and process injection behaviors.

- Block or monitor outbound connections to jysync[.]info and investigate redirects to ciscocyber[.]com; enforce DNS filtering.
- Conduct vishing awareness training and simulations focused on Teams impersonation and remote support scams.

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
JS#SMUGGLER Uses Compromised Sites and HTA/PowerShell Chain to Install NetSupport RAT	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have analyzed JS#SMUGGLER, a multi-stage web-based campaign that injects an obfuscated JavaScript loader into compromised sites, pivots to a stealthy HTA via mshta.exe, and culminates in a PowerShell payload installing NetSupport RAT with persistence.

This matters to financial services because NetSupport RAT enables full remote control, data theft, and proxy capabilities; the web-delivered, fileless execution chain lowers detection odds across enterprise endpoints and browser-driven workflows.

Technical Details

- Stage 1 uses an obfuscated JavaScript loader with rotating arrays, numeric index mapping, and massive comment blocks to hide logic. It profiles device type and branches to iframe (mobile) or remote script (desktop).
- First-visit persistence logic via localStorage ensures execution only once per user, reducing noise and improving stealth during repeated browsing sessions.
- The loader triggers Stage 2 retrieval of a stealth HTA, dynamically generated from attacker infrastructure, executed covertly via mshta.exe.
- The HTA writes an encrypted PowerShell stager to disk, decrypts with AES-256-ECB + Base64 + GZIP and executes in memory to minimize forensic artifacts.
- Execution Policy Bypass is used to guarantee stager run; temporary artifacts are deleted post-run to reduce detection.
- Stage 3 PowerShell payload downloads a ZIP, extracts under ProgramData, and launches cli*.exe via hidden JScript.

- Persistence is achieved through disguised Startup shortcuts, ensuring automatic RAT execution on login across reboots.
- The final malware is NetSupport RAT, enabling remote desktop, file operations, command execution, keylogging (if added), and proxy tunneling.
- Behavioral traits indicate an actively maintained, modular framework optimized for stealth, control, and domain/device rotation.
- Node.js sandbox testing confirmed DOMContentLoaded handling, localStorage checks, and conditional redirection behaviors.

Recommendations

- Strengthen endpoint defenses: Detect HTA/mshta.exe abuse, fileless PowerShell execution, and anomalous chains (mshta.exe → powershell.exe → wscript.exe).
- Restrict script execution: Block untrusted JavaScript, HTA, and PowerShell from browser caches, %TEMP%, and internet-sourced paths.
- Enable advanced logging: Turn on PowerShell ScriptBlock/command-line logging; monitor Startup shortcuts and ProgramData/TEMP creations.
- Validate downloads: Enforce policies that only allow software from verified vendor domains; scrutinize web redirects from compromised sites.
- User awareness: Train users on web-based social engineering and drive-by risks; report unexpected redirects or update prompts.

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

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – JS#SMUGGLER

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Akira Ransomware Targets Hyper-V and ESXi to Encrypt VMs at Scale via Hypervisor Exploitation	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers report a surge in ransomware operations targeting hypervisors, with Akira increasingly focusing on Hyper-V and VMware ESXi. By abusing management interfaces and built-in tools, attackers can encrypt many virtual machines simultaneously.

This matters to financial services because compromise of the hypervisor layer bypasses traditional endpoint controls, amplifies blast radius across critical workloads, and accelerates time-to-impact for business-critical systems and services.

Technical Details

- Hypervisors present limited visibility for conventional security tools, letting attackers perform encryption at scale with fewer alerts and slower detection.
- Case data shows hypervisor ransomware involvement jumping from ~3% in H1 2025 to ~25% in H2 2025, with Akira driving the trend across virtualized environments.
- Adversaries pivot hypervisors using compromised internal credentials when segmentation fails, reaching management pages and gaining elevated control.
- Built-in utilities (e.g., openssl) are misused to encrypt VM volumes directly, removing the need to deploy custom ransomware binaries to endpoints.
- Operations include modifying VM settings, disabling defenses, and tampering with virtual switches to prepare hosts for mass encryption.
- Type 1 hypervisors are prime “land-and-expand” targets where EDR cannot be installed, creating a strategic blind spot similar to hardened VPN appliances.
- Attacks leverage management plane weaknesses and over-privileged domain accounts, enabling rapid lateral movement to ESXi and vCenter.
- Ransomware payloads can be deployed centrally from the host, impacting dozens or hundreds of VMs from a single interface.
- Lack of strict access controls and audited admin paths increases likelihood of silent persistence and large-scale impact.
- The trend reflects a shift from endpoint-centric ransomware to infrastructure-level compromise of virtualization controllers.

Recommendations

- Secure access & least privilege: Use dedicated local hypervisor accounts, enforce MFA, strong vault-stored passwords, and limit roles to minimum required.
- Segment the management plane: Isolate hypervisor management on dedicated VLANs; restrict access to approved, static-IP admin devices via a monitored jump box.
- Harden runtime: Enforce code-execution controls on hosts; keep hypervisors patched and minimize exposed services to reduce exploitation paths.
- Backup & recovery: Maintain immutable snapshots and tested rapid-restore procedures to recover VM workloads after host-level encryption.
- Monitor & assume breach: Enhance logging for management interfaces, detect anomalies, and continuously hunt for credential misuse and lateral movement.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
GrayBravo Uses ClickFix Technique to Deliver CastleLoader Malware Across Multiple Industries	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have analyzed GrayBravo (formerly TAG-150), a technically advanced threat actor operating a malware-as-a-service (MaaS) ecosystem. Recent campaigns leverage the ClickFix technique to distribute CastleLoader malware through phishing lures impersonating global logistics firms and Booking.com.

This campaign is significant for financial services and other sectors because CastleLoader enables delivery of additional malware families, including remote access trojans (RATs) and infostealers, increasing risks of credential theft, data exfiltration, and persistent access.

Technical Details

- GrayBravo operates a multi-tiered infrastructure supporting CastleLoader, CastleRAT, SecTopRAT, WarmCookie, and other malware families.
- Four distinct activity clusters were identified, each using unique TTPs and targeting profiles, reinforcing GrayBravo's MaaS model.
- TAG-160 cluster impersonates logistics firms, using phishing lures and ClickFix to distribute CastleLoader via spoofed emails and freight-matching platforms.
- TAG-161 cluster impersonates Booking.com, delivering CastleLoader and Matanbuchus alongside custom phishing email management tools.
- CastleLoader infrastructure includes domains sharing WHOIS SOA email addresses, indicating centralized registration by the threat actor.
- CastleRAT variants (C and Python) communicate via custom binary protocol secured with RC4 encryption and hard-coded keys; capabilities include remote shell, file execution, and in C variant, credential theft and screen capture.
- Infrastructure analysis revealed overlapping traffic patterns and shared RC4 keys (e.g., "NanuchkaUpyachka"), suggesting deliberate redundancy and interconnected C2 nodes.
- Threat actor uses compromised infrastructure for phishing email distribution, evidenced by malware logs containing stolen credentials for hosting accounts.
- Malvertising and fake software update mechanisms observed in additional clusters, expanding attack surface beyond email-based lures.
- Victim IP analysis indicates infections primarily in the U.S., with some targeting logistics and hospitality sectors; infections may occur on individual machines within organizational networks.

Recommendations

- Monitor and block validated infrastructure tied to CastleLoader, CastleRAT, and related malware families; integrate indicators into detection systems.

- Deploy updated detection rules (YARA, Snort, Sigma) for current and historical infections.
- Implement advanced email filtering to detect spoofed domains and phishing lures; enforce DMARC, SPF, and DKIM policies.
- Monitor for data exfiltration attempts and unusual connections to legitimate internet services (e.g., Pastebin) abused for staging.
- Educate users on phishing risks and verify authenticity of logistics or booking-related communications before interaction.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – GrayBravo

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
NANOREMOTE Backdoor Exploits Google Drive API for Covert Control on Windows Systems	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have discovered NANOREMOTE, a newly observed Windows backdoor linked to espionage operations and similar to FINALDRAFT and REF7707 implants. The malware uses Google Drive API for data exfiltration and payload staging, creating a stealthy channel that complicates detection.

This campaign is significant for financial services as it enables covert command execution, reconnaissance, and file transfers through trusted cloud services, bypassing traditional network monitoring and increasing risk of sensitive data exposure.

Technical Details

- NANOREMOTE is delivered via WMLOADER, a loader masquerading as Bitdefender software with an invalid digital signature.
- The implant is a 64-bit Windows executable written in C++ without obfuscation, featuring reconnaissance, command execution, and file transfer capabilities.
- Uses Google Drive API for queuing, pausing, resuming, and canceling file transfers, as well as generating refresh tokens for persistence.
- Network communication occurs over HTTP using POST requests with JSON data compressed via Zlib and encrypted with AES-CBC (16-byte key).
- Generates a unique GUID via CoCreateGuid, hashes it with Fowler-Noll-Vo (FNV), and uses it for victim identification during C2 requests.

- Includes 22 command handlers supporting host info collection, beacon timeout modification, file/directory operations, and cleanup routines.
- Custom PE loader executes files from disk using libPeConv, manually mapping sections into memory to bypass traditional Windows loader and evade detection.
- Supports execution of encoded PE files directly in memory, enabling fileless persistence and stealth.
- Observed similarities with FINALDRAFT, including GUID generation, FNV hashing, and heap-validation checks, indicating code reuse.
- Potential evasion techniques include hardware breakpoints, invalid code signatures, shellcode injections, and image hollowing from unusual stack contexts.

Recommendations

- Monitor for abnormal use of Google Drive API and outbound HTTP POST requests with encrypted payloads.
- Enable memory threat detection for shellcode injection and fileless execution patterns; enforce behavioral rules for PE loading anomalies.
- Block execution of binaries with invalid signatures and restrict use of unsigned modules.
- Deploy EDR with telemetry for command-line auditing, ScriptBlock logging, and detection of custom loaders leveraging libPeConv.
- Investigate alerts for connections to commonly abused web services and anomalies in GUID-based identification routines.

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
ConsentFix Attack Hijacks Microsoft Accounts via Azure CLI OAuth in Browser-Only Flow	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified “ConsentFix,” a browser-native attack that phishes OAuth tokens by coercing victims to copy-paste a localhost URL containing an authorization code into an attacker page. The technique abuses the implicitly trusted Microsoft Azure CLI OAuth app to create a tokenized connection without credentials or MFA.

This matters to financial services because it bypasses email controls, endpoint visibility, and phishing-resistant authentication. The attack leverages compromised, high-reputation sites and advanced anti-analysis to covertly link victim Microsoft accounts to an attacker’s Azure CLI instance.

Technical Details

- The victim reaches a compromised site via Google Search; a fake Cloudflare Turnstile gate collects email and enforces target-list checks.
- Conditional loading filters by approved domains and IP; if not matched, the page returns to normal, suppressing analysis and repeat triggers.
- The attacker generates an Azure CLI OAuth authorization code visible in a localhost URL; the victim pastes this full URL into the phishing page.
- Copy-paste of the URL (including code) creates an OAuth connection between the victim's Microsoft account and the attacker's Azure CLI.
- First-party app trust: Azure CLI is implicitly trusted in Entra ID, allowed to request permissions, resistant to default third-party restrictions.
- The app can hold special scopes (tenant-wide service, legacy/undocumented graph, internal client ops), increasing exploitation potential.
- Detection evasion includes synchronized IP blocking across sites, per-session checks, and withholding JavaScript packages unless all conditions matches.
- The attack runs entirely in the browser context—no endpoint touch—undermining traditional ClickFix detections and email defenses.
- No login or MFA prompt appears; passkeys and phishing-resistant methods provide no protection in this flow.
- Backend indicators: anomalous logins to "Microsoft Azure CLI" with resource differences (e.g., "Windows Azure Active Directory" vs. "Azure Resource Manager").

Recommendations

- Monitor sign-ins to Microsoft Azure CLI and flag logins outside admin/developer groups; investigate "Windows Azure Active Directory" resource logins.
- Enforce policy that forbids users from copy-pasting localhost OAuth URLs or following non-approved cloud auth steps in browsers.
- Strengthen web controls: filter search-driven watering-hole pages; scrutinize pages using Turnstile-style gates that request corporate emails.
- Enhance investigation playbooks for browser-only OAuth token abuse; instrument logs to differentiate legitimate Azure CLI from phishing-derived flows.
- Conduct targeted awareness: teach users that internal IT will never request copy-paste of authorization codes or localhost URLs into external pages.

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
Adversary-in-the-Middle Phishing Campaign Targets Microsoft 365 and Okta SSO Users	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an active phishing campaign hijacking Microsoft 365 and Okta single sign-on (SSO) flows. The campaign uses proxy-based phishing pages to capture credentials and session cookies, bypassing MFA methods that are not phishing-resistant.

This campaign is critical for financial services organizations using federated identity providers, as it enables attackers to impersonate legitimate sessions and gain direct access to sensitive applications, including Microsoft 365 environments.

Technical Details

- The phishing campaign impersonates legitimate Okta login pages using lookalike domains and proxy's requests to the real tenant, preserving branding and customization.
- URLs include parameters such as /?company=<target>.okta.com to dynamically target specific organizations.
- Injected JavaScript hooks the window.fetch method to rewrite URLs and steal Okta session cookies before and after authentication.
- Captured cookies allow attackers to impersonate authenticated sessions without requiring MFA revalidation.
- Related Microsoft 365 phishing pages proxy traffic to legitimate Microsoft endpoints, injecting scripts to auto-click prompts and steal credentials/session tokens.
- Lures focus on compensation and benefits themes; phishing links are often embedded in password-protected PDFs shared via email.
- Infrastructure is hosted on Cloudflare, using Turnstile checks to block automated analysis and lend legitimacy.
- Advanced evasion includes conditional loading based on email domain/IP and redirecting non-targeted users back to the original site.
- Okta logs may show anomalies in user.authentication.auth_via_mfa events or mismatched origin data; FastPass users may see risk indicators in debugContext.debugData.
- Attackers attempt to access Okta Dashboard or directly initiate SSO to Microsoft 365, triggering user.authentication.sso events with target_app:office365.

Recommendations

- Monitor Okta and Microsoft 365 logs for anomalous authentication events, including mismatched origins and unexpected MFA flows.

- Enforce phishing-resistant MFA methods (e.g., FIDO2/WebAuthn) for all SSO and cloud access.
- Implement strict email filtering and sandboxing for PDFs containing external links; block password-protected attachments from unknown senders.
- Deploy behavioral detection for proxy-based phishing indicators, including unusual Cloudflare-hosted domains and Turnstile checks.
- Educate users on benefits-themed phishing lures and reinforce verification of login URLs before entering credentials.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
JSCEAL Infostealer Adopts Hardened C2 and Anti-Analysis Tactics to Target Crypto Users	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Cato CTRL have observed a new JSCEAL campaign targeting users of cryptocurrency applications, featuring revamped command-and-control infrastructure, stricter access controls, and a refactored script engine for stealth. The operation replaces earlier hyphenated C2 domains with standardized single-word domains, consistent subdomains, and multi-stage payload delivery.

This matters to financial services and virtual asset platforms because JSCEAL's quiet evolution enables resilient data theft via PowerShell communications that blend with normal traffic, reducing detection and increasing risk to crypto-adjacent workflows.

Technical Details

- Old campaign (1H 2025) used hyphenated .com domains and malvertising that redirected to MSI installers; branding and domain patterns were predictable.
- New campaign shifts to single-word C2 domains (e.g., emberstolight[.]com) spanning.org/.link/.net, registered in bulk on fixed intervals for scalability.
- Each C2 domain exposes standardized .faro and .api subdomains, indicating templated deployment and predictable structure.
- Strict access control returns HTTP 404 to non-PowerShell User-Agents, blocking browsers and many sandboxes to hinder analysis.
- Multi-stage retrieval requires a PDF check before fetching "/script," adding validation layers and complicating automated inspection.

- Refactored PowerShell scripts implement new logic for stealth; loaders are updated to fit the redesigned infrastructure.
- build.zip stage modified—filenames and file types changed—signaling broader refactoring of later components.
- Frequent beaconing to a hardcoded domain and PowerShell C2 traffic help JSCEAL evade traditional AV/EDR heuristics.
- The campaign remains active and targets cryptocurrency application users with increased resilience.
- Focus is on quiet hardening rather than exploiting headline vulnerabilities, emphasizing operational stealth.

Recommendations

- Monitor PowerShell traffic for non-browser User-Agents and staged requests (PDF → "/script") to detect JSCEAL patterns.
- Block newly registered single-word domains and watch for standardized .faro/.api subdomains across varied TLDs.
- Inspect endpoint telemetry for frequent beaconing to hardcoded C2 and unusual PowerShell network behaviors.
- Harden ad-based entry points: restrict MSI installs from web lures and validate software sources before execution.
- Enhance sandboxing to emulate PowerShell User-Agents and multi-stage checks, improving visibility into the loader chain.

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
Operation MoneyMount-ISO Delivers Phantom Stealer via ISO-Mounted Executables	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Seqrite Labs have uncovered a phishing campaign originating from Russia that uses fake payment confirmation emails to deliver Phantom Stealer through ISO-mounted executables. The attack chain begins with a ZIP archive containing a malicious ISO file, which mounts as a virtual drive and executes a disguised payment confirmation executable.

This campaign poses significant risk to finance and accounting roles, enabling credential theft, payment fraud, and lateral movement into IT systems. The use of ISO-based delivery reflects a growing trend to bypass email security and endpoint defenses.

Technical Details

- Initial lure: Russian-language phishing email impersonating financial/trading firms, claiming to confirm a bank transfer.
- Attachment: ZIP archive (~1 MB) containing a malicious ISO file; opening the ISO auto-mounts a virtual CD drive.
- Payload: Executable disguised as payment confirmation launches Phantom Stealer upon execution.
- Anti-analysis: Malware includes AntiAnalysis class to detect virtualized or sandboxed environments; triggers SelfDestruct.Melt() if checks fail.
- Data theft modules:
    - BrowserWallets: Extracts data from crypto wallet extensions in Chromium-based browsers.
    - ClipLogger: Monitors clipboard for sensitive data.
    - Keylogger: Captures global keystrokes.
    - Browser credential theft: Passwords, cookies, credit card details from Chromium browsers.
- Exfiltration channels:
    - Telegram module: Uses encrypted bot token to send data via Telegram Bot API.
    - Discord module: Uploads stolen data to attacker-controlled Discord webhook.
    - FTP module: Implements asynchronous file uploads via UploadAllAsync and SendMessageAsync.
- Objective: Credential theft and financial fraud targeting finance, treasury, and payment workflows.
- Campaign reflects strategic shift toward ISO-based delivery for stealth and evasion of perimeter controls.

Recommendations

- Block ISO and containerized attachments in finance-facing email workflows; enforce attachment filtering policies.
- Deploy EDR with memory-behavior monitoring to detect staged payload execution and anti-analysis routines.
- Monitor for suspicious clipboard access, keylogging behaviors, and unauthorized browser data extraction.
- Inspect outbound traffic for Telegram, Discord, and FTP connections originating from endpoints.
- Conduct phishing awareness training for finance and accounting teams; verify payment confirmation requests through out-of-band channels.

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

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Operation MoneyMount

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft Zero-Day Vulnerabilities Enable Privilege Escalation and Remote Code Execution	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Microsoft has disclosed three zero-day vulnerabilities, including one actively exploited flaw in Windows Cloud Files Mini Filter Driver and two publicly disclosed issues affecting GitHub Copilot for JetBrains and PowerShell. These vulnerabilities allow privilege escalation and remote code execution, posing severe risks to enterprise environments.

For financial services, exploitation could lead to full system compromise, credential theft, and lateral movement across networks, creating opportunities for ransomware or advanced persistent threats.

Technical Details

- CVE-2025-62221 — Actively Exploited
  - Component: Windows Cloud Files Mini Filter Driver
  - Type: Elevation of Privilege (Use-After-Free)
  - Impact: Authenticated attackers can escalate privileges to SYSTEM, gaining full control of the system.
- CVE-2025-64671 — Publicly Disclosed
  - Component: GitHub Copilot for JetBrains IDEs
  - Type: Remote Code Execution (Command Injection)
  - Cause: Improper neutralization of special command elements in terminal commands.
  - Impact: Attackers can append malicious commands to auto-approved terminal actions.
- CVE-2025-54100 — Publicly Disclosed
  - Component: Windows PowerShell
  - Type: Remote Code Execution
  - Cause: Command injection via Invoke-WebRequest when retrieving scripts from webpages.
  - Impact: Arbitrary command execution locally through crafted web content.
- Other notable RCE vulnerabilities:

  - CVE-2025-62554 — Microsoft Office RCE
  - CVE-2025-62557 — Microsoft Office RCE
  - CVE-2025-62562 — Microsoft Outlook RCE
- Potential impact:
  - Full system compromise via RCE
  - SYSTEM-level privilege escalation
  - Unauthorized code execution from malicious files or injected commands
  - Lateral movement enabling ransomware or APT operations.

Recommendations

- Apply Microsoft's latest security updates immediately across all endpoints and servers.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Actively Exploited Zero-Day in Google Chrome Requires Immediate Patch	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Google has released an urgent update for Chrome Desktop addressing three vulnerabilities, including a high-severity zero-day (issue 466192044) actively exploited in the wild. Technical details remain undisclosed, but exploitation has been confirmed. Two additional medium-severity flaws affect the Password Manager and Toolbar components.

For financial services organizations, this zero-day poses a critical risk as it could enable attackers to compromise endpoints, steal credentials, and establish persistence through browser exploitation. Immediate patching is essential to mitigate exposure.

Technical Details

- High-Severity Zero-Day (Issue 466192044)
  - Status: Actively exploited in the wild; CVE pending.
  - Severity: High.
  - Description: Google has not disclosed specifics but confirmed real-world exploitation.
- Other Vulnerabilities:
  - CVE-2025-14372: Medium — Use-after-free in Password Manager.
  - CVE-2025-14373: Medium — Inappropriate implementation in Toolbar.
- Fixed Versions:

- Chrome Stable Channel Update for Desktop:
- 143.0.7499.109/.110 for Windows/Mac
- 143.0.7499.109 for Linux

Recommendations

- Deploy Chrome update 143.0.7499.109/.110 immediately across all endpoints.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Apple Patches Actively Exploited WebKit Zero-Days Across iOS, macOS, and Safari	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Apple has released urgent security updates for iOS, iPadOS, macOS, tvOS, watchOS, visionOS, and Safari to address multiple vulnerabilities, including two WebKit flaws confirmed to be actively exploited in targeted attacks. These vulnerabilities enable arbitrary code execution via malicious web content and affect a wide range of Apple devices.

For financial services, exploitation of these flaws could allow attackers to compromise endpoints through browser-based attacks, bypassing traditional defenses and enabling credential theft or system takeover.

Technical Details

- CVE-2025-43529 — Critical (CVSS 9.8)
    - Component: WebKit rendering engine
    - Type: Use-after-free vulnerability
    - Impact: Arbitrary code execution when processing crafted web content.
- CVE-2025-14174 — High (CVSS 8.8)
    - Component: WebKit (ANGLE graphics library, Metal renderer)
    - Type: Memory corruption vulnerability
    - Impact: Out-of-bounds memory access leading to code execution.
    - Note: Mirrors a flaw patched in Google Chrome, indicating cross-platform exploitation.
- Exploitation confirmed on iOS versions earlier than iOS 26; attacks described as highly targeted and sophisticated.
- Impact:
    - Full system compromises via malicious web content.
    - Increased attack surface across multiple Apple platforms and apps.

- Potential for stealthy exploitation in targeted campaigns.

Software Updates Details

Latest Versions	Available for
iOS 26.2 and iPadOS 26.2	iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later
iOS 18.7.3 and iPadOS 18.7.3	iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later
macOS Tahoe 26.2 macOS Sequoia 15.7.3	macOS Tahoe macOS Sequoia
macOS Sonoma 14.8.3	macOS Sonoma
tvOS 26.2	Apple TV HD and Apple TV 4K (all models)
watchOS 26.2	Apple Watch Series 6 and later
visionOS 26.2	Apple Vision Pro (all models)
Safari 26.2	macOS Sonoma and macOS Sequoia

Recommendations

- Apply Apple's latest security updates immediately across all supported devices and operating systems.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple High-Severity Flaws in Firefox and Thunderbird	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Mozilla has released security updates addressing multiple vulnerabilities across Firefox, Firefox ESR, and Thunderbird. Several high-severity flaws were identified that could lead to memory corruption, sandbox escape, elevated privileges, or arbitrary code execution, potentially resulting in full browser compromise.

Technical Details

- High-Severity Vulnerabilities
  - CVE-2025-14321 – WebRTC: Signaling A use-after-free vulnerability in the WebRTC Signaling component could lead to memory corruption and possible code execution.
  - CVE-2025-14322 – Graphics: CanvasWebGL A flaw caused by incorrect boundary conditions in the CanvasWebGL component could allow a sandbox escape.
  - CVE-2025-14323 – DOM: Notifications A privilege escalation issue in the DOM Notifications component may allow elevated browser permissions.

- CVE-2025-14324, CVE-2025-14325 – JavaScript Engine: JIT A miscompilation issue in the JavaScript JIT engine may lead to unpredictable script execution or exploitation.

- Impact: Exploitation of these vulnerabilities can lead to significant security risks, including memory corruption, sandbox escape, elevated privileges within the browser, arbitrary code execution, and ultimately full compromise of the browser environment.
- Fixed Versions:
  - Firefox 146
  - Firefox ESR 115.31
  - Firefox ESR 140.6
  - Thunderbird 146
  - Thunderbird 140.6.

Recommendations

- Apply Mozilla's latest security updates.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
SAP December 2025 Security Updates Address Critical Code Injection and Deserialization Flaws	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

SAP has released its December 2025 security updates, fixing multiple vulnerabilities across core products including SAP Solution Manager, SAP Commerce Cloud, SAP jConnect, SAP NetWeaver, SAP BusinessObjects, SAP S/4HANA, SAPUI5, and SAP Enterprise Search. These flaws range from critical to medium severity and could enable code execution, authentication bypass, denial of service, and sensitive data exposure.

For financial services organizations leveraging SAP for ERP, finance, and procurement workflows, exploitation could result in system compromise, unauthorized transactions, and operational disruption.

Technical Details

- Critical Severity:
  - CVE-2025-42880 — Code Injection in SAP Solution Manager (CVSS 9.9)
  - CVE-2025-55754 / CVE-2025-55752 — Apache Tomcat vulnerabilities in SAP Commerce Cloud (CVSS 9.6)
  - CVE-2025-42928 — Deserialization vulnerability in SAP jConnect SDK for ASE (CVSS 9.1)

- High Severity:
  - CVE-2025-42878 — Sensitive data exposure in SAP Web Dispatcher & ICM (CVSS 8.2)
  - CVE-2025-42874 — DoS in SAP NetWeaver (Xcelsius) (CVSS 7.9)
  - CVE-2025-48976 — DoS in SAP BusinessObjects (CVSS 7.5)
  - CVE-2025-42877 — Memory corruption in Web Dispatcher, ICM & Content Server (CVSS 7.5)
  - CVE-2025-42876 — Missing authorization check in S/4HANA Financials GL (CVSS 7.1)
- Medium Severity:
  - CVE-2025-42875 — Missing authentication in NetWeaver ICF (CVSS 6.6)
  - CVE-2025-42904 — Information disclosure in Application Server ABAP (CVSS 6.5)
  - CVE-2025-42872 — XSS in SAP NetWeaver Enterprise Portal (CVSS 6.1)
  - CVE-2025-42873 — DoS in SAPUI5 framework (Markdown-it) (CVSS 5.9)
  - CVE-2025-42891 — Missing authorization check in SAP Enterprise Search (CVSS 5.5)
  - CVE-2025-42896 — SSRF in SAP BusinessObjects BI Platform (CVSS 5.4)

Recommendations

- Apply SAP's December 2025 security patches immediately across all affected products.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Ivanti Endpoint Manager Update Fixes Critical XSS and High-Severity File Manipulation Flaws	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Ivanti has released a security update for Ivanti Endpoint Manager (EPM) addressing four vulnerabilities—one critical and three high-severity—impacting EPM core and remote consoles. These flaws include stored XSS, arbitrary file write, path traversal, and improper cryptographic validation, which could enable remote code execution, unauthorized file manipulation, and administrative compromise.

While no exploitation has been observed in the wild, financial services organizations should prioritize patching to prevent potential compromise of endpoint management infrastructure.

Technical Details

- CVE-2025-10573 — Stored Cross-Site Scripting (XSS)
  - Severity: Critical (CVSS 9.6)
  - CWE: 79 — Improper Neutralization of Input During Web Page Generation

  - Impact: Remote unauthenticated attackers can inject malicious JavaScript that executes in an administrator session; requires user interaction.

- CVE-2025-13659 — Arbitrary File Write Leading to Potential RCE
  - Severity: High (CVSS 8.8)
  - Impact: Improper validation of dynamic resources allows remote unauthenticated attackers to write arbitrary files to the server; user interaction required.
- CVE-2025-13661 — Authenticated Path Traversal File Write
  - Severity: High (CVSS 7.1)
  - Impact: Directory traversal flaw enables remote authenticated attackers to write files outside permitted directories; user interaction required.
- CVE-2025-13662 — Improper Cryptographic Signature Verification
  - Severity: High (CVSS 7.8)
  - Impact: Patch management component fails to validate cryptographic signatures, allowing arbitrary code execution if a malicious file is imported.
- Affected Versions:
  - Ivanti Endpoint Manager: 2024 SU4 and earlier
- Fixed Version:
  - Ivanti Endpoint Manager: 2024 SU4 SR1

Recommendations

- Apply Security Update: Upgrade all EPM core and remote consoles to EPM 2024 SU4 SR1; ensure no outdated consoles remain connected.
- Validate Server Exposure: Restrict EPM access to internal networks; ensure EPM is not exposed to the public internet.
- Restrict Connections: Ensure endpoints only connect to trusted EPM core servers; validate certificates and configurations.
- Tighten Import Controls: Import only trusted configuration or patch files; implement file validation and signature checks.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Fortinet December 2025 Security Updates Address Critical FortiCloud SSO Authentication Bypass	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Fortinet has released December 2025 security updates fixing two critical vulnerabilities and multiple high-severity flaws across FortiOS, FortiProxy, FortiWeb, FortiSwitchManager, FortiVoice, and FortiSandbox. The most severe issues involve improper access control and cryptographic signature verification, allowing unauthenticated attackers to bypass FortiCloud SSO login and potentially gain full administrative access.

For financial services organizations, exploitation could lead to complete compromise of network security infrastructure, enabling lateral movement and privilege escalation. Immediate patching and disabling FortiCloud SSO until updates are applied is strongly recommended.

Technical Details

- Critical Vulnerabilities:
    - CVE-2025-59718 / CVE-2025-59719 — Improper Access Control
        - Severity: Critical (CVSS 9.1)
        - Impact: Authentication bypass via crafted SAML message when FortiCloud SSO login is enabled.
        - Affected Products: FortiOS, FortiWeb, FortiProxy, FortiSwitchManager.
        - Note: FortiCloud SSO is disabled by default but enabled during FortiCare registration unless manually turned off.
- High-Severity Vulnerabilities:
    - CVE-2025-60024 — Path Traversal in FortiVoice (CVSS 7.7)
        - Impact: Arbitrary files write and privilege escalation.
    - CVE-2025-53949 — OS Command Injection in FortiSandbox (CVSS 7.0)
        - Impact: Unauthorized command execution.
    - CVE-2025-64447 — Authentication Cookie Forgery in FortiWeb (CVSS 7.1)
        - Impact: Privilege escalation via forged cookies.
- Affected Versions & Fixes:
    - FortiOS: 7.6.0–7.6.3 → Upgrade to 7.6.4+; 7.4.0–7.4.8 → Upgrade to 7.4.9+; 7.2.0–7.2.11 → Upgrade to 7.2.12+
    - FortiProxy: 7.6.0–7.6.3 → Upgrade to 7.6.4+; 7.4.0–7.4.10 → Upgrade to 7.4.11+
    - FortiWeb: 8.0.0 → Upgrade to 8.0.1+; 7.6.0–7.6.4 → Upgrade to 7.6.5+

- FortiVoice: 7.2.0–7.2.2 → Upgrade to 7.2.3+
- FortiSandbox: 5.0.0–5.0.2 → Upgrade to 5.0.3+

Recommendations

- Apply all Fortinet security updates immediately, prioritizing systems exposed to administrative access or external networks.
- Disable FortiCloud SSO login on FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager until patched.
- Restrict management interfaces to internal networks; enforce strong access controls and MFA.
- Validate server certificates and configurations; block untrusted connections to EPM core servers.
- Monitor for suspicious activity such as unauthorized file writes, cookie manipulation, and command injection attempts.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Supply-Chain Exposure in Notepad++ Updater Enables Malware Delivery via Manipulated Network Traffic	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Researchers have identified a supply-chain style attack targeting Notepad++ users through its update mechanism. Adversaries exploited redirectable network traffic and weak signature validation in older versions to replace legitimate installers with malware. Version 8.8.9 introduces strict mitigations, including enforced signature checks and trusted source validation, but requires manual installation.

This vulnerability is critical for financial services organizations relying on Notepad++ for secure workflows, as exploitation could lead to endpoint compromise and credential theft.

Technical Details

- Issue Type: Insecure update delivery via WinGUp updater.
- Root Cause: Manipulable XML-sourced download path enabling traffic redirection.
- Abused Files: %TEMP%\update.exe, %TEMP%\AutoUpdater.exe.
- Detection Indicators: gup.exe connecting to unknown URLs; unexpected processes spawned by updater.
- Severity: High
- Root Cause Factors:

1. Redirectable Network Traffic: Attackers intercepted and redirected updater traffic to malicious infrastructure.
2. Self-Signed Certificate (≤ v8.8.7):
   - Certificate included in GitHub source allowed attackers to craft binaries appearing superficially legitimate.
   - Victims ignored "Unknown Publisher" warnings.
3. Insufficient Signature Validation: Older versions did not enforce strict checks on downloaded installers.

- Impacted Versions:
  - Vulnerable: Up to v8.8.7 and v8.8.8 (incomplete hardening).
  - Patched: v8.8.9 with:
    - Mandatory trusted sources (GitHub only).
    - Signature and certificate validation (GlobalSign).
    - Automatic abortion on validation failure.

Recommendations

- Manually Update to v8.8.9 Immediately: Download only from official Notepad++ site or GitHub link referenced there.
- Verify Update Integrity: Ensure installer is signed by Notepad++ (GlobalSign certificate); do not proceed if "Unknown Publisher" appears.
- Perform IOC-Based Threat Hunting:
  - Check network logs for suspicious outbound connections from gup.exe.
  - Inspect %TEMP% for update.exe or AutoUpdater.exe; treat systems as compromised if found.
- Conduct Endpoint Malware Scanning: Run full scans using reputable EDR/AV solutions.

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Storm-0249 MITRE TTPs

ID	TACTICS AND TECHNIQUES
T1566.001	Phishing: Spear Phishing Attachment
T1218	Exploit Public-Facing Application
T1059.001	Signed Binary Proxy Execution (LOLBins)
T1203	Exploitation for Client Execution
T1082	System Information Discovery
T1027	Obfuscated Files or Information
T1568.002	Dynamic Resolution: Domain Generation Algorithms
T1574.002	Hijack Execution Flow: DLL Side-Loading

Jssmuggler MITRE TTPs

TACTICS	TECHNIQUES
Initial Access	T1189 – Drive-by Compromise
Execution	T1059 – JavaScript Execution
	T1059.001 – PowerShell
	T1218 – Signed Binary Proxy Execution (mshta.exe Abuse)
Persistence	T1053 – Scheduled Task / Startup Folder Persistence
Defense Evasion	T1027 – Obfuscated / Encrypted Payloads
Execution	T1027: Obfuscated Files or Information
	T1140: Deobfuscate/Decode Files or Information
	T1620: Reflective Code Loading
	T1036.005: Match Legitimate Name or Location
	T1562.001: Disable or Modify Tools (Windows Defender)

	T1497.003: Time Based Evasion (Ping Delay)
Credential Access	T1056.001: Input Capture: Keylogging
Command and Control	T1105 – Ingress Tool Transfer
	T1219 – Remote Access Tools (NetSupport RAT)

Graybravos MITRE TTPs

TACTICS	TECHNIQUES
Initial Access: Phishing	T1566
Initial Access: Drive-by Compromise	T1189
Execution: User Execution: Malicious File	T1204.002
Execution: User Execution: Malicious Copy and Paste	T1204.004
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: Command and Scripting Interpreter: AutoHotKey & AutoIT	T1059.010
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Resource Development: Acquire Access	T1650
Resource Development: Obtain Capabilities: Tool	T1588.002
Resource Development: Compromise Accounts: Email Accounts	T1586.002
Defense Evasion: Masquerading	T1036
Command-and-Control: Proxy: External Proxy	T1090.002
Command-and-Control: Application Layer Protocol: Web Protocols	T1071.001
Command-and-Control: Ingress Tool Transfer	T1105
Collection: Data from Local System	T1005

Operation Moneymount MITRE TTPs

TACTICS	TECHNIQUES	TECHNIQUE ID
Initial Access	Phishing: Attachment	T1566.001
	User Execution: Malicious File	T1204.002
	Drive-by Social Engineering	T1654
Execution	Native API Execution / Binary Execution	T1106
	Execution of ISO-Mounted File	T1204.002
Defense Evasion	Encrypted/Obfuscated Payload	T1027
	Steganography / Payload in Image	T1027.003
	Virtualization/Sandbox Evasion	T1497
	Masquerading	T1036
	Self-Deletion	T1070.004
Payload Loading	DLL Injection	T1055.001
	Reflective Loading / In-Memory Execution	T1620
Credential Access	Credential Access from Web Browsers	T1555.003
Discovery	System Information Discovery	T1082
	Process Discovery	T1057
	Security Software Discovery	T1518.001
Collection	Keylogging	T1056.001
	Clipboard Collection	T1115
	File Collection	T1039
	Browser Data Collection	T1119
	Application Token Theft (Discord)	T1528
	Cryptocurrency Wallet Theft	T1555
Exfiltration	Exfiltration Over Web Services (Telegram)	T1567.002
	Exfiltration to Cloud/Webhook (Discord)	T1530
	Exfiltration Over Unencrypted/FTP Channels	T1048
	Data Staged in Archive (ZIP)	T1560.001

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
AES-CBC	Advanced Encryption Standard (Cipher Block Chaining) symmetric encryption used for data protection.
ANGLE (Metal Renderer)	Graphics library component linked to a memory corruption issue mirrored across platforms.
Apple iOS/iPadOS/macOS Updates	Security releases addressing actively exploited WebKit zero-days across platforms.
APT	Advanced Persistent Threat: a long-term targeted operation aiming for data theft or disruption.
Ashen Lepus	Middle East espionage actor (aka WIRTE) deploying AshTag suite with improved OpSec.
AshTag	Modular .NET malware enabling data exfiltration
Azure CLI	Microsoft command-line app implicitly trusted in Entra ID; abused in ConsentFix phishing.
C2	Command and Control: attacker infrastructure to manage compromised systems and issue commands.
CastleLoader	Loader malware used by GrayBravo to deploy RATs/infostealers.

CastleRAT	Remote Access Trojan for command execution
Chaos	Ransomware group claiming ThinkMarkets breach; promotes multi-OS ransomware and affiliate model.
Chrome Stable 143.0.7499.109/.110	Fixed versions addressing a high-severity zero-day and medium CVEs.
ClickFix	Social engineering method that tricks users into running malicious commands
ConsentFix	Browser-native flow that phishes OAuth tokens
CSC	UAE Cyber Security Council
CVE	Common Vulnerabilities and Exposures: standardized identifier for publicly known vulnerabilities.
CVSS	Common Vulnerability Scoring System measuring severity (e.g.
Deserialization Vulnerability	Executing code by loading untrusted serialized data into application objects.
DLL Sideloading	Loading a malicious DLL via a trusted executable to evade detection.
EDR	Endpoint Detection and Response: tooling detects and responds to endpoint threats.
EtherRAT	Implant using Ethereum smart contracts for C2
Fileless Execution	Malware that runs in memory (no disk artifacts)
FNV Hash	Fowler-Noll-Vo non-cryptographic hash function used for fast hashing (e.g.
FortiCloud SSO	Fortinet single sign-on for administrative access; affected by authentication bypass.
FortiCloud SSO Toggle	Device registration option that may enable SSO unless explicitly disabled.
Fortinet December 2025 Updates	Fixes for FortiCloud SSO bypass and multiple high-severity issues across product lines.
GlobalSign Certificate	Trusted code-signing certificate used to verify installer authenticity (e.g.
GUID	Globally Unique Identifier used to uniquely identify systems/objects.
HTA	HTML Application file type used to execute scripts; abused via mshta.exe.
Invoke-WebRequest (PowerShell)	Command that can trigger script execution from web content (linked RCE issue).
IoC	Indicator of Compromise: artifacts pointing to potential malicious activity or breach.
ISO-Mounted Executable	Executable delivered within an ISO image that auto-mounts as a virtual drive when opened.
Ivanti EPM	Ivanti Endpoint Manager platform for centralized endpoint administration and security.
Ivanti EPM 2024 SU4 SR1	Fixed release resolving critical XSS and high-severity file manipulation/signature flaws.
JSCEAL	Infostealer targeting crypto users with hardened C2 and staged PowerShell delivery.
Lightshot DLL Hijacking	Technique bundling legitimate Lightshot.exe with a malicious DLL to execute payloads.
Malvertising	Malicious ads that deliver malware via legitimate ad networks.
MFA	Multi-Factor Authentication: additional verification steps beyond a password.
mshta.exe	Windows binary used to run HTA files; often leveraged for covert execution.
NANOREMOTE	Windows backdoor uses Google Drive API for covert data transfer and tasking.
NetSupport RAT	Repurposed remote-admin tool enabling full remote control
Notepad++ v8.8.9	Patched release enforcing trusted sources and strict signature validation for updates.
OAuth	Open Authorization protocol enabling delegated access without sharing passwords.
Okta FastPass	Okta authentication method: logs include risk fields to flag anomalies.
Pastebin (LIS)	Legitimate internet service sometimes used by attackers to stage data or payloads.
Path Traversal	Technique to access files outside intended directories by manipulating file paths.
Phantom Stealer	Information-stealing malware targeting credentials
PowerShell Reflection	Loading .NET assemblies directly into memory for fileless execution.
ProgramData / Startup Shortcuts	Locations used for persistence (e.g.

RC4	Rivest Cipher 4 stream cipher used to encrypt communications in some malware.
React2Shell	Exploitation chain against React Server Components enabling unauthenticated code execution.
SAP December 2025 Updates	Patch set addressing critical code injection/deserialization and multiple high-severity issues.
SAP NetWeaver	Core SAP application server platform supporting business processes and integrations.
SentinelAgentWorker.exe	Trusted EDR process abused for DLL sideloading in Storm-0249 operations.
SSO	Single Sign-On: one login provides access to multiple applications.
SSRF	Server-Side Request Forgery: forcing a server to make unauthorized outbound requests.
Storm-0249	Initial Access Broker shifting from mass phishing to precise EDR exploitation (DLL sideloading/LOLBins).
Turnstile (Cloudflare)	Site gate used to filter targets and block analysis in phishing campaigns.
Use-After-Free	Memory flaw where free memory is re-used
VSCode Extensions (Bitcoin Black / Codo AI)	Malicious extensions deploying infostealers via Lightshot DLL hijacking.
WebKit	Apple browser engine: flaws enable code execution via malicious web content.
Windows Cloud Files Mini Filter Driver	Windows component affected by privilege-escalation zero-day (CVE-2025-62221).
WinGUp	Windows Generic Updater used by Notepad++ for retrieving and executing updates.
XSS	Cross-Site Scripting: injection of malicious scripts into web pages.