TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	24/4/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 24 April 2026

10	6	1	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Finance Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a concentrated surge in leveraging social engineering, trusted-tool abuse, and exploitation of critical vulnerabilities across widely used enterprise platforms. Activity includes Microsoft Teams based human-operated intrusions, abuse of signed software update mechanisms and major vulnerabilities affecting Microsoft, Cisco, Fortinet, Adobe, and Google Chrome. Attackers increasingly misuse legitimate workflows remote support, code-signed software, OAuth, and SSO to bypass controls with minimal malware. From a financial sector perspective, this activity increases risk across identity, access, collaboration, and endpoint security, raising exposure to credential compromise, data theft, and reputational pressure. Requiring expedited patch, tighter access controls, reduced implicit trust, and strengthened stakeholder safeguards.

ADGM THREAT INTELLIGENCE SUMMARY

Name	Threat Severity Rating	TLP	Attribution	Originating Source
MuddyWater-Aligned Reconnaissance and Intrusion Campaign Targeting the Middle East	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a coordinated, multi-stage cyber campaign with tradecraft aligned to MuddyWater, the campaign used a mix of vulnerability exploitations including RCE flaws like CVE-2025-54068 (Laravel Livewire), CVE-2025-52691 (SmarterMail), CVE-2025-68613 (n8n), and CVE-2025-34291 (Langflow) with OWA brute-force attacks, and newly identified command-and-control infrastructure. What began as reconnaissance escalated into successful intrusions, resulting in confirmed exfiltration of sensitive data.

This campaign may impact organizations in the financial sector that operate internet-facing services within the Middle East or rely on shared regional infrastructure. The observed focus on credential harvesting, enterprise email access, and structured data exfiltration could affect financial institutions with exposed systems or weak authentication controls.

Technical Details

- The campaign followed a structured lifecycle that began with large-scale reconnaissance of more than 12,000 internet-facing systems and later shifted to targeted intrusion activity. This sequencing shows deliberate targeting rather than random or opportunistic exploitation.
- The threat actor rapidly weaponized several newly disclosed vulnerabilities to scan exposed web applications, email servers, and automation platforms. Reconnaissance activity was organized by vulnerability type, indicating automated and continuous scanning operations.
- After identifying vulnerable systems, the activity moved away from broad scanning toward selective exploitation of higher-value environments. This transition suggests prioritization based on the results of the reconnaissance phase.
- Credential harvesting became a primary intrusion method during later stages of the campaign. Attackers conducted brute-force attempts against Outlook Web Access using custom scripts and multi-threaded tooling.
- Targeted username enumeration was observed against specific organizations within the Middle East. This approach increased the likelihood of successful credential compromise during brute-force operations.
- Once access was obtained, the attackers relied on a modular command-and-control infrastructure. The setup supported communication over TCP, HTTP, and UDP, allowing flexible management of compromised systems.
- Command-and-control communications were encrypted and used custom headers and session identifiers. These mechanisms helped manage infected hosts while reducing the chance of detection.

- The campaign progressed into data collection and staging within compromised environments. Confirmed exfiltrated data included structured records such as identity documents, payroll information, and financial-related files.

Recommendations

- Review and patch all internet-facing systems, prioritizing recently disclosed high-risk vulnerabilities.
- Strengthen authentication controls on email and remote access services, including enforcing multi-factor authentication.
- Monitor authentication logs for brute-force patterns and abnormal login behavior targeting enterprise email systems.
- Inspect outbound network traffic for unusual or multi-protocol communication patterns that may indicate command-and-control activity.
- Conduct proactive threat hunting focused on reconnaissance artifacts, credential abuse, and unauthorized data staging.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – MuddyWater-Aligned Reconnaissance and Intrusion Campaign Targeting the Middle East

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
Seedworm Campaign Abusing Microsoft Teams to Deploy Dindoor Backdoor	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a targeted intrusion campaign attributed to Seedworm that abused Microsoft Teams as an initial access vector by reaching out to the victim as an external user via Microsoft team to deliver a custom backdoor known as Dindoor. The activity relied on social engineering, impersonation of IT support staff, and a malicious installer masquerading as a legitimate Windows update.

This campaign may impact organizations in the financial sector that rely on collaboration platforms such as Microsoft Teams for daily operations. Financial institutions should be aware that social engineering delivered through trusted enterprise tools could affect users with limited visibility into external tenant interactions.

Technical Details

- The intrusion began with social engineering conducted through Microsoft Teams, where the attacker contacted the victim as an external user impersonating IT support. A deceptive Microsoft 365 tenant domain was used to closely resemble a legitimate helpdesk environment.
- During the interaction, the victim was persuaded to execute a malicious MSI installer disguised as a Windows update package. This installer functioned as the initial dropper for the Dindoor backdoor.
- The MSI installer was digitally signed with a revoked certificate, increasing its perceived legitimacy during execution. Once run, it deployed multiple components into a hidden directory on the infected system.
- Dropped artifacts included a legitimate runtime binary, scripting files, and supporting modules required for backdoor execution. These components were observed executing shortly after the installer was launched.
- The attackers abused a legitimate JavaScript and TypeScript runtime to execute an obfuscated payload directly in memory. This approach minimized on-disk artifacts and reduced the likelihood of detection.
- After decoding, the in-memory payload established command-and-control communications with remote infrastructure. Initial communications included the exfiltration of basic host information such as username, hostname, and operating system details.
- Additional payloads were retrieved through a dropped PowerShell script that contacted attacker-controlled servers. Network traffic showed distinct request patterns tied to the abused runtime environment.
- Persistence was achieved by creating a deceptive registry Run key designed to blend in with legitimate system services. This ensured the malware executed automatically after system restarts.

Recommendations

- Restrict or monitor external communications in collaboration platforms, particularly unsolicited messages requesting action from end users.
- Enhance user awareness around social engineering delivered through non-email enterprise tools such as chat and collaboration platforms.
- Monitor endpoint activity for suspicious installer executions and the abuse of legitimate runtimes for in-memory payload execution.
- Review registry autorun locations for newly created entries that mimic legitimate system services.
- Correlate endpoint and network telemetry to identify unusual outbound connections initiated by scripting or runtime binaries.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Seedworm Campaign Abusing Microsoft Teams to Deploy Dindoor Backdoor

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
Mirai-Like Botnet Exploiting CVE-2023-33538 in TP-Link Routers	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an active campaign involving automated scanning and exploitation attempts against end-of-life TP-Link Wi-Fi routers by a Mirai-like botnet. The activity abuses CVE-2023-33538, a command injection vulnerability in the router's web management interface, to download and execute malicious binaries.

This campaign may impact organizations in the financial sector that continue to operate legacy or unmanaged networking devices. Financial institutions should be aware that compromised edge devices could be leveraged as part of broader botnet infrastructure, potentially affecting availability or enabling follow-on attacks.

Technical Details

- The campaign targets CVE-2023-33538, a command injection vulnerability affecting multiple end-of-life TP-Link router models. The flaw exists due to unsanitized input passed through the ssid1 parameter in HTTP GET requests.
- Attackers conducted large-scale automated scans and sent crafted requests to the router's wireless configuration endpoint. These requests attempted to inject shell commands into the vulnerable parameter.
- Observed exploit attempts aimed to download an ELF binary named arm7 to the router and execute it. The command sequence followed patterns commonly used by Mirai-based botnets.
- The downloaded arm7 binary was identified as a Mirai-like variant with similarities to the Condi IoT botnet family. The malware connects to a command-and-control server to receive further instructions.
- Once executed, infected devices become part of a botnet and can act as HTTP servers. These compromised routers are used to deliver malware to other vulnerable devices.
- The malware includes update logic that retrieves additional binaries for multiple CPU architectures. This allows the botnet to propagate across different device types.
- Analysis confirmed that several in-the-wild exploit attempts were flawed. Common errors included targeting the wrong parameter and relying on utilities not present in the router's limited environment.
- Despite these flaws, the underlying vulnerability is valid and exploitable. Successful exploitation requires authenticated access to the router's web interface, which is often possible due to default credentials.

Recommendations

- Identify and decommission end-of-life network devices that no longer receive security updates.
- Enforce strong authentication and remove default credentials on all network infrastructure.
- Restrict or disable remote management interfaces on routers where not operationally required.

- Monitor network traffic for unusual outbound connections originating from edge devices.
- Conduct asset visibility reviews to ensure unmanaged or legacy routers are not present within the environment.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Mirai-Like Botnet Exploiting CVE-2023-33538 in TP-Link Routers

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
DPRK-linked Actor 'Sapphire Sleet' macOS Social Engineering Intrusion Campaign	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a macOS-focused intrusion campaign attributed to the DPRK-linked actor Sapphire Sleet that relies on social engineering rather than software exploitation. The campaign impersonates legitimate software updates, persuading users to manually execute malicious AppleScript files that initiate credential theft and data collection.

This campaign may impact organizations in the financial sector that rely on macOS devices or support digital asset operations. Financial institutions should be aware that user-initiated execution within trusted system tools could affect environments where sensitive credentials, personal data, or cryptocurrency assets are accessed.

Technical Details

- The campaign begins with social engineering lures that present malicious files as legitimate software updates. Victims are convinced to manually run these files, bypassing automatic security enforcement.
- The initial lure is delivered as a compiled AppleScript file that opens in macOS Script Editor by default. Users are instructed to execute the script, placing the activity within a trusted, user-approved context.
- Execution relies on user-initiated actions rather than exploiting software vulnerabilities. This allows the attacker to operate outside several built-in macOS protections.
- After execution, the script retrieves additional payloads using native system tools. These payloads expand the intrusion while minimizing suspicious on-disk artifacts.
- AppleScript is used as a late-stage component for credential harvesting. This includes accessing saved passwords, authentication material, and other sensitive user data.

- The campaign manipulates macOS permissions to enable further access without triggering visible prompts. This increases attacker control while reducing user awareness.
- Persistence is established using trusted system mechanisms. These techniques allow continued access across system restarts.
- Compromised systems are used to collect and exfiltrate personal data and digital asset-related information. Exfiltration occurs after the attacker has confirmed sustained access.

Recommendations

- Strengthen user awareness around unexpected software update prompts and script execution requests.
- Restrict or monitor execution of AppleScript files and other user-initiated scripting where possible.
- Review macOS systems for abnormal persistence mechanisms and unauthorized permission changes.
- Monitor endpoint activity for unusual use of native tools performing network or credential-access operations.
- Ensure macOS devices are kept up to date with the latest security protections and platform updates.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – DPRK-linked Actor 'Sapphire Sleet' macOS Social Engineering Intrusion Campaign

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multi-Persona Campaign Driving Destructive and Influence Operations	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a coordinated cyber campaign operating under rotating alias including Homeland Justice, Karma, KarmaBelow80 and Handala. Rather than independent hacktivist groups, these identities function as branded layers of a single operational ecosystem used to conduct destructive intrusions, data exfiltration, and influence operations.

This campaign may impact organizations in the financial sector. Financial entities should be aware that these campaigns combine technical compromise with public attribution and narrative shaping, increasing both operational and reputational risk.

Technical Details

- Across all personas, the actors follow a consistent intrusion lifecycle that includes initial access, long-term persistence, internal reconnaissance, credential harvesting, and structured data exfiltration. These intrusions are often maintained for extended periods prior to public exposure.
- Destructive activity is selectively employed based on operational objectives and includes ransomware-style encryption, disk wiping, and system incapacitation. These actions are typically executed after data collection is complete, maximizing both technical disruption and downstream influence impact.
- Public disclosure is a core component of the campaign. Controlled websites and Telegram channels are used to claim responsibility and release stolen data.
- Infrastructure analysis shows repeated reuse of domain naming conventions and hosting strategies across personas. Domains are frequently rotated across different top-level domains to ensure resilience and continuity rather than long-term persistence of individual assets.
- The actors perform distinct operational roles within the same ecosystem. Homeland Justice emphasizes punitive and disruptive action, Karma and KarmaBelow80 provide adaptive interfaces for regional targeting, and Handala focuses on sustained influence operations, curated leaks, and narrative shaping.
- The campaign integrates surveillance and monitoring capabilities alongside intrusion tooling, enabling ongoing observation of compromised environments and affected individuals, including journalists and dissidents.
- Overall activity reflects centralized direction and coordination rather than decentralized hacktivism. The consistent tradecraft, timing, infrastructure overlap, and rhetorical framing indicate a structured, state-directed operation.

Recommendations

- Monitor for signs of long-dwell intrusions combined with staged data exfiltration and delayed public attribution.
- Review exposure of internet-facing services and tighten access controls on externally reachable management interfaces.
- Incorporate reputational and influence-operation risk into incident response planning, alongside technical containment.
- Track emerging campaign branding and narrative shifts, as persona changes do not indicate a change in underlying capability.
- Ensure crisis communication and legal teams are prepared for coordinated hack-and-leak scenarios.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Multi- Persona Campaign Driving Destructive and Influence Operations

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 PhantomCLR: Stealth Post-Exploitation via AppDomain Hijacking	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified Operation PhantomCLR, a sophisticated post-exploitation campaign that abuses the .NET AppDomainManager mechanism to execute malicious code within a legitimate, digitally signed Windows utility. The technique allows attackers to hijack application initialization and run in-memory malware without modifying the trusted executable.

This campaign may impact organizations in the financial sector operating in the Middle East and EMEA regions. Financial institutions should be aware that trusted binary abuse and in-memory execution techniques could affect environments that rely on traditional endpoint and network security controls.

Technical Details

- The campaign abuses the .NET AppDomainManager feature to hijack application startup logic. This causes attacker-controlled code to execute before the legitimate application initializes.
- A digitally signed windows utility is used as the execution host. The original binary is not modified, allowing malicious activity to inherit trust from the signed executable.
- Attackers deploy a malicious configuration file alongside the trusted executable. The .NET runtime automatically loads this configuration during application startup.
- The configuration file instructs the runtime to load a rogue .NET assembly as the AppDomainManager. This enables stealth code execution within a trusted process context.
- Malicious code is executed entirely in memory using just-in-time execution techniques. This reduces disk artifacts and limits traditional detection opportunities.
- The framework uses computational delays and constrains key derivation loops. These techniques are designed to evade sandbox analysis and automated inspection.
- Command-and-control communication is established through cloud-based content delivery infrastructure. This masks malicious traffic as legitimate cloud service activity.
- Anti-forensic mechanisms are employed to remove memory artifacts after execution. This complicates post-incident investigation and forensic reconstruction.

Recommendations

- Review endpoints for unexpected configuration files associated with trusted .NET executables.
- Monitor .NET process initialization for abnormal AppDomainManager usage or unexpected assembly loading.
- Enhance endpoint monitoring for in-memory execution patterns and abnormal JIT behavior.
- Inspect outbound traffic for cloud-based communication patterns originating from non-browser processes.
- Treat any suspected compromise involving trusted binary abuse as a full system compromise and initiate incident response accordingly.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Operation PhantomCLR: Stealth Post-Exploitation via AppDomain Hijacking

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
QEMU Abuse Enables Stealth Credential Theft and Ransomware Operations	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified active campaigns abusing QEMU, an open-source machine emulator, to conceal malicious activity inside hidden virtual machines. The technique allows attackers to perform credential harvesting, data exfiltration, and ransomware staging while remaining largely invisible to host-based security controls.

This campaign may impact organizations in the financial sector that rely on traditional endpoint detection and monitoring. Financial institutions should be aware that hidden virtualization layers could affect environments where attackers seek long-term access, credential theft, and follow-on ransomware deployment.

Technical Details

- Attackers abused QEMU to run hidden Linux virtual machines directly on compromised Windows hosts. Malicious activity executed inside the VM remains largely unseen by endpoint security running on the host system.

- The campaign leveraged QEMU as a covert access mechanism rather than deploying traditional backdoors. This allowed attackers to operate in an isolated environment with minimal forensic artifacts left behind.
- In one campaign, attackers created a scheduled task to launch a QEMU virtual machine under SYSTEM-level privileges. The virtual disk image was disguised using misleading file extensions to blend in with normal files.
- The hidden VM established a reverse SSH tunnel to provide attackers with persistent remote access. Port forwarding was used to expose SSH access while avoiding detection on the host.
- The virtual machine ran a lightweight Linux distribution and hosted attacker tooling. These tools enabled credential harvesting, network discovery, data staging, and command execution.
- Post-compromise activity included creating volume shadow copies and copying Active Directory database files and registry hives. Native system tools were used to reduce suspicion during credential extraction.
- A second campaign used vulnerability-based initial access and deployed remote access software for persistence. QEMU was then introduced to host tools used for directory reconnaissance and credential abuse.
- In later stages, attacker activity inside the VM supported ransomware preparation and deployment. The use of virtualization allowed attackers to maintain flexibility while minimizing detection risk.

Recommendations

- Audit environments for unauthorized virtualization software and unexpected QEMU executions.
- Review scheduled tasks and services running with elevated privileges for abnormal behavior.
- Monitor systems for hidden virtual disk images using uncommon file extensions.
- Inspect outbound network traffic for unusual SSH tunnels or port forwarding activity.
- Treat detections involving hidden VMs as potential indicators of extended compromise and investigate accordingly.

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
Black Basta-Style Social Engineering Campaign Targeting Executives	MEDIUM	CLEAR	Cyber Breach	Open Source

Executive Summary

Researchers have identified a coordinated social engineering campaign targeting executive users that builds on the tradecraft previously associated with the Black Basta ransomware group. The activity combines automated email bombing with Microsoft Teams based help desk impersonation to rapidly gain remote access to executive-level systems.

This campaign may impact organizations in the financial sector where executive users have elevated access privileges. Financial institutions should be aware that targeting executives directly could affect environments by reducing the need for lateral movement and enabling faster progression to post-compromise activity.

Technical Details

- The campaign revives and evolves a social engineering playbook historically used by Black Basta affiliates. The approach emphasizes speed, automation, and executive-level targeting rather than widespread phishing.
- Attacks begin with large-scale email bombing campaigns designed to overwhelm a victim's inbox. This disruption creates urgency and primes the target for follow-on social engineering.
- Shortly after the email bombing starts, attackers contact victims via Microsoft Teams while impersonating internal IT or help desk staff. Messages are often sent rapidly and in close succession.
- The impersonated support personnel offer assistance with stopping the email flood. Conversations are structured to build trust and lower suspicion during the interaction.
- Victims are persuaded to grant remote access using legitimate remote management tools. In observed cases, attackers progressed from Teams messaging to script execution within minutes.
- C-suite roles are deliberately prioritized due to their elevated exposure. This reduces the attacker's need for additional privilege escalation or internal reconnaissance.
- The targeting logic appears automated, with refined selection of titles and roles. Lower-privilege users are increasingly excluded from targeting workflows.
- Campaign metrics show a significant increase in executive targeting during early 2026. The activity suggests a single, coordinated effort rather than unrelated copycat attacks.

Recommendations

- Enforce out-of-band verification for any help desk request involving remote access, especially for senior staff.
- Restrict and closely monitor the use of remote management and support tools across the environment.
- Provide targeted security awareness training for executives focused on collaboration-platform abuse.
- Monitor for high-volume email activity followed by rapid inbound collaboration messages.

- Test executive incident response readiness through simulations that reflect compressed attack timelines.

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
Signed Adware (PUP) Update Mechanism Enables Large-Scale Defense Evasion	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a large-scale campaign in which digitally signed adware, classified as potentially unwanted programs (PUPs), abused a legitimate software update mechanism to disable endpoint security controls. The operation leveraged trusted code-signed executables to deploy SYSTEM-level payloads that systematically removed and blocked antivirus protections.

This campaign may impact organizations in the financial sector where adware or browser-based utilities are present on corporate endpoints. Financial institutions should be aware that signed PUP components can be repurposed into supply-chain-like attack vectors capable of bypassing endpoint defenses at scale.

Technical Details

- The campaign involved executables signed by Dragon Boss Solutions LLC, a publisher associated with browser-like adware tools. While initially classified as PUPs, the software exhibited advanced post-installation behavior.
- A commercial update framework was used to polling remote servers for updates. The mechanism ran silently, frequently, and with SYSTEM privileges, allowing payload execution without user interaction.
- Update payloads were delivered as MSI installers and PowerShell scripts. These payloads executed multi-stage routines designed to identify, terminate, uninstall, and block reinstallation of multiple antivirus products.
- Prior to execution, the payloads performed host reconnaissance, including privilege checks, virtualization detection, connectivity validation, and registry queries to identify installed security software.
- Persistence was established through Windows Management Instrumentation (WMI) event subscriptions and scheduled tasks. These mechanisms ensured the defensive tampering re-executed at boot, logon, and fixed time intervals.
- The antivirus suppression logic repeatedly terminated security processes, invoked vendor uninstallers, removed registry entries, and modified system configurations to prevent recovery of protections.

- A critical risk was identified in the update configuration: a primary update domain used by the software was unregistered. Control of this domain would allow any actor to distribute arbitrary payloads to all infected systems.
- After researchers registered and sinkholed the domain, tens of thousands of compromised endpoints contacted the infrastructure within hours. This demonstrated the scale and immediacy of exposure.
- The campaign transformed a widespread PUP deployment into a latent supply-chain attack platform. With endpoint security disabled, the environment was primed for future delivery of more destructive payloads.

Recommendations

- Audit enterprise environments for the presence of signed PUPs and browser-based utilities running with elevated privileges.
- Review and restrict execution of third-party auto-updaters, especially those operating silently with SYSTEM access.
- Strengthen controls around trusted code-signing assumptions and software allowlisting policies.
- Monitor for WMI-based persistence and repeated security-tool termination behavior.
- Treat widespread PUP detections as potential early indicators of defense-evasion activity rather than benign nuisance software.

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
Remote Support Social Engineering via Microsoft Teams with Follow-On Lateral Movement	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers have identified a human-operated intrusion campaign in which threat actors abuse cross-tenant Microsoft Teams communications to impersonate IT or helpdesk personnel. Victims are socially engineered into granting remote support access, enabling attackers to establish interactive control without exploiting software vulnerabilities.

This campaign may impact organizations in the financial sector that rely on collaboration platforms and remote support tools. Financial institutions should be aware that user-approved access combined with trusted tooling may enable attackers to move laterally and access sensitive data while appearing to conduct legitimate IT operations.

Technical Details

- The intrusion begins with cross-tenant Microsoft Teams messages initiated by external users posing as internal IT or helpdesk staff. The interaction relies on real-time communication to build trust and urgency around account or security issues.
- Victims are persuaded to initiate remote support sessions using legitimate tools such as Quick Assist. Access is explicitly user-approved, allowing attackers to gain interactive system control without triggering exploit-based detections.
- Once connected, attackers perform rapid interactive reconnaissance to validate privileges, domain membership, and network reach. Native command-line utilities are used to blend activity with normal administrative behavior.
- Malicious payloads are staged in user-writable directories and executed through trusted, signed applications. This technique allows attacker-supplied code to run while evading traditional security alerts.
- Execution state is maintained using registry-based mechanisms. These ensure continuity of access across subsequent intrusion phases.
- Command-and-control traffic is established over standard network protocols. Communications resemble routine enterprise activity, complicating detection.
- Lateral movement is performed using built-in administrative protocols. Attackers pivot toward higher-value systems, including domain-joined assets.
- Follow-on remote management tools may be deployed to expand control across the environment. These tools provide persistent access without introducing obvious malware artifacts.
- Data collection targets business-relevant information. Staging and transfer are performed using common data synchronization utilities to external cloud storage.

Recommendations

- Enforce out-of-band verification before approving remote support requests, especially those initiated via external collaboration channels.
- Restrict and closely monitor cross-tenant collaboration and remote assistance tool usage.
- Train users to recognize social engineering that leverages trusted workplace platforms.
- Monitor for patterns linking remote support sessions to immediate administrative activity.
- Treat abuse of trusted tools as a potential early indicator of broader compromise.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Remote Support Social Engineering via Microsoft Teams with Follow-On Lateral Movement

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Cisco ISE and Webex Vulnerabilities Enable RCE and Authentication Bypass	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Cisco has disclosed multiple vulnerabilities affecting Cisco Identity Services Engine (ISE), ISE Passive Identity Connector (ISE-PIC), and Cisco Webex Services. The issues include several remote code execution flaws caused by insufficient input validation, as well as an authentication bypass in Webex Single Sign-On due to improper certificate validation.

These vulnerabilities may impact organizations in the financial sector that rely on Cisco ISE for network access control and Webex for collaboration. Financial institutions should be aware that successful exploitation could affect authentication services, privileged access controls, and user identity integrity if the affected systems remain unpatched.

Technical Details

- Cisco ISE and ISE-PIC are affected by a critical remote code execution vulnerability tracked as CVE-2026-20147. The flaw is triggered by crafted HTTP requests and stems from insufficient input validation, requiring administrator credentials to exploit.
- Successful exploitation of CVE-2026-20147 allows arbitrary command execution and privilege escalation to root. In certain cases, it can also cause node crashes, leading to denial-of-service conditions and network authentication disruption.
- A related vulnerability, CVE-2026-20148, impacts Cisco ISE and ISE-PIC through a path traversal flaw. This issue also requires administrator credentials and is exploitable via crafted HTTP requests.
- CVE-2026-20148 enables attackers to read sensitive system files. Depending on file exposure, this may lead to credential disclosure or further follow-on exploitation.
- Cisco ISE is additionally affected by critical RCE vulnerabilities CVE-2026-20180 and CVE-2026-20186. These flaws are exploitable using read-only administrator privileges, lowering the barrier to exploitation.
- Exploitation of CVE-2026-20180 and CVE-2026-20186 enables operating system command execution and escalation to root. In single-node deployments, this can also result in denial-of-service conditions.
- Cisco Webex Services are impacted by CVE-2026-20184, an authentication bypass vulnerability in SSO-enabled environments. The flaw is caused by improper certificate validation and does not require authentication.
- CVE-2026-20184 allows attackers to craft malicious SSO tokens and impersonate arbitrary users. This can lead to unauthorized access, account takeover, and potential data exposure within Webex services.

Recommendations

- Upgrade Cisco ISE and ISE-PIC deployments to the fixed patch versions corresponding to their installed releases.
- Validate that patches are consistently applied and active across all ISE nodes in distributed environments.

- Review administrative access levels on Cisco ISE to limit exposure from lower-privilege accounts.
- Update the SAML identity provider certificate for Webex SSO in the Control Hub as advised.
- Verify certificate trust chains and expiration dates to prevent future SSO authentication bypass risks.

Vulnerability and affected product details can be found *here*, *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Critical Vulnerabilities Across Adobe Products Enable Code Execution	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Adobe has released security updates addressing multiple vulnerabilities across a broad set of products, including Acrobat Reader, InDesign, InCopy, Experience Manager, FrameMaker, Connect, ColdFusion, Bridge, Photoshop, DNG SDK, and Illustrator. The disclosed issues span arbitrary code execution, authentication and security bypass, cross-site scripting, privilege escalation, information disclosure, and denial-of-service conditions.

These vulnerabilities may impact organizations in the financial sector that rely on Adobe products for document handling, content management, collaboration, and development workflows. Financial institutions should be aware that unpatched systems could affect endpoint security, application integrity, and access to sensitive data if exploited.

Technical Details

- Adobe Acrobat Reader is affected by prototype pollution vulnerabilities that may allow arbitrary code execution or unauthorized file system reads. These issues could be triggered through crafted content processed by the application.
- Adobe InDesign contains multiple critical vulnerabilities that enable arbitrary code execution. Additional issues may cause denial-of-service or expose memory contents during document processing.
- Adobe InCopy is impacted by critical flaws that allow arbitrary code execution. Exploitation could occur when handling malicious or specially crafted files.
- Adobe Experience Manager includes several vulnerabilities related to cross-site scripting. In certain circumstances, these flaws could be chained to enable code execution within affected environments.
- Adobe FrameMaker is affected by numerous critical vulnerabilities enabling arbitrary code execution. Additional issues expose file system contents or memory data under specific conditions.
- Adobe Connect contains multiple critical deserializations and cross-site scripting vulnerabilities. These issues can lead to code execution and include a separate flaw that allows privilege escalation.

- Adobe ColdFusion is affected by critical path traversal, arbitrary code execution, and security bypass vulnerabilities. Exploitation could allow attackers to access restricted resources or fully compromise the application.
- Adobe Bridge, Photoshop, and Illustrator each contain critical vulnerabilities that enable arbitrary code execution when processing crafted files. These issues primarily affect systems used for media handling workflows.
- Adobe DNG SDK includes vulnerabilities that may result in denial-of-service or memory exposure. These issues could impact applications that integrate the SDK.

Recommendations

- Apply the latest Adobe security updates across all affected products without delay.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Fortinet Vulnerabilities Enable Remote Code Execution and Unauthorized Access	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Fortinet has disclosed multiple critical and high-severity vulnerabilities affecting a broad range of products, including FortiOS, FortiManager, FortiAnalyzer, FortiSandbox, FortiClientEMS, FortiSOAR, and FortiWeb. The most severe issues allow remote code execution, authentication bypass, and arbitrary file operations, in some cases without authentication.

These vulnerabilities may impact organizations in the financial sector that rely on Fortinet products for perimeter security, network management, and security orchestration. Financial institutions should be aware that exploitation could affect security monitoring, network access control, and sensitive data protection if exposed systems remain unpatched.

Technical Details

- A heap-based buffer overflow vulnerability (CVE-2026-22828) affects FortiAnalyzer Cloud, allowing unauthenticated remote code execution through crafted requests sent to the oftpd daemon. Successful exploitation provides attackers with remote execution capability.
- FortiSandbox is impacted by an OS command injection vulnerability (CVE-2026-39808) that allows unauthenticated attackers to execute arbitrary commands via malicious HTTP requests. Affected versions include 4.4.0 through 4.4.8, with fixes available in version 4.4.9 and later.

- SQL injection vulnerabilities affect FortiClientEMS (CVE-2026-39809) and FortiDDoS-F (CVE-2026-39815). Authenticated attackers may execute arbitrary SQL queries, potentially accessing or modifying sensitive backend data.
- An authentication bypass and path traversal flaw (CVE-2026-39813) in the FortiSandbox API allows attackers to bypass authentication controls. The issue affects FortiSandbox versions 5.0.0 through 5.0.5 and 4.4.0 through 4.4.8, with fixes in later releases.
- FortiSOAR contains an authentication bypass vulnerability related to 2FA replay (CVE-2026-23708), reducing the effectiveness of multi-factor authentication protections.
- Multiple vulnerabilities in FortiSOAR and FortiClientEMS expose credentials due to weak storage practices and hardcoded cryptographic keys. These issues increase the likelihood of credential compromise if access is gained.
- Cleartext transmission of sensitive data was identified in multiple Fortinet products, increasing the risk of interception in certain deployment scenarios.
- A path traversal vulnerability (CVE-2025-61624) affects FortiOS, FortiPAM, FortiProxy, and FortiSwitchManager, enabling arbitrary file write or delete operations through the CLI.

Recommendations

- Apply the latest Fortinet firmware and security patches immediately across all affected products.
- Prioritize systems exposed to the internet (FortiOS, FortiManager, FortiAnalyzer).

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft April 2026 Security Updates Address Actively Exploited SharePoint Zero-Day	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Microsoft has released its April 2026 Patch Tuesday updates, remediating 167 security vulnerabilities across its ecosystem. The release includes a critical, actively exploited zero-day vulnerability affecting Microsoft SharePoint Server, alongside multiple remote code execution, elevation of privilege, and security bypass issues across Windows components and enterprise services.

These vulnerabilities may impact organizations in the financial sector that operate Microsoft infrastructure, including SharePoint, Active Directory, Remote Desktop, and Windows clients. Financial institutions should be aware that exploitation could affect publicly exposed services, enable post-compromise privilege escalation, and weaken key security controls if updates are not applied promptly.

Technical Details

- The April 2026 release addresses an actively exploited zero-day vulnerability, CVE-2026-32201, affecting Microsoft SharePoint Server. The flaw is a spoofing vulnerability and has been confirmed as exploited in the wild.
- Multiple critical unauthenticated remote code execution vulnerabilities were fixed in core networking services. These include CVE-2026-33824 in Windows IKEv2 and CVE-2026-33827 in Windows TCP/IP.
- Active Directory is affected by a critical remote code execution vulnerability (CVE-2026-33826). Successful exploitation could allow attackers to compromise directory services in enterprise environments.
- Client-side remote code execution vulnerabilities were patched in the Remote Desktop Client and Microsoft Office. This includes CVE-2026-32157 and a cluster of Office RCE flaws (CVE-2026-32190, CVE-2026-33114, CVE-2026-33115).
- The release includes a high concentration of elevation of privilege vulnerabilities across Windows components. Affected areas include WinSock, the CLFS driver, Desktop Window Manager, Windows COM, UPnP Device Host, and Function Discovery.
- Multiple elevation of privilege flaws enable attackers with initial access to escalate permissions locally. These vulnerabilities significantly increase the impact of phishing or user-level compromise.
- Security feature bypass vulnerabilities affect critical Windows protections. These include bypasses for UEFI Secure Boot, Windows Hello, and BitLocker encryption.
- Additional spoofing vulnerabilities were remediated in Remote Desktop Protocol and the Windows Shell. In certain scenarios, these issues could be leveraged to deceive users or facilitate further exploitation.

Recommendations

- Apply the April 2026 Microsoft security updates immediately across all supported systems.
- Prioritize securing public-facing SharePoint servers and other internet-exposed services, and immediately isolate or restrict access to vulnerable SharePoint instances.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Medium-Severity Vulnerabilities Identified Across Cisco Products	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Cisco has disclosed multiple vulnerabilities affecting several products, including Secure Web Appliance, Webex Contact Center, Unity Connection, ThousandEyes Enterprise Agent, and Identity Services Engine (ISE). The issues span authentication bypass, cross-site scripting, SQL injection, privilege escalation, and arbitrary file access.

These vulnerabilities may impact organizations in the financial sector that use Cisco products for secure web access, identity management, contact center operations, and network monitoring. Financial institutions should be aware that successful exploitation could affect confidentiality and integrity of systems if recommended mitigations are not applied.

Technical Details

- Cisco Secure Web Appliance is affected by an authentication bypass vulnerability (CVE-2026-20152). Improper validation mechanisms allow an unauthenticated attacker to gain unauthorized access to the system, potentially exposing administrative functionality.
- Cisco Webex Contact Center contains a cross-site scripting vulnerability (CVE-2026-20170). Attackers could inject malicious scripts into the web interface, potentially leading to session hijacking or unauthorized access to user data.
- Cisco Unity Connection is impacted by multiple vulnerabilities (CVE-2026-20059, CVE-2026-20060, CVE-2026-20061). These include cross-site scripting, open redirect, and SQL injection issues that may allow script execution, redirection to malicious sites, or backend database manipulation.
- Additional Cisco Unity Connection vulnerabilities (CVE-2026-20078, CVE-2026-20081) enable arbitrary file downloads. Exploitation could permit attackers to retrieve sensitive system files without proper authorization.
- Cisco ThousandEyes Enterprise Agent is affected by an arbitrary file overwrite vulnerability (CVE-2026-20161). An attacker could overwrite critical system files, potentially leading to service disruption or further compromise.
- Cisco Identity Services Engine contains multiple cross-site scripting vulnerabilities (CVE-2026-20132). These issues could allow injection of malicious scripts into the administrative web interface.
- Cisco Identity Services Engine also includes an authenticated privilege escalation vulnerability (CVE-2026-20136). A low-privileged user may be able to elevate privileges and gain broader control over the system.

Recommendations

Apply the mitigations or workarounds provided by Cisco for each affected product.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Critical Vulnerabilities in Google Chrome	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Google has released a Stable Channel security update for Chrome addressing 31 vulnerabilities across the browser, including multiple critical memory corruption flaws. The most severe issues involve heap buffer overflows and use-after-free conditions that could be exploited to achieve remote code execution through malicious web content.

These vulnerabilities may impact organizations in the financial sector where Google Chrome is widely used for web-based banking portals, trading platforms, and internal applications. Financial institutions should be aware that successful exploitation could affect endpoint security and user sessions if browsers are not promptly updated.

Technical Details

- Several critical vulnerabilities were identified in core Chrome components related to graphics, rendering, and browser internals. These include heap buffer overflows in ANGLE (CVE-2026-6296) and Skia (CVE-2026-6298), which handle graphics and image processing.
- Multiple use-after-free vulnerabilities were fixed in high-risk browser components such as the Proxy service (CVE-2026-6297), Prerender functionality (CVE-2026-6299), and XR features (CVE-2026-6358). These flaws could allow memory corruption during browser operations.
- High-severity issues affect widely exercised components responsible for video handling, codecs, CSS processing, file system interactions, and rendering pipelines. Exploitation may occur during normal browsing activity when processing specially crafted pages or media.
- Chrome's JavaScript engine and optimization components were impacted by type confusion vulnerabilities in Turbofan (CVE-2026-6301, CVE-2026-6307). These issues could allow attackers to manipulate execution flow within the browser.
- Several vulnerabilities were found in PDFium, Chrome's PDF rendering engine, including multiple heap buffer overflows. These flaws increase risk when users open embedded or downloaded PDF files in the browser.
- Additional high-severity flaws include insufficient policy enforcement in passwords and cross-origin resource sharing logic. These issues could weaken isolation boundaries under certain conditions.
- Medium-severity vulnerabilities include type confusion in the V8 engine and additional use-after-free flaws in payments and codecs components. While less severe, these still contribute to overall attack surface.

Recommendations

- Upgrade Google Chrome to the fixed version or the latest available Stable Channel release immediately.
- All issues have been fixed in Chrome version 147.0.7727.101/102 for Windows and macOS, and 147.0.7727.101 for Linux.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Vercel Discloses Security Incident Linked to Third Party OAuth Compromise	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Researchers disclosed a security incident at Vercel involving unauthorized access to internal systems following the compromise of a third-party OAuth integration. The intrusion originated from a third-party AI service used by an employee, allowing attackers to leverage OAuth permissions to access internal environments and certain customer configuration data.

This campaign may impact organizations in the financial sector that rely on third-party SaaS integrations and OAuth-based access models. Financial institutions should be aware that compromised OAuth tokens could affect environments where non-sensitive credentials or configuration variables are accessible through trusted cloud platforms.

Technical Details

- The intrusion originated from a security incident at a third-party AI service that had OAuth access to a Vercel employee's Google Workspace account. The attacker reused valid OAuth permissions without triggering password or multi-factor authentication challenges.
- Using the compromised OAuth access, the attacker took over the employee's Workspace account. This provided a pathway into certain internal Vercel systems connected to that identity.
- The attacker demonstrated rapid lateral movement and familiarity with internal systems. Access was escalated to selected environments rather than across the full production infrastructure.
- Environment variables belonging to a limited subset of customers were exposed. Only variables not explicitly marked as "sensitive" were readable.
- Environment variables designated as sensitive were protected in encrypted storage. There was no evidence that these protected values were accessed.
- No service disruption was reported during the incident. Platform availability remained intact while containment actions were underway.
- Impact was limited to a small number of customers. Affected users were contacted directly and instructed to rotate credentials.
- Investigation and response actions included engagement with external incident response support, notification of law enforcement, and coordination with the third-party provider to assess root cause.

Recommendations

- Review third-party OAuth applications connected to identity providers and remove integrations that are no longer required.
- Enforce least-privilege OAuth permissions for SaaS tools accessing enterprise identity platforms.
- Rotate credentials and environment variables that are not explicitly protected or marked as sensitive.
- Review audit logs for abnormal access patterns associated with legitimate OAuth applications.
- Reassess internal access paths that rely on employee SaaS identities to access production or customer environments.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Vercel Discloses Security Incident Linked to Third Party OAuth Compromise

Reference to the Source

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

MuddyWater-Aligned Reconnaissance and Intrusion Campaign Targeting the Middle East

ATT&CK Tactic	ATT&CK Technique (ID)	Description
Reconnaissance	Active Scanning (T1595)	Large-scale scanning of >12,000 internet-exposed systems, vulnerability-specific grouping; automated continuous recon
Initial Access	Exploit Public-Facing Application (T1190)	Selective exploitation attempts against high-value targets using newly disclosed vulnerabilities in public-facing platforms
Credential Access	Brute Force (T1110)	Enterprise email brute-force using custom scripting and automated tooling
Discovery	Account Discovery (T1087)	Targeted username/account enumeration against specific organizations
Persistence / Defense Evasion	Valid Accounts (T1078)	Use of compromised credentials to access enterprise services
Command and Control	Application Layer Protocol (T1071) and/or Non-Application Layer Protocol (T1095)	Multi-protocol C2 (socket-based and web-based), modular controllers, custom message format
Command and Control	Encrypted Channel (T1573)	Encrypted data exchange in web-based controllers
Collection	Data from Information Repositories (T1213)	Collection of sensitive data from compromised environments (identity/travel, payroll, financial, internal documents)
Collection	Data Staged (T1074)	Structured data collection and staging prior to exfiltration (~200 files staged)
Exfiltration	Exfiltration Over C2 Channel (T1041)	Confirmed exfiltration of staged sensitive data from victim environment

Seedworm Campaign Abusing Microsoft Teams to Deploy Dindoor Backdoor

Tactic	Technique	Description
Initial Access	Phishing (T1566)	External actor contacts the victim via Microsoft Teams while impersonating IT support and requests assistance.
Execution	User Execution (T1204)	The user is convinced to execute an “update”-themed installer masquerading as a Windows update.
Defense Evasion	Masquerading (T1036)	Impersonation of IT support and use of deceptive naming designed to resemble legitimate support context; persistence name also mimics legitimate audio service.
Defense Evasion	Obfuscated/Compressed Files and Information (T1027)	The runtime executes a highly obfuscated, Base64-encoded payload.
Defense Evasion	Subvert Trust Controls Code Signing (T1553.002)	The dropper installer is described as being signed with a certificate that was revoked at the time of investigation.
Persistence	Registry Run Keys/Startup Folder (T1547.001)	Persistence via creation of a deceptive registry Run key pointing to attacker-delivered malware, named to resemble a legitimate service.

Command and Control	Application Layer Protocol Web Protocols (T1071.001)	Decoded payload establishes C2 communications; network traffic shows web requests consistent with the abused runtime's user agent.
Discovery	System Information Discovery (T1082)	Exfiltrated host metadata includes hostname and operating system details.
Discovery	System Owner/User Discovery (T1033)	Exfiltrated host metadata includes the username.
Command and Control / Collection	Ingress Tool Transfer (T1105)	A dropped script is responsible for retrieving additional payloads after initial infection.
Execution	Command and Scripting Interpreter PowerShell (T1059.001)	A PowerShell script is explicitly described as retrieving additional payloads.
Execution	Command and Scripting Interpreter Visual Basic (T1059.005)	A VBScript component is listed among items dropped and used in the intrusion timeline.
Execution	Command and Scripting Interpreter JavaScript (T1059.007)	The attacker abuses the Deno runtime to execute an encoded payload directly in memory.
Defense Evasion	Hidden Files and Directories (T1564.001)	Several components are deployed into a hidden directory as part of the dropper's activity.
Exfiltration	Exfiltration Over C2 Channel (T1041)	The decoded payload communicates with C2 and exfiltrates username/hostname/OS details

Mirai-Like Botnet Exploiting CVE-2023-33538 in TP-Link Routers

Tactic	Technique	Description
Initial Access	T1190 Exploit Public-Facing Application	Command injection via the router's web management functionality can lead to arbitrary command execution when properly exploited.
Initial Access	T1078.001 Valid Accounts Default Accounts	Researchers found exploitation requires authentication to the web interface and highlighted reliance on default credentials as a practical enabler.
Execution	T1059.004 Command and Scripting Interpreter Unix Shell	The vulnerable input is incorporated into a command executed by the system shell, enabling attacker-supplied command execution.
Command and Control	T1105 Ingress Tool Transfer	Observed attempts aimed to retrieve a malicious executable and run it on the device; the malware also supports update downloads.
Defense Evasion / Execution Enablement	T1222.001 File and Directory Permissions Modification	The observed command sequence included changing permissions to allow execution of the downloaded payload.
Command and Control	T1071.001 Application Layer Protocol Web Protocols	The malware's update and communication routines included HTTP-style requests and operating an HTTP service to facilitate distribution

DPRK-linked Actor 'Sapphire Sleet' macOS Social Engineering Intrusion Campaign

Tactic	Technique	Description
Initial Access	T1566.003 Spearphishing via Service	Recruiter-style outreach and delivery of a convincing "update" lure through online platforms to persuade download/execution.
Execution	T1204.002 User Execution Malicious File	Compromise depends on the user opening and running the lure in a trusted macOS scripting application.
Execution	T1059.002 Command and Scripting Interpreter AppleScript	Multi-stage payloads are AppleScript-based and executed via macOS scripting interpreters.
Execution	T1059.004 Command and Scripting Interpreter Unix Shell	Shell commands are executed from scripting context, including use of an interactive shell for privileged operations.
Defense Evasion	T1218 Signed Binary Proxy Execution	Abuse of Apple-signed utilities and trusted execution contexts to reinforce legitimacy and reduce security friction.
Defense Evasion	T1564.001 Hide Artifacts Hidden Files and Directories	Use of hidden-style artifacts and naming conventions to reduce user visibility and blend into expected directories.
Discovery	T1082 System Information Discovery	Collection of user/host/system time/OS install details and hardware/OS version for profiling and tracking.
Discovery	T1057 Process Discovery	Repeated process listing to understand running activity and environment state.
Command and Control	T1071.001 Application Layer Protocol Web Protocols	Network communication and periodic beaconing consistent with web based C2 patterns described in the campaign.
Credential Access	T1555.001 Credentials from Password Stores Keychain	Collection includes keychain-related data as part of the data theft phase
Credential Access	T1555.003 Credentials from Password Stores Web Browsers	Collection includes browser-related credential/data theft.
Credential Access	T1056 Input Capture	Native-looking password dialog prompts the user to enter credentials, which are then validated and stolen.
Privilege Escalation	T1548.003 Abuse Elevation Control Mechanism Sudo and Sudo Caching	Interactive shell context is used to perform privileged operations that rely on sudo-style elevation.
Persistence	T1543.004 Create or Modify System Process Launch Daemon	Persistence is established via a launch daemon so components run at startup.
Defense Evasion	T1222.002 File and Directory Permissions Modification	File permissions/ownership are adjusted to enable execution with elevated privileges.
Defense Evasion / Privilege Escalation	T1556 Modify Authentication Process (conceptual fit)	Direct manipulation of the macOS consent/permissions database to grant automation rights without prompts.

Defense Evasion	T1620 Reflective Code Loading	In-memory loading of additional payloads received from C2 rather than writing them to disk. [microsoft.com]
Collection	T1074 Data Staged	Data is collected, staged, and prepared prior to exfiltration.
Collection	T1560 Archive Collected Data	Data is compressed as part of the staging/exfiltration workflow.
Exfiltration	T1567.002 Exfiltration Over Web Service	Exfiltration includes sending stolen credentials via a messaging-platform bot service interface.

Multi-Persona Campaign Driving Destructive and Influence Operations

Tactic	Technique	Description
Initial Access	Exploit Public-Facing Application	Initial foothold described via exploitation of an internet-facing SharePoint weakness and other exposed services.
Initial Access	Valid Accounts	Initial access described as occurring via credential compromise in multiple intrusions.
Execution	PowerShell	PowerShell-based propagation is described for destructive tooling deployment
Persistence	Server Software Component Web Shell	Webshells deployed on compromised servers to maintain durable access and enable command execution.
Discovery	Network and System Discovery	Systematic internal reconnaissance to enumerate topology, identify key systems, and map trust relationships.
Defense Evasion	Signed Binary Proxy Execution	Use of signed binaries is noted as supporting evasion and trust abuse in destructive deployment.
Credential Access	Credential Dumping	Credential harvesting described as a central component of post-compromise activity.
Credential Access	Account Manipulation	Account creation/modification and related manipulation described via email infrastructure access.
Lateral Movement	Remote Services	Lateral movement conducted using standard administrative protocols such as remote desktop and file-sharing/transfer mechanisms.
Collection	Email Collection	Compromise of email infrastructure used to access and extract large volumes of sensitive communications.
Command and Control	Protocol Tunneling	Reverse SSH tunneling referenced as part of the toolkit during the Karma phase.
Command and Control	Web Service	Telegram is described as a persistent platform for amplification/coordination, and surveillance capabilities are noted as leveraging Telegram-based command-and-control.
Exfiltration	Exfiltration Over C2 Channel or Staged Exfiltration	Data staging and controlled extraction described ahead of public leak phases.
Impact	Data Encrypted for Impact	Ransomware-style encryption used as part of the disruption model.
Impact	Disk Wipe or Data Destruction	Destructive wiping, manual deletion, and disk formatting described to maximize disruption and complicate recovery.
Impact	Inhibit System Recovery	Destructive tooling described as emphasizing rapid incapacitation, including preventing successful system boot.

Operation PhantomCLR: Stealth Post-Exploitation via AppDomain Hijacking

Tactic	Technique	Description

Initial Access	Phishing (Spearphishing Attachment)	Delivery via spear-phishing with an archive containing all components needed for execution.
Execution	User Execution	Relies on the victim manually extracting content and launching a disguised shortcut to start the chain.
Defense Evasion	Masquerading	Uses a double-extension style visual masquerade and icon mimicry to appear as a benign document while executing a shortcut.
Defense Evasion	Signed Binary Proxy Execution	Launches malicious activity through a legitimate, digitally signed utility to inherit trust and reduce suspicion.
Defense Evasion	Hijack Execution Flow (AppDomainManager)	Forces CLR to load attacker-controlled code during application-domain initialization via a weaponized runtime configuration.
Defense Evasion	Obfuscated/Encrypted Data	Uses Base64+XOR string obfuscation and AES encryption to conceal payload and runtime strings until execution.
Defense Evasion	Virtualization/Sandbox Evasion	Implements a timing gate with CPU-intensive computation and a high-iteration constrained derivation loop to outlast sandbox windows.
Defense Evasion	Native API / Direct System Calls	Uses NTDLL-mediated direct syscall patterns to bypass userland API monitoring for sensitive operations.
Defense Evasion	Reflective Loading	Reflectively loads decrypted payload into memory and applies memory protections per section to resemble legitimate loading.
Command and Control	Web Protocols (HTTPS)	Establishes command-and-control over HTTPS once execution is complete.
Command and Control	Domain Fronting	Hides C2 using CDN-based domain fronting to complicate network detection and blocking.
Defense Evasion	Indicator Removal (In-Memory Cleanup)	Performs multi-step memory cleanup to erase artifacts and hinder post-incident investigation

Remote Support Social Engineering via Microsoft Teams with Follow-On Lateral Movement

Tactic	Technique	Description
Initial Access	Spearphishing via Service (T1566.003) using cross-tenant Teams impersonation	Stage 1 explicitly labels Teams initial contact as T1566.003 and describes impersonation of helpdesk via external Teams collaboration.
Execution	Trusted vendor-signed application execution with attacker-supplied modules (side-loading)	Stage 4 describes executing trusted signed apps alongside attacker-supplied modules to run code under a trusted context.
Persistence / Defense Evasion	Registry-backed encrypted configuration retrieved and decrypted in memory	Stage 5 describes writing a large, encoded registry value used as an encrypted configuration container, decrypted in memory to reduce disk artifacts.
Command and Control	Outbound encrypted communications over HTTPS that mimic normal traffic	Stage 6 describes outbound HTTPS communications enabling operator control while blending into routine activity.
Discovery	Interactive reconnaissance to validate privileges, host identity, OS and domain affiliation	Stage 3 describes rapid cmd-driven checks and environment validation soon after remote access.
Lateral Movement	Credential-backed remote management pivoting toward identity/domain infrastructure	Stage 7 describes internal movement using native remote management toward high-value assets including domain controllers.
Persistence	Deployment of additional commercial remote management tooling	Stage 8 describes installing an additional management platform to maintain access independent of earlier components.

Exfiltration	Data transfer using a file-synchronization utility to external cloud storage	Stage 9 describes targeted exfiltration of business-relevant documents to external cloud storage with transfer exclusions

Vercel Discloses Security Incident Linked to Third Party OAuth Compromise

Tactic	Technique	Description
Initial Access	Supply Chain Compromise (T1195)	Compromise originated with a third-party AI tool used by an employee, which served as the starting point for the intrusion.
Credential Access	Valid Accounts (T1078)	Attacker took over the employee's Google Workspace account and used that authenticated access to proceed.
Lateral Movement	Remote Services (T1021)	Attacker leveraged access from the compromised enterprise account to gain further access into Vercel environments.
Privilege Escalation	Valid Accounts (T1078)	"Series of maneuvers" escalating from the compromised account resulted in broader access to environments.
Discovery	Cloud Service Discovery (T1526)	Attacker enumerated environment variables within the platform to extend access.
Collection	Data from Information Repositories (T1213)	Attacker accessed environment variables that were not marked as sensitive, which may include secrets if stored incorrectly.

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
Active Directory	A core identity and access management service for enterprise environments.
Adobe Products	Widely used document and content tools affected by numerous code-execution vulnerabilities.
Adware	Software designed for advertising that, in this context, was repurposed to disable defenses and enable follow-on attacks.
Antivirus	Malware protection software that was deliberately disabled in some observed campaigns.
Authentication Bypass	A flaw allowing access without valid credentials or standard authentication processes.
C2 (Command and Control)	Infrastructure attackers use to manage and control compromised systems.
Certificate Validation	A security process that verifies trust in digital identities; failures enable impersonation.
Cisco ISE	Identity Services Engine; controls network access and authentication across enterprises.
Cloud Services	Internet-hosted platforms targeted through identity, access, and configuration weaknesses.
Code Signing Certificate	A digital trust mechanism that verifies software authenticity; abused to make malicious activity appear legitimate.
CSC	UAE Cyber Security Council
Cyber Influence Operation	Activity that blends cyber attacks with public messaging or data leaks to influence perception, behavior, or political outcomes.
Data Exfiltration	Unauthorized transfer of sensitive data outside an organization.
Defense Evasion	Techniques used to bypass, disable, or permanently impair security controls such as antivirus or EDR tools.
EDR (Endpoint Detection and Response)	Security platforms that detect and investigate suspicious endpoint behavior.
Endpoint Security	Tools designed to protect workstations and servers from malware and intrusions.
Executive Targeting	Deliberate focus on senior leadership due to their elevated privileges and access to sensitive systems.
Fortinet Products	Security platforms used for perimeter, network, and monitoring functions with multiple disclosed vulnerabilities.
FortiOS	Operating system powering Fortinet security appliances, impacted by RCE and bypass flaws.
Google Chrome	A widely used web browser impacted by multiple critical memory corruption flaws.
Hack-and-Leak	A tactic combining unauthorized data theft with deliberate public release to cause reputational and operational damage.
Handala	A persona used in hack-and-leak and influence operations, emphasizing public data releases.
Heap Buffer Overflow	Writing data beyond allocated memory space, potentially enabling attacker-controlled execution.
Homeland Justice	A branded cyber persona used for destructive intrusions combined with public attribution.
Human-Operated Intrusion	Attacks conducted manually by attackers who interact with systems in real time rather than relying purely on automated malware.

Karma / KarmaBelow80	Rotating personas assessed to be operational fronts of a coordinated state-aligned cyber capability rather than independent hacktivists.
Lateral Movement	Movement from one compromised system to others within the same environment.
Memory Corruption	Software flaws that allow unintended memory manipulation, often leading to code execution.
Microsoft Teams	Collaboration platform abused to impersonate IT or helpdesk staff and initiate social-engineering attacks.
MOIS	Ministry of Intelligence and Security.
OAuth	An authorization framework granting limited third-party access to accounts without passwords.
Operational Disruption	Impact that prevents business operations or security services from functioning normally.
Patch Tuesday	Microsoft's monthly release cycle for security updates.
Persistence	Techniques attackers use to maintain access to systems after initial compromise.
Privilege Escalation	Methods used by attackers to gain higher-level permissions after initial access.
PUP (Potentially Unwanted Program)	Software often treated as low risk but capable of enabling serious security compromise when misused.
Quick Assist	Built-in Windows remote support feature used by attackers to gain interactive access to endpoints.
RCE (Remote Code Execution)	A vulnerability allowing attackers to execute commands on a system remotely.
Remote Support Tools	Legitimate IT support software that allows remote system control and can be abused with user consent.
Reputational Risk	Potential damage to organizational trust and brand following cyber incidents or data leaks.
SharePoint	An enterprise collaboration platform affected by an actively exploited vulnerability.
Signed Software	Digitally signed applications trusted by systems and security tools, which can be abused to bypass defenses.
Social Engineering	Manipulation of individuals into performing actions or granting access that enables cyber intrusions.
SSO (Single Sign-On)	A system allowing access to multiple services using a single authentication step.
Supply Chain Risk	Exposure introduced through trusted third-party software, update mechanisms, or service providers.
SYSTEM Privileges	The highest level of access on Windows systems, allowing full control of the operating system.
Trusted Application Abuse	Exploitation of legitimate software to perform malicious actions.
Update Mechanism	The process used by software to automatically download and install updates, which may be hijacked by attackers.
Use-After-Free	A memory flaw where freed memory is reused incorrectly, enabling exploitation.
Webex	A collaboration service affected by identity and authentication vulnerabilities.
WMI (Windows Management Instrumentation)	A Windows management framework abused to establish stealthy, long-term persistence.
Zero-Day Vulnerability	A flaw actively exploited before vendors or defenders have widely deployed fixes.