TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	21/5/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 21 May 2026

7	7	0	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Financial Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the Middle East impacting Financial Sector

Summary

This week's cybersecurity newsletter highlights a surge in complex intrusion chains and high-impact vulnerabilities spanning mobile, enterprise and blockchain ecosystems. Multi-stage campaigns leveraged trusted platforms and tooling ranging from Android "device take over" malware and developer surveillance RATs to collaboration-platform social engineering while several espionage operations relied on stealthy execution methods like signed-binary abuse and DLL sideloading. From a financial sector perspective, these developments may impact identity assurance, transaction integrity, and service availability especially where remote access tools, cross-chain dependencies, and internet-facing infrastructure are in play. Prioritize rapid patching of critical and high-severity products called out this week (network edge, identity/authentication components, and widely deployed enterprise software), and strengthen monitoring for living-off-the-land execution patterns, credential theft, and abnormal remote-control behaviour across endpoints and cloud services.

ADGM THREAT INTELLIGENCE SUMMARY

New TrickMo Variant: Device Take Over Malware Targeting Banking, Fintech, Wallet & Auth apps [Campaign] [High]

Seedworm Espionage Campaign Uses Signed Binaries and Node.js to Hide Intrusions [Campaign] [High]

APT Campaign Targets Entities with Updated FDMTP Backdoor [Campaign] [High]

Multi-Stage EtherRAT and TukTuk Activity Leads to The Gentlemen Ransomware [Campaign] [Medium]

ModeloRAT Campaign Abuses Microsoft Teams to Capture Domain Credential [Campaign] [Medium]

Lazarus Group 'OtterCookie' Malware Expands Developer Surveillance Operations [Campaign] [Medium]

Gremlin Stealer Hides Payloads in .NET Resources to Evade Analysis and Steal Browser and Wallet Data [Campaign] [Medium]

Cisco SD-WAN Auth Bypass Under Active Exploitation [Vulnerability] High]

Microsoft May 2026 Patch Tuesday Fixes 137 Vulnerabilities [Vulnerability] [High]

SAP May 2026 Patches Fix Critical S/4HANA and Commerce Cloud Flaws [Vulnerability] [High]

Fortinet Addresses Critical and High Severity Flaws in FortiOS and FortiSandbox Products [Vulnerability] [High]

Zoom Patches High-Severity Windows Privilege Escalation Flaws [Vulnerability] [High]

Palo Alto PAN-OS High-Severity Flaws Enable Unauthenticated RCE, Auth Bypass, and DoS [Vulnerability] [High]

F5 NGINX Heap Overflow in Rewrite Module Under Active Exploitation [Vulnerability] [High]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
New TrickMo Variant: Device Take Over Malware Targeting Banking, Fintech, Wallet & Auth apps	HIGH	CLEAR	Campaign	Open Source

Executive Summary

TrickMo is distributed via social-media TikTok-themed lures that push a malicious Android dropper, which installs a fake "Google Play Services" host and downloads a runtime module. It then tricks users into enabling Accessibility, enabling full device takeover (overlay phishing, keylogging, screen streaming/remote control) and OTP interception/suppression to commit banking/wallet fraud. The operation is hardened by routing C2 over TON (The Open Network) and adding SSH/SOCKS5 (Socket Secure 5) tunneling to use infected devices as network pivots/exit nodes.

This campaign could affect financial services by supporting real-time account interaction including overlay-based credential capture and OTP notification suppression and by adding tunnelling/proxy options that may help traffic appear to originate from a victim's own environment, organizations in the financial sector should be aware of these capabilities when monitoring mobile fraud and anomalous access patterns.

Technical Details

- According to researchers, the malware is hitting banking and wallet users in France, Italy, and Austria through different campaigns, and it looks like it's replacing previous TrickMo activity.
- The new build is described as a platform overhaul aimed at improved stealth, resilience, and operator reach, rather than a complete rewrite of user-facing capabilities.
- The host APK (Android Package Kit) primarily provides launch/persistence behavior, while a separately downloaded "dex[.]module" is injected at runtime to enable the main malicious functions.
- The infection relies on coercing Accessibility Service permission, which enables "Device Take Over" through accessibility-driven automation and control.
- Credential theft is supported via Fullscreen WebView overlays that imitate legitimate apps, along with keylogging of typed text and related field metadata.
- Operators can stream/record the screen and remotely control the device by replaying gestures and inputs through the Accessibility channel.
- The malware intercepts SMS and notifications, including the ability to silently suppress one-time-password push notifications.
- A major architectural change is the migration of primary C2 to The Open Network (TON), using ADNL (Abstract Datagram Network Layer) endpoints routed through an embedded local TON proxy.
- The new variant adds network-focused commands (recon probes and reachability checks) plus SSH tunnelling and authenticated SOCKS5 proxying to turn devices into pivots/traffic-exit nodes.

Recommendations

- Monitor for newly granted Accessibility Service permissions and investigate apps that aggressively prompt for accessibility enablement.

- Detect and triage signs of overlay phishing and keylogging-like behavior affecting sensitive financial applications on Android devices.
- Hunt for mobile behaviors consistent with DTO remote control, such as unexpected screen streaming/recording and automation-like navigation sequences.
- Monitor for anomalous TON proxy usage and unexpected SSH/SOCKS tunnelling activity from mobile endpoints as potential indicators of device-based pivoting.
- Incorporate review steps for campaigns that distribute Android lures via social platforms, aligning investigations with the report's observed campaign patterns.

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 Espionage Campaign Uses Signed Binaries and Node.js to Hide Intrusions	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers have identified a Seedworm espionage campaign that hit at least nine organizations across multiple countries and sectors. Although the initial access method is unclear, Seedworm post-compromise ran a "Node[.]js" driven loader that invoked PowerShell to perform reconnaissance and fetch additional payloads. The attacker then used DLL sideloading by pairing legit, signed binaries with malicious DLLs to run malware under trusted processes and evade detection. They also set persistence via "HKCU\...\Run" and exfiltrated data through the public file-transfer service to blend with normal traffic.

This campaign may impact organizations in the financial sector because the operators used stealth-focused execution (signed binaries), credential theft, and proxy/tunnelling tradecraft that may enable deeper access and harder-to-trace activity; financial services teams should be aware of these patterns when investigating suspicious "legitimate" processes and script-driven environment enumeration.

Technical Details

- The activity set is attributed to Seedworm (also tracked as MuddyWater) and was assessed as a global espionage campaign spanning at least nine victims across four continents.
- In one of the cases, the first observed actions were PowerShell-based discovery commands to profile the host, user context, and domain environment.
- The early process tree showed "node[.]exe" as an ancestor for command execution, indicating automation via a "Node[.]js" loader rather than purely hands-on activity.
- The operators used WMI to enumerate installed antivirus tooling, likely to understand and avoid defensive controls before deploying more tooling.
- A "Node[.]js" driven chain pulled additional scripts, including reconnaissance and screenshot collection, consistent with confirming user activity and environment.

- The campaign relied heavily on DLL sideloading, pairing validly signed third-party executables with malicious DLLs to blend in as benign software.
- The report states the malicious DLLs contained ChromElevator, a publicly available tool used for stealing data from Chromium-based browsers.
- Persistence was established using a standard user Run-key mechanism to re-launch the sideloading chain when the user logged in.
- Credential access included registry hive theft (SAM/SECURITY/SYSTEM) and additional credential-harvesting attempts, alongside a privilege-escalation step to reach higher access.
- Data exfiltration was performed via a public file-transfer service, reflecting an effort to blend theft with legitimate-looking outbound traffic.

Recommendations

- Alert on signed-but-unexpected executables loading adjacent DLLs from user-writable or newly created staging directories, especially when followed by scripted discovery.
- Hunt for node.exe spawning command shells or PowerShell in enterprise endpoints, particularly when it precedes screenshot capture or repeated discovery loops.
- Monitor for registry hive export activity and other credential-access attempts that indicate rapid escalation and preparation for lateral movement.
- Detect persistence via user Run-key additions that point to uncommon binaries or recently staged paths tied to sideloading execution.
- Review outbound transfers to public file-transfer services from endpoints with concurrent discovery/credential activity, as this may indicate data staging and exfiltration.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Seedworm Espionage Campaign Uses Signed Binaries and Node.js to Hide Intrusions

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
APT Campaign Targets Entities with Updated FDMTP Backdoor	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a campaign, aligning with Twill Typhoon tradecraft, where affected hosts contacted Content Delivery Network (CDN) impersonating infrastructure (Yahoo, Apple etc.) and then downloaded a legitimate executable plus a matching config file and a malicious DLL to run the backdoor inside a trusted process. The sideloaded code loads a modular, obfuscated (.NET) remote-access framework that registers to C2 via a cluster-style bootstrap before entering persistent remote tasking.

This campaign could affect organizations in the financial sector as Darktrace observed finance-sector activity within the same pattern, and the backdoor's modular design, persistence mechanisms, and remote tasking

may enable stealthy access and ongoing control. Organizations in the financial sector should be aware of the behavioral sequence rather than relying on static indicators.

Technical Details

- Darktrace observed the activity with multiple affected hosts making HTTP requests to infrastructure masquerading as CDN endpoints for well-known platforms.
- Across cases, the intrusion chain followed a consistent order: legitimate executable download, matching (.config) retrieval, then a malicious DLL, followed by repeated DLL downloads and C2 traffic.
- The technique relies on search-order hijacking: the legitimate process loads a same-named DLL from its directory, allowing the malicious DLL to run inside a trusted executable.
- A representative archive contained a legitimate executable alongside a malicious DLL named to match an expected library, enabling sideloaded execution when the program calls LoadLibrary-style APIs.
- The loader decrypts embedded strings (XOR noted in the analysis), dynamically loads the (.NET) runtime, and executes managed code in memory by loading (.NET) assemblies.
- For C2 setup, the malware performs a "cluster" registration request (GetCluster-style), using a verification token and receiving compressed/encoded addressing for follow-on communications.
- Recently, Darktrace observed a finance-sector endpoint repeatedly fetching legitimate binaries and associated config/DLL components over an extended window to maintain the chain.
- The campaign abused legitimate .NET-related binaries and configuration to force loading of a malicious DLL via a custom AppDomainManager, with analysis noting logging suppression.
- Persistence was achieved via scheduled-task creation and registry-based plugin persistence, including storage under user registry paths associated with IME-related keys.
- The core payload is described as a heavily obfuscated backdoor using custom TCP with DMTP, assessed as an updated FDMTP version, supporting structured remote tasking in a loop.

Recommendations

- Alert on the behavioral sequence of legitimate executable + matching config + newly dropped DLL, especially when followed by repeated DLL retrieval and outbound C2 setup.
- Investigate endpoints reaching CDN-lookalike infrastructure shortly before loading unexpected DLLs within legitimate processes, as this pattern was central to the campaign.
- Detect and triage DLL sideloading/search-order hijacking where signed or expected executables load same-directory DLLs that were recently created or downloaded.
- Monitor for suspicious scheduled task creation and unusual registry writes that resemble plugin persistence described in the report.
- Prioritize detections anchored to behavioral chains (staged payload delivery and repeated component refresh) to remain resilient to infrastructure rotation.

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-Stage EtherRAT and TukTuk Activity Leads to The Gentlemen Ransomware	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers observed an intrusion where a user executed a malicious MSI (Microsoft Installer) masquerading as a Sysinternals RAMMap installer, which will deploy a Windows EtherRAT variant and then pulled a portable Node.js runtime to run obfuscated JavaScript. The malware established persistence via a registry Run key and used an Ethereum "EtherHiding" approach to fetch and later update its C2 configuration dynamically.

This campaign could affect organizations in the financial sector because the actor combined SaaS-based C2, remote management tooling, and cloud data exfiltration before deploying ransomware, which may complicate traditional network-based detection and response; organizations in the financial sector should be aware of multi-stage activity that blends into common third-party services and administrative workflows.

Technical Details

- Initial execution began when a user ran a malicious MSI posing as a legitimate utility, leading to EtherRAT installation on Windows.
- After launch, EtherRAT downloaded a portable Node.js runtime and executed obfuscated JavaScript as the primary execution layer.
- Persistence was created through a registry Run key, enabling recurring execution of the Node.js-driven chain.
- EtherRAT queried an Ethereum-hosted configuration (via an RPC access path) to obtain C2 settings; initially, active C2 was not available.
- The actor later updated the blockchain-hosted configuration to point the implant to new tunneling-based infrastructure and pushed decoy endpoints to complicate analysis.
- Once active C2 was established, the intrusion shifted to host and domain discovery, including system profiling, AV enumeration, and LDAP-based user activity checks.
- Additional payloads were downloaded from cloud storage, culminating in deployment of the TukTuk framework disguised as legitimate software and launched via DLL sideloading.
- TukTuk established primary C2 through SaaS platforms and maintained fallback options (including other SaaS and direct HTTP-style channels), increasing resiliency.
- Post-compromise activity included hands-on-keyboard actions, Kerberoasting, credential discovery, and broader credential dumping (including LSASS/NTDS-related activity).
- The actor used compromised service account credentials to deploy remote management tooling laterally, exfiltrated data with Rclone to cloud storage, then deployed "The Gentlemen" ransomware via domain-wide GPO/scheduled task execution after disabling defenses and clearing artifacts.

Recommendations

- Monitor for msiexec executions from user download/desktop paths that spawn unexpected child processes, especially when followed by script or archive staging.
- Alert on endpoints downloading and launching portable runtimes (e.g., Node.js) that then run obfuscated scripts, and investigate associated persistence via registry Run keys.
- Review outbound traffic for unusual use of blockchain/Web3 configuration retrieval, public tunneling, or unexpected SaaS access from hosts that do not normally require them.
- Maintain an approved inventory of remote management tools and alert on unapproved installations or lateral deployment behavior across servers and domain controllers.
- Hunt for Rclone execution and large outbound transfers to cloud storage, and closely monitor GPO changes and scheduled-task creation used to execute payloads broadly.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Multi-Stage EtherRAT and TukTuk Activity Leads to The Gentlemen Ransomware

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
ModeloRAT Campaign Abuses Microsoft Teams to Capture Domain Credential	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers investigated a recent intrusion begins with abuse of Microsoft Teams external access, where the attacker posed as “IT Support” and contacted a user, shortly after the interaction, a hidden PowerShell command ran on the endpoint to stage the initial payload, which downloaded a Dropbox-hosted ZIP containing a portable WinPython environment and then launched ModeloRAT-linked Python scripts to establish C2.

This activity may impact organizations in the financial sector by enabling rapid escalation from a single user interaction into remote access, SYSTEM privilege escalation, and domain-credential harvesting. Organizations in the financial sector should be aware of this collaboration-led entry path and the quick shift into identity-focused compromise.

Technical Details

- The intrusion started with an external Teams chat impersonating IT support, leveraging Teams external access to reach a targeted employee. Soon after the interaction, a hidden PowerShell command executed to stage the initial payload on the endpoint.
- The PowerShell stager downloaded a ZIP from a cloud file-hosting service into the user profile, extracted it, and deleted the archive to reduce on-disk artifacts. The extracted content included a portable WinPython environment used to run the next-stage scripts in the background via “pythonw[.]exe”.

- The first Python module (collector) performed host fingerprinting and system profiling, then saved reconnaissance results locally for later operator use. Rapid7 noted this reconnaissance relied on native discovery commands executed through hidden PowerShell sessions to avoid visible windows.
- The second Python module (Pmanager) established HTTP beaconing and provided remote tasking, including the ability to run PowerShell, launch additional Python scripts, and install packages. It also handled persistence and could update or remove itself as part of the operator workflow.
- The attacker deployed additional access modules, including a TCP reverse shell, to maintain interactive control beyond the initial beaconing. This access was used to attempt credential reuse testing via WebDAV authentication attempts against internal systems.
- A separate HTTP-based backdoor "internal[.]py" created a persistent PowerShell session, repeatedly polling for commands, executing them, and returning output to the operator. The same channel supported file operations and screenshot capture, blending activity into common web traffic patterns.
- Privilege escalation to SYSTEM was achieved via exploitation of CVE-2023-36036, after which tooling was relaunched under elevated context. The attacker then added scheduled-task persistence to repeatedly execute the backdoor with SYSTEM privileges.
- The operator deployed a fake Windows lock screen designed to trick the user into entering their password, capturing the domain credential to disk. With valid credentials obtained, the intrusion shifted into Active Directory discovery and remote access activity involving additional hosts.

Recommendations

- Restrict and monitor Teams external access and investigate unexpected external chats claiming to be internal support.
- Alert on hidden PowerShell that downloads archives, extracts them into user-writable paths, and launches portable runtimes such as Python via background execution.
- Detect suspicious Python/PowerShell persistence, especially scheduled tasks created to run script engines or long-lived hidden PowerShell sessions.
- Prioritize patching for CVE-2023-36036 and investigate privilege changes tied to unusual DLL execution patterns used to launch payloads.
- Monitor for WebDAV-based authentication testing and lock-screen impersonation behavior consistent with credential harvesting.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – ModeloRAT Campaign Abuses Microsoft Teams to Capture Domain Credential

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
Lazarus Group 'OtterCookie' Malware Expands Developer Surveillance Operations	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified OtterCookie as a separate JavaScript/Node[.]js RAT operating alongside BeaverTail within the Lazarus-attributed "Contagious Interview" ecosystem, expanding intrusion outcomes from stored-data theft into ongoing monitoring of active developer workstations. The report describes delivery reach supported via a npm and Vercel layer, with the implant connecting to a "Socket[.]IO" control plane that maintains live session state rather than one-off HTTP collection.

This campaign may impact organizations in the financial sector particularly those with fintech, virtual-asset, or blockchain exposure because OtterCookie's continuous collection focuses on developer secrets and wallet-related artifacts, and it monitors live activity such as clipboard and screen content, rather than only what was already saved on disk.

Technical Details

- OtterCookie is described as its own JavaScript/Node.js RAT (not a BeaverTail variant) within the same operation, with different roles across BeaverTail, OtterCookie, and InvisibleFerret.
- Command-and-control uses Socket.IO over "Engine[.]IO" v4, enabling persistent sessions and server-side awareness of connected victims.
- The C2 maintains a live roster of connected machines and broadcasts that roster on a fixed cadence (observed as a 30-second clock in the report).
- Red Asgard's analysis indicates the victim-facing channel behaved as one-way command dispatch (server-to-client), with extensive client-side event testing yielding no command execution from that side.
- Collection is continuous and oriented to "live activity capture," including clipboard monitoring, system-wide keystroke capture, and recurring screenshots (including multi-monitor).
- The implant targets browser data (credentials/cookies), wallet artifacts (including browser-extension wallet material), and developer secrets such as (.env) files, SSH material, cloud credentials, and source-control tokens.
- Identifier-like protocol fields (uid and userKey) were observed colliding across distinct victims, leading the authors to assess they represent deployment batch labels rather than unique hardware fingerprints.
- The roster broadcast cadence varied across related nodes (e.g., up to ~120 seconds elsewhere), which the report describes as a server-side configuration choice.
- Red Asgard notes npm and Vercel delivery broadened reach and frames the operational shift as moving from "victim archives" to an ongoing "victim feed".

Recommendations

- Review developer endpoint monitoring to detect continuous surveillance behaviors such as repeated screenshotting, keystroke capture patterns, and persistent clipboard monitoring consistent with the report's collection profile.
- Strengthen controls around developer secrets storage and access (e.g., tighter handling of .env files, SSH material, cloud credentials, and source-control tokens) in line with the targeted data types described.
- Increase scrutiny of "Node[.]js" based tooling on developer workstations and investigate unexpected Socket.IO-style persistent connections that resemble the described control plane behavior.

- Apply stricter governance for software acquisition paths used by developers, focusing on risk from npm-delivered components and related delivery layers referenced in the report.
- Incorporate behavior-based detections that look for a transition from initial stored-data theft to ongoing "live surveillance" activity, reflecting the operational shift highlighted by the authors.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Lazarus Group 'OtterCookie' Malware Expands Developer Surveillance 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
Gremlin Stealer Hides Payloads in .NET Resources to Evade Analysis and Steal Browser and Wallet Data	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Unit 42 analyzed a new Gremlin stealer variant that conceals its malicious payload inside the (.NET) Resource section using XOR encoding, and in some cases adds a sophisticated commercial packing layer with instruction virtualization to hinder static analysis. The malware targets browsers, the system clipboard, and local storage to steal sensitive data and then packages the harvest for exfiltration.

This activity may impact organizations in the financial sector because the stealer explicitly targets payment card details, session tokens, cryptocurrency wallet data, and credentials (e.g., FTP/VPN), and also adds "active financial interference" via clipboard manipulation of cryptocurrency addresses; organizations in the financial sector should be aware of the shift toward stealthier collection and real-time fraud-enabling behaviors.

Technical Details

- Unit 42 identified a new Gremlin stealer variant and noted it exfiltrates stolen data to attacker-controlled infrastructure, with a workflow that prepares data for potential publication or sale.
- After stealing data, the malware bundles collected artifacts into a ZIP archive including browser cookies, session tokens, clipboard contents, wallet data, and FTP/VPN credentials and uploads the archive to attacker-controlled infrastructure.
- The latest iteration increases stealth by moving the malicious payload into the (.NET) Resource section and masking it with XOR encoding to evade signature and heuristic scanning.
- Unit 42 recovered plaintext configuration by applying a single-byte XOR routine, which revealed hard-coded C2 URLs and exfiltration paths embedded in the resource data.
- Compared to older samples that exposed symbols and exports, the newer version uses staged loading, decrypting and mapping functions into memory from resources only when needed.

- The analysis describes architectural upgrades that broaden targeting, including a dedicated Discord token extraction module aimed at digital identity and social-engineering value.
- The "crypto clipper" feature continuously monitors clipboard content for cryptocurrency wallet patterns and replaces matching addresses in real time to divert funds.
- A WebSocket-based session hijacking module is described as a major upgrade, enabling theft from live browser sessions by requesting data directly from the running browser process.
- One examined sample was packed with a commercial utility using instruction virtualization, converting code into custom bytecode executed by a private VM to resist analysis.
- The report highlights layered obfuscation: identifier renaming ("no-labels"), resource-backed string decryption, and control-flow obfuscation to disrupt decompilation and triage.

Recommendations

- Hunt for suspicious (.NET) applications that heavily use embedded resource blobs with simple decode routines (e.g., XOR) before network communication.
- Monitor for endpoint behaviors consistent with collection and staging, such as rapid aggregation of browser cookies/session tokens/clipboard data followed by ZIP creation and upload activity.
- Detect clipboard-monitoring patterns and investigate processes that appear to replace cryptocurrency wallet strings during user transactions.
- Watch for signs of live session hijacking where processes request sensitive data directly from running browser processes using memory-resident techniques.
- Prioritize triage of binaries exhibiting commercial packer virtualization and multi-layer obfuscation, as Unit 42 observed this approach in newer Gremlin builds.

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
Cisco SD-WAN Auth Bypass Under Active Exploitation	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Cisco has disclosed a critical authentication bypass vulnerability (CVE-2026-20182, CVSS 10.0) affecting Cisco Catalyst SD-WAN Controller and SD-WAN Manager platforms, where flaws in peering authentication and control-connection handshaking can be abused over the network to bypass authentication. Successful exploitation enables an unauthenticated remote attacker to establish unauthorized peer relationships and obtain administrative-level access to impacted SD-WAN components.

This activity may impact organizations in the financial sector because exploited internet-exposed SD-WAN deployments could allow attackers to manipulate SD-WAN fabric configurations, deploy persistence, and maintain long-term access within enterprise environments; organizations in the financial sector should be aware of the confirmed in-the-wild exploitation and treat remediation as an urgent priority.

Technical Details

- CVE-2026-20182 is a critical, network-reachable authentication bypass in Cisco Catalyst SD-WAN, scored 10.0 (CVSS v3.1) and mapped to CWE-287 (Improper Authentication).
- The vulnerability affects peering authentication and control connection handshaking, allowing bypass of validation checks and unauthorized establishment of peer connections.
- Exploitation requires no privileges and no user interaction, enabling unauthenticated remote compromise when the target is reachable over the network.
- Impacted components include Cisco Catalyst SD-WAN Controller and SD-WAN Manager (vManage), as well as vSmart and vBond.
- Cisco Talos has confirmed active exploitation targeting internet-exposed SD-WAN deployments in the wild.
- Reported post-exploitation objectives include administrative-level access, NETCONF service access, and manipulation of SD-WAN fabric configurations.
- Observed threat activity includes rogue peer registration, persistence establishment, and webshell deployment as part of maintaining access.
- Exposed services noted in attack activity include DTLS services and UDP port for vdaemon, aligning with SD-WAN control-plane exposure.
- The issue affects multiple deployment types, including on-prem, Cloud-Pro, Cisco-managed cloud, and government/FedRAMP variants.

Recommendations

- Identify all Cisco SD-WAN assets (Controller/Manager/vSmart/vBond) and prioritize systems reachable from the internet.
- Upgrade vulnerable systems to the listed fixed releases or migrate to a fixed release if running earlier than 20.9.
- Restrict external exposure of SD-WAN management and control-plane interfaces and disable unnecessary public access paths.
- If compromise is suspected, open a Severity 3 TAC case and reference CVE-2026-20182 as Cisco recommends.

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

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft May 2026 Patch Tuesday Fixes 137 Vulnerabilities	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Microsoft has published its May 2026 Security Updates addressing 137 flaws across Azure, Windows, SharePoint, Dynamics 365, Azure DevOps, Hyper-V, and other enterprise cloud services. Successful exploitation of the addressed issues could enable remote code execution, elevation of privilege, spoofing, information disclosure, or broader compromise in enterprise environments.

This update set may impact organizations in the financial sector because many affected products commonly support identity, collaboration, cloud operations, and core Windows infrastructure. Organizations in the financial sector should be aware that delayed patching could increase exposure to vulnerabilities that enable high-impact outcomes such as RCE or privilege escalation across critical business services.

Technical Details

- Microsoft's May 2026 release addresses 137 vulnerabilities spanning Azure, Windows, SharePoint, Dynamics 365, Azure DevOps, Hyper-V, and enterprise cloud services.
- The update includes multiple critical vulnerabilities across cloud and on-prem workloads, with impact types including RCE, elevation of privilege, spoofing, and information disclosure.
- Critical items listed include Azure DevOps information disclosure (CVE-2026-42826) and Microsoft Team Events Portal information disclosure (CVE-2026-33823).
- Multiple Azure-focused critical issues are included, such as Apache Cassandra Managed Instance RCE (CVE-2026-33109, CVE-2026-33844) and Azure Logic Apps elevation of privilege (CVE-2026-42823).
- Identity and access-related items include Azure Cloud Shell spoofing (CVE-2026-35428) and Microsoft Enterprise Security Token Service spoofing (CVE-2026-40379).
- Windows infrastructure critical issues include Windows Netlogon RCE (CVE-2026-41089) and Windows DNS Client RCE (CVE-2026-41096).
- Virtualization impact is noted through Windows Hyper-V elevation of privilege (CVE-2026-40402).
- Business application risk is highlighted by Dynamics 365 On-Premises RCE (CVE-2026-42898, CVE-2026-42833).
- Other notable vulnerabilities include Windows GDI RCE (CVE-2026-35421).
- SharePoint is called out with multiple RCE vulnerabilities, including CVE-2026-33110, CVE-2026-33112, CVE-2026-35439, CVE-2026-40357, and CVE-2026-40365.

Recommendations

- Apply Microsoft's May 2026 security updates as a priority across impacted enterprise and cloud environments.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
SAP May 2026 Patches Fix Critical S/4HANA and Commerce Cloud Flaws	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

SAP has released its May 2026 security updates to address multiple vulnerabilities across SAP products, including critical flaws in SAP S/4HANA (Enterprise Search for ABAP) and SAP Commerce Cloud configuration. The issues span attack paths such as SQL injection, missing authentication/authorization checks, OS command injection, code injection, and cross-site scripting, which could be triggered by attackers to gain unauthorized access or execute malicious actions.

These vulnerabilities may impact organizations in the financial sector because SAP platforms often support core business and financial workflows, and exploitation could affect confidentiality and integrity of enterprise data or configurations. Organizations in the financial sector should be aware that unpatched instances may face increased risk of unauthorized access, privilege escalation, service disruption, or broader compromise across affected SAP environments.

Technical Details

- SAP reported two critical (CVSS 9.6) issues: CVE-2026-34260 (SQL injection) in SAP S/4HANA – Enterprise Search for ABAP and CVE-2026-34263 (missing authentication check) in SAP Commerce Cloud configuration.
- The SQL injection flaw may allow attackers to inject malicious queries, potentially enabling unauthorized data access or manipulation within impacted S/4HANA search functionality.
- The missing authentication flaw may allow unauthorized access to Commerce Cloud configuration, enabling configuration manipulation without proper checks.
- A high severity issue, CVE-2026-34259 (CVSS 8.2), is an OS command injection vulnerability in SAP Forecasting & Replenishment, enabling execution of arbitrary commands if exploited.
- Medium severity issues include CVE-2026-40135 (OS command injection) in SAP NetWeaver AS for ABAP/ABAP Platform and multiple missing authorization checks in SAP components.
- Web-layer risks include XSS (e.g., CVE-2026-40137, CVE-2026-27682) and CSRF (CVE-2026-0502) affecting specified SAP applications and platforms.
- Additional medium issues include code injection (CVE-2026-40129), content spoofing (CVE-2026-34258), and DoS (CVE-2026-40136) in listed SAP products.
- A low severity issue, CVE-2026-40131 (CVSS 3.4), is a SQL injection vulnerability in SAP HANA Deployment Infrastructure (HDI) Deploy Library.
- SAP notes successful exploitation could lead to arbitrary command execution, code injection, authentication/authorization bypass, sensitive data access, system compromise, or service disruption across affected environments.

Recommendations

- Apply SAP's May 2026 security updates promptly across all affected SAP products and landscapes.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Fortinet Addresses Critical and High Severity Flaws in FortiOS and FortiSandbox Products	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Fortinet has disclosed multiple critical and high-severity vulnerabilities affecting FortiOS, FortiAuthenticator, and FortiSandbox, where weaknesses in wireless controller services, API endpoints, and web UI authorization mechanisms could allow code or command execution. The issues include an out-of-bounds write in FortiOS CAPWAP handling and unauthorized code/command execution paths in FortiAuthenticator and FortiSandbox via crafted requests.

This vulnerability set may impact organizations in the financial sector because these products are commonly deployed at security and authentication boundaries, and exploitation could affect perimeter controls or analysis environments. Organizations in the financial sector should be aware that internet-facing FortiAuthenticator and FortiSandbox deployments are explicitly called out for prioritization, and rapid remediation can reduce exposure.

Technical Details

- FortiOS includes CVE-2025-53844 (FG-IR-26-123, CVSS 8.3), an out-of-bounds write (CWE-787) in the CAPWAP daemon that may allow execution privileges on a FortiGate device.
- Exploitation of CVE-2025-53844 requires an attacker controlling an authenticated FortiAP, FortiExtender, or FortiSwitch to target the FortiGate CAPWAP process.
- Affected FortiOS versions include 7.6.0–7.6.3, 7.4.0–7.4.8, and 7.2.0–7.2.11, with fixes in 7.6.4+, 7.4.9+, and 7.2.12+ respectively.
- FortiAuthenticator is affected with CVE-2026-44277 (FG-IR-26-128, CVSS 9.1), an improper access control issue (CWE-284) enabling unauthenticated unauthorized code or command execution via crafted requests.
- Affected FortiAuthenticator versions include 8.0.0 and 8.0.2 (fix: 8.0.3+), 6.6.0–6.6.8 (fix: 6.6.9+), and 6.5.0–6.5.6 (fix: 6.5.7+).
- FortiSandbox includes CVE-2026-26083 (FG-IR-26-136, CVSS 9.1), a missing authorization issue (CWE-862) in the web UI allowing unauthenticated unauthorized code or command execution via HTTP requests.
- Affected FortiSandbox versions include 5.0.0–5.0.1 (fix: 5.0.2+) and 4.4.0–4.4.8 (fix: 4.4.9+), with additional impact across FortiSandbox Cloud and FortiSandbox PaaS versions requiring migration to fixed releases where specified.

Recommendations

- Upgrade FortiOS to 7.6.4+, 7.4.9+, or 7.2.12+ (as applicable) and prioritize FortiAuthenticator/FortiSandbox upgrades to their stated fixed releases.
- Prioritize remediation for internet facing FortiAuthenticator and FortiSandbox deployments and reduce public exposure of management interfaces.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Zoom Patches High-Severity Windows Privilege Escalation Flaws	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Zoom has disclosed two high-severity local privilege escalation vulnerabilities affecting Windows-based Zoom products: Zoom Rooms for Windows and the Zoom Workplace VDI Plugin for Windows installers. The issues (CVE-2026-30906 and CVE-2026-30905) involve Windows path handling weaknesses that could allow a locally authenticated user with low privileges to escalate privileges during installation-related activity.

This update may impact organizations in the financial sector because Zoom Rooms and VDI plugin deployments are often present on enterprise-managed Windows endpoints and meeting room systems, and local privilege escalation could affect device integrity and administrative control. Organizations in the financial sector should be aware of these installer-focused weaknesses and prioritize upgrading affected Zoom components to reduce exposure in managed environments.

Technical Details

- CVE-2026-30906 (ZSB-26008) is a high-severity privilege escalation issue in Zoom Rooms for Windows with CVSS v3.1 score 7.8 and a local attack vector.
- The vulnerability type for CVE-2026-30906 is Untrusted Search Path, impacting all versions prior to 7.0.0 of Zoom Rooms for Windows.
- CVE-2026-30905 (ZSB-26007) is a high-severity privilege escalation issue in the Zoom Workplace VDI Plugin for Windows with CVSS v3.1 score 7.8 and a local attack vector.
- The vulnerability type for CVE-2026-30905 is External Control of File Name or Path, affecting installer builds 6.6.10 and earlier.
- Both issues are described as local privilege escalation vulnerabilities, indicating the attacker needs local access and some level of privileges but no user interaction per the provided vectors.

Recommendations

- Upgrade Zoom Rooms for Windows to 7.0.0 or later across all applicable systems.
- Upgrade Zoom Workplace VDI Plugin for Windows to 6.6.11 or later across all applicable systems.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Palo Alto PAN-OS High-Severity Flaws Enable Unauthenticated RCE, Auth Bypass, and DoS	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Palo Alto Networks has addressed multiple high-severity vulnerabilities in PAN-OS that could be exploited by unauthenticated attackers over the network. The issues include buffer overflows in IKEv2 processing and DNS

proxy/DNS server features, as well as an authentication bypass condition when Cloud Authentication Service (CAS) is enabled, potentially allowing code execution, bypass, or denial of service on affected firewalls.

These vulnerabilities may impact organizations in the financial sector because PAN-OS often sits at critical network boundaries, and exploitation could affect perimeter availability and access controls. Organizations in the financial sector should be aware that internet-facing services and configurations (IKEv2, DNS features, and CAS-enabled environments) may increase exposure and warrant accelerated patching and monitoring.

Technical Details

- CVE-2026-0263 (CVSS 7.2) - A buffer overflow in IKEv2 processing could allow an unauthenticated attacker to execute arbitrary code with elevated privileges or cause a denial of service (DoS).
- CVE-2026-0264 (CVSS 7.2) - A buffer overflow in DNS proxy and DNS Server features could allow an unauthenticated attacker to cause DoS or potentially execute arbitrary code through specially crafted network traffic.
- CVE-2026-0265 (CVSS 7.2) - An authentication bypass vulnerability could allow an unauthenticated attacker to bypass authentication when Cloud Authentication Service (CAS) is enabled.

Recommendations

- Apply currently available PAN-OS security fixes immediately, prioritizing devices exposed to the internet.
- Upgrade to the vendor-listed fixed versions for your branch (12.1.7+/11.2.12+/11.1.15+/10.2.18-h6+ or the specified hotfix releases).

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
F5 NGINX Heap Overflow in Rewrite Module Under Active Exploitation	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

F5 has disclosed CVE-2026-42945, a critical heap buffer overflow in NGINX Open Source and NGINX Plus within the “ngx_http_rewrite_module”, which can be triggered via remote, unauthenticated HTTP requests. The issue may allow attackers to crash NGINX worker processes and, under specific conditions, potentially achieve remote code execution (RCE), and a public PoC is available.

This vulnerability may impact organizations in the financial sector because NGINX is commonly deployed in front of business-critical web services, and active exploitation attempts were observed shortly after public disclosure. Organizations in the financial sector should be aware that internet-facing NGINX instances within the affected version ranges could face increased risk until patches and configuration reviews are completed.

Technical Details

- CVE-2026-42945 is a heap buffer overflow affecting NGINX Open Source and NGINX Plus and is described as being actively exploited in the wild.

- The vulnerable component is “ngx_http_rewrite_module”, indicating exploitation is tied to rewrite-module processing paths.
- The attack vector is remote / unauthenticated HTTP requests, meaning no prior authentication is required to trigger the flaw.
- The reported impact includes worker process crashes, which can result in service instability or denial-of-service conditions.
- Under specific conditions, exploitation may potentially lead to RCE, indicating a higher-impact outcome beyond process disruption.
- Affected NGINX Open-Source versions are 0.6.27 through 1.30.0 and affected NGINX Plus releases are R32 through R36.
- Security researchers observed exploitation attempts soon after disclosure, suggesting rapid threat actor weaponization.

Recommendations

- Apply the latest security updates and patches provided by F5 NGINX
- Fixed versions for NGINX Open Source are 1.31.0 and 1.30.1, addressing the vulnerable code paths.
- Fixed versions for NGINX Plus are R36 P4, R35 P2, and R32 P6, aligning remediation to supported patch trains.

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

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Seedworm Espionage Campaign Uses Signed Binaries and Node.js to Hide Intrusions

Tactics	Techniques	Description
Execution	Command and Scripting Interpreter (PowerShell)	PowerShell scripts used for reconnaissance and post-exploitation tasks.
Execution	Command and Scripting Interpreter (JavaScript)	Node.js-based implant used to orchestrate execution chain.
Defense Evasion	DLL Side-Loading	Legitimate signed executables abused to load malicious libraries stealthily.
Defense Evasion	Masquerading	Use of legitimate and security-related binaries to disguise malicious activity.
Credential Access	Credential Dumping	Extraction of sensitive system credential data including registry hives.
Credential Access	Credentials from Web Browsers	Theft of stored browser credentials and sensitive data.
Collection	Screen Capture	Screenshots captured from compromised systems.
Command and Control	Proxy	Reverse-proxy tunneling used for covert communication.
Exfiltration	Exfiltration Over Web Service	Data exfiltrated through public file-sharing platforms.
Privilege Escalation	Privilege Escalation	Elevation of privileges performed during compromise.

Multi-Stage EtherRAT and TukTuk Activity Leads to The Gentlemen Ransomware

Tactics	Techniques	Description
Initial Access	User Execution	A user manually executed a malicious installer disguised as a legitimate tool
Execution	DLL Sideloading	Trojanized applications loaded malicious components during execution
Persistence	Registry Run Keys	Malware established persistence via user-level startup mechanisms
Command and Control	Dynamic Resolution	Malware retrieved updated control configurations from decentralized infrastructure
Credential Access	Credential Dumping and Kerberos Abuse	The actor harvested credentials and targeted privileged accounts
Lateral Movement	Remote Services	Compromised credentials were used to expand access across the network
Exfiltration	Exfiltration Over Web Services	Sensitive data was transferred to cloud-based storage
Impact	Data Encryption	Ransomware was deployed broadly across the environment

ModeloRAT Campaign Abuses Microsoft Teams to Capture Domain Credential

Tactics	Techniques	Description
Initial Access	Spearphishing via Service	Fake IT Support message delivered through Microsoft Teams to initiate compromise
Initial Access	External Remote Services	Abuse of Teams external access to directly contact internal users
Execution	User Execution	Victim executed a delivered payload enabling malware deployment

Command and Control	Application Layer Protocol	Python payload established command-and-control communications
Persistence	Implant Deployment	Multiple backdoors deployed within the environment
Privilege Escalation	Exploitation for Privilege Escalation	Exploited a vulnerability to gain SYSTEM-level privileges
Credential Access	Input Capture	Fake Windows lock screen used to harvest domain credentials
Credential Access	Valid Accounts	Stolen credentials enabled further access and escalation
Discovery	System and Network Discovery	Internal environment mapping performed after initial compromise
Lateral Movement	Remote Services	Movement from initial compromised endpoint to another host
Collection	Data from Local System	System memory collected using legitimate tools
Exfiltration	Exfiltration Over External Services	Data likely exfiltrated through an anonymous file-sharing service

Lazarus Group 'OtterCookie' Malware Expands Developer Surveillance Operations

Tactics	Techniques	Description
Initial Access	Supply Chain Compromise	Malware delivered via package ecosystems and developer tooling
Execution	Command and Scripting Interpreter	Use of JavaScript/Node.js execution environment
Persistence	External Remote Services	Persistent Socket.IO connections maintained with C2
Command and Control	Web Protocols	Use of Engine.IO/Socket.IO for communication
Command and Control	Application Layer Protocol	Continuous communication and broadcast of victim status
Collection	Input Capture	Keylogging and clipboard monitoring
Collection	Screen Capture	Continuous screenshot capture from infected hosts
Credential Access	Credentials from Web Browsers	Extraction of browser secrets and stored credentials
Discovery	System Information Discovery	Monitoring active developer workstation activity

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
.adnl	TON addressing namespace referenced for TrickMo C2 endpoints inside the TON overlay.
APT	Advanced Persistent Threat: A highly resourced adversary group that maintains long-term access for espionage or strategic objectives.
Asgard vaults	THORChain vault mechanism referenced as the target area in the reported exploit activity.
Authentication bypass	A flaw or technique allowing access without valid credentials by skipping or defeating authentication checks.
Authorization	Access control decision-making that determines what an authenticated user/system is allowed to do.
C2	Command and Control: Infrastructure/channel used by attackers to manage compromised systems and issue instructions.
CAPWAP	Control and Provisioning of Wireless Access Points: Protocol area referenced in FortiOS CAPWAP daemon vulnerability context (per the newsletter entry).
CAS	Cloud Authentication Service: A feature referenced in PAN-OS where an authentication bypass issue applies when enabled (per the newsletter entry).
Clipboard hijacking / “crypto clipper”	Malware behavior that monitors clipboard content and replaces copied cryptocurrency addresses to divert funds.
Cloud Shell	A cloud-hosted shell environment referenced as affected by a spoofing vulnerability in the Microsoft Patch Tuesday entry.
CSC	UAE Cyber Security Counsil
CVE	Common Vulnerabilities and Exposures: Standard identifier for publicly tracked software vulnerabilities (e.g., CVE-2026-6722).
CVSS	Common Vulnerability Scoring System: Numerical severity scoring used to communicate vulnerability impact and exploitability.
CWE	Common Weakness Enumeration: Category label describing the underlying weakness type (e.g., improper authentication).
DeFi	Decentralized Finance: Digital-asset ecosystem term used in the THORChain breach reporting context.
DEX / “dex.module”	Android DEX module concept used in the described TrickMo modular loading approach (“dex.module”).
DLL	Dynamic Link Library: Windows library file type often abused via sideloading to execute malicious code in a legitimate process.

DLL sideloading	Technique where a legitimate executable loads a malicious DLL placed alongside it, enabling stealthy execution.
DMTP / FDMTP	Duplex Message Transport Protocol reference used in the described modular .NET backdoor communications and “updated FDMTP” framing.
DNS proxy / DNS Server (feature)	PAN-OS DNS-related features referenced as affected by a buffer overflow vulnerability (per the newsletter entry).
DNS-over-HTTPS (DoH)	DNS lookups performed over HTTPS to reduce visibility/control by local resolvers; noted in the TrickMo variant behavior.
DoS	Denial of Service: An outcome where a system/service is disrupted or made unavailable.
DTLS	Datagram Transport Layer Security: Service exposure referenced in SD-WAN attack observations (per the newsletter entry).
DTO	Device Take Over: Malware-enabled remote control of a victim device, referenced for Android banking malware behavior.
Endpoint	A user or server system (e.g., workstation, meeting room device) that can be targeted for compromise.
Engine.IO / Socket.IO	Web communication frameworks used as the control plane for certain malware C2 channels, enabling persistent connections.
EoP	Elevation of Privilege: An attack outcome where an attacker gains higher privileges than initially available.
ESTS	Enterprise Security Token Service: Microsoft identity service referenced as affected by a spoofing vulnerability in the Patch Tuesday entry.
EtherHiding	Term used to describe EtherRAT’s approach of using Ethereum-hosted configuration for dynamic C2 updates.
Exfiltration	Unauthorized transfer of data out of an environment, often to attacker-controlled destinations.
Heap buffer overflow	Memory corruption condition that can crash processes and sometimes enable code execution, referenced for NGINX and PAN-OS issues.
IKEv2	Internet Key Exchange v2: VPN/key exchange protocol area referenced in PAN-OS vulnerability affecting IKEv2 processing (per the newsletter entry).
Implant	Malware component deployed to maintain access or perform actions on a compromised system.
Information disclosure	Vulnerability outcome where sensitive data is exposed to unauthorized parties.
Kerberoasting	Credential access technique referenced in the EtherRAT/TukTuk intrusion narrative (per the newsletter entry).
Keylogging	Capturing user keystrokes to steal credentials or sensitive information; noted in mobile malware behavior.
Lateral movement	Post-compromise activity where attackers move from one system to others inside the environment.
Lock screen impersonation	Credential harvesting method using a fake Windows lock screen to capture a user’s password.
Multi-chain exploit	Exploit impacting multiple blockchain networks in one incident, referenced in the THORChain breach reporting.
NETCONF	Network configuration protocol referenced as accessible/abusable post-exploitation in the SD-WAN vulnerability entry.
NGINX Open Source / NGINX Plus	Web server products referenced as affected by a critical rewrite-module heap overflow vulnerability (per the newsletter entry).
Node.js	JavaScript runtime used legitimately and also leveraged by malware loaders and RATs in multiple entries.
Obfuscation	Techniques that make code harder to analyze (e.g., encrypted strings, control-flow tricks), highlighted in stealer/RAT analysis.
OS command injection	Vulnerability class enabling an attacker to run operating system commands via a vulnerable application function.

Out-of-bounds write	Memory corruption weakness where data is written outside intended bounds; referenced in a FortiOS issue (per the newsletter entry).
Patch Tuesday	Monthly Microsoft security update release cadence referenced in the May 2026 update entry.
Persistence	Techniques used by attackers/malware to maintain access across reboots or sessions (e.g., Run keys, scheduled tasks).
PoC	Proof of Concept: A demonstration exploit referenced as available for the NGINX vulnerability entry.
PowerShell	Windows scripting tool frequently used in intrusion chains for staging, reconnaissance, and execution.
Privilege escalation	The act of increasing privileges (e.g., user to SYSTEM/admin), referenced across several incident chains and vulnerability entries.
Proxy / tunneling	Mechanisms to route traffic through compromised systems (e.g., SOCKS5, SSH tunnels), enabling stealthy access paths.
Ransomware	Malware that encrypts systems/data for extortion; referenced as the final stage in one multi-stage intrusion chain.
RAT	Remote Access Trojan/Tool: Malware enabling remote control and tasking on infected systems (e.g., .NET RAT, Node.js RAT).
RCE	Remote Code Execution: Vulnerability outcome where an attacker can run code remotely on a target system.
Resource section (.NET Resources)	.NET area used to store embedded data; described as used to conceal payload/configuration in the Gremlin stealer analysis.
Run key	Windows registry persistence mechanism (CurrentVersion\Run) referenced in multiple intrusion chains (conceptually in entries).
SAM hive	Windows Security Account Manager database (registry hive) referenced as targeted for credential theft in Seedworm activity.
Scheduled task	Windows persistence/execution mechanism used for recurring execution, referenced in multiple intrusion narratives.
Screen streaming / recording	Remote viewing/capture capability referenced in mobile device takeover behavior.
SD-WAN	Software-Defined Wide Area Network: Network technology referenced as affected by a critical authentication bypass vulnerability entry.
SOAP	Simple Object Access Protocol: Web service protocol referenced as the attack surface for the PHP SOAP RCE vulnerability entry.
SOCKS5	Proxy protocol referenced as used by malware for routing traffic through an infected device/host.
SQL injection (SQLi)	Vulnerability class where attackers inject SQL commands through inputs to manipulate queries or access data.
SSH tunneling	Encrypted tunneling technique referenced as used for pivoting/traffic routing in malware capabilities.
Token / session token	Credential-like values used to maintain authenticated sessions; referenced as targeted by stealers and as identity service context.
TON	The Open Network: Decentralized network referenced as used for TrickMo C2 transport via .adnl endpoints.
UAF	Use-After-Free: Memory safety flaw type referenced for the PHP SOAP extension vulnerability that can lead to RCE.
VDI	Virtual Desktop Infrastructure: Context for Zoom Workplace VDI Plugin product affected by local privilege escalation vulnerabilities (per the entry).
vManage / vSmart / vBond	SD-WAN components referenced as affected in the Cisco SD-WAN vulnerability entry.
WebDAV	Web Distributed Authoring and Versioning: Protocol feature abused for credential validation attempts in the ModeloRAT intrusion chain.

Webshell	Malicious server-side script allowing remote command execution through a web interface; referenced as observed activity type in an intrusion/vulnerability context.
WebView overlay	Mobile phishing technique where a fullscreen embedded browser view imitates a legitimate app to capture credentials.
WMI	Windows Management Instrumentation: Used for querying system/security info; referenced in Seedworm reconnaissance activity.
XOR encoding	Simple encoding/encryption method referenced in payload/config hiding for Gremlin stealer and noted in some malware loading logic.
ZIP staging	Packaging technique where data or payloads are bundled into ZIP archives for delivery or exfiltration