TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	23/7/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 23 July 2026

10	7	0	0
Campaigns	Vulnerabilities	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 significant increase in both threat activity and critical vulnerability disclosures affecting enterprise, cloud, SaaS, development, and end-user environments. Threat actors continued to evolve their tradecraft through AI-assisted intrusion workflows, OAuth abuse, software supply chain compromises, ClickFix-based social engineering, phishing campaigns, and sophisticated credential theft operations targeting government entities, financial organizations, developers, and cryptocurrency users. Multiple malware families were observed leveraging legitimate services, trusted software repositories, AI platforms, and open-source ecosystems to gain access, steal sensitive data, establish persistence, and evade detection. For organizations in the financial sector, these developments reinforce the growing risk posed by identity compromise, SaaS abuse, supply chain attacks, and information-stealing malware. The newsletter also highlights numerous critical vulnerabilities affecting Microsoft, WordPress, SAP, ServiceNow, Fortinet, Zoom, NGINX, and other widely deployed technologies, including several actively exploited vulnerabilities and unauthenticated remote code execution flaws. Financial institutions should prioritize patch management, strengthen monitoring of SaaS and identity platforms, review third-party dependencies, enhance phishing defences, enforce strong authentication controls, and closely monitor for signs of credential theft, unauthorized access, and data exfiltration.

ADGM THREAT INTELLIGENCE SUMMARY

AI-Assisted Intrusion Campaign Targets Government and Financial Organizations Across Multiple Countries [Campaign] [High]

CylindricalCanine Deploys Golden Gh0st Malware in Certificate Theft Campaign [Campaign] [High]

OkoBot Framework Targets Cryptocurrency Users Through Multi-Stage Malware Deployment [Campaign] [High]

ShinyHunters Tradecraft Driving Large-Scale SaaS Data Exfiltration [Campaign] [High]

Fake GitHub Repositories Deliver BoryptGrab Lineage Infostealer [Campaign] [Medium]

AsyncAPI npm Supply Chain Compromise Enables Import-Time Payload Execution [Campaign] [Medium]

Threat Actors Abuse Claude Shared Chats to Deploy MacSync Stealer Malware [Campaign] [Medium]

TAG-150 Leverages DinDoor and DenoRAT to Deploy NightshadeC2 [Campaign] [Medium]

Disguised TrueType Font (.ttf) Files Used in Multi-Stage Malware Delivery Operations [Campaign] [Medium]

ClickLock Stealer Targeting macOS Users Through ClickFix Techniques [Campaign] [Medium]

Microsoft Addresses Multiple Actively Exploited Zero-Days in July 2026 Security Updates [Vulnerability] [High]

Fortinet Addresses Security Vulnerabilities Across Multiple Products [Vulnerability] [High]

wp2shell - Pre-Authentication RCE in WordPress Core via REST Batch-Route Confusion and SQL Injection [Vulnerability] [High]

Zoom Fixes Critical Account Compromise Vulnerability in Windows Clients [Vulnerability] [High]

F5 Addresses Critical and High Severity Flaws in NGINX [Vulnerability] [High]

Critical ServiceNow AI Platform Sandbox Escape Enables Remote Code Execution [Vulnerability] [Medium]

SAP July 2026 Security Updates Address Critical Vulnerabilities Across Multiple Products [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
AI-Assisted Intrusion Campaign Targets Government and Financial Organizations Across Multiple Countries	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Hunt[.]io have identified an intrusion campaign targeting government, financial, and other strategic organizations across multiple countries. The activity leveraged a combination of artificial intelligence models, reconnaissance platforms, custom exploitation tools, phishing infrastructure, and command-and-control frameworks to support target discovery, exploitation, credential harvesting, and post-compromise operations.

Organizations in the financial sector should be aware that the campaign demonstrates how AI-assisted workflows can accelerate attack execution, refine exploitation techniques, and support credential theft activities. The combination of automated reconnaissance, cloud account targeting, and phishing operations may impact institutions that rely on internet-facing applications, cloud services, and remote access platforms.

Technical Details

- Researchers discovered the campaign after investigating infrastructure associated with a known command-and-control framework.
- An exposed server revealed operational files containing victim data, exploit scripts, phishing pages, malware samples, and attacker logs, providing visibility into the group's activities.
- The attackers maintained a network of servers that supported reconnaissance, vulnerability assessment, malware hosting, and command-and-control operations.
- Before targeting victims, the operators conducted large-scale scanning activities to identify government and other high-value systems for further investigation.
- AI models were integrated into the attack process to assist with attack planning, exploit modification, script generation, and operational decision-making.
- The attackers used AI-assisted tools to develop and improve phishing pages designed to capture user credentials from targeted organizations.
- Observed activity included attempts to exploit vulnerable web applications and gain unauthorized access to targeted environments.
- Following access, the operators collected sensitive information, including source code, databases, credentials, and cloud-related data from compromised systems.
- The campaign targeted government organizations in multiple countries while also identifying financial organizations as part of its broader targeting scope.
- Recovered evidence indicated ongoing infrastructure management, continued exploitation efforts, and sustained operational activity across victim environments.

Recommendations

- Review internet-facing applications for security weaknesses and remediate identified vulnerabilities promptly.
- Monitor authentication systems for suspicious login attempts, unusual access patterns, and possible credential abuse.
- Enforce multi-factor authentication for administrative, remote access, and cloud-based services.
- Enhance monitoring for phishing activity and educate users to identify suspicious login pages and credential requests.
- Increase visibility into cloud and endpoint activity to detect unauthorized access, data collection, and lateral movement attempts.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – AI-Assisted Intrusion Campaign Targets Government and Financial Organizations Across Multiple Countries

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
CylindricalCanine Deploys Golden Gh0st Malware in Certificate Theft Campaign	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Expel has identified 'CylindricalCanine', a subgroup of the 'GoldenEyeDog' cybercrime operation, using 'Golden Gh0st' malware in campaigns targeting organizations in the Asia-Pacific region, including financial entities. The activity relied on phishing emails and support portal submissions to deliver malware, enabling unauthorized access and supporting the theft of code-signing certificates.

Organizations in the financial sector should be aware that the campaign combines social engineering, malware delivery, and certificate abuse to make malicious files appear more legitimate. The use of trusted code-signing certificates could affect security controls that rely on reputation and trust indicators when evaluating executable files.

Technical Details

- The threat group primarily targeted victims through phishing emails and submissions sent through support portal workflows, attempting to persuade users to open malicious content.
- Once a victim interacted with the lure, the attackers deployed Golden Gh0st Loader, the first-stage malware used to initiate the infection process.

- The loader retrieved multiple components needed for execution, including a legitimate application, a malicious DLL, and an encrypted payload.
- The attackers used DLL sideloading to abuse the legitimate application, causing it to load the malicious DLL instead of the expected component.
- The malicious DLL decrypted the payload in memory and launched Golden Gh0st RAT without exposing the final malware directly to the user.
- After execution, Golden Gh0st RAT provided remote access capabilities, allowing the attackers to control infected systems and issue commands.
- The malware supported activities such as credential theft, keylogging, screenshot collection, process discovery, and file access.
- Additional functionality allowed the attackers to establish persistence, maintain access, and support remote connectivity to compromised systems.
- In a significant incident observed by researchers, the operators gained access to a support employee's device and intercepted code-signing certificate activation data intended for customers.
- The stolen certificates were subsequently used to sign the group's malware, helping malicious files appear more trustworthy during delivery and execution.

Recommendations

- Strengthen phishing defenses and provide awareness training focused on malicious attachments and support-related communications.
- Monitor for unusual execution chains involving legitimate applications loading unexpected DLL files.
- Restrict execution of unapproved software and validate digitally signed files before allowing deployment.
- Enable monitoring for credential theft behavior, remote access activity, and unauthorized persistence mechanisms.
- Review certificate management processes and investigate the use of newly observed or unexpected code-signing certificates within the environment.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – CylindricalCanine Deploys Golden Gh0st Malware in Certificate Theft 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
OkoBot Framework Targets Cryptocurrency Users Through Multi-Stage Malware Deployment	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Kaspersky have identified OkoBot, a sophisticated malware framework targeting cryptocurrency users through a multi-stage infection chain designed to steal wallet data, credentials, and seed phrases. The framework uses the TookPS downloader, SSH-based communication, and more than 20 malicious modules to establish access, deploy additional payloads, and collect sensitive information from compromised systems.

Organizations in the financial sector should be aware that the framework demonstrates a highly modular approach to credential theft and digital asset targeting. The campaign could affect institutions and users involved with cryptocurrency services, virtual assets, and blockchain-related operations through the theft of authentication data, wallet information, and other sensitive records.

Technical Details

- The attack begins when victims execute malicious content delivered through ClickFix lures or software hosted on GitHub that is disguised as legitimate applications.
- Execution triggers the TookPS downloader, which establishes the initial foothold and retrieves additional commands and malicious components from attacker-controlled infrastructure.
- The malware installs and configures an SSH tunnel, allowing the attackers to communicate with infected systems and manage later stages of the attack remotely.
- An automated SSH bot connects to the compromised device, gathers system information, and prepares the environment for further payload delivery.
- The framework deploys multiple malware modules that support persistence, remote command execution, information theft, and ongoing control of the infected system.
- One component modifies browser processes to load and hide malicious browser extensions used to collect sensitive user information.
- The framework includes keylogging, credential theft, file collection, and video recording capabilities that allow attackers to monitor user activity and harvest valuable data.
- A dedicated module targets cryptocurrency wallet applications and monitors for connected hardware wallets used to manage digital assets.
- When cryptocurrency wallets are detected, the malware displays phishing interfaces designed to trick users into revealing wallet seed phrases.
- Collected credentials, wallet information, seed phrases, and other sensitive data are then exfiltrated, enabling attackers to access and potentially steal digital assets.

Recommendations

- Educate users about ClickFix-style social engineering techniques and the risks of executing unsolicited scripts or commands.
- Restrict software installation to trusted and verified sources and monitor for unauthorized application downloads.
- Monitor systems for unexpected SSH activity, remote access behavior, and unusual outbound connections.
- Implement detection rules for credential theft, browser manipulation, keylogging, and unauthorized extension installation.
- Strengthen monitoring around cryptocurrency-related systems and investigate attempts to access wallet applications or seed phrase information.

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
ShinyHunters Tradecraft Driving Large-Scale SaaS Data Exfiltration	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Microsoft has identified campaigns associated with ShinyHunters tradecraft that target SaaS-based applications by abusing trusted OAuth relationships. The attackers used voice phishing, compromised third-party integrations, and misconfigured access controls to gain unauthorized access, inherit user privileges, and access customer relationship management (CRM) data without exploiting vulnerabilities in the SaaS platform itself.

Organizations in the financial sector should be aware that these techniques could affect SaaS environments that rely on OAuth-connected applications and third-party integrations. Because the activity leverages legitimate trust relationships and authorized access paths, it may enable data access and exfiltration while reducing visibility through conventional authentication monitoring.

Technical Details

- The campaign targeted SaaS-based applications by focusing on trusted OAuth relationships rather than exploiting software vulnerabilities.
- One attack path involved voice phishing calls in which attackers impersonated support personnel and convinced users to approve malicious OAuth-connected applications.

- Once OAuth consent was granted, the malicious application obtained the same access rights and permissions as the victim user.
- A second intrusion path involved compromising trusted third-party workflows and integrations already connected to customer SaaS environments.
- The attackers abused these existing trusted connections to access customer environments without requiring traditional account compromise.
- Researchers also observed activity involving misconfigured guest access permissions that exposed additional opportunities for unauthorized access.
- After gaining access, the attackers leveraged inherited user and application privileges to enumerate SaaS environments and identify valuable records.
- The activity enabled queries of CRM data and other business information while appearing as legitimate application activity.
- Because access occurred through authorized applications and trusted integrations, the activity could evade traditional sign-in and authentication-based detection methods.
- The campaigns ultimately resulted in persistent access and large-scale data exfiltration from targeted SaaS environments.

Recommendations

- Review all OAuth-connected applications and remove integrations that are no longer required.
- Restrict user ability to grant consent to third-party applications without appropriate approval processes.
- Regularly validate permissions assigned to connected applications and reduce excessive access rights.
- Monitor SaaS environments for unusual application activity, large data queries, and unexpected data exports.
- Review guest access configurations and continuously assess third-party integrations for security risks.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – ShinyHunters Tradecraft Driving Large-Scale SaaS Data Exfiltration

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
Fake GitHub Repositories Deliver BoryptGrab Lineage Infostealer	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Arctic Wolf has identified a large-scale campaign in which threat actors created more than 290 fake GitHub repositories impersonating trusted software, security products, fintech services, and cryptocurrency platforms. The repositories contained deceptive download links that redirected users to malicious websites hosting a BoryptGrab-lineage infostealer designed to steal credentials, wallet data, and other sensitive information.

Organizations in the financial sector should be aware that the campaign abuses trust in widely used software repositories and targets credentials, browser data, payment information, and cryptocurrency assets. The activity could affect employees who download software from unverified sources, particularly those involved in financial services, fintech, virtual asset, and cryptocurrency-related operations.

Technical Details

- The campaign began with the creation of at least 292 fake GitHub repositories that impersonated legitimate software vendors, security tools, fintech services, and cryptocurrency-related products.
- The repositories contained marketing-style README files designed to appear authentic and included concealed links directing users to attacker-controlled download infrastructure.
- Victims searching for software online were redirected through GitHub-hosted pages to fake download portals that displayed trusted branding and verification-themed messages.
- The malicious websites delivered ZIP archives that frequently changed their filenames and payload packaging, making simple file-based detection more difficult.
- Each archive contained a legitimate signed executable alongside a malicious DLL used to execute the malware.
- When the victim launched the executable, DLL sideloading was used to load the malicious DLL and initiate the next stage of the infection.
- The malicious DLL decoded and launched a BoryptGrab-lineage infostealer directly in memory, reducing its exposure on disk.
- Once active, the malware collected credentials, cookies, payment information, and other stored data from more than 19 web browsers.
- The infostealer also searched for information associated with cryptocurrency wallets, messaging platforms, gaming accounts, and Windows credential stores.
- The collected data was packaged and exfiltrated to attacker-controlled infrastructure for further abuse and monetization.

Recommendations

- Restrict software downloads to verified vendor websites and approved software repositories.

- Educate users to verify repository ownership and avoid downloading software from search results alone.
- Monitor for DLL sideloading activity involving legitimate signed applications loading unexpected DLL files.
- Deploy controls to detect credential theft, browser data access, and unauthorized collection of wallet-related information.
- Review and rotate credentials if users are suspected of downloading software from untrusted sources.

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
AsyncAPI npm Supply Chain Compromise Enables Import-Time Payload Execution	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Microsoft has identified a coordinated supply chain compromise affecting multiple AsyncAPI npm packages used for API development and code generation. The attackers republished malicious versions of widely used packages, embedding a loader that executes when the package is imported, allowing malware deployment on developer workstations, CI/CD pipelines, container builds, and production environments.

Organizations in the financial sector should be aware that this campaign demonstrates how trusted software dependencies can be weaponized to gain access to development and build environments. The activity could affect organizations that rely on open-source packages within software development pipelines, potentially enabling unauthorized access, persistence, and credential theft through compromised dependencies.

Technical Details

- The attack targeted the AsyncAPI npm ecosystem by publishing malicious versions of several widely used packages within a trusted software development project.
- The compromise originated from abuse of a GitHub Actions workflow, allowing the attackers to obtain privileged access and inject malicious code into package releases.
- After gaining access, the attackers modified package contents and triggered legitimate release workflows to publish trojanized packages through trusted channels.
- Unlike many npm supply chain attacks, the malicious code was designed to execute when the affected package was imported into an application rather than during installation.
- As a result, common mitigations that disable installation scripts would not prevent execution of the malicious payload.
- When the compromised package was loaded, an embedded loader executed and retrieved additional malware components from external infrastructure.

- The second stage deployed a modular malware framework capable of establishing command-and-control communications and maintaining persistence on infected systems.
- Researchers observed support for multiple communication channels and decentralized fallback mechanisms designed to maintain connectivity with attacker-controlled infrastructure.
- The malware framework included capabilities that could support credential harvesting, remote access, propagation, and deployment of additional malicious functions.
- Because the affected packages were widely used and included transitive dependencies, the compromise had the potential to impact numerous downstream applications and development environments.

Recommendations

- Identify and remove affected package versions from development, build, and production environments.
- Review CI/CD pipelines and software development workflows for the use of compromised dependencies.
- Rotate credentials, tokens, API keys, and secrets that may have been accessible from affected systems.
- Monitor developer workstations and build infrastructure for unauthorized processes, persistence activity, and suspicious outbound communications.
- Implement dependency monitoring and package integrity validation to detect future supply chain compromises.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Threat Actors Abuse Claude Shared Chats to Deploy MacSync Stealer Malware	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Zscaler has identified a ClickFix campaign that abuses shared Claude chats to distribute MacSync Stealer malware to macOS users. The attackers used paid search advertisements to redirect victims to legitimate Claude-hosted shared chats containing malicious instructions that persuaded users to execute commands, leading to the download and installation of the malware.

Organizations in the financial sector should be aware that the campaign demonstrates how threat actors can abuse trusted AI platforms and legitimate services to increase the credibility of social engineering attacks. The activity could affect users involved in cryptocurrency, fintech, and digital asset operations through the theft of credentials, sensitive files, wallet information, and cloud-related access data.

Technical Details

- The attack began with paid advertisements targeting users searching for Claude-related software and services.
- Victims who clicked the advertisements were redirected to shared Claude chats hosted on a legitimate AI platform, making the content appear trustworthy.
- The attackers configured the shared chats to appear as if they were associated with technical support, increasing the likelihood that users would follow the provided instructions.
- The chats contained ClickFix-style instructions that directed victims to copy and execute an encoded command in the macOS Terminal.
- After execution, the command downloaded and launched a multi-stage infection chain while suppressing visible output to reduce suspicion.
- Additional scripts were retrieved from attacker-controlled infrastructure and used to deploy the final MacSync Stealer payload.
- The malware attempted to obtain elevated access and establish persistence on the compromised system to maintain long-term access.
- Once active, MacSync Stealer collected browser credentials, authentication data, keychain information, and files stored on the system.
- The malware also targeted developer-related credentials, cloud access data, messaging application information, and cryptocurrency wallet data.
- Stolen information was compressed, exfiltrated to attacker-controlled infrastructure, and local traces of the activity were removed to hinder investigation.

Recommendations

- Educate users about ClickFix-style social engineering techniques and the risks of executing commands provided by websites or online chats.
- Restrict the execution of unauthorized scripts and monitor for unusual Terminal activity on macOS systems.
- Monitor for attempts to access browser credentials, keychain data, cryptocurrency wallets, and developer-related secrets.
- Implement endpoint monitoring capable of detecting multi-stage malware execution and persistence attempts.
- Review privileged account activity and investigate systems exhibiting suspicious data collection or outbound transfer behavior.

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
TAG-150 Leverages DinDoor and DenoRAT to Deploy NightshadeC2	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at eSentire has identified a TAG-150 intrusion campaign that uses ClickFix social engineering to deploy a multi-stage malware chain consisting of DinDoor, DenoRAT, and NightshadeC2. The attack begins when a user executes a malicious command from the Windows Run prompt, leading to the installation of a Deno-based loader, a remote access trojan, and a final information-stealing payload.

Organizations in the financial sector should be aware that the campaign combines user-driven execution, abuse of legitimate development tools, and multiple malware stages to establish remote access and steal sensitive information. The activity could affect organizations that rely on endpoint access controls and user awareness to defend against social engineering-based attacks.

Technical Details

- The attack begins with a ClickFix-style social engineering lure that persuades a user to execute a malicious command through the Windows Run prompt.
- The command downloads and launches an MSI installer, which serves as the first stage of the infection process.
- The MSI installer writes and executes a PowerShell script named Griffin20.ps1 that prepares the environment for additional malware deployment.
- The PowerShell script installs or locates the Deno runtime, allowing the attackers to use a legitimate development framework to execute later stages.
- Once Deno is available, the script retrieves and launches DinDoor, a Deno-based loader responsible for advancing the infection chain.
- DinDoor then deploys additional staging components that lead to the installation of DenoRAT on the compromised system.
- After execution, DenoRAT provides remote access capabilities and enables the attackers to maintain control over the infected device.
- The malware supports functions such as command execution, file operations, screenshots, host reconnaissance, persistence, and information theft.
- DenoRAT ultimately acts as a loader for NightshadeC2, receiving instructions from attacker-controlled infrastructure to launch the final payload.
- The final stage uses an in-memory Python loader to decrypt and execute NightshadeC2, a remote access and information-stealing payload designed to collect sensitive data while minimizing artifacts on disk.

Recommendations

- Educate users about ClickFix-style lures and prohibit execution of commands copied from untrusted websites or messages.

- Monitor for suspicious use of PowerShell, MSI installers, and Deno-related processes across endpoints.
- Restrict unauthorized installation of development tools and runtimes on user workstations where operationally feasible.
- Deploy endpoint detection capabilities to identify remote access tools, in-memory execution, and persistence mechanisms.
- Investigate unusual outbound communications, command execution activity, and data collection behavior originating from user systems.

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
Disguised TrueType Font (.ttf) Files Used in Multi-Stage Malware Delivery Operations	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Fortinet has identified a large-scale phishing campaign that uses heavily obfuscated JavaScript and malicious Lua-based loaders disguised as TrueType Font (.ttf) files to deploy malware on Windows systems. The campaign relies on phishing emails impersonating well-known organizations and uses multi-stage loaders, fileless techniques, and anti-analysis mechanisms to deliver remote access trojans and information stealers.

Organizations in the financial sector should be aware that the campaign combines phishing, persistence mechanisms, and low-detection malware loaders to evade traditional security controls. The activity could affect organizations through credential theft, unauthorized remote access, and data collection conducted by a range of deployed malware families.

Technical Details

- The attack begins with phishing emails that impersonate legitimate companies and use business cooperation, invoice, shipping, or payment-related themes to entice recipients into opening attachments.
- Victims receive malicious archives either directly through attachments or via links that download the archive from attacker-controlled infrastructure.
- Inside the archive is a heavily obfuscated JavaScript file designed to evade both automated and manual analysis through extensive junk code and code obfuscation techniques.
- When executed, the script checks the environment, copies itself to the system, and establishes persistence through a scheduled task.

- The JavaScript then extracts and decodes additional embedded components required for the next stage of the infection.
- These components include a legitimate AutoIt or LuaJIT interpreter and a malicious script disguised with a ".ttf" file extension to resemble a legitimate font file.
- The disguised ".ttf" file is not a font file but a Lua-based loader that performs multiple de-obfuscation and decryption steps before launching the next payload.
- The loader uses fileless execution techniques to run shellcode directly in memory, reducing artifacts written to disk and limiting detection opportunities.
- Researchers observed advanced evasion features including anti-analysis techniques, custom decryption routines, and memory-based execution designed to hinder detection and investigation.
- The final stage delivers malware such as remote access trojans, keyloggers, and information stealers capable of credential theft, remote system access, and data collection.

Recommendations

- Strengthen phishing defenses and educate users about business-themed and payment-related phishing lures.
- Block or restrict execution of scripting engines and interpreters that are not required for business operations.
- Monitor for scheduled task creation, unusual JavaScript execution, and unauthorized use of AutoIt or Lua-related processes.
- Inspect files based on content and behavior rather than relying solely on file extensions for trust decisions.
- Deploy endpoint monitoring capable of detecting memory-based execution, persistence mechanisms, and credential theft activity.

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
ClickLock Stealer Targeting macOS Users Through ClickFix Techniques	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Group-IB has identified ClickLock Stealer, a new modular macOS malware that is likely distributed through ClickFix-style phishing pages. The attack relies on users copying and executing malicious commands in Terminal, after which the malware deploys multiple components to steal credentials,

cryptocurrency wallet data, browser information, and other sensitive content while establishing persistent access.

Organizations in the financial sector should be aware that the campaign combines social engineering, credential theft, and coercive user manipulation to gain access to sensitive information. The activity could affect users involved in virtual asset, cryptocurrency, and financial operations through the theft of browser credentials, password manager data, wallet information, and authentication secrets.

Technical Details

- The attack begins with a ClickFix-style lure that directs victims to copy and execute a malicious command in the macOS Terminal.
- After execution, the malware displays a fake verification process while quietly downloading and launching additional malicious components in the background.
- The malware presents a convincing macOS password prompt that includes the victim's username and visual elements intended to resemble a legitimate system request.
- The entered password is validated locally before being transmitted to attacker-controlled infrastructure, ensuring only valid credentials are collected.
- If the user refuses to provide the password, ClickLock deploys persistence mechanisms that reactivate the attack after login and system restarts.
- The malware uses aggressive process termination techniques that repeatedly close user applications, browsers, system tools, and monitoring utilities to pressure victims into complying.
- Once credentials are obtained, the malware attempts to gain access to keychain-protected information and browser encryption keys.
- The stealer collects browser credentials, cookies, password manager data, shell history, and other stored authentication information from the system.
- Researchers observed dedicated collection capabilities targeting cryptocurrency wallet extensions, desktop wallet applications, and blockchain-related data.
- The malware also deploys a backdoor component to maintain ongoing access while exfiltrating collected information to attacker-controlled infrastructure.

Recommendations

- Educate users about ClickFix-style attacks and prohibit execution of Terminal commands copied from websites or unsolicited messages.
- Restrict and monitor Terminal activity for unusual command execution and unauthorized script downloads.
- Monitor macOS systems for suspicious ‘LaunchAgent’ creation, persistence attempts, and repeated process termination activity.
- Require strong authentication controls and promptly rotate credentials if exposure is suspected.
- Increase monitoring of systems involved in cryptocurrency, digital asset, and financial operations for signs of credential theft or unauthorized access.

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
Microsoft Addresses Multiple Actively Exploited Zero-Days in July 2026 Security Updates	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Microsoft has released its July 2026 security updates, addressing more than 600 vulnerabilities across Windows, Microsoft Office, SharePoint, Active Directory, SQL Server, Hyper-V, Exchange Server, Visual Studio, Dynamics, Azure components, and other Microsoft services. The release includes three zero-day vulnerabilities, two of which are being actively exploited, including vulnerabilities affecting Active Directory Federation Services (AD FS) and Microsoft SharePoint Server that can lead to privilege escalation.

Organizations in the financial sector should be aware that the updates address a significant number of critical remote code execution and elevation of privilege vulnerabilities affecting widely deployed enterprise technologies. The actively exploited vulnerabilities may impact organizations that rely on AD FS for identity services and SharePoint for collaboration, while several critical flaws could affect internet-facing and business-critical systems if not remediated promptly.

Technical Details

- Microsoft addressed more than 600 security vulnerabilities across its product portfolio, including Windows, Office, SharePoint, SQL Server, Exchange Server, Hyper-V, Dynamics, Azure components, and other enterprise services.
- Three zero-day vulnerabilities were included in the release, consisting of two vulnerabilities that are actively being exploited and one vulnerability that was publicly disclosed prior to patch availability.
- CVE-2026-56155 affects Active Directory Federation Services and allows an authenticated attacker to obtain administrative privileges through elevation of privilege within AD FS environments.
- CVE-2026-56164 affects Microsoft SharePoint Server and enables an unauthenticated remote attacker to gain elevated privileges over the network without requiring valid credentials.
- The actively exploited SharePoint vulnerability impacts SharePoint Server 2019 and SharePoint Server Subscription Edition deployments.
- CVE-2026-50661 is a publicly disclosed Windows BitLocker security feature bypass vulnerability that can allow attackers to bypass device encryption protections and access encrypted data.
- The update contains 59 Critical vulnerabilities, the majority of which enable Remote Code Execution or Elevation of Privilege across enterprise systems.

- Critical vulnerabilities affect Microsoft SharePoint, Exchange Server, DHCP Server, Remote Desktop Protocol, SQL Server ODBC Driver, Windows FTP Service, Windows Message Queuing Service, Windows Kernel, Windows GDI+, and Windows Server Network Driver components.
- Several critical vulnerabilities carry CVSS scores between 9.6 and 9.9, indicating the potential for severe impact if vulnerable systems remain unpatched.

Recommendations

- Immediately deploy the July 2026 Microsoft security updates across all supported Windows systems, servers, and Microsoft products.
- Prioritize patching Active Directory Federation Services (AD FS) and Microsoft SharePoint Server environments due to active exploitation.
- Microsoft recommended enabling Antimalware Scan Interface (AMSI) and configuring Request Body Scan Mode to Full on SharePoint servers to help mitigate exploitation until updates are applied.
- Verify successful installation of the latest cumulative security updates across endpoints, servers, virtual machines, and cloud-hosted workloads.
- Prioritize remediation of internet-facing services and business-critical systems before addressing lower-risk internal assets.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Fortinet Addresses Security Vulnerabilities Across Multiple Products	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Fortinet has released security updates addressing seven vulnerabilities affecting FortiOS, FortiProxy, FortiPAM, FortiSandbox, and FortiSASE products. The vulnerabilities include unauthenticated access, buffer overflow, cross-site scripting, path traversal, buffer over-read, and HTTP header injection issues. The most severe vulnerability, CVE-2026-59835, affects FortiSandbox and could allow unauthenticated attackers to access the Virtual Network Computing (VNC) service exposed on all network interfaces.

Organizations in the financial sector should be aware that the vulnerabilities affect multiple security and access management platforms commonly used within enterprise environments. The unauthenticated FortiSandbox vulnerability may impact exposed deployments, while several medium-severity issues could affect system availability, management functions, and user interactions if vulnerable systems remain unpatched.

Technical Details

- Fortinet disclosed seven vulnerabilities impacting multiple products, including FortiOS, FortiProxy, FortiPAM, FortiSandbox, and FortiSASE.
- The highest-severity issue, CVE-2026-59835, affects FortiSandbox and may allow unauthenticated attackers to access the VNC service exposed across all network interfaces.
- Successful exploitation of CVE-2026-59835 could enable unauthorized access to active sandbox sessions without requiring authentication.
- CVE-2026-59837 is a stack-based buffer overflow vulnerability affecting FortiOS, FortiPAM, and FortiProxy through log report functionality.
- CVE-2026-23573 is a reflected cross-site scripting vulnerability affecting SSL-VPN functionality in FortiOS, FortiPAM, and FortiProxy deployments.
- CVE-2026-59839 is a path traversal vulnerability affecting FortiOS, FortiPAM, and FortiProxy that may allow deletion of files from the root file system through a CLI command.
- CVE-2025-62675 is an HTTP header injection vulnerability affecting web filter warning pages in FortiOS and FortiProxy installations.
- CVE-2025-62826 is an HTTP header injection vulnerability affecting captive portal authentication forms in FortiOS and FortiProxy products.
- CVE-2025-43892 is a buffer over-read vulnerability affecting authd and wad daemons in FortiOS, FortiProxy, and FortiSASE.
- The affected products span numerous supported software versions, requiring organizations to verify exposure across firewall, proxy, privileged access management, sandboxing, and secure access service edge deployments.

Recommendations

- Immediately apply the latest Fortinet security updates for affected products.
- Prioritize remediation of FortiSandbox (CVE-2026-59835) due to its unauthenticated nature.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
wp2shell - Pre-Authentication RCE in WordPress Core via REST Batch-Route Confusion and SQL Injection	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

WordPress has released security updates to address CVE-2026-63030, a critical vulnerability in WordPress Core affecting the WordPress REST API batch endpoint. The vulnerability allows an unauthenticated remote attacker to execute arbitrary code on vulnerable WordPress installations, potentially resulting in complete website compromise, unauthorized access to sensitive information, website defacement, malware deployment, and server takeover. The issue affects default WordPress deployments and does not require additional plugins to be present.

Organizations in the financial sector should be aware that the vulnerability affects one of the most widely deployed content management systems and can be exploited without authentication or user interaction. The public disclosure of exploitation techniques, availability of multiple proof-of-concept repositories, and automated exploitation tooling could affect internet-facing WordPress environments that remain on vulnerable versions.

Technical Details

- CVE-2026-63030 is a critical unauthenticated remote code execution vulnerability affecting WordPress Core through the WordPress REST API batch endpoint.
- The vulnerability affects default WordPress installations and does not require vulnerable plugins, themes, or special configurations to be present.
- Successful exploitation can be performed remotely over the network without authentication or user interaction.
- The issue primarily impacts WordPress installations where a persistent object cache is not enabled.
- The vulnerability has a CVSS v3.1 score of 9.8 and is classified as Critical due to the potential for complete compromise of affected websites and servers.
- Researchers disclosed an attack chain involving CVE-2026-63030 and CVE-2026-60137, where a route-confusion flaw can be combined with an SQL injection vulnerability to achieve unauthenticated remote code execution on affected WordPress branches.
- Public exploitation tooling has rapidly emerged following disclosure, including multiple proof-of-concept repositories, automated exploitation frameworks, large-scale scanning capabilities, and techniques intended to bypass common web application firewall protections.
- Successful exploitation could allow attackers to execute arbitrary code, gain unauthorized access, deploy malware, alter website content, access sensitive information, and potentially take control of the underlying server.

Recommendations

- Upgrade affected WordPress installations immediately.
- WordPress versions 7.0.2, 6.9.5, 6.8.6, and 7.1 beta2 have been released, containing fixes for the vulnerabilities.

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

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Zoom Fixes Critical Account Compromise Vulnerability in Windows Clients	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Zoom has disclosed CVE-2026-53412, a critical vulnerability affecting Zoom Workplace for Windows and Zoom Workplace VDI Client for Windows. The vulnerability is caused by improper input validation and could allow an unauthenticated remote attacker to compromise user accounts without requiring valid credentials, user interaction, or local access to the target system.

Organizations in the financial sector should be aware that the vulnerability affects widely deployed collaboration software used for business communications and remote work. Successful exploitation may impact user accounts and enterprise environments that rely on Zoom services, making timely remediation important for organizations operating Windows-based Zoom clients.

Technical Details

- CVE-2026-53412 is a critical vulnerability affecting Zoom Workplace for Windows and Zoom Workplace VDI Client for Windows.
- The vulnerability has been assigned a CVSS v3.1 score of 9.8, reflecting the potential severity of successful exploitation.
- The issue is caused by improper input validation, classified under CWE-20.
- The vulnerability can be exploited by a remote attacker without requiring authentication.
- Exploitation does not require valid user credentials or prior access to the target environment.
- No user interaction is required for successful exploitation.
- The vulnerability may allow attackers to compromise affected user accounts.
- Zoom published advisory ZSB-26014 to address the vulnerability and provide remediation guidance.

- The advisory was initially released on 14 July 2026 and later revised on 15 July 2026 to clarify that the Zoom Meeting SDK for Windows is not affected.
- Affected products include Zoom Workplace for Windows versions prior to 7.0.0 and Zoom Workplace VDI Client for Windows versions prior to 7.0.10, 6.6.15, and 6.5.18 in their respective release branches.

Recommendations

- Upgrade Zoom Workplace & Zoom Workplace VDI Client for Windows to fixed version or later.
- Immediately upgrade Zoom Workplace for Windows to version 7.0.0 or later.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
F5 Addresses Critical and High Severity Flaws in NGINX	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

F5 has released security updates addressing three memory safety vulnerabilities affecting NGINX Open Source and NGINX Plus. The most severe issue, CVE-2026-42533, is a critical heap buffer overflow vulnerability in the NGINX map directive that may enable remote code execution under specific conditions. Additional vulnerabilities affect the NGINX slice module and SSI module, potentially leading to memory corruption and application instability.

Organizations in the financial sector should be aware that these vulnerabilities impact widely deployed web servers, application delivery platforms, API gateways, web application firewall deployments, and ingress controllers. The affected components are commonly used in internet-facing environments, and successful exploitation could affect application availability, integrity, and potentially expose critical business services if vulnerable versions remain in operation.

Technical Details

- F5 disclosed three memory safety vulnerabilities affecting NGINX Open Source and NGINX Plus, with impacts spanning HTTP request processing components and associated modules.
- CVE-2026-42533 is a heap buffer overflow vulnerability in the NGINX map directive and has been assigned a CVSS v4.0 score of 9.2, making it the most severe issue in this advisory.
- The vulnerability affects request-processing logic associated with the map directive and may allow remote code execution under specific circumstances.
- CVE-2026-60005 is an uninitialized memory access vulnerability affecting the “ngx_http_slice_module” and carries a CVSS v4.0 score of 8.8.
- Improper handling of memory within the slice module could result in unintended memory access during HTTP request processing.

- CVE-2026-56434 is a use-after-free vulnerability affecting the “ngx_http_ssi_module” and has a CVSS v4.0 score of 8.3.
- The vulnerability may trigger access to previously released memory during SSI processing operations, potentially leading to memory corruption or service instability.
- Additional affected products include NGINX Instance Manager, F5 WAF for NGINX, NGINX App Protect WAF, NGINX Gateway Fabric, and multiple NGINX Ingress Controller releases that incorporate vulnerable NGINX components.

Recommendations

- Update all affected F5 products to vendor-recommended versions.
- Verify internet-facing NGINX deployments are running supported versions.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical ServiceNow AI Platform Sandbox Escape Enables Remote Code Execution	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

ServiceNow has released security updates to address CVE-2026-6875, a critical vulnerability affecting the ServiceNow AI Platform. The vulnerability is a sandbox escape flaw that could allow an unauthenticated remote attacker, under certain circumstances, to escape the AI platform sandbox and execute arbitrary code within the ServiceNow environment. The issue affects multiple ServiceNow release families, including Brazil, Australia, Zurich, and Yokohama.

Organizations in the financial sector should be aware that the vulnerability affects a widely deployed enterprise platform used for IT service management, workflow automation, and AI-driven operations. The lack of authentication and user interaction requirements could affect exposed or vulnerable ServiceNow deployments if patching is delayed, potentially enabling unauthorized code execution within critical business environments.

Technical Details

- CVE-2026-6875 is a critical sandbox escape vulnerability affecting the ServiceNow AI Platform.
- The vulnerability has been assigned a CVSS v4 score of 9.5, reflecting the potential severity of successful exploitation.
- The affected component is the AI Platform sandbox environment used within the ServiceNow platform.
- The vulnerability can be exploited remotely and does not require local access to the target environment.
- No authentication is required for exploitation, allowing attacks to be initiated without valid credentials.

- Successful exploitation does not require user interaction, reducing the barriers to potential abuse.
- Under certain circumstances, an attacker may escape the intended sandbox restrictions imposed by the AI Platform.
- Once sandbox protections are bypassed, the vulnerability may enable execution of arbitrary code within the ServiceNow environment.
- The vulnerability affects multiple ServiceNow release families, including Brazil, Australia, Zurich, and Yokohama.

Recommendations

- Upgrade all affected self-hosted ServiceNow AI Platform deployments to a supported patched version.
- Verify that hosted ServiceNow instances have received the latest vendor security update.
- ServiceNow has released security updates for affected versions, including Brazil EA/GA, Australia Patch 2, Zurich Patch 7b and Patch 9, and Yokohama Patch 12 Hot Fix 1b and Patch 13.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
SAP July 2026 Security Updates Address Critical Vulnerabilities Across Multiple Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

SAP has released its July 2026 Security Patch Day updates, addressing 16 new Security Notes, one GitHub Security Advisory, and three updates to previously released advisories. The updates remediate vulnerabilities affecting multiple enterprise products, including SAP NetWeaver Application Server ABAP, SAP Approuter, SAP Commerce Cloud, SAP Integration Suite, SAProuter, SAP S/4HANA, SAP NetWeaver Java, SAP Fiori, and SAP HANA. Several vulnerabilities carry Critical severity ratings and affect core components widely deployed across enterprise environments.

Organizations in the financial sector should be aware that the updates address vulnerabilities that could allow memory corruption, HTTP request smuggling, directory traversal, remote code execution, credential misuse, and other high-impact attacks against critical SAP services. The vulnerabilities may affect business-critical ERP, application, integration, and web access infrastructure, making timely remediation important for organizations operating SAP environments.

Technical Details

- SAP released July 2026 security updates containing 16 new Security Notes, one GitHub Security Advisory, and three updates to previously published advisories affecting multiple SAP products.

- The most severe vulnerability, CVE-2026-44747, affects SAP NetWeaver Application Server ABAP and is a memory corruption vulnerability with a CVSS score of 9.9.
- Successful exploitation of CVE-2026-44747 could allow a low-privileged user to compromise the confidentiality, integrity, and availability of an affected SAP system.
- CVE-2026-27690 is a critical HTTP Request Smuggling vulnerability affecting SAP Approuter with a CVSS score of 9.1.
- CVE-2026-44761 affects SAP Commerce Cloud and involves insecure sample credentials that could expose vulnerable environments to unauthorized access.
- SAP updated guidance for CVE-2026-40128, a critical directory traversal vulnerability affecting SAP NetWeaver Application Server Java Web Container.
- CVE-2026-40860 affects SAP Integration Suite Edge Integration Cell and addresses multiple Apache Camel vulnerabilities, including CVE-2026-40453 and CVE-2026-33454.
- CVE-2026-0487 is a DLL hijacking vulnerability affecting SAProuter on Windows platforms and carries a CVSS score of 8.4.
- CVE-2026-44752 affects the SAP NetWeaver AS Java Configuration Wizard and could enable cross-site scripting attacks against affected deployments.
- Additional high-severity vulnerabilities include CVE-2026-44745 in SAP Approuter, multiple Apache Tomcat vulnerabilities affecting SAP Commerce Cloud, and CVE-2026-58233, a remote code execution vulnerability affecting the SAP Change and Transport System Attach Tool (ctsattach).

Recommendations

- Apply all relevant SAP July 2026 Security Notes according to SAP's priority guidance.
- Prioritize remediation of all Critical vulnerabilities, especially CVE-2026-44747, CVE-2026-27690, CVE-2026-44761, and CVE-2026-40128.

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

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

AI-Assisted Intrusion Campaign Targets Government and Financial Organizations Across Multiple Countries

Tactic	Technique	Observed Activity
Reconnaissance	Gather Victim Network Information (T1590)	Enumeration of domains, subdomains, certificates, adjacent IPs, VPN gateways, Git and Jira services.
Reconnaissance	Active Scanning (T1595)	Scanning of thousands of government systems and extensive service fingerprinting activities.
Resource Development	Phishing for Information (T1598)	Creation and maintenance of cloned government and organizational login pages for credential harvesting.
Initial Access	Exploit Public-Facing Application (T1190)	SQL injection and exploitation of exposed web applications and cloud-connected services.
Initial Access	Valid Accounts (T1078)	Abuse of exposed cloud credentials and compromised accounts to access backend infrastructure.
Execution	Command and Scripting Interpreter (T1059)	Use of custom scripts and exploit code to execute actions against target systems.
Persistence	Server Software Component Web Shell (T1505.003)	Deployment of web shells on compromised systems for persistent command execution.
Credential Access	Credentials from Password Stores / Credentials from Web Resources (T1555/T1552)	Collection of cloud credentials, enterprise platform authentication material, and messaging credentials.
Discovery	Network Service Discovery (T1046)	Identification and profiling of web services, mail services, cloud-connected assets, and infrastructure components.
Collection	Data from Information Repositories (T1213)	Extraction of databases, citizen complaint records, source code repositories, and administrative data.
Collection	Data from Local System (T1005)	Collection of source code, configuration information, and application data from compromised systems.
Exfiltration	Exfiltration Over Web Service (T1567)	Theft of databases, credentials, source code, and other sensitive organizational data.
Command and Control	Application Layer Protocol (T1071)	Malware communications and command-and-control activity over web-based protocols

CylindricalCanine Deploys Golden Gh0st Malware in Certificate Theft Campaign

Tactics	Techniques	Observed Activity
Initial Access	Phishing	The malware was primarily delivered through phishing emails and support portal submissions.
Execution	User Execution	The attack relied on a support user opening malicious submitted content, enabling malware execution on the device.
Defense Evasion	DLL Side-Loading	The loader used a legitimate executable with a malicious library to decrypt and execute the final payload.
Defense Evasion	Code Signing	The actors accessed certificates intended for legitimate customers and used code-signing trust to improve malware legitimacy.
Credential Access	Credentials from Web Browsers	Golden Gh0st RAT included browser credential theft capability.

Collection	Screen Capture	Golden Gh0st RAT could capture screenshots from compromised systems.
Credential Access	Keylogging	Golden Gh0st RAT included keylogging capability.
Discovery	Process Discovery	The malware could enumerate running processes on infected systems.
Execution	Command and Scripting Interpreter	Golden Gh0st RAT supported command execution on compromised systems.
Command and Control	Proxy	The malware supported proxy tunneling for operator activity.
Defense Evasion	Clear Windows Event Logs	Golden Gh0st RAT could clear event logs to hinder investigation.
Persistence	Create Account	Some samples could create a privileged backdoor account for continued access.
Persistence	Event Triggered Execution	Some samples modified Windows logon settings to support remote access persistence

ShinyHunters Tradecraft Driving Large-Scale SaaS Data Exfiltration

Tactic	Technique	Observed Activity
Initial Access	Phishing: Voice Phishing (T1598.004)	Threat actors impersonated IT support personnel and socially engineered users through vishing campaigns.
Initial Access	Valid Accounts (T1078)	Access was obtained through authorized user accounts and inherited OAuth permissions.
Initial Access	External Remote Services (T1133)	Actors leveraged trusted SaaS applications and existing cloud services for access.
Persistence	Additional Cloud Roles / Cloud Account Permissions (T1098.003)	Malicious OAuth applications were granted permissions enabling continued access.
Persistence	Account Manipulation (T1098)	OAuth consent abuse enabled persistent access within Salesforce environments.
Credential Access	Credentials from Password Stores / Access via Trusted Integrations (T1555)	Supply-chain compromises enabled use of connection secrets and OAuth-based access through trusted integrations.
Discovery	Cloud Service Discovery (T1526)	Actors enumerated Salesforce instances belonging to targeted organizations.
Discovery	Permission Groups Discovery (T1069)	Threat actors leveraged inherited user and application privileges to understand accessible resources.
Collection	Data from Information Repositories (T1213)	CRM records, including account, contact, and service-related data, were queried and collected.
Collection	Automated Collection (T1119)	GraphQL and API-based requests were used to systematically retrieve large datasets.
Exfiltration	Exfiltration Over Web Service (T1567)	Data was exfiltrated through legitimate application access and SaaS APIs.
Defense Evasion	Trusted Relationship (T1199)	Actors abused trusted OAuth relationships and third-party integrations to blend with legitimate activity.
Defense Evasion	Exploitation of Misconfigured Cloud Resources (T1529)	Misconfigured guest-user permissions were abused to gain unauthorized access to data.

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
AD FS	Active Directory Federation Services. A Microsoft identity service that enables single sign-on and federated authentication across applications and organizations.
Agent Tesla	Credential theft malware commonly used to collect passwords and sensitive information.
AI	Artificial Intelligence. Technology that enables systems to perform tasks normally requiring human intelligence, such as analysis, decision making, and automation.
AMSI	Antimalware Scan Interface. A Microsoft security feature that allows security tools to inspect scripts and content before execution.
API	Application Programming Interface. A mechanism that allows software applications to communicate and exchange data with one another.
App-Bound Encryption	A browser security mechanism that ties encrypted data to a specific application instance to help protect stored credentials.
ASEP	Auto-Start Extensibility Point. A persistence mechanism that allows software to automatically execute when a system starts or a user logs in.

AutoIt	A scripting language commonly used for task automation on Windows systems. It can also be abused by malware.
BitLocker	Microsoft's disk encryption technology used to protect data stored on Windows devices.
BoryptGrab	Information-stealing malware focused on credentials, browser data, wallets, and messaging platforms.
Browser Extension	Software that adds functionality to a web browser. Threat actors often target extensions to steal credentials or session data.
C2	Command and Control. Infrastructure used by attackers to communicate with and manage compromised systems.
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart. A challenge used to distinguish human users from automated bots.
CI/CD	Continuous Integration / Continuous Delivery. Automated software development and deployment processes used to build and release applications.
ClaudeFix	Campaign that abused shared AI chat links to distribute malware through ClickFix-style techniques.
ClickFix	A social engineering technique where users are tricked into copying and executing malicious commands under the guise of fixing an issue or completing verification.
ClickFix	Social engineering technique that tricks users into copying and executing attacker-provided commands.
ClickLock	Malware campaign combining ClickFix social engineering with coercive techniques to steal credentials from macOS users.
ClickLock Stealer	macOS-focused information stealer that pressures victims into disclosing credentials.
Cloudflare Verification	A legitimate website verification mechanism that is frequently impersonated by attackers in phishing and ClickFix campaigns.
CMS	Content Management System. Software used to create, manage, and publish website content. WordPress is a common example.
Command Execution	The ability to run operating system commands locally or remotely on a system.
Connected Application	Third-party application granted access to another service through authorization mechanisms such as OAuth.
Copilot	Microsoft's AI-powered assistant platform.
Credential Harvesting	Collection of user credentials for unauthorized access.
Credential Theft	The unauthorized collection of usernames, passwords, tokens, or authentication secrets.
CRM	Customer Relationship Management. Systems used to manage customer information, interactions, and business relationships.
CSC	UAE Cyber Security Council
Cryptocurrency Wallet	Software or hardware used to store and manage digital assets.
CVE	Common Vulnerabilities and Exposures. A standardized identifier assigned to publicly disclosed security vulnerabilities.
CVSS	Common Vulnerability Scoring System. A framework used to measure and communicate the severity of security vulnerabilities.
CylindricalCanine	Threat group identified as a subgroup of a larger criminal operation and linked to Golden Gh0st malware activity.
Deno	A JavaScript and TypeScript runtime used for application development. It was abused in observed malware delivery chains.
DenoRAT	A remote access trojan built using the Deno runtime that enables attackers to control compromised systems.
DenoRAT	Remote access trojan built using the Deno runtime, enabling remote control and information theft.

DHCP	Dynamic Host Configuration Protocol. A network protocol that automatically assigns IP addresses and network settings to devices.
Digital Asset	Electronic asset such as cryptocurrency or blockchain-based tokens.
DinDoor	Deno-based malware loader used to execute and stage additional malicious payloads.
Directory Traversal	Vulnerability that permits unauthorized access to restricted directories or files.
DLL	Dynamic-Link Library. A file containing code and functions shared by Windows applications.
DLL Hijacking	A technique where a malicious DLL is loaded instead of a legitimate library.
DLL Sideloading	A technique where attackers force a legitimate application to load a malicious DLL.
DLL Sideloading	Method of executing malicious code through a legitimate application loading a rogue DLL file.
DNS	Domain Name System. The system that converts domain names into IP addresses.
Dynamic Analysis	Examination of software while it is running to understand behavior and identify threats.
Dynamics 365	Microsoft's business application suite for ERP and CRM functions.
EDR	Endpoint Detection and Response. Security technology used to detect, investigate, and respond to threats on endpoints.
EoP	Elevation of Privilege. A vulnerability or technique that allows an attacker to obtain higher permissions than initially granted.
ERP	Enterprise Resource Planning. Software used to manage and integrate core business processes.
Event Monitoring	The collection and analysis of activity logs to identify unusual or suspicious behavior.
Exchange Server	Microsoft email and messaging platform used by enterprises.
Exfiltration	Unauthorized transfer of data from a system or network to an attacker-controlled location.
FortiOS	Operating system used by Fortinet security appliances.
FortiProxy	Fortinet secure web proxy platform.
FortiSandbox	Fortinet sandboxing platform used to analyze suspicious files and activity.
FTP	File Transfer Protocol. A protocol used to transfer files between systems over a network.
Gh0st RAT	Open-source remote access trojan family that has been used in cyber operations for many years.
GitHub Actions	A workflow automation platform used for software builds, testing, and deployment.
GitHub Actions	Automation platform used to build, test, and release software.
Golden Gh0st Loader	Initial malware component responsible for deploying the final Golden Gh0st RAT payload.
Golden Gh0st RAT	Remote access trojan providing attackers with control over infected systems.
GoldenEyeDog	Cybercrime group associated with credential theft, malware operations, and abuse of code-signing certificates.
GSocket	An open-source networking tool that can be abused to establish covert remote access.
Hardware Wallet	A dedicated device used to securely store cryptocurrency private keys offline.
Hardware Wallet	Dedicated device used to securely store cryptocurrency credentials offline.
HMAC	Hash-Based Message Authentication Code. A cryptographic mechanism used to verify data authenticity and integrity.
HTTP	Hypertext Transfer Protocol. The protocol used to transfer web traffic between clients and servers.
HTTP Request Smuggling	A technique that manipulates web server request processing to bypass security controls or access unauthorized functions.
Hyper-V	Microsoft virtualization platform used to host virtual machines.

Identity Federation	Process of sharing authentication and identity information across systems or organizations.
Identity Platform	Systems used to manage authentication, authorization, and user identities.
Infostealer	Malware designed to collect credentials, cookies, financial information, wallet data, and other sensitive information.
In-Memory Execution	Execution of malicious code directly in memory, reducing artifacts written to disk and making detection more difficult.
IPFS	InterPlanetary File System. A decentralized content-sharing platform used to distribute files across multiple systems.
JavaScript	A scripting language commonly used in websites and web applications.
JWT	JSON Web Token. A token format used to securely transmit information between systems.
Keychain	Apple's password and secret storage mechanism used on macOS devices.
Keylogger	Malware that records user keystrokes to capture credentials and sensitive information.
Keylogging	Recording of keystrokes to capture credentials or sensitive information.
Lateral Movement	Movement by an attacker from one system to another after initial access is obtained.
LaunchAgent	A macOS persistence mechanism that automatically starts applications or scripts when a user logs in.
Ledger	Popular cryptocurrency wallet platform targeted by several malware campaigns.
LLM	Large Language Model. An AI model trained on large datasets to generate and analyze language.
Lua	A lightweight scripting language observed in malware loaders and attack chains.
LuaJIT	A high-performance implementation of the Lua scripting language.
MacSync Stealer	macOS information-stealing malware targeting credentials, files, and cryptocurrency wallet data.
Malvertising	Use of online advertisements to redirect victims to malicious content.
Malware Loader	Malicious software responsible for downloading, decrypting, or launching additional payloads.
Memory Corruption	A class of vulnerability that results from improper memory handling and may lead to code execution or crashes.
Miasma	Modular malware framework observed in software supply chain attacks.
MSI	Microsoft Installer. A Windows installation package format used for software deployment.
MSMQ	Microsoft Message Queuing. A Microsoft messaging service used to exchange data between applications.
NGINX	Web server, reverse proxy, and application delivery platform.
NightshadeC2	Malware platform providing command-and-control and information-stealing capabilities.
OAuth	An authorization framework that allows third-party applications to access resources on behalf of users without exposing passwords.
OAuth Abuse	Misuse of trusted application permissions to gain access to data without stealing passwords.
Object Cache	A caching mechanism used by WordPress to store and retrieve frequently used data.
OIDC	OpenID Connect, an authentication framework commonly used with cloud applications.
OkoBot	Multi-stage malware framework targeting cryptocurrency users through numerous malware modules.
PatchAgent	A multi-stage malware framework associated with remote access and command execution capabilities.

PatchAgent	Multi-stage malware framework used to install backdoor capabilities and execute attacker commands.
Path Traversal	Technique allowing access to files or directories outside intended locations.
Persistence	A technique used by attackers to maintain access to a compromised system after reboots or logouts.
Persistence	Techniques used to maintain access after reboot, logout, or remediation attempts.
Phishing	A social engineering technique used to trick users into revealing information or executing malicious content.
PowerShell	A Microsoft command-line shell and scripting platform frequently used by administrators and threat actors.
Process Hollowing	A technique where malicious code is injected into a legitimate process to conceal execution.
Process Hollowing	Technique where malicious code runs inside a legitimate process to evade detection.
Proof of Concept (PoC)	Demonstration code or tooling showing how a vulnerability can be exploited.
Ransomware	Malware that encrypts or restricts access to systems and data to demand payment.
RAT	Remote Access Trojan. Malware that allows attackers to remotely control compromised systems.
RCE	Remote Code Execution. The ability for an attacker to execute arbitrary code on a target system remotely.
RDP	Remote Desktop Protocol. Microsoft's remote access protocol used to connect to Windows systems.
Remcos RAT	Remote access trojan commonly used to control compromised systems.
Remote Code Execution (RCE)	Ability to run arbitrary code on a target system remotely.
Request Smuggling	Manipulation of web requests to bypass security controls or access hidden functionality.
REST API	Representational State Transfer Application Programming Interface. A web-based interface used for application communication.
Route Confusion	A vulnerability where application routing logic can be manipulated to reach unintended functionality.
Route Confusion	Exploitation of application routing logic to reach unintended functionality.
SaaS	Software as a Service. Cloud-based software delivered over the internet.
SaaS	Software delivered as an online service rather than installed locally.
Salesforce	Cloud-based customer relationship management platform targeted through OAuth abuse campaigns.
Sandbox Escape	A vulnerability that allows code to break out of an isolated execution environment and access broader system resources.
Sandbox Escape	Ability to break out of an isolated environment and access broader system resources.
SAP NetWeaver	SAP application platform used to run enterprise workloads.
Security Feature Bypass	Technique that defeats built-in security protections without directly exploiting the protected resource.
Seed Phrase	Recovery phrase used to restore access to a cryptocurrency wallet.
ServiceNow	Enterprise workflow, IT service management, and automation platform.
SharePoint	Microsoft's web-based collaboration and document management platform.
SharePoint	Microsoft collaboration and document management platform.
Shellcode	Compact executable code often used as a payload for exploitation and malware deployment.
ShinyHunters	Threat actor group associated with data theft and extortion activities, including abuse of SaaS application trust relationships.

SIEM	Security Information and Event Management. Technology used to collect, correlate, and analyze security events.
Single Sign-On (SSO)	Authentication mechanism allowing one login to access multiple systems.
SQL Injection	A vulnerability that allows attackers to manipulate database queries through crafted input.
SQL Server	Microsoft's enterprise database platform.
SSH	Secure Shell. A protocol used for secure remote administration and communications.
SSI	Server Side Includes. A web server feature that dynamically inserts content into web pages.
Supply Chain Attack	An attack that compromises trusted software, services, vendors, or dependencies to affect downstream users.
Supply Chain Attack	Compromise of trusted software, libraries, vendors, or update mechanisms to impact downstream users.
TAG-150	Threat group associated with ClickFix-based intrusions and deployment of Deno-based malware frameworks.
TeviRAT	Remote access malware observed as part of OkoBot infection chains.
Third-Party Integration	Connection between separate software platforms for data exchange and workflow automation.
Token	Digital credential used by applications and services to authorize access.
Transitive Dependency	A software dependency indirectly included through another package or application component.
Trezor	Cryptocurrency wallet platform frequently targeted for seed phrase theft.
Trusted Publisher	Automated publishing process that allows software releases to be signed and distributed through approved workflows.
TTF Trap	Malware campaign that disguised malicious Lua scripts as benign TrueType Font files.
TTPs	Tactics, Techniques, and Procedures. The methods and approaches used by threat actors during operations.
VDI	Virtual Desktop Infrastructure. Technology that delivers desktop environments from centralized infrastructure.
Vishing	Voice Phishing. A social engineering attack conducted through phone calls or voice communications.
VNC	Virtual Network Computing. A technology that enables remote graphical control of systems.
Voice Phishing (Vishing)	Social engineering attack conducted through phone calls or voice communications.
WAF	Web Application Firewall. A security solution designed to monitor and filter web application traffic.
Wallet Extension	Browser extension used to manage cryptocurrency accounts and transactions.
WebShell	A malicious web-based script that provides attackers remote access to a compromised web server.
WordPress	Widely used content management system for websites and web applications.
XSS	Cross-Site Scripting. A vulnerability that allows injection of malicious scripts into web applications.
XWorm	Malware capable of remote control, persistence, and data theft.
ZIP Slip	A path traversal vulnerability that allows files to be written outside the intended extraction directory during archive extraction.
Zoom Workplace	Collaboration and communication platform used by organizations for meetings and teamwork.