TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	12/3/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 12 March 2026

10	4	0	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Finance Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights coordinated social engineering and identity abuse across enterprise platforms, supply chain abuse of developer ecosystems, and a regional surge in targeted operations. Adversaries used teams impersonation to deliver malware, abused OAuth redirection to push malware, and shipped digitally signed payloads that installed RMM tools, while hiding command and control through DNS tunneling and blockchain smart contracts. Conflict themed lures have increased across the GCC. The attack surface expanded to iOS via the Coruna exploit kit and to Windows through BoryptGrab and VIP_Keylogger, with theft of credentials, wallets, and sensitive data in focus. For financial services, the blend of brand impersonation, developer trust abuse, and persistent RMM access raises risk of account takeover, data loss, and fraud across customer, employee, and engineering workflows. Priorities include rapid patching of Chrome, AWS LC, Cisco FMC, and Nessus issues, stronger governance of OAuth and RMM, and continuous monitoring for JSON RPC traffic, DNS tunneling, and newly registered conflict themed domains. Reinforce awareness for meeting and purchase order lures, verify software sources before execution, and harden identity and egress controls to contain post compromise activity.

ADGM THREAT INTELLIGENCE SUMMARY

New A0Backdoor Campaign Targets Financial Services via Teams Impersonation [Campaign] [High]

OCRFix Botnet Campaign Utilizes BNB Smart Chain for C2 Infrastructure [Campaign] [High]

Phishing Campaign Exploits OAuth Redirection Mechanisms to Deliver Malware [Campaign] [High]

Signed Malware Campaign Targets Workplace Applications to Deploy RMM Backdoors [Campaign] [High]

BoryptGrab Campaign Targets Windows Users via Deceptive GitHub Pages [Campaign] [High]

Middle East Conflict Themed Threat Surge Targets GCC and Beyond [Campaign] [High]

MuddyWater Campaign Targets MENA with Custom C2 Frameworks [Campaign] [High]

New Coruna Exploit Kit Targets iOS Devices with Advanced Exploitation Techniques [Campaign] [Medium]

North Korean APT Campaign Deploys DEV#POPPER RAT and OmniStealer via Weaponized GitHub Repositories [Campaign] [Medium]

MAAS VIP_Keylogger Campaign Targets Users with Sophisticated Spear-Phishing Techniques [Campaign] [Medium]

Critical Vulnerabilities in Cisco Secure Firewall Management Center Software [Vulnerability] [High]

Google Chrome Vulnerabilities Could Allow Arbitrary Code Execution [Vulnerability] [High]

Multiple Vulnerabilities Disclosed in AWS-LC Cryptographic Library [Vulnerability] [High]

High-Severity Path Traversal Vulnerability in Nessus Manager Exposes Operating System Files [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
New A0Backdoor Campaign Targets Financial Services via Teams Impersonation	HIGH	CLEAR	Campaign	Open Source

Executive Summary

BlueVoyant Security Operations Center has identified a new campaign leveraging email bombing and IT-support impersonation through Microsoft Teams to deploy a backdoor dubbed A0Backdoor. The attack begins with adversaries flooding victims' inboxes with spam, followed by impersonation tactics to gain remote access via Quick Assist, allowing for deeper infiltration into the victim's system.

This campaign may impact organizations within the financial services sector, as it has been observed targeting professionals at financial institutions. The use of social engineering techniques, alongside the deployment of a sophisticated backdoor, highlights the need for financial organizations to remain vigilant against evolving threats that blend into enterprise infrastructure.

Technical Details

- The campaign initiates with email flooding, followed by impersonation via Microsoft Teams to request Quick Assist access.
- Once access is granted, adversaries sideload a malicious DLL to establish the A0Backdoor.
- The backdoor employs anti-sandbox evasion techniques to hinder detection and analysis.
- Command-and-control (C2) communications utilize a covert DNS mail exchange-based channel, limiting direct traffic to trusted resolvers.
- The malware is delivered through digitally signed MSI packages, complicating detection efforts.
- The A0Backdoor uses runtime decryption to obscure its core functionality and evade static analysis.
- It establishes communication with its C2 infrastructure via DNS tunneling, avoiding direct connections to attacker-controlled servers.
- The malware crafts unique subdomains for each request, minimizing caching and detection risks.
- The actors have been observed using previously registered domains to blend in with legitimate traffic.
- Victimology indicates a focus on the finance and health sectors, leveraging open-source reconnaissance for targeted attacks.

Recommendations

- Implement multi-factor authentication (MFA) for remote access tools to enhance security.
- Conduct regular training for employees on recognizing social engineering tactics, particularly via email and messaging platforms.

- Monitor for unusual email activity and implement filtering to reduce spam exposure.
- Review and restrict permissions for remote assistance applications like Quick Assist.
- Regularly audit and update software packages to ensure only legitimate applications are installed.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – MuddyWater APT 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
OCRFix Botnet Campaign Utilizes BNB Smart Chain for C2 Infrastructure	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified the OCRFix botnet, a sophisticated three-stage malware campaign that conceals its command and control (C2) infrastructure within BNB Smart Chain testnet smart contracts. The botnet employs a ClickFix phishing technique to lure victims into executing a PowerShell command, which initiates the infection process without requiring binary updates for subsequent stages. Each stage of the botnet is designed to perform specific functions, including downloading additional payloads, privilege escalation, and maintaining persistence on infected systems.

This campaign may impact organizations in the financial services sector, particularly those involved in blockchain and virtual asset management. The use of legitimate blockchain nodes for C2 communications complicates detection efforts, making it crucial for financial institutions to remain vigilant against such evolving threats that leverage advanced obfuscation techniques and blockchain technology.

Technical Details

- The OCRFix botnet operates in three stages, with each stage querying BNB Smart Chain contracts to retrieve the current C2 domain.
- Initial access is gained through a ClickFix phishing lure that prompts users to execute a PowerShell command via a fake CAPTCHA.
- The botnet's payloads are compiled using VBSEdit and obfuscated with various arithmetic expressions, making detection challenging.
- Stage 1 acts as a downloader, retrieving further payloads from the resolved C2 URL.
- Stage 2 is responsible for privilege escalation and establishing persistence through scheduled tasks.
- Stage 3 functions as a bot that checks in every 60 seconds to receive commands from the operator.
- The botnet rotates its C2 infrastructure frequently, utilizing blockchain transactions to update contract storage.

- Detection requires inspecting JSON-RPC response bodies for hex-encoded URLs, as traditional domain blocking methods are ineffective.
- The campaign has been observed to use legitimate high traffic blockchain nodes, complicating defensive measures.
- The bot employs anti-forensics techniques to delete older files, enhancing its stealth capabilities.

Recommendations

- Implement network monitoring solutions that can inspect JSON-RPC response bodies for potential malicious indicators.
- Educate employees on recognizing phishing attempts, particularly those involving fake CAPTCHAs and PowerShell commands.
- Enforce strict access controls and privilege management to limit the impact of potential privilege escalation attempts.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by such malware.
- Utilize endpoint detection and response (EDR) solutions to identify and respond to suspicious activities on endpoints.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – OCRFix Botnet 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
Phishing Campaign Exploits OAuth Redirection Mechanisms to Deliver Malware	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Microsoft Defender Security Research Team has identified a phishing campaign that exploits OAuth's redirection functionalities to deliver malware. This campaign targets various sectors, including government and public organizations, using crafted URLs to redirect victims to malicious sites without the need for token theft. The attackers utilize familiar authentication flows to deceive users into engaging with their phishing links.

The implications of this campaign may impact organizations in the financial services sector, as the techniques employed can bypass conventional phishing defenses. Financial institutions should be aware of the potential for similar tactics being used against their clients, leading to unauthorized access and data breaches.

Technical Details

- The attack begins with the creation of a malicious application configured with a redirect URI pointing to a malware-hosting domain.
- Attackers distribute phishing links that prompt targets to authenticate with the malicious application, leveraging user familiarity with OAuth flows.
- Phishing emails often contain themes related to e-signatures, social security, and financial matters to entice recipients to click the links.
- The OAuth redirection technique is used to embed crafted URLs into phishing lures, allowing attackers to manipulate user redirection paths.
- Attackers exploit OAuth's error handling by using invalid parameters to trigger silent redirects to attacker-controlled pages.
- Once redirected, users may encounter phishing frameworks like EvilProxy designed to intercept credentials and session cookies.
- The campaign includes the use of fake calendar invites and meeting-related messaging to enhance the legitimacy of the phishing attempts.
- After redirection, victims may be sent to download malicious payloads, including ZIP files containing executable scripts.
- The downloaded files execute PowerShell commands for host reconnaissance and establish connections to external command and control (C2) endpoints.
- The campaign highlights the operational abuse of OAuth standards, emphasizing the need for enhanced security measures against identity-based threats.

Recommendations

- Organizations should closely govern OAuth applications by limiting user consent and regularly reviewing application permissions.
- Implement identity protection and Conditional Access policies to mitigate risks associated with OAuth redirection abuse.
- Enhance email security measures to detect and block phishing attempts that utilize OAuth URLs.
- Conduct regular training for employees to recognize phishing attempts and suspicious authentication requests.
- Monitor for unusual OAuth activity and establish alerts for potential phishing indicators within the organization.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Signed Malware Campaign Targets Workplace Applications to Deploy RMM Backdoors	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Microsoft Defender Experts have identified multiple phishing campaigns attributed to an unknown threat actor, utilizing workplace meeting lures and counterfeit PDF attachments to deliver signed malware. The malware, disguised as legitimate software, is digitally signed with an Extended Validation certificate from TrustConnect Software PTY LTD, enabling the attacker to install remote monitoring and management (RMM) tools for persistent access on compromised systems.

The implications of this campaign may impact organizations in the financial services sector, as the use of familiar branding and trusted digital signatures can bypass user suspicion. Financial institutions should be aware of the potential risks associated with such tactics, as they could lead to unauthorized access and data breaches within their environments.

Technical Details

- The campaign employs phishing emails that direct users to download malicious executables masquerading as legitimate applications.
- Malicious files include "msteams[.]exe", "trustconnectagent[.]exe", and "adobereader[.]exe", all signed with a certificate from TrustConnect Software PTY LTD.
- Once executed, the malware installs RMM tools like ScreenConnect, Tactical RMM, and Mesh Agent to establish persistent access.
- Attackers use counterfeit PDF attachments that redirect users to spoofed download pages for malicious software.
- Phishing emails also mimic legitimate meeting requests, prompting users to download software disguised as Teams or Zoom applications.
- The malware creates a Windows service to ensure stealthy execution during system startup and establishes a connection to a Command and Control (C2) domain.
- The campaign utilizes encoded PowerShell commands to download additional payloads from attacker-controlled infrastructure.
- Multiple RMM frameworks are deployed to ensure redundancy and maintain access even if one mechanism is detected.
- The persistence strategy involves embedding malicious registry entries to facilitate ongoing remote access.
- The use of revoked certificates for executables indicates a deliberate attempt to obfuscate malicious activity.

Recommendations

- Implement Windows Defender Application Control or AppLocker to block unapproved IT management tools.
- Enforce multifactor authentication (MFA) for approved RMM systems to enhance security.
- Regularly search for unapproved RMM software installations and reset passwords for any compromised accounts.
- Activate cloud-delivered protection in Microsoft Defender Antivirus to cover evolving threats.
- Utilize Safe Links and Safe Attachments in Microsoft Defender for Office 365 to mitigate phishing risks.

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
BoryptGrab Campaign Targets Windows Users via Deceptive GitHub Pages	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Trend Micro have identified the BoryptGrab campaign, which utilizes fake SEO-optimized GitHub repositories to distribute a data-stealing malware family targeting Windows users. The malware, known as BoryptGrab, is capable of harvesting sensitive information such as browser data, cryptocurrency wallet details, and system information, while also delivering a reverse SSH backdoor known as TunnesshClient.

This campaign is particularly relevant to organizations in the financial services sector as it highlights the increasing sophistication of cyber threats that exploit trust in legitimate platforms. The use of deceptive download pages and the ability to capture sensitive financial data may impact institutions that handle customer information and digital assets, necessitating heightened awareness and proactive security measures.

Technical Details

- The BoryptGrab malware is distributed through numerous public GitHub repositories masquerading as legitimate software tools.
- The infection chain begins when a ZIP file is downloaded from a fake GitHub page, often containing malicious executables.
- The malware is capable of harvesting browser data, cryptocurrency wallet information, and system details, along with capturing screenshots and extracting passwords.

- TunnesshClient, a backdoor delivered during the attack, establishes a reverse SSH tunnel to facilitate communication with the attacker.
- The campaign employs various techniques, including DLL side-loading and VBS scripts, to download and execute payloads.
- The malware's code includes Russian-language comments and log messages, suggesting a possible origin for the threat actor.
- BoryptGrab can dynamically stage payloads and bypass analysis through anti-VM and anti-debug checks.
- The malware collects data from multiple browsers and cryptocurrency wallet applications, targeting specific directories.
- After data collection, BoryptGrab archives and uploads the stolen information to the attacker's server.
- The campaign's reliance on fake GitHub repositories underscores a trend of exploiting trust in open-source ecosystems.

Recommendations

- Financial institutions should implement strict monitoring of software downloads and ensure that only verified applications are used.
- Organizations should educate employees about the risks of downloading software from unofficial sources, particularly GitHub.
- Employ endpoint protection solutions that can detect and block malicious payloads associated with this campaign.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by malware.
- Consider implementing multi-factor authentication (MFA) to protect sensitive accounts and data from 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
Middle East Conflict Themed Threat Surge Targets GCC and Beyond	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Zscaler ThreatLabz have uncovered a rise in cyber activity linked to ongoing tensions in the Middle East, particularly targeting the GCC region. This campaign employs conflict-themed lures to deliver backdoors, distribute malware, and execute phishing schemes impersonating government and payment services, posing a significant risk to entities in the UAE.

The implications for the financial services sector are noteworthy, as organizations may face increased threats from credential theft, remote access attacks, and fraud losses through fake donation drives and storefronts. Sectors with high public trust, including finance and e-commerce, should be particularly vigilant against social-engineering tactics that exploit regional narratives.

Technical Details

- A surge of over eight thousand newly registered conflict-themed domains has been observed, many of which are poised for malicious use.
- The campaign includes multiple concurrent operations, such as a targeted GCC operation using conflict-themed archives and a separate chain linked to Mustang Panda delivering the LOTUSLITE backdoor.
- Phishing schemes have been identified that replicate government and toll-payment portals, as well as fraudulent donation drives and storefronts.
- In one method, a compressed archive fetched a compiled help file that displayed a decoy document while launching a legitimate executable to sideload a malicious library.
- Persistence was established through user-level autorun, with the loader decrypting embedded shellcode and executing it in memory.
- Mustang Panda's operation involved pairing a legitimate multimedia executable with a malicious library for DLL sideloading, achieving persistence through autorun settings.
- The StealC information stealer was delivered via device-aware JavaScript on fake news blogs, redirecting victims to a password-protected archive.
- A fraudulent government service portal attempted to push a legitimate remote monitoring tool for remote access, while a fake toll-payment site harvested victim details.
- The campaigns reflect a mix of traditional cybercrime techniques with opportunistic fraud, leveraging the current news cycle for exploitation.

Recommendations

- Harden initial access paths by inspecting all web and email traffic inline, including encrypted sessions, to disrupt archive-based lures and staged payload retrieval.
- Constrain sideloading and persistence through application control, blocking unauthorized library loading, and alerting on suspicious autorun additions.
- Tighten identity defenses with strong multi-factor authentication and least-privilege access to limit post-compromise movement.
- Counter social-engineering tactics by enhancing security awareness regarding conflict-themed lures and controlling downloads of remote management tools.
- Continuously test and monitor defenses using deception techniques and third-party risk assessments, focusing on newly registered conflict-themed domains.

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
MuddyWater Campaign Targets MENA with Custom C2 Frameworks	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at "Ctrl Alt Intel" have exposed a campaign attributed to MuddyWater, revealing operational artifacts and infrastructure linked to espionage activities. The campaign utilizes multiple custom command-and-control (C2) frameworks and targets various regions, indicating a significant threat to organizations in the area.

The implications of this campaign may impact organizations in the financial services sector, particularly due to the targeting of critical services and commercial enterprises. With the use of advanced techniques for reconnaissance, initial access, and data exfiltration, financial institutions should be aware of the potential risks associated with internet-facing systems and the need for robust security measures.

Technical Details

- The campaign employs three custom C2 frameworks: "KeyC2" (Python-based UDP controller), "PersianC2" (web-polled platform), and "ArenaC2" (HTTP-based framework).
- The C2 infrastructure includes a botnet that resolves commands via Ethereum smart contracts, enhancing evasion techniques.
- Initial access methods involve broad scanning and exploitation of known vulnerabilities, including two novel SQL injection flaws.
- The actor utilized password spraying against enterprise email and mail gateways to gain access.
- Post-exploitation tactics included automated privileged account creation and persistence on network devices.
- Exfiltration methods featured multiple channels, including lightweight HTTP file receivers and cloud storage services.
- Stolen data sets comprised travel, identity, and legal/financial documents, indicating a focus on sensitive information.
- Researchers noted the rapid weaponization of public proof-of-concepts (PoCs) and diversified exfiltration techniques.
- The operation underscores a persistent espionage threat that necessitates disciplined exposure management and behavior-based detections.

Recommendations

- Prioritize remediation of known vulnerabilities while enforcing compensating WAF/virtual patches.
- Alert on suspicious admin creation and configuration changes on edge devices to detect exploit-to-persistence flows.

- Enforce least-privilege outbound access and monitor for anomalous WebSocket and blockchain traffic from endpoints.
- Implement strong MFA and lockout policies for enterprise mail and authentication endpoints to harden identity surfaces.
- Instrument DLP and egress monitoring for bulk transfers to cloud storage and scrutinize unauthorized tools used for data movement.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – MuddyWater 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
New Coruna Exploit Kit Targets iOS Devices with Advanced Exploitation Techniques	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Google Threat Intelligence Group has identified a new exploit kit named "Coruna" that targets Apple iPhone models running iOS versions from 13.0 to 17.2.1. This exploit kit comprises five full iOS exploit chains and utilizes sophisticated exploitation techniques, including non-public methods and mitigation bypasses, making it particularly dangerous for affected devices.

The proliferation of the Coruna exploit kit highlights the growing sophistication of cyber threats, particularly those targeting financial information. Organizations in the financial services sector should be aware of this exploit kit's capabilities, as it may impact users accessing financial applications on vulnerable iOS devices, potentially leading to unauthorized access to sensitive financial data.

Technical Details

- The Coruna exploit kit contains five full iOS exploit chains and a total of 23 exploits targeting various iOS versions.
- Advanced exploitation techniques include non-public methods and mitigation bypasses, enhancing the kit's effectiveness.
- The exploit kit was initially observed in targeted operations by a surveillance vendor's customer before being used in broader campaigns.
- It has been deployed in watering hole attacks by the suspected Russian espionage group UNC6353.
- The kit is also linked to UNC6691, a financially motivated threat actor operating from China, indicating a market for "second hand" zero-day exploits.

- The exploit kit is designed to evade detection by bailing out if the device is in Lockdown Mode or if the user is in private browsing.
- It employs a unique cookie mechanism to generate resource URLs for its exploits, complicating detection efforts.
- The final payload, named PlasmaLoader, is capable of stealing financial information and can analyze text for sensitive keywords related to cryptocurrency.
- Communication with the command and control (C2) server is encrypted, and the payload can download additional modules for further exploitation.
- The exploit kit is ineffective against the latest iOS versions, emphasizing the importance of timely updates for users.

Recommendations

- Ensure all iOS devices are updated to the latest version to mitigate the risk of exploitation by the Coruna kit.
- Implement Lockdown Mode on devices where updates cannot be applied to enhance security.
- Educate users about the risks of accessing financial applications through untrusted websites, especially those related to cryptocurrency.
- Monitor network traffic for unusual patterns that may indicate exploitation attempts or communication with known C2 servers.
- Consider deploying endpoint protection solutions that can detect and block known exploit kits and their associated payloads.

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
North Korean APT Campaign Deploys DEV#POPPER RAT and OmniStealer via Weaponized GitHub Repositories	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

eSentire's Threat Response Unit (TRU) has identified a sophisticated campaign attributed to a North Korean state-sponsored APT group that utilizes the DEV#POPPER Remote Access Trojan (RAT) and OmniStealer malware. The attack begins with victims cloning a malicious GitHub repository disguised as an eCommerce platform, which triggers a multi-stage infection chain aimed at stealing sensitive credentials and compromising development environments.

This campaign may impact organizations in the financial services sector, particularly those involved in software development and cryptocurrency transactions. The use of weaponized repositories highlights the need for heightened security awareness and proactive measures to prevent supply chain attacks that could lead to significant data breaches and financial loss.

Technical Details

- The attack chain initiates when a victim clones a malicious GitHub repository named "ShoeVista" and launches its frontend application.
- A hidden malicious script is triggered, leading to the deployment of DEV#POPPER RAT and OmniStealer through multiple obfuscated stages.
- The malware targets cryptocurrency wallets and developers, aiming to steal source code credentials, API keys, and sensitive data.
- Initial access is facilitated by a Node.js-based backdoor embedded in the repository's configuration file.
- The malware employs various anti-analysis techniques to evade detection and complicate reverse engineering efforts.
- Communication with command and control (C2) servers is established to exfiltrate sensitive data and retrieve additional payloads.
- DEV#POPPER RAT utilizes persistent C2 communications and can operate across multiple operating systems, including macOS, Windows, and Linux.
- The OmniStealer component specifically targets credentials stored in browsers and cryptocurrency applications, exfiltrating them to the threat actor's C2.
- The malware's obfuscation techniques include RC4 encryption and base64 encoding, making it difficult to analyze and detect.

Recommendations

- Organizations should block access to crypto-network APIs that may be used for malware payload staging.
- Developers must verify the authenticity of repositories and audit code before execution, especially from untrusted sources.
- Implement a Phishing and Security Awareness Training (PSAT) program to educate employees on recognizing potential threats.
- Partner with a Managed Detection and Response (MDR) provider for continuous threat monitoring and rapid incident response.
- Utilize Next-Gen AV or Endpoint Detection and Response (EDR) solutions to enhance threat detection capabilities.

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
MAAS VIP_Keylogger Campaign Targets Users with Sophisticated Spear-Phishing Techniques	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at K7 Labs have identified a campaign utilizing spear-phishing emails to distribute a malicious executable disguised as a purchase order. The executable, when executed, extracts and runs the VIP_Keylogger in memory, evading detection by not writing to disk. This campaign has been observed targeting multiple countries with variations in its delivery method and execution flow.

The implications of this campaign may impact organizations in the financial services sector, as the VIP_Keylogger is capable of capturing sensitive information such as login credentials, credit card details, and other personal data from various applications. Financial institutions should be aware of the potential risks associated with this type of malware, particularly given the sophisticated social engineering tactics employed to lure victims.

Technical Details

- The campaign employs spear-phishing emails that trick users into opening a RAR file containing a malicious executable.
- The executable is named similar to "*******_xlsx[.]exe" and executes the VIP_Keylogger directly in memory.
- In one case, a ".NET" PE file uses steganography to hide two DLLs, which are then used to retrieve the final payload.
- The APIs used for process hollowing include functions from "Kernel32[.]dll" and Ntdll, such as `CreateProcessA` and `WriteProcessMemory`.
- Another variant contains AES encrypted payloads in its ".data" section, which are decrypted in memory to load the VIP_Keylogger.
- The keylogger captures sensitive data from various browsers and applications, converting it into an SQLite database for exfiltration.
- It extracts credentials from browsers like Chrome, Firefox, and email clients such as Outlook and Thunderbird.
- Information is exfiltrated through multiple channels, including SMTP and FTP, with one observed method using email for data transfer.
- Some features of the keylogger, such as AntiVM and ProcessKiller, are reportedly disabled, potentially indicating a developmental stage.
- The campaign highlights the use of social engineering techniques to spread sophisticated malware.

Recommendations

- Implement robust email filtering to detect and block spear-phishing attempts.

- Educate employees on recognizing phishing emails and the importance of verifying attachments.
- Utilize endpoint protection solutions that can detect and respond to suspicious executable behavior.
- Regularly update and patch software to mitigate vulnerabilities that could be exploited by malware.
- Monitor network traffic for unusual data exfiltration patterns, especially through SMTP channels.

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
Critical Vulnerabilities in Cisco Secure Firewall Management Center Software	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Cisco has identified two critical vulnerabilities in its Secure Firewall Management Center (FMC) software that could allow unauthenticated remote attackers to execute arbitrary scripts and Java code with root privileges. The vulnerabilities, CVE-2026-20079 and CVE-2026-20131, have been assigned a CVSS score of 10.0, indicating a critical risk level, with no available workarounds.

Organizations in the financial services sector should be aware that these vulnerabilities may impact their security posture, especially if Cisco FMC is deployed in their environments. Immediate action is recommended to mitigate exposure by upgrading to the latest fixed software releases and restricting network access to the management interface.

Technical Details

- CVE-2026-20079 allows an unauthenticated remote attacker to bypass authentication and execute arbitrary scripts with root privileges on the affected system.
- The vulnerability exploits improper system processes created at boot time, enabling attackers to bypass authentication via crafted HTTP requests.
- CVE-2026-20131 permits remote execution of arbitrary Java code due to insecure deserialization in the web management interface.
- Attackers can escalate privileges and compromise the entire system through this vulnerability.
- Both vulnerabilities are network-based and do not require authentication to exploit.
- The affected products include Cisco Secure FMC Software and Security Cloud Control (SCC) Firewall Management.
- ASA Software and FTD Software are not affected by these vulnerabilities.
- Limited exposure exists if the FMC web interface is not publicly accessible.

- Both vulnerabilities pose a critical risk to organizations utilizing Cisco's firewall management solutions.

Recommendations

- Upgrade affected Cisco FMC instances to the latest fixed versions as provided in the Cisco advisories.
- Limit access to the FMC management interface to trusted internal networks only.
- Implement network segmentation and firewall rules to prevent public access to the management interface.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Google Chrome Vulnerabilities Could Allow Arbitrary Code Execution	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Google has released security updates for the Chrome browser addressing multiple vulnerabilities, some rated as Critical. These vulnerabilities could enable attackers to execute arbitrary code or compromise affected systems if exploited. The vulnerabilities include integer overflows and object lifecycle issues that may pose risks to users and organizations relying on the browser for daily operations.

Organizations in the financial services sector should be aware of these vulnerabilities, as they could potentially impact the security of sensitive data and transactions. Keeping software updated is crucial to mitigate risks associated with such vulnerabilities, particularly in environments handling financial transactions and personal information.

Technical Details

- CVE-2026-3536: An integer overflow vulnerability in ANGLE could allow attackers to execute arbitrary code.
- CVE-2026-3537: An object lifecycle issue in PowerVR may lead to memory corruption if exploited.
- CVE-2026-3538: Another integer overflow vulnerability in Skia could compromise affected systems.
- CVE-2026-3539: An object lifecycle issue in DevTools has been identified as a high severity vulnerability.
- CVE-2026-3540: Inappropriate implementation in WebAudio could result in security risks.
- CVE-2026-3541: An inappropriate implementation in CSS may lead to potential exploitation.
- CVE-2026-3542: Similar issues in WebAssembly could allow for security breaches.
- CVE-2026-3543: An inappropriate implementation in V8 poses additional risks to users.
- CVE-2026-3544: A heap buffer overflow in WebCodecs could allow for arbitrary code execution.

- CVE-2026-3545: Insufficient data validation in Navigation may expose users to security threats.

Recommendations

- Update Google Chrome to the latest version to mitigate vulnerabilities.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities Disclosed in AWS-LC Cryptographic Library	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Amazon Web Services has disclosed multiple vulnerabilities in the AWS-LC cryptographic library, which is utilized by various AWS services and applications. Exploitation of these vulnerabilities could allow attackers to bypass critical certificate and signature validation mechanisms, potentially leading to unauthorized access or data manipulation.

The impact of these vulnerabilities may affect organizations in the financial services sector that rely on AWS for secure transactions and data integrity. Financial institutions should be aware of the potential risks associated with these vulnerabilities and take appropriate measures to mitigate any possible exploitation.

Technical Details

- CVE-2026-3336: An improper certificate validation vulnerability may allow attackers to bypass certificate chain verification when processing PKCS7 objects with multiple signers.
- CVE-2026-3337: Timing discrepancies during AES-CCM decryption could enable attackers to infer authentication tag validity through timing analysis, posing a risk of unauthorized access.
- CVE-2026-3338: An improper signature validation vulnerability may allow attackers to bypass signature verification when processing PKCS7 objects with authenticated attributes.
- The vulnerabilities are categorized as high severity, indicating a significant risk if exploited.
- These vulnerabilities could be exploited in scenarios where secure communications are critical, such as financial transactions.
- The AWS-LC library is widely used across various AWS services, increasing the potential attack surface.
- Attackers may leverage these vulnerabilities to perform man-in-the-middle attacks or data tampering.
- The vulnerabilities highlight the importance of robust validation mechanisms in cryptographic libraries.

Recommendations

- Update the AWS-LC cryptographic library to the latest version as recommended by AWS.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Path Traversal Vulnerability in Nessus Manager Exposes Operating System Files	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Tenable has released security updates for Nessus Manager addressing a high-severity path traversal vulnerability, tracked as CVE-2026-3493. This vulnerability allows an authenticated remote attacker to read arbitrary operating system files on affected installations, posing a risk to sensitive data and system integrity. Organizations using Nessus Manager versions 10.10.2 and earlier, as well as versions 10.11.0 through 10.11.2, are particularly vulnerable to this issue.

The financial services sector should be aware of this vulnerability as it may impact the security posture of organizations utilizing Nessus Manager for vulnerability management. The ability to read arbitrary files could potentially lead to further exploitation or data breaches, making it essential for institutions to prioritize the upgrade to the latest or fixed version of the software.

Technical Details

- The vulnerability is identified as CVE-2026-3493 and has a high severity rating.
- It falls under the CWE classification of CWE-35, which pertains to path traversal vulnerabilities.
- Affected products include Nessus Manager versions 10.10.2 and earlier, as well as versions 10.11.0 through 10.11.2.
- An authenticated remote attacker can exploit this vulnerability to read arbitrary operating system files.
- Successful exploitation could lead to unauthorized access to sensitive information stored on the system.
- The vulnerability underscores the importance of maintaining up-to-date software to mitigate security risks.

Recommendations

- Upgrade Nessus Manager to the latest or fixed version as recommended by Tenable.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

New A0Backdoor Campaign Targets Financial Services via Teams Impersonation

TACTIC	TECHNIQUE
Impact	T1667 Email Bombing
Execution	T1204.001 User Execution: Malicious Link
Persistence	T1574.002 Hijack Execution Flow: DLL Side-Loading
Defense Evasion	T1116 Code Signing
Defense Evasion	T1027.002 Obfuscated Files or Information: Software Packing
Defense Evasion	T1497 Virtualization/Sandbox Evasion
Defense Evasion	T1140 Deobfuscate/Decode Files or Information
Command and Control	T1071.004 Application Layer Protocol: DNS
Discovery	T1082 System Information Discovery
Defense Evasion	T1480.001 Execution Guardrails: Environmental Keying
Defense Evasion	T1027.009 Obfuscated Files or Information: Embedded Payloads
Command and Control	T1572 Protocol Tunneling
Command and Control	T1105 Ingress Tool Transfer
Command and Control	T1132.002 Data Encoding: Non-Standard Encoding
Defense Evasion	T1622 Debugger Evasion

OCRFix Botnet Campaign Utilizes BNB Smart Chain for C2 Infrastructure

TACTIC	TECHNIQUE
Initial Access	T1566 Phishing
Execution	T1204.004 Malicious copy/paste
Execution	T1059.001 PowerShell
Execution	T1059.005 Visual Basic
Defense Evasion	T1218.007 Msiexec

Execution	T1047 WMI
Execution	T1053.005 Scheduled task
Privilege Escalation	T1548.002 UAC bypass
Defense Evasion	T1562.001 Impair defences
Defense Evasion	T1027 Obfuscated files
Defense Evasion	T1140 Deobfuscate/decode
Discovery	T1033 System owner discovery
Command and Control	T1071.001 Web protocols
Command and Control	T1102 Web service
Command and Control	T1105 Ingress tool transfer
Defense Evasion	T1070.004 File deletion

MuddyWater Campaign Targets MENA with Custom C2 Frameworks

TACTIC	TECHNIQUE
Reconnaissance	T1595.002 Active Scanning: Vulnerability Scanning
Reconnaissance	T1590.002 Gather Victim Network Information: DNS
Reconnaissance	T1595.003 Active Scanning: Wordlist Scanning
Resource Development	T1583.003 Acquire Infrastructure: Virtual Private Server
Resource Development	T1587.001 Develop Capabilities: Malware
Resource Development	T1588.005 Obtain Capabilities: Exploits
Resource Development	T1588.002 Obtain Capabilities: Tool
Initial Access	T1190 Exploit Public-Facing Application
Initial Access	T1110.003 Brute Force: Password Spraying
Initial Access	T1110.001 Brute Force: Password Guessing
Discovery	T1082 System Information Discovery
Execution	T1059.001 Command and Scripting Interpreter: PowerShell
Execution	T1059.007 Command and Scripting Interpreter: JavaScript

Execution	T1059.003 Command and Scripting Interpreter: Windows Command Shell
Persistence	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys
Persistence	T1505.003 Server Software Component: Web Shell
Persistence	T1136.001 Create Account: Local Account
Defense Evasion	T1027 Obfuscated Files or Information
Defense Evasion	T1140 Deobfuscate/Decode Files or Information
Command and Control	T1071.001 Application Layer Protocol: Web Protocols
Command and Control	T1095 Non-Application Layer Protocol
Command and Control	T1102.001 Web Service: Dead Drop Resolver
Command and Control	T1571 Non-Standard Port
Command and Control	T1573.001 Encrypted Channel: Symmetric Cryptography
Command and Control	T1090.002 Proxy: External Proxy
Exfiltration	T1041 Exfiltration Over C2 Channel
Exfiltration	T1567 Exfiltration Over Web Service
Exfiltration	T1048 Exfiltration Over Alternative Protocol
Collection	T1005 Data from Local System

Appendix B – Threat Severity Ratings & Definitions

In this newsletter, each campaign, breach, and vulnerability has been assigned a severity level—High, Medium, or Low—based on a contextual assessment of its impact, relevance to the financial sector, regional exposure, and exploit status.

A **High** severity rating is assigned to threats that involve widely used technologies, nation-state actors, or actively exploited zero-day vulnerabilities. These incidents pose a significant risk due to their potential for widespread disruption, data compromise, and strategic targeting of core infrastructure.

A **Medium** severity rating reflects threats that are technically impactful but have limited regional exposure or affect less prominent entities. These may include ransomware attacks on mid-sized firms, blockchain-based malware delivery mechanisms, or smart contract exploits in DeFi platforms.

A **Low** severity rating is applied to threats that are peripherally related to the financial sector, have no confirmed impact in the region, or target non-critical systems. These include credential stuffing attacks on platforms outside the MENA region or supply chain breaches that have not yet affected local infrastructure.

Threat Score Ratings & Definitions

1. **Severe**: Widespread, high-impact attacks ongoing. Critical infrastructure affected by destructive malware or multiple zero-day exploits.
2. **High**: Confirmed breaches or coordinated campaigns in progress. High-impact threat actor activity and zero-day exploitation observed.
3. **Elevated**: Active exploitation of known vulnerabilities or targeted campaigns detected. Some breaches or zero-days may surface.
4. **Guarded**: Slight increase in malicious activity. Low-level campaigns or threat actor reconnaissance may be underway.
5. **Normal**: No significant cyber activity beyond baseline. No major breaches, campaigns, or zero-day activity observed.

Appendix C – Traffic Light Protocol (TLP) Definitions and Usage

TLP	When should it be used?	How should it be shared?
TLP:Red	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:Amber+Strict	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:Amber	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:Green	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible

		channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:Clear	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Appendix D - Acronyms & Technical Terms

Term / Acronym	Meaning / Description
.NET PE	Executable where a variant hid DLLs using steganography.
A0Backdoor	Backdoor deployed after email bombing and Teams based IT support impersonation that uses DLL sideloading and DNS based C2.
AES CCM	Authenticated encryption mode referenced in the timing issue.
AES encrypted payload	Payload stored in encrypted form and decrypted in memory.
ANGLE	Chrome graphics component with an integer overflow.
Anti debug checks	Logic that prevents or hinders debugging to hide malware behaviour.
Anti sandbox evasion	Malware logic that detects or avoids automated analysis environments.
Anti VM checks	Malware behaviour that avoids virtual machines used by analysts.
ArenaC2	HTTP based framework used by MuddyWater for command traffic.
Authentication bypass	Condition where an attacker can access a system without valid credentials.
Autorun persistence	Startup setting at user level that relaunches a loader after reboot.
AWS-LC	AWS cryptographic library with issues in certificate and signature validation and timing analysis.
Blockchain node	Legitimate blockchain endpoint leveraged to fetch data that points to attacker C2.
BlueVoyant SOC	Security Operations Center that identified the A0Backdoor campaign.
BNB Smart Chain testnet	Blockchain network used in the campaign to conceal C2 updates.
BoryptGrab	Data stealing malware spread via fake SEO optimized GitHub repositories.
Broad scanning	Wide Internet scanning to find and exploit exposed services.
C2	Command and Control infrastructure used by attackers to manage compromised hosts.
Certificate validation	Process that verifies a certificate chain which could be bypassed in AWS-LC.
Cisco Secure FMC	Firewall management software with critical flaws that allow root level code execution.
ClickFix phishing	Lure that convinces users to run a PowerShell command often behind a fake CAPTCHA.
Cloud storage exfiltration	Sending stolen data to cloud storage services controlled by attackers.
Conditional Access	Policy control advised to restrict risky authentication and OAuth activity.
Coruna exploit kit	iOS exploit kit with five full chains and many exploits that target versions 13.0 to 17.2.1.
CreateProcessA	API called to start a process that will be hollowed.
Cryptocurrency wallet data	Information targeted by stealers such as keys and stored wallet details.
CSC	UAE Cyber Security Council
CSS	Style component with an inappropriate implementation issue.
Ctrl Alt Intel	Research group that exposed MuddyWater operations and tooling.
CVE 2026 3493	Identifier for the Nessus Manager path traversal vulnerability.

CWE 35	Classification for path traversal vulnerabilities.
DEV#POPPER RAT	Remote Access Trojan delivered after a malicious repository is cloned and launched.
Device aware JavaScript	Script that checks device traits before delivering a payload such as StealC.
DevTools	Developer tools component with a high severity lifecycle issue.
Digitally signed MSI	Installer package signed to appear legitimate that is used to deliver malware.
DLL sideloading	Loading a malicious library through a trusted executable to run attacker code quietly.
DNS MX based channel	C2 traffic that hides inside DNS mail exchange lookups to blend with normal resolver activity.
DNS tunneling	Using DNS queries and responses to carry hidden communications with attacker servers.
Email bombing	Flooding a user inbox with spam to create urgency and distract before social engineering.
Encoded PowerShell	Obfuscated PowerShell commands that fetch and run additional payloads.
Encrypted C2	Command traffic that is encrypted to hinder inspection.
eSentire TRU	Threat Response Unit that reported the DPRK linked repository campaign.
Ethereum smart contracts for C2	Use of contract storage to resolve commands and enhance evasion.
EvilProxy	Phishing framework used after redirection to intercept credentials and session cookies.
Exposure management	Discipline to reduce Internet facing risk and focus detections on behaviour.
Extended Validation certificate	High assurance code signing certificate used to make malware appear trustworthy.
Fake toll payment site	Phishing page that harvests victim details by mimicking payment portals.
Fraudulent donation drive	Scam site themed around conflict narratives used to steal money or data.
FTD Software	Cisco product noted as not affected by the FMC issues.
FTP	File transfer protocol used as another exfiltration path.
GCC	Gulf Cooperation Council region that saw a rise in conflict themed cyber activity.
Hex encoded URL	Indicator value encoded in hexadecimal inside JSON RPC responses for evasion.
HTTP file receiver	Lightweight service used to collect exfiltrated data over HTTP.
Insecure deserialization	Flaw in web management that allows remote execution of Java code.
JSON RPC	Protocol where response bodies may contain hex encoded URLs used to update C2 locations.
JSON RPC traffic monitoring	Network inspection recommended to spot malicious indicators in responses.
K7 Labs	Researchers who analysed the VIP_Keylogger campaign.
Kernel32.dll	Windows library whose functions were used during process hollowing.
KeyC2	Python based UDP controller used by MuddyWater.
Lockdown Mode	iOS setting that causes the kit to bail out and is advised when updates are not possible.
LOTUSLITE	Backdoor delivered through DLL sideloading with autorun based persistence.
Man in the middle	Attack where communications are intercepted or altered due to crypto flaws.
MDR	Managed Detection and Response provider for continuous monitoring and rapid response.
Mesh Agent	RMM agent used to establish remote control on compromised hosts.
MFA	Multi factor authentication recommended for remote tools and identity surfaces.
Microsoft Defender Experts	Team that analysed the signed malware and RMM deployment campaign.
Microsoft Teams impersonation	Attackers pose as support staff in Teams to request remote access from victims.
MuddyWater	Adversary group operating across the MENA region with custom C2 frameworks.
Mustang Panda	Actor linked to delivery of the LOTUSLITE backdoor in conflict themed operations.
Navigation	Component with insufficient data validation.
Nessus Manager	Vulnerability management product affected by a high severity path traversal issue.
Network device persistence	Maintaining access by changing configurations on edge or network devices.

Newly registered domains	Focus area for monitoring due to surge in conflict themed registrations.
Node.js backdoor	Backdoor embedded in repository configuration that initiates the attack chain.
North Korean APT	State linked group that deployed DEV#POPPER RAT and OmniStealer via a weaponized repository.
Ntdll	Windows library used alongside Kernel32 in process hollowing.
OAuth error handling	Supplying invalid parameters to trigger silent redirects to attacker controlled pages.
OAuth redirection abuse	Use of crafted redirect URIs and error handling to send users to attacker pages without stealing tokens.
OCRFix botnet	Three stage malware that retrieves C2 details from BNB Smart Chain testnet smart contracts.
OmniStealer	Malware that targets credentials in browsers and cryptocurrency applications.
Password spraying	Trying common passwords across many accounts to gain access.
Path traversal	Issue that lets an authenticated attacker read arbitrary operating system files.
PersianC2	Web polled command framework used by MuddyWater.
Persistence	Methods that keep attacker access across reboots such as scheduled tasks or services.
PKCS7	Format where flaws allowed bypass of certificate or signature checks.
PlasmaLoader	Final payload in the kit that can steal financial information and analyse crypto related text.
PowerShell command	Script based execution used to download payloads and perform host actions.
PowerVR	Component with an object lifecycle issue that may cause memory corruption.
Private browsing	Browser mode that also causes the kit to bail out during checks.
Privilege escalation	Steps used by malware to gain higher permissions on a system.
Privileged account creation	Attacker step to add admin accounts after exploitation.
Process hollowing	Running malicious code inside a benign process using Windows APIs.
PSAT	Phishing and Security Awareness Training program to reduce user susceptibility.
Quick Assist	Remote assistance feature used by attackers to gain user granted access.
RAR file	Compressed archive used to package the malicious executable.
RC4 encryption	Obfuscation used within the campaign to protect data and payloads.
Redirect URI	Configured address in an OAuth app that attackers point to a malware hosting domain.
Registry persistence	Malicious registry entries that ensure continued execution after reboot.
Remote monitoring tool abuse	A fraudulent portal that attempts to push a legitimate tool for attacker access.
Reverse SSH tunnel	Connection that lets attackers reach a host from the outside by tunneling out.
Revoked certificate	Code signing certificate that has been invalidated but may still appear on malware.
RMM	Remote Monitoring and Management tools that attackers install for persistent remote access.
Runtime decryption	Technique where malware decrypts its code only when running to hinder static analysis.
Safe Attachments	Microsoft Defender for Office 365 feature to detect and block harmful files.
SCC Firewall Management	Security Cloud Control Firewall Management also affected alongside FMC.
ScreenConnect	RMM tool installed by the signed malware campaign to maintain access.
Session cookie	Browser token that maintains a logged in session and can be stolen for access.
Signature validation	Check that ensures content is signed correctly which could be bypassed.
Skia	Graphics library with an integer overflow vulnerability.
Smart contract	On chain storage used to hold or update values that direct malware to new C2.
SMTP	Email protocol used as one channel for exfiltrating stolen data.
Spear phishing	Targeted email that delivered a RAR archive with a disguised executable.
SQL injection	Input flaw used to gain initial access as noted in two novel cases.
SQLite database	Local database used by the keylogger to store captured data before exfiltration.

Steganography	.NET variant hid two DLLs inside another file to evade inspection.
Tactical RMM	RMM framework deployed to provide redundancy and persistence.
Tenable	Vendor that released updates for the Nessus Manager flaw.
Timing analysis	Observation of time differences during AES CCM decryption that can reveal tag validity.
TrustConnect Software PTY LTD certificate	Specific certificate observed signing the malicious executables.
TunnesshClient	Backdoor that opens a reverse SSH tunnel to attacker infrastructure.
UNC6353	Suspected Russian espionage group that used the kit in watering hole operations.
UNC6691	Financially motivated actor operating from China linked to second hand zero day use.
V8	JavaScript engine with an inappropriate implementation issue.
VBS script	Script used in the infection chain to stage and execute payloads.
VBSEdit	Utility referenced in compiling payloads that contributes to obfuscation in the botnet.
VIP_Keylogger	Keylogger executed in memory from a purchase order themed spear phishing lure.
WAF or virtual patch	Compensating control recommended while fixing known vulnerabilities.
Watering hole attack	Compromise of a site visited by targets to deliver exploits and payloads.
Weaponized GitHub repository	Project that hides backdoors and scripts which trigger a multistage infection.
WebAssembly	Execution component with identified risks in implementation.
WebCodecs	Media component with a heap buffer overflow.
WebSocket traffic monitoring	Detection focus for anomalous outbound connections tied to custom C2.
Windows service	Background service created by malware so it starts at boot without user action.
WriteProcessMemory	API used to place malicious code into the target process.
Zscaler ThreatLabz	Research team that reported the conflict themed surge and related tactics.