TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	14/1/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 14 January 2026

2	0	8	9
Cyber Breach	**Threat Actors**	**Campaigns**	**Vulnerability**
Major Compromises and breaches	Threat actor activities in the UAE & Middle East impacting Finance Sector	Recent Threat campaigns within financial institutions	Actively Exploited & Critical Vulnerabilities

Summary

This week's cybersecurity newsletter highlights a series of significant threats and vulnerabilities impacting the financial services sector, particularly within the realms of cryptocurrency, data protection, and software security. Key incidents include a $26 million exploit of the Truebit blockchain protocol, a data breach at Ledger affecting customer information, and a spear-phishing campaign by the Muddy Water APT group utilizing advanced malware. Additionally, multiple critical vulnerabilities were identified in widely used software, including Microsoft PowerPoint and Veeam Backup & Replication, posing risks of remote code execution and data breaches. The implications for the financial sector are profound, underscoring the urgent need for enhanced security measures, including robust incident response protocols, regular software updates, and comprehensive employee training on phishing and credential protection. Organizations must prioritize patching known vulnerabilities and strengthening third-party vendor risk management to safeguard sensitive data and maintain operational integrity.

ADGM THREAT INTELLIGENCE SUMMARY

High-Severity Vulnerability in Forcepoint One DLP Client Allows Code Execution [Vulnerability] [Medium]

High-Severity Privilege Escalation Vulnerability in Tenable Nessus Agent on Windows [Vulnerability] [Medium]

Critical Vulnerability in jsPDF Allows Remote File Access [Vulnerability] [Medium]

High-Severity Vulnerability in Google Chrome WebView Could Bypass Security Policies [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Truebit Suffers $26 Million Exploit, TRU Token Collapses	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

Truebit, a blockchain verification protocol, experienced a significant security breach resulting in the loss of approximately $26 million. The attacker drained around 8,500 Ether (ETH) from a smart contract, leading to a complete collapse of the TRU token's value within 24 hours. The stolen funds were transferred to two wallet addresses, linking the attacker to previous exploits.

The incident highlights the severe impact of cyber breaches on the financial services sector, particularly in the cryptocurrency space. With nearly 80% of hacked projects failing to recover their full value, the Truebit hack serves as a stark reminder of the potential long-term damage to trust and liquidity in the market, exacerbating the ongoing challenges faced by the industry.

Technical Details

- The exploit involved draining approximately 8,500 Ether (ETH) from a smart contract associated with Truebit.
- The total financial loss from the hack is estimated at around $26.4 million.
- The stolen funds were sent to two separate wallet addresses, indicating a planned extraction.
- The attacker has been linked to a prior exploit involving another project, Sparkle, occurring shortly before the Truebit incident.
- Following the breach, the TRU token experienced a 100% drop in value within a single day.
- CoinGecko flagged Truebit with an exploit warning due to the drastic market value loss.
- The broader cryptocurrency industry has suffered over $90 billion in losses from hacks and scams, with minimal recovery.
- Security experts warn that hacks can lead to lasting damage, as users often abandon compromised projects.
- The incident follows a reported 60% decrease in exploits in December 2025 compared to November.
- The Truebit hack is noted as the first major crypto exploit of 2026.

Recommendations

- Implement robust smart contract audits to identify vulnerabilities before deployment.

- Enhance monitoring of wallet addresses associated with known exploits to prevent fund transfers.
- Educate users on security practices to safeguard their assets and maintain confidence in the platform.
- Establish incident response protocols to quickly address breaches and communicate transparently with stakeholders.
- Collaborate with blockchain security firms for ongoing assessments and threat intelligence sharing.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Ledger Confirms Customer Data Exposure in Global-e Security Breach	**MEDIUM**	**CLEAR**	**Cyber Breach**	**Open Source**

Executive Summary

Ledger, a French hardware wallet maker, has reported a data breach involving customer information due to an incident at Global-e, an e-commerce service provider. The breach primarily affected order data stored in Global-e's cloud infrastructure, impacting customers who purchased from Ledger.com using Global-e as the Merchant of Record.

This incident is significant for the financial services sector as it highlights vulnerabilities in third-party service providers, particularly in e-commerce. The exposure of personal order data, while not compromising sensitive financial information, raises concerns about potential phishing attempts targeting affected customers, which could further endanger their digital assets.

Technical Details

- The breach involved unauthorized access to order data on Global-e’s cloud infrastructure.
- Affected data includes personal information such as names, addresses, emails, and purchase details.
- Ledger confirmed that its own infrastructure, including hardware and software systems, remained secure.
- No private keys, seed phrases, or user wallets were compromised in the breach.
- Global-e has not publicly acknowledged the incident or issued a statement regarding the breach.
- Ledger was informed of the breach by Global-e and coordinated efforts to notify impacted users.
- Global-e serves as the Merchant of Record for various international retailers, managing payment processing and fulfillment.
- The full extent of the data accessed remains unclear, but Ledger emphasized the lack of access to cryptographic secrets.
- Customers were warned to be cautious of phishing attempts that may exploit the leaked data.
- Global-e has communicated directly with affected customers regarding the breach.

Recommendations

- Financial institutions should review and strengthen their third-party vendor risk management policies.
- Implement multi-factor authentication (MFA) for customer accounts to enhance security.
- Educate customers on recognizing phishing attempts and the importance of safeguarding personal information.
- Regularly monitor for unusual account activity and establish alert systems for potential breaches.
- Ensure that incident response plans are updated to address breaches involving third-party service providers.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Muddy Water APT Campaign Targets Financial Sector in the Middle East with RustyWater Implant	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

CloudSEK's TRIAD has identified a spear-phishing campaign attributed to the Muddy Water APT group, targeting various sectors in the Middle East, including financial entities. The campaign employs icon spoofing and malicious Word documents to deliver a Rust-based implant known as RustyWater, which enhances their operational capabilities significantly.

The introduction of RustyWater marks a notable evolution in Muddy Water's toolkit, moving away from traditional PowerShell and VBS loaders to more sophisticated Rust-based implants. This shift poses a heightened risk to the financial services sector, as the implant's capabilities allow for long-term persistence and dynamic post-access functionality, complicating detection and response efforts.

Technical Details

- The campaign utilizes spear-phishing emails with malicious attachments, specifically a document titled "Cybersecurity.doc."
- The RustyWater implant is capable of asynchronous command and control (C2) communication, enhancing stealth and operational efficiency.
- Initial access is achieved through user execution of the malicious Word document containing embedded macros.
- The implant employs anti-analysis and anti-debugging mechanisms to evade detection by security tools.

- RustyWater establishes persistence by modifying Windows registry keys for AutoStart on system boot.
- It uses layered encryption (JSON -> Base64 -> XOR) to obfuscate data before transmission to its C2 server.
- Malware can detect and evade over 25 antivirus products, significantly reducing the likelihood of detection.
- It implements randomized sleep intervals between C2 callbacks to further complicate traffic analysis.
- The implant's modular design allows for the addition of new functionalities without requiring new binaries.
- The campaign has demonstrated a high risk of long-term silent persistence, complicating incident response efforts.

Recommendations

- Monitor registry persistence mechanisms for anomalous writes to AutoStart locations, particularly in C:\ProgramData.
- Implement detection for layered C2 behaviors, focusing on unusual outbound HTTP traffic patterns.
- Hunt for memory allocation and thread manipulation events indicative of process injection techniques.
- Flag signed binaries executed from writable paths that subsequently load non-signed modules.
- Treat transitions from passive to active behaviors in RATs as potential indicators of compromise.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Muddy Water 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
GoBruteforcer Botnet Campaign Targets Financial Services with Weak Passwords and AI-Generated Defaults	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at Check Point have identified a campaign involving the GoBruteforcer botnet, which exploits weak passwords and AI-generated server defaults to compromise Linux servers. This botnet targets services such as FTP, MySQL, PostgreSQL, and phpMyAdmin, leveraging a modular structure to brute-force user

credentials and expand its reach across vulnerable systems. The campaign is particularly focused on databases associated with crypto and blockchain projects, indicating a financial motive behind the attacks.

The implications for the financial services sector are significant, as the botnet's ability to exploit misconfigured servers and weak credentials poses a serious risk to sensitive data and operational integrity. With over 50,000 internet-facing servers potentially vulnerable, financial institutions must prioritize securing their infrastructure against such automated threats, which exploit common vulnerabilities rather than relying on sophisticated techniques.

Technical Details

- GoBruteforcer is a modular botnet written in Go, designed to brute-force passwords for various services on Linux servers.
- The botnet spreads through a chain of web shell, downloader, IRC bot, and bruteforcer modules, allowing for extensive control over compromised hosts.
- The current campaign leverages AI-generated server deployment examples, leading to the use of common usernames and weak default passwords.
- More than 50,000 internet-facing servers are estimated to be vulnerable to GoBruteforcer attacks, particularly those running legacy web stacks like XAMPP.
- The botnet targets services such as FTP, MySQL, PostgreSQL, and phpMyAdmin, with a focus on databases related to crypto and blockchain projects.
- Attackers utilize a small, stable pool of weak passwords, rotating them frequently to maximize the chances of successful logins.
- The botnet employs an IRC-based command and control mechanism, allowing attackers to issue commands and updates to infected hosts.
- Successful brute-force attempts are reported back to the command and control server via HTTP requests.
- The botnet's modularity and use of weak credentials make it a persistent threat, capable of rapidly compromising large numbers of systems.
- The campaign highlights the need for improved security practices, including robust credential management and continuous exposure monitoring.

Recommendations

- Implement strong password policies and enforce multi-factor authentication for all internet-facing services.
- Regularly audit server configurations to ensure that default credentials are changed and unnecessary services are disabled.
- Utilize intrusion detection systems to monitor for unusual access patterns indicative of brute-force attacks.
- Conduct regular vulnerability assessments to identify and remediate misconfigured servers and exposed services.
- Educate staff on secure deployment practices, particularly when using automated tools or AI-assisted configurations.

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
Malicious NPM Packages Deliver NodeCordRAT Targeting Developers	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Zscaler ThreatLabz has identified three malicious NPM packages—bitcoin-main-lib, bitcoin-lib-js, and bip40—that deliver a remote access trojan (RAT) known as NodeCordRAT. This malware is designed to steal sensitive data, including Chrome credentials and MetaMask wallet information, and utilizes Discord for command-and-control communication. The malicious packages were disguised to resemble legitimate libraries within the bitcoinjs ecosystem, leading to several thousand downloads before their removal from the NPM database.

The emergence of NodeCordRAT highlights significant software supply chain vulnerabilities that can affect developers in the financial services sector. As these types of threats become more prevalent, financial institutions must remain vigilant against similar attacks that exploit trusted platforms and libraries, potentially leading to severe data breaches and financial losses.

Technical Details

- NodeCordRAT is deployed through NPM packages that execute a post install script to install the malicious payload.
- The attack flow involves downloading wrapper packages that require the malicious bip40 package, which contains the RAT.
- The malware uses Discord for command-and-control (C2) communication, establishing a private channel for the attacker.
- NodeCordRAT performs host fingerprinting to generate unique identifiers for compromised machines.
- It extracts sensitive data, including Chrome credentials and MetaMask wallet information, from the infected system.
- The malware can execute arbitrary shell commands and capture screenshots of the infected device.
- Data exfiltration occurs through Discord's API, sending stolen information as message attachments.
- The malicious packages were designed to appear credible by mimicking legitimate repositories.
- The post install script automates the execution of the RAT using Process Manager 2 (PM2) for persistence.
- The malware does not require user interaction to execute, making it particularly insidious.

Recommendations

- Implement strict code review processes for third-party libraries and dependencies in development environments.
- Educate developers on the risks of typo squatting and the importance of verifying package authenticity.
- Use application security tools to monitor and analyze NPM packages for known vulnerabilities.
- Enforce multi-factor authentication (MFA) for accessing sensitive data and systems.
- Regularly audit and update security policies to address emerging threats in the software supply chain.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Malicious NPM Packages Deliver NodeCordRAT

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 Actors Exploit Misconfigured Routing to Spoof Domains in Financial Sector	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Microsoft Threat Intelligence has identified that phishing actors are exploiting complex routing scenarios and misconfigured spoof protections to spoof domains, delivering phishing emails that appear to be sent internally. This attack vector has been linked to various phishing-as-a-service platforms, including Tycoon2FA, and has been used to conduct financial scams against organizations.

The significance of this threat to the financial services sector lies in the potential for credential compromise, which can lead to data theft and business email compromise (BEC) attacks. Organizations must take proactive measures to configure their email systems properly to mitigate the risk of falling victim to these opportunistic phishing campaigns.

Technical Details

- Phishing actors exploit complex routing and misconfigured spoof protections to spoof domains.
- The attack vector is particularly effective as it makes phishing emails appear to be internally sent messages.
- Phishing messages often use themes such as voicemails, shared documents, and HR communications to lure victims.
- Successful credential compromise can lead to data theft or financial scams requiring extensive remediation.

- Organizations using Microsoft Exchange with MX records pointing to Office 365 are protected by built-in spoofing detections.
- Attackers utilize phishing-as-a-service platforms like Tycoon2FA to deliver their campaigns.
- Emails may include clickable links or QR codes leading to phishing landing pages.
- Common indicators of spoofed emails include the same address in both "To" and "From" fields.
- Misconfigured DMARC and SPF policies can allow spoofed emails to bypass filters.
- Financial scams often involve fake invoices and urgent payment requests, exploiting trust within organizations.

Recommendations

- Configure strict DMARC rejection and SPF hard fail policies to prevent spoofing.
- Ensure proper configuration of any third-party connectors to enhance spoof detection.
- Regularly review and update email authentication settings to mitigate phishing risks.
- Educate employees on recognizing phishing attempts and the importance of verifying unexpected requests.
- Implement multi-factor authentication (MFA) to add an additional layer of security against credential theft.

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
Salat Stealer Campaign Targets Cryptocurrency Users with Advanced Evasion Tactics	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

This report details an investigation into the Salat Stealer, a malware family that poses significant risks to users with digital assets. The malware employs sophisticated techniques to steal passwords and cryptocurrency wallet information while maintaining a low profile within the infected systems. It utilizes built-in Windows tools to evade detection, making it a formidable threat to financial services and asset management sectors.

The implications for the financial services sector are profound, as the Salat Stealer specifically targets cryptocurrency wallets and sensitive credentials. Its persistence mechanisms and ability to blend in with legitimate processes highlight the need for enhanced vigilance and proactive measures to safeguard digital assets against such stealthy threats.

Technical Details

- The Salat Stealer is a 64-bit Windows executable that is unsigned, indicating potential malicious intent.
- It modifies the Windows Registry to create a Run key for a file named build.exe, ensuring persistence across system reboots.
- Malware employs privilege escalation tactics to enhance its capabilities and evade detection.
- It utilizes the svchost.exe process to disguise its operations, blending in with legitimate system tasks.
- Outbound communication is established with command-and-control servers, specifically targeting domains salat[.]cn and tonapi[.]io.
- The malware attempts to communicate over Port 137, a non-standard port for typical web traffic, raising red flags for network security.
- It exhibits beaconing behavior, indicating a consistent attempt to connect to its infrastructure for data exfiltration.
- The malware is designed to harvest cryptocurrency wallet strings and browser credentials, making it a specialized tool for asset theft.
- Indicators of compromise include specific file hashes, domain names, and registry modifications that can be monitored for detection.
- The investigation confirms the malware's operational consistency across various analysis techniques, reinforcing its threat level.

Recommendations

- Manually delete the build.exe entry from the Registry Run keys and locate the source file in AppData to eliminate persistence.
- Conduct audits on all endpoints to check for the presence of build.exe in the CurrentVersion\Run registry key.
- Implement blacklisting of the domains salat[.]cn and tonapi[.]io at the router or firewall level to disrupt malware communication.
- Advise users to rotate all passwords and transfer crypto-assets to secure, cold-storage wallets immediately if infected.
- Enforce restrictions on the execution of binaries from the %AppData% and %Temp% folders using AppLocker or similar security tools.

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
Rise in DocuSign Impersonation Campaign Targets Financial Sector	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Group-IB has observed a significant increase in phishing attacks impersonating DocuSign, particularly affecting organizations in the financial sector. These attacks utilize spoofed emails that closely mimic legitimate DocuSign communications, directing users to credential-harvesting pages built with the LogoKit framework. Emails often address recipients by their login names, enhancing their credibility and increasing the likelihood of user interaction.

The implications for the financial services sector are considerable, as successful phishing attempts can lead to unauthorized access to sensitive information and financial losses. The sophisticated nature of these attacks, which leverage trusted business tools and real-time data scraping, underscores the need for robust email protection measures to safeguard against evolving phishing tactics.

Technical Details

- Phishing emails impersonate DocuSign, featuring a polished design that closely resembles legitimate communications.
- Spoofed sender addresses often mimic the recipient's own domain, increasing the likelihood of user engagement.
- The emails contain a "Review document" button that links to credential-harvesting pages hosted on IPFS or AWS S3.
- The phishing page dynamically builds itself using the victim's organization's branding, including background images and favicons.
- The URL includes the target's email address, which is passed to the phishing page for customization.
- Indicators of compromise include SPF failures, mismatched Reply-To headers, and URLs leading to known phishing infrastructure.
- Group-IB's Business Email Protection platform employs multi-layer detection to identify and block these phishing attempts.
- The detection system analyzes sender behavior, message content, and embedded URLs to uncover hidden indicators of phishing.
- Time-of-Click analysis evaluates the phishing page in real-time, allowing for immediate blocking if malicious behavior is detected.
- The campaign highlights the need for continuous adaptation of defenses against sophisticated phishing tactics.

Recommendations

- Implement advanced email filtering solutions that can detect spoofed sender addresses and phishing indicators.

- Educate employees on recognizing phishing attempts, particularly those that impersonate trusted services like DocuSign.
- Utilize multi-factor authentication (MFA) to add an additional layer of security against credential theft.
- Regularly review and update security protocols to address emerging phishing tactics and techniques.
- Monitor user activity for signs of unauthorized access or unusual behavior following potential phishing incidents.

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 Exploit VMware ESXi Flaws to Deploy VSOCKpuppet Backdoor	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Huntress has identified a sophisticated intrusion involving the exploitation of VMware ESXi vulnerabilities. The attack likely began through a compromised SonicWall VPN, allowing threat actors to deploy an exploit toolkit that targets ESXi hypervisors. This toolkit includes a backdoor named VSOCKpuppet, which facilitates covert communication and control over the compromised environment.

The implications for the financial services sector are significant, as the exploitation of hypervisor vulnerabilities can lead to severe data breaches and operational disruptions. Organizations using VMware ESXi should prioritize patching and monitoring to mitigate the risks associated with these vulnerabilities, especially given the potential for ransomware attacks stemming from such exploits.

Technical Details

- The vulnerability is tracked as CVE-2009-0556 and falls under CWE-94 (Improper Control of Generation of Code).
- It exists in the way PowerPoint handles OutlineTextRefAtom objects, leading to memory corruption when an invalid index is used.
- Attackers can execute arbitrary code with the privileges of the affected user upon exploitation.
- The attack vector requires minimal user interaction; victims only need to open a specially crafted PowerPoint file.
- Once executed, attackers can inject malicious instructions that may alter program execution or steal sensitive data.
- The flaw allows for lateral movement within organizational networks, increasing the risk of broader compromise.

- CISA has added this vulnerability to its Known Exploited Vulnerabilities Catalog, highlighting its urgency.
- Microsoft has released security patches for affected PowerPoint versions to mitigate the risk.
- Organizations are advised to discontinue the use of vulnerable PowerPoint versions if patches cannot be applied.
- Security teams should conduct vulnerability assessments to identify and remediate exposed systems before the CISA-imposed deadline.

Recommendations

- Immediately apply the latest patches for VMware ESXi 7.0 and 8.0 to mitigate known vulnerabilities.
- Implement strict access controls and monitoring for VPN connections to prevent unauthorized access.
- Regularly audit and monitor firewall rules to detect unauthorized modifications.
- Utilize endpoint detection and response (EDR) solutions to monitor unusual processes and network traffic on ESXi hosts.
- Educate staff on the risks associated with driver signing and the importance of maintaining up-to-date security practices.

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 Campaign Distributes Malware via Fake WinRAR Installer	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a new campaign distributing malware through fake WinRAR installers linked from various Chinese websites. These installers often masquerade as legitimate software, utilizing multi-layered packing techniques to deliver malicious payloads that can compromise systems and exfiltrate sensitive data.

The implications for the Financial Services sector are significant, as the malware can establish backdoors for remote access, potentially leading to data breaches and financial theft. Institutions must remain vigilant against such deceptive tactics that exploit common software downloads.

Technical Details

- The malware is delivered through a fake WinRAR installer named winrar-x64-713scp.zip, which contains multiple layers of obfuscation.
- Initial analysis reveals that the installer is a UPX packed file requiring special options to unpack due to deliberate anomalies in the executable.
- The unpacked file executes embedded programs immediately after extraction, indicating a sophisticated multi-stage attack.
- One of the embedded files is a legitimate WinRAR installer, included to reduce suspicion among users.
- Another file, setup.hta, is dynamically unpacked into memory, complicating static analysis efforts.
- The malware is associated with Winzipper malware, which is known for deploying hidden backdoors on compromised systems.
- The malware accesses sensitive Windows data, including Windows Profiles information, to tailor its attack based on the system's configuration.
- The campaign leverages social engineering tactics, encouraging users to download software from unofficial sources.
- Malwarebytes has identified and blocked domains associated with the malicious files, enhancing protective measures against this threat.
- The malware's capabilities include establishing persistence, downloading further malware, and exfiltrating data.

Recommendations

- Financial institutions should enforce policies to only download software from official and trusted sources to mitigate risks.
- Implement real-time, up-to-date anti-malware solutions to detect and block threats before execution.
- Educate employees on the dangers of downloading software from unofficial sites and the importance of verifying sources.
- Regularly update security protocols to respond to emerging threats and ensure systems are resilient against malware attacks.
- Monitor network traffic for unusual activity that may indicate the presence of malware 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
CISA Warns of Microsoft PowerPoint Code Injection Flaw Actively Exploited	HIGH	CLEAR	Vulnerability	Open Source

Executive Summary

CISA has issued a critical alert regarding a severe code-injection vulnerability in Microsoft PowerPoint, tracked as CVE-2009-0556. This flaw allows attackers to execute arbitrary code with the privileges of the affected user, potentially leading to full system compromise. The vulnerability is triggered when a specially crafted PowerPoint file containing an invalid OutlineTextRefAtom index is opened, causing memory corruption.

This vulnerability poses a significant threat to organizations in the financial services sector, as it can lead to data theft, system compromise, and network infiltration. Given the ease of exploitation and the potential impact, organizations are urged to prioritize patch deployment and implement necessary mitigations to safeguard their systems against this high-priority threat.

Technical Details

- The vulnerability is tracked as CVE-2009-0556 and falls under CWE-94 (Improper Control of Generation of Code).
- It exists in the way PowerPoint handles OutlineTextRefAtom objects, leading to memory corruption when an invalid index is used.
- Attackers can execute arbitrary code with the privileges of the affected user upon exploitation.
- The attack vector requires minimal user interaction; victims only need to open a specially crafted PowerPoint file.
- Once executed, attackers can inject malicious instructions that may alter program execution or steal sensitive data.
- The flaw allows for lateral movement within organizational networks, increasing the risk of broader compromise.
- CISA has added this vulnerability to its Known Exploited Vulnerabilities Catalog, highlighting its urgency.
- Microsoft has released security patches for affected PowerPoint versions to mitigate the risk.
- Organizations are advised to discontinue the use of vulnerable PowerPoint versions if patches cannot be applied.
- Security teams should conduct vulnerability assessments to identify and remediate exposed systems before the CISA-imposed deadline.

Recommendations

- Apply Microsoft security patches immediately for all affected PowerPoint versions.
- Discontinue use of vulnerable PowerPoint versions if patches cannot be applied.

- Strengthen email security controls to filter suspicious attachments.
- Enhance user awareness training regarding the risks of opening unexpected presentations from untrusted sources.
- Implement network segmentation to limit lateral movement if an exploit occurs.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities Discovered in Trend Micro Apex Central Affecting Windows Installations	HIGH	CLEAR	Vulnerability	Open Source

Executive Summary

Trend Micro has identified multiple vulnerabilities in its Apex Central (on-premise) product, affecting versions below Build 7190. These vulnerabilities include a critical remote code execution flaw and two denial-of-service vulnerabilities, which can be exploited by unauthenticated remote attackers. The vulnerabilities are tracked under CVE-2025-69258, CVE-2025-69259, and CVE-2025-69260.

The financial services sector should take these vulnerabilities seriously, as they could allow attackers to execute malicious code or disrupt services, potentially leading to significant operational and reputational damage. Organizations using Trend Micro Apex Central are urged to apply the critical patch to mitigate these risks.

Technical Details

- CVE-2025-69258: A LoadLibraryEX vulnerability could allow an unauthenticated remote attacker to execute code with SYSTEM privileges.
- CVE-2025-69259: An unchecked NULL return value vulnerability could enable a denial-of-service condition on affected installations.
- CVE-2025-69260: An out-of-bounds read vulnerability could also lead to denial-of-service condition.
- The vulnerabilities affect Trend Micro Apex Central versions below Build 7190 on Windows platforms.
- The CVSS scores for these vulnerabilities range from 7.5 to 9.8, indicating a high to critical severity level.
- Authentication is not required to exploit the denial-of-service vulnerabilities.
- Trend Micro has released Critical Patch Build 7190 to address these vulnerabilities.
- Customers are encouraged to visit the Trend Micro Download Center for prerequisite software before applying the patch.
- Timely application of patches and updated solutions is essential for mitigating these vulnerabilities.

- Organizations should review remote access policies and perimeter security to enhance protection.

Recommendations

- Immediately apply Critical Patch Build 7190 to all affected installations of Trend Micro Apex Central.
- Regularly review and update security policies regarding remote access to critical systems.
- Monitor systems for any unusual activity that may indicate exploitation attempts.
- Educate staff on the importance of applying security updates promptly.
- Consider implementing additional security measures such as network segmentation to limit exposure.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Code Execution Vulnerabilities in Veeam Backup & Replication	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Veeam has released security updates addressing multiple critical remote code execution (RCE) vulnerabilities in Veeam Backup & Replication. These vulnerabilities could allow privileged backup roles to execute arbitrary code and write files, potentially leading to full system compromise.

The vulnerabilities affect Backup Administrators, Backup Operators, and Tape Operators, who can exploit these flaws to gain unauthorized access. This situation is particularly concerning for the financial services sector, as it may expose sensitive data and disrupt operations, necessitating immediate attention to patch affected systems.

Technical Details

- CVE-2025-59470 allows Backup or Tape Operators to achieve RCE as the postgres user via a malicious parameter.
- CVE-2025-55125 enables RCE as root through a malicious backup configuration file created by Backup or Tape Operators.
- CVE-2025-59468 permits Backup Administrators to execute RCE as the postgres user by sending a malicious password parameter.
- CVE-2025-59469 allows Backup or Tape Operators to write arbitrary files as root, increasing the risk of system compromise.
- The vulnerabilities are rated with CVSS scores ranging from 6.7 to 9.0, indicating critical to high severity.
- Affected versions include Veeam Backup & Replication 13.0.1.180 and all earlier v13 builds.

- Versions 12.x and earlier are not affected by these vulnerabilities.
- The fixed version is Veeam Backup & Replication 13.0.1.1071.
- Exploitation of these vulnerabilities could lead to unauthorized access and control over backup systems.
- Organizations using affected versions should prioritize applying the security updates to mitigate risks.

Recommendations

- Immediately update Veeam Backup & Replication to version 13.0.1.1071 to mitigate the vulnerabilities.
- Review and restrict access permissions for Backup Administrators, Backup Operators, and Tape Operators.
- Implement monitoring to detect any unauthorized attempts to exploit these vulnerabilities.
- Regularly audit backup configurations and parameters to ensure they are secure.
- Stay informed about future security updates from Veeam to maintain system integrity.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Code Execution Vulnerabilities in n8n Expose Financial Services to Systemic Risk	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

n8n, a workflow automation tool, is currently affected by two critical Remote Code Execution (RCE) vulnerabilities, CVE-2026-21858 and CVE-2026-21877, both rated with a maximum CVSS score of 10.0. The first vulnerability allows unauthenticated attackers to fully compromise n8n instances, while the second enables low-privileged authenticated users to achieve full RCE, posing a significant threat to organizations using this tool for managing sensitive data.

The implications for the Financial Services sector are severe, as n8n is often used to store sensitive information such as API keys, OAuth tokens, and database credentials. Exploitation of these vulnerabilities could lead to enterprise-wide compromises, making it critical for financial institutions to assess their n8n deployments and implement necessary security measures to mitigate risks.

Technical Details

- CVE-2026-21858 allows unauthenticated RCE through arbitrary file read and authentication bypass, posing a critical risk.
- CVE-2026-21877 enables low-privileged authenticated users to execute arbitrary file writes, leading to full RCE.

- Both vulnerabilities have a CVSS score of 10.0, indicating maximum severity.
- Affected versions include all n8n versions ≤ 1.65.0 for CVE-2026-21858 and versions >= 0.123.0 and < 1.121.3 for CVE-2026-21877.
- The vulnerabilities can escalate to enterprise-wide compromise due to the sensitive information n8n handles.
- The vulnerabilities highlight systemic security risks for exposed or weakly controlled n8n deployments.
- Recent disclosures of critical vulnerabilities in n8n indicate a pattern of security issues, raising concerns over its security posture.
- Previous vulnerabilities include CVE-2025-68613 and CVE-2025-68668, both with high severity ratings.
- Organizations using n8n should prioritize patching to the fixed versions: 1.121.0 for CVE-2026-21858 and 1.121.3 for CVE-2026-21877.
- Continuous monitoring and assessment of n8n deployments are essential to mitigate risks associated with these vulnerabilities.

Recommendations

- Immediately update n8n to the latest versions to mitigate the identified vulnerabilities.
- Conduct a thorough assessment of n8n deployments to identify any exposed or weakly controlled instances.
- Implement strict access controls to limit authenticated user privileges within n8n.
- Regularly monitor and audit n8n configurations and logs for any suspicious activities.
- Establish a vulnerability management program to stay informed about future security issues related to n8n.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Command Injection Vulnerability in D-Link Routers Actively Exploited	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical security flaw affecting legacy D-Link DSL gateway routers has been actively exploited, allowing unauthenticated remote attackers to execute arbitrary commands via the dnscfg.cgi endpoint. This vulnerability enables full control over DNS settings, leading to persistent compromise of downstream devices. Many affected devices are end-of-life and cannot be patched, increasing the risk of exploitation.

The vulnerability, identified as CVE-2026-0625, has a CVSS v3.1 score of 9.3, indicating its critical nature. It poses significant risks to the financial services sector, as compromised routers can lead to unauthorized

modification of DNS settings, potential redirection of network traffic, and persistent threats to connected devices, which may include sensitive financial data.

Technical Details

- CVE-2026-0625 is a command injection vulnerability allowing remote code execution on affected D-Link routers.
- The flaw exists due to improper input validation in the dnscfg.cgi endpoint, enabling unauthenticated attackers to execute arbitrary commands.
- Attackers can modify DNS settings, leading to potential redirection, interception, or blocking of all network traffic downstream.
- Active exploitation has been observed targeting legacy firmware versions without requiring user interaction.
- Affected legacy models include DSL-2640B (firmware <= 1.07), DSL-2740R (firmware < 1.17), DSL-2780B (firmware <= 1.01.14), and DSL-526B (firmware <= 2.01).
- Exploitation allows for persistent compromise of all connected devices, posing a significant risk to network integrity.
- The vulnerability has a CVSS v3.1 score of 9.3, classifying it as critical.
- Many impacted devices are end-of-life (EoL) and cannot be patched, leaving them vulnerable to ongoing attacks.
- Attackers can control DNS settings, which can lead to severe consequences for organizations relying on these devices.
- The vulnerability highlights the importance of maintaining updated and supported hardware in network environments.

Recommendations

- Replace legacy DSL gateways with supported devices to mitigate risks.
- Monitor DNS settings for unauthorized changes regularly.
- Ensure firmware is updated on all supported devices to protect against vulnerabilities.
- Conduct audits of connected devices for any suspicious activity indicative of compromise.
- Stay informed on official D-Link updates for affected models and follow guidance for remediation.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerability in Forcepoint One DLP Client Allows Code Execution	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

A high-severity vulnerability has been identified in the Forcepoint One Data Loss Prevention (DLP) Client, which may allow attackers to bypass sandbox restrictions and execute arbitrary code on protected endpoints. This flaw could significantly weaken DLP enforcement and compromise overall endpoint security.

The vulnerability, tracked as CVE-2025-14026, poses a risk to financial services organizations relying on DLP solutions to protect sensitive data. The ability to bypass DLP controls and evade security monitoring could lead to unauthorized access and manipulation of critical financial information.

Technical Details

- The vulnerability is identified as CVE-2025-14026 with a CVSS score of 7.8, categorized as high severity.
- The Forcepoint One DLP Client includes a legacy Python 2.5.4 runtime, originally intended for internal use.
- The ctypes library, which provides access to system-level functions, was removed to prevent misuse.
- Attackers can bypass the limitation by transferring the missing ctypes module and applying a version-header patch.
- Once the ctypes module is restored, the Python environment can execute arbitrary shellcode or DLL-based payloads.
- Successful exploitation grants attackers' full control within the client process.
- This vulnerability may enable attackers to bypass DLP controls, compromising data protection measures.
- Affected versions include Forcepoint One DLP Client 23.04.5642 and potentially earlier releases.
- Fixed versions are available in Forcepoint One Endpoint builds v23.11 and later (Forcepoint DLP v10.2+).
- Organizations using affected versions should prioritize updates to mitigate the risk.

Recommendations

- Immediately update to Forcepoint One Endpoint builds v23.11 or later to mitigate the vulnerability.
- Conduct a thorough assessment of all endpoints using the Forcepoint One DLP Client to identify affected versions.
- Implement additional monitoring measures to detect any unusual activity related to DLP controls.
- Educate staff about the risks associated with legacy software and the importance of timely updates.
- Regularly review and update security policies to ensure robust endpoint protection.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Privilege Escalation Vulnerability in Tenable Nessus Agent on Windows	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Tenable has disclosed a high-severity local privilege escalation vulnerability affecting the Nessus Agent Tray Application on Windows hosts. This vulnerability stems from improper handling during the installation and uninstallation processes, enabling a locally authenticated attacker with low privileges to escalate to higher system privileges.

This vulnerability is significant for the financial services sector as it could allow attackers to gain unauthorized access to sensitive systems and data, potentially leading to further exploitation. Organizations utilizing the affected versions of the Nessus Agent should prioritize applying the necessary updates to mitigate the risk of privilege escalation attacks.

Technical Details

- The vulnerability is identified as CVE-2025-36640 and has a CVSS v3 Base Score of 8.8, indicating a high severity level.
- It affects the Nessus Agent Tray Application on Windows, specifically during its installation and uninstallation routines.
- The attack type is classified as Local Privilege Escalation, allowing low-privileged users to gain higher system privileges.
- Affected products include Nessus Agent versions prior to 10.9.3 and versions 11.0.0 through 11.0.2.
- Fixed versions are Nessus Agent 10.9.3 and 11.0.3, which address the vulnerability effectively.
- The improper handling during installation and uninstallation is the root cause of vulnerability.
- Organizations should be aware that exploitation requires local access, limiting the attack vector to authenticated users.
- The risk factor is categorized as high, emphasizing the need for immediate remediation.
- Tenable has released an advisory (TNS-2026-01) detailing the vulnerability and its implications.
- Users are encouraged to review their Nessus Agent versions and apply updates to ensure security.

Recommendations

- Immediately update to Nessus Agent version 10.9.3 or 11.0.3 to mitigate the vulnerability.
- Conduct a review of all systems running the Nessus Agent to identify affected versions.
- Implement strict access controls to limit local access to systems running the Nessus Agent.

- Regularly monitor for updates and advisories from Tenable regarding security vulnerabilities.
- Educate staff on the importance of maintaining updated software to prevent exploitation.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerability in jsPDF Allows Remote File Access	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

A critical security vulnerability has been identified in jsPDF, a widely used JavaScript library for PDF document generation. Tracked as CVE-2025-68428, this flaw allows unauthenticated remote attackers to read arbitrary files from the server's local file system when jsPDF is utilized in Node.js environments. The vulnerability stems from improper input validation of file paths, potentially exposing sensitive information embedded in generated PDF documents.

This vulnerability poses significant risks to the financial services sector, as it could lead to the exfiltration of sensitive data such as configuration secrets and credentials. The ability for attackers to access and embed this information into PDF documents can severely compromise confidentiality and trust, making it imperative for organizations to address this flaw promptly.

Technical Details

- The vulnerability is tracked as CVE-2025-68428 with a CVSS v4.0 score of 9.2, indicating critical severity.
- It affects jsPDF versions 3.0.4 and earlier, specifically in Node.js environments.
- This flaw allows unauthenticated remote attackers to perform Local File Inclusion (LFI) and Path Traversal attacks.
- Improper input validation of file paths passed to jsPDF methods is the root cause of vulnerability.
- Sensitive files, including configuration secrets and application data, can be exfiltrated and embedded in PDF documents.
- Associated weaknesses include CWE-35 (Path Traversal) and CWE-73 (External Control of File Name or Path).
- Affected versions are jsPDF versions ≤ 3.0.4, while patched versions are ≥ 4.0.0.
- Node.js --permission flag can be used as a workaround to restrict file system access.
- This feature is stable for production use in Node.js versions 22.13.0, 23.5.0, and 24.0.0.
- Organizations should prioritize upgrading to the patched version to mitigate risks.

Recommendations

- Upgrade jsPDF to version 4.0.0 or later to eliminate vulnerability.
- Implement the Node.js --permission flag in production to restrict file system access.

- Regularly audit and monitor file access permissions in Node.js applications.
- Educate development teams on secure coding practices to prevent similar vulnerabilities.
- Establish a routine for vulnerability assessments and patch management.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerability in Google Chrome WebView Could Bypass Security Policies	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Trend Micro has identified multiple vulnerabilities in its Apex Central (on-premise) product, affecting versions below Build 7190. These vulnerabilities include a critical remote code execution flaw and two denial-of-service vulnerabilities, which can be exploited by unauthenticated remote attackers. The vulnerabilities are tracked under CVE-2025-69258, CVE-2025-69259, and CVE-2025-69260.

The financial services sector should take these vulnerabilities seriously, as they could allow attackers to execute malicious code or disrupt services, potentially leading to significant operational and reputational damage. Organizations using Trend Micro Apex Central are urged to apply the critical patch to mitigate these risks.

Technical Details

- CVE-2025-69258: A LoadLibraryEX vulnerability could allow an unauthenticated remote attacker to execute code with SYSTEM privileges.
- CVE-2025-69259: An unchecked NULL return value vulnerability could enable a denial-of-service condition on affected installations.
- CVE-2025-69260: An out-of-bounds read vulnerability could also lead to denial-of-service condition.
- The vulnerabilities affect Trend Micro Apex Central versions below Build 7190 on Windows platforms.
- The CVSS scores for these vulnerabilities range from 7.5 to 9.8, indicating a high to critical severity level.
- Authentication is not required to exploit the denial-of-service vulnerabilities.
- Trend Micro has released Critical Patch Build 7190 to address these vulnerabilities.
- Customers are encouraged to visit the Trend Micro Download Center for prerequisite software before applying the patch.
- Timely application of patches and updated solutions is essential for mitigating these vulnerabilities.
- Organizations should review remote access policies and perimeter security to enhance protection.

Recommendations

- Immediately apply Critical Patch Build 7190 to all affected installations of Trend Micro Apex Central.
- Regularly review and update security policies regarding remote access to critical systems.
- Monitor systems for any unusual activity that may indicate exploitation attempts.
- Educate staff on the importance of applying security updates promptly.
- Consider implementing additional security measures such as network segmentation to limit exposure.

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Muddy Water APT Campaign Targets Financial Sector in the Middle East with RustyWater Implant

ATT&CK Tactic	Technique ID	Technique Name	Evidence from Report

Initial Access	T1566.001	Phishing: Spear phishing Attachment	Malicious email with Cybersecurity.doc attachment
Initial Access	T1204.002	User Execution: Malicious File	User opens Doc leading to payload drop and execution
Execution	T1059.005	Command and Scripting Interpreter	VBA Macro in Word Document
Execution	T1106	Native API	Use of RegOpenKeyExW, GetUserNameW, GetComputerNameExW, CreateWaitableTimerExW
Execution	T1047	Windows Management Instrumentation	WMI used to execute CertificationKit.ini via Win32_Process.Create
Execution	T1620	Reflective Code Loading	Hex coded PE payload decode in memory and dropped

Malicious-npm-Packages-Deliver-nodecordrat

Tactic	Technique ID	Technique name	Description
Initial Access	T1588.006	Obtain Capabilities: Code Signing Certificates	The attacker creates a compelling narrative around a legitimate looking npm package (via typo squatting) that contains the malicious code.
Initial Access	T1584.007	Compromise Infrastructure: Development Platforms	The attacker uses a typo squatted npm package to distribute the malware, taking advantage of developers downloading or using incorrect package names in their projects.
Execution	T1059.007	Command and Scripting Interpreter: JavaScript/JScript	The core malicious payload is a Node.js script. This technique involves executing malicious code written in JavaScript, which is native to the Node.js environment.
Defense Evasion	T1027	Obfuscated Files or Information	The original code used minimal obfuscation (hexadecimal characters, uninformative variable names) to confuse automated analysis and frustrate human reverse-engineering.
Discovery	T1082	System Information Discovery	The script gathers detailed system information, including operating system (os.platform()), and executes operating system-specific commands (wmic, ioreg) to create a unique fingerprint (UUID/Machine ID) for the compromised host.
Discovery	T1016	System Network Configuration Discovery	The script implicitly relies on network access to establish the Discord connection and C2 channel.

Command and Control (C2)	T1102.002	Web Service: Social Media	The script uses the Discord API as its primary C2 communication channel for sending and receiving commands, and exfiltrating data, using a dedicated, private channel per endpoint.
Collection	T1552.001	Unsecured Credentials: Credentials in Files	The script actively searches for and exfiltrates unencrypted or weakly-encrypted files (e.g., .env files) containing sensitive plaintext credentials and configuration secrets.
Collection	T1539	Steal Web Session Cookie	The script targets the Chrome User Data directory, indicating an intent to steal web browser session data, cookies, and saved login credentials.
Collection	T1213.001	Data from Local System: File Sharing	The custom !sendfile command allows the threat actor to exfiltrate any specific file from the compromised system's local file system.
Collection	T1113	Screen Capture	The implementation of the !screenshot command allows the attacker to visually monitor user activity and discover sensitive information displayed on the screen.
Credential Access	T1555.003	Credentials from Web Browsers	The script specifically targets the Chrome Login Data and Local State files with the intent to decrypt, and harvest protected and saved browser credentials. This also includes the highly targeted exfiltration of LevelDB files found near the MetaMask wallet extension ID.
Exfiltration	T1041	Exfiltration Over C2 Channel	All sensitive data gathered (e.g., passwords, .env files, screenshots) is uploaded directly to the dedicated Discord C2 channel, using the existing connection for exfiltration.

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
API Keys	Authentication credentials for application integration.
APT	Advanced Persistent Threat; a sophisticated, persistent cyber-attack group.
AWS S3	Amazon cloud storage services.
Base64	Encoding mechanism to convert binary to text.
BEC	Business Email Compromise fraud technique.
Blockchain	Decentralized digital ledger used to record transactions.
C2 / Command and Control	Communication channel used by attackers to manage compromised systems.
CoinGecko	Crypto market-tracking platform.
CSC	UAE Cyber Security Council
ctypes	Python library enabling low-level system calls.
CVE	Common Vulnerabilities and Exposures; unique ID for security flaws.
CVSS	Common Vulnerability Scoring System for rating severity.
CWE	Common Weakness Enumeration; classification of software weaknesses.
DLL	Dynamic Link Library used by Windows applications.
DMARC	Domain-based Message Authentication, Reporting & Conformance email authentication policy.
Domain Spoofing	Forging an email/domain to appear legitimate.
ETH / Ether	Cryptocurrency used on the Ethereum blockchain.
FTP	File Transfer Protocol for server file transfers.
HTA	HTML Application file type used in malware execution.
IPFS	InterPlanetary File System; decentralized hosting system.

IRC	Internet Relay Chat; used by some botnets for C2 communication.
JSON	Lightweight data-interchange format.
KDU	Kernel Driver Utility used to load unsigned drivers.
LFI / Local File Inclusion	Technique allowing attackers to read files on a server.
LoadLibraryEX	Windows API function involved in vulnerability exploitation.
Local Privilege Escalation	Gaining higher system rights from an existing low-privilege account.
LogoKit	Phishing framework that dynamically customizes credential harvest pages.
MAESTRO	Orchestrator tool used in ESXi exploitation chain.
MetaMask	Cryptocurrency wallet used for blockchain applications.
MySQL	Relational database management system.
Node.js	JavaScript runtime used for backend applications.
NPM	JavaScript package manager.
OAuth Tokens	Authorization credentials for accessing protected resources.
Path Traversal	Exploit allowing access to files outside allowed directories.
Phishing-as-a-Service (PhaaS)	Platforms that enable attackers to run phishing campaigns.
phpMyAdmin	Web-based database management tool.
PM2	Node.js process manager used for application persistence.
PostgreSQL	Open-source relational database system.
PowerShell	Windows scripting language often abused by malware.
Python Runtime	Software environment running Python code (legacy in Forcepoint case).
RAT	Remote Access Trojan that provides attackers remote control of a device.
Rust	A programming language used to build secure and efficient software.
RustyWater	Rust-based malware implant used by Muddy Water APT.
Smart Contract	Self-executing contract with terms directly written into code.
SonicWall VPN	Remote access appliance referenced as initial compromise vector.
Spear-Phishing	Highly targeted phishing attack aimed at specific individuals or organizations.
SPF	Sender Policy Framework; email spoof-prevention standard.
System Privileges	Highest Windows permission level.
TLP:CLEAR	Traffic Light Protocol designation allowing unrestricted information sharing.
TRU Token	Truebit project's native digital token.
Tycoon2FA	A PhaaS platform mentioned in phishing attacks.
UPX	Executable packer used for software compression and obfuscation.
VBS	Visual Basic Script, used for automation and sometimes exploited by attackers.
VMware ESXi	Enterprise hypervisor for virtual machine hosting.
VSOCK	Virtual socket interface used for inter-VM communication.
WebView	Embedded browser component inside applications.
Winzipper	Malware family associated with fake installer campaigns.
XAMPP	Local development environment package.
XOR	Data obfuscation technique used in malware.