









# ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI



CATEGORY		ACTIONABLE
AUDIENCE		ADGM FSRA ENTITIES
DATE		24/12/2025
OVERALL THREAT SCORE		GUARDED
TARGET SECTOR		FINANCIAL SERVICES
TARGET REGION		UAE, MENA & GLOBAL
ATTRIBUTION		MULTIPLE
TLP		CLEAR

## WEEKLY SUMMARY REPORT – 24 December 2025

0

### Cyber Breach

Major Compromises and breaches

0

### Threat Actors

Threat actor activities in the UAE & Middle East impacting Finance Sector

7

### Campaigns

Recent Threat campaigns within financial institutions

8

### Vulnerability

Actively Exploited & Critical Vulnerabilities

## Summary

This week's cybersecurity newsletter highlights a range of emerging threats and vulnerabilities impacting the financial services sector, with a particular focus on ransomware, phishing campaigns, and critical software vulnerabilities. Key observations include the resurgence of the CyberVolk group with its VolkLocker ransomware, the identification of the BlackForce phishing kit capable of bypassing multi-factor authentication, and the discovery of critical zero-day vulnerabilities in Cisco and SonicWall products that could lead to unauthorized access and data breaches. Additionally, the newsletter discusses the implications of malicious software targeting cryptocurrency wallets and the risks associated with supply chain attacks.

The financial services sector must remain vigilant in the face of these evolving threats, emphasizing the importance of robust cybersecurity measures such as multi-factor authentication, regular software updates, and comprehensive employee training. Organizations are urged to implement proactive security strategies, including monitoring for unusual activity, enhancing incident response protocols, and conducting regular security assessments to safeguard sensitive data and maintain operational integrity.

## ADGM THREAT INTELLIGENCE SUMMARY

[Ongoing Crypto Mining Campaign Targets AWS EC2 and ECS Using Compromised IAM Credentials](#) [Campaign] [High]

[CyberVolk Campaign Returns with Enhanced VolkLocker Ransomware](#) [Campaign] [Medium]

[BlackForce Phishing Kit Targets Financial Services with Advanced MitB Techniques](#) [Campaign] [Medium]

[Malicious NuGet Package Typosquats .NET Tracing Library to Steal Wallet Passwords](#) [Campaign] [Medium]

[ClickFix Campaign Exploits Human Verification to Deploy StealC and Qilin Ransomware](#) [Campaign] [Medium]

[New SantaStealer Malware Campaign Targets Financial Sector with Advanced Information Theft Capabilities](#) [Campaign] [Medium]

[DarkGate Malware Campaign Exploits Social Engineering via Fake "Word Online" Error Message](#) [Campaign] [Medium]

[Critical Zero-Day Vulnerability in Cisco AsyncOS Email Security Appliances Actively Exploited](#) [Vulnerability] [High]

[SonicWall SMA1000 Appliance Vulnerability Allows Remote Code Execution](#) [Vulnerability] [High]

[Critical Remote Code Execution Vulnerability in HPE OneView Software](#) [Vulnerability] [Medium]

[Critical Remote Code Execution Vulnerability in pgAdmin Exposes Database Servers](#) [Vulnerability] [Medium]

[High-Severity OS Command Injection Vulnerability in systeminformation Node.js Library](#) [Vulnerability] [Medium]

[High-Severity Vulnerability in Zoom Rooms for Windows Allows Privilege Escalation](#) [Vulnerability] [Medium]

[High-Severity Vulnerabilities in React Server Components Require Immediate Attention](#) [Vulnerability] [Medium]

[Microsoft Discloses Critical Vulnerabilities in Azure and Office Products](#) [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Ongoing Crypto Mining Campaign Targets AWS EC2 and ECS Using Compromised IAM Credentials	HIGH	CLEAR	Campaign	Open Source

### Executive Summary

Researchers at AWS have identified an ongoing cryptocurrency mining campaign that exploits compromised AWS Identity and Access Management (IAM) credentials to target Amazon Elastic Container Service (ECS) and Amazon Elastic Compute Cloud (EC2). The campaign employs a novel persistence technique that complicates incident response and extends the duration of mining operations. Attackers quickly deploy crypto mining resources within minutes of gaining access, leveraging various AWS services to maximize their impact.

This campaign poses significant risks to the financial services sector, as it not only compromises cloud resources but also highlights vulnerabilities in identity and access management practices. The use of compromised credentials underscores the need for robust security measures, including multi-factor authentication and least privilege access, to prevent unauthorized access to critical cloud environments.

### Technical Details

- The campaign utilizes compromised IAM credentials, allowing unauthorized users to access AWS services without exploiting vulnerabilities.
- Attackers employ a persistence technique using the ModifyInstanceAttribute API to disable API termination, complicating remediation efforts.
- Initial access is gained through compromised IAM user credentials with admin-like privileges, triggering anomaly detection alerts.
- The threat actor systematically probes AWS environments to identify deployable resources and test permissions using the DryRun flag.
- Malicious Docker Hub image (yenik65958/secret) was used to deploy crypto miners, which has since been removed but may reappear under different names.
- The campaign involves creating numerous ECS clusters and deploying mining tasks with aggressive scaling parameters.
- Attackers utilize both Spot and On-Demand Instances to maximize resource consumption and evade detection.
- GuardDuty effectively identifies malicious activities through threat intelligence and anomaly detection across EC2 and ECS.
- The campaign demonstrates advanced persistence methodologies that security teams must be vigilant against.
- AWS recommends enabling GuardDuty Runtime Monitoring for enhanced detection and response capabilities.

## Recommendations

- Implement strong identity and access management controls, including the use of temporary credentials and enforcing multi-factor authentication (MFA).
- Monitor for unusual API usage patterns, particularly the use of the DryRun flag, as an early warning indicator of compromise.
- Ensure GuardDuty is enabled across all accounts and regions, with Runtime Monitoring activated for comprehensive coverage.
- Integrate GuardDuty with AWS Security Hub and automated response tools to facilitate rapid remediation of high-severity findings.
- Establish specific incident response procedures for crypto mining attacks, including handling instances with disabled API termination.

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
CyberVolk Campaign Returns with Enhanced VolkLocker Ransomware	MEDIUM	CLEAR	Campaign	Open Source

## Executive Summary

CyberVolk, a pro-Russia hacktivist group, has resurfaced with a new ransomware-as-a-service (RaaS) offering known as VolkLocker, which features Telegram-based automation and a unique encryption mechanism. This resurgence follows a period of dormancy and highlights the group's ongoing alignment with Russian governmental interests. The ransomware employs a flawed design, allowing potential victims to recover files without paying the ransom due to the storage of encryption keys in plaintext.

The implications for the Financial Services sector are significant, as the use of Telegram for command and control reflects a broader trend among politically motivated threat actors. With the ability to automate attacks and manage operations through a widely used messaging platform, CyberVolk lowers the barriers for ransomware deployment, posing a heightened risk to financial institutions and their clients. The vulnerabilities associated with VolkLocker necessitate immediate attention and proactive measures to safeguard sensitive data.

## Technical Details

- VolkLocker payloads are developed in Golang, supporting both Linux and Windows environments, and are distributed without obfuscation.
- The ransomware employs a UAC bypass technique (T1548.002) to escalate privileges, allowing it to execute with elevated permissions.

- It performs environmental checks to detect virtual machines, querying MAC addresses against known vendor prefixes to avoid execution in such environments.
- AES-256 encryption in GCM mode is utilized for file encryption, with a hardcoded master key that is stored in plaintext, creating a recovery pathway for victims.
- The ransomware modifies multiple registry keys to disable system recovery options and terminates processes associated with analysis tools.
- A ransom note is generated as a dynamic HTML file, featuring a countdown timer that is purely cosmetic, while a separate enforcement timer manages actual system destruction.
- The malware deletes critical user folders and Volume Shadow Copies during its destructive routine, leading to significant data loss.
- CyberVolk's operations are managed entirely through Telegram, allowing for streamlined communication and control over infected systems.
- The service has expanded to include standalone RAT and keylogger tools, indicating a diversification of their criminal offerings.
- The presence of plaintext key backups suggests a lack of quality control in the deployment of their ransomware, potentially undermining their operational effectiveness.

### Recommendations

- Implement robust endpoint detection and response solutions to identify and mitigate ransomware behaviors.
- Regularly update and patch systems to protect against known vulnerabilities that could be exploited by ransomware.
- Educate employees on recognizing phishing attempts and the risks associated with Telegram and other messaging platforms.
- Establish a comprehensive data backup strategy, ensuring backups are stored offline and are not accessible from the network.
- Monitor network traffic for unusual behavior indicative of ransomware communication or command and control activities.

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
BlackForce Phishing Kit Targets Financial Services with Advanced MitB Techniques	MEDIUM	CLEAR	Campaign	Open Source

### Executive Summary

Researchers at Zscaler ThreatLabz have identified a new phishing kit named BlackForce, which is capable of stealing credentials and executing Man-in-the-Browser (MitB) attacks to bypass multi-factor authentication (MFA). The kit has been observed impersonating over 11 brands and is actively marketed on Telegram forums.

This development is significant for the financial services sector as it highlights the evolving tactics of cybercriminals, particularly their ability to bypass MFA, which is a critical security measure. The rapid evolution of BlackForce indicates a persistent threat that financial institutions must address to protect sensitive customer data and maintain trust.

### Technical Details

- BlackForce employs a dual-channel communication architecture, separating the phishing server from a Telegram drop to secure stolen data.
- The phishing kit uses cache-busting techniques to ensure victims download the latest malicious scripts.
- It features a legitimate-looking codebase, with over 99% of its JavaScript content derived from production builds of React.
- The attack chain includes a vetting system to qualify targets before a live operator orchestrates the attack.
- BlackForce utilizes MitB techniques to deploy fake MFA pages, capturing victim MFA codes in real-time.
- Anti-analysis filters are implemented to block traffic from security vendors and web crawlers.
- The kit has evolved from a stateless to a stateful model, allowing it to retain stolen credentials across sessions.
- BlackForce's C2 panel manages all actions from the victim's landing on the phishing page to data theft.
- The phishing kit is under active development, with multiple versions released in a short timeframe.
- Evasion techniques include a comprehensive blocklist for user agents and ISPs, enhancing its resilience against detection.

### Recommendations

- Implement a zero-trust architecture to limit access and reduce potential damage from attacks.
- Regularly update and patch systems to protect against known vulnerabilities.
- Educate employees and customers on recognizing phishing attempts and the importance of MFA.

- Monitor network traffic for unusual patterns indicative of phishing activity.
- Utilize advanced threat detection solutions that can identify and block phishing attempts in real-time.

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

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – [BlackForce Phishing Kit](#)

[Reference to the Source](#)

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Malicious NuGet Package Typosquats .NET Tracing Library to Steal Wallet Passwords	MEDIUM	CLEAR	Campaign	Open Source

### Executive Summary

Researchers at Socket Threat Research Team have uncovered a malicious NuGet package, Tracer.Fody.NLog, which impersonates the legitimate Tracer.Fody library. This package is designed to function as a cryptocurrency wallet stealer, scanning for Stratis wallet files and exfiltrating sensitive data to a threat actor-controlled IP address in Russia.

The presence of this malicious package in the NuGet Gallery for over five years poses significant risks to the financial services sector, particularly for organizations utilizing .NET technologies. The stealthy nature of the attack, leveraging trusted libraries and disguising malicious behavior within common development practices, highlights the need for enhanced vigilance in supply chain security.

### Technical Details

- The malicious package Tracer.Fody.NLog typosquats the legitimate Tracer.Fody library, using homoglyph tricks to deceive users.
- It scans the default Stratis wallet directory for \*.wallet.json files, extracting wallet data and passwords.
- Data is exfiltrated to a Russian IP address (176.113.82.163) via HTTP GET requests, ensuring stealthy operation.
- The package disguises its malicious behavior by embedding itself in a commonly used helper function, Guard.NotNull<T>.
- The threat actor employs Cyrillic homoglyphs to create visually similar identifiers, complicating detection efforts.
- The malicious code operates silently, catching all exceptions to avoid alerting users or breaking the host application.

- The package has been downloaded approximately 2,000 times, increasing the likelihood of widespread embedding in developer environments.
- The threat actor's infrastructure remains active, indicating ongoing malicious operations targeting .NET developers.
- The attack exemplifies risks associated with supply chain compromises, particularly in trusted ecosystems like NuGet.
- Similar tactics may be employed in future attacks, targeting other blockchain wallets and sensitive data.

### Recommendations

- Implement strict package review processes to verify the legitimacy of dependencies before integration.
- Utilize automated tools to scan for known malicious packages and suspicious behaviors during development.
- Educate developers on the risks of typosquatting and the importance of verifying package maintainers.
- Monitor network traffic for unusual egress patterns that may indicate data exfiltration attempts.
- Regularly audit and update dependencies to mitigate risks from long-standing vulnerabilities in third-party libraries.

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

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Malicious NuGet Package

[Reference to the Source](#)

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
ClickFix Campaign Exploits Human Verification to Deploy StealC and Qilin Ransomware	MEDIUM	CLEAR	Campaign	Open Source

### Executive Summary

Researchers at Sophos Counter Threat Unit have uncovered a ClickFix-style fake human-verification scheme that led to the installation of a remote-access tool, followed by StealC v2 infostealer activity and the deployment of Qilin ransomware. This campaign highlights how user-assisted steps can enable credential theft and ransomware impact within organizations.

The ClickFix technique poses significant risks to the financial services sector in the UAE, where the prevalence of Windows endpoints and internet-facing services increases vulnerability. The exploitation of



user interactions through deceptive verification processes can lead to severe consequences, including data breaches and operational disruptions.

### Technical Details

- The ClickFix campaign begins with a compromised legitimate website that uses a fake human-verification process to lure victims.
- Users are tricked into completing a verification flow, which leads to the installation of a remote-access tool.
- A batch-style installer is used to deploy the remote-access tool, establishing persistence via a registry Run key.
- StealC v2 infostealer is launched through DLL sideloading, utilizing a legitimate Windows media component.
- Approximately one month later, the attackers deploy Qilin ransomware after accessing the network with stolen credentials.
- Qilin operates as ransomware-as-a-service (RaaS) and employs double-extortion tactics.
- The campaign demonstrates how user interaction can facilitate credential theft and subsequent ransomware deployment.
- Researchers assess that an initial access broker may have obtained credentials via StealC and transferred them to a Qilin affiliate.
- The campaign emphasizes the need for timely patching of internet-facing services and minimizing exposure of remote-desktop services.
- Defensive measures include enforcing phishing-resistant MFA and deploying capable endpoint detection and response (EDR) solutions.

### Recommendations

- Enable phishing-resistant MFA everywhere and force immediate password resets for any account showing unusual activity.
- Tighten script and app-control policies now, blocking untrusted installers and unsigned DLL loading to reduce user-assisted execution.
- Hunt for unauthorized remote-access tooling and new persistence entries; isolate any endpoint with unexpected remote-access behavior.
- Review and harden VPN and remote-desktop exposure, patch internet-facing services, and restrict external access to business-critical needs only.
- Notify users immediately: avoid “human verification” prompts that ask to press keys or run commands; report and close such pages on sight.

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
<b>New SantaStealer Malware Campaign Targets Financial Sector with Advanced Information Theft Capabilities</b>	<b>MEDIUM</b>	<b>CLEAR</b>	<b>Campaign</b>	<b>Open Source</b>

### Executive Summary

Rapid7 Labs has identified a new malware-as-a-service information stealer named "SantaStealer," actively promoted on Telegram and underground forums. This malware is designed to collect and exfiltrate sensitive data, including documents, credentials, and cryptocurrency wallets, operating primarily in-memory to evade detection. The stealer is now production-ready and expected to be deployed widely in the near future.

The emergence of SantaStealer is significant for the financial services sector, as it demonstrates a growing trend of sophisticated malware targeting sensitive financial data. Its capabilities to bypass security measures and operate stealthily pose a serious risk to institutions handling sensitive information, necessitating heightened vigilance and robust cybersecurity measures.

### Technical Details

- SantaStealer is designed to operate entirely in-memory, avoiding file-based detection mechanisms.
- The malware collects sensitive data from various applications, including browsers and cryptocurrency wallets.
- Stolen data is compressed and split into 10 MB chunks before being sent to a command-and-control (C2) server over unencrypted HTTP.
- The malware features a custom C polymorphic engine, although samples analyzed show it is not fully undetected.
- Anti-analysis techniques are under development, including checks for virtual machines and debuggers.
- The malware can selectively target or avoid victims from Commonwealth of Independent States (CIS) countries based on user configuration.
- SantaStealer employs a modular design, allowing for multiple data collection methods, including screenshots and credential theft.
- The malware uses ChaCha20 encryption for obfuscation of sensitive data within its payload.
- The C2 server IP addresses are hardcoded in the malware, making tracking straightforward at this stage.
- The pricing model for SantaStealer suggests a professional-grade service, with basic and premium variants available for monthly subscriptions.

### Recommendations

- Implement strict email filtering to block unrecognized links and attachments that may deliver malware.

- Educate employees on recognizing phishing attempts and suspicious technical support requests.
- Enforce multi-factor authentication (MFA) for sensitive accounts to mitigate credential theft risks.
- Regularly update and patch systems to protect against known vulnerabilities that could be exploited by malware.
- Monitor network traffic for unusual patterns that may indicate data exfiltration attempts.

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

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – [New SantaStealer Malware Campaign](#)

[Reference to the Source](#)

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
DarkGate Malware Campaign Exploits Social Engineering via Fake “Word Online” Error Message	MEDIUM	CLEAR	Campaign	Open Source

### Executive Summary

Researchers at GBHackers have identified a sophisticated social engineering campaign that utilizes a fraudulent “Word Online” extension error message to distribute DarkGate malware. This attack employs the “ClickFix” technique, tricking users into executing malicious commands disguised as legitimate troubleshooting steps, thereby bypassing traditional security defenses through human interaction.

The implications for the financial services sector are significant, as the rise of ClickFix attacks represents an evolution in social engineering tactics. By exploiting user trust and familiarity with standard troubleshooting procedures, attackers can circumvent technical security controls, leading to potential data breaches and unauthorized access to sensitive information.

### Technical Details

- The attack begins with a fake message claiming the “Word Online” extension is missing, prompting users to click a “How to fix” button.
- Attackers use a multi-layered obfuscation technique, including nested Base64 encoding, to conceal malicious commands.
- A malicious JavaScript snippet is embedded in the HTML, which decodes a hidden PowerShell command when the button is clicked.
- The PowerShell command connects to a compromised WordPress site and downloads an HTA file named “dark.hta”.
- The HTA file executes a malicious payload and establishes communication with the attacker's

infrastructure.

- The infection chain includes creating directories and deploying Autolt executables that run automatically.
- The Autolt component drops additional files, including executables implementing the DES algorithm.
- DarkGate establishes persistent communication with command and control servers for remote command execution and data theft.
- Infected systems may show symptoms like degraded performance, unauthorized browser changes, and suspicious network traffic.
- Traditional antivirus solutions may struggle to detect the initial compromise due to user-initiated actions.

### Recommendations

- Implement comprehensive security awareness training to help users recognize ClickFix-style social engineering tactics.
- Deploy endpoint detection and response solutions to monitor PowerShell and script execution activities.
- Enforce application allowlisting to prevent unauthorized executables from running on systems.
- Maintain updated security patches across all systems and browsers to mitigate vulnerabilities.
- Monitor for telltale symptoms of infection, such as performance issues and unexpected system changes.

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
<b>Critical Zero-Day Vulnerability in Cisco AsyncOS Email Security Appliances Actively Exploited</b>	<b>HIGH</b>	<b>CLEAR</b>	<b>Vulnerability</b>	<b>CSC</b>

### Executive Summary

Cisco has identified a critical zero-day vulnerability in its AsyncOS Email Security Appliances, allowing unauthenticated remote attackers to execute arbitrary commands with elevated privileges. This vulnerability, tracked as CVE-2025-20393, poses a significant risk as it is currently being exploited in the wild, targeting products such as the Cisco Secure Email Gateway and Cisco Secure Email and Web Manager.

The financial services sector must take immediate action to mitigate this vulnerability due to its potential impact on confidentiality, integrity, and availability of sensitive data. The exploitation can lead to

unauthorized access and persistent threats, making it crucial for organizations to implement recommended security measures to protect their email security infrastructure.

### Technical Details

- The vulnerability is tracked as CVE-2025-20393 with a CVSS score of 10.0, indicating critical severity.
- It allows remote attackers to execute arbitrary commands with root privileges on affected appliances.
- Successful exploitation requires the Spam Quarantine feature to be enabled and accessible from the internet.
- Affected Products include Cisco AsyncOS Email Security Appliances:
  - Cisco Secure Email Gateway (SEG)
  - Cisco Secure Email and Web Manager (SEWM)
- Attackers have deployed tools such as ReverseSSH, Chisel, AquaPurge, and AquaShell to maintain access and evade detection.
- The AquaShell backdoor listens for unauthenticated HTTP POST requests and executes commands via the system shell.
- Persistence mechanisms identified may survive standard remediation actions, complicating recovery efforts.
- The impact includes potential loss of confidentiality, integrity, and availability of data.
- Cisco recommends rebuilding affected appliances as the only reliable method to remove persistence mechanisms.
- Mitigations include restricting internet exposure, limiting access to trusted IPs, and monitoring logs for suspicious activity.
- Organizations are advised to enforce strong authentication and update default credentials to enhance security.

### Recommendations

- Restrict or remove internet exposure of affected appliances to minimize attack vectors.
- Limit access to trusted IPs and segregate management interfaces to enhance security.
- Disable HTTP access and unnecessary services on affected appliances.
- Monitor logs for any suspicious activity to detect potential exploitation attempts.
- If compromise is suspected, rebuild affected appliances to ensure full remediation of the vulnerability.

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

[back to top](#)



Name	Threat Severity Rating	TLP	Attribution	Originating Source
SonicWall SMA1000 Appliance Vulnerability Allows Remote Code Execution	HIGH	CLEAR	Vulnerability	CSC

### Executive Summary

SonicWall has released a security update for an actively exploited zero-day vulnerability affecting the SMA1000 appliance management console. The flaw, tracked as CVE-2025-40602, enables attackers to escalate privileges and gain broader system control, potentially leading to unauthenticated remote code execution with root privileges when exploited in conjunction with another critical vulnerability, CVE-2025-23006.

This vulnerability poses significant risks to the financial services sector, as successful exploitation could allow attackers to compromise systems and access sensitive data. Financial institutions using affected versions of the SMA1000 appliance are urged to apply the security patch immediately to mitigate the risk of exploitation.

### Technical Details

- The vulnerability CVE-2025-40602 is categorized as a local privilege escalation due to insufficient authorization in the SonicWall SMA1000 appliance management console.
- It allows attackers to escalate privileges and gain broader control over the system, leading to potential unauthorized access.
- The flaw has been confirmed to be actively exploited in real-world attack scenarios, particularly in conjunction with CVE-2025-23006.
- CVE-2025-23006 has a higher CVSS score of 9.8 and enables unauthenticated remote code execution with root privileges.
- Affected versions include SMA1000 - 12.4.3-03093 and earlier, as well as 12.5.0-02002 and earlier.
- The exploitation chain requires either the presence of CVE-2025-23006 or access to a local system account.
- Systems that remain unpatched are at high risk of full appliance compromise, especially if management interfaces are exposed to the internet.
- SonicWall has provided a patch to mitigate the vulnerabilities, with recommended versions being 12.4.3-03245 and higher, and 12.5.0-02283 and higher.
- Workarounds include restricting access to the management console and disabling public internet access for SSH and SSL VPN management interfaces.

### Recommendations

- Immediately upgrade SonicWall SMA1000 appliances to the latest fixed versions to address the vulnerability.
- Implement access restrictions to the management console, allowing SSH access only via VPN or specific admin IPs.

- Disable SSL VPN management interface and SSH access from the public internet to reduce exposure.
- Regularly monitor and patch systems to ensure vulnerabilities are addressed promptly.
- Conduct security assessments to identify and remediate any systems that may still be vulnerable.

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
<b>Critical Remote Code Execution Vulnerability in HPE OneView Software</b>	<b>MEDIUM</b>	<b>CLEAR</b>	<b>Vulnerability</b>	<b>CSC</b>

### Executive Summary

Hewlett Packard Enterprise (HPE) has released a security bulletin addressing a critical remote code execution (RCE) vulnerability affecting HPE OneView Software. Identified as CVE-2025-37164, this flaw allows a remote, unauthenticated attacker to execute arbitrary code on affected systems, posing a significant risk to organizations using this software. Immediate remediation is strongly recommended due to the potential for full system compromise.

This vulnerability matters to the financial services sector as it could lead to unauthorized access and control over critical infrastructure, jeopardizing sensitive financial data and operations. Organizations utilizing HPE OneView must prioritize upgrading to the fixed version or applying security hotfixes to mitigate the risk associated with this critical vulnerability.

### Technical Details

- CVE ID: CVE-2025-37164, classified as a critical remote code execution vulnerability.
- CVSS v3.1 base score of 10.0 indicates maximum severity and potential for full system compromise.
- The attack vector is network-based, requiring no authentication from the attacker.
- User interaction is not needed for exploitation, increasing the vulnerability's risk.
- Affected products include all versions of HPE OneView prior to v11.00.
- The fixed version is HPE OneView v11.00 or later.
- Immediate action is required to upgrade affected deployments to the fixed version.
- For those unable to upgrade immediately, applying the HPE-provided security hotfix for versions 5.20–10.20 is recommended.
- Ensure that hotfixes are reapplied after any appliance upgrade or reimage to maintain security..

### Recommendations

- Upgrade all affected HPE OneView deployments to version 11.00 or later without delay.
- Deploy the HPE-provided security hotfix for versions 5.20–10.20 where immediate upgrades are not

feasible.

- Implement a schedule for regular updates and patches to maintain system security.
- Conduct a security audit to identify any other potential vulnerabilities in the infrastructure.
- Train staff on recognizing and responding to potential security threats related to RCE vulnerabilities.

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
<b>Critical Remote Code Execution</b> <b>Vulnerability in pgAdmin</b> <b>Exposes Database Servers</b>	<b>MEDIUM</b>	<b>CLEAR</b>	<b>Vulnerability</b>	<b>CSC</b>

### Executive Summary

A critical Remote Code Execution (RCE) vulnerability has been identified in pgAdmin, the widely used open-source PostgreSQL management tool. Tracked as CVE-2025-13780, this flaw allows authenticated attackers to execute arbitrary system commands on the pgAdmin server through a maliciously crafted database restore file. This vulnerability bypasses a previously implemented security fix and poses a severe risk to database servers operating in server mode.

This vulnerability is particularly concerning for the financial services sector, as it could lead to significant data breaches and infrastructure compromise. Organizations utilizing pgAdmin in server mode must prioritize immediate remediation efforts to safeguard sensitive financial data and maintain operational integrity.

### Technical Details

- CVE ID: CVE-2025-13780, classified as a critical Remote Code Execution vulnerability.
- CVSS v3 Score: 9.1, indicating a high severity level for potential exploitation.
- The vulnerability allows authenticated attackers to execute arbitrary system commands on the pgAdmin server.
- Exploitation occurs through a maliciously crafted database restore file in PLAIN-format SQL dump.
- Affected deployment mode: Server mode, which is commonly used in production environments.
- All versions of pgAdmin up to and including 9.10 are vulnerable.
- The flaw represents a bypass of a prior security fix (CVE-2025-12762).
- Fixed versions are available in pgAdmin 9.11 or later.
- Organizations are urged to apply patches or mitigations immediately.
- Potential for large-scale data and infrastructure compromise if left unaddressed.

### Recommendations

- Immediately apply patches to upgrade to pgAdmin version 9.11 or later to mitigate the vulnerability.

- Review and restrict access to pgAdmin servers to limit potential exploitation by unauthorized users.
- Implement monitoring for unusual activity on pgAdmin servers to detect potential exploitation attempts.
- Educate staff on the risks associated with malicious database restore files and secure handling practices.
- Regularly review and update security policies to address vulnerabilities in open-source tools.

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity OS Command Injection Vulnerability in systeminformation Node.js Library	MEDIUM	CLEAR	Vulnerability	CSC

### Executive Summary

A high-severity security vulnerability, tracked as CVE-2025-68154, has been identified in the widely used systeminformation Node.js library. The flaw affects Windows-based environments and exposes applications to OS Command Injection, potentially resulting in Remote Code Execution (RCE). Given the library's extensive adoption—reportedly exceeding 16 million downloads per month—the potential impact is significant.

Affected applications include monitoring dashboards, command-line utilities, and web applications that rely on systeminformation to retrieve filesystem and operating system metrics. If successfully exploited, this vulnerability may allow attackers to execute arbitrary PowerShell commands with the privileges of the running Node.js process, leading to full system compromise.

### Technical Details

- CVE ID: CVE-2025-68154, categorized as a high-severity OS Command Injection vulnerability.
- The vulnerability affects the fsSize() function within the systeminformation library.
- Affected versions include systeminformation v5.27.13 and earlier, specifically on Windows platforms.
- The flaw allows for Remote Code Execution (RCE), enabling execution of arbitrary commands.
- Attackers can read sensitive files and exfiltrate data if the vulnerability is exploited.
- Privilege escalation is possible if the Node.js process runs with elevated privileges.
- Compromised systems can be used for lateral movement within the internal network.
- Attackers may deploy ransomware by downloading and executing malicious payloads.
- The patched version, systeminformation v5.27.14, includes proper input sanitization to mitigate the vulnerability.

- Applications that pass user-controlled input to fsSize(drive) are particularly at risk.

### Recommendations

- Immediately update the systeminformation library to version 5.27.14 or later to mitigate the vulnerability.
- Implement input validation and sanitization for any user-controlled input passed to the fsSize() function.
- Monitor applications using systeminformation for unusual behavior indicative of exploitation attempts.
- Conduct regular security assessments to identify and remediate vulnerabilities in third-party libraries.
- Educate development teams on secure coding practices to prevent similar vulnerabilities in the future.

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerability in Zoom Rooms for Windows Allows Privilege Escalation	MEDIUM	CLEAR	Vulnerability	Open Source

### Executive Summary

Zoom has released security updates addressing a high-severity vulnerability, CVE-2025-67460, affecting its Zoom Rooms for Windows products prior to version 6.6.0. This flaw may allow an unauthenticated user to escalate privileges via local access, posing a significant risk to system integrity.

The vulnerability, rated 7.8 on the CVSS scale, highlights the importance of timely software updates in the financial services sector. Exploitation could lead to unauthorized access and manipulation of sensitive data, emphasizing the need for organizations to implement robust patch management practices.

### Technical Details

- The vulnerability is classified as a 'Protection Mechanism Failure' in Zoom Rooms for Windows prior to version 6.6.0.
- It allows for potential escalation of privileges by an unauthenticated user with local access to the system.
- The CVE-ID for this vulnerability is CVE-2025-67460, with a CVSS score of 7.8.
- No proof-of-concept exploit is publicly available at this time.
- Zoom has released a patch to mitigate the vulnerability and recommends immediate upgrades.
- There are currently no reports of exploitation of this vulnerability in the wild.
- The flaw underscores the necessity for organizations to maintain updated software to prevent potential security breaches.



- Administrators are urged to prioritize the application of the latest security updates to safeguard their systems.
- The vulnerability could lead to unauthorized access, increasing the risk of data breaches.
- Prompt action is advised to alleviate any potential threats associated with this vulnerability.

### Recommendations

- Upgrade to Zoom Rooms for Windows version 6.6.0 or later to mitigate the vulnerability.
- Implement a regular patch management process to ensure timely updates of all software.
- Conduct security assessments to identify and remediate any potential vulnerabilities in the system.
- Educate staff on the importance of maintaining updated software and recognizing security threats.
- Monitor systems for any unusual activity that may indicate attempts to exploit vulnerabilities.

[Reference to the Source](#)

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerabilities in React Server Components Require Immediate Attention	MEDIUM	CLEAR	Vulnerability	Open Source

### Executive Summary

The React team has released security updates addressing two high-severity vulnerabilities in the React Server Components (RSC) product, tracked as CVE-2025-55184 and CVE-2025-67779. These vulnerabilities, categorized as 'Deserialization of Untrusted Data', can lead to service disruptions through specially crafted payloads but do not permit remote code execution.

The financial services sector should be particularly vigilant as successful exploitation could lead to complete service disruption (DoS), impacting operations and customer trust. With the increasing exploitation of related vulnerabilities, it is crucial for organizations to apply the recommended patches and ensure their systems are updated to mitigate potential threats.

### Technical Details

- Two high-severity vulnerabilities identified in React Server Components, CVE-2025-55184 and CVE-2025-67779, both rated 7.5 on the CVSS scale.
- The vulnerabilities are related to deserialization issues in Server Function request handling, which can trigger infinite loops.
- Successful exploitation could allow a remote threat actor to cause a denial of service (DoS) by using crafted circular reference payloads.
- The vulnerabilities do not allow for remote code execution, limiting the scope of potential attacks.
- A proof-of-concept (PoC) exploit for CVE-2025-55184 has been published on GitHub, increasing the

urgency for patching.

- The affected versions of React Server Components include those prior to 19.0.3, 19.1.4, and 19.2.3.
- Administrators are advised to upgrade to the latest versions immediately to mitigate risks.
- Previous updates related to other critical vulnerabilities may require further action to ensure complete protection.
- As of now, there are no reports of active exploitation of these vulnerabilities.
- The React team emphasizes the importance of vigilance due to the rising threats in the ecosystem.

### Recommendations

- Immediately upgrade to React Server Components versions 19.0.3, 19.1.4, or 19.2.3 to mitigate vulnerabilities.
- Review and apply any outstanding patches related to previous critical vulnerabilities.
- Monitor for any signs of exploitation or unusual activity in your systems.
- Educate staff on the importance of timely updates and the risks associated with unpatched software.
- Implement robust monitoring solutions to detect potential denial of service attacks.

[Reference to the Source](#)

[back to top](#)

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft Discloses Critical Vulnerabilities in Azure and Office Products	MEDIUM	CLEAR	Vulnerability	Open Source

### Executive Summary

Microsoft has disclosed a series of vulnerabilities affecting its Azure and Office product lines, including critical flaws with CVSS scores of 10.0. These vulnerabilities can lead to unauthorized remote code execution, privilege escalation, and spoofing, posing significant risks to systems and data within the financial services sector.

The implications of these vulnerabilities are considerable, especially for organizations utilizing Microsoft products for their operations. The potential for exploitation could lead to severe disruptions in services, unauthorized access to sensitive data, and financial losses, highlighting the need for immediate attention to security updates and patches.

### Technical Details

- CVE-2025-65041: Critical flaw in Microsoft Partner Center due to improper authorization, with a CVSS score of 10.0.
- CVE-2025-65037: Critical vulnerability in Azure Container Apps related to improper control of code

generation, also rated 10.0.

- CVE-2025-64677: High severity issue in Office Out-of-Box Experience due to improper neutralization of input, CVSS score of 8.2.
- CVE-2025-64676: Vulnerability in Microsoft Purview, rated 7.2, associated with improper control of code generation.
- CVE-2025-64675: High severity flaw in Azure Cosmos DB due to improper neutralization of input, with a CVSS score of 8.3.
- CVE-2025-64663: SSRF vulnerability with a CVSS score of 9.9, affecting various Microsoft products.
- The vulnerabilities can lead to unauthorized remote code execution, privilege escalation, and spoofing.
- Microsoft has provided patches and security updates to mitigate the identified flaws.
- No reports of active exploitation of these vulnerabilities have been noted at this time.
- Organizations should prioritize applying the available mitigations to safeguard their systems.

### Recommendations

- Ensure all Microsoft products are updated with the latest patches and security updates.
- Conduct a thorough assessment of systems utilizing affected Microsoft services to identify vulnerabilities.
- Implement monitoring solutions to detect any unusual activities related to the vulnerabilities.
- Educate staff on the risks associated with these vulnerabilities and the importance of security hygiene.

[Reference to the Source](#)

[back to top](#)

## Appendix A - Tactics, Techniques & Procedures (TTPs)

### BlackForce Phishing Kit Targets Financial Services with Advanced MitB Techniques TTPs

ID	TECHNIQUE
T1566	Phishing
T1027	Obfuscated Files or Information
T1557	Adversary-in-the-Middle
T1555	Credentials from Password Stores
T1665	Hide Infrastructure
T1567	Exfiltration Over Web Service
T1657	Financial Theft

### Malicious NuGet Package Typosquats .NET Tracing Library to Steal Wallet Passwords TTPs

ID	TECHNIQUES
T1585	Establish Accounts
T1587.001	Develop Capabilities: Malware
T1608.001	Stage Capabilities: Upload Malware
T1195.002	Supply Chain Compromise: Compromise Software Supply Chain
T1204.005	User Execution: Malicious Library
T1036	Masquerading
T1656	Impersonation
T1552	Unsecured Credentials
T1005	Data from Local System
T1041	Exfiltration Over C2 Channel
T1657	Financial Theft

## New SantaStealer Malware Campaign Targets Financial Sector with Advanced Information Theft Capabilities TTPs

TACTICS	TECHNIQUES
T1087	Account Discovery
T1020	Automated Exfiltration
T1002	Data Compressed
T1217	Browser Information Discovery
T1560	Archive Collected Data
T1030	Data Transfer Size Limits
T1560.002	Archive via Library
T1119	Automated Collection
T1041	Exfiltration Over C2 Channel
T1115	Clipboard Data
T1622	Debugger Evasion
T1087.003	Email Account
T1083	File and Directory Discovery
T1552.001	Credentials In Files
T1555	Credentials from Password Stores
T1005	Data from Local System
T1503	Credentials from Web Browsers
T1657	Financial Theft
T1555.003	Credentials from Web Browsers
T1081	Credentials in Files
T1587.001	Malware
T1057	Process Discovery
T1114.001	Local Email Collection



T1213.005	Messaging Applications
T1113	Screen Capture
T1583.004	Server
T1518	Software Discovery
T1497.001	System Checks
T1574.001	DLL
T1082	System Information Discovery
T1614.001	System Language Discovery
T1497.003	Time Based Evasion
T1497	Virtualization/Sandbox Evasion
T1140	Deobfuscate/Decode Files or Information
T1071.001	Web Protocols
T1145	Private Keys
T1552.004	Private Keys
T1027.007	Dynamic API Resolution
T1528	Steal Application Access Token
T1539	Steal Web Session Cookie
T1027.009	Embedded Payloads
T1027.013	Encrypted/Encoded File
T1070.004	File Deletion
T1107	File Deletion
T1055.002	Portable Executable Injection
T1055.012	Process Hollowing
T1093	Process Hollowing
T1620	Reflective Code Loading

## 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	Recipients may share TLP:AMBER+STRICT

	information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	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
AES-256-GCM	Strong encryption mode used by ransomware to lock files or hide data.
API	Application Programming Interface: rules that let software talk to other software.
APT	Advanced Persistent Threat: a prolonged, targeted intrusion where an attacker stays hidden for a long time.
AquaPurge	Helper tool observed alongside AquaShell to maintain attacker access.
AquaShell	Backdoor observed on compromised Cisco email appliances for command execution.
Autolt	Windows scripting tool; attackers use it to automate malicious tasks.
AWS	Amazon's cloud services for running applications and storing data.
AWS Security Hub	AWS dashboard that centralizes and prioritizes security findings.
Azure	Microsoft's cloud platform for compute, storage, and security services.
Azure Container Apps	Azure service to run apps in containers; a critical vulnerability required fixes.
Azure Cosmos DB	Fully managed NoSQL database service in Azure; recent input-neutralization flaw required fixes.
Base64	A simple encoding used to conceal scripts or commands in attacks.
BlackForce	Phishing toolkit that can bypass MFA using man-in-the-browser techniques to

	steal logins.
C2	Command and Control: servers/services attackers use to control infected machines.
Cache busting	Forcing browsers to load the latest script; phishing kits use it for updated malicious code.
ChaCha20	Fast stream cipher used to obfuscate data in malware payloads.
Chisel	Lightweight tunneling tool used to bypass network restrictions.
Cisco AsyncOS	Cisco's email security software used in Secure Email Gateway appliances.
Cisco Secure Email and Web Manager	Central management for Cisco email/web security appliances.
Cisco Secure Email Gateway	Cisco appliance that filters and protects email; a recent zero-day allowed remote commands.
ClickFix	Fake 'human verification' or 'how to fix' steps that trick users into running attacker commands.
CSC	UAE Cyber Security Council
CVE	Common Vulnerabilities and Exposures: public list of known security flaws.
CVSS	Common Vulnerability Scoring System: severity score for security flaws.
CyberVolk	Pro-Russia hacktivist group running ransomware operations and coordinating via Telegram.
DarkGate	Malware delivered via social-engineering prompts; enables remote control and data theft.
Denial of Service (DoS)	Knocking a system offline by overwhelming or crashing it.
DES	Older encryption algorithm sometimes found in malware components.
Deserialization of untrusted data	Turning attacker-controlled data into program objects—can crash or lead to exploits.
Disable API termination	Prevents shutting down a cloud instance via API; attackers use it to persist.
DLL	Dynamic Link Library: shared code used by Windows programs.
DLL sideloading	Tricking a legitimate app into loading a malicious library.
Docker Hub	Public site for sharing container images; attackers may upload malicious images.
Double extortion	Steal data first, then encrypt systems to pressure payment.
DryRun (AWS)	Test flag in AWS API calls to check if permissions would succeed—attackers probe access with it.
EC2	AWS virtual machines used to run applications.
ECS	AWS service to run and scale containerized applications.
EDR	Endpoint Detection and Response: monitors computers and responds to threats.
Exfiltration	Quietly sending data out of your network to an attacker's server.
fsSize() (systeminformation)	Function in a popular Node.js library that had an injection flaw on Windows.
Golang	Language often used for cross-platform malware and tooling (Linux/Windows).
Guard.NotNull<T>	.NET helper function that was abused to hide malicious behavior in a typosquatted package.
GuardDuty	AWS threat-detection service that flags suspicious activity in accounts.
Homoglyph attack	Using visually similar letters (Latin vs. Cyrillic) to disguise malicious names/domains.
HPE OneView	HPE infrastructure management software; a critical flaw enabled remote code execution.
HTA (HTML Application)	Windows app format that can execute scripts—often abused in phishing.
IAM	Identity and Access Management: controls who can access what in systems.
Initial Access Broker (IAB)	Sells stolen credentials or footholds to other threat actors (e.g., ransomware affiliates).
In-memory (fileless) malware	Runs mainly in memory, avoiding files so traditional antivirus is less likely to catch it.
Keylogger	Tool that records keystrokes to steal passwords and other sensitive data.
MFA	Multi-Factor Authentication: use two or more checks (e.g., password + phone) to sign in.
Microsoft Partner Center	Microsoft portal for partners; a critical flaw was disclosed requiring patching.



Microsoft Purview	Microsoft data governance and compliance service; had a notable security issue.
MitB	Man-in-the-Browser: malware alters what a user sees/does in the browser to steal data.
Obfuscation	Hiding code/commands to avoid detection or make analysis harder.
Office OOBE	Office Out-of-Box Experience: initial setup flow; an input neutralization bug was patched.
On-Demand Instances	Standard priced AWS compute capacity without long-term commitment.
OS Command Injection	User input passed to system commands lets attackers run their own commands.
pgAdmin	GUI tool to manage PostgreSQL databases; server-mode flaw allowed command execution during restore.
Phishing-resistant MFA	Strong MFA (e.g., security keys) that prevents attackers from stealing one-time codes.
PoC (Proof of Concept)	Demonstration showing a vulnerability is real and exploitable.
Privilege escalation	Gaining higher-level access on a system than intended.
Qilin	Ransomware-as-a-service group known for double-extortion (data theft + encryption).
RaaS	Ransomware-as-a-Service: criminals sell or rent ransomware to others.
RAT	Remote Access Tool: software that lets attackers control a computer from afar.
RCE	Remote Code Execution: attackers run their own code on your system remotely.
React Server Components (RSC)	Part of React used on servers; flaws could crash services (denial of service).
ReverseSSH	Tool that opens hidden outbound connections for remote control.
SantaStealer	Malware-as-a-service info-stealer marketed on Telegram/underground forums; targets credentials and wallets.
SMB	Server Message Block: Windows file-sharing network protocol.
SonicWall SMA1000	SonicWall's secure remote access appliance; recent flaws enabled privilege escalation and RCE.
Spam Quarantine (Cisco)	Holding area for suspected spam; internet exposure can become an attack entry point.
Spot Instances	Discounted spare AWS compute capacity; attackers may abuse for cheap scaling.
SSRF (Server-Side Request Forgery)	Forcing a server to make internal requests—can leak data or reach internal services.
StealC	Infostealer malware used to steal logins and sensitive data from infected systems.
Supply-chain attack	Compromising a trusted provider to infect many downstream users.
Telegram (as C2)	Messaging platform abused to control malware or coordinate criminal operations.
Term / Acronym	Meaning / Description
TTP	Tactics, Techniques, and Procedures: how attackers operate.
Typosquatting	Publishing a look-alike package/app name to trick people into installing it.
UAC	User Account Control: Windows feature that prevents unauthorized changes.
VolkLocker	CyberVolk's ransomware service that encrypts files to extort payment; design flaws can allow recovery.
Volume Shadow Copy (VSS)	Windows snapshots; ransomware deletes these to block easy recovery.
Windows Registry Run key	Startup setting; malware writes here to relaunch on boot.
Zero Trust	Never trust, always verify': limit access by default and continuously check user/device posture.
Zero-Day	A flaw exploited before a fix is available from the vendor.
Zoom Rooms (Windows)	Zoom's conference room solution for Windows; a bug allowed local privilege escalation.