TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	16/7/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 16 July 2026

7	3	0	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Financial Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the Middle East impacting Financial Sector

Summary

This week's cybersecurity newsletter highlights a broad mix of identity-focused phishing campaigns, software supply chain threats, cloud-service abuse, credential theft operations, and high-impact vulnerabilities affecting enterprise technologies. Threat actors were observed targeting developers through malicious software packages, abusing Microsoft 365 authentication workflows, conducting large-scale GitHub reconnaissance, stealing cloud-hosted data through identity compromise, and expanding covert infrastructure using compromised networking devices. For organizations in the financial sector, these developments reinforce the importance of securing identities, privileged access, backup infrastructure, cloud collaboration platforms, and externally accessible services. Several newly disclosed vulnerabilities could enable unauthorized access, privilege escalation, or remote code execution, while multiple campaigns demonstrate a continued shift toward credential theft, session hijacking, cloud data access, and post-compromise persistence. Organizations should prioritize timely patching, strengthen authentication controls, monitor for anomalous account activity, and ensure critical systems are continuously reviewed for signs of unauthorized access and abuse.

ADGM THREAT INTELLIGENCE SUMMARY

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Typosquatting Campaign Targets Payment SDK Users Across npm and PyPI	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Socket has identified a coordinated typosquatting campaign involving 17 malicious packages published across npm and PyPI. The packages impersonate software development kits associated with widely used payment applications and are designed to steal credentials and authentication tokens by masquerading as legitimate development tools.

Organizations in the financial sector should be aware that developers relying on third-party packages could unknowingly introduce malicious code into their environments. The activity may impact payment-related development workflows and could affect systems where exposed credentials or tokens provide access to sensitive services and resources.

Technical Details

- The campaign involved 17 malicious packages published almost simultaneously across the npm and PyPI repositories, indicating a coordinated operation.
- The packages were crafted to imitate legitimate payment SDKs used by developers, increasing the likelihood of accidental installation.
- Several packages presented themselves as functional payment libraries and exposed methods that appeared similar to legitimate payment and customer management operations.
- The fake SDKs returned successful responses to users, creating the impression that normal application functionality was occurring.
- Instead of communicating with legitimate payment services, the packages collected sensitive information from the local environment.
- The malware specifically attempted to access credentials and configuration values stored as environment variables, including API-related information.
- When sensitive information was identified, the malicious code-initiated data theft activity and transmitted stolen credentials and tokens to attacker-controlled infrastructure.
- The packages included anti-analysis checks designed to avoid execution in security testing environments and automated analysis systems.
- The malware checked system characteristics such as processor availability, hostname values, and user account names for indicators commonly associated with sandbox environments.
- Infrastructure details were concealed through multiple decoding stages, making it more difficult to identify attacker-controlled destinations during analysis.

Recommendations

- Review development environments for the affected packages and remove any unauthorized or unverified dependencies.

- Validate all third-party packages before installation and confirm package names against official project sources.
- Rotate credentials, API keys, and tokens that may have been exposed through affected development systems.
- Monitor developer workstations and build environments for unusual access to environment variables and credential stores.
- Strengthen package governance processes, including dependency approval, monitoring, and continuous review of newly introduced libraries.

For a detailed breakdown of Tactics, Techniques, and Procedures (TTPs), refer to the Annexure – Typosquatting Campaign Targets Payment SDK Users Across npm and PyPI

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
Forg365 PhaaS Targeting Microsoft 365 Through Device Code and AiTM Phishing	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at ZeroBEC has identified Forg365, a Telegram-distributed phishing-as-a-service platform targeting Microsoft 365 users. The platform combines device code phishing and adversary-in-the-middle (AiTM) techniques, using convincing business-themed lures and legitimate authentication workflows to trick users into authorizing attacker-controlled sessions, while enabling the theft of authentication tokens and browser session data.

Organizations in the financial sector should be aware that token-focused phishing campaigns such as Forg365 could affect cloud-based collaboration and email environments even when users are protected by multi-factor authentication. The platform's post-compromise capabilities may impact organizations that rely heavily on Microsoft 365 services by facilitating unauthorized mailbox access, session persistence, and further account abuse.

Technical Details

- The Forg365 operation is distributed through Telegram and provides operators with a phishing-as-a-service platform designed specifically to target Microsoft 365 accounts. The service includes tools for phishing campaign creation, token management, and post-compromise operations.
- Attack campaigns begin with phishing emails that use business document or approval-themed lures. The messages are designed to encourage recipients to follow embedded links and interact with attacker-controlled workflows.

- The phishing infrastructure uses legitimate email delivery and hosting services to make campaign traffic appear more trustworthy and blend with normal business communications.
- Victims are directed through a series of redirects that determine whether they are presented with a device code phishing flow or an AiTM phishing page. The selected path depends on traffic classification and visitor conditions.
- In the device code phishing workflow, victims are shown a Microsoft-styled verification page and guided through a legitimate authentication process that ultimately authorizes an attacker-controlled session.
- The AiTM component acts as an intermediary between the victim and authentication services, enabling the collection of session information, authentication tokens, and browser cookies after successful login.
- Captured tokens are stored and managed through a dedicated token vault, allowing operators to organize and use compromised account access.
- The platform includes mailbox intelligence and monitoring capabilities that help operators review compromised mailboxes and search for information of interest.
- A browser extension known as ForgCookie is used to refresh Microsoft single sign-on cookies, helping attackers maintain browser-based access over time.
- Anti-bot and cloaking mechanisms redirect suspected security researchers or VPN users to benign content, reducing the visibility of phishing pages and hindering analysis efforts.

Recommendations

- Monitor Microsoft 365 environments for suspicious device-code authentication events and unexpected consent activity.
- Review and restrict device code authentication where it is not required for business operations.
- Continuously monitor for unusual mailbox access, token usage, and session activity across cloud environments.
- Implement user awareness training focused on document-themed phishing lures and unexpected authentication requests.
- Investigate and revoke active sessions, tokens, and credentials associated with suspected compromised accounts.

For a detailed breakdown of Tactics, Techniques, and Procedures (TTPs), refer to the Annexure – Forg365 PhaaS Targeting Microsoft 365 Through Device Code and AiTM Phishing

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
Coordinated GitHub API Campaign Uses Ghost Accounts and Token Abuse for Reconnaissance	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Datadog Security Research has identified several coordinated campaigns that systematically enumerate GitHub organizations, repositories, and user accounts through the GitHub API. The activity relies on automated scraping tools, long-dormant "ghost" accounts, and compromised OAuth or personal access tokens to blend reconnaissance activity into normal API traffic while mapping corporate development environments.

Organizations in the financial sector should be aware that this activity could affect software development and source code management environments by exposing information about organizational structures, repositories, and developer accounts. In a limited number of cases, the activity progressed beyond reconnaissance and appeared to result in access to private repositories, highlighting the risks associated with compromised access tokens.

Technical Details

- Researchers observed multiple overlapping campaigns rather than a single threat actor operation. The activity focused on systematically collecting information about GitHub organizations, repositories, and associated user accounts.
- Attackers used automated tools to query GitHub APIs over extended periods, allowing them to build detailed maps of targeted organizations and their development ecosystems.
- The campaigns relied heavily on dormant "ghost" accounts that had been created years earlier and left inactive before being used for reconnaissance operations. This helped the activity appear more legitimate than newly created accounts.
- More than 50 ghost accounts were observed conducting API requests in coordinated bursts across multiple organizations. Activity often lasted for several weeks before the accounts became inactive again.
- Much of the reconnaissance focused on publicly accessible GitHub data, including repositories, organization memberships, user relationships, and other information available through GitHub APIs.
- The attackers primarily used GraphQL queries, while also leveraging REST API routes to gather information from different parts of the GitHub platform.
- To reduce suspicion, the tools used custom or legitimate-sounding user-agent names that resembled analytics, monitoring, or dashboard applications.
- In addition to ghost accounts, researchers observed the abuse of compromised OAuth credentials and personal access tokens belonging to legitimate users. These credentials enabled activity to originate from trusted accounts.

- Some campaigns targeted private repository commit paths using compromised tokens from dozens of legitimate accounts within short time periods. This represented a move beyond basic reconnaissance.
- In a small number of observed cases, the activity appeared to escalate from information gathering to the successful cloning of private repositories, resulting in unauthorized access to source code.

Recommendations

- Review GitHub audit logs for unusual API activity, especially large-scale enumeration originating from unfamiliar accounts or user agents.
- Audit OAuth applications and personal access tokens regularly, and revoke any tokens that are unnecessary, exposed, or inactive.
- Monitor for unexpected access to private repositories, repository cloning activity, and unusual commit-path requests.
- Implement least-privilege access controls and restrict token permissions to only the resources required for business operations.
- Investigate developer accounts exhibiting abnormal API usage patterns or access behavior that differs from established baselines.

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
Vidar Stealer MaaS Affiliate Target Users Through Fake Cracked Software	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Unit 42 has identified a financially motivated campaign in which a Vidar Stealer malware-as-a-service affiliate uses malicious advertisements and fake cracked software downloads to infect victims. Users searching for pirated software are redirected to fraudulent download pages hosting password-protected archives that deploy both the Vidar Stealer and the XMRig cryptocurrency miner, enabling credential theft and illicit Cryptomining from a single infection.

Organizations in the financial sector should be aware that this campaign may impact employees who download unauthorized software on corporate devices. The combination of information theft and cryptocurrency mining could affect system security and operational performance, particularly where compromised credentials provide access to business applications or sensitive resources.

Technical Details

- The campaign begins with malvertising activity that targets users searching online for cracked or pirated versions of commercial software. Victims are redirected to convincing download pages that impersonate legitimate software sources.

- Users are instructed to download password-protected archives that appear to contain the desired software. The protected archive structure helps the malware avoid some automated inspection processes.
- Once the downloaded file is executed, a loader is launched that prepares the environment for the delivery of additional malicious payloads. The loader is responsible for deploying both credential-stealing and cryptomining components.
- The attackers use the Factory-v3 framework, which acts as the delivery mechanism for the malware payloads and supports large-scale distribution efforts.
- To reduce the chances of detection, the loader uses file inflation techniques that significantly increase file size by appending large amounts of unnecessary data.
- Researchers also observed the use of fake code-signing metadata designed to make the malicious files appear more trustworthy to users.
- The malware attempts to weaken security controls by interfering with scanning mechanisms before deploying its payloads. This helps the attackers execute additional malicious activity with less visibility.
- After execution, Vidar Stealer collects sensitive information from the infected device, including browser-stored credentials, cookies, cryptocurrency wallet information, and other user data.
- At the same time, XMRig is deployed to use the victim's computing resources for cryptocurrency mining, generating additional revenue for the attackers.
- This dual-payload approach allows the operators to monetize each compromised device through both data theft and ongoing cryptomining activity.

Recommendations

- Restrict the download and execution of unauthorized or pirated software on corporate systems.
- Monitor endpoints for unusual resource consumption that may indicate unauthorized cryptocurrency mining.
- Review systems for signs of credential theft activity and promptly rotate potentially exposed credentials.
- Implement application control policies to prevent execution of untrusted files and installers.
- Educate users about the risks of downloading software from unofficial sources and suspicious advertisements.

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
Helix Data Extortion Campaign Targets Identity and Cloud Collaboration Platforms	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at ReliaQuest has identified Helix, a data extortion group that targets cloud collaboration and identity platforms through voice phishing, device code phishing, and multi-factor authentication abuse. The attackers impersonate trusted individuals to convince users to authorize attacker-controlled sessions, then establish persistence and access cloud-hosted data within Microsoft 365 environments.

Organizations in the financial sector should be aware that identity-focused attacks such as those used by Helix could affect cloud collaboration platforms without requiring malware deployment or software exploitation. The campaign may impact organizations that rely heavily on cloud-based document repositories and identity services, particularly where compromised accounts provide access to sensitive business information.

Technical Details

- The campaign begins with targeted voice phishing calls in which attackers impersonate trusted personnel and use organizational details to build credibility with victims. This social engineering approach is used to initiate the compromise process.
- During the interaction, victims are guided through a device code phishing workflow that authorizes an attacker-controlled session. The technique allows attackers to gain account access without requiring the victim's password.
- After obtaining access, the operators quickly register a new MFA authenticator on the compromised account. This provides a persistent method of access that remains under attacker control.
- The attackers use infrastructure and access methods designed to blend with normal user activity. Researchers observed the use of residential proxy services and rotating source addresses to reduce suspicion.
- Once persistence is established, the operators begin exploring the cloud environment to identify accessible resources and locations containing valuable information.
- The group conducts SharePoint reconnaissance by inventorying available sites and content before beginning large-scale collection efforts. This activity serves as a consistent pattern across observed incidents.
- Following reconnaissance, attackers automate the collection and download of files from accessible repositories. The objective is to gather data that can later be used for extortion.
- Researchers observed a separation of roles between compromised accounts in some incidents. One account was used for data collection activities, while another account was later used to deliver extortion messages internally.
- This separation of activities complicates investigations because the account responsible for extortion may not be the same account involved in data theft.

- The campaign focuses on data extortion rather than malware deployment, using stolen cloud-hosted information as leverage to pressure victims after exfiltration.

Recommendations

- Disable device code authentication where it is not required for business operations.
- Monitor for new MFA registration events and investigate unexpected changes to authentication methods.
- Review cloud collaboration platforms for unusual file enumeration, bulk downloads, and large-scale data access activity.
- Train employees to independently verify unexpected requests received through phone calls, messaging platforms, or email.
- Restrict access to sensitive cloud resources through managed devices and enforce continuous monitoring of privileged accounts.

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
GigaWiper Destructive Backdoor Integrating Multiple Malware Families	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Microsoft Threat Intelligence has identified GigaWiper, a sophisticated Golang-based backdoor that combines multiple malware families into a single framework capable of espionage, remote control, and destructive operations. The malware provides attackers with command-and-control functionality and allows them to trigger different destructive actions on demand, including disk wiping, ransomware-like file encryption, and system-level sabotage.

Organizations in the financial sector should be aware that GigaWiper could affect enterprise environments by providing threat actors with prolonged access before destructive actions are executed. The combination of surveillance, remote administration, and multiple data destruction methods may increase the risk of operational disruption if attackers successfully establish a foothold within critical systems.

Technical Details

- Microsoft first observed GigaWiper during destructive incidents in October 2025 and identified it as a modular Golang-based backdoor rather than a standalone wiper. The malware combines command-and-control functions with several destructive capabilities.
- The malware was assembled from multiple malware families, allowing operators to select different destructive actions through on-demand commands instead of deploying separate tools.

- Once deployed, GigaWiper establishes persistent access and enables attackers to maintain control of compromised systems before initiating destructive activity.
- One destructive component operates directly at the physical disk level, overwriting raw disk content and removing partition information to render systems inoperable.
- A second destructive capability mimics ransomware by encrypting files with randomly generated keys that are never saved. As a result, affected files cannot be recovered even though the activity resembles a ransomware attack.
- Another wiping component targets the Windows drive and performs multiple overwrite passes, increasing the difficulty of recovering affected systems and data.
- Beyond destruction, the backdoor supports reconnaissance and monitoring activities, including collecting system information and managing processes, services, and registry settings.
- The malware can capture screenshots, record screen activity, and provide remote access capabilities, allowing operators to observe and interact with compromised systems.
- Researchers observed command-and-control functionality that enables attackers to issue instructions, execute actions remotely, and coordinate activity across compromised environments.
- The framework demonstrates a shift from traditional single-purpose wipers by combining long-term access, surveillance, and multiple destructive options within one unified platform.

Recommendations

- Monitor for unusual administrative activity, remote-control behavior, and unexpected command execution on critical systems.
- Restrict and regularly review privileged access to reduce opportunities for attackers to establish persistent footholds.
- Maintain secure, offline backups and periodically test recovery procedures to support restoration following destructive incidents.
- Investigate unauthorized system discovery, screen-capture activity, or changes to critical services and registry settings.
- Implement continuous monitoring to detect post-compromise activity before destructive commands can be executed.

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
China Nexus Actor UAT-7810 Builds ORB Infrastructure with New Backdoor Toolset	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Cisco Talos has identified continued activity by UAT-7810, a China-nexus threat actor responsible for maintaining and expanding the LapDogs Operational Relay Box (ORB) network. The group compromises internet-facing networking devices by exploiting known vulnerabilities in unpatched routers and deploys an evolving malware toolkit, including the new LONGLEASH backdoor, to create relay infrastructure that can be leveraged for follow-on malicious operations.

Organizations in the financial sector should be aware that ORB infrastructure can obscure the origin of malicious activity and complicate attribution and detection efforts. The evolving malware capabilities observed in this campaign could affect organizations that rely on internet-facing networking devices, particularly where unpatched systems provide opportunities for attackers to establish persistent relay nodes.

Technical Details

- UAT-7810 continues to maintain and expand the LapDogs ORB network, which consists of compromised networking devices that act as relay infrastructure for subsequent threat activity. The actor is assessed to focus on building and sustaining this infrastructure rather than directly conducting end-target operations.
- The campaign primarily targets internet-facing networking devices, including wireless routers and embedded systems. Attackers gain access by exploiting known vulnerabilities in systems that have not been patched.
- Researchers observed exploitation of multiple vulnerabilities in Ruckus wireless routers, a technique that has remained part of the group's operations since 2025. Additional targeting of ASUS routers suggests efforts to broaden the available pool of compromised devices.
- After gaining access, the operators deploy custom malware to establish control of the device and integrate it into the broader relay network. The malware is tailored for multiple hardware architectures, including MIPS, ARM, and x64 platforms.
- The group has developed LONGLEASH, a new version of its previously known SHORTLEASH backdoor. The updated malware expands the functionality available to operators and demonstrates ongoing development efforts.
- LONGLEASH supports command-and-control communications, network tunneling, web server hosting, and the ability to function as both a client and a server within the relay infrastructure.
- Researchers also identified DOGLEASH, a Linux backdoor that enables command execution, file operations, operating system information retrieval, and execution of code directly in memory on compromised devices.
- Another tool, JARLEASH, provides administrative capabilities for compromised systems and supports activities such as file management and remote service operations.

- The threat actor additionally uses LEASHTEST, a utility designed to test functionality on embedded devices, indicating continued refinement and validation of the malware toolkit.
- Multiple new servers were observed hosting malware payloads and supporting campaign operations, demonstrating continued investment in expanding and maintaining the ORB infrastructure.

Recommendations

- Prioritize patching internet-facing networking devices, particularly routers and embedded systems, to address known vulnerabilities.
- Conduct regular inventories of network infrastructure and remove or replace unsupported devices that no longer receive security updates.
- Monitor networking devices for unexpected administrative activity, unauthorized services, or unusual outbound communications.
- Restrict management access to networking equipment and enforce strong authentication controls for administrative interfaces.
- Review network telemetry for indications of tunneling, relay behavior, or device communications that deviate from normal operational patterns.

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Pre-Authentication Vulnerabilities in BeyondTrust Remote Support and Privileged Remote Access	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

BeyondTrust has disclosed four vulnerabilities affecting Remote Support (RS) and Privileged Remote Access (PRA), including two critical authentication bypass flaws that could allow unauthenticated attackers to gain unauthorized access to affected appliances. The vulnerabilities stem from improper authentication validation and can be exploited under specific authentication configurations, potentially enabling attackers to bypass normal access controls without valid credentials.

Organizations in the financial sector should be aware that successful exploitation may impact remote administration and privileged access management environments that support critical operations. The vulnerabilities could affect organizations using self-hosted deployments, particularly where exposed management systems provide opportunities for unauthorized access or service disruption if security updates are not applied promptly.

Technical Details

- BeyondTrust disclosed four vulnerabilities affecting Remote Support and Privileged Remote Access appliances, including two Critical and two High severity issues. The vulnerabilities impact versions 25.3.2 and earlier.
- CVE-2026-40138 is a Critical authentication bypass vulnerability with a CVSS v4 score of 9.2. The issue stems from improper authentication validation and may allow an unauthenticated remote attacker to gain unauthorized access under specific authentication configurations.
- CVE-2026-40139 is a second Critical authentication bypass vulnerability with a CVSS v4 score of 9.2. The flaw could enable attackers to bypass access controls without valid credentials when certain deployment conditions are present.
- Both Critical vulnerabilities occur before authentication is completed, allowing attackers to target affected appliances without first obtaining legitimate user credentials.
- CVE-2026-40140 is a High severity denial-of-service vulnerability with a CVSS v4 score of 8.7. The issue results from insufficient client input validation.
- An unauthenticated attacker can exploit CVE-2026-40140 to trigger excessive resource consumption on the appliance, potentially causing service degradation or denial-of-service conditions.
- CVE-2026-40141 is a High severity vulnerability with a CVSS v4 score of 8.5 related to improper handling of query logic and authorization controls.
- The vulnerability may allow an authenticated user with specific permissions to access application resources that were not intended to be available to them.
- The issues affect both BeyondTrust Remote Support and Privileged Remote Access deployments running version 25.3.2 and earlier.

Recommendations

- Immediately upgrade BeyondTrust Remote Support and Privileged Remote Access deployments to version 25.3.3 or later.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft Defender 'RoguePlanet' Privilege Escalation Vulnerability	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Microsoft has released an out-of-band security update for CVE-2026-50656, also known as RoguePlanet, a high-severity elevation of privilege vulnerability affecting the Microsoft Malware Protection Engine (mpengine.dll) used by Microsoft Defender Antivirus. The flaw stems from a race condition within the engine

and allows a local attacker with standard user privileges to elevate access to NT AUTHORITY\SYSTEM, potentially giving them complete control over the affected Windows system.

Organizations in the financial sector should be aware that successful exploitation could affect endpoint security by enabling attackers who already have local access to gain highly privileged permissions. The risk may be increased by the public availability of proof-of-concept exploit code, making timely verification of Defender engine updates important even though no active exploitation has been publicly confirmed.

Technical Details

- CVE-2026-50656, known as RoguePlanet, is a local privilege escalation vulnerability affecting the Microsoft Malware Protection Engine used by Microsoft Defender Antivirus.
- The vulnerability is rated High severity with a CVSS score of 7.8 and allows a user with standard privileges to elevate access to NT AUTHORITY\SYSTEM.
- The issue is caused by a race condition within the Microsoft Malware Protection Engine, creating an opportunity for privileged operations to be manipulated during execution.
- The weakness is classified as CWE-362, Concurrent Execution using Shared Resource with Improper Synchronization, commonly referred to as a race condition.
- Successful exploitation requires local access to the affected system and does not provide initial access on its own.
- An attacker who gains access to a low-privileged account could use the vulnerability to obtain SYSTEM-level privileges and execute actions with the highest level of authority on the device.
- SYSTEM-level access may allow attackers to modify security settings, interact with protected system resources, and establish deeper control over compromised endpoints.
- Public proof-of-concept exploit code was released in June 2026 by security researcher Nightmare-Eclipse, increasing the likelihood of testing and exploitation attempts.
- At the time of disclosure, no confirmed in-the-wild exploitation activity was reported.
- Microsoft addressed the vulnerability in Microsoft Malware Protection Engine version 1.1.26060.3008, which is distributed through Microsoft Defender update mechanisms.

Recommendations

- Verify that all Windows endpoints are running Microsoft Malware Protection Engine version 1.1.26060.3008 or later.
- Confirm successful deployment of Defender engine updates through Microsoft Defender, Microsoft Defender for Endpoint, or centralized endpoint management tools.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Authentication Bypass Vulnerability OAuth Single Sign-On (SSO) WordPress Plugin	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

miniOrange has disclosed CVE-2026-57807, a critical authentication bypass vulnerability affecting the OAuth Single Sign-On (SSO) WordPress plugin. The flaw originates from an insecure password recovery implementation that fails to properly enforce authentication controls, allowing an unauthenticated remote attacker to bypass login protections and authenticate as any registered WordPress user, including administrators.

Organizations in the financial sector should be aware that successful exploitation could affect internet-facing websites and portals relying on the vulnerable plugin for authentication services. The vulnerability may enable unauthorized administrative access, potentially leading to malicious configuration changes, content manipulation, or further compromise of affected WordPress environments.

Technical Details

- CVE-2026-57807 is a critical authentication bypass vulnerability affecting the miniOrange OAuth Single Sign-On (SSO) WordPress plugin. The issue carries a CVSS v3.1 score of 9.8.
- The vulnerability is classified as CWE-288, Authentication Bypass Using an Alternate Path or Channel, indicating that attackers can circumvent normal authentication mechanisms.
- The flaw stems from an insecure implementation of the plugin's password recovery functionality. Authentication controls are not properly enforced during the recovery process.
- An unauthenticated remote attacker can exploit the vulnerability over the network without requiring valid credentials or prior access to the target environment.
- The attack requires no user interaction, reducing the barriers to exploitation and increasing exposure for publicly accessible WordPress deployments.
- Successful exploitation allows attackers to authenticate as any registered WordPress user within the affected site.
- Attackers can target privileged accounts, including administrator users, resulting in complete administrative access to the affected WordPress instance.
- With administrative access, attackers may gain the ability to modify site configurations, manage users, alter website content, and perform actions normally restricted to trusted administrators.
- The vulnerability affects all plugin versions up to and including version 38.5.8, leaving a broad range of deployments exposed.
- At the time of disclosure, no official vendor patch was available, although virtual patching through web application firewall protections has been identified as a temporary mitigation measure.

Recommendations

- Immediately disable or remove the vulnerable miniOrange OAuth Single Sign-On (SSO) plugin from affected WordPress environments where operationally feasible.
- Implement web application firewall protections, including available virtual patching measures, to reduce exposure until an official fix is released.

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

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Typosquatting Campaign Targets Payment SDK Users Across npm and PyPI

Tactic	Technique	Observed Activity
Initial Access	T1195 – Supply Chain Compromise	Malicious packages were published to npm and PyPI repositories and disguised as trusted payment SDKs.
Defense Evasion	T1036 – Masquerading	Counterfeit packages mimicked legitimate payment-service SDK functionality and interfaces.
Defense Evasion	T1027 – Obfuscated Files or Information	Command-and-control infrastructure was concealed through encoded and transformed strings.
Discovery	T1082 – System Information Discovery	Malware collected host-related information including system attributes and execution context.
Discovery	T1083 – File and Directory Discovery	The malware gathered information about the current working directory as part of victim profiling.
Discovery	T1497 – Virtualization/Sandbox Evasion	The malware checked CPU availability and system naming indicators associated with analysis environments.
Credential Access	T1552 – Unsecured Credentials	Environment variables containing credentials, secrets, tokens, passwords, authentication data, and API-related values were collected.
Collection	T1005 – Data from Local System	Sensitive environment data and system information were gathered prior to exfiltration.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Collected data was transmitted to attacker-controlled infrastructure

Forg365 PhaaS Targeting Microsoft 365 Through Device Code and AiTM Phishing

Tactic	Technique	Observed Activity
Initial Access	Phishing (T1566)	Delivery of phishing emails impersonating business documents to lure victims into attacker-controlled workflows.
Credential Access	Adversary-in-the-Middle (T1557)	AiTM phishing workflow used to intercept authentication sessions and capture access material.
Credential Access	Steal or Forge Authentication Credentials (T1649)	Collection and management of authentication tokens and session material through platform capabilities.

Defense Evasion	Traffic Signaling / Conditional Access Evasion (Mapped Closely to Traffic Filtering Behaviors)	Traffic classification and redirection of selected visitors to benign content to hinder analysis and detection.
Persistence	Web Session Cookie (T1539)	Browser extension used to refresh Microsoft single sign-on cookies and maintain access.
Collection	Email Collection (T1114)	Mailbox-access workflows, keyword monitoring, and account intelligence functions against compromised accounts.
Discovery	Account Discovery (T1087)	Account intelligence features used to enumerate and monitor compromised user accounts.
Credential Access	Device Code Authentication Abuse (ATT&CK-related identity abuse activity)	Use of device-code phishing workflows to obtain access to attacker-controlled session

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
AiTM	Adversary-in-the-Middle. A phishing technique where an attacker positions infrastructure between the user and a legitimate service to capture authentication sessions or tokens.
AMSI	Antimalware Scan Interface. A Windows security feature that allows security products to inspect scripts and other content for malicious activity.
API	Application Programming Interface. A mechanism that allows software applications to communicate and exchange information with each other.
APT	Advanced Persistent Threat. A sophisticated threat actor that maintains long-term access to targeted environments.
Authentication Bypass	A security flaw that allows attackers to gain access to a system without successfully completing normal authentication requirements.
Backup Server	A system responsible for managing and storing backup operations and recovery data.
BinaryFormatter	A .NET serialization mechanism used to convert objects into a transferable format. Insecure implementations can introduce security risks.
BlackFile	A data extortion group referenced in relation to activity and infrastructure overlaps observed during Helix investigations.
BlueRabbit	An alternative tracking name used by other researchers for the malware framework identified as GigaWiper.
Browser Cookie	Data stored by web browsers that helps maintain authenticated sessions and user preferences.
C2 / Command-and-Control	Infrastructure used by attackers to communicate with and manage compromised systems.
ClickFix	A social engineering technique that persuades users to execute commands or actions themselves rather than exploiting a software vulnerability.
Cloud Collaboration Platform	Cloud-hosted services used for document sharing, communication, and collaborative work.
Cloud Identity	Digital identities and authentication mechanisms used to access cloud-hosted applications and services.
Conditional Access	Security policies that control access to applications and data based on defined conditions such as user identity, device state, or location.
Credential Theft	The unauthorized collection of usernames, passwords, tokens, or other authentication information.
Cryptomining	The process of using computing resources to generate cryptocurrency. Attackers often abuse compromised systems for unauthorized mining.
CSC	UAE Cyber Security Council
CVE	Common Vulnerabilities and Exposures. A standardized identifier assigned to publicly disclosed security vulnerabilities.
CVSS	Common Vulnerability Scoring System. A framework used to measure the severity of security vulnerabilities.
CWE	Common Weakness Enumeration. A classification system for common software security weaknesses.

Deserialization	The process of reconstructing data objects from stored or transmitted formats. Improper handling can enable code execution.
Device Code Phishing	A phishing technique that tricks users into approving attacker-controlled authentication sessions using legitimate device authentication workflows.
DOGLEASH	A Linux backdoor identified in the UAT-7810 campaign that allows command execution and remote control of compromised devices.
Dormant Account	An account that remains inactive for a prolonged period before being used for operational activity.
DoS	Denial of Service. An attack that consumes resources or disrupts service availability for legitimate users.
Endpoint	A user device such as a workstation, laptop, or server connected to a network.
Exfiltration	The unauthorized transfer or theft of data from a system or environment.
Exploit	Code or a technique used to take advantage of a vulnerability.
Extortion	A threat tactic where attackers seek payment or leverage by threatening to release, disclose, or misuse stolen information.
Factory-v3	A malware delivery framework observed in the Vidar Stealer campaign and used to deploy malicious payloads.
FlockWiper	A destructive malware family whose functionality was incorporated into the GigaWiper framework.
Forg365	A phishing-as-a-service platform targeting Microsoft 365 accounts through device code phishing and session theft techniques.
ForgCookie	A browser extension associated with Forg365 that helps maintain access by refreshing authentication sessions.
Ghost Account	A dormant account left inactive for long periods before being used for malicious activity.
GigaWiper	A modular destructive malware framework combining backdoor functionality, espionage capabilities, and multiple data destruction methods.
GitHub Enumeration	The process of collecting information about repositories, users, projects, and organizations hosted on GitHub.
GitHub GraphQL	A query interface used to retrieve structured information from GitHub services.
Golang / Go	A programming language used to develop software, including legitimate applications and malware.
Information Stealer	Malware designed primarily to collect credentials, session information, financial data, and other sensitive information.
JARLEASH	A Java-based administration backdoor used by UAT-7810 to manage compromised systems and infrastructure.
Kali365	A Microsoft 365-focused phishing ecosystem referenced due to similarities with Forg365 phishing operations.
LapDogs	An Operational Relay Box (ORB) infrastructure consisting of compromised networking devices used as relay nodes.
Lateral Movement	Techniques used by attackers to move from one system to another after initial access has been established.
LDAP	Lightweight Directory Access Protocol. A protocol used to access and query directory services such as Active Directory.
LEASHTEST	A utility observed in the UAT-7810 campaign that is used to test malware functionality on embedded devices.

Local Privilege Escalation (LPE)	A technique that enables a user or process to obtain higher privileges on a system.
LONGLEASH	An enhanced version of the SHORTLEASH backdoor that expands relay, proxying, and command-and-control capabilities.
Malware-as-a-Service (MaaS)	A business model in which malware capabilities are provided to affiliates or customers.
MFA	Multi-Factor Authentication. A security control requiring more than one form of identity verification.
Microsoft 365 Device Authentication	A legitimate authentication workflow that allows devices to connect to Microsoft services using authorization codes.
NT AUTHORITY\SYSTEM	A highly privileged Windows account with extensive control over the operating system.
OAuth	Open Authorization. A framework used to grant applications limited access to user accounts without sharing passwords.
ORB	Operational Relay Box. A network of compromised devices used to relay attacker traffic and obscure its origin.
Password Recovery Mechanism	A feature that allows users to regain account access when credentials are lost or forgotten.
Password-Protected Archive	A compressed file secured with a password. Attackers frequently use these archives to evade automated security scanning.
PAT	Personal Access Token. A token used to authenticate access to services such as GitHub without a password.
Persistence	Techniques that allow attackers to maintain access to a compromised system over time.
Phishing-as-a-Service (PhaaS)	A service model that provides phishing tools and infrastructure to subscribers or affiliates.
PoC	Proof of Concept. Demonstration code or techniques showing how a vulnerability can be exploited.
Post-Exploitation	Activities performed after initial compromise, such as reconnaissance, credential access, persistence, or data theft.
PRA	Privileged Remote Access. A solution used to manage and secure remote privileged sessions.
Privilege Escalation	The act of obtaining higher permissions than originally assigned to a user or process.
Privileged Access Management (PAM)	Security controls and technologies used to manage highly privileged accounts and administrative access.
Proof-of-Concept (PoC) Exploit	Demonstration code showing how a vulnerability can be successfully exploited. Public availability often increases risk.
Proxying	Routing network traffic through another system to hide origin or facilitate communications.
Python Requests	A commonly used Python library for making web requests. It may appear in automated tools and scripts.
Query Injection	Manipulation of application queries to access unauthorized data or resources.
RabbitMQ	A messaging platform used for communication between software components and observed in GigaWiper command infrastructure.
Race Condition	A software flaw that occurs when multiple operations interact with shared resources in an unintended order.
RCE	Remote Code Execution. The ability for an attacker to execute commands or code on a remote system.

Redis	An in-memory data storage platform often used for caching, messaging, and application communication.
Relay Infrastructure	Intermediary systems used by attackers to route malicious traffic and obscure the true origin of operations.
Remote Access Tooling	Software or capabilities that allow remote administration, management, or control of systems.
Remote Monitoring and Management (RMM)	Software used to remotely manage and administer systems across an organization.
Residential Proxy	Internet traffic routed through residential internet connections, making activity appear more legitimate.
RoguePlanet	The publicly known name assigned to CVE-2026-50656 affecting the Microsoft Malware Protection Engine.
RS	Remote Support. A solution used to provide remote assistance and support to systems and users.
Session Cookie	Information stored in a browser that maintains an authenticated user session.
SharePoint	A Microsoft platform commonly used for document management, collaboration, and content sharing.
SharePoint Enumeration	The process of identifying and cataloging available SharePoint sites, libraries, and documents prior to data access or collection.
ShinyHunters	A well-known data theft and extortion threat group mentioned in connection with infrastructure and operational similarities observed in Helix activity.
SHORTLEASH	The earlier version of the backdoor used by UAT-7810 before the development of LONGLEASH.
SMB	Server Message Block. A protocol used for file and resource sharing across a network.
Social Engineering	Techniques that manipulate individuals into revealing information or performing actions that benefit attackers.
SOCKS Proxy	A network protocol that forwards traffic between systems and can be used to route communications.
SQL	Structured Query Language. A language used to manage and query databases.
SSO	Single Sign-On. An authentication method allowing users to access multiple services through one login process.
Supply Chain Attack	An attack that targets software, development tools, or third-party dependencies to gain access to downstream users or organizations.
Telegram-Distributed	Refers to threat services or tooling marketed, supported, or distributed through the Telegram messaging platform.
Threat Actor	An individual, group, or organization responsible for conducting malicious cyber activity.
Token	A digital authentication artifact that grants access to systems or services after successful authentication.
Token Vault	A repository used by attackers to store stolen authentication tokens for later access.
Tunnel / Tunneling	A method of transporting network traffic through intermediary systems to bypass controls or conceal activity.
Typosquatting	A technique where attackers register or publish resources with names similar to legitimate ones to trick users into using them.

UAT-5918	A separate China-aligned threat actor reported as leveraging infrastructure associated with UAT-7810.
UAT-7810	A threat actor tracked by researchers as responsible for maintaining and expanding ORB infrastructure using custom malware.
Unauthorized Access	Access gained to systems, applications, or data without proper authorization or approval.
User Agent	An identifier sent by software when interacting with web services that helps identify the client application.
Veeam Backup & Replication	Enterprise software used for backup, recovery, and data protection operations.
Vidar Stealer	Information-stealing malware designed to collect credentials, browser data, and other sensitive information.
Virtual Patching	Protection provided by security controls such as a web application firewall when a software patch is unavailable.
Vishing	Voice Phishing. Social engineering conducted through phone calls to trick users into revealing information or performing actions.
WAF	Web Application Firewall. A security solution that filters and monitors HTTP/HTTPS traffic to web applications.
Wiper Malware	Malware designed to destroy, overwrite, or render data and systems unusable.
XMR	A cryptocurrency associated with Monero and commonly targeted in illicit mining operations.
XMRig	Cryptocurrency mining software that can be abused by attackers to mine cryptocurrency on compromised systems
Zero-Day	A vulnerability exploited before a vendor patch or official fix is available. Although not central to these articles, executives frequently encounter the term in risk discussions.