Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

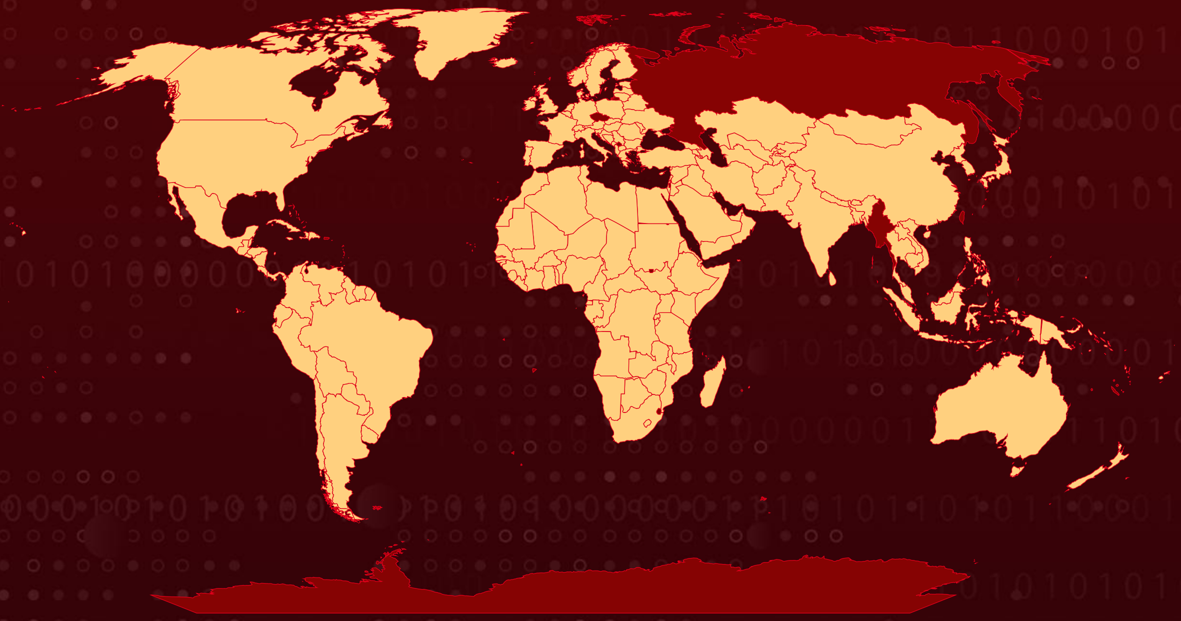
Attackers Hijack Open VSX Extensions to Spread GlassWorm Malware

Date of Publication	Admiralty Code	TA Number
February 03, 2026	A1	TA2026032

Summary

First Seen: January 30, 2026
Targeted Regions: Worldwide (excluding Russia)
Targeted Platforms: macOS
Malware: GlassWorm
Attack: A sophisticated supply-chain attack struck the Open VSX Registry after threat actors compromised the legitimate developer account “oorzc” and used it to distribute malicious updates embedding the GlassWorm malware loader across four trusted VS Code extensions with more than 22,000 combined downloads. Once installed, the malware targets macOS systems, stealing credentials, cryptocurrency wallet information, and sensitive developer data.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

🟨 Targeted 🟥 Non-Targeted

Attack Details

#1

A trusted software supply channel was quietly turned into a malware delivery mechanism on January 30, 2026, after attackers compromised the publishing credentials of a legitimate Open VSX developer known as “oorzc.” Leveraging this access, they released poisoned updates for four popular extensions—FTP/SFTP/SSH Sync Tool, I18n Tools, vscode mindmap, and scss to css. Since these extensions had been widely used for more than two years and accumulated over 22,000 downloads, the malicious updates spread through an already trusted ecosystem, bypassing common detection triggers such as typosquatting or fake developer accounts.

#2

The malicious updates embedded nearly identical loaders inside extension code, where an AES-256-CBC encrypted payload was decrypted at runtime and executed through eval(). The loader also profiled system environments and deliberately avoided running on systems configured with Russian-language locales, a tactic often associated with campaigns tied to Russian-speaking threat actors. To further evade detection, the attackers employed EtherHiding techniques, using Solana blockchain transaction memos to dynamically resolve command-and-control infrastructure without needing to update the compromised extensions again.

#3

Once executed, the GlassWorm malware established persistence on macOS systems using a LaunchAgent mechanism, ensuring automatic execution at login. It then began collecting sensitive information, including browser credentials, cookies, browsing history, cryptocurrency wallet data from both browser extensions and desktop wallet applications, iCloud Keychain contents, Apple Notes databases, Safari cookies, and files stored in common user directories. VPN configuration data was also targeted, expanding the scope of potential access.

#4

The harvested data was transmitted to attacker-controlled infrastructure while communications relied on a resilient, multi-layered command-and-control structure combining direct IP connections, blockchain-based dead drops, and backup communication channels through Google Calendar events. Of particular concern is the theft of developer and cloud credentials, such as npm tokens, GitHub authentication artifacts, and SSH or AWS keys, which could enable attackers to infiltrate enterprise environments, move laterally across networks, and potentially compromise additional software packages in a cascading supply-chain attack.

Recommendations

Audit Installed Extensions: Immediately scan all development environments to identify and remove any installed extensions from the compromised author "oorzc" and verify extension integrity across all developer workstations.

Investigate Network Logs: Review network logs for indicators of the GlassWorm loader including connections, and verify that no unauthorized data exfiltration has occurred from development systems.

Rotate Credentials: Any systems that had the compromised extensions installed should undergo full credential rotation including npm tokens, GitHub credentials, SSH keys, AWS credentials, and any stored authentication material.

Enable MFA for Developer Accounts: Enforce multi-factor authentication for all developer accounts on Open VSX, VS Code Marketplace, npm, GitHub, and other publishing platforms to prevent credential-based account takeovers.

Restrict Marketplace Access: Evaluate and restrict access to extension marketplaces where possible, implementing allow-lists for approved extensions and limiting auto-update functionality on developer machines.

Review LaunchAgent Persistence: On macOS systems, regularly audit LaunchAgent configurations for unauthorized persistence mechanisms that may indicate GlassWorm or similar malware infections.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Persistence	T1543: Create or Modify System Process	T1543.001: Launch Agent
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1140: Deobfuscate/Decode Files or Information	
Credential Access	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1552: Unsecured Credentials	
	T1539: Steal Web Session Cookie	
Collection	T1005: Data from Local System	
	T1560: Archive Collected Data	
Command and Control	T1102: Web Service	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Discovery	T1083: File and Directory Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
Open VSX Extensions	oorzc.ssh-tools, oorzc.i18n-tools-plus, oorzc.mind-map, oorzc.scss-to-css-compile, Angular-studio.ng-angular-extension, awesome-codebase.codebase-dart-pro, cudra-production.vsce-prettier-pro, dev-studio-sense.php-comp-tools-vscode, ko-zu-gun-studio.synchronization-settings-vscode, littensy-studio.magical-icons, pretty-studio-advisor.prettyxml-formatter, sol-studio.solidity-extension, studio-jjalaire-team.professional-quarto-extension, studio-velte-distributor.pro-svelte-extension, sun-shine-studio.shiny-extension-for-vscode, tucyzirille-studio.angular-pro-tools-extension, vce-brendan-studio-eich.js-debuger-vscode
Solana address	BjVeAjPrSKFiingBn4vZvghsGj9KCE8AJVtbc9S8o8SC
AES key	wDO6YyTm6DL0T0zJ0SXhUql5Mo0pdlSz
AES IVs (hex)	c4b9a3773e9dced6015a670855fd32b
IPv4	45[.]32[.]150[.]251

References

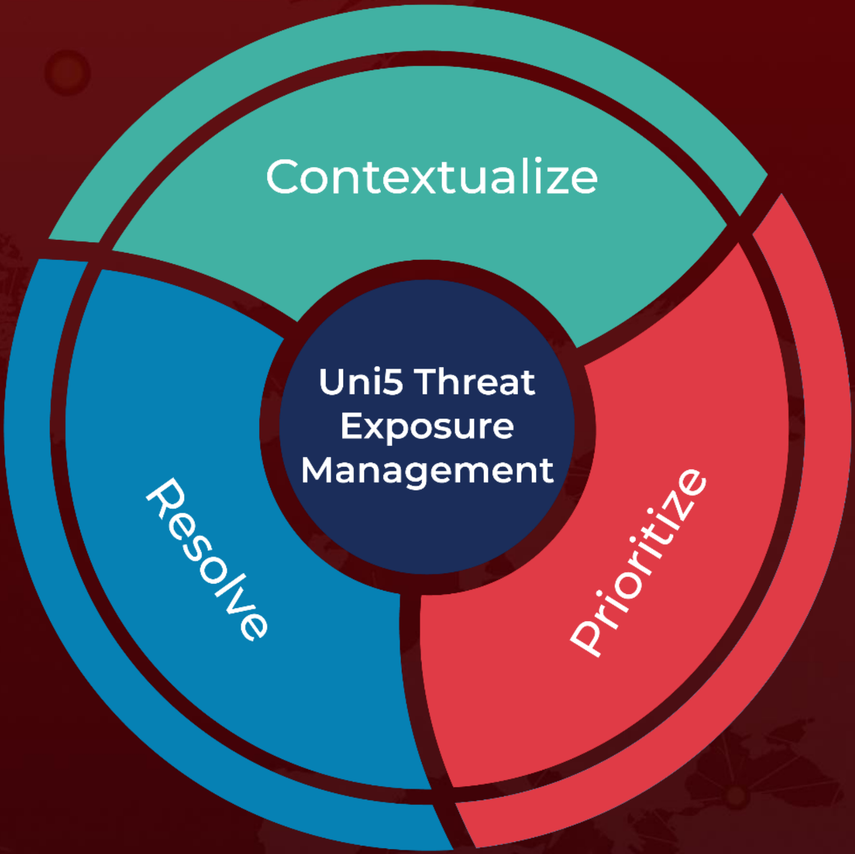
https://socket.dev/blog/glassworm-loader-hits-open-vsx-via-suspected-developer-account-compromise

https://hivepro.com/threat-advisory/glassworm-quiet-infiltration-of-mac-systems/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 03, 2026 • 6:50 AM

More at www.hivepro.com