Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

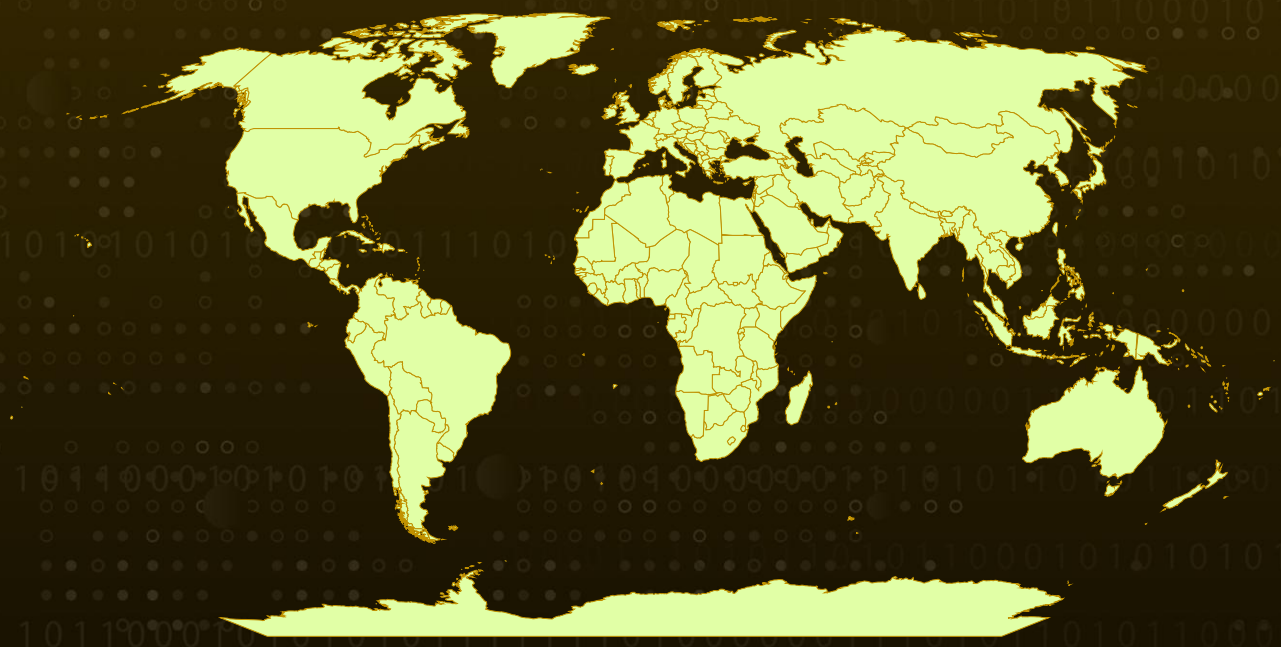
Evelyn Stealer's Stealth Campaign Against Developers

Date of Publication	Admiralty Code	TA Number
January 21, 2026	A1	TA2026020

Summary

First Seen: December 8, 2025
Targeted Region: Worldwide
Targeted Industries: Software Development, Technology
Affected Platform: Windows
Malware: Evelyn Stealer
Attack: This campaign represents a highly sophisticated, multi-stage information-stealing operation that abuses the trusted Visual Studio Code extension ecosystem to target software developers. By disguising malicious components as legitimate VS Code extensions, the attackers quietly deliver the Evelyn Stealer and initiate a layered infection chain that combines DLL sideloading, stealthy PowerShell execution, and process hollowing. Once embedded, the malware systematically harvests sensitive data, including browser credentials, cryptocurrency wallet information, Wi-Fi passwords, clipboard contents, and detailed system metadata, before packaging and exfiltrating the stolen information to attacker-controlled FTP infrastructure.

Attack Regions



Attack Details

#1 On December 8, 2025, new findings emerged detailing a targeted malware campaign aimed at software developers through the abuse of weaponized Visual Studio Code extensions. The activity centers on the Evelyn information stealer, which is delivered through a carefully orchestrated multi-stage infection chain designed to blend into trusted development environments. By abusing tools developers use daily, the campaign capitalizes on implicit trust while quietly establishing persistence. From the earliest stages, Evelyn employs layered anti-analysis techniques to evade sandboxes and security research environments, allowing it to operate with minimal risk of early detection.

#2 The infection begins with a malicious VS Code extension that masquerades as a legitimate Lightshot DLL, executed alongside the genuine Lightshot.exe to maintain credibility. Once loaded, the malicious DLL imitates expected Lightshot behavior to preserve the illusion of legitimacy while executing its hidden payload in parallel. To avoid duplicate execution, the malware enforces a singleton model using internal checks and a mutex mechanism. It then spawns a concealed PowerShell process to download a second-stage payload, saved as “runtime.exe” in the local temporary directory, ensuring a seamless transition to the next phase without alerting the user.

#3 The second-stage payload acts as a process hollowing injector responsible for deploying the final Evelyn Stealer component. This stage decrypts the third-stage payload using AES-256-CBC encryption with a predefined key and initialization vector before injecting it into the legitimate Windows process “grpconv.exe.” Once execution resumes, Evelyn dynamically resolves the Windows APIs required for process injection, file system interaction, registry access, clipboard monitoring, and network communication. These actions are deliberately obfuscated, reflecting a strong focus on evasion and resilience against both manual analysis and automated defenses.

#4 Before initiating large-scale data theft, the malware conducts extensive checks to confirm it is not operating in a virtualized or sandboxed environment. These checks include GPU profiling, hostname validation, disk size inspection, process enumeration, and registry key analysis. Only after the environment is deemed trustworthy does Evelyn create a dedicated directory structure within the user’s AppData folder to stage its operations. It then prepares for credential harvesting by terminating active browser processes and locating its decryption component, “abe_decrypt.dll,” either locally or by retrieving it from an FTP server if necessary.

#5 With its components in place, Evelyn proceeds to harvest browser credentials via DLL injection, capture desktop screenshots, and collect a wide range of sensitive data, including system information, clipboard contents, Wi-Fi credentials, and cryptocurrency wallet details. The stolen data is consolidated into a ZIP archive and exfiltrated to the attacker’s command-and-control infrastructure over FTP, using structured filenames for tracking and organization. Overall, the campaign illustrates a mature and deliberate approach to targeting developer ecosystems, transforming trusted development tools into delivery mechanisms.

Recommendations

- **Audit and Vet VS Code Extensions:** Review all installed Visual Studio Code extensions within your development environment and remove any unrecognized or untrusted extensions, particularly those published by unverified developers or with low download counts and no reviews.
- **Implement Extension Whitelisting:** Establish an approved list of VS Code extensions for your organization and configure policies to prevent installation of extensions outside the whitelist, reducing the risk of trojanized extension installation.
- **Deploy Endpoint Detection Rules:** Implement detection rules for the specific file hashes and behavioral indicators associated with this campaign, including monitoring for process injection, suspicious PowerShell execution from VS Code contexts, and FTP traffic to unknown destinations.
- **Monitor PowerShell Activity:** Enable comprehensive PowerShell logging, including script block logging and module logging, to detect hidden PowerShell commands used by the malware downloader component.
- **Restrict Browser Launch Parameters:** Monitor and alert on browser processes launched with suspicious command-line arguments such as headless mode, disabled sandbox, or off-screen window positioning that indicate potential credential theft activity.
- **Implement Zero-Trust for Development Environments:** Apply zero-trust architecture principles specifically to developer workstations and development workflows, treating these as high-value assets with access to production systems and intellectual property.
- **Isolate Cryptocurrency Operations:** Separate cryptocurrency wallet access and operations from development systems to prevent credential theft from compromising digital assets.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration

TA0011 Command and Control	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1574** Hijack Execution Flow
T1574.001 DLL	**T1055** Process Injection	**T1055.012** Process Hollowing	**T1497** Virtualization/Sandbox Evasion
T1497.001 System Checks	**T1140** Deobfuscate/Decode Files or Information	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1113 Screen Capture	**T1115** Clipboard Data	**T1005** Data from Local System	**T1041** Exfiltration Over C2 Channel
T1071 Application Layer Protocol	**T1071.002** File Transfer Protocols	**T1057** Process Discovery	**T1566** Phishing

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	369479bd9a248c9448705c222d81ff1a0143343a138fc38fc0ea00f54fcc1598, 92af258d13494f208ccf76f53a36f288060543f02ed438531e0675b85da00430, aba7133f975a0788dd2728b4bbb1d7d948e50571a033a1e8f47a2691e98600c5, 74e43a0175179a0a04361faaaaf05eb1e6b84adca69e4f446ef82c0a5d1923d5
Files	Lightshot.dll, iknowyou.model, EvelynStealer.exe, abe_decrypt[1].dll, server09.mentality.cloud, syn1112223334445556667778889990.org

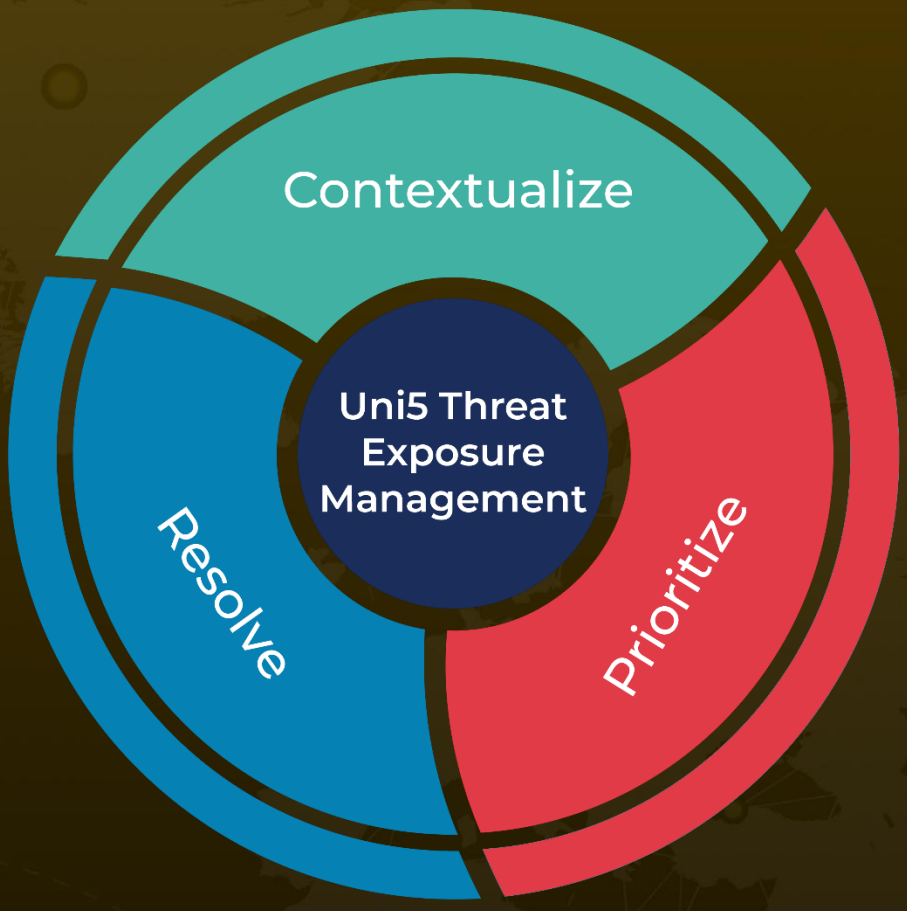
References

https://www.trendmicro.com/en_us/research/26/a/analysis-of-the-evelyn-stealer-campaign.html

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

January 21, 2026 • 6:30 AM

More at www.hivepro.com