GlassWorm – Self-Propagating VSCode Extension Worm

GlassWorm is the first self-propagating worm targeting VS Code extensions on OpenVSX marketplace. The attack uses invisible Unicode characters to hide malicious code from code editors and review processes, combined with blockchain-based command and control infrastructure on the Solana blockchain that cannot be taken down.

Seven OpenVSX extensions were compromised on October 17, 2025, with 35,800 total downloads, and ten extensions were still actively distributing malware two days later. The malware harvests NPM, GitHub, and Git credentials, targets 49 different cryptocurrency wallet extensions, deploys SOCKS proxy servers turning developer machines into criminal infrastructure, and installs hidden VNC servers for complete remote access. The stolen credentials are used to automatically compromise additional packages and extensions, creating exponential spread through the developer ecosystem. It uses Google Calendar as backup C2 server. This means Glassworm is using a triple layer C2 set up with the Solana blockchain, the use of a direct IP connection and Google Calendar, making it very robust.

On October 19, a new infected extension was detected in Microsoft's VSCode marketplace and it's stiill active. [1]

Affected Products

OpenVSX Extensions (with malicious versions):

codejoy.codejoy-vscode-extension@1.8.3

codejoy.codejoy-vscode-extension@1.8.4

l-igh-t.vscode-theme-seti-folder@1.2.3

kleinesfilmroellchen.serenity-dsl-syntaxhighlight@0.3.2

JScearey.rust-doc-viewer@4.2.1

SIRILMP.dark-theme-sm@3.11.4

CodeInKlingon.git-worktree-menu@1.0.9

CodeInKlingon.git-worktree-menu@1.0.91

ginfuru.better-nunjucks@0.3.2

ellacrity.recoil@0.7.4

grrrck.positron-plus-1-e@0.0.71

jeronimoekerdt.color-picker-universal@2.8.91

srcery-colors.srcery-colors@0.3.9

sissel.shopify-liquid@4.0.1

TretinV3.forts-api-extention@0.3.1

Microsoft VSCode Extensions:

cline-ai-main.cline-ai-agent@3.1.3

Exploitation

This is an active campaign.

Recommended Actions

- Make an audit of your installed extensions. Check for abnormal activity such as suspicious network connections, vulnerable dependencies and strange API usage.
- Scan new extensions before you install them.
- Only install extensions you need, and remove extensions that are no longer in use. Each installed extension extends your attack surface.
- Evaluate extensions before installing them, check for reviews, extension history, publisher reputation etc.
- Be careful when using auto-update, a compromised extension might install malware when auto-update is turned on.
- Keep an extension inventory.
- Consider a centralized allowlist for VSCode extensions.

Detection

Command & Control:

217.69.3.218 (primary C2 server)

140.82.52.31:80/wall (exfiltration endpoint)

Solana Wallet: 28PKnu7RzizxBzFPoLp69HLXp9bJL3JFtT2s5QzHsEA2

Transaction

49CDiVWZpuSW1b2HpzweMgePNg15dckgmqrrmpihYXJMYRsZvumVtFsDim1keESPCrKcW2CzYjN3nSQDGG14KKFM

Google Calendar C2:

https://calendar.app.google/M2ZCvM8ULL56PD1d6

Organizer: uhjdclolkdn@gmail.com

Payload URLs:

http://217.69.3.218/qQD%2FJoi3WCWSk8ggGHiTdg%3D%3D

http://217.69.3.218/get_arhive_npm/

http://217.69.3.218/get_zombi_payload/qQD%2FJoi3WCWSk8ggGHiTdg%3D%3D

Persistence Mechanisms:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\Run