GlassWorm Goes Native: Same Infrastructure, Hardened Delivery

By Lotan Sery,,

Archived: 2026-04-29 02:12:01 UTC

GlassWorm is back. Again. Since we first exposed this campaign in October, we've seen two waves, over 45,000 victims, and one attacker who won't quit.

After our last disclosure, things went quiet for a few weeks. Then, on November 22, a familiar Solana wallet woke up with a fresh transaction and a new C2 IP. And within days, malicious extensions started appearing again.

But this wave is different.

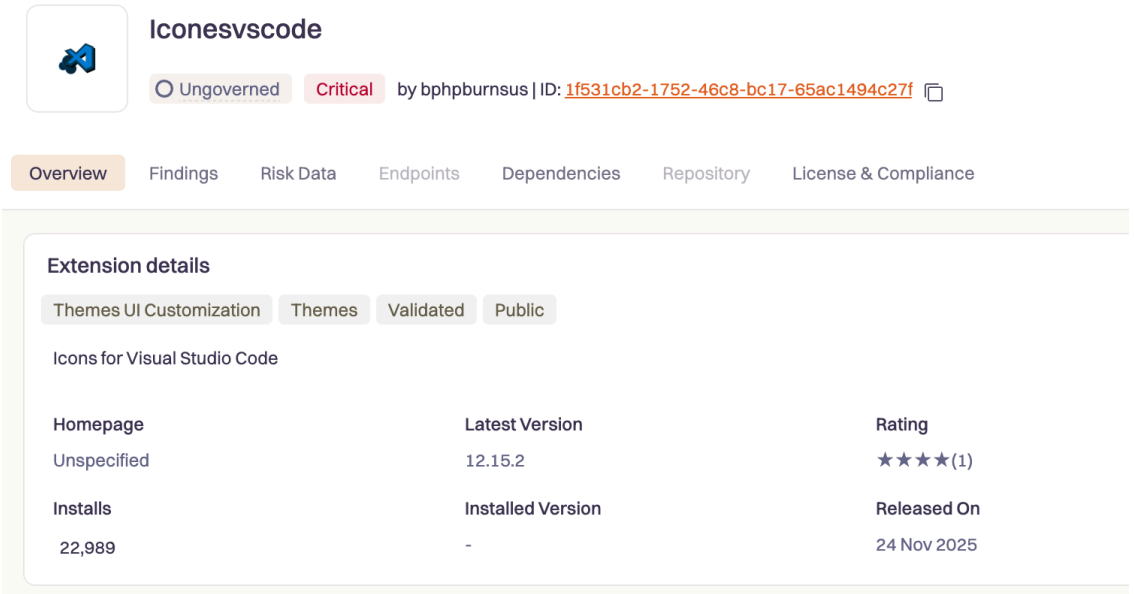
The invisible Unicode technique we exposed in our first report? Completely gone.

Instead, we found compiled Rust binaries. All the functionality we decoded from those invisible characters – Solana C2 lookups, AES decryption, payload staging – is now compiled into native code that you can't just decode anymore. You'd need to reverse engineer Rust binaries to see what's happening.

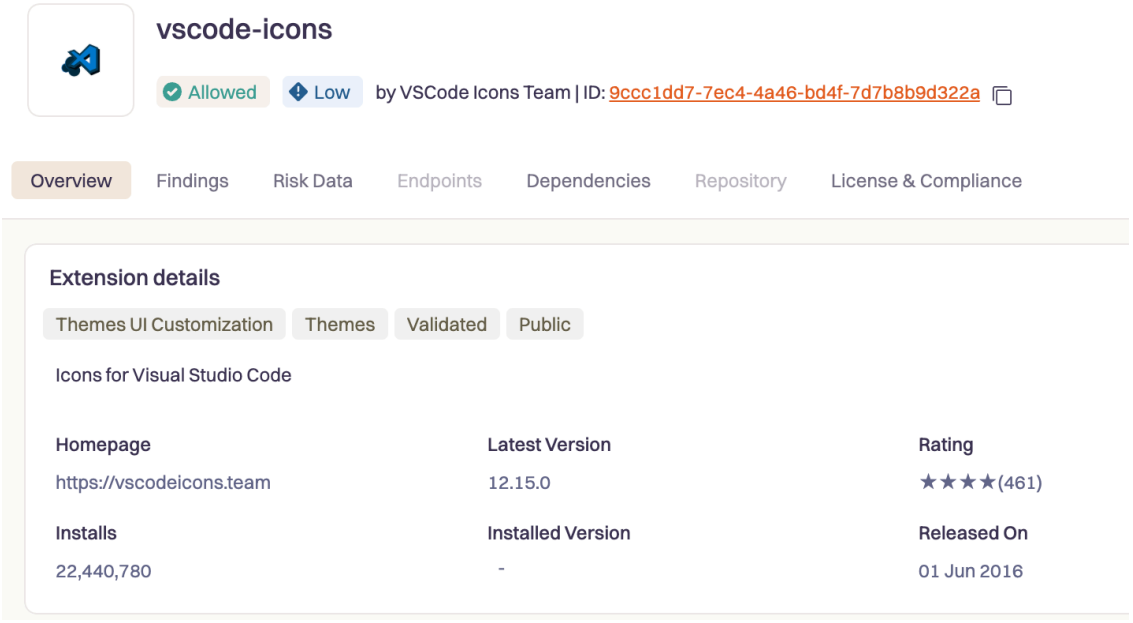
This time they also expanded beyond OpenVSX, targeting Microsoft's official VSCode marketplace too, publishing clean extensions first, then updating them with malware.

The wallet and attack chain remain the same, but the payload is now hidden inside native binaries.

Let's look at `Iconesvscode`, an extension that impersonates the popular `vscode-icons theme`:



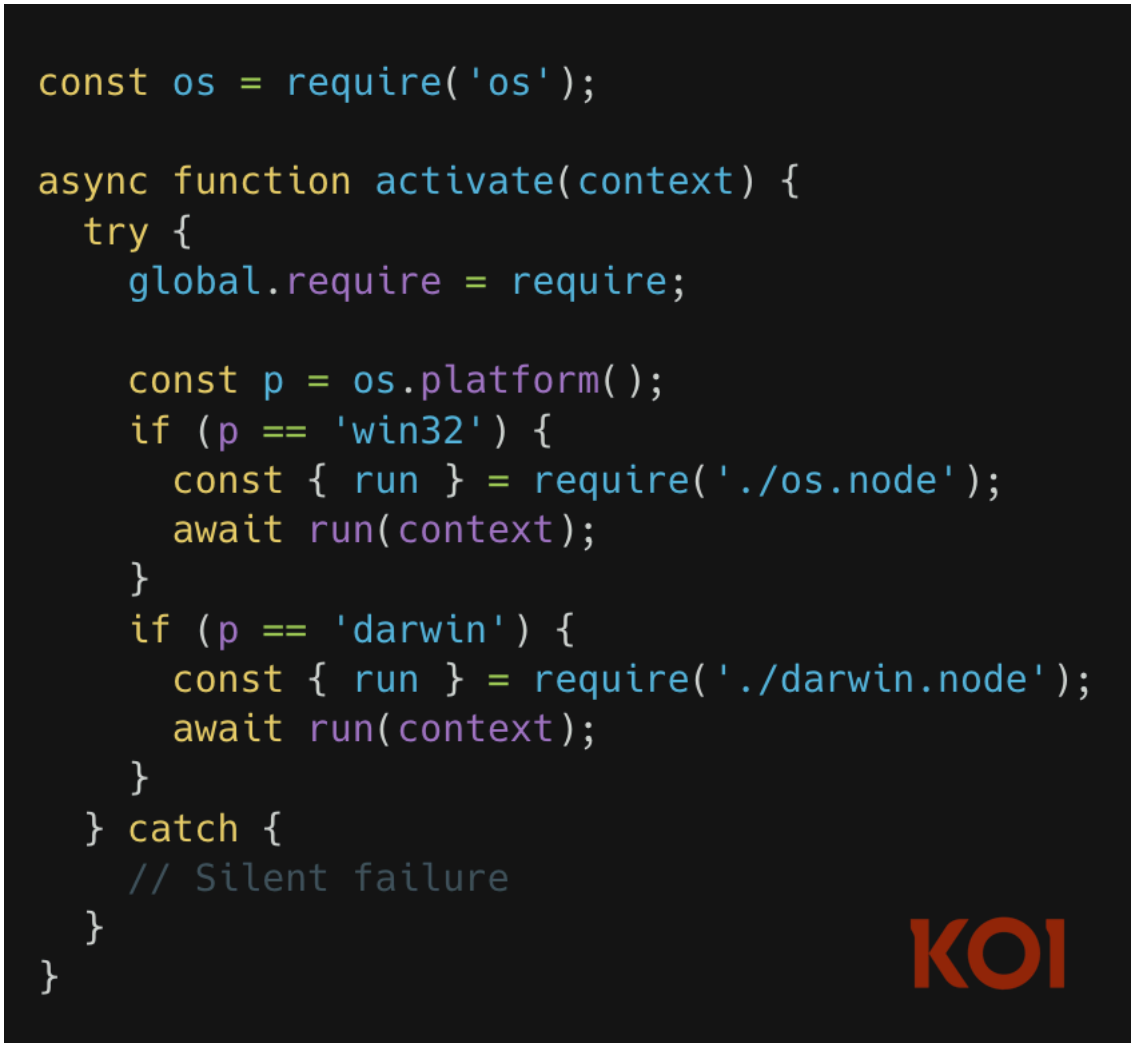
The fake Iconesvscode extension on Koidex



The real vscode-icons extension on Koidex

Version 12.15.0? Clean. A legitimate icon theme with 22,765 lines of JavaScript doing exactly what an icon theme should do.

But when versions 12.15.1 and 12.15.2 came out, the entire codebase got replaced with this:



Rust binary loader

Only 33 lines remained, no icon theme functionality, just a binary loader that detects your operating system and executes a native binary.

Those `.node` files – `darwin.node` for macOS, `os.node` for Windows – are Rust binaries, and they contain everything.

What's Inside the Binaries

Each extension come packed with these native binaries

The structure:

- Rust-based (the project is literally named `rust_implant`)
- Separate builds for Windows (`os.node`) and macOS (`darwin.node`)
- Around 2.4 MB each
- Node.js addon format

The functionality:

- Queries Solana blockchain for C2 instructions
- Fetches and decrypts payloads (Base64, AES-256-CBC)
- Google Calendar fallback built in

Developer traces:

The macOS binary contains paths like:

`/Users/davidioasd/Downloads/rust_implant/target/release/deps/librust_implant.dylib`

`/Users/davidioasd/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/http-body-util-0.1.3/src/combinators/collect.rs`

That `davidioasd` string matches patterns we saw in the first wave binaries. Same developer, same campaign, weeks apart.

What's Next

The extensions have all been taken down.

The Solana wallet is still there, the attacker's infrastructure is still up, and they've shown twice now that takedowns don't stop them for long.

We're continuing to monitor. Based on the pattern, this probably isn't the last wave.

IOCs

Extensions

OpenVSX:

- bphpburn.icons-vscode
- clangdcode.clangd-vscode
- csvmech.csv-sql-tsv-rainbow
- cweijamysq.sync-settings-vscode
- eamodas.shiny-vscode
- flutcode.flutter-extension
- iconkief.icon-theme-material
- msjsdreact.react-native-vscode
- saoudrizvsce.claude-dev
- saoudrizvsce.claude-devsce
- solblanco.svelte-vscode
- svltsweet.svetle-for-cursor
- tailwind-nuxt.tailwindcss-for-react
- vitalik.solidity
- yamlcode.yaml-vscode-extension

Microsoft VSCode:

- bphpburnsus.iconesvscode
- iconkieftwo.icon-theme-materiall
- clangdcode.clangd-vsce
- codevsce.codelddb-vscode
- csvmech.csvrainbow
- cweijamysq.sync-settings-vscode
- dart-vsc.code-dart
- flutcode.flutter-extension
- klustfix.kluster-code-verify
- lyywemhan.code-formatter-and-minifier-vscode
- msjsdreact.react-native-vsce
- prettier-vsc.vsce-prettier
- prisma-inc.prisma-studio-assistance
- redmat.vscode-quarkus-pro
- saoudrizvsce.claude-devsce
- solblanco.svetle-vsce
- vims-vsce.vscode-vim
- vsceue.volar-vscode
- yamlcode.yaml-vscode-extension

Rust Implants (SHA-256)

darwin.node

- 026873b940176d103d45b41c9fba73f14cfcaca60e3117be81d2eadef85a4d17
- 9bd105ce732218f30719fd69d4555967b362d37f4f6aec04741c18aaa7411a73
- fb07743d139f72fca4616b01308f1f705f02fda72988027bc68e9316655eadda

os.node

- cbb3f830731fe2c9194f7fe5aa55479cffdae184039b0df078b1394209d7a49f
- 29875e74f033c819c1acab58ef08bc35646aab5f4a2747ee0933ca41150d7099
- 6ebeb188f3cc3b647c4460c0b8e41b75d057747c662f4cd7912d77deaccfd2f2

Command & Control:

- 217.69.13.229
- 45.76.45.151
- 45.32.151.157
- 107.191.62.170
- 104.238.191.54 (exfiltration server)
- 108.61.208.161 (exfiltration server)
