Investigadores en ciberseguridad han identificado un gusano autorreplicante que se propaga a través de extensiones de Visual Studio Code (VS Code) en el registro Open VSX y en el Microsoft Extension Marketplace, lo que pone de manifiesto que los desarrolladores se han convertido en un objetivo privilegiado para los atacantes.

La amenaza, bautizada *GlassWorm* por Koi Security, es el segundo ataque a la cadena de suministro que golpea al ámbito DevOps en el plazo de un mes, tras el gusano Shai-Hulud que afectó al ecosistema npm a mediados de septiembre de 2025.

Lo que hace único a este ataque es el uso de la cadena de bloques de Solana para el control y mando (C2), lo que vuelve la infraestructura difícil de desmantelar. Además, emplea Google Calendar como mecanismo de respaldo para C2.

Otro aspecto novedoso es que la campaña GlassWorm se apoya en *"caracteres Unicode invisibles que hacen que el código malicioso literalmente desaparezca de los editores de código"*, señaló Idan Dardikman en un informe técnico. *"El atacante usó selectores de variación Unicode —caracteres especiales que forman parte de la especificación Unicode pero que no producen ninguna representación visual."*

El objetivo final del ataque es recolectar credenciales de npm, Open VSX, GitHub y Git, vaciar fondos de 49 extensiones de billetera criptográfica diferentes, desplegar servidores proxy SOCKS para convertir máquinas de desarrolladores en conductos de actividades delictivas, instalar servidores VNC ocultos (HVNC) para acceso remoto, y explotar las credenciales robadas para comprometer paquetes y extensiones adicionales y seguir propagándose.

Los nombres de las extensiones infectadas —trece en Open VSX y una en el Microsoft Extension Marketplace— son los siguientes. Estas extensiones acumulan alrededor de 35,800 descargas. La primera oleada de infecciones ocurrió el 17 de octubre de 2025. Aún se desconoce cómo fueron secuestradas estas extensiones.

- codejoy.codejoy-vscode-extension 1.8.3 y 1.8.4
- l-igh-t.vscode-theme-seti-folder 1.2.3

- kleinesfilmroellchen.serenity-dsl-syntaxhighlight 0.3.2
- JScearcy.rust-doc-viewer 4.2.1
- SIRILMP.dark-theme-sm 3.11.4
- CodeInKlingon.git-worktree-menu 1.0.9 y 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
- cline-ai-main.cline-ai-agent 3.1.3 (Microsoft Extension Marketplace)

El código malicioso oculto en las extensiones está diseñado para buscar transacciones relacionadas con una billetera controlada por el atacante en la cadena de bloques de Solana y, si las encuentra, extraer una cadena en Base64 del campo memo que decodifica la dirección del servidor C2 (*"217.69.3[.]218"* o *"199.247.10[.]166"*) usada para recuperar la carga siguiente.

La carga es un *stealer* que recoge credenciales, tokens de autenticación y datos de billeteras criptográficas, y además consulta un evento de Google Calendar para parsear otra cadena en Base64 y contactar al mismo servidor para obtener una carga denominada *Zombi*. Los datos exfiltrados se envían a un punto remoto (*"140.82.52[.]31:80"*) gestionado por el actor malicioso.

Programado en JavaScript, el módulo *Zombi* transforma una infección de GlassWorm en una comprometida completa: instala un proxy SOCKS, módulos WebRTC para comunicación peer-to-peer, la tabla distribuida de hash (DHT) de BitTorrent para distribución descentralizada de comandos, y HVNC para control remoto.

El problema se agrava porque las extensiones de VS Code están configuradas para actualizarse automáticamente, lo que permite a los atacantes distribuir código malicioso sin

que el usuario tenga que interactuar.

“This isn’t a one-off supply chain attack,” dijo Dardikman. *“It’s a worm designed to spread through the developer ecosystem like wildfire.”*

“Attackers have figured out how to make supply chain malware self-sustaining. They’re not just compromising individual packages anymore – they’re building worms that can spread autonomously through the entire software development ecosystem.”

Este suceso coincide con un aumento en el uso de blockchains para alojar cargas maliciosas, debido a la seudonimidad y flexibilidad que ofrecen, técnica que incluso actores vinculados a Corea del Norte han utilizado tanto en campañas de espionaje como en operaciones con motivación financiera.