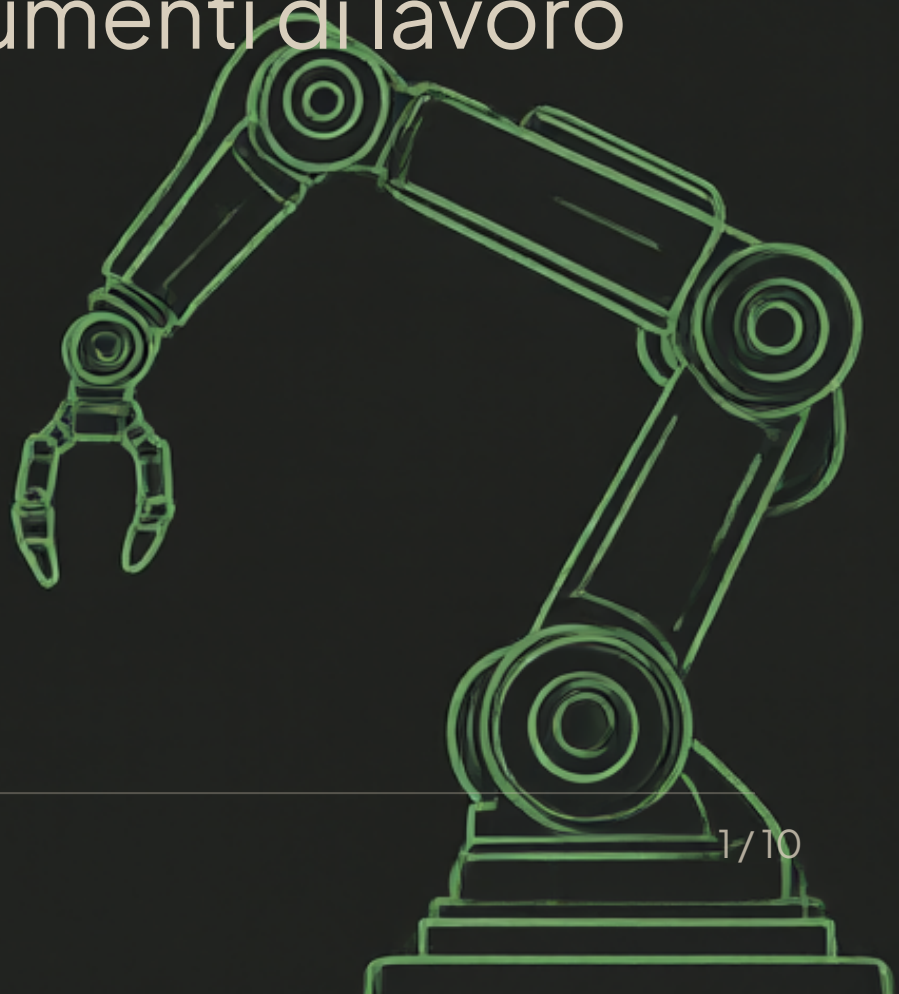
TECNICAI

Un'estensione ufficiale ha infettato i PC di chi aggiorna in automatico.

Il 29 ottobre il canale di distribuzione di Claude Code è stato compromesso. È la storia giusta per chi usa strumenti di lavoro con dentro i dati dei clienti.



29 ottobre 2026. Il negozio di estensioni di Cursor distribuisce la versione 2.1.313 di Claude Code.

È l'estensione di Anthropic, con l'ID ufficiale.

Dentro, sessantasei righe di codice malevolo prima del codice vero.

Chi aveva l'aggiornamento automatico l'ha installata senza scegliere nulla.

Fonte: OpenSourceMalware, analisi tecnica, 30/10/2026



Fonte: OpenSourceMalware, analisi tecnica, 30/10/2026

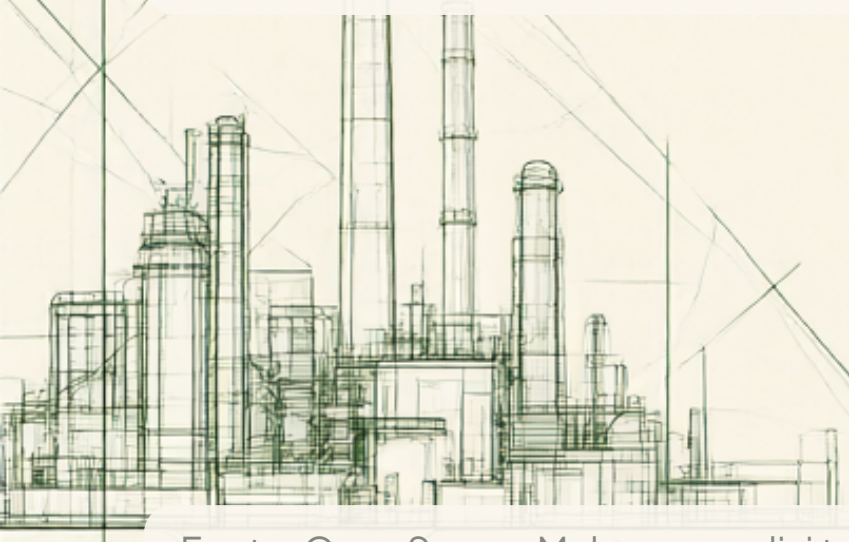
Basta aprire l'editor. Non serve usare l'AI.

Il codice malevolo parte all'avvio del programma.

Aggiunge al PC una chiave SSH: una porta aperta che permette di entrare da fuori.

La firma «svc-telemetry», per sembrare un servizio di sistema.

Fonte: OpenSourceMalware, analisi tecnica, 30/10/2026



Fonte: OpenSourceMalware, analisi tecnica, 30/10/2026

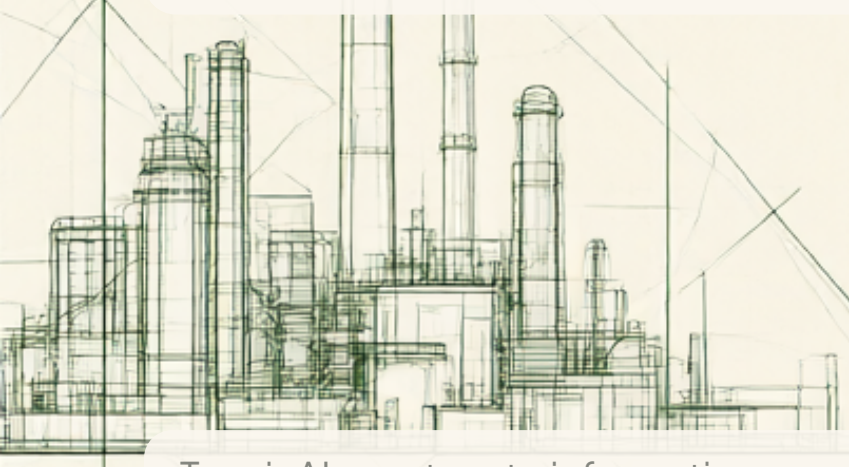
Poi fa l'inventario della macchina.

Indirizzo pubblico, nome del PC, utente, sistema operativo, email di git.

E l'elenco dei nomi delle variabili che contengono KEY, TOKEN, SECRET, AWS, GCP.

Solo i nomi, non i valori.

Basta a chi guarda per sapere quali conti cloud sono aperti su quel PC, prima ancora di entrarci.



Cursor ha precisato: quella versione non è stata sviluppata da Anthropic.

Vero. E non risponde alla domanda.

Il problema è il canale: l'aggiornamento automatico si fida del negozio, e il negozio è stato compromesso.

In pratica, la fiducia che il tuo PC ripone in un aggiornamento non è la tua.

Il pacchetto ufficiale npm è sano. Il negozio Microsoft è sano. Open VSX è sano.

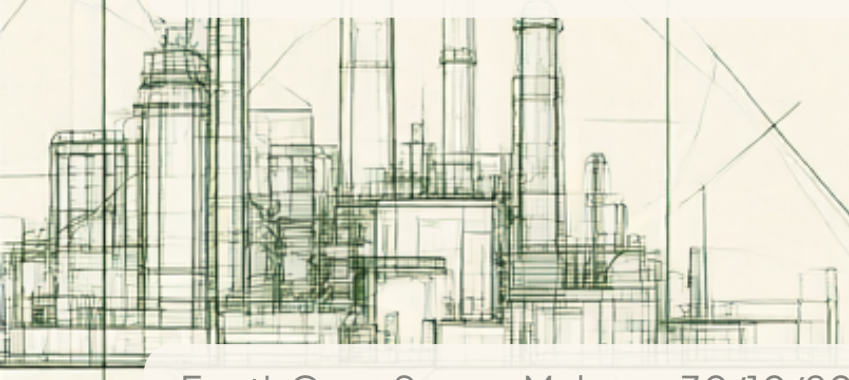
La finestra è durata undici ore, su un solo canale.

I dispositivi coinvolti sono al massimo cinquemila.

La versione pulita, la 2.1.314, è già disponibile.

Non è un problema dell'AI. È una cattiva giornata di un distributore.

Fonti: OpenSourceMalware 30/10/2026; comunicato Cursor, per resoconto stampa



Fonti: OpenSourceMalware 30/10/2026; comunicato Cursor, per resoconto stampa

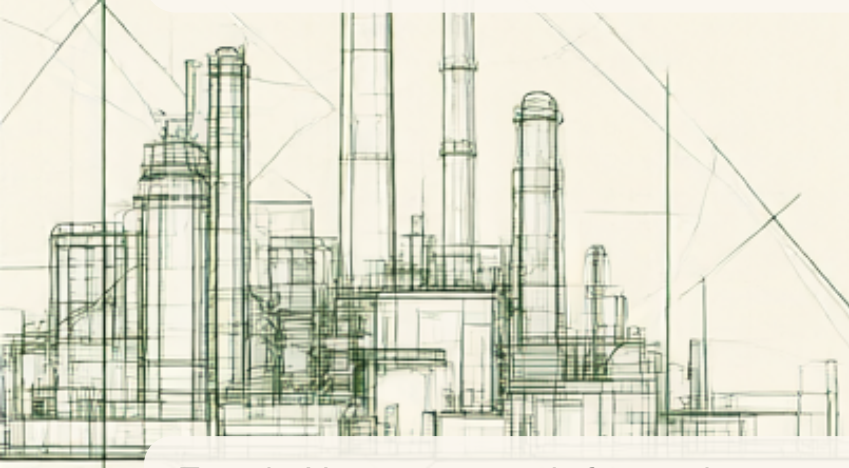
PER IL TUO LAVORO

Un editor di codice in studio è un trattamento di dati.

Contiene cartelle dei clienti, accessi ai servizi, configurazioni.

Un componente che si aggiorna da solo affida la sicurezza dei tuoi clienti a un soggetto terzo, senza contratto e senza verifica.

L'articolo 32 del GDPR chiede misure di sicurezza adeguate al rischio. Il canale di aggiornamento è una di queste.



Tre regole da non sviluppatori.

Uno. Gli strumenti che contengono dati dei clienti si aggiornano a mano, dopo qualche giorno dall'uscita della versione.

Due. Una volta l'anno: quali programmi vedono le cartelle dei clienti, e verso quali servizi cloud puntano?

Tre. La provenienza conta più della notorietà. Lo stesso software, sul canale giusto, era sano.



Tre domande da fare al tuo PC.

1. Quale software si aggiorna da solo, qui sopra?
2. Quali cartelle dei clienti può leggere?
3. Da quale canale arriva il suo aggiornamento?

Dieci minuti, una volta. È l'inventario che precede ogni sicurezza.



MI PRESENTO:

La macchina aggiorna e distribuisce. La persona verifica e giudica.

Dubbi sul PC dove fai girare l'AI? Scrivici: info@tecnicai.it

Iscritto all'Ordine dei Periti Industriali di Padova · RSPP · Professionista antincendio n° PD01774P00344 · Docente dal 2012 · Fondatore TecnicAI · Co-fondatore Omeda Studios.

Contenuto informativo, non consulenza legale. Altri documenti gratuiti su tecnicai.it/news

