KILLSWITCH · ISSUE #11 · 11 NOV 2026

Uninstalling Isn't Cleaning Up: The Fake Claude Code Extension in Cursor's Marketplace

A tampered Claude Code extension planted an SSH key and startup scripts. Removing it leaves both behind.

Killswitch rating: Check your developer machines

By Emmanuel Aigbehi Walstra

Uninstalling isn't cleaning up

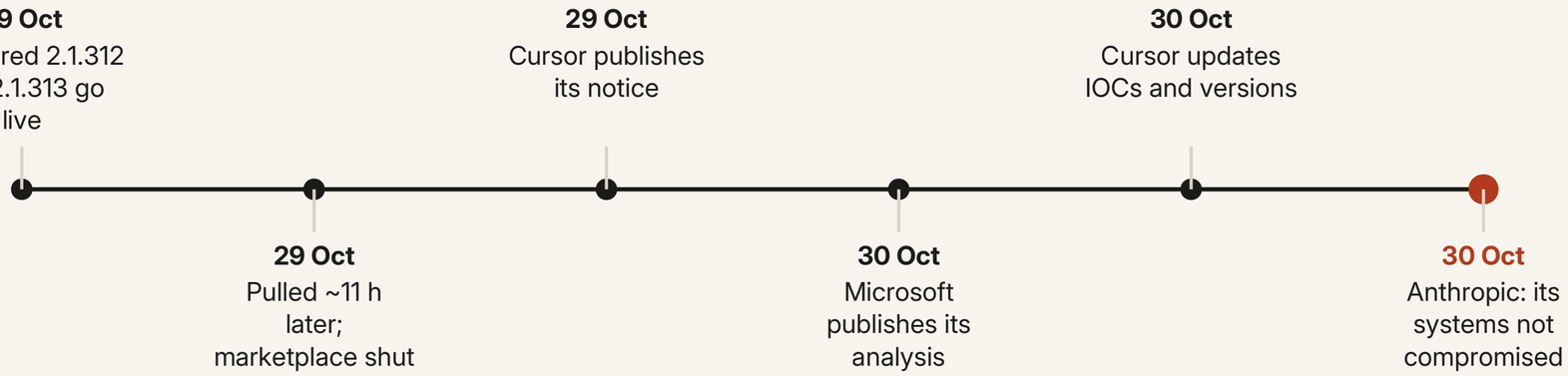
On 29 October Cursor's marketplace served tampered Claude Code builds 2.1.312 and 2.1.313 for macOS and Windows for about 11 hours [1].

- "Uninstalling the extension may not be sufficient" (Cursor) [1].
- The payload writes an SSH key and startup scripts outside the extension folder [1][2].

Not built by Anthropic. Limited to Cursor's marketplace.

- Cursor: the versions "were not developed by Anthropic" [1].
- Anthropic told Microsoft its systems were not compromised [2].
- Not distributed via the Visual Studio Marketplace or npm [2]. Someone from Anthropic: 2.1.313 was never on its official hosts [11].
- 'Up to 5,000' is Cursor's early estimate, reported by Sophos and StepSecurity [3][9].

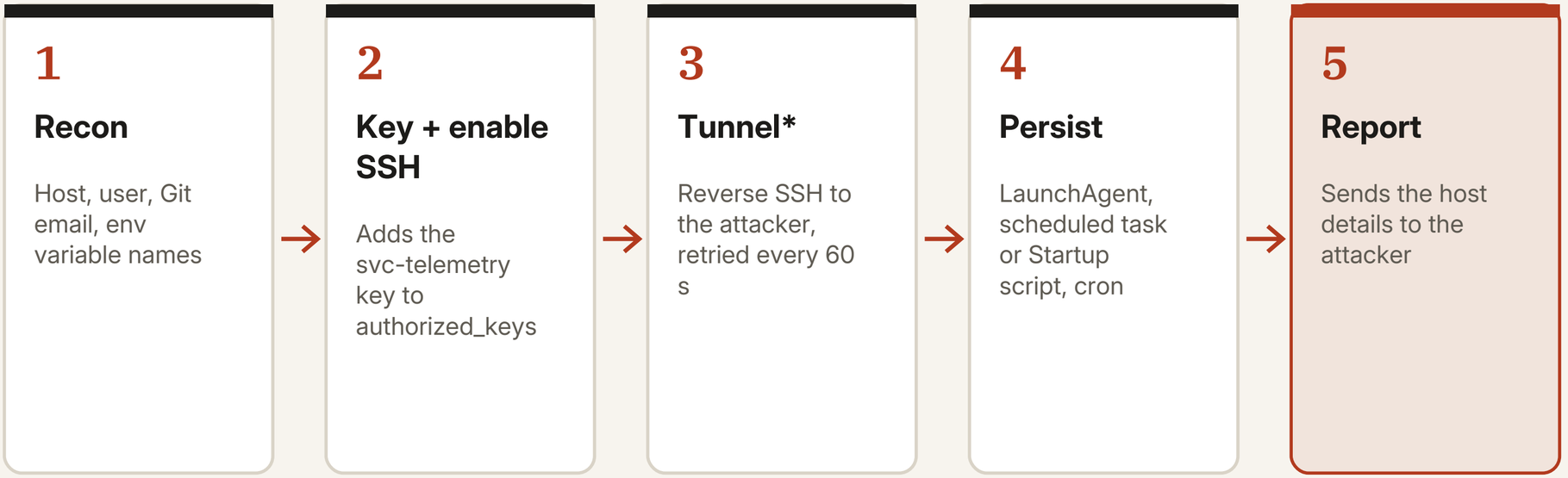
Eleven hours in the marketplace



Cursor [1], Microsoft [2], StepSecurity [9]. All dates 2026.

Exact window: see Cursor's notice [1]. "About 11 hours" is our arithmetic.

What it does, in order



Code execution order per Microsoft [2]. *Login through the tunnel fails on most hosts: enabling SSH needs admin rights [1].

The login mostly failed. The backdoor did not.

- Switching on SSH needs admin rights the extension lacks on most macOS and Windows hosts [1].
- There, the attacker could not log in through the tunnel [1].
- But the key, the startup scripts and the host report still happened [1][2].
- Env variable **names**, not values, were sent [2].

06 · RESPOND

If you installed it: check, then clean up

1. **Is the key there?**
   Look for the svc-telemetry key in authorized_keys
2. **Hunt**
   Endpoint, network and extension-install telemetry
3. **Isolate**
   Hosts with signs the payload ran
4. **Remove, then decide on rebuild**
   Key, startup entries, tunnel processes
5. **Rotate from a clean machine**
   Credentials and sessions the host could reach

Cursor's five steps [1], shortened. Preserve evidence first [2].

Four controls that blunt the next one

1 Allowlist publishers

Any entry blocks the rest unless "*" is allowed

2 Install cooldown

Default 0 (off). Set hours fleet-wide

3 Signature verification

Require valid Open VSX signatures (Enterprise)

4 Extension inventory

Who runs what version, from which marketplace

Cursor controls [4][5][8]. The inventory is a Killswitch addition.

A cooldown of 12 hours or more would probably have kept these builds out: our inference, not a vendor claim [1][4].

Where this lives in your frameworks

Prevent	A.5.19, A.5.21, A.8.19, A.8.32 · NIS2 21(2)(d), (e) · Evidence: allowlist and cooldown settings
Know	A.5.9, A.8.2 · NIS2 21(2)(i) · Evidence: extension inventory
Respond	A.5.26, A.5.28 · NIS2 21(2)(b) · Evidence: key check and rotation log
Learn	A.5.27 · NIS2 21(2)(b), (c) · Evidence: post-incident review

Killswitch's own mapping. Check ISO titles against your licensed copy.

ISO/IEC 27001:2022 [6] · NIS2 Art. 21(2), Art. 23 [7]. Killswitch mapping.

09 · STILL OPEN

What we don't know yet

- How the builds got in: not disclosed by Cursor [1]. Someone from Anthropic, on Hacker News: an attacker "used access to Cursor's marketplace" [10][9]. An individual's comment; Cursor has not confirmed it.
- Linux: no Linux build listed, but the payload has a Linux code path [1][2].
- 'Up to 5,000' is Cursor's early estimate, reported by Sophos and StepSecurity [3][9].

This week

- Find every machine running Cursor; check 29 Oct installs and updates.
- Run Cursor's key check; preserve evidence; follow the five steps [1].
- Rotate reachable credentials from a clean machine.
- Set an allowlist and a non-zero install cooldown [4][5].
- Start an extension inventory; keep the evidence.

Sources

[1] Cursor: Security notice, malicious version of Anthropic.claude-code (2.1.312 and 2.1.313) in the Cursor VS Code Extension Marketplace (29 Oct 2026, updated 30 Oct)
[2] Microsoft Security Blog: Inside a malicious Claude Code-branded extension and its persistent SSH backdoor (30 Oct 2026)
[3] Sophos X-Ops: Malicious Claude Code extension distributed through Cursor marketplace
[4] Cursor Help: Extensions (marketplace install cooldown, allowed extensions, signature verification)
[5] Cursor Docs: Security and Privacy Hardening
[6] ISO/IEC 27001:2022 Information security management systems
[7] NIS2 Directive (EU) 2022/2555, Articles 21 and 23
[8] Cursor Docs: Deployment Patterns (AllowedExtensions policy)
[9] StepSecurity: Trojanized Claude Code Extension Delivered Persistent SSH Backdoor to Developer Machines (30 Oct 2026, updated 1 Nov)
[10] Hacker News: comment by Felix Rieseberg (felixrieseberg, self-identified as from Anthropic), item 50304129 (30 Oct 2026)
[11] Hacker News: comment by David Dworken (ddworken, self-identified as from Anthropic), item 50305148 (30 Oct 2026)

Facts are from Cursor's security notice and Microsoft's analysis, with Sophos and StepSecurity where stated, as published by 2 Nov 2026. How the tampered builds got into the marketplace has not been fully disclosed. The cooldown reasoning, the extension inventory control and the framework mapping are Killswitch's own.

FROM THE PUBLISHERS OF KILLSWITCH

Know every tool on your developer machines, and who approved it

GRCOMPLIANCE

Keep an inventory of approved software and suppliers, link the evidence, and map controls to ISO 27001 and NIS2.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.