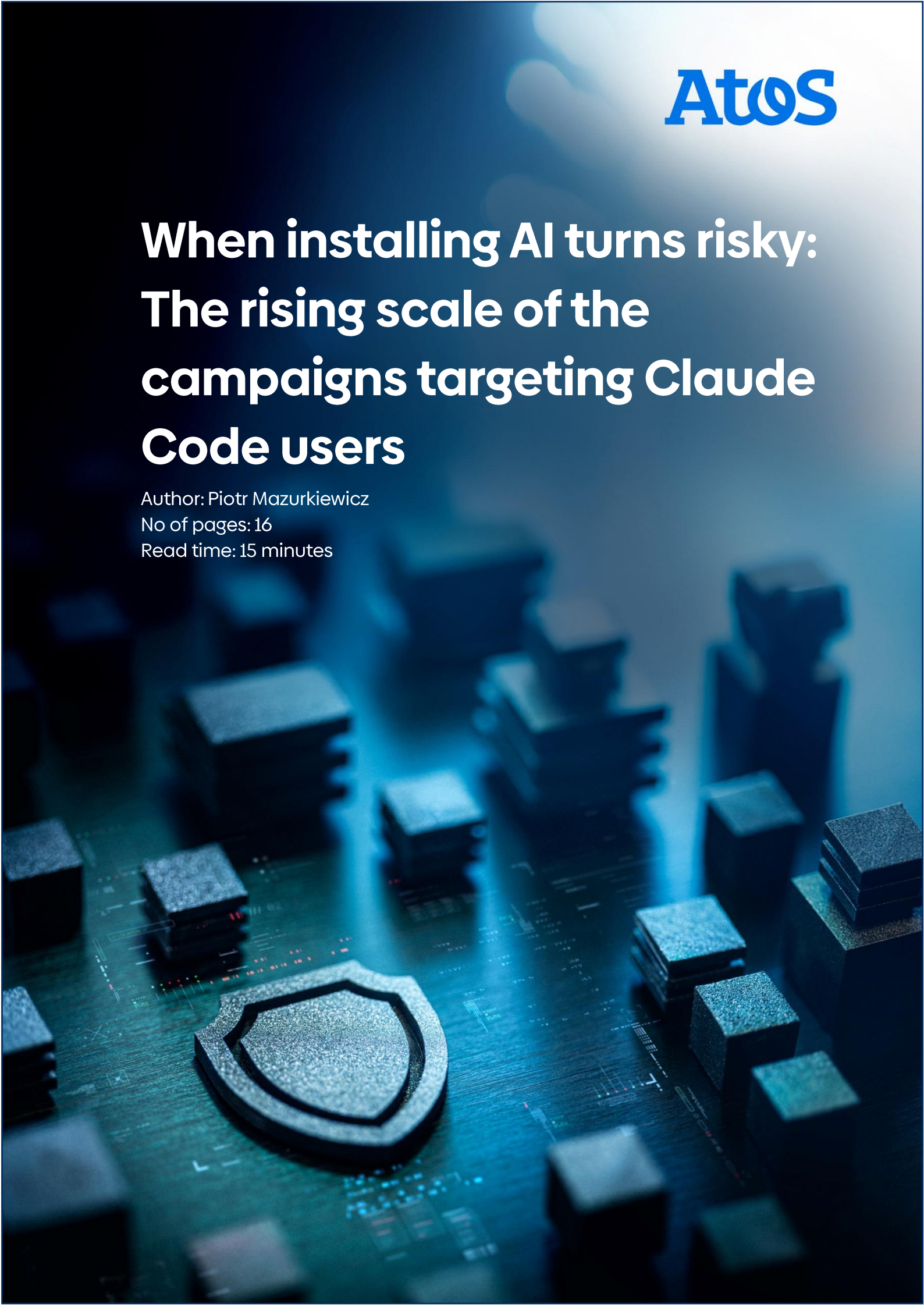
When installing AI turns risky: The rising scale of the campaigns targeting Claude Code users

Author: Piotr Mazurkiewicz
No of pages: 16
Read time: 15 minutes



Contents

1 Summary

The rapid adoption of Anthropic's Claude Code LLM has been followed by a visible rise in targeted attacks aimed at developers and security practitioners. The common thing across these operations is not just brand impersonation, but an abuse of normal developer behavior: searching for installation guidance, trusting high-ranking search results, and pasting one-line commands into a terminal without deeply validating the source.

The most prominent of these operations is the so-called InstallFix campaign, which combines malvertising, SEO poisoning, and cloned websites and/or documentation to push victims toward malicious PowerShell or bash commands. In several cases, the attacker deliberately installs the legitimate tool in the foreground, so the victim assumes everything worked as expected while credential theft continues quietly in the background.

What makes these campaigns especially serious is the profile of the victim. Claude Code users are typically developers, security engineers, and cloud engineers working from privileged workstations. A successful compromise can expose valuable information like browser sessions, enterprise chat tokens, API keys, SSH keys, cloud credentials, cryptocurrency wallets, source code access, and secrets stored in environment variables or system keychains.

Atos' Threat Research Center is actively monitoring multiple campaigns and groups involved in leveraging search engine results and AI popularity. The activity described in next sections of this article shows a broadening ecosystem of lures. While Claude Code is a central theme, the same infrastructure and tradecraft also appear around Gemini CLI and other developer tools. That suggests the campaign is less about one product alone and more about monetizing trust around fast-growing AI-assisted development workflows.

2 Campaign Overview

The campaign activity described in this article was already present at the start of 2026 but began to ramp up noticeably in early March. From there, it sustained a high level of activity throughout May and surged even further in early June, marking the most intense phase we've observed so far.

At a high level, the campaign blends sponsored search placements, typosquatted domains, cloned product pages, and social engineering techniques to make malicious installation steps appear ordinary. This lowers suspicion significantly, as victims are not prompted to download clearly malicious files or explicitly weaken their security posture. Instead, everything is framed to resemble a standard software setup process, borrowing familiar visuals and workflows.

Targets are typically drawn in via search queries like "Claude Code download", "Claude Code CLI install", or similar brand-related terms. After landing on a fake site, they are guided through modified installation instructions. On Windows systems, this may result in execution of fileless payloads via PowerShell. On macOS, users may be redirected to what appears to be a legitimate shared chat on claude.ai, where the instructions include base64-encoded terminal commands.

In both cases, the attacker shifts the trust decision away from a downloaded file and onto the perceived legitimacy of the instructions themselves, making the entire flow feel routine rather than risky.

3 Why Claude Code Users Are an Attractive Target

Claude Code users sit at the intersection of high privilege and high velocity. They often have local access to source repositories, cloud credentials, production secrets, chat platforms, and browser sessions that reach sensitive internal systems. A single foothold on that endpoint can therefore generate both immediate criminal value and longer-term access opportunities.

The campaign also benefits from the culture around AI-assisted coding. Developers are increasingly used to rapid experimentation, copying commands from documentation, and trusting tools that promise a faster path from prompt to working code. That habit creates fertile ground for lures that only need to look plausible for a few seconds.

A second-order risk appears in the source material as well: prompt injection, malicious plugins, and package-based compromise. In other words, the danger is not limited to fake installers. It extends to the broader ecosystem of AI coding assistants, third-party extensions, and dependencies that can be manipulated to expose local secrets or introduce malicious code into the supply chain.

4 Key Judgments

- InstallFix is effective because it weaponizes a routine developer action: copying installation commands from search results or online guides.
- Malvertising and SEO poisoning remain the primary initial-access channels for Windows-focused Claude Code impersonation campaigns.
- macOS users are being targeted through a distinct but equally effective pattern: malicious instructions embedded in legitimate public Claude shared chats.
- Payloads are tuned to developer workstations and prioritize theft of credentials, browser sessions, API tokens, SSH keys, AWS material, and other cloud-relevant secrets.
- The campaign set is evolving beyond credential theft into longer-term access, evidenced by backdoors such as Beagle and supply-chain style propagation through malicious packages and plugins.
- The same operators, or at minimum the same playbook, appear to be extending into adjacent AI brands and popular developer tooling to increase reach.

5 How the Attack Chain Works

Stage 1: Discovery: The victim searches for Claude Code installation guidance or clicks an advertisement that appears to point to a legitimate vendor resource.

Stage 2: Impersonation: The actor redirects the victim to a cloned or typosquatted site that closely mirrors real documentation or branding.

Stage 3: Command substitution: Legitimate npm, curl, or shell instructions are swapped for malicious PowerShell, bash, or other base64-encoded commands.

Stage 4: Compromise: A fileless infostealer or backdoor executes, often while the real software is installed simultaneously to reduce suspicion.

Stage 5: Collection and exfiltration: The malware targets browser credentials, session tokens, keychain data, API and SSH keys, AWS material, wallets, and other secrets, then forwards them to attacker-controlled infrastructure.

Stage 6: Follow-on access: In more advanced cases, the actor establishes persistence or remote control through sideloaded DLLs, encrypted C2 channels, or package-based propagation into build environments.

6 Observed delivery vectors and related payloads

Attack Vector	Primary Payload	Representative Malicious Domains / Lures
SEO poisoning	Amatera infostealer	claudecode[.]co[.]com, claude-setup[.]com
Malvertising	Beagle backdoor / staged payloads	download[.]version-516[.]com, download-version[.]1-5-8[.]com
Shared chats	MacSync (macOS)	Public claude[.]ai shared chats containing base64 commands
Package / plugin lures	Shai-Hulud-style secret theft, malicious plugin behavior	npm, PyPI, GitHub-hosted lure content

7 Technical Analysis by Platform

7.1 Windows

Windows-focused campaigns lean heavily on fileless execution. The material provided repeatedly points to mshta.exe and PowerShell as launch mechanisms for staged code that runs largely in memory. This matters because it allows an attacker to blend into administrative activity and reduce the visible footprint on disk.
Amatera is described as a common payload in these operations. Its collection priorities include browser credentials, session cookies, communication-platform tokens, and wallet-related data. The campaign notes also reference attempts to blind local inspection by disabling or interfering with AMSI and ETW before collection begins.
A more capable post-compromise option, Beagle, is associated with DLL sideloading through a signed antivirus binary. In the example supplied, a fake Claude AI site delivered a large ZIP archive containing NOVupdate.exe and a malicious avk.dll, which then executed DonutLoader shellcode in memory to establish persistent remote access over encrypted channels.

7.2 macOS

The macOS branch of the campaign reflects a different social engineering style.

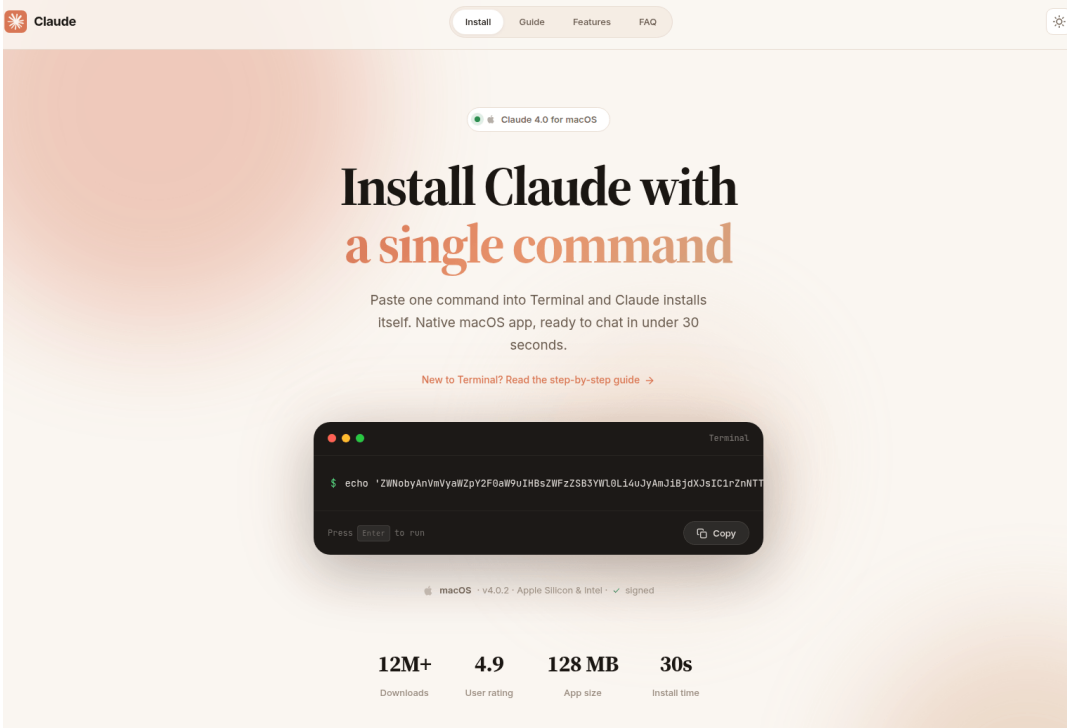


Figure 1 Broad InstallFix campaign against MacOS users (atlastgpt-browser[.]com)

In addition to fake download pages, attackers used real public Claude shared chats that appeared to contain installation guidance. Because the hosting domain was legitimate, users had fewer visual cues that anything was wrong.
The analysis names AMOS (Atomic Stealer) and MacSync as the principal macOS threats. Their objectives are tightly aligned with developer environments: exfiltrating data from the macOS Keychain, browser stores, local SSH folders, AWS configuration directories, and cryptocurrency wallets.

8 What the Recent Numbers Suggest

The activity is heavily concentrated between March and June 2026, reaching its highest levels in May and early June. Based on the data from Atos' TRC monitored campaigns - Windows accounts for the majority of observed payload activity at around 65%, followed by macOS at 30%, while Linux-related activity is estimated at 5%.
The same material also ranks initial-access patterns by frequency. Google Ads-driven malvertising leads with a count of 45 observed lures, followed by SEO poisoning at 30, shared Claude chats at 20, and GitHub-based lure repositories at 15. Taken together, those numbers point to a mature campaign stack rather than a single opportunistic wave.

Metric	Observed Value / Interpretation
Campaign period emphasized in source material	March–June 2026, with heightened activity in May 2026
Estimated OS distribution	Windows 65% | macOS 30% | Linux 5%
Most frequent lure type	Google Ads / malvertising (45 observed lures)
SEO poisoning activity	30 observed lures tied to typosquatted or highly ranked fake sites
Shared-chat lures	20 observed lures using real claude.ai shared URLs
GitHub lure activity	15 observed repositories / forks / bait content

9 Defensive Considerations

- Treat installation instructions as untrusted content until the source domain, package name, and signing context have been verified independently.
- Block or aggressively monitor access to newly registered, typosquatted, and ad-amplified domains associated with AI tooling and developer software.
- Harden PowerShell, mshta.exe, and script interpreter telemetry; alert on encoded commands, AMSI/ETW tampering, and unusual child-process trees from browsers.
- On macOS, monitor Terminal execution launched from copied content, access to Keychain material, and exfiltration attempts touching ~/.ssh, ~/.aws, and browser stores.
- Apply browser-session protection and token hygiene for Slack, Teams, Zoom, GitHub, cloud consoles, and internal developer portals.
- Restrict unapproved package sources, review developer plugins and extensions, and implement guardrails around CI/CD secrets and package publication workflows.
- Publish internal installation playbooks for approved AI developer tools so engineers are not forced to rely on ad-driven search results or unofficial tutorials.

10 Infrastructure Summary

Category	Examples
Lure domains	claudecode[.]co[.]com claude-setup[.]com claudecode[.]lat nodejs-setup[.]com
C2 and exfiltration	events[.]msft23[.]com events[.]ms709[.]com customroofingcontractors[.]com
Payload hosting	download[.]version-516[.]com download-version[.]1-5-8[.]com
Shared-chat delivery	Legitimate public claude[.]ai shared URLs containing attacker-supplied commands

11 Indicators of Compromise

Claude Code & Anthropic impersonation

- atlasgpt-browser[.]com
- claudemac.netlify[.]app
- payforwin.github[.]io
- buyaneli876-oss.github[.]io
- www.trashbutler[.]com/clod/
- vignesh2027.github[.]io
- sites.google[.]com/view/claudeapps/claude
- claudecode-ai.netlify[.]app/desktop.html
- cxotoday[.]com/clade/
- sites.google[.]com/view/bossclaude/claude
- mypelvi[.]com/clu/
- huysosi-guboitryasi[.]com
- clavdiydetka[.]com
- claudecode[.]co[.]com
- claude-setup[.]com
- claude-pro[.]com
- claudecode[.]lat
- claudecode-buy[.]com
- blog-anthropic[.]com
- claude-code-install[.]squarespace[.]com
- claudecode-developers[.]squarespace[.]com
- claude-code-macos[.]com
- license[.]claude-pro[.]com
- www[.]claude-code-ai[.]online
- www[.]claude-setup[.]com
- www[.]phil-anthropic[.]space
- anthropic[.]hoosese[.]com
- anthropic[.]json[.]freebitcoin[.]tech
- anthropic[.]motorcycles
- anthropic[.]www[.]mx[.]blockchainpoker[.]io
- anthropic[.]www[.]myapple[.]app
- claude-ai[.]cc
- claude-code-tutorial[.]com
- claude-code[.]official-version[.]com/claude
- claude-code[.]org[.]cn
- www[.]anthropic[.]motorcycles
- www[.]claude-code-tutorial[.]com
- www[.]claudecode[.]lat
- www[.]claudecode[.]tokyo
- anthropic[.]cpcontacts[.]freebitcoin[.]tech
- www[.]mcp-anthropic[.]com
- claude-code-learn[.]tilkly[.]com

- claude-code[.]official-version[.]com
- www[.]claudecode[.]inc
- www[.]claude-code[.]ink
- www[.]claude-code[.]official-version[.]com
- www[.]claudecode[.]christmas

Gemini CLI & Google AI impersonation

- geminicli[.]co[.]com
- gemini-setup[.]com
- gemini-ai[.]co[.]com
- download[.]version-516[.]com
- download-version[.]1-5-8[.]com
- www[.]gemini-setup[.]com
- www[.]wp-gemini-cli[.]top

Broader developer lures

- nodejs-setup[.]com
- cursor-setup[.]com
- openclaw-install[.]com
- keepassxc-setup[.]co[.]com
- chocolatey-install[.]com

C2 / exfiltration / payload hosting

- events[.]msft23[.]com
- events[.]ms709[.]com
- customroofingcontractors[.]com
- bernasibutuwqu2[.]com
- hgjbulk[.]pages[.]dev
- claude-code-docs-site[.]pages[.]dev

Observed paths and installation endpoints

- claude-setup[.]com/check
- claude-setup[.]com/install
- gemini-setup[.]com/index

About Atos Group

Atos Group is a global leader in digital transformation with c. 56,000 employees and annual revenue of c. €7.2 billion (at the go-forward perimeter), operating in 54 countries under two brands - Atos for services and Eviden for products and systems. European number one in cybersecurity and a leader in cloud, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is listed on Euronext Paris.

Find out more about us

atos.net
atos.net/career