

Forum:[Hack Forums](#)

Thread: [Fake OpenAI repository on Hugging Face pushes infostealer malware](#)

MadScientist - May 9, 2026, 5:18 pm

A malicious Hugging Face repository that reached the platform's trending list impersonated OpenAI's "Privacy Filter" project to deliver information-stealing malware to Windows users.

The repository briefly reached #1 on Hugging Face and accumulated 244,000 downloads before the platform responded to reports and removed it.

The Hugging Face platform lets developers and researchers share AI models, datasets, and machine learning (ML) tools. Models are pre-trained AI systems hosted on the platform comprising weight files, configuration, and code.

Researchers at HiddenLayer, a company focused on safeguarding AI and ML models against attacks, discovered the campaign on May 7, after noticing a malicious repository named Open-OSS/privacy-filter.

"The repository had typosquatted OpenAI's legitimate Privacy Filter release, copied its model card nearly verbatim, and shipped a loader.py file that fetches and executes infostealer malware on Windows machines," the researchers explain.

The 'loader.py' Python script included fake AI-related code to appear harmless, but in the background, it disabled SSL verification, decoded a base64 URL pointing to an external resource, and then fetched and executed a JSON payload containing a PowerShell command.

The command, which is executed in an invisible window, downloads a batch file (start.bat) that performs privilege escalation, downloads the final payload (sefirah), adds it to Microsoft Defender's exclusions for it, and executes it.

The final payload is a Rust-based infostealer that targets the following sensitive data:

- Browser data from Chromium- and Gecko-based browsers (e.g., cookies, saved passwords, encryption keys, browsing data, session tokens)
- Discord tokens, local databases, and master keys
- Cryptocurrency wallets and wallet browser extensions
- SSH, FTP, and VPN credentials and configuration files, including FileZilla
- Sensitive local files and wallet seeds/keys
- System information
- Multi-monitor screenshots

The stolen data is compressed and exfiltrated to a command-and-control (C2) server at [recargapopular\[.\]com](#).

Read More -

<https://www.bleepingcomputer.com/news/security/fake-openai-repository-on-hugging-face-pushes-in-fostealer-malware/>

