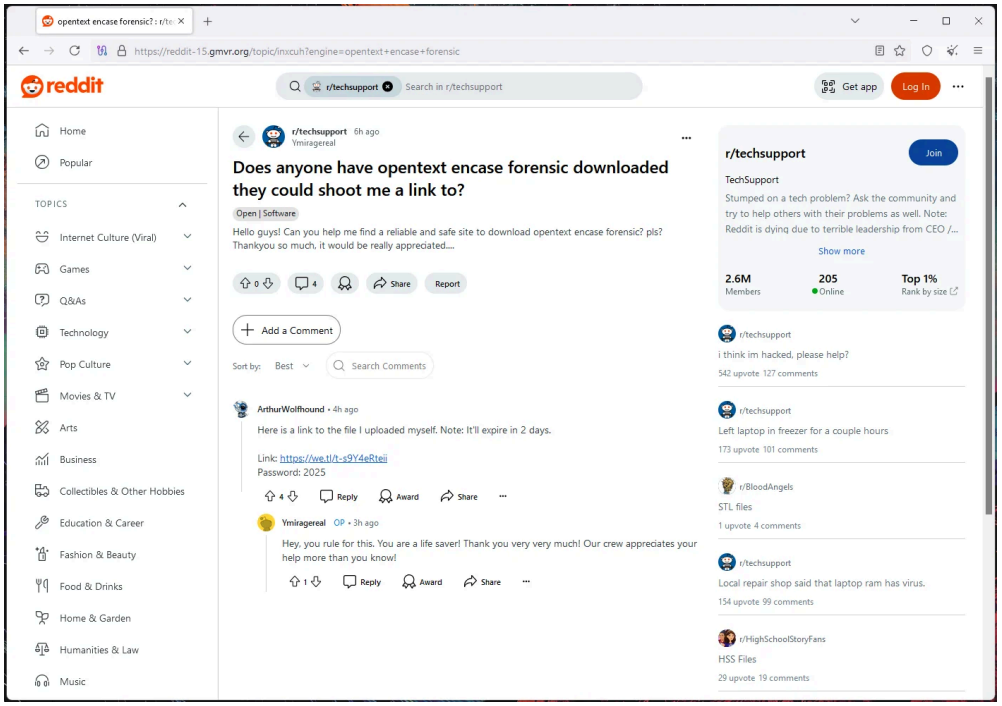
Hundreds of fake Reddit sites push Lumma Stealer malware

By Bill Toulas

Published: 2025-01-23 · Archived: 2026-04-05 17:13:57 UTC

Hackers are distributing close to 1,000 web pages mimicking Reddit and the WeTransfer file sharing service that lead to downloading the Lumma Stealer malware.

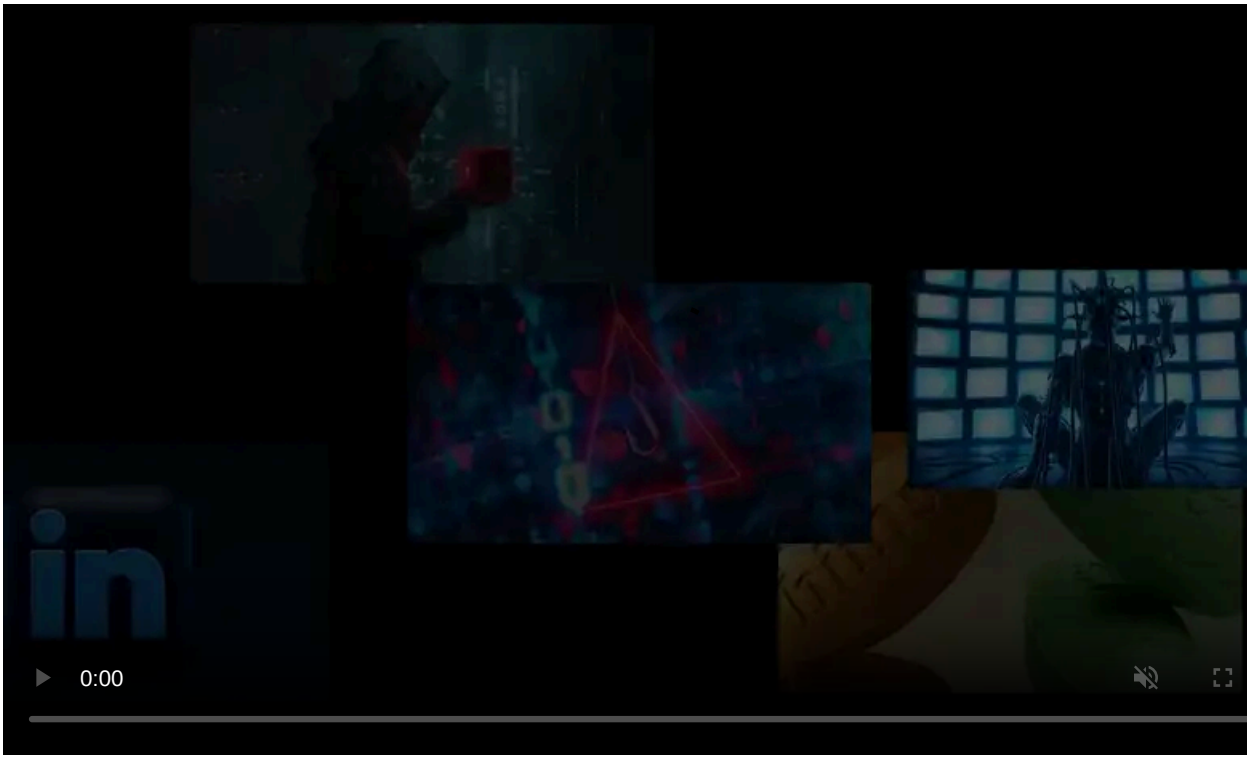
On the fake pages, the threat actor is abusing the Reddit brand by showing a fake discussion thread on a specific topic. The thread creator asks for help to download a specific tool, another user offers to help by uploading it to WeTransfer and sharing the link, and a third thanks him to make everything appear legitimate.

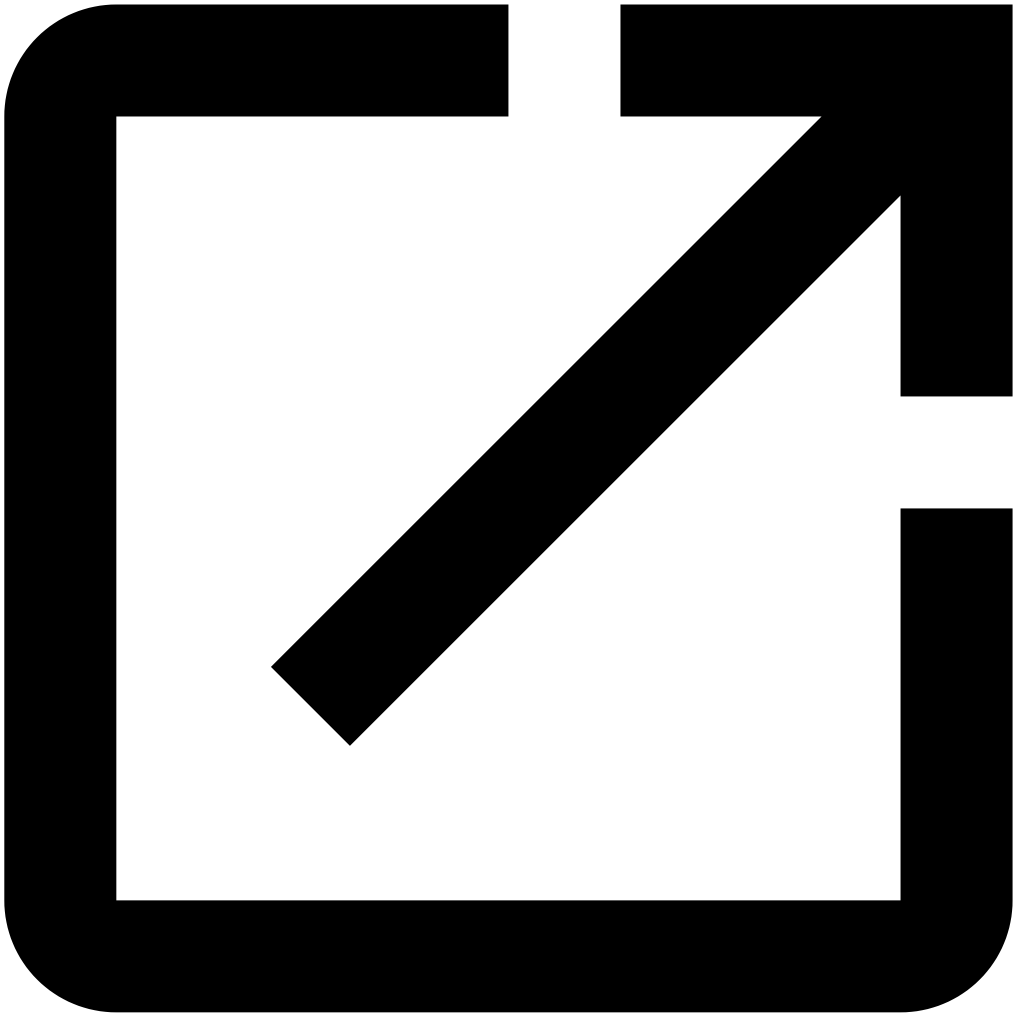


Phony Reddit site

Source: BleepingComputer

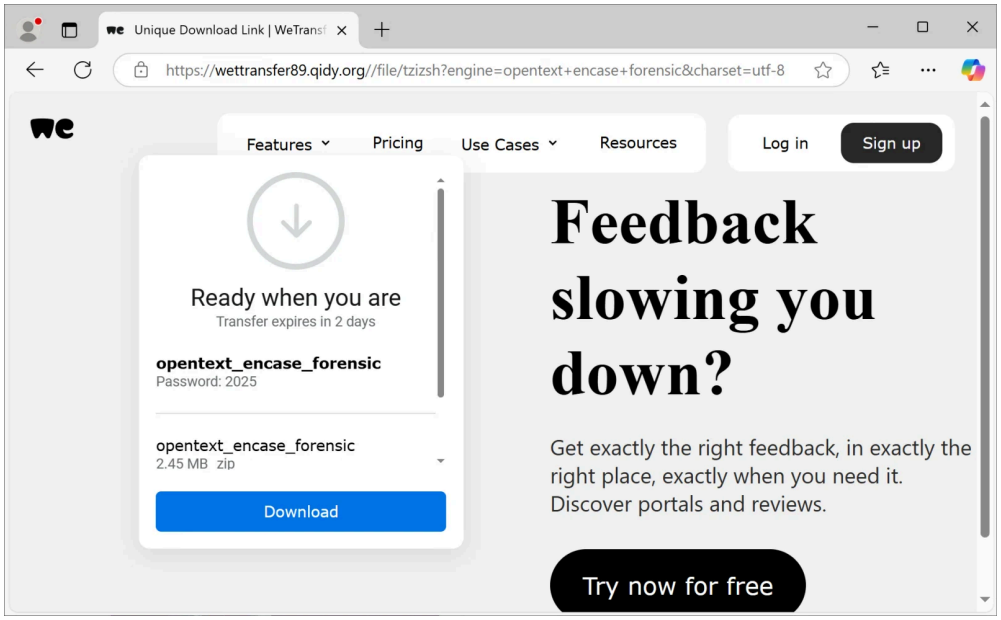
Unsuspecting victims clicking on the link are taken to a fake WeTransfer site that mimicks the interface of the popular file-sharing service. The ‘Download’ button leads to the Lumma Stealer payload hosted on “weighcobbweo[.]top.”


0:00



All sites used in this campaign contain a string of the brand they impersonate followed by random numbers and characters to appear legitimate at a quick glance. The top-level-domains are either “.org” or “.net.”

All sites part of the campaign contain a string of the brand they impersonate followed by random numbers and characters to appear legitimate at a quick glance. The top-level-domains are either “.org” or “.net.”



Fake WeTransfer portal
Source: BleepingComputer

These fake websites were found by Sekoia researcher crep1x, who shared a complete list of web pages participating in the scheme. In total, there are 529 pages impersonating Reddit and 407 posing as the official WeTransfer service serving a download.

The researcher told BleepingComputer that he was unable to retrieve any clues about the previous stages of the infection chain, but the specific topics used indicate some form of elaboration.

The attack might begin with malvertising, SEO poisoning, malicious websites, direct messages on social media, and other means.

A year ago, the same researcher discovered a similar campaign where 1,300 sites abused the AnyDesk brand to push the Vidar Stealer malware.

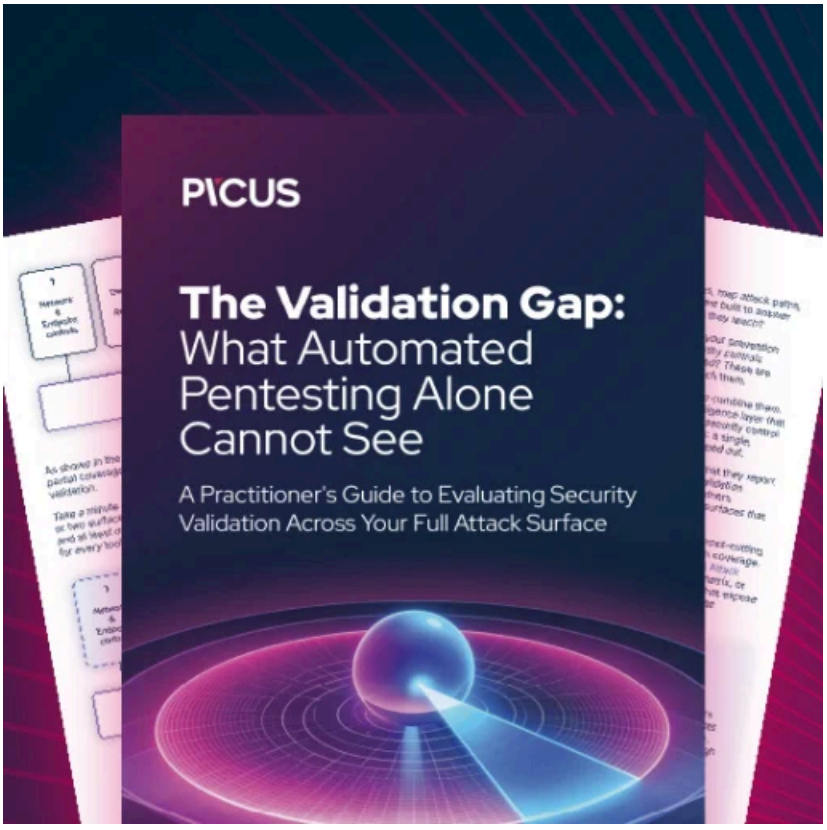
Risk of info-stealer malware

Lumma Stealer is a potent tool with advanced evasion and data theft mechanisms. The malware is sold to hackers who distribute it through various methods, including GitHub comments, deepfake nude generator sites, and malvertising.

Info-stealing malware can collect, among other things, passwords stored on web browsers and session tokens that can be used to hijack accounts without knowing the credentials.

This type of threat is commonly used to exfiltrate sensitive login data from companies and the details are usually sold on hacker forums.

Most recently, infostealers enabled high-impact attacks on PowerSchool, HotTopic, CircleCI, and Snowflake.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/hundreds-of-fake-reddit-sites-push-lumma-stealer-malware/