The Spamhaus Project (@spamhaus@infosec.exchange)

By The Spamhaus Project

Published: 2024-02-28 · Archived: 2026-04-05 13:22:18 UTC

❗Spamhaus Researchers observed a new version of "Xehook Stealer" downloaded by Smokeloader. The stealer has similarities with Agniane Stealer, another malware written by the same author.

In this case, the stealer is performing a GET request to get the following configuration (Image 1).

Based on its properties, it appears to be targeting cryptocurrency-related domains, as well as applications. This is further confirmed by the embedded configuration inside the stealer where the build ID is "cryptostage" with version "2.0.8 Stable" (Image 2).

Here is the URL and sample hash on @abuse_ch's URLHaus Database:

https://urlhaus.abuse.ch/url/2771798/
