

en_mars_stealer_technical_analysis_report.pdf

Archived: 2026-04-06 00:53:14 UTC

Sida 3 av 18

1

Preview

Mars Stealer is a powerful malware presented on Russian hacker forums. Thanks to the analyzes carried out, it has been determined that Mars Stealer is a redesigned version of the malware called Oski, which was discontinued in the middle of 2020.

Commonly, spam email, compressed file or download link is the most common distribution method. Creating a malicious website that looks like pirated software is another common method of spreading this malware.

Computers that are infected with this malware;

- Credit card information,
- Automatic filling of the browser data,
- Browser extension data,
- Crypto wallets,
- Access to crypto extension information.

Source: https://drive.google.com/file/d/14cmYxzowVLyuiS5qDGOKzgi2_vak2Fve/view