Mars Stealer Malware Analysis – ThreatMon

threatmon.io/mars-stealer-malware-analysis-threatmon/

threat2022 December 29, 2022

Skip to content

What is Mars Stealer?

Mars stealer is an improved successor of Oski Stealer, supporting stealing from current browsers and targeting crypto currencies and 2FA plugins.

Mars Stealer written in ASM/C using WinApi, weight is 95 kb. Uses special techniques to hide WinApi calls, encrypts strings, collects information in the memory, supports secure SSL-connection with C&C, doesn't use CRT, STD.Let's take a look at how it works.

Mars Stealer analysis
Tags malware malware analysis Mars Stealer StealerCategories Report