Malware Analysis: Stealer - Mutex Check, Stackstrings, IDA (Part 1)

Published: 2020-10-03 · Archived: 2026-04-05 16:58:59 UTC

Kommentarer 21

I den här videon

Kapitel

Beskrivning

Malware Analysis: Stealer - Mutex Check, Stackstrings, IDA (Part 1)

117Gilla-markeringar

5 006Visningar

20203 okt.

In this series I will be analysing a crime stealer from basics to more advanced concepts in malware analysis. Get a cup of tea and watch me slowly analyse malware :-) No sample (Sorry!) Sample:

- Build: June Build 1.1.6 (I think - the latest)

0:00:00 - Introduction 0:01:19 - Windows Defender malware analysis instructions for beginners 0:01:57 - Malwares ad text and images from forum 0:09:01 - Static Analysis PE Studio 0:12:00 - In IDA free with the packed sample 0:21:00 - In x32dbg with the packed sample 0:31:18 - Modifying binary sample for unpacked executable 0:34:11 - Unpacked sample in IDA 0:37:16 - Identifying an interesting function 0:41:25 - String analysis in unpacked sample 0:46:43 - Back in IDA to the interesting function 0:50:47 - Unpacked sample in x32dbg analysis 0:55:30 - Stack string identification in IDA 1:00:00 - Mutex analysis in x32dbg 1:03:30 - Process tokens analysis in x32dbg 1:10:00 - Debugger flow manipulation (Z flag modification) 1:14:09 - Next time Further research from Cyber Ark: https://www.cyberark.com/resources/th... Trend Micro research: https://blog.trendmicro.com/trendlabs...

Följ med i transkriptionen.

Manuskript