Malware Analysis: Stealer - XOR, CyberChef, x64Dbg Scripting (Part 2)

Published: 2020-10-18 · Archived: 2026-04-05 14:40:38 UTC

Kommentarer 4

I den här videon

Kapitel

Beskrivning

Malware Analysis: Stealer - XOR, CyberChef, x64Dbg Scripting (Part 2)

72Gilla-markeringar

2 991Visningar

202018 okt.

Part two looking at some more assembly and looking at scripting. 00:00:00 - Introduction 00:01:40 - Disassembly problems 00:03:52 - Locale XOR in IDA 00:07:45 - Debugging XOR Locale in x32dbg 00:09:45 - Endianness 00:10:54 - Dissecting the loop in x32dbg 00:19:46 - Repeated loops identification for locale in IDA 00:20:36 - Back to x32dbg on the loop 00:22:30 - Understanding the exit conditions in steaker while in IDA 00:23:15 - Using CyberChef to manually deobfuscate the loop data 00:27:00 - Back in x32dbg checking the locales protected 00:29:25- Using x32dbg for identifying XOR loops through scripting 00:42:31 - Analysing the XMM0 XOR Loop 00:47:45 - Identifying string functions and base64 decoding

Följ med i transkriptionen.

Manuskript
