Cobalt Strike Decoding and C2 Extraction - 3 Minute Malware Analysis

By @karanb2067 för 2 år sedan

Published: 2024-02-08 · Archived: 2026-04-05 18:28:36 UTC

Kommentarer 6

I den här videon

Kapitel

Beskrivning

Cobalt Strike Decoding and C2 Extraction - 3 Minute Malware Analysis

99Gilla-markeringar

2 914Visningar

20247 feb.

Decoding a Cobalt Strike shellcode loader with CyberChef and Emulation. You can obtain the sample on Malware Bazaar with SHA256:acc23a776415d931b64e95919b3372562b17a7c2717e1d530b031a6f29404b94\ 00:00 - Overview 00:13 - Base64 Identification 00:25 - GZIP Identification 00:38 - CyberChef Decoding 01:23 - XOR Decoding 01:45 - ShellCode Emulation With SpeakEasy 02:15 - Identifying C2 Address

Följ med i transkriptionen.

Embee Research

2 220 prenumeranter

Manuskript