Malware Analysis - 3CX SmoothOperator ffmpeg.dll with Binary Ninja

Published: 2023-04-03 · Archived: 2026-04-05 16:02:34 UTC

Kommentarer 25

I den här videon

Kapitel

Outro

36:45

Beskrivning

Malware Analysis - 3CX SmoothOperator ffmpeg.dll with Binary Ninja

100Gilla-markeringar

3 037Visningar

20233 apr.

We analyze the trojanized ffmpeg.dll that was used in the supply chain attack called SmoothOperator. Me mark up the decompiled code in Binary Ninja and decrypt the next stage. Malware analysis courses: https://malwareanalysis-for-hedgehogs... Buy me a coffee: https://ko-fi.com/struppigel Follow me on Twitter: _/ struppigel_ Tools: Binary Ninja: https://binary.ninja/ PortexAnalyzerGUI: https://github.com/struppigel/PortexA... Sysinternals: https://learn.microsoft.com/en-us/sys... Samples: 3CXDesktopApp.msi: https://tria.ge/230330-3nzfjshc2s ffmpeg: https://bazaar.abuse.ch/sample/7986bb... d3dcompiler_47.dll: https://bazaar.abuse.ch/sample/11be18... 00:00 Intro 00:36 Bleepingcomputer article 03:03 3CXDesktopApp.msi unpacking 03:50 Finding the malicious code 09:00 Marking up the code in Binary Ninja 19:24 Certificate parser markup 30:51 Decryption function 33:31 Unpacking code from d3dcompiler_47.dll 36:45 Outro #malware #malwareanalysis #reverseengineering #3cx #msi #unpacking #shellcode #binaryninja

Så skapades det här

Automatiskt dubbad

Ljudspår har genererats automatiskt för vissa språk. Läs mer

Kapitel

Intro

0:00

Bleepingcomputer article

0:36

3CXDesktopApp.msi unpacking

3:03

Finding the malicious code

3:50

Manuskript

Följ med i transkriptionen.

MalwareAnalysisForHedgehogs

29 500 prenumeranter

Videor

Om

Twitter

Malware Theory - Basic Structure of PE Files

av MalwareAnalysisForHedgehogs

Manuskript

Source: https://www.youtube.com/watch?v=fTX-vgSEfjk