Full malware analysis Work-Flow of AgentTesla Malware

Published: 2021-12-08 · Archived: 2026-04-05 13:00:11 UTC

Kommentarer 14

I den här videon

Kapitel

Kapitlen har genererats automatiskt

Beskrivning

Full malware analysis Work-Flow of AgentTesla Malware

185Gilla-markeringar

7 724Visningar

20217 dec.

This video is about full malware analysis Work-Flow of AgentTesla Malware. This video was created for educational purposes. Covers: Initial MS Office document abusing external references. RTF document downloaded as external referenced object - exploiting CVE-2017-11882. Shellcode reversing and analysis - part of exploitation chain. Last stage reversing - final payload - VB wrapped-packed AgentTesla. AgentTesla deobfuscation and analysis. Github Link: https://github.com/Dump-GUY/Malware-a... AnyRun Link: https://app.any.run/tasks/d124fd0d-34...

Följ med i transkriptionen.

DuMp-GuY TrIcKsTeR

5 270 prenumeranter

Manuskript
