Powershell and DnSpy tricks in .NET reversing – AgentTesla [Part1]

Published: 2021-11-22 · Archived: 2026-04-05 13:50:29 UTC

This video covers reversing path to the final payload of AgentTesla. This video was created for educational purposes. Github GUIDE (All scripts and sample to download) - Link: https://github.com/Dump-GUY/Malware-a... Content: This part covers extraction of all stages during reversing original sample and obtaining final payload. Most of the video is about advanced usage of DnSpy like in memory patching obfuscated modules for deobfuscated which got loaded runtime as next stages. I will provide simple way how one can benefit from views like Call Stack, Memory View, Modules View, Locals etc.. In memory (during runtime) replacing obfuscated next stage modules for deobfuscated ones is one of the trick which will be shown. Many tricks how one can interact with .NET assembly via Powershell will be introduced (Loading .NET assembly, Invoking methods (even private), patching methods, getting assembly field values etc..). The biggest advantage all of this is that we will have all execution process under control.
