Ryuk Ransomware - Advanced using of Scylla for Imports reconstruction

Published: 2021-03-01 · Archived: 2026-04-05 17:30:25 UTC

Kommentarer 13

I den här videon

Kapitel

Beskrivning

Ryuk Ransomware - Advanced using of Scylla for Imports reconstruction

87Gilla-markeringar

5 366Visningar

202128 feb.

This video covers Imports rebuilding using well known tool Scylla. It shows how one can use combination of tools - IDA + x64dbg + the Scylla´s not only the build in feature as IAT Autosearch (Normal vs Advanced) which in some situations like this does not work. You will learn how to use Scylla to specify memory address range of IAT where Dynamically resolved API function addresses are populated during the runtime. As an example the Ryuk Ransomware sample is used. This guide can serve also for other samples where we have to properly set the Scylla tool and not only using the default searching feature for IAT reconstruction. Links: Ryuk sample: https://app.any.run/tasks/fbe53216-85... Ryuk malware family: https://malpedia.caad.fkie.fraunhofer... Scylla tool: https://github.com/NtQuery/Scylla

Följ med i transkriptionen.

DuMp-GuY TrIcKsTeR

5 260 prenumeranter

Manuskript
