Cheatography

Remnux Malware Analysis Cheat Sheet

by Jorgen Ordonez (j3rg) via cheatography.com/191613/cs/39819/

General information

manalyze malware.exe

I mainly use this to get the compile date and time of the malware being examined

Imported & Exports Functions

manalyze *--dump=imports*

pedump *--imports*

pedump *--exports*

Headers/Sections

manalyze *--dump=sections* malware.exe

pedump *--sections* malware.exe

pedump --pe* malware.exe	--mz, --rich, and much more exist check the help

Packer

pedump *--packer-only* malware.exe

Resource

pedump *--resources** malware.exe	Use to check the resources in the malware
pedump malware.exe *--extract resource:0x4060** > extracted_resource	where 0x4060 offset of resource and extracted_resource is itself extracted from the malware.

Exports

manalyze *--dump=exports* malware.dll

pedump *--exports* malware.dll

By **Jorgen Ordonez** (j3rg)
cheatography.com/j3rg/

Not published yet.
Last updated 5th June, 2024.