IRC Botnet Reverse Engineering Part 1 - Preparing Binary for Analysis in IDA PRO

By @OALABS @OALABS

Published: 2020-05-31 · Archived: 2026-04-05 14:36:37 UTC

The first part of our in-depth malware reverse engineering series analyzing an IRC worm from 2010. In this part we use IDA Pro and Python to decrypt the strings and resolved the dynamic imports to prepare the binary for analysis.... ----- OALABS DISCORD _ / discord _ OALABS PATREON _ / oalabs _ OALABS TIP JAR https://ko-fi.com/oalabs OALABS GITHUB https://github.com/OALabs UNPACME - AUTOMATED MALWARE UNPACKING https://www.unpac.me/#/ ----- Automated Malware Unpacking https://www.unpac.me/ Unpacked binary (malshare) https://malshare.com/sample.php?actio... SHA256 hash: 4eb33ce768def8f7db79ef935aabf1c712f78974237e96889e1be3ced0d7e619 IDA Pro string decryption script https://gist.github.com/herrcore/72b0... Hex Copy IDA plugin for fast data copy-paste https://gist.github.com/herrcore/0176... In-depth string decryption and import resolving video series with REvil ransomware: _ • REvil Ransomware Unpacked - Cheeky Hack To... _ MalwareAnalysisForHedgehogs - Network Worm Basics _ • Malware Theory - Network Worm Basics _ Feedback, questions, and suggestions are always welcome :) Sergei _ / herrcore _ Sean _ / seanmw _ As always check out our tools, tutorials, and more content over at https://www.openanalysis.net #IDAPro #Botnet #MalwareAnalysis

---