Reverse Engineering Warzone RAT - Part 1

Published: 2021-05-19 · Archived: 2026-04-05 13:15:17 UTC

Join us as we reverse engineer Warzone Rat! Expand for more details.... ----- 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/#/ ---- Chapters: 0:00 Introduction 4:25 Setting Up IDA 6:15 How to Force hex-rays to Decompile All Functions 7:42 Methodology for Identifying an Embedded Configuration File 9:16 C++ Reversing Basics 18:53 Adding a Struct in IDA 22:10 Fixing Incorrect Struct Size 26:39 Quickly Reversing Functionality 28:42 Reverse Engineering With Structs 32:04 Malware Trick Used to Locate Address in Memory 36:43 Walking a PE File Using Pointers 41:21 Creating and Importing IDC Files Automated unpacking: https://www.unpac.me/#/ Unpacked sample https://malshare.com/sample.php?actio... IDC script (download don't copy paste): https://gist.github.com/herrcore/ccf4... The following tutorials may help with some of the basic concepts presented in this video. C++ Reversing Basics _ • Reverse Engineering C++ Malware With IDA Pro _ IDA Pro Microcode and x86 Calling Conventions _ • IDA Pro Decompiler Basics Microcode and x8... _ RC4 Crypto _ • Reverse Engineering RC4 Crypto For Malware... _ 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 #ReverseEngineering #Malware #WarZoneRat

---

Source: https://www.youtube.com/watch?v=81fdvmGmRvM