Unpacking Gootkit Malware With IDA Pro and X64dbg - Subscriber Request

Published: 2018-03-04 · Archived: 2026-04-05 18:24:23 UTC

Open Analysis Live! We use IDA Pro and x64dbg to unpack a recently packed Gootkit malware (stage1). This was a subscriber request asking us to determine how this was packed. Video bookmarks to skip ahead... ----- 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/#/ -----

- Deobfuscating strings with IDA Python 5:15
- Identify anti-analysis tricks after string deobfuscation 9:03
- Mutex trick 14:40
- CreateFile ShareMode trick 17:33
- Fully unpacking with x64dbg 20:25
- Searching for PE in memory using x64dbg 23:24
- Carving PE files from a memory dump with a hex editor 26:24
- Final overview of the whole process 27:59

Packed sample: Sha256: 38933984f5ff8b71c054d1c1155e308ac02377b89315ef17cea859178a30dbab https://malshare.com/sample.php?actio... Unpacked Gootkit (stage 1): Sha256: e61082d8f711d775b5c427af649c64ab50fac695f334720dca467598c5817b7a https://malshare.com/sample.php?actio... x64dbg: https://x64dbg.com/#start IDA: https://www.hex-rays.com/products/ida... Packer string decryption script (IDAPython): https://gist.github.com/herrcore/4731... Tutorial examining the CreateFile share anti-analysis trick: _ • Unpacking Process Injection Malware With I... _ Feedback, questions, and suggestions are always welcome :) Sergei _ / herrcore _ Sean _ / seanmw _ As always check out our tools, tutorials, and more content over at http://www.openanalysis.net

---