Investigating NullMixer - Identifying Initial Packing Techniques

Published: 2023-01-31 · Archived: 2026-04-05 18:39:22 UTC

UPDATED: This will now be part of a three video series :) This video will be the first of a three part series in which we take a look at unraveling the basics of how NullMixer works. In the first video, we'll explore the initial layers of how NullMixer is delivered, which includes NullSoft Self-Extracting installer and 7zip self-extracting archives. We'll use tools such as Detect-It-Easy and simply 7z commands to unravel the first stages. By the end of this video, we'll identify the main payloads and the binary responsible for executing them. Cybersecurity, reverse engineering, malware analysis and ethical hacking content! 🎓 Courses on Pluralsight 👉 https://www.pluralsight.com/authors/j... 🌶️ YouTube 👉 Like, Comment & Subscribe! 🙏 Support my work 👉 _/joshstroschein_ 🌎 Follow me 👉 _/jstrosch_, _/joshstroschein_ ⚙️ Tinker with me on Github 👉 https://github.com/jstrosch Tools used: REMnux, Detect-it-Easy, 7-zip, terminal. Sample SHA256: 7a4df2fc82c0b553d0b703f51635fd62cf02553706f942c66d752c1d8fae207b 00:00 Introduction 00:39 Viewing our Sample on Triage Sandbox 01:57 Open-Source Reporting 04:33 Investigating Process Activity 05:49 Investigating the Binary with Detect-It-Easy 07:48 Overlays in PE Files 09:25 Finding the Payloads! 12:51 Detecting More Packing

---