Fast API resolving of REvil Ransomware related to Kaseya attack

Published: 2021-07-14 · Archived: 2026-04-05 18:05:28 UTC

This sample of REvil Ransomware is performing dynamically resolving of API functions via API name hashing. In this video I will show you 4 fast methods how you can do the API resolving of REvil Ransomware related to Kaseya attack. 3 methods are for IDAPro (renimp.idc + memsnapshot, Universal Unpacker Manual Reconstruct, Pe-Tree) and last 1 method (x64dbg + Scylla plugin) REvil Ransomware sample: https://tria.ge/210703-cggr9ffskx https://bazaar.abuse.ch/sample/9b1171...

Så skapades det här

Automatiskt dubbad

Ljudspår har genererats automatiskt för vissa språk. Läs mer
