Tag 4: Ransomware 💖 API Hashing

- Malware Spotlight
- String Obfuscation
- API Hashing

String Obfuscation

- Reminder: RC4
- Automatisierung ist out of scope
- Cyberchef Rezept / BinRef Pipeline

API Hashing

- Dynamic API Resolution
- Hashing
- Sieht schlimm aus, ist es aber nicht
- API Hashing kann man leicht erkennen

Demo: Netwalker

Indizien für API Hashing

- Aufrufsignatur: Komische Konstante
- Rückgabewert wird aufgerufen
- Fieses PE Parsing (Piraten-Style)
- Wenig Imports

Aufgabe 9

https://mal.re/tmp/classes/hsbund-2025/aufgabe9.md