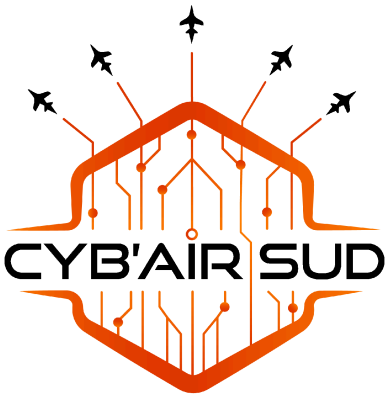


Malware Analysis with r2ai and MCP

Abstract for CFP 2025

Speaker: Axelle APVRILLE

Short Description

Using AI to decompile a recent 2025 malware sample.

Keywords

Radare2, r2ai, MCP, AI, assembler, malware

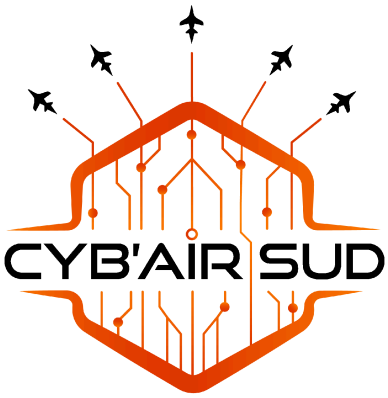
Detailed Abstract

Disassembly and decompilation are at the core of any static malware analysis. In an ideal scenario, an anti-virus analyst would dream of having clean, easy-to-understand source code. In reality, assembly remains painful to read, and even the best professional decompilers produce messy code (bad names, misinterpreted loops, scattered gotos...). Analysts often end up trying to understand "C-like assembly" (with errors, too).

In this presentation, we will analyze a recent 2025 malware. We enhance Radare2 with an AI plugin and an MCP server. The produced code is easy to read and understand, which is the undeniable advantage of AI. It is not perfect, however: while suitable for a "general" view, AI often mislabels details. We will learn how to detect such situations.

Additional Information

- Language: French
- TLP Classification: CLEAR
- Recording: yes



Analyse de malware avec r2ai et MCP

Résumé pour CFP 2025

Intervenant : Axelle APVRILLE

Description concise

Utiliser l'IA pour décompiler un malware récent de 2025.

Mots-clés

Radare2, r2ai, MCP, IA, assembleur, malware

Résumé détaillé

Le désassemblage et la décompilation sont le coeur de toute analyse statique de malware. Dans un scénario idéal, un analyste anti-virus rêverait de disposer d'un code source propre et facile à comprendre. En réalité, l'assembleur reste pénible à lire, et même les meilleurs décompileurs professionnels livrent du code sale (mauvais noms, boucles mal interprétées, goto dispersés...). On se retrouve souvent à tenter de comprendre "de l'assembleur écrit en C" (avec des erreurs de surcroit).

Dans cette présentation, nous allons analyser un malware récent de 2025. Nous agrémentons Radare2 d'un plugin pour l'intelligence artificielle et d'un serveur MCP. Le code produit est facile à relire et à comprendre, c'est l'atout indéniable de l'IA. Tout n'est pas parfait cependant : parfaite pour une vue "générale", l'IA se trompe souvent dans ce qu'elle qualifie de "détail". Nous apprendrons à détecter ces situations.

Autres informations

- Langue : fr
- Classification TLP : CLEAR
- Enregistrement : oui