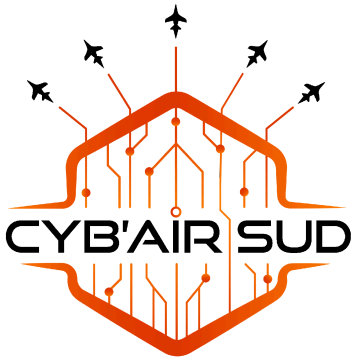


Malware Analysis through AI

CFP 2025 — English Version

Speaker: Gledis Shkurti

Classification and dissemination

TLP: **GREEN**.

Presentation language: **French**. Recording and redistribution: **Allowed**.

Title

Malware Analysis through AI

Presentation Objective

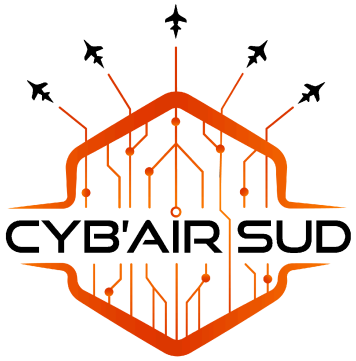
To show how artificial intelligence — and in particular ChatGPT — can support analysts in understanding and deobfuscating malware. The goal is to highlight the practical benefits of these tools within the analysis process while emphasizing their limitations and the precautions required for their responsible use.

Abstract

Malware analysis remains a demanding discipline, especially when facing code intentionally obfuscated to hide its true purpose. This presentation begins with a brief overview of reverse engineering fundamentals and common obfuscation techniques, before explaining why AI is becoming a valuable ally for saving time and improving code readability.

Through practical examples, ChatGPT will be presented as a support tool that can help clarify obfuscated code, suggest possible behavioral interpretations, and generate concise summaries from raw analysis outputs. The session will also address the limitations of this approach — analytical errors, incomplete or overly generic answers — and the ongoing need to validate results through traditional reverse engineering methods.

Finally, the talk will open a reflection on the potential misuse of such technologies, as some actors may repurpose them to automate the generation and obfuscation of malicious code.



L'analyse malware via l'IA

CFP 2025 — Version Française

Intervenante : Gledis Shkurti

Classification et diffusion

TLP : **VERTE**.

Langue de présentation : **Français**. Enregistrement et rediffusion : **Autorisés**.

Titre de la conférence

L'analyse malware via l'IA

Objectif de la présentation

Présenter comment l'intelligence artificielle, et en particulier ChatGPT, peut soutenir les analystes dans la compréhension et la déobfuscation de malwares. L'objectif est de montrer les apports concrets de ces outils dans le processus d'analyse tout en soulignant leurs limites et les précautions nécessaires à leur utilisation.

Résumé

L'analyse de malware reste un exercice exigeant, surtout face à des codes volontairement obfusqués pour masquer leurs fonctions. Cette présentation revient d'abord sur les principes de base du reverse engineering et sur les techniques d'obfuscation les plus fréquentes, avant d'expliquer pourquoi l'IA devient un atout pour gagner du temps et améliorer la lisibilité du code.

À travers des exemples d'utilisation, ChatGPT sera présenté comme un outil d'appui à l'analyse qui peut contribuer à rendre plus lisible un code obfusqué, suggérer des pistes d'interprétation, ou encore générer des synthèses claires à partir de résultats bruts d'analyse.

La présentation abordera aussi les limites de cette approche : erreurs d'analyse, réponses incomplètes ou trop générales, et nécessité de toujours valider les résultats par des méthodes classiques de reverse engineering.

Enfin, une réflexion sera ouverte sur le risque d'usage malveillant de ces mêmes outils, certains acteurs pouvant les détourner pour automatiser la génération et l'obfuscation de code malveillant.