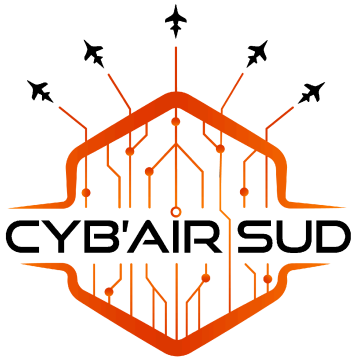


Malware Operations Under the Microscope: From Binary Artifacts to Strategic Insights

CFP 2025 — English Version

Speaker: Ricardo Rodriguez

Abstract

Malware analysis has traditionally focused on reverse engineering binaries and studying their behavior in isolated environments. However, modern threats demand a broader perspective: malware is no longer just code, but part of an industrialized operation that combines engineering, economics, and social dynamics.

This talk will explore malware analysis from a multi-layered perspective:

— **Technical layer:** How we extract, analyze, and interpret binary artifacts, memory traces, and behavioral data using formal methods, sandboxes, and similarity detection techniques.

— **Operational layer:** Understanding how malware families evolve, reuse code, and adapt to evade defenses. Case studies on malware grouping and classification highlight attackers' tactics.

— **Strategic layer:** How technical findings are incorporated into incident response, attribution, and long-term resilience strategies.

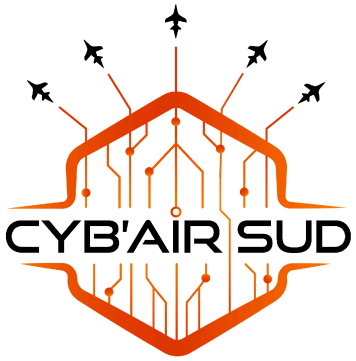
By connecting these layers, the presentation will highlight how malware analysis can go beyond code analysis to provide actionable intelligence for defenders, decision-makers, and organizations.

Audience Takeaways

— A clear overview of how malware analysis integrates into incident response and cyber defense workflows.

— Real-world examples of analytical methods that go beyond static or dynamic analysis.

— Insights into the challenges and opportunities of applying AI and formal techniques to clustering and malware family classification.



Opérations Malware sous le Microscope : des Artéfacts Binaires aux Insights Stratégiques

CFP 2025 — Version Française

Intervenant : Ricardo Rodriguez

Résumé

L'analyse de malware a traditionnellement été centrée sur la rétro-ingénierie des binaires et l'étude de leur comportement dans des environnements isolés. Cependant, les menaces modernes nécessitent une perspective plus large : le malware n'est plus seulement du code, mais fait partie d'une opération industrialisée combinant ingénierie, économie et dynamique sociale.

Cette présentation explorera l'analyse de malware selon une perspective multi-couches :

- **Couche technique :** Comment nous extrayons, analysons et interprétons les artéfacts binaires, traces mémoire et données comportementales à l'aide de méthodes formelles, sandbox et techniques de détection de similarité.
- **Couche opérationnelle :** Comprendre comment les familles de malware évoluent, réutilisent du code et s'adaptent pour échapper aux défenses. Des études de cas sur le regroupement et la classification des malware illustreront les tactiques des attaquants.
- **Couche stratégique :** Comment les résultats techniques sont intégrés dans la réponse aux incidents, l'attribution et les stratégies de résilience à long terme.

En connectant ces couches, la présentation montrera comment l'analyse de malware peut dépasser la simple analyse de code pour fournir des renseignements exploitables aux défenseurs, décideurs et organisations.

Points clés pour le public

- Une vue claire de l'intégration de l'analyse de malware dans les workflows de réponse aux incidents et de défense cyber.
- Des exemples concrets de méthodes analytiques allant au-delà de l'analyse statique ou dynamique.

— Des perspectives sur les défis et opportunités de l'application de l'IA et des techniques formelles pour le clustering et la classification des familles de malware.