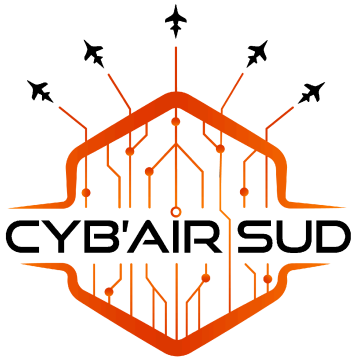


Dynamic Analysis of Malware in the Light of Evasion: Platform, Sandboxes, and Limitations

CFP 2025 — English Version

Speaker: Dorian Bachelot

Duration

30 minutes

Short Description

In an ecosystem where evasion, obfuscation, and anti-analysis are becoming the norm, dynamic malware analysis techniques are being challenged, while remaining reliable and robust alternatives to static analysis. This talk will first present a new malware processing and storage platform for the academic world, called *ShareMal*, and then introduce the various methods and tools for dynamic analysis. Finally it will address the challenges related to evasion, and the solutions being studied for the ShareMal platform.

Detailed Description

The presentation is structured around three main themes: the academic malware processing and storage platform called *ShareMal*, the context and challenges of dynamic analysis, and finally, the possible solutions to these issues. The talk is intended for a technical audience, though not necessarily expert in the field.

First, the context surrounding the creation of the ShareMal platform will be presented, as well as the actors involved: the High Security Laboratory (LHS) in Rennes and the DefMal project under the French PEPR Cybersecurity program. The talk will discuss the specificities of academic research for malware processing and storage, and how they differ from industrial use cases. This will help justify the ShareMal platform's relevance and functionalities. A short demonstration will illustrate its main functionalities. For reference, ShareMal is a non-profit, free service provided by the Rennes' LHS for the academic community, as part of the DefMal project.

Then, the talk will move from ShareMal's dynamic analysis services to a broader overview of other available tools and approaches, as well as their limitations. It will describe different methods for performing dynamic analysis of executable binaries, and from the perspective of evasion and obfuscation, will highlight the limitations of most existing approaches and tools.

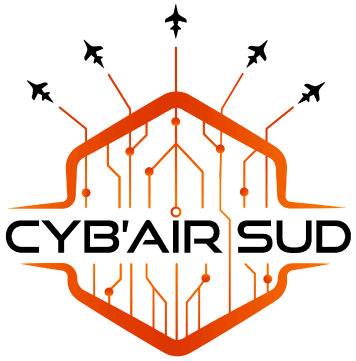
Finally, the solutions being explored to address these issues will be discussed, as well as LHS's ongoing work to integrate them into the ShareMal platform. The data format used by the main sandboxes in the literature will be examined , as well as their limitations in detecting and circumventing evasion methods.

Other Information

— Language: French
— TLP: RED
— Recording / Redistribution: No

About the Speaker

Dorian Bachelot is a Research Engineer within the PIRAT\'); Team at CentraleSupélec, working on malware analysis and cybersecurity research. He contributes to the development of academic infrastructures for malware collection, analysis, and sharing — notably through the DefMal project and the High Security Laboratory (LHS) in Rennes. His research interests include malware dynamic analysis, offensive security automation and advanced evasion techniques.



Analyse dynamique des logiciels malveillants à l'épreuve de l'évasion : plateforme, bacs à sable et limites

CFP 2025 — Version Française

Intervenant : Dorian Bachelot

Durée

30 minutes

Description concise

Dans un écosystème où l'évasion, l'obfuscation et l'anti-analyse deviennent la norme, les techniques d'analyse dynamique des logiciels malveillants sont mises à l'épreuve, tout en restant des alternatives fiables et robustes face à l'analyse statique. Cette conférence commencera par présenter une nouvelle plateforme de traitement et stockage de maliciel pour le monde académique, nommée *ShareMal*, puis introduira les différentes méthodes et solutions permettant de mener une analyse dynamique. Les difficultés liées à l'évasion et les solutions étudiées pour la plateforme ShareMal seront ensuite abordées.

Résumé détaillé

La conférence s'articule autour de trois axes : la plateforme académique de traitement et stockage de logiciels malveillants nommée *ShareMal*, la présentation du contexte et des défis de l'analyse dynamique, et enfin les possibles solutions à ces problématiques. Celle-ci devrait être accessible à un public technique, mais non expert du domaine.

Dans un premier temps, le contexte autour de la création de la plateforme ShareMal sera présenté, ainsi que les acteurs impliqués : le LHS (Laboratoire Haute Sécurité) de Rennes et le projet DefMal (projet du PEPR Cybersécurité). Il sera question des spécificités de la recherche académique pour le traitement et le stockage de maliciel, et des différences avec les usages industriels. Cela permettra de justifier l'intérêt et les fonctionnalités de la plateforme ShareMal. Enfin, une courte démonstration sera présentée pour énumérer les grandes fonctionnalités de la plateforme. Pour référence, ShareMal n'a aucun objectif lucratif et constitue

un service gratuit offert par le LHS de Rennes au monde académique, dans le cadre du projet DefMal.

Ensuite, la conférence rebondira depuis les offres de services d'analyse dynamique de la plateforme ShareMal vers les autres outils et approches disponibles ainsi que leurs limites. Il sera en particulier décrit les différentes méthodes permettant d'effectuer une analyse dynamique de binaire exécutable, puis, par le prisme de l'évasion et de l'obfuscation, les limites de la plupart des approches et outils existants seront mis en évidence.

Enfin, seront abordées les solutions étudiées pour faire face à ces problématiques, et les travaux du LHS en cours pour les implémenter dans la plateforme ShareMal. Le format de données utilisé par les principaux bacs à sable de la littérature sera notamment examiné , ainsi que leurs limites pour repérer et contourner des méthodes d'évasion.

Autres informations

— Langue : Français
— TLP : RED
— Enregistrement / Rediffusion : Non

À propos de l'intervenant

Dorian Bachelot est ingénieur de recherche au sein de l'équipe PIRAT de CentraleSupélec, spécialisé dans l'analyse de logiciels malveillants et la cybersécurité. Il participe au développement d'infrastructures académiques dédiées à la collecte, l'analyse et le partage de maliciels, notamment dans le cadre du projet DefMal et du Laboratoire Haute Sécurité (LHS) de Rennes. Ses travaux portent principalement sur l'analyse dynamique des logiciels malveillants, l'automatisation de la sécurité offensive et les techniques d'évasion avancées.