RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

cea cnrs Inria

FRANCE 2030 PROGRAMME DE RECHERCHE CYBERSÉCURITÉ

Défense contre les programmes malveillants
DefMal – 22-PECY-0007

Revue ANR Année 3 (T0 – T0 + 36), Juin 2025

Jean-Yves MARION

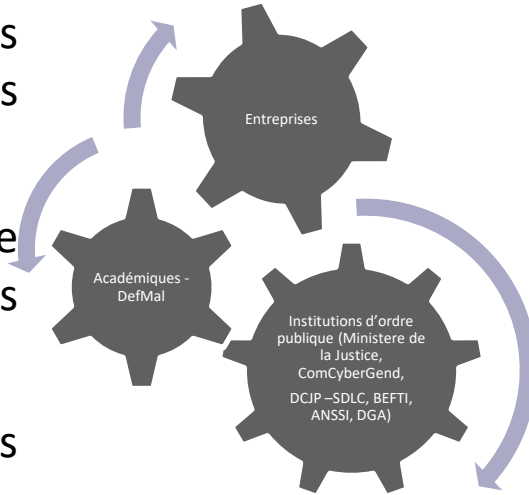
UNIVERSITÉ DE LORRAINE

anr agence nationale de la recherche

Une approche systémique de la lutte contre les programmes malveillants

Création d'une communauté interdisciplinaire, alliant acteurs de la recherche, industriels et étatiques pour améliorer la lutte contre les programmes malveillants et mieux comprendre les questions de recherche des partenaires;

- Création de la première plateforme sécurisée ouverte à la communauté d'analyse de programmes malveillants;
- Faire émerger de nouvelles technologies et des startups de lutte contre les logiciels.



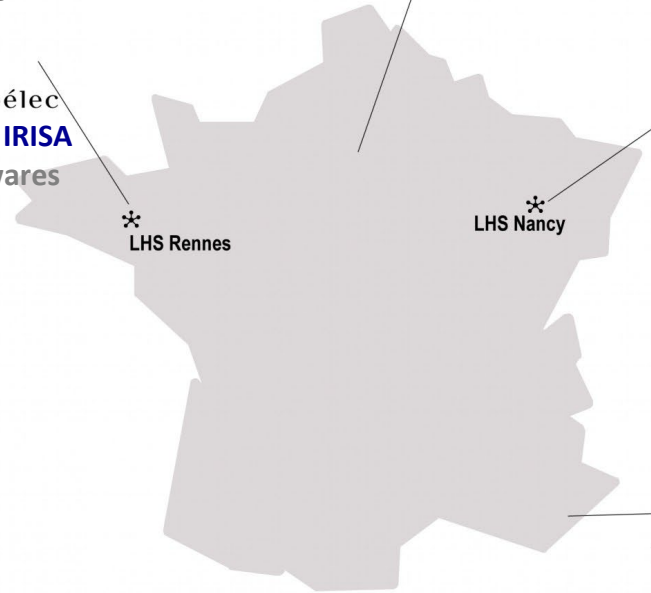
Cinq établissements partenaires

Dylan Marinho (SU)
NGUYEN Nga (Vinci)

Tayssir Touili, IRIF
Intégrante des WP1, WP5 et WP6

Sébastien BARDIN, CEA-List
WP2: Compréhension (et aide à a rétro-ingénierie)

Valérie Viet Triem Tong, IRISA
WP3: Détection de malwares



Jean-Yves MARION, LORIA
WP0: Gestion du projet;
WP1: Évaluation, méthodologie et jeux de tests;
WP5: Écosystème du malware;
WP6: Plateforme de partage de données et outils.

Simone AONZO, Security Group
WP4: Analyse forensique (et Attribution)

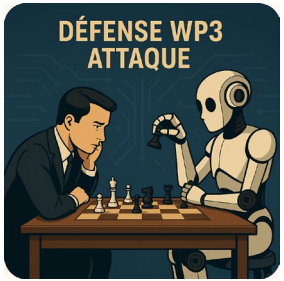
Android, IOS

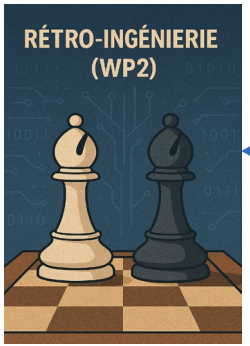
Windows, Linux MacOS

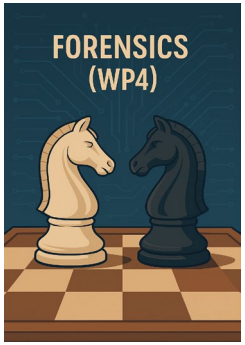
Firmware, IOT

Une approche **systémique** de la lutte contre les malwares

DefMal







Écosystème des malwares
WP5

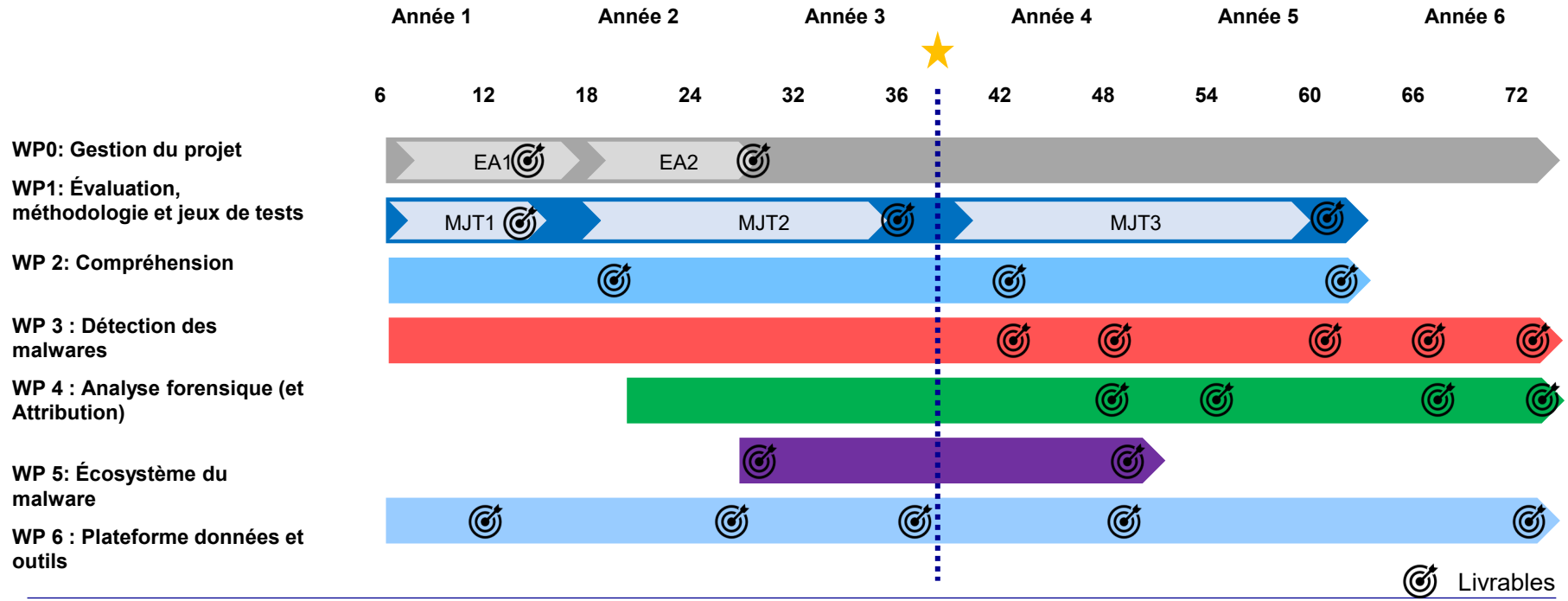
Plateforme de données et outils
WP1, WP6

WP0 - Organisation et Pilotage

- Direction : Gestionnaire de projet (50%) et Resp. du projet
  - *Suivi des livrables*
  - *Animation de la communauté DefMal*
  - *Organisation d'évènements,*
  - *Relations avec les partenaires : état et entreprises*
- Bureau composé par les responsables scientifiques de chaque site qui se réunit tous les mois

- Site web, listes de diffusion et espace partagé
- Au moins 2 évènements importants par an
- Une plateforme (@LHS) de partage des codes malveillants et outils
- Séminaires internes/externes en visio : Une fois par mois
- Newsletter vers les partenaires (2x/an) – 255 abonnées -
- Posts LinkedIn

État d'avancement du projet – Résultats obtenus



Quelques beaux résultats de cette année

- BreizhCTF et CHE (WP1)

Rétro-ingénierie

- Xyntia (WP2)

Defense/Attaque

- Protection des détecteurs de malware contre les attaques adversariale (WP3)
- Construction d'exemples adverses (WP3)
- Chaine d'attaque (Junalco) complète (WP3)
- Model Checking et détection (WP3)

Ecosystème

- Journée écosystème
- Projet EU Ensemble
- Appropriation de l'IA

Plateforme

- Droidungeon
- PoneyPot
- GoaTracer/Baguette
- Darkforums

Effet levier

- 2 start-up
- 8 projets financés dont 1 PC ERC !
- Advisory Group Research (EC3) Europol

Et la suite ?

https://anr.hal.science/search/index/?q=*&anrProjectReference_s=ANR-22-PECY-0007

Citez DefMal dans les publications

Travaux à Sophia-Antipolis

Thursday, June 5
From 08h30: Welcome coffee
9h00 - 9h20: Workshop introduction by Jean-Yves Marion, Scientific Responsible for the DefMal
9h20 - 9h40: Aurélien Francillon (Eurecom), PEPR Cybersecurité : **REV project presentation**
9h40-10h10: Géraud Canet (CEA) - **French PEPR Cybersécurité ecosystem**
10h10 - 11h00: Invited speaker - Juan Caballero (IMDEA Software Institute) - **Cryptocurrency and Blockchain Abuse by Malware**
11h00 - 11h30: Coffee break
11h30 - 12h20: Invited speaker - Luca Demetrio (University of Genoa) - **Pick Two: Robustness, Accuracy, Generalization in Malware Detection with AI**
12h30 - 14h00: Lunch time
14h00-14h30: François Teyssier et Michel Mauny (INRIA) - **PTCC**
14h30-15h00: Gregoire Menguy (CEA List) **Binsec: A Reverse Engineering Point of View**
15h00-16h00: Focus on DefMal Platforms – presentations, demo, discussion.
-Threat Nemesis – 15 minutes
-Poneypot - 15 minutes
-GoatTracer - 15 minutes
15 minutes pour les discussions
16h00-16h30: Coffee break
16h30-17h00: Dataset Brainstorming Session: Listing and Mapping Resources
-Une présentation avec Jean-François Lalande - sur les données que nous avons.
17h30-18h00: Bureau DefMal
19h00: Dinner together at L'Esterel (https://www.esterel-plage-restaurant-juan-les-pins.com/)

Friday, June 6

From 08h30- Welcome coffee

9h00 - 9h50: Invited speaker - Juan Tapiador, Universidad Carlos III de Madrid, **The Threat Actor Naming Mess**

09h50-10h10: Vincent Raulin (CentraleSupélec/IRISA) - **Learning and Using Expert Knowledge with Machine Learning: CROISSANT**

10h10-10h40: Charles-Henry Bertrand Van Ouytsel (Université catholique de Louvain) - **Static, Dynamic, Symbolic: Exploring Binary Representations for machine learning classification**

10h40-11h00: Coffee break

11h00-11h30: Sébastien Killian (CentraleSupelec/IRISA) - **A Deep Dive into Offensive Security Datasets: Examples and Methodology**

11h30 - 12h00: Yufei Han (INRIA/IRISA) - **Does Code LM really understand Code**

12h00-12h30: Sébastien Larinier (Université de Lorraine, LORIA) - **Dive in stalkerware ecosystem**

12h30 - 14h00: Lunch break

14h00 - 14h30: Olzhas Zhangeldinov (CNRS/IRIF) - **LTL model-checking for Concurrent Self-modifying Malware Detection** (visio)

14h30 - 15h00: Leo Bertrand, (Université de Lorraine, LORIA) - **The Use of LLMs to Automate Cyberattacks**

15h00 - 15h30: Jean-Marie Mineau (CentraleSupelec/IRISA) - **Android of Theseus: Patching applications to improve analysis**

15h30 - 15h50: Coffee break

15h50 - 16h20: Shijie Lin (CNRS/IRIF) **Reachability Analysis of Upper-Stack manipulating Binary code** (visio)

16h30 : Conclusions