Dépêche n° 701738
Sécurité globale - Sécurité publique
Par: Romain Haillard - Publiée le 30/10/2023 à 15h55
Lien dépêche

4 min de lecture

A usage unique de : **Service CLIENTS**

# Avec DefMal, la recherche contre les logiciels malveillants veut "sortir du laboratoire" et aider les forces de l'ordre

"L'objectif de DefMal est de comprendre l'écosystème des cybercriminels et de lutter contre", résume Jean-Yves Marion, qui a été directeur du Loria (Laboratoire lorrain de recherche en informatique et ses applications) pendant dix ans. À l'occasion des assises universitaires du droit et de la cybersécurité à Nancy, le professeur a mis en avant ce projet financé par l'État à hauteur de 5 millions d'euros sur six ans. Le programme ne fera pas seulement de la recherche fondamentale mais aspire à créer des outils pour et avec ses partenaires, dont la SDLC, le Comcybergend, l'OCLCTIC, la BL2C.

Sur l'une des vitres du LHS (laboratoire de haute sécurité) du Loria, des post-it forment un rond jaune fendu d'une grande bouche poursuivant un fantôme, une référence à Pac Man, célèbre jeu d'arcade. Le DefMal, pour Defence against Malware (défense contre les logiciels malveillants), tout jeune programme de recherche de cette unité mixte (CNRS, Inria, et université de Lorraine), a le même objectif : poursuivre les logiciels malveillants. La dizaine de chercheurs affiliée au programme, un nombre appelé à doubler d'ici 12 à 18 mois, va orienter ses recherches vers une meilleure compréhension de l'écosystème de la cybercriminalité.

## 5 millions d'euros

Les recherches ne mobiliseront pas seulement des informaticiens, mais également des juristes, des sociologues et des économistes. "Il faut étudier le recrutement au sein des groupes d'affiliés cybercriminels, le suivi des cryptoactifs et des circuits de blanchiment", explique Jean-Yves Marion, professeur à l'université de Lorraine et responsable du programme. "L'idée, c'est ensuite de pouvoir anticiper leurs prochains mouvements à partir de signaux faibles."

Le programme de recherche commence ses travaux après avoir obtenu en 2022 un financement de 5 millions d'euros étalés sur six ans avec le plan d'investissement de l'État France 2030. "C'est beaucoup pour de la recherche en informatique", souligne celui qui a dirigé le laboratoire de 2013 à 2023. Il souligne le caractère exceptionnel de ce financement : "Il y a dix ans, peu d'universitaires et de chercheurs français travaillaient sur la cybersécurité et ils étaient très peu visibles." Le programme DefMal va également candidater pour un financement européen du fonds Horizon Europe Framework Programme, dont une partie soutient les projets pour lutter contre les cybermenaces.

## De nombreuses institutions policières partenaires

Parmi les partenaires de DefMal figurent la SDLC (sous-direction de la lutte contre la cybercriminalité de la DNPJ), le Comcybergend, l'OCLCTIC, la BL2C (brigade de lutte contre la cybercriminalité de la Préfecture de police), la SDAEF (sous-direction des affaires économiques et financières de la Préfecture de olice) et la DRPJ. "Nous avons discuté avec les forces de l'ordre et la justice pour orienter les bonnes questions de recherche", rapporte l'expert en informatique, désireux d'avoir des débouchés opérationnels pour son programme. De ces discussions ont découlé de grandes orientations du programme : "Nous voulons travailler sur le Forensic, c'est-à-dire l'analyse post-mortem d'une cyberattaque. L'idée est de savoir ce qu'il s'est passé, quelles données ont été altérées ou exfiltrées, reconnaître le mode opératoire d'attaque de groupes déjà existants pour éventuellement faire de l'attribution."

Les gendarmes seraient particulièrement intéressés par l'étude des objets connectés, sur laquelle elle travaille déjà (lire sur AEF info). "À partir d'un produit, étudier ses fonctionnalités, connaître s'il existe aussi des fonctionnalités cachées et d'éventuelles portes dérobées", développe l'universitaire. L'une des parties du programme pourrait basculer vers un volet plus offensif, "avec beaucoup de réserves", précise Jean-Yves Marion. "Faire de la recherche du côté du hacking éthique, pour envisager des ripostes après attaque ou pour des applications en infiltration dans le cadre d'enquête : cette question scientifique est plus excitante, parce qu'il y a un réel changement de posture par rapport à une culture très défensive."

## Une analyse morphologique des logiciels

Le programme ne va pas se limiter à des publications scientifiques. "Développer des outils fait partie de notre feuille de route. Nous ferons aussi des prototypes pour les mettre à disposition de nos partenaires", précise Jean-Yves Marion. L'expression revient souvent, les scientifiques du Loria veulent "sortir du laboratoire". À ce titre, Cyber-detect fait figure d'exemple. Cette start-up et son outil Gorille sortent tout droit des travaux du laboratoire lorrain. Régis Lhoste, passé lui aussi par le LHS, a fondé cette entreprise en 2017 après dix années de recherche. Il exploite ses travaux sur l'analyse morphologique des logiciels malveillants et va aussi les mettre au service du programme DefMal.

Cette analyse issue du Loria permet de reconnaître les logiciels malveillants par leur composition. "De plus en plus, les attaques deviennent sophistiquées et les logiciels malveillants sont fabriqués spécialement pour une attaque", explique le cofondateur de Cyber-detect. Parce que ces logiciels sont confectionnés et donc considérés comme nouveaux, ils passent plus facilement sous les radars des antivirus ou EDR (Endpoint Detection and Response), les outils classiques de détection de menaces.

"Contrairement aux EDR, nous ne nous intéressons pas à la forme complète d'un exécutable, mais aux morceaux de codes potentiellement malveillants." Régis Lhoste explique : "Un hacker va réécrire d'une nouvelle manière des lignes de code déjà écrites et déjà utilisées. S'il y a un petit bout de BlackMatter ou de HermerticWiper - deux malwares connus - alors je le détecte, je sais ce qu'il va faire et comment réagir, faire de l'identification de menace et de l'attribution. L'objectif, c'est de les détecter avant qu'ils fassent des dégâts." Selon une étude menée par l'Enisa entre 2021 et 2022, les rançongiciels auraient provoqué 18 milliards d'euros de dommages, soit 57 fois plus qu'en 2015.

AEF info est un **groupe de presse professionnelle numérique et organisateur d'évènements**. AEF info produit tous les jours une information de haute qualité qui mobilise une équipe de **80 journalistes** spécialisés permanents à Paris et en régions.

C'est un outil de travail, d'aide à la décision, d'information et de documentation utilisé tous les jours par plus de **20 000 professionnels et 2 000 organisations abonnées** (médias, institutions, collectivités territoriales, entreprises, fédérations, syndicats, associations).

**5 SERVICES D'INFORMATION, 18 DOMAINES ET 2 HEBDOS**
Les cinq services d'information spécialisés d'AEF info diffusent (Social RH, Enseignement Recherche, Développement durable,

Habitat & urbanisme, Sécurité Globale) à leurs abonnés un service d'information continue par courrier électronique et via l'application mobile. Être abonné à ces services, c'est avoir l'assurance d'être informé rapidement, précisément et objectivement des faits essentiels.

**Cliquez ici pour tester gratuitement les services d'information AEF info**

---