

# AVEC DEFMAL, LA RECHERCHE LORRAINE EN PREMIÈRE LIGNE SUR LA CYBERSÉCURITÉ

Lancé dans le cadre du plan France relance et porté par l'Université de Lorraine, le programme de recherche en cybersécurité Defmal va mobiliser 5 millions d'euros sur six ans. Aux avant-postes, à Nancy, le Loria, le laboratoire lorrain de recherche en informatique et ses applications, et son Laboratoire de haute sécurité,



© INRIA - KAKSONEN

L'accès à la salle «serveur» du Laboratoire haute sécurité du Loria, à Nancy, est rigoureusement contrôlé.

Changer de regard pour mieux comprendre. C'est en substance le point de vue adopté par Jean-Yves Marion, professeur à l'Université de Lorraine, chercheur au Loria et responsable du programme DefMal. Lancé en 2022 dans le cadre du plan France Relance et porté par l'Université de Lorraine, le programme de recherche en cybersécurité DefMal, portant sur l'étude des logiciels et programmes malveillants, entame une phase d'accélération. Doté d'un budget de 5 millions d'euros sur 6 ans, DefMal va notamment s'attacher à comprendre le modèle économique de la cybercriminalité : «D'après les derniers chiffres dont nous disposons, les cybercriminels ont amassé plus de 10 milliards d'euros en 2019», rappelle Jean-Yves Marion. Au fur et à mesure que les outils numériques s'imposent dans les

entreprises et les administrations, les logiciels malveillants représentent une menace exponentielle, s'infiltrant dans l'ensemble de l'environnement numérique : les objets connectés, les véhicules autonomes, les systèmes industriels et l'ensemble de l'infrastructure informatique, y compris le cloud, les smartphones et, de manière générale, les logiciels internes de l'ensemble des produits électroniques.

## ÉCOUTER LE TRAFIC ET COLLECTER LES LOGICIELS MALVEILLANTS

L'enjeu est de parvenir à développer de nouvelles méthodes d'analyse et de défense face aux malwares, d'appréhender les aspects économiques, juridiques, criminels et sociologiques qui sous-tendent cet écosystème. «La démultiplication des menaces ces dernières années

rend indispensable une mobilisation universitaire interdisciplinaire, en lien constant avec le monde de l'entreprise et les pouvoirs publics», estime Jean-Yves Marion, qui a structuré le projet autour de collaborations européennes, avec le Centre de cybersécurité CISPA, à Sarrebruck en Allemagne ou internationales, comme avec le Japan Advanced Institute of Science and Technology basé à Kanazawa au Japon et le National Institute of Information and Communications Technology de Tokyo.

En Lorraine, le Loria, le Laboratoire lorrain de recherche en informatique avec ses applications, dispose d'une pièce maîtresse avec le LHS, le Laboratoire de haute sécurité. Sas d'accès contrôlé, vitres blindées, les chercheurs travaillent ici dans une ambiance particulière visant à protéger deux salles contenant des serveurs. Dans ces machines, les chercheurs du Loria ont développé des outils capables d'écouter le trafic internet, à la recherche des mouvements suspects. Autre mission du LHS, la collecte des logiciels malveillants. Pour attirer les attaquants, les chercheurs du Loria ont déployé un «honey pot», soit un pot de miel : une machine faussement vulnérable, permettant à un attaquant de passer à l'attaque. En déployant son logiciel malveillant dans cette machine, le hacker va finalement enrichir la collection du LHS, qui n'en compte déjà pas loin de 35 millions. C'est pour prévenir les risques de fuite que les serveurs du LHS sont aussi sécurisés.

Jean-François Michel