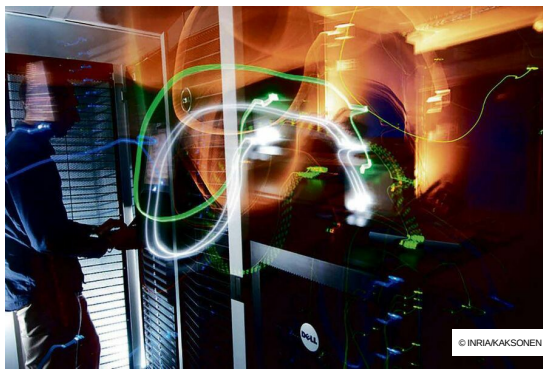
L'USINENOUVELLE

A Nancy, le Loria en pointe dans la détection précoce des cyberattaques

À Nancy, les recherches du laboratoire Loria ciblent la détection des malwares par l'IA et l'analyse morphologique.

Pauline Bandelier

21 janvier 2024 \ 11h00



© INRIA/KAKSONEN

Dans les sous-sols du Loria, le Laboratoire lorrain de recherche en informatique et ses applications, un imposant sas protège le LHS, le Laboratoire de haute sécurité informatique. Cette plateforme située à Villers-lès-Nancy (Meurthe-et-Moselle), dédiée à la recherche en cybersécurité, l'une des deux en France avec celle de Rennes, abrite dans sa salle de serveurs «35 millions de malwares», et de nombreuses données sensibles. L'objectif : «*analyser les modes opératoires et les comprendre pour pouvoir mieux y réagir*», explique Jean-Yves Marion, professeur à l'université de Lorraine et chercheur au Loria.

Pour cela, les scientifiques lorrains collaborent notamment avec leurs homologues du National institute of information and communications technology (NICT) de Tokyo, avec lesquels ils échangent des sondes ou des «pots de miel»: des faux serveurs remplis de vulnérabilités qui servent à attirer les cybercriminels.

Deux start-up déjà créées

Car les attaques sont de plus en plus complexes à détecter, à l'image de celle menée en 2021 contre le système de santé irlandais et qui a mis trois mois avant d'être repérée. «*Tous les objets connectés sont attaquables et forment une chaîne qui permet aux cybercriminels de progresser discrètement dans le système*», rappelle Jean-Yves Marion. Les modes opératoires des rançongiciels ont également évolué, «avec l'exfiltration systématique des données de la victime».

Pour répondre à cette nouvelle réalité, le Loria a obtenu le financement d'un projet unique en Europe, le programme et équipement prioritaire de recherche (PEPR) en cybersécurité DefMal, la défense contre les programmes malveillants. Lancé en 2022 pour une durée de six ans et financé à hauteur de cinq millions d'euros, il vise une avancée décisive dans l'analyse et la défense face aux rançongiciels ou à l'espionnage. Pour que sa recherche reste en lien avec les besoins des entreprises, le Loria a également créé un laboratoire commun avec l'éditeur de logiciels Wallix, ainsi que deux start-up issues de ses travaux de recherche.

La première, Cybi, utilise l'intelligence artificielle pour prédire les chemins d'attaques et générer automatiquement un audit de cybersécurité et un plan de remédiation priorisé des vulnérabilités. S'il existe déjà sur le marché des solutions, «*aucune n'utilise l'intelligence artificielle ni n'est en mesure de trouver le chemin d'attaques associées à ces vulnérabilités*», selon Abdelkader Lahmadi, le cofondateur de Cybi. Créée en 2017, la start-up Cyber-Detect, elle, est spécialisée dans la détection et la caractérisation de programmes malveillants grâce à l'analyse morphologique. La méthode, baptisée «Gorille», est «*plus performante qu'un antivirus classique*», affirme Régis Lhoste, le président de Cyber-Detect. En effet, elle «*cartographie chaque fonctionnalité d'un fichier afin devoir si l'une d'elles correspond à un caractère malveillant*». La start-up a déjà établi des partenariats avec les pépites françaises Tehtris et Quarkslab afin de proposer une méthode complète.

En parallèle, le Loria collabore de manière étroite avec des économistes et des juristes, afin de «*comprendre l'écosystème et le mode organisationnel des cybercriminels et des cyberattaquants. La manière dont ils communiquent et recrutent, comment ils blanchissent l'argent*», détaille Jean-Yves Marion. Dans le but, toujours, de mieux anticiper les futurs mouvements des cybercriminels.