L'USINENOUVELLE
L'Usine Nouvelle (site web)
mercredi 8 novembre 2023 - 11:00 GMT+1 1172 mots

Au Loria, l'innovation au service de la détection précoce des cyberattaques

[L'instant tech] Situé à Villers-lès-Nancy (Meurthe-et-Moselle), le Laboratoire de Haute Sécurité (LHS) de l'Université de Lorraine est un lieu quasi-unique en France. A travers un programme de recherche inédit en Europe et deux start-up innovantes, ses chercheurs travaillent sur l'analyse et la détection précoce des attaques.

Dans les sous-sols du laboratoire Lorrain de Recherche en Informatique et ses Applications (Loria), situé à Villers-lès-Nancy (Meurthe-et-Moselle), un imposant sas protège le Laboratoire de Haute sécurité (LHS). Cette plateforme dédiée à la recherche en cybersécurité, fruit d'un partenariat de l'Université de Lorraine avec l'INRIA et le CNRS, est l'une des deux seules de ce type en France avec celle de l'IRISA à Rennes. Visant la détection des intrusions et la protection contre les logiciels malveillants, elle abrite dans sa salle de serveurs « 35 millions de malwares », mais aussi de nombreuses données sensibles.

A l'intérieur de la salle de travail, les chercheurs observent sur des ordinateurs les « bruits de fonds » des données pour repérer d'éventuelles attaques. Dans le cadre d'une collaboration avec le National Institute of Information and Communications Technology (NICT) de Tokyo, les chercheurs lorrains et tokyoïtes s'échangent des sondes ou des « pots de miel » c'est-à-dire des faux serveurs remplis de vulnérabilités afin d'attirer les cybercriminels. L'objectif: « Analyser les modes opératoires, les détecter et les comprendre pour pouvoir mieux y réagir », précise, à l'occasion d'une visite, Jean-Yves Marion, professeur à l'Université de Lorraine et ancien directeur du Loria. Un projet de recherche unique en Europe

En effet souligne Jean-Yves Marion, les attaques, de plus en plus sophistiquées, sont également plus complexes à détecter, à l'image de celle menée en 2021 contre le système de santé irlandais et qui a mis trois mois à être repérée. « Tous les objets connectés sont attaquables et forment une chaîne qui permet aux cybercriminels de progresser discrètement dans le système », rappelle le chercheur du Loria. Des cyberattaques qui font aussi des dégâts toujours plus importants, à l'image de celle menée contre le port de Nagoya, paralysé pendant plus de trois jours en juillet 2023. « Les modes opératoires des rançongiciels ont évolué, avec l'exfiltration systématique des données de la victime. Les groupes sont structurés, avec un modèle économique, et sont capables d'attaques ciblées », rappelle Jean-Yves Marion.

Pour répondre à cette nouvelle réalité, le Loria a obtenu le financement d'un projet de recherche unique en Europe, le programme et équipement prioritaire de recherche (PEPR) en cybersécurité DefMal (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 où à l'espionnage : « DefMal illustre la volonté étatique d'accélérer les choses. Ce programme va nous permettre de faire avancer la recherche fondamentale qui est un facteur important d'innovation » estime Jean-Yves Marion. Autre source d'avancées, le partage de données avec des institutions partenaires comme le NICT japonais, le CISPA allemand et d'autres institutions partenaires dans la Sarre, au Luxembourg et en Belgique. 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, et deux start-up issues de ses travaux de recherche ont été fondées. Cybi : l'IA pour détecter les chemins d'attaques

Cofondée en mai 2022 par Abdelkader Lahmadi, enseignant chercheur à l'Université de Lorraine, Cybi est le résultat de 10 ans de recherche au sein des laboratoires lorrains Loria et Inria Nancy. Son ambition ? Utiliser l'intelligence artificielle pour prédire les chemins d'attaques et générer automatiquement un audit de cybersécurité et un plan de remédiation priorisé des vulnérabilités. L'IA développée par le chercheur du Loria et ses collègues a été entraînée à partir de « milliards de documents de sécurité » précise Abdelkader Lahmadi. Ce dernier, qui a notamment travaillé sur la sécurité des objets connectés, rappelle que pour chaque dispositif, plus de 160 vulnérabilités sont détectées en moyenne chaque jour, et jusqu'à 5000 par mois. Des chiffres qui font que les analystes de cybersécurité se retrouvent vite submergés et incapables de prioriser les interventions.

S'il existe déjà sur le marché des solution de détection de vulnérabilités, « aucune n'utilise l'intelligence artificielle ni n'est en mesure de trouver le chemin d'attaque associé à ces vulnérabilités » selon Abdelkader Lahmadi. En termes de commercialisation, si Cybi en est encore aux prémisses, l'idée est de proposer un accès à la solution par abonnement ou via la vente de jetons d'analyse. « Au travers de nos revendeurs et distributeurs, nous avons déjà effectué des démonstrations auprès d'industriels travaillant dans différents secteurs d'activité, dont la fabrication

d'équipements, l'aéronautique ou l'énergie », précise le chercheur. Cyber-Detect, l'analyse morphologique des malwares

Créée en 2017 à l'issue de 10 années de recherche au sein du Laboratoire de Haute Sécurité du Loria, la start-up Cyber-Detect est spécialisée dans la détection et la caractérisation de malwares (logiciels malveillants) grâce à l'analyse morphologique. « Aujourd'hui, les malwares se transforment spécifiquement pour attaquer les entreprises... Pour protéger les infrastructures, il faut pouvoir détecter ces variants avant qu'ils ne passent à l'attaque. L'enjeu est aussi de distinguer ceux qui présentent un réel danger et les faux positifs, afin d'alerter uniquement lorsque cela est nécessaire » introduit le président de Cyber-Detect, Régis Lhoste.

La méthode, baptisée « Gorille », est « plus performante qu'un antivirus classique », puisqu'elle permet de « cartographier chaque fonctionnalité d'un fichier afin de voir si l'une d'elles correspond à un caractère malveillant », explique Régis Lhoste. En d'autres termes, l'enjeu est de décomposer le contenu de l'attaque, afin de mieux la comprendre. La start-up a déjà établi des partenariats avec les pépites françaises Tehtris et Quarklab afin de proposer une méthode complète. « Notre objectif est de travailler avec des intégrateurs et des éditeurs comme une brique complémentaire des EDR (Détection et réponse aux points finaux), qui ne sont pas actuellement en mesure de prendre des décisions sur un certain nombre de fichiers » détaille le président de Cyber-Detect. Savoir attaquer pour mieux se défendre

En parallèle, les chercheurs du Loria collaborent avec la police et la gendarmerie afin de les aider à mieux appréhender le mode opératoire des cybercriminels. Mais aussi pour élaborer des scénarios d'attaque. Car, pointe Jean-Yves Marion, « une des meilleures façons de se défendre est parfois d'attaquer ». Un domaine de recherche dans lequel la France est plutôt en retard, selon lui. Pour remédier à cette situation, Gabriel Sauger, l'un des deux doctorants intégré au programme DefMal, collabore notamment avec la section informatique de l'Université d'Arizona à Tucson.

La recherche collaborative porte sur la construction d'une attaque contre des systèmes de défense basés sur l'intelligence artificielle, afin de repérer d'éventuels défauts dans le système de protection. Enfin, le Loria collabore de manière étroite avec des économistes et des juristes, afin d'approcher la cybercriminalité dans toutes ses dimensions. « Nous cherchons à comprendre l'écosystème et le mode organisationnel des cybercriminels et des cyberattaquants. La manière dont ils communiquent, recrutent, comment ils blanchissent l'argent » détaille Jean-Yves Marion, qui espère à l'avenir intégrer également la psychologie et la sociologie. Dans le but, toujours, de mieux anticiper les futurs mouvements des cybercriminels.