

Lorraine

Cybercriminalité : partager le savoir pour traquer les intrusions

Face à la menace de logiciels malveillants dans nos usages quotidiens, le laboratoire Haute sécurité du Loria (Laboratoire lorrain de Recherche en Informatique et ses Applications) prône une vigilance scientifique mutualisée. Les dispositifs des hackers sont structurés de manière criminelle.

Hôpital-ordinateur : même combat ? Avec un sas de filtrage préalable à toute entrée dans le LHS (Laboratoire Haute Sécurité) du Loria (Laboratoire lorrain de Recherche en Informatique et ses Applications), le parallèle entre la menace sanitaire du virus dans les couloirs des établissements hospitaliers et celle qui guette les systèmes numériques des sociétés contemporaines, vient à l'esprit assez naturellement.

La menace est bien réelle et plus personne ne l'ignore aujourd'hui. À la maison, sur son téléphone ou au travail, les malwares nous guettent.

« Nous ne sommes plus à l'époque où le hacker s'assemblait à un adolescent bouton-neux, désireux d'impressionner sa copine au fond du garage », illustre Jean-Yves Marion.

« Les objets aujourd'hui attaquables sont les objets connectés. Les attaques disposent de moyens sophistiqués ».



Régis Lhoste est le fondateur de la start-up Cyber-Detect, spécialisée dans la détection des malwares (logiciels malveillants). Photo Parice Saucourt

« Nouvelles approches d'analyses »

Porteur du programme de cybersécurité DefMal, ce professeur à l'Université de Lorraine défend les vertus d'un partage de savoirs et de connaissances entre experts. « Cette dynamique répond aux grandes transitions de notre monde », a-t-il expli-

qué en milieu de semaine dans les entrailles du Loria, à des journalistes et experts de la cybercriminalité. Face à la profusion et l'intelligence des logiciels malveillants (malwares) aux aguets pour pénétrer nos codes secrets, DefMal vise à développer « de nouvelles approches d'analyse et de détection ». Autour d'Hélène Boulan-

ger, présidente de l'Université de Lorraine, les experts présents ont ciblé, en particulier, la nécessité d'une intervention de protection rapide dans les dispositifs de cybersécurité, pour limiter les risques. Car la course contre la montre est désormais engagée avec des univers criminels structurés et suffisamment habiles, au

point de savoir eux-mêmes... protéger les malwares des dispositifs hostiles anti-malwares.

« Localiser les tentatives d'intrusion »

Le Loria s'est associé dans cette démarche avec la start-up Cyber-DéTECT, fruit de travaux en recherches en interne. « L'objectif est de comprendre les défis que rencontrent les entreprises, les collectivités, les institutions ou les États, et de renforcer le lien entre le monde académique et celui de l'innovation », insiste le Pr Jean-Yves Marion. Figurant parmi les dix premiers projets de recherche ciblés par le gouvernement, le programme DefMal sera ainsi porté et défendu lors de conférences internationales.

Président de Cyber-DéTECT, Régis Lhoste souligne au passage l'intérêt des solutions de détection du dispositif « Gorille », conscient toutefois de la nécessité de ne jamais baisser la garde. « Les collaborations de recherches nous permettent d'être au plus près des agresseurs du numérique », dit-il. « Il faut continuer de construire des outils bâtis sur la complémentarité des dispositifs pour déterminer en particulier les chemins d'attaques et localiser les tentatives d'intrusion. »

● Antoine Pétry

« Il faut apprendre à vivre avec l'intelligence artificielle »

« On est en train de changer de monde ». La phrase pourrait malheureusement s'appliquer à toute notre planète en crise(s). Elle concernait ce jeudi 26 octobre, au Centre de congrès Jean-Prouvé de Nancy, le numérique et nos vies désormais digitales. Pas un mois sans qu'une entreprise, un hôpital ou une collectivité ne soient attaqués et rançonnés par des hackers. Une menace invisible qui est pourtant partout, d'un mail à une clé USB, du Bluetooth au wifi de votre smartphone ou votre ordinateur.

Organisées par la Faculté de Droit de Nancy et le Loria (CNRS, Inria, Université de Lorraine), en partenariat avec la Région Grand Est, Grand-Est, la Métropole du Grand Nancy et le laboratoire Irénée, les assises universitaires Droit et cybersécurité privilégiées, comme lors de la première édition en 2022, « une approche transverse juridique, économique et organisationnelle ». « Cette rencontre interdisciplinaire est l'occasion de dresser l'état

de l'art », revendiquent Jean-Yves Marion (professeur à l'Université de Lorraine, directeur du Loria) et Marc Burg (préfet chargé de mission au secrétariat général du Ministère de l'Intérieur et professeur associé à l'Université de Lorraine).

« La donnée au centre de tout »

Pour bien se rendre compte que notre rapport au temps est totalement bouleversé, prenons l'exemple de ChatGPT. Est-il encore besoin de présenter cette Intelligence artificielle (IA) conversationnelle disponible gratuitement en ligne ? En quelques mois à peine, elle s'est invitée, même imposée dans le débat. « La donnée est au centre de tout », insiste Marc Burg. « Et l'IA vient encore lui donner davantage de valeur. Rendez-vous compte : ChatGPT, lancé en 2017, intégrait 117 millions de paramètres. Un an plus tard, 1,5 milliard. Avec ChatGPT 4 sorti cette année, nous en



ChatGPT a totalement pulvérisé sa puissance de calcul en quelques mois. Pour les professionnels réunis à Nancy, il ne faut pas interdire l'IA mais davantage apprendre à la dompter. Photo ER/Lionel Vadam

sommes à 175 milliards de paramètres... »

D'où cette question, soulevée en conclusion de la journée : comment canaliser cette puissance de calcul définitivement exponentielle ? « Dans les années 2000, au début d'internet, il y avait déjà des ayatollahs de la

sécurité », se souvient Édouard Jeanson, Chief information security officer (Ciso) chez CapGemini France, un des experts présents en Lorraine. « Ils voulaient nous empêcher de connecter le moindre poste. Aujourd'hui, c'est pareil : il ne faut pas interdire l'IA mais ap-

prendre à vivre avec. Se poser les bonnes questions en essayant de prendre un peu de recul. Le tout, avec beaucoup de bon sens paysan pour pouvoir se dire, si besoin : je m'arrête là. Mais en aucun cas, on peut se dire, je refuse l'IA ».

● Paul-Marie Pernet