29 octobre 2023

Informatique: un labo pour détecter les pirates avant intrusion

Villers-lès-Nancy (France) (AFP) – Détecter l'attaque informatique avant même qu'elle se concrétise : près de Nancy, des chercheurs analysent le mode de fonctionnement des cybercriminels dans un programme de recherche unique en Europe.

Publié le : 29/10/2023 - 08:25 Modifié le : 29/10/2023 - 08:23 4 mn

Jean-Yves Marion, à la tête du Loria (Laboratoire lorrain de recherche en informatique et ses applications), à Villers-les-Nancy (Meurthe-et-Moselle), le 25 octobre 2023 © Jean-Christophe VERHAEGEN / AFP

Au sous-sol du Laboratoire lorrain de recherche en informatique et ses applications (Loria), à Villers-lès-Nancy (Meurthe-et-Moselle), est située une salle de recherche "hautement sécurisée": ses fenêtres pourraient résister à sept coups de hache.

A l'intérieur du "laboratoire de haute sécurité" (LHS), des écrans d'ordinateur avec lesquels les chercheurs écoutent "les bruits de fond" des données, en partenariat avec le National Institute of Information and Communications Technology de Tokyo. Concrètement, des mouvements sont repérés sur des adresses IP "qui ne devraient pas être utilisées", ce qui peut présager d'une attaque à venir.

Et avec leur technique du "pot de miel", les universitaires attirent déjà au quotidien les attaquants dans des pièges, pour ensuite analyser leur mode de piratage.

La France compte deux laboratoires de haute sécurité, l'autre se trouve à Rennes.

Fini le temps où les antivirus permettaient de protéger ses données face au pirate de base qui lançait ses attaques "au fond d'un garage", souligne Jean-Yves Marion, ancien directeur du Loria. Ils sont désormais plus organisés.

Ces dernières années, la menace s'est "démultipliée" selon lui, rendant "indispensable une mobilisation universitaire (...) en lien constant avec le monde de l'entreprise et des pouvoirs publics".

Attaques sophistiquées

Depuis la création du Loria en 2010, les chercheurs ont collecté plus de 35 millions de programmes malveillants. Si cela leur permet de les analyser et de les tester, "c'est insuffisant", insiste M. Marion.

Désormais, un nouveau programme de recherche lancé en juin, le "DefMal", pour "Défense contre les programmes malveillants", vient s'inscrire "dans une stratégie d'accélération annoncée par le président de la République", souligne Lorraine Université d'Excellence.

Un spécialiste en cybersécurité procède à une analyse morphologique d'un logiciel infecté par un virus, au Loria, à Villers-les-Nancy, le 25 octobre 2023 © Jean-Christophe VERHAEGEN / AFP

Présenté comme unique en Europe, un budget "inédit" de 5 millions d'euros sur six ans lui a été attribué. "Il permettra surtout d'embaucher des doctorants et des ingénieurs", selon Jean-Yves Marion.

L'enjeu, aujourd'hui, est "de détecter ces logiciels malveillants avant qu'ils ne passent à l'attaque".

Une attaque débute par l'exfiltration des données, qui sont ensuite chiffrées.

Certaines peuvent durer des mois, insistent les chercheurs: l'exfiltration se fait par petits morceaux, pour ne pas alerter.

Et signe de la professionnalisation des cybercriminels, les attaques sont de plus en plus sophistiquées, souligne Régis Lhoste, président de la société Cyber-Detect, qui a été créée dans la continuité des travaux du Loria: les programmes malveillants sont "aujourd'hui conçus spécifiquement pour attaquer votre entreprise", sur mesure, tout en reprenant quelques structures déjà vues par le passé.

Entreprises et institutions

Sa jeune pousse travaille avec de nombreuses entreprises ou institutions, leur proposant son expertise pour anticiper les attaques ou les comprendre, via des analyses des virus informatiques semblables à celles utilisées dans la recherche médicale.

Abdelkader Lahmadi, enseignant-chercheur au Loria et co-fondateur, avec d'autres chercheurs, de la jeune pousse Cybi, explique que les grandes entreprises "sont submergées" par les rapports de failles de vulnérabilité qui se multiplient.

Le professeur Jean-Yves Marion, dirigeant du Loria, devant un écran montrant l'analyse dynamique par le logiciel Gorille d'un programme infecté, à Villers-les-Nancy, le 25 octobre 2023 © Jean-Christophe VERHAEGEN / AFP

La solution mise au point par les chercheurs et désormais commercialisée, fondée sur l'intelligence artificielle, permet de "révéler les chemins d'attaque" qui pourraient être utilisés: cela peut, par exemple, débuter par le piratage d'une caméra de surveillance sur un parking, pour ensuite porter atteinte à toute l'unité de production d'un industriel.

Avec DefMal, les universitaires vont aller plus loin, en cherchant à déterminer le mode de fonctionnement des organisations cybercriminelles: comment recrutent-elles et communiquent-elles ? Comment blanchissent-elles l'argent ?

Cette analyse nécessite un travail "main dans la main" avec juristes et économistes, selon Jean-Yves Marion.

Les chercheurs du Loria travaillent aussi avec la police ou la gendarmerie sur certaines enquêtes.

© 2023 AFP