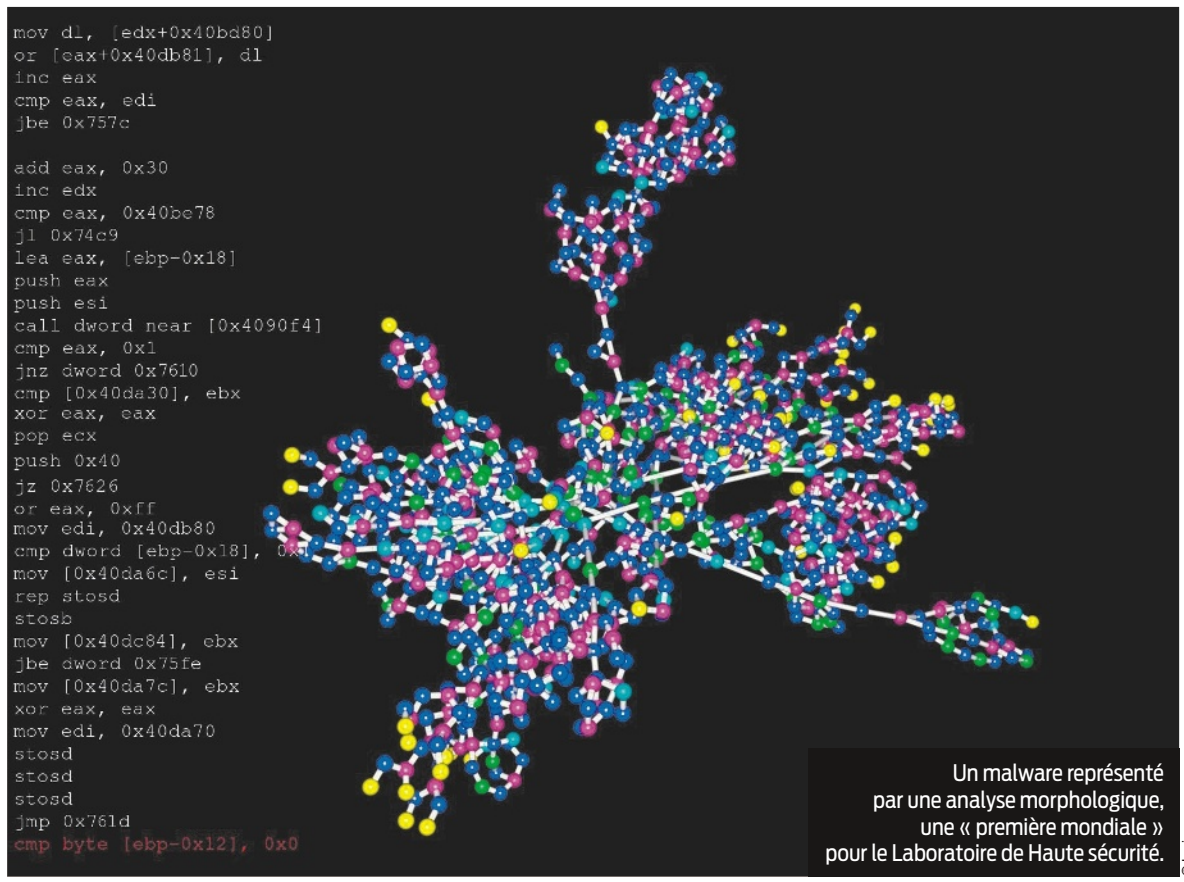
Une Semaine à...

Lorraine / TECHNOLOGIE

Cybersécurité : les virus du monde entier analysés depuis Nancy

Quelques jours après les **ASSISES UNIVERSITAIRES DROIT ET CYBERSÉCURITÉ** organisées à Nancy, « La Semaine » plonge au cœur du référent mondial en matière de cybersécurité qui constitue la première force de recherche nationale dans ce domaine : le laboratoire de Haute sécurité (LHS) installé au sein du Loria et de l'Inria.



Un malware représenté par une analyse morphologique, une « première mondiale » pour le Laboratoire de Haute sécurité.

© Loria

C'est un lieu pas comme les autres. Dans les méandres du Laboratoire lorrain de recherche en informatique et ses applications (Loria) et de l'Institut national de recherche en sciences et technologies du numérique (Inria), au détour d'un couloir, après un sas surprotégé, des vitres blindées, deux pièces hautement sécurisées sont enfin accessibles. **C'est dans cet antre totalement clos et retiré du reste de l'agitation universitaire et scientifique que les chercheurs s'affairent.** Depuis 2010, toute une équipe est mobilisée autour des questions de cybersécurité. Avec un objectif : lutter contre la prolifération de malwares, ces logiciels malveillants qui touchent les objets connectés et les systèmes industriels. Ils étudient les logiciels malveillants (malwares), de rançonnage bien souvent, leurs variants et analysent leur morphologie en vue de les détecter le plus tôt possible. Car bien souvent, ils parviennent à échapper aux systèmes de protection existants des entités privées comme publiques en utilisant une technique d'offuscation de code. **Encore récemment en Meurthe-et-Moselle, l'entreprise Baccarat en a été victime.** À quelques kilomètres des frontières départementales, deux hôpitaux de la plaine vosgienne ont aussi été touchés ces derniers jours. Les attaquants vont bloquer les systèmes en cryptant les données. Ils récupèrent ces données et demandent une rançon pour les libérer ou les revendre.

Afin de détecter ces codes malveillants, les chercheurs *« écoutent les bruits »* par le biais d'un *« télescope virtuel »*. Ce super outil scrute, observe et recense les vagues de cyberattaques en temps réel, permettant aux chercheurs d'observer des milliers d'attaques en direct. Si elles sont généralement constantes, des grands moments qui vont faire l'actualité peuvent être détectés avec un flux d'attaques ou de bruits bien plus conséquent. **« Ce fut le cas lors des élections américaines de 2016, pendant le conflit Ukraine-Russie aussi par exemple**. *Mais sur le conflit au Proche-Orient, c'est plus compliqué. Il y a eu une activité. Mais il est très difficile de l'attribuer à quelqu'un. Et encore moins de déterminer une source géographique. On ne peut rien en déduire comme type d'information. On écoute de manière très large. De temps en temps, quand on a de la chance, on peut relier l'activité à un événement. Mais le plus souvent, c'est lié à une vulnérabilité qui a été découverte ou à un tas d'autres raisons »*, explique Jean-Yves Marion, professeur à l'Université de Lorraine, chercheur au Loria et membre de l'Institut universitaire de France.

« Comme en biologie, certains virus sont des mutants »

Pour intercepter et collecter tous ces logiciels malveillants, le laboratoire dispose d'un **« pot de miel virtuel »**. Une ruse qui attire les cyberattaquants en leur faisant croire qu'ils ont trouvé la proie idéale. Mais pas question de contaminer l'ensemble du réseau du Laboratoire de Haute sécurité, l'analyse des malwares est alors permise sans risques. À ce jour, le laboratoire dispose d'une base de données de près de 35 millions de malwares que les chercheurs ont minutieusement analysés. Et après ? **Toute cette collecte leur a permis de développer une technique d'analyse morphologique.** Cette méthode, *« première mondiale »*, repose sur un système d'intelligence artificielle, entraîné par apprentissage automatique, permettant d'identifier les fonctionnalités cachées dans les programmes tels que des applications et des mises à jour en se basant sur la forme du virus. Cela permet de détecter rapidement les intrusions qui échappent aux systèmes de détection existants. Les chercheurs dissèquent le virus pour déterminer si des souches sont déjà connues ou non. Ils les répertorient et déterminent leurs fonctionnalités au cas où un même comportement serait revu quelques semaines plus tard dans une autre attaque. Mais pas question de garder toute cette prouesse dans les deux pièces sécurisées. **Depuis 2017, cette solution est commercialisée par la start-up** *Cyber-Detect* à travers le logiciel « Gorille ». Un dispositif utilisé par des entreprises privées comme des entités gouvernementales avec une mise à jour constante. *« Comme en biologie, certains virus sont des mutants. Les cyberattaquants les font varier pour tromper les antivirus »*, précise Régis Lhoste, fondateur de Cyber-Detect.

Autre entreprise issue du LHS : Cybi. Encore hébergée dans les locaux, cette entité développe, **Skuba, basé sur l'intelligence artificielle.** Alors que de plus en plus d'attaques utilisent les objets connectés peu sécurisés pour rebondir et s'introduire dans les systèmes, Skuba va analyser et prédire tous les chemins d'attaques, toutes les vulnérabilités de l'entreprise et proposer des solutions pour éviter que ces objets connectés ne permettent aux pirates de pénétrer le système.

La recherche lorraine à la pointe

Si des solutions existent, pas question d'arrêter la recherche. **Le Loria reste à la pointe et représente l'une des premières forces de recherche académique en France dans la cybersécurité.** Ses travaux, menés en étroite collaboration avec d'autres structures de recherche universitaire en France et en Europe, sont à l'origine d'avancées significatives dans la détection précoce des menaces cyber pour mieux les combattre.

Dans ce sens, le programme de recherche en cybersécurité, *DefMal*, portant sur l'étude des logiciels et programmes malveillants, s'intensifie après son évaluation à un an. Lancé en 2022 dans le cadre du plan France Relance et porté par l'Université de Lorraine, mobilisant les mondes de la recherche et de l'entreprise, bénéficiant de collaborations à l'échelle européenne et internationale, ce projet vise à renforcer la détection des malwares et rançongiciels tout en appréhendant les aspects économiques, juridiques, criminels et sociologiques qui sous-tendent cet écosystème. **Avec un budget de cinq millions d'euros échelonné sur six ans,** il s'agit de l'un des dix premiers projets de recherche ciblés qui s'inscrivent dans une stratégie nationale d'accélération annoncée par le président de la République. *« L'évaluation du projet, un an après son lancement, va nous permettre de répondre à l'objectif fondamental de se doter de capacités d'anticipation et de réactions rapides face aux cyber-attaques par programme malveillant et de permettre aux entreprises, administrations et institutions d'en profiter. Il faut saluer l'engagement du gouvernement à renforcer la cybersécurité et à soutenir la recherche dans ce domaine »* conclut Jean-Yves Marion.

Les résultats du programme *DefMal* seront présentés lors de conférences internationales. Le projet s'impliquera également dans la formation de jeunes chercheurs et établira des échanges avec les services de l'État et les entreprises. Un élément supplémentaire d'excellence pour l'Université de Lorraine.

Baptiste Zamaron