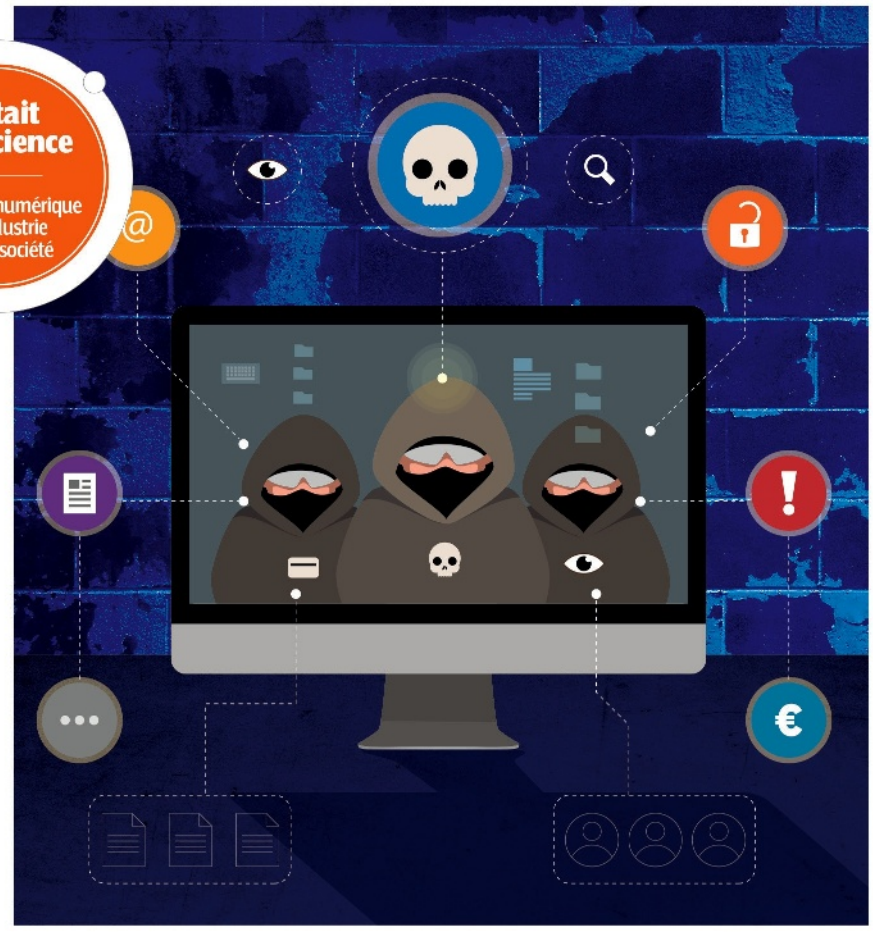
CYBER-SÉCURITÉ

Il était une science

Transition numérique de l'industrie et de la société

COMPRENDRE L'ÉCOSYSTÈME DES CYBERCRIMINELS POUR MIEUX LES COMBATTRE



Les cybercriminels ne sont plus de jeunes geeks qui agissent dans leur coin mais des organisations criminelles qui s'accaparent des données pour les monnayer en exigeant des rançons. Dans le cadre du projet DefMal (Défense contre les programmes malveillants), Lorraine Université d'Excellence mène des recherches en matière de cybersécurité. Les explications de Jean-Yves Marion, professeur à l'Université de Lorraine, à l'École Nationale Supérieure des Mines de Nancy (ENSMN) ainsi qu'au LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications – CNRS, Inria, Université de Lorraine).

Nul n'est à l'abri. La cybercriminalité concerne les particuliers comme les organisations, les entreprises comme les états. Comprendre que la cybersécurité est un enjeu majeur. Différents partenaires de Lorraine Université d'Excellence (LUE) mènent des travaux de recherche en matière de cybersécurité. Ils portent sur la cryptographie, la vérification des protocoles (communication entre deux ordinateurs) notamment en lien avec le vote électronique, ou bien encore sur les programmes malveillants. Dans la continuité d'un premier projet appelé Impact DigiTrust destiné à redonner « confiance dans le numérique », LUE a permis de lancer DefMal (Défense contre les programmes malveillants) qui est un projet du programme France Relance.

Des groupes organisés comme des entreprises

Les recherches se concentrent sur la compréhension des écosystèmes cybercriminels pour être en mesure de détecter les signaux faibles et d'anticiper les attaques. « *Certains de ces groupes sont organisés comme de véritables petites entreprises avec un service en charge de développer des logiciels d'attaque, des services de négociation, d'aide aux victimes pour qu'ils puissent payer en bitcoin, d'exfiltration des données, de blanchiment de l'argent… Et au bas de l'échelle, il y a les affiliés qui vont perpétrer l'attaque. C'est une sorte d'ubérisation de la cybercriminalité, ce qui fait que l'arrestation de l'ensemble d'un groupe de cybercriminels est très compliquée* », a expliqué Jean-Yves Marion, professeur à l'Université de Lorraine, à l'ENSMN et au LORIA, lors d'un webinaire auquel participait aussi Bertrand Pailhes, directeur des technologies et de l'innovation à la CNIL qui est revenu sur les missions et priorités de la Commission nationale de l'informatique et des libertés. La cybercriminalité est donc portée par des organisations et des procédures au service d'un modèle économique. « *Et la concurrence entre les groupes est vive car il est important de séduire et de fidéliser les affiliés car ce sont eux qui sont à la manœuvre, en sachant que l'on n'est pas chez les bisounours* », précise l'expert qui a dirigé le LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications – CNRS, Inria, Université de Lorraine) durant 10 ans.

Programmes malveillants : détecter et anticiper

Mieux comprendre ces écosystèmes cybercriminels dans leurs multiples dimensions (organisationnelle, technologique, juridique…), c'est le premier volet de DefMal qui mobilise des experts en informatique ainsi que des économistes ou des juristes. Et demain, peut-être, des sociologues, des psychologues ou des anthropologues. Jean-Yves Marion plaide en tout cas pour qu'il en soit ainsi. À ce volet s'en ajoute un second qui porte plus spécifiquement sur la détection et l'analyse des programmes malveillants à l'heure de l'Intelligence Artificielle qui « industrialise le phishing et le hacking humain ». Là encore l'ambition est d'anticiper sur les programmes, variants et menaces à venir, alors que la multiplication des objets connectés s'accompagne de nouvelles vulnérabilités. « *La surface d'attaque ne fait qu'augmenter : caméras, capteurs, voitures, avions, drones… L'informatique est partout* », souligne le chercheur non sans évoquer toute l'importance de ce que l'on appelle la « *Security by design* », autrement dit la nécessité d'intégrer la sécurité dans le développement même des objets (connectés) avec pour priorité de réduire leur vulnérabilité.

À noter que ces travaux qui relèvent de la recherche fondamentale ont déjà des applications très concrètes comme le confirme, par exemple, la création de la start-up Cyber-Detect qui commercialise une solution innovante d'analyse de logiciels malveillants.