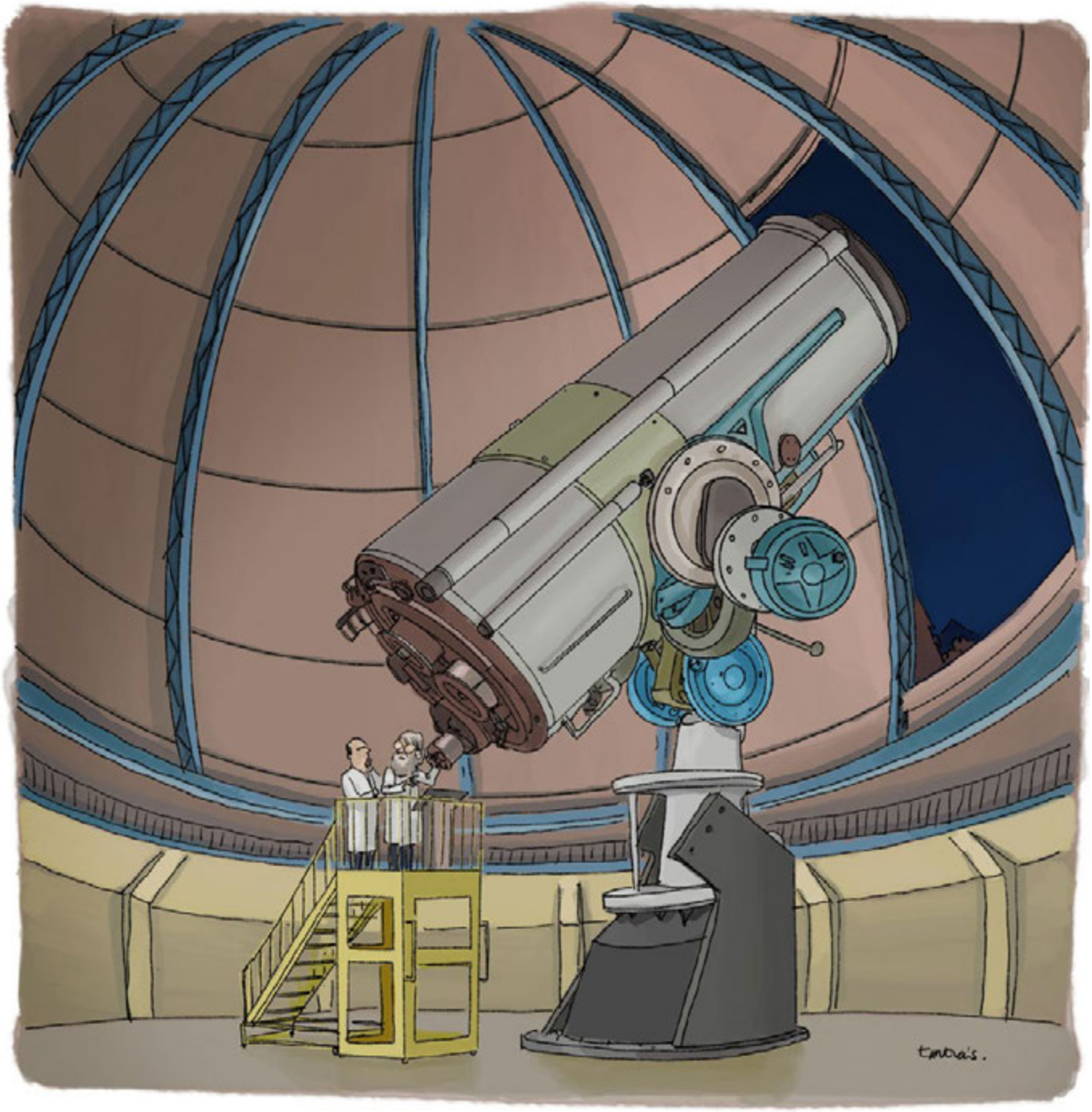
# Le télescope qui surv




Trouver Pegasus dans le cyberespace ? C'est plutôt lui qui devrait nous trouver, non ?

ILLUSTRATION : TARTRAIS POUR «LE POINT»

# eille le cyberespace

**Antivirus.** À l'heure de l'espionnage informatique généralisé, un laboratoire scrute les millions de virus qui prolifèrent sur le Net.

PAR BAUDOUIN ESCHAPASSE

C'est une sorte de bunker à moitié enterré à flanc de coteau, sur la commune de Vandœuvre-lès-Nancy (Meurthe-et-Moselle). Un bâtiment discret sur le campus du technopôle lorrain dont les hublots sont dotés de vitres pare-balles. Les visiteurs ne peuvent y accéder qu'après avoir montré patte blanche. Et seules deux personnes sont habilitées à ouvrir ses lourdes portes blindées commandées par un double système d'identification. De l'autre côté du sas ? Une petite pièce circulaire dotée d'une demi-douzaine d'ordinateurs et un data-center où clignotent des serveurs, aux faux airs de coffres-forts numériques.

Les précautions prises pour sécuriser ce site, placé sous la triple tutelle du Centre national de la recherche scientifique (CNRS), de l'Université de Lorraine et de l'Institut national de recherche en informatique et en automatique (Inria), ne tiennent pas seulement au coût des équipements qu'il abrite. Mais aussi et surtout à la dangerosité des données qu'il renferme. Ce laboratoire, unique en Europe, stocke en effet quelque 35 millions de logiciels malveillants. Certains sont particulièrement redoutables *(voir encadré p. 68)*. Capables d'infecter, de manière très discrète, les systèmes informatiques de nombreuses entreprises et administrations, ils pourraient paralyser des secteurs d'activité aussi cruciaux pour le pays que la santé, la finance, mais aussi les télécoms, l'énergie, voire la défense nationale. Une agglomération du nord de l'Allemagne en a fait l'expérience. Paralysés depuis le 9 juillet par une panne informatique, les services administratifs du district d'Anhalt-Bitterfeld n'ont pu verser ni allocations, ni aides sociales pendant plusieurs semaines, au grand dam de la population.

L'infrastructure, installée dans la banlieue de Nancy depuis 2009, vise précisément à empêcher que la France ne se retrouve dans la même situation. L'équipement est souvent comparé aux centres de recherche labellisés P4, où sont stockés les virus biologiques les plus létaux. *« Ce n'est pas à cause de ces virus-là qu'on a besoin de porter des masques »*, sourit Bruno Lévy, directeur du centre Inria Nancy-Grand Est, qui chapeaute ce laboratoire de haute sécurité (LHS). Quand on lui demande d'en expliquer l'utilité, son cofondateur, Jean-Yves Marion, par ailleurs directeur du Laboratoire lorrain de recherche en informatique et ses applications (Loria), recourt à une analogie avec l'astrophysique. *« Notre installation est une sorte de télescope pointé sur le cyberespace »*, dit-il. Il aurait tout aussi bien pu comparer cet outil à un microscope scrutant les agents pathogènes qui gangrènent le Net.

**35 millions**
C'est le nombre de logiciels malveillants que stocke le LHS de l'Inria Nancy-Grand Est, laboratoire unique en Europe.

**15 millions**
C'est le nombre de sollicitations que reçoivent chaque jour les fausses adresses IP, appelées « pots de miel », installées par les chercheurs de l'Inria, du CNRS et de l'Université de Lorraine, qui travaillent sur place.

Avec 35 millions de spécimens, donc, la base de données du LHS de Nancy est l'une des plus importantes au monde. Constituée de nombreux « variants », elle rassemble en réalité 500 000 souches différentes. C'est un panel particulièrement précieux pour qui veut comprendre la menace qui pèse sur les réseaux. *« Si nous les conservons, c'est pour en étudier à la fois les propriétés mais aussi la morphologie, et ce afin de mettre en place des dispositifs de détection de plus en plus performants »*, explique Fabrice Sabatier, ingénieur de recherche au CNRS, qui fait partie de la quinzaine de scientifiques qui travaillent quotidiennement sur site.

**Chevaux de Troie.** Pour collecter ces lignes de code toxiques qui circulent sur le Web, les chercheurs lorrains ont placé des dizaines de pièges sur la Toile mondiale. Ils les appellent des « pots de miel » en ce qu'ils simulent l'activité d'ordinateurs standards. Ces fausses adresses IP, que les hackers prennent pour des cibles, reçoivent, chaque jour, près de 15 millions de sollicitations. Des messages porteurs de pièces jointes parfois vérolées. Ce que les spécialistes appellent des chevaux de Troie, ou des vers informatiques. Certains de ces programmes espionnent ou détruisent les disques durs. D'autres prennent en otage les ordinateurs, encodant les données qu'ils renferment et exigeant une rançon des internautes pour qu'ils puissent récupérer ■■■

DAVID BETZINGER/INRIA

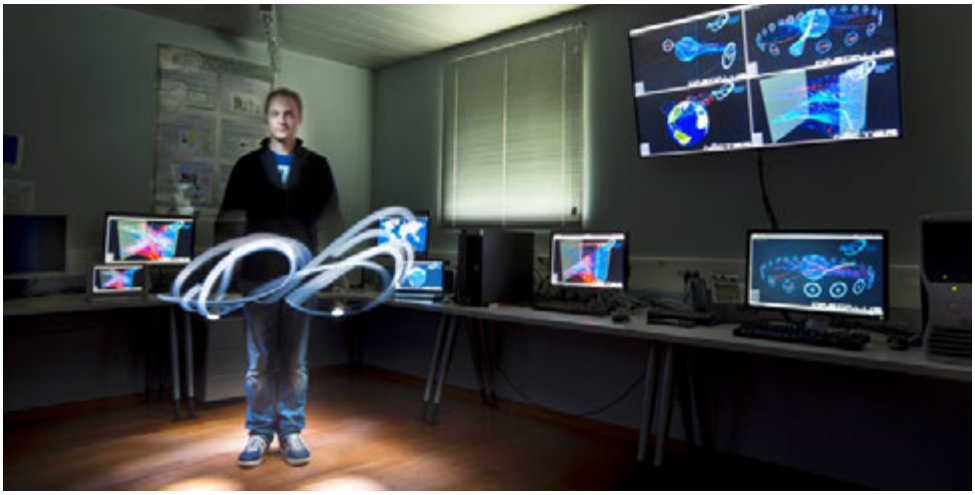
« Ce n'est pas à cause de ces virus-là qu'on a besoin de porter des masques. »
**Bruno Lévy,** directeur du centre Inria Nancy-Grand Est

■■■ leurs biens (une promesse souvent non tenue). Une poignée transforme enfin des armées de machines en « zombies » générant des attaques coordonnées pour faire disjoncter des serveurs, ou inonder des messageries de spams, dont certains sont, eux-mêmes, dotés d'« hameçons » destinés à récupérer les données sensibles, notamment bancaires, des internautes.

**Failles.** Aspirés par un « trou noir », ces différents spécimens de virus informatiques se retrouvent placés en « éprouvette » sur un réseau scellé qui permet d'exécuter des expériences sensibles, de manière totalement sécurisée. Leur activation se fait ainsi dans des « bacs à sable » afin d'empêcher leur prolifération dans la nature. *« Il faut être de plus en plus rusé car les concepteurs de certains de ces logiciels sont très malins. Il arrive que leurs virus se mettent en sommeil quand ils suspectent d'être tombés dans un piège. Nous devons alors simuler autour d'eux une activité bureautique qui leur fasse croire qu'ils sont dans une vraie machine pour qu'ils s'activent »*, glisse Abdelkader Lahmadi, maître de conférences à l'Université de Lorraine, par ailleurs chercheur au LHS.

Plus de 210 chercheurs et 120 doctorants travaillent chaque année sur place. Mais deux équipes sont plus assidues. La première fait partie du département « Resist » du Loria. Ses membres imaginent des modes de supervision nouveaux pour les réseaux et services dynamiques. Baptisée « Carbone », une autre équipe développe des méthodes formelles de détection des menaces grâce à des algorithmes intégrant des modèles mathématiques complexes qui permettent aux machines d'anticiper l'évolution des logiciels malveillants. *« Actuellement, la plupart des antivirus traquent les malwares une fois que ceux-ci ont été identifiés. Nous développons des outils qui les repèrent avant qu'ils aient sévi »*, indique Frédéric Beck, ingénieur de recherche à l'Inria, qui développe avec Abdelkader Lahmadi un projet de start-up destiné à sécuriser les objets connectés. Ils constituent une porte d'entrée royale dans les systèmes pour les pirates informatiques.

Pour ce faire, les chercheurs scrutent les activités suspectes dans les machines potentiellement infectées. *« Pour rester le plus furtifs possible, les virus décomposent leur*



**Traçage.** Frédéric Beck, ingénieur de recherche à l'Inria, analyse les lignes de code toxiques archivées par le laboratoire.

« Certains virus sont souvent habillés, pour ne pas dire déguisés, en autre chose. »

**Fabrice Sabatier,** ingénieur au CNRS qui travaille à l'Inria

## Pegasus, une vieille connaissance…

Les équipes du Laboratoire de haute sécurité (LHS) ont repéré le code espion Pegasus dès 2017. *« Cette version ancienne de ce logiciel développé par le groupe NSO visait clairement à infecter les ordinateurs et à en extraire des données »*, se remémore Fabrice Sabatier, chercheur au CNRS, détaché au Loria. *« Même si ce n'est pas à proprement parler un virus informatique mais un programme commercialisé par une entreprise, il se comporte indéniablement de manière malveillante en infiltrant téléphones et serveurs par le biais de vulnérabilités »*, complète Jean-Yves Marion, directeur du Loria. Pour protéger les machines, plusieurs chercheurs du LHS ont développé des start-up spécialisées en cybersécurité. La première, Lybero, fondée en 2016, entend créer un environnement numérique sanctuarisé comme une *« boîte à secrets inviolable »*, expose Jean-Yves Marion. Une autre, immatriculée en 2017 sous le nom Cyber-Detect, propose un dispositif de détection avancée des fichiers exécutables malveillants. *« Nous les repérons avant qu'ils aient pu éventuellement extraire des informations sensibles d'une machine »*, indique Régis Lhoste, son président. Ces deux entreprises comptent parmi leurs clients diverses administrations publiques, dont la Direction générale de l'armement et plusieurs acteurs clés de la défense nationale. En septembre, un partenariat devrait être annoncé entre le LHS et le groupe français Wallix dans le but de renforcer encore ces savoir-faire. Et une troisième start-up devrait voir le jour autour d'une technologie baptisée Scuba. *« Un outil qui permet de cartographier les vulnérabilités exploitables des systèmes d'information, autant de failles utilisées par les hackeurs comme points d'entrée »*, révèle son cocréateur, Abdelkader Lahmadi ■ **B. E.**

CHRISTIAN MOREL/INRIA - CYBER-DETECT

*progression dans les systèmes d'information en une multitude de mouvements, a priori insignifiants. C'est quand on les met bout à bout qu'on se rend compte de leurs intentions malignes »*, explique Jean-Yves Marion. Ses équipes apprennent aussi à percer les tenues de camouflage que revêtent parfois ces programmes malveillants. *« Certains virus sont souvent habillés, pour ne pas dire déguisés, en autre chose. Mais leur biomorphologie nous permet de retrouver leur squelette, et donc leur vraie identité »*, décrypte Fabrice Sabatier. Le reste du temps, les informaticiens se glissent dans la peau des hackers et testent les failles des machines pour voir où cela peut les conduire. C'est ainsi que les chercheurs lorrains sont parvenus à pointer les fragilités des clés de chiffrement, qui sécurisent aujourd'hui la plupart des transactions bancaires. Mais aussi à exposer les défaillances des systèmes de vote électronique de la mairie de Moscou ! Ce qui explique que les universités étrangères se pressent aujourd'hui à leur porte dans l'espoir de nouer des collaborations ■

## Comment sont isolés les virus informatiques

**Pots de miel**
Les chercheurs du LHS ont disposé sur la Toile mondiale des dizaines de pièges à virus. Ces *honeypots* (ou « pots de miel »), selon leur terminologie, leurrent les attaquants en se faisant passer pour d'inoffensifs ordinateurs. Les hackers y déposent leurs malwares.

**Trous noirs**
Les logiciels malveillants sont « aspirés » à travers un trou noir, pour se retrouver sur les serveurs du campus de Vandœuvre-lès-Nancy. Ils ne peuvent a priori plus en ressortir.

**Éprouvettes**
Les virus informatiques sont examinés à la loupe dans un environnement sécurisé, comme in vitro. Leur code source est analysé et comparé avec les échantillons déjà connus.

**Bacs à sable**
Les logiciels malveillants dont on veut apprendre à connaître les propriétés peuvent être exécutés dans une *sandbox*, un « bac à sable » déconnecté du reste du réseau.

Sources : Loria, Inria, CNRS.

ILLUSTRATIONS : TARTRAIS POUR « LE POINT » (X5)

## L'effroyable bestiaire de Nancy

Parmi les virus informatiques conservés sur le campus lorrain, certains constituent de véritables bijoux technologiques, capables de pénétrer les serveurs les plus sécurisés et d'y demeurer, invisibles, pendant des mois, voire d'effacer les traces de leur passage…

**Trisis**
De facture iranienne, ce malware a été retrouvé en août 2017 dans les réseaux informatiques de plusieurs groupes pétroliers. Ce virus peut prendre le contrôle d'une raffinerie et lui causer des dommages irréversibles. En 2012, son grand frère, baptisé Shamoon, dont la paternité est également attribuée à Téhéran, avait mis hors service près de 30 000 ordinateurs en Arabie saoudite.

**Emotet**
Ce cheval de Troie, repéré en 2014, avait été conçu, initialement, pour récupérer les données bancaires des internautes. Repérant les codes d'accès aux services financiers en ligne, il a permis de détourner d'importantes sommes d'argent pendant plusieurs années. Ce logiciel malveillant a, depuis, été sophistiqué. Il ne se contente plus de conduire des braquages numériques, mais espionne les machines, tous azimuts, ciblant les listes de contacts des utilisateurs comme le contenu des pièces jointes attachées à leurs courriels.

**Regin**
C'est un « couteau suisse » du cyberespionnage : un programme capable d'infecter des serveurs télécoms pour écouter les conversations, mais aussi d'intercepter mails et documents confidentiels. Découvert en Belgique, fin 2013, ce malware très discret (retrouvé dans les machines de plusieurs institutions européennes) a, selon plusieurs sources, été développé par la National Security Agency (NSA) et le Government Communications Headquarters (CGHQ).

**Mirai**
Découvert en 2016, ce code malveillant a pour objet de prendre le contrôle d'objets connectés à travers le monde. Des milliers de caméras de surveillance ont ainsi été détournées de leur usage pour conduire des attaques par « déni de service » (DDoS) contre de grandes compagnies – bloquant ainsi leurs activités.

**WannaCry**
Présenté, à son apparition en 2017, comme un ransomware, ce virus a infecté en quelques heures près de 300 000 machines dans plus de 150 pays. Conçu par un groupe cybercriminel nord-coréen, baptisé Lazarus, ce malware n'était-il pas tout simplement une cyberarme de destruction massive ? Les ingénieurs informatiques le pensent de plus en plus. Le groupe de hackers russes REvil a en effet recouru au même outil pour attaquer 1 500 groupes industriels américains, début juillet.