SCIENCES ET AVENIR
33 RUE VIVIENNE
75002 PARIS - 01 44 76 92 31

MARS 13
Mensuel
OJD : 256530

Surface approx. (cm²) : 1292
N° de page : 76-78

Les futurs experts de la cyberguerre

A Laval, des élèves d'une école d'ingénieurs se forment à la guerre informatique. Objectif : protéger les entreprises et les services de l'Etat contre l'espionnage en adoptant la « vision » de l'attaquant.

« **Quand je vois** *ce que je suis capable de faire avec un ordinateur à seulement 21 ans, je trouve ça inquiétant !* » Dire que Valentin peut tout faire depuis son clavier est, en effet, à peine exagéré. Elève ingénieur de l'Ecole supérieur d'informatique, électronique, automatique (ESIEA) de Laval (Mayenne), il est d'ores et déjà considéré comme un expert de l'infiltration informatique et fait partie de l'élite de sa promotion qui comprend 200 étudiants. Leur spécialité : la « cyberguerre » ou comment prendre le contrôle à distance d'un ordinateur, aussi protégé soit-il.

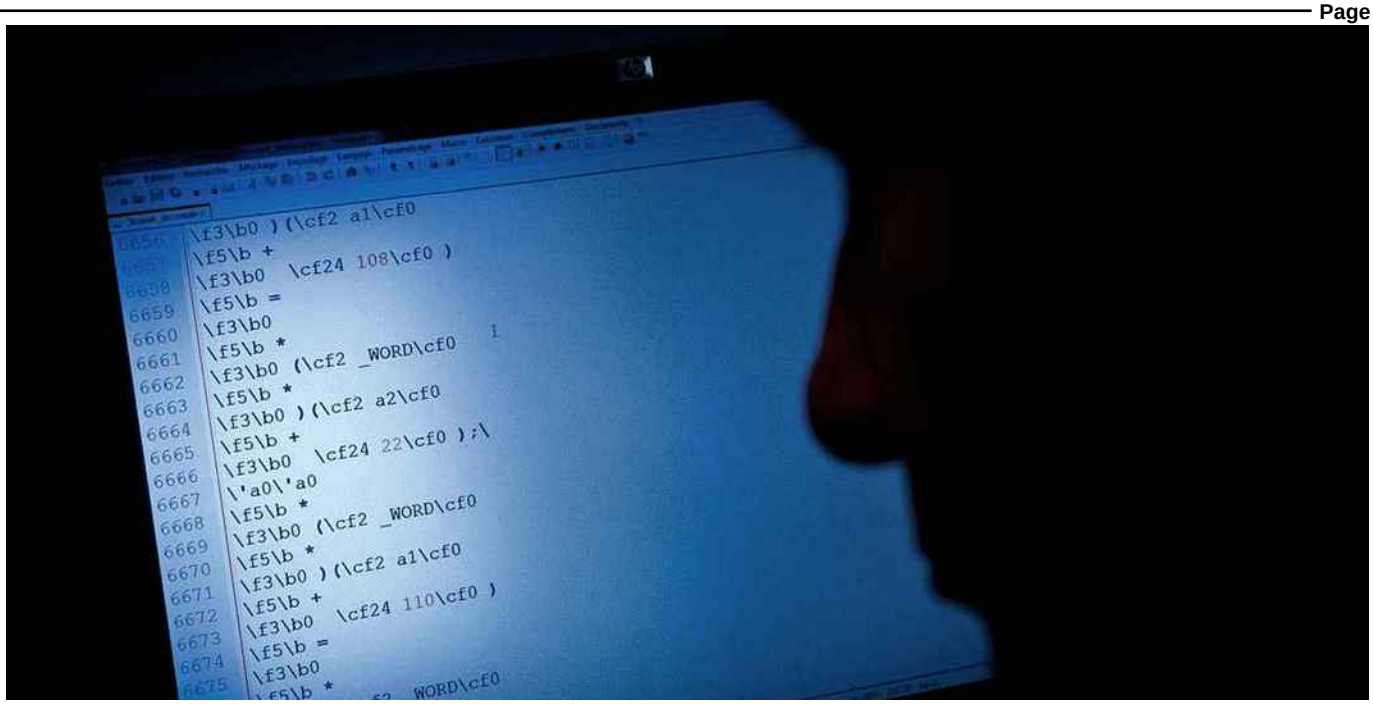
Repérés dès le début de leur cursus, ces étudiants de choc ne se contentent pas de suivre les enseignements « classiques ». Habilités « confidentiel défense » par le ministère, ils participent tous en parallèle aux recherches hautement sensibles de l'école au sein du Laboratoire de cryptologie et virologie opérationnelles sous tutelle de la Défense et sous contrat avec des grandes entreprises du secteur comme DCNS. Objectif : former, en cinq à six ans d'études (master et master spécialisé), des experts de la guerre informatique, capables de parer les attaques les plus innovantes pour protéger les entreprises et les services de l'Etat contre l'espionnage informatique. Mais aussi, et c'est là l'originalité de cette formation unique en France, de les concevoir. « *Notre credo est d'élaborer une défense en prenant le point de vue de l'attaquant. Nous formons des spécialistes des "cyber-armes"*, affirme ainsi Eric Filiol, ancien lieutenant-colonel de l'armée de terre, directeur scientifique de l'ESIEA et patron du laboratoire de cryptologie et virologie opérationnelles qui défend cette approche offensive de la sécurité numérique. *Chaque élève doit apprendre à maîtriser tous les volets d'une attaque : phase de renseignement, planification, élaboration des scénarios et enfin, conduite de la manœuvre, c'est-à-dire l'attaque proprement dite.* »

Selon nos sources, en France, les services de l'Etat subiraient plus de 1000 attaques critiques chaque année. Et la cybercriminalité coûterait près de 2,5 milliards d'euros par an, selon l'étude Norton Cybercrime Report, publiée en septembre 2012 par l'éditeur d'antivirus Symantec (1). La cyberdéfense a donc été désignée comme une priorité nationale dans le rapport du sénateur Bockel (2) paru en juillet 2012, qui met l'accent sur le fait que des pays comme les Etats-Unis ou la Chine se sont déjà dotés de moyens importants dans ce domaine. Ces derniers mènent régulièrement des attaques ciblées censées protéger leurs

SCIENCES ET AVENIR
33 RUE VIVIENNE
75002 PARIS - 01 44 76 92 31

MARS 13
Mensuel
OJD : 256530

Surface approx. (cm²) : 1292
N° de page : 76-78



Au laboratoire de cryptologie et virologie opérationnelles de l'ESIEA (à gauche), les élèves ingénieurs analysent des virus de style Stuxnet (ci-dessus).

intérêts, y compris contre des pays « amis ». Ainsi, les Américains sont-ils soupçonnés d'être à l'origine de l'attaque retentissante contre les services de l'Elysée, menée au cours de l'été 2012 pour s'emparer de documents confidentiels.

« La France se met donc avec prudence et retard à la cyberguerre », affirme Eric Filiol qui justifie ainsi l'approche offensive de l'ESIEA, véritable « camp d'entraînement » des forces spéciales de l'Internet. *« Nous leur apprenons à concevoir des virus* [lire les Repères] *très avancés, qui sont ensuite testés en milieu confiné, c'est-à-dire sur des réseaux de PC non connectés avec le monde extérieur pour éviter toute fuite »*, explique Eric Filiol. Ces exercices d'attaque sont souvent menés sur des réseaux simulant des installations critiques comme celles de centrales nucléaires, cibles potentielles de cyber-agressions *(lire l'encadré p. 78)*.

Eric Filiol, directeur scientifique de l'ESIEA

Ces infrastructures virtuelles fonctionnent, comme dans la réalité, avec leur trafic de données (courriels, Web, télémaintenance, etc.) dotées des multiples protections censées les mettre à l'abri de toute intrusion. Les étudiants sont ainsi formés à les analyser, à chercher les failles et à les attaquer. L'arsenal qu'ils utilisent pour y parvenir comporte des virus mutants indétectables qu'ils ont spécialement développés. Ceux-ci échappent à tout contrôle en réécrivant eux-mêmes leur code *(lire les Repères)* toutes les secondes ou lorsqu'ils passent d'un ordinateur à l'autre. De fait, les antivirus, qui fonctionnent essentiellement en reconnaissant des bouts de code malveillants déjà connus et analysés, restent impuissants à les repérer. L'intervention de ces derniers est d'autant plus vaine que, au contraire des virus les plus « classiques », ceux mis au point au sein du laboratoire disposent de codes chiffrés qui rendent leur analyse très difficile, voire impossible. On ne peut en effet les « lire » sans la bonne clé de chiffrement. Or, tester toutes les clés possibles exigerait 10 milliards de siècles à un puissant PC…

Autre arme conçue à l'ESIEA : le virus mimétique. Sa force est de se faire passer pour un logiciel légitime, un inoffensif traitement de texte par exemple. L'antivirus ne voyant aucune menace, le laisse infecter librement les machines ciblées. Tout aussi malin, le virus « invisible » : lorsque l'antivirus, ou un utilisateur spécialiste en sécurité informatique, cherche à analyser les fichiers à risque, le virus fournit lui-même une liste de tous les fichiers suspects… dans laquelle il ne figure pas !

La difficulté pour rendre de telles armes opérationnelles est de les installer au préalable sur les ordinateurs ou les smartphones ciblés. Des techniques qui, là encore, se perfectionnent lors du cursus de formation des cyberattaquants. L'une des stratégies consiste à envoyer aux cibles des courriels « vérolés ». *« Grâce au logiciel que j'ai élaboré, je peux abaisser la vigilance du destinataire en lui donnant l'illusion que le courriel provient, par exemple, de l'un de ses collègues »*, explique Baptiste, l'un des étudiants. *« Le courriel peut contenir en pièce jointe un document PDF dans lequel se trouve le virus qui va s'infiltrer dans la machine »*, poursuit Valentin. Le jeune apprenti ingénieur a développé de nouvelles techniques pour piéger ces fichiers de bureautique parmi les plus couramment échangés et lus par le logiciel Acrobat Reader. Il utilise pour ce faire des virus extrêmement petits, composés de quelques lignes de code à

REPÈRES

CODE OU CODE SOURCE : texte écrit dans un langage de programmation pour donner à l'ordinateur les instructions à suivre (programme). Il est ensuite traduit en code binaire (succession de 0 et de 1). Un virus, comme un programme, est constitué d'un code source écrit par son concepteur.

VIRUS : ce terme regroupe l'ensemble des différents types de menaces : virus, ver, cheval de Troie… Au sens strict, les virus sont des programmes cachés dans un autre programme (traitement de texte, tableur…) qui s'installent sur des ordinateurs, smartphones et tablettes afin d'exécuter les opérations souhaitées par son concepteur (vol de données, prise de contrôle de l'ordinateur à distance, etc.). Certains codes malveillants ne sont pas dissimulés dans un autre programme. Ce sont des « vers » informatiques.

ANTIVIRUS : logiciels visant à détecter et à supprimer les virus informatiques. Ils fonctionnent essentiellement en identifiant des bouts de codes appartenant à des virus connus.

SCIENCES ET AVENIR
33 RUE VIVIENNE
75002 PARIS - 01 44 76 92 31

MARS 13
Mensuel
OJD : 256530

Surface approx. (cm²) : 1292
N° de page : 76-78

D'inquiétants cybersaboteurs

Stuxnet est un code malveillant identifié en juillet 2010 par la société de sécurité informatique biélorusse VirusBlokAda. Véritable cyber-saboteur, il ciblait exclusivement les automates conçus par Siemens et pilotant les centrifugeuses destinées à enrichir l'uranium des centrales nucléaires iraniennes. L'objectif était d'en perturber leur fonctionnement jusqu'à les détruire. Très sophistiqué, il exploitait sept failles du système ciblé, dont quatre « Zero-days », c'est-à-dire des failles jusqu'alors inconnues. Or, les Zero-days sont très rares. Seules sept ont été recensés cette année-là dans le monde entier. Autre particularité de Stuxnet, sa taille importante : 600 ko, contre 15 ou 20 pour un virus classique. De plus, afin de compliquer son analyse, il comportait de nombreux pièges, notamment des « bouts » de codes n'ayant aucune fonction particulière, sinon d'égarer les analystes, et livrait des informations mystérieuses, sans doute volontairement erronées. *« Il mentionnait une date dans son code à laquelle nous n'avons jamais pu donner un sens »*, explique Laurent Heslault, directeur des stratégies de sécurité chez Symantec. Quant à Flame, il rassemble tout ce qui est imaginable en matière d'attaque : vol de documents, copies d'écran, écoute par le micro de l'ordinateur ou encore enregistrement des frappes sur le clavier. Découvert en mai 2012, il a servi pendant plusieurs années à des attaques très ciblées sur des particuliers ou des entreprises, essentiellement au Moyen-Orient. Ce « virus » a une particularité, il est énorme : environ 20 Mo, soit quarante fois plus que Stuxnet. Mais le mystère reste entier sur son origine : seul le laboratoire hongrois CrySys et les sociétés d'antivirus Kaspersky et Symantec ont pu l'analyser. Des experts internationaux, comme Eric Filiol, patron du Laboratoire de cryptologie et virologie opérationnelle de Laval, émettent des doutes sur l'existence même de ce super virus, refusant de croire les fabricants d'antivirus sur parole et craignant une opération d'« intox ». *« Certains de mes étudiants ont assisté à une formation sur Flame proposée par CrySys aux Pays-Bas. Or, ils n'ont jamais eu accès à la moindre ligne de code. C'est inédit. Pourquoi ce code n'est pas rendu public ? Tant que nous n'aurons pas vu le code de Flame, nous refusons de croire à son existence comme il est décrit. Nous sommes prêts à l'analyser pour l'Etat français dans des conditions sécurisées "confidentiel défense" »*, suggère Eric Filiol.

peine, afin de s'infiltrer dans les moindres failles du logiciel. Toute l'astuce réside dans le fait que ces minivirus, une fois installés, ont une seule mission : obliger les machines infectées à télécharger des virus de plus grande taille, disposant, eux, de nombreuses fonctionnalités dont celle de mener une attaque d'envergure. *« Dès lors, je n'ai plus de limites dans l'ampleur de l'offensive ! »* précise Valentin. Il peut prendre le contrôle de la Webcam de l'ordinateur cible, extraire les fichiers, intercepter les courriels ou envoyer des messages piégés à tous les contacts du carnet d'adresses pour contaminer d'autres machines…

Dorian a lui aussi intégré le Laboratoire en tant qu'étudiant. Sa spécialité : le « computer forensic » ou l'informatique légale, c'est-à-dire toutes les techniques mises en œuvre par les services de police et de renseignement pour enquêter sur des données numériques. Par exemple, l'analyse du disque dur de l'ordinateur d'un suspect pour récupérer des fichiers qui auraient pu être effacés. Mais Dorian sait aussi comment mettre en place des techniques beaucoup plus « offensives » : *« Je peux prendre le contrôle à distance d'un ordinateur ou d'un smartphone pour y injecter de faux documents pouvant servir de preuves : photos compromettantes ou fichiers sensibles. Je peux aussi créer de faux échanges de SMS sur les téléphones. C'est indétectable. Policiers et magistrats n'y verraient que du feu ! »* Quelques instants lui suffisent pour brancher son PC portable sur le téléphone laissé sans surveillance. Même si le smartphone est éteint ou verrouillé par un mot de passe et un code pin, les codes malveillants s'insèrent dans toutes les applications (jeux, GPS, appareil photo, éditeur de SMS…) sans que le fonctionnement de l'appareil en soit affecté.

En quelques secondes, ce boîtier aspire les données d'un smartphone.

Une attaque perfectionnée par Thibaut, autre étudiant : il a conçu un dispositif gros comme un paquet de cigarettes qui permet de s'émanciper du PC portable. En quelques secondes, celui-ci prend le contrôle du smartphone, aspire son contenu et y injecte des données compromettantes. Pour l'heure, ce prototype, dont le mode de fonctionnement est gardé secret, exige encore un contact physique avec le téléphone, le temps d'opérer l'échange de données. Mais Thibaut travaille sur une version sans fil pour piratage à distance. Et pour éviter de se faire repérer pendant ces opérations spéciales, le jeune ingénieur a conçu en équipe plusieurs systèmes capables de brouiller, aveugler ou détruire à distance les caméras de vidéosurveillance. Les modalités techniques de leur fonctionnement seront dévoilées lors de la conférence Hack in Paris qui aura lieu du 17 au 21 juin.

L'une de ces technologies permet ainsi de masquer un visage sur l'image captée par une caméra grâce à un dispositif implantable sur une simple casquette. Une casquette bien plus discrète qu'une cagoule et indispensable pour mener des intrusions dans les salles informatiques d'une entreprise ou d'une administration. De fait, aussi paradoxal que cela puisse paraître, ces experts en cyberattaques sont aussi formés aux techniques d'effraction « conventionnelles ». Un spécialiste du crochetage des serrures vient ainsi former les étudiants à l'art de pénétrer dans des locaux fermés. *« La cyberattaque peut commencer par là : à quoi bon mettre des antivirus et autres systèmes de protection sur des serveurs si l'attaquant peut accéder directement à la salle informatique en crochetant une porte ? »* s'amuse Eric Filiol. Même en pleine cyberguerre, les vieilles méthodes ont toujours la cote.

Olivier Hertel
Photos : Dung Vo Trung/ Lookatsciences pour Sciences et Avenir

(1) http //2doc net/2v2rr
(2) http //2doc net/p8ugg