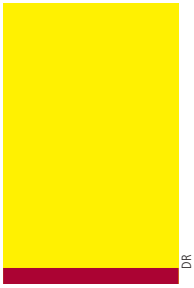
Menaces sur la sécurité informatique

Une importante cyberattaque a frappé de plein fouet de nombreux ministères en France. La Bourse de Paris et une grande banque font face à une agression sans précédent. Science-fiction ? Evidemment, car en France, à la manière du nuage de Tchernobyl, il semble que tout s'arrête à nos frontières !



DR

Eric Filiol
Directeur du laboratoire de virologie et de cryptologie opérationnelles de l'ESIEA Laval (Ecole supérieure d'informatique électronique automatique).

Quels sont les véritables risques en matière de criminalité informatique ?

Eric Filiol > Les atteintes envisageables concernent la confidentialité des informations et des données, leur intégrité et leur disponibilité. Mais une évolution récente de la cybercriminalité y ajoute désormais l'incrimination à tort de tiers innocents dans la réalisation d'un crime ou d'un délit. Ces risques sont bien réels et si la confidentialité des données (que la plupart des utilisateurs assimilent à tort à la protection de la vie privée, mais n'en est qu'un aspect réduit) est un risque à peu près connu du plus grand nombre, les deux autres le sont moins.

Pouvez-vous nous donner des exemples ?

E F > De nombreux professionnels de la vente en ligne sont persuadés de ne pas être une cible car aucune donnée confidentielle n'est présente sur leur site, alors que leur cœur de métier réside justement dans la disponibilité de ce site. Une attaque par déni de service sera alors plus efficace qu'un vol de données. Il s'agit là des « briques de base », mais leur combinaison peut être autrement plus redoutable et permettre un grand nombre d'actions. Imaginez le dépôt de photos pédophiles par un pirate sur l'ordinateur d'une personnalité, combiné à la manipulation de son téléphone mobile pour créer de toutes pièces des communications avec des pédophiles ! Ou, à plus grande échelle, l'attaque de la Chine contre les serveurs de la communication de défense taïwanaise en juin 2006, la manipulation des populations, des cours de la Bourse… Tout cela est techniquement possible.

A vous entendre, plus que la fin d'un monde, Internet serait la fin du monde !

E F > Non, c'est la fin de notre monde à nous, avec nos certitudes et notre façon de vivre. Aujourd'hui, nous pensons être protégés par la sagesse des juges et la notion de la preuve, mais demain, il n'y aura plus de preuves tangibles puisque tout pourra être falsifié. C'est un changement complet de repères. La notion de préjudice changera. Hier, faire un hold-up dans une banque réclamait du temps et des moyens. Maintenant, en un simple clic, vous pouvez détourner des millions de cartes bleues. Non seulement, nous assistons à une accélération du temps, mais à une amplification des moyens.

Sommes-nous tous égaux face à ces attaques ?

E F > Il faut relativiser la réalité et la portée de ces attaques en fonction de notre dépendance vis-à-vis des systèmes d'information et de communication. Un pays comme l'Estonie, dont les services gouvernementaux sont informatisés à 90%, est ainsi beaucoup plus vulnérable que la Géorgie, par exemple. Pour preuve, la paralysie totale de ses services pendant trois semaines en 2007.

Réaliser le casse du siècle, *provoquer des émeutes ou bloquer les cotations boursières…* ***d'un simple clic****.*

Le risque est donc fortement proportionnel à cette dépendance. A la suite de ce problème, les Estoniens ont demandé que soit créée une commission européenne sur le sujet. Face au silence de la Commission européenne, seule l'OTAN a répondu présente pour créer en son sein une cyberdéfense. Pourquoi la France a-t-elle refusé d'y participer ? Pourquoi n'est-elle pas active au niveau européen ? Pourquoi est-elle également absente au niveau international dans les grands organismes de standardisation comme la WebForce International Federation (ITU) ? Alors qu'elle a subi l'année dernière six cents attaques majeures au niveau du gouvernement, soit deux par jour, et sur des sites d'une sensibilité extrême.

Il n'y a aucun moyen technique d'empêcher les attaques ciblées.

Pourtant, nous avons créé l'Agence nationale de la sécurité des systèmes d'information dirigée par Patrick Pailloux !

E F > Disposer d'agences spécialisées et d'une communauté académique de pointe est une condition nécessaire, mais nullement suffisante. C'est tout ce qui fait la différence entre des pays comme l'Allemagne ou les Etats-Unis et la France, qui, de ce point de vue, accuse un retard de plus en plus préoccupant. Simplement, parce que la France fait de la sécurité une affaire réservée aux « élites ». Lesquelles sont complètement décorrélées de la réalité et n'ont aucune idée de ce qu'il est possible de faire techniquement. Hors des grands concepts, elles sont perdues face à la réalité du terrain.

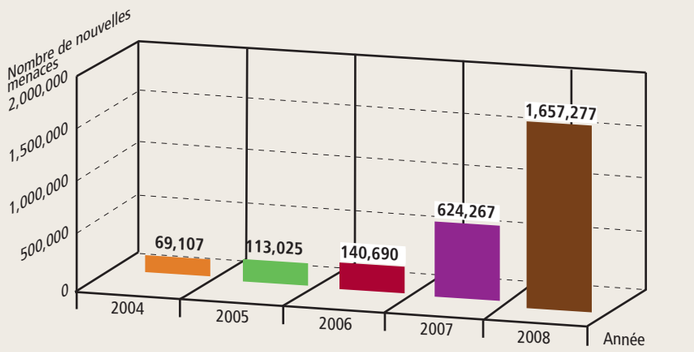
Chez nous, si vous n'êtes pas normalien ou polytechnicien, n'espérez pas pouvoir contribuer au débat, quelle que soit votre compétence technique. Je connais un jeune titulaire de BTS informatique qui « parle » assembleur couramment, c'est-à-dire qu'il peut faire sauter n'importe quelle application. Le gouvernement a souhaité l'embaucher, mais, compte tenu de son niveau d'études, Bac+2, il entrait dans la catégorie des fonctionnaires C, soit un salaire de 1 100 euros par mois. Aussi, lorsque les Américains, qui connaissaient également sa valeur professionnelle, lui ont proposé 6 000 euros par mois tout en restant en France, devinez où il est allé !

Je peux vous citer des dizaines de cas comme celui-là. Le résultat, c'est que ces jeunes informaticiens et hackers français partent à l'étranger ou travaillent pour des sociétés étrangères en France. Notre pays est ainsi privé d'une ressource critique précieuse.

Existe-t-il un autre gros facteur de risque ?

E F > L'autre grand risque, c'est l'interconnexion frénétique et interdépendante des réseaux dont il est aujourd'hui impossible de dresser la cartographie complète et exacte.
Il est, par exemple, terrifiant de découvrir qu'une centrale nucléaire américaine est connectée au réseau Internet pour la télémaintenance et que son réseau informatique a été paralysé en janvier 2003 par le ver Slammer. Plus l'interconnexion est riche, plus le risque augmente. Ainsi, pour attaquer une cible principale, qui est probablement protégée, il suffit de créer un effet domino en attaquant des systèmes dont cette cible dépend mais qui, eux, ne sont pas protégés. Il est donc clair que les pays les plus fortement informatisés sont les plus vulnérables. De manière plus large, tout repose sur un point critique : la dépendance vis-à-vis de standards et de produits extranationaux. Notre sécurité, celle de nos entreprises et de nos foyers, repose encore essentiellement sur des produits étrangers, fermés, des services souvent délocalisés (par exemple, la supervision des réseaux téléphoniques ou la réalisation de nos applications logicielles, certaines sensibles) et des standards douteux… Le risque est donc de sous-traiter notre sécurité. Se contenter d'une gestion de la sécurité fondée sur la politique de la rustine (attendre le prochain correctif) est une absurdité.

Nombre de nouveaux codes malveillants dans le monde



Source : Symantec

Quelles différences faites-vous entre des attaques génériques et ciblées ?

E F > Dans le premier cas, l'attaque peut faire des dégâts, mais on finit par la détecter et la gérer (c'est le cas d'une attaque par un ver comme Conficker). On ne peut l'éviter, mais son niveau technique est relativement faible. Il est donc possible de se protéger. Dans le second cas, les attaques ciblées, le risque est maximal. Il n'y a aucun moyen technique pour les empêcher, les détecter et lutter contre. Il s'agit d'attaques de faible envergure (en termes du nombre de cibles), d'un niveau technique élevé à très élevé et visant des ressources à haut potentiel économique ou humain, pour un préjudice maximal. La victime ne saura sans doute jamais qu'elle a été attaquée. Toutes les solutions de sécurité seront inutiles. A titre d'exemple, nous avons participé en 2004 à une expertise technique dans une entreprise française très sensible, qui avait été victime d'espionnage. L'étude de leur système informatique a montré qu'effectivement un virus espion avait été installé sur tous les postes de la direction. Malgré les antivirus en place et le pare-feu, le code exfiltrait des données vers l'extérieur. Cinq ans après, ce fameux virus, que nous avons éliminé, est toujours indétectable par les antivirus actuels. Son analyse a montré que sa fabrication complexe était probablement d'origine étatique étrangère.

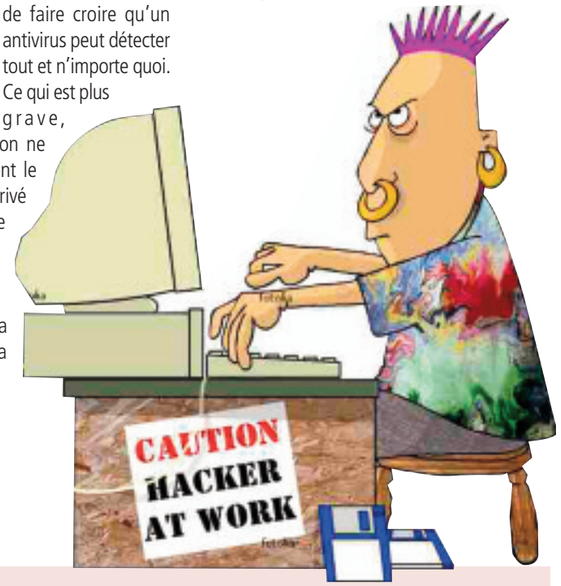
600 attaques majeures au niveau du gouvernement français en 2008.

Les responsables des services informatiques sont-ils suffisamment informés ?

E F > Non malheureusement ! La plupart des services informatiques sont complètement démunis. En plus de la surcharge de travail interdisant une veille technologique sérieuse, la réduction des coûts se traduit très souvent par une réduction du nombre de personnes affectées à la sécurité des systèmes. Ce qui est une hérésie. Savamment entretenue, d'ailleurs, par les consultant et autres éditeurs d'applications de sécurité qui font de cette dernière une affaire de produits – ceux qu'ils ont à vendre –, alors qu'il s'agit avant tout d'un processus de pensée, au cœur duquel l'humain doit être placé. Rien n'est pire pour un officier de sécurité de passer après un consultant ou un VRP qui a vendu le produit miracle à un patron ou à un directeur des systèmes d'information. Le meilleur exemple est celui des antivirus : on sait que ce problème n'a pas de solution (on le dit mathématiquement indécidable) et que toute politique antivirale efficace relève du domaine de la politique de sécurité. Mais les vendeurs d'antivirus continuent de faire croire qu'un antivirus peut détecter tout et n'importe quoi. Ce qui est plus grave, c'est que cette situation ne concerne pas seulement le secteur économique privé générique, mais touche de plus en plus le secteur étatique et les sociétés dites sensibles. Notre laboratoire a ainsi été consulté il y a quelques semaines par une entreprise fabriquant des systèmes de contrôle d'accès pour des sites très sensibles en France (étatiques et/ou privés). Cette société voulait nous faire évaluer leur nouveau produit fondé sur la technologie Web 2.0. Nous avons refusé : ce choix technologique était incompatible avec la notion même de sécurité, surtout pour un aussi haut niveau de sécurité.

Comment sensibiliser tout le monde à la sécurité informatique ?

E F > Sans un accès libre, ouvert et total, aucune information et sensibilisation n'est véritablement possible. Or, de nos jours, le travail de hacker ou de chercheur en sécurité est devenu extrêmement difficile, pour ne pas dire impossible.



Hacker ou cracker ?

Un hacker est une personne qui plonge au plus profond d'un système (logiciel, matériel, concept) pour l'étudier à fond, en comprendre les mécanismes intimes et, donc, être capable d'identifier des faiblesses conceptuelles d'implémentation ou d'utilisation. Du fait de cette capacité à aller au-delà des apparences et d'identifier les zones de faiblesse, le grand public confond le hacker avec le pirate ou le cracker qui, eux, utilisent ce type de connaissances et d'outils à des fins malveillantes et malhonnêtes. Le hacker est généralement un activiste, dans la mesure où il utilise ses connaissances et ses compétences dans le cadre d'une démarche citoyenne. Sa démarche vise à identifier les déficiences d'une technologie donnée dès lors qu'elles peuvent avoir un impact sur la vie des utilisateurs et, plus largement, des sociétés, et à les rendre publiques afin, d'une part, de sensibiliser les utilisateurs et les pouvoirs publics et, d'autre part, d'empêcher les attaquants de profiter de ces vulnérabilités du fait de l'ignorance générale.

Identifier une faille ou une vulnérabilité suppose de recourir à des techniques souvent condamnées. Les rendre publiques, publier des résultats, devient punissable par la loi (en France, le renforcement de l'article 323 du code pénal par la loi pour la confiance en l'économie numérique rend potentiellement interdite toute publication de ce type). Tout cela pour protéger les éditeurs de logiciels et de systèmes ! Révéler une faille les oblige, en théorie, à la corriger, ce qui leur coûte cher. Si rien n'est su, qui les contraindra à effectuer cette correction ?
On comprend pourquoi les hackers tendent à devenir beaucoup plus discrets, privant les Etats d'une connaissance critique. Privés de cette connaissance, nos systèmes restent gravement vulnérables. Dernier exemple : la justice a condamné le magazine en ligne Zataz qui révélait les problèmes de sécurité informatique d'une société informée de cette faille et qui avait refusé de réagir. Le journaliste avait décidé que c'était de son devoir d'avertir les clients qu'ils couraient un danger potentiel.

En prenant l'exemple du Webtifada, une attaque contre des sites israéliens, peut-on imaginer inverser le cours d'une guerre au travers du Net ?

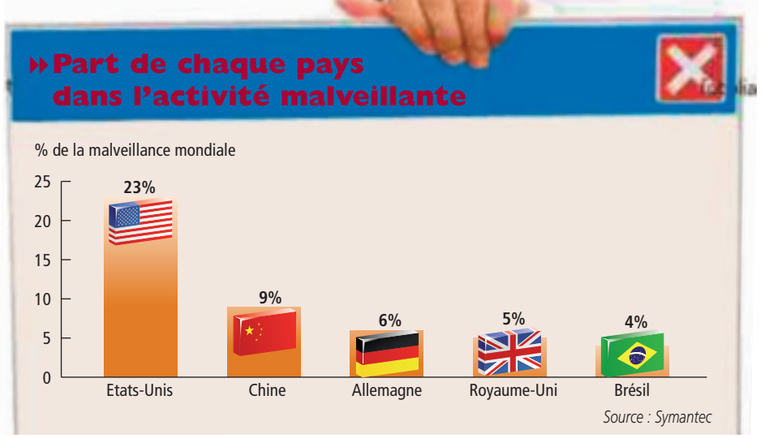
E F > Oui et de ce point de vue, les Etats modernes sont très en retard, alors qu'ils sont très vulnérables, ne serait-ce que par l'extrême dépendance de leurs sociétés vis-à-vis des réseaux et d'Internet.

Les attaques informatiques vont bien au-delà du simple « défacement » d'un site Web ou d'une attaque par déni de service (DDoS) visant à paralyser un serveur. Les atteintes aux personnes (diffamation numérique, incrimination à tort de tiers innocents) peuvent mettre hors service une personne critique, une personnalité importante (décideur, leader syndical, journaliste…) au moment opportun, alors que ces personnes sont un élément clef d'une attaque coordonnée. Provoquer des émeutes dans des zones sensibles en quelques clics de souris – ce fut le cas en France fin 2008, mais heureusement localisées – est un autre moyen. Il reste à combiner tout cela, exploiter l'incapacité des Etats à utiliser des solutions fortes pour des problèmes d'opinion publique et s'appuyer sur le volet informationnel (en particulier, les techniques InfoOps de l'OTAN) et vous aurez de quoi monter un thème tactique digne d'un très bon bureau de planification d'état-major. Mais il est important de conserver à l'esprit que l'informatique et nos réseaux ne sont pas une réalité indépendante de la sphère physique réelle. La guerre ou n'importe quelle attaque vise à obtenir un effet sur le terrain (contrôle de zones, appropriation de ressources, manipulation des esprits, atteinte contre la culture…) et toute attaque informatique ne sera qu'un maillon, le plus déterminant quelquefois, d'une attaque multi-niveaux. Prenons un exemple. En 2007, l'armée israélienne a bombardé des installations syriennes suspectées d'abriter un site de production de matière fissible (effet physique). Les services israéliens avaient rendu l'agression possible en attaquant informatiquement le système de surveillance syrien modélisant et surveillant l'espace aérien (espace de bataille numérisé). Cette attaque a permis de détourner certains capteurs pour ménager une sorte de corridor aveugle permettant aux pilotes israéliens de survoler la Syrie en toute sécurité. Un autre exemple concerne le renseignement, dont on sait la valeur stratégique dans un conflit ou une opération militaire.

> ***« C'est le syndrome de la porte blindée sur un mur en carton. »***

Une attaque informatique peut consister à acquérir ces renseignements et contribuer à inverser le cours d'une guerre. Il existe de nombreux exemples récents. Peu sont connus malheureusement. Mais si l'on comprend que le réseau Internet est devenu le carrefour de nombreux autres réseaux (téléphoniques, bancaires, même militaires comme en Afghanistan pour les Etats-Unis), la collecte d'informations est facilitée.

Part de chaque pays dans l'activité malveillante



Source : Symantec

Un cyberguerrier peut-il déclencher seul une attaque d'envergure ?

E F > Si on entend déclencher une attaque nucléaire, par exemple, la réponse est non, du moins tant que les réseaux sensibles concernés restent extrêmement sécurisés. Croisons les doigts pour qu'ils le demeurent. Mais, encore une fois, il faut élargir la notion d'attaque et de cible. Provoquer une panne électrique généralisée, bloquer tous les distributeurs de billets (en Estonie, en 2007), paralyser le trafic aérien (aux Etats-Unis, en 2007) ou ferroviaire (aux Etats-Unis, en 2003), provoquer des pertes graves de données sensibles (comme pendant l'été 2007, l'affaire d'espionnage qui a frappé la chancellerie allemande), provoquer des pollutions généralisées (en Australie, en 2006), bloquer les cotations d'une place boursière (à Moscou, en 2006 et à Londres, en 2007), provoquer des décès dans une unité de soins intensifs (dans les pays d'Europe de l'Ouest, en 2009)… tout cela est possible et ces attaques ont déjà eu lieu.

Sauf en France ! Les attaques informatiques, comme les nuages radioactifs, s'arrêtent à nos frontières !

Vous affirmez que dans le domaine numérique tout est falsifiable. Quid de l'e-administration, du vote numérique, du passeport biométrique ?

E F > Oui tout est falsifiable et les technologies que vous mentionnez sont vulnérables. Mais encore faut-il comprendre pourquoi elles le sont. Entre un concept de sécurité en apparence acceptable – mais qui n'a quelquefois jamais été prouvé, comme la plupart des mécanismes de cryptographie à clef publique — et son utilisation réelle dans un système, il y a un fossé.
Le meilleur exemple est celui de la cryptographie, à la base de tous les mécanismes de sécurité des systèmes que vous citez. C'est le syndrome de la porte blindée sur un mur en carton. L'attaquant se gaussera de votre porte et passera par le mur. Peu lui importe que le fabricant lui certifie que la porte est inviolable. Toutes les technologies mentionnées ont été attaquées et ces attaques présentées dans les plus grandes conférences de hackers. Jusqu'à la cryptographie quantique, pierre philosophale de la sécurité moderne, dont les différentes implémentations ont été récemment mises en défaut.
Certains concepts cohabitent mal avec la réalité : c'est ce qu'ont oublié nos élites. Affirmez à un hacker qu'un système de sécurité est impossible à contourner, et il s'acharnera à vous prouver le contraire, souvent avec une élégance confondante.
Les fabricants et les éditeurs (récemment, Apple avec l'iPhone) en font régulièrement la douloureuse expérience.
La véritable question est de savoir si nous avons réellement besoin de ces mécanismes numériques : il est sidérant que dans un pays comme la France où nous pouvons organiser des élections nationales en une journée et avoir une estimation très précise en quelques minutes et des résultats définitifs en une poignée d'heures, avec une confiance quasi totale (le bourrage d'urnes se voit tout de suite, l'équivalent numérique sera impossible à détecter, s'il est bien fait), on veuille un système de vote électronique pour une chose aussi sérieuse. Il est des domaines où l'homme doit rester seul maître. ■