Technique & Pratique

Sécuriser Windows

en 5 étapes

Benoît Chevalier
Ingénieur

Céline Chevalier
Élève de l'École Normale Supérieure

Emmanuel Cornet
Doctorant en informatique

Sébastien Desreux
Docteur en informatique

Alexandre Hérault
Enseignant dans le supérieur

Mickaël Profeta
Ancien élève de l'École Normale Supérieure

Avec l'aide précieuse de
Marie François et Deborah Levine

Avant-propos

Lorsqu'Internet a commencé à séduire le public, chaque éditeur de logiciels s'est précipité pour occuper le terrain en offrant, le premier, de nouveaux services, de nouvelles fonctions, de nouveaux gadgets. L'inventivité était la règle, et au diable les précautions.

Cette ruée nous a permis de disposer très rapidement d'outils adaptés à ce nouveau territoire qu'est Internet, mais elle a aussi légué d'énormes problèmes dans le domaine de la sécurité – toujours le premier laissé pour compte lorsqu'il faut arbitrer entre travailler vite et travailler bien.

Maintenant que ces logiciels sont là, il serait économiquement déraisonnable de les réécrire complètement pour qu'ils intègrent les impératifs de sécurité dans leur structure même. Alors les éditeurs, Microsoft en tête, distribuent des « correctifs de sécurité » comme autant de rustines posées sur une chambre à air qui doit affronter un univers beaucoup plus hostile que prévu. Car Internet ne facilite pas seulement votre quotidien et celui des banquiers des éditeurs de logiciels : c'est aussi un formidable outil pour disséminer toutes sortes de programmes malveillants.

L'enjeu de la lutte entre les pirates et les programmeurs de Microsoft, c'est votre vie privée, votre portefeuille, et votre ordinateur. Force est de constater que les premiers sont, hélas, toujours en avance sur les seconds.

Mais l'insécurité n'est pas une fatalité. Les outils qui font défaut à Windows pour assurer votre tranquillité sont disponibles chez d'autres éditeurs, parfois gratuitement. Comme beaucoup de choses en informatique, s'en servir est plutôt facile quand on sait le faire, et quasiment impossible sinon. Nous vous montrerons, en 5 petites étapes, comment les utiliser pour reprendre le contrôle de votre ordinateur.

Nous verrons notamment :

- comment interdire aux pirates l'accès à votre PC ;
- comment éradiquer les virus, vers, chevaux de Troie et autres logiciels espions ;
- quels programmes minent le plus votre sécurité et par quoi les remplacer ;
- quels sont les signes qui doivent inciter à la prudence sur Internet.

Toutes les démarches sont détaillées pas à pas et illustrées de nombreuses copies d'écran prises en situation réelle.

Nous vous invitons à utiliser dès le début de votre lecture le lexique situé à partir de la page 119. Il présente plus de 50 mots qui vous permettront de vous familiariser sans peine avec le vocabulaire informatique. Lorsque nous rencontrerons un nouveau terme, au fil de l'ouvrage, sa présence dans le lexique sera signalée par des PETITES CAPITALES.

Nous espérons que vous aurez autant de plaisir à lire cet ouvrage que nous en avons eu à l'écrire ; nous savons qu'il vous sera utile en pratique. Vos critiques comme vos éloges nous aideront à l'améliorer encore : vous pouvez en faire part à l'éditeur, à l'adresse

`contact@H-K.fr`

Si vous rencontrez ce que vous estimez être une erreur ou une imprécision gênante dans l'ouvrage, nous vous serions reconnaissants de nous en faire part également.

Bonne lecture !

Les auteurs

Table des matières

Faut-il vraiment sécuriser Windows ?

Emmanuelle D. est professeur d'histoire et géographie en collège. Il y a trois ans, elle s'est équipée d'un PC sous Windows pour l'aider dans son travail. Elle prépare ses cours et documents pédagogiques avec Word, et elle stocke dans une base Access les données qu'elle collecte pour la thèse qu'elle prépare en parallèle. Les gains de productivité dus à l'informatique sont pour elle une réalité quotidienne. Pendant trois ans, elle a été globalement satisfaite de son ordinateur.

Pendant l'été 2005, elle est entrée de plain-pied dans l'informatique du XXI^{e} siècle en se connectant à Internet en haut débit. Elle a choisi Wanadoo, un fournisseur d'accès réputé, et comme elle avait entendu parler des VIRUS, elle a souscrit un pack sécurité de la même marque. Elle ignorait malheureusement qu'elle devait aussi tenir son système à jour régulièrement. Les choses ont commencé à se gâter.

L'ordinateur est devenu plus lent. Des programmes qui se lançaient d'habitude presque instantanément prenaient plusieurs secondes supplémentaires. L'interface était moins réactive : il pouvait s'écouler un temps très perceptible entre un clic et son résultat. Des programmes ont ensuite montré un comportement erratique : sans raison apparente, ils annonçaient une *erreur générale de protection* ou faisaient des *opérations interdites*, voire disparaissaient de façon imprévisible. Un peu plus tard, c'est le système lui-même qui a souffert : Windows se figeait et devait être redémarré avec le bouton « On/Off » de l'ordinateur, ou affichait l'« écran bleu de la mort ».

Une semaine seulement après avoir été connecté à Internet, le PC d'Emmanuelle D. était totalement inutilisable : quelques secondes après le démarrage, Windows se figeait et ne répondait à aucune sollicitation. Sans l'aide d'un collègue enseignant et expert en informatique, tous ses cours et tout son travail de recherche auraient été perdus.

Cette histoire vraie n'est, hélas, pas isolée. Connecter son PC à Internet (en haut débit ou même par un modem classique) sans le protéger activement, ce n'est pas courir un risque, c'est le condamner de manière certaine.

Une protection partielle laisse, elle aussi, la porte ouverte à des désagréments, moins graves mais néanmoins pénalisants. Sur un ordinateur de test (sous Windows XP) protégé seulement par un PARE-FEU (soit la première de nos cinq étapes), nous avons rapidement constaté l'apparition de publicités surgissant à l'écran sans raison, d'icônes sur le bureau conduisant à des sites de casinos et à des sites pornographiques, le dérèglement de la page de démarrage d'Internet Explorer vers un site de poker en ligne, etc.

Les désagréments techniques ne sont pas les seules menaces, ni même les pires. En 2003, le virus Klez profitait d'un défaut d'Outlook Express pour envoyer au carnet d'adresses des passages choisis au hasard parmi les courriers reçus ou envoyés : parions que cela a causé des déceptions sentimentales et des problèmes de confidentialité en entreprise. Un autre donnait le contrôle total du PC à un PIRATE qui, à distance, pouvait déplacer le pointeur de la souris à votre place, sous vos yeux[1]. Nous verrons dans quelques pages d'autres menaces très réelles, comme les vols d'informations personnelles.

1. Ce qui permet à un pirate de faire exécuter toutes sortes de commandes à un ordinateur sous Windows, c'est que tous les utilisateurs ont les mêmes autorisations que l'administrateur de l'ordinateur. Une méthode simple et radicale pour se protéger serait de restreindre les autorisations des utilisateurs. Certains systèmes, comme Linux, le font. Malheureusement, Windows n'a pas été conçu dans cette optique et des fonctions très simples ne fonctionneraient alors plus correctement.

Cet ouvrage vous présentera pas à pas une solution complète pour mettre votre ordinateur sous Windows[2] à l'abri de toutes les menaces et, par conséquent, lui éviter le sort du PC d'Emmanuelle D. Pour bien appliquer ces méthodes, il faut bien comprendre les problèmes : la suite de ce chapitre va vous présenter les pirates, leurs objectifs et leurs outils.

Qui sont les pirates ?

En 1983, le film *WarGames* mettait en scène un petit génie de l'informatique qui, depuis sa chambre, piratait les ordinateurs de son école, puis ceux de l'armée américaine, sans que les meilleurs experts ne parviennent à le contrer. Depuis, de nombreux films ont opposé un adolescent surdoué aux réseaux les mieux défendus, au point d'en faire un thème classique. Si cette vision romantique du piratage est propice aux intrigues à sensations, elle n'a plus guère de rapport avec la réalité : le piratage à la papa a fait son temps[3].

Aujourd'hui, les pirates[4] n'attaquent plus directement des ordinateurs un à un. Ils écrivent des programmes qui vont attaquer pour eux, automatiquement, jour et nuit, méthodiquement, tous les ordinateurs connectés à Internet. Ce n'est plus un hobby mais une industrie de plusieurs milliards d'euros[5], contre laquelle le FBI américain mobilise son troisième poste

2. Il existe des systèmes beaucoup mieux sécurisés, tels que Linux ou OpenBSD. Le présent ouvrage, cependant, se limitera à Windows.

3. Les pirates isolés réalisant des exploits ciblés existent toujours, mais ils ne sont responsables que d'une infime partie des actes commis. Ces techniques restent en revanche d'actualité dans l'espionnage industriel.

4. Par « pirate » on entend une personne qui introduit des programmes dans votre ordinateur dans le but d'en prendre le contrôle. Ceci est complètement différent de la copie non autorisée de musiques et de films sans intention lucrative, même si les maisons de disques et Hollywood entretiennent (à dessein) la confusion.

5. Le ministère des finances américain évalue les bénéfices du « cybercrime » à 105 milliards de dollars en 2004, soit plus que ceux des trafics de drogue la même année.

de dépenses (après le terrorisme et le contre-espionnage). Au lieu d'adolescents rebelles, ils traquent en fait d'authentiques criminels organisés en mafias.

Un exemple parmi d'autres : le réseau *Shadow Crew*, démantelé en octobre 2004 aux États-Unis, réunissait 4 000 pirates. Lors des perquisitions, les enquêteurs (FBI et services secrets) trouvèrent deux millions de numéros de cartes bancaires, dix-huit millions d'adresses électroniques et de quoi usurper des milliers d'identités – ainsi que des fusils d'assaut chargés. Seules vingt-huit personnes purent être appréhendées : les autres pirates ne furent pas identifiés ou, tout simplement, habitaient dans un autre pays. Parmi ces vingt-huit, aucun n'était adolescent, aucun ne vivait en marge de la société. Le chef du réseau habitait tranquillement avec sa femme, ses deux enfants et sa mère.

Pourquoi s'intéressent-ils à *mon* PC ?

L'objectif premier des pirates, celui qui rendra possible tous les autres, est de prendre le contrôle d'un grand nombre d'ordinateurs. Pas du vôtre en particulier, mais de tous ceux qu'ils peuvent attraper, de manière aveugle et anonyme, donc notamment le vôtre. La force de frappe d'une équipe de pirates réside dans le nombre d'ordinateurs qu'elle contrôle.

Voici schématiquement comment ils s'y prennent. Le point de départ est de créer un petit programme capable de contourner les défenses de Windows afin de leur donner le contrôle à distance d'un PC. Il leur faut ensuite disséminer ce programme, ce qui peut emprunter plusieurs chemins : attaques au hasard, sites web infectés, virus joints à des courriers électroniques, programmes vérolés, etc. La troisième étape, enfin, est de faire travailler pour eux les ordinateurs conquis.

Ce schéma est si classique que des termes lui ont été associés. Ainsi, les programmes qui réalisent automatiquement

une infection sont appelés des BOTS[6], abrégé de « robots ». Un PC dont un pirate a pris le contrôle est un *zombie*. Un réseau de PC sous le contrôle d'une équipe de pirates est un *botnet* (abrégé de *robot network*, « réseau de robots ») ou une « armée zombie ».

En octobre 2005, la police néerlandaise a arrêté une équipe composée de trois pirates seulement, mais qui avait sous son contrôle 100 000 PC zombies. Des PC comme le vôtre, anonymes à leurs yeux et dont aucun ne les intéressait en particulier. Ainsi, les pirates ne s'intéressent pas à *vous*, mais à *toute* machine connectée à Internet.

Pourquoi détruisent-ils les ordinateurs ?

Comme le montre l'exemple d'Emmanuelle D. (et il y en a bien d'autres), le piratage peut rendre un ordinateur totalement inutilisable. Cependant, ce n'est souvent pas fait à dessein : nul ne cherche à détruire au sens propre votre matériel informatique, si tant est que cela soit possible[7]. Pour les pirates, votre PC est un outil ; leur intérêt est qu'il demeure en bon état, et votre ordinateur peut d'ailleurs être contrôlé par un pirate sans que vous constatiez quoi que ce soit d'anormal[8].

6. Le même terme est utilisé, plus largement, pour les programmes qui réalisent une tâche précise et répétitive en continu, par exemple les comparateurs de prix, ou les moteurs de recherche comme Google qui passent automatiquement en revue toutes les pages web.

7. Notons tout de même que l'on peut faire exploser certains anciens modèles d'écrans à distance en leur imposant des fréquences d'affichage avec lesquelles ils ne sont pas compatibles. Un pirate peut aussi modifier ou effacer des programmes qui sont nécessaires à certains composants matériels – comme le BIOS de la carte mère ou le *firmware* du lecteur de DVD – et de la sorte endommager irrémédiablement ces derniers. Il peut également supprimer toutes les données du disque dur.

8. Les « petits génies », ceux pour qui le piratage est un défi et non un business, peuvent en revanche causer des dégâts informatiques ; par exemple, le virus *I Love You* effaçait les fichiers MP3 présents sur l'or-

Deux facteurs peuvent compromettre cet objectif. Le premier est une simple conséquence de l'accumulation de programmes. En temps normal, Windows gère les quelques programmes que vous contrôlez à l'écran (par exemple Word, Internet Explorer, un lecteur de CD audio, etc.), plus, en tâche de fond, quelques dizaines de programmes invisibles qui servent au bon fonctionnement du système (on ne voit pas ces programmes à l'écran, de la même manière qu'au restaurant on ne voit pas ce qui se passe dans les cuisines). Or, un ordinateur peut aisément être infecté par des *centaines* de programmes parasites. Aucun d'eux n'est spécialement gourmand en ressources, mais lorsque tous sollicitent l'ordinateur en parallèle, c'en est trop pour le matériel. La machine devient très peu réactive. Dans les cas graves, Windows lui-même ne peut plus gérer tous ces programmes et finit par planter.

L'autre facteur est inhérent à l'informatique : tout programme comporte des BUGS. Ceux des virus sont particulièrement dangereux pour Windows car ces programmes utilisent des fonctions très puissantes. Une erreur de programmation, et tout l'édifice peut s'écrouler. En particulier, les virus malmènent souvent un composant fondamental de Windows, la BASE DE REGISTRE. Une fois celle-ci abîmée, tous les autres programmes (Excel, Outlook, etc.) peuvent en souffrir.

En résumé, faire planter votre Windows est à l'opposé des objectifs des pirates. Et pourtant, c'est bien ce qui finit par se produire si vous ne réagissez pas.

Les principaux types de délits

Dans cette partie, nous allons voir comment les pirates parviennent, à vos dépens, à transformer le contrôle de milliers de PC en millions de dollars à la banque.

dinateur. Ce type de piratage tend à disparaître.

Leurs cibles peuvent être découpées schématiquement en trois catégories : les particuliers propriétaires des ordinateurs infectés, les autres particuliers, et les entreprises. Sans surprise, les premiers payent le plus lourd tribut.

Les particuliers dont l'ordinateur est infecté

Le moyen le plus immédiat de rentabiliser une armée zombie est de la louer à quelqu'un d'autre, en général pour installer des ADWARES et envoyer du SPAM.

Les *adwares* sont des programmes qui font surgir de la publicité à des moments impromptus et placent sur votre bureau des icônes menant à des sites web. Ce sont principalement des sites de casinos en ligne et des sites pornographiques qui rémunèrent les pirates pour qu'ils vous montrent ces publicités. Il s'agit de l'un des rares cas où le pirate ne cherche pas à passer inaperçu.

Un autre usage classique des ordinateurs contrôlés est l'envoi de *spam*, c'est-à-dire de courriers électroniques non sollicités, qui proposent des placements mirifiques, des substituts médicamenteux, des logiciels piratés, des vêtements et bijoux contrefaits ou encore des opérations chirurgicales dont on ne parlerait pas à son médecin traitant. Une armée zombie contrôlée par une seule petite équipe de pirates peut envoyer des milliards de *spams* en 24 heures[9].

L'échelon au-dessus de la simple location des zombies est de collecter sur les PC infectés, via des SPYWARES[10], des informations qui seront ensuite revendues à des criminels du monde réel. Un type de logiciels est particulièrement utile

9. En supposant qu'un PC envoie ne serait-ce qu'un seul courrier électronique par seconde, pour que cette activité demeure indétectable par l'utilisateur de la machine, cela représente 86 400 courriers en 24 h. Avec une armée de 100 000 PC, on atteint 8,6 milliards de *spams*.

10. *Spy* signifie « espion » en anglais. Le suffixe *-ware* désigne, quant à lui, un bien, une marchandise. Les anglophones l'utilisent beaucoup en informatique : on le trouve aussi dans *software* (les logiciels), *hardware* (le matériel), *adware* (les publicités), etc.

pour jouer à *Big Brother* : les KEYLOGGERS, qui enregistrent tout ce que vous tapez et transmettent l'information aux pirates quotidiennement, via Internet. Des programmes spécialement conçus pour analyser ces données partent alors à la recherche de vos mots de passe (par exemple celui que vous utilisez pour la banque en ligne), votre numéro de carte bleue, etc. En outre, si vous utilisez un logiciel pour gérer vos finances, toutes les informations que vous lui avez confiées pourront être récupérées.

Mais ce ne sont pas seulement vos informations financières qui peuvent être captées : c'est votre identité même qui est en jeu. Fausses cartes d'identité, faux passeports, faux permis de conduire, faux certificats en tous genres : c'est votre nom qui sera écrit dessus. Si vous utilisez des sites d'enchères, votre pseudo pourra être usurpé pour mener des « enchères roumaines », dans lesquelles les marchandises sont payées mais jamais expédiées.

Les pirates ne cherchent pas seulement à monnayer l'usage de votre PC, ils s'en servent aussi pour des activités « associatives ». Un grand classique est d'héberger chez vous des contenus qu'ils rendront ensuite accessibles via des sites web de *warez*[11] eux aussi hébergés sur des ordinateurs infectés. On y trouve pêle-mêle des logiciels piratés, des films tout juste sortis en salle, des rubriques pornographiques, etc. Tout ceci se trouve sur les PC qu'ils contrôlent, mais leurs propriétaires ne le savent pas et ne le voient pas.

Il existe également des pratiques marginales mais inquiétantes pour l'avenir. Par exemple, on a rapporté en 2005 le cas d'un particulier dont tous les fichiers avaient été cryptés par un pirate, qui demandait une rançon pour les rendre de nouveau accessibles. La seule limite est l'imagination des vrais criminels.

11. Ce mot désigne des logiciels commerciaux que l'on peut télécharger illégalement sur Internet.

Les autres particuliers

Même les particuliers dont l'ordinateur est bien protégé subissent les actions des pirates, en tout premier lieu via le *spam*, c'est-à-dire les envois de courriers électroniques en masse. Il s'agit le plus souvent de publicités qui, pour agaçantes qu'elles soient, ne font pas de dégâts – tant que vous ne vous laissez pas aller à acheter des médicaments par Internet, car ils peuvent être contrefaits.

Les courriers non sollicités (envoyés par les PC infectés) entrent dans la catégorie du PHISHING[12] lorsqu'ils tentent d'abuser de votre confiance. Vous recevez un mail qui semble provenir de votre banque, ou d'un site de commerce, ou encore d'un site d'enchères, qui vous demande de vous rendre sur un site web pour « confirmer » vos coordonnées bancaires. En cliquant sur le lien contenu dans le mail, vous voyez apparaître une page web qui ressemble en tout point à la page de votre banque, du site de commerce ou d'enchères. Même l'adresse web en `www` semble correcte, grâce à une technique de camouflage. Mais il s'agit invariablement d'une tromperie. Vos coordonnées sont directement récoltées par des pirates.

Les abus de confiance ne sont pas tous aussi sophistiqués. La bonne vieille arnaque du monde réel a trouvé des transpositions directes sur Internet. On vous dit par exemple que la fille de tel ancien chef d'état veut faire sortir plusieurs dizaines de lingots d'or du pays, ou des millions coincés en Suisse, que l'on a bien sûr besoin de votre aide mais qu'elle sera remboursée au centuple... Ces arnaques proviennent le plus souvent d'Afrique. On les appelle d'ailleurs fréquemment des *scam 419*, du nom de l'article du code pénal nigérian qui les sanctionne[13].

12. On dit aussi hameçonnage en français.

13. Voir par exemple `www.secretservice.gov/alert419.shtml` (en anglais). Une recherche Google sur `Nigeria 419` renvoie 1,5 million de réponses.

Ces problèmes n'existeraient pas si les pirates n'avaient pas à leur disposition des PC infectés. Il est de la responsabilité de chacun de maintenir son ordinateur à l'abri des pirates, ne serait-ce que pour protéger autrui. C'est le sens d'un projet de loi australien qui infligerait une amende aux propriétaires d'ordinateurs infectés si, après avoir été informés d'un problème, ils n'agissaient toujours pas pour se protéger.

Les entreprises

Les entreprises ont tout à redouter des pirates car elles font l'objet d'attaques ciblées. Qu'un seul de ses ordinateurs soit infecté et il peut devenir une porte d'entrée béante pour l'espionnage industriel, le vandalisme d'activistes ou encore le besoin de reconnaissance de pirates irresponsables, comme celui qui avait volé et distribué sur Internet le code source d'un jeu vidéo quelques semaines avant sa sortie en magasin.

Les entreprises sont également soumises à une forme de racket que l'on appelle le *déni de service distribué*[14]. Lorsqu'un pirate ordonne à tous les PC zombies qu'il contrôle de se connecter simultanément à un site web, en envoyant des requêtes aussi vite que leurs connexions internet le leur permettent, ce site fait subitement face à un trafic équivalent à celui qu'il enregistre habituellement en plusieurs semaines. Les serveurs sur lesquels les pages demandées sont hébergées ne peuvent pas suivre et le site s'écroule, rendant toute opération commerciale impossible. Le pirate maintient cette pression jusqu'à ce que l'entreprise lui ait versé une rançon. Dans ce schéma, la sécurité de l'entreprise n'est pas en cause : le pirate ne contrôle aucun de ses ordinateurs. Il se sert seulement des PC de particuliers négligents.

Nous avons vu qu'il existe bien des manières pour un pirate de tirer parti d'un ordinateur infecté. Nous espérons vous avoir convaincu que votre propre ordinateur est en danger s'il

14. *Distributed Denial of Service* en anglais, en abrégé « DDoS ».

n'est pas défendu, au même titre que tout Windows connecté à Internet. L'anonymat ne vous protège pas, et les conséquences d'une négligence peuvent être graves.

Passons maintenant à l'envers du décor : comment allons-nous protéger votre ordinateur, vos fichiers, votre compte en banque et, finalement, votre tranquillité ?

En pratique

Les programmes malveillants n'ont que deux manières d'entrer dans votre ordinateur : soit directement, soit camouflés dans un programme ou un service d'apparence anodine.

L'intrusion est directe lorsque votre ordinateur a été sélectionné au hasard par un *bot* et que celui-ci parvient à tromper Windows. Les enquêtes de sécurité montrent qu'il ne s'écoule que 40 minutes en moyenne entre le moment où un Windows XP Service Pack 2 tout neuf est connecté à Internet, et le moment où il est infecté par une attaque directe réussie. Pour empêcher cela, nous utiliserons dès la première étape un *pare-feu*. Son principe est très simple : interdire tout échange d'informations entre Windows et Internet, hormis pour les programmes que vous aurez explicitement autorisés à le faire.

L'intrusion est indirecte lorsque le programme malveillant est caché dans un autre, ce qui est un abus de confiance. Vous pensez par exemple installer un économiseur d'écran ou un logiciel d'échange de fichiers, et celui-ci installe en sus un autre programme sans vous prévenir. Nous repérerons ces tricheurs à l'aide d'un antivirus (étape 2) et d'un anti-spyware (étape 3).

Les logiciels que vous aurez autorisés à communiquer avec Internet sont eux-mêmes plus ou moins bien sécurisés, plus ou moins susceptibles de vous transmettre des programmes malveillants. Nous vous montrerons à l'étape 4 comment remplacer les deux pires « passoires » (Internet Explorer et Outlook Express) par des logiciels dignes de votre confiance.

Enfin, le piratage n'est pas seulement technique et il est connu que des personnes par ailleurs très cartésiennes peuvent devenir naïves lorsqu'elles sont confrontées à des informations provenant d'Internet. Nous vous indiquerons à l'étape 5 comment rester vigilant.

Ainsi, en installant quelques programmes une bonne fois pour toutes, puis en suivant quelques règles simples d'hygiène informatique, vous serez en sécurité.

En résumé, ne laissez pas les pirates prendre en main votre destin : selon la formule d'Andy Groove[15], « Seuls les paranoïaques survivent ! »

15. Ancien PDG d'Intel, le célèbre fabricant de processeurs.

Étape 1 : Empêcher les intrusions

Imaginons un instant que votre ordinateur soit un village situé dans une région peu sûre. Chaque échange avec Internet correspond à un échange entre le village (votre ordinateur) et le reste du monde. Pour pouvoir contrôler les événements, il faut limiter le nombre de routes qui mènent à votre village. Une méthode qui a fait ses preuves consiste à l'entourer d'un solide rempart, percé de quelques portes pour permettre les entrées et les sorties. Inutile alors d'inspecter la totalité de la périphérie du village : il suffit de surveiller le trafic passant par les voies d'accès.

Comme on suppose que l'ennemi vient de l'extérieur, on contrôle plus attentivement les personnes qui tentent de pénétrer dans le village. Mais un individu qui tente de franchir une barrière pour sortir après le couvre-feu est tout aussi suspect : il s'agit peut-être d'un espion venu recueillir des informations pour les communiquer à l'ennemi. Il faut aussi inspecter régulièrement les abords du village, pour s'assurer qu'il n'existe pas de tunnels souterrains permettant d'entrer en échappant à la vigilance des gardes. En informatique, le rempart s'appelle un pare-feu.

Le principe des attaques informatiques directes est d'envoyer des demandes de connexion au hasard aux ordinateurs reliés à Internet. Votre PC reçoit ce type de requêtes plusieurs fois par minute et la majorité d'entre elles sont des tentatives de piratage. Pourquoi votre ordinateur accepte-t-il d'y répondre ? Un ordinateur connecté à Internet doit accepter de recevoir des informations venant de l'extérieur. Elles peuvent provenir de votre fournisseur d'accès et être nécessaires au

Étape 2 :
Éradiquer les virus

Reprenons notre image du village, et modernisons-la un peu : des voitures entrent et sortent désormais du village. Voici ce qui s'est passé dans le chapitre précédent :

- L'installation du pare-feu a bâti une épaisse muraille autour du village : plus personne ne pouvait entrer ni sortir. La sécurité était parfaite... et l'autarcie totale.
- Grâce à la période d'apprentissage progressif du pare-feu, nous avons percé plusieurs portes dans cette muraille, chacune destinée à laisser passer une certaine catégorie de voitures.

Cependant, les « gardes frontières » ne sont pas habilités à ouvrir les coffres. Ils se contentent de demander au conducteur : « Où allez-vous ? ». Si sa réponse est satisfaisante (un conducteur entrant déclare « Je viens livrer des informations à votre navigateur internet. », un conducteur sortant affirme « Je vais porter un e-mail à la ville voisine. »), les gardes lui permettent d'accéder au service en question.

Qui nous dit que les conducteurs sont tous de bonne foi ? Comment sait-on ce qu'ils transportent effectivement dans leur voiture ? Le conducteur prétextant qu'il apporte des données pour votre navigateur internet n'a-t-il pas dissimulé un microbe qui risque de contaminer toute la population, ou une bombe prête à exploser ? Cela arrive bien plus fréquemment en informatique que dans le monde réel. La solution, c'est bien sûr de fouiller toutes les voitures, et d'éliminer les intrus qui pourraient s'y cacher : les virus.

Étape 3 :
Éliminer les espions

Dans les deux chapitres précédents, nous avons vu comment votre ordinateur, à l'instar d'un village se défendant contre des envahisseurs, pouvait limiter les entrées et sorties au strict nécessaire (étape 1) et organiser des fouilles à différentes étapes pour se protéger des intrus, les virus (étape 2).

Si le village a des ennemis, ceux-ci ne vont pas seulement tenter de l'attaquer de front ou de contaminer la population. Ils sont aussi susceptibles de chercher à l'espionner. Les informations collectées sont utilisées autant, voire plus, pour mener des « attaques » commerciales que pour préparer des assauts militaires. L'espionnage, dans le cas de votre ordinateur, est fait par un logiciel conçu spécialement pour cela : le *spyware*.

Kazaa est un célèbre logiciel d'échange de fichiers sur Internet. Mais pour la sécurité de votre ordinateur, c'est surtout un programme à éviter. Kazaa est gratuit : vous ne payez pas pour le télécharger, l'installer et l'utiliser. Mais ses créateurs ne sont pas pour autant des bénévoles. Leur logiciel affiche des publicités, et ce sont les marques correspondantes qui rémunèrent ses auteurs. Jusque-là, rien d'anormal.

Mais cette publicité n'arrive pas au hasard. En s'installant, Kazaa place aussi sur votre disque le sous-programme Gator. Celui-ci est chargé d'observer quelles pages web vous consultez, quels mots vous tapez dans les moteurs de recherche (comme `google.fr`), en bref de vous espionner pour savoir quelles publicités vous correspondent le mieux.

Étape 4 :
Choisir les bons outils

Nous avons comparé dans les chapitres précédents votre système à un village se défendant successivement contre les assauts, les intrusions et les espions. Cela suffirait à assurer sa sécurité si les personnes qui travaillent dans le village étaient elles-mêmes prudentes et ne laissaient pas les clés sous le paillasson. Malheureusement, il y a parmi les employés du village au moins deux personnes dont la négligence, pour tout ce qui concerne la sécurité, est de notoriété publique. Leurs noms : Internet Explorer et Outlook Express.

Contrairement à ce que nous avons fait avec Windows dans les étapes 1 à 3, on ne peut pas sécuriser convenablement ces logiciels, car les réglages proposés sont inadaptés, et les outils de configuration très insuffisants. Le point positif, c'est qu'il existe des équivalents gratuits et mieux sécurisés de ces deux applications. Nous vous proposons donc simplement ici de remplacer Internet Explorer et Outlook Express par des logiciels faciles à utiliser, totalement gratuits, et beaucoup plus fiables : Firefox et Thunderbird.

4.1 Surfez en toute sécurité avec Firefox

Votre navigateur internet est l'un des logiciels que vous utilisez le plus souvent. Et c'est justement d'Internet que viennent la plupart des dangers qui menacent votre PC. Un bon navigateur se doit d'être véloce et ergonomique, mais aussi de constituer un rempart face aux agressions constantes (visibles ou non) dont votre système est victime.

Étape 5 :
Rester vigilant

Votre ordinateur sous Windows est désormais équipé d'un service de sécurité redoutable. Il ne laisse pas entrer n'importe qui grâce au pare-feu, il fouille consciencieusement chaque nouvel arrivant à l'aide de l'antivirus et il chasse les espions avec l'anti-*spyware*. En outre, vous vous êtes entouré d'alliés dignes de confiance si vous utilisez les logiciels conseillés à l'étape précédente.

Tout cela est-il suffisant pour vous garantir une sécurité maximale ? Presque, mais pas encore. Le principal danger pour votre ordinateur, désormais, c'est vous. Aucun outil informatique ne remplace l'homme, son bon sens et sa vigilance. Il ne s'agit pas de devenir paranoïaque, mais d'être aussi circonspect que dans le monde réel face aux situations inconnues et potentiellement dangereuses. C'est l'objet de cette dernière étape.

5.1 Les e-mails suspects

Le courrier électronique a pris une telle ampleur ces dernières années qu'il est devenu pratiquement indispensable ; il est maintenant aussi courant de demander à quelqu'un son adresse électronique que son numéro de téléphone. Cette évolution est arrivée très vite ; si vite que les précautions élémentaires prises dans la vie de tous les jours ont été oubliées.

L'e-mail est aussi le moyen le plus répandu pour transmettre un virus. En effet, la messagerie électronique, et plus particulièrement l'usage de carnets d'adresses, offre aux pirates un moyen simple et efficace pour atteindre tous les ordinateurs connectés à Internet.

Lexique

Ce lexique regroupe des explications sur tous les termes techniques rencontrés dans cet ouvrage. Au fil du texte, nous avons signalé les mots présentés ici au moyen de PETITES CAPITALES. Nous conserverons cette convention dans les définitions.

Ad-Aware : ANTI-SPYWARE gratuit, présenté dans cet ouvrage.

Voir aussi p. 80.

Adresse IP : (pour *Internet Protocol*) il s'agit de quatre chiffres compris entre 0 et 255, séparés par des points, qui permettent d'identifier une machine au sein d'un réseau. Par exemple : « 192.168.0.1 ».

Voir aussi p. 40.

Adresse réseau : voir ADRESSE IP.

Adware : une catégorie de SPYWARE à vocation publicitaire.

Anti-spyware : logiciel qui examine votre ordinateur à la recherche de SPYWARES et les élimine.

Voir aussi p. 80.

Antivirus : logiciel qui recherche les VIRUS sur votre ordinateur, leur barre la route et, selon les cas, répare, efface ou met en QUARANTAINE les fichiers infectés.

Voir aussi p. 52.

Application : synonyme de « logiciel » ou de « programme ».

Avast ! : ANTIVIRUS gratuit, présenté dans cet ouvrage.
Voir aussi p. 56.

Backdoor : porte dérobée sur un ordinateur, permettant à un pirate d'en prendre le contrôle à distance.

Base de définitions : ensemble des descriptions des VIRUS ou des MOUCHARDS connus. L'ANTIVIRUS et l'ANTI-SPYWARE s'en servent pour reconnaître les intrus. Cette base doit être tenue à jour régulièrement.
Voir aussi p. 53. et 85

Base de registre : endroit du système où Windows stocke de nombreux réglages de votre ordinateur.
Voir aussi p. 87.

Boîte de dialogue : fenêtre, généralement de taille réduite, ouverte par un logiciel afin de vous permettre de répondre à une question. Une boîte de dialogue s'ouvre, par exemple, lorsque vous choisissez l'article « Enregistrer sous... » dans le menu « Fichier » de la plupart des traitements de texte.

Bombe logique : VIRUS qui se déclenche à retardement, par exemple à une date préprogrammée.

Bot : abréviation de « robot ». Logiciel destiné à attaquer automatiquement par Internet les ordinateurs qui ne sont pas munis d'un PARE-FEU assez solide.

Bug : erreur de programmation commise par les concepteurs d'un logiciel. Certaines de ces erreurs constituent des TROUS DE SÉCURITÉ sur le système qui en est victime.

Cheval de Troie : VIRUS dissimulé à l'intérieur d'un logiciel.
Voir aussi p. 52.

Faille : défaut de conception d'un logiciel qui le rend vulnérable à certaines attaques extérieures.

Firewall : nom anglais de PARE-FEU.

Firefox : navigateur internet gratuit et bien sécurisé qui remplace avantageusement Internet Explorer.

Voir aussi p. 93.

Hoax : littéralement, « canular ». Rumeur non fondée, qui circule le plus souvent par e-mail.

Voir aussi p. 108.

Kaspersky : marque d'un ANTIVIRUS particulièrement efficace et très réactif face aux nouveaux virus. Kaspersky Antivirus est présenté dans cet ouvrage.

Voir aussi p. 66.

Keylogger : type particulier de SPYWARE qui espionne tout ce que vous saisissez au clavier.

Lien : parfois « hyperlien ». Sur une page web, c'est une image, un mot ou un groupe de mots cliquable, pointant vers une autre page web. Les liens textuels sont mis en évidence dans la page (ils sont souvent soulignés, et de couleur bleue).

Logiciel libre : logiciel le plus souvent gratuit, et dont le « code source » (la recette de fabrication) est public. N'importe quel programmeur peut le consulter et proposer, s'il le souhaite, des améliorations (notamment sur le plan de la sécurité).

Mouchard : synonyme de SPYWARE.

Navigateur internet : programme informatique utilisé pour afficher les pages web et, selon l'expression consacrée, pour « surfer sur le WEB ».

Par défaut : désigne en informatique le réglage « standard » d'une fonction ou d'un logiciel. Ainsi, le navigateur par défaut est celui qui apparaît spontanément quand vous cliquez sur un lien internet.

Pare-feu : logiciel qui protège votre ordinateur des attaques extérieures. C'est une véritable muraille entre votre ordinateur et Internet.

Voir aussi p. 19.

Patch : fragment de programme visant à corriger les BUGS qui menacent la sécurité d'un système.

Voir aussi p. 42.

Phishing : tentative d'escroquerie consistant à vous faire croire que vous êtes sur un site de confiance dans le but de vous dérober des informations, comme votre numéro de carte bancaire, le plus souvent sous prétexte de « mettre à jour vos informations ».

Pirate : nom communément donné aux personnes qui créent des virus ou qui essaient de pénétrer dans les ordinateurs illégalement.

Port : porte de communication utilisée par un ordinateur pour échanger des données avec l'extérieur.

Voir aussi p. 21.

Quarantaine : option de certains ANTIVIRUS pour mettre de coté les fichiers infectés qu'il n'est pas possible de réparer.

Regcleaner : logiciel permettant de nettoyer la BASE DE REGISTRE, présenté dans cet ouvrage.

Voir aussi p. 88.

Scan : analyse de votre disque, à la recherche de VIRUS ou de SPYWARES.

Service Pack 2 : évolution majeure du SYSTÈME D'EXPLOITATION Windows XP et dont l'objectif principal est de renforcer la sécurité.

Voir aussi p. 45.

Spam : courrier indésirable, le plus souvent publicitaire.

Spyware : logiciel espion installé sur votre ordinateur pour collecter des informations personnelles sur vous, à des fins publicitaires ou plus malveillantes.

Voir aussi p. 78.

Système d'exploitation : logiciel qui permet d'utiliser les ressources matérielles de votre ordinateur et qui sert de base à toutes les autres applications. Exemples : Windows (de Microsoft), Mac OS (d'Apple), Linux.

Thunderbird : logiciel de messagerie électronique qui remplace avantageusement Outlook Express, notamment sur le plan de la sécurité.

Voir aussi p. 98.

Trou de sécurité : synonyme de FAILLE.

Ver : VIRUS extrêmement contagieux, se propageant par le réseau sans intervention de votre part.

Voir aussi p. 51.

Virus : programme parasite infectant les fichiers d'un ordinateur et utilisant les ressources de celui-ci pour se propager et effectuer des opérations malveillantes.

Voir aussi p. 49.

Vulnérabilité : synonyme de FAILLE.

Web : (de l'anglais *web*, « toile ») abréviation de *World Wide Web* (littéralement : « toile mondiale »). C'est l'ensemble de toutes les pages accessibles sur Internet et affichables à l'aide d'un NAVIGATEUR INTERNET.

Windows Update : application développée par Microsoft afin de pouvoir mettre à jour le SYSTÈME D'EXPLOITATION Windows via Internet. Elle est présentée dans cet ouvrage.

Voir aussi p. 44.

ZoneAlarm : PARE-FEU gratuit, performant et facile d'utilisation présenté dans cet ouvrage.

Voir aussi p. 24.

Liste des attaques décrites dans ce livre : **CoolWebSearch** (voir p. 79), **Funner** (p. 51), **Gator** (p. 77), **I Love You** (p. 104), **Klez** (p. 50), **Melissa** (p. 51), **Mydoom** (p. 51), **Quox** (p. 51), **Sasser** (p. 51), **Slammer** (p. 43), **Sober.Z** (p. 106) et **Zotob** (p. 20).