

Part. 2

-Introduction

- Risques et conséquences (perte de données / destruction de données / indisponibilité / vol de données).

- Formes d'atteintes numériques (logiciels malicieux : (Virus - spyware – adwares)

- Formes d'atteintes extérieures et non numériques.

- Présentation des différent éditeurs

-Ingénierie sociale vs attaques numériques

- Deux grandes familles d'attaques par failles « humaines » ou « numériques».

- Vulnérabilité du réseau.

- Vulnérabilité matérielle.

- Vulnérabilité système et logicielle.

- Problématique particulière du sans fil.

-Planifier la sécurité des SI

- Sécurité physique du poste fixe.

- Sécurité physique des SI et événements extérieurs non numériques.

- Plan de sauvegarde et de retour à l'activité.

-Sécurité des informations et contenus

- Intrusion et sécurité des données.

Typologies des risques informatiques

Cette section propose une classification des principales catégories de risques à la confidentialité, l'intégrité et la disponibilité des systèmes d'information. Ces risques sont organisés en deux groupes : dans un premier groupe principal les risques pouvant causer des dommages matériels et dans le second les risques causant des dommages immatériels.

Les dommages matériels

Il s'agit ici des risques pouvant causer des dommages matériels ou physiques aux divers éléments des systèmes d'information d'une organisation. Ces atteintes ne représentent qu'un faible pourcentage des sinistres informatiques.



PHÉNOMÈNES ACCIDENTELS

Les phénomènes accidentels identifient les événements causés par l'environnement technique des systèmes d'information. Ceux-ci incluent des événements naturels dont les conséquences sont aisément identifiables. Nous en identifions les principaux.

Risque	Exemples de conséquence
Bris accidentels	Non-disponibilité du système d'information; Dommages aux systèmes d'informations;
Panne accidentelle	Non-disponibilité du système d'information; Dommages aux systèmes d'informations;
Incendie	Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;
Inondation	Destruction de données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;

Désastre environnemental	Destruction de données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;
Tremblement de terre	Destruction de données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;
Tornade - Ouragan	Destruction de données Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;
Panne de courant	Modification des données; Destruction de données; Non-disponibilité du système d'information; Dommages aux systèmes d'informations;

Pointes de courant	<p>Modification des données;</p> <p>Destruction de données;</p> <p>Non-disponibilité du système d'information;</p> <p>Dommages aux systèmes d'informations;</p>
Champs électromagnétiques	<p>Destruction de données;</p> <p>Destruction du matériel</p> <p>Destruction des réseaux</p>
Dommages collatéraux (Guerre)	<p>Destruction de données;</p> <p>Destruction du matériel</p> <p>Destruction des réseaux</p>

VANDALISME

Le vandalisme identifie des situations par lesquelles une ou plusieurs personnes détruisent sciemment ou subtilisent un système d'information [Denning, 2000] [Denning, 2000(1)].

Risque	Exemples de conséquence
Vol	Accès non autorisé aux données; Destruction de données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;
Incendie	Modification des données; Destruction de données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;
Sabotage	Accès non autorisé aux données; Modification des données; Destruction de données; Copie des données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;

Guerre	Destruction de données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures;
Activisme ou cyberactivisme	Accès non autorisé aux données; Modification des données; Destruction de données; Copie des données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures; Dommages ou destruction physique d'infrastructures critiques; Blessures ou Pertes de vie humaines;
Terrorisme ou cyberterrorisme	Accès non autorisé aux données; Modification des données; Destruction de données; Copie des données; Non-disponibilité du système d'information; Dommages ou destruction physique des systèmes d'informations et des infrastructures; Dommages ou destruction physique d'infrastructures critiques; Blessures ou Pertes de vie humaines;

LES DOMMAGES IMMATÉRIELS

L'ERREUR

L'erreur est l'acte involontaire d'un membre de l'organisation qui à la suite d'une mauvaise manipulation. Cet acte aura pour conséquence de détruire, modifier ou corrompre des données. Il en résulte des dommages immatériels comme la perte d'un fichier, la mauvaise exécution d'un programme, ou encore à l'exécution d'une commande destructrice. Ces phénomènes peuvent aboutir à des pertes très importantes pour l'organisation.

Risque	Exemples de conséquence
Erreur de manipulation	Données erronées; Modification des données; Destruction de données; Non-disponibilité du système d'information; Destruction de la salle informatique si une personne fume dans la salle, suite a une émanation de gaz Holon
Erreur dans l'entrée des données	Données erronées; Modification des données; Destruction de données;
Erreur de programmation	Données erronées; Modification des données; Destruction de données; Non-disponibilité du système d'information;

La fraude économique

La fraude économique représente une partie importante des sinistres informatiques. Il s'agit le plus souvent de virements bancaires frauduleux ou du vol de fichiers contenant des numéros de carte de crédit. Ces actes peuvent être l'œuvre d'un tiers, mais sont souvent le fait de membres d'une organisation.

Risque	Exemples de conséquence
Virement frauduleux	Perte économique
Détournement de biens	Non-disponibilité du système d'information;
Erreur volontaire dans l'entrée des données	Dépôt ou transfert de fonds
Erreur volontaire de programmation	Perte des fractions (arrondis) sur de nombreuses transactions

Cyber crimes

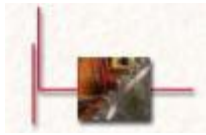
On regroupe sous le nom de cyber crimes les fraudes informatiques réalisées par l'intermédiaire des systèmes d'informations ou de réseaux de télécommunications. C'est l'intrusion illégale d'un tiers à l'intérieur d'un système d'information, d'une base de données afin de les manipuler, les altérer ou d'en tirer profit.

Risque	Exemples de conséquence
Virus	Modification des données; Destruction de données; Ralentissement des traitements; Non-disponibilité du système d'information;
Vers	Modification des données; Destruction de données; Ralentissement des traitements; Non-disponibilité du système d'information;
Cheval de Troie	Modification des données; Destruction de données; Ralentissement des traitements; Non-disponibilité du système d'information;
Attaques ciblées immédiates	Accès non autorisé aux données; Modification des données; Destruction de données; Copie des données; Non-disponibilité du système d'information;

Attaques ciblées retardées	<p>Accès non autorisé aux données;</p> <p>Modification des données;</p> <p>Destruction de données;</p> <p>Copie des données;</p> <p>Non-disponibilité du système d'information;</p>
Attaques ciblées distribuées	<p>Accès non autorisé aux données;</p> <p>Modification des données;</p> <p>Destruction de données;</p> <p>Copie des données;</p> <p>Non-disponibilité du système d'information;</p>
Cyber Sabotage	<p>Accès non autorisé aux données;</p> <p>Modification des données;</p> <p>Destruction de données;</p> <p>Copie des données;</p> <p>Non-disponibilité du système d'information;</p>
Cyber activisme	<p>Accès non autorisé aux données;</p> <p>Modification des données;</p> <p>Destruction de données;</p> <p>Copie des données;</p> <p>Non-disponibilité du système d'information;</p>

Cyber terrorisme	<p>Accès non autorisé aux données;</p> <p>Modification des données;</p> <p>Destruction de données;</p> <p>Copie des données;</p> <p>Non-disponibilité du système d'information;</p> <p>Dommages ou destruction physique des systèmes d'informations et des infrastructures;</p> <p>Dommages ou destruction physique d'infrastructures critiques;</p> <p>Blessures ou Pertes de vie humaines;</p>
------------------	--

Pourquoi sécuriser



Alors que l'informatique est devenue pour l'entreprise un outil incontournable de gestion, d'organisation, de production et de communication, les données mises en œuvre par le système d'information ainsi que les échanges internes et externes sont exposés aux **actes de malveillance** de différentes natures et sans cesse changeants.

Il convient en conséquence de ne pas renoncer aux bénéfices de l'informatisation, et pour cela de faire appel à des spécialistes qui apportent une **garantie contre les risques**, d'une manière permanente, en préservant la stricte confidentialité des données, et pour un budget raisonnable.

La problématique du travail en réseau



→ Le réseau : un outil de production exposé

L'informatique est devenue un outil incontournable de gestion, d'organisation, de production et de communication.

Le réseau de l'entreprise met en œuvre des données sensibles, les stocke, les partage en interne, les communique parfois à d'autres entreprises ou personnes, voire les importe d'au-delà les murs.

Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.

Il est impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données leur caractère électronique et confidentiel.

Les données sensibles du système d'information de l'entreprise sont donc exposées aux actes de malveillance dont la nature et la méthode d'intrusion sont sans cesse changeantes.

Les prédateurs et voleurs s'attaquent aux ordinateurs surtout par le biais d'accès aux réseaux qui relient l'entreprise à l'extérieur.

☞ Une protection juridique faible

Les malfaiteurs sont difficilement identifiables, comme ils agissent à distance, à travers des relais.

Si les attaques sont souvent transfrontalières, les lois — elles —, ne le sont pas.

La lenteur de la coopération judiciaire inter états s'ajoute aux différences de législations d'un état à l'autre.

De sorte que l'impunité reste de fait.

Il est d'autre part difficile de prouver l'effraction réelle.

Seule la mise en place d'une sécurité forte peut conduire à prouver le vol et les pertes engendrées.

Ainsi, comme les données informatiques peuvent être volées par copie, une capacité d'analyse pointue des traces d'activité se révèle absolument nécessaire.

☞ Des obligations légales à respecter

Obligation de protéger l'accès aux données nominatives (clients, patients, salariés, etc.) : l'article 226-17 du code pénal punit de 5 ans d'emprisonnement ou/et 2 MF d'amende.

Obligation contractuelle de surveillance, dans le cadre d'accords de partenariat (B to B, secret Défense, etc.).

Obligation de respect du domaine privé des salariés : les échanges privés ne sauraient être écoutés ou lus par l'employeur, s'agissant notamment de la messagerie électronique.

Les attaques et le piratage



☞ La délinquance informatique : une réalité

Les pirates informatiques ne sont plus seulement des "brico-leurs", ce sont des malfaiteurs qu'il faut traiter comme tels : les statistiques Europol - G8 Nice révèlent que 60% des équipes effectuant des attaques lourdes sont financées par le crime organisé.



Leur but est le profit et leur idéologie supposée est souvent de façade, pour justifier des actes délictueux : selon les mêmes statistiques, 80% des attaques sont à but financier.

Les attaquants disposent d'outils efficaces, leur ouvrant l'accès à des réseaux pourtant conçus par des professionnels de bon niveau.

Puisque 44% des sites Internet ont pu être piratés malgré la présence de "pare-feux", comment résisteraient les 93% de sites représentant des cibles faciles à pénétrer ?

La gravité des impacts

Le piratage informatique :

- met en jeu la survie de l'entreprise : une étude du Gardner Group montre que 95% des sociétés de taille moyenne ayant été piratées sévèrement en 1998 ont stoppé leur activité dans les douze mois qui suivaient ;
- paralyse : destruction des données, de la capacité de production ; dégradation de l'image de l'entreprise ;
- vole : détournement de fonds, chantage, impayés.

Exemples frappants :

- chantage à la destruction : une banque américaine, 10 M de \$US de rançon versée ;
- vol d'un cœur de métier : un éditeur de logiciels, la mise en circulation de versions pirates cause un manque à gagner majeur ;
- vol de données portant sur une clientèle de particuliers : une société de sondage pour la télé, vol d'un fichier des sondés contenant leur profil psychologique ; 3 M d'euros de dommages et intérêts et fermeture de la société.

Impacts négatifs "courants" :

- fonctionnels : perte de crédibilité, d'exploitation (indisponibilité des outils), de compétitivité (vol d'informations), de savoir faire (destruction de données) ;
- financiers : perte de valorisation boursière, perte d'exploitation, perte de compétitivité ; extorsion ou détournement de fonds ;
- structurels : perte de confiance interne et externe dans l'entreprise (l'image donnée d'elle est négative).



Protéger son réseau d'entreprise



→ L'organisation à mettre en place

Bien évidemment, l'entreprise a à définir une politique générale de sécurité interne vis-à-vis de ses salariés et visiteurs : règles de travail, droits d'accès physiques et logiques, etc.

Autre considération de poids :

- l'entreprise doit veiller à la protection physique des installations (prévoir le risque d'incendie ; fournir une alimentation électrique permanente et régulée ; contrôler l'accès pour lutter contre les volontés de dégradation, sabotage et autres actes malveillants)
- cette protection doit être associée à une politique de sauvegarde régulière, avec stockage distant des sauvegardes.

S'agissant de la sécurité logique de ses applications informatiques, l'entreprise doit la faire prendre en compte dans la programmation (sécurité intégrée dans l'application) et — en permanence —, dans l'administration des applications et dans leur exploitation (gestion des droits d'accès des utilisateurs, tenue à jour des systèmes et des langages, etc.).

Doit également être assurée la surveillance du système d'information (réseau interne de l'entreprise) : activité, analyse des journaux d'activité, audit, ...

Enfin, la protection et la surveillance des points d'accès au réseau nécessitent une vigilance particulière : la protection des connexions entre le réseau privé de l'entreprise et le réseau public (Internet) passe par la mise en place de points de filtrage devant être sûrs et surveillés, si l'on veut détecter toute tentative d'attaque et la bloquer avant qu'elle cause des dégâts.

→ Les nouveaux défis posés à la DSI (Direction du Service Informatique)

L'évolution des besoins oblige à une véritable mutation du service informatique, qui doit prendre en compte :



- la nécessité de passer par des réseaux publics : interconnexion des sites de l'entreprise, développement des accès à l'Internet ;
- l'intégration d'outils de Net-économie, avec accès aux données de l'entreprise.

Les risques se modifient et s'ajoutent : des centaines de nouveaux virus apparaissent chaque mois, l'ingéniosité des attaquants est grandissante, le piratage informatique à visée mercantile progresse rapidement et vise essentiellement les entreprises, etc.

Si la prise de conscience des risques et le besoin de leur évaluation s'imposent d'eux-mêmes, après un acte grave de piratage, il est admis désormais que l'on ne doit plus attendre pour agir :

- dès 1999, une étude Price Waterhouse Cooper (2 250 entreprises interrogées en 1999 dans 49 pays) montrait que 59% inscrivaient la politique de sécurité informatique en priorité haute pour l'entreprise, outre 32% qui la mettent en priorité moyenne ;
- cette politique est définie aujourd'hui à 40% par la DSI, à 24% par la Direction Générale, à 21% par la Direction de la Sécurité.

Des facteurs importants freinent la mise en place d'un système de sécurité informatique et rendent difficile sa maintenance :

- disponibilité trop faible des services informatiques internes, qui ne peuvent pas surveiller 24h/24 et protéger l'accès au réseau d'entreprise qui fonctionne en permanence (poids : 24%) ;
- carences, face à la complexité technologique : il manque des compétences au niveau des services informatiques internes de l'entreprise, dans un marché de l'emploi pourvoyant difficilement les profils requis (poids : 19%) ;
- évolution rapide des technologies de sécurité et des procédés d'attaque utilisés par les pirates (poids : 16%).

Nos recommandations les meilleures

Demandez un **audit-sécurité** de votre système d'information :

- l'objectif est de dresser un état des lieux des vulnérabilités et de proposer s'il y a lieu des solutions ;
- des tests intrusifs évalueront les risques portés par vos accès externes (interconnexions avec les autres sites, Internet, accès

distants) : usurper les privilèges d'utilisateur ou d'administrateur, introduire des « chevaux de Troie » ; infecter le système d'information avec des virus ; déni de service ; accès à des informations protégées (via la consultation et/ou la modification des fichiers) ; efficacité des éléments d'interconnexion (routeurs, filtres, "pare-feux") ; possibilité de rebondir, d'un site distant à un autre ; etc.

Bâissez le **réseau virtuel global** de votre entreprise :

- protégez les données de l'entreprise, les transferts d'informations entre les différents sites d'implantation ;
- augmentez la productivité du système d'information : par la mutualisation des équipements et des services liés à la sécurité, par une plus grande facilité de management, par la mise en place d'un système unique si votre entreprise a plusieurs sites.

Choisissez l'**externalisation** vers un partenaire spécialisé :

- il est possible de déléguer la protection des accès à votre réseau d'entreprise ;
- vous régleriez d'un coup toutes les difficultés liées à la maîtrise permanente de technologies complexes et très (trop) spécifiques ;
- vous ne perdriez pas d'énergie dans la gestion délicate de contraintes humaines (heures supplémentaires, service à assurer 24h/24, quelles équipes et procédures de relais, etc.).



Informatique personnelle et sécurité

La sécurité informatique est une question essentielle, à une époque où tous les ordinateurs, ou presque, bénéficient d'un accès permanent à Internet.

Or, les utilisateurs sont souvent mal informés des dangers qui les menacent et des comportements à adopter pour réduire leur exposition à ces dangers.

C'est sur cela que jouent la plupart des auteurs de logiciels malveillants. Cet article présente les principales techniques de protection d'un *ordinateur personnel*, qui ont pour but d'empêcher les intrusions, d'assurer la sécurité du système, de prévenir la diffusion des données personnelles de l'utilisateur, etc.



Sommaire

1. Quelques rappels juridiques
2. Typologie des menaces
 1. Malware
 2. Spyware
 3. Trojan
 4. Keylogger
 5. Screenlogger
 6. Rootkit
 7. Bootkit
 8. Backdoor
 9. Rogue
 10. Adware
 11. Virus
 12. Worm
 13. Crack
 14. Cookie
 15. Script
 16. Macro
 17. Plugin
 18. Phishing
 19. Spam
3. Lutter contre les menaces (conseils basiques)
 1. Prévention des menaces
 1. Si vous ne savez pas, ne cliquez pas
 2. Si vous ne connaissez pas, ne vous y fiez pas
 3. Un antivirus ne remplace pas votre vigilance
 4. Les 10 règles immuables de la sécurité informatique
 2. Neutralisation des menaces



1. Ne pas connecter un ordinateur directement à Internet
 2. Utiliser un Firewall
 1. Paramétrer le Firewall de Windows 7
 2. Utiliser un Firewall tiers
 3. Utiliser un Firewall sur Mac
 4. Le filtrage des connexions sortantes n'est pas toujours suffisant
 5. Ressources firewall et réseau
 3. Mettre à jour régulièrement ses logiciels
 4. Utiliser les logiciels de sécurité adaptés aux menaces
 5. Désactiver les scripts, macros et plugins
 1. Désactiver les macros
 2. Désactiver les scripts et plugins dans les pages Web
 6. Nettoyer les cookies et le cache de navigation
 3. Suppression des menaces
 4. Lutte contre les menaces (conseils avancés)
 1. Identifier les services et processus en cours
 2. Filtrer les IP
 3. Utiliser un VPN
 1. Structure du réseau Internet
 2. Principe des proxy VPN
 3. Quelques aspects juridiques
 4. Remarques complémentaires
 4. TOR
 1. Principe
 2. Mise en oeuvre
 3. Critique
 5. SSL/https
-

6. Utiliser un OS fiable
 7. Placer les fichiers importants sur support amovible
 8. Opérations critiques : utiliser un OS “Live USB”
 9. Chiffrer les données sensibles
 1. Inconvénients
 2. Sécurité
 3. Mise en oeuvre
 4. Aspects juridiques
 10. Utiliser un clavier virtuel
 11. Vérifier l'état physique du matériel
 12. Changer ses DNS au niveau du navigateur
 13. Sandboxing et Virtualisation
5. Conclusion



Quelques rappels juridiques

Avant d'aborder les aspects de technique informatique, il est nécessaire de procéder à quelques rappels juridiques.

Je vous parlais en effet, il y a quelques temps, du [projet de loi LOPPSI et de son article 23](#), permettant à l'autorité judiciaire de placer des logiciels « mouchards » dans des ordinateurs, à partir du réseau Internet. L'objet de l'article était de montrer que l'efficacité de ce procédé est extrêmement douteuse, puisqu'il existe de nombreux moyens de se protéger contre les logiciels nuisibles. Le présent article va plus loin en montrant comment mettre en oeuvre différentes techniques de protection contre les logiciels espion et les différentes menaces pour la sécurité des ordinateurs personnels.

La première question que peut se poser le lecteur, arrivé à ce stade de sa lecture, est celle de savoir si cet article a pour but d'expliquer comment violer la loi en empêchant la police judiciaire d'utiliser un logiciel espion. La réponse est négative. L'objet de cet article est beaucoup plus large puisqu'il s'agit de présenter certains moyens de se protéger contre *tous* les logiciels espion, et contre la plupart des menaces courantes de sécurité pour les ordinateurs personnels (à l'exclusion des serveurs). Ces moyens de protection sont techniques et, par conséquent, « neutres » : ils combattent telle ou telle technologie, sans prendre en compte la finalité de son utilisation. Si le dispositif de la loi LOPPSI est neutralisé par les mesures de protection décrites ici, c'est parce qu'il fonctionne comme de nombreux logiciels malicieux que ces mesures ont pour but de combattre.

Il faut ensuite rappeler qu'aucune règle de droit français n'interdit à une personne de sécuriser son ordinateur afin d'empêcher son utilisation frauduleuse. Au contraire, c'est l'utilisation de logiciels espion qui est pénalement incriminée : « *Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.* ». Le secret des correspondances, violé par les logiciels espions, est d'ailleurs protégé par l'article 8 de la [Convention européenne de sauvegarde des droits de l'Homme](#) et par

l'article 5 de la [directive 2002/58 « vie privée et communications électroniques »](#).

Toutes les techniques décrites ici sont donc parfaitement licites, dès lors qu'on les utilise afin de se protéger contre les atteintes à l'intimité de sa vie privée et non dans le but de violer la loi ou de causer préjudice à autrui.



Typologie des menaces

« Connais ton ennemi et connais-toi toi-même; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux. Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales. Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites. »

(Sun Tzu, [L'Art de la guerre](#), Chapitre 3)

Avant de savoir *comment* se défendre, il faut savoir *contre quoi* se défendre. Voici donc une description non exhaustive des principaux types de menaces.

Il est important de noter que **ces menaces ne sont pas exclusives les unes des autres**. Bien au contraire, dans la plupart des cas, elles oeuvrent de concert pour compromettre la sécurité du système et permettre la réalisation d'agissements frauduleux.

Malware

Le terme *malware* ne désigne pas un type particulier de logiciel en fonction de la technique employée mais, plus généralement, tous les logiciels « nuisibles » ou « malicieux ».

Spyware

Le terme générique *spyware* désigne tous les logiciels qui ont pour finalité de recueillir des données sur l'ordinateur d'une personne à son insu, puis de les transmettre par Internet à une tierce personne.



Trojan [horse]

Les *chevaux de Troie* sont des logiciels qui reprennent certaines caractéristiques du cheval introduit par Ulysse dans la ville de Troie :

- un cheval de Troie est généralement (mais pas toujours) caché dans un autre logiciel que l'utilisateur installera en toute confiance sur son système ;
- un cheval de Troie se cachera dans les fichiers système et évitera de signaler sa présence à l'utilisateur (il sera alors probablement accompagné d'un *rootkit*) ;
- un cheval de Troie (particulièrement bien conçu) parasitera un exécutable système afin d'être identifié par l'utilisateur et par le système d'exploitation, non en tant que tel, mais comme une composante de ce dernier ;
- un cheval de Troie ouvrira une connexion Internet entre l'ordinateur infecté et un serveur tiers (tout comme les Grecs ouvrirent les portes de Troie, une fois sortis de leur cheval) ;

On distingue deux grandes catégories de chevaux de Troie. Ceux de la première catégorie ont pour but de récupérer des données personnelles (adresses e-mail, mots de passe, numéro de carte bancaire, etc.) et de les transmettre à l'auteur du logiciel. Ceux de la deuxième catégorie ont pour but de transformer l'ordinateur en « zombie » et de le mettre au service de l'auteur du logiciel, afin de mener une attaque de grande ampleur. Dans la plupart des cas, il s'agira d'une attaque de *spam*, qui consiste à utiliser l'ordinateur comme serveur d'envoi de courrier électronique, ou d'une [attaque DDoS](#), visant à saturer un serveur en l'inondant de requêtes.

Keylogger

Le terme *keylogger* désigne un logiciel qui « capture » et enregistre (« log » signifie « [journaliser](#) ») les touches du clavier (« key ») pressées par l'utilisateur. Un keylogger permet donc de récupérer en clair les mots de passe entrés par l'utilisateur lors de ses visites sur le Web. Peu importe, à cet égard, que la connexion entre l'ordinateur et le serveur du site visité soit sécurisée (v. *infra*), puisque le keylogger agit sur l'ordinateur de l'internaute, lorsqu'il utilise son clavier. Les chevaux de Troie installent parfois des keyloggers, et ceux-ci sont la plupart du temps accompagnés d'un rootkit.

Screenlogger

Il s'agit d'un logiciel qui capture et enregistre les images affichées à l'écran en agissant, non pas sur le clavier comme un keylogger, mais sur la carte graphique de l'ordinateur.

Rootkit

Le terme « root » (qui signifie « racine ») désigne, en langage informatique, l'administrateur système. L'utilisateur root est unique, sur chaque système, et ignore toutes les restrictions de lecture, d'écriture et d'exécution des fichiers de l'ordinateur. Autrement dit, l'utilisateur root peut tout faire, sans aucune restriction. Un « rootkit » est un logiciel qui a pour but d'activer et d'utiliser les pouvoirs de l'utilisateur root, ou de permettre à un logiciel malveillant ou à une personne d'utiliser localement ou à distance le compte root. Il est fréquent que les rootkits utilisent les pouvoirs de l'utilisateur root afin de se dissimuler dans le système, d'empêcher leur suppression par l'utilisateur, de se lancer au démarrage du système, et se relancer en cas de crash ou d'arrêt manuel, etc. Les rootkits neutralisent en outre la plupart des techniques de protection présentées dans cet article. Par exemple, ils n'apparaîtront pas dans la liste des processus actifs (v. *infra*) ou ils désactiveront le firewall et l'antivirus, empêchant ainsi leur détection. Les rootkits servent généralement de support à un autre type de menace. De tous les logiciels nuisibles présentés ici, ce sont les plus dangereux.

Bootkit

Le terme *bootkit* désigne un logiciel malveillant qui agit au niveau du lancement de la machine (*boot*). Pour mémoire, un ordinateur se lance selon la séquence suivante : lancement du BIOS (firmware) qui donne les premières instructions au processeur et permet de localiser les volumes de démarrage (e.g. le disque dur sur lequel est installé le système d'exploitation), lecture du MBR (*Master Boot Record*) qui se charge de lancer le *BootLoader*, qui lance à son tour et l'*OSLoader* et le noyau du système d'exploitation. Les premiers bootkits étaient des virus placés sur une disquette et s'insérant dans le MBR du disque dur lorsque

l'ordinateur était démarré à partir de la disquette. Ces virus nécessitant un accès physique à la machine et reposant sur un support tombé en désuétude (les disquettes), ils ont aujourd'hui disparu. Toutefois, de nouvelles menaces se propageant par le réseau sont récemment apparues –[depuis une proof of concept de 2005](#)–, et se comportent comme les bootkits traditionnels (avec, bien entendu, les différences nécessaires à leur mise en oeuvre à distance). Le bootkit le plus connu est [sinowal](#). Les bons côtés des bootkits : 1) leur difficulté de mise en oeuvre (ce sont des logiciels particulièrement sophistiqués, que seuls des experts peuvent élaborer) ; 2) ils sont de ce fait très rares ; 3) ils ne sont pas forcément très difficiles à supprimer –démarrer Windows en mode console, puis taper la commande **fixmbr** est parfois suffisant–. Les mauvais côtés des bootkits : puisqu'ils agissent au niveau du boot 1) il est très difficile de s'en protéger ; 2) une fois l'ordinateur infecté, le bootkit est tout puissant.

Backdoor

Littéralement « porte de derrière », une backdoor est une faille de sécurité introduite dans un système afin de permettre l'intrusion ou la prise de contrôle de l'ordinateur à l'insu de l'utilisateur. Il ne s'agit pas d'un type de logiciel, mais de la conséquence de l'exécution de certains logiciels nuisibles, tels que les rootkits.

Rogue

Le mot « rogue » peut être traduit par « malfrat », « voyou » ou « corrompu ». Les logiciels *rogue* s'entourent d'une apparence de respectabilité afin de masquer leurs véritables desseins. L'exemple le plus courant de *rogue* est le faux logiciel de sécurité, de nettoyage ou d'optimisation du système. Celui-ci s'installe à l'insu de l'utilisateur lorsqu'il navigue sur un site web conçu pour l'infecter. Le rogue modifie ensuite le centre de sécurité de Windows afin de remplacer l'antivirus installé (qu'il désactivera totalement au prochain démarrage de la machine). Le rogue présente l'interface graphique d'un antivirus -ou d'un anti-malware au sens large, ou d'un utilitaire de nettoyage ou d'optimisation du système, etc.-, mais n'a aucune de ses fonctions de protection : c'est une « coquille vide ». Le rogue vous fera croire que votre ordinateur est infecté, et qu'il peut le nettoyer, afin de vous amener à sortir votre carte bancaire... Bien



entendu, votre compte bancaire sera détourné par les auteurs du logiciel rogue, et celui-ci cessera tout simplement d'agir. Désinstaller un rogue sans endommager irrémédiablement le système peut être difficile (s'il a le soutien d'un rootkit), voire impossible. En outre, le rogue désactivant toutes les protections de l'ordinateur, il vous expose à de nombreuses menaces. Mais, paradoxalement, il est facile de ne pas être infecté par un rogue : il suffit, avant d'installer un prétendu logiciel de protection ou d'optimisation du système, d'en vérifier la réputation auprès de la communauté des internautes (concrètement : tapez le nom du logiciel sur Google, et lisez les avis).

Adware

Le préfixe « ad » est la contraction du mot anglais « advertisement » signifiant, ici, « publicité ». Un adware est donc un logiciel introduisant de la publicité sur un ordinateur, sans qu'elle ait été sollicitée ou même acceptée par l'utilisateur.

Virus

Le virus informatique partage plusieurs caractéristiques des virus biologiques :

- il « infecte » des fichiers exécutables, c'est-à-dire qu'il les modifie en se rajoutant à leur contenu ;
- il a pour but premier de se « répliquer », c'est-à-dire d'infecter d'autres fichiers exécutables lorsque le fichier exécutable porteur est exécuté ;
- il est nuisible au système (en général, il détruit les fichiers comme un virus biologique détruit des cellules).

Il existe des [sous-catégories de virus](#) qui partagent les caractéristiques précitées tout en se différenciant sur d'autres points.

Worm

Les vers sont des virus évolués dont les deux caractéristiques principales sont les suivantes :

- un ver est autonome : il n'a pas besoin de parasiter un fichier exécutable ;



- un ver a pour but de se propager dans un réseau d'ordinateurs, là où le virus classique se limite à infecter les fichiers sains de l'ordinateur sur lequel il se trouve.

Crack

Un « crack » est un logiciel ayant pour fonction de « casser » les protections d'un autre logiciel. La plupart des cracks visent les logiciels commerciaux, afin de permettre leur utilisation sans acquérir de licence d'utilisation auprès de leur éditeur. Les cracks ne sont, *a priori*, pas nuisibles au système sur lequel ils sont exécutés. Toutefois, de nombreux cracks véhiculent des logiciels nuisibles comme des chevaux de Troie, des virus ou des vers.

Cookie

Les cookies ne sont pas des logiciels nuisibles. Ce ne sont pas des logiciels et ils ne sont, en principe, pas nuisibles. Ce sont des fichiers de texte brut enregistrés par un navigateur web sur le disque dur de l'ordinateur de l'internaute, afin que certaines informations persistent après que l'internaute ait quitté un site, et soient disponibles lorsqu'il le visite à nouveau. Les cookies fournissent un grand confort à l'utilisateur qui n'aura pas à saisir les mêmes informations (par exemple, son nom d'utilisateur et son mot de passe) à chaque visite d'un site. Cependant, les cookies présentent un danger dès lors qu'ils contiennent des informations personnelles entrées par l'internaute. On appelle « cookies traceurs » (*tracking cookies*) les cookies trop indiscrets, qui ont pour but de créer un profil commercial ou comportemental de l'utilisateur.

Script

Les scripts font partie, comme les cookies, des techniques permettant d'augmenter le confort d'utilisation des sites Web. A l'origine, les pages Web écrites dans le langage HTML étaient purement « passives » : elles se contentaient de décrire au navigateur un contenu à afficher. Les scripts permettent de les rendre « actives » en demandant au navigateur de *faire* telle

ou telle chose. En d'autres termes, les pages dépourvues de script ont un « état » alors que les pages pourvues de scripts ont un « comportement ». A l'instar des cookies, certains scripts peuvent être malicieux et engendrer un risque pour la sécurité des données de l'utilisateur ou de son système.

Macro

Les macros sont des scripts insérés, non pas dans une page Web, mais dans un fichier. Les macros sont exécutées par le logiciel qui ouvre le fichier et ne sont pas, *a priori* nuisibles. La plupart des macros malicieuses se situent dans des fichiers MS Word (.doc) ou Excel (.xls).

Plugin

Les plugins sont des logiciels tiers greffés au navigateur afin de lui permettre d'afficher certains contenus multimédia. Par exemple, le plugin *Flash* est actuellement nécessaire pour afficher les vidéos sur YouTube. Comme les cookies et les scripts, les plugins sont, en principe, des moyens d'améliorer l'expérience de l'utilisateur sur le web. Ils peuvent également constituer un risque pour la sécurité, lorsqu'un site malicieux parvient à exploiter une faille de sécurité. En outre, ils ralentissent considérablement le navigateur (voire le système) et l'affichage des pages. Ils peuvent également entraîner des « crash » du navigateur. Pour couronner le tout, ils permettent d'afficher de nombreux bandeaux publicitaires sur les pages Web.

Phishing

Le « phishing » (ou « hameçonnage » en français québécois) est une technique qui consiste à amener l'utilisateur sur un site web, tout en lui faisant croire qu'il visite un autre site. Ainsi, l'internaute piégé fournit ses coordonnées bancaires lorsqu'il se trouve sur le site d'une personne mal intentionnée alors qu'il croit se trouver sur le site de sa banque.



Spam

Un « spam » est un courrier électronique non sollicité. La plupart des spams (mais pas tous) sont malveillants : ils participent souvent au phishing, ou à des escroqueries réalisées dans le monde réel. Compte tenu des mesures anti-spam prises ces dernières années par la plupart des fournisseurs de courrier électronique, les personnes à l'origine du spam ont progressivement évolué de l'utilisation d'un serveur dédié vers l'infection des ordinateurs des internautes par des vers ou chevaux de Troie, afin d'envoyer leurs messages depuis ces ordinateurs.

Concernant l'infection par un virus (cheval de troie, ver, etc.) originaire d'un e-mail, voir l'article : [Démystification: peut-on être infecté par un virus à cause d'un e-mail ?](#).

Lutte contre les menaces (conseils basiques)

La lutte contre les différentes menaces précédemment exposées, qu'elles se présentent individuellement ou simultanément, passe par deux étapes, avant infection, de prévention et de neutralisation et par une troisième étape, en cas d'infection, de suppression.

Prévention des menaces

#1 – « Si vous ne savez pas, ne cliquez pas »

Une blague courante parmi les informaticiens dit que « *le seul danger se situe entre la chaise et le clavier* ». Bien entendu, ce n'est pas vrai. Pourtant, il est indéniable que la plupart des failles de sécurité sont créées par les utilisateurs eux-mêmes, qui manquent d'information et de vigilance. La mauvaise connaissance de l'informatique et la crédulité des utilisateurs sont très

largement exploitées par les personnes à l'origine des menaces précédemment décrites. « *Donnez-nous votre adresse e-mail* » (... pour que nous puissions vous envoyer des spams), « *suivez ce lien vers le site de votre banque* » (... qui n'est pas vraiment le site de votre banque, mais qui vous demandera tout de même votre mot de passe), « *ouvrez ce fichier qu'un ami vous envoie* » (... ou plutôt, que l'ordinateur infecté d'un ami vous envoie, pour infecter votre ordinateur), etc.

La première règle de sécurité est donc la plus importante : en cas de doute, ne cliquez pas, n'acceptez pas, ne validez pas... En cas de doute, quittez la page web, supprimez le fichier, fermez le logiciel, etc.

Sous Windows, par exemple, un logiciel qui tente de modifier les fichiers système générera une boîte de dialogue vous demandant si vous voulez autoriser l'exécution de ce logiciel avec les privilèges administrateur (root). Depuis cette fenêtre, vous pouvez connaître l'emplacement exact de l'exécutable, son éditeur et vérifier l'éventuel certificat numérique de cet éditeur. Si les informations indiquées par Windows à propos de ce logiciel vous paraissent suspectes, refusez lui les privilèges administrateur. Il en va de même sous Mac, où une boîte de dialogue vous demandera de taper le mot de passe administrateur afin de permettre l'exécution du logiciel. Sous Linux, vous devrez exécuter le logiciel en tant qu'administrateur (avec la commande *sudo*), ce qui suppose que vous lui faites confiance.

#2 – « Si vous ne connaissez pas, ne vous y fiez pas »

De la première règle découle une seconde règle, tout aussi importante : en cas de doute, vous devez présumer le pire.

Par exemple, ne téléchargez pas de logiciels « craqués » ou de cracks sur Internet. Toutes les personnes qui diffusent des logiciels contrefaits ne sont pas des idéalistes libertaires luttant contre la société de consommation. Certaines sont très bien intégrées dans cette société de consommation, et ne vous fournissent gratuitement un logiciel payant que parce qu'elles l'ont préalablement infecté avec un logiciel nuisible qui leur transmettra vos informations personnelles. Pour une sécurité optimale, achetez vos logiciels auprès de leur éditeur.



Ne faites pas non plus confiance aux ordinateurs des cyber-cafés : ils sont probablement sur-infectés, et vous n'avez aucun moyen de le savoir. Ne tapez donc jamais des mots de passe importants, et n'achetez rien en ligne, sur l'ordinateur d'un cyber-café (à moins d'utiliser un système *live* ; v. *infra*).

Ne restez pas dans l'ignorance. Si vous avez un doute sur un site, un fichier, un logiciel, consacrez un peu de votre temps à rechercher des informations sur le Web. Vous saurez alors généralement si vous pouvez avoir confiance, ou pas, en fonction de ce qu'en disent les internautes.

#3 – « Un antivirus ne remplace pas votre vigilance »

Nombreux sont les utilisateurs qui installent un antivirus et croient pouvoir ainsi ne plus se préoccuper de la sécurité de leur ordinateur. Cassons tout de suite le mythe : aucun antivirus ne protège contre toutes les menaces. Certains ne protègent tout simplement pas contre un certain type de menaces ([par exemple, les rootkits](#)). Tous ignorent certaines menaces appartenant à des types de menaces connus (99% de menaces détectées, ce n'est pas 100%...).

Un antivirus peut, sous Windows, vous permettre de ne pas tomber dans la paranoïa et d'avoir l'esprit un peu plus tranquille. Mais il n'exonère pas pour autant de prendre certaines mesures basiques de sécurité.

#3 – Les 10 règles immuables de la sécurité informatique

Microsoft a publié, dans sa base de données technique destinée aux professionnels, [les 10 règles immuables de la sécurité informatique](#). Il n'est pas question de discuter ici du caractère exhaustif de cette liste ou de la formulation des règles, mais simplement de les exposer. En voici donc une traduction en français :

1. Si une personne mal intentionnée vous persuade de lancer son logiciel sur votre ordinateur, ce n'est plus votre ordinateur.



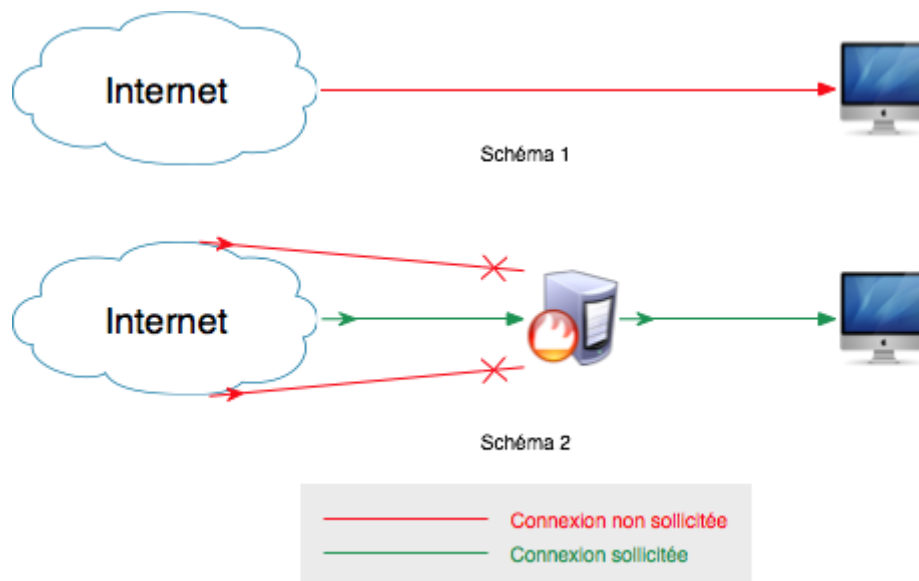
2. Si une personne mal intentionnée est en mesure de modifier le système d'exploitation de votre ordinateur, ce n'est plus votre ordinateur.
3. Si une personne mal intentionnée possède un accès physique illimité à votre ordinateur, ce n'est plus votre ordinateur.
4. Si vous permettez à une personne mal intentionnée de mettre en ligne des logiciels sur votre site Web, ce n'est plus votre site web.
5. Un mot de passe trop simple rend inopérantes toutes les autres mesures de sécurité.
6. La sécurité d'un opérateur est proportionnelle au degré de confiance que l'on peut placer en son administrateur.
7. La sécurité des données chiffrées est proportionnelle à la sécurité de la clé de déchiffrement.
8. Un antivirus qui n'est pas mis à jour ne vaut pas mieux qu'aucun antivirus.
9. L'anonymat total est illusoire, tant dans la vie réelle que sur le Web.
10. La technologie n'est pas la panacée.

Neutralisation des menaces

#1 – Ne pas connecter un ordinateur directement à Internet

Un ordinateur connecté directement au réseau, sans protection et sous Windows, ne restera pas plus de quelques minutes avant d'être infecté par un logiciel malveillant (probablement un ver). De la même manière, le système sera directement exposé sur le réseau et ses failles de sécurité pourront aisément être exploitées par des personnes mal intentionnées.

Il est donc très important d'éviter toute connexion directe au réseau, en passant par un routeur.



Le schéma ci-dessus expose les deux configurations. Dans le premier cas, l'ordinateur est connecté directement au réseau (avec un modem analogique, par exemple). L'adresse IP visible sur Internet est celle de l'ordinateur. Dans le second cas, l'ordinateur est connecté au routeur, qui lui attribue une adresse IP dans le réseau interne. L'adresse IP visible sur Internet est celle du routeur, et non celle de l'ordinateur.

Sans rentrer dans les détails techniques (que vous trouverez notamment dans l'article [sur la Livebox et Airport](#)), on pourrait dire que, schématiquement :

- sans routeur, l'ordinateur reçoit toutes les connexions ouvertes par d'autres ordinateurs depuis Internet ;
- avec un routeur, l'ordinateur ne reçoit aucune connexion de l'extérieur et ne peut communiquer avec d'autres ordinateurs que s'il prend l'initiative de les contacter.

Le routeur fait office de « filtre » entre l'ordinateur et le réseau. Il constitue une première barrière de sécurité efficace et indispensable.

#2 – Utiliser un Firewall

La plupart des routeurs font également office de *firewall* (« pare-feu ») matériel, c'est-à-dire de dispositif de filtrage des connexions entre votre ordinateur et

Internet. Ce premier niveau de protection doit être complété par un second niveau logiciel, sur l'ordinateur.

Les firewalls logiciels permettent en effet une protection beaucoup plus fine que les firewalls des « box » Internet des fournisseurs d'accès. Schématiquement, le routeur matériel (du moins, tel que présent dans les « box » des fournisseurs d'accès français) se limite à n'autoriser que les connexions qui suivent une certaine route, sans se préoccuper de leur provenance et de leur destination. Les firewalls logiciels permettent d'interdire des connexions en fonction de leur provenance ou de leur destination, même si elles passent par la bonne route.

Les firewalls logiciels *bidirectionnels* agissent sur les connexions *entrantes* (d'Internet vers votre ordinateur) et les connexions *sortantes* (de votre ordinateur vers Internet). Les deux types de filtrage sont complémentaires :

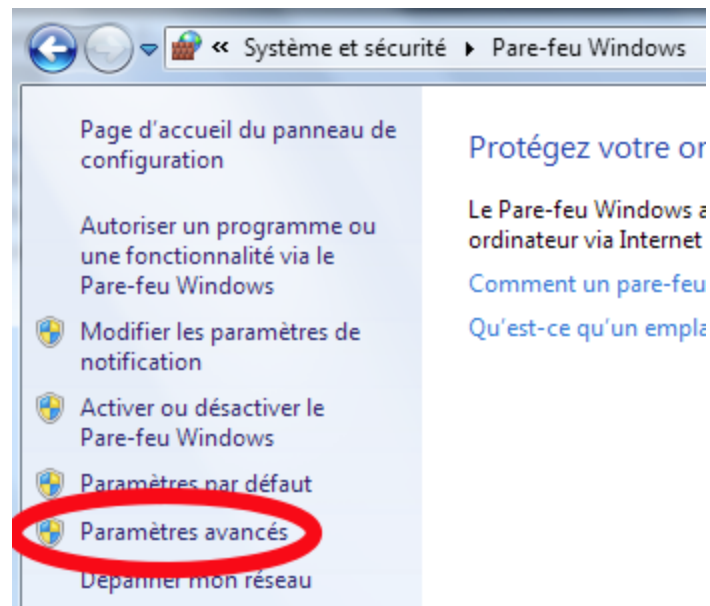
- un bon filtrage des connexions entrantes réduit les risques d'infection (par des vers, notamment) et l'exploitation des failles de sécurité ;
- un bon filtrage sortant permet, en cas d'infection, d'empêcher les données de l'ordinateur d'être communiquées à des tiers par Internet.

Le firewall intégré à Windows 7 est paramétré par défaut pour filtrer les connexions entrantes : il les refuse toutes, sauf celles qui correspondent à une demande de l'utilisateur. En revanche, il ne filtre aucune connexion sortante : elles sont toutes autorisées. Il est donc nécessaire de modifier ce dernier paramétrage, afin de refuser toutes les connexions sortantes, sauf celles expressément autorisées par l'utilisateur. C'est une condition insuffisante à elle seule, mais absolument nécessaire, à la neutralisation des logiciels espion.

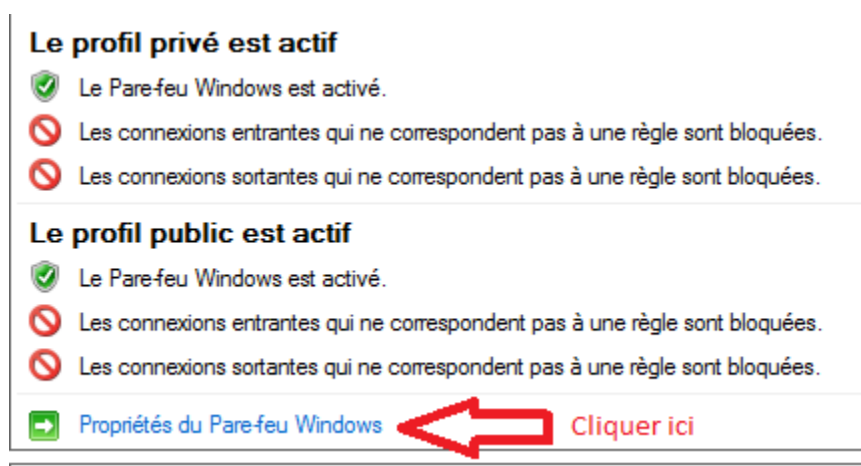
Paramétrer le Firewall de Windows 7

1) Ouvrez le **menu Démarrer**, puis le **Panneau de configuration**. Allez dans **Système et sécurité**, puis **Pare-feu Windows** et cliquez, dans le menu à gauche de la fenêtre, sur **Paramètres avancés**.

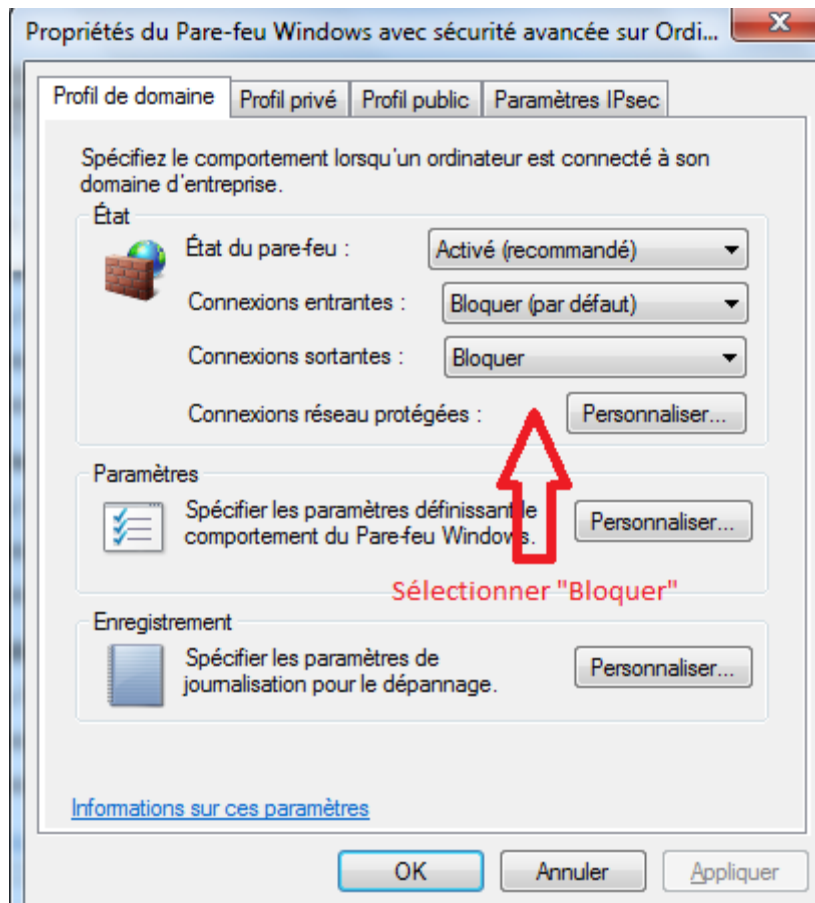




2) Cliquez ensuite sur **Propriétés du pare-feu Windows**, au centre de la fenêtre de configuration.

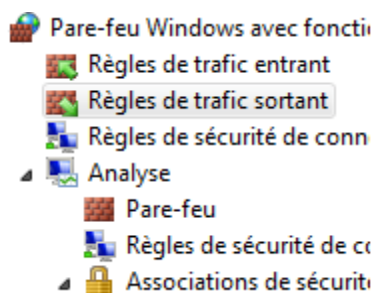


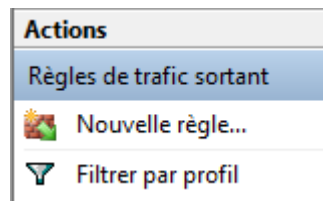
3) Dans les 3 onglets *Profil du domaine*, *Profil privé* et (surtout) *Profil public*, sélectionnez **Bloquer** dans le menu déroulant **Connexions sortantes**. Cliquez également sur le bouton **Personnaliser...** et vérifiez que toutes les cases sont cochées. Validez les modifications et fermez la fenêtre en cliquant sur **OK**.



Après ces trois étapes, toutes les connexions sortantes sont bloquées. Cela signifie plus aucun de vos logiciels n'a accès à Internet. Il faut donc ensuite autoriser « manuellement » les connexions sortantes pour certaines logiciels, en lesquels vous avez confiance. Les étapes suivantes sont à répéter pour chaque logiciel que vous voulez autoriser à envoyer des données par Internet.

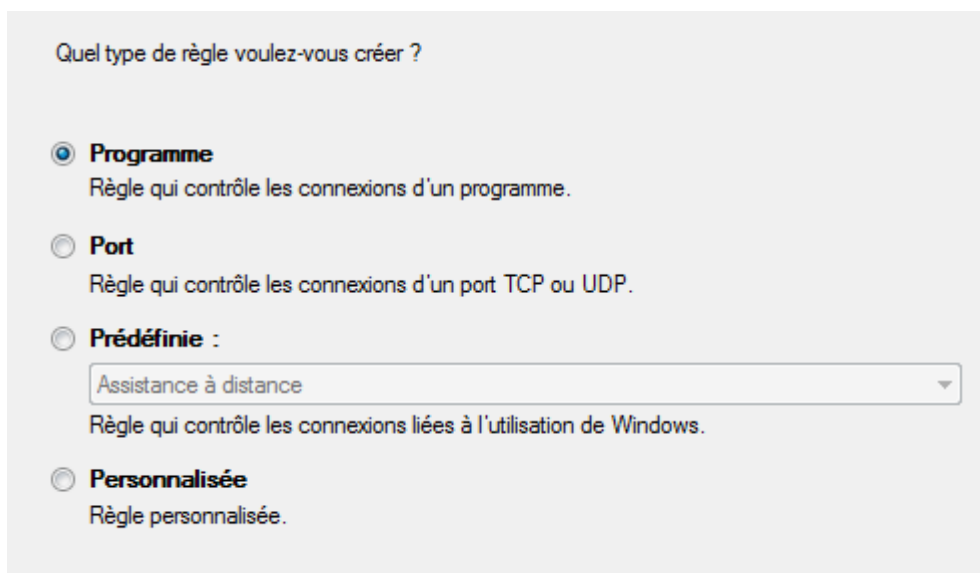
4) En haut à gauche de la fenêtre du logiciel d'administration du firewall de Windows (si vous n'avez plus cette fenêtre, reportez-vous à l'étape 1. ci-dessus), cliquez sur **Règles de trafic sortant**, puis, dans la partie droite de la même fenêtre, cliquez sur **Nouvelle règle**.





5) L'assistant de création de règles personnalisées s'affiche à l'écran. La première page de l'assistant vous propose de choisir le type de règle. Vous pouvez en effet créer des règles relatives aux logiciels, aux ports, aux services Windows, ou à plusieurs de ces éléments en même temps. Le plus simple est de créer une règle par logiciel : sélectionnez

Programme et cliquez sur **Suivant**.



6) Sélectionnez **Au programme ayant pour chemin d'accès...**, cliquez sur **Parcourir...** et sélectionnez le fichier exécutable (se terminant par « .exe ») du logiciel que vous voulez autoriser. Vous trouverez vos logiciels dans *C:\Program Files* ou *C:\Programmes*. En l'occurrence, nous avons choisi de créer la règle pour Internet Explorer. Cliquez sur **Suivant**.

Cette règle s'applique-t-elle à tous les programmes ou à un programme spécifique ?

☐ **Tous les programmes**
La règle s'applique à toutes les connexions de l'ordinateur qui correspondent à d'autres propriétés de règles.

☒ **Au programme ayant pour chemin d'accès :**

Exemples : c:\chemin\program.exe
 %ProgramFiles%\Internet Explorer\iexplore.exe

7) Sélectionnez **Autoriser la connexion**, puis cliquez sur **Suivant**.

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

☒ **Autoriser la connexion**
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

☐ **Autoriser la connexion si elle est sécurisée**
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

☐ **Bloquer la connexion**

😊 Sélectionnez **Domaine** et **Privé**. Ne sélectionnez **Public** que pour les logiciels vraiment indispensables que vous êtes susceptibles d'utiliser avec une connexion dans un lieu public (par exemple, un navigateur internet ou un logiciel de messagerie). Cliquez sur **Suivant**.

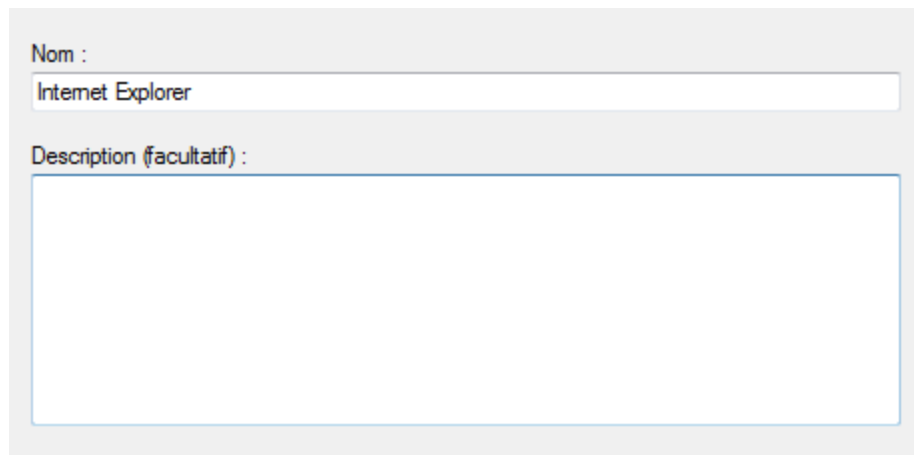
Quand cette règle est-elle appliquée ?

☒ **Domaine**
Lors de la connexion d'un ordinateur à son domaine d'entreprise.

☒ **Privé**
Lors de la connexion d'un ordinateur à un emplacement réseau privé.

☒ **Public**
Lors de la connexion d'un ordinateur à un emplacement public.

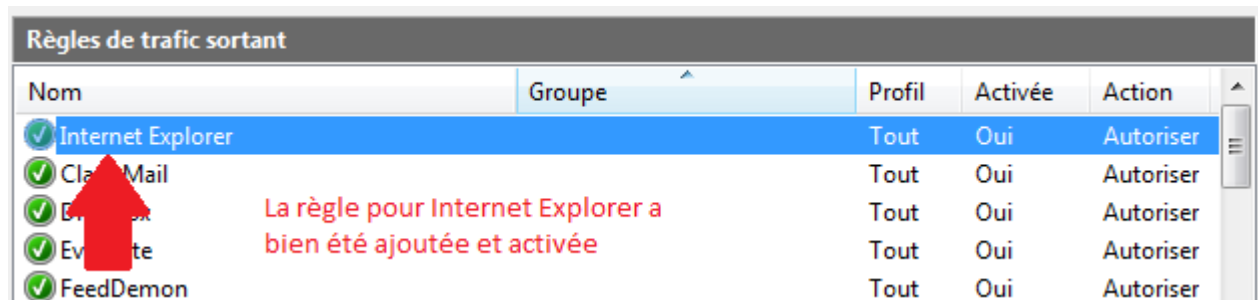
9) Donnez un nom à la règle. Indiquer le nom du logiciel est une bonne idée. Cliquez ensuite sur **Terminer**.



Nom :
Internet Explorer

Description (facultatif) :

Vous pouvez vérifier que la règle a bien été créée dans la liste des règles du trafic sortant. Les règles actives ont une pastille verte à gauche de leur nom, tandis que les règles inactives ont une pastille grise. N'activez une règle que si vous êtes certain d'en avoir besoin.



Règles de trafic sortant				
Nom	Groupe	Profil	Activée	Action
✓ Internet Explorer		Tout	Oui	Autoriser
✓ Classic Mail		Tout	Oui	Autoriser
✓ Evénement		Tout	Oui	Autoriser
✓ Événement		Tout	Oui	Autoriser
✓ FeedDemon		Tout	Oui	Autoriser

La règle pour Internet Explorer a bien été ajoutée et activée

Utiliser un firewall tiers

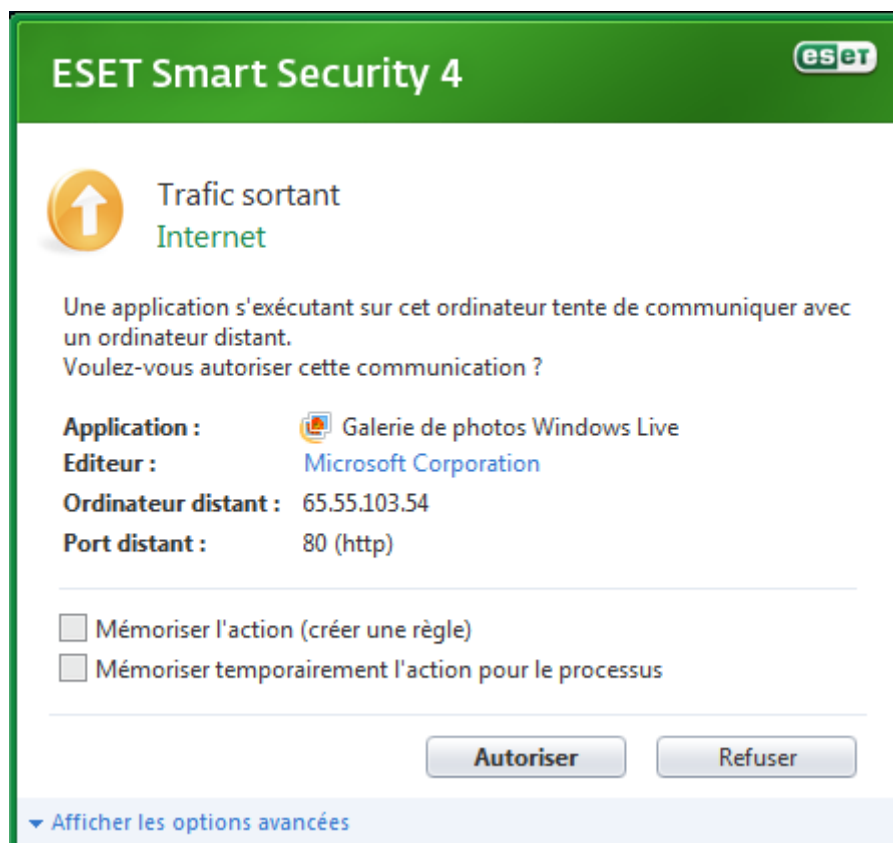
Le firewall intégré à Windows 7 est parfaitement efficace et suffisant pour une utilisation domestique. Il présente également l'avantage d'être gratuit et préinstallé avec le système. La procédure de création de règles personnalisées pour chaque logiciel peut toutefois se révéler rapidement fastidieuse. Vous pouvez donc lui préférer un firewall commercial qui vous permettra de créer des règles plus facilement et plus rapidement.

Les firewalls commerciaux sont nombreux sous Windows. En voici quelques uns :

- [ZoneAlarm](#)
- [Comodo](#)

- [ESET SmartSecurity](#)
- [Kaspersky](#)
- [Norton](#)

Quel que soit votre choix, pensez à vérifier que le firewall puisse être paramétré de manière à vous proposer la création d'une règle pour chaque nouvelle connexion (Norton le permet, Kaspersky non). Voici un exemple de la fenêtre qu'ouvre le firewall d'ESET lorsqu'il détecte une nouvelle connexion ne correspondant à aucune règle existante :



Utiliser un Firewall sur Mac

Bien qu'il n'existe, à l'heure actuelle, aucune menace *sérieuse* sur Mac, le filtrage des connexions sortantes n'est pas superflu, ne serait-ce que pour *avoir le choix* de permettre ou d'interdire à vos logiciels de communiquer avec l'extérieur.

L'excellent [Little Snitch](#) vous permet d'intercepter toute connexion sortante et de créer une règle en quelques clics. Little Snitch est un firewall unidirectionnel (il ne filtre que le trafic sortant), mais il est particulièrement bien réalisé. Ainsi,

lorsqu'une connexion sortante est détectée, Little Snitch vous permet d'autoriser ou de refuser la connexion :

- pour ce logiciel / vers le serveur contacté / sur le port utilisé / sur le port et vers le serveur
- une fois / jusqu'à la fermeture du logiciel / pour toujours.



Mac OS X est par ailleurs livré avec un firewall intégré, qui n'est pas activé par défaut. Pour l'activer, il faut se prendre dans le *menu Pomme > Préférences système > section Sécurité > onglet Coupe-feu*.

Le filtrage des connexions sortantes n'est pas toujours suffisant

Le filtrage des connexions sortantes est nécessaire, mais insuffisant. En effet, le filtrage manuel, tel que présenté ici, pose plusieurs problèmes majeurs.

En premier lieu, il ne protège pas contre l'injection d'un code malicieux dans un logiciel fiable. Le scénario est le suivant : vous autoriser un logiciel en lequel vous avez confiance (par exemple, Internet Explorer) ; vous êtes infecté par un malware qui modifie ce logiciel, afin de faire passer par lui ses connexions vers Internet ; votre firewall respecte la règle autorisant les connexions de ce logiciel,

sans savoir qu'il a été modifié. Il est donc indispensable, sous Windows, de compléter le filtrage des connexions sortantes par d'autres techniques, notamment un antivirus (au sens large) et un système permettant de détecter les modifications malveillante de vos logiciels.

En deuxième lieu, le paramétrage manuel des connexions sortantes peut vous amener à créer, par inadvertance, une règle permissive qui supprime les autres règles. Considérez par exemple les règles suivantes : *bloquer toutes les connexions* ; *autoriser les connexions sur le port 80* ; *autoriser les connexions du logiciel X*. Aucune règle ne concerne spécifiquement le logiciel Y, il tombe donc sous le coup de la première règle, qui bloque toutes les connexions. Cependant, si le logiciel Y tente de communiquer par le port 80, la deuxième règle autorisera cette connexion. Il faut donc prendre garde à créer les règles les plus spécifiques possibles. A cet égard, *Little Snitch*, sur Mac, est très efficace puisqu'il permet de définir, pour chaque logiciel, le port et le serveur distant.

En troisième lieu, plus les règles sont précises, plus il doit y avoir de règles. La nécessité incessante de créer de nouvelles règles peut rapidement déranger l'utilisateur, qui prendra l'habitude d'accepter la connexion sans lire le message d'alerte. C'est l'effet « yes-whatever-button » constaté par les ingénieurs de Microsoft à propos de Windows Vista : à la *nième* alerte, l'utilisateur se dira « *encore un message, on s'en fiche, je clique sur oui* ». Il ne faut jamais relâcher sa vigilance, quitte à perdre quelques secondes. C'est la première leçon en matière de sécurité.

Ressources firewall et réseau

Divers outils en ligne permettent de tester l'efficacité de votre firewall et la cohérence de votre politique NAT :

- [ShieldsUp!](#)
- [McAfee HackerWatch](#)
- [Inoculer.com](#)
- [Norton Security Scan](#)
- [PCFlank](#)
- [Zebulon.fr](#) (en français)

Plus de renseignements (techniques) sur les Firewalls :

- [tauceti.jonction.free.fr](#)



Tests et classement des firewall pour Windows :

- Matousec.com

Liste des firewalls et utilitaires de sécurité pour Windows :

- SpywareWarrior

#3 – Mettre régulièrement à jour ses logiciels

La mise à jour régulière des logiciels est impérative afin de garantir la sécurité d'un ordinateur. Contrairement à ce que l'on pourrait penser, les logiciels ne sont plus, depuis longtemps, de simples mécanismes qui se contentent de faire une seule chose, d'une seule manière. Les logiciels sont de plus en plus complexes : ils permettent de faire de plus en plus de choses, et souvent d'obtenir un résultat de plusieurs manières. L'auteur d'un logiciel peut prévoir les résultats d'une action dans un certain contexte. Mais il ne peut pas envisager toutes les situations dans lesquelles cette action survient, qui sont susceptibles d'en modifier le résultat. Toutes ces situations imprévues constituent potentiellement des « failles de sécurité » ou des « bugs », lorsqu'elles aboutissent à l'altération du bon fonctionnement d'un logiciel. Les mises à jour des logiciels permettent de corriger les bugs et de [comblent les failles de sécurité](#).

Il est également important de mettre à jour les définitions des logiciels de protection (antivirus, firewall, filtre IP, anti-spyware, etc.) afin de prendre en compte les nouvelles menaces. Enfin, la mise à jour des pilotes matériel (« drivers »), sous Windows, peut améliorer la prise en charge de vos périphériques par le système, le rendant ainsi plus stable.

Il faut donc faire régulièrement les mises à jour :

- du système d'exploitation (Panneau de configuration > Windows Update ; Pomme > Mise à jour de logiciels... sous Mac ; ou votre gestionnaire de paquets sous Linux) ;
- de vos logiciels ;
- des signatures de vos logiciels de protection ;
- de vos pilotes, sous Windows.



#4 – Utiliser les logiciels de sécurité adaptés aux menaces

Un antivirus ne fait pas tout. Il protège contre les virus et les vers, mais pas forcément contre les autres types de menaces portant sur vos données personnelles et votre vie privée, malgré les vœux des utilisateurs. Installez donc, de préférence, un antivirus qui protège, au sens large, contre les logiciels nuisibles. Complétez cette installation par celle de logiciels spécialisés dans la lutte contre un type précis de menaces.

Pour vous protéger *spécifiquement* contre les logiciels espion et publicitaires, sous Windows 7 :

- [Microsoft Windows Defender](#) (intégré dans l'antivirus Microsoft Security Essentials)
- [Spybot Search&Destroy](#)
- [Malwarebytes' Anti-Malware](#)
- [SpywareBlaster](#)
- [SUPERAntiSpyware](#)
- [Ad-Aware](#)
- [Glary Utilities](#)
- etc.

Pour détecter *spécifiquement* les rootkits :

- [GMER](#) (Windows)
- [MS RootkitRevealer](#) (Windows)
- [RootkitBuster](#) (Windows)
- [F-Secure Blacklight](#) (Windows)
- [Rootkit Unhooker](#) (Windows)
- [IceSword](#) (Windows)
- [DarkSpy](#) (Windows)
- [chkrootkit](#) (Unix)
- [rkhunter](#) (Unix)
- [\[D'autres utilitaires anti-rootkit\]](#)

Ces logiciels n'offrent pas de protection en temps réel (du moins, pas tous et pas dans leurs versions gratuites), contrairement aux antivirus commerciaux. Cela n'est pas vraiment nécessaire. Ils permettent en revanche d'analyser l'ordinateur « manuellement », ou suivant une planification. Une analyse par semaine (précédée d'une mise à jour des définitions), est généralement suffisante. Eventuellement, vous pouvez procéder à une analyse après avoir installé de nouveaux logiciels, et avant de les utiliser.



Pour vous protéger en temps réel contre les menaces les plus importantes (virus, vers...) :

- [Microsoft Security Essentials](#) (gratuit, léger)
- [Avira](#) (gratuit, léger)
- [ESET Nod32](#) (léger et efficace)
- [Kaspersky](#) (lourd mais très complet)
- [Norton](#) (lourd mais très complet)
- [AVG](#)
- [F-Secure](#)
- [McAfee](#)
- [BitDefender](#)
- [G-Data](#)
- etc.

Pour une comparaison des différents antivirus, v. :

- [AV-Comparatives.org](#) (en anglais — les meilleurs comparatifs)
- [PegHorse's Blog](#) (tests en situation réelle, dans des vidéos en français)
- [AV-Test.org](#) (en anglais)
- [TopTenReviews](#) (en anglais)
- [CNET](#) (en anglais)
- [Firewallguide.com](#)
- [PCWorld](#)
- [Clubic](#)
- etc.

Vous pouvez également compléter votre logiciels antivirus et vos logiciels anti-spywares avec la consultation régulière de sites spécialisés, proposant des analyses en ligne basées sur des définitions des menaces actualisées en temps réel :

- [Inoculer.com](#) (en français)
- [Symantec Security Check](#)
- [McAfee Free Scan](#)
- [Kaspersky Free Virus Scanner](#)
- [Panda ActiveScan](#) et [MalwareRadar](#)
- [F-Secure Online Scanner](#)
- [BitDefender Online Scanner](#)
- [Avast OnlineScan](#)
- etc.

Enfin, en cas d'infection, il vous faudra probablement utiliser un logiciel spécialisé dans la désinfection (v. *infra*) :

- Logiciels de désinfection Kaspersky
- Logiciels de désinfection Norton
- Logiciels de désinfection Secuser
- Logiciel générique de désinfection Stinger (McAfee)
- Logiciel générique de désinfection Avast Cleaner

Pour plus d'informations sur l'évolution des menaces en temps réel :

- [Kaspersky Viruslist](#) (en français)

Liste des antivirus/malware et utilitaires de sécurité pour Windows :

- [SpywareWarrior](#)

#5 – Désactiver scripts, macros et plugins

Les scripts, macros et plugins sont des moyens parfaitement légitimes de rendre les fichiers ou les pages web « interactifs ». Ils sont indispensables pour réaliser certaines opérations et, plus généralement, très utiles afin d'améliorer l'ergonomie d'une interface. Il existe cependant des scripts, macros et des applications reposant sur certains plugins, qui sont extrêmement malveillants. Par exemple, un virus peut être transmis dans un fichier MS Word, à l'aide d'une macro ; un fichier PDF ou un bandeau Flash, chargés dans un navigateur, peuvent exploiter une faille de sécurité afin de nuire à l'ordinateur, etc.

La meilleure façon de se protéger contre ce type de menaces est de désactiver par défaut l'exécution des scripts, macros et plugins, et d'autoriser, au cas par cas, les scripts, macros et plugins sur les sites web ou dans les fichiers en lesquels on a confiance.

Désactiver les macros

Les macros sont des programmes exécutables insérés à l'intérieur de certains fichiers, qui le permettent (la plupart des fichiers ne le permettent pas). La plupart des macros malveillantes sont insérées dans des fichiers Microsoft Office, afin de viser une grande audience.

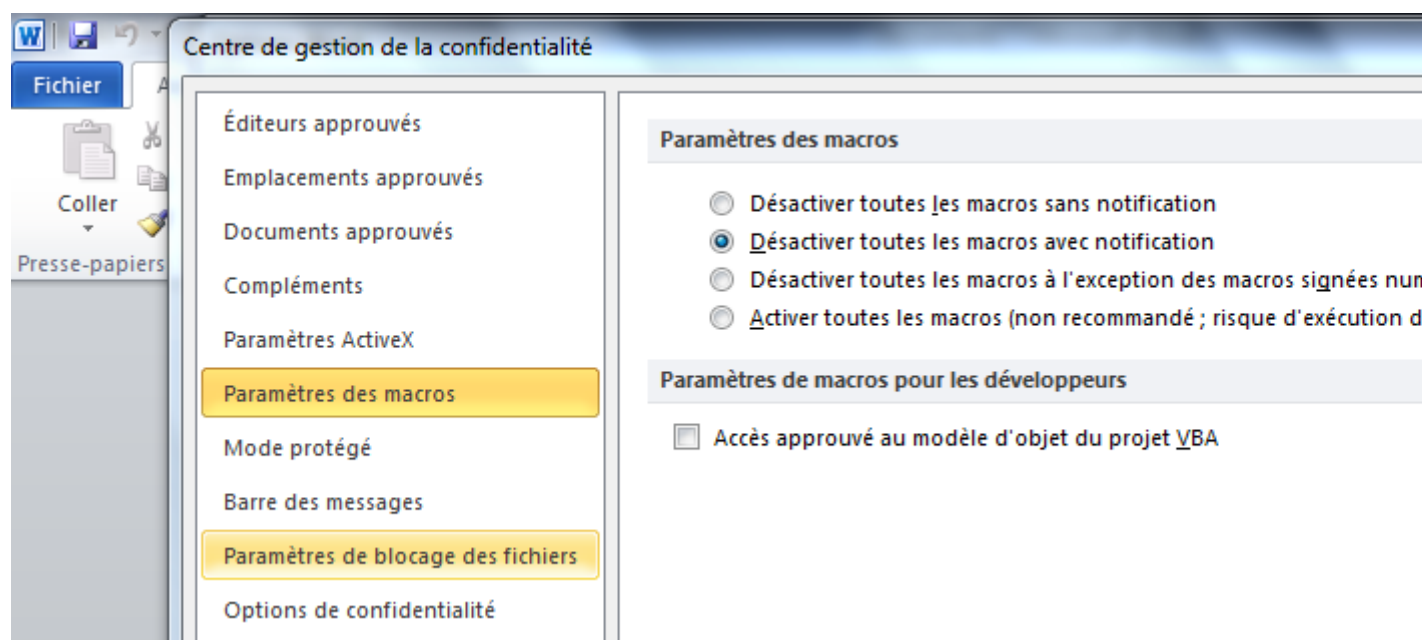
Pour se protéger contre les macros MS Office :

- analyser les fichiers MS Office reçus avant votre antivirus ;

- désactiver par défaut les macros dans MS Office, et ne les autoriser, pour un fichier donné, que si l'on est sûr que ce fichier n'est pas nuisible.

Dans Microsoft Word 2010, allez dans le menu **Fichier** et cliquez sur **Options**. Dans le menu à gauche de la fenêtre qui s'ouvre, sélectionnez **Centre de gestion de la confidentialité** puis, dans la partie droite de la même fenêtre, cliquez sur **Paramètres du Centre de gestion de la confidentialité**. Une troisième fenêtre s'ouvre. Dans le menu à gauche de cette fenêtre, cliquez sur **Paramètres des macros** puis, dans la partie droite, sélectionnez **Désactiver toutes les macros avec notification**.

NB : l'option **Désactiver toutes les macros à l'exception des macros signées numériquement** n'est pas sûre, dès lors qu'il est possible d'auto-signer une macro avec une fausse signature numérique.



Désactiver les scripts et plugins dans les pages Web

En premier lieu, et sans discussion possible, il ne faut plus utiliser Internet Explorer. Le navigateur peut être installé par défaut, rapide, beau, pratique, il n'en demeure pas moins qu'il n'est pas sécurisé. En outre, compte tenu de sa part de marché écrasante, il est le premier navigateur ciblé par les auteurs de logiciels malveillants.

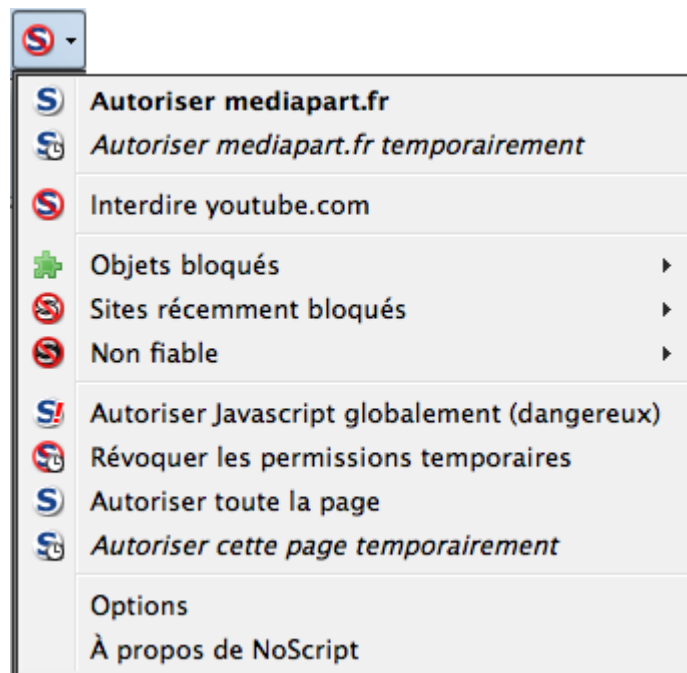
Il est préférable d'installer [Mozilla Firefox](#) avec les extensions suivantes :

- [AdBlock Plus](#)
- [NoScript](#)

La première extension, AdBlock Plus, permet de bloquer les éléments publicitaires contenus dans les pages Web. Sa fonction première n'est pas de renforcer la sécurité du navigateur, mais il y concourt. En effet, de nombreuses menaces passent, sur le Web, par des bandeaux publicitaires. AdBlock Plus bloque par défaut la plupart des publicités. Il insère un bouton dans la barre d'outils de Firefox qui permet à l'utilisateur d'autoriser l'affichage de certains éléments, ou de tous les éléments, d'une page donnée.



La seconde extension, NoScript, permet de bloquer tous les scripts et plugins des pages Web en permettant, à l'instar d'AdBlock Plus, de les activer au cas par cas, ponctuellement ou pour toujours, pour un site donné. La plupart des sites font aujourd'hui une utilisation intensive des scripts et des plugins. Aussi, de nombreux sites cesseront de fonctionner avec les réglages par défaut de NoScript. Il vous faudra alors les autoriser, ce qui ne prendra pas plus de quelques secondes — et ce quelques secondes sont un mal devenu absolument nécessaire, compte tenu du nombre de menaces reposant sur les scripts et plugins.



#6 – Nettoyer les cookies et le cache de navigation

Les cookies ne sont pas des menaces « actives » : ce ne sont pas des programmes exécutables qui nuiront à votre système. En revanche, certains cookies malicieux (appelés des « cookies traceurs » ou « tracking cookies ») ont pour objet de transmettre certaines des informations permettant de « profiler » l'utilisateur.

La plupart des suites de sécurité (v. *supra*) permettent de détruire les cookies traceurs. Vous pouvez également utiliser des outils gratuits, tels que [CCleaner](#) (Windows, gratuit) ou [Onyx](#) (Mac, gratuit), pour supprimer *tous* les cookies.

Enfin, la plupart des navigateurs modernes proposent une fonction permettant d'effacer les cookies. Dans Firefox, cette fonction est accessible dans le menu **Outils**, puis **Supprimer l'historique récent...**



Nettoyez aussi l'historique de votre navigateur si vous désirez préserver l'intimité de votre vie privée. Ce conseil est souvent donné, mais jamais expliqué. Il ne s'agit pas de se protéger contre des personnes qui viendraient physiquement fouiner sur l'ordinateur pour voir les pages web visitées, mais contre des sites malveillants qui profilent les internautes à l'aide de leur historique de navigation. Les navigateurs permettent en effet aux sites Web d'accéder à l'historique de navigation, afin de déterminer quels liens ont déjà été suivis (ils seront affichés en violet, par défaut) et quels autres ne l'ont pas été (ils seront affichés en bleu par défaut). Un site malveillant contiendra typiquement plusieurs centaines de liens, affichés en blanc sur fond blanc (par exemple) afin de rester invisibles, et un script permettant de déterminer lesquels ont déjà été visités. Il suffit alors à ce site d'associer les adresses des sites visités avec l'adresse IP (ou le compte utilisateur) de l'internaute, afin de le profiler. Le site whattheinternetknowsaboutyou.com met en oeuvre cette technique pour démonstration.

Suppression des menaces

Malgré tous les moyens de protection précédemment exposés, il se peut qu'un logiciel malveillant parvienne à s'installer. Les différentes protection suggérées ici, notamment le filtrage des connexions sortantes (v. *supra*) et des IP (v. *infra*), devraient l'empêcher de transmettre vos informations personnelles sur le réseau. Ce n'est cependant pas une raison pour conserver cette menace. Or, la suppression des logiciels malveillants peut se révéler très difficile. Ces logiciels, en plus de se cacher de l'utilisateur, ont pour habitude de prendre des mesures visant à empêcher leur suppression ou à rendre le système inutilisable en cas de suppression. Afin de contourner ces mesures, les éditeurs de logiciels antivirus fournissent de petits programmes visant à supprimer tel ou tel logiciel nuisible. Ces programmes sont parfois difficiles à manier (exécution en mode sans échec, depuis un LiveCD, depuis la ligne de commande, etc.), mais leur utilisation peut être la seule manière de se débarrasser d'un logiciel nuisible particulièrement coriace.

Si votre antivirus ou anti-malware identifie une menace, procédez ainsi :

- 1) Notez le nom et les références du logiciel nuisible détecté.
- 2) Recherchez des informations sur le Web à propos de ce logiciel (commencez par taper son nom sur Google et poursuivez en lisant ce qui est dit à son propos sur les forums spécialisés). Cette étape est absolument nécessaire. Ne vous contentez jamais de supprimer un fichier sans vous être renseigné à son propos. En effet, les conséquences peuvent être désastreuses : le logiciel espion n'est pas supprimé ; vous avez *supprimé* un fichier infecté qui est nécessaire au système d'exploitation, alors qu'il aurait fallu le *nettoyer* (résultat, votre système est inutilisable), etc.
- 3) Sauf contre indication résultant de l'étape 2), tentez de supprimer le logiciel nuisible à l'aide du logiciel anti-malware qui l'a identifié ; si cela fonctionne, relancez l'analyse de votre ordinateur pour confirmer la suppression, sinon passez à l'étape suivante ;
- 4) Recherchez un utilitaire spécialisé dans la suppression de cette menace, réalisé par un éditeur d'anti-virus et *lisez attentivement son mode d'emploi* ; si cela fonctionne, relancez l'analyse de votre ordinateur pour confirmer la suppression, sinon passez à l'étape suivante ;



5) Suivez les instructions données sur le Web pour supprimer le menace manuellement.

6) Si rien de tout cela n'a fonctionné, sauvegardez vos données, formatez votre disque dur et réinstallez le système.

Lutte contre les menaces (conseils avancés)

1# – Identifier les services et processus en cours

Les logiciels en cours d'exécution sont représentés, dans le gestionnaire de tâches du système d'exploitation, dans leurs processus actifs. Un utilisateur familiarisé par les processus légitimes habituellement actifs sur son système (même s'ils ont des noms « barbares »), saura repérer d'un coup d'oeil tout nouveau processus révélant l'exécution d'un logiciel malveillant.

Sous Windows, faites un clic droit sur la barre de tâches du menu Démarrer et sélectionnez **Démarrer le Gestionnaire des tâches** dans le menu déroulant. Activez ensuite l'onglet **Processus** et cliquez sur le bouton **Afficher les processus de tous les utilisateurs** (afin de voir les logiciels exécutés en tant que *root* – sur l'utilisateur root, v. *supra*).

Certains logiciels vont plus loin, en décomposant les processus et en affichant plus de détails ; ils sont réservés à un public averti. On peut citer [MS Process Explorer](#) et [MS Process Monitor](#) (voir aussi [les autres outils Microsoft](#)), ou le célèbre [Hijackthis](#).

On peut également trouver, sur le Web, des informations relatives aux processus :

- [Liste non-exhaustive des processus Windows légitimes](#)
- [Liste non-exhaustive des processus malicieux sous Windows](#)

Dans la version 2010 de sa suite de sécurité Norton 360, Symantec a implémenté une fonction de validation des processus par la communauté des utilisateurs ([Norton Insight](#)), afin de permettre à ces derniers d'obtenir plus d'informations sur un processus inconnu et d'en vérifier la légitimité.

Sous Mac OS, ouvrez le **Moniteur d'activité** situé dans */Applications/Utilitaires/*.

Plus généralement, avec les systèmes Unix (Mac OS X, Linux, *BSD, etc.), la commande ***sudo crontab -l*** (à taper dans le terminal) permet de révéler l'exécution programmée d'un processus malveillant sous l'autorité du compte root. La réponse *no cronjob for root* (ou équivalente) indique l'absence de tâche planifiée pour l'utilisateur root. C'est la situation normale sous Mac OS X, où [plusieurs chevaux de Troie connus](#) peuvent être repérés par l'ajout d'un cronjob identifié, par la commande précitée par une ligne du type : * * * * *
"/Library/Internet Plug-Ins/plugins.settings">/dev/null 2>&1.

Il est important de noter que :

- cette procédure ne révèle que les exécutable en cours d'exécution, elle est donc inefficace contre les menaces non-exécutables (les cookies traceurs, par exemple) ;
- elle ne permet donc pas de révéler les scripts ou les injections s'exécutant à l'intérieur d'un logiciel légitime (seuls les processus du logiciel légitime apparaîtront) ;
- elle ne permet pas de révéler les processus cachés, notamment par un rootkit.

2# – Filtrer les IP

Le filtrage des adresses IP est un moyen de protection très efficace contre les menaces provenant du Web. Ce procédé permet de bloquer *le site qui contient la menace*. Il intervient donc avant que la menace elle-même doive être analysée par d'autres outils, comme un firewall ou un antivirus. Toutefois, en raison de l'évolution permanente du réseau Internet, le filtrage des IP ne peut pas être exhaustif. En conséquence :

- le filtrage des IP est un des moyens de protection les plus efficaces, lorsque l'IP en cause est effectivement identifiée comme permettant la diffusion d'un logiciel malicieux ;
- le filtrage est totalement inopérant si l'adresse IP n'est pas identifiée (s'il s'agit d'un site *miroir*, par exemple).

Le filtrage des IP doit être mis en oeuvre en plus des autres moyens de protection, à l'aide d'un logiciel spécialisé. On peut citer [Malwarebytes's Anti-Malware](#) (Windows, version payante) ou [PeerGuardian](#) (Windows, Mac, Linux, gratuit), notamment.



3# – Utiliser un VPN

L'installation d'une connexion VPN ne fournit pas une protection contre les logiciels malicieux. J'ai toutefois décidé de parler des connexions VPN dans cet article, car elles constituent un moyen de protéger ses données personnelles et sa vie privée en anonymisant sa connexion. « VPN » est l'abréviation de *Virtual Private Network* ou *Réseau privé virtuel*. Pour comprendre ce que cela signifie, il faut revenir un instant sur le fonctionnement d'Internet.

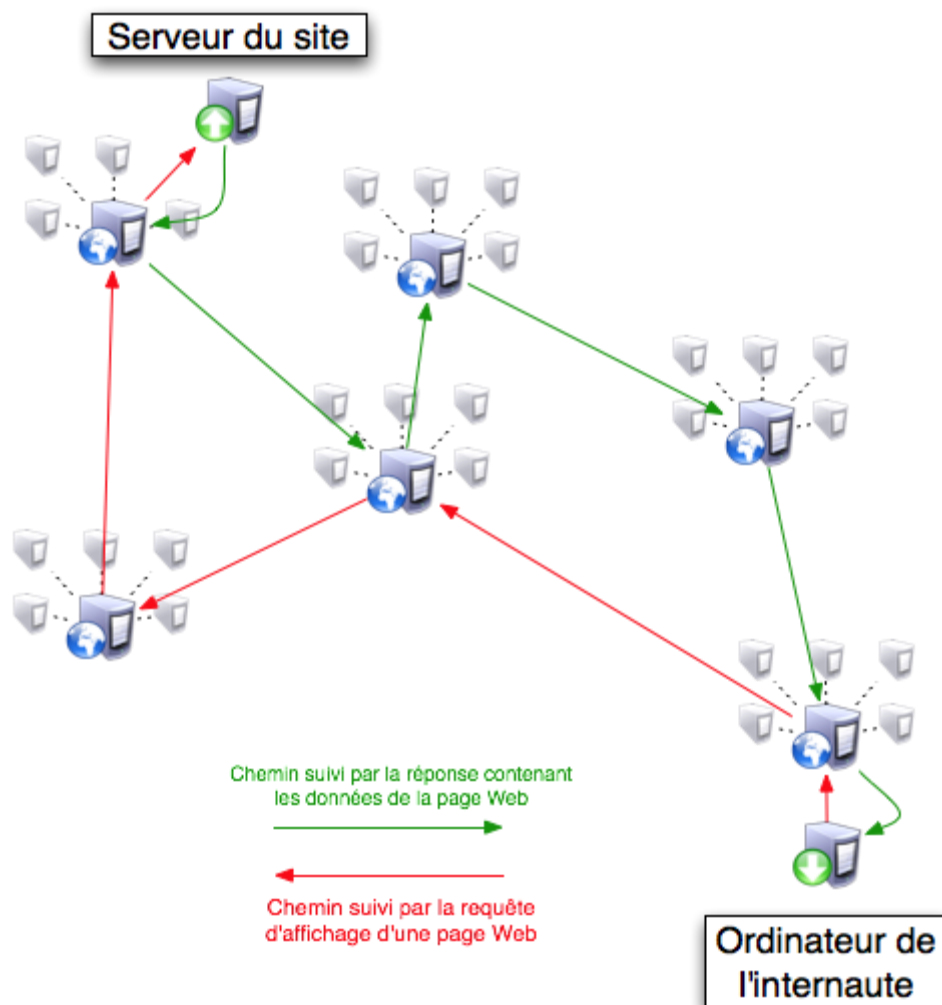
Structure du réseau Internet

Internet est le « réseau des réseaux » (*inter-networks*), c'est-à-dire un réseau global de réseaux locaux. Un réseau local est un réseau d'ordinateurs situés derrière une même passerelle. Un foyer peut avoir, par exemple, un ordinateur fixe, un ordinateur portable et un iPhone, connectés à une « box » (Livebox, Freebox, etc.). La « box » est la passerelle, qui se voit assigner une adresse IP par le fournisseur d'accès (FAI). A son tour, la passerelle assigne une adresse IP à chaque périphérique connecté à elle. L'ensemble des périphériques constitue le réseau local, connecté par la « box » aux ordinateurs du FAI. On appelle cet ensemble un « noeud ». Le réseau du FAI, composé des réseaux locaux de ses abonnés, intègre un réseau plus vaste, par exemple le réseau français. Ce réseau est lui même intégré dans un réseau plus vaste, par exemple le réseau ouest-européen, et ainsi de suite. Ce que l'on appelle « Internet », c'est le plus haut niveau possible : l'ensemble de tous les réseaux de plus bas niveau.

Lorsqu'un internaute charge une page Web, une connexion est ouverte entre son ordinateur et le serveur qui héberge la page demandée. Une première vague de données est envoyée de l'ordinateur de l'internaute vers le serveur : il s'agit de la requête de données. Le serveur traite la requête et renvoie, dans une deuxième vague, les données requises vers l'ordinateur de l'internaute. Le point important est le chemin suivi par les données : celles-ci « sautent » d'un noeud à un autre, se frayant un passage d'un serveur à l'autre, jusqu'à leur destination. En d'autres termes, les données ne passent pas directement de A à Z, elles passent de A à B, de B à C, ..., de Y à Z. Le schéma ci-dessous l'illustre (voir aussi,

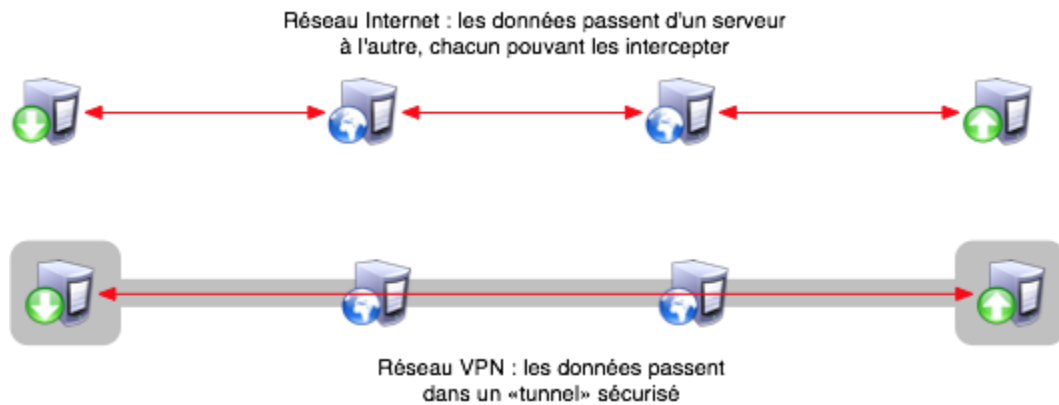
[ce schéma](#), plus réaliste, sur [Wikipédia](#)).





Principe des proxy VPN

Ces quelques rappels techniques étant effectués, voici l'énoncé du problème : les données circulent *en clair* d'un noeud à l'autre, et chaque noeud est susceptible de les intercepter ou d'enregistrer les méta-données de la connexion (date et heure, émetteur et destinataire, etc.). La création d'un réseau VPN a pour but de résoudre ce problème. Une connexion VPN crée un « tunnel » entre l'ordinateur client et le serveur VPN. Tant qu'elles sont dans le tunnel, les données sont chiffrées et ne peuvent pas être interceptées. Le schéma ci-dessous illustre les deux configurations, avec et sans VPN.



L'établissement d'un tunnel VPN a une autre conséquence, lorsque le serveur VPN est un serveur mandataire (*proxy*). En effet, le passage par un proxy permet de cacher au serveur sollicité, et à tous les serveurs intermédiaires, l'identité (l'adresse IP) de l'ordinateur qui a émis la requête. Le mandataire se charge de récupérer les données auprès du serveur, puis de les transmettre au client par un tunnel sécurisé. Ainsi, le serveur et chaque noeud intermédiaire n'ont pour seul interlocuteur que le proxy. Ils considéreront que le proxy est le destinataire final des données envoyées et c'est son adresse IP qui apparaîtra dans les journaux (« logs »). C'est aussi son adresse IP qui sera filtrée, le cas échéant.



Le précédent schéma illustre la double protection du réseau VPN :

- la requête chiffrée est envoyée du client vers le proxy par un tunnel VPN, aucun noeud intermédiaire ne peut l'intercepter ;
- le proxy reformule la requête et l'envoie, en clair, au serveur ;
- le serveur croit que le proxy est le destinataire final des données, il lui renvoie en clair les données correspondant à sa requête ;
- le proxy transmet les données reçues vers le client, en passant à nouveau par le tunnel sécurisé.

Quelques aspects juridiques

L'utilisation d'une connexion VPN et d'un proxy est bien entendu parfaitement licite (en France). Si l'on assimile parfois ces technologies à des moyens illicites,

c'est parce qu'elles rendent caduques plusieurs techniques employées par les opérateurs et la justice afin de faire respecter le droit sur Internet.

Comme nous l'avons vu, les connexions proxy/VPN permettent, en premier lieu, de faire croire au serveur que le destinataire final des données est le serveur proxy. Imaginons l'hypothèse suivante : un contenu illicite dans le pays A est diffusé sur Internet depuis un serveur situé dans le pays B. Une décision de justice, rendue dans le pays A, ordonne au propriétaire du serveur dans le pays B de refuser toutes les connexions originaires du pays A. Cette décision reçoit l'exequatur dans le pays B, et le propriétaire du serveur s'y conforme en mettant en place un filtrage des adresses IP. Un internaute du pays A tente de se connecter au serveur du pays B, et se heurte à un refus du serveur. Il se connecte alors à un serveur proxy, situé dans le pays C, et tente de nouveau de se connecter au serveur B. Pour le serveur B, les données sont requises par un ordinateur du pays C, qui en est également le destinataire final. La mesure de filtrage n'est donc pas mise en oeuvre et les données sont transmises. Le filtrage ordonné à l'opérateur du pays B n'ayant pas été ordonné aux opérateurs du pays C, les données sont envoyées du proxy vers le client. La mesure de filtrage a été contournée.

En second lieu, le mécanisme précédemment décrit permet d'anonymiser les connexions. Le serveur, et tous les noeuds entre lui et le proxy, ignorant l'identité (et même l'existence) du client, il ne peuvent qu'enregistrer l'adresse IP du proxy. Si l'on veut « remonter à la source » pour identifier, par exemple, l'internaute ayant mis en ligne un contenu illicite, on aboutira au serveur proxy. Si celui-ci ne garde aucune trace des connexions émises par les clients, il sera impossible de remonter plus loin et d'aboutir au client.

Remarques complémentaires

Il découle des explications précédentes que la sécurisation du serveur proxy fournissant la connexion VPN est une condition *sine qua non* de la sécurité et de la confidentialité des données transmises.

Un serveur proxy qui n'est pas fiable constitue ainsi un risque de sécurité : il peut enregistrer toutes les connexions qui passent par lui, ainsi que leur contenu. Dans ce contexte, il est plus sûr de ne pas utiliser de proxy VPN plutôt que d'utiliser un proxy VPN fourni par un opérateur à l'intégrité douteuse.



Les opérateurs suivant n'ont, jusque'à présent, donné aucun raison de douter de leur intégrité : [Relakks](#) et [IPREDator](#) (Suède), [PureVPN](#) (plusieurs pays).

L'établissement d'une connexion VPN engendre un autre risque pour la sécurité : la connexion étant directe entre le proxy et le client, les firewalls matériels ne peuvent plus accomplir leur entière mission de protection.

4# – TOR

TOR ou « The Onion Router » est un réseau permettant, à l'instar des serveurs VPN, de chiffrer les données transmises sur le réseau, tout en garantissant l'anonymat du client au regard du serveur.

Principe

Contrairement aux réseaux VPN, TOR ne repose pas sur un serveur proxy central. Ce sont en effet toutes les connexions, entre chaque noeud (constituant les différentes couches de « l'oignon » TOR), qui sont chiffrées. Sur la route (v. les schémas, *supra*) entre le client et le serveur, chaque noeud TOR connaît *uniquement* son prédécesseur et son successeur. Ainsi, le premier noeud connaît votre adresse IP, mais le second noeud ne connaît que l'adresse IP du premier noeud, et ainsi de suite. De même, chaque noeud possède une clé privée, pour le chiffrement des données, qui lui est propre.

Mise en oeuvre

La mise en oeuvre de TOR nécessite l'installation locale d'un serveur proxy, tel que [Privoxy](#), et du logiciel TOR sur l'ordinateur client. L'activation de TOR peut se faire très simplement, en utilisant par exemple l'extension [TorButton](#) pour Firefox.



Critique

L'utilisation de TOR ne fournit pas une sécurité absolue. On peut en effet imaginer plusieurs scénarios dans lesquels l'anonymat de la connexion ou les données transmises sont compromis.

Le premier scénario est celui d'une attaque globale contre TOR ; l'anonymat du client est alors compromis. En effet, une personne ayant (hypothétiquement) une vision globale du réseau peut suivre les données de la source jusqu'à la destination. Il est également possible d'intercepter les données en cours de transit, en les « entourant » d'autres données : ces autres données formeront une sorte de « moule » qu'il suffira de suivre pour connaître le chemin des données passant par TOR.

Le second scénario est celui d'une attaque du contenu par [compromission du dernier noeud](#). En effet, si la requête du client est chiffré pendant qu'elle transite sur le réseau TOR, elle doit être déchiffrée avant d'atteindre le serveur, faute de quoi celui-ci ne pourra pas l'exploiter. C'est le dernier noeud TOR qui la déchiffre, avant de l'envoyer au serveur. Ce noeud a donc une connaissance du message *en clair* et il suffit d'en prendre le contrôle pour compromettre la sécurité des données. Par conséquent, il ne faut jamais transmettre par TOR des informations confidentielles qui ne sont pas directement chiffrées par le client et déchiffrées par le serveur.

5# – SSL/https

Les connexions SSL sont chiffrées par le client et déchiffrées par le serveur, ou vice-versa. Les données transmises peuvent être interceptées durant leur transfert, mais elles ne seront exploitables qu'après déchiffrement (ce qui est, en pratique, quasiment impossible). Les données sensibles (informations personnelles, mots de passe, numéros de carte de crédit, etc.) doivent toujours être transmises à l'aide d'une connexion SSL.

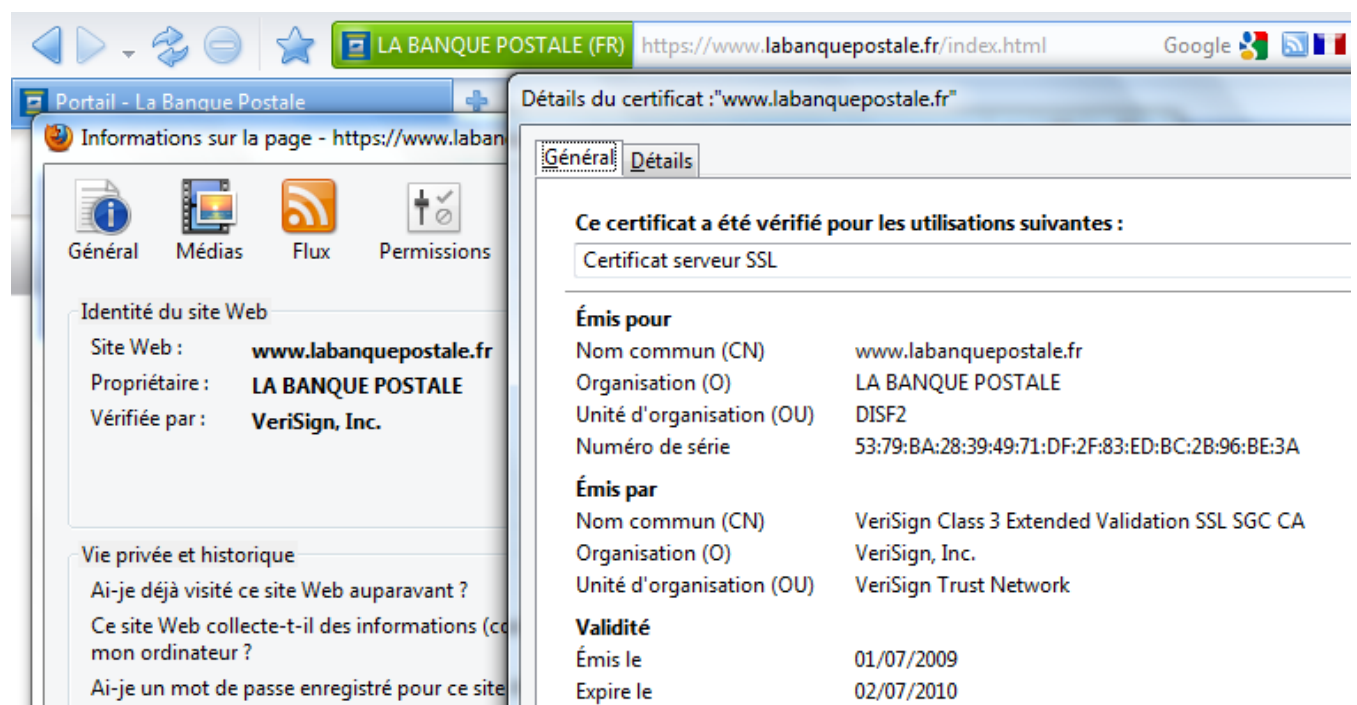
L'existence d'une connexion SSL peut être vérifiée directement dans le navigateur : l'adresse de la page ne débute pas par « http:// » mais par « https:// ». La connexion SSL garantit que les données ne seront pas exploitables si elles venaient à être interceptées par un des noeuds du réseau. Les navigateurs modernes possèdent d'autres indicateurs permettant de déterminer l'existence



d'une connexion SSL : par exemple, une icône de cadenas dans la barre des tâches ou une référence à l'identité du serveur dans la barre d'URL.

Toutefois, cela n'est pas suffisant pour assurer la sécurité des données. Il faut, en outre, vérifier la validité du *certificat numérique* qui permet de mettre en oeuvre la connexion SSL, ainsi que l'identité de l'organisme qui l'a émis et la date de son expiration. Un certificat auto-signé n'a ainsi aucune valeur : les données ne seront pas interceptées, certes, mais leur destinataire peut aussi bien être un imposteur.

Avec Firefox, le nom du serveur est affiché à gauche de l'adresse URL du site, sur fond vert. En cliquant sur ce fond vert, on peut ouvrir une fenêtre montrant les détails du certificat numérique, comme l'illustre l'image ci-dessous.



6# – Utiliser un OS fiable

L'utilisation d'un système d'exploitation (OS) fiable comprend à la fois le bon paramétrage du système d'exploitation, et l'utilisation d'un système sécurisé adapté à ses besoins.

Pour un usage domestique (c'est-à-dire, sans logiciel serveur actif), Windows est le pire système d'exploitation à utiliser. Ce n'est pas que Windows est

intrinsèquement moins sécurisé que Mac OS X ou Linux, mais c'est qu'il est le premier système ciblé par les auteurs de logiciels malveillants, en raison de son énorme part de marché. Il existe des centaines de milliers de logiciels malveillants visant Windows, alors qu'il n'en existe qu'une (petite) dizaine visant Mac ou Linux. Il est donc préférable d'utiliser Mac ou Linux à la maison.

- Si vous voulez installer des jeux ou des logiciels spécialisés, qui ne sont pas diffusés auprès du public, et qui ne fonctionnent qu'avec Windows, utilisez Windows.
- Dans le cas contraire, préférez Mac OS X (vraiment ! on peut tout faire sur Mac, plus facilement encore que vous Windows, sauf jouer...).
- Si vous ne voulez que des logiciels libres et gratuits (mais moins agréables à utiliser), et que vous ne voulez pas jouer, utilisez Linux.

Il est également possible d'utiliser Mac ou Linux comme système principal, et de *virtualiser* Windows pour utiliser certains logiciels spécifiques (v. *infra*). La solution fonctionne très bien pour tous les logiciels qui ne sont pas trop gourmands en ressources. Cela n'exclut, *a priori*, que les jeux et les très gros logiciels serveur, scientifiques (nécessitant une grande puissance de calcul), ou artistiques (Photoshop sur de grosses images RAW, montage vidéo, etc.).

Pour un usage en tant que serveur, la problématique est différente. Un système Linux n'est pas plus sûr qu'un système Windows, au contraire, mais pour des raisons indépendantes des différents logiciels malicieux qui peuvent l'infecter. L'avantage de Windows et de Mac OS X, dans leurs versions serveur, est d'être fournis avec des outils qui facilitent la sécurisation et l'administration du système. A l'inverse, ce sera à l'administrateur du système de sécuriser son système Linux, ce qui nécessite de très grandes compétences en matières de réseaux, de sécurité informatique, et de systèmes Unix. Bref, c'est l'affaire d'un spécialiste.

7# – Placer les fichiers importants sur support amovible

Pour ne pas perdre ses données, il faut les sauvegarder. Une sauvegarde sur le disque dur de l'ordinateur permet de récupérer les fichiers corrompus (à cause d'un bug dans un logiciel, par exemple) ou effacés par erreur, mais elle ne suffit pas en cas d'infection virale. Il est donc conseillé de réaliser des sauvegardes sur des supports externes à l'ordinateur (gravure sur CD ou DVD, stockage sur un disque dur externe ou une clé USB).

Mais on peut aller plus loin, en stockant directement ses données sur un support externe à l'ordinateur -tout en réalisant des sauvegardes sur un autre support externe- , qui n'est connecté qu'en cas de besoin. Bien entendu, il faudra s'assurer que le système est sain avant toute connexion du support externe.

8# – Opérations critiques: utiliser un OS “Live USB”

Pour les opérations critiques en matière de sécurité, la meilleure façon de s'assurer que son système est sain est d'utiliser un système « live ». Les systèmes « live » sont des systèmes pré-installés sur un support amovible, comme un CD/DVD ou une clé USB.

Ce procédé présente plusieurs avantages :

1) Il permet d'utiliser ponctuellement un système d'exploitation autre que celui installé sur la machine hôte, tout en conservant ce-dernier installé sur le disque dur pour une utilisation quotidienne.

Les ordinateurs des cyber-café étant pour la plupart sur-infectés, lancer un système live sain sur un ordinateur de cyber-café permet de travailler en confiance.

2) Il permet d'utiliser un système d'exploitation totalement fonctionnel et doté des logiciels utiles, sans installer quoi que ce soit sur l'ordinateur. Il est ainsi possible de préinstaller sur le système live des logiciels spécialisés, développés pour des besoins spécifiques et que l'on ne trouve pas dans le commerce, afin de les utiliser sans installation sur n'importe quel ordinateur. De la même manière, l'utilisation d'un système live permet de retrouver tous ses logiciels avec leur configuration, sur n'importe quel ordinateur (dans un cyber-café, par exemple).

3) Enfin et surtout, le système live sur une clé USB peut être configuré, au moment de sa création, pour ne stocker aucune donnée créée lors de son utilisation. Sur un CD ou DVD, ce n'est pas une option : aucune donnée ne peut être enregistrée une fois que le support est gravé. En cas de perte ou de vol du support, la sécurité des données n'est donc pas compromise.

Mieux que cela, l'impossibilité d'enregistrer des données neutralise de fait la plupart des logiciels malicieux. Les virus et les vers, qui ont pour but de se répliquer, les keylogger, qui récupèrent des données et les envoient à leur



auteur, ou les chevaux de Troie, qui se cachent dans le système avant d'agir, etc., n'ont de sens que s'ils établissent une présence durable dans le système. Ils sont donc *a priori* conçus pour s'installer sur le disque dur et s'exécuter à chaque démarrage de la machine. S'ils ne peuvent pas s'installer sur le disque dur, comme c'est le cas avec un système live, ils n'ont plus de raison d'être. En somme, seuls les logiciels visant spécifiquement les systèmes live, ou résidant dans la mémoire RAM, constituent encore des dangers.

9# – Chiffrer les données sensibles

Le chiffrement des données permet de les rendre illisibles pour toutes personnes qui ignore l'algorithme et ne détient pas la clé de chiffrement. L'avantage que cela procure est évident : si les données venaient à être détournées par un logiciel malicieux, elles seraient inexploitable. C'est pour cette raison que les sites Web qui nécessitent une grande sécurité des échanges (banques, commerce électronique, etc.) utilisent le chiffrement SSL (v. *supra*).

Inconvénients

Parmi les principaux inconvénients du chiffrement, on peut citer les suivants :

- impossibilité d'accéder aux données en cas de perte de la clé ou de l'algorithme (par exemple, si le logiciel utilisé pour chiffrer les données n'est plus édité et qu'aucun autre logiciel n'utilise le même chiffre...) ;
- ralentissement de l'accès aux données et sollicitation du processeur (au lieu de « lire » ou « écrire » simplement le fichier, l'ordinateur doit le chiffrer ou le déchiffrer : c'est une opération supplémentaire, qui prend du temps et utilise des ressources) ;
- altération des données plus facile et perte potentielle de l'ensemble des données en cas d'altération.

Sécurité

Aucun chiffre n'est vraiment « incassable ». Plusieurs angles d'attaque sont possibles. On peut d'abord envisager une attaque dite par la « force brute » (en

anglais, *brute force*), qui consiste à programmer un ordinateur pour tester toutes les possibilités de clé jusqu'à obtenir la bonne. La sécurité de la plupart des chiffres modernes repose sur le fait qu'une telle attaque n'est possible qu'avec une puissance de calcul phénoménale (que seuls les États pourraient obtenir). Le code [Rivert-Shamir-Adleman](#) (RSA), réputé inviolable, repose par exemple sur le fait que le temps nécessaire pour le « casser » croît exponentiellement avec la longueur de la clé.

Il faut alors envisager une autre manière de procéder, par exemple une méthode heuristique reposant sur l'analyse du contexte, comme le temps nécessaire pour chiffrer un message d'une certaine longueur. Enfin, certaines attaques peuvent exploiter une faille logicielle ou matérielle dans le processus de chiffrement ou de déchiffrement. Par exemple, le RSA a pu être compromis par [l'exploitation du système d'anticipation](#) des processeurs modernes (qui consiste à exécuter une instruction avant la fin de l'exécution de l'instruction précédente). Une telle faille nécessite cependant un accès au processeur, ce qui suppose un accès physique à la machine ou ... la présence d'un logiciel espion.

Plus fondamentalement, la manière la plus simple et efficace d'accéder à des données chiffrées n'est pas de les décrypter (c'est-à-dire de les déchiffrer sans posséder la clé), mais d'obtenir la clé de chiffrement. Un keylogger présent sur la machine au moment du chiffrement pourra intercepter le mot de passe entré par l'utilisateur, et reconstituer ainsi la clé. Les données chiffrées avant infection resteront sûres, mais ce ne sera pas le cas des données chiffrées ou déchiffrées après infection. Le chiffrement est donc un excellent moyen de protection *ex ante*, mais il cesse de l'être une fois le système infecté.

Mise en oeuvre

La plupart des systèmes d'exploitation modernes permettent à l'utilisateur de chiffrer automatiquement le contenu du dossier destiné à ses fichiers personnels : [BitLocker](#) sous Windows ou [FileVault](#) sous Mac OS X, sont par exemple intégrés au système. Ces solutions sont faciles à mettre en oeuvre, mais elles chiffrent tous les fichiers sans distinction. On court ainsi le risque de devoir chiffrer d'énormes fichiers multimédia afin de protéger quelques fichiers de texte. L'impact sur les performances de la machine ne justifie pas cela et rend préférable, dans la plupart des situations, l'utilisation d'un logiciel permettant de choisir individuellement les fichiers à chiffrer.



Aspects juridiques

Les chiffres et les logiciels permettant de chiffrer les données ont pendant longtemps été considérés, par le droit français, comme des armes de guerre. Leur utilisation était donc interdite. Ce n'est plus le cas depuis la Loi pour la Confiance dans l'Économie Numérique (LCEN) du 21 juin 2004. Toutefois, certaines restrictions continuent de s'appliquer à [l'importation et à l'exportation](#) de moyens de chiffrement.

Il faut également faire attention aux situations internationales (déplacement d'un ordinateur portable ou envoi d'un fichier chiffré par Internet, par exemple), car un moyen de chiffrement autorisé en France peut être interdit à l'étranger.

10# – Utiliser un clavier virtuel

L'utilisation d'un clavier virtuel est un moyen efficace de protection contre les keyloggers. Il s'agit d'écrire un mot de passe en cliquant sur un clavier qui s'affiche à l'écran, plutôt que d'utiliser un clavier physique dont la sécurité est potentiellement compromise.

Certaines suites de sécurité, comme [Kaspersky 2010](#) sont fournies avec un clavier virtuel. On peut également trouver des claviers virtuels sur certains sites sécurisés, par exemple celui de [La Banque Postale](#) (paradoxalement, il faudra autoriser les scripts et les plugins dans son navigateur pour l'activer...). Ce clavier virtuel est particulièrement bien conçu, puisqu'il suffit de survoler les touches avec le curseur de la souris, sans cliquer, ce qui rend inopérants les logiciels espions qui intercepteraient les clics de souris. En outre, les touches changent de place d'une visite à l'autre, ce qui rend inutile l'enregistrement de la position du curseur par un logiciel malveillant.

11# – Vérifier l'état physique du matériel

L'état physique d'un périphérique peut révéler un problème de sécurité. Par exemple, un disque dur qui « gratte » révèle la lecture ou l'écriture de données.



Si l'utilisateur n'est pas en train d'utiliser ce disque, et qu'aucun logiciel n'est censé le solliciter (pour une sauvegarde automatique, par exemple), il peut s'agir de l'activité d'un logiciel espion.

De la même manière, il peut être utile de surveiller l'état des diodes présentes sur les différents périphériques. L'information n'est pas forcément pertinente : un rootkit peut, par exemple, activer une webcam tout en neutralisant la diode indiquant l'activité ; mais elle peut tout de même être utile : par exemple, les diodes de la « box » Internet s'affolent, alors qu'aucun chargement n'est censé être en cours.

12# – Changer ses DNS au niveau du navigateur

Les [serveur DNS](#) gèrent le chemin suivi par les données sur le réseau. Une attaque très courante consiste à modifier les serveurs DNS utilisés par une machine, afin de faire croire à l'utilisateur qu'il se rend sur un site tout en l'envoyant sur un autre site. La sécurisation des serveurs DNS utilisés est donc primordiale.

Les serveurs DNS utilisés peuvent être spécifiés à plusieurs niveaux : sur le routeur, sur le système d'exploitation, ou sur le navigateur. De nombreux logiciels malveillants sous Windows modifient la configuration du système afin d'utiliser des serveurs DNS compromis plutôt que ceux indiqués au niveau du routeur par le fournisseur d'accès.

Pour se protéger contre ce genre d'attaque, il faut :

- protéger la configuration des serveurs DNS au niveau du système (la plupart des suites de sécurité pour Windows empêchent la modification des DNS par un logiciel tiers en protégeant [le fichier hosts](#) qui se trouve dans `c:\windows\system32\drivers\etc\`) ;
- pour les plus paranoïaques : vérifier « manuellement » que le fichier `hosts` n'a pas été modifié (dans le répertoire `c:\windows\system32\drivers\etc\` sous Windows, dans le répertoire `/etc/` sous Mac et Linux) ;
- spécifier les adresses DNS au niveau du navigateur. Cela n'est possible qu'avec certains navigateurs, tels que Firefox (une raison de plus pour ne plus utiliser Internet Explorer).

13# – Sandboxing et Virtualisation

Le « sandboxing » et la « virtualisation » ont pour but d'exécuter un logiciel potentiellement dangereux dans un lieu placé « en quarantaine » et isolé du système. De cette manière, si la menace se concrétise, elle ne pourra pas causer de dommage au système et n'aura d'effet qu'à l'intérieur de la zone en quarantaine. Certaines suites de sécurité moderne, comme [Kaspersky 2010](#) permettent le sandboxing ponctuel d'un fichier exécutable.

Dans la terminologie des systèmes Unix (Linux, Mac OS X, BSD, etc.), on parle de « [chroot](#) ». « Chrooter » un logiciel revient à le faire s'exécuter dans une « prison » virtuelle, de laquelle il ne pourra pas sortir.

Il est également possible de créer un système à l'intérieur du système : Windows XP à l'intérieur de Mac OS X, par exemple. Il s'agit de la « virtualisation », que l'on peut mettre en oeuvre grâce à un logiciel spécifique comme [VirtualBox](#) (gratuit), [VMWare](#) ou [Parallels](#). L'auteur du blog [Peghorse](#), qui teste les antivirus du marché, détruit régulièrement dans ses tests des systèmes Windows virtualisés, sans pour autant compromettre la sécurité de son ordinateur.

L'utilisation d'un système virtualisé est donc un moyen efficace de protection. Deux remarques (importantes) doivent toutefois être faites.

En premier lieu, la sécurité du système virtualisé n'est pas garantie dès lors que celle du système hôte ne l'est pas. Par exemple, rien ne sert de virtualiser Linux dans un Windows infecté par un keylogger : ce que l'on écrira dans Linux passera d'abord par Windows et sera intercepté par le keylogger.

En second lieu, la virtualisation d'un système peut être source d'insécurité, dès lors que la machine virtuelle offre un moyen de communication entre les deux systèmes. Par exemple, Parallels pour Mac intègre le système Windows virtualisé au système Mac hôte, afin de le rendre plus facile et plus agréable à utiliser : les dossiers de l'utilisateur peuvent se confondre sur les deux systèmes. Il ne s'agit pas d'une copie mais d'une réplique virtuelle : les fichiers sont dans le dossier « Documents » sur Mac, mais ils apparaissent dans Windows comme s'ils étaient dans « Mes Documents ». De cette manière, si un fichier est supprimé par Windows dans « Mes documents », il sera également supprimé dans « Documents » sur le système Mac. Imaginons un cheval de Troie « vilain.exe » ayant pour but de récupérer des données personnelles et de les envoyer à un tiers. Ce logiciel ne fonctionnera pas sur le système hôte, car il est conçu pour Windows, et qu'il n'est donc pas exécutable sur Mac. En revanche, il peut

parfaitement fonctionner sur le système Windows virtualisé et, en agissant sur le dossier « Mes documents », agir de fait sur le contenu du dossier « Documents » sur le Mac. Il est par conséquent impératif, pour obtenir un niveau maximal de sécurité, d'isoler complètement la machine virtuelle du système hôte (ce que les logiciels de virtualisation précités permettent de faire).

Conclusion

L'exposé des techniques de sécurisation d'un ordinateur personnel présenté n'est ni exhaustif ni imparable. De nouvelles menaces apparaissent tous les jours, si bien qu'il est impossible de garantir la sécurité absolue d'un ordinateur sur le long terme. Toutefois, le dénominateur commun à la plupart de ces menaces réside dans l'exploitation du manque d'information ou de vigilance de l'utilisateur. La meilleure mesure de sécurité reste donc le respect des règles fondamentales « si je ne sais pas, je ne clique pas », « si je ne connais pas, je ne fais pas confiance », « rien ne remplace ma vigilance ».

