Guide
Cybercriminalité

(Edition Mai 2025 – Version 2025.05)

<u>Première règle élémentaire de sécurité :</u>
On réfléchit puis on clique et pas l'inverse.
Les fichiers/programmes c'est comme les bonbons,
quand ça vient d'un inconnu, on n'accepte pas !

CORSAIRE
5 rue de Montplaisir – 28320 BAILLEAU-ARMENONVILLE
www.corsaire-services.com - contact@corsaire-services.com
Téléphone : 06 60 35 18 88

Assistance informatique et internet destinée aux particuliers à domicile
Déclarée services à la personne SAP802642900 du 08/08/2014 – Membre de CORSAIRE Group.
SAS Unipersonnelle au capital de 150€ – RCS Chartres 802 642 900 – SIRET 802 642 900 00012 – APE 6202B

Guide
Virus

Présentation

Ce guide est destiné à vous aider à comprendre et à mieux se protéger des virus informatiques et sur les différents risques de sécurité.

Pas d'inquiétude, ce guide sur les virus n'est pas une revue technique, nous utiliserons des mots simples et nous ne rentrerons pas dans des détails techniques. Pour chaque rubrique, en rentrant dans le détail, il serait possible d'écrire plusieurs milliers de pages ! Ma première version de ce document comportait plus de 50 pages et je n'avais évoqué que 10% du sujet.

L'auteur

Identité : Stéphane-Ludovic NICON
Niveau d'étude : Ingénieur (secteur informatique)
Années d'expérience : Technicien = + de 10 ans, puis Ingénieur = + de 18 ans
Activités : Dirigeant de société, formateur, ingénieur systèmes et réseaux
Membre du conseil d'administration dans différentes structures

Site personnel : www.nicon-stephane.com

Mentions Légales

Editeur : CORSAIRE Services SAS | Responsable de la publication : Stéphane-Ludovic NICON

Crédit photos : Internet, sauf indication contraire.
Sources : Divers, sauf indication contraire.
Rédaction, adaptation et traduction : Stéphane-Ludovic NICON
Imprimé par nos soins, ne pas jeter sur la voie publique.

1. Présentation

Selon Symantec, le nombre de virus, vers et logiciels espions, sur des réseaux informatiques dans le monde était de 1 122 311 à la fin de l'année 2007. En 2016, ce nombre monte à 8 258 600 !

De ce nombre, les deux tiers ont été créés en 2007, rapporte l'éditeur de logiciels de sécurité et de protection des données Symantec dans son dernier rapport semestriel sur la sécurité d'Internet.

Selon ce rapport, les pirates abandonnent les attaques massives et ciblent plutôt les utilisateurs d'ordinateurs individuels via le Web pour infiltrer les réseaux. Symantec croit que cette tendance vient probablement du fait que les attaques sur les réseaux d'entreprises ont plus de chance d'être déjouées. Il est plus difficile de détecter une activité malveillante sur les ordinateurs des utilisateurs et sur des sites Web.

Le cheval de Troie, qui permet de prendre le contrôle d'une machine connectée au réseau, représente 71% des cinquante codes infectieux les plus utilisés au cours du second semestre 2007. Les pirates comptent sur la confiance que l'utilisateur a envers certains sites, comme les réseaux sociaux, afin qu'il laisse agir sur son ordinateur et qu'il ouvre sans méfiance les documents ou applications qu'il télécharge. La modification cachée de navigateurs et de pages Internet (phishing), notamment sur des sites financiers serait également un phénomène en croissance.

Par ailleurs, le pourriel serait en hausse. Il représentait 71% des courriels échangés dans le monde au cours du second semestre 2007, contre 61% pour la même période un an plus tôt.

Top 10 des virus informatiques 2017 (source : Kaspersky France) :

- 1 - Le cheval de Troie : sous couvert d'un programme d’apparence inoffensive, il véhicule une charge malveillante.
- 2 - Le téléchargement "drive-by" : il s’agit d’une méthode courante de propagation de malware. Les cybercriminels recherchent des sites web non sécurisés afin d’implanter un script malveillant dans le code de leurs pages.
- 3 - Le détournement de clic : cette méthode consiste à inciter un utilisateur à cliquer sur un objet sur une page web tout en lui faisant croire qu’il clique sur un autre.
- 4 - Les bots Tinder : ces programmes automatiques se font passer pour de véritables utilisateurs sur les sites de rencontre.
- 5 - Le chat-phishing : des cybercriminels fréquentent des sites de rencontre ou des forums, y encourageant les utilisateurs à cliquer sur des liens vers des forums de live sex et autres sites pornographiques.
- 6 - Le ransomware : les cybercriminels utilisent des "bloqueurs" pour interdire à la victime l’accès à sa propre machine, invoquant souvent la présence de « contenu pornographique illicite » en misant sur le fait que quiconque ayant consulté des sites pour adultes est moins enclin à se plaindre aux autorités.
- 7 - Le vers : ce type de programme se reproduit sans écrire son code dans d’autres fichiers. Au lieu de cela, il s’installe une fois sur la machine d’une victime puis recherche un moyen de se propager à d’autres.
- 8 - Le pornware : il peut s’agir d’un programme authentique mais aussi d’un adware installé par un autre programme malveillant et conçu pour afficher du contenu inapproprié sur la machine de la victime.
- 9 - Le spyware : logiciel d’espionnage qui permet à un pirate d’obtenir subrepticement des informations sur les activités en ligne de la victime et de les exfiltrer de sa machine.
- 10 - Le faux antivirus : de prétendus logiciels antivirus exploitent la crainte des utilisateurs que des malwares aient été installés pendant qu’ils visionnaient des contenus pornographiques.

2. Histoire

(Source : Rédaction Clubic, août 2018)
Les menaces de sécurité et les solutions de protection évoluent sans cesse. Depuis les premiers virus apparus dans les années 70, les vers, chevaux de Troie, botnets ou ransomwares ont transformé ce qui était une simple plaisanterie de "hacker" en une économie parallèle... Et un challenge continu obligeant les éditeurs de logiciels de sécurité à redoubler d'efforts afin de protéger nos machines.

Comment en est-on arrivés là ? Remontons le temps pour retracer cette histoire !

Aux origines... une plaisanterie
1971 : l'arbre généalogique des malwares commence, pour la plupart des historiens, par une petite blague, le ver Creeper. Créé par Bob Thomas, il se limite à afficher un message : " I'm the creeper, catch me if you can ! " (Littéralement : " je suis la plante grimpante, attrapez-moi si vous pouvez "). Précurseur, Creeper utilise déjà ce qu'on appelle encore ARPANET pour se propager. D'autres virus "poétiques" se développent, comme Elk Cloner en 1982. Jusqu'ici, tout va bien. L'idée est avant tout d'annoncer fièrement qu'on peut le faire, sans qu'il n'y ait aucun risque pour l'utilisateur.

« Ça tourne mal »
Les choses prennent un tournant plus inquiétant en 1986 avec un des premiers chevaux de Troie, PC-Writer, qui se fait passer pour un programme légitime et efface tous les fichiers de l'ordinateur infecté... Deux ans plus tard, le ver Morris met à genoux le réseau ARPANET pendant 24 heures.

En 1991, le virus Michelangelo est le premier à bénéficier d'une couverture médiatique. Ce dernier, conçu pour infecter le BIOS des machines (via DOS), se déclenche chaque 6 mars (date anniversaire de l'artiste de la Renaissance) afin de remplacer les premiers secteurs du disque principal par de zéros. Pas très sympa la tortue ninja.

L'empire contre-attaque
Les premiers antivirus, signés Norton ou McAfee apparaissent à la même époque. En fait d'antivirus, on pourrait plutôt les comparer à ce qu'on connaît aujourd'hui avec des outils de nettoyage comme Malwarebytes, qui scannent l'ordinateur à la recherche d'un virus connu, et l'éradiquent. Les définitions sont mises à jour, par disquette, tous les trimestres. On est encore très loin des signatures poussées par le cloud en quasi-temps réel.

« T'AS FAIT UN SCAN ANTIVIRUS ? »

Parmi les précurseurs, on trouve McAfee et son VirusScan, G DATA, Solomon, Alwil (Avast) ou encore Avira. Norton Antivirus voit le jour en 1991, suivi au milieu des années 90 par de nouveaux acteurs d'Europe de l'Est, Kaspersky et BitDefender. A l'époque, "T'as fait un scan antivirus ?" est une phrase régulièrement employée, surtout après, "Vous avez essayé de l'éteindre et de le redémarrer ?".

Années 2000 : Windows sous le feu des menaces
Avance rapide sur la fin des années 90 qui voit Internet se développer auprès du grand public. Windows et Internet Explorer dominent alors le marché de manière écrasante. L'hégémonie de cette évolution inévitable en fait malheureusement la cible d'attaques massives de logiciels malveillants, et va créer une onde de choc.

C'est l'époque, par exemple, de CIH (également appelé Tchernobyl) en 1998. Ce virus avait le bon gout de tout simplement dézinguer le BIOS de l'ordinateur infecté à la date anniversaire de la catastrophe nucléaire du même nom. La seule solution pour récupérer son ordinateur sans changer de carte mère était donc de flasher la puce EEPROM (Electrically Erasable Programmable Read-Only Memory) sur un autre ordinateur ; en faisant un échange de puce à chaud donc. Simple. Basique.

On comprend mieux pourquoi les ingénieurs ont ensuite protégé les BIOS un tout petit peu mieux.

Des vers... et droit dans le mur
Après la mode des macro virus, la première partie de la décennie 2000 voit défiler les vers, qui se propagent d'une machine à l'autre en utilisant des scripts intégrés aux emails ou des vulnérabilités du système d'exploitation et/ou du navigateur web. Loveletter et son fameux mail « I love you », Code Red, Sasser ou Nimda font partie des plus « célèbres ». Code Red utilise la technique du « buffer overflow » (ou dépassement de tampon, c'est un peu moins classe en VF) qui consiste à surcharger le système en écrivant des données à l'extérieur du tampon qui leur est alloué. Une fois installé, le ver lance des attaques de déni de service sur des adresses IP fixes prédéterminées, dont celle de la Maison-Blanche. Sasser utilise des techniques similaires pour cibler, avec succès les serveurs de l'AFP, Delta Airlines, et plusieurs banques, assurances ou services de poste à travers le monde. Un joli bazar qui entraine des annulations et blocages en série.

Patchez, patchez, patchez !
Microsoft prend la mesure de l'ampleur des dégâts en 2001 et en tire une refonte totale de la sécurité de Windows XP, qui aboutira aux Service Pack 1 et 2, et au traditionnel Patch Tuesday.

L'exploitation de vulnérabilités est et reste le vecteur d'infection le plus prisé par les auteurs de logiciels malveillants, face à des utilisateurs qui ne pensent pas à mettre à jour leur système d'exploitation, leur navigateur web ou les nombreux plug-ins qui peuvent être détournés, tels que Flash, Adobe Reader ou Java.

Vélocité ou sécurité
La protection des antivirus évolue parallèlement. Les logiciels de sécurité s'enrichissent d'une protection résidente, permettant de contrer les menaces en direct, à partir d'une base de signature, mais aussi de plus en plus via des mécanismes heuristiques ou d'analyse proactive. Plutôt que d'analyser des menaces déjà connues, l'idée est de repérer et bloquer les comportements suspects. Cette évolution a un coût en ressources, et c'est à cette époque qu'on commence à pester contre la lourdeur de certains logiciels.

« C'EST À CE MOMENT QUE NAIT LE CONCEPT DE SOLUTIONS "INTERNET SECURITY" »

C'est un problème délicat à résoudre : d'un côté, la multiplicité des menaces incite à utiliser des solutions de sécurité de plus en plus complètes. C'est à ce moment que nait le concept de solutions "Internet Security" incluant, en plus de l'antivirus, un pare-feu, des solutions de contrôle parental ou encore des outils spécifiques pour protéger ses mots de passe ou ses données bancaires. De l'autre, les ressources des PC ne sont pas illimitées, et ces solutions peuvent mettre à genoux un ordinateur d'entrée de gamme.

Encore aujourd'hui, les utilisateurs sont divisés : certains préfèrent le confort d'une solution tout-en-un, et les autres, plus technophiles, souhaitent contrôler leur PC dans les moindres détails et composer eux-mêmes leur solution à partir de logiciels ciblés et spécifiques.

Cache-cache
Dans le jeu du chat et de la souris que se livrent développeurs de malwares et éditeurs de logiciels de sécurité, l'art du déguisement est une technique très prisée dans la deuxième moitié des années 2000. On assiste à une montée en puissance de chevaux de Troie, qui cachent un programme malveillant dans un logiciel apparemment sans risque, et de rootkits, des malwares furtifs qui parviennent à passer sous le radar des antivirus.

« LA VERSION MODERNE DES CHARLATANS »

Profitant de la popularité des antivirus gratuits, dont le succès est dû en partie à la mauvaise réputation acquise par certaines suites de sécurité "poids lourd", on commence aussi à voir apparaître de faux antivirus qui se dissimulent sous une interface imitant souvent celle des gratuits, et notamment du Windows Live OneCare de Microsoft.

Peu nocifs en fait, ils servent surtout un but : soutirer de l'argent à l'utilisateur avec un placebo. Le logiciel détecte des virus fictifs sur le disque de l'utilisateur, et bien entendu, la version gratuite ne permet pas de les supprimer. La version moderne des charlatans et leur potion magique.

Cash-cash
Il faut y voir une évolution de la motivation des « hackers » et des éditeurs de logiciels malveillants. Leur but n'est plus la plaisanterie ou le chaos, mais les bénéfices en arnaquant les utilisateurs, ou en prenant contrôle de leur machine pour diffuser du spam. En 2006 et 2009 respectivement, les botnets Zeus et Aurora causent des dégâts profonds, tandis que les menaces se politisent avec des attaques comme Stuxnet. Le ver qui cible des infrastructures nucléaires en Iran en 2010 est suspecté d'être l'œuvre conjointe des États-Unis et d'Israël. La cyber guerre est devenue réalité !

Du côté des éditeurs d'antivirus, face à des menaces de plus en plus variées et de plus en plus nombreuses, on voit apparaître la tendance du cloud à partir de 2009.

Le recours à une infrastructure en ligne permet de libérer des ressources système, et de mettre chaque utilisateur à profit pour détecter de nouveaux logiciels malveillants grâce à un système de réputation en ligne. Une base « participative » qui abat déjà une partie du travail d'identification des fichiers. Les techniques d'analyse heuristique se perfectionnent en parallèle.

On voit notamment apparaître des solutions qui utilisent la virtualisation pour exécuter un fichier suspect dans un "bac à sable" isolé du système de l'utilisateur et décortiquer son comportement.

La tendance actuelle : Ransomwares et iOT
L'écosystème des menaces a considérablement changé plus de 40 ans après le premier virus. L'ère des attaques massives de vers est également révolue, alors que les petites frappes de multiples logiciels malveillants sont devenues la norme. Parmi les tendances des dernières années, on peut toutefois noter la montée en puissance des ransomwares, qui peuvent avoir un énorme impact.

Conçus pour extorquer de l'argent à l'utilisateur, le ransomware chiffre ses données personnelles et promet de les déchiffrer en l'échange d'une rançon. Que l'utilisateur paye ou pas n'a pas forcément d'incidence sur l'issue : la restauration est loin d'être systématique. Certains honorent leur "promesse", d'autres non.

CryptoLocker en 2014, et surtout WannaCry en 2017 se sont montrés particulièrement nocifs. Le dernier a immobilisé de nombreuses entreprises infectées. La seule solution efficace est la protection en amont des données utilisateur, en empêchant au préalable leur modification.

Connectés, oui. Sécurisés, non.
Autre star sinistre de ces dernières années, le botnet Mirai découvert en 2016 ciblait les objets connectés tels que les caméras de sécurité de certains fabricants, profitant de leurs vulnérabilités. La multiplication des objets dans la maison est un vecteur d'infection à ne pas sous-estimer. De plus en plus accessibles, ils proviennent de fournisseurs parfois peu fiables, et exécutent des micrologiciels au niveau de sécurité qui peut être très bas.

Le préjudice, pour l'utilisateur, n'est pas directement perceptible. Le but de Mirai est essentiellement de lancer des attaques de déni de service sur les serveurs de nombreuses entreprises, dont l'incapacité à exercer leur activité peut, elle, avoir des répercussions indirectes sur l'utilisateur. Le botnet a ainsi perturbé l'usage de Netflix, Twitter, GitHub, Airbnb ou Reddit, en utilisant les ressources système de foyers qui peuvent être ses clients. Mais ce client ne fera pas forcément le rapprochement entre les deux.

La parade pour y remédier est la surveillance d'activités anormales sur le réseau, en passant notamment par une solution physique qui peut être intégrée au routeur ou proposé sous la forme d'une « box » dédiée comme la BitDefender Box. Ainsi, même les appareils qui ne peuvent pas embarquer de protection antivirus peuvent être protégés et leur trafic illégitime stoppé.

Et maintenant, on fait quoi ?
En plus de 40 ans, nous sommes donc passés d'un micro phénomène touchant uniquement des passionnés d'informatiques un peu farceurs à une industrie qui peut ralentir l'activité d'entreprises ou de services publics, confisquer les données d'utilisateurs ou détourner l'usage de leurs objets connectés.

Ce serait franchement terrifiant si ce mouvement ne s'était pas heureusement accompagné d'une évolution en parallèle des solutions permettant de prévenir ou de remédier à ces attaques. Pas toujours en accord avec les besoins des utilisateurs, parfois créatrices d'autres problèmes de consommation de ressources système, ces solutions demeurent malgré tout un filet de sécurité nécessaire, notamment pour le grand public qui n'a pas forcément conscience des risques qu'il encourt.

3. Cybercriminalité

Quelles sanctions pour l'intrusion dans les systèmes informatiques ?

En l'absence de définition en droit interne et européen, les Nations unies ont tenté de dessiner les contours de la cybercriminalité en déclarant qu'il s'agit de « toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique ». Dans son rapport de 2011, l'Observatoire national de la délinquance et des réponses pénales (ONDRP) regroupe les infractions en deux catégories :

- Les infractions où l'informatique est le moyen du délit. Sont alors visées toutes les formes d'infractions classiques facilitées par l'informatique : l'escroquerie, la pédopornographie, les atteintes à la vie privée, la propagande terroriste, etc. ;
- Les infractions où l'informatique est l'objet du délit. Il s'agit des atteintes à la sécurité des systèmes et des réseaux ou des données informatiques (piratage, intrusion sur les sites, vols de données, etc.), comme notamment la "cyber attaque" dont a été victime TV5 Monde.

Les sanctions pour les infractions de cette dernière catégorie sont prévues aux articles 323-1 à 323-7 du Code pénal, issus de la loi n°88-19 du 5 janvier 1988 et complétés par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Ainsi, aux termes de 323-1 du Code pénal, « [l]e fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende ». La sanction est portée à 3 ans d'emprisonnement et 45 000 euros d'amende lorsqu'il y a en plus, soit suppression ou modification de données contenues dans le système, soit une altération du fonctionnement de ce système (C. pén., art. 323-1, al. 2).

S'agissant du fait d'entraver ou de fausser le fonctionnement d'un système, la peine encourue est de 5 ans d'emprisonnement et de 75 000 euros d'amende (C. pén., art. 323-2).
Outre ces sanctions, l'article 323-5 du Code pénal prévoit des peines complémentaires telles que la privation des droits civiques, civils et familiaux, l'interdiction d'exercer une fonction publique ou d'exercer l'activité professionnelle dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

Sources : Rép. pén., Fr. Chopin, V° « Cybercriminalité » ; Féral-Schuhl, Cyberdroit 2011/2012, 6e éd., Dalloz, coll. « Praxis », 2010.
http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

Référence : Code pénal

Article 323-1
« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende. »
Article 323-2
« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »
Article 323-5
« Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

4. Virus : généralités et protection

Fléau majeur de l'informatique, les virus sont aussi présents sur internet. Qu'ils s'attaquent au secteur d'amorce de vos disques, aux fichiers exécutables ou aux documents incluant des macros, leur but est toujours le même : proliférer en cachette, se faire subitement remarquer, puis souvent détruire vos données. La meilleure protection reste la prévention : méfiez-vous des disquettes introduites dans des ordinateurs peu sûrs, et des fichiers douteux téléchargeables sur internet ou reçus en pièce jointe d'un courrier.

Les virus sont un fléau majeur de l'informatique, et pas seulement sur internet : un simple échange de disquettes entre copains ou collègues de travail peut contaminer votre disque dur, sans même éveiller vos soupçons. Car la bestiole est souvent rusée.

Il y a de fortes chances que si vous ne vous protégez pas, votre ordinateur sera infecté dans la première journée d'utilisation. Certains spécialistes disent même qu'un PC a une durée de vie de 4 à 20 minutes sur le réseau selon la vitesse de connexion (xDSL, fibre...).

"C'est n'importe quoi ! Je suis connecté depuis des mois et il ne s'est rien passé."
En apparence, il ne s'est rien passé. Quand vous êtes infecté, la plupart du temps, vous ne vous en apercevez pas. Si cela fait un mois que vous avez acheté votre ordinateur et que vous débutez en informatique, il y a 99.99% de chances que votre ordinateur soit infecté.

Qu'est-ce qu'un virus ?
Un virus est un petit programme conçu pour se cacher dans votre ordinateur, puis se multiplier, se répandre de par le monde et enfin déclencher une action (message, destruction, petite musique, etc.). On dénombre plusieurs catégories de virus, en fonction de la cible visée dans l'ordinateur.

Les différentes familles de virus
La première catégorie regroupe les virus de secteur d'amorce (= virus de "boot sector", c'est-à-dire affectant la zone du disque qui est lue en premier au démarrage) tels que Form, jack the ripper, french boot, parity boot... Ces virus remplacent le secteur d'amorce du disque infecté par une copie d'eux-mêmes, puis déplacent le secteur original vers une autre portion du disque. Le virus est ainsi chargé en mémoire bien avant que l'utilisateur ou un logiciel ne prenne le contrôle de l'ordinateur.

Les virus d'applications infectent les fichiers exécutables, c'est-à-dire les programmes (.exe, .com ou .sys). Pour simplifier, disons que le virus remplace l'amorce du fichier, de manière à ce qu'il soit exécuté avant le programme infecté, puis il lui rend la main, camouflant ainsi son exécution aux yeux de l’utilisateur.

Les virus macro sont des virus qui infectent uniquement des documents (Word, Excel...), en utilisant le langage Visual Basic pour Application. Ces virus se propagent actuellement dans de fortes proportions et peuvent malheureusement causer de grands dégâts (formatage du disque dur par exemple).

Enfin, il y a les virus de mail, également appelés vers. Ces virus se servent des programmes de messagerie (notamment Microsoft Outlook) pour se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentent dans le carnet d'adresses. Leur premier effet est de saturer les serveurs de messagerie, mais ils peuvent également avoir des actions destructives pour les ordinateurs contaminés. Ils sont particulièrement redoutables, car le fait de recevoir un mail d'une personne connue diminue la méfiance du destinataire, qui ouvre alors plus facilement le fichier joint contaminé.

A noter que certains virus sont des virus polymorphes. A chaque fois que l'un d'eux infecte un fichier, il se crypte différemment. Résultat, il faut que l'antivirus analyse la technique d'encryptage de chaque virus pour déceler, dans les fichiers contaminés, une sorte de "manie" caractéristique, une constante.

Il ne faut pas confondre les virus avec les troyens ou les emails "bombs". Contrairement à son cousin le virus, qui profite de toute occasion pour se multiplier, le troyen véritable ne se reproduit pas. Par ailleurs, plusieurs vulnérabilités dans les logiciels Internet Explorer, Outlook font que certains virus peuvent infecter votre

ordinateur à la simple ouverture du message ou lors de sa lecture dans la fenêtre de visualisation voire en consultant une page web si Internet Explorer n'a pas été "patché" contre cette vulnérabilité.

Fonctionnement d'un virus
Quel que soit le type de virus, aucun ne contamine - pour l'instant - les fichiers compressés. Cela ne garantit pas qu'un fichier compressé soit exempt de virus : il peut très bien avoir été infecté avant compression, et se révélera donc dangereux une fois décompressé.

Pour bien comprendre le mode de fonctionnement d'un virus, il faut se souvenir de l'analogie avec le virus biologique. Comme lui, le virus informatique essaie de contaminer tout ce qu'il peut, de se dissimuler aux yeux de l'organisme infecté, et de se répandre le plus largement possible. Les virus infectent un maximum de fichiers puisqu'ils demeurent en mémoire dès le démarrage de l'ordinateur. Ils interceptent les commandes du Bios, et agissent ainsi selon leur humeur...

Comment savoir si mon ordinateur est contaminé ?
Tout comme les troyens, les virus sont le plus souvent repérés trop tard, par les conséquences potentiellement désastreuses de leur activité : affichage de messages intempestifs, émission de sons ou de musiques inattendus, mais aussi plantage de l'ordinateur, formatage du disque dur, etc.

Pourtant, de nombreux indices peuvent mettre la puce à l'oreille de l'internaute vigilant : mémoire système disponible inférieure à ce qu'elle devrait être, changement du nom de volume d'un disque, programmes ou fichiers subitement absents, apparition de programmes ou de fichiers inconnus, ou encore comportement anormal de certains programmes ou fichiers.

Que faire en cas de contamination ?
La solution la plus simple, reste de vous procurer un logiciel antivirus. La plupart propose une procédure permettant de désinfecter le contenu du disque avant d'installer le logiciel, mais le mieux est d'installer l'antivirus avant toute contamination afin de bénéficier de l'ensemble de ses fonctionnalités (surveillance des transferts de fichiers ou de l'accès aux fichiers sensibles, inoculation des fichiers pour repérer tout changement de taille suspect, etc.).

Vous pouvez également utiliser un antivirus gratuit en ligne pour procéder immédiatement à l'analyse ainsi qu'à l'éradication de virus éventuellement présents sur vos disques.

Pour les virus macro, il est conseillé de rechercher le fichier normal.dot et de le supprimer, puis ensuite de détruire tous vos documents. Cette méthode supprime les virus macro définitivement, mais aussi malheureusement votre travail.

Déjà vu
Certains virus ne font qu'effacer la partition, ce qui fait que l'utilisateur débutant (ou le technicien incompétent ou malhonnête) n'arrive plus à reformater son disque dur et par conséquent le change, alors qu'il suffit d'exécuter une commande et de recréer une partition. Attention cependant : si vous êtes un complet débutant, faites-vous aider par un ami ou un collègue plus expérimenté, sans quoi vous risqueriez de faire pire que le virus...

5. Les intrusions

Les intrusions consistent à pénétrer sur un ordinateur ou un réseau distant, dans le cas des ordinateurs particuliers, deux manières sont particulièrement utilisées.

Intrusion au moyen d'un troyen
Cette sorte de virus permet l'intrusion et la prise de contrôle de votre ordinateur par celui qui vous l'aura envoyé. Le téléchargement de fichiers d'origine douteuse est le principal moyen de contamination par les programmes de type troyen. Ces derniers permettent à votre agresseur de contrôler à distance votre machine, et lui donne tout pouvoir sur les fichiers de votre disque dur (lecture, suppression, vol, etc.).

Pour plus d'informations, voir la rubrique concernant les troyens

Intrusion au moyen des ressources partagées
Comme son nom l'indique, le partage de fichiers vous permet de partager des fichiers avec d'autres utilisateurs, donc de laisser ceux-ci venir lire, modifier, créer voire supprimer des fichiers sur votre disque dur.

Cette fonctionnalité peut s'avérer très utile lorsque vous êtes en réseau local (quelques machines connues reliées ensemble), mais devient très dangereuse si vous donnez, en le sachant ou non, ces permissions à n'importe qui sur internet.

Comment savoir si mon ordinateur avec Windows est exposé ?
C'est très simple. Il suffit de vous rendre le menu "Réseau" de votre ordinateur : pour cela, cliquez sur le bouton "Démarrer", sélectionnez ensuite "Paramètres" puis "Panneau de configuration", et enfin double-cliquez sur l'icône "Réseau". Dans la fenêtre qui s'ouvre, cliquez sur le bouton "Partage de fichiers et d'imprimantes...".

Si ce bouton apparaît en grisé et n'est pas cliquable, c'est que le partage ne peut pas être activé (à moins d'installer un service client) : votre ordinateur n'est donc pas exposé.
Si ce bouton est bien cliquable, vous devez voir s'ouvrir une seconde fenêtre, avec deux options : "Permettre à d'autres utilisateurs d'accéder à mes fichiers" et "Permettre à d'autres utilisateurs d'utiliser mes imprimantes". Si une case ou les deux sont cochées, c'est que le partage est activé pour la ressource concernée...

Alors, que faire dans le cas d'un poste isolé ? Certains systèmes d'exploitation récents sont censés vous prévenir en cas d'établissement d'une connexion avec partage de fichiers, mais il vaut mieux ne pas jouer avec le feu...

La meilleure chose à faire est de désactiver le partage de fichiers et le partage d'imprimantes si votre machine ne fait pas partie d'un réseau local, c'est-à-dire dans la majorité des cas (ordinateur isolé ou plusieurs machines non connectés entre elles) : pour cela, il suffit de décocher les cases précédemment évoquées, ce qui inactive les deux options de partage (selon les versions et les configurations, le CD-Rom d'installation de Windows vous sera demandé, et la machine devra rebooter).
Et si je suis en réseau local ? Si vous devez absolument conserver le partage de fichiers actif, il faut alors impérativement adopter les précautions suivantes : créez à la racine du disque dur (C:, a priori) un répertoire - et un seul ! - que vous partagerez, et protégez immédiatement son accès par un mot de passe. Ce répertoire devra accueillir tous les fichiers que vous voulez mettre en commun et/ou échanger avec d'autres utilisateurs : à vous ensuite de les déplacer ou d'effectuer tout autre traitement. C'est le prix de la sécurité...

Autres problèmes amenant à des intrusions

Les deux cas particuliers s'appliquent tout particulièrement aux particuliers, bien que les professionnels soient aussi impliqués, mais pour ceux-ci d'autres problèmes se posent. En particulier, la non sensibilisation des utilisateurs induit des fautes à l'origine de failles de sécurité importantes, surtout dans le cas de réseau ou une faille d'un utilisateur provoque une ouverture vers un ensemble de machines. Ces faiblesses peuvent être de plusieurs ordres, d'abord un choix de mot de passe aberrant (la date de naissance de sa femme, ou mieux un mot de passe collé avec un post-it sous le clavier !), en effet il existe des "dictionnaires" de mots de passe les plus courants et des tests avec un logiciel approprié permet de trouver le précieux Sésame, (pour plus d'informations : les mots de passe, conseils).

Aussi, chaque utilisateur devrait être informé des précautions à prendre pour éviter des fautes très connues et utilisées par les pirates. De plus, la mauvaise compétence d'un certain nombre d'administrateur réseau, insuffisamment formé à la sécurité laisse des failles dans les systèmes utilisés, par exemple de nombreux services sont laissés aux utilisateurs de réseaux alors que la nécessité ne s'en fait pas sentir. Les intrusions en utilisant une faille de sécurité d'un service réseau pourtant connus sont à l'origine de nombreux piratage, alors que des mises à jour sont régulièrement données par les éditeurs de logiciels ou des systèmes d'exploitation.

6. Les attaques

Une attaque à distance est une agression contre une machine par une personne n'ayant pas les droits sur elle. Une machine distante est "toute machine autre que la sienne et que l'on peut joindre grâce à un protocole à travers un réseau. De nombreuses méthodes existent, avec différents buts, en voilà quelques-unes des plus répandues.

Le Flood
Le flood consiste à envoyer très rapidement de gros paquets d'information a une personne (à condition d'avoir un PING (temps que met l'information pour faire un aller-retour entre 2 machines) très court). La personne visée ne pourra plus répondre aux requêtes et le modem va donc déconnecter. C'est cette méthode qui a été employé à grande échelle dans l'attaque des grands sites commerciaux (Yahoo, Etrade, Ebay, Amazon...) en février 2000.
Pour l'éviter une solution consiste à ne pas divulguer son adresse IP (ce qui est possible pour un particulier, mais pas pour une entreprise possédant un nom de domaine).

Les sniffers
Un "sniffer" est un dispositif, logiciel ou matériel, qui permet de capturer les informations qui transite sur la machine où il se trouve. Les "sniffers" ne sont pas des dispositifs illégaux, ils servent par exemple à détecter des failles de sécurité ou à régler des conflits. Cependant, leur utilisation se révèle illégale quand la personne concernée n'a pas donné son accord. Ils peuvent ainsi, capturer le texte saisi sur la machine mais aussi toutes informations provenant des machines du réseau passant par la machine en question. L'usage le plus malveillant consiste à intercepter les mots de passe.

Les scanners
Un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les scanners servent pour les hackers à savoir comment ils vont procéder pour attaquer une machine. Leur utilisation n'est heureusement pas seulement malsaine, car les scanners peuvent aussi vous permettre de déterminer quels ports sont ouverts sur votre machine pour prévenir une attaque.

Le Nuke
Les nukes sont des plantages de Windows dû à des utilisateurs peu intelligents (qui connaissent votre adresse IP) qui s'amusent à utiliser un bug de Windows 95 (qui a été réparé avec Windows 98) qui fait que si quelqu'un envoie à répétition des paquets d'informations sur le port 139, Windows affiche un magnifique écran bleu du plus bel effet, qui oblige à redémarrer.
Pour se protéger il existe des patches permettant de corriger le bug, voir la rubrique mise à jour.

Le Mail Bombing
Le mail bombing consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres pour la faire saturer. En effet les mails ne sont pas directs, ainsi lorsque vous relèverez le courrier, celui-ci mettra beaucoup trop de temps et votre boîte aux lettres sera alors inutilisable...
Il existe toutefois des solutions, avoir plusieurs boîtes aux lettres permet de limiter les dégâts, une importante que vous ne divulguez qu'aux personnes dignes de confiance, et une à laquelle vous tenez moins. Des plus des logiciels anti-spam existent, ils interdiront la réception de plusieurs messages identiques à un intervalle de temps trop court.

Le spoofing IP
Le spoofing IP consiste en une usurpation, par un utilisateur du réseau, d'une adresse IP, afin de se faire passer pour la machine à laquelle cette adresse correspond normalement. Cette technique repose sur les liens d'authentification et d'approbation qui existent au sein d'un réseau. Lorsque des machines sur un même réseau connaissent l'adresse d'autres machines et qu'il existe des relations de confiance entre elles, elles peuvent exécuter des commandes à distance.

7. Spamming et mailbombing

Spamming et mailbombing sont deux techniques réprouvées par la Nétiquette, qui prennent pour cible votre boîte aux lettres et vous font perdre du temps. Au pire elles vous font perdre des données. Il existe quelques astuces pour réagir intelligemment, mais le mieux reste toujours la prévention : en combinant une divulgation prudente de son adresse email, la gestion de plusieurs comptes d'email et le filtrage des messages entrant, il est ainsi possible d'atténuer voire de complètement éliminer la nuisance que représente le spamming, tout en préservant sa vie privée sur le Net.

Définitions
Le spamming désigne l'action d'envoyer un message non souhaité et dérangeant - appelé "spam" - à une personne ou à un groupe de personnes, généralement dans un but promotionnel ou publicitaire. Sont notamment considérés comme des actes de spamming :

- Le fait d'envoyer un mail à un ou plusieurs inconnus pour leur suggérer de visiter un site web ou d'acheter un produit ;
- Le fait de poster dans un forum de discussion ou un newsgroup un message sans rapport avec le thème abordé, dans un but provocateur ou commercial ;
- Le fait d'utiliser le système de messagerie interne à Windows pour faire apparaître sur le poste d'un internaute une boîte de dialogue contenant un message publicitaire ;
- Le fait d'inclure un individu dans une liste de diffusion sans son consentement préalable et/ou de l'empêcher de se désabonner.

De manière plus globale, le spamming peut être défini comme l'usage abusif d'un système de messagerie électronique ou de traitement automatisé de données destiné à exposer délibérément et généralement de manière répétée tout ou partie de ses utilisateurs à des messages ou à des contenus non pertinents et non sollicités couramment appelés "spams", en faisant en sorte de les confondre avec les messages ou les contenus habituellement échangés ou recherchés par ces utilisateurs. Le support utilisé importe peu (courriel, messagerie instantanée, SMS, forum, moteur de recherche, livre d'or, etc.), de même que le nombre de messages envoyés par le spammer. Le spamming s'accompagne souvent de la part du spammer d'une ou plusieurs pratiques généralement reconnues comme illégales au niveau mondial (usurpation d'identité, collecte déloyale de données personnelles, contrefaçon de marque, escroquerie, entrave volontaire à un système...), mais ces pratiques sont à considérer comme des circonstances aggravantes et non des caractéristiques intrinsèques du spamming.

Le mailbombing est une technique d'attaque basique qui consiste à envoyer des centaines, des milliers voire des dizaines de milliers de messages appelés "mailbombs" à un unique destinataire, dans un but évidemment malveillant. Ces messages sont vides, revendicatifs voire injurieux, et potentiellement accompagnés de fichiers volumineux selon que l'objectif est une attaque DoS du serveur de messagerie ou la saturation de la boîte aux lettres de la victime. Certains virus comme Sircam ou Sobig.F pratiquent aussi le mailbombing, et sont ainsi capables de s'envoyer en plusieurs centaines d'exemplaires à la même personne en un temps réduit.

Les conséquences pour le spammé... et le spammer
A première vue, le spamming n'est pas bien méchant. Pourtant, il devient très vite agaçant par la perte de temps qu'il engendre : publicités pour des produits dont vous n'avez que faire voire pour des sites pornographiques, produits médicaux, gadgets, messages dans une langue incompréhensible... le téléchargement de mails inutiles augmente le temps de connexion lorsque vous relevez votre courrier, et surtout il faut ensuite passer du temps à trier et éliminer les courriers publicitaires ou parasites, au risque de supprimer un message valable.

Pour sa part, le mailbombing a clairement l'intention nuire, et à la perte de temps s'ajoute le risque de déni de service pour le serveur de messagerie visé par l'attaque et la perte de données pour l'utilisateur. En effet, la plupart des fournisseurs d'accès ou d'adresses email gratuites définissent une taille maximale pour les boîtes aux lettres, généralement quelques méga-octets. Si le mailbombing sature complètement la capacité de votre boîte, les courriers suivants seront perdus faute de place pour les stocker.

Dans l'état actuel de la législation, en France le spammer encourt généralement la fermeture ou la suspension sans préavis de son compte internet par son fournisseur d'accès, l'interdiction de procéder à du spamming étant généralement incluse dans les contrats de service. Dans le cas d'une entreprise, cette dernière risque également une forte dégradation de son image, le spamming étant particulièrement impopulaire. Des sanctions plus sévères peuvent cependant être envisagées lorsque le spamming s'accompagne de faits répréhensibles, comme la collecte déloyale de données personnelles ou la détention de bases de données illégales.

En cas de mailbombing ou si le spamming perturbe le bon fonctionnement d'un équipement du réseau, l'auteur peut également être poursuivi en justice : un internaute français a été condamné en février 2003 à quatre mois de prison avec sursis et 20.000 euros de dommages-intérêts pour avoir voulu se venger d'un rival amoureux en bombardant sa boîte aux lettres de messages.

Comment réagir face à un spammer ?
Dans le cas d'un internaute inexpérimenté qui veut que vous veniez visiter son site, ne répondez pas ou expliquez-lui gentiment que ce qu'il fait c'est du spamming, et que le spamming c'est contraire aux bonnes pratiques du Net.

S'il persévère ou dans le cas d'un message non sollicité envoyé par une entreprise française, passez à l'offensive et adressez-vous directement au propriétaire du serveur de mails utilisé (souvent celui du fournisseur d'accès du spammer). Il s'agit de déposer plainte, donc il faut fournir des preuves : joignez à votre email la copie de l'entête du message non sollicité (sélectionnez le mail dans votre boîte de réception, puis "Affichage des propriétés" ou du "Source de la page"). Exemple :

Received: from server15.exemple.info [190.21.56.47] ---> *(1)*
by smtp.votre-fai.com with ESMTP (SMTPD32-4.06) id A09D3203BC;
Tue, 05 Jan 1999 13:57:33 EST
Received: from argamemnon ([192.249.17.1]) ---> *(2)*
by server15.exemple.info (8.7.5) ID LAA28548; ---> *(3)*
tue, 5 Jan 1999 11:56:11 -0700 (MST)
Message-ID: <007901be38dc$e19a50e0$01010118@argamemnon> ---> *(4)*
Reply-To: billgates@micro$oft.com ---> *(5)*
From: zorro@masque.com ---> *(6)*
To: votre-adresse@votre-fai.com ---> *(7)*
Subject: Visitez mon site !!! ---> *(8)*
Date: tue, 5 Jan 1999 19:54:10 +0100
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8759-2"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.3110.5 ---> *(9)*
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.3110.3
X-UIDL: 568
Status: U

(1) adresse IP du serveur par lequel a transité le spam
(2) adresse IP du spammer
(3) serveur SMTP utilisé par le spammer
(4) nom réseau de l'ordinateur du spammer
(5) adresse où sera acheminée votre réponse éventuelle.
(6) adresse présumée du spammer (peut avoir été supprimée ou falsifiée)
(7) votre adresse email
(8) objet du mail
(9) logiciel de mail utilisé par le spammer

Dans cet exemple, il faut envoyer votre plainte à abuse@exemple.info voire aussi à postmaster@exemple.info (attention : remplacez exemple.info par le nom de domaine du FAI ou du serveur SMTP utilisé par votre spammer). Vous pouvez aussi tenter de vous rendre sur le site www.exemple.info afin de trouver le nom de la société à qui il appartient, ainsi que le numéro de téléphone ou l'adresse email du support technique. Si vous n'avez que l'adresse IP du perturbateur, vous pouvez utiliser un traceur pour savoir ce qui se cache derrière.

S'il s'agit de spammers internationaux, il n'y a par contre pas grand-chose à faire si ce n'est filtrer les messages (voire plus loin) : la plupart du temps ils utilisent des comptes d'emails temporaires voire de fausses adresses, et envoient leurs messages depuis des serveurs situés dans des pays hors réglementation. Ne songez même pas à utiliser le lien de désabonnement présent dans le spam reçu, car le plus souvent il s'agit d'une astuce pour vérifier que l'adresse email est valide et que les messages sont lus. Préférez même faire le tri dans votre boîte de réception en étant hors ligne, afin de ne pas déclencher les web-bugs éventuellement cachés dans les messages au format HTML et qui signaleraient aux spammers que vous avez ouvert leurs messages, au risque d'en recevoir encore davantage.

D'une manière générale, il ne faut jamais donner suite à un spam, afin de ne pas encourager cette activité et ne pas en recevoir davantage soi-même. Il faut au contraire prendre l'habitude de supprimer le courrier non sollicité dès sa réception et ne cliquer sur aucun de ses liens, même s'ils paraissent intéressants et même si les spammers utilisent toutes les astuces imaginables pour tenter de vous berner. On peut citer notamment :

- La fausse réponse, envoyée avec comme titre "Re : [phrase accrocheuse]". Elle tente de se faire passer pour une réponse à un message que vous n'avez bien sûr jamais envoyé ;
- Le faux message égaré, envoyé avec une adresse email semblant appartenir à une vraie personne. Cordial voire familier, l'expéditeur s'adresse à vous en vous appelant par le prénom d'un autre pour vous vanter les mérites d'un service ou d'un produit. En vous faisant croire à un message mal adressé, il tente de piquer votre curiosité ;
- Le faux message de confirmation d'abonnement à une newsletter. Généralement très bref, il fait en réalité la promotion d'un site dont il indique rapidement l'adresse ;
- L'adresse surprise, de la forme http://%59%38%36%33.%74%6b, que le spam vous propose de copier/coller dans votre navigateur pour découvrir le site (souvent pornographique) dont il fait la promotion;
- Le message envoyé avec de véritables adresses emails en destinataire et/ou en copie, afin de laisser croire à un message envoyé par un proche à un groupes d'amis ou collègues ;
- Le message envoyé à vous-même avec comme adresse d'expéditeur votre propre adresse email, pour passer la barrière psychologique de l'expéditeur inconnu... et les filtres anti-spams ;
- Le message au format HTML dont le contenu est une image, afin d'éviter toute présence de texte analysable par les logiciels anti-spam.

Il ne faut jamais donner suite à ce genre de message, et plus généralement à ceux envoyés par des inconnus, d'autant que leur but peut aussi être de vous orienter vers un site dont la page est piégée par un virus ou par l'exploitation d'une faille de votre navigateur.

Comment réagir en cas de mailbombing ?
Si vous êtes victime d'un mailbombing, lors de la levée du courrier votre boîte de réception se remplit de dizaines d'exemplaires du même message. Si les messages envoyés sont volumineux et que vous êtes connecté à internet via un accès bas débit (notamment RTC), vous pouvez avoir l'impression que le logiciel de messagerie se connecte mais que rien n'arrive, car les messages mettent plusieurs dizaines de secondes à se télécharger.

Dans le cas de messages volumineux, arrêtez la récupération du courrier en cours, puis configurez votre logiciel de messagerie pour qu'il ne récupère que les mails de taille inférieure à 10 ou 15 Ko. Vous pourrez ainsi vider immédiatement votre boîte aux lettres de la majorité des messages importants, la plupart des courriers échangés avec vos correspondants ne faisant habituellement que quelques kilo-octets.

Lancez ensuite le petit programme gratuit Magic Mail Monitor : ce dernier vous permet d'examiner le contenu de votre boîte aux lettres directement sur le serveur, avant de télécharger les messages. Il vous permet aussi de sélectionner et de supprimer sur le serveur les messages parasites : supprimez-les tous sauf un, afin de garder un exemplaire pour analyse détaillée de son entête (voir ci-dessus). Vous n'avez plus ensuite qu'à relever le courrier comme habituellement, puis à porter plainte auprès du propriétaire du serveur de mails utilisé par votre agresseur (voir ci-dessus).

Même si le mailbomber utilise un autre serveur de mails que celui de son fournisseur d'accès pour envoyer ses messages parasites, il est indispensable d'en avertir le propriétaire : il pourra modifier la configuration du serveur en question et empêcher ainsi son utilisation par d'autres que ses clients ou abonnés. Il s'y prêtera d'ailleurs bien volontiers, car en restreignant l'accès à son serveur, il économisera des ressources.

Si les bombardements de votre boîte aux lettres se renouvellent à partir de la même adresse mail avant que le propriétaire du serveur ait eu le temps de prendre les mesures qui s'imposent, et si votre logiciel de messagerie en possède un, configurez le gestionnaire de la boîte de réception pour qu'il ne télécharge pas les messages provenant de cette adresse, mais qu'il les détruise systématiquement sur le serveur.

Conseils et techniques anti-spamming
Afin de lutter plus efficacement contre le spamming voire le mailbombing, et en attendant une évolution de la législation, la meilleure solution reste la prévention. Commencez donc par gérer si possible votre courrier au travers de plusieurs boîtes aux lettres :

- N'utilisez jamais publiquement l'adresse email confiée par votre fournisseur d'accès ou votre entreprise, réservez-la à un cercle restreint d'amis ou de collègues en lesquels vous avez toute confiance. Des robots parcourent internet (sites personnels, sites professionnels, forums, etc.) dans le seul but de collecter des adresses emails qui seront ensuite spammées sans relâche ;
- Définissez une adresse spécifique à vos abonnements aux newsletters chez un fournisseur d'adresses email gratuites (Laposte.net, Hotmail.fr, etc.) : même si vous devez changer de fournisseur d'accès ou d'entreprise, vous n'aurez pas à vous réabonner à toutes vos listes de diffusion ;
- Définissez une autre adresse gratuite pour la vie de tous les jours (échange de courriers électroniques avec des inconnus, participation aux forums de discussion et aux chats, abonnements ou demandes d'informations à des sites douteux en matière de vie privée, etc.). En cas de problèmes de spamming ou de mailbombing, vous devrez pouvoir sacrifier cette boîte aux lettres sans états d'âme. Si vous faites en sorte de choisir une boîte aux lettres gratuite consultable par une interface web (webmail), vous pourrez supprimer facilement la plupart des messages importuns d'après leur objet, sans avoir à la télécharger.

Par ailleurs, il est nécessaire de penser dès vos débuts sur internet à ne laisser qu'un minimum de traces, voire à brouiller les pistes :

- Réfléchissez bien avant de dévoiler votre identité réelle, que ce soit sur un site internet ou dans un forum de discussion (dans le corps du message, dans votre adresse email type prénom.nom@fournisseur.fr ou encore dans le nom d'expéditeur du message). Les moteurs de recherche et certains sites spécialisés permettront ensuite et pour très longtemps à quiconque (personne malveillante, employeur, etc.) de faire une recherche avec votre nom comme mot-clé et de connaître ainsi le contenu de vos interventions, vos passions, votre adresse email, etc.
- Vérifiez que votre adresse email ne sera pas diffusée sans votre accord explicite. Certains fournisseurs d'accès ou prestataires peuvent automatiquement vous inscrire dans un annuaire web, un forum fera figurer l'adresse saisie dans tous vos messages, certains annuaires publient l'adresse email des webmasters en même temps que les autres caractéristiques de leur site, etc. Méfiez-vous notamment des sites qui vous demandent votre adresse pour vous envoyer par email ce que vous pourriez consulter ou télécharger facilement par le web (référencement ou position de votre site dans les moteurs de recherche, scripts pour webmasters, etc.). Consultez la charte "vie privée" ou "données personnelles" du site si elle existe, tout en gardant à l'esprit qu'elle peut n'engager que celui qui la lit... ;
- En cas de doute, saisissez une fausse adresse ou maquillez votre véritable adresse. Lorsque vous intervenez dans un forum, même si vous utilisez une adresse gratuite vous pouvez ajouter une expression parasite au début ou à la fin de cette adresse (ex. : pasdespam-votre@adresse.com ou votre-at-adresse.com) afin de tromper les robots en rendant l'adresse invalide tout en laissant la possibilité aux autres participants de deviner votre adresse et de vous écrire (ces astuces tromperont également les virus qui collectent des adresses emails dans les pages visitées par l'internaute pour s'y envoyer). Sachez cependant que ces astuces sont déjouées par ces mêmes robots dès qu'elles deviennent populaires (c'est souvent le cas par exemple de "nospam-") ;

- Ne diffusez pas vous-même les adresses des autres internautes. Lorsque vous envoyez un message à plusieurs personnes, mettez si possible les adresses emails des destinataires dans le champ "Cci" (copie carbone invisible) et non "A" (destinataire) ou "Cc" (copie carbone), afin que chaque destinataire n'ait pas connaissance de l'adresse de tous les autres (et donc ne puisse pas les récupérer). De même, lorsque vous transférez ou copiez dans un forum un message reçu par email, retirez-en les adresses emails éventuellement présentes dans l'entête "---Message d'origine---" afin qu'elles ne puissent pas être récupérées par les robots ;
- Évitez de choisir ou d'utiliser certaines adresses emails. Des adresses comme : contact@votredomaine.com, info@votredomaine.com, clients@votredomaine.com, sales@votredomaine.com, feedback@votredomaine.com, marketing@votredomaine.com ou billing@votredomaine.com, couramment utilisées pour les contacts commerciaux, sont automatiquement spammées par certains logiciels une fois récupéré le nom de domaine des sites web à prospecter ;
- Installez un firewall personnel. Les postes sous Windows peuvent être spammés via un utilitaire de messagerie interne, ce qui provoque l'affichage d'une boîte de dialogue au premier plan à l'écran. Pour s'en prémunir, les utilisateurs peuvent installer un firewall personnel afin de bloquer les ports impliqués dans la transmission et plus généralement d'améliorer la sécurité de leur ordinateur ;
- Si vous êtes webmaster, pour votre rubrique contact utilisez des formulaires en veillant à ne pas faire figurer l'adresse email des destinataires dans le code source de la page web, afin de prévenir toute récupération. Ne mentionnez pas en clair votre adresse ni celles des membres de votre équipe ou de votre société, même en utilisant des astuces comme le codage en javascript ou le remplacement du caractère @ par son code ASCII &# 64. Ces techniques sont aisément contournables ou le seront dès qu'elles deviendront populaires, et donc qu'il deviendra rentable de les contourner.

Enfin, si vous êtes déjà victime de spamming ou que vous ne pouvez pas limiter la diffusion de votre adresse à quelques personnes de confiance, vous pouvez filtrer le courrier reçu :

- Essayez les fonctionnalités anti-spam éventuellement disponibles dans votre logiciel de messagerie ou votre webmail. Plutôt que la suppression immédiate, optez pour le déplacement des messages suspects dans un répertoire poubelle, afin de vérifier au moins dans un premier temps que les messages écartés sont bien tous des spams ;
- Filtrez les messages reçus à leur arrivée dans votre logiciel de messagerie. Dans Outlook choisissez "Outils" puis "Assistant Gestion des messages...", dans Outlook Express choisissez "Outils" puis "Règles de messages" puis "Courrier...", dans Mozilla sélectionnez le compte puis cliquez sur "Create message filters" et laissez-vous guider.
- Définissez une règle de filtrage pour que les messages comportant l'expression "ADV:", "[ADV]" ou "ADV " dans leur objet soient redirigés vers un répertoire poubelle. Ces expressions sont parfois utilisées par les spammers pour signaler que le message est une publicité (advertisement, en anglais) ;
- Définissez une règle de filtrage pour que les messages comportant l'expression "ks_c_5601-1987", "KS_C_5601-1987" ou "euc-kr" dans leur entête soient redirigés vers un répertoire poubelle, si vous n'avez pas de correspondant coréen. Ces expressions correspondent précisément aux jeux de caractères du Coréen, une langue très fréquente dans les spams internationaux ;
- Définissez une règle de filtrage pour que les messages contenant l'expression ".com.br", ". com.tw", ".net.tw", ".co.kr", ".co.jp" ou ".com.cn" dans l'adresse d'expéditeur ou dans leur entête soient redirigés vers un répertoire poubelle, si vous n'avez pas de correspondant brésilien, taïwanais, coréen, japonais ou chinois. Ces domaines exotiques sont également assez largement utilisés dans les spams internationaux ;
- Installez le plug-in gratuit SpamBayes si vous utilisez le logiciel de messagerie Microsoft Outllook 2000/XP pour Windows, mais aussi pour les plateformes Linux et Mac OS. Avec Outlook Express 5/6 et également Outllook 2000/XP vous pouvez utiliser SpamPal ;
- Ne donnez jamais donner suite aux spams reçus, sauf à les dénoncer à l'adresse abuse@ du propriétaire du serveur utilisé pour les envoyer.

Il existe par ailleurs une technique qui permet de mettre fin définitivement à la perte de temps engendrée par le spamming, au prix d'une petite implication de vos interlocuteurs. Elle est basée sur le fait que le spammer ne peut pas connaître votre nom ou votre pseudo autrement qu'en analysant votre adresse email. Si vous demandez à vos correspondants de vous insérer dans leur carnet d'adresses avec un nom de contact plus ou moins différent du login de votre adresse ("Jean Dupond" ou "Super Dupond" si votre email est j.dupond@exemple.info, "-star-" si votre email est star@exemple.info) vous êtes en mesure de filtrer les messages entrant pour ne retenir que ceux qui vous ont réellement été envoyés par vos correspondants, ainsi le cas échéant que via le formulaire de votre site web : il suffit de définir une règle qui envoie dans un répertoire poubelle tous les messages sauf ceux qui comportent le nom de contact (ici "Jean Dupond", "Super Dupond" ou "-star-") dans leur entête ou dans les champs A/Cc. Si vous êtes en copie cachée, le message ne peut cependant pas être distingué d'un spam, à moins que vous ne prévoyiez des exceptions pour certains correspondants choisis.

En combinant une divulgation prudente de son adresse email, la gestion de plusieurs comptes d'email et le filtrage des messages entrant, il est ainsi possible d'atténuer voire de complètement éliminer la nuisance que représente le spamming, tout en préservant sa vie privée sur le Net.

8. Les méthodes anti-spam

Le filtrage bayésien
Les statistiques Bayésiennes ont d'abord été mises en évidence par le scientifique anglais T. Bayes.
Ses principales caractéristiques consistent en l'utilisation des expériences passées pour effectuer des prédictions.
La méthode bayésienne est présentée comme une approche "intelligente" qui examine tous les aspects d'un courrier électronique, par opposition au contrôle de seuls mots-clefs ou chaînes interdites.
S'agissant du spam, si une certaine chaîne de caractères se présente souvent dans des courriers indésirables, alors la prochaine fois que cette même chaîne de caractères se représentera dans un nouveau courrier, on pourra supposer que ce courrier est probablement "indésirable".

La probabilité peut être calculée en tenant compte du nombre de fois que cette chaîne se présente en tant que spam par rapport au courrier légitime. Cette probabilité varie avec les destinataires.

Si la probabilité est plus grande qu'un certain seuil, alors le message est considéré comme indésirable.

- Brièvement, voici quelques avantages du filtrage bayésien :
- Il tient compte de l'ensemble du message ;
- Il est multilingue et international ;
- Il utilise l'intelligence artificielle ;
- Il est difficile à contourner.

Le filtrage heuristique
Le filtrage heuristique est une technique de filtrage fondée sur l'analyse du contenu des messages.
La technique analyse et note la présence de forme (par exemple l'objet du message tout en MAJUSCULE), de code (présence exagérée de code HTML visant à dégrader les performances d'un filtre sémantique).
Cette technique de filtration à l'avantage d'être indépendante de la langue de l'utilisateur.
De plus, elle vérifie un nombre important de règles : 800 règles sont couramment employées dans les solutions anti-spam.
Par contre le filtrage heuristique nécessite une maintenance assez importante, car en général les spammeurs s'adaptent aux règles et ajoutent de "nouvelles règles". Ainsi, la mise à jour de ces règles dans ce système de filtrage est permanente.

Exemple d'objets dans un message pouvant être filtrées par cette méthode :

- so|utions to common hea1th problems
- cred1ted to your acc0unt when you s1gn up
- Best s0ftware prices.
- We are having specials on C|AL|S, V1AGRA, PR0ZAC, ZYBAN and C3LEBREX

Vous pouvez ainsi constater que les "i" sont remplacés par des "1" ou "|" ; les "o" par des "0", etc...

Les listes noires et RBL
En quelques mots, nous pouvons définir les listes "blanches" et "noires" de la manière suivante : les expéditeurs en liste noire sont bloqués et les expéditeurs en liste blanche sont les bienvenus.
Les listes noires sont les listes ayant identifié des spams collectifs et sont listés afin de ne pas les délivrer.
Sur le même principe que les listes blanches, il y a des listes noires "locales", et des listes noires générales, communément appelées les RBL.

RBL ou Realtime Blackhole List
La RBL est une liste noire de machines ou de domaines bannis, mise à jour en temps réel.

Les filtres anti-spam s'appuyant sur cette méthode, consultent en général automatiquement la mise à jour des bases.

Il existe différentes RBL, comme :
- MAPS RBL
- ORBS
- SBL et XBL
- DSBL...

La base de données OBRS est utilisée par de nombreuses sociétés, parmi lesquelles GearHost Inc. Aux USA qui rejette 5 500 000 d'emails par jour, ou encore Bigfoot avec 4 000 000 d'adresses rejetées journalièrement.

SBL
Enfin, concernant la SBL ; le projet de Spamhaus.org donne plus de moyens aux fournisseurs Internet pour couper à la source les courriers non sollicités, qui polluent nos boîtes aux lettres électroniques.
Cette liste XBL est conçue pour être exploitée parallèlement à la liste noire traditionnelle déjà mise en place par Spamhaus (la SBL), qui recense les adresses IP de spammeurs identifiés, et non de centres-relais.
Ces services sont gratuits et ne font l'objet d'aucune propriété quelconque.
En cas d'erreur Spamhaus donne la possibilité de retirer une adresse IP de ses listes.

L'anti-spoofing
Tout d'abord, il convient de définir ce qu'est l'IP Spoofing. En clair, cela signifie usurpation d'adresse IP.
Bien que cette attaque soit bien connue, elle reste d'actualité.
Effectivement, cette attaque peut être utilisée de deux manières différentes :
- La première utilité de l'IP Spoofing va être de falsifier la source d'une attaque.
- L'autre utilisation de l'IP Spoofing va permettre de profiter d'une relation de confiance entre deux machines pour prendre la main sur l'une des deux.

Il existe plusieurs types d'IP Spoofing :
La première est dite "Blind Spoofing", c'est une attaque en aveugle. Les paquets étant forgés avec une adresse IP usurpée, les paquets réponses iront vers cette adresse. Il sera donc impossible à l'attaquant de récupérer ces paquets.
Pour le deuxième type, il s'agit d'utiliser l'option "IP Source Routing" qui permet d'imposer une liste d'adresses IP des routeurs que doit emprunter le paquet IP. Il suffit que l'attaquant route le paquet réponse vers un routeur qu'il contrôle pour le récupérer.

Néanmoins, la grande majorité des routeurs d'aujourd'hui ne prennent pas en compte cette option IP et jettent tous paquets IP l'utilisant.

Les manières de s'en protéger sont de quatre sortes :
- Supprimer tous les services de type rsh et rlogin.
- Ne pas utiliser uniquement l'adresse IP comme méthode d'authentification.
- Vérifier que son système n'a pas des numéros de séquence TCP facilement prédictible.
- Utiliser une fonction anti-spoofing.

Le blocage des serveurs "open relay"
Ces serveurs ouverts "open relay" autorisent n'importe quel expéditeur à envoyer à n'importe quel destinataire des e-mails, le plus souvent du spam.

Des sites, tels que ORDB ou DSBL les traquent et permettent aux administrateurs système de s'en prémunir, mais la tâche est vaste.

Normalement, un serveur de mail correctement paramétré n'accepte que des expéditeurs et des destinataires appartenant à son domaine local ou à sa gamme d'IP.

Quand ce n'est pas le cas, faute de sécurisation suffisante, le serveur devient une cible idéale pour des spammeurs toujours à l'affût de passerelles gratuites masquant leurs agissements.

Par exemple, votre fournisseur d'accès Internet s'appelle "Fournisseur" et vous fournit un serveur de mail appelé smtp.fournisseur.com. Si des internautes qui ne sont pas clients de "Fournisseur" sont autorisés à utiliser smtp.fournisseur.com, alors c'est un open relay.

Le test de Turing
Les utilitaires anti-spam à base de test de Turing, plutôt rares pour l'instant, représentent une les meilleures solutions anti-spam actuelle.

Il s'agit de s'assurer de l'humanité d'un émetteur de courrier électronique : est-ce bien un humain ou est-ce un robot ?

Concrètement, on va lui demander de résoudre une énigme, simplissime pour l'humain, impossible pour la machine, raison pour laquelle certains tests de Turing s'appellent "Challenge Message".

S'il y a une réponse satisfaisante, on considère que l'émetteur est réellement un humain et son adresse et placée automatiquement en liste blanche. Il ne lui sera plus infligé de test de Turing. Dans tous les autres cas, l'émetteur n'est probablement pas légitime.

Le résultat est immédiat:
- Soit l'adresse de l'expéditeur du courrier est une véritable adresse mais usurpée (en cas de spoofing par exemple) donc, comme il ne vous à rien envoyé, il ne répond pas à l'énigme posée par le test de Turing et sa correspondance prétendue n'est pas délivrée. Le message électronique reste en quarantaine.
- Soit l'adresse de l'expéditeur est forgée de toutes pièces donc elle n'existe pas et personne ne répondra jamais à l'énigme. Le message électronique reste également en quarantaine.
- Soit l'adresse est celle d'un robot et elle n'est jamais relevée. Le résultat est le même (quarantaine).
- Soit l'adresse est réelle et correspond au spammeur ou à son commanditaire. Sous l'avalanche d'énigmes à résoudre, il ne peut rien faire.
- Soit l'adresse est réelle et l'expéditeur est humain et la réponse au test de Turing est positive. Le test est passé permettant le "laisser-passer" du message.

Les messages placés en quarantaine peuvent être ensuite consultés par le destinataire qui décide du sort réservé à ces emails.

Conclusion
Ces différentes méthodes de gestion et de filtrage des messages électroniques vous permettent d'avoir une base de réflexion pour le choix de votre outil anti-spam.

Pour une utilisation individuelle et monoposte, vous avez par exemple Spam Assassin qui analyse les emails entrant avec un filtre heuristique et utilise les listes noires.

Ainsi, un outil anti-spam vraiment fonctionnel et utile doit pouvoir utiliser au moins deux méthodes de filtrages pour vous assurer une protection minimale.

Enfin, le test de Turing et le filtrage bayésien sont les deux méthodes les plus évoluées. Bon à savoir pour choisir son logiciel anti-spam.

9. Spywares : ces logiciels à votre écoute

Rien ne les différencie en apparence des logiciels classiques, à part leur propension à la gratuité. Les spywares sont pourtant les représentants d'un nouveau modèle économique, dans lequel les produits et services s'échangent contre une parcelle de vie privée. Après les scandales provoqués en 1999 par la découverte de spywares dans deux logiciels très populaires, la pratique est devenue plus transparente mais les abus restent nombreux.
Téléchargés sur internet ou trouvés dans le CD-Rom d'un magazine informatique, les spywares sont des logiciels (presque) comme les autres.

Qu'est-ce qu'un spyware?
Un spyware, en français "espiogiciel" ou "logiciel espion", est un programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

Même préalablement informé d'un éventuel tracking, l'utilisateur n'en reste pas moins soumis à une surveillance dont la nature peut s'avérer illégale du point de vue de la législation de son pays. L'analyse de sa navigation sur internet peut ainsi par exemple permettre de déduire et de stocker des informations - réelles ou supposées - sur ses origines raciales, ses opinions politiques, philosophiques ou religieuses ou encore son appartenance syndicale, ce qui est interdit en France sans le consentement de l'intéressé.

Une autre définition du spyware pourrait être un logiciel commercial (c'est-à-dire légalement disponible dans le commerce, payant ou gratuit) que son mode de financement ou son mode de fonctionnement amène à recueillir puis transmettre à un tiers des données personnelles concernant ses utilisateurs, sans avoir obtenu au préalable une autorisation explicite et éclairée de ces derniers. Les spywares sont donc différents des chevaux de Troie et autres enregistreurs de frappes au clavier (keyloggers), contrairement à une déformation récente de leur définition, même si ces derniers peuvent également être utilisés pour collecter et envoyer des données sensibles, dans un but cette fois clairement malveillant. Ces derniers sont détectés et supprimés de façon systématique par les antivirus, ce qui n'est pas le cas des spywares, qui peuvent malgré tout avoir été installés volontairement par certains utilisateurs.

Les spywares sont parfois confondus avec les adwares, ces logiciels dont l'auteur se rémunère par l'affichage de bannières publicitaires, sans pour autant recueillir ni transmettre de données personnelles et sans forcément porter atteinte à la vie privée de leurs utilisateurs (le navigateur Opéra avant le 20/09/05 ou le logiciel de messagerie Eudora en version gratuite sont des adwares). Ils sont également confondus à tort avec les cookies et les web-bugs, qui ne sont pas des programmes espions mais plutôt des procédés techniques dont la mise en œuvre peut être détournée pour porter atteinte à la vie privée.

Deux types de spywares
Une première classification des spywares peut être établie en tenant compte de leur fonction, à savoir le commerce ou le renseignement :

Les spywares commerciaux collectent des données sur leurs utilisateurs et interagissent de manière visible avec eux, en gérant l'affichage de bannières publicitaires ciblées, en déclenchant l'apparition de fenêtres pop-up, voire en modifiant le contenu des sites web visités afin par exemple d'y ajouter des liens commerciaux. Ce sont les spywares les plus courants. Leur existence est généralement mentionnée dans la licence d'utilisation du logiciel concerné, mais souvent dans des termes ambigus et/ou dans une langue étrangère, ce qui fait que l'utilisateur n'est pas correctement informé. Ils se présentent généralement sous la forme de logiciels gratuits, pour les éditeurs desquels ils constituent une source de revenu ;
les mouchards collectent également des données sur leurs utilisateurs mais le font dans la plus totale discrétion. La surveillance et la réutilisation éventuelle des données collectées se font à l'insu des utilisateurs, généralement dans un but statistique ou marketing, de débogage ou de maintenance technique, voire de cybersurveillance. L'existence de ces mouchards est délibérément cachée aux utilisateurs. Ils peuvent concerner n'importe quel logiciel, qu'il soit gratuit ou payant, mais de par leur nature ils sont peu fréquent, le risque en terme d'image en

cas de découverte et médiatisation de l'existence du mouchard par un utilisateur étant à lui seul dissuasif pour la plupart des éditeurs.
Une seconde classification peut être opérée en fonction de la nature des spywares, à savoir leur constitution logicielle :

Le spyware intégré (ou interne) est une simple routine incluse dans le code d'un programme ayant une fonction propre pour lui donner en plus la possibilité de collecter et de transmettre via internet des informations sur ses utilisateurs. Les logiciels concernés sont par exemple Gator, New.net, SaveNow, TopText, Alexa ou Webhancer ainsi que la totalité des mouchards. Le spyware et le programme associé ne font qu'un et s'installent donc simultanément sur l'ordinateur de l'utilisateur ; le spyware externalisé est une application autonome dialoguant avec le logiciel qui lui est associé, et pour le compte duquel elle se charge de collecter et de transmettre les informations sur ses utilisateurs. Ces spywares sont conçus par des régies publicitaires ou des sociétés spécialisées comme Radiate, Cydoor, Conducent, Onflow ou Web3000, avec lesquelles les éditeurs de logiciels passent des accords. Le spyware de Cydoor est par exemple associé au logiciel peer-to-peer KaZaA, et s'installe séparément mais en même temps que lui.
Une nouvelle tendance encore plus contestable concerne les utilisateurs du navigateur Internet Explorer. Certains spywares comme Gator cherchent à s'installer automatiquement sur le poste de l'internaute au moyen de la technologie ActiveX, lors de la visite de pages web peu recommandables.

Fonctionnement d'un spyware
Dans le cas des spywares commerciaux, avant de pouvoir procéder à l'installation du logiciel gratuit convoité l'utilisateur est généralement invité à fournir certaines informations personnelles voire nominatives (email, nom, âge, sexe, pays, profession, etc.). Un identifiant unique est alors attribué à l'ordinateur de l'internaute, qui permettra de relier les données collectées et centralisées dans une gigantesque base de données aux informations personnelles fournies par l'utilisateur, voire éventuellement à d'autres informations recueillies sans préavis (configuration, logiciels installés, etc.).

L'analyse de ces données permet de déterminer les habitudes d'utilisation, les centres d'intérêts voire les comportements d'achat de l'utilisateur et de lui proposer ainsi des bannières publicitaires, des courriers électroniques promotionnels ou des informations commerciales contextuelles toujours plus ciblés, en rémunérant au passage les éditeurs de logiciels partenaires. Dans le cas du spyware commercial Cydoor, l'installation du programme copie sur le disque les fichiers nécessaires au fonctionnement de l'application (cd_load.exe, cd_clint.dll et cd_htm.dll), crée un répertoire pour stocker les bannières qui seront affichées à l'utilisateur même lorsqu'il sera hors ligne (Windows/System/AdCache/), puis modifie la base de registres.

La plupart des spywares fonctionnent avec une extrême discrétion : ils agissent en tâche de fond, apparaissent rarement dans le Menu Démarrer de Windows et même dans le cas des spywares externalisés sont le plus souvent absents de la liste des programmes installés figurant dans le Panneau de configuration. Dans le cas des spywares commerciaux, il est normalement fait état de leur existence dans la licence du logiciel mais ça n'est pas toujours le cas et c'est souvent en des termes trompeurs, décrivant rarement le détail des informations collectées et l'utilisation qui en sera faite. Quel que soit le type de spywares, les données collectées et transmises sont définies dans le code source du spyware, et le cryptage des transmissions fait qu'il est difficile de s'assurer de leur nature exacte.

Le spyware s'exécute souvent automatiquement au démarrage de Windows et mobilise donc en permanence une partie des ressources du système. Pour collecter certaines données, les spywares peuvent également être amenés à modifier des fichiers vitaux gérant par exemple les accès à internet, ce qui peut conduire à des dysfonctionnements importants en cas d'échec de l'installation ou de la désinstallation du spyware. Certaines fonctionnalités annexes comme la mise à jour automatique peuvent aussi représenter un danger pour la sécurité de l'utilisateur, en permettant le téléchargement et l'installation à son insu d'un autre programme ou d'un autre spyware, voire d'un programme hostile dans le cas du détournement du système par une personne malveillante.

Règles générales de protection
Depuis les scandales provoqués en 1999 par la découverte de spywares dans SmartUpdate (Netscape) et RealJukeBox (Real Networks), la pratique est devenue plus transparente dans le cas des spywares commerciaux, même si les abus restent nombreux. Quelques règles simples peuvent être observées :

- Lisez attentivement les conditions d'utilisation d'un logiciel avant de l'installer. L'existence d'un spyware commercial et de ses fonctionnalités annexes y sont normalement signalées, même s'il faut bien souvent lire entre les lignes car le spyware y est présenté en des termes édulcorés voire trompeurs, voire parce que tout est fait pour que l'utilisateur évite de lire lesdites conditions d'utilisation. Si vous ne comprenez pas la langue dans laquelle est rédigée une licence d'utilisation vous ne devriez pas installer le logiciel concerné ;
- Réfléchissez bien avant de dévoiler des informations personnelles. Dans le meilleur des cas, les conditions d'utilisation sont généralement conformes au droit américain, donc beaucoup moins protectrices en matière de vie privée qu'en Europe. Notamment ne donnez pas votre adresse email permanente chez votre fournisseur d'accès mais plutôt un compte d'email gratuit qui pourra être fermé en cas de spamming ;
- N'acceptez pas sans réfléchir les programmes supplémentaires éventuellement proposés lors de l'installation d'un logiciel. New.net, SaveNow et Webhancer sont ainsi proposés par défaut lors de l'installation de KaZaA, mais il suffit de décocher les cases correspondantes pour qu'ils ne soient pas installés ;
- Installez un firewall personnel et surveillez les demandes d'autorisation de connexion à internet, afin de détecter toute application suspecte. C'est une autre bonne raison d'installer un firewall personnel ;
- Informez-vous auprès de sites spécialisés;
- Gardez enfin à l'esprit qu'installer un logiciel n'est jamais une opération anodine : cela revient à autoriser le programme à effectuer toutes les opérations qu'il souhaite sur votre disque dur. Outre un spyware, un programme douteux peut contenir un virus ou un troyen, donc un minimum de précaution s'impose.
- Les spywares commerciaux n'étant pas des virus ni des troyens, analyser son disque dur avec un antivirus à jour n'assure pas de l'absence d'un spyware. Il existe cependant d'autres moyens de les détecter voire de les éliminer : il est ainsi utile d'exécuter un antispyware périodiquement ou après l'installation d'un logiciel douteux, pour s'assurer de ne pas avoir installé un spyware sans le savoir.

Comment détecter la présence d'un spyware ?
Le plus simple pour détecter la présence d'un spyware est de procéder par des moyens indirects, à savoir son activité, la présence de fichiers caractéristiques ou le nom du logiciel suspect. Les moyens ci-dessous sont assez faciles à mettre en oeuvre, mais ne concernent que les spywares commerciaux ainsi que les mouchards dont l'existence a été découverte.

Il existe ainsi des listes de spywares, consultables en l'état, sous forme de moteurs de recherche ou encore d'utilitaires dédiés. Près d'un millier de logiciels (spywares intégrés ou programmes associés à un spyware externalisé) ont ainsi été recensés, dont Babylon Translator, GetRight, Go!Zilla, Download Accelerator, Cute FTP, PKZip, KaZaA ou encore iMesh :

Cette méthode de détection est simple, mais aucun site ne peut prétendre à l'exhaustivité : même l'utilitaire Ad-Search (LavaSoft) édité par un spécialiste du sujet est incomplet. Elle ne constitue donc qu'une première approche, qui reste très pédagogique car elle permet de mesurer l'ampleur du phénomène.

Certains firewalls personnels sont capables de filtrer le trafic sortant sur une base applicative, c'est-à-dire que chaque application souhaitant accéder à internet doit au préalable y avoir été autorisée.

Cette solution donne de bons résultats avec la plupart des spywares, y compris si le spyware est un fichier DLL (l'application qui tente de se connecter à internet est alors RUNDLL32.EXE), mais elle ne peut rien contre les spywares intégrés si le logiciel concerné a déjà été autorisé à accéder à internet dans le cadre de son fonctionnement normal. L'utilisateur doit par ailleurs être suffisamment compétent pour pouvoir décider si l'application qui tente de se connecter doit ou non y être autorisée.

C'est pourquoi des antispywares ont été conçus sur le modèle des anti-virus, afin de détecter les spywares sur la base de signatures. Utilisables facilement même par des non-initiés, ils permettent de détecter un spyware même s'il n'est pas actif, mais restent dépendants de la mise à jour du fichier des signatures.

OptOut étant abandonné, le plus performant des antispywares gratuits actuels est Ad-Aware (LavaSoft), qui a par ailleurs le mérite d'exister en version française.

Ce programme permet de scanner la mémoire de l'ordinateur, la base de registres et les différents disques à la recherche des composants indiquant la présence d'un spyware connu. En version payante, il dispose même d'un moniteur capable de surveiller le système en permanence et d'empêcher l'installation d'un spyware en temps réel.

Comment faire pour éliminer un spyware ?
La désinstallation d'un logiciel ne supprime pas forcément le spyware installé avec lui. Ainsi, la désinstallation de KaZaA ne supprime ni son spyware externalisé Cydoor, ni les autres spywares installés avec ce logiciel.

Pour éliminer un spyware intégré, il suffit le plus souvent de désinstaller l'application correspondante depuis le Panneau de configuration de Windows. Dans le cas d'un spyware externalisé, il est par contre généralement nécessaire de passer par une procédure fournie par son éditeur dans une obscure FAQ, ou plus efficacement d'utiliser Ad-Aware en supprimant les fichiers constitutifs du spyware.

Dans la plupart des cas, l'élimination d'un spyware externalisé fera que le logiciel associé cessera de fonctionner, affichant un message du type : "Vous avez effacé un composant du logiciel nécessaire à son exécution. Le logiciel ne fonctionnera plus mais vous pouvez le réinstaller". Certains antispywares permettent de bloquer ou de neutraliser un spyware tout en continuant à utiliser son logiciel associé, mais leur utilisation est assimilable à du piratage, les contrats de licence faisant généralement du spyware une contrepartie obligatoire à l'utilisation gratuite du logiciel associé.

NB : les logiciels antispywares incluent souvent la détection de certains cookies dans leurs signatures, au risque d'affoler les non-initiés car les cookies ne sont pas des spywares. Ce sont de simples fichiers texte gérés par votre navigateur Internet qui permettent aux sites web visités de stocker certaines informations sur votre disque dur - personnelles ou non, en fonction des données que vous confiez à ces sites - afin de pouvoir les retrouver lors de votre parcours dans le site ou lors de votre prochaine visite. Si vous ne souhaitez pas autoriser les sites web à utiliser des cookies, il suffit de désactiver ou de limiter strictement cette option dans votre navigateur web.

Spyware or not spyware ?
S'il ne peut y avoir aucune hésitation à condamner les mouchards et plus globalement le principe visant à espionner les utilisateurs à leur insu, contrairement à la publicité en ligne telle que pratiquée par la régie DoubleClick - qui par l'intermédiaire des sites web de tous ses clients collecte et centralise elle aussi des données sur les préférences de chaque internaute* - le tracking opéré par les spywares commerciaux a le mérite de ne concerner que les utilisateurs qui décident d'installer un de ces logiciels, laissant donc la liberté aux autres internautes de ne pas en installer ou d'opter pour une version payante dépourvue de spyware.

Malheureusement, au lieu d'opter pour la transparence et d'en expliquer clairement les enjeux, beaucoup d'éditeurs de logiciels ont été tentés de profiter de la discrétion des spywares pour en dissimuler l'existence ou pour les laisser implanter même après la désinstallation du logiciel associé. Des pratiques abusives qui ont rapidement décrédibilisé le concept, jetant la suspicion y compris sur la nature réelle des informations collectées. Les spywares commerciaux sont ainsi devenus aux freewares et aux sharewares ce que le spamming est à l'e-mailing. Ils ont d'ailleurs également créé un marché spécifique, puisqu'aux spywares qui exploitent la confiance ou l'ignorance des internautes viennent désormais s'ajouter un nombre croissant d'utilitaires antispywares payants qui exploitent les peurs - et il faut bien le dire aussi parfois l'ignorance - de ces mêmes internautes.

Qu'il se résigne à voir ses données personnelles converties en dollars à son insu par d'obscurs logiciels ou qu'il choisisse de se protéger par l'acquisition d'utilitaires toujours plus nombreux et coûteux, l'internaute est-il condamné à payer la facture des spywares quelle qu'en soit la monnaie? Heureusement que non, mais sauf à renoncer à installer de nouveaux programmes sur son ordinateur, il devra chercher à s'informer et surtout faire preuve d'un minimum de vigilance s'il souhaite que sur Internet sa vie reste privée.

10. Les troyens

Les troyens sont des sortes de virus permettant l'intrusion et la prise de contrôle d'un ordinateur à distance par celui qui vous l'aura envoyé.

Le téléchargement de fichiers d'origine douteuse est le principal moyen de contamination par les programmes de type troyen. Ces derniers permettent à votre agresseur de contrôler à distance votre machine, et lui donne tout pouvoir sur les fichiers de votre disque dur (lecture, suppression, vol, etc.).

Comment savoir si mon micro est infecté par un troyen ? Lors de son installation, le troyen s'installe en mémoire et s'arrange pour être exécuté à chaque démarrage de votre machine. Si vous ne vous rendez compte de rien, vous le détecterez tôt ou tard par ses conséquences négatives, voire désastreuses, liées au fait que le troyen permet à votre agresseur de contrôler à distance votre ordinateur lorsque vous être connecté à d'internet.

Une indication symptomatique est de voir clignoter les diodes de votre modem, ou d'entendre votre disque dur "mouliner" alors vous êtes connecté mais que vous ne faite rien (ni navigation sur internet, ni téléchargement de programme) : il est fort probable que cette activité soit due à la présence d'un troyen, et qu'en ce moment même un individu soit en train de visiter votre disque dur...

Histoire
Les chevaux de Troie ou troyens sont basés sur une anecdote historique qui s'est déroulé il y a bien longtemps.

C'est l'histoire ancestrale du "cheval de Troie". Les Grecs effectuaient le siège de la ville de Troie et n'arrivaient pas à faire plier la ville assiégée. Les assaillants eurent l'idée de construire un énorme cheval de bois et de l'offrir aux Troyens.

Ceux-ci prirent le cheval de bois pour un cadeau des Dieux et l'accueillère à l'intérieur de leur ville. Cependant, le cheval était rempli de soldats qui s'empressèrent d'en sortir à la tombée de la nuit, alors que la ville entière était endormie ...
Cette ruse permis aux Grecs de pénétrer dans la ville et de gagner la bataille.

Un cheval de Troie (informatique) est donc un programme caché dans un autre qui exécute des commandes sournoises.

Un peu comme le virus, le cheval de Troie est un code (programme) nuisible. Il exécute des instructions nuisibles lorsque vous exécutez le programme sain. Il peut par exemple voler des mots de passe, copier des données, ou exécuter toute autre action nuisible ...

Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur.

Principe
Les troyens ou chevaux de Troie permettent à une personne malveillante d'ouvrir des brèches dans un système, c'est à dire d'ouvrir un port sur la machine distante qui va permettre aux deux machines de communiquer. Pour que la communication s'établisse il faut deux parties essentielles, un logiciel serveur qui doit être installé sur la machine distante et un logiciel client qui permettra de piloter l'ordinateur distant.

La première étape consiste à envoyer à la machine cible le logiciel serveur. Étant donné la nuisance que peut occasionner un cheval de Troie, l'utilisateur cible ne va pas de son plein gré exécuté le programme s'il sait de quoi il s'agit. Aussi, le cheval de Troie en lui-même va être présenté comme différent, un logiciel pour casser les mots de passe ou un antivirus par exemple, et lorsque l'utilisateur se plaindra que le programme ne fonctionne pas, la personne va s'en étonner en expliquant pour elle le logiciel ne présente pas de problème. Ainsi, ce déroule souvent une infection, à la suite d'un dialogue sur ICQ, IRC ou tout autre espace de chat.

Autre méthode, plus subversive, existe, elle consiste à introduire le troyen directement dans un logiciel, aussi divers soit-il, puis de le faire parvenir à la personne visée, dès lors tout programme peut être infecté ! De plus, selon la personne visée, ses intérêts, sa vigilance, le mode d'infection peut être personnalisé.

Après l'infection, il faut attendre l'exécution du programme. Dans ce cas deux solutions, soit le cheval de Troie a été exécuté seul, alors un message d'erreur s'affiche, soit le troyen incorporé dans un autre logiciel, s'exécute sans changer le comportement du logiciel.

La partie active du programme (soit le troyen en lui-même, soit la partie nocive d'un logiciel) va se renommer, prend un nom qui ne soit pas suspect (qui change avec le cheval de Troie) et se place dans un dossier généralement peu fréquenté (du type C:\windows, ou C:\windows\system, où il existe un grand nombre de fichiers dont l'utilité est parfaitement inconnue.). De plus, le troyen va généralement écrire dans la base de registre pour pouvoir s'exécuter à chaque lancement de l'ordinateur.

A la suite de ces opérations, le cheval de Troie est actif et prêt à être utilisé, suivant la méthode utilisée par le troyen, celui-ci va attendre qu'il détecte la possibilité de se connecter à un serveur sur Internet ou alors que le pirate tente de se connecter à la machine. La technique est toujours la même, après une requête du pirate, le programme ouvre un port, qui permet par la suite toute communication entre les deux logiciels (serveur et client), de telle sorte que le pirate peut accéder à tous les fichiers de la personne infectées.

Dès lors, le pirate peut réaliser de très nombreuses choses sur l'ordinateur distant. Lorsqu'une liaison est établie entre le serveur (la personne "infecté") et le pirate de nombreux renseignements peuvent être récupérés :

- Nom du DNS
- L'adresse IP (cependant celle-ci doit généralement être connue auparavant)
- La présence d'un firewall qui pourrait empêcher la connexion du pirate
- La présence d'un proxy
- De nombreuses information sur les interfaces (type, vitesse, etc.)
- Les caractéristiques de l'ordinateur (processeur, mémoire, disque dur...)
- Les navigateurs installés (Internet Explorer, Netscape)
- Les logiciels de messagerie (Outlook, Eudora, etc.)
- Programmes enregistrés
- Nom réel d'utilisateur
- Nom d'utilisateur
- Adresse E-Mail

Les logiciels pour lutter contre les troyens
Les antivirus récents sont capables d'éliminer la plupart des troyens, en particulier InoculateIT qui possède grâce à sa mise à jour régulière un taux de reconnaissance important. Mais il existe également des logiciels spécifiques, l'un des programmes les plus performants est The Cleaner 2.0. Ce shareware vérifie s'il n'y a pas de troyen en mémoire, puis scanne le disque dur.

Pour ceux qui ne comprennent pas l'anglais un petit logiciel sympathique et gratuit : Bouffetroyen, très performant également. Ce programme recherche en mémoire divers genres de troyens, de type serveur FTP, Socket de Troie et DMSETUP. Puis il scanne le disque dur et supprime les troyens trouvés et nettoie la base de registre et les fichiers .ini qui peuvent aussi être infecté.

Voici également quelques logiciels de protection contre des troyens spécifiques :

- Antigen
- BoDetect contre Back Orifice, le troyen le plus répandu.
- NoBackO
- Dmcleanup qui lutte contre DMSETUP
- Netbuster
- Wolfysoft Notroyen
- Antisocket25

Mais le problème de tous ces logiciels est qu'il existe un temps de latence entre le moment de la sortie d'un nouveau troyen et la mise à jour des logiciels qui luttent contre, c'est une éternel course contre la montre. Pour cela, comme pour les virus (dont les troyens possèdent certaines fonctions) il faut être vigilants sur les programmes téléchargés, mettre son antivirus à jour régulièrement (tous les 15 jours semblent être un bon compromis).

Ainsi, si on possède de bonnes notions en informatique et qu'on détecte des anomalies, la meilleure méthode consiste à vérifier soi-même son système, ce qui n'ai pas très difficile, suivez les instructions.

Pour enlever la plupart (99 % selon certains) des troyens, il faut se rendre dans la base de registre, qui stocke de nombreuse informations sur le système. Pour cela, cliquer sur "Démarrer", puis "Exécuter", taper alors "regedit" (sans les guillemets) et valider (cliquer sur OK). Il s'ouvre alors une fenêtre, c'est la base de registre (bdr en abrégé). Alors à l'aide de la partie de gauche et des dossiers qui s'ouvrent, il faut aller dans :
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Il y a dans ce répertoire plusieurs dossiers commençant par Run, il faut alors examiner attentivement les clés (dans la partie de droite) en particulier les "données" qui correspondent à l'adresse des programmes exécutés par windows au démarrage. S'il y a des fichiers suspects (par exemple un fichier keyhook.dll ou encore C:\windows\system\.exe qui correspondent à des troyens) il faut supprimer les clés.
Après cela et un redémarrage, il faut supprimer les fichiers qui avaient été détectés comme suspect et voilà le cheval de Troie est supprimé normalement, il faut cependant faire attention à ne pas l'exécuter à nouveau...

Un bon moyen de se protéger contre les troyens et en général de protéger son ordinateur ou un réseau local, est d'installé un firewall qui bloquera les tentatives d'intrusions, pour cela allez voir la rubrique sur les firewalls.

11. Le phishing

Qu'est-ce que le phishing?
Le phishing (en français "hameçonnage") est une technique de fraude mélangeant spamming (envoi en masse de messages à des adresses électroniques collectées illégalement ou composées automatiquement) et ingénierie sociale (usurpation d'identité) dans le but de subtiliser des informations sensibles aux victimes (identité complète, numéro de carte bancaire, identifiants d'accès à un site Internet, etc.). Au lieu de tenter de piéger une après l'autre des personnes choisies pour leur naïveté ou leur vulnérabilité, l'escroc contacte simultanément plusieurs milliers voire dizaines de milliers de victimes potentielles en tentant de se faire passer pour leur banque ou n'importe quel autre organisme ou site Internet, comptant sur ce grand nombre pour trouver des destinataires crédules ou imprudents.

Une attaque par phishing se présente souvent en deux temps : l'internaute reçoit en général un message de sa banque ou d'une autre société (voir deux exemples visant la banque LCL et le site eBay) qui l'informe d'un problème de sécurité ou d'une autre action nécessitant qu'il se rende sur le site concerné et qui l'invite pour cela à cliquer sur un lien hypertexte. Or ce dernier ne conduit pas au site officiel mais vers une imitation souvent identique à l'original contrôlée par un individu malveillant, aussi si l'internaute clique sur le lien et saisit des informations elles seront transmises directement à l'escroc. D'autres variantes existent cependant, comme un formulaire à remplir intégrer dans le message ou une demande de réponse par retour du courriel (voir exemple visant Windows Live).

D'où vient le terme "phishing"?
Le mot "phishing" proviendrait de la contraction des mots "phreaking" (piratage des lignes téléphoniques) et "fishing" (pêche). En d'autres termes, le phishing est une sorte de pêche aux victimes via les réseaux de communication.

Que faire en cas de phishing?
Si vous n'avez pas fourni les informations demandées dans le message frauduleux, il n'y a rien à faire de particulier à part supprimer le message concerné. Si par contre vous avez été abusé et avez communiqué ces renseignements à l'auteur du phishing, connectez-vous immédiatement au véritable site de la société dont l'identité a été usurpée en saisissant manuellement son adresse dans votre navigateur, puis changez votre mot de passe afin d'empêcher le détournement de votre compte. En fonction des informations transmises, il peut être nécessaire d'entreprendre d'autres actions, notamment faire opposition si vous avez communiqué votre numéro de carte bancaire.

Les logiciels antiphishing sont-ils efficaces?
Les fonctions ou logiciels antiphishing se proposant d'alerter l'utilisateur lorsqu'il accède à une imitation d'un site officiel utilisée dans le cadre d'une attaque par phishing peuvent être utiles mais ne sont en aucun cas suffisants car il arrive trop fréquemment qu'un site douteux ne soit pas détecté. La meilleure protection est encore l'utilisateur et le respect d'un conseil simple : il ne faut ne jamais cliquer sur les liens hypertextes contenus dans un message non sollicité demandant au destinataire de fournir des données sensibles ou confidentielles, même s'il semble provenir d'un expéditeur connu. En cas de doute, préférez vérifier la réalité de la demande par téléphone auprès de la société concernée ou vous rendre sur le site de cette société en saisissant manuellement son adresse dans votre navigateur, afin de ne pas risquer de cliquer sur un lien piégé ou conduisant vers une page web piégée.

12. Le cheval de Troie et bombe logique

À l'inverse des virus, les chevaux de Troie et autres bombes logiques n'ont pas la capacité de se reproduire. pour autant, ils s'avèrent des armes redoutables. Tapis entre les lignes de code d'un programme, ils attendent que vous double-cliquiez sur l'icône du programme qui les héberge pour devenir les maîtres de votre PC.

Définition :
Le cheval de Troie (également appelé troyen ou trojan) et la Bombe logique sont des programmes informatiques qui contiennent des fonctions cachées pouvant s'exécuter en toile de fond à l'insu de l'utilisateur. Dans le cheval de Troie, la fonction cachée est exécutée immédiatement, alors que dans la bombe logique, elle se déclenche à un instant défini.

Caractéristiques
Les bombes logiques et les chevaux de Troie sont des programmes simples. Ils n'ont pas la capacité de se reproduire comme le font les virus et les vers et ils ne peuvent donc pas se propager par eux-mêmes. Mais, à l'inverse, un virus peut agir comme un cheval de Troie ou une bombe logique !

Cheval de Troie
Pour gagner une machine, ces petits programmes doivent être installés à partir d'un support physique ou par téléchargement. A l'image de la légende homérique relatant comment les Grecs ont provoqué la destruction de la ville de Troie après s'être cachés dans un cheval en bois, ils se dissimulent avant d'agir. Les chevaux de Troie ou Trojans se nichent ainsi à l'intérieur de programmes gratuits ou commerciaux qui semblent anodins aux yeux de l'utilisateur : patchs ou mises à jour, utilitaires, logiciels de jeux, etc. La bombe logique est également soigneusement dissimulée au sein du système d'exploitation ou d'un logiciel quelconque. Une fois ledit programme exécuté, ils sont prêts à effectuer la tâche plus ou moins nuisibles pour laquelle ils ont été programmés.

Bombe logique
Mais à la différence du cheval de Troie qui est immédiatement opérationnel au lancement du logiciel hôte, la bombe logique attend le moment opportun pour se déclencher. Cet évènement, déterminé par le programmeur malveillant, peut être une date particulière, une combinaison de touches, une action spécifique ou un ensemble de conditions précises. Ainsi, un employé mal intentionné peut implanter une bombe logique chargée de vérifier si son nom disparaît sur les listes, la bombe logique se déclenche et détruit les données de la société.

Conséquences
Que leurs effets soient différés ou immédiats, ces programmes simples ont des fonctions diverses. Ils ont la capacité, par exemple, d'afficher une boîte de dialogue, de détruire des fichiers, de copier des données confidentielles ou des mots de passe. L'action la plus pernicieuse reste toutefois la prise de contrôle à distance de l'ordinateur. Une fonction tellement répandue qu'elle est désormais associée au cheval de Troie. Ce type de Trojan peut ouvrir un port de l'ordinateur à la communication ou profiter d'une faille de sécurité sans que l'utilisateur s'en aperçoive. Une fois installé, le Trojan agit comme l'élément serveur d'un logiciel de prise en main à distance classique. Ensuite, tout est possible pour l'utilisateur distant : lire et écrire des données, transférer des fichiers, prendre le contrôle de la souris et du clavier, etc. Mais le pirate doit toutefois connaître l'adresse IP de la machine ciblée avant de pouvoir agir.

Le plus célèbre de ces Trojans est une application client/serveur développée en 1998 par le CdC (The Cult of the dead Cow), un groupe de hackers très actif. Baptisée "Back Orifice" en référence à la suite logicielle de Microsoft "Back Office", cette application a été développée pour mettre en évidence les failles de sécurité de Windows. Utilisé à bon escient, "Back Orifice" est un puissant outil d'administration à distance mais il peut également être utilisé par les pirates en étant intégré dans un autre logiciel ou en étant renommé pour laisser croire que c'est un programme inoffensif.

13. Les hoax

Définition d'un hoax
Un hoax est une information fausse, périmée ou invérifiable propagée spontanément par les internautes. Les hoax peuvent concerner tout sujet susceptible de déclencher une émotion positive ou négative chez l'utilisateur : alerte virus, disparition d'enfant, promesse de bonheur, pétition, etc. Ils existent avant tout sous forme écrite (courrier électronique, message dans un forum, etc.) et contrairement aux rumeurs hors ligne incitent le plus souvent explicitement l'internaute à faire suivre la nouvelle à tous ses contacts, d'où une rapide réaction en chaîne.

Hoax, rumeur, spam et canular
Le terme "hoax" signifie en anglais "canular", mais cette seule traduction ne convient pas vraiment pour désigner les hoax circulant sur Internet :

- contrairement au canular, qui est une blague ou une farce dont la victime peut elle-même rire ou sourire une fois que la vérité lui est révélée, dans le cas d'un hoax la victime n'est jamais informée de la supercherie. De plus, certains hoax poussent les internautes à accomplir des actions dangereuses pour l'intégrité ou la sécurité de leur ordinateur, ce qui n'a plus rien d'humoristique ;
- contrairement au spam, qui est un message créé délibérément puis envoyé par un individu unique dans le but d'exposer un grand nombre de personnes à son contenu indésirable, généralement publicitaire ou promotionnel, un hoax peut avoir été créé par accident, peut concerner n'importe quel sujet et surtout est propagé par les internautes eux-mêmes, en général sans intention malveillante puisque eux-mêmes victimes ;
- contrairement à la rumeur, qui est une nouvelle officieuse vraie ou fausse qui se répand dans le public, un hoax est toujours une information fausse ou invérifiable, et même dans ce cas le plus souvent intuitivement perçue comme douteuse, excessive ou erronée.

Si comme les spams les hoax peuvent toucher un grand nombre d'internautes, ils sont surtout un hybride de canular et de rumeur : du premier ils tirent leur faculté à tromper l'internaute en suscitant chez lui une vive émotion (peur, compassion, révolte, espoir, etc.) et de la seconde leur capacité à se propager spontanément au sein de la communauté. C'est pourquoi le terme hoax reste encore le plus approprié pour désigner les "cyber-rumeurs" ou "canulars du web".

14. Règles générales de protection

Pas besoin d'être un expert pour bien protéger son ordinateur. Quelques astuces très simples, des logiciels parfois gratuits et un peu de bon sens suffisent le plus souvent à laisser les pirates dehors.

Les pirates sont rarement très doués. Ils préfèrent les proies faciles aux défis technologiques. Et on les comprend: internet regorge d'ordinateurs personnels ouverts aux quatre vents dont ils peuvent prendre le contrôle à distance en quelques minutes. Il suffit de peu de choses pour changer de camp... et ne plus être importuné.
La prévention paie toujours.

Quelques règles simples peuvent être appliquées :

- Gardez votre PC à jour : S'il ne devait y avoir qu'un conseil, ce serait celui-là : appliquez les correctifs ! La quasi-totalité des incidents, et notamment les dernières grandes épidémies de vers qui ont circulé sur l'internet, utilisent une faille de sécurité connue pour laquelle existe déjà une rustine. Pour les ordinateurs équipés de Windows, la solution la plus simple pour rester à jour est d'activer le service de mise à jour, Windows Update, depuis le Menu Démarrer ou se connecter directement sur le site consacré. Attention, ce dernier ne corrige que le système d'exploitation et les applications de Microsoft : pensez à vous tenir au courant des correctifs disponibles pour vos autres logiciels! Malheureusement, il n'y pas de système de mise à jour centralisé. Certains programmes disposent néanmoins de leur propre fonction de mise à jour automatique, qu'il convient d'activer spécifiquement.

- Choisissez de bons outils de navigation : Les navigateurs "alternatifs" sont moins sujets aux attaques. Bien qu'Internet Explorer soit un navigateur tout à fait correct, s'il est tenu à jour, n'hésitez pas à essayer des alternatives réputées plus sûres telles Google Chrome, Firefox ou Opera. L'avantage de ces applications réside dans le fait qu'elles n'exploitent pas, par exemple, la technologie ActiveX propre à Microsoft et largement détournée par les pirates pour piéger des pages web. Et elles sont historiquement moins sujettes à des failles de sécurité à répétition.

- Installez un pare-feu : En utilisant un pare-feu lorsque vous êtes en réseau, vous isolez votre PC du monde extérieur. Il agit tel un garde-barrière et contrôle les tentatives de connexions à votre ordinateur. Certains d'entre eux permettent aussi de décider quelles applications installées sur votre disque dur ont le droit de se connecter à l'internet. Depuis Windows 2000, toutes les moutures du système de Microsoft disposent d'un pare-feu intégré qu'il suffit d'activer. Ceux de Windows 2000 et Windows XP SP1 ne font que contrôler les connexions entrantes, tandis que le SP2 de Windows XP et Vista offrent un programme plus complet. Dans tous les cas, vous pouvez l'activer en allant dans menu "propriété" de la connexion réseau (internet ou réseau local) que vous souhaitez protéger. Pour aller plus loin, vous pouvez installer à la place du pare-feu du système un autre comme ZoneAlarm ou Norton Firewall... Ces produits offrent une plus grande souplesse de configuration, des interfaces plus agréables à utiliser et permettent de contrôler les applications qui peuvent se connecter à l'internet.

- Installez un antivirus : Personne n'est à l'abri d'une erreur : même si vous êtes sûr de vous et ne cliquez pas sur n'importe quoi, installer un antivirus reste une bonne idée. Des codes malicieux peuvent se cacher dans les pages des sites web que vous visitez ou dans les documents Office que vous ouvrez, et les petits programmes amusants que vous recevez de vos amis peuvent contenir des chevaux de Troie. L'antivirus est là pour les déloger.

  !!! Pensez à mettre votre antivirus à jour !!!

  Choisissez-le capable non seulement d'analyser vos fichiers, mais aussi de fonctionner avec votre logiciel de courrier électronique afin d'intercepter les courriers avant qu'ils ne soient visibles dans la liste des messages. De même, si vous pratiquez la discussion sur des messageries instantanées telles MSN Messenger ou Yahoo! Messenger, préférez un antivirus qui soit également capable de contrôler les fichiers reçus par ce canal.

Et bien sûr, une fois l'antivirus installé, pensez à activer la mise à jour automatique de sa base de signatures ! Si vous possédez une connexion haut-débit (Fibre, xDSL, câble…), vous pouvez opter pour une mise à jour quotidienne, vous ne la verrez pas passer.

- Installez un antispyware :
  "Spywares" et "adwares" ne sont pas que les deux derniers mots à la mode : ce sont surtout les deux nuisances parmi les plus répandues. Les adwares sont des logiciels clandestins installés en même temps que des applications (souvent gratuites) que vous téléchargez sur l'internet, voire des sites web que vous visitez si votre navigateur n'est pas à jour de ses correctifs de sécurité. Leur rôle peut être d'afficher de la publicité additionnelle durant sessions de surf ou d'étudier vos habitudes de consommation. Leur objectif est alors de renseigner les sociétés de marketing qui les installent.
  Les spywares, quant à eux, sont clairement malicieux : ce sont des logiciels espions dont le rôle est de collecter des données confidentielles sur votre ordinateur et les transmettre aux pirates qui les ont installés. Eux aussi peuvent être contractés via des pages web malicieuses ou des utilitaires imprudemment téléchargés.
  Pour s'en débarrasser, ne comptez pas sur votre antivirus : les éditeurs de ces derniers n'ont jamais vraiment pris la peine de lutter pleinement contre ce type de nuisance. Ils commencent tout juste à s'y intéresser. Deux logiciels gratuits s'en chargent de toute façon très bien : Spybot Search & Destroy et Ad-aware de Lavasoft.

- Ne cliquez pas n'importe où ! Bien sûr, il ne vous viendrait pas à l'idée de cliquer sur les multiples pièces jointes exécutables que vous recevez par e-mail. Méfiez-vous des fichiers joints aux messages que vous recevez : analysez avec un antivirus à jour tout fichier avant de l'ouvrir, et préférez détruire un mail douteux plutôt que d'infecter votre machine, même si l'expéditeur est connu. Mais le danger ne réside pas seulement dans les programmes : les liens que vous recevez dans un message, par exemple, peuvent être déguisés pour vous mener vers une toute autre destination que celle affichée. Vous pouvez ainsi penser être dirigé vers le site de téléchargement d'un éditeur connu et vous retrouvez en réalité sur un site pirate qui distribue des versions piégées de l'utilitaire que vous cherchiez. Ou encore croyant accéder au site de votre banque en ligne, communiquer en fait avec une copie de celui-ci. Pour éviter ce piège, avant d'aller vers un site sensible dont on vous propose le lien, pensez à faire un copier-coller de l'adresse telle qu'elle s'affiche, et de l'ouvrir dans une nouvelle fenêtre de votre navigateur. Vous serez certain d'arriver à bon port !

- N'exécutez pas n'importe quoi !
  Ne téléchargez pas des programmes d'origine douteuse, qui peuvent vous être proposés sur des sites persos ou des chats eux-mêmes plus ou moins douteux.
  Il n'y a pas que les programmes "traditionnels" qui puissent être activés et causer des dégâts à votre système! Les auteurs de virus utilisent souvent d'autres types de fichiers pour diffuser leurs parasites. C'est le cas par exemple des économiseurs d'écran (fichiers .scr), des raccourcis de programmes DOS (.pif), des scripts (.vbs, .wsh...) et même des fichiers de commandes de Windows (.bat) par exemple. Soyez vigilant avant de cliquer sur un fichier à l'extension exotique !

- Testez votre sécurité : Plusieurs services en ligne, souvent gratuits, vous permettent de savoir rapidement si votre ordinateur est accessible depuis l'internet. Ils testent en réalité votre pare-feu en essayant de déterminer les ports ouverts sur votre PC. Certains vont plus loin et tentent de repérer d'éventuels chevaux de Troie qui seraient déjà installés sur votre système (Symantec Security Check par exemple). De nombreux éditeurs d'antivirus proposent également une analyse gratuite de votre disque dur directement depuis le réseau mondial. Vous en trouverez la liste sur le site http://www.inoculer.com. Enfin, des services payants ou gratuits permettent de détecter, toujours depuis le net, d'éventuelles failles avant que les pirates ne les exploitent. N'hésitez à abuser de ces services tout au long de l'année : la sécurité est un processus qui doit être contrôlé dans la durée !

- Fuyez les disquettes, CD, clés USB et autres supports d'origine douteuse (ou ayant transité dans des lieux publics vulnérables comme les salles de cours ou TP des écoles ou universités), et protégez-les vôtres en écriture;

- Créez dès maintenant, si ce n'est pas déjà fait, une CD de boot contenant un antivirus (la plupart des antivirus le proposent) pour une désinfection d'urgence;

- Procédez régulièrement à des sauvegardes du contenu important de votre disque dur après avoir vérifié l'absence de virus : cela peut paraître fastidieux, mais en cas d'infection (ou même simplement en cas de crash de disque dur), ça vous sauvera la mise...

- Un internaute averti en vaut deux ! Tenez-vous au courant des apparitions de nouveaux virus. Plusieurs sites vous offrent ce service en émettant des alertes lorsqu'un virus connaît une diffusion importante, sur les escroqueries du moment ainsi que sur les failles de sécurité non corrigées. Les informations (nom du virus, mode de transmission connu, etc.) sont alors consultables sur le site internet. Connaître l'existence du virus, c'est déjà le tuer à moitié... Tenez-vous informé.

En complément de ces règles de prévention, la meilleure protection - et le principal remède en cas de contamination - consiste à installer un antivirus (certains sont gratuits). Une solution qui reste toute relative, car aucun produit ne détecte 100% des virus, 100% du temps : d'où l'importance de la prévention. Par ailleurs, de nouveaux virus apparaissant chaque jour, il faut veiller à régulièrement actualiser les bases de données virales du logiciel : la plupart des éditeurs proposent une mise à jour au minimum mensuelle, mais pas toujours gratuite...

Et n'oubliez pas :

On réfléchit puis on clique et pas l'inverse
Les fichiers/programmes c'est comme les bonbons, quand ça vient d'un inconnu, on n'accepte pas !

15. Faut-il arrêter d'acheter un antivirus ?

Sources : Mark Hachman, PCWorld

Dans le domaine des antivirus, il y a toujours eu la dichotomie entre les solutions gratuites et payantes. Avec Defender (aujourd'hui Windows Security), Microsoft a changé la donne et l'alternative gratuite et intégrée rivalise avec les offres payantes.

Il n'est plus nécessaire de payer pour un logiciel antivirus. Le service gratuit Windows Defender de Microsoft, intégré à Windows 10, protège désormais aussi bien que les solutions antivirus/antimalwares payantes auxquels certains sont peut-être abonnés depuis plusieurs années. Il y a deux raisons pour lesquelles les utilisateurs de PC ont accepté de payer pour un logiciel antivirus : d'abord, les bonnes alternatives gratuites étaient rares ; ensuite, la protection offerte par Windows était plus que minimale, laissant le champ libre à des éditeurs comme Norton, Kaspersky et d'autres fournisseurs. En fait, les capacités de protection contre les malwares, offertes par Windows étaient si mauvaises que des organismes de test comme AV-comparatives.org et AV-test.org ont utilisé Defender comme base référence des plus mauvais résultats dans leurs évaluations de produits antivirus. Ainsi, lorsqu'en décembre 2013, AV-test.org a testé la capacité de 23 fournisseurs d'antivirus à bloquer des échantillons de vrais malwares sous Windows 8.1, Defender est arrivé dernier.

Mais ce temps est révolu. Depuis, Microsoft a pris la sécurité des terminaux à bras le corps. En 2019, Windows Defender Antivirus (connu aujourd'hui sous l'appellation Windows Security incluant un pare-feu et d'autres outils), intégré directement et gratuitement à Windows 10, surpasse souvent les services payants. Même s'il reste des imperfections. Par exemple, la génération de « faux positifs », quand la solution confond les applications légitimes avec des logiciels malveillants, peut être élevée. Un autre test a montré aussi que le service intégré avait un impact plus important sur la performance des PC bas de gamme. Il revient donc à chaque utilisateur de décider si ces inconvénients sont supportables ou s'il préfère payer plus de 60 euros/an pour un antivirus plus performant et plus efficace. Nos confrères de PC World testent régulièrement les applications antivirus et certaines fonctionnalités peuvent justifier le choix d'une solution payante. Mais, à quel niveau se situe aujourd'hui Windows Defender par rapport à ces solutions payantes et dans quelle mesure peut-il devenir son antivirus principal ?

Des comparatifs sans équivoque

Deux laboratoires de tests AV-comparatives et AV-test classent Defender presqu'en tête de leurs produits antivirus. Il est important de noter que ces tests sont très longs à réaliser. Même des sites comme AV-comparatives s'appuient sur des tests automatisés pour parcourir le Web à la recherche de sites et d'URL malveillants afin de reproduire les situations auxquelles tout utilisateur peut être confronté au quotidien. Dans le test d'AV-comparatives, la solution Windows Defender faisait partie des quatre solutions, sur un total de seize, ayant réussi à bloquer tous les malwares et à les empêcher de prendre le contrôle de ses systèmes de test. Par contre, des PC protégés par les solutions de grands éditeurs spécialisés comme McAfee et Symantec ont fini par être compromis par des malwares. À noter que ces derniers et les mécanismes de protection évoluent constamment. Pour donner une idée du niveau « moyen » de protection dans le temps, les tests d'AV-comparatives ont été réalisés de février à mai 2019.

Pour être exact, les tests d'AV-Comparatives montrent quand même que Defender souffre de quelques faiblesses. En particulier, ils révèlent trois situations « dépendantes de l'utilisateur » dans lesquelles l'antivirus n'a pas immédiatement identifié le malware et a demandé à l'utilisateur la permission d'installer le fichier. Ce n'est pas la meilleure pratique, car les utilisateurs ont tendance à valider l'installation de logiciels sur leur système. La solution a également généré un nombre exceptionnellement élevé de faux positifs, bloquant 74 applications et services légitimes. D'ailleurs, c'est un test que chacun peut réaliser : comptabiliser combien d'applications légitimes Defender a bloqué sur son système. En juin 2019, AV-test a également classé Windows Defender comme l'un des meilleurs produits antivirus qu'il a évalué. Il a bloqué tous les malwares envoyés lors des tests, y compris tous les échantillons « zero-day » qui reproduisaient des situations réelles, avec zéro faux positif. Defender a obtenu la plus haute note de 6 sur 6 des produits testés. La solution avait déjà obtenu ou presque obtenu ce score lors des tests d'avril, février, décembre 2018 et octobre 2018 réalisés par AV-test.

Cette protection contre les attaques zero-day est importante, car historiquement, c'était l'une de ses grandes faiblesses : il n'était pas capable de réagir assez rapidement et assez efficacement aux attaques critiques. Les succès répétés de Defender dans les tests tiers prouvent que Microsoft a surmonté cet obstacle. AV-test a également classé Defender au-dessus de la moyenne de l'industrie en terme de performance, notamment pour l'installation d'applications et la copie de fichiers. Il y a donc eu une amélioration significative par rapport au test réalisé en avril par AV-comparatives, où Defender avait enregistré de mauvais résultats dans ces mêmes évaluations. Le SELabs britannique, autre pourvoyeur reconnu de tests antimalwares, a également classé le service Microsoft en tête de sa liste de solutions. Le rapport (disponible uniquement sous forme de fichier PDF téléchargeable) accorde à Defender un taux d'exactitude de 100 %. Ainsi, dans les tests réalisés par ces trois meilleures agences de tests antivirus, Defender a obtenu trois points sur trois.

Les multiples résultats des tests montrent que l'offre de Microsoft est suffisamment efficace pour protéger un PC contre les virus et les logiciels malveillants. Bien sûr, il va de soi que l'utilisateur doit toujours adopter de bonnes pratiques pour sécuriser sa navigation Internet, par exemple, ne pas cliquer sur des liens et des pièces jointes inconnus, et ne pas errer dans les recoins obscurs du Web. À sujet, on peut rappeler que le service Sandbox (ajouté aux machines Windows 10 Pro dans le cadre de la mise à jour de mai 2019) apporte cette protection supplémentaire au cas où vous voudriez explorer un site ou une application à risque.

Des options anti-malwares tierces bien acceptées

Considéré comme un outil de sécurité intégré, l'ouverture de Defender à d'autres solutions de sécurité a longtemps était décriée. Pour autant, il permet d'installer une couche de protection supplémentaire contre les malwares. En raison de conflits potentiels, l'exécution simultanée de deux programmes antivirus a toujours été déconseillée. Or, Windows 10 accepte le programme antimalware de son choix et laisse Defender vérifier périodiquement les menaces. (Aller dans Paramètres > Mise à jour et sécurité > Sécurité Windows, puis cliquer sur Protection contre les virus et les menaces. Défiler vers le bas jusqu'aux options de Windows Defender Antivirus et vérifier que l'analyse périodique est activée.)

Les options antivirus gratuits ne manquent pas, d'AVG à Avast en passant par Avira et bien d'autres. L'option gratuite de BitDefender Internet Security est très efficace et très discrète au point qu'on finit vite par l'oublier, un point vraiment important pour un programme antivirus. Selon AV-test et AV-comparatives, BitDefender est également l'un des meilleurs produits de sa catégorie, même si ce classement concerne dans les deux cas les versions payantes. D'après nos confrères de PCWorld, il n'y a pas de différence entre la version payante et la version gratuite en termes de protection anti-malware. Encore une fois, ils estiment que, pour un usage courant, Windows Defender est suffisant pour se protéger contre les malwares, surtout qu'il permet aussi de dédoubler cette capacité en laissant tourner un second antivirus sur la machine.

Un produit antivirus payant, pour qui ?

Des éditeurs reconnus comme McAfee, Symantec et d'autres ont enrichi les fonctionnalités de leurs produits antivirus/antimalwares en ajoutant du VPN, des coffres-forts de mots de passe et autres services de sécurité. L'accès à ces services supplémentaires, groupés dans un seul package, peut justifier le choix d'une solution antivirus et antimalware payante. Les produits de ces éditeurs ne se limitent plus aux protections traditionnelles. Ils se sont enrichis de services connexes comme les VPN, la surveillance et la protection des dépenses par carte de crédit, des coffres-forts en ligne pour stocker des mots de passe et autres documents sensibles. Si l'objectif de certains attaquants se limite juste à faire crasher votre système, il ne faut pas oublier les attaques par ransomware - le malware crypte le PC et les pirates demandent le paiement d'une rançon pour livrer la clef de déchiffrement - représentent une source importante de revenus pour les pirates. Malwarebytes et BitDefender, entre autres, ont tous deux développé des solutions anti-ransomwares alternatives gratuites. Windows dispose de ses propres protections gratuites pour lutter contre les ransomwares. L'OS permet aussi de verrouiller et de sécuriser des dossiers protégés.

Rien n'est parfait, et personne ne peut dire avec certitude qu'une prochaine attaque ne pourra pas briser les protections de Windows. Mais, de ce point de vue, les services payants sont tout aussi exposés. Chacun peut également déployer sa propre suite de sécurité à la carte, en s'appuyant sur le service antimalware de Windows. L'utilisateur peut par exemple choisir un fournisseur de VPN, s'abonner à LifeLock ou à un service de monitoring des dépenses effectuées par carte de crédit. Google Chrome et d'autres navigateurs peuvent gérer les mots de passe ou permettent de choisir de bons gestionnaires de mots de passe via leurs modules. L'avantage des suites antimalwares payantes, c'est qu'elles s'appuient sur des services approuvés, regroupés dans un pack soigné et facile à gérer. Elles apportent par conséquent une certaine tranquillité d'esprit. Mais tout cela a un coût annuel récurrent. Vous pouvez, si cela vous convient, continuer à payer pour ce genre de services.

16. Les WEB

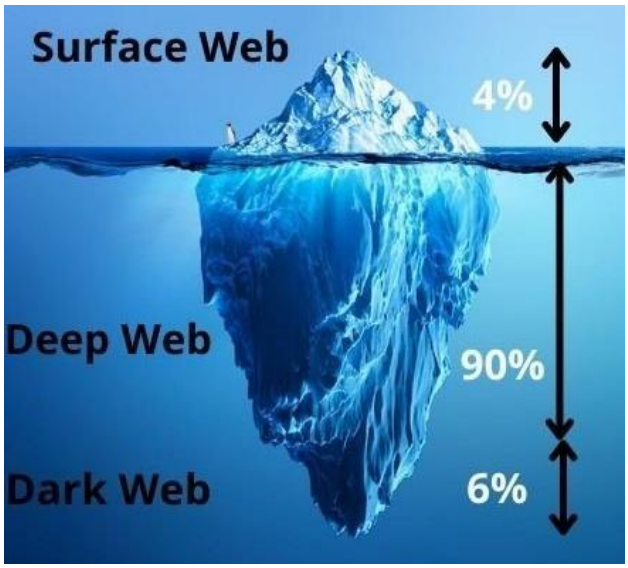
Le clearweb
Le clear web correspond à toutes les pages indexées par les moteurs de recherche classiques, du type Google, Bing ou encore Baidu. Il englobe donc aussi bien Wikipedia et YouTube que les blogs, les sites d'e-commerce, les sites d'information, les sites vitrines, les sites personnels… Il représente seulement 4% de la totalité d'internet.

Le deepweb
Le deepweb, ou « web profond », parfois même « web invisible », est souvent défini comme le web accessible mais non indexé par les moteurs de recherche. L'exemple le plus simple est celui d'un site web bancaire. Ce dernier possède une partie publique, référencée par les moteurs de recherche, et une privée, qui concerne les informations bancaires du client et se situe derrière un mécanisme d'authentification. La deuxième est accessible au client mais pas au moteur de recherche. On y retrouve par exemple, les forums, les sites médicaux, certaines parties de site internet… Cette part représente 90% de la totalité d'internet.

Les darknets
Un darknet, puisqu'il en existe plusieurs, est un réseau qui pourrait être qualifié de parallèle et qui ne serait accessible qu'à l'aide d'outils spécifiques. Les plus connus sont Tor, i2p et Freenet, mais il en existe beaucoup d'autres. Ces réseaux sont dits « superposés » car ils reposent sur un autre pour fonctionner, internet en l'occurrence. Pas d'internet, pas de darknet.

Le darkweb
Le darkweb, ou « web clandestin », serait le web non indexé et non accessible par des moyens standard. Le terme « darkweb » est aussi généralement utilisé pour désigner le web criminel au sens large, indépendamment de son indexation ou de son accessibilité. Dans l'imaginaire collectif, le darkweb regroupe donc ces deux définitions, c'est-à-dire à la fois les sites dédiés aux activités criminelles et les sites utilisant le réseau Tor, qu'ils soient dédiés au cybercrime ou non.

Sur les forums cybercriminels, les notions de deepweb et de darkweb sont souvent utilisées l'une pour l'autre indifféremment sans que cela ne pose de problème. Pour décrire la différence entre ces deux concepts, l'image d'un iceberg avec au sommet le web surfacique (le web « classique ») et, sous l'eau, le deepweb puis le darkweb fait référence. Il faut être prudent avec cette illustration car elle est imparfaite : elle suppose une forme de hiérarchie ou de gradation entre les concepts qui ne correspond pas à la réalité. De nombreux experts considèrent d'ailleurs que le darkweb en tant que tel n'existe pas et qu'il ne s'agit en fait que d'une fraction du web. Il n'y a donc pas lieu de le traiter différemment. Cette part représente 6% de la totalité d'internet.



Un réseau pas si inaccessible

Qu'il s'agisse du darkweb, du darknet ou du deepweb, ces réseaux sont tous réputés pour leur difficulté d'accès. Celle-ci est à relativiser : il existe des solutions techniques comme les passerelles (onion.link, onion.cab ou encore onion.to par exemple) qui permettent d'y accéder sans modification du navigateur. Grâce à elles, Google indexe des sites qui ne devraient être accessibles que par Tor. Il faut savoir qu'elles sont également utilisées par des programmes malveillants pour communiquer avec leur serveur de Command and Control (un serveur centralisé qui envoie des commandes et qui reçoit en retour des informations des postes compromis) sans avoir à modifier la configuration du navigateur de la victime.

Par ailleurs, il convient de rappeler que le darkweb n'a pas l'exclusivité du cybercrime : les cybercriminels n'ont bien évidemment pas attendu l'arrivée de Tor pour se livrer à leurs activités. En fonction de leurs spécialités, ces derniers peuvent même utiliser des plateformes tout à fait ouvertes et grand-public comme des groupes Facebook ou des comptes Twitter. Ces réseaux sociaux ferment d'ailleurs régulièrement des groupes destinés aux cybercriminels.

Autre remarque, le darkweb n'est pas que dark. L'usage de Tor n'est pas réservé aux cybercriminels et il existe de nombreux usages tout à fait légitimes de ce réseau. Que ce soit pour échapper à la censure ou pour aider les lanceurs d'alerte, le réseau Tor offre de nombreuses possibilités. Celui-ci n'est donc pas intrinsèquement malveillant, il s'agit en réalité d'un outil. Seule la manière dont il va être utilisé peut-être malveillante. Le réseau social Facebook dispose par exemple d'une version officielle en .onion.

17. Glossaire

Adresse IP :
Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP (Internet Protocol), composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Ces numéros servent aux ordinateurs du réseau pour se reconnaître, ainsi chaque ordinateur du réseau possède sa propre adresse IP unique.

Par exemple, 194.153.205.26 est une adresse TCP/IP donnée sous une forme technique. Ce sont ces adresses que connaissent les ordinateurs qui communiquent entre eux.

C'est l'IANA (Internet Assigned Numbers Agency) qui est chargée d'attribuer ces numéros.

Le protocole utilisé actuellement est IPv4. Il est en cours de remplacement par le protocole IPv6 (appelé également IPng pour IP new generation). Il est composé de 8 nombres (8 octets) en hexadécimal entre 0 et 65535. La forme de l'Ipv6 : 8000:0000:0000:0000:0123:4567:89AB:CDEF

AdWares :
En français, Publiciel. Ces logiciels s'installent le plus souvent (mais pas toujours) au cœur des navigateurs pour remplacer le moteur de recherche et installer des pseudo-barres de recherches. Ils affichent des fenêtres publicitaires indésirables. Certains adwares transforment le résultat de toutes vos recherches pour n'afficher que des liens sponsorisés. D'autres transforment à la volée le contenu des pages Web pour ajouter leurs propres publicités même sur les pages qui en sont normalement dépourvues. Les Adwares sont en théorie inoffensifs. En pratique, ils affichent des publicités pour des produits parfois illégaux et sont susceptibles de véhiculer des menaces par le biais de bandeaux publicitaires infectés. Certains capturent toutes vos activités Web et tiennent davantage du spyware tant ils communiquent d'information sur votre privée. Surtout, ils risquent d'afficher des images choquantes sur les ordinateurs de vos enfants ! D'une manière générale, les Adwares ruinent votre expérience Web voire votre expérience PC en anéantissant les performances de la machine.

APT :
Advanced Persistant Threats : En français, Menace Permanent Avancée. Désigne un type de menaces très complexes qui visent particulièrement les serveurs des entreprises et qui combinent à la fois différents vecteurs d'attaques et différentes phases pour rester infiltrées le plus longtemps possible sur le réseau sans être détectées.

Bot :
C'est l'une des pires menaces de l'Internet. Les bots sont des programmes malveillants qui une fois infiltrée sur les ordinateurs enrôle votre PC dans un Botnet (réseau de Zombies), autrement dit un réseau virtuel piloté par des cybercriminels. Les bots sont créés pour recevoir des ordres à distance, l'objectif étant d'utiliser les milliers voire les millions de machines infectées comme une force de frappe. Ils sont donc utilisés pour héberger des images pédopornographiques, propager des malwares, diffuser du spam ou porter des attaques contre des serveurs Web. Les ordres sont le plus souvent émis d'un centre de commandes (C&C) mais certains prennent leurs ordres en écoutant Twitter ou en réalisant des recherches spécifiques sur Google.

Bloatware :
(également appelé logiciel mémorivore, inflagiciel, obésiciel ou boufficiel) désigne tantôt un logiciel utilisant une quantité excessive de ressources système, tantôt un logiciel accumulant une quantité importante de fonctionnalités disparates.

Blog :
Site personnel sur Internet rédigé sous forme de carnet intime, généralement rédigé à la première personne. Il peut être mis à jour facilement grâce à des outils fournis par l'hébergeur du blog.

Browser Hijacker :
Désigne spécifiquement les Adwares qui s'incrustent au cœur même des navigateurs pour pister vos activités Web.

Chat : « bavardage », espace de discussion sur Internet dans lequel les participants conversent au moyen d'outils de messagerie instantanée, les réponses étant le plus souvent publiques. (Voir également Messagerie instantanée)

DNS (Domain Name System) :
Chaque ordinateur directement connecté à internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 194.153.205.26 mais avec des noms de machine ou des adresses plus explicites (appelées adresses FQDN) du type http://www.c-prod.fr/.

Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System).
On appelle résolution de noms de domaines (ou résolution d'adresses) la corrélation entre les adresses IP et le nom de domaine associé.

Droppers :
En français, injecteurs. Programme spécialement conçu pour ne pas être détecté par les antivirus les plus populaires et installer à votre insu des malwares.

E-mail :
Abréviation d'Electronic mail ; représente l'adresse de l'internaute sur le réseau et permet de recevoir et d'envoyer des messages en temps réel. Appelé également en français Courriel ou mèl.

FAQ (Frequently Asked Question) :
Questions les plus souvent posées à partir d'un sujet ou d'un groupe de discussion.

Fenêtre Pop-Up :
Petite fenêtre s'ouvrant brutalement en même temps qu'une page Web et contenant généralement un bandeau publicitaire.

Firewall (pare-feu) :
Dispositif matériel et logiciel permettant de limiter fortement les risques d'intrusion dans les systèmes informatiques.

Forum de discussion :
Service sur le Web permettant aux internautes d'envoyer des messages sur des sujets variés. Les échanges y sont moins immédiats que par Messagerie instantanée (chat) et restent affichés en permanence. Les forums peuvent être modérés (c'est-à-dire qu'un modérateur ou un surveillant lit les messages avant de les publier).

FAI (Fournisseur d'Accès à Internet) :
Désigne une entreprise qui commercialise l'accès à Internet ; intermédiaire indispensable entre un particulier et le web. Par exemple : FREE/Iliad, Orange, SFR, Bouygues Télécom…

Intrusion informatique :
Action de s'introduire dans un ordinateur ou un réseau informatique sans y être autorisé. C'est un délit puni par la loi.

Internaute :
Utilisateur d'Internet.

Internet :
Réseau mondial, formé d'une quantité innombrable de réseaux interconnectés, qui permet à des centaines de millions de personnes d'échanger de l'information.

Keyloggers :
En français, enregistreur de frappe. C'est un type particulier de Spywares qui espionne tout ce que vous saisissez au clavier et envoie ces informations aux cybercriminels qui le pilotent. Les Keyloggers sont typiquement utilisés pour dérober les logins et mots de passe ou encore les numéros de comptes bancaires.

Lien Hypertexte :
Textes ou images soulignés dans une page qui permettent de naviguer vers d'autres documents reliés par des liens ; ils proposent un raccourci vers d'autres pages Web.

Logiciel de filtrage :
Logiciel qui limite l'accès des jeunes à Internet. Les logiciels de filtrage peuvent bloquer les sites ou des moyens de communication (chats, forum…). Ils peuvent aussi surveiller les activités des jeunes en ligne et le temps qu'ils y consacrent.

Malware :
Contraction de « malicious » et « software », malware est un terme générique pour désigner tous les exécutables (programmes et codes) malveillants, autrement dit toutes les sales bestioles informatiques présentées dans ce lexique.

Messagerie instantanée :
Logiciel permettant de dialoguer en direct avec un cercle restreint d'amis (MSN..). Appelé également CHAT.

Moteur de recherche :
Outil qui permet de rechercher des sites grâce à des mots-clés. Par exemple : Google, Yahoo…

Navigateur Internet :
Logiciel servant à surfer sur le Web. Par exemple : Internet Explorer, Firefox, Opera, Safari…

Netiquette :
Ensemble des règles comportementales à observer sur Internet.

Nom de domaine :
TLD signifie Top Level Domain : c'est la partie finale (ou extension) du nom de domaine. Il existe des TLD mondiaux (.com, .net, .org, .biz, .info, .name) et des TLD nationaux (un par pays, comme .fr pour la france).
Le nom de domaine à cette forme : c-prod.fr

Peer-to-Peer (P2P):
Système d'échange de fichiers d'ordinateur à ordinateur, sans passer par l'intermédiaire d'un serveur central. Pour que l'échange se fasse, il faut qu'un Internaute mette ses fichiers à disposition et qu'un autre décide de les télécharger.

Phishing :
En français, hameçonnage. Désigne des sites Web factices qui se font passer pour des sites Web légitimes afin de voler vos identifiants. PayPal, eBay, les banques, le site des impôts, les sites de Pôle-Emploi, les sites de La Poste, les sites des FAI, Gmail, Facebook et Twitter sont les principales cibles du Phishing. Mais tout site qui réclame un login/mot de passe est susceptible d'être la cible des « Phishers », ceux qui créent les sites de Phishing. Les informations ainsi récoltées sont soit exploitées directement par les cybercriminels soit revendues en masse sur le « Darknet » (les réseaux de cybercriminels).

Ports :
De nombreux programmes TCP/IP peuvent être exécutés simultanément sur Internet (vous pouvez par exemple ouvrir plusieurs navigateurs simultanément ou bien naviguer sur des pages HTML tout en téléchargeant un fichier par FTP). Chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données.

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits: un port (la combinaison adresse IP + port est alors une adresse unique au monde, elle est appelée socket).

L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau tandis que le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante. S'il s'agit d'une requête à destination de l'application, l'application est appelée application serveur. S'il s'agit d'une réponse, on parle alors d'application cliente.
Il existe des milliers de ports (ceux-ci sont codés sur 16 bits, il y a donc 65536 possibilités), c'est pourquoi une assignation standard a été mise au point par l'IANA (Internet Assigned Numbers Authority), afin d'aider à la configuration des réseaux.

Les ports 0 à 1023 sont les « ports reconnus » ou réservés (« Well Known Ports »). Ils sont, de manière générale, réservés aux processus système (démons) ou aux programmes exécutés par des utilisateurs privilégiés. Un administrateur réseau peut néanmoins lier des services aux ports de son choix.
Les ports 1024 à 49151 sont appelés « ports enregistrés » (« Registered Ports »).
Les ports 49152 à 65535 sont les « ports dynamiques et/ou privés » (« Dynamic and/or Private Ports »).
Voici certains des ports reconnus les plus couramment utilisés :

Port	Service ou Application
21	FTP
23	Telnet
25	SMTP (envoi de courrier)
53	Domain Name System
63	Whois
70	Gopher
80	HTTP (Web)
110	POP3 (réception de courrier)
119	NNTP (Newsgroup)
995	POP3 SSL (réception de courrier sécurisée)

Ainsi, un serveur (un ordinateur que l'on contacte et qui propose des services tels que FTP, Telnet, ...) possède des numéros de port fixes auxquels l'administrateur réseau a associé des services. Ainsi, les ports d'un serveur sont généralement compris entre 0 et 1023 (fourchette de valeurs associées à des services connus).

Du côté du client, le port est choisi aléatoirement parmi ceux disponibles par le système d'exploitation. Ainsi, les ports du client ne seront jamais compris entre 0 et 1023 car cet intervalle de valeurs représente les ports connus.

Ransomwares :
En français, rançongiciel. Plutôt récents, mais véritable fléau du moment, les Ransomwares sont des codes malveillants qui prennent votre PC ou vos données en otage. Dans le premier cas, ils affichent un message à l'écran (parfois en se faisant passer pour la Police, la Gendarmerie ou Hadopi) dès le démarrage du PC et vous demandent de payer une « contravention » pour récupérer l'accès à votre PC. Dans le second cas, une fois installés, ils chiffrent tous vos fichiers et photos personnels qui deviennent alors illisibles. Vous devez alors payer pour obtenir l'outil qui vous permettra de les déchiffrer. Certains Ransomwares sont plus sournois : ils vous font croire que vos fichiers sont endommagés mais qu'en achetant « l'outil spécial de réparation » vous pourrez les récupérer. À noter que les Ransomwares ne se limitent plus aux PC. Ils ont fait, depuis 2015, leur apparition sur mobiles (Android).

Rogues :
Aussi appelés Scareware, les « rogues » sont des logiciels arnaques. Installés à votre insu (le plus souvent après visite d'une page Web infectée ou au travers d'un bandeau publicitaire vous alertant que votre PC est lent ou infecté), ils se font passer pour des antivirus ou des outils d'optimisation. Ces outils sont complètement factices. Ils trouvent toujours des problèmes même sur les PC totalement neufs. Évidemment, pour « réparer » votre ordinateur, vous devez acheter la « version complète ». C'est une simple arnaque pour vous soutirer de l'argent et dans certains cas pour directement dérober vos numéros de carte bancaire avec son code CVC. La version complète est évidemment tout aussi factice que la version « d'essai » installée à votre insu. On trouve de nombreux rogues également sur mobiles (sous Android).

RAT :
Acronyme de Remote Administration Tool. Ce sont des logiciels de prise de contrôle à distance des ordinateurs. Certains peuvent être légitimes, mais lorsqu'ils sont installés à votre insu, ils deviennent de vrais dangers.

Rootkit :
Un rootkit est un malware avancé conçu pour masquer son existence et masquer l'existence des autres malwares qu'il protège. Un rootkit cache ses fichiers et masque son exécution pour ne pas être repérable par les outils classiques. Le plus souvent, les Rootkits masquent également les communications entre votre PC et les cybercriminels qui le contrôlent.

Site :
Lieu virtuel mis à la disposition des internautes par des entreprises ou des particuliers et constitué d'un ensemble de pages reliées entre elles par des liens.

Spam :
Courrier électronique non sollicité envoyé en masse. Ce sont généralement des publicités, mais il peut s'agir également de messages expédiés automatiquement par des virus informatiques.

Spyware :
En français, Logiciels espions ou Espiogiciels. Comme son nom le suggère, les spywares sont des codes malveillants qui ont pour objectif de surveiller votre activité et de collecter toutes sortes d'informations. Ils peuvent capturer ce que vous saisissez, ce qui s'affiche sur votre écran, les clics de souris, les sites visités, les mots saisis sur les moteurs de recherche, votre position géographique, le contenu de vos fichiers personnels. Certains Spywares sont capables d'analyser les photos, de déterminer le taux de peau sur l'image et d'envoyer les photos susceptibles d'être des photos de nus aux cybercriminels (qui les publient alors sur des sites qui les rémunèrent).

Surfer :
Fait d'aller de lien en lien sur Internet.

Télécharger :
Opération qui permet de transférer dans l'ordinateur une information, un programme, un logiciel… disponible sur Internet.

Trojan Horse :
En français, Chevaux de Troie. Inspiré de la mythologie Grecque est un logiciel, le plus souvent furtif, qui ouvre une porte dérobée sur votre ordinateur, le plus souvent soit pour en permettre le contrôle à distance, soit pour faciliter l'installation à votre insu d'autres malwares comme des spywares ou des keyloggers.

Virus :
Programme informatique dont l'objectif est d'infecter les ordinateurs et d'y provoquer éventuellement des dégâts. Les virus désignent un type bien particulier de codes malveillants : des programmes qui ont la faculté de se répliquer automatiquement de machine en machine, de programme en programme, de disquette en disquette, de clé USB en clé USB. Pourtant aujourd'hui, le terme Virus est souvent employé par les non-initiés comme un terme générique pour désigner les malwares.

Watering Holes :
Attaques ciblées contre un site fréquenté par des populations bien identifiées (les développeurs d'une entreprise, les fans du PSG, les auto-entrepreneurs, etc.). Le site infecté devient un Watering Hole, reprenant l'image du point d'eau où les animaux viennent se désaltérer.

Worm :
En Français, « Vers ». Les Worms désignent une catégorie particulière de virus informatiques qui se répandent à travers un réseau. Les Worms peuvent aussi se répandre par email, typiquement en piratant votre carnet d'adresses et en envoyant une copie de lui-même à tous vos correspondants.

Mes notes