Sécurité des ordinateurs

Les principaux dangers qui guettent les utilisateurs, leurs données ou leur portefeuille :

Les malwares : virus, ver, troyens, spywares, ...

Les moyens de se prémunir de ces dangers

Sources : recherches web

diverses conférences sur le sujet

Quelques situations qui pourraient être réelles

- « Dès que je me connecte à l'Internet, des pages de publicités apparaissent constamment, sans que je ne demande rien. Qui me les envoie ? »
- « Le pointeur de souris se déplace tout seul sur mon écran. »
- « Des applications s'ouvrent, d'autres se ferment sans mon intervention. »
- « L'ordinateur s'éteint tout seul… Y a-t-il des lutins facétieux dans mon PC ou y a-t-il une autre explication ? »
- « La banque de Mr Dupont lui réclame la somme 2450 € pour des achats de matériel électroménager effectués avec sa carte de crédit, le mois passé, en Espagne. Mr Dupont n'a jamais mis les pieds en Espagne. Qui a utilisé sa carte de crédit ? »

Plan du cours (1/2)

- Les malwares
- Les virus : les virus se multiplient à nos dépens.
- Les vers : quelle différence entre un ver et un virus ?
- Les chevaux de Troie : quelqu'un cherche à ouvrir la porte.
- Autres nuisances :
  - les spywares : votre comportement est espionné.
  - Les adwares : une petite publicité pour la route ?
  - Les Key loggers : tout ce que vous frapperez au clavier sera connu.
  - Les dialers : vous n'aviez jamais téléphoné aux Iles Caïman ? On va le faire pour vous.
  - Le phishing : non, ce n'est pas votre banque qui vous demande votre numéro de carte de crédit.
  - Le pourriel (spam)

Plan du cours (2/2)

- Tentatives d'intrusions : fermez les portes, on essaie d'entrer dans votre ordinateur.
- Hoaxes : des blagues qui ne font plus rire personne.
- Comportements dangereux
- **Les solutions**
  - Antivirus : un outil indispensable
  - Pare-feu : pour éviter les intrusions.
  - Anti adwares : pour éviter les publicités envahissantes et les espiogiciels.
  - Anti-pourriels : des filtres pour éviter les courriers indésirables.
  - Logiciels moins sensibles : certains logiciels sont moins sensibles aux pestes d' Internet.
  - Comportements : les comportements à éviter, ceux qui sont recommandés.

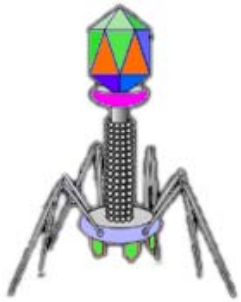
Les malwares

- **Définition** : un malware est une catégorie de programmes plus ou moins autonomes visant à modifier le fonctionnement normal d'un ordinateur de façon plus ou moins grave.
- **Cycle de vie d'un malware**
  - La première étape, la phase de recherche. Durant ce stade, le malware cherche des victimes potentielles (parfois, c'est la victime elle-même qui va le chercher).
  - Une fois trouvé, il faut s'implanter dessus discrètement et vient ensuite la phase de contamination unique ou multiple de la machine.

Les malwares

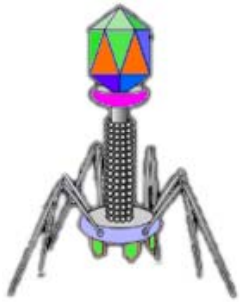
- **Définition** : un malware est une catégorie de programmes plus ou moins autonomes visant à modifier le fonctionnement normal d'un ordinateur de façon plus ou moins grave.
- **Cycle de vie d'un malware**
  - Après cette implantation et éventuellement une période d'incubation, arrive la phase d'exécution où le malware effectue ce pour quoi il est programmé, tout en cherchant éventuellement de nouvelles victimes.
  - Il peut parfois s'en suivre une période d'hibernation pendant laquelle il sera presque indétectable avant de pouvoir reprendre son activité.

Virus informatique



- **Définition**
  - Les virus sont des programmes de taille réduite qui vivent au travers d'un hôte, généralement une application. Le virus informatique injecte le code dont il est formé dans le code d'un programme qu'il trouve sur l'ordinateur cible. Il ne peuvent se reproduire sans l'aide du programme hôte.
  - Le virus est programmé pour se répliquer autant que possible vers d'autres cibles pour, sur un critère donné, déclencher la charge virale.
  - On peut donc tout à fait avoir une machine saine avec un virus dans un programme. Tant que ce programme ne sera pas exécuté, le virus ne sera pas lancé et ne pourra donc pas se dupliquer.
- 1966 : Premier virus crée au Pakistan infectant le secteur de boot et premier Troyen (PC-write).

Virus informatique



- Comment le virus peut-il arriver dans un ordinateur puisqu'il a besoin d'un programme à infecter et ne peut se transmettre que par cette voie ?
- Un virus arrive toujours sur un ordinateur dans un **fichier exécutable**. Il faut donc toujours se méfier de ce type de fichiers.

=> **systématiquement afficher les extensions des fichiers**

Rappel : fichiers exécutables (systèmes Windows)

Extension	Programme
.exe	écrit en langage machine, directement interprétable par l'ordinateur
.com	écrit en langage machine, directement interprétable par l'ordinateur
.vbs	écrit en langage Visual Basic et exécutable sous Windows
.doc	destiné au logiciel de traitement de textes Word. Il peut contenir des programmes (des macros) exécutables par Word
.xls	destiné au tableur Excel. Il peut contenir des programmes (des macros) exécutables par Excel
.bat	destiné à l'interpréteur de commandes
.cmd	destiné à l'interpréteur de commandes
.scr	destiné à réaliser un écran de veille
.pif	destiné à d'anciennes versions de Windows et contenant des informations nécessaires à l'exécution de certaines programmes et/ou des instructions exécutables sous Windows
.zip	éventuellement compressé et exécutable après décompression par un utilitaire de type IZarc, WinZip,...

Effets des virus

- En plus de s'auto-reproduire, un virus a en général une autre activité plus ou moins gênante pour l'utilisateur.
- Les virus sont capables de
  - S'auto-envoyer sous la forme de courrier électronique aux personnes dont les adresses figurent dans l'ordinateur infecté.
  - Envoyer sur l'Internet des données confidentielles récoltées sur l'ordinateur infecté.
  - Utiliser l'ordinateur infecté pour lancer une attaque contre un ordinateur connecté à Internet : si des milliers d'ordinateurs infectés se connectent au même moment, l'ordinateur attaqué sera saturé et ne pourra plus remplir son rôle.

Effets des virus

- En plus de s'auto-reproduire, un virus a en général une autre activité plus ou moins gênante pour l'utilisateur.
- Les virus sont capables de
  - Modifier ou supprimer des données dans l'ordinateur infecté.
  - Provoquer une panne matérielle non réparable (rare aujourd'hui).
  - Ralentir ou bloquer l'ordinateur infecté (le virus occupant toute la capacité de travail du PC).
  - Provoquer l'extinction de l'ordinateur à intervalles réguliers.
  - Etc.

Comment les virus se transmettent-ils ?

- Les disquettes ou clés USB qui passent d'ordinateur à ordinateur sont de très efficaces transporteurs de virus. Les CD-ROM sont moins sensibles car les virus ne peuvent pas s'y inscrire.
- Les documents (traitement de texte ou tableur) transmis par une personne bien connue peuvent contenir des virus de macros.
- Les pièces jointes au courrier électronique sont également un vecteur bien connu. Il faut toutefois que la pièce jointe soit ouverte pour que le virus puisse s'activer.
- Le téléchargement de logiciels ou de fichiers de nature inconnue sur des sites non fiables peut amener des virus. On croit télécharger un "additif" gratuit pour un jeu d'ordinateur et l'on télécharge un virus.
- Le téléchargement de logiciels piratés sur des réseaux de pair à pair (peer-to-peer) comme Kazaa, eMule, Torrent.
- …

Pourquoi les virus informatiques ?

Les raisons qui poussent des personnes à concevoir et diffuser des virus informatiques sont variées.

- Dans certains cas, il s'agit de crime organisé et de racket. Un virus peut être conçu pour s'attaquer aux ordinateurs d'une société précise. Cette société est alors menacée et "invitée" à payer pour éviter l'attaque.
- D'autres raisons financières ont pu motiver ceux qui ont conçu un virus capable d'envoyer des millions de courriers électroniques publicitaires (Spam) à partir d'ordinateurs infectés.

Pourquoi les virus informatiques ?

Les raisons qui poussent des personnes à concevoir et diffuser des virus informatiques sont variées.

- Certains auteurs de virus font partie de "gangs" dans lesquels ils tirent un certain prestige au vu de l'effet d'un virus conçu par eux.
- Pour d'autres, il s'agit de marquer le cyberespace de sa marque.
- D'autres encore se donnent des raisons politiques ou idéologiques.
- ...

Le Ver informatique

- **Définition**
  - Un ver est une **version plus évolué du virus**, indépendant, il se propage automatiquement via les réseaux en utilisant des bugs dans les applications ou des paramétrages incorrects. Il n'a pas besoin d'hôte pour assurer sa duplication et se propage plus rapidement que les virus.
  - Certains vers ou virus sont **polymorphes** c'est à dire qu'ils changent légèrement de forme pour se rendre plus difficile à identifier.
  - Ce changement est basé soit sur l'ajout d'instruction sans conséquence (NOP en assembleur, assigner des valeurs à des registres non utilisés) soit en tirant parti de l'associativité de calculs arithmétique ou d'instructions machines.

Buts de l'action des vers

- Pur vandalisme gratuit : provoquer la saturation d'un réseau sous l'effet exponentiel de sa multiplication.
- Attaque ciblée : attente furtive au sein de milliers d'ordinateurs ; à une date précise, chaque ver se connecte à un seul et même serveur provoquant sa mise hors service.
- Prise de commande à distance de votre ordinateur.
- Espionnage des frappes au clavier, y compris des numéros de cartes de crédit.
- Ouverture de portes de l'ordinateur pour faciliter l'accès par d'autres vers ou virus.
- Envoi de milliers de courriers électroniques publicitaires non sollicités depuis votre ordinateur.
- Effacement de fichiers, envoi de vos fichiers (confidentiels) sur Internet, ...

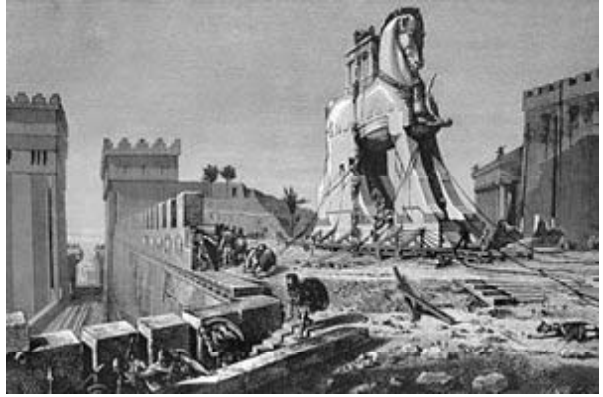
Exemple de vers

- **Le ver Sasser**
  - Parti d'un ordinateur distant, il se connecte à votre ordinateur comme s'il était une commande normale. Celle-ci est reconnue et son traitement commence. Mais, la commande est mal formée et contient **trop** d'information par rapport à ce qui est attendu dans ce cas précis.
  - Le trop-plein d'informations est stocké dans la mémoire au-delà de la zone prévue.
  - A cause d'une erreur de conception du programme qui traite la commande, le surplus d'information est alors exécuté comme un programme normal. Le ver s'installe alors au sein du système et tente immédiatement de se propager vers d'autres ordinateurs qui présentent la même déficience.

Exemple de vers

- **Le ver Netsky**
  - Le ver Netsky parvient à entrer dans un ordinateur en profitant d'une imperfection dans certaines versions du logiciel de courrier électronique Outlook. Pour que le ver s'active, il n'est même pas nécessaire que l'utilisateur ouvre une pièce jointe : le ver est contenu dans le message lui-même. Le seul fait de cliquer sur le message suffit à activer le ver.
  - Dès qu'il est actif, Netsky s'auto-envoie par courrier électronique. De plus, l'ordinateur infecté sert de « zombie » qui participe à l'attaque du site web Windows Update.
  - Un ordinateur infecté peut expédier plusieurs dizaines de vers à la minute. On notera généralement un fort ralentissement de l'ordinateur…

Chevaux de Troie



- **Définition**
  - Un cheval de Troie, en référence à l'Iliade, est un ver ayant des fonctionnalités partiellement différentes.
  - En informatique, un Cheval de Troie ou Troyen (Trojan en anglais) est un logiciel malveillant qui se présente comme un programme utile ou une application intéressante.
  - Le résultat de l'utilisation de ce fichier peut être simplement la destruction de fichiers ou la récupération de vos mots de passe.
  - La différence essentielle entre un Troyen et un ver réside dans le fait que le ver tente de se multiplier. Ce que ne fait pas le Troyen.

Exemple de Cheval de Troie

- Le ver "ILOVEYOU" se présente comme un courrier électronique amical.
- Une fois installé, le ver envoie les mots de passe qu'il trouve sur l'ordinateur vers une adresse électronique.
- Ver écrit en Visual Basic
- S’est répandu très vite par la messagerie électronique

Les Backdoors (porte de derrière)

- **Définition**
  - Il s'agit d'un cheval de Troie permettant de se connecter à distance sur l'ordinateur infecté.
  - Une fois les « portes » ouvertes, l'ordinateur pourra être utilisé par d'autres logiciels malveillants ou par des pirates.
  - Pour pénétrer dans un ordinateur, il suffit d'ouvrir un port non utilisé. Dès qu'un port est ouvert, il est possible de prendre entièrement le contrôle de la machine depuis n'importe quel ordinateur connecté à Internet.

Utilisation des Chevaux de Troie / Backdoor

- Sur un réseau, un cheval de Troie est vraisemblablement utilisé pour espionner et voler des informations sensibles (espionnage industriel). Les intérêts des agresseurs peuvent inclure :
  - Tous détails des comptes (mots de passe email, connexion à distance, services Web, etc.)
  - Documents confidentiels
  - Adresses email (par exemple, les contacts de clients)
  - Images ou conception confidentielles
  - Informations sur l'emploi du temps d'un utilisateur, sur ses déplacements
  - Information de cartes de crédit (souvent utilisées pour l'enregistrement de nom de domaine ou des achats en ligne)
  - Utiliser votre ordinateur avec des intentions illégales, comme hacker, scanner, noyer ou infiltrer d'autres machines sur le réseau ou sur Internet.

Exemple de Backdoor

- Backdoor.BackOrifice
- BackOrifice est une application client/serveur qui permet au logiciel client de surveiller, administrer, et effectuer à distance n'importe quelle action (réseau, multimédia, redémarrage, fichiers,…) sur la machine exécutant le serveur.
- Origine et buts de "Back Orifice
  - Cette application a été développée en 1998 par un groupe de "hackers" nommé "Cult of the Dead Cow" (cDc) et diffusée sur Internet très rapidement, dans le but (d'après leurs auteurs) de mettre en évidence les trous de sécurité existant dans Windows 95/98 (et donc de dévaloriser ce système).

Statistiques sur les virus et troyens (2011)

- L'Australie est le continent le plus touché car un email sur 351,6 abrite un virus ou un trojan.
- Pour l'Allemagne, la statistique annonce un email sur 462.
- Sur tous les messages électroniques enregistrés au Canada, un email sur 492,8 est infesté de virus et de cheval de Troie.
- Aux Etats-Unis, le chiffre annoncé est de un email sur 551,4.
- Les Pays-Bas et le Japon sont les moins touchés par le virus et le trojan avec un email sur 834,7 et sur 1063,3.

Autres nuisances logicielles

- **Spywares**
- **Adwares**
- **Key loggers**
- **Dialers**

Spyware (ou espiogiciel)

- Les spywares font partie des nouveaux fléaux, du simple cookie stocké sur la machine aux applications tournant en tâche de fond, les plus discrètes, ces spywares épient votre vie privée et l'utilisation de votre machine.
- Le spyware collecte des informations sur l'utilisateur d'un ordinateur, et les envoie vers son concepteur ou un commanditaire.
- La collecte d'information permet de créer et de revendre des bases de données énormes à des sociétés publicitaires pour l'envoi de Spam par exemple.
- Parfois plusieurs centaines de spywares cohabitent ensemble mais finissent par mettre les performances de la machine à rude épreuve.

Spyware (ou espiogiciel)

- Certains spywares sont intégrés, plus ou moins discrètement, à des logiciels gratuits. D'autres tentent de s'installer simplement lors de la visite d'une page web.
- Vous visitez tel site web, vous vous attardez sur telle page qui présente tel article en vente. Le spyware en prend bonne note et envoie ces informations vers un serveur.
- Un peu plus tard, vous travaillez calmement sur votre ordinateur, quand une publicité pour un produit similaire apparaît. Sans que vous ayez rien demandé. Vous fermez la fenêtre publicitaire. Deux minutes plus tard, elle revient.

  ⇒ Vous êtes victime d'un spyware
- Parmis les logiciels couramment utilisés et qui renferment des spywares, on trouve : Mirabilis ICQ, RealNetworks RealPlayer, Burn4Free, Kazaa et bien d'autres…

Les adwares (ou pubgiciel)

- Les adwares sont des logiciels du même type que les spywares. Ils s'installent généralement sans que l'utilisateur ait bien pris conscience du fait qu'il installe un tel logiciel.
- Ces logiciels ajoutent des publicités dans les pages web visitées ou dans des fenêtres séparées.
- A la différence des spywares, les adwares ne communiquent pas d'information vers un serveur. Ils peuvent donc travailler même si l'ordinateur qu'ils colonisent n'est pas connecté à Internet.
- Ils utilisent des ressources de l'ordinateur : occupation de mémoire, utilisation du processeur, utilisation du disque dur. L'ordinateur est donc ralenti. De plus, ces programmes sont souvent mal écrits et contiennent des bugs qui font "planter" l'ordinateur.

Installation d'un adware

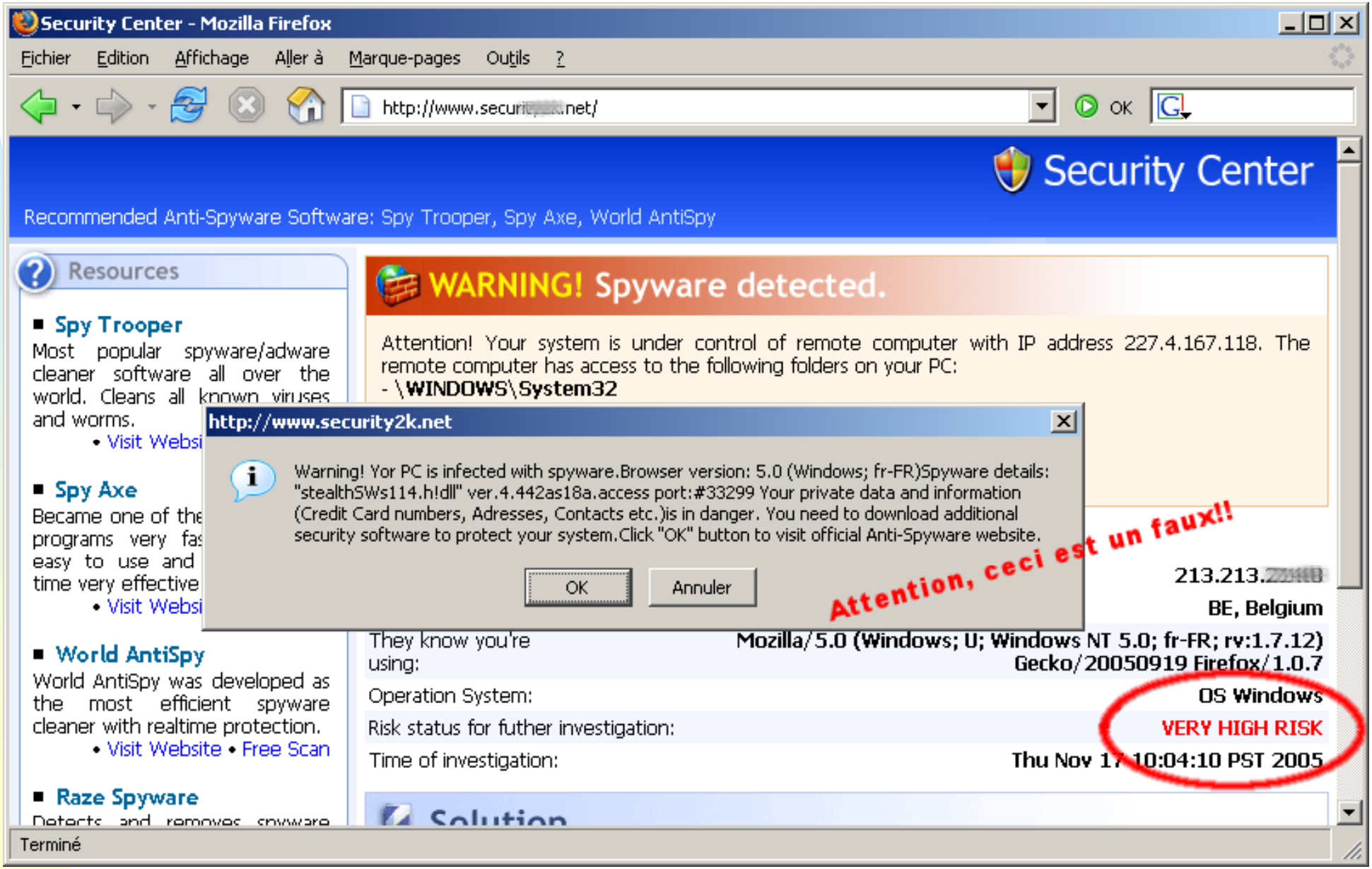
- Il suffit que le niveau de sécurité du navigateur web soit trop faible. Des logiciels peuvent alors s'installer sans prévenir.
- Dans d'autres cas, l'utilisateur clique trop facilement sur le bouton qui donne son accord, sans avoir compris à quoi il s'engage

Installation d’un adware agressif

- Certains adwares ou spywares sont extrêmement agressifs et vicieux : des produits se font passer par exemple pour des anti-spywares.
- Ils persuadent l'utilisateur que son ordinateur est infesté de spywares.
- Celui-ci télécharge alors le logiciel qui ne fait que leur ajouter des spywares, adwares ou dialers supplémentaires.

=> Ne pas se laisser attraper par les publicités agressives.

Installation d'un adware agressif



Les Keyloggers (ou enregistreurs de frappes)

- Il ne s'agit, cette fois, plus de publicité. Les Keyloggers sont généralement des logiciels commerciaux (en vente libre) qui permettent d'espionner tout ce que fait l'utilisateur d'un ordinateur: frappes au clavier (y compris les mots de passe, numéros de carte de crédit, ...), sites web visités, copies de l'écran, etc.
- Toutes les informations sont ensuite transmises vers une adresse de courrier électronique.
- Les Keyloggers sont souvent présentés comme des solutions (discutables) pour des parents qui souhaitent savoir ce que font leur enfant ou des patrons qui désirent savoir ce que font leurs employés lorsqu'ils sont devant leur ordinateur.
- Certains virus ou Chevaux de Troie peuvent contenir des Keyloggers.

Les dialers (composeurs téléphoniques)

- Un dialer peut être une application tout à fait honnête. Pour obtenir une information, pour acheter un produit ou un service, on vous propose d'appeler un numéro de téléphone surtaxé (si usage d'un modem).
- Le fournisseur de service peut vous proposer de télécharger un petit logiciel qui se chargera de réaliser l'appel surtaxé.
- **Méfiance ! Vous ne savez pas quel numéro sera appelé par le logiciel. Il pourra s'agir d'un appel vers un numéro surtaxé dans un pays exotique. Vous continuez de profiter du service mais en étant connecté à un serveur situé aux antipodes.**

Le phishing (ou hameçonnage)

- Le phishing est une technique par laquelle des malfaiteurs tentent d'entraîner un client d'une banque vers un site web qui ressemble très fort à celui de sa banque.
- Ils persuadent la personne de fournir son numéro de carte de crédit ou son login et le mot de passe qui y est associé, ce qui leur permet ensuite très facilement de faire des achats ou de retirer de l'argent sur le compte en banque de leur victime.
- Le phishing ne cible généralement pas les clients connus d'une banque. Les malfaiteurs envoient des courriers électroniques tous azimuts, en utilisant les mêmes techniques que les spammeurs.
- Parmi les personnes qui reçoivent le courrier électronique, certaines sont réellement clientes d'une banque cible.

Exemple de phishing

X-Server-Uuid: 0627D933-0E11-4119-B36A-CE08648593E2
X-Server-Uuid: 6C567EC4-4768-4F66-893F-838D00B15500
From: "LaSalleBank" <important@lasallebank.com>
Subject: IMPORTANT: Account Verification
Date: Wed, 22 Jun 2005 03:50:16 -0700
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
To: undisclosed-recipients: ;
X-WSS-ID: 6EA667CC2SK717526-01-04
X-OriginalArrivalTime: 22 Jun 2005 00:53:26.0127 (UTC)
FILETIME=[CC2FA7F0:01C576C4]
X-WSS-ID: 6EA667AF25S188785-01-04

We are glad to inform you, that our bank has a new security system. The new updated technology will ensure the security of your payments through our bank.

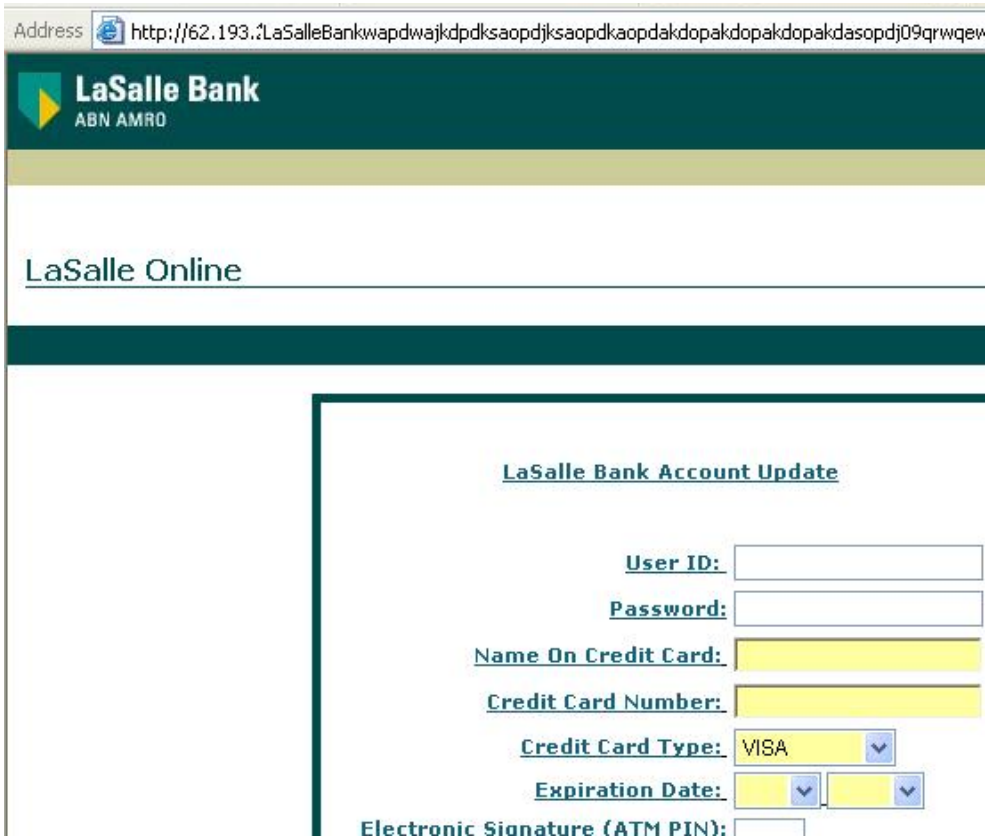
Hoping you understand that we are doing this for your own safety we suggest you to update your account , this update will maintain the safety of your account . All you have to do is to complete our online secured form . Thank You.

Continue

Lorsque la victime clique sur le bouton Continue, au bas du message qu'elle a reçu, elle aboutit sur un site web qui ressemble à s'y méprendre au site web de la banque

Exemple de phishing

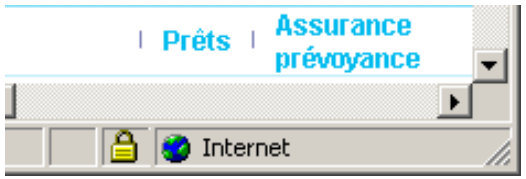
- Elle est invitée à y fournir des informations relatives à sa carte de crédit.
- Le problème est qu'il ne s'agit pas du site web de la banque, mais d'une copie conforme. Si le client fournit les informations demandées, celles-ci sont alors transmises aux malfaiteurs.
- Dans le cas présenté ci-dessus, certains indices montrent clairement qu'il s'agit d'une supercherie :



- L'adresse URL de la banque ne figure pas dans la barre d'adresse
- La connexion vers la banque n'est pas sécurisée : http et non https
- On ne trouve pas le symbole de la connexion sécurisée dans le navigateur

Exemple de phishing

- **Symboles de sécurité**
  - Internet Explorer :



  - Firefox :

  - Dans certains cas, les pirates cachent l'adresse de destination à l'aide d'un petit programme qui superpose un rectangle où figure la vraie adresse de la banque.
  - La technique est d'ailleurs parfois imparfaite, comme sur l'exemple ci-dessous ou le "cache" apparaît bien (l'adresse URL est un peu décalée vers le bas) :

Statistiques sur le phishing (2011)

- Pour le phishing, un grand écart est enregistré entre plusieurs nations.
- Le Royaume-Uni est le plus touché par le phishing avec un email sur 254,8.
- Il est suivi par l'Australie avec un email sur 454,5.
- Au Canada, les spécialistes font état d'un email hameçonné sur 869,3.
- Les Etats-Unis n'en est pas loin avec un email sur 981,9.
- Les trois pays les plus sûrs sont l'Allemagne avec un mail sur 2 506, les Pays-bas avec un email sur 3 439 et le Japon avec un email sur 10 217.

Le Spam (ou pourriel)

- Spam est à l'origine le nom d'une marque de conserves dont une publicité en radio consistait en la répétition abrutissante du nom de la marque.
- Le "spamming" ou "spam" est l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière:
  - soit au moyen de moteurs de recherche dans les espaces publics d'Internet (sites web, forums de discussion, listes de diffusion, chat...),
  - soit que les adresses aient été cédées sans que les personnes en aient été informées et sans qu'elles aient été mises en mesure de s'y opposer ou d'y consentir.

Le Spam (ou pourriel)

- *De toute façon, personne ne lit tous ces trucs. Je me demande bien quel intérêt ont ceux qui envoient toutes ces publicités.*

- *Dire que "personne ne lit", n'est pas tout à fait vrai. Le coût de l'envoi de dizaines de milliers de courriers publicitaires est très faible.* ***Il suffit que quelques personnes réagissent et passent commande pour le produit pour que la campagne soit bénéficiaire.***
  Et ça fonctionne, puisque les spams se multiplient.

- *N'empêche, ils doivent pouvoir se payer de gros ordinateurs, pour inonder la planète de courriers électroniques, ces spammeurs.*

- *Ce n'est pas forcément nécessaire. Il leur suffit d'utiliser votre ordinateur (et quelques milliers d'autres).*

Le Spam

- Une solution trouvée par les spammeurs est donc d'utiliser des ordinateurs répartis sur la planète pour envoyer leurs courriers. Il leur suffit de contrôler ces ordinateurs à distance et d'y implanter des serveurs de courrier électronique.
- Pour prendre le contrôle d'un ordinateur distant, ils peuvent utiliser des virus ou des vers. Ceux-ci ouvrent des ports des ordinateurs qu'ils infectent. Il ne reste plus aux spammeurs qu'à détecter les ordinateurs qui leur répondent pour en prendre le contrôle.
- C'est ainsi que votre ordinateur peut être utilisé par les spammeurs.

Le Spam

- Les pirates qui veulent utiliser votre ordinateur à distance doivent donc constamment être à la recherche d'ordinateurs connectés à Internet et dont certains ports sont ouverts.
- Un ordinateur connecté à Internet subit généralement des tentatives d'intrusion après quelques minutes.
- Il est donc impératif de toujours vérifier que votre pare-feu est actif.
- Le risque est bien de voir votre connexion utilisée pour envoyer du spam. Votre connexion sera donc ralentie et vous risquez de recevoir des plaintes pour envoi de spam.

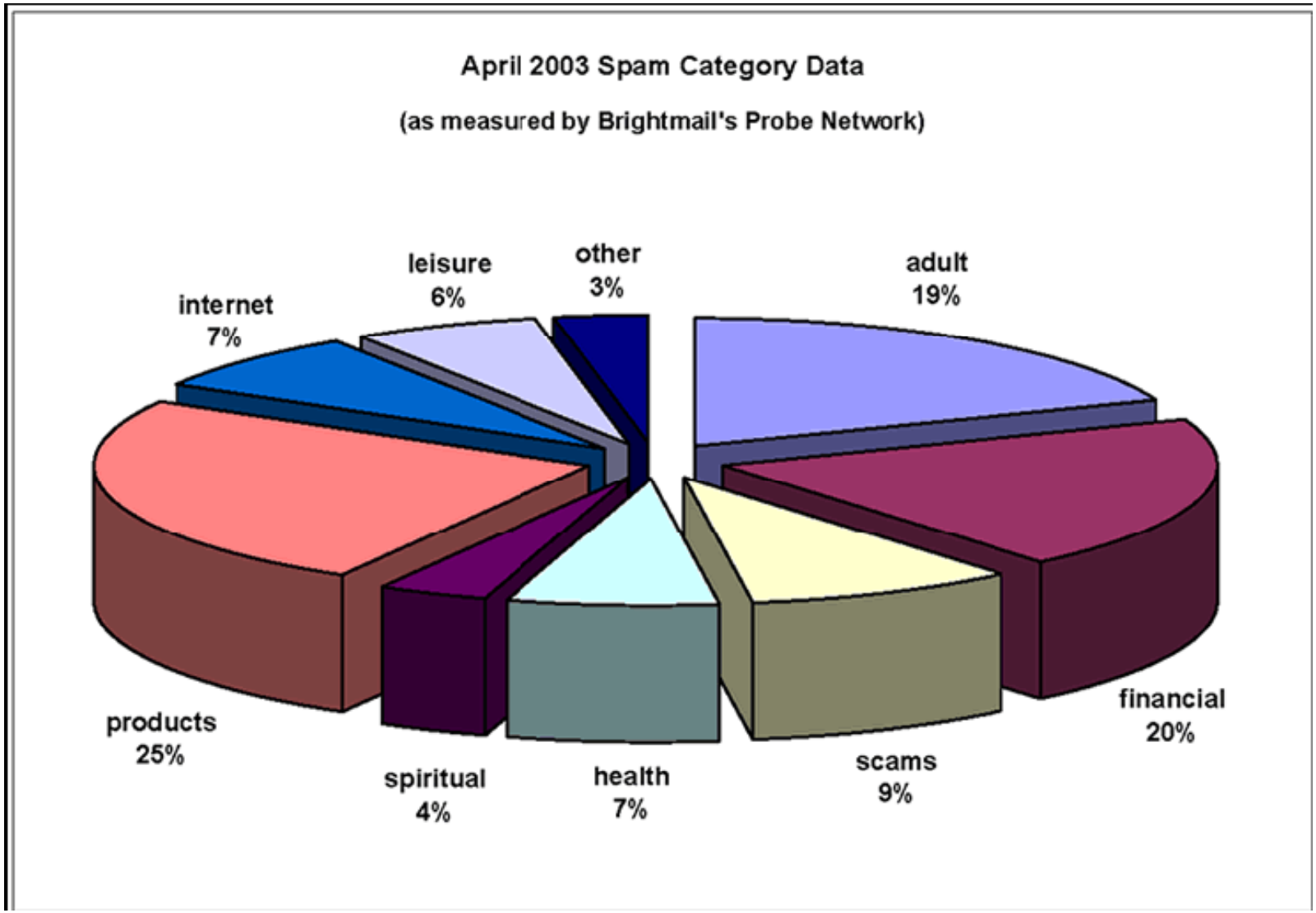
La Loi relative au Spam

- **Le mail est une correspondance privée**
  - Son détournement est illégal
  - Son détournement par un fonctionnaire est considéré comme plus grave

Les différentes catégories de Spam

- Adult : Porno, Rencontres, …
- Health : Santé, Herbe, Médecine, …
- Products : Vente de produits divers ..
- Financial : Finances, Banque, …
- Scams : Chaîne d'argent, Nigéria, Escroquerie…
- Internet : Hébergement, Ventes liste email, ..
- Leasure : Casino, Jeu, …
- Spiritual : Astrologie, Org. Religieuses, …
- Autre : le reste.

Les différentes catégories de Spam



Pourquoi filtrer le SPAM ?

- C’est près de 90 % du trafic email journalier.
- Consommateur
  - en bande passante
  - en CPU, mémoire, espace disque
- Les usagers ont une messagerie polluée
  - Inefficacité du traitement du courriel => donc perte d’argent pour les usagers ou l’entreprise.
- Pas de possibilités de se désinscrire
  - Les adresses « Unsubscribe » fonctionnent à 37% (Statistique U.S.)

Les impacts économiques du SPAM

- Il ne coûte rien au spammeur
- Coûte 10 milliards d'Euros par an en Europe

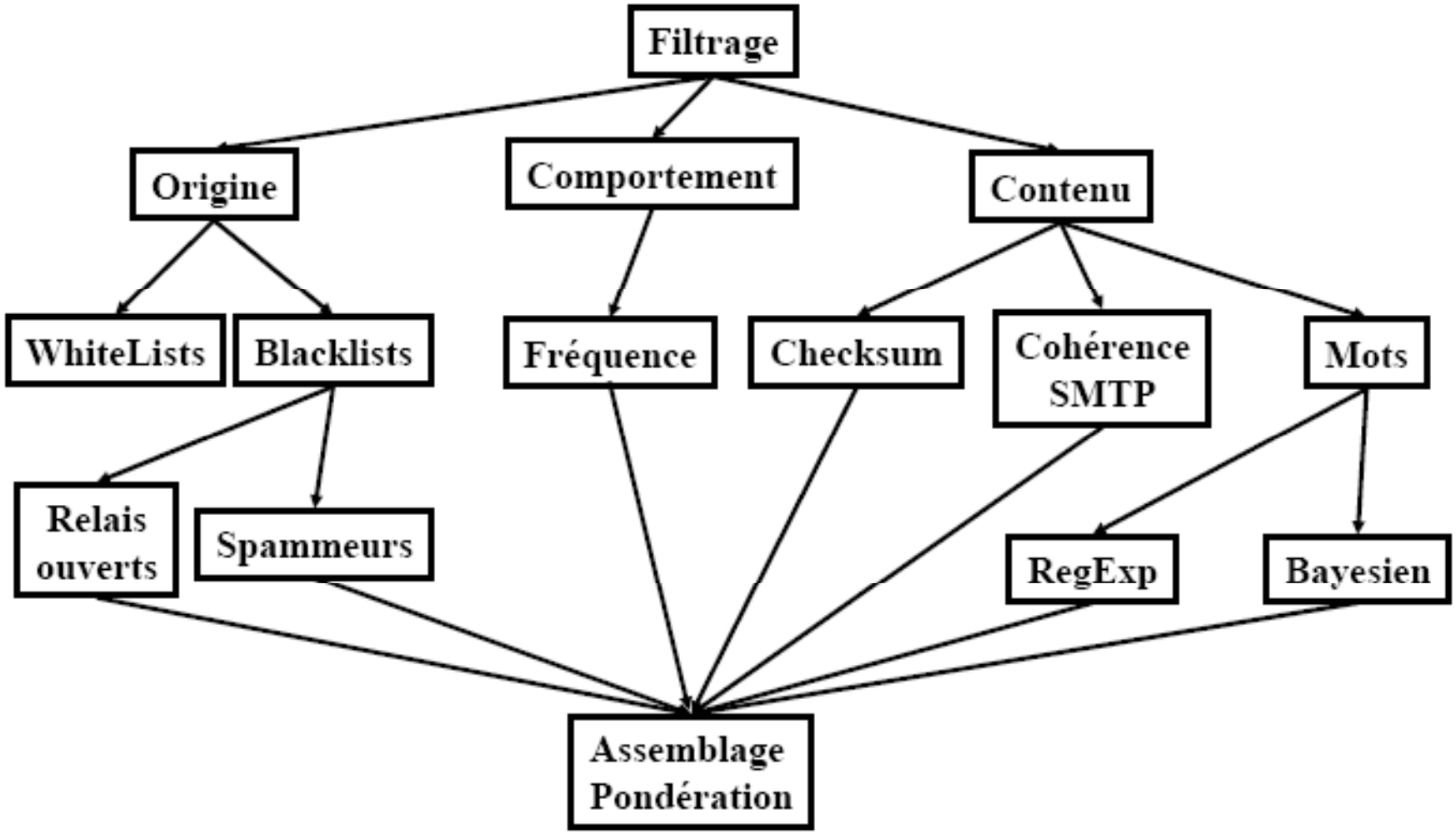
  => un marché est apparu : combattre les SPAMS. Des sociétés sont présentes sur ce secteur et ont été rejointes par les éditeurs d'antivirus

Combat contre le Spam

Les solutions

- Détecter les spams sur le serveur de courriel : tendre vers le « Zéro-configuration » :
- Utilisation de plusieurs règles pour déterminer si un message est un spam ou non.
  - Utilisation de logique « floue » pour les règles
  - Le résultat de ces règles est combiné pour produire un « score »
  - En fonction d'un seuil défini, le message est considéré comme un spam.
  - Filtres bayésiens (corrélations)
- Une règle seule ne peut pas déterminer si un message doit être considéré comme un spam

Filtrage : De nombreux critères



Statistiques sur le spam (2011)

- Le spam est devenu un fléau pour tous les utilisateurs du monde entier.
- En Allemagne, 93,1% des messages électroniques qui circulent sur le réseau sont des spam.
- Aux Pays-bas, le taux est de 93%.
- La Chine occupe la troisième place avec 92,4%, suivi des Etats-Unis avec un taux de trafic de spam évalué à 91,1%.
- Pour le Royaume-Uni, 90,1% des emails envoyés sont des spam. Il en est de même pour le taux de spam enregistré en Australie.
- Seuls les taux de spam enregistrés sur tout le trafic de messages électroniques enregistrés au Canada et au Japon se situent en dessous de 90% avec un taux respectifs de 89,5% et 87,5%.

Statistiques sur le spam (2011)

- **Les secteurs d'activité les plus spammés**
- l'ingénierie arrive en tête avec 94,7%
- l'éducation : 91,9%
- grande distribution : 91,8%
- services informatiques : 91,6%
- secteur pharmaceutique et l'industrie chimique: 91,1%
- finance : 89,5%
- secteur public : 89,1%.

Les hoaxes (canulars)

- De nombreux courriers électroniques circulent pour nous informer de faits graves, importants, urgents... mais souvent inexistants.
- Il s'agit souvent de **courriers de type chaînes** que vous êtes invité à relayer vers tout votre carnet d'adresses.
- Il ne faut jamais renvoyer ces messages pour une simple raison mathématique : l'effet obtenu serait simplement une saturation du réseau.

génération	Nombre de messages en circulation
1	20
2	400
3	8.000
4	160.000
5	3.200.000

Le site français de référence pour la vérification des canulars :
http://www.hoaxbuster.com/

Autre danger de l'Internet : votre comportement

- Certains **comportements** lors de l'utilisation de l'Internet ne sont pas sans poser de problèmes à cause des dangers qu'ils représentent.
  - Visite de certains sites web pornographiques : dangers pour les adwares et les dialers.
  - Téléchargements sur les réseaux d'échanges de fichiers : danger de télécharger n'importe quelle peste : virus, ver, adware,...
  - Téléchargement de logiciels gratuits : ces logiciels sont souvent payés par les publicités qu'ils afficheront sur votre écran.
  - Les logiciels libres, par contre, sont souvent gratuits mais ne posent pas ce type de problème.

Autre danger de l'Internet : votre comportement

- Certains comportements lors de l'utilisation de l'Internet ne sont pas sans poser de problèmes à cause des dangers qu'ils représentent.
  - Utilisation de l'ordinateur sans antivirus (parfaitement à jour) et/ou sans pare-feu.
  - Ouverture de n'importe quel courrier électronique dont vous ne connaissez pas l'auteur.
  - Ouverture des pièces jointes aux courriers électroniques, même si l'on connaît l'auteur. Un virus ou un ver peut s'auto-envoyer en volant l'identité d'une personne que vous connaissez bien.

Autre danger de l'Internet : votre comportement

- Un ami vous envoie un mail et vous demande de l'envoyer à tout votre carnet d'adresses. Il est marqué:

  « Un nouveau virus viens d'être découvert et a été classé par Microsoft comme étant le + destructeur n'ayant jamais existé. Ce virus a été découvert hier après midi par McAfee et aucun vaccin n'a encore été développé.
  Ce virus détruit le secteur zéro de votre disque dur, là où les informations vitales au fonctionnement de votre système sont emmagasinées. »

1. Vous transmettez à tout votre carnet d'adresses, comme demandé
2. Vous jetez à la corbeille sans même vérifier, même si vous n'avez jamais entendu parler de cela
3. Vous vérifiez et puis vous jetez à la corbeille

Les solutions

Antivirus : un outil indispensable

Pare-feu : pour éviter les intrusions.

Anti adwares : pour éviter les publicités envahissantes et les espiogiciels.

Anti-pourriels : des filtres pour éviter les courriers indésirables.

Logiciels moins sensibles : certains logiciels sont moins sensibles aux pestes de l'Internet (Linux, Firefox,...).

Comportements : les comportements à éviter, ceux qui sont recommandés.

Les Antivirus

- Un antivirus est un programme capable de détecter les virus, les vers, les troyens et parfois les spywares qui peuvent infecter un ordinateur.
- L'antivirus devrait être résident sur l'ordinateur, mais il existe aussi des tests d'infection virale disponibles sur le web.
- Vendus dans le commerce
- Certains antivirus sont plus efficaces que d'autres. Il est bon de s'informer avant d'acheter un des produits proposés.
- Parmi les critères importants, il faut considérer la fréquence des mises à jour. Elle devrait être quotidienne.

L'antivirus résident

- Installé sur l'ordinateur comme n'importe quel autre programme classique.
- Doit démarrer en même temps que l'ordinateur et rester actif durant tout le temps que dure la session de travail.
- Le logiciel antivirus devrait obligatoirement figurer sur tout ordinateur, même non connecté à l'Internet.
- Un bon antivirus doit intervenir au moment même de l'entrée ou de la tentative d'entrée d'un quelconque virus, ver, troyen.
- **Petit test** : télécharger les fichiers référencés ici :

  http://www.eicar.org/anti_virus_test_file.htm

Antivirus gratuits

- Il existe un certain nombre d'antivirus gratuits disponibles au téléchargement. Même si l'on peut parfois se poser des questions sur la qualité des produits gratuits, cette solution est certainement meilleure que l'absence d'antivirus.

  http://www.avast.com/

  http://www.free-av.com/

  http://www.grisoft.com/doc/289/lng/us/tpl/tpl01

  http://www.clamwin.com/ (logiciel libre)

  http://www.clamav.net/ (logiciel libre pour Linux)

Efficacité des Antivirus – Test Janvier 2010

- **Analyse d'un dossier entièrement infecté**

  Le dossier en question contient donc 17 virus différents, au sein de 75 fichiers tous infectés. Voici les résultats des détections (toutes réalisées avec le maximum d'options d'analyse sélectionnées

	Fichiers infectés	Pourcentage
McAfee	71	94.5 %
BitDefender	75	100 %
BullGuard	75	100 %
Norton	75	100 %
NOD32	71	94.5 %
Kaspersky	75	100 %
avast!	75	100 %
F-secure	75	100 %
PC-cillin 12	75	100 %
AntiVir	71	94.5 %
Panda 2005	75	100 %
AVG	71	94.5 %

Source : http://www.pcworld.fr/article/materiel/logiciels/comparatif-de-8-anti-virus/107551/

Efficacité des Antivirus – Test Janvier 2010

- **Analyse d'un dossier contenant des virus au sein d'une majorité de fichiers sains.**

  Pour cette partie du test nous avons placé 98 virus au sein de plusieurs dossiers et sous dossiers. La majeure partie des ces virus sont les même que précédemment. Pour compliquer la tache des antivirus, nous avons ajouté des archives infectées ainsi que les dossiers temporaires d'Internet Explorer eux-mêmes infectés.

	Fichiers analysés	Fichiers infectés	Taux de détection	Temps d'analyse	Fichiers / secondes
McAfee	2963	88	89.8 %	28	106
BitDefender	6636	94	95.9 %	24	276
BullGuard	6940	82	83.7 %	39	178
Norton	3183	89	90.8%	/	NA
NOD32	2951	92	93.9 %	14	210
Kaspersky	3143	93	94.8 %	71	44
avast!	3135	86	87.7 %	15	209
F-secure	3102	95	96.9 %	36	86
PC-cillin 12	2943	89	90.8%	7	420
AntiVir	2947	88	89.8 %	28	105
Panda 2005	3106	94	95.9 %	26	120
AVG	3038	84	85.7 %	11	276

Source : http://www.pcworld.fr/article/materiel/logiciels/comparatif-de-8-anti-virus/107551/

Efficacité des Antivirus – Test Janvier 2010

- **Gestion des infections du courrier électronique.**

	Réaction de l'antivirus
McAfee	Trouve 100% des fichiers infectés et les supprime
BitDefender	Bloque le transfert de l'email dès le premier virus
BullGuard	Bloque le transfert de l'email dès le premier virus
Norton	Trouve 100% des fichiers infectés et les supprime
NOD32	Trouve 100% des fichiers infectés et les supprime
Kaspersky	Trouve 100% des fichiers infectés et les supprime
F-secure	Trouve 100% des fichiers infectés et les supprime
avast!	Trouve 100% des fichiers infectés et propose une action
PC-cillin 12	Bloque le transfert de l'email dès le premier virus
AntiVir	Absence de scanner POP3
Panda 2005	Trouve 100% des fichiers infectés et les supprime
AVG	Trouve 100% des fichiers infectés et les supprime

Source : http://www.pcworld.fr/article/materiel/logiciels/comparatif-de-8-anti-virus/107551/

Efficacité des Antivirus – Test Janvier 2010

Comportement face à une tentative d'accès à un fichier infecté

Pour les besoins de ce test nous avons sélectionné deux fichiers infectés de type EICAR (fichier contenant une signature de virus, mais non infectés) : un fichier .TXT et un fichier .COM. Les actions que nous avons tenté sur ces fichiers sont les suivantes : une sélection et une tentative de lancement. Pour le fichier .TXT nous avons aussi tenté de le renommer en .COM, action visant à le rendre potentiellement beaucoup plus dangereux qu'au format texte. Ces tests simples visent à tester la protection en temps réel offerte par les antivirus.

	Fichier.COM	
	Sélection	Lancement
McAfee	OK	Refus
BitDefender	OK	Refus
BullGuard	OK	Refus
Norton	OK	Suppression
NOD32	OK	Suppression
Kaspersky	Négatif	Accepte
avast!	Négatif	Refus
F-secure	Négatif	Refus
PC-cillin 12	OK	Suppression
AntiVir	OK	Refus
Panda 2005	Négatif	Suppression
AVG	OK	Refus

	Fichier .TXT		
	Sélection	Lancement	Renommer
McAfee	OK	Refus	Refus
BitDefender	OK	Refus	Refus
BullGuard	OK	Refus	Refus
Norton	OK	Suppression	Suppression
NOD32	Négatif	Accepte	Suppression
Kaspersky	Négatif	Accepte	Accepte
avast!	Négatif	Accepte	Accepte
F-secure	Négatif	Refus	Refus
PC-cillin 12	OK	Suppression	Suppression
AntiVir	OK	Refus	Refus
Panda 2005	Négatif	Accepte	Refus
AVG	Négatif	Accepte	Accepte

Source : http://www.pcworld.fr/article/materiel/logiciels/comparatif-de-8-anti-virus/107551/

Efficacité des Antivirus – Test Janvier 2010

Conclusion sur les performances de sécurité

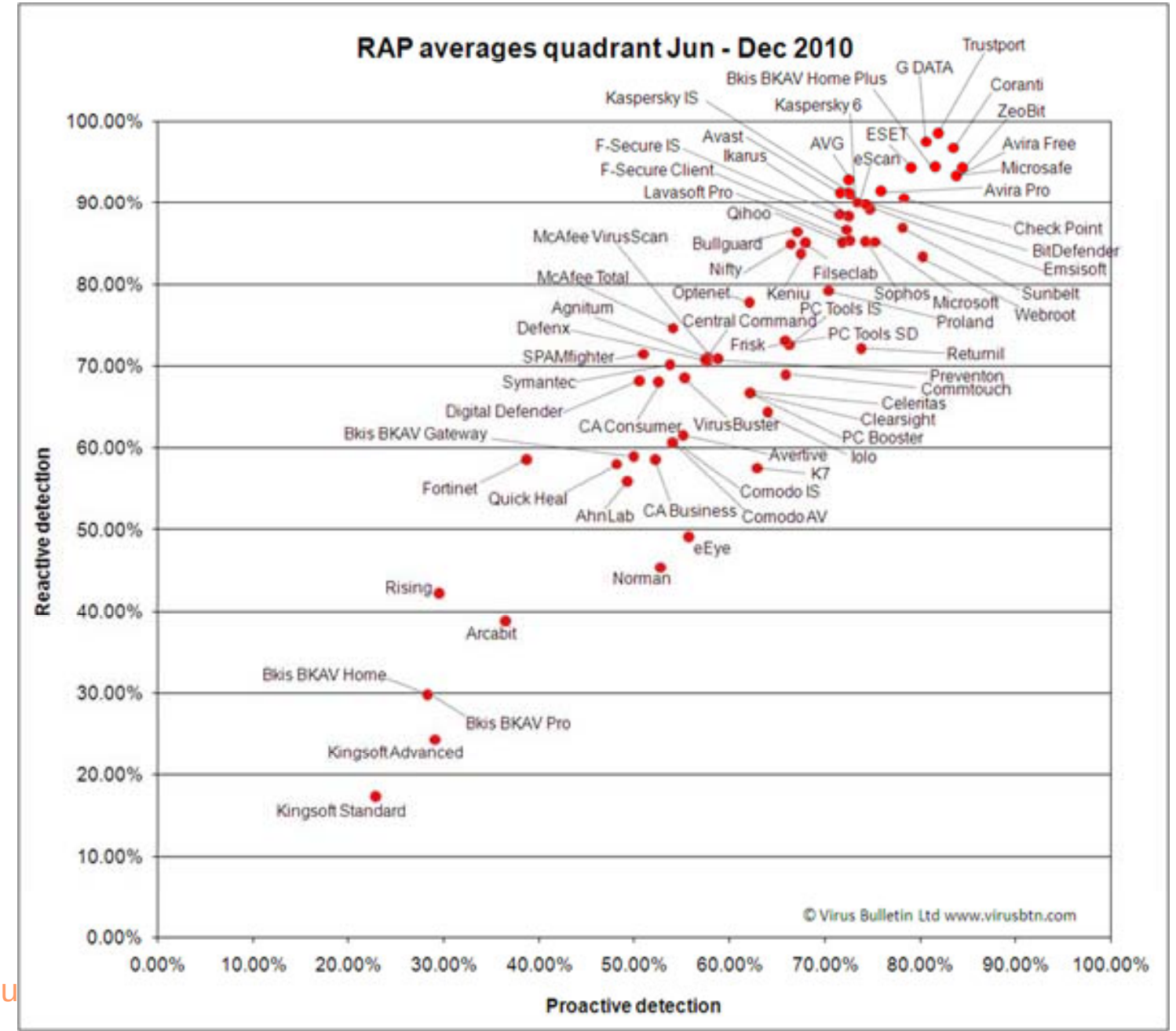
Nous avons comptabilisé le nombre de "couleurs" que chacun des antivirus a amassé au cours des différents tests.

	Vert	Orange	Rouge
BitDefender	13	1	0
Panda	11	3	0
McAfee	9	4	1
NOD32	9	5	0
PC-cillin	9	2	3
F-secure	8	6	0
Antivir	8	5	1
BullGuard	7	3	4
Norton	7	4	3
Kaspersky	6	6	2
AVG	6	3	5
avast!	4	7	3

Source : http://www.pcworld.fr/article/materiel/logiciels/comparatif-de-8-anti-virus/107551/

Site de référence : Virus Bulletin

http://www.virusbtn.com/



Les antivirus en ligne

- Un certain nombre de sites web proposent des outils antivirus qui peuvent être utilisés en ligne.
- Ces outils ne remplacent pas un antivirus résident. Ils permettent toutefois une vérification rapide de l'état de l'ordinateur si l'on pense avoir été infecté.
- Ces antivirus ne permettent pas d'empêcher l'infection virale ; ils peuvent seulement éventuellement agir après.
- http://fr.trendmicro-europe.com/consumer/housecall/housecall_launch.php
- http://www.secuser.com/antivirus/

  (ne fonctionne qu'avec Internet Explorer)
- http://www.bitdefender.fr/scan/license.php

  (ne fonctionne qu'avec Internet Explorer)
- http://www.virustraq.com/service/antivirus_en_ligne/check/

  (ne fonctionne qu'avec Internet Explorer)

Le pare-feu (ou firewall)

- Le pare-feu est un dispositif matériel ou logiciel dont le rôle est d'empêcher les intrusions dans un ordinateur connecté à un réseau et d'éviter que des informations sortent de l'ordinateur sans l'accord de l'utilisateur. C'est donc un filtre à double-sens.
- De nombreux logiciels malveillants sont conçus pour ouvrir des ports de manière à permettre des intrusions. Le pare-feu empêchera l'intrusion même si un port est ouvert. Eventuellement, le problème sera signalé à l'utilisateur.
- Inversement, si un spyware tente d'envoyer des informations vers un serveur distant, le pare-feu pourra agir pour empêcher ce transfert.
- **Le pare-feu n'est donc nécessaire que pour les ordinateurs qui sont connectés à Internet ou à un réseau Intranet non sûr.**

Comment se procurer un pare-feu

- Les logiciels pare-feu sont vendus dans le commerce.
- Un pare-feu est intégré à Windows (voir les propriétés avancées de la connexion ou le centre de sérurité)
- Il est activé par défaut
- Ce pare-feu peut être remplacé par un pare-feu plus efficace.
- Matousec est un organisme indépendant qui teste régulièrement tous les pare-feux du marché et dresse un classement sous forme de comparatif. Près de 150 tests sont ainsi lancés pour pouvoir établir ces résultats.

  http://www.matousec.com/projects/proactive-security-challenge/results.php

Comment se procurer un pare-feu

- Il existe un certain nombre de pare-feu logiciels gratuits disponibles au téléchargement. Même si l'on peut parfois se poser des questions sur la qualité des produits gratuits, cette solution est certainement meilleure que l'absence de pare-feu.

Product	Product score	Level reached	Protection level	Recommendation	Report	Award
Comodo Internet Security 4.0.141842.828 FREE	100 % / 148	10+	Excellent – 100 %	GET IT NOW!		
Online Solutions Security Suite 1.5.14905.0	99 % / 148	10+	Excellent	GET IT NOW!		
Outpost Security Suite Free 7.0.4.3418.520.1245.401 FREE	97 % / 148	10+	Excellent	GET IT NOW!		
Outpost Security Suite Pro 7.0.1.3376.514.1234.401	97 % / 148	10+	Excellent	GET IT NOW!		
Kaspersky Internet Security 2011 11.0.1.400	92 % / 148	10+	Excellent	GET IT NOW!		
Malware Defender 2.6.0	90 % / 148	10	Very good	N/A		
Privatefirewall 7.0.21.1 FREE	86 % / 148	9	Very good	N/A		
BitDefender Internet Security 2011 14.0.24.330	84 % / 148	10+	Very good	GET IT NOW!		
ZoneAlarm Extreme Security 9.1.008.000	59 % / 148	7	Poor	*Not recommended*		–

Source : http://www.matousec.com/projects/proactive-security-challenge/results.php

Les Anti-adwares et spywares

- Les adwares et les spywares doivent pouvoir être extraits des ordinateurs qu'ils colonisent puisqu'ils contribuent à les rendre moins stables, ou à diffuser des informations que tout le monde n'a pas à connaître.
- Certains anti-spywares sont gratuits, d'autres sont payants. Se renseigner sur l'efficacité de ces produits avant d'opter pour l'un ou l'autre d'entre eux.

http://www.clubic.com/article-127290-10-guide-comparatif-antispyware.html

http://www.generation-nt.com/anti-spyware-antispyware-gratuit-meilleur-test-comparatif-adware-trojan-vers-dialer-bot-malware-article-69694-6.html

Anti-SPAM

- La lutte contre les spam passe principalement par la prudence.
- Un certain nombre de logiciels anti-spam sont toutefois disponibles. La plupart d'entre eux doivent être **installés sur les serveurs de courrier électronique**.
- Certains fournisseurs d'accès à Internet fournissent un service anti-spam gratuit ou payant.
- **La prudence est de rigueur** : la meilleure façon de ne pas être la victime des spam est de **ne pas les attirer**.
  - Des robots parcourent sans relâche les pages du web, à la recherche d'adresses électroniques auxquelles il sera possible d'envoyer des publicités
  - L'inscription à un service gratuit demande de fournir une adresse électronique valide : celle-ci sera peut-être revendue.
  - L'achat d'un article en ligne suppose de donner une adresse électronique ? Des courriers provenant du vendeur sont à attendre.

Anti-SPAM

- **Les solutions**
  - Ne pas donner sa vraie adresse électronique quand ce n'est pas indispensable.
  - Utiliser une adresse électronique « poubelle » dont on accepte qu'elle soit spammée un jour. A ce moment, on l'abandonne.
  - Utiliser une adresse électronique jetable : jetable.org, SpamGourmet, Trashmail, HaltoSpam, ...
  - NE JAMAIS se désinscrire lorsqu'un spam vous arrive et vous propose une solution de désinscription pour ne plus recevoir d'autres courriers.
  - Si vous vous désinscrivez, vous indiquez par la même occasion que votre adresse électronique est valide. Votre adresse prend donc de la valeur commerciale et vous recevrez d'autant plus de spam
  - *Cette dernière remarque n'est pas forcément valable dans les pays où une loi anti-spam existe.*

Les logiciels Anti-SPAM

- Des logiciels clients de courrier électronique intègrent une fonction qui lui permet de séparer automatiquement le spam du courrier normal.
  - Thunderbird
  - Windows Live mail
- Des logiciels du commerce permettent de séparer le courrier commercial non sollicité de son précieux courrier personnel. Ils sont disponibles dans le commerce.
- Certains logiciels libres ou gratuits sont disponibles au téléchargement.
  - http://www.mailwasher.net/
  - http://spambayes.sourceforge.net/

Eradication du virus PEBCAK

- Virus PEBCAK

  Acronyme de "Problem Exist Between Chair And Keyboard“
- Le problème se situe exactement entre la chaise et le clavier
- Continuez à vous conduire en Gogo naïf ou Cliqueur fou face au côté obscur d’Internet !
- **Vous êtes le problème !**

=> Quelques règles de comportement qui relèvent du **simple bon sens**

Comportement à adopter en tout temps

Utiliser des logiciels moins sensibles

- Les logiciels Microsoft sont extrêmement répandus. Ils en deviennent donc des cibles privilégiées pour les pirates et tous les logiciels malveillants.
- On pourra éviter une grande partie des risques en utilisant des logiciels moins répandus
  - Système d'exploitation: Linux, MacOS, ...
  - Navigateur web : Firefox, Opera,...
  - Logiciel de courrier électronique : Thunderbird
- Il est important de télécharger très rapidement les mises à jour de son système d'exploitation. Lorsqu'une faille de sécurité est trouvée, elle est généralement très vite utilisée par les logiciels malveillants.

Comportement à adopter en tout temps

- **Eviter les logiciels piratés**
- Il n'existe évidemment aucune garantie quant au bon fonctionnement de logiciels piratés.
- Aucune garantie non plus qu'ils ne contiennent pas de logiciel malveillant.
- Ceux qui cherchent à se procurer des logiciels de qualité sans dépenser des centaines d'Euros pour équiper leur ordinateur se tourneront volontiers vers le logiciel libre.
- Il est souvent gratuit et, le code source étant publié, il ne contient jamais de virus ou autre peste.
- Logiciels libres : http://www.framasoft.net/

Comportement à adopter en tout temps

Etre prudent avec les logiciels gratuits

- De nombreux logiciels gratuits n'ont cette qualité que parce qu'ils sont rentabilisés par la publicité qu'ils permettent de faire.
- Spywares et Adwares accompagnent souvent ce type de logiciels.
- Il existe cependant de nombreux logiciels gratuits de qualité. Il faut toujours bien s'informer avant d'installer un tel logiciel.

Comportement à adopter en tout temps

- **Eviter les téléchargements sur les réseaux d'échanges de fichiers**
- Les réseaux d'échanges du type Kazaa, eMule, Torrent, sont extrêmement tentants pour ceux qui recherchent des programmes, des films ou de la musique... sans débourser un €.
- Malheureusement, un grand nombre de virus, vers et autres pestes y attendent patiemment d'être téléchargés et, à nouveau, échangés.
- La plus grande prudence s'impose.

Comportement à adopter en tout temps

- **Ne pas faire de sa machine un laboratoire d'essais**
- Ne pas installer sans cesse tous les nouveaux trucs qui sortent.
- Plus encore : n'installez jamais, dès leurs sorties, les nouvelles versions de vos applications déjà installées.
- Il faut toujours attendre plusieurs mois (3 à 6 mois)
  - que les bogues et les failles de sécurité aient été découvertes et au moins partiellement corrigées,
  - que les additifs malveillants aient été découverts et contrecarrés.

Comportement à adopter en tout temps

- **Ne jamais révéler d'informations personnelles sur Internet**
- Ne donnez que des informations fausses :
  - fausse adresse, faux numéros de tout, faux âge,
  - faux profil, faux métier, faux revenus,
  - faux nombre de personnes au foyer,
  - faux niveau d'équipement
  - etc.
- Ayez plusieurs adresses e-mail poubelles
- Ne répondez jamais aux spammeurs !

Comportement à adopter en tout temps

- **Réactions à avoir face à la découverte d'un parasite**
- La présence, sur une machine, de parasites ou d'outils apparemment anodins, mais inattendus, ne doit pas être prise à la légère
- Agir dans 3 directions différentes simultanément
  - **Corriger les effets** : corriger immédiatement les effets de la contamination et supprimant la contamination elle-même mais cela ne suffit pas.
  - **Rechercher la causes en amont**
  - **Prévoir les conséquences en aval** : chercher les conséquences éventuelles de son action à l'encontre de notre machine, nos données, notre réseau, notre entreprise et nous même

Comportement à adopter en tout temps

- **Au travail, ayez un comportement en accord avec le contrat qui vous lie à votre employeur**
- Sachez que vous pouvez être surveillé
- Ne faites jamais à autrui ce que vous ne voudriez pas que l'on vous fasse.
- Mettez-vous à la place de votre employeur : trouverez-vous normal que les gens que vous salariez en échange d'un travail, utilisent les ordinateurs que vous avez achetés pour chatter, télécharger de la musique, surfer sur des sites pornographiques, rédiger du courrier personnel, etc. ?

Comportement à adopter en tout temps

- **Evaluez froidement la perte de vos disques durs avec tous les programmes et toutes les données qui y sont stockées, classées**
- Quelles tranches de vie, privées ou professionnelles, risquez-vous en n'étant pas protégé ?
- Quel serait le coût de reconstruction de ces données si tant-est qu'elles puissent l'être ?
- Ayez toujours une conscience aiguë du risque et de cette évaluation.
- Soyez Pro : faites des sauvegardes et protégez correctement votre machine.
- En somme, conduisez-vous en adulte responsable.

Pour en savoir plus :

http://assiste.com.free.fr/index.html