Malwares

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 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 crédit ? »

- 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.

**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

Virus Informatique

- 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,...

Virus Informatique

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.

Virus Informatique

Effets des virus

- 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.

Virus Informatique

Comment les virus se transmettent -ils ?

- Les 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. ..

Virus Informatique

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.

Virus Informatique

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.

Le Ver Informatique

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, ...

Le Ver Informatique

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.

Le Ver Informatique

Exemple de vers

- **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.
- 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.

Chevaux de Troie

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

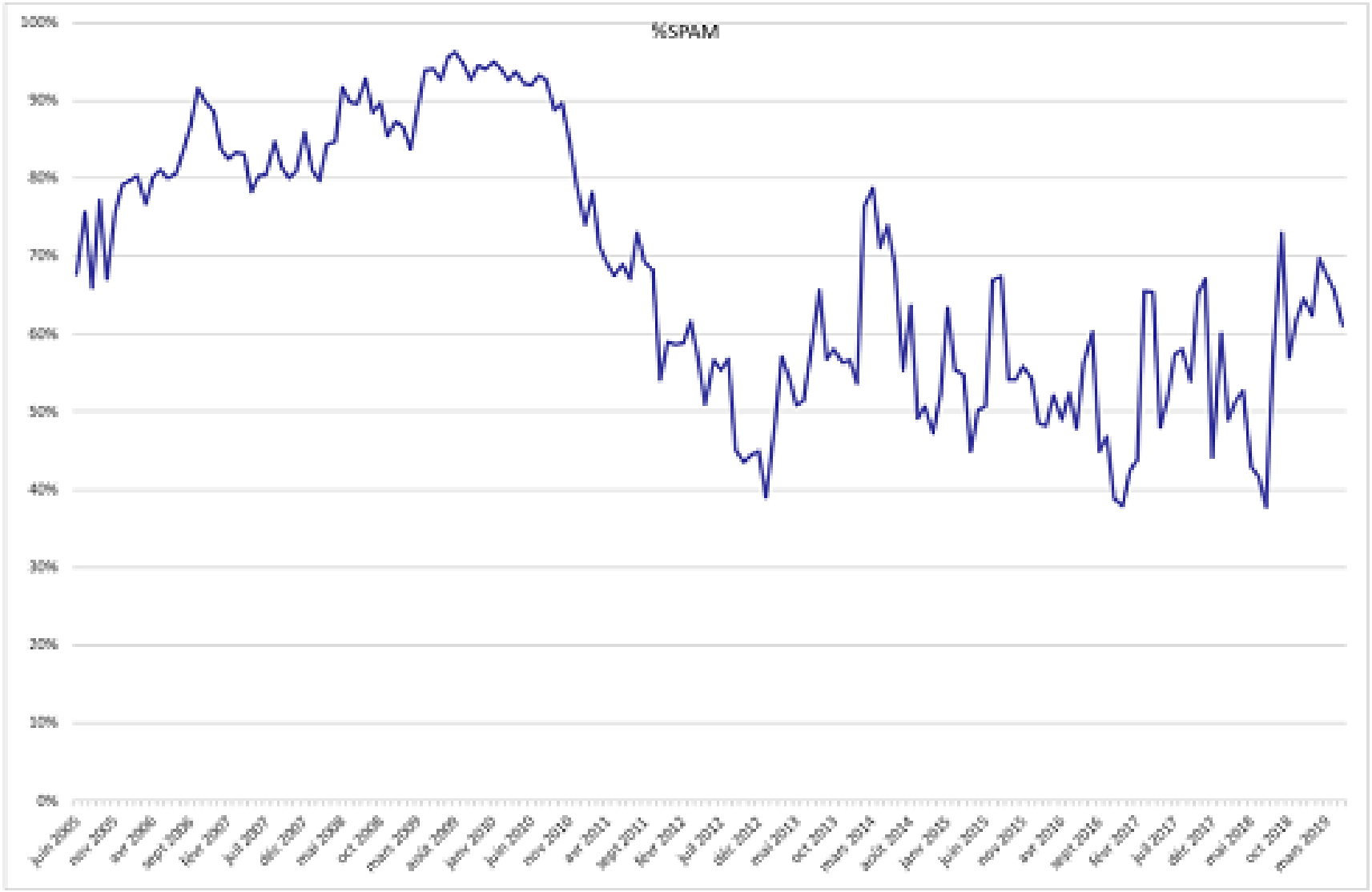
- Sur un réseau, un cheval de Troie est vraisemblablement utilisé pour espionner et voler des informations sensibles (espionnage industriel). Les intérêts des agresseurs peuvent inclure :
- Tous détails des comptes (mots de passe email, connexion à distance, services Web, etc.)
- Documents confidentiels
- 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).

Utilisation des Chevaux de Troie / Backdoor

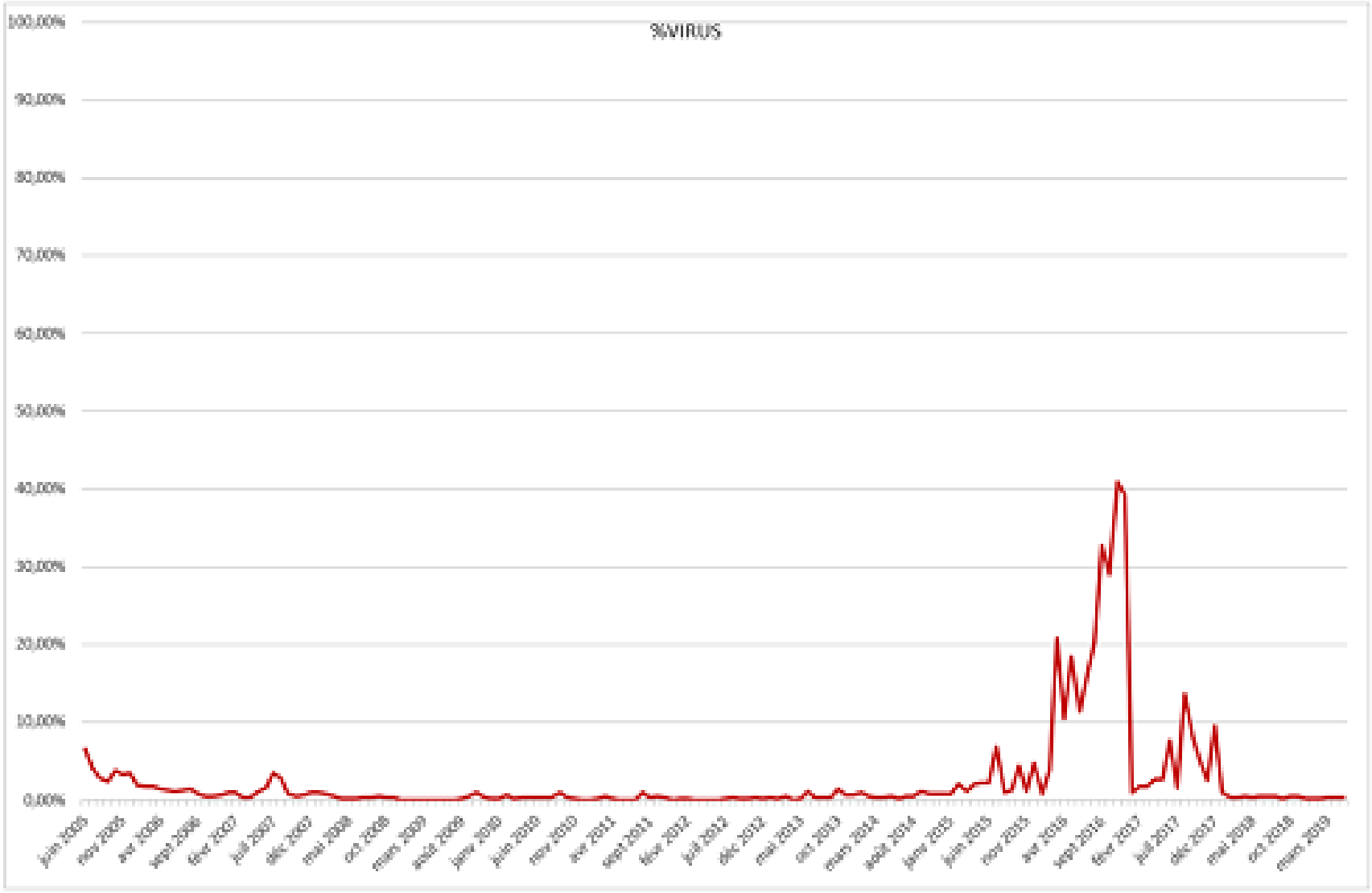
- Sur un réseau, un cheval de Troie est vraisemblablement utilisé pour espionner et voler des informations sensibles (espionnage industriel). Les intérêts des agresseurs peuvent inclure :
- Tous détails des comptes (mots de passe email, connexion à distance, services Web, etc.)
- Documents confidentiels
- 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.

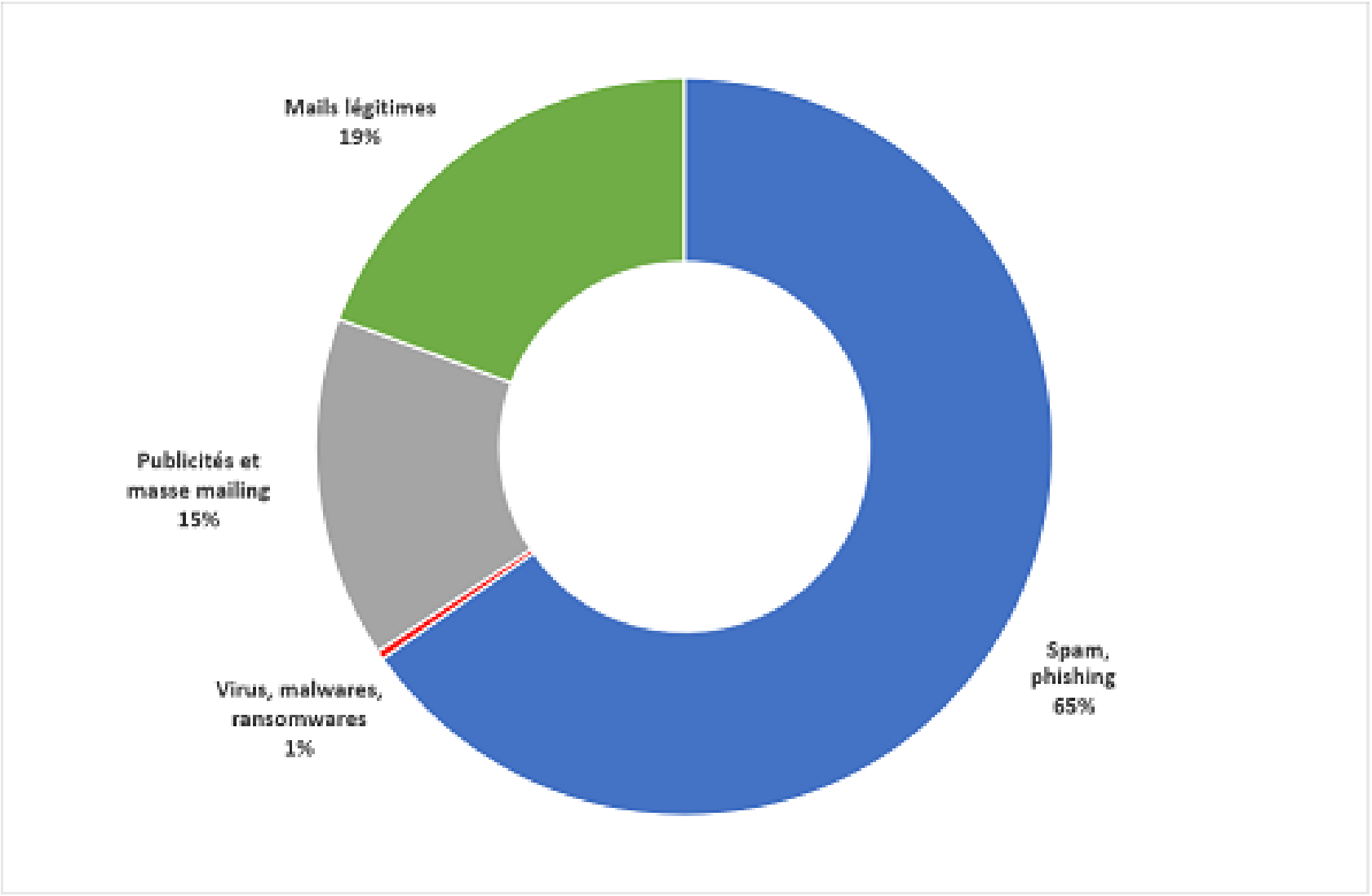

%SPAM
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
juin 2005
nov 2005
avr 2006
sept 2006
févr 2007
juil 2007
déc 2007
mai 2008
oct 2008
mars 2009
août 2009
janv 2010
juin 2010
nov 2010
avr 2011
sept 2011
févr 2012
juil 2012
déc 2012
mai 2013
oct 2013
mars 2014
août 2014
janv 2015
juin 2015
nov 2015
avr 2016
sept 2016
févr 2017
juil 2017
déc 2017
mai 2018
oct 2018
mars 2019

Évolution du taux de spams et de phishing depuis 2005

- En 2005, le taux moyen de spam représentait environ 70% du nombre total des emails reçus.
- Pendant l'année 2009, un pic significatif a frôlé 96% de spams sur les mois de juillet et d'août.
- Grâce au démantèlement de botnets, le nombre de spams a fortement diminué entre 2010 et 2012.
- Les spams étaient moins nombreux, mais se sont complexifiés.
- Depuis 2013, nous voyons une fluctuation du taux de spams qui varie entre 50 % et 60 % en moyenne, et frôle de temps en temps les 70 à 80% du trafic mail.
- La moyenne sur le 1er semestre 2019 étant à 65,26%.

Évolution du ratio de malwares dans les emails




Mails légitimes
19%
Publicités et
masse mailing
15%
Virus, malwares,
ransomwares
1%
Spam,
phishing
65%

- Il apparaît donc qu'actuellement, la situation est à peu près stable : la menace malware est au plus bas.
- Cela est certainement lié à l'efficacité des systèmes antivirus qui permettent de rapidement contrer chaque attaque.
- À moins que ce soit le calme avant la tempête…
- Le flux de spams en revanche reste très élevé, en partie dû au fait que le procédé compte par définition sur la masse de messages envoyés.
- Malgré un taux infime de retour de destinataires, l'envoi en masse de spams reste rentable.

Spyware (ou espiogiciel)

- Les spywares font partie des nouveaux fléaux du simple, 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
- Parmi 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'es t pas connecté à Internet.
- Il 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

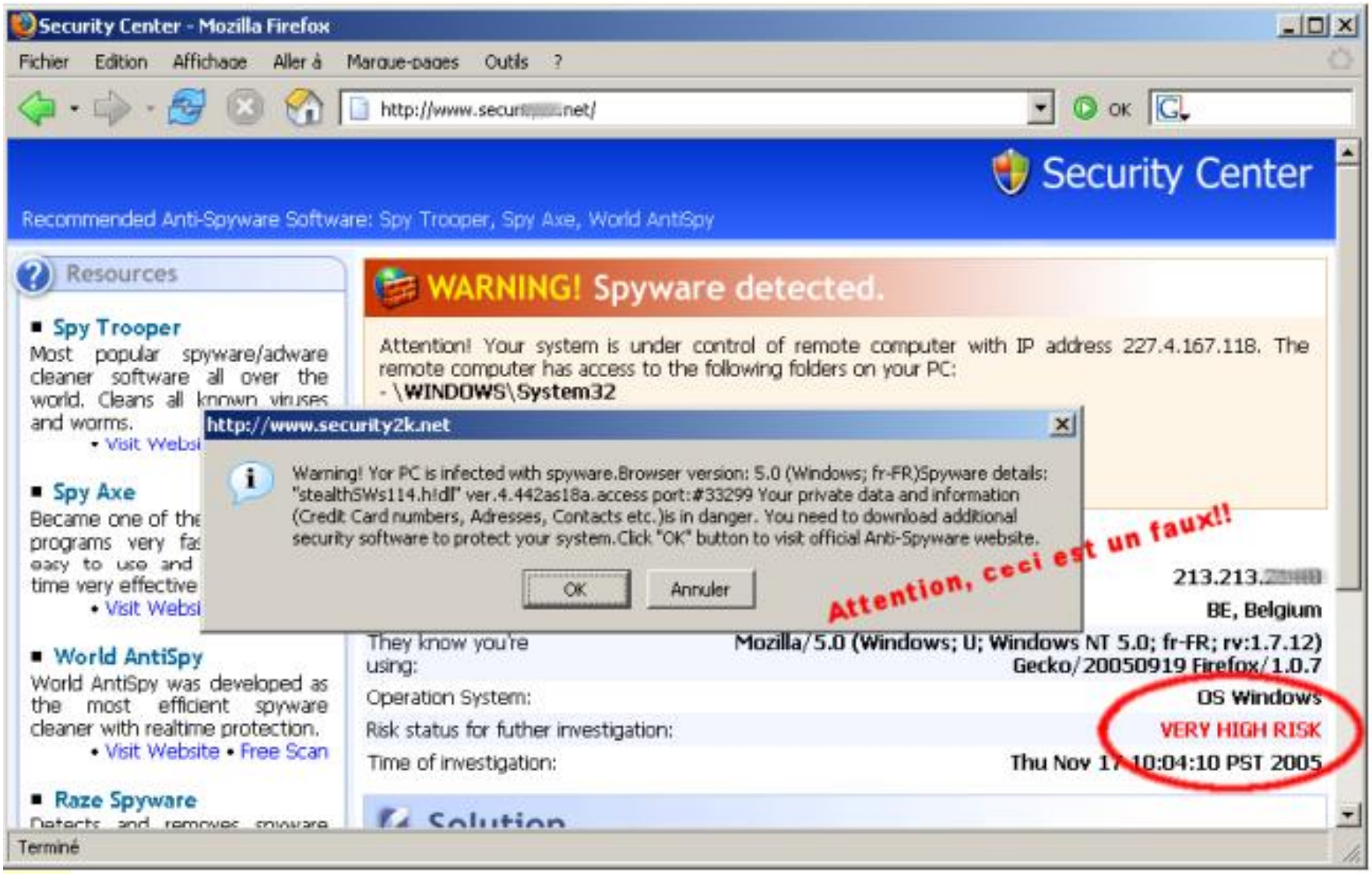
- Il suffit que le niveau de sécurité du navigateur web soit trop faible. Des logiciels peuvent alors s'installer sans prévenir.
- Dans d'autres cas, l'utilisateur clique trop facilement sur le bouton qui donne son accord sans avoir compris à quoi il s'engage.

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, 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)

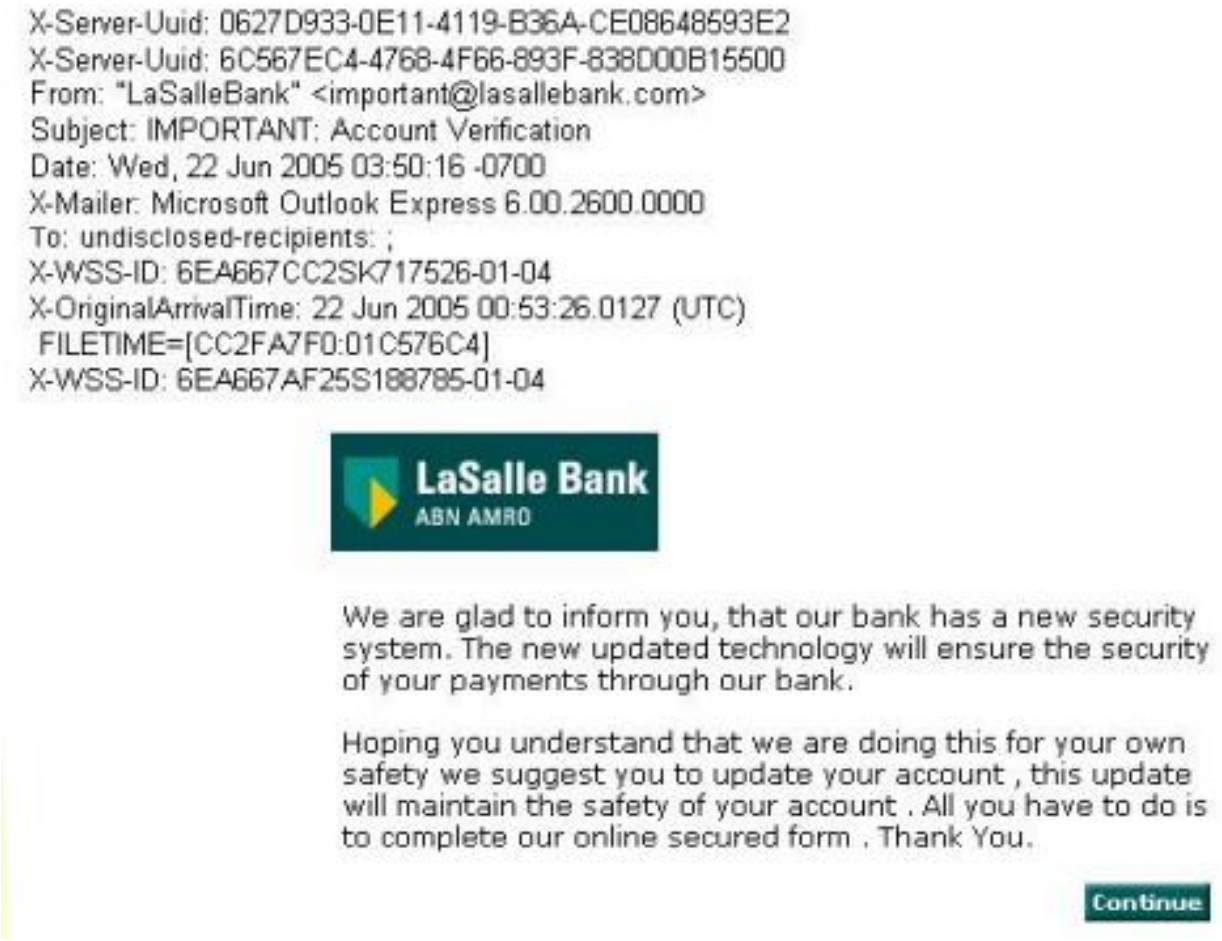
- Un dialer peut être une application tout à fait honnête. Pour obtenir une information, pour acheter un produit ou un service, on vous propose d'appeler un numéro de téléphone surtaxé (si usage d’un modem).
- Le fournisseur de service peut vous proposer de télécharger un petit logiciel qui se chargera 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.

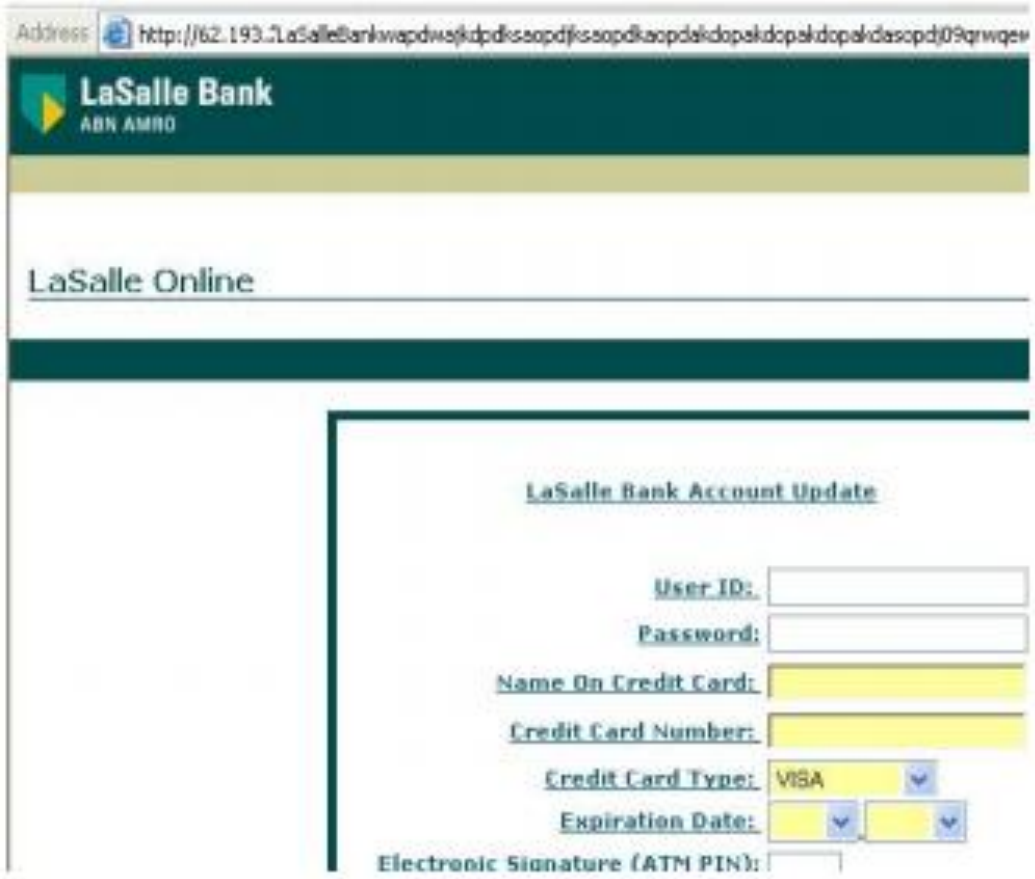
Exemple de phishing

- 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


Address
http://62.193.7LaSalleBankwapdwejkdpdkssopdjkssopdkaopdakdopakdopakdopakdascpdj09qrwqew
LaSalle Bank
ABN AMRO
LaSalle Online
LaSalle Bank Account Update
User ID:
Password:
Name On Credit Card:
Credit Card Number:
Credit Card Type:
VISA
Expiration Date:
Electronic Signature (ATM PIN):

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 (ou pourriel)

- 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 (ou pourriel)

- 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

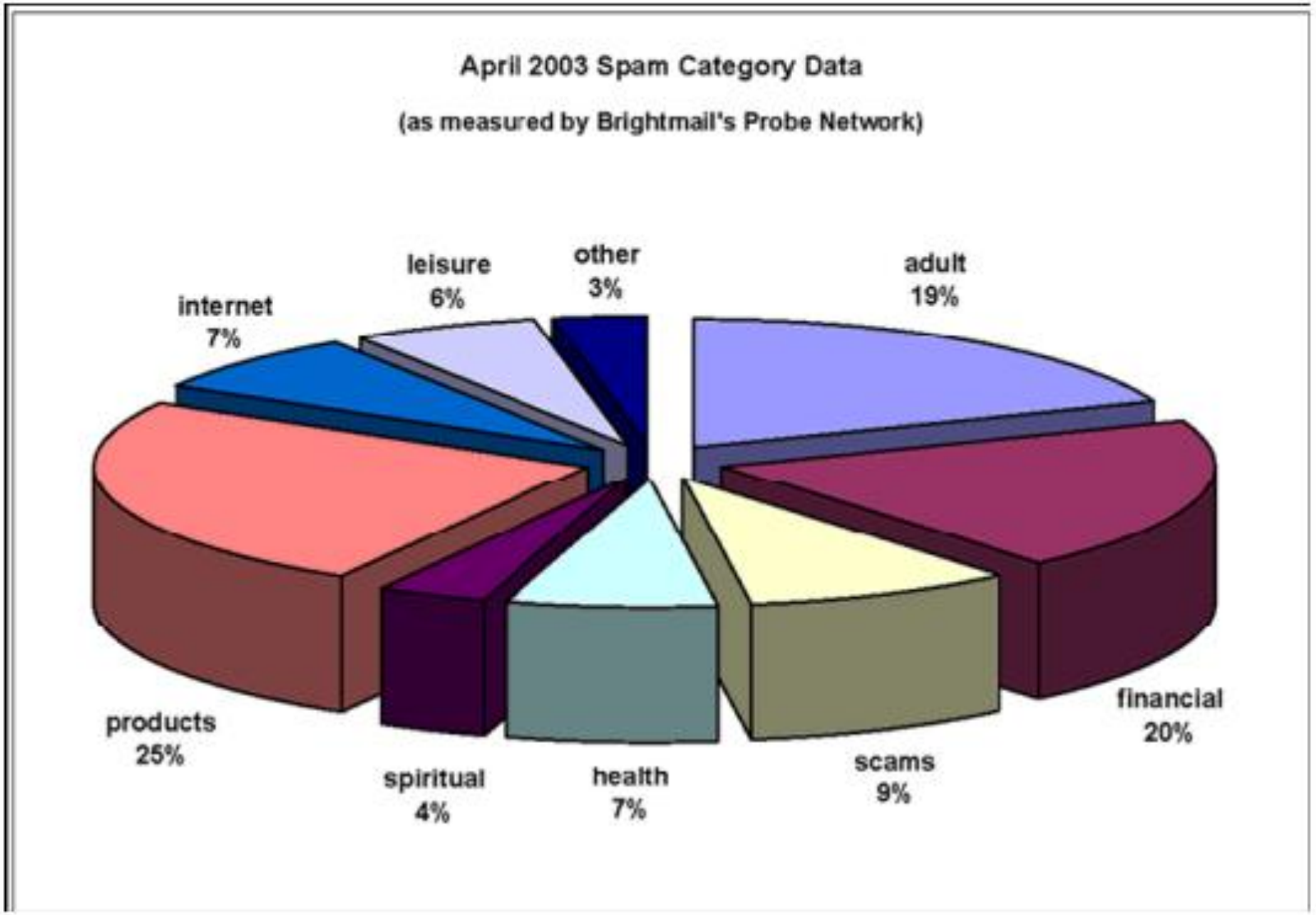
  - Son détournement est illégal

  -Son détournement par un fonctionnaire est considéré comme plus grave

Les différentes catégories de Spam

- 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

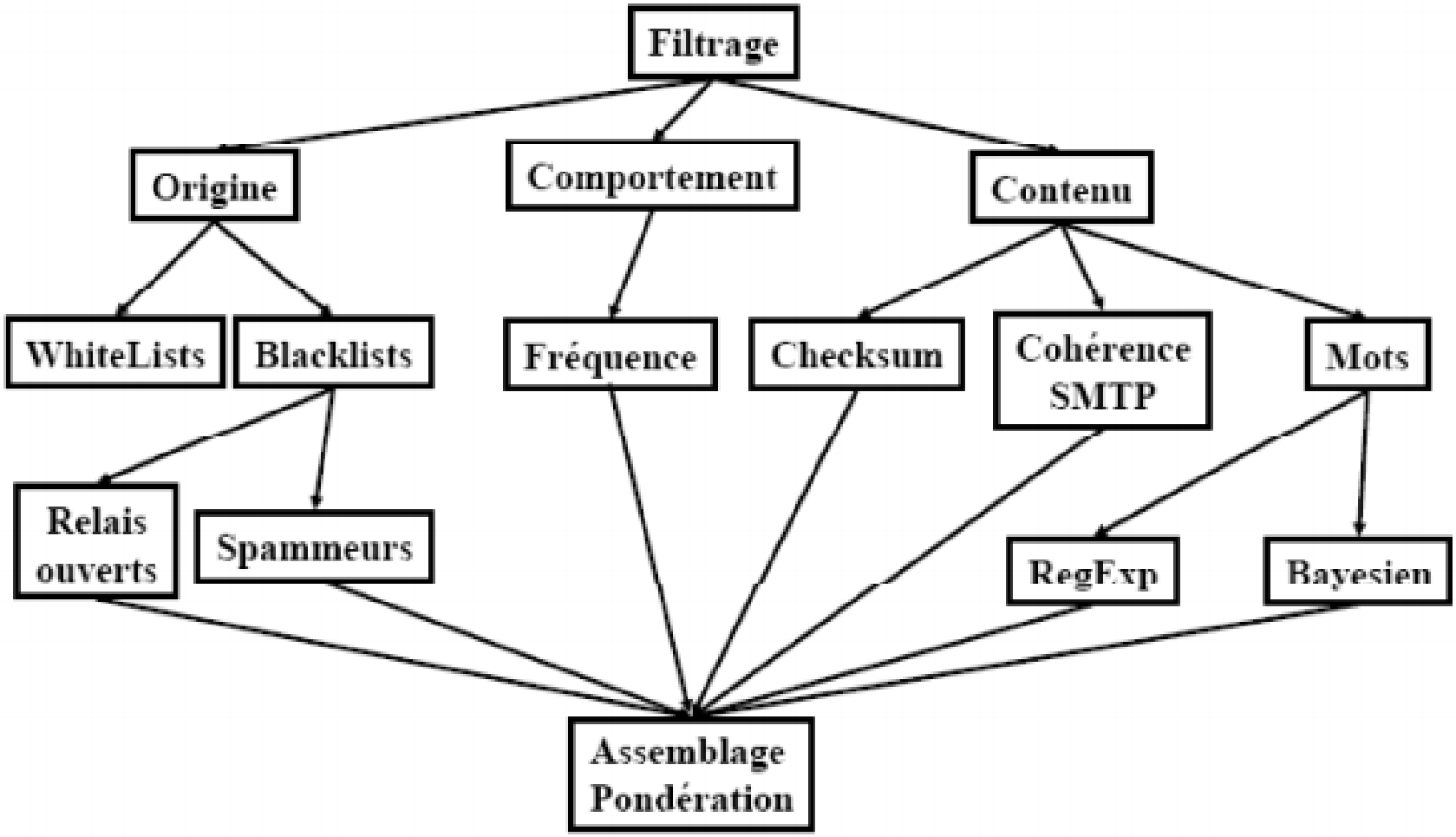
- Il ne coûte rien au spammeur
- Coûte plus de 10 milliards d'Euros par an en Europe => un marché est apparu : combattre les SPAMS.
- Des sociétés sont présentes sur ce secteur et ont été rejointes par les éditeurs d'antivirus

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 message.
  - 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 message doit être considéré comme un spam

Filtrage : De nombreux critères



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

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 : 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

- Certains comportements lors de l'utilisation de l'Internet ne sont pas sans poser de problèmes à cause des dangers qu'ils représentent:
- 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.