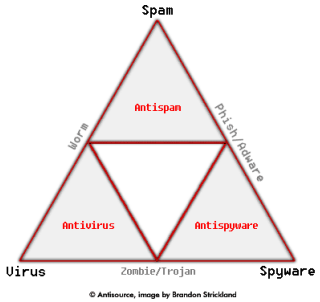
Security Competency

CyberDefense : Nouvelles menaces, nouvelles parades…

4ème Forum des Architectes – La Sécurité Informatique



Serge RICHARD, Architecte Sécurité - CISSP®

Objectifs de la session

Dans le passé, les pirates informatiques étaient mus par le désir de se faire valoir alors qu'aujourd'hui, de nombreuses menaces viennent d'activités criminelles inspirées par l'appât du gain. La nature des menaces évolue et les entreprises doivent s'adapter.

Les objectifs de cette session sont de :

- ✓ **Décrire les événements et les tendances de ces derniers mois**
- ✓ **Décrire les stratégies à mettre en place**
- ✓ **Décrire l'évolution des menaces pour les prochains mois**

Agenda

- ✓ Le petit glossaire de la CyberDefense
- ✓ Evénements et tendances
- ✓ Architecture de sécurité pour l'entreprise
- ✓ Evolutions des menaces
- ✓ Questions/Réponses

Le petit glossaire de la CyberDefense

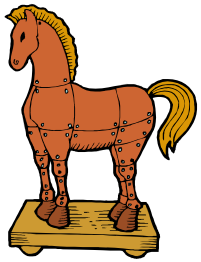
Les principes

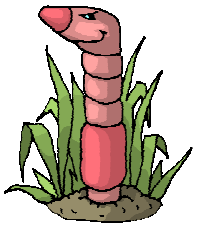
✓ Vulnérabilité (Vulnerability) :

Le terme vulnérabilité se réfère à une faiblesse dans un système, permettant à un attaquant de porter atteinte à la sécurité d'une information ou d'un système d'information. On parle aussi de faille de sécurité informatique.
Les vulnérabilités peuvent résulter d'une erreur de programmation ou d'une faiblesse de conception dans le système. Celles-ci peuvent n'exister qu'en théorie, ou bien peuvent avoir un exploit connu. Elles deviennent particulièrement intéressantes lorsqu'un programme contenant une de ces vulnérabilités est lancé avec des privilèges spéciaux, qu'il permet une authentification sur un système, ou bien encore lorsqu'il fournit un accès à des données sensibles.

✓ Logiciel malveillant (Malware) :

C'est un logiciel développé dans le but de nuire à un système informatique. Les virus et les vers sont les deux exemples de logiciels malveillants les plus connus.
Logiciel malveillant est une traduction de l'anglais malware qui est lui même un mot-valise, contraction de malicious (malveillant et non malicieux) et software (logiciel).





Les logiciels malveillants (1/4)

- **Virus (Virus) :**

Un virus informatique est un logiciel malveillant écrit dans le but de se dupliquer sur d'autres ordinateurs. Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, les clefs USB, etc.

Son appellation provient d'une analogie avec le virus biologique puisqu'il présente des similitudes dans sa manière de se propager et de se reproduire.

- **Vers (Worm) :**

Un ver informatique est un logiciel malveillant qui se reproduit sur des ordinateurs à l'aide d'un réseau informatique comme l'Internet.

Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources afin d'assurer sa reproduction.

La définition d'un ver s'arrête à la manière dont il se propage de machine en machine, mais le véritable but de tels programmes peut aller au delà du simple fait de se reproduire : espionner, offrir un point d'accès caché (porte dérobée), détruire des données, faire des dégâts, envoi de multiples requêtes vers un site internet dans le but de le saturer, etc. Les effets secondaires peuvent être aussi un ralentissement de la machine infectée, ralentissement du réseau, plantage de services ou du système, etc.

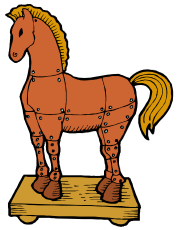
Les logiciels malveillants (2/4)

- **Wabbit (Wabbit) :**

Un wabbit est un type de logiciel malveillant qui s'auto-réplique. Contrairement aux virus, il n'infecte pas les programmes ni les documents. Contrairement aux vers, il ne se propage pas par les réseaux.

- **Chevaux de Troie (Trojan horses) :**

Ce nom vient de la célèbre ruse imaginée par Ulysse. Ces programmes prétendent être légitimes (souvent de petits jeux ou utilitaires), mais comportent des routines nuisibles exécutées sans l'autorisation de l'utilisateur. Les chevaux de Troie ne sont pas des virus car il leur manque la fonction de reproduction, essentielle pour qu'un programme puisse être considéré comme un virus.



- **Porte dérobée (Backdoor) :**

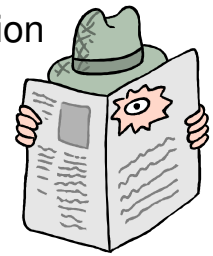
C'est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. En sécurité informatique, la porte dérobée peut être considérée comme un type de cheval de Troie. Une porte dérobée peut être introduite soit par le développeur du logiciel, soit par un tiers, typiquement un pirate informatique. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle (par exemple, par contournement de l'authentification). Enfin, selon l'étendue des droits que le système d'exploitation donne au logiciel contenant la porte dérobée, le contrôle peut s'étendre à l'ensemble des opérations de l'ordinateur.

Les logiciels malveillants (3/4)

- **Logiciel espion (Spyware) :**

C'est un logiciel (espiogiciel, mouchard) qui infecte un ordinateur dans le but de collecter et de transmettre à des tiers des informations de l'environnement sur lequel il est installé, sans que l'utilisateur n'en ait connaissance.

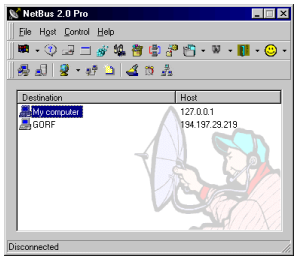
L'essor de ce type de logiciel est associé à celui d'Internet, qui sert de moyen de transmission des données.



- **Exploitation (Exploit) :**

Dans le domaine de la sécurité informatique, un exploit est un programme permettant à un individu d'exploiter une faille de sécurité informatique dans un système d'exploitation que ce soit à distance (remote exploit) ou sur la machine sur laquelle cet exploit est exécuté (local exploit).

Prononcer comme en anglais « explo-ï-te » et non « exploi », le mot provenant de exploitation (de faille informatique) et non pas du fait de réaliser un quelconque exploit extraordinaire.



Les logiciels malveillants (4/4)

- **Programme malveillant Furtif (Rootkit) :**

C'est un programme ou ensemble de programmes permettant à un pirate de maintenir - dans le temps - un accès frauduleux à un système informatique. Le pré-requis du rootkit est une machine déjà compromise.

Un rootkit s'utilise après une intrusion et l'installation d'une Backdoor afin de camoufler tous les changements effectués lors de l'intrusion. Ainsi l'on peut préserver l'accès à la machine un maximum de temps, en effet les rootkits sont difficilement détectables et seule une analyse forensique approfondie peut en révéler la présence.

Les « rootkit » opèrent une suite de modifications, notamment au niveau des commandes système, voire du noyau.

- **Publiciel (Adware) :**

C'est un logiciel propriétaire gratuit (graticiel) dont le créateur conserve les droits d'auteur, mais ne réclame aucune redevance pour son utilisation.

Le propriétaire reçoit une compensation car le logiciel est financé par la publicité qu'il affiche, ce qui lui permet de distribuer sa création gratuitement.

Le mot publiciel vient de publicité et logiciel. Le terme anglais adware vient de advertising supported software.

Des vecteurs de diffusion (1/2)

✓ Pourriel (SPAM) :

Cela désigne les communications électroniques massives, notamment de courrier électronique, non sollicitées par les destinataires.

Le spam peut appartenir aux catégories suivantes :

- Messages publicitaires
- Messages politiques
- Appels à la charité
- Arnaques financières
- Chaînes de courriels
- Faux spam destiné à distribuer des logiciels malveillants

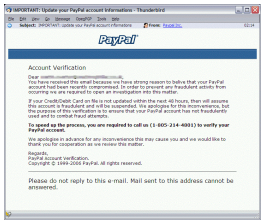
✓ Hameçonnage (Phishing) :

C'est une forme d'attaque informatique consistant à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des données confidentielles : mot de passe, numéro de carte de crédit, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale ainsi que des courriers électroniques et des sites Web falsifiés

Le terme phishing viendrait de la contraction de phone et fishing : « téléphone » et « pêche

Originellement le phishing c'est l'arnaque téléphonique qui consiste à se faire passer pour quelqu'un d'autre.

Des vecteurs de diffusion (1/2)



- **Pharming (Pharming) :**

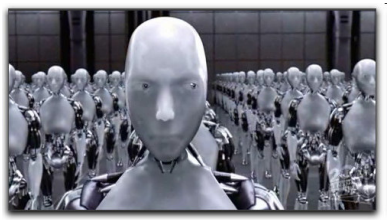
Escroquerie visant à rediriger des internautes vers de faux sites web malgré la saisie d'une URL valide. Le pharming consiste à manipuler la résolution du nom via DNS ou par configuration locale (Hosts-File), dans le but de rediriger l'utilisateur sur un serveur falsifié et d'accéder ainsi à des données confidentielles (données d'ouverture de session).

Si le pharming, peut sembler similaire au hameçonnage (Phishing), cette technique est toutefois plus insidieuse car vous pouvez en plus, être redirigé vers un faux site Web à votre insu.

- **Botnet / Zombies (Botnet / Zombies) :**

Ce sont des réseaux de PC infectés par des virus informatiques ou par des chevaux de Troie, contrôlés via Internet le plus souvent à des fins malveillantes. Une ou plusieurs personnes prenant le contrôle de toutes les machines infectées obtiennent ainsi une capacité considérable.

En plus de servir à paralyser le trafic (attaque par déni de service), de moteur à la diffusion de spam, les botnets peuvent également être utilisés pour commettre des délits comme le vol de données bancaires et identitaires à grande échelle. Les botnets sont plus à l'avantage d'organisations criminelles (mafieuses) que de pirates isolés, et peuvent être même loués à des tiers peu scrupuleux.



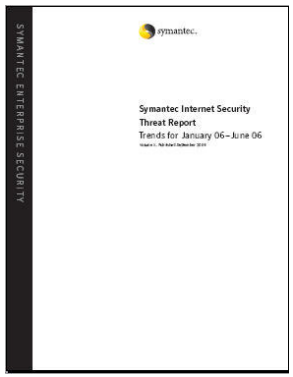
Evénements et tendances

Sources

- **IBM :**
  Security Threats and Attack Trends Report

- **McAfee :**
  Global Threat Report

- **Symantec :**
  Internet Security Threat Report



Pays à l'origine des attaques

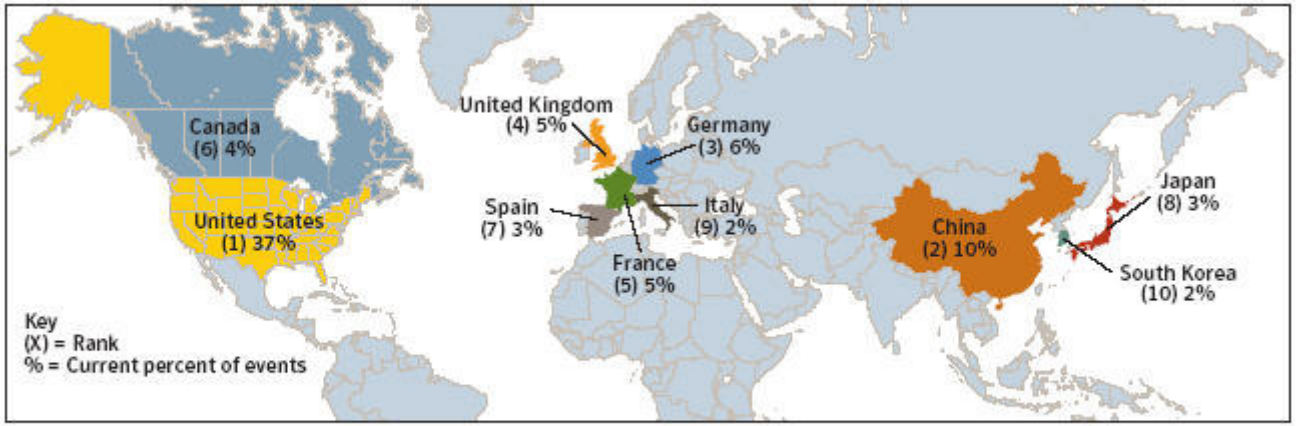


Figure 15. Top originating countries
Source: Symantec Corporation

- **Analyse :**
  Ce schéma montre l'origine des attaques, mais ce n'est pas forcement l'origine de l'attaquant.

  La position de numéro des Etats-Unis est dû en autre à une forte augmentation de l'accès à internet des utilisateurs américains.

Top 10 des cibles

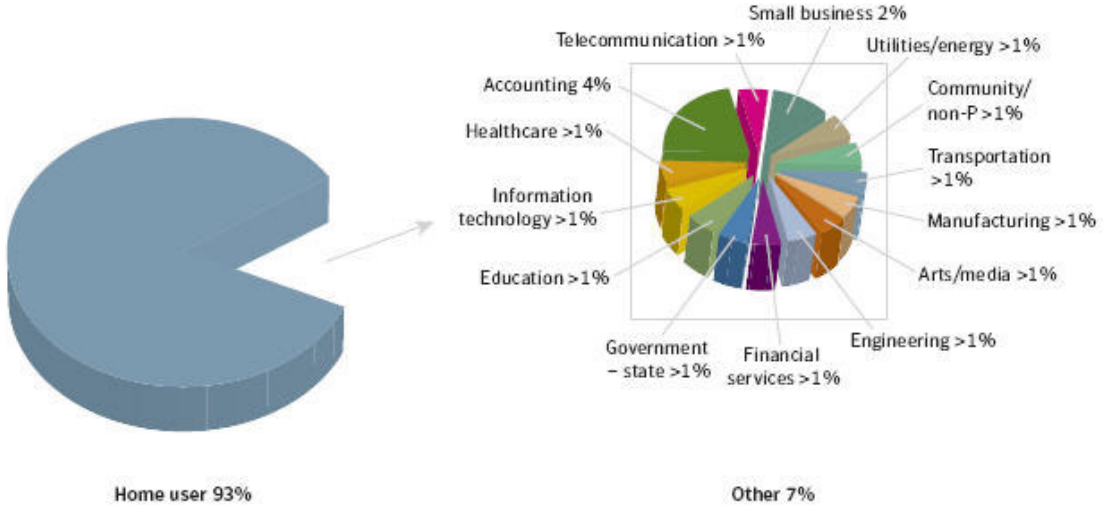


Figure 41. Industry representational breakdown
Source: Symantec Corporation

- **Analyse :**

  86% des attaques ont pour cible les PCs des utilisateurs. Cela est dû au fait que de plus en plus d'utilisateurs ont une connexion internet à la maison.

  14% des attaques ont pour cible le secteur financier. Cela est dû à l'appât du gain.

Volumes par logiciels malicieux

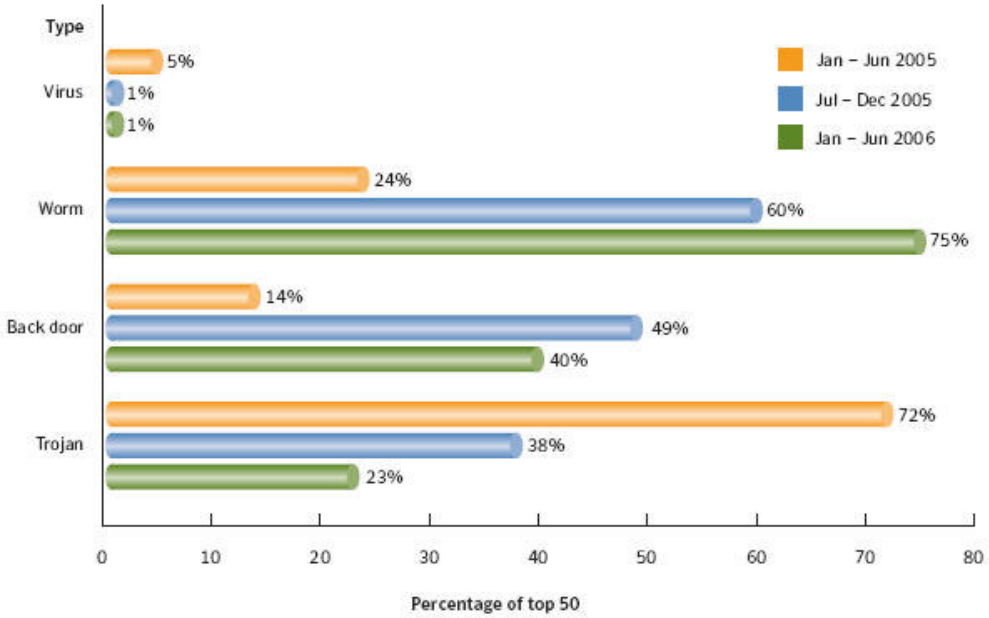


Figure 27. Malicious code types by volume
Source: Symantec Corporation

- **Analyse :**

  Il apparait qu'il n'existe pratiquement plus de logiciel malicieux de type Virus.

  Par contre le nombre de logiciels malicieux de type Vers explose.

Vecteurs de diffusion

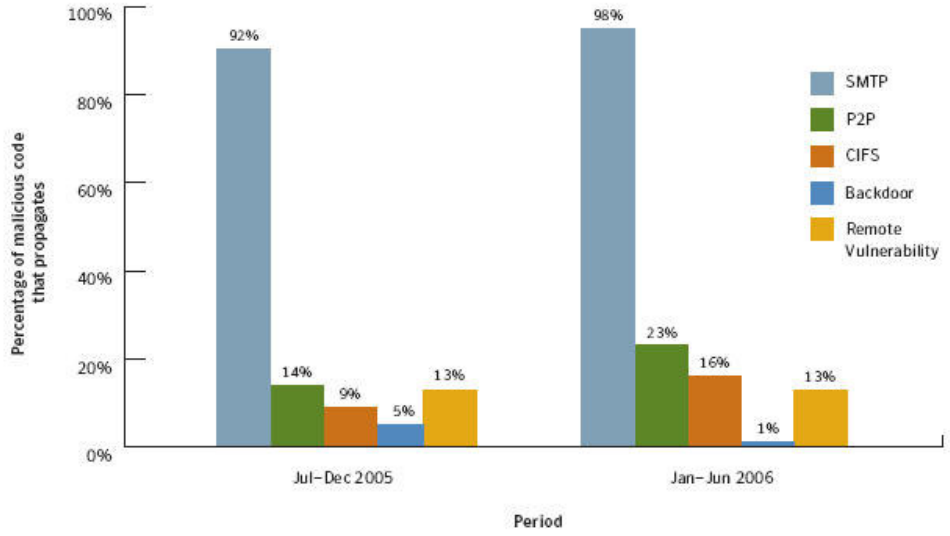


Figure 34. Malicious code propagation vectors
Source: Symantec Corporation

- ✓ **Analyse :**

  La messagerie est un vecteur important de diffusion des logiciels malicieux.

  Les logiciels P2P ainsi que CIFS (partage de fichier Windows) sont des vecteurs à ne pas négliger.

Situation sur les réseaux Bot

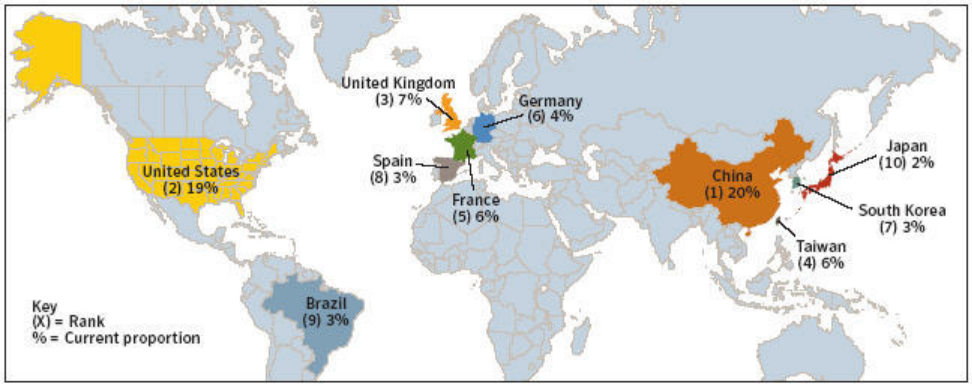


Figure 13. Top countries by bot-infected computers
Source: Symantec Corporation

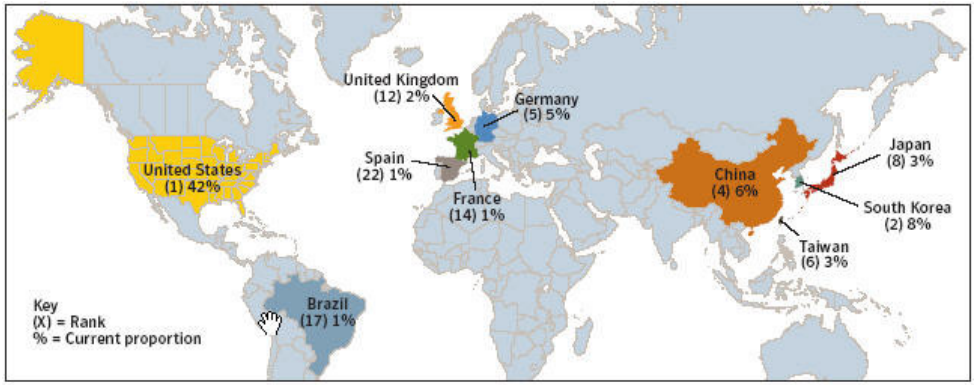


Figure 14. Distribution of command-and-control servers in top ten bot-infected countries
Source: Symantec Corporation

- ✓ **Analyse :**
  La Chine a le plus nombre d'ordinateur compromis.

  Mais ce sont les Etats-Unis qui ont le plus grand nombre de « centre de commande » des ordinateurs compromis.

Attaques Phishing par secteur

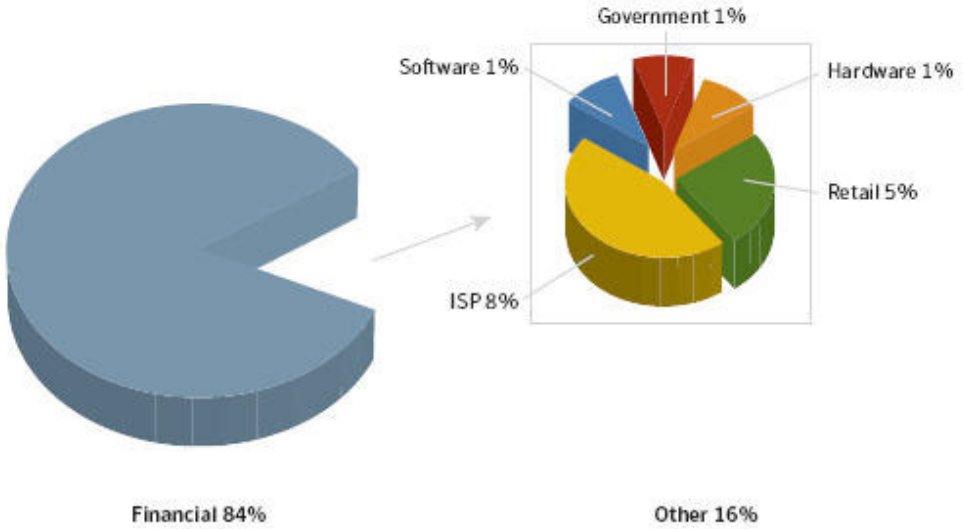


Figure 8. Phishing activity by sector
Source: Symantec Corporation

- **Analyse :**
  84% des attaques Phishing ont pour cible des services financiers.

  Cela est dû à l'appât du gain potentiel que peuvent produire ce type d'entreprise.

Evolution des attaques Phishing

- **Augmentation des attaques**
  Près de 17 000 par mois en 2006.

- **Localisation des attaques**
  Près de 40% des attaques ont lieu dans des langues autres que l'anglais.

- **Complexité des attaques**
  Attaque avec des logiciels malveillants du type enregistreurs de frappe (+ 130%).
  Attaque couplée avec des technologies de VoIP.
  Utilisation de certificat valide pour des sessions HTTP.

- **Aucune sensibilisation de l'attaqué (utilisateur final)**
  Près de 90% des participants n'identifient pas les tentatives.
  Près de 25% ne tiennent pas compte des messages de sécurité.
  Près de 50% ne tiennent pas compte des messages relatifs à l'expiration des certificats.

Exemples d'attaque Phishing

To: 419@arachnophiliac.com
Subject: Important Alert
From: Paypal <support@paypal.com>
Reply-To:
Date: Tue, 13 Sep 2005 05:13:57 +0000

Display all headers

PayPal The way to send and receive money online

Important Alert

Hello Sir/Madam,

Founded in 2005, PayPal, an eBay Company, enables any individual or business with an email address to securely, easily and quickly send and receive payments online.

PayPal always look forward for the security purpose of their clients. Therefore, PayPal is proud to announce about their new updated secure system. We updated are new SSL servers to give our customers a better, fast and secure service.

Due to the recent update of the servers, you are requested to please update your account info at the following link.

Click here to update your account.

Edward A. Wrick
Security Advisor
PayPal.com

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your P
footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP059

IMPORTANT: Update your PayPal account informations - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Subject: IMPORTANT: Update your PayPal account informations **From:** Paypal Inc. 02:14

PayPal

Account Verification

Dear [redacted],
You have received this email because we have strong reason to belive that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.
Copyright © 1999-2006 PayPal. All rights reserved.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

Evolution du nombre des vulnérabilités

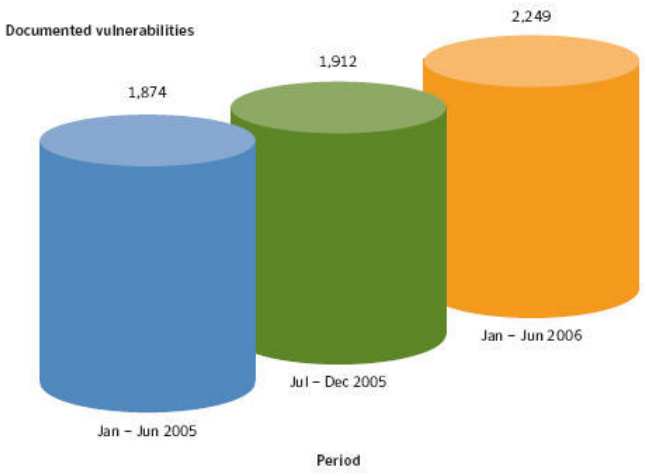


Figure 16. Total volume of vulnerabilities
Source: Symantec Corporation

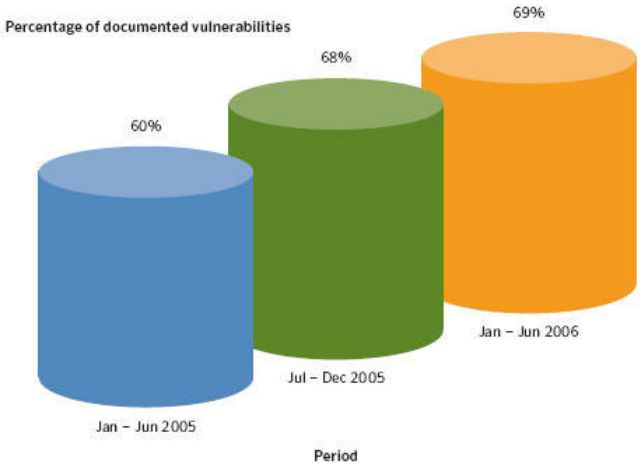


Figure 17. Web application vulnerabilities
Source: Symantec Corporation

- **Analyse :**

  Les vulnérabilités croissent en nombre mais également dans différents domaines.

  Toutefois un grand nombre de vulnérabilité se trouve sur les applications WEB.

Vulnérabilités exploitables par type

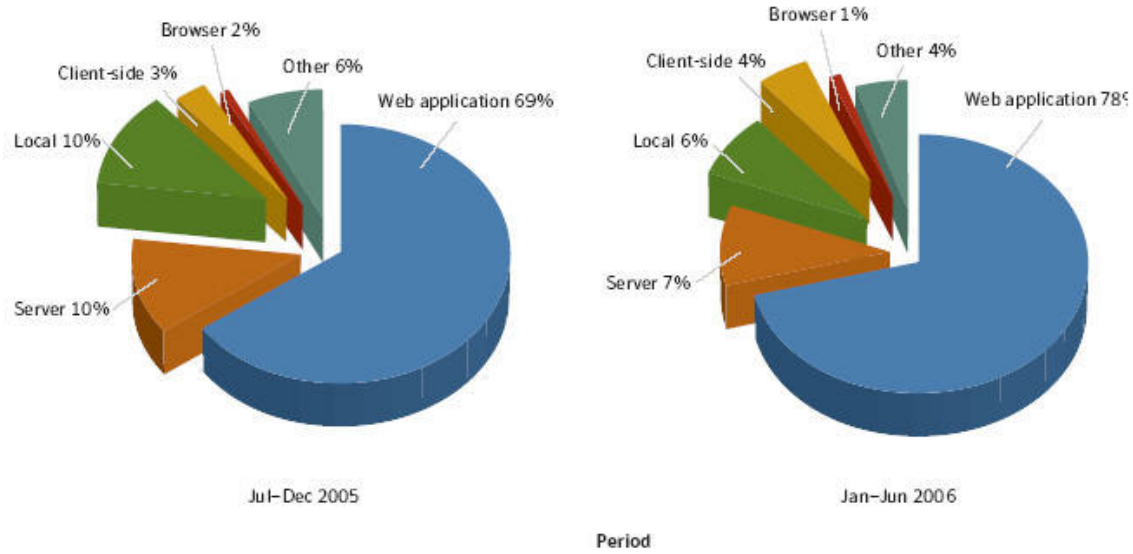


Figure 19. Easily exploitable vulnerabilities by type
Source: Symantec Corporation

- **Analyse :**

  80% des vulnérabilités sont facilement exploitables.

  78% de ces vulnérabilités concernent les applications WEB.

Temps d'exposition des vulnérabilités

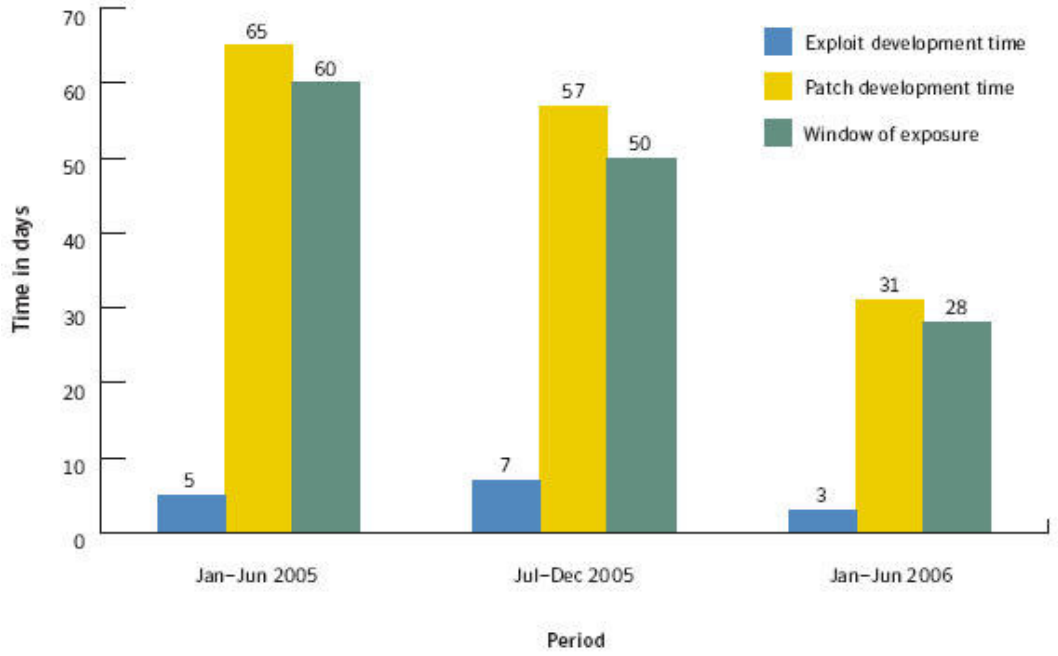


Figure 2. Window of exposure, enterprise vendors
Source: Symantec Corporation

- ✓ **Analyse :**

  Le temps de disponibilité d'un « exploit » est de plus en plus cours.

  Toutefois la disponibilité des correctifs est de plus en plus rapide.

Point sur les vulnérabilités et Zero Day Attack

- **Attaque Jour Zéro (Zero Day Attack) :**

La publication des failles des systèmes d'exploitation et des applications est utilisée de plus en plus systématiquement par les auteurs de programme malveillant afin de développer des attaques exploitants ces failles avant qu'un correctif ne soit déployé, ou même disponible : c'est l'attaque "zero day".

La rapidité des attaques est en elle-même un facteur de dangerosité.

En effet, les défenses opposées à ces attaques reposent aujourd'hui essentiellement sur la diffusion de signatures antivirales permettant de les identifier et de les stopper.

- **Vulnérabilités rémunérées :**

Autrefois l'apanage de chercheurs bénévoles, la découverte et la divulgation des vulnérabilités doivent désormais compter avec un nouveau facteur : l'attrait financier.

- **Deux visions de la sécurité :**

La sécurité par l'obscurité et la divulgation complète.

Mise à disposition des « Exploits »

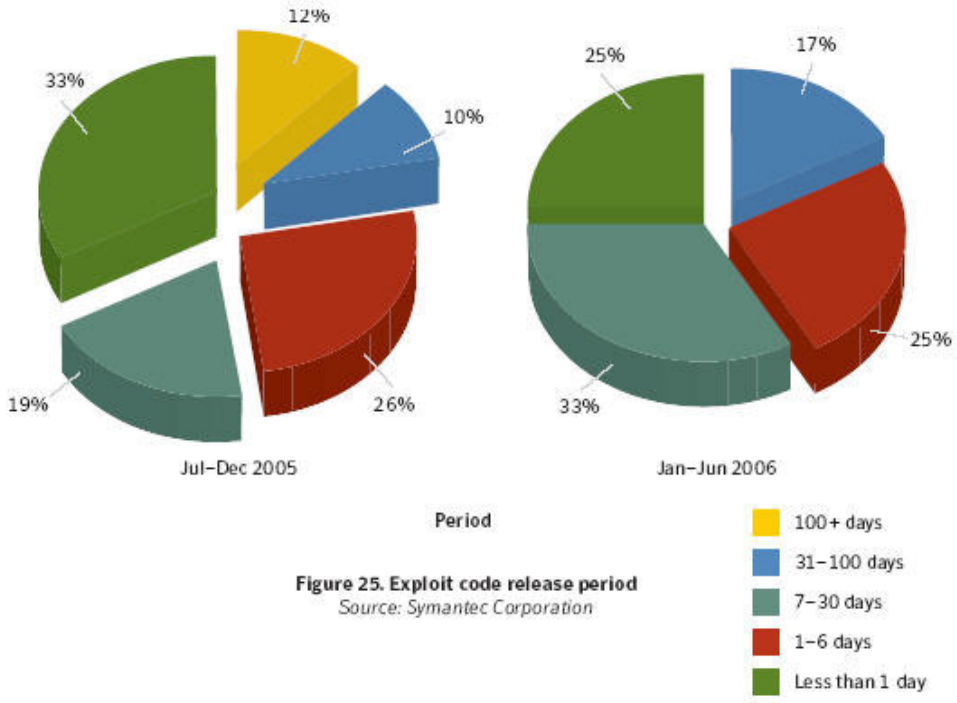


Figure 25. Exploit code release period
Source: Symantec Corporation

✓ **Analyse :**

Le temps de production d'un « exploit » est de plus en plus faible.

Le nombre important d'outils sur internet permettant la recherche de vulnérabilité et de création d'exploit est un facteur aggravant de cette situation.

Temps de mise à disposition des correctifs

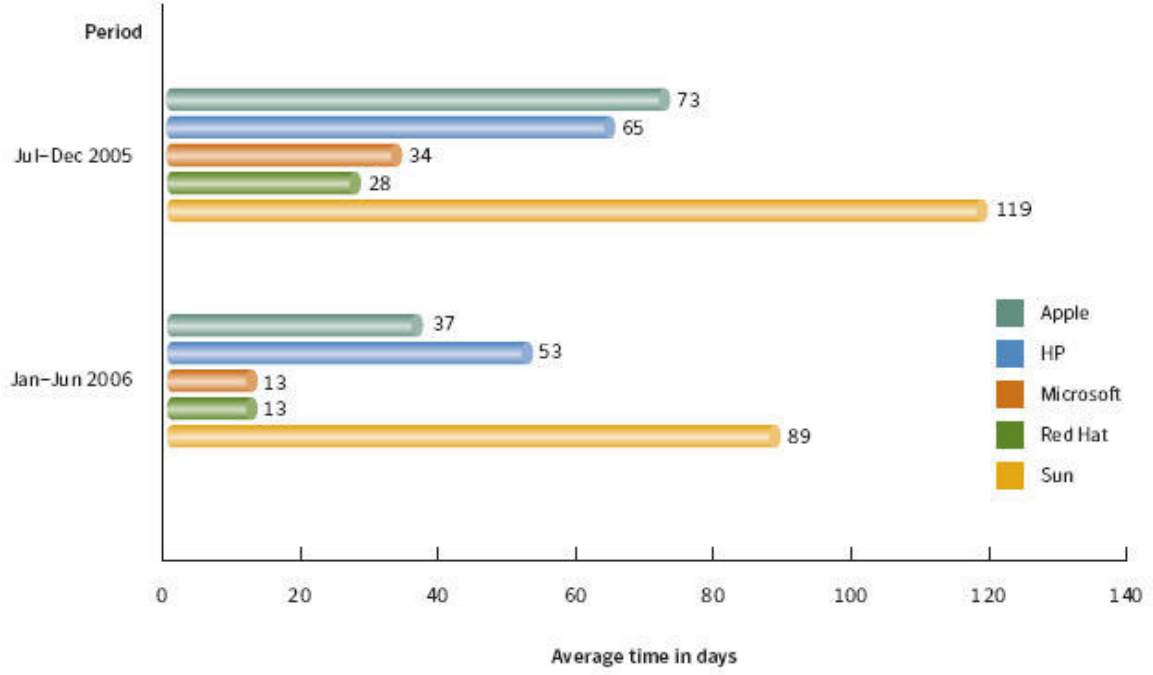


Figure 3. Operating system patch development time
Source: Symantec Corporation

✓ **Analyse :**

Microsoft est l'éditeur qui fournis le plus rapidement les correctifs.

A l'inverse Apple est l'éditeur le plus lent.

Répartition des SPAM

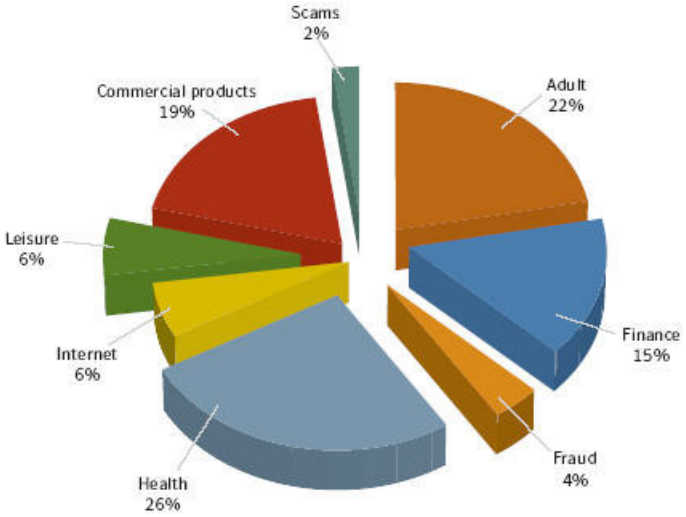


Figure 38. Spam categories
Source: Symantec Corporation

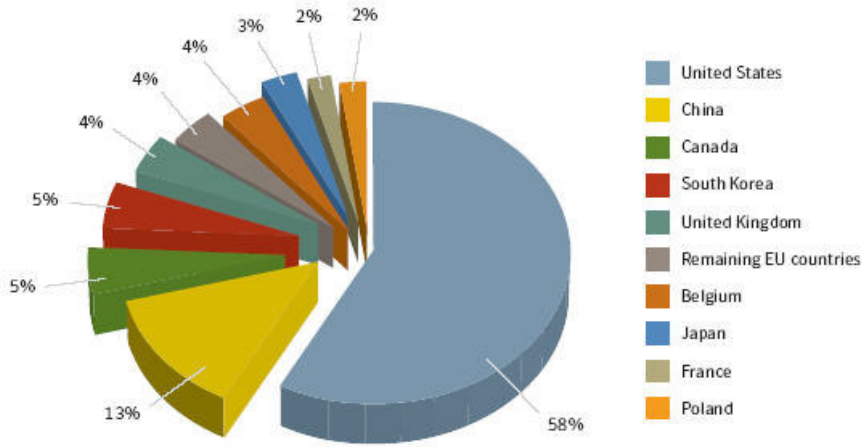


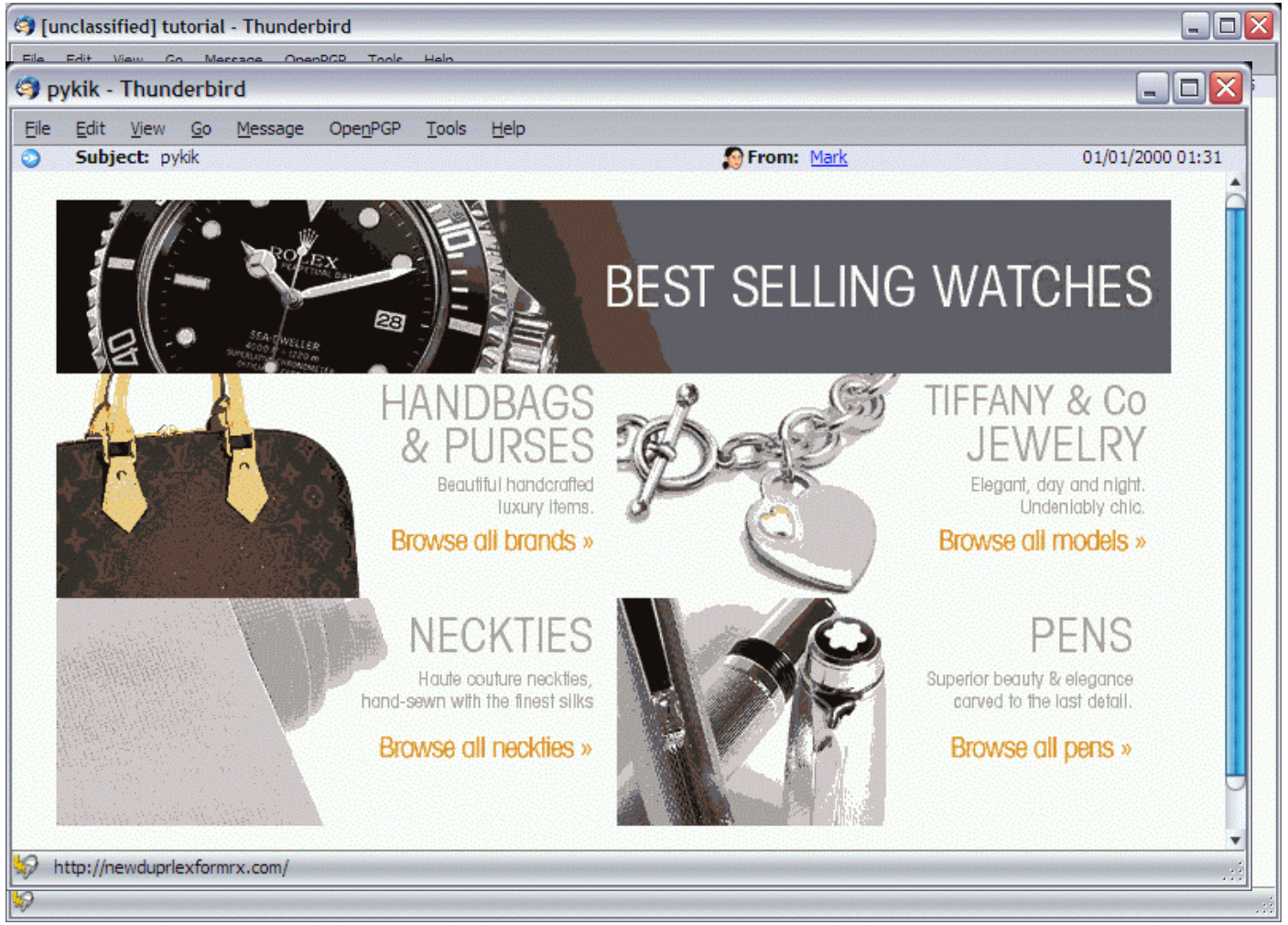
Figure 39. Top ten countries of spam origin
Source: Symantec Corporation

✓ **Analyse :**

La diffusion des SPAM, comme pour les réseaux Bot, provient des Etats-Unis et de la Chine.

Toutefois moins de 1% des SPAM contiennent des programmes malveillants.

Nouveauté : SPAM graphique

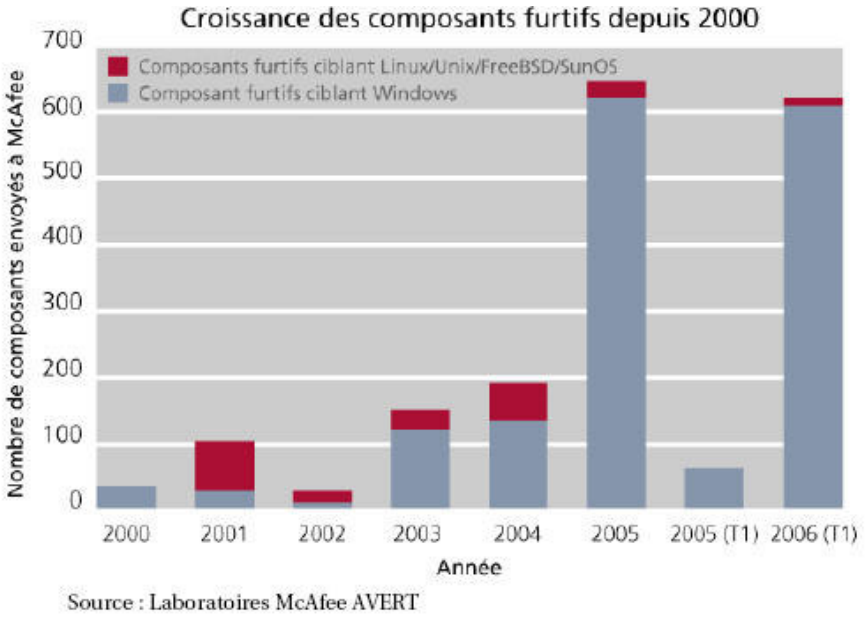


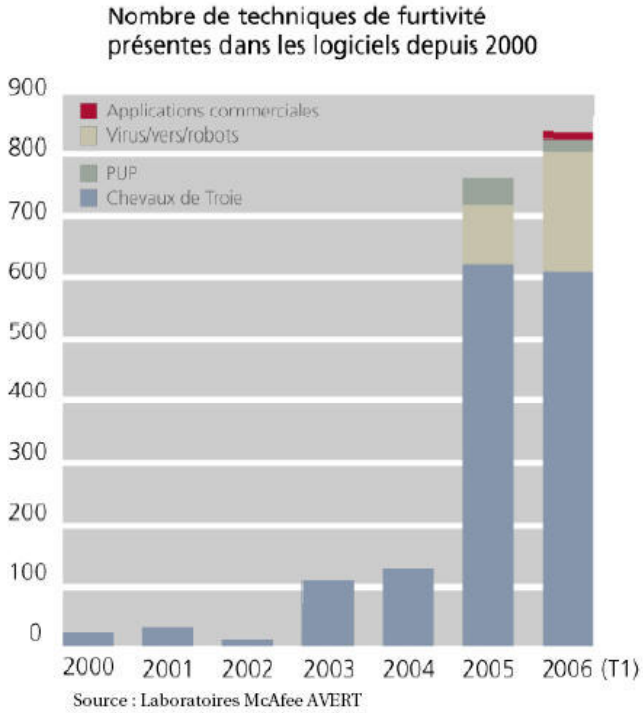
Nouveauté : Spam en GIF animé

Autres sources de SPAM

- ✓ Instant Messaging
- ✓ Voice Over IP
- ✓ Mobile et telephone
- ✓ Windows Messenger
- ✓ Snail Mail
- ✓ Blogs
- ✓ Mail Forms

Evolution des logiciels furtifs





✓ **Analyse :**

En l'espace de trois années seulement, l'utilisation des techniques de furtivité dans les programmes malveillants a progressé de plus de 600 pour cent.

De 2000 à 2005, la complexité des rootkits a augmenté de plus de 400 pour cent. Entre le 1er trimestre 2005 et le 1er trimestre 2006, cette tendance s'est chiffrée à plus de 900 pour cent.

Evolution des logiciels Espions

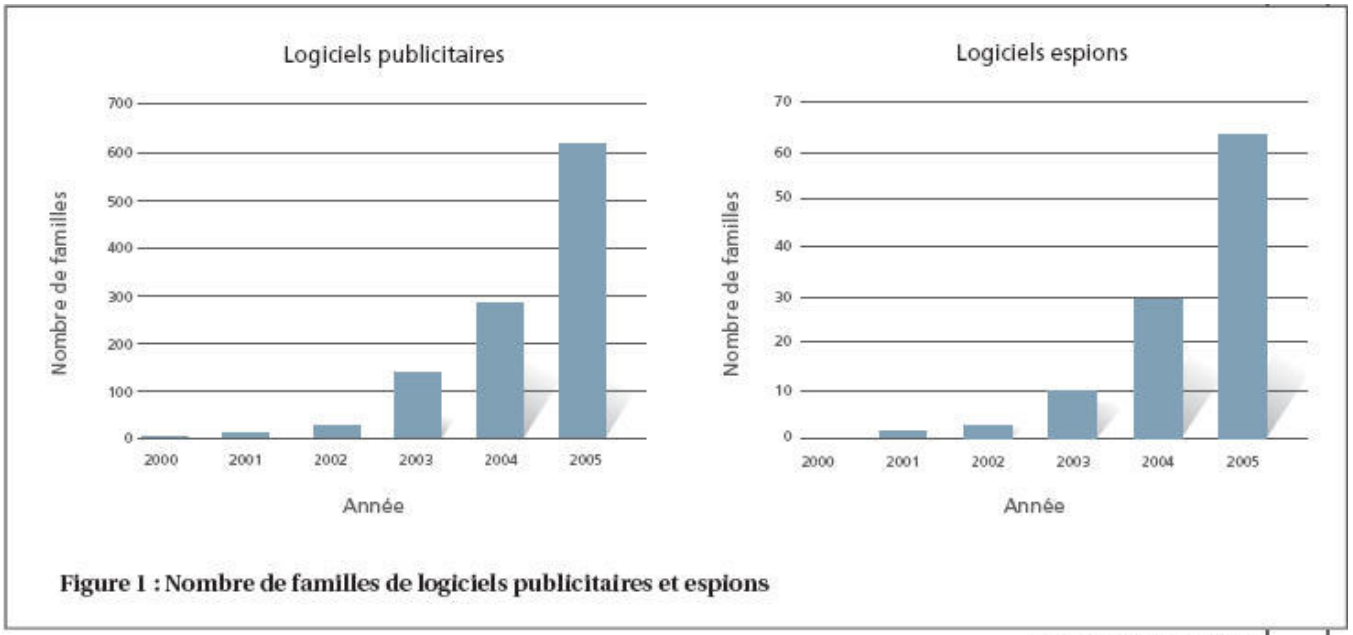


Figure 1 : Nombre de familles de logiciels publicitaires et espions

Source : McAfee Avert Labs

- **Analyse :**
  Les logiciels publicitaires et espions, souvent classés dans la catégorie des programmes potentiellement indésirables (PUP) et non des programmes malveillants, ont enregistré une augmentation impressionnante depuis 2003.

Conclusion

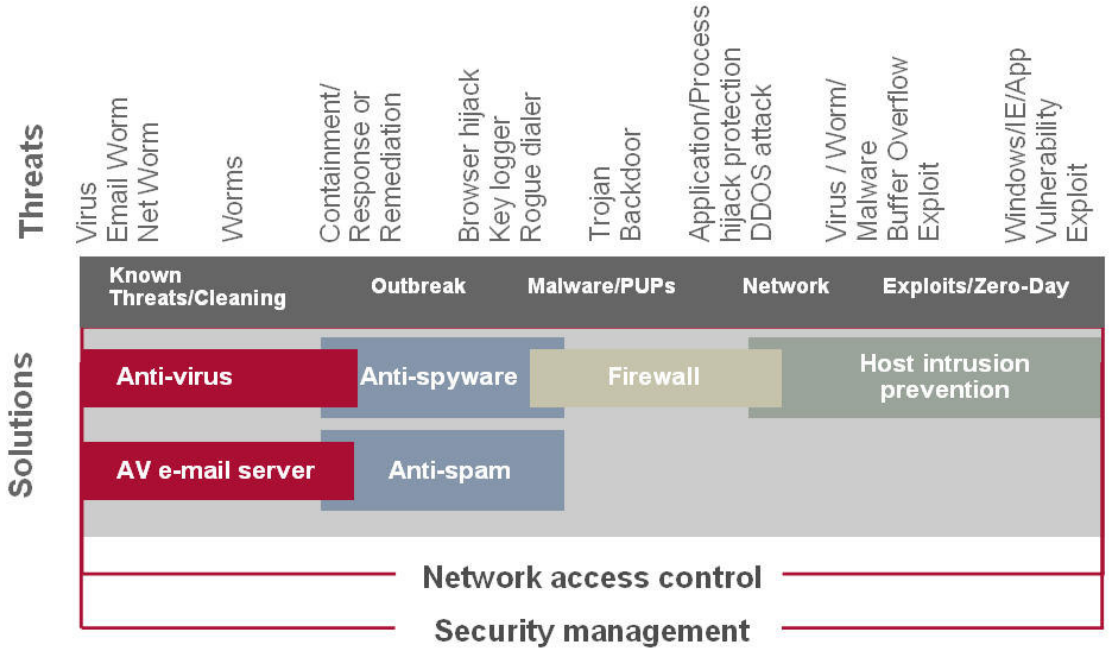
- ✓ « Vénalisation » des programmes malveillants
- ✓ Rémunération pour la découverte des vulnérabilités
- ✓ Augmentation du nombre de vulnérabilités
- ✓ Prévalence croissante des techniques de furtivité des programmes malveillants
- ✓ Augmentation du nombre de réseau Bot
- ✓ Augmentation et complexité accrue des technologies de Phishing
- ✓ Combinaison des menaces
- ✓ Le poste de travail et les applications WEB sont majoritairement la cible des attaques

Architecture de sécurité pour l'entreprise

Rappel sur les aspects d'un logiciel antivirus

- ✓ L'efficacité d'un logiciel antivirus est liée au dernier niveau de mise à jour du fichier des signatures.
- ✓ L'antivirus est une petite mais importante part d'une solution globale d'anti-programmes malveillants :
  - Avec un antivirus ayant un taux moyen d'une détection des Virus de 98%, et considérant une base de 10 Virus, la chance d'être infecté est de :
    - **1 (0.98) 10 = 19%**
  - Avec un antivirus ayant un taux moyen d'une détection de Spyware de 70%, et considérant une base de 10 Spyware, la chance d'être infecté est de :
    - **1 (0.7) 10 = 98%**
- ✓ En fait, il n'existe pas de solution 100% efficace, le mieux que l'on peut espérer c'est 98% et seulement si la solution est correctement étudiée et implémenté/

Les composants de sécurité à mettre en place



- ✓ Il est nécessaire d'utiliser différents type de solution anti-programmes malveillants en fonction des différentes menaces et vulnérabilités.
- ✓ La mise en place de ces différentes solutions s'intègre dans le schéma directeur sécurité du système d'information.

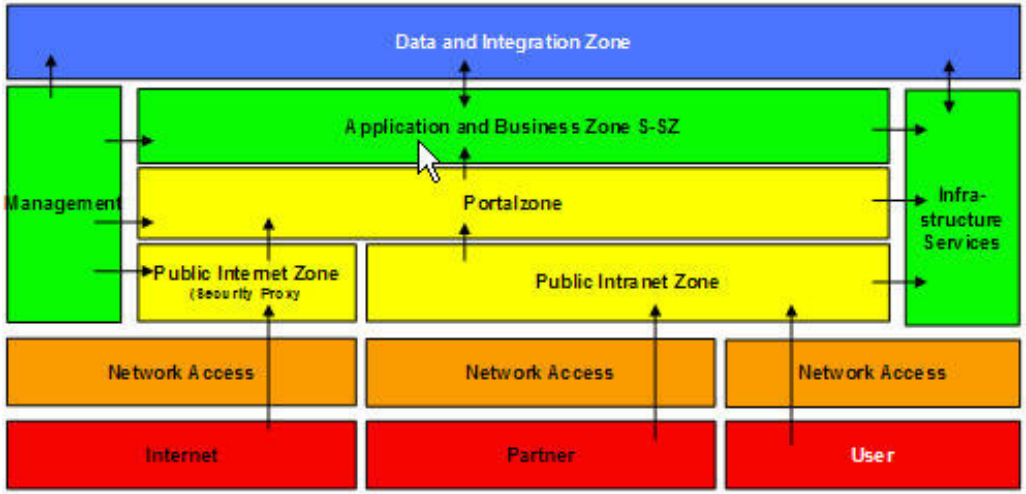
La stratégie de la CyberDefense

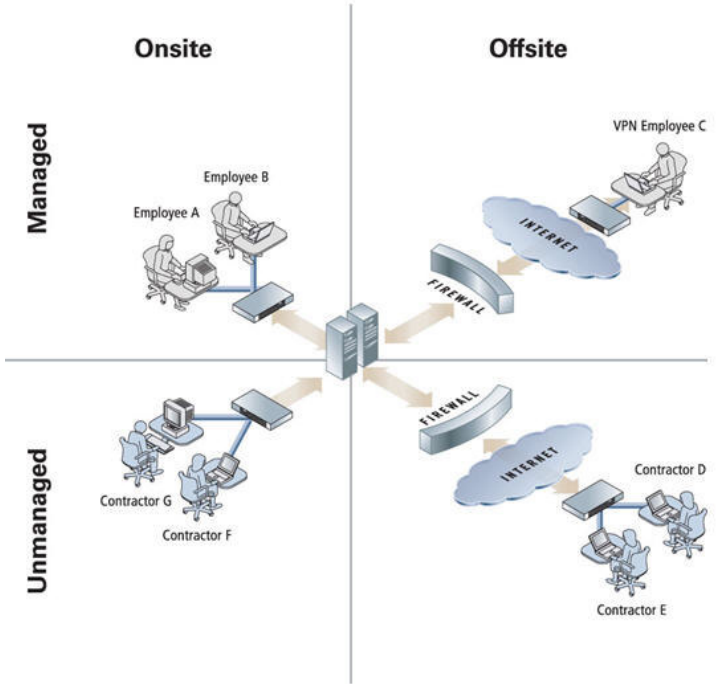
- ✓ **Définition des zones de sécurité réseau**
  Mettre en place une stratégie basée sur les zones de confiance.

- ✓ **Méthode de défense en profondeur**
  Mettre en place plusieurs mesures successives et indépendantes les unes des autres, afin de prévenir ou de maîtriser les incidents possibles et leurs conséquences, telle est la méthode de défense en profondeur.

- ✓ **Définition d'une stratégie multicouche**
  Mettre en place une stratégie de logiciel anti-programmes malveillants avec différents éditeurs logiciel pour les différentes couches de l'infrastructure de sécurité.

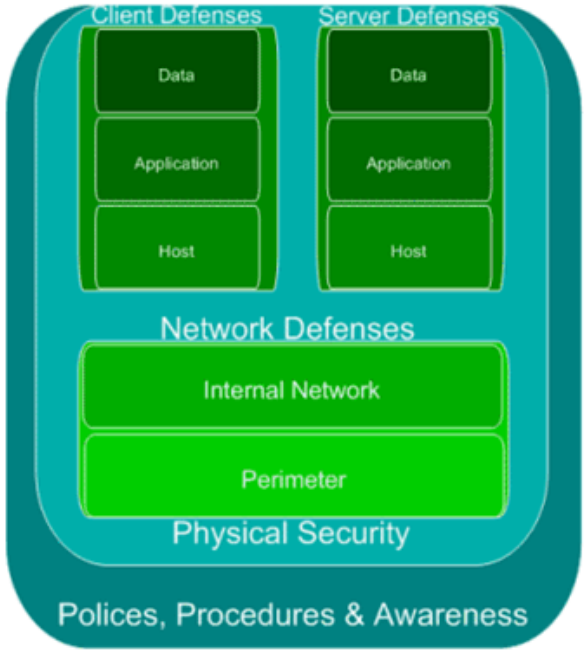
Définition des zones de sécurité

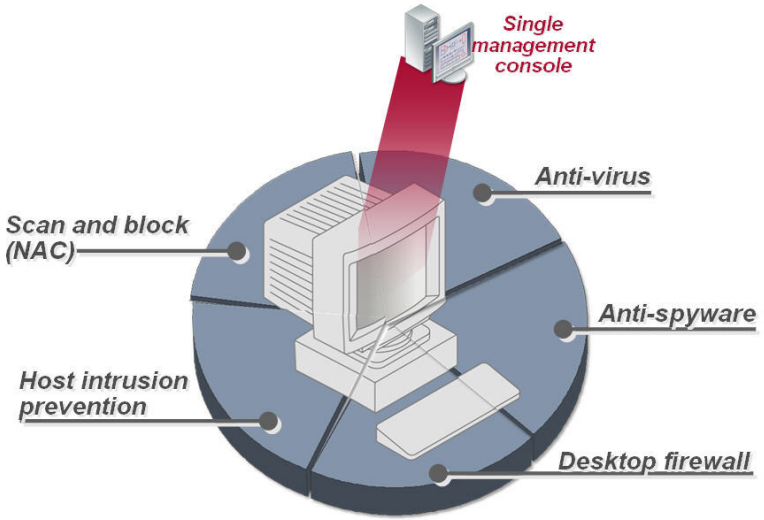




- ✓ Basée sur la méthodologie MASS d'IBM (Method for Architecting Secure Solution), cette méthode consiste à définir des zones de sécurité (non contrôlée, contrôlée, sécurisée, restreinte) en fonction de la confiance apportée aux mécanismes et informations qui s'y trouvent.
- ✓ Cette méthodologie définie aussi les échanges entre les différentes zones.

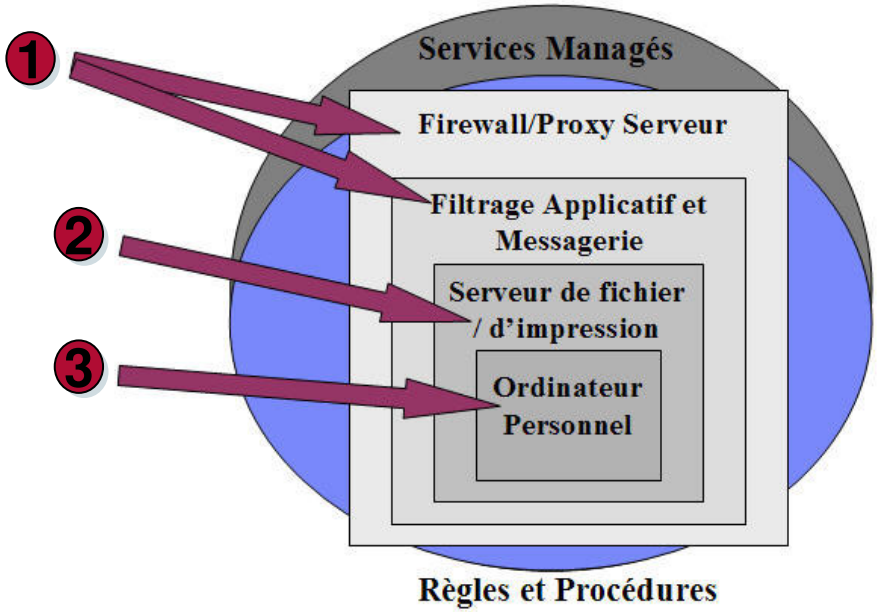
Modèle défense en profondeur





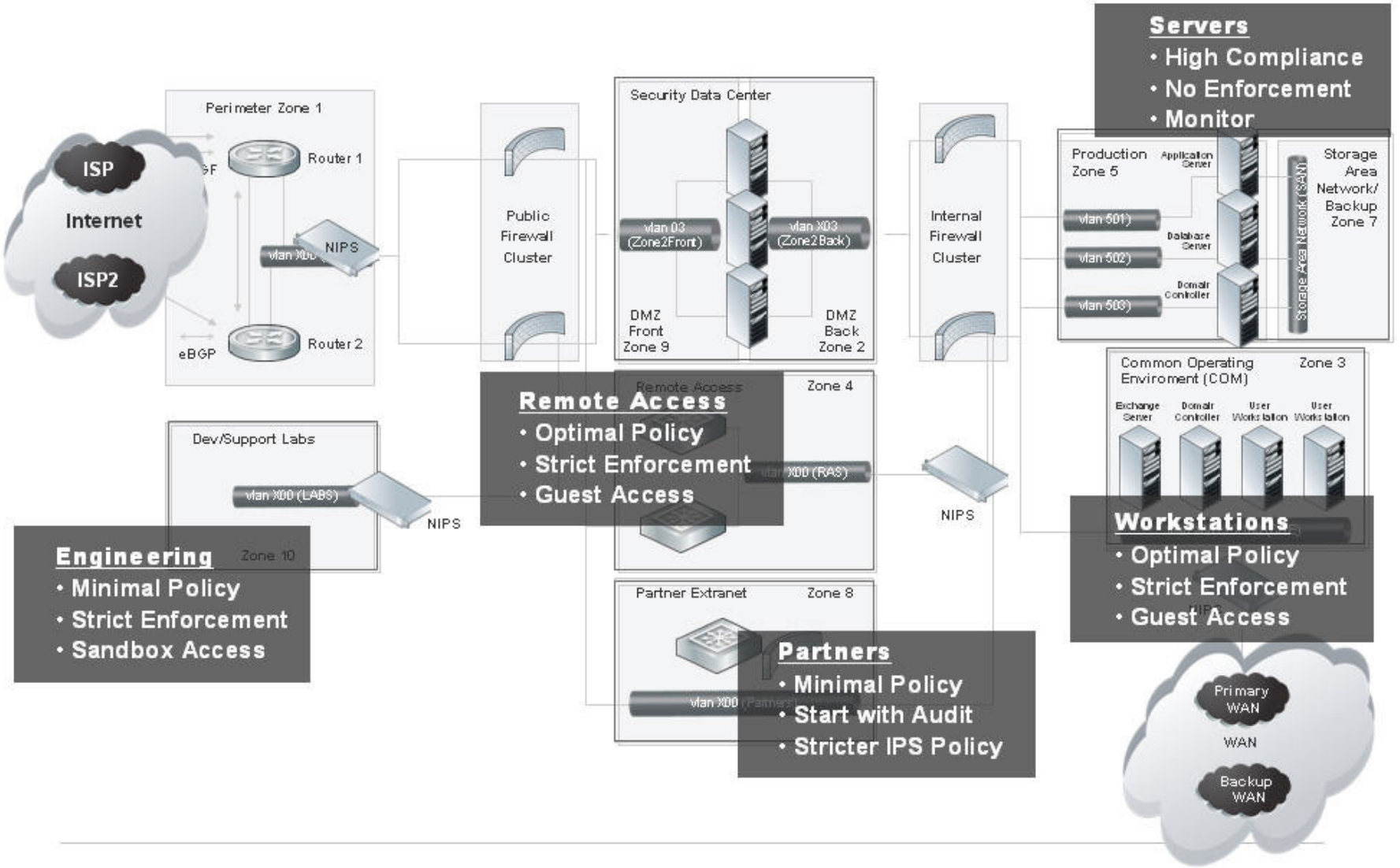
- ✓ Le modèle s'inscrit dans le schéma directeur sécurité du système d'information et il couvre les différents services de celui-ci (applicatif, serveur, station de travail, réseau,...)
- ✓ Dans le cas d'une station de travail il est nécessaire, pour répondre aux différentes menaces existantes, que celle-ci soit équipée des mécanismes antivirales, pare-feux, détection/prévention d'intrusion et de management des correctifs.
- ✓ Pour des raisons évidentes d'administration, il est préférable d'opter pour des mécanismes administrables à partir d'une même console de supervision.

Stratégie multicouche pour la CyberDefense

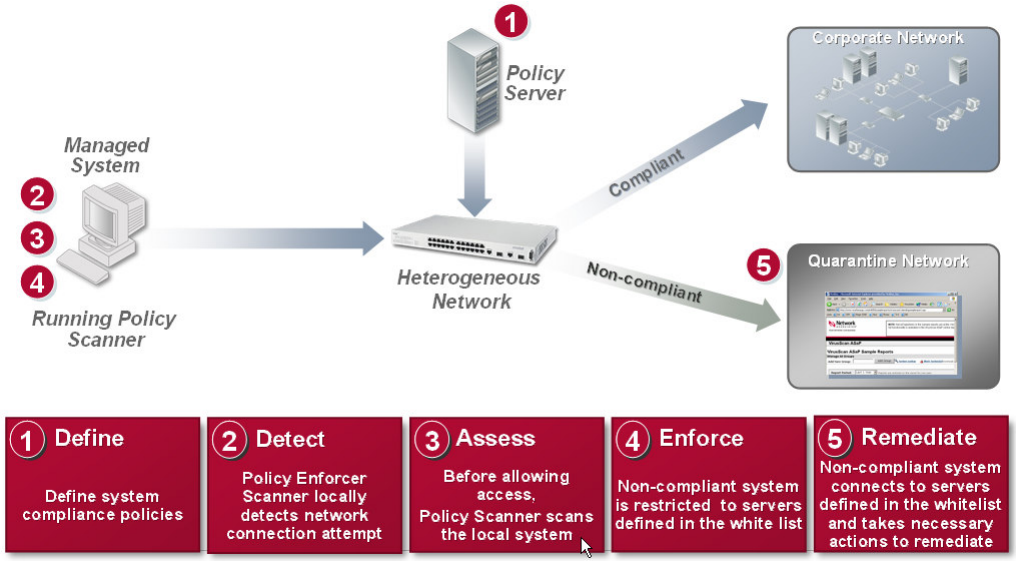


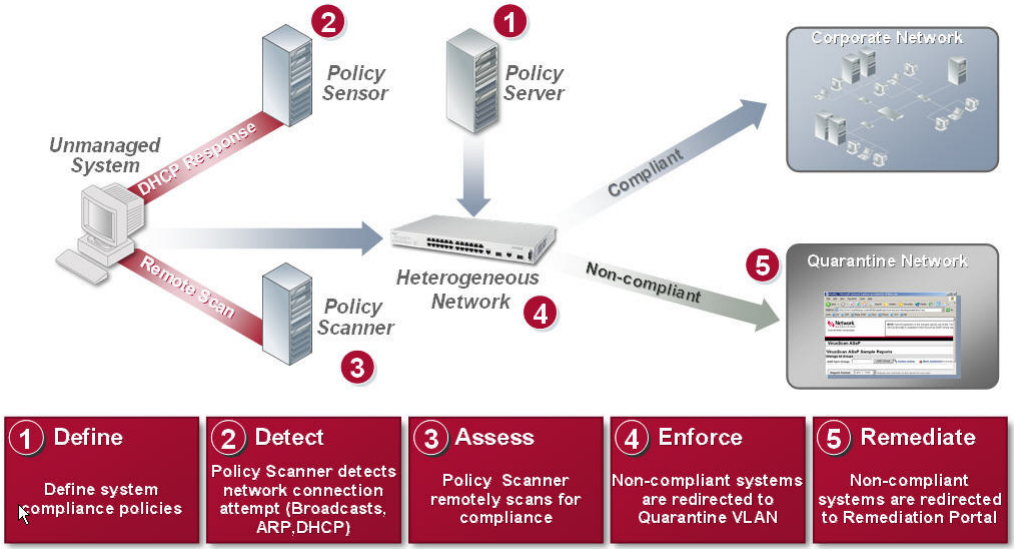
- Sur l'infrastructure antivirale, il nécessaire de ne pas utiliser le même éditeur. En effet il est préférable d'effectuer des filtrages avec différent type de moteur et de fichier de signature.
- 1 – Antivirus type 1, NIDS/NIPS (Network Intrusion Detection/Prevention System), filtrage et blocage du contenu (HTTP, SMTP antivirus).
- 2 – Antivirus type 2, Host IDS, filtrage applicatif.
- 3 – Antivirus type 3, IDS personnel, pare-feux personnel et gestion de la conformité du poste

Exemple d'infrastructure de sécurité



Exemple de sécurité d'accès





Attention aux impacts des mécanismes de sécurité

Exemple de la mise en place d'une stratégie

Layer	Current	Tactical	Strategic
Workstation	▪ Antivirus	▪ Antivirus + AntiSpyware	▪ Integrated Workstation Security solution : – Antivirus – Antispyware – Firewall – IPS – Compliance Checking ▪ End User with Low privileges
Network Perimeter	▪ Firewalls and Proxy protection, limited border infrastructure only	▪ N-IDS Refresh ▪ ISS FW Extension to unsupported servers. ▪ Central Management	▪ Trust domain with Network IPS. ▪ All workstation protected with IWSS.
Vulnerability Management	▪ Unused Qualys Scan.	▪ Qualys Vulnerability Scan and Correction. ▪ ISS IPS on unsupported platforms mitigating the risk	▪ Application Assessment. ▪ Fastest Migration for unsupported OS.
Internet Infrastructure	▪ Limited AntiSpam Solution	▪ HTTP Antivirus	▪ Standardized Internet Architecture. ▪ Renewed AntiSpam Solution ▪ Central Log Management

Les évolutions des menaces

Les prévisions des nouvelles menaces (1/2)

- **Le système d'exploitation Microsoft Windows VISTA**

  Le nouveau système d'exploitation de Microsoft fera l'objet de toutes les convoitises de la part des auteurs de programmes malveillants.

- **L'accroissement de découverte du nombre des vulnérabilités**

  La technologie du FUZZING permettra de mettre à jour de nouvelles vulnérabilités.
  Le fuzzing est une technique pour tester des logiciels. L'idée est d'injecter des données aléatoires dans les entrées d'un programme. Si le programme échoue (par exemple, en crachant ou en générant une erreur), alors il y a des défauts à corriger.
  Le grand avantage du fuzzing est que l'écriture de tests est extrêmement simple, et ne demande aucune connaissance du fonctionnement du système. D'ailleurs, le fuzzing est également utilisé pour traquer des failles de sécurité ou dans la rétro-ingénierie.

- **L'accroissement des programmes malveillants polymorphes**

  Cela désigne un code malicieux capable de modifier sa signature à chaque nouvelle génération, ce qui le rend très difficilement détectable pour les antivirus se basant uniquement sur un base de données de signature.
  Cette technologie sera utilisée pour des cibles spécifiques.

Les prévisions des nouvelles menaces (2/2)

✓ Les nouvelles technologies liées aux applications

• **AJAX :** pour Asynchronous JavaScript And XML (« XML et Javascript asynchrones ») est un acronyme désignant une méthode informatique de développement d'applications Web. Contrairement à une technologie client/serveur ou les requêtes sont traitées sur la machine serveur, dans le cas d'AJAX les requêtes sont traitées sur le poste de travail. L'utilisation de cette technologie va donc augmenter le nombre de cible potentielle pour les programmes malveillants. Au-delà des vers et autres virus, Ajax amplifie les risques d'attaques de type phishing, ayant pour objet la récupération frauduleuse d'informations personnelles de l'utilisateur.

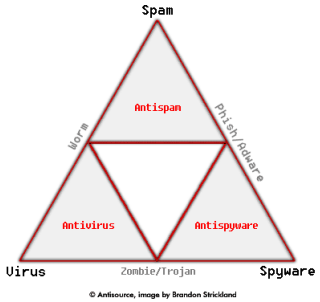
• **WEB 2.0 :** Considéré comme l'évolution naturelle du web actuel, le web 2.0 est un concept d'utilisation d'internet qui a pour but de valoriser l'utilisateur et ses relations avec les autres (services collaboratifs et interactifs). Cette technologie présente de par ce fait un nombre important de considération de sécurité. Les programmes malicieux peuvent facilement tirer avantage des relations de confiance qui sont mis en place entre les différentes plateformes collaboratives.

Les programmes malveillants ne sont pas la cause de tous les problèmes informatique …

Security Competency

CyberDefense : Nouvelles menaces, nouvelles parades…

4ème Forum des Architectes – La Sécurité Informatique



Serge RICHARD, Architecte Sécurité - CISSP®
serge.richard@fr.ibm.com