Les points noirs de la sécurité informatique

Luxembourg 11 avril 2008

Il faut être aware !!!

Claude Marson
rcmarson@wanadoo.fr
rcmarson@vdn.ca
Tel : (33) 6 08 84 20 86
(1) 514 362 9682

De l'amusement de potache aux cybercriminels

- La sécurité devient une préoccupation majeure : ISO 27001
- Les failles traditionnelles du S.I : une passoire
- Les moyens de protection évoluent : IPS, NBA, la gestion des logs
- Les failles nouvelles : Wi-Fi, IM, téléphonie IP, hyperviseur
- Les techniques « à la mode » : flooding, spoofing, rootkits
- Les botnets et la cybercriminalité
- Les méthodes modernes de biométrie et l'authentification forte

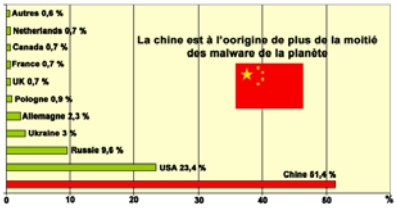
La problématique sécuritaire

« …La sécurité devient un enjeu majeur des SI modernes.
Les « amusements » des hackers et crackers ne sont que de sinistres présages aux véritables attaques de demain, qui seront initiées par des organisations mafieuses.
La cybercriminalité ne requiert pas de gros moyens, seulement de la compétence et la volonté de nuire.
Avant 5 ans, terrorisme et cybercriminalité auront fait leur jonction.
C'est le véritable défi qui attend les DSI…. »

- **D'ores et déjà (LEXSI), il y a six grands réseaux de cybercriminalité organisée**
  Anglophones, asiatiques, brésiliens, djihadistes, russophones, sub-sahariens
- **Les activités principales (par ordre décroissant, LEXSI)**
  Collecte d'informations bancaires, monétisation d'identifiants et blanchiment de fonds, développement de malware, location de botnets, arnaques sur actions boursières, intrusion ou « défacements » de sites commerciaux, vente de base de données d'emails spécialisés, gestion de sites de jeux en ligne, monétisation de contenus pornographiques

Page 3/56

La véritable cyber-criminalité commence



Les dégâts économiques que peuvent entraîner des attaques coordonnées sont sans aucune mesure avec ceux des attaques terroristes classiques.
Une période s'ouvre où chacun d'entre nous pourra devenir acteur (involontaire) d'une action malveillante de grande envergure

Page 4/56

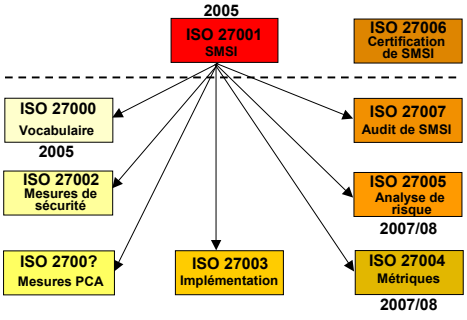
Globalement, un laxisme évident…

- **Dés lors que le SI est ouvert et connecté à Internet, des failles de sécurité sont exploitables.**
- **Le système est un ensemble de services ouverts via un port. Pour être tranquille…il faut tout fermer. Mais on ne peut plus communiquer !!! L'ouverture est donc inévitable, ce qui ne veut pas dire que l'on doit faire n'importe quoi.**

- Contrôles d'accès aux routeurs inappropriés
- Points d'accès RAS mal protégés et mal surveillés
- Fuites d'informations en interne
- Services inutiles sur machines hôtes
- Mots de passe faciles à deviner
- Comptes ayant des droits inutiles ou excessifs
- Firewall mal configuré ou listes ACL de routeur trop libérale…
- Logiciels non patchés, périmés, maintenus dans leur configuration par défaut
- Accès trop libéraux aux fichiers et répertoires
- Relations de confiance…trop confiantes !!!
- Capacités de détection et de surveillance inappropriées
- Absence de règles et de procédures correctement diffusées dans l'entreprise

La certification ISO 27001

- **Une garantie offerte aux clients et partenaires que les meilleures conditions de sécurité ont été mises en œuvre**
- **Issue du référentiel BS 7799-2, concerne le SMSI : Système de Management de la Sécurité de l'Information**



- Il y a une seule autorité de certification par pays : COFRAC pour la France, mais de nombreuses organisations de certification, souvent privées : LSTI, BSI, BVQI…en France
- Fin 2006, seules 3 sociétés françaises étaient certifiées, contre 324 en Grande-Bretagne et 1.907 au Japon !!!

- **ISO 27001 comporte 5 grands chapitres :**
  - PDCA (Plan – Do – Check – Act)
  - Engagement et responsabilité de la direction
  - Audits internes du SMSI
  - Réexamen du SMSI par la direction
  - Amélioration du SMSI

Les bonnes règles de gestion des mots de passe

- Choisir un mot de passe complexe : de nombreux comptes ont un mot de passe blanc
- Ne pas utiliser le nom de son chien, le prénom de sa femme, celui de l'équipe locale de rugby ou de football, voire son propre prénom
- Ne pas utiliser le mot "password" ou "psw"
- Utiliser un mélange le plus long possible de majuscules, de minuscules,de chiffres, de signes de ponctuation
- Le changer fréquemment
- Eviter de l'écrire n'importe où : postit sur l'écran…
- Ne jamais le divulguer : comme l'a dit Benjamin Franklin, deux personnes peuvent conserver un secret, à condition que l'une des deux soit morte…
- Attaques par dictionnaire
  - Si l'on connait le login, il est possible d'en déduire le mot de passe correspondant, si celui-ci a un "sens" (une chance sur deux)
  - Des dictionnaires sont disponibles qui effectuent la relation…en différentes langues
  - Face à des mots de passe chiffrés, les systèmes de recherche de mots de passe chiffrent chaque mot de passe du dictionnaire avec le même algorithme de chiffrage et comparent avec ce qu'ils trouvent dans le répertoire chiffré (vrai aussi sous Windows avec les fichiers SAM)
  - C'est la raison pour laquelle il ne faut pas que les mots de passe aient un sens : Sd0xx44rtz est un bon mot de passe
  - Ce n'est pas mon prénom, ni LOSC, ni PSG, ni Alouette

Le « buddy punching » est cette mauvaise habitude qui consiste à s'indiquer les mots de passe…pour raisons de commodité

Un sport national, le vol d'identités

- **Pourquoi se « casser la tête » à essayer de pénétrer les systèmes d'information, alors qu'il suffit souvent de s'assurer de complicités pour récupérer des données confidentielles**
- **L'AARP (American Association Retired Persons), distingue cinq familles de sources de vols d'identités**
  - Piratage ou attaque externe
  - Vol de matériels…parfois il suffit de récupérer un vieux PC abandonné
  - Divulgation involontaire de données
  - Accès internes malintentionnés
  - Pertes de sauvegardes

- **Selon Javelin Strategy and Research, le vol d'identités a représenté un préjudice de 49,9 milliards $ en 2006**
- **Ce que rapporte une identité volée aux Etats-Unis d'après Identity Theft Spy**
  - Un numéro de carte bancaire : 1 $
  - Le code sécurité d'une carte bancaire : entre 3 et 5 $
  - Le code carte et PIN : entre 10 et 100 $
  - Un numéro de sécurité sociale : entre 5 et 10 $
- **3 % des ménages américains ont été les victimes de ces vols en 2006**
- **Quelques exemples célèbres**
  - Les données confidentielles de 1,3 million de clients de la Texas Guaranteed Student Corp en 2006, suite au vol du portable d'un employé de Hummingbird
  - La sauvegarde d'un important établissement financier canadien qui vient de se « perdre » entre Montréal et Toronto
  - Les données personnelles de 26,5 millions d'anciens combattants en 2006

Le « sniffing » entre collègues

- **Le sniffing ou reniflage est une autre forme de vol d'identités, il s'applique aux informations volées dans le cadre de l'entreprise…entre collègues**
- **Il consiste à écouter le trafic qui passe entre les boîtiers de raccordement et les passerelles**
- **Il suffit qu'un hacker ou une structure malveillante dispose de complicités « techniques » internes pour récupérer des données confidentielles, car les outils sont disponibles sur Internet**
- **Les techniques les plus utilisées**
  - Bibliothèque Pcap (Unix, Linux et Windows) pour déverrouiller les cartes réseaux et Tcpdump pour intercepter des données
  - Mieux, l'outil Etherreal permet de recomposer en format html tout le trafic qu'il intercepte
  - Pour s'en protéger il ne faut pas installer de hubs ni de bornes Wi-Fi non authentifiées WPA
  - Ettercap, outil diabolique pour lancer des attaques de type « man in the middle » et se substituer à une cible : masquarade d'adresses IP et Mac
  - Globalement la meilleure parade consiste à ne jamais utiliser de protocoles en clair de type FTP, http ou Telnet mais plutôt SSH ou SSL sur https ou FTPS


Le reniflage ne date pas d'aujourd'hui, rappelez-vous les avions renifleurs

Page 9/56

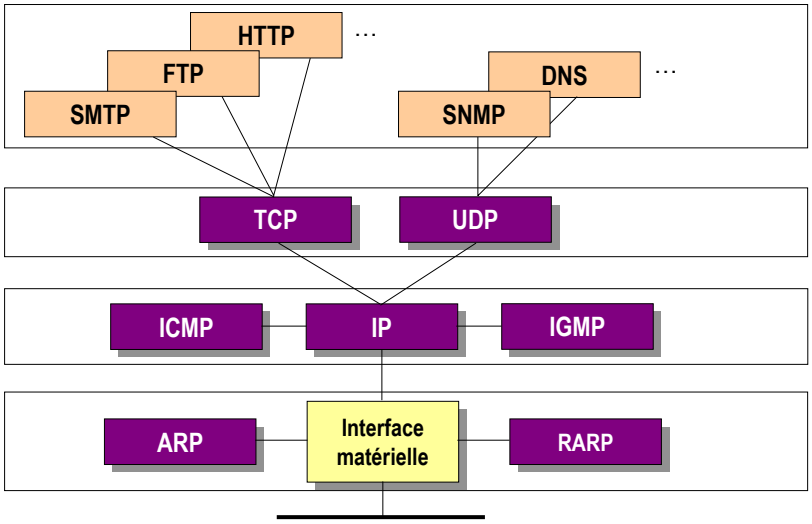
Quelques failles génériques du S.I

- Les attaques potentielles dans un réseau IP
- Le spoofing ARP
- Les problèmes liés à IP
- TCP : une calamité
- La criticité des failles diminue



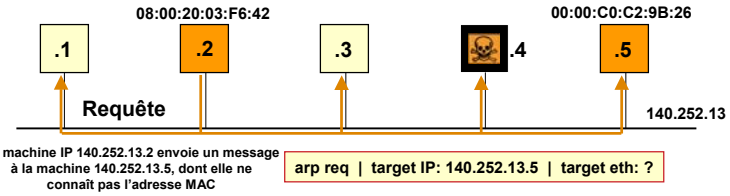
Page 10/56

Les attaques potentielles dans un réseau IP



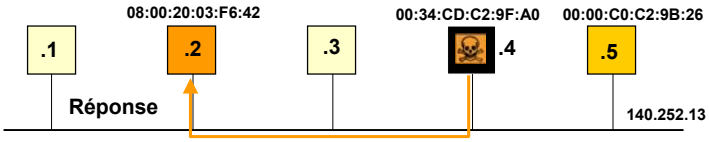
Le spoofing ARP ou la masquarade MAC

- Le principe : vous envoyez une requête pour une machine IP qui correspond à une adresse MAC et un imposteur se fait passer pour cette adresse Mac



La machine IP 140.252.13.2 envoie un message à la machine 140.252.13.5, dont elle ne connait pas l'adresse MAC

arp req | target IP: 140.252.13.5 | target eth: ?



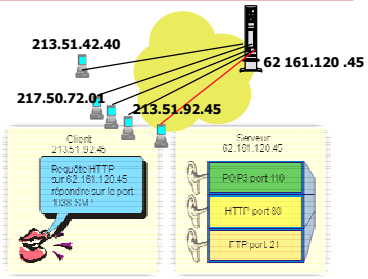
arp rep | sender IP: 140.252.13.5 | sender eth: 00:34:CD:C2:9F:A0

Le service ARP spoofé répond que la machine IP 140.252.13.5 correspond à l'adresse MAC du hacker. Le message parvient à la mauvaise adresse

TCP : Transmission Control Protocol

- **Fournit un service orienté connexion, fiable, vers les services de niveaux supérieurs**
- **Orienté connexion**
  - Une phase d'établissement de la connexion est effectuée avant le transfert de données
  - Des informations d'état sont gérées aux deux extrêmités : numéros de séquences, taille de fenêtre, etc
- **Très facile à pénétrer**
- **Un serveur peut être mystifié si on lui fait croire que le paquet provient d'une source digne de confiance**
  - Certaines applications se servent de l'adressse IP comme d'un moyen élémentaire d'authentification
- **Le mécanisme de handshaking se prête à l'attaque en déni de service**

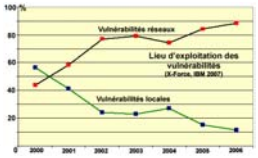
La notion de « port » TCP

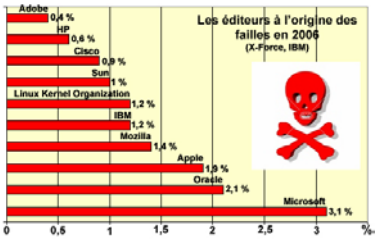


Le processus de handshaking de TCP/IP constitue l'une des faiblesses majeures des systèmes IP

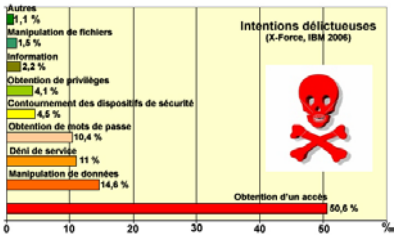
La criticité des failles diminue

- **Globalement les éditeurs écrivent un code de plus en plus sûr**
- **Le nombre de failles critiques diminue, tendance qui se confirme depuis 2004**
- **Microsoft ne représente que 3,1 % des failles recensées…mais il constitue la cible de la plupart des attaques**
- **Quand une faille est détectée, deux attitudes :**
  - De nombreux petits éditeurs la laissent en état et publient une nouvelle version débarrassée de la faille
  - Les grands éditeurs choisissent de publier des patchs, à charge pour les utilisateurs de les installer :
  - 14 % des vulnérabilités des 10 plus grands éditeurs ne sont pas corrigées, contre 65 % aux éditeurs de taille moins importante





Selon X-Force (IBM), 14 % des vulnérabilités viennent des grands éditeurs…



Les intentions délictueuses de l'exploitation des failles

Les failles les plus exploitées : OS

- **Internet Explorer**
  - IE est souvent le moyen pour un hacker d'exécuter du code malicieux sans intervention de l'utilisateur, à l'occasion d'une visite Web ou de l'arrivée d'un courriel
  - Souvent des attaques zero-day
  - IE est également vulnérable à travers d'autres modules Windows, liés à IE, tels que le HTML Help ou le GRE : Graphics Rendering Engine, mais aussi par les ActiveX installés par Microsoft et les autres éditeurs
  - Les protections pour XP
    - Passer à XP SP2
    - Passer à IE 7 qui est sensiblement mieux protégé
    - Utiliser un outil tel que DropMyRights de Microsoft qui permet d'implémenter la politique dite de « Least Privileges » de IE (LUA), qui consiste à attribuer aux acteurs du système: utilisateurs et outils, le niveau minimum de privilèges d'accès et d'exécution
- **Les librairies Windows**
  - Les librairies dll et OCX servent souvent à des attaques distantes, il suffit de convaincre un visiteur de cliquer sur un lien ou une image (entre autre)
  - Les principales librairies visées : Explorer, Hyperlink Object Library, HTML Help, le GRE…
  - Pour se protéger
    - Bloquer les ports 135-139/tcp, 445/tcp, utilisés par Windows pour ses accés réseaux
    - Utiliser le filtrage TCP/IP qui existe dans Windows XP, ainsi que son firewall
    - Appliquer le principe du « moindre privilège » pour limiter l'action éventuelle d'un ver ou d'un cheval de Troie
    - Rester très vigilant vis-à-vis des pièces attachées aux courriers

Les failles les plus exploitées : OS

- **Office**
  - Office étant de très loin le système de bureautique le plus utilisé, ses éléments Word, Excel, etc, constituent une cible de choix pour les hackers
  - De nombreuses failles ont été détectées en 2007
  - Techniques pour se protéger (entre autres)
    - Déconnecter l'ouverture automatique d'un fichier Office dans IE
    - Configurer Outlook avec le niveau de sécurité amélioré
    - Mettre en œuvre un filtrage Web et courrier efficace
- **Les services Windows**
  - Certains services noyau de Windows peuvent servir de véhicules aux attaques : RPC, protocole CIFS (Common Internet File System)
  - Les failles récentes
    - Server Service
    - iRouting et Remote Access Service
    - Exchange Service
  - Protections
    - Déconnecter les services…si c'est possible
    - Bloquer les ports dangereux : 139/tcp et 445/tcp
    - Installer SP2 pour XP et Windows 2003 SP1 et R2

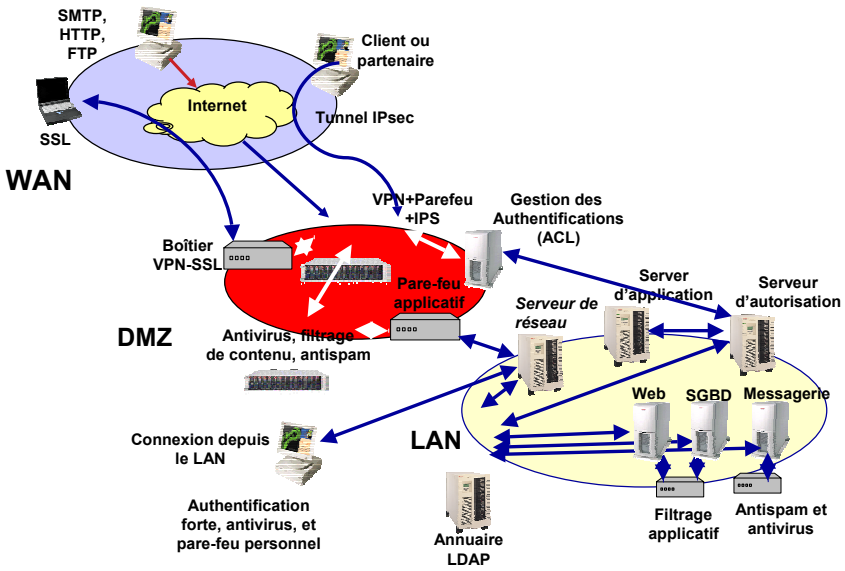
- **La gestion des mots de passe sous Windows**
  - Les mots de passe constituent l'une des faiblesses les plus importantes de Windows, de nombreuses attaques l'ont exploitées en 2007, souvent de force brute (hijacking)
  - Il est essentiel de s'en protéger, en plus d'une politique stricte en termes d'expiration et de structure
    - Empêcher Windows de stocker les mots de passe en mode LM Hash dans AD ou SAM, jugé trop fragile et lui préférer la solution NT Hash (Microsoft a publié le mode opératoire)
    - Mettre en place une politique de tests périodiques des mots de passe à l'aide d'outils externes tels que THC Hydra (outil de recherche des mots de passe), LophtCrack ou John the Ripper

Les failles les plus exploitées : autres OS

- **Mac OS X**
  - Mac OS X qui est une distribution Unix n'échappe pas à la « mode »
  - Ses faiblesses sont regroupées en cinq familles
    - Safari, le browser Web par défaut de Apple, qui comporte de nombreuses faiblesses
    - ImageIO, le framework de gestion et traitement des images
    - Unix lui-même
    - Le mode sans-fil
    - Les virus et chevaux de Troie qui se multiplient
- **Le mode de configuration standard de Unix et Linux**
  - La procédure d'installation par défaut de Red Hat met en place des services tels que cups : Common Unix Printing System), portmap : support RPC, sendmail : agent de transport de messagerie, shhd : Serveur Open SSH, qu'il faudra « débrancher » si nécessaire
  - Les attaques les plus virulentes concernent les services FTP, Telnet et SSH
- **Des centaines de failles sont trouvées dans les applications courantes**
  - Gestion de contenu (CMS), Wikis, forums..
  - Les frameworks PHP, .Net, JavaEE, Ruby On Rails, Cold Fusion…présentent tous des failles, plus ou moins dangereuses

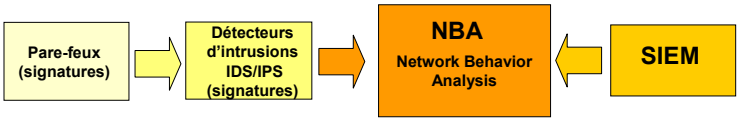
Les mondes Mac OS X et Linux (ou Unix) ne sont plus à l'abri

Une architecture globale de sécurité



Du pare-feu aux NBA et SIEM

Pour une sécurité globale du SI



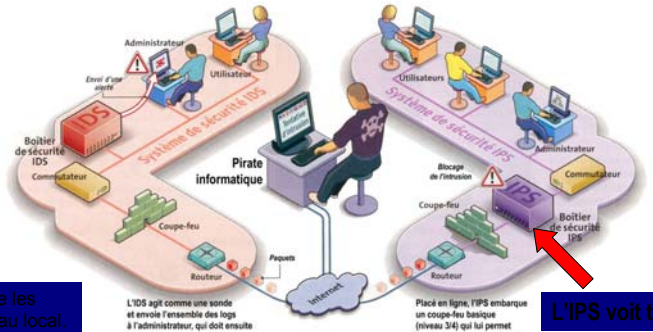
- On passe d'une protection de type « périmétrique » (on cherche à empêcher l'assaillant de pénétrer) à une protection de type aéroportuaire : tout entrant est potentiellement suspect.
- Le NBA, fondé sur l'analyse comportementale, peut être complémentaire de solutions fondées sur les signatures
- Les logiciels SIEM concernent l'analyse et le traitement des fichiers log

Editeur	Solution
ArcSight	ArcSight Enterprise Security Manager (ESM)
Cisco	MARS (Monitoring, Analysis and Response System)
Computer Associates	eTrust Audit et eTrust Security Command Center
Prism Microsystems	EventTracker
Quest Software	In Trust
NetForensics	nFX
IBM	Netcool/NeuSecure
NetIQ	NetIQ Security Manager
OSSIM (Open Source)	Open Source Project
Q1 Labs	QRadar Network Security Management
Symantec	Security Information Manager
Novell	Sentinel

Quelques solutions de traitement des logs : un passage obligé

IDS contre IPS

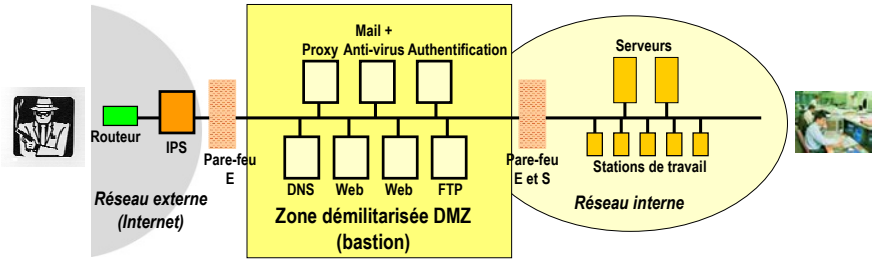
- L'IPS bloque les flux qu'il juge malicieux (à partir d'un certain seuil paramétrable)
- Complète efficacement le pare-feu
- Très simple à installer
- Assure une supervision globale en décodant la plupart des protocoles : messagerie, http..., là où l'IDS se contente d'envoyer des alertes
- Encore cher : boîtier + mise à jour des signatures



L'IDS est placé derrière les commutateurs du réseau local. L'IPS est en tête de ligne, entre le commutateur et le routeur.

L'IPS voit tout

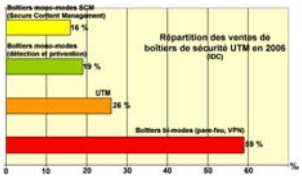
Le firewall et la DMZ



- **La DMZ reste la meilleure manière d'isoler un réseau interne des flux externes, potentiellement malveillants**
- **Il existe en 2006 trois familles de pare-feux selon le type de contrôle :**
  - Filtrage par adresse ou protocole (avec ou sans état)
    - Performances réduites avec un nombre de filtres élevé
    - Laissent passer les codes type cheval de Troie, car ne contrôlent pas le contenu des paquets (effet tunnel)
  - Filtrage applicatif
    - Niveau 7, filtrent le contenu des paquets : évitent l'effet tunnel
    - Contrôlent les flux applicatifs et les commandes autorisées
    - Coûteux, nécessitent une grande puissance de calcul
  - Pare-feu d'authentification
    - Une sous-famille des filtres applicatifs : l'autorisation est fondée sur l'identité et pas sur une adresse IP

L'UTM, tendance à l'intégration des fonctions de sécurité

- La tendance est à la convergence des équipements, surtout pour les PME, à la recherche de solutions intégrées et faciles à mettre en place
- Tendance au regroupement des solutions de sécurité dans un « tout en un », l'UTM : Unified Threat Management
- Comporte :
  - Un pare-feu réseau et applicatif
  - Un outil de filtrage de contenu
  - Un antivirus
  - Des passerelles VPN modes SSL et IPSec
- Un outil capable d'effectuer des analyses comportementales
- Seul problème : l'inquiétude subsiste chez certains utilisateurs de confier la totalité de leur politique de sécurité à un même fournisseur



Quelques UTM du marché

Solutions	Caractéristiques
TippingPoint de 3Com	Fondé sur une architecture IPS, avec pare-feu, VPN IPSec, routage, gestion dynamique de bande passante, de filtrage d'URL et de contenu, 3,470 €.
A210R de Arkoon Network Security	Pare-feu, passerelle VPN IPSec, IDS contextuel, filtrage de contenus, antispam, QoS, authentification. Carte accélératrice. 5.000 € pour 100 postes.
Safe@Office de CheckPoint	Dédié PME, pare-feu, antivirus de passerelle, VPN, filtrage Web, administration de type Web
C12 de Crossbeam Systems	Pare-feu avec débit de 4 Gbps, antivirus, IDS et IPS, sécurisation de flux XML, filtrage d'URL
Fortigate de Fortinet	Pare-feu, VPN IPsec et SSL, antispyware, antispam, filtrage d'URL
SonicWall	Pare-feu aec VPN 30 Mbps, antivirus, antispyware IPS, filtrage d'URL
Firebox de WatchGuard	Pare-feu, passerelle VPN, IPS, filtrage d'URL, antispam, antivirus, antispyware

CheckPoint

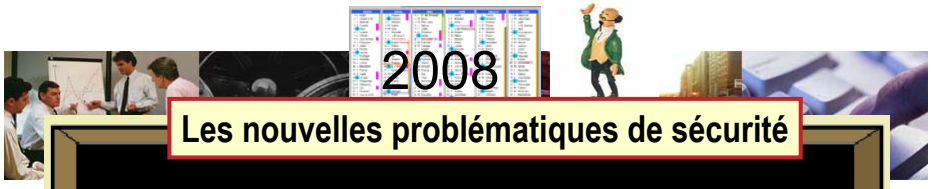
Watchguard

Un nouveau concept : NBA (Network Behavior Analysis)

- Plate-forme de pilotage qui permet à un opérateur de réagir intelligemment à une attaque. Se situe entre les outils IPS et SIEM.
- Très intéressant pour les attaques sophistiquées, « lentes » ou « zero day »
- Complète l'IPS par un contrôle interne du réseau
- Un NBA analyse le trafic « propriétaire » qui provient des équipements de réseau, formaté en fonction de leur origine : Net Flow de Cisco, cFlow de Juniper, NetStream de Huawei, sFlow de Foundry Networks…
- Le NBA repère les activités suspectes par des mécanismes déterministes (signatures) ou non déterministes (anomalies) : connexions de machine à machine, client qui devient serveur, usage détourné de protocole ou d'application, violation de la politique de sécurité, pic de trafic inhabituel, consommation anormale de bande passante
- Les interventions sont à faire manuellement…mais ce n'est pas un retour en arrière !!!

Ne pas confondre avec la célèbre NBA…

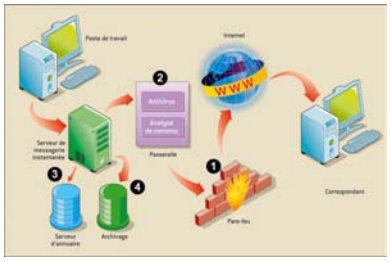
Editeur	Solution
Arbor Networks	PeakFlow
GraniteEdge Networks	ESP
Lancope	StealthWatch
Cisco	MARS
Intrusic	Threat Intelligent System
Q1 Labs	QRadar
Mazu Networks	Profiler

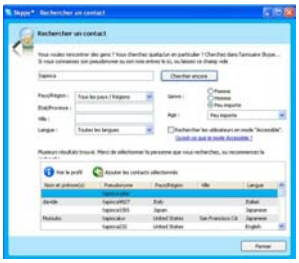


Les nouvelles problématiques de sécurité

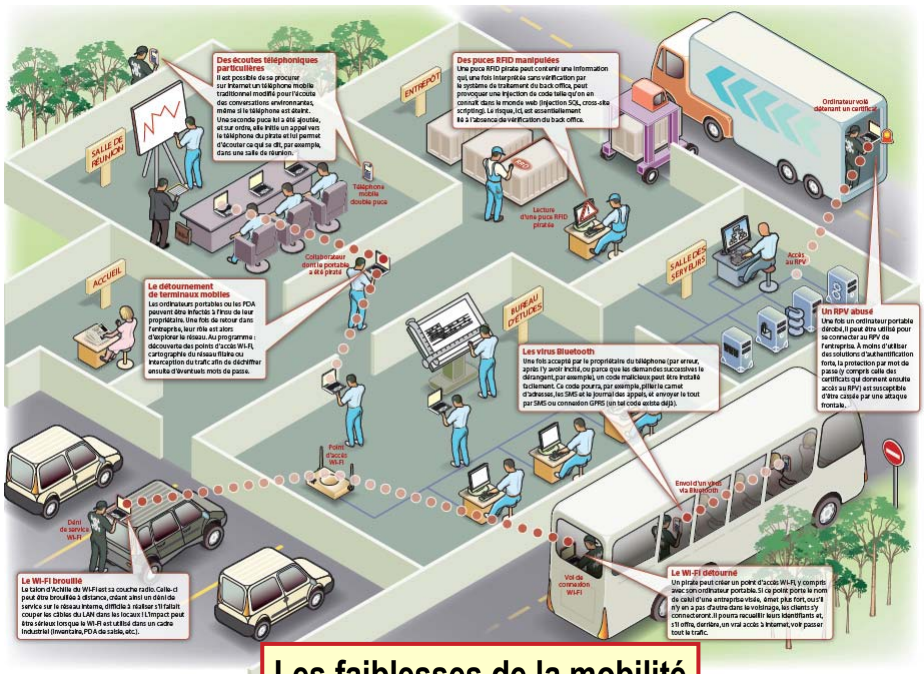
- Messagerie instantanée
- Wi-Fi
- Les PABX téléphoniques
- Une faille nouvelle : les hyperviseurs

La sécurité liée à la messagerie instantanée





- **L'IM induit des failles supplémentaires :**
  spam : il suffit de faire une recherche sur Skype pour avoir tous les Tapioca de la planète
  possibilité d'encapsuler le trafic IM dans des trames http80, donc de faire passer du trafic de nature douteuse…(cheval de Troie, bot)
- **Il n'y a que 11 % des entreprises qui appliquent une politique de sécurité IM (Radicati)**
- **Plus de 80 % des nouvelles menaces de 2005 concernaient l'IM**
- **La solution :**
  1. bloquer les ports, mais ça ne règle pas le problème du port 80
  2. analyser le contenu des trames pour le trafic IM qui emprunte le port 80
  3. authentifier et chiffrer : connexion à un annuaire et chiffrage SSL
  4. archiver les messages pour revenir dessus en cas de litige



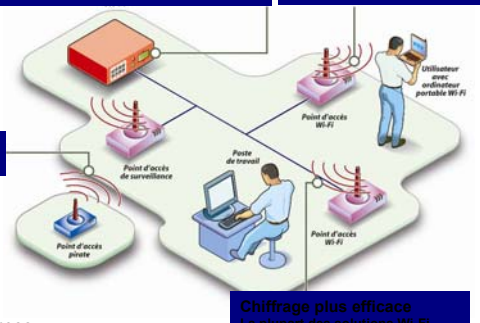
Les faiblesses de la mobilité

La sécurité Wi-Fi

Contrôle centralisé
Le contrôle peut aussi être assuré par un commutateur Wi-Fi associé à des points d'accès allégés, à un point d'accès maître (Cisco) ou à un module spécifique ajouté au commutateur standard.

Difficultés d'administration
Certaines options de sécurité : AES, RPV IPSec et mécanismes d'authentification nécessitent d'intervenir sur les postes clients

- **La sécurité intervient à deux niveaux :**
  - le chiffrage pour garantir la confidentialité des flux
  - l'authentification pour garantir les droits à émettre et recevoir



La surveillance est souvent assurée par les points d'accès

- **La sécurité au niveau des bornes d'accès et/ou cartes clientes est souvent mal assurée :**
  - réglage puissance d'émission des bornes :
  - étude du rayonnement des cellules (ne pas trop "inonder")
  - désactivation des services d'administration disponibles et inutiles
  - changement du SSID par défaut
  - désactivation du Broadcast de SSID
  - filtrage des adresses MAC

Chiffrage plus efficace
La plupart des solutions Wi-Fi utilisent des clés temporaires TKIP

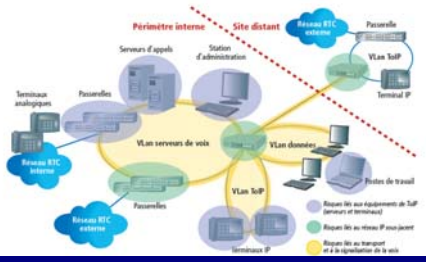
Wi-Fi : un problème qui se règle

- A l'origine : WEP (Wired Equivalent Privacy), avec une clé 64 bits permanente : 5 heures pour la retrouver, tous les outils sont sur Internet : Web_crack, Web_decrypt…
- Solutions de protection
  - WPA1 (Wi-Fi Protected Access)
    - Mise à jour logicielle sur les points d'accès et pilote de carte réseau
    - Nouveau protocole de chiffrement, avec clé de 128 bits renouvelée tous les 10.000 paquets, contrôle d'intégrité de message
  - WPA2
    - Basé sur AES, meilleur que RC4 de WEP, mais nécessite le changement de la puce Wi-Fi, clé de 128 bits et nouveau système d'authentification

Fabricant	Solution Wi-Fi	Fonctions de base	Nb d'accès
Aruba	Commutateur Aruba 800/2400/5000 et point d'accès AP60/52	Chiffrage WEP, WPA, WAP2, authentification 802.1x/EAP, terminaison VPN, détection de points d'accès pirates, prévention d'intrusions	8 max
Cisco	Point d'accès Aironet série 1200, WDS et WLSE	Chiffrage WEP, WPA, WAP2, authentification 802.1x/EAP, pas de VPN, détection de points d'accès pirates, prévention d'intrusions	16 max
	Cisco Wireless LAN Controler Série 4100 et points d'accès Cisco série 1000 (suite à l'acquisition d'Airespace)	Chiffrage WEP, WPA, WAP2, authentification 802.1x/EAP, terminaison VPN, détection de points d'accès pirates, prévention d'intrusions	16 max
Colubris Networks	Point d'accès CN1250	Chiffrage WEP, WPA, WAP2, authentification 802.1x/EAP, terminaison VPN, détection de points d'accès pirates, prévention d'intrusions annoncée grâce au partenariat avec AirMagnet	
Siemens	Routeur Beacon Works, points d'accès BeaconPoint (acquisition de Chantry Networks)	Chiffrage WEP, WPA, WAP2, authentification 802.1x/EAP, pas de VPN, détection de points d'accès pirates, prévention d'intrusions	16 max

Les failles méconnues de la téléphonie IP

- L'IPBX est devenu une cible privilégiée
- Il y a peu d'informations sur les attaques, les utilisateurs sont discrets…
- **Les vulnérabilités**
  - Modem de télémaintenance non protégé (Login/psw)
  - Ports de communication ouverts par défaut
  - Accès X.25 non protégé
  - Modem connecté à un PC, lui-même connecté au LAN de l'entreprise
  - Combifax connecté au réseau téléphonique et au LAN de l'entreprise
  - SDA (Sélection Directe à l'Arrivée): poste accessible sans contrôle depuis l'extérieur



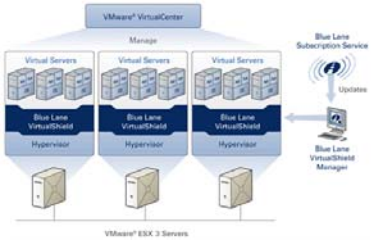
- **Les risques**
  - Déni de service
    - Revente de minutes téléphoniques
    - Utilisation d'un PABX tiers pour accéder à des services surtaxés
    - Ecoute type VoMIT (Voice Over Misconfigured Internet Telephones) : espionnage industriel
    - Détournement de PABX pour le compte d'un tiers
    - Phishing
    - Chantage
    - SPLIT : Spam téléphonique et risque de
    - Flooding des boîtes vocales (le spit est dix fois

Les précautions

Cloisonnement voix-données avec un VLAN, doté de règles strictes
VPN pour les liaisons VoIP sur réseau étendu
Renforcement des protocoles de transport et de signalisation, ex : Secure RTP plutôt que RTP (transport), chiffrement SSH et HTTP pour l'administration et la gestion à distance
Renforcement des procédures d'authentification, installation régulière des patch, durcissement des OS

Page 31/56

Une faille nouvelle : l'hyperviseur VMWare



- En prenant le contrôle de VMWare, un hacker peut prendre la main sur n'importe quelle machine virtuelle
- Ce qui est d'autant plus délicat que les utilisateurs exploitent justement VMWare pour isoler les applications les une des autres

- Un utilisateur ayant des droits administrateur sur la machine virtuelle peut parvenir à corrompre la mémoire du processeur hôte et donc potentiellement exécuter du code arbitraire sur le système d'accueil
- Une faille du serveur DHCP livré avec VMWare peut être exploitée pour acquérir les droits administrateur sur le système hôte vulnérable
- Plusieurs problèmes dans la manipulation de requêtes MS-RPC de SAMBA peuvent être exploités pour provoquer un débordement de pile côté serveur
- Egalement une vulnérabilité du serveur DNS
- Récemment une vulnérabilité dénoncée par Core Security Technologies qui concerne les postes de travail qui peuvent « sortir » de l'OS invité et hacker le système hôte
- Les premières protections apparaissent : un appliance ServerShield (avec la technologie VirtualShield) chez Blue Lane, VMShield chez Catbird, un agent logiciel de surveillance, Tripware Enterprise for VMWare ESX, un auditeur de configuration et de la politique de sécurité

Page 32/56

Les techniques des hackers

- **Analogies avec une action militaire**
  - Rassembler des informations sur la cible
  - Mettre en évidence les faiblesses adverses
  - Préparer et lancer une attaque
- **Ils "travaillent" en trois phases**
  - Compréhension de l'infrastructure cible : la partie administrative de l'attaque
    - Contacts, plage d'adresses IP, serveurs DNS, serveurs de messagerie, firewalls, systèmes de détection d'intrusion, noms de domaines
    - Les serveurs whois sont aujourd'hui démultipliés, ex : www.whois.net
    - On peut interroger les DNS s'ils sont mal protégés
  - Recensement des services actifs et les ports correspondants pour mettre en évidence les faiblesses : le scanning
    - Systèmes actifs et accessibles via Internet, protocoles actifs (TCP/UDP…), OS, patch, ports actifs
    - Caractéristiques des accès distants (RAS) : numéros de téléphone analogiques/numériques, mécanismes d'authentification, RPV et protocoles adaptés : IPSEC, PPTP
  - Recherche des comptes valides : userid (login), noms de groupes…

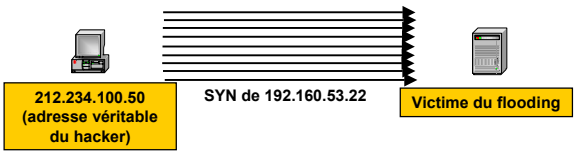
Le Déni De Service (DDS) ou DoS

- **Saturer la machine cible avec du trafic inutile afin de mettre son système « à genou ».**
- **Cette méthode d'attaque se nomme aussi *flooding* car il s'agit *d'inonder* un système pour le noyer sous un flot d'information. Le but est d'empêcher la cible d'accomplir sa tâche habituelle**
- **Deux types de Dénis de Service: ils peuvent concerner**
  - Les applicatifs
  - Les réseaux (TCP/IP)
- **Difficultés évidentes liées aux attaques DdS**
  - Possibilité de le confondre avec du vrai trafic utile (faux positifs)
- **Moyens de protections**
  - Augmenter la capacité du serveur (coûteux et peu efficace)
  - Dresser une liste d'IP suspectes et en interdire l'accès…ça ne sert pas à grand-chose
  - Analyser le comportement du réseau : détection des IP d'attaque, essayer d'arrêter l'émetteur, établir un référentiel de charge du réseau pour analyser les écarts

En 2001 CNN a été bloqué par une attaque de flooding, tout comme eBay, Amazon, Yahoo! et les DNS primaires .com américains : spectaculaire et très difficile à empêcher

Exemple de Déni de Service : SYN Flooding

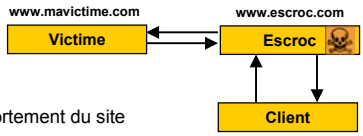
- **Utilise la connexion en trois temps du protocole TCP/IP :**
  - Envoi d'un message de synchronisation par le client (SYN)
  - Accusé de réception envoyé par le serveur (SYN-ACK)
  - Confirmation du client (ACK)
- **Le SYN flooding consiste à ne pas envoyer de message ACK pour laisser en suspens les demandes de connexions. Il suffit de ne pas mettre l'adresse IP source**
- **Ces connexions en suspens, en grand nombre, utilisent beaucoup de ressources et bloquent facilement le système cible.**



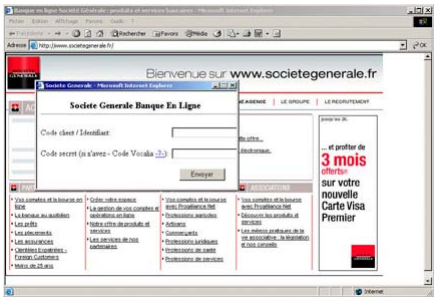
La victime est inondée de demandes de synchronisation TCP auxquelles elle ne peut pas répondre, puisqu'elle ne trouve pas l'adresse IP à qui l'envoyer (jusqu'au time out)

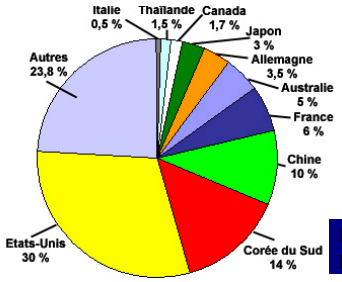
Le spoofing

- **Spoofing : imposture, faux, se faire passer pour quelqu'un d'autre**
- **Objectif : accéder à des informations confidentielles**
- **Différentes formes de spoofing : IP spoofing, DNS spoofing, Mail spoofing, Web spoofing**
- **Ex : web spoofing**
  - Un client se connecte à un serveur http://www.mavictime.com
  - Un spoofer s'interpose et remplace l'adresse http://www.mavictime.com par http://www.escroc.com
  - Le spoofer récupère les bonnes pages, mais les modifie avant de les renvoyer au demandeur
  - Protections
    - SSL
    - Patch et mise à jour du navigateur
    - Désactiver Java et Active X (???)
    - Barre d'adresse toujours visible
    - Affichage source du document
    - Toujours rester sceptique et vigilant sur le comportement du site
  - Une parade efficace
    - Utilisation d'un"SYN relay" qui n'envoie au web que les requêtes dont l'adresse source est valide



Le phishing : ne jamais avoir confiance





- Le phishing consiste à faire croire à un internaute qu'il est connecté sur un site familier : une banque, site de commerce, d'enchères, etc pour lui demander des informations confidentielles sous prétexte de restructuration ou de problème technique (mots de passe).
- Le pirate reconstruit le site à l'identique.
- Ce type d'attaque devient encore plus dangereux s'il est associé au CSS (Cross Site Scripting), une faille des serveurs qui les fait réagir à des scripts insérés dans une URL d'accès et qui permet d'insérer du code malicieux dans le véritable site.
- Le pharming est issu de cette technologie, qui nécessite au préalable l'infection du serveur DNS

La Chine et les USA, des cibles privilégiées…on n'arrête pas le progrès…

John Draper
est le père du piratage téléphonique

Marc Abene
Détournement de lignes téléphoniques en 1994

Johan Helsingius
A l'origine (1988) de l'un des plus grands remailers anonymes de l'histoire

Ivanov et Gorshkov
Hackers russes, volent des n° de cartes bancaires, mais tombent dans un traquenard du FBI

Yeron Bolondi
attaque de la banque Sumitomo à Londres en 2005 (keylogger matériel)

Gary McKinnon
(le hacker du Pentagone : risque 70 années de prison)

Kevin Mitnick
Le hacker le plus célèbre. Un film a été tourné sur son Histoire.

Brian Salcedo
En 2004, condamné à 9 ans de prison pour avoir tenté de voler des données bancaires sur le réseau Wi-Fi de Lowe

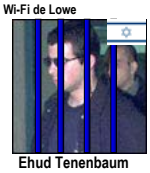
Vladimir Levin
Pirate Citybank et détourne 10 M$. Arrêté par Interpol. 3 ans.

Ian Murphy
La première personne inculpée (1981) pour crime informatique : intrusion dans le SI de ATT

Quelques hackers célèbres

Kevin Poulsen
En 1990, prend le contrôle des lignes d'une radio de LA et gagne une Porshe !!!

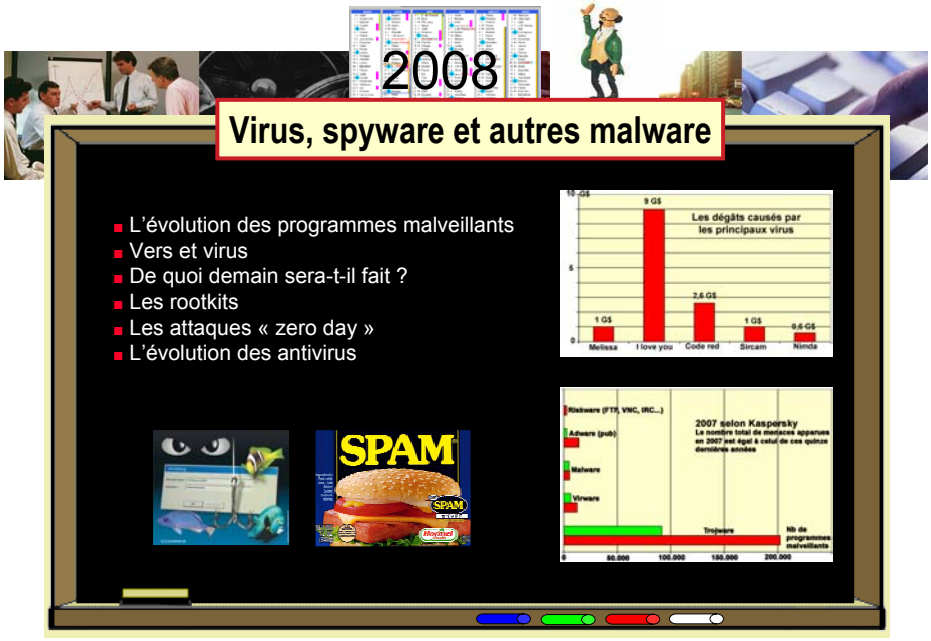
Eric Raymond
Hacker mais connu aussi pour son essai de défense du libre : « la cathédrale et le Bazar ».



Ehud Tenenbaum
Le pirate du Pentagone, mais aussi de la NASA, du FBI et de l'US Air Force !!!

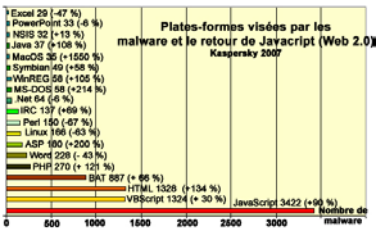
Michael et Ruth Haephrati
DDoS à la demande sur des cibles ponctuelles

Tsutomu Shimomura
Joue un rôle majeur dans l'arrestation de Mitnick (San Diego Supercomputing Center)



L'évolution des programmes malveillants

- **Le cru 2007 : le nombre de menaces a plus que doublé**
  - Trojware, Virware, Malware, Adware, Riskware : 220.000 en 2007
- **Les tendances de l'année :**
  - Vol de données
  - Développement des chevaux de Troie de chiffrement
  - Les premiers véritables vers et virus pour le Mac
  - L'apparition de chevaux de Troie pour J2Me
  - Développement des outils de simulation d'activités, tels que SubVirt et BluePill
  - Les cibles se diversifient avec l'IM
- **Les programmes malveillants les plus répandus (Kaspersky)**
  - Les Trojware : chevaux de Troie qui ne peuvent pas se démultiplier seuls : porte dérobée,outils de dissimulation d'activités et tous les chevaux de Troie, ont progressé de 119,7 % (ils représentent 89,45 % du total)
  - Les Virware : virus et vers qui se démultiplient…sans aide, progressent de 97,64 % (6,11 %)
  - Les autres Malware : 4,44 % du total

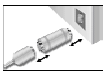


Tous les cibles de malware, cumulées en 2007 (8.487), ne représentent que 3,7 % des attaques sur Windows (228.593)

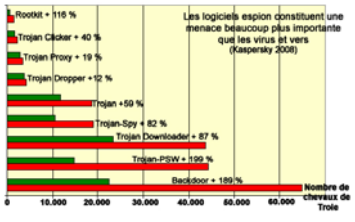
La palme de la stupidité

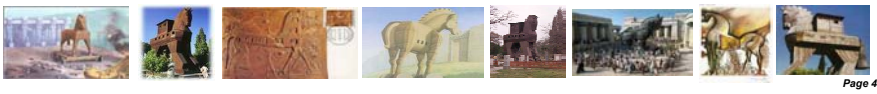
Le virus qui parle (en turc) : un ver qui se propage par mail, avec l'objet « écoutez et souriez » et se sert de l'application Speech Engine de Microsoft :
« How are you ? I am back. My name is mister Hamsi. I am seeing you. Haaaaaaaa. You must come to Turkiye. I am cleaning your computer. 5. 4. 3. 2. 1. Gule. Gule »

Le cheval de Troie



- **On assiste à une résurgence de cette technique : + 119 % en 2007**
- **Le renifleur de clavier (keylogger ou password stealer) est un cheval de Troie qui enregistre les caractères frappés au clavier**
  - Un Israëlien, Yeron Bolondi, s'attaque en mars 2005 à Londres à la banque japonaise Sumitomo Mitsui et place des renifleurs matériels pour récupérer les éléments de pénétration et effectuer des transferts électroniques de fonds.
  - Michaël Haephrati (Israël) et sa femme, vendaient du DDoS sur des clients ciblés, « dotés » au préalable d'un cheval de Troie pour en prendre le contrôle : 3.000 € l'opération (en 2005)
- **Les chevaux de Troie les plus répandus**
  - **Backdoor** : Utilitaire système installé dans un logiciel à l'insu de son propriétaire qui permet d'en prendre le contrôle à distance ultérieurement
  - **Trojan** : programmes qui endommagent les machines des victimes et menacent l'intégrité de leurs données
  - **Trojan-clicker** : redirige vers d'autres sites Web, pour augmenter le nombre de visites ou lancer une attaque DDS
  - **Trojan-Downloader** : télécharge et installe des programmes malveillants ou des bannières publicitaires
  - **Trojan-Dropper** : permet d'installer d'autres programmes malveillants
  - **Trojan-Proxy** : donne un accès anonyme depuis les Ordinateurs attaqués, populaire auprès des spammeurs
  - **Trojan–PSW** : volent des informations confidentielles
  - **Trojan–Spy** : enregistrent les frappes au clavier, les journaux…

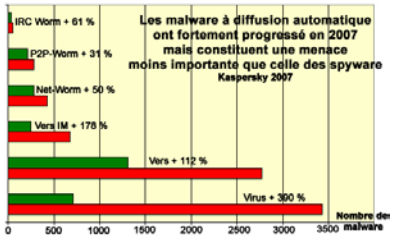




Les vers et virus

- + 97% en 2007 par rapport à 2006
- Ce sont les virus traditionnels qui ont affiché la plus forte croissance, du fait de la popularité des clés USB
- Gros danger avec les virus polymorphes
- Avec des épidémies moins nombreuses
  - Toujours ciblées géographiquement et réparties en 3 groupes
  - Le ver Nyxem.e, surtout en Inde et Amérique du Sud (Pérou), avec une fonction malveillante, qui supprime le 3 de chaque mois tous les fichiers utilisateurs
  - Les vers des familles Bagle et Warezov (plus de 20 variantes de ce ver apparues en un temps très court), mais aussi le ver « asiatique » Viking (surtout en Chine)
  - Différentes versions du cheval de Troie de chiffrement Gpcode, surtout dans la zone russophone d'Internet, chiffre les données utilisateurs, puis exige une rançon pour effectuer le déchiffrage
    La première version de GPcode.ac utilisait un algorithme RSA avec une clé de 56 bits

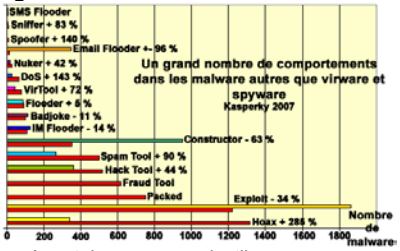
- **Les formes les plus courantes de vers et virus**
  - **Vers e-mail** : se propagent via des messages infectés : pièce jointe ou lien vers site infecté
  - **Vers-IM** : se propagent par des liens vers des sites infectés, à partir de la liste des contacts
  - **Vers-IRC** : s'attaquent aux canaux de chat, envois vers des sites infectés ou envois de fichiers infectés aux contacts
  - **Vers-réseaux** : copient le ver dans les ressources réseaux, pénètrent les réseaux publics, utilisent souvent d'autres vers comme porteurs du logiciel malveillant
  - **Vers-P2P** : se copient dans un répertoire partagé par les membres du P2P
  - **Vers** et **virus** traditionnels



Les autres malware…et tendances connexes

- **L'imagination des hackers ne se limite pas aux virus, vers et chevaux de Troie**
- **Toute une série de programmes malveillants, difficiles à classer, sont apparus, moins nombreux, mais potentiellement très dangereux**

- **Constructor** : des outils qui permettent de fabriquer des codes malveillants. Interface visuelle et conviviale (?) : on choisit le type de virus, les objets à attaquer, les options de chiffrage, les protections contre le désassemblage…
- **Bad Jokes, Hoax** : n'infectent pas la machine cible, affichent de faux avertissements. Il faut avoir le sens de l'humour !!!
- **Exploit** : logiciels qui exploitent une faille du système, de la messagerie, du serveur HTTP, etc



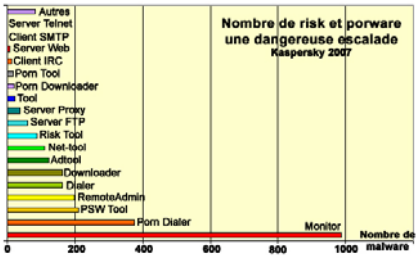
- **Flooder** : Logiciels qui inondent les canaux avec des données et des messages inutiles
- **Hack Tools** : Outils pour transformer les machines en zombies (via backdoor) ou pour télécharger d'autres programmes malveillants, sur la machine de la victime
- **IM-Flooder** : Identiques aux flooders, mais se servent des canaux spécifiques de l'IM
- **Spam Tools** : Logiciels non souhaités
- Deux nouveaux venus : Packed et Fraud tools

- **Deux fortes tendances connexes :**
  - Chantage (ransomware) : blocage de la machine ou blocage de l'accès aux données et rançon
    6 chevaux de Troie pour cela en 2006 : Krotten, Daideneg, Schoolboys, Cryzip, MayArchive, GpCode
  - Logiciels publicitaires : pas dangereux, mais exploitent de plus en plus des techniques de virus

Riskware et Pornware

- **Les riskware sont des programmes légitimes qui peuvent être détournés à des fins malveillantes**
  - Suppression, blocages des accès, modification ou copie d'informations, perturbation de la machine ou du réseau : Monitor est le plus répandu
  - Nombreux désaccords entre les éditeurs des logiciels de riskwares et les éditeurs d'antivirus : plusieurs procès intentés en 2007, gagnés le plus souvent par les éditeurs d'antivirus
- **Les pornware**
  - Dialers : numéroteurs vers des sites pornographiques payants…d'où procès avec les opérateurs téléphoniques
- **PSW-Tool (récupération de mots de passe) et RemoteAdmin se sont fortement répandus**

Au total une progression de 100 % pour 2690 risk et pornwares



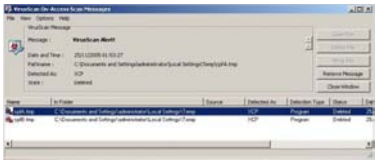
Les malware empruntent tous les chemins possibles : pornographique, publicitaires (+ 456 % en 2007)

Les rootkits

- **Les rootkits viennent du monde Unix : des progammes qui modifient les kernel syscalls, les liens entre les services kernel et les applications**
- **Utilisés à des fins malveillantes, ils permettent de rendre invisibles un autre programme et son activité : processus, fichiers et connexions d'un pirate**
- **Il faut une machine déjà compromise**
- **Ils ne se répliquent pas (ce ne sont pas des vers)**
- **Parfaits pour cacher des bots, des backdoors, des spyware et autres programmes indésirables**
- **Les plus connus : FURookit, IsPro, Hacker Defender et Sony BMG**
- **Scandale de Sony BMG : un rootkit permettait de rendre invisible le système de protection XCP de Sony…et donc d'autres programmes malveillants de la machine**
- **Sony l'a retiré…mais non sans mal !!!**

Les rootkits ont progressé de 116 % en 2007 : essentiellement du fait de l'activité du ver Zhelatin

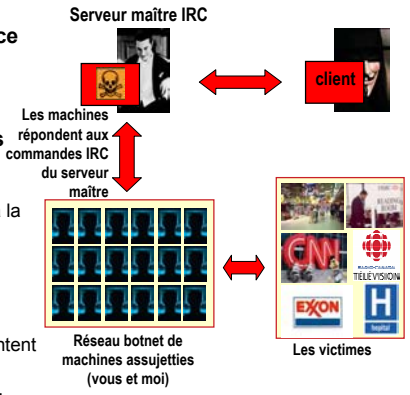
La proposition F-Secure



Hacker Defender est maintenant détecté par les anti-virus

Les botnets : le danger vient de partout

- **Les robots ou bots, installés sur les ordinateurs des réseaux, les transforment en zombies, pour servir de relais de spam, phishing, pour capturer des mots de passe, désactiver un pare-feu ou un antivirus et contribuer à une attaque DDoS**
- **Ensemble ils constituent des botnets, au service de criminels, qui les louent au profit de tiers (entre 50 et 1000 € le botnet)**
- **On est bien dans le domaine de la cybercriminalité et 6000 entreprises auraient déjà payées les rançons demandées (Rand Corp)**



- Février 2004 : une rançon de 28 M$ est demandée à la banque japonaise Softbank pour que ne soient pas divulgués les comptes de 4,5 millions de clients
- Octobre 2005 : 3 hommes sont arrêtés en Hollande, qui voulaient attaquer en DDoS eBay et PayPal, avec un botnet de 100.000 machines
- Novembre 2005 : des hackers au Moyen-Orient montent un botnet de 17.000 machines
- Et la star (!!) : Jeanson Ancheta, en novembre 2005, arrêté et condamné pour avoir loué des botnets avec 400.000 machines infectées : 5 ans de prison

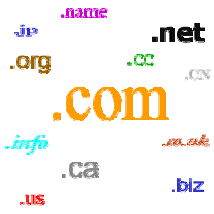

Quelques spécificités de 2007

- Globalement les attaques ont été beaucoup plus sophistiquées
- D'après F-Secure, le million de virus sera atteint fin 2008 : il fait état de 25.000 nouvelles attaques par jour
- **Les techniques nouvelles de diffusion**
  - Drive-by-Download : la victime est dirigée vers un site Web infecté qui installe et exécute un malware (il suffit de cliquer sur un lien « attrayant »)
  - De plus en plus de publicités sont infectées : TV4.se, Expedia, NHL, MLB…
  - Technique de multiplication des mots clés, indexés par Google : il suffit d'attendre que la victime visite les sites infectés
  - Hacking des sites à fort tirage, avec exécution d'un code JavaScript sur le poste de l'utilisateur : s'est répandu sur les sites de magazines
- **Sophistication des attaques** : quelques exemples pour 2007
  - iFrame (Inline Frame) : permet d'insérer un cadre et d'afficher des pages HTML locales ou distantes
  - La victime visite un site piégé (avec un iFrame invisible) et se retrouve redirigé vers un site Web où se trouve le code PHP MPack (ou IcePack, n404…), un outil commercial de piratage développé et maintenu par des pirates russes (vendu entre 700 et 1.000 €), très simple à installer

En juin 2007, déjà 10.000 sites touchés par les iFrame détournés (80 % en Italie), mais 80.000 à la fin 2007 !!!
Il suffit d'attirer la victime vers un site piégé…

Quelques spécificités de 2007

- **StormWorm** : un botnet P2P (sans doute le plus subtil), qui cible Windows, se propage par mail et incite la victime à se connecter sur un site qui exploite une faille et proposant des contenus attrayants.
Très difficile à éradiquer
- **Domain Tasting** : consiste à exploiter la procédure d'enregistrement et de facturation des « registrar » noms de domaines. Un grand nombre de domaines éphémères ont été utilisés à des fins malveillantes en 2007.
- **Carding** : le marché mondial aux « voleur », avec trois phases : le « coding » (piratage proprement dit), « vending » (vente) et « cashing » (fausses transactions financières pour blanchir l'argent récolté – Wester Union est mis en cause)
  - En 2005 : affaire Card System aux USA avec 70.000 cartes piratées…et utilisées
  - En 2007 : affaire TJX avec 45 millions de cartes piratées
- **Rootkit très sophistiqué** : Mebroot apparu fin 2007, diffusé par Drive-by-Download, fondé sur une vielle technique, le remplacement du MBR (Master Boot Record) par un code infecté.
Les premiers rootkits MBR ont été des chevaux de Troie bancaires ciblant des banques en ligne



Le Domain Tasting est détourné à des fins malveillantes : il suffit d'utiliser les noms de domaines créés pendant cinq jours et de ne jamais les payer !!!

TJX

Quelques spécificités de 2007 : l'attaque sur les mobiles

- Les premiers chevaux de Troie pour mobiles
  - Kiazha en Chine : infection suite au téléchargement d'un shareware sur le smartphone
  - La victime reçoit un message qui lui réclame 7 $ pour la désinfection…
- Les vers Beselo se sont répandus via MMS et Bluetooth pour smartphones Symbian (extension SIS)
  - La victime croit qu'elle télécharge un fichier visuel ou musical
  - Les fichiers les plus utilisés : beauty.jpg, sex.mp3, love.rm : il faut répondre non à toute installation
- HatiHati.A est un ver qui se propage par les cartes MMC
  - Il diffuse des SMS vers un numéro prédéfini très coûteux
- Et même l'iPhone, cracké par Charlie Miller
  - Il suffit que l'utilisateur soit invité, via un mail ou un simple SMS à se rendre sur une page Web infectée par un code qui s'activerait sur le téléphone, le mettant en contact direct avec le pirate.
  - Celui-ci n'a plus qu'à sélectionner le type d'information recherchée (données personnelles) et à les faire remonter. Il est aussi envisageable de bloquer l'appareil par le même procédé, de lui faire exécuter des appels, ou de le transformer en "ordinateur-zombie" pour transmettre des spams…

Charlie Miller et une équipe de chercheurs ont démontré la « violabilité » de l'iPhone…

Page 51/56

De quoi demain sera-t-il fait ?

- **Les prévisions pour les années à venir**
  - Chevaux de Troie pour vol de données : pour les utilisateurs de systèmes bancaires, de systèmes de paiement en ligne et d'accros des jeux en ligne
  - La fusion entre les virus et les spam va se poursuivre : les hackers utiliseront de plus en plus les machines infectées pour diffuser du courrier indésirable
  - Les voies les plus courantes de pénétration : messagerie instantanée ou non, vulnérabilités des navigateurs. Les attaques directes sur les ports seront moins nombreuses, l'IM sera très utilisé et à un degré moindre les réseaux P2P et IRC
  - Les épidémies et attaques seront encore plus localisées
    - Chevaux de Troie et vers pour les jeux en ligne avec fonctions virales en Asie
    - Chevaux espions et portes dérobées en Europe et Amérique du Nord
  - Les technologies sous-jacentes seront toujours plus complexes et les hackers exploiteront encore plus les techniques de polymorphisme et de dissimulation d'activités
  - Le nombre d'attaques visant les petites et moyennes entreprises va augmenter, avec Office de Microsoft, comme point d'entrée privilégié.

Les clients qui « ont à préserver le secret » de leurs transactions seront visés en premier…

Page 52/56

Ayez l'œil en 2008, les attaques se diversifient

- Attaques sur les réseaux sociaux : Facebook, MySpace
- Déjà arrivé en 2007 : l'idée est de placer du code malveillant dans les pages personnelles (PHP…)
- Portails de partage

- Attaques sur les applications hébergées (Saas)
- Ex de Salesforce.com

- Attaques sur les mondes virtuels
- Vols de mots de passe pour accéder à des comptes utilisateurs via des keyloggers (blanchiment d'argent…)

- ToIP
- L'interconnexion de la ToIP et des équipements réseaux induit une nouvelle politique de sécurité

- Vista
- Il y aura une vingtaine de failles en 2008

- Attaques par les mobiles
- Les applications embarquées sur les mobiles deviennent des cibles privilégiées

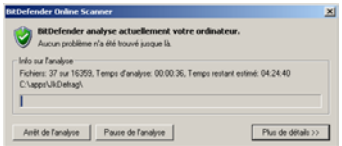
- Bots et rootkits
- La grande « mode » des prochaines années, car difficilement détectables

- Détournement de MP3
- Et d'autres pièces attachées : flash, etc.
- Véhicules à spam et malware

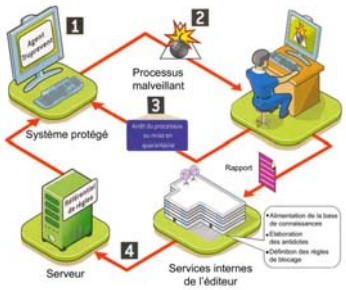
La sécurité en ligne et analyse comportementale

- Principe : détecter des agissements illicites par analyse du comportement des processus noyau
- Comportement illicite : ouverture de n copies d'un même processus, dépassement de la mémoire tampon allouée…
- Inconvénient : génère des faux-positifs
- Panda Software (Truprevent) ou Bee Ware (Intelliwall)

- **Sécurité en ligne**
  - Nombreuses solution d'analyse en ligne
  - Anti-virus : Panda (NanoScan), BitDefender, F-Secure, Trend Micro (House Call)…
- **Systèmes complets**
  - Le chinois Baidu
  - PSB de F-Secure : anti-spyware, anti-virus, pare-feu, anti-spam, anti-rootkit
  - Norton 360 de Symantec, One Care de Microsoft, Total Protection SMB de McAfee
  - …et Google Apps : Message Discovery



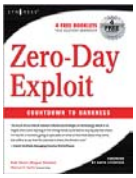
百度安全中心



1. Surveillance des ressources sensibles.
   L'agent Truprevent analyse les trames réseau et les mémoires tampon des processus, l'accès à la base de registres et à certains processus jugés sensibles. L'inspection peut se faire en continu, à la demande ou de façon périodique.
2. Détection d'un processus suspect
3. Mise à jour des règles comportementales.
   Le référentiel de l'éditeur (Panda pour Truprevent) est régulièrement enrichi.
4. Déclenchement de la riposte.
   L'administrateur reçoit une alerte. En général, le processus est stoppé. Si c'est possible, il est sorti du noyau. Le programme qui l'a initialisé est mis en quarantaine.

Que faire contre les attaques « zero day »

- Une attaque « zero day » consiste à exploiter (l'exploit) une faille détectée, avant que l'éditeur du système attaqué, n'ait eu le temps de diffuser une parade.
- Les failles non détectées constituent un nouveau marché, avec des « détecteurs », des « acheteurs » et des « exploiteurs » de ces failles. Tout se monnaie…entre 500 et 2.000 $
- Les attaques zero-day en 2006/07 ont surtout ciblé Windows et à un niveau moindre Apple. Unix et Linux n'ont donné lieu à aucune attaque répertoriée de ce type
  - Six failles dans IE
  - Une faille dans la « graphical Device Interface Library » (wmf)
  - Cinq failles dans Office, 3 pour Powerpoint, une pour Excel et une pour Word
  - Une faille dans le Windows Help File Viewer
  - Une faille commune à IE et Outlook
  - Une faille dans un ActiveX XML HTTP
  - Quatre failles pour Apple : 2 pour Mac OS X et 2 pour Safari
  - mais aussi Real Player, ICQ, Kazaa via l'ActiveX « Download Manager », le SDK Direct X de Microsoft, le Jet Database de Microsoft (exploitable dans Word), Firefox, le MacBook Air…



- La seule solution disponible en 2008 pour contrer les attaques consiste à faire de la prévention et à analyser en permanence les services, machines, fichiers « à priori » vulnérables et toute anomalie de trafic.
- L'analyse comportementale avec ses risques de détection de faux positifs entre dans cette catégorie

iDefense, filiale de Verisign, et TippingPoint, division sécurité de 3COm, proposent de racheter les failles au fur et à mesure de leur apparition, avant qu'elles ne commettent des dégâts. IDefense a même organisé un concours début 2006 pour susciter la découverte de failles…qui ne seraient donc plus à découvrir !!!

DEFENSE
A VeriSign Company

ppingPoint
Technologies

Les points noirs de la sécurité informatique

Je vous remercie de votre attention