Panorama de la cybercriminalité

Année 2005

Objectifs du panorama

Apprécier l'émergence de nouveaux risques et les tendances de risques déjà connus

Relativiser ou mettre en perspective des incidents qui ont défrayé la chronique

Englober la criminalité haute technologie, comme des atteintes plus « rustiques »

Sélection réalisée par un groupe de travail pluriel (assureur, avocat, journaliste, officier de gendarmerie et police, offreurs de biens et de services, RSSI).

Sélection des événements médias

Illustration

- d'une émergence,
- d'une tendance,
- d'un volume d'incidents.

Cas particulier

- Impact ou enjeux,
- Cas d'école.

Les informations utilisées proviennent de sources ouvertes,

Les entreprises sont parfois citées par souci de précision et parce que leur nom a été communiqué dans les médias

Retour sur le panorama 2004

- Vol de données : code source et bases de données
  - Vol de code source Microsoft
- Chantage – extorsion – racket sur Internet
  - Pgpcoder et le rançonnage des fichiers
- Cyberterrorisme : de quoi parle-t-on ?
  - « Financement indirect » par usurpation de numéros de téléphones

Retour sur le panorama 2004

- Menaces sur la mobilité : GSM, VoIP, WiFi...
  - Aperçus sporadiques à travers le monde (ex. Jeux Helsinki)

Retour sur le panorama 2003

- Phishing : la triple imposture
  - Evolutions technologiques : pharming
  - Ciblage élargi : distribution, eBay, Google, USAF...

Quelques références

Vol de code source :

- Connecticut Man Pleads Guilty in U.S. Court to Selling Stolen Microsoft Windows Source Code, DOJ NYC, 29/08/2005

Chantage – extorsion – racket sur Internet :

- Les escrocs se mettent à la prise de fichiers en otage, 01net, 03/06/2005
- Nouvelle menace sur Internet : des fichiers d'ordinateur pris en "otages", AP 24/06/2005
- Apparition d'un nouveau virus rançonneur, AFP, 01/06/2005

Quelques références

CyberTerrorisme :

http://www.theregister.co.uk/2005/12/19/terror_phone_clone_scam/

Terrorists Turn to the Web as Base of Operations, Washington Post, 07/08/05

Menaces sur la mobilité :

- Commwarrior, le premier virus qui se propage par MMS, ZDnet 09/03/2005
- Helsinski : un virus attaque les mobiles au stade olympique ! Silicon.fr 11/08/2005(http://www.silicon.fr/getarticle.asp?ID=10996)

Quelques références

Phishing :

- Phishers target Yahoo Instant Messenger (http://news.com.com/Phishers+target+Yahoo+Instant+Messenger/2100-7349_3-5634007.html)
- Phishing : alertes sur des banques françaises (http://www.silicon.fr/getarticle.asp?ID=11049)
- La FIFA, victime d'une attaque par phishing, PCinpact,28/09/05
- Dangers of phishing and pharming, The Telegraph, 24/10/2005
- Phishing sous Paypal, PCINpact, 08/11/2005
- Supermarkets next in line for phishing attacks (http://www.theregister.co.uk/2005/03/14/supermarket_sweep/)
- Pharming protection for Internet users, Out-Law News, 22/04/2005
- EBay users hit by mass phishing attacks, vnunet, 03/01/2006

Panorama 2005

- Economie souterraine: robots, keyloggers, rootkits
- Espionnage économique: la convoitise
- Vol et pertes de données : les risques d'usurpation d'état civil
- Du harcèlement jusqu'aux violences physiques

L'Économie Souterraine

Sommaire

- La persistance des robots
- La vitalité des chevaux de Troie conventionnels (backdoors & keyloggers…)
- Le retour des rootkits

Persistance des robots

Rappel

Les robots sont des programme malveillant permettant une prise de contrôle à distance de machines vulnérables afin de former un réseau d'attaque caché (ou botnet).

Pour s'implanter, il utilise des méthodes classiques ; il peut être déposé sur la cible par :

- Un courrier électronique (spam),
- Un vers ou virus,
- Un cheval de Troie,
- Un autre robot déjà actif sur la machine.

Il peut posséder son propre module de propagation et exploiter :

- une vulnérabilité,
- des partages ouverts (open shares),
- des mots de passe faibles ou manquants.

Persistance des robots

Rappel

- Chaque robot est créé dans un but précis.
- On en découvre entre 25 et 50 nouvelles chaque jour !
- Le robot s'exécute silencieusement sur chaque système piraté et se connecte automatiquement à un serveur IRC prédéfini pour rejoindre son botnet.
- Chaque système piraté peut, dès lors, être piloté à distance par son concepteur ou par celui qui « loue » ses services,
- Il capturera de l'information,
- Il participera à des attaques groupées (DDoS),
- Il servira de relais de spamming et/ou de phishing,
- En 2005, il fut aussi largement utilisé comme diffuseur de programmes indésirables (adwares).

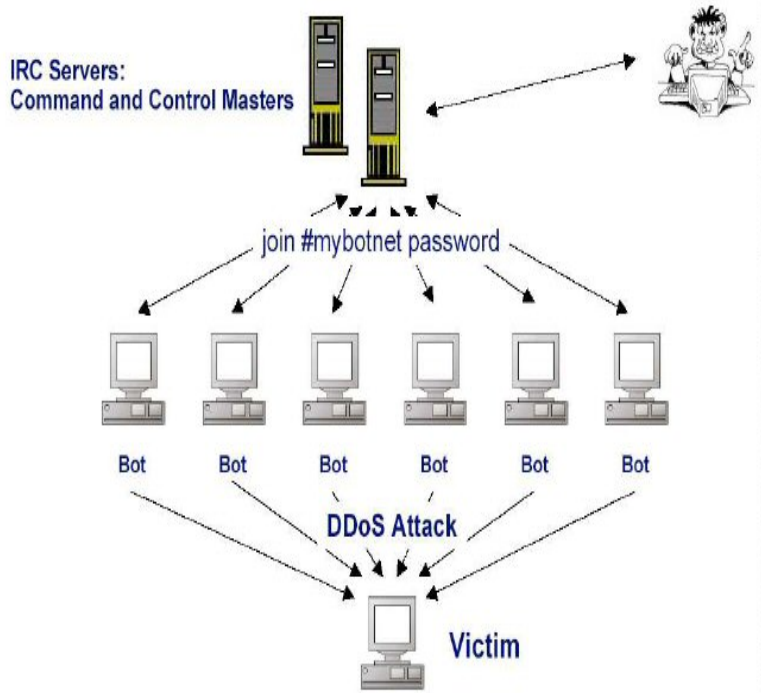


Schéma issu du document : Sécurité des postes de travail : Botnet, Alain Hugentobler

Persistance des robots

Exemples

Octobre 2005 : La police Hollandaise arrête 3 hommes soupçonnés de diriger un réseau de 100 000 ordinateurs. Ils se proposaient de mener des attaques DDOS et s'intéressaient aux comptes PayPal et Ebay de leurs victimes.

Novembre 2005 : Un groupe de pirates basé au Moyen-Orient serait parvenu à prendre le contrôle de 17 000 ordinateurs.

Novembre 2005 : Aux Etats-Unis, un homme est détenu sans possibilité de libération sous caution. Entre juin 2004 et août 2005, il a loué des réseaux de robots destinés à diffuser du spam ou à mener des attaques DDOS. L'homme était aussi rémunéré pour diffuser des adwares. On estime qu'il a ainsi mis la main sur plus de 400 000 ordinateurs.

Persistance des robots

États-unis

Août 2005

- 180solutions porte plainte contre sept de ses affiliés pour avoir diffusé ses adwares sans consentement initial. La société dénonce ainsi les agissements de personnes malintentionnées en Grande-Bretagne, en Australie, au Canada, au Liban, en Slovénie et en Hollande.
- Toutes ces personnes sont nommément désignées au FBI.

> The lawsuit alleges that the defendants -- Eric de Vogt of Breda, the Netherlands; Jesse Donohue of South Melbourne, Australia; Khalil Halel of Beirut; Imran Patel of Leicester, England; Zarox Souchi of Toronto; Youri van den Berg of Deventer, the Netherlands; and Anton Zagar of Trbovlje, Slovenia -- used botnets to install 180Solutions' software. The company has notified the FBI about its findings, but an FBI spokesman declined to say whether the agency was investigating the claims.

- Afin d'augmenter leurs gains (entre 7 et 50 cents par installation), elles auraient utilisées des réseaux de robots (botnet). Selon les experts, un réseau de 5000 machines permettait un revenu de $744 par jour, ou $22.346 par mois.
- 180solutions avoue avoir ainsi rétribué pour un montant total de $60.000 ces affiliés indélicats.

Persistance des robots

Pays-Bas

Octobre 2005

- Début octobre, la police Hollandaise arrête trois jeunes gens (19, 22 et 27 ans) accusés de s'être infiltrés dans 100 000 ordinateurs pour les contrôler à l'aide d'un programme viral dénommé « Toxbot ».
- Ils sont accusés de piratage, de destruction de données et de diffusion d'adwares et de spywares.
- 15 jours plus tard, la police annonce que le trio avait sous son contrôle plus 1,5 millions de machines et de serveurs.

Novembre 2005

- La société 180solutions annonce être un témoin clé dans cette affaire. Elle accuse ces trois personnes d'avoir mené –à ses dépens– des attaques en DDOS après qu'elle ait décidé de terminer le contrat d'affiliation qui la liait à ces individus.
- Alors que 180solutions fait tout pour améliorer son image de marque en se défendant de diffuser des produits sans le consentement des utilisateurs, elle poursuit également des sociétés de sécurité (tels que ZoneAlarm) pour préjudice commercial.

Persistance des robots

#Botz4sale (alias Jeanson James Ancheta)

U.S. Department of Justice

Debra Wong Yang
United States Attorney
Central District of California

United States Courthouse
312 North Spring Street
Los Angeles, California 90012

PRESS RELEASE

FOR IMMEDIATE RELEASE
November 3, 2005

For Information, Contact Public Affairs
Thom Mrozek (213) 894-6947

COMPUTER VIRUS BROKER ARRESTED FOR SELLING ARMIES OF INFECTED COMPUTERS TO HACKERS AND SPAMMERS

Indictment also Alleges Scheme to Use Botnets to Install Adware for Profit
Botnet Indictment

Los Angeles, CA - In the first prosecution of its kind in the nation, a well-known member of the "botmaster underground" has been indicted on federal charges for profiting from the use of "botnets" – armies of computers that are under the control of the botmaster and are used to launch destructive attacks or to send huge quantities of spam across the Internet.

Persistance des robots

#Botz4sale (alias Jeanson James Ancheta)

Juillet 2004

- Tout débute par la création d'une variante de « rxbot »,
- Première ventes en vue de spamming et d'attaques en DDOS.

> 91. Between on or about July 10, 2004 and August 7, 2004, ANCHETA sold bots to circa and received payments from circa via Paypal totaling approximately $400.

Août 2004

- Optimisation des ventes, chaque botnet est limité à 2000 machines.

> 103. In or about August 2004, ANCHETA updated his advertisement to increase the price of bots and proxies, to limit the purchase of bots to 2,000 "due to massive orders," and to warn, "I am not responsible for anything that happens to you or your bots after you see your amount of bots you purchased in your room [IRC channel]."

Persistance des robots

#Botz4sale (alias Jeanson James Ancheta)

Août 2004 à octobre 2004

- Mise en place, avec un complice, d'un système de diffusion d'adwares par le biais des machines contaminées. Le suspect devient l'affilié de plusieurs sociétés commerciales qui commencent à rétribuer son travail
- Les adwares sont modifiés sans la permission des sociétés éditrices afin de faciliter leurs propagations.
- Des sites gouvernementaux vont bientôt être « infectés ».

156. ANCHETA and SoBe would cause the advertising affiliate companies whose adware would be surreptitiously installed on an infected computer to be notified of that instance of installation, and to credit one of their affiliate identification numbers for that installation.

157. ANCHETA and SoBe would receive periodic payments from advertising service companies based upon the number of installations of adware that were credited to them.

Persistance des robots

#Botz4sale (alias Jeanson James Ancheta)

Novembre 2004 à avril 2005

- Le système de diffusion est bien rodé, les rétributions tombent régulièrement.

COUNT	APPROXIMATE DATES	APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION	APPROXIMATE PAYMENT
SEVEN	November 1, 2004 through November 19, 2004	26,975	$4,044.26 from Gammacash
EIGHT	November 16,2004 through December 7,2004	8,744	$1,306.52 from LOUDcash
NINE	January 15, 2005 through February 7, 2005	19,934	$2,988.11 from Gammacash
TEN	March 1, 2005 through March 22, 2005	53,321	$7,996.10 from Gammacash
ELEVEN	April 1, 2005 through April 22, 2005	28,066	$4,010.81 from Gammacash

Persistance des robots

#Botz4sale (alias Jeanson James Ancheta)

Novembre 2005

- Jeanson James Ancheta est arrêté, il plaide coupable. 17 chefs d'accusation sont lancés contre lui : conspiration, blanchiment d'argent, transmission de code à un ordinateur du gouvernement, accès non autorisé à un ordinateur protégé, fraude... Il risque jusqu'à 50 ans de prison ferme.

a. All right, title, and interest in any and all property involved in each offense, or conspiracy to commit such offense, for which the defendant is convicted, and all property traceable to such property, including the following:

(1) the approximately $2,989.81 in proceeds generated from the sale of bots and proxies, as alleged in Counts One through Three of the Indictment, and deposited into Wells Fargo Bank accounts ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(2) the approximately $58,357.86 in proceeds generated from the surreptitious install of adware on protected computers accessed without authorization, as alleged in Counts Four through Eleven of the Indictment, and deposited into a Wells Fargo Bank account ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(3) a 1993 BMW 325is, Vehicle Identification Number WBABF4318PEK09502, California license plate number j4m3zzz, which

Persistance des robots

Conclusion

- L'utilisation de programmes malveillants dans la diffusion d'adwares ne se limite pas à ces quelques exemples,
- Pour des personnes peu scrupuleuses, c'est un moyen facile de gagner de l'argent,
- Pour les sociétés publicitaires, c'est une nouvelle atteinte à leur image de marque,
- Quelques jours après l'apparition de la vulnérabilité touchant les images WMF (27 décembre 2005), plus de 6 sites Internet utilisaient cette faille pour diffuser des adwares.

L'Économie Souterraine

Persistance des robots - Références

- Computer virus broker arrested for selling armies of infected computers to hackers and spammers
  http://www.usdoj.gov/usao/cac/pr2005/149.html
  http://www.usdoj.gov/usao/cac/pr2005/Botnet_Indictment.pdf
- Adware Firm Accuses 7 Distributors of Using 'Botnets'
  http://www.washingtonpost.com/wp-dyn/content/article/2005/08/16/AR2005081600727.html
- Un adware témoin clé du FBI dans l'affaire botnet
  http://fr.news.yahoo.com/07112005/308/un-adware-temoin-cle-du-fbi-dans-l-affaire-botnet.html/
- Botnet operation controlled 1.5m PCs
  http://www.vnunet.com/vnunet/news/2144375/botnet-operation-ruled-million
- Cops Smash 100,000 Node Botnet, Botnet Army Disarmed
  http://www.governmentsecurity.org/forum/index.php?s=0ab4deb7fc036ad7ef7ce5165b859bfd&showtopic=16795
- Instant Messenger RootKit Worm Tied to Worldwide Bot Network Controlled by Group in Middle East
  http://www.facetime.com/pr/pr051117.aspx
- Un pirate au virus détenu sans caution aux États-Unis
  http://www2.canoe.com/techno/nouvelles/archives/2005/11/20051109-103854.html

L'Économie Souterraine

Sommaire

- La persistance des robots
- La vitalité des chevaux de Troie conventionnels (backdoors & keyloggers…)
- Le retour des rootkits

Importance des chevaux de Troie

Rappel

Les chevaux de Troie d'hier sont toujours à la mode :

- La porte dérobée (*backdoor*) : programme implémenté secrètement sur une machine et permettant ensuite à son concepteur de s'y introduire à distance.
- Le renifleur de clavier ou de mot de passe (*keylogger, password stealer*) : dissimulé sur l'ordinateur de sa victime, le programme saisie certaines frappes au clavier et collecte des noms d'utilisateur, des mots de passe et des informations personnelles et parfois confidentielles. Les données sont ensuite renvoyés et employés à des fins frauduleuses. Il existe également des solutions matérielles.

Importance des chevaux de Troie

Michaël et Ruth Haephrati

- Découverte en 2005, l'escroquerie durait depuis plus d'un an.
- Chaque cible faisait l'objet d'une attaque au travers d'un cheval de Troie unique créé à cet effet.
- L'anti-virus était inefficace (au moment des faits) car le programme ne circulait pas dans la nature.
- Le cheval de Troie était envoyé par e-mail ou intégré à un CD contenant une proposition commerciale imaginaire.

18 Arrested In Israeli Probe Of Computer Espionage

By Glenn Frankel
Washington Post Foreign Service
Tuesday, May 31, 2005; Page E01

JERUSALEM, May 30 -- Israel's business sector has been rocked by a major computer espionage scandal that was uncovered when a husband-and-wife book-writing team complained to police that someone had hacked into their computer system and stolen files.

Police said investigators traced the alleged theft to the wife's former son-in-law, a computer programmer, and determined that he had also sold copies of so-called Trojan horse software to private detectives, who used it to spy for corporate clients on competing firms.

Last week, police arrested 16 people in Israel, including senior executives of some of the country's leading high-tech companies and the private investigators they had allegedly employed. At the same time, British authorities, acting on an Israeli request, arrested the former son-in-law and his wife in London and are holding them

Michael Haephrati, 41, and his wife, Ruth Brier-Haephrati, 28, shown in an undated photo, were arrested in London. (Haaretz Daily

- Une fois installée, et contre 3000€, le concepteur fournissait à son client une adresse IP, un nom d'utilisateur et un mot de passe pour qu'il accède lui même au PC de sa victime.

Importance des chevaux de Troie

Communiqué du NISCC

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

NISCC Briefing 08/2005
Issued 16 June 2005

Une attaque d'une envergure sans précédent frappe depuis plusieurs jours les réseaux informatiques du Royaume-Uni. Selon les premières estimations faites par le Centre britannique de coordination de la sécurité de l'infrastructure nationale (NISCC), près de 300 sites clés vitaux ont été la cible d'attaques virales via l'Internet et les courriers électroniques.

Key Points

- A series of trojanised email attacks are targeting UK Government and companies.
- The attackers' aim appears to be covert gathering and transmitting of commercially or economically valuable information.
- Trojans are delivered either in email attachments or through links to a website.
- The emails employ social engineering, including use of a spoofed sender address and information relevant to the recipient's job or interests to entice them into opening the documents.
- Once installed on a user machine, trojans may be used to obtain passwords, scan networks, exfiltrate information and launch further attacks.
- Anti-virus software and firewalls do not give complete protection. Trojans can communicate with the attackers using common ports (e.g HTTP, DNS, SSL) and can be modified to avoid anti-virus detection.
- This document provides detection and protective advice. There is no complete mitigation for computers connected to the Internet.

Un autre type de keylogger

Banque Sumitomo

- En mars 2005, on découvre que les bureaux londoniens de la banque japonaise Sumitomo sont, depuis plusieurs mois la cible d'un gang de pirates.
- Dans un premier temps, on imagine qu'ils ont utilisé un keylogger logiciel comme il en existe des milliers.
- Quelques jours plus tard, on découvre que ce renifleur de clavier était une solution matérielle comme il en existe plusieurs sur le marché.

BBC NEWS

UK version | International version | About the versions | Low gr

Last Updated: Thursday, 17 March, 2005, 13:39 GMT

E-mail this to a friend | Printable version

UK police foil massive bank theft

Police in London say they have foiled one of the biggest attempted bank thefts in Britain.

Yeron Bolondi was arrested for money laundering and deception

The plan was to steal £220m ($423m) from the London offices of the Japanese bank Sumitomo Mitsui.

Computer experts are believed to have tried to transfer the money electronically after hacking into the bank's systems.

A man has been arrested by police in Israel after the plot was uncovered by the National Hi-Tech Crime Unit.

Unit members worked closely with Israeli police.

The investigation was started last October after it was discovered that computer hackers had gained access to Sumitomo Mitsui bank's computer system in London.

Un autre type de keylogger

Solutions matérielles du commerce

- Mémoire flash de 64 Ko à 2 Mo,
- Indétectable par logiciel,
- Transparent pour le système d'exploitation de la machine cible,
- Une fois l'équipement récupéré, la lecture se fait à partir d'un PC Windows 9x/Me/XP ou 2000.
- Prix rencontrés : de $20 à $200 selon la capacité,
- Possibilité d'acheter les plans et le matériel pour fabriquer soit même le dispositif.

Importance des chevaux de Troie

Conclusion

- Les attaques sont (et vont être) de plus en plus ciblées. On visera une entreprise, un groupe de dirigeants ou une seule et unique personne.
- Même si les détections génériques sont de plus en plus efficace, si un programme est créé spécifiquement pour une attaque ciblé, il risque de passer inaperçu.
- Restons vigilants face aux solutions d'espionnage de type « matériel ». A trop surveiller son environnement logiciel, nous risquons d'oublier notre environnement matériel.

L'Economie Souterraine

Importance des chevaux de Troie - Références

- Espionnage économique à grande échelle en Israël grâce à un cheval de Troie
http://cyberpolice.over-blog.com/archive-6-2005.html
- 21 people, including top executives, held in unparalleled industrial spying affair
www.haaretz.com/hasen/spages/581819.html
- UK court approves extradition of Trojan Horse couple
seclists.org/lists/isn/2005/Aug/0127.html
- Les Trojans attaquent les réseaux de Sa Majesté
http://rfi.fr/actufr/articles/066/article_36923.asp
- NISCC Briefing 08/2005 – Issued 18 June 2005
Targeted Trojan Email Attacks
http://www.niscc.gov.uk/niscc/docs/ttea.pdf
- Mission Impossible at the Sumitomo Bank
http://www.theregister.co.uk/2005/04/13/sumitomu_bank/
- Digital highwaymen
http://www.futureintelligence.co.uk/modules.php?op=modload&name=News&file=article&sid=49&mode=thread&order=0&thold=0
- KeeLogger, un keylogger pour clavier PS2
http://www.pcinpact.com/actu/news/KeeLogger_un_keylogger_pour_clavier_PS2.htm

L'Économie Souterraine

Sommaire

- La persistance des robots
- La vitalité des chevaux de Troie conventionnels (backdoors & keyloggers…)
- Le retour des rootkits

Les rootkits

Rappel

Rootkit : Programme permettant de rendre totalement furtif un autre programme en les rendant (lui et son rootkit) invisibles à un outil de sécurité tel qu'un anti-virus. Dans tous les cas, le but est d'empêcher que l'utilisateur ne perçoive des informations indiquant la présence d'activités clandestines sur son ordinateur.

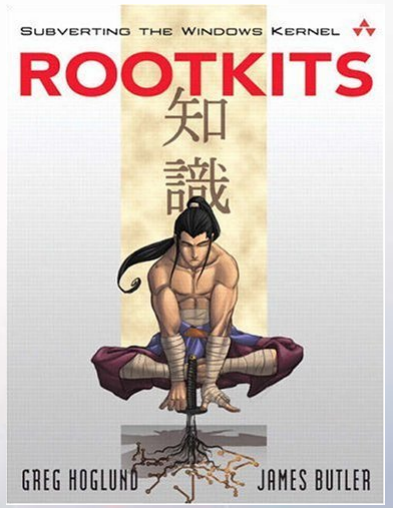
- Il rend invisible les processus, les fichiers et les connexions réseaux du pirate.
- Ils sont difficile à détecter par les anti-virus. Ils doivent être absolument détectés avant d'être installés

Le terme *rootkit* vient des mondes Unix et Linux où ces programmes modifient les *kernel syscalls* (communications entre le *kernel* (noyau système) et les applications).

Les rootkits existent depuis plusieurs années. Le projet *Chkrootkit* dédié au développement d'un outil de détection pour plateformes Linux, *BSD, Solaris et HP-UX a été démarré en 1997.

Dans le monde Windows, Gred Hoglund fait office de précurseur dans ce domaine. Il fit en 1999 la démonstration des capacités de son propre outil *NT Rootkit*. De tels programmes ont déjà été repérés en 2002 (*Slanret, IERK* et *Backdoor-ALI*).

J'ai décidé de mettre, cette année, un focus sur ce phénomène, car il prend de l'ampleur et se complexifie.



Les rootkits

Objectifs crapuleux ou commerciaux

Ils permettent une meilleure furtivité pour des programmes malicieux déjà connus (robots, renifleurs de mot de passe, portes dérobées…),

Des sociétés commerciales utilisent le concept comme outil de dissimulation et le monde « underground » en profite :

- rootkit - adware,
- Sony BMG.

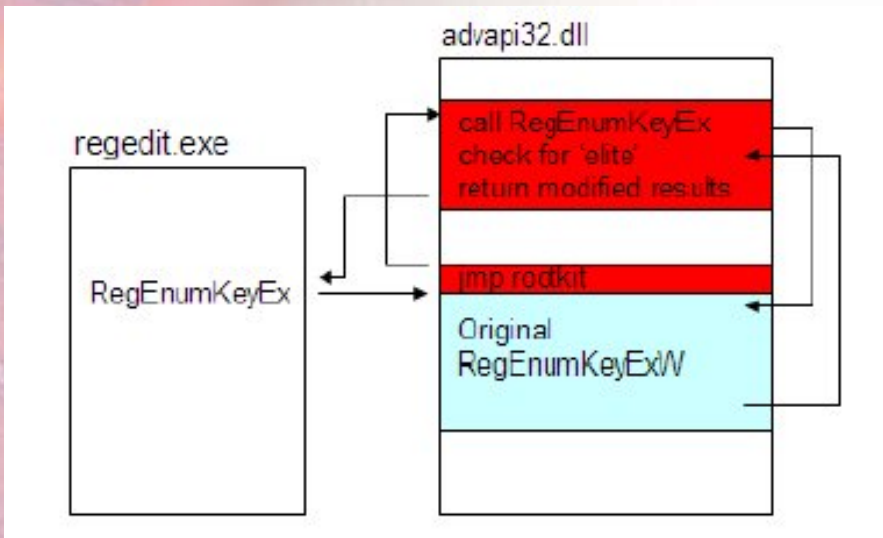
Des organisations douteuses les mettent en vente sur Internet.

Les rootkits

Un peu de technique

Usermode

- Détournement des tables d'appels à certaines fonctions standards.
- Le code qui s'exécute appelle la fonction mais modifie les données retournées.



Kernel mode

- Détournement de la table de description des services adressant certaines API système.
- L'API qui s'exécute n'est plus l'API standard, mais un pilote associé à un fichier de configuration contenant les données à cacher ou celles dont on doit interdire l'accès.

Usermode : Elitebar/SearchMiracle

Kernel mode : CommonName, ISearch

Les rootkits

Dans le TOP-10 (*)

NUMERO 1 : FURootkit

- Il se propage par le biais des botnets,
- #5 depuis janvier 2005, #3 on octobre 2005

NUMERO 2 : IsPro

- Il est inconnu du public mais pourtant bien présent,
- #7 depuis janvier 2005, #15 en octobre 2005

NUMERO 3 : Hacker Defender

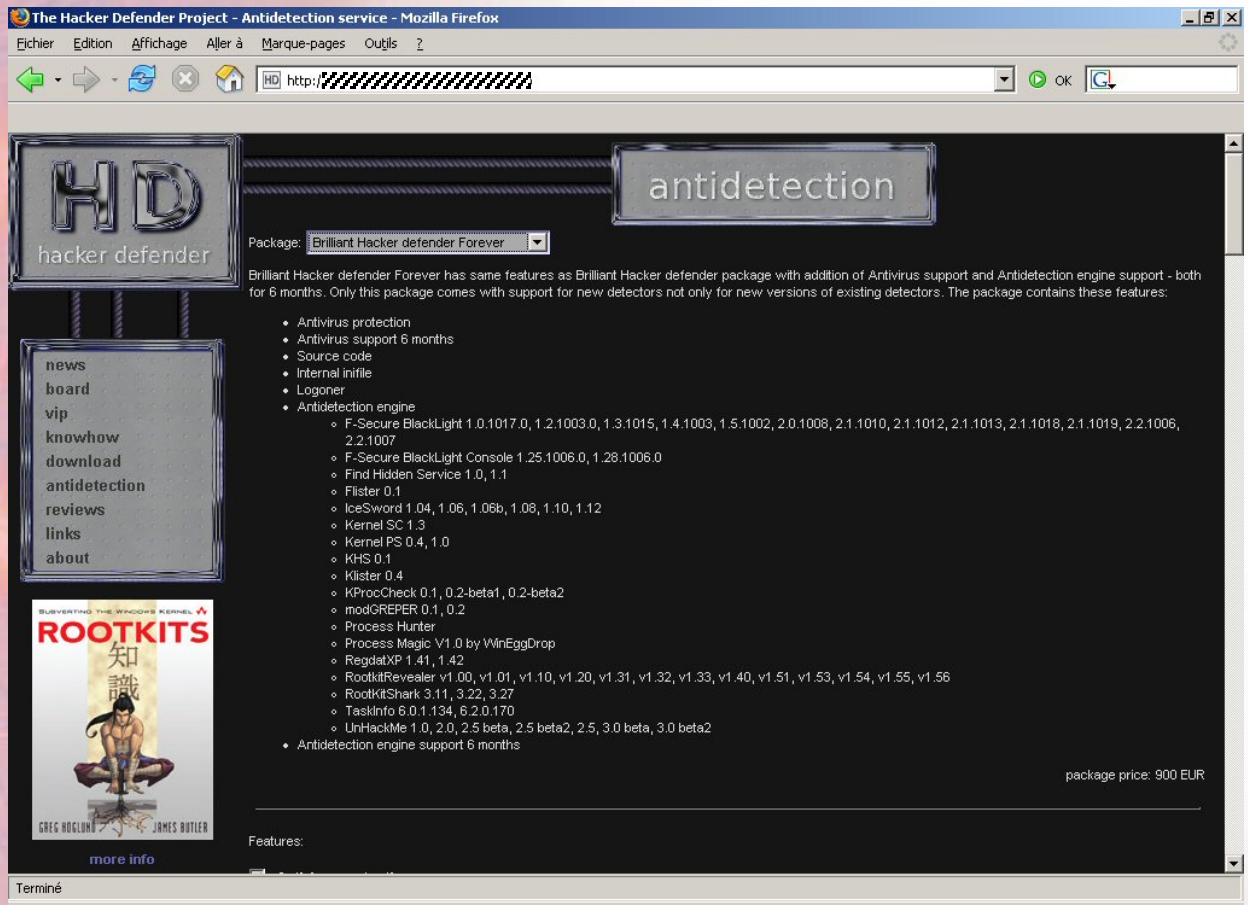
- Il est distribué sous la forme d'un « produit commercial »

NUMERO ?? : SONY BMG (DRM-rootkits - Digital Rights Management)

(*) Statistiques issues des remontées faites par MSRT (outil de suppression de logiciels malveillants Microsoft Windows pour Windows Server 2003, Windows XP ou Windows 2000)

Les rootkits

Exemple : vente en ligne « hacker defender »



- Antivirus protection
- Antivirus support 6 months
- Source code
- Internal inifile
- Logoner
- Antidetection engine
- Antidetection engine 6 months

Package price : 900€

Les rootkits

Exemple : vente en ligne « hacker defender »

On en parle déjà en 2002,
(http://www.vulnerabilite.com/actu/20020308151752rootkit_windows.html)

Le site propose aujourd'hui des versions payantes (entre 600 et 900 €uros) avec contrat de mise à jour assurant à l'acheteur une indétectabilité par les logiciels de sécurité (licence sur 1, 2 ou 6 mois),

Si W32/HackDef est présent sur une machine, il masque en général d'autres logiciels potentiellement indésirables présents sur l'ordinateur (adwares/spywares).

Pour afficher le nom du logiciel masqué par W32/HackDef, on cherchera dans le répertoire hôte du rootkit un fichier de configuration avec l'extension de .ini. En éditant ce fichier, on déterminera le logiciel que Win32/HackDef masque sur l'ordinateur.

Les rootkits

Exemple : SONY BMG - DRM

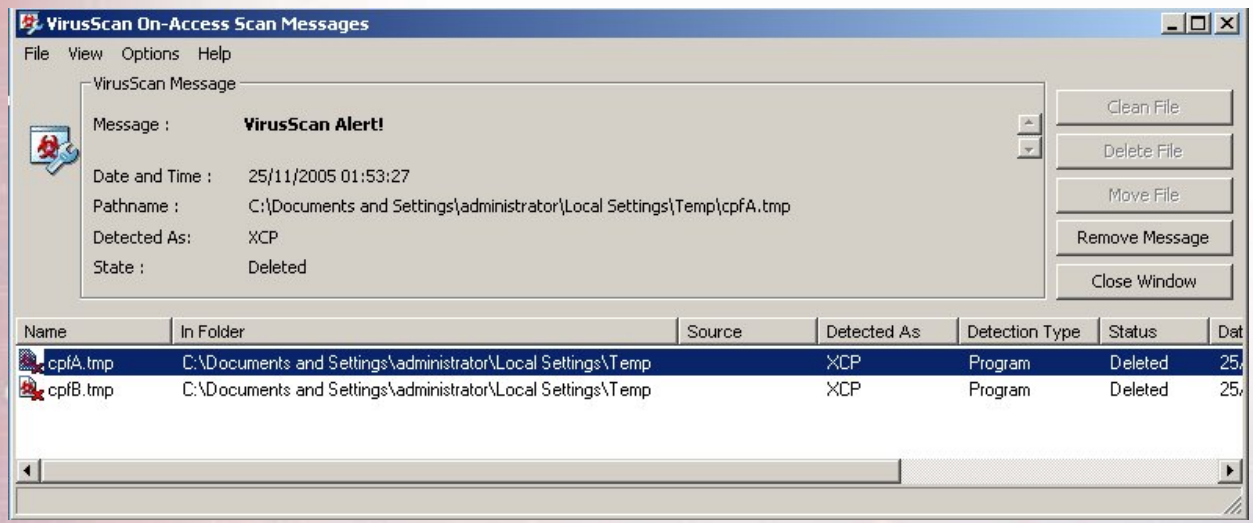
Digital Rights Management (DRM)

- eXtended Copy Protection (XCP)
- Annonce publique de la découverte : le 31 octobre 2005

Les rootkits

Exemple : SONY BMG - DRM

- 3 novembre 2005, Sony indique que le système existe depuis environ 8 mois. Il propose des outils de détection et de désinstallation.
- Diverses vulnérabilités sont mises à jour.
- Le rootkit est réutilisé par le monde underground (contournement du système anti triche du jeu de rôle en ligne World of Warcraft)
- Le rootkit est maintenant détecté par les anti-virus



Les rootkits

Détection

SysInternals propose le freeware RootkitRevealer :

- Il effectue une première passe qui consiste à obtenir la liste de tous les fichiers du système en utilisant l'API normale de Windows
- Puis une seconde passe est menée, ou il construit une nouvelle liste de fichiers en lisant directement le contenu du disque, sans passer par les API Windows.
- La comparaison des deux états permet de mettre en évidence les fichiers cachés (fichiers légitimes ou non).

Autres outils ou utilitaires :

- BlackLight, UnHackMe, Attack Tool Kit (ATK – Open-Source – GPL), RKDetector, Process Guard, Anti Hook,
- HijackThis, Ekinx, CodeStuff Starter

Les rootkits

Détection

Les anti-virus seront (sont) aussi la bonne solution :

- Les recherches actuelles montrent qu'il est possible de mettre en œuvre des détections génériques (détection « new rootkit » avec VirusScan depuis juillet 2005).
- Pour l'instant, la meilleure technique de détection passe par la recherche de processus cachés en mémoire.
- Il sera sans doute toujours nécessaire pour le rootkit de se lancer au reboot de la machine. C'est au moment de ce chargement qu'il faut le repérer.

Les rootkits

Conclusion

- On reparlera des rootkits en 2006 !
- Il est à craindre que certains rootkits – ceux là malveillants – restent un temps indétectés.
- Indétectés, non pas à cause d'une impossibilité technique, mais simplement du fait qu'il n'auront pas été jusqu'alors repérés.

L'Economie Souterraine

Les rootkits - Références

- Techniques of adwares and spyware

Eric Chien - Conférence Virus Bulletin de 2005

- Les fonctionnalités des rootkits et comment les contrer (Alexey Monastyrsky, Konstantin Sapronov, Yury Mashevsky - Analyste Virus, Kaspersky Lab).

http://www.viruslist.com/fr/analysis?pubid=167948065

- Sony, Rootkits and Digital Rights Management Gone Too Far (Mark's Sysinternals Blog)

http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

- More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home (Mark's Sysinternals Blog)

http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html

- The Hacker Defender Project (Holy Father)

http://hxdef.czweb.org/

- Les Rootkits Windows de plus en plus sophistiqués (2002)

http://www.vulnerabilite.com/actu/20020308151752rootkit_windows.html

- Le contrôle d'intégrité et ses limites (actes du symposium SSTIC05, Cyril Leclerc, ARSeO)

http://actes.sstic.org/SSTIC05/Limites_du_controle_d_integrite_classique/SSTIC05-article-Leclerc-Limites_du_controle_d_integrite_classique.pdf

- RootkitReleaver (SysInternals Freeware)

http://www.sysinternals.com/Utilities/RootkitRevealer.html

- "RootkitRevealer" : la riposte aux "rootkits" Windows (CERT-IST)

http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/Environnement_Microsoft/RootkitRevealerlariposteauxrootkitsWindows/

- Le rootkit de Sony permet aussi de tricher sous WoW !

http://fr.news.yahoo.com/04112005/308/le-rootkit-de-sony-permet-aussi-de-tricher-sous-wow.html

Panorama 2005

- Economie souterraine: robots, keyloggers, rootkits
- Espionnage économique: la convoitise
- Vol et pertes de données : les risques d'usurpation d'état civil
- Du harcèlement jusqu'aux violences physiques

Espionnage économique : la convoitise

- Plusieurs cas d'espionnage économique présumés ou avérés ont marqué l'actualité en 2005.

- Les faits :
  - Piratage d'Ericsson en Suède (jugé)
  - Transmission de secrets de fabrication à des concurrents aux Etats-Unis (inculpations)
  - Affaire Valéo en France : (instruction non terminée au moment de l'édition du présent document)
  - Affaire d'espionnage avec cheval de Troie en Grande Bretagne et Israël : concerne plusieurs pays, affaire en cours.

Espionnage économique : la convoitise

- Les faits (suite) :
  - Suède : en avril 2005, un consultant informatique hongrois est condamné à 3 ans de prison pour espionnage industriel. Il fait appel de sa condamnation.

    De mars 2002 à juin 2004, il s'était introduit dans les systèmes informatiques de la société de téléphonie Ericsson et y avait accédé frauduleusement à des informations. L'un des chefs d'inculpation visait la détention non autorisée d'informations secrètes.

Espionnage économique : la convoitise

- Les faits (suite) :
  - selon les informations rapportées par des médias suédois, il avait accédé aux noms d'utilisateurs et leurs mots de passe, et s'était également emparé d'informations cryptées, de codes sources utilisés dans les téléphones mobiles de Ericsson, et des données militaires secrètes. L'un des clients de Ericsson étant le Ministère suédois de la Défense.

Espionnage économique : la convoitise

- Les faits (suite) :
  - Toujours selon les informations rapportées par des médias suédois, le pirate a expliqué qu'en réalité, il voulait montrer les failles de sécurité du système de Ericsson et obtenir un emploi dans cette entreprise. Mais le juge ne l'a pas entendu de cette oreille, lui opposant qu'il avait un autre plan : vendre au plus offrant sur Internet les données auxquelles il avait accédé, et que s'il souhaitait un emploi, il aurait dû contacter l'entreprise pour proposer sa candidature.

Espionnage économique : la convoitise

- Les faits (suite) :
  - Etats-Unis : en 2005, l'ancien directeur IT de Lightwave Microsystems plaide coupable d'avoir proposé à un concurrent des données contenant des secrets de fabrication de cet employeur.

    Il a reconnu avoir volé les sauvegardes informatiques où se trouvaient les informations qu'il comptait revendre au concurrent. Fait inhabituel, le concurrent contacté, JDS-Uniphase, avait prévenu le FBI.

Espionnage économique : la convoitise

- Les faits (suite) :
  - Etats-Unis : en 2005, une 3ème cadre de l'entreprise BES (Business Engine Software Corporation), ici l'ancien PDG, reconnaît avoir planifié l'intrusion du système informatique d'un concurrent, NiKU.

    Pendant 10 mois, des données de NIKU auraient ainsi été copiées et ventilées chez BES, pour en tirer profit commercial.

Espionnage économique : la convoitise

- Les faits (suite) :
  - C'est au cours d'une session de formation en-ligne organisée par NIKU par l'intermédiaire d'un site web spécialisé que l'intrusion aurait été commise.

Espionnage économique: la convoitise

- Les faits (suite) :
  - France (avril 2005) : affaire en cours, la personne mise en examen est présumée innocente au moment où ce document est édité.
  - L'équipementier automobile Valéo porte plainte.
  - Une étudiante chinoise stagiaire dans l'entreprise est soupçonnée d'avoir copié des données sur un disque dur personnel.
  - Elle est mise en examen fin avril 2005 et placée en détention provisoire pendant 53 jours.
  - L'AFP révèle cette affaire dans une dépêche qui signale l'incarcération de la jeune fille « soupçonnée d'espionnage industriel ».

Espionnage économique: la convoitise

- Les faits (suite) :
  - La justice a été saisie pour accès frauduleux dans un système automatisé de données, et abus de confiance.
  - Selon des informations publiées par divers médias, la jeune stagiaire aurait sorti des données de l'entreprise et les aurait emportées chez elle.
  - La jeune femme explique à la presse qu'elle a copié les données pour son rapport de stage.

Espionnage économique: la convoitise

- Les faits (suite) :
  - Dans un entretien publié le 21 juin 2005 par le quotidien Libération, la jeune femme explique au journaliste qui lui demande : Pourquoi avez-vous copié des fichiers de Valeo sur votre disque dur portable ?

    « Pour préparer mon rapport de stage. A l'école, les étudiants ont tellement l'habitude d'apporter leur disque dur que j'ai fait la même chose en entreprise. Pour nous, c'est vraiment naturel. »

Espionnage économique: la convoitise

- Faits (suite):
  - Dans le même entretien pour le quotidien Libération, elle explique qu'elle a chargé des fichiers pour en faire ensuite le tri chez elle.
  - Parle de 30 ou 40 fichiers
  - Indique qu'elle avait accès à tous les fichiers sur l'intranet et qu'elle ne pensait pas que c'était confidentiel.
  - Explique avoir effacé des données d'un PC de Valéo par manque d'espace pour travailler.
  - Quelle que soit l'issue de cette affaire, elle pose la question de la sécurité du patrimoine informationnel dans les entreprises.

Espionnage économique : la convoitise

- Les faits (suite) :

Grande-Bretagne/ Israël :

- Il s'agit là aussi d'une affaire en cours dans laquelle les suspects restent présumés innocents.
- Un écrivain israëlien découvre sur Internet des chapitres d'un livre « L for Lies » ou en français
- « M comme mensonges » écrit avec son épouse Varda, alors que le livre n'est pas encore publié.
- Il porte plainte à la police, qui examine l'ordinateur de l'écrivain.

Espionnage économique : la convoitise

- Les faits (suite) :

Grande-Bretagne/ Israël :

  - L'ordinateur aurait été compromis par un email envoyé par l'ex-mari de la fille de Varda, email contenant un cheval de Troie, présenté comme un formulaire d'inscription scolaire pour leur petite-fille.

Espionnage économique : la convoitise

- Les faits (suite) :
  - Peu de temps après la découverte de leur livre sur Internet, le couple aurait reçu de leur ex-gendre un CD Rom prétendument envoyé par un étudiant de l'écrivain. L'écrivain précise qu'il n'a pas installé ce CDRom sur son ordinateur.
  - Sur le serveur où était copié le livre subtilisé, les policiers font d'autres découvertes : des données prises dans de nombreux autres ordinateurs.
  - C'est ainsi qu'est révélée en 2005 une affaire d'espionnage économique de grande ampleur.

Du harcèlement jusqu'aux violences physiques

- les Faits (suite) :
  - L'ancien gendre du couple d'écrivains est arrêté à Londres, en Angleterre, par Scotland Yard, en mai 2005, sur mandat israélien d'extradition. Son épouse également.
  - Il leur est reproché la modification non autorisée du contenu d'ordinateurs.
  - L'ex-gendre de l'écrivain est soupçonné d'avoir vendu des exemplaires sur mesure du cheval de Troie à des sociétés de détectives privés, pour le compte de clients voulant espionner leurs concurrents.

Du harcèlement jusqu'aux violences physiques

- Les faits (suite) :
  - Les victimes présumées, citées par les medias, comptent des entreprises de plusieurs secteurs d'activité : téléphonie, automobile, télévision par câble, mode, eaux minérales, alimentation, finance, haute technologie, presse, édition, etc.
  - Les chevaux de Troie sur mesure auraient été envoyés à leurs cibles soit au moyens d'emails, soit au moyen de CD présentés comme des CD d'offres promotionnelles envoyés par des partenaires commerciaux. Il ne s'agirait pas d'une diffusion massive mais de diffusion ciblée.
  - Emails et CDRom procurent l'effet de provenir de connaissances ou partenaires: personnalisation.

Espionnage économique : la convoitise

- Les faits (suite) :
  - Les dirigeants de plusieurs sociétés de renseignement privé sont entendus par les policiers en Israël, et quelques inculpations s'ensuivent en Juillet 2005.
  - Justice : l'affaire intéresse la Justice en Israël et Grande-Bretagne, pour l'instant. La police n'excluant pas que des entreprises américaines, européennes ou autres aient été touchées, il pourrait y avoir d'autres pays concernés par cette affaire.
  - A suivre…

Espionnage économique : la convoitise

- Conséquences et enjeux :
  - Chaque année apporte son lot d'affaires d'espionnage économique, une activité qui apparaît ne pas faire relâche.
  - Diversité des moyens employés :
  - De l'intrusion, au vol, en passant par le recours à des programmes malveillants conçus sur mesure.
  - Les affaires d'espionnage sont parfois difficiles à détecter, et peuvent être difficiles à traiter sur le plan judiciaire, en fonction de l'existence ou non de textes de lois adaptés.

Espionnage économique : la convoitise

Quelques sources :

Agence France Presse

http://www.thelocal.se/article.php?ID=1076&date=20050309

http://news.zdnet.co.uk/internet/security/0,39020375,39193998,00.htm

http://www.infoworld.com/article/05/04/26/HNsonyhacker_1.html?APPLICATION%20SECURITY

http://www.usdoj.gov/usao/can/press/html/2005_12_08_oneilguiltyplea.htm

http://www.baselinemag.com/article2/0,1397,1741503,00.asp

http://www.liberation.fr/page.php?Article=305532

http://www.guardian.co.uk/international/story/0,,1495669,00.html

http://www.haaretz.com/hasen/spages/581819.html

http://www.globes.co.il/serveen/globes/docview.asp?did=931923&fid=942

http://www.ynetnews.com/articles/0,7340,L-3133649,00.html

http://web.israelinsider.com/Articles/Briefs/5702.htm

http://www.spectrum.ieee.org/print/2145

http://www.washingtonpost.com/wp-dyn/content/article/2005/05/30/AR2005053000486.html

Panorama 2005

- Economie souterraine: robots, keyloggers, rootkits
- Espionnage économique: la convoitise
- Vol et pertes de données : les risques d'usurpation d'état civil
- Du harcèlement jusqu'aux violences physiques

Vols et pertes de données

- Les faits : de nombreuses affaires de divulgation en masse de données personnelles (y compris bancaires) ont été mises en lumière en 2005 :
  - Vols d'ordinateurs
  - Pertes de supports de sauvegarde
  - Compromissions de systèmes

Vols et pertes de données

- Les faits (suite)
  - Ces affaires, du fait du volume et du type de données divulguées, mettent en avant non seulement les risques de fraudes financières mais aussi d'usurpation d'état civil.
  - Les exemples cités proviennent essentiellement des Etats-Unis, du fait de lois imposant aux entreprises victimes de divulgations de données personnelles d'alerter les personnes concernées.

Vols et pertes de données

- Chronologie et détails : les vols d'ordinateurs
  - Groupe médical San Jose (mars 2005): perte de données personnelles de 185 000 patients.
    - Données de facturation transférées depuis les serveurs du réseau de l'hôpital vers deux postes de travail pour les besoins de l'audit annuel de la structure.
    - Vol des deux ordinateurs.
    - Alerte des patients par l'hôpital (en application de la loi américaine).
    - Une partie seulement des données chiffrées sur les disques durs.

Vols et pertes de données

- Chronologie et détails : les vols d'ordinateurs (suite)
  - Université de Berkeley (avril 2005)
    - Vol d'un ordinateur portable contenant des données personnelles (dont numéros de sécurité social) de 98 000 personnes.
    - Le portable aurait été vendu sur un site d'enchères en ligne et retrouvé par la police, disque dur reformaté.
    - A priori, pas de preuve d'exploitation malveillante de ces données.

Vols et pertes de données

- Chronologie et détails : pertes de supports de sauvegarde
  - Ameritrade Holding (avril 2005) :
    - Perte d'une bande lors d'une transfert sur site distant par une société spécialisée.
    - Dossiers de 200 000 clients divulgués.
  - Bank of America (février 2005) :
    - Perte de bandes (vol de bagagistes ?) contenant des informations bancaires relatives à 1,2 million d'employés du gouvernement
    - Les données contenaient des informations sur les détenteurs de comptes (numéros de comptes et adresses par exemple)

Vols et pertes de données

- Chronologie et détails : pertes de supports de sauvegarde (suite)
  - Citigroup (avril 2005) :
    - Perte par UPS de bandes contenant les données (relevés de transaction et n° de sécurité sociale) de 3,9 millions de clients.
    - Perte occasionnée lors du transfert vers une institution de vérification de l'historique.

Vols et pertes de données

- Chronologie et détails : compromissions
  - Cardsystems (avril 2005) :
    - Prestataire technique de Visa et Mastercard assurant le traitement des transactions
    - Découverte de la compromission du réseau de Cardsystems, avec potentiellement accès à 40 millions de numéros de cartes de crédits (qui n'auraient pas du être conservés !)
    - Récupération de 68000 numéros; des établissements bancaires internationaux indiquent que cette divulgation aurait entraîné des transactions frauduleuses

Vols et pertes de données

- Chronologie et détails : compromissions (suite)
  - ChoicePoint (origine de l'affaire en octobre 2004)
    - Société spécialisée dans la fourniture de données financières aux organismes de crédit.
    - Vol d'informations (150.000 personnes) : numéros de sécurité sociale, de téléphone, adresses e-mail, situation d'endettement, etc. via l'usurpation de de sociétés de crédit.
    - Détournement de correspondances adressées aux clients
    - 750 plaintes déposées pour usurpation d'identité, enquête en cours

Vols et pertes de données

- Chronologie et détails : compromissions (suite)
  - LexisNexis (avril 2005)
    - édition et informations professionnelles (juridiques, financières et économiques).
    - Plusieurs dizaines d'incidents de sécurité découverts au sein d'une base de données au sein du système d'information d'une filiale (Seisint) du groupe.
    - informations concernant 32.000 personnes : noms, adresses, numéros de sécurité sociale, permis de conduire ...

Vols et pertes de données

- Chronologie et détails : compromissions (suite)
  - Jackson Community College (mai 2005)
    - Intrusion dans le réseau et accès potentiel à 8000 numéros de sécurité social
    - Accès aux mots de passe des étudiants et des professeurs, qui sont aussi les mots de passe à l'ouverture des nouveaux comptes utilisateurs, sans que ces mots de passe soient systématiquement modifiés.

Vols et pertes de données

- Enjeux et conséquences : l'usurpation d'état civil
  - Les données personnelles deviennent un bien recherché et monnayable :
    - Soit directement, l'attaque est dirigée sur les données.
    - Soit indirectement, suite à des vols d'ordinateurs ou des pertes de support, les données peuvent se retrouver disponibles à des objectifs de vols d'identité.
    - Exemple : arrestation de 17 personnes en Arizona, la police retrouve un ordinateur portable contenant un volume important de données personnelles et bancaires.

Vols et pertes de données

- Enjeux et conséquences : l'usurpation d'état civil (suite)
  - Les risques de divulgation de données personnelles sont aggravés par la faible sensibilisation du public envers ces questions :
    - Les données personnelles peuvent être livrées assez facilement par leur propriétaire.
    - Exemple : enquête du Londoners (mars 2005) qui montre que 92% d'un échantillon de 200 personnes donnent des informations personnelles (adresse, nom des parents, des enfants) à un enquêteur qui offre des places de théâtre gratuites en échange de réponses à un sondage

Vols et pertes de données

- Enjeux et conséquences : l'usurpation d'identité (suite)
  - Deux types de protections contre l'usurpation d'identité :
    - Des mesures **techniques** : sécurité des systèmes et des réseaux, chiffrement des données sensibles sur les support de sauvegardes et les portables.
    - Des mesures **organisationnelles** : sensibilisation des collaborateurs sur les mesures de sécurité, procédures de contrôle et d'évaluation de la sécurité.

Vols et pertes de données

- Enjeux et conséquences : l'usurpation d'identité (suite)
  - Protéger les données n'est pas suffisant car on s'aperçoit que certains éléments :
    - se retrouvent conservés sur de nombreux systèmes, dont les niveaux de protection peuvent parfois être très faibles,
    - peuvent être donnés assez facilement directement par leur propriétaire.
  - Il faut donc également renforcer les procédures d'authentification utilisant les données personnelles pour rendre plus difficiles les actes de malveillance une fois les données compromises.

Vols et pertes de données

- Enjeux et conséquences : l'usurpation d'identité (suite)
  - Illustration du besoin de renforcer les procédures d'authentification : exemple d'un couple propriétaire d'une villa au Texas, qui retrouve un inconnu installé à leur domicile à leur retour de voyage. Cette personne présente en toute bonne foi un acte prouvant qu'il a versé de l'argent pour acquérir ce bien. L'escroquerie est basée au départ sur le vol de données personnelles de madame. Les numéro de sécurité social, numéro de permis de conduire et copie de la signature ont suffit à établir ce faux document de vente.

Vols et pertes de données

Les liens pour en savoir plus :

- http://www.californiahealthline.org/index.cfm?Action=dspItem&itemID=110469
- http://www.pcinpact.com/actu/news/LUniversite_de_Berkeley_retrouve_ses_donnees_perdu.htm
- http://www.theregister.co.uk/2005/04/29/backup_tapes_are_backdoor_for_id_thieves/
- http://www.pcinpact.com/actu/news/Bank_of_America_a_un_petit_probleme_de_perte_de_me.htm
- http://news.zdnet.com/2100-1009_22-5733971.html
- http://www.msnbc.msn.com/id/8260050/
- http://www.msnbc.msn.com/id/6969799/
- http://www.silicon.fr/getarticle.asp?ID=8633
- http://www.vnunet.fr/actualite/securite/piratage/20050412015
- http://www.crime-research.org/news/29.05.2005/1264/
- http://www.reseaux-telecoms.net/actualites/lire-vol-d-identites-arrestations-en-serie-11213.html
- http://www.vnunet.com/vnunet/news/2127049/uk-wide-open-identity-theft
- http://www.plastic.com/article.html;sid=05/08/23/19205287;cmt=60

Panorama 2005

- Economie souterraine: robots, keyloggers, rootkits
- Espionnage économique: la convoitise
- Vol et pertes de données : les risques d'usurpation d'état civil
- Du harcèlement jusqu'aux violences physiques

Du harcèlement jusqu'aux violences physiques

Des agressions et des violences qui ne sont pas « virtuelles »

Du harcèlement jusqu'aux violences physiques

- Les faits :

Une multitude de cas révélés ou résolus en 2005 nous rappellent que la criminalité informatique est le fait d'êtres humains, qu'elle touche des êtres humains et pas seulement des machines.

La souffrance engendrée peut être intense, violente, et va parfois jusqu'à la mort.

L'outil informatique sert ici aux agresseurs à défouler leur rage, porter atteinte à l'intimité, offenser autrui, inciter à la haine, se vanter de leurs méfaits, appâter leurs victimes, et dans quelques cas, débouche sur des meurtres bien réels.

Du harcèlement jusqu'aux violences physiques

- Les faits (suite):
  - Grande-Bretagne : Une femme harcèle pendant 3 ans son ex-amant d'une nuit : piratage de sa messagerie, diffusion de faux emails, création d'un site web proclamant qu'il est homosexuel, inscription à son insu sur des sites, dont une liste de discussion de prisonniers homosexuels, diffusion de rumeurs affirmant qu'il est atteint de MST, etc. Condamnation de la jeune femme en janvier 2005.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :
  - Singapour : un homme est condamné en octobre 2005 à un mois de prison pour avoir menacé par SMS son ex-petite amie de diffuser sur Internet des photos d'elle nue.
  - France : l'ex-femme d'un magistrat et son fils condamnés en avril 2005 pour avoir diffusé sur Internet des photos de sa nouvelle épouse nue, et contacté plusieurs journaux les invitant à se connecter au site web où elles étaient exposées.

Du harcèlement jusqu'aux violences physiques

- faits (suite) :
  - France: une jeune fille mineure est alertée qu'une séquence vidéo d'elle prise à son insu dans l'intimité du vestiaire d'une piscine se trouve sur un site web pornographique aux Etats-Unis.
  - France :dérapages dans l'expression sur des blogs. Plusieurs lycéens sont expulsés de leur établissement scolaire en 2005 pour avoir insulté ou calomnié des camarades de classe ou des enseignants.

Du harcèlement jusqu'aux violences physiques

- Faits (suite):
  - France (novembre 2005) :

    L'auteur du site web « S.O.S France » est condamné pour injures aux personnes à raison de leur appartenance à une religion. Des écrits diffusés sur ce site web qualifiaient les musulmans de « racaille ».

Du harcèlement jusqu'aux violences physiques

- Faits (suite):
  - France (novembre 2005) : publication de messages francophobes sur Internet, et de messages appelant à attaquer des commissariats de police.
  - France (novembre 2005) : interpellation de bloggeurs dans les Bouches du Rhône et en Seine Saint-Denis au moment des émeutes urbaines. En cause : la provocation à une dégradation volontaire, dangereuse pour les personnes, par le biais d'Internet.

Du harcèlement jusqu'aux violences physiques

- Faits (suite):
  - 2 actions pédagogiques intéressantes à souligner :
  - Pour aider les internautes et éditeurs de contenus à éviter les dérapages qui excèdent la liberté d'expression, le Forum des Droits sur Internet publie un document : « Je blogue tranquille » et l'association « Ni putes ni soumises » un « guide du respect » destiné à apprendre à se respecter l'un l'autre.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :

Japon : blog, journal d'un meurtre ? (novembre 2005)

Une jeune fille mineure arrêtée, elle raconte sur son blog la dégradation progressive de l'état de santé de sa mère, qu'elle est soupçonnée d'avoir empoisonnée.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :

  Le fait d'agresser une personne pour filmer la scène sur son téléphone portable pour la rediffuser à des connaissances par téléphone ou sur Internet est appelé « Happy slapping ».

  Pour l'instant, seuls quelques cas sont signalés en 2005.

  La technologie (téléphone portable) n'est pas en cause, mais l'usage qui en est fait.

  Le fait d'amplifier l'agression par sa captation filmée peut être considéré comme aggravant.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :

Suisse : juin 2005 : deux écoliers de 13 ans frappent un enfant et filment la séquence sur leur téléphone portable.

France : en novembre 2005, dans la Vienne, trois jeunes hommes sont mis en examen pour viol en réunion, captation et diffusion d'images pornographiques de mineurs.

Ils auraient filmé la scène avec un téléphone portable.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :

- Grande-Bretagne (mai 2005): une jeune fille est agressée et blessée pour une séquence filmée par téléphone portable.
- Grande-Bretagne (avril 2005) : un adolescent de 14 ans se pend après avoir subi une agression filmée par ses camarades de classe.

- Grande-Bretagne (septembre 2005): condamnation d'un homme à 14 ans de prison pour avoir agressé et violé une jeune fille : il avait filmé la scène sur son téléphone pour l'envoyer à des amis.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :
  - Autre phénomène : le cyberbullying. Pour mieux connaître le phénomène du harcèlement-brimades par moyens informatiques interposés, deux chercheurs américains ont réalisé une étude en 2005, portant sur près de 1500 adolescents :
  - 16,7 % des adolescents rapportent l'avoir fait online.
  - 50% disent qu'ils l'ont fait pour s'amuser.
  - Environ 35% considèrent que cela apporte quelque chose aux victimes ou les rend plus fortes.
  - Voir les détails des résultats préliminaires de l'étude de Sameer Hinduja et Justin W.Patchin sur le site cyberbullying.us

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :
  - Australie : fermeture en juin 2005 d'un site de discussions pour violeurs. Sur le site,« The Rape Club », description de faits d'armes de violeurs et et propositions de photos de viol dits « authentiques ».
  - France : en octobre 2005, à Besançon, un homme déjà sanctionné pour attouchements sur mineurs est condamné à 7 ans de prison ferme pour agressions commises sur mineurs. Il se servait d'Internet pour recruter des « baby sitters ».

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :
  - France : mise en examen d'un homme en octobre 2005 dans le Nord de la France pour provocation à la commission d'un crime par voie de presse. L'homme se serait fait passer sur des forums pour une femme dont le fantasme serait de se faire violer, pour recruter des personnes allant violer l'une de ses voisines. Affaire en cours.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :
- France : recrutement de tueur à gage sur Internet. En avril2005, un homme est mis en examen à Nancy pour offre de commettre un assassinat. Il aurait cherché à faire éliminer le concubin de sa maîtresse par un tueur à gages en faisant maquiller l'élimination du rival en accident.
- Japon : une femme porte plainte contre un homme qu'elle avait engagé sur Internet comme tueur à gages pour éliminer la femme de son amant et qui n'avait pas « exécuté »son contrat. Il est condamné pour escroquerie volontaire en décembre 2005.

Du harcèlement jusqu'aux violences physiques

- Faits (suite) :
  - Chine : un homme de 41 ans a poignardé un de ses compagnons de jeu. Il n'a pas supporté que celui-ci revende le sabre virtuel gagné dans un jeu multi-joueurs en ligne, sabre qu'il lui avait prêté. Selon les médias qui rapportent cette affaire, l'homme était d'abord allé se plaindre auprès de la police du vol de son arme virtuelle. La loi étant muette sur le cas de la propriété d'objets virtuels, sa plainte n'aurait pas abouti et furieux, l'homme en serait venu à tuer son compagnon de jeu.
  - Il a été condamné à mort avec sursis à exécution, peine qui peut être commuée en peine de prison à vie.

Du harcèlement jusqu'aux violences physiques

- Enjeux et conséquences :

Internet est un fabuleux outil de communication et de connaissances.

Dans certains cas, il est devenu aussi un nouveau théâtre et nouveau vecteur de violences.

L'aspect humain des souffrances engendrées chez les victimes à cause de ces offenses ou violences doit être considéré.

Les atteintes, offenses, violences psychologiques sont longues à guérir.

Les violences physiques sont parfois irréparables.

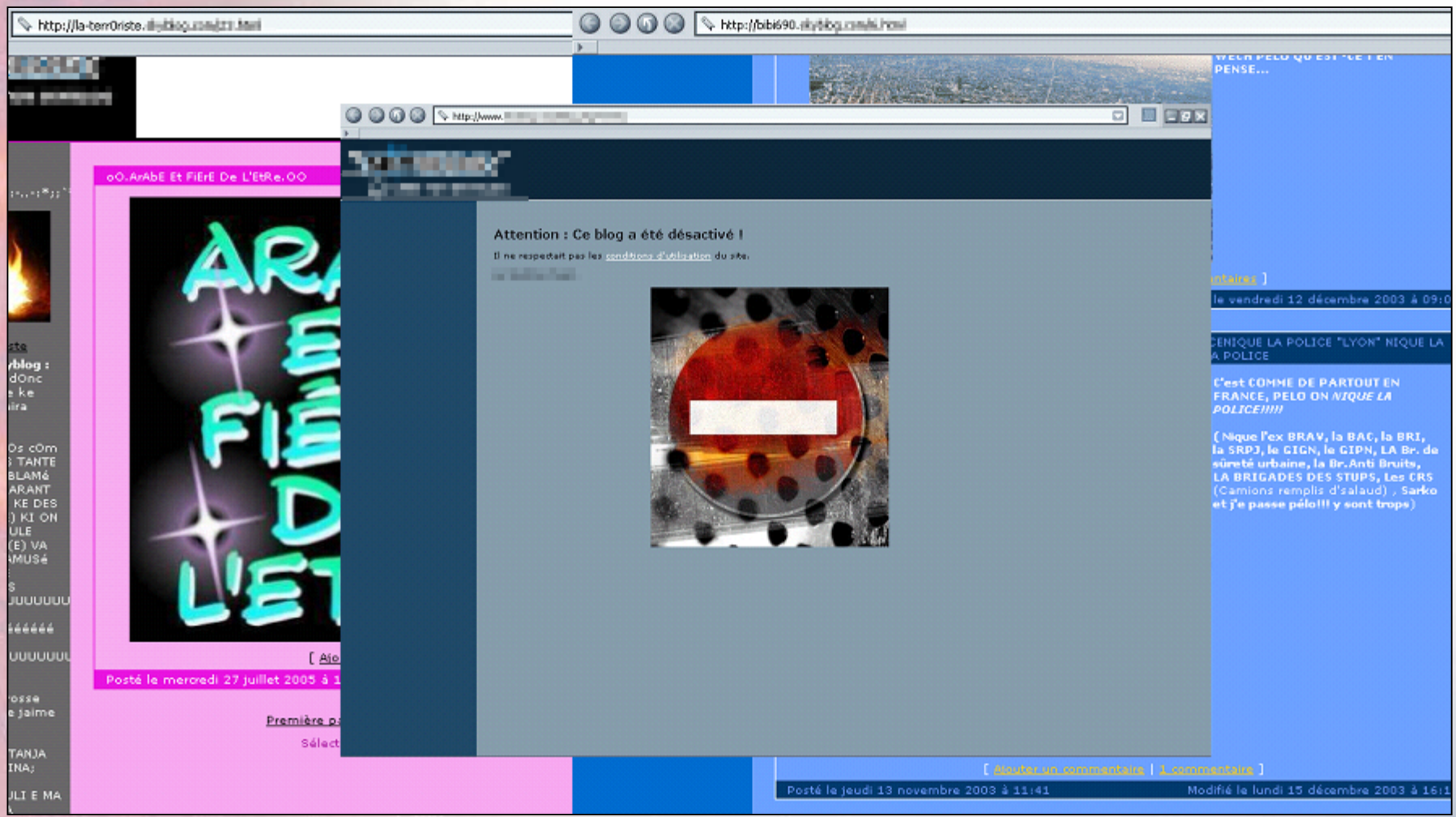
Du harcèlement jusqu'aux violences physiques

- Enjeux et conséquences :

Besoin d'information et de prévention contre certaines de ces atteintes

Impossibilité de prévenir certaines formes de ces violences

Du harcèlement jusqu'aux violences physiques



Du harcèlement jusqu'aux violences physiques

Quelques sources:

Agence France Presse

http://foruminternet.org

http://www.niputesnisoumises.com

http://www.theregister.co.uk/2005/01/28/cyberstalker_sentence/

http://news.bbc.co.uk/1/hi/england/leicestershire/4217191.stm

http://www.manchesteronline.co.uk/men/news/s/159/159553_girl_16_held_over_happy_slap_attack.html

http://www.manchesteronline.co.uk/men/news/s/163/163172_happy_slap_mums_fury.html

http://www.cyberbullying.us

http://www.marianne-en-ligne.fr/archives/e-docs/00/00/41/82/document_article_marianne.phtml

http://news.bbc.co.uk/1/hi/technology/4072704.stm