Les Virus Informatiques

Historique - Techniques - Luttes

Plan

- Présentation Historique
- Infections Informatiques
 - Aspects Généraux
 - Les types d'infections
- Les modes d'action des virus
- Classification
 - des virus
 - des vers
- La lutte antivirale
- Quelques cas pratiques

Introduction

- Les virus : un « vieux » problème...
- Des études mathématiques ont été réalisées sur le virus (formalisation et détection)
- ◆ La lutte est bien plus efficace quand on connaît l'adversaire
- C'est également une lutte commerciale
- Problèmes très importants depuis l'arrivée des réseaux et encore plus avec les connexions permanentes actuelles (même au niveau « familial » avec l'ADSL).

Virus – définitions

- Virus (Fred Cohen, 1986):
 - « Un virus est une séquence de symboles qui, interprétée dans un environnement donné (adéquat), modifie d'autres séquences de symboles dans cet environnement, de manières à y inclure une copie de lui-même, cette copie ayant éventuellement évolué. »
 - « Un programme capable d'infecter d'autres programmes en les modifiant de manière qu'ils contiennent une copie de luimême, parfois évoluée. »

Historique

La préhistoire Les expériences de Fred Cohen Les vrais virus

Historique – Core Wars

- Simulation d'un environnement
- Plusieurs programmes viraux s'y affrontent :
 - Objectif : survie et non sa reproduction
- Plusieurs conclusions :
 - Les petits programmes peuvent être dissimulés plus facilement
 - Les gros programmes permettent de détecter plus facilement leurs ennemis
 - Faire un compromis...
- Célèbre grâce à une publication dans le « Scientific American » sous le titre « Computer Recreations » en 1984 (http://www.koth.org/info/sciam/)

Historique – le ver Xerox

- John Shoch et Jon Hupp (chercheurs au Xerox PARX de Palo Alto, en Californie):
 - Utilisation d'un programme se répliquant sur les machines inactives (concept novateur à l'époque).
 - Une nuit, ce programme est tombé en erreur et a été répliqué plus qu'il ne le faut au point de bloquer les machines du centre.
 - Programme surnommé : « Infamous Xerox worm » (l'infâme ver Xerox).
 - Publié en mars 1982 dans : « Communications of the ACM »

Historique

La préhistoire Les expériences de Fred Cohen Les vrais virus

Fred Cohen – Première expérience (novembre 1983)

- Virus pour une plateforme VAX 11/750 sous Unix
 - Très peu de détails sur le virus en lui-même
 - Nombreuses précautions pour tracer et contrôler le virus
 - Mesure de désinfection systématique sur tous les programmes infectés durant l'expérience
- Dissémination très rapide du virus (au delà de ce que Fred Cohen avait prévu)
 - Certains utilisateurs ayant des droits super-utilisateurs furent infectés
- Dès les premiers résultats, les administrateurs ont interdit la poursuite de l'expérience :
 - « les problèmes que l'on n'étudie pas n'existent pas... »
 - Mais le risque est bien réel et ne peut être ignoré!

Fred Cohen – Seconde expérience (juillet 1984) (1/2)

- Système Univac 1108, maximum de précautions (traçage, contrôle des infections, limitations de ressources physiques disponibles, nombres de compte disponibles...)
- But : montrer la faisabilité d'un virus sous un système implémentant le modèle de sécurité Bell-LaPadula (modèle de référence à l'époque, http://en.wikipedia.org/wiki/Bell-LaPadula_model).
 - Définit par David Bell et Len LaPadula en 1973 pour le département de la Défense aux EU. C'est un modèle formel à étatstransitions. Il décrit un ensemble de contrôle d'accès pour chaque objet (top secret, secret, confidentiel, non classé) et des règles de transitions.

Fred Cohen – Seconde expérience (juillet 1984) (2/2)

- Le virus a infecté un groupe composite de simples utilisateurs, administrateurs et responsables de sécurité informatique.
- Il a contourné les systèmes de droits utilisateurs et a obtenu des privilèges supérieurs à ceux qu'il détenait initialement.
- Virus assez « simple » : 300 lignes d'assembleur, Fortran et de commandes interprétées.
- Résultats : système à risque, et un virus un peu plus élaboré pourrait faire beaucoup « mieux » !

Fred Cohen – Troisième expérience (août 1984)

- Les résultats de la seconde expérience ont bousculé et ouvert les esprits :
 - Nouveau test autorisé en août 1984 sur un VAX sous Unix
 - But : mesurer la dissémination virale, notamment à travers le partage de fichiers.
 - Considération de certains aspects comme les groupes d'utilisateurs « à risques »

Résultats :

- Les administrateurs se sont fait infectés, bien souvent en exécutant des programmes extérieurs en étant root.
- Le mépris des droits et des précautions indispensables en terme gestion a permis au virus d'agir très rapidement.

Historique

La préhistoire Les expériences de Fred Cohen Les vrais virus

1981 : un virus Apple II

- Premier « vrai » virus...
- But similaire à l'évolution et la sélection naturelle : basé sur la reproduction. Donc les auteurs ont cherché à produire un virus qui se reproduisait tout seul.
- Propagé par le système de formatage des disquettes sur Apple II qui pouvait alors contenir l'OS lui-même.
- ♦ 3 versions de ce virus :
 - une première version, peu répandue en raison de ses effets secondaires.
 - une deuxième, cantonnée aux disquettes des membres créateurs au départ, mais il s'échappe de ce petit cercle... Il provoque certains bugs avec certains programmes
 - une troisième : cette version a en fait été beaucoup plus répandue que ce que l'on croyait, mais ne faisait rien de méchant...

quelques virus...

- ◆ 1983 : Elk Cloner
 - Virus fonctionnant sous AppleDOS 3.3 : il affichait le mauvais type de fichier, inversait l'affichage et provoquait des clics dans les haut-parleurs.
- 1986 : Brain (de Ralf Burger)
 - Premier virus pour plateforme PC, basé sur l'infection de fichiers .COM (ancêtre des .EXE). L'infection modifiait le secteur de démarrage des disques, pour permettre son exécution et sa réplication.

1987 : une année très riches en virus...

- Lehigh: virus infectant le fichier COMMAND.COM. Il efface le contenu de tous les disques à son lancement (déploiement limité sur le campus de l'Université Lehigh).
- Cascade : premier virus chiffré (polymorphisme)
- Christma Exec : premier « ver » d'e-mail pour les gros-systèmes IBM
- premier virus pour Amiga : affichant « Something wonderful has happened, Your AMIGA is alive » (référence au film 2010 sorti en 1984).

la suite...

- ◆ 1988 : la période des vers. Principal virus : Jerusalem (infection des .COM et .EXE, activable tous les vendredi 13).
 - Repérable par des modifications continues du même fichier.
 - Recherche d'une infection en regardant les tailles des fichiers
- ◆ 1989 : les vers...
 - Naissance de la revue « Virus Bulletin » (http://www.virusbtn.com/).
- ◆ 1990 : les virus polymorphes et à cibles multiples
- ♦ 1995 : les virus macros
- 1997 : les chevaux de Troie, virus IRC...
- 1998 : CIH (ou Spacefiller, Chernobyl)
- ◆ 1999 : Melissa (virus de macros)
- ◆ 2000 : virus VBScript (ILOVEYOU, ...)

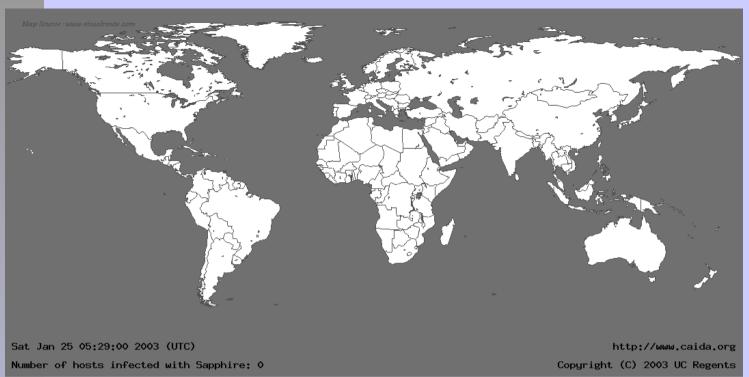
Aspects généraux des infections informatiques

Quelques chiffres

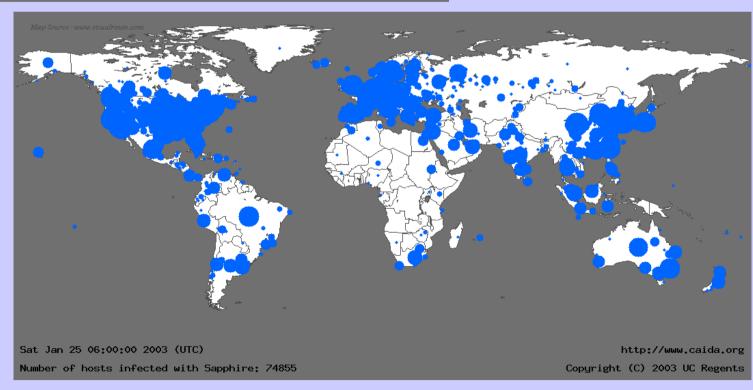
Définition et concepts de bases Diagramme fonctionnel et cycle de vie Conséquence d'une infection informatique Conception d'une infection informatique

Quelques chiffres (sources F-Secure)

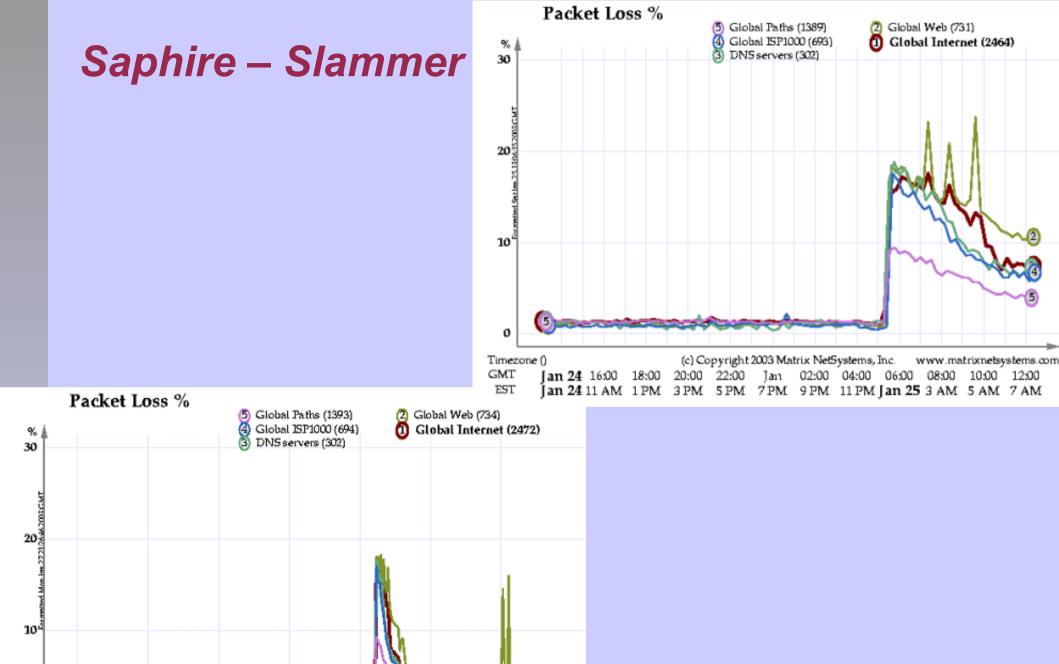
- en 1998, le virus CIH a obligé des milliers d'utilisateurs à changer la carte mère de leur ordinateur après avoir détruit le BIOS, et bien souvent perdu les données du disque dur.
- en 2000, le ver lloveYou infecte plus de 45 millions de machines dans le monde (estimation à 8,75 milliards d'euros de dégâts)
- en 2003, le ver Slammer/Saphire a infecté plus de 75000 serveurs en dix minutes (total de 200000 serveurs).
- en 2003, le vers W32/Sobig.F a infecté plus de 100 millions d'utilisateurs
- en 2003, le vers W32/Lovsan ou W32.Blaster a perturbé l'accès de plusieurs fournisseurs internet.



Saphire – Slammer



S. Rampacek 20 M2 STIC INFO – 2005/2006 – Proto Secu – Virus



www.matrixnetsystems.com

Jan 26

1/27

0

GMT

EST

Timezone ()

Tan

Jan 20

1/22

Jan 21

1/23

Jan 22

(c) Copyright 2003 Matrix NetSystems, Inc.

Jan 23

1/24

1/25

Jan 24

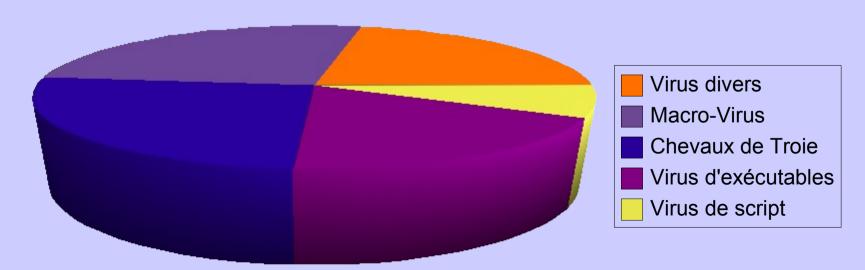
1/26

Jan 25

Données et indices numériques

- Très difficile d'obtenir des chiffres représentatifs.
- Les éditeurs d'antivirus ont des enjeux commerciaux : donc adaptent leurs chiffres en conséquence.
- Suivant Sophos et le livre « Les virus informatiques » [1] :
 - en janvier 2002 : 70000 virus (y compris les variantes)
 - ♦ 800 à 1200 virus chaque mois

Répartion des types d'infections (janvier 2002)

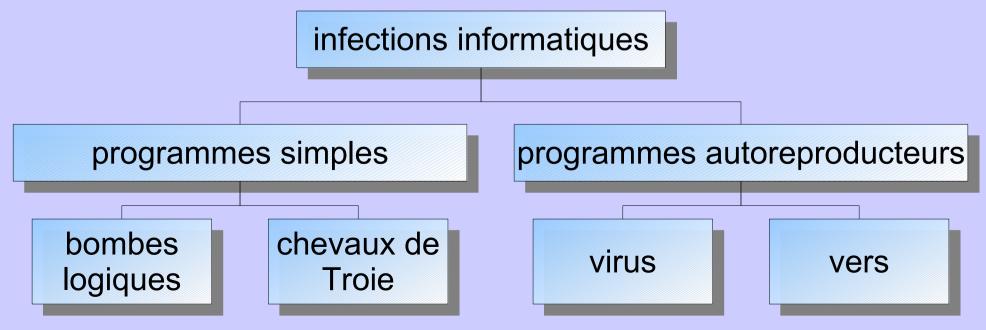


Aspects généraux des infections informatiques

Quelques chiffres
Définition et concepts de bases
Diagramme fonctionnel et cycle de vie
Conséquence d'une infection informatique
Conception d'une infection informatique

Définition d'une infection informatique

- Infection informatique (def. adoptée par Eric Filiol dans son livre):
 - « Programme simple ou auto-reproducteur, à caractère offensif, s'installant dans un système d'information, à l'insu du ou des utilisateurs, en vue de porter atteinte à la confidentialité, l'intégrité ou la disponibilité de ce système, ou susceptible d'incriminer à tort son possesseur ou l'utilisateur dans la réalisation d'un crime ou d'un délit. »



Concepts de base d'une infection

- De nombreux utilisateurs minimisent l'impact de leur infection : « de toute façon, ma machine ne contenait rien de confidentiel ».
- Mais, maintenant, le but des attaquants est :
 - passerelle pour mieux attaquer (« zombie »)
 - avoir entrepôts de données
 - **•** ...
- Les traces d'infection sont généralement effacées (par le virus même ou l'attaquant)
- Deux possibilités d'infections
 - manuel : l'utilisateur exécute un programme qui s'avère être un virus
 - automatique : en utilisant des failles de sécurité du système.

Concepts de base d'une infection (suite)

- Les infections manuelles peuvent être évitées :
 - avertissement de l'utilisateur
- Les infections utilisant les failles de sécurité peuvent être généralement évitées :
 - dans la plupart des cas, un correctif pour la faille est disponible bien avant le virus l'exploitant
- Par contre, les virus ne sont pas ciblés sur un seul système, il suffit d'avoir un système contenant les éléments suivants :
 - mémoire de masse (dans laquelle le programme infecté se trouve sous forme inactive)
 - mémoire vive (dans laquelle le programme est copié lorsqu'il est exécuté)
 - processeur ou micro-contrôleur (exécution du programme)
 - système d'exploitation (ou équivalent)

Aspects généraux des infections informatiques

Quelques chiffres
Définition et concepts de bases
Diagramme fonctionnel et cycle de vie
Conséquence d'une infection informatique
Conception d'une infection informatique

Diagramme fonctionnel d'un virus ou d'un ver

Routine de recherche des programmes cibles

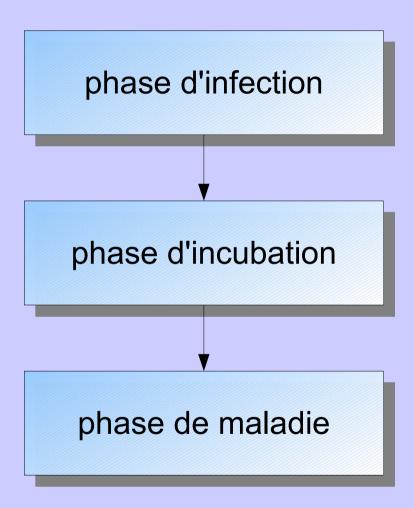
Routine de copie

Routine d'anti-détection

Charge finale
Déclenchement différé

- Routine de recherche doit rechercher les fichiers exécutables (étendu au dossier, au disque, etc)
- La routine de copie infecte par différentes méthodes les fichiers trouvés à l'étape précédente (en limitant les accès disque) et ne doit les modifier qu'une fois
- Routine d'anti-détection : furtivité et polymorphisme
- La charge finale et le déclenchement différé peuvent être optionnels. Dans certains cas, l'infection correspond directement à la charge finale (Slammer)

Le cycle de vie d'un virus ou d'un ver



La phase d'infection

- infection passive (diffusion du virus):
 - le dropper (programme d'apparence inoffensive contenant le virus même, il est généralement attrayant (animation Flash, etc.)) est copié sur un support et transmis.
 - il est déjà arrivé que des professionnels de l'industrie informatique diffuse des logiciels contenant des virus ou des vers
 - virus 1099 par l'intermédiaire de disquette vierge
 - virus Warrier par l'intermédiaire d'un site de téléchargement de shareware sous la forme d'un jeu appelé Packman.
 - virus CIH par l'intermédiaire d'un patch pour le firmware d'un graveur CD, etc.
- infection active (le virus est exécuté) :
 - l'utilisateur exécute le dropper

La phase d'incubation

- Généralement la plus grande partie de la vie d'un virus
- Phase correspondant à la survie du virus. Le virus ne doit pas être détecté :
 - ni par l'utilisateur : par le biais de message d'erreurs
 - ni par l'antivirus : développement par le virus de technique lui permettant de se camoufler

La phase de maladie

- Correspond au déclenchement de la charge finale.
- Peut se déclencher à divers moments (suivant l'endroit dans le code où la routine offensive a été placée).
 - en tête de code
 - en fin de code
 - en milieu de code
- Son déclenchement peut également être différé
 - une date système (vendredi 13)
 - le nombre d'infections réalisées
 - la frappe d'une séquence particulière de touches un certain nombre de fois
 - nombre d'ouvertures d'un document Word

Comparaison biologique/informatique

Virus biologiques	Virus informatiques
Attaques spécifiques de cellules	Attaques spécifiques de format
Les cellules touchées produisent de nouveaux virus	Le programme infecté génère d'autres programmes viraux
Modification de l'information génétique de la cellule	Modification des actions du programme
Les virus utilise les structures de la cellule hôte pour se multiplier	Multiplication uniquement via un programme infecté
Interactions virales	Virus binaires ou virus anti-virus
Multiplication uniquement dans des cellules vivantes	Nécessité d'une exécution pour la dissémination
Une cellule infectée n'est pas surinfectée par le même virus	Lutte contre la surinfection
Rétrovirus	Virus luttant spécifiquement contre un antivirus – Virus de code source
Mutation virale	Polymorphisme viral
Porteur sain	Virus latents
Antigènes	Signatures

Aspects généraux des infections informatiques

Quelques chiffres
Définition et concepts de bases
Diagramme fonctionnel et cycle de vie
Conséquence d'une infection informatique
Conception d'une infection informatique

Conséquence d'une infection Effets de nature non létale

- Effets de nature non létale :
 - affichage d'images ou d'animations, de messages
 - émission de sons ou de musiques
 - Il s'agit en général d'attaques dont le but est de s'amuser (attaques ludiques) ou d'attirer l'attention

Conséquence d'une infection Effets de nature létale

- Il s'agit là de porter atteinte :
 - à la confidentialité des données (évasion de données)
 - à l'intégrité du système ou des données (formatage des disques durs, destruction totale ou partielle de données, modifications aléatoires de données, etc.)
 - à la disponibilité du système (redémarrage aléatoire du système d'exploitation, saturation, simulation de pannes de périphériques) ou des données (chiffrement du disque dur)
 - incrimination des utilisateurs (introduction de données compromettantes, utilisation du système à des fins délictueuses ou criminelles)

Peut-on endommager le matériel?

- Arrive une question : « peut-on endommager le matériel avec un virus ? »
- CIH endommage le BIOS (assimilable à un firmware, donc un programme).
- mais on peut imaginer utiliser une faille d'un contrôleur dans la protection même d'une tête de lecture par exemple
 - dans ce cas, le virus est très ciblé, et a peu de chance de toucher un grand nombre de machines
 - par contre, le danger est réel : peu de détection par l'antivirus dans ce cas !

Aspects généraux des infections informatiques

Quelques chiffres
Définition et concepts de bases
Diagramme fonctionnel et cycle de vie
Conséquence d'une infection informatique
Conception d'une infection informatique

La conception d'une infection informatique

- Détermination du référentiel de travail :
 - la nature de la ou des cibles (environnement matériel, versions de système d'exploitation, logiciels utilisés, etc.)
 - le niveau de savoir-faire des victimes en matière de sécurité (utilisateurs, administrateurs, antivirus en place, firewall en place, correctifs de sécurités appliqués, etc.)
 - les habitudes des utilisateurs
 - la nature des logiciels de sécurité que l'infection informatique devra affronter

La conception d'une infection informatique

- Conception (et qualité de programmation) :
 - tester les valeurs de retour de toutes les fonctions utilisées
 - tester les routines critiques isolément (tester le générateur d'adresse IP, etc.)
 - gestion de la surinfection
- Comment déployer le virus ??

Les infections simples

résident, furtif ou persistant ? Les bombes logiques Les chevaux de Troie

Les différents modes

- mode résident : le programme est actif en mémoire
- mode furtif : résident + l'utilisateur ne doit pas se rendre compte de sa présence
- mode persistant : en cas d'effacement ou de désinstallation, la copie active en mémoire doit pouvoir se réinstaller ellemême. On peut rencontrer également plusieurs copies dans les dossiers systèmes, des clés dans la base de registre permettant de le relancer au prochain démarrage, etc.

Les bombes logiques

- ◆ Définition : « une bombe logique est un programme infectant simple, s'installant dans le système et qui attend un événement (date, action, données particulières...) appelé en général « gâchette », pour exécuter sa fonction offensive. »
- Très difficile à lutter contre les bombes logiques avant leur identification : sous Unix, comment différencier cela d'un cron ?
- Exemple : CIH, chaque 26 avril.

Les chevaux de Troie et leurres (1/2)

- ◆ Définition : « un cheval de Troie est un programme simple, composé de deux parties, le module serveur et le module client. Le module serveur, installé dans l'ordinateur de la victime, donne discrètement à l'attaquant accès à tout ou partie de ses ressources, qui en dispose via le réseau (en général), grâce à un module client (il est le « client » des « services » délivrés inconsciemment par la victime) ».
- ◆ La partie « serveur » du cheval de Troie est généralement dissimulée dans un programme tout autre (attractif). Une fois ce programme attractif lancé, le « serveur » peut s'installer où « il veut » !
- Exemples: Back Orifice (port 31337, UDP), Netbus (port 12345, TCP), SubSeven

Les chevaux de Troie et leurres (2/2)

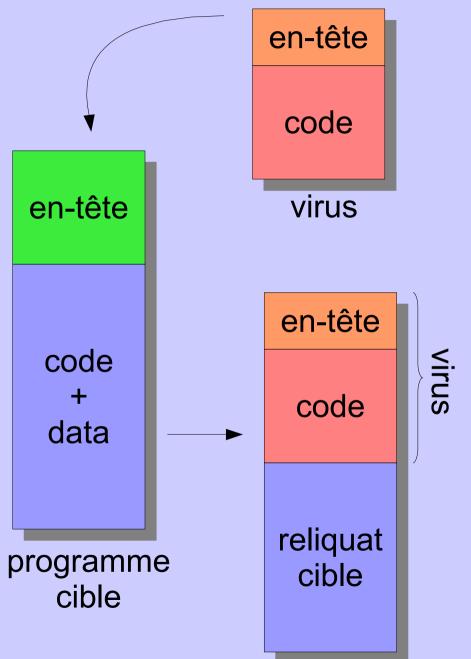
- Détection par les antivirus relativement difficile avant réelle identification par signature : comment détecter une infection d'un programme normal qui s'installe et veut écouter sur un port ?
- ◆ L'aide d'un firewall est bienvenue : même si des manières existent pour le contourner, et tout dépend de sa configuration... (accès total à tous les ports de la machine sur le réseau local, etc.)

Introduction
Les différents modes d'action
Les techniques de non-détection

- Le procédé d'un virus est donc :
 - trouver une cible
 - infection du fichier exécutable (directement sur le disque)
- Il en résulte un code plus ou moins similaire entre les virus, donc une détection basée sur l'heuristique possible (même dans le cas de codes polymorphes)

Introduction
Les différents modes d'action
Les techniques de non-détection

Virus par écrasement de code



- trois cas possible :
 - écrasement de la partie initiale du code de la cible (schéma ci-contre)
 - écrasement en partie centrale ou terminale : le virus doit inclure dans le restant du programme un saut vers lui-même pour être exécuté (peut simuler l'erreur d'un programme)
 - remplacement complet de la cible : « facile » à détecter car la taille du fichier est identique pour chaque cible infectée

Virus par recouvrement de code

- Le code du virus est accolé à celui de la cible.
- Il en résulte une augmentation de la taille du programme infecté si aucune technique de furtivité n'est appliquée.
- Deux cas :
 - tout au début : mais nécessite le recalcul de certaines adresses dans le cadre de fichier binaires de type EXE composés de plusieurs segments. Ce qui entraîne plusieurs lectures/écritures «facilement» détectables.
 - à la fin : le plus simple. Le virus doit juste modifié un morceau du programme pour ajouter un saut vers lui-même.

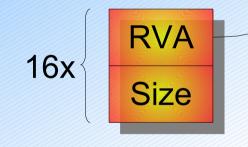
Virus par entrelacement de code

SECTION_DATA

IMAGE_SECTION_HEADER

SECTION_DATA

IMAGE_SECTION_HEADER



IMAGE_OPTIONAL_HEADER

IMAGE_FILE_HEADER

ENTETE DOS

SEC. 2

 Typique de l'infection des exécutable au format PE 32 bits (Windows 95)

SEC.

 Chaque section a une taille arrondie au bloc supérieur de 512 octets. Ils utilisent ces zones « vides » en modifiant légèrement l'en-tête

ENTETE PE

- Ils totalisent les avantages de l'écrasement de code (taille cible identique), et ajout de code (fonctionnement du programme hôte non modifié)
 - Exemple : CIH...

S. Rampacek 51 M2 STIC INFO – 2005/2006 – Proto Secu – Virus

Virus par accompagnement de code

- Virus ne modifiant pas le programme cible. Le virus s'exécute avant le programme réel demandé. Plusieurs façons :
 - Sous DOS: un .COM est exécuté avant un .EXE, lui-même exécuté avant un .BAT. Sous Windows: modifications de la cible des icônes (qui ne sont généralement que des raccourcis)
 - Modification du PATH
 - ◆ Le virus renomme le fichier cible et prend son nom original.
- Une fois le virus démarré par une de ces 3 façons, il peut exécuter son propre code, puis, ensuite, exécuter le programme original
- Avantage : totalement transparent pour l'utilisateur !

Virus de code source

- Le virus (sous forme binaire), infecte un programme cible (sous forme code source) par un virus (code source).
- Avantage : le code binaire généré est homogène et n'a pas été modifié « binairement » après compilation.
- Usage typique : ajouter une inclusion d'un fichier ressemblant à une bibliothèque standard.
- Possibilité de détection :
 - lecture attentive du code source (que faire dans le cas d'un très gros programme ?)
 - fichiers de contrôle MD5 (si le virus est capable de modifier le source, il y a de forte chance qu'il puisse modifier ce fichier MD5 également).
- K. Thompson (Reflections on Trusting Trust, ACM, 1984) a même imaginé un compilateur infectant le code source qu'il compile... On peut étendre aussi à un processeur...

Introduction
Les différents modes d'action
Les techniques de non-détection

La furtivité

◆ Ensemble des techniques visant à leurrer l'utilisateur, le système et les logiciels de protection afin de faire croire à l'absence de logiciel malveillant, en le rendant hors de portée de la surveillance.

Obtenu par :

- dissimulation dans des secteurs clefs (secteurs déclarés faussement défectueux, zones non utilisées par le système d'exploitation, etc.)
- leurrage de structures particulières (table d'allocation des fichiers) ou de fonctions ou de ressources logicielles du système (détournement d'interruption, d'API Windows...)
- Dans certains cas, le virus peut se désinfecter totalement ou partiellement après l'action de la charge finale, diminuant ainsi le risque de détection

Le polymorphisme

- Les antivirus fonctionnant en grande partie sur la recherche de signatures virales, le but du polymorphisme est de faire varier, de copie en copie virale, tout élément fixe.
- Deux principales méthodes :
 - réécriture de code par utilisation de code équivalent.
 - par exemple : obtenir un nombre aléatoire n, et lors de la copie, modifier la copie virale afin d'ajouter n à une variable et retrancher n quelques instructions plus loin...
 - utilisation de techniques de chiffrement basique sur tout ou partie du virus ou du ver.
 - la première fonction du programme doit donc consister au déchiffrement du virus, et cette fonction doit être en clair
 - nécessité de changer la fonction de chiffrement à chaque copie virale, sinon, ce sera la signature du virus!

Les autres techniques...

- mise en sommeil des logiciels de protection
 - W32/Klez.H (ver): tente de désactiver les antivirus en tuant environ 50 processus et en effaçant 10 fichiers utilisés par ces derniers
 - W32/Bugbear-A (ver) : visait plus d'une centaine de logiciels de sécurité !
- saturation des logiciels de protections, perturbations, etc.
- désinstallation pure et simple de ces logiciels

Classification des virus et des vers

Nomenclature des virus Nomenclature des vers

Virus d'exécutables

- Virus les plus connus
- Caractéristiques :
 - petites tailles
 - de bas niveau
 - généralement, ils utilisent l'assembleur
- Voir diapos précédentes pour plus de détails

Virus de documents (1/2)

Définition :

« Un virus de document est un code contenu dans un fichier de données, non exécutable, activé par un interpréteur contenu de façon native dans l'application associée au format de ce fichier (déterminé par son extension). L'activation du code malveillant est réalisée, soit par une fonctionnalité prévue dans l'application (cas le plus fréquent), soit en vertu d'une faille interne de l'application considérée (de type buffer overflow par exemple). »

Virus de documents (2/2)

- Ces virus peuvent être contenus dans un format texte (VBS, JS, RTF, PS, PDF, ...) ou binaire (DOC, XLS, PPT, PPS, ...)
- Virus de macros :
 - essayent généralement de se mettre dans les modèles de document (normal.dot pour word).
 - et modifient le comportement de certaines fonctions (FileSaveAs, ToolsMacros) ou raccourcis (Shift, ...)
 - utilisent la fonction AutoExec s'exécutant à l'ouverture du document (suivant les paramètres de l'application)

Virus de démarrage

- Virus de BIOS
 - Très peu répandu (la seule vraie démonstration est CIH).
 - Modifie ou détruise le BIOS de la machine (qui au départ était « Read Only », ce qui n'est plus le cas maintenant).
 - Avantages :
 - contrôle total de la machine
 - accès à tous les fichiers du disque (sous forme binaire) sans aucun droit, etc... imposé par le système d'exploitation.
 - difficilement détectable
- Virus de démarrage
 - remplace le MBR sur le disque dur
 - intérêts :
 - indépendant du système d'exploitation
 - accès total également à toutes les données du disque

Virus comportementaux

- Certains parlent également de :
 - virus résidents
 - utilisation de l'interruption logicielle 21H sous DOS, de module VxD sous Windows, de « cron » sous Unix (en étant super-utilisateur), ou s'incluant dans le .profile
 - virus binaires
 - deux « petits » virus combinant leurs actions pour avoir plus de possibilités (surveillance de l'un, etc...)
 - virus blindés
 - virus essayant de rendre leur désassemblage le plus difficile possible
 - rétrovirus
 - utilisation de faiblesse d'un antivirus pour ne pas se faire détecter

Virus psychologiques

Définition :

- « Un virus psychologique est une désinformation incitant l'utilisateur, par des techniques d'ingénierie sociale, à produire des effets équivalents à celui d'un virus ou d'un ver : propagation et action offensive ».
- http://www.hoaxbuster.com/

Classification des virus et des vers

Nomenclature des virus Nomenclature des vers

Les vers

- Les vers n'ont pas besoin d'être attachés à un autre programme
- Mais la duplication est bien là : donc un ver est un virus particulier
- ◆ Le ver se distingue également du virus par son pouvoir infectieux : si l'effet d'un virus classique est généralement limité dans l'espace à une région ou un petit groupe de pays, celui du ver, en particulier depuis 2/3 ans, est planétaire!
- ◆ Les pouvoirs infectieux sont énormes : Codered 2, en 14h, à infecté près de 400000 serveurs Web IIS.
- Sapphire/Slammer, en janvier 2003, a isolé totalement la Corée du Sud du réseau Internet. En 10 minutes, 75000 serveurs ont été ainsi infectés.

Exemple de ver : le ver Internet

- Il utilise des vulnérabilités logicielles :
 - ◆ Démon de messagerie sendmail
 - Utilitaire finger
- Utilisation des logiciels rsh et rexec
 - rexec : connaissance des login et mot de passe nécessaire (donc étape de crackage de mot de passe nécessaire)
 - rsh : exploite les faiblesses du protocole, notamment celui basé sur le principe de mutuelle confiance
- Machines attaquées ont été uniquement des machines SUN ou VAX (adresses de machines récupérées dans /etc/hosts.equiv, .rhosts, .forward)
- Comptes attaqués : mots de passe faibles (aucun mot de passe, nom d'utilisateur, surnom, prénom, endroit, etc.)

Les vers simples

- les vers simples (le premier exemple est le ver Internet (1988)
 - Ils exploitent généralement les failles logicielles permettant l'exécution de programmes sur une machine distante
 - Ils exploitent aussi des faiblesses dans les protocoles réseaux pour se disséminer (mots de passe faibles, authentification sur la seule adresse IP, principe de mutuelle confiance)
 - Sapphire/Slammer (janvier 2003), W32/Lovsan (août 2003)

Les macro-vers

- Programmes hybrides virus (infection de support transmis par réseau) et vers (utilisation du réseau pour la transmission).
- ◆ Le mode d'activation est le plus souvent le fait d'une action humaine, ce qui correspond plus à un mécanisme de virus.
- Le mode de dissémination se fait par des pièces jointes contenant des documents bureautiques infectés (se rapprochent des macro-virus)
- ◆ L'ouverture de la pièce jointe provoque :
 - L'infection du logiciel bureautique concerné
 - Le ver propage l'infection en parcourant le carnet d'adresses
 - Exécute une éventuelle charge finale
- Melissa en 1999

Les vers d'emails (ou mass-mailing worm)

- Le principal médium de propagation est la pièce jointe, activée :
 - soit directement par l'utilisateur
 - soit indirectement par l'application de courrier électronique, en vertu de failles (Outlook Express version 5 par exemple, lance automatiquement tout code exécutable présent dans les pièces jointes).
- ◆ La propagation est fulgurante, mais s'éteint assez vite, car les mesures de lutte se mettent rapidement en place.
- IloveYou en 2000 (45 millions de machines infectées, pour une lettre d'amour), BugBear en octobre 2002, Sobig en août 2003

Quelques problèmes que l'on peut rencontrer...

Les types MIME

- ◆ MIME (Multipurpose Internet Mail Extensions) définit, entre autres, le format des messages Internet afin de prendre en compte des formats non textuels (image, son, application) et des corps de message multi-part.
- ◆ Plusieurs vulnérabilités existent, induites par l'en-tête MIME et ses deux champs les plus importants : Content-Type et Content-Disposition (présents dans les mails et les en-têtes HTTP).
 - Content-Type: indique le format des données (image, son, texte, vidéo, application, ...)
 - Content-Disposition: indique s'il s'agit d'une pièce jointe ou d'un fichier à télécharger
 - En cas de mauvaise gestion des champs, on peut imaginer le pire! (une application définit comme un fichier audio, etc.)

MIME et vulnérabilités

- Exécution automatique :
 - Certaines versions de Outlook ou Outlook Express exécutent directement les pièces jointes ayant audio/wav pour Content-Type.
 - Donc si on met un exécutable en pièce jointe, il sera directement exécuté...
- Usurpation du type de contenu
 - Prenons une pièce jointe ayant pour nom : « supermusic.wav [un grand nombre d'espace] .vbs ».
 - L'utilisateur (suivant les versions d'Outlook) verra :
 - supermusic.wav
 - supermusic.wav ...
 - que va faire l'utilisateur ?
 - En empêchant d'afficher les extensions connues : fichier.txt.vbs s'affiche fichier.txt dans l'explorateur. Que va faire l'utilisateur ?

La lutte anti-virale

La lutte contre les infections Les techniques antivirales et les antivirus Les règles et conduite

La lutte contre les infections informatiques (1/2)

- Fred Cohen : déterminer si un programme est infecté est un problème en général indécidable.
- Il est toujours possible de leurrer un logiciel antivirus. L'activité virale depuis 2002-2003 montre également que l'on peut leurrer également les pare-feux (Nimda).
- Quelques chiffres :
 - détection proche du 100% dans le cadre des virus connus
 - 80 à 90% dans le cadre des virus inconnus (plus exactement dans le cadre de virus inconnus utilisant des techniques virales connues)
- Plus difficile pour les vers :
 - les éditeurs sont plus dans une situation de réaction que d'anticipation
- désinfection très difficile (d'où l'utilisation de petits utilitaires
 S. Rampacek
 Spécifiques)
 M2 STIC INFO 2005/2006 Proto Secu Virus

La lutte contre les infections informatiques (2/2)

- Le problème avec les vers est leur nombre impressionnant de copie : occasionnant des perturbations/saturations des réseaux et serveurs.
- En corrélant antivirus et firewalls, on peut arriver à de très bons résultats. Les firewalls peuvent arrêter des chevaux de Troie inconnus.
- La lutte antivirale représente aussi un enjeu commercial :
 - logiciel ergonomique
 - logiciel rapide
 - logiciel compact (au détriment de la taille de base de signatures)
- Des tests effectués au Laboratoire de Virologie et de Cryptographie de l'Ecole Supérieure et d'Applications de Transmissions ont montré que certains virus anciens ne sont plus

La lutte anti-virale

La lutte contre les infections Les techniques antivirales et les antivirus Les règles et conduite

Les techniques anti-virales statiques

- Recherche de signatures
 - discriminante : ne pas détecter une variante du virus comme le virus lui-même
 - non incriminante : cas des signatures trop petites
 - se limite aux virus connus et facilement contournables (il suffit d'étudier la base de signature)
- Analyse spectrale
 - établir la liste des instructions d'un programme et rechercher une instruction très peu utilisée par un programme non viral.
- Analyse heuristique
 - étudier le comportement d'un programme
- Contrôle d'intégrité
 - calculer un checksum de tous les fichiers pouvant potentiellement contenir un virus

Les techniques anti-virales dynamiques

- la surveillance comportementale
 - tentatives de lecture/écritures, ...
 - utilisation d'interruptions ou d'API
 - utile pour certains virus inconnus (CIH et Norton antivirus)
- l'émulation de code
 - s'apparente à la méthode statique : émule le code dans un environnement confiné

Le rôle de l'antivirus

- Trois catégories :
 - Les scanners lisent des informations sur les supports de stockage et dans la mémoire et recherchent des schémas caractéristiques d'un virus connu
 - Les moniteurs d'activité examinent les opérations en temps réel dans l'ordinateur, et font sonner l'alarme quand ils repèrent un événement potentiellement dangereux
 - Les logiciels de détections de modifications prennent un instantané des détails du système, et alertent l'utilisateur quand une modification a été effectuée

Les différentes fonctions possibles d'un antivirus

- Identification de virus connu (détection de virus spécifique)
 - Méthode la plus répandue et la plus simple à mettre en œuvre : tout est dans la base de définitions de virus. Méthode basée sur la réactivité
- Détection de virus soupçonnés et encore inconnus des logiciels de détection de virus spécifique (détection générique)
- Blocage de virus possibles, impliquant une détection générique
- Désinfection d'objets infectés (habituellement associée à des produits de virus spécifiques)
- Suppression, écrasement ou remplacement des objets infectés. Cette fonction est courante dans les produits génériques et les produits de virus spécifiques lorsque la désinfection est techniquement impossible ou considérée comme risquée

Le virus EICAR

- Pour s'assurer que son antivirus est actif, on peut tester avec le faux-virus EICAR.
- Au début, les éditeurs fournissaient des faux-virus de tests, ils correspondaient bien souvent à une chaîne de caractères inoffensives.
- La chaîne la plus utilisée est EICAR (disponible sur http://www.eicar.org/anti_virus_test_file.htm)
 - voici la chaîne (sans les retours à la ligne)
 X50!P%@AP[4\PZX54(P^)
 7CC)7}\$EICAR-STANDARD ANTIVIRUS-TEST-FILE!\$H+H*
 - Mettre cette chaîne dans un fichier .COM
 - L'exécution affiche : EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

La lutte anti-virale

La lutte contre les infections Les techniques antivirales et les antivirus Les règles et conduite

Les règles d'hygiène informatique

- politique de sécurité
 - elle doit évoluer au cours du temps (ce qui était vrai il y a quelques années ne l'est plus forcément aujourd'hui)
- contrôle des individus
 - virus psychologiques
 - habitudes des utilisateurs
- contrôle des contenus
 - installation de logiciels non autorisés (carte de voeux électronique, écran de veille, etc...)
 - copie illégale d'un logiciel (souvent infectée)
- choix des logiciels
- diverses autres mesures :
 - sauvegardes, séquence de boot, ...

Attitudes à adopter

- Tenir à jour les différents logiciels de protections
- Tenir à jour les différents logiciels
- Tenir à jour les systèmes d'exploitations
- Tenir à jour les différents services s'exécutant sur chaque machine
- Désactiver tous les services qui ne servent pas
- Ne pas mettre une copie de sauvegarde saine sur un ordinateur non sain (ou non totalement vérifié).

Conduite à tenir en cas d'infection

- Isoler du réseau la ou les machines incriminées
- Sauvegarde des données qui ne l'auraient pas encore été (discutable, mais certaines fois, il vaut mieux un fichier infecté que sa disparition complète).
- Sauvegarde des fichiers infectés (préférer la mise en quarantaine plutôt que l'effacement)
- Passer l'antivirus en mode éradication. Redémarrer en mode « sans-échec » ou sur un live-CD contenant un antivirus à jour. Utiliser les outils de désinfections. En cas de très grosse infection : formater et ré-installer la machine si nécessaire
- Essayer de trouver par où est apparu le virus et corriger le problème si possible (règles firewall, etc...). Changer les mots de passe, etc.

Se tenir informer

- CERT (Computer Emergency Response Team)
- EICAR (European Institute for Computer Antivirus Research)
- Site des éditeurs antivirus
 - Symantec
 - Trend Micro
 - McAffee
 - Sophos
 - Fsecure
 - **•** ...
- Mailings-lists de sécurité (Linux, Windows, MacOS).

Quelques cas pratiques

IIS_Worm
Xanax
CIH

Analyse du code d'IIS_Worm

- Ver créé en Juillet 1999 par Trent Waddington (alias QuantumG)
- Exploite une faille dans le logiciel Internet Information Server (IIS), version 4.0 de Microsoft.
- La faille est du type débordement de tampon (buffer overflow) et permet d'exécuter du code sur une machine équipée d'une version non corrigée de ce logiciel.
- 90% des serveurs Web sous NT étaient vulnérables (Source : eEye Digital Security - http://www.eeye.com/)
- Premier ver attaquant les serveurs IIS. D'autres vers exploitant d'autres vulnérabilités ont suivi rapidement : Codered (version 1 et 2)

IIS_Worm - Principes

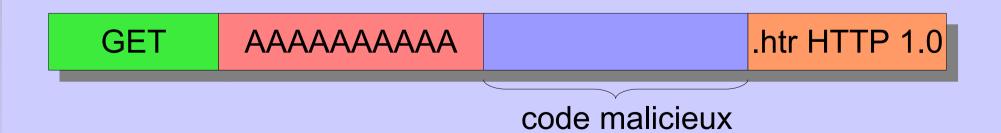
- Le processus viral, exécuté sur une machine infectée, se connecte à un serveur IIS distant.
- Si c'est une version 4.0 non corrigée, alors un code y est exécuté en exploitant un débordement de tampon.
- Ce code consiste à faire se connecter la machine cible en retour sur la machine infectée appelante, pour y télécharger une copie du ver (iisworm.exe)
- Ensuite, le ver examine tous les fichiers *.htm à la recherche d'adresses Internet que le ver tentera d'attaquer.

Débordement de tampon (ou buffer overflow)

- Un buffer :
 - char buffer[N];
 - char *buffer = (char*)calloc(N, sizeof(char));
- ◆ L'écriture hors tableau (indice supérieur ou égal à N)
 - Allocation statique : entraîne généralement un segmentation fault
 - Allocation dynamique : si ce débordement est soigneusement calculé, il peut permettre l'exécution d'un éventuel code (malveillant ou non)
- Exploitation de différentes manières :
 - strcpy(buffer, argv[1])
 - Il vaut mieux utiliser: strncpy(buffer, argv[1], si-zeof(buffer))

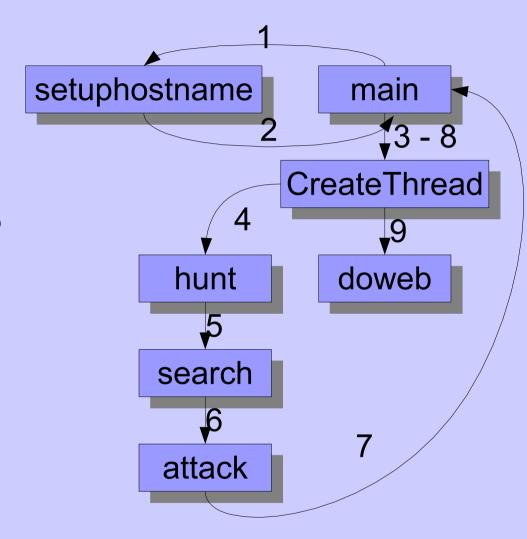
Faille IIS et débordement de tampon

- ◆ Faille détectée par une équipe de la société eEye Digital Security et publiée le 8 juin 1999. Elle affecte les versions 4 d'IIS, sous NT 4.0, SP4 et 5.
- IIS 4.0 permet d'administrer à distance les mots de passe utilisateur au moyen de fichiers internes comportant l'extension .HTR.
- Les requêtes (http) à ces fichiers sont traitées par une DLL externe : ISM.DLL, contenant des tampons non vérifiés (taille des données reçues).



IIS_Worm – étude détaillée du code

- Le code du ver est disponible sur Internet.
- Le code de l'exploit luimême, permettant de se connecter sur le serveur IIS cible, est contenu sous forme hexadécimale dans un tableau déclaré en variable globale



IIS_Worm – étude détaillée du code

- main:
 - charge en mémoire une copie de l'exécutable et gère l'ordonnancement des différentes tâches
- setuphostname:
 - modifie la copie mémoire pour permettre à la cible de se connecter sur l'émetteur pour télécharger le code même du fichier binaire
 - la copie du virus comportant toujours le même nom est une « erreur » : facilement détectable par les antivirus
- hunt:
 - se contente de lancer la recherche (fonctions search) dans les dossiers: \www.root, \inetpub\www.root, etc.

IIS_Worm – étude détaillée du code

- search:
 - recherche les URL du type http://
 - par contre, se contente de récupérer la première rencontrée dans chaque fichier html
- attack:
 - envoie la requête permettant de faire un buffer-overflow
 - si l'attaque échoue (serveur cible mis à jour), seule une entrée dans le fichier de log est réalisée
- doweb:
 - téléchargement du fichier exécutable du ver par le processus fils

IIS_Worm – conclusion

- IIS_Worm présente de nombreux défauts
- Très peu de différences entre un ver et un virus
 - Les fonctions de recherche et de copie sont présentes
 - La procédure d'infection est légèrement différente :
 - Fonctionnement par le réseau pour le ver

Quelques cas pratiques

IIS_Worm
Xanax
CIH

Analyse du code du ver Xanax

- Classe des vers d'emails
 - mais également exploitation des canaux de type IRC
 - infection classique des fichiers EXE
- Premier trimestre 2001
- Nombreux bugs, manque d'optimisation...
 - très représentatif de sa catégorie
- Il a inspiré plusieurs programmeurs de vers
- ◆ Fichier exécutable Win32 (format PE), écrit en Visual C++
- Taille de 60ko, possède une forme compressée de 33792 octets
- Les copies du ver se nomment : xanax.exe et xanstart.exe
- ◆ Le code comporte du C et du VBS

Xanax – infection des emails

- Plusieurs étapes :
 - Détermination du nom du code viral en cours d'exécution
 - Détermination du chemin du dossier Windows
 - Ajout d'une clef dans la base de registre
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
 Version\Run
 - Default=<répertoire_windows>\xanstart.exe
 - Le ver installe une copie, dénommée xanax.exe, dans le dossier Windows.
 - Regarde si le fichier xanstart.exe est présent, et le crée par copie si nécessaire. S'il est déjà présent, il affiche une boîte de dialogue.

Xanax – infection des emails (le VBS)

- Si le fichier xanax.sys n'est pas présent, alors le ver ajoute le fichier wscript.exe (script VBS)
- Ce script récupère le carnet d'adresse et envoie un message aux 1000 premières adresses, contenant :
 - en pièce jointe : le ver
 - un corps de message attrayant vantant les mérites du « Xanax » sur le stress :
 - Hi there! Are you so stressed that it makes you ill? You're not alone! Many people suffer from stress, these days. Maybe you find Prozac too strong? Then you NEED to try Xanax, it's milder. Still not convinced? Check out the medical details in the attached file. Xanax might change your life!"

Xanax – Infection des fichiers exécutables

- L'infection se fait par ajout ou recouvrement de code, en position initiale.
- Teste la non présence du fichier exécutable c:\windows\expostrt.exe (disponible sous Windows 95) pour continuer
- Ensuite, il infecte tous les fichiers exécutables du répertoire c:\windows dont les noms ne commencent pas par R, E, T, W, S
- Et si le fichier ne comporte pas déjà la signature :
 - ny en 19 et 20ème octets du fichier cible

Xanax – Infection via les canaux IRC

- Le ver vérifie la présence de mirc32.exe
- Infecte les fichiers exécutables contenus dans c:\mirc\download (ou assimilé)
- Recherche le fichier script.ini et le remplace par un script IRC permettant d'envoyer xanax.exe à toutes les personnes connectés sur le client IRC

Quelques cas pratiques

IIS_Worm
Xanax
CIH

Le virus CIH (dit « Chernobyl » ou encore « Spacefiller »)

- Crée en 1998 par Chen Ing-Hau, élève-ingénieur en informatique au Taiwan Tatung Institute of Technology (T-TIT)
- Affecte les exécutables 32 bits (format PE) pour Windows 95 et 98 uniquement.
- Plusieurs variantes :
 - CIH v1.2 TTIT : 1003 octets, se déclenche le 26 avril
 - CIH v1.3 TTIT : 1010 octets, se déclenche le 26 juin
 - CIH v1.4 TATUNG : 1019 octets, se déclenche le 26 de chaque mois
 - WinCIH ver 1.5 by TATUNG, Thailand : 26 de chaque mois (10xx octets)
- Le nom « Chernobyl » vient de la coïncidence avec la date de la catastrophe de Tchernobyl (26 avril 1986)

CIH – fonctionnement et infection

Fonctionnement :

- CIH déroute l'interruption 03H (utilisée par les commandes Go et Proceed de DEBUG pour la gestion des points d'arrêts)
- Lors de l'appelle à 03H, CIH regarde si la valeur DR0 est nulle. Si c'est le cas, CIH modifie cette valeur et alloue de la mémoire pour se reconstituer à partir des différents segments de données dispersés dans le PE.
- Repasse ensuite la main au programme hôte

Infection :

- Regarde l'en-tête du fichier (PE\0 veut dire déjà infecté)
- CIH fragmente son code dans les différentes sections non utilisées du fichier PE

CIH – attaque du BIOS et des disques durs

- Modification du BIOS rendu possible grâce au Plug&Play :
 - CIH modifie 128 octets dans la partie « Power On Self Test », rendant impossible un redémarrage
 - Ne fonctionne pas tout le temps (BIOS flashable, protection etc...)
- CIH écrase les 2048 premiers secteurs (soit généralement 1Mo de données) sur tous les disques présents dans la machine. Ce qui a pour effet d'écraser :
 - le MBR (boot impossible)
 - la table des partitions
 - la première FAT (table d'allocation des fichiers)
 - la copie de la FAT (suivant la taille de la première FAT)
 - Soit une perte totale des données dans la majorité des cas

Conclusion

Conclusion

- Bien connaître les virus est déjà un grand pas !
- Les administrateurs doivent :
 - être très précautionneux
 - avoir une vraie politique antivirale (antivirus, firewall, mise à jour régulière, audits)
 - établir une charte informatique interdisant aux utilisateurs d'installer tout et n'importe quoi
- Les utilisateurs doivent :
 - être informés et formés sur les risques
 - ne pas relayer d'information fausse (les vrais alertes au virus viennent des administrateurs)
 - ne pas dire : « l'administrateur s'occupe de tout, je suis protégé, je ne risque plus rien »

Bibliographie

- ◆ [1] Les virus informatiques : théorie, pratique et applications, Eric Filiol, ed. Springer, 2004
- [2] Virus, Définitions, mécanismes et antidotes, D. Harley,
 R. Slade, E. Gattiker, ed. CampusPress, 2002
- ◆ [3] MISC Multi-System & Internet Security Cookbook, ed.
 Diamond Editions, n°3, 5, 8, 21
- [4] Les sites des différents éditeurs antivirus (Sophos, Symantec, etc.)