Securité Windows "Home User"

Romeo Verdier, Aurelien Beaugendre

Vendredi 7 Mars 2003

Table des matières

Chapitre 1

Ce qu'il faut savoir pour commencer...

1.1 Désactiver le compte invité

Le compte 'invité' donne l'accès en anonyme à la machine. S'assurer que ce compte est désactivé, peut prevenir l'utilsation abusif de service laissé ouvert par mégarde. Vous pouvez le désactiver de la façon suivante (Windows 2000 et XP) :
Panneau de Configuration — Utilisateurs et Mots de Passe
Ensuite, clicquez sur l'onglet Options Avancées ; et choisissez "Avancées". Vous pouvez modifier les propriétés du compte "Invité" dans le répertoire "Utilisateurs". Certaines personnes confondent le groupe "Tout le monde" avec le compte "Invité". "Tout le monde" représentes TOUT les utilisateurs qui sont authentifiés peu importe le compte. Si vous etes un utilisateur d'un PC, vous etês automatiquement un membre du groupe "Tout le monde". Si un utilisateur n'a aucun moyen de s'authentifier, l'acces est authorisé par defaut au compte/groupe "Invité". C'est pour cela qu'il est conseillé de le désactiver.

1.2 Désactiver les partages cachés

Ces partages cachés et installés par Windows sont des partages administratifs présents sur chaque PC et utilisé par le compte SYSTEM. Vous pouvez lancer une console de commande Windows et voir tous ces partages en tapant la commande NET SHARE. Vous pouvez désactiver ces partages par de deux façons différentes. La première des façons, un peu radicale certe, est de désactiver ou de stopper le service Serveur de windows, ce qui engendrerai toute possibilité de partager quoi que ce soit. Vous pouvez le désactiver via : Panneau de Configuration — Outils d'Administration — Services. Clicquez sur Manuel ou Désactivé.

L'autre méthode passe par l'edition de la base de registre de Windows et plus particulièrement la clé :

HKEYLocalMachine\SYSTEM\CurrentControlSet\Services\LanManServer\
Parameters

Editer (ou ajouter) AutoShareWks avec une REG_DWORD Valeur à 0. Gardez en tête que la désactivation de ces partages peut etre une mesure poussé de sécurité, mais peut également poser des problèmes dans l'environnement du réseau windows. Les partages cachés par defaut sont :

C$ D$ E$ Racine de chaque partition. Pour un PC sous windows NT workstation/Windows 2000, seuls les administrateurs ou les opérateurs de sauvegarde peuvent se connecter sur ces partages.

ADMIN$ Ce partage est utilisé par le système pendant n'importe quel administration distante de l'ordianteur. Le chemin de cette ressource

IPC$ Les connections temporaires entre les serveurs se font à l'aide de pipe essentiel pour la communication inter - programme. Ce partage est utilisé également pendant l'administration distante de la machine. Cer partage est vraiment dangereux et peut être utilisé pour avoir enormement de renseignements sur votre réseau.

NetLogon Ce partage est utilisé par le service d'authentification distante de Windows 2000.

PRINT$ %SYSTEMROOT%\SYSTEM32\SPOOL\DRIVERS Utilisé pour l'administration distante des imprimantes.

1.3 Désactiver le port 135

Désactiver COM Distribué (Ceci ferme le port 135)
Cliquez sur Démarrer — Exécuter — et entrer : C :\WinNT\System32 \Dcomcnfg.exe. Cliquez ensuite sur l'onglet "Applications". Beaucoup de programme "supportent" la communication distribuée (DCOM) mais peu d'entre eux les utilisent vraiment. Ces programmes sont par exemple Windows Media ou Wordpad.

Quand vous regardez cette option, regardez les tierces parties concernant les applications qui ont besoin le support réseau. Pour trouver si ces programmes utilisent et nécessite le DCOM, vous devez le désactiver, lancer vos programmes, et regardez ce qui se passe. Les programmes Microsoft sont conçus pour fonctionner sans nécessite du réseau. Pour désactiver DCOM, allez dans l'onglet Propriétés par défaut et décochez la case nommé "Activer Distributed COM(DCOM) sur cet ordinateur".
Redémarrer, et essayer de lancer les programmes qui sont susceptibles de ne pas fonctionner. L'avantage réside dans le fait que tous les programmes peuvent continuer à fonctionner correctement. Si ce n'est pas le cas, faites un retour en arriere et activer une nouvelle fois DCOM. Une fois réactivé, allez également dans l'onglet "Protocoles par défaut" et enlevez tous les protocoles excéptés "TCPIP orienté connexion".

Ceci ne rajoute pas un peu plus de sécurité mais réduit le nombre de méthodes de connexion sur lesquelles vous devez jeter un oeil. Si jamais la désactivation fonctionnait, vous pourriez alors enlevez la totalité des protocoles. Vous n'en auriez plus besoin, ceci arrêterai l'écoute sur le port 135.

1.4 Protection contre Denial Of Service Attack

La protection contre les attaques de déni de service a été publié par Microsoft et explique comment proteger la pile TCP/IP de Windows NT/2000 contre ces attaques. La faille de la base de registre documenté ici provient de source de Microsoft.

Ne faites pas de modifications dans votre base de registre si vous n'êtes pas expérimenté dans le domaine. Vous pourriez causer de sérieux dégas sur le système d'exploitation. Faites toujours une sauvegarde de votre base de registre avant de faire que ce soit.

La protection contre Synattack implique la reduction du nombre de retransmissions pour les SYN-ACKS, qui reduit le temps d'où les ressources doivent demeurer assignées. L'allocation des entrées des routes ne s'effectue pas tant qu'il n'y a pas de connexion. Si synattackprotect = 2, l'indication de raccordement à AFD est retardé jusqu'à ce que les communications soient terminées. Notez en outre que les mesures prises par le mécanisme de protection se produisent seulement si les paramètres de TcpMaxHalfOpen et de TcpMaxHalfOpenRetried sont excédés. Appliquez la faille suivante sur la base de registre :

Hive : HKEY_LOCAL_MACHINE

Clé :SYSTEM\CurrentControlSet\Services \Tcpip\Parameters

Nom : SynAttackProtect

Type : REG_DWORD Valeur : 0 Pas de SynAttack protection

Valeur : 1 reduit les tentives de transmissions et de retard de RCE(Route Cache Entry) si les paramètres de TcpMaxHalfOpen et TcpMaxHalfOpen-Retried sont bons.

Valeur : 2

Ce paramètrage assure la meilleure protection. Cette valeur implique des delais additionnels sur les connexions et ajoute des timeout rapides sur les requetes TCP quand il y a une SYN Attack. Quand le système se trouve attaqué par lui - même les options suivantes permettent la désactivation de n'importe quelle socket : Scalable Windows (RFC 1323) et paramétrage TCP des interfaces(Initial RTT, window size). C'est ainsi parce que quand la protection sur les entrées des routes fonctionne, le cache des routes n'est pas solicité avant la SYN-ATTACK soit envoyé et les options de Winsock ne sont pas encore disponible à ce stade de connexion. Le paramètre TcpMaxHalfOpen controle le nombre de connexions permises dans l'etat SYN-RCVD, avant que la protection contre la SYN-ATTACK commence à opérer. Si SynAttackProtect est mis à 1, assurez-vous que cette valeur est plus petite que le nombre de log d'écoute du port que vous voulez protéger.

Hive :HKEY_LOCAL_MACHINE
Clé : SYSTEM\CurrentControlSet\Services \Tcpip\Parameters
Nom : TcpMaxHalfOpen
Type : REG_DWORD Valeur : 100 Professionel, Serveur
Valeur : 500

EnablePMTUDiscovery : Quand ce paramètre est à 1 (Vrai) When this parameter is set to 1 (True) TCP essaie de trouver la plus grande unité de transmission (MTU ou la plus grosse taille pour un packet). En trouvant le chemin du MTU et en limitant la taille des segments à cette taille maximale, TCP peut éliminer la fragmentation aux routeurs sur le brin utilisé par le réseau des différents MTUs. Cette fragmentation compromet les sorties TCP et la surcharge du réseau. En mettant ce paramètre à 0, cela engendre un MTU de 576 Bites pour l'utilisation de toutes les connexions vers les hôtes du sous - réseau local.

Hive : HKEY_LOCAL_MACHINE
Clé : SYSTEM\CurrentControlSet\Services \Tcpip\
Nom du Paramètre : TcpMaxHalfOpenRetried
Type : REG_DWORD
Valeur : 1 recommendé
Valeur : 0 défaut

NoNameReleaseOnDemand : Ce paramètre détermine si l'ordinateur a libéré son nom NETBIOS quand il reçoit une requête de Release-Name de la part du réseau. Cela rajoute l'accès à l'administrateur de protéger sa machine

contre les attaques malicieuses de Name-Release.

Hive : HKEY_LOCAL_MACHINE
Clé : SYSTEM\CurrentControlSet\Services \Tcpip\
Nom du Paramètre : NoNomReleaseOnDemand
Type : REG_DWORD
Valeur : 1 recommendée
Valeur : 0 défaut

EnableDeadGWDetect : Quand ce paramètre est à 1, TCP peut détecter les passerelles mortes. Avec ce dispositif, TCP peut demander à IP de passer sur une passerelle de secours si le nombre de connexions commencent à connaître des difficultés. Les passerelles de secours sont définis dans la section avancés des paramètres de TCP/IP.

Hive : HKEY_LOCAL_MACHINE
Clé : SYSTEM\CurrentControlSet\Services \Tcpip\
Nom du Paramètre : EnableDeadGWDetect
Type : REG_DWORD
Valeur : 0 recommendé - Une attaque pourrais forcer le serveur à changer pour passer sur une passerelle non voulue.
Valeur : 1 défaut

KeepAliveTime : Ce paramètre essaie de vérifier si une connexion idle ne reste pas en vie uniquement grace à un envoi de packet. Si le système distant reste accessible et fonctionnel, il reconnais les transmissions Keep-Alive. Les paquets Keep-alive ne sont pas envoyé par défaut. Cet option peut être activé par une connexion via une application.

Hive : HKEY_LOCAL_MACHINE
Clé : SYSTEM\CurrentControlSet\Services \Tcpip\
Nom du Paramètre : KeepAliveTime
Type : REG_DWORD
Valeur : 300,000 Valeur recommendée : 7,200,000 (2 heures) défaut

PerformRouterDiscovery : Ce paramètre controle si Windows 2000 essaie d'executer la découverte du routeur selon la RFC 1256 basé sur la recherche par interface.

Hive : HKEY_LOCAL_MACHINE
Clé : SYSTEM\CurrentControlSet\Services \Tcpip\Parameters
Nom : PerformRouterDiscovery
Type : REG_DWORD
Valeur : 0 recommendé - Ceci prévient d'un eventuel bug du routeur.
Valeur : 1 activé
Valeur : 2 activé seulement si le DHCP envoie une option de découverte du routeur

EnableICMPRedirects : Ce paramètre controle si Windows 2000 veut altérer la table des routes en réponse à un message ICMP redirigé qui serait envoyé aux interfaces réseaux comme un message venant d'un routeur.

Hive : HKEY_LOCAL_MACHINE
Clé : SYSTEM \CurrentControlSet\Services \Tcpip\
Nom du Paramètre : EnableICMPRedirects
Type : REG_DWORD
Valeur : 0 recommendée
Valeur : 1 défaut

Chapitre 2

Chiffrements : aspects legaux

2.1 Pourquoi chiffrer ?

Avant l'utilisation massive des ordinateurs, les principaux utilisateurs de moyens de chiffrement furent les gouvernements et les militaires (pour échanger des ordres ou des informations secrètes par exemple). Pour ces utilisateurs le besoin de conserver le secret de leurs communications était primordial. Ce n'est seulement qu'après les années 60, que la cryptographie a commencé a être utilisée à des fins non plus strictement gouvernementales, mais également privées. Ceci s'explique par le développement de l'informatique, des télécommunications, et des réseaux (Internet) qui ont fait augmenter considérablement le nombre d'informations échangées dans le monde. Aujourd'hui le chiffrement est toujours une arme très importante pour les militaires, mais elle est également très utilisée par les banques et les institutions financières (par l'intermédiaire des cartes de crédits, ...) et des Entreprises. On peut constater également que depuis ces dix dernières années, elle entre dans nos vies de tous les jours par l'intermédiaire du courrier électronique (pour protéger ses informations les plus personnelles), et de l'Internet en

général (jeux, casinos virtuels, commerce électronique, et de plus en plus de nouvelles applications liées aux nouvelles technologies numériques et au traitement automatisé massif de l'information...)

Le chiffrement à deux problèmes majeurs à résoudre. Le premier est la protection des fichiers de données enregistrés sur des supports de masse (disques ou CD-Rom par exemple) ou échangées sur le réseau contre des destructions ou des modifications non voulues. C'est ce qu'on nomme le problème d'intégrité des données : des modifications de fichiers non autorisées par un tiers doivent être détectées. Le second est le problème de la confidentialité. Protéger les informations importantes d'une Entreprise devient de plus en plus essentiel pour maintenir un niveau de compétitivité suffisant. Le vol ou la destruction/endommagement de données confidentielles ou importantes (hacking, espionnage industriel), entraîne pour une Entreprise des dommages financiers très coûteux, c'est pourquoi elles se doivent de se protéger, et utiliser des méthodes de chiffrement efficaces qui ne pourront pas être trop facilement brisés par des esprits malveillants.
Le chiffrement permet souvent en outre l'authentification c'est à dire de s'assurer de l'identité d'une personne ; que celle-ci est bien celle à qui l'on s'adresse sans aucun doute possible. Dans le même ordre d'idées elle permet un filtrage d'accès c'est à dire, elle permet de limiter et contrôler l'ensemble des personnes ayant un droit d'accès sur des informations de diverses natures. Enfin la cryptographie peut garantir l'envoi d'une information et sa réception sans que l'émetteur, ni le récepteur puissent nier la transaction ainsi que son contenu (très important pour le commerce électronique), on parle alors en droit de non répudiation.

Enfin il peut être le garant de nos libertés individuelles et collectives dans le cadre de nos droits de citoyenneté (respect de sa vie privée).

Comme nous l'avons vu précédemment, le chiffrement peut être considéré comme une arme de guerre, il doit donc être soumis à des règles bien précises.

2.2 Le chiffrement en France

D'abord un rappel de la façon dont la législation Française voit le chiffrement paraît intéressant. L"article 28 de la loi n° 90-1170 déclare : " On entend par prestations de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet. "

Ensuite il convient de mettre en valeur que le chiffrement est fortement réglementé en France. Nul n'a le droit chiffrer ses communications personnelles, puisqu'il n'y a pas une légalisation de l'utilisation des moyens de chiffrement en France aujourd'hui. Nul n'a le droit de fournir, utiliser ou exporter des moyens ou des prestations de chiffrement sans autorisation préalable du SCSII (Service Central de la Sécurité des Systèmes d'Information, organisme chargé d'accorder ou non l'utilisation de moyens de chiffrement à des tiers), toujours d'après la Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications. Pour obtenir une autorisation de cet organisme, il faut passer par des démarches administratives plus ou moins longues (un peu comme pour la déclaration de fichiers nominatifs avec la CNIL).

Des sanctions ont été prévues à l"encontre des personnes qui ne respecteraient pas ces mesures :

- fourniture ou utilisation sans autorisation d"un moyen de chiffrement : amende de 10000 francs (et 20000 francs si récidive).

- fourniture sans autorisation d"une prestation de chiffrement ou exportation illégale d'un programme : amende de 6000 à 300000 francs et / ou emprisonnement de 1 à 3 mois.

Cette loi permet cependant une libre utilisation de moyens permettant uniquement l'authentification. Il n'y à alors pas d'obligation d'autorisation préalable à la SCSII. C'est le cas notamment des cartes à puces, qui contiennent souvent des moyens cryptographiques garantissant l'identité du détenteur. Cette loi améliore donc les précédentes lois qui étaient plus restrictives en considérant toutes les prestations de cryptographie comme des armes militaires.

Il y a trois façons de gérer le chiffrement par les états. Le premier est la liberté totale : chacun a le droit de chiffrer ses messages et ses fichiers à sa guise. C'est le cas d'un certain nombre de pays démocratiques européens (Danemark, Autriche, Finlande). Le second est la liberté sur le territoire national : elle impose des restrictions à l'exportation. C'est notamment le cas des Etats-Unis, de l'Allemagne, l'Espagne ou encore l'Angleterre. Enfin le régime d'interdiction sauf autorisation spéciale. La France se trouve dans ce dernier cas (bien sûr le plus restrictif), en compagnie des régimes dictatoriaux comme l'Irak. Il est vrai qu'on a du mal à comprendre aujourd'hui encore la position de la France sur ce domaine. D'ailleurs, elle est source d'un débat passionné entre défenseurs et opposants au chiffrement.

Il existe cependant aussi un quatrième régime possible : celui du Tiers de confiance : il s'agirait d'obliger toute personne usant de la cryptographie à confier des copies de ses clés à un tiers (d'où son qualificatif de "confiance"),

à qui s'adressera la justice (voire la police) quand elle souhaitera accéder au contenu de nos échanges d'informations.

La législation française, une des plus restrictives au monde comme nous venons de le voir, se dirige vers un certain assouplissement. La loi n°96-659 du 26 juillet 1996 modifie la législation sur l'utilisation du chiffrement en France, et les décrets pris en 1997 vont dans ce sens. Cependant cette liberté est toute relative puisqu'elle imposerait un tiers de confiance. Ce système n'est pas sans poser un certain nombre de questions et problèmes.

Chapitre 3

Firewall Personnel

Il existe aujourd'hui des firewalls personnels c'est a dire des softs, ils sont généralement moins coûteux (voir gratuit) et plus facile à configurer pour un utilisateur lambda qu'un firewall classique.

3.1 L'intérêt d'un firewall

Lorsqu'un ordinateur est connecté à Internet (ou à n'importe quel réseau), celui-ci est une cible potentielle pour des attaques. De nombreux paquets de données sont envoyés au hasard par des hackers afin de repérer des machines connectées. Ces derniers cherchent une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.

Ainsi, il est nécessaire, notamment pour les internautes ayant une connexion Internet (notamment de type câble ou ADSL), de se protéger des intrusions réseaux en installant un système pare-feu. Un pare-feu (firewall en anglais), est un système permettant de protéger un ordinateur des intrusions provenant du réseau (ou bien protégeant un réseau local des attaques provenant d'Internet).

D'autre part un firewall permet également de contrôler l'accès au réseau des applications installées sur la machine. En effet, les chevaux de Troie sont une sorte de virus ouvrant une brèche dans le système pour permettre une prise en main à distance de la machine par un pirate informatique. Le firewall permet d'une part de repérer les connexions suspectes de la machine, mais il permet également de les empêcher.

3.2 Un peu de théorie

Le protocole TCP/IP est le protocole de base d'Internet, puisqu'il assure la transmission de données. Sur l'ordinateur de l'expéditeur, TCP (Transmission Control Protocol) découpe l'information à envoyer en petits paquets facilement transportables, puis IP (Internet Protocol) achemine les paquets en empruntant le chemin le plus court parmi les machines constituant le réseau. Chaque machine y est identifiée par un numéro unique, actuellement composé de 12 chiffres (IPv4) : la fameuse adresse IP (XXX.XXX.XXX.XXX).

En plus de la portion d'information qu'il transporte, chaque paquet comporte des données de contrôle (notamment les adresses IP de l'expéditeur et du destinataire), ce qui permet aux différents paquets de se retrouver au final sur un seul et même ordinateur. A l'arrivée chez le destinataire, TCP reconstitue l'information initialement envoyée à partir des paquets reçus.

3.3 Quels sont les risques ?

TCP/IP est un protocole particulièrement ingénieux, mais qui n'a pas vraiment été pensé en termes de sécurité.
Des individus malintentionnés peuvent ainsi espionner les communications en interceptant les paquets de données, dont le contenu n'est pas crypté. Ce risque reste toutefois mineur dans le cas d'une connexion à Internet, car les paquets sont susceptibles d'emprunter des chemins très différents. Par ailleurs, d'autres protocoles viennent compléter TCP/IP lorsqu'il s'agit par exemple d'assurer la sécurisation des paiements en ligne, et il est également possible de crypter le contenu des transmissions avant de les envoyer.

Aussi, le risque le plus sérieux est celui de plantage ou d'intrusion dans l'ordinateur, notamment si on dispose d'une adresse IP fixe (câble, ADSL, ligne spécialisée, etc.) : le pirate a alors tout son temps pour étudier le système et tenter d'y trouver une faille. Mais même si on dispose d'une adresse IP dynamique, on n'est pas à l'abri : outre les logiciels permettant de scanner automatiquement des plages d'adresses IP, certains programmes trahissent l'adresse IP lorsque on est connectés.

3.4 Comment se protéger ?

L'idéal est de pouvoir surveiller chaque paquet de données entrant ou sortant, en examinant ses données de contrôle : c'est ce que permet un firewall. Comme la surveillance s'exerce au niveau TCP/IP, les paquets hostiles ou simplement indésirables sont bloqués avant même que l'information originelle ne soit reconstituée.

Il convient simplement de configurer au préalable le firewall, afin de lui dire ce qu'il doit laisser passer et ce qu'il doit bloquer : ce sont les règles de filtrage. On peut ainsi interdire l'accès à certains sites depuis son ordinateur, ou empêcher l'envoi sur Internet d'informations confidentielles définies à l'avance. Réciproquement, on peut décider de bloquer la réception de données envoyées par certains serveurs, par exemple un serveur de mails utilisé par des spammers, ou encore de refuser les paquets contenant certains mots-clés.

3.5 Un Firewall performant et gratuit

Il existe des firewalls simples, performants et même gratuits : c'est notamment le cas de ZoneAlarm, gratuit dans le cadre d'un usage personnel. Les paramètres par défaut de ZoneAlarm assurent une protection optimale pour une utilisation personnelle : vérifiez simplement que dans la section "SECURITY" le niveau de sécurité est sur "High" pour Internet et si besoin que la fonction "MailSafe" est enclenchée. Cette dernière a un rôle préventif et renomme l'extension des fichiers sensibles (notamment les scripts .VBS et les fichiers exécutables .EXE et .COM) afin d'attirer votre attention sur leur danger potentiel en cas d'ouverture.

Il existe un grand nombre de firewalls personnels dont voici une liste :

- ZoneAlarm (gratuit)
- Desktop Firewall de Symantec
- Tiny Personal Firewall (gratuit)
- SafeGuard Personnal Firewall
- TGB : :BOB Personnal Firewall
- NetBarrier Personnal firewall (Mac)
- Personal Firewall de McAfee
- Personal firewall (Gratuit) de Sygate
- BlackIce Defender de Network ICE
- Look 'n' stop Personal Firewall

Il faut préciser que Microsoft a inclus un Firewall personnel dans la version WinXP.

Chapitre 4

Les mots de passe

La stratégie la plus fréquente des malveillants qui cherchent à prendre possession d'un système, consiste d'abord à usurper l'identité d'un utilisateur ; puis, dans un deuxième temps, à utiliser les failles connues du système pour devenir super administrateur sur une machine. Dans la plupart des systèmes, en particulier sous Windows NT et UNIX, lorsque le pirate a réussi la première étape d'usurpation, plus rien ne peut l'arrêter tant qu'il n'est pas détecté. Or, le système d'authentification par mot de passe, n'est efficace que dans la mesure où chacun a conscience que celui-ci constitue un secret précieux. La sécurité de tous repose sur la capacité de chacun à conserver consciencieusement cet important secret. Les trois lois fondamentales qu'il faut connaître et appliquer pour que ce secret ne tombe jamais entre des mains " qui ne vous veulent que du mal ", sont à graver dans le marbre.

4.1 Solide tu le choisiras

Des techniques existent pour tenter de casser les mots de passe. La plus utilisée consiste à faire des essais systématiques à partir de dictionnaires : on connaît l'algorithme de codage des mots de passe, il suffit alors de l'appliquer à des dictionnaires choisis astucieusement - sur Internet, il y en a en de nombreuses langues - et de comparer le résultat à chacune des entrées du fichier système contenant les mots de passe, qu'on a réussi à extraire au préalable. Par cette technique, on arrive à casser en moyenne plus de 20% des mots de passe d'un fichier en moins d'une heure. La loi de composition d'un bon mot de passe doit rendre cette technique inefficace, d'où la règle suivante :
Règle 1 : Votre mot de passe ne doit pas pouvoir être trouvé dans un dictionnaire
Les deux autres techniques utilisées, consistent à essayer toutes les combinaisons possibles, soit sur un jeu réduit de caractères, soit en cherchant une chaîne de caractères de petite longueur. Pour faire échouer ces tentatives, il faut élargir au maximum le champ des combinaisons possibles, ce qui conduit à énoncer les deux règles suivantes :

Règle 2 : Votre mot de passe doit contenir un mélange de caractères alphanumériques et de caractères spéciaux (- +! § %, ...), Règle 3 : Votre mot de passe doit faire au moins 8 caractères

4.2 Jamais tu ne le partageras

Un mot de passe est un secret entre l'utilisateur et sa machine qui ne doit être partagé par personne d'autre. Il ne faut pas non plus écrire son mot de passe sur un support, à proximité de la machine ou de manière qu'un rapprochement puisse être fait avec le système qu'il est censé protéger. Les " stickers " sous le clavier ou le tapis de la souris, ne sont pas une bonne idée !

4.3 Souvent tu en changeras

Les mots de passe circulent en clair sur les réseaux. Des techniques simples (sniffers, espions, chevaux de Troie ...), peuvent être mises en oeuvre pour capter le couple (identifiant, mot de passe) à l'insu des utilisateurs et administrateurs. Ces dispositifs peuvent rester en place pendant des mois avant d'être découverts. Pendant ce temps, tapis à l'écoute du réseau, ils captent tous les mots de passe qui circulent. C'est pourquoi, même robuste, un mot de passe doit être modifié régulièrement - au moins tous les trois mois. Mais cette exigence pose un problème de mémorisation, qui devient insurmontable lorsqu'on a plusieurs mots de passe à se rappeler et qu'on applique scrupuleusement les règles ci-dessus. C'est pourquoi un mot de passe ne peut être un pur aléa. Il faut avoir une règle de constitution mnémotechnique.

4.3.1 Méthode poétique

Elle consiste à apprendre un vers par coeur et à constituer le mot de passe en prenant un caractère de chaque mot. Exemple : " Tant va la cruche à l'eau qu'à la fin elle se casse ". Pour chaque mot du vers qui possède plus de trois caractères, je prends le premier caractère. Les autres mots sont ignorés. J'alterne 1 minuscule, une virgule, 2 majuscules, un point-virgule, 2 minuscules, 1 majuscule, pour que la chaîne fasse 8 caractères. Résultat : t,CE ;feC. Certes, la méthode peut paraître compliquée au premier abord, mais, avec un peu d'habitude on s'y fait très bien. Une version simplifiée, consistant à ne prendre que les premiers caractères de chaque mot du vers, est souvent utilisée. Mais le résultat est considéré comme faible, dès lors que l'attaquant connaît votre méthode de mémorisation.

4.3.2 Méthode par substitution

On apprend par coeur une chaîne C de caractères spéciaux. On prend un mot ou un nom qu' on peux retenir facilement. Par exemple : Robert. On remplace les voyelles par les caractères successifs de la chaîne C. On met une majuscule à chaque bout du mot et on le complète, si nécessaire, à 8 caractères avec le reste de la chaîne C. Résultat : Rb+rT$/. Quand on change mon mot de passe, on ne change que la " graine " (ici Robert) et on garde toujours la même chaîne C qu'on mémorise définitivement. Les mots obtenus sont aussi très robustes.

Chapitre 5

Pourquoi un Antivirus ?

Pour Sécuriser les ordinateurs et préserver l'intégrité des données d'un ordinateur, qui peuvent être d'une importance énorme (par exemple, la base de données d'une banque ne doit sous aucun prétexte être modifiée par un virus...)

5.1 Aspects techniques et technique de recherche

Les Antivirus rivalisent souvent d'ingéniosité pour combattre les virus. Cependant ces derniers trouvent souvent la parade. Nous allons parler ici des différentes techniques utilisées par les Antivirus pour combattre leur raison de vivre.

Principales techniques de recherche virus Nous présenterons quatre techniques majoritairement utilisées par les Antivirus pour localiser les virus. Il s'agit du scanning, du moniteur de comportement, du contrôleur d'intégrité et de la recherche heuristique. Brièvement présenté, le scanneur recherche dans tous les fichiers ou en RAM un code spécifique qui est censé indiquer la présence d'un virus.

Le moniteur de comportement surveille les actions habituellement menées par les virus, les contrôleurs d'intégrité signalent les changements intervenus dans les fichiers et enfin la recherche heuristique recherche des instructions généralement utilisées par les virus.

5.2 Recherche de la signature

On nomme ça aussi scanning. C'est la méthode la plus ancienne et la plus utilisée. Son avantage est qu'elle permet de détecter les virus avant leur exécution en mémoire. Son principe est de rechercher sur le disque dur toute chaîne de caractères identifiée comme appartenant à un virus.

Cependant comme chaque virus a sa propre signature, il faut, pour le détecter avec un scanneur que le concepteur de Antivirus ait déjà été confronté au virus en question et l'ait intégré à une base de données. Un scanneur n'est donc pas en mesure de détecter les nouveaux virus ou les virus polymorphes (car ceci changent de signature à chaque réplication.) Cette méthode est à la fois la plus simple à programmer mais aussi la plus longue à mettre en ouvre car elle n'est utile que si elle recense tous les virus existant.

Cela représente une somme de travail considérable et est quasiment impossible à réaliser. C'est pour ça que les concepteurs Antivirus proposent des mises à jour de la base de donnée tous les mois sur leur site WEB, c'est le seul moyen pour le scanneur de détecter les nouveaux virus.

5.3 Contrôleur d'intégrité et Moniteur de comportement

Schématiquement, un contrôleur d'intégrité va construire un fichier contenant les noms de tous les fichiers présents sur le disque dur auxquels sont associés quelques caractéristiques. Ces dernières peuvent prendre en compte la taille, la date et l'heure de la dernière modification ou encore un checksum (somme de contrôle)Un CRC (code de redondance cyclique), ou un algorithme de checksum avec un système de chiffrement propriétaire pourra détecter toute modification ou altération des fichiers en recalculant le checksum à chaque démarrage de l'ordinateur(si Antivirus n'est pas résident), ou dès qu'un fichier exécutable est ouvert par un programme (si Antivirus est résident) ; en effet si le checksum d'un programme avant et après son exécution est différent, c'est qu'un virus a modifié le fichier en question, l'utilisateur en est donc informé.

D'autre part Antivirus peut aussi stocker la date et la taille de chaque fichier exécutable dans une base de données, et tester les modifications éventuelles au cours du temps. Il est en effet rare de modifier la taille ou la date d'un fichier exécutable. La parade pour les virus est de sauvegarder la date du fichier avant la modification et de la rétablir après.

Les moniteurs de comportement ont pour rôle d'observer l'ordinateur à la recherche de toute activité de type virale, et dans ce cas de prévenir l'utilisateur.Typiquement, un moniteur de comportement est un programme résident que l'utilisateur charge à partir du fichier AUTOEXEC.BAT. et qui reste actif en arrière plan, surveillant tout comportement inhabituel. Que va faire

le zouave ? Description d'attaque virale. Les tentatives d'ouverture en lecture/écriture des fichiers exécutables. Les tentatives d'écriture sur les secteurs de partitions et de démarrage. Les tentatives pour devenir résident.

5.4 Démarche heuristique et Analyse spectrale

Fondamentalement, l'analyse heuristique concerne la recherche de code correspondant à des fonctions virales. Elle est différente dans son principe, d'un moniteur de comportement qui surveille des programmes ayant une action de type virale. L'analyse heuristique est comme le scanning, passive. Elle considère le code comme une simple donnée, et n'autorise jamais son jamais son exécution.

5.4.1 Analyseur Heuristique

Un analyseur heuristique va donc rechercher du code dont l'action est suspecte s'il vient à être exécuté.L'analyse heuristique permet par exemple, pour les virus polymorphes de chercher une routine de déchiffrement. en effet une routine de déchiffrement consiste à parcourir le code pour ensuite la modifier. Ainsi lors de l'analyse heuristique, Antivirus essaie de rechercher non pas des séquences fixes d'instructions spécifiques au virus mais un type d'instruction présent sous quelque forme que ce soit. Pour en revenir à notre exemple de virus polymorphes, Antivirus cherche une suite d'instructions de lecture suivie d'une suite d'instruction d'écriture. Cette méthode est donc un peu plus intelligente que les autres : car elle vise à analyser les fonctions et instructions les plus souvent présentes et que l'on retrouve dans la majorité des virus. Cette méthode permet ainsi, contrairement au scanning, de détecter des nouveaux virus dont la signature n'a pas été ajoutée à la base de données.

5.4.2 Analyse Spectrale

Analyse spectrale Tout code généré automatiquement est supposé contenir des signes révélateurs du compilateur utilisé. De même, au contraire, il est impossible de retrouver dans un vrai programme exécutable compilé certaines séquences de code. C'est grâce à ce principe qu'entre en jeu l'analyse spectrale. Cette analyse vise à repérer les virus polymorphes qui sont indétéctables autrement (leur signature changeant à chaque réplication).

En effet, lorsqu'un virus polymorphe crypte son code, la séquence en résultant contient certaines associations d'instructions que l'on ne trouve pas en temps normal ; c'est ce que va détecter l'analyse spectrale. Par exemple, si dans un programme exécutable, Antivirus trouve une instruction de lecture d'un octet au-delà de la taille limite de la mémoire, on sera probablement en présence de code crypté, donc d'un virus polymorphe.

5.5 Techniques d'éradication de virus

Une fois un virus détecté, que ce soit en mémoire ou sur le disque dur, il reste à le supprimer. Une fonction primordiale des Antivirus est donc la suppression des virus. Leur but est de débarrasser l'utilisateur de ce programme malveillant. Mais il n'est pas si simple que l'on croit de les éradiquer et de récupérer le programme original.

En effet cela est impossible dans le cas de virus avec recouvrement : ils détruisent une partie du programme sain lors de sa duplication. La seule solution est la destruction des fichiers infectés ou carrément le formatage du disque dur. Pour les autres, même si ce n'est pas irréalisable, la tache est cependant très ardue : il faut savoir très précisément où est localisé, dans le fichier, le virus en question sachant qu'il peut être composé de plusieurs parties, ensuite il faut le supprimer, et enfin aller chercher la partie durogramme dont le virus avait pris la place et la restaurer.

Toutes ces manipulations nécessitent une connaissance parfaite du virus et de son mode d'action. Cette éradication se faisant par une recherche (du virus, de la partie déplacée), toutes les caractéristiques des différents virus doivent être répertoriées dans une base de donnée mise à jour pratiquement quotidiennement. Il vous reste cependant un moyen de minimiser les risques d'infections, en évitant d'ouvrir des pièces jointes de mail qui serait suspectes. Par exemple des fichiers .pif, ou .exe, ou .zip etc... Votre méfiance vous assurra une vie élétronique saine :).

Chapitre 6

Cheval de Troie

Le cheval de Troie, qu'est ce que c'est ? C'est pas un truc en bois construit pas des mecs en armure pour prendre une ville fortifiée par la ruse, en tout cas, pas là. Si ça s'appelle comme ça, vous l'aurez compris, c'est parce que ça reprend la méthode... La forteresse c'est le PC, le cheval c'est le programme, l'assaillant se trouve être vous et la victime c'est vous. La méthode consiste à envoyer à un mec le troyen et de lui faire croire qu'il sagit d'autre chose... Le mec le lance et là, si vous avez son adresse IP, vous pouvez contrôler son ordinateur. Vous pouvez imprimer des trucs avec son imprimante, lui piquer des fichiers, jouer à ses jeux, formater son disque, diriger le pointeur de sa souris, piquer ses passwords etc...

6.1 Présentation

Le troyen a existé en trois versions différentes. Les deux premiers étaient des programmes que l'on envoyait en faisant croire que c'était autre chose (des nukers par exemple, ça intéresse tellement de monde sous irc) mais dès le lancement du programme, un message d'erreur s'affichait (exemple : GT0075FR.dll has not found) et vous étiez infecté alors que vous pensiez juste : "Ce programme ne fonctionne pas". Et puis un jour, sans savoir pourquoi, alors que vous reveniez sur irc, vous n'avez plus le contrôle de votre pc, dommage...

La troisième version est la plus sournoise, elle se compose comme les précédentes de deux parties, l'une que l'on envoie à la victime et l'autre que l'on garde et qui nous permet de contrôler l'ordinateur distant. Dans cette version, on garde les deux programmes, car ce que l'on envoie n'est plus un troyen mais un programme sain (la dernière version de netscape par exemple) que l'on a infecté avec un troyen. Et ce qui est terrible c'est que le programme infecté n'augmente même pas de volume (certains disent que le programme augmente de 100 Mo mais c'est faux) et qu'il fonctionne très bien.

Il ne faut pas que ceci vous incite à ne plus revenir sous irc ou icq car il existe des "bouffe-troyens" qui se charge d'inspecter votre disque dur et de vous débarasser des chevals de troies. Par contre, un programme de base, il ne peut se faire détecter par un bouffe-troyen car il ne ne se met en service que quand un bouffe-troyen vérifie le système. Donc jusque là il n'est pas considéré comme troyen. Alors la personne très contente de posséder ce programme miracle ne se doute pas quelle est contaminée...

Alors quand on vous envoie un programme par Internet, vous le testez avec le bouffe-troyen au moins deux fois de suite et vous avez 99% de chances qu'il ne vous arrive rien. Mais comme les personnes qui programment ces trojans auront toujours une longueur d'avance sur ceux qui essayent de les en empêcher, faîtes gaffe de ne pas accepter des .exe, .bat, .zip et .com de tout le monde.

Avec BO (back Orifice) il y a un autre moyen de voir si vous avez été infecté mais ça ne marche que pour BO et ça n'empêche pas au bouffetroyen d'être efficace. Cette manière c'est de faire un ping vers l'ip 127.0.0.1 (ouvrez une fenêtre MS-DOS et tapez "ping-a 127.0.0.1") et si vous y voyez le nom de votre ordinateur c'est que vous êtes infecté.

6.2 Comment ça marche ?

Dès que la victime lance la partie virus du troyen (celle qu'on lui refile), le programme va chercher a créer plusieurs fichiers .exe (généralement 3). La partie virus ne sert qu'à créer ces fichiers. Les fichiers sont souvent crées dans Windows/System mais ça dépends en fait du troyen. S'ils se placent là c'est pour une bonne raison. Tous les ordinateurs ayant windows ont un point commun, ils ont windows. Cela permet au troyen de ne pas a avoir a chercher un emplacement sympas différent dans chaque ordinateur où il va.

Une fois bien caché et reprodui en suffisamment grand nombre pour que vous ne les viriez pas tous, ils vont chercher à se lancer au démarrage de la machine. Pour cela, ne croyez pas qu'il vous se contenter de se mettre dans Windows/Menu démarrer/Démarrage, certaines clés de registre permette justement le lancement au démarrage de certains programmes. Ces tonnes d'informations sont consultables en lançant regedit dans Exécuter. Allez jeter un coup d'oeil et vous comprendrez pourquoi ils se placent là. Si vous connaissez pas l'emplacement où ils se mettent c'est même pas la peine d'espérer. Mais les anti troyens les trouvent très bien donc il n'est pas nécessaire de connaître l'emplacement.

Leur but n'est pas simplement de se lancer au démarrage ou de se reproduire. Ils ont fait ça pour leur propre sécurité et pour être sûr de pouvoir être opérationnel dès que l'ordi est allumé. Opérationnel pourquoi ? Les moyens de rentrer sur un ordi sont les ports et pour y rentrer il faut qu'ils soient ouverts. Les programmes crées sur l'ordi de la victime servent à ça. Le port le plus souvent utilisé est le telnet (port 23) mais d'autre comme le ftp peuvent aussi servir. Ces programmes se camouflent de manière à ce que vous ne puis-

siez pas voir s'ils sont lancés et donc ne pas les interrompre. Ex : Ctrl +Alt + Suppr n'est pas efficace pour les stopper puisque leur nom ne se trouve pas dans la fenêtre de win.

La deuxième partie du troyen, celle que vous n'avez pas envoyé a la victime vous sert de poste de contrôle en quelque sorte et permet de communiquer avec les programmes crées sur le disque de la victime. C'est pour ça qu'ils doivent rester opérationnel, pour que vous ne puissiez pas perdre la connection avec le pc de la victime (si bien sûr elle est connectée).

La contamination se fait très sournoisement, puisque le bout de code des trojans peuvent se mettre dans n'importe quel executable. Filtrez un maximum vos messages e-mails, installez vous des antivirus et le firewall personnel devrai détecter les ports de communication des trojans.