Date: Jeudi 07 octobre 2004 à 18:32:10
Sujet: 3 Sécurité et Hacking

Un Cheval de Troie ou Trojan Troyens

Les chevaux de Troie ("Trojan horses" ou "Trojans" en anglais) tirent leur nom de la célèbre légende mythologique. Comme dans cette dernière, ils utilisent une ruse pour agir de façon invisible, le plus souvent en se greffant sur un programme anodin.

Qu'est-ce que c'est ? Les chevaux de Troie ("Trojan horses" ou "Trojans" en anglais) tirent leur nom de la célèbre légende mythologique. Comme dans cette dernière, ils utilisent une ruse pour agir de façon invisible, le plus souvent en se greffant sur un programme anodin. Ils font partie des grandes menaces que l'on peut rencontrer sur le web, parmi les virus et autres vers. Pourtant, contrairement à ceux-ci, les chevaux de Troie de ne reproduisent pas (en tout cas, ce n'est pas leur objectif premier). Ce sont à la base de simples programmes destinés à être executés à l'insu de l'utilisateur. Objectifs Leur objectif est le plus souvent d'ouvrir une porte dérobée ("backdoor") sur le système cible, permettant par la suite à l'attaquant de revenir à loisir épier, collecter des données, les corrompre, contrôler voire même détruire le système. Certains chevaux de Troie sont d'ailleurs tellement évolués qu'ils sont devenus de véritables outils de prise en main et d'administration à distance. Mode d'action Leur mode opératoire est souvent le même; ils doivent tout d'abord être introduits dans le système cible le plus discrètement possible. Les moyens sont variés et exploitent le vaste éventail des failles de sécurité, du simple économiseur d'écran piégé (envoyé par mail ou autre, du type cadeau.exe, snow.exe, etc, etc...) jusqu'à l'exploitation plus complexe d'un buffer overflow.

Après leur introduction dans le système, ils se cachent dans des répertoires système ou se lient à des exécutables. Ils modifient le système d'exploitation cible (sous Windows, la base des registres) pour pouvoir démarrer en même temps que la machine. De plus, ils sont actifs en permanence (car un cheval de Troie est un véritable serveur, il reste à l'écoute des connections provenant de l'attaquant pour recevoir des instructions) mais ils restent furtifs et sont rarement détectables par l'utilisateur. Ainsi, un listing des tâches courantes ne fournira pas d'indication suffisante : soit le cheval de Troie y sera invisible, soit son nom sera tout ce qu'il y a de plus banal ("Patch.exe", ".exe", "winamp34.exe", "winrar.exe", "setup.exe", "rundlls").

Contre-mesures Du fait qu'ils ne se répliquent pas (contrairement aux virus), ils ne possèdent pas de signature de réplication et ne sont donc pas détectables par les anti-virus, en tout cas à ce niveau là. De plus, les chevaux de Troie n'altèrent en général pas les données vitales de la cible (MBR...) qui sont protégées.

Par contre, comme ils restent des programmes assez répandus

sur internet et qu'ils sont rarement modifiés par les apprentis hackers, il est assez facile de les détecter avec les anti-virus actuels qui connaissent très précisément leur empreinte ou leur code. Le problème est un peu plus compliqué lorsqu'il s'agit de programmes dont les sources sont disponibles librement sur internet. Il devient alors aisé de modifier le code et de le recompiler afin d'obtenir un cheval de Troie dont l'empreinte sera unique et donc inconnue des anti-virus. Si l'on ne peut pas détecter leur présence, on peut essayer de détecter leur activité : un cheval de Troie est obligé d'ouvrir des voies d'accès pour pouvoir communiquer avec l'extérieur. Ainsi, plusieurs ports de la machine risquent de le trahir (par exemple 12345, 31337, etc...) surtout s'ils sont habituellement inutilisés. D'autres chevaux de Troie ont détourné cette faiblesse en utilisant des ports plus communs (relatifs aux services ftp, irc...). Là encore, un utilisateur capable de voir ces ports ouverts doit se poser la question de savoir pourquoi tel service est actif.

=> Rappelons que la commande netstat permet d'obtenir de telles informations sous Linux et Windows. Du point de vue réseau, il est également possible de détecter ce traffic (services/ports inhabituels) ou l'activité secondaire du cheval de Troie. En effet, il arrive que la cible infectée serve de point d'entrée à l'attaquant pour se propager dans tout le réseau. Pour cela, il devra effectuer différentes tâches dont certaines sont aisément détectables (scan de machines et de ports...). Dans la majorité des cas, de telles données trahissent non seulement la présence du cheval de Troie mais fournissent également des informations sur son identité, permettant ainsi de mieux l'éradiquer. Il est même possible d'installer par la suite des leures qui garderont des traces des tentatives de connections externes (trahissant l'attaquant).

Cas concrets Voici les fonctionnalités d'un des chevaux de Troie les plus répandus :

• Accès Telnet

permet de lancer une application en mode texte type "Ms-Dos" ou "Invite de commande" de façon invisible et de rediriger l'entrée/sortie standard vers un port particulier. L'attaquant n'a plus qu'à s'y connecter (via telnet) pour communiquer directement avec l'application.

• Accès HTTP avec un navigateur, supporte le téléchargement et l'envoi de fichiers

permet de créer un serveur web basique dont la racine est celle du disque dur (défaut). Ainsi, un simple navigateur web permet de naviguer dans l'arborescence des fichiers, d'en télécharger et même d'en rajouter.

• Information sur le système distant

• Récupère tous les mots de passe

permet d'accéder aux fichiers mots de passe Windows (pwl et autres) et d'en afficher le contenu. A noter que les mots de passe utilisés pour des connections distantes, partages de documents, etc, sont également récupérés.

• Envoi de boite de dialogue (version Windows) avec réponse de l'utilisateur

permet de communiquer avec l'utilisateur.
• Télécharger/Envoyer/Supprimer/Créer des fichiers
permet d'accéder au système de fichiers dans sa totalité.
• Ouverture/Fermeture des fenêtres actives
permet d'interagir avec le système cible.
• Accés a la base de registre
• Augmenter/Diminuer le volume sonore
• Ajouter des plugins
• Démarrage d'application
• Jouer des fichiers .wav
• Afficher des images
• Ouvrir des documents
• Imprimer
• Fonction keylogger
permet d'enregistrer toute frappe au clavier pour récupération et traitement ultérieur (mots de passe sur le web, mails, etc..).
Cette fonctionnalité existe également en version temps-réel : affichage des frappes clavier en direct chez l'attaquant.
• Capture d'écran
permet de visualiser le poste de travail et les actions de l'utilisateur tout en économisant la bande-passante (par rapport au streaming video)
• Capture d'image si l'ordinateur est équipé d'une webcam
opération basée sur l'utilisation détournée des librairies système (COM) qui supportent les webcams. Le résultat est complètement indétectable pour l'utilisateur.
• Capture du son si l'ordinateur/Serveur est équipé d'un microphone
• Eteindre l'ordinateur
• Redémarrer l'ordinateur
• Déconnecter l'ordinateur du réseau
• Dialogue avec l'utilisateur
• Ouverture/Fermeture du CD-ROM
• Inversion des bouton de la souris
• Envoyer l'utilisateur a une URL choisie
• Blocage du clavier
Cette interface permet de modifier le cheval de Troie avant de l'envoyer à la cible : quel port doit-il écouter, quelle méthode de démarrage utiliser...
Il est même possible de protéger l'accès au futur cheval de Troie par login/password ce qui évitera que d'autres attaquants ne s'y connectent. La partie cliente d'un cheval de Troie est l'application utilisée par l'attaquant pour se connecter au serveur, c'est-à-dire au programme installé sur la cible. Ce client permet d'automatiser et de simplifier nombre de tâches, et même de gérer plusieurs serveurs ! On y retrouve les fonctionnalités citées précédement (telnet, capture d'écran, etc...) et quelques autres comme la redirection de ports qui permet de récupérer tout le traffic que reçoit la cible sur des ports donnés, et donc de l'utiliser pour rebondir (le but étant de ne pas compromettre l'adresse IP de l'attaquant). Back Orifice ("BO") est sans doute le cheval de

Troie le plus connu. Il a été créé par The Cult Of The Dead Cow (cDc), un groupe de hackers formé en 1984. Sa version actuelle est la version 2000 (BO2k), et ses sources sont maintenant disponibles sur internet en license GPL. Cela a sensiblement changé son statut puisqu'il autorise tout personne à vérifier le contenu de l'application pour en être sûr (en effet, nombre de logiciels commerciaux sont accusés de receler une porte dérobée sous prétexte que leur code source n'est pas libre). Cela assure également son évolution et sa pérennité futures.

Un autre point concernant BO2k est son extrême efficacité et ingéniosité. De nombreux bugs ont été corrigés par rapport aux versions précédentes et il possède un grand nombre d'extensions ou "plugins" qui lui donnent une modularité sans limites. Ainsi, il est possible de visualiser en temps réel les déplacements de la souris sur la machine cible.

Tout comme il est possible de diriger cette souris et de contrôler le clavier.

Il existe également des plugins supportant le cryptage de manière à protéger les communications client-serveur; les algorithmes supportés sont nombreux : RC6 384, IDEA 128, CAST 256; Back Orifice 2000 supporte même le tunneling SSH ! Regardons de plus près l'interface de configuration de BO2k : Il y a 3 zones principales : la première où l'on spécifie le fichier du serveur que nous allons configurer (l'executable sera modifié), la seconde où nous définissons les extensions que nous allons utiliser plus tard (qui seront rajoutées à l'executable). La dernière zone concerne les paramètres de chaque fonctionnalité, y compris les extensions que nous venons d'ajouter. Ici nous pouvons voir que l'option de connexion par TCP a été choisie et que le port à utiliser est le 31337. C'est à partir de cette interface de configuration que l'on peut modifier si l'on veut le nom du cheval de Troie. Une fois lancé, BO2k s'installe dans WindowsSystem ou WinNTSystem32 sous ce nom là (par défaut UMGR32.EXE). Après il modifie la base des registre.

• Sous Windows 95/98, la commande d'éxécution du serveur est écrite dans :

HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRunServices

• Sous Windows NT, la commande d'éxécution du serveur est écrite dans :

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun

Le fichier initial peut ensuite être effacé (ou s'auto-effacer si spécifié). BO2k devient ensuite actif à chaque démarrage du système et reste en mémoire. Sous NT, le cheval de Troie utilise une astuce pour éviter d'être tué par le Gestionnaire de Tâches. Il change son PID constamment et créé des processus fils qui lui permettent de rester actif si l'un d'entre eux est tué. De plus, son nom comporte un grand nombre d'espaces et de 'e', ce qui a pour

effet de renvoyer une erreur lorsqu'on tente de le tuer à partir de Windows (tout en n'affectant en rien son fonctionnement). Seule solution : le tuer à partir du DOS !

Sous Windows 9x, le fichier se renomme ".exe" (c'est-à-dire sans nom), ce qui le rend invisible dans le gestionnaire de tâches.

Back Orifice 2000 : fiche technique

• Toutes les versions comportent au minimum :

o un client

o un serveur

o un application graphique de configuration du serveur

• Le serveur ne marche que sous Windows (les dernières versions supportent Windows NT).

• Le client était disponible pour Windows ou Unix dans ses versions précédentes. La version 2000 est réservée aux plateformes Win32.

• Le serveur est totalement configurable (numero de port, type de liaison TCP/UDP...)

• Les fonctionnalités disponibles (de base) comprennent :

Liste de serveurs (style Address Book)

Extensibilité via plugins

Connections serveurs multiples (concurrentes possibles)

Connections de plusieurs clients possible

Journalisation de sessions

Journalisation de frappes clavier

Supporte HTTP pour navigation dans le système de fichiers (chargements possibles)

Gestion du partage de fichiers Microsoft (ajout/suppression de partages, monitoring)

Gestion directe de la Base de Registres

Navigation directe dans le système de fichiers (transferts TCP, gestion...)

Mises à jour à distance, ainsi que installation/désinstallation

Redirection de connections TCP/IP

Redirection d'applications texte pour accès via Telnet

Support multimedia, capture audio/video, lecture audio

Récupération de mots de passe stockés dans la SAM (NT registry) et économiseurs d'écran sous Win9x

Contrôle/arrêt/lancement/listing des processus

Affichage de message à l'écran

Compression de fichiers propriétaire

Redémarrage de la machine à distance

Locking de la machine à distance

Récupération d'informations système

Résolution de noms DNS

Conclusion Les chevaux de Troie représentent aujourd'hui un phénomène inquiétant car grandissant. Ils ont changé les règles du jeu, ouvert de nouvelles voies dans lesquelles se retrouvent de plus en plus d'apprentis hackers. Car contrairement aux virus, ils sont faciles à utiliser, accessibles à tous (sans pré-requis en programmation) et très efficaces. En témoigne leur utilisation croisante à des fins professionnelles : prise en main à

distance (help desk, etc...), administration centralisée, gestion de parcs informatiques. Bien sûr, la majorité des produits utilisés dans ce secteur restent des produits commerciaux, mais la récente percée de Back Orifice 2000 démontre -s'il en était encore besoin- que les choses changent.

Loin d'en promouvoir l'utilisation, rappelons enfin l'énorme menace que les chevaux de Troie représentent : ces outils sont conçus pour espionner et infiltrer les systèmes. Ils sont furtifs et très difficiles à détecter, surtout tant que l'attaquant ne cherche pas à se manisfester. Et cette efficacité ne se limite pas qu'à leur action; il ne faut pas négliger l'impact médiatique entrainé par la découverte d'un tel programme dans le système d'une entreprise : compromission, espionnage industriel, remise en cause de la politique de sécurité, etc.