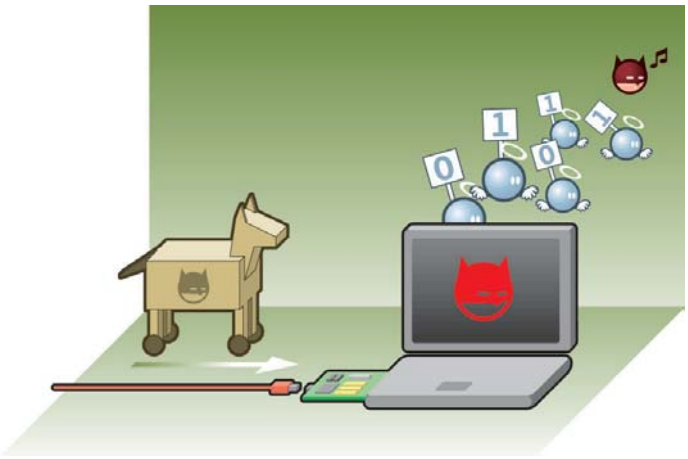
Chevaux de troie

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Ce document traite des chevaux de Troie qui ont pour vocation d'infecter une machine, comme un ordinateur ou un serveur, à l'insu des utilisateurs, dans le but de créer et de maintenir un accès permanent non-autorisé sur une machine.
Les chevaux de Troie peuvent concerner toute personne lors des échanges d'informations par courrier électronique, par transferts via des médias ou bien en téléchargeant des logiciels, documents et tout autre type de fichiers depuis Internet. Sont décrits dans ce document les principes de fonctionnement et de propagation des chevaux de Troie, les impacts possibles ainsi que les mesures préventives.

Table des matières



1 C'est quoi ?

Le terme cheval de Troie apparaît dans la mythologie grecque dans l'Illiade de Homer racontant l'histoire des Grecs décidés à envahir la ville de Troie. Les Grecs savaient que la ville de Troie était trop bien protégée pour tenter de l'assaillir. Ainsi, ils décidèrent de construire un grand cheval de bois et l'envoyèrent à Troie en guise de cadeau et de signe de paix.

Le peuple de Troie apprécia ce geste et emmena le cheval dans la ville. Plus tard dans la nuit, quelques soldats grecs, alors à l'intérieur du ventre du cheval en bois, sortirent de leur cachette, et ouvrirent les portes de Troie pour permettre à l'armée grecque, qui attendait dehors, de s'emparer de la ville.

Ce concept s'est transposé en technologie informatique. En effet, sur Internet, un cheval de Troie est considéré comme un logiciel ou morceau de logiciel - également appelé code exécutable (qui se présente comme un logiciel anodin mais qui en réalité, et de façon très similaire à un virus, a pour vocation d'infecter une machine, dans le but d'ouvrir une porte, à l'insue des utilisateurs. A la différence d'un virus ou d'un ver, un cheval de Troie n'a pas vocation à se reproduire ou à se propager, mais peut cependant être aussi destructeur dans certains cas.

2 Qui est concerné ?

Tous les citoyens, PME et administrations confondues, échangeant des informations par courrier électronique, ou par transferts via des médias tels que disquettes, CD-ROMs, memory sticks, mais également en téléchargeant des logiciels, documents et tout autre type de fichiers depuis Internet.

3 Comment cela fonctionne-t-il ?

La majorité des chevaux de Troie parfois aussi appelés « trojan » sont cachés dans des fichiers ou logiciels ayant des extensions de type .exe, .bin, .com, .zip et similaires.

Exemple de technique d'intrusion : des chevaux de Troie prétendent vouloir désinfecter une machine comme un ordinateur ou un serveur de virus mais en réalité en introduisent de nouveaux sur la machine.

En général, le cheval de Troie sert à créer et maintenir un accès permanent non-autorisé sur une machine, lorsque cette dernière est connectée sur Internet.

suite au verso

Chevaux de troie

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

Certains ouvrent simplement un accès à des fichiers de la machine infectée, d'autres permettent une interaction complète avec la machine infectée depuis Internet ou un réseau local.

Les chevaux de Troie sont généralement classés selon six catégories : d'accès à distance, d'envoi de données, destructifs, de type «denial of service», de type «proxy», ou encore de type FTP (File Transfer Protocol).

Généralement les chevaux de Troie sont classifiables dans plusieurs catégories à la fois.

Exemple : chevaux de Troie d'accès à distance.

Ce type de trojan ouvre un port réseau spécifique permettant à l'intrus de contrôler la machine infectée à distance. Un port réseau est une «porte virtuelle» vers un service d'une machine connectée à un réseau.
C'est par cette «porte» que transitent les informations échangées sur le réseau.
Les exemples les plus connus de chevaux de Troie de type porte dérobée sont : «Subseven», «Backorifice» et «Netbus».

4 Pourquoi se protéger ?

Parce que les chevaux de Troie constituent une menace considérable pour tous les utilisateurs de systèmes informatiques, il convient de se protéger.

En effet, ils peuvent causer des pertes importantes :

pertes financières directes

- destruction de données cruciales,
- mise hors service de tout le système informatique,
- ...

perte de réputation

- mise en cause de la crédibilité dans le cas de divulgation d'informations hautement confidentielles,
- ...

perte de temps

- élimination des chevaux de Troie du système informatique,
- fermeture des portes dérobées ouvertes par les chevaux de Troie,
- efforts pour rétablir les données détruites,
- ...

5 Comment se protéger ?

Pour vous protéger contre un cheval de Troie, il existe trois mesures préventives principales qui sont :

- Utilisez un(des) logiciel(s) de type anti-virus et pare-feu (Firewall). Il est important de vérifier que le logiciel se met à jour régulièrement afin de se protéger contre l'apparition de nouveaux chevaux de Troie. ***(Consultez les deux documents : « Anti-virus » et « Firewall »)***.

Citoyens : vous pouvez acheter ces logiciels dans les grandes surfaces commerciales. Ces produits donnent souvent droit à des mises à jour gratuites de plusieurs mois à quelques années.

- Évitez d'ouvrir des courriers électroniques (e-mails), logiciels, ou tout autre fichier dont le sujet ou le contenu vous semble inhabituel voire anormal.
- Appliquez régulièrement les patchs de votre système d'exploitation (OS) et autres logiciels installés, qui permettent de vous protéger dans la majorité des cas contre les chevaux de Troie. ***(Consultez le document : « Patch »)***.

D'une manière générale, nous vous conseillons d'appliquer les mesures suivantes :

> Assurez un contrôle d'accès individuel aux applications.

> Maintenez un système de sauvegarde performant.

> Protégez physiquement vos machines.

> Tenez-vous informés sur les nouvelles menaces.