

Les chevaux de Troie

S. Cavin, C. Ehret, M. Rey, N. Zwahlen

Détachement de cryptologie de l'Armée Suisse

août 2008

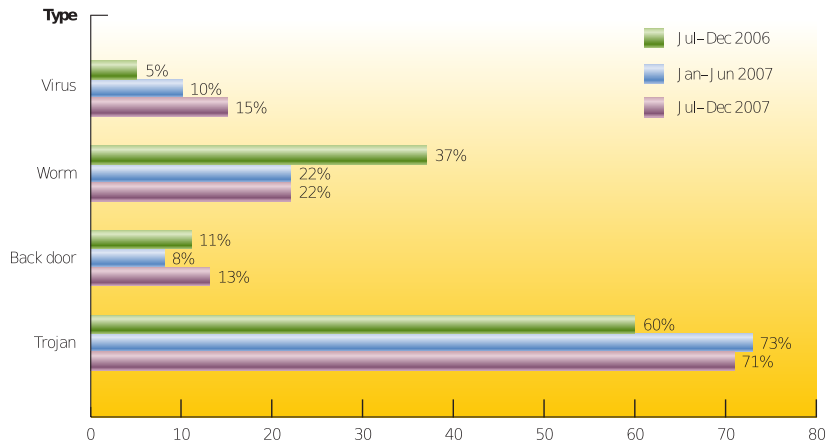
Origine mythologique

Le nom *cheval de Troie* vient de la guerre de Troie dans la mythologie grecque (Homère, *Iliade* et *Odyssée*).

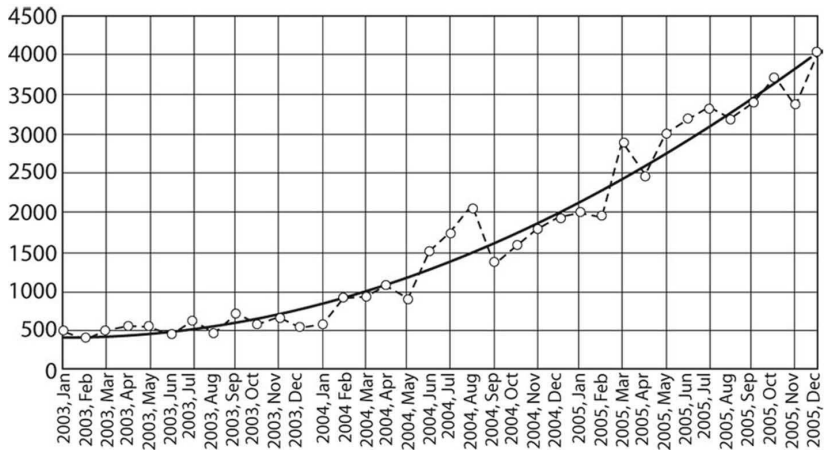


Timeo Danaos et dona ferentes
Je crains les Grecs, même quand ils font des cadeaux
Virgile, *Énéide*, chant II, vers 49

Pourcentage des attaques par type de logiciel malveillant



Nombre de troyens interceptés par Kaspersky Lab



Vecteurs d'infection

- Social engineering : l'utilisateur installe le cheval de Troie volontairement
- Failles de sécurité
 - navigateurs ou plug-ins
 - clients mail
 - serveurs web, mail ou ftp
 - clients de messagerie instantanée
 - ...



Classification

troyens à porte dérobée (backdoor trojans)

troyens voleurs (password-stealing trojans)

troyens espions (trojan spies)

troyens cargo (trojan droppers)

troyens téléchargeurs (trojan downloaders)

troyens relais (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

Back Orifice

- application client-serveur développée en 1998 par *The Cult of the Dead Cow* ;
- version actuelle **BO2k** (licence GPL).

Fonctionnalités

- chiffrement de la communication (AES, Serpent, ...) ;
- accès streaming à l'écran hôte ;
- récupération des mots de passe ;
- modification/ajout/destruction/partage des fichiers ;
- tuer, lister ou créer un processus ;
- modification de la base de registre ;
- *keylogging* ;
- ...

Saboteur constitué d'un fichier compressé standard

- fichier de 4,3 Go rempli de 0, compressé et démultiplié ;
- l'antivirus décompresse les archives pour les inspecter ;
- 42 kilooctets \Rightarrow 4,5 petaoctets :

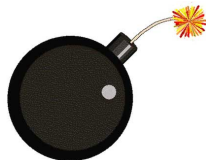
16 · 4'294'967'295 \simeq 68 Go

16 · 68'719'476'720 \simeq 1 To

16 · 1'099'511'627'520 \simeq 17 To

16 · 17'592'186'040'320 \simeq 281 To

16 · 281'474'976'645'120 \simeq 4,5 Po



- \Rightarrow bloque les ressources (cpu, mémoire, stockage) ;
- \Rightarrow destruction de l'antivirus \Rightarrow nouvelle infection.

GpCode

- **GpCode** est un ransomware (cyber-chantage) :
 - crypte les documents Office, zip, C++, pdf, jpg etc.
 - version 2005 : clé RSA 660 bits
 - version 2008 : clé RSA 1024 bits
 - propose un déchiffrement payant (10 – 500 \$)
- Kaspersky Lab offre un outil de déchiffrement pour la version 2005, grâce a une erreur dans l'implémentation de RSA
- défi cryptographique **Operation Stop GpCode** : casser la clé RSA-1024 de la version 2008
- pour se protéger, il suffit d'archiver ses documents sur un support externe



SilentBanker

- SilentBanker a été détecté en décembre 2007
- troyen espion, voleur, relais, téléchargeur et redirecteur
- fraude bancaire
 - vole les informations bancaires d'une victime
 - modifie les données de la transaction
- attaque adaptée à 400 banques
 - intercepte les communications sécurisées
 - modifie les paramètres DNS pour attaque MitM
 - vole les cookies et les certificats si nécessaire
- revenus annexes : redirection sur 600 sites porno



Comment éviter d'être infecté

- maintenir son système à jour ;
- ne pas télécharger/ouvrir des fichiers inconnus ;
- éviter les programme d'échange de fichiers *peer-to-peer* ;
- toujours afficher l'extension des fichiers ;
- ne jamais activer les fonctions ouverture automatique ou aperçu ;
- utiliser un logiciel pare-feu (firewall) ;
- éviter les navigateurs Internet peu fiables ;
- utiliser un système d'exploitation sécurisé ;

Symptômes d'une infection

- une activité anormale de la carte réseau ou du disque ;
- des réactions curieuses de la souris ;
- une ouverture involontaire de programmes ;
- des pannes ou redémarrages répétés.

Comment se débarrasser d'un cheval de Troie

- Nouvelle installation propre.
- Détection et suppression par des logiciels antivirus ;
Pour ce faire, ces logiciels peuvent se baser sur les faits suivants :
 - ces logiciels sont rarement modifiés code ou empreinte identifiable ;
 - ils produisent leur activité sur un port habituellement fermé ;
 - par contre, pas de signature de réplication.

Il est souvent nécessaire de combiner différents antivirus.

Conclusion

- Les chevaux de Troie représentent la majorité des logiciels malveillants en circulation.
- Les chevaux de Troie sont de plus en plus utilisés à des fins lucratives ou criminelles.
- L'utilisation d'un anti-virus, d'un pare-feu et une installation régulière des patches de sécurité sont primordiales pour éviter de se faire infecter par un cheval de Troie.