Les chevaux de Troie

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

Détachement de cryptologie de l'Armée Suisse

2008

Tables des matières

Origine mythologique

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

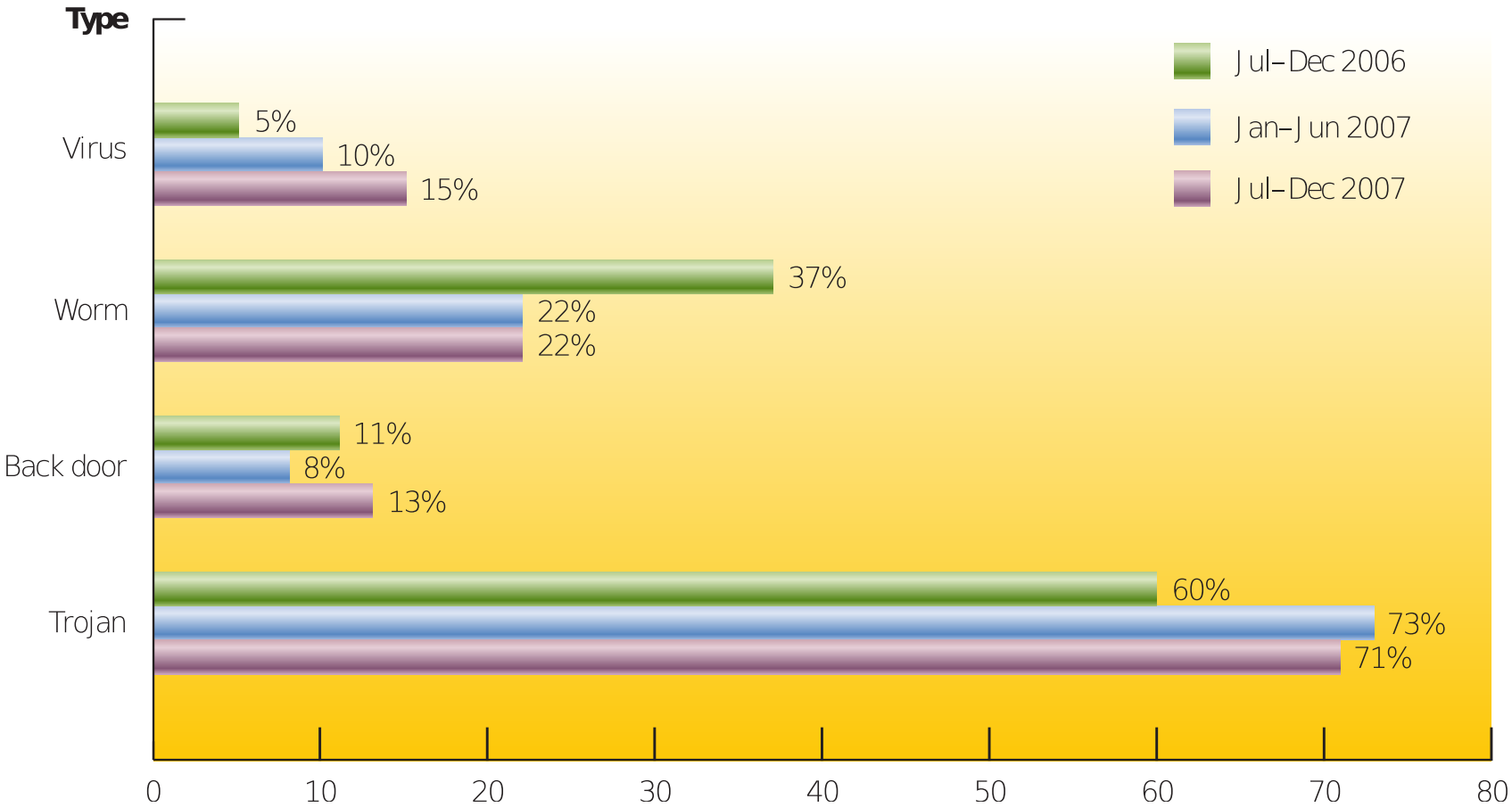
Timeo Danaos et dona ferentes

Je crains les Grecs, même quand ils font des cadeaux

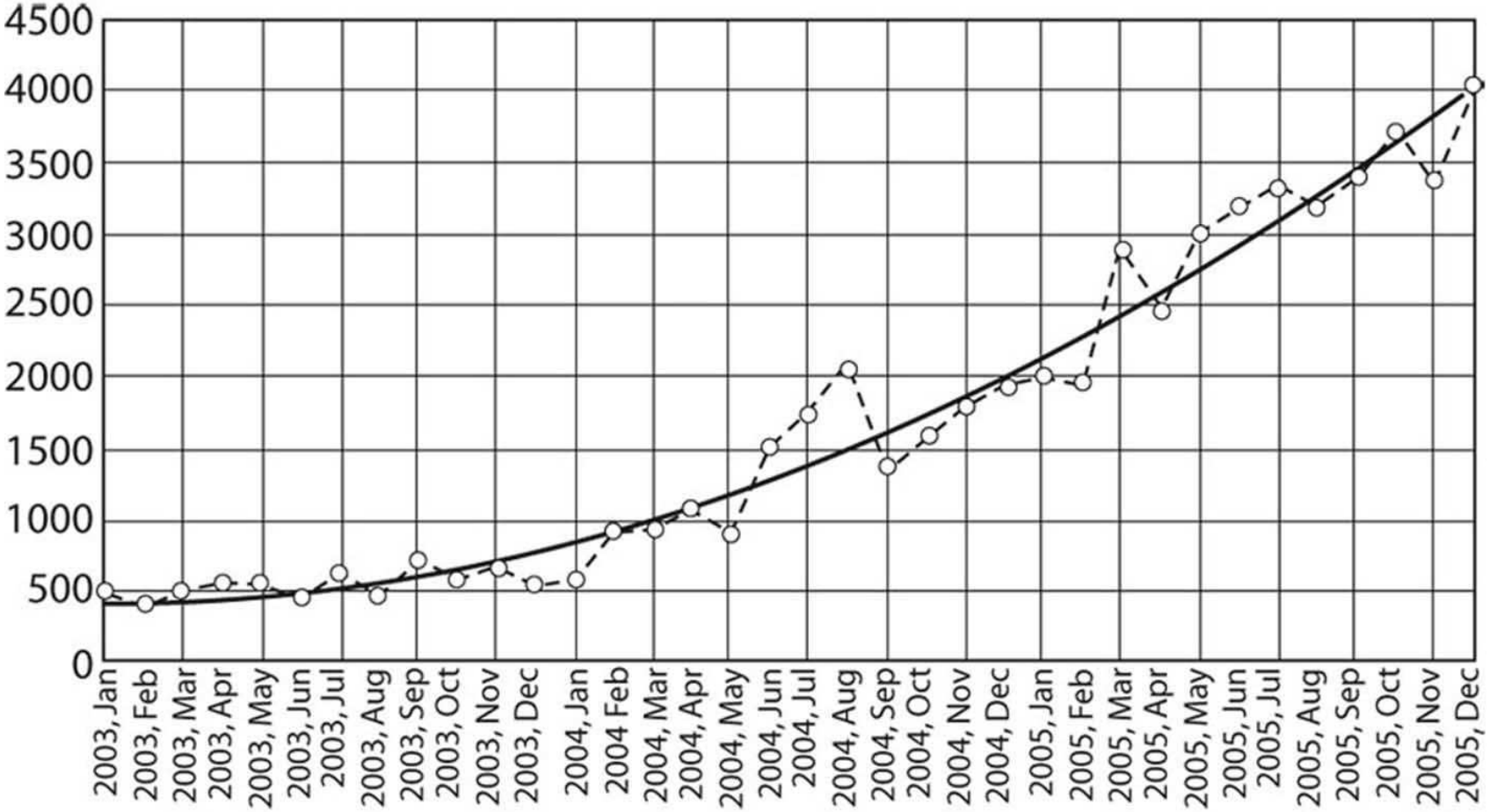
Virgile, Énéide, chant II*, vers 49*

Tables des matières

Pourcentage des attaques par type de logiciel malveillant



Nombre de troyens interceptés par Kaspersky Lab



Tables des matières

Vecteurs d'infection

- L'utilisateur
- Failles de sécurité
  - Sites Web
  - Email
  - Ports ouverts

Vecteurs d'infection

- L'utilisateur
- Failles de sécurité
  - Sites Web
  - Email
  - Ports ouverts

Vecteurs d'infection

- L'utilisateur
- Failles de sécurité
  - Sites Web
  - Email
  - Ports ouverts

Vecteurs d'infection

- L'utilisateur
- Failles de sécurité
  - Sites Web
  - Email
  - Ports ouverts

Vecteurs d'infection

- L'utilisateur
- Failles de sécurité
  - Sites Web
  - Email
  - Ports ouverts

Tables des matières

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

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 serveurs (trojan proxies)

troyens saboteurs (ArcBombs)

troyens redirecteurs (trojan clickers)

Tables des matières

Back Orifice

42.zip

GpCode

SilentBanker

Tables des matières

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.

Tables des matières

Conclusion