CASPER Le Gentil Trojan

Eric DETOISIEN
valgasu@rstack.org

Objectifs

Conception d'un cheval de Troie furtif et efficace sur un poste utilisateur Windows 2K/XP sécurisé situé sur un réseau d'entreprise sécurisé :

- Droits utilisateur restreints
- Firewall Personnel
- Anti-Virus
- Proxy avec authentification
- Firewall

Moyens

Utilisation de technologies Windows natives et connues depuis toujours :

- APIs WININET.DLL pour sortie en HTTP
- Injection de code pour contournement du Firewall Personnel et survie du trojan (multi-injection)
- API Hooking via patch des DLLs en mémoire pour les APIs `connect` et `send` afin de detecter le trafic HTTP, la présence d'un proxy et d'une authentification

Conclusion

- Sécurité en amont avec divers filtrages
- Education de l'utilisateur
- Logiciels spécialisés dans la protection du système

DEMO

http://valgasu.rstack.org/casper/