

Petit trojan hardware

SSTIC

31 mai 2007

Stéphane Jourdois

Petit trojan hardware (1/5)

Problématique :

- Accès au réseau local d'un SI.

Solutions :

- **Cheval de Troie (Trojan) "software" :**
 - Exploite d'une vulnérabilité technique,
 - Modifie le SI logique ;
- **Trojan Hardware :**
 - Basé sur un Gumstix (TM) par exemple,
 - Exploite d'une vuln de contrôle d'accès physique,
 - Très discret.

Petit trojan hardware (2/5)

Problématique :

- Contrôler le réseau local de l'extérieur, donc sortir du SI, ou « reverse-connect ».

Solutions :

- Canaux cachés classiques (ICMP, DNS, etc.),
- Proxy HTTP d'entreprise :
 - Le trouver : protocole WPAD sur le DNS, DHCP, sniff, etc.
 - L'utiliser :
 - pas d'authentification ou auth BASIC...
 - Auth NTLM : le sniff ne suffit plus ?

Petit trojan hardware (3/5)

Problématique :

- Passer l'auth NTLM du proxy HTTP.

Rappels :

- « **Secrets d'authentification sous Windows** »,
A. Bordes, SSTIC2007
 - Principes du Challenge/Response NTLM,
 - Le mdp n'est pas nécessaire, le hash NTLM suffit.
- **Contenu du hash Challenge NTLM proxy :**
 - id incrémental (anti rejeu),
 - identifiant client, etc.,
 - domaine cible.

Petit trojan hardware (3bis/5)

Problématique :

- Passer l'auth NTLM du proxy HTTP.

Solutions :

- Les pages HTML circulent en clair entre le client et le proxy :
 - Man in the Middle, ajout d'une image, le client demande l'image et calcule le challenge pour nous.
 - Il n'y a plus qu'à remplacer le GET foo/bar.jpg par CONNECT foo et réutiliser la réponse au challenge.

Petit trojan hardware (4/5)

Implémentation :

- **Gumstix, Linux, µLibc,**
- **arpspoof pour le MiM et netfilter pour intercepter le port 8080 et le rediriger sur le démon,**
- **le démon « proxy » :**
 - écoute le client sur le port 8080, se connecte au proxy (il est lui-même client du proxy),
 - lit et modifie les pages HTML (attention au gzip...),
 - une fois la réponse au challenge NTLM sur le bon domaine détectée, écoute sur un port arbitraire pour OpenVPN, qui se connecte sur ce port,
 - fonctionne en mode transparent (simple copie d'une socket à une autre) tant que OpenVPN est lancé.
 - Les sockets vers le proxy sont à usage unique, donc le proxy met en queue des sockets d'avance...

Petit trojan hardware (5/5)

Conclusion :

- **Discret physiquement et logiquement (sauf arpspoof), transparent pour les clients légitimes.**
- **Contre-mesures :**
 - Interdire le CONNECT sauf sur une whitelist...
 - Interdire de sortir sur Internet ?
- **A quand une véritable authentification chiffrée entre les navigateurs et les proxy HTTP ?**

Stéphane Jourdois

Tél. : +33 1 41 58 56 47

Mail : sjourdois@arseo.com

© ARSeO

Ce document a été conçu et préparé
par ARSeO.

31 mai 2007

Toute représentation ou reproduction
intégrale ou partielle faite sans le
consentement de l'auteur ou de ses
ayants droits ou ayant cause est illicite
selon le Code de la propriété
intellectuelle (article L 122-4) et
constitue une contrefaçon réprimée par
le Code pénal.

Dans tous les cas, toute reproduction
doit être accompagnées par le titre, la
date et la mention « Source ARSeO ».

This document is copyrighted by
ARSeO. It is not to be copied or
reproduced in any way without ARSeO
express permission. Copies of this
document must be accompanied by title,
date and this copyright notice

ARSeO

8 rue de Valmy

93100 Montreuil

France

www.arseo.com