RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 13 Mai 2008

Rappel sur les attaques physiques

Malgré toutes les protections, l'accès physique aux machines est un facteur de vulnérabilités

- Dump de mémoire après extinction (cold boot attack)
  - un coup de refroidissement pour le faire une heure après
  - scan de la mémoire pour repérer les chaines totalement aléatoires (Clés transitoires AES)
- le port firewire pour pirater windows, linux, etc.
  - utilisation du DMA Mastering
  - même problème avec PCMCIA (ajout d'une carte firewire)
  - certainement le même problème avec l'"USB on the go" et l'eSATA.

Sources

http ://citp.princeton.edu/memory/
http ://tinyurl.com/63pk6s
Michel Arboi et Nicolas Ruff

50 attaques de petits chinois, et moi et moi et moi

Après l'Allemagne, l'Angleterre, les Pays Bas, la France, nouvelles informations de l'Inde et de la Belgique sur des attaques ciblées provenant de chine.

- Le P.L.A. est-il en cause ?
- Les fournisseurs chinois ne sont-ils que "vecteurs" ?

Sources

http ://tinyurl.com/4qooke
http ://tinyurl.com/3j2nkl

Un concours pour léser les antivirus... avec un grand B

Pour le defcon 16, un concours Race to Zero est organisé

- Réussir à légèrement modifier des virus existants
- Les garder fonctionnels
- Leur éviter la détection par un certain nombre d'antivirus

Les réactions des auteurs d'antivirus sont.... intéressantes.

Sources

http ://www.racetozero.net
http ://tinyurl.com/3zdrfc
http ://tinyurl.com/534umo

Génération automatique d'exploit à partir de patchs

L'angoisse

- Un groupe de Carnegie Mellon University
- Du temps à perdre
- A partir des patches on obtient immédiatement un exploit

La réalité

- Tous les patches ne sont pas concernés
- La démonstration génère un DoS, pas de réelle intrusion.
- Un bon hacker ferait ça mieux.

Source

http ://www.cs.cmu.edu/ dbrumley/pubs/apeg.html

Etudiants : la nouvelle cible du phishing

Le paysage du spam évolue

- Les méthodes antispams "noires" sont de moins en moins efficaces
- Des listes blanches se constituent
- Problème pour les pirates : comment passer dans ces listes blanches ?

La solution :

- Passer les mails par des serveurs en liste blanche
- Donc utiliser des comptes valides
- Donc faire du phishing sur des étudiants (US d'abord, Français maintenant)

Source

http ://www.securityfocus.com/news/11504

Les DNS de certains FAI peuvent mentir

Certains FAI souhaitent concurrencer verisign dans le mensonge technologique

- Leur DNS résout "marketinguement" les noms qui n'existent pas
- exemple : fdjsqfjsdm.univ-tlse1.fr pointe sur une page publicitaire

Problème

- Ces pages publicitaires sont parfois sujettes au XSS
- Le domaine étant univ-tlse1.fr, on fournit le cookie
- et aucune solution....

Source

http ://tinyurl.com/5gs6an

Que faire quand on perd un MD5 ?

Petit site rigolo pour retrouver sa clé MD5

- http ://www.authsecu.com/decrypter-dechiffrer-cracker-hash-md5/decrypter-dechiffrer-cracker-hash-md5.php
- Résultat immédiat
- Mais ne marche que si on n'utilise pas de salt.....

- Tests d'intrusions : collecte d'informations, méthodologies et études de cas

Société ITrust