RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 22 Septembre 2009

Webmail : trop facile

100 € pour pirater un compte webmail (gmail, hotmail, etc.)

- des propositions de piratage pullullent,
- apparemment de simples urls sur des sites de fausses bannières.

Alors que google est faillible

- "débordement" de comptes dans google apps,
- université Américaine touchée,
- documents privés visibles sur Google Search,
- problème limité (dixit google).

La faille SMB V2

Faille découverte en septembre 2009.

- porte sur tous les windows (y compris Vista SP1),
- exploitable à distance,
- pas besoin d'authentification
- prise de contrôle complète,
- plugin intégré dans metasploit,
- pas de correctif (patch tuesday ?).

Solutions :

- désactivation du SMB v2 (outil fourni par Microsoft)

La BBox est piratable

Faille récente sur la Bouygues Box.

- Génération de la clé WPA/WPA2 problématique,
- lien entre le SSID "Bbox-1234AB" et la clé,
- Outil disponible (BTHHkeygen).

Solutions :

- Générer une clé WPA,
- pas de solution industrielle pour l'instant.

Infiltrating a botnet

- Interview d'un hacker par un chercheur de chez CISCO,
- chat IRC,
- quelques informations intéressantes (prix, utilisation, etc.)
- hacker très zen.

IETF Draft for Remediation of Bots in ISP Networks

- Tentative de "normalisation" de la lutte Anti Bots,
- A destination des FAI,
- Comment détecter ?
- Comment prévenir ?
- Comment désinfecter ?
- Sans doute éternel draft.

Sujets du jour

- La déclinaison de l'ANSI/TIA 942 (standard de spécification des espaces de télécommunications dans les data centers) aux exigences de sécurité.

  M. Jean-Pierre Yché.

- Les aspects juridiques du scan et des tests d'intrusion. Le droit en matière de scan et tests d'intrusion sera rappelé, et illustré par diverses situations rencontrées par ITrust.

  M. Yoann Garot (ITrust).