RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 18 Novembre 2008

Le mois des ISP bulletproof

Sale temps pour les ISP BulletProof, après la migration du RBN vers la chine :

- Fermeture de Intercage (Californie) alias Atrivo [1]
  - Le 20 septembre 2008
  - Chute nette,
  - Mais reprise très rapide (quelques jours)
- Fermeture de McColo [2]
  - Les spammeurs éjectés de Intercage se sont réfugiés chez McColo
  - Chute spectaculaire des spams (50%)
  - Arrêt très net des botnets srizbi et Mega-D

[1] http://www.spamcop.net
[2] http://www.mxlogic.com

Josh randall en short sur Internet

La société express scripts (protection santé) [3]

- se fait pirater des informations confidentielles
- reçoit les informations complètes de 75 patients
- avec une demande de rançon

Réaction ?

- remboursera tout frais associé à ce piratage
- met une prime de 1 million de dollar sur la tête des hackers

[3] http://www.securityfocus.com/brief/854

Pour le WiFi la sécurité c'est WEP WPA WPA2

Après WEP (mais qui l'utilise encore ?), WPA (mais aussi certaines versions de WPA2) et sa rotation de clés TKIP est malmenée. [4] et [5]

- 2 chercheurs trouvent une faille à TKIP
- permet de déchiffrer des trames vers la station
- au rythme de 1 octet par minute
- et dans une même période d'association

Ce n'est pas le pérou, mais c'est sans doute le début de la fin pour TKIP. Conclusion : CCMP/AES

[4] http://www.securityfocus.com/news/11537
[5] http://sid.rstack.org/blog/index.php/305-des-fameuses-faiblesse-de-tkip

On va tous mourir ! ! !

C'est l'année des annonces de la fin du monde.

- Dan Kaminsky et sa faille DNS : réelle mais quel boucan !
- Robert E. Lee et Jack C. Louis et la super faille TCP : oui / non / phil barney ?
- Les attaques sur les bugs CPU
- etc.

La sécurité et le marketing se marient bien... Mais pour le bien de qui ?

Averell fait des patches

Concours entre les firmes : laquelle tiendra le plus longtemps pour combler un trou de sécurité ? [6]

- Adobe ? 10 mois
- Oracle ? 889 jours

And the winner is ?

- Microsoft avec 12 ans (faille authentification SMB)

[6] http://sid.rstack.org/blog/index.php/306-a-tout-seigneur-tout-honneur

Tempest sur un clavier : et hop sans keylogger

A combien de mètres porte les radiations électromagnétiques de mon clavier ?

- On connaissait le 50 mètres des claviers wireless de Microsoft
- maintenant 20 mètres pour les claviers filaires
- démonstration : http://lasecwww.epfl.ch/keyboard/

Qui s'est fait réellement piraté aujourdhui ?

Petit site rigolo pour savoir si vos données privées sont dans la nature

- http://datalossdb.org/
- 344,482 2008-11-12 University of Florida College of Dentistry
- ...
- 100,000 2008-11-04 Baylor Health Care System Inc.

Intéressant....

SQLMAP : quand on n'est pas un bon pirate

Outil de test sql injection

- http://sqlmap.sourceforge.net
- Utilisation simple : 1 url avec les paramètres

En mode GET pour obtenir les tables

sqlmap -u
"http ://appliweb.univ-tlse1.fr/stages/get_stage.php ?id=1" –tables

- fait du "blind SQL injection"
- moi aussi je suis un hacker de vrai de vrai....

Pour ceux qui ne savent pas faire de l'intrusion, mais veulent se faire peur

- Que font les ESCI du SRPJ de Toulouse
  Commandant Yves Le Hir
- La norme ISO 27001
  Alexandra VAGNER/Laurent PELUD.