RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 8 Novembre 2011

Il court, il court le hacker

Il court, il court le hacker

Il est passé par ici

- Areva se fait pirater
- Depuis plus de 2 ans
- Au bout de 10 jours d'analyse
- sur un SI international
- "aucune information sensible n'a été dérobée"

Il repassera par là

- PSN (Playstation Network) à nouveau piraté
- seulement 0.1% de ses comptes ==> 93 000
- entre le 7 et le 10 Octobre
- Rappel : le précédent c'était en Avril 2011

DuQu DuQu DuQu

DuQu DuQu DuQu

DuQu : encore une attaque sexy

- Fils de stuxnet (au moins spirituel)
- ciblé réseau SCADA
- communique
  - en HTTP ET HTTPS
  - vers 206.183.111.97 et 77.241.93.160 (HS)
  - avec des .jpg
  - embarque du P2P sur SMB
- keylogger
- un 0day sur word
- s'injecte dans IE et Firefox
- peu répandu

SSL : Sécurité Sous LSD ?

Sécurité Sous LSD ?

SSL

- Diginotar : 531 certificats frauduleux
- BEAST : TLS 1.0 compromis

SSL : DigiNotar

- ComodoHacker pirate DigiNotar
- Génère 531 certificats (dont *.google.com : utile pour l'Iran)
- Clients gouvernementaux (surtout hollandais)
- Un mois de délai entre détection et réaction
- Une sécurité faible
- Vive "Perspectives"
- PS : DigiNotar n'est plus.

SSL : BEAST

- Faille théorique de SSL connue depuis 2004
- Implémentée par Juliano Rizzo et Thai Duong
- Ne concerne que TLS 1.0
- Solutions ?
  - TLS 1.1 et TLS 1.2 ne sont pas vulnérables
  - mais beaucoup de navigateurs de font pas du TLS 1.1
  - les serveurs refusent souvent le TLS 1.1
  - la faille n'est pas massivement exploitable

Réf : http://www.bortzmeyer.org/beast-tls.html

TOR : les oignons font pleurer

TOR : les oignons font pleurer

TOR : les oignons font pleurer

- TOR : réseau de proxy
- The Onion Router
- Cassé par l'équipe d'Eric Filiol à l'Esiea
- Phases
  - Inventaire : 5827 machines dont 181 noeuds cachés (tor bridge)
  - Infection des noeuds vulnérables (1 tiers)
  - Saturation des noeuds invulnérables
- Tor ne semble pas avoir été contacté et conteste les résultats
  - https://metrics.torproject.org/
- Corrigé par la version 0.2.2.34

Réf : http://pro.01net.com/editorial/544024/des-chercheurs-francais-cassent-le-reseau-danonymisation-tor/

Phishing

Sujets du jour

Présentation de l'outil Ikare

ITrust

Le cycle de protection et de défense de sa marque : le point sur les noms de domaine

M. Miroslav KURDOV, Brev&Sud