RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 21 Avril 2015

Les piratages et attaques

Les piratages et attaques

TV5Monde

- Attaque débute le mercredi 8 avril 22h00
- Attribuée aux djihadistes, mais pas revendiquée par DAESH
- Twitter, Facebook, puis l'infrastructure interne
- Paralysie de toute l'informatique pendant 48h
- Intervention de l'ANSSI
- Gros retentissement médiatique et politique
- Analyses non finalisées mais
  - Mots de passe en clair "visibles" à la TV
  - Utilisation potentielle d'une variante de njRAT (novembre 2012)
  - Piratage d'un serveur quelques semaines avant.
  - Décalage entre la présentation et les informations recueillies. (Firewall dernière générération).
  - Le piratage pourrait en fait avoir été simple.

Thalès

- Mercredi 1er Avril : message du RSSI
- Peu de retentissement médiatique (Le canard, le monde,)
- Passage par les filiales étrangères puis françaises
- Difficile de mettre sur le même plan.

source : le monde informatique

Uber

- Mai 2014, découvert en septembre 2014
- Données sur plus de 50000 chauffeurs américains
- Recrutement du responsable cybersécurité de Facebook

GitHub

- Mai 2014, découvert en septembre 2014
- Visiblement attaqué par le "Great Cannon" chinois
  - Dérivé du Great Firewall
  - Insertion d'un code javascript attaquant 2 projets GitHub
    - https ://github.com/greatfire/ Online Censorship In China
    - https ://github.com/cn-nytimes/ le mirror du NewYork Times

source : http://insight-labs.org/

Piratage de la territoriale

- 85 sites web protégés par F5 BIGIP
- www.xxx.territorial.gouv.fr
- Message clair "Fuck Gouv Fr"

Informations diverses

Informations diverses

Android For Works

- Zone virtuelle chiffrée sur les android
- Destinée aux entreprises
- Utile uniquement pour ICS, JB et KK, car Lollipot l'embarque
- Intégrable dans les outils de gestion MDM (mais avec compte entreprise google)
- Store spécifique "Google Entreprise"

ANSSI donne 12 conseils

- l'ANSSI donne 12 conseils pour les PME
- Didactiques et compréhensibles
- En collaboration avec la CGPME

source : ANSSI

Classement des OS et des applications en vulnérabilités 2014

- IOS et OS/X les plus troués, suivi de Linux, puis des Windows
- IE, Chrome, Firefox, Flash, Java

source : GFI

La CNIL valide le déchiffrement SSL

- Depuis début avril 2015
- Sous certaines conditions (avertissement des employés, limites, etc.)
- Un employeur peut déchiffrer les flux SSL
- Mais
  - le HTTPS Certificate Pinning
  - et sa généralisation avec la RFC 7469

source : CNIL
source : ANSSI
source : OWASP
source : Bortzmeyer

Orange change le mot de passe des livebox

- Le mot de passe admin par défaut change sur les livebox
- Il dépend de la livebox : 8 premiers caractères de la clé de sécurité
- Les mots de passe ont été changés même si ce n'était pas celui par défaut

source : CLUBIC

Netflix en HTTPS

- Avant dernier des grands prestataires à passer en full HTTPS
- Reste encore Amazon

Simda

- Fermeture du Botnet SIMDA
- 800 000 machines en 6 mois sur 190 pays
- Interpol, Microsoft, Kaspersky, TrendMicro

Microsoft Nano server

- Version très allégée de Windows Server, sans GUI
- 92 % de bulletins de sécurité en moins
- 80 % de redémarrages en moins en comparaison à Windows Server

source :Microsoft

Les failles

Les failles

FREAK

- Faille demandée par la NSA depuis 1990, et découverte en mars 2015
- capacité, en position de Man-In-the Middle de descendre le chiffrement
- Passage en clé 512 bit (50€ chez amazon pour casser)
- Navigateurs quasiment tous corrigés
- Serveurs progressivement en cours de correction
- Microsoft aussi touché

source : Wikipedia

Sujets du jour

MM. Benoit Léger et Nicolas Chalanset - Société STELAU

Mécanismes de sécurité des passeports biométriques

M. Gilles SOULET - CNES

Retour d'expérience.