RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Jeudi 31 Mars 2011

Certificats Comodo

Certificats Comodo : Les faits

- L'autorité de certification Comodo se fait compromettre
- La génération des certificats était automatique (DLL) chez InstantSSL

```
public ASCR ()
        {
        this.url = "https://secure.comodo.net/products/";
        this.url_nos = "https://secure.comodo.net/products/";
        this.login = "gtadmin";
        this.password = "TRIMMEDIT";
        this.numberOfTries = 5;
        }
```

- au moins neuf certificats véreux sont émis
  - login.live.com
  - mail.google.com, www.google.com
  - login.skype.com
  - addons.mozilla.org
- 800 mots de passe récupérés
- d'autres AC compromises

Certificats Comodo : Les suppositions

- Le pirate serait iranien
- Il serait seul
- Il aurait agi pour des raisons patriotiques
- Il ne serait pas lié à l'iraniane Cyber Army
- Son nouveau petit nom : ComodoHacker.

Certificats Comodo : Les conséquences

- Les certificats compromis ont été blacklistés
  - dans IE, Firefox, etc,
  - mais par MAJ
- Comodo vérifie désormais les demandes de certificats
- Maintenant, c'est long de les obtenir.

Certificats Comodo : Comment contrer

- Utiliser OCSP (mais il faut que les faux-certificats soient repérés)
  - pour firefox : about :config
  - security.OCSP.require à true
- Utiliser l'extension "perspectives" y compris pour les sites valides !
- Considérer qu'une société qui vend de la sécurité
  - vend d'abord
  - sécurise après... si nécessaire

Plus d'infos :
http://sid.rstack.org/blog/index.php/468-des-vereux-de-comodo

RSA : securid

RSA : securid

- RSA victime d'une APT (Advanced Persistent Threat)
- Le système d'authentification à 2 facteurs SecurID "affaibli"
- Informations sensibles dérobées. Mais lesquelles ?
  - L'algorithme du code ? Il est connu (Cain & Abel)
  - La clé dépendrait d'un algorithme ? apparemment non
  - Base de données avec les clés associée aux numéros de série ?

McAfee : failles web

McAfee : failles web

- Un groupe de hacker (YGN Ethical Hacker)
- Vulnérabilités XSS sur mcafee.com
- McAfee averti
- 1 mois et demi après : il reste des failles
- Les failles sortent en "Full disclosure"

Pour le fun

Les trucs rigolos

- MySQL.com et Sun.com victimes de failles SQL
- NetQin (éditeur de sécurité chinois) fabrique des malwares.
- Les serveurs de la NASA aisément piratables.

Sujets du jour

Nomadisme et sécurité : enjeux et solutions, et cas spécifique des Smartphones

M. Clément SAAD, Pradeo

Il court, il court, le fichier : méthodes d'identification de fichiers connus sur des supports numériques ou paquets réseau.

M. Pierre-Yves Bonnetain, B&A Consultants