Computer Emergency Response Team
Industrie Services Tertiaire

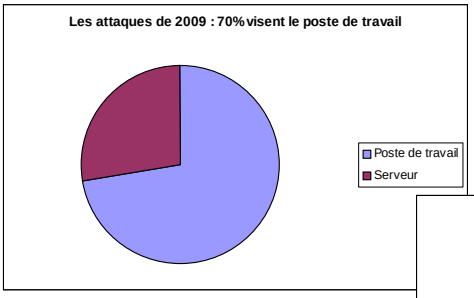
Exemple d'un cas réel d'infection du poste de travail par l'intermédiaire du navigateur

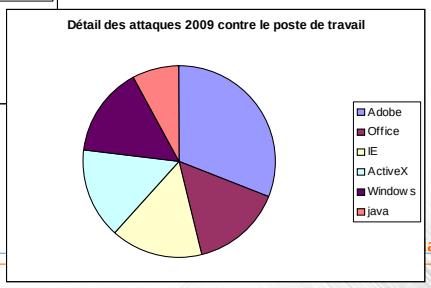
Réunion ReSIST 30/09/2010

Philippe Bourgeois

Bilan Cert-IST 2009 des failles et attaques

- 70 % des situations à risques sont dues à des attaques visant le postes de travail
- Elles utilisent des vulnérabilités dans les logiciels clients (Acrobat Reader, etc…)

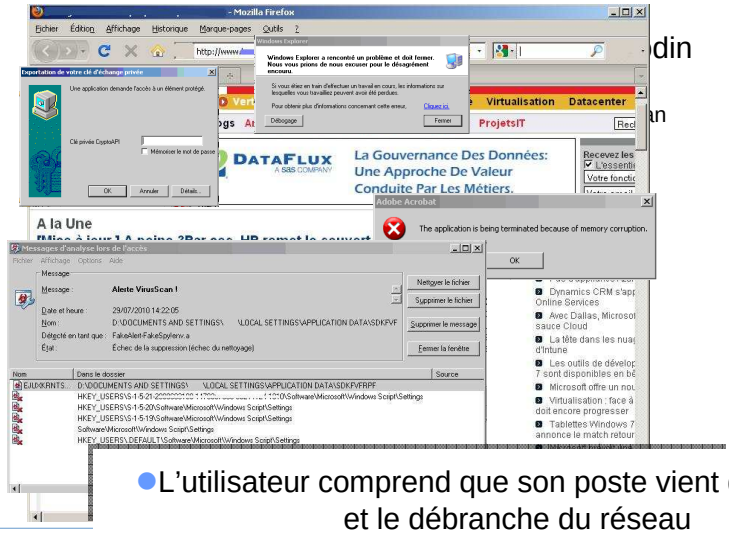




Exemple d'un cas réel d'incident

- Tiré d'un incident traité durant l'été 2010
  - Typique de ce type d'incident
  - Démontre la fragilité du poste de travail
- Le poste visé est un poste en entreprise
  - Protégé par l'infrastructure d'entreprise (Firewall)
  - Equipé d'un anti-virus maintenu à jour
  - Mis à jour régulièrement au niveau OS

L'incident (reconstitution)



- L'utilisateur comprend que son poste vient d'être infecté et le débranche du réseau

Analyse de l'incident

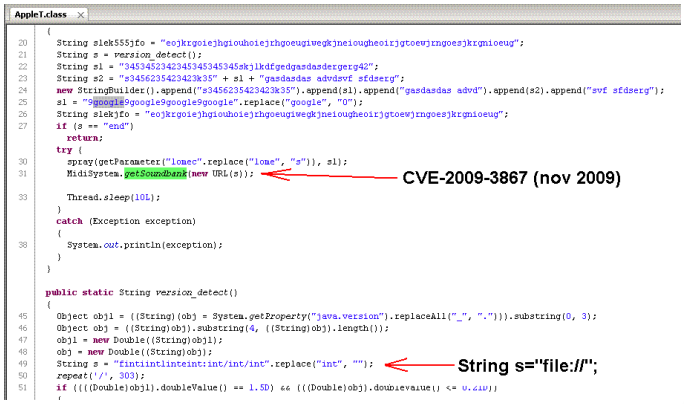
- L'analyse MAC-time du disque montre :
  - Le lancement d'un fichier JAR
    - C:\Documents and Settings\xxx\Local Settings\Temp\ jar_cache4855171583194739268.tmp"
  - L'arrivée de plusieurs exécutables dans « Local Settings\Temp\ »
    - Temp\tmp77373732727.tmp
    - Temp\0.06719136123156277.exe
    - Temp\7397540.exe
    - Temp\tmp77373732727.tmp
    - Temp\3590006.exe
  - Le lancement du malware « SpyEye »
    - C:\WINNT\Prefetch\CLEANSWEEP.EXE-07D4E65B.pf
    - C:\cleansweep.exe\
    - C:\cleansweep.exe\config.bin
  - Arrivée de plusieurs Fichiers PDF
    - \Temp\Acr75DC.tmp, etc…
  - Etc..

Analyse de l'incident

- Autres éléments constatés
  - Vol de données FileZilla
    - Application Data\FileZilla\sitemanager.xm
  - Vol de données MSN
    - Application Data\Microsoft\Windows Live Contacts\{1cf26f-xxxx-520}\DBStore\contacts.edb
  - Envoi de SPAM via le compte Outlook de l'utilisateur
- A propos de SpyEye
  - Apparu en janvier 2010. Se présente comme le challenger de Zeus
  - S'installe dans C:\cleansweep.exe\ (répertoire caché)

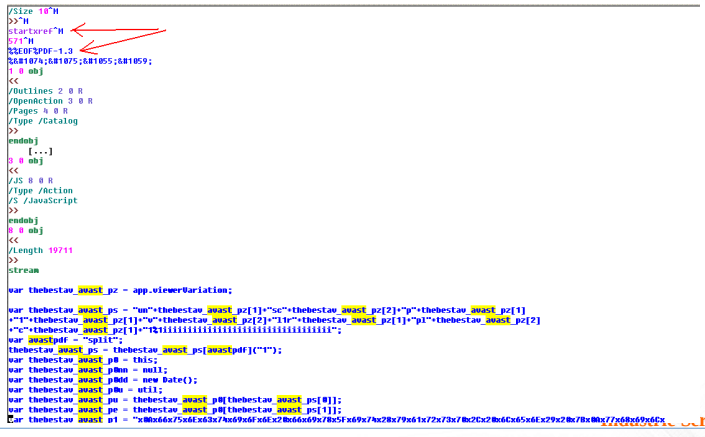
Le fichier JAR malveillant

- Fichier « AppleT.class »
  - Détection par VirusTotal : 1/42 (01/08/2010) puis 6/43 (13/09/2010)



Le fichier PDF malveillant

- Fichier « Acr75DC.pdf »
  - Détection par VirusTotal : 8/42 (01/08/2010) puis 17/43 (13/09/2010)
  - Structure complexe (5 PDF concaténés)



Conclusion de l'incident

- Infection d'un poste pas à jour via JAVA-JRE
  - Vecteur très efficace car Java est :
    - Multi-navigateurs
    - Souvent requis (exemples : VPN-SSL, applications d'entreprises, etc.),
    - Indispensable (selon les versions) pour des applications "Métiers"
    - Difficile à maintenir (sur certains parc)
- L'infection déclenche une cascade d'action malveillantes
  - Vol de mots de passe et de comptes
  - Spam
  - Escroquerie vis-à-vis de l'utilisateur (faux anti-virus)
  - Espionnage des sessions utilisateurs (vol de données bancaires)
- L'origine de l'infection n'a pas été identifiée
  - Bandeau publicitaire malveillant ?
  - Redirigeant l'internaute vers un Exploit-kit ? (exemple : Phoenix)

Computer Emergency Response Team
Industrie Services Tertiaire

Solutions la sécurité de la navigation web

Solutions ?

- Maintenir le poste de travail à jour !
  - Nota : Pour vérifier la version du JRE sur un poste Windows :
    - Panneau de configuration / Java : A propos de
- Utiliser des greffons pour renforcer la sécurité
  - Par exemple : Adblock Plus & NoScript
- Virtualiser le navigateur web
  - Sur le poste de travail
    - « Secure Browser » (Dell Kace) : Firefox dans un bac à sable.
    - Etc …
  - Dans une DMZ de l'entreprise :
    - « Virtual Browser » (CommonIT.com) : Un client léger pour accéder à des applications s'exécutant dans un environnement virtualisé

Industrie Services Tertiaire

Q & R ?

Fin de la présentation

Industrie Services Tertiaire