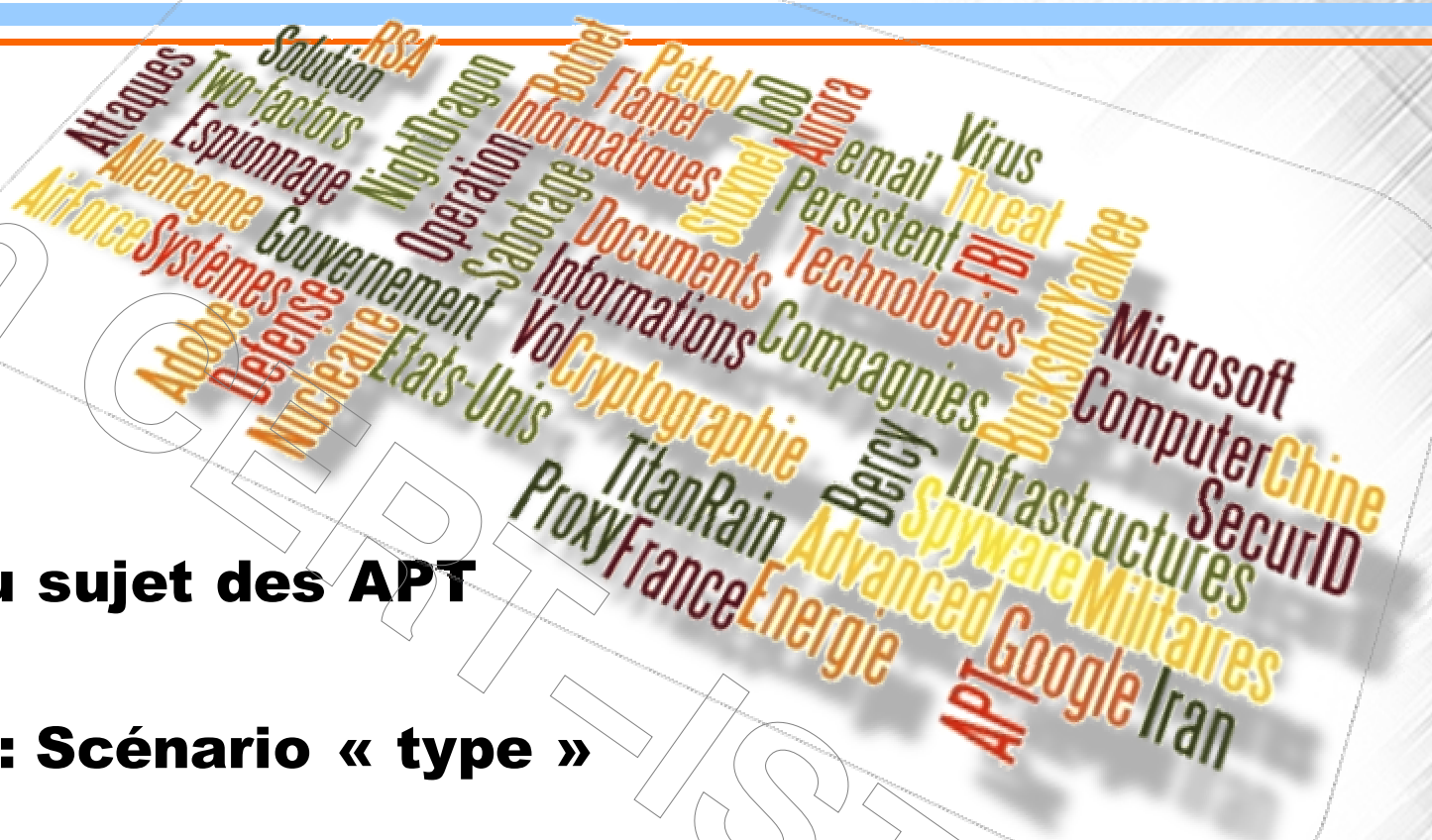
Retour d'expérience sur les investigations d'attaques APT

David TRESGOTS

13 juin 2012
Forum Cert-IST 2012

Industrie Services Tertiaire

Sommaire



- **Petits rappels au sujet des APT**
  - **Attaque APT : Scénario « type »**
    - **Investigation d'une APT : du scénario au terrain**
      - **« Back to Basics » : du retour de terrain aux fondamentaux**

Petits rappels au sujet des APT

Advanced Persistent Threat

- **Attaque par Infiltration préparée et « scénarisée »**
  - Non-improvisée
  - Plusieurs phases :
    - Reconnaissance, Intelligence informationnelle, Ingénierie Sociale…
    - Stratégique (cibles de repli : humaines et informatiques,…)
- **Attaque dite « avancée » mettant en œuvre de nombreuses techniques d'attaques « basiques » connues**
  - *Phishing, injection SQL, XSS*
  - Exploitant très souvent des vulnérabilités classiques non corrigées (Java, PDF, etc.).
- **Attaque conçue pour contourner les moyens de protections actuels**
  - *Périmétriques (firewal, proxies), du poste de travail (antivirus, ASLR, DEP),…*

- **Attaque visant à rester le plus longtemps possible dans le SI**
  - Plusieurs mois / Plusieurs années !
  - Furtive (Under the Radar)
- Sa 1ère cible est souvent l'Humain !
  - Spear phishing, usurpation d'email, clé USB « égarée » dans un parking, …

Industrie Services Tertiaire

Une réalité, pas une nouveauté !

Industrie Services Tertiaire

Un phénomène qui a changé d'échelle, car …

La question n'est plus de savoir

« Si on sera attaqué »

mais plutôt de savoir

« Quand on sera attaqué. »

« Si ce n'est pas déjà le cas. »

Nos constats


Bilan Cert-IST 2011 des failles et attaques

1) Introduction

Comme chaque année, le Cert-IST fait un bilan de l'année écoulée. L'objectif est de retracer les événements marquants de 2011 de façon à mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger.

Dans un premier temps, nous faisons un bilan des principales attaques survenues au cours de l'année (cf. chapitre 2).

Ensuite, nous identifions les événements les plus marquants de l'année et analysons la t
pourraient influencer le domaine de la sécurité dans les années à venir (cf. chapitre 3).

- Une tendance en constante augmentation depuis 2010
  - cf. Bilans Cert-IST 2010, 2011
- Pas spécifique aux « grosses » organisations ou Etats
- Souvent déclenchées sous forme de « campagnes sectorielles »
  - Energie, Aéronautique, Telco, Spatiale, IT, Armement, e-Commerce…
- Souvent découvertes fortuitement et tardivement

Industrie Services Tertiaire

Motivations et Objectifs ?

- Quelques soient les motivations…
  - Espionnage
    - industriel, concurrentiel, stratégique, militaire …
  - Déstabilisation
    - commerciale, politique, géopolitique
  - Escroquerie, détournement d'argent
  - Propagande idéologique (à défaut de trouver une vrai cause)
  - …

- Les objectifs sont les mêmes :
  - Reconnaissance de l'écosystème de la cible (Humain, Informationnel, etc.)
    - Gangrène du SI
  - *Infiltration des cibles*
  - *Surveillance des échanges (emails, ToIP, données, etc.)*
    - *Collecte, tri, compression des informations*
  - *Exfiltration des données*
  - *Persistance et Furtivité*
    - *Réactions du pirate aux mesures de protection (cibles de replis…). Il a le temps.*

Attaque APT : Scénario « type »

Industrie Services Tertiaire

Reconnaissance et intelligence informationnelle

- Identification de l'écosystème de la cible
  - Entreprise / Organisation, Activité, Clients
  - Employés

    - recherches d'informations sur les personnes ciblées (réseaux sociaux, Internet, publications, centres d'intérêts, …)
  - Système d'information
  - Visibilité sur Internet

    - site web, nom de domaine, WhoIS, DNS, …

- Ingénierie Sociale
  - Emails / Appels téléphoniques
  - Cartographie des acteurs et des cibles potentielles
    - Organigramme, hiérarchie, contacts importants, etc.
  - …

Tentative de compromission

- Les vecteurs d'attaques sont nombreux
  - cf. présentation Cert-IST du Forum de l'an dernier

- Le plus commun est la réception d'un email avec une pièce jointe piégée
  - Sur un centre d'intérêt (ou pas)
  - Envoyé à une cible ou un groupe de destinataires ciblés
  - Voire du SPAM dans le cas de campagne « tout azimut »
    - Antagoniste avec le but d'une APT qui est d'être furtive, mais ça c'est vu…

- Ou bien
  - par échange de fichiers/liens via les réseaux sociaux, les chats, les forums…

- Ou encore
  - Via des supports amovibles piégés

Compromission

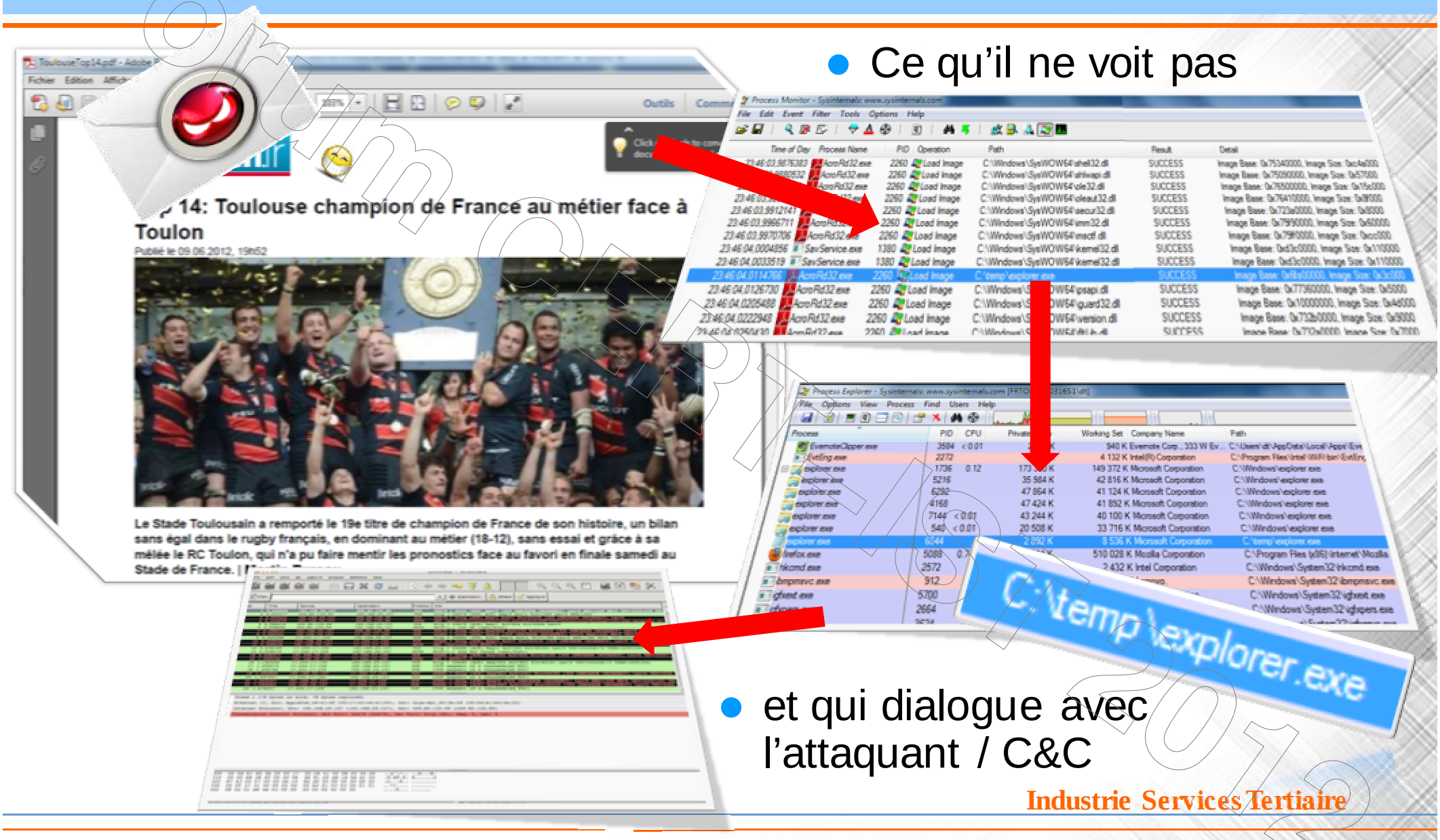
- La victime
  - Affiche la pièce jointe reçue (souvent un PDF, mais on a vu des .SCR ou EXE !)
  - Ouvre un document trouvé sur une clé USB (par exemple)
  - Clique, clique, clique sur une URL de l'email reçu !
  - etc.

- ~~En général,~~ Très souvent, il ne se passe rien !!!

  … de visible

  - Un exemple
    - L'exemple qui suit est fictif mais caractérise des cas traités par le Cert-IST.
    - Ceci n'est qu'UN exemple ! L'imagination est sans limite (faux fichiers d'imprimante, faux billets d'avion, etc…)
    - D'autres vecteurs peuvent aussi être utilisés.

Exemple : Un utilisateur ouvre un document de travail transmis par email



- Ce qu'il ne voit pas
- et qui dialogue avec l'attaquant / C&C

Industrie Services Tertiaire

Post-Compromission d'une cible

- Installation d'un arsenal d'outils par l'attaquant
  - Outils de type RAT (Remote Administration Tool)
  - Outils de récupération des condensats (hash) des mots de passe
  - Outils de collecte d'informations (énumération des ressources, etc.)
  - Outils de récupération des emails (ex. PST, …)
  - Outils de compression
  - Outils de relayage de flux
  - …

- Installation de Backdoors
  - Le pirate s'installe, et s'organise pour revenir.
  - A défaut de revenir, il fait peut faire en sorte que les données viennent à lui (ex. botnet).
  - …

Post-Compromission : Nouvelles cibles du SI

- Compromission de nouveaux Comptes / Systèmes
  - Attaque des comptes locaux (brute force, etc.), nomades (AD)
  - Acquisition/Escalade de privilèges (attaque « Pass-The-Hash »)
  - Enumération des ressources accessibles
  - Découverte de nouvelles cibles
  - … compromission de celles-ci

- Persistance dans les systèmes du SI
  - Lancement au démarrage, machines de rebond, etc.
  - Le pirate n'agit que rarement dans l'urgence

- Reconnaissance de l'écosystème cible compromis
  - Recherche de nouvelles cibles

Recueil et exfiltration des données

- Quête du Graal
  - Accès utilisateurs (login)
  - Documents sensibles / confidentiels
  - Emails stratégiques de l'Exécutif, des managers, de la R&D, des commerciaux
  - Des codes sources, de plans, etc…

- Exfiltration du butin via
  - Covert channels
  - Botnet
  - Emails
  - Partage en ligne (Dropbox, etc…)
  - Services FTP, …
  - etc…

… Chiffré, bien sûr !

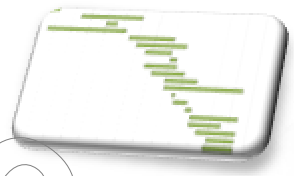
Investigation d'une APT : du scénario au terrain

Industrie Services Tertiaire

Sur le terrain…

- L'investigation commence toujours comme ça
  - Trouver une aiguille dans une botte de foin
- Ce qu'il faut éviter ?
  - Le mode « Panic »
    - La machine a café n'a probablement pas été compromise…
    - Investiguer tout est n'importe quoi devient vite ingérable surtout si l'incident date !!!

- Par où commencer ?
  - Réunir et coordonner les acteurs
    - Equipes SSI, Métiers, Décideurs, Investigation, service de Communication (si nécessaire)
  - Reconstruire la Timeline des évènements
  - Prendre du recul sur l'incident



- Interroger les victimes
  - Pas toujours possible
  - Mais souvent sources de précieuses informations

Industrie Services Tertiaire

L'investigation : des problèmes, des difficultés et des Questions aussi

- Les responsables du SI savent-ils encore … ?
  - Trouver les bonnes sauvegardes
  - Relire les supports magnétiques ?
  - Réinstaller d'anciens serveurs Oracle, BD, autres
  - Trouver la bonne connectique des disques
  - Accéder / extraire / exploiter les logs (s'il y en a !)
  - Synchroniser les évènements
  - …

- mais aussi … ?
  - Reconstruire le réseau à des dates précises ?
  - Quid des accès VPN ?

- Savent-ils aussi… ?
  - Gérer les volumes de données d'aujourd'hui
  - Extraire des données du Cloud
  - Extraire des systèmes compromis du Cloud
  - …

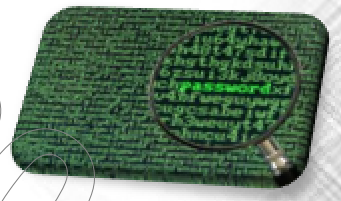
Industrie Services Tertiaire

Analyse Forensic : de la méthode et des choix, et de la chance aussi !

- Adapter la réponse Forensic au contexte de l'incident.
  - C'est une affaire de compromis « Comprendre l'incident » vs « Retour opérationnel ». Et de temps…

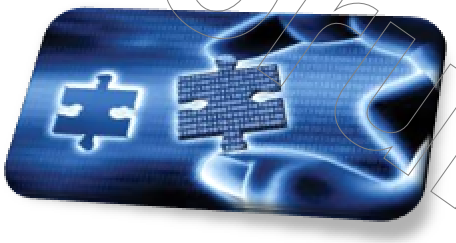
- Mettre en quarantaine les systèmes suspects
  - Pas toujours possible
    - Machines opérationnelles, etc.
  - Souvent trop tard
    - Si l'incident date, l'état du poste a évolué.
    - Les administrateurs sont passés par là.
    - L'utilisateur a joué les apprentis sorciers.
  - Pas toujours souhaitable
    - Capture réseau (dialogue avec un C&C), …

- Chercher des fichiers inhabituels dans des endroits inhabituels ?
  - RAR.EXE, GETMAIL.EXE, CRACKME.EXE, READPST.EXE… dans %System%/system32 ?
  - Regarder les processus qui tournent et leurs privilèges
    Tiens « LSASSSS.EXE » en cours d'exécution dans le gestionnaire de processus !! (cela ressemble au vrai !)
  - Les connexions en cours aussi…
  - Mais les systèmes d'exploitation sont si complexes que l'on peut s'y perdre (ex. analyser l'Active Directory).



Industrie Services Tertiaire

Mode opératoire : Chercher, comprendre les motivations de l'attaquant



- Il manque souvent des pièces du puzzle.

- Découvrir le modus operandi de l'exfiltration des données reste complexe.
  - Le pirate a souvent énormément d'avance. C'est frustrant.
    - Des mois, des années. Sa posture évolue.
    - Il a le temps.
    - Le pirate laisse généralement très peu de choses.
  - L'analyse Forensic est donc un travail de fourmis chronophage.
  - La moindre altération des données peut remettre en cause toutes les hypothèses d'analyse.

Comment améliorer les choses ?

« Back to Basics » : du retour de terrain aux fondamentaux

Industrie Services Tertiaire

Renforcer les fondamentaux

- Maintenir à jour les systèmes et équipements
  - Suivre l'évolution des vulnérabilités et menaces.
  - C'est l'un des rôles du Cert-IST.

- Superviser son infrastructure (SOC, SIEM, etc.)
  - Journaliser, Journaliser, Journaliser…
    - ✓ Analyser les besoins de journalisation
    - ✓ Journaliser n'est pas QUE l'affaire des experts sécurité. Il faut impliquer le METIER, les projets. Cela ne s'improvise ~~pas~~ plus.
  - Surveiller les évènements
    - ✓ « Classiques » (scans réseaux, de ressources, etc.)
    - ✓ Mais aussi les signaux faibles (évènements souvent anodins)

- Sensibiliser les utilisateurs, le HelpDesk, les VIP
  - Rappeler les règles SSI et les bonnes pratiques en matière de sécurité
  - Mener des **campagnes internes de tests de phishing**
  - Faciliter le **signalement d'évènements IT suspects**

Industrie Services Tertiaire

Des questions : Mais pas de réponses toutes faîtes

- Les utilisateurs ont-ils réellement besoin d'être administrateur de leur poste de travail ?

- Les mots de passe sont ils robustes ?
  - Rappeler les bonnes pratiques
  - Vérifier la solidité de mots de passe, leur non réutilisation…
  - Pas évident

- JavaScript est-il réellement nécessaire dans votre lecteur PDF ?

- Les utilisateurs ont-ils réellement besoin de partager des données dans le Cloud ?
  - Dropbox, Google Drive, SkyDrive, SendSpace, …

Industrie Services Tertiaire

La sécurité n'est pas QUE l'affaire des experts sécurité

- Une attaque APT ne doit pas être considéré comme un incident classique de sécurité.
- Reformater un poste, effacer les fichiers suspects n'éradique pas forcément le problème et donne un faux sentiment de sécurité.

- Une compréhension globale de l'incident doit être faite par les responsables et acteurs du SI.
- Une analyse approfondie de la surface du SI affectée doit être faite et doit permettre de définir un plan d'actions cohérent et adapté.
  - Il ne faut rien négliger.
  - Cela sera long et complexe !

Industrie Services Tertiaire

Des Questions ?

Merci pour votre attention