Computer Emergency Response Team
Industrie Services Tertiaire

Evolution des failles et attaques
Bilan de l'année 2011

www.cert-ist.com

Industrie Services Tertiaire

Mars 2012

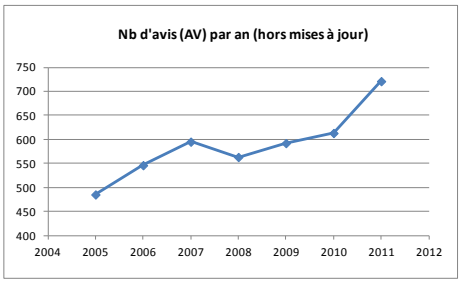
Philippe Bourgeois

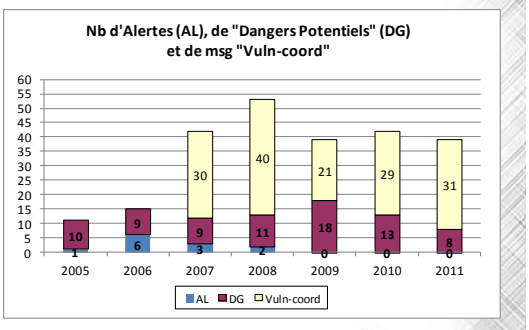
Plan de la présentation

- Présentation du Cert-IST
- Résumé des épisodes précédents
  - Des attaques qui visent le poste de travail
  - Professionnalisation des attaquants et défenseurs
  - Une informatique d'entreprise plus ouverte
- Evénements marquants de 2011
  - Attaques par infiltration (APT)
  - Des réseaux insuffisamment sécurisés
  - Vulnérabilité SCADA
  - Cyber-activisme
  - Sécurité des smartphones
- Conclusions
  - Le début d'un cycle de renforcement de la sécurité

Présentation du Cert-IST

- Centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises
  - Computer Emergency Response Team – Industrie Service & Tertiaire
- Veille sur les vulnérabilités et le menaces





- Aide à la résolution d'incidents de sécurité

Evolution des attaques

- En 2000 : des infections massives saturent les réseaux (CodeRed, Sasser, Slammer, etc…)
- Depuis, la menace pour l'entreprise est devenue plus souterraine
  - Apparition des Fuzzers pour la recherche des failles
  - Apparition du phénomène des 0-days et du marché noir des failles
  - Arrivée de la cyber-criminalité avec des attaques visant principalement le grand public (phishing, vol de données bancaires et escroqueries).
- Aujourd'hui la menace se tourne vers l'entreprise
  - Phénomène des attaques APT
  - Attaque Stuxnet attaquant les systèmes SCADA
  - Cyber-hacktivisme

Computer Emergency Response Team
Industrie Services Tertiaire

Résumé des épisodes précédents

Des attaques qui visent le poste de travail

- Infection de l'internaute lors de sa navigation Internet
  - Déclenchée automatiquement lors de la visite d'un site web infecté (Drive-by download attack)
  - Utilise des vulnérabilités dans les logiciels applicatifs plutôt que dans Windows (JRE, PDF Reader, publicité flash piégée, logiciels Office, navigateur web)
  - Les outils d'attaque sont sophistiqués (Exploit Kits : Mpack, IcePack, Phoenix, etc…) et les attaques discrètes
  - De nombreux sites web relaient involontairement les attaques (ils sont compromis)

  Naviguer sur Internet avec un ordinateur non à jour est devenu TRES dangereux.

- Les défenses actuelles restent d'une efficacité limitées
  - Les antivirus ont une efficacité limité
  - Les malwares utilisent des flux autorisés (flux HTTP sortants)
  - Et savent se dissimuler pour survivre sur le système infecté (rootkit)

Professionnalisation des attaquants et des défenseurs

- Des logiciels d'attaque sophistiqués
  - Stormworm (2007), Conficker (2009), Zeus (et SpyEye) (2009)
  - Botnets et infrastructure d'attaque (fast-flux, Bullet-proof hosting)
  - Le cyber-crime est une industrie : marché des failles, développement structuré, etc…
- Des défenseurs qui se structurent également
  - Collaborations à large échelle : Technique et judiciaire
    - Exemple : Démantélement de Kneber, Waledac, Mariposa (2010)
  - Renforcement du cadre légal
    - Renforcement des lois, les forces judiciaires acquièrent des capacités offensives
  - Les constructeurs ont également progressé
    - Processus de gestion des vulnérabilités, déploiement de correctifs complexes
- Globalement le paysage se durcie et se professionnalise
  - Des attaquants et des défenseurs de plus en plus aguerris
  - L'entreprise doit également continuer à améliorer ses processus et sa capacité à maitriser le risque d'attaque.

Une informatique d'entreprise plus ouverte

- Dans le même temps le paysage s'est complexifié
  - Web 2.0, réseaux sociaux (induit de nouveaux risques)
  - AAA : Anywhere, Anytime, Anyway (nomadisme, évolution des usages)
  - Smartphone, tablettes, BYOD
  - Cloud

Computer Emergency Response Team
Industrie Services Tertiaire

Evénements marquants de 2011

Attaques par infiltration (APT) 1/3

- APT : Advanced Persistent Threat
  - Attaques par infiltration : compromettre une cible et y rester pour agir silencieusement
  - Scénario type :
    - Envoi d'un email avec une pièce jointe piégée : compromission d'un poste (installation d'un bot ou d'un RAT sur le poste infecté)
    - Contrôle à distance du bot par le pirate : Exploration du poste et du réseau
    - Décision de nouvelles actions : attaques internes de l'entreprise
    - Jusqu'à atteindre l'objectif visé : espionnage industriel
  - Exemples 2011 :
    - Ministère des finances (Bercy)
    - RSA et Lockeed Martin (USA), Areva (France) , Mitsubishi Heavy Industries (Japon), etc…
    - Opération « Night Dragon » , opération « Lurid », opération « Nitro »
- Elles ne datent pas de 2011
  - Acronyme popularisé en janvier 2010 (Attaque « Aurora » contre Google)
  - Depuis 2005 (au moins) des attaques ciblées contre les états ou les industries sont identifiées (ex: Titan Rain, Michaël Haephrati, etc…)
  - MAIS le phénomène a changé d'échelle : la question n'est plus « Serez vous attaqués ? » mais « Quand serez vous attaqués ? » et « Comment réagirez vous ? »

Industrie Services Tertiaire

Attaques par infiltration (APT) 2/3

- Exemple RSA
  - Le 18/03/2011 RSA annonce qu'elle a été attaquée
    - Un fichier EXCEL piégé ("2011 Recruitment plan.xls") contient un Flash malicieux (attaque 0-day via la vulnérabilité CVE-2011-0609)
    - Installation d'un RAT de type « Poison Ivy » sur les postes compromis
    - Récupération des mots de passe d'utilisateurs et d'administrateurs
    - Accès aux serveurs de l'entreprise
    - Vol de donnée sur les tokens SecurID vendus par RSA
    - Exfiltration des données volées via FTP
  - Le 28/05/2011 tentatives d'attaque de Lockeed Martin au moyen des données RSA volées.

- Nota :
  - 12/01/2012 : « alienvault.com » découvre une variante de « Sykipot » conçue pour espionner les lecteurs de cartes « ActivIdentity »

- <u>Ces attaques sont construites et déterminées</u>

Attaques par infiltration (APT) 3/3

- Les attaques par infiltration sont l'événement majeur de 2011
  - 3 axes d'action pour y répondre
    - Maintien à jour des équipements (en particulier le poste de travail)
    - Développer la capacité de détecter les postes compromis le plus tôt possible
    - Renforcer la sécurité interne de l'entreprise (que se passe-t-il si un poste interne est compromis)

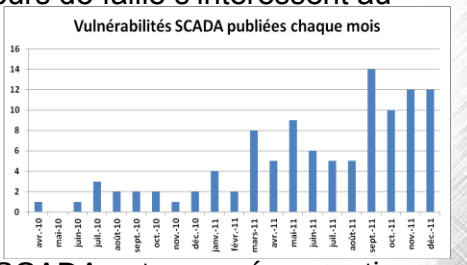
  Nota : le maillon humain est souvent le point faible.

Des réseaux insuffisamment sécurisés

- Exemple de sites « de confiance » attaqués en 2011
  - RSA (mars 2011)
  - DigiNotar (juillet 2011)
  - SourceForge.net (janvier 2011)
  - Wordpress.com (avril 2011)
  - Kernel.org (août 2011)
  - MySQL.com (septembre 2011)
- Comment ces attaques sont-elles possibles ?
  - Le facteur humain
  - La faiblesse des architectures sécurités mises en place
  - Des attaquants plus audacieux

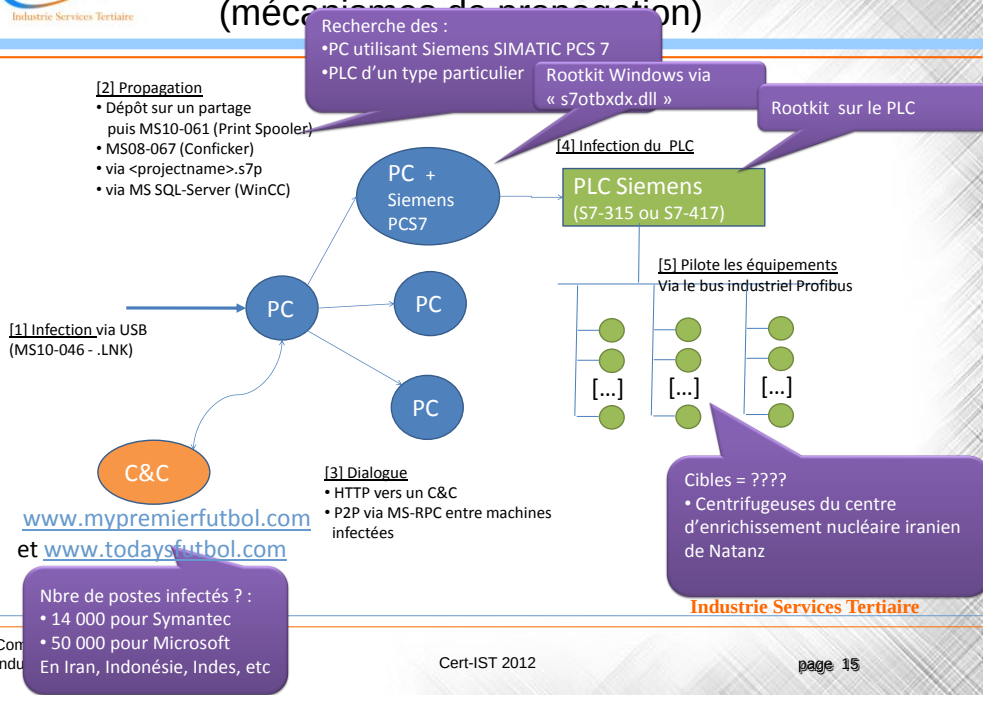
Vulnérabilité SCADA

- SCADA = Supervisory Control And Data Acquisition
  - Ce terme est employé au sens large pour désigner l'informatique industrielle
- L'année 2010 a été l'année de la découverte de STUXNET
  - Ver probablement conçu pour détruire les centrifugeuses iraniennes d'enrichissement nucléaire.
- 2011 est l'année ou les chercheurs de faille s'intéressent au SCADA
  - Luigi Auriemma publie 54 vulnérabilités
  - Gleg publie son pack « Agora SCADA+ exploit pack »



- La sécurisation des systèmes SCADA est une préoccupation majeure

Illustration du cas Stuxnet (mécanismes de propagation)



Cyber-activisme = Hacktivisme

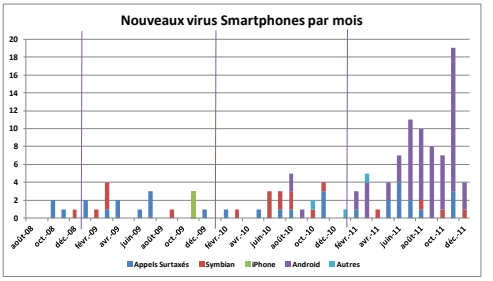
- 2011 : Les cyber-attaques deviennent un outil de protestation
  - Décembre 2010 – Les Anonymous prennent la défense de WikiLeak
    - DDOS contre Paypal, Visa, MasterCard (et Amazon)
  - Mai et juin 2011 – LulzSec s'amuse à pirater des sites de renom

Nota : Mouvements multi-formes difficiles à cerner, allant du jeu à l'action politique.

- Faut-il craindre les Hacktivistes ?
  - De réels succès
  - Des proies faciles et mal protégées
  - Il faut prendre en compte ce risque et préparer un plan de réponse
    - Nos sites web sont-ils piratables ?
    - Quelle communication en cas d'attaque DDOS ?

Sécurité des smartphones

- Augmentation importante du nombre d'applications malveillantes (surtout pour Android)



- Quelques malwares avec des capacités techniques étonnantes
  - ZitMO (Zeus in the Mobile) , SpitMO (SpyEye in the Mobile) pour capturer les SMS d'authentification 2-facteurs.
- L'escroquerie numéro 1 reste les appels vers des numéros surtaxés

Industrie Services Tertiaire

Sécurité des smartphones (2/2)

- Les périphériques mobiles introduisent de nouveaux risques
  - Ils contiennent des données sensibles
  - Ils sont souvent non protégés
  - Il peut être difficile d'imposer des règles de sécurité
    - Phénomène du BYOD : Bring Your Own Device
- La priorité est à la prise de conscience des dangers
  - Sensibiliser les utilisateurs, sensibilisation des entreprise
  - Protéger les données sensibles stockées sur ces périphériques
    - Mise en place d'outils de gestion de flotte (Mobile Devices Management)
    - Procédures d'effacement (à distance et avant recyclage)
    - Chiffrement lorsque c'est possible
    - Ne plus stocker de données d'entreprise sur le périphérique ?

Industrie Services Tertiaire

Conclusions

Industrie Services Tertiaire

Conclusions (1/2)

- Les attaques par infiltration sont l'événement majeur de 2011
  - 3 axes d'action pour y répondre
    - Maintien à jour des équipements (en particulier le poste de travail)
    - Développer la capacité de détecter les postes compromis le plus tôt possible
    - Renforcer la sécurité interne de l'entreprise (que se passe-t-il si un poste interne est compromis)

    Nota : le maillon humain est souvent le point faible.
  - Elles sont la suite « logique » de la professionnalisation des attaques
    - Avant 2000 : les vers → Amusement, expérimentation
    - 2005 : Botnets → Criminalisation et profits (DDOS, cyber-escrocs)
    - 2011 : Infiltrations → Espionnage, Attaques politiques, cyber-armes
- Elles marquent le début d'un nouveau cycle de sécurisation ?

Conclusions (2/2)

- Les autres tendances 2011 sont des menaces en devenir
  - Sécurité SCADA
  - Sécurité Smartphone
  - Cyber-activisme

Nota : Le bilan 2011 complet est disponible sur le site Cert-IST :

http://www.cert-ist.com/fra/news/bilan2011/