Computer Emergency Response Team
Industrie Services Tertiaire

Panorama des failles et attaques
Bilan de l'année 2013

www.cert-ist.com

Industrie Services Tertiaire

Avril 2014

Philippe Bourgeois

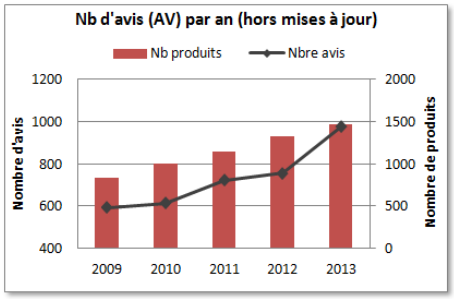
Plan de la présentation

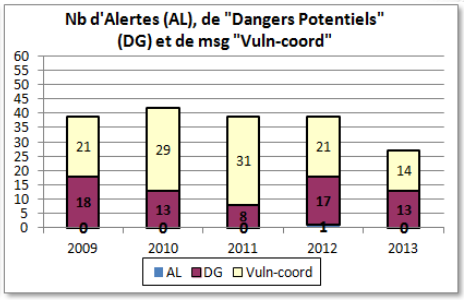
- Présentation du Cert-IST
- Paysage actuel de la menace
  - Profil type des attaquants et leurs motivations
  - Evolution de la menace depuis 2010
- Les événements marquants de 2013
  - L'affaire Snowden change la perception du risque « cyber-espionnage »,
  - Les attaques matérielles une menace désormais réelle,
  - La sécurité offensive de plus en plus présente.
- Les attaques visant les entreprises : comment se protéger ?
  - Les attaques par infiltration (APT), principalement réalisées par les cyber-espions,
  - Les attaques opportunistes, le plus souvent le fait d'hacktivistes,
  - Les attaques visant les systèmes industriels (les SCADA).
- Quelques vulnérabilités remarquables
- Conclusions

Industrie Services Tertiaire

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

Les chiffres de 2013

- Avis de sécurités en 2013
  - 976 avis (et 2700 mises à jour) : Forte augmentation en 2013 (+ 29%)
- Les menaces : Pas d'Alerte, et 13 Dangers Potentiels (DG)
  - 6 DG concernent **Windows**, dont 4 pour Internet Explorer,
  - 4 DG sur le JRE de **Java**,
  - 1 DG sur **Adobe Reader**,
  - 1 DG sur le malware **CryptoLocker**,
  - 1 DG sur un système de video-conférence **Cisco TelePresence** System.

Computer Emergency Response Team
Industrie Services Tertiaire

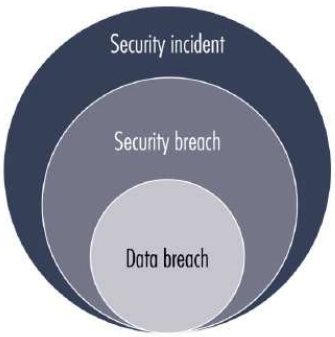
1) Paysage actuelle de la menace

1.1) Profil type des attaquants et leurs motivations

- Attaques par des amateurs
  - Escrocs amateurs : Defacement de sites web, Nigerian scam
  - Hacktivism : Attaques par des Anonymous ou SEA (Syrian Electronic Army)
- Attaques par des professionnels
  - Cyber-criminels visant le grand public (depuis 2005)
    - Spam
    - Botnets
    - Vol de données bancaires
    - Escroquerie visant le particulier (faux antivirus, ransomware)
  - Cyber-espions : Attaques par infiltration (APT)
    - cyber-espionnage ou sabotage

1.1) Profil type des attaquants et leurs motivations

- Quid des attaques internes (Insider Threat) ?
  - Il est couramment admis que 80% des incidents sont d'origine interne
- Le rapport Verizon DBIR-2013 propose une explication intéressante :
  - 69% des incidents proviennent de l'intérieur de l'entreprise
  - 92% des attaques volontaires proviennent e l'extérieur de l'entreprise



1.2) Evolution de la menace depuis 2010

- 2010 = Stuxnet
  - Les systèmes SCADA sont des cibles de choix, à protéger activement.
- 2011 = APT + Hactivisme
  - Les attaques par infiltration (APT) visant les entreprises se sont multipliées (principalement dans un but de cyber-espionnage)
  - L'hacktivisme fait son apparition et démontre que des attaques opportunistes et relativement peu sophistiquées peuvent avoir un impact significatif en termes d'image.
- 2012 = 0-days
  - La multiplication des attaques 0-day montre qu'aucun système n'est à l'abri d'une attaque réussie
  - Les S.I. doivent être conçus en prenant en compte le fait qu'ils seront compromis.
- 2013 = L'affaire Snowden
  - Certains groupes (spécialisés dans les attaques de niveau étatiques) ont développé un arsenal d'attaques bien plus poussé que ce que l'on pouvait imaginer jusque là.

En 4 ans le risque "Cyber-attaque" a considérablement changé !!

Computer Emergency Response Team
Industrie Services Tertiaire

2) Les événements marquants de 2013

2.1) Snowden et la NSA changent la perception du risque « cyber-espionnage »

- Snowden révèle les activités de Cyber-espionnage de la NSA
  - **PRISM** : La NSA dispose d'un accès direct à (certaines ?) données des hébergeurs (Google, Facebook, Yahoo!, etc…) et des opérateurs télécom (Verizon)
  - **XKeyscore** : La NSA (et d'autres états : UK, etc..) effectue des écoutes de masse sur les réseaux IP (capture du trafic et reconstitution des conversations)
  - **Attaques contre le chiffrement** (programme Bullrun) : accords avec des constructeurs, algo affaiblis (Dual_EC_DRBG).
  - **Catalogue de backdoors** (ANT catalog) : backdoor BIOS, etc…
- Est-ce vraiment une nouveauté?
  - Les éléments techniques ne sont pas nouveaux (pas de révolution technologique)
  - Mais ces risques étaient jusque là purement théoriques
- Depuis ~10 ans les gouvernements travaillent à développer un arsenal offensif
  - La NSA l'utilise abondamment depuis au moins 2008
  - Les autres pays aussi …

Industrie Services Tertiaire

2.2) Attaques matériels : une menace désormais réelle

- Depuis plusieurs années la recherche sur les attaques de bas niveau est active
  - Attaques « ring-2 » via les SMI et le mode SMM (2008/2009) : Joanna Rutkowska (BluePill) et Loïc Duflot.
  - Attaques DMA / PCI (LAAS/IRIT)
  - Modification du code KBC – Keyboard Controler (SSTIC-2011)
  - Backdoor expérimentale dans le firmware d'un disque (Eurecom) (illustration)
  - BadBios (infection BIOS + Audio Networking + USB + IPv6 covert-channel)
- Visiblement, la NSA dispose déjà de ce type de backdoors
  - IRONCHEF, DEITYBOUNCE : Backdoor BIOS (attaque SMM) pour HP Proliant ou Dell PowerEdge
  - IRATEMONK : Backdoor pour disque Maxtor, Samsung, Seagate, and Western Digital
  - Etc…

Industrie Services Tertiaire

2.3 La sécurité offensive de plus en plus présente

- Les mentalités évoluent
  - Avant 1996 : Le chiffrement est une arme de guerre
  - 2004 : LCEN : Détenir des codes offensifs est interdit
  - 2011 : LOPPSI 2 : La police peut s'introduire sur les ordinateurs et y placer des mouchards
  - 2013 : Livre Blanc de la Défense Nationale et LPM : la sécurité offensive est reconnue comme une composante à part entière de la Défense Nationale
  - 2013 : La vente de 0-days est une pratique admise (cf. Vupen)
- C'est une évolution « pragmatique »
  - Compréhensible pour un état : la maitrise du Cyber est impératif
  - Mais dangereuse si elle se banalise et s'étend au monde de l'entreprise

Industrie Services Tertiaire

3) Les attaques visant les entreprises : comment se protéger ?

Cert IST
Industrie Services Tertiaire

3.1) Lutter contre les APT

- Contrer les vecteurs d'attaque
  - Ingénierie sociale – Informer les utilisateurs sur les risques et la conduite à tenir
  - Vulnérabilité du poste de travail – Maintenir à jour les OS et logiciels applicatifs
  - Attaques 0-days – Intégrer les risque 0-day dans la gestion de la menace
  - Propagation de l'infection – Mise en place de solutions de gestion des comptes à privilèges
- Améliorer la maîtrise de la sécurité du S.I.
  - Adapter l'architecture pour limiter l'impact d'une attaque réussie
  - Mettre en place une surveillance active au sein de l'entreprise
  - Développer les procédures de réaction en cas d'intrusion

3.2) Lutter contre les attaques opportunistes (exemple : Hacktivisme)

- Cibles traditionnelles : les sites web
  - Trop de sites web ne sont pas maintenus en termes de correctifs de sécurité.
  - Au bout de 3 ans des vulnérabilités découvertes dans les framework (Joomla, WordPress), rendent les attaques triviales.

- Nouveautés 2013 : Comptes Twitter et DNS
  - Prise de contrôle par les pirates de comptes sensibles
    - Phishing ou même appel au Help-Desk pour obtenir un mot de passe
  - Comptes Twitter d'entreprises
    - Associated Press (avril), The Guardian, New York Post
  - Comptes de revendeurs de noms de domaines DNS
    - Modification d'enregistrements DNS pour Twitter, New York Times , le Quatar

3.3) Lutter contre les attaques Scada

- Rappels
  - 2010 : Stuxnet = prise de conscience de la vulnérabilité des SCADA
  - 2011-2012 : Les chercheurs de failles se tournent vers le SCADA.
- 2013 :
  - Un peu moins de failles SCADA publiées
  - Mais des failles génériques sont découvertes (ex: Vulnérabilité sur le protocole DNP3)
  - Trend-Micro publie une étude sur un honeypot SCADA

  Le domaine reste donc très actif

- Le SCADA reste un domaine prioritaire à sécuriser
  - L'ANSSI a publié plusieurs guides de sécurisation début 201

Computer Emergency Response Team
Industrie Services Tertiaire

Quelques vulnérabilités remarquables

CertIST
Industrie Services Tertiaire

Les vulnérabilités / attaques de 2013

- Vulnérabilités dans Java (de janvier à avril 2013)
- Vulnérabilités du protocole UPnP (janvier 2013)
- Attaque DDOS record contre Spamhaus (mars 2013)
- Vulnérabilités dans IPMI/BMC (août 2013)
- Attaques CryptoLocker (octobre 2013)
- Attaque Adobe et vol de code source (octobre 2013)
- Attaques visant la chaine de magasins TARGET (décembre 2013)

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

Conclusions

Cert IST
Industrie Services Tertiaire

Conclusions

- **L'entreprise doit composer avec une situation complexe**
  - Un risque accru d'attaque
    - Risque d'APT, risque SCADA, risque d'Hacktivisme
  - Une demande utilisateur pour plus d'ouverture (Cloud, BYOD, etc…)
  - Il faut connaitre les risques pour arbitrer
    - Le Cert-IST donne une vision argumenté de la menace
    - Et rappelle que le modèle de sécurité éprouvé est celui de la sécurité en profondeur
- **La veille sur les vulnérabilités et menaces est une composante indispensable de la SSI**
  - Importance de la gestion des vulnérabilités dans l'entreprise
    - 4000 vulnérabilités par an, 900 avis de sécurité Cert-IST
  - Il ne s'agit pas simplement de déployer des correctifs
    - Mise en place de mesures de protections spécifique en cas de menace
    - Considérer que la compromission d'un poste ou un serveur est un événement possible

Industrie Services Tertiaire