Computer Emergency Response Team
Industrie Services Tertiaire

# Panorama des menaces


Juin 2012

Philippe Bourgeois

## Plan de la présentation

- Les grands axes d'évolution
  - Evolution des attaques au cours des 10 dernières années
  - Faits techniques les plus significatifs
    - Des attaques qui visent le poste de travail
    - Professionnalisation des attaquants et défenseurs
    - Une informatique d'entreprise plus ouverte
- Les événements marquants de l'année
  - Les attaques visant mes fournisseurs
  - Des réseaux insuffisamment sécurisés
  - Attaques par infiltration (APT)
  - Vulnérabilités SCADA
  - Cyber-activisme
  - Sécurité des smartphones
- Conclusions

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

# Les grands axes d'évolution


## Evolution des attaques au cours des 10 dernières années

- 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).
  - Constitution de botnets regroupant les machines infectées
- Aujourd'hui la menace se tourne vers l'entreprise
  - Phénomène des attaques par infiltration (APT)
  - Attaque Stuxnet visant les systèmes SCADA
  - Cyber-hacktivisme

Industrie Services Tertiaire

## Fait technique 1 : Des attaques qui visent le poste de travail

- Infection de l'internaute lors de sa navigation Internet
  - Déclenchement automatiquement lors de la visite d'un site web infecté (Drive-by download attack)
  - Utilisation 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 limitée
  - 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)

Industrie Services Tertiaire



## Fait technique 2 : 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 : Démantèlement 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 durcit 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.

Industrie Services Tertiaire

## Fait technique 3 :
## 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

# Les événements marquants de l'année

## Les attaques visant mes fournisseurs

- Exemples 2011/12 d'incidents fournisseurs impactant potentiellement les entreprises clientes
  - Vol de données relatives aux calculettes RSA SecurID
    - Mes accès VPN sont-il toujours sûrs ?
  - Vol de certificats SSL (Compromissions de CA : DigiNotar, Comodo)
    - HTTPS est-il d'un niveau de sécurité suffisant ?
  - Vol des codes sources : PcAnyWhere, VMware
    - Mes infrastructures sont-elles en danger ?

- C'est une nouvelle forme de menace
  - Différent du schéma classique vulnérabilité / correctif des produits
    - Souvent, le fournisseur minimise ou nie le problème
  - L'analyse de ces événements n'est pas triviale
    - La menace est-elle réelle? Doit on se protéger ? Comment ?
  - Il s'agit de menaces indirectes
    - Ma sécurité dépend d'acteurs extérieurs
    - Dont le niveau de sécurité est finalement questionnable

Industrie Services Tertiaire



## Attaques par infiltration (APT) 1/2

- 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 », « Duqu », « Flame », etc

- 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 industriels 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) 2/2

- Ces attaques sont construites et déterminées
  - Attaques RSA SecurID : les données volées en mars à RSA ont été utilisées en mai pour tenter d'attaquer Lockeed Martin


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

- L'attaquant adapte ses moyens aux défenses en place
  - Le niveau de défense doit être suffisant pour dissuader l'attaquant d'utiliser l'arme informatique
  - En l'absence de défense l'attaque informatique est très rentable
    efficacité = butin / ( coût * prise de risque)
- Beaucoup de victimes semblent avoir été des proies faciles
  - Le niveau de sécurité à l'intérieur de l'entreprise est-il suffisant ?
  - Exemples : RSA, DigiNotar,

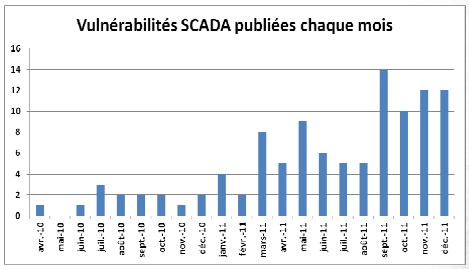


## Des réseaux insuffisamment sécurisés

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

## Vulnérabilités SCADA

- 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 où les chercheurs de failles s'intéressent au SCADA
  - Luigi Auriemma publie 54 vulnérabilités
  - Gleg publie son pack « Agora SCADA+ exploit pack »




- Ces « recherches » déboucheront fatalement sur des attaques
  - La sécurisation des systèmes SCADA est une préoccupation majeure

Industrie Services Tertiaire



## 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

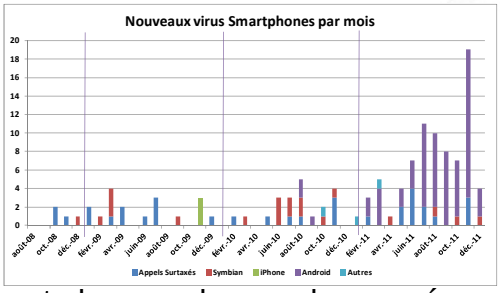
Nota : Mouvements multi-formes difficiles à cerner, allant du jeu à l'action politique.

- Faut-il craindre les Hacktivistes ?
  - De réels succès
  - Contre 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 ?

Industrie Services Tertiaire

## Sécurité des smartphones

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




- L'escroquerie numéro 1 reste les appels vers des numéros surtaxés
  - Au moyen de fausses applications, disponibles (principalement) en dehors du « market » officiel
- 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.
  - Mais peu d'attaques évoluées constatées.



## 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 et les entreprises
  - 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 ?

  (Cf. le rapport sur les risques induits par les smartphones publié fin 2010 par l'ENISA)

Computer Emergency Response Team
Industrie Services Tertiaire

# Conclusions

Cert IST
Industrie Services Tertiaire

## Conclusions (1/2)

- Sur le front des attaques le paysage se durcit
  - Les vulnérabilités du SI vont certainement être exploitées
    - Par des attaquants opportunistes : par exemple des hacktivistes
    - Par des attaquants professionnels : attaques par infiltration (APT)
- Pour contrer cette menace montante l'entreprise doit
  - Mesurer son exposition et renforcer ses défenses
    - En renforçant ses fondamentaux ou en se tournant vers de nouvelles offres ?
  - Se tenir informée sur les vulnérabilités et les menaces
- Ce mouvement marque sans doute le début d'un nouveau cycle de sécurisation

Industrie Services Tertiaire

# Conclusions (2/2)

- Les attaques par infiltration sont l'événement majeur de l'année
- 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/