Computer Emergency Response Team
Industrie Services Tertiaire

Panorama des Menaces

David TRESGOTS

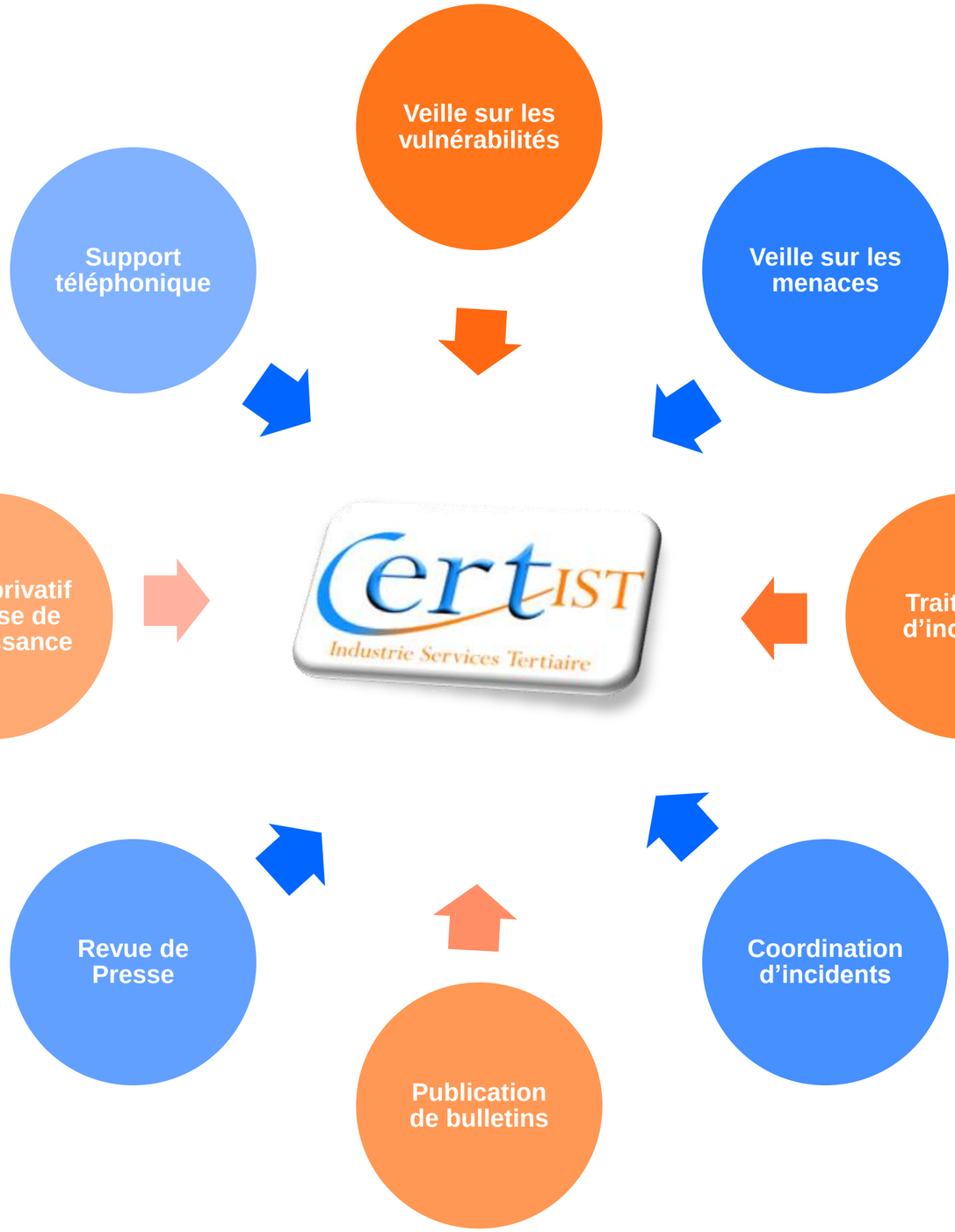
11 juin 2013
Forum Cert-IST 2013

Sommaire

- **Les services du Cert-IST**
- **Veille sur les vulnérabilités et les menaces**
- **Evénements majeurs de 2012**
- **Sujets d’actualité**

Les services du Cert-IST

Nos services

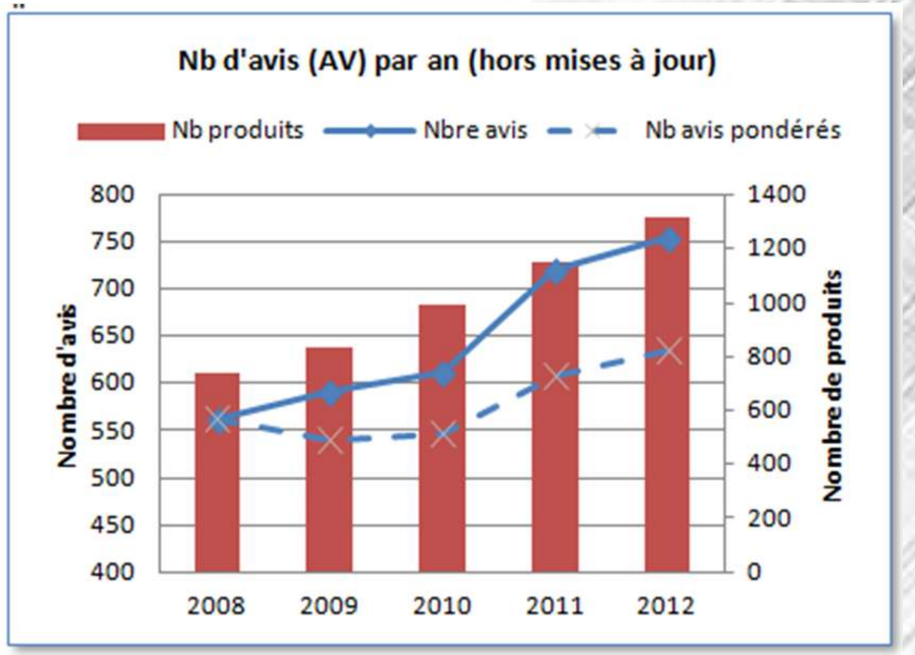


Veille sur les vulnérabilités et les Menaces

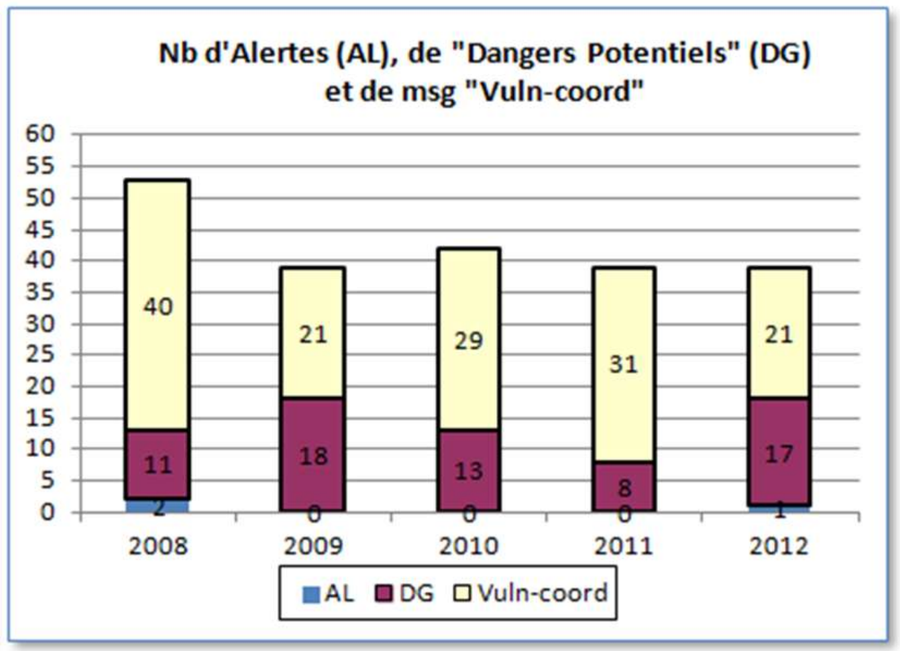
Avis, Dangers Potentiels et Alertes émis en 2012

- 755 Avis de sécurité (AV) émis en 2012
  - Le nombre de vulnérabilités (AV) découvertes par an ne faiblit pas

Un système non mis à jour se dégrade donc au fur et à mesure du temps



- 1 Alerte (Java) et 17 Dangers Potentiels (DG)
  - Le danger provient souvent du fait que des vulnérabilités récentes sont intégrées aux outils d'attaques
  - Cette intégration est de plus en plus rapide : Vulnérabilité ⇨ Metasploit ⇨ Blackhole



Les Alertes et DG émis par le Cert-IST en 2012

- Multiplication des attaques contre Java
- Navigateur :
  - Internet Explorer est toujours une cible privilégiée
- Système :
  - Windows reste une cible de choix également (ou ses composants)
  - Mac OS-X n'est pas exempt de défauts cependant (Attaque Flashback !)
  - Android attire de plus en plus les pirates
- Autres
  - Quelques failles graves peu médiatisées : Oracle, Samba, Networker, ClearQuest
  - Vol de code source (PCAnywhere), vulnérabilités Sophos
- Faits notables !
  - 1er DG sur un produit SCADA (PLC Modicom de Schneider-Electric)
  - Pas d'Alerte ou DG concernant Adobe Reader en 2012 !

Evolution du paysage de la menace

Le paysage de la menace ne cesse d'évoluer

- Il y a bien longtemps …
  - Attaques tout azimut
    - Ludiques (script kiddies)
    - Recherche de notoriété
    - Dégradation « bête et méchante » (infection virale), etc.

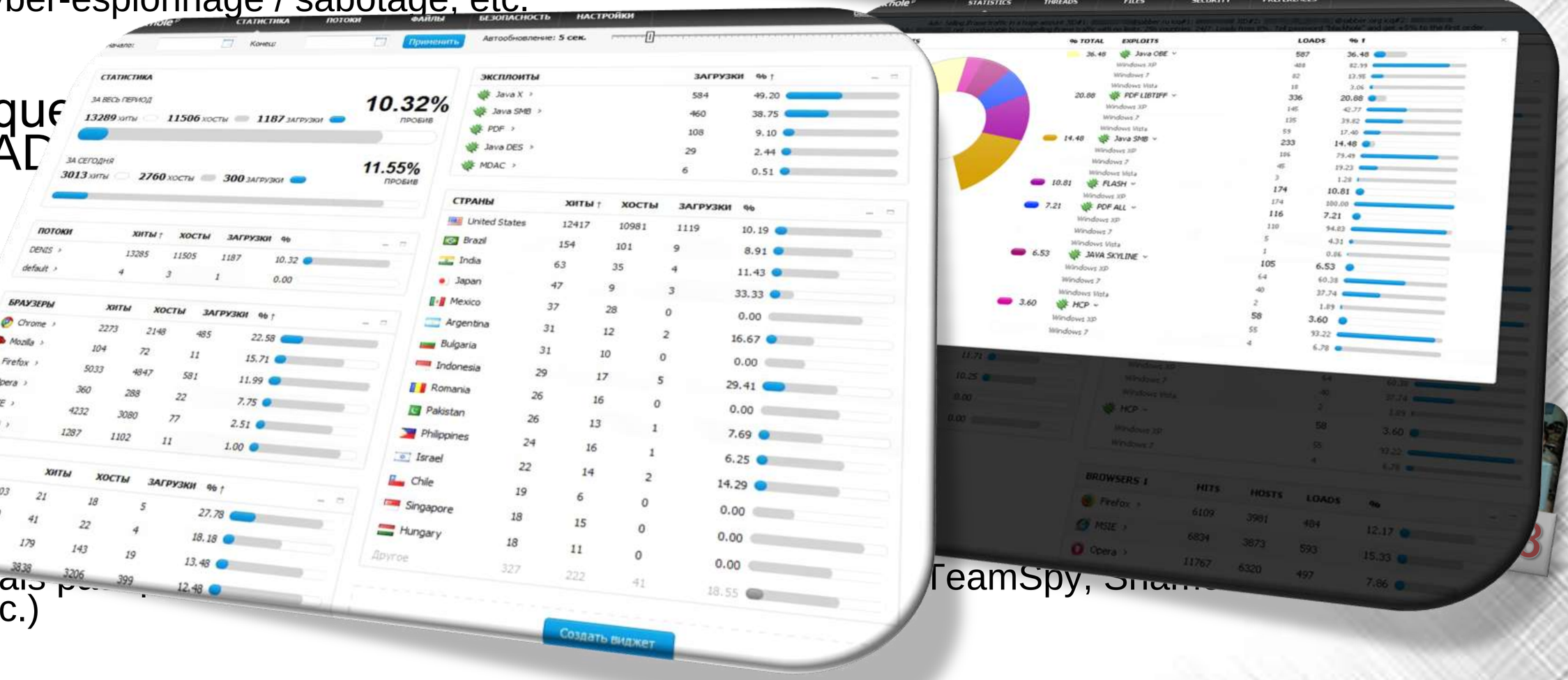
- … Encore hier
  - Attaques opportunistes
  - Cibles plutôt faciles
    - « Defacements » de sites web
    - Envoi de Spam
    - Botnets
    - Vol de données bancaires
    - Escroquerie visant les particuliers (faux antivirus, ransomware « virus de la Police »)
  - Auteurs isolés (plus ou moins)
  - Niveau « amateur » (plus ou moins)
    - Ayant acquis de la compétence ou des outils « presse-bouton »
  - Certains se sont structurés pour en faire un Business
    - Groupes Cyber-criminels visant le grand public et les industries
  - D'autres y voit un moyen de propagande
    - Attaques hacktivistes (ex. Anonymous, Lulzec)

Aujourd'hui : Les lignes bougent … continuent de bouger

- Attaques de nature « professionnelle »
  - Ex. : Blackhole

- Attaques par infiltration (APT)
  - cyber-espionnage / sabotage, etc.

- Attaque
(SCAD



- Men
  - [
  - [
  - Mais pa … TeamSpy, Sham… etc.)

Un phénomène qui prend de l'ampleur

- Montée de la Sécurité Offensive
  - Certains états s'y préparent, d'autres sont déjà prêts
  - Risque d'inciter certaines victimes à faire de même
    - Individus, organismes , entreprises, etc., mais pas que
    - Pourtant la loi est claire (c'est interdit)
  - Attention aux dérives !
    - Victimes collatérales
    - « Auto-défense »

- Dans la plupart des cas, cela ne sera pas de l'auto-défense !
  - Car prémédité
  - Car très probablement moyens disproportionnés

Evénements majeurs de 2012
(pour les menaces visant les Entreprises)

1) SCADA : la menace progresse

- SCADA = Supervisory Control And Data Acquisition
  - Ce terme est employé ici au sens large pour désigner l'informatique industrielle et les systèmes de contrôle industriel (ICS)

- Petit rappel : 2010, prise de conscience dans le monde SCADA
  - Effet STUXNET !
  - Catalyseur du besoin de sécurité dans le monde SCADA
  - Ver probablement conçu pour détruire les centrifugeuses iraniennes d'enrichissement nucléaire.
  - De plus en plus de chercheurs de failles s'intéressent désormais au SCADA
    - Ex : Luigi Auriemma – revuln.com , Gleg.net : « Agora SCADA+ exploit pack »

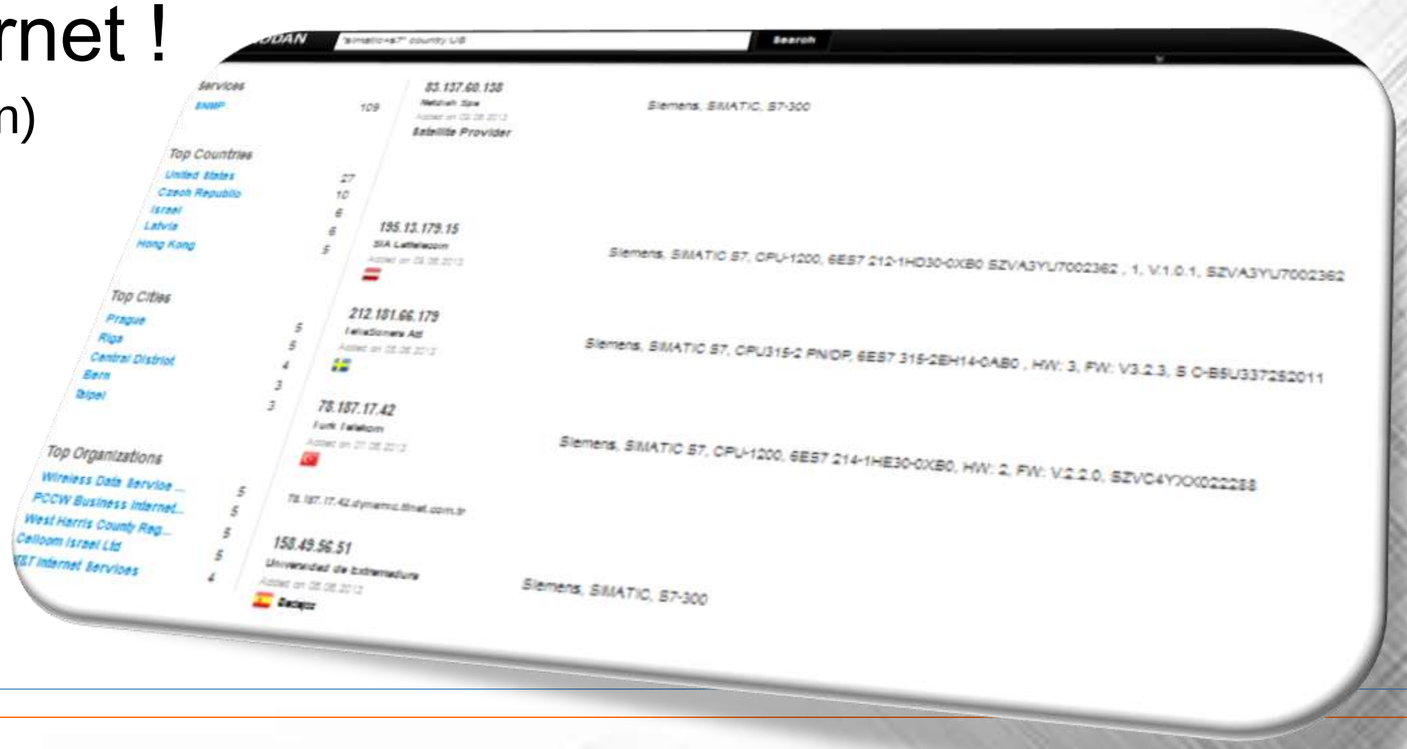
- Actualité 2012 :
  - Pas d'incident majeur, mais plusieurs attaques visant le domaine de l'énergie :
    - Shamoon contre Aramco & RasGas, Intrusion chez Telvent (Schneider) visant le produit OASys
  - Un niveau de sécurité parfois inquiétant
    - 500 000 équipements industriels accessibles depuis Internet ? (moteur de recherche Shodan)
  - Une nouvelle classe de failles ? Les « forever-day » ou « insecure by design » !
  - Les professionnels du SCADA se mettent à publier des failles
    - Projet « Base camp » de Digital-Bond
    - Les vulnérabilités identifiées sont plus critiques

- La sécurisation des systèmes SCADA est une préoccupation majeure !

Pris en compte du risque SCADA par les entreprises

- Il faut intégrer le risque lié aux vulnérabilités SCADA
  - Malgré le retard de la sécurité SCADA sur l'IT
  - Identifier les produits utilisés (au même titre que les produits IT)
  - Limiter la visibilité des équipements SCADA (DMZ, etc.)
  - Avoir un service de veille sur les vulnérabilités affectant ces produits

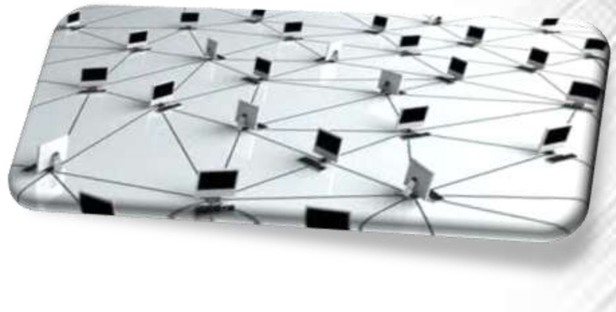
- Pas d'équipements sur Internet !
  - Si, si ça existe encore (ex. Shodan)



2) Attaques par infiltration (APT)

- L'attaque par infiltration, un risque « nouveau » pour les entreprises ?
  - Pas si nouveau, en fait (cf. nos présentations au forum Cert-IST 2011 & 2012)

- Sujet préoccupant depuis 2 ans
  - Les attaques se multiplient et touchent un plus grand nombre d'organismes (changement d'échelle)
  - Un grand nombre d'organismes sont vulnérables
  - Phénomène révélateur d'une montée de la sécurité offensive
  - Effet boule de neige ?



- Qui sont les attaquants ?
  - Des états ? (pour des objectifs stratégiques)
  - Des individus isolés ? (agissant pour des commanditaires)
  - Bientôt / déjà, des cyber-groupes indépendants ? (agissant pour eux-mêmes dans l'objectif de revendre leurs prises)

Pris en compte du risque APT par les entreprises

- Comment contrer ces attaques ?
  - Renforcer les fondamentaux :
    - Sensibiliser les utilisateurs,
    - Renforcer les mots de passes, limiter les comptes administrateurs,
    - Protéger les données sensibles sur des serveurs sécurisés,
    - Appliquer les correctifs de sécurité
    - Mettre en place une collecte et une gestion des logs centralisée
    - Quelques références :
      - 20 Critical Security Controls for Effective Cyber Defense (USA)
      - Guide de l'hygiène informatique (France – ANSSI)
  - Mettre en place une surveillance active au sein de l'entreprise, au travers d'une structure responsable de la supervision de la sécurité.
  - Définir une procédure de réaction en cas d'incident définissant le comportement à adopter et les personnes à impliquer
  - Traiter les attaques par une équipe spécialisée

3) Augmentation du risque 0-day

- 0-day : Vulnérabilité gardée secrète jusqu'au jour où elle est utilisée dans une attaque réelle

- Depuis 2005, on sait que le risque 0-day existe

- On se rend compte aujourd'hui que le risque est plus grand qu'estimé jusque là
  - Quatre 0-days utilisés en 2010 dans une seule attaque (Stuxnet)
  - L'étude Elderwood (Symantec - 2012) montre que certains groupes (sponsorisés par des états ?) possèdent de nombreux 0-days
  - L'étude « Before we knew it » (Symantec - 2012) estime qu'un 0-day reste en moyenne non découvert pendant 300 jours
  - Le 0-day est devenu un vrai commerce

Pris en compte du risque 0-day par les entreprises

- Il faut intégrer le risque 0-day à la gestion de la menace
  - Détecter au plus tôt son occurrence
  - Limiter la conséquence pour le S.I. de la compromission d'un poste de travail ou d'un serveur,
  - Définir une procédure d'isolation, d'analyse d'impact et de remise en service des éléments compromis.

3 : Sujets d’actualité

Actualité 2012 : Cloud & Big Data

- Cloud : les risques sont désormais bien identifiés

  - 2010 : Attention danger ! : les experts préviennent des dangers potentiels
  - 2011 : Le détail des difficultés : les experts détaillent les difficultés sur les volets contractuels, juridiques et techniques
  - 2012 : Prêts pour la mise en pratique : les RSSI connaissent désormais bien les difficultés et les chantiers à couvrir dans un projet Cloud. L'effort à déployer est bien sûr proportionnel au niveau de sécurité à assurer.

- BIG-Data : Sujet à la mode, ou réel problème pour les entreprises ?
  - Modèle distribué des applications, des données
  - Multiplicité des sources ; Quid de la sécurité ?
  - Big data = Big Brother ?

Actualité 2012 : Smartphones, BYOD, …

- Smartphones : Pas d'évolution significative de la menace
  - Android est la plate-forme préférée des malwares mobiles
  - Montée en flèche du nombre de malwares détectés par les éditeurs antivirus
  - La majorité des attaques consistent à cloner des applications à succès et à leurs ajouter une fonction cachée qui génère automatiquement des appels vers des numéros surtaxés
  - Les techniques d'attaques reproduisent les techniques connues du mode IT : (drive-by download, botnet, Ransomware).
  - Pas de cas d'attaque sophistiquée répertorié à notre connaissance

- BYOD : le sujet le plus commenté en 2012
  - Phénomène émergeant avec des risques réels
  - Prolongement du Cloud ? (en termes de risque)
  - Pas d'incident connu où le BYOD aurait été un vecteur d'attaque (mais c'est théoriquement possible)

Actualité 2012 : Réseaux sociaux, APT, …

- Réseaux sociaux
  - Attaques de sites connus
    - LinkedIn (vol d'identifiants) 6,5 millions de comptes volés en juin 2012
    - Facebook (atteinte à la vie privée), etc.

- Cyber-espionnage et APT

- La montée des états
  - Mise en place ou le renforcement de structures dédiées à la cyber sécurité (ANSSI = 2009)
  - Officialisation de la possibilité de cyber-guerres (USA 2011 = Plan « Cyber 3.0 ») (OTAN 2012 = Manuel de Tallinn)
  - Médiatisation d'incidents supposés d'origines étatiques : Chine, USA, Israël, Iran ?

Actualité 2012 : Hacktivisme, Cybercriminalité, …

- Hacktivisme : Des revendications « fantaisistes » montrent certaines limites des mouvements de type Anonymous
  - Plusieurs arrestations de leaders

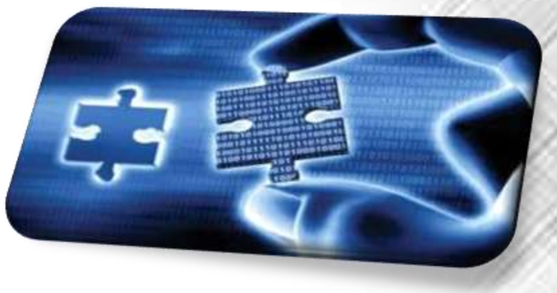
- Cybercrime : 2012 a vu la montée en flèche des ransomwares avec malware « Reveton » (faux avertissement de la Police)

- Vol de données personnelles
  - Logins/mots de passe, numéros de cartes bleues…
  - Le phénomène s'amplifie d'années en année. Exemples :
    - Zappos : 24 millions de coordonnées clients volées en janvier 2012
    - Apple : 12 millions de données relatives à des terminaux iPad, iPod et Iphone volés en septembre 2012
    - Etc.

Conclusions

Conclusions

- **L'entreprise doit composer avec une situation complexe**
  - Un risque accru d'attaque
    - Risque d'APT, risque SCADA, risque d'Hacktivisme
  - Des outils d'attaque de plus en plus professionnels
  - 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, 800 avis de sécurité Cert-IST
  - Il ne s'agit pas simplement de déployer des correctifs
    - Mise en place de mesures de protections spécifiques en cas de menace
    - Considérer que la compromission d'un poste ou d'un serveur est un événement probable

Merci

Notre bilan 2012 est disponible sur le site public du Cert-IST.

www.cert-ist.com/fra/news/bilan2012