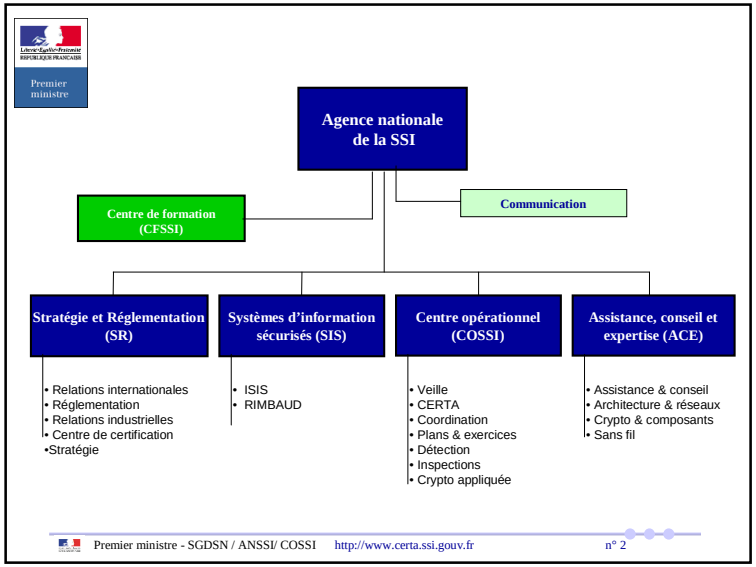
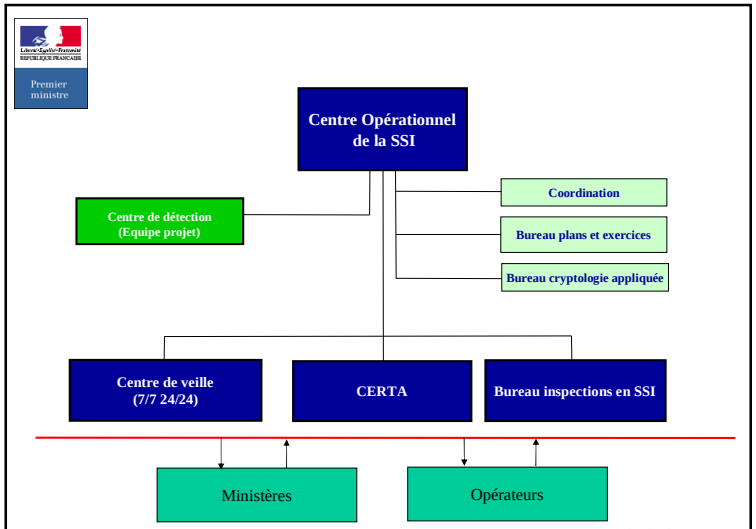
Agence Nationale de la Sécurité des Systèmes d'Information

Panorama des attaques vues par le CERTA

Nathalie FAVIER





Faille Microsoft MS08-67

- Octobre 2008 : faille critique corrigée par Microsoft.
- Criticité de cette faille largement sous estimée : exploitations massives de cette faille apparues plutôt en 2009. L'attention s'est particulièrement focalisée sur le ver Conficker (et ses variantes).
- Résultats :
  - pagaille sur les réseaux,
  - interruptions plus ou moins importantes des systèmes d'information,
  - infection de systèmes protégés et isolés de l'internet via des clés USB,
  - plus d'un an après, ce ver est encore présent dans de nombreux réseaux et continue à perturber le fonctionnement des réseaux.

Attaques par filoutage

- Les premier filoutages imitaient des banque anglo-saxonnes en raison de leur mode de fonctionnement, puis la palette s'est élargie à des clients de banques françaises.
- D'abord rédigés en un français approximatif, les pourriels se sont ensuite nettement améliorés, provoquant des campagnes de communication des organismes bancaires.
- Autres cibles : PAYPAL, eBay ou encore la SNCF, mais aussi l'administration fiscale ou les caisses d'allocations familiales, pour lesquelles les pourriels incitent les usagers à divulguer leurs données personnelles sous couvert d'une perspective de remboursement… Les FAI et fournisseurs de services de messagerie sont également impactés.

Courriels personnalisés piégés

- Des utilisateurs occupant un poste sensible reçoivent des courriels personnalisés contenant une pièce jointe ou un lien pointant vers un site malveillant. Lors de l'ouverture de la pièce jointe ou de la visite du site, des programmes malveillants sont installés sur l'ordinateur.

Botnet

- Mi-février 2010 : KNEBER. Estimation : 75 000 ordinateurs de particuliers, d'entreprises et d'administrations auraient fait partie de ce réseau de machines compromises.
- Mars 2010 : MARIPOSA : 12 millions de systèmes compromis.
- Menace en forte progression : ressources gratuites permettant de commettre des méfaits de façon anonyme. L'infection se produit via des chevaux de Troie, qui permettent aux attaquants d'en prendre le contrôle total de façon fortuite.

Botnet (2)

- Ils sont devenus très perfectionnés :
- Propagation et infection de nouveaux systèmes (les machines infectées tentent de propager l'infection pour incorporer de nouveaux membres dans le réseau ;
- Mise à jour (les programmes s'améliorent pour éviter leur détection et s'adapter aux besoins du BotMaster) ;
- Opérationnels -> besoin de dégager des revenus -> peuvent émettre des pourriels (commerciaux ou filoutage), manipuler des cours de bourse, « dérober » des informations personnelles, lancer des attaques en déni de service distribué pour paralyser la cible… Sont partie prenante d'une économie souterraine.

Botnet (3)

- Etude de cas : fin mars 2009, une administration française a été la cible d'une attaque en déni de service distribué. L'envoi massif de données en provenance de nombreux pays étrangers a eu pour conséquence une paralysie des moyens de communication avec internet.
- Volonté de nuire évidente mais motivation indéterminée.
- Détection rapide par l'administration du dysfonctionnement -> déplacement du CERTA pour analyse des éléments techniques disponibles en vue de proposer des parades à l'attaque.
- Parallèlement, une procédure judiciaire a été engagée.

Représentation graphique de l'étude de cas

Merci de votre attention