Protection contre les cyberrisques: où trouver de l'appui et comment envisager la défense

Conférence protection population / Cyberrisques
EPFL – 10.11.2017

Mathieu Simonin, Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Le constat: un risque ne pouvant être ignoré par aucune entreprise ou administration

- Des attaques sophistiquées, ciblant des informations précises et mobilisant des ressources illimitées
- Des criminels à la recherche du meilleur retour sur investissement, voulant accéder à de l'argent en:
  - Prenant le contrôle de systèmes informatiques (maliciels)
  - Manipulant leur interlocuteur (ingénierie sociale)
  - Exerçant un chantage (cyber extorsion)
- Et tous les autres: hacktivistes, script kiddies, etc.
- Les entreprises/administrations sont en première ligne
- Où trouver de l'appui ? Comment envisager la défense ?

Au cœur de ces problématiques: MELANI

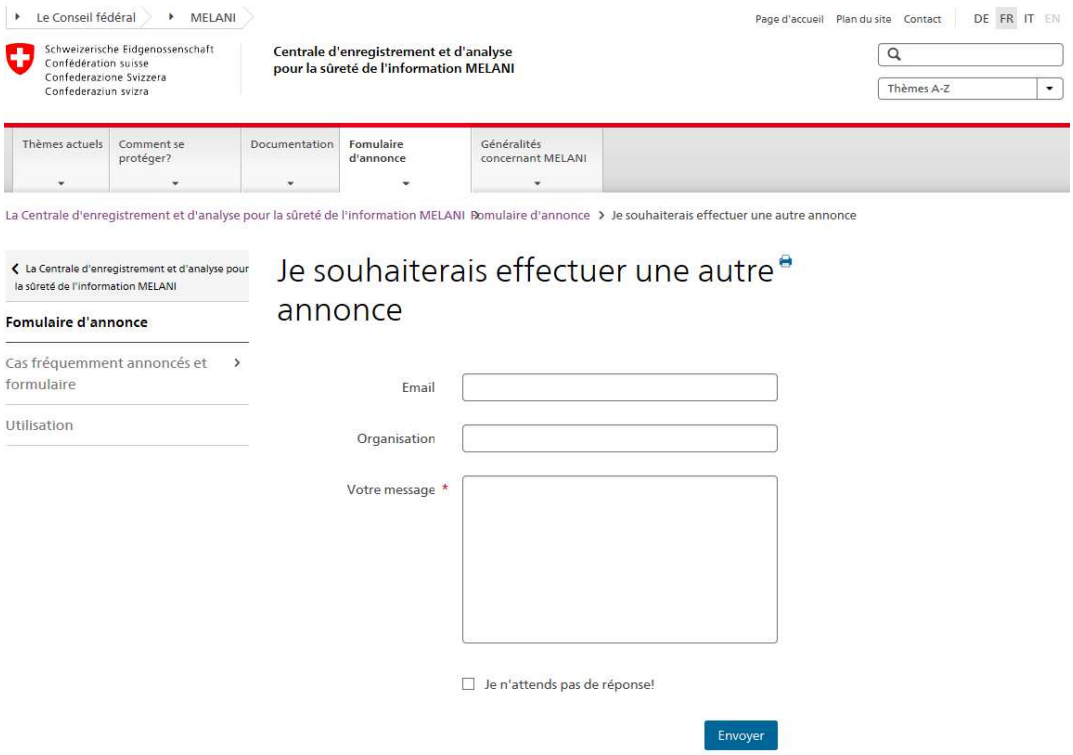
- Active depuis 2004
- Répartie entre DDPS et DFF; comprenant GovCERT
- Protection des infrastructures critiques comme mission première
- Prestations pour la population et les entreprises
- PPP
- Participation volontaire des partenaires, MELANI n'est pas un régulateur
- Subsidiarité

Tâches de MELANI

- **Observation de la situation nationale/recueil d'information dans un but de :**
  - Prévention (moyen/long terme)
  - Alerte/Incident handling (court-terme)

  - Cercle fermé de MELANI :
    - Établissement et maintien d'un **réseau** avec les opérateurs des infrastructures critiques
    - Soutien des opérateurs des infrastructures critiques : partage d'information; évaluation de la menace; soutien en cas d'incident
  - Cercle ouvert de MELANI :
    - Mesures de prévention pour les PME et la population
    - **Prestations** visant à diminuer l'impact de différentes menaces

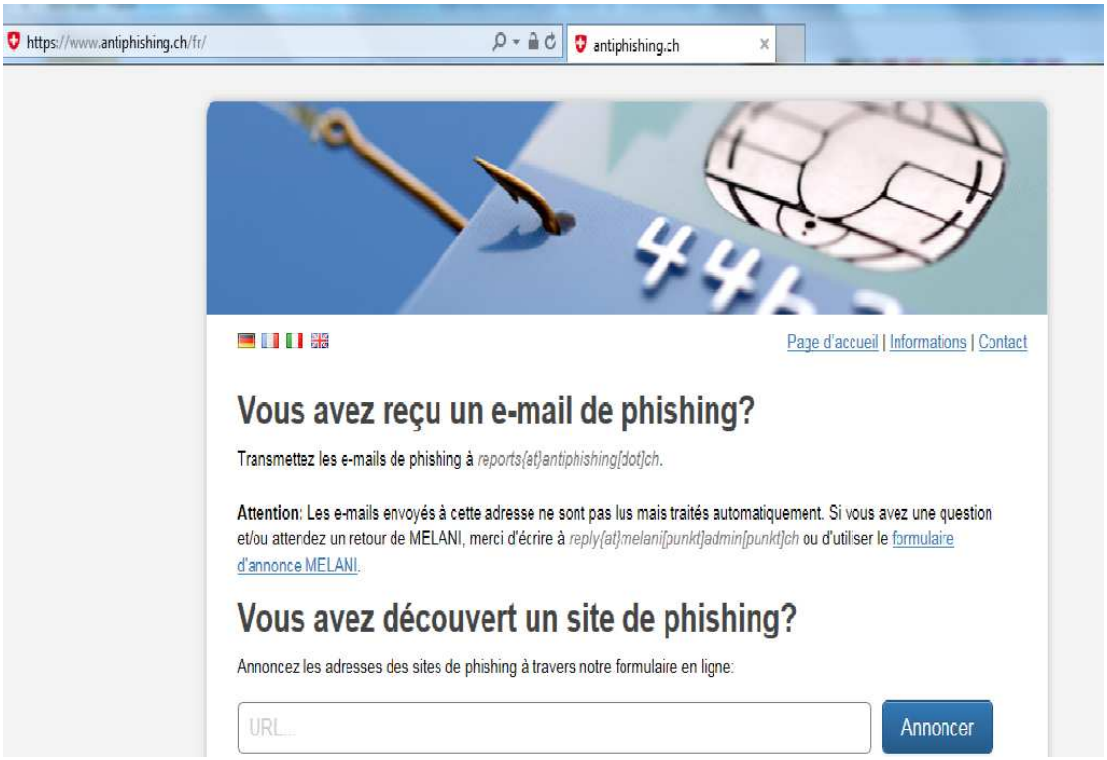
Un point de contact pour le public



Pourquoi annoncer des cas?

- Des conseils de prévention généraux
- Une expertise technique
- Profiter d'une vue d'ensemble de la situation
- Aussi un service d'orientation
- Pour nous, un senseur incontournable en vue de mesures de prévention
- Permet de diminuer l'impact des menaces

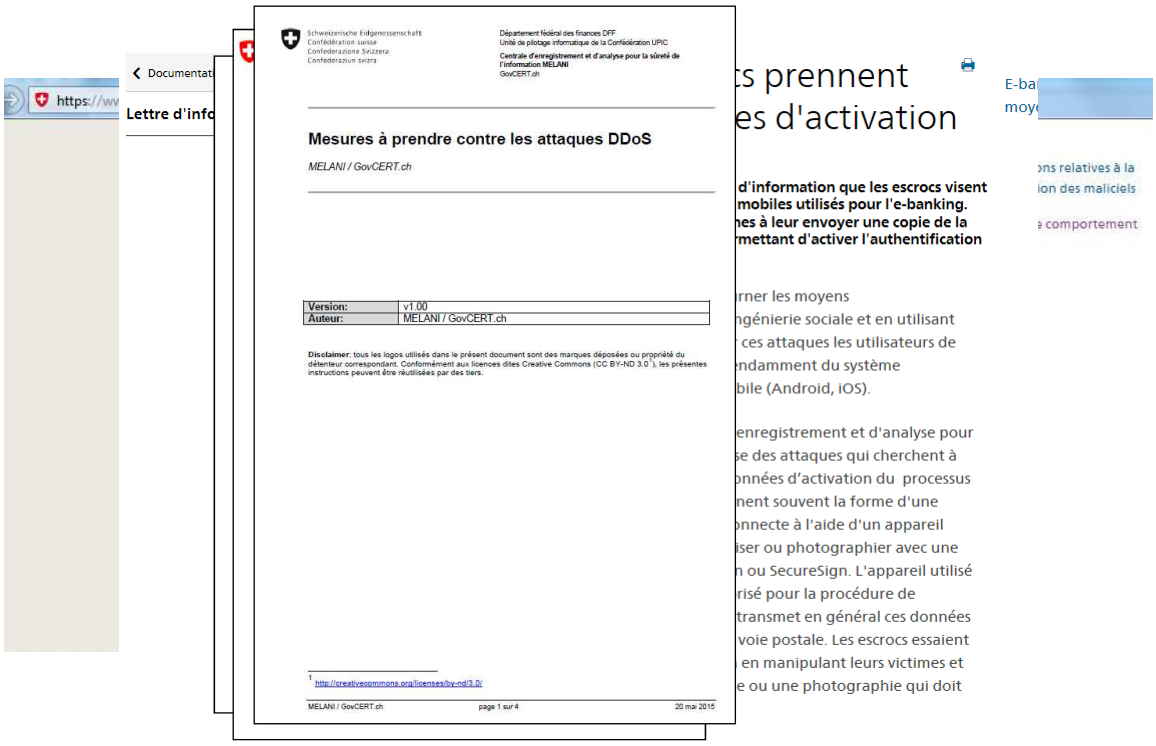
Action contre les sites de phishing



Lutte contre les maliciels

Source: http://www.govcert.ch

Information et prévention générale



Appréhension du risque

- La première étape est une prise de conscience: cela n'arrive pas qu'aux autres!
- A partir de là, il est nécessaire d'identifier les (ses) risques
- Comme préalable à cette réflexion, se connaître soi-même: quelles données, quelle valeur, quelle possibilité d'accès…
- Chaque entreprise n'aura pas non plus les mêmes priorités
- De la volonté de gérer ces risques découleront des mesures technologiques, humaines, organisationnelles
- Cette prise de conscience doit se faire au niveau du management, car elle nécessitera des budgets

Répondre à une menace à multiples facettes

- De nombreux acteurs aux motivations diverses
- Consolidation de certains modes opératoires ayant fait leur preuve mais également recherche constante de nouvelles opportunités
- Face à des cybercriminels «rationnels»: se protéger c'est souvent dissuader l'attaquant
- Mais pour des attaques plus perfectionnées: la capacité à détecter l'anomalie et y répondre doit être une priorité
- Une certitude: la voie unilatérale est une impasse → face à des attaquants échangeant efficacement de l'information, le partage entre pairs et avec les autorités est primordial (modes opératoires, indicateurs, bonnes pratiques, etc.)

Merci pour votre attention

Plus d'informations sur notre site web:
http://www.melani.admin.ch