Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SRC / UPIC
Centrale d'analyse et d'enregistrement pour la sûreté de l'information MELANI

Attaques sur la confidentialité des données: l'expérience de MELANI

Mathieu Simonin, Analyste MELANI

MELANI: Les étapes

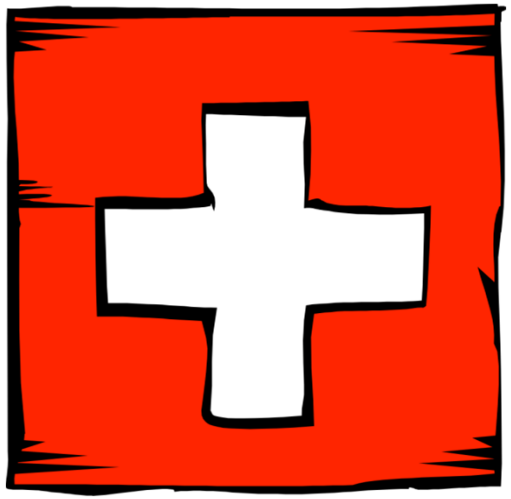
- 29.10.2003: Le Conseil Fédéral décide la mise en place de la centrale d'enregistrement et d'analyse pour la sûreté de l'information
- 01.10.2004: MELANI est opérationnel
- 01.04.2008: GovCERT.ch est opérationnel
- 01.02.2010: Adhésion à FIRST
- 01.06.2011: Adhésion à EGC
- Juin 2012: Présentation de la stratégie nationale de protection de la Suisse contre les cyber-risques

Mandat: Protection des infrastructures critiques

Infrastructures critiques

- Énergie
- Télécommunication
- Finance/Economie
- Transports publics et logistique
- Gouvernement
- etc.

Partenariat entre le secteur privé et le gouvernement (PPP)



- Constitution fédérale, Article 2: „La Confédération favorise la prospérité commune“

- Impossible sans la collaboration entre le secteur privé et le gouvernement → Public Private Partnership (PPP)

Tâches de MELANI

- **Observation de la situation nationale/recueil d'information** (dans le domaine de la sécurité des systèmes informatiques et de l'Internet) **:**
  - 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 en cas d'incident

  - Cercle ouvert de MELANI :
    - **Mesures de prévention** pour les PME et la population
    - www.melani.admin.ch

Les données sous attaque

Confidentialité – Intégrité – Disponibilité

Attaques visant l'intégrité des données

•Stuxnet: la première grande opération de sabotage numérique

- Premier cheval de Troie connu s'étant attaqué à des systèmes SCADA
- Utilisation de 4 failles "zero day"
- Emploi abusif de certificats de logiciels.
- Attaque ciblant les logiciels WinCC de Siemens.
- Fonctions Rootkit pour WinCC
- Utilisation de mots de passe codés en dur dans les logiciels Siemens.
- Propagation par USB.

Attaques visant la disponibilité des données

DDoS

- Extorsion
- Diversion
- Activisme/politique

Cryptolocker

Attaques visant la confidentialité des données

- L’aspect le plus attaqué
- Le moins facilement détectable
- Différents types d’acteurs
  - Criminels (groupes ou individus isolés)
  - États
  - Activistes
- Valeur de l’information

Acteurs criminels

Au quotidien: Phishing etc..

Mise à jour de vos informations du compte

Civilité * : Mr

Nom * :

Prenom * :

Date de naissance * : jour / mois / année

Adresse 1 * :

Email * :

Mote de Passe * :

Code postal * :

Ville * :

N° du compte de carte de crédit 0000

Carte de crédit * Mastercard

Numéro de carte de crédit *

Valable jusqu au * 01 / 2010

Code CVC/CIN * Où puis-je trouver le code CVC/CIN?

* Ces champs doivent être remplis! Suivant

Méthodes plus perfectionnées

Acteurs étatiques

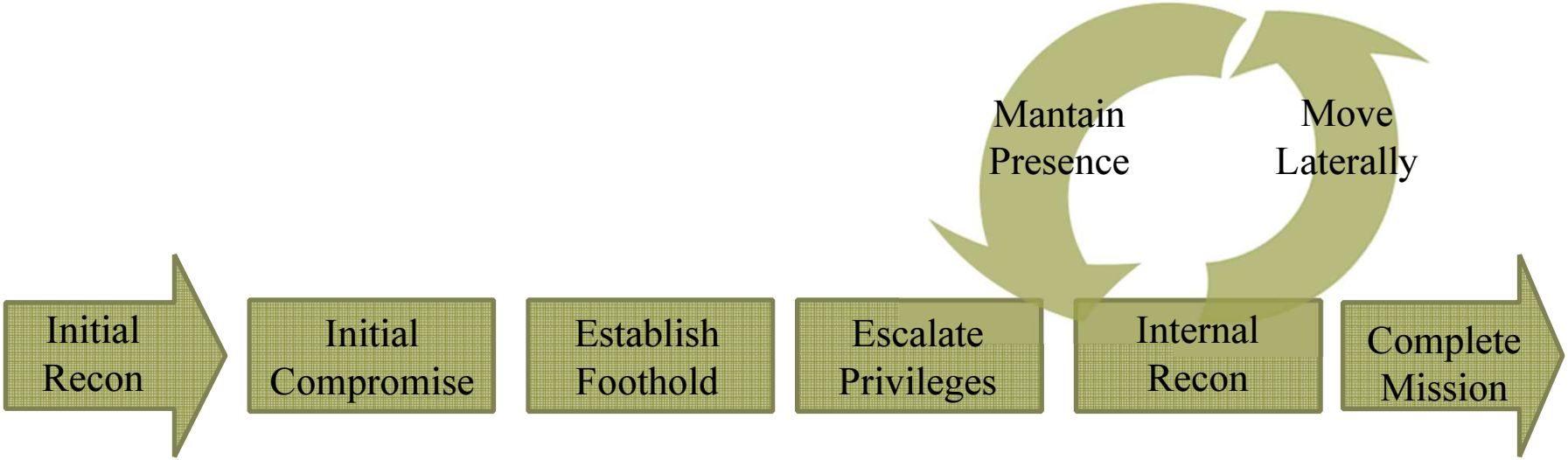
Advanced Persistent Threat (APT)

- Ce type d'attaque présente la particularité de mobiliser **différentes méthodes** pour s'introduire dans les systèmes visés et y mener ses **activités malveillantes**, de s'inscrire dans la **durée** et d'opérer de manière **furtive**.

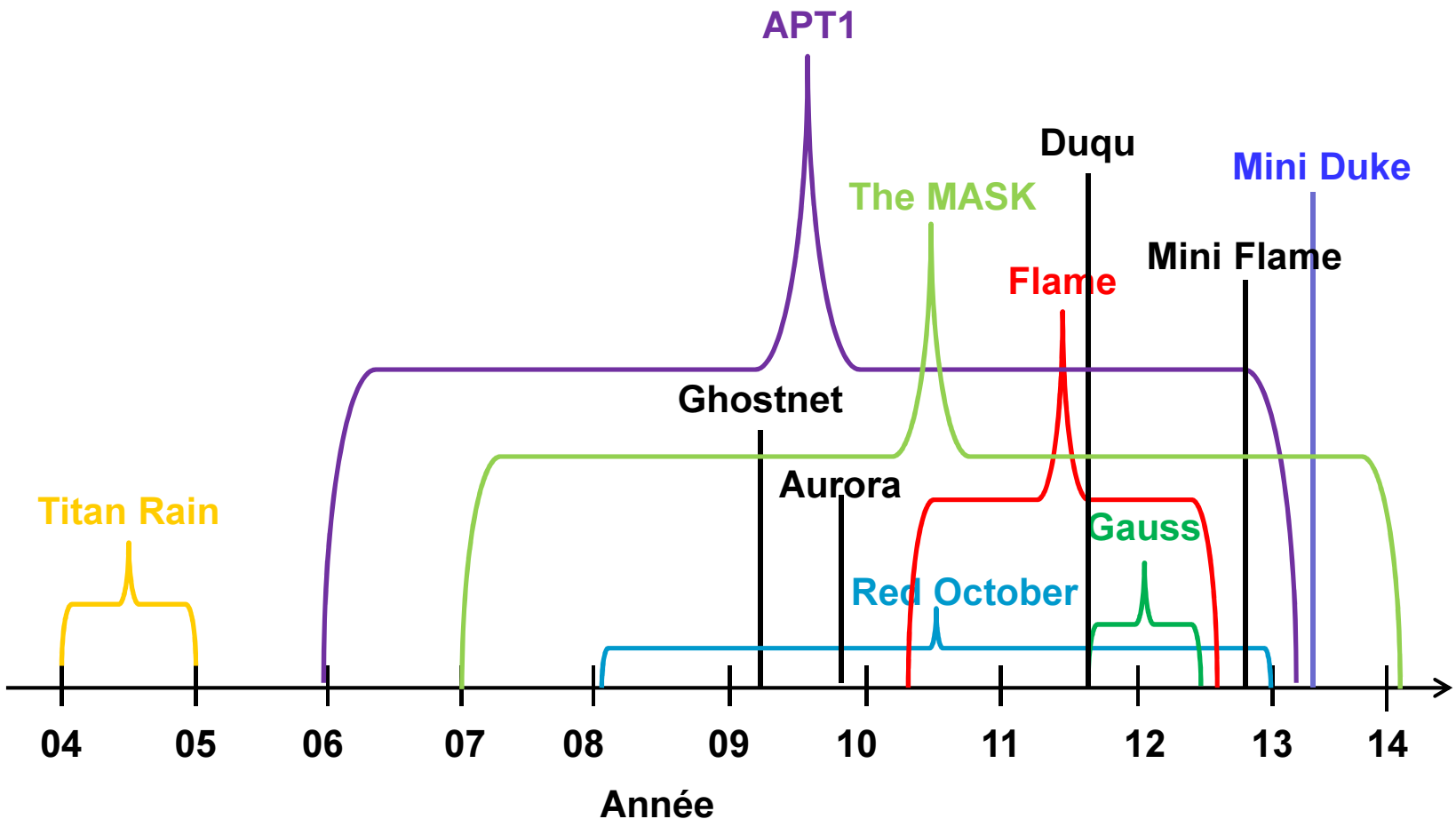
- Buts: Vol de données avant tout/destruction de données

- Attribution: Etats principalement (mais rarement précis…)

APT: cycle de vie



APT/ Timeline



The Mask/Careto

Source: Kaspersky, février 2014

Red October

Source: Kaspersky, janvier 2013

Début 2013

The New York Times

Business Day
Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Hackers in China Attacked The Times for Last 4 Months

Bloomberg News Quick Markets Personal Finance Tech U.S. Politics Sustainability Luxury

BREAKING NEWS Nuclear Operator Exelon to Buy Utility Operator Pepco for About $27.25 per Share Cash TWEET

Microsoft Joins Apple, Facebook as Target of Cyberattack

Save + By Dina Bass | Feb 23, 2013 6:01 AM GMT+0100 | 7 Comments Email Print

REUTERS EDITION: U.S. SIGN IN

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

Pentagon to boost cybersecurity force

WASHINGTON | Mon Jan 28, 2013 12:09am EST

0 COMMENTS | Tweet 16 Share 1 Share this 8+1 0 Email Print

RELATED NEWS

Pentagon cutting jobs, maintenance due to budget

(Reuters) - The Pentagon plans to assign significantly more personnel in coming years to counter increasing threats against

APT1

Source: Mandiant, février 2013

Révélations de Snowden – surveillance des communications à large échelle

SRC / UPIC
Centrale d'analyse et d'enregistrement pour la sûreté de l'information MELANI

NSA Mission Statement, SIGINT Strategy 2012 - 2016

"…Defeat adversary cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere."

Source: The New York Times, novembre 2013

Accès aux données

- Méthodes «passives»
  - Fibre optique (câbles), notamment TEMPORA
    Collaboration avec les fournisseurs de service (PRISM)

- Méthodes «actives»
  - Opérations ciblées (TAO- «Tailored Access Operations»)

Exploitation des données

- XKeyscore
- Action sur les systèmes de cryptage

Quelle réponse?

- Une approche globale de réduction du risque

- Au centre de la réflexion: les données et leur valeur
  - Classification des données
  - Quel accès, pour qui
  - Un traitement adapté au niveau de confidentialité

- Sensibilisation de l'utilisateur

- Evaluation du catalogue des fournisseurs
  - Où sont-ils basés (à qui doivent-ils répondre?)
  - A quoi ont-ils accès dans l'entreprise

Perspectives

- La Suisse une cible de choix
- “The Internet is broken: Act accordingly” ?
- Des contradictions:
  - Confidentialité s’oppose à certaines caractéristiques ayant façonné Internet et les services que nous connaissons:
    - L’idée « de base » d’un Internet standard, stable et robuste
    - Des services gratuits et faciles à utiliser
    - Dans lesquels un acteur a une position hégémonique