Protection des infrastructures informatiques des entreprises face à la cybercriminalité

Vincent Lemoine, Charles Perez, Marc Lemercier, Pierre Vitard,

Virginie Bensoussan-Brulé, Alain Corpel, Rida Khatoun, Babiga Birregah

Projet CPER CyNIC (Cybercriminalité, Nomadisme et Intelligence éConomique)

UMR STMR

Projet Cybercriminalité, Nomadisme et Intelligence éConomique

- Objectifs du projet
  - Analyse et évaluation des outils d'investigation numérique
  - Conception d'applications sécurisées pour terminaux nomades
  - Recherche source ouverte (réseaux sociaux)
  - Intelligence économique (aspects juridiques, dimension sociétale, confiance numérique)

- Partenaires
  - UMR STMR / ICD [ERA + CREIDD]
  - IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale)
  - GE : Devanlay (Lacoste)
  - PME : Eutech-SSII
  - Cabinet d'avocats Alain Bensoussan
  - EPIC ADIT (Agence pour la Diffusion de l'Information Technologique)

Contexte

- Nouvelles technologies (Internet, terminaux nomades) révolutionnent le fonctionnement des entreprises
  - Sphère commerciale, la gestion de projets, mécanismes d'échanges d'information

- Entreprises doivent revoir leur stratégie digitale et leur système d'information pour intégrer ces nouveaux canaux de communication
  - Référencement et e-réputation sur Internet
  - Marketing viral et relation client via Internet (eCRM)

- Logique crosscanal symbole actuel de modernité et d'efficacité économique
  - Réseaux sociaux numériques (Facebook, LinkedIn, Twitter, etc.)
  - Dispositifs nomades interconnectés via le cloud (smartphones, tablettes)

Terminaux nomades, Réseaux Sociaux Numériques

- Mutation rapide conduit les entreprises à s'exposer de plus en plus
  - Accès à leurs infrastructures informatiques ainsi qu'aux données stratégiques

- Entreprises deviennent cible d'attaques informatiques (cybercriminalité) de plus en plus sophistiquées
  - Vol de données à caractère personnel ou professionnel,
  - Malveillances
    - Dysfonctionnement de systèmes, logiciels et réseaux
    - Atteinte à la réputation ou bris de carrière

- Désorganisation de l'entreprise visée
  - Intégrer le concept de sécurité globale permettant d'assurer
    - un niveau suffisant de prévention et de protection contre la cybercriminalité
    - Prendre en compte leurs obligations règlementaires et juridiques.

Cybercriminalité

- Problématique
  - L'accès à l'information numérique est de plus en plus facilité, grâce à la multiplication des terminaux d'accès, qu'il s'agisse des ordinateurs, smartphones ou tablettes.
  - De ce fait, les acteurs malveillants disposent de moyens de plus en plus ~~en~~ importants pour identifier, traquer les particuliers et les entreprises.
- Définition de la cybercriminalité
  - La définition donnée de la Cybercriminalité par le Ministère de l'Intérieur est : « l'ensemble des informations pénales commises sur le réseau Internet »
  - Elle semble malheureusement trop restrictive, car elle est commise par tout mode et moyens de communication

Risques Juridiques

- Les particuliers et les entreprises sont soumis à de nombreuses réglementations qu'il est important de connaitre. Ce cadre juridique constitue un premier niveau de sécurité pour les entreprises mais aussi un recours en cas de dommage.

- Par les particuliers (salariés), les infractions commises peuvent être :
  - Abus de confiance, usurpation d'identité,
  - Accès à des données privés en vu de mener du chantage
  - Violation du secret de fabrication
  - Compromission
  - Espionnage, l'intelligence avec une puissance étrangère

- Par les entreprises (DSI, RSSI)
  - Manquement à la sécurisation des données
  - Divulgation illicite de certaines données personnelles
  - Violation du secret professionnel
  - Complicité par assistance ou fourniture de moyens

Textes et réglementations liées à la Cybercriminalité

- Repose principalement sur deux types d'incriminations

- Intrusion sur les S.T.A.D
  - Elle concerne les dispositions de la Loi Godfrain n°88-19 du 05 janvier 1988 reprises dans les dispositions des articles 323-1 à 323-4 du Code Pénal.

- Réglementation CNIL
  - Elle concerne les dispositions de la Loi Informatique et Liberté n°78-17 du janvier 1978 reprises dans les articles 226-16 à 226-24 du Code Pénal.

- Convention Cybercriminalité 21.11.2001(STCE n°185)

Gestion d'un incident de sécurité

L'actualité met en évidence une sous-estimation des risques liés à la cybercriminalité par les PMI-PME, mais également par des sociétés plus importantes. Il se traduit par un absence de sécurité, de tests, etc..

Un Google Dork : Google multimon ups status page

Un accès à un SI :

http://ams.cern.ch/cgi-bin/multimon.cgi

Données facilement accessibles, hors ...

APCUPSD UPS Network Monitor
Sun Jan 13 08:12:17 CET 2013

System	Model	Status	Battery Chg	Utility	UPS Load	UPS Temp	Batt. Run Time	Data
ams	Smart-UPS 3000	ONLINE	100.0 %	227.5 VAC	27.9 %	22.9° C	15.0 min.	All data
ams backup	Smart-UPS 2200 RM	ONLINE	100.0 %	231.8 VAC	47.4 %	23.8° C	16.0 min.	All data
pcamso0	Smart-UPS 1000	ONLINE	100.0 %	231.8 VAC	48.1 %	21.6° C	25.0 min.	All data
NetworkSwitch	Smart-UPS 1500	ONLINE	100.0 %	231.8 VAC	13.0 %	33.3° C	55.0 min.	All data
pcamsf4	Back-UPS RS 1500	ONLINE	100.0 %	226.0 VAC	37.0 %	-	21.9 min.	All data
pcamsf3	Smart-UPS 2200 RM	ONLINE	100.0 %	231.8 VAC	21.4 %	21.6° C	44.0 min.	All data
scamsfs0	Smart-UPS 2200 RM	ONLINE	100.0 %	230.4 VAC	39.0 %	24.3° C	23.0 min.	All data
pcamsi01	Smart-UPS 2200 RM	ONLINE	100.0 %	223.2 VAC	40.3 %	23.4° C	19.0 min.	All data
pcamsf9	Smart-UPS 1500	ONLINE	100.0 %	231.8 VAC	0.0 %	27.0° C	433.0 min.	All data
scamsfs1	Smart-UPS 1500	ONLINE	100.0 %	233.2 VAC	35.1 %	24.7° C	36.0 min.	All data
pcamsi0	Smart-UPS 1500	ONLINE	100.0 %	228.9 VAC	58.5 %	30.6° C	21.0 min.	All data

Whois Lookup For ams.cern.ch:

```
[Querying whois.nic.ch]
whois: This information is subject to an Acceptable Use Policy.
See http://www.nic.ch/terms/aup.html


Domain name:
cern.ch

Holder of domain name:
CERN - European Organisation for Nuclear Research
Shade John
IT department - CS group
route de Meyrin
CH-1211 Genève 23
Switzerland
Contractual Language: English
```

Gestion d'un incident de sécurité

- Bilan
  - Aspects juridiques doivent être connus
  - Mise en place d'une politique de sécurité et d'un PCA / PRA en cas d'incident

- Actions doivent être compatibles avec une action judiciaire
  - Entreprises doivent se doter de « *response team* » pour répondre aux questions suivantes :

- De quoi s'agit il ? (*infraction, incident de sécurité ?*)

- Remise en œuvre des S.I (*oui, mais…)*

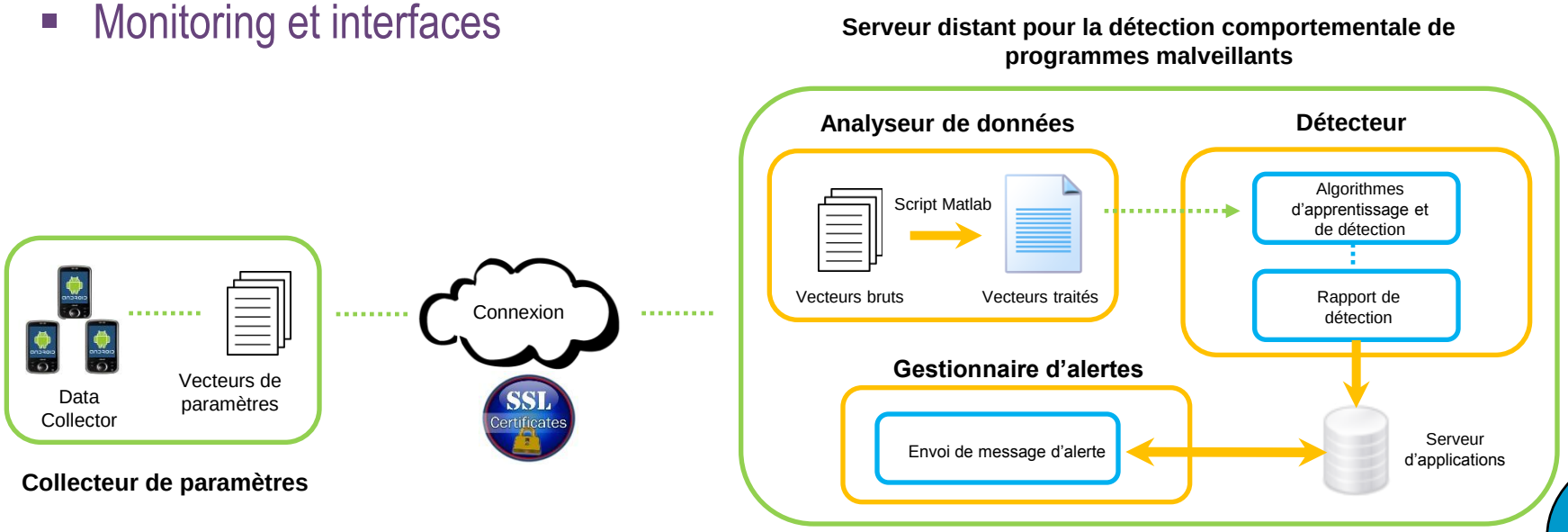
- *Collecte des éléments, analyse, (qui, comment?)*

Investigation numérique (Forensics)

- Définition de l'investigation numérique
  - Analyse post incident est l'ensemble des techniques visant à analyser un système informatique en vue de recréer une image des activités ayant eu lieu sur le Système d'Information
- Nécessite un processus d'analyse précis réalisé en 7 étapes (DFRWS) :
  - L'identification
  - La préservation
  - La collecte
  - L'examen
  - L'analyse
  - La présentation
  - La décision
- Elles peuvent être réalisées selon deux méthodes en fonction des faits
  - Post Incident
  - Live Forensic

Détection de malware : analyse comportementale

- Objectif
  - Développer une plateforme de surveillance / outil de diagnostic d'anomalies dans les smartphones
    - Approche comportementale. Détection sans signature du malware (code)
- Plateforme
  - Système de détection d'intrusions à distance
  - Surveillance par un client installé sur le smartphone (démonstrateur développé)
  - Monitoring et interfaces



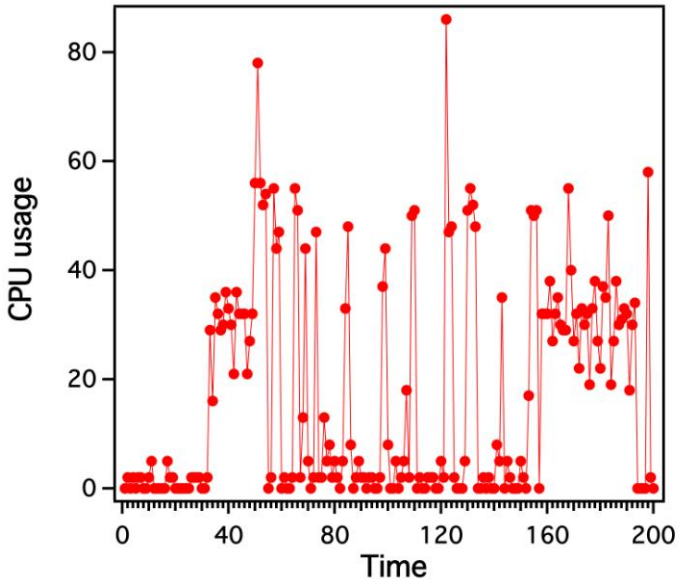
Méthodes et outils de sécurisation des données sensibles

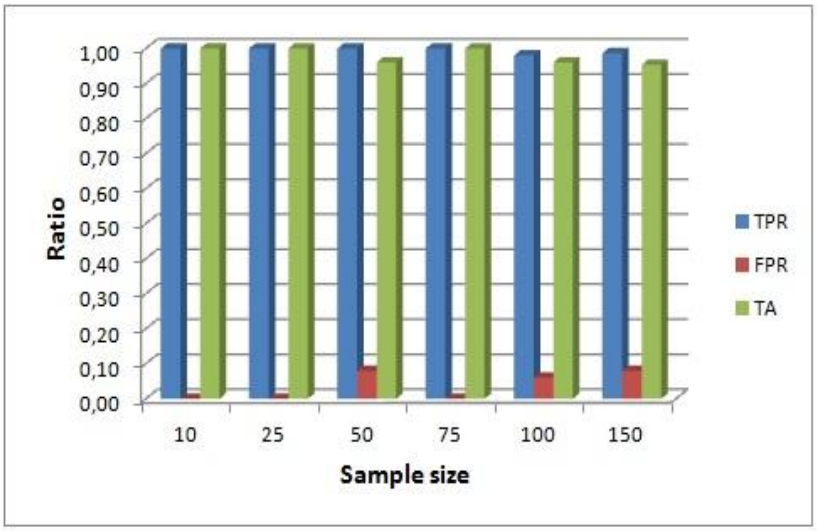
- Premiers résultats de diagnostic
  - Approche avec des Réseaux Bayésiens
    - Malware de test développé par une équipe de recherche à Linköping University
    - Comportement normal basé sur une enquête de 500 utilisateurs
    - Critères d'évaluation

$$TPR = TP/(TP + FN)$$

$$FPR = FP/(FP + TN)$$

$$TA = (TP + TN)/(TP + TN + FP + FN)$$



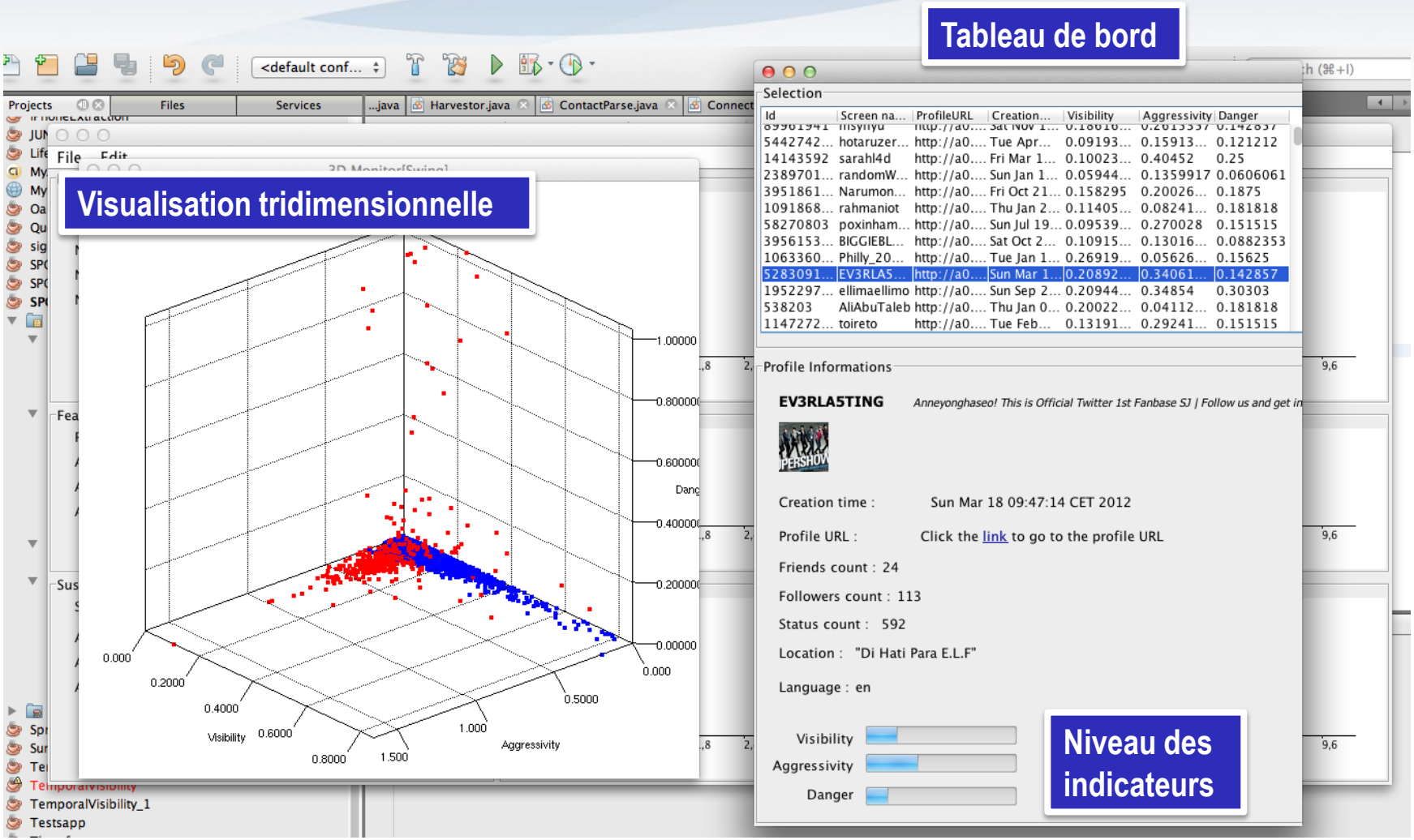


Réseaux sociaux numérique : approche globale
SPOT 1.0 (Scoring Suspicious Profiles on Twitter)

- Réseaux sociaux numériques : une opportunité pour les acteurs malveillants
  - Forte quantité d'utilisateurs (particuliers, professionnels)
  - Forte quantité de données (personnelles, stratégiques, etc.)

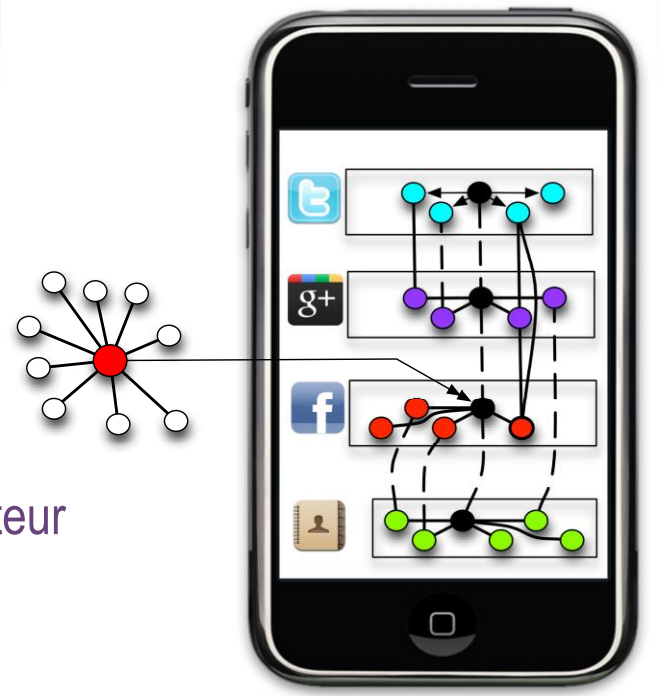
- Fonctionnement de l'outil SPOT 1.0
  - Collecte, traitement, détection et évaluation de profils malveillants sur Twitter
  - Repose sur des techniques de classification supervisées
  - Mesures de la virulence des profils
  - Visualisation sous forme d'outil d'aide à la décision

SPOT 1.0 (Scoring Suspicious Profiles on Twitter)
Etude de cas : détection de profil spammeur



Réseaux sociaux numérique : approche locale

- Analyse des contacts de l'utilisateur
  - Ceux qui ont un accès direct à vos données
  - Mesure de niveaux de confiance



- Modèle multi-couche
  - Représentation des interactions sociales d'un utilisateur de smartphone
  - Mise en évidence et extraction d'entités transverses
  - Mise en pratique sous forme d'application pour terminaux mobiles

Conclusion

- Différentes formes de la cybercriminalité → nous sommes tous concernés
  - Acteurs : citoyens, collaborateurs,
  - Systèmes : des smartphones aux systèmes industriels de type Scada

- Des outils de recherche
  - Méthodes comportementales de détection de malwares sur smartphones
  - Méthodes d'évaluation d'entités malveillantes sur les réseaux sociaux numériques

- Approche globale et intégrée
  - Prévention et protection des entreprises
  - Intégration des obligations réglementaires et juridiques
  - Outils et méthodes des organismes de l'état (police et gendarmerie)