Une plateforme unique en France

Expertise en Sécurité Informatique (audit, recherche de vulnérabilités...)

- Collecte et analyse de données
- Sécurité Réseau : P2P, analyse des requêtes DNS malveillantes
- SCADA : Analyse de protocoles, vulnérabilité
- Virologie: Analyse de binaires, Anti-Virus, Botnets

https://lhs.loria.fr

Une infrastructure physique dédié

- Environnement de travail séparé et « isolé »
- Contrôle d'accès renforcé
- Réseau cloisonné
- Possibilité de simuler un « Internet »
- DMZ pour la diffusion des résultats

Loria

Telescope réseaux

- Architecture multi-provider
- Architecture virtualisée et cloisonnée

- 583 525 376 attaques
- Dont **184 184 886 attaques malicieuses**
- 15 806 221 malwares téléchargés
- **295 177 binaires uniques** capturés

Quotidiennement

- 400 000 attaques dont 125 000 malicieuses
- **20 000 binaires téléchargés**

Base de données de codes malveillants

- **760 000 malwares**
- **Hébergeur de malware.lu : 6 millions de malware**

Traces réseau

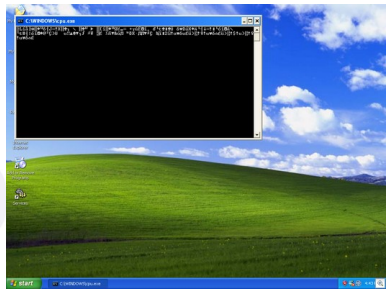
- **8,5 To de données PCAP**
- 110 Go de flux NetFlow
- 6 Go de flux Tor anonymisés

Loria

Une attaque typique

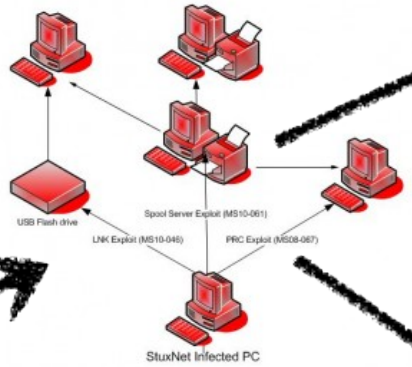
Ingénierie Sociale

Infection



0-day exploit
Faille de sécurité, i.e. un bug

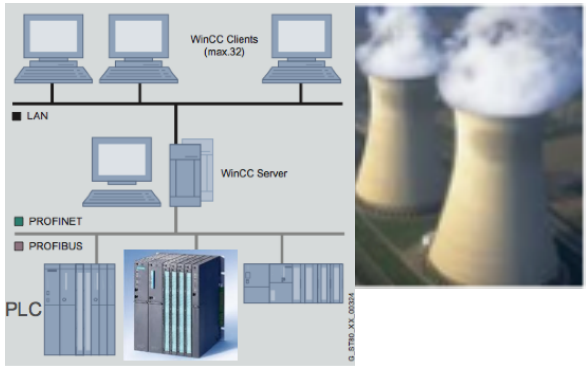
propagation
vol de certificats



Communication

vol d'informations
mise à jour ...

attaque ciblée



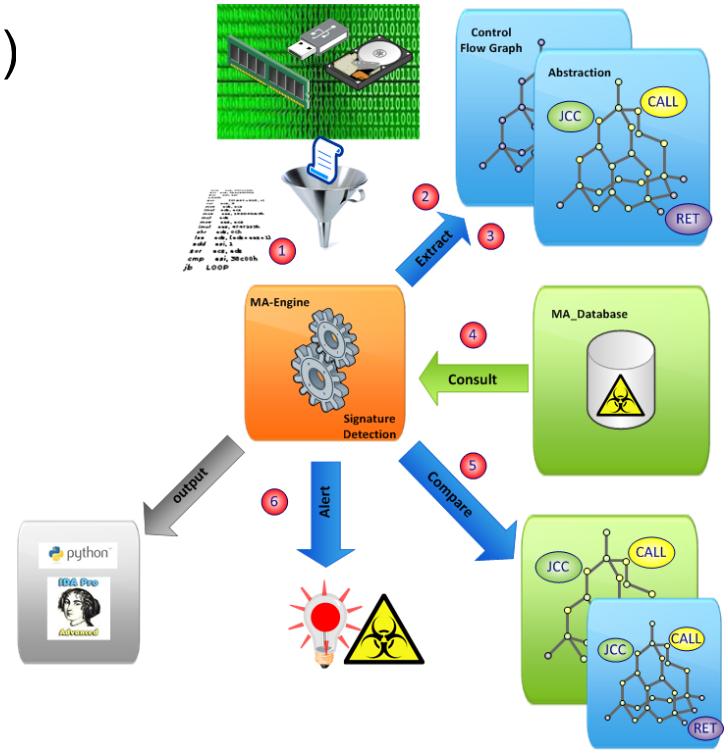
Historique
Début en Juin 2009
Activité Mars et Avril 2010
Connaissance en Juillet 2010

Loria

Virologie

Objectifs

- Analyse de codes malveillants (reverse)
  - Code obfusqué
  - Code auto-modifiant (95%)
- Identification de fonctions/librairie
  - Fonctions de crypto
- Visualisation et comparaison de codes
  - Ré-alignement sous IDA
- Détection des codes malveillants
  - Anti-Virus
  - Analyse morphologique
- Botnets



Détection de Duqu

Export functions	Numbers of nodes in the MA-signature of Duqu	Number of nodes matching Stuxnet MA-signature	Ratio	Time in ms
_1	959	605	63.09%	0.06
_2	1458	796	54.60%	0.09
_3	692	476	68.79%	0.04
_4	1212	655	54.04%	0.08
_5	2879	1397	48.52%	0.24
_6	937	613	65.42%	0.07
_7	1998	1079	54.00%	0.14
_8	959	605	63.09%	0.06
Dll EntryPoint	1248	945	75.72%	0.10

Alarme

Duqu est détecté à partir de Stuxnet par notre anti-virus

➡ *Scan de la mémoire*

➡ *Détection d'une mutation inconnue (Duqu) à partir de son ancêtre (Stuxnet)*

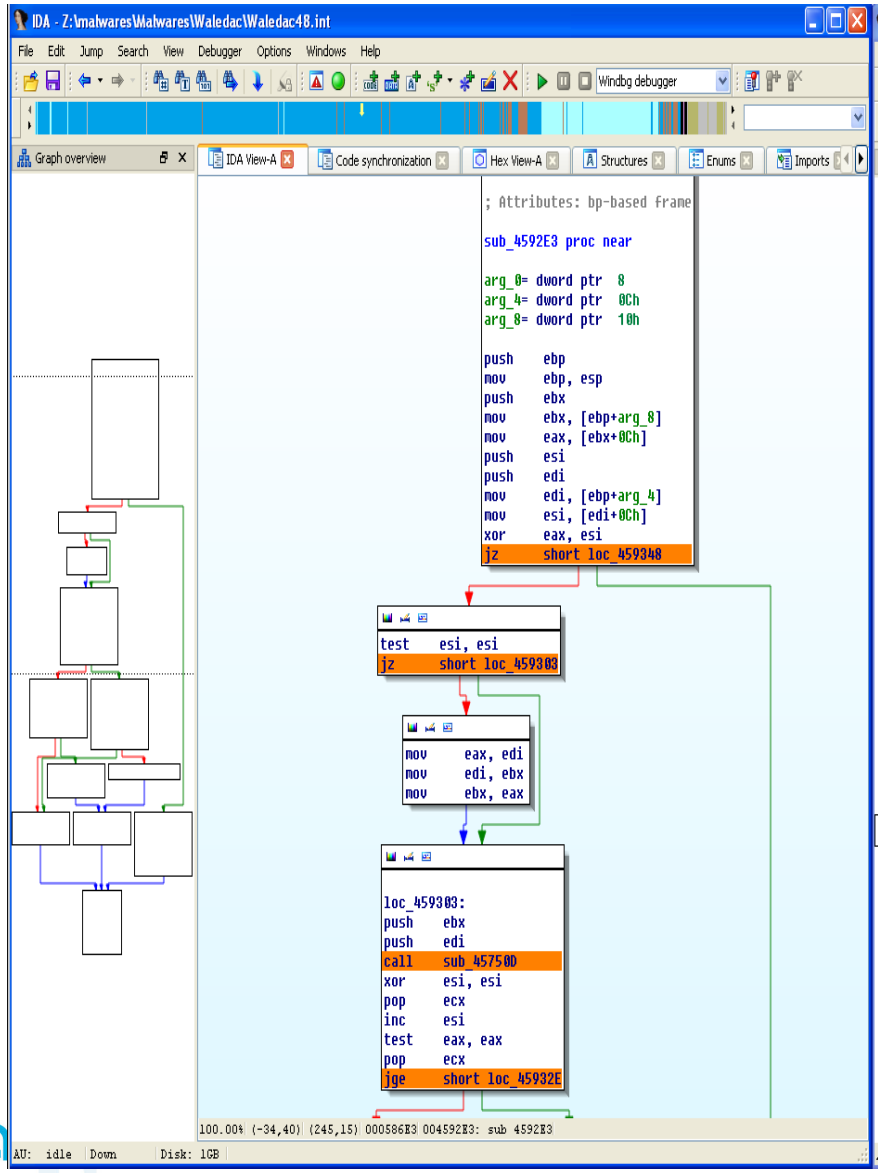
➡ *Faible taux de faux positifs*

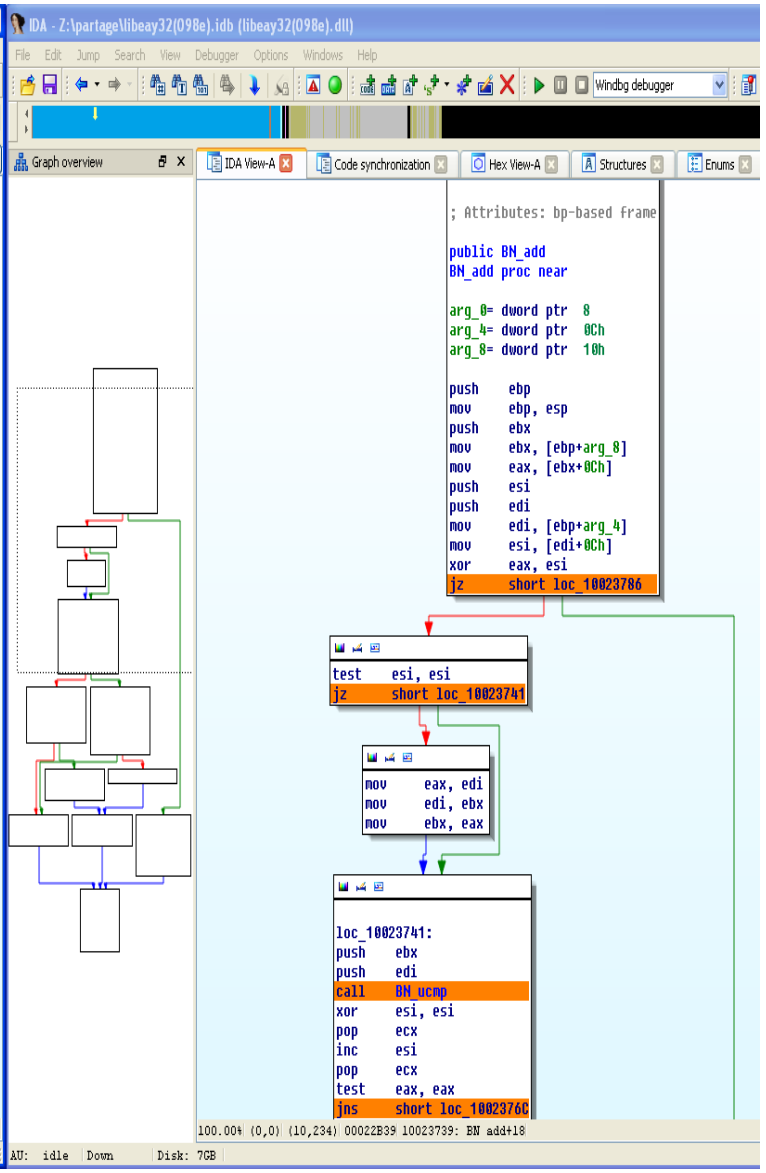
➡ *Reconnaissance des briques logicielles de même fonctionnalité*

Loria

Waledac sub_4592E3

OpenSSL BN_add





Team

•Guillaume Bonfante – guillaume.bonfante@loria.fr
•Jean-Yves Marion – jean-yves.marion@loria.fr
•Fabrice Sabatier – fabrice.sabatier@inria.fr

Doctorants:
•Aurélien Thierry
•Ta Thanh Dinh
•Joan Calvet