

# TP Threat Intel – Conception d’un outil de détection d’hameçonnage ciblé

georges.bossert@sekoia.fr

24 janvier 2018

## Objectifs de réalisation

Un flux d’information au format STIXv2 de sites d’hameçonnages ciblés.

## Format du TP

Travail en groupe (entre 2 et 4 personnes par groupe)

## Consignes

Imaginer, concevoir puis implémenter une solution chargée de détecter automatiquement des sites web utilisés dans le cadre de campagne d’hameçonnages ciblés. La solution retenue devra reposer à minima sur deux sources d’informations parmi les sources suivantes :

- CertStream Cali Dog Security ;
- Alexa Top 1 Million Sites ;
- Umbrella Popularity List ;
- VirusTotal : URL Abuse ;
- BGP Ranking / CIRCL.

Développé dans le langage de votre choix, votre solution stockera la liste des alertes de détection de sites web d’hameçonnage dans un fichier. L’alerte exprimée au format STIXv2 (type Indicator<sup>1</sup>) comportera à minima les informations suivantes :

- l’url du site web détecté ;
- l’heure exacte de la collecte de l’url.

Un dossier de conception sera rédigé et comportera les points suivants :

- les objectifs de votre outil (rappeler ce qu’est une attaque par hameçonnage ciblé) ;
  - repérer les sites de phishing souhaitant usurper les sites gouvernementaux.
- la liste des sources et services utilisés par votre solution et leurs descriptions succinctes ;
  - .csv comportant une liste des sites gouvernementaux référencés dans le monde : (url source) ;
  - une liste de mots clés en plusieurs langues, à élargir en fonction du nombre de matches possibles (assemblée, ambassade, ministère, impôt, président, taxe, passeport . . . ) ;

---

1. <https://oasis-open.github.io/cti-documentation/examples/indicator-for-malicious-url>

- geoAPI + circl ;
- virustotal.
- le fonctionnement général de votre solution.

## **Livrables**

Les livrables suivants devront être envoyés par email à l'adresse :

- un dossier de conception envoyé par email avant la fin de séance de TP ;
- le compte rendu final du TP comportant le dossier de conception, les résultat d'exécutions et les sources de l'outil. Il devra être envoyé au maximum 14 jours après la séance de TP (7 février 2018).

## **Evaluation**

En plus du respect des consignes, la créativité de la solution sera évaluée.