

IDS – DOSSIER DE CONCEPTION

KHOUBI Sina

BOUGAUD Yves

LEBRETON Mickaël



MASTER 2 CYBERSÉCURITÉ

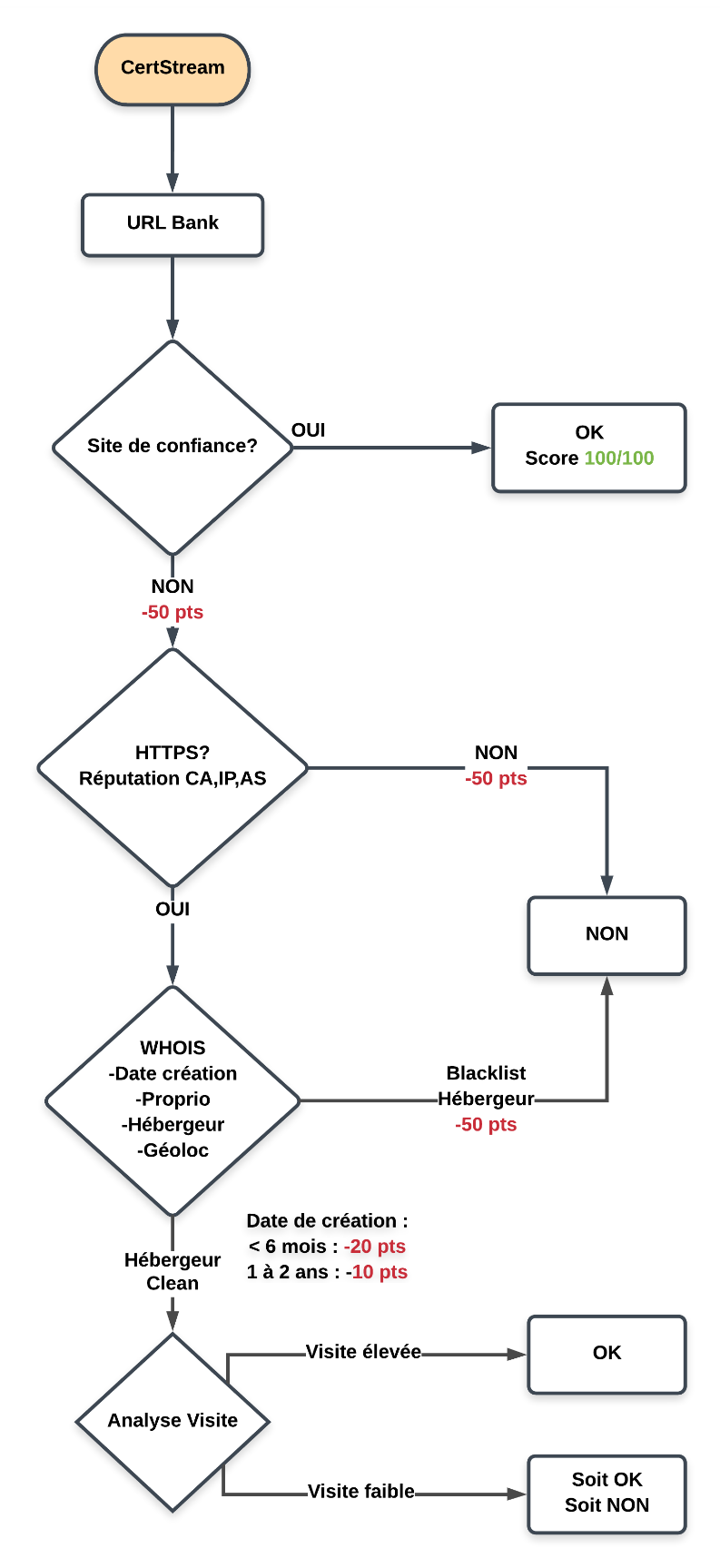
ISTIC – UNIVERSITÉ DE RENNES 1

2018-2019

# Introduction

Le but de ce TP est de développer un outil de détection, afin de détecter automatiquement des sites web utilisés dans le cadre de campagne d’hameçonnages ciblées. Nous utiliserons ici le langage Python. Nous nous restreindrons ici aux sites bancaires. Les sites auront au départ 100 points, qui diminuerons en fonction de nos vérifications sur l’URL.

# Processus de détection



Nous avons choisi certains critères que nous avions lister au début du TP, qui sont les suivants :

* Variation d’URL
* Date de réservation du nom de domaine
* HTTPS activé ou non
* Analyse des données de WHO.IS
* Réputation de l’hébergeur
* Analyse de la fréquence de visite du site

On a également choisi d’autres critères, qui seront implémenter en fonction de la performance de notre programme, pour améliorer les résultats.

Le CertStream nous renvoie plusieurs URL. Dans URL Bank, nous trierons ces URL avec des mots clés tels que « banque », « bank », ou encore « credit ». Une fois ces URL triées, si certaines contiennent une des mots clés, elle est envoyée à notre fonction de vérification de site de confiance.

En nous basant sur un fichier répertoriant presque tous les sites de banques, si l’URL appartient à cette liste, notre programme renvoie « OK », ce qui veut dire que le site n’est pas dangereux.

Dans le cas contraire, 50 points sont directement enlevés. Nous renvoyons ensuite l’URL vers une autre fonction, qui vérifie si l’HTTPS est activé. Si ce n’est pas le cas, 50 points sont encore retirés, pour arriver à 0. Le programme renvoie alors une alerte, car l’URL ne sera pas dans les sites de confiance, et n’aura pas l’HTTPS d’activé, donc il est très probable que ce soit un site dangereux.

Si l’HTTPS est activé, l’URL fera l’objet d’une analyse avec l’outil WHO.IS, afin d’obtenir plusieurs informations, telles que l’hébergeur (pour connaitre sa réputation), ou encore la date de création du site.

Plusieurs points pourront être retirés en fonction de ces résultats.

Enfin, nous effectuerons une dernière analyse sur l’URL, afin d’obtenir des statistiques sur les visites. Ceci nous permettra de savoir si c’est un site fréquenter ou non, et si c’est un site potentiellement dangereux ou non.

Nous enverrons ensuite le résultat avec le score.

# Code source

https://github.com/AsPhiXie/IDS