Projet de Fin d'Etudes
VAP SSR 2015

Lutte contre le phishing HTTPS

Institut Mines-Télécom

Auteurs

Florian CHEBRE

Arthur MAHE

Ressources

Encadrants

Joaquin GARCIA-ALFARO

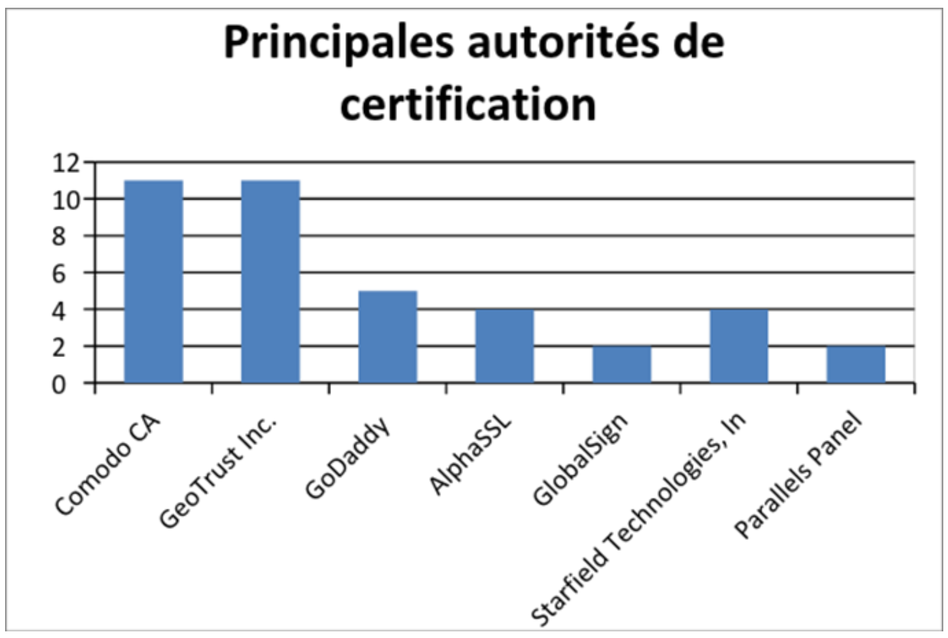
Gregory BLANC

I. Analyse et documentation

Phishing – Protocole SSL/TLS - Certificat

- Le protocole SSL/TLS est à la base du chiffrement des échanges en HTTPS. Pour établir une telle connexion, il y a deux phases : l'établissement d'un tunnel SSL puis le chiffrement de l'information.

- Les certificats, à la base de la confiance accordée par les internautes, sont de deux sortes : on trouve les sites à domaines propres (une gestion maitrisée de leurs certificats et de leurs ressources) et sites parasites (une gestion beaucoup moins flexible mais avec l'avantage de profiter d'un certificat reconnu et donc d'être beaucoup plus difficilement blocable).



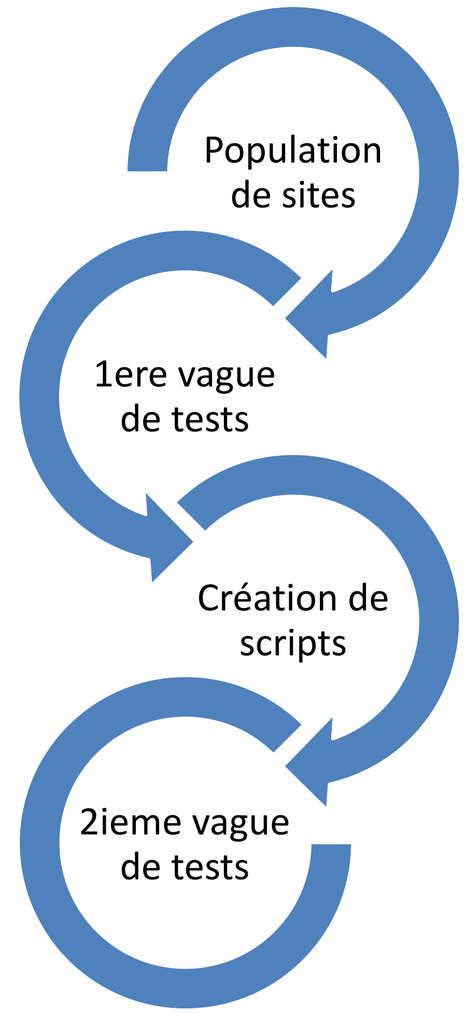
III. Les Contre-Mesures

Algorithme & Parades

- **Authentification forte :** Utiliser un secret partagé par le client et le serveur pour chaque connexion en plus du login. (Un attaquant qui obtient les identifiants par le bais d'un site de phishing ne pourra rien faire vu qu'il ne possède pas le secret partagé). Cela limite l'exploitation mais ne permet pas la détection des sites malveillants.

- **Algorithme de caractéristiques :** Un algorithme calcul un score en fonction des caractéristiques d'un site. Si le score atteint un certain pallier, alors le site est considéré comme dangereux. Cela permet de trouver des sites de phishing qui n'ont pas encore été placés dans une black-list ou dans une base de données utilisée par les navigateurs

- **Sensibilisation :** Sensibiliser les internautes sur la vérification des certificats, sur l'identification des sources non fiables dans les mails, etc.



II. Etudes statistiques

PhishTank – Analyse - Résultats

- **PhishTank** : site communautaire sur lequel les internautes votent sur la dangerosité des sites présumés de phishing.

- Le phishing **HTTPS** représente environ **50%** des sites de phishing selon notre étude basée sur deux vagues de tests.

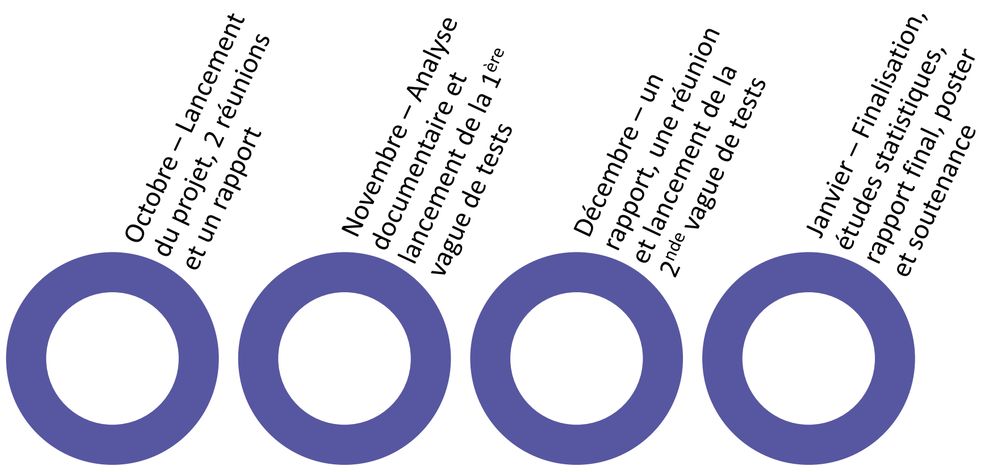
- Nous avons analysé **117** sites.

- **Comodo CA** et **GeoTrust Inc**. sont les deux principales autorités de certification que nous avons pu enregistrer. Ceci s'explique par le fait qu'ils permettent l'utilisation de leurs certificats sur un nombre illimité de machines.

- **Paypal** est la principale cible du phishing.

- Les sites de phishing ne sont **pas stables** dans le temps. Au cours du mois séparant les deux vagues de tests de notre étude, 12% des sites ont changé d'autorité de certification et 15% ont perdu leur certificat.

- L'étude du certificat d'un site permet de douter de son intégrité si son champ **« Identity »** est différent du nom de domaine.



Contact florian.chebre@telecom-sudparis.eu
arthur.mahe@telecom-sudparis.eu

Site web www.telecom-sudparis.eu