# Plateforme de confinement pour les bots HTTP


Institut Mines-Télécom

Auteurs

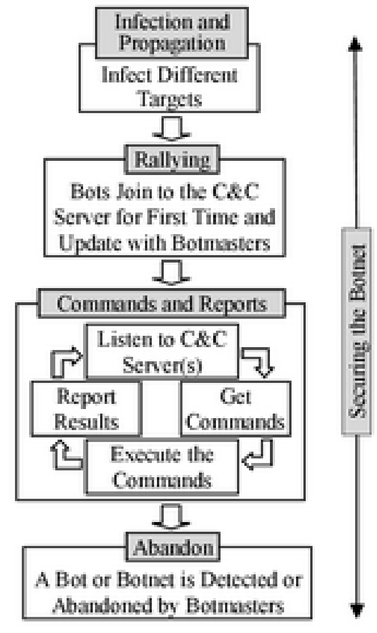
Alexandre FRANZ

Jérémy PARRIAUD

Encadrés par :

Gregory BLANC

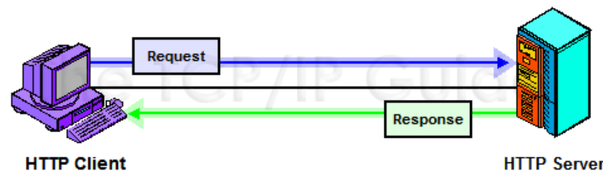
Joaquin GARCIA-ALFARO


## Les bots HTTP : une menace furtive

L'analyse des bots HTTP requiert un confinement préalable

- HTTP est un protocole fiable, surutilisé, sans état et chiffrable
- Il est couramment exploité par les malwares pour duper le filtrage




- Après exécution, le bot contacte son C&C sur un serveur web
- Le jeu des requêtes GET et POST assure une communication bidirectionnelle
- La machine zombie part en quête de sources douteuses : fichiers de configuration, outils logiciels, spywares…

- Ces URLs peuvent être analysées par une méthode de clustering développée dans un PFE précédent (A.V.)
- Encore faut-il pourvoir produire des trames HTTP malveillantes en toute sécurité !


Outils utilisés

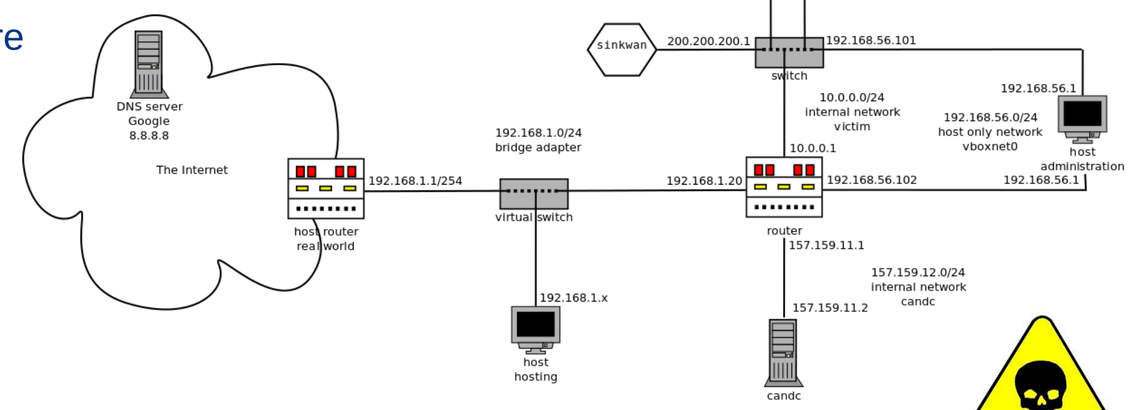



## Observabilité, Confinement, Efficacité

Notre plateforme reproduit un environnement d'émulation maîtrisé

- Un ensemble de machines virtuelles reproduit le scénario d'une infection
- Chacune implémente des couches logicielles fonction de son rôle
- Le bot s'épanouit, s'exprime et envoie des trames depuis les entités victimes
- Le réseau ainsi virtualisé canalise, filtre et capture les flux de communication
- Un script scapy récolte les URLs en fin de parcours

  - Une machine victime contient le malware
  - L'autre teste sa propagation
  - Le switch écoute les échanges
  - Le routeur simule un réseau interne
  - Le C&C contrôle et manipule le bot



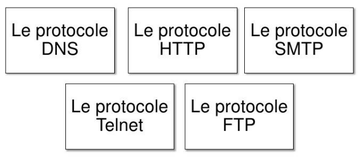

## Porter plus loin l'étude des malwares

Notre travail présente un potentiel prometteur

- Les logiciels utilisés sont gratuits et pérennes
- L'ensemble de notre outil est portatif
- L'installation et la manipulation sont grandement automatisables par des scripts
- Les snapshots de VirtualBox permettent de procéder par étape

- La plateforme est malléable, adaptative et sujette à de nombreuses améliorations
  - Interception du HTTPS
  - Reproduction d'un internet malveillant
  - Installation d'un honeypot
  - Elargissement de l'analyse à d'autres protocoles
  - Introduction de signatures d'attaques








Projet de Fin d'Etude

Janvier 2015



Contact Jeremy.parriaud@telecom-sudparis.eu

Site web rst.telecom-sudparis.eu