Génération d'attaques dans un environnement d'émulation de communications véhiculaires au sein d'un réseau cellulaire

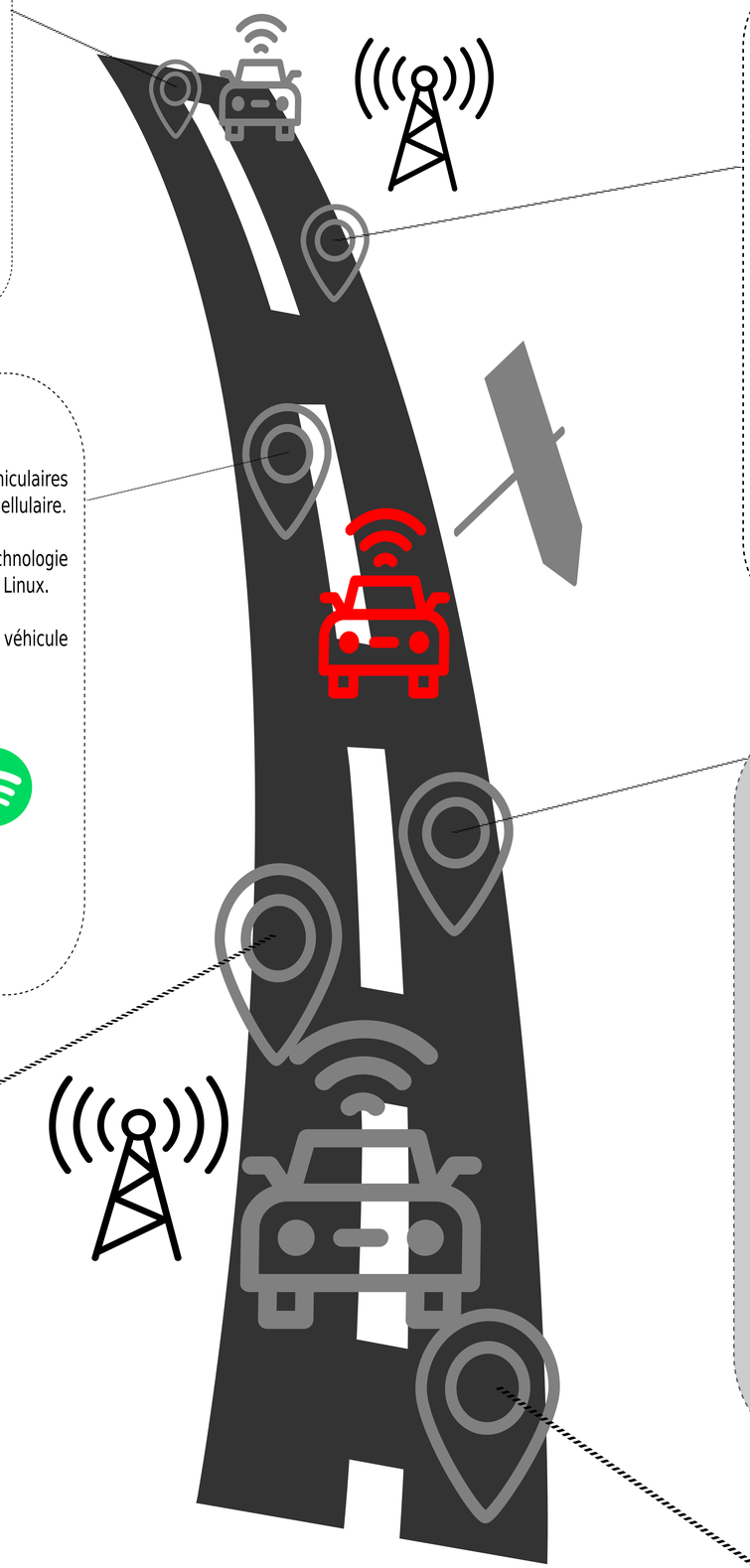
Etudiant: ANSER Omar, 4IR/TLS-SEC Encadrants: Quentin Ricard, P. Owezarski LAAS-CNRS

Contexte

Dans le cadre d'une thèse de doctorat dont la problématique est la détection d'anomalie en temps réel dans des communications véhiculaires au sein d'un réseau cellulaire, l'une des parties consistait à générer deux types de jeux de données réseaux :
Un premier correspondant à un scénario réaliste d'une utilisation légitime d'un véhicule connecté,
et un second, qui est conforme à une utilisation illicite.

Objectif

Apporter une contribution technique ainsi que, dans certains points, des propositions de solutions, afin de pouvoir finaliser ce volet.



Environement technique: AUTOBOT

- AUTOBOT est un environnement d'émulation de communications véhiculaires émulant le comportement de véhicules connectés au sein d'un réseau cellulaire.
- AUTOBOT est implémenté en Python et utilise DOCKER qui est une technologie de conteneurisation qui permet la création et l'utilisation de conteneurs Linux.
- Un conteneur représente le système d'infodivertissement d'un véhicule fonctionnant sous linux et intégrant un ensemble d'applications.

Contributions

Enrichissement du trafic réseau au sein d'AUTOBOT en développant le système d'infodivertissement avec deux applications : waze et spotify.

Le lancement de Spotify s'effectue à un temps paramétrable.

État de l'art sur:

- Les systèmes de communications embarqués des architectures actuelles des voitures connectées, incluant les procédés de communications internes et externes.
- Les principaux protocoles utilisés dans les communications véhiculaires au sein d'un réseau cellulaire.
- La sécurité des voitures connectées d'un point de vue réseaux et les principales vulnérabilités connues.
- Les méthodes d'exploitation des principales vulnérabilités des voitures connectées.
- Une introduction sur les méthodes de détections d'anomalies en temps réel.

GÉNÉRATION D'ATTAQUES

Problématique

Pouvoir créer une architecture depuis laquelle plusieurs types d'attaques peuvent être lancées.
L'architecture doit faire abstraction des types d'attaques générées, rendant ainsi la possibilité de les enrichir et de les diversifier.

Les types d'attaques à implémenter :
Scan, DNS tunneling and data exfiltration, ransomware, DDOS, remote exploitation.

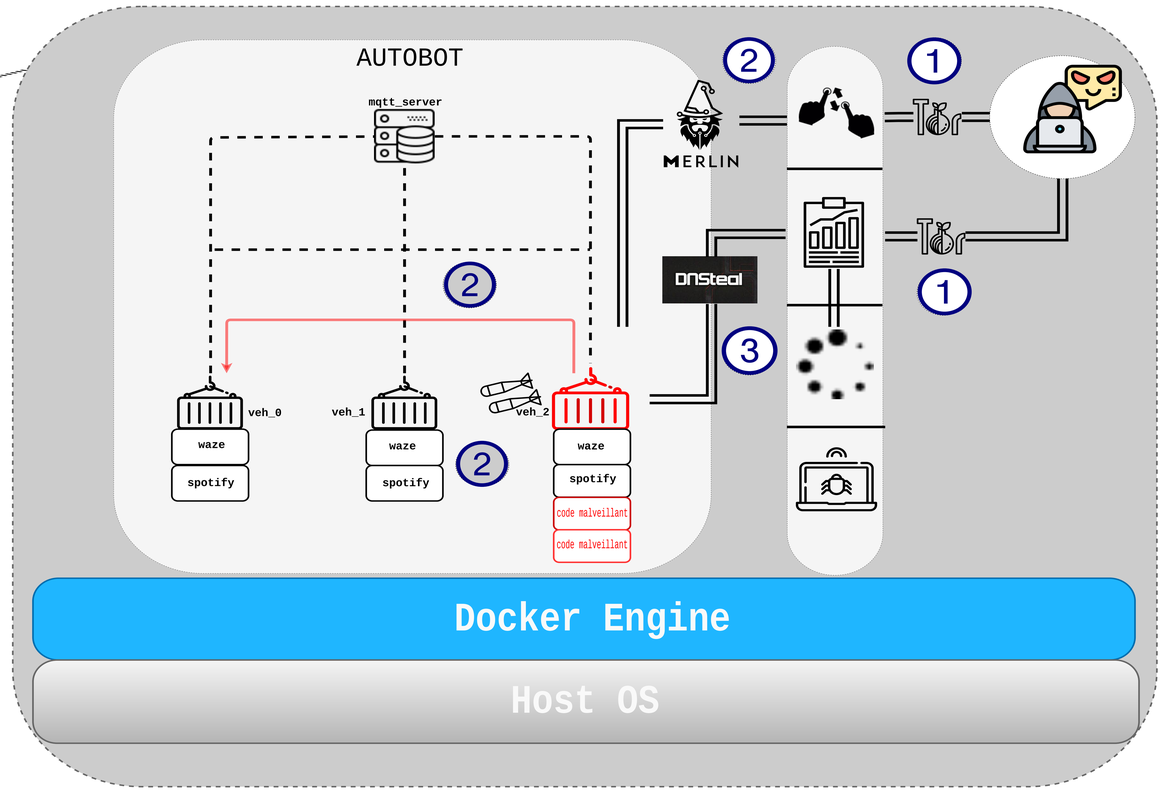
Réalisation

L'attaquant utilise plusieurs serveurs intermédiaires et communique avec deux d'entres eux à travers le réseau TOR, il est donc difficilement traçable et repérable.

Les scénarios d'attaques sont lancés par un attaquant, ce dernier dispose d'une boîte à outils (command and control server, loader server, report server ..) lui permettant de lancer les attaques implémentées.

Déploiement

1. L'attaquant se connecte, via SSH et à travers le réseau TOR, au command and control serveur (C&C) et au report serveur.
2. Depuis le C&C, l'attaquant contrôle un noeud du réseau (un véhicule ou autre) grâce auquel il va pouvoir soit effectuer un scan du réseau soit lancer des attaques sur des véhicules (DDOS, remote exploit).
3. Suite au scan ou à l'attaque exécutée, le noeud malveillant envoi un rapport de l'action effectuée au report serveur.
   Le loader serveur quant à lui utilise ces mêmes résultats pour tenter d'infecter un nouveau véhicule (en lui téléchargeant à son insu un malware ou un ransomware depuis un serveur distant)



Conclusion

Stage joignant l'aspect recherche et l'application de connaissances techniques.
Stage formateur sur:

- La méthodologie de la recherche scientifique (étude bibliographique et réalisation pratique).
- Des technologies et outils: Docker, dnscat2, merlin, dnsteal.
- Capacité à s'adapter rapidement à un nouvel environnement technique de travail.
- Le travail en autonomie.