Vortessence Core: Analyse de malware interactif avec détection d'anomalie automatisée

Filière d'études: BSc en Informatique | Orientation: IT-Security
Chargés: Prof. Dr. Endre Bangerter, Beni Urech
Expert: Dr. Joachim Wolfgang Kaltz

Les cyberattaques ciblées sont de plus en plus fréquentes. Les antivirus traditionnels sont relativement inefficaces contre ce genre d'attaque et des techniques pour les détecter ont été développés, l'une d'elles est l'analyse forensique de la mémoire. Vortessence est un outil qui a pour but de développer la discipline en offrant un outil qui permet d'automatiser du moins partiellement cette analyse.

Contexte

L'Analyse forensique de mémoire (RAM) est une technique qui est idéale pour la détection et l'analyse d'infection. Tous les logiciels qu'il soit légitime ou malveillant doivent être chargés en mémoire. Une fois, charger en mémoire un logiciel va inévitablement laisser des traces. Ces traces peuvent être analysées et des anomalies peuvent être identifiées. Cependant un analyste doit posséder de très bonnes connaissances en système d'exploitation et malware afin d'être capable de faire la différence entre ce qui est légitime ou malicieux.

Afin de rendre cette technique plus accessible, le projet «Vortessence» a vu le jour. Il est développé par le SEL(Security Engineering Labs) de la BFH. Le but de ce projet est d'automatiser, du moins en partie, l'analyse d'images mémoire. Il fonctionne par comparaison à l'aide d'une base de données de référence appeler «Whitelist». Cette base de données est peuplée avec des images de système qui sont a priori saines. Une fois notre base de données construite, on peut détecter des anomalies à l'aide de règle prédéfinie gérée par le «Rule Engine». Ceci fonctionne essentiellement en comparant les données de notre image cible avec notre base de référence. Bien évidemment, toutes les anomalies détectées ne sont pas nécessairement des signes d'infection. Mais c'est une façon de filtrer une grande partie des données.

Objectif

Le but de ce travail est de créer une version 2.0 du logiciel, avec notamment deux catégories à améliorer: le noyau et l'interface utilisateur.

Les améliorations du noyau se traduisent par des améliorations de performance et efficacité. Pour ce qui est de l'interface utilisateur, une nouvelle interface web plus compréhensible ainsi qu'une API en python permettent l'accès aux données.

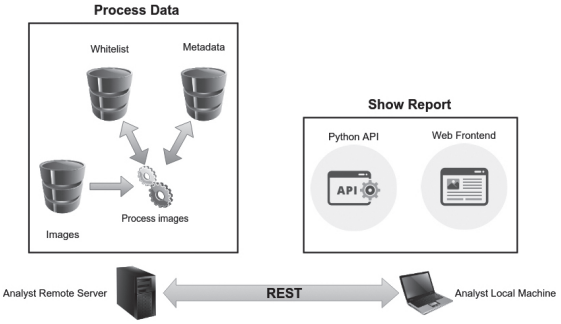
Les nouveautés du noyau:

- Un nouveau système de prétraitement permet à un utilisateur d'avoir accès aux données plus rapidement, accélérant le flux de travail.
- Un système de filtrage par entropie permet de comparer des données similaires, réduisant les faux positifs et détecter si des anomalies similaires se répandent à travers les processus.
- Le noyau a été découplé de son interface via une REST API

Les nouveautés UI:

- Une interface web entièrement refaite afin d'utiliser la REST API.
- Une petite API en python permet l'utilisation des données de Vortessence avec une console interactive Jupyter/Iphython ou autre.

Christian Das Neves



Nouvelle architecture

Capture d'écran de la nouvelle intérface