File Carving & Memory Forensics

Domaine spécialisé: IT-Security
Chargé: Dr. Endre Bangerter
Expert: Reto Inversini (MELANI)

L'expansion des logiciels malveillants ne cesse de s'accroître, et l'utilisation massive des moyens de communication modernes, notamment des smartphones accentue la tendance.
Le but de ce projet est de développer un logiciel s'appuyant sur une nouvelle approche dans le domaine de l'étude de malwares, en associant la technique du file carving à l'analyse de mémoire.

Analyse de logiciels malveillants

Actuellement, un malware analyst dispose de deux techniques principales pour l'étude d'un logiciel malveillant: l'analyse statique et dynamique.
Dans le cas d'une analyse statique, l'objectif est de récupérer le maximum d'informations sans exécuter le malware. On va essayer d'identifier des structures à l'intérieur du programme, ou utiliser un désassembleur pour analyser le code. Cela peut se révéler très efficace, mais montre rapidement ses limites en présence de malwares complexes.
L'analyse dynamique vise à exécuter le malware pour comprendre son comportement. On observe alors les interactions entre le malware et le système sur lequel il s'exécute. Il y a toutefois un risque de ne pas observer certaines fonctionnalités, car certains malwares modifient leur comportement losrsqu'ils se sentent analysés.

Memory forensics

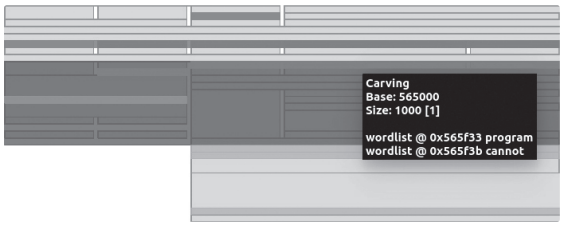
Cette technique fait partie de la catégorie de l'analyse dynamique, et étudie la mémoire utilisée par un logiciel malveillant. Cette technique permet de retrouver des informations en clair, alors qu'elles étaient offusquées ou chiffrées avant exécution en RAM. Il est toutefois actuellement difficile de trouver précisément des informations recherchées, principalement dues à la quantité à traiter.

Carving

La technique du file carving, ou simplement carving est une technique d'analyse qui recherche des fichiers ou tout type d'information dans une région mémoire basée sur le contenu plutôt que sur les métadonnées. À l'origine utilisée pour retrouver des données sur un disque dur, elle sera dans ce projet étendu à l'analyse de mémoire.
Le file carving s'opère en recherchant la structure des fichiers voulus. Cela peut se faire en cherchant le début/fin d'un fichier dans une portion mémoire, des constantes propres à un type de données, d'entropie, ou encore en observant la taille de régions mémoires.

Visualisation

La solution développée ajoute une dimension graphique aux résultats et donne une perspective intéressante, aidant à une représentation générale du comportement d'un processus étudié. En effet, le programme permet d'afficher les artefacts contenus dans la mémoire pour une analyse facilitée. La figure ci-dessous illustre l'affichage d'un fichier exécutable au sein de la mémoire.



Représentation d'un fichier exécutable en mémoire

En pratique

Le logiciel développé est fonctionnel et répond au cahier des charges donné en début de projet. Il donne un nouveau moyen d'analyser le contenu de la mémoire à partir de données capturées depuis la RAM, aidant les analystes dans l'étude de malwares. En exploitant et en faisant évoluer un environnement performant, il a su trouver sa place en amenant de nouvelles possibilités.
Ce projet répond à la problématique de l'aiguille dans une botte de foin, dans le contexte de l'analyse de mémoire. À savoir: comment retrouver précisément certaines informations dans une immense quantité de mémoire: La méthode du carving appliquée à la mémoire virtuelle d'un processus permet de connaître précisément son contenu, de manière dissociée de toute autre donnée.
L'ajout graphique aide à se représenter le contenu de la mémoire d'un processus, et d'avoir une vision d'ensemble de son évolution.

Damien Schaeffer
schaeffer.dami3n@gmail.com