

TP 4 Guillaume Sanchez

Nous allons déterminer dans ce TP les avantages et inconvénients de l'analyse statique et dynamique et établir une liste logiciels gratuits.

Analyse statique

En termes d'avantages, l'analyse statique ne nécessite pas l'exécution du code malveillant, ce qui réduit le risque de contamination du système d'analyse. Elle est généralement plus rapide que l'analyse dynamique car elle ne nécessite pas l'exécution du code. Elle est efficace pour détecter les signatures connues de logiciels malveillants. Elle permet une inspection approfondie du code, des métadonnées et des ressources du fichier.

En termes d'inconvénients, l'analyse statique peut être limitée à cause de l'obfuscation qui consiste à protéger la vie privée sur internet, peut rendre l'analyse statique inefficace. Elle peut également générer des faux positifs en identifiant des éléments bénins comme malveillants. De plus, elle ne peut pas observer le comportement réel du logiciel malveillant en cours d'exécution ce qui limite grandement l'analyse d'un malware en action.

Analyse dynamique

En termes d'avantages, l'analyse dynamique permet d'observer le comportement réel du logiciel malveillant en cours d'exécution. Elle est efficace pour détecter les comportements malveillants qui ne sont pas visibles dans le code statique. Elle peut détecter des variantes de logiciels malveillants inconnues ou complexes.

En termes d'inconvénients, l'analyse dynamique peut créer un risque de contamination, en effet l'exécution du code malveillant peut infecter le système d'analyse. Etant donné qu'on étudie un logiciel malveillant pendant son exécution, elle demande plus de temps et de ressources et est donc en général plus coûteuse. L'analyse dynamique peut également être détectée par les logiciels malveillants qui en réponse vont arrêter leur exécution avant d'être étudié.

Les logiciels gratuits

Logiciel	Description	Type d'analyse
Wireshark	Analyseur de protocole réseau pour capturer et analyser le trafic réseau	Dynamique
PeStudio	Outil pour identifier et mettre en quarantaine les fichiers suspects	Statique
Cuckoo Sandbox	Environnement de sandbox pour analyser le comportement des logiciels malveillants	Dynamique
Ghidra	Outil de désassemblage et de traduction des logiciels malveillants en code lisible	Statique
Process Hacker	Outil pour surveiller et analyser les processus en cours d'exécution	Dynamique

Source : <https://www.varonis.com/fr/blog/danalyse-des-malwares>