

TP 7 Guillaume Sanchez

Quelle norme ISO convient-il d'utiliser pour réaliser une analyse statique ou dynamique ? Et pourquoi est-ce nécessaire ?

Salut

Analyse statique de procexp.exe contenu dans la Suite Sysinternals :

- Nom du fichier, taille, date de compilation, propriétaire, ...

File Name	C:\Users\Utec\Downloads\SysinternalsSuite\procexp.exe
File Size	4.32 MB (4531120 bytes)
Created	Tuesday 28 May 2024, 16.11.02
CompanyName	Sysinternals - www.sysinternals.com

- Signature (hash), quelle est son utilité ?

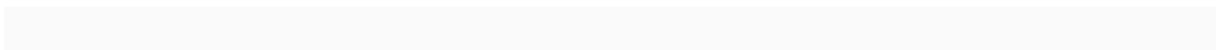
MD5	94C60E6704B5DD11A139F2FFEBDE9135
SHA-1	CD89F1CF9428A3EAB554A3EB9FF6CA869E5BC368

L'utilité d'une signature est de garantir son authenticité, que le fichier n'a pas été modifié ou n'a été corrompu.

- Examinez Les chaînes de caractères (Unicode, ASCII), trouvez-vous des informations intéressantes et pourquoi le sont-elles ?

On peut retrouver plusieurs types d'information, par exemple on peut y retrouver les fichiers de configuration, des scripts et des données. Naturellement on y retrouve toutes les métadonnées comme les informations sur l'auteur, des descriptions et des commentaires. On peut y retrouver également des paramètres de configuration, des chemins de Fichiers en URLs des informations de Profilage etc.

- Les interactions que l'outil peut avoir avec le SE (ex: création de clé registre,...) ?



Oui on peut voir des chaînes comme `HKEY_LOCAL_MACHINE\...` qui indiquent que le programme accède à une clé de registre spécifique ou encore des chemins comme `C:\Program Files\...` indiquent que le programme lit ou écrit dans un fichier de configuration.

Vous analyserez le fichier (AffichezMoi) mis à disposition par la secrétaire. Le fichier ne s'ouvre pas.

On peut voir à l'aide du logiciel CFF Explorer, qu'en réalité il ne s'agit pas d'un PE donc il est normal que le fichier ne s'ouvre pas.