After being introduced to Volatility and Yara Rules during my masters I realised that the plugin yarascan would only run a file of Yara Rules at a time, however there could be the need to use multiple files of rules to do a preliminary diagnostic to the memory image and understand which family of malware it could be infected with.

In my thesis I decided to address this problem by developing a plugin that makes use of yarascan but can run more than one file on the same memory image, with this plugin there is also the intent to make easier for beginners to start to use both Volatility and Yara Rule since the usage of this module is quite simple.

When we use this plugin to run multiple files it puts all the results and their respective CSV file, was also added some repositories with rules from different sources on GitHub.

In the images below we can see the running of the main command to run the files and its results, these were just some dummy files that were used to test the plugin along the development.

This plugin was also developed with the intent to be used with Volatility 3 and Python 3.

There is README file that goes along with this document with the instructions as how the module works and what it needs.

Uma imagem com texto

Descrição gerada automaticamente

Figure 1 Execution of plugin in Windows

Uma imagem com mesa

Descrição gerada automaticamente

Figure 2 Result of one of the Yara Rules files run with the previous execution

This plugin simplifies the use of the yarascan and if we have the need to run multiple files of rules it cuts the time spent on it by using this plugin instead of running them by the native method through yarascan, therefore helping analysts in their work since they can even prepare their own package of rules and run them in memory images with unknown malware to see if it matches with any of it, and that’s one of the main reasons I think it should win since it’s a plugin that would help optimise and automate some work that would have to be done by the analyst.

In the table below it can be seen a comparison of time in seconds of how long it would take to run a respective number of files.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Amount of Files | | | |
|  | 1 | 2 | 4 | 8 |
| yarascan | 33s | 60s | 66s | 102s |
| Developed plugin | 28s | 28s | 33s | 45s |

There is also the simplicity of it that could help beginners start to use Yara Rules that they can even get from the repositories that were included in this plugin.