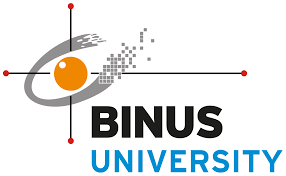
Volatility2 Standalone

Shylock.vmem



Group Members :

Ruben Pangestu (2502010950)

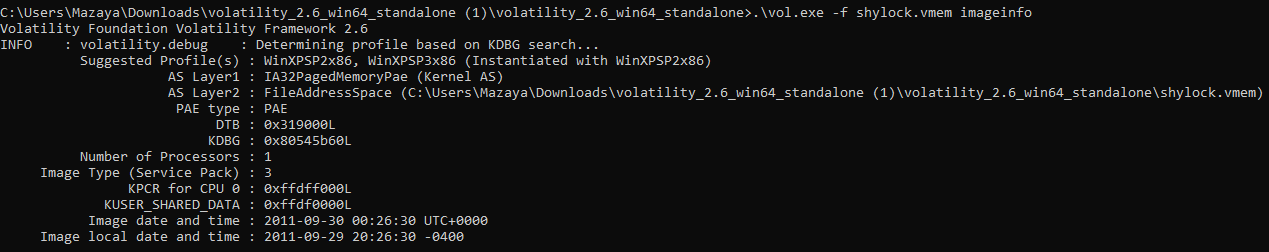
Muhammad Mazaya R S (2502005723)

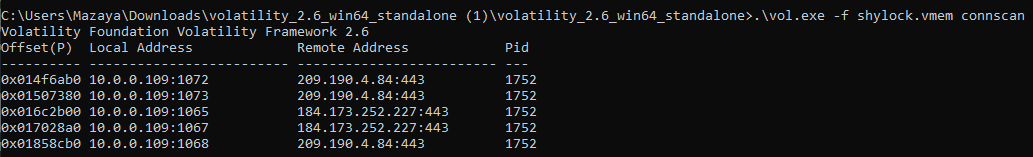
Marvell Rivandy (2502003844)

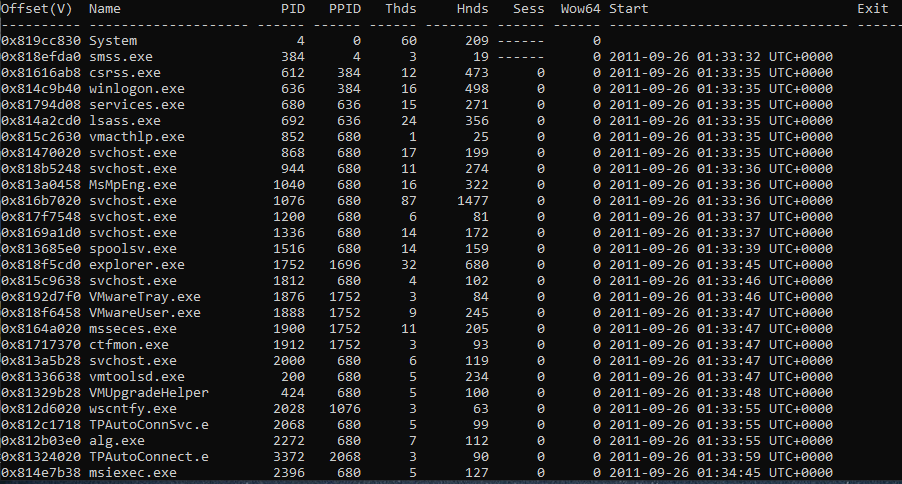
David (2501994506)

Ronan Sundjojo (2502007382)

We are going to analyze shylock.vmem with volatility2 standalone/

First of all, we try to see the general information.

We then check the network connections.

After that er check all the processes that were running in the memory

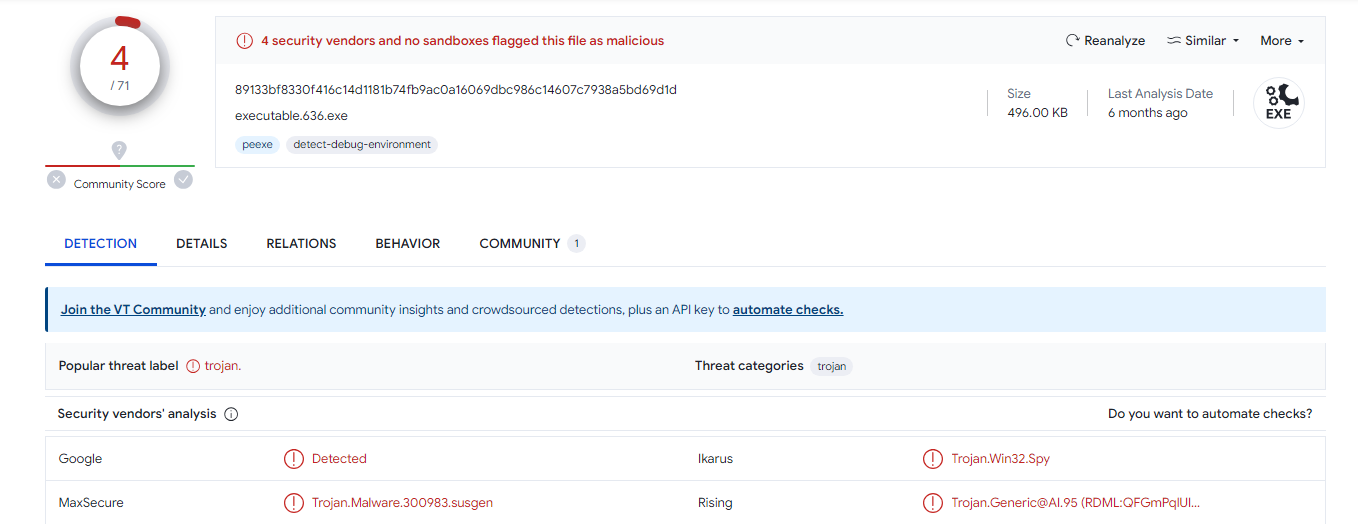
We still cannot find anything unusual.

So we try to find the executable that modified the memory.

We found several executables that modified the memory, lets just use this winlogon.exe as an example.

Lets now do a dlldump

These are the output files that are not empty.

We can then scan it with virustotal.

This is the scan result from one of the files.

It looks like it is a trojan.

Lets try another one, this time explorer.exe

