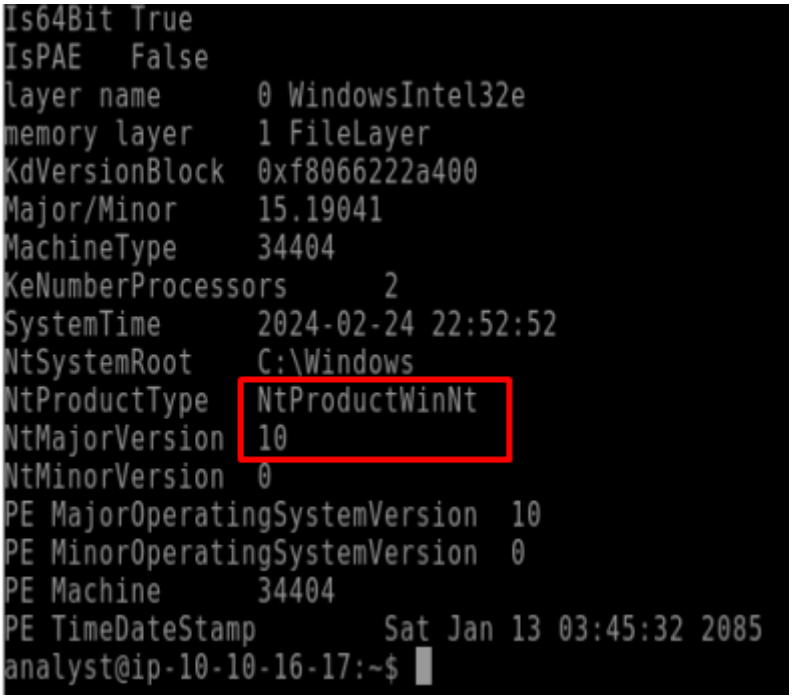
ANÁLISIS FORENSE – TRYTOHACKME MEMORY WINDOWS - CASO 04

Incident Scenario

Our user "Hattori" has reported strange behavior on his computer and realized that some PDF files have been encrypted, including a critical document to the company named important_document.pdf. He decided to report it; since it was suspected that some credentials might have been stolen, the DFIR team has been involved and has captured some evidence. Join the team to investigate and learn how to get information from a memory dump in a practical scenario.

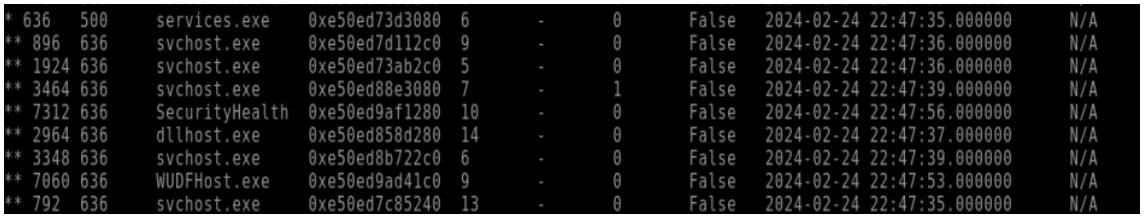
1.- Sistema operativo del volcado de memoria

$ vol -f memdump.mem windows.info

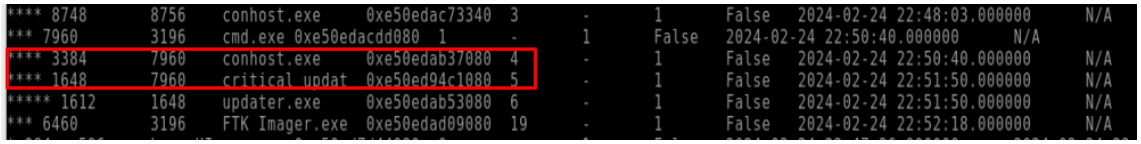


2.- Procesos sospechosos en el sistema

$ vol -f memdump.mem windows.pstree

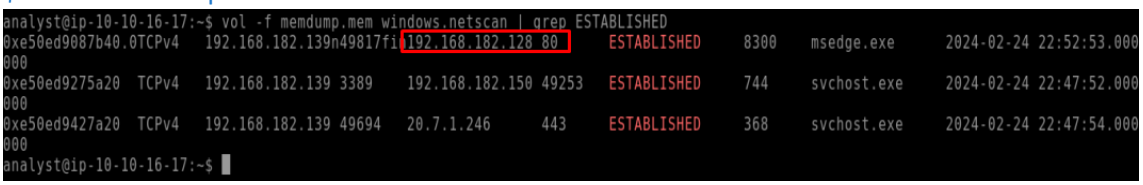


$ vol -f memdump.mem windows.pstree | grep critical -B 2



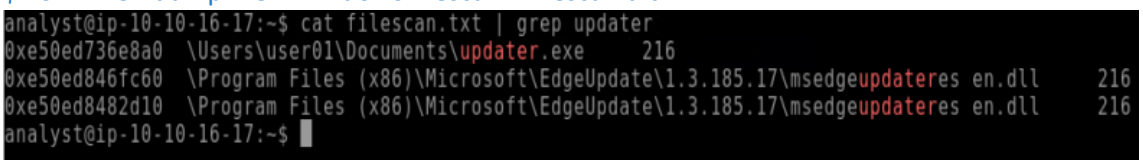
3.- Procesos de red activos en el sistema conectado al puerto 80

$ vol -f memdump.mem windows.netscan



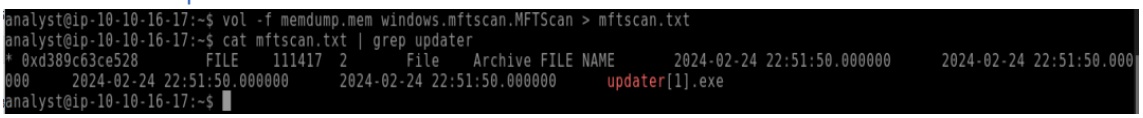
4.- Ficheros que se han accedido o ejecutado en el sistema

$ vol -f memdump.mem windows.filescan > filescan.txt



5.- Ficheros que se han accedido o ejecutado en el sistema

vol -f memdump.mem windows.mftscan.MFTScan > mftscan.txt

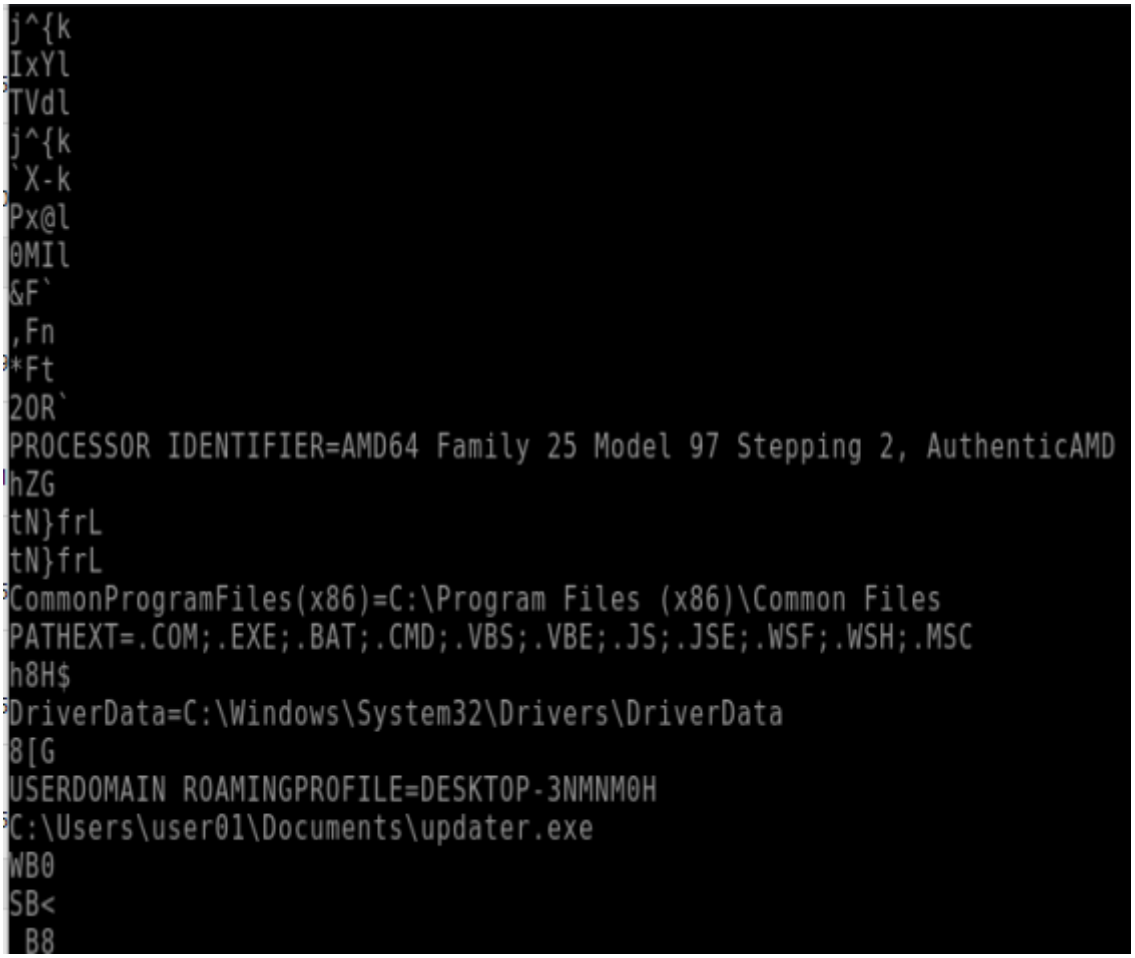


6.- Volcado del proceso pid 1612 updater.exe

$ vol -f memdump.mem -o . windows.memmap --dump --pid 1612

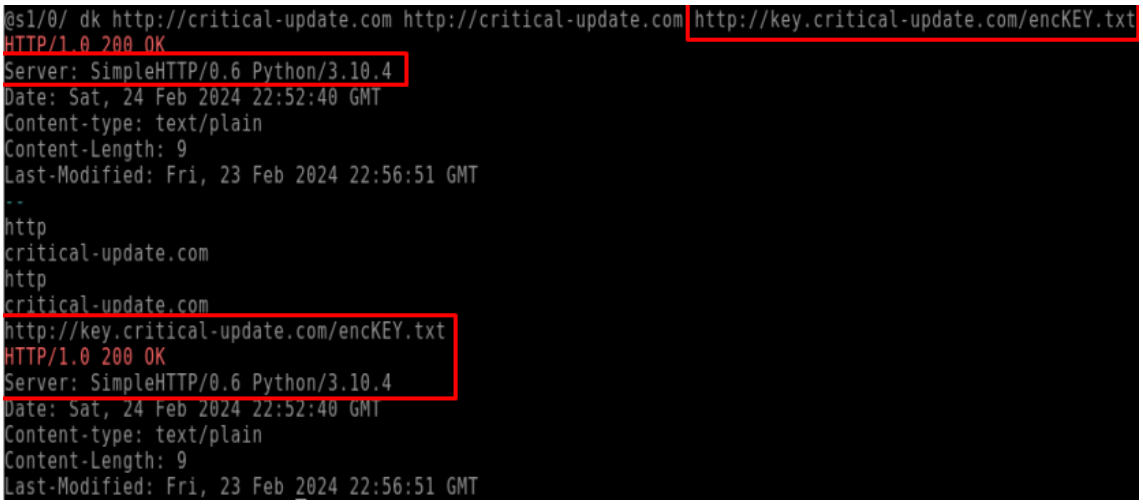
7.- Buscamos strings en el proceso pid 1612

$ strings pid.1612.dmp | less



Veamos peticiones http con resultado OK

$ strings pid.1612.dmp | grep 'HTTP\/1\.0 200 OK' -C 5



Recursos:

https://tryhackme.com/r/room/critical

Volatility 3