Virtual Machine : Ubuntu12.04(32 bit)
Malware Analyzed : Ransomeware.Rex
Source code URL:
https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Rex/

1) How did you make volatility work, and how did you dump the memory?

Steps to make the volatility work and taking memory dump :

1. Install volatility in your virtual machine as well as the base machine.

2. From your base machine open the terminal and type in the following command to take the memory dump before installation of malware. "vboxmanage debugvm Ubuntu12.04 dumpvmcore BEFORE.DUMP". Make sure to take the memory dump while your virtual machine is in running state.

3. Since the base machine doesn't come with a profile which is required for the analysis of memory dump just created ("BEFORE.DUMP"). We need to create a profile from the virtual machine and paste it to the destination folder in the base machine where the python script "vol.py" is located.

The following steps need to be conducted on the system being examined:

1. Install dwarfdump. For Ubuntu-based systems use command apt-get install dwarfdump
2. Copy the tools/linux subfolder from within the volatility tarball up to the system being examined(the base system).
3. Build the module.dwarf file by typing make within the tools/linux folder that you copied in step 2. This should create a file named module.dwarf in the same folder.
4. Copy the System.map file for the system under investigation into the same folder where the module.dwarf file is located.
5. Create a zip file containing the module.dwarf file and the System.map file: zip Ubuntu1204.zip module.dwarf System.map
6. Copy this zip file off to your examination workstation, along with the memory dump. This zip file is the profile for your system that contains the information about the kernel data structures and symbols. Volatility will use it to parse out and interpret the memory dump created previously.

4. The profile created using the above step is to be added to the base machine by pasting to the folder tools/linux inside the base system. (Command to verify the created profile : "python vol.py --plugins=tools/linux –info " from the base machine where vol.py is located.) It will display the name of profile added to the machine, in my case : profile=Linuxubuntu1204x86

5. Next step is to download the Ransomeware.Rex.zip from the URL and save it the virtual machine.

6. The next most important move is to turn off the network capabilities inside your virtual machine as we do not want the malware to go out of the sandbox and infect our base machine in any manner.

7. Unzip the malware file and execute it on the virtual machine. To analyze the post effect try to take the memory dump while the malware is in running state. Take the memory dump after installation "AFTER.DUMP" again from the base machine.

(2) What kind of malware you have analyzed?

Malware analyzed is Ransomeware.Rex a linux based virus.

(3) What observations did you make from the malware analysis

Observations are made based on following metrics:

- linux_pslist - Gather active tasks by walking the task_struct->task list

  Found the entries corresponding to WTEpZSFwgb with PID 2122

  python vol.py --plugins=tools/linux --profile=Linuxubuntu1204x86 linux_pslist -f AFTER.DUMP>AFTER_PSLIST.txt

- linux_netscan - Carves for network connection structures

  python vol.py --plugins=tools/linux --profile=Linuxubuntu1204x86 linux_netscan -f AFTER.DUMP > AFTER_linux_netscan.txt

- linux_netstat - Lists open sockets

  python vol.py --plugins=tools/linux --profile=Linuxubuntu1204x86 linux_netstat -f AFTER.DUMP > AFTER_linux_netstat.txt

- linux_psscan - Scan physical memory for processes

  Found the entries corresponding to WTEpZSFwgb with PID 2122

  python vol.py --plugins=tools/linux --profile=Linuxubuntu1204x86 linux_psscan -f AFTER.DUMP > AFTER_linux_psscan.txt

- linux_bash_env - Recover a process' dynamic environment variables

  Found the entries corresponding to WTEpZSFwgb with PID 2122

  Command: python vol.py --plugins=tools/linux --profile=Linuxubuntu1204x86 linux_bash_env -f AFTER.DUMP > AFTER_linux_bash_env.txt

- linux_memmap - Dumps the memory map for linux tasks

  Found the entries corresponding to WTEpZSFwgb with PID 2122