Impfuzzy

Information Security Inc.

Contents

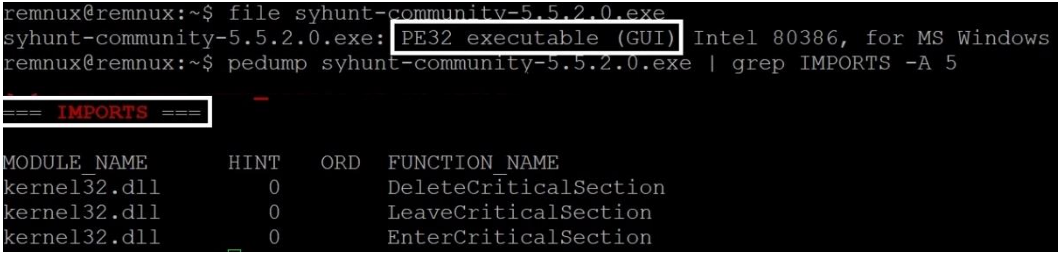
- About impfuzzy
- About Volatility Framework
- Impfuzzy for Volatility
- References

About impfuzzy

- impfuzzy is Fuzzy Hash (fuzzy hash function: the hash value for modified codes is close to that of the original codes) calculated from import API of the PE files

- impfuzzy uses “impfuzzy” method which compares the similarities of Windows executable files based on hash values generated from Import API

- Imports API and the PE file



```
remnux@remnux:~$ file syhunt-community-5.5.2.0.exe
syhunt-community-5.5.2.0.exe: PE32 executable (GUI) Intel 80386, for MS Windows
remnux@remnux:~$ pedump syhunt-community-5.5.2.0.exe | grep IMPORTS -A 5

=== IMPORTS ===

MODULE_NAME      HINT   ORD  FUNCTION_NAME
kernel32.dll        0        DeleteCriticalSection
kernel32.dll        0        LeaveCriticalSection
kernel32.dll        0        EnterCriticalSection
```

About Volatility Framework

- The Volatility Framework is a completely open collection of tools, implemented in Python, for the extraction of digital artifacts from volatile memory (RAM) samples

Testing Envinronment

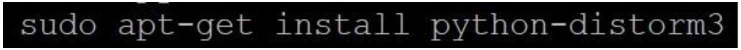
- Linux (Ubuntu 16.04.3 LTS)
- Memory sample (Dark Comet)

Impfuzzy for Volatility

- Volatility plugin for comparing the impfuzzy and imphash. This plugin can be used to scan malware in memory image

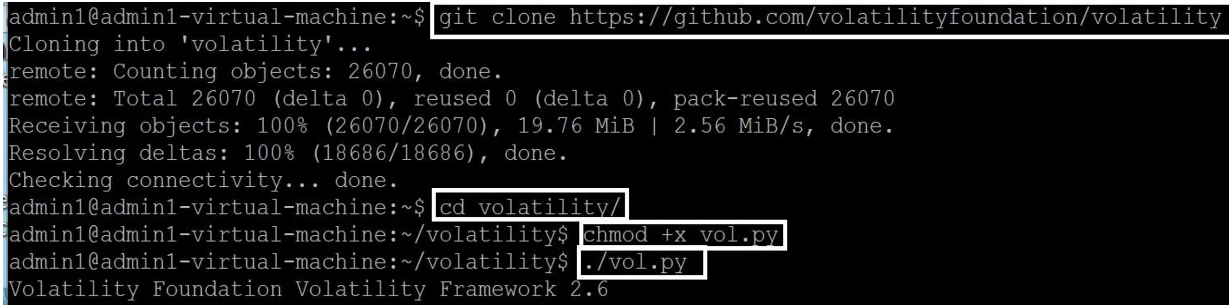
- Install Volatility

◎ Install requirements (distorm3)



```
sudo apt-get install python-distorm3
```

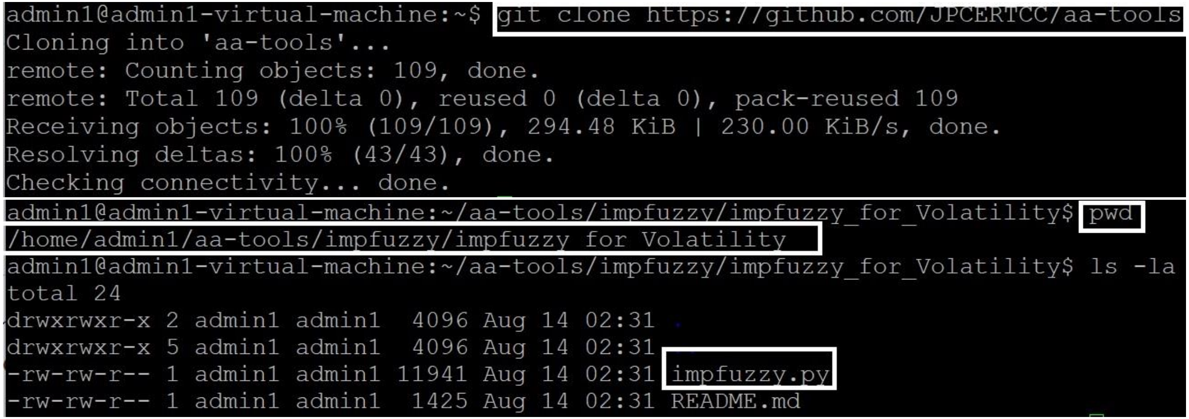
◎ Download volatility and run it



```
admin1@admin1-virtual-machine:~$ git clone https://github.com/volatilityfoundation/volatility
Cloning into 'volatility'...
remote: Counting objects: 26070, done.
remote: Total 26070 (delta 0), reused 0 (delta 0), pack-reused 26070
Receiving objects: 100% (26070/26070), 19.76 MiB | 2.56 MiB/s, done.
Resolving deltas: 100% (18686/18686), done.
Checking connectivity... done.
admin1@admin1-virtual-machine:~$ cd volatility/
admin1@admin1-virtual-machine:~/volatility$ chmod +x vol.py
admin1@admin1-virtual-machine:~/volatility$ ./vol.py
Volatility Foundation Volatility Framework 2.6
```

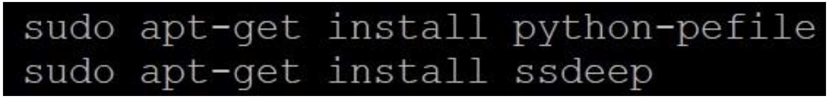
Impfuzzy for Volatility

- Download impfuzzy (https://github.com/JPCERTCC/aa-tools/)



```
admin1@admin1-virtual-machine:~$ git clone https://github.com/JPCERTCC/aa-tools
Cloning into 'aa-tools'...
remote: Counting objects: 109, done.
remote: Total 109 (delta 0), reused 0 (delta 0), pack-reused 109
Receiving objects: 100% (109/109), 294.48 KiB | 230.00 KiB/s, done.
Resolving deltas: 100% (43/43), done.
Checking connectivity... done.
admin1@admin1-virtual-machine:~/aa-tools/impfuzzy/impfuzzy_for_Volatility$ pwd
/home/admin1/aa-tools/impfuzzy/impfuzzy_for_Volatility
admin1@admin1-virtual-machine:~/aa-tools/impfuzzy/impfuzzy_for_Volatility$ ls -la
total 24
drwxrwxr-x 2 admin1 admin1  4096 Aug 14 02:31 .
drwxrwxr-x 5 admin1 admin1  4096 Aug 14 02:31 ..
-rw-rw-r-- 1 admin1 admin1 11941 Aug 14 02:31 impfuzzy.py
-rw-rw-r-- 1 admin1 admin1  1425 Aug 14 02:31 README.md
```

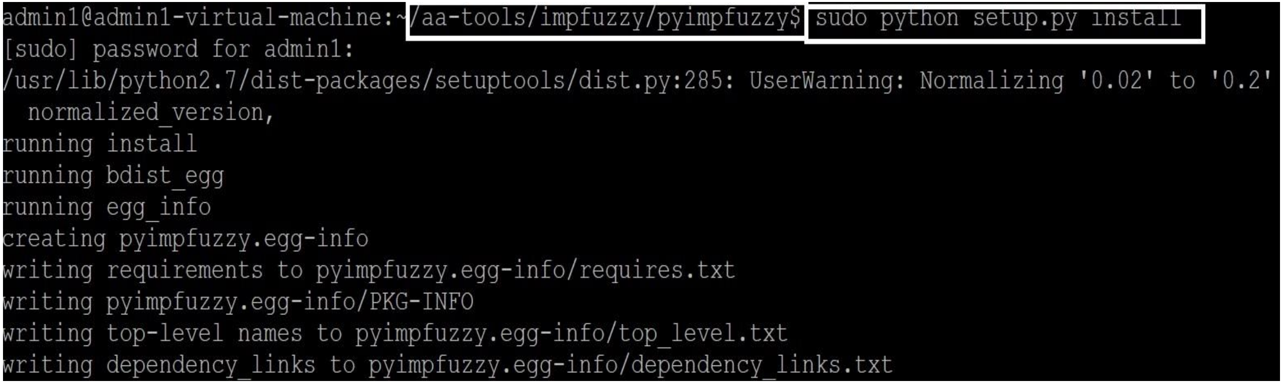
- Install requirements (pefile and ssdeep)



```
sudo apt-get install python-pefile
sudo apt-get install ssdeep
```

Impfuzzy for Volatility

- Install pyimpfuzz

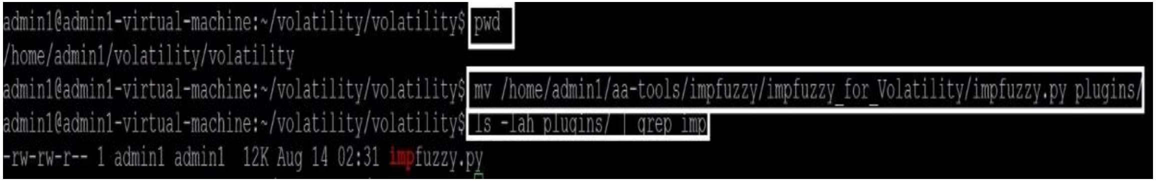


```
admin1@admin1-virtual-machine:~/aa-tools/impfuzzy/pyimpfuzzy$ sudo python setup.py install
[sudo] password for admin1:
/usr/lib/python2.7/dist-packages/setuptools/dist.py:285: UserWarning: Normalizing '0.02' to '0.2'
  normalized_version,
running install
running bdist_egg
running egg_info
creating pyimpfuzzy.egg-info
writing requirements to pyimpfuzzy.egg-info/requires.txt
writing pyimpfuzzy.egg-info/PKG-INFO
writing top-level names to pyimpfuzzy.egg-info/top_level.txt
writing dependency_links to pyimpfuzzy.egg-info/dependency_links.txt
```

Impfuzzy for Volatility

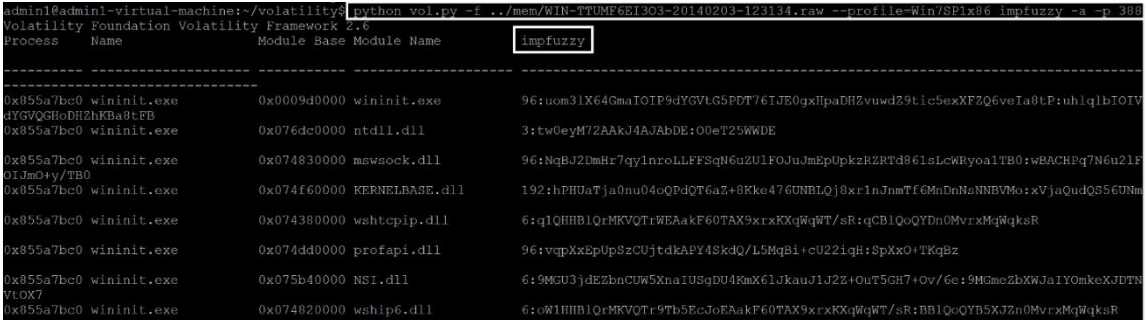
- Use impfuzzy plugin with Volatility

◎ Move impfuzzy.py to volatility /plugin folder



```
admin1@admin1-virtual-machine:~/volatility/volatility$ pwd
/home/admin1/volatility/volatility
admin1@admin1-virtual-machine:~/volatility/volatility$ mv /home/admin1/aa-tools/impfuzzy/impfuzzy_for_Volatility/impfuzzy.py plugins/
admin1@admin1-virtual-machine:~/volatility/volatility$ ls -lah plugins/ | grep imp
-rw-rw-r-- 1 admin1 admin1  12K Aug 14 02:31 impfuzzy.py
```

◎ Use the plugin with Dark Comet image



```
admin1@admin1-virtual-machine:~/volatility$ python vol.py -f ../mem/WIN-TTUMF6EI3O3-20140203-123134.raw --profile=Win7SP1x86 impfuzzy -a -p 388
Volatility Foundation Volatility Framework 2.6
Process    Name                 Module Base Module Name          impfuzzy

---------- -------------------- ----------- -------------------- ------------------------------------------------------------------------------
--------------------------------
0x855a7bc0 wininit.exe          0x0009d0000 wininit.exe          96:uom3lX64GmaIOIP9dYGVtG5PDT76IJE0gxHpaDHZvuwdZ9tic5exXFZQ6veIa8tP:uhlqlbIOIV
dYGVQGHoDHZhKBa8tFB
0x855a7bc0 wininit.exe          0x076dc0000 ntdll.dll            3:tw0eyM72AAkJ4AJAbDE:O0eT25WWDE

0x855a7bc0 wininit.exe          0x074830000 mswsock.dll          96:NqBJ2DmHr7qy1nroLLFFSqN6uZUlFOJuJmEpUpkzRZRTd861sLcWRyoa1TB0:wBACHPq7N6u2lF
OIJmO+y/TB0
0x855a7bc0 wininit.exe          0x074f60000 KERNELBASE.dll       192:hPHUaTja0nu04oQPdQT6aZ+8Kke476UNBLQj8xr1nJnmTf6MnDnNsNNBVMo:xVjaQudQS56UNm

0x855a7bc0 wininit.exe          0x074380000 wshtcpip.dll         6:q1QHHBlQrMKVQTrWEAakF60TAX9xrxKXqWqWT/sR:qCBlQoQYDn0MvrxMqWqksR

0x855a7bc0 wininit.exe          0x074dd0000 profapi.dll          96:vqpXxEpUpSzCUjtdkAPY4SkdQ/L5MqBi+cU22iqH:SpXxO+TKqBz

0x855a7bc0 wininit.exe          0x075b40000 NSI.dll              6:9MGU3jdEZbnCUW5XnaIUSgDU4KmX6lJkauJ1J2Z+OuT5GH7+Ov/6e:9MGmeZbXWJaIYOmkeXJDTN
VtOX7
0x855a7bc0 wininit.exe          0x074820000 wship6.dll           6:oW1HHBlQrMKVQTr9Tb5EcJoEAakF60TAX9xrxKXqWqWT/sR:BBlQoQYB5XJZn0MvrxMqWqksR
```

References

- Github

https://github.com/JPCERTCC/aa-tools/blob/master/impfuzzy/README.md

- Volatility

http://www.volatilityfoundation.org/

- DarkComet

https://en.wikipedia.org/wiki/DarkComet