Penetration Testing Report

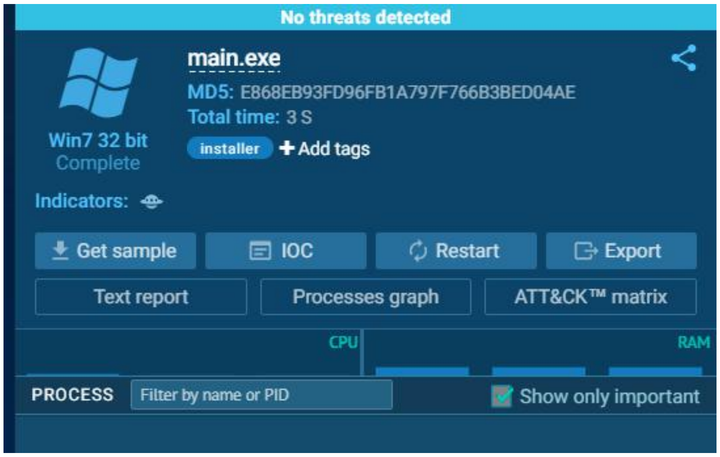
For

“Noobsware”

S.NO.	Title	#
1.	Challenge Category	Malware Analysis
2.	Challenge Related Files	flag.txt.g147, logs.txt, noobsware
3.	File Link / Target IP	N/A

PROCEDURE

1. The log file tell us that there is some bug in the windows binary. So let's start with that.
A MD5 hash is present probably of the binary. On googling about online malware sandboxes, you'll encounter ANY RUN. Searching the hash against the public uploads, you'll find the binary sample.

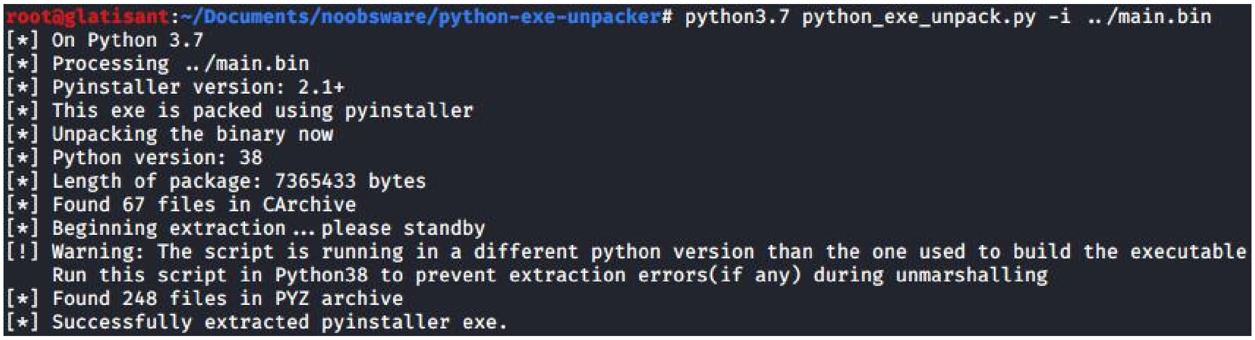


No threats detected

main.exe
MD5: E868EB93FD96FB1A797F766B3BED04AE
Total time: 3 S

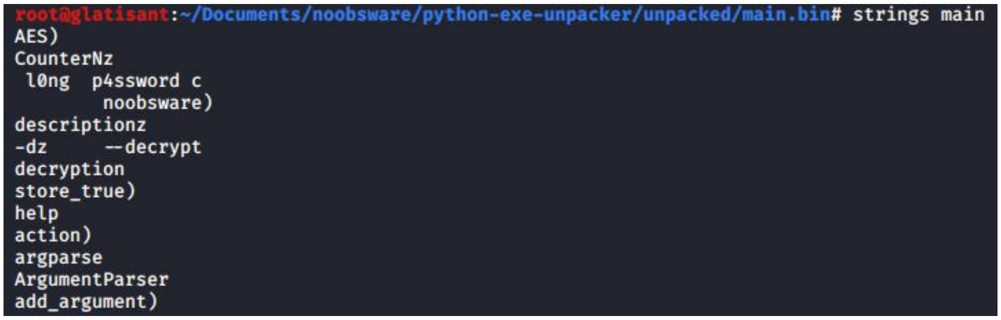
Win7 32 bit
Complete

2. Now its clearly stated in the logs that the ransomware has been written in Python. With F-Secure's Blog as reference, you can decompile the binary to get the source code.



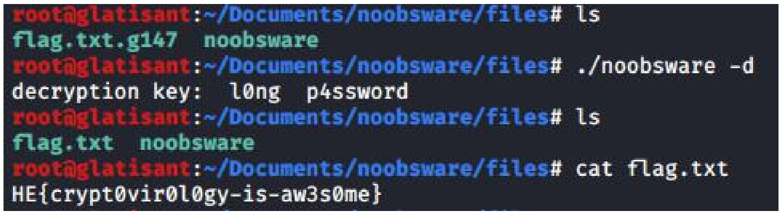
```
root@glatisant:~/Documents/noobsware/python-exe-unpacker# python3.7 python_exe_unpack.py -i ../main.bin
[*] On Python 3.7
[*] Processing ../main.bin
[*] Pyinstaller version: 2.1+
[*] This exe is packed using pyinstaller
[*] Unpacking the binary now
[*] Python version: 38
[*] Length of package: 7365433 bytes
[*] Found 67 files in CArchive
[*] Beginning extraction...please standby
[!] Warning: The script is running in a different python version than the one used to build the executable
    Run this script in Python38 to prevent extraction errors(if any) during unmarshalling
[*] Found 248 files in PYZ archive
[*] Successfully extracted pyinstaller exe.
```

3. Running a strings analysis on the partially decompiled file - main, you'll get a key.



```
root@glatisant:~/Documents/noobsware/python-exe-unpacker/unpacked/main.bin# strings main
AES)
CounterNz
 l0ng  p4ssword c
        noobsware)
descriptionz
-dz     --decrypt
decryption
store_true)
help
action)
argparse
ArgumentParser
add_argument)
```

4. After playing little bit with both the binaries & a little bit of guessing, you'll come to know where exactly to use the key.



```
root@glatisant:~/Documents/noobsware/files# ls
flag.txt.g147  noobsware
root@glatisant:~/Documents/noobsware/files# ./noobsware -d
decryption key:  l0ng  p4ssword
root@glatisant:~/Documents/noobsware/files# ls
flag.txt  noobsware
root@glatisant:~/Documents/noobsware/files# cat flag.txt
HE{crypt0vir0l0gy-is-aw3s0me}
```

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{crypt0vir0l0gy-is-aw3s0me}