Joseph Pepe & Karandeep Jaswal

1251897 & 1256917

NYIT

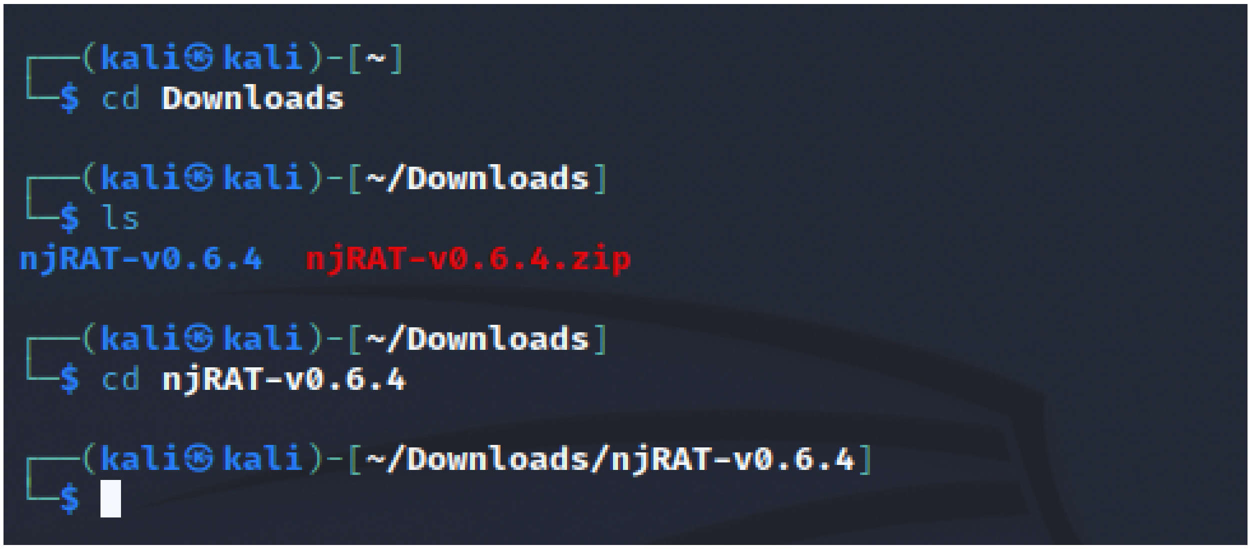
INCS 745

Lab 4: Malware Detection

Table of Contents

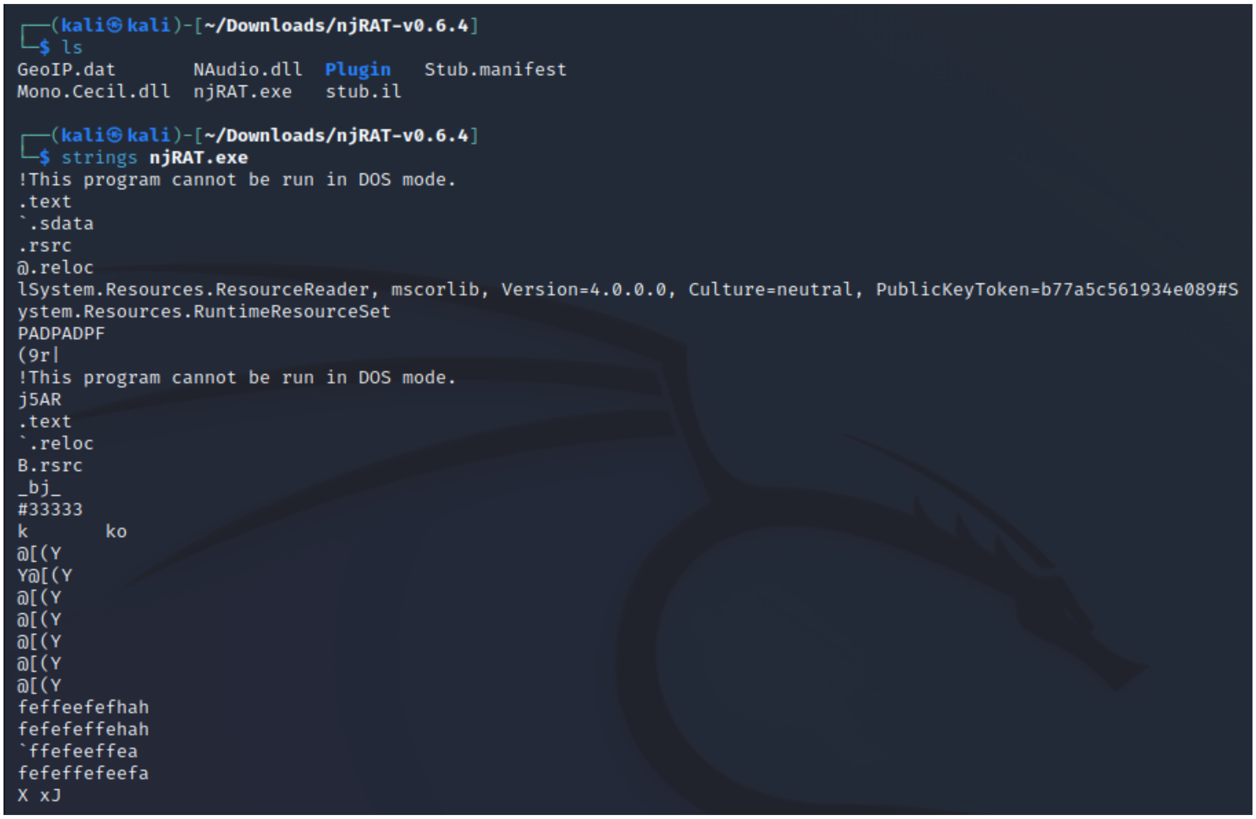
Task 1:

Step 1: Downloaded file from Canvas on Kali. Extracted the file moved into the correct directory.



```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
njRAT-v0.6.4  njRAT-v0.6.4.zip

┌──(kali㉿kali)-[~/Downloads]
└─$ cd njRAT-v0.6.4

┌──(kali㉿kali)-[~/Downloads/njRAT-v0.6.4]
└─$ 
```

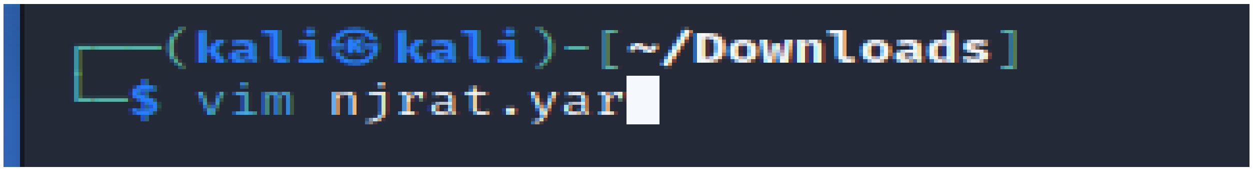
Step 2: Use ls to confirm all properties from the folder are present. Then use the strings njRAT.exe command to view the properties of the .exe file. This will be helpful for upcoming steps.



```
┌──(kali㉿kali)-[~/Downloads/njRAT-v0.6.4]
└─$ ls
GeoIP.dat       NAudio.dll  Plugin   Stub.manifest
Mono.Cecil.dll  njRAT.exe   stub.il

┌──(kali㉿kali)-[~/Downloads/njRAT-v0.6.4]
└─$ strings njRAT.exe
!This program cannot be run in DOS mode.
.text
`.sdata
.rsrc
@.reloc
lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#S
ystem.Resources.RuntimeResourceSet
PADPADPF
(9r|
!This program cannot be run in DOS mode.
j5AR
.text
`.reloc
B.rsrc
_bj_
#33333
k       ko
@[(Y
Y@[(Y
@[(Y
@[(Y
@[(Y
@[(Y
@[(Y
feffeefefhah
fefefeffehah
`ffefeeffea
fefeffefeefa
X xJ
```

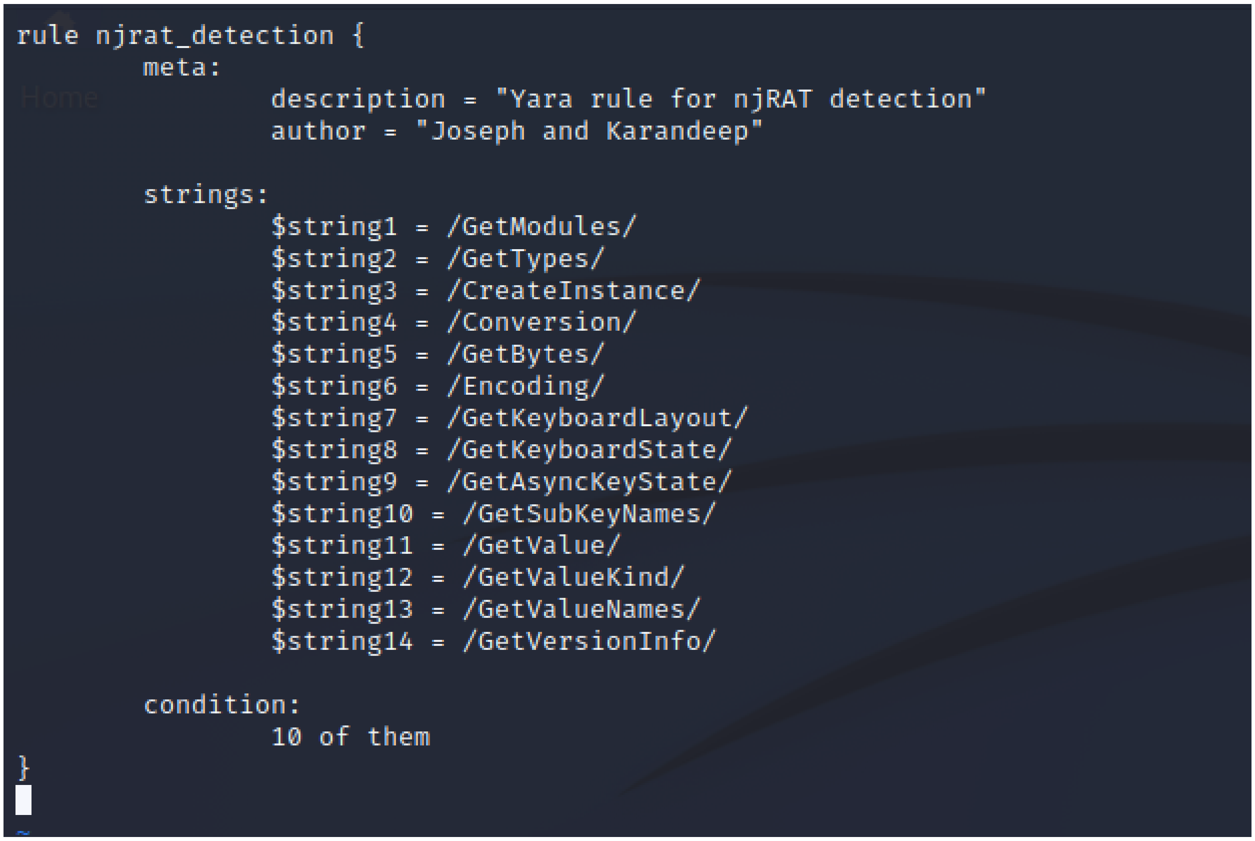
Step 3: We head to online resources and select some common API'S used in Malware. Reference: https://book.hacktricks.xyz/reversing-and-exploiting/common-api-used-in-malware

Step 4: We use vim to create our njrat.yar file



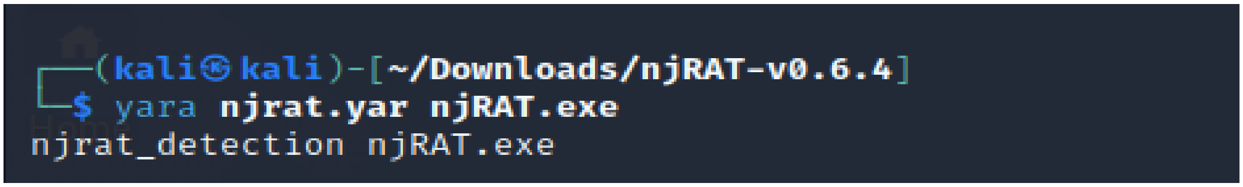
```
┌──(kali㉿kali)-[~/Downloads]
└─$ vim njrat.yar
```

Step 5: We begin creating the yara rules



```
rule njrat_detection {
        meta:
                description = "Yara rule for njRAT detection"
                author = "Joseph and Karandeep"

        strings:
                $string1 = /GetModules/
                $string2 = /GetTypes/
                $string3 = /CreateInstance/
                $string4 = /Conversion/
                $string5 = /GetBytes/
                $string6 = /Encoding/
                $string7 = /GetKeyboardLayout/
                $string8 = /GetKeyboardState/
                $string9 = /GetAsyncKeyState/
                $string10 = /GetSubKeyNames/
                $string11 = /GetValue/
                $string12 = /GetValueKind/
                $string13 = /GetValueNames/
                $string14 = /GetVersionInfo/

        condition:
                10 of them
}

~
```

Step 6: We now use yara command and check output to see if the conditions were met

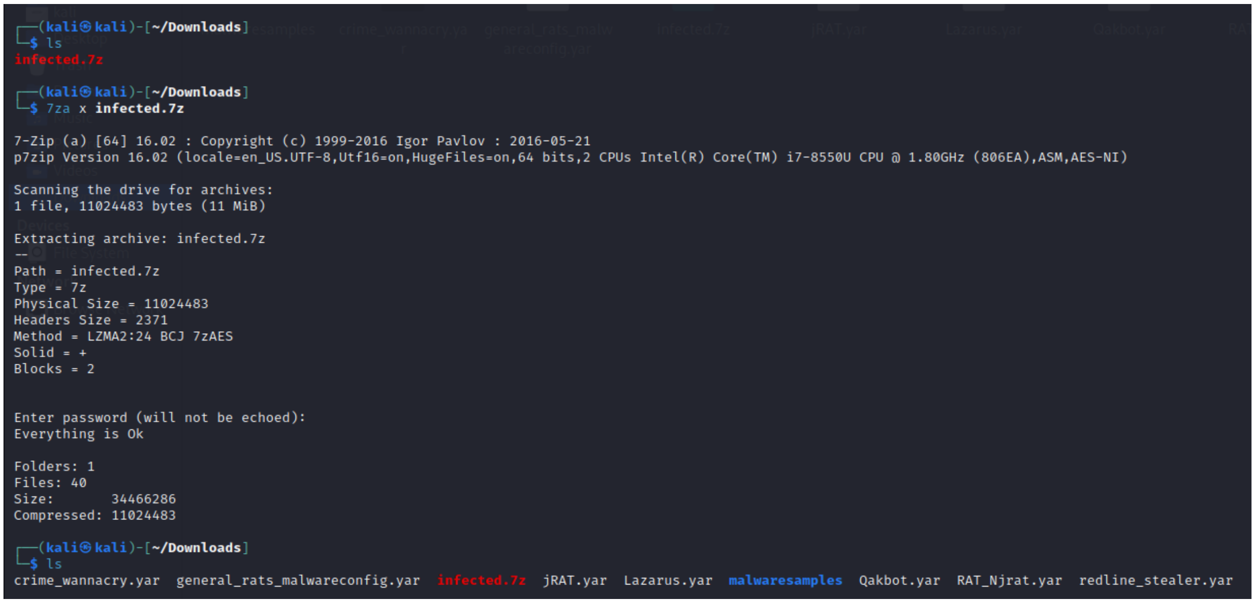


```
┌──(kali㉿kali)-[~/Downloads/njRAT-v0.6.4]
└─$ yara njrat.yar njRAT.exe
njrat_detection njRAT.exe
```

Step 7: We can conclude that the conditions were met that 10 of the strings matched and that this file is indeed Malware.

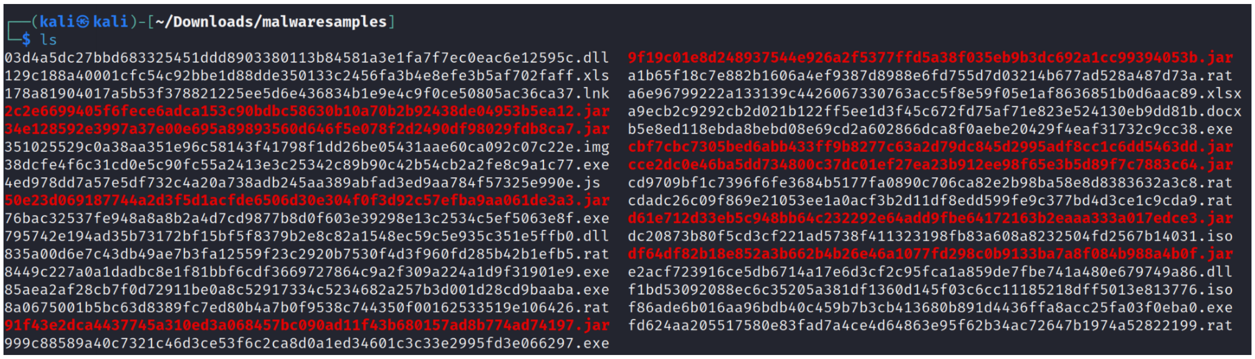
Task 2:

Step 1: Unzip the infected.7z file by using - **7za e infected.7z**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
infected.7z

┌──(kali㉿kali)-[~/Downloads]
└─$ 7za x infected.7z

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz (806EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 11024483 bytes (11 MiB)

Extracting archive: infected.7z
--
Path = infected.7z
Type = 7z
Physical Size = 11024483
Headers Size = 2371
Method = LZMA2:24 BCJ 7zAES
Solid = +
Blocks = 2


Enter password (will not be echoed):
Everything is Ok

Folders: 1
Files: 40
Size:       34466286
Compressed: 11024483

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
crime_wannacry.yar  general_rats_malwareconfig.yar  infected.7z  jRAT.yar  Lazarus.yar  malwaresamples  Qakbot.yar  RAT_Njrat.yar  redline_stealer.yar
```

After unzipping the file, we see there are 7 yara rule files- crime_wannacry.yar, general_rats_malwareconfig.yar, jRAT.yar, Lazarus.yar, Qakbot.yar, RAT_Njrat.yar, and redline_stealer.yar. Additionally, there's a folder called "**malwaresamples"** that contains these 33 malware samples:

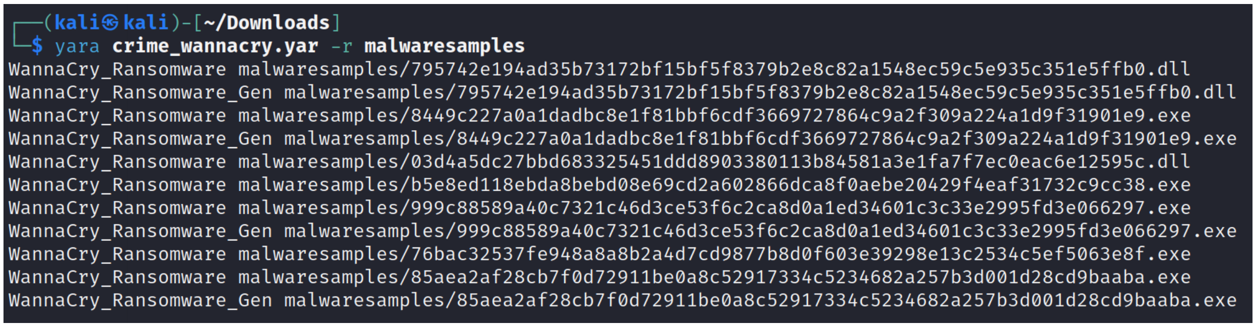


```
┌──(kali㉿kali)-[~/Downloads/malwaresamples]
└─$ ls
03d4a5dc27bbd683325451ddd8903380113b84581a3e1fa7f7ec0eac6e12595c.dll  9f19c01e8d248937544e926a2f5377ffd5a38f035eb9b3dc692a1cc99394053b.jar
129c188a40001cfc54c92bbe1d88dde350133c2456fa3b4e8efe3b5af702faff.xls  a1b65f18c7e882b1606a4ef9387d8988e6fd755d7d03214b677ad528a487d73a.rat
178a81904017a5b53f378821225ee5d6e436834b1e9e4c9f0ce50805ac36ca37.lnk  a6e96799222a133139c4426067330763acc5f8e59f05e1af8636851b0d6aac89.xlsx
2c2e6699405f6fece6adca153c90bdbc58630b10a70b2b92438de04953b5ea12.jar  a9ecb2c9292cb2d021b122ff5ee1d3f45c672fd75af71e823e524130eb9dd81b.docx
34e128592e3997a37e00e695a89893560d646f5e078f2d2490df98029fdb8ca7.jar  b5e8ed118ebda8bebd08e69cd2a602866dca8f0aebe20429f4eaf31732c9cc38.exe
351025529c0a38aa351e96c58143f41798f1dd26be05431aae60ca092c07c22e.img  cbf7cbc7305bed6abb433ff9b8277c63a2d79dc845d2995adf8cc1c6dd5463dd.jar
38dcfe4f6c31cd0e5c90fc55a2413e3c25342c89b90c42b54cb2a2fe8c9a1c77.exe  cce2dc0e46ba5dd734800c37dc01ef27ea23b912ee98f65e3b5d89f7c7883c64.jar
4ed978dd7a57e5df732c4a20a738adb245aa389abfad3ed9aa784f57325e990e.js   cd9709bf1c7396f6fe3684b5177fa0890c706ca82e2b98ba58e8d8383632a3c8.rat
50e23d069187744a2d3f5d1acfde6506d30e304f0f3d92c57efba9aa061de3a3.jar  cdadc26c09f869e21053ee1a0acf3b2d11df8edd599fe9c377bd4d3ce1c9cda9.rat
76bac32537fe948a8a8b2a4d7cd9877b8d0f603e39298e13c2534c5ef5063e8f.exe  d61e712d33eb5c948bb64c232292e64add9fbe64172163b2eaaa333a017edce3.jar
795742e194ad35b73172bf15bf5f8379b2e8c82a1548ec59c5e935c351e5ffb0.dll  dc20873b80f5cd3cf221ad5738f411323198fb83a608a8232504fd2567b14031.iso
835a00d6e7c43db49ae7b3fa12559f23c2920b7530f4d3f960fd285b42b1efb5.rat  df64df82b18e852a3b662b4b26e46a1077fd298c0b9133ba7a8f084b988a4b0f.jar
8449c227a0a1dadbc8e1f81bbf6cdf3669727864c9a2f309a224a1d9f31901e9.exe  e2acf723916ce5db6714a17e6d3cf2c95fca1a859de7fbe741a480e679749a86.dll
85aea2af28cb7f0d72911be0a8c52917334c5234682a257b3d001d28cd9baaba.exe  f1bd53092088ec6c35205a381df1360d145f03c6cc11185218dff5013e813776.iso
8a0675001b5bc63d8389fc7ed80b4a7b0f9538c744350f00162533519e106426.rat  f86ade6b016aa96bdb40c459b7b3cb413680b891d4436ffa8acc25fa03f0eba0.exe
91f43e2dca4437745a310ed3a068457bc090ad11f43b680157ad8b774ad74197.jar  fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199.rat
999c88589a40c7321c46d3ce53f6c2ca8d0a1ed34601c3c33e2995fd3e066297.exe
```

Step 2: Run each of the 7 yara rules against the **malwaresamples** directory.

1. crime_wannacry.yar

Run **yara crime_wannacry.yar -r malwaresamples** to run the yara rule against all the files in the **malwaresamples** directory.

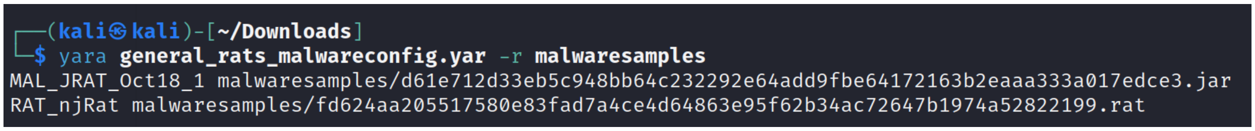


```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara crime_wannacry.yar -r malwaresamples
WannaCry_Ransomware malwaresamples/795742e194ad35b73172bf15bf5f8379b2e8c82a1548ec59c5e935c351e5ffb0.dll
WannaCry_Ransomware_Gen malwaresamples/795742e194ad35b73172bf15bf5f8379b2e8c82a1548ec59c5e935c351e5ffb0.dll
WannaCry_Ransomware malwaresamples/8449c227a0a1dadbc8e1f81bbf6cdf3669727864c9a2f309a224a1d9f31901e9.exe
WannaCry_Ransomware_Gen malwaresamples/8449c227a0a1dadbc8e1f81bbf6cdf3669727864c9a2f309a224a1d9f31901e9.exe
WannaCry_Ransomware malwaresamples/03d4a5dc27bbd683325451ddd8903380113b84581a3e1fa7f7ec0eac6e12595c.dll
WannaCry_Ransomware malwaresamples/b5e8ed118ebda8bebd08e69cd2a602866dca8f0aebe20429f4eaf31732c9cc38.exe
WannaCry_Ransomware malwaresamples/999c88589a40c7321c46d3ce53f6c2ca8d0a1ed34601c3c33e2995fd3e066297.exe
WannaCry_Ransomware_Gen malwaresamples/999c88589a40c7321c46d3ce53f6c2ca8d0a1ed34601c3c33e2995fd3e066297.exe
WannaCry_Ransomware malwaresamples/76bac32537fe948a8a8b2a4d7cd9877b8d0f603e39298e13c2534c5ef5063e8f.exe
WannaCry_Ransomware malwaresamples/85aea2af28cb7f0d72911be0a8c52917334c5234682a257b3d001d28cd9baaba.exe
WannaCry_Ransomware_Gen malwaresamples/85aea2af28cb7f0d72911be0a8c52917334c5234682a257b3d001d28cd9baaba.exe
```

These 11 malware samples were detected by crime_wannacry.yar.

2. general_rats_malwareconfig.yar

Run **yara general_rats_malwareconfig.yar -r malwaresamples** to run the yara rule against all the files in the **malwaresamples** directory.

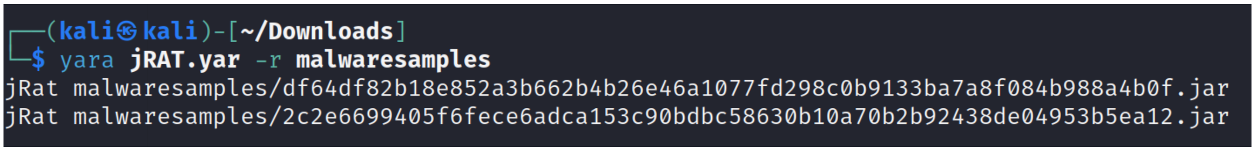


```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara general_rats_malwareconfig.yar -r malwaresamples
MAL_JRAT_Oct18_1 malwaresamples/d61e712d33eb5c948bb64c232292e64add9fbe64172163b2eaaa333a017edce3.jar
RAT_njRat malwaresamples/fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199.rat
```

These 2 malware samples were detected by general_rats_malwareconfig.yar.

3. jRAT.yar

Run **yara jRAT.yar -r malwaresamples** to run the yara rule against all the files in the **malwaresamples** directory.

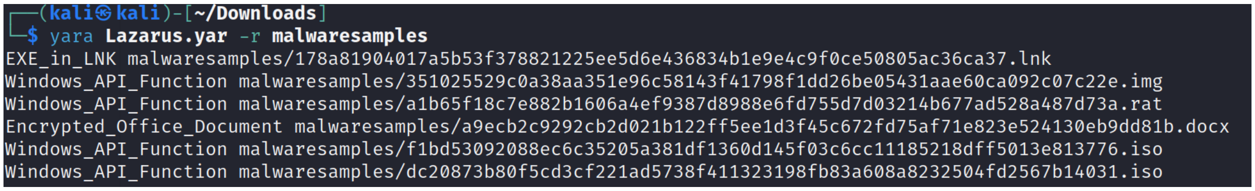


```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara jRAT.yar -r malwaresamples
jRat malwaresamples/df64df82b18e852a3b662b4b26e46a1077fd298c0b9133ba7a8f084b988a4b0f.jar
jRat malwaresamples/2c2e6699405f6fece6adca153c90bdbc58630b10a70b2b92438de04953b5ea12.jar
```

These 2 malware samples were detected by jRAT.yar.

4. Lazarus.yar

Run **yara Lazarus.yar -r malwaresamples** to run the yara rule against all the files in the **malwaresamples** directory.

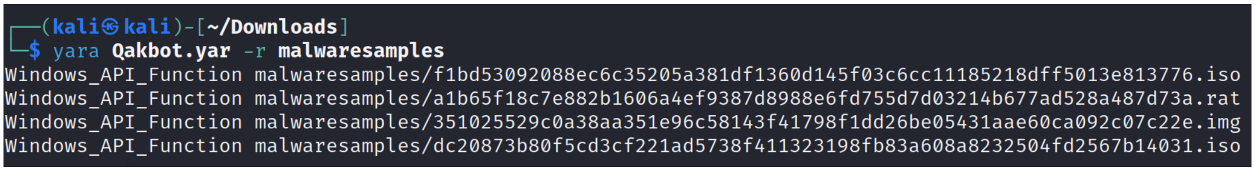


```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara Lazarus.yar -r malwaresamples
EXE_in_LNK malwaresamples/178a81904017a5b53f378821225ee5d6e436834b1e9e4c9f0ce50805ac36ca37.lnk
Windows_API_Function malwaresamples/351025529c0a38aa351e96c58143f41798f1dd26be05431aae60ca092c07c22e.img
Windows_API_Function malwaresamples/a1b65f18c7e882b1606a4ef9387d8988e6fd755d7d03214b677ad528a487d73a.rat
Encrypted_Office_Document malwaresamples/a9ecb2c9292cb2d021b122ff5ee1d3f45c672fd75af71e823e524130eb9dd81b.docx
Windows_API_Function malwaresamples/f1bd53092088ec6c35205a381df1360d145f03c6cc11185218dff5013e813776.iso
Windows_API_Function malwaresamples/dc20873b80f5cd3cf221ad5738f411323198fb83a608a8232504fd2567b14031.iso
```

These 6 malware samples were detected by Lazarus.yar.

5. Qakbot.yar

Run **yara Qakbot.yar -r malwaresamples** to run the yara rule against all the files in the **malwaresamples** directory.

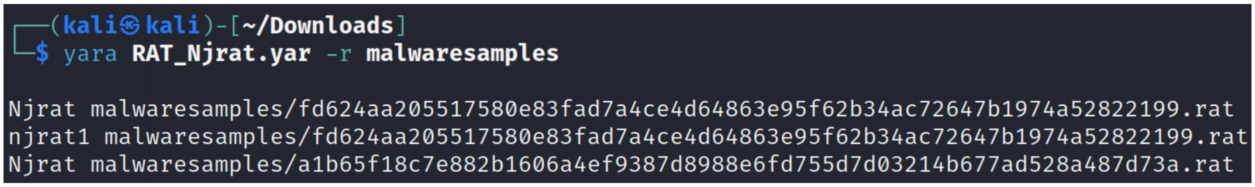


```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara Qakbot.yar -r malwaresamples
Windows_API_Function malwaresamples/f1bd53092088ec6c35205a381df1360d145f03c6cc11185218dff5013e813776.iso
Windows_API_Function malwaresamples/a1b65f18c7e882b1606a4ef9387d8988e6fd755d7d03214b677ad528a487d73a.rat
Windows_API_Function malwaresamples/351025529c0a38aa351e96c58143f41798f1dd26be05431aae60ca092c07c22e.img
Windows_API_Function malwaresamples/dc20873b80f5cd3cf221ad5738f411323198fb83a608a8232504fd2567b14031.iso
```

These 4 malware samples were detected by Qakbot.yar.

6. RAT_Njrat.yar

Run **yara RAT_Njrat.yar -r malwaresamples** to run the yara rule against all the files in the **malwaresamples** directory.

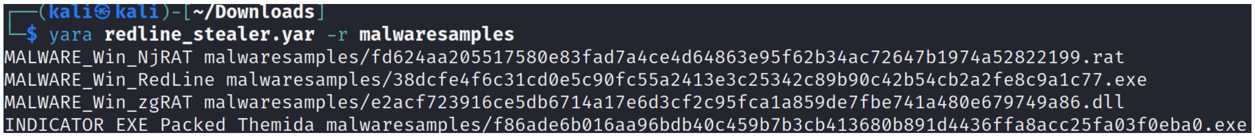


```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara RAT_Njrat.yar -r malwaresamples

Njrat malwaresamples/fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199.rat
njrat1 malwaresamples/fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199.rat
Njrat malwaresamples/a1b65f18c7e882b1606a4ef9387d8988e6fd755d7d03214b677ad528a487d73a.rat
```

These 3 malware samples were detected by RAT_Njrat.yar.

7. redline_stealer.yar

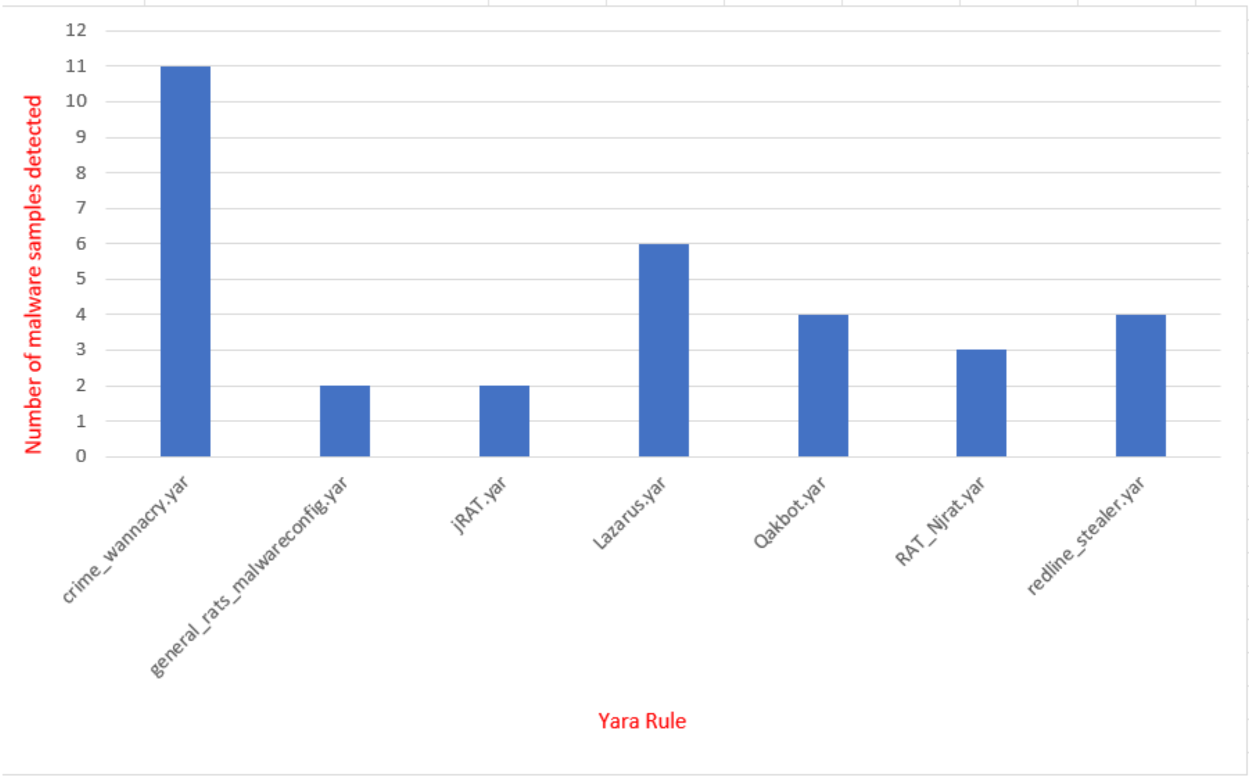
Run **yara redline_stealer.yar -r malwaresamples** to run the yara rule against all the files in the **malwaresamples** directory.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara redline_stealer.yar -r malwaresamples
MALWARE_Win_NjRAT malwaresamples/fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199.rat
MALWARE_Win_RedLine malwaresamples/38dcfe4f6c31cd0e5c90fc55a2413e3c25342c89b90c42b54cb2a2fe8c9a1c77.exe
MALWARE_Win_zgRAT malwaresamples/e2acf723916ce5db6714a17e6d3cf2c95fca1a859de7fbe741a480e679749a86.dll
INDICATOR_EXE_Packed_Themida malwaresamples/f86ade6b016aa96bdb40c459b7b3cb413680b891d4436ffa8acc25fa03f0eba0.exe
```

These 4 malware samples were detected by redline_stealer.yar.

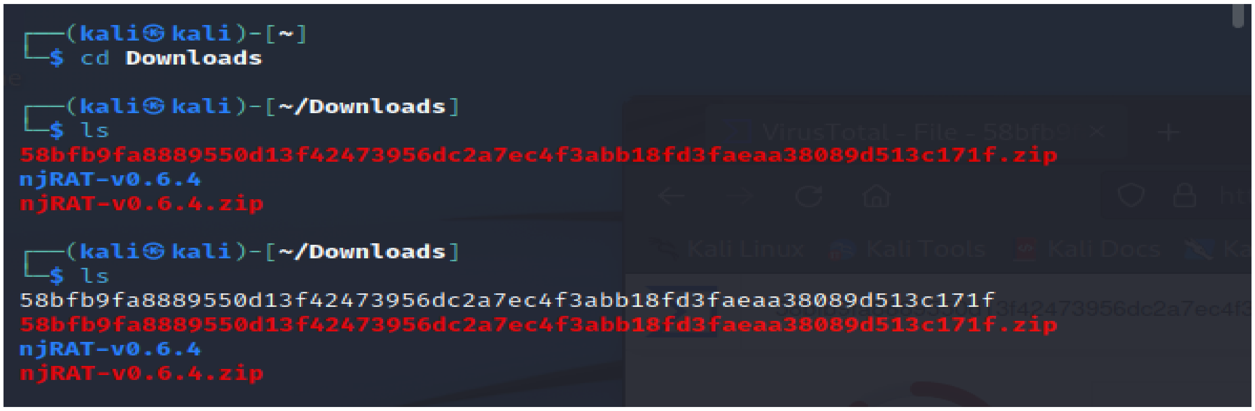
Bar graph illustrating our findings:



From the graph, it's evident that crime_wannacry.yar detected the most amount of malware samples- 11 in count. Whereas, jRAT.yar and general_rats_malwareconfig.yar detected the least amount of malware samples - 2 in count.

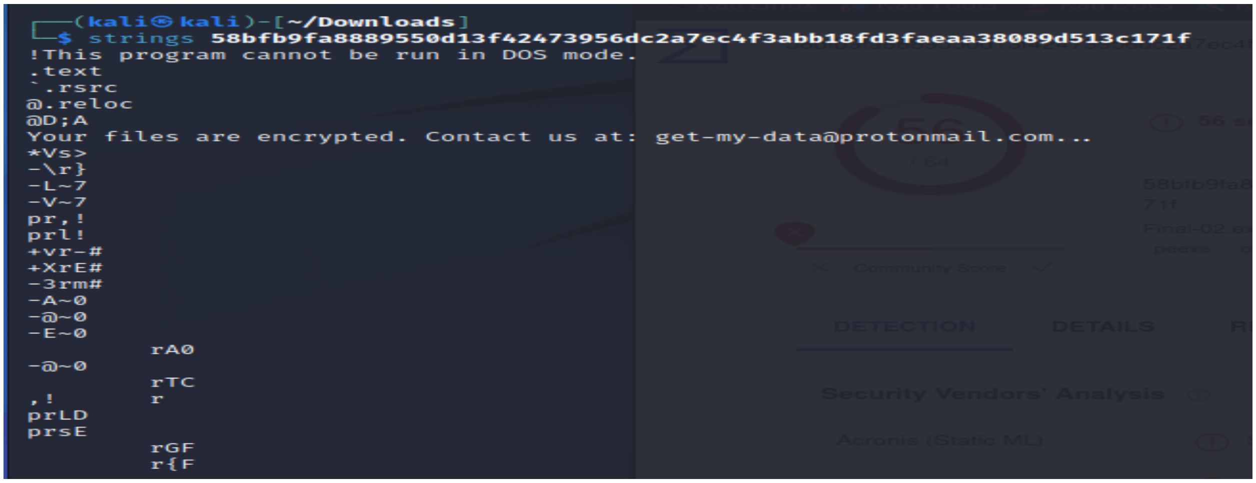
Task 3:

Step 1: Downloaded our group's sample file and extracted the file on Kali.



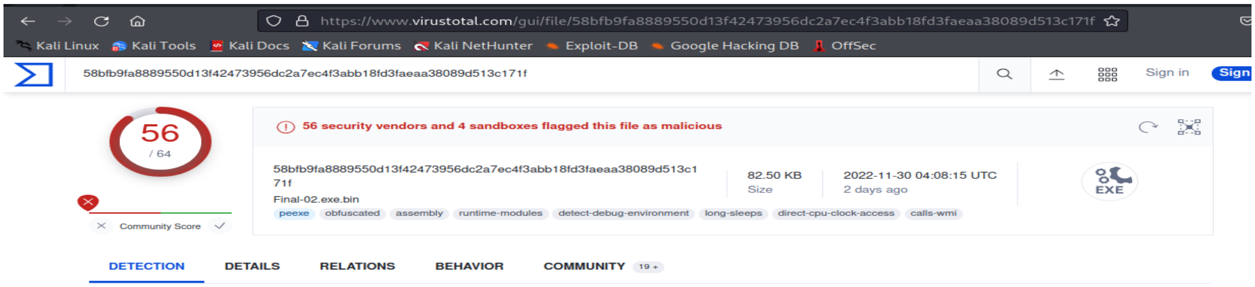
```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f.zip
njRAT-v0.6.4
njRAT-v0.6.4.zip

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f.zip
njRAT-v0.6.4
njRAT-v0.6.4.zip
```

Step 2: Ran command strings 58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f



```
┌──(kali㉿kali)-[~/Downloads]
└─$ strings 58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
@D;A
Your files are encrypted. Contact us at: get-my-data@protonmail.com...
*Vs>
-\r}
-L~7
-V~7
pr,!
prl!
+vr-#
+XrE#
-3rm#
-A~0
-@~0
-E~0
        rA0
-@~0
        rTC
,!      r
prLD
prsE
        rGF
        r{F
```

Step 3: Upload the file to virus total



https://www.virustotal.com/gui/file/58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
Sign in
Sign
56
/ 64
Community Score

56 security vendors and 4 sandboxes flagged this file as malicious

58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
Final-02.exe.bin
peexe obfuscated assembly runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access calls-wmi

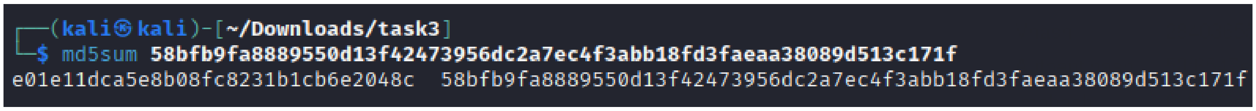
82.50 KB
Size

2022-11-30 04:08:15 UTC
2 days ago

Step 4: Analyze the following topics:

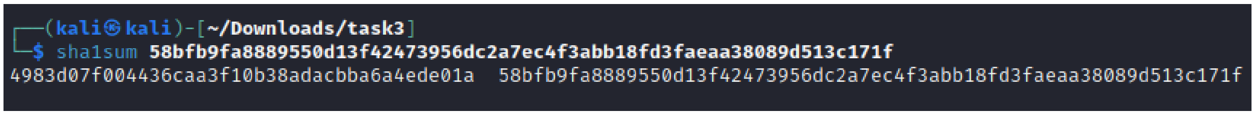
- Hashes - md5, sha1sum, sha256sum

md5:



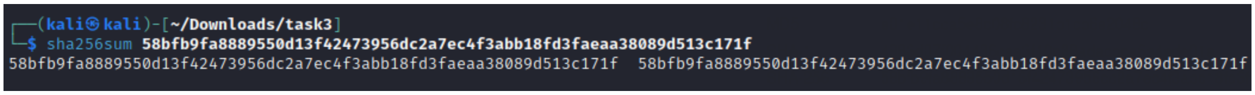
```
┌──(kali㉿kali)-[~/Downloads/task3]
└─$ md5sum 58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
e01e11dca5e8b08fc8231b1cb6e2048c  58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
```

sha1sum:



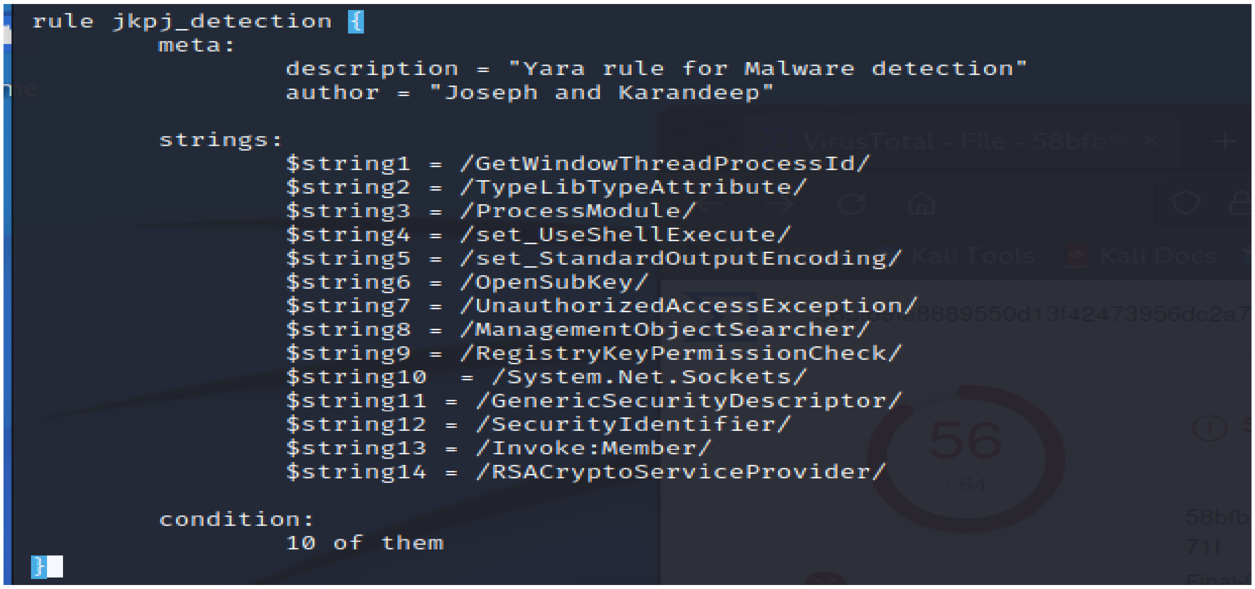
```
┌──(kali㉿kali)-[~/Downloads/task3]
└─$ sha1sum 58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
4983d07f004436caa3f10b38adacbba6a4ede01a  58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
```

sha256sum

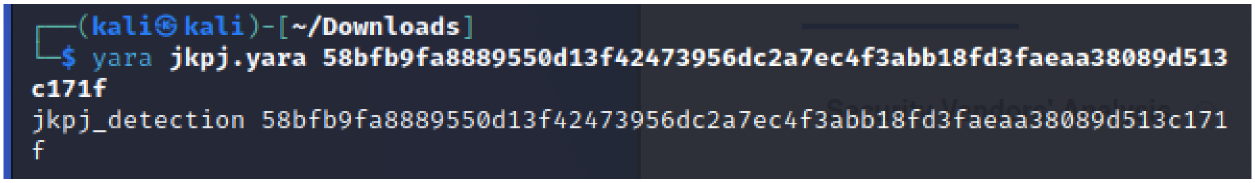


```
┌──(kali㉿kali)-[~/Downloads/task3]
└─$ sha256sum 58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f  58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
```

●Yara rule



```
rule jkpj_detection {
        meta:
                description = "Yara rule for Malware detection"
                author = "Joseph and Karandeep"

        strings:
                $string1 = /GetWindowThreadProcessId/
                $string2 = /TypeLibTypeAttribute/
                $string3 = /ProcessModule/
                $string4 = /set_UseShellExecute/
                $string5 = /set_StandardOutputEncoding/
                $string6 = /OpenSubKey/
                $string7 = /UnauthorizedAccessException/
                $string8 = /ManagementObjectSearcher/
                $string9 = /RegistryKeyPermissionCheck/
                $string10  = /System.Net.Sockets/
                $string11 = /GenericSecurityDescriptor/
                $string12 = /SecurityIdentifier/
                $string13 = /Invoke:Member/
                $string14 = /RSACryptoServiceProvider/

        condition:
                10 of them
}
```



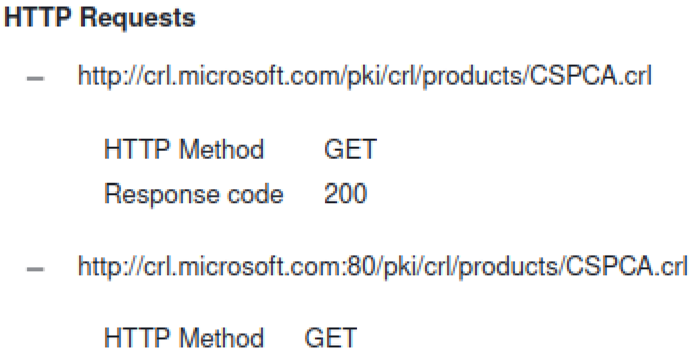
```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara jkpj.yara 58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513
c171f
jkpj_detection 58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171
f
```

●Common Windows API used

1) Read
2) set_UseShellExecute
3) VirtualAllocEx
4) WriteProcessMemory
5) CreateToolhelp32Snapshot
6) ReadProcessMemory
7) CreateFile
8) GetTempPath
9) WriteFile
10) Write
11) Send

These malicious Windows APIs were found in our sample that are intended to target the system for nefarious purposes. For example, WriteFile is used to write data to a specified file or input/output (I/O) device. Harmful scripts can be written via this Windows API.

●Network communication (URLs and suspicious IPs)



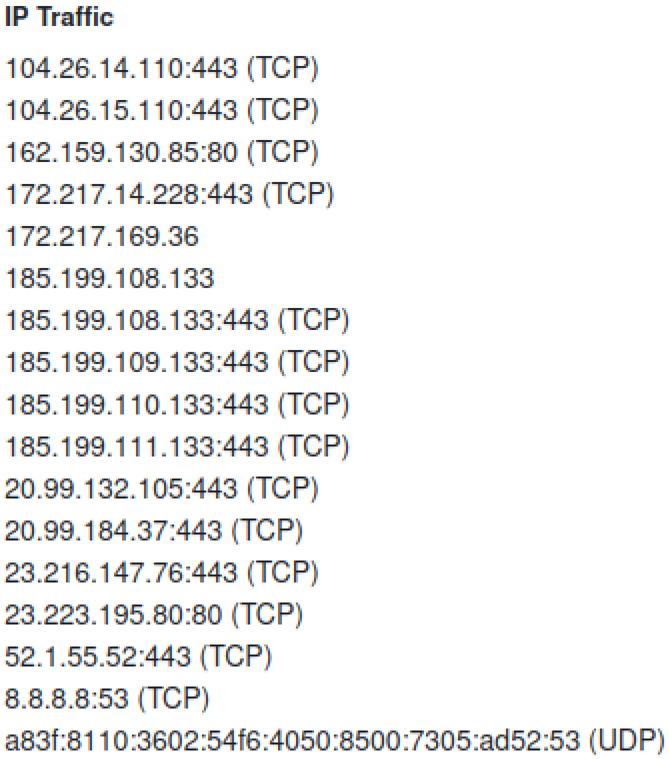
HTTP Requests

- http://crl.microsoft.com/pki/crl/products/CSPCA.crl

  HTTP Method GET
  Response code 200

- http://crl.microsoft.com:80/pki/crl/products/CSPCA.crl

  HTTP Method GET

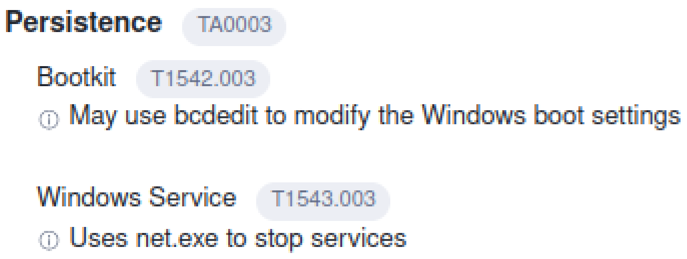


IP Traffic

```
104.26.14.110:443 (TCP)
104.26.15.110:443 (TCP)
162.159.130.85:80 (TCP)
172.217.14.228:443 (TCP)
172.217.169.36
185.199.108.133
185.199.108.133:443 (TCP)
185.199.109.133:443 (TCP)
185.199.110.133:443 (TCP)
185.199.111.133:443 (TCP)
20.99.132.105:443 (TCP)
20.99.184.37:443 (TCP)
23.216.147.76:443 (TCP)
23.223.195.80:80 (TCP)
52.1.55.52:443 (TCP)
8.8.8.8:53 (TCP)
a83f:8110:3602:54f6:4050:8500:7305:ad52:53 (UDP)
```

Our sample included these HTTP requests and IP traffic. From the IP traffic we can see the walware was Trying to communicate to port 80 - which communicates without encryption.

●Persistence mechanism



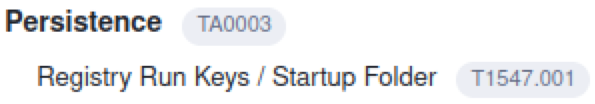
Persistence TA0003

Bootkit T1542.003

ⓘ May use bcdedit to modify the Windows boot settings

Windows Service T1543.003

ⓘ Uses net.exe to stop services

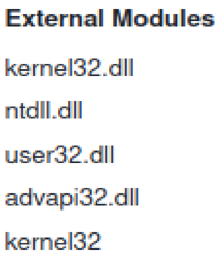


Persistence TA0003

Registry Run Keys / Startup Folder T1547.001

Persistence mechanisms were detected on our malware sample. Persistence mechanismsare tools that allows the malware to stay on the victim's computer for a longer period of time.

● Imported DLLs (Dynamically Loaded Libraries)



External Modules

kernel32.dll

ntdll.dll

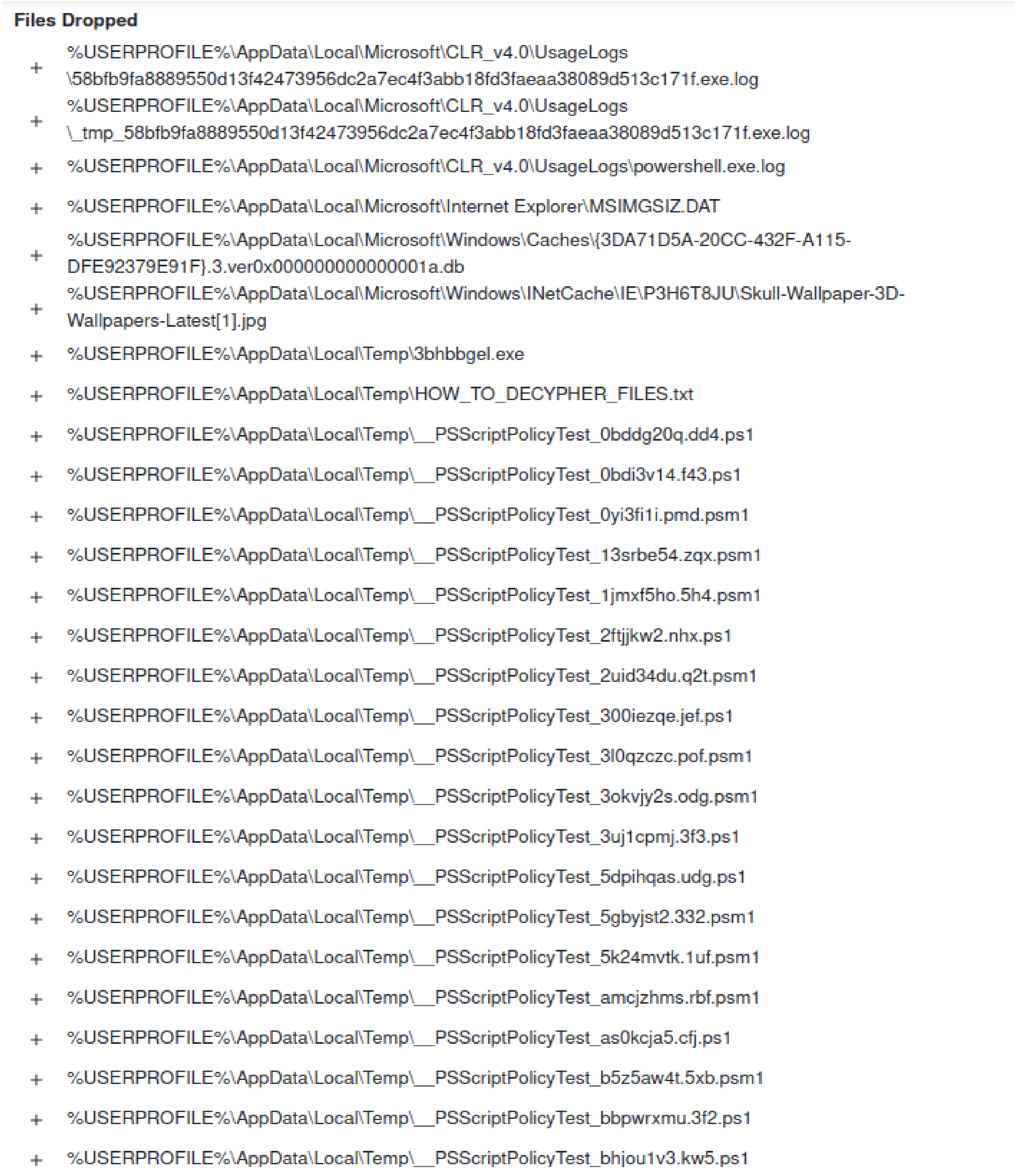
user32.dll

advapi32.dll

kernel32

DLL files are code libraries that can be used by more than one program at the same time.

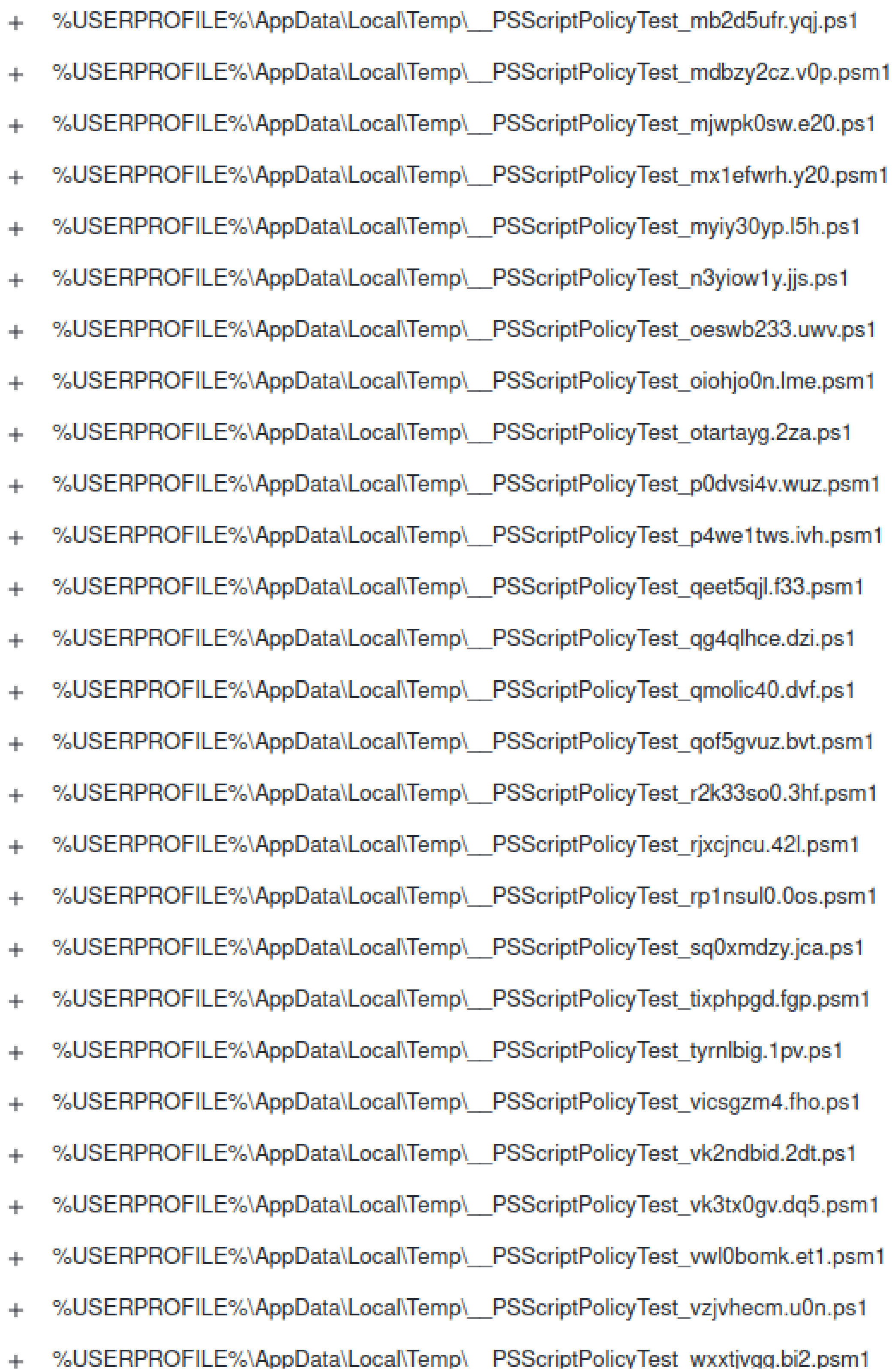
- Dropped files



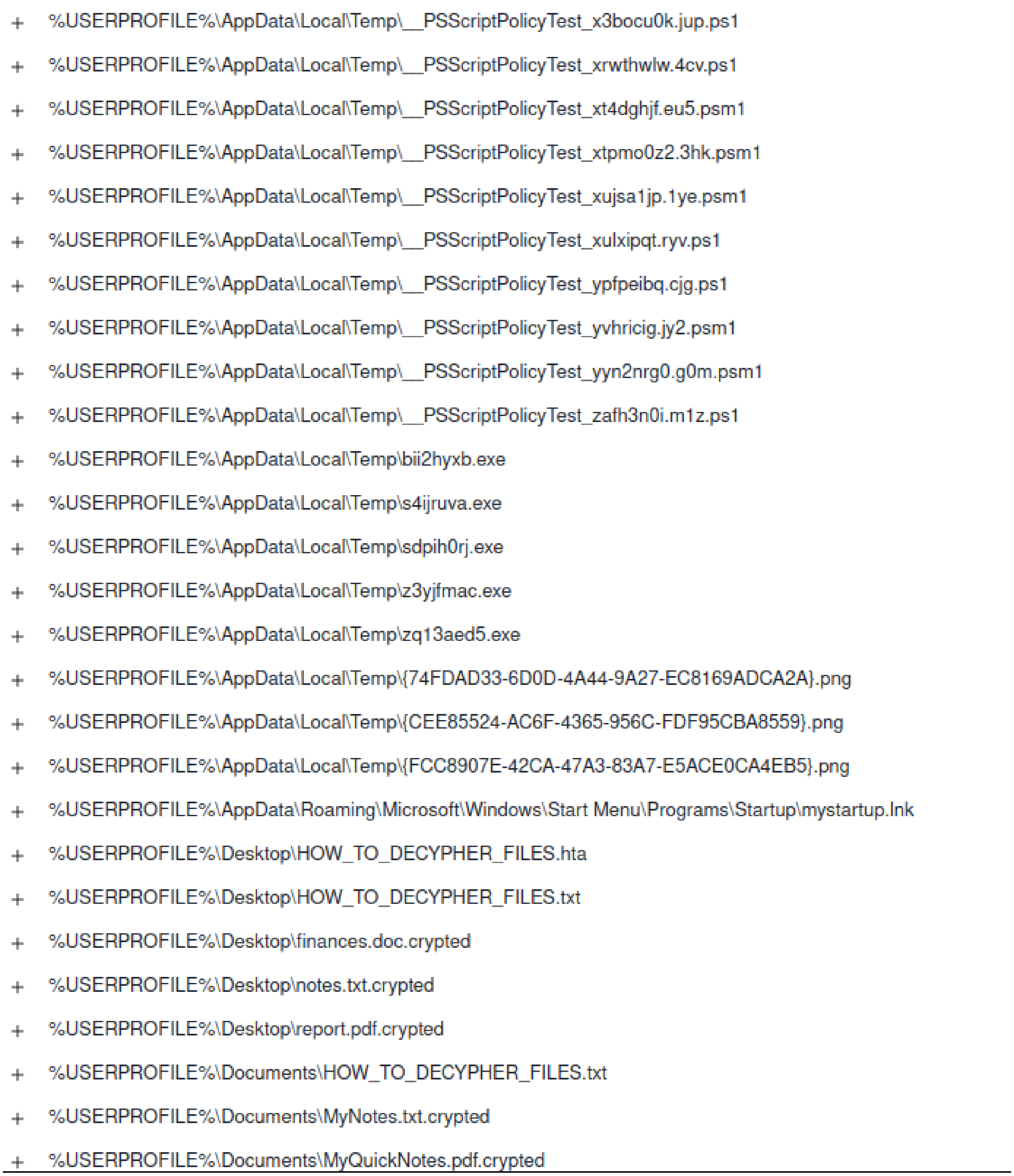
Files Dropped

```
+ %USERPROFILE%\AppData\Local\Microsoft\CLR_v4.0\UsageLogs
  \58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f.exe.log
+ %USERPROFILE%\AppData\Local\Microsoft\CLR_v4.0\UsageLogs
  \_tmp_58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f.exe.log
+ %USERPROFILE%\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log
+ %USERPROFILE%\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
+ %USERPROFILE%\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-
  DFE92379E91F}.3.ver0x000000000000001a.db
+ %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\IE\P3H6T8JU\Skull-Wallpaper-3D-
  Wallpapers-Latest[1].jpg
+ %USERPROFILE%\AppData\Local\Temp\3bhbbgel.exe
+ %USERPROFILE%\AppData\Local\Temp\HOW_TO_DECYPHER_FILES.txt
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_0bddg20q.dd4.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_0bdi3v14.f43.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_0yi3fi1i.pmd.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_13srbe54.zqx.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_1jmxf5ho.5h4.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_2ftjjkw2.nhx.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_2uid34du.q2t.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_300iezqe.jef.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_3l0qzczc.pof.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_3okvjy2s.odg.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_3uj1cpmj.3f3.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_5dpihqas.udg.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_5gbyjst2.332.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_5k24mvtk.1uf.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_amcjzhms.rbf.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_as0kcja5.cfj.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_b5z5aw4t.5xb.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_bbpwrxmu.3f2.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_bhjou1v3.kw5.ps1
```

- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_bodabkvg.qmd.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_cfjgpk5h.oye.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_cfxt1eq0.dsd.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_csnwodlk.wpw.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_cv10h0ni.1mx.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_cypg4b1p.y5p.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_dc03cyei.3h3.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_dfklivaj.pfc.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_e4nnen3l.sxy.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_ebxho4hj.3oe.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_fhv5x2zi.fzk.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_fy55yh4f.toz.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_g14ma13o.dae.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_g1x1jk3h.blb.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_g51dwxim.3a5.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_gc0y4oos.eex.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_ifqdfnj5.g0j.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_ilbvb4ba.tbb.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_imzizjh2.bou.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_ipvh0u3q.qwf.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_jgvt2buh.ysa.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_kc1hdjdo.11k.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_khklay3u.t2f.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_kzm5ym3p.q2m.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_m1of23dn.uog.psm1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_m3c221re.pba.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_m3rljnfm.53w.ps1
- %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_m5hobvqk.bmt.ps1



+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_mb2d5ufr.yqj.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_mdbzy2cz.v0p.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_mjwpk0sw.e20.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_mx1efwrh.y20.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_myiy30yp.l5h.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_n3yiow1y.jjs.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_oeswb233.uwv.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_oiohjo0n.lme.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_otartayg.2za.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_p0dvsi4v.wuz.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_p4we1tws.ivh.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_qeet5qjl.f33.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_qg4qlhce.dzi.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_qmolic40.dvf.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_qof5gvuz.bvt.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_r2k33so0.3hf.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_rjxcjncu.42l.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_rp1nsul0.0os.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_sq0xmdzy.jca.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_tixphpgd.fgp.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_tyrnlbig.1pv.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_vicsgzm4.fho.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_vk2ndbid.2dt.ps1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_vk3tx0gv.dq5.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_vwl0bomk.et1.psm1
+ %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_vzjvhecm.u0n.ps1
+ %USERPROFILE%\AppData\Local\Temp\   PSScriptPolicyTest wxxtjvgg.bi2.psm1

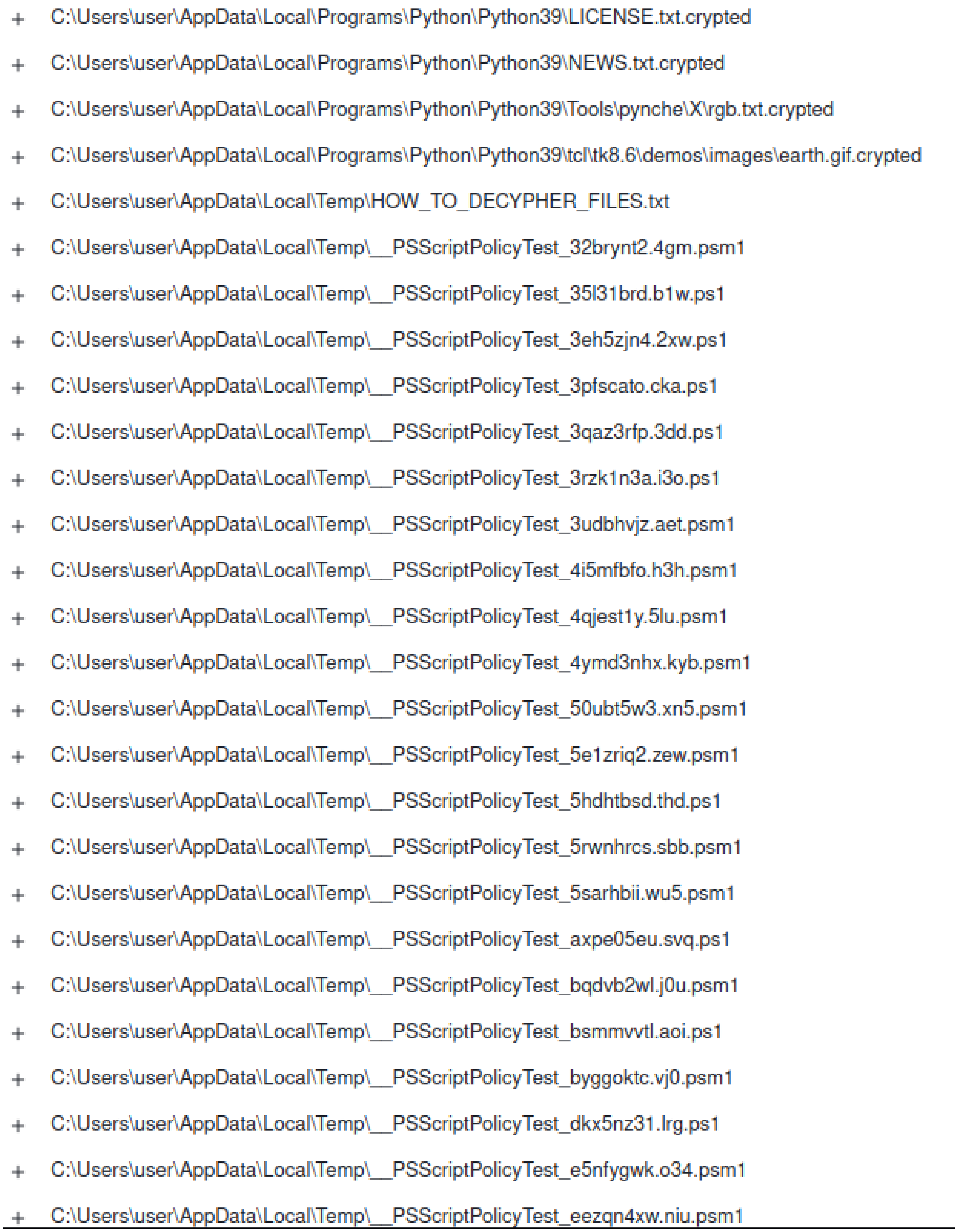


```
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_x3bocu0k.jup.ps1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_xrwthwlw.4cv.ps1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_xt4dghjf.eu5.psm1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_xtpmo0z2.3hk.psm1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_xujsa1jp.1ye.psm1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_xulxipqt.ryv.ps1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_ypfpeibq.cjg.ps1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_yvhricig.jy2.psm1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_yyn2nrg0.g0m.psm1
+   %USERPROFILE%\AppData\Local\Temp\__PSScriptPolicyTest_zafh3n0i.m1z.ps1
+   %USERPROFILE%\AppData\Local\Temp\bii2hyxb.exe
+   %USERPROFILE%\AppData\Local\Temp\s4ijruva.exe
+   %USERPROFILE%\AppData\Local\Temp\sdpih0rj.exe
+   %USERPROFILE%\AppData\Local\Temp\z3yjfmac.exe
+   %USERPROFILE%\AppData\Local\Temp\zq13aed5.exe
+   %USERPROFILE%\AppData\Local\Temp\{74FDAD33-6D0D-4A44-9A27-EC8169ADCA2A}.png
+   %USERPROFILE%\AppData\Local\Temp\{CEE85524-AC6F-4365-956C-FDF95CBA8559}.png
+   %USERPROFILE%\AppData\Local\Temp\{FCC8907E-42CA-47A3-83A7-E5ACE0CA4EB5}.png
+   %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mystartup.lnk
+   %USERPROFILE%\Desktop\HOW_TO_DECYPHER_FILES.hta
+   %USERPROFILE%\Desktop\HOW_TO_DECYPHER_FILES.txt
+   %USERPROFILE%\Desktop\finances.doc.crypted
+   %USERPROFILE%\Desktop\notes.txt.crypted
+   %USERPROFILE%\Desktop\report.pdf.crypted
+   %USERPROFILE%\Documents\HOW_TO_DECYPHER_FILES.txt
+   %USERPROFILE%\Documents\MyNotes.txt.crypted
+   %USERPROFILE%\Documents\MyQuickNotes.pdf.crypted
```

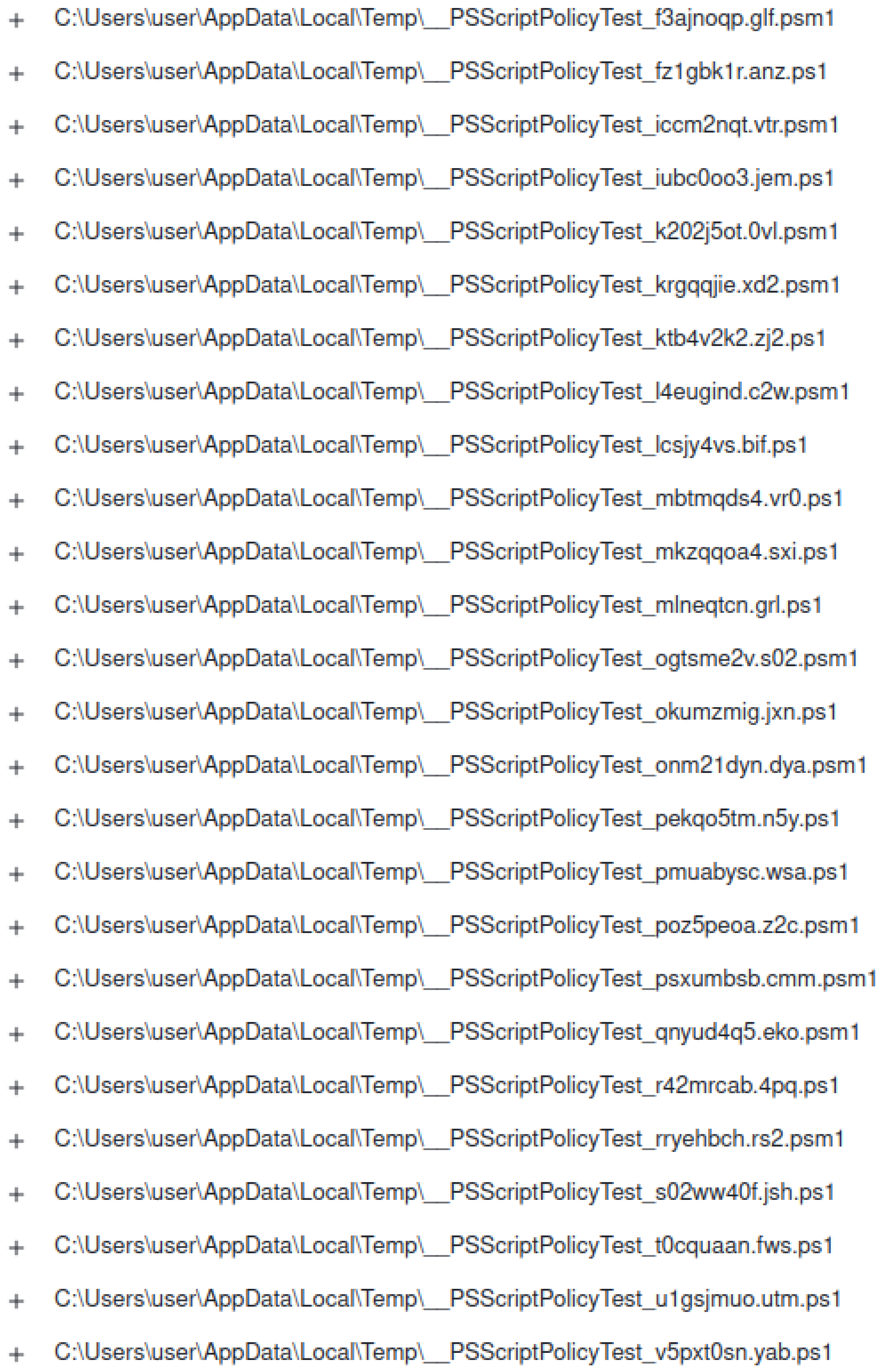
+ %USERPROFILE%\Documents\Outlook Files\HOW_TO_DECYPHER_FILES.txt
+ %USERPROFILE%\Documents\Outlook Files\Outlook.pst.crypted
+ %USERPROFILE%\Documents\WorkSlideshow.ppt.crypted
+ %USERPROFILE%\Documents\finances.doc.crypted
+ %USERPROFILE%\Documents\notes.txt.crypted
+ %USERPROFILE%\Documents\passwords&pics.docx.crypted
+ %USERPROFILE%\Documents\report.pdf.crypted
+ %USERPROFILE%\Downloads\HOW_TO_DECYPHER_FILES.txt
+ %USERPROFILE%\Downloads\summerend.jpg.crypted
+ %USERPROFILE%\Music\FavSong1.mp3.crypted
+ %USERPROFILE%\Music\FavSong2.mp3.crypted
+ %USERPROFILE%\Music\HOW_TO_DECYPHER_FILES.txt
+ %USERPROFILE%\Pictures\HOW_TO_DECYPHER_FILES.txt
+ %USERPROFILE%\Pictures\RoadTown.jpg.crypted
+ %USERPROFILE%\Pictures\angela.jpg.crypted
+ %USERPROFILE%\Pictures\jenny.jpg.crypted
+ %USERPROFILE%\Videos\HOW_TO_DECYPHER_FILES.txt
+ %USERPROFILE%\Videos\funny_video.mp4.crypted
+ C:\$RECYCLE.BIN
+ C:\$RECYCLE.BIN\%SID%
+ C:\$RECYCLE.BIN\%SID%\desktop.ini
+ C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\HOW_TO_DECYPHER_FILES.txt
+ C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png.crypted
+ C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png.crypted
+ C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png.crypted

+ C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png.crypted
+ C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\HOW_TO_DECYPHER_FILES.txt
+ C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png.crypted
+ C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png.crypted
+ C:\ProgramData\Microsoft\Diagnosis\HOW_TO_DECYPHER_FILES.txt
+ C:\ProgramData\Microsoft\Storage Health\HOW_TO_DECYPHER_FILES.txt
+ C:\ProgramData\Microsoft\Storage Health\StorageHealthModel.dat.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\Abby.dat.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\HOW_TO_DECYPHER_FILES.txt
+ C:\ProgramData\Microsoft\User Account Pictures\defaultuser0.dat.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\guest.png.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\user-192.png.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\user-32.png.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\user-40.png.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\user-48.png.crypted
+ C:\ProgramData\Microsoft\User Account Pictures\user.png.crypted
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WERCAAD.tmp
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WERCAAD.tmp.WERInternalMetadata.xml
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WERCABF.tmp
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WERCABF.tmp.csv
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBA8.tmp
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBA8.tmp.WERInternalMetadata.xml
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC73.tmp
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC73.tmp.csv
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WERECB2.tmp

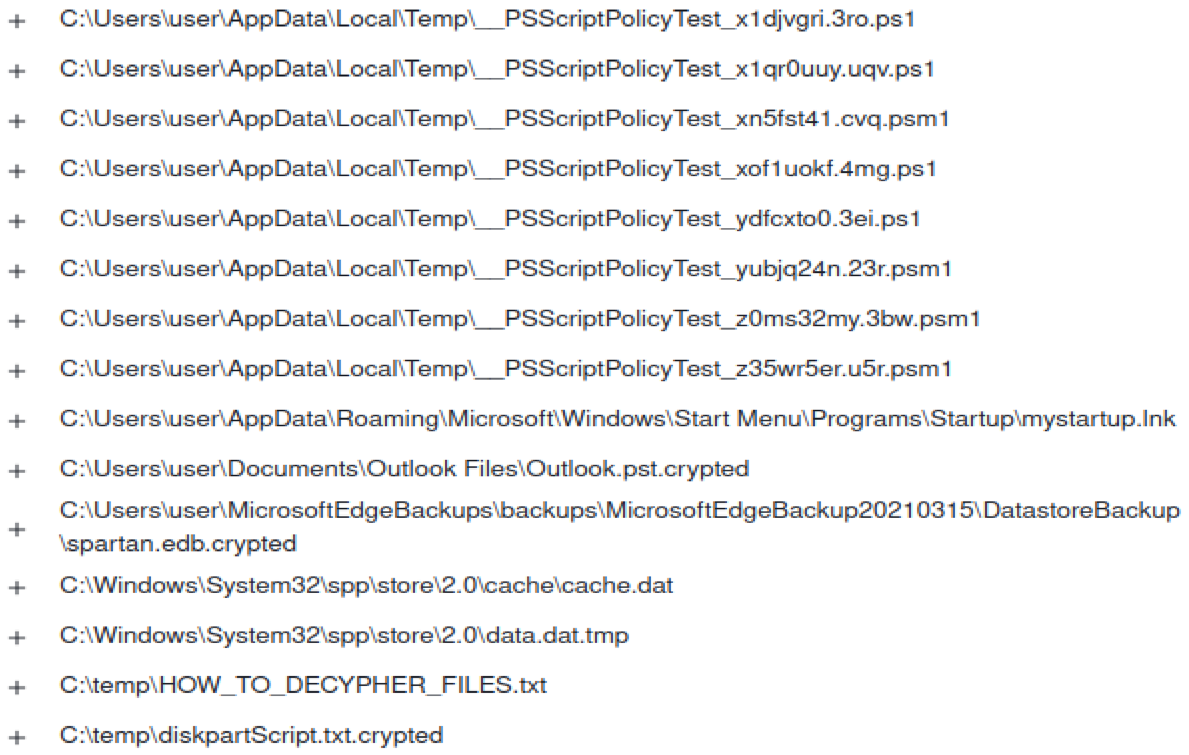
+ C:\ProgramData\Microsoft\Windows\WER\Temp\WERECB2.tmp.txt
+ C:\Users\Admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
+ C:\Users\Admin\AppData\Local\Temp\RGI989C.tmp
+ C:\Users\Admin\AppData\Local\Temp\RGI9968.tmp
+ C:\Users\Admin\AppData\Local\Temp\RGI9979.tmp
+ C:\Users\Admin\AppData\Local\Temp\RGI998A.tmp
+ C:\Users\Admin\AppData\Local\Temp\RGI99C9.tmp
+ C:\Users\Admin\AppData\Local\Temp\TMP4352$.TMP
+ C:\Users\Admin\AppData\Local\Temp\hkehc13w.2ty.psm1
+ C:\Users\Admin\AppData\Local\Temp\hs5b1i3g.sbt.ps1
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ETCJ2WHM\RE4nqTh[1].png.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ETCJ2WHM\RWFFrK[1].png.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ETCJ2WHM\edge[1].htm.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\RE4GhRT[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\RE4Y415[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\RE4YbW8[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\RE4ncJa[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\RWMIHM[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\RWQD5M[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\RWQN5w[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\F2EF8UYV\aabe8539-2c25-4f4a-9e34-a4531e76ccf5[1].dat.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\R0IAZP7Z\RE4Vu9f[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\R0IAZP7Z\RE4VvRZ[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\R0IAZP7Z\RE4VvS2[1].jpg.crypted
+ C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\R0IAZP7Z\RE4YbW5[1].jpg.crypted



```
+ C:\Users\user\AppData\Local\Programs\Python\Python39\LICENSE.txt.crypted
+ C:\Users\user\AppData\Local\Programs\Python\Python39\NEWS.txt.crypted
+ C:\Users\user\AppData\Local\Programs\Python\Python39\Tools\pynche\X\rgb.txt.crypted
+ C:\Users\user\AppData\Local\Programs\Python\Python39\tcl\tk8.6\demos\images\earth.gif.crypted
+ C:\Users\user\AppData\Local\Temp\HOW_TO_DECYPHER_FILES.txt
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_32brynt2.4gm.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_35l31brd.b1w.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_3eh5zjn4.2xw.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_3pfscato.cka.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_3qaz3rfp.3dd.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_3rzk1n3a.i3o.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_3udbhvjz.aet.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_4i5mfbfo.h3h.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_4qjest1y.5lu.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_4ymd3nhx.kyb.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_50ubt5w3.xn5.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_5e1zriq2.zew.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_5hdhtbsd.thd.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_5rwnhrcs.sbb.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_5sarhbii.wu5.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_axpe05eu.svq.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_bqdvb2wl.j0u.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_bsmmvvtl.aoi.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_byggoktc.vj0.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_dkx5nz31.lrg.ps1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_e5nfygwk.o34.psm1
+ C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_eezqn4xw.niu.psm1
```

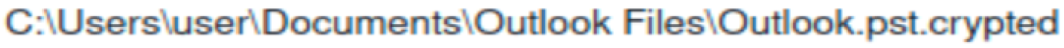


```
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_f3ajnoqp.glf.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_fz1gbk1r.anz.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_iccm2nqt.vtr.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_iubc0oo3.jem.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_k202j5ot.0vl.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_krgqqjie.xd2.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_ktb4v2k2.zj2.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_l4eugind.c2w.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_lcsjy4vs.bif.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_mbtmqds4.vr0.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_mkzqqoa4.sxi.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_mlneqtcn.grl.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_ogtsme2v.s02.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_okumzmig.jxn.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_onm21dyn.dya.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_pekqo5tm.n5y.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_pmuabysc.wsa.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_poz5peoa.z2c.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_psxumbsb.cmm.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_qnyud4q5.eko.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_r42mrcab.4pq.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_rryehbch.rs2.psm1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_s02ww40f.jsh.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_t0cquaan.fws.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_u1gsjmuo.utm.ps1
+  C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_v5pxt0sn.yab.ps1
```



- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_x1djvgri.3ro.ps1
- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_x1qr0uuy.uqv.ps1
- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_xn5fst41.cvq.psm1
- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_xof1uokf.4mg.ps1
- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_ydfcxto0.3ei.ps1
- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_yubjq24n.23r.psm1
- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_z0ms32my.3bw.psm1
- C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_z35wr5er.u5r.psm1
- C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mystartup.lnk
- C:\Users\user\Documents\Outlook Files\Outlook.pst.crypted
- C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20210315\DatastoreBackup\spartan.edb.crypted
- C:\Windows\System32\spp\store\2.0\cache\cache.dat
- C:\Windows\System32\spp\store\2.0\data.dat.tmp
- C:\temp\HOW_TO_DECYPHER_FILES.txt
- C:\temp\diskpartScript.txt.crypted

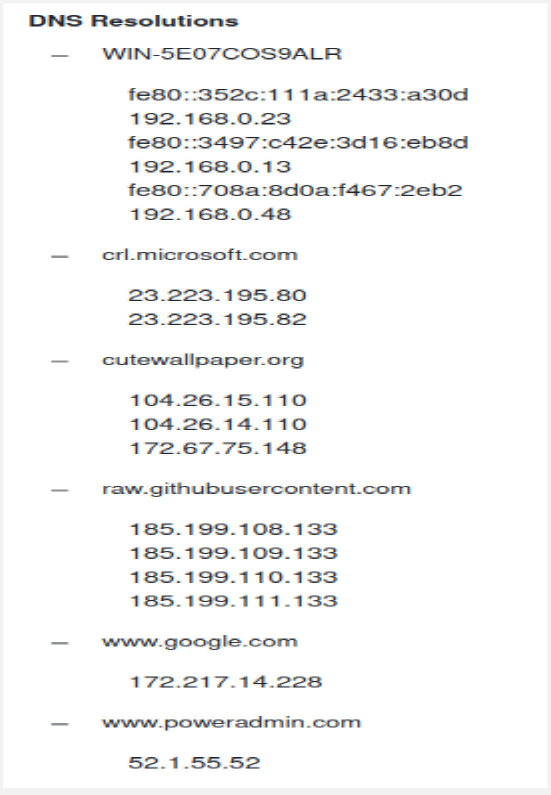
These are all the files that were created when the malware was ran in VirusTotal's sanbox environment.



C:\Users\user\Documents\Outlook Files\Outlook.pst.crypted

This dropped file seems to be an encrypting user's outlook pst file which contain's user's Outlook emails stored on the computer (Outlook's file are cached on the system, hence their emails are stored on the system).

●DNS info



```
DNS Resolutions
  —   WIN-5E07COS9ALR

        fe80::352c:111a:2433:a30d
        192.168.0.23
        fe80::3497:c42e:3d16:eb8d
        192.168.0.13
        fe80::708a:8d0a:f467:2eb2
        192.168.0.48

  —   crl.microsoft.com

        23.223.195.80
        23.223.195.82

  —   cutewallpaper.org

        104.26.15.110
        104.26.14.110
        172.67.75.148

  —   raw.githubusercontent.com

        185.199.108.133
        185.199.109.133
        185.199.110.133
        185.199.111.133

  —   www.google.com

        172.217.14.228

  —   www.poweradmin.com

        52.1.55.52
```

Virustotal detected these DNS resolutions used by our malware file to translate domain names to IP addresses. If any of these DNS resolution systems are compromised, we can under attacks such as DDOS and DNS Hijacking.

Conclusion:

In this lab, we first analyzed the njrat malware file. We used the strings command to see what strings are inside the file. This allowed us to take the strings and use them to write a yara rule. The yara rule confirmed for us that the njrat file is indeed a malware file by checking 10 of the strings written out in the rule.

Next, we moved onto task two. We used 7 different yara rules and scanned a directory containing 33 different types of malware files. By scanning these malware samples using these 7 yara rules, we were able to identify the number of malware samples detected by each yara rule. We used a bar graph to better illustrate our results.

Lastly, we finished up this lab doing task three. We were assigned our specific malware file and used virustotal to investigate this malware file. We provided information on the following: Hashes - md5, sha1sum, sha256sum, Yara rule, Common Windows API used, Network communication, Persistence mechanism, Imported DLLs (Dynamically Loaded Libraries), Dropped files , and DNS info. We proceeded to break down each of the suspicious activities and provide research on each one.

Overall, this lab allowed us to learn how to create a yara rule, investigate different types of malware files, and lastly further investigate the different aspects of malware files.