Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

Reversing Project

Hassan Alshehri

Malware: xblkpfZ8Y4.exe

SOURCE:

urlhaus.abuse.ch/url/3308463/

HOST:

158.101.35.62

SHA-1:

6e45a340c41c62cd51c5e6f3b024a73c7ac85f88

SHA-256:

832640671878e0d9a061d97288ffaae303ba3b4858ed5d675c2170e7770ec8a6

Analysis Stages

1. Basic Static Analysis
    a. Strings
    b. UPX
    c. PEview and Resource Hacker
    d. VirusTotal
2. Basic Dynamic Analysis
    a. Regshot
    b. Process Monitor
3. Advanced Static Analysis
    a. IDA
4. Advanced Dynamic Analysis
    a. X64dbg

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

Basic Static Analysis

1 Strings

```
C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>strings64 xblkpfZ8Y4.exe |more

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
UPX0
UPX1
.rsrc
4.24
UPX!
uIA
/K_
cY-Z
jKQ
w>1
 Os
6T\
4&Hz
*4^
O"d
z>v
5~e
bG@
```

First I try to do “String64” and without any string option and it give me a lot of the length that are c but you can see in the screenshot that the malware is in “UPX” which is a subset of the obfuscated hidding in the malware and you can see in the malware it is not in “DOS mode” which is massage to typical in PE which is a portable executable files showe that the binary is likely a Windows executable.

```
C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>strings64 -n 6 xblkpfZ8Y4.exe |more

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
XdfJ5V#UH+
tp3j)T5~
KD?M$n
IZHEE-K
p{y8&w+
U0;h]L
p`/y`~p
?S6q#n
k\dkqyf
}OH80f
FDb!-g
Fg-F$!
-+H/C@p
$<\V]F;t9
_[AtC)(
cC(J(Z
$]d4U>w
:ayA?Qo
6or-H2lO
hJ/MN%
[^v8Lz
```

Ater that I try to do a “String64” with “-n 6” option which is to get rid of the string that of 6 length and below which is the gibberish string that are completely worthless from the reversing perspective and in the “String64” with “-n 6” option give me a lot of useful information which is this:

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level="asInvoker"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
  <compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
    <application>
      <!--The ID below indicates application support for Windows Vista -->
      <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/>
      <!--The ID below indicates application support for Windows 7 -->
      <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
      <!--The ID below indicates application support for Windows 8 -->
      <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/>
      <!--The ID below indicates application support for Windows 8.1 -->
      <supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/>
      <!--The ID below indicates application support for Windows 10 -->
      <supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"/>
    </application>
  </compatibility>
</assembly>
ADVAPI32.dll
CRYPT32.dll
dbghelp.dll
IPHLPAPI.DLL
KERNEL32.DLL
msvcrt.dll
ole32.dll
SHELL32.dll
USER32.dll
USERENV.dll
WS2_32.dll
FreeSid
CertOpenStore
SymGetOptions
GetAdaptersAddresses
ExitProcess
GetProcAddress
LoadLibraryA
VirtualProtect
CoTaskMemFree
SHGetKnownFolderPath
ShowWindow
GetUserProfileDirectoryW
```

For the first part of the screenshot which is the “Embedded XML” the manifest specifies with compatibility different Windows versions which is the “Windows 7” and “Windows 8” and “Windows 8.1” and “Windows 10” and this make it smooth to execution in multiple windows platforms and in the same XML there is a “<requestedExecutionLevel level-"asInvoker"/>” which is a set to make the program runs with the same privileges as the user.

For the second part of the screenshot which is the “DLLs and Functions” the program has a lot of the Windows API libraries like “KERNEL32.DLL” which is used for the core system operation. The next one is “USER32.dll” which is used for the handle user interface-related functions. The next one is “ADVAPI32.dll” which is used to provide access to the advanced Windows features such as security and registry functions. The next one is “WS2_32.dll” which is used to networking capabilities. The next one is “CRYPT32.dll” which is used to encryption or decryption functionality might be present. The next one is “IPHLPAPI.DLL” which is used to provides a set of the network-related functions like information about the IP configurations and routing and interfaces. There is other DLL like “dbghelp.dll” and “USERENV.dll” and “msvcrt.dll” and these libraries together make the program more adaptable which is allowing to deal with important system components like network configurations and encryption and even debugging processes.

For the function part like “CertOpenStore” which is to open the certificate store and it is for certificates used in authentication or encryption. The next one is “GetAdaptersAddresses” which is to get the IP address configuration of the network adapters. The next one is “ExitProcess” which is used to ends the all of caller process and all of its threads which to make a cleanly exit for the program. The next one is “GetProcAddress” which is to get the address of the imported function or variable from a DLL. The next

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

one is “LoadLibraryA” which is used to install the DLL in the address space of the calling process which is maybe used to install hidden libraries. The next one is “SHGetKnownFolderPath” which is used to get the path of know folder. The next one is “ShowWindow” which is used to set the view o the window. The next one is “GetUserProfileDirectoryW” which is used to get the directory path for the user. There is other function like “FreeSid” and “SymGetOptions” and “VirtualProtect” and “CoTaskMemFree” and this function make the program adaptable which is allowing for interaction with user-specific directories and the network configurations and memory management and certificates.

2 UPX

```
C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>upx -o unpacked_xblkpfZ8Y4.exe -d xblkpfZ8Y4.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.2       Markus Oberhumer, Laszlo Molnar & John Reiser    Jan 3rd 2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   9561088 <-   2995200   31.33%    win64/pe     unpacked_xblkpfZ8Y4.exe

Unpacked 1 file.
```

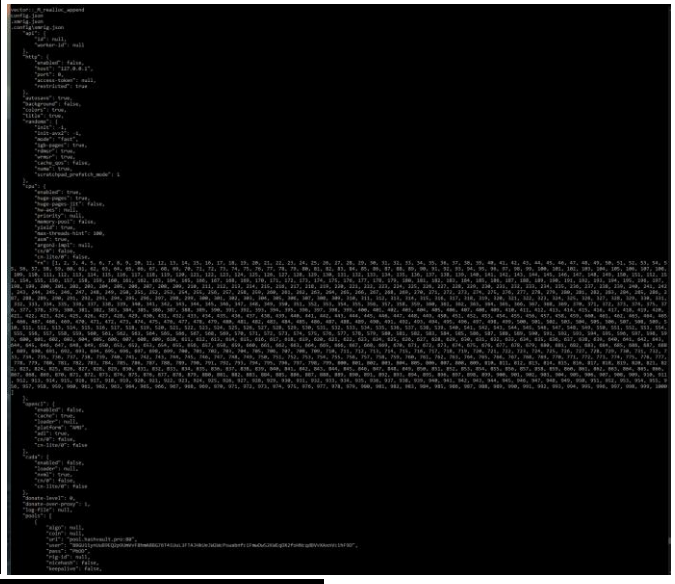
The next thing I do after the “String64” is to unpacked any UPX packet after I notes that the program has a UPX and in the command was “upx -o unpacked_xblkpfZ8Y4.exe -d xblkpfZ8Y4.exe” the “-o” option to make the output of the program and the option “-d” to decompress.

Then I put the unpacked program in the “String64” without option and this is what I gat:

```
C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>strings64 unpacked_xblkpfZ8Y4.exe |more

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
.text
`.data
.rdata
@.pdata
@.xdata
@.bss
.idata
.CRT
.tls
.rsrc
@.reloc
ff.
8MZu
HcP<H
8PE
tfH
tP1
tEf
D$
ATUWVSH
hlO
ttH
 [^_]A\
 [^_]A\
AUATUWVSH
H+u
S(H
C0tcH
```

If you see the program with “String64” before the unpacked there is some different like the “.text” and “.data” and “@.pdata” and “@.xdata” and “@.bss” and “.idata” and “.CRT” and “.t1s” and “.rsrc” and “@.reloc” and this all are a sections of a Portable Executable (PE) file format which is used to define the structure of a Windows executable or the DLL and the program give me a lot of the length that are gibberish string.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
Then I put the unpacked program in the “String64” with option “-n 6” so can I get a good view of the string and this is what I get:



There is a lot going on with this program and here some of it I think there is a mining algorithm in this malware because of using some of string like this “cryptonight” and “randomx” and “cn-lite” and “cn-heavy” which is a show that the binary is compatible with a variety of mining methods cryptocurrencies.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project


```
    },
    "donate-level": 0,
    "donate-over-proxy": 1,
    "log-file": null,
    "pools": [
        {
            "algo": null,
            "coin": null,
            "url": "pool.hashvault.pro:80",
            "user": "8BGU1iynUuB9EQ2p9UmVvF8hmA8BG76T4iUuL3FTAJHkUeJW2WcPswabnfciFmwDw52KWEqDX2foHNcqdBVvXAxnVcihF9D",
            "pass": "PbOD",
            "rig-id": null,
            "nicehash": false,
            "keepalive": false,
            "enabled": true,
            "tls": false,
            "tls-fingerprint": null,
            "daemon": false,
            "socks5": null,
            "self-select": null,
            "submit-to-origin": false
        },
        {
            "algo": null,
            "coin": null,
            "url": "142.202.242.43:80",
            "user": "8BGU1iynUuB9EQ2p9UmVvF8hmA8BG76T4iUuL3FTAJHkUeJW2WcPswabnfciFmwDw52KWEqDX2foHNcqdBVvXAxnVcihF9D",
            "pass": "PbOD",
            "rig-id": null,
            "nicehash": false,
            "keepalive": false,
            "enabled": true,
            "tls": false,
            "tls-fingerprint": null,
            "daemon": false,
            "socks5": null,
            "self-select": null,
            "submit-to-origin": false
        },
        {
            "algo": null,
            "coin": null,
            "url": "142.202.242.45:80",
            "user": "8BGU1iynUuB9EQ2p9UmVvF8hmA8BG76T4iUuL3FTAJHkUeJW2WcPswabnfciFmwDw52KWEqDX2foHNcqdBVvXAxnVcihF9D",
            "pass": "PbOD",
            "rig-id": null,
            "nicehash": false,
            "keepalive": false,
            "enabled": true,
            "tls": false,
            "tls-fingerprint": null,
            "daemon": false,
            "socks5": null,
            "self-select": null,
            "submit-to-origin": false
        }
```

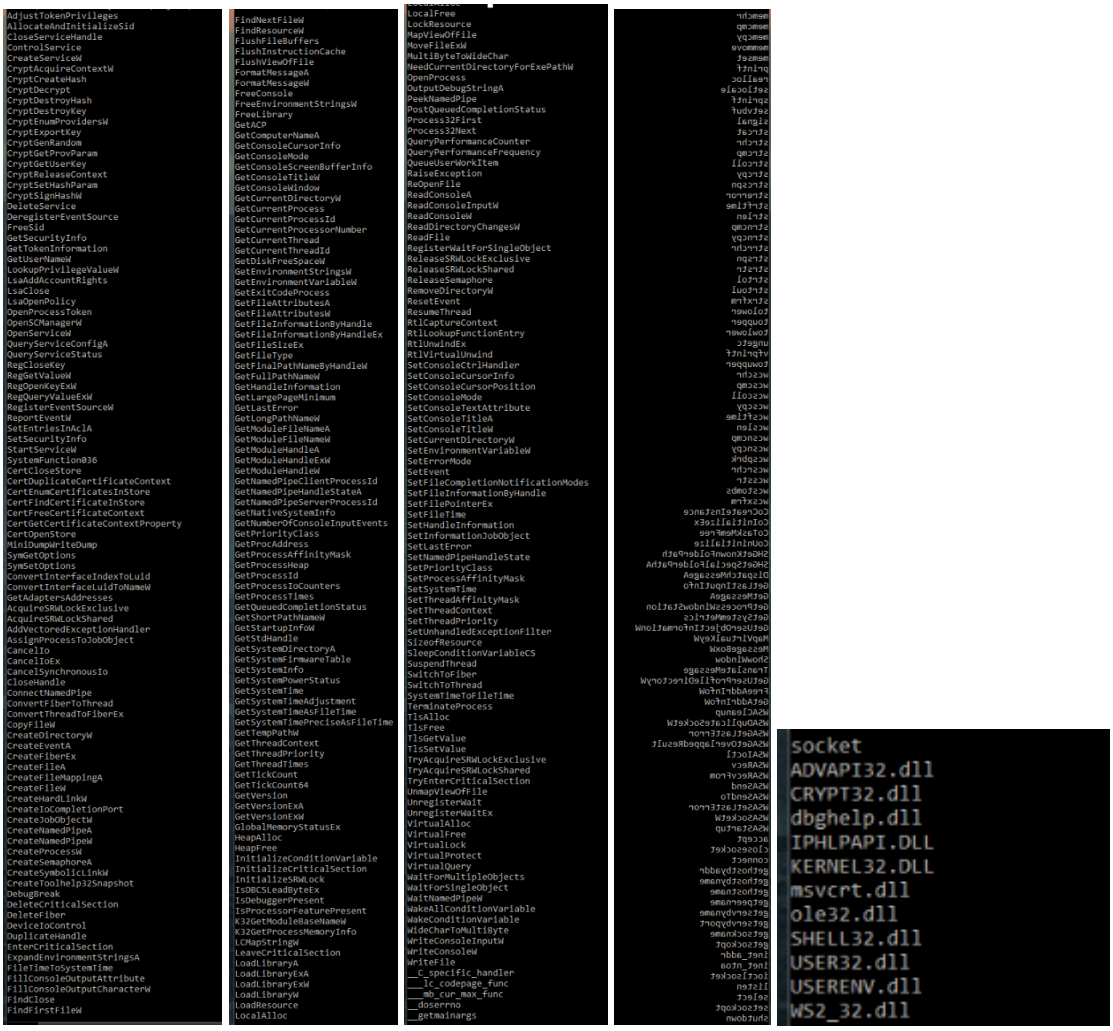

There is also a pool configuration with the mining pool URLs which is a in the “.config\xmrig. Json” and have a mining pool URLs which is a “"pool.hashvault.pro:80" and "142.202.242.45:80” and this address show where the mining tool connected and there is a user and password in the configuration two authenticate the miner with the pool and the user was “8BGU1iynUuB9EQ2p9UmVvF8hmA8BG76T4iUuL3FTAJHkUeJW2WcPswabnfc1FmwDw52KWEqDX2foHNcqdBVvXAxnVcihF9D” and the password was “PbOD”


```
    "randomx": {
        "init": -1,
        "init-avx2": -1,
        "mode": "fast",
        "1gb-pages": true,
        "rdmsr": true,
        "wrmsr": true,
        "cache_qos": false,
        "numa": true,
        "scratchpad_prefetch_mode": 1
    },
```


This is the “randomx” configuration section in the JSON as you can see the “mode” is in “fast” which is for maximum performance which is make it more suspects.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

There is more of the “DLLs and Functions” after the unpacked malware which is a lot compare before the unpacked this show to as that the malware was hidden libraries and the DLLs in the UPX.



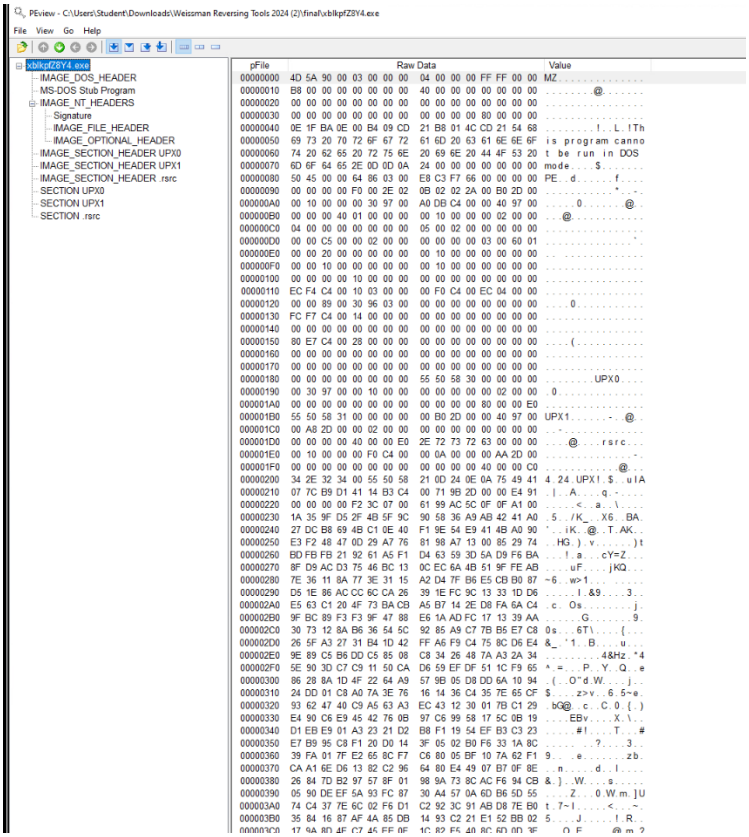
There is some of the impotent functions like “AdjustTokenPrivileges” and “AllocateAndInitializeSid” which is maybe used to give a privilege and management the security token. There is a “GetSecurityInfo” and “SetSecurityInfo” which is to sets the security descriptors. There is a “CreateServiceW” and “StartServiceW” and “DeleteService” which is used to create and start and delete a service which is make it suspects. There is a “CreateFileW” and “DeleteFileW” and “WriteFile” which is to create and delete and write for file. There is a “RegQueryValueExW” and “RegSetValueExW” which is used to querying and set the registry entries.

There is also a “ole32.dll” which is maybe use to allow the malware the link to the embed and link to document and other objects.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

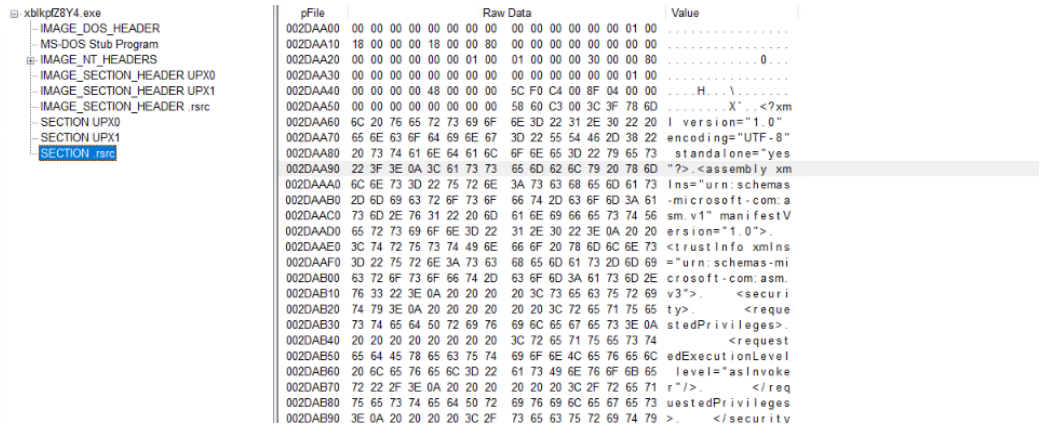
3 PEview and Resource Hacker

Then I use the PEview with the xblkpfZ8Y4.exe to get more information about the Melewar.



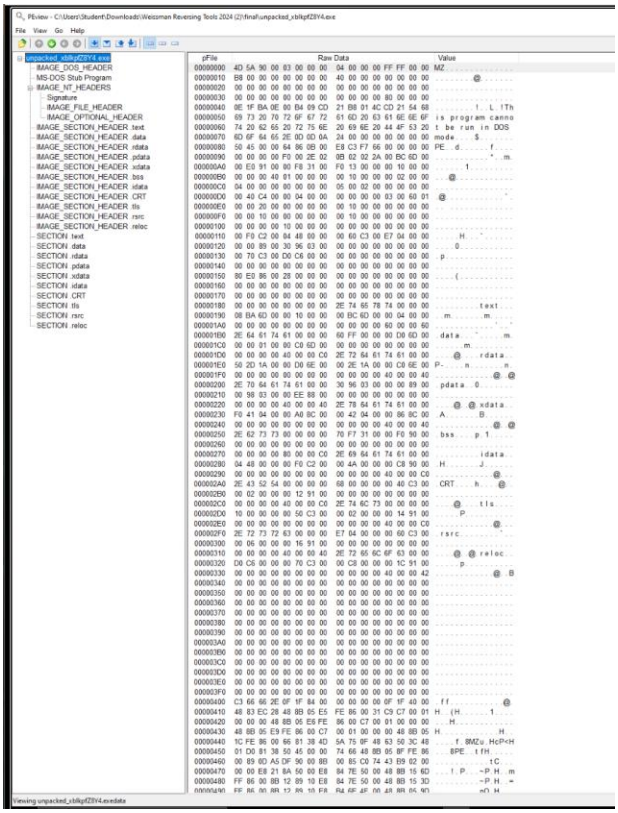
As you can see the first 2 letters in the value sections it is showing the “MZ” which is the “4D 5A” and it is a valid for the DOS which is stander for the all of the PE file. There is a message in the value section which is a “This program cannot be run in DOS mode” which is for the DOS stub displays.

As you can see the “SECTION .rsrc” which is have shown the XML which is the code in the malware that support the Windows operating which is the “Windows 7,8,8.1,10” and the program does not require the administrative privileges



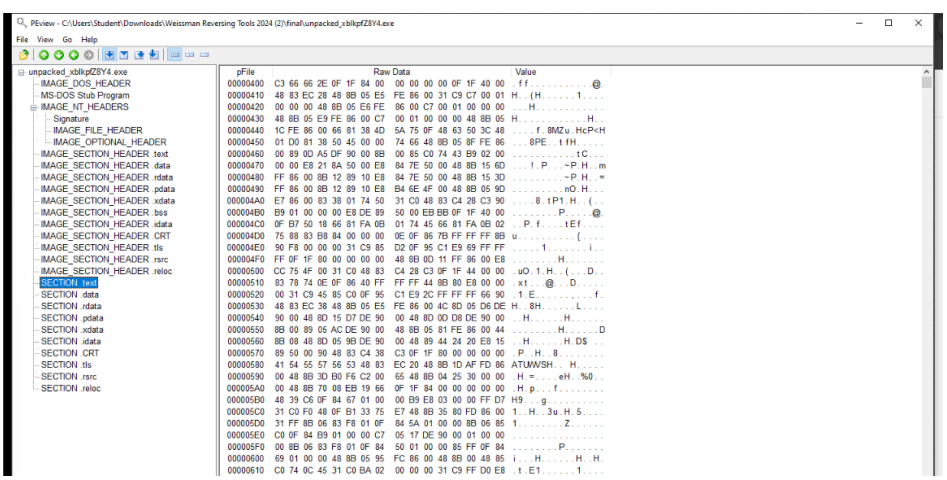
Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

There is “SECTION UPX0” and “SECTION UPX1” which does not have any thing interested so I dosed to put the program after the unpacked and this is what I get:

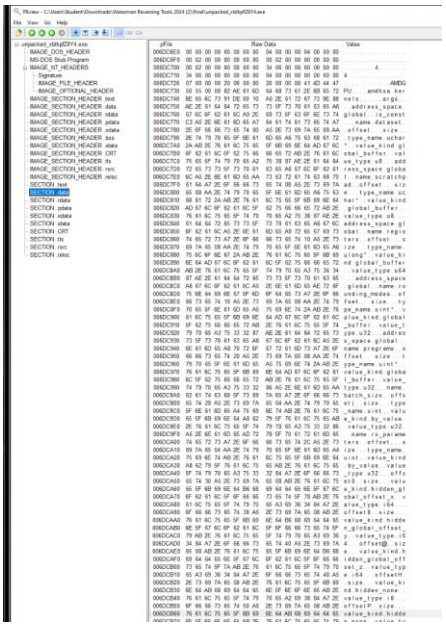


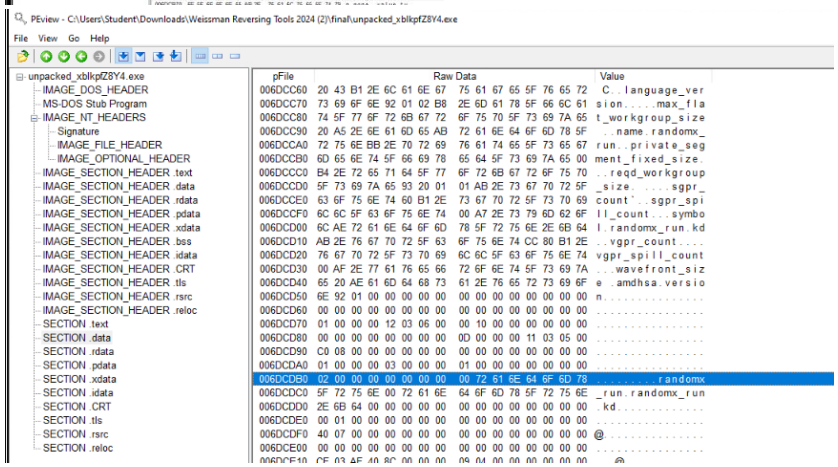
As you can see the program have a lot of the section that was hiding in the UPX like the “SECTION .text” “SECTION .data” “SECTION .rdata” “SECTION ,pdata” “SECTION .xdata” “SECTION .idata” “SECTION .CRT” “SECTION .tls” “SECTION .reloc” and the same with the “IMAGE_SECTION_HEADER”

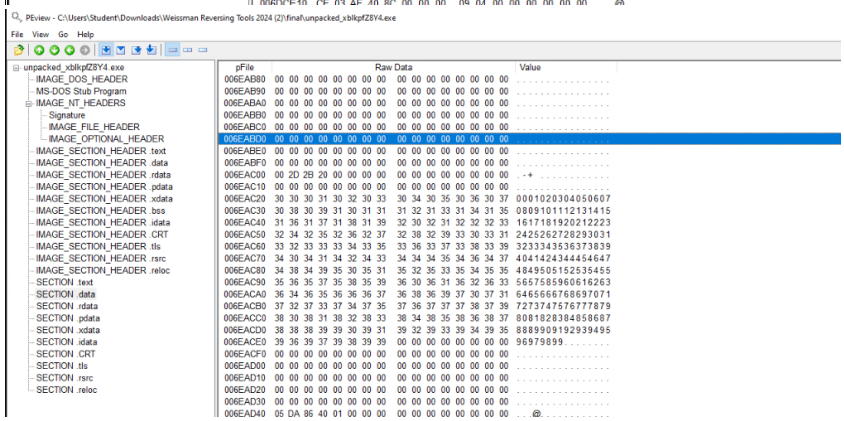
For the first section is the “SECTION .text” which was having nothing there was a lot of the letters with unknown meaning which maybe gibberish string.



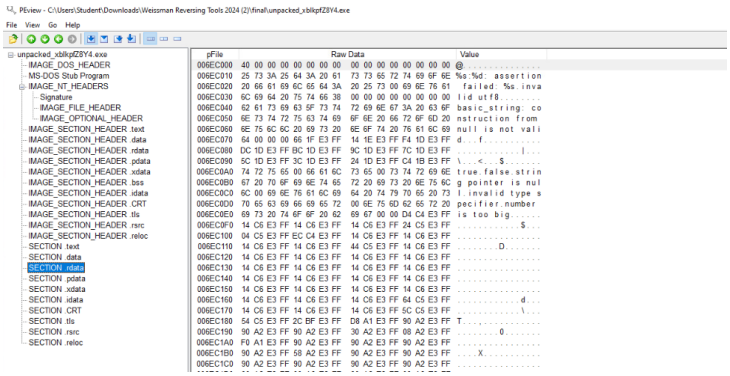
Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
For the second section is the “SECTION .data” which was have a lot of the visible string like “amdhsa.kernels” and “address_space” and “global_buffer” and there have a “randomx_run” and there was a lot of the number that there unknown meaning or gibberish string and have some of unknown sign like “@”

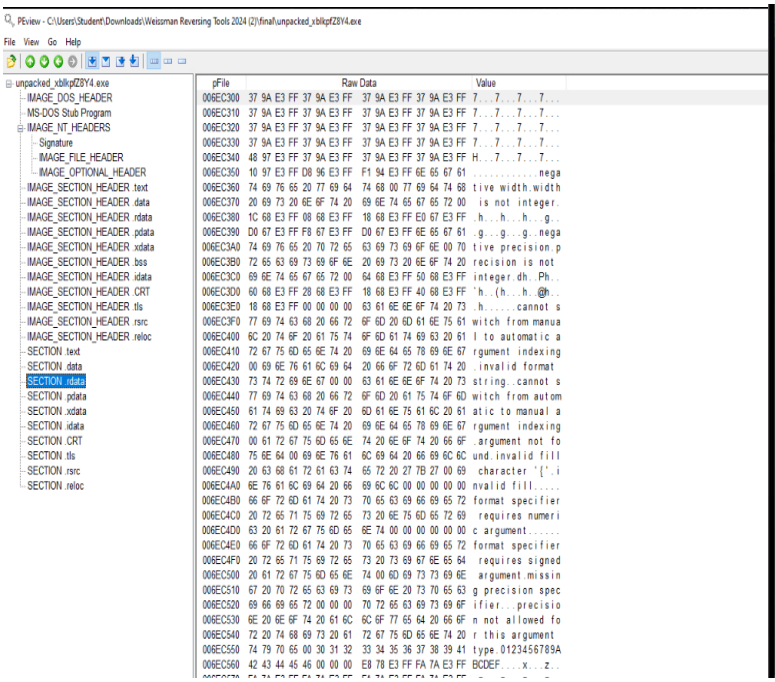


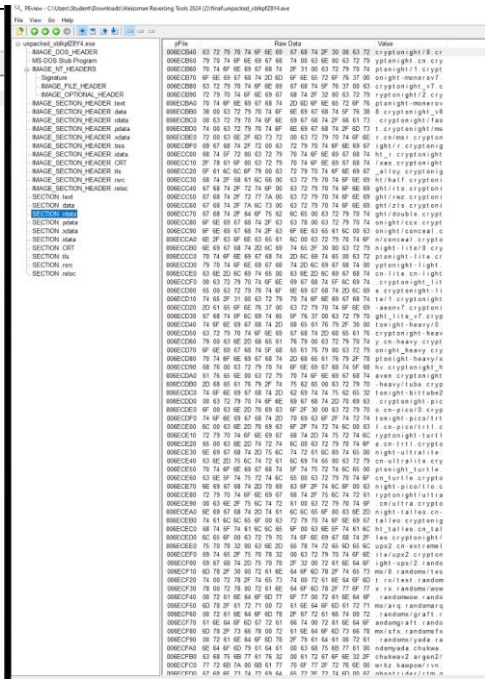


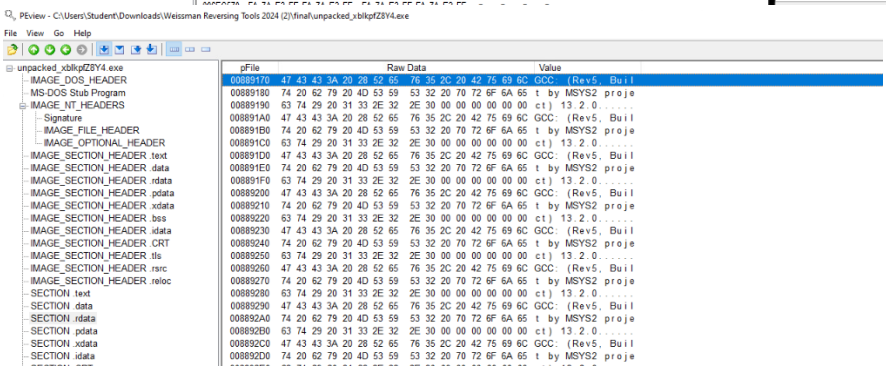


Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
For the next one which is the “SECTION .rdata” was having lot of the information like the crypt string and was having the JSON config code and was having the “GCC: (Rev5. Built by MSYS2 project) 13.2.0” which is used for developers to build the binary platform and was having in different version.

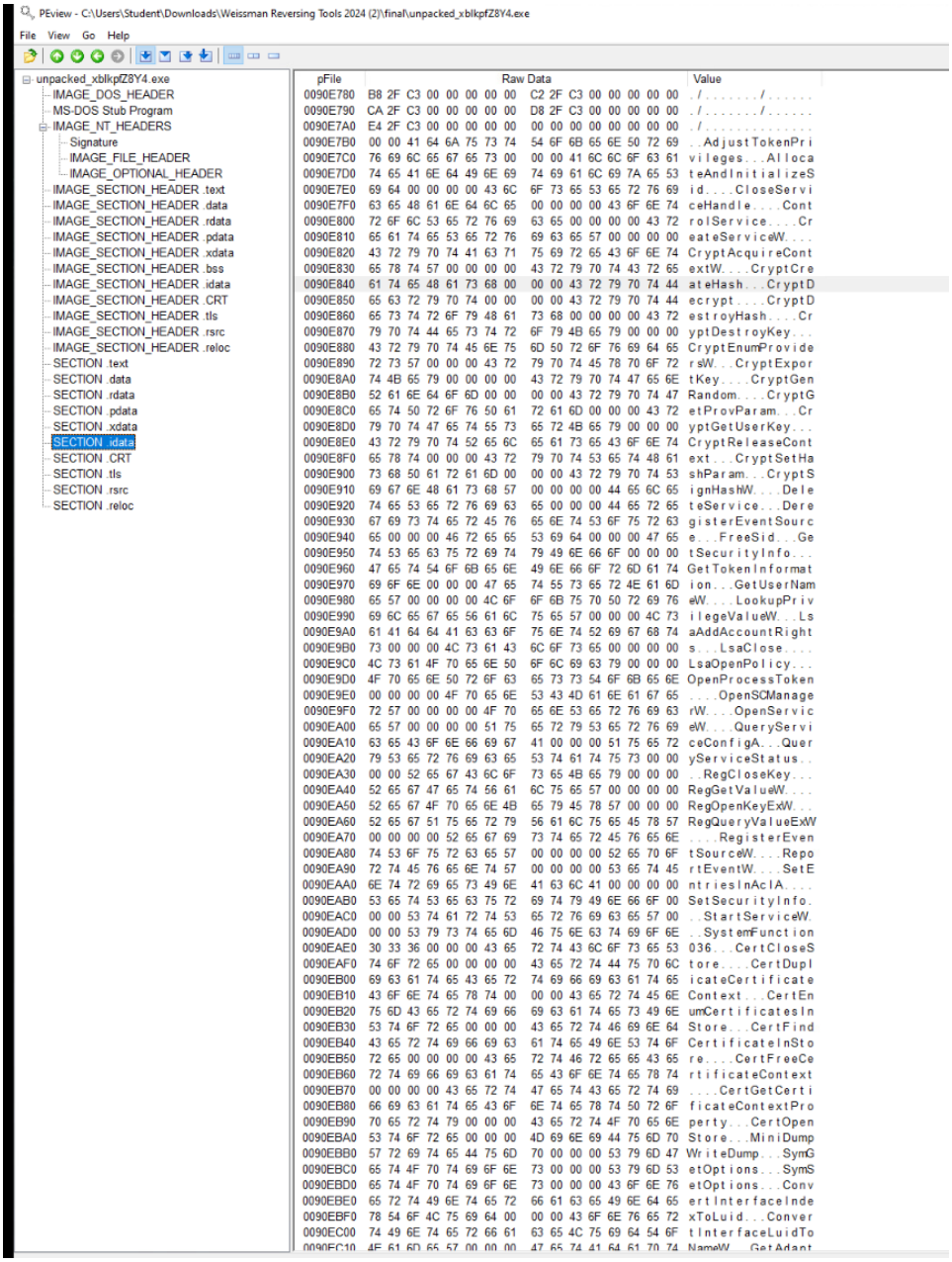


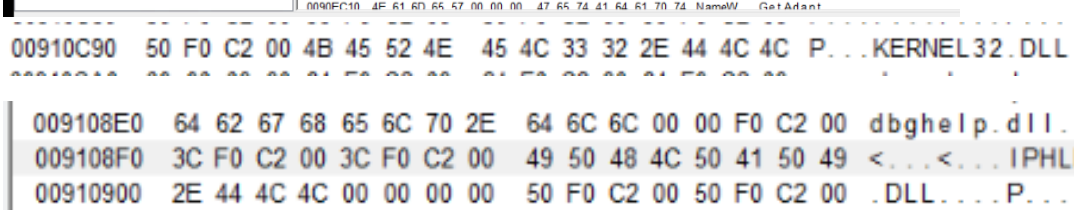






Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
For the next one which is SECTION .idata” was having a lot of the function and the DLL.

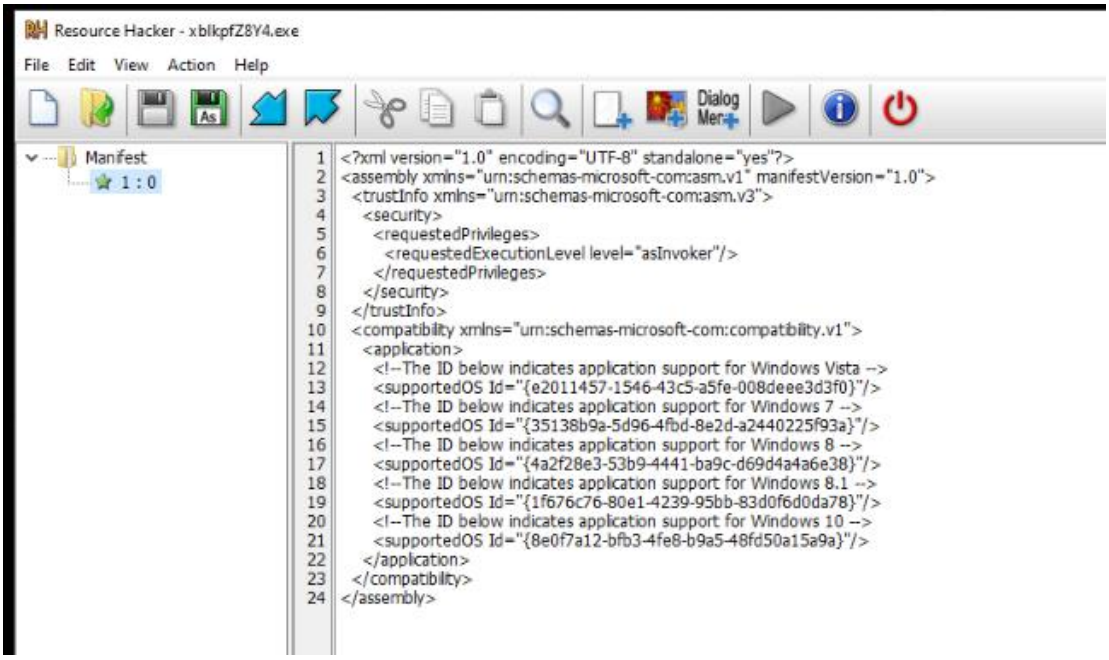




For the rest which is “SECTION ,pdata” and “SECTION .xdata” and “SECTION .CRT” and “SECTION .tls” and “SECTION .reloc” was having a unknown letter and number and sign that was a gibberish string.

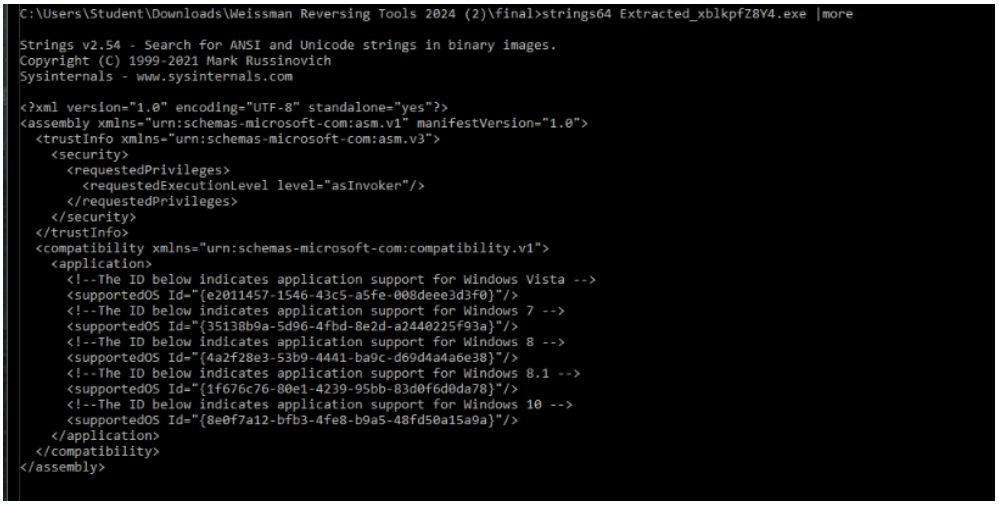
Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

Then I use the **Resource Hacker** with the xblkpfZ8Y4.exe to get more information about the Melewar and this is what I get:



As you can see there is a “Embedded XML” the manifest specifies with compatibility different Windows versions which is the “Windows 7” and “Windows 8” and “Windows 8.1” and “Windows 10” and this make it smooth to execution in multiple windows platforms and in the same XML there is a “<requestedExecutionLevel level-"asInvoker"/>” which is a set to make the program runs with the same privileges as the user.

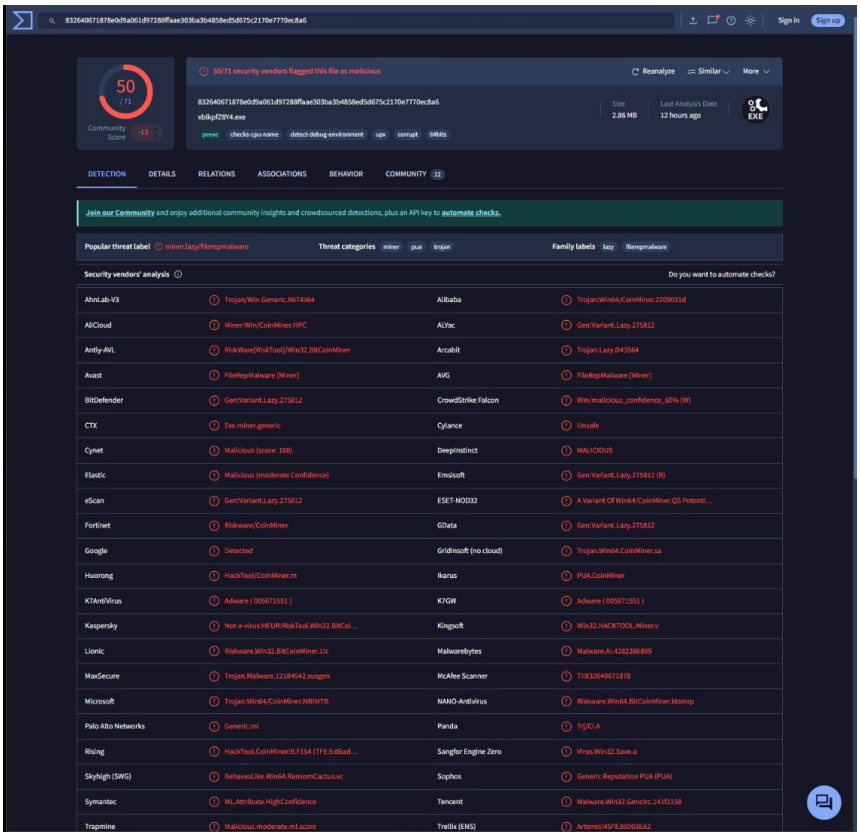
I try to save the resource to a BIN and tray to ran it in the string64 but after I do it there was nothing there just was the Embedded XML.



Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

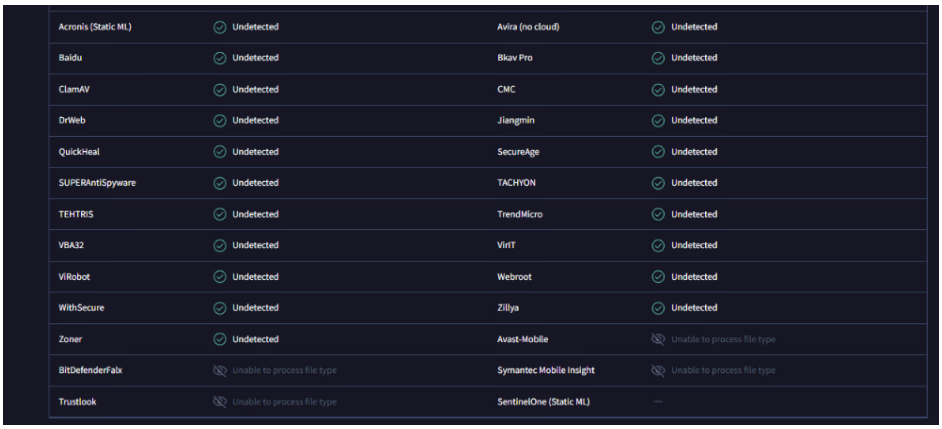
4 VirusTotal

Then I use the VirusTotal with the xblkpfZ8Y4.exe to get more information about the Malware from the 71 multiple antivirus engines.



There is a 50 from 71 of the security vendors flagged that the file is malware and the Popular threat of this program is “miner.lazy/filerepmalware” with threat categories of “miner” and “pua” and “trojan” and the family labels are “lazy” and “filerepmalware”.

There are the security vendors that does not have flagged that the file is malware which is 11 security vendors.



Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
Then I go to the “detail” option of the VirusTotal to see more information about the Malware and this is what I get:

DETECTION | DETAILS | RELATIONS | ASSOCIATIONS | BEHAVIOR | COMMUNITY 12

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	45fe36d03ea2a066f6dd061c0f11f829
SHA-1	6e45a340c41c62cd51c5e6f3b024ar3c7ac85f88
SHA-256	832640671878e0d9a061d97288ffaae303ba3b4858ed5d675c2170e7770ec8a6
Vhash	02603e0f7d1013z13z4015z17z13z15z17z
Authentihash	7569b83cee85405d963bbf14514736b0984c9da0e19b9cb2412760e65af8679d
Imphash	17fb7e76da9d0e277bd22cf9f3d5242c
SSDEEP	49152:5R+FNIC1gMk0gEB/N86YQNma1e3gQZDCY1EMkTiIpLRYvTaMQRmWWJgNVRuME:S6Mga18YgaoQQhMMkvGjocmNVR
TLSH	T121D533E2E85022236E3EF187BA7641A5C7410A5BCDC35F8509E9BA17FD702E7C53CA14A
File type	Win32 EXE executable windows win32 pe peece
Magic	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
TrID	UPX compressed Win64 Executable (63.5%) | UPX compressed Win32 Executable (24.5%) | Win16 NE executable (generic) (4.5%) | Windows Icons Library (generic) (1.8…
DetectitEasy	PE64 | Packer: UPX (4.24) [LZMA,brute]
Magika	PEBIN
File size	2.86 MB (2995200 bytes)

History

Creation Time	2024-09-28 08:52:56 UTC
First Seen In The Wild	2024-11-27 14:12:40 UTC
First Submission	2024-10-28 11:11:03 UTC
Last Submission	2024-12-01 23:58:08 UTC
Last Analysis	2024-12-06 12:02:43 UTC

Names

xbIkpfZ8Y4.exe
832640671878e0d9a061d97288ffaae303ba3b4858ed5d675c2170e7770ec8a6.exe
xbIkpfZ8Y4.exe.bin

Portable Executable Info

Header

Target Machine	x64
Compilation Timestamp	2024-09-28 08:52:56 UTC
Entry Point	12901280
Contained Sections	3

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
UPX0	4096	9508224	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	9912320	2994176	2992128	8	23a31e34a748363fc1edsf42a46e4270	272.49
.rsrc	12906496	4096	2560	4.5	73fe2d7a116eab748a0d15c8b1e87201	96904.85

Imports

+ ADVAPI32.dll
+ CRYPT32.dll
+ dbghelp.dll
+ IPHLPAPI.DLL
+ KERNEL32.DLL
+ msvcrt.dll
+ ole32.dll
+ SHELL32.dll
+ USER32.dll
+ USERENV.dll
+ WS2_32.dll

Contained Resources By Type

RT_MANIFEST	1

Contained Resources By Language

NEUTRAL	1

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
a73f26a8d504043f785d7360e8febf2eeb8522ec873a0d4dd5d1d4bfd1e67d3d	XML	RT_MANIFEST	NEUTRAL	5.14	11779.32

There is a basic properties of this Malware which is the “SHA-256” which was “832640671878e0d9a061d97288ffaae303ba3b4858ed5d675c2170e7770ec8a6” and the “File type” which was “Win32 EXE cxecutable windows win32 pe peece” and the “TrID” which was “UPX compressed Win64 Executable (63.5%) | UPX compressed Win32 Executable (24.5%) |Win16 NE executable (generic) (4.5%) |Windows Icons Library (generic) (1.8)” and the “File size” which was “2.86 MB (2995200 bytes)” and there is more like the “MD5” SHA-1” “Vhash” “Authentihash” “Imphash” “SSDEEP” “TLSH” “Magic” “DetectitEasy” “Magika”

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

There are History of the malware which was :

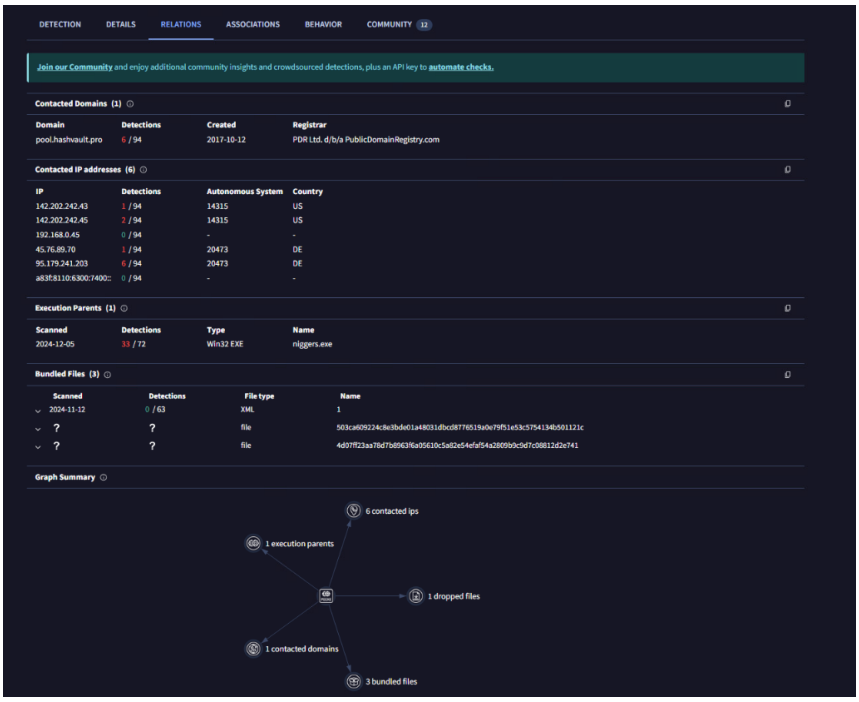
Creation Time	2024-09-28 08:52:56 UTC
First Seen in The Wild	2024-11-27 14:12:40 UTC
First Submission	2024-10-28 11:11:03 UTC
Last Submission	2024-12-01 23:58:08 UTC
Last Analysis	2024-12-06 12:02:43 UTC

And this is give as that the malware was creation around 2 mounth age and give as that the first submission was around the month ago and the first seen in the wild was less then week which make it more suspect.

There was another Names of the malware which is “832640671878e0d9a061d97288ffaae303ba3b4858ed5d675c2170e7770ec8a6.exe” and “xblkpfZ8Y4.exe.bin” and “xblkpfZ8Y4.exe”.

There was Portable Executable information of the malware which was have in the header the “Target Machine” and was “x64” also the section was having the “UPX0” and the “UPX1” and the “.rsrc” also the impots was having the “ADVAPI32.dll” “CRYPT32.dll” “dbghelp.dll” “IPHLPAPI,DLL” “KERNEL32.DLL” “msvcrt.dll” “ole32.dll” “SHELL32.dll” “USER32,dll” “USERENV.dll” “WS2_32.dll” also the Contained Resources was having the “a73f26a8d504043f785d7360e8febf2eeb8522ec873a0d4dd5d1d4bfd1e67d3d” which was “XML”.

Then I go to the “RELATIONS” option of the VirusTotal to see more information about the malware and this is what I get:

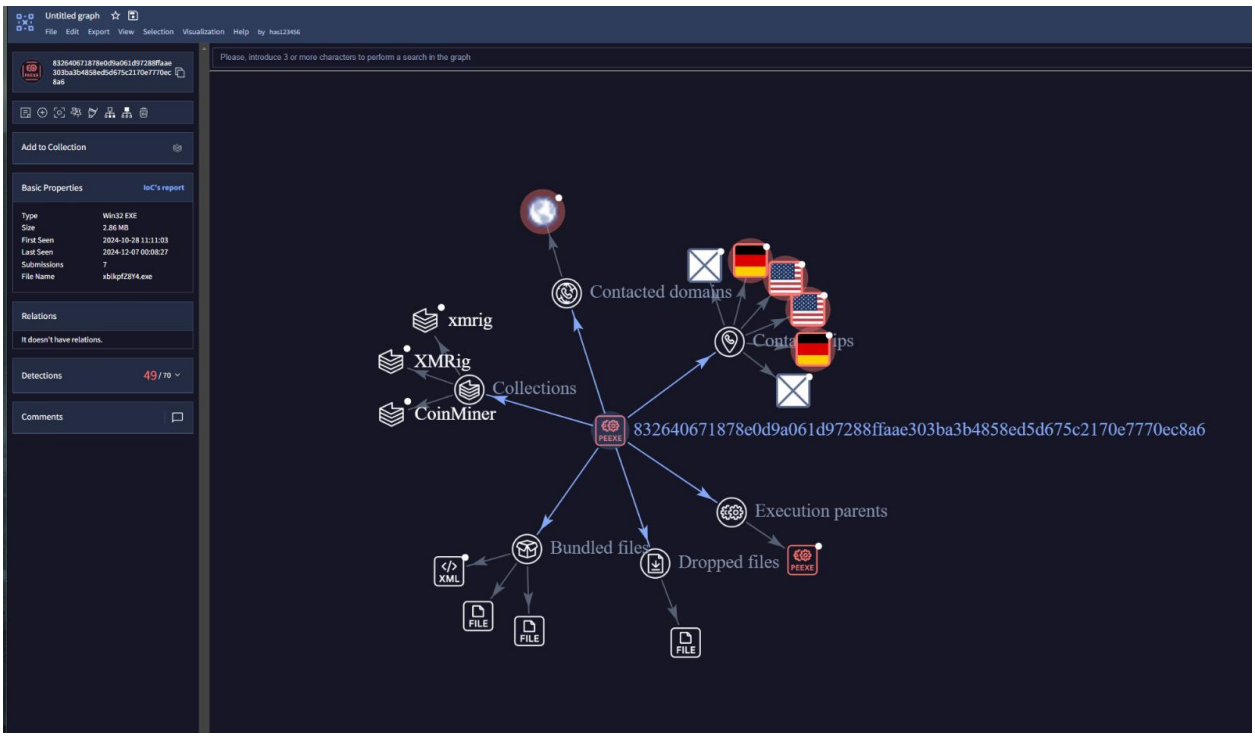


Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
There was a contacted domains which is the domain “pool.hashvault.pro” and it was registrar in “PDR Ltd. d/b/a PublicDomainRegistry.com”

There was also a 6 contacted IP addresses which is:

IP	Country
142.202.242.43	US
142.202.242.45	US
192.168.0.45	-
45.76.89.70	DE
95.179.241.203	DE
a83f:8110:6300:7400	-

There was a graph Summary which is like this:



As you can see in the secrenshot ther is a IP addresse in Germany and US which is make it more suspect of this malware.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

Basic Dynamic Analysis Tool

1 Regshot

Here I try to do the frist dynamic analysis to the malware and first thing I do is the “1st shot” without doing nothing then after the “1st shot” finish I run the malware then I do the “2nd shot” after that I compare the to get the output and this what I gat:

```
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2024/12/7 23:45:53  ,  2024/12/7 23:47:35
Computer: DESKTOP-VI4396B , DESKTOP-VI4396B
Username: Student , Student

----------------------------------
Keys deleted: 1
----------------------------------
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Search\JumplistData

----------------------------------
Keys added: 7
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\17980
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001F07EC
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000330564
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000360216
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000007405FA
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

----------------------------------
Values deleted: 1
----------------------------------
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Search\JumplistData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI:  4F AF

----------------------------------
Values added: 35
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\17980\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\17980\Reason: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\17980\CreationTime:  59 B9 30 5F 02 49 DB 01
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\\Device\HarddiskVolume2\Users\Student\Downloads\Weissman Reversing Tool
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\\Device\HarddiskVolume2\Users\Student\Downloads\Weissman Reversing
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Fghqrag\(
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001F07EC\VirtualDesktc
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000330564\VirtualDesktc
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000360216\VirtualDesktc
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000007405FA\VirtualDesktc
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\Student\Downloads\Weissmar
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Rev: 6
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\FFlags
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Vid: "
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Mode:
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Logica
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\IconSi
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Sort:
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\ColIn
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Group\
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupE
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupE
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupE
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Rev: 0x0000000
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\FFlags: 0x4120
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Vid: "{137E770
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Mode: 0x000000
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\LogicalViewMode
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\IconSize: 0x00
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Sort:  00 00 0
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\ColInfo:  00 0
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupView: 0x0
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:FMT
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:PID:
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByDirecti

----------------------------------
Values modified: 28
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime:  E8 61 23 2B 02 49 DB 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime:  E9 A7 E6 4E 02 49 DB 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75:  71 09 00 00 00 00 00 00 04 00 04 00 01 00 01 00 01 01 00 00 CD AD 05 01 35 00 02 00 00 6
C2 21 D1 00 CC C1 01 01 DA D8 7E 00 E6 19 9B 00 02 00 40 01 00 00 4B 11 B4 00 9F 27 FF 00 01 00 41 01 00 00 2A B7 22 01 01 00 42 01 00 00 27 69 12 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75:  7D 09 00 00 00 00 00 00 04 00 04 00 01 00 01 00 01 01 00 00 CD AD 05 01 45 00 02 00 00 6
6F 00 22 00 06 00 00 00 04 92 1E 01 1A FA 99 00 29 00 D8 00 2D 85 BA 00 55 5F 2A 01 59 E5 D3 00 5E 42 C4 00 5F 6C DC 00 63 3E 99 00 65 7F 0E 01 7D 23 B1 00 82 E6 F4 00 91 50 8A
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475:  4A 07 00 00 00 00 00 00 04 00 04 00 01 02 04 00 00 00 00 00 34 00 00 00 0D 78 79 00 07 6
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475:  4B 07 00 00 00 00 00 00 04 00 04 00 01 02 04 00 00 00 00 00 34 00 00 00 0D 78 79 00 07 6
```

```
----------------------------------
Total changes: 72
----------------------------------
```

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

In the compare output I get “Keys deleted: 1” and “Keys added: 7” and “Values deleted: 1” and “Values added: 35” and “Values modified: 28” which was a total of 72 changes.

As you can see in the added keys there is a path for this

```
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001F07EC
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000330564
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000360216
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000007405FA
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
```

And this keys store session of information of the file paths and virtual desktop data.

As you can see the added values there is a path for this “KLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\17980\Terminator: "HAM"” which is show that the malware maybe have change or edit the error reporting and this maybe limiting the crash report. Also there is a some of the sessioninfo which reflect to the interaction with user session metadata in the virtual desktop

```
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\\Device\HarddiskVolume2\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final\xblkpfZ8Y4.exe:  CF E4 AD 73 02 49 DB 01 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Fghgrag\Qbjaybnqf\Jrvffzna Erirefvat Gbbyf 2024 (2)\svany\koyxcsMBL4.rkr:  00 00 00 00 01 00 00 00 01 00 00 00 2
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001F07EC\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000330564\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000360216\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000007405FA\VirtualDesktop:  10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3204009595-3950962059-2982198161-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final\xblkpfZ8Y4.exe:  53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00
```

As you can see in the modified values there is some path which is this :

```
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\SequenceNumber: 0x0000015A
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\SequenceNumber: 0x0000015C
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\\Device\HarddiskVolume2\Windows\System32\conhost.exe:  D3 1D DE 26 F7 48 DB 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\\Device\HarddiskVolume2\Windows\System32\conhost.exe:  3B 95 BE 73 02 49 DB 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy:  2A 3D 09 40 4E 48 DB 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-2982198161-1001\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy:  BA 1B 33 5F 02 49 DB 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
```

and the “bam” which is a Background Activity Moderator and use to setting the background application activity and here the malware have some of the change and edit of the “bam” which maybe the malware is tring to work in the background which make it more suspe Suspect.

There is more of the chang and the add and deleted of the keys and the values but this is what I notest.

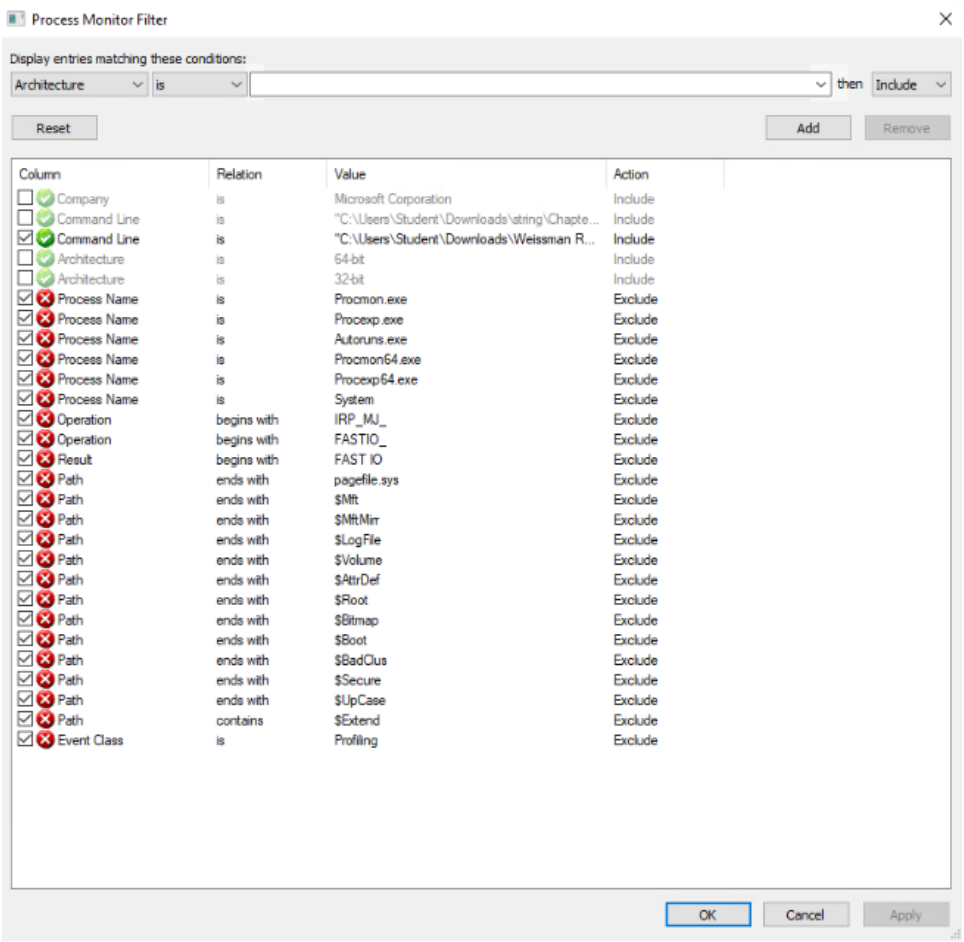
Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

2 Process Monitor

Here I try to do the second dynamic analysis to the malware and first thing I do it is to run the malware than I get some filter to git the output of the malware and the filter was colum “Command Line” and the relation “is” and the value of the “path of the malware which is

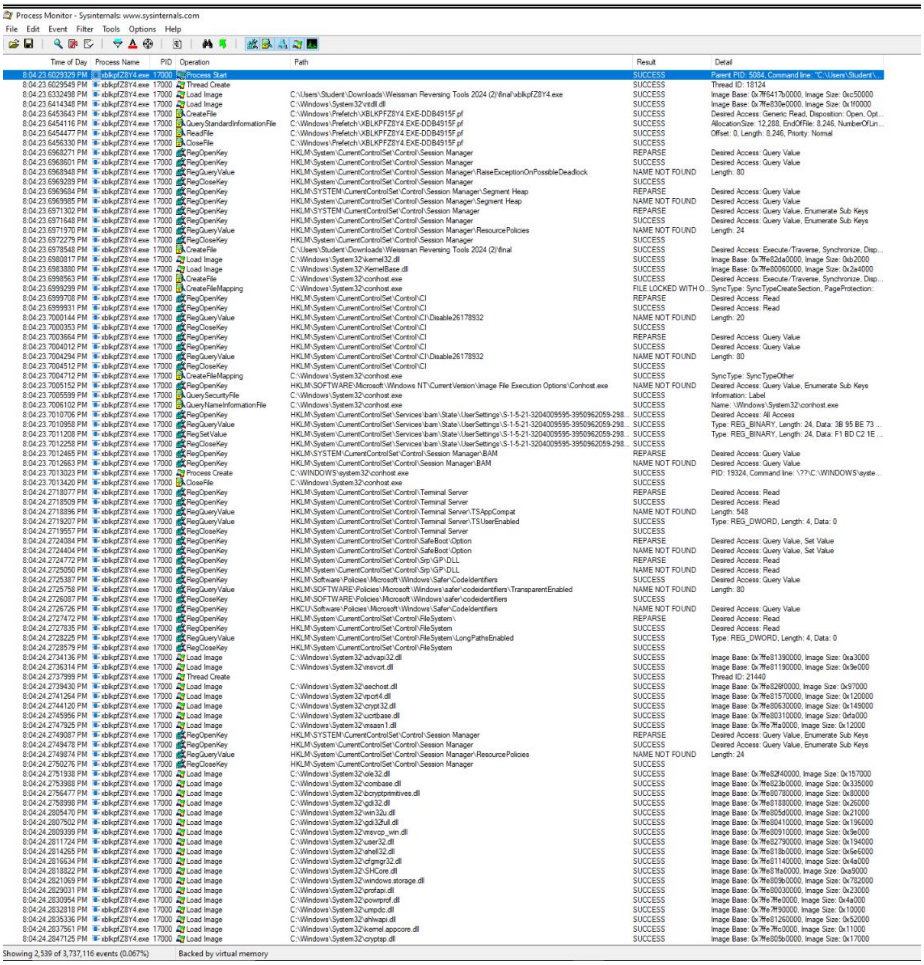
"C: \Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\fnal\xblkpfZ8Y4.exe”

This the action “Include” which is basically the filter will show the only event that from the path of the malware which makes it easy to get information on the activities that the malware is doing kowing that the process monitor showing 2.605.444 events goint on in the PC which is a lot.



Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

After I do the filter there was a 2509 events that going on in the malware and this is what I gat :



Time of Day	Process Name	PID	Operation	Path	Result	Detail
8:04:23.6029329 PM	xblkpfZ8Y4.exe	17000	Process Start		SUCCESS	Parent PID: 5084, Command line: "C:\Users\Student\...
8:04:23.6029545 PM	xblkpfZ8Y4.exe	17000	Thread Create		SUCCESS	Thread ID: 18124
8:04:23.6332498 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final\xblkpfZ8Y4.exe	SUCCESS	Image Base: 0x7ff617b0000, Image Size: 0xc50000
8:04:23.6414348 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ff830e0000, Image Size: 0x1f0000
8:04:23.6453643 PM	xblkpfZ8Y4.exe	17000	CreateFile	C:\Windows\Prefetch\XBLKPFZ8Y4.EXE-DDB4915F.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Opt...
8:04:23.6454116 PM	xblkpfZ8Y4.exe	17000	QueryStandardInformationFile	C:\Windows\Prefetch\XBLKPFZ8Y4.EXE-DDB4915F.pf	SUCCESS	AllocationSize: 12,288, EndOfFile: 8,246, NumberOfLin...
8:04:23.6454477 PM	xblkpfZ8Y4.exe	17000	ReadFile	C:\Windows\Prefetch\XBLKPFZ8Y4.EXE-DDB4915F.pf	SUCCESS	Offset: 0, Length: 8,246, Priority: Normal
8:04:23.6455330 PM	xblkpfZ8Y4.exe	17000	CloseFile	C:\Windows\Prefetch\XBLKPFZ8Y4.EXE-DDB4915F.pf	SUCCESS	
8:04:23.6968271 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
8:04:23.6968601 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
8:04:23.6968948 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80
8:04:23.6969289 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
8:04:23.6969634 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value
8:04:23.6969985 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Query Value
8:04:23.6971302 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
8:04:23.6971648 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
8:04:23.6971970 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
8:04:23.6972279 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
8:04:23.6978548 PM	xblkpfZ8Y4.exe	17000	CreateFile	C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disp...
8:04:23.6980817 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ff82da0000, Image Size: 0xb2000
8:04:23.6983380 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ff80060000, Image Size: 0x2a4000
8:04:23.6998563 PM	xblkpfZ8Y4.exe	17000	CreateFile	C:\Windows\System32\conhost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disp...
8:04:23.6999299 PM	xblkpfZ8Y4.exe	17000	CreateFileMapping	C:\Windows\System32\conhost.exe	FILE LOCKED WITH O...	SyncType: SyncTypeCreateSection, PageProtection:
8:04:23.6999708 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: Read
8:04:23.6999931 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: Read
8:04:23.7000144 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND	Length: 20
8:04:23.7000353 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
8:04:23.7003664 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: Query Value
8:04:23.7004012 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: Query Value
8:04:23.7004294 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND	Length: 80
8:04:23.7004512 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
8:04:23.7004712 PM	xblkpfZ8Y4.exe	17000	CreateFileMapping	C:\Windows\System32\conhost.exe	SUCCESS	SyncType: SyncTypeOther
8:04:23.7005152 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Conhost.exe	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
8:04:23.7005599 PM	xblkpfZ8Y4.exe	17000	QuerySecurityFile	C:\Windows\System32\conhost.exe	SUCCESS	Information: Label
8:04:23.7006102 PM	xblkpfZ8Y4.exe	17000	QueryNameInformationFile	C:\Windows\System32\conhost.exe	SUCCESS	Name: \Windows\System32\conhost.exe
8:04:23.7010706 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	Desired Access: All Access
8:04:23.7010958 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 3B 95 BE 73 ...
8:04:23.7011208 PM	xblkpfZ8Y4.exe	17000	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	Type: REG_BINARY, Length: 24, Data: F1 BD C2 1E ...
8:04:23.7012258 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	
8:04:23.7012465 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM	REPARSE	Desired Access: Query Value
8:04:23.7012663 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\BAM	NAME NOT FOUND	Desired Access: Query Value
8:04:23.7013023 PM	xblkpfZ8Y4.exe	17000	Process Create	C:\WINDOWS\system32\conhost.exe	SUCCESS	PID: 19324, Command line: \??\C:\WINDOWS\syste...
8:04:23.7013420 PM	xblkpfZ8Y4.exe	17000	CloseFile	C:\Windows\System32\conhost.exe	SUCCESS	
8:04:24.2718077 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: Read
8:04:24.2718509 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
8:04:24.2718896 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT FOUND	Length: 548
8:04:24.2719207 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
8:04:24.2719557 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
8:04:24.2724084 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value
8:04:24.2724404 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
8:04:24.2724772 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read
8:04:24.2725050 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: Read
8:04:24.2725387 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
8:04:24.2725758 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
8:04:24.2726087 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS	
8:04:24.2726726 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Query Value
8:04:24.2727472 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem\	REPARSE	Desired Access: Read
8:04:24.2727835 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS	Desired Access: Read
8:04:24.2728225 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\FileSystem\LongPathsEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
8:04:24.2728579 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS	
8:04:24.2734136 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ff81390000, Image Size: 0xa3000
8:04:24.2736314 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ff81190000, Image Size: 0x9e000
8:04:24.2737999 PM	xblkpfZ8Y4.exe	17000	Thread Create		SUCCESS	Thread ID: 21440
8:04:24.2739430 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ff81290000, Image Size: 0x97000
8:04:24.2741264 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7ff81570000, Image Size: 0x120000
8:04:24.2744120 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\crypt32.dll	SUCCESS	Image Base: 0x7ff80630000, Image Size: 0x149000
8:04:24.2745956 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7ff80310000, Image Size: 0xfa000
8:04:24.2747925 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\msasn1.dll	SUCCESS	Image Base: 0x7ff7ffa0000, Image Size: 0x12000
8:04:24.2749007 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
8:04:24.2749478 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
8:04:24.2749874 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
8:04:24.2750276 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
8:04:24.2751938 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\ole32.dll	SUCCESS	Image Base: 0x7ff82f40000, Image Size: 0x157000
8:04:24.2753988 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\combase.dll	SUCCESS	Image Base: 0x7ff823b0000, Image Size: 0x335000
8:04:24.2756477 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	Image Base: 0x7ff80790000, Image Size: 0x80000
8:04:24.2758998 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ff81880000, Image Size: 0x26000
8:04:24.2805470 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\win32u.dll	SUCCESS	Image Base: 0x7ff805d0000, Image Size: 0x21000
8:04:24.2807502 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ff80410000, Image Size: 0x196000
8:04:24.2809399 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\msvcp_win.dll	SUCCESS	Image Base: 0x7ff80910000, Image Size: 0x9e000
8:04:24.2811724 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7ff82790000, Image Size: 0x194000
8:04:24.2814255 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\shell32.dll	SUCCESS	Image Base: 0x7ff813b0000, Image Size: 0x5e6000
8:04:24.2816634 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\cfgmgr32.dll	SUCCESS	Image Base: 0x7ff81140000, Image Size: 0x4e000
8:04:24.2818822 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\SHCore.dll	SUCCESS	Image Base: 0x7ff81fa0000, Image Size: 0xa9000
8:04:24.2821069 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\windows.storage.dll	SUCCESS	Image Base: 0x7ff809b0000, Image Size: 0x792000
8:04:24.2829031 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\profapi.dll	SUCCESS	Image Base: 0x7ff80030000, Image Size: 0x23000
8:04:24.2830954 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\powrprof.dll	SUCCESS	Image Base: 0x7ff7ffe0000, Image Size: 0x4a000
8:04:24.2832818 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\umpdc.dll	SUCCESS	Image Base: 0x7ff7ff90000, Image Size: 0x10000
8:04:24.2835536 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\shlwapi.dll	SUCCESS	Image Base: 0x7ff81260000, Image Size: 0x52000
8:04:24.2837561 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\kernel.appcore.dll	SUCCESS	Image Base: 0x7ff7ffc0000, Image Size: 0x11000
8:04:24.2847125 PM	xblkpfZ8Y4.exe	17000	Load Image	C:\Windows\System32\cryptsp.dll	SUCCESS	Image Base: 0x7ff805b0000, Image Size: 0x17000

Showing 2,539 of 3,737,116 events (0.067%) Backed by virtual memory

8:04:23.6998563 PM	xblkpfZ8Y4.exe	17000	CreateFile	C:\Windows\System32\conhost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disp...
8:04:23.6999299 PM	xblkpfZ8Y4.exe	17000	CreateFileMapping	C:\Windows\System32\conhost.exe	FILE LOCKED WITH O...	SyncType: SyncTypeCreateSection, PageProtection:
8:04:23.6999708 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: Read
8:04:23.6999931 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: Read
8:04:23.7000144 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND	Length: 20
8:04:23.7000353 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
8:04:23.7003664 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: Query Value
8:04:23.7004012 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: Query Value
8:04:23.7004294 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND	Length: 80
8:04:23.7004512 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
8:04:23.7004712 PM	xblkpfZ8Y4.exe	17000	CreateFileMapping	C:\Windows\System32\conhost.exe	SUCCESS	SyncType: SyncTypeOther
8:04:23.7005152 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Conhost.exe	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
8:04:23.7005599 PM	xblkpfZ8Y4.exe	17000	QuerySecurityFile	C:\Windows\System32\conhost.exe	SUCCESS	Information: Label
8:04:23.7006102 PM	xblkpfZ8Y4.exe	17000	QueryNameInformationFile	C:\Windows\System32\conhost.exe	SUCCESS	Name: \Windows\System32\conhost.exe
8:04:23.7010706 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	Desired Access: All Access
8:04:23.7010958 PM	xblkpfZ8Y4.exe	17000	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 3B 95 BE 73 ...
8:04:23.7011208 PM	xblkpfZ8Y4.exe	17000	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	Type: REG_BINARY, Length: 24, Data: F1 BD C2 1E ...
8:04:23.7012258 PM	xblkpfZ8Y4.exe	17000	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3204009595-3950962059-298...	SUCCESS	
8:04:23.7012465 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM	REPARSE	Desired Access: Query Value
8:04:23.7012663 PM	xblkpfZ8Y4.exe	17000	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\BAM	NAME NOT FOUND	Desired Access: Query Value
8:04:23.7013023 PM	xblkpfZ8Y4.exe	17000	Process Create	C:\WINDOWS\system32\conhost.exe	SUCCESS	PID: 19324, Command line: \??\C:\WINDOWS\syste...
8:04:23.7013420 PM	xblkpfZ8Y4.exe	17000	CloseFile	C:\Windows\System32\conhost.exe	SUCCESS	

Here in the secrenshot the malwaer is focus in accessisng the session manager and the BAM Keys and accessis the image file execution options (IFEO) for Conhost.exe which make it Suspicious.

8:04:25.1241398 PM	xblkpfZ8Y4.exe	17000	TCP Connect	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rc...
8:04:25.1862869 PM	xblkpfZ8Y4.exe	17000	TCP Send	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 568, startime: 58056457, endtime: 58056463, ...
8:04:25.1916562 PM	xblkpfZ8Y4.exe	17000	TCP Receive	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 731, seqnum: 0, connid: 0
8:04:25.2780435 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 0.4531250 seconds, Kernel Time: 0.18750...
8:04:26.2702672 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 1.0312500 seconds, Kernel Time: 0.37500...
8:04:26.6255622 PM	xblkpfZ8Y4.exe	17000	Thread Create		SUCCESS	Thread ID: 19076
8:04:26.6265690 PM	xblkpfZ8Y4.exe	17000	Thread Create		SUCCESS	Thread ID: 16752

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

In the almost the end there was a TCP Connect to the IP “142.202.245.45” on port “80” which is HTTP and there is TCP Send to the IP addresse and the size of the data that was send is 558 byets then there is a TCP Receive from the same remote IP address over the HTTP and the size of the receivesd data was 731 bytes.

8:04:37.0686262 PM	xblkpfZ8Y4.exe	17000	TCP Receive	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 471, seqnum: 0, connid: 0
8:04:37.2755863 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 16.3125000 seconds, Kernel Time: 1.0625...
8:04:38.2884890 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 18.0625000 seconds, Kernel Time: 1.0937...
8:04:39.2746305 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 19.8906250 seconds, Kernel Time: 1.1250...
8:04:40.2863203 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 21.8125000 seconds, Kernel Time: 1.1875...
8:04:41.2707860 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 23.7187500 seconds, Kernel Time: 1.2500...
8:04:42.3250721 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 25.3281250 seconds, Kernel Time: 1.2968...
8:04:43.2941200 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 26.3437500 seconds, Kernel Time: 1.3281...
8:04:43.4136657 PM	xblkpfZ8Y4.exe	17000	TCP Receive	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 471, seqnum: 0, connid: 0

Then there was a TCP Receive from the remote IP address “142.202.242.45” port “80” and the size of the received data was 471 after like 6 secand there was a TCP Receive from the same IP address with 471 data receive.

8:04:25.1241398 PM	xblkpfZ8Y4.exe	17000	TCP Connect	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rc...
8:04:25.1862869 PM	xblkpfZ8Y4.exe	17000	TCP Send	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 568, startime: 58056457, endtime: 58056463, ...
8:04:25.1916562 PM	xblkpfZ8Y4.exe	17000	TCP Receive	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 731, seqnum: 0, connid: 0
8:04:25.2780435 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 0.4531250 seconds, Kernel Time: 0.18750...
8:04:26.2702672 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 1.0312500 seconds, Kernel Time: 0.37500...
8:04:26.6255622 PM	xblkpfZ8Y4.exe	17000	Thread Create		SUCCESS	Thread ID: 19076
8:04:26.6265690 PM	xblkpfZ8Y4.exe	17000	Thread Create		SUCCESS	Thread ID: 16752
8:04:27.2939949 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 1.9843750 seconds, Kernel Time: 0.40625...
8:04:28.3759241 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 2.8281250 seconds, Kernel Time: 0.42187...
8:04:29.3195760 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 3.6250000 seconds, Kernel Time: 0.43750...
8:04:30.2618404 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 5.0937500 seconds, Kernel Time: 0.50000...
8:04:31.2928589 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 6.7500000 seconds, Kernel Time: 0.59375...
8:04:32.2945847 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 8.2968750 seconds, Kernel Time: 0.65625...
8:04:33.2780711 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 9.9062500 seconds, Kernel Time: 0.73437...
8:04:34.2661519 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 11.6406250 seconds, Kernel Time: 0.7968...
8:04:35.2721695 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 13.3437500 seconds, Kernel Time: 0.8750...
8:04:36.2791134 PM	xblkpfZ8Y4.exe	17000	Process Profiling		SUCCESS	User Time: 14.7812500 seconds, Kernel Time: 0.9218...
8:04:37.0686262 PM	xblkpfZ8Y4.exe	17000	TCP Receive	DESKTOP-VI4396B.rit.edu:62431 -> 142.202.242.45:http	SUCCESS	Length: 471, seqnum: 0, connid: 0

I notest that after the TCP proses there was a lot of the Process Profiling which is the a tool to check the amount of the processor time used by each process also for the memory use so as you can see there is a lot between the TCP Receive so I think there is a high on the CPU usage in User Time and Kernel Time so it could there is a computationally intensive tasks going on doring this time which is the algretham that the IP send it to do the mining.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

Advanced Static Analysis

1 IDA

First I try to put the malware without UPX unpacked to see the point when malware start after the UPX unpacked and I notest there is just one functions in there which is “start” and there is lot of the code but after more debug I see that all the code go to one of group nodes which is jump to “ word_140013F0” which is does not have any value of it after that there is the end of the UPX0.

```
UPX1:0000000140C4E74E sub     rsp, 0FFFFFFFFFFFFFF80h
UPX1:0000000140C4E752 jmp     near ptr qword_1400013F0
UPX1:0000000140C4E752 start endp ; sp-analysis failed
UPX1:0000000140C4E752
```

```
UPX0:00000001400013F0 qword_1400013F0 dq 12E532h dup(?)       ; CODE XREF: start+BB2↓j
UPX0:00000001400013F0 UPX0            ends
UPX0:00000001400013F0
```

I also notest the “TlsCallback_0” after the end of the group nodes which is coulde be importint functens that hiding in the UPX.

```
UPX1:0000000140C4E757                 public TlsCallback_0
UPX1:0000000140C4E757 TlsCallback_0   db 0C3h                 ; CODE XREF: start+B98↑p
UPX1:0000000140C4E757                                         ; DATA XREF: start+B83↑w ...
UPX1:0000000140C4E758 ; ---------------------------------------------------------------------------
```

There is a “TlsDirectory” and “TlsStart” that all hiding in the UPX.

```
UPX1:0000000140C4E77C ; ---------------------------------------------------------------------------
UPX1:0000000140C4E77D                 align 20h
UPX1:0000000140C4E780 TlsDirectory    dq offset TlsStart
UPX1:0000000140C4E788 TlsEnd_ptr      dq offset TlsCallbacks
UPX1:0000000140C4E790 TlsIndex_ptr    dq offset TlsIndex
UPX1:0000000140C4E798 TlsCallbacks_ptr dq offset TlsCallbacks
UPX1:0000000140C4E7A0 TlsSizeOfZeroFill dd 0
UPX1:0000000140C4E7A4 TlsCharacteristics dd 0
UPX1:0000000140C4E7A8 TlsStart        dq 0                    ; DATA XREF: UPX1:TlsDirectory↑o
UPX1:0000000140C4E7B0 TlsCallbacks    dq offset TlsCallback_0 ; DATA XREF: UPX1:TlsEnd_ptr↑o
UPX1:0000000140C4E7B0                                         ; UPX1:TlsCallbacks_ptr↑o
UPX1:0000000140C4E7B8                 dq 0
UPX1:0000000140C4E7C0                 align 80h
UPX1:0000000140C4E800                 dq 100h dup(?)
UPX1:0000000140C4E800 UPX1            ends
UPX1:0000000140C4E800
UPX1:0000000140C4E800
UPX1:0000000140C4E800                 end start
```

Then I open the malware ater the UPX unpackedto see what will gite and there was lot of functens around the 2000 so I start to go arount the functens I notest the functens for the “xmig” which wsa have code for the URL and the Uesre and the Password and the mining algrithem and the network for the Remot URL which I think it is the way that mining happened.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

```
.text:000000014001CA70
.text:000000014001CA70 loc_14001CA70:
.text:000000014001CA70 mov     r8d, 21h ; '!'
.text:000000014001CA76 mov     rcx, rbx
.text:000000014001CA79 lea     rdx, aUsageXmrigOpti ; "Usage: xmrig [OPTIONS]\n\nNetwork:\n"
.text:000000014001CA80 mov     rsi, 3FFFFFFFFFFFFFFFh
.text:000000014001CA8A call    sub_1406A1C30
.text:000000014001CA8F mov     rax, rsi
.text:000000014001CA92 sub     rax, cs:qword_14090F208
.text:000000014001CA99 cmp     rax, 34h ; '4'
.text:000000014001CA9D jbe     loc_14001DAF0
```

And if it true will end and retern if not will go to the group nodes which is the URL and you can see in the secrenshort that there is URL of mining server.

```
.text:000000014001CAA3 mov     r8d, 35h ; '5'
.text:000000014001CAA9 lea     rdx, aOUrlUrlUrlOfMi ; "  -o, --url=URL                URL of "...
.text:000000014001CAB0 mov     rcx, rbx
.text:000000014001CAB3 call    sub_1406A1C30
.text:000000014001CAB8 mov     rax, rsi
.text:000000014001CABB sub     rax, cs:qword_14090F208
.text:000000014001CAC2 cmp     rax, 52h ; 'R'
.text:000000014001CAC6 jbe     loc_14001DAF0

aOUrlUrlUrlOfMi db '  -o, --url=URL                URL of mining server',0Ah,0
                                                    ; DATA XREF: sub_14001C8E0+1C9↑o
```

And if it true will end and retern if not will go to the group nodes which is the mining algrithem and you can see in the secrenshort that there is “mining algorithm https://xmrig.com/docs/algorithms'”

```
.text:000000014001CACC mov     r8d, 53h ; 'S'
.text:000000014001CAD2 lea     rdx, aAAlgoAlgoMinin ; "  -a, --algo=ALGO               mining "...
.text:000000014001CAD9 mov     rcx, rbx
.text:000000014001CADC call    sub_1406A1C30
.text:000000014001CAE1 mov     rax, rsi
.text:000000014001CAE4 sub     rax, cs:qword_14090F208
.text:000000014001CAEB cmp     rax, 41h ; 'A'
.text:000000014001CAEF jbe     loc_14001DAF0

aAAlgoAlgoMinin db '  -a, --algo=ALGO               mining algorithm https://xmrig.co'
                                                    ; DATA XREF: sub_14001C8E0+1F2↑o
                db 'm/docs/algorithms',0Ah,0
```

And if it true will end and retern if not will go to the group nodes which is the coin and you can see in the secrenshort that there is “specify coin instead of algorithm'”

```
.text:000000014001CAF5 mov     r8d, 42h ; 'B'
.text:000000014001CAFB lea     rdx, aCoinCoinSpecif ; "      --coin=COIN               specify"...
.text:000000014001CB02 mov     rcx, rbx
.text:000000014001CB05 call    sub_1406A1C30
.text:000000014001CB0A mov     rax, rsi
.text:000000014001CB0D sub     rax, cs:qword_14090F208
.text:000000014001CB14 cmp     rax, 3Ah ; ':'
.text:000000014001CB18 jbe     loc_14001DAF0

aCoinCoinSpecif db '      --coin=COIN               specify coin instead of algorithm'
                                                    ; DATA XREF: sub_14001C8E0+21B↑o
                db 0Ah,0
```

And if it true will end and retern if not will go to the group nodes which is the user name and you can see in the secrenshort that there is “username for mining server”

```
.text:000000014001CB1E mov     r8d, 3Bh ; ';'
.text:000000014001CB24 lea     rdx, aUUserUsernameU ; "  -u, --user=USERNAME           usernam"...
.text:000000014001CB2B mov     rcx, rbx
.text:000000014001CB2E call    sub_1406A1C30
.text:000000014001CB33 mov     rax, rsi
.text:000000014001CB36 sub     rax, cs:qword_14090F208
.text:000000014001CB3D cmp     rax, 3Ah ; ':'
.text:000000014001CB41 jbe     loc_14001DAF0

aUUserUsernameU db '  -u, --user=USERNAME           username for mining server',0Ah,0
                                                    ; DATA XREF: sub_14001C8E0+244↑o
```

And if it true will end and retern if not will go to the group nodes which is the password and you can see in the secrenshort that there is “password for mining server”

```
.text:000000014001CB47 mov     r8d, 3Bh ; ';'
.text:000000014001CB4D lea     rdx, aPPassPasswordP ; "  -p, --pass=PASSWORD           passwor"...
.text:000000014001CB54 mov     rcx, rbx
.text:000000014001CB57 call    sub_1406A1C30
.text:000000014001CB5C mov     rax, rsi
.text:000000014001CB5F sub     rax, cs:qword_14090F208
.text:000000014001CB66 cmp     rax, 48h ; 'H'
.text:000000014001CB6A jbe     loc_14001DAF0

aPPassPasswordP db '  -p, --pass=PASSWORD           password for mining server',0Ah,0
                                                    ; DATA XREF: sub_14001C8E0+26D↑o
```

And if it true will end and retern if not will go to the group nodes which is the username:password and you can see in the secrenshort that there is “username:password pair for mining'”

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

```
.text:000000014001CB70 mov     r8d, 49h ; 'I'
.text:000000014001CB76 lea     rdx, aOUserpassUPUse ; "  -O, --userpass=U:P          usernam"...
.text:000000014001CB7D mov     rcx, rbx
.text:000000014001CB80 call    sub_1406A1C30
.text:000000014001CB85 mov     rax, rsi
.text:000000014001CB88 sub     rax, cs:qword_14090F208
.text:000000014001CB8F cmp     rax, 3Eh ; '>'
.text:000000014001CB93 jbe     loc_14001DAF0

aOUserpassUPUse db '  -O, --userpass=U:P          username:password pair for mining'
                                                  ; DATA XREF: sub_14001C8E0+296↑o
                db ' server',0Ah,0
```

And if it true will end and retern if not will go to the group nodes which is the proxy=HOST: PORT and you can see in the secrenshort that there is “connect through a SOCKS5” knoing that the port is SOCKS5 for the connecten which is a network protpcol that allows the clint to communicat with the server through the firewall

```
.text:000000014001CB99 mov     r8d, 3Fh ; '?'
.text:000000014001CB9F lea     rdx, aXProxyHostPort ; "  -x, --proxy=HOST:PORT        connect"...
.text:000000014001CBA6 mov     rcx, rbx
.text:000000014001CBA9 call    sub_1406A1C30
.text:000000014001CBAE mov     rax, rsi
.text:000000014001CBB1 sub     rax, cs:qword_14090F208
.text:000000014001CBB8 cmp     rax, 5Fh ; '_'
.text:000000014001CBBC jbe     loc_14001DAF0

aXProxyHostPort db '  -x, --proxy=HOST:PORT        connect through a SOCKS5 proxy',0Ah
                                                  ; DATA XREF: sub_14001C8E0+2BF↑o
                db 0
```

And if it true will end and retern if not will go to the group nodes which is the keepalive and you can see in the secrenshort that there is “send keepalived packet for prevent timeout (needs pool support)”.

```
.text:000000014001CBC2 mov     r8d, 60h ; '`'
.text:000000014001CBC8 lea     rdx, aKKeepaliveSend ; "  -k, --keepalive              send ke"...
.text:000000014001CBCF mov     rcx, rbx
.text:000000014001CBD2 call    sub_1406A1C30
.text:000000014001CBD7 sub     rsi, cs:qword_14090F208
.text:000000014001CBDE cmp     rsi, 3Bh ; ';'
.text:000000014001CBE2 jbe     loc_14001DAF0

aKKeepaliveSend db '  -k, --keepalive              send keepalived packet for preven'
                                                  ; DATA XREF: sub_14001C8E0+2E8↑o
                db 't timeout (needs pool support)',0Ah,0
```

And if it true will end and retern if not will go to the group nodes which is the nicehash and you can see in the secrenshort that there is “enable nicehash.com support” which is to enable the nicehash.com support and knoing that the nicehash.com is software for mining cryptocurrency.

```
.text:000000014001CBE8 mov     r8d, 3Ch ; '<'
.text:000000014001CBEE mov     rcx, rbx
.text:000000014001CBF1 lea     rdx, aNicehashEnable ; "      --nicehash              enable "...
.text:000000014001CBF8 mov     rsi, 3FFFFFFFFFFFFFFFh
.text:000000014001CC02 call    sub_1406A1C30
.text:000000014001CC07 mov     rax, rsi
.text:000000014001CC0A sub     rax, cs:qword_14090F208
.text:000000014001CC11 cmp     rax, 5Ch ; '\'
.text:000000014001CC15 jbe     loc_14001DAF0

aNicehashEnable db '      --nicehash              enable nicehash.com support',0Ah,0
                                                  ; DATA XREF: sub_14001C8E0+311↑o
```

And if it true will end and retern if not will go to the group nodes which is the tls and you can see in the secrenshort that there is “enable SSL/TLS support (needs poo 1 support)”.

```
.text:000000014001CC44 mov     r8d, 4Ch ; 'L'
.text:000000014001CC4A lea     rdx, aTlsEnableSslTl ; "      --tls                   enable "...
.text:000000014001CC51 mov     rcx, rbx
.text:000000014001CC54 call    sub_1406A1C30
.text:000000014001CC59 mov     rax, rsi
.text:000000014001CC5C sub     rax, cs:qword_14090F208
.text:000000014001CC63 cmp     rax, 5Fh ; '_'
.text:000000014001CC67 jbe     loc_14001DAF0

aTlsEnableSslTl db '      --tls                   enable SSL/TLS support (needs poo'
                                                  ; DATA XREF: sub_14001C8E0+36A↑o
                db 'l support)',0Ah,0
```

After some group nodes there was a group nodes config=FILE and you can see in the secrenshort that there is “load a JSON-format configuration file”

```
.text:000000014001D7D4 mov     r8d, 46h ; 'F'
.text:000000014001D7DA lea     rdx, aCConfigFileLoa ; "  -c, --config=FILE            load a "...
.text:000000014001D7E1 mov     rcx, rbx
.text:000000014001D7E4 call    sub_1406A1C30
.text:000000014001D7E9 mov     rax, rsi
.text:000000014001D7EC sub     rax, cs:qword_14090F208
.text:000000014001D7F3 cmp     rax, 3Fh ; '?'
.text:000000014001D7F7 jbe     loc_14001DAF0

aCConfigFileLoa db '  -c, --config=FILE            load a JSON-format configuration '
                                                  ; DATA XREF: sub_14001C8E0+EFA↑o
                db 'file',0Ah,0
```

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
After that there was a group nodes which is background and you can see in the secrenshort that there is “run the miner in the background” which is run the miner in the background of the screan and this make the malware work in the hide seen

```
.text:000000014001D7FD mov     r8d, 40h ; '@'
.text:000000014001D803 lea     rdx, aBBackgroundRun ; "  -B, --background              run the"...
.text:000000014001D80A mov     rcx, rbx
.text:000000014001D80D call    sub_1406A1C30
.text:000000014001D812 mov     rax, rsi
.text:000000014001D815 sub     rax, cs:qword_14090F208
.text:000000014001D81C cmp     rax, 43h ; 'C'
.text:000000014001D820 jbe     loc_14001DAF0

aBBackgroundRun db '  -B, --background              run the miner in the background',0Ah
                                                     ; DATA XREF: sub_14001C8E0+F23↑o
                db 0
```

Then I notest the three functens of the “Tls_Callback” which is for set up the devis with the functens and the DLL befor start the connecten with the remot IP address and start mining the first Tls_Callback_0 which have the conditional execute that go to different paths based on the value and this maybe to see the setup environment.

Then I go to the next Tls_Callback_1 which have simpler then the Tls_Callback_0 but I notest that all of the Tls_Callback_0 and Tls_Callback_1 if it is true will call the same funcetes which is “sub_1404F8A10” so I go to see the functens and this is what I gat :

```
.text:00000001404F8AF0 lea     rcx, stru_140C2DBE0
.text:00000001404F8AF7 call    cs:__imp_InitializeCriticalSection
```

```
.text:00000001404F8A32 loc_1404F8A32:
.text:00000001404F8A32 mov     cs:dword_140C2DBC8, 1
```

And this is one of the group nodes which for the to initialize critical section stru_140C2DBE0 after the initialize the function sets a flag to 1 if it fails will end .

```
.text:00000001404F8AC5 call    cs:__imp_DeleteCriticalSection
```

There is a group nodes which have a function deletes the critical section and after that the function will returns after doing these operations.

For the last one of the Tls_Callback_2 which most complex of the three

```
.text:000000014050C8A9 call    cs:__imp_TlsGetValue
```

There is a call for the TlsSetValue to set TLS indices.

```
.text:000000014050C9B3 call    cs:__imp_CloseHandle
```

There were a critical system functions like CloseHandle which may cleanup the track of the malware and this is more suspect.

For the Tls_Callback_2 I think it is for management the advanced operations and have to cleanup to avoid detection.

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

Advanced Dynamic Analysis

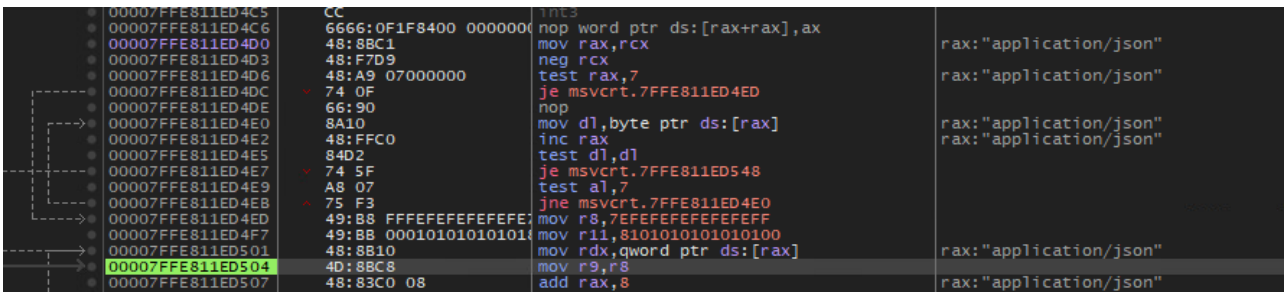
1 x64dbg

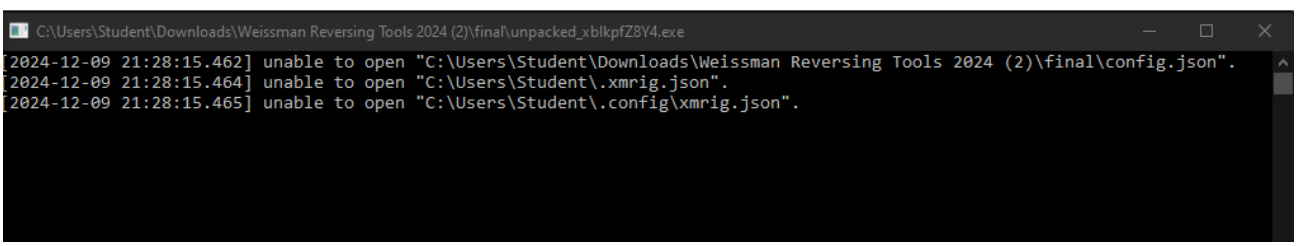
Here I opened the malware after the UPX unpacked which was have a lot of the string and the code in the CPU I searched in the sting about the JSON to see where the file would start the connect to the mining pool and I noticed the “application/json” so I put a breakpoint there so I notest in the malware output that of the malware which is the binary string to open the JSON in different three file design and all three is unable to open which is:

"C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final\config. json".

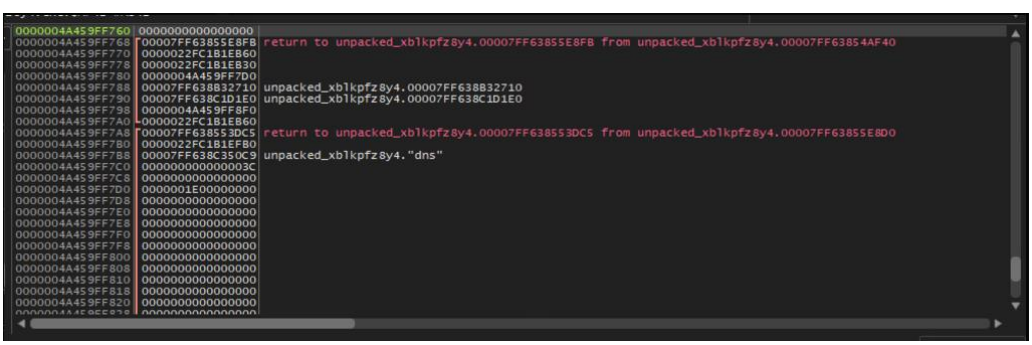
"C:\Users\Student\.xmrig. json".

"C: \Users\Student\.config\xmrig. json".





And I noticed that in the call stack there is a “unpacked_xb1kpfz8y4."dns" “ which shows that the malware might be there is addressing to the domain names or to communicating with network APIs for.



Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project
Then after a little of the F7 and F8 the malware found the JSON file and now is trying to ping the IPV6 and the DNS mining server and using the TTL which is the time to live which is to set the communication time with the DNS.

```
7FF63855E8E3   48:8901              mov qword ptr ds:[rcx],rax
7FF63855E8E6   48:89D6              mov rsi,rdx                                  rdx:"ipv6"
7FF63855E8E9   48:8B15 98E96B00     mov rdx,qword ptr ds:[7FF638C1D288]          rdx:"ipv6", 00007FF638C1D288:&"ipv6"
7FF63855E8F0   48:89CB              mov rbx,rcx
7FF63855E8F3   48:89F1              mov rcx,rsi
7FF63855E8F6   E8 45C6FEFF          call unpacked_xblkpfz8y4.7FF63854AF40
7FF63855E8FB   44:8B43 04           mov r8d,dword ptr ds:[rbx+4]
7FF63855E8FF   48:8B15 7AE96B00     mov rdx,qword ptr ds:[7FF638C1D280]          rdx:"ipv6", 00007FF638C1D280:&"ttl"
```

```
7FF63855E96F   E8 54B44E00          call <JMP.&strlen>
7FF63855E974   48:C74424 48 00000000 mov qword ptr ss:[rsp+48],0                 [rsp+48]:"dns"
7FF63855E97D   49:89C5              mov r13,rax
7FF63855E980   66:897424 4E         mov word ptr ss:[rsp+4E],si
7FF63855E985   48:B8 0000000000000050 mov rax,4050000000000000
```

```
7FF63855E94E   48:C701 00000000     mov qword ptr ds:[rcx],0
7FF63855E955   48:8B2D 2CE96B00     mov rbp,qword ptr ds:[7FF638C1D288]          00007FF638C1D288:&"ipv6"
7FF63855E95C   48:89CB              mov rbx,rcx
7FF63855E95F   48:89D7              mov rdi,rdx                                  rdx:"ttl"
7FF63855E962   4C:8971 08           mov qword ptr ds:[rcx+8],r14
7FF63855E966   0FB632               movzx esi,byte ptr ds:[rdx]                  rdx:"ttl"
7FF63855E969   48:89E9              mov rcx,rbp
7FF63855E96C   83C6 09              add esi,9
7FF63855E96F   E8 54B44E00          call <JMP.&strlen>
7FF63855E974   48:C74424 48 00000000 mov qword ptr ss:[rsp+48],0                 [rsp+48]:"dns"
```

Then after a little of the F7 and F8 the malware I noticed that the communication with the DNS was going on and now the malware is trying to connect the “pool hashvault. Pro” which is the mining pool known as the mining platform and it is using another mining platform that “nicehash.com” which is could be the malware using 2 different mining platform or it is for backup which is if one does not connect will use the second as a backup and there is a user name of the pool.

```
7FF638572332   F641 48 01           test byte ptr ds:[rcx+48],1
7FF638572336   74 15                je unpacked_xblkpfz8y4.7FF63857234D
7FF638572338   48:83B9 E8000000 00  cmp qword ptr ds:[rcx+E8],0                  [rcx+E8]:"pool.hashvault.pro"
7FF638572340   74 0B                je unpacked_xblkpfz8y4.7FF63857234D
7FF638572342   66:83B9 08010000 00  cmp word ptr ds:[rcx+108],0
7FF63857234A   0F95C0               setne al
7FF63857234D   C3                   ret
```

```
48:8B15 50B26A00   mov rdx,qword ptr ds:[7FF638C1D2E0]   00007FF638C1D2E0:&"nicehash.com"
```

```
48:8B8B 80000000   mov rcx,qword ptr ds:[rbx+80]   [rbx+80]:"8BGU1iynUuB9EQ2p9UmVVF8hmA8BG76T4iUuL3FTAJHkUeJW2WcPswabnfciFmwDw52KWEqDX2foHNcqdBVVXAxnVcihF9D"
48:85C9            test rcx,rcx
```

Then after a little of the F7 and F8 the malware there is an IP address which is the “142.202.242.43” then after that there is another IP address which is the “142.202.242.45” which is now is trying to connect to the pool with the user name “8BGU1iynUuB9EQ2p9UmVVF8hmA8BG76T4iUuL3FTAJHkUeJW2W cPswabnfciFmwDw52KWEqDX2foHNcqdBVVXAxnVcihF9D".

```
00007FF638572232   48:C741 D0 00000000   mov qword ptr ds:[rcx-30],0   [rcx-30]:"142.202.242.43:80"
```

```
48:83B9 E8000000 00   cmp qword ptr ds:[rcx+E8],0   [rcx+E8]:"142.202.242.45"
```

```
00007FF638572188   48:C781 58FFFFFF 000( mov qword ptr ds:[rcx-A8],0   [rcx-A8]:"8BGU1iynUuB9EQ2p9UmVVF8hmA8BG76T4iUuL3FTAJHkUeJW2WcPswabnfciFmwDw52KWEqDX2foHNcqdBVVXAxnVcihF9D"
00007FF638572188   48:C781 58FFFFFF 000( mov qword ptr ds:[rcx-A8],0
00007FF638572188   48:C781 60FFFFFF 000( mov qword ptr ds:[rcx-A0],0
```

Then after a little of the F7 and F8 the malware there is an RDX: "//xmrig.com/wizard" "active" which the active connects to the mining pool.

```
FFE811ED519   48:8B50 F8   mov rdx,qword ptr ds:[rax-8]   rdx:"//xmrig.com/wizard", rax-08:"active"
FFE811ED51D   84D2         test dl,dl
```

Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

Then after a little of the F7 and F8 the malware output gives some of the information which is about the using tool and it is “XMRig/6.22.1-dev “ which is used for cryptocurrency mining and it is free software and there is information about the CPU and the memory and motherboard of the device and that means the malware is take information about the device which makes it strange and suspicious and there is the three POOL of the mining with algo auto.

```
[2024-12-10 00:08:56.476] unable to open "C:\Users\Student\.config\xmrig.json".
 * ABOUT        XMRig/6.22.1-dev gcc/14.1.0 (built for Windows x86-64, 64 bit)
 * LIBS         libuv/1.48.0 OpenSSL/3.0.13 hwloc/2.10.0
 * HUGE PAGES   unavailable
 * 1GB PAGES    unavailable
 * CPU          Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz (2) 64-bit AES VM
                L2:0.5 MB L3:50.0 MB 2C/2T NUMA:1
 * MEMORY       4.7/16.0 GB (29%)
                RAM slot #0: 16 GB DRAM @ 0 MHz RAM slot #0
 * MOTHERBOARD  VMware, Inc. - VMware Virtual Platform
 * DONATE       0%
 * ASSEMBLY     auto:intel
 * POOL #1      pool.hashvault.pro:80 algo auto
 * POOL #2      142.202.242.43:80 algo auto
 * POOL #3      142.202.242.45:80 algo auto
 * COMMANDS     hashrate, pause, resume, results, connection
```

Then after a little of the F7 and F8 the malware output gave as some the information which is about the state of what is going on now I you can see in the screenshot the malware first used the pool of “142.202.242.45: in port 80 and after sections there is a new job from the “pool.hashvault.pro:80” with “diff 36000 algo” which may the algorithm of the mining then there is the randomx “allocated 2336 MB” after that there is a new job from the “pool.hashvault.pro:80” with “diff 36000 algo” after that randomx give a “dataset ready (21743 ms)” this is all happened in less in second which I think it is for make everything ready for mining

After 30 seconds the CPU will use profile rx (1000 threads) scratchpad 2048 KB and will give a ready for it.

```
[2024-12-10 00:08:56.474] unable to open "C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final\config.json".
[2024-12-10 00:08:56.475] unable to open "C:\Users\Student\.xmrig.json".
[2024-12-10 00:08:56.476] unable to open "C:\Users\Student\.config\xmrig.json".
 * ABOUT        XMRig/6.22.1-dev gcc/14.1.0 (built for Windows x86-64, 64 bit)
 * LIBS         libuv/1.48.0 OpenSSL/3.0.13 hwloc/2.10.0
 * HUGE PAGES   unavailable
 * 1GB PAGES    unavailable
 * CPU          Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz (2) 64-bit AES VM
                L2:0.5 MB L3:50.0 MB 2C/2T NUMA:1
 * MEMORY       4.7/16.0 GB (29%)
                RAM slot #0: 16 GB DRAM @ 0 MHz RAM slot #0
 * MOTHERBOARD  VMware, Inc. - VMware Virtual Platform
 * DONATE       0%
 * ASSEMBLY     auto:intel
 * POOL #1      pool.hashvault.pro:80 algo auto
 * POOL #2      142.202.242.43:80 algo auto
 * POOL #3      142.202.242.45:80 algo auto
 * COMMANDS     hashrate, pause, resume, results, connection
 * OPENCL       disabled
 * CUDA         disabled
[2024-12-10 00:38:08.798]  net      use pool pool.hashvault.pro:80  142.202.242.45
[2024-12-10 00:38:08.799]  net      new job from pool.hashvault.pro:80 diff 36000 algo rx/0 height 3299670 (23 tx)
[2024-12-10 00:38:08.800]  cpu      use argon2 implementation SSSE3
[2024-12-10 00:38:08.801]  msr      to access MSR registers Administrator privileges required.
[2024-12-10 00:38:08.801]  msr      FAILED TO APPLY MSR MOD, HASHRATE WILL BE LOW
[2024-12-10 00:38:08.802]  randomx  init dataset algo rx/0 (2 threads) seed ede5e439528eee83...
[2024-12-10 00:38:08.824]  randomx  allocated 2336 MB (2080+256) huge pages 0% 0/1168 +JIT (22 ms)
[2024-12-10 00:38:30.361]  net      new job from pool.hashvault.pro:80 diff 36000 algo rx/0 height 3299670 (26 tx)
[2024-12-10 00:38:30.568]  randomx  dataset ready (21743 ms)
[2024-12-10 00:38:30.588]  cpu      use profile  rx  (1000 threads) scratchpad 2048 KB
[2024-12-10 00:38:31.363]  cpu      READY threads 1000/1000 (1000) huge pages 0% 0/1000 memory 2048000 KB (775 ms)
```

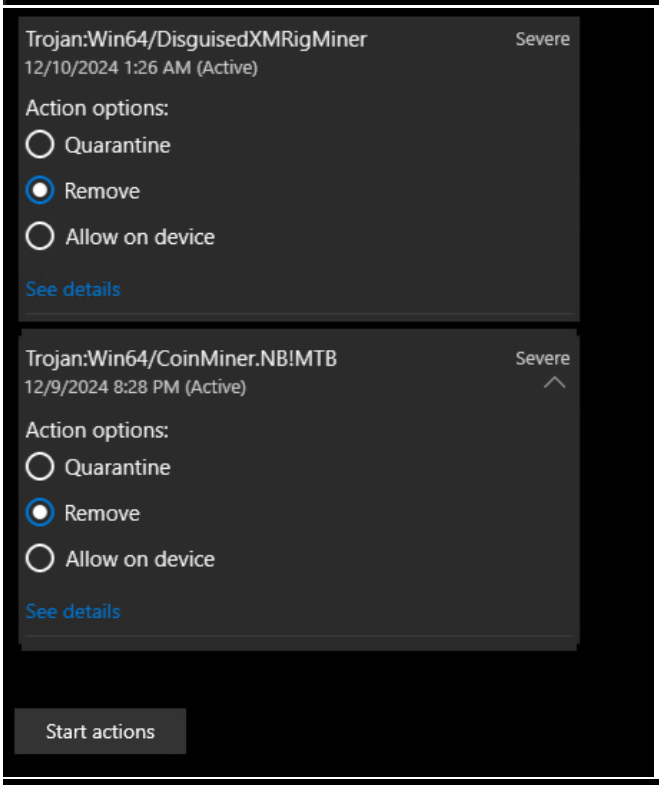
Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

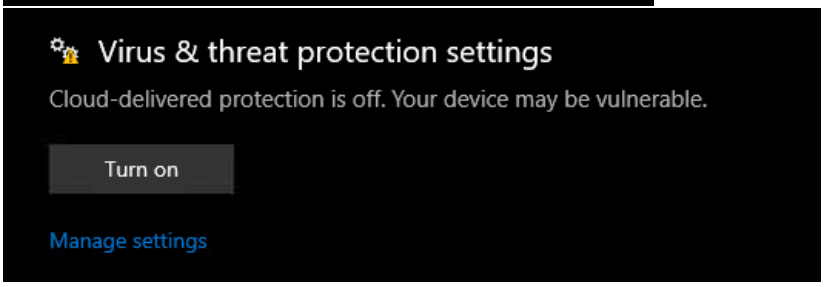
How to remove the malware

The first I do I chack the task menager to see if the malware is still run I did not see it so I ran the CMD administrator to kill the malware I delete the all of the files that are related to the malware than I check the Virus & threat protection to see what happand I see there is a two "Trojan:Win64/DisguisedXMRigMiner" and "Trojan:Win64/CoinMiner.NB!MTB" was found in the scan and I remove it after that I turn on the Virus & threat protection to make sure.

```
C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>del xblkpfZ8Y4.exe

C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>del unpacked_xblkpfZ8Y4.exe
```

```
C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>del xblkpfZ8Y4.exe

C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>del unpacked_xblkpfZ8Y4.exe

C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>del Extracted_xblkpfZ8Y4.exe

C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>del xblkpfZ8Y4.exe.i64

C:\Users\Student\Downloads\Weissman Reversing Tools 2024 (2)\final>del unpacked_xblkpfZ8Y4.exe.i64
```





Name: Hassan Alshehri
Class: CSEC.202.01 - Reverse Engineering Fund
Reversing Project

SUMMARY

The analysis of the xblkpfZ8Y4.exe malware which is I use the four stages: Basic Static Analysis and Basic Dynamic Analysis and Advanced Static Analysis and Advanced Dynamic Analysis. During the Basic Static Analysis stage tools like a PEview and Resource Hacker and Strings and UPX and VirusTotalwere used to get more information of the malware behavior. The malware was found to use a multiple Windows APIs and DLL like KERNEL32.DLL, USER32.dll, ADVAPI32.dll, CRYPT32.dll, IPHLPAPI.DLL, WS2_32.dll and have UPX packed to execute hidden code and and connections to domains like "pool.hashvault.pro" and remot IP like “142.202.242.45:80””142.202.242.43:80” were identified which is use for a cryptocurrency mining purpose. Additionally, there was strings obfuscated strings and API calls to evade detection using the UPX.

The Basic Dynamic Analysis stage confirmed the execution of the malware and analyzed network activity. There was network captures revealed connections to mining pools which is the “remote IP address “142.202.242.45” port “80”” and after the conecten there was a procec going on which consistent with the cryptocurrency mining behavior that already found. Tools like Process Monitor provided additional evidence of network traffic and process modifications.

In the Advanced Static Analysis stage disassembling the binary in IDA revealed the use a lot of functens that are complex and related to each other. The malware used the three of TLS Callbacks to execute code before the main entry point of the mining which give as further demonstrating its complex character.

The Advanced Dynamic Analysis stage used tools like x64dbg to trace the malware runtime behavior. This stage confirmed that the malware have main gool was to mine cryptocurrency by hijacking system resources and connecting to mining pools. Additionally the malware tries to keep the connection to the remort pool.