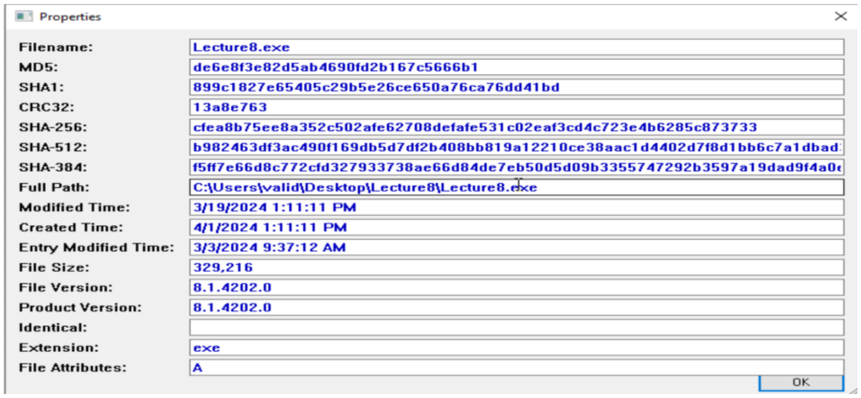
Vivek Madala

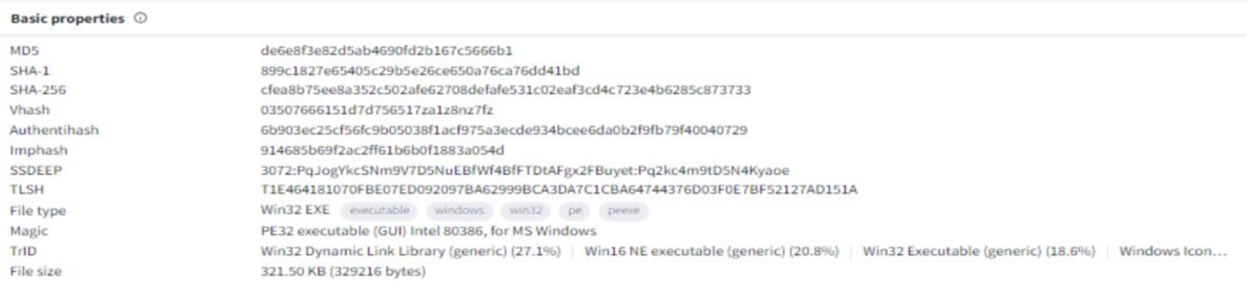
3/17/2024

CYBV 454-Galde

Lecture 8 Malware Analysis

- **Hash Analysis**
  - First in order to proceed with my initial hash analysis I extracted the file using HashMyFiles as source to cross reference the information I find through VirusTotal, these were the hashes I could verify and cross referenced using VirusTotal analysis.
  - MD5: de6e8f3e82d5ab4690fd2b167c5666b1
  - SHA1: 899c1827e65405c29b5e26ce650a76ca76dd41bd
  - SHA-256: cfea8b75ee8a352c502afe62708defafe531c02eaf3cd4c723e4b6285c873733
  - 

Filename:	Lecture8.exe
MD5:	de6e8f3e82d5ab4690fd2b167c5666b1
SHA1:	899c1827e65405c29b5e26ce650a76ca76dd41bd
CRC32:	13a8e763
SHA-256:	cfea8b75ee8a352c502afe62708defafe531c02eaf3cd4c723e4b6285c873733
SHA-512:	b982463df3ac490f169db5d7df2b408bb819a12210ce38aac1d4402d7f8d1bb6c7a1dbad
SHA-384:	f5ff7e66d8c772cfd327933738ae66d84de7eb50d5d09b3355747292b3597a19dad9f4a0
Full Path:	C:\Users\valid\Desktop\Lecture8\Lecture8.exe
Modified Time:	3/19/2024 1:11:11 PM
Created Time:	4/1/2024 1:11:11 PM
Entry Modified Time:	3/3/2024 9:37:12 AM
File Size:	329,216
File Version:	8.1.4202.0
Product Version:	8.1.4202.0
Identical:	
Extension:	exe
File Attributes:	A

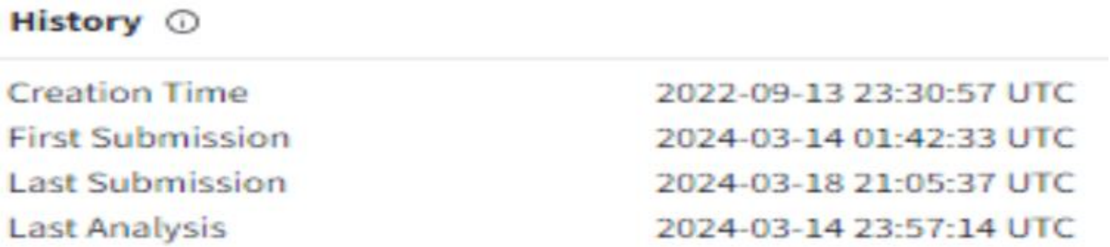


Basic properties ⓘ

MD5	de6e8f3e82d5ab4690fd2b167c5666b1
SHA-1	899c1827e65405c29b5e26ce650a76ca76dd41bd
SHA-256	cfea8b75ee8a352c502afe62708defafe531c02eaf3cd4c723e4b6285c873733
Vhash	03507666151d7d756517za1z8nz7fz
Authentihash	6b903ec25cf56fc9b05038f1acf975a3ecde934bcee6da0b2f9fb79f40040729
Imphash	914685b69f2ac2ff61b6b0f1883a054d
SSDEEP	3072:PqJogYkcSNm9V7D5NuEBfWf4BfFTDtAFgx2FBuyet:Pq2kc4m9tD5N4Kyaoe
TLSH	T1E464181070FBE07ED092097BA62999BCA3DA7C1CBA64744376D03F0E7BF52127AD151A
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Dynamic Link Library (generic) (27.1%) | Win16 NE executable (generic) (20.8%) | Win32 Executable (generic) (18.6%) | Windows Icon...
File size	321.50 KB (329216 bytes)

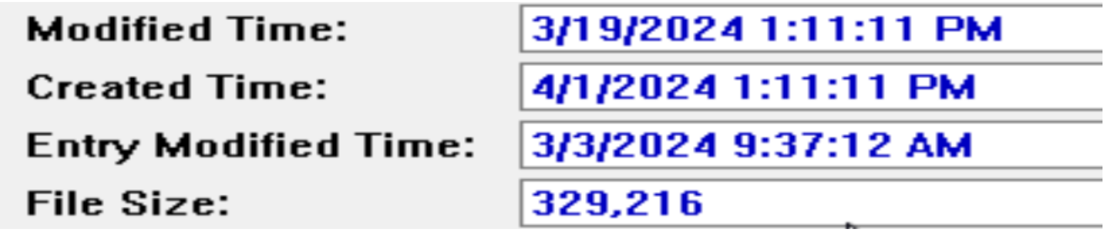
- **Vendor Analysis**
  - For my Vendor Analysis using VirusTotal, these were the following results: **58/73** vendors flagged this file as **malicious**. The most popular threat label given was **ransomware.lockbit/blackmatter** and the threat categories widely agreed upon were ransomware and trojan with the family labels being lockbit, blackmatter, and encoder. There were several big vendors who detected and flagged the file such as Crowdstrike Falcon, Google, Fortinet, and Elastic but there were also several that did not detect it such as Palo Alto Networks, Kingsoft, Baidu and several others.
- **File History**
  - The first file submission to VirusTotal being 2024-03-14 0:42:33 UTC which is a critical indicator of when the malware was likely first detected and began to be analyzed by security vendors and analysts. The creation time is also significant, 2022-09-13 which means the malware has mutated and created a new variant since its initial creation time or it's a means for analysis obfuscation and is incorrect. Although the last submission date in VirusTotal indicates 2024-03-18, using HashMyFiles I was able to find more accurate results for creation time

being 4/1/2024 1:11:11 PM which means there's a conflict in time details of the file.

- 

  History

Creation Time	2022-09-13 23:30:57 UTC
First Submission	2024-03-14 01:42:33 UTC
Last Submission	2024-03-18 21:05:37 UTC
Last Analysis	2024-03-14 23:57:14 UTC

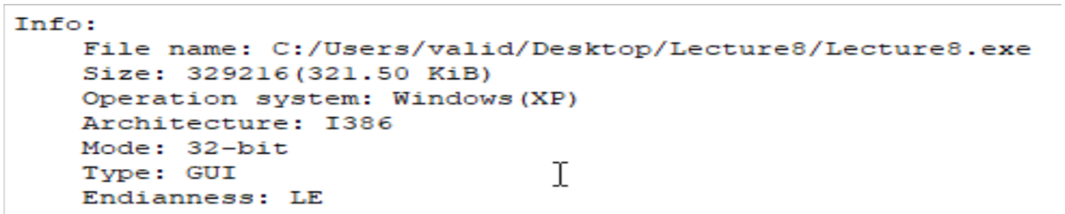
- 

Modified Time:	3/19/2024 1:11:11 PM
Created Time:	4/1/2024 1:11:11 PM
Entry Modified Time:	3/3/2024 9:37:12 AM
File Size:	329,216

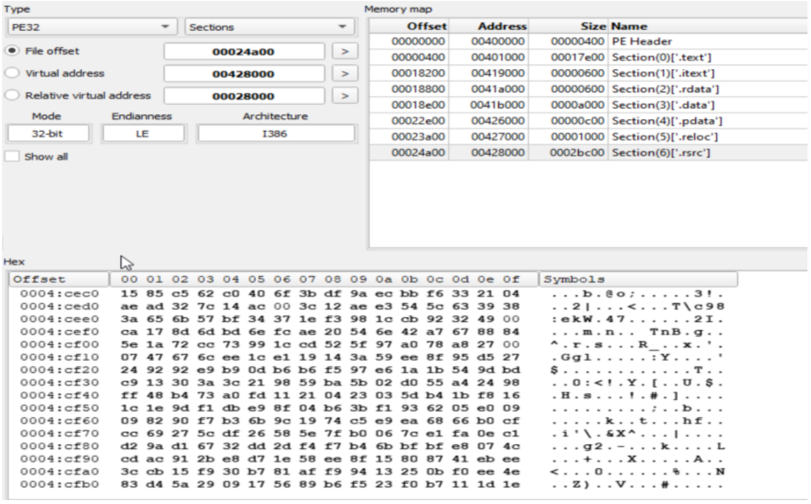
- **Community**
  - I have provided a VirusTotal comment that summarizes my analysis and research of Lecture 8 malware. The malware is an extremely persistent piece of ransomware that demands money from the victim while using encryption to lock down their system files and is a part of the Blackmatter malware family. https://www.virustotal.com/gui/file/cfea8b75ee8a352c502afe62708defafe531c02eaf3cd4c723e4b6285c873733

- **File Info**
  - For my initial DIE analysis, I gathered file information that is valuable, the file is a 32-bit executable that's named "Lecture8.exe" with a size of approximately 321.50 KB's and was designed to run on a Windows XP operating system (this could be a tactic to appear as a legacy system application). It has an Intel 386

architecture which means it's meant for x86 processors, and the file is a GUI application rather than command line so the user can expect some sort of graphical interface. The endianness is Little Endian which represents the byte order format for storing binary information in the file.

- 

```
Info:
    File name: C:/Users/valid/Desktop/Lecture8/Lecture8.exe
    Size: 329216(321.50 KiB)
    Operation system: Windows(XP)
    Architecture: I386
    Mode: 32-bit
    Type: GUI
    Endianness: LE
```

- **Memory Map**
  - For my memory map analysis these were the following sections that were found using DIE for Lecture8.exe; a PE Header section, '.text', '.itext', '.rdata', '.data', '.pdata', '.reloc', '.rsrc' sections which relatively new sections I have not done seen before such as '.itext'. There wasn't a single section except for PE header section that was legible, the entire memory map symbols for every single section were all scrambled indicating a high level of obfuscation to avoid analysis.
  - 

Type: PE32 · Sections

● File offset: 00024a00
○ Virtual address: 00428000
○ Relative virtual address: 00028000

Mode: 32-bit · Endianness: LE · Architecture: I386

□ Show all

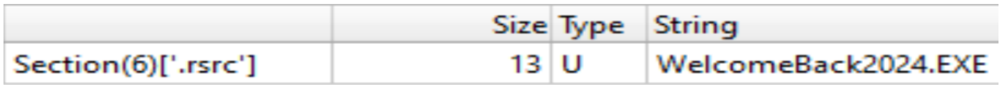
Memory map

Offset	Address	Size	Name
00000000	00400000	00000400	PE Header
00000400	00401000	00017e00	Section(0)['.text']
00018200	00419000	00000600	Section(1)['.itext']
00018800	0041a000	00000600	Section(2)['.rdata']
00018e00	0041b000	0000a000	Section(3)['.data']
00022e00	00426000	00000c00	Section(4)['.pdata']
00023a00	00427000	00001000	Section(5)['.reloc']
00024a00	00428000	0002bc00	Section(6)['.rsrc']

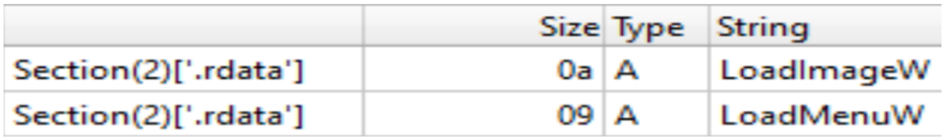
Hex

```
Offset      00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f   Symbols
0004:cec0   15 85 c5 62 c0 40 6f 3b df 9a ec bb f6 33 21 04   ...b.@o;.....3!.
0004:ced0   ae ad 32 7c 14 ac 00 3c 12 ae e3 54 5c 63 39 38   ..2|...<...T\c98
0004:cee0   3a 65 6b 57 bf 34 37 1e f3 98 1c cb 92 32 49 00   :ekW.47......2I.
0004:cef0   ca 17 8d 6d bd 6e fc ae 20 54 6e 42 a7 67 88 84   ...m.n.. TnB.g..
0004:cf00   5e 1a 72 cc 73 99 1c cd 52 5f 97 a0 78 a8 27 00   ^.r.s...R_..x.'.
0004:cf10   07 47 67 6c ee 1c e1 19 14 3a 59 ee 8f 95 d5 27   .Ggl.....:Y....'
0004:cf20   24 92 92 e9 b9 0d b6 b6 f5 97 e6 1a 1b 54 9d bd   $............T..
0004:cf30   c9 13 30 3a 3c 21 98 59 ba 5b 02 d0 55 a4 24 98   ..0:<!.Y.[..U.$.
0004:cf40   ff 48 b4 73 a0 fd 11 21 04 23 03 5d b4 1b f8 16   .H.s...!.#.]....
0004:cf50   1c 1e 9d f1 db e9 8f 04 b6 3b f1 93 62 05 e0 09   .........;..b...
0004:cf60   09 82 90 f7 b3 6b 9c 19 74 c5 e9 ea 68 66 b0 cf   .....k..t...hf..
0004:cf70   cc 69 27 5c df 26 58 5e 7f b0 06 7c e1 fa 0e c1   .i'\.&X^...|....
0004:cf80   d2 9a d1 67 32 dd 2d f4 f7 b4 6b bf bf e8 07 4c   ...g2.-...k....L
0004:cf90   cd ac 91 2b e8 d7 1e 58 ee 8f 15 80 87 41 eb ee   ...+...X.....A..
0004:cfa0   3c cb 15 f9 30 b7 81 af f9 94 13 25 0b f0 ee 4e   <...0......%...N
0004:cfb0   83 d4 5a 29 09 17 56 89 b6 f5 23 f0 b7 11 1d 1e   ..Z)..V...#.....
```

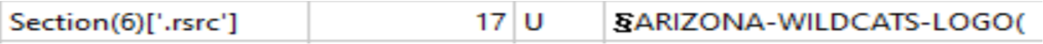
- **Strings**

    - For my string analysis of Lecture8.exe I looked for specific strings that indicated any possible ill intentions. The first strings I found were in relation to ".exe" and I found an interesting string named "WelcomeBack2024.exe" which is awfully suspicious and indicates the executable changes its own name and is greeting to the user. There are also strings in relation to the command line being accessed, 'GetCommandLineA' and 'GetCommandLineW' which indicates the program intends to access the command line interface which is unusual. I then located two very suspicious strings being 'LoadImageW' and 'LoadMenuW' which indicates this executable is looking to load a GUI onto the user's interface with an image. I found one another string in relation to a logo named 'Arizona Wildcats Logo' which indicates this could be part of the menu that is loaded.
    - 

	Size	Type	String
Section(6)['.rsrc']	13	U	WelcomeBack2024.EXE

    - 

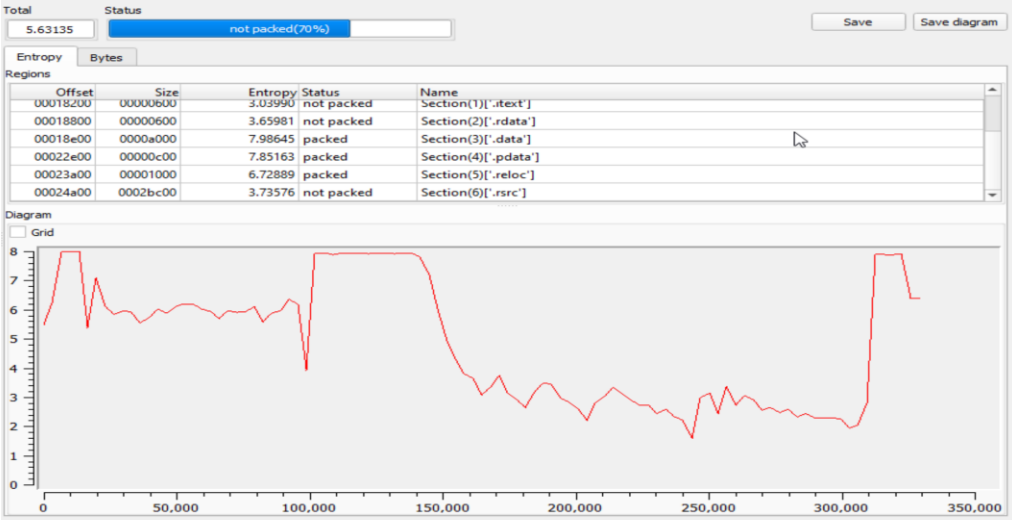
	Size	Type	String
Section(2)['.rdata']	0a	A	LoadImageW
Section(2)['.rdata']	09	A	LoadMenuW

    - 

Section(6)['.rsrc']	17	U	§ARIZONA-WILDCATS-LOGO(

- **Entropy**
    - Using DIE I gathered analysis on the Entropy of the malware, DIE has given Lecture8.exe an **entropy value of 5.63135 with a 70% confidence** that the file is **not packed**. Looking through the individual sections and their entropy values, the sections that were identified to be packed were section **'.text', '.data', '.pdata', and '.reloc'** with the highest entropy section being '.data' with a value of

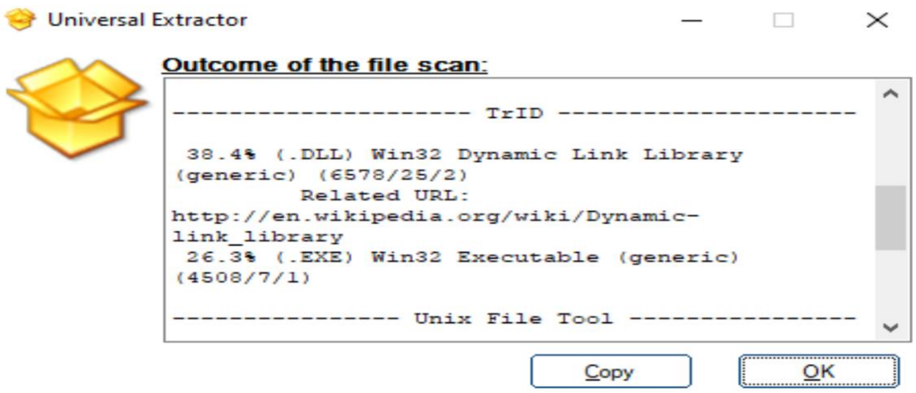
7.98645. To unpack the file, I used Universal Extractor, and it gathered similar results, the file is **not packed,** and it did not find anything in the PEiD using ext and hard methods; Universal Extractor did find TrID but listed both to be “generic”.

- 

Total: 5.63135

Status: not packed(70%)

Offset	Size	Entropy	Status	Name
00018200	00000600	3.03990	not packed	Section(1)['.itext']
00018800	00000600	3.65981	not packed	Section(2)['.rdata']
00018e00	0000a000	7.98645	packed	Section(3)['.data']
00022e00	00000c00	7.85163	packed	Section(4)['.pdata']
00023a00	00001000	6.72889	packed	Section(5)['.reloc']
00024a00	0002bc00	3.73576	not packed	Section(6)['.rsrc']

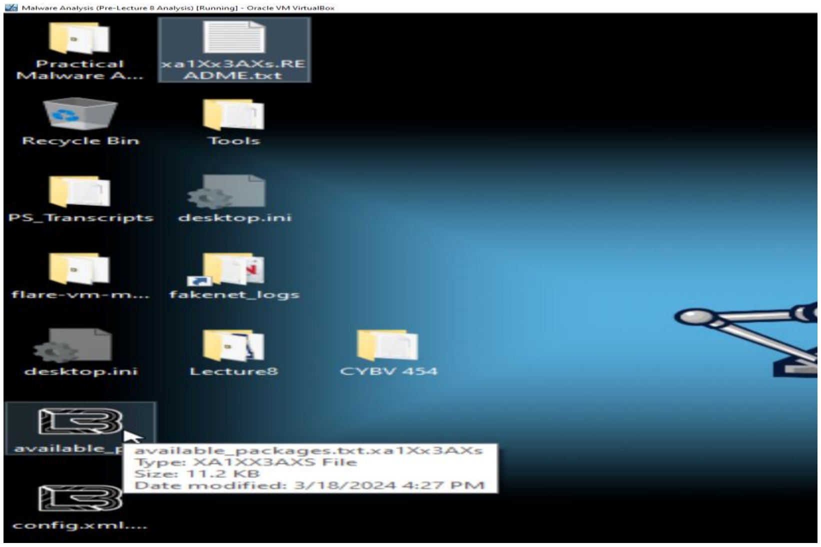
- 

Outcome of the file scan:

```
---------------------- TrID ----------------------

 38.4% (.DLL) Win32 Dynamic Link Library
(generic) (6578/25/2)
         Related URL:
http://en.wikipedia.org/wiki/Dynamic-
link_library
 26.3% (.EXE) Win32 Executable (generic)
(4508/7/1)

---------------- Unix File Tool ----------------
```

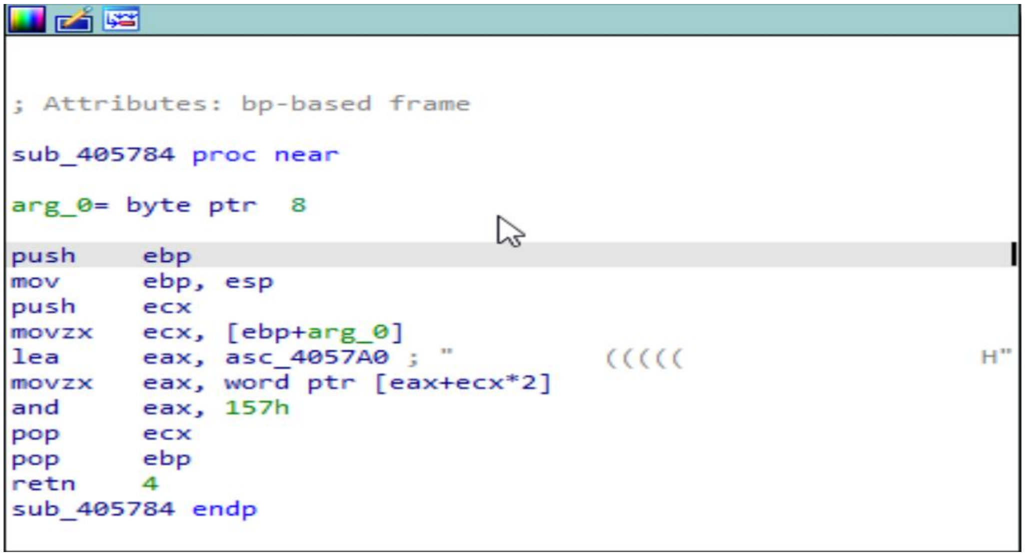
Overall Assessment of this area: Based on my static analysis my overall assessment is that Lecture8.exe indicates a very high probability of having multiple malicious intentions, based on the vendor analysis with 58/73 vendors on VirusTotal identifying it as a Ransomware, and considering its ties with Blackmatter malware family. The file displays extremely concerning strings in relation to fetching command line, intent to load a menu and image which are extremely troubling signs that point to this executable being a persistent ransomware that will make the victim pay money if they run this malware. With the memory map being extremely obfuscated signs point to detection evasion by the malware and several sections within the entropy showcase they are packed which are bad signs.

Next, you will continue your analysis using a disassembler of your choice. You will do the following sections by providing an analysis based on your findings.

- Start Point
    - Using IDA Pro disassembler I was not able to locate any entry points for this executable as the problem arose when I would try to run the executable within IDA Pro for more precise analysis, the ransomware detected my attempts of analysis and quickly locked everything down and so I am stuck with the basic unrun view of IDA Pro which is not able to detect the entry point of the program.
    - 

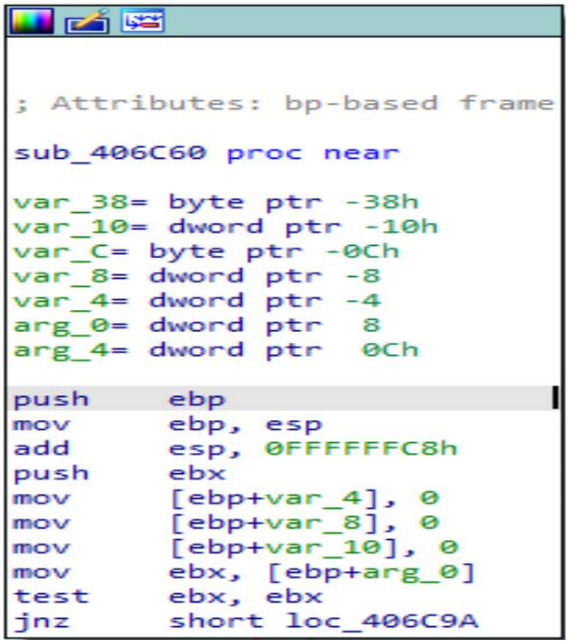
Malware Analysis (Pre-Lecture 8 Analysis) [Running] - Oracle VM VirtualBox

available_packages.txt.xa1Xx3AXs
Type: XA1XX3AXS File
Size: 11.2 KB
Date modified: 3/18/2024 4:27 PM

- Identify Functions
    - Function **sub_405784:** In this function the use of '**push ebp**' and '**mov ebp, esp**' indicates the start of a function that's setting up the stack frame. The '**pop ebp**' followed by a '**ret**' indicates the end of a function which then restores the base pointer and returns to the calling function. Operations involving registers such as '**EAX**' AND '**ECX**' could be performing some sort of pointer arithmetic which is often used to access array elements or structures. In the case of ransomware, this could be part of the routine of the program to access files and encrypt or manipulate data buffers on the users system. The '**and**' instruction performs a bitwise AND operation, this could be used for flag manipulation, bit masking to extract specific bit or to clear bits in a register as part of the programs obfuscation or cryptographic desire. The use of '**lea**' (load effective address) instruction is sometimes used for string operations and could be part of the program's mechanism for creating file paths, URL's or any other stings needed to execute.
    - 

```
; Attributes: bp-based frame

sub_405784 proc near

arg_0= byte ptr  8

push    ebp
mov     ebp, esp
push    ecx
movzx   ecx, [ebp+arg_0]
lea     eax, asc_4057A0 ; "          (((((                    H"
movzx   eax, word ptr [eax+ecx*2]
and     eax, 157h
pop     ecx
pop     ebp
retn    4
sub_405784 endp
```

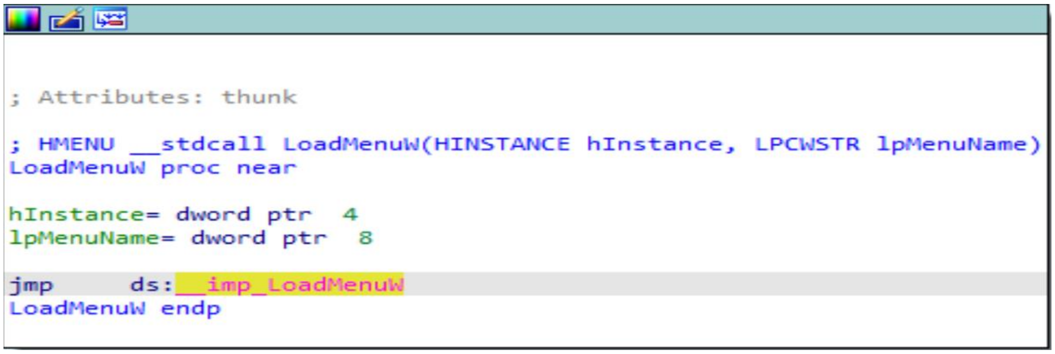
- Function **sub_406C60**: Since my options were limited without being able to run the executable through IDA Pro for more clear cut details I identified another function for analysis, in this function the '**push ebp**' and '**mov ebp, esp**' instructions set up a new stack frame which is usually at the start of a function to save the base pointer and establish a new base for local variables. The '**add esp, 0FFFFFFC8h'** instruction is allocating space for local variables to zero and this could be used to hold temporary data or flags during the function's execution. The function is setting up local variables and checking an argument's value to determine its path of execution, the use of zero initialization and a test for a zero indicates conditional logical based on the input argument which is likely part of a bigger logical process within the program itself.

- 

```
; Attributes: bp-based frame

sub_406C60 proc near

var_38= byte ptr -38h
var_10= dword ptr -10h
var_C= byte ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4
arg_0= dword ptr  8
arg_4= dword ptr  0Ch

push    ebp
mov     ebp, esp
add     esp, 0FFFFFFC8h
push    ebx
mov     [ebp+var_4], 0
mov     [ebp+var_8], 0
mov     [ebp+var_10], 0
mov     ebx, [ebp+arg_0]
test    ebx, ebx
jnz     short loc_406C9A
```

- For the last function rather than sticking to the typical instructions that didn't provide valuable insights into the functions are being used itself, IDA Pro did identify several functions in the case of string names and this one is in relation to

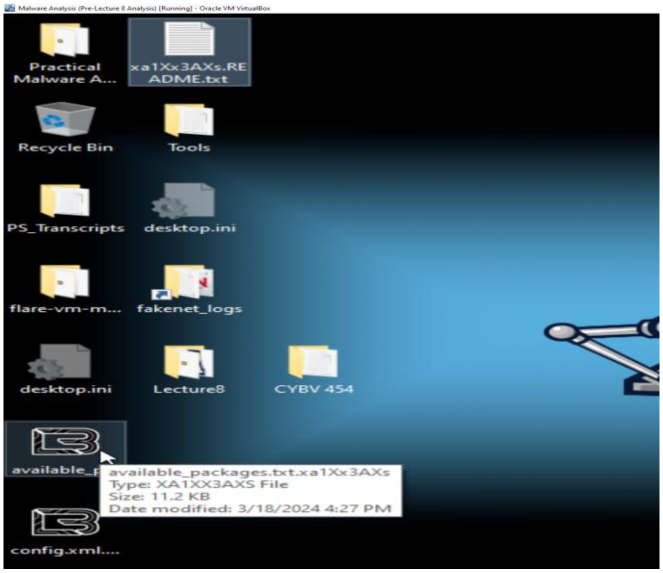
‘**LoadMenuW**’ this is considered a thunk, a stub that’s used to indirectly call another function. The ‘**jmp ds: _imp__LoadMenuW**’ instructions is an indirect jump to the address specified. This label usually indicates it’s an imported function from a DLL which in this case is a Windows API that loads a menu resource from the executable’s resources. The context of this function name is inherently suspicious would could indicate that this is part of the program which calls a Windows API as part of it’s executable process and loads a menu onto the user’s machine after running it.

- 

```
; Attributes: thunk

; HMENU __stdcall LoadMenuW(HINSTANCE hInstance, LPCWSTR lpMenuName)
LoadMenuW proc near

hInstance= dword ptr  4
lpMenuName= dword ptr  8

jmp     ds:__imp_LoadMenuW
LoadMenuW endp
```

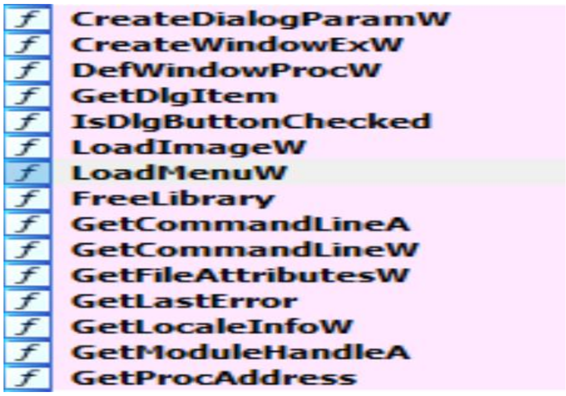
Host Based IOC’s and Network Based IOC

- The first Host-based IOC that I identified was when I tried to IDA Pro and run the file within the decompiling analyzer, the executable file got pretty upset and instantly shutdown my attempts to do disassembly and first ran a ransomware GUI that quickly loaded and then spawned 3 text files one in relation ransomware instructions that seemed to lock down my system with steps to remove the ransomware. This is extremely concerning and is a major red flag and indicates the executable is an extremely malicious piece of malware that does not like certain analysis attempts and will lock down the victim’s machine if detected.

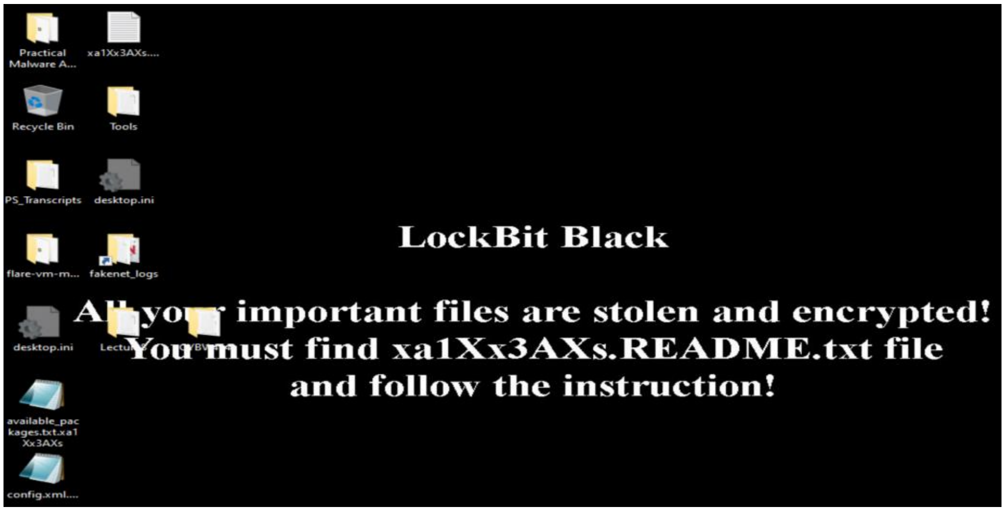
- 

available_packages.txt.xa1Xx3AXs
Type: XA1XX3AXS File
Size: 11.2 KB
Date modified: 3/18/2024 4:27 PM

- The second Host Based IOC that I identified in my earlier static analysis was the presence of strings such as WelcomeBack2024.exe, LoadImageW, LoadMenuW and several other suspicious strings. These strings in particular are extremely unusual as the name change to WelcomeBack2024.exe sounds like more a eerie greeting to the user and the use of strings for command line and loading image and loading menu indicate malicious behavior on the part of the executable program. These are strong indicators of compromise that are extremely suspicious and could be part of a larger execution process by the program itself on the victim.

- 
CreateDialogParamW
CreateWindowExW
DefWindowProcW
GetDlgItem
IsDlgButtonChecked
LoadImageW
LoadMenuW
FreeLibrary
GetCommandLineA
GetCommandLineW
GetFileAttributesW
GetLastError
GetLocaleInfoW
GetModuleHandleA
GetProcAddress

- Another host based IOC that was almost immediate was when I would try to open new Flare-VM malware analysis tools to possibly test with, the program did not like this and would instantly lock down the system and close all applications while displaying information about ‘LockBit Black’ stating that the files are stolen and encrypted and to follow the instructions. This is a clear cut indicator of compromise, the executable does not like analysis being conducted on it by certain programs and does not hesitate to quickly run if any major forms of analysis are to be conducted.

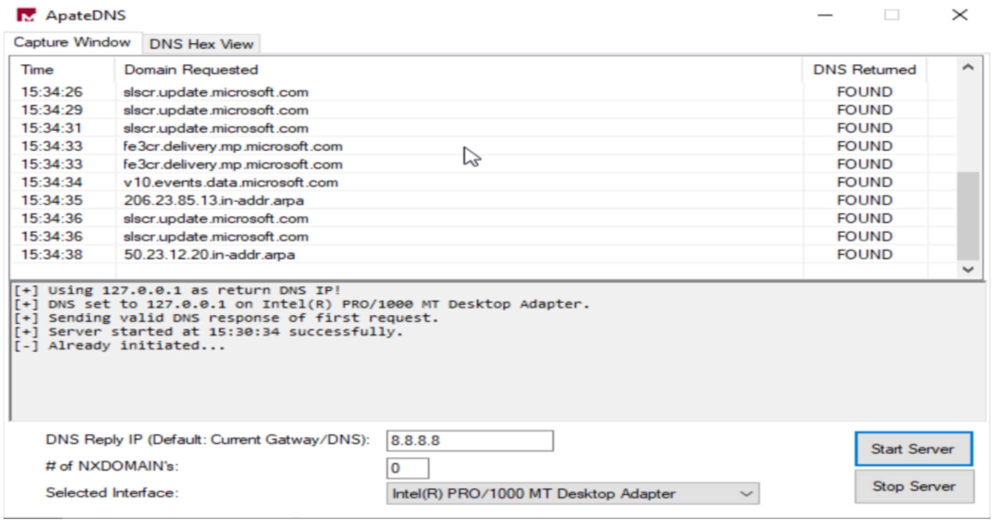
- 

LockBit Black

All your important files are stolen and encrypted!
You must find xa1Xx3AXs.README.txt file
and follow the instruction!

- The Network based IOC that I identified was in relation to my results with APATEDNS, it was extremely difficult to pinpoint the same network activity using FakeNet so it was extremely frustrating to deal with. But the presence of several IP addresses having requested domains as well as slscr.update.microsoft and fe3cr.delivery.mp.microsoft.com are extremely suspicious and are strong network based IOC’s that point to possible command and control network communications by the malware in a very sophisticated stealth manner to conceal it’s real activity. Considering I was not able to identify any network activity with

Procmon or Procexp it’s not shocking that the malware might be trying to evade network communication activity by hiding as legitimate domain names.

- 

Time	Domain Requested	DNS Returned
15:34:26	slscr.update.microsoft.com	FOUND
15:34:29	slscr.update.microsoft.com	FOUND
15:34:31	slscr.update.microsoft.com	FOUND
15:34:33	fe3cr.delivery.mp.microsoft.com	FOUND
15:34:33	fe3cr.delivery.mp.microsoft.com	FOUND
15:34:34	v10.events.data.microsoft.com	FOUND
15:34:35	206.23.85.13.in-addr.arpa	FOUND
15:34:36	slscr.update.microsoft.com	FOUND
15:34:36	slscr.update.microsoft.com	FOUND
15:34:38	50.23.12.20.in-addr.arpa	FOUND

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 15:30:34 successfully.
[-] Already initiated...
```

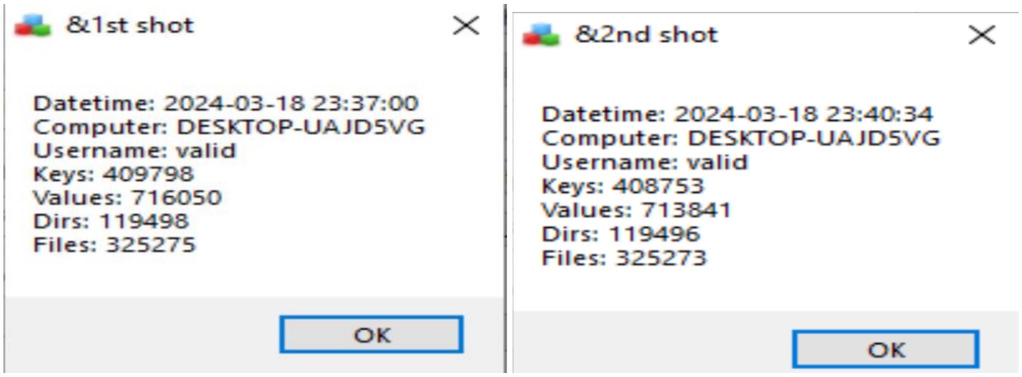
DNS Reply IP (Default: Current Gatway/DNS): 8.8.8.8

# of NXDOMAIN's: 0

Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter

Next, you will run the malicious file in your malware analysis environment and record your findings.

- **Registry Observations**
    - After running both the first and second regshot these were the observations I made, there were nearly 1 thousand key’s that were deleted from the first to second regshot, there were also nearly 2.5 thousand values that were deleted, 2 directories were deleted, and 2 files were also deleted in the process. Based on the results from both regshot’s the program was busy deleting several keys, values, directories, and files from the system.

    - 

      &1st shot

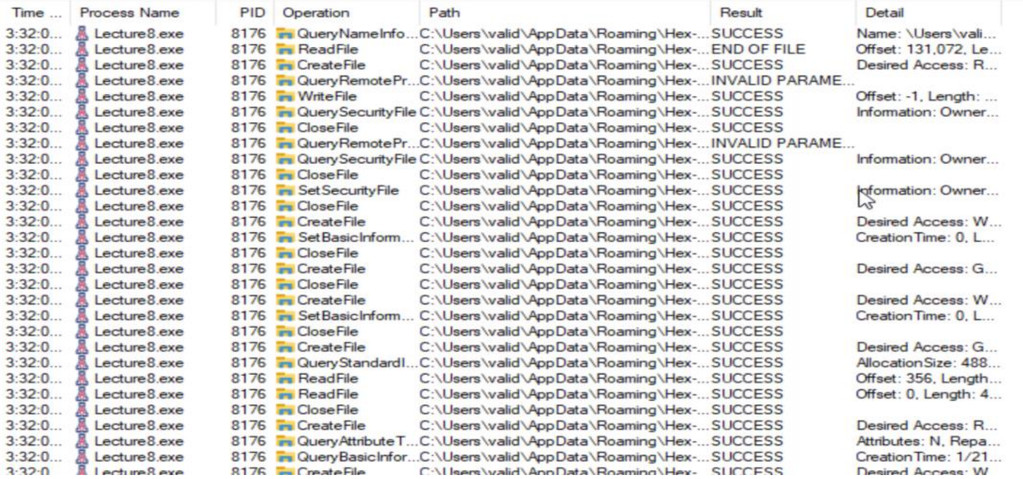
      ```
      Datetime: 2024-03-18 23:37:00
      Computer: DESKTOP-UAJD5VG
      Username: valid
      Keys: 409798
      Values: 716050
      Dirs: 119498
      Files: 325275
      ```

      &2nd shot

      ```
      Datetime: 2024-03-18 23:40:34
      Computer: DESKTOP-UAJD5VG
      Username: valid
      Keys: 408753
      Values: 713841
      Dirs: 119496
      Files: 325273
      ```

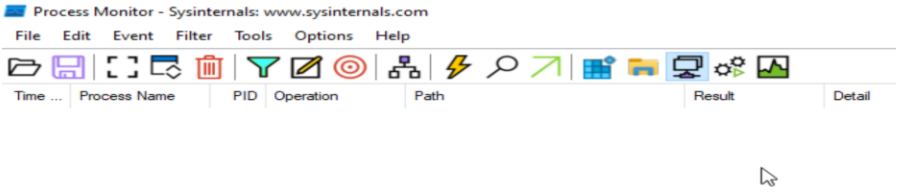
- **Observation**
    - For my analysis environment I am running a Flare-VM using Windows 10 with multiple snapshots in place for pre-dynamic analysis. There are several tools that come in handy with Flare-VM but the ones I used for this analysis are HashMyFiles, DIE, RegShot, IDA Pro, Procmon, Procexp, APATEDNS and FAKENET for network activity analysis.
    - Use the Procmon tool to describe any interactions with the following activities:
        - Using Procmon in the short amount of time that I had to capture information there was no registry activity found in relation to Lecture8.exe, this is not unusual the malware was shown to be deleting over a 1000 registry keys rather than having any indication of creating registry keys. It was extremely hard to conduct throughout analysis using any tool especially Procmon as the ransomware would forcibly close any application I had open after a few minutes of it running.

- Using process manager, I was thankfully able to also capture file system activity in relation to Lecture8.exe before the malware forcibly closed out of any application, I had open to run its ransomware service on the system. Lecture8.exe had several file system operations such as QueryNameInfo, ReadFile, CreateFile, WriteFile, SetBasicInformation, CloseFile, SetSecurity File with several results being success or invalid parameters.

- 

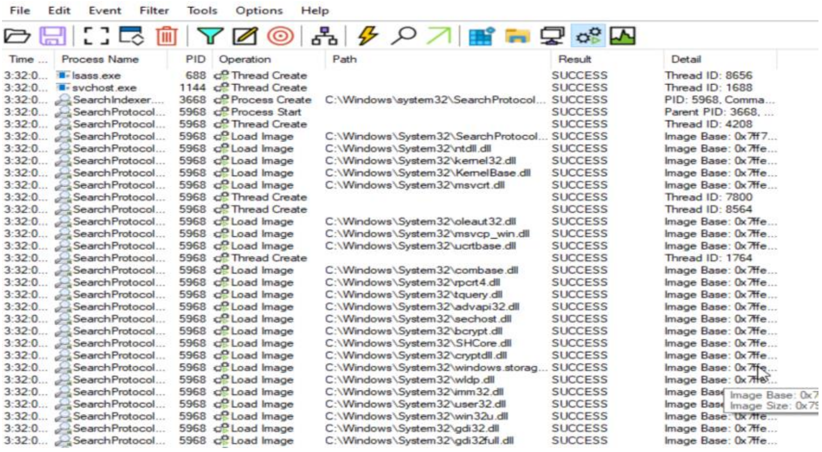
Time ...	Process Name	PID	Operation	Path	Result	Detail
3:32:0...	Lecture8.exe	8176	QueryNameInfo...	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Name: \Users\vali...
3:32:0...	Lecture8.exe	8176	ReadFile	C:\Users\valid\AppData\Roaming\Hex-...	END OF FILE	Offset: 131,072, Le...
3:32:0...	Lecture8.exe	8176	CreateFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Desired Access: R...
3:32:0...	Lecture8.exe	8176	QueryRemotePr...	C:\Users\valid\AppData\Roaming\Hex-...	INVALID PARAME...	
3:32:0...	Lecture8.exe	8176	WriteFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Offset: -1, Length: ...
3:32:0...	Lecture8.exe	8176	QuerySecurityFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Information: Owner...
3:32:0...	Lecture8.exe	8176	CloseFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	
3:32:0...	Lecture8.exe	8176	QueryRemotePr...	C:\Users\valid\AppData\Roaming\Hex-...	INVALID PARAME...	
3:32:0...	Lecture8.exe	8176	QuerySecurityFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Information: Owner...
3:32:0...	Lecture8.exe	8176	CloseFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	
3:32:0...	Lecture8.exe	8176	SetSecurityFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Information: Owner...
3:32:0...	Lecture8.exe	8176	CloseFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	
3:32:0...	Lecture8.exe	8176	CreateFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Desired Access: W...
3:32:0...	Lecture8.exe	8176	SetBasicInform...	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	CreationTime: 0, L...
3:32:0...	Lecture8.exe	8176	CloseFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	
3:32:0...	Lecture8.exe	8176	CreateFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Desired Access: G...
3:32:0...	Lecture8.exe	8176	CloseFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	
3:32:0...	Lecture8.exe	8176	CreateFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Desired Access: W...
3:32:0...	Lecture8.exe	8176	SetBasicInform...	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	CreationTime: 0, L...
3:32:0...	Lecture8.exe	8176	CloseFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	
3:32:0...	Lecture8.exe	8176	CreateFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Desired Access: G...
3:32:0...	Lecture8.exe	8176	QueryStandardI...	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	AllocationSize: 488...
3:32:0...	Lecture8.exe	8176	ReadFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Offset: 356, Length...
3:32:0...	Lecture8.exe	8176	ReadFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Offset: 0, Length: 4...
3:32:0...	Lecture8.exe	8176	CloseFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	
3:32:0...	Lecture8.exe	8176	CreateFile	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Desired Access: R...
3:32:0...	Lecture8.exe	8176	QueryAttributeT...	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	Attributes: N, Repa...
3:32:0...	Lecture8.exe	8176	QueryBasicInfor...	C:\Users\valid\AppData\Roaming\Hex-...	SUCCESS	CreationTime: 1/21...
3:32:0	Lecture8.exe	8176	CreateFile	C:\Users\valid\AppData\Roaming\Hex-	SUCCESS	Desired Access: W

- Process manager was not able to pick up on any network activity in relation to Lecture8.exe at all.



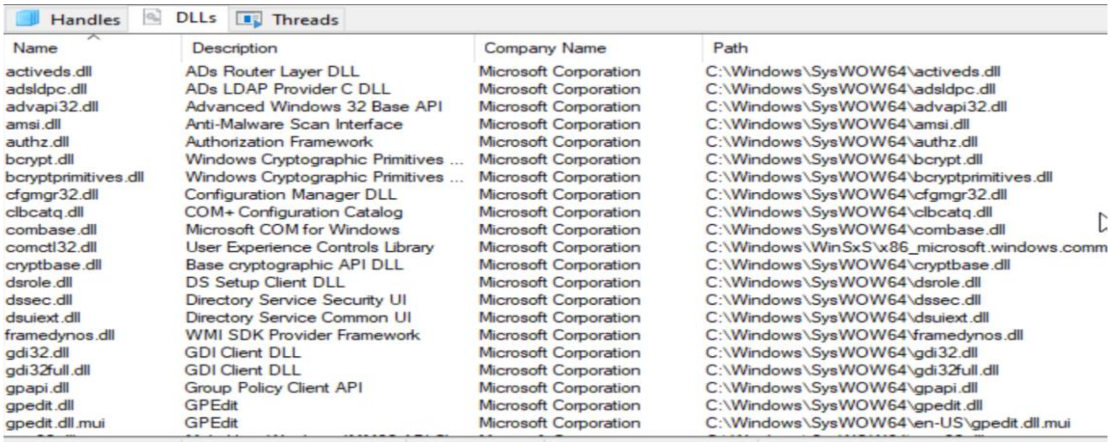
-

- Procmon was not able to capture and process and thread activity related to Lecture8.exe, I also did not have enough time to do analysis before the ransomware executed and closed out Procmon but there were no apparent ties to Lecture8.exe that I could identify in the short period of time.

- 

Time ...	Process Name	PID	Operation	Path	Result	Detail
3:32:0...	lsass.exe	688	Thread Create		SUCCESS	Thread ID: 8656
3:32:0...	svchost.exe	1144	Thread Create		SUCCESS	Thread ID: 1688
3:32:0...	SearchIndexer....	3668	Process Create	C:\Windows\system32\SearchProtocol...	SUCCESS	PID: 5968, Comma...
3:32:0...	SearchProtocol...	5968	Process Start		SUCCESS	Parent PID: 3668, ...
3:32:0...	SearchProtocol...	5968	Thread Create		SUCCESS	Thread ID: 4208
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\SearchProtocol...	SUCCESS	Image Base: 0x7ff7...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Thread Create		SUCCESS	Thread ID: 7800
3:32:0...	SearchProtocol...	5968	Thread Create		SUCCESS	Thread ID: 8564
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\oleaut32.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\msvcp_win.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Thread Create		SUCCESS	Thread ID: 1764
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\combase.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\tquery.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\bcrypt.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\SHCore.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\cryptdll.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\windows.storag...	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\wldp.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\imm32.dll	SUCCESS	Image Bas
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Bas
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\win32u.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ffe...
3:32:0...	SearchProtocol...	5968	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ffe...

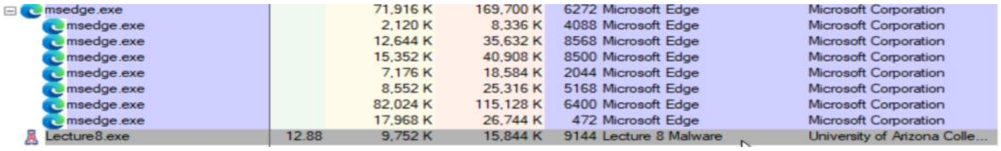
- Use the Process Explorer tool and identify any:
  - I did not have long to identify libraries used by Lecture8.exe before the malware closed out Procexp forcefully but I did locate some very interesting libraries that I could immediately identify such as amsi.dll which is for Anti-Malware Scan Interface, cryptbase.dll which is used for Base cryptographic API DLL, comctl32.dll for User Experience Controls Library which could indicate some sort of command and control setup by the malware itself.

- 

Handles | DLLs | Threads

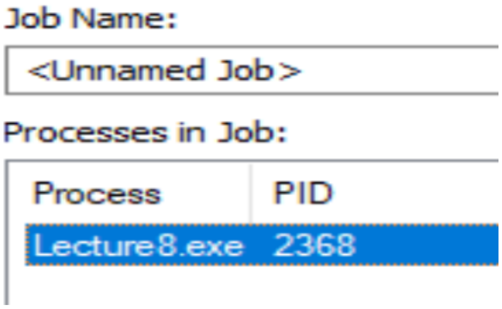
Name	Description	Company Name	Path
activeds.dll	ADs Router Layer DLL	Microsoft Corporation	C:\Windows\SysWOW64\activeds.dll
adsldpc.dll	ADs LDAP Provider C DLL	Microsoft Corporation	C:\Windows\SysWOW64\adsldpc.dll
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\SysWOW64\advapi32.dll
amsi.dll	Anti-Malware Scan Interface	Microsoft Corporation	C:\Windows\SysWOW64\amsi.dll
authz.dll	Authorization Framework	Microsoft Corporation	C:\Windows\SysWOW64\authz.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\SysWOW64\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\SysWOW64\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\SysWOW64\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\SysWOW64\clbcatq.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\SysWOW64\combase.dll
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\WinSxS\x86_microsoft.windows.comm
cryptbase.dll	Base cryptographic API DLL	Microsoft Corporation	C:\Windows\SysWOW64\cryptbase.dll
dsrole.dll	DS Setup Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\dsrole.dll
dssec.dll	Directory Service Security UI	Microsoft Corporation	C:\Windows\SysWOW64\dssec.dll
dsuiext.dll	Directory Service Common UI	Microsoft Corporation	C:\Windows\SysWOW64\dsuiext.dll
framedynos.dll	WMI SDK Provider Framework	Microsoft Corporation	C:\Windows\SysWOW64\framedynos.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\gdi32.dll
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\SysWOW64\gdi32full.dll
gpapi.dll	Group Policy Client API	Microsoft Corporation	C:\Windows\SysWOW64\gpapi.dll
gpedit.dll	GPEdit	Microsoft Corporation	C:\Windows\SysWOW64\gpedit.dll
gpedit.dll.mui	GPEdit	Microsoft Corporation	C:\Windows\SysWOW64\en-US\gpedit.dll.mui

- The parent process that was identified was msedge.exe with the child process hiding underneath as Lecture8.exe.

- 

msedge.exe		71,916 K	169,700 K	6272	Microsoft Edge	Microsoft Corporation
msedge.exe		2,120 K	8,336 K	4088	Microsoft Edge	Microsoft Corporation
msedge.exe		12,644 K	35,632 K	8568	Microsoft Edge	Microsoft Corporation
msedge.exe		15,352 K	40,908 K	8500	Microsoft Edge	Microsoft Corporation
msedge.exe		7,176 K	18,584 K	2044	Microsoft Edge	Microsoft Corporation
msedge.exe		8,552 K	25,316 K	5168	Microsoft Edge	Microsoft Corporation
msedge.exe		82,024 K	115,128 K	6400	Microsoft Edge	Microsoft Corporation
msedge.exe		17,968 K	26,744 K	472	Microsoft Edge	Microsoft Corporation
Lecture8.exe	12.88	9,752 K	15,844 K	9144	Lecture 8 Malware	University of Arizona Colle...

- The only PID identifiable for Lecture8.exe was 2368 with no additional process names attached that could be identified in the short period of time I had for analysis.

- 

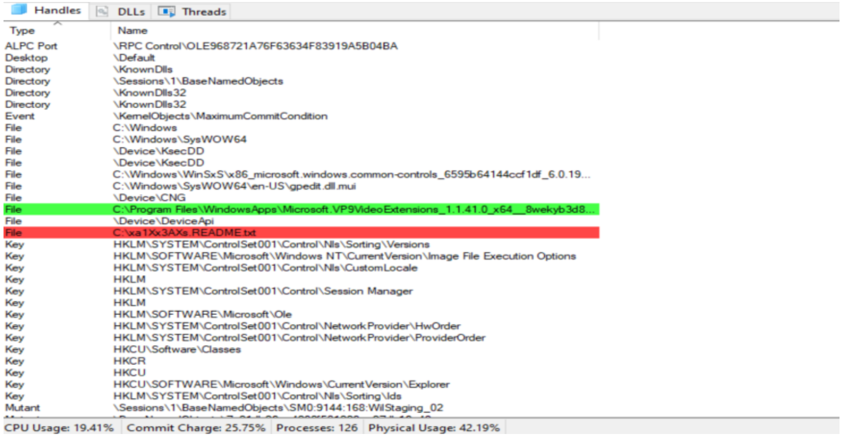
Job Name:

<Unnamed Job>

Processes in Job:

Process	PID
Lecture8.exe	2368

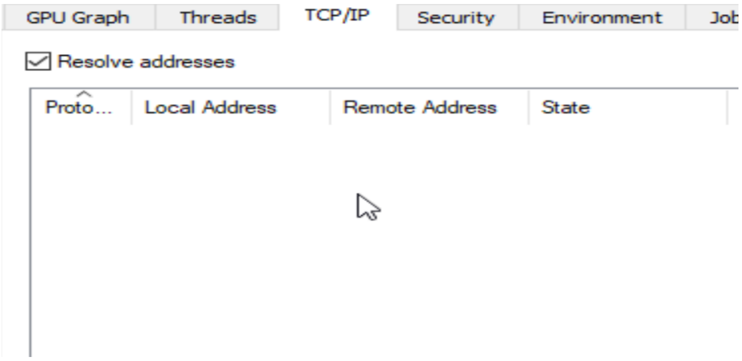
- Again with limited amounts of time screen grab and conduct analysis I found some very useful handles such as several files in relation to Windows system, Device/KsecDD, Microsoft windows common controls, VP9 Video Extensions, Device API, and a README.txt file associated with the ransomware popup that contains instructions for the victim. There were also several key’s in relation to HKLM system and software Windows and Control sets for Image file execution options or Session managers.

- 

Type	Name
ALPC Port	\RPC Control\OLE968721A76F63634F83919A5B04BA
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Directory	\KnownDlls32
Directory	\KnownDlls32
Event	\KernelObjects\MaximumCommitCondition
File	C:\Windows
File	C:\Windows\SysWOW64
File	\Device\KsecDD
File	\Device\KsecDD
File	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19...
File	C:\Windows\SysWOW64\en-US\gpedit.dll.mui
File	\Device\CNG
File	C:\Program Files\WindowsApps\Microsoft.VP9VideoExtensions_1.1.41.0_x64__8wekyb3d8...
File	\Device\DeviceApi
File	C:\xa1Xx3AXs.README.txt
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKLM\SYSTEM\ControlSet001\Control\NetworkProvider\HwOrder
Key	HKLM\SYSTEM\ControlSet001\Control\NetworkProvider\ProviderOrder
Key	HKCU\Software\Classes
Key	HKCR
Key	HKCU
Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Mutant	\Sessions\1\BaseNamedObjects\SM0:9144:168:WilStaging_02

CPU Usage: 19.41% | Commit Charge: 25.75% | Processes: 126 | Physical Usage: 42.19%

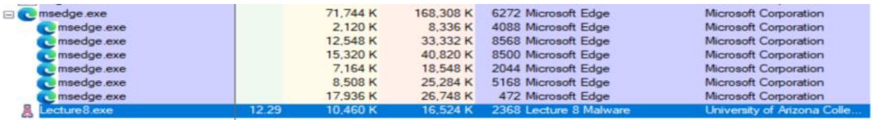
- Using Procexp there were no identifiable TCP/IP activities that were identifiable by the tool for Lecture8.exe.

- 

☑ Resolve addresses

Proto...	Local Address	Remote Address	State

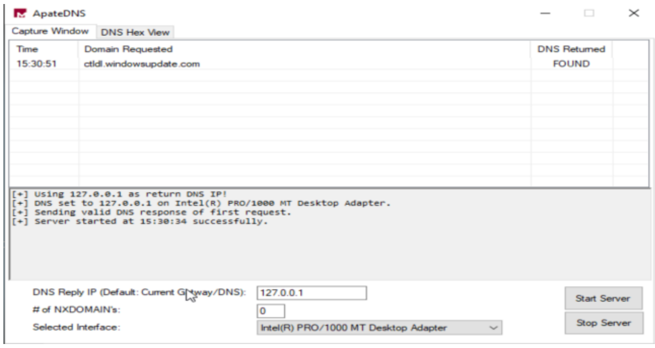
- There were no process replacements that I could easily verify, as the only process that I had time to identify was Lecture8.exe was a child process within msfedge.exe.

- 

msedge.exe		71,744 K	168,308 K	6272	Microsoft Edge	Microsoft Corporation
msedge.exe		2,120 K	8,336 K	4088	Microsoft Edge	Microsoft Corporation
msedge.exe		12,548 K	33,332 K	8568	Microsoft Edge	Microsoft Corporation
msedge.exe		15,320 K	40,820 K	8500	Microsoft Edge	Microsoft Corporation
msedge.exe		7,164 K	18,548 K	2044	Microsoft Edge	Microsoft Corporation
msedge.exe		8,508 K	25,284 K	5168	Microsoft Edge	Microsoft Corporation
msedge.exe		17,936 K	26,748 K	472	Microsoft Edge	Microsoft Corporation
Lecture8.exe	12.29	10,460 K	16,524 K	2368	Lecture 8 Malware	University of Arizona Colle...

- Identify Network activity.

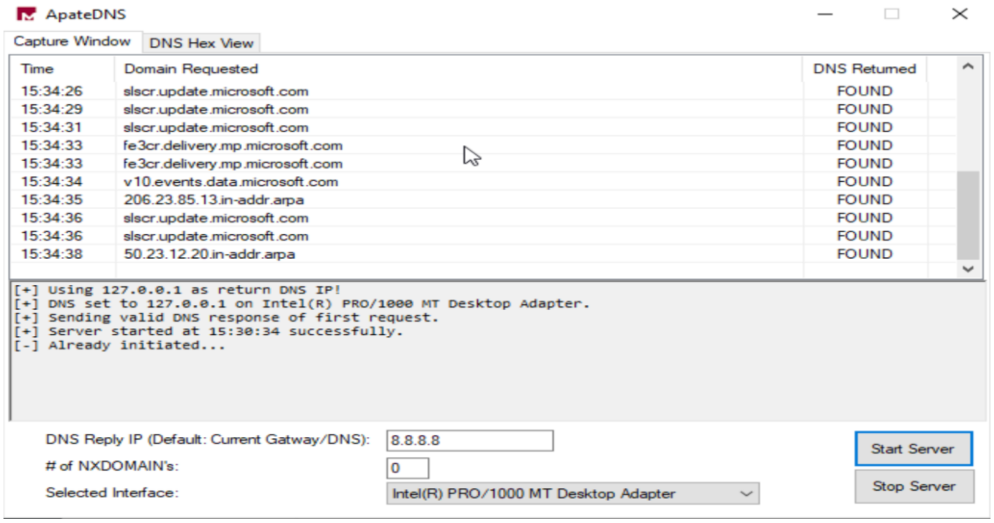
  - Using APATEDNS there was only domain request that was populating after executing Lecture8.exe which was ctldl.windowsupdate.com for the limited time I was able to leave APATEDNS running before it was also forcibly closed by the malware. The domain name requested is either legitimate or a form of obfuscation used by the executable program to make network analysis extremely difficult by making the process name seem like a regular windows update domain request. But then I switched the DNS reply IP to 8.8.8.8 and found several new domain requests to two IP's being 206.23.85.13 and 50.23.12.20 as well as several slcr.update.microsoft.com and fe3cr.delivery.mp.microsoft.com.

  - 

Time	Domain Requested	DNS Returned
15:30:51	ctldl.windowsupdate.com	FOUND

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 15:30:34 successfully.
```

DNS Reply IP (Default: Current Gateway/DNS): 127.0.0.1
# of NXDOMAIN's: 0
Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter

- 

Time	Domain Requested	DNS Returned
15:34:26	slscr.update.microsoft.com	FOUND
15:34:29	slscr.update.microsoft.com	FOUND
15:34:31	slscr.update.microsoft.com	FOUND
15:34:33	fe3cr.delivery.mp.microsoft.com	FOUND
15:34:33	fe3cr.delivery.mp.microsoft.com	FOUND
15:34:34	v10.events.data.microsoft.com	FOUND
15:34:35	206.23.85.13.in-addr.arpa	FOUND
15:34:36	slscr.update.microsoft.com	FOUND
15:34:36	slscr.update.microsoft.com	FOUND
15:34:38	50.23.12.20.in-addr.arpa	FOUND

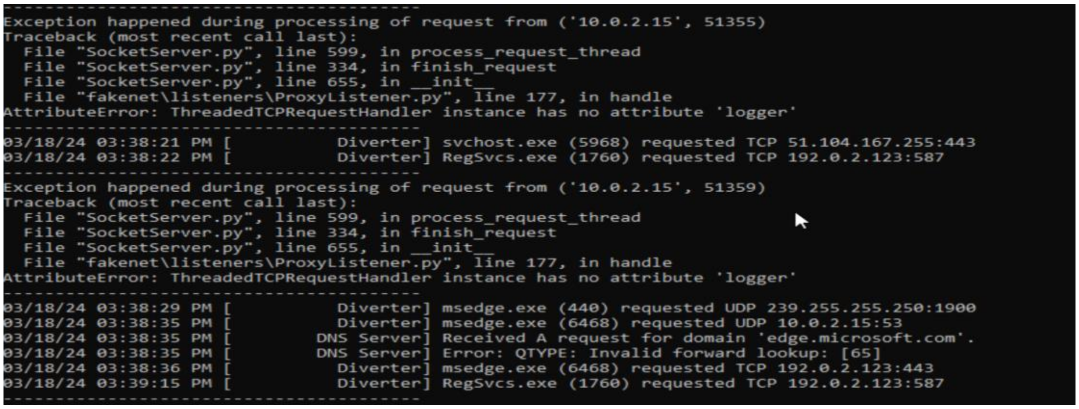
```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Desktop Adapter.
[+] Sending valid DNS response of first request.
[+] Server started at 15:30:34 successfully.
[-] Already initiated...
```

DNS Reply IP (Default: Current Gatway/DNS): 8.8.8.8

# of NXDOMAIN's: 0

Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter

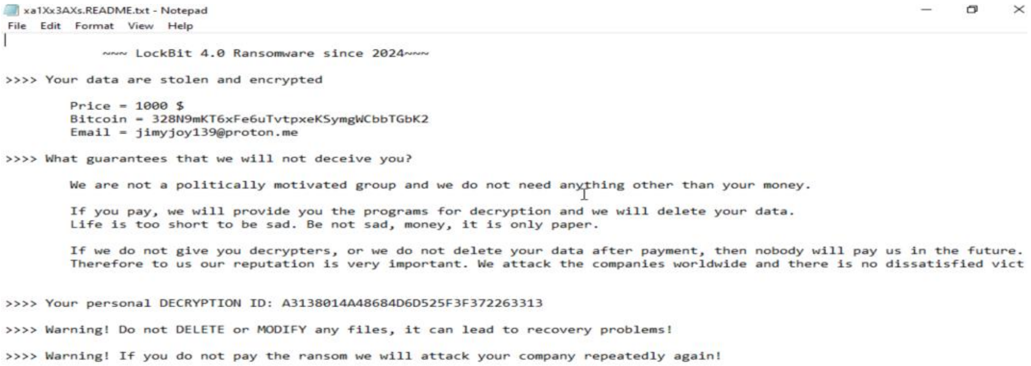
- Using FakeNet I was able to identify some suspicious network activity in relation to a diverter call to svchost.exe and RegSvcs.exe processing which is not usually used for making network requests so it is unusual. The process could be an extremely stealth way for the malware to have network communication to contact command control but it’s extremely hard to point the other activity to the malware as those were already there.

- 

```
----------------------------------------
Exception happened during processing of request from ('10.0.2.15', 51355)
Traceback (most recent call last):
  File "SocketServer.py", line 599, in process_request_thread
  File "SocketServer.py", line 334, in finish_request
  File "SocketServer.py", line 655, in __init__
  File "fakenet\listeners\ProxyListener.py", line 177, in handle
AttributeError: ThreadedTCPRequestHandler instance has no attribute 'logger'
----------------------------------------
03/18/24 03:38:21 PM [           Diverter] svchost.exe (5968) requested TCP 51.104.167.255:443
03/18/24 03:38:22 PM [           Diverter] RegSvcs.exe (1760) requested TCP 192.0.2.123:587
----------------------------------------
Exception happened during processing of request from ('10.0.2.15', 51359)
Traceback (most recent call last):
  File "SocketServer.py", line 599, in process_request_thread
  File "SocketServer.py", line 334, in finish_request
  File "SocketServer.py", line 655, in __init__
  File "fakenet\listeners\ProxyListener.py", line 177, in handle
AttributeError: ThreadedTCPRequestHandler instance has no attribute 'logger'
----------------------------------------
03/18/24 03:38:29 PM [           Diverter] msedge.exe (440) requested UDP 239.255.255.250:1900
03/18/24 03:38:35 PM [           Diverter] msedge.exe (6468) requested UDP 10.0.2.15:53
03/18/24 03:38:35 PM [         DNS Server] Received A request for domain 'edge.microsoft.com'.
03/18/24 03:38:35 PM [         DNS Server] Error: QTYPE: Invalid forward lookup: [65]
03/18/24 03:38:36 PM [           Diverter] msedge.exe (6468) requested TCP 192.0.2.123:443
03/18/24 03:39:15 PM [           Diverter] RegSvcs.exe (1760) requested TCP 192.0.2.123:587
----------------------------------------
```

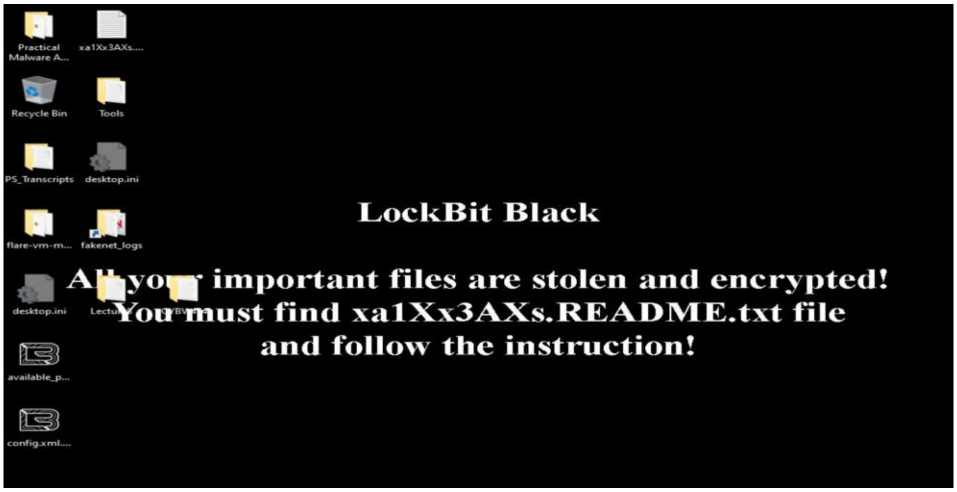
- **Aftermath**

- When I initially ran Lecture8.exe almost instantly there are 2 text files and 1 xml file that populate on the system, one for available_packages.txt, config.xml and a README.txt file these appear nearly in every directory and even change the logos of several analysis tool applications that I interacted with before opening. It takes a few minutes on average before there is a visual queue that the system has been infected with ransomware stating “LockBit Black”, “All your important files are stolen and encrypted, you must find README.txt file and follow the instructions. The README.txt file itself is named LockBit 4.0 Ransomware and the price to release is $1000 in the form of Bitcon with a email present. The file further claims it is not for political reasons but is attacking companies worldwide and says if it is not paid the attackers will continue to attack repeatedly as a threat. They claim that the company’s reputation is on the line and that money is only paper.



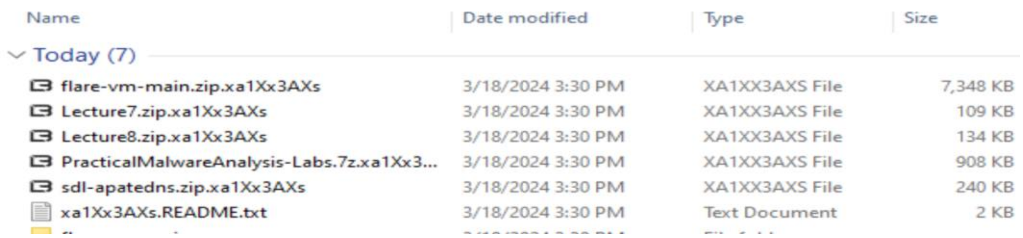
```
             ~~~ LockBit 4.0 Ransomware since 2024~~~

>>>> Your data are stolen and encrypted

        Price = 1000 $
        Bitcoin = 328N9mKT6xFe6uTvtpxeKSymgWCbbTGbK2
        Email = jimyjoy139@proton.me

>>>> What guarantees that we will not deceive you?

        We are not a politically motivated group and we do not need anything other than your money.

        If you pay, we will provide you the programs for decryption and we will delete your data.
        Life is too short to be sad. Be not sad, money, it is only paper.

        If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
        Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied vict


>>>> Your personal DECRYPTION ID: A3138014A48684D6D525F3F372263313

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!
```

-

  - 

    LockBit Black

    All your important files are stolen and encrypted!
    You must find xa1Xx3AXs.README.txt file
    and follow the instruction!

  - 

    Today (7)

Name	Date modified	Type	Size
flare-vm-main.zip.xa1Xx3AXs	3/18/2024 3:30 PM	XA1XX3AXS File	7,348 KB
Lecture7.zip.xa1Xx3AXs	3/18/2024 3:30 PM	XA1XX3AXS File	109 KB
Lecture8.zip.xa1Xx3AXs	3/18/2024 3:30 PM	XA1XX3AXS File	134 KB
PracticalMalwareAnalysis-Labs.7z.xa1Xx3...	3/18/2024 3:30 PM	XA1XX3AXS File	908 KB
sdl-apatedns.zip.xa1Xx3AXs	3/18/2024 3:30 PM	XA1XX3AXS File	240 KB
xa1Xx3AXs.README.txt	3/18/2024 3:30 PM	Text Document	2 KB

- **Impact**

- The impact on a home user can be extremely severe even though this ransomware is intended for “Companies”, home users on average are not advanced in cybersecurity measures and practices and may not have regular backups of their data so the encryption of personal files by Lecture8.exe ransomware can lead to loss of very important documents, finances and other’s due to the encryption of the files and the nature of the attack. Business users would face significant operational and financial reputational damage from this LockBit ransomware, the locking of critical files can completely put a halt to business operations and lead to loss of customer trust and result in substantial financial losses. Considering how sophisticated the ransomware is and it’s ability to evade detection makes it extremely dangerous, especially to government users in this case the implications of a ransomware attack would cause disruption to public services, theft of sensitive documents and data, and impact national security at the highest level if the files are also stolen. The ability for the ransomware to delete registry keys and files can undermine government infrastructure and integrity and lead to a loss of public trust.

- **Mitigation**
  - To mitigate a dangerous piece of malware such as Lecture8.exe ransomware, users need to deploy and maintain advanced endpoint protection platforms with advanced behavioral analysis to detect and respond to unknown threats or signatures. For users across the board software needs to be updated, especially operating systems and antivirus solutions and ensure they are regularly patched and checked for vulnerabilities that could be used for exploitation by ransomware such as this. Users across the board can again implement a backup strategy that would include regular backups of critical data and have backups stored offline or in a secure cloud environment to prevent them from being encrypted by ransomware. Businesses and Governments need to have an incident response plan in place to ensure rapid and effective responses in the event of an infection by ransomware such as this. Finally there needs to be user education, conducting cybersecurity awareness training for all users to recognize signs of phising, suspicious links and the importance of not downloading files from untrusted sources is critical.
- **Evaluation**
  - My evaluation of Lecture8.exe ransomware is based on my static and dynamic analysis alike, the malware showcases advanced evasion tactics, the ability to

detect and react to analysis attempts by locking down the analysis environment forcibly and it’s ability to mutate and create file history data indicates a sophisticated piece of malware meant to hinder tracking and analysis. This level of sophistication along with it’s ability too delete registry keys and system files shows the design of this malware to maintain long term access to the victim’s system while avoiding analysis detection. With a significant amount of security vendors on VirusTotal identifying Lecture8.exe as malicious and specifically ransomware belonging to Lockbit/Blackmatter family shows the consensus of the cybersecurity community’s stance on this executable file. The use of GUI interface, suspicious strings and renaming the executable to ‘WelcomeBack2024’.exe are signs of a dangerous file. Dynamic analysis revealed the ransomware’s instant response to execution with file creation and visual queues of infection, the aggressive nature reduces the time that a user has for mitigation and increases the chance for successful encryption by the file. The README.txt files presence in multiple directories and alterations of logos demonstrates the malware’s capability to interact with user files aggressively and system interface.

Finally, I would like you to add your closing thoughts and reflect on this piece of malware. What did you find, what did you observe, and what did you experience during this evaluation?

- **Reflection**
    - Throughout my analysis and interaction with Lecture8.exe malware I encountered a highly sophisticated ransomware that consistently challenged traditional methods of analysis. The malware’s ability to detect and evade analysis methods

was not only technically interesting but was a reminder of the evolving nature of cybersecurity methods. The deceptive use of tactics to disguise it's process to leverage legitimate sounding domain names for command and control operations and it's intentions to delete registry keys, values and modify the integrity of existing data files itself made this extremely dangerous and difficult to deal with. Its aggressive countermeasures was extremely frustrating at first as it kept forcing my hand to lean to alternative forms of analysis or simply not conduct the type of analysis I wanted to with certain tools such as IDA Pro. The sophistication of this ransomware made it extremely hard as a cybersecurity analyst to conduct through analysis without being made aware of its highly advanced evasion techniques, making this an extremely dangerous piece of malware.