Section 1: Static Analysis

I. The malware file used is “Lab20-01.exe”.

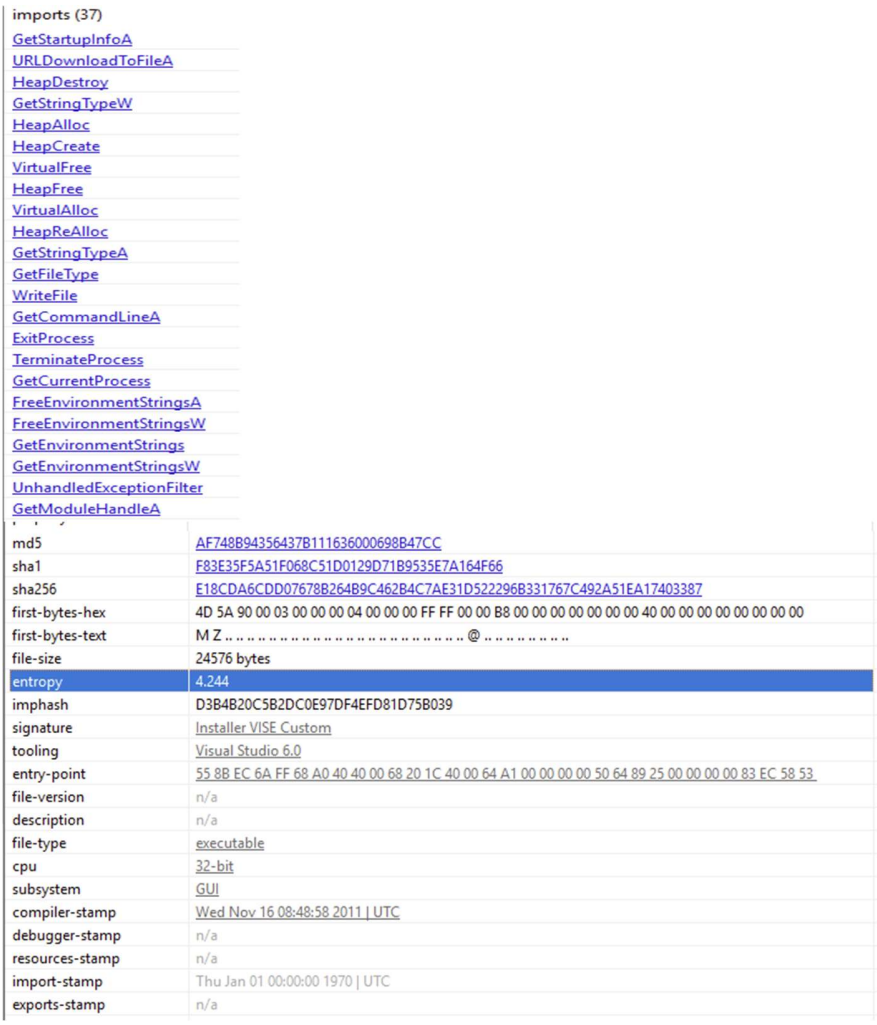
II. Below is a table containing the extracted strings

!This program cannot be run in DOS mode. Rich .text `.rdata @.data runtime error TLOSS error SING error DOMAIN error R6028 - unable to initialize heap R6027 - not enough space for lowio initialization R6026 - not enough space for stdio initialization R6025 - pure virtual function call R6024 - not enough space for _onexit/atexit table R6019 - unable to open console device R6018 - unexpected heap error R6017 - unexpected multithread lock error R6016 - not enough space for thread data abnormal program termination R6009 - not enough space for environment R6008 - not enough space for arguments R6002 - floating point not loaded Microsoft Visual C++ Runtime Library Runtime Error! Program: ... <program name unknown> GetLastActivePopup GetActiveWindow MessageBoxA user32.dll	URLDownloadToFileA urlmon.dll GetModuleHandleA GetStartupInfoA GetCommandLineA GetVersion ExitProcess HeapAlloc TerminateProcess GetCurrentProcess UnhandledExceptionFilter GetModuleFileNameA FreeEnvironmentStringsA FreeEnvironmentStringsW WideCharToMultiByte GetEnvironmentStrings GetEnvironmentStringsW SetHandleCount GetStdHandle GetFileType HeapDestroy HeapCreate VirtualFree HeapFree RtlUnwind WriteFile VirtualAlloc HeapReAlloc GetCPInfo GetACP GetOEMCP GetProcAddress LoadLibraryA MultiByteToWideChar LCMapStringA LCMapStringW GetStringTypeA GetStringTypeW KERNEL32.dll http://www.practicalmalwareanalysis.com/cpp.html empdownload.exe

III. In the strings, there are many points of interest that should be noted. First, The domain "http://www.practicalmalwareanalysis.com/cpp.html" seems to be a C++ payload that the malware intends to download, we see more evidence of downloading with the "empdownload.exe" file and the *URLDownloadToFileA* import.

Second, the virus intends to Write Files, and Terminate itself through the imports (*WriteFile*, *TerminateProcess, GetModuleFileName,* and *GetCurrentProcess*).

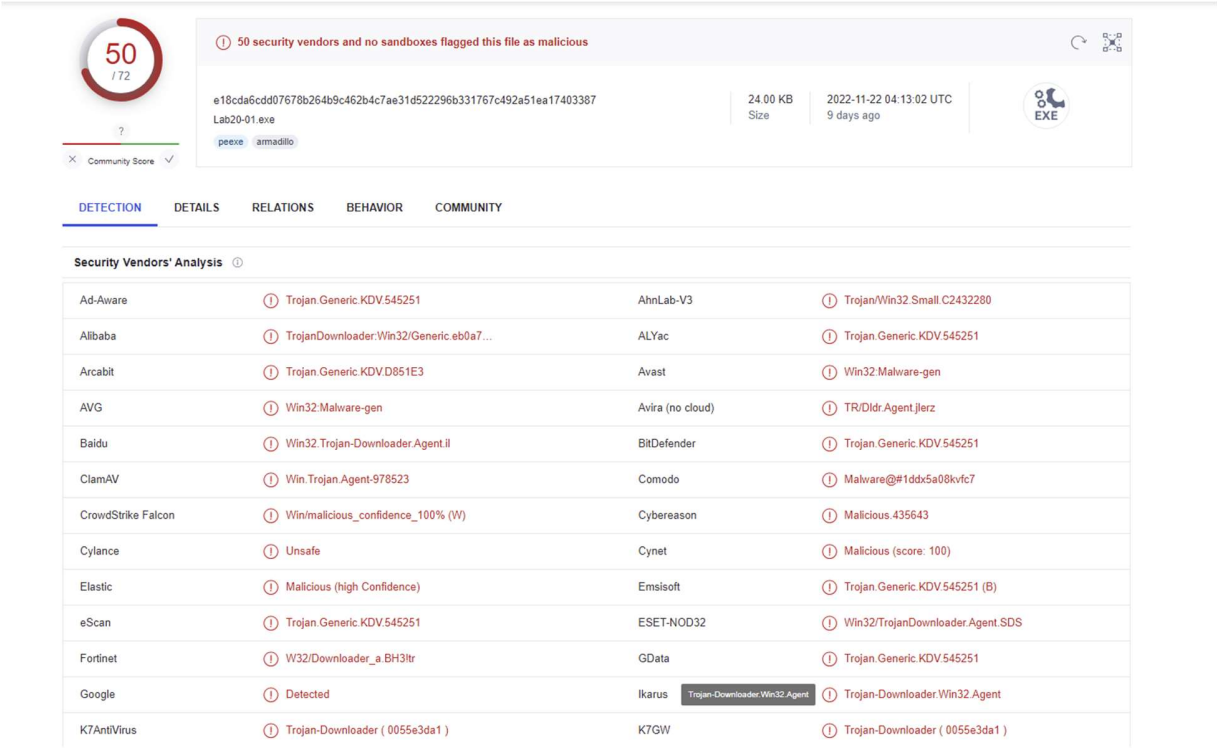
IV. Lab20-01.exe is not packed for two reasons. The first is that the number of imports is high (37 imports for this file to be exact), and the second is that the entropy value is low (4.244). Below is evidence from PEstudio:



imports (37)
GetStartupInfoA
URLDownloadToFileA
HeapDestroy
GetStringTypeW
HeapAlloc
HeapCreate
VirtualFree
HeapFree
VirtualAlloc
HeapReAlloc
GetStringTypeA
GetFileType
WriteFile
GetCommandLineA
ExitProcess
TerminateProcess
GetCurrentProcess
FreeEnvironmentStringsA
FreeEnvironmentStringsW
GetEnvironmentStrings
GetEnvironmentStringsW
UnhandledExceptionFilter
GetModuleHandleA

md5	AF748B94356437B111636000698B47CC
sha1	F83E35F5A51F068C51D0129D71B9535E7A164F66
sha256	E18CDA6CDD07678B264B9C462B4C7AE31D522296B331767C492A51EA17403387
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	24576 bytes
entropy	4.244
imphash	D3B4B20C5B2DC0E97DF4EFD81D75B039
signature	Installer VISE Custom
tooling	Visual Studio 6.0
entry-point	55 8B EC 6A FF 68 A0 40 40 00 68 20 1C 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 58 53
file-version	n/a
description	n/a
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	Wed Nov 16 08:48:58 2011 | UTC
debugger-stamp	n/a
resources-stamp	n/a
import-stamp	Thu Jan 01 00:00:00 1970 | UTC
exports-stamp	n/a

Section 2: Static Analysis with PEstudio



VirusTotal has 50/72 vendors that recognized the file as a Trojan, with some specifying it to be a Trojan-Downloader.

I. The malware is malicious according to the highlighted VirusTotal vendors:

Bkav	clean	22.11.2022	17
Lionic	Trojan.Win32.Generic.4!c	22.11.2022	17
Elastic	malicious (high confidence)	17.11.2022	22
MicroWorld-eScan	Trojan.Generic.KDV.545251	22.11.2022	17
CMC	clean	22.11.2022	17
CAT-QuickHeal	clean	21.11.2022	18
McAfee	RDN/Generic Downloader.x	23.10.2022	47
Cylance	Unsafe	22.11.2022	17
VIPRE	Trojan.Generic.KDV.545251	21.11.2022	18
Sangfor	Trojan.Win32.Agent.SDS	10.11.2022	29
K7AntiVirus	Trojan-Downloader (0055e3da1)	22.11.2022	17
Alibaba	TrojanDownloader:Win32/Generic.eb0a73c3	27.05.2019	1292
K7GW	Trojan-Downloader (0055e3da1)	21.11.2022	18
Cybereason	malicious.435643	30.03.2021	619
Baidu	Win32.Trojan-Downloader.Agent.il	18.03.2019	1362
VirIT	Trojan.Win32.Generic.ATFX	21.11.2022	18
Cyren	clean	22.11.2022	17
Symantec	ML.Attribute.HighConfidence	21.11.2022	18
tehtris	clean	22.11.2022	17
ESET-NOD32	Win32/TrojanDownloader.Agent.SDS	22.11.2022	17
APEX	Malicious	19.11.2022	20

II. The file signatures for Lab20-01.exe are screenshotted below:

md5	AF748B94356437B111636000698B47CC
sha1	F83E35F5A51F068C51D0129D71B9535E7A164F66
sha256	E18CDA6CDD07678B264B9C462B4C7AE31D522296B331767C492A51EA17403387

III. This virus has been around for a while, according to VirusTotal, it has been spotted by Baidu as early as March 2019:

Cybereason	malicious.435643	30.03.2021	619
Baidu	Win32.Trojan-Downloader.Agent.il	18.03.2019	1362
VirIT	Trojan.Win32.Generic.ATFX	21.11.2022	18
Cyren	clean	22.11.2022	17

IV. The malware file is 32-bit. It is also an executable:

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4EC378FA	Wed Nov 16 08:48:58 2011 | UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel-386**
sections	0x0003	3
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

V. Highlighted in blue are the API functions that we should keep an eye on:

imports (37)	flag (5)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (8)	type (1)	ordinal (0)	library (2)
GetStartupInfoA	-	0x00004512	0x00004512	336 (0x0150)	reckoning	implicit	-	kernel32.dll
URLDownloadToFileA	x	0x000044DC	0x000044DC	62 (0x003E)	network	implicit	-	urlmon.dll
HeapDestroy	-	0x00004664	0x00004664	413 (0x019D)	memory	implicit	-	kernel32.dll
GetStringTypeW	-	0x0000475C	0x0000475C	342 (0x0156)	memory	implicit	-	kernel32.dll
HeapAlloc	-	0x00004552	0x00004552	409 (0x0199)	memory	implicit	-	kernel32.dll
HeapCreate	-	0x00004672	0x00004672	411 (0x019B)	memory	implicit	-	kernel32.dll
VirtualFree	-	0x00004680	0x00004680	703 (0x02BF)	memory	implicit	-	kernel32.dll
HeapFree	-	0x0000468E	0x0000468E	415 (0x019F)	memory	implicit	-	kernel32.dll
VirtualAlloc	-	0x000046B2	0x000046B2	699 (0x02BB)	memory	implicit	-	kernel32.dll
HeapReAlloc	-	0x000046C2	0x000046C2	418 (0x01A2)	memory	implicit	-	kernel32.dll
GetStringTypeA	-	0x0000474A	0x0000474A	339 (0x0153)	memory	implicit	-	kernel32.dll
GetFileType	-	0x00004656	0x00004656	277 (0x0115)	file	implicit	-	kernel32.dll
WriteFile	x	0x000046A6	0x000046A6	735 (0x02DF)	file	implicit	-	kernel32.dll
GetCommandLineA	-	0x00004524	0x00004524	202 (0x00CA)	execution	implicit	-	kernel32.dll
ExitProcess	-	0x00004544	0x00004544	125 (0x007D)	execution	implicit	-	kernel32.dll
TerminateProcess	x	0x0000455E	0x0000455E	670 (0x029E)	execution	implicit	-	kernel32.dll
GetCurrentProcess	-	0x00004572	0x00004572	247 (0x00F7)	execution	implicit	-	kernel32.dll
FreeEnvironmentStringsA	-	0x000045B8	0x000045B8	178 (0x00B2)	execution	implicit	-	kernel32.dll
FreeEnvironmentStringsW	-	0x000045D2	0x000045D2	179 (0x00B3)	execution	implicit	-	kernel32.dll
GetEnvironmentStrings	x	0x00004602	0x00004602	262 (0x0106)	execution	implicit	-	kernel32.dll
GetEnvironmentStringsW	x	0x0000461A	0x0000461A	264 (0x0108)	execution	implicit	-	kernel32.dll
UnhandledExceptionFilter	-	0x00004586	0x00004586	685 (0x02AD)	exception	implicit	-	kernel32.dll
GetModuleHandleA	-	0x000044FE	0x000044FE	294 (0x0126)	dynamic-library	implicit	-	kernel32.dll
GetModuleFileNameA	-	0x000045A2	0x000045A2	292 (0x0124)	dynamic-library	implicit	-	kernel32.dll
GetProcAddress	-	0x000046F2	0x000046F2	318 (0x013E)	dynamic-library	implicit	-	kernel32.dll
LoadLibraryA	-	0x00004704	0x00004704	450 (0x01C2)	dynamic-library	implicit	-	kernel32.dll
GetStdHandle	-	0x00004646	0x00004646	338 (0x0152)	console	implicit	-	kernel32.dll
GetVersion	-	0x00004536	0x00004536	372 (0x0174)	-	implicit	-	kernel32.dll
WideCharToMultiByte	-	0x000045EC	0x000045EC	722 (0x02D2)	-	implicit	-	kernel32.dll
SetHandleCount	-	0x00004634	0x00004634	621 (0x026D)	-	implicit	-	kernel32.dll
RtlUnwind	-	0x0000469A	0x0000469A	559 (0x022F)	-	implicit	-	kernel32.dll
GetCPInfo	-	0x000046D0	0x000046D0	191 (0x00BF)	-	implicit	-	kernel32.dll
GetACP	-	0x000046DC	0x000046DC	185 (0x00B9)	-	implicit	-	kernel32.dll
GetOEMCP	-	0x000046E6	0x000046E6	305 (0x0131)	-	implicit	-	kernel32.dll
MultiByteToWideChar	-	0x00004714	0x00004714	484 (0x01E4)	-	implicit	-	kernel32.dll
LCMapStringA	-	0x0000472A	0x0000472A	447 (0x01BF)	-	implicit	-	kernel32.dll
LCMapStringW	-	0x0000473A	0x0000473A	448 (0x01C0)	-	implicit	-	kernel32.dll

VI. The libraries of interest are:

library (2)	flag (1)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (37)	description
urlmon.dll	x	0x000044D4	0x00004094	implicit	1	OLE32 Extensions for Win32
kernel32.dll	-	0x00004440	0x00004000	implicit	36	Windows NT BASE API Client DLL

Section 3: Dynamic Analysis with SysAnalyzer

Running the program with SysAnalyzer shows that the program replaces a file called "WMIprvse.exe" with a substitute that contains embedded malware. In the screenshot below, the executed file "Lab20-01.exe" was analyzed and a new file "WMIPrvSE.exe" appeared.

```
\analysis
  debug.log
  ProcWatch.log
  Report_3.58pm.log
  sample_Lab20-01.exe_
  WmiPrvSE
    WmiPrvSE_dmp.exe_
    WmiPrvSE_sample.exe_
    WmiPrvSE_strings.log
```

Find | Find | All

```
DefaultNetworkServiceHost
Decoupled:Com:
IDI_ICON3
VS_VERSION_INFO
StringFileInfo
040904B0
CompanyName
Microsoft Corporation
FileDescription
WMI Provider Host
FileVersion
10.0.17763.1 (WinBuild.160101.0800)
InternalName
Wmiprvse.exe
LegalCopyright
 Microsoft Corporation. All rights reserved.
OriginalFilename
Wmiprvse.exe
ProductName
Microsoft
 Windows
 Operating System
ProductVersion
10.0.17763.1
VarFileInfo
Translation
```

This new file houses many malware libraries and functions:

```
GetObjectAsync
PutClassAsync
DeleteClassAsync
CreateClassEnumAsync
PutInstanceAsync
DeleteInstanceAsync
CreateInstanceEnumAsync
ExecQueryAsync
ExecMethodAsync
HostProcessIdentifier
WQL:References
WQL:Associators
WQL:V1ProviderDefined
DefaultSecuredHost
SOFTWARE\Microsoft\WBEM\CIMOM\CompatibleHostProviders
FoldIdentity
```

```
SupportsQuotas
OperationTimeoutInterval
InitializationTimeoutInterval
SupportsThrottling
ConcurrentIndependantRequests
InitializationReentrancy
InitializeAsAdminFirst
PerUserInitialization
PerLocaleInitialization
Pure
HostingModel
SecurityDescriptor
LocalServer32
InProcServer32
wmiprvse.exe
Sink Transmit Buffer Size
Software\Microsoft\WBEM\CIMOM
DefaultRpcStackSize
Software\Microsoft\Wbem\Cimom
ClearAfter
__EventProviderCacheControl=@
__ObjectProviderCacheControl=@
```

Section 4: Dynamic Analysis with FakeNet

To further investigate this file, we have employed the tool called FakeNet. When opened during the execution of the file, it shows 2 requests that seem unusual, as the VM we used was isolated from the network. First, there appears to be a request for the domain "www.practicalmalwareanalysis.com" which is probably a download site. Another point of contention is the request for the domain "canonicalizer.ucsuri.tcs", this seems to be attributed to the malware in some way, possibly to decode hashing or something similar.

```
12/07/22 04:38:59 PM [          Diverter] svchost.exe (3324) requested UDP 239.255.255.250:1900
12/07/22 04:39:00 PM [          Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101
12/07/22 04:39:02 PM [          Diverter] svchost.exe (1500) requested UDP 192.168.56.101:53
12/07/22 04:39:02 PM [        DNS Server] Received A request for domain 'www.practicalmalwareanalysis.com'.
12/07/22 04:39:04 PM [          Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101
12/07/22 04:39:05 PM [          Diverter] svchost.exe (3324) requested UDP 239.255.255.250:1900
12/07/22 04:39:07 PM [          Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101
12/07/22 04:39:13 PM [          Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101
12/07/22 04:39:16 PM [          Diverter] svchost.exe (1500) requested UDP 192.168.56.101:53
12/07/22 04:39:16 PM [        DNS Server] Received NS request for domain 'canonicalizer.ucsuri.tcs'.
12/07/22 04:39:16 PM [        DNS Server] Received A request for domain 'nf.smartscreen.microsoft.com'.
12/07/22 04:39:18 PM [          Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101
12/07/22 04:39:20 PM [          Diverter] ICMP type 3 code 1 192.168.56.101->192.168.56.101
```