

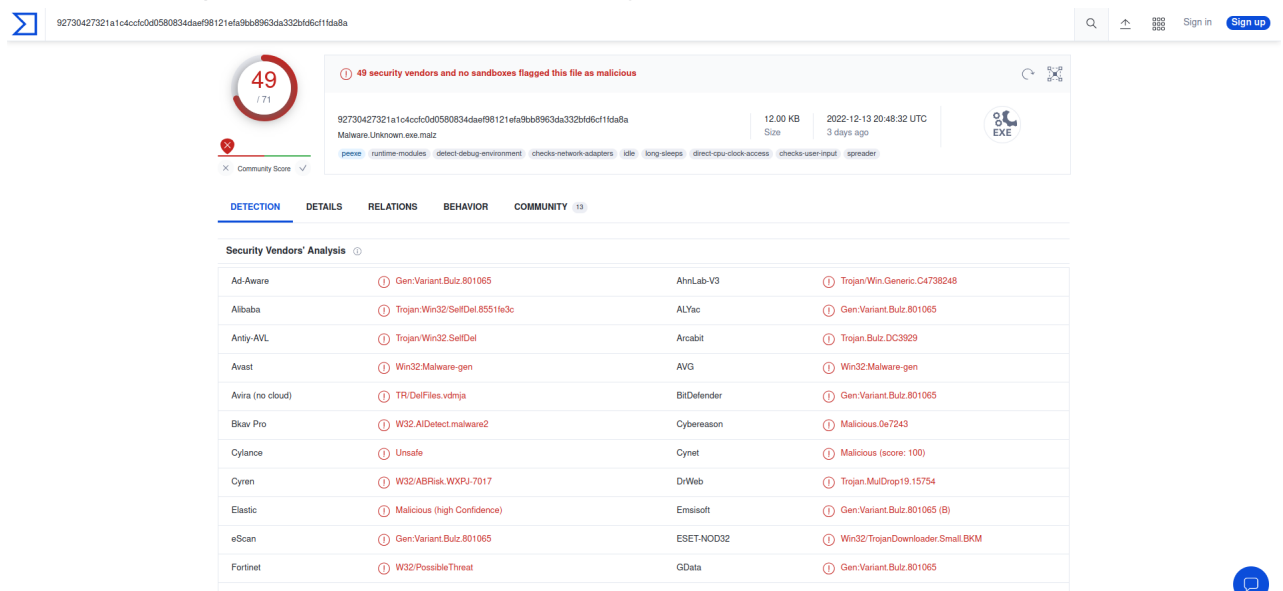
# BASIC STATIC ANALYSIS

- Primeira etapa da análise estática
  - Desarmar o malware, removendo o poder de execução, mudando a extensão do mesmo;
  - Tirar o hash da amostra.

```
C:\Users\toper\Desktop
λ sha256sum.exe Malware.Unknown.exe.malz
92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a *Malware.Unknown.exe.malz

C:\Users\toper\Desktop
λ md5sum.exe Malware.Unknown.exe.malz
1d8562c0adcaee734d63f7baaca02f7c *Malware.Unknown.exe.malz
```

- Passo 02
  - Com o hash é possível identificar se o mesmo já foi visto anteriormente.



92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

49 / 71

49 security vendors and no sandboxes flagged this file as malicious

Malware.Unknown.exe.malz

12.00 KB Size

2022-12-13 20:48:32 UTC 3 days ago

EXE

peexe runtime-modules detect-debug-environment checks-network-adapters idle long-sleeps direct-cpu-clock-access checks-user-input spreader

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	Gen:Variant.Bulz.801065	AhnLab-V3	Trojan.Win.Generic.C4738248
Alibaba	Trojan.Win32/SelfDel.8551fe3c	ALYac	Gen:Variant.Bulz.801065
Antiy-AVL	Trojan.Win32/SelfDel	Arcabit	Trojan.Bulz.DC3929
Avast	Win32/Malware-gen	AVG	Win32/Malware-gen
Avira (no cloud)	TR/DelFiles.vdmja	BitDefender	Gen:Variant.Bulz.801065
Bkav Pro	W32.AIDetect.malware2	Cybereason	Malicious.0e7243
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/ABRisk.WXPJ-7017	DrWeb	Trojan.MalDrop19.15754
Elastic	Malicious (high Confidence)	Emisoft	Gen:Variant.Bulz.801065 (B)
eScan	Gen:Variant.Bulz.801065	ESET-NOD32	Win32/TrojanDownloader.Small.BKM
Fortinet	W32/PossibleThreat	GData	Gen:Variant.Bulz.801065
Gridin	Detected	GridinSoft	Detected

- Também seria o caso de submeter a própria amostra no **VirusTotal**.

- Passo 03
  - Ver as strings presentes no binário, nesse caso estou usando o FLOSS, para pegar essas strings, uma diferença do FLOSS para o comando **strings**, é que ele já tenta decodar e

desobfuscar as strings da amostra.

```
C:\Users\toper\Desktop
λ FLOSS.exe Malware.Unknown.exe.malz
FLOSS static ASCII strings
!This program cannot be run in DOS mode.
r&cgr
rRich
.text
`.rdata
@.data
.rsrc
@.reloc
[ _^]
[ _^]
h02@
u_Ph
@PPh
h81@
h13@
D$`Ph@1@
SSVRP
SSVRP
| ;u
jdRP
Y_^[
h01@
=MC@
u"hPC@
h\C@
Y_^[
=LC@
=PC@
hPC@
hhC@
>csm
%xC@
Y__^[
SVW3
nte1
5ineI
5Genu
t#=`
_^[3
%\0@
%`0@
%h0@
%d0@
%|0@
WVS3
WVU3
v N+D$
RSDSL
C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb
GCTL
.text$mn
.idata$5
.00cfg
```

- Passo 04

- Com o PEvent podemos obter informações importante sobre a amostra, a primeira delas se encontra no campo/coluna **Value**, onde podemos ver o qual a assinatura do arquivo "MZ" que

nesse caso é um *DOS MZ executable*.

PMAT-FlareVM (pre-detonation) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

PEview - C:\Users\tope\Desktop\Malware.Unknown.exe.malz

File View Go Help

Malware.Unknown.exe.malz

- IMAGE\_DOS\_HEADER
- IMAGE\_DEBUG\_TYPE\_
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - Signature
  - IMAGE\_FILE\_HEADER
  - IMAGE\_OPTIONAL\_HEADER
  - IMAGE\_SECTION\_HEADER .text
  - IMAGE\_SECTION\_HEADER .rdata
  - IMAGE\_SECTION\_HEADER .data
  - IMAGE\_SECTION\_HEADER .rsrc
  - IMAGE\_SECTION\_HEADER .reloc
- SECTION .text
- SECTION .rdata
  - IMPORT Address Table
  - IMAGE\_DEBUG\_DIRECTORY
  - IMAGE\_LOAD\_CONFIG\_DIRECTORY
  - IMAGE\_DEBUG\_TYPE\_CODEVIEW
  - IMAGE\_DEBUG\_TYPE\_
  - IMAGE\_DEBUG\_TYPE\_
  - IMPORT Directory Table
  - IMPORT Name Table
  - IMPORT Hints/Names & DLL Names
- SECTION .data
- SECTION .rsrc
  - IMAGE\_RESOURCE\_DIRECTORY Type
  - IMAGE\_RESOURCE\_DIRECTORY NameID
  - IMAGE\_RESOURCE\_DIRECTORY Language
  - IMAGE\_RESOURCE\_DATA\_ENTRY
  - MANIFEST 0001 0409
- SECTION .reloc
  - IMAGE\_BASE\_RELOCATION

pFile	Raw Data	Value	
00000000	4D 5A 90 00 03 00 00 00	04 00 00 00 FF FF 00 00	MZ.....
00000010	B8 00 00 00 00 00 00 00	40 00 00 00 00 00 00 00	.....@.....
00000020	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000030	00 00 00 00 00 00 00 00	00 00 00 00 F8 00 00 00	.....F.....
00000040	0E 1F BA 0E 00 B4 09 CD	21 B8 01 4C CD 21 54 68	.....!..L..!Th
00000050	69 73 20 70 72 6F 67 72	61 6D 20 63 61 6E 6E 6F	is program canno
00000060	74 20 62 65 20 72 75 6E	20 69 6E 20 44 4F 53 20	t be run in DOS
00000070	6D 6F 64 65 2E 0D 0D 0A	24 00 00 00 00 00 00 00	mode...\$. ....
00000080	F4 70 F6 21 B0 11 98 72	B0 11 98 72 B0 11 98 72	.p!...r...r...r
00000090	B9 69 0B 72 BA 11 98 72	0E 60 9D 73 A4 11 98 72	...r...r...s...r
000000A0	0E 60 9C 73 BC 11 98 72	0E 60 9B 73 B5 11 98 72	...s...r...s...r
000000B0	0E 60 99 73 B4 11 98 72	EB 79 99 73 B9 11 98 72	...s...r...y...s...r
000000C0	B0 11 99 72 8C 11 98 72	26 63 91 73 B1 11 98 72	...r...r&c...s...r
000000D0	26 63 67 72 B1 11 98 72	26 63 9A 73 B1 11 98 72	&cgr...r&c...s...r
000000E0	52 69 63 68 B0 11 98 72	00 00 00 00 00 00 00 00	Rich...r...r...r
000000F0	00 00 00 00 00 00 00 00	50 45 00 00 4C 01 05 00	...PE...L...
00000100	C0 B6 33 61 00 00 00 00	00 00 00 00 E0 00 02 01	...3a...r...r...r
00000110	0B 01 0E 1C 00 16 00 00	00 18 00 00 00 00 00 00	.....
00000120	F1 15 00 00 00 10 00 00	00 30 00 00 00 00 40 00	.....0...@.....
00000130	00 10 00 00 00 02 00 00	06 00 00 00 00 00 00 00	.....
00000140	06 00 00 00 00 00 00 00	00 70 00 00 00 04 00 00	.....p...r...r...r
00000150	00 00 00 00 03 00 40 81	00 00 10 00 00 10 00 00	.....@...r...r...r
00000160	00 00 10 00 00 10 00 00	00 00 00 00 10 00 00 00	.....
00000170	00 00 00 00 00 00 00 00	34 38 00 00 F0 00 00 00	.....48...r...r...r
00000180	00 50 00 00 E0 01 00 00	00 00 00 00 00 00 00 00	...P...r...r...r
00000190	00 00 00 00 00 00 00 00	00 60 00 00 B8 01 00 00	.....
000001A0	98 33 00 00 70 00 00 00	00 00 00 00 00 00 00 00	...3...p...r...r...r
000001B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000001C0	08 34 00 00 40 00 00 00	00 00 00 00 00 00 00 00	...4...@...r...r...r
000001D0	00 30 00 00 FC 00 00 00	00 00 00 00 00 00 00 00	...0...r...r...r
000001E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000001F0	2E 74 65 78 74 00 00 00	A1 15 00 00 00 10 00 00	...t text...r...r...r
00000200	00 16 00 00 00 04 00 00	00 00 00 00 00 00 00 00	.....

Outra info que podemos estar pegando é quando o binário foi compilado.

PMAT-FlareVM (pre-detonation) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

PEview - C:\Users\tope\Desktop\Malware.Unknown.exe.malz

File View Go Help

Malware.Unknown.exe.malz

- IMAGE\_DOS\_HEADER
- IMAGE\_DEBUG\_TYPE\_
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - Signature
  - IMAGE\_FILE\_HEADER
  - IMAGE\_OPTIONAL\_HEADER
  - IMAGE\_SECTION\_HEADER .text
  - IMAGE\_SECTION\_HEADER .rdata

pFile	Data	Description	Value
000000FC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000FE	0005	Number of Sections	
00000100	6133B6C0	Time Date Stamp	2021/09/04 Sat 18:11:12 UTC
00000104	00000000	Pointer to Symbol Table	
00000108	00000000	Number of Symbols	
0000010C	00E0	Size of Optional Header	
0000010E	0102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

Na sessão IMAGE\_SECTION\_HEADER.txt é um dos cinco locais no binário onde podemos ler as informações em tempo de execução. E uma info que devemos estar atentos é o **Virtual Size** e o **Size of Raw Data**

VIRTUAL

- 5537 bytes

- Esse valor corresponde aos dados em disco quando é execução

- RAW

- 5632 bytes


Quando o valor do **Virtual Size** é bem maior do que o do **raw**, podemos deduzir que inicialmente há mais dados disponíveis no entanto o binário está empacotando essa informação.

- Na sessão **SECTION .rdata\IMPORT\_Address\_table**, está contida uma das mais importantes informações que podemos obter com o PEView, pois podemos ver dlls carregadas/importadas, APIs que foram chamadas.

pFile	Data	Description	Value
00001A00	00003A20	Hint/Name RVA	0274 GetModuleFileNameW
00001A04	00003A36	Hint/Name RVA	0086 CloseHandle
00001A08	00003A44	Hint/Name RVA	00E5 CreateProcessW
00001A0C	00003EB4	Hint/Name RVA	0218 GetCurrentProcessId
00001A10	00003ECA	Hint/Name RVA	021C GetCurrentThreadId
00001A14	00003E7E	Hint/Name RVA	0386 IsProcessorFeaturePresent
00001A18	00003EE0	Hint/Name RVA	02E9 GetSystemTimeAsFileTime
00001A1C	00003EFA	Hint/Name RVA	0363 InitializeSListHead
00001A20	00003F10	Hint/Name RVA	037F IsDebuggerPresent
00001A24	00003E6A	Hint/Name RVA	058C TerminateProcess
00001A28	00003E56	Hint/Name RVA	0217 GetCurrentProcess
00001A2C	00003F24	Hint/Name RVA	0278 GetModuleHandleW
00001A30	00003E1C	Hint/Name RVA	05AD UnhandledExceptionFilter
00001A34	00003E38	Hint/Name RVA	056D SetUnhandledExceptionFilter
00001A38	00003E9A	Hint/Name RVA	044D QueryPerformanceCounter
00001A3C	00000000	End of Imports	KERNEL32.dll
00001A40	00003A80	Hint/Name RVA	0591 _Query_perf_frequency
00001A44	00003A98	Hint/Name RVA	05B6 _Thrd_sleep
00001A48	00003AA6	Hint/Name RVA	0590 _Query_perf_counter
00001A4C	00003ABC	Hint/Name RVA	05CC _Xtime_get_ticks
00001A50	00000000	End of Imports	MSVCP140.dll
00001A54	00003A64	Hint/Name RVA	01B7 ShellExecuteW
00001A58	00000000	End of Imports	SHELL32.dll

- Na imagem acima podemos ver as informações citadas anteriormente, e havendo dúvidas sobre o propósito das dlls ou das chamadas de APIs, é só dar um google.
- Uma outra forma de nos auxiliar com essas dúvidas, é acessando [malapi.io](https://malapi.io), que é basicamente como o **MITRE ATT&CK** que nesse caso trackeia as APIs, nos informando para qual TTP aquela API possivelmente é usada.

MalAPI.io    Contribute    FAQ    Other



mrdox

Mapping mode: OFF (Export Table)

Enumeration	Injection	Evasion	Spying	Internet	Anti-Debugging	Ransomware
CreateToolhelp32Snapshot	CreateFileMappingA	CreateFileMappingA	AttachThreadInput	WinExec	CreateToolhelp32Snapshot	CryptAcquireContextA
EnumDeviceDrivers	CreateProcessA	DeleteFileA	CallNextHookEx	FtpPutFileA	GetLogicalProcessorInformation	EncryptFileA
EnumProcesses	CreateRemoteThread	GetModuleHandleA	GetAsyncKeyState	HttpOpenRequestA	GetLogicalProcessorInformationEx	CryptEncrypt
EnumProcessModules	CreateRemoteThreadEx	GetProcAddress	GetClipboardData	HttpSendRequestA	GetTickCount	CryptDecrypt
EnumProcessModulesEx	GetModuleHandleA	LoadLibraryA	GetDC	HttpSendRequestExA	OutputDebugStringA	CryptCreateHash
FindFirstFileA	GetProcAddress	LoadLibraryExA	GetDCEx	InternetCloseHandle	CheckRemoteDebuggerPresent	CryptHashData
FindNextFileA	GetThreadContext	LoadResource	GetForegroundWindow	InternetOpenA	Sleep	CryptDeriveKey
GetLogicalProcessorInformation	HeapCreate	SetEnvironmentVariableA	GetKeyboardState	InternetOpenUrlA	GetSystemTime	CryptSetKeyParam
GetLogicalProcessorInformationEx	LoadLibraryA	SetFileTime	GetKeyState	InternetReadFile	GetComputerNameA	CryptGetHashParam

- Passo 04.1
  - Um malware empacotado/encapsulado é basicamente quando o mesmo foi comprimido ou usado algum mecanismo para criptografalo fazendo-o parecer diferente.  
Como um arquivo zipado por exemplo, quando comprimimos, meio que parece apenas um único arquivo, porém pra saber o que tem dentro, somente abrindo-o/extraindo o conteúdo.
  - Um packer comumente utilizado é o [UPX](#).

- Encapsulado:

PEView - C:\Users\tope\l\Desktop\Malware.Packed.exe.malz

File View Go Help

Malware.Packed.exe.malz

- IMAGE\_DOS\_HEADER
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - Signature
  - IMAGE\_FILE\_HEADER
  - IMAGE\_OPTIONAL\_HEADER
  - IMAGE\_SECTION\_HEADER UPX0
  - IMAGE\_SECTION\_HEADER UPX1
  - IMAGE\_SECTION\_HEADER .rsrc
- SECTION UPX0
- SECTION UPX1
- SECTION .rsrc
  - IMAGE\_RESOURCE\_DIRECTORY Type
  - IMAGE\_RESOURCE\_DIRECTORY NameID
  - IMAGE\_RESOURCE\_DIRECTORY Language
  - IMAGE\_RESOURCE\_DATA\_ENTRY
  - VERSION 0001 0409
  - IMPORT Directory Table
  - IMPORT Address Table
  - IMPORT DLL Names
  - IMPORT Hints/Names

pFile	Raw Data	Value	
00000000	4D 5A 90 00 03 00 00 00	04 00 00 00 FF FF 00 00	MZ .....
00000010	B8 00 00 00 00 00 00 00	40 00 00 00 00 00 00 00	.....@.....
00000020	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000030	00 00 00 00 00 00 00 00	00 00 00 00 E8 00 00 00	.....
00000040	0E 1F BA 0E 00 B4 09 CD	21 B8 01 4C CD 21 54 68	.....!..L!Th
00000050	69 73 20 70 72 6F 67 72	61 6D 20 63 61 6E 6E 6F	is program canno
00000060	74 20 62 65 20 72 75 6E	20 69 6E 20 44 4F 53 20	t be run in DOS
00000070	6D 6F 64 65 2E 0D 0D 0A	24 00 00 00 00 00 00 00	mode...\$.....
00000080	93 38 F0 D6 D7 59 9E 85	D7 59 9E 85 D7 59 9E 85	.8...Y...Y...Y...
00000090	AC 45 92 85 D3 59 9E 85	54 45 90 85 DE 59 9E 85	.E...Y...TE...Y...
000000A0	B8 46 94 85 DC 59 9E 85	B8 46 9A 85 D4 59 9E 85	.F...Y...F...Y...
000000B0	D7 59 9F 85 1E 59 9E 85	54 51 C3 85 DF 59 9E 85	.Y...Y...TQ...Y...
000000C0	83 7A AE 85 FF 59 9E 85	10 5F 98 85 D6 59 9E 85	.z...Y...Y...
000000D0	52 69 63 68 D7 59 9E 85	00 00 00 00 00 00 00 00	Rich.Y.....
000000E0	00 00 00 00 00 00 00 00	50 45 00 00 4C 01 03 00	.....PE...L...
000000F0	A9 56 5B 4A 00 00 00 00	00 00 00 00 E0 00 0F 01	.V[J].....
00000100	0B 01 06 00 00 B0 00 00	00 10 00 00 00 C0 00 00	.....
00000110	30 7B 01 00 00 D0 00 00	00 80 01 00 00 00 40 00	0{.....@.....
00000120	00 10 00 00 00 02 00 00	04 00 00 00 00 00 00 00	.....
00000130	04 00 00 00 00 00 00 00	00 90 01 00 00 10 00 00	.....
00000140	00 00 00 00 02 00 00 00	00 00 10 00 00 10 00 00	.....
00000150	00 00 10 00 00 10 00 00	00 00 00 00 10 00 00 00	.....
00000160	00 00 00 00 00 00 00 00	C4 87 01 00 40 01 00 00	.....@.....
00000170	00 80 01 00 C4 07 00 00	00 00 00 00 00 00 00 00	.....
00000180	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000190	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000001A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000001B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000001C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000001D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000001E0	55 50 58 30 00 00 00 00	00 C0 00 00 10 00 00 00	UPX0.....
000001F0	00 00 00 00 04 00 00 00	00 00 00 00 00 00 00 00	.....
00000200	00 00 00 00 80 00 00 E0	55 50 58 31 00 00 00 00	.....UPX1.....
00000210	00 B0 00 00 00 D0 00 00	00 AE 00 00 00 04 00 00	.....
00000220	00 00 00 00 00 00 00 00	00 00 00 00 40 00 00 E0	.....@.....
00000230	2E 72 73 72 63 00 00 00	00 10 00 00 00 80 01 00	.rsrc.....
00000240	00 0A 00 00 00 B2 00 00	00 00 00 00 00 00 00 00	.....
00000250	00 00 00 00 40 00 00 C0	00 00 00 00 00 00 00 00	.....@.....
00000260	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000270	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000280	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
00000290	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000002A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000002B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000002C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000002D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
000002E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....

Como podemos ver na imagem acima, temos os campos SECTION UPX0 e SECTION UPX1, que são os encapsuladores/empacotadores usados nessa payload.

Malware.Packed.exe.malz

- IMAGE\_DOS\_HEADER
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - Signature
  - IMAGE\_FILE\_HEADER
  - IMAGE\_OPTIONAL\_HEADER
  - IMAGE\_SECTION\_HEADER UPX0
  - IMAGE\_SECTION\_HEADER UPX1
  - IMAGE\_SECTION\_HEADER .rsrc
- SECTION UPX0
- SECTION UPX1
- SECTION .rsrc
  - IMAGE\_RESOURCE\_DIRECTORY Type
  - IMAGE\_RESOURCE\_DIRECTORY NameID
  - IMAGE\_RESOURCE\_DIRECTORY Language
  - IMAGE\_RESOURCE\_DATA\_ENTRY
  - VERSION 0001 0409
  - IMPORT Directory Table
  - IMPORT Address Table
  - IMPORT DLL Names
  - IMPORT Hints/Names

pFile	Data	Description	Value
0000BA3C	000188AC	Hint/Name RVA	0000 FreeSid
0000BA40	00000000	End of Imports	ADVAPI32.dll
0000BA44	000188D4	Hint/Name RVA	0000 LoadLibraryA
0000BA48	000188B6	Hint/Name RVA	0000 ExitProcess
0000BA4C	000188C4	Hint/Name RVA	0000 GetProcAddress
0000BA50	000188E2	Hint/Name RVA	0000 VirtualProtect
0000BA54	00000000	End of Imports	KERNEL32.DLL
0000BA58	000188F2	Hint/Name RVA	0000 _job
0000BA5C	00000000	End of Imports	MSVCRT.dll
0000BA60	000188F8	Hint/Name RVA	0000 WSARcv
0000BA64	00000000	End of Imports	WS2_32.dll
0000BA68	8000006F	Ordinal	006F
0000BA6C	00000000	End of Imports	WSOCK32.dll

- Diferente do modelo anterior, podemos ver que a Address Table está bem enxuta.
- Um ponto que podemos tirar da Address Table é que há duas APIs (**LoadLibraryA** e **GetProcAddress**) que são usadas para importar/fazer outras chamadas de dlls, endereços,

## funções, processos...

PEView - C:\Users\toper\Desktop\Malware.Packed.exe.malz

File View Go Help			
Malware Packed.exe.malz			
IMAGE_DOS_HEADER	pFile	Data	Description
MS-DOS Stub Program	000001E0	55 50 58 30	Name
IMAGE_NT_HEADERS	000001E4	00 00 00 00	Value
Signature	000001E8	0000C000	Virtual Size
IMAGE_FILE_HEADER	000001EC	00001000	RVA
IMAGE_OPTIONAL_HEADER	000001F0	00000000	Size of Raw Data
IMAGE_SECTION_HEADER UPX0	000001F4	00000400	Pointer to Raw Data
IMAGE_SECTION_HEADER UPX1	000001F8	00000000	Pointer to Relocations
IMAGE_SECTION_HEADER .rsrc	000001FC	00000000	Pointer to Line Numbers
SECTION UPX0	00000200	0000	Number of Relocations
SECTION UPX1	00000202	0000	Number of Line Numbers
SECTION .rsrc	00000204	E0000080	Characteristics
IMAGE_RESOURCE_DIRECTORY Type		00000080	IMAGE_SCN_CNT_UNINITIALIZED_DATA
IMAGE_RESOURCE_DIRECTORY NameID		20000000	IMAGE_SCN_MEM_EXECUTE
IMAGE_RESOURCE_DIRECTORY Language		40000000	IMAGE_SCN_MEM_READ
IMAGE_RESOURCE_DATA_ENTRY		80000000	IMAGE_SCN_MEM_WRITE
VERSION 0001 0409			
IMPORT Directory Table			
IMPORT Address Table			
IMPORT DLL Names			
IMPORT Hints/Names			

- Um outro ponto que vale a pena olhar e que já foi mencionado é a diferença entre o **Raw Data** e o **Virtual Size**, nesse caso específico como o Raw Data está zerado, podemos inferir o mesmo precisa ser inicializado.

## Passo 05

### USANDO O PESTUDIO

pestudio 9.46 - Malware Initial Assessment - www.winator.com - [c:\users\toper\desktop\malware.unknown.exe.malz]

file settings about	
c:\users\toper\desktop\malware.unknown.exe.m	property
indicators (48)	value
virustotal (error)	md5
dos-header (64 bytes)	sha1
dos-stub (184 bytes)	sha256
rich-header (Visual Studio)	first-bytes-hex
file-header (Intel-386)	first-bytes-text
optional-header (console)	file-size
directories (6)	entropy
sections (5)	imphash
libraries (flag)	signature
imports (flag)	tooling
exports (n/a)	entry-point
exceptions (n/a)	file-version
tls-callback (n/a)	description
relocations (208)	file-type
.NET (n/a)	cpu
resources (manifest)	subsystem
strings (255) *	compiler-stamp
debug (3)	debugger-stamp
manifest (asInvoker)	resources-stamp
version (n/a)	import-stamp
overlay (n/a)	exports-stamp

- Acima está a primeira tela, logo que é carregado o arquivo, que diferente já do peview, o pestudio já nos dá os hashes, podendo assim já submeter ao vírus total por exemplo.
- Outras informações interessantes apresentada são os primeiro bytes tanto em texto quanto em hexadecimal, a arquitetura do binário.



pestudio 9.46 - Malware Initial Assessment - www.winitor.com - [c:\users\toper\desktop\malware.unknown.exe.malz]

file settings about

c:\users\toper\desktop\malware.unknown.exe.m	indicator (48)	detail	level
indicators (48)	strings > flag	8	1
virustotal (error)	imports > flag	8	1
dos-header (64 bytes)	library > flag	Internet Extensions for Win32 Library	1
dos-stub (184 bytes)	library > flag	OLE32 Extensions for Win32	1
rich-header (Visual Studio)	URL > pattern	http://huskyhacks.dev	1
file-header (Intel-386)	URL > pattern	http://ssl-6582datamanager.helpdeskbrots.local/favicon.ico	1
optional-header (console)	file > checksum > invalid	0x00000000	3
directories (6)	rich-header > offset	0x00000080	3
sections (5)	entry-point > location	0x000015F1	3
libraries (flag)	file > image-base	0x00400000	3
imports (flag)	rich-header > checksum	0x72981180	3
exports (n/a)	resources > instances > standard	1	3
exceptions (n/a)	libraries > count	11	3
tls-callback (n/a)	file > size	12288 bytes	3
relocations (208)	dos-stub > size	184 bytes	3
.NET (n/a)	strings > count	255	3
resources (manifest)	resources > file-ratio	3.10%	3
strings (255) *	rich-header > hash	3D26CE315365D78C3AFA8F152E010B12	3
debug (3)	section > alignment	4096 bytes	3
manifest (asInvoker)	file > alignment	512 bytes	3
version (n/a)	imports > count	52	3
overlay (n/a)	file > debug > symbols	C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb	3
	file > signature	Microsoft Visual C++	3
	debug > stream > name	PGO	3
	debug > stream > name	RSDS	3
	file > score > error	The server name or address could not be resolved	3
	file > tooling	Visual Studio 2008	3
	file > os > target	Windows Server 2008	3
	security > protection	address-space-layout-randomization (ASLR) > ON	3
	resources > manifest	available	3
	security > protection	code-integrity (CI) > OFF	3
	file > subsystem	console	3
	security > protection	control-flow-guard (CFG) > OFF	3
	security > protection	data-execution-prevention (DEP) > ON	3
	feature > group	dynamic-library	3
	feature > group	exception	3
	feature > group	execution	3
	feature > group	file	3
	strings > label	format-string	3
	feature > group	memory	3
	feature > group	network	3
	feature > group	reconnaissance	3
	security > protection	stack-buffer-overflow-detection (GS) > ON	3
	feature > group	synchronization	3
	strings > label	url-pattern	3

- Na aba **indicator** podemos ver algumas strings, referencias de URL, link simbólicos... Cada informação com seu respectivo grau de severidade (sendo do menor pro maior).

pestudio 9.46 - Malware Initial Assessment - www.winitor.com - [c:\users\toper\desktop\malware.unknown.exe.malz]

file settings about

c:\users\toper\desktop\malware.unknown.exe.m	library (11)	duplicate (0)	flag (2)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (52)	description
indicators (48)	KERNEL32.dll	-	-	-	0x00003924	0x00003000	implicit	15	Windows NT BASE API Client
virustotal (error)	SHELL32.dll	-	-	-	0x00003978	0x00003054	implicit	1	Windows Shell Library
dos-header (64 bytes)	MSVCP140.dll	-	-	-	0x00003964	0x00003040	implicit	4	Microsoft C Runtime Library
dos-stub (184 bytes)	urlmon.dll	-	x	-	0x00003A18	0x000030F4	implicit	1	OLE32 Extensions for Win32
rich-header (Visual Studio)	WININET.dll	-	x	-	0x00003994	0x00003070	implicit	2	Internet Extensions for Win32 Library
file-header (Intel-386)	VCRUNTIME140.dll	-	-	-	0x00003980	0x0000305C	implicit	4	Microsoft C Runtime Library
optional-header (console)	api-ms-win-crt-stdio-l1-1-0.dll	-	-	-	0x00003A08	0x000030E4	implicit	3	n/a
directories (6)	api-ms-win-crt-runtime-l1-1-0.dll	-	-	-	0x00003988	0x00003094	implicit	19	n/a
sections (5)	api-ms-win-crt-math-l1-1-0.dll	-	-	-	0x00003980	0x0000308C	implicit	1	n/a
libraries (flag)	api-ms-win-crt-locale-l1-1-0.dll	-	-	-	0x000039A8	0x00003084	implicit	1	n/a
imports (flag)	api-ms-win-crt-heap-l1-1-0.dll	-	-	-	0x000039A0	0x0000307C	implicit	1	n/a
exports (n/a)									
exceptions (n/a)									
tls-callback (n/a)									
relocations (208)									
.NET (n/a)									
resources (manifest)									
strings (255) *									
debug (3)									
manifest (asInvoker)									
version (n/a)									
overlay (n/a)									

- Na aba **libraries** temos todas as **DLLs** que foram carregadas no programa, sendo que de fato nem todas são necessariamente maliciosas, o que devemos ter atenção é na coluna **flag**, que



destaca as DLLs comumente usadas de forma maliciosa.

pestudio 9.46 - Malware Initial Assessment - www.winitor.com - [c:\users\tope\desktop\malware.unknown.exe.malz]

file settings about

c:\users\tope\desktop\malware.unknown.exe.m

indicators (48)

virustotal (error)

dos-header (64 bytes)

dos-stub (184 bytes)

rich-header (Visual Studio)

file-header (Intel-386)

optional-header (console)

directories (6)

sections (5)

libraries (flag)

imports (flag)

exports (n/a)

exceptions (n/a)

tls-callback (n/a)

relocations (208)

.NET (n/a)

resources (manifest)

strings (255)

debug (3)

manifest (asInvoker)

version (n/a)

overlay (n/a)

encoding (2)	size (bytes)	location	flag (8)	label (67)	group (8)	value (255)
ascii	13	0x00024446	x	import	execution	CreateProcess
ascii	19	0x00028B86	x	import	reconnaissance	GetCurrentProcessId
ascii	18	0x00028C8C	x	import	execution	GetCurrentThreadid
ascii	12	0x0002516	x	import	network	InternetOpen
ascii	15	0x0002502	x	import	network	InternetOpenUrl
ascii	12	0x00024666	x	import	execution	ShellExecute
ascii	16	0x000286C	x	import	execution	TerminateProcess
ascii	17	0x00024E0	x	import	network	URLDownloadToFile
unicode	4	0x02731D6C	-	utility	-	open
unicode	76	0x02731CD0	-	utility	-	ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
unicode	11	0x02731C88	-	user-agent	-	Mozilla/5.0
unicode	21	0x02731CA0	-	url-pattern	-	http://huskyhacks.dev
unicode	57	0x02731B88	-	url-pattern	-	http://ss1-6582datamanager.helpdeskbro.local/favicon.ico
ascii	12	0x0002456	-	library	-	KERNEL32.dll
ascii	12	0x00024D0	-	library	-	MSVCP140.dll
ascii	11	0x0002474	-	library	-	SHELL32.dll
ascii	16	0x0002588	-	library	-	VCRUNTIME140.dll
ascii	11	0x0002524	-	library	network	WININET.dll
ascii	30	0x00027FC	-	library	-	api-ms-win-crt-heap-l1-1-0.dll
ascii	32	0x00027DA	-	library	-	api-ms-win-crt-locale-l1-1-0.dll
ascii	30	0x00027BA	-	library	-	api-ms-win-crt-math-l1-1-0.dll
ascii	33	0x0002798	-	library	-	api-ms-win-crt-runtime-l1-1-0.dll
ascii	31	0x0002778	-	library	-	api-ms-win-crt-stdio-l1-1-0.dll
ascii	10	0x00024F4	-	library	network	urlmon.dll
ascii	11	0x0002438	-	import	-	CloseHandle
ascii	17	0x0002858	-	import	execution	GetCurrentProcess
ascii	17	0x0002422	-	import	dynamic-library	GetModuleFileName
ascii	15	0x0002926	-	import	dynamic-library	GetModuleHandle
ascii	23	0x00028E2	-	import	file	GetSystemTimeAsFileTime
ascii	19	0x00028FC	-	import	synchronization	InitializeListHead
ascii	17	0x0002912	-	import	reconnaissance	IsDebuggerPresent
ascii	25	0x0002880	-	import	reconnaissance	IsProcessorFeaturePresent
ascii	23	0x000289C	-	import	reconnaissance	QueryPerformanceCounter
ascii	27	0x000283A	-	import	exception	SetUnhandledExceptionFilter
ascii	24	0x000281E	-	import	exception	UnhandledExceptionFilter
ascii	19	0x00024A8	-	import	-	_Query_perf_counter
ascii	21	0x0002482	-	import	-	_Query_perf_frequency
ascii	11	0x000249A	-	import	-	_Thrd_sleep
ascii	16	0x000248E	-	import	-	_Xtime_get_ticks
ascii	19	0x0002532	-	import	-	_current_exception
ascii	27	0x0002548	-	import	-	_current_exception_context
ascii	10	0x0002664	-	import	-	_p_argis
ascii	10	0x0002692	-	import	-	_p_argis
ascii	12	0x0002708	-	import	-	_p_commode
ascii	16	0x00025DA	-	import	-	_setusermatherr

sha256: 9273b427321a1c4ccfcd0580834DAEF98121EFA98B8963DA332BF06CF1FDA8A    cpu: 32-bit    file-type: executable    subsystem: console    entry-point: 0x000015F1    signature: Microsoft Visual C++

- Na aba **strings**, como o nome é sugestivo, temos as strings extraídas do binário, sendo a coluna **flag** destacando pontos possivelmente malisiosos, já coluna label temos basicamente uma categorização daquela string.