TUGAS KEAMANAN JARINGAN KOMPUTER

“ MALWARE “

NAMA : DESY MARITA

NIM : 09011281320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

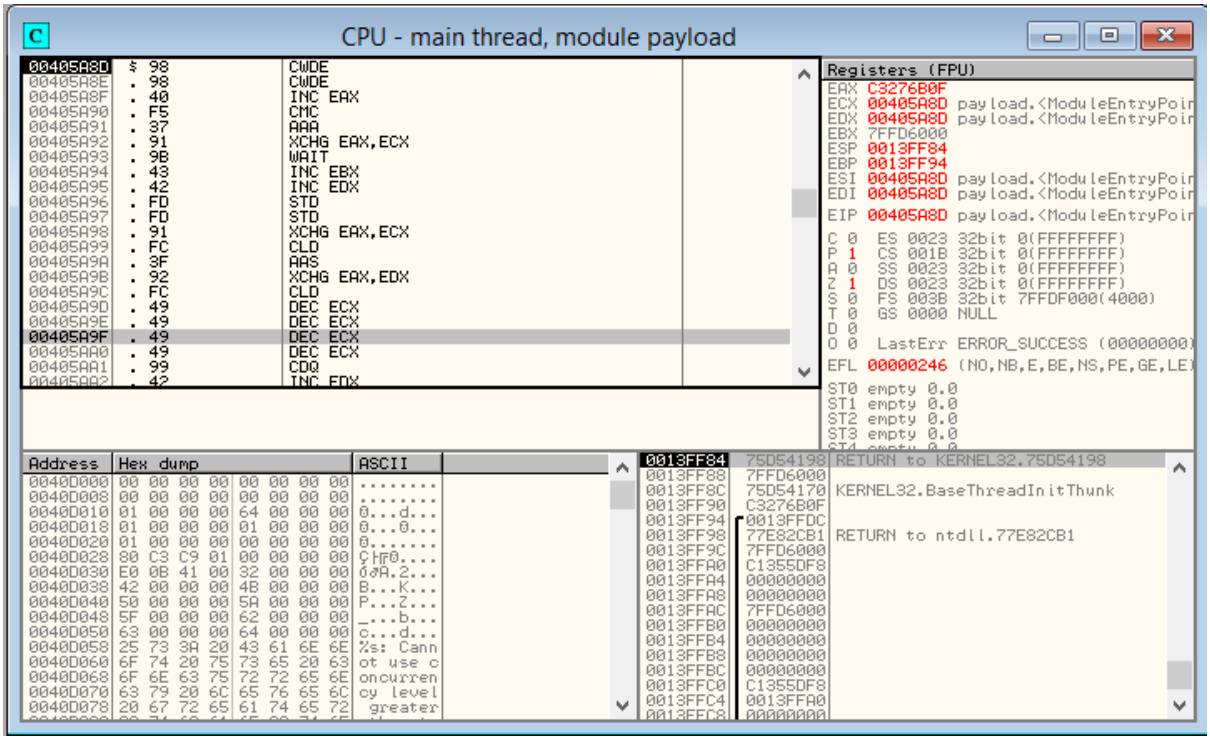
Serangan terhadap keamanan komputer maupun sistem informasi yang sedang populer saat ini yaitu melalui kode program yang dinamakan Malware. Malware merupakan suatu perangkat lunak atau suatu kode program yang bertujuan untuk masuk ke dalam sistem atau jaringan komputer agar dapat mengakses data-data pribadi milik target/korban.

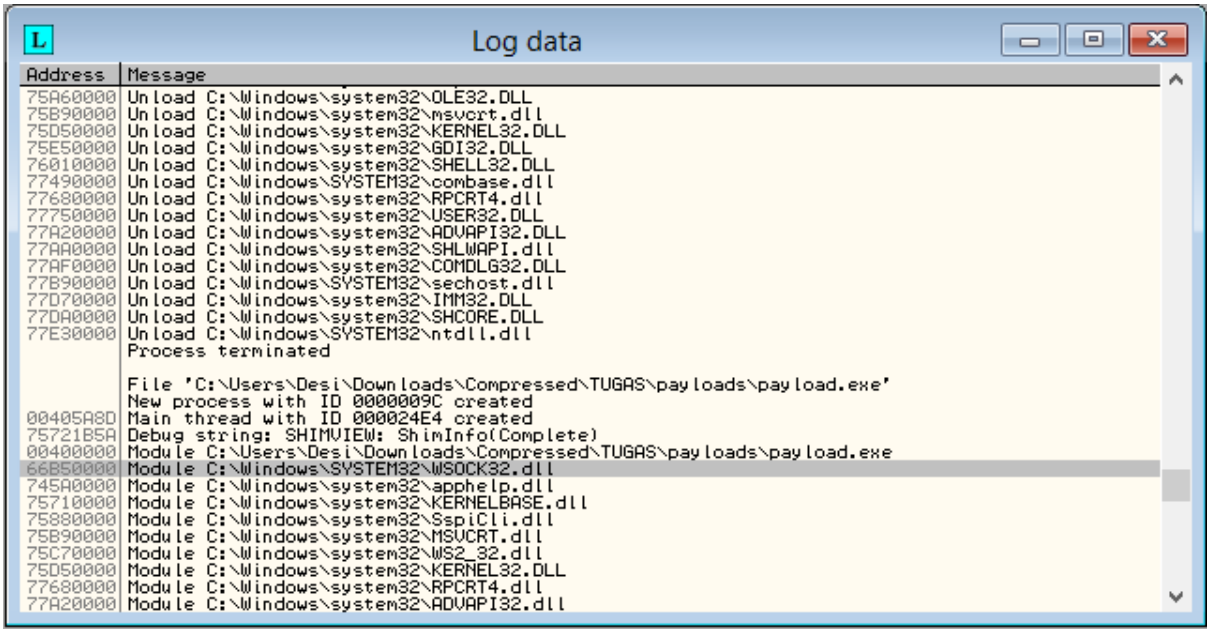
Tools yang di gunakan dalam analisa Malware ini yaitu :

1. OllyDbg

OllyDBG merupakan sebuah tools cracking www.ollydbg.de yang bisa digunakan untuk cracking sebuah aplikasi. Seperti menemukan serial number sebuah aplikasi, membuat clone aplikasi dan memungkinkan user dapat menikmati sebuah aplikasi yang full version tanpa membeli serial number sepeser pun. OllyDBG dapat membantu kita dalam mendapatkan sebuah aplikasi yang kita inginkan dengan bantuan tools lain seperti PEiD, sebuah tools unpacking untuk aplikasi yang ter-pack.

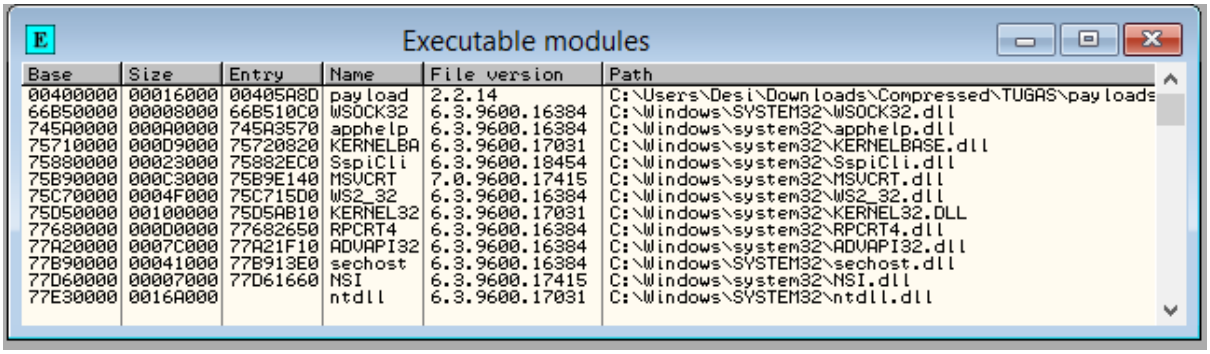
Berikut Hasil File payload dengan tools OllyDbg :





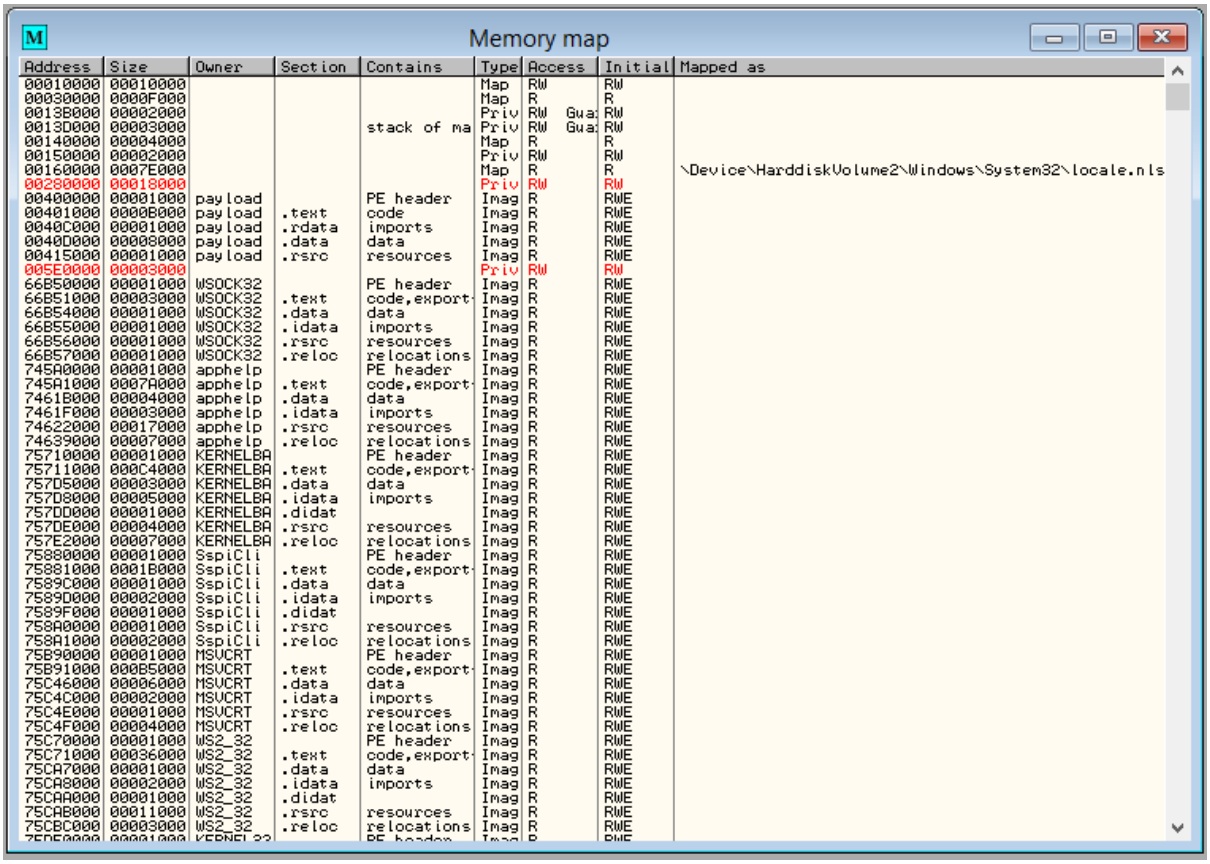
Log data

Address	Message
75A60000	Unload C:\Windows\system32\OLE32.DLL
75B90000	Unload C:\Windows\system32\msvcrt.dll
75D50000	Unload C:\Windows\system32\KERNEL32.DLL
75E50000	Unload C:\Windows\system32\GDI32.DLL
76010000	Unload C:\Windows\system32\SHELL32.DLL
77490000	Unload C:\Windows\SYSTEM32\combase.dll
77680000	Unload C:\Windows\system32\RPCRT4.dll
77750000	Unload C:\Windows\system32\USER32.DLL
77A20000	Unload C:\Windows\system32\ADVAPI32.DLL
77AA0000	Unload C:\Windows\system32\SHLWAPI.dll
77AF0000	Unload C:\Windows\system32\COMDLG32.DLL
77B90000	Unload C:\Windows\SYSTEM32\sechost.dll
77D70000	Unload C:\Windows\system32\IMM32.DLL
77DA0000	Unload C:\Windows\system32\SHCORE.DLL
77E30000	Unload C:\Windows\SYSTEM32\ntdll.dll
	Process terminated
	File 'C:\Users\Desi\Downloads\Compressed\TUGAS\payloads\payload.exe'
	New process with ID 0000009C created
00405A8D	Main thread with ID 000024E4 created
75721B5A	Debug string: SHIMVIEW: ShimInfo(Complete)
00400000	Module C:\Users\Desi\Downloads\Compressed\TUGAS\payloads\payload.exe
66B50000	Module C:\Windows\SYSTEM32\WSOCK32.dll
745A0000	Module C:\Windows\system32\apphelp.dll
75710000	Module C:\Windows\system32\KERNELBASE.dll
75880000	Module C:\Windows\system32\SspiCli.dll
75B90000	Module C:\Windows\system32\MSVCRT.dll
75C70000	Module C:\Windows\system32\WS2_32.dll
75D50000	Module C:\Windows\system32\KERNEL32.DLL
77680000	Module C:\Windows\system32\RPCRT4.dll
77A20000	Module C:\Windows\system32\ADVAPI32.dll



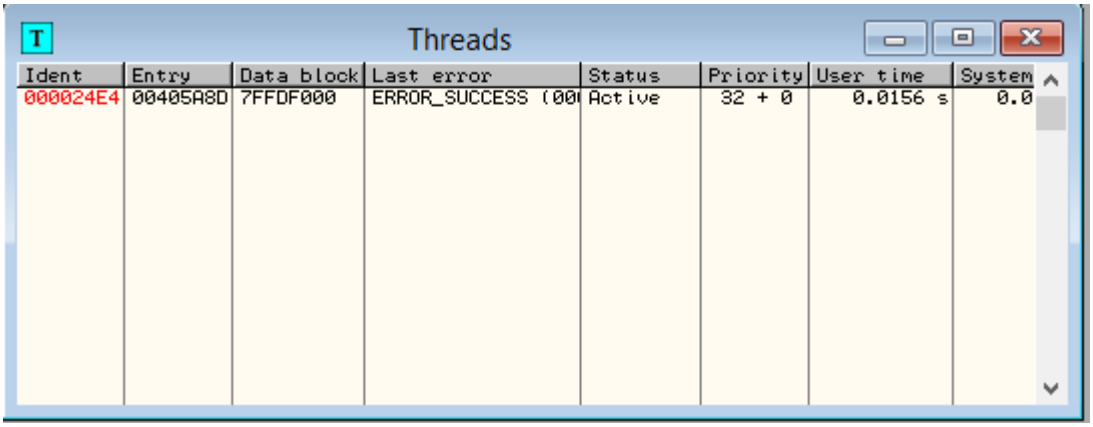
Executable modules

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405A8D	payload	2.2.14	C:\Users\Desi\Downloads\Compressed\TUGAS\payloads
66B50000	00008000	66B510C0	WSOCK32	6.3.9600.16384	C:\Windows\SYSTEM32\WSOCK32.dll
745A0000	000A0000	745A3570	apphelp	6.3.9600.16384	C:\Windows\system32\apphelp.dll
75710000	000D9000	75720820	KERNELBA	6.3.9600.17031	C:\Windows\system32\KERNELBASE.dll
75880000	00023000	75882EC0	SspiCli	6.3.9600.18454	C:\Windows\system32\SspiCli.dll
75B90000	000C3000	75B9E140	MSVCRT	7.0.9600.17415	C:\Windows\system32\MSVCRT.dll
75C70000	0004F000	75C715D0	WS2_32	6.3.9600.16384	C:\Windows\system32\WS2_32.dll
75D50000	00100000	75D5AB10	KERNEL32	6.3.9600.17031	C:\Windows\system32\KERNEL32.DLL
77680000	000D0000	77682650	RPCRT4	6.3.9600.16384	C:\Windows\system32\RPCRT4.dll
77A20000	0007C000	77A21F10	ADVAPI32	6.3.9600.16384	C:\Windows\system32\ADVAPI32.dll
77B90000	00041000	77B913E0	sechost	6.3.9600.16384	C:\Windows\SYSTEM32\sechost.dll
77D60000	00007000	77D61660	NSI	6.3.9600.17415	C:\Windows\system32\NSI.dll
77E30000	0016A000		ntdll	6.3.9600.17031	C:\Windows\SYSTEM32\ntdll.dll



Memory map

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00030000	0000F000				Map	R	R	
0013B000	00002000				Priv	RW Gua	RW	
0013D000	00003000			stack of ma	Priv	RW Gua	RW	
00140000	00004000				Map	R	R	
00150000	00002000				Priv	RW	RW	
00160000	0007E000				Map	R	R	\Device\HarddiskVolume2\Windows\System32\locale.nls
00280000	00018000				Priv	RW	RW	
00400000	00001000	payload		PE header	Imag	R	RWE	
00401000	0000B000	payload	.text	code	Imag	R	RWE	
0040C000	00001000	payload	.rdata	imports	Imag	R	RWE	
0040D000	00008000	payload	.data	data	Imag	R	RWE	
00415000	00001000	payload	.rsrc	resources	Imag	R	RWE	
005E0000	00003000				Priv	RW	RW	
66B50000	00001000	WSOCK32		PE header	Imag	R	RWE	
66B51000	00003000	WSOCK32	.text	code,export	Imag	R	RWE	
66B54000	00001000	WSOCK32	.data	data	Imag	R	RWE	
66B55000	00001000	WSOCK32	.idata	imports	Imag	R	RWE	
66B56000	00001000	WSOCK32	.rsrc	resources	Imag	R	RWE	
66B57000	00001000	WSOCK32	.reloc	relocations	Imag	R	RWE	
745A0000	00001000	apphelp		PE header	Imag	R	RWE	
745A1000	0007A000	apphelp	.text	code,export	Imag	R	RWE	
7461B000	00004000	apphelp	.data	data	Imag	R	RWE	
7461F000	00003000	apphelp	.idata	imports	Imag	R	RWE	
74622000	00017000	apphelp	.rsrc	resources	Imag	R	RWE	
74639000	00007000	apphelp	.reloc	relocations	Imag	R	RWE	
75710000	00001000	KERNELBA		PE header	Imag	R	RWE	
75711000	000C4000	KERNELBA	.text	code,export	Imag	R	RWE	
757D5000	00003000	KERNELBA	.data	data	Imag	R	RWE	
757D8000	00005000	KERNELBA	.idata	imports	Imag	R	RWE	
757DD000	00001000	KERNELBA	.didat		Imag	R	RWE	
757DE000	00004000	KERNELBA	.rsrc	resources	Imag	R	RWE	
757E2000	00007000	KERNELBA	.reloc	relocations	Imag	R	RWE	
75880000	00001000	SspiCli		PE header	Imag	R	RWE	
75881000	0001B000	SspiCli	.text	code,export	Imag	R	RWE	
7589C000	00001000	SspiCli	.data	data	Imag	R	RWE	
7589D000	00002000	SspiCli	.idata	imports	Imag	R	RWE	
7589F000	00001000	SspiCli	.didat		Imag	R	RWE	
758A0000	00001000	SspiCli	.rsrc	resources	Imag	R	RWE	
758A1000	00002000	SspiCli	.reloc	relocations	Imag	R	RWE	
75B90000	00001000	MSVCRT		PE header	Imag	R	RWE	
75B91000	000B5000	MSVCRT	.text	code,export	Imag	R	RWE	
75C46000	00006000	MSVCRT	.data	data	Imag	R	RWE	
75C4C000	00002000	MSVCRT	.idata	imports	Imag	R	RWE	
75C4E000	00001000	MSVCRT	.rsrc	resources	Imag	R	RWE	
75C4F000	00004000	MSVCRT	.reloc	relocations	Imag	R	RWE	
75C70000	00001000	WS2_32		PE header	Imag	R	RWE	
75C71000	00036000	WS2_32	.text	code,export	Imag	R	RWE	
75CA7000	00001000	WS2_32	.data	data	Imag	R	RWE	
75CA8000	00002000	WS2_32	.idata	imports	Imag	R	RWE	
75CAA000	00001000	WS2_32	.didat		Imag	R	RWE	
75CAB000	00011000	WS2_32	.rsrc	resources	Imag	R	RWE	
75CBC000	00003000	WS2_32	.reloc	relocations	Imag	R	RWE	

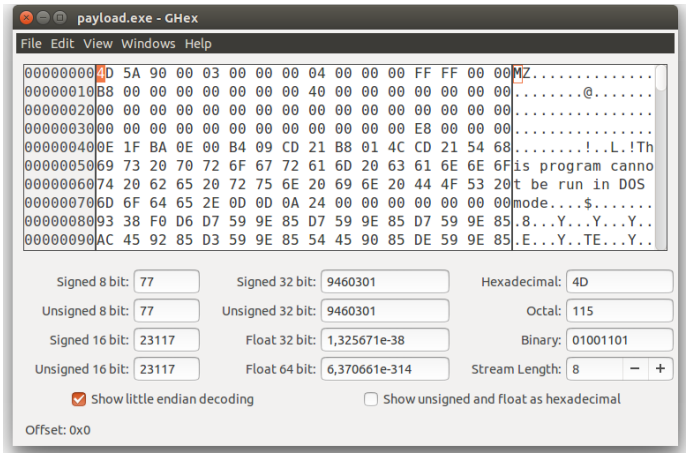


2. Ghex

Berikutnya hasil menggunakan tools Ghex dengan target File payload.exe

- File dengan ekstensi “ payload.exe “

setelah saya membuka file tersebut dengan aplikasi hex ini, saya dapat mengetahui digit kode pada file tersebut yaitu 4D 5A 90 00



Kemudian saya melakukan pencocokan file signature dengan daftar yang ada pada tautan https://en.wikipedia.org/wiki/List_of_file_signatures

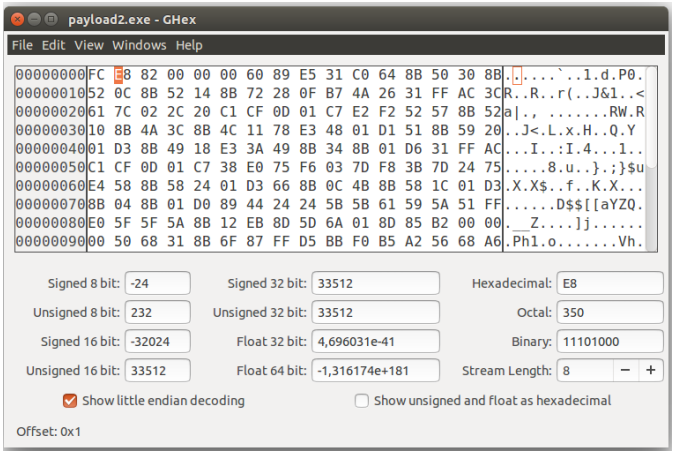
exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A

kemudian saya mencocokan nya pada tabel kode yang ada pada halaman web http://www.garykessler.net/library/file_sigs.html.

4D 5A 90 00 03 00 00 00	MZ.....	
	API	Acrobat plug-in
	AX	DirectShow filter
	FLT	Audition graphic filter file (Adobe)
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF	MZ..... ....ÿÿ	
	ZAP	ZoneAlam data file

ZAP (ZoneAlam data file) yaitu program firewall pribadi (personal). Zone Alam dapat memantau segala aktivitas program-program yang mencurigai,mengirim atau menerima informasi luar Zone Alarm seperti diibaratkan seperti satpam pada komputer anda.

- File dengan ekstensi “ payload2.exe “



file signature dengan daftar yang tidak terdapat pada tautan https://en.wikipedia.org/wiki/List_of_file_signatures dan pada tautan http://www.garykessler.net/library/file_sigs.html juga tidak terdapat file signaturenya.

3. Strings

Tools berikutnya yang di pakai yaitu Strings. Berikut Hasil File payload.exe dengan tools Strings :