

TUGAS KEAMANAN JARINGAN KOMPUTER



NAMA: SYAMSUDIN
NIM: 09011281320012

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Alat

1. GHex
2. OllyDbg

Tugas

- Analisis cara kerja program payload.exe dan payload2.exe

Dasar Teori

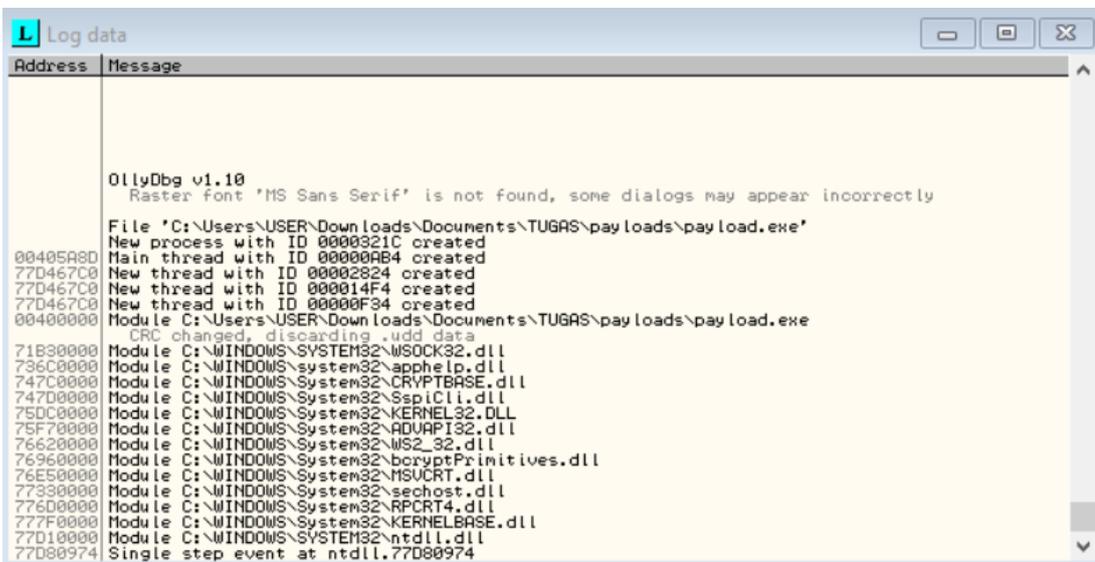
Malware adalah sebuah software atau kode yang diciptakan oleh seseorang dengan tujuan jahat. Sebenarnya Malware itu adalah sebuah software atau program komputer, namun Malware dibuat dengan tujuan untuk merugikan orang lain. Malware dapat mengubah data (menghapus, menyembunyikan, dan mencuri), menghabiskan bandwidth dan juga sumber daya lain tanpa seijin pemilik komputer yang tentunya akan merugikan orang lain. Contoh malware yaitu Virus, Worm, Trojan Horse dan Spyware.

Trojan Horse atau Kuda troya merupakan program perangkat lunak berbahaya yang bersembunyi di dalam program lain. Program ini memasuki komputer dengan bersembunyi di dalam program yang sah, seperti screen saver. Kemudian dia akan menaruh kode ke dalam sistem operasi yang memungkinkan hacker untuk mengakses komputer yang terinfeksi. Kuda troya biasanya tidak menyebar sendiri. Mereka disebar oleh virus, worm, atau perangkat lunak yang diunduh.

Percobaan

“Analisis cara kerja program payload.exe”

Menggunakan tools OllyDbg untuk mendapatkan informasi dari program “payload.exe”



```
Log data
Address  Message
-----  -----
OllyDbg v1.10
Raster font 'MS Sans Serif' is not found, some dialogs may appear incorrectly
File 'C:\Users\USER\Downloads\Documents\TUGAS\payloads\payload.exe'
00405A80 New process with ID 0000321C created
77D467C8 Main thread with ID 00000A84 created
77D467C8 New thread with ID 00002824 created
77D467C8 New thread with ID 000014F4 created
77D467C8 New thread with ID 00000F34 created
00400000 Module C:\Users\USER\Downloads\Documents\TUGAS\payloads\payload.exe
CRC changed, discarding .udd data
71B30000 Module C:\WINDOWS\SYSTEM32\WSOCK32.dll
736C0000 Module C:\WINDOWS\system32\apphelp.dll
747C0000 Module C:\WINDOWS\System32\CRVPTBASE.dll
747D0000 Module C:\WINDOWS\System32\SspiCli.dll
75DC0000 Module C:\WINDOWS\System32\KERNEL32.DLL
75F70000 Module C:\WINDOWS\System32\ADVAPI32.dll
76620000 Module C:\WINDOWS\System32\WS2_32.dll
76960000 Module C:\WINDOWS\System32\bcryptPrimitives.dll
76E50000 Module C:\WINDOWS\System32\MSUCRT.dll
77330000 Module C:\WINDOWS\System32\sechost.dll
776D0000 Module C:\WINDOWS\System32\RPCRT4.dll
777F0000 Module C:\WINDOWS\System32\KERNELBASE.dll
77D10000 Module C:\WINDOWS\SYSTEM32\ntdll.dll
77D80974 Single step event at ntdll.77D80974
```

Figure 1

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	Rw	Rw	
00040000	00016000				Map	R	R	
00095000	0000B000				Priv	Rw	Gua:Rw	
0019B000	00002000				Priv	Rw	Gua:Rw	
0019D000	00003000			stack of ma	Priv	Rw	Gua:Rw	
001A0000	00004000				Map	R	R	
001B0000	00002000				Priv	Rw	Rw	
001F5000	0000B000				Priv	Rw	Gua:Rw	
002B0000	00004000				Priv	Rw	Rw	
002C1000	00003000			data block	Priv	Rw	Rw	
002C4000	00003000			data block	Priv	Rw	Rw	
002C7000	00003000			data block	Priv	Rw	Rw	
002CA000	00001000			data block	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	
00420000	000C1000				Map	R	R	\Device\HarddiskU
00510000	00006000				Priv	Rw	Rw	
0061D000	00002000				Priv	Rw	Gua:Rw	
0061F000	00001000			stack of th	Priv	Rw	Gua:Rw	
00655000	0000B000				Priv	Rw	Gua:Rw	
00695000	0000B000				Priv	Rw	Gua:Rw	
00700000	0000D000				Priv	Rw	Rw	
008FD000	00002000				Priv	Rw	Gua:Rw	
008FF000	00001000			stack of th	Priv	Rw	Gua:Rw	
009FD000	00002000				Priv	Rw	Gua:Rw	
009FF000	00001000			stack of th	Priv	Rw	Gua:Rw	
00B00000	00003000				Priv	Rw	Rw	
68070000	00077000				Imag	R	RwE	
680F0000	0000A000				Imag	R	RwE	

Figure 2

Ident	Entry	Data block	Last error	Status	Priority	User time	System
00000004	00405A80	002C1000	ERROR_SUCCESS (00	Active	32 + 0	0.0156 s	0.0
00000F34	77D467C0	002CA000	ERROR_SUCCESS (00	Active	32 + 0	0.0000 s	0.0
000014F4	77D467C0	002C7000	ERROR_SUCCESS (00	Active	32 + 0	0.0000 s	0.0
00002824	77D467C0	002C4000	ERROR_SUCCESS (00	Active	32 + 0	0.0000 s	0.0

Figure 3

Address	Hex dump	ASCII
0040D000	00 00 00 00 00 00 00 00
0040D008	00 00 00 00 00 00 00 00
0040D010	01 00 00 00 64 00 00 00	0...d...
0040D018	01 00 00 00 01 00 00 00	0...0...
0040D020	01 00 00 00 00 00 00 00	0.....
0040D028	80 C3 C9 01 00 00 00 00	ChF0....
0040D030	E0 0B 41 00 32 00 00 00	0A.R.2...
0040D038	42 00 00 00 4B 00 00 00	B...k...
0040D040	50 00 00 00 50 00 00 00	P...z...
0040D048	5F 00 00 00 62 00 00 00	P...b...
0040D050	63 00 00 00 64 00 00 00	c...d...
0040D058	25 73 3A 20 43 61 6E 6E	%s: Cann
0040D060	6F 74 20 75 73 65 20 63	ot use c
0040D068	6F 6E 63 75 72 72 65 6E	oncurre
0040D070	63 79 20 6C 65 76 65 6C	cy level
0040D078	20 67 72 65 61 74 65 72	greater

Figure 4

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405A00	payload	2.2.14	C:\Users\USER\Downloads\Documents\TUGAS\payloads\
71B30000	00008000	71B31730	WSOCK32	10.0.14393.0 (r	C:\WINDOWS\SYSTEM32\WSOCK32.dll
736C0000	00092000	7370F7C0	apphelp	10.0.14393.0 (r	C:\WINDOWS\system32\apphelp.dll
747C0000	0000A000	747C2A90	CRVPTBAS	10.0.14393.0 (r	C:\WINDOWS\System32\CRVPTBASE.dll
747D0000	0001E000	747DBA20	SspiCli	10.0.14393.576	C:\WINDOWS\System32\SspiCli.dll
75DC0000	000E0000	75DD5F00	KERNEL32	10.0.14393.206	C:\WINDOWS\System32\KERNEL32.DLL
75F70000	00077000	75FE9900	ADVAPI32	10.0.14393.0 (r	C:\WINDOWS\System32\ADVAPI32.dll
76620000	00063000	7663B7E0	WS2_32	10.0.14393.0 (r	C:\WINDOWS\System32\WS2_32.dll
76960000	0005A000	769A2960	bcryptPr	10.0.14393.0 (r	C:\WINDOWS\System32\bcryptPrimitives.dll
76E50000	000E0000	76E856A0	MSUCRT	7.0.14393.0 (rs	C:\WINDOWS\System32\MSUCRT.dll
77390000	00041000	773471C0	sechost	10.0.14393.0 (r	C:\WINDOWS\System32\sechost.dll
776D0000	000C1000	776F14E0	RPCRT4	10.0.14393.0 (r	C:\WINDOWS\System32\RPCRT4.dll
777F0000	001A1000	778AE600	KERNELBA	10.0.14393.206	C:\WINDOWS\System32\KERNELBASE.dll
77D10000	00183000		ntdll	10.0.14393.206	C:\WINDOWS\SYSTEM32\ntdll.dll

Figure 5

Address	Hex dump	ASCII	Registers (FPU)
77331000	90 68337740		EAX 00405A80 payload.<ModuleEntryPoint>
77331005	7D 34		ECX 00000000
77331007	77 60		EDX 00000000
77331009	813477 14823677		EBX 002BE000
77331010	0000		ESP 0019FFF0
77331012	0000		EBP 00000000
77331014	0000		ESI 00000000
77331016	0000		EDI 00000000
77331018	0000		EIP 77D00974 ntdll.77D00974
7733101A	0000		C 0 ES 002B 32bit 0(FFFFFFFF)
7733101C	0000		F 0 DS 0023 32bit 0(FFFFFFFF)
7733101E	0000		A 0 SS 002B 32bit 0(FFFFFFFF)
77331020	7A 67		Z 0 DS 002B 32bit 0(FFFFFFFF)
77331022	3377 01		S 0 FS 0053 32bit 2C1000(FFF)
77331025	0000		T 0 GS 002B 32bit 0(FFFFFFFF)
77331027	0000		D 0
77331029	0000		O 0 LastErr ERROR_SUCCESS (00000000)
7733102B	0000		EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
7733102D	0000		ST0 empty 0.0
7733102F	006A 02		ST1 empty 0.0
77331032	0108		ST2 empty 0.0
77331034	0000		ST3 empty 0.0
77331036	0000		ST4 empty 0.0
[40773368]=???			
00400000	00 00 00 00 00 00 00 00	0019FFF4 00405A80 payload.<ModuleEntryPoint>
00400010	01 00 00 00 64 00 00 00	...d...	0019FFF8 00000000
00400018	01 00 00 00 01 00 00 00	0...0...	0019FFFC 00000000
00400020	01 00 00 00 00 00 00 00	0.....	
00400028	80 C3 C9 01 00 00 00 00	Chf0...	
00400030	E0 06 41 00 32 00 00 00	00A.2...	
00400038	42 00 00 00 48 00 00 00	B...K...	
00400040	50 00 00 00 5A 00 00 00	P...Z...	
00400048	5F 00 00 00 62 00 00 00	...d...	
00400050	63 00 00 00 64 00 00 00	...b...	
00400058	25 73 3A 20 43 61 6E 6E	%s: Cann	
00400060	6F 74 20 75 73 65 20 63	ot use c	
00400068	6F 6E 63 75 72 72 65 6E	oncurren	
00400070	63 79 20 6C 65 76 65 6C	cy level	
00400078	20 67 72 65 61 74 65 72	greater	

Figure 6

Menggunakan tools GHex untuk mendapatkan informasi dari program “payload.exe”

```
root@sam-VirtualBox:/home/sam/Downloads/TUGAS/payloads# ls
html payload2.exe payload.exe
root@sam-VirtualBox:/home/sam/Downloads/TUGAS/payloads# ghex payload.exe
```

Figure 7

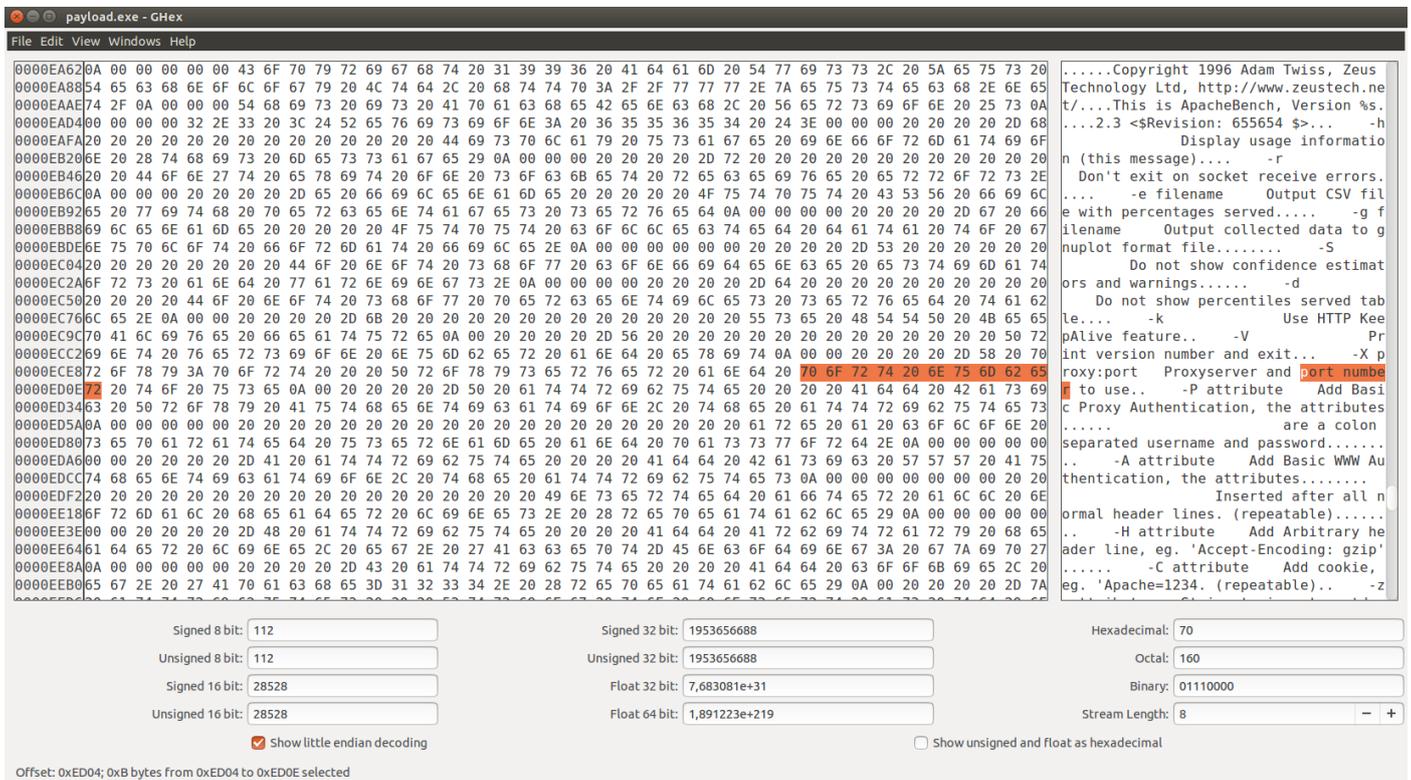


Figure 14

Dari kedua tools yang sudah digunakan yaitu OllyDbg dan GHEx, diketahui bahwa program “payload.exe” beroperasi pada system operasi Windows, hal ini bisa diketahui dari melihat ekstensi dari program payload yaitu .exe, selain itu juga bisa dilihat pada (Figure 8) terdapat string “MZ” dengan offset 0x0 pada sky dum yang merupakan salah satu ciri khas dari setiap file .exe.

Program “payload.exe” beroperasi menggunakan port karena terdapat displayed string “port number” pada sky dum (Figure 14) yang mana port ini akan digunakan sebagai portal dalam melakukan eksploitasi, program ini menggunakan socket sebagai interface jaringan komunikasinya (Figure 13), socket sendiri terdiri dari beberapa elemen yaitu Protokol, Local IP, Local Port, Remote IP, Remote Port. Dikarenakan menggunakan socket berarti akan terjadi pertukaran data secara continue atau terus menerus. Adapun protocol yang digunakan dalam komunikasinya adalah protocol TCP (The Transmission Control Protocol) (Figure 12).

Pada (Figure 5) diketahui bahwa program "payload.exe" executable pada beberapa modul di komputer victim, yaitu pada WSOCK32 apphelp, CRYTBAS, SspiCli, KERNEL32, ADVAPI32, WS2_32, bryptOr, MSVCRT, sechost, RPCRT4, KERNELBA, ntdll. Pada modul atau dll seperti WSOCK32 yang menyediakan WinSock API. WinSock mendukung multiple stack protocol, interface, dan service provider. Ini yang dieksploit oleh program “payload.exe”. Dengan dapatnya melakukan eksekusi pada modul penting tersebut memungkinkan computer victim untuk dilakukan eksploitasi dan juga spy karena dapat melakukan remote access.

“Analisis cara kerja program payload2.exe”

Menggunakan tools OllyDbg untuk mendapatkan informasi dari program “payload2.exe”

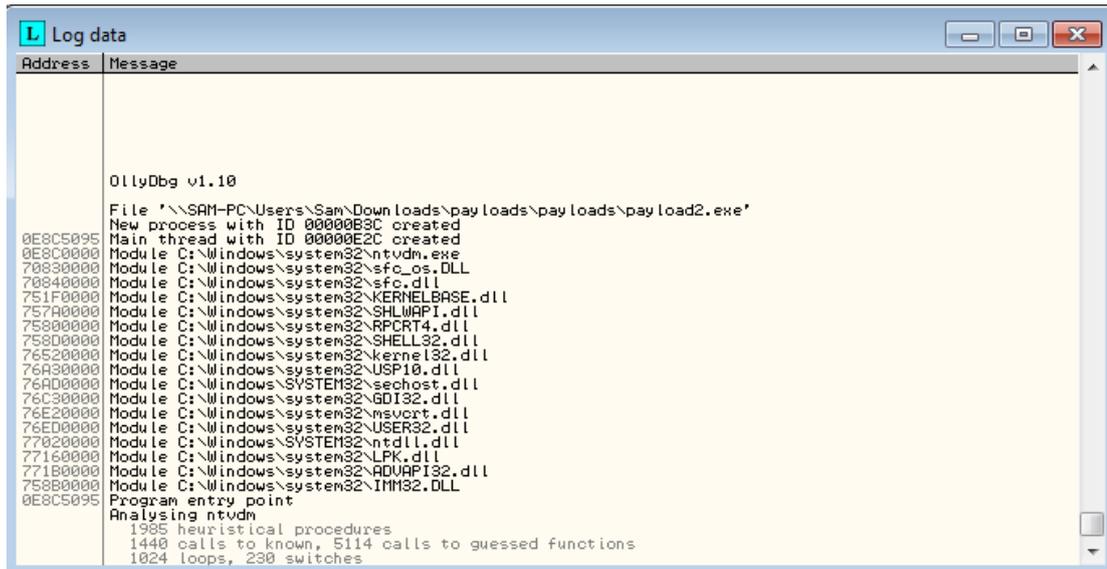


Figure 15

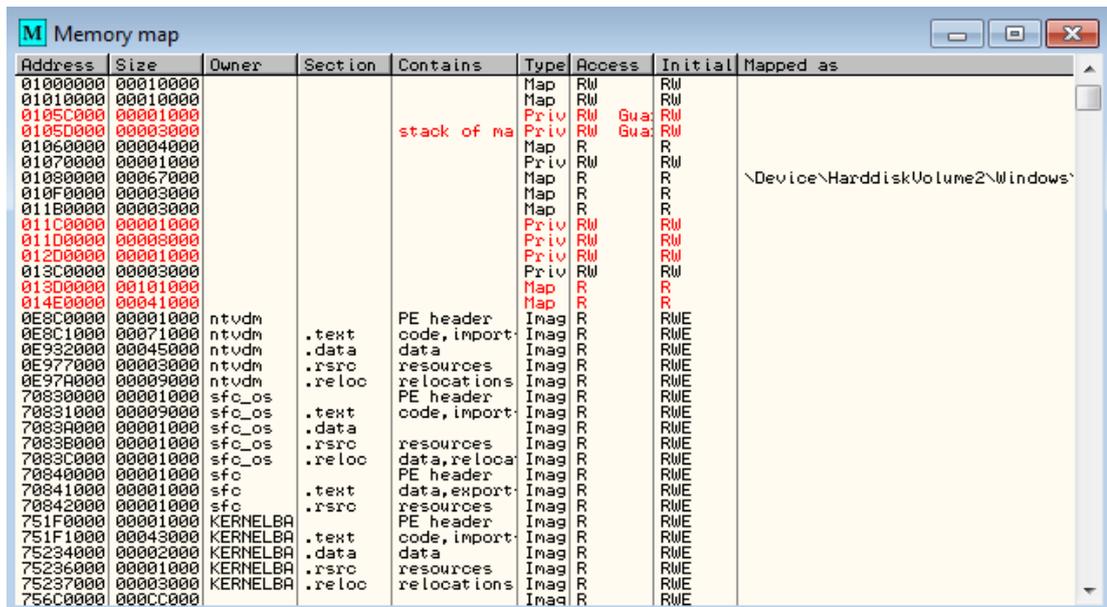


Figure 16

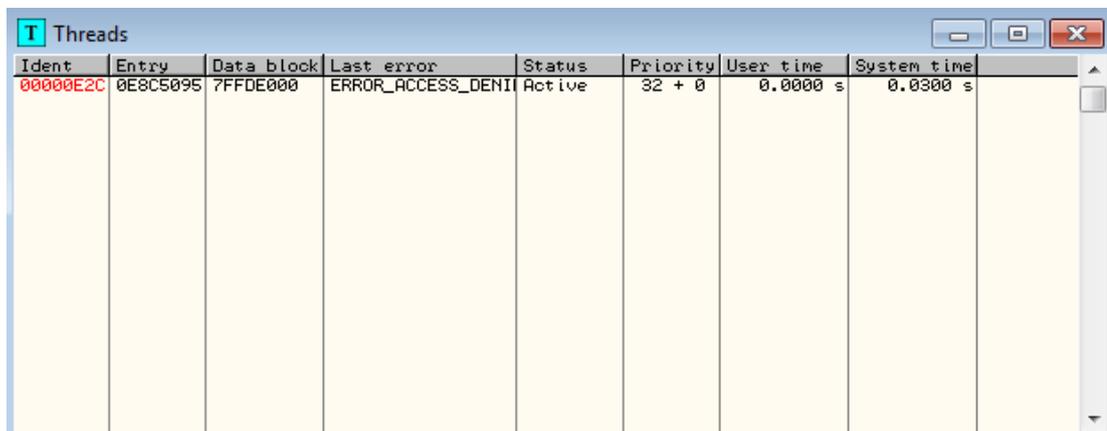


Figure 17

Base	Size	Entry	Name	File version	Path
0E8C0000	000C3000	0E8C5095	ntvdm	6.1.7600.16385	C:\Windows\system32\ntvdm.exe
70830000	0000D000	70831392	sfc_os	6.1.7600.16385	C:\Windows\system32\sfc_os.DLL
70840000	00003000		sfc	6.1.7600.16385	C:\Windows\system32\sfc.dll
751F0000	0004A000	751F709D	KERNELBA	6.1.7600.16385	C:\Windows\system32\KERNELBASE.dll
75700000	00057000	7570B24A	SHLWAPI	6.1.7600.16385	C:\Windows\system32\SHLWAPI.dll
75800000	000A1000	7583AFD4	RPCRT4	6.1.7600.16385	C:\Windows\system32\RPCRT4.dll
758B0000	0001F000	758B1355	IMM32	6.1.7600.16385	C:\Windows\system32\IMM32.DLL
758D0000	00C49000	7594D45A	SHELL32	6.1.7600.16385	C:\Windows\system32\SHELL32.dll
76520000	00004000	765710C5	kernel32	6.1.7600.16385	C:\Windows\system32\kernel32.dll
76A30000	0000D000	76A647D7	USP10	1.0626.7600.16385	C:\Windows\system32\USP10.dll
76AD0000	00019000	76AD4975	sechost	6.1.7600.16385	C:\Windows\SYSTEM32\sechost.dll
76C30000	0004E000	76C3EC49	GDIP32	6.1.7600.16385	C:\Windows\system32\GDIP32.dll
76E20000	000AC000	76E29472	msvcrt	7.0.7600.16385	C:\Windows\system32\msvcrt.dll
76ED0000	000C9000	76EEF7C9	USER32	6.1.7600.16385	C:\Windows\system32\USER32.dll
77020000	0013C000		ntdll	6.1.7600.16385	C:\Windows\SYSTEM32\ntdll.dll
77160000	0000A000	7716136C	LPK	6.1.7600.16385	C:\Windows\system32\LPK.dll
771B0000	0000A000	771D2DD9	ADVAPI32	6.1.7600.16385	C:\Windows\system32\ADVAPI32.dll

Figure 18

Address	Hex dump	ASCII	Disassembly	Registers (FPU)
76AD1000	8F	???	Unknown command	EAX: 76571162 kernel32.BaseThreadInitThunk
76AD1001	1F		Modification of	EAX: 00000000
76AD1002	2175 00		POP DS	EDX: 0E8C5095 ntvdm.<ModuleEntryPoint>
76AD1005			AND DWORD PTR SS:[EBP],ESI	EBX: 7FFDF000
76AD1007	00A401 54760000		ADD BYTE PTR DS:[EAX],AL	ESP: 0105FC08
76AD100E	0000		ADD BYTE PTR DS:[EAX],AL	ESI: 00000000
76AD1010	^76 F1		JBE SHORT sechost.76AD1003	EDI: 00000000
76AD1012	56		PUSH ESI	EIP: 0E8C5095 ntvdm.<ModuleEntryPoint>
76AD1013	<76 7D		JBE SHORT sechost.76AD1092	C 0 ES 0023 32bit 0(FFFFFFFF)
76AD1016	56		PUSH ESI	F 1 CS 001B 32bit 0(FFFFFFFF)
76AD1017	<76 00		JBE SHORT sechost.76AD1019	A 0 SS 0023 32bit 0(FFFFFFFF)
76AD1019	0000		ADD BYTE PTR DS:[EAX],AL	Z 1 DS 0023 32bit 0(FFFFFFFF)
76AD101B	0067 05577600		ADD BYTE PTR DS:[EDI+765705],DH	S 0 FS 0036 32bit 7FFDE000(FFF)
76AD1021	0000		ADD BYTE PTR DS:[EAX],AL	O 0 GS 0000 NULL
76AD1023	00C2		ADD DL,AL	D 0
76AD1025	691F 756B6B1F		IMUL EBX, DWORD PTR DS:[EDI],1F6B6B75	O 0 LastErr ERROR_ACCESS_DENIED (00000000)
76AD102D	<75 00		JNZ SHORT sechost.76AD102D	EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
76AD102F	00A8 B81F7597		ADD BYTE PTR DS:[EAX+7751FB8],CH	ST0 empty 0.0
76AD1035	<7F 1F		JG SHORT sechost.76AD1056	ST1 empty 0.0
76AD1037	<75 5B		JNZ SHORT <&API-MS-Win-Core-ProcessThre	ST2 empty 0.0
76AD1039	6C		INS BYTE PTR ES:[EDI],DX	ST3 empty 0.0
			I/O command	ST4 empty 0.0
				ST5 empty 0.0
0E932000	8C 16 2C 0E 01 00 00 00	..t.00...	0105FC08 76571174 RETURN to kernel32.76571174	
0E932008	4E E6 40 BB B1 19 BF 44	Np00004D	0105FC0C 7FFDF000	
0E932010	E0 AF 24 0E 00 00 00 00	<>>000...	0105FC10 0105FC50	
0E932018	E0 AF 24 0E 01 01 00 00	<>>000...	0105FC14 7707B3F5 RETURN to ntdll.7707B3F5	
0E932020	00 00 00 00 00 00 00 00	0105FC18 7FFDF000	
0E932028	00 10 00 00 00 00 00 00	0105FC1C 760C1551 SHELL32.760C1551	
0E932030	00 00 00 00 00 00 00 00	0105FC20 00000000	
0E932038	00 00 00 00 02 00 00 00	...@....	0105FC24 00000000	
0E932040	01 00 00 00 00 00 00 00	0105FC28 00000000	
0E932048	00 00 00 00 00 00 00 00	0105FC2C 7FFDF000	
0E932050	00 00 00 00 00 00 00 00	0105FC30 00000000	
0E932058	00 00 00 00 02 00 00 00	...@....	0105FC34 00000000	
0E932060	02 00 00 00 00 00 00 00	@.....	0105FC38 0105FC1C	
0E932068	00 00 00 00 00 00 00 00	0105FC3C 00000000	
0E932070	00 00 00 00 00 00 00 00	0105FC40 FFFFFFFF End of SEH chain	
0E932078	00 00 00 00 00 00 00 00	0105FC44 7703D74D SE handler	
0E932080	00 00 00 00 00 00 00 00	0105FC48 000EEC99	
0E932088	00 00 00 00 00 00 00 00	0105FC4C 00000000	
0E932090	00 00 00 00 00 00 00 00	0105FC50 0105FC68	

Figure 19

Menggunakan tools GHex untuk mendapatkan informasi dari program “payload2.exe”

```
root@sam-VirtualBox: /home/sam/Downloads/TUGAS/payloads# ls
html payload2.exe payload.exe
root@sam-VirtualBox: /home/sam/Downloads/TUGAS/payloads# ghex payload2.exe
```

Figure 20

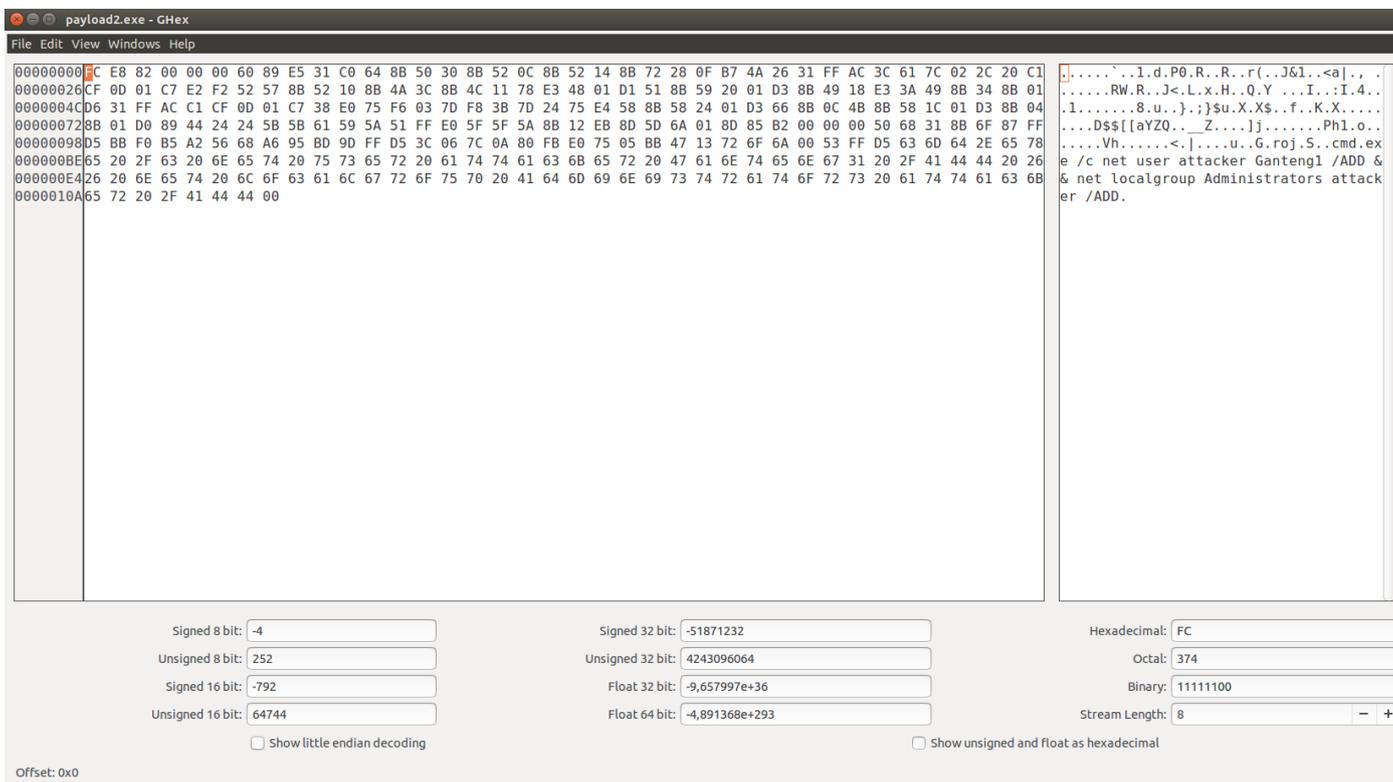


Figure 21

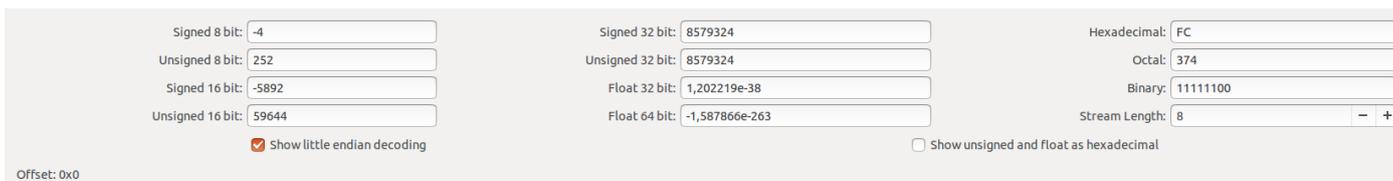


Figure 22

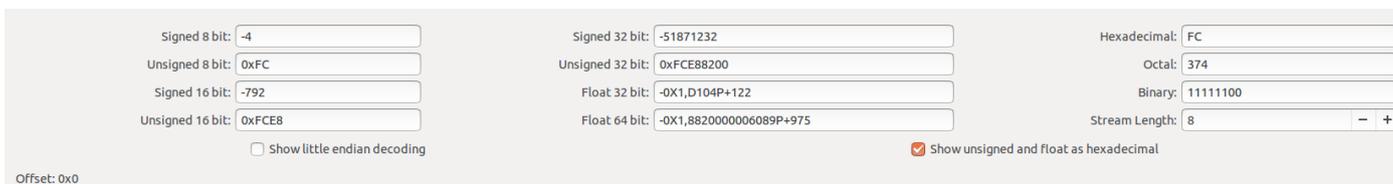


Figure 23

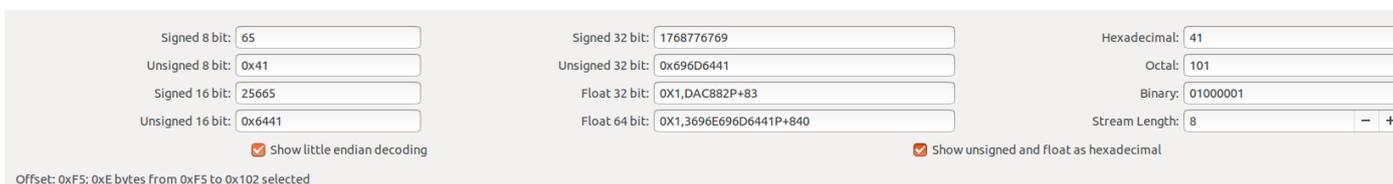


Figure 24

Pada (Figure 18) diketahui bahwa program "payload2.exe" executable pada beberapa modul di komputer victim, yaitu pada ntdm, sfc_os, sfc, KERNELBA, SHLWAPI, RPCRT4, IMM32, SHELL32, kernel32, USP10, sechost, GDI32, msvort, USER32, ntdll, LPK, ADVAPI32. Melihat dari modul-modul yang executable seperti USER32 dan juga melihat dari displayed string "Administrator attacker" pada sky dum (Figure 21) malware payload2.exe ini dapat melakukan manipulasi atau eksploitasi system administrator pada komputer victim.

Daftar Pustaka

- Anonim, 2013, Apa itu Socket dan apa Fungsinya dalam Jaringan?, [online], (<http://akfive.blogspot.co.id/2013/04/apa-itu-socket-dan-apa-fungsinya-dalam.html>, diakses tanggal 5 April 2017)
- Anonim, 2014, Perbedaan Malware, Virus, Trojan, Spyware, dan Worm, [online], (<https://www.maxmanroe.com/perbedaan-malware-virus-trojan-spyware-dan-worm.html>, diakses tanggal 5 April 2017)
- Anonim, 2015, Cara mencegah dan menghapus virus dan malware lainnya, [online], (<https://support.microsoft.com/id-id/help/129972/how-to-prevent-and-remove-viruses-and-other-malware>, diakses tanggal 5 April 2017)