

Keamanan Jaringan Komputer Analisis Payload



**Disusun Oleh :
Nama : Imam Mustofa
NIM : 09011181320028**

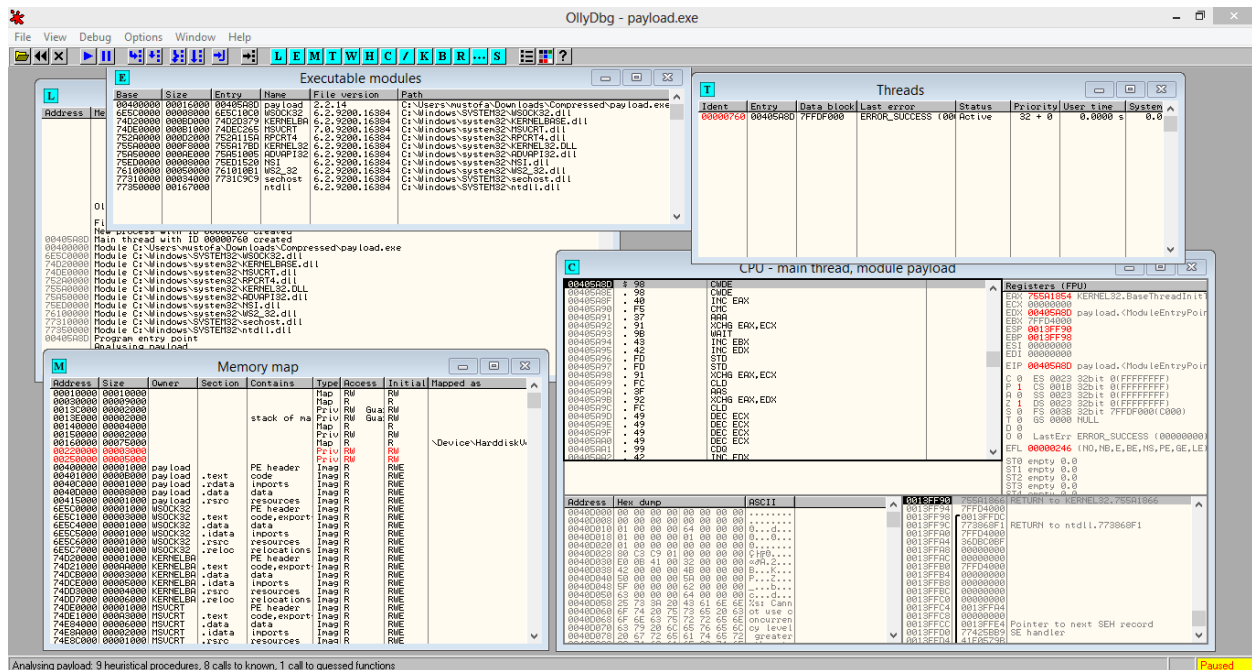
**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2015**

**Laporan Praktikum
Mikroprosesor dan Mikrokontroller**



Disusun Oleh :
Nama : Imam Mustofa
NIM : 0901181320028

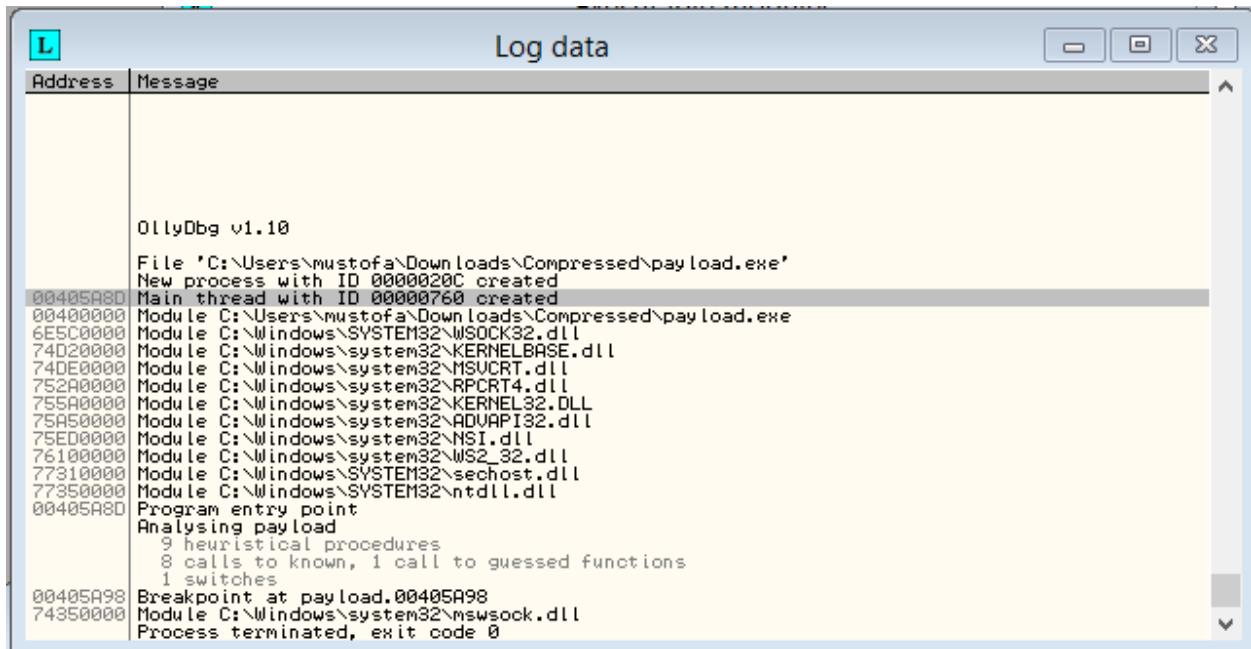
SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017



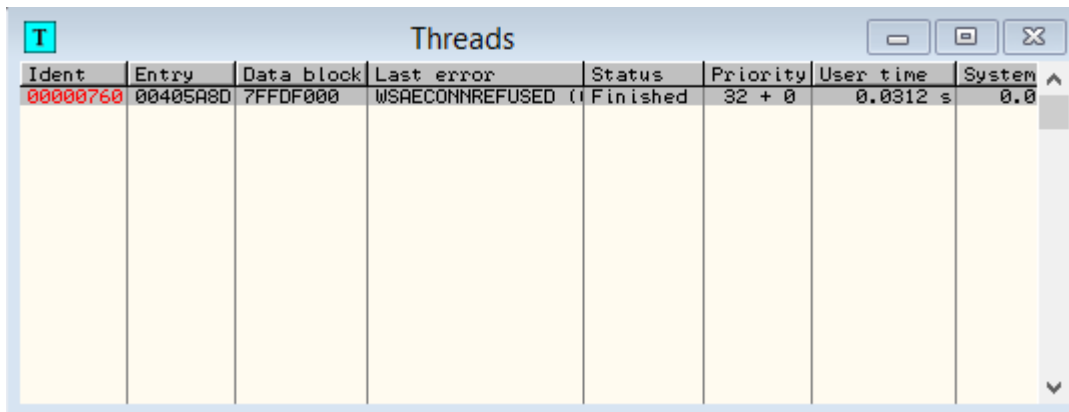
Dari data yang dibuka pada aplikasi diatas didapatkan pembacaan terhadap thread atau ancaman. Secara terpecah datanya akan ditampilkan sebagai berikut.

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00020000	00001000				Priv	RWE	RWE	
00030000	00009000				Map	R	R	
0013C000	00002000			stack of ma	Priv	RW	Guar	RW
0013E000	00002000				Priv	RW	Guar	RW
00140000	00004000				Map	R	R	
00150000	00002000				Priv	RW	RW	
00160000	00075000				Map	R	R	\\Device\HarddiskU
00220000	00003000				Priv	RW	RW	
00250000	00019000				Priv	RW	RW	
00400000	00001000	payload		PE header	Imag	R	RWE	
00401000	0000B000	payload	.text	code	Imag	R	RWE	
0040C000	00001000	payload	.idata	imports	Imag	R	RWE	
00415000	00001000	payload	.data	data	Imag	R	RWE	
00420000	002D5000	payload	.rsrc	resources	Imag	R	RWE	
6E5C0000	00001000	WSOCK32		PE header	Imag	R	RWE	
6E5C1000	00003000	WSOCK32	.text	code,export	Imag	R	RWE	
6E5C4000	00001000	WSOCK32	.data	data	Imag	R	RWE	
6E5C5000	00001000	WSOCK32	.idata	imports	Imag	R	RWE	
6E5C6000	00001000	WSOCK32	.rsrc	resources	Imag	R	RWE	
6E5C7000	00001000	WSOCK32	.reloc	relocations	Imag	R	RWE	
74350000	00001000	msocket		PE header	Imag	R	RWE	
74351000	00030000	msocket	.text	code,export	Imag	R	RWE	
74381000	00010000	msocket	SANONTCP	code	Imag	R	RWE	
74391000	00002000	msocket	.data	data	Imag	R	RWE	
74393000	00002000	msocket	.idata	imports	Imag	R	RWE	
74395000	00001000	msocket	.rsrc	resources	Imag	R	RWE	
74396000	00004000	msocket	.reloc	relocations	Imag	R	RWE	
74D10000	00001000	KERNELBA		PE header	Imag	R	RWE	
74D21000	000A0000	KERNELBA	.text	code,export	Imag	R	RWE	

Gambar diatas menampilkan data map dari memori komputer. Didalamnya terdiri alamat, ukuran, pemilih, section, pemuatan, type, dan seterusnya.



Log dari proses yang dilakukan oleh aplikasi tercatat pada gambar bagian diatas.



Thread diatas didapatkan active ketika aplikasi dijalankan, memiliki berbagai informasi yang dibutuhkan sebagai acuan pemrosesan seperti priority dan data block

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405A80	payload	2.2.14	C:\Users\mustofa\Downloads\Compressed\payload.exe
6E5C0000	00008000	6E5C10C0	WSOCK32	6.2.9200.16384	C:\Windows\SYSTEM32\WSOCK32.dll
74350000	0004A000	743510A1	mswsock	6.2.9200.16384	C:\Windows\system32\mswsock.dll
74D20000	000BD000	74D20379	KERNELBA	6.2.9200.16384	C:\Windows\system32\KERNELBASE.dll
74DE0000	000B1000	74DEC265	MSUCRT	7.0.9200.16384	C:\Windows\system32\MSUCRT.dll
752A0000	000D2000	752A115A	RPCRT4	6.2.9200.16384	C:\Windows\system32\RPCRT4.dll
755A0000	000F8000	755A17BD	KERNEL32	6.2.9200.16384	C:\Windows\system32\KERNEL32.DLL
75A50000	000AE000	75A51005	ADVAPI32	6.2.9200.16384	C:\Windows\system32\ADVAPI32.dll
75ED0000	00008000	75ED1520	NSI	6.2.9200.16384	C:\Windows\system32\NSI.dll
76100000	00050000	761010B1	WS2_32	6.2.9200.16384	C:\Windows\system32\WS2_32.dll
77310000	00034000	7731C9C9	sechost	6.2.9200.16384	C:\Windows\SYSTEM32\sechost.dll
77350000	00167000		ntdll	6.2.9200.16384	C:\Windows\SYSTEM32\ntdll.dll

Bagian-bagian data informasi diatas akan ditemukan pada payload yang kedua, hanya saja data yang ada didalamnya seperti jenis dan aktivitas yang ada kemungkinan memiliki perbedaan.

OlyDbg - payload2.exe

File View Debug Options Window Help

Log

Threads

Executable modules

CPU - main thread, module ntdm

Registers (FPU)

Memory map

Analysing ntdm: 1561 heuristic procedures, 1472 calls to known, 2655 calls to guessed functions

Paused

The screenshot displays the OlyDbg application interface. At the top, there's a menu bar (File, View, Debug, Options, Window, Help) and a toolbar with navigation icons. The main area is divided into several panes:

- Log:** Shows a list of events, including file operations and process creation.
- Threads:** A table with columns for IDent, Entry, Data block, Last error, Status, and Priority. It shows a single active thread.
- Executable modules:** A table listing loaded modules with columns for Base, Size, Entry, Name, File version, and Path. It includes system DLLs like ntdm, sfc_os, and kernel32.
- CPU - main thread, module ntdm:** Shows assembly instructions with their addresses and hex values.
- Registers (FPU):** Displays the current state of CPU registers like EAX, ECX, EDI, etc.
- Memory map:** A table showing memory segments with columns for Address, Size, Owner, Section, Contains, Type, Access, Initial, and Mapped as.

At the bottom, a status bar indicates the analysis progress: "Analysing ntdm: 1561 heuristic procedures, 1472 calls to known, 2655 calls to guessed functions". A "Paused" button is visible in the bottom right corner.

Bahan-bahan diatas dapat dijadikan percobaan, analisis data, dan acuan terhadap ancaman atau malware yang digunakan.