Nama : Muhammad Fachrurroji Ilham Saputra

Nim : 09011181322025

Analisa malware

Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub program atau data yang bertujuan jahat dalam sebuah file elektronik.

Ada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.

• Sebagai bahan praktek, digunakan bahan yang telah diberikan berupa payload.exe, dan payload2.exe . tools yang digunakan untuk menganalisa bahan yang diberikan berupa ghex, hexdump, strings, ollydbg, dan ida pro.Ghex berguna untuk debugging masalah dengan kode, dan untuk memuat data dari file, melihat dan mengedit hex dan ascii.

Pertama yang dilakukan membuka file yang diberikan :

Terdapat dua file pada gambar dibawah berupa payload.exe dan payloads2.exe



Pada langkah selanjutnya kita melakukan terlebih dahulu pada payload.exe. dengan cara klik kanan pada file tersebut dan open with dengan ghex maka akan tampil seperti gambar dibawah yang menampilkan kode yang diblok berwarna hijau tersebut.

payload.exe -	GH	ex.																																	•	90
File Edit View	Nind	lows.	Help																																	
90090001F09 9009001F09 9009003E09 900900506E 900906506E	5A 00 00 6E 00	90 00 0E 6F 00	00 00 1F 74 00	03 00 BA 20 93	00 0E 62 38	90 00 65 F0	8 80 84 20 06	84 80 89 72 07	00 00 CD 75 59	00 21 6E 9E	00 00 88 20 85	FF 00 01 69 D7	FF 00 4C 6E 59	00 00 CD 20 9E	00 00 21 44 85	88 00 54 4F D7	00 00 68 53 59	00 00 69 20 9E	00 00 73 60 85	80 80 20 6F AC	80 80 70 64 45	00 00 72 65 92	88 6F 2E 85	48 80 67 80 03	00 00 72 00 59	00 00 61 6A 9E	00 00 60 24 85	00 20 00 54	00 E8 63 00 45	00 00 61 00 90	M2 nnot be run 	1L n in	. ! Thi DOS (s progr tode	ram (
00000005800 0000005800 0000005800 0000011700 0000013500	DE 85 00 00 00 00 00 00	59 DF 00 00 00 00	9E 59 00 00 60	85 9E 00 E0 00 01	88 85 00 00 00 00	46 83 90 9F 90 90 90	94 7A 90 91 40 10	85 AE 80 80 80 80	DC 85 89 81 80 80 80	59 FF 88 86 10 80	9E 59 00 00 00 00	85 9E 08 08 08 08	88 85 69 89 69 60	46 18 00 00 10 02	9A 5F 50 00 00 00	85 98 45 00 00 00	04 85 00 40 04 00	59 06 00 00 00	9E 59 4C 00 00 00	85 9E 01 00 10	07 85 84 80 80 80 80	59 52 89 89 89 89 89 89 89	9F 69 47 00 10	85 63 71 80 80 80	1E 68 D6 5A 04 06 06	59 D7 49 00 00 00	9E 59 00 00 00	85 9E 00 00 10	54 85 98 10 00 00	51 99 99 99 99 90 90 90		Y	FY	YRict	Y1	0
1000015510 10000174C8 1000019300 1000018200 1000018200	00 07 10 00 00 00 00	00 00 00	00 00 00 00	00 00 00 00 00	00 00 00 00 10	90 90 90 90	80 80 80 80 80 80 80 80 80	60 60 60 60 60 60	90 90 90 90 90	00 00 00 00 00	66 66 68 68 68 68 60	68 68 68 68 68 68	00 00 00 00	00 00 00 00 00	00 00 00 00 00 2E 00	00 00 00 74 00	00 00 00 65 00	00 00 00 00 00 00 00 00 00	6C 80 80 81 74 80	60 60 80 20	80 80 80 80 80 80	60 60 60 60 60	78 88 88 88 88 66 66 68	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 72	00 00 00 00 64	00 00 00 00 61	58 68 68 10 74	61 68 88 60 61	00 00 00 00			tex	LX 	data	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1000022E00 1000022E00 1000022E00 1000022E00 1000026008 1000028800	40 00 10 00	0F 2E 00 01 00	64 60 60 60	60 61 00 00 00	00 74 00 00 00	61 00 00 00	00 00 40 00 00	00 00 00 00 00	00 00 00 00 00	10 50 00 80 80	00 70 2E 00 00	00 00 72 00 00	00 73 00 00	00 72 00 90	00 D0 63 00 00	00 00 40 00	00 00 00 00	00 00 00 00 00	40 C8 40 90	90 90 87 80 89	80 80 80 80	00 00 00 00	00 00 00 00 00	00 50 60 60	00 01 68 08	00 00 00 00	00 00 00 00 00	00 00 10 00 00	40 00 00 00 00	00 00 00 00 00	.e.data	\prs	rc(8P		A 14 14 14 14
		sig	ved 8	bt	q										13	Sign	et 32	bit:	102	4											Hexatecima	00				
	14	Insig	ud B	bil:	a	_	_	_	-						. Lin	sign	ed 32	bitz	102	4	_	_	_	_							Octa	000	0			
		Sign	ed 10	bt	102	4										FIG	at 32	bit:	1.43	493	0e-43	E.									Binary	000	000000			
	Ur	nëgre	ed 18	bit	102	4											6.64	bit:	1,29	1023	7 0 -30	14				_					Streem Length				1	- 1
Offset: 0x7: 0x8 t	ytes	: tron	0x0	E to D) shi 17 se	ow It	tie e	idian	deco	ding																• 5	how	unsiq	net i	013	loat as hexadecima	¢.				

Langkah selanjutnya kita dapat mencari di list file signature, dapat dilihat dari gambar dibawah terdapat file yaitu file mz. File MZ ialah jenis file yang hanya tersedia untuk windows dan berjenis aplikasi.

C O www.garyk	essler	net	rtibr	ier y/	film_	iii ga	him	1				- 17							
									311.3	Statistical value popularization and scattering test wate (Also see "MILES" and "MV2C" signatures)	MZ	1.07							
	4.0	56	32	43					MLS	NV2C Milestones v2.1a project management and scheduling software (Also see "MILES" and "MV214" signatures)									
	4D CO	5A M. D	DLL.	DR	6, EX	(E, 1	917, (yts, (ACM AX CPL FON OCX OLB SCR VBX VXD, 386	Visidows DOS executable file (See The MZ_EXE.File Format page for the insustance of an EXE file, with coverage of NE, TLINK, PE, self-extincting archives, and more.) Note: MZ_are the initials of Mark Zhikowski, designer of the DOS executable file format. MS and/so compression manager driver Library cache file Control panel application Feat file ActiveX or OLE Custom Control OLE object library Sereen saver VisualBASIC application Windows virtual device drivers									
	ΗĐ.	38	90	10	-99	110	.00		API AX FLT	Acrobat plug-in. DirectShew filter Audition graphic filter file (Adobe)									
	4D 04	5A 00	90 00	00	03 79	00 F7	08	00	ZAP	Zone Alam data file									
	4D 74	69 20	63 43	72 29	6F 43	73 28	6F 28	66	PDB	HL⊂rnoor 1. C/C++ Microsoft C++ debugging symbols file									
	4D 74 20	69 20 53	63 56 74	72 69 75	6F 73 64	73 75 69	6F 61 6F	66 62 20		Microsof t Vismal Studio									

Berikut kita lakukan file yang kedua yaitu payloads2.exe. gambar dibawah ini menunjukan hasil dari kode hex pada file payloads2.exe



Kita dapat melakukkan perintah diterminal untuk menampilkan file strings payload.exe, maka yang akan tampil seperti gambar dibawah.



Kita dapat melakukkan perintah tersebut pada dua file yaitu strings payload.exe dan payload2.exe Pada gambar dibawah terdapat hasil convert file tersebut dalam assembly.

Functions endow 67: X Functions name 7 sole, 199301 7 sole, 199301 7 sole, 199309 7 sole, 199309 7 sole, 199309	IN INCLASS
4 2	<pre>cont news the state of the</pre>

Terdapat graph alur pada payload.exe

WinGraph32 - Call flow of payload.exe	
File View Zoom Move Help	
0 4 4 2 7 + + C 8 2 8 X	
THE ALL ALL ALL ALL ALL ALL ALL ALL ALL AL	42,4949 40,4587 611 40,4925 1
	61.4H21

Pada gambar dibawah inilah hasil dari hex.

Functions window	D # X	ID.4	View-A	0	18		to: Vitere-L		11	0	Stort	int.	0		Dura		1.63	Toports	0	F	Equite	0
ction name	0.04	01221	10	18 51	51	67 15	F8 17	41	-	96 8	2.78		88 29	H.PQ	1	15.)-4.						
7 o.b. 436310	0.04	81241	E3 (18 A1	EF	E8 04	AC 00	00	68 8	E# 5	F 40	1.7E	87.94	2-86	F+L8	12.0"++						
ad allering	020	01051	CB (N 00	83	C4 8	38 53	58	68.4	4C 4	8 41	BF	E# F0		8558	il∰#+Fn						
2 at 10500	0.04	81261	99 :	19 01	48	55 K	F2 45	49	80 1	85 A	IC 40	1.41	92 52	·*-1	WE.*	31.0MR						
SAD_101007	0 day	81871	50 1	10 55	FA	51.5	E8 44	40	00.1	88.5	IE 55	90	80 46	6760	DHED'T'	E.						
SUD_10404-	BrEn	18918	FE I	ID 40	FB	58 51	68 14	82	49.1	88.5	2 E	DE.	49 90	0.50	rine							
0.00_404050	8.61	11601		15 61	187	HF 182	62 88		88 2	15 1	10 61	-14	** *	- 3* -		58-9						
SUD_404E30	0.04	M1001	DL I	ID 40	82	CH 0:	83 78	24		17.4	10 10	.44	88 23		-24.9	£1						
🖉 start	and a second	111001	CR I	IR 88		17 4		2.4	-	10.1	7 40		HE 23			969.10						
5.6,4054CE		6118L1	16.	12.2	12	6E 61			5.9.5	2.1												
Z sub_408C70	Dist.	11001	1.00					1.22				1.0	2.2			and the second second						
7 sub. #0.4940	Contract of the second	0100.1			1.0			- 22		2.4		÷.,										
	1000	A											C									
	0.00	01544					10.00			2.1		1.2			1	1.00						
	0.00	81111	45	NT 84					-	10.1			88.77	1.4								
	1000	01121	-	10.00		1.0	5.8 15	4.0			1 6			hall								
	0.00	011111	68	M 81	1.1			1.0	08.4	82.1			55 11									
	0.00	01151	85.1	E 15		BC AL	1 88 83	-	10.0	77 1	10 11	5.8	80.80	8.8	B.64-	w. 17						
	020	01161	0.0	D 10	hh.	70. A	00 77	0.0	-	88.1	10 22	5.0	29 53		R.w	Tall						
	(DE)	01171	FF 1	15 60	61	Ch E	41 51	17	31.1	58.5	9 92	40	80. 01		-042.8	.16						
	0.04	01181	57	D FD	16	F5 8	E9 88	183	101	00 3	10 13	.68	82 41	W.*.).Te							
	0.04	01191	24	4 10	1.58	80 01	82 95	E.F.	EP 3	2A 3	17.44	1.83	54 78	.t.]		59.3-1						
	884	81161	88 4	0.10	51	E8 04	25, 82	0.0	83.5	ca I	14,78	1.63	75 W	17900	F151							
	0.04	81101	.07.1	K 41	04	41.8	01.00		88.3	28 1	F #1	24	88 21			·T						
	8:04	81101	10.1	18 E.I	1.50	84 H	84 14	MD.	89.1	99.5	-B F7	15	78.51	1.13								
	0.04	41101	188.5	11, 29	18	6.W. VI	1 A1 HI	74	10.1		19 26	-51	88,11	9.9.	'ia.t.	hatte.F						
	8.84	RTIET	0.00	15 III		ND (D)	B) 88	55	10.5	52.4	4 11	RE.	28,52	R		8111-5						
	8184	M13F1	80.0	14 M	28	EB, 75	10.11	82	0.41	82.4	17,00	1.82	88,23	A	*#Ø							
	8.04	#12#1	0.001	9.75	81	10.9	1 80 13	29	38.4	11.1	E) 121	184	83.85	-115-	*-)*	A-15						
	1990	81211	811	14.51	111	15 71	E E S 48	14.00	12.1	15.7	1. 161	्याः	10.01									

Gambar dibawah langkah melakukkan file yang kedua yaitu payload2.exe

unction name														
7 alb 10196		seg000:0100	1.1											
200"10100		seg800:8100	This	file has		ted by Th		. Marra		and the second s	-			
		5000010100	11115	Copuri	aht (c) 291	5 Hex-Rap	s. (support6	Rex-rass	comper (1					
		seg800;8100			Licens	e info: 4	8-8611-7234-	-88			i -			
		seg800:8100	111	Desk	ey Lee, Kis	gsoft Into	ernet Securi	ity Softw	APP -					
		50080018100												
		501899:8198	Input HPS	: 5148	0815F368811	ARE 79E 7 MET	F01678C0							
		509888:8188	; input CR	32 : 7999	0563									
		Seg888:8188												
		5492284:2188	. Tile Non		aronanta an			der bert	THEAT	-	menta.			and the street of a
		5498881 8188	; Format	= HS-0	OS COM-File	a second	S (Manual S C S	and the second	College Streets			ay roads (,,	and during range save
		seg888:8188	; Base Addr	ress: 1008	h Range: 18	10m-1021	2h Loaded le	mgth: 11	2h					
		seg880:8108												
		seg800:8108		.686	P									
		549880;8108		.nod	el time									
		seg880:8108												
		seg800:8100	;											
		segeou:enue	: Second 1	upp - Russ	cada									
		5000010100	500000	seen	ent bute pu	01ic 'C000	E' use16							
		509899:8198		assu	ne csiseg@									
		seg899:8198		org	199h									
		50080018108		3550	ne es:nothi	ng, ssino	thing, ds:se	ig ana , is	enothing.	95:00	ching			
		501899;8198		publ	ic start									
		509889:8188	start:											
		Seg888:8188		cld										



Contoh gambar convert assembly pada file payload2.exe

Terdapat dua contoh gambar hasil dari masing – masing file:

Gambar dibawah ialah hasil dari file payload.exe





Gambar dibawah ialah hasil dari file payload2.exe