

91812488 성우상 91812866 이승훈 91812139 김성준



# 1. Web hacking

# 2. Reversing







# 페이지를 들어가보면 이런 문구가 뜬다. 보아하니 비밀번호를 찾아야하는 것 같다.



# F12를 누르면 개발자 도구가 뜬다. 여기서 ctrl F를 누른다음 pass단어를 찾아 보자. 찾아보니 비밀번호가 나와있다.



# VIRUS LOADING

A.html

입력을 해보니 가운데에 A.html이라는 문구가 나타났다. 주소창에 쳐서 들어 가보자.



새로운 창이 열렸다.



# Click을 눌러보면 창이 나타날 것이다.

Q, 드라이브 검색			~
공유 문서함 > ranso	mware 👻 😩		
파일			
	nageta 10 Kan		
		=	
_		•	
🗾 file	🖹 readme.txt	ti⊒ run.exe	



# 리버싱(Reverse Code Engineering)이란?

- 리버스(reverse-뒤집다)와 엔지니어링(engineering-공학기술) 의 합성어로 리버싱이라고 줄여 말한다.

# #리버싱 기술

```
-완성된 프로그램을 거꾸로 분석하여 설계도를 축출
-완성된 시스템을 역추적 (역공학)
-소프트웨어의 유지보수
-프로그램 동작변경
-복제프로그램 개발(대표적인 크랙)
향상된 프로그램 개발
-악성 코드 분석(보안)
```

📄 file	2012-03-04 오후	파일	9KB
📄 readme.txt	2012-03-12 오전	텍스트 문서	1KB
📧 run.exe	2012-03-04 오후	응용 프로그램	10KB

# 주어진 zip파일을 풀면 이렇게 세 개의 파일이 나온다.



# 일단 readme.txt 부터 열어보면 파일을 Decrypt 하란다. 파일 종류는 exe인 것 같다.

III C:₩Users₩성준₩Desktop₩리버싱기초 이해₩ransomware₩run.exe

## 나는 나쁜놈이다! 나는 매우 나쁘기 때문에 너의 파일을 암호화했다! 너의 파일을 복구하고 싶다면 5천억 달러를 입금하고 받은 키값으로 파일을 복구해라!

⟨ey ∶

# run.exe 을 실행하면 이런 화면이 뜬다. Key를 입력하면 그 Key를 가지고 Decrypt 하는 건가 보다. 5천억을 진짜 입금할 순 없으니 살펴보자.

Offerst (b)	00	0.1	0.2	0.2	0.4	OF	06	07	0.0	00	0.7	OP	00	OD	OF	OF	
Offset(n)	00	01	02	03	04	05	06	07	08	09	UA	ОВ	UC	0D	UE.	0E	
00000000	DE	CO	<b>1</b> B	8C	8C	93	9E	86	98	97	9A	8C	73	6C	9A	8B	ÞÀ.ŒŒ"ž†~—šŒslš<
00000010	34	8F	93	9E	86	9C	97	9A	CC	8C	93	9A	8B	8C	8F	93	4."ž†œ—šÌŒ"š<Œ."
00000020	9E	86	9C	97	9A	8C	8C	93	9A	8B	8C	8F	93	9E	86	9C	ž†œ— šœŒ" š<Œ. "ž†œ
00000030	97	9A	8C	8C	93	9A	8B	8C	8F	93	9E	86	6C	97	9A	8C	— šŒE" š< Œ."ž†l— šŒ
00000040	82	8C	20	85	8C	3B	9A	53	A7	24	96	D6	41	AD	C7	F2	,Œ …Œ;šS§\$-ÖA.Çò
00000050	E2	FF	AF	E3	EC	E9	FB	E5	FB	E1	AC	FO	FB	E5	E2	EO	âÿ ãìéûåûá⊣ðûåâà
00000060	E7	BE	E4	F9	<b>B7</b>	E8	F9	E2	B3	F3	E5	AC	CB	DC	CD	A6	ç¾äù èùâ³óå⊣ËÜͦ
00000070	F1	F8	FE	E9	A2	9E	97	81	A8	8F	93	9E	86	9C	97	9A	ñøþ颞—."."žtœ—š
08000000	81	CD	37	OA	C2	AC	45	50	D7	A6	56	54	D3	AC	46	50	.17.¬EPצVTӬFP
00000090	40	E5	DE	4C	DB	BE	4C	5F	<b>B1</b>	CC	DA	4F	D9	BA	41	4F	@å₽LÛ¾L_±ÌÚOÙ°AO
000000A0	<b>A</b> 9	C5	FE	45	C7	B7	50	4F	CC	CB	C3	48	C7	AF	59	5D	©ÅþEÇ · POÌËÃHÇ Y]
00000B0	CF	BC	5C	59	FD	AC	59	59	AD	DA	EE	50	DE	A6	56	54	ϼ\Yý¬YY.ÚîP₽¦VT
00000000	BC	DA	DC	50	D2	AB	46	4C	<b>B</b> 5	<b>C</b> 8	D1	5F	DF	BA	46	4F	₩ÚÜPÒ≪FLµÈÑ_ß°FO
00000000	C1	F3	E8	E4	C6	B3	54	45	9C	97	9A	8C	8C	93	9A	8B	Áóè䯳TEœ—ĕŒŒ"š<
000000E0	8C	8F	93	9E	86	9C	97	9A	8C	8C	93	9A	8B	8C	8F	93	Œ."ž†œ—ăŒŒ"ă∢Œ."
00000F0	CE	C3	9C	97	D6	8D	8F	93	26	AO	DF	CO	93	9E	86	9C	ÎÜ—Ö∿& BÀ∿ž†œ
00000100	97	9A	8C	8C	73	9A	88	8D	84	92	94	86	9C	<b>B</b> 7	9A	8C	—šŒŒӟš^."′″†œ∘šŒ
00000110	8C	83	9A	8B	8C	2F	92	9E	36	55	96	9A	8C	3C	92	9A	Œſš<Œ/′ž6U−šŒ<′š
00000120	8B	5C	8E	93	9E	86	DC	97	9A	9C	8C	93	9A	89	8C	8F	<∖Ž~ž†Ü—ĕœŒ~ĕ‱Œ.
00000130	96	9E	87	9C	97	9A	8C	8C	96	9A	8A	8C	8F	93	9E	86	–ž‡œ—šŒŒ−šŠŒ."ž†
00000140	9C	77	9B	8C	8C	83	9A	8B	8C	8F	93	9E	85	9C	D7	1B	œw≯ŒŒfš<Œ."ž…œ×.
00000150	8C	8C	83	9A	8B	9C	8F	93	9E	86	8C	97	9A	9C	8C	93	ŒŒfš<œ."ž†Œ—šœŒ"
00000160	9A	8B	8C	8F	83	9E	86	9C	97	9A	8C	8C	93	9A	8B	8C	š<Œ.fž†œ—šŒŒ"š<Œ
00000170	7B	42	9F	86	40	97	9A	8C	8C	43	9B	8B	78	8E	93	9E	{BŸ†@— šœec >< xŽ``ž
00000180	86	9C	97	9A	8C	8C	93	9A	8B	8C	8F	93	9E	86	9C	97	tœ—ĕŒŒ"ĕ<Œ."žtœ—
00000190	9A	8C	8C	93	9A	8B	8C	8F	93	9E	86	9C	97	9A	8C	8C	šŒŒ"š<Œ."ž†œ—šŒŒ
000001A0	93	9A	8B	8C	8F	93	9E	86	9C	97	9A	8C	8C	93	9A	8B	"š<Œ."ž†œ—šŒŒ"š<
000001B0	8C	8F	93	9E	86	9C	97	9A	8C	8C	93	9A	8B	8C	8F	93	Œ."ž†œ—ĕŒŒ"š< <mark>Œ."</mark>
000001C0	9E	86	9C	97	9A	8C	8C	93	9A	8B	8C	8F	93	9E	86	90	žtœ— šœŒ∵š∢œ. "žtœ
000001D0	97	9A	8C	8C	93	9A	8B	8C	8F	93	9E	86	90	97	9A	8C	—šŒŒ"š<Œ."ž†œ—šŒ
000001E0	8C	93	9A	8B	8C	8F	93	9E	D3	CC	CF	AA	8C	8C	93	9A	œ"š∢œ."žóÌï≏œœ"š
000001F0	8B	2C	8E	93	9E	96	90	97	9A	8C	8C	93	9A	8F	8C	8F	<,Ž~ž–œ—šŒŒ~š.Œ.

널 패딩이 있을 만한곳에 0xD만큼 특정 값이 반복되는 것을 볼 수 있었 다. 따라서 키값은 0xD이다.

- [CPU - main thread, module run] <u>C</u> File View Debug Plugins Options Window Help

		LEMTWHC/KBRS		
<b>00ECECDE</b>	00	DB 00	· · · · · · · · · · · · · · · · · · ·	Registers (FPU)
<b>00ECECDF</b>	0060BE00	DD run.00BE6000		F9X 68262FF9
00ECECE3	DØ	DB DØ		ECX AAECECEA rup <moduleentr< th=""></moduleentr<>
00ECECE4	EC	DB EC		EDX AAECECEA rup (NoduleEnt
00FCFCF5	008DBF00	DD run.00BE8D00		FRV 00258000
<b>ANECECE9</b>	40	DB 40	CHAR '@'	
<b>NAECECEA</b>	53	DB 53	CHAR 'S'	EDD 0017FF04
<b>ANECECER</b>	FF	DR FF		ECT GOECECEG num /WadulaEnta
<b>NAECECEC</b>	57	PUSH EDT		EDT AGECECEO run. (ModuleEntr
<b>ANECECED</b>	. FR AR	INP SHORT run AAECECEA		
<b>ANECECEE</b>	90	NOP		EIP 00ECECE0 run. <noduleentr< th=""></noduleentr<>
<b>ANECECEN</b>	> 8006	NOV AL RYTE PTR DS (EST)		
00ECECE2	46			
<b>MAECECE3</b>	. 8807	NOV BYTE PTR DS.[EDT] AL		
00ECECE5				TH 0 33 002D 32D11 0(FFFFFF
00ECECE6		AND FRX FRX		
00ECECE8	75 07	INZ SHORT rup AAECEDA1		15 0 F5 0000 32D11 200000(F1
<b>ANECECEA</b>	> 881F	NOV ERX NUORD PTR DS-[EST]		D G UUZD JZDIL U(FFFFFF
<b>ANECECEC</b>	83FF FC	SUB EST -6		0 0 Lastenn EDDOD SUCCESS (
<b>ANECECEE</b>	11DR	ANC FRX FRX		0 0 Lasterr Error_Success
00ECED01	$2^{-72}$ FD	JR SHORT rup OMECECEM		EFL 00000246 (NO,NB,E,BE,NS,
00ECED03	้ หรื ค้าคดคดคด	MOV FAX 1		CTO anatu O O
00ECED08	> A1DB	AND FRX FRX		STU EMPLY U.U
<b>ANECEDAA</b>	. 75 07	INZ SHORT rup 00ECED13		STI empty 0.0
<b>ANECEDAC</b>	881F	WOV EBX DWORD PTR DS [EST]		ST2 empty 0.0
<b>ANECEDAE</b>	83FF FC	SUB EST -6		STJ empty 0.0
00ECED11	1108	ADC FRX FRX		ST4 Empty 0.0
<b>ANECED13</b>	> 1100	ADC FAX FAX		STG ompty 0.0
00FCFD15	01DB	ADD FBX.FBX		ST7 ompty 0.0
00FCFD17	. 73 AB	JNB SHORT run AAECED24		317 empty 0.0 3.2.1.0
00FCFD19	<b>75 28</b>	JNZ SHORT run.00ECED43		EST 0000 Cond 0 0 0 0 Fre
00ECED1B	. 8B1E	MOV EBX.DWORD PTR DS:[ESI]		ECW 027E Proc NEOR 53 Wash
00FCFD1D	83FF FC	SUB FST4		TOIL 0271 TIEC HEIRE, 00 HUSP
00ECED20	. 11DB	ADC EBX.EBX		
00ECED22	., 72 1F	JB SHORT run.00ECED43		
00ECED24	> 48	DEC EAX		
00ECED25	. 01DB	ADD EBX.EBX		
00ECED27	75 07	JNZ SHORT run.00ECED30		
00ECED29	. 8B1E	MOV EBX, DWORD PTR DS:[ESI]		
AAECED2B	83EF FC	SUB_EST_6	· · · · · · · · · · · · · · · · · · ·	<u></u>
Address	Hex dump	Disassembly	Comment ^ 0019FF	84 76D38484 RETURN to KERNEL
00ECF000	0000	ADD BYTE PTR DS:[EAX].AL	0019FF	88 00258000
00ECF002	0000	ADD BYTE PTR DS:[EAX],AL	0019FF	8C 76D38460 KERNEL32.BaseThr
00ECF004	0000	ADD BYTE PTR DS:LEAX1,AL	0019FF	90 68242EEA
00ECF006	0000	ADD BYTE PTR DS:[EAX],AL	0019FF	94 0019FFDC
00ECF008	04 00	ADD AL,0	0019FF	98 77AC2EC0 RETURN to ntdll.
00ECF00A	0000	ADD BYTE PTR DS:[EAX],AL	0019FF	90 00258000
00ECF00C	0000	ADD BYTE PTR DS:LEAX1,AL	0019FF	A0 3B614214

올리디버거로 분석해보니 entry point가 pushad 로 시작한다 pushad로 시작하니깐 아마 upx로 패킹 했흘거라 생각한다.

UULGELZH	. 37	FUSH LUI		Keg1	STERS (F	PU)
00ECEE2B	. 48	DEC EAX		FAX	68242FFF	
00ECEE2C	. F2:AE	REPNE SCAS BYTE PTR ES:[EDI]		FCX	ØØFCECEØ	run. <m< th=""></m<>
00ECEE2E	. 55	PUSH EBP		FDX	<b>MAECECER</b>	run <m< th=""></m<>
00ECEE2F	. FF96 F8E1AC0(	CALL DWORD PTR DS:[ESI+ACE1F8]		FRX	00258000	
00ECEE35	. 0900	OR EAX.EAX		ESP	<b>0019EE8</b>	
00ECEE37	., 74 07	JE SHORT run.00ECEE40		FRP	0019EE9/	
ANECEE39	8903	MAY DWARD PTR DS+[FBX] FAX		FOT	<b>ABECECE</b>	
<b>ANECEE3B</b>	8303 04	ADD FRX &		EDT	<b>ABECECE</b>	
<b>NAECEE3E</b>	^ FB F1	INP SHORT run AAECEE21		LDT	OOLULULU	run.vr
00ECEE40	> FF96 08F20C00	CALL DWORD PTR DS [EST+ACE208]		EIP	<b>00ECECE</b>	∣run.<∦
00ECEE46	> 8BAE ECELACO	WAV ERP DWARD PTR DS+[EST+ACE1EC]		c o	EC 0000	99634
00ECEE4C	8DRE AAEAEEE	IFA ENT NWORD PTR DS:[EST-1000]		D 1	CC 0020	) J2DIL
00ECEE40	RR 0010000	NOV FRX 1000			60 0023	32D11
00ECEE57	50	PIISH FOX		H U	- 33 00ZE	JZDIL
00ECEE57	. 50	DIIGH FOD			DS 0020	32D11
00ECEE50	. 54			50	F5 0000	JZD11
00ECEE5P	59	DIISH ERV		10	65 0020	5 J2D11
00ECEESD	. 55	DIICH ENT		0 0		EDDOD
00ECEE5D	· 57			00	LastErr	EKKUK
OOLCELJD	- FFUJ 0007 0F030000	UNCE LOF		FFL	00000246	(NO.NB
00LULLJF	. 0007 0F020000 0000 7F	AND DUTE DTD DE FENVI 7F		0.7.0		,
00LCLLCJ	. 0020 1F 9020 30 7F	AND DYTE FIR DJ.ILHAJ,7F AND DUTE DTD DC.FEAV.901 7F		SIU	empty 0.	V
00ECEECO	. 0000 20 /F	HND DYTE FIR DƏ:LEHATZOI,7F Dod Eov		511	empty 0.	N
00LCLLCC	. JO 50	FUF LHA Diigu Eav		512	empty 0.	0
00ECEEOD	. 30 E/	PUƏN EHA Duqu Fod		\$13	empty U.	U
	. 04 EQ	PUƏN EƏP Duqu Foy		S14	empty 0.	0
OUELEEDF	. 30 E0	РОЭП ЕНХ		\$15	empty 0.	0
00ELEE70	. 33	PUƏN EDA Ducu EDA		S16	empty 0.	0
	. 37	PUSH EDI		ST7	empty 0.	0
00EUEE72	. FFU5	CHLL EBP				32
	. 58	PUP EHX		FST	0000 Co	nd 0 0
00ELEE75	. 61	PUPHU		FCH	027F Pr	ec NEAR
ØØEUEE76	. 804424 80	LEH EHX,DWURD PIK 55:LESP-801				
OUECEE/H	> 6H 00	PUSH 0				
UUEUEE/U	. 3904	UMP ESP, EHX				
UUEUEE/E	. <b>/5</b> FH	JNZ SHUKI run.00ECEE/H				
UNECEE80	. 83EC 80	SUB ESP, -80				
UNECEE83	E9 13BE57FF	JMP_run.0044HC9B				
UNECEE88	48	DB 48	CHHR 'H'			
NNELLERA	ии	ПВ ИИ				
Address	Hex dump	Disassembly	Connent ^ 10191-12		6038484	RETURN
00ECF000	0000	ADD BYIE PTR DS:[EAX],AL	0019FF8	00 0	0238000	KEDNEL O
UVECF002	0000	HDD BYTE PTR DS:LEAXI,AL	0019FF		0030400	REKNELJ
00ECF004	0000	ADD BYTE PTR DS: [EAX], AL	0019FFS		0Z4ZEEH	
00ECF006	0000	ADD BYIE PTR DS:[EAX],AL	0019FFS	74 <b>[</b> ]	UTALENC	DETUDN
00ECF008	04 00	ADD AL,0	0019FFS	70 1	7HUZEUU	KETUKN
00ECF00A	0000	ADD BYTE PTR DS:[EAX],AL	0019FFS		0258000	
00ECF00C	0000	ADD BYTE PTR DS:[EAX],AL	0019FFF	E UN	00000000	
00ECF00E	0100	ADD DWORD PTR DS:[EAX],EAX	UU19FFF	14 0	00000000	
00ECF010	1800	SBB BYTE PTR DS:[EAX],AL	0019FFF	18 0	0000000	
00ECF012	0000	ADD BYTE PTR DS:[EAX],AL	0019FFF		0258000	
00ECF014	1800	SBB BYTE PTR DS:[EAX],AL	0019FFE	50 0	00000000	
NAEAEA4 C	0000 0000000	ADD DUTE DTD DA LEAUL AL		e e - 1 - 1 - 1 - 1 - 1	the set of the set of the set	

쭉 아래로 내려가다 보면 0x00ECEE83 다음주소로 이동하는데 oep 즉 진짜 시작주소다.

<u>File</u> <u>V</u> lew	<u>D</u> ebug <u>P</u> lugins Op <u>t</u> ions <u>w</u> ind	ow <u>H</u> elp		
		L E M T W H C / K B R S 🔚 📰 ?		
00660776	5B	POP FRX		^ Registers (EPH)
00440775	68 00014400	PUSH rup 0044C10C	OSCIT "Kou · "	
00441770	EE15 D0C0//00	COLL BUODD DTD DC.[//COD01	NCUCD100 printf	
0044H77H	FF13 D0004400	ODD FOD (	HOVERIOU. Printi	EUX UUEUEUEU run. <moduleentr< td=""></moduleentr<>
0044H780	8JL4 04			EDX 00ECECE0 run. <moduleentr< td=""></moduleentr<>
0044H783	F8 \868FRFF	<u>CHLL run.00401000</u>		EBX 00381000
0044A788	68 70D34400	PUSH run.0044D370		ESP 0019EE84
0044A78D	68 B4C14400	PUSH run.0044C1B4	ASCII "%s"	EBP 0019EE96
00448792	FF15 B8C04400	CALL DWORD PTR DS:[44C0B8]	MSVCR100.scanf	EST QQECECEQ rup (ModuleEntr
00440798	8304 08	ADD ESP 8		EDT QAECECEA mun (MadulaEntr
0044079R	C745 E8 70D3444	NOV DWORD PTR SS-[ERP-18] rup 0044D370		
004411770	0D/5 E0 7000440	NOU ENV NUNDO DTD CC.[EDD_10]		EIP 0044AC9B run.0044AC9B
0044H7HZ	0D4J L0 0000 01	ADD FOU 1		
0044H7H3	8368 81	HUU EHA,I		C 1 ES 002B 32bit 0(FFFFFF
0044H7H8	8945 E4	MUV DWURD PIR SS:LEBP-ICI,EHX		P 1 CS 0023 32bit 0(FFFFFF
0044H/HB	8B4D E8	MUV ECX,DWURD PIR SS:LEBP-18J		A 0 SS 002B 32bit 0(FFFFFF
0044A7AE	8A11	MOV DL,BYTE PTR DS:[ECX]		7 0 DS 002B 32bit 0(FFFFFF
0044A7B0	8855 E3	MOV BYTE PTR SS:[EBP-1D],DL		S 0 ES 0053 325it 386000/EE
0044A7B3	8345 F8 Ø1	ADD DWORD PTR SS:[FBP-18].1		T $A$ $GS$ $AA2R$ $32hi+$ $Affectered$
004407B7	807D E3 00	CWP RVTE PTR SS [ERP-101 0		
004407RR	^ 75 FF	INZ SHOPT run 0044070R		
0044H7DD	0D/5 E0	NOU EON BUODD DTD CC.[EDD 10]		U Ø LASTERR EKKUK_SULLESS (
0044H7DD	0D4J E0 0D(E E(	MUY EHA, DHURD FIR 33:LEDF-101		EEL AAAAA2A7 (NO B NE BE NS
0044H7U0	2040 E4	SUB EHX, DWUKD PIK SS: LEBP-ILI		
0044H7C3	8945 DC	MUV DWURD PIR SS:LEBP-24J,EHX		STO empty 0.0
0044A7C6	8B4D DC	MOV ECX,DWORD PIR SS:LEBP-24J		ST1 emptv 0.0
0044A7C9	894D F4	MOV DWORD PTR SS:[EBP-C],ECX		ST2 empty A A
0044A7CC	E8 2F68FBFF	CALL run.00401000		ST3 ompty 0.0
00660701	C745 E8 000000	NOV DWORD PTR SS·[EBP-81 0		STO Empty 0.0
00440708	68 B8C14400	PIISH rup 0066C188	ASCIT "rb"	CTE anaty 0.0
00440700	68 BCC14400		OSCIT "filo"	
00440700	EE15 0000//00			SIG empty 0.0
0044H7EZ	FF13 HUUU4400	ODD FOD O	HSVCK100.Topen	SI/ empty 0.0
0044H7E8	8364 08	HUU ESP,8		3210
0044H7EB	8945 FC	MUV DWURD PIR SS:LEBP-4J,EHX		FST 0000 Cond 0 0 0 0 Err
0044A7EE	E8 ØD68FBFF	CALL run.00401000		FCW 027F Prec NEAR.53 Mask
0044A7F3	837D FC 00	CMP_DWORD_PTR_SS:[EBP-4],0		,,
0044A7F7	√ <b>75 20</b>	JNZ SHORT run.0044A819		
0044A7F9	E8 0268FBFF	CALL run.00401000		
004407FF	68 64614400	PUSH run 0044C1C4		
00440803	FE15 R0C06600	COLL NUORD PTR DS+[44COR0]	WSVCR100 printf	
00440000	FF13 D0004400	ODD FED /		
0044H007	0364 04 Fo FF(3FDFF	HUU ESF, 4		
0044H80C	E8 EF67FBFF	UHLL run.00401000		
ИИААНХТТ		рия и		
Address	Hex dump	Disassembly	Connent	0019FF84 76D38484 RETURN to KERNEL
<b>ANECENNA</b>	0000	AND BYTE PTR DS [EAX] AL		0019FF88 00381000
<b>ANECENN</b> 2	0000	AND RVTE PTR DS-LEAX1 AL		0019FF8C 76D38460 KERNEL32.BaseThr
ANELCE ON T	0000	AND RUTE DTD DC. (EAVI AL		AN19FE9A F7EDC82A
000000004	0000	ADD DITE DID DO LEAVI OL		
00ELF006	0000	HUD BYTE PIK US:LEHXI,HL		0010EE00 77002EC0 DETIIDN ++-
UNFCEN08	04 00	HUU HL,0		DULTERSON THUSELU KEIUKM TO NTOLL.
<b>00ECF00A</b>	0000	ADD BYIE PTR DS:[EAX],AL		
AAFAFAAA	0000	ADD DUTE DTD DA FEAUL AL		

아까 oep에서 아래 쪽 말고 위쪽으로 올라오다 보면 scanf함수를 찾을 수 있다. scanf 아랫부분에 브레이크 포인트를 걸어두고 f9(브레이크포인트 걸 리기 전 까지 명령 모두실행)을 해준다.

[CPU - main thread, module run]

C <u>F</u> ile <u>V</u> iew	Debug Plugins Options Wind	ow <u>H</u> elp		
🖻 📢 🗙 🕨 ►		LEMTWHC/KBRS 📰 📰 ?		
0044A76A	50	PUSH EAX		^ Registers (EPH)
0044A76B	58	POP EAX		EAX 0000001
0044A76C	53	PUSH EBX		ECX 65E65000 MSVCR100 65
0044A76D	5			EDX 65EB65D0 DEESET MSVD
0044A76E	6 C:#Users#성준#Deskt	ap#리버징기소 이애#ransomware#run.exe	= L X	FRX AAAAAAAA
0044A76F	6나는 났쁞놈이다!			ESP 0019EE06
0044A770	9남등 뱊욹 날을길 뱃	문에 너의 파일을 암호화했다! 그 사다며 다친어 다기로 이그렇고 바오 미간이로 파이오 보		ERP 0019EE3C
0044A771	5 피의 파일들 목구이-	신 앞다면 5선역 열려를 입금이고 얻는 기쉾으도 파일을 속~	구애감!	EST AAAAAAA
0044A772	5Kev : asd			EDT AAECAC3C run AAECAC3
0044A773	5			
0044A774	5			EIP 0044H798 run.0044H79
0044A775	6			C 0 ES 002B 32bit 0(EEE
0044A77A	F			P 1 CS 0023 32bit 0(FFF
0044A780	8			A 0 SS 002B 32bit 0(FEE
0044A783	E			Z 0 DS 002B 32bit 0(FFF
0044A788	6			S 0 FS 0053 32bit 38400
0044A78D	6			T 0 GS 002B 32bit 0(FFF
<u>0044A792</u>	F			D 0
0044A7/98	8			0 0 LastErr ERROR_SUCCE
0044A79B	C			EEL AAAAA2A6 (NO NR NE O
0044H7H2	8			
0044H7H5	8			STO empty 0.0
0044H7H8	8			ST1 empty 0.0
0044H/HB	8			ST2 empty 0.0
0044H7HE	8			ST3 empty 0.0
0044H7B0	8			ST4 empty 0.0
0044H/BJ	8			ST5 empty 0.0
0044H7B7				SI6 empty 0.0
0044H/DD	<b>6</b>			SI/ empty 0.0
0044H7DU	0 2865 F6	SUB LOV NUODO DID SSALERD_1CI		3210
00441700	2043 L4 8945 DC	WAY BUADD DTD SS.[ERD_26] FAY		F51 0000 Cond 0 0 0
004411/03	8840 DC	NOV DHORD FIR 33.1LDF=24J,LHA		FUW 027F Prec NEHR,53
00440700	894D E4	WAY DWARD PTR SS.[ERP_C1 FCX		
00440700	E8 2E68EBEE	$\begin{array}{c c c c c c c c c c c c c c c c c c c $		
00440700	C745 E8 000000	WAY DWARD PTR SS [FRP-8] A		
00440708	68 B8C14400		ASCII "rb"	
004411700	68 BCC14400		ASCII "filo"	
004411100	EE15 ACC06600	CALL NWORD PTR DS · [ & & CAACAAC ]	WSVCR100 fonen	
0044117E2	8304 08	AND ESP 8	Hoven100.10pen	¥
Oddmaga	Hau dunn	Diagoanhlu	Connent A 881	19EEAA AAAAC1RA OSCITT "%e"
AGECEGGG		ODD BALE DID DG'LEONI OF	GORREITL	19EEN8 NA44D37N ASCTT "asd"
00ECE000	0000	ADD DTIL FIR DOLLEHAL,HL	003	
OOLUFUUZ	0000	AND DITE TIR DOLLEHAL, HE	001	
00ECF004	0000	AND BYTE FIR DOLLEHAL, HE	001	19FF14 0000000
00ECE000	04 00	OND OF A	001	19FE18 65E1D1E0 RETURN to MS
00ECE000	0000	OND RUTE PTD DS. (FOX1 OF	001	19FF1C 0019FF40
00ECE00H	0000	OND RVTE PTR DS.LENAJ, HL	001	19FF20 0044AA43 RETURN to ru

아무 값이나 key로 입력해주고 엔터를 누르고 우리가 생각한대로 scanf명 령다음에 브레이크가 걸려서 멈추게 된다.

		LEMTWHC/KBRS 📰 📰 ?		
0044A897	E8 6467FBFF	CALL run.00401000	^	Registers (FP
0044A89C	C745 F8 000000	MOV DWORD PTR SS:[EBP-81,0		EAX 00000001
0044A8A3	~ EB 09	JMP_SHORT_run.0044A8AE		ECX 65E65AA0
0044A8A5	8B45 F8	MOV EAX, DWORD PTR SS:[EBP-8]		EDX 65EB45D0
0044A8A8	83C0 01	ADD EAX,1		EBX 0000000
0044A8AB	8945 F8	MOV DWORD PTR SS:[EBP-8],EAX		ESP 0019FF04
0044A8AE	8B4D F8	MOV ECX, DWORD PTR SS: [EBP-8]		EBP 0019FF3C
0044H8B1	3B4D F0	CMP ECX, DWURD PIR SS: TEBP-101		ESI 00000001
0044H8B4	~ /3 49	JNB SHUKI run.0044H8FF		EDI 00ECAC3C
0044H8B6	8855 F8	MUV EDX, DWURD PIR SS: [EBP-8]		ETP 00440798
0044H859	OPIE EO	MUVSX ELX,BYIE PIK DS:LEDX+3413B81		
0044H8U0	8043 F8	MUV EHX,DWUKD PIK 55:LEBP-81 Vod Edv edv		C 0 ES 002B
0044H0CJ	3302 E775 E7	AUK EVA,EVA DTU DUADD DTD CC.[EDD C1		P 1 US 0023
00440000	0ERE92 70D3//00	MAUSY ENV RUTE DTD NS·[ENV+//N370]		H 0 55 002B
0044H0C0	3300	NOV SA LDA, DTTL TTR DJ. LLDA 4403701 NOD FRV FNV		
00440001	8845 F8	MON FOX NUORD PTR SS [FRP-8]		5 0 F5 0000
00440001	8888 B8155600	MOV BYTE PTR DS·[FAX+561588] CI		1 0 65 002B
00440800	E8 2167EREE			
0044A8DF	8B4D F8	MOV ECX.DWORD PTR SS:[EBP-8]		0 0 LastLII
0044A8E2	0FBE91 B8155400	MOVSX EDX.BYTE PTR DS:[ECX+5415B8]		EFL 00000206
0044A8E9	81F2 FF000000	XOR EDX, ØFF		STA empty A A
0044A8EF	8B45 F8	MOV EAX, DWORD PTR SS:[EBP-8]		ST1 empty 0.0
0044A8F2	8890 B8155400	MOV BYTÉ PTR DS:[EAX+5415B8],DL		ST2 empty 0.0
0044A8F8	E8 0367FBFF	CALL run.00401000		ST3 empty 0.0
0044A8FD	^ EB A6	JMP_SHORT_run.0044A8A5		ST4 empty 0.0
0044A8FF	8B4D FC	MOV ECX,DWORD PTR SS:[EBP-4]		ST5 empty 0.0
0044A902	51	PUSH ECX		ST6 empty 0.0
0044A903	FF15 A0C04400	CALL DWORD PTR DS:[44C0A0]	MSVCR100.fclose	ST7 empty 0.0
0044A909	8304 04	ADD ESP, 4		
0044A90C		CALL run.00401000	AGATT H LH	FST 0000 Con
0044H911	68 UUU14400	PUSH run.0044C1DC	HSUII WD	FCW 027F Pre
0044H910		PUSH FUN.0044LIE0		
0044H71B	FF15 HUUU4400	CHLL DWORD PIK DS: [4460H6]	HOVERIOD. LOBEU	
0044H721	0364 00 9945 EC	HUD ESP,0 Nov nuodn dtd ssiferd_1/1 eov		
004411724	E8 D466EREE	ΠΟΥ DHORD FIR 33:LEDF-14],EHA COLL rup 00/01000		
004411727	E8 CE66EBEE			
004411720	C745 E8 000000	NOV DWORD PTR SS-[FRP=8] 0		
00440938	FR A9	INP SHORT run AA&A9&3		
00440930	8855 F8	MOV EDX DWORD PTR SS [ERP-8]		
0044A93D	8302 01	ADD FDX.1		
00448940	8955 F8	MOV DWORD PTR SS:[EBP-8].EDX		
00448943	8B45 F8	MOV EAX.DWORD PTR SS:[EBP-8]	✓	
Address	Hex dump	Disassembly	Connept ^ 0019EE	04 0044C1B4 A
ANECENNA	0000	ADD BYTE PTR DS [EAX] AL	0019FF	08 0044D370 A
00FCF002	0000	ADD BYTE PTR DS: [FAX1. A]	0019FF	0C 00ECAC3C r
<b>NAECENA</b>	0000	ADD BYTE PTR DS-IEAX1 AL	0019FF	10 0000001
00ECE004	0000	ODD DUTE DTD DC. (EOVI OL	0019EE	16 00000000

fopen 함수를 통해 'file' 읽어드린후에 pe 바이너리를 암호화한다. xor ecx,edx xor edx,000000ff 순서로 연산하는데 이를 해석해보면 (originalData[i]^key)^0xff=암호화 된 데이터[i]//i는 문자열 인덱스가 될 수 있겠다. 따라서 키값에 대한 식으로 다시 바꾸면 (암호화 된 데이터[i] ^ key) ^ 0xff=originalData[i]라고 할 수 있다.

₩0 HxD - [C:₩	Users₩성	ć준₩D	esktop	아입버	싱기초	이해₩	ranson	nware₩	run.ex	e]			
🔝 파일(F) 편	집(E) 쳦	と기(S)	보기	(/) 분	석(A)	기타 실	철정(X)	창 설	점(W)	?			
📄 📸 <del>-</del> 🗐	(m) 🥴	<b>* </b>	16	~	ANSI		$\sim$	16 진수	~				
🔝 readme.txt	📓 rui	n.exe											
Offset(h)	00 01	02	03 0	4 05	06 0	7 08	09 0	A 0B	0C 0	D OE O	F		
00000000	4D 57	90	00 0	3 00	00 0	0 04	00 0	0 00	FF F	F 00 0	0	MZ	
00000010	B8 00	00	00 0	00 00	00 0	0 40	00 0	0 00	00 0	0 00 0	0		
00000020	00 00	00	00 0	00 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000030	00 00	00 (	00 0	00 00	00 0	0 00	00 0	0 00	FO O	0 00 0	0	ð	
00000040	0E 11	BA	0E 0	0 B4	09 C	D 21	B8 0	1 4C	CD 2	1 54 6	8	°′.Í!,.LÍ! <mark>Th</mark>	
00000050	69 73	3 20	70 7	2 6F	67 7	2 61	6D 2	0 63	61 6	E 6E 6	F	is program canno	
00000060	74 20	) 62	65 2	0 72	75 6	E 20	69 6	E 20	44 4	F 53 2	0	t be run in DOS	
00000070	6D 61	64	65 2	E OD	0D 0.	A 24	00 0	0 00	00 0	0 00 0	0	mode\$	
00000080	B8 71	E4	19 F	TC 10	8A 4	A FC	10 8	A 4A	FC 1	.0 8A 4	A	.qa.u.SJu.SJu.SJ	
00000090	6F 5E	12	4A F	D 10	8A 4	A 93	66 1	6 4A	FE 1	0 8A 4	A	o^.Jý.SJ~f.Jþ.SJ	
000000A0	93 66	5 14	4A F	D 10	8A 4	A 93	66 2	0 4A	EF 1	0 8A 4	A	"f.Jý.SJ"f Ji.SJ	
00000080	93 66	21	4A P	E 10	8A 4	A FS	68 1	9 4A	FF 1	0 8A 4	A .	"I!Jp.SJon.Jy.SJ	
000000000	PC 10	1 3 5	4A C	.F 10	8A 4	A 93	60 2	5 4A	FD 1	0 8A 4	A	u.KJI.SJ~IsJY.SJ	
0000000000	93 66		-A - C	0 00	00 0	0 00	00 0	0 00	00 0	0 00 0	A	1.09.30RIChu.30	
000000E0	50 49	. 00	00 4	C 01	03 0	0 32	28 5	3 4 8	00 0		0	PF T. 2+50	
00000100	00 00	00	00 E	0 00	03 0	1 0B	01 0	A 00	00 2	0 00 0	0	à	
00000110	00 10	00	00 0	0 CO	AC 0	0 E0	EC A	C 00	00 D	0 AC 0	0	À¬àì¬Ð¬.	
00000120	00 F0	AC	00 0	0 00	40 0	0 00	10 0	0 00	00 0	2 00 0	0	.8	
00000130	05 00	0 01	00 0	00 00	00 0	0 05	00 0	1 00	00 0	0 00 0	0		
00000140	00 00	DA (	00 0	0 10	00 0	0 00	00 0	0 00	03 0	0 40 8	1		
00000150	00 00	10	00 0	0 10	00 0	0 00	00 1	0 00	00 1	0 00 0	0		
00000160	00 00	00 (	00 1	0 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000170	B8 F1	AC	00 D	C 00	00 0	0 00	FO A	C 00	B8 0	1 00 0	0	,ñ¬.Üð¬.,	
00000180	00 00	00	00 0	0 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000190	00 00	00	00 0	0 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
0A100000	00 00	00 0	00 0	00 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000180	00 00	00	00 0	00 00	00 0	0 88	EE A	00 00	48 0		0	··············	
00000100	00 00		00 0	0 00	00 0	0 00	00 0	0 00	00 0		0		
000001E0	00 00		00 0	0 00	00 0	0 55	50 5	8 30	00 0		0	UPYO	
000001E0	00 00	AC	00 0	0 10	00 0	0 00	00 0	0 00	00 0	4 00 0	0	. À¬	
00000200	00 00	00	00 0	0 00	00 0	0 00	00 0	0 00	80 0	0 00 E	:0	êà	
00000210	55 50	58	31 0	0 00	00 0	0 00	20 0	0 00	00 D	0 AC 0	0	UPX1	
00000220	00 20	00	00 0	0 04	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000230	00 00	00	00 4	0 00	00 E	0 2E	72 7	3 72	63 0	0 00 0	0	@à.rsrc	
00000240	00 10	00 (	00 0	0 F0	AC 0	0 00	04 0	0 00	00 2	4 00 0	0	ð¬\$	
00000250	00 00	00	00 0	00 00	00 0	0 00	00 0	0 00	40 0	0 00 C	:0	â	
00000260	00 00	00	00 0	00 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000270	00 00	00	00 0	00 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000280	00 00	00	00 0	0 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
00000290	00 00	00 0	00 0	00 00	00 0	0 00	00 0	0 00	00 0	0 00 0	0		
고 세트 개트	00 00					0.00		7101- 2				터어사기	
L 二 (火, 4E		글족 4	E-OF					날아, 2	4			코이쓰기	

hxd통해 run.exe의 pe 바이너리를 보면 'This is program cannot be run in DOS'라는 문구를 볼 수 있다. 이는 exe파일의 가장 큰 특징이다.

€ HxD - [C:₩Users₩성준₩Desktop₩리버싱기초 이해₩ransomware₩run.exe]	₩ HxD - [C:#Users#성쥰#Desktop#리버싱기초 이해#ransomware₩file]
쾳 파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?	圖 파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?
📄 📸 🖌 💭 🔤 16 🔍 ANSI 💟 16 진수 🗸	📄 🚵 🗸 💭 🥔 🗱 16 🗸 ANSI 🗸 16 진수 🗸
🛔 readme.txt 📓 run.exe	ile 👔 file
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZÿÿ	00000000 DE CO 1B 8C 8C 93 9E 86 98 97 9A 8C 73 6C 9A 8B ÞÀ.OCE"ž†"—-šCEslš<
00000010 B8 00 00 00 00 00 00 40 00 00 00 00 00 00	00000010  34 8F 93 9E 86 9C 97 9A CC 8C 93 9A 8B 8C 8F 93  4."ž†œ—šÌœ"š<Œ."
00000020 00 00 00 00 00 00 00 00 00 00 0	00000020 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 9C žtoe—š00CC°š∢0C.°žtoe
00000030 00 00 00 00 00 00 00 00 00 00 0	00000030 97 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 6C 97 9A 8C —š020C™š∢CL.∿ž†l—š0C
00000040 OE 1F BA OE 00 B4 09 CD 21 B8 01 4C CD 21 54 68	00000040 82 8C 20 85 8C 3B 9A 53 A7 24 96 D6 41 AD C7 F2 ,ŒŒ;ŠS\$\$-ÖA.Çò
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 1s program canne	00000050 E2 FF AF E3 EC E9 FB E5 FB E1 AC <mark>F0 FB E5 E2 E0</mark> âÿ¯ãiéûåûá⊣ <mark>ðúåáa</mark>
00000060 [74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 C De Fun in Dos	00000060 E7 BE E4 F9 B7 E8 F9 E2 B3 F3 E5 AC CB DC CD A6 <mark>c≯äù èùå</mark> ≯óå⊣ËÜͦ
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 mode	00000070  F1 F8 FE E9 A2 9E 97 81 A8 8F 93 9E 86 9C 97 9A  ñøþ颞−.∵.``žtœ−š
00000080 B8 /1 E4 19 FC 10 8A 4A FC 10 8A 4A FC 10 8A 4A , ga.u.SJu.SJu.SJ	00000080 81 CD 37 0A C2 AC 45 50 D7 A6 56 54 D3 AC 46 50 .17.Â-EPצVTÓ-FP
00000000 67 5E 12 4A FD 10 5A 4A 93 66 16 4A FE 10 5A 4A 6". UV.SJ"I.UD.SJ	00000090 40 E5 DE 4C DB BE 4C 5F B1 CC DA 4F D9 BA 41 4F $a$
00000000 93 66 14 4A FD 10 6A 4A 93 66 20 4A EF 10 6A 4A TLUY.SJT 01.SJ	000000A0 A9 C5 FE 45 C7 B7 50 4F CC CB C3 48 C7 AF 59 5D @ÅþEÇ·POÌËÄHÇ <sup>-</sup> Y]
00000000 93 66 21 44 FE 10 64 44 F3 66 19 44 FE 10 64 44 1:00.3000.09.30	000000B0 CF BC 5C 59 FD AC 59 59 AD DA EE 50 DE A6 56 54 Ï4\Yý¬YY.ŰîPÞ¦VT
00000000 FC 10 60 44 FC 10 64 44 55 66 25 44 FD 10 64 44 U.(01.50 180y.50	000000C0 BC DA DC 50 D2 AB 46 4C B5 C8 D1 5F DF BA 46 4F ¼ÚÜPÔ«FLµÈŇ_ß°FO
	000000D0 C1 F3 E8 E4 C6 B3 54 45 9C 97 9A 8C 8C 93 9A 8B Áóè䯳TE∞=šŒE°š<
00000000 50 45 00 00 46 01 03 00 92 28 53 45 00 00 00 00 DF T 2+50	000000E0  8C 8F 93 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93  (E.``žtœ—š@CE``š<(E.``
	000000F0 CE C3 9C 97 D6 8D 8F 93 26 A0 DF C0 93 9E 86 9C ÎÃ∞—Ö∿& BÀ°ž†œ
00000110 00 10 00 00 00 00 00 00 00 00 0	00000100 97 9A 8C 8C 73 9A 88 8D 84 92 94 86 9C B7 9A 8C —š@CEsš^.,/″tœ-š@C
	00000110  8C 83 9A 8B 8C 2F 92 9E 36 55 96 9A 8C 3C 92 9A  0Efš<0E/′ž6U−š0E<′š
	00000120 8B 5C 8E 93 9E 86 DC 97 9A 9C 8C 93 9A 89 8C 8F ∢\Ž"ž†Ü−šœŒ"šħæ.
00000140 00 00 AD 00 00 10 00 00 00 00 00 00 03 00 40 81	00000130  96 9E 87 9C 97 9A 8C 8C 96 9A 8A 8C 8F 93 9E 86  −ž‡œ—šŒDE-šŠŒ~ž†
00000150 00 00 10 00 00 10 00 00 00 00 10 00 00	00000140  9C 77 9B 8C 8C 83 9A 8B 8C 8F 93 9E 85 9C D7 1B  œwxEdfš<(E."ž…œ×.
00000160 00 00 00 10 00 00 00 00 00 00 00 00 00	00000150  8C 83 9A 8B 9C 8F 93 9E 86 8C 97 9A 9C 8C 93  002fð<0e.~žt0—šoc0:~
00000170 B8 F1 AC 00 DC 00 00 00 F0 AC 00 B8 01 00 00 .ñ-,Üð-,	00000160 9A 8B 8C 8F 83 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C š∢C.∫ž†œ—š@CC."š∢C
00000180 00 00 00 00 00 00 00 00 00 00 00 00 0	00000170 7B 42 9F 86 40 97 9A 8C 8C 43 9B 8B 78 8E 93 9E {Bϔ+0,—š0ECC∨xްž
00000190 00 00 00 00 00 00 00 00 00 00 00 00 0	00000180 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 9C 97 ta⇔≝002C°ĕ∢0E.°žta⇔
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 0	00000190 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 9C 97 9A 8C 8C ĕŒŒ™š<Œ.∿ž†œ—šŒŒ
000001B0 00 00 00 00 00 00 00 00 88 EE AC 00 48 00 00 00îjH	000001A0 93 9A 8B 8C 8F 93 9E 86 9C 97 9A 8C 8C 93 9A 8B "ă<(Œ.°Ž†œ—ăŒE°ă<
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 0	000001B0  8C 8F 93 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93  €.``ž†œ—ĕœœ°š<€.``
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 0	000001C0 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 9C žta≔-ă00C°š∢(C.°žtae
000001E0 00 00 00 00 00 00 00 55 50 58 30 00 00 00 00UPX0	000001D0 97 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 9C 97 9A 8C —š0D2C°š∢0C.∿ž†na—š0C
000001F0 00 C0 AC 00 00 10 00 00 00 00 00 00 00 04 00 00 .À¬	000001E0  8C 93 9A 8B 8C 8F 93 9E D3 CC CF AA 8C 8C 93 9A  Œ`š<Œ.`žÓÌϪŒŒ`š
00000200 00 00 00 00 00 00 00 00 00 00 0	000001F0 8B 2C 8E 93 9E 96 9C 97 9A 8C 8C 93 9A 8F 8C 8F ≺,Ž`ž-œ—šŒŒ`š.Œ.
00000210 55 50 58 31 00 00 00 00 00 20 00 00 D0 AC 00 UPX1Ь.	00000200 93 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C 0F 93 9E 66 °°Ž†æ—ŠŒE°š<Œ.°Žf
00000220 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00	00000210  C9 C7 C2 BD 8C 93 9A 8B 8C AF 93 9E 86 2C 96 9A  ÉÇÂ¥Œ™Š<Œ¯™ž†,−š
00000230 00 00 00 00 40 00 00 E0 2E 72 73 72 63 00 00 00@à.rsrc	00000220  8C 90 93 9A 8B 88 8F 93 9E 86 9C 97 9A 8C 8C 93  (E.`š∢^.`ž†œ—š@CE`
00000240 00 10 00 00 00 F0 AC 00 00 04 00 00 00 24 00 00ð¬\$	00000230 9A 8B 8C 8F D3 9E 86 7C B9 E8 FF FE F0 9A 8B 8C š∢Œ.ÓŽ† ≐èÿpðš∢Œ
00000250 00 00 00 00 00 00 00 00 00 00 00 00 40 00 0	00000240 8F83 9E869C479B8C8C979A8B8CAF939E .fžtœG>000_š<0⊂ <sup>™</sup> ž
00000260 00 00 00 00 00 00 00 00 00 00 00 00 0	00000250 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93 DE 86 9C 57 tα—š000C°š∢0C.°ÞrhaeW
00000270 00 00 00 00 00 00 00 00 00 00 00 00 0	00000260 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 9C 97 9A 8C 8C šOBE™š∢OE."ކoz—šOBE
00000280 00 00 00 00 00 00 00 00 00 00 00 00 0	00000270 93 9A 8B 8C 8F 93 9E 86 9C 97 9A 8C 8C 93 9A 8B °š∢CE.°ž†œ—šCEC°š<
00000290 00 00 00 00 00 00 00 00 00 00 00 00 0	00000280  8C 8F 93 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93  0E.°ž†œ—š0CE°š<(E.°
	= 00000290 9E 86 9C 97 9A 8C 8C 93 9A 8B 8C 8F 93 9E 86 9C ž†o≔-š003C*š∢0C.**ž†oe

'file'은 원래 exe라고 했다. 따라서 암호화하기 전에는 드래그 한 부분이 run.exe 처럼 cannot be run이라는걸 알 수 있다. 이정보를 토대로 c로 코 드를 짜보면

 $\blacksquare < >$  **b**  $\Box \land \circ >$  **b**  $\Box \land \circ >$  **c** main.c > No Selection

93		
94		
95	#include <stdio.h></stdio.h>	
96		
97	<pre>int main(){</pre>	
98	int decode[] = $\{0 \times F0, 0 \times FB, 0 \times E5, 0 \times E2, 0 \times E0, 0 \times E1, 0 \times $	,0xE7,0xBE,0xE4,0xF9,0xB7,0xE8,0xF9,0xE2,0x00};
99	char *origin = "cannot be run";	
100	<pre>printf("key:");</pre>	
101	<pre>char *Keys=(char*)malloc(sizeof(char)*14) for (int i=0.i(1()))</pre>	); 2 A Implicitly declaring library function 'malloc' with type 'void *(unsigned long)'
102	for (int $j=0; j<14; ++j)$ {	
103	$if((abar))((dacada[i] \land kay) \land article for the formula of the fo$	/1 ff) origin[i]){
104	printf("%c" key) · 0x1	
105		
107	}	
108	}	
109	<pre>getchar();</pre>	
110	return (0);	
111	}	
112		
113		
114		
115		
116		
117		
	key	y:letsplaychess
Auto 😂	I Filter All O	Output ≎
<b>_</b> 1_		
ヲ[_	값이 'letsplaychess'단걸 알 수	
ر حد		

< 🛆 >

한번 run에 집어 넣어서 file을 복구시키자.

#### I C:₩Users₩성준₩Desktop₩리버싱기초 이해₩ransomware₩run.exe

나는 나쁜놈이다! 나는 매우 나쁘기 때문에 너의 파일을 암호화했다! 너의 파일을 복구하고 싶다면 5천억 달러를 입금하고 받은 키값으로 파일을 복구해라!

Key : letsplaychess

파일을 복구했다! 나는 몹시 나쁘지만 약속은 지키는 사나이다! 따라서 너가 나에게 돈을 줬고, 올바른 키값을 받았다면 파일은 정상화 되어 있을 것이다! 하지만 만약 잘못된 키를 넣었다면 나는 아주아주 나쁘기 때문에 너의 파일은 또 망가질 것이다!

# 키 값을 입력하면 복호화를 진행해준다.

 $\times$ 

❷ HxD - [C:₩	#Users	₩Q.	ć₩D	eskt	op₩	리버	장기	조 0	<b>⊳</b>  ₩	ranso	omw	are₩	file]								
🔊 파일(F) 편	편집(E)	찾	71(S)	보	21(2)	) 분	석(A	) 7	타성	설정()	x) を	: 설	정(W	) ?							
🗅 🙈 🕶 🥅	Same		<del>+</del> +	16		$\sim$	AN	SI		$\sim$	16	진수	~	1							
n file	1 4.					_															
a nie																					
Offset(h)	00	01	02	03	04	05	06	07	08	09	оA	0В	0C	OD	0E	OF					
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZÿÿ				
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	FO	00	00	00	ð	•			
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	°´.İ!,.Lİ!Th	1			
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno	2			
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS				
00000070	60	61	54	65	26	20	CD	Ca	24	20	00	00	40	20	00	00	mode				
00000080	00	-11 6F	52	90	49	20	CA	C3	26	20	56	C3	47	20	CA	C3	THE TAKE TAKE TAKE TAKE TAKE TAKE TAKE TAK	λ. Δ			
000000000	2.6	56	52 60	C3	5B	20	CA	C3	40	58	59	C3	4B	20	CA	C3	LA VYZK ÉŽ SVYZK ÉŽ	ŝ			
00000080	49	20	CB	C3	71	20	CA	C3	26	56	61	C3	40	20	CA	C3	I ËÃO ÊÃsVaÃO ÊÃ	ŝ			
000000000	26	56	50	C3	48	20	CA	C3	26	56	57	C3	48	20	CA	C3	&VPĂH ÊĂ&VWĂH ÊĂ	4			
00000000	52	69	63	68	49	20	CA	C3	00	00	00	00	00	00	00	00	RichI ÊÃ				
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
000000F0	50	45	00	00	4C	01	03	00	BC	2B	53	4F	00	00	00	00	PEL↓₄+SO				
00000100	00	00	00	00	ΕO	00	03	01	0B	01	AO	00	00	20	00	00	à				
00000110	00	10	00	00	00	AO	01	00	BO	C9	01	00	00	BO	01	00	°É°	•			
00000120	00	DO	01	00	00	00	40	00	00	10	00	00	00	02	00	00	.Ð@	•			
00000130	05	00	01	00	00	00	00	00	05	00	01	00	00	00	00	00		4			
00000140	00	EO	10	00	00	10	00	00	00	00	10	00	03	10	40	81	.a@.	·			
00000150	00	00	10	00	10	10	00	00	00	00	10	00	00	10	00	00					
00000170	F4	100	01	00	DC	00	00	00	00	DO	01	00	F4	01	00	00	ÂÑ Ü Đ Â	·			
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	00	00	00	00	00	00	00	00	55	50	58	30	00	00	00	00	UPX0	•			
000001F0	00	AO	01	00	00	10	00	00	00	00	00	00	00	04	00	00					
00000200	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	EO	ۈ	1			
00000210	55	50	58	31	00	00	00	00	00	20	00	00	00	BO	01	00	UPX1	·			
00000220	00	10	00	00	40	04	00	FO	25	72	73	72	63	00	00	00	a à rero				
00000230	00	10	00	00	00	DO	01	00	00	04	00	00	00	20	00	00		·			
00000250	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	co	ά	A			
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	0.0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					

# hxd로보면 pe헤더가 mz로 시작한다 올바르게 복호화 된 것이다. 이제 확장자를 .exe로 바꾸고 실행 해보자.



2017-07-12 오후 5:36 응용 프로그램

9KB

# 복호화 됐으니 exe파일로 바꿔서 실행을 시켜보자.

## III C:₩Users₩성준₩Desktop₩리버싱기초 이해₩ransomware₩file.exe

Key -> Colle System

# 키 값이 나왔다.

