

CPU - thread 00002228, module Script

5C4DC1F9	8BE8	MOV EBP, EAX
5C4DC1FB	33C0	XOR EAX, EAX
5C4DC1FD	85ED	TEST EBP, EBP
5C4DC1FF	7E 11	JLE SHORT Script.5C4DC212
5C4DC201	8B93 4C1F0000	MOV EDX, DWORD PTR DS:[EBX+1F4C]
5C4DC207	8A0C10	MOV CL, BYTE PTR DS:[EAX+EDX]
5C4DC20A	8B0C06	MOV BYTE PTR DS:[ESI+EAX], CL
5C4DC20D	40	INC EAX
5C4DC20E	3BC5	CMP EAX, EBP
5C4DC210	7C EF	JL SHORT Script.5C4DC201
5C4DC212	0FB615 A3C3A45C	MOVZX EDX, BYTE PTR DS:[5CA4C3A3]
5C4DC219	8B2D E0C3A45C	MOV EBP, DWORD PTR DS:[5CA4C3E0]
5C4DC21F	03FA	ADD EDI, EDX
5C4DC221	81BD D4180000 F	CMP DWORD PTR SS:[EBP+18D4], 0FA
5C4DC22B	897C24 20	MOV DWORD PTR SS:[ESP+20], EDI
5C4DC22F	0F8C 89000000	JL Script.5C4DC2BE
5C4DC235	81C5 D8180100	ADD EBP, 118D8
5C4DC23B	C74424 10 F90000	MOV DWORD PTR SS:[ESP+10], 0F9
5C4DC243	68 00010000	PUSH 100
5C4DC248	6A 00	PUSH 0

DS:[0BD14C1A]=0BD1CFD8
EDX=0BD1CFD8

Registers (FPU)

EAX 00000001
ECX 00000081
EDX 0BD1CFD8
EBX 0BD12CC8
ESP 0EEBF60C
EBP 00000004
ESI 0BD133B4
EDI 0BD07A6D
EIP 5C4DC201 Script.5C4DC201
C I ES 002B 32bit 0(FFFFFFFF)
P O CS 0023 32bit 0(FFFFFFFF)
A I SS 002B 32bit 0(FFFFFFFF)
Z O DS 002B 32bit 0(FFFFFFFF)
S I FS 0053 32bit CA2000(FFF)
T O GS 002B 32bit 0(FFFFFFFF)
D O
O O LastErr ERROR_SUCCESS (00000000)
EFL 00000293 (NO, B, NE, BE, S, PO, L, LE)
ST0 empty 277775.7812500000000
ST1 empty 1.000000000000000000

Address Hex dump ASCII

0BD1D288 02 00 00 00 43 00 AB AB AB AB AB AB EE FE 7...C. 4444444444444444
0BD1D298 EE FE EE FE EE FE EE FE 00 00 00 00 00 00 00 00
0BD1D2A8 7F D4 32 58 09 46 00 1A 01 00 00 00 43 00 AB AB y2X.F.→r...C. 4444
0BD1D2B8 AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00
0BD1D2C8 7F D4 31 58 08 46 00 00 C8 D8 D1 08 E8 AB D1 08 ytl]CF...30424444
0BD1D2D8 EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE
0BD1D2E8 7F D4 32 58 08 46 00 1A 01 00 00 00 43 00 AB AB y2XCF.→r...C. 4444
0BD1D2F8 AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00
0BD1D308 7F D4 31 5D 08 46 00 00 E0 C8 D1 08 C0 00 D1 08 ytl]CF...44444444
0BD1D318 7F D4 32 58 0E 46 00 1A 01 00 00 00 43 00 AB AB y2XDF.→r...C. 4444
0BD1D328 AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00
0BD1D338 7F D4 31 5D 08 46 00 00 10 85 D1 08 68 EA D1 08 ytl]CF...+zh-2
0BD1D348 7F D4 32 58 0E 46 00 1A 01 00 00 00 43 00 AB AB y2XDF.→r...C. 4444
0BD1D358 AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00
0BD1D368 65 D4 32 42 08 46 00 18 01 00 00 00 00 00 00 00 ey2BDF.Tf.....

Executable modules

Base	Size	Entry	Name	File version	Path
008C0000	00041000	008D7600	karano	2, 0, 0, 8	D:\MyFiles\Projects\
58040000	02883000	59165C70	nvd3dum	31.0.15.3141	C:\Windows\System32\
5C450000	00063000	5C49FEA0	D3D1M700	10.0.19041.1 (W	C:\Windows\SYSTEM32\
5C4C0000	0059A000	5C508093	Script		D:\MyFiles\Projects\
5C460000	0022A000	5CA66AEB	nvspcap	3.27.0.112	C:\Windows\System32\
5CF00000	000F3000	5CF58230	Window_l	10.0.19041.1 (W	C:\Windows\System32\
5D030000	000E9000	5D0412A0	ddraw	10.0.19041.2604	C:\Windows\SYSTEM32\
5D120000	00096000	5D14F7C0	nvidumd	31.0.15.3141	C:\Windows\System32\
5D1C0000	001FF000	5D37EC0D	d3dx9_43	9.29.952.3111	C:\Windows\SYSTEM32\
5D3C0000	000ED000	5D485E00	InputHos	10.0.19041.1741	C:\Windows\System32\
5D500000	00007000	5D502020	DCIMAN32	10.0.19041.2075	C:\Windows\SYSTEM32\
5D510000	00073000	5D56ED80	WindowMa		C:\Windows\System32\
5D590000	00050000	5D599DA3	Sound		D:\MyFiles\Projects\

Breakpoints

Address	Module	Active	Disassembly
5C4DC212	Script	Always	MOVZX EDX, BYTE PTR DS:[5C4DC212]

여기가 이름 받아오는파트는 맞음

5C4DC207 MOVE CL BYTE PTR DS:[EAX+EDX]

여기서 CL에 EDX로부터 EAX만큼의 오프셋을 이동시킨 WORD하나를 추출해온다.

5C4DC20A MOV BYTE PTR DS:[ESI+EAX],CL

이부분이 (CL에 추출된 글자)를 메모리에 하나씩 넣는 부분.

그렇다면 원본은 어디서부터 시작됐느냐?

반복구문이 시작되는 곳에서 EDX에 받아왔음.

5C4DC201 MOV EDX,DWORD PTR DS:[EBX+1F4C]

EDX에 [EBX+1F4C]라는 주소에 있는 값을 넣는데 이걸 자세히 생각하기에는 뇌에 과부하가 왔으니 생략

어차피 EDX에 다 받아왔고 EDX가 가리키는 부분의 값을 바꾸면 게임화면 출력값도 바뀜

결론1 : 이름추출은 5C4DC201, EDX 인줄 알았는데 아닌가봄 ππππππππ

Assembly dump showing instructions and registers. The instruction at address 81 is `INC EAX`, which increments the EAX register. The registers window shows EAX as 00000001. The memory dump shows the value 01 at address 81.

Registers (FPU):

- EAX: 00000001
- ECX: 00000001
- EDX: 00000000
- EBX: 00000000
- ESP: 00000000
- EBP: 00000000
- ESI: 00000000
- EDI: 00000000

Memory dump (Address 81):

Address	Hex dump	ASCII
00B055A8	81 75 82 A0 81 5C 81 5C 3C 8F AC 89 48 3C 82 B1	はね、おはよう
00B055B8	82 C0 82 C8 3E 81 A1 82 A8 82 C0 82 E6 82 A4 81	はね、おはよう
00B055C8	76 00 81 42 00 A8 AB AB AB AB AB AB FE EE FE	はね、おはよう
00B055D8	00 00 00 00 00 00 00 7F D4 32 58 04 A6 05 1A	はね、おはよう
00B055E8	03 00 00 00 43 00 AB AB AB AB AB AB AB EE FE	はね、おはよう
00B055F8	00 00 00 00 00 00 00 65 D4 32 42 08 46 05 18	はね、おはよう
00B05608	01 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05618	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05628	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05638	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05648	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05658	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05668	18 43 8D 08 00 00 00 CC 88 D1 08 00 00 00 00	はね、おはよう
00B05678	C8 88 D1 08 00 00 00 FC D0 08 00 00 00 00 00	はね、おはよう
00B05688	F8 D0 D1 08 00 00 00 0C AB 8D 08 00 00 00 00	はね、おはよう

본격적으로 CL로 한글자씩 뽑아내는 것을 확인가능. 사진상에서 81이 ECX의 마지막(CL)부분에 들어갔고, 이는 문장 시작지점의 WORD값인 81과 동일한 것이 보인다.

Assembly dump showing instructions and registers. The instruction at address 81 is `INC EAX`, which increments the EAX register. The registers window shows EAX as 00000001. The memory dump shows the value 01 at address 81.

Registers (FPU):

- EAX: 00000001
- ECX: 00000001
- EDX: 00000000
- EBX: 00000000
- ESP: 00000000
- EBP: 00000000
- ESI: 00000000
- EDI: 00000000

Memory dump (Address 81):

Address	Hex dump	ASCII
00B055A8	81 75 82 A0 81 5C 81 5C 3C 8F AC 89 48 3C 82 B1	はね、おはよう
00B055B8	82 C0 82 C8 3E 81 A1 82 A8 82 C0 82 E6 82 A4 81	はね、おはよう
00B055C8	76 00 81 42 00 A8 AB AB AB AB AB AB FE EE FE	はね、おはよう
00B055D8	00 00 00 00 00 00 00 7F D4 32 58 04 A6 05 1A	はね、おはよう
00B055E8	03 00 00 00 43 00 AB AB AB AB AB AB AB EE FE	はね、おはよう
00B055F8	00 00 00 00 00 00 00 65 D4 32 42 08 46 05 18	はね、おはよう
00B05608	01 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05618	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05628	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05638	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05648	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05658	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05668	18 43 8D 08 00 00 00 CC 88 D1 08 00 00 00 00	はね、おはよう
00B05678	C8 88 D1 08 00 00 00 FC D0 08 00 00 00 00 00	はね、おはよう
00B05688	F8 D0 D1 08 00 00 00 0C AB 8D 08 00 00 00 00	はね、おはよう

Dump창에서 메모리에 81이 들어갔다. INC EAX로 1씩 증가시키면서 EBP와 비교하는데, 이전에 문자길이 잦을 때 21을 저장한 곳이 바로 이 때를 위함이다.

Assembly dump showing instructions and registers. The instruction at address 81 is `INC EAX`, which increments the EAX register. The registers window shows EAX as 00000001. The memory dump shows the value 01 at address 81.

Registers (FPU):

- EAX: 00000001
- ECX: 00000001
- EDX: 00000000
- EBX: 00000000
- ESP: 00000000
- EBP: 00000000
- ESI: 00000000
- EDI: 00000000

Memory dump (Address 81):

Address	Hex dump	ASCII
00B055A8	81 75 82 A0 81 5C 81 5C 3C 8F AC 89 48 3C 82 B1	はね、おはよう
00B055B8	82 C0 82 C8 3E 81 A1 82 A8 82 C0 82 E6 82 A4 81	はね、おはよう
00B055C8	76 00 81 42 00 A8 AB AB AB AB AB AB FE EE FE	はね、おはよう
00B055D8	00 00 00 00 00 00 00 7F D4 32 58 04 A6 05 1A	はね、おはよう
00B055E8	03 00 00 00 43 00 AB AB AB AB AB AB AB EE FE	はね、おはよう
00B055F8	00 00 00 00 00 00 00 65 D4 32 42 08 46 05 18	はね、おはよう
00B05608	01 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05618	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05628	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05638	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05648	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05658	00 00 00 00 00 00 00 00 00 00 00 00 00 00	はね、おはよう
00B05668	18 43 8D 08 00 00 00 CC 88 D1 08 00 00 00 00	はね、おはよう
00B05678	C8 88 D1 08 00 00 00 FC D0 08 00 00 00 00 00	はね、おはよう
00B05688	F8 D0 D1 08 00 00 00 0C AB 8D 08 00 00 00 00	はね、おはよう

한번 원본값을 바꿔보자.

CPU - thread 00002208, module Script		Registers (FPU)		Memory map	
5C4DC1E6	8050 01	LEA EDX,DWORD PTR DS:[EAX+1]	EAX 0000000B	7AF8A000	00001000 cfmgr32 .data
5C4DC1E9	80A24 00000000	LEA ESP,DWORD PTR SS:[ESP]	ECX 000000AC	7AF85000	00002000 cfmgr32 .idata
5C4DC1F0	8A08	MOV CL,BYTE PTR DS:[EAX]	EDX 00005A8	7AF87000	00001000 cfmgr32 .idata
5C4DC1F2	40	TNC EAX	EBX 0BD12C28	7AF88000	00001000 cfmgr32 .rsrc
5C4DC1F3	8AC9	TEST CL,CL	ESP 0EEBF60C	7AF89000	00002000 cfmgr32 .reloc
5C4DC1F5	75 F9	JNZ SHORT Script.5C4DC1F0	EBP 00000021	7AF8C000	00001000 KERNELBA
5C4DC1F7	2BC2	SUB EAX,EDX	ESI 0BD13B4	7AF8D000	00001000 KERNELBA
5C4DC1F9	8BE8	MOV EBP,EAX	EDI 0BB07A90	7AF8E000	00001000 KERNELBA
5C4DC1FB	33C0	XOR EAX,EAX	EIP 5C4DC20E	7AF8F000	00001000 KERNELBA
5C4DC1FD	85ED	TEST EBP,EBP	C I ES 0028 32bit 0(FFFFFFFF)	7AF90000	00001000 SHCORE
5C4DC1FF	7E 11	JLE SHORT Script.5C4DC212	P 0 CS 0023 32bit 0(FFFFFFFF)	7AF91000	00001000 SHCORE
5C4DC201	8B93 AC1F0000	MOV EDX,DWORD PTR DS:[EBX+1F4C]	A 0 SS 0023 32bit 0(FFFFFFFF)	7AF92000	00001000 SHCORE
5C4DC207	8A0C10	MOV CL,BYTE PTR DS:[EAX+EDX]	Z 0 DS 0028 32bit 0(FFFFFFFF)	7AF93000	00001000 SHCORE
5C4DC20A	8B0C06	MOV BYTE PTR DS:[ESI+EAX],CL	S 0 FS 0053 32bit CA2000(FFF)	7AF94000	00001000 SHCORE
5C4DC20D	40	TNC EAX	T 0 GS 0028 32bit 0(FFFFFFFF)	7AF95000	00001000 SHCORE
5C4DC20E	3BC5	CMP EAX,EBP	D 0	7AF96000	00001000 SHCORE
5C4DC210	7C EF	JL SHORT Script.5C4DC201	0 0 LastErr ERROR_SUCCESS (00000000)	7AF97000	00001000 SHCORE
5C4DC212	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]	EFL 00000203 (NO,B,NE,BE,NS,PO,GE,G)	7AF98000	00001000 SHCORE
5C4DC219	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]	ST0 empty 277775.78125000000000	7AF99000	00001000 SHCORE
5C4DC21F	03FA	ADD EDI,EDX	ST1 empty 1.000000000000000000	7AF9A000	00001000 SHCORE
5C4DC220	40	TNC EAX		7AF9B000	00001000 SHCORE
5C4DC22E	3BC5	CMP EAX,EBP		7AF9C000	00001000 SHCORE
5C4DC230	7C EF	JL SHORT Script.5C4DC201		7AF9D000	00001000 SHCORE
5C4DC232	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF9E000	00001000 SHCORE
5C4DC239	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF9F000	00001000 SHCORE
5C4DC23F	03FA	ADD EDI,EDX		7AF80000	00001000 cfmgr32 .data
5C4DC240	40	TNC EAX		7AF81000	00001000 cfmgr32 .idata
5C4DC242	8AC9	TEST CL,CL		7AF82000	00001000 cfmgr32 .rsrc
5C4DC244	75 F9	JNZ SHORT Script.5C4DC230		7AF83000	00001000 cfmgr32 .reloc
5C4DC246	2BC2	SUB EAX,EDX		7AF84000	00001000 cfmgr32 .text
5C4DC248	8BE8	MOV EBP,EAX		7AF85000	00001000 cfmgr32 .code,export
5C4DC24A	33C0	XOR EAX,EAX		7AF86000	00001000 cfmgr32 .text
5C4DC24C	85ED	TEST EBP,EBP		7AF87000	00001000 cfmgr32 .code,export
5C4DC24E	7E 11	JLE SHORT Script.5C4DC232		7AF88000	00001000 cfmgr32 .text
5C4DC250	8B93 AC1F0000	MOV EDX,DWORD PTR DS:[EBX+1F4C]		7AF89000	00001000 cfmgr32 .code,export
5C4DC252	8A0C10	MOV CL,BYTE PTR DS:[EAX+EDX]		7AF8A000	00001000 cfmgr32 .text
5C4DC254	8B0C06	MOV BYTE PTR DS:[ESI+EAX],CL		7AF8B000	00001000 cfmgr32 .code,export
5C4DC256	40	TNC EAX		7AF8C000	00001000 cfmgr32 .text
5C4DC258	3BC5	CMP EAX,EBP		7AF8D000	00001000 cfmgr32 .code,export
5C4DC25A	7C EF	JL SHORT Script.5C4DC250		7AF8E000	00001000 cfmgr32 .text
5C4DC25C	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF8F000	00001000 cfmgr32 .code,export
5C4DC25E	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF90000	00001000 cfmgr32 .text
5C4DC260	03FA	ADD EDI,EDX		7AF91000	00001000 cfmgr32 .code,export
5C4DC262	40	TNC EAX		7AF92000	00001000 cfmgr32 .text
5C4DC264	3BC5	CMP EAX,EBP		7AF93000	00001000 cfmgr32 .code,export
5C4DC266	7C EF	JL SHORT Script.5C4DC260		7AF94000	00001000 cfmgr32 .text
5C4DC268	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF95000	00001000 cfmgr32 .code,export
5C4DC26A	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF96000	00001000 cfmgr32 .text
5C4DC26C	03FA	ADD EDI,EDX		7AF97000	00001000 cfmgr32 .code,export
5C4DC26E	40	TNC EAX		7AF98000	00001000 cfmgr32 .text
5C4DC270	3BC5	CMP EAX,EBP		7AF99000	00001000 cfmgr32 .code,export
5C4DC272	7C EF	JL SHORT Script.5C4DC270		7AF9A000	00001000 cfmgr32 .text
5C4DC274	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF9B000	00001000 cfmgr32 .code,export
5C4DC276	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF9C000	00001000 cfmgr32 .text
5C4DC278	03FA	ADD EDI,EDX		7AF9D000	00001000 cfmgr32 .code,export
5C4DC27A	40	TNC EAX		7AF9E000	00001000 cfmgr32 .text
5C4DC27C	3BC5	CMP EAX,EBP		7AF9F000	00001000 cfmgr32 .code,export
5C4DC27E	7C EF	JL SHORT Script.5C4DC27C		7AF80000	00001000 cfmgr32 .data
5C4DC280	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF81000	00001000 cfmgr32 .idata
5C4DC282	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF82000	00001000 cfmgr32 .rsrc
5C4DC284	03FA	ADD EDI,EDX		7AF83000	00001000 cfmgr32 .reloc
5C4DC286	40	TNC EAX		7AF84000	00001000 cfmgr32 .text
5C4DC288	3BC5	CMP EAX,EBP		7AF85000	00001000 cfmgr32 .code,export
5C4DC28A	7C EF	JL SHORT Script.5C4DC286		7AF86000	00001000 cfmgr32 .text
5C4DC28C	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF87000	00001000 cfmgr32 .code,export
5C4DC28E	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF88000	00001000 cfmgr32 .text
5C4DC290	03FA	ADD EDI,EDX		7AF89000	00001000 cfmgr32 .code,export
5C4DC292	40	TNC EAX		7AF8A000	00001000 cfmgr32 .text
5C4DC294	3BC5	CMP EAX,EBP		7AF8B000	00001000 cfmgr32 .code,export
5C4DC296	7C EF	JL SHORT Script.5C4DC294		7AF8C000	00001000 cfmgr32 .text
5C4DC298	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF8D000	00001000 cfmgr32 .code,export
5C4DC29A	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF8E000	00001000 cfmgr32 .text
5C4DC29C	03FA	ADD EDI,EDX		7AF8F000	00001000 cfmgr32 .code,export
5C4DC29E	40	TNC EAX		7AF90000	00001000 cfmgr32 .text
5C4DC2A0	3BC5	CMP EAX,EBP		7AF91000	00001000 cfmgr32 .code,export
5C4DC2A2	7C EF	JL SHORT Script.5C4DC2A0		7AF92000	00001000 cfmgr32 .text
5C4DC2A4	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF93000	00001000 cfmgr32 .code,export
5C4DC2A6	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF94000	00001000 cfmgr32 .text
5C4DC2A8	03FA	ADD EDI,EDX		7AF95000	00001000 cfmgr32 .code,export
5C4DC2AA	40	TNC EAX		7AF96000	00001000 cfmgr32 .text
5C4DC2AC	3BC5	CMP EAX,EBP		7AF97000	00001000 cfmgr32 .code,export
5C4DC2AE	7C EF	JL SHORT Script.5C4DC2AC		7AF98000	00001000 cfmgr32 .text
5C4DC2B0	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF99000	00001000 cfmgr32 .code,export
5C4DC2B2	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF9A000	00001000 cfmgr32 .text
5C4DC2B4	03FA	ADD EDI,EDX		7AF9B000	00001000 cfmgr32 .code,export
5C4DC2B6	40	TNC EAX		7AF9C000	00001000 cfmgr32 .text
5C4DC2B8	3BC5	CMP EAX,EBP		7AF9D000	00001000 cfmgr32 .code,export
5C4DC2BA	7C EF	JL SHORT Script.5C4DC2B8		7AF9E000	00001000 cfmgr32 .text
5C4DC2BC	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF9F000	00001000 cfmgr32 .code,export
5C4DC2BE	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF80000	00001000 cfmgr32 .data
5C4DC2C0	03FA	ADD EDI,EDX		7AF81000	00001000 cfmgr32 .idata
5C4DC2C2	40	TNC EAX		7AF82000	00001000 cfmgr32 .rsrc
5C4DC2C4	3BC5	CMP EAX,EBP		7AF83000	00001000 cfmgr32 .reloc
5C4DC2C6	7C EF	JL SHORT Script.5C4DC2C4		7AF84000	00001000 cfmgr32 .text
5C4DC2C8	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF85000	00001000 cfmgr32 .code,export
5C4DC2CA	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF86000	00001000 cfmgr32 .text
5C4DC2CC	03FA	ADD EDI,EDX		7AF87000	00001000 cfmgr32 .code,export
5C4DC2CE	40	TNC EAX		7AF88000	00001000 cfmgr32 .text
5C4DC2D0	3BC5	CMP EAX,EBP		7AF89000	00001000 cfmgr32 .code,export
5C4DC2D2	7C EF	JL SHORT Script.5C4DC2D0		7AF8A000	00001000 cfmgr32 .text
5C4DC2D4	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF8B000	00001000 cfmgr32 .code,export
5C4DC2D6	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF8C000	00001000 cfmgr32 .text
5C4DC2D8	03FA	ADD EDI,EDX		7AF8D000	00001000 cfmgr32 .code,export
5C4DC2DA	40	TNC EAX		7AF8E000	00001000 cfmgr32 .text
5C4DC2DC	3BC5	CMP EAX,EBP		7AF8F000	00001000 cfmgr32 .code,export
5C4DC2DE	7C EF	JL SHORT Script.5C4DC2DC		7AF90000	00001000 cfmgr32 .text
5C4DC2E0	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF91000	00001000 cfmgr32 .code,export
5C4DC2E2	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF92000	00001000 cfmgr32 .text
5C4DC2E4	03FA	ADD EDI,EDX		7AF93000	00001000 cfmgr32 .code,export
5C4DC2E6	40	TNC EAX		7AF94000	00001000 cfmgr32 .text
5C4DC2E8	3BC5	CMP EAX,EBP		7AF95000	00001000 cfmgr32 .code,export
5C4DC2EA	7C EF	JL SHORT Script.5C4DC2E8		7AF96000	00001000 cfmgr32 .text
5C4DC2EC	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF97000	00001000 cfmgr32 .code,export
5C4DC2EE	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF98000	00001000 cfmgr32 .text
5C4DC2F0	03FA	ADD EDI,EDX		7AF99000	00001000 cfmgr32 .code,export
5C4DC2F2	40	TNC EAX		7AF9A000	00001000 cfmgr32 .text
5C4DC2F4	3BC5	CMP EAX,EBP		7AF9B000	00001000 cfmgr32 .code,export
5C4DC2F6	7C EF	JL SHORT Script.5C4DC2F4		7AF9C000	00001000 cfmgr32 .text
5C4DC2F8	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF9D000	00001000 cfmgr32 .code,export
5C4DC2FA	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF9E000	00001000 cfmgr32 .text
5C4DC2FC	03FA	ADD EDI,EDX		7AF9F000	00001000 cfmgr32 .code,export
5C4DC2FE	40	TNC EAX		7AF80000	00001000 cfmgr32 .data
5C4DC300	3BC5	CMP EAX,EBP		7AF81000	00001000 cfmgr32 .idata
5C4DC302	7C EF	JL SHORT Script.5C4DC300		7AF82000	00001000 cfmgr32 .rsrc
5C4DC304	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF83000	00001000 cfmgr32 .reloc
5C4DC306	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF84000	00001000 cfmgr32 .text
5C4DC308	03FA	ADD EDI,EDX		7AF85000	00001000 cfmgr32 .code,export
5C4DC30A	40	TNC EAX		7AF86000	00001000 cfmgr32 .text
5C4DC30C	3BC5	CMP EAX,EBP		7AF87000	00001000 cfmgr32 .code,export
5C4DC30E	7C EF	JL SHORT Script.5C4DC30C		7AF88000	00001000 cfmgr32 .text
5C4DC310	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF89000	00001000 cfmgr32 .code,export
5C4DC312	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF8A000	00001000 cfmgr32 .text
5C4DC314	03FA	ADD EDI,EDX		7AF8B000	00001000 cfmgr32 .code,export
5C4DC316	40	TNC EAX		7AF8C000	00001000 cfmgr32 .text
5C4DC318	3BC5	CMP EAX,EBP		7AF8D000	00001000 cfmgr32 .code,export
5C4DC31A	7C EF	JL SHORT Script.5C4DC318		7AF8E000	00001000 cfmgr32 .text
5C4DC31C	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF8F000	00001000 cfmgr32 .code,export
5C4DC31E	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF90000	00001000 cfmgr32 .text
5C4DC320	03FA	ADD EDI,EDX		7AF91000	00001000 cfmgr32 .code,export
5C4DC322	40	TNC EAX		7AF92000	00001000 cfmgr32 .text
5C4DC324	3BC5	CMP EAX,EBP		7AF93000	00001000 cfmgr32 .code,export
5C4DC326	7C EF	JL SHORT Script.5C4DC324		7AF94000	00001000 cfmgr32 .text
5C4DC328	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF95000	00001000 cfmgr32 .code,export
5C4DC32A	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF96000	00001000 cfmgr32 .text
5C4DC32C	03FA	ADD EDI,EDX		7AF97000	00001000 cfmgr32 .code,export
5C4DC32E	40	TNC EAX		7AF98000	00001000 cfmgr32 .text
5C4DC330	3BC5	CMP EAX,EBP		7AF99000	00001000 cfmgr32 .code,export
5C4DC332	7C EF	JL SHORT Script.5C4DC330		7AF9A000	00001000 cfmgr32 .text
5C4DC334	0FB615 A3C3AA5C	MOVZX EDX,BYTE PTR DS:[5C4AC3A3]		7AF9B000	00001000 cfmgr32 .code,export
5C4DC336	8B20 E0C3A45C	MOV EBP,DWORD PTR DS:[5C4AC3E0]		7AF9C000	00001000 cfmgr32 .text
5C4DC338	03FA	ADD EDI,EDX		7AF9D000	00001000 cfmgr32 .code,export
5C4DC33A	40	TNC EAX		7AF9E0	

정리

1. 이름추출은 5C4DC201, EDX
2. 대사추출은 5C4DC201, EDX
3. 어라? 같은코드 쓰는구먼...

HOOK(대충 스크립트.dll에서연결!0x5C4DC201,TRANS(???EDX???,TWobyte,OVERWRITE(IGNORE)),RETNPOS(COPY))

이런식으로 나오긴 할 듯..

추가) 프로세스 새로 열어도 똑같이 잘 작동함

The screenshot displays a debugger interface with three main panels:

- Assembly View:** Shows instructions starting from address 5C4DC1F9. Key instructions include:
 - MOV EBP, EAX
 - TEST EBP, EBP
 - JLE SHORT Script.5C4DC212
 - MOV EDI, DWORD PTR DS:[EBX+1FAC]
 - MOV CL, BYTE PTR DS:[EAX+EDX]
 - MOV BYTE PTR DS:[ESI+EAX], CL
 - INC EAX
 - CMP EAX, EBP
 - JL SHORT Script.5C4DC201
 - MOVZX EDX, BYTE PTR DS:[5CAAC3A3]
 - MOV EBP, DWORD PTR DS:[5CAAC3E0]
 - ADD EDI, EDX
 - CMOV DWORD PTR SS:[EBP+18DA], OFA
 - MOV DWORD PTR SS:[ESP+20], EDI
 - JL Script.5C4DC2BE
 - ADD EBP, 18DB
 - MOV DWORD PTR SS:[ESP+10], OF9
 - PUSH 100
 - PUSH 0
- Registers (FPU):** Shows the EIP register at address 5C4DC201, pointing to the instruction "Script.5C4DC201".
- Memory Dump:** Shows a hex dump of memory starting at address 0B090DE0. The ASCII column contains Japanese text: "gvgvgVgVEBカツオブシムシの幼虫が兄のコートを食べているかもしれないからどうしようかなと思っ".

