

Dreamhack-Autoruns

1 LEVEL 1

Autoruns

forensics

335 147 2024.10.02. 09:22:25

문제 파일 받기

일단 C:\Users\victim\malware.exe

이 경로에 들어가면 malware가 실행되는 걸 알수있다.

The screenshot shows a forensic tool interface with a file list and a hex dump. The file list on the left shows the following files:

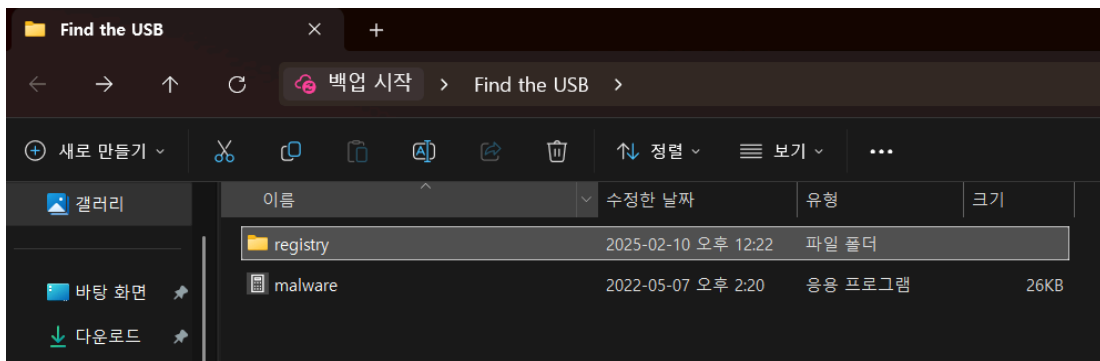
Name	Size	Type	Date Modified
Videos	256 (1 KB)	Directory	2024-04-04 오후 1...
시작 메뉴	268 (1 KB)	Reparse Po...	2024-01-17 오전 2...
\$I30	8,192 (8 KB)	NTFS Index...	2024-04-04 오후 1...
\$TXF_DATA	56 (1 KB)	NTFS Logg...	2024-04-04 오후 1...
malware.exe	26,624 (26 ...)	Regular File	2022-05-07 오전 5...
NTUSER.DAT	1,310,720 (...)	Regular File	2024-04-04 오후 1...
NTUSER.DAT.FileSlack	196,608 (19...	File Slack	
ntuser.dat.LOG1	253,952 (24...	Regular File	2024-01-17 오전 2...
ntuser.dat.LOG1.FileSlack	81,920 (80 ...)	File Slack	
ntuser.dat.LOG2	434,176 (42...	Regular File	2024-01-17 오전 2...

The hex dump on the right shows the following data:

```
0000 4D 5A 90 00 03 00 00 00-04 00 00 FF FF 00 00 MZ-----y~--
0010 B8 00 00 00 00 00 00 00-40 00 00 00 00 00 00 -----@-----
0020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 -----
0030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 -----
0040 0E 1F BA 0E 00 B4 09 CD-21 B9 01 4C CD 21 54 68 .....!.,.L!Th
0050 69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6F .....is program canno
0060 74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20 t be run in DOS
0070 6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 mode.....
0080 B4 30 DC 14 F0 51 B2 47-F0 51 B2 47 F0 51 B2 47 '00!G0!G0!G0!G
0090 F9 29 21 47 F6 51 B2 47-BB 29 B1 46 F1 51 B2 47 à) !G0!G0!G0!G
00a0 F0 51 B3 47 D7 51 B2 47-BB 29 B3 46 F9 51 B2 47 0!G0!G0!G0!G
00b0 BB 29 B6 46 E4 51 B2 47-BB 29 BA 46 F3 51 B2 47 ») $F0!G0!G0!G
00c0 BB 29 B7 46 F2 51 B2 47-BB 29 4D 47 F1 51 B2 47 ») :F0!G0!G0!G
00d0 BB 29 B0 46 F1 51 B2 47-52 69 63 68 F0 51 B2 47 ») *F0!G0!G0!G
00e0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 -----
00f0 50 45 00 00 4C 01 05 00-2E CA 53 0A 00 00 00 PE-.L....ES-----
0100 00 00 00 00 E0 00 02 01-0B 01 0E 1E 00 12 00 00 .....â-----
0110 00 54 00 00 00 00 00-E0 1C 00 00 00 10 00 00 .....T-----â-----
0120 00 30 00 00 00 00 00-40 00 00 10 00 00 02 00 00 .....@-----
0130 0A 00 00 00 0A 00 00 00-0A 00 00 00 00 00 00 -----
0140 00 B0 00 00 00 04 00 00-E6 D2 00 00 02 00 40 C1 .....@-----â-----
0150 00 00 04 00 00 20 00 00-00 00 10 00 00 10 00 00 -----
0160 00 00 00 10 00 00 00 00-00 00 00 00 00 00 00 -----
0170 A0 40 00 00 A0 00 00 00-00 50 00 08 47 00 00 @.....P...G..
```

ftk들어가서 malware에 들어가서 추출해준다

아까 그파일에 넣으면 쉽게 볼 수 있다



그럼 계산기 프로그램을 볼 수 있다

md5를 사용하기 때문에 우리가 다운받았던 hashcalc을 열어서 그 파일을 넣는다



MD5로 복호화 한 값인 302021d31f2d0bce01d7afc26bfe2ba2 가 플래그 이다.

FLAG: DH{302021d31f2d0bce01d7afc26bfe2ba2}