

Autoruns

- 문제

Description

[함께실습] **Autoruns**에서 실습하는 문제입니다.

드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 후에, 컴퓨터를 재부팅할 때마다 계산기 프로그램이 실행되고 있어요. 도대체 어떻게 된 일일까요?

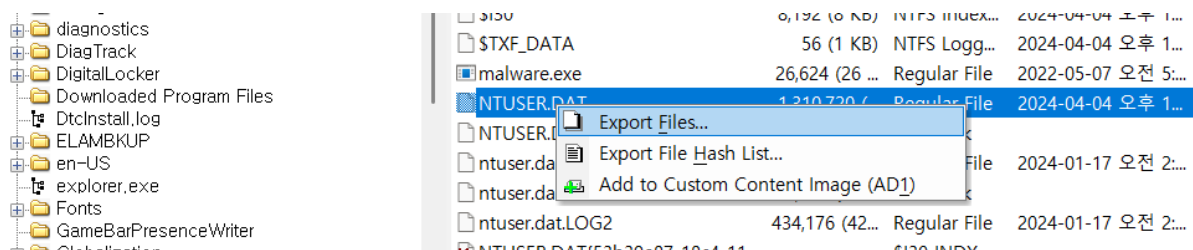
Windows 레지스트리를 분석해 플래그를 찾아보세요.

Info

FLAG = `DH{ MD5(File) }` FLAG는 자동 실행되고 있는 `exe` 파일을 MD5 해시로 계산한 값을 이용해 만듭니다. 예를 들어 대상 파일의 MD5 해시값이 `00112233445566778899AABBCCDDEEFF` 라면, 플래그는 `DH{00112233445566778899AABBCCDDEEFF}` 입니다.









- FLAG = `DH{ MD5(File) }`
- FLAG는 자동 실행되고 있는 `exe` 파일을 MD5 해시로 계산한 값을 이용해 만듭니다. 예를 들어 대상 파일의 MD5 해시값이 `00112233445566778899AABBCCDDEEFF` 라면, 플래그는 `DH{00112233445566778899AABBCCDDEEFF}` 입니다.

1. FTK Imager로 NTUSER.DAT Export file



2. **NTUSER.DAT** 추출 후 **Run** 경로에 설정된 path를 보면 `C:\Users\victim\malware.exe` 파일이 부팅될 때 실행

3. Autopsy로 malware.exe의 MD5확인

	malware.exe		0	2022-05-07 14:20:18 KST	2024-04-04 21:09:10 KST	2024-04-04 21:41:01 KST	2024-04-04 21:10:46 KST	26
	NTUSER.DAT		0	2024-04-04 21:39:18 KST	2024-01-17 11:06:28 KST	2024-04-04 21:39:18 KST	2024-01-17 11:06:28 KST	13
	ntuser.dat.LOG1		0	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	25
	ntuser.dat.LOG2		0	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	43
	NTUSER.DAT(53b39e88-18c4-11ea-a811-000d3aa		0	2024-01-17 11:07:27 KST	2024-01-17 11:07:27 KST	2024-01-17 11:07:27 KST	2024-01-17 11:06:28 KST	65
	NTUSER.DAT(53b39e88-18c4-11ea-a811-000d3aa		0	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	2024-04-04 21:39:18 KST	2024-01-17 11:06:28 KST	52
	NTUSER.DAT(53b39e88-18c4-11ea-a811-000d3aa		3	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	52
	ntuser.ini		1	2024-01-17 11:06:28 KST	2024-01-17 11:07:28 KST	2024-01-17 11:06:28 KST	2024-01-17 11:06:28 KST	20

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Metadata

Name:

/img_DiskImage.E01/Users/victim/malware.exe

Type:

File System

MIME Type:

application/x-msdownload

Size:

26624

File Name Allocation:

Allocated

Metadata Allocation:

Allocated

Modified:

2022-05-07 14:20:18 KST

Accessed:

2024-04-04 21:41:01 KST

Created:

2024-04-04 21:10:46 KST

Changed:

2024-04-04 21:09:10 KST

MD5:

302021d31f2d0bce01d7afc26bfe2ba2

1 LEVEL 1 Autoruns
문제를 해결했습니다.