

Dreamhack-Autoruns(level1)

문제

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.

풀이

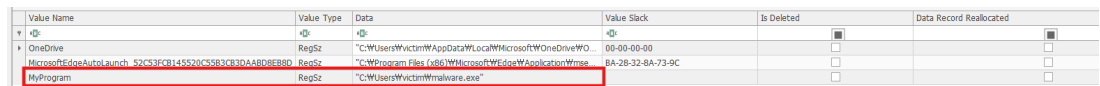
1. 문제 파악

자동 실행 설정된 .exe 파일의 이름 (또는 경로)을 레지스트리에서 찾아야 함

레지스트리 분석을 통해 해당 자동 실행 파일을 찾고 .exe 파일의 MD5 해시값 FLAG를 찾아야 함

2. 문제 풀이

분석한 파일 : `SOFTWARE` , `NTUSER.DAT`



분석 내용 : 해당 레지스트리 경로는 사용자가 로그인할 때 자동으로 실행되는 프로그램을 설정하는 영역,
"MyProgram"이라는 이름의 실행 파일이 등록되어 있음.



(2) 분석 내용 : "MyProgram" 이 파일인 줄 알고 추출하여 해시값 입력했지만 틀려서 .exe 파일을 다시 찾아보았다,,

| File List | | | |
|---------------------------|----------------|--------------|-----------------|
| Name | Size | Type | Date Modified |
| Pictures | 576 (1 KB) | Directory | 2024-01-17 오... |
| PrintHood | 296 (1 KB) | Reparse ... | 2024-01-17 오... |
| Recent | 252 (1 KB) | Reparse ... | 2024-01-17 오... |
| Saved Games | 152 (1 KB) | Directory | 2024-01-17 오... |
| Searches | 56 (1 KB) | Directory | 2024-01-17 오... |
| SendTo | 252 (1 KB) | Reparse ... | 2024-01-17 오... |
| Templates | 264 (1 KB) | Reparse ... | 2024-01-17 오... |
| Videos | 256 (1 KB) | Directory | 2024-04-04 오... |
| 시작 메뉴 | 268 (1 KB) | Reparse ... | 2024-01-17 오... |
| \$I30 | 8,192 (8 ... | NTFS Ind... | 2024-04-04 오... |
| \$TXF_DATA | 56 (1 KB) | NTFS Lo... | 2024-04-04 오... |
| malware.exe | 26,624 (2... | Regular F... | 2022-05-07 오... |
| NTUSER.DAT | 1,310,72... | Regular F... | 2024-04-04 오... |
| NTUSER.DAT.FileSlack | 196,608 (...) | File Slack | |
| ntuser.dat.LOG1 | 253,952 (...) | Regular F... | 2024-01-17 오... |
| ntuser.dat.LOG1.FileSlack | 81,920 (8 ...) | File Slack | |



(3) 경로 : C:\Users\victim\malware.exe

분석 내용 : malware.exe HashCalc 도구를 이용하여 해당 실행 파일의 MD5 해시값을 계산
[MD5: 302021d31f2d0bce01d7afc26bfe2ba2]

축하합니다!

1 LEVEL 1 Autoruns 문제를 해결했습니다.

대단해요. 문제를 어떻게 해결하셨나요?
풀이를 작성하면 포인트까지 받을 수 있어요.

괜찮아요

풀이 작성하기