103 – A suspicious developer

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description The auditing department of a software development company received an internal whistleblower report stating that a developer from the development team had outsourced a project to another company for execution. The auditing department initiated an investigation to determine whether there had been a violation of internal labor and security regulations. In response, that developer claimed to have personally developed the project and submitted the program source files and the resulting executable files to the audit team as evidence. The auditing department obtained the previous deliverables (executable files) that the developer had submitted by retrieving them from company's project management server. Verify the accuracy of the internal whistleblower's claims.

Target	Hash (SHA1)
Files.zip	26B11C75AD1F469B35284A29D973B716C030C71B

Questions

Please solve all problems based on UTC+9 time zone.

1) Write the items indicating the build tool version information stored in the given two PE format executable files in the format of "[ProductID].[BuildID].[Count]". (80 points)
   - Write 9 items per file and do so for both two files. (40 points each)
2) Write the build folder paths for the given two executable files. (20 points)
   - Write the build folder paths for both files. (10 points each)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

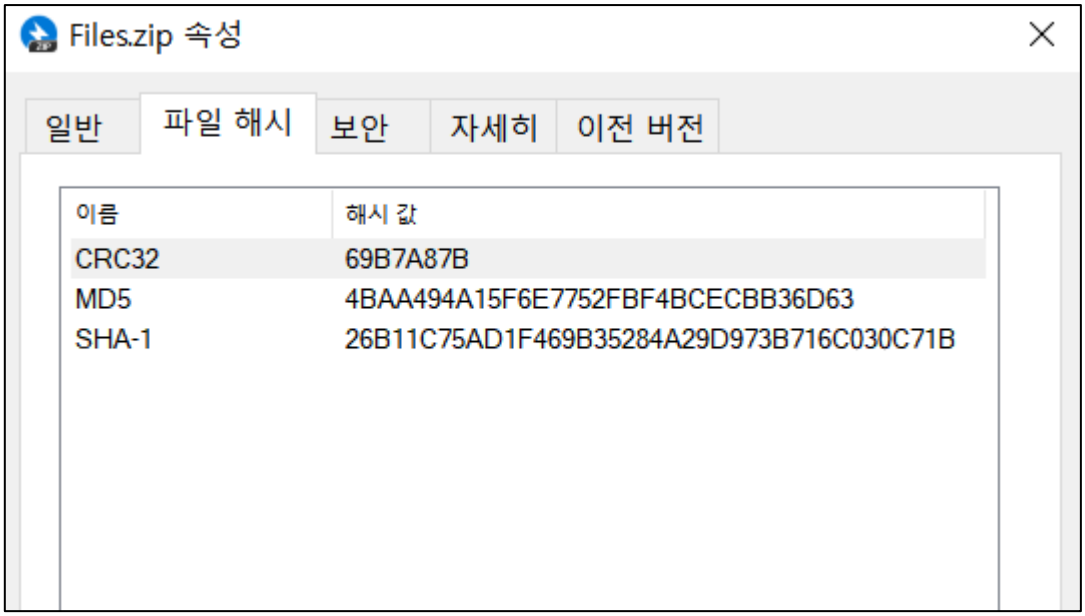
Tools used:

Name:	pestudio	Publisher:	Marc Ochsenmeier
Version:	9.53		
URL:	https://www.winitor.com/		

Name:	richprint	Publisher:	dishather
Version:	-		
URL:	https://github.com/dishather/richprint		

Name:	Hashtab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Step-by-step methodology:



[그림 1] 증거 파일의 해시 값 확인

분석을 수행하기 전 파일의 해시 값 산출을 통해 SHA1 해시 값이 일치함을 확인하였습니다.

1) Write the items indicating the build tool version information stored in the given two PE format executable files in the format of "[ProductID].[BuildID].[Count]". (80 points)

   - Write 9 items per file and do so for both two files. (40 points each)

문제에서 요구하는 두 개의 PE 파일에 저장된 ProductID, BuildID, Count에 관한 빌드 도구 버전 정보를 확인하기 위해서 PE 파일의 rich header를 살펴보았습니다. rich header 정보 확인에는 pestudio 도구를 사용하였습니다.

- **FromDeveloper.exe**

product-id (9)	build-id (3)	count
Utc1400_C	Visual Studio 2005 - 08.00	7
Implib800	Visual Studio 2005 - 08.00	23
Import	Visual Studio	505
Masm900	Visual Studio 2008 - 9.0	26
Utc1500_C	Visual Studio 2008 - 9.0	138
Utc1500_CPP	Visual Studio 2008 - 9.0	135
Utc1500_LTCG_CPP	Visual Studio 2008 - 9.0	3
Cvtres900	Visual Studio 2008 - 9.0	1
Linker900	Visual Studio 2008 - 9.0	1

[그림 2] FromDeveloper.exe의 rich-header(Visual Studio) 정보

- **FromBuildServer.exe**

product-id (9)	build-id (3)	count
Utc1310_C	Visual Studio 2003 - 7.10 SDK	7
Implib710	Visual Studio 2003 - 7.10 SDK	23
Import	Visual Studio	504
Masm800	Visual Studio 2005 - 08.00	25
Utc1400_C	Visual Studio 2005 - 08.00	136
Utc1400_CPP	Visual Studio 2005 - 08.00	133
Utc1400_LTCG_CPP	Visual Studio 2005 - 08.00	3
Cvtres800	Visual Studio 2005 - 08.00	1
Linker800	Visual Studio 2005 - 08.00	1

[그림 3] FromBuildServer.exe의 rich-header(Visual Studio) 정보

그리고 교차 검증을 위해 richprint 오픈소스 도구를 사용하여 빌드 버전 정보를 식별하였습니다.

```
sinsa@SINSA:~/richprint-master$ ./richprint FromDeveloper.exe
Processing FromDeveloper.exe
Target machine: x32
@comp.id   id version count   description
006dc627   6d  50727     7 [ C ] VS2005 build 50727
007bc627   7b  50727    23 [IMP] VS2005 build 50727
00010000    1      0   505 [---] Unmarked objects
0095521e   95  21022    26 [ASM] VS2008 build 21022
0083521e   83  21022   138 [ C ] VS2008 build 21022
0084521e   84  21022   135 [C++] VS2008 build 21022
008a521e   8a  21022     3
0094521e   94  21022     1 [RES] VS2008 build 21022
0091521e   91  21022     1 [LNK] VS2008 build 21022
sinsa@SINSA:~/richprint-master$ ./richprint FromBuildServer.exe
Processing FromBuildServer.exe
Target machine: x32
@comp.id   id version count   description
005f0fc3   5f   4035     7 [ C ] Windows Server 2003 SP1 DDK build 4035 (*)
005d0fc3   5d   4035    23 [IMP] Windows Server 2003 SP1 DDK build 4035 (*)
00010000    1      0   504 [---] Unmarked objects
007dc627   7d  50727    25 [ASM] VS2005 build 50727
006dc627   6d  50727   136 [ C ] VS2005 build 50727
006ec627   6e  50727   133 [C++] VS2005 build 50727
0072c627   72  50727     3
007cc627   7c  50727     1 [RES] VS2005 build 50727
0078c627   78  50727     1 [LNK] VS2005 build 50727
```

[그림 4] richprint 도구를 통해 확인한 pe 파일의 rich header 정보

이를 토대로 두 PE 파일의 빌드 버전 정보를 문제에서 요구하는 형식에 맞게 다음의 표와 같이 정리하였습니다.

[표 1] 두 PE 파일에 대한 빌드 도구 버전 정보 리스트

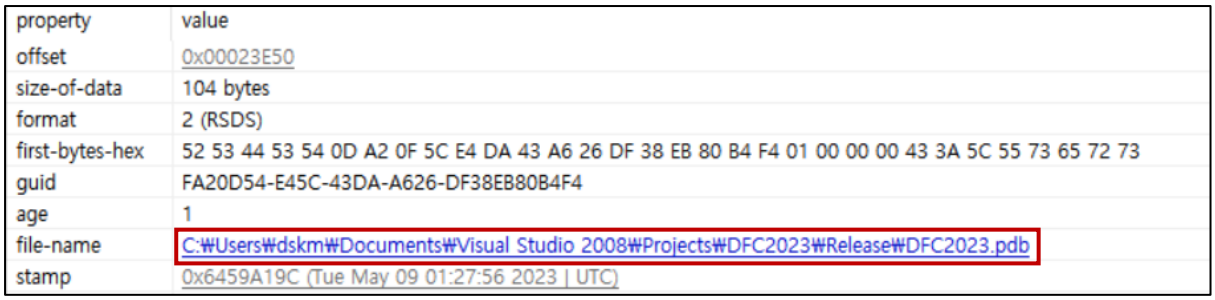
FromDeveloper.exe	FromBuildServer.exe
[Utc1400_C].[Visual Studio 2005 - 08.00].[7] [Implib800].[Visual Studio 2005 - 08.00].[23] [Import].[Visual Studio].[505] [Masm900].[Visual Studio 2008 - 9.0].[26] [Utc1500_C].[Visual Studio 2008 - 9.0].[138] [Utc1500_CPP].[Visual Studio 2008 - 9.0].[135] [Utc1500_LTCG_CPP].[Visual Studio 2008 – 9.0].[3] [Cvtres900].[Visual Studio 2008 - 9.0].[1] [Linker900].[Visual Studio 2008 - 9.0].[1]	[Utc1310_C].[Visual Studio 2003 - 7.10 SDK].[7] [Implib710].[Visual Studio 2003 - 7.10 SDK].[23] [Import].[Visual Studio].[504] [Masm800].[Visual Studio 2005 - 08.00].[25] [Utc1400_C].[Visual Studio 2005 - 08.00].[136] [Utc1400_CPP].[Visual Studio 2005 - 08.00].[133] [Utc1400_LTCG_CPP].[Visual Studio 2005 - 08.00].[3] [Cvtres800].[Visual Studio 2005 - 08.00].[1] [Linker800].[Visual Studio 2005 - 08.00].[1]

2) Write the build folder paths for the given two executable files. (20 points)

- Write the build folder paths for both files. (10 points each)

두 실행 파일의 build folder path는 Visual Studio를 통해 빌드한 exe 파일이 주로 함께 위치하고 있는 pdb 심볼 파일이 위치한 경로로 확인하였습니다. 주로 디버깅 정보가 PE 파일에 포함될 수 있는데, 이는 프로그램 내에 원본 소스 코드 경로 및 exe 파일 경로와 같은 경로 정보를 포함하는 경우가 있습니다. 따라서, 디버깅 정보를 저장하는 심볼인 pdb 파일의 경로 정보를 PE studio 도구에서 확인하였고, **두 PE 파일의 build folder path가 다르다는 것을 확인하였습니다**.

- **FromDeveloper.exe**



property	value
offset	0x00023E50
size-of-data	104 bytes
format	2 (RSDS)
first-bytes-hex	52 53 44 53 54 0D A2 0F 5C E4 DA 43 A6 26 DF 38 EB 80 B4 F4 01 00 00 00 43 3A 5C 55 73 65 72 73
guid	FA20D54-E45C-43DA-A626-DF38EB80B4F4
age	1
file-name	C:₩Users₩dskm₩Documents₩Visual Studio 2008₩Projects₩DFC2023₩Release₩DFC2023.pdb
stamp	0x6459A19C (Tue May 09 01:27:56 2023 | UTC)

[그림 5] FromDeveloper.exe의 build folder path

- **FromBuildServer.exe**

property	value
offset	0x00024B28
size-of-data	79 bytes
format	2 (RSDS)
first-bytes-hex	52 53 44 53 C6 CE 35 9E F6 D7 70 48 9A 86 68 9D 86 D6 DF 68 01 00 00 00 64 3A ...
guid	9E35CEC6-D7F6-4870-9A86-689D86D6DF68
age	1
file-name	d:₩BusinessDev₩DFC_Company₩DFC2023₩Release₩DFC2023.pdb
stamp	0x6466D0D3 (Fri May 19 01:28:51 2023 | UTC)

[그림 6] FromBuildServer.exe의 build folder path

이를 통해 두 PE 파일에서 발견된 build folder path 정보를 다음과 같이 표로 정리하였습니다.

[표 2] 각 실행 파일의 Build Folder Path

Executable File Name	Build folder path
FromDeveloper.exe	C:₩Users₩dskm₩Documents₩Visual Studio 2008₩Projects₩DFC2023₩Release₩DFC2023.pdb
FromBuildServer.exe	d:₩BusinessDev₩DFC_Company₩DFC2023₩Release₩DFC2023.pdb