

103 – A suspicious developer

Team Information

Team Name: kimbabasaksaksak

Team Member: Jaeheon Kim, Donghyun Kim, Soyoung Yoo, Minhee Lee

Email Address : uaaoong@gmail.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:	HxD	Publisher:	mh-nexus
Version:	2.5.0.0		
URL:	https://mh-nexus.de/en/		

Name:	PE-bear	Publisher:	hasherezade
Version:	0.6.5.2		
URL:	https://github.com/hasherezade/pe-bear		

Step-by-step methodology:

Q1. 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)

문제에서 주어진 2개의 실행 파일에 저장된 빌드 도구 버전 정보는 각 파일의 Rich Header 정보를 통해 파악할 수 있다. Rich Header는 프로그램을 빌드한 컴파일러에 대한 정보 및 실행파일이 생성된 환경에 대한 정보가 저장된 영역이다. HxD 도구로 PE 구조를 살펴보면, 0x80 Offset부터 Rich Header 구조를 확인할 수 있는데, "Rich" 구분자 바로 뒤 4바이트 hex 값으로 XOR 인코딩되어 존재한다. XOR Key로 디코딩 시 초기 "DanS" 문자열 시그니처를 확인할 수 있으며 제로 패딩 값 이후 컴파일러 정보가 기록되어 있다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....YY..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E8	00	00	00ë.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..*..!..Li!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode.....\$.....
00000080	2C	17	16	3B	68	76	78	68	68	76	78	68	68	76	78	68	...;hvkhvhvkhvkh
00000090	AB	79	27	6B	6F	76	78	68	AB	79	25	6B	7F	76	78	68	ey'hovkhvkh.vxkh
000000A0	68	76	79	68	90	77	78	68	4F	B0	05	68	71	76	78	68	hvyh.wxkhO".hqvkh
000000B0	4F	B0	15	68	E0	76	78	68	4F	B0	16	68	ED	76	78	68	O".hävkhO".hivkh
000000C0	4F	B0	0A	68	6B	76	78	68	4F	B0	04	68	69	76	78	68	O".hkvxhO".hivkh
000000D0	4F	B0	00	68	69	76	78	68	52	69	63	68	68	76	78	68	O".hivkhRichvkh
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00PE..L...
000000F0	D3	D0	66	64	00	00	00	00	00	00	00	00	00	00	00	00	Obfd.....ä...
00000100	0B	01	08	00	00	00	00	00	00	00	00	00	00	00	00	00

0x68767868로 XOR한 값

FromBuildServer.exe

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....YY..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00ë.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..*..!..Li!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode.....\$.....
00000080	72	5C	AA	F3	36	3D	C4	A0	36	3D	C4	A0	36	3D	C4	A0	r*06=A 6=A 6=A
00000090	11	FB	A9	A0	31	3D	C4	A0	11	FB	BF	A0	21	3D	C4	A0	.ü@ 1=Ä .ü¿ 1=Ä
000000A0	36	3D	C5	A0	CF	3C	C4	A0	28	6F	51	A0	2C	3D	C4	A0	6=Ä I<Ä (oQ ,=Ä
000000B0	28	6F	47	A0	BC	3D	C4	A0	28	6F	40	A0	B1	3D	C4	A0	(oG 4=Ä (o@ ±=Ä
000000C0	28	6F	4E	A0	35	3D	C4	A0	28	6F	50	A0	37	3D	C4	A0	(oN 5=Ä (oP 7=Ä
000000D0	28	6F	55	A0	37	3D	C4	A0	52	69	63	68	36	3D	C4	A0	(oU 7=Ä Rich6=A
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	50	45	00	00	4C	00	00	00	00	00	00	00	00	00	00	00	FE...L...;Yd...
00000100	00	00	00	00	E0	00	00	00	00	00	00	00	00	00	00	00	...ä...ü...

0x363DC4A0로 XOR한 값

FromDeveloper.exe

Rich Header 분석 기능을 제공하는 PE-Bear 도구를 사용하여 각 파일의 ProductID, BuildID, Count 값을 확인할 수 있었다.

Disasm	General	DOS Hdr	Rich Hdr	File Hdr	Optional Hdr	Section Hdrs	Imports	Resources	Debug	LoadConfig
Offset	Name	Value	Unmasked Value	Meaning	Productid	Buildid	Count	VS version		
80	DanS ID	3b16172c	536e6144	DanS						
84	Checksumed padding	68787668	0	0						
88	Checksumed padding	68787668	0	0						
8C	Checksumed padding	68787668	0	0						
90	Comp ID	6878766f682779ab	7005f0fc3	4035.95.7	Utc1310_C	4035	7	Visual Studio 2003 07.10		
98	Comp ID	6878767f682579ab	17005d0fc3	4035.93.23	Implib710	4035	23	Visual Studio 2003 07.10		
A0	Comp ID	6878779068797668	1f800010000	0.1.504	Import0	0	504	Visual Studio		
A8	Comp ID	687876716805b04f	19007dc627	50727.125.25	Masm800	50727	25	Visual Studio 2005 08.00		
B0	Comp ID	687876e06815b04f	88006dc627	50727.109.136	Utc1400_C	50727	136	Visual Studio 2005 08.00		
B8	Comp ID	687876ed6816b04f	85006ec627	50727.110.133	Utc1400_CPP	50727	133	Visual Studio 2005 08.00		
C0	Comp ID	6878766b680ab04f	30072c627	50727.114.3	Utc1400_LTCG_CPP	50727	3	Visual Studio 2005 08.00		
C8	Comp ID	687876696804b04f	1007cc627	50727.124.1	Cvtres800	50727	1	Visual Studio 2005 08.00		
D0	Comp ID	687876696800b04f	10078c627	50727.120.1	Linker800	50727	1	Visual Studio 2005 08.00		
D8	Rich ID	68636952		Rich						
DC	Checksum	68787668	68787668							

FromBuildServer.exe

Disasm	General	DOS Hdr	Rich Hdr	File Hdr	Optional Hdr	Section Hdrs	Imports	Resources	BaseReloc.	Debug
Offset	Name	Value	Unmasked Value	Meaning	Productid	Buildid	Count	VS version		
80	DanS ID	f3aa5c72	536e6144	DanS						
84	Checksumed padding	a0c43d36	0	0						
88	Checksumed padding	a0c43d36	0	0						
8C	Checksumed padding	a0c43d36	0	0						
90	Comp ID	a0c43d31a0a9fb11	7006dc627	50727.109.7	Utc1400_C	50727	7	Visual Studio 2005 08.00		
98	Comp ID	a0c43d21a0bffb11	17007bc627	50727.123.23	Implib800	50727	23	Visual Studio 2005 08.00		
A0	Comp ID	a0c43ccfa0c53d36	1f900010000	0.1.505	Import0	0	505	Visual Studio		
A8	Comp ID	a0c43d2ca0516f28	1a0095521e	21022.149.26	Masm900	21022	26	Visual Studio 2008 09.00		
B0	Comp ID	a0c43dbca0476f28	8a0083521e	21022.131.138	Utc1500_C	21022	138	Visual Studio 2008 09.00		
B8	Comp ID	a0c43db1a0406f28	870084521e	21022.132.135	Utc1500_CPP	21022	135	Visual Studio 2008 09.00		
C0	Comp ID	a0c43d35a04e6f28	3008a521e	21022.138.3	Utc1500_LTCG_CPP	21022	3	Visual Studio 2008 09.00		
C8	Comp ID	a0c43d37a0506f28	10094521e	21022.148.1	Cvtres900	21022	1	Visual Studio 2008 09.00		
D0	Comp ID	a0c43d37a0556f28	10091521e	21022.145.1	Linker900	21022	1	Visual Studio 2008 09.00		
D8	Rich ID	68636952		Rich						
DC	Checksum	a0c43d36	a0c43d36							

FromDeveloper.exe

리치헤더 구조에 따라 확인한 "[ProductID].[BuildID].[Count]"는 아래와 같다. ProductID에 매칭되는 Int 값은 아래 Github 정보를 참고하였다.

- <https://github.com/kirschju/richheader/blob/master/prodids.py>

	FromBuildServer.exe	FromDeveloper.exe
1	[95(Utc1310_C)].[4035].[7]	[109(Utc1400_C)].[50727].[7]
2	[93(Implib710)].[4035].[23]	[123(Implib800)].[50727].[23]
3	[1(Import0)].[0].[504]	[1(Import0)].[0].[505]
4	[125(Masm800)].[50727].[25]	[149(Masm900)].[21022].[26]

5	[109(Utc1400_C)].[50727].[136]	[131(Utc1500_C)].[21022].[138]
6	[110(Utc1400_CPP)].[50727].[133]	[132(Utc1500_CPP)].[21022].[135]
7	[114(Utc1400_LTCG_CPP)].[50727].[3]	[138(Utc1500_LTCG_CPP)].[21022].[3]
8	[124(Cvtres800)].[50727].[1]	[148(Cvtres900)].[21022].[1]
9	[120(Linker800)].[50727].[1]	[145(Linker900)].[21022].[1]

Q2. Write the build folder paths for the given two executable files. (20 points)

Build folder path는 PDB Path를 통해 알 수 있다. PDB 파일은 PE 파일에 대한 디버깅 관련 정보를 담고 있으며, PE 파일의 디버그 섹션에 존재하는 타입 중 CODEVIEW 타입 정보에서 해당 PE와 연결된 PDB 파일의 이름과 경로를 획득할 수 있다. 아래는 PE-Bear 도구를 사용하여 각 실행파일의 빌드 폴더를 확인한 내용이다.

2-1) FromBuildServer.exe

프로젝트 폴더는 d:\BusinessDev\DFC_Company이고, 실행 파일 및 pdb 파일이 위치한 경로는 d:\BusinessDev\DFC_Company\DFC2023\Release이다. 그리고 pdb 파일의 경로는 d:\BusinessDev\DFC_Company\DFC2023\Release\DFC2023.pdb 이다.

Visual C++ (CodeView) [1 entry]		
Offset	Name	Value
24B28	CvSig	RSDS
24B2C	Signature	{9E35CEC6-D7F6-4870-9A86-689D86D6DF68}
24B3C	Age	1
24B40	PDB	d:\BusinessDev\DFC_Company\DFC2023\Release\DFC2023.pdb

2-2) FromDeveloper.exe

프로젝트 폴더는 C:\Users\wskm\Documents\Visual Studio 2008\Projects\DFC2023이고, 실행 파일 및 pdb 파일이 위치한 경로는 C:\Users\wskm\Documents\Visual Studio 2008\Projects\DFC2023\Release이다. 그리고 pdb 파일의 경로는 C:\Users\wskm\Documents\Visual Studio 2008\Projects\DFC2023\Release\DFC2023.pdb 이다.

Visual C++ (CodeView) [1 entry]		
Offset	Name	Value
23E50	CvSig	RSDS
23E54	Signature	{0FA20D54-E45C-43DA-A626-DF38EB80B4F4}
23E64	Age	1
23E68	PDB	C:\Users\wskm\Documents\Visual Studio 2008\Projects\DFC2023\Release\DFC2023.pdb