

APT Attacks on Domestic Companies Using Library Files

ASEC asec.ahnlab.com/en/23717/

By jcleebobgatenet

June 4, 2021



Recently, there have been continuous attacks targeting domestic companies. Most of the malicious files collected from the companies' breached systems have been dynamic library (DLL) files, but the files used in the attacks this time are different from general DLL files. The collected files had their normal libraries modified maliciously through a variety of methods.

It has not been found how the malicious files were created in the system and what the initial attack path was. Also, due to the nature of libraries which cannot be run on their own, they require trigger behaviors that run libraries, but this and the additional file information have not been confirmed. Still, the analysis of the files collected so far revealed clear characteristics of the recent attacks.

- Malicious files that modified (added, replaced, or changed) the export information of normal library (DLL) files
- The attacker requires valid arguments or data files to run malicious files
- The attacker can modularize or replace features through arguments or data files

Characteristics of Attacks that Use Library Files

The attacker created malicious files by newly adding export functions to normal library files, exchanging function formats, or changing codes of the existing functions. As most of the codes are normal, users are highly likely to judge files as being normal unless they inspect

them carefully.

A valid argument or data file is needed to run the malicious files, which means there is limit to fully analyze the attack with just individual files. Even the automated analysis device was unable to produce meaningful execution results.

Attackers fragmented (modularized) features using arguments or data files, and depending on the input information, the codes run on memory or C&C address might change. If the system is dominated, the attacker can continuously change features in real-time.

Malicious File Types by Library Modification and Operation Method

The malicious library files collected from the companies' breached systems can be categorized into four types based on modifications and operation methods. [Table 1] lists the normal library filenames assumed to be modified by the attacker, filenames of malicious library files at the time of collection, and DLL names stated in 'Export Directory' on the PE file format by type. Looking at the file features alone, the types do not seem to be directly related.

The collected malicious library files are modified forms of the original normal library files, but filenames are different. If filenames were the same, the attacker would have run the malware with the DLL Hijacking method of replacing library files. But because the additional information including the initial path of the attack is not yet ascertained, it is unknown whether the filenames were changed or the original library files were simply modified and disguised. In other words, it has not been confirmed how the malicious library files were run.

The collected malicious library filenames are different from the DLL names stated on the 'Export Directory' struct. Yet as DLL names of the 'Export Directory' struct do not affect the library when it is loaded, they do not have much significance. Still, one can expect that the attacker might have changed filenames when modifying the original library files.

Type	Normal DLL Filename	Malicious DLL Filename	Export DLL name of Malicious DLL File
A	libGLESv2.dll	–	libGLESv2.dll
B-1	libxml2.dll	pchsvc.dll	libxml2.dll
B-2	Unknown	srsvc.dll	audiosrv.dll
C	NppExport.dll	wmicr.dll	svcloder.dll
D	dokan1.dll	–	dokan1.dll
D	dokan1.dll	uso.dat	dokan1.dll

D dokan1.dll zlib1.cab dokan1.dll

Categorization of malicious file types used in attacks

[Type A] Adds malicious export function. Needs argument

The malicious export function `gllnitTexture` was added to the normal `libGLESv2` library file. Because a function was added, there is one more export function in the 'Export Directory' struct than the normal one. When the `gllnitTexture` function is run, it checks the run argument condition of 32 characters. It processes internally using the argument and runs the malicious PE in memory. As valid argument information was not found, the team could not identify the features of the executed PE.

Offset	Name	Value	Meaning
3A8AE0	Characteristics	0	
3A8AE4	TimeDateStamp	5F977048	화요일, 27.10.2020 00:56:40 UTC
3A8AE8	MajorVersion	0	
3A8AEA	MinorVersion	0	
3A8AEC	Name	3AB456	libGLESv2.dll
3A8AF0	Base	1	
3A8AF4	NumberOfFunctions	2BB	
3A8AF8	NumberOfNames	2BB	
3A8AFC	AddressOfFunctions	3A9908	
3A8B00	AddressOfNames	3AA3F4	
3A8B04	AddressOfNameOrdinals	3AAEE0	

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
3A95C0	2AF	1D860	3AE205	?UnmapBufferOES@gl@@YAEI@Z	
3A95C4	2B0	23690	3AE220	?UseProgramStages@gl@@YAXIII@Z	
3A95C8	2B1	23690	3AE23F	?ValidateProgramPipeline@gl@@YAXI@Z	
3A95CC	2B2	23810	3AE263	?VertexAttribBinding@gl@@YAXII@Z	
3A95D0	2B3	1D8C0	3AE284	?VertexAttribDivisorANGLE@gl@@YAXII@Z	
3A95D4	2B4	23870	3AE2AA	?VertexAttribFormat@gl@@YAXIHIEI@Z	
3A95D8	2B5	23900	3AE2CD	?VertexAttribFormat@gl@@YAXIHII@Z	
3A95DC	2B6	23990	3AE2F0	?VertexBindingDivisor@gl@@YAXII@Z	
3A95E0	2B7	DDF0	3AE312	?WaitClient@egl@@YAIXZ	
3A95E4	2B8	DDF0	3AE329	?WaitGL@egl@@YAIXZ	
3A95E8	2B9	DF50	3AE33C	?WaitNative@egl@@YAIH@Z	
3A95EC	2BA	E200	3AE354	?WaitSync@egl@@YAIPEAXOH@Z	
3A95F0	2BB	26980	3AF467	gllnitTexture	

Export function of the Type A malicious file

[Type B-1] Replaces normal function with malicious `ServiceMain` function. Needs ADS data

The `DllMain` function, the first export function of the normal `libxml2` library file, was replaced with the malicious `ServiceMain` function. There is no change in the number of export functions. Being a `ServiceMain` function, it operates as a Windows service. When it is run, the malicious file reads the ADS (Alternate Data Streams) data. Using ADS, it hides the malicious data needed for the execution from the user. Zone and data stream are key data

needed to decrypt encrypted data and passwords respectively. After processing internally, the file runs the malicious PE in memory. The executed malicious PE requires the rsrc stream data. Its final feature is the connection to C&C.

Offset	Name	Value	Meaning
15F9F0	Characteristics	0	
15F9F4	TimeDateStamp	5F922F6A	금요일, 23.10.2020 01:18:34 UTC
15F9F8	MajorVersion	0	
15F9FA	MinorVersion	0	
15F9FC	Name	1654C8	libxml2.dll
15FA00	Base	1	
15FA04	NumberOfFunctions	678	
15FA08	NumberOfNames	678	
15FA0C	AddressOfFunctions	161418	
15FA10	AddressOfNames	162DF8	
15FA14	AddressOfNameOrdinals	1647D8	

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
15FA18	1	F8B30	1654D4	ServiceMain	
15FA1C	2	20620	1654E0	UTF8TOHtml	
15FA20	3	15E00	1654EB	UTF8Toisolat1	
15FA24	4	1C8C0	1654F9	__docbDefaultS...	
15FA28	5	1C900	165511	__htmlDefaultS...	
15FA2C	6	1C980	165529	__oldXMLWDco...	
15FA30	7	1C9C0	165541	__xmlBufferAllo...	
15FA34	8	1CA60	165558	__xmlDefaultBu...	
15FA38	9	1CB00	16556F	__xmlDefaultSA...	
15FA3C	A	1CB40	165586	__xmlDefaultSA...	

Export function of Type B-1 malicious file

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 31 59 6A 49 7A 71 73 78 6A 69 62 31 5A 53 6C 31 1YjIzqsxjiblZS1l
00000010 64 48 4E 51 62 67 44 66 64 67 42 57 64 6D 76 42 dHNQbgDfdgBWdmvB|

```

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 26 FB C5 FA 79 98 8D 0F B4 15 09 9D ED 26 E9 48 &UÁúy~...í&éH
00000010 B0 A9 9F 40 B7 BD 08 7E D5 DE 1E CC 3F 11 39 73 °@Y@~%~.ÖP.Î?.9s
00000020 0A 53 B1 BE 2D 72 E3 3F 30 3C FD 3F 82 EF 99 60 .S±%~rã?0<ý?,i™`
00000030 BD 01 1B FA 38 04 7E 27 C5 74 D5 A9 5E B1 29 B1 %..ú8.~'ÁtÖ@^±)±
00000040 3A 93 7F B1 97 2E A6 EF 4F D6 59 51 9E 9D F5 94 :".±~.¡iOÖYQž.õ"
00000050 DC 5B 38 FA BC 54 62 AB 83 BA B2 85 6B 7E 00 07 Ü[8ú4Tb«f°°...k~..
00000060 BC E5 7A 75 7F 1C DA DD 12 B7 2B 2B 09 55 EA F7 4ãzu..ÚÝ.~++.Uê÷
00000070 B6 C0 0E C6 B6 A2 D3 FC D8 18 5D 4B D8 81 14 F3 qÀ.Æqçóúø. ]Kø..ó
00000080 7A 72 9B 94 56 03 5E 25 35 A4 B9 99 FF 80 6B 27 zr>"V.^%5m²™yEk'
00000090 A7 EA 9B 7A 46 59 17 59 B2 F3 C3 39 AE 26 D3 51 $ê>zrFY.Y²óÄ9ø&óQ
000000A0 77 FA BA 62 7E 94 68 57 AC 72 2F 6A 0D F5 74 BF wú°b~"hW~r/j.ötç
000000B0 C6 B2 DE 15 B3 75 47 08 DC 65 DB 6D D3 68 BE 1E È²P.²uG.ÜeÜmÓh%.
000000C0 4A 8F E7 CC 23 D5 61 FC 35 84 6E 40 A9 F6 3E 90 J.çİ#Öâu5,,n@ø>.
000000D0 04 54 7C 07 9D CA EB 43 E6 A9 0B 28 7E EA A8 E3 .T|..ÈèCæ@.(~è"ã
000000E0 43 33 5E 81 4B 43 8F 93 1B 81 40 21 AC 17 D2 4F C3^..KC."..@!~.òO
000000F0 2F 99 58 79 55 FB 6F AB DB DC 1F 6C B9 5F 10 5A /™XyUúo«ÜÜ.1²_2

```

'data' ADS data and 'zone' ADS data

[Type B-2] Only malicious ServiceMain function exists. Needs ADS data

It is uncertain whether the normal library files exist at all. This file only has the Windows service ServiceMain function as the export function. Unlike other types, there is no file resource version information. Also, considering it does not have any export functions except the malicious ServiceMain function, the type may be a malicious library file that was solely created. There are some differences between codes, but the malicious file of this type has a feature similar to that of type B-1 malicious file and needs the ADS data named zone and data. As the stream data was not collected, the team could not know further features.

Offset	Name	Value	Meaning
230E70	Characteristics	0	
230E74	TimeStamp	5FA8F550	월요일, 09.11.2020 07:52:48 UTC
230E78	MajorVersion	0	
230E7A	MinorVersion	0	
230E7C	Name	231EA2	audiosrv.dll
230E80	Base	1	
230E84	NumberOfFunctions	1	
230E88	NumberOfNames	1	
230E8C	AddressOfFunctions	231E98	
230E90	AddressOfNames	231E9C	
230E94	AddressOfNameOrdinals	231EA0	

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
230E98	1	151790	231EAF	ServiceMain	

Export function of Type B-2 malicious file

000007FE ECB2143A	C74424 20 03000000	mov dword ptr ss:[rsp+20],3	[rsp+20]:L":zone"
000007FE ECB21442	BA 00000080	mov edx,80000000	
000007FE ECB21447	FF15 03D40E00	call qword ptr ds:[<&CreateFileW>]	
000007FE ECB2144D	48:8BF8	mov rdi, rax	
000007FE ECB21450	48:83F8 FF	cmp rax,FFFFFFFFFFFFFFFF	
000007FE ECB21454	0F84 DC010000	je a.7FE ECB21636	
000007FE ECB2145A	48:89B424 50080000	mov qword ptr ss:[rsp+850],rsi	
000007FE ECB21462	33D2	xor edx,edx	
000007FE ECB21464	4C:89B424 58080000	mov qword ptr ss:[rsp+858],r14	
000007FE ECB2146C	48:8BC8	mov rcx, rax	
000007FE ECB2146F	4C:89BC24 10080000	mov qword ptr ss:[rsp+810],r15	[rsp+810]: "MZ"
000007FE ECB21477	FF15 03D40E00	call qword ptr ds:[<&GetFileSize>]	
000007FE ECB2147D	8BD0	mov edx, eax	
000007FE ECB2147F	41:8D4D 40	lea ecx, qword ptr ds:[r13+40]	
000007FE ECB21483	44:8BF8	mov r15d, eax	
000007FE ECB21486	FF15 4CD40E00	call qword ptr ds:[<&LocalAlloc>]	
000007FE ECB2148C	4C:8D4C24 40	lea r9, qword ptr ss:[rsp+40]	
000007FE ECB21491	4C:896C24 20	mov qword ptr ss:[rsp+20],r13	[rsp+20]:L":zone"

Approaching ADS data

[Type C] Adds malicious functions besides ServiceMain. Needs data file

The malicious file of this type modified the NppExport library of the Notepad++ plugin. Four export functions not presented in the normal library were added. Besides ServiceMain and ServiceHandler to operate as a Windows Service, there are two other functions: AttachMove and DetachMove. The features of AttachMove and DetachMove functions are normal in

terms of features, and the codes in the DIIMain function in the normal library were moved. The malicious file calculates internally using the wmicc.dat data file existing in the fixed directory and runs the malicious PE in memory. The malicious PE that is run needs the wmicd.dat data file. Its final feature is to connect to C&C.

Offset	Name	Value	Meaning
16500	Characteristics	0	
16504	TimeDateStamp	4F697423	수요일, 21.03.2012 06:24:35 UTC
16508	MajorVersion	0	
1650A	MinorVersion	0	
1650C	Name	1718C	svcloader.dll
16510	Base	1	
16514	NumberOfFunc...	A	
16518	NumberOfNames	A	
1651C	AddressOfFunc...	17128	
16520	AddressOfNames	17150	
16524	AddressOfNam...	17178	

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
16528	1	4910	1719A	AttachMove	
1652C	2	4880	171A5	DetachMove	
16530	3	4780	171B0	ServiceHandler	
16534	4	4810	171BF	ServiceMain	
16538	5	4D60	171CB	benotified	
1653C	6	4D50	171D6	getFuncsArray	
16540	7	4D40	171E4	getName	
16544	8	4D70	171EC	isUnicode	
16548	9	4D70	171F6	messageProc	
1654C	A	4C50	17202	setinfo	

Export function of Type C malicious file

[Type D] Changes the existing function's codes. Needs arguments. Creates and loads data file

The normal Dokan library was modified. This is the most unique type of modification. No export functions were added or changed. Only the binary code within the function was changed. Like previous types, it is not easy to confirm whether the library was modified or not with just the 'Export Directory' struct information. Also, because the file changed the entire code pattern by packing the previous VC++ file with Vmprotect, it is difficult to check its features and whether the code was changed. The changed code can be checked by unpacking Vmprotect and comparing by export function. DokanNotifyXAttrUpdate is the function that had its code changed.

When calling the malicious export function, it operates only when the valid argument starting with '-s' is sent. When the argument is given, the type can create the VirtualStore.cab data file in the system %Temp% directory. If the argument fits the specific condition, it loads the data file. The Data file includes code running for C&C communication and the URL information. Multiple VirtualStore.cab data files were found in the breached systems. It appears that the attacker changed the C&C server in real-time.

```

; Exported entry 13. DokanNotifyXAttrUpdate

; Attributes: bp-based frame

; int __stdcall DokanNotifyXAttrUpdate(char ArgList)
public DokanNotifyXAttrUpdate
DokanNotifyXAttrUpdate proc near

ArgList= byte ptr 8

push    ebp
mov     ebp, esp
mov     ecx, dword ptr [ebp+ArgList] ; ArgList
mov     edx, 4
push    3 ; int
call   sub_100066E0
pop     ebp
retn   4
DokanNotifyXAttrUpdate endp

```

```

; Exported entry 13. DokanNotifyXAttrUpdate

; Attributes: bp-based frame fuzzy-sp

; int __usercall DokanNotifyXAttrUpdate@<eax>(int<ecx>, int<edi>, int<esi>)
public DokanNotifyXAttrUpdate
DokanNotifyXAttrUpdate proc near
push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF8h
sub     esp, 54h
push    ebx
push    esi
push    edi
call   sub_6D27AC47

```

```

locret_6D108591:
retn
DokanNotifyXAttrUpdate endp

```

Function code patch of Type D Malicious file

```

00000000 F0 31 3B 06 9C BA 43 08 05 BE 83 15 38 FB 4F 22  01;.œ°C..%f.8ûO"
00000010 6F 6E 15 65 83 32 12 28 46 24 56 BC E3 3A BF B3  on.ef2.(FQV4ã:¿³
00000020 67 89 3C D8 78 EB 31 E0 72 31 82 7F BA 3B 0D 39  gñ<0xëIàr1,.°;.9
00000030 6D D6 7E A8 1E 53 4A 60 28 CF 25 53 E1 95 C3 03  mÔ~".SJ`(`I&SÁ·Ã.
00000040 9D D6 D1 94 F1 5C 6E 5F AB A3 20 83 2A 9E 7D 36  .ÖÑ"ñ\n_«£ f*ž}6
00000050 B4 D9 29 4F 3E 63 94 5E B8 46 72 4A 3F B5 B9 F1  `Û)O>c"^^_FrJ?µ²ñ
00000060 8E EB BD BB 50 94 2A 7F E6 BC 56 EF CB A8 31 BC  Žë»»P"*.æ4ViË"14
00000070 EA 65 84 99 BD F0 3D 8B 72 32 B4 E8 D1 F7 EB 36  êe,,²»sð=<r2`èÑ÷è6
00000080 55 73 64 A2 A8 06 C4 05 42 72 D2 02 83 87 8A 7C  Usdc".Ä.BrÒ.f+S|
00000090 12 6F E2 FE F0 60 F3 71 48 11 08 04 41 39 21 4F  .oâpð`òqH...A9!O
000000A0 C2 45 0E 45 1A C8 88 8A 6D 1A F1 DC BD 9A 82 52  ÆE.E.È^Šm.ñÛ÷sš,R
000000B0 A8 50 78 2D 06 38 8A 95 DE 0E 4C EC BF 6B B0 9A  `Px-.8Š•P.Liçk°š
000000C0 10 25 D5 02 41 59 C3 FF 60 8B 71 6E 34 71 86 0E  .%Ö.AYÄÿ`<qñ4qt.
000000D0 5F 01 3D 83 9C 90 B1 C3 2E C2 B9 66 03 98 BB CA  _.=fœ.±Ä.Ä³f.~»Ê
000000E0 37 71 32 80 F1 07 84 58 C1 1D F3 3F BE 62 48 49  7q2ëñ..„XÄ.ó?²bHI
000000F0 A5 52 49 D3 12 EB 9C C8 0E 03 5D 45 8B 03 3A 99  ¥RIÓ.ëœÈ...]Eç.:™

```

VirtualStore.cab data file

6C233121	68 00000080	push 80000000	
6C233126	8985 F0F7FFFF	mov dword ptr ss:[ebp-810],eax	[ebp-810]:&"ð)#l@+#lp*#l°+#l
6C23312C	FF70 04	push dword ptr ds:[eax+4]	[eax+4]:"C:\\Users\\MONGCH~1
6C23312F	56	push esi	
6C233130	E8 79F01700	call sample.6C3B21AE	
6C233135	8BF8	mov edi,eax	edi:&"ð)#l@+#lp*#l°+#lÀ,#lD,;
6C233137	83FF FF	cmp edi,FFFFFFFF	edi:&"ð)#l@+#lp*#l°+#lÀ,#lD,;
6C23313A	74 1C	je sample.6C233158	
6C23313C	6A 00	push 0	
6C23313E	57	push edi	edi:&"ð)#l@+#lp*#l°+#lÀ,#lD,;
6C23313F	50	push eax	eax:&"ð)#l@+#lp*#l°+#lÀ,#lD,;
6C233140	E8 72B61600	call sample.6C39E7B7	
6C233145	8BF0	mov esi,eax	eax:&"ð)#l@+#lp*#l°+#lÀ,#lD,;
6C233147	89B5 ECF7FFFF	mov dword ptr ss:[ebp-814],esi	
6C23314D	85F6	test esi,esi	
6C23314F	75 19	jne sample.6C23316A	

+4]=[0043267C &"C:\\Users\\ \\AppData\\Local\\Temp\\.. \\VirtualStore.cab" =00433FB0 "C:\\Users\\

Approaching the data file in the DokanNotifyXAttrUpdate function

76B29197	8BFF	mov edi,edi	InternetOpenW
76B29199	55	push ebp	
76B2919A	8BEC	mov ebp,esp	
76B2919C	83EC 2C	sub esp,2C	
76B2919F	53	push ebx	
76B291A0	56	push esi	esi:&" ?#1I"
76B291A1	33DB	xor ebx,ebx	
76B291A3	33C0	xor eax,eax	
76B291A5	8D4D D4	lea ecx,dword ptr ss:[ebp-2C]	
76B291A8	40	inc eax	
76B291A9	51	push ecx	
76B291AA	50	push eax	
76B291AB	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]:L"http://pasc.co.kr/family/data/smartlist.asp"
76B291AE	895D F8	mov dword ptr ss:[ebp-8],ebx	

Connection to C&C address

[File Detection]

Backdoor/Win.Akdoor

Trojan/Win.Agent

Data/BIN.Encrypted

Data/BIN.EncryptKey

Data/BIN.EncPe

[IOC]

141c6e0f5a90b133b00a8d85aa22be67
a4a22eef112bf5d37f0fe422ebf629e5
0c1bd80923691eb5277f5969dc456c50
2ba1443fa75ced874f49586d39fa929a
798038a1546d2a0625b258885ceba88e
460507242876e7582d6744fa628cfcb6
c59552c62fb99bfd7d63f988c20125ad
08f6ab305b6fcb1ed14b48f6c8b8db76
d4e401a7ce5e5518b13e9344f70f2382
36e1c4a359e2f60007b3f87194503750
dd0eddacd65fe208baf06548635584a7
47a07dc9a87ec29f2aee20287330fa34
78c6f1cb87039ad99f39b8a880a016b2
fcb1cbc5abfa4f5644b32368f2593de3
4e3724128e3a8775d8b8ec98ea94dbc2
9731ae209364fe224d873b49e284a19f
e600fe93690175b85415f021165ca111
1509727ff1d47cf701068000d8b137ab
2fec123d69d8958c5f1e1c512da30888
dfa0adb2d2d8208f0dc7dabe97541497

hxxps://www.dbclock.com/bbs/media/preview.php

hxxp://www.krtnet.co.kr/images/support/faq.php

hxxp://www.donganmiso.com/hm_board/works/libs/info.php

hxxps://www.akdjbcc.co.kr/api/score_list.asp
hxxp://charmtour.co.uk/common/shopsearch.asp
hxxps://www.okcc.co.kr/html/board/reserve03_add.asp
hxxp://www.kwangneungcc.co.kr/admin/board/Event/list_add.asp
hxxps://www.shoppingbagsdirect.com/.well-known/validation.asp
hxxps://www.kkw119.com/.well-known/pki-validation/auth.asp
hxxps://www.shoppingbagsdirect.com/.well-known/validation.asp
hxxps://www.myungokhun.co.kr/_proc/member/sitemap.asp
hxxp://youthc.or.kr/community/template.asp
hxxp://paadu.or.kr/sitemap.asp
hxxps://www.shoppingbagsdirect.com/.well-known/validation.asp
hxxp://www.youthc.or.kr/community/template.asp
hxxp://pasc.co.kr/family/data/smartlist.asp
hxxp://www.paadu.or.kr/sitemap.asp

For the entire code and more detailed explanation of features, check ATIP, ‘the next-generation threat intelligence platform.’

Categories:[Malware Information](#)

Tagged as:[APT](#),[Company Attack](#),[DLL](#)