라이브러리 파일 이용 국내 기업 APT 공격

asec.ahnlab.com/ko/22975/

2021년 5월 13일

최근 국내 기업들을 대상으로 지속적인 타깃 공격이 발생하였다. 기업의 침해 시스템에서 수집된 악성 파일 중 상당수는 동적 라이브러리(DLL) 파일이었다. 그러나 이번 공격에 사용된 파일은 일반적인 DLL 파일과는 달랐다. 수집된 파일은 정상 라이브러리가 다양한 방식으로 악의적으로 변조된 파일이었다.

어떤 경로로 시스템에 악성 파일이 생겼는지, 최초 공격 유입 경로는 무엇이었는지는 알려지지 않았다. 또한 단독 실행이 불가능한 라이브러리 특성상 이를 실행하는 트리거 행위나 추가 파일 정보도 확인되지 않았다. 그러나 현재까지 수집된 파일만으로도 이번 공격의 명확한 특징이 있다.

- 정상 라이브러리(DLL) 파일의 Export 정보를 변조(추가, 교체, 변경)한 악성 파일
- 악성 파일을 실행하기 위해 유효한 인자나 데이터 파일 필요
- 인자나 데이터 파일을 통해 기능의 모듈화 및 기능 교체 가능

라이브러리 파일 이용 공격 특징

정상 라이브러리 파일에 Export 함수를 새로 추가하거나 함수 형식을 교체, 또는 기존 함수의 코드를 변경하는 방식으로 악성 파일을 제작하였다. 정상적인 코드가 대부분이기 때문에 유심히 보지 않으면 정상 파일로 오판할 가능성이 높다.

악성 파일이 실행되기 위해서는 유효한 인자나 데이터 파일이 필요하다. 즉, 단독 파일만으로는 파악할 수 있는 기능에 한계가 있다. 자동화된 분석 장비에서도 유의미한 실행 결과가 나오지 않는다.

인자나 데이터 파일을 이용하여 기능을 파편화(모듈화)하였다. 어떤 정보가 입력되는지에 따라 메모리에서 실행되는 코드나 C&C 주소 등이 달라질 수 있다. 시스템이 장악된 상태라면 공격자가 기능을 실시간으로 계속 교체할 수 있다.

라이브러리 변조 및 동작 방식에 따른 악성 파일 유형

기업 침해 시스템에서 수집된 악성 라이브러리 파일은 변조 및 동작 방식에 따라 4가지 유형으로 분류 가능하다. [표 1]은 공격자가 변조했을 것으로 추정되는 정상 라이브러리 파일명과 악성 라이브러리 파일의 수집 당시 파일명, 그리고 PE 파일 포맷 상 'Export Directory'에 명시된 DLL 이름을 유형별로 나열한 것이다. 파일의 기능만 보았을 때는 유형 간 직접적인 연관성은 없다.

수집된 악성 라이브러리 파일은 정상 원본 라이브러리 파일을 변조한 형태이지만 파일명은 다르다. 만약 파일명이 동일했다면 공격자가 라이브러리 파일을 교체하는 DLL 하이재킹(Hijacking) 방식으로 악성코드를 실행했을 가능성이 있다. 그러나 공격의 최초 유입 경로를 포함한 부가 정보가 확인되지 않았기 때문에 파일명이 변경된 것인지, 단순히 정상 라이브러리 파일을 변조해 위장한 것인지는 알 수 없다. 즉, 어떻게 악성 라이브러리 파일을 실행했는지는 현재 확인되지 않는다.

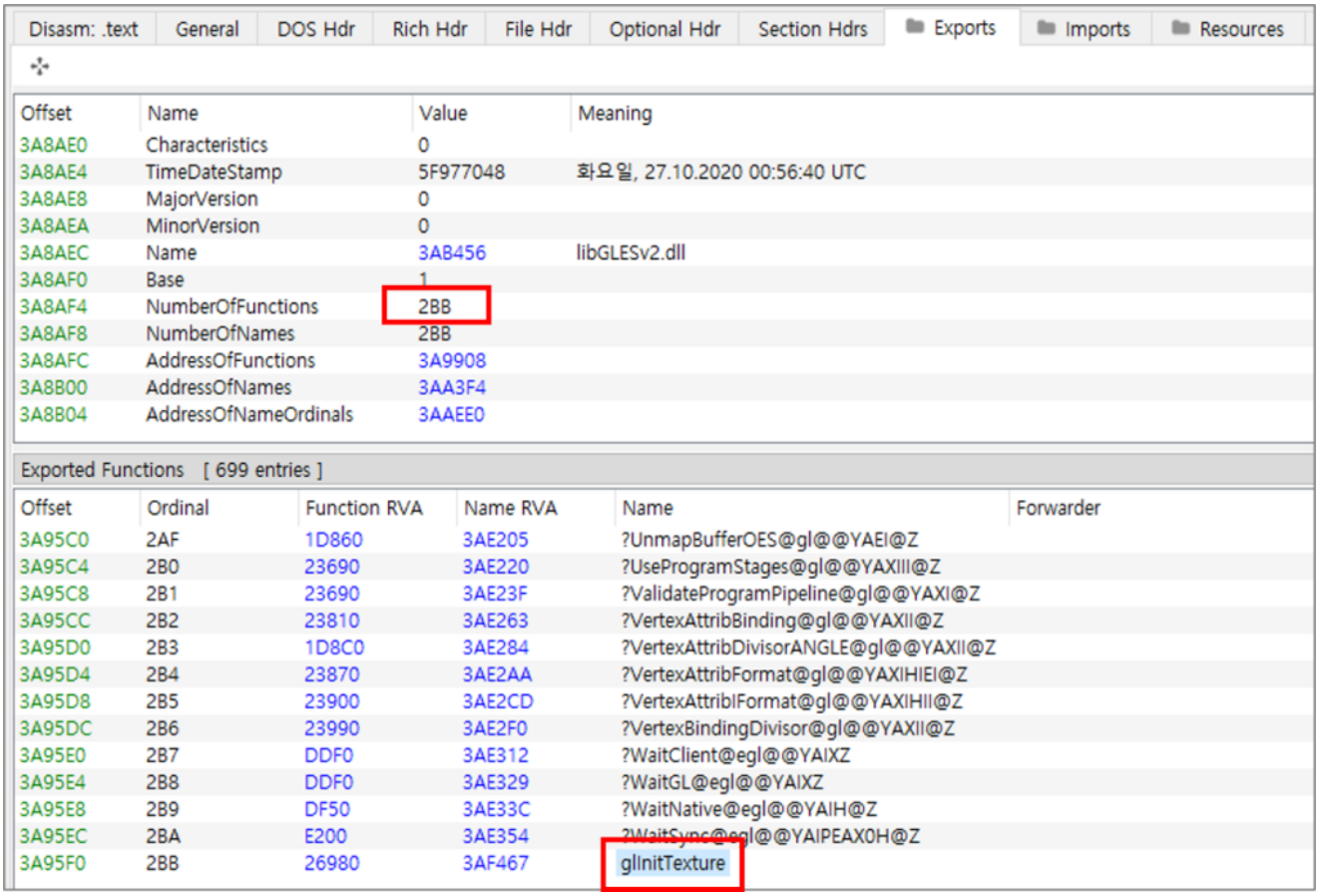
수집된 악성 라이브러리 파일명은 'Export Directory' 구조체에 명시된 DLL 이름과도 다르다. 그러나 'Export Directory' 구조체의 DLL 이름은 라이브러리가 로드될 때 영향을 주지 않는 영역이기 때문에 큰 의미는 없다. 다만 공격자가 정상 라이브러리 파일을 변조하는 과정에서 이를 수정했을 것으로 예상된다.

유형	정상 DLL 파일명	악성 DLL 파일명	악성 DLL 파일의 Export DLL 이름
A	libGLESv2.dll	–	libGLESv2.dll
B-1	libxml2.dll	pchsvc.dll	libxml2.dll
B-2	알 수 없음	srsvc.dll	audiosrv.dll
C	NppExport.dll	wmicr.dll	svcloader.dll
D	dokan1.dll	–	dokan1.dll
D	dokan1.dll	uso.dat	dokan1.dll
D	dokan1.dll	zlib1.cab	dokan1.dll

공격에 이용된 악성 라이브러리 파일 유형 분류

[유형 A] 악성 Export 함수 추가, 인자 필요

정상 libGLESv2 라이브러리 파일에 악성 Export 함수 glInitTexture를 추가하였다. 함수가 추가된 것이기 때문에 'Export Directory' 구조체의 Export 함수 개수도 정상보다 1개 더 많다. glInitTexture 함수가 실행되면 32자 길이의 실행 인자 조건을 확인한다. 인자를 이용하여 내부 연산을 하고 이후 메모리에서 악성 PE를 실행한다. 유효 인자 정보가 확인되지 않아 실행되는 PE의 기능은 알 수 없다.



Disasm: .text | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Exports | Imports | Resources

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	

Exported Functions [699 entries]

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
3A95C0	2AF	1D860	3AE205	?UnmapBufferOES@gl@@YAEI@Z	
3A95C4	2B0	23690	3AE220	?UseProgramStages@gl@@YAXII@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	?VertexAttribIFormat@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@@YAIPEAX0H@Z	
3A95F0	2BB	26980	3AF467	glInitTexture	

유형 A 악성 파일의 Export 함수

[유형 B-1] 정상 함수를 악성 ServiceMain 함수로 교체, ADS 데이터 필요

정상 libxml2 라이브러리 파일의 첫번째 Export 함수인 DllMain 함수를 악성 ServiceMain 함수로 교체하였다. Export 함수 개수는 변화가 없다. ServiceMain 함수이기 때문에 윈도우 서비스로 동작한다. 실행 과정에서 ADS (Alternate Data Streams) 데이터를 읽는다. ADS를 이용해 실행에 필요한 악성 데이터를 사용자 눈에 보이지 않게 숨겼다. zone과 data 스트림은 각각 암호화된 데이터와 암호를 풀기위한 키 데이터이다. 내부 연산 이후 메모리에서 악성 PE를 실행한다. 실행된 악성 PE는 rsrc 스트림 데이터를 필요로 한다. 최종 기능은 C&C 접속이다.

Disasm: .text | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Exports | Imports | Resources

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	

Exported Functions [1656 entries]

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...	

유형 B-1 악성 파일의 Export 함수

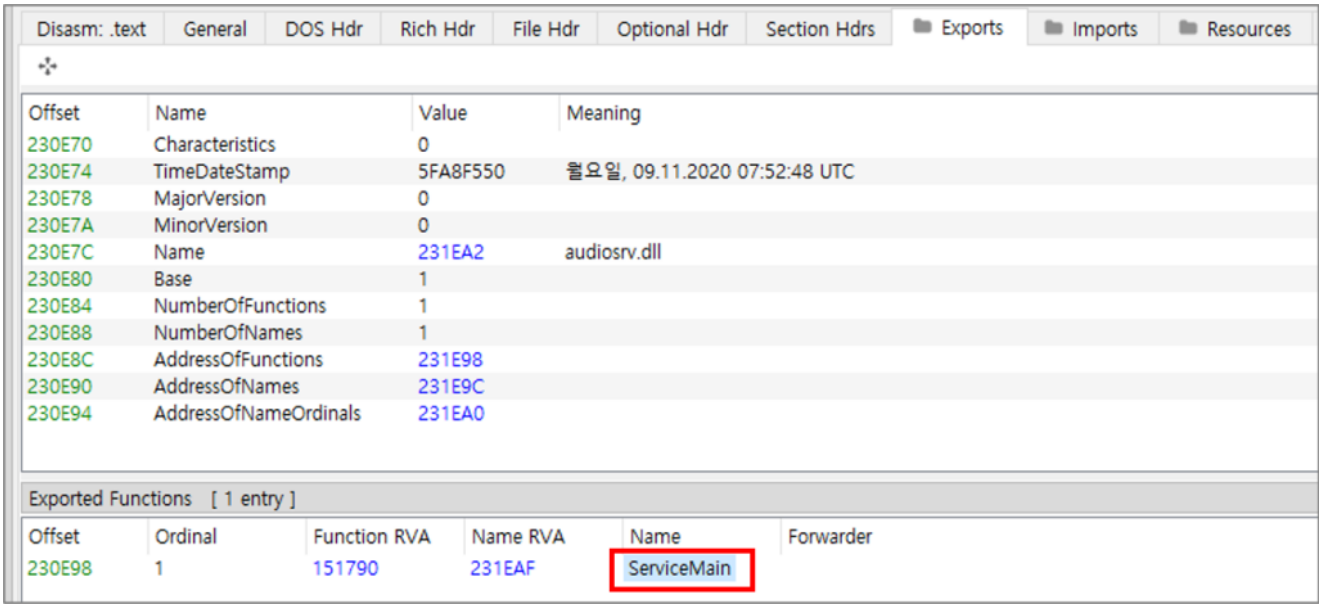
```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   31 59 6A 49 7A 71 73 78 6A 69 62 31 5A 53 6C 31  1YjIzqsxjib1ZSl1
00000010   64 48 4E 51 62 67 44 66 64 67 42 57 64 6D 76 42  dHNQbgDfdgBWdmvB
```

```
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  &ûÅúy˜..´...í&éH
00000010   B0 A9 9F 40 B7 BD 08 7E D5 DE 1E CC 3F 11 39 73  °©Ÿ@·½.~ÕÞ.Ì?.9s
00000020   0A 53 B1 BE 2D 72 E3 3F 30 3C FD 3F 82 EF 99 60  .S±¾-rã?0<ý?,ï™`
00000030   BD 01 1B FA 38 04 7E 27 C5 74 D5 A9 5E B1 29 B1  ½..ú8.~'ÅtÕ©^±)±
00000040   3A 93 7F B1 97 2E A6 EF 4F D6 59 51 9E 9D F5 94  :".±—.¦ïOÖYQž.õ"
00000050   DC 5B 38 FA BC 54 62 AB 83 BA B2 85 6B 7E 00 07  Ü[8ú¼Tb«ƒº²…k~..
00000060   BC E5 7A 75 7F 1C DA DD 12 B7 2B 2B 09 55 EA F7  ¼åzu..ÚÝ.·++.Uê÷
00000070   B6 C0 0E C6 B6 A2 D3 FC D8 18 5D 4B D8 81 14 F3  ¶À.Æ¶¢ÓüØ.]KØ..ó
00000080   7A 72 9B 94 56 03 5E 25 35 A4 B9 99 FF 80 6B 27  zr›"V.^%5¤¹™ÿ€k'
00000090   A7 EA 9B 7A 46 59 17 59 B2 F3 C3 39 AE 26 D3 51  §ê›zFY.Y²óÃ9®&ÓQ
000000A0   77 FA BA 62 7E 94 68 57 AC 72 2F 6A 0D F5 74 BF  wú°b~"hW¬r/j.õt¿
000000B0   C6 B2 DE 15 B3 75 47 08 DC 65 DB 6D D3 68 BE 1E  Æ²Þ.³uG.ÜeÛmÓh¾.
000000C0   4A 8F E7 CC 23 D5 61 FC 35 84 6E 40 A9 F6 3E 90  J.çÌ#Õaü5„n@©ö>.
000000D0   04 54 7C 07 9D CA EB 43 E6 A9 0B 28 7E EA A8 E3  .T|..ÊëCæ©.(~ê¨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  /™XyUûo«ÛÜ.l¹_.Z
```

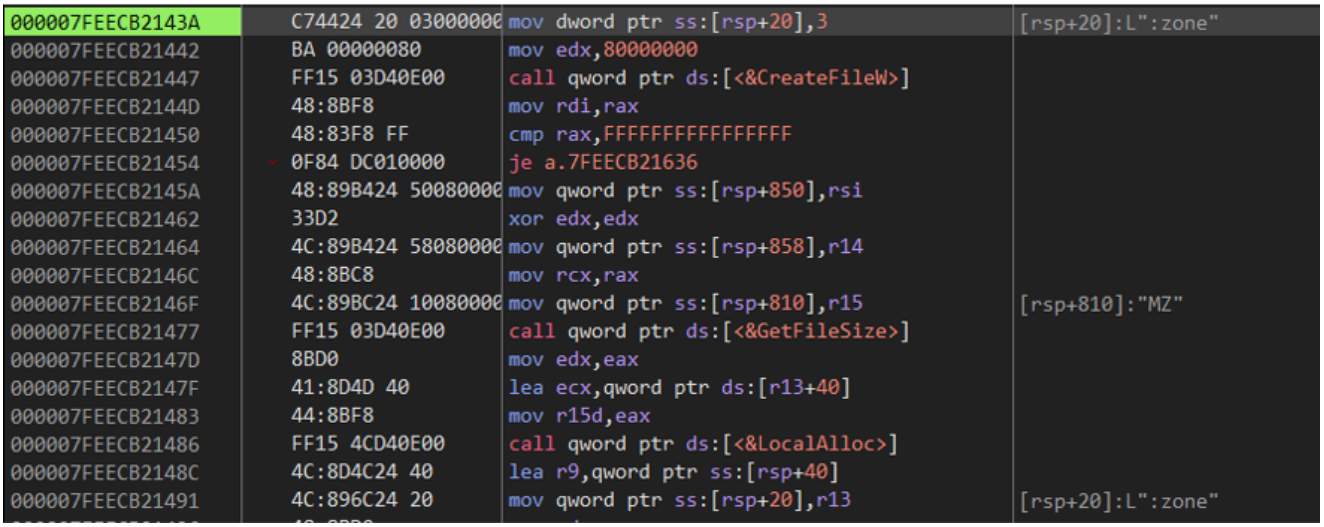
'data' ADS 데이터와 'zone' ADS 데이터

[유형 B-2] 악성 ServiceMain 함수 단독 존재, ADS 데이터 필요

정상 라이브러리 파일 존재 여부가 불분명하다. Export 함수로 윈도우 서비스 ServiceMain 함수만 존재한다. 다른 유형과는 다르게 파일 리소스 버전 정보가 없고 악성 ServiceMain 함수를 제외한 Export 함수가 없는 점을 고려하였을 때 단독으로 제작된 악성 라이브러리 파일일 수 있다. 코드 전개 차이는 있지만, B-1 유형과 기능이 유사하며 zone과 data 이름의 ADS 데이터가 필요하다. 스트림 데이터가 수집되지 않아 이후 기능은 알 수 없다.



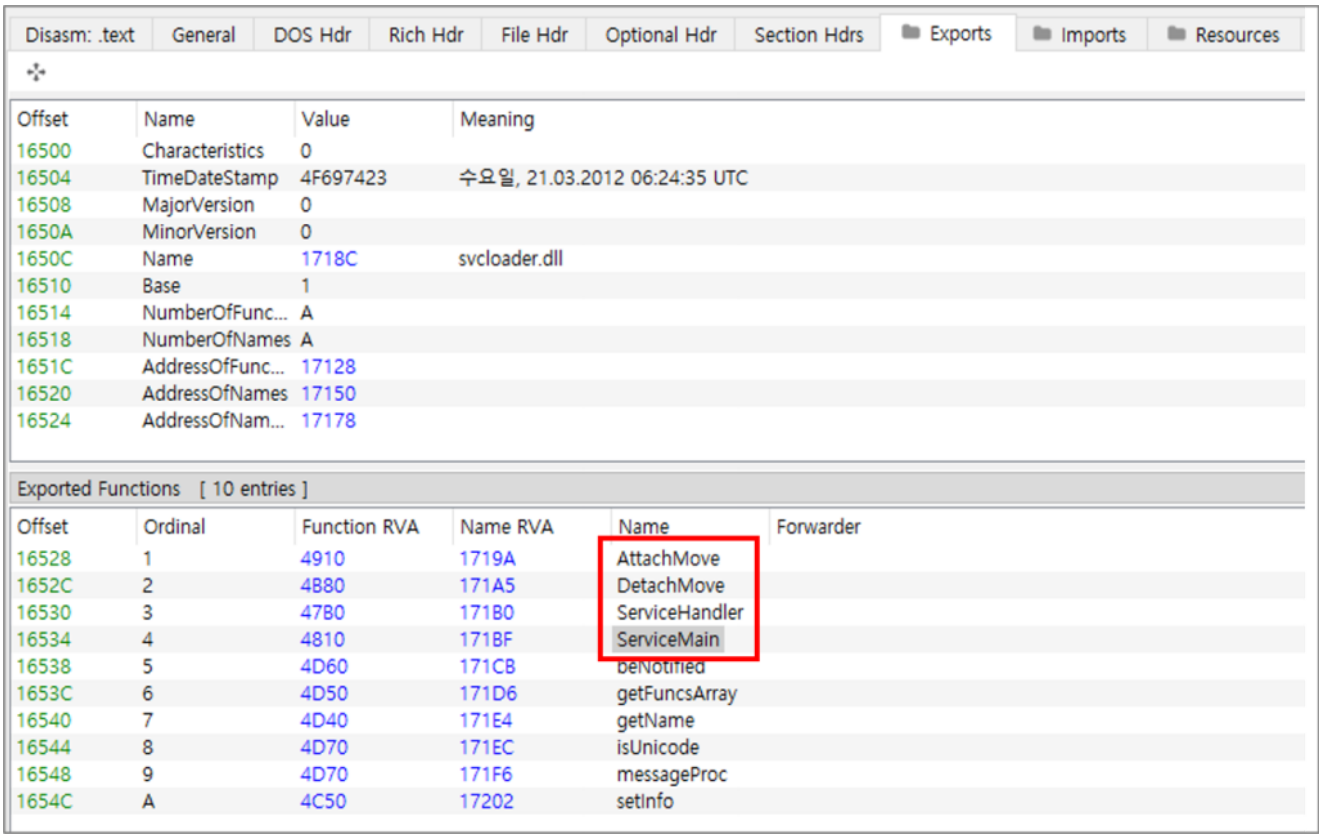
유형 B-2 악성 파일의 Export 함수



ADS 데이터에 접근

[유형 C] 악성 ServiceMain 외 함수 추가, 데이터 파일 필요

Notepad++ 플러그인 NppExport 라이브러리를 변조하였다. 정상 라이브러리에는 없는 Export 함수를 4개 추가하였는데, 윈도우 서비스로 동작하기 위한 ServiceMain과 ServiceHandler 악성 함수 외에 AttachMove와 DetachMove 함수가 특징적이다. AttachMove와 DetachMove 함수는 기능상으로는 정상이며, 원본 라이브러리에서 DllMain 함수에 있던 코드가 옮겨졌다. 고정 경로에 존재하는 wmicc.dat 데이터 파일을 이용하여 내부 연산을 하고, 이후 메모리에서 악성 PE를 실행한다. 실행된 악성 PE는 wmicd.dat 데이터 파일이 필요하고 최종 기능은 C&C 접속이다.



Disasm: .text | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Exports | Imports | Resources

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	

Exported Functions [10 entries]

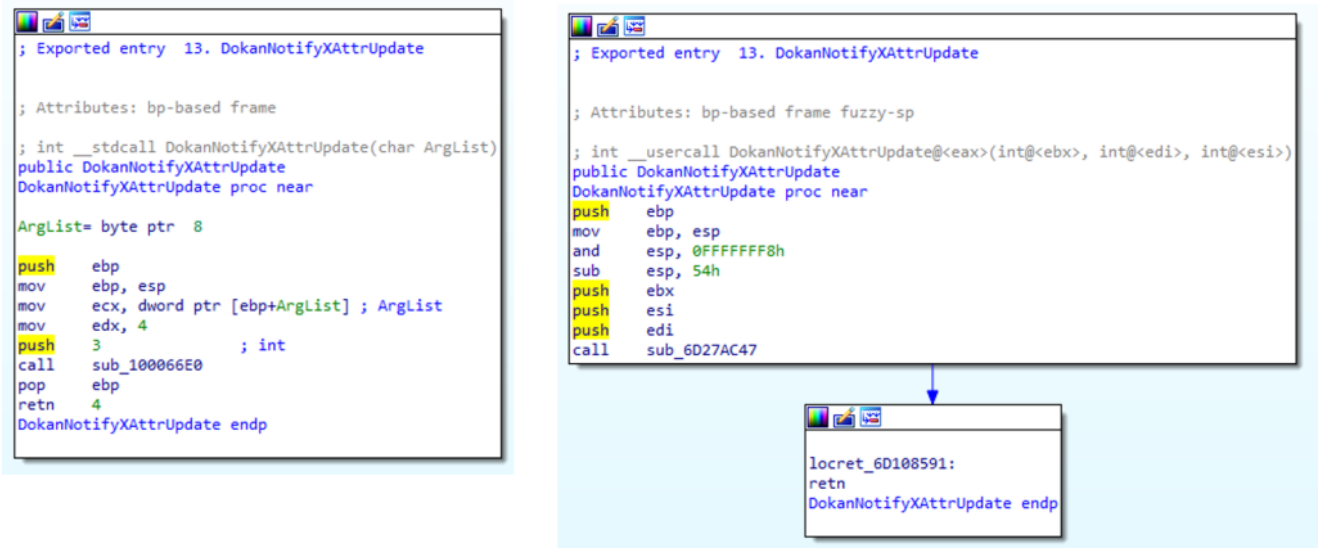
Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
16528	1	4910	1719A	AttachMove	
1652C	2	4B80	171A5	DetachMove	
16530	3	47B0	171B0	ServiceHandler	
16534	4	4810	171BF	ServiceMain	
16538	5	4D60	171CB	beNotified	
1653C	6	4D50	171D6	getFuncsArray	
16540	7	4D40	171E4	getName	
16544	8	4D70	171EC	isUnicode	
16548	9	4D70	171F6	messageProc	
1654C	A	4C50	17202	setInfo	

유형 C 악성 파일의 Export 함수

[유형 D] 기존 함수의 코드 변경, 인자 필요, 데이터 파일 생성 및 로드

정상 Dokan 라이브러리를 변조하였다. 가장 독특한 변조 형태로서 Export 함수 추가나 교체가 아닌 함수 내 바이너리 코드만 변경하였다. 기존 유형처럼 'Export Directory' 구조체 정보로는 변조 여부를 확인하기가 쉽지 않다. 또한 기존 VC++ 파일을 Vmprotect로 패킹하여 전체 코드 패턴을 바꿨기 때문에 코드 변경 여부와 기능 파악을 어렵게 하였다. Vmprotect를 언패킹하고 Export 함수별로 비교하여 변경된 코드를 확인할 수 있다. 코드가 변경된 함수는 DokanNotifyXAttrUpdate 이다.

악성 Export 함수 호출 시 '-s' 로 시작하는 유효 인자가 전달되어야 동작한다. 인자가 주어지면 시스템 %Temp% 경로에 VirtualStore.cab 데이터 파일을 생성할 수 있고, 특정 조건에 맞는 인자일 경우에는 데이터 파일을 로드한다. 데이터 파일은 C&C 통신을 위한 코드 실행과 URL 정보이다. 침해 시스템에서 다수의 VirtualStore.cab 데이터 파일이 확인되었는데, 공격자가 C&C 서버를 실시간으로 바꾼 것으로 보인다.



```
; 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@<ebx>, 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
```

유형 D 악성 파일의 함수 코드 패치

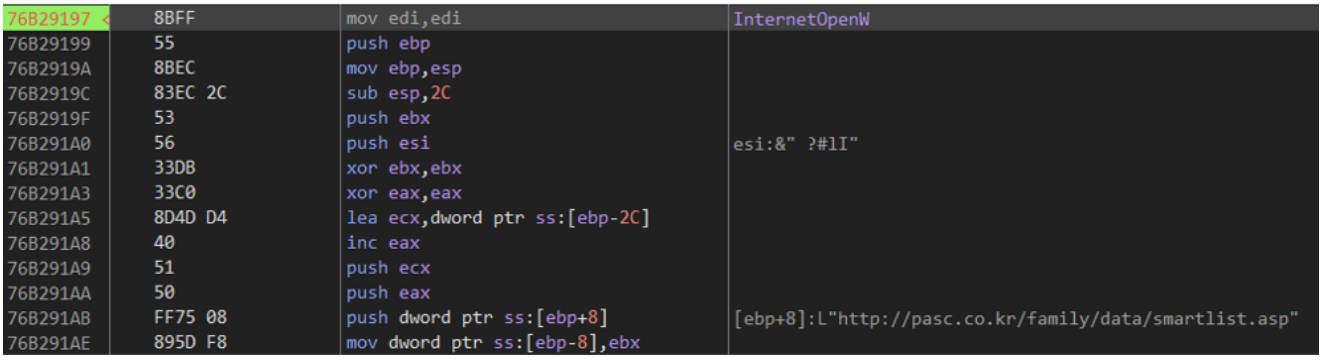
```
00000000  F0 31 3B 06 9C BA 43 08 05 BE 83 15 38 FB 4F 22  ð1;.œºC..¾ƒ.8ûO"
00000010  6F 6E 15 65 83 32 12 28 46 24 56 BC E3 3A BF B3  on.eƒ2.(F$V¼ã:¿³
00000020  67 89 3C D8 78 EB 31 E0 72 31 82 7F BA 3B 0D 39  g‰<Øxë1àr1‚.º;.9
00000030  6D D6 7E A8 1E 53 4A 60 28 CF 25 53 E1 95 C3 03  mÖ~¨.SJ`(Ï%Sá•Ã.
00000040  9D D6 D1 94 F1 5C 6E 5F AB A3 20 83 2A 9E 7D 36  .ÖÑ"ñ\n_«£ ƒ*ž}6
00000050  B4 D9 29 4F 3E 63 94 5E B8 46 72 4A 3F B5 B9 F1  ´Ù)O>c"^¸FrJ?µ¹ñ
00000060  8E EB BD BB 50 94 2A 7F E6 BC 56 EF CB A8 31 BC  Žë½»P"*.æ¼VïË¨1¼
00000070  EA 65 84 99 BD F0 3D 8B 72 32 B4 E8 D1 F7 EB 36  êe„™½ð=‹r2´èÑ÷ë6
00000080  55 73 64 A2 A8 06 C4 05 42 72 D2 02 83 87 8A 7C  Usd¢¨.Ä.BrÒ.ƒ‡Š|
00000090  12 6F E2 FE F0 60 F3 71 48 11 08 04 41 39 21 4F  .oâþð`óqH...A9!O
000000A0  C2 45 0E 45 1A C8 88 8A 6D 1A F1 DC BD 9A 82 52  ÂE.E.È^Šm.ñÜ½š‚R
000000B0  A8 50 78 2D 06 38 8A 95 DE 0E 4C EC BF 6B B0 9A  ¨Px-.8Š•Þ.Lì¿k°š
000000C0  10 25 D5 02 41 59 C3 FF 60 8B 71 6E 34 71 86 0E  .%Õ.AYÃÿ`‹qn4q†.
000000D0  5F 01 3D 83 9C 90 B1 C3 2E C2 B9 66 03 98 BB CA  _.=ƒœ.±Ã.Â¹f.˜»Ê
000000E0  37 71 32 80 F1 07 84 58 C1 1D F3 3F BE 62 48 49  7q2€ñ.„XÁ.ó?¾bHI
000000F0  A5 52 49 D3 12 EB 9C C8 0E 03 5D 45 8B 03 3A 99  ¥RIÓ.ëœÈ..]E‹.:™
```

VirtualStore.cab 데이터 파일

```
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,#lÐ,
6C233137    83FF FF             cmp edi,FFFFFFFF                    edi:&"ð)#l@+#lp*#l°+#lÀ,#lÐ,
6C23313A    74 1C               je sample.6C233158
6C23313C    6A 00               push 0
6C23313E    57                  push edi                            edi:&"ð)#l@+#lp*#l°+#lÀ,#lÐ,
6C23313F    50                  push eax                            eax:&"ð)#l@+#lp*#l°+#lÀ,#lÐ,
6C233140    E8 72B61600         call sample.6C39E7B7
6C233145    8BF0                mov esi,eax                         eax:&"ð)#l@+#lp*#l°+#lÀ,#lÐ,
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\
```

DokanNotifyXAttrUpdate 함수에서 데이터 파일 접근



```
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:&" ?#lI"
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
```

C&C 주소 접속

[파일 진단]

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.shopingbagsdirect.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

전체 코드와 보다 자세한 기능 설명은 '차세대 위협 인텔리전스 플랫폼' ATIP 에서 제공하고 있습니다.

Categories:악성코드 정보

Tagged as:APT, DLL, 기업공격