북 킴수키(Kimsuky) 조직의 정책 자문 위장 스피어 피싱 주의!

alyacofficialblog.tistory.com/5354

알약(Alyac) March 12, 2024

상세 컨텐츠

본문 제목

북 킴수키(Kimsuky) 조직의 정책 자문 위장 스피어 피싱 주의!

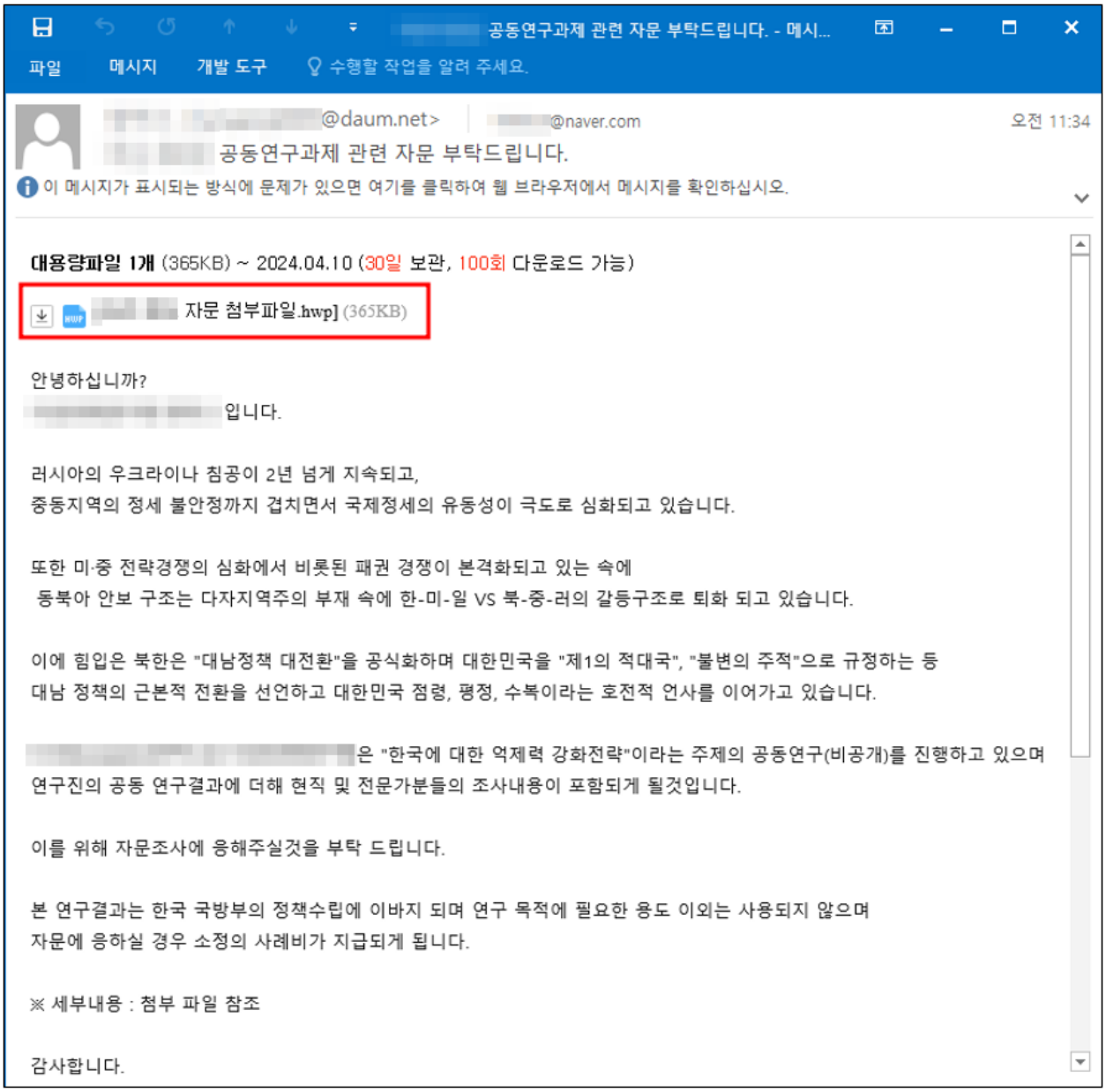
악성코드 분석 리포트
by 알약4 2024. 3. 12. 15:03

본문

안녕하세요? 이스트시큐리티 시큐리티대응센터(이하 ESRC)입니다.

국내 외교안보분야의 민간 정책연구원을 사칭하여, 실제 국방 관련 국가기관에 소속되어 있는 특정인을 타깃으로 한 스피어피싱 공격이 발견되어 주의가 필요합니다.

이번 피싱 메일은 'OO-OOOO 공동연구과제 관련 자문 부탁드립니다.' 라는 제목으로 유포되었고, 대용량파일 'OO-OO 자문 첨부파일.hwp'의 다운로드를 유도하고 있습니다.



[그림 1] 민간 정책연구원 사칭 메일

해당 첨부파일의 다운로드 버튼을 클릭하면 아래와 같이 네이버 로그인을 위장한 피싱 사이트로 연결되고, 여기에 입력한 계정 정보는 공격자의 서버로 전송됩니다.

[그림 2] 네이버 로그인으로 위장한 피싱 페이지

Body

Name	Value
id	ghdrlfehd
pw	1q2w3e4r

[그림 3] 공격자의 서버로 전송되는 계정 정보

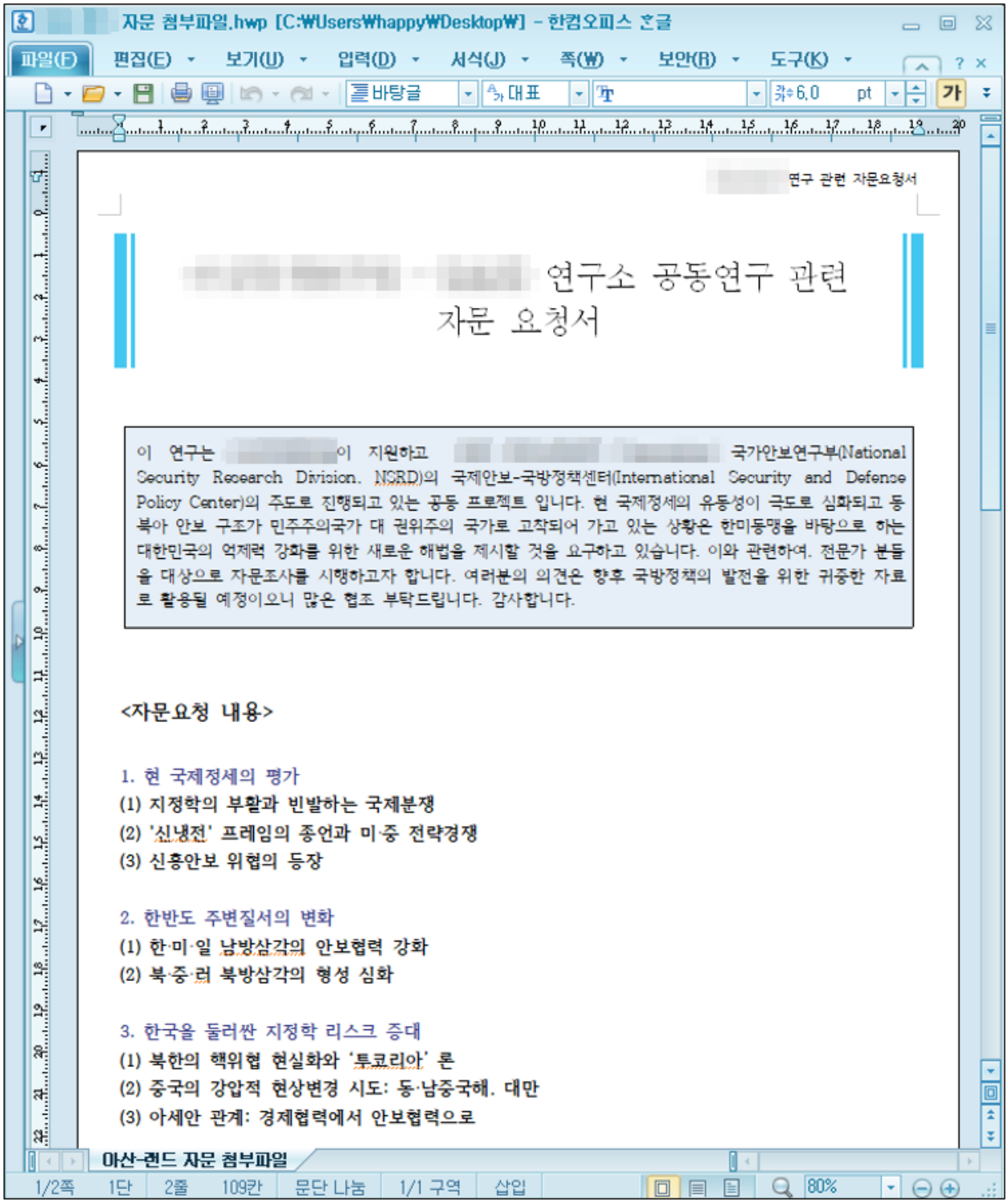
여기까지는 일반적인 피싱이라고 생각할 수 있지만 메일의 첨부파일로 위장한 '[OO-OO 자문 첨부파일.hwp]' 부분의 코드를 살펴보면, a 태그를 이용한 단순 링크가 아닌 form 태그를 사용하였고 hidden 타입으로 된 input 태그에 base64로 인코딩된 문자열이 확인됩니다.

이를 풀어 보면 “[피싱대상ID]**[실제첨부파일url]”의 형태로 구성된 것을 볼 수 있고, 실제 공격 타깃이 계정 정보를 입력해 정상적으로 로그인하였다면 공격자에게 계정정보가 넘어가고, 피해자는 정상 HWP(OO-OO 자문 첨부파일.hwp) 첨부파일을 다운로드 받아 계정정보 탈취 사실을 눈치채지 못하였을 것으로 보입니다.

[그림 4] 악성 사이트로 링크된 스크립트

```
ftstblue**https://attach.mail.daum.net/bigfile/v1/urls/d/J8GlYRtO-JymJaVe98UOikfj-Qo/HVOueYVOw4C-LGO5zkTSsg
```

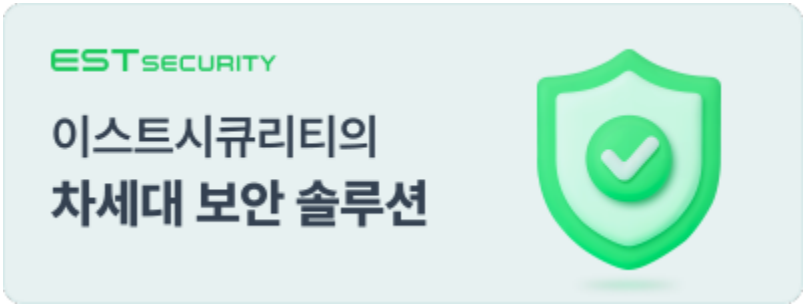
[그림 5] 숨겨진 base64 문자열 디코딩 내용



[그림 6] 실제 첨부 HWP 파일

ESRC는 분석결과를 토대로 해당 공격을 북 킴수키(Kimsuky) 조직의 소행으로 결론지었으며, 공격자들은 다양한 주제를 활용해 외교·안보·국방·통일 및 대북 분야에 대한 사이버 공격을 꾸준히 이어가고 있어 관련 종사자는 사이버 안보에 대한 경각심을 가지고, 보안에 만전을 기해야 합니다.

IoC
hxxps://nid.naveer.p-e[.]kr/loading/
naveer.p-e[.]kr



'악성코드 분석 리포트' 카테고리의 다른 글

ESRC 주간 Email 위협 통계 (3월 넷째주)	**(0)**	2024.03.26
ESRC 주간 Email 위협 통계 (3월 셋째주)	**(0)**	2024.03.19
ESRC 주간 Email 위협 통계 (3월 둘째주)	**(0)**	2024.03.12
ESRC 주간 Email 위협 통계 (3월 첫째주)	**(0)**	2024.03.05
ESRC 주간 Email 위협 통계 (2월 넷째주)	**(0)**	2024.02.27

관련글 더보기

- ESRC 주간 Email 위협 통계 (3월 넷째주)

  2024.03.26

- ESRC 주간 Email 위협 통계 (3월 셋째주)

  2024.03.19

- ESRC 주간 Email 위협 통계 (3월 둘째주)

  2024.03.12

- ESRC 주간 Email 위협 통계 (3월 첫째주)

  2024.03.05

댓글 영역