[SOLDESK;]

랜섬웨어

랜섬웨어에 대한 연구 및 분석

과정 : 모의해킹 침해대응 정보보안 22기

강사 : 백승찬

학생 : 이지훈, 문학진

목 차

1. 실습환경구성 3

환경 구축 3

1. UTM 구축 3

2. SANDBOX 구축 4

3. 랜섬웨어 제작 8

4. ClamWin 구축 12

2. 랜섬웨어 실습 20

랜섬웨어 실습 시나리오 20

1. 랜섬웨어 공격 성공 20

2. 랜섬웨어 공격 실패 20

3 랜섬웨어 분석 21

랜섬웨어 **Wannacry** 분석 21

1. Wannacry 행위 분석 21

2. Wannacry API 분석 22

[레퍼런스**]** 23

1. 실습환경구성

환경 구축

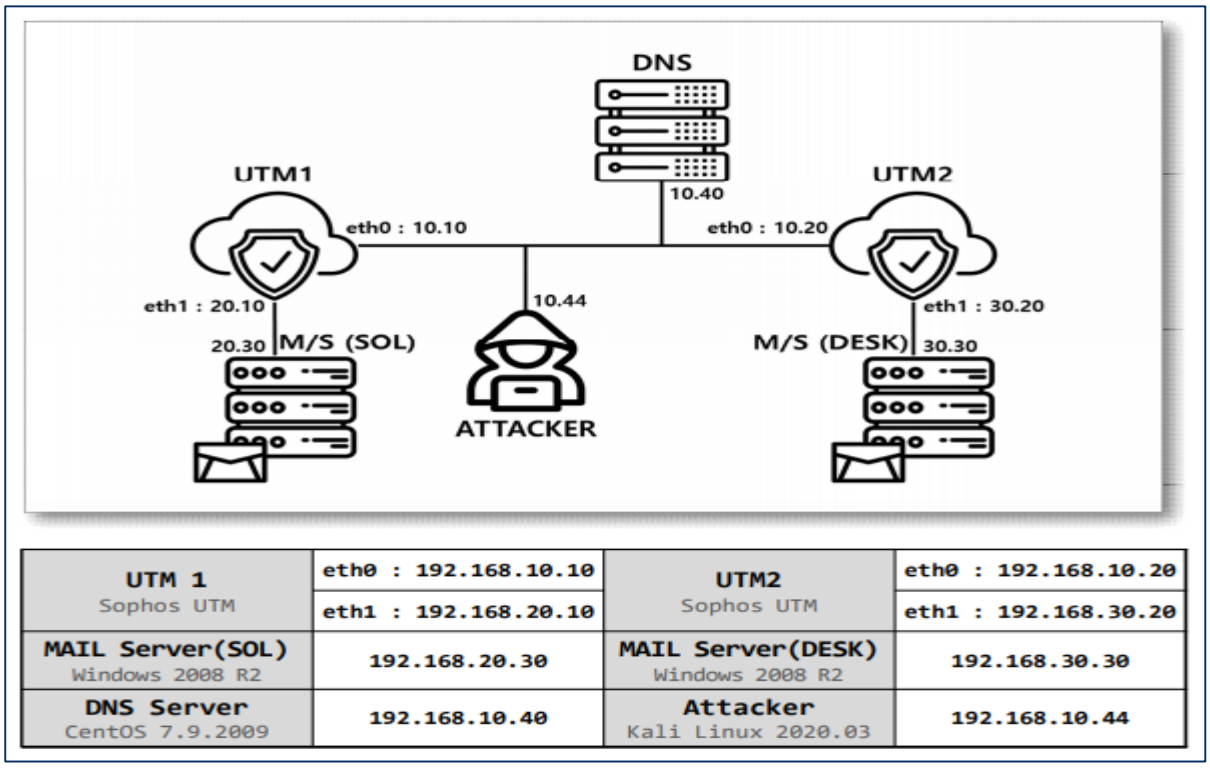
1. UTM 구축

사용 시스템

1. UTM (제품: Sophos UTM 9.7)
2. DNS server (CentOS 7), MAIL Server (Windows 2008 R2), Attacker (Kali Linux)

구축 환경

(링크 참조) 기존에 잘 만들어진 UTM_MAIL_Protection 문서를 참조한다.



UTM 1 Sophos UTM	eth0 : 192.168.10.10 eth1 : 192.168.20.10	UTM2 Sophos UTM	eth0 : 192.168.10.20 eth1 : 192.168.30.20
MAIL Server(SOL) Windows 2008 R2	192.168.20.30	MAIL Server(DESK) Windows 2008 R2	192.168.30.30
DNS Server CentOS 7.9.2009	192.168.10.40	Attacker Kali Linux 2020.03	192.168.10.44

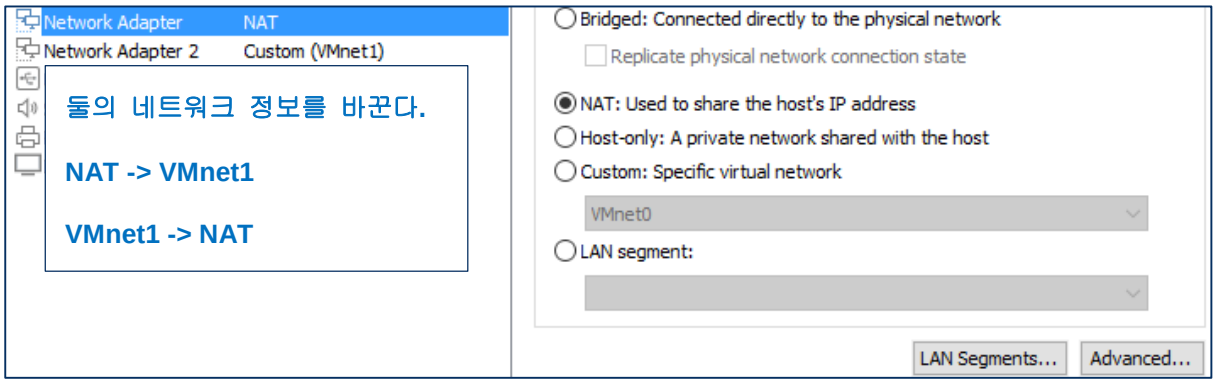
UTM, Mail server, DNS server, Attacker 주요 구성 요소에 대한 정보

UTM: SPAM 필터링 및 보안과 관련된 이메일 보호 기능을 담당한다.

Mail server, DNS server: 일반적인 Mail server 와 DNS 서버이다. 다만 UTM 과 Mail server 가 연동하기 위해서는 UTM 에서 DNS server 를 참조해야 하며, Mail server 에서도 UTM 으로 패킷 릴레이 설정이 되어 있어야 한다.

Attacker: 공격자가 수집한 이메일을 자신의 이메일인 것처럼 속이는 사회 공학 기법을 통해 랜섬웨어를 전파할 것이다.

(설치 중 주의사항) UTM_MAIL_Protection.pdf 파일의 내용을 그대로 따라해주면 된다. VMnet 의 NIC 이 connection 과 잘 안 붙는 경우가 있는데 이때는 IP 정보를 바로 바꿔줄 수 없어서 NIC 위치를 바꾼 후 재부팅 해준다.



2. SANDBOX 구축

사용 시스템

1. SANDBOX (제품: cuckoo sandbox)
2. Virtual Machine(제품: Oracle VM VirtualBox-5.2)

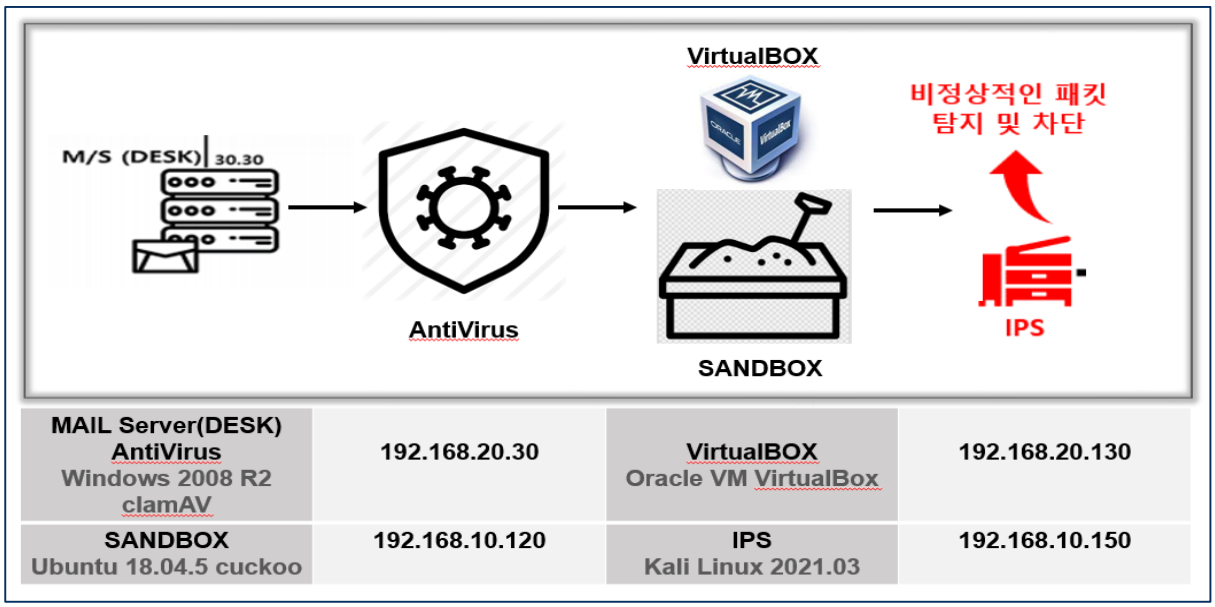
구축 환경

(링크 참조 1) 기존에 잘 만들어진 [웹 문서 1 링크]를 참조한다.

(링크 참조 2) 기존에 잘 만들어진 [웹 문서 2 링크]를 참조한다.

(설치 전 주의사항)

위의 두 문서는 비슷하지만 차이점이 존재한다. 차이점을 찾아 적용하면서 진행해준다.



MAIL Server(DESK) **AntiVirus** Windows 2008 R2 clamAV	**192.168.20.30**	**VirtualBOX** Oracle VM VirtualBox	**192.168.20.130**
SANDBOX Ubuntu 18.04.5 cuckoo	**192.168.10.120**	**IPS** Kali Linux 2021.03	**192.168.10.150**

Mail server(DESK), AV, SANDBOX, IPS 주요 구성 요소에 대한 정보

AV: AntiVrius 제품이다. DESK 유저가 랜섬웨어를 실행을 하게 되었을 때 랜섬웨어로 의심되면 실행하지 못하게 한 후 SANDBOX 로 보낸다.

Mail server(DESK): Attacker 에 의해 사회 공학 기법으로 랜섬웨어를 모르고 설치한 후 실행하게 되었다.

IPS: 이상 행위가 감지될 경우, Rule 을 통해 공격을 차단한다. 지금은 랜섬웨어 행위를 감지하여 공격을 차단한다.

SANDBOX: AV 가 보내준 파일이 랜섬웨어인지를 동적 분석을 통해 판단 후 랜섬웨어가 맞다면 IPS 에 알린다.

VirtualBOX: 악성코드가 실행되는 VM 이다.

설치 중 문서에는 없어서 **Error** 가 발생한 부분에 대해서 서술한다.

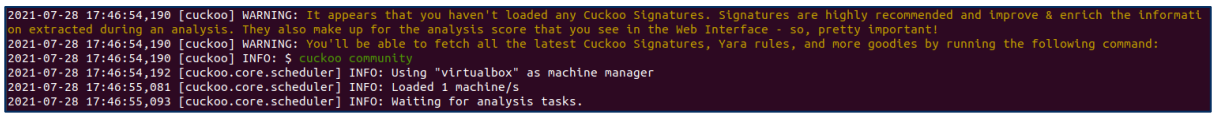
설치 중 주의사항 1	해결책
파이썬 **pip** 를 업그레이드 해야 한다. **# sudo pip installcuckoo** 위의 명령어를 입력하면 에러가 날 것이다. **pip** 를 업데이트 한 후 다시 설치하도록 한다.	**# python –m pip install –upgrade pip**

설치 중 주의사항 2	해결책
cuckoo 를 실행할 때 **openssl** 관련 에러가 나올 수 있다.	**# pip uninstall pyopenssl** 이후 다시 **# pip install pyopenssl**

(실행 중 주의사항 1) cuckoo 실행 절차를 아래와 같이 진행한다. 그렇지 않으면 에러가 발생한다.

1. 문서대로 구성이 완료되었다면 virtualbox 를 종료한다.

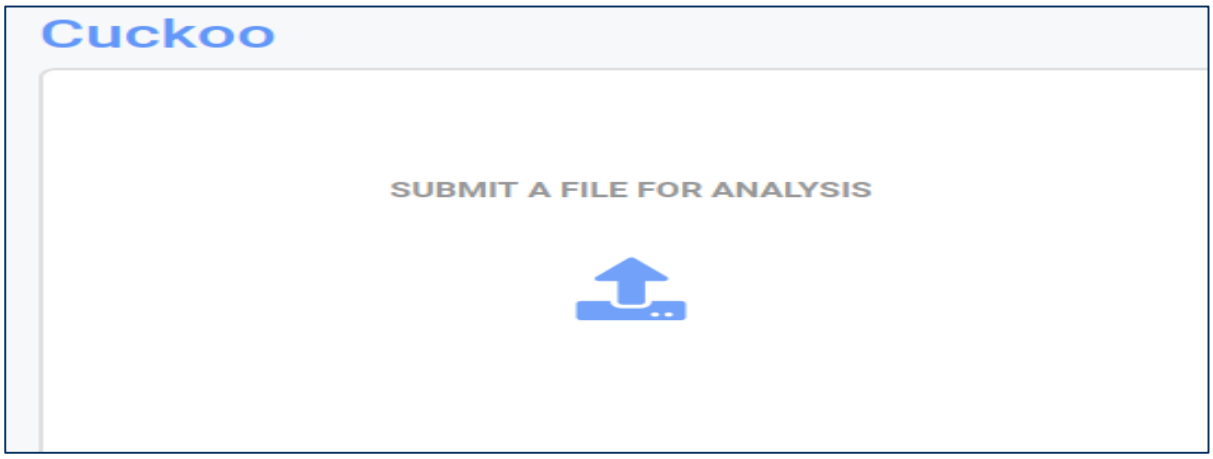
2. cuckoo 명령어를 실행한다.

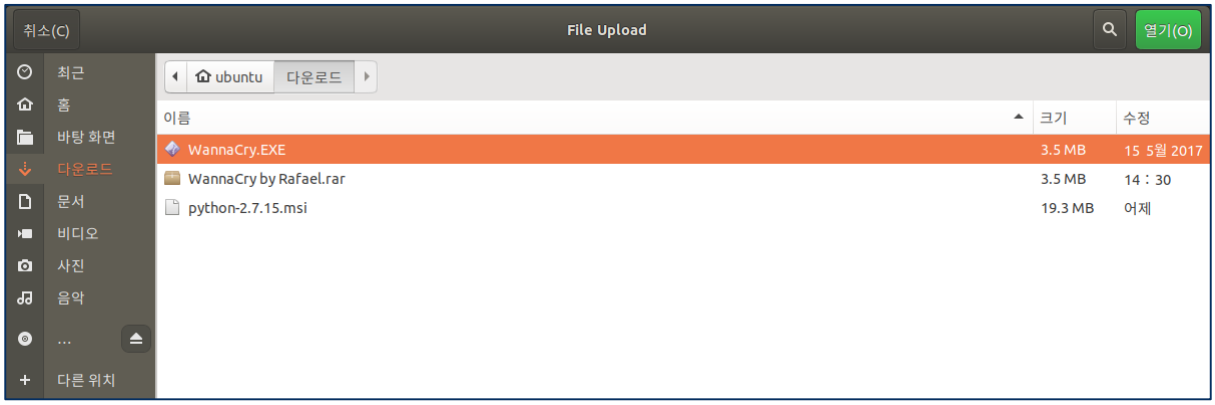


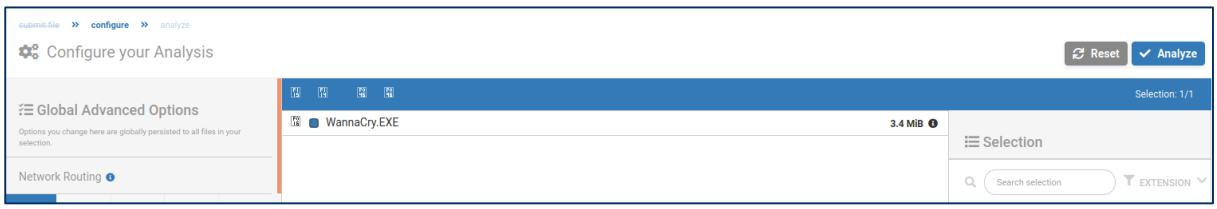
3. cuckoo web runserver 명령어를 실행한다.

```
ubuntu@ubuntu-virtual-machine:~/.cuckoo/conf$ cuckoo web runserver
Performing system checks...

System check identified no issues (0 silenced).
July 28, 2021 - 17:47:19
Django version 1.8.4, using settings 'cuckoo.web.web.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

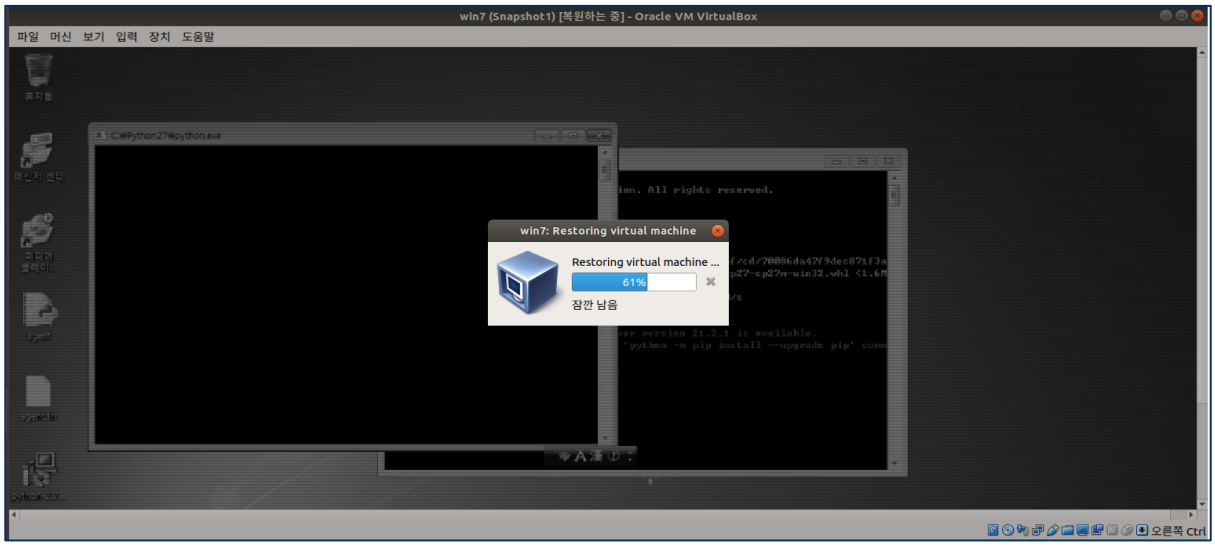
4. 랜섬웨어를 선택하고 submit 이후 analyze 를 눌러주면 virtualbox 가 실행되면서 분석 이후 종료된다. 아래는 4 번의 실행 화면이다.

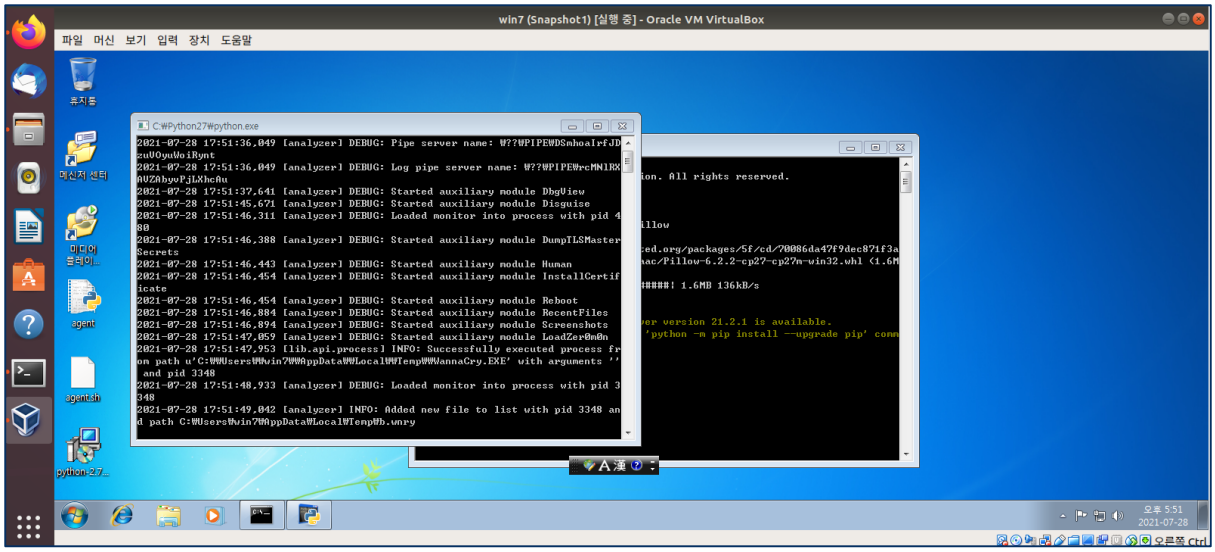




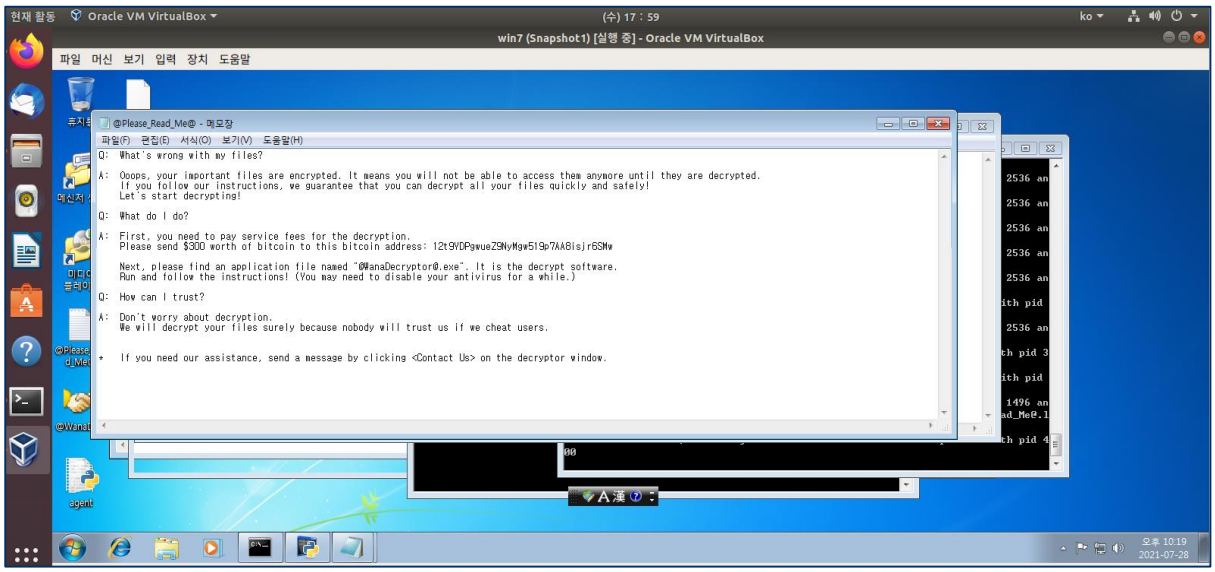


(실행 중 주의사항 1-1) 4 번을 작업하고 있을 때 virtualbox 를 따로 킨 상태라면 충돌이 발생하여서 win7 이 DOWN 되므로 이전에 켜놓은 virtualbox 를 꼭 종료한다.





WannaCry.EXE **실행** **화면**



3. 랜섬웨어 제작

(제작 전 주의사항) 랜섬웨어는 굉장히 위험하므로 꼭 네트워크가 닿지 않고 중요한 자료가 없는 곳에서 작업을 할 수 있도록 한다. 그리고 분석 작업을 진행할 때도 꼭 cuckoo sandbox 와 같은 sandbox 기법을 사용하도록 한다.

<제작 방식>

1. 직접 만들기

    ① 툴을 가지고 만들기 (Virus Maker) – sourceforge

    ② 직접 제작 (powershell, batch script) – .bat 방식이나 파워쉘 방식

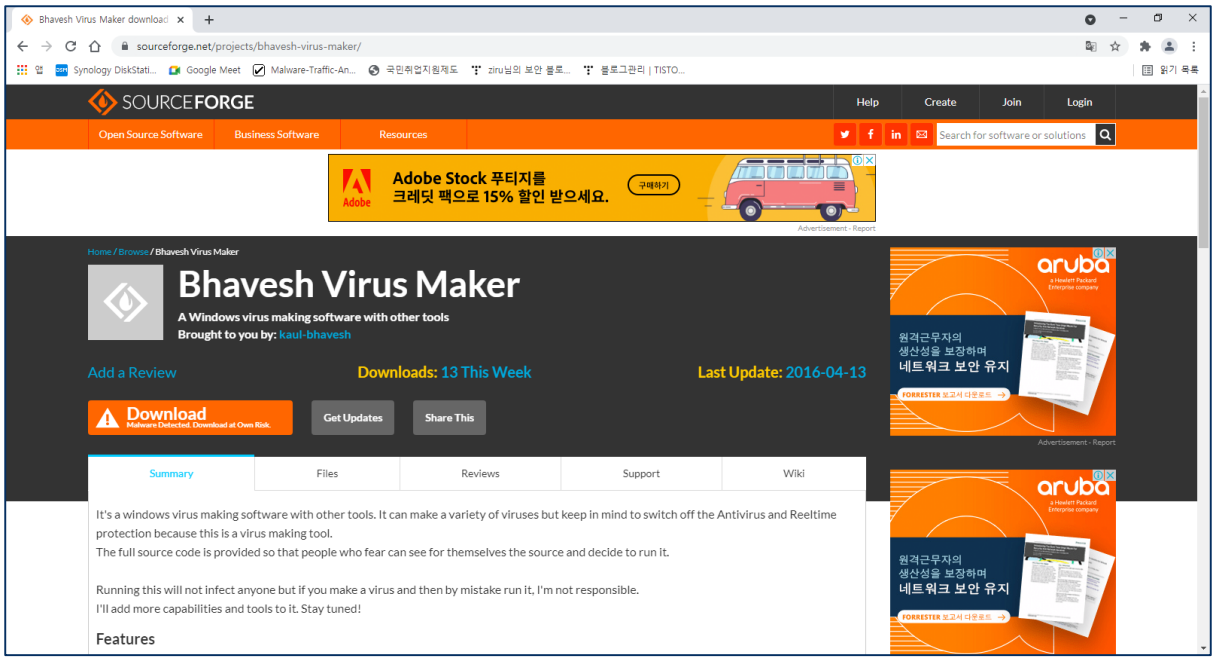
2. 다운로드

    ① virusshare.com -> sandbox (cuckoo sandbox)

    ② (참조) [기타 링크] # 랜섬웨어 관련 자료

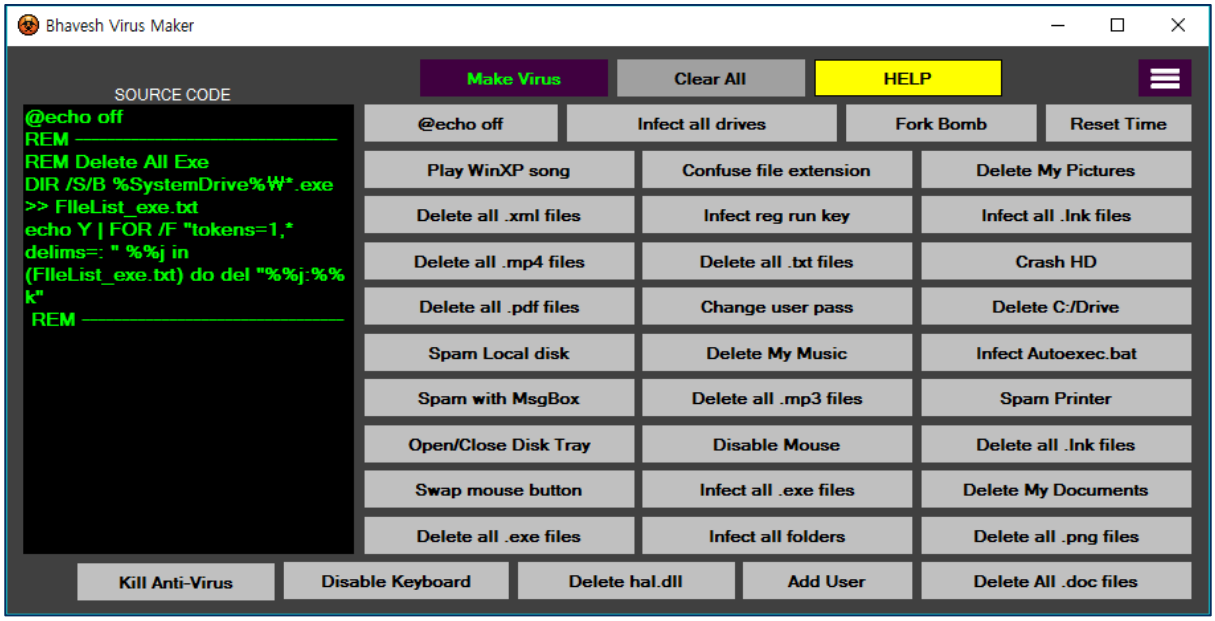
제작한 랜섬웨어 및 다운로드한 랜섬웨어

① 툴을 가지고 만들기 (Virus Maker) – sourceforge



1. sourceforge 사이트에서 Bhavesh Virus Maker 설치한다.

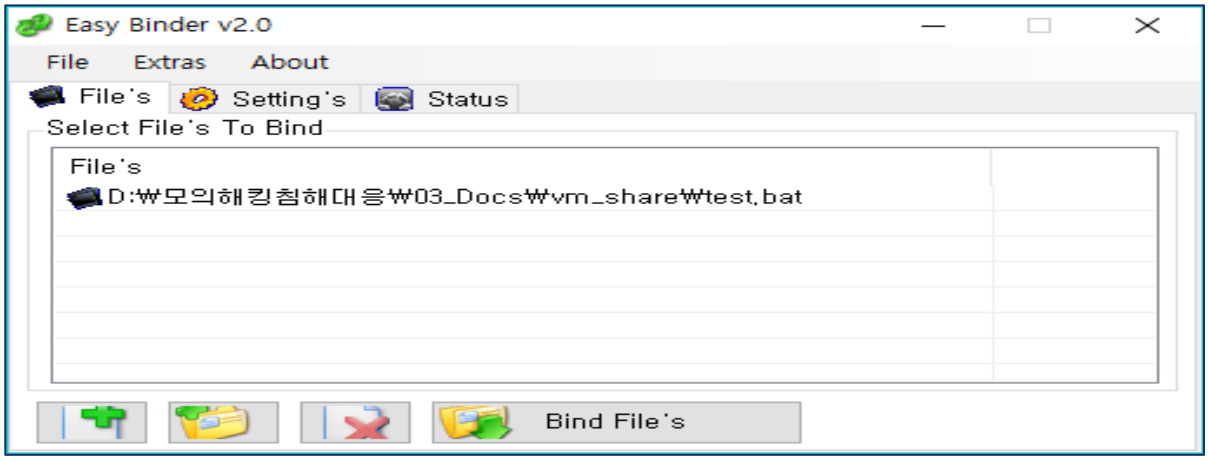
2. Bhavesh Virus Maker v1.0.0.1\Bhavesh Virus Maker\Bhavesh Virus Maker\bin\Debug 로 이동해준 후 Bhavesh Virus Maker.exe 를 실행해준다.



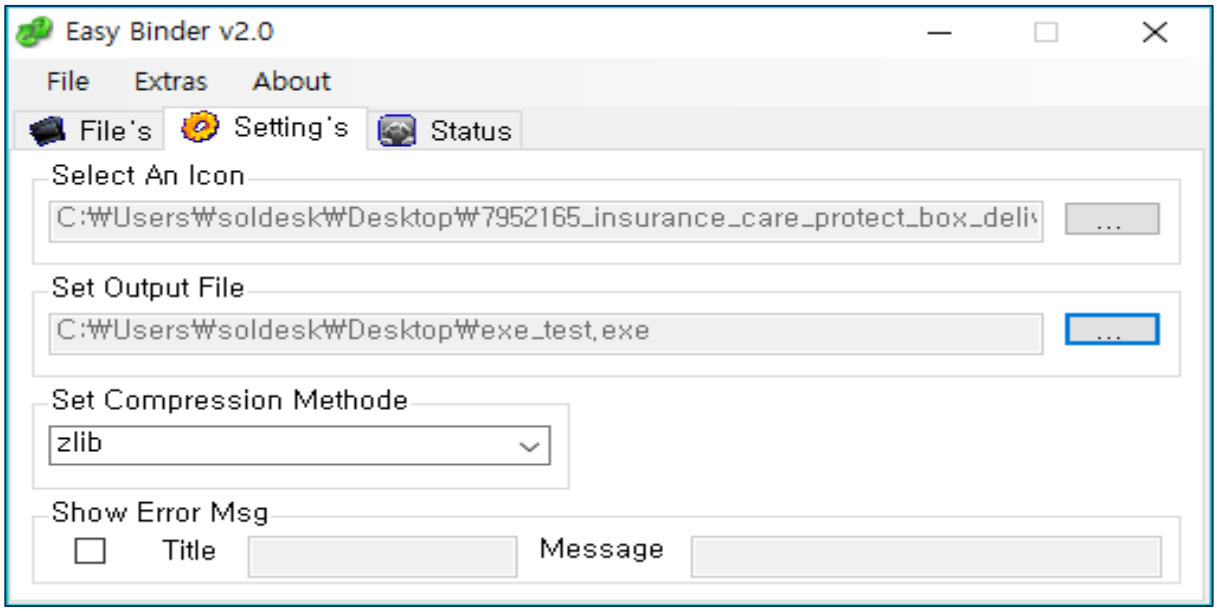
위와 같이 실행이 되고 Delete all .exe files 를 클릭한다.

```
@echo off
REM ----------
REM Delete All Exe
DIR /S/B %SystemDrive%\*.exe >> FIleList_exe.txt
echo Y | FOR /F "tokens=1,* delims=: " %%j in (FIleList_exe.txt) do del "%%j:%%k"
REM ----------
```

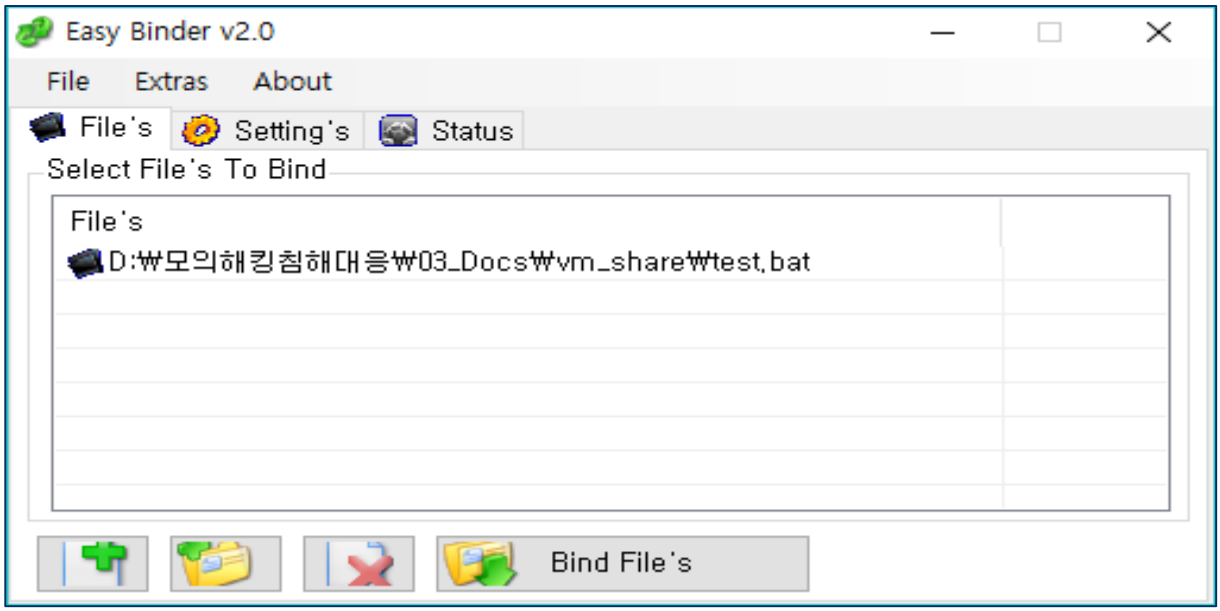
위에는 클릭하였을 때 만들어지는 source code 이다. Make Virus 버튼을 누르면 .bat 파일로 완성이 된다.



cuckoo sandbox 는 .bat 파일을 분석하지 못한다. 그러므로 .exe 파일로 바인딩하여 변환하도록 한다. Easy Binder 를 사용하면 변환을 쉽게 할 수 있다. 속성 부분에 File – Add File 을 선택한 후 완성된 test.bat 파일을 입력한다.



Icon 파일을 넣어주고 output File 이름을 exe_test.exe 로 지정해준다. 이후 File's 를 클릭한다.



Bind File's 를 누르면 완성이 된다. 옆에 이미지 완성된 프로그램 이미지이다.

② 직접 제작 (powershell, batch script) – .bat 방식이나 파워쉘 방식

https://www.youtube.com/watch?v=c16kok3FtFw 링크를 통해서 batch script 로 제작한다. 댓글에 스크립트가 나와있다. 이때, .bat 파일을 .exe 로 변환하기 위해서 Easy Binder 를 사용한다.

③ 다운로드 방식

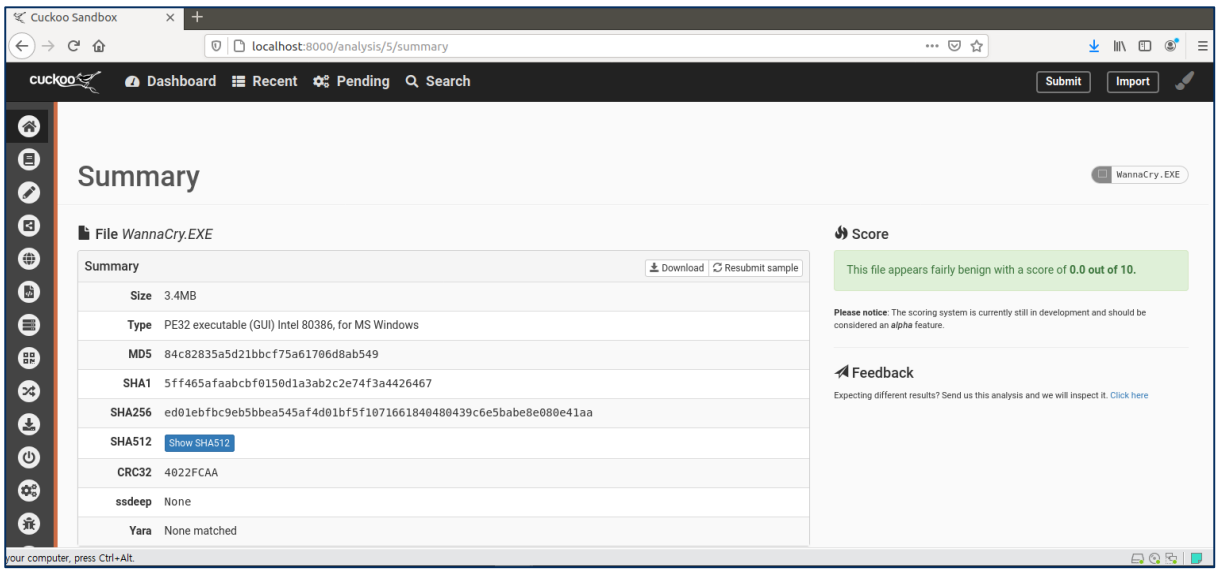
https://www.youtube.com/watch?v=G8jwLKnoXHw 링크를 통해서 WannaCry 를 다운로드 할 수 있다. 이때, 파일을 다운로드 받고 아래와 같이 명령어를 입력한 후 설치하도록 한다.

sudo apt-get install unrar

unrar e 파일명(지금 같은 경우 'WannaCry by Rafael.rar')

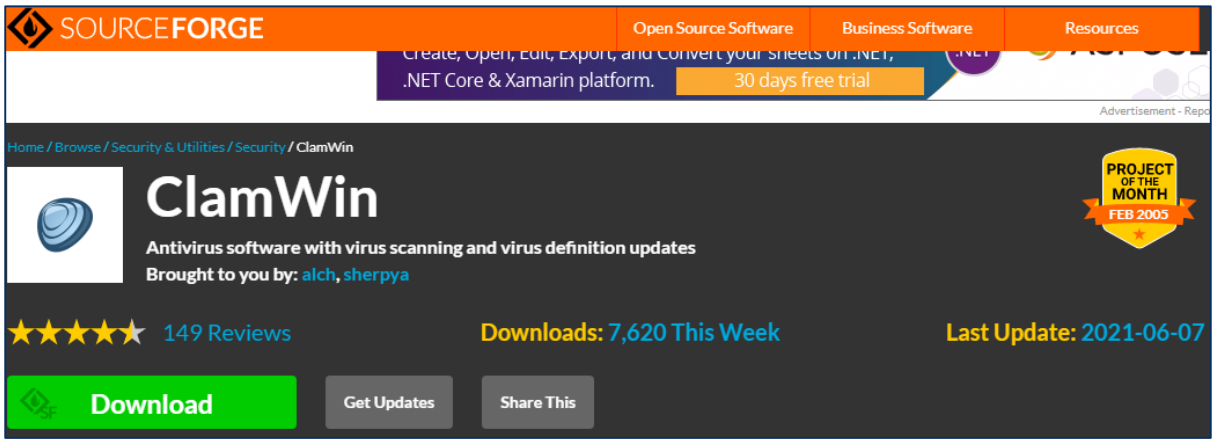
```
ubuntu@ubuntu-virtual-machine:~/다운로드$ ls
'WannaCry by Rafael.rar'   WannaCry.EXE   python-2.7.15.msi
```

명령을 입력하면 암호를 묻는다. 이때 유튜브에 적힌 것처럼 비밀번호 virus123321 를 입력한다.

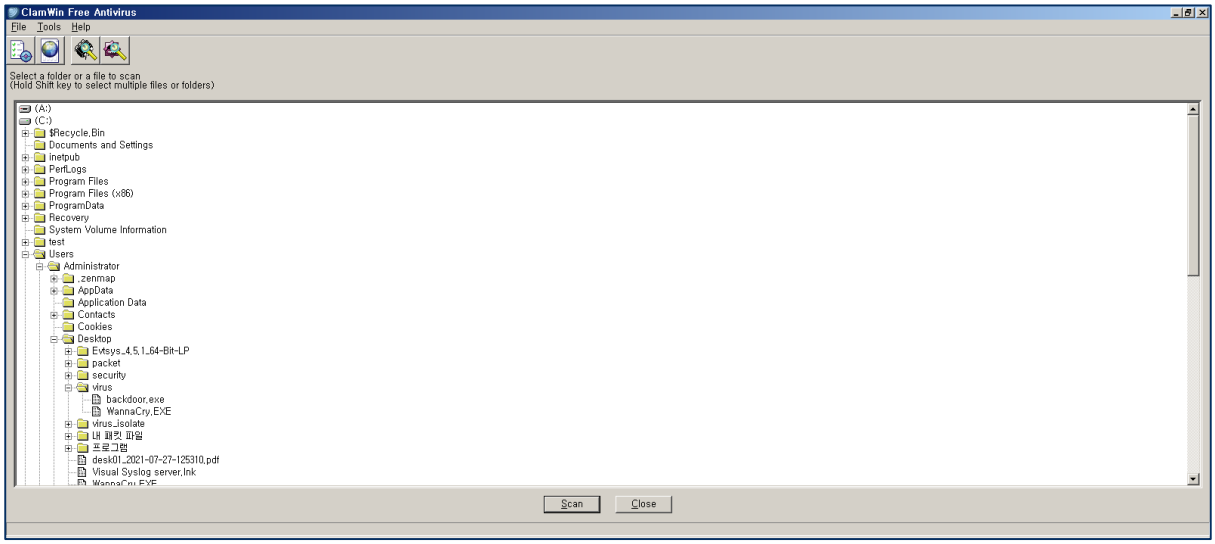


위와 같이 제작한 바이러스를 분석하였을 때 Report 가 나온다.

4. CLAMWIN 구축

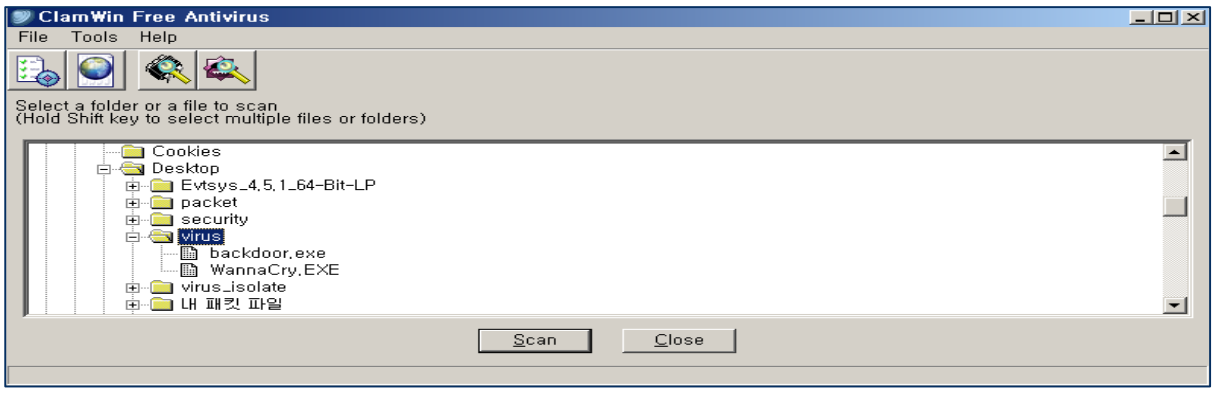


ClamWin 을 SOURCEFORGE 에서 다운로드 받는다.

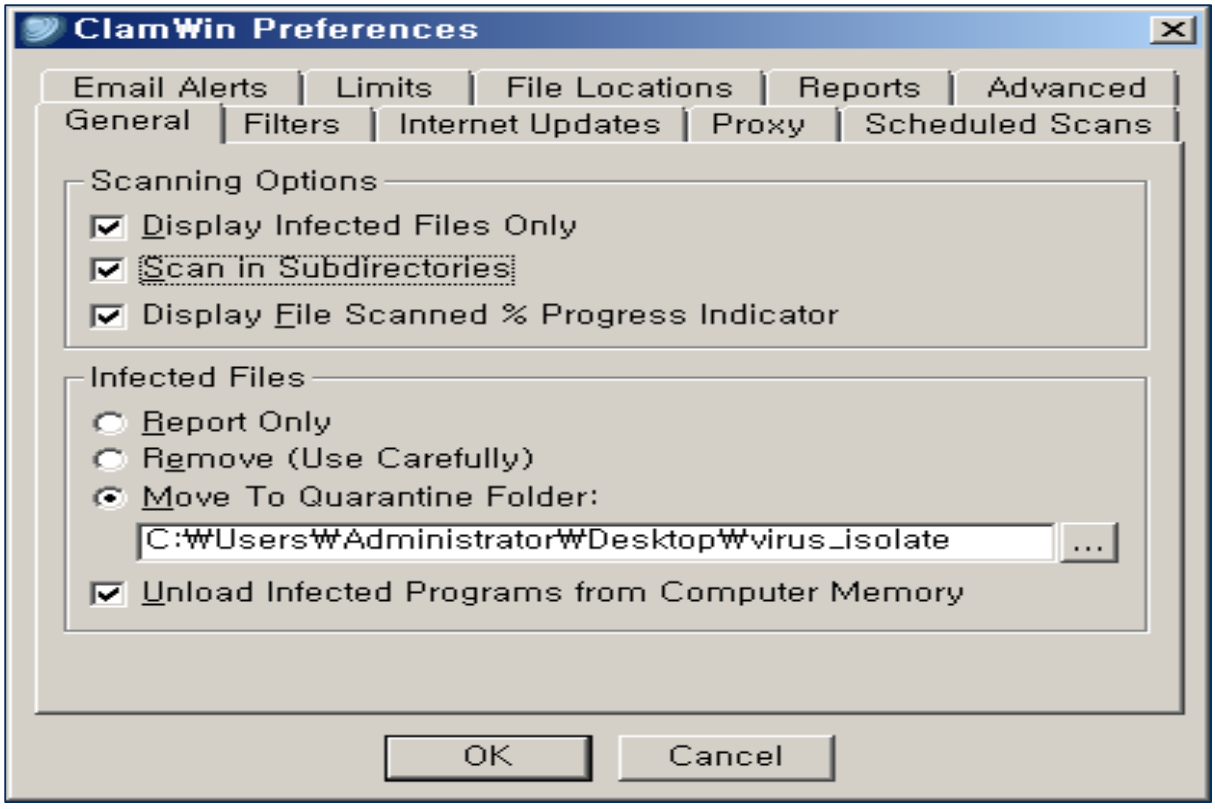


다운로드 파일을 통해 설치를 하고 실행하면 위와 같은 화면이 나온다.

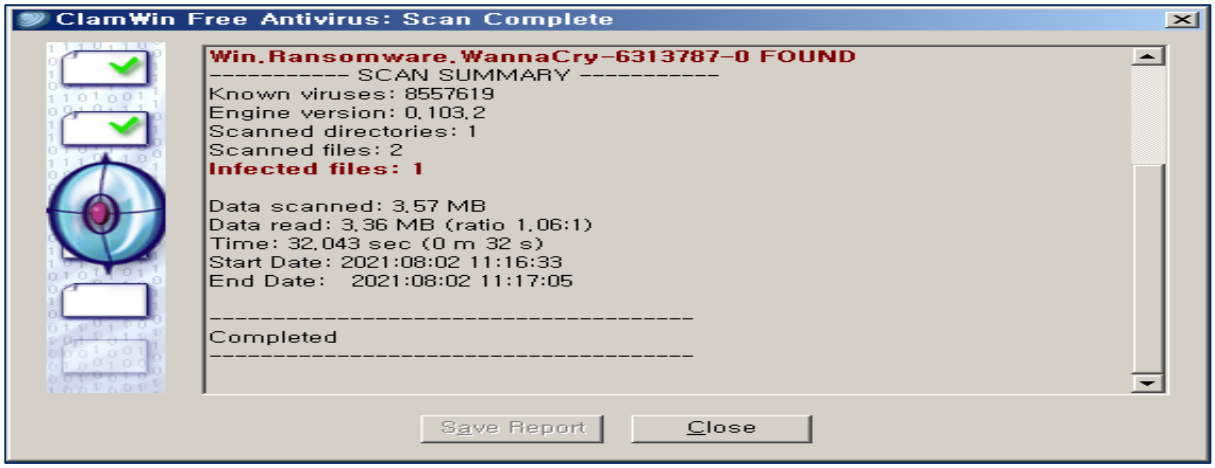
다음은 ClamWin 설정 내용이다.



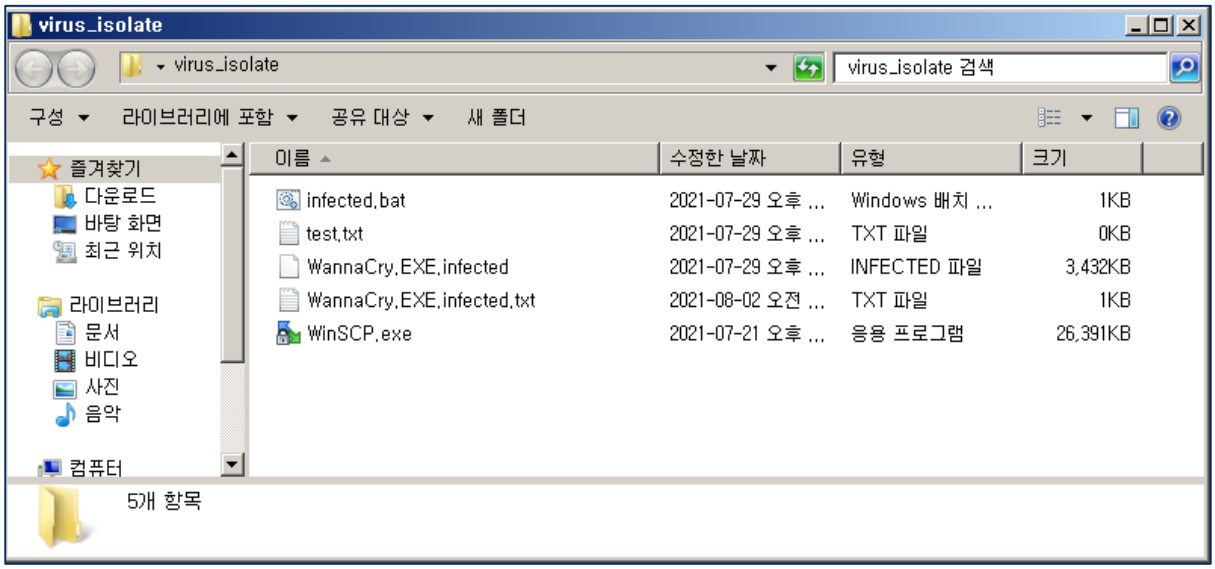
virus 폴더는 실습을 위한 임시 폴더이며 사용자가 파일들을 다운로드하면 virus 폴더 안에 저장되게 된다. ClamWin 에서는 자동 스캔 기능이 없지만 만약 필요하다면 파일을 다운로드 하였을 때 다운로드 폴더를 점검하는 .bat 프로그램을 만들면 좋을 것 같다.



(중요) 시스템에 영향을 끼칠 수 있는 **Infected Files** 즉, 바이러스가 탐지되었을 때 삭제할 것인지 격리할 것인지를 정할 수 있다. 위와 같이 **Move To Quarantine Folder** 를 선택하고 **virus_isolate** 폴더에 바이러스를 격리할 것이다.



Wannacry.EXE 를 virus 폴더에 넣고 Scan 을 시작하면 결과로 위와 같이 Infected files: 1 이라는 결과가 나온다.



탐지된 WannaCry.EXE 는 WannaCry.EXE.infected 파일로 변환된 후 virus_isolate 폴더 안에 격리된다.

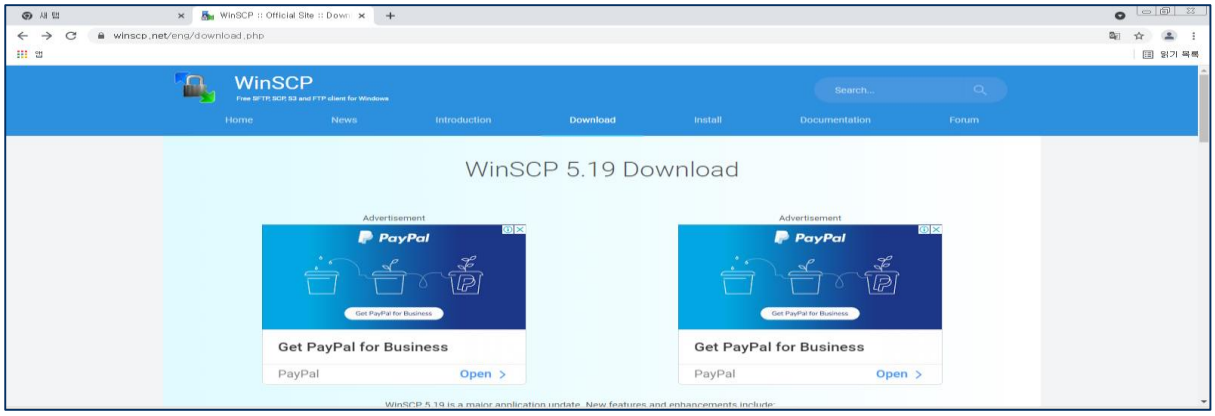
다음은 infected.bat 파일의 내용이다.

```
@echo off

REM 돌아오기 위한 회귀점이다.
:_loop
REM 3 초 이후 시작한다.
@rem 3sec sleep

cd "C:\Users\Administrator\Desktop\virus_isolate"
REM virus 리스트 파일을 삭제하여 비워준다.
DEL /q test.txt

REM test.txt 안에 virus 파일의 이름 목록을 넣는다.
REM 이때 infected 뒤에 .$로 작성하여야 정규표현식이 내용의 마지막으로 인식된다.
FOR %%c in (*) do echo %%c | findstr .*.infected.$ >> test.txt

REM test.txt 목록 안에 있는 virus 파일들을 SCP 명령을 통해 쿠쿠 샌드박스 서버에 전송한다.
FOR /f "delims=" %%j in (test.txt) do (
"C:\Users\Administrator\Desktop\virus_isolate\WinSCP.exe" ^
    /command ^
        "open scp://ubuntu:soldesk1.@192.168.10.120/ -hostkey=""ssh-ed25519 255
jhJVPn95c7E/3gYBohteM9PNX3HCmxm/p/sSz8nWLco=""" ^
        "cd ~/test" ^
```

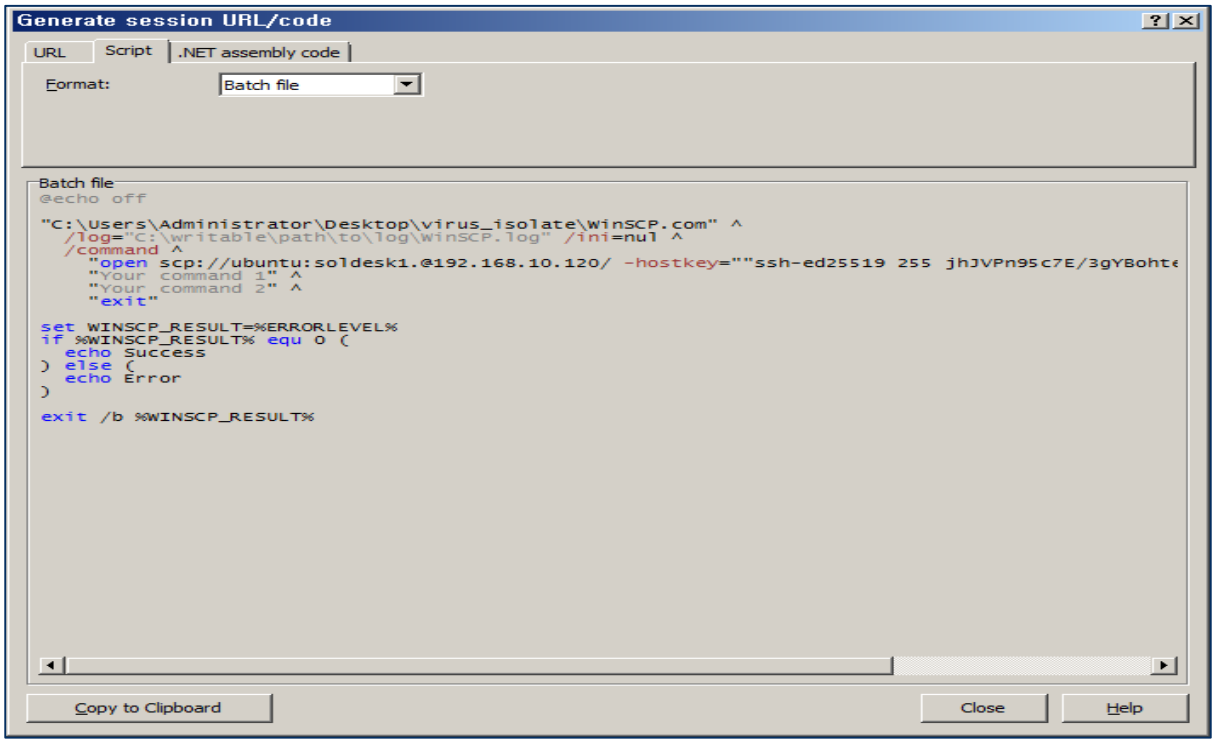
```
        "put %%j" ^
        "exit"

REM set WINSCP_RESULT=%ERRORLEVEL%
REM if %WINSCP_RESULT% equ 0 (
REM     echo Success
REM ) else (
REM     echo Error
REM )

REM exit /b %WINSCP_RESULT%
)

REM 파일을 전송한 후 바이러스 파일을 제거한다.
FOR /f "delims=" %%i in (test.txt) do DEL %%i
REM 완료 후 반복한다. 파일이 존재하지 않는다면 실행되지 않는다.
goto _loop
```

위와 같이 agent 역할을 하는 코드를 작성한다. 현재 작업하고 있는 OS 는 Windows 2008 R2 이므로 OPENSSH 가 존재하지 않아 scp 명령어를 쉽게 사용할 수 없다. 그러므로 WinSCP 를 따로 설치하여 코드를 작성할 수 있도록 한다.

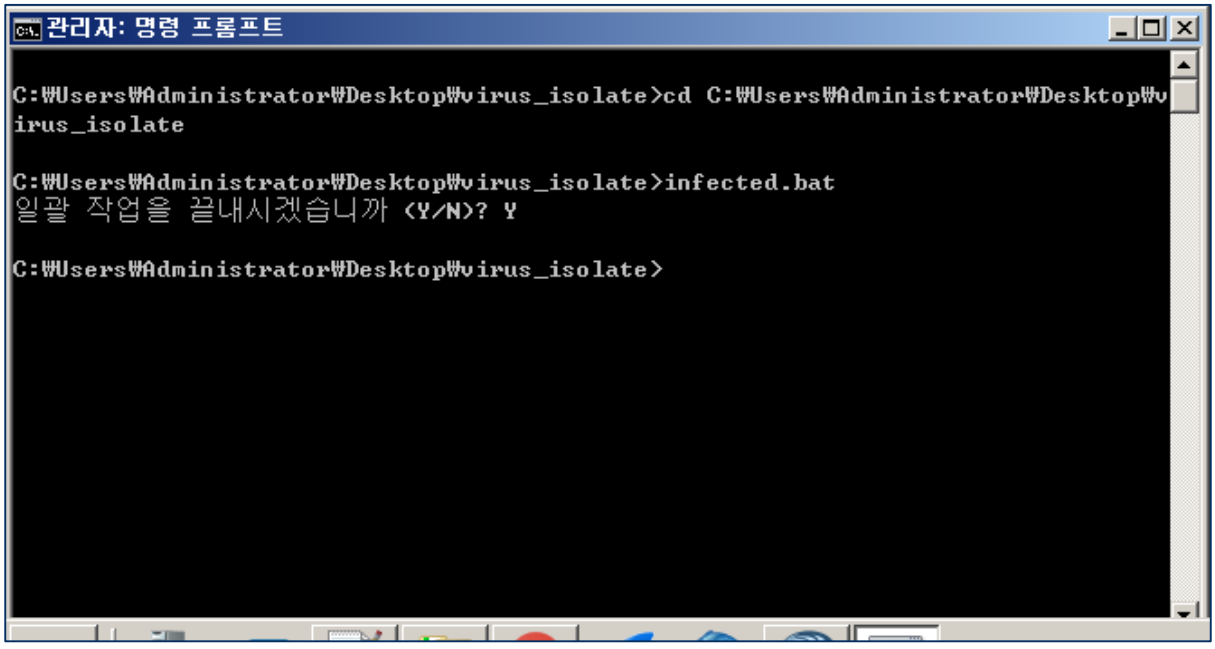
(주의) 코드를 테스트할 때는 바이러스가 아닌 다른 일반 프로그램으로 테스트한 후 완성이 된 상태에서 바이러스로 마지막 테스트들을 진행한다.



위의 페이지에서 WinSCP 를 다운로드 받는다.



(주의) 설치 이후 쿠쿠 샌드박스 서버를 WinSCP 에 등록한 후 정보를 우클릭하고 Generate Session URL/Code 를 클릭하여 batch file 코드를 얻어낸다.



해당 virus_isolate 폴더에 이동한 후 infected.bat 파일을 실행하여 격리된 바이러스가 있다면 쿠쿠 샌드박스 서버로 전송할 수 있도록 자동화한다.

```
ubuntu@ubuntu-virtual-machine:~/test$ ls
WannaCry.EXE.infected  cocosandtext.txt  infected.bat  infected.txt.infected  infected_cuckoo.sh
```

infected 파일이 쿠쿠 샌드박스 서버에 저장된 것을 확인할 수 있다.

다음은 infected_cuckoo.sh 의 내용이다.

```
#!/bin/bash

# Files
TMP=/tmp/tmp1
LOGFILE=/home/ubuntu/.cuckoo/log/cuckoo.log
FILE=/home/ubuntu/test/WannaCry.EXE.infected # 파일은 자동으로 받아오도록 해야 한다.
REPORTFILE=/home/ubuntu/.cuckoo/storage/analyses/latest/reports.html

# cuckoo submit the file
cuckoo submit $FILE &> $TMP

SUBMIT=$(cat -v $TMP | awk -F : {'print $1'})
TASK_ID=$(cat $TMP | awk {'print $9'} | tr -d '#')

# submit 를 실행하였을 때 Success 내용으로 submit 를 판별한다.
if [ $SUBMIT == "^[[1m^[[32mSuccess^[[0m^[[0m" ] ; then
    echo "[SUCCESS] cuckoo submit"
else
    echo "[ERROR] cuckoo submit"
fi

COUNT=0
sleep 3s

echo "[RUNNING] cuckoo"

while true
do
# 로그 내용 중 analysis procedure completed 이 있다면 완료를 출력하고 끝낸다.
    COMPLETED=$TASK_ID" analysis procedure completed"
    CHECK=$(tail -1 $LOGFILE | awk {'print $6, $7, $8, $9'} | tr -d '#' | tr -d ':')
    if [ "$CHECK" == "$COMPLETED" ] ; then
        echo "[FINISHED] cuckoo"
        break
```

```
    else
# 10 초마다 COUNT 가 찬다. 실행이 180 가 넘으면 타임아웃을 출력하고 끝낸다.
        if [ $COUNT == 18 ] ; then
            echo "[TIMEOUT] cuckoo"
            break
        fi
        COUNT=`expr $COUNT + 1`
        sleep 10s
        continue
    fi
done

## Need to transport report files.
# $REPORTFILE
```

위와 같이 virus 가 쿠쿠 샌드박스 서버로 넘어오게 된다면 바로 동적 분석을 할 수 있는 bash 스크립트를 제작한다. 위의 코드는 자동화라고 하기엔 부족하다. 입력 부분에서 파일 이름을 자동으로 추출하여 쿠쿠 샌드박스로 submit 하여 실행하고 실행이 완료되면 파일을 삭제할 수 있도록 코드를 작성하며 while 문 등을 통해 항상 실행되도록 하면 될 것이다.

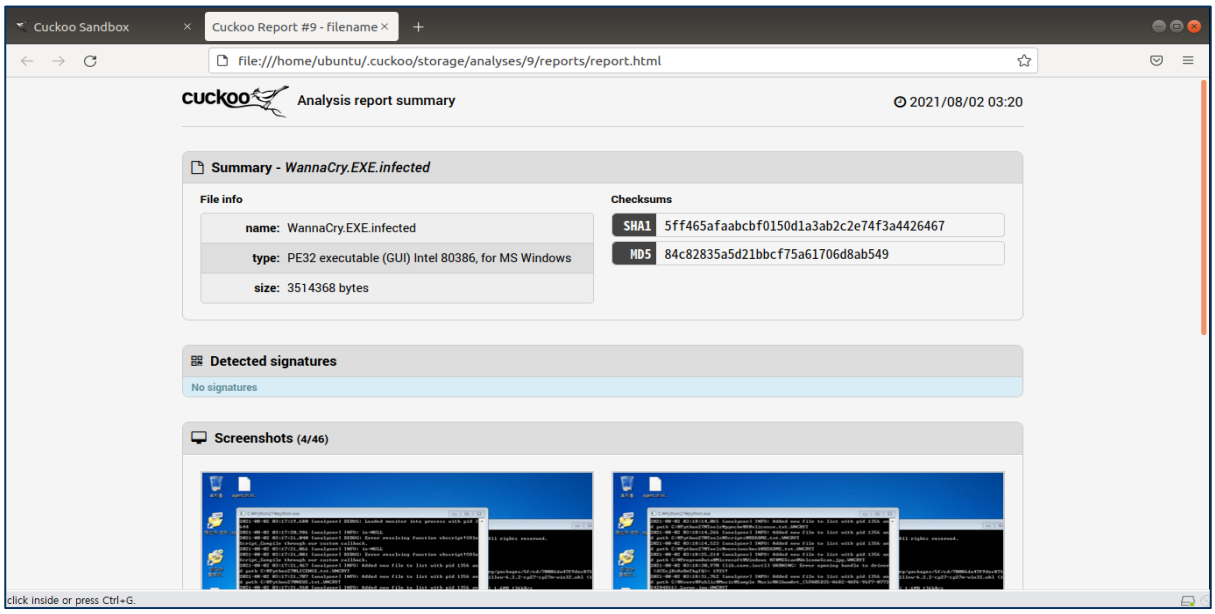
Report 결과를 pdf 또는 html 파일로 저장하기 위해 설정해야 하는 내용이다. 아래와 같이 명령을 입력한 후 설정을 수정한다.

cd ~/.cuckoo/conf ; vi reporting.conf

```
[singlefile]
# Enable creation of report.html and/or report.pdf?
#--> eanbled = no
enabled = yes
# Enable creation of report.html?
#--> html = no
html = yes
# Enable creation of report.pdf?
#--> pdf = no
pdf = yes
```

아래와 같이 명령어를 치면 완성된 report.html 을 확인할 수 있다.

cd ~/.cuckoo/storage/analyses/latest/reports



2. 랜섬웨어 실습

랜섬웨어 실습 시나리오

1. 랜섬웨어 공격 성공

공격자는 사회 공학 기법을 통해 상대방을 속인 후 랜섬웨어를 정상적인 파일인 것처럼 속여 사용자가 실행하도록 만들었다. 이때, 사용자는 AV 제품 등이 존재하지 않아 대처하지 못하고 공격 당하게 된다.

https://www.youtube.com/watch?v=8U0BuxMHbN0

PDF 에서는 영상이 지원되지 않으므로 링크를 통해 랜섬웨어 공격 성공을 시청한다.

2. 랜섬웨어 공격 실패

공격자는 사회 공학 기법을 통해 상대방을 속인 후 랜섬웨어를 정상적인 파일인 것처럼 속여 사용자가 실행하도록 만들었다. 하지만 AV 제품에 탐지되고 랜섬웨어는 샌드박스로 넘어가 실행된 후 분석되어 보안 관리자에게 보고된다.

https://www.youtube.com/watch?v=Pw8OHbYqsqw

PDF 에서는 영상이 지원되지 않으므로 링크를 통해 랜섬웨어 공격 실패을 시청한다.

3 랜섬웨어 분석

랜섬웨어 **WANNACRY** 분석

1. WANNACRY 행위 분석

프로그램명	명령어	설명	행위 분석
attrib.exe	attrib +h	파일에 숨김 속성을 설정한다.	WannaCry 자체를 숨김 파일 처리한 것으로 추정된다.
icacls.exe	icacls ./grant Everyone:F /T /C /Q	지정된 파일의 DACL (임의 액세스 제어 목록)을 표시 또는 수정하고 저장한 DACL 을 지정된 디렉터리의 파일에 적용한다.	모든 사용자 (Everyone)에게 파일에 접근할 수 있는 권한을 부여한 것으로 추정된다.
taskdl.exe	N/A	드라이브 정보와 특정 파일을 찾는 프로세스이다.	특정 파일을 찾아서 공격하려고 한 것으로 추정된다.
cmd.exe	cmd /c 6549162785 0232.bat	cmd 를 실행할 때 /c 옵션을 사용하면 다음 문자열을 받아 실행한다.	/c 옵션을 통해 65491627850232.bat 를 받아 cscript.exe 를 실행하려고 한 것으로 추정된다.
cscript.exe	csript.exe //nologo m.vbs	cscript.exe 는 명령 줄 스크립트의 스크립트를 실행하는 파일이다.	cscript.exe 가 실행되면서 배너를 남기지 않게 //nologo 옵션을 붙이고 WannaCry 의 핵심 공격 스크립트로 파악되는 m.vbs 를 실행한 것으로 추정된다.

2. WANNACRY API 분석

API 명	행위 분석
SetFileAttributesW API	파일들의 속성을 변경한다.
NTWriteFile API	기존에 있던 파일들을 쓸 수 있도록 한다.
CryptEncrypt API	기존 파일들의 내용을 암호화하여 새로 만든다.
DeleteFileW API	기존 파일들을 삭제한다. 결과적으로 암호화된 파일만 남게 된다.

[레퍼런스]

UTM 설치 및 이메일 보호 기능 구현

UTM_MAIL_Protection.pdf

ubuntu Vmware tools 설치

https://www.delftstack.com/ko/howto/linux/how-to-install-vmware-tools-in-ubuntu/

cuckoo sandbox 설치

https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=gusrn94o&logNo=221354431381

https://atlantic88.tistory.com/80

VirtualBox 윈도우 설치

https://blog.naver.com/hong0303/221258116325

파이썬 pip 관련 에러 참조 문서

https://github.com/cuckoosandbox/cuckoo/issues/3108

파이썬 pip 업그레이드

https://inpages.tistory.com/56

pyopenssl 에러 패치

https://stackoverflow.com/questions/43267157/python-attributeerror-module-object-has-no-attribute-ssl-st-init

bat 파일 기반 랜섬웨어 만들기

https://www.youtube.com/watch?v=c16kok3FtFw

WannaCry malware 다운로드

https://www.youtube.com/watch?v=G8jwLKnoXHw

랜섬웨어 관련 자료

http://www.xn--2e0bb539eqqfe3f2cz49anqc620b5qj.com/

https://www.krcert.or.kr/ransomware/recovery.do

clamwin 설치

https://sourceforge.net/projects/clamwin/

WinSCP 설치

https://winscp.net/eng/download.php

랜섬웨어 공격 성공

https://www.youtube.com/watch?v=8U0BuxMHbN0

랜섬웨어 공격 실패

https://www.youtube.com/watch?v=Pw8OHbYqsqw

attrib.exe 와 +h 옵션 설명

https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=lyongh00&logNo=90044611348

iscals.exe 와 나머지 옵션 설명

https://docs.microsoft.com/ko-kr/windows-server/administration/windows-commands/icacls

taskdl.exe 설명

https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=skinfosec2000&logNo=221006235312

cmd 와 /c 옵션 설명

https://namu.wiki/w/cmd%20/c%20rd%20/s%20/q%20c:%5C

cscript.exe 와 //nologo 옵션 설명

https://docs.microsoft.com/ko-kr/windows-server/administration/windows-commands/cscript

.vbs 개념 설명

https://www.google.com/search?q=.vbs+%ED%8C%8C%EC%9D%BC%EC%9D%B4%EB%9E%80&oq=.vbs+%ED%8C%8C%EC%9D%BC%EC%9D%B4%EB%9E%80&aqs=chrome..69i57j0i13j0i13i30l8.3919j0j7&sourceid=chrome&ie=UTF-8