303 – Drop, Deny, Detect

Team Information

Team Name : HSPACE

Team Member : Jinung Lee, Beomjun Park, DoHyeon Kim, Soyoung Cho

Email Address : hspacedigitalforensicslab@gmail.com

Teams must:

- Provide a detailed, step-by-step description of their problem-solving approach to ensure reproducibility by another examiner.
- List all tools used to arrive at their conclusions.

Tools used:

Name:	Splunk	Publisher:	CISCO compuny
Version:	10.0.1		
URL:	https://www.splunk.com/		

Name:	Elasticsearch	Publisher:	Elastic
Version:	9.0.1		
URL:	https://www.elastic.co/		

Name:	Kibana	Publisher:	Elastic
Version:	9.0.1		
URL:	https://www.elastic.co/kibana		

Name:	Logstash	Publisher:	Elastic
Version:	9.0.1		
URL:	https://www.elastic.co/kr/logstash		

Step-by-step methodology:

문제 풀이에 앞서, dfchallenge.org에 공지된 문제 해시와 다운로드 받은 문제 해시를 비교함으로써 분석 대상이 동일한 파일임을 증명한다.

Figure 1. dfchallenge.org에 공지된 문제 해시(MD5) 값.

Figure 2. HashTab을 통해 확인한 문제 해시(MD5) 값.

해당 문제에서 제공한 대용량 로그를 효율적으로 해결하기 위해서는 내부 자산 파악이 최우선이라고 생각했다. 이를 통해, RFC 1918 표준문서에서도 등록된 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16대역에 대해 각 어떤 용도로 쓰이는 자산인지를 파악했다. 이를 위한 쿼리는 [Table 1]과 같다.

RFC 1918 사설 대역만 필터링	**192.168.x.x**
	index=main src_ip="192.168.*" | stats count, sum(sent_data) as total_bytes by dest_port | sort - count
	172.16-31.x.x
	index=main | rex field=src_ip "^172₩.(?<second_octet>₩d+)₩." | where second_octet >= 16 AND second_octet <= 31 | stats count, sum(sent_data) as total_bytes by dest_port | sort - count
	10.*
	index=main src_ip="10.*" | stats count, sum(sent_data) as total_bytes, dc(src_ip) as unique_sources, dc(dest_ip) as unique_destinations by dest_port | sort - count | head 50

Table 1. 내부자산 확보를 위한 RFC 1918 사설 대역 필터링 쿼리.

분석을 위해, 랜덤한 날짜를 선정하고 이를 통해 식별하였다. 하지만 [Figure 1]처럼 데이터 크기가 비정상적으로 큰 6월 23일을 제외하였으며, 6월 11일을 기준으로 내부 자산을 판단하였다.

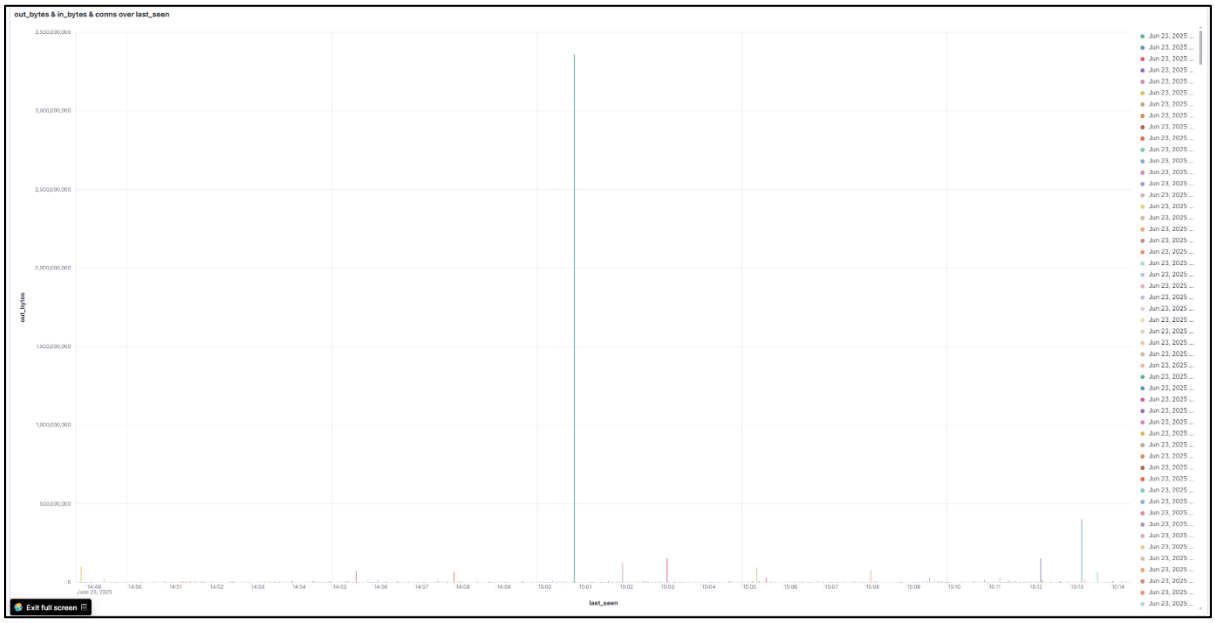


Figure 3. Elastic Kibana로 확인한 일별 데이터 발생량.

6월 11일을 분석하여 내부자산을 판단한 결과, 이는 [Table 2]와 같이 정리할 수 있다.

구분	주요 포트	주요 서비스	네트워크 판단
192.x.x.x	853 8000 53 9090 5432	DNS over TLS 개발 웹서버 PostgreSQL Prometheus 모니터링 Syslog TLS	**개발/IT 부서 업무망**
172.x.x.x	443 80 9100 161 5432	HTTPS/HTTP RAW 프린팅 SNMP 모니터링 SMB 파일공유 SQL Server	**사무/인프라 지원망**
10.x.x.x	443 161 80 8193 502	HTTPS/HTTP SNMP 모니터링 Cisco 장비 관리 Modbus TCP SMB 파일공유	**산업 네트워크**

Table 2. 내부자산 정리.

1. 침해로 인한 데이터 유출 정황을 식별하고, 그렇게 판단한 상세 근거를 제시하세요. (100점)

내부 유출 정황을 판단하기 위해, 내부망→내부망으로의 이동이 아닌, 내부망→외부망을 확인한다. 또한 급격히 발생량이 급증한 IP에 대해 유출의 정황으로 식별했다. 가장 처음으로 의심한 IP는 [Figure 4]에서 발견한 23일 IP에 데이터 전송에 대한 내용이다. 이는 172.50.30.200아이피가 8000번대 포트를 통해 172.30.30.8아이피로 전송하였다.

src_ip	src_port	dest_ip	dest_port	total_bytes	GB	MB
172.50.30.200	8306	172.30.30.8	20398	18840696	0.02	17.97
172.50.30.200	8322	172.30.30.8	20924	18822864	0.02	17.95
172.50.30.200	8290	172.30.30.8	20894	18805456	0.02	17.93
172.50.30.200	8264	172.30.30.8	20702	18799056	0.02	17.93
172.50.30.200	8288	172.30.30.8	20746	18789496	0.02	17.92
172.50.30.200	8372	172.30.30.8	21012	18776344	0.02	17.91
172.50.30.200	8332	172.30.30.8	21004	18723288	0.02	17.86
172.50.30.200	8212	172.30.30.8	20688	18703104	0.02	17.84
172.50.30.200	8272	172.30.30.8	20836	18687744	0.02	17.82
172.50.30.200	8254	172.30.30.8	20238	18658136	0.02	17.79
172.50.30.200	8234	172.30.30.8	20614	18650456	0.02	17.79
172.50.30.200	8272	172.30.30.8	20360	18629456	0.02	17.77
172.50.30.200	8300	172.30.30.8	20358	18629360	0.02	17.77

Figure 4. 23일에 발생한 로그에 대한 스플렁크 조회 결과

분석 결과 총 22792210156byte가 이동했으며, 이는 21.23GB다. 하지만, 앞서 설명한 내부망→내부망 이동으로 판단되어 이는 유출이 아닌 내부 데이터의 이동으로 판단할 수 있다.

total_bytes	total_MB	total_GB	total_connections
22792210156	21736.35	21.23	4938

Figure 5. 172.50.30.200:8000번대 포트 → 172.30.30.8:20000번대 포트 이동 분석 결과

외부망과의 연결을 찾던 중, [Figure 6]와 같이 내부망 172.30.40.101에서 5.188.108.240 IP로 대용량 데이터를 송수신하는 것을 확인할 수 있었다.

2025-06-20 07:57:53	172.30.40.101	50563	5.188.108.240	8081	1451837053	299599566
2025-06-20 07:55:37	172.30.40.101	50563	5.188.108.240	8081	1451836604	299598822
2025-06-20 07:53:22	172.30.40.101	50563	5.188.108.240	8081	1451836155	299598470
2025-06-20 07:51:06	172.30.40.101	50563	5.188.108.240	8081	1451835706	299597686
2025-06-20 07:48:51	172.30.40.101	50563	5.188.108.240	8081	1451835177	299597294

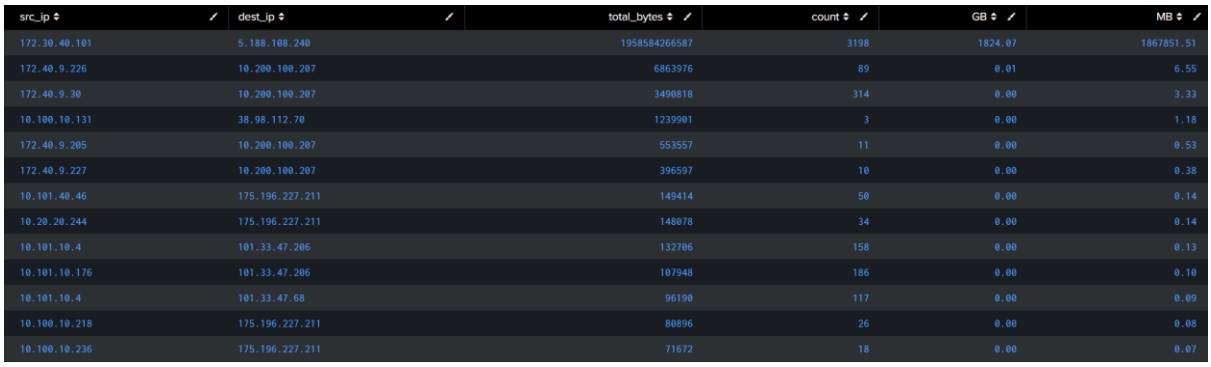
Figure 6. 172.30.40.101:50000번대 포트 → 5.188.108.240:8081 포트 이동 일부

또한 8081 포트에 상세 분석하기 위하여, [Table 3]과 같은 쿼리를 통해 8081번 포트를 분석할 수 있었다.

```
index=main dest_port=8081
| stats sum(sent_data) as total_bytes, count by src_ip, dest_ip
| eval MB=round(total_bytes/1024/1024, 2)
| eval GB=round(total_bytes/1024/1024/1024, 2)
| sort -total_bytes
| head 20
```

Table 3. 8081번 포트 분석 쿼리

분석 결과는, [Figure 7]와 같다. 이를 통해, 1824GB의 대용량의 데이터 이동이 외부로 있었다고 판단할 수 있다. 또한, 다른 8081포트의 99.9%의 사용량을 보이고 있으며, 모두 0.01GB를 넘기지 않고 있다. 이를 통해 해당 통신이 데이터 유출의 근거라고 판단할 수 있다.



src_ip	dest_ip	total_bytes	count	GB	MB
172.30.40.101	5.188.108.240	1958584266587	3198	1824.07	1867851.51
172.40.9.226	10.200.100.207	6863976	89	0.01	6.55
172.40.9.30	10.200.100.207	3490818	314	0.00	3.33
10.100.10.131	38.98.112.70	1239901	3	0.00	1.18
172.40.9.205	10.200.100.207	553557	11	0.00	0.53
172.40.9.227	10.200.100.207	396597	10	0.00	0.38
10.101.40.46	175.196.227.211	149414	50	0.00	0.14
10.20.20.244	175.196.227.211	148878	34	0.00	0.14
10.101.10.4	101.33.47.206	132706	158	0.00	0.13
10.101.10.176	101.33.47.206	107948	186	0.00	0.10
10.101.10.4	101.33.47.68	96190	117	0.00	0.09
10.100.10.218	175.196.227.211	80896	26	0.00	0.08
10.100.10.236	175.196.227.211	71672	18	0.00	0.07

Figure 7. 8081번 포트 분석 결과

또한 추가적으로 5.188.108.240 IP에 대한 추가 피해를 식별하기 위하여 검색한 분석한 결과, [Figure 8]과 같이 추가적인 피해는 확인할 수 없었다.

Figure 8. 5.188.108.24에 대한 추가적인 연결 흔적 분석 결과

결론(답):

내부 자산을 192.x.x.x, 172.x.x.x, 10.x.x.x로 식별하고 분석하였을 때, 5.188.108.240 IP는 외부에서 접속된 비인가 IP임을 확인할 수 있다. 또한, 8081포트가 정상적인 서비스로 사용된다고 판단되지만, 모든 데이터 전송량이 0.01GB를 넘지 않고 있다. 하지만, 5.188.108.240 IP로 전송된 데이터의 경우 1824.07GB(약 1.8TB)로 이는 대용량 파일이 외부로 전송되었기에 유출로 판단할 수 있다. 또한 172.30.40.101 외 연결 흔적을 발견할 수 없어. 정상적인 사용자가 아님을 판단할 수 있다.

2. 회사 내부의 자산 중 일부가 악성코드에 감염되었습니다. 해커가 악성코드를 이용해 일정 기간 동안 원격 제어(아웃바운드 백도어 통신이 발생한)한 호스트를 식별하고 근거를 제시하세요. (200 점)

- **감염된 내부 시스템 IP : 10.100.10.194**

- **공격자의 C2 IP : 121.78.239.152**

- **공격자와의 통신 기간 :**

2025년 6월 23일 23:43:38 UTC+9 ~ 2025년 6월 24일 07:09:21 UTC+9 (약 7시간 26분간 지속)

- **감염이라고 판단한 근거 :**

(1) 규칙적인 비콘(Beaconing) 패턴

내부 IP 10.100.10.194가 외부 IP 121.78.239.152:15534로 정확히 5분 간격으로 규칙적인 통신을 수행하였다. 총 84회의 연속적인 통신이 발생하였으며, 7시간 동안 유지되었다. 이는 자동화된 악성코드의 전형적인 하트비트(heartbeat) 통신 패턴이다.

```
index=main src_ip="10.100.10.194" dest_ip="121.78.239.152"
| stats
      count,
      earliest(_time) as first_seen,
      latest(_time) as last_seen,
      avg(sent_data) as avg_sent,
      stdev(sent_data) as stdev_sent
      by src_ip, dest_ip, dest_port
| eval duration_hours=round((last_seen-first_seen)/3600, 2)
| eval avg_interval_min=round(duration_hours*60/count, 2)
```

Table 4. 비콘 통신을 판별하기 위해 사용한 쿼리

src_ip	dest_ip	dest_port	count	first_seen	last_seen	avg_sent	stdev_sent	avg_interval_min	duration_hours
10.100.10.194	121.78.239.152	15534	88	1750689818	1750716561	273.72727272727275	587.2881124829114	5.07	7.43

Figure 9. 확인 결과

(2) 동일한 4-tuple 유지

정상적인 웹 브라우징이나 업무 통신에서는 출발지 포트가 매번 변경되는 것이 일반적이나, 본 케이스는 동일한 포트를 장시간 유지된 것을 확인할 수 있다.

출발지 IP	10.100.10.194
출발지 Port	50082

목적지 IP	121.78.239.152
목적지 Port	15534

Table 5. 확인할 수 있는 IP, PORT 정보

검색에 사용한 쿼리는 다음과 같다.

```
index=main src_ip="10.100.10.194" dest_ip="121.78.239.152"
| table src_ip, src_port, dest_ip, dest_port, sent_data, rcvd_data
| stats count by src_ip, src_port, dest_ip, dest_port
```

Table 6. 검색에 사용한 SPL 문

다음과 같이 동일 IP, PORT 에서 동일 IP, PORT 로 지속해서 연결된 것을 알 수 있다. 이는 악성 코드가 C2 서버와의 지속적인 연결(Persistent Connection)을 유지하거나, 동일한 소켓을 재사용하는 백도어 통신의 전형적인 특징이다. 특히 출발지 포트가 50000번대 고정 포트로 유지되는 것은 일반 사용자 애플리케이션의 동작 패턴과 명확히 구분된다.

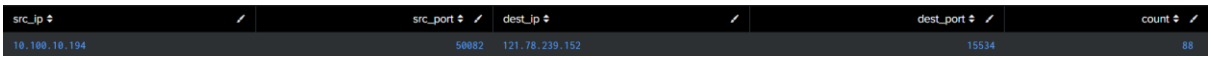


Figure 10. 동일 IP 와 PORT 로 지속 연결한 모습

(3) 일정한 데이터 전송량

대부분의 통신에서 송신 데이터: **204바이트**, 수신 데이터: **80~84바이트**로 거의 동일한 크기를 유지하였다. 이는 "살아있음"을 알리는 Keep-Alive 메시지 또는 명령 대기 상태를 나타내는 전형적인 C2 비콘 통신이다.

```
index=main src_ip="10.100.10.194" dest_ip="121.78.239.152"
| table src_ip, dest_ip, sent_data, rcvd_data
|   sort _time
```

Table 7. 검색에 사용한 쿼리

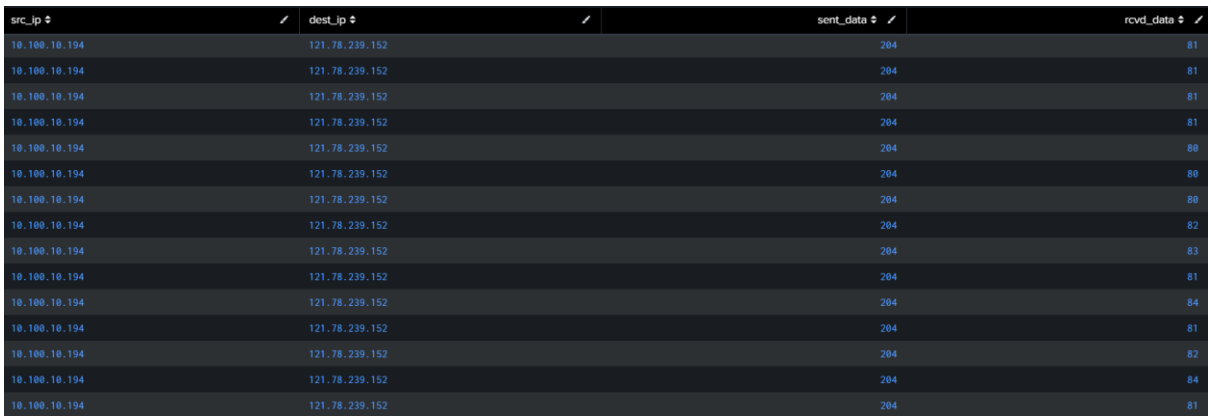


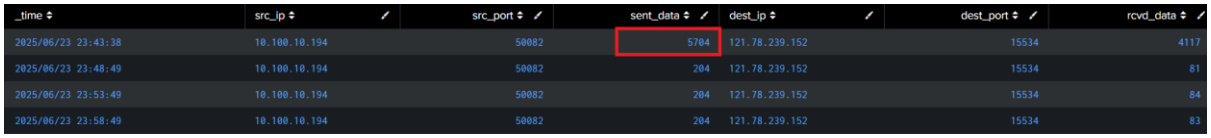
Figure 11. 일정 데이터를 전송하는 모습

(4) 초기 대용량 데이터 전송

최초 통신(23:43:38)에서 송신 5,704바이트, 수신 4,117바이트의 상대적으로 큰 데이터가 전송되었다. 이는 악성코드가 감염 후 초기 정보 수집(시스템 정보, 사용자 계정 등)을 C2 서버로 전송할 때 자주 나타나는 패턴이다.

```
index=main src_ip="10.100.10.194" dest_ip="121.78.239.152"
| table _time src_ip, src_port, sent_data, dest_ip, dest_port, rcvd_data
| sort _time
```

Table 8. 초기 데이터 전송량 확인 쿼리



_time	src_ip	src_port	sent_data	dest_ip	dest_port	rcvd_data
2025/06/23 23:43:38	10.100.10.194	50082	5704	121.78.239.152	15534	4117
2025/06/23 23:48:49	10.100.10.194	50082	204	121.78.239.152	15534	81
2025/06/23 23:53:49	10.100.10.194	50082	204	121.78.239.152	15534	84
2025/06/23 23:58:49	10.100.10.194	50082	204	121.78.239.152	15534	83

Figure 12. 초기 많은 데이터를 송신하는 모습

(5) 비정상적인 통신 시간대

2025년 6월 23일 23:43부터 6월 24일 07:09까지 심야 및 새벽 시간대(00시~07시)에도 지속적으로 외부 통신을 수행하였다.

일반적인 업무 환경에서는 사용자의 근무 시간(09시~18시)에 네트워크 활동이 집중되며, 심야 시간대에는 통신량이 현저히 감소하거나 중단되는 것이 정상이다. 그러나 본 케이스에서는 사용자가 부재한 시간대에도 5분 간격의 규칙적인 통신이 중단 없이 발생하였다.

```
index=main src_ip="10.100.10.194" dest_ip="121.78.239.152"
| eval hour=strftime(_time, "%H")
| stats
      count as connections,
      earliest(_time) as first_seen,
      latest(_time) as last_seen
      by hour, src_ip, dest_ip
| sort hour
| table hour, src_ip, dest_ip, connections, first_seen, last_seen
```

Table 9. 통신 시간 확인 쿼리

hour	src_ip	dest_ip	connections	first_seen	last_seen
00	10.100.10.194	121.78.239.152	11	1750691029	1750694334
01	10.100.10.194	121.78.239.152	11	1750694634	1750697937
02	10.100.10.194	121.78.239.152	12	1750698237	1750701542
03	10.100.10.194	121.78.239.152	12	1750701843	1750705146
04	10.100.10.194	121.78.239.152	12	1750705447	1750708752
05	10.100.10.194	121.78.239.152	12	1750709052	1750712356
06	10.100.10.194	121.78.239.152	12	1750712657	1750715960
07	10.100.10.194	121.78.239.152	2	1750716260	1750716561
23	10.100.10.194	121.78.239.152	4	1750689818	1750690729

Figure 13. 통신 시간 확인 결과