HTTP 이상징후

❶ 비정상 메소드 사용

❷ 외부행 데이터 전송

❸ Mime-type과 파일 확장자 불일치

❹ 사이트 이동 후 실행파일 다운로드

❺ 프록시 서버 접속

❶ 비정상 메소드 사용

- Head, Delete, Trace, Option 과 같은 메소드가 네트워크에서 지속적으로 보인다는 것은 정상적인 사용자의 활동이라 보기 어려움

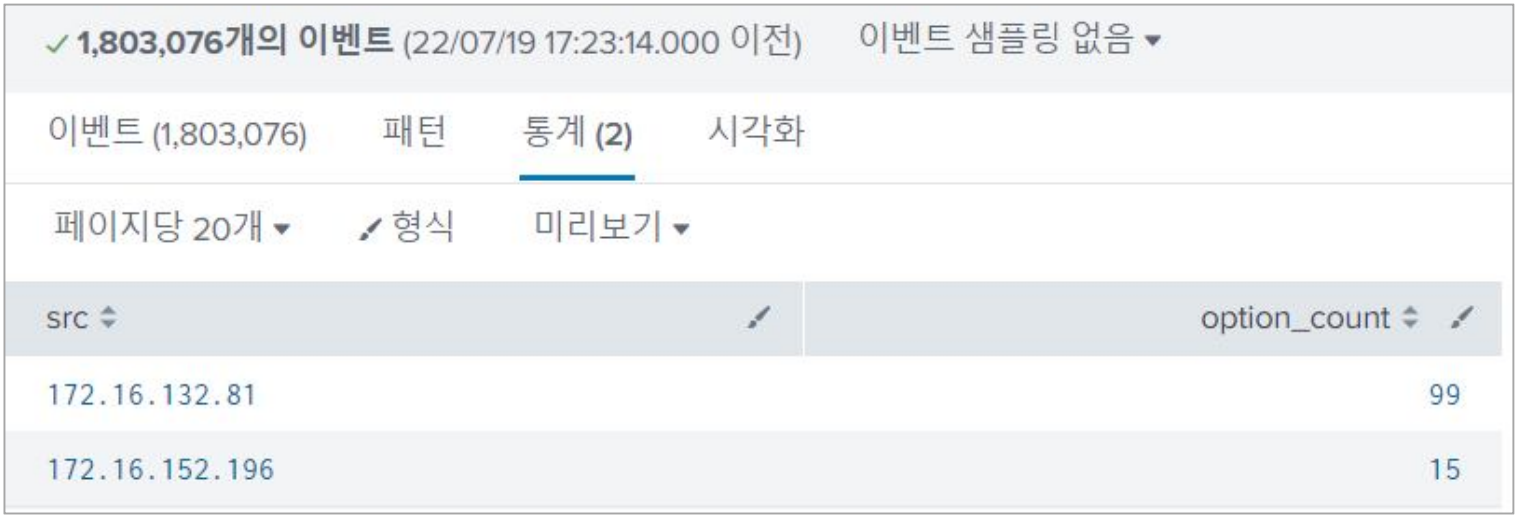
```
index=httplog sourcetype=httplog
| stats count(method) by src
```

송신지를 기준으로 접속에 사용한 메소드의 종류별 개수 검색

```
index=httplog sourcetype=httplog
| stats count(eval(method="OPTIONS")) AS option_count by src
| where option_count > 10
| sort option_count desc
```

❶ 비정상 메소드 사용

```
index=httplog sourcetype=httplog
| stats count(eval(method="OPTIONS")) AS option_count by src
| where option_count > 10
| sort option_count desc
```



```
index=httplog sourcetype=httplog
| where NOT match(method, "(GET|POST|-)")
| stats count(src) as src_count by method
| sort - src_count
```

✓ **6,934개의 이벤트** (22/07/19 17:44:05.000 이전) 이벤트 샘플링 없음

이벤트 (6,934) 패턴 **통계 (6)** 시각화

페이지당 20개 형식 미리보기

method	src_count
HEAD	6564
OPTIONS	187
PUT	102
PROPFIND	79
DELETE	1
RCON	1

❷ 외부행 데이터 전송

```
sourcetype=httplog (request_body_len!=0 OR response_body_len!="0") domain!="-"
```

```
| stats sum(request_body_len) as outTotal sum(response_body_len) as inTotal by src, dst
```

```
| eval oMB=round(outTotal/(1024*1024),2)  | eval iMB=round(inTotal/(1024*1024),2)
| search oMB!=0 AND iMB!=0
| iplocation dst
| eval isUp=if((oMB/iMB)>1, "Yes","No")  | where isUp="Yes"
| table src,dst, iMB, oMB, Country, City
```

❷ 외부행 데이터 전송

```
index=httplog sourcetype=httplog
(request_body_len!=0 OR response_body_len!="0") domain!="-"
| stats sum(request_body_len) as outTotal sum(response_body_len) as inTotal by src, dst
| eval oMB=round(outTotal/(1024*1024),2)  | eval iMB=round(inTotal/(1024*1024),2)
| search oMB!=0 AND iMB!=0 | iplocation dst
| eval isUp=if((oMB/iMB)>1, "Yes","No")  | where isUp="Yes"
| table src,dst, iMB, oMB, Country, City
```

✓ **556,655개의 이벤트** (22/07/19 17:52:54.000 이전) 이벤트 샘플링 없음 ▾ 작업 ▾

이벤트 (556,655) 패턴 **통계 (9)** 시각화

페이지당 20개 ▾ 형식 미리보기 ▾

src	dst	iMB	oMB	Country	City
172.16.129.69	103.243.220.234	0.05	0.10	Singapore	Singapore (Downtown Core)
172.16.129.69	103.243.221.108	0.01	0.12	Singapore	Singapore (Downtown Core)
172.16.129.69	104.254.150.108	0.05	0.19	United States	New York
172.16.129.69	104.254.150.179	0.03	0.13	United States	New York
172.16.132.57	203.205.219.196	0.04	0.08	Hong Kong	Hong Kong
172.16.138.2	67.227.186.229	0.02	0.18	United States	Lansing
172.16.138.2	72.52.161.233	0.02	0.18	United States	Lansing
172.16.143.56	203.205.151.204	0.02	0.03	Singapore	Singapore
172.16.156.145	203.205.128.104	0.01	0.02	Hong Kong	Hong Kong

❸ Mime-type과 파일 확장자 불일치

```
index=httplog sourcetype=httplog resp_mime_types="application/x-dosexec" uri!="-“
| eval filename1=mvindex(split(uri,"/"),-1)
| eval filename=if(like(filename1,"%?%"), mvindex(split(filename1,"?"),0),filename1)
| eval filetype=if(match(filename,"(.exe|.bat|.ps1|.dll|.ocx)$"), "PE", "Not_PE")
| table domain, uri, filename, filetype, resp_mime_types
| where filetype=="Not_PE"
| dedup filename
```

MIME-Type

- MIME(Multipurpose Internet Mail Extensions) Type은 미디어 타입(Media Type)이라고도 부름
- 인터넷에서 데이터 형식을 식별하기 위해 사용되는 Type
- 인터넷의 모든 MIME Type은 국제인터넷주소관리기구(ICANN)에서 관리
- MIME Type을 정의하기 위해서는 슬래시(/)를 사용하며 공백이나 탭이 존재할 수 없음

(형식) Type/SubType

폰트	font/woff, font/ttf, font/otf
영상 및 이미지	image/jpeg, image, png, image/svg+xml
텍스트	text/plain, text/csv, text/html
멀티파트	HTML Form을 POST 전송하는 경우: multipart/form-data
pdf 및 json	application/pdf, application/json

Content-Type

- HTTP 헤더에 존재하는 매개변수로 어떤 유형의 데이터가 전송되는지 웹 클라이언트 또는 웹 서버에 알리는 역할
- 웹 클라이언트가 text/html을 요청하는 경우 웹 서버는 요청에 대한 응답에 content-Type: text/html을 포함

(형식) Type/SubType

```
Content-Type: Mutlipart/related
Content-Type: Application/X-FixedRecord
Content-Type: text/xml
```

MIME Type & Content-Type

- MIME Type과 Content-Type은 인터넷에서 데이터(텍스트, 파일, 이미지 등) 형식을 식별하기 위해 사용
- MIME Type은 Content-Type보다 상위 개념
- Content-Type은 웹에서 사용

❹ 사이트 이동 후 실행파일 다운로드

```
index=httplog sourcetype=httplog referrer!="-" status_code=200
```

```
Hypertext Transfer Protocol
> [truncated]GET /combiner/c?v=201003241632&css=base.201003241632.css,modules.201003241633.c
  Host: a.espncdn.com\r\n
  User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.8) Gecko/20100214 Ubuntu/9.10
  Accept: text/css,*/*;q=0.1\r\n
  Accept-Language: en-us,en;q=0.5\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
  Keep-Alive: 300\r\n
  Connection: keep-alive\r\n
  Referer: http://espn.go.com/\r\n
  \r\n
```

❹ 사이트 이동 후 실행파일 다운로드

```
| eval filename1=mvindex(split(uri,"/"),-1)
| eval filename=if(like(filename1,"%?%"), mvindex(split(filename1,"?"),0),filename1)
```

/cgi-bin/PelicanC.dll?impr?pageid=002k&out=iframe

split(uri,"/")

cgi-bin | PelicanC.dll?impr?pageid=002k&out=iframe

filename1=mvindex(split(uri,"/"),-1)

PelicanC.dll | impr | pageid=002k&out=iframe

split(filename1,"?")

filename=mvindex(split(filename1,"?"),0)

❹ 사이트 이동 후 실행파일 다운로드

```
| where cidrmatch("0.0.0.0/0",domain)
```

```
| where match(resp_mime_types,"application/x-dosexec") OR match(filename,"(exe|dll|com|src)$")
| eval URL=domain+" :: " + filename
| stats count by src, URL
| stats list(URL) as Target list(count) as Source by src
```

File name	Mime type
googletoolbarinstaller....exe	application/x-dosexec
..._chrome_installer.exe	application/x-dosexec
GoogleUpdateSetup.exe	application/x-dosexec

❹ 사이트 이동 후 실행파일 다운로드

```
index=httplog sourcetype=httplog referrer!="-" status_code=200
| eval filename1=mvindex(split(uri,"/"),-1)
| eval filename=if(like(filename1,"%?%"), mvindex(split(filename1,"?"),0),filename1)
| where cidrmatch("0.0.0.0/0",domain)
| where match(resp_mime_types,"application/x-dosexec") OR match(filename,"(exe|dll|com|src)$")
| eval URL=domain+" :: " + filename
| stats count by src, URL
| stats list(URL) as Target list(count) as Source by src
```

✓ 1개의 이벤트 (22/07/19 18:52:28.000 이전) 이벤트 샘플링 없음

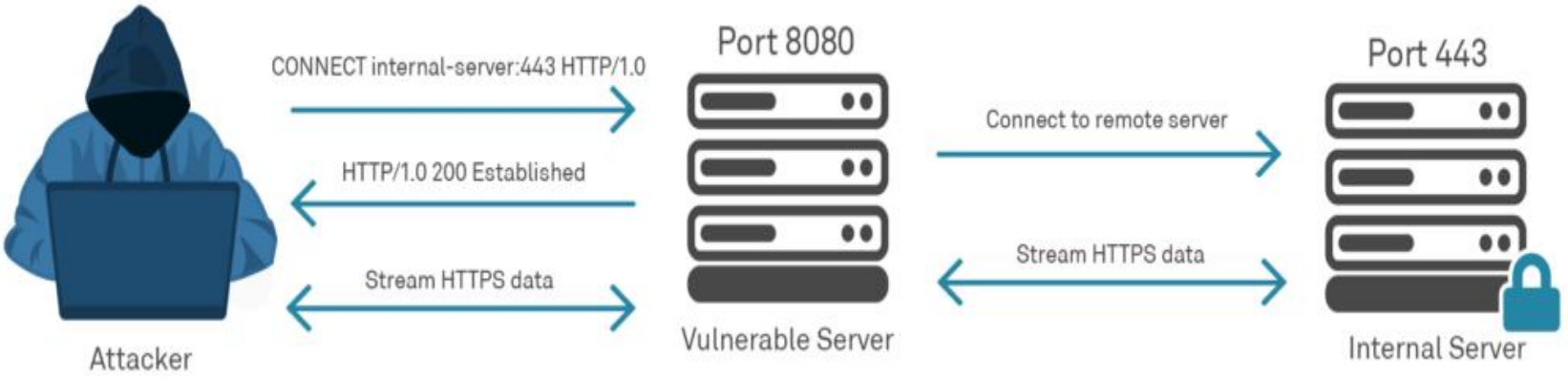
이벤트 (1) 패턴 통계 (1) 시각화

페이지당 20개 형식 미리보기

src	Target	Source
172.16.154.10	27.101.137.41 :: PelicanC.dll	1

Proxy Server

- Connect method : 웹서버에 Proxy 기능을 요청 시 사용




```
> Frame 43: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface \Device\NPF_{BD0DBB8D-64FC-47A9-
> Ethernet II, Src: VMware_5f:2c:a1 (00:0c:29:5f:2c:a1), Dst: Fortinet_99:4a:b3 (70:4c:a5:99:4a:b3)
> Internet Protocol Version 4, Src: 194.247.5.7, Dst: 85.25.246.38
> Transmission Control Protocol, Src Port: 57556, Dst Port: 8080, Seq: 1, Ack: 1, Len: 237
v Hypertext Transfer Protocol
  v CONNECT weberblog.net:443 HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): CONNECT weberblog.net:443 HTTP/1.1\r\n]
      Request Method: CONNECT
      Request URI: weberblog.net:443
      Request Version: HTTP/1.1
    Host: weberblog.net:443\r\n
    Proxy-Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 S
    \r\n
    [Full request URI: weberblog.net:443]
    [HTTP request 1/1]
    [Response in frame: 45]
```

HTTPS Connection through a proxy:
method: CONNECT,
while URI lists only the host (without the path)

Proxy Server

- URI에 접속 대상의 전체 주소가 기록 된 경우

  * 클라이언트가 자체적으로 프록시를 설정하고 운영하는 경우

Attacker

uri
http://updates.cdc.carbonblack.io/update/x_vdf/xbv00200.vdf.gz
http://updates.cdc.carbonblack.io/update/x_vdf/aevdf.dat.gz
http://updates.cdc.carbonblack.io/update/idx/ave2-win64-int.info.gz
http://updates.cdc.carbonblack.io/update/idx/xvdf.info.gz
http://updates.cdc.carbonblack.io/update/idx/savapi4lib-win64-en.info.gz
http://updates.cdc.carbonblack.io/update/idx/master.idx

❺ 프록시 서버 접속

```
index=httplog sourcetype=httplog (uri="http://*" OR method="connect")
| table src, domain, uri
```

✓ **6개의 이벤트** (22/07/19 18:57:19.000 이전) 이벤트 샘플링 없음 ▾

이벤트 (6) 패턴 **통계 (6)** 시각화

페이지당 20개 ▾ 형식 미리보기 ▾

src	domain	uri
172.16.156.145	updates.cdc.carbonblack.io	http://updates.cdc.carbonblack.io/update/x_vdf/xbv00200.vdf.gz
172.16.156.145	updates.cdc.carbonblack.io	http://updates.cdc.carbonblack.io/update/x_vdf/aevdf.dat.gz
172.16.156.145	updates.cdc.carbonblack.io	http://updates.cdc.carbonblack.io/update/idx/ave2-win64-int.info.gz
172.16.156.145	updates.cdc.carbonblack.io	http://updates.cdc.carbonblack.io/update/idx/xvdf.info.gz
172.16.156.145	updates.cdc.carbonblack.io	http://updates.cdc.carbonblack.io/update/idx/savapi4lib-win64-en.info.gz
172.16.156.145	updates.cdc.carbonblack.io	http://updates.cdc.carbonblack.io/update/idx/master.idx