# Digital Forensics (01) Assignment1 Task2 Report

2171056 강승연

### Brief Introduction of IcedID

IcedID란, 2017년도에 처음 발견된 뱅킹 트로이 목마이다. 이 악성코드는 Shatak(aka. TA551) 공격 집단에 의해 MaaS에 사용되고 있다. 주로 Emotet와 같은 다른 초기 악성 코드에 의존하는 2단계 악성코드이나, 이메일과 같은 다른 경로로도 감염될 수 있다. 그리고 다른 악성코드를 배포할 수 있는 로더 역할 또한 가능하다.

금융 기관의 사용자 계정에 대한 로그인 자격 증명을 수집하는 데 특화되어 있다. 브라우저 내에서 동작하는 man-in-the-browser 공격을 통해 금융 정보를 탈취한다. 이렇게 탈취한 금융 정보를 이용해 자동화된 사기 거래를 수행한다.

## Explain what is the IP address of the localhost and how you identify it

Localhost IP address: 10.10.31.101

| Time        | Source          | Destination     | Protocol |
|-------------|-----------------|-----------------|----------|
| 1 0.000000  | 10.10.31.101    | 10.10.31.1      | DNS      |
| 2 0.113504  | 10.10.31.1      | 10.10.31.101    | DNS      |
| 3 0.117203  | 10.10.31.101    | grafielucho.com | TCP      |
| 4 0.161532  | grafielucho.com | 10.10.31.101    | TCP      |
| 5 0.161684  | 10.10.31.101    | grafielucho.com | TCP      |
| 6 0.161896  | 10.10.31.101    | grafielucho.com | HTTP     |
| 7 0.196456  | grafielucho.com | 10.10.31.101    | TCP      |
| 8 1.202525  | grafielucho.com | 10.10.31.101    | TCP      |
| 9 1.202589  | grafielucho.com | 10.10.31.101    | TCP      |
| 10 1.202696 | grafielucho.com | 10.10.31.101    | TCP      |

위 캡쳐는 Task 2에서 분리한 패킷 .cap 파일 중 제일 첫번째 파일을 Wireshark 로 확인한 것이다.

Wireshark 의 네트워크 주소 해석 기능을 이용하여 IP 주소를 해석된 네트워크 주소로 바꾸었다. 그 결과 10.10.31.101 IP 주소가 계속해서 Source 와 Destination 에서 나타남을 발견하였고, 이 IP 주소가 Localhost IP 주소임을 확인할 수 있었다.

# Explain IoCs (Indications-of-Compromise) from the captured network packets

IoC란, 침해지표이다. C2 IP 주소, 악성 파일의 해시 파일이 그 예가 될 수 있는데, 네트워크 패킷 캡쳐로 침해 지표를 파악해야 하므로 C2 IP 주소 혹은 감염된 window host의 IP주소를 찾는 것을 목적으로 한다.

먼저, 침해 경로를 확인하기 위해 Wireshark 에서 http Protocol로 필터링을 진행했다.

| No. |      | Time       | Source          | Destination     | Protocol Length Info                       |
|-----|------|------------|-----------------|-----------------|--|
|     | 6    | 0.161896   | 10.10.31.101    | 104.21.32.6     | HTTP 361 GET / HTTP/1.1                    |
|     | 1992 | 3.263415   | 104.21.32.6     | 10.10.31.101    | HTTP 1083 HTTP/1.1 200 OK (application/gzi |
|     |      |            |                 |                 |  |
| No. |      | Time       | Source          | Destination     | Protocol Lengtr Info                       |
|     | 637  | 84.789491  | 10.10.31.101    | 192.229.211.108 | HTTP 371 GET /MFEwTzBNMEswSTAJBgUrDgN      |
|     | 640  | 84.841406  | 192.229.211.108 | 10.10.31.101    | OCSP 791 Response                          |
|     | 693  | 85.377744  | 10.10.31.101    | 192.229.211.108 | HTTP 294 GET /MFEwTzBNMEswSTAJBgUrDgN      |
|     | 698  | 85.424063  | 192.229.211.108 | 10.10.31.101    | OCSP 791 Response                          |
|     | 1072 | 101.166366 | 10.10.31.101    | 72.21.81.240    | HTTP 340 GET /msdownload/update/v3/st      |
|     | 1078 | 101.204774 | 72.21.81.240    | 10.10.31.101    | HTTP 342 HTTP/1.1 304 Not Modified         |
|     | 1089 | 101.212743 | 10.10.31.101    | 72.21.81.240    | HTTP 336 GET /msdownload/update/v3/st      |
|     | 1094 | 101.258542 | 72.21.81.240    | 10.10.31.101    | HTTP 345 HTTP/1.1 304 Not Modified         |
|     | 1104 | 101.349290 | 10.10.31.101    | 72.21.81.240    | HTTP 306 GET /msdownload/update/v3/st      |
|     | 1107 | 101.386187 | 72.21.81.240    | 10.10.31.101    | HTTP 342 HTTP/1.1 304 Not Modified         |
|     | 1110 | 101.393176 | 10.10.31.101    | 72.21.81.240    | HTTP 336 GET /msdownload/update/v3/st      |
|     | 1115 | 101.445752 | 72.21.81.240    | 10.10.31.101    | HTTP 345 HTTP/1.1 304 Not Modified         |
|     | 1237 | 161.938576 | 10.10.31.101    | 209.197.3.8     | HTTP 336 GET /msdownload/update/v3/st      |
|     | 1239 | 162.022468 | 209.197.3.8     | 10.10.31.101    | HTTP 245 HTTP/1.1 304 Not Modified         |
|     | 1240 | 162.031467 | 10.10.31.101    | 209.197.3.8     | HTTP 306 GET /msdownload/update/v3/st      |
|     | 1242 | 162.098034 | 209.197.3.8     | 10.10.31.101    | HTTP 243 HTTP/1.1 304 Not Modified         |
|     | 1243 | 162.105449 | 10.10.31.101    | 209.197.3.8     | HTTP 336 GET /msdownload/update/v3/st      |
|     | 1245 | 162.159495 | 209.197.3.8     | 10.10.31.101    | HTTP 245 HTTP/1.1 304 Not Modified         |
|     | 1250 | 162.222966 | 10.10.31.101    | 209.197.3.8     | HTTP 336 GET /msdownload/update/v3/st      |
|     | 1252 | 162.279690 | 209.197.3.8     | 10.10.31.101    | HTTP 245 HTTP/1.1 304 Not Modified         |

그 결과 많은 수의 패킷을 확인할 수 있었다. 대부분의 패킷이 의심스러운 행동으로 분류될 수 있는 활동들이다.

먼저 맨 위 103.21.32.6 과 주고받은 패킷은 아래와 같다.

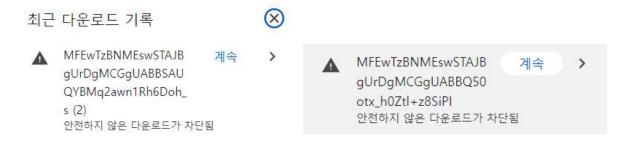
| No.        | Time            | Source                | Destination            | Protocol      | Length Info             |  |
|------------|-----------------|-----------------------|------------------------|---------------|-------------------------|--|
| -          | 6 0.161896      | 10.10.31.101          | 104.21.32.6            | HTTP          | 361 GET / HTTP/1.1      |  |
| <b>←</b> 1 | 1992 3.263415   | 104.21.32.6           | 10.10.31.101           | HTTP          | 1083 HTTP/1.1 200 OK    | (application/gzip)                     |
| > Fr       | ame 6: 361 byte | es on wire (2888 bit: | s), 361 bytes captured | d (2888 bits) | on interface unknown,   | id 0                                   |
| > Et       | hernet II, Src: | GigaByteTech_2d:69    | ee (fc:aa:14:2d:69:ee  | e), Dst: fa:f | ff:c2:e2:63:64 (fa:ff:c | 2:e2:63:64)                            |
| > In       | ternet Protocol | Version 4, Src: 10    | .10.31.101, Dst: 104.2 | 21.32.6       |                         |  |
| > Tr       | ansmission Cont | rol Protocol, Src Po  | ort: 56108, Dst Port:  | 80, Seq: 1,   | Ack: 1, Len: 307        |  |
| → Hy       | pertext Transfe | er Protocol           |                        |               |                         |  |
| ~          | GET / HTTP/1.1  | \r\n                  |                        |               |                         |  |
|            | ▼ [Expert Inf   | o (Chat/Sequence): G  | ET / HTTP/1.1\r\n]     |               |                         |  |
|            |                 | TTP/1.1\r\n]          |                        |               |                         |  |
|            | [Severit        | y level: Chat]        |                        |               |                         |  |
|            | [Group:         | Sequence]             |                        |               |                         |  |
|            | Request Met     | hod: GET              |                        |               |                         |  |
|            | Request URI     | : /                   |                        |               |                         |  |
|            | Request Ver     | sion: HTTP/1.1        |                        |               |                         |  |
|            | Connection: Ke  | ep-Alive\r\n          |                        |               |                         |  |
| >          | [truncated]Co   | okie:gads=2411184     | 569:1:515819:137; _ga  | t=10.0.19045  | 6.64; _ga=2.6295328.0.4 | ; _u=4445534B544F502D30303244373648:6A |
|            | Host: grafielu  | cho.com\r\n           |                        |               |                         |  |
|            | \r\n            |                       |                        |               |                         |  |
|            | [Full request   | URI: http://grafielu  | icho.com/]             |               |                         |  |
|            | [HTTP request   | 1/1]                  |                        |               |                         |  |
|            | [Response in f  | rame: 1992]           |                        |               |                         |  |

http://grafielucho.com/ 와 GET 통신을 진행했다. 아마 이 경로를 통하여 최초로 감염 경로를 제공했을 것으로 파악된다.

다음은 192.229.211.108과 주고 받은 패킷이다.

|   |   | Time  | Source   | Destination  | Protocol     | Length             | IIIIO                              |                 |
|---|---|---|--|--|--------------|--------------------|------------------------------------|-----------------|
|   | 637   | 84.789491   | 10.10.31.101   | 192.229.211.108  | HTTP         | 371                | GET /MFEWTzBNM                     | NESWSTAJBgUrDgM |
|   | 640   | 84.841406   | 192.229.211.108  | 10.10.31.101   | OCSP         | 791                | Response                           |                 |
|   | 693   | 85.377744   | 10.10.31.101   | 192.229.211.108  | HTTP         | 294                | GET /MFEwTzBNM                     | NESWSTAJBgUrDgM |
|   | 698   | 85.424063   | 192.229.211.108  | 10.10.31.101   | OCSP         | 791                | Response                           |                 |
|   | 1072  | 101.166366  | 10.10.31.101   | 72.21.81.240   | HTTP         | 340                | GET /msdownloa                     | id/update/v3/st |
|   | 1078  | 101.204774  | 72.21.81.240   | 10.10.31.101   | HTTP         | 342                | HTTP/1.1 304 N                     | lot Modified    |
| F | rame  | 637: 371 byte   | s on wire (2968 bit  | s), 371 bytes capture  | d (2968 bit  | s) on              |                                    | own, id 0       |
| E | thern   | et II, Src: G   | igaByteTech_2d:69:e  | e (fc:aa:14:2d:69:ee)  | , Dst: fa:f  | f:c2:e             | 2:63:64 (fa:ff                     | :c2:e2:63:64)   |
| ] | ntern   | et Protocol V   | ersion 4, Src: 10.1  | 0.31.1 <mark>01, Dst: 1</mark> 92.22   | 9.211.108    |                    |                                    |                 |
| 1 | ransm   | ission Contro   | l Protocol, Src Por  | t: 56221, Dst Port: 8  | 0, Seq: 1,   | Ack: 1             | , Len: 317                         |                 |
| ŀ | lypert  | ext Transfer  | Protocol   |  |              |                    |                                    |                 |
| 1 | ✓ GET   | /MFEwTzBNMEs  | wSTAJBgUrDgMCGgUABB  | SAUQYBMq2awn1Rh6Doh%2F   | FsBYgFV7gQL  | A95QNV             | bRTLtm8KPiGxvDl                    | 17I90VUCEAJ0Lq  |
|   |   | [Expert Info  | (Chat/Sequence): GET   | MEENT-RNMEENSTAIR  | InDaMCGallAR | RSALIOVE           | Ma 2 au m 1 Ph C Dah 9             | /2F-PV-FV7-0UA  |
|   |   | Lampa, a z  | (char, sequence), ac   | I THI CMIZDINICSWOTHOUGH   | I DELICGEDAD | DOMOGII            | pridzamitkuppouv                   | OZFSDIBLALBÓNY  |
|   | *   |   |  | CGgUABBSAUQYBMq2awn1Rh   |              |                    |                                    |                 |
|   |   | [GET /MFEw]   |  |  |              |                    |                                    |                 |
|   | *   | [GET /MFEw]   | ΓzBNMEswSTAJBgUrDgMC<br>Level: Chat]   |  |              |                    |                                    |                 |
|   |   | [GET /MFEw]<br>[Severity]   | rzBNMEswSTAJBgUrDg <mark>M</mark> C<br>Level: Chat]<br>quence]   |  |              |                    |                                    |                 |
|   |   | [GET /MFEwl<br>[Severity]<br>[Group: Sec<br>Request Method  | FzBNMEswSTAJBgUrDgMC<br>Level: Chat]<br>quence]<br>d: GET  |  | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   | 1   | [GET /MFEwl<br>[Severity]<br>[Group: Sec<br>Request Method  | TzBNMEswSTAJBgUrDgMC<br>Level: Chat]<br>quence]<br>d: GET<br>/MFEwTzBNMEswSTAJBgU  | GgUABBSAUQYBMq2awn1Rh  | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   |   | [GET /MFEw]<br>[Severity ]<br>[Group: Sec<br>Request Method<br>Request URI: ,<br>Request Version  | TzBNMEswSTAJBgUrDgMC<br>Level: Chat]<br>quence]<br>d: GET<br>/MFEwTzBNMEswSTAJBgU  | GgUABBSAUQYBMq2awn1Rh  | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   | Cac   | [GET /MFEw]<br>[Severity ]<br>[Group: Sec<br>Request Method<br>Request URI: ,<br>Request Version  | TzBNMEswSTAJBgUrDgMC<br>Level: Chat]<br>quence]<br>d: GET<br>/MFEwTzBNMEswSTAJBgU<br>on: HTTP/1.1<br>ax-age = 7200\r\n   | GgUABBSAUQYBMq2awn1Rh  | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   | Cac   | [GET /MFEw] [Severity ] [Group: Sec<br>Request Method<br>Request URI: ,<br>Request Version<br>he-Control: m   | TzBNMEswSTAJBgUrDgMC<br>Level: Chat]<br>quence]<br>d: GET<br>/MFEwTzBNMEswSTAJBgU<br>on: HTTP/1.1<br>ax-age = 7200\r\n   | GgUABBSAUQYBMq2awn1Rh  | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   | I<br>I<br>Cac<br>Con<br>Acc                   | [GET /MFEW] [Severity ] [Group: Sec Request Method Request URI: , Request Version he-Control: m nection: Keep ept: */*\r\n  | TzBNMEswSTAJBgUrDgMC<br>Level: Chat]<br>quence]<br>d: GET<br>/MFEwTzBNMEswSTAJBgU<br>on: HTTP/1.1<br>ax-age = 7200\r\n   | :GgUABBSAUQYBMq2awn1Rh<br>JrDgMCGgUABBSAUQYBMq2a                             | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   | Cac<br>Con<br>Acc                             | [GET /MFEW] [Severity ] [Group: Sec Request Method Request URI: , Request Version he-Control: m nection: Keep ept: */*\r\n Modified-Sinc                              | TzBNMEswSTAJBgUrDgMC<br>Level: Chat]<br>quence]<br>d: GET<br>/MFEwTzBNMEswSTAJBgU<br>on: HTTP/1.1<br>ax-age = 7200\r\n<br>-Alive\r\n   | GgUABBSAUQYBMq2awn1Rh<br>JrDgMCGgUABBSAUQYBMq2a<br>02:08:20 GMT\r\n          | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   | Cac<br>Con<br>Acc<br>If-                      | [GET /MFEW] [Severity ] [Group: Sec Request Method Request URI: , Request Version he-Control: m nection: Keep ept: */*\r\n Modified-Sinc                              | <pre>TzBNMEswSTAJBgUrDgMC Level: Chat] quence] d: GET /MFEwTzBNMEswSTAJBgU on: HTTP/1.1 ax-age = 7200\r\n -Alive\r\n e: Mon, 23 Oct 2023 osoft-CryptoAPI/10.6</pre>  | GgUABBSAUQYBMq2awn1Rh<br>JrDgMCGgUABBSAUQYBMq2a<br>02:08:20 GMT\r\n          | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | (PiGxvDl7I90VUC |
|   | Cac<br>Con<br>Acc<br>If-                      | [GET /MFEW] [Severity ] [Group: Sec Request Method Request VRI: , Request Version he-Control: m nection: Keep ept: */*\r\n Modified-Sinc r-Agent: Micr t: ocsp.digic  | <pre>TzBNMEswSTAJBgUrDgMC Level: Chat] quence] d: GET /MFEwTzBNMEswSTAJBgU on: HTTP/1.1 ax-age = 7200\r\n -Alive\r\n e: Mon, 23 Oct 2023 osoft-CryptoAPI/10.6</pre>  | GgUABBSAUQYBMq2awn1Rh<br>JrDgMCGgUABBSAUQYBMq2a<br>02:08:20 GMT\r\n          | 6Doh%2FsBY   | gFV7gQl            | JA95QNVbRTLtm8K                    | PiGxvD17I90VU   |
|   | Cac<br>Con<br>Acc<br>If-<br>Use<br>Hos<br>\r\ | [GET /MFEW] [Severity ] [Group: Sec Request Method Request VRI: , Request Version he-Control: m nection: Keep ept: */*\r\n Modified-Sinc r-Agent: Micro t: ocsp.digic | <pre>TzBNMEswSTAJBgUrDgMC Level: Chat] quence] d: GET /MFEwTzBNMEswSTAJBgUron: HTTP/1.1 ax-age = 7200\r\n -Alive\r\n e: Mon, 23 Oct 2023 osoft-CryptoAPI/10.0 ert.com\r\n</pre>                                  | GgUABBSAUQYBMq2awn1Rh<br>JrDgMCGgUABBSAUQYBMq2a<br>02:08:20 GMT\r\n          | aswn1Rh6Doh% | gFV7gQL<br>2FsBYgI | JA95QNVbRTL±m8K<br>FV7gQUA95QNVbRT | PiGxvD17I90VU0  |
|   | Cac<br>Con<br>Acc<br>If-<br>Use<br>Hos<br>\r\ | [GET /MFEW] [Severity ] [Group: Sec Request Method Request VRI: , Request Version he-Control: m nection: Keep ept: */*\r\n Modified-Sinc r-Agent: Micro t: ocsp.digic | <pre>TzBNMEswSTAJBgUrDgMC Level: Chat] quence] d: GET /MFEwTzBNMEswSTAJBgUrDgm: HTTP/1.1 ax-age = 7200\r\n -Alive\r\n e: Mon, 23 Oct 2023 osoft-CryptoAPI/10.0 ert.com\r\n</pre> <pre>L: http://ocsp.digio</pre> | GgUABBSAUQYBMq2awn1Rh<br>JrDgMCGgUABBSAUQYBMq2a<br>02:08:20 GMT\r\n<br>0\r\n | aswn1Rh6Doh% | gFV7gQL<br>2FsBYgI | JA95QNVbRTL±m8K<br>FV7gQUA95QNVbRT | PiGxvDl7I90VU0  |

해당 IP와 주고받은 패킷 중 의심되는 URL이 두개 발견되어 접속해본 결과 안전하지 않은 다운 로드로 분류되어 파일 다운로드가 차단되었다.



해당 두 파일이 IcedID의 악성코드 혹은 IcedID를 위한 1단계 악성코드일 것으로 추정된다.

그리고 72.21.81.240 IP 주소에도 의심스로운 URL이 있어 접속해본 결과, 이 URL도 악성파일을 다운받는 URL로 추정되는 사이트에 접속되었다.

| No. |        | Time          | Source              | Destination            | Protocol     | Length Info  |
|-----|--------|---------------|---------------------|------------------------|--------------|--|
| -   | 1072   | 101.166366    | 10.10.31.101        | 72.21.81.240           | HTTP         | 340 GET /msdownload/update/v3/static/trustedr/en/disallowed    |
| -   | 1078   | 101.204774    | 72.21.81.240        | 10.10.31.101           | HTTP         | 342 HTTP/1.1 304 Not Modified                                  |
|     | 1089   | 101.212743    | 10.10.31.101        | 72.21.81.240           | HTTP         | 336 GET /msdownload/update/v3/static/trustedr/en/pinrulesst    |
|     | 1094   | 101.258542    | 72.21.81.240        | 10.10.31.101           | HTTP         | 345 HTTP/1.1 304 Not Modified                                  |
|     | 1104   | 101.349290    | 10.10.31.101        | 72.21.81.240           | HTTP         | 306 GET /msdownload/update/v3/static/trustedr/en/disallowed    |
|     | 1107   | 101.386187    | 72.21.81.240        | 10.10.31.101           | HTTP         | 342 HTTP/1.1 304 Not Modified                                  |
| F   | rame   | 1072: 340 by  | tes on wire (2720 b | oits), 340 bytes captu | red (2720 b  | its) on interface unknown, id 0                                |
|     |        |               |                     |                        |              | ff:c2:e2:63:64 (fa:ff:c2:e2:63:64)                             |
|     |        |               |                     | .10.31.101, Dst: 72.21 |              |  |
|     |        |               |                     | ort: 56239, Dst Port:  |              | Ack: 1, Len: 286   |
| H   | lypert | ext Transfer  | Protocol            |                        |              |  |
| -   | ✓ GET  | /msdownload   | /update/v3/static/t | rustedr/en/disallowed  | certstl.cab? | 2883e05df12204f0f HTTP/1.1\r\n                                 |
|     | ~      | [Expert Info  | (Chat/Sequence): G  | ET /msdownload/update  | /v3/static/t | rustedr/en/disallowedcertstl.cab?883e05df12204f0f HTTP/1.1\r\n |
|     |        | [GET /msdc    | ownload/update/v3/s | tatic/trustedr/en/disa | allowedcerts | tl.cab?883e05df12204f0f HTTP/1.1\r\n]                          |
|     |        | [Severity     | level: Chat]        |                        |              |  |
|     |        | [Group: Se    | equence]            |                        |              |  |
|     |        | Request Metho | od: GET             |                        |              |  |
|     | >      | Request URI:  | /msdownload/update  | /v3/static/trustedr/e  | n/disallowed | certstl.cab?883e05df12204f0f                                   |
|     |        | Request Versi | ion: HTTP/1.1       |                        |              |  |
|     | Con    | nection: Kee  | p-Alive\r\n         |                        |              |  |
|     | 100    | ont . */*\n\n |                     |                        |              |  |

Accept: \*/\*\r\n

If-Modified-Since: Tue, 26 Sep 2023 18:01:51 GMT $\r$ 

If-None-Match: "746787a3f0d91:0"\\n User-Agent: Microsoft-CryptoAPI/10.0\r\n Host: ctldl.windowsupdate.com\r\n

\r\n

[Full request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?883e05df12204f0f]

[HTTP request 1/2] [Response in frame: 1078] [Next request in frame: 1089]

### **Server Error**

#### 404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

해당 패킷들의 경우 계속해서 파일의 무결성을 요청하는 패킷 또한 발견되었다. (304 Not Modified)

http 뿐만 아니라 의심스럽게 많은 접속이 있었던 IP가 존재했다.

| ip.addr == 162.33.179.136 |      |           |                |                |          |        |                                |  |
|---------------------------|------|-----------|----------------|----------------|----------|--------|--------------------------------|--|
| No.                       |      | Time      | Source         | Destination    | Protocol | Length | Info                           |  |
|                           | 2617 | 66.736223 | 10.10.31.101   | 162.33.179.136 | TLSv1.2  | 236    | Client Hello (SNI=asleytomafa. |  |
|                           | 2636 | 66.795554 | 162.33.179.136 | 10.10.31.101   | TCP      | 60     | 443 → 56133 [ACK] Seq=1 Ack=18 |  |
|                           | 2637 | 66.800929 | 162.33.179.136 | 10.10.31.101   | TLSv1.2  | 1360   | Server Hello, Certificate, Ser |  |
|                           | 2638 | 66.802647 | 10.10.31.101   | 162.33.179.136 | TLSv1.2  | 147    | Client Key Exchange, Change Ci |  |
|                           | 2674 | 66.862628 | 162.33.179.136 | 10.10.31.101   | TCP      | 60     | 443 → 56133 [ACK] Seq=1307 Ack |  |
|                           | 2675 | 66.862668 | 162.33.179.136 | 10.10.31.101   | TLSv1.2  | 312    | New Session Ticket, Change Cip |  |
|                           | 2677 | 66.863815 | 10.10.31.101   | 162.33.179.136 | TLSv1.2  | 281    | Application Data               |  |
|                           | 2678 | 66.863815 | 10.10.31.101   | 162.33.179.136 | TLSv1.2  | 89     | Application Data               |  |

분할한 모든 패킷에서 해당 ip의 Client Hello 가 발견됨을 확인했다.

해당 url에 접속 불가능함을 확인했다. (asleytomafa.com)

결과적으로 확인할 수 있었던 침해 지표는 다음과 같다.

| >  | 6 0.161896      | 10.10.31.101 | 104.21.32.6     | HTTP 3    | 61 GET / HTTP/1.1   |                     |
|----|-----------------|--------------|-----------------|-----------|---------------------|---------------------|
| 4- | 1992 3.263415   | 104.21.32.6  | 10.10.31.101    | HTTP 10   | 83 HTTP/1.1 200 OK  | (application/gzip)  |
|    |                 |              |                 |           |                     |                     |
|    | 637 84.789491   | 10.10.31.101 | 192.229.211.108 | HTTP      | 371 GET /MFE        | wTzBNMEswSTAJBgUrDg |
|    |                 |              |                 |           |                     |                     |
|    | 693 85.377744   | 10.10.31.101 | 192.229.211.108 | HTTP      | 294 GET /MFE        | wTzBNMEswSTAJBgUrDg |
|    |                 |              |                 |           |                     |                     |
|    | 1072 101.166366 | 10.10.31.101 | 72.21.81.240    | HTTP      | 340 GET /msdown     | load/update/v3/stat |
|    |                 |              |                 |           |                     |                     |
|    |                 |              |                 |           |                     |                     |
|    | 604 57.732831   | 10.10.31.101 | 162.33.179.136  | TLSv1.2 2 | 36 Client Hello (SN | I=asleytomafa.com)  |
|    |                 |              |                 |           |                     |                     |
|    | 79 62.423569    | 10.10.31.101 | 162.33.179.136  | TLSv1.2 2 | 36 Client Hello (SN | II=asleytomafa.com) |
|    |                 |              |                 |           |                     |                     |
|    | 16 57.879565    | 10.10.31.101 | 162.33.179.136  | TLSv1.2   | 236 Client Hello (S | NI=asleytomafa.com) |
|    |                 |              |                 |           | -                   | -                   |
|    | 13 57.997956    | 10.10.31.101 | 162.33.179.136  | TLSv1.2   | 236 Client Hello (S | NI=asleytomafa.com) |
|    |                 |              |                 |           |                     |                     |
|    | 47 61.368389    | 10.10.31.101 | 162.33.179.136  | TLSv1.2   | 236 Client Hello (S | NI=asleytomafa.com) |