

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 캡처는 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 캡처로 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/gzip)

No.	Time	Source	Destination	Protocol	Length	Info
637	84.789491	10.10.31.101	192.229.211.108	HTTP	371	GET /MFEwTzBNMEswSTAJBgUrDgMCGgl
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 /MFEwTzBNMEswSTAJBgUrDgMCGgl
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/static
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
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
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/static
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/static
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/static
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/static
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/static
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
1992	3.263415	104.21.32.6	10.10.31.101	HTTP	1083	HTTP/1.1 200 OK (application/gzip)

> Frame 6: 361 bytes on wire (2888 bits), 361 bytes captured (2888 bits) on interface unknown, id 0

> Ethernet II, Src: GigaByteTech_2d:69:ee (fc:aa:14:2d:69:ee), Dst: fa:ff:c2:e2:63:64 (fa:ff:c2:e2:63:64)

> Internet Protocol Version 4, Src: 10.10.31.101, Dst: 104.21.32.6

> Transmission Control Protocol, Src Port: 56108, Dst Port: 80, Seq: 1, Ack: 1, Len: 307

▼ Hypertext Transfer Protocol

▼ GET / HTTP/1.1\r\n

▼ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n][GET / HTTP/1.1\r\n][Severity level: Chat][Group: Sequence]Request Method: GETRequest URI: /Request Version: HTTP/1.1Connection: Keep-Alive\r\n> [truncated]Cookie: __gads=2411184569:1:515819:137; _gat=10.0.19045.64; _ga=2.6295328.0.4; _u=44455348544F502D30303244373648:6AHost: grafielucho.com\r\n\r\n[Full request URI: http://grafielucho.com/][HTTP request 1/1][Response in frame: 1992]

다음은 192.229.211.108과 주고 받은 패킷이다.

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

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

그리고 72.21.81.240 IP 주소에도 의심스러운 URL이 있어 접속해본 결과, 이 URL도 악성파일을 다운로드하는 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/disallowedcertstl.cab?883e05df12204f0f HTTP/1.1\r\n
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/pinrulesstl.cab?883e05df12204f0f HTTP/1.1\r\n
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/disallowedcertstl.cab?883e05df12204f0f HTTP/1.1\r\n
1107	101.386187	72.21.81.240	10.10.31.101	HTTP	342	HTTP/1.1 304 Not Modified

> Frame 1072: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface unknown, id 0
> Ethernet II, Src: GigaByteTech_2d:69:ee (fc:aa:14:2d:69:ee), Dst: fa:ff:c2:e2:63:64 (fa:ff:c2:e2:63:64)
> Internet Protocol Version 4, Src: 10.10.31.101, Dst: 72.21.81.240
> Transmission Control Protocol, Src Port: 56239, Dst Port: 80, Seq: 1, Ack: 1, Len: 286
▼ Hypertext Transfer Protocol
▼ GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?883e05df12204f0f HTTP/1.1\r\n
▼ [Expert Info (Chat/Sequence): GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?883e05df12204f0f HTTP/1.1\r\n]
[GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?883e05df12204f0f HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
> Request URI: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?883e05df12204f0f
Request Version: HTTP/1.1
Connection: Keep-Alive\r\n
Accept: */*\r\n
If-Modified-Since: Tue, 26 Sep 2023 18:01:51 GMT\r\n
If-None-Match: "746787a3f0d91:0"\r\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.com)
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, Server Key Exchange, Change Cipher Spec, Application Data
2638	66.802647	10.10.31.101	162.33.179.136	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Application Data
2674	66.862628	162.33.179.136	10.10.31.101	TCP	60	443 → 56133 [ACK] Seq=1307 Ack=18
2675	66.862668	162.33.179.136	10.10.31.101	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Application Data
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	361 GET / HTTP/1.1
←	1992	3.263415	104.21.32.6	10.10.31.101	HTTP	1083 HTTP/1.1 200 OK (application/gzip)
→	637	84.789491	10.10.31.101	192.229.211.108	HTTP	371 GET /MFEwTzBNMEswSTAJBgUrDg
→	693	85.377744	10.10.31.101	192.229.211.108	HTTP	294 GET /MFEwTzBNMEswSTAJBgUrDg
→	1072	101.166366	10.10.31.101	72.21.81.240	HTTP	340 GET /msdownload/update/v3/stat
→	604	57.732831	10.10.31.101	162.33.179.136	TLSv1.2	236 Client Hello (SNI=asleytomafa.com)
→	79	62.423569	10.10.31.101	162.33.179.136	TLSv1.2	236 Client Hello (SNI=asleytomafa.com)
→	16	57.879565	10.10.31.101	162.33.179.136	TLSv1.2	236 Client Hello (SNI=asleytomafa.com)
→	13	57.997956	10.10.31.101	162.33.179.136	TLSv1.2	236 Client Hello (SNI=asleytomafa.com)
→	47	61.368389	10.10.31.101	162.33.179.136	TLSv1.2	236 Client Hello (SNI=asleytomafa.com)