2024-09-04

1. alert 확인
2. 수상한 활동들 기록

23[.]220[.]251[.]149 => txt 요청 - S1

79[.]124[.]78[.]197 => Koi Stealer C2 - S2

172[.]17[.]0[.]99 + 172[.]17[.]0[.]17 => kerberos principal name overflow - S3

3. S1 필터링

```
▸ Frame 54: 241 bytes on wire (1928 bits), 241 bytes captured (1928 b
▸ Ethernet II, Src: Cisco_51:8c:b6 (00:02:4b:51:8c:b6), Dst: Intel_b6
▸ Internet Protocol Version 4, Src: 23.220.251.149, Dst: 172.17.0.99
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 49766, Seq:
▸ Hypertext Transfer Protocol
▾ Line-based text data: text/plain (1 lines)
    Microsoft Connect Test
```

- 악성 아닌걸로 판단

4. S2 필터링

No.	Time	Source	Destination	Protocol	Length	Info
1668	155.893205	172.17.0.99	79.124.78.197	HTTP	497	POST /foots.php HTTP/1.1
1670	156.538183	79.124.78.197	172.17.0.99	HTTP	222	HTTP/1.1 200 OK
1672	156.539791	172.17.0.99	79.124.78.197	HTTP	516	POST /foots.php HTTP/1.1
1695	157.273715	79.124.78.197	172.17.0.99	HTTP	222	HTTP/1.1 200 OK
1697	157.365533	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
1700	158.024230	79.124.78.197	172.17.0.99	HTTP	222	HTTP/1.1 200 OK
2227	159.998250	172.17.0.99	79.124.78.197	HTTP	145	GET /index.php?id=&subid=qIOuKk7U HTTP/1.1
2232	160.653102	79.124.78.197	172.17.0.99	HTTP	289	HTTP/1.1 200 OK (text/html)
2236	161.227849	172.17.0.99	79.124.78.197	HTTP	159	POST /index.php HTTP/1.1
2238	161.904137	79.124.78.197	172.17.0.99	HTTP	228	HTTP/1.1 200 OK (text/html)
2347	226.462867	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1

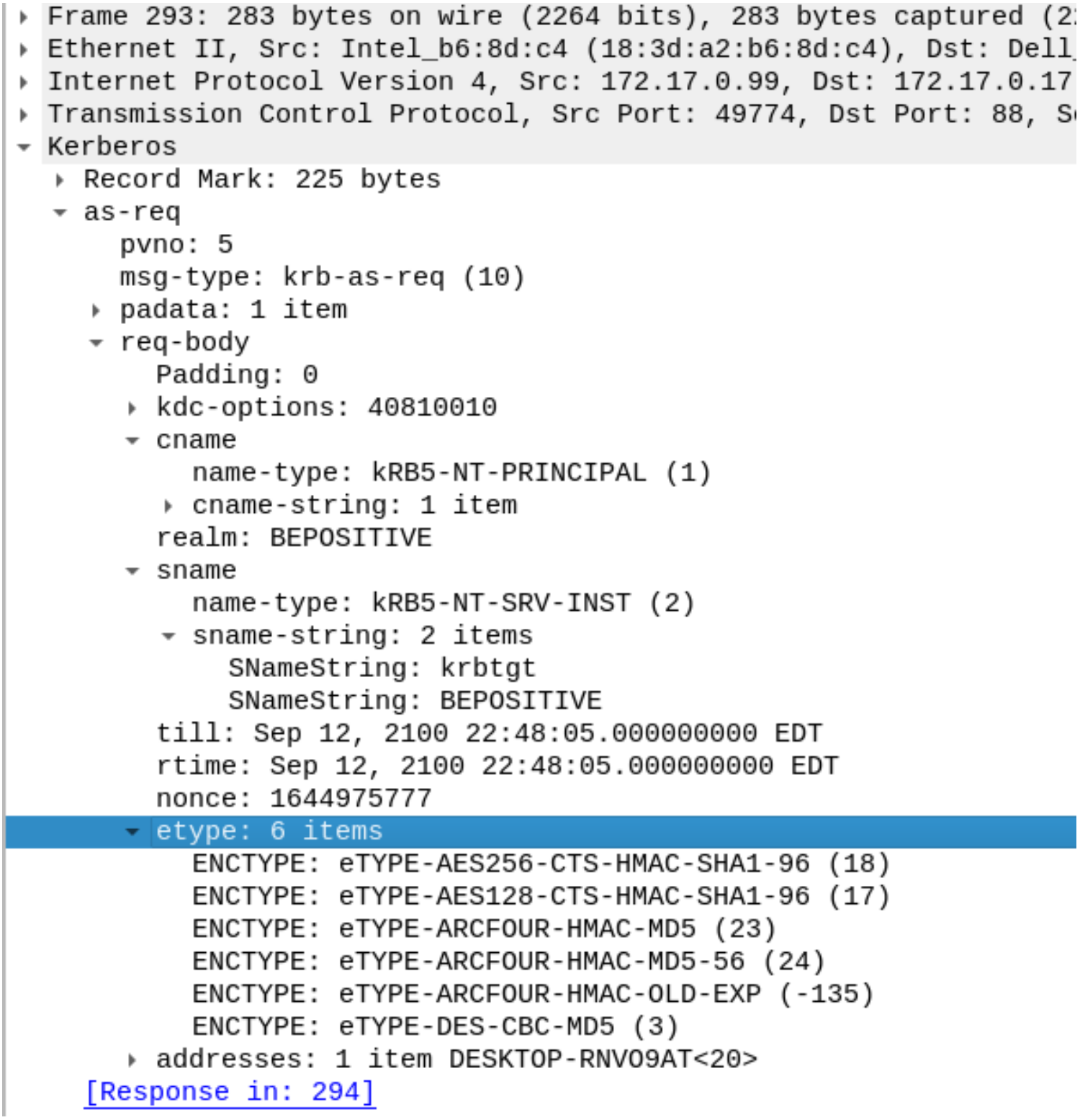
- 2347번 이후 패킷부터는 그냥 같은 내용만 반복

3130327c33303136383231332d336265302d613735312d383161302d6366336232323863383363534

- POST 패킷들을 보면 공통점이 있음

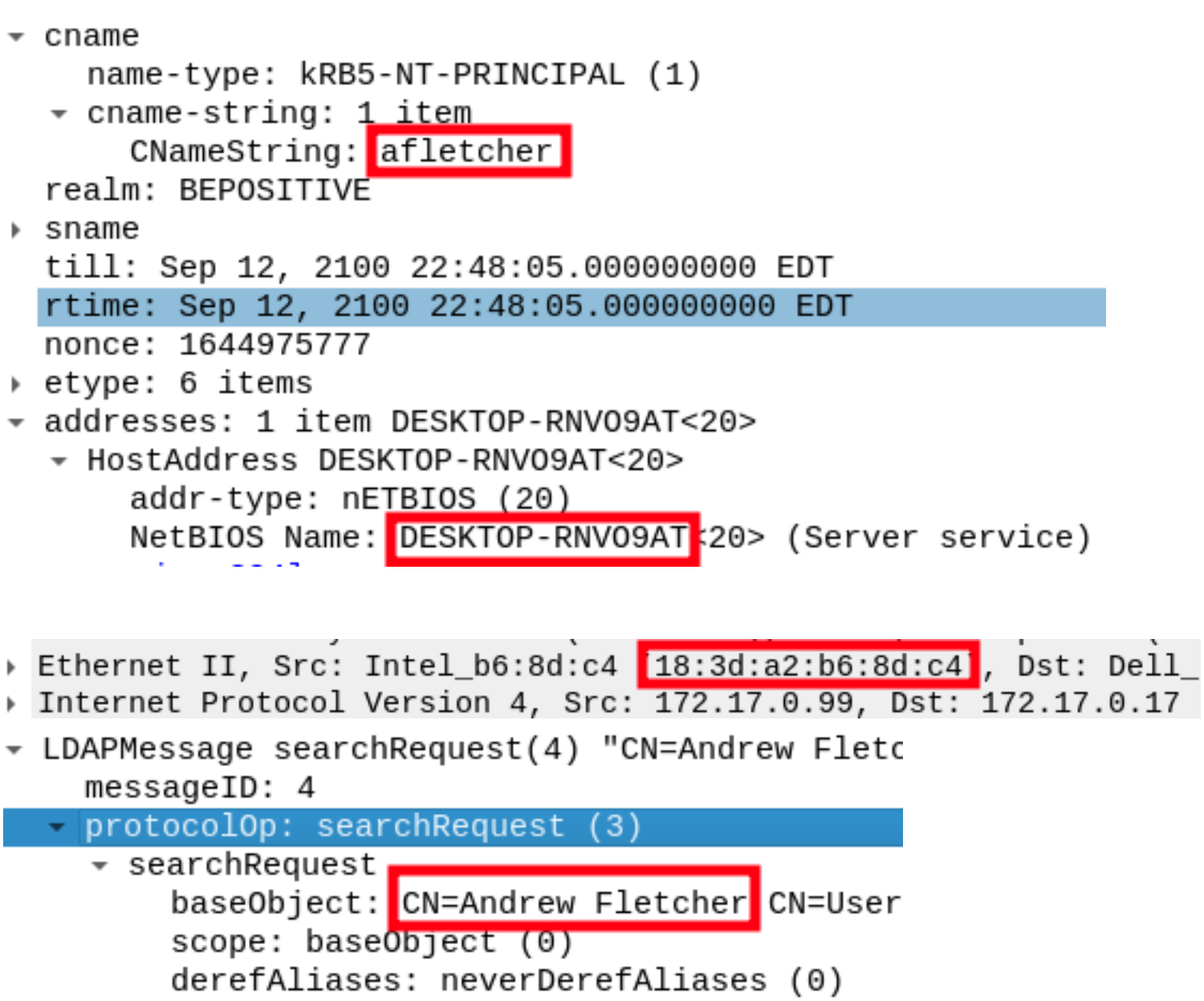
101|30168213-3be0-a751-81a0-cf3b228c8654|

5LHtVruc|f3f3oMg2lz4XGyHy0LidzFiNvSftke//
k+COyrO9aBI=
111|30168213-3be0-a751-81a0-cf3b228c8654|
XHfhyxOtsArXQLiP|=¬ª|U7÷#±/ónåH -øî1
Rm¹UÂO
ÖyBÓÌ\vK¹sâl4ð]7ø´1
Z
102|30168213-3be0-a751-81a0-cf3b228c8654
4. S3 필터
필터: ip[.]src == 172[.]17[.]0[.]99 and ip[.]dst ==
172[.]17[.]0[.]17 and tcp[.]srcport == 49774 and
tcp[.]dstport == 88



- 왜 alert가 발생했는지는 모르겠음

5. 감염된 호스트 정보 추출



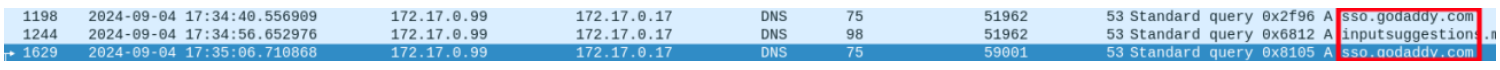
18:3d:a2:b6:8d:c4

DESKTOP-RNVO9AT

afletcher

Andrew Fletcher

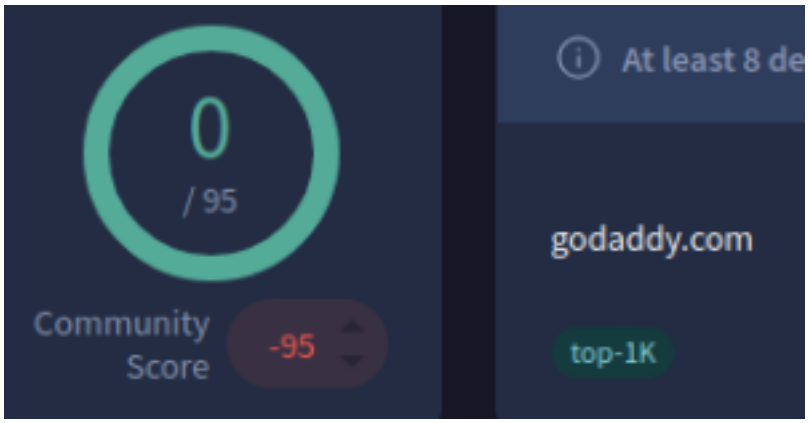
6. 감염경로를 찾기 위해 DNS 기록 확인



7. C2 서버에 연결하기 직전에 검색한 도메인 확인

No.	Time	Source	Destination	Protocol	Length	src port	dst port	Info
1630	2024-09-04 17:35:06.752557	172.17.0.17	172.17.0.99	DNS	168	53	59001	Standard query response 0x8105 A sso.godaddy.com
1631	2024-09-04 17:35:06.752627	172.17.0.99	23.195.212.189	TCP	66	49812	443	49812 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1632	2024-09-04 17:35:06.753489	172.17.0.99	79.124.78.197	TCP	66	49813	80	49813 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
1633	2024-09-04 17:35:06.786405	23.195.212.189	172.17.0.99	TCP	66	443	49812	443 → 49812 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
1634	2024-09-04 17:35:06.786405	172.17.0.99	23.195.212.189	TCP	60	49812	443	49812 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1635	2024-09-04 17:35:06.787464	172.17.0.99	23.195.212.189	TLSv1.2	343	49812	443	Client Hello (SNI=sso.godaddy.com)
1636	2024-09-04 17:35:06.836452	23.195.212.189	172.17.0.99	TCP	60	443	49812	443 → 49812 [ACK] Seq=1 Ack=290 Win=64128 Len=0
1637	2024-09-04 17:35:06.836839	23.195.212.189	172.17.0.99	TLSv1.2	1430	443	49812	Server Hello
1638	2024-09-04 17:35:06.836954	23.195.212.189	172.17.0.99	TCP	1430	443	49812	443 → 49812 [PSH, ACK] Seq=1377 Ack=290 Win=6412
1639	2024-09-04 17:35:06.837066	23.195.212.189	172.17.0.99	TCP	1398	443	49812	443 → 49812 [PSH, ACK] Seq=2753 Ack=290 Win=6412

8. 바이러스 토탈 검색

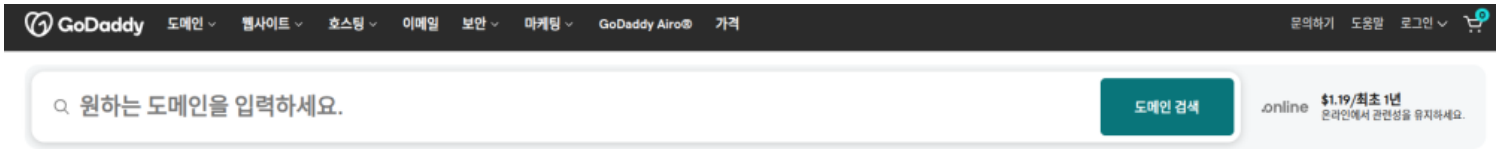


- 악성 사이트가 아니라지만 커뮤니티 스코어가 낮음

9. urlscan 사이트를 이용해서 직접 확인

> **Access Denied**
>
> You don't have permission to access "http://www.godaddy.com/" on this server.
>
> Reference #18.93d71302.1759034684.4c279874
>
> https://errors.edgesuite.net/18.93d71302.1759034684.4c279874

10. 직접 확인



- 도메인을 파는 사이트같음
- 여기 도메인을 사서 C2로 활용한 듯