2020년 5월 10일 일요일

4월 셋째 주(성준)

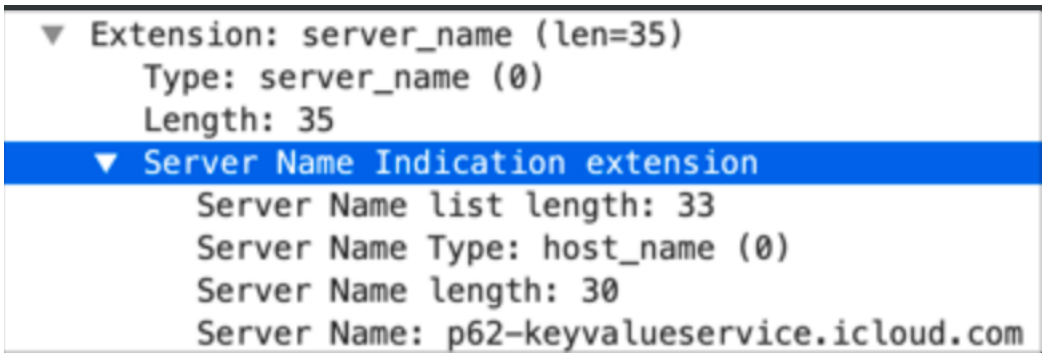
유해사이트 차단 우회

<이번주 진행된 내용>

1. 유해사이트 차단 원리 이해
    1. URL 차단 -> ‘HTTPS’ , ‘VPN’ 사용으로 파훼가능
    2. HTTPS 의 Client hello SNI(Server Name Incation) 필드차단
    3. 블랙리스트에 있는 유해사이트 접근시 ISP에서 탐지하고 RST packet을 보냄
2. 유해사이트 차단 우회 방법 연구.
    1. SNI bypass
        1. Client hello 분할 방법

- SNI 필드 차단은 Client hello packet 의 Server Name Incation 으로 Server Name을 확인하여 차단하는데 Client hello packet 을 분할하여 전송.

- 가끔 사이트 접속시 HTTPS사이트가 HTTP 으로 통신하는 경우 발생(원인 찾는중)



3. RST packet drop
    1. Packet tcp header 의 Reset Flag 를 확인하여 RST 활성상태 파악

- RST packet 발생하지 않는 경우 발생

<다음주 진행 할 내용>

- 조사한 자료 기반으로 SNI bypass, RST drop 코드작성