SNI 필드 불법사이트 차단 우회

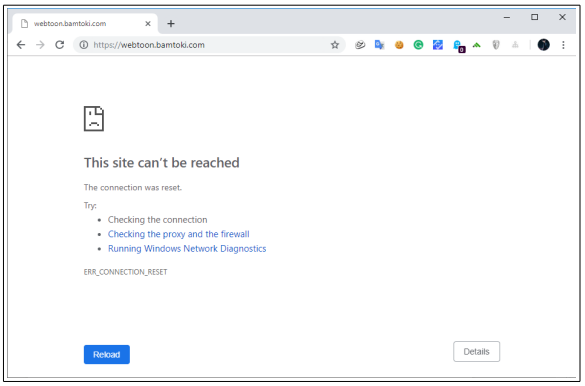
작성자: 최현우(supjerk)

1. Abstract

정부가 이전보다 더욱 강력한 웹사이트 차단 기술을 적용하기 시작했다. 해외 유해 정보 차단 등을 목적으로 하고 있지만, 표현의 자유 위축이나 감청·검열 논란 등을 제기하는 목소리도 있다.

방송통신위원회는 12 일 "불법음란물 및 불법도박 등 불법정보를 보안접속 및 우회접속 방식으로 유통하는 해외 인터넷사이트에 대한 접속차단 기능을 고도화했다"고 밝혔다.
방통위는 "2 월 11 일 방송통신심의위원회의 통신심의 결과(불법 해외사이트 차단결정 895 건)부터 이를 적용한다"고 설명했다. KT·LGU+·SK 브로드밴드·삼성 SDS·KINX·세종텔레콤·드림라인 등 7 개 인터넷서비스제공사업자(ISP)가 이를 적용했다.
새로 도입된 차단 기술은 '서버네임인디케이션(SNI) 필드차단' 방식이다. 정부는 이전에 쓰던 웹사이트 차단 방식이 쉽게 무력화되자 지난해 SNI 필드차단 기술의 도입을 예고했다.
[출처 :
http://news.chosun.com/site/data/html_dir/2019/02/12/2019021201923.html]

2. Introduction



정부는 밤토끼 사건 이후로 DNS 단 차단방식을 이용해 여러 불법사이트를 유해물로 간주, 차단하고 있었지만 1.1.1.1 등의 타 DNS 를 적용하는 시도가 늘어나면서 이 방법 역시 무용지물이 되고, 정부는 다시 이를 막기 위해 SNI 필드에서의 차단을 실시했다. 이를 우회할 것이다.

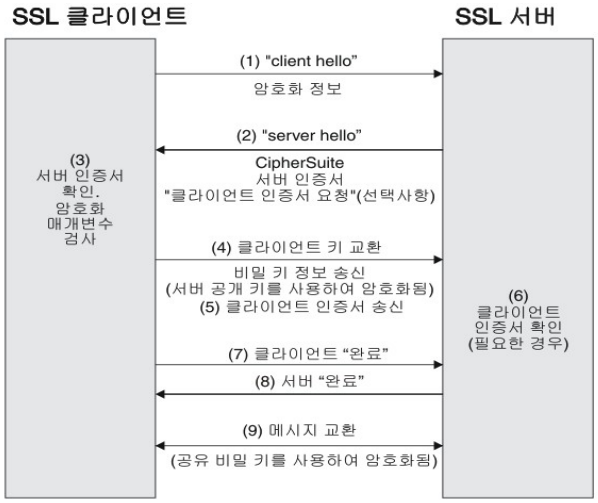
왼쪽은 현재는 막혀있는 밤토끼 사이트다.

2.1 Background

2.1.1 HTTPS

HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer) 는 기존의 HTTP 보안을 강화시킨 버전이며 SSL/TLS 와 함께 쓰이며 기본적으로 포트 번호는 443 으로 설정된다.

2.1.2 SSL/TLS



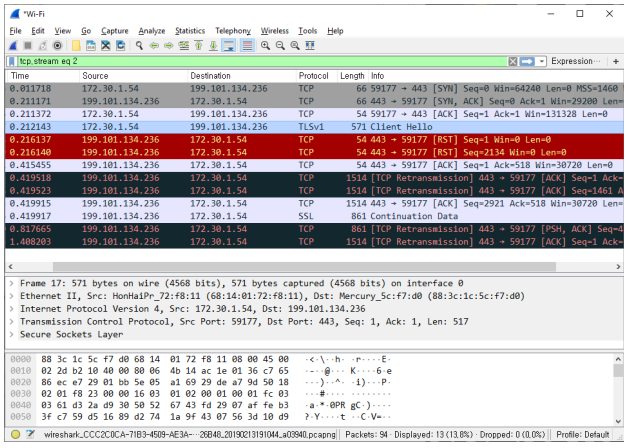
SSL(Secure Socket Layer)는 암호 규약이며 TLS 는 SSL 의 표준화 버전이라 봐도 무방하다. SSL/TLS 는 RSA 등의 대칭키 암호화를 사용해 SSL/TLS Handshake 라는 방식으로 통신한다. 이는 기본적인 TCP 3-way-handshake 가 성공한 뒤에 실행되며 왼쪽 그림 (https://www.ibm.com/support/knowledgecenter/ko/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660a.gif) 과 같은 순서로 실행된다. 부가적인 설명은 Reference 의 SSL/TLS Handshake 를 참고하자.

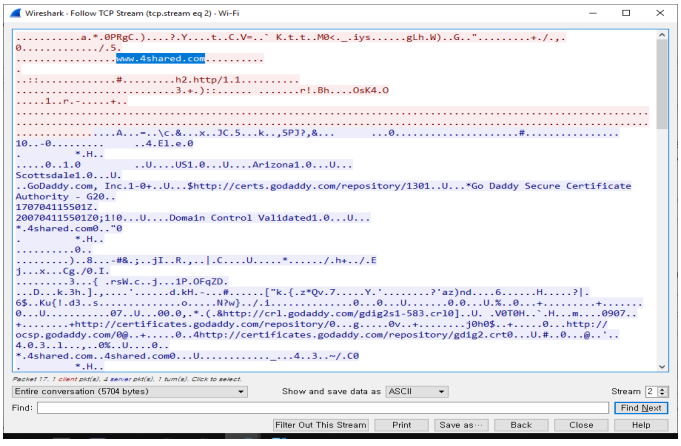
2.1.3 DNS

DNS(Domain Name Service) 는 "www.google.co.kr" 과 같은 IP 로 이루어지지 않은, 도메인의 이름을 IP 로 바꿔 요청해야 할 때 전화번호부와 같이 DNS 에서 원하는 도메인 네임을 아이피로 응답받을 수 있다

2.1.4 SNI

SNI(Server Name Indication)는 하나의 공인 IP 아래 여러 사이트의 SSL/TLS 인증서를 호스팅할 수 있게 하는 방법이다. 이는 보통 호스팅 회사에서 일어나며 "인증서 선택" 이라는 문제를 타파시킬 수 있는 해결법이다. 일반적으로 CLIENT HELLO 에 웹사이트의 호스트 이름을 기재한다. 아래 사진들은 SNI 가 평문으로 전송되는 모습이다.





3. Bypass Methodology

방법론의 설명에 앞서 2/11/2019 부터 적용된 불법사이트 차단방식의 개요에 대해 다시 짚고 넘어가겠다.

핵심은 “CLIENT HELLO 의 SNI 필드를 검사해 유해 사이트인지 확인한다.” 이다. 이것만 알면 제대로 우회할 수 있다.

3.1 Client Hello data fragmentation (Checked)

정부는 기본적인 DPI(Deep Packet Inspection)의 기능만 구현해 사용하고 있다. 이로 인해 CLIENT HELLO 가 대부분 한 패킷 안에 담기는 경우를 고려해 첫번째 CLIENT HELLO 만 검사한다.
이는 CLIENT HELLO 를 분할해 SNI 필드를 첫번째 패킷 이후에 전송한다면 간단히 우회할 수 있다.

3.1.2 Adjust MTU (Checked)

3.1 의 응용본이다. 기본적으로 TCP 통신의 MTU(maximum transmission unit)는 1500 바이트로 설정돼 있다. CLIENT HELLO 를 여러 패킷으로 분할해 보낼 수 있도록 약 300~400 바이트로 설정한다면 역시 간단히 우회할 수 있다. 다만 이는 패킷의 수가 다량 증가한다는 단점이 존재한다.

3.2 Use DNS over HTTPS&ESNI(Checked)

기본적으로 DNS 에서 아이피를 요청할 때 이루어지는 과정은 이전의 HTTP 시절과 동일하다.
다만 DoH(DNS over HTTPS)를 사용해 HTTPS 처럼 SSL/TLS 를 사용함으로 SNI 를 암호화 시킬 공개키를 받아와 SNI 를 대칭키 암호화시키는 것이다.
이렇게 한다면 SNI 필드 역시 도청/감청할 수 없는 상황에 놓인다.

3.3 Alphabet Trick(UnChecked)

SNI 필드를 대/소문자 데이터로 난해하게 변경하고 SNI 이전에 공백을 몇번 주는 것만으로도 간단히 우회가 가능해 보인다. (지금 상태는 그만큼 허술하다.)

3.4 Use VPN

외국 VPN(Virtual Private Network)을 사용함으로서 통제 자체를 벗어나는 것이다. 다만 이는 제한적인 속도, 한국에서만 지원하는 서비스는 이용 불가, 익명성 보장 불가 등 단점도 여럿 존재한다.

4. Conclusion

지금 현재 정부가 적용한 차단 방식은 기본적인 기능만 적용돼 있는 상태이며 이는 간단한 기술, 트릭들로 쉽게 우회할 수 있다. 사실 이를 정부가 제대로 대응하며 막는다 해도 VPN 등 최후의 보루는 언제까지나 남아있다. 암시장에서 특정 주파수대로 통신하며 유해물을 거래하는 등을 시도하면 사실 정부는 막을 방법도 없다. 정부가 통제하면 통제할 수록 습득인과 비습득인의 차이가 명백하게 나버린다. 정부는 이를 심히 여겨 판단해야 할것이다.

Reference

https://www.pickaweb.co.uk/kb/what-is-https/ - What is HTTPS?
https://github.com/ValdikSS/GoodbyeDPI -
https://ko.wikipedia.org/wiki/%EC%A0%84%EC%86%A1_%EA%B3%84%EC%B8%B5_%EB%B3%B4%EC%95%88 – 전송 계층 보안
https://hanjungv.github.io/2017-11-07-1_CS_SSL/ - SSL/TLS Handshake

https://www.ibm.com/support/knowledgecenter/ko/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm – SSL/TLS Handshake
https://tools.ietf.org/html/rfc3546#section-3.1 – What is SNI?
https://www.globalsign.com/en/blog/what-is-server-name-indication/ - What is SNI?
https://www.youtube.com/watch?v=7V2aUErljjU – SNI 필드 차단 우회 (data fragmentation)