쉽게 읽는 보안기술

SSL/TLS 트래픽의 보안 허점, 해결 방안은?

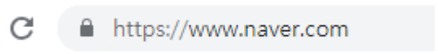
– SSL 가시성 확보 복호화 솔루션!

2019.03

SOMANSA

주소창 옆 작고 앙증맞은 자물쇠 하나,
바로 SSL/TLS

구글 지메일, 네이버 웹메일, 구글 드라이브, 드롭박스, 인스타그램, 페이스북 등…
하다 못해 일반기업/기관 홈페이지와 NGO단체 홈페이지까지…
우리가 사용하는 대부분의 웹서비스들은
대부분 SSL/TLS 기반으로 만들어져 있습니다.
주소창 옆에 작고 앙증맞은 자물쇠 하나가 새초롬하게 달려있죠.
HTTPS라고 하면 더 이해하기 쉬울까요?



SSL/TLS,
원래 금융기관에서 주로 사용했던 기술

SSL/TLS는 기존 HTTP의 한계를 상쇄하기 위해 도입되었습니다.
왜냐하면 HTTP에서는 패킷이 그대로 보였기 때문입니다.
오고 가는 패킷 속에서 비밀번호, 인증번호 등이 노출되면 안됐거든요.
해커들이 탈취할 수 있으니까요.

그래서 SSL/TLS는 인증서, 비밀번호가 탈취되면 치명적인 결과를 초래할 수 있는
은행, 증권, 보험 등의 금융 기관에서 주로 사용했던 기술입니다.

이미지 구매처 : 클립아트코리아

패킷의 송수신이 그대로 보이는 HTTP 프로토콜,
도감청의 위험 있어

하지만 시간이 지날수록 개인정보, 기밀정보에 대한 관심이 두드러졌고
실제로 해커들이 패킷이 송수신되는 채널에 몰래 도청장치를 심어놓고
패킷을 관찰 또는 가로채는 일까지 벌어졌습니다.
(이를 패킷 스니핑이라고 하죠)

암호화된 패킷이 송수신 되는 SSL/TLS,
도감청의 위험 없어

정보유출을 걱정한 보안 담당자들은
서둘러 모든 패킷이 암호화되어 오고 가도록 웹서비스를 변경했습니다.

그것이 바로 SSL/TLS입니다.

SSL/TLS가 적용되면 서버와 클라이언트 PC 사이에 둘만의 암호를 가져
그 외의 사람들은 알아볼 수 없게 됩니다.
해커가 패킷을 가로채는데 성공하더라도
암호화처리 되어 있기 때문에 패킷을 봐도 뭐가 뭔지 알 수 없지요.

SSL/TLS 암호화 트래픽은
이제 전세계 프로토콜의 72%를 차지

원래 2015년 기준으로 SSL/TLS 기반 웹서비스는
전세계 프로토콜의 25% 정도 밖에 되지 않았습니다.
국내는 도입속도가 이보다 더딘 편이었습니다.
그런데 어느 순간부터
다음 웹메일, 네이버 웹메일이 SSL/TLS 기반으로 변신을 시작하더니
다른 웹서비스도 하나하나 SSL/TLS 기반으로 바뀌기 시작했습니다.

왜냐하면 구글에서 SSL/TLS를 적용하지 않은 사이트들은
'주의 요함: 이 사이트에 접속하는 접속자는
신용카드번호, 비밀번호를 도난당할 수 있음'으로 무섭게 표시했거든요.

포티넷의 2018년 3분기 '글로벌 보안 위협 전망 보고서'에 따르면
SSL/TLS 트래픽은 이제 전체 네트워크 트래픽의 72%이상을 차지한다고 합니다.
금융, 정보통신, 클라우드 등 보안이 중시되는 산업은
이미 80%이상 적용이 완료되었고요.
3년 사이에 약 3배 증가한 셈입니다.

스니핑 위험에서는 벗어났지만…
DDos, APT, 악성코드 공격은?

자, 이제 패킷이 암호화되어 송수신 되니 해커의 정보탈취 위험에서는 벗어났습니다.

스니핑 위험에서 벗어났어요!

하지만 해커가 SSL/TLS 웹서비스를 이용해서 역으로 공격을 한다면 어떻게 될까요?
암호화된 패킷이 클라이언트 PC로 전송되기 때문에
송수신자간의 데이터 교환이 일어나는 발생하는 일에 대해서는 깜깜해집니다.
즉 개인정보 유출이나 DDos, APT, 악성코드 공격이 발생할 경우 무력화됩니다.
무엇이 클라이언트PC로 들어왔는지
네트워크에서는 네트워크 보안장비가 파악할 수 없기 때문입니다.

그래서 네트워크 보안장비, DDos, APT 대응장비 및 IPS, IDS 장비들이
제 기능을 발휘하지 못 합니다.

사태를 파악했을 때는 이미 공격을 당한 이후겠죠.

이미지 구매처 : 클립아트코리아

실제로 20만대 이상의 악성코드를 제어하는 C&C서버들이 SSL을 사용하고 있습니다.
기업을 타깃으로 한 네트워크 공격의 50%이 이상이
SSL 트래픽을 이용한다고 합니다.
유명한 랜섬웨어, 봇넷, 루트킷 등은 SSL을 이용하여 공격을 하고 있습니다.

하지만 기존 보안 솔루션은 SSL 가시성을 확보하지 못하고 있죠.

패킷이 암호화되었기 때문에 DLP 솔루션은 내용기반 통제가 안되고
유해사이트 차단 솔루션은 사이트의 차단이 어렵습니다.
IPS/IDS 솔루션은 내가 무슨 공격을 Bypass 했는지도 모를겁니다.

SSL/TLS 복호화 및 가시성 확보 필요

이러한 상황에서 가장 필요한 것은
바로 SSL/TLS를 복호화해 가시성을 확보하는 기술입니다.

SSL/TLS를 통해 들어오는 패킷을 클라이언트 PC로 들여보내기 전에 복호화한다면
해당 패킷이 평범한 정보인지
아니면 나쁜 마음을 먹고 들어오는 해킹공격인지 파악할 수 있을테니까요.

게다가 개인정보가 유출된 후에 후회하는 것보다
아예 패킷을 모두 확인하고 사전에 차단하는게 낫지 않을까요?

시중에 나와있는 SSL/TLS 복호화 솔루션은
443포트를 중심으로 검사하고 복호화하여 보안솔루션에 제공합니다.
보안 솔루션은 정상적인 패킷인지 확인한 후
이를 클라이언트 PC로 중개할지 말지 결정을 합니다.

조금 더 고도화된 기능을 적용한 솔루션의 경우

1. 인라인(DLP, IPS, SWG)/미러링(악성코드분석, IDS, 포렌식, APT) 연동방식 지원
2. 인증서 자동배포
3. 세션 투명성 보장: 출발지 IP/PORT, 목적지 IP/PORT의 정보변경 없이 유지
4. 다양한 암호화 프로토콜 커버: HTTPS, SMTPS 등
5. H/W, S/W 바이패스 기능: 장애가 발생할 경우
   바이패스 또는 소프트웨어 자동복구 기능으로 가용성 보장
6. 이슈분석 자료 제공: SSL/TLS 처리이슈 발생시 디버깅정보 및 pcap파일 다운로드

같은 기능을 제공하기도 합니다.

소만사의 SSL/TLS 복호화
및 가시성 확보 솔루션은
기획단계부터 보안솔루션과의 일체화를 염두

소만사의 SSL/TLS 트래픽 가시성 확보 솔루션 <T-Proxy v1.0>은
기획단계부터 보안솔루션과의 일체화를 목표로 삼았기 때문에
외산대비 패킷처리 성능이 30%이상 우월합니다.

그렇기 때문에 IPS, APT, IDS, DLP, SWG, 포렌식 장비 등과 연동해도
성능저하가 없습니다.

네트워크의 흐름은 이제 SSL/TLS!
데이터 송수신에서의 보안위험을 차단하기 위해
복호화 솔루션이 반드시 필요

기껏 암호화한 트래픽을 다시 복호화하다니,
아이러니하다고 생각할 수 있겠습니다.

하지만 시대의 흐름은 이미 SSL/TLS로 바뀌었습니다.
그렇기에 패킷스니핑의 위험을 차단하기 위해서라면 암호화는 필수적인 것이고
데이터 송수신에서 발생하는 보안위험을 차단하기 위해서라면
복호화 역시 필수불가결한 것이라 생각합니다.

변화하는 환경 속에서 끊임없이 발생하고 있는
보안의 허점을 찾아내고 차단하기 위해
소만사는 오늘도 고군분투하고 있습니다.

개인정보보호 전문기업 소만사
Website: www.somansa.com
Tel: 02-2636-8300
Mail: privacy@somansa.com

SOMANSA