DNS 서비스 제공자의 보안접속 악용 사례와 대응

고남현O
O한국방송통신대학교 컴퓨터과학과
e-mail: gnh1201@knou.ac.krO

Response to SSL communication abuse cases by DNS service providers

Namhyeon GoO
ODept. of Computer Science, Korea National Open University

● 요 약 ●

오늘날 도메인 네임 시스템(DNS) 서비스는 단순히 IP 주소를 .com, .net 등의 도메인으로 변환해주는 기능을 넘어 컨텐츠 가속(CDN) 서비스, 고가용성(HA) 서비스, 분산 서비스 거부공격(DDoS) 방어 서비스, 통신 구간 암호화 서비스로서 그 용도를 넓혀가고 있다. 이용자들은 이러한 업체가 외부 기관에 정보를 넘기지 않고, 모든 통신 구간은 서비스 업체도 그 내용을 들여다보지 못할 정도로 철저히 암호화한다는 도덕적인 영업과 운영을 할 것으로 기대하지만, 실제 사례를 살펴보면 그렇지 못하다는 점이 드러난다. 본 논문에서는 2021년 기준으로 최소 7년간 이어져온 것으로 추정되는 유명 DNS 서비스 업체의 보안접속 악용 사례를 중심으로 이러한 악용이 어떻게 이루어지고 이것에 대응하기 위해 사용할 수 있는 표준화 기술은 이 문제에 효용성이 있는지를 DNS 업체와 동일한 실제 환경 구성을 통해 검증하였다.

키워드: 도메인 네임 시스템(DNS), 보안접속(SSL), 보안접속 납치(SSL Hijacking)

I. 개요

오늘날 도메인 네임 시스템(DNS)은 IP 주소를 도메인으로 변환해주는 본연의 기능을 넘어 컨텐츠 가속, 고가용성, 공격 방어 등의 다양한 기능을 제공하고 있다. 하지만 DNS의 역할이 커지면서 DNS 서비스 업체의 신뢰성에도 의문이 커졌다. DNS 서비스 제공자는 IP 주소와 도메인 사이의 변환을 담당하는 중간 역할로서 개입할 수 있는 모든 행위를 할 수 있는 위치에 있다. 컨텐츠를 임의로 차단하거나 변경할 수도 있고, 더 과감하게는 이용자 사이의 암호화 통신도 일부 복호화할 수 있다.

이것은 DNS 서비스 제공자가 컨텐츠 소비자와 생산자의 중간자로서 가지는 지배적 역할에서 비롯된 단순한 의심으로만 치부되었지만, 최근 들어 이러한 역할의 특징을 적극적으로 활용한 사례가 나오고 있어 논란이 되고 있다.

II. 선행연구

2.1. 리버스 프록시 (Reverse Proxy)

역방향 프록시는 사설 네트워크에서 방화벽 뒤에 위치하여 클라이언트의 요청을 적절한 백엔드 서버로 전달하는 프록시 서버의 유형이다. 로드 밸런싱(Load Balancing), 웹 가속(Web acceleration), 보안 및 익명성 확보 등의 목적으로 쓰인다.[1]

2.2. HSTS (HTTP Strict Transport Security)

HTTP Strict-Transport-Security response header (종종 HSTS로 약칭)는 HTTP 대신 HTTPS만을 사용하여 통신해야 한다고 웹 사이트가 브라우저에 알리는 보안 기능이다.[2]

2.3. SSL 인증서

SSL(보안 소켓 계층) 인증서는 브라우저 또는 사용자의 컴퓨터와 서버 또는 웹사이트 간에 암호화된 연결을 수립하는 데 사용한다. SSL 연결은 인증되지 않은 사용자의 방해로부터 각 방문(세션) 중에 교환된 중요한 데이터(예: 신용카드 정보)를 보호한다.[3]

III. 제안방법

3.1. 공격 측 방식

3.1.1. 제휴사를 통한 DNS의 배포

일반적으로, 인터넷 서비스 제공자(ISP) 등의 DNS가 아니라면 컴퓨터 사용자가 수동으로 DNS를 설정하도록 하여야 한다. 하지만 안티바이러스(Antivirus) 및 이와 유사한 보안업체와의 제휴를 통해 DNS를 자동으로 변경하는 방법이 있다. 기존에 신뢰를 얻은 고객들을 대상으로 DNS를 배포할 수 있다.

3.1.2. 리버스 프록시 구축

리버스 프록시를 위해 많이 사용되는 NGINX를 이용하여, 국내외 포털 및 주요 기업 웹 사이트를 프록시 목적지로 하는 리버스 프록시 서버를 구축하였다. 예를 들어, reddit.com, microsoft.com, naver.com 등을 목적지로 설정한다. 여기서는 “victim.com”으로 설정한 것으로 가정한다.

3.1.3. 자체서명(Self-signed) 인증서 발급

이후, 리버스 프록시 서버에는 OpenSSL를 이용하여 임의의 자체서명(Self-signed) 웹 SSL 인증 발급받은 뒤 NGINX에 적용한다. 인증서를 발급할 때 발급 대상의 도메인을 뜻하는 CN(Common Name)은 “search.example.org”로 설정한 것으로 가정한다.

3.1.4. 가짜 DNS 설정

실제 DNS 서버가 없으므로, 클라이언트에서 DNS 역할을 가짜로 수행해줄 `hosts` 파일을 수정하여 (3.1.1)에서 설정했던 주요 기관과 기업 사이트의 도메인이 프록시 서버를 지칭하도록 한다.

가령, “victim.com 127.0.0.1”으로 설정한다.

3.1.5. 클라이언트가 웹 사이트에 접속

클라이언트가 “victim.com”으로 접속하면 이전에 (3.1.2)에서 발급받았던 인증서의 도메인과 이름이 다르므로(“victim.com”과 “search.example.org”는 불일치) 클라이언트는 웹 브라우저로부터 SSL 경고를 받을 수 있다. 여기서 클라이언트가 인증서 경고를 대수롭지 않게 여겨 무시하기를 기다린다.

3.1.6. 정보 취득 및 증거 지우기

이미 “victim.com”에 도착하기 전에 리버스 프록시 서버(“search.example.org”)를 거치므로 SSL 암호화를 무력화하고 사용자가 의도했던 정보를 취득하는 결과를 얻을 수 있다. 이후 (3.1.3)에서 설정하였던 가짜 DNS에 등록된 IP와 도메인 정보를 해제하면 앞서 설명한 과정이 같은 접속 환경에서 재현되지 않음으로서 감청의 증거를 지울 수 있다.

3.2. 방어 측 방식

3.2.1. HSTS 적용

공격 측인 DNS 공급자에 의해 “victim.com”이 임의의 리버스 프록시 서버(“search.example.org”)를 거치는 것을 막을 순 없다. 단, HSTS가 적용된 웹 사이트는 웹 브라우저가 도메인이 불일치한 경우 지속적으로 정상적인 도메인으로 리다이렉션(Redirection)을 시도하므로 방어 관점에서 효과가 있다.

IV. 결론

이와 같은 방법으로 이용자들의 보안접속(SSL) 통신 내용을 가로채오던 DNS 업체는, 국내에서도 전투기 개발 등으로 인지도가 높은 군사 기술 연구개발 기업 ‘L’사의 자회사이다.

이러한 SSL 통신 가로채기의 중심이 된 특정 서버(“search.dnsadvantage.com”)의 경우[4], 구글 검색 2021년 12월 기준 SSL 악용 사례가 의심된다고 주장하는 자료가 28,300건 검색된다.

이러한 행위가 군사 목적에 의한 것인지 마케팅 목적의 일환인지는 확인할 수 없으나 DNS 서비스 제공자의 지위를 남용한 것은 우려스럽다.

REFERENCES

[1] NGINX, https://www.nginx.com/
[2] Mozilla MDN, https://developer.mozilla.org/
[3] Digicert, https://www.digicert.com/
[4] Github, https://github.com/gnh1201/dns-disadvantage