청와대 등 주요 인터넷사이트 동시다발 DDoS 공격에 불통 충격

2009.07.08 01:12:39 / 이유지 기자 yjlee@ddaily.co.kr

관련기사

데이터센터, DDoS 공격으로 대책마련에 분주
백신업계도 DDoS 공격 대응 '비상'
1 만 8000 대 좀비 PC 가 청와대 공격
포털 업계, 네이버 서비스 중단에 '긴장'
DDoS 공격, 금융권 비상체제 가동
범정부 DDoS 특별대응체계 긴급 가동
"손쓸틈도 없이" DDoS 공격에 무방비… 이용자 PC 백신 설치가 최선

특정 사이트만 집중공격, 1.25 인터넷 대란과는 성격 달라

- 국회 · 네이버 · NHN · 옥션 · 신한은행 등 서비스 접속 장애 또는 불안

청와대와 국회, 한나라당, 네이버, 옥션 등 국내 주요 대형 인터넷 사이트가 동시에 분산서비스거부(DDoS) 공격을 받아 서비스가 마비되는 사태가 발생했다.

7 일 오후 6~7 시부터 8 일 자정이 지난 현재, 청와대와 국회, 포털사이트 네이버의 이메일과 블로그 · 옥션 · 조선닷컴 · 신한은행 · 외환은행 등 국내 사이트가 접속이 안되거나 불안한 상태다.

방송통신위원회와 한국정보보호진흥원(KISA)은 이날 오후 7 시경부터 이들 주요 인터넷 사이트에 서비스가 중단되는 현상이 발생하자, 긴급히 상황 분석 작업을 벌였다.

그 결과, 대량 유해 트래픽을 수반하는 DDoS 공격으로 인해 국내 일부 사이트에 대한 인터넷 접속이 지연되거나 접속이 되지 않는 것으로 파악했다.

조선닷컴은 8 일 12 시 38 분에 "7 일 오후 6 시 20 분쯤부터 4 시간 30 분동안 국적불명의 해커에 의한 DDoS 공격으로 추정되는 해킹을 당해 사이트 접속이 불가능한 상태에 빠졌다"며, "해킹 발생 직후부터 최선을 다해 서비스 장애를 복구했지만 일부 지역에 접속장애가 지속되고 있다"고 공지했다.

이번 DDoS 공격은 보안이 취약한 PC 를 경유한 사이버 공격으로, 국내 특정사이트에 대한 접속이 불안정한 상태이다.

이에 KISA 는 8 일 자정 현재 국내 인터넷서비스사업자(ISP)와 협력해 DDoS 공격을 유발하는 중간 명령 제어 서버를 파악하고 있다.

이번 DDoS 공격은 인터넷 이용자들의 특정 웹 사이트에 대한 접속만을 어렵게 한다는 점에서 인터넷 접속 자체를 불가능 하게 하였던 1.25 인터넷 침해사고와는 다른 것으로 분석하고 있다.

DDoS 공격의 배후에 대해서는 아직 정확히 알려지지 않았으며, 사법기관과 공조를 통해 파악 중인 것으로 알려졌다.

방통위 관계자는 “현재 DDoS 공격으로 국내 6~7 개 사이트 접속이 안되거나 불안한 것으로 파악되고 있다”며, “특정사이트를 대상으로 공격을 벌이고 있어 과거 1.25 대란처럼 인터넷 서비스가 마비되지는 않을 것으로 예상되며, 현재 공격 근원지를 파악 중”이라고 설명했다.

KISA 는 인터넷 이용자들은 자신의 PC 가 이와 같은 DDoS 공격의 근원지로 악용되지 않도록 백신 소프트웨어를 통한 주기적인 악성코드 점검과 윈도 최신 보안패치를 당부했다.

최근 DDoS 공격을 유발하는 악성프로그램인 봇(BOT)에 감염되지 않기 위해서는 윈도 보안패치를 설치하고 백신프로그램을 최신패턴으로 업데이트해야 한다.

KISA 인터넷침해사고대응지원센터는 기술적인 지원이 필요한 인터넷 사용자에게 보호나라 홈페이지(http://www.boho.or.kr)를 방문하거나 인터넷침해사고대응지원센터 전문상담 직원의 도움(전화 118)을 받을 수 있다고 밝혔다.

<이유지 기자> yjlee@ddaily.co.kr