방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2011. 3. 4.(금)

보도자료

2011년 3월 4일(금) 배포 시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 네트워크정보보호팀 박철순 팀장 (☎750-2750)
네트워크정보보호팀 이상국 사무관 (☎750-2757) sklee@kcc.go.kr

18:30분경 추가 DDoS공격 발생, 실질적 장애는 없는 수준

- 정부 및 민간 신속 합동 대응 중, 이용자들의 주의 요망 -

□ 정부는 18:30분으로 예상되었던 DDoS공격이 시작되었음을 확인하여 정부 및 민간이 함께 적극 대응하고 있으며, 기 구축된 DDoS 대응 체계에서 감내할 수 있는 수준의 공격으로 실제 서비스 장애를 일으키고 있지 않는 것으로 파악되고 있다고 밝혔다.

□ 정부는 3.3일 07:50 청와대·국방부 등 국가·공공기관 등 홈페이지에 대한 DDoS 공격시도를 탐지, 긴급 차단하는 한편 국내 유관기관과 함께 비상대응체제를 가동하고 있다.

□ 금일(3.4) 10:00 및 18:30분에 추가 공격이 있음을 사전에 인지하여 관련부처 합동으로 '사이버위기 평가회의'를 개최, 10:00부로 사이버 위기 경보를 '주의'로 2단계 상향 조정하였으며 全 국가·공공기관은 물론 KT, SKB, LG U+ 등 국내 주요 ISP에도 긴급 전파하여 대응토록 하였다.

o 사고발생 탐지 즉시, 금번 공격에 사용된 악성 프로그램 샘플을 입수·분석, 공격 대상기관의 인터넷주소와 과도한 트래픽을 유발하는 악성코드가 내포되어 있음을 확인하였다.

o 이에 긴급 전용백신을 배포하고, 악성프로그램의 샘플 및 분석 결과를 안철수연구소·하우리 등 백신업체에도 제공하여 백신개발을 독려하는 등 민간 전문업체와 공조체제를 가동했다.

□ 또한, 정부는 예상되는 추가공격에 대비하여

o 3월 4일 14:00 '국가사이버안전 실무회의'를, 16:00에는 관련부처(11개 기관)로 구성된 '국가사이버안전 대책회의'를 개최, DDoS 대응장비 정상 가동 여부 및 위기대응 매뉴얼에 따른 부처별 조치사항 등 국가차원의 비상대책을 점검하였다.

o 방통위는 네이버, 다음, 옥션 등 민간분야에 대한 사고조사 및 대응책 마련과 함께 주요 ISP, 백신사와 민간 DDoS 긴급대응 회의를 열고 실시간 공격 차단체계를 유지하고 있으며, 국방부는 사이버사령부를 중심으로 24시간 대응체제를 가동하고 있다.

o 행안부는 관계 전문가로 구성된 사이버안전협의회를 긴급 소집하였으며, 정부통합전산센터를 중심으로 비상대응체제를 가동하고 유관 중앙부처 및 지자체에 사이버 침해대응 상황실 설치와 24시간 비상근무체계로 전환토록 하여 대규모 디도스 공격대응에 만전을 기하고 있다.

o 또한, 금융기관들도 정부와의 유기적인 협조와 대응시스템으로 인터넷 뱅킹, 사이버 트레이딩 등 대고객 서비스를 정상적으로 제공하고 있다.

□ 금번 사태와 관련하여 정부문서가 유출되거나 업무가 마비되는 등의 피해는 없었으며 현재 각 부처는 국가업무를 정상적으로 수행중이라고 밝혔다.

□ 한편, 정부는 DDoS 공격에 이용된 감염 PC는 수일 후 PC의 하드 디스크를 손상시키는 것으로 알려져 이용자들의 적극적인 예방 및 치료 노력이 필요하다고 당부했다.

o 인터넷 이용자들은 주요 포탈(네이버, 다음 등), 주요 ISP업체(KT, SKB, LG U+ 등), 안철수연구소(www.ahnlab.com), 하우리(www.hauri.co.kr), KISA 보호나라(www.boho.or.kr, www.krcert.or.kr) 홈페이지를 방문하여 DDoS 공격 악성코드를 치료하는 전용백신을 설치하는 등 철저한 주의를 기울이는 것이 필요하다. 끝.