방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2011.3.15.(화)

보도자료

2011년 3월 15일(화) 배포 시점부터 보도하여 주시기 바랍니다.

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

정부, 사이버 위기경보 해제 (주의→정상)

정부는 대규모 DDoS 공격에 대응하여 지난 3월 4일 10시부로 발령한 사이버 위기 경보('주의' 단계)를 3월 15일(화) 18시를 기해 해제한다고 밝혔다. 3차례의 DDoS 공격이 이미 종결되었고 악성코드에 의한 PC 하드디스크 손상 관련 신고도 일단락되었을 뿐만 아니라 새로운 공격 징후도 더 이상 발견되지 않는다는 점을 고려하여 위기 경보를 해제한 것이다.

※ 사이버위기 경보 단계는 '관심→주의→경계→심각'으로 구분('09. 7.7 DDoS 공격 시에도 '주의' 경보 발령)

정부는 3.4 DDoS 공격과 관련하여 한국인터넷진흥원(KISA)을 통해 공격로그 기록을 광범위하게 수집하여 정밀 분석한 결과, 동원된 좀비 PC가 총 116,299대에 달하는 것으로 최종 집계되었다고 발표하였다. 이는 3월 6일(일)까지 수집된 로그 기록을 분석하여 잠정 집계한 후 3월 7일(월) 아침에 발표한 77,207대보다는 증가된 것으로써 7.7 DDoS 공격시의 115,044대와 비슷한 수치이다. 7.7 DDoS 공격 때와 달리 금번의 악성코드에 감염된 좀비PC들은 공격 종료 시점이 없어 전용 백신에 의해 치료되거나 삭제 프로그램에 의해 하드디스크가 손상되지 않는 한 공격을 계속 하도록 되어 있어 후속 모니터링을 통해 공격 로그 기록을 지속적으로 수집할 수 있었고 공격대상 사이트에서

3월 6일(일)까지 수집되지 못한 로그 기록이 추가되면서 차이가 나게 된 것으로 분석되었다.

※ 3.4 DDoS에 동원된 좀비PC 대수 : 116,299대 (중복 IP 제외)
① 3월 4일 10시 1차공격(29개 사이트) : 24,696대
② 3월 4일 18시30분 2차공격(40개 사이트) : 51,434대
③ 3월 5일 오전 3차공격(29개 사이트) : 50,402대
- 27개 사이트는 10시45분, 2개 사이트는 8시에 공격시작

또한, 정부는 PC 하드디스크 손상과 관련하여 총 756건이 신고되었다고 밝히고 이 신고 건수는 7.7 DDoS의 PC 하드디스크 손상 관련 신고가 1,466건 접수된 것에 비해 절반에 불과한 것으로써 7.7 DDoS 당시에는 특정 조건이 만족되어야 PC 하드디스크가 손상되었던 점을 감안하면 상당 수준 피해가 줄어들었다고 평가하였다.

그리고 정부는 악성코드 유포 및 명령 사이트로 추정되는 72개국의 748개 IP(서버)를 확보하여 한국인터넷진흥원(KISA)과 ISP를 통해 긴급 차단하였으며, 안철수연구소 등의 백신업체, ISP, 포털 등의 협조와 네티즌들의 자발적·적극적 참여에 힘입어 전용 백신이 총 11,513,951건 배포되었다고 밝혔다.

※ 한국인터넷진흥원(KISA) 보호나라(www.boho.or.kr)를 통한 배포 4,550,992건,
안철수연구소·하우리·이스트소프트 등의 백신업체, ISP, 포털을 통한 배포 6,962,959건

정부는 금번 3.4 DDoS 공격이 7.7 DDoS 공격과 비슷한 정도의 규모였음에도 불구하고 심각한 서비스 장애가 나타나지 않았던 것은 우선 7.7 DDoS를 계기로 범정부 차원의 '국가 사이버위기 종합대책'('09.9)을 수립하여 국정원, 방통위, 국방부, 행안부 등 각 정부기관의 대응기능을 명확히 하고 대국민·언론 홍보 기능을 일원화 하는 등 대응체계를 정립하고 DDoS 대응장비 구축·확충 등의 정보보호 투자를 대폭 늘렸을 뿐만 아니라, 금융기관, 포털, ISP, 보안업체 등의 주요 민간기관도

DDoS 대응 투자 증액 및 대응인력 보강 등 사전적 대비를 한층 강화한 것 등이 작용한 것으로 보고 있다.

특히 국정원, 방통위, 한국인터넷진흥원(KISA), 안철수연구소 등 민·관이 악성코드를 조기에 탐지하고 분석한 결과를 공유하여 전용백신을 개발·보급하는 등 신속히 대응했을 뿐만 아니라, 주요 ISP들과 포털사들을 통한 감염 PC 치료 안내, 신문과 방송의 적극적 보도, 네티즌의 협조와 신속한 대응이 피해 최소화에 주효하였다고 평가하였다.

※ 사이버치료체계 : 방통위가 '10년 KISA에 구축한 것으로써 피해 사이트의 공격 로그를 분석하여 좀비PC의 IP를 파악한 후 좀비PC가 인터넷에 접속하는 경우 악성코드에 감염되었음을 알리고 팝업창 등을 통해 이용자에게 백신치료 방안을 안내하여 치료토록 하는 시스템

국정원, 방통위, 행안부, 국방부 등 정부기관은 향후에도 DDoS 공격에 의한 피해를 최소화하기 위해 DDoS 공격 24시간 모니터링을 지속하고 대응체계 강화를 위한 투자를 계속할 것이며, 금번 DDoS 공격에서 효과적으로 작동한 민·관 협력체계를 더욱 공고히 해 나갈 계획이다. 또한 정부는 이번 DDoS 공격 악성코드의 초기 유포지로 알려진 보안이 취약한 웹하드 업체들에 대해 주기적인 보안강화 조치 권고, 무료 보안진단 및 기술적 지원, 자가 점검 및 보안 도구의 제작·배포, 법·제도적 장치 마련 등도 추진할 예정이다.

정부 관계자는 정부차원의 노력 이외에도 민간 기업들의 자체적인 보안 강화 및 투자가 DDoS 공격을 효과적으로 방어하는 데 핵심적인 역할을 한다는 것을 강조하는 한편, 무엇보다도 국민 개개인이 자신의 PC가 악성코드에 감염되어 DDoS 공격에 동원되는 일이 없도록 정기적으로 백신 프로그램을 이용한 악성코드 점검 및 최신 보안패치 설치 등 정보보호를 생활화해야 함을 당부하였다. 끝.