방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2011.3.5.(토)

보도자료

2011. 3. 5(토) 배포 시점부터 보도하여 주시기 바랍니다.

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

4일 저녁 2차 DDoS 공격부터 영향 미약
- 7.7 DDoS 후의 DDoS 대응 투자 증대 및 민·관의 신속한 공동 대응 주효 -

정부는 3.4(금) 18:30부터 발생한 2차 DDoS 공격에 좀비PC 5만1천여 대가 동원되었지만, 정부기관의 피해는 없었으며 민간 주요기관의 서비스도 실질적 장애가 없었던 것으로 파악되었다. 또한 3.5(토) 오전 예상되었던 3차 DDoS 공격도 서비스 장애를 일으키고 있지는 않다.

공격 규모가 커졌음에도 불구하고 서비스 장애가 나타나고 있지 않은 것은 민·관이 악성코드를 조기에 탐지하고 분석한 결과를 공유하여 전용백신을 개발·보급하는 등 신속히 대응했을 뿐만이 아니라, 신문과 방송의 적극적 보도와 네티즌의 협조와 신속한 대응으로 지금까지 200만건 정도의 백신 다운로드를 통한 사전 조치 및 대응에 크게 힘입은 바 크다고 판단된다.

특히 '09년 7.7 DDoS 이후 정부 및 민간기관에서 DDoS 대응 장비 구축 및 확충, 대응 체계의 강화, 인력의 보강 등 많은 투자가 이뤄졌으며, 국민들의 사이버 보안에 대한 인식도 많이 제고되었다고 판단하고 있다.

방통위는 지금까지 이번 DDoS 공격의 원격 조정지(C&C)로 파악된 145곳의 IP를 차단하는 한편, 작년 KISA에 구축한 '사이버 치료체계'를 통해 금번 DDoS 공격에서 좀비PC가 인터넷에 접속하려는 경우, 악성코드에 감염되었음을 알리고 악성코드 전용백신을 설치하도록 팝업창 등을 통해 이용자에게 치료방안을 안내하고 있다.(현재까지 KISA 보호나라 107만건, 안철수연구소 80만건, NHN 10만건 다운로드)

또한 발견되는 악성코드 샘플 및 분석결과를 안철수연구소 등 백신업체들과 공유하고 신속히 전용백신을 개발하도록 하였으며, 특히 안철수연구소는 악성코드 샘플 채집 및 분석, 전용 백신 개발 등에 큰 기여를 하고 있다. 주요 ISP 3사(KT, SKB, 티브로드)는 감염 PC에 감염사실을 알려주어 백신 치료를 독려하고, 네이버, 다음 등의 주요 포털도 전용백신 배포를 지원하였다.

정부는 현재까지의 악성코드 분석정보를 바탕으로, 1,2,3차에 걸친 주요 공격 시도로부터 인터넷 서비스 장애 또는 서버 다운과 같은 심각한 위협을 민·관이 체계적으로 대응하고 있다고 평가하였다.

그러나 잠복하고 있는 좀비PC가 더 있을 것으로 보고 향후 추가적인 DDoS 공격 발생 가능성을 염두에 두고 철저히 대비하고 있다. 추가적인 DDoS공격에 대비해 국정원, 방통위, 행안부, 국방부, 정부통합전산센터 및 한국인터넷진흥원 등 각 기관별로 24시간 비상대응체제를 가동하여 상황을 예의주시하고 있다.

"행안부"와 "정부통합전산센터"는 비상대응체계를 가동하여 각 중앙행정기관·지자체 비상근무 지시, 통합전산센터 소관 시스템에 대한 유해IP 분석·차단 및 유관기관 통보 등의 조치를 하였으며, 아울러 3.7(월) 공무원이 출근 시 즉시 좀비PC 감염 점검

및 치료를 할 수 있도록 문자메시지 및 팝업창을 통한 공지를 하고, P2P사이트에 접속을 하지 않도록 필요한 조치를 할 예정이다.

한편, 정부는 이번 DDoS 공격에 이용된 좀비PC가 전염된 날로부터 수일 내에 스스로 자신의 하드디스크를 파괴할 것으로 분석되어 차후 인터넷 이용자들의 추가적인 피해가 우려됨에 따라, 악성코드 유포지로 활용되는 정보공유 사이트에는 당분간 접속을 자제하고 반드시 전용백신을 이용해 자신의 PC를 점검하도록 당부하였다.

악성코드를 치료하는 전용백신은 보호나라(www.boho.or.kr) 또는 안철수연구소, 하우리 등의 주요 백신사에서 다운로드 받을 수 있으며, 기술적인 지원 또는 도움이 필요한 인터넷 이용자들은 '침해사고 24시간 무료 상담센터'(국번없이 118)에 전화하여 전문 상담직원의 도움을 받을 수 있다. 끝.

<첨부 1. 감염PC 사이버 치료체계>

□ 개 념

o 자신도 모르게 침해사고를 유발하는 좀비PC 이용자에게 인터넷 접속 시, 감염사실 통보 및 치료수단 제공하는 체계

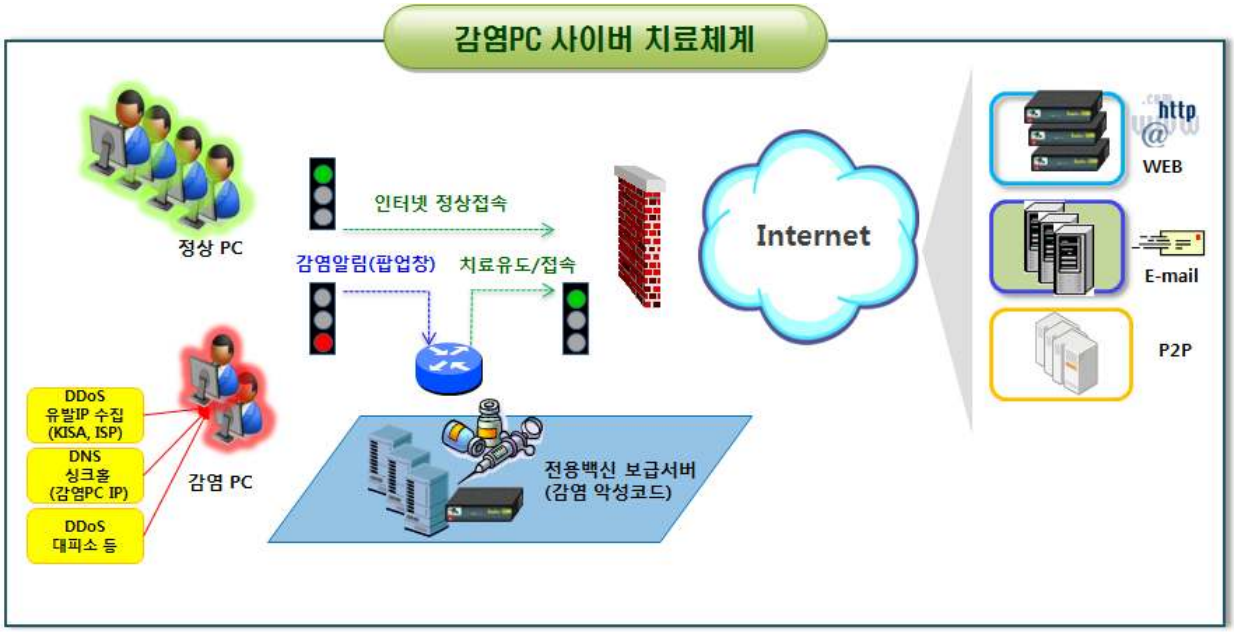
- **(평 시)** 악성코드 감염PC 이용자에게 자신이 타인에게 피해를 주고 있다는 **감염사실 통보 및 치료수단**(맞춤형 전용백신) **제공**

※ '10년 대상 ISP : KT, SK브로드밴드, 티브로드

- **(유사시)** 정부차원에서 안정적인 대국민 **전용백신 보급체계로 활용**

※ 일부 백신업체 홈페이지가 7.7 DDoS 공격대상에 포함되어 접속지연 발생

□ 감염PC 사이버 치료 서비스 절차



① 감염PC IP 신고접수

② 한국인터넷진흥원(KISA) → ISP로 감염IP 전달

③ 감염IP를 사용하는 인터넷 가입자 인증정보 조회 (ISP 측)

④ 감염PC 이용자가 인터넷 접속 시 감염알림

⑤ 팝업창 등을 통해 치료방안도 안내 받음 (맞춤형 전용백신 다운로드 링크 제공)

⑥ 감염PC 치료유도, 안전하게 인터넷 이용