"분산서비스거부(DDoS) 공격으로 인한 인터넷 기업의 피해가 지속적으로 발생하고 정부 · 공공기관의 위협도 크게 가중되면서, 정부가 공공과 민간의 DDoS 공격 대응력을 강화하기 위한 종합대책을 마련하고 있어 관심이 모아진다."

〈2009년 4월 20일 디지털데일리, '정부, DDoS 공격 종합대책 마련한다' 기사 발췌〉

민간 DDoS 대응협의회 출범하다

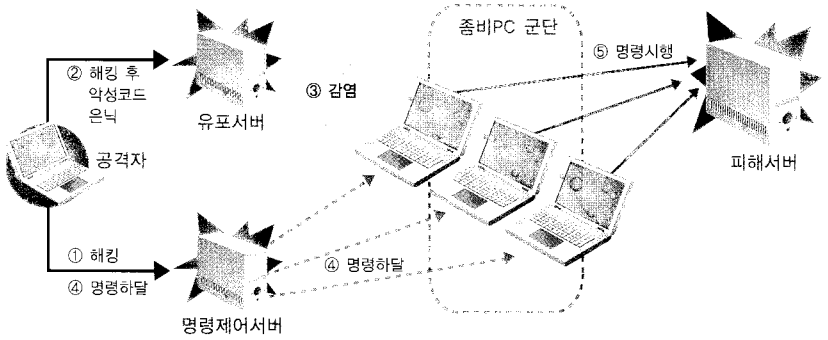
DDoS 공격이 증가하는 가운데, 민간 DDoS 대응협의회가 발족했다. DDoS 공격 대응을 위한 종합대책이 요구되는 상황에서 협의회가 어떤 역량을 발휘하게 될지 정보보호 관계자의 눈과 귀가 협의회로 집중되고 있다.

글 **신대규** | KISA 상황관제팀 팀장

지난 4월 21일 방송통신위원회에서 제1차 민간 DDoS 대응협의회 회의가 개최됐다. 최근 급증하고 있는 DDoS 공격으로 인한 피해를 방지하고, 사고발생 시 효과적으로 대응하기 위해 방송통신위원회, 외교통상부, 경찰청, KISA, 중소기업기술정보진흥원 등 정부기관을 비롯해 인터넷기업, 협회 등 40여개 기관 및 기업이 참여하는 민간분야 'DDoS 대응협의회'가 첫 회의를 가진 것이다.

최근 DDoS 공격의 동향

DDoS 공격은 공격자(해커)가 악성코드에 감염된 다수의 PC를 이용해 대량의 유해 트래픽을 특정 시스템에 전송함으로써 네트워크 및 시스템의 과부하를 유발해 정상적인 서비스를 방해하는 사이버 공격을 말한다.



▲ DDoS 공격 개념도

공격자(해커)가 DDoS 공격을 수행하는 대표적인 방법을 설명하면 다음과 같다. 첫째, 공격자는 자신의 명령을 좀비PC에게 전달할 명령제어서버를 해킹한다. 둘째, 공격자는 홈페이지를 해킹한 후, 자신이 해킹한 명령제어서버로부터 명령을 받도록 코딩되어 있는 악성코드를 은닉한다. 셋째, 보안이 취약한 이용자 PC가 악성코드가 은닉된 홈페이지에 접속하면 악성코드에 감염되며, 공격자의 명령을 따르는 좀비PC가 된다. 넷째, 공격자가 명령제어서버에 DDoS 공격명령을 하달하면 악성코드에 감염된 다수의 좀비PC가 공격명령에 따라 특정사이트를 공격한다.

최근 DDoS 공격은 협박, 금품 요구를 목적으로 하는 범죄적 양상을 지닌 공격이 급격히 증가하고 있으며, 이에 따라 조직화되어가는 추세를 보인다. 과거에는 신고가 어렵다는 점을 이용해 성인 및 도박 사이트 등 불법 사이트를 대상으로 이뤄지던 공격이 점점 게임아이템 거래사이트, 여행사이트, 쇼핑몰, 금융기관까지도 공격대상으로 삼는 등 사회전반에 광범위한 공격이 이루어지고 있다.

또한, 사회적 갈등의 표출 수단으로써도 DDoS 공격이 활용되고 있다. 최근 포털 사이트의 한 카페에서 강제탈퇴 당한 10대 청소년이 이에 앙심을 품고 보복성 DDoS 공격을 시도해 불구속 입건된 사례에서도 알 수 있듯, 최근에는 중국 등지에서 만들어진 공격도구가 국내에 유포돼 누구나 간단한 조작만으로도 DDoS 공격을 할 수 있게 되고 있다.

1차 민간 DDoS 대응협의회 주요 논의사항

이런 상황에서 지난 3월 13일 DDoS 공격으로 인해 피해를 입은 업체들의 애로사항을 청취하고 의견을 수렴하기 위한 사업자 간담회가 개최됐다. 참석한 인터넷기업들은 DDoS 공격에 대응하기 위한 협의회 구성, 인터넷에 유포되고 있는 공격 프로그램의 차단, 영세 중소기업에 대한 정부차원의 지원, ISP 차원의 공격 트래픽 차단, 해외발 공격에 대한 외교적 대응 강화 등 다양한 의견을 제시했다. DDoS 대응협의회 출범은 당시 간담회의 후속조치로 이뤄졌다.

제1차 민간 DDoS 대응협의회는 외교통산부, 경찰청 등 부처별 DDoS 대응관련 정책방향을 발표하고 정부의 DDoS 대응관련 정책방향 검토 및 정책제안 등이 이뤄졌으며, 논의된 내용을 요약하면 다음과 같다.

제1차 민간 DDoS 대응협의회 주요 논의내용

■ DDoS 공격 조장 게시물 차단

악성(해킹) 프로그램 유포 판단을 위한 가이드(기준)를 마련하고 한국인터넷자율정책기구를 통해 포털의 자율정화를 유도하는 한편, 방송통신심의위원회를 통해 불법 게시물을 삭제한다.

■ 영세 중소 인터넷기업 지원

DDoS 공격을 당한 영세 중소기업을 대상으로 'DDoS 긴급대피소'를 구축, 운영해 일정기간 무료 DDoS 방어 서비스를 제공함으로써 정상적인 서비스가 지속될 수 있도록 지원하고 저렴한 DDoS 대응서비스 이용 활성화를 유도한다.

※ DDoS 공격 긴급대피소 : 영세 중소기업의 시스템으로 향하는 DDoS 공격 트래픽이 KISA의 DDoS 방어시스템을 통과하도록 함으로써 정상적인 트래픽만 전달되도록 일정기간 방어해 주는 서비스

■ ISP망 차원의 트래픽 차단

DDoS 피해 업체와 ISP간 차단요청 및 승인절차를 정립하고, 정부의 DDoS 대응시스템 시범구축사업에 대한 효과분석을 통해 ISP의 DDoS 대응시스템 구축 등에 대한 투자를 유도한다.

■ 대중국 외교 대응 능력 강화

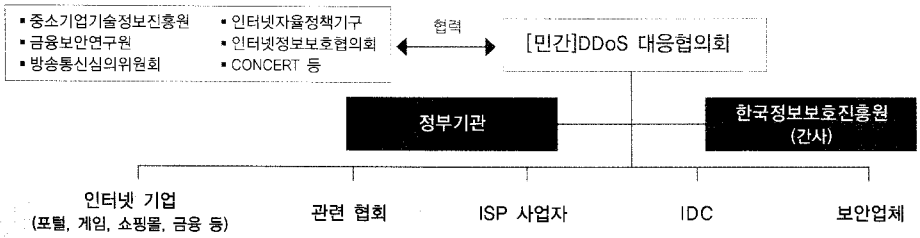
외교통상부를 중심으로 한·중 외교실무회의를 통한 의제제안 등의 협조체계를 구축하고, 경찰청을 중심으로 한·중 사이버 침해사고 공조 수사체계를 강화한다.

■ 기타

KISA의 악성코드 은닉사이트 차단, Bot DNS Sinkhole 확대, 이용자 및 사업자 정보보호 인식제고 강화 등 기존사업을 지속적으로 확대해 추진하고 정보통신망법 개정안 내에 PC 보안조치 의무화를 반영한다.

이처럼 DDoS 공격 피해사례 및 최신 보안기술 등의 정보를 공유하고 사고 발생 시 효과적인 대응 방안을 마련하는 한편, 피해방지를 위해 필요한 정책을 제안하는 등 공동으로 노력할 방침이다.

DDoS 대응협의회의 체계도 및 기관별 역할은 아래와 같다.



▲ DDoS 대응협의회 체계도

기 관	역 활	비고
정부	▪사업자 의견에 대한 정책 개선방안 마련	
KISA	▪협의회 카페 개설 및 신규회원 접수, 메일링 리스트 운영 ▪DDoS 관련 최신정보 제공 및 관련 세미나 개최 등 ▪사고발생 시 공동대응 주관 ▪회의개최 의견 수렴 및 회의 준비	간사
중소기업기술정보진흥원	▪중소기업 정보보안 기술 지원	
인터넷 기업	▪문제점 발굴 및 정책 제안 ▪사고발생 시 신속한 신고 및 공동대응 요청	
포털	▪이용자 정보보호 인식 제고 ▪DDoS 공격 툴 제거 협조	
금보연 및 금융기관	▪금융분야 DDoS 공격 관련 정책 제안	
한국인터넷기업협회	▪다양한 기업의 의견 수렴	
ISP	▪ISP 차원의 DDoS 공격 트래픽 차단 협조 ▪주요망 보안투자 활성화	
IDC	▪DDoS 차단 서비스 활성화 ▪사고발생 시 ISP 등 협력	
보안업체	▪DDoS 공격 대응방안 의견제안 ▪DDoS 공격 툴 분류 기준 마련 협조	

▲ DDoS 대응협의회 기관별 역할

협의회 운영 방안

협의회는 논의된 내용을 바탕으로 지속적이고 효과적으로 추진하기 위하여 정례회의를 반기별로(년 2회) 개최하고, 주요 이슈가 발생하거나 참여기관이 요청할 경우 수시로 실무회의를 개최할 계획이다.

협의회에 참여를 희망하는 업체 및 기관은 메일 등을 통해 상시 신청(02-405-5241)할 수 있으며, 협의회 회원사로 등록하게 되면 인터넷 카페 및 메일링 리스트를 이용해 상시정보를 공유하고 DDoS 피해 방지에 참여할 수 있게 된다.

이번에 발족한 협의회는 온라인을 통해 참여기관 간 정보공유 및 DDoS 문제 해결을 위해 공동으로 노력하기로 했다. 이번 협의회 구성으로 회원사 간 정보 공유를 통해 DDoS 공격에 대한 자체 대응능력을 향상시킴은 물론, 업체의 의견을 정부에 전달할 수 있는 공식적인 창구를 마련했다는데 큰 의의가 있다고 볼 수 있다. 향후 협의회가 DDoS에 대한 효과적인 예방 및 대응활동을 통해 향후 안전한 인터넷 이용환경 조성에 이바지할 수 있기를 기대한다. **S**