Anti-DoS 솔루션은 HTTP 페이지를 반복 요청함으로써 웹서버나 애플리케이션 부하를 증가시키는 HTTP 플러딩 공격도 효과적으로 방어할 수 있는 수단이다.

인터넷 강국 좀먹는 DDoS공격

2007년 '인포네틱스 리서치' 의 발표에 따르면 IT 분야의 보안 위협 중 DDoS공격으로 인한 위협이 가장 큰 것으로 보고되고 있다. 통계적으로 대기업의 경우 연간 30억원의 보안 피해를 입는데 이중 50%는 DDoS공격에 의한 것이다. 국내에서도 2007년 한해 DDoS공격으로 인한 피해 사례가 급증했으며, 특히 온라인 서비스를 위주로 하는 기업들의 DDoS공격 피해액은 수백억원대로 추정되고 있다.

국내로 유입되는 DDoS공격의 유형을 분석해 본 결과, 불행하게도 2008년에는 공격의 규모와 이로 인한 피해가 더욱 커질 것으로 예상된다. 대부분의 공격은 금전적 이득을 목표로 하고 있으며 이를 위해 공격 목표를 먼저 선정한 뒤 서비스를 다운시키고 돈을 갈취하는 수법을 사용하고 있다. 이러한 요구는 1회에 그치지 않고 계속 이어지며 요구가 받아들여지지 않을 경우 다시 공격을 가해 서비스를 다운시키곤 한다. 실제로 외부에 드러나지는 않았지만 많은 온라인 기업들이 이러한 공격의 피해 때문에 불합리한 요구를 들어주고 있는 실정이며, 특히 보안 시스템을 제대로 갖추지 못한 중소규모 사이트의 피해가 더욱 큰 것이 사실이다. Attacker 또한 서비스를 다운시키기 좋고 협상이 용이한 중소규모 사이트를 주 공격대상으로 삼고 있다.

이러한 공격들은 중국에 기반을 둔 기업형 Attacker 들에 의해 발생되는 것으로 추정되는데 기존의 경우 해외망을 통한 공격 유입이 주류였으나, 이제는 국내에 봇(Bot) 에이전트를 심어놓고 컨트롤 서버를 이용해 공격하는 형태로 변모했다. 또한 공격의 경우 UDP, ICMP, TCP 기반의 플러딩 공격이 모두 활용된다. 공격 트래픽의 경우 초기에는 1~2Gbps 정도였으나 최근에는 많은 봇 에이전트를 확보하면서 10G 이상의 공격도 발생하고 있으며, 이로 인해 회선 대역폭 고갈 문제도 대두되고 있다. 하지만, 회선을 제공하는 인터넷 데이터센터도, 그 안에서 온라인 서비스를 운영하는 사업자들도 모두 DDoS공격의 근본 대책을 못 찾고 있는 것이 현실이다.

가장 근본인해결책은 봇 에이전트로 활용되는 PC를 없애는 것인데, 사용자들이 보안 백신을 설치하고 정기적으로 업데이트해야 한다. 하지만 보통의 경우 이러한 관리에 소홀한 것이 사실이며 단시간 안에 이 문제가 크게 개선될 것으로 보이지는 않는다. 따라서 기업 입장에서 체계적인 준비가 필요할 것이다.

DDoS공격을 막는 방법으로 L3 스위치, 백본 스위치 및 방화벽에서 ACL(액세스 리스트)를 이용해 차단하거나, IPS(Intrusion Prevention System)를 이용하는 방법이 많이 쓰이지만 근본적인 해결책은 되지 못하고 있다. K

라드웨어코리아 대표
김 도 건
kevink@radware.com