지상 최대의 화두, DDoS 공격을 막아라

DDoS(Distributed Denial of Service) 공격이 정보보호 분야의 최대 뉴스 메이커로 떠올랐다. 실제로, 지난 3월 13일 민간 기업 및 기관 정보보호 담당자들이 모인 2008년 한해 정보보호 이슈를 전망해 보는 'CONCERT FORECAST 2008-기업 정보보호 이슈 전망'에서 기업 정보보호 담당자들은 DDoS 공격을 최대 이슈로 꼽는데 주저하지 않을 만큼 DDoS 공격은 더 이상 '남의 집 불구경'이 아닌 것이 돼 버렸다. 하지만 공론화되는 DDoS에 대한 이슈만큼이나 정보보호 관계자들을 답답하게 하는 것은 DDoS 공격에 대해 아직까지 국내는 물론, 해외에서 조차 속 시원한 해법을 내놓는 전문가가 없다는 점이다. 이번 호에서는 DDoS 공격에 대해 기업, ISP, IDC 등에서 마련하고 있는 DDoS 대응현황을 살펴보고자 한다.

정보보호뉴스 취재팀

DDos 공격이 뭐예요?

최근 뉴스 지면을 통해 자주 접할 수 있는 서비스 거부 공격(DDoS : Distributed Denial of Service)은 특정 웹 서버나 DNS 서버 등 서버 시스템과 네트워크 장비에 일순간 많은 양의 트랙픽을 집중시킴으로써, 해당 기업이 제공하는 서비스를 지연 혹은 마비시키는 공격 형태로 정의할 수 있다. 웹 사이트에 접속자가 일순간 집중돼 발생하는 '◎◎사이트, 접속자 폭주로 웹 서비스 마비'라는 뉴스 기사를 볼 수 있는데, 이것이 바로 DDoS 공격의 원리라고 볼 수 있다. 이 같은 DDoS 공격은 크게 대역폭(Bandwidth)을 이용한 공격과 프로토콜을 이용한 공격으로 구분된다.

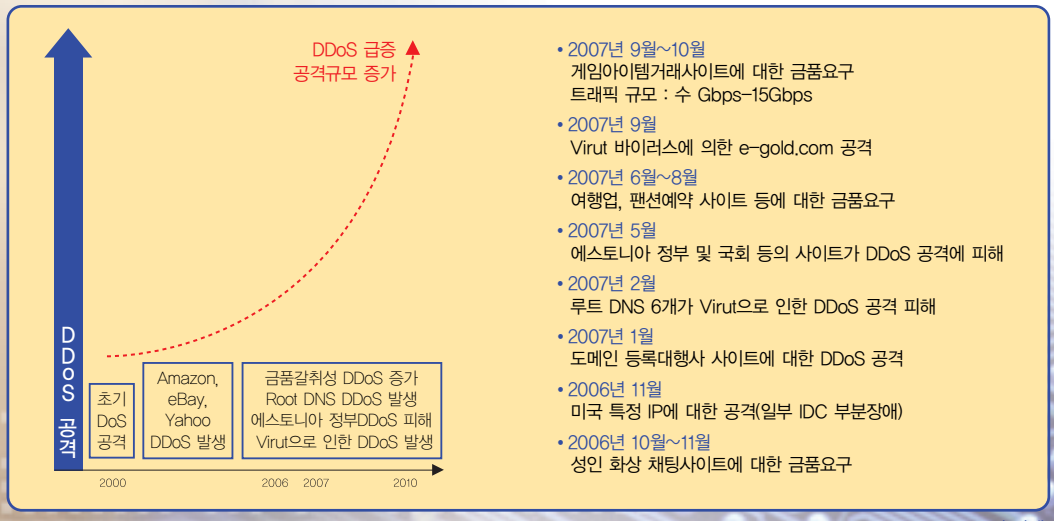
자원 고갈시키는 DDoS 공격

DDoS 공격은 네트워크와 시스템의 자원을 고갈시키는 공격유형으로, 기업이 갖고 있는 대역폭이나 시스템의 처리 한계치를 넘어선 엄청난 양의 패킷을 전송해 이들 장비 및 시스템이 정상적인 서비스를 제공하지 못하는 것은 물론, 시스템과 네트워크를 마비시켜 어떤 징후 없이도 일순간의 공격에 의해 서비스를 중단시킬 수 있다.

주요 공격 방법으로는 최근 UDP 프로토콜을 이용한 Bandwidth Consuming, TCP Syn Flooding을 이용한 PPS Consuming, 그리고 동일 URL 접속을 시도하는 httpd Flooding 등이 있는 것으로 알려져 있다.

그러나 이런 DDoS 공격은 IP 스푸핑(Spoofing)을 이용해 공격자의 IP 주소를 조작할 수 있어, 공격자의 추적도 쉽지 않아 사전대응은 물론, 사후 추적까지 어려운 것으로 알려져 있다.

일반적으로 새로운 악성코드와 사회공학적 방법을 동원해 관리자 몰래 시스템과 네트워크에 접속해 중요 정보를 빼내는 기존 해킹과 달리, DDoS 공격은 서비스를 원천적으로 차단시킨다는 점에서 구분되며, 새롭게 등장한 공격방법은 아니라고 볼 수 있다. 그런데 이런 DDoS 공격이 최근 왜 이렇게 이슈가 되고 있는 것일까. 가장 큰 원인은 인터넷 서비스 자체의 취약점을 이용하는 이 공격에 대해 일반 기업 및 기관에서는 대응하기 쉽지 않다는 점과, 최근에는 급기야 공격 중단을 전제로 금품을 요구하는 협박성 DDoS 공격까지 등장하고 있기 때문이다.



▲주요 DDoS 공격 사례

금품 요구하는 DDoS 공격의 출현

최근의 DDoS 공격 특징은 일정 이상의 금액을 요구하며, 돈을 입금하지 않을 경우 서비스를 중단시키겠다는 협박으로 이어진다는 점이다. 그동안 언론을 통해 알려진 것처럼 공격자들은 시스템 관리자에게 메신저 등으로 접근, 금품을 요구하고 있으며 실제로 몇몇 인터넷 사이트는 DDoS 공격으로 서비스 중단 사태를 경험하고 이로 인해 심각한 후유증을 앓고 있는 것으로 알려져 있다. 한 정보보호 업계 관계자에 따르면, 최근에는 일회성 금품 요구뿐만 아니라, 매월 일정 비용을 요구하는 등 협박의 정도가 더욱 심해지고 있다고 한다. 또한 지난해 협박성 DDoS 공격이 등장했을 당시만 해도, 공격대상 사이트는 채팅/도박 등 불법적으로 운영되는 음성적인 사이트에 국한됐지만, 올해부터는 그 대상이 일반 웹 서비스 제공업체들에까지 확대될 것으로 예상되는 만큼 DDoS 공격에 대한 정보보호 관계자들의 우려의 목소리는 더욱 커져가고 있다.

DDoS 공격 대응 왜 어려운가

앞서 언급한 것처럼 DDoS 공격은 과도한 트래픽을 동시다발적으로 특정 기업의 네트워크나 서버로 발송함으로써 서비스를 제공해야 할 시스템이 정상적으로 작동하지 못하도록 하는데 그 목적이 있다. 마치 하루 평균 1,000대의 차량이 지나갈 수 있는 도로에 100,000대의 차량이, 그것도 특정 시간 동안 집중돼 도로의 기능을 상실케 하는 것과 마찬가지다. 또 굳이 DDoS 공격임을 표방하지 않더라도 특정 서버에 서비스 이용자가 집중될 경우, 해당 서비스는 마비가 될 수 있어 DDoS 공격에 대한 문제는 웹 서비스를 제공하는 기업이라면 공통적으로 가질 수밖에 없는 구조적인 문제이기도 하다. 여기에 DDoS 공격에 이용되는 패킷은 웜이나 바이러스처럼 일정한 패턴을 지닌 악성코드가 아니라는 점에서 네트워크 모니터링이나 정보보호 솔루션을 활용해 사전 예방체계를 갖추는 식의 대응도 쉽지 않다.

물론 DDoS 공격을 견딜 만큼의 서버와 처리용량을 갖추면 되지 않겠느냐는 질문이 있을 수 있겠지만 일부 기업을 제외한 대부분의 웹 서비스 업체들의 경우, DDoS 공격에 대응하기 위해 무작정 서비스 유지비용을 늘려나갈 수 없다는 현실적인 문제도 존재한다. 설사 기존 처리용량의 2배 혹은 3배 이상의 시스템을 구축한다고 해도 공격의 트래픽은 그만큼 더 증가될 수 있어, 트래픽 처리 용량의 증설은 근본적인 해결책이라고 볼 수 없다.

Anti-DDoS라는 보안 솔루션도 등장

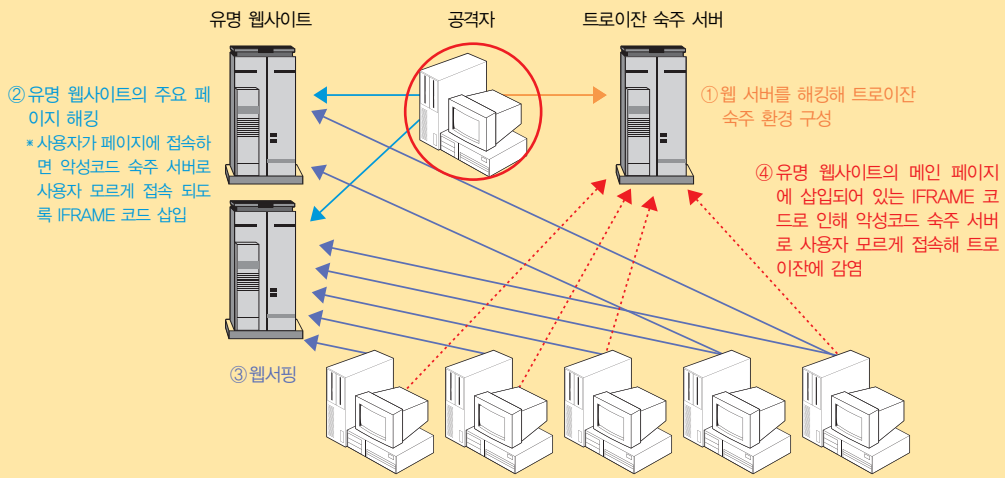
특정 공격유형의 등장은 이에 대응하는 보안 솔루션의 출현으로 이어져 왔고, 그런 과정이 정보보호 솔루션의 발전사이기도 하다. 그런 의미에서 최근 DDoS 공격에 특화된 Anti-DDoS 솔루션에 대한 관심도 높아지고 있다. 이런 Anti-DDoS 보안 솔루션의 기술은 어디까지 왔을까. 현재 출시되고 있는 Anti-DDoS 솔루션들의 기본 원리는 기업 네트워크단에 설치돼 유입되는 트래픽을 감시하며 급격하게 트래픽이 증가하거나, DDoS로 의심되는 트래픽의 유형이 발견될 경우, 해당 트래픽을 곧바로 제거하는 방식이다. 특히, 시그니처에 기반해 공격유무를 판단하는 기존의 IPS나 바이러스 월 등의 보안 솔루션이 악성코드나 일반적인 해킹 공격에 효과적인 반면, Anti-DDoS 솔루션은 트래픽 자체를 모니터링하기 때문에 트래픽을 이용한 DDoS 공격에 신속하게 대응(한 Anti-DDoS 솔루션 업체 관계자에 따르면, 이 시간을 18초 내외라고 주장한다)할 수 있다는 것이

솔루션 업체들의 주장이다.

그러나 한편으로는 Anti-DDoS 솔루션이 가지는 한계도 지적되고 있는데, 예를 들어 보안 솔루션이 처리할 수 있는 트래픽 용량이 10기가라고 한다면, 그 이상의 공격이 등장할 경우에는 또다시 보안 솔루션의 처리 속도와 용량을 고려해야 한다는 것이다. 또 현재 Anti-DDoS 솔루션의 가격이 상당히 고가라는 점에서 많은 기업에게 Anti-DDoS 솔루션은 '그림의 떡'이 될 가능성이 높다는 지적도 무시할 수 없는 대목이다.

도대체 DDoS 공격을 어떻게 하길래

대규모 트래픽을 유발시키는 DDoS 공격은 엄청난 양의 트래픽을 발생시키기 위해 그에 상응하는 PC 장비들을 필요로 한다. 일반적으로 공격자는 1,500~2,000여대의 좀비 PC를 보유하고, 이들 PC들로부터 특정 시점에 특정 시스템과 네트워크로 DDoS 공격 트래픽을 발송하는 것으로 알려져 있다. 국내 초고속 인터넷망과 PC의 성능을 감안해 볼 때 PC 한 대가 유발할 수 있는 트래픽의 양이 10Mbps 내외라고 한다면, 불과(?) 1,500~2,000여대가 유발하는 트래픽의 양은 무려 15~20기가 이상이 될 수 있다는 얘기다. 공격자가 공격에 이용하는 좀비 PC는 아래의 그림처럼 웹 서버의 취약점을 악용해 접속하는 PC를 감염시켜 공격자가 조정이 가능하도록 악성코드를 설치하는 방법이 최근에는 주로 이용되고 있다. 때문에 KISA에서는 DDoS 공격의 원인을 제공하는 악성코드가 유포된 서버를 찾아 해당 악성코드를 제거하거나, DNS Sinkhole 등을 운영함으로써 DDoS 공격에 대한 예방활동에 주력하고 있다.



▲웹 사이트를 통한 악성코드 전파의 예

기댈 곳은 IDC, ISP인데

이처럼 각 기업 단위에서 DDoS 공격에 대한 현실적인 대응과 예방, 그리고 보안 솔루션의 도입이 현실적으로 어렵다는 점에서 대규모 호스팅 서비스를 제공하는 IDC나 인터넷 망을 관리하는 ISP 차원의 대응책 마련이 필수적이라고 정보보호 관계자들은 입을 모은다. "네트워크 회선을 임대하거나 호스팅 서비스를 받는 일

반 기업에서는 DDoS 공격 대응문제만큼은 IDC나 ISP의 대응능력에 전적으로 기댈 수밖에 없다. ISP나 IDC가 트래픽에 대한 모니터링을 실시하고, 이상 트래픽 현상이 발생할 경우 이에 대한 적극적인 차단이 이뤄진다면 DDoS 공격에 대한 걱정도 줄어들 수 있을 것" 이라는 한 기업 정보보호 담당자의 얘기는 DDoS 공격의 대상이 되는 모든 관계자들의 공통된 생각일 것이다.

그렇다면 IDC나 ISP에서는 과연 무엇을 어떻게 해야 할까. 기업 정보보호 담당자들의 주장에 따르면, DDoS 공격 트래픽이 해당 기업의 네트워크나 서버로 유입된 이후에는 더 이상의 대응방법은 없다고 한다. 때문에 거시적 차원에서 트래픽의 유입을 관장할 수 있는 ISP, 혹은 IDC가 공격 징후 발견 시 트래픽을 적극적으로 차단해줘야 한다는 것이 주장의 요지다. 국내 IDC와 ISP는 이 같은 주장에 대해 어떻게 생각하고 있을까.

DDoS 공격 대응을 위한 준비가 단 시간 내에 이뤄지기 어렵다고 전제한 한 ISP 관계자는 "전체 트래픽을 모니터링할 수 있는 관제센터 운영을 통해 연동구간에 Access Module을 설치해 사전대응이 가능하도록 하는 한편, Anti-DDoS 솔루션 도입을 위해 장비를 테스트하고 있는 실정" 이라고 설명했다. 반면, 한 IDC 관계자는 "IDC가 DDoS 대응을 위해 필요한 모든 비용을 처리하기에는 어려움이 있는 것이 사실" 이라며, "IDC에 입주한 일부 고객들과의 협의를 통해 대응책을 마련하고 있지만, 각 기업들 역시 하나의 DNS 서버만을 운영하는 것이 아닌, 2개 이상의 DNS 서버를 운영함으로써 위험요소를 분산시킬 방안을 찾는 노력도 병행되어야 한다" 고 덧붙였다.

DDoS 공격이 현재 정보보호의 최대 이슈임에는 분명하다. 또 그에 따라 웹 서비스 제공기업을 비롯해 IDC, ISP 등 관련 기업과 기관이 대응책 마련에 부심하고 있는 것 역시 사실이다. 분명한 것은 국내외적으로 아직 명확한 대응책이 마련되지 않고 있는 DDoS 공격에 대해 기업과 관련 기관이 모두 머리를 맞대야 할 시점이 지금이라는 점이다. S

지금 KISA에서는

민간 기업들을 대상으로 DDoS 공격이 증가되면서, KISA는 DDoS 공격에 대한 예방활동을 펼치는 데 주력하고 있다. KISA의 대응양상은 크게 일반 사용자, 홈페이지를 운영하는 사업자, ISP/IDC로 구분돼 진행된다.

현재 대부분의 DDoS 공격이 좀비 PC를 기반하고 있다는 점에서 KISA는 일반 사용자에게 'PC 자동 보안 업데이트 프로그램'을 개발해 보급하고 있다. 이를 통해서 사용자가 보다 쉽게 보안 업데이트를 수행해 개인 PC의 보안성을 향상시킬 수 있도록 유도하는 한편, 만약 사용자 PC에 바이러스/악성코드 등의 문제가 발생한 경우, 보호나라 홈페이지를 통해 PC 원격점검 서비스가 가능해 PC에 발생한 문제를 해결할 수 있다.

홈페이지를 운영하는 사업자 대상으로는 MC Finder를 통한 악성코드 탐지 및 웹 취약점 점검 서비스(http://webcheck.krcert.or.kr)를 꼽을 수 있다. MC Finder는 국내 주요 홈페이지에 은닉된 악성코드를 찾아내는 시스템으로 홈페이지가 공격을 당한 후에 삽입되는 악성코드를 탐지하게 된다. 웹 취약점 점검 서비스는 여건 상 보안 관리자가 없는 소규모 업체를 대상으로 홈페이지에 존재하는 취약점을 찾아내서 개선하도록 하는데 일조하고 있다.

마지막으로 ISP/IDC와의 협력관계를 통한 악성도메인 및 악성코드 유포지 차단, DNS Sinkhole 적용 등이 있다. KISA는 악성 봇에 감염된 좀비 PC들이 명령전달자인 공격자 서버에 접속하지 못하도록 하는 DNS Sinkhole을 개발해 운영하고 있으며, 국내 주요 ISP/IDC들은 자사 네트워크에 DNS Sinkhole을 적용해 DDoS 공격에 악용되지 않도록 조치를 취하고 있다. 또한 KISA가 탐지한 악성도메인 및 악성코드 유포/경유 사이트에 대해서는 사업자에게 차단조치를 요청하면서 ISP/IDC와 악성도메인 및 트래픽에 대해서 공동으로 대응하고 있다.

만일 DDoS가 발생하게 되면 KISA는 공격에 가담한 사용자의 PC를 신속하게 분석하고 추출된 악성도메인 및 유포사이트에 대해서 ISP/IDC에 차단조치를 시행하고 이로 인한 DDoS 공격의 추가 피해를 방지하는 체계를 운영하고 있다.