White Paper

DDoS 공격 대응의 새로운 패러다임

AhnLab TrusGuard DPX

Revision Version: AhnLab TrusGuard DPX White Paper ver. 1.0

Release Date: April, 2010

AhnLab, Inc.
6th Fl., CCMM Bldg.
12 Yeouido-dong,
Yeongdeungpo-gu, Seoul 150-869,
Korea
82-2-2186-6000
www.ahnlab.com

Contents

Ⅰ. 개요

인터넷을 이용하는 환경은 악성코드 감염, 개인 정보 유출, 서비스 해킹, 서비스 거부 등 다양한 보안 위협에 노출되어 있다. 그 중 가장 가시적인 피해 양상을 나타내는 위협은 바로 DDoS(Distribute Denial of Service) 공격이다. 국내의 경우 2006년도부터 본격적으로 대두되기 시작한 DDoS 공격은 2009년 7.7 DDoS 대란에서 경험한 바와 같이 이제는 대형 컨텐츠 사업자뿐만 아니라 정부, 금융 기관까지도 공격의 목표가 되고 있다. 특히 DDoS 공격으로 인한 피해는 서비스 가용성의 문제를 초래하여 인터넷 비즈니스의 마비라는 가시적인 피해 양상을 나타낼 수 있으며, 아울러 해당 사업자의 서비스 신뢰도 및 대외 인지도에 큰 영향을 받을 수 있으며, 나아가 고객의 이탈이라는 피해까지 전개될 수 있기 때문에 문제가 심각하다고 할 수 있다.

Ⅱ. DDoS 공격의 발전 양상 및 기존 장비의 한계점

DDoS 공격은 과거 단순한 Packet 형태의 트래픽을 과도하게 발송하는 공격 기법에서 발전하여 정상적인 요청 및 응답을 수행하여 기존의 비정상적인 패킷을 구분하는 방어 기법을 무력화 시키는 양상을 보이고 있다. 또한 작은 트래픽 규모로 공격을 감행하는 기법을 이용하여 DDoS 공격 대응 장비에서의 탐지를 회피하는 등 다양한 공격 형태로 지속적으로 발전하고 있다. 특히 종전의 좀비(Zombie) PC를 제어하는 C&C(Command & Control) 서버 기반의 봇넷(BotNet) 기반 기술에서 최근에는 좀비 PC를 감염시키는 악성코드가 직접 공격 명령을 업데이트하여 공격을 수행하는 형태와 C&C 서버와 좀비 PC를 은폐하기 위하여 패스트-플럭스(Fast Flux) 기술 기반의 봇넷 형태로도 발전하고 있다.

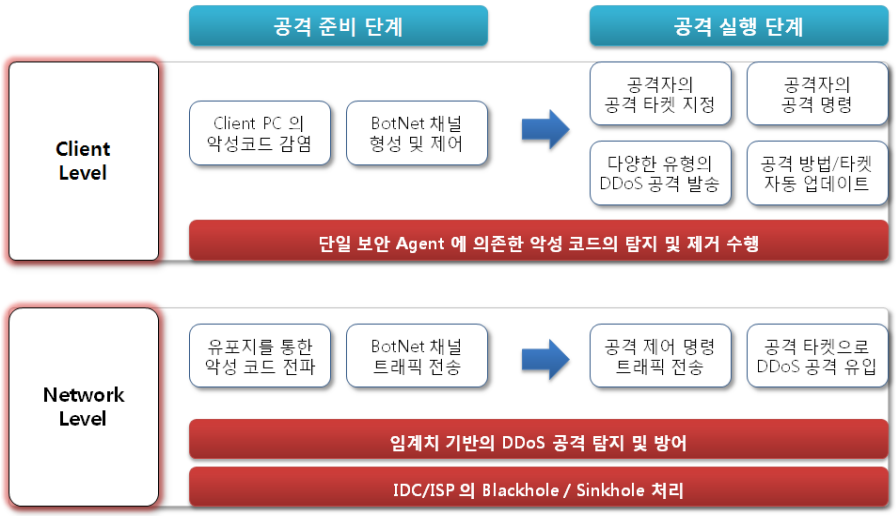
[그림 1] DDoS 공격 발전 양상

이에 따라 지속적으로 발전하는 DDoS 공격에 대응하기 위해서는 DDoS 공격 대응 전용 장비만으로는 사실상 한계에 이르게 된다. 특히 지능적으로 발전하는 다양한 공격 유형들에 대한 분석을 통한 신속한 대응이 반드시 지원되어야만 한다.

특히, DDoS 공격을 방어하기 위해서는 기존의 Network Level 에서의 임계치 기반의 이상 트래픽 탐지/방어 기법과 더불어 DDoS 공격의 근본적인 원인인 Client PC Level 에서의 분석, 탐지, 방어 기법이 동시에 지원되어야 한다. 즉, Zombie PC 감염과 DDoS 공격

을 실행하는 악성 코드에 대한 분석이 이루어져야 하며, Client Level 과 Network Level 의 유기적인 대응 체계를 바탕으로 DDoS 공격에 대응해야 원천적인 방어가 가능하다.

하지만, 최근까지의 DDoS 공격 대응 방법을 살펴보면, Client Level 의 경우 Anti-Virus 등 Agent 기반의 보안 제품이 개별적인 악성 코드 검출 형태로만 조치가 이루어졌으며, 아울러 Network Level 에서는 DDoS 공격 전용 대응 장비가 평상시 트래픽 유형의 임계치와 이상 트래픽 현황을 비교하여 탐지 및 차단하는 방식으로 대응하였다. 아울러 Client Level 과 Network Level 의 유기적인 방어 체계 역시나 없었던 것이 사실이다.

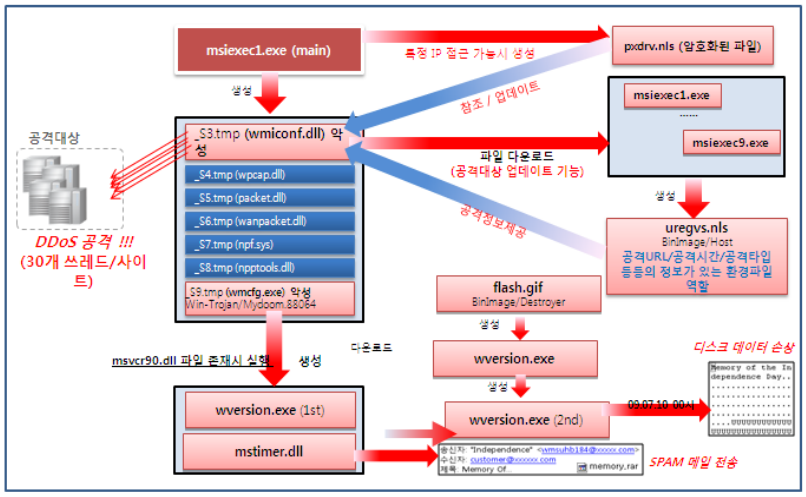


[그림 2] 기존 DDoS 대응 방법의 한계

따라서, 새로운 DDoS 공격을 대응하기 위해서는 DDoS 공격 발생의 근원인 '좀비 PC 감염'을 유발하는 악성코드의 분석 기술과 DDoS 공격 대응 전용 장비의 유기적인 연동 등 입체적인 DDoS 공격 대응의 프로세스가 필요하다.

Ⅲ. 새로운 DDoS 공격 대응 패러다임

먼저, DDoS 공격의 근원은 악성코드 기반의 좀비 PC의 감염으로 시작된다. 따라서, 단순히 네트워크 레벨에서의 분석이 아닌 악성코드가 감염되는 클라이언트(Client) PC 레벨에서의 분석 기술이 필요하다. 이를 통하여 문제를 일으키는 악성코드가 어디서 유포되는지에 대한 정보를 빠르게 분석할 수 있게 된다. 즉, 이 악성코드가 어떠한 형태로 공격 명령을 수행하는지, 그리고 어떤 유형의 DDoS 공격 트래픽을 유발하는지에 대한 정확한 분석이 뒷받침 되어야 한다. 이런 과정을 거쳐야만 2009년 7.7 DDoS 대란과 같이 공격 대상과 공격 시간의 정확한 예측까지도 가능하게 되는 것이다.



[그림 3] 안철수연구소가 분석한 7·7 DDoS 대란 공격 파일 관계도

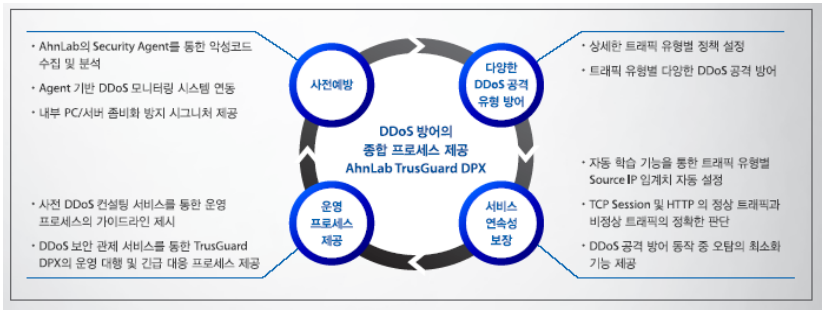
이러한 정보를 바탕으로 네트워크 레벨에서 방어하는 역할을 하는 보안 제품 및 DDoS 공격 대응 전용 장비는 내부 클라이언트/서버에 대해 좀비 감염을 사전에 예방해준다. 이를 통하여 내부 클라이언트/서버의 좀비 감염으로 인한 아웃바운드(Outbound) DDoS 공격을 사전에 예방하는 효과를 얻을 수 있다. 이와 함께 DDoS 공격 대응 전용 장비는 분석된 악성코드의 DDoS 공격 트래픽 유형에 맞는 방어 정책의 설정 및 업데이트가 이루어져, 공격 방어를 효과적으로 수행할 수 있게 된다. 더불어 클라이언트 PC 레벨에서의 DDoS 공격 발생 탐지를 통해 네트워크 레벨에서의 공격 방어 정보를 유기적으로 연동할 수 있다. 물론, 악성코드를 탐지한 클라이

언트 PC/서버에서는 명확한 악성코드 정보가 있으므로, DDoS 공격을 유발하는 악성코드를 원천적으로 제거함으로써 DDoS 공격을 원천적으로 차단할 수 있게 된다.

또한, 국내 DDoS 시장에서는 DDoS 공격에 체계적인 대응을 하기 위해서는 DDoS 대응 시스템 도입 및 운영뿐만 아니라 24시간 침해 대응 관제 체제 구축과 DDoS 대응 매뉴얼 마련, DDoS 공격 대응 모의 훈련 수행까지 요구 사항이 확대되고 있다. 이는 기존의 전용 제품의 경우 구매 후 관리, 유지 보수, 긴급 공격 대응 등 일련의 운영을 위한 프로세스는 사실상 구매한 제품과는 별개의 개별적인 운영 프로세스를 새롭게 수립해야 하므로, 운영의 안정화까지는 다소 많은 시일이 소요되는 문제를 해결하기 위한 사항이다. 따라서, DDoS 공격 대응을 위한 운영 프로세스가 DDoS 공격 대응 제품과 함께 제공되어야 DDoS 공격 대응을 위한 효율적인 운영이 가능하다.

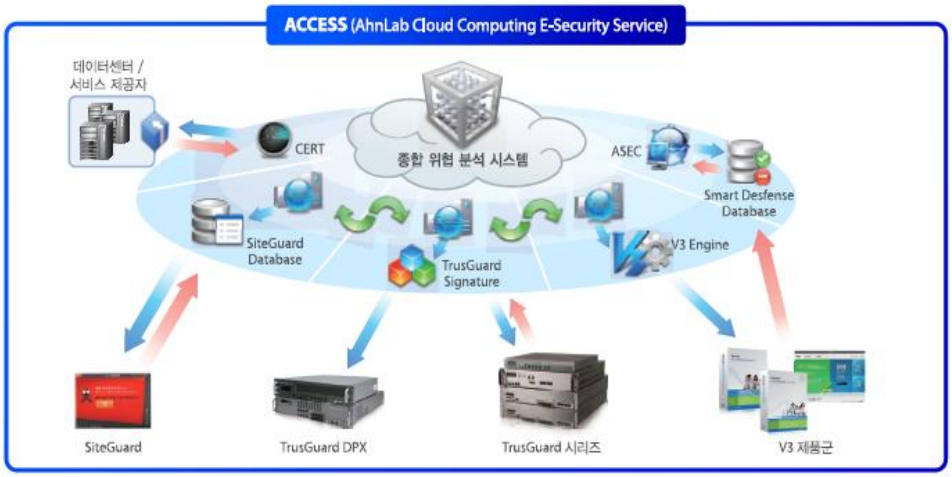
IV. 입체적인 DDoS 공격 대응 프로세스, AhnLab Trus Guard DPX

이에 대해 안철수연구소는 클라우드 컴퓨팅 기반의 DDoS 공격 대응을 수행하는 DDoS 전문 장비인 트러스가드 DPX(DDoS Prevention eXpress) 출시를 통하여 새로운 형태의 DDoS 공격 기법을 제시한다. 특히 ACCESS(AhnLab Cloud Computing E-Security Service)의 전략 하에 악성코드 분석 기술과 대응 기술, 클라이언트부터 네트워크까지 이르는 모든 제품들의 유기적인 연동을 통하여 제품 단독으로의 공격 대응이 아닌 입체적인 DDoS 공격 대응을 할 수 있다. 이를 통하여 트러스가드 DPX 는 DDoS 공격의 사전 예방→정확한 공격 방어→오탐 최소화→운영 프로세스 제공의 4단계 순환 고리 형태의 입체적인 DDoS 공격 대응 방법을 제시한다.



[그림 4] AhnLab TrusGuard DPX 4단계 공격 대응 프로세스

먼저 'DDoS 공격의 사전 예방'은 안철수연구소의 '클라우드 컴퓨팅 기반의 DDoS 공격 탐지 및 차단 기술 특허'를 이용한 것으로, 트러스가드 DPX 제품과 유기적인 연동을 통하여 클라이언트 레벨과 네트워크 레벨의 DDoS 공격 탐지 및 방어 기능을 제공한다. 즉, V3 Lite 등 클라이언트 레벨의 보안 제품에서 DDoS 공격을 유발하는 악성코드 및 DDoS 공격을 탐지하며 이 정보를 네트워크 레벨의 트러스가드 DPX가 악성코드 전파의 사전 예방과 동시에 DDoS 공격 트래픽 방어를 위한 정책 권고 및 업데이트한다. 아울러 클라이언트 레벨에서는 악성코드 제거를 통한 원천적인 DDoS 공격을 차단한다.



[그림 5] ACCESS 기반의 DDoS 방어 프로세스 제공

물론, DDoS 공격 대응 전용 장비로써 공격의 정확한 탐지와 오탐 최소화 기능은 필수 요건이다. 트러스가드 DPX는 수년 간의 DDoS 장비 구축 및 운영 노하우와 악성코드 분석 기술을 통하여 발생하는 대부분의 DDoS 공격에 대응할 수 있다. 즉, 클라이언트 레벨과 네트워크 레벨의 공격 탐지 및 차단의 연동을 통하여 신속하고 정확한 공격 방어 기능을 수행하게 된다. 또한 기존의 제품들이 가장 문제가 되는 공격 방어 동작 시 오탐 발생을 최소화하는 기능이 내장되어 있다.

[그림 6] TrusGuard DPX의 강력한 오탐 회피 기능

아울러 DDoS 공격 대응의 운영 프로세스를 위하여 안철수연구소는 트러스가드 DPX 출시와 동시에 다양한 서비스 상품도 함께 출시했다. 고객의 환경과 요구 사항에 따라 DDoS 제품 구축 전 운영 프로세스의 가이드라인 마련을 위한 'DDoS 사전 컨설팅 서비스 상품'과 정기적인 DDoS 공격 대응 운영 프로세스를 점검할 수 있는 전문가의 'DDoS 모의 공격 대응 훈련 서비스' 및 24시간 365일 DDoS 제품의 운영을 원격 또는 파견 아웃 소싱 서비스를 제공하는 'DDoS 보안 관제 서비스' 등 고객의 필요에 따라 추가적인 서비스 상품을 이용할 수 있다.

Ⅴ. 결론

앞서 살펴본 바와 같이 DDoS 공격은 더 이상 하나의 포인트에서만의 대응은 불가능하도록 지능적으로 변화하고 있다. 따라서, DDoS 공격에 효율적으로 대응하기 위해서는 클라이언트 레벨과 네트워크 레벨의 공격 탐지 및 방어가 입체적으로 이루어져야 한다. 이와 함께 효과적인 운영 프로세스를 통하여 보다 빠르고 정확한 공격 대응이 가능해야 한다. 따라서 전문 조직의 입체적인 DDoS 공격 대응 프로세스를 기반을 통하여 IT 환경의 사이버 위협에 대해 적극적으로 대처해 나아가야 할 시점이다.

