이것만은 알아야 할 네트워크 보안 이야기

Part 5. DDoS 1. DDoS 공격의 방식과 유형, DDoS 방어 장비

글. 이선응 아이크래프트 수석

연재 목차

이번 호에서는 DDoS 공격에 대해 알아보도록 하겠다. DDoS는 Distributed Denial of Service의 약자로 분산된 서비스 거부 공격이라고 하여 인터넷에 연결된 여러 개의 단말(통상 좀비PC)이 특정한 목적지(공개된 웹, DNS 서버 등)로 패킷을 대량으로 전송하여 해당 서버가 정상적으로 서비스되는 것을 방해하는 행위를 뜻한다. 이 공격은 정치적인 이슈에 대한 주장을 위한 과시, 경쟁업체 방해를 통한 사익추구, 협박을 통한 금전적 이익 추구 등 다양한 목적으로 발생하는 공격행위로 인터넷의 보급이 늘어나기 시작한 1999년부터 시작되어 2010년 이후 급속히 증가하기 시작하였다.

그럼 DDoS 공격이 어떻게 이루어지는지 알아보자. [그림 1]과 같이 공격자는 사전에 확보한 악성코드에 감염된 좀비PC를 C&C(Command & Control) 서버를 통해 관리하면서, 공격대상이 정해지면 공격 유형을 결정하여 명령을 내린다. 공격 명령을 받은 C&C 서버는 관리하는 좀비PC에 공격대상 IP와 공격 시간, 공격방식 등을 지정하여 내려보내면, 좀비 PC가 실제 공격을 수행하게 되어 있다. 또한 새로운 공격방식이 개발되면 C&C 서버에서 좀비PC로 새로운 공격 모듈을 보내서 공격방식을 업그레이드하고 DDoS 공격 이외에도 스팸 메일을 보내거나, 감염PC의 정보를 탈취하는 등 다양한 종류의 공격을 수행할 수 있게 지속적으로 관리된다.

최근에는 일반 PC나 노트북 등의 전통적인 개인용 단말 장비뿐만 아니라 인터넷 연결이 가능한 통신 모듈이 설치된 가전제품, 센서 장비, 가정용 네트워크 공유기 등의 IoT(Internet Of Things) 장비를 해킹하여 공격을 수행하는 장비로 활용되고 있다. 각종 단말 장비의 보안이 강화되면서 단말을 해킹하는 난이도가 높아지게 되자 인터넷상에 공개되어 불특정 다수에게 다양한 서비스를 제공하는 공개 서버들, 예를 들면 표준시간 정보를 제공해주는 NTP 서버, 도메인네임 질의에 응답해주는 DNS 서버, 네트워크 서비스나 정보를 찾기 위해 사용하는 SSDP 서버 등을 활용하여 공격을 수행하는 서비스 반사증폭공격(Reflection/Amplification Attacks)이 최신 DDoS 공격방식으로 유행하고 있다.

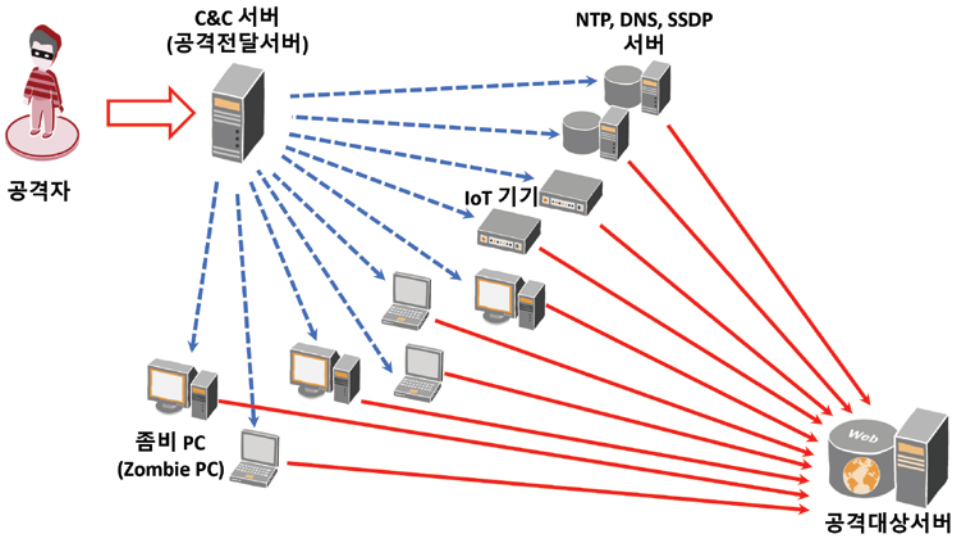

그림 1. DDoS 공격의 실행 방식

공격을 수행하는 좀비PC나 각종 IoT 장비의 CPU 성능이 높거나, 인터넷에 연결된 회선의 대역폭이 넓을수록 공격의 강도가 증가한다. 최근에는 멀티코어 CPU의 보급과 100Mbps 이상의 속도를 내는 회선에 연결된 단말이 증가하면서, 적은 수의 좀비PC나 IoT 장비로도 대용량의 DDoS 공격을 손쉽게 수행할 수 있는 환경을 갖추어 지고 있다.

DDoS 공격에는 어떤 종류가 있는지 알아보자. 최초로 나온 공격이면서, 최근까지도 가장 많은 공격 빈도를 보이는 공격이 용량(Volume) 기반 공격이다. 말 그대로, 대용량 트래픽을 공격목표로 무차별적으로 다량의 패킷을 전송하는 방식으로 주로 핑(Ping : 네트워크 연결상태 확인 용도)을 이용할 때 사용하는 ICMP와 집에서 보는 IPTV에서 사용되는 멀티캐스팅에 사용되는 IGMP, 그리고 가장 빈번하게 사용되는 UDP 패킷을 이용하는 공격이다. 이 공격은 인터넷에서 공격대상이 연결된 인터넷 회선의 대역폭을 소모시켜 회선 사용량을 100%로 만드는 단순하고 무식한 방법이지만 효과는 확실한 공격으로 서버 자체를 공격하는 것이 아니고 서버까지 가는 길목을 막아버리는 것이 목적이다. 대역폭 사용량이 100%가 되어 버리면, 더 이상 신규 트래픽을 수용할 수 없어서 정상서비스가 불가능해지는 방식으로, 회선 대역폭의 증설 밖에는 답이 없지만, 회선을 증설한다고 해도 손쉽게 증설한 양 만큼 공격트래픽이 채워버리면 무용지물이 되는 공격방식이다. [그림 2]와 같이 다수의 좀비 단말이 다량의 패킷을 생성하여 한곳의 공격대상으로 동시에 전송하는 방식으로 동작하여 공격을 수행한다.

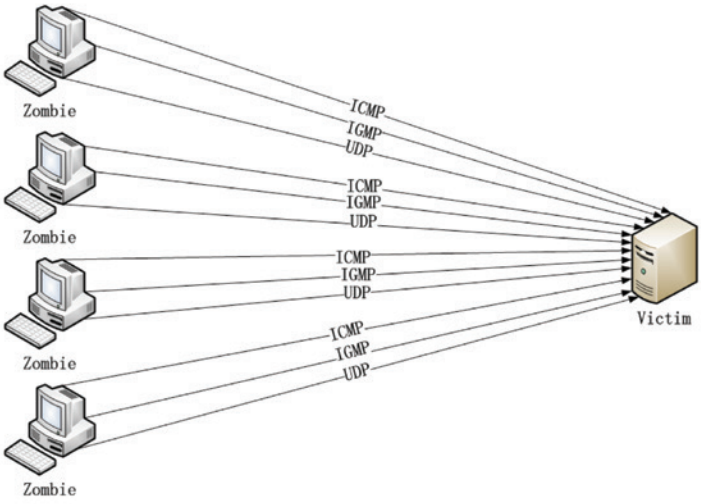

그림 2. ICMP/ IGMP/ UDP Flood 공격

두 번째 공격 유형은 자원 소모 공격으로 대표적인 공격은 TCP SYN Flood가 있다. 이 공격 유형은 회선 대역폭이 아니라 공격대상 서버의 TCP 연결 자원을 소모시켜 더 이상 신규 연결을 못 하게 차단하는 방식으로 동작한다. 즉 길목을 막는 것이 아니라 대상서버 자원을 소모시키는 것이 목적인 공격이다. [그림 3]의 왼쪽 그림과 같이 TCP 연결이 되기 위해서는 3way handshake라고 하여 연결이 필요한 단말이 대상 서버와 3단계(SYN- SYN/ACK-ACK) 통신을 통해 패킷 전송 준비를 하는 과정이 필요하다. 공격은 [그림 3]의 오른쪽 그림과 같이 연결 단계를 악용하여 최초의

SYN만 계속 보내고 서버가 보내는 2번째 SYN/ACK에 대한 3번째 ACK를 고의로 보내지 않아 서버가 계속 TCP 연결을 완료하지 못하게 해서 서버가 감당할 수 있는 TCP Queue를 초과하게 만드는 공격이다. 이렇게 큐가 Full이 되면 신규 TCP 연결이 안 되기 때문에 정상적인 서비스가 불가능하게 된다.

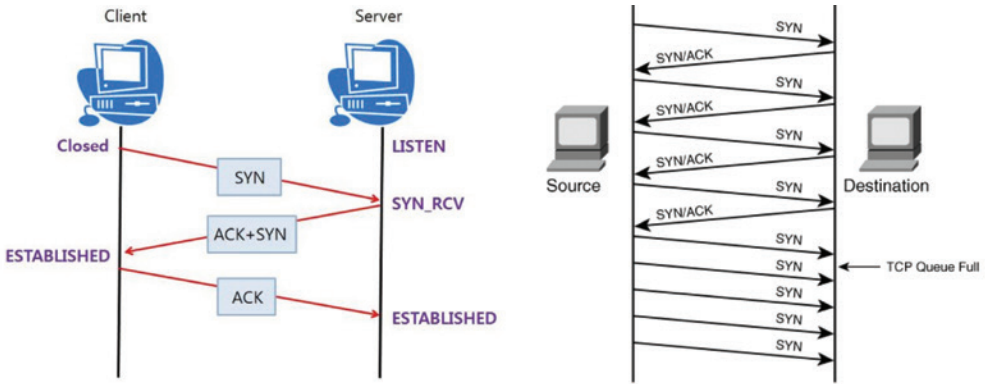

그림 3. TCP SYN Flood 공격

다음 공격 유형은 애플리케이션 공격으로, 앞의 2가지 공격은 주로 OSI 7계층 중 3~4계층을 이용한 공격이라면 이 공격은 7계층에서 이루어지는 공격이다. 사용자들이 가장 많이 사용하는 HTTP, DNS, VoIP 등은 외부에 공개되어 서비스되어야 하기에, 빈번하게 DDoS의 공격대상이 된다. [그림 4]와 같이 HTTP Get/Post 요청 트래픽을 대량으로 보내 웹 서버 데몬이 처리할 수 있는 한계를 넘겨서 더는 새로운 웹 접속이 못하게 방해하거나 HTTPS 기반 웹 서버의 경우 SSL 연결 과정을 악용하여 신규 접속을 방해하는 방식을 사용한다. DNS Flooding 공격의 경우 서버에 과도한 질의 요청을 보내 해당 서버의 DNS 데몬을 마비시키거나 VoIP 서버에 많은 양의 패킷을 보내 서버가 음성데이터를 처리할 수 없게 마비시키는 공격 등이 사용되고 있다.

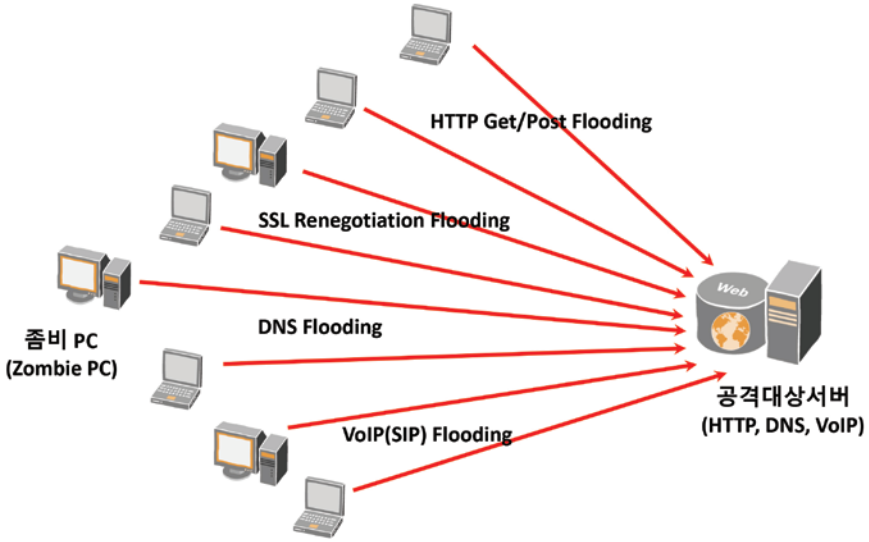

그림 4. Application(HTTP, DNS, VoIP) DDoS 공격

마지막으로 최근 5년 전부터 유행하기 시작한 서비스 반사/증폭 공격이 있다. 이 공격은 좀비PC나 IoT 장비를 활용하지 않고 공공적인 목적으로 공개되는 다양한 서버나 장비를 이용하는 공격으로 최근에 각광받고 있는 공격 유형이다. 통칭해서 DRDoS(Distributed Reflection Denial of Service)라고 불리는 공격으로 [그림 5]와 같이 정상적으로는 자신의 실제 IP를 이용하여 공개된 서버에 질의를 하면 해당 서버들은 정상적인 응답을 질의한 대상으로 응답을

보내게 되는데 이때 공격자가 자신의 IP가 아닌 공격대상 서버의 IP를 사용하여 응답 패킷이 공격대상으로 전송되게 만든다. 공격자는 'ntpdc -n -c monlist 192.168.34.85' 명령어를 서버로 보내면 NTP 서버에서 자신이 모니터링 중인 리스트의 상태 값을 공격대상 서버로 응답하게 되는 명령어인데 응답값이 최초에 질의한 명령어 대비 굉장히 많은 데이터를 가지고 있는 특징이 있다. 질의 요청에 대해 응답을 보내는 과정이 마치 공격자에게 와야 하는 트래픽을 공격대상 서버로 반사하는 것 같이 동작하고, 명령어 한 줄을 보냈는데, 수백~수천 라인의 응답이 마치 증폭되어 전달된다고 해서 반사/증폭공격 이라고 한다. 이 공격도 본질적으로는 용량 기반 공격과 동일한 효과를 낸다.

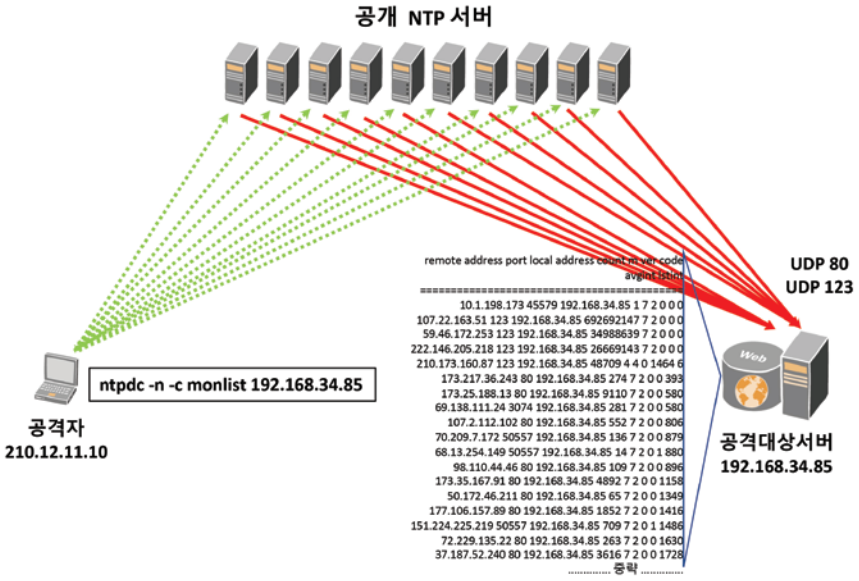

그림 5. NTP 반사, 증폭 DDoS 공격의 개념도

이런 유형의 공격이 유행하는 이유는 앞에서 예를 든 NTP뿐만 아니라 다양한 서비스들이 반사/증폭 공격에 활용 가능하기 때문이다. [그림 6]과 같이 DNS, SSDP, Chargen 등 다양한 프로토콜들이 공격에 활용되고 있으며, 공격명 옆의 수치에 있는 2017, 2018년 분기별 공격 탐지 횟수와 공격 크기와 같이 수백Gbps 단위의 공격이 탐지된 것을 확인할 수 있다. 아무래도 DNS 서비스가 광범위하게 사용 중이라서 공격 발생 수와 공격 크기에서 수위를 차지하고 있는 것을 확인할 수 있다. 만약에 좀비단말 등을 이용하여 100Gbps의 공격트래픽을 발생시키기 위해서는 수백~수천 개의 좀비단말이 필요하겠지만 공개 서버를 이용하면 훨씬 적은 자원으로 대용량의 공격이 가능한 장점이 있어 빈번하게 발생한다고 생각된다.

Reflection Amplification Stats

ATTACK TYPE	2017 2H	2018 2H	2017 2H Attack Size	2018 2H Attack Size
DNS Amplification	307,810	251,355	529 Gbps	388 Gbps
NTP Amplification	235,550	206,586	529 Gbps	260 Gbps
SSDP Amplification	51,501	79,960	528 Gbps	287 Gbps
Chargen Amplification	47,223	22,150	157 Gbps	128 Gbps
TCP SYN/ACK Amplification	1,546	21,628	77.9 Gbps	156 Gbps
SNMP Amplification	13,293	18,523	158 Gbps	210 Gbps
rpcbind Amplification	640	9,011	53.3 Gbps	121 Gbps
memcached Amplification	3,700	5,125	43.9 Gbps	245 Gbps
mDNS Amplification	485	1,616	8.28 Gbps	186 Gbps
MS SQL RS Amplification	437	1,593	105 Gbps	75.8 Gbps
NetBIOS Amplification	51	856	24.4 Gbps	121 Gbps
RIPv1 Amplification	68	293	21.2 Gbps	64.7 Gbps
TOTALS	658,651	716,437		

그림 6. DRDoS(반사/증폭 DDoS)의 종류별 공격 횟수 및 크기 / 출처 : 아버네트웍스

DRDoS가 트랜드를 선도하는 핫한 공격방식이 되면서, 공격자들은 기존에 사용 중인 프로토콜을 분석하여 공격에 활용할 수 있는 대상을 계속 찾아내

고 있다. [그림 7]과 같이 원소주기율표 같이 표시된 표는 2018, 2019년도에 탐지된 새로운 유형의 DRDoS를 명칭과 탐지 연도, 공격에 악용되는 서버의 개수를 기준으로 산출한 위험도 그리고 증폭지수를 표시하여 나열하였다. 증폭지수라는 것은 공격을 유발하기 위해 전송한 데이터양 대비 응답으로 발생하는 데이터양의 비율을 표시한 값이다. 예를 들면 증 지수가 100:1이라고 하면 공격자가 1Mbyte를 서버로 전송하면 서버는 100Mbyte의 응답 패킷을 공격대상 서버로 전송하는 것을 의미한다. 즉 증폭지수가 높을수록 효율적인 공격이 가능한 것을 의미한다. 2020년 이후에도 반사/증폭 공격에 악용되는 프로토콜이 추가될 것으로 예상된다.

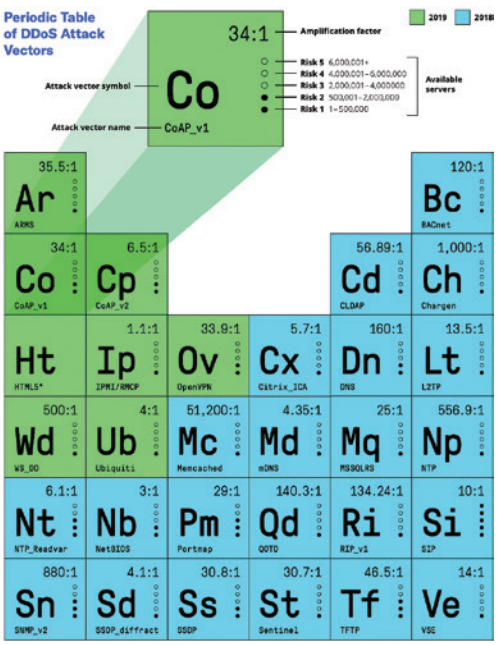

그림 7. DRDoS 유형별 증폭지수 및 공격 위험도
/ 출처 : 아버네트웍스

앞에서 설명한 다양한 DDoS 공격 유형을 [표 1]과 같이 정리하였다. 용량기반 공격은 다량의 덩치가 큰 패킷을 보내기 때문에 공격을 측정하는 단위가 BPS가 된다. 즉 특정한 출발지에서 특정한 목적지로 보내지는 트래픽의 양(Bit)을 초 단위로 측정하여 일정 임계치를 넘어서면 공격으로 판단하기 위해 BPS 단위가 활용되는 것으로 DRDoS도 이 공격 유형에 포함된다. 자원소모 공격의 경우 패킷의 크기가 아니고 패킷의 개수가 중요하다. 즉 크기가 작은 패킷이라도 초당 얼마나 많은 패킷을 보냈는지 측정하여 공격 여부 판단에 사용하기 때문에 PPS라는 단위가 사용된다. 마지막으로 애플리케이션 공격의 경우 OSI 7계층에서 이루어지는 공격이므로 초당 얼마나 많은 요청(Request)이 전달되었는지가 공격 판단의 기준으로 사용되기 때문에 RPS라는 단위가 사용되는 것이다. 일단 공격이 들어오면 처음에는 BPS와 PPS 단위로 동시에 측정이 되기 때문에 각 공격의 특성에 따라 어떤 단위를 기준으로 분석할 건지 숙지해야 해당 트래픽이 공격인지 정상적인 트래픽인지 확인이 가능하다.

용량 기반 공격 **Volumetric Attacks**	UDP / ICMP Floods IP / TCP / UDP Fragments floods **DNS / NTP / SSDP Amplification (반사증폭공격)**	**BPS** **(Bit Per Seconds)**
자원 소모 공격 **State Exhaustion**	TCP SYN (ACK) Floods Window Size Attacks (Sock stress) Slow TCP Connections (TCP Idling)	**PPS** **(Packet Per Seconds)**
애플리케이션 기반 공격 **Application Layer Attacks**	HTTP Get / Post Floods (LOIC, HOIC) HTTP Slow request (Slowloris, Pyloris) DNS Floods (DNS water torture) DNS Authentication SSL Renegotiation (THC, Pushdo) VoIP Floods (SIP)	**RPS** **(Request Per Seconds)**

표 1. DDoS 공격의 유형 / 출처 : 아버네트웍스

그럼 앞에서 설명한 다양한 DDoS 공격들이 어느 정도 빈번하게 발생하고 공격의 크기(강도)는 어떻게 되는지 통계정보를 알아보자. [그림 8]과 같이 공격의 60%는 볼륨 기반 공격이 차지하고 있다. 최근 서비스 반사/증폭 공격이 유행하면서 볼륨 기반 공격이 압도적인 탐지 횟수를 자랑하고 있다. 공격의 사이즈 즉 강도는 500Mbps가 70% 정도로 탐지되고 있고, 1Gbps 이상의 크기도 20% 정도를 차지 하나 이 비율은 증가하고 있는 추세이다. 이 통계자료는 아버

네트웍스라는 벤더에서 전 세계에 설치된 장비에서 탐지된 공격을 기반으로 작성한 자료이므로 실제 공격 추이와는 다를 수 있으나, 전 세계 ISP와 대형 고객에 주로 설치되어 동작 중인 장비라서 대략적인 공격 트랜드와 추이 변화에는 참고할 수 있는 자료라 생각된다.

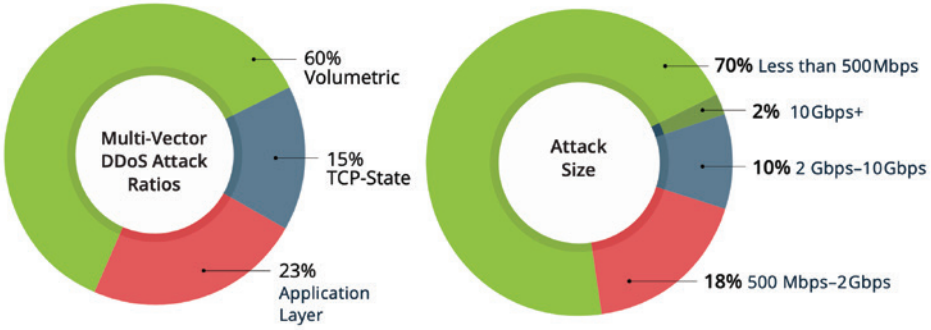

그림 8. 최근 DDoS 공격의 종류와 공격 크기 통계(2018년 기준) / 출처 : 아버네트웍스

[그림 9]는 장비가 설치된 지리적인 정보를 기반으로 실시간으로 탐지되는 DDoS 공격에 대한 현황을 확인할 수 있는 그림이다. 그림에서 노란색은 공격이 출발하는 곳이고 주황색은 공격목적지인데, 그림을 캡처한 시간에는 미국과 남미, 중동지역이 공격목적지가 되는 것이 확인되고, 대한민국의 경우 국내에서 이루어지는 DDoS 공격이 소규모 탐지되는 것을 확인할 수 있다.

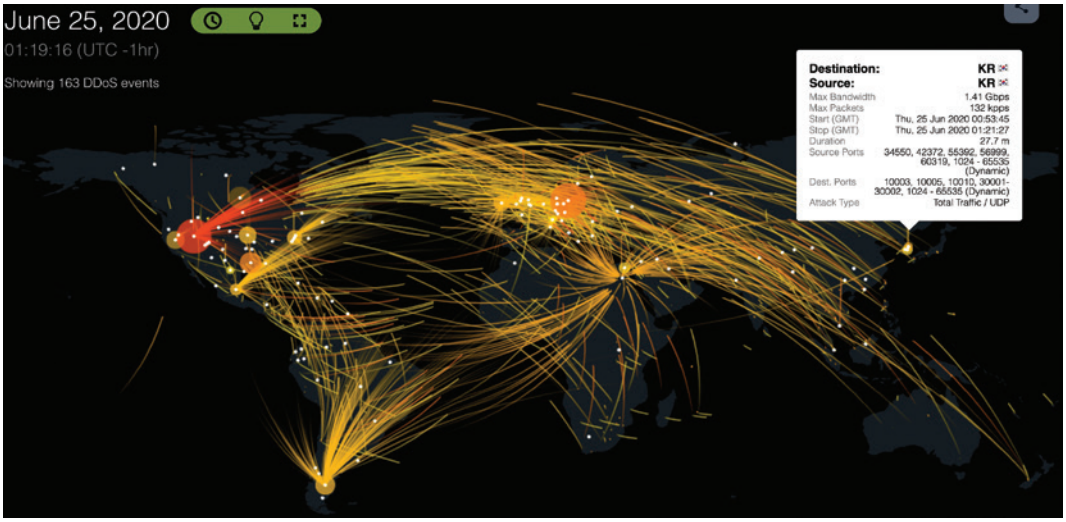

그림 9. 글로벌 실시간 DDoS 공격 현황 / 출처 : 아버네트웍스

다음으로 이렇게 다양한 DDoS 공격을 정확하게 탐지하고, 탐지한 공격을 완벽하게 차단하기 위해 어떤 DDoS 방어 장비(Anti-DDoS)가 사용되고 있는지 알아보자. 관리자의 입장에서는 악의적인 공격자가 실제로 DDoS 공격을 해서 웹서버가 마비되었는지 아니면 정상적인 많은 사용자가 짧은 시간 안에 폭주해서 마비되었는지 정확하게 구분하기가 힘들다. 웹서버를 관리하는 입장에서는 웹데몬(홈페이지를 전달해 주는 프로그램)이 죽는 것으로밖에 확인되지 않고, 라우터, 스위치 장비에서는 특정 시간대에 많은 양의 패킷이 왔다는 것밖에 확인되지 않기 때문에 정확한 공격 여부를 확인하기 힘들다.

인터넷 회선의 제일 앞에서 공격을 방어하는 방화벽에서는 DDoS 공격을 탐지하고 차단할 수는 있을까. 대부분의 방화벽에서는 용량기반이나 자원소모 공격에 대해 부분적으로 탐지와 차단은 가능하나 완벽한 차단은 불가능하다.

UDP/ICMP/SYN Flood 공격의 경우 초당 들어오는 패킷 개수를 측정하여 PPS 단위로 임계치를 지정하여 임계치 이상으로 들어오는 패킷은 무조건 차단할 수 있는 기능이 있지만, 이런 기능으로는 초보적인 방어만 가능하며 더욱이 애플리케이션 기반 공격은 탐지와 차단 차제가 불가능하다.

그래서 DDoS 공격만 전문적으로 방어하는 장비가 등장하게 되었다. DDoS 공격을 방어하기 위해서는 크게 탐지와 차단 두 가지 기능으로 구분 할 수 있다. 아무리 차단이 잘 되더라도 탐지가 되지 않으면 방어 자체가 불가능하다. 일반적으로 가장 많이 사용하는 탐지 방법이 임계치를 지정하여 임계치를 넘으면 공격으로 판단하는 방법이다. 임계치를 어떻게 설정하느냐에 따라 공격 탐지의 정확도가 좌우된다. 특정한 서버의 IP로 들어오는 트래픽을 모니터링하는데 24시간 중에 밤보다는 낮 시간대, 낮에서도 출근 시간 후 1~2시간 그리고 퇴근 1~2시간 전과 같이 특정한 시간에 트래픽이 증가하게 된다. 이렇게 시간에 따라 트래픽의 양이 변하게 되는데, 고정된 임계치를 사용한다면 공격 탐지의 정확도가 낮아지게 된다.

또한, 임계치를 지정하는 기준이 특정한 목적지 IP로 들어오는 트래픽을 합산한 양인지, 출발지 IP를 기준으로 합산한 양인지, 아니면 출발지, 목적지 IP를 쌍으로 하여 모든 연결에 대해 각각의 트래픽 합산 양을 임계치로 사용할 건지에 따라 공격 탐지의 정확도가 달라지게 된다. 초기 장비의 경우 구현이 쉽고 장비에 부하가 가지 않는 방법인 출발지 혹은 목적지 IP 기준으로 모니터링하였으나 이런 방법이 공격 탐지에 그다지 효과적이지 않다고 판별되고, 시스템의 연산처리 성능이 증가하면서 출발지, 목적지를 모두 모니터링하는 방식으로 발전하게 되었다. 보다 자세한 공격 탐지에 대한 내용은 다음 호에서 소개하도록 하겠다.

전문적인 DDoS 방어 장비는 완전히 새로운 장비가 아니고 기존에 존재하던 보안장비에 있는 기능을 활용하는 방식으로 개발이 시작되었다. 방화벽이나 IPS, 혹은 L7 스위치, QoS(Quality of Service) 장비 등에서 공격 탐지와 방어에 유용한 기능을 재활용하고, 재활용된 기능을 좀 더 강화하여 옵션을 추가하는 방식으로 발전하게 되었다. 그래서 여러 벤더에서 개발된 방어 장비는 어떤 보안장비를 베이스로 개발되었는지에 따라 장단점이 존재하게 된다. 기존의 보안장비에서 어떤 기능이 DDoS 공격방어에 활용되는지 [표 2]를 통해 확인해 보자. 방화벽의 보안정책기술은 이미 알려진 공격자나 국가의 IP를 차단할 때 활용되고, IPS의 패턴탐지기능은 패킷 내 특정 패턴을 탐지하여 공격을 탐지/차단하는데 활용된다. L7 스위치의 경우 트래픽 세션 분석과 HTTP 등 애플리케이션 레벨 탐지 기능을 활용하여 복합적인 L3~L4 레벨 및 L7 공격을 방어할 수 있다. 마지막으로 QoS 장비의 쉐이핑(Shaping) 기술은 공격대상으로 가는 대용량 트래픽을 일정량 이하로 줄여서 서버가 받는 부하를 일정 수준 밑으로 유지시켜 주는데 사용된다.

보안장비	차용 기술	DDoS 방어 적용 분야
방화벽	보안정책	알려진 공격자 IP 차단 블랙/화이트 리스트 적용 국가별 트래픽 허용/차단
IPS	L3/L4 계층 검사	ICMP/UDP/SYN Flooding 탐지
	L7 계층 패턴 검사	특정 패턴 공격 트래픽 차단
L7 스위치	트래픽 세션 분석	공격 단말의 공격 트래픽 탐지/차단
	HTTP/HTTPS/DNS/VoIP 트래픽 분석	L7 기반 공격에 대한 탐지 및 차단
QoS	트래픽 용량 제한	필터 조건에 따라 트래픽 양을 일정량 이하로 제한

표 2. 기존 보안장비에서 차용된 DDoS 방어 기술

이렇게 발전된 방어 장비는 [그림 10]과 같이 크게 인라인(Inline) 방식과 아웃오브패스(Out of Path) 방식으로 구분되어 진화하게 되었다. 먼저 인라인 방식의 장비가 현재 시장에서 가장 흔하게 볼 수 있는 방식으로 인터넷과 서버가 연결된 회선 라인상에 장비를 설치하여, 서버와 단말 간의 트래픽을 모니터링하다가 공격을 탐지하게 되면 직접 차단을 수행하는 방식으로 작동하는 장비이다. 그림의 녹색 라인은 정상적인 트래픽이고, 빨간색은 공격으로 탐지된 트래픽으로 방어 장비에서 차단되게 된다. 이렇게 라인 위에 위치하기 때문에 인라인 타입이라고 불린다. 소규모에서 대규모까지 다양한 방어 성능을 제공하는 제품라인업이 있으며, 시장의 70~80%는 인라인 방식의 장비가 보급되어 있다.

다음으로 아웃오브패스 방식의 장비는 탐지와 차단 장비가 분리되어 작동한다. 평상시에는 탐지 장비가 트래픽을 모니터링하고 있고 트래픽은 차단 장비를 거치지 않고 바로 서버로 전달된다. 탐지 장비가 공격을 탐지하게 되면, 공격 대상 서버 IP 주소를 확인하여, 해당 서버로 가는 트래픽만 선별적으로 차단 장비로 우회시켜 공격을 차단하는 방식으로 작동한다. 그림에서 녹색 라인은 정상적인 트래픽이므로 차단 장비를 거치지 않고 바로 전달되고, 빨간색 라인은 공격으로 탐지되어 차단 장비로 우회되어 차단되게 된다. 공격대상으로 가는 정상적인 트래픽도 차단 장비로 전달되지만 차단 장비에서 정상 트래픽으로 판단하면 차단되지 않고 서버로 전달되게 된다. 탐지와 차단이 분리되어 있어 인라인장비에 비해 좀 더 효율적으로 공격 대응이 가능하지만, 비교적 공급 단가가 높은 점과 설치가 다소 까다롭기 때문에 적용 가능한 환경이 한정적인 단점이 존재한다.

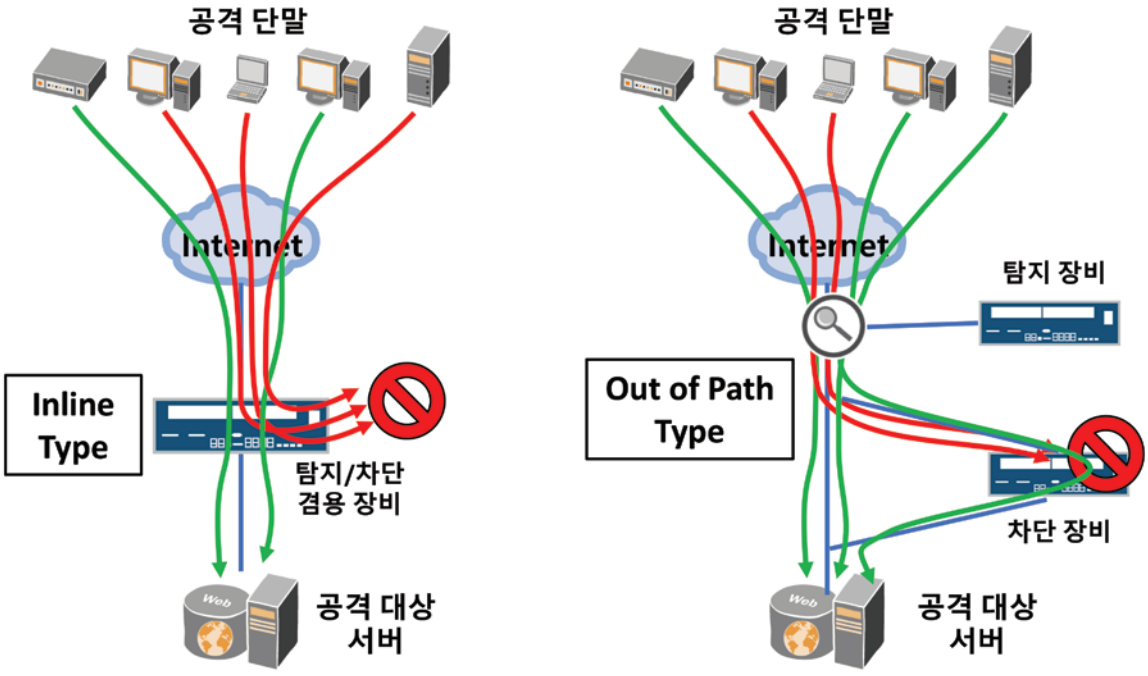

그림 10. Inline 방식과 Out of Path 방식의 DDoS 방어 장비

마지막으로 인라인 장비와 아웃오브패스 장비의 장단점을 비교하면서 이번 호를 마무리하겠다. [표 3]과 같이 인터넷 회선이 1~4개로 적은 일반적인 소~중규모 기업의 경우에는 인라인 장비가 설치가 간편하고 유지보수에 유리한 점이 있다. 그에 비해 아웃오브패스 방식 장비는 반드시 회선 위에 설치될 필요가 없어 모니터링해야 하는 회선이 많은 KT, SKT 같은 회선 사업자나 대기업 혹은 중견기업 등 별도의 IDC를 운영하는 기업에 적합하다. 실제로 국내에 있는 대부분의 기업은 인라인 방식의 장비가 운영 중이며 KT, SKT, LGT, 삼성 등과 같은 대규모의 회선을 보유한 기업은 아웃오브패스 방식의 장비가 운영 중이다.

모니터링하는 회선을 정원에 있는 나무라고 가정해 보자. 나무가 얼마 없는 고객사는 그냥 나무만 직접 확인하면서 병충해가 없는지 가지는 쳐야 하는지, 영양제는 언제 줘야 하는지 등 직접 관리하는데 문제가 없지만, 나무가 굉장히 많아 거의 숲을 이루는 규모에서는 나무 하나하나를 직접 관리하기가 힘들다. 이때는 높은 곳에서 숲을 바라보고 있다가 잎의 색깔이 바뀌거나, 잎이 많이 떨어져서 앙상할 경우에만 그 나무로 가서 직접 확인해 보고된다. 회선의 경우도 마찬가지이다. 모니터링 대상이 얼마 없으면 장비가 직접 회선에 흐르는 트래픽을 직접 모니터링하면서 관리하면 되지만, 관리해야 하는 대상이 많은 경우에는 회선에 흐르는 트래픽을 일일이 모니터링하기에는 조직의 자원이 부족하다. 이럴 경우 L4 레벨의 트래픽만 모니터링하다가 무언가 낌새가 이상하거나 조금이라도 문제가 있다고 생각될 때, 해당 트래픽만 선별적으로 직접 트래픽을 확인해서 실제 공격 트래픽이면 차단하는 방식을 사용하는 것이 아웃오브패스 방식의 동작 방식이다.

내용	Inline 방식	Out of Path 방식
설치 위치	제한적임 (트래픽 발생 위치에 설치해야 함)	제한 사항 없음 (트래픽 발생지점과 분리되어 설치)
동시 탐지회선	제한적임	무제한
구성 난이도	낮음 (인라인 혹은 TAP 장비에 설치)	높음 (탐지와 차단 장비 별도 설치)
탐지/차단 구성	탐지/차단을 한 장비에서 수행함	탐지/차단 장비가 분리되어 구성됨
탐지 속도	1분 이내 탐지 가능	1~5분 소요됨
시스템 부하	높음 (L7까지 모니터링 시)	낮음 (L4까지만 탐지)
시스템 장애 영향	구성에 따라 서비스 영향 있음 (서비스라인에 설치 시 장애 발생)	서비스 영향 없음 (장애 발생 시 서비스와 무관함)
탐지 범위	L7까지 탐지 가능 (직접 트래픽을 수집하여 분석)	L4까지 탐지 가능 (Flow 기반의 데이터로 분석)
권장 탐지 위치	기업 단위의 단일~이중화 회선 사용지점	ISP 레벨의 많은 회선의 대용량 트래픽 발생지점
권장 적용 분야	소~중용량 (중~소 규모 기업)	중~대용량 (ISP 나 ISP 레벨의 기업)

표 3. 인라인 방식과 아웃오브패스 방식의 장단점

그럼 다음 호에서는 어떻게 DDoS 공격을 오탐(정상트래픽을 공격으로 탐지) 및 미탐(공격트래픽을 정상으로 탐지) 없이 탐지할 수 있는지 대해 알아보도록 하겠다.