IP SWAP

한신대학교 IT대학 정보통신학부
김용학, 이경호, 장시찬

본 아이디어 제안서는 DDoS(Distributed Denial of Service)라는 서비스 거부 공격을 통해 발생하는 악성코드의 감염, 서버 마비, 개인정보 유출 등의 피해를 막기 위해 공격 목표가 된 서버의 IP를 SWAP하는 시스템을 구현하고자 한다. DDoS는 한 번에 여러 대의 PC를 동작하게 하여 특정 서버에 접속시켜 비정상적으로 트래픽을 늘려 해당 서버를 마비시키는 해킹방법이다. 이러한 공격 방식을 차단하기 위해 평시에 트래픽 및 응답대기시간을 감시하여 특정 트래픽 수치 및 정해진 기준의 응답대기시간을 초과하게 되면 기존의 공격목표가 되었던 IP에서 목표가 아닌 안전한 IP로 SWAP함으로서 서버 마비 및 제 2의 피해를 줄이고자 한다.

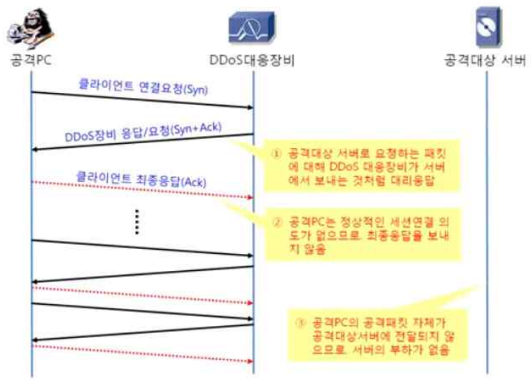
1. 아이디어 제안 배경 및 필요성

DDoS(Distributed Denial of Service)는 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래의 의도된 용도로 사용하지 못하게 되는 기술인 DoS(Denial of Service)에 일종이지만 이와 달리 여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 서버를 공격하는 해킹 기술이다.

카스퍼스키랩의 3분기 DDoS 공격 보고서에 따르면 이번 분기에는 전 세계 79개국에서 DDoS 공격으로 인한 피해가 발생했고 우리나라를 포함한 중국(1위), 미국(2위)이 DDoS 공격에 가장 많이 노출된 것으로 드러났다. 특히 우리나라는 DDoS 공격이 2분기 대비 7.9% 증가한 17.7%의 비율을 차지, 가장 큰 증가폭을 기록하며 3위에 올랐다. 중국은 34.5%, 미국은 20.8%를 기록했지만 증가폭은 5%를 넘지 않았다.[1] 피해도 늘어나고 있지만 공격기술이 점점 더 지능적으로 발전해가고 있는데 기존의 기술에서 공격지속시간은 짧아지고 있지만 공격에 사용되는 대역폭이 매년 증가하고 있다.

2. 목표

기존의 DDoS 공격 대응 방안으로는 공격대상 서버에 DDoS 대응 장비를 연결하여 공격 시작 시 직접적으로 서버에 피해를 주는 것이 아닌 대응 장비에 공격이 가해지게 된다.



[그림 1] DDoS 공격 대응 장비의 방어 과정

대응 장비를 통해 DDoS 공격의 피해는 막을 수 있지만 대응 장비의 유지 및 보수비용을 무시할 수는 없다. 또한 대응 장비 역시 최대 한계용량을 지니고 있는데 이러한 한계용량을 뛰어넘는 공격을 받게 된다면 대응 장비는 무용

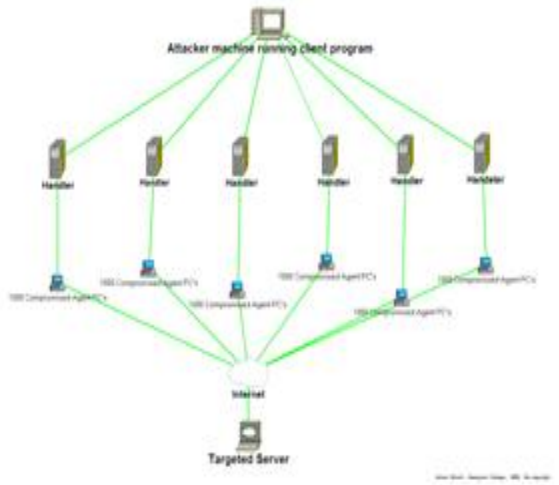
지물이 된다. 하지만 보안회사의 서버나 대응 장비에서 가상의 또는 실질적으로 사용하지 않는 IP를 공격대상의 서버의 IP와 바꾼다면 서비스 거부 공격으로 인한 서버의 피해를 줄이고자 한다. 대응 장비의 한계용량에 구애 받지 않으며 유지 및 보수비용도 줄일 수 있다.

3. 분석 및 아이디어 내용

3.1 DDoS 분석

3.1.1공격구성도

ddos는 웹하드 등 여러 경로를 이용해 다수의 agent를 만들어 분산적으로 대상을 공격해 event를 일으킨다.



[그림2]ddos 공격 구성도

공격자(해커)는 handler역할을 하는 master를 만들어 명령을 한다. handler역할을 하는 PC는 그 하위에 있는 agent pc로서 victim(공격대상)에 공격을 가한다. 공격자들은 DDOS공격을 위해 Trinoo, TFN, TFN2K, Stacheldraht와 같은 프로그램들을 사용한다.

3.1.2공격방식

다수의 agent를 이용한다는 점에서는 유사하지만 ddos의 공격의 큰 틀은 대역폭 소진공격과 서비스(어플리케이션) 마비공격으로 나뉘어진다. 대역폭 소진 공격은 다수의 pc를 이용하여 대량의 패킷을 전송하여 네트워크 대역폭의 처리 한계를 초과시켜 event를 발생시킨다. 이는 bps를 이용한 공격으로 주로 1Gbyte 이상의 급작스런 트래픽 증가가 발생하여 같은 네트워크에 있는 다른 서버까지 접속 쟁애가 유발된다. 자원고갈 공격과 어플리케이션 공격도 tcp를 이용한 pps(Packet Per Second)를 증가시키는 공격과 과다 접속을 유발하여 cpu부하를 일으키고 접속장애를 일으킨다.

비고	대역폭 소진공격	서비스(어플리케이션) 마비공격
대표 공격유형	UDP/ICMP Flooding, SYN Flooding	HTTP GET Flooding
공격의 형태	○UDP/ICMP Traffic Flooding UDP/ICMP Flooding, DNS Query Flooding 등 ○TCP Traffic Flooding SYN Flooding, SYN+ACK Flooding 등 ○IP Flooding IP Header Option 변조(LAND Attack), IP Fragment Packet Flooding (Teardrop, HTTP Continuation 등) 등	○HTTP Traffic Flooding GET Flooding, GET with Cache-Control ○HTTP Header/Option Spoofing Slowris, Fragmented HTTP Header Attack(Slowloris/Pyloris) 등 ○TCP Traffic Flooding TCP Session, SYN Flooding, TCP Slow Read 등 ○Other L7 Service Flooding Hash DoS, Hulk DoS, FTP/SMTP Attack 등
프로토콜 (OSI 7-Layer 기준)	3~4계층 (Network, Transport 계층) : IP, ICMP, IGMP, UDP, TCP 등	7계층 (Application 계층) : HTTP, DNS, FTP, SMTP 등

[그림3]ddos 공격 유형 분류

대표 유형에는

㉠UDP/ICMP Flooding

㉡SYN Flooding

㉢HTTP Traffic Flooding

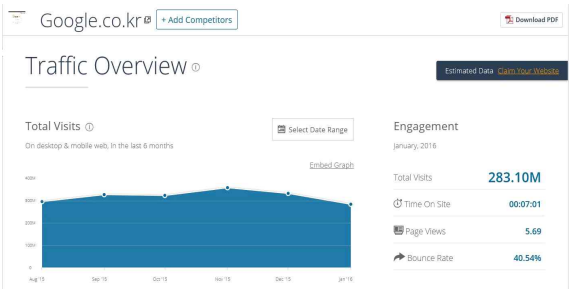
㉣GET flooding 등이 있다. hendler가 사용하는 프로그램, victim의 피해 대상은 다르지만 장비간의 통신에 의한 공격이라는 점은 동일하다. agent들은 공격대상의 주소를 포함한 명령을 받는다.

3.2 검출 조건

위에서 설명하였듯이 DDoS는 트래픽과 Server의 응답여부에 따라 공격을 판단할 수 있다. 그렇기 때문에 제안하는 아이디어를 평소에 작동하는 것 보다는 일정한 기준을 정해 기준치보다 높은 트래픽이나 백로그 큐를 감시하여 공격이 발생하게 되면 실행하고자 한다.

3.2.1 트래픽(Traffic)

트래픽(Traffic)은 웹 사이트에 방문하는 사람들이 데이터를 주고받은 양으로 이는 방문자 수와 방문 페이지 수에 따라 결정된다.[4] 웹 사이트의 서버가 DDoS 공격을 받게 된다면 기존의 트래픽에서 월등히 높은 트래픽이 발생하게 된다. 시만텍은 2014년 최고 400Gbps에 이르는 공격을 처음으로 발견했다. 2013년 최대 공격 대역폭은 300Gbps였다.[5] 하지만 평균 웹 서비스 서버의 트래픽의 경우 앞에서 말한 것보다 훨씬 적은 트래픽이 발생하게 된다.[6]

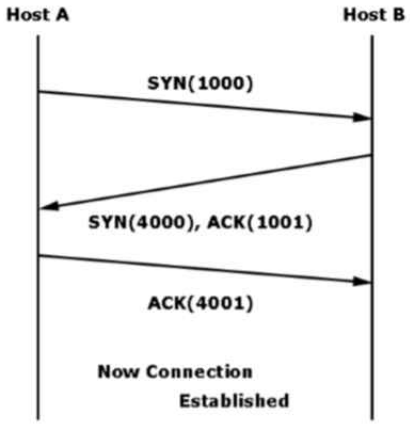


[그림 4] 구글코리아의 최근 3개월 트래픽 분석

이와 같이 서버의 트래픽을 실시간으로 조사하고 통계를 통해 기준의 상한선을 정할 수 있도록 한다.

3.2.2 백로그 큐(Backlog Queue) 감시

DDoS의 경우 TCP Half Open연결을 대량으로 생성하여 정상적인 세션연결을 시스템 자원을 고갈시키는 방법이 주로 이루어진다.[7]



[그림 5] TCP의 “ 3 Way handshaking ”

TCP Half Open 상태는 SYN+ACK 패킷을 받은 B 호스트는 A 로부터 응답이 올 것을 기대하고 반쯤 열린 “Half Open” 상태가 되어 대기 상태에 머무른 후 일정 시간(75초) 후에 다음 요청이 오지 않으면 해당 연결을 초기화하게 되는데, 초기화하기 전까지 이 연결은 메모리 공간인 백로그 큐(Backlog Queue)에 계속 쌓이게 된다. 백로그 큐의 크기는 각 서버마다 다르기 때문에 백로그 큐의 크기를 파악 후 평상시에 감시를 하여 백로그 큐가 3분의 2 이상이 사용될 시 공격감지를 할 수 있도록 한다.

위의 두 가지의 검출 조건을 통해 DDoS 공격을 감지하여 제안하는 아이디어, IP Swap를 할 수 있도록 하고자 한다.

3.3 IP SWAP 기술

3.3.1 Passive Scan & Active Scan

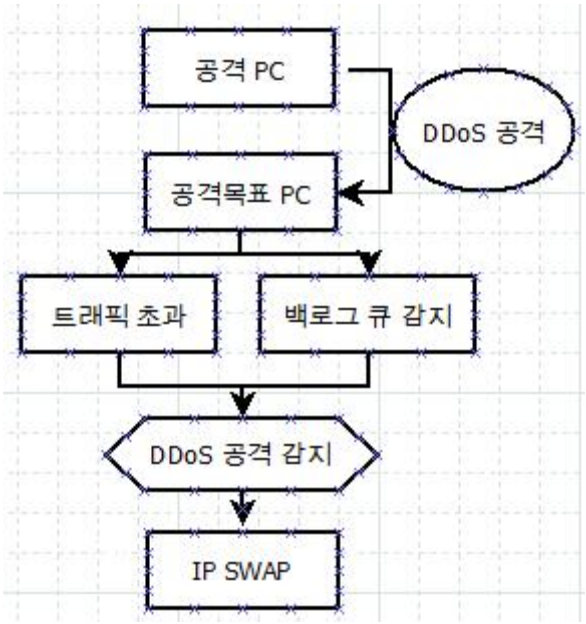
Passive Scan이란 무선랜 AP가 주기적으로 (예를 들면, 일반적으로 100ms) 보내는 비콘(beacon) 프레임을 단말이 수신해서 무선랜 AP의 존재를 확인하는 방법이다. 이 기술을 이용해서 AP 탐색이 아닌 사전에 등록해둔 여분의 IP를 탐색한다. Active Scan은 단말이 직접 프로브 요청 프레임(probe request frame)

을 AP에게 보내고, AP가 이 probe request frame을 수신하면, 프로브 응답 프레임(probe response frame)을 단말에게 응답함으로써 AP가 자신의 존재를 단말에게 알리는 방법이다. DDoS공격이 감지되면 Passive Scanning이 작동되어 IP를 자동으로 탐색하고, Active Scanning이 작동되면서 서버에서 프로브 요청 프레임을 Victim에게 보내고, Victim은 자동으로 수신되어 프로브 응답 프레임을 서버에 보낸다. 응답을 보냄으로써 DDoS공격을 받았다는 것으로 판단하여 IP Swap이 된다.

3.3.2 IP Swap

일정한 기준의 트래픽을 초과하였거나, 백로그 큐가 3분의 2이상이 사용될 시 DDoS 공격을 감지하여 Scanning기술을 자동으로 작동시켜 빠른 IP Swap을 한다. Scanning기술을 이용하여 IP를 감지할 것이다. 휴대전화에서 WIFI를 연결 전 신호를 검색하고 사용자가 선택하여 연결하는 것과 같은 방식으로 보안프로그램 서버나 국가에서 방어용 IP를 사용자 서버와 통신하여 송신을 시켜줌으로서 사용자 서버는 보안서버나 국가에서 송신시키는 IP를 감지한다. 하지만 조건에 충족하지 않는다면 감지만 할 뿐 Swap하지 않는다.

공격이 감지되면 감지한 IP로 바꿔 공격을 우회시켜 제 2의 피해를 막을 수 있다. 바뀐 IP를 보안서버나 국가에서는 분석을 통해 공격의 근원지나 공격방식을 발견하여 방어체계를 견고하게 하며 DDoS 공격을 줄일 수 있는 효과를 얻을 수 있다. 단순히 트래픽 뿐만 아니라 행동을 분석하여 이상 징후를 파악해 IP 별로 차단하는 것이 DDoS 공격을 방지하기에 가장 효과적일 것으로 판단한다.



[그림6]IP SWAP 순서도

4. 참고문헌

[1] 'DDos 공격대응 가이드' 한국인터넷진흥원(KISA) 2012

[2] 'DDos 지속공격 비교분석 및 대응방안' 한국방송통신전파진흥원 ,2013

[3] https://ko.wikipedia.org/wiki/%EC%9BB9_%ED%8A%B8%EB%9E%98%ED%94%BD

[4] http://it.donga.com/19554/

[5] https://www.similarweb.com/website/google.co.kr#overview

[6] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=15662