중소기업융합학회 논문지 제5권 제1호 pp. 19-23, 2015 ISSN 2234-4438

분산처리 공격에 대한 방어방법 연구

신미예
충북대학교

Distributed Attack Analysis and Countermeasure

Miyea Shin
Chungbuk National University

요 약 분산 서비스 거부 공격은 공격자가 한 지점에서 서비스 공격을 수행하는 형태를 넘어서 광범위한 네트워크를 이용하여서 다수의 공격 지점에서 한 곳을 집중적이게 공격을 하는 형태의 서비스 거부 공격이다. 특정 서버나 클라이언트에게 많은 접속 시도를 만들어서 정상적인 서비스를 사용하지 못하게 하는 방법 등등의 공격이 있다. DDoS 공격의 대응 방법에는 관리적 측면과 기술적 측면의 대응 이 두 가지를 제안 하였다.

주제어 : DDos 공격, 악성코드, 정보보호, Web 보안, 악성 봇 감염PC

Abstract Distributed Denial of Service attack is a form of denial of service attacks, the attacker to attack a place in a number of points of attack by a wide variety of forms over the network to perform a service on a point attack . Do not use a specific server or client attempts to make a connection to many services available that prevents this attack and so normally used . Corresponding methods of DDoS attacks has a corresponding managerial aspects and technical aspects of the proposed two .

Key Words : DDos, Malware, information Security, Web, Malicious bot-infected PC

1. 서론

디도스 공격은 네트워크를 통해 분포하는 호스트들이 서로 비정상적 패킷을 다량으로 일으키는 형태이다. 이러한 공격 형태는 망자원과 호스트들의 시스템 자원을 소비해서 정상적인 사용자들이 시스템이나 망에 들어와서 서비스를 이용하는 것을 방해하는 것이다. 이런 방해하는 것을 정상적인 이용자들이 효율적인 서비스 이용과 관리를 위해 디도스 공격에 도움을 주는 대응방법이 요구되고 있다 본 보고서의 구성은 다음과 같다. 2장에서는 DDoS와 DDoS의 공격 방법 및 유형 3장에서는 DDoS공격의 대응방안을 가술 했다. 마지막으로 4장에서는 본 보고서를 마무리하는 결론으로 나누어져 있다.

2. DDoS

2.1 DDoS

DDoS란 Distributed Denial of Service의 약자로써, DDoS공격은 공격자가 한 지점에서 서비스 공격을 수행하는 형태를 넘어 광범위한 네트워크를 이용하여 다수의 공격 지점에서 동시에 한 곳을 공격하도록 하는 형태의 서비스 거부 공격이다. Fig. 1은 DDoS 공격의 기본적인 구성도이다. Attacker는 공격을 주도하는 해커의 컴퓨터

Received 2015-02-15 Revised 2015-02-22 Accepted 2015-03-05
*Corresponding author : Miyea Shin (myshiny@cbnu.ac.kr)

이고 Master는 공격자에게 직접적으로 명령을 받는 시스템으로 여러 대의 에이전트를 관리한다. Agent는 공격 대상에게 직접적으로 공격을 가하는 시스템이다.[1]

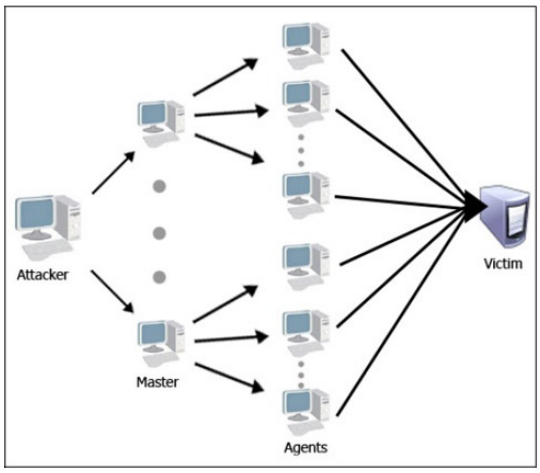

Fig. 1. Distributed Service Attack Configuration

2.2 DoS공격 방법

DDoS공격은 PPS(Packet Per Second)와 대용량 트래픽, 웹 서비스 지연의 유형으로 크게 공격이 있다. PPS(Packet Per Seconds) 증가 공격은 IP Spoofed Syn Flooding 공격, TCP Connection Flooding 공격, TCP Out-of-State Packet Flooding 공격이 있다.

이 3가지의 공격은 공격 대상 시스템 또는 동일 네트워크에서 사용 중인 모든 시스템을 피해를 입힌다. 사용 프로토콜은 TCP에서 사용하고 공격 PC 위치는 국내/국외이고 IP변조여부는 변조/실제IP 둘 다 같이 쓴다. 이 공격의 효과는 네트워크 장비, 보안장비, 서버 등의 부하를 발생하는 효과를 나타낸다. 대용량 트래픽 전송 공격은 UDP/ICMP Flooding 공격이 있다. 이 공격은 동일 네트워크에서 사용 중인 모든 시스템을 피해를 입힌다. 사용 프로토콜은 주로 UDP/ICMP이고 공격 PC 위치는 국내이다. IP변조여부는 변조/실제IP 둘 다 같이 쓴다. 이 공격의 효과는 회선 대역폭 초과를 시켜버린다. Http Flooding 공격은 동일한 URL 반복 접속 시도와 조회 반복시도가 있다. 이 2가지의 공격은 공격 대상 시스템만 피해를 입힌다. 사용 프로토콜은 HTTP이며 공격 PC 위치는 국내/국외이고 IP변조여부는 실제IP로 사용된다. 이 공격의 효과는 웹서버에 부하를 발생하는 효과를 나타낸다.

2.3 DoS 공격의 유형

DoS공격에는 취약점 공격형, 자원 고갈 공격형으로 나누어진다.

취약점 공격형에서는 3가지 공격이 있다. Boink, Bonk, TearDrop 공격이 있다. 이 3가지 공격은 오류 제어 로직을 악용하여 시스템의 자원을 고갈시키는 공격이다. TCP Protocol은 데이터 전달의 유효성이나 효율성을 위해 시퀀스 넘버 기반의 오류 제어 방식을 사용하여 특정 연결의 유효성을 제어한다. TCP는 신뢰성 있는 연결을 위해 다음의 기능을 제공한다.

- 패킷의 순서가 정확한지 확인
- 중간에 손실된 패킷의 유무 확인
- 손실된 패킷의 재전송 요구 확인

따라 프로토콜은 이러한 사항이 확인 되지 않으면 데이터 전송에서 신뢰도를 확보하기 위해 반복적인 재요청과 수정을 하게 된다.

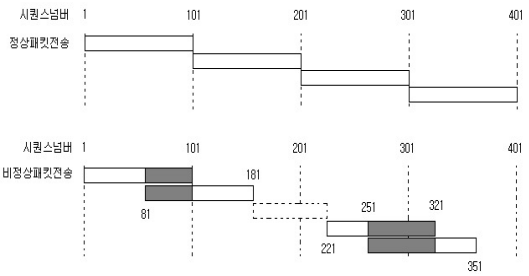

Fig. 2. TearDrop Attack

취약점 공격형의 Land공격도 있다. Land 공격은 말 그대로 시스템을 나쁜 상태에 빠지게 만드는 것이며, 그 방법은 매우 간단하다. 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소값을 똑같이 만들어 공격대상에게 보내는 것이다 물론 이때 조작된 IP 주소값은 공격 대상의 IP 주소여야 한다.

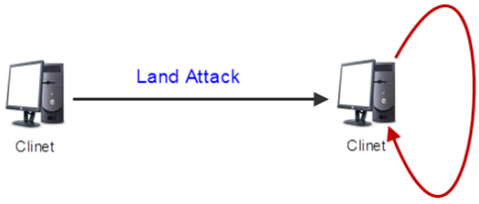

Fig. 3. Land Attack

두 번째로는 자원 고갈 공격형이다. 자원 고갈 공격형에는 Ping of Death 공격, Smurf 공격, Mail Bomb 공격 등이 있다.

첫 번째 공격에는 Ping of Death 공격은 NetBIOS 해킹과 함께 시스템 파괴를 하는 데 흔하게 쓰였던 초기의 DoS 공격방법으로, '죽음의 핑 날리기'라고도 한다. e-mail로 5MB 파일을 보낼 때, 5MB 크기의 데이터 패킷이 하나가 '퉁~'하고 가는 것이 아니고, 수만 개의 패킷으로 나뉘어 전송되는 것처럼 네트워크에서도 패킷을 전송하기 적당한 크기로 잘라서 보내는데 바로 이런 특성을 이용한 것이다.

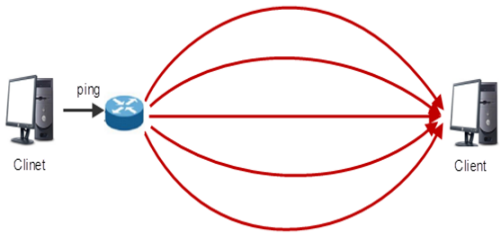

Fig. 4. Ping of Death

두 번째 공격에는 Smurf 공격 이다. 이 공격은 ICMP 패킷과 네트워크에 있는 임의적인 시스템들을 이용하여 패킷을 확장시켜 서비스 거부 공격을 수행 방법으로, 네트워크 공격할 때 많이 사용된다.

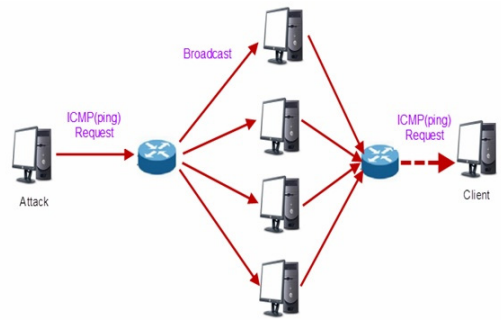

Fig. 5. Smurf Attack

세 번째는 Mail Bomb이다. 메일 봄은 흔히 폭탄 메일이라고 하는데, 스팸 메일과 같은 종류이다. 메일 서버는 각각 사용자에게 일정한 양의 디스크 공간을 할당받는데, 메일이 폭주하여 디스크 공간을 가득 매우면 정상적으로 받아야 하는 메일을 받을 수 없기 때문이다. 이런 이유로 스팸 메일은 DoS공격으로 분류된다.

2.4 DDos 공격의 종류

디도스 공격은 공격 유형에 따라서 시스템에 영향을 주는 것이 각각 틀리다.

PPS공격 유형 - IP Spoofed Syn Flooding 공격이 있다. 이 공격의 특징은 IP를 변조 한 뒤 대량의 패킷을 공격 대상의 서버로 전송하는 것이다. 공격 받은 서버는 대량의 SYN_RECEIVED 세션 상태가 발생하고 서버의 CPU 및 관련성 자원의 고갈을 발생시킨다.

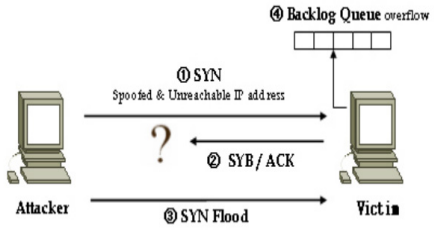

Fig. 6. SYN Flooding에 의한 DOS 공격

Fig. 6은 SYN Flooding 공격의 개념도이다. 먼저 공격자는 검색할 수 없는 호스트의 IP로 스푸핑하여 계속 SYN/ACK 패킷을 보내게 되면 공격대상은 검색할 수 없는 호스트에게 ACK를 받을 때까지 계속 큐에 저장하게 된다. 시간이 지나면 큐는 오버플로우가 일어나고, 이후에 큐로 들어오는 ACK는 거부하게 된다. [2]

PPS공격 유형으로 TCP Connection Flooding 공격이 있다. 이 공격의 특징은 IP를 변조 하지 않고 대량의 패킷을 공격 대상 서버로 전송한다. 공격받은 서버는 대량의 ESTABLISHED 세션 상태가 일어나고 서버의 CPU 및 관련성 자원의 고갈을 발생시킨다. 마지막으로 PPS 공격 유형인 TCP Out-of-State Packet Flooding 공격이 있다. 공격의 특징은 대량의 ACK/SYN+ACK/FIN/RST 등의 패킷을 공격 대상 서버로 전송하는 것이다. 방화벽이나 L4등과 같이 세션을 관리하는 보안장비에서 차단한다. 일부 네트워크 장비 와 서버의 CPU 사용량을 올리게 하는 오작동을 일으킨다.

두 번째로 웹 서비스 지연 공격 유형 - 동일한 URL로 반복적인 접속 시도(웹서버의 부하 발생)이 있다. 이 공격의 특징은 IP를 변조하지 않고 정상적인 3 way handshake 후에 동일한 URL를 반복 요청한다. 번째 공격 유형으로 대용량 트래픽 전송이다.

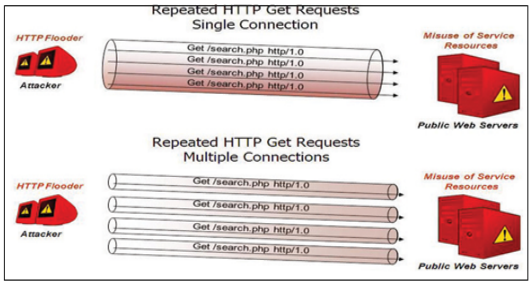

Fig. 7. Same URL Repeat Request Attack

대용량 트래픽 전송 공격 유형에는 UDP/ICMP Flooding 공격이 있다. 이 공격의 특징은 큰 패킷을 공격 대상 서버로 전송한다. 네트워크 회선 대역폭을 고갈시키고 공격 대상 서버와 같은 네트워크에 운영 중인 모든 서버의 접속을 장애를 일으킨다. 기타 공격 유형에는 특정 패턴을 가진 DOS공격이나 네트워크 장비, 서버, PC 등의 취약점을 이용해 하는 DOS 공격이 있다.[5]

2.5 DDoS공격 피해 사례

2.5.1 7.7 디도스

2009년 7월 7일 오후 7시부터 7월 9일까지 청와대와 국내 포털 및 중요한 주요사이트 24개의 대상으로 DDoS 공격이 있었으며, 공격의 목적은 분명하지가 않았다. 7.7 디도스 공격은 공격이 끝나고 감염된 좀비 PC의 하드디스크를 파괴한 후에 공격을 끝냈으며, 이 DDoS 공격을 하기위해 감염시킨 좀비 PC는 무려 11만대가 넘어섰다.

2.5.2 3.4 디도스

2011년 3월 3일 오후 5시부터 3월 4일까지 청와대와 국내 사이트 40개의 대상으로 DDoS 공격이 있었으며, 모든 Windows 운영체제의 부트섹터들을 파괴시켰다. 또한 이 DDoS 공격은 host파일의 변조를 통해서 백신프로그램 업데이트 및 홈페이지의 접근을 방해하는 방식이었고, 이 DDos 공격을 위해서 감염되었던 좀비PC는 약 7만 가량 대 이상이었다.

2.5.3 6. 25 디도스

2013년 6월 25일 오전 9시 30분 청와대와 비롯하여 정부의 주요기관 및 10개의 언론사의 대상으로 디도스 공격과 악성코드를 이용하는 해킹이 있었으며, 시스템의 중요한 파일들을 유출한 뒤 소멸하고 하드디스크의 부트섹터를 삭제시켰다. 이번 디도스 공격에는 악성코드 감염을 한 후의 행적을 포렌식으로 통해서 추적하지 못하게 치밀하게 준비되었다. 6. 25 디도스 공격은 청와대의 관련 인물 9만 명, 정치원 11만 명, 미군 보병사단 장병 650명, 미군 해병사단 장병 2900명의 신상정보를 유출하는 큰 규모의 공격이었다.[4]

3. DDoS공격 대응방법

3.1 라우터에 의한 차단

대규모 데이터를 보내는 공격을 대응하기 위해선 네트워크의 접근 통제가 필요하다. 모든 공격 주소로부터 모든 패킷을 차단해야만 한다. 그 디도스 공격의 특성 공격자 주소는 하나도 아닌 수십 수천 수백 개가 될수 있기 때문이다. 위장된 주소일 수도 있고 공격이 시작한 후에 네트워크 이상이 생기기까지가 시간이 단시간으로 걸리기 때문에 주소 단위로 차단하는 건 쉽지 않다. [6]

3.2 관리적 측면 대응 방법

DDoS 공격 예방과 신속한 조치를 위해 보안업체와 DDoS 대응 방안에 대한 사전 협의가 필요하며, 그 후 조직간의 협조를 위해 DDoS 대응을 위한 사전대비팀을 구성하고 팀조직 구성원의 권한과 책임을 명확히 하여서 DDoS 공격 발생 시에 신속하게 대응할 수 있도록 하여야 한다. 평시에는 유관기관(국가사이버안전센터, KISA 등)과 최신 동향 과 기술 관련 정보를 공유하고 PC나 서버의 보안관리자는 DDoS 공격패턴에 대한 최신 동향을 수시로 분석하고, 위험도가 높은 공격인 경우 모든 팀 및 기관에 전파한다. 그 후 PC가 감염되지 않게 정기적으로 정보보호교육을 실시하고 안티바이러스 소프트웨어를 철저히 업데이트 하며 관리하여야한다.

3.3 기술적 측면 대응 방법

네트워크 통신장비에 ACL(Access Control List)을 적용하여서 DoS 공격일 가능성이 큰 패킷을 전 또는 후에 차단함으로 다음 DDoS 공격에 대응할 수 있다. 패킷의 출발지 IP 주소가 정상이 아닌 주소인 경우, 이를 먼저 차단해야한다. 출발지 주소가 사설 IP주소인 경우 거의 스푸핑 패킷이므로 모두 차단해야 하며, 사설 IP 주소에 대한 Louting이 필요한 경우에는 사용하는 IP주소만 허용하고 그 이외의 IP주소는 모두 차단하여야 한다. 네트

워크에 들어오는 패킷이 일반적인 UDP나 ICMP의 패킷이 보다 클 경우 이를 전에 차단함하여야 대역폭 고갈 공격에서 대응할 수 있다. 예를 들어서 UDP 패킷의 크기가 2메가 이상이면 Drop을 명령을 하고, ICMP 패킷 크기가 256킬로 이상이면은 Drop을 명령 한다. 또 IDS 나 IPS 등의 보안 네트워크 장비 설정을 하고, 실시간 탐지 시스템의 이벤트를 지속적인 모니터링을 하며, DDoS의 관련 패턴들을 분석하여 상시로 업데이트 해여야 한다. 방화벽을 통하여서 DDoS 공격에 대해 대응할 수 있어야하며, 대역폭 공격에 대응하기 위해서는 불필요한 프로토콜에 대해 차단하는 정책을 적용하는 것을 선호한다.[3]

3.4 좀비PC 예방법

안랩에서 좀비 PC예방법 10계명을 발표했다.

우리나라 대표적인 백신회사에서 발표한 것이니 이 10계명을 지켜서 예방했으면 좋겠다.

1. 윈도우 운영체제와 웹브라우저 등 최신으로 보안패치를 모두 적용하는 것
2. 믿을 수 없는 사이트, 신용이 가지 않는 사이트들을 접속을 자제한다.
3. 웹하드, P2P 등 파일 공유 프로드램들을 이용할 때에는 꼭 백신으로 검사한 뒤 이용한다.
4. 스팸메일은 절대 보지 않는다.
5. SNS에서 알 수 없는 인터넷링크들은 접속하지 않는다.
6. 비밀번호은 특수문자를 조합하여 8자리 이상으로 설정하고 달 주기로 바꾼다.
7. 메신저에서 파일을 받을 때에는 보내는 사람을 꼭 확인하고 받는다.
8. 신뢰가 없는 프로그램들은 절대 설치하지 않는다.
9. 정품 소프트웨어를 사용한다.
10. 백신 프로그램들은 항상 최신버전으로 업데이트 해준다.[7]

4. 결론

DDoS 공격은 경제적인 이유로 DDoS 공격 횟수가 증가하면서 번번이 일어났지만, 최근에는 정치적이나 국가대 국가의 목적으로 공격하는 경우가 증가했다. BotNet 등과 같이 DDoS 공격을 위한 프로그램(Tool)이 확산되어가면서 해커집단과 일반인도 공격을 할 수 있어서 언제 어디서 어떻게 일어날지 예측하기 어렵기 때문에 DDoS 공격은 대응하기가 힘든 공격이기도 한다. DDoS 공격은 확실하게 대응할 수 는 없다. 그러나 평소에 DDoS 공격에 대해서 예방을 수시적으로 하고 각 시스템에 적합한 피해복구방법과 유지보수관리가 필요하다.

REFERENCES

[1] P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[2] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[3] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, IEEE INFOCOM'06, 2006.

[4] R. K. C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial, Computer J. IEEE Commun. Magazine, Vol. 40, no. 10, pp. 42-51, 2002.

[5] R. Puri, Bots and Botnet - an overview, Aug. 08, 2003, [online] http://www.giac.org/practical/GSEC/Ramneek Puri GSEC.eps

[6] B. Todd, Distributed Denial of Service Attacks, Feb. 18, 2000, [online] http://www.linuxsecurity.com/resource files/intrusion detection/ddos - whitepaper.html

[7] CERT, Denial of Service Attacks, June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html

저 자 소 개

신 미 예(Miyea Shin) [정회원]

- 1990년 8월 한밭대학교 전자계산학과 (공학학사)
- 1998년 8월 충북대학교 전자계산학과 (이학석사)
- 2010년 2월 충북대학교 전자계산학과 (이학박사)

- E-Mail : myshiny@chungbuk.ac.kr

<관심분야> : 정보보호, 네트워크보안, 자동차보안