KISA 한국인터넷진흥원

DDoS 공격 대응 가이드

중소기업 대상

KISA KOREA INTERNET & SECURITY AGENCY

KISA 한국인터넷진흥원

DDoS 공격 대응 가이드 중소기업 대상

본 문서는 **사이버대피소에서 작성한 중소기업을 위한 가이드**입니다.
이 가이드는 **DDoS(Distributed Denial of Service) 공격에 대한 대응 방안**을 안내합니다.

CONTENTS

PART 1
개요

DoS(Denial of Service) 공격은 정상적으로 네트워크 및 시스템을 사용할 수 없게 만드는 시도이다.
(예: 인터넷 쇼핑몰 웹사이트 서비스 이용 불가)
DoS공격으로 인해 사용 가능한 네트워크 및 시스템 리소스 속도가 느려지거나 서버가 손상 될 수 있다.
DoS 공격이 불특정 다수에 의해 동시 다발적으로 발생하면 DDoS(Distributed Denial of Service) 공격이라고 한다.

일반적인 DDoS 공격은 공격자가 공격 대상 서버 및 네트워크에 직접 많은 양의 악의적인 트래픽을 전송할 때 발생한다. 공격자가 할 수 있는 공격 방법 중 하나는 봇넷을 이용하여 트래픽을 전송하는 것이다. 봇넷은 공격 도구로 이용하기 위한 악성코드에 감염된 수 많은 좀비(숙주)시스템이며 인터넷을 통해 연결되어 서로 통신하고 제어할 수 있다. [그림 1-1]에서 알 수 있듯이 공격자가 봇넷을 사용하여 DDoS를 수행하면 봇넷에 연결된 좀비들 중 일부 또는 전부가 공격을 수행하게 된다. 따라서 DDoS는 피해자 리소스에 과부하를 유도하게끔 규모를 확대하게 되어 여러 네트워크에서 발생하게 되고 가능한 여러 국가에서 발생 하는 것이다.

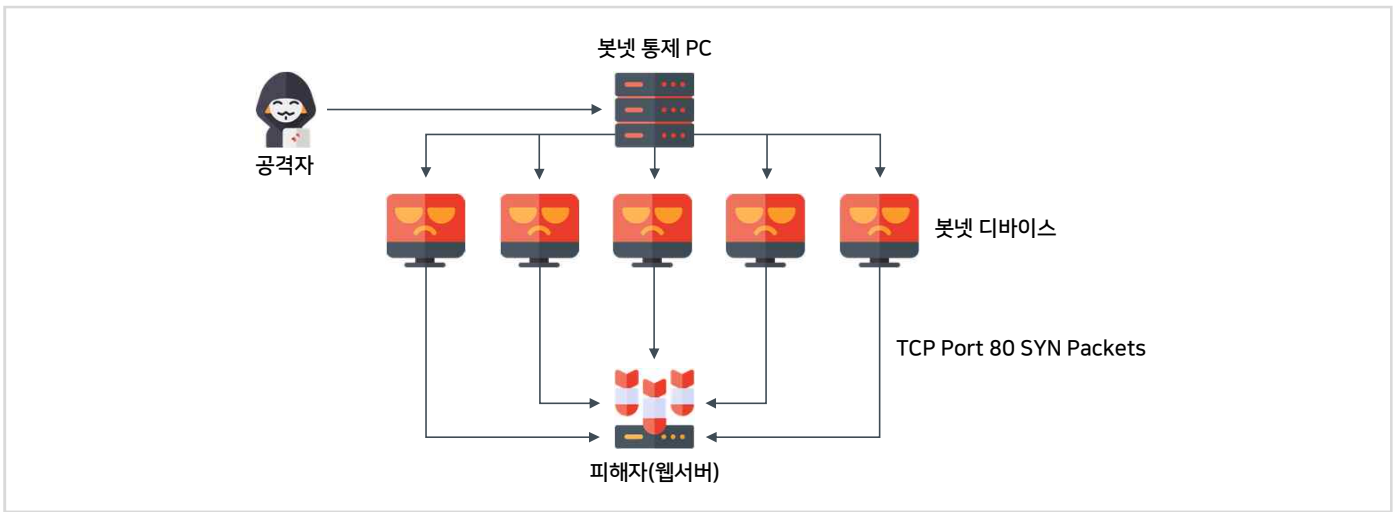

그림 1-1 일반적인 DDoS SYN Flood

반사 DDoS 공격은 공격자가 IP 주소를 도용할 때 발생한다. 정상적인 서버에 서비스 요청을 보낼 때 공격자가 자신의 IP 주소가 아닌 공격 대상 시스템의 IP 주소를 도용하여 서비스를 요청하면 정상적인 웹서버 측에서는 요청 받은 서비스에 대한 응답을 도용된 IP 주소(피해자)로 보내게 된다.
또한, 공격 효율성을 높이기 위해 피해자에게 전송되는 응답이 해당 요청보다 큰 증폭 기술이 일반적으로 함께 사용된다.

[**그림 1-2**] 에서 알 수 있듯이 공격자가 IP 주소를 도용하여 피해자인 것 처럼 가장하고 악의적인 서비스 요청을 공개 DNS 서버에 요청한다. 공격자는 크기가 작은 요청을 전송하지만 피해자는 증폭기술에 의한 많은 양의 데이터를 공개 DNS서버로 부터 받게 된다.

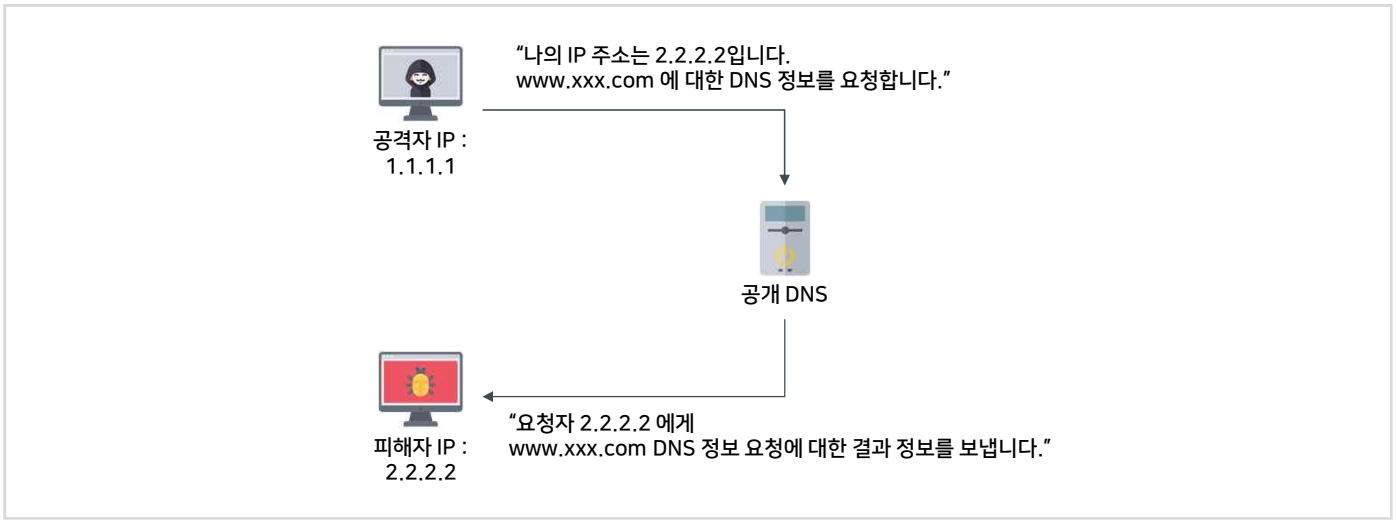

그림 1-2 DNS 반사 및 증폭 공격 예제

공격자는 인터넷상에 자유롭게 무료 및 유료인 다양한 DDoS 공격도구를 쉽게 구할 수 있으며 [그림 1-3]처럼 오픈소스 도구로 제작된 LOIC(Low Orbit Ion Cannon) 및 HOIC(High Orbit Ion Cannon) 공격 도구 등이 일반적인 예제이다.

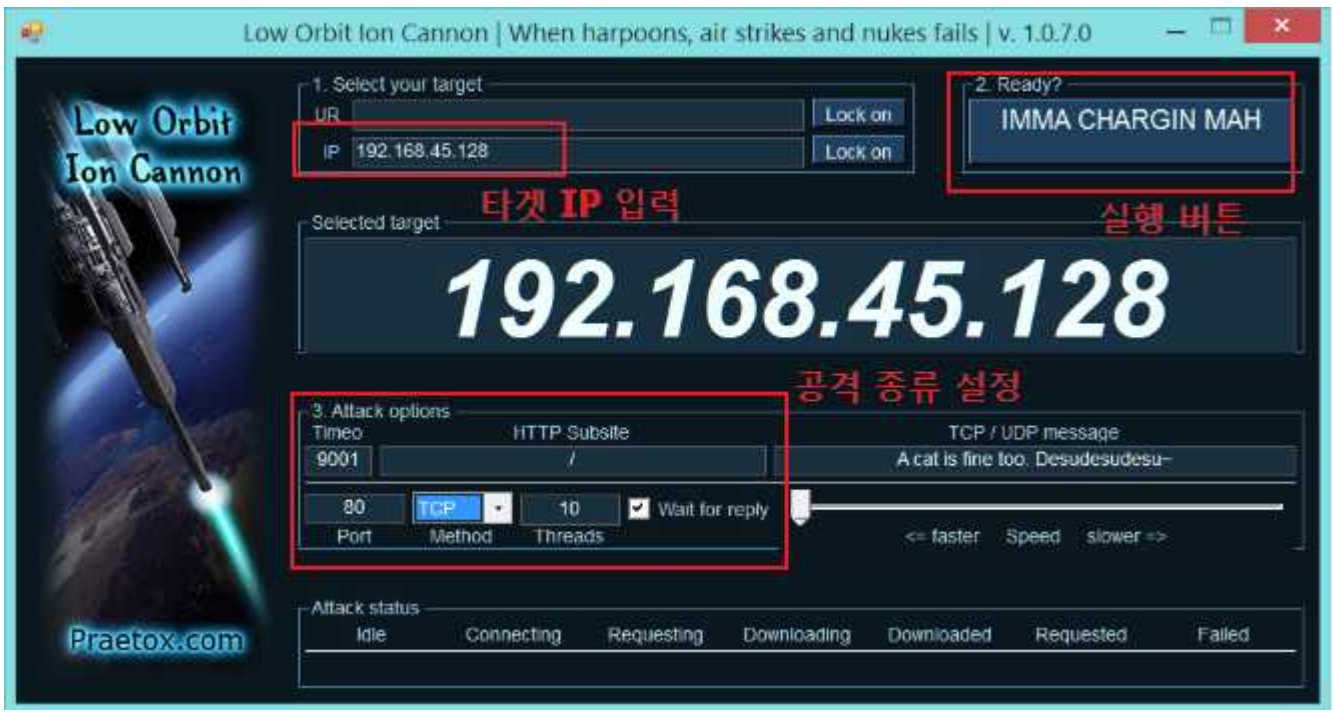

그림 1-3 LOIC GUI 화면

PART 2

일반적인 DDoS 공격형태

- SYN Flood

SYN Flood는 DDoS 공격 형태 중 가장 많이 사용되는 오래된 공격 형태 중 하나이다. 이 형태는 정상적인 사용자가 서버를 사용할 수 없도록 서버의 리소스를 소비하기 위해, 공격자가 피해자 시스템에 TCP(SYN) 연결 요청을 연속해서 전송 할 때 발생한다. 공격방식은 서버가 SYN 연결 요청을 받으면, 클라이언트가 연결을 확인하기 위해 보내는 응답신호(ACK)를 기다리는 위해 통신을 열린 상태로 유지하지만, SYN Flood는 응답 신호를 보내지 않으므로 설정된 연결 시간이 초과 될 때까지 서버의 리소스를 소비한다. 따라서 피해자 서버가 정상적인 사용자에 대한 연결이 불가능한 서비스 장애가 발생한다.

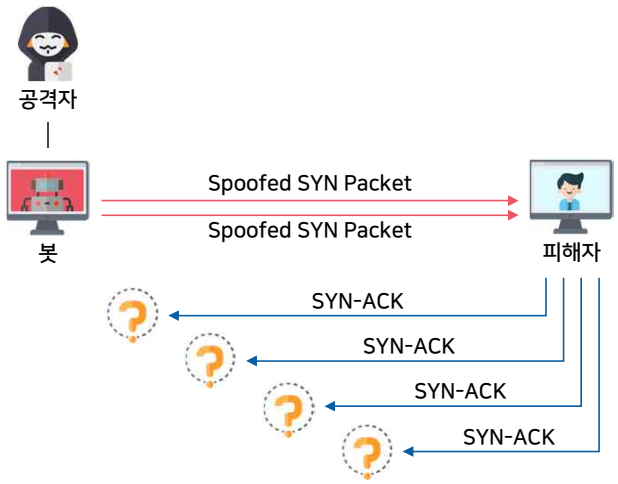

그림 2-1 일반적인 SYN Flood

대응방안

- SYN Flood 를 확인하려면 네트워크 로그를 조사하고 TCP SYN flag 를 찾는다.
  - TCPdump 또는 Wireshark 등의 패킷 분석 Tool 이용 할 수 있다.
- TCP SYN 패킷은 정상적인 것이며 악의적인 활동을 나타내는 것은 아니다. 그러나 짧은 기간동안 많은 수의 SYN 패킷이 발생할 경우에는 DDoS 공격으로 볼 수 있다.
- 공격이 확인된 경우 네트워크 서비스 공급자(ISP, IDC 등)가 서버에 전달 되기 전에 공격을 완화할 수 있도록 네트워크 서비스 공급자에게 요청 한다.
- SYN Flood 공격의 피해를 최소화하려면 방화벽 및 프록시 서버와 같은 모든 주변 장치에서 "TCP 연결 유지" 및 "최대 연결" 규칙을 정의 한다.
- 방화벽 장비의 "SYN 쿠키" 기능을 사용하여 SYN Flood 의 영향을 완화 할 수 있다. SYN 쿠키를 사용하면 트래픽이 서버에 전달되기 전에 방화벽이 클라이언트와 서버 간의 TCP 연결을 확인 한다.
  공격자가 연결에 대한 최종 승인을 보내지 않으면 방화벽은 연결을 끊는다.

PART 2

일반적인 DDoS 공격형태

- UDP Flood

UDP Flood는 SYN Flood 와 매우 유사하다. 공격자가 봇넷을 사용하여 공격 대상 서버로 상당히 크고 많은 양의 트래픽을 전송한다. TCP Flood 와의 차이점은 상대적으로 훨씬 빠르며 서버 리소스를 소모하지 않고, 서버의 네트워크 환경에서 사용 가능한 모든 대역폭을 소비하여 정상적인 사용자에 대한 접근을 막는다. 이 공격은 네트워크 포트 중 UDP 패킷(예: 50555 포트)을 수신하는 서버가 해당 포트를 오픈하고 수신 대기하는 응용 프로그램이 작동하기 때문이다. 만약 해당 포트에서 수신 대기중인 것이 없으면 ICMP Destination Unreachable 패킷을 사용하여 UDP 패킷을 보낸 요청자에게 회신한다.

공격하는 동안 크고 많은 수의 UDP 패킷이 전송되며 대부분의 서버에서 응답하기에 빠르게 모든 사용 가능한 공격 대상 대역폭을 잠식한다.

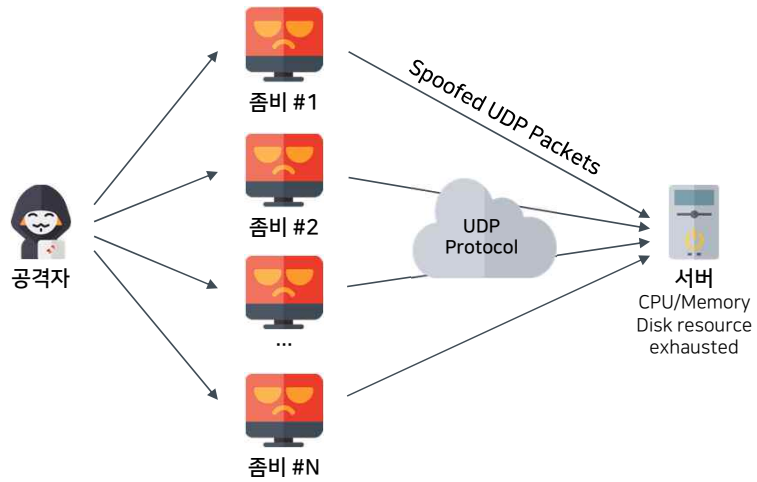

그림 2-2 일반적인 UDP Flood

대응방안

- UDP Flood 를 확인하기 위해 네트워크 로그를 조사하고 많은 수의 원본 IP 주소에서 오는 불규칙한 네트워크 포트의 통신 요청을 통해 공격 UDP 패킷을 찾는다.
  - 인터넷의 많은 정상적인 서비스가 UDP 를 사용하며 일반적인 UDP 포트는 53(DNS), 88(Kerberos), 137/138/445(Windows) 및 161(SNMP)이다.
- 공격이 확인된 경우 네트워크 서비스 공급자(ISP, IDC 등)가 서버에 전달되기 전에 공격을 완화할 수 있도록 네트워크 서비스 공급자에게 요청 한다.
- UDP Flood 공격의 피해를 최소화하려면 방화벽과 같은 주변 네트워크 장치에 대한 보안 규칙을 정의하여 필요한 포트에서만 인바운드 트래픽을 허용한다.

PART 2

일반적인 DDoS 공격형태

- ICMP Flood

ICMP Flood는 공격자가 봇넷을 사용하여 사용 가능한 모든 대역폭을 소비하고 정상적인 사용자의 접근을 막기 위해 많은 수의 ICMP 패킷을 공격 대상 서버로 전송하는 형태이다.

이 공격은 대량의 ICMP 트래픽을 공격 대상 네트워크의 사용 가능한 모든 대역폭을 잠식할 수 있는 충분한 ICMP 요청 및 응답 트래픽 발생이 가능해야 한다.

이 공격의 예로 "ping" 명령으로 주로 네트워크 두 지점 간 연결을 테스트하는데 사용된다. 그러나 명령과 매개변수를 이용하여 ping의 크기와 요청 주기를 조정할 수 있어 처리 가능한 공격 대상 네트워크 대역폭을 모두 소진 시킬 수 있다.

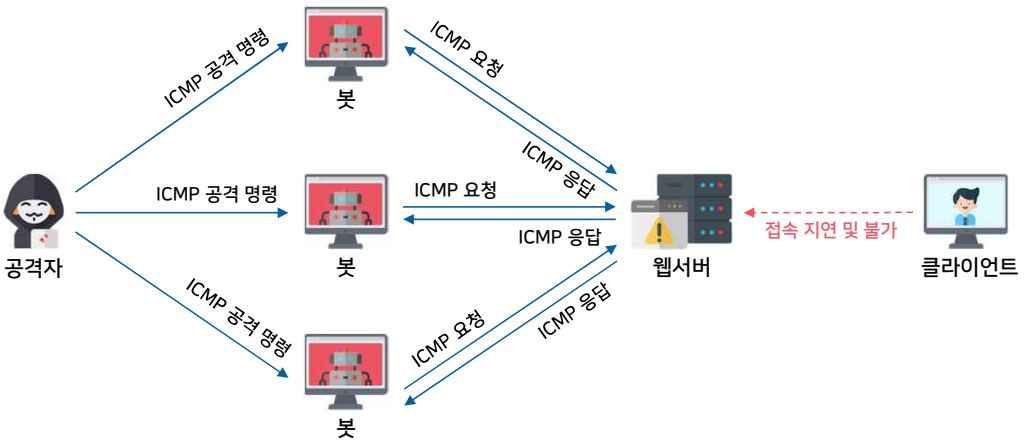

그림 2-3 일반적인 ICMP Flood

대응방안

- ICMP Flood 를 확인하기 위해 많은 사용자로부터 요청되는 인바운드 ICMP 트래픽을 네트워크 로그에서 조사한다.
  - 로그를 조사하는데 사용하는 도구에 따라 ICMP 를 확인할 수 있다.(예: Wireshark)
    ICMP 는 TCP 및 UDP 와 같은 네트워크 포트를 사용하지 않는다.
  - 네트워크 프로토콜을 번호 값으로 표하는 도구를 사용하는 경우 ICMP 프로토콜은 숫자 "1" 로 구분한다.
- 공격이 확인된 경우 네트워크 서비스 공급자(ISP, IDC 등)가 서버에 전달되기 전에 공격을 완화할 수 있도록 네트워크 서비스 공급자에게 요청 한다.
- ICMP Flood 공격의 피해를 최소화하려면 라우터와 같은 네트워크 경계 장치에 ICMP 트래픽의 임계치를 설정한다. 또한 주변 라우터에서 ICMP 요청에 대한 초당 패킷 허용 임계 값을 설정한다. 인바운드 ICMP 트래픽 양이 임계 값을 초과하면 초과 트래픽은 일정 시간까지 무시된다. 초당 패킷 수 임계 값은 ICMP 트래픽으로 네트워크가 오버런 되는 것을 효과적으로 방지한다.

PART 2

일반적인 DDoS 공격형태

- HTTP Flood

HTTP Flood는 공격자가 공격 대상 웹사이트에 대한 지속적인 많은 양의 HTTP GET 요청을 통해 웹서버의 리소스를 소진하게 하여 정상적인 사용자가 이용할 수 없도록 한다.

이 경우 공격자 요청에 대해 웹서버가 응답을 시도하지만 공격자는 응답을 처리하지 않고 대기 시킨다. 그 결과 웹서버는 응답 확인을 위하여 일정 시간동안 각 연결에 대한 고정된 리소스를 배정하여 연결 대기를 유지한다. 공격자는 웹서버에 많은 HTTP GET 요청을 하고 응답을 회신하지 않아서, 공격을 받은 웹서버는 모든 통신 리소스를 소모하여 정상 사용자의 웹사이트 서비스가 불가능 하게 된다.

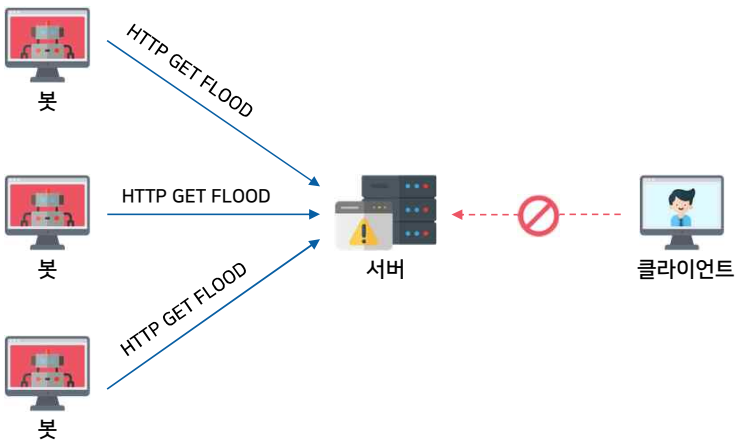

그림 2-4 일반적인 HTTP Flood

대응방안

- HTTP GET Flood 를 확인하기 위해 대상 포트가 80이고 TCP 프로토콜을 사용하는 대량의 요청을 네트워크 로그에서 조사한다.
  로그를 조사하는데 사용하는 도구는 TCPdump 및 Wireshark 를 추천한다.
- 공격이 확인된 경우 DDoS 방어 서비스를 제공하는 전문업체를 이용한다.
- 정상적인 웹서비스 요청수단이 이용되기 때문에 이 공격을 차단하기 위한 사전 예방대책을 세우기 어렵다. 공격의 출발지 IP 주소는 대규모 봇넷의 일부분이므로 모든 출발지 IP 주소를 차단하는 것은 효율적이지 않으며 정상 사용자가 포함될 수 있다.
  - 웹방화벽(WAF)을 사용하여 공격에 대한 피해를 최소화할 수 있다.

PART 3

반사 DDoS 공격 형태

- SYN+ACK 반사 공격

SYN+ACK Flood는 DRDoS의 형태를 지닌 공격방식으로서, 공격자가 피해자의 IP를 도용한 후 반사체로 악용될 서버에 SYN 패킷을 보내고 해당 응답인 SYN/ACK 패킷을 피해자에게 전송하게 하는 공격이다.
피해자는 SYN/ACK패킷을 대량으로 전송 받게 되면 해당 패킷을 처리하기 위해 리소스를 소모하게 되고, 그 과정에서 서버의 부하가 발생되어 정상 사용자들이 접속할 수 없게 된다. DRDoS의 형태를 보이기 때문에 반사체 서버들은 상대방(피해자)이 응답을 주지 않으면 패킷이 정상적으로 전달되지 못한 것으로 판단하여 재 전송하기 때문에 공격의 효과가 더 커지게 된다.

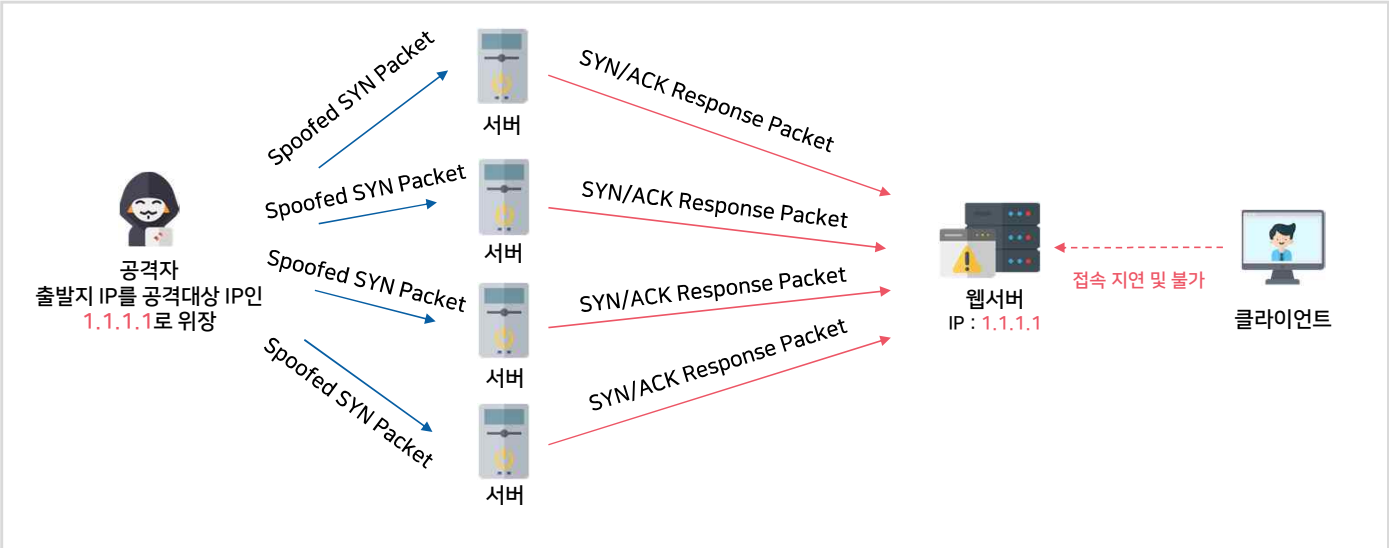

그림 3-1 SYN+ACK 반사 공격

대응방안

- SYN/ACK Flood 를 확인하려면 네트워크 로그를 조사하고 TCP ACK flag 를 찾는다.
  - TCPdump 또는 Wireshark 등의 패킷 분석 Tool 이용 할 수 있다.
- TCP SYN/ACK 패킷은 3 way handshaking 과정에서 수신 받는 패킷으로서 그 자체로선 정상 패킷이지만 짧은 시간안에 급격하게 증가한다면 DDoS공격으로 의심할 수 있다.
- 공격이 확인된 경우 네트워크 서비스 공급자(ISP, IDC 등)가 서버에 전달 되기 전에 공격을 완화할 수 있도록 네트워크 서비스 공급자에게 요청 한다.
- SYN/ACK Flood 공격의 피해를 최소화하려면 방화벽 및 프록시 서버와 같은 모든 주변 장치에서 목적지 IP 기반 SYN/ACK 패킷 임계치를 설정하여 차단 한다.

PART 3

반사 DDoS 공격 형태

- NTP 반사 및 증폭 공격

NTP(Network Time Protocol) 반사 공격은 공격자가 정상적인 NTP 서버의 트래픽을 사용하여 공격하는 형태이다. NTP는 네트워크로 연결된 컴퓨터의 시간을 동기화하는데 사용되며 UDP 123 포트를 통해 실행 된다. 공격자는 공격 대상의 IP 주소로 도용하고 NTP 서버가 많은 양의 응답 트래픽(고정된 패킷 크기)을 공격 대상 서버에게 보내도록 요청한다.

NTP 서버의 응답이 공격자가 보낸 요청보다 크기가 큰 증폭기술이 활용되어 공격 효율성을 크게 높일 수 있다.

공격자는 다수의 인터넷에 공개된 NTP 서버에 monlist 요청을 하면 서버는 monlist 요청에 대한 응답을 일제히 공격 대상으로 전송하고 공격 대상은 네트워크 대역폭을 모두 소진하여 정상적인 사용자에 대한 서비스 장애가 발생한다.

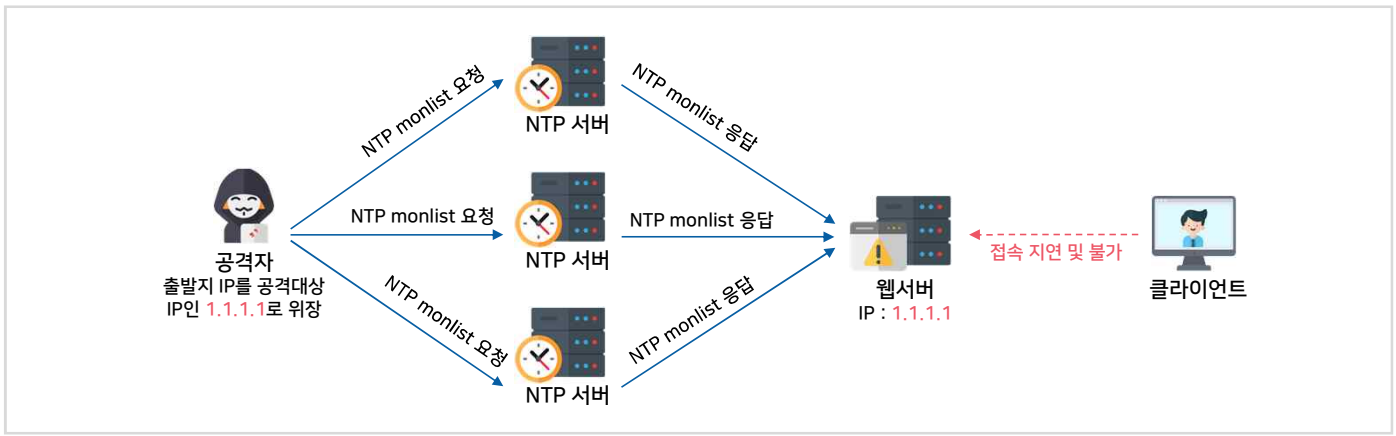

그림 3-2 NTP 반사 공격

대응방안

- NTP 반사 및 증폭 공격을 확인하기 위해 출발지 중 UDP 123 포트와 특정 패킷 크기를 가진 트래픽을 네트워크 로그에서 조사한다.
- 공격이 확인된 경우 공격에 사용된 정보(IP주소, 패킷 크기 등)를 네트워크 서비스 공급자(ISP, IDC 등)에게 제공하여 필터링 조치를 요청한다.
- 인바운드 공격에 대한 해결과 함께 NTP 서버가 다른 사용자를 공격하는데 사용되지 않도록 다음과 같은 예방 조치를 취한다.
  - NTP 서버를 2.4.7 이상으로 업그레이드하여 monlist 명령을 완전히 제거하거나 OpenNTPD와 같이 monlist 명령을 활용하지 않는 NTP 버전을 이용한다.
  - 서버를 업그레이드 할 수 없는 경우 ntp.conf 파일에 “disable monitor”을 추가하고 NTP 프로세스를 재시작하여 monlist 쿼리 기능을 비활성화 한다.
  - NTP 서버에 대한 무단 트래픽을 제한하는 방화벽 규칙을 적용한다.

PART 3

반사 DDoS 공격 형태

- DNS 반사 및 증폭 공격

DNS(Domain Name System) 반사 공격은 공격자가 DNS 시스템을 악용하여 많은 양의 트래픽을 전송하는 형태의 공격이다. DNS 시스템은 일반 인터넷 사용자가 입력한 문자 기반의 도메인 주소를 IP 주소로 변환해 주는 역할을 한다. DNS 반사 공격은 공격자가 피해자의 IP 주소로 도용하여 DNS 조회 요청을 공용 DNS 서버에 보내는 절차를 이용한다. 공용 DNS 서버는 요청에 대한 응답을 피해자에게 보내며 이때 응답 크기는 공격자가 DNS 조회 요청에 지정한 옵션에 따라 달라진다. 최대 증폭을 얻기 위해, 공격자는 요청에 "ANY" 라는 옵션을 사용할 수 있으며, 이것은 DNS 영역에 대한 모든 정보를 반환한다. 공격자가 피해자 IP 주소로 도용하여 다수의 공용 DNS 서버에 DNS 조회 요청을 전송하면 증폭된 응답은 공격 대상에게 전송되어 결국 사용 가능한 피해자 대역폭을 모두 소진하게 된다.

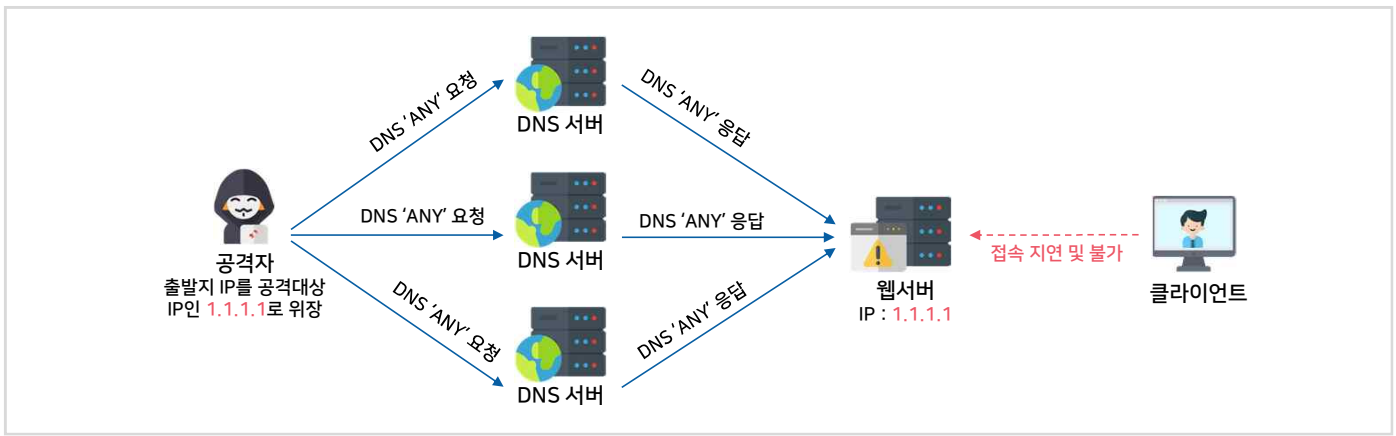

그림 3-3 DNS 반사 공격

대응방안

- DNS 반사 및 증폭 공격을 확인하기 위해 DNS 쿼리 요청이 없는 인바운드 DNS 쿼리 응답을 네트워크 로그에서 조사한다.
- 공격이 확인된 경우 네트워크 서비스 공급자(ISP, IDC 등)에게 문의하여 공격 패킷이 서버에 전달 되기 전에 필터링 될 수 있도록 요청한다.
- DNS 서비스에서는 DNS 개발사(BIND, Microsoft 등)에서 제공한 지침에 따라 DNS 재귀 기능을 사용하지 않도록 한다.
  - 공용 DNS 서버가 공격에 악용될 수 있는지 확인 및 테스트 하는 사이트
    URL: openresolverproject.org

PART 3

반사 DDoS 공격 형태

- CLDAP 반사 및 증폭 공격

CLDAP(Connection-less Lightweight Directory Access Protocol) 반사 공격은 공격자가 공격대상 IP 주소로 도용하고 LDAP 서버로 CLDAP 요청을 보내는 형태의 공격이다. CLDAP은 공유 인터넷 디렉토리를 연결/검색/수정하는데 사용되며 UDP 389 포트를 사용한다.

공격자가 도용된 IP 주소로 CLDAP 쿼리를 여러 LDAP 서버로 전송할 때 CLDAP 반사 공격이 발생하며 LDAP 서버는 요청에 대한 응답 데이터를 도용된 피해자 IP 주소로 보낸다. 피해자는 대량의 LDAP/CLDAP 데이터를 동시에 처리 할 수 없기 때문에 정상적인 서비스가 불가능 하다.

UDP LDAP 프로토콜은 52배에서 70배까지 증폭이 가능한 증폭기술을 사용하여 공격 효율성을 높인다.

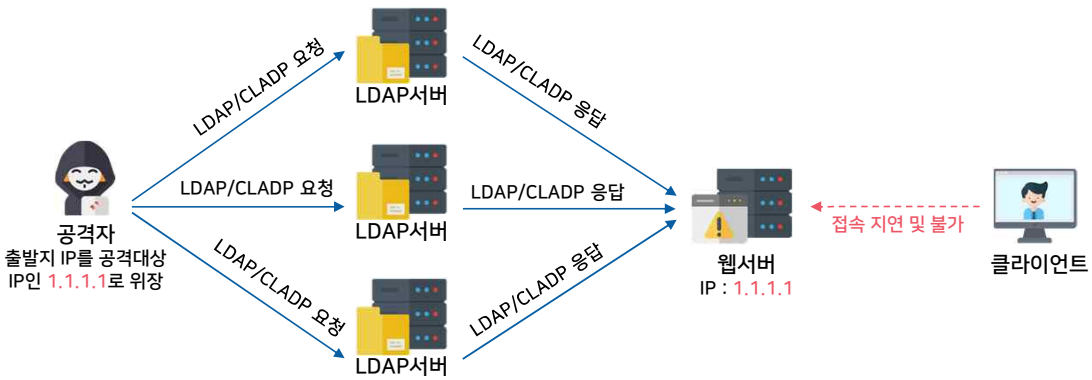

그림 3-4 CLDAP 반사 공격

대응방안

- 출발지에서 UDP 389 포트를 사용하는 요청을 네트워크 로그에서 조사한다.
- 공격이 확인된 경우 네트워크 서비스 공급자(ISP, IDC 등)에게 문의하여 공격 패킷이 서버에 전달 되기 전에 필터링 될 수 있도록 요청한다.
- LDAP 서버를 운영하는 경우 방화벽 규칙을 설정하여, 공격에 악용되지 않도록 예방 조치한다.

PART 4

DDoS 공격 피해 감소 전략

DDoS 공격이 시도되고 발생할 때 빠른 대응을 가능하게 하여 피해를 최소화 한다.

1. 네트워크 서비스 제공 업체에서 제공하는 DDoS 방어 서비스를 알고 있어야 한다. DDoS 공격의 경우, 네트워크 서비스 제공 업체에서 조치하는 것이 대응이 빠르다.
2. DDoS 공격에 대한 방어서비스를 계약하는 것을 고려한다.
3. DDoS 공격이 발생하면 네트워크 서비스 제공 업체에 공격 IP 주소를 제공한다.
4. 허용된 트래픽과 거부된 트래픽에 대한 방화벽 로그를 확인하여 DDoS 공격 발생 위치를 확인한다.
5. 방화벽 및 프록시 서버와 같은 주변 장치에서 "TCP keepalive" 및 "최대 연결"을 설정하여 SYN Flood 공격을 예방한다.
6. 네트워크 서비스 제공 업체에서 포트 및 패킷 크기 필터링이 가능한지 확인하여 설정 한다.
7. 공개 웹사이트의 기본 트래픽 패턴(볼륨 및 유형)을 파악하고, 이상 패턴이 발생하는지 정기적으로 확인 한다.
8. 네트워크/보안 장비의 패치는 적절한 테스트 및 검증을 거친 후 적용한다.
9. 예약된 IP 주소(0/8), 루프백(127/8), 사설(RFC 1918 블록 10/8, 172.16/12 및 192.168/16), 할당되지 않은 DHCP 클라이언트(169.254.0/16), 멀티캐스트(224.0.0/4) 및 RFC 5735 에 나열된 다른 주소에서 출발되는 인바운드 트래픽을 차단하도록 방화벽을 구성한다. 이 구성은 네트워크 서비스 제공 업체에도 요청되어야 한다.
10. 비즈니스 목적에 필요한 프로세스와 네트워크 대역폭을 파악하고, 서버에 설정을 반영한다.
11. 비즈니스 목적과 보안 정책을 고려하여 방화벽 설정을 한다.
12. 이상 징후 발생 시 즉시 인지할 수 있도록 방화벽 및 침입 탐지 서비스를 구성한다.
13. DDoS 공격으로 네트워크 서비스 장애가 발생할 것을 대비하여, 대체 연결 수단을 준비한다.
14. 중소기업 대상으로 DDoS 공격 대응 서비스를 무료로 제공하고 있는 [DDoS 사이버대피소] 이용을 고려한다. ※이용문의: 02-405-4769 http://www.boho.or.kr "보안서비스 > 사이버대피소"

KISA KOREA INTERNET & SECURITY AGENCY