DDoS 공격
대응 가이드

과학기술정보통신부

KISA 한국인터넷진흥원

CONTENTS

본 문서는 한국인터넷진흥원에서 작성한 가이드입니다.
이 가이드는 DDoS(Distributed Denial of Service) 공격에 대한 대응 방안을 안내합니다.

CONTENTS

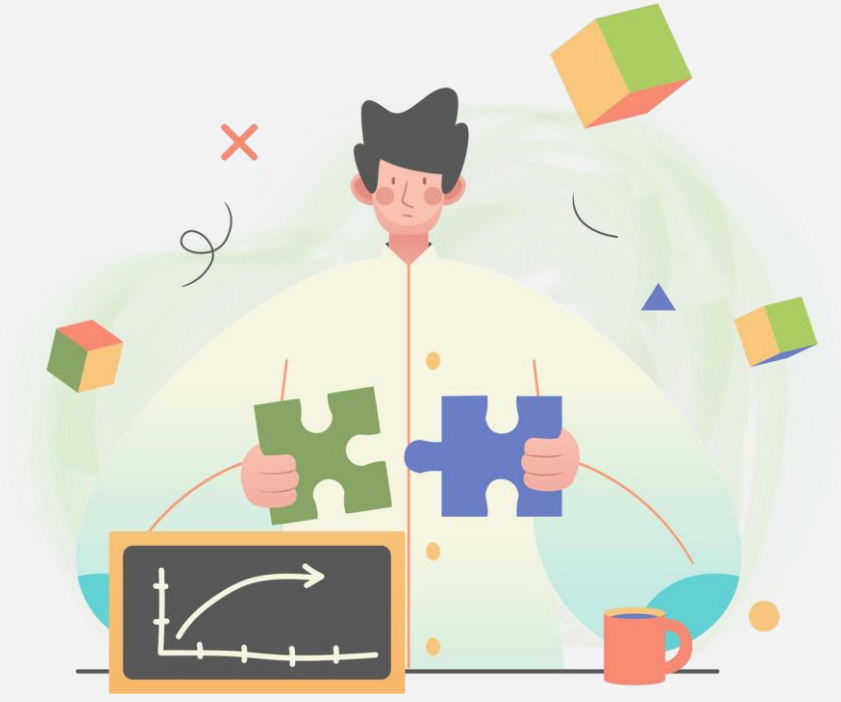
본 문서는 한국인터넷진흥원에서 작성한 가이드입니다.
이 가이드는 DDoS(Distributed Denial of Service) 공격에 대한 대응 방안을 안내합니다.

PART 1

개요

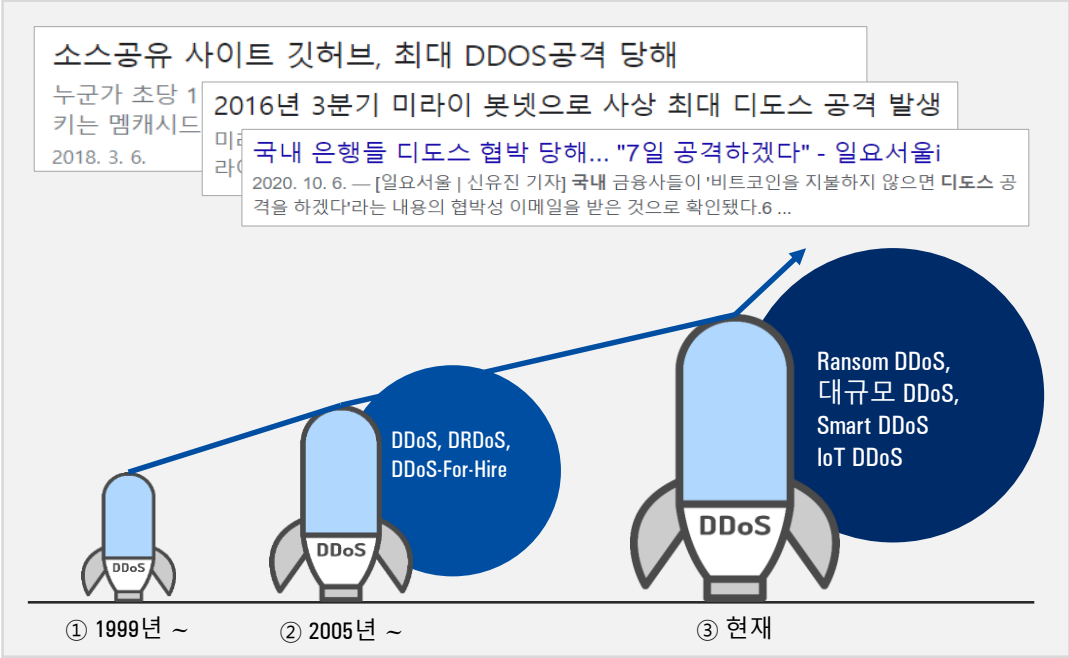
I. 증가하는 DDoS 공격의 위협

II. DDoS 공격이란?



PART 1 개요

I. 증가하는 DDoS(Distributed Denial of Service) 공격의 위협



DDoS 공격 발전형태

① 1999년 ~

- DoS 공격 : Ping of Death, Tear Drop, Smuff, Land Attack 등 비교적 단순한 형태의 DoS 공격

② 2005년 ~

- DDoS 방어 인프라를 압도하기 위해 다수의 봇넷(Botnet)으로 대규모 트래픽을 유발하는 DDoS / DRDoS 공격 및 DDoS-For-Hire[1] 등장

③ 현재

- 대응 시스템을 우회 & 압도하기 위한 고도화된 신규 DDoS 공격 유형 등장

  (Smart Attack[2], Memcached Reflection Attack, Carpet Bombing[3] 등)

- 랜섬 디도스(Ransom DDoS)[4] 등장
- CDN 서비스, 클라우드 서비스 등을 통하여 대규모 DDoS 공격을 대응 시스템 도입 활성화

---

[1] DDoS For Hire : 돈을 받고 DDoS 공격을 수행해주는 시스템

[2] Smart Attack : 기술적으로 정교하고 고도화된 DDoS 공격

[3] Carpet Bombing : 융탄폭격 이라는 의미로 하나의 IP가 아닌 같은 대역대의 여러 IP로 트래픽을 분산시켜서 공격하는 방식 공격 유무 판별 및 대상 식별이 어려움(2020년 10월부터 발생된 랜섬 디도스 공격이 대부분 해당 공격을 이용하여 발생)

[4] 랜섬 디도스 : Ransom(협박)과 DDoS 의 합성어로서 공격 전 DDoS 공격 협박을 통해 돈을 갈취하는 형태의 DDoS 공격

PART 1 개요

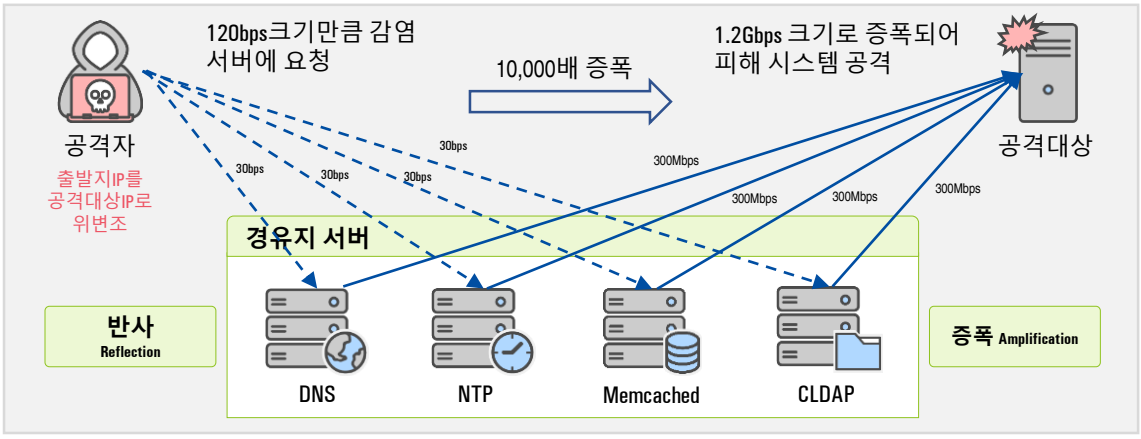
II. DDoS(Distributed Denial of Service) 공격이란?

다수의 서버, PC등을 이용해 비정상적인 트래픽을 유발시켜서 대상 시스템을 마비시키는 공격 행위

DDoS 공격 개념도

공격자는 취약한 서버를 공격하여 악성코드를 배포하고, 유포지/경유지 서버에서 악성코드를 내려 받은 서버/기기들을 이용하여 봇넷[1]을 구축한다.

공격자는 봇넷에 명령을 전달하여 대규모의 트래픽을 유발 (DDoS공격) 시키거나, 취약한 서버를 악용하여 반사공격(DRDoS 공격)을 수행 한다.



DRDoS 공격 개념도

[1] 봇넷(Botnet) : 악성코드 등에 의해 감염된 피해PC, IoT기기, 서버들로 구성된 네트워크 집단으로 주로 공격자의 공격도구로 사용됨

PART 2

공격유형 & 대응 방안

I. DDoS 공격형태

II. 대역폭 공격

III. 자원 소진 공격

IV. 웹/DB 부하 공격

PART 2 공격 유형 및 대응 방안

I. DDoS 공격 형태

DDoS 공격은 공격 형태에 따라 크게 △대역폭 공격, △자원 소진 공격, △웹/DB 부하 공격이 있다.

각각의 공격 형태마다 특징이 있으며, 대응하는 방법도 각기 다르다.

모든 DDoS 공격은 공격을 수행하는 봇넷의 규모에 따라 위험도가 비례하고, 통상 대부분의 공격은 여러 공격 유형을 혼합하는 멀티벡터 공격을 사용한다. 예를 들어 웹/DB 부하 공격을 대역폭 공격과 함께 사용할 경우 공격 식별 및 대응이 어려워 진다.

DDoS 공격 유형별 구분

구분	대역폭 공격	자원 소진 공격	웹/DB 부하 공격
공격 특성	높은 bps[1]	높은 pps[2], 높은 connection[3]	높은 pps, 높은 connection
공격 유형	UDP Flooding 및 UDP 기반 반사공격 (DNS, NTP, CLDAP, SSDP 등), Tsunami syn flooding, ICMP Flooding 등	TCP SYN, ACK Flooding 등	GET Flooding, POST Flooding 등
피해 대상	동일 회선을 사용하는 모든 시스템 접속 불가	대상 서버 , 네트워크 장비 등의 과부하 발생	대상 웹 /DB서버 과부하 발생
Protocol	UDP, ICMP, TCP, GRE	TCP	HTTP, HTTPS
IP 위/변조 여부	위/변조 가능	위/변조 가능	위/변조 불가능 (실제 IP로 공격)
비고	일시적으로 대량의 트래픽을 발생시키기 때문에 회선 대역폭이 작으면 방어가 어려움	대역폭 공격에 비해 적은 트래픽으로도 서버 과부하를 유발할 수 있음	정상적으로 세션을 맺은 후 과도한 HTTP 요청으로 웹/DB서버의 과부하를 유도함

[1] bps(bit per second): 초당 bit 수를 지칭하는 약어

[2] pps(packet per second): 초당 packet 수를 지칭하는 약어

[3] connection: 데이터를 주고 받기 위해 클라이언트와 서버 간에 서로 연결된 상태

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (1) - UDP, ICMP Flooding

1. UDP Flooding

(1) UDP Flooding 개념

UDP Flooding은 대역폭 공격 중 가장 대표적인 공격 방식이다. 데이터를 전송할 때 TCP프로토콜의 연결 지향(connection-oriented)이 아닌 UDP 프로토콜의 비연결형 (connectionless) 특성을 악용한 공격이다.

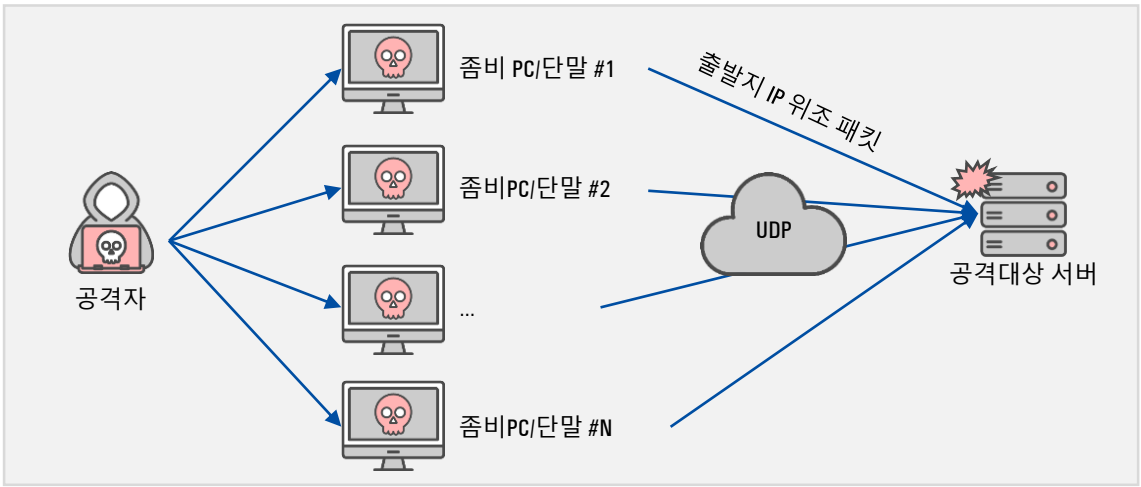
출발지 IP를 위/변조한 후 UDP 프로토콜로 대규모 데이터를 생성해 피해대상 시스템을 향해 전달한다. UDP Flooding은 대상서버에서 UDP Port를 사용하지 않아도 공격할 수 있으며, 공격을 수행하는 감염된 기기가 많을수록 위험도는 증가한다. 단순한 공격방식과 강력한 효과로 과거부터 현재까지 지속적으로 사용되는 공격방식이다.

(2) 공격원리

① 공격자는 사전에 악성코드 등을 이용해 봇넷을 확보

② 확보한 봇넷들을 이용해 피해 서버로 대규모의 UDP Packet을 전달

③ 대규모의 UDP Packet이 피해자의 시스템으로 전달되면서 피해 시스템의 회선 대역폭을 고갈시킴



UDP Flooding 공격 원리

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (1) - UDP, ICMP Flooding

1. UDP Flooding

(3) 대응 방안

① UDP 패킷 차단

- UDP 프로토콜을 사용하지 않는다면 웹서버 상단의 라우터 혹은 방화벽 장비에 UDP 프로토콜을 원천 차단하는 설정을 적용
- UDP 프로토콜을 사용한다면 필요한 서비스 Port만 허용한 후, 임계치 기반 차단 정책을 적용 (예시 – 초당 100개 이상의 UDP 패킷 인입 시 차단)

※ UDP Flooding 공격은 동일 회선을 사용하는 모든 시스템에 영향을 미침

따라서 피해를 최소화하기 위해 공격 받는 서버로 오는 모든 트래픽을 라우터나 백본과 같은 네트워크 최상단 장비에서 Null0 라우팅[1]을 통해 대역폭을 보장하는 방식의 대응이 필요

② DDoS 방어 서비스 이용

- UDP Flooding은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 UDP Flooding의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

[1] Null0 라우팅: 패킷을 라우팅하지 않고 폐기한다는 의미로, 특정 IP에 대해 null0 라우팅 설정을 하면 해당 IP로 가는 모든 패킷을 폐기하게 됨

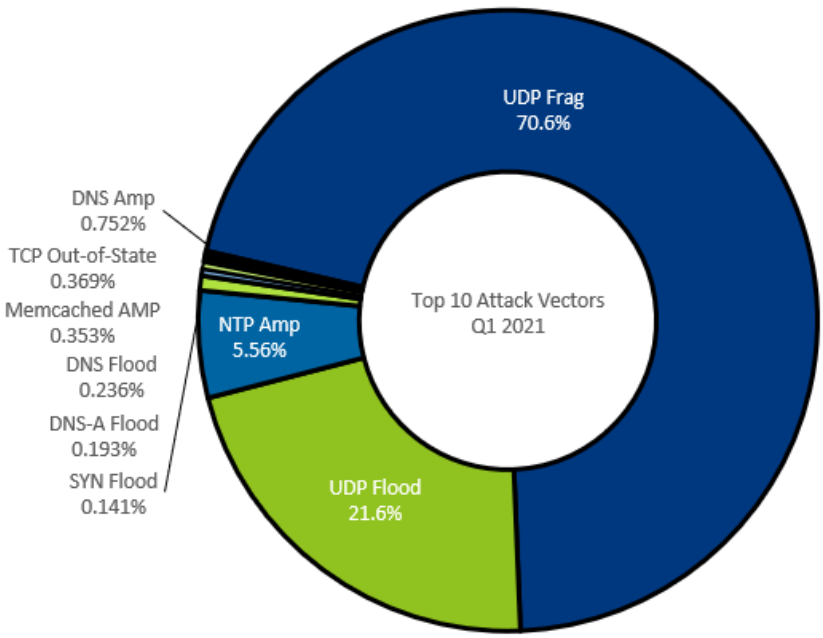
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (1) - UDP, ICMP Flooding

1. UDP Flooding

최근 공격 동향

- 대역폭 공격 유형 중 가장 오랫동안 사용된 공격
- 의미 없는 데이터로 채워진 많은 양의 UDP Packet을 다수의 봇넷을 통해 피해자 시스템으로 보내는 방식의 단순 공격이지만 그 효과가 크기 때문에 꾸준하게 사용되는 공격 유형이며, 가장 많이 발생하는 공격인 만큼 각별한 주의가 필요
- 반사 공격이 등장하면서 단일 UDP Flooding의 비중은 줄어들었지만 여전히 대역폭 공격에선 가장 많은 비중을 차지
- Radware에서 발표한 2021년 1분기 보고서에 따르면 전체 대역폭 공격 중 UDP Flooding, UDP Frag Flooding이 차지하는 비율이 90%가 넘는 것을 알 수 있음



2021년 1분기 DDoS 공격 유형 Top10
(출처: Radware, Quarterly DDoS Attack Report)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (1) - UDP, ICMP Flooding

2. ICMP Flooding

(1) ICMP Flooding 개념

Internet Control Message Protocol은 장치간 연결을 진단하는 ping 명령에 대표적으로 쓰이는 프로토콜로서 주로 ICMP Request와 Reply를 사용한다.

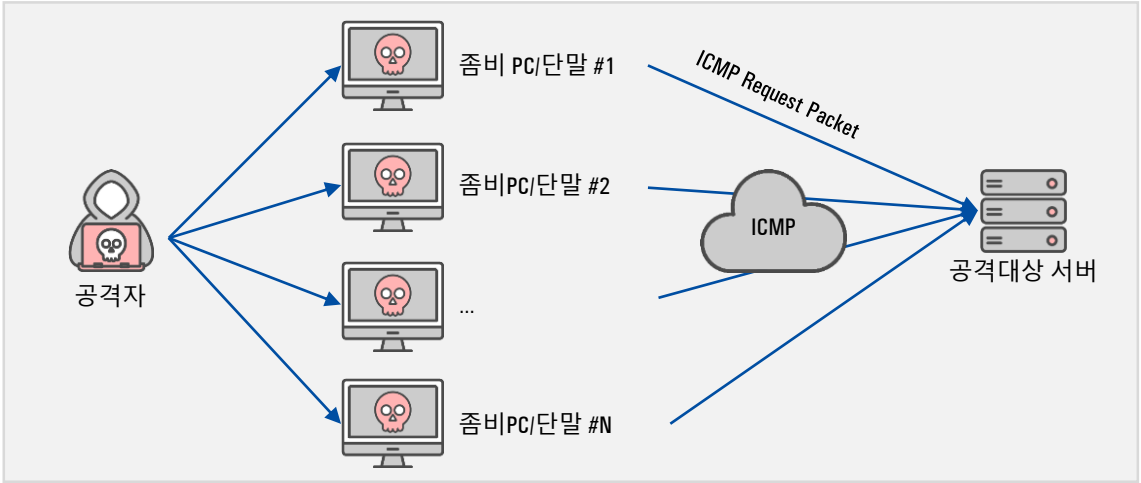
ICMP Flooding은 ICMP Request 패킷을 이용하여 피해서버로 대량의 ICMP 패킷을 생성해 전달하여 피해서버의 대역폭을 고갈시키는 공격방식이다. 반사공격과 다르게 ICMP Flooding은 증폭이 발생하지 않기 때문에 공격기기의 대역폭에 따라 공격 규모가 결정된다.

(2) 공격원리

① 공격자는 사전에 악성코드 등을 이용해 봇넷을 확보

② 확보한 봇넷들을 이용해 피해 서버로 대규모의 ICMP Request Packet을 전달

③ 대규모의 ICMP Request Packet이 피해자의 시스템으로 전달되면서 피해 시스템의 회선 대역폭을 고갈시킴



ICMP Flooding 공격 원리

PART 2 공격 유형 및 대응 방안

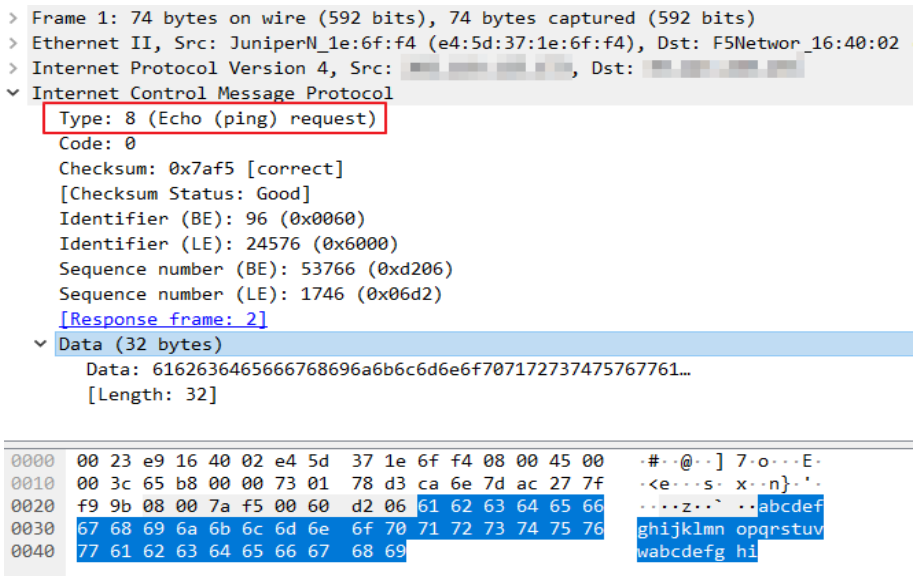
II. 대역폭 공격 (1) - UDP, ICMP Flooding

2. ICMP Flooding

(3) 대응방안

① ICMP 패킷 차단

- 외부로부터의 ICMP를 사용하지 않는 환경이라면 외부로부터 인입되는 ICMP 패킷에 대하여 네트워크 상단의 라우터 혹은 방화벽 장비에서 ICMP 프로토콜을 원천 차단하는 설정을 적용
- ICMP를 사용한다면 임계치 설정을 적용하여 짧은 시간에 과도하게 많은 ICMP 패킷을 전달하는 IP를 차단하도록 설정 (예시 – 초당 10개 이상의 ICMP 패킷 인입 시 해당 IP 차단)



ICMP Request Packet (샘플)

② DDoS 방어 서비스 이용

- ICMP Flooding은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 ICMP Flooding의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

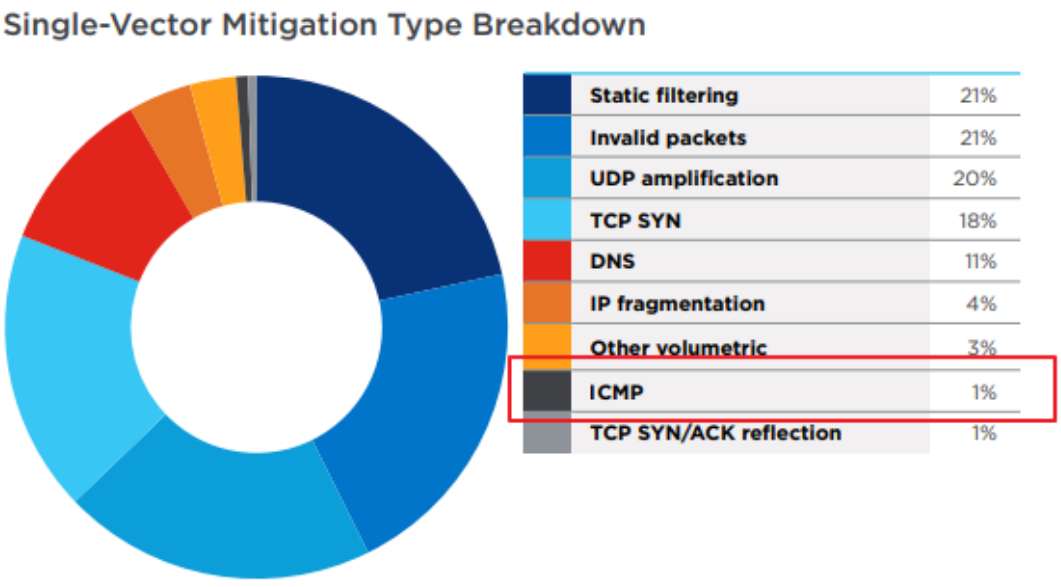
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (1) - UDP, ICMP Flooding

2. ICMP Flooding

최근 동향

- ICMP Flooding은 다른 DDoS 공격에 비하여 효율이 떨어지고 대응 방안이 비교적 잘 알려져 있기 때문에 최근에는 많이 사용되는 공격은 아님
- 단일 공격 보다는 다수의 유형을 혼합하여 공격하는 복합공격 형태로 사용되는 것이 대부분임



ICMP Flooding 공격 비율
(출처: Lumen 2021년 1분기 DDoS 보고서)

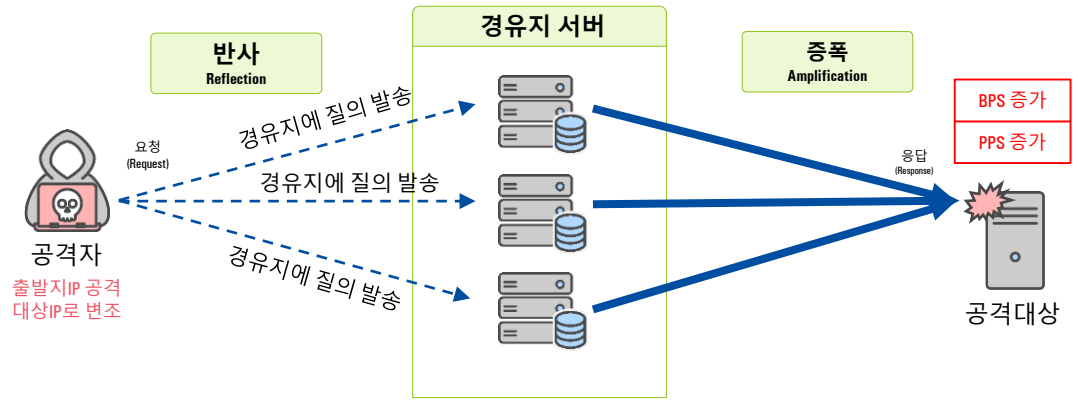
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

DRDoS(Distributed Reflection Denial of Service) 공격은 단순 DDoS 공격에서 더 발전된 공격형태다. 봇넷 기기들이 직접 공격을 수행하는 것이 아닌 증폭공격에 활용되는 서비스를 제공하는 서버 및 서버 역할을 할 수 있는 단말 장비(네트워크 장비, 공유기 등)까지 공격기기로 이용한다는 특징이 있다.

✓ DRDoS 공격

- 공격자는 외부에 노출된 취약한 서버를 경유지 서버로 악용 하는데, 이 때 경유지 서버는 적은 요청으로 큰 응답 값을 가져오는 서버를 대상으로 함
- 경유지 서버에 요청할 출발지 IP를 공격대상의 IP로 변조, 대량의 요청을 보낸 후 경유지 서버로부터의 증폭된 응답 값을 공격대상이 받게 함
- 증폭된 응답 값을 통해 공격 대상의 회선 대역폭을 가득 차게 만들어서 공격 대상의 서비스를 마비시키는 공격 기법
- 공격을 반사하여 증폭하는 공격이라고 해서 '반사·증폭공격'이라고 함



※ 공격 원리

① 공격자는 많은 수의 경유지 서버에 특정 질의 명령어(요청)를 일괄적으로 보낸다.
이 때 자신의 IP를 공격대상 IP로 변조하여 공격 대상 IP가 응답을 받도록 한다.
효과적인 공격을 위하여 경유지 서버가 응답하는 양이 큰 질의 명령어를 사용한다.
(예시 : DNS 서버에 'Any' 질의를 하면, DNS 서버는 입력한 명령어의 약 26~52배의 문자로 답변을 한다.)

② 경유지 서버는 정상 요청으로 인식하여 공격대상 서버에 명령어 결과(응답)을 보낸다.

③ 많은 수의 경유지 서버로부터 응답을 받은 공격대상 네트워크는 트래픽이 급증하여 회선 대역폭이 가득 차게 된다.

DRDoS 공격 방식

PART 2 공격 유형 및 대응 방안

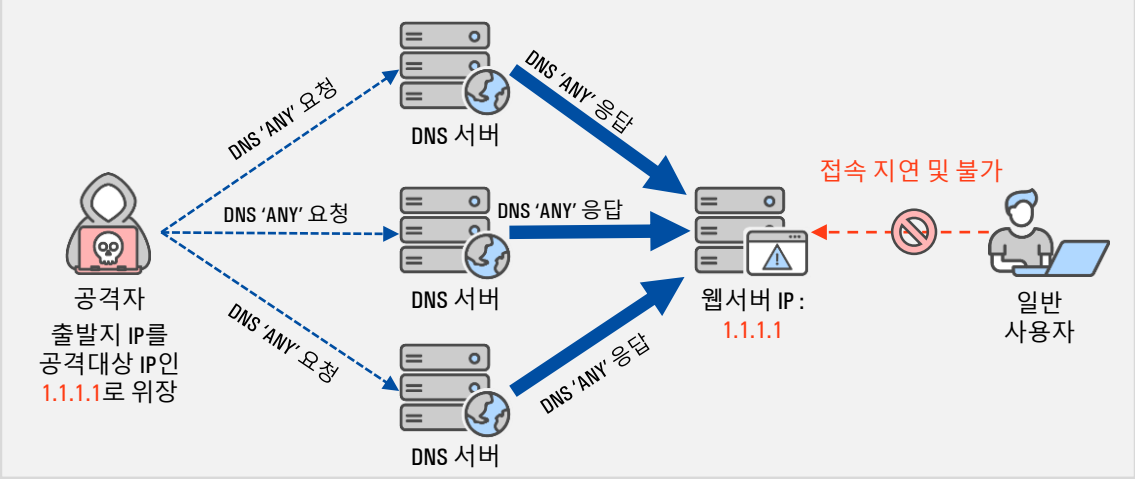
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

1. DNS Reflection Attack

(1) DNS Reflection Attack 개념

DNS(Domain Name System)는 도메인 이름을 IP주소로 응답주거나 IP주소를 도메인 이름으로 응답주는 시스템이다. 사람이 기억하기 어려운 IP주소를 보완하기 위해 사용된다.

DNS Reflection Attack은 공격자가 피해자의 IP로 위장(스푸핑 [1])하여 네임서버에 비정상 DNS 질의를 요청하고, 요청을 받은 네임서버는 DNS 응답 값을 위장한 IP로 전송하여 공격 대상의 회선 대역폭을 고갈시키는 공격이다. 공격 트래픽 양을 높이기 위하여 단순 DNS Query가 아닌 Zone의 모든 정보를 요청하는 "ANY" Type[2] 레코드를 요청하는 특징이 있다.



DNS Reflection Attack 원리

[1] 스푸핑(Spoofing): 출발지 IP를 변조하는 행위로서 공격자가 공격 근원지의 추적을 회피하기 위해서 사용된다. DRDoS에서는 공격을 받는 대상IP로 출발지 IP로 변조할 때 사용된다.

[2] ANY Type Query : 질의 도메인에 대해 네임서버의 Zone에 등록된 모든 레코드 값을 전부 요청하는 Type의 DNS Query

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

1. DNS Reflection Attack

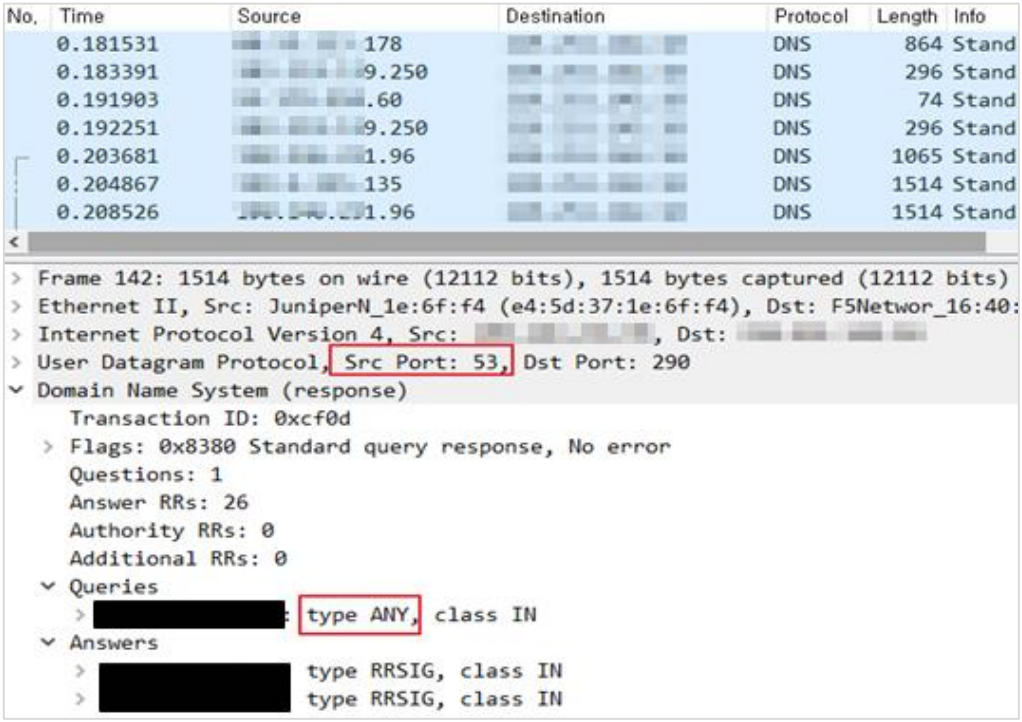
(2) 공격원리

① 공격자는 사전에 취약한 DNS 서버들의 목록들을 확보

② 피해자의 IP로 스푸핑한 다음 확보한 서버들을 대상으로 가능한 많은 응답 사이즈를 만들어 내기 위해 ANY Type의 DNS Query 패킷을 요청

③ 취약한 DNS서버들은 요청 받은 Query패킷에 대한 증폭된 응답 값을 피해자의 시스템으로 전달 (증폭률 28～54배)

④ 대규모의 DNS Response 패킷이 피해자의 시스템으로 전달되어서 피해서버의 회선 대역폭을 고갈시킴



DNS Reflection Attack 공격 패킷(샘플)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

1. DNS Reflection Attack

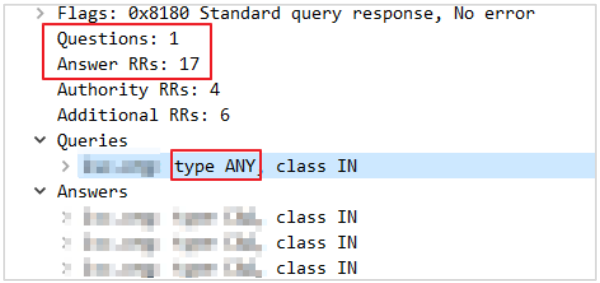
(3) 대응 방안

① UDP 패킷 차단설정

- 출발지 포트가 53/UDP이면서 목적지 주소가 DNS 서버가 아닌 패킷을 차단

※ DNS 응답은 DNS 서버 간의 통신이며 실제 사용자 기기에 전달되는 DNS 응답은 모든 질의 과정을 마친 내부DNS(로컬DNS)를 통해 이루어짐. 따라서 인터넷에서 인입되는 모든 DNS 응답 패킷은 DNS 서버IP로만 통신, 대상 IP가 DNS서버가 아니라면 비정상 공격 패킷으로 판단 가능

※ DNS 서버를 대상으로 인입되는 DNS 응답 패킷에서 짧은 시간안에 ANY Type으로 대규모 패킷이 인입될 경우 공격 행위임을 의심 해볼 수 있음



ANY Type DNS 응답 패킷(샘플)

- UDP를 사용하지 않는 시스템일 경우 UDP Flooding 방어 방법과 동일하게 상단 라우터 및 보안장비를 통해 UDP 프로토콜 패킷 원천 차단
- DNS Query를 사용하는 시스템일 경우 DNS Query 패킷에 대한 임계치 값을 설정하여 임계치 이상으로 인입되는 패킷 차단

② DNS 취약점 체크

- 네임서버를 운영하고 있다면 본인의 서버가 반사체로 악용되지 않도록 확인해야 함
- 공격에 활용되는 DNS Query 패킷은 "ANY" type으로 요청하며, 재귀 쿼리[1]를 시도함 따라서 반드시 필요한 상황이 아니면 DNS 재귀기능을 비활성화 하고, 과도한 OutBound 트래픽이 생성되는지 모니터링이 필요함

✓ 네임서버가 공격에 악용될 수 있는지 확인하는 사이트

https://openresolver.com

[1] 재귀 쿼리 : 요청 받은 DNS Zone 정보를 갖고 있지 않을 경우 최상위 DNS부터 마지막 DNS서버에 이르기까지 반복적으로 DNS Query를 수행하는 방식

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

1. DNS Reflection Attack

(3) 대응 방안

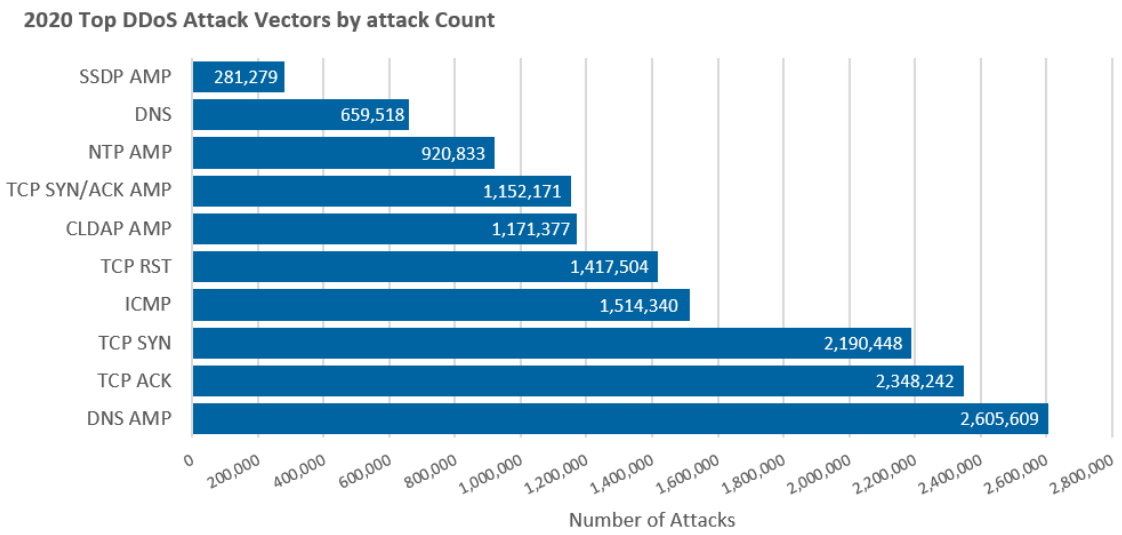
③ DDoS 방어 서비스 이용

- DNS Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 UDP Flooding의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

최근 공격 동향

- 반사공격 유형 중에서 가장 오랫동안 사용된 공격 유형이다.
- 해외 DDoS 대응 업체인 NETSCOUT의 2020년 위협보고서에도 DNS 증폭 공격이 DDoS 공격 유형중 가장 많은 비중을 차지하였다. (아래 그림 참조)



2020년 DDoS 공격 유형 Top 10

(출처: NETSCOUT, NETSCOUT THREAT INTELLIGENCE REPORT)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

2. NTP Reflection Attack

(1) NTP Reflection Attack 개념

시간동기화를 위해 사용되는 NTP(Network Time Protocol) 서버를 반사서버로 악용한 공격이다. 스푸핑된 IP(피해자의 IP)로 NTP 서버에게 비정상적인 요청 패킷을 보내서 되돌아오는 응답 값을 공격 payload[1]로 활용하는 공격 유형이다.

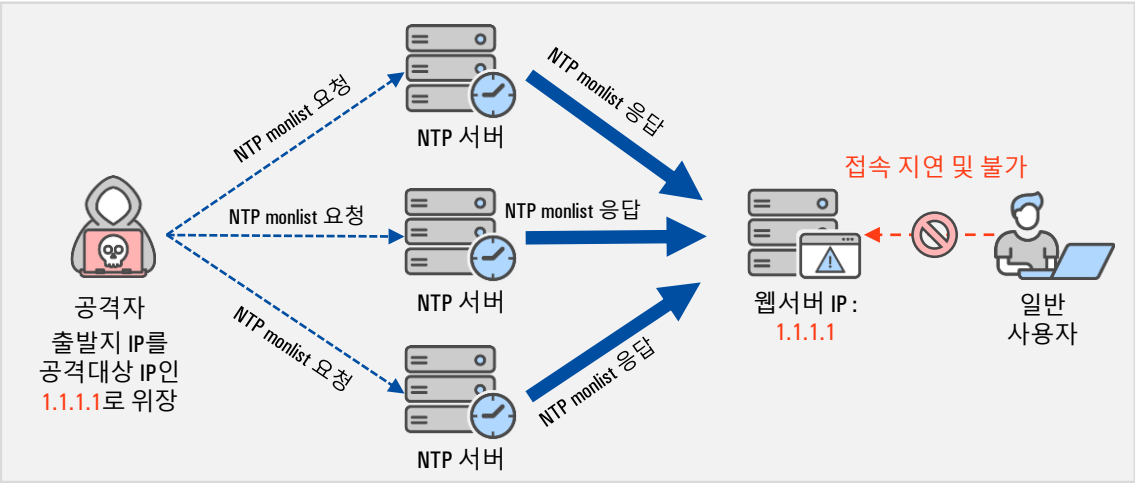
(2) 공격원리

① 공격자는 사전에 취약한 NTP 서버들의 목록을 확보

② 피해자의 IP로 스푸핑 한 다음 확보한 서버들을 대상으로 가능한 많은 응답 패킷을 만들어 내기 위해 monlist[2] 를 요청하는 명령을 전송

③ 취약한 NTP서버들은 요청 받은 monlist 명령어에 대한 응답 패킷으로 증폭된 응답 값을 피해자의 시스템으로 전달 (증폭률 최대 550배)

④ 대규모의 monlist 패킷이 피해자의 시스템으로 전달되어서 피해서버의 회선 대역폭을 고갈시킴



NTP Reflection Attack 원리

[1] payload : 통신 패킷에서 헤더나 메타데이터를 제외한 본문 데이터에 해당하는 부분

[2] monlist : 구버전의 NTP서버에서 사용하는 명령어로, 최근 접속한 최대 600개의 접속 호스트에 대한 정보를 응답 받을 수 있는 명령어 (v2.4.7 이상에서는 해당 명령어가 삭제됨)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

2. NTP Reflection Attack

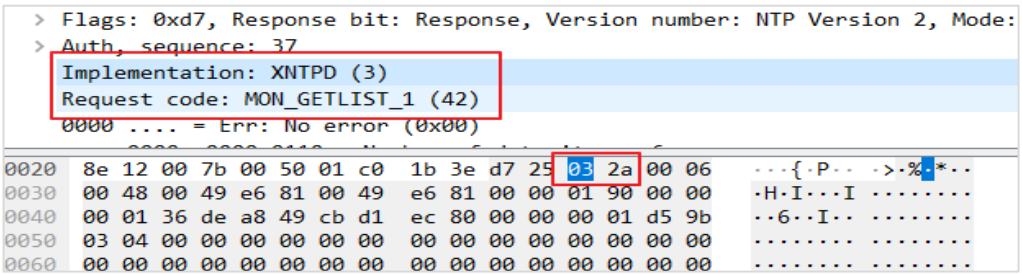
(3) 대응 방안

① UDP 패킷 차단설정

- 반사공격을 수행하는 패킷은 NTP 서버가 응답한 트래픽이므로 출발 포트가 123/UDP인 패킷을 차단

※ 이 차단 설정을 적용하기 위해서는 모든 IT 인프라가 사용하는 시간 동기화를 반드시 내부망에 구축한 NTP 서버로만 설정해야 함. 그래야 내부 NTP 서버만이 외부 NTP 서버와 통신하기 때문에 그 외 서버의 외부 NTP 통신을 공격 징후로 판단할 수 있음

- UDP 프로토콜을 사용하지 않으면 UDP Flooding 방어 방법과 동일하게 상단 라우터 및 보안장비를 통해 UDP 프로토콜 패킷 원천 차단
- 외부 NTP서버를 사용하는 경우 지정된 NTP 서버만 허용하도록 설정
- 패킷에 monlist 값이 포함될 경우 차단



NTP monlist 응답 패킷(샘플)

② 운영 중인 NTP 서버 설정 및 취약점 점검

- NTP 서버를 내부망에서만 사용하고 인터넷망에 노출시키지 않아야 함
- 운영 중인 NTP서버는 본인의 서버가 반사체로 악용되지 않도록 주의하고 정기적으로 취약점 점검을 수행함

✓ 취약 NTP 서버 확인 방법

→ ntpdc –n –c monlist [IP 주소] → timed out이 뜨면 안전 / 목록이 뜨면 취약

✓ NTP서버에서 monlist를 사용하지 않은 방법 (버전 업그레이드)

→ NTP 버전 4.2.7 이상으로 업그레이드 (monlist 미사용 버전)

✓ monlist 기능 비활성화 방법 (업그레이드 불가시)

→ /etc/ntp.conf 파일에서 “disable monitor” 추가 후 NTP 서비스 재시작

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

2. NTP Reflection Attack

(3) 대응 방안

③ DDoS 방어 서비스 이용

- NTP Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 NTP Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

3. CLDAP Reflection Attack

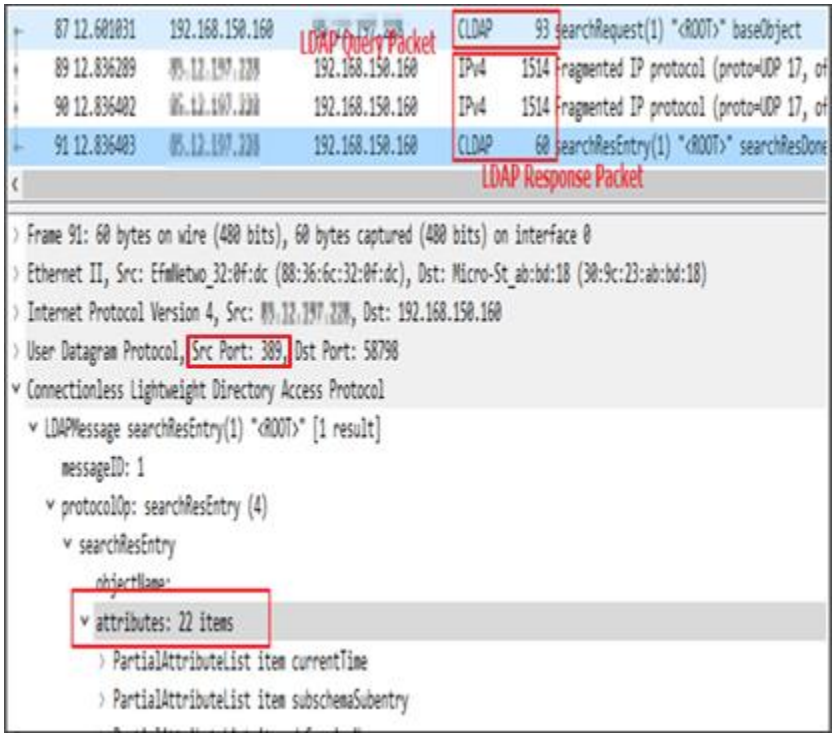
(1) CLDAP Reflection Attack 개념

CLDAP(Connection-less Lightweight Directory Access Protocol)이란 네트워크상에서 디렉토리를 연결/검색/수정하기 위해 사용되는 프로토콜이다.

CLDAP Reflection Attack은 CLDAP 서버를 반사서버로 악용한 공격으로서, 피해자의 IP로 스푸핑된 IP를 통해 CLDAP 서버에게 비정상적인 Query를 보낸 후 되돌아오는 응답 값을 공격 패킷으로 활용하는 공격 유형이다.

(2) 공격원리

CLDAP 서버가 갖고 있는 모든 Entry 및 Attribute 값을 요청한다. CLDAP 서버가 갖고 있는 Node 정보가 많을수록 응답 패킷의 규모가 커진다. (증폭률 56~70배)



CLDAP 요청/응답 패킷(샘플)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

3. CLDAP Reflection Attack

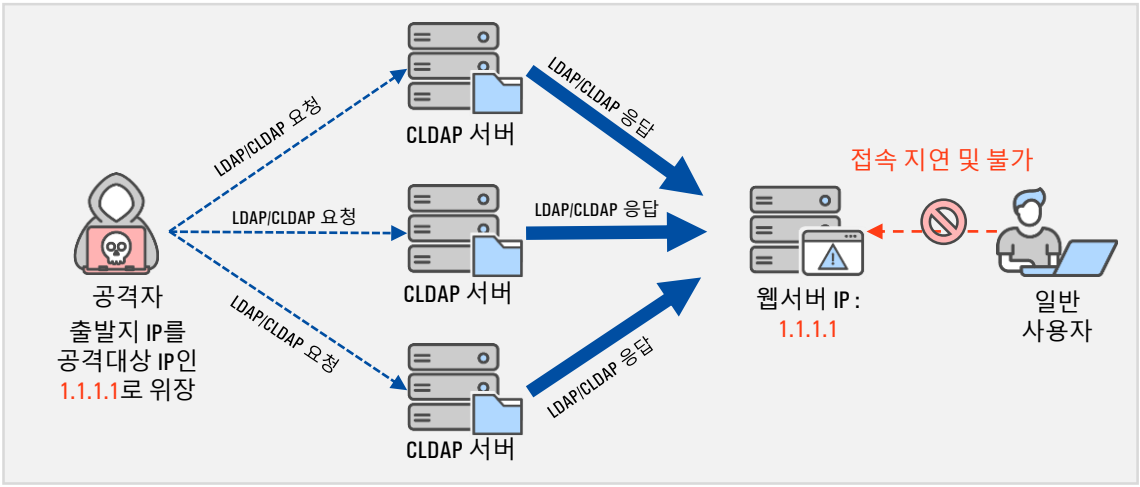
(2) 공격원리

① 공격자는 사전에 인터넷에 노출된 CLDAP 서버들의 목록을 확보

② 피해자의 IP로 스푸핑한 다음 확보한 서버들을 대상으로 가능한 많은 응답 패킷을 만들어 내기 위해 Search Entry Request 패킷을 요청

③ CLDAP 서버들은 요청 Packet에 대한 증폭된 응답 패킷을 피해자 시스템으로 전송

④ 대규모의 CLDAP Response 패킷이 피해자의 시스템으로 전달되면서 피해 서버의 회선 대역폭을 고갈 시킴



CLDAP Reflection Attack 원리

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

3. CLDAP Reflection Attack

(3) 대응 방안

① UDP 패킷 차단설정

- CLDAP Reflection Attack 패킷은 UDP 프로토콜을 사용하며 389번을 출발지 Port로 사용
- CLDAP/LDAP은 내부에서만 사용하는 프로토콜이므로 외부로부터 들어오는 CLDAP Response 패킷(UDP 프로토콜을 사용하며 출발지 Port는 389번을 사용함)은 차단

② CLDAP 외부 노출 확인

- CLDAP Reflection Attack은 외부에 노출된 CLDAP서버들을 악용하는 공격이기 때문에 LDAP 서버를 운영한다면 외부에서 접근하지 못하도록 차단해야 하며, 외부에서 LDAP 쿼리를 받지 않도록 설정해야 함

✓ LDAP 서버 외부노출 확인 방법

- ldapsearch –x –h [서버 IP] –s base
- 출력되면 외부 Open된 상태

③ DDoS 방어 서비스 이용

- CLDAP Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 CLDAP Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

3. CLDAP Reflection Attack

최근 공격 동향

- 2016년 처음 등장한 이후 현재까지 계속해서 DDoS 공격에 사용되는 주요 공격 유형중 하나
- 2020년 2월, AWS의 2020년 1분기 위협 동향 보고서(Threat Landscape Report – Q1 2020)에 의하면 CLDAP을 통해 트래픽을 약 70배까지 증폭시켜 2.3Tbps 규모의 DDoS 공격 트래픽이 발생되었다고 언급
- 기존 DDoS 공격은 기가(Gbps) 규모로 관찰되는 것이 일반적이지만, 사물인터넷(IoT) 장치가 대중화되고 해커들이 이를 악용하기 시작하면서 테라(Tbps) 규모의 DDoS 공격을 발생시킴

PART 2 공격 유형 및 대응 방안

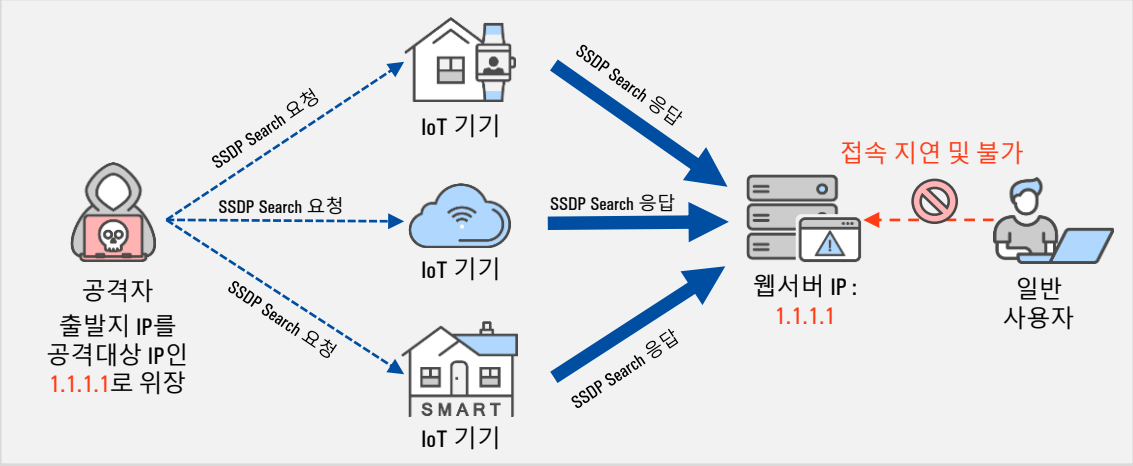
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

4. SSDP Reflection Attack

(1) SSDP Reflection Attack 개념

SSDP(Simple Service Discovery Protocol)는 UPnP 장치를 탐색할 때 주로 사용되는 프로토콜로서 네트워크상의 다른 장치를 찾거나 알리는 역할을 수행한다. SSDP 프로토콜은 웹캠, 공유기, 미디어, 스마트TV, 프린터 등 스마트 홈을 구성하는 IoT 기기들에 널리 사용되고 있다.

SSDP Reflection Attack은 이러한 SSDP 기능을 악용하여 가능한 한 많은 데이터를 요청하는 Search 명령을 보내서, 스푸핑된 피해자의 서버 IP로 대규모 응답이 가게 만드는 공격기법이다.



SSDP Reflection Attack 원리

(2) 공격원리

① 공격자는 사전에 취약한 IoT 기기들의 목록을 확보

② 피해자의 IP로 스푸핑한 다음 확보한 목록을 대상으로 더 많은 응답 패킷을 만들어 내기 위해 ssdp:all 혹은 ssdp:rootdevice 값이 포함된 Search 명령을 요청

③ IoT 기기들은 요청 받은 Search 패킷의 크기와 비교하여 훨씬 더 많은 크기의 응답 패킷을 피해자의 시스템으로 전달 (증폭률 최대 30배)

④ 대규모의 SSDP Response 패킷들이 피해자의 시스템으로 전달되어서 피해 시스템의 회선 대역폭을 고갈 시킴

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

4. SSDP Reflection Attack

(3) 대응 방안

① UDP 패킷 차단설정

- SSDP Reflection Attack 패킷은 UDP 프로토콜을 사용하며 1900번을 출발지 Port로 사용함

```
> User Datagram Protocol, Src Port: 1900, Dst Port: 1025
v Simple Service Discovery Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Server: Custom/1.0 UPnP/1.0 Proc/Ver\r\n
    EXT:\r\n
    Location: http://[redacted]/dyndev/uuid:00027130-dfcf-cfdf-3071-02000230cf0000\r\n
    Cache-Control:max-age=1800\r\n
    ST:urn:schemas-upnp-org:service:WANPPPConnection:1\r\n
    USN:uuid:00027130-dfcf-cfdf-3071-02000230cf0002::urn:schemas-upnp-org:service:WANPPPConnection:1\r\n
    \r\n
```

SSDP Reflection Packet (샘플)

- SSDP 프로토콜은 내부에서만 사용하도록 설정되기 때문에 외부로부터 들어오는 SSDP Response 패킷(UDP 프로토콜을 사용하며 출발지 Port는 1900번을 사용함)은 차단

② 외부 노출 기기 확인

- SSDP Reflection Attack은 외부에 노출된 IoT 기기들을 악용하는 공격이기 때문에 외부에서 내부의 IoT 기기들로 접근하지 못하도록 차단해야 하며, 외부로 나가는 SSDP 트래픽에 대한 모니터링이 필요함

> ✓ SSDP 노출 확인 사이트 https://badupnp.benjojo.co.uk

③ DDoS 방어 서비스 이용

- SSDP Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 SSDP Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

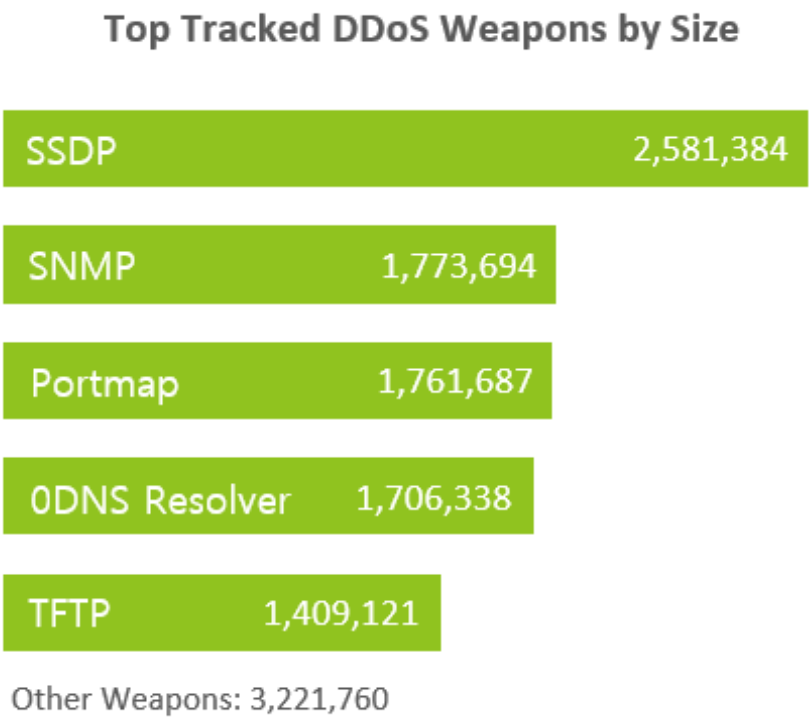
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

4. SSDP Reflection Attack

최근 공격 동향

- IoT기기의 사용이 증가함에 따라서 SSDP Reflection 공격의 위험성도 비례하여 증가하고 있음
- 2020년 상반기 A10Networks 보고서에 의하면 SSDP 프로토콜이 주 공격벡터로 사용되었으며, 약 250만개 이상의 기기가 악용되고 있음(아래 그림 참조)



2020년 상반기 공격유형 Top 5

(출처: A10Networks, The State of DDoS Weapons Report)

PART 2 공격 유형 및 대응 방안

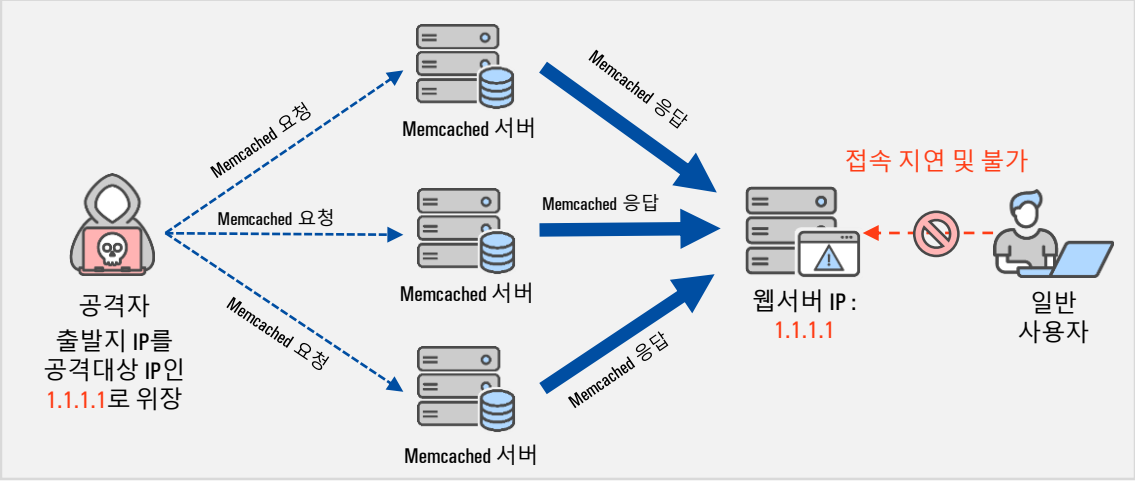
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

5. Memcached Reflection Attack

(1) Memcached Reflection Attack 개념

Memcached 서비스는 내부에서 DB부하감소 및 응답속도 증가를 위해 분산된 메모리에 데이터를 캐싱하는 서비스다. 내부에서만 접근하여 사용하도록 설계되었으며, "Key"값으로 "Data"를 매핑하는 구조이다.

Memcached Reflection Attack은 이러한 Memcached 서버의 기능을 악용하여 저장된 캐싱 데이터를 가능한 한 많이 요청하는 request 명령을 요청하고, 스푸핑된 피해자의 IP로 대규모 응답이 가게 만드는 공격기법이다.



Memcached Reflection Attack 원리

(2) 공격원리

① 공격자는 사전에 외부에 노출된 Memcached 서버들의 목록을 확보

② 확보한 Memcached 서버들에서 공격으로 악용할 Key값 및 Data값을 확보 (공격자가 외부에서 데이터를 작성하여 캐싱 시킬 수 도 있음)

③ 피해자의 IP로 스푸핑 한 후 확보한 Memcached 서버들에게 사전에 확보한 Key값에 대한 Data를 요청

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

5. Memcached Reflection Attack

(2) 공격원리

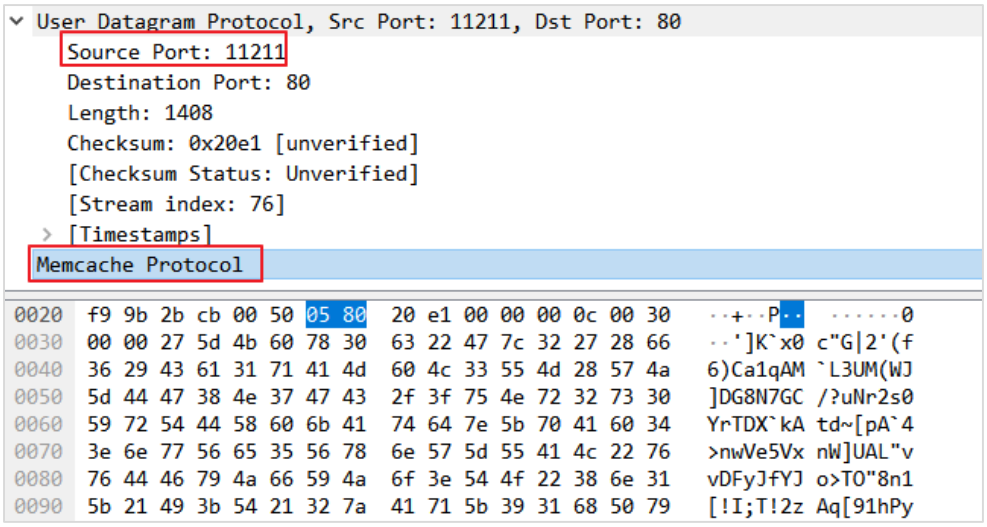
④ Memcached 서버들은 요청 받은 Key값과 매핑된 Data값을 피해자의 시스템으로 응답 (증폭률 최대 51,000배)

⑤ 대규모의 Memcached Response 패킷들이 피해자 시스템으로 전달되면서 피해 시스템의 회선 대역폭을 고갈 시킴

(3) 대응 방안

① UDP 패킷 차단설정

- Memcached Reflection Attack 패킷은 UDP 프로토콜을 사용하며 11211번을 출발지 Port로 사용
- Memcached는 내부에서만 사용하도록 설정되기 때문에 외부로부터 인입되는 Memcached Response 패킷 (UDP 프로토콜을 사용하며 출발지 Port는 11211번을 사용함)은 차단



Memcached Reflection Packet (샘플)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

5. Memcached Reflection Attack

(3) 대응 방안

② DDoS 방어 서비스 이용

- Memcached Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 Memcached Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

③ Memcached 서버 외부 노출 차단

- ✓ config 파일의 option값 변경
  → /etc/sysconfig/memcached 파일에서 OPTION="-l(영문L 소문자) 로컬IP대역" 추가
- ✓ memcached "–l" 명령어 사용
  → memcached –l "로컬IP대역"
- ✓ 1.5.6 버전이상으로 업데이트
  → http://www.memcached.org 사이트를 통해 최신 버전 설치

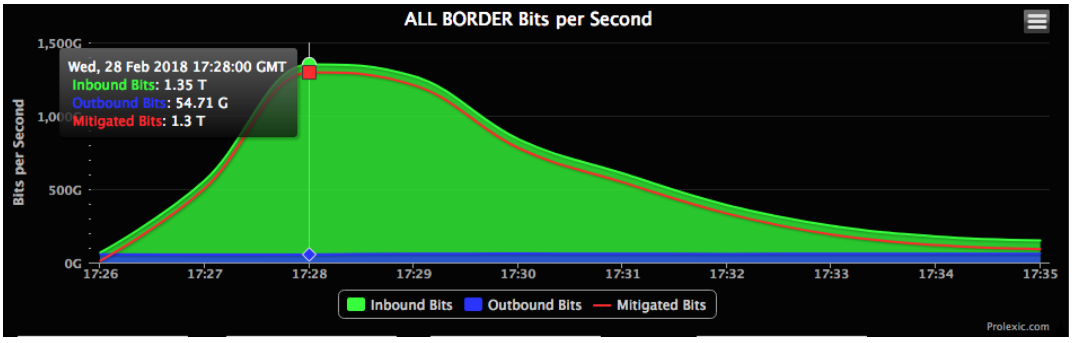
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

5. Memcached Reflection Attack

최근 공격 동향

- 2018년 2월 Github를 대상으로 1.35Tbps의 사상 최대 규모의 디도스 공격이 발생 (아래 그림 참조)
- 캐싱된 데이터를 활용해서 반사 공격 유형 중에서 가장 큰 중폭률(최대 51,000배)을 보임



소스공유 사이트 깃허브, 최대 DDOS공격 당해

| 멤캐시드 UDP 반사 공격…권한설정 없이 인터넷 노출된 서버포트 악용 기법

깃허브는 수많은 개발자들이 소스코드를 공유하고 오픈소스 프로젝트를 호스팅하는 곳이다. 해당 시점에 깃허브에 의존해 동작하는 수많은 소프트웨어 및 서비스가 운영상 차질을 빚었을 수 있는데, 깃허브는 "공격에 데이터의 기밀성이나 무결성에 문제가 발생한 지점은 없었다"고 밝혔다.

깃허브 설명에 따르면 대규모 DDoS 공격은 수만 곳의 고유 엔드포인트를 포함하는 1천여개 자동화 시스템을 통해 발생했다. 누군가 초당 1억2천690만패킷을 통해 최대시점에 1.35Tbps 트래픽을 발생시키는 멤캐시드(memcached) 기반 증폭(Amplification) 공격, 또는 '멤캐시드 UDP 반사(reflection)' 공격을 수행했다는 설명이다.

Memcached 반사 공격 사례 (출처: ZDNet)

PART 2 공격 유형 및 대응 방안

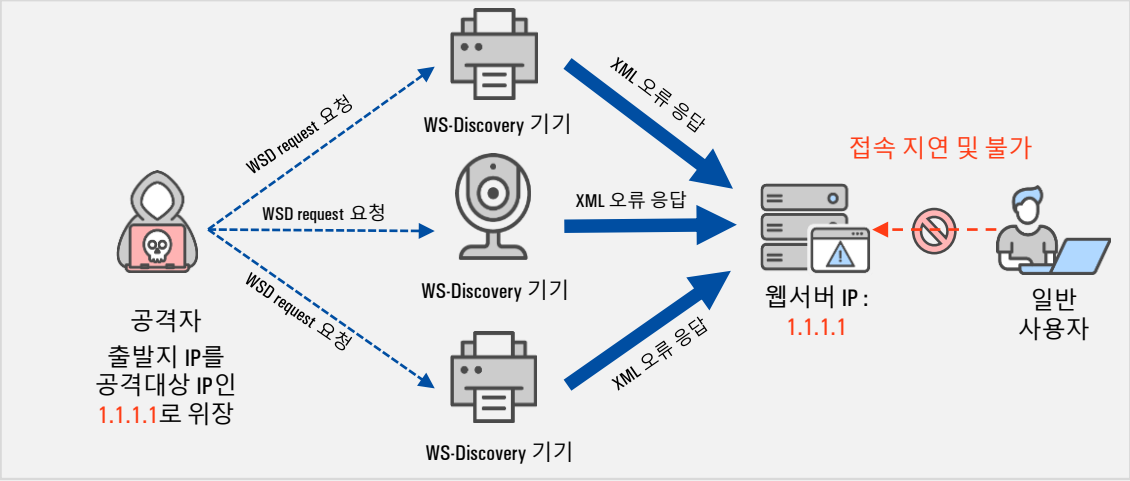
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

6. WS-Discovery Reflection Attack

(1) WS-Discovery Reflection Attack 개념

WS-Discovery 서비스는 윈도우 기반 기계들이 네트워크 프린터 등을 자동으로 찾아서 연결 설정을 완료하는데 사용되는 서비스이며, 원래는 내부 네트워크(비인터넷)망에서만 사용되지만 인터넷망에 노출될 경우에는 디도스 공격으로 악용된다.

WS-Discovery Reflection Attack은 윈도우 기반 기기들에게 요청을 할 때 고의적으로 XML오류 응답 메시지를 반복적으로 유발시키는 명령을 요청하고, 스푸핑 된 피해자의 IP로 대규모 응답이 가게 만드는 공격기법이다.



WS-Discovery Reflection Attack 원리

(2) 공격원리

① 공격자는 사전에 외부에 노출된 WSD 사용 기기들의 목록을 확보

② 피해자의 IP로 스푸핑한 후 확보한 WSD 사용 기기들에게 XML오류 응답 메시지를 반복적으로 유발시키는 명령을 대량 요청

③ 취약 기기들은 해당 요청에 대한 응답 값으로 대량의 XML 에러 메시지를 피해자의 시스템으로 발송(증폭률 최대 500배)하여 회선 대역폭을 고갈시킴

PART 2 공격 유형 및 대응 방안

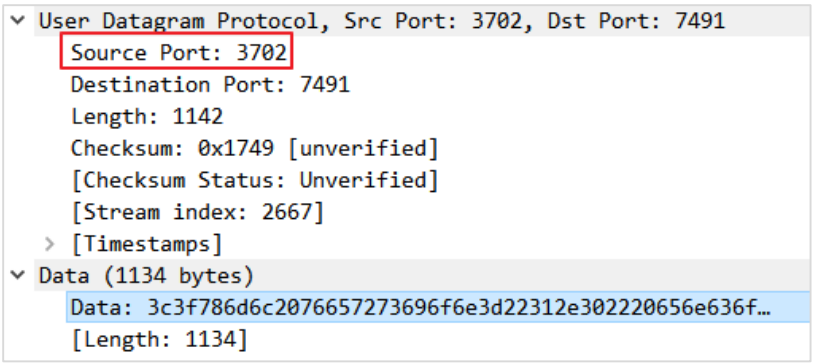
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

6. WS-Discovery Reflection Attack

(3) 대응 방안

① UDP 패킷 차단설정

- WS-Discovery Reflection Attack 패킷은 UDP 프로토콜을 사용하며 3702번을 출발지 Port로 사용함
- WS-Discovery Service는 비인터넷망에서만 사용되는 프로토콜이기에 외부로부터 인입되는 UDP 프로토콜(출발지 Port 3702)을 차단해야 함



WS-Discovery Reflection Packet (샘플)

② WS-Discovery 사용 기기들의 외부 노출 확인

- WS-Discovery Reflection Attack은 내부에서만 사용되는 WS-Discovery 프로토콜이 외부로 노출될 경우 반사체로 악용되기 때문에 외부에서 접근할 수 없도록 해야 함
- Gateway를 통과하여 외부망과 통신하는 기기가 있는지 모니터링 해야 하며, 외부로 과도한 OutBound 트래픽을 보내는 대상이 있는지 확인해야 함

③ DDoS 방어 서비스 이용

- WS-Discovery Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 WS-Discovery Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

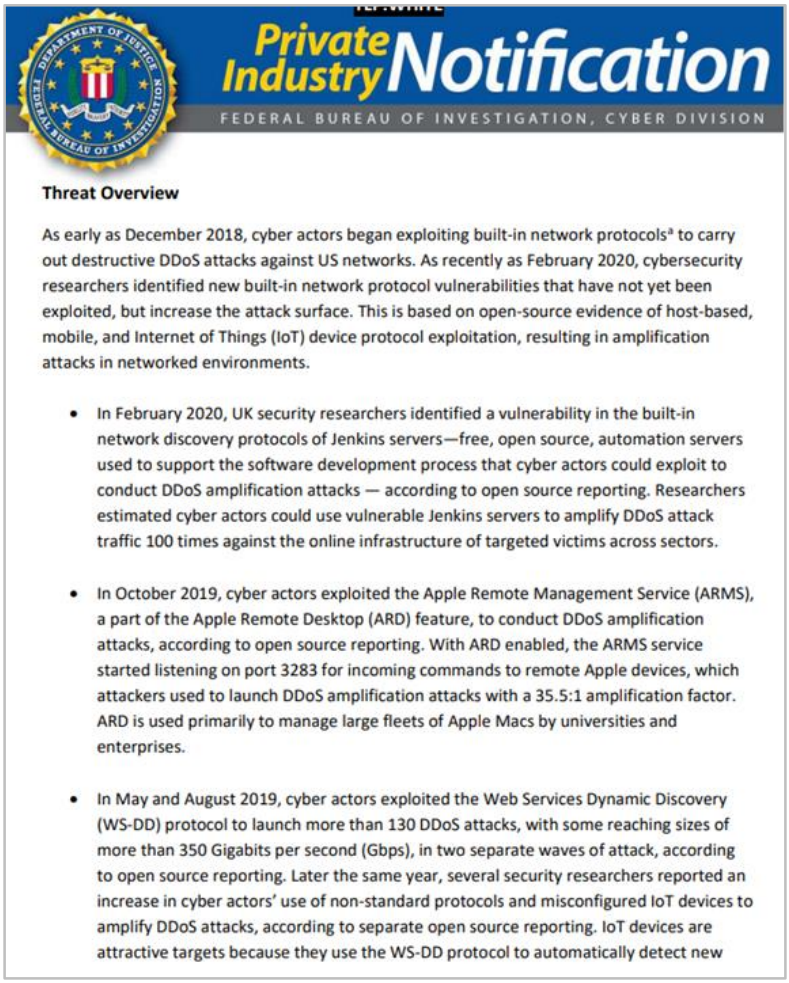
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

6. WS-Discovery Reflection Attack

최근 공격 동향

- FBI(미국 연방 수사국)가 경고한 DDoS 공격 유형 중 하나로서 새로운 DDoS 공격유형으로 언급되고 있는 공격(아래 그림 참조)
- WSD 기반 공격은 2019년도부터 탐지되기 시작했고 2020년도에 본격적으로 많은 공격이 발생, 전 세계적으로 약 80만 개의 IP주소가 WS-Discovery 공격에 악용될 수 있는 기기로 확인



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

As early as December 2018, cyber actors began exploiting built-in network protocols[a] to carry out destructive DDoS attacks against US networks. As recently as February 2020, cybersecurity researchers identified new built-in network protocol vulnerabilities that have not yet been exploited, but increase the attack surface. This is based on open-source evidence of host-based, mobile, and Internet of Things (IoT) device protocol exploitation, resulting in amplification attacks in networked environments.

- In February 2020, UK security researchers identified a vulnerability in the built-in network discovery protocols of Jenkins servers—free, open source, automation servers used to support the software development process that cyber actors could exploit to conduct DDoS amplification attacks — according to open source reporting. Researchers estimated cyber actors could use vulnerable Jenkins servers to amplify DDoS attack traffic 100 times against the online infrastructure of targeted victims across sectors.
- In October 2019, cyber actors exploited the Apple Remote Management Service (ARMS), a part of the Apple Remote Desktop (ARD) feature, to conduct DDoS amplification attacks, according to open source reporting. With ARD enabled, the ARMS service started listening on port 3283 for incoming commands to remote Apple devices, which attackers used to launch DDoS amplification attacks with a 35.5:1 amplification factor. ARD is used primarily to manage large fleets of Apple Macs by universities and enterprises.
- In May and August 2019, cyber actors exploited the Web Services Dynamic Discovery (WS-DD) protocol to launch more than 130 DDoS attacks, with some reaching sizes of more than 350 Gigabits per second (Gbps), in two separate waves of attack, according to open source reporting. Later the same year, several security researchers reported an increase in cyber actors' use of non-standard protocols and misconfigured IoT devices to amplify DDoS attacks, according to separate open source reporting. IoT devices are attractive targets because they use the WS-DD protocol to automatically detect new

DDoS 공격 경고 (출처:FBI 홈페이지)

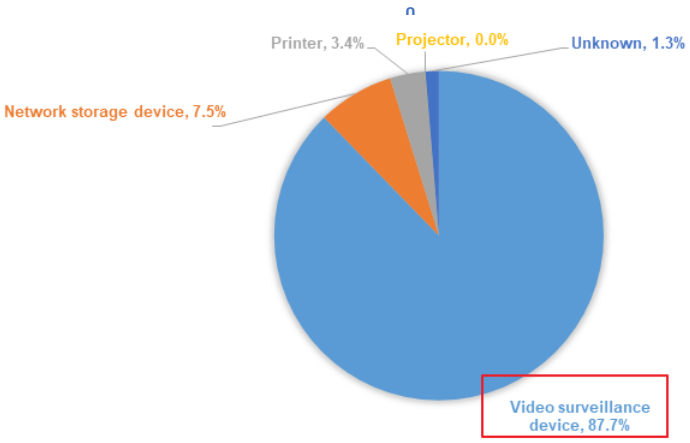
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

6. WS-Discovery Reflection Attack

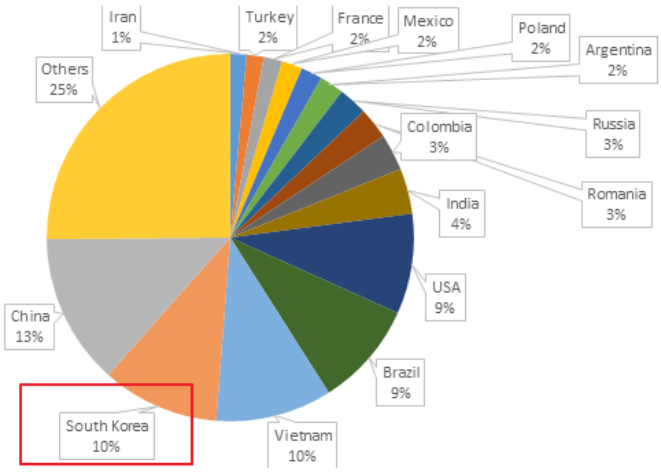
최근 공격 동향

- 80만개의 악용 가능한 기기 중 약 70만개는 영상 감시 장치로 확인



취약한 WSD 장치 종류(출처:NSFOCUS)

- 한편, WSD 취약 단말의 나라별 분포를 보면 중국, 한국, 베트남, 브라질 및 미국순으로 한국이 중국(13%)에 이어 10%를 기록하며 2위에 오름



취약한 WSD 장치 국가별 분포 현황(출처:NSFOCUS)

PART 2 공격 유형 및 대응 방안

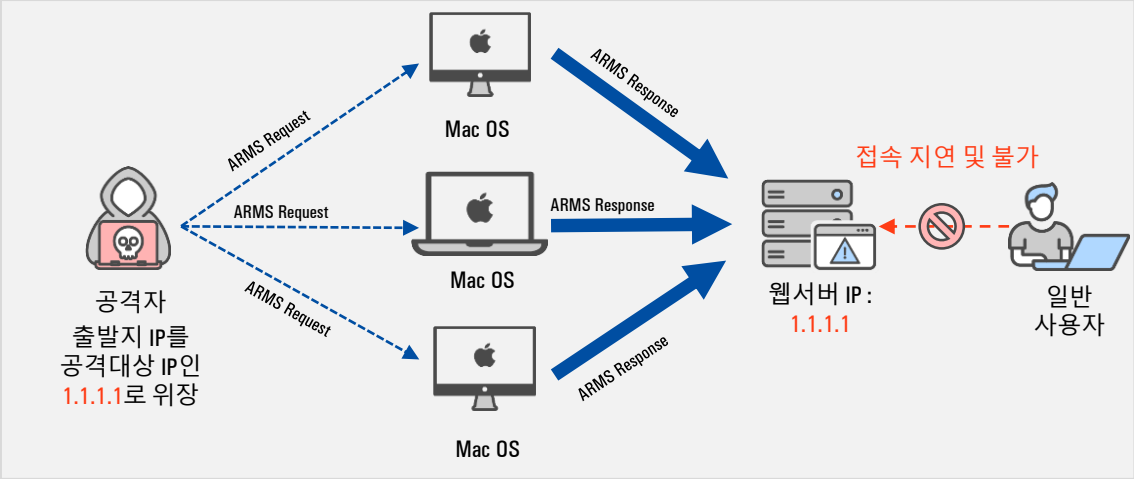
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

7. ARMS Reflection Attack

(1) Apple Remote Management Service Reflection Attack 개념

ARMS는 Apple社 기기(mac OS)들의 원격 제어 기능을 활성화 할 때 사용되는 데스크탑 원격 제어 프로토콜로서 TCP/UDP 3283번 Port를 사용한다.

ARMS Reflection Attack은 피해자의 IP로 출발지 IP를 변조한 후 취약한 Apple Mac 컴퓨터를 대상으로 원격접속 요청을 보내고, 돌아오는 응답 Packet을 피해자 시스템으로 보내는 공격기법이다.



ARMS Reflection Attack 원리

(2) 공격원리

① 공격자는 사전에 외부에 노출된 Apple社 기기들의 목록을 확보

② 피해자의 IP로 스푸핑한 후 확보된 기기들에게 대량의 request 패킷 요청

③ Apple 기기들은 해당 요청에 대한 응답 패킷을 피해자의 시스템으로 발송하여 피해자 시스템의 회선 대역폭을 고갈시킴 (증폭률 최대 35.5배)

PART 2 공격 유형 및 대응 방안

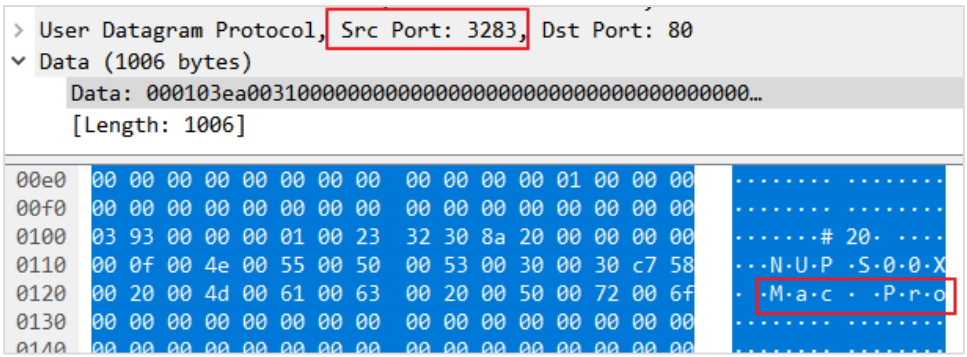
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

7. ARMS Reflection Attack

(3) 대응방안

① UDP 패킷 차단설정

- ARMS Reflection Attack 패킷은 UDP 프로토콜을 사용하며 3283번을 출발지 Port로 사용
- Apple Remote Port는 인가된 사용자만을 대상으로 허용해야 하며 외부 노출이 되지 않아야 하기 때문에 외부에서 UDP 프로토콜로 3283번 Port로 인입되는 패킷은 차단해야 함



ARMS Reflection Packet (샘플)

② ARMS 서버 외부 노출 확인

- ARMS Reflection Attack은 외부에 노출된 Apple Mac들을 악용한 공격이기 때문에 사용중인 Apple Mac에서 ARMS Port가 설정되어 있다면 외부에서 접근할 수 있는지 반드시 확인이 필요함
- ARMS를 사용할 경우 방화벽을 통해 IP를 제어해야 하며 외부로 나가는 ARMS Response Packet이 있는지 확인이 필요함

③ DDoS 방어 서비스 이용

- ARMS Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 ARMS Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

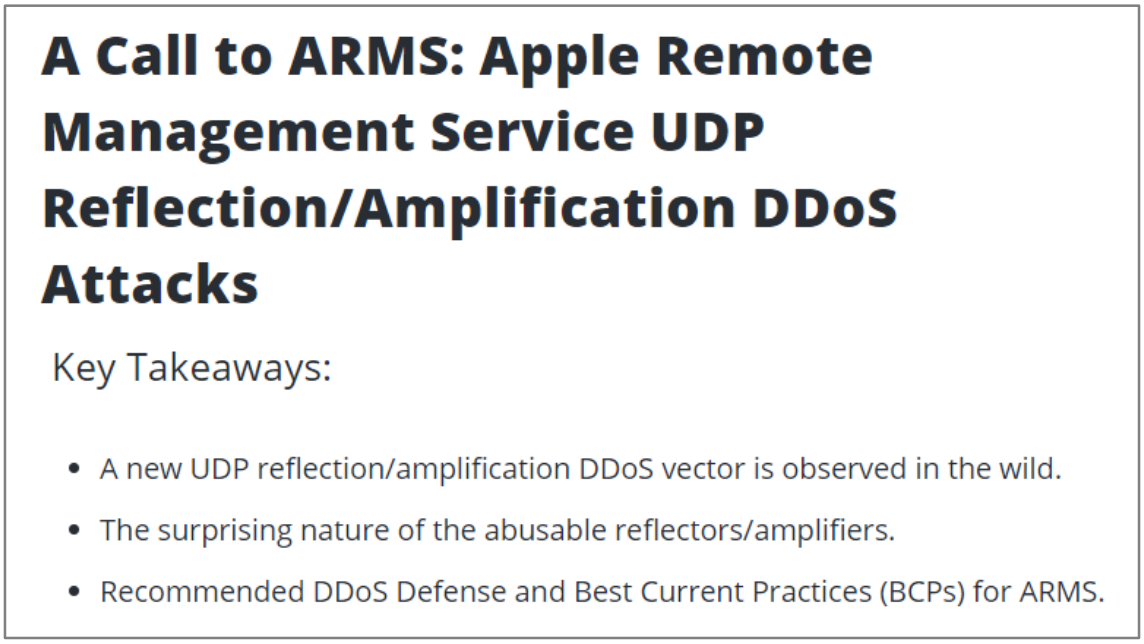
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

7. ARMS Reflection Attack

최근 동향

- WS-Discovery, CoAP와 함께 FBI(미국 연방 수사국)에서 위험한 신규 DDoS 공격유형으로 경고함
- 2019년도에 NETSCOUT에서 70Gbps 규모의 공격으로 처음 등장하였으며, 점점 더 많이 발생하고 있는 공격유형 (NETSCOUT 분석 – 아래 그림 참조)
- NETSCOUT에 의하면 2019년도 인터넷에 노출되어 공격 가능한 ARMS 지원 MacOS 기기는 약 54,000여개가 있다고 밝힘
- 전통적인 Reflection 공격들에 비해서 아직까지는 그 비중이 크진 않아서 잘 알려지지 않은 공격 유형이기 때문에 선제적 방어 정책 수립이 필요



2019 NETSCOUT에서 발표한 ARMS 분석 내용 (출처: NETSCOUT)

PART 2 공격 유형 및 대응 방안

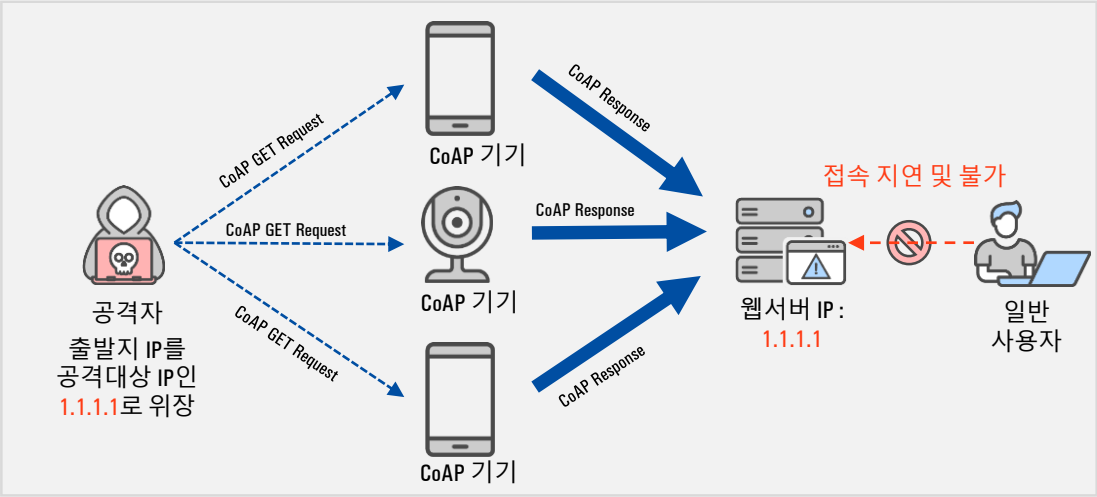
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

8. CoAP Reflection Attack

(1) Constrained Application Protocol Reflection Attack 개념

Constrained Application Protocol이란 IoT 기기들을 위해 사용되는 프로토콜의 일종으로서, 주로 저전력 컴퓨터들을 위해 만들어진 간단한 UDP 프로토콜이다. HTTP 형식과 유사한 모양을 보이며 UDP프로토콜의 5683번 Port를 사용한다.

CoAP Reflection Attack은 피해자 IP로 스푸핑한 출발지 IP에서 외부 노출된 IoT 기기 및 모바일 장치들을 대상으로 변조된 GET Request를 보내고, 돌아오는 응답 Packet을 피해자 시스템으로 보내서 피해시스템의 회선 대역폭을 고갈시키는 공격기법이다.



CoAP Reflection Attack 원리

(2) 공격원리

① 공격자는 사전에 외부에 노출된 CoAP 프로토콜 사용기기의 목록을 확보

② 피해자의 IP로 스푸핑 한 후 확보한 기기에 CoAP GET Request를 전달

③ CoAP기기는 요청 받은 CoAP GET Packet의 응답을 피해자 시스템으로 보내서 피해시스템의 회선 대역폭을 고갈시킴(증폭률 최대 50배)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

8. CoAP Reflection Attack

(3) 대응 방안

① UDP 패킷 차단설정

- CoAP Reflection Attack 패킷은 UDP 프로토콜을 사용하며 5683번을 출발지 Port로 사용
- CoAP는 내부망(비인터넷망)에서만 사용되며 외부 노출이 되지 않아야 하기 때문에 5683번 Port로 인입되는 UDP 프로토콜 패킷은 차단해야 함

② CoAP 기기 외부 노출 확인

- CoAP Reflection Attack은 외부에 노출된 CoAP 기기들을 악용한 공격이기에 CoAP기기들을 사용중인 환경이라면 외부에서 접속할 수 없는지 접근 여부를 반드시 확인해야 함
- SSDP와 마찬가지로 외부에서 접근할 수 없도록 차단 설정을 해야 하며, 외부로 나가는 OutBound Packet을 모니터링 해야 함

③ DDoS 방어 서비스 이용

- CoAP Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 CoAP Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

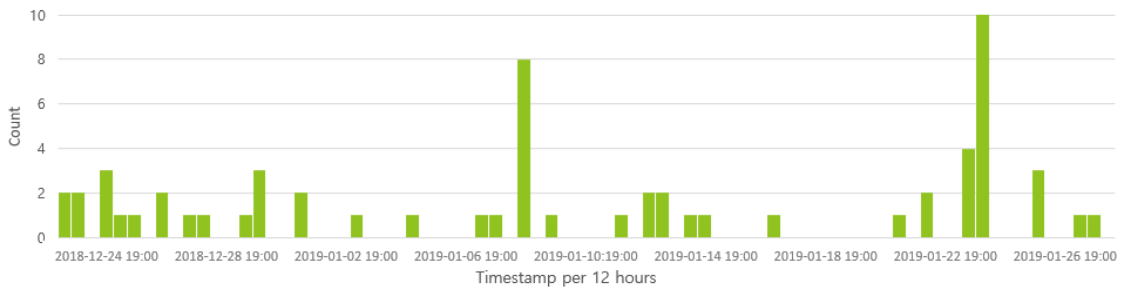
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

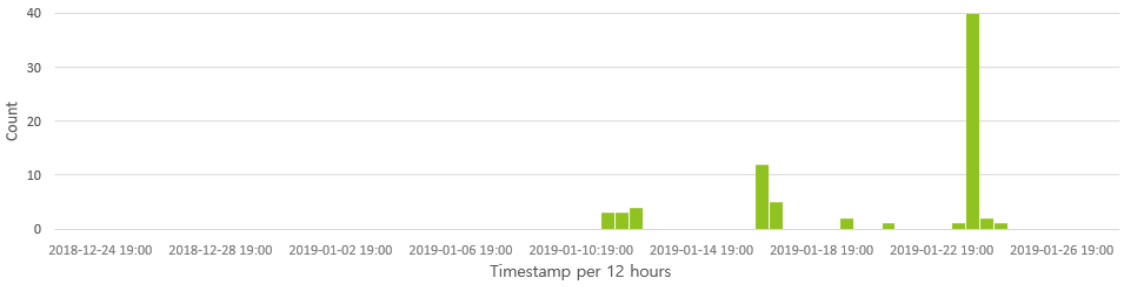
8. CoAP Reflection Attack

최근 동향

- WS-Discovery, ARMS Reflection Attack과 함께 FBI(미국 연방 수사국)에서 위험한 신규 DDoS 공격유형으로 경고함
- 해외 DDoS 대응업체인 NETSCOUT에 의하면 2019년 1월부터 CoAP의 스캔활동 및 DDoS 공격이 증가하고 있으며, 평균 공격은 초당 약 100개의 패킷을 생성하여 90초 이상 지속된다고 밝힘



2019년 CoAP 스캔 활동
(출처: NETSCOUT, CoAP Attacks In The Wild)



2019년 CoAP 공격 활동
(출처: NETSCOUT, CoAP Attacks In The Wild)

- 현재까지 확인된 CoAP 장치의 위치는 대부분 중국이며, 모바일 P2P 네트워크를 주로 사용
- CoAP 장치는 SSDP와 다르게 IP정보가 2주 이내에 80%이상 변경되는 특징이 있기 때문에 공격자 입장에서는 봇넷 구축을 위해 지속적으로 갱신해야 하는 단점이 있지만, 잘 알려지지 않은 유형의 DDoS 반사 공격이기 때문에 앞으로 더욱 발전될 가능성이 높음

PART 2 공격 유형 및 대응 방안

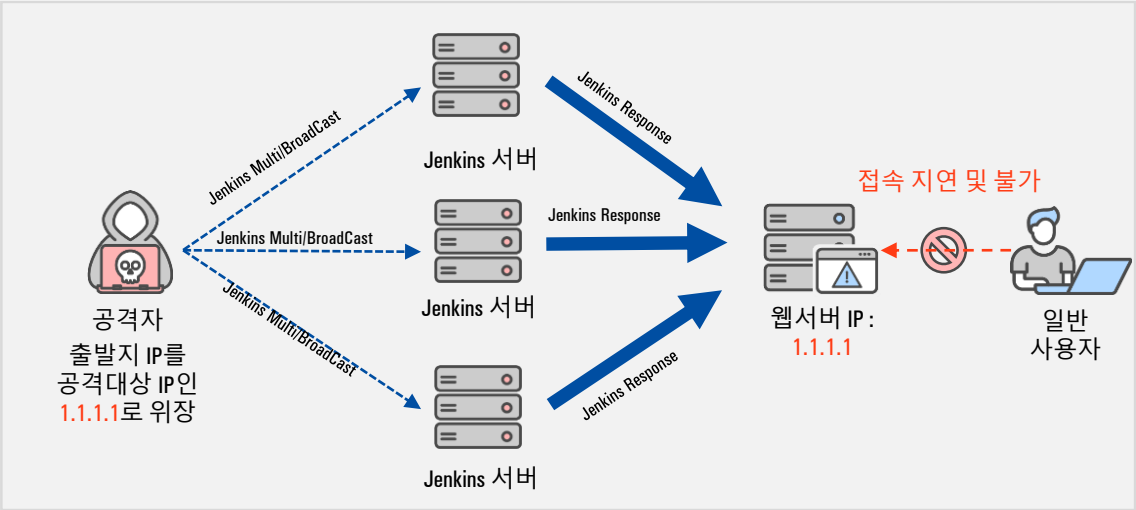
II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

9. Jenkins Reflection Attack

(1) Jenkins Reflection Attack개념

Jenkins란 소프트웨어 개발 시 지속적으로 통합 서비스를 제공해주는 툴이다. 다수의 개발자들이 하나의 프로그램을 개발할 때 발생할 수 있는 버전 충돌을 방지하기 위해 각자 작업한 내용을 공유 영역에 업로드 함으로써 지속적 통합을 지원해준다.

Jenkins가 DDoS로 악용 될 수 있는 원인은 취약버전에서 Jenkins 검색을 위해 사용되는 UDP 프로토콜(포트 33848번)의 요청을 검증없이 응답하기 때문이다. 자동 검색 프로토콜이 활성화된 상태에서 검색 요청 Packet을 받으면 요청 값에 관계없이 Jenkins 메타 데이터의 XML 결과값을 응답 한다. 이런 취약점을 통해 피해자의 IP로 스푸핑 한 후 검색 요청 Packet을 보낸다. 그 결과 XML 형식의 응답이 피해 시스템으로 전달되어 피해 시스템의 회선 대역폭을 고갈 시킨다.



Jenkins Reflection Attack 원리

(2) 공격원리

① 공격자는 사전에 외부에 노출된 취약한 Jenkins 서버 목록을 확보

② 피해자의 IP로 스푸핑한 후 확보한 Jenkins 서버들에게 자동검색 Packet을 요청

③ Jenkins 서버는 피해자 IP로 요청 받은 검색 Packet에 대한 증폭된 응답Packet을 전달함으로써 피해 시스템의 회선 대역폭을 고갈 시킴(증폭률 최대 100배)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

9. Jenkins Reflection Attack

(3) 대응방안

① UDP 패킷 차단설정

- Jankins Reflection Attack 패킷은 UDP 프로토콜을 사용하며 33848번을 출발지 Port로 사용
- Jenkins 자동 검색 서비스는 외부에 노출되지 않도록 설정해야 하기에 인입되는 UDP 프로토콜 중 출발지 Port를 33848번으로 사용하는 패킷(Jenkins Response Packet)에 대하여 차단하는 정책 설정

② 취약한 Jenkins 서버 조치

- Jenkins Reflection Attack은 취약한 Jenkins 버전(Jenkins 2.218이전 버전)에서 자동 검색 프로토콜이 자동 활성화 되어있기 때문에 발생함
- 따라서 자동 검색 프로토콜을 비활성화 하거나 Jenkins 버전을 2.219(자동 검색기능 비활성화 패치)로 업그레이드 해야 함

③ DDoS 대응 서비스 이용 검토

- Jenkins Reflection Attack은 방어 장비가 있어도 기업 네트워크 회선의 수용가능한 트래픽 양을 초과하면 결국 서비스 장애로 이어짐
- 따라서 Jenkins Reflection Attack의 효과적인 차단을 위해서는 기업 네트워크 회선에 공격 트래픽이 인입되기 전에 사전 차단하는 것이 가장 효과적임
- 이를 위해 DDoS 방어 서비스를 이용한 대응 프로세스를 준비해야 함

※ 기업의 네트워크 환경/공급자에 따라서 이용할 수 있는 DDoS 서비스가 다를 수 있으므로 이용 가능한 DDoS 서비스를 사전에 검토하여 대응 프로세스를 준비하는 것을 권장

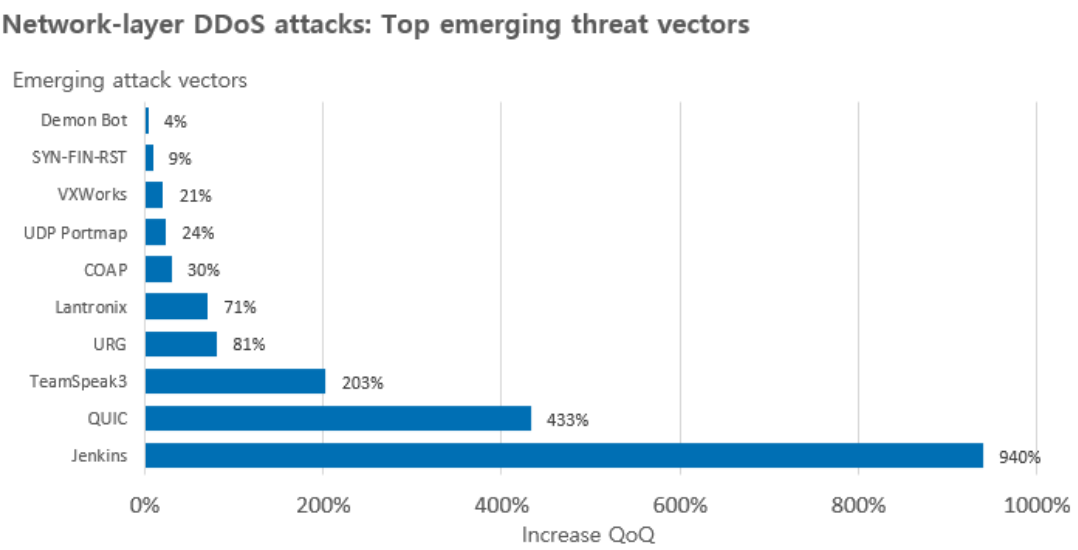
PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

9. Jenkins Reflection Attack

최근 동향

- Jenkins는 오래전부터 개발자들이 사용한 Tool 이지만 DDoS 위험요소가 언급된 것은 2020년 1월 Jenkins 취약점이 발견된 이후임
- 취약점 보안 패치를 2020년 1월 29일 게시했지만 패치가 적용되지 않은 취약서버들이 남아있기 때문에 공격 위험요소는 여전히 존재함
- CloudFlare 2021년 1분기 보고서에 의하면 Jenkins 기반 DDoS 공격이 2020년 4분기와 비교하여 약 940% 정도 크게 증가했다고 밝힘(아래 그림 참조)



2021년 1분기 L4 Layer DDoS 공격 유형 증가율
(출처: CloudFlare, DDoS attack trends for 2021 Q1)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

10. 기타 Reflection Attack

(1) SNMP Reflection Attack

① 내용

- SNMP(Simple Network Management Protocol) 장치들을 반사 기기로 악용한 공격으로서 UDP프로토콜을 사용하며 출발지 Port로 161번을 사용함

② 대응 방안

- 다른 반사공격들과 마찬가지로 회선 대역폭을 고갈시키는 공격이며, UDP 프로토콜을 사용하면서 161번을 출발지 Port로 사용하는 패킷을 최상단에서 차단

(2) Chargen Reflection Attack

① 내용

- Chargen 프로토콜은 네트워크를 통해 문자열을 생성하고 보내는 프로토콜로서, 반사공격에선 생성된 문자열을 payload로 활용함
- UDP 프토토콜을 사용하며 출발지 Port로 19번을 사용함

② 대응 방안

- 다른 반사공격들과 마찬가지로 회선 대역폭을 고갈시키는 공격이며, UDP 프로토콜을 사용하면서 19번을 출발지 Port로 사용하는 패킷을 최상단에서 차단

(3) SunRPC Reflection Attack

① 내용

- RPC(Remote Procedure Call) 프로토콜은 원격으로 함수를 호출하여 사용할 수 있게 하는 프로토콜로서 UDP 프로토콜 111번 Port를 사용하며 RPC mapper라는 서비스를 통해 이뤄짐
- SunRPC Reflection Attack은 RPC mapper를 악용하여 RPC mapper response 패킷을 피해시스템에게 보내 대역폭을 고갈 시킴

② 대응 방안

- 다른 반사공격들과 마찬가지로 회선 대역폭을 고갈시키는 공격이며, UDP 프로토콜을 사용하면서 111번을 출발지 Port로 사용하는 패킷을 최상단에서 차단

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

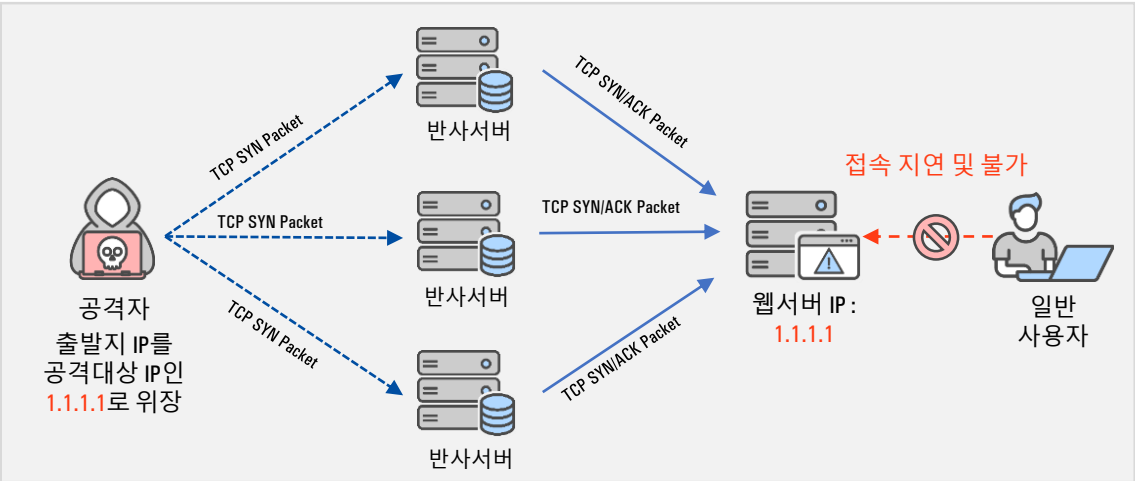
10. 기타 Reflection Attack

(4) SYN/ACK Reflection Attack

① 내용

- TCP 프로토콜을 사용한 반사 공격으로 UDP 프로토콜을 사용하는 대역폭 공격과 다르게 대규모의 SYN/ACK 패킷을 피해대상에게 보내서 서버의 리소스를 소모시키는 공격 방식
- 피해자의 IP로 스푸핑 한 후 반사서버를 향해 대규모의 SYN 패킷을 보내면 SYN 패킷에 대한 응답으로 SYN/ACK 패킷이 피해서버로 반사되어 전달되는 방식

※ SYN/ACK Reflection Attack 은 반사서버를 이용하여 트래픽을 유발하는 "대역폭 공격"이 아니고 대량의 SYN/ACK 패킷으로 웹서버의 부하를 유발하는 "자원 소진 공격" 형태임



SYN/ACK Reflection Attack 원리

② 대응 방안

- SYN/ACK Reflection Attack의 방어도 ACK Flooding을 차단하는 방법과 동일
- SYN/ACK Packet에 대해 일정시간에 정해진 임계치 이상으로 인입되는 IP가 확인될 경우 정해진 시간만큼 차단하는 정책 적용

(예시 - 동일 IP에서 1초에 1000개 이상의 ACK Packet이 인입될 경우 해당 IP를 차단)

PART 2 공격 유형 및 대응 방안

II. 대역폭 공격 (2) - DRDoS (Distributed Reflection Denial of Service)

10. 기타 Reflection Attack

※ 참고 : 유형별 반사공격 증폭률 (참조 : us-cert.cisa.gov, NSFOCUS)

프로토콜	포트번호 (UDP)	증폭률(배)
DNS	53	28 ~ 54
NTP	123	556.9
SNMPv2	161	6.3
NetBIOS	137	3.8
SSDP	1900	30.8
Chargen	19	358.8
QOTD	17	140.3
BitTorrent	6881	3.8
Kad	751	16.3
Quake Network Protocol	27960	63.9
Steam Protocol	27015	5.5
Multicast DNS (mDNS)	5353	2 ~ 10
RIPv1	520	131.24
Portmap(RPCbind)	111	7 ~ 28
LDAP	389	46 ~ 55
CLDAP	389	56 ~ 70
TFTP	69	60
Memcached	11211	10,000 ~ 51,000
WS-Discovery	3702	10 ~ 500
ARMS	3283	5 ~ 35.5
COAP	5683	10 ~ 50
Jenkins	33848	100

PART 2 공격 유형 및 대응 방안

III. 자원 소진 공격

1. SYN Flooding

(1) SYN Flooding 개념

SYN Flooding은 자원 소진 공격에 가장 대표적인 공격방식으로서 과거부터 현재까지 가장 많이 사용되는 공격방법이다.

TCP Protocol의 3-way-handshake[1]를 악용한 공격기법으로 SYN Flag만 지속적으로 전달하고 돌아오는 SYN/ACK 패킷에 대한 응답을 주지 않아서 피해 서버의 자원를 소모하게 만드는 공격기법이다.

bps에 비해 높은 pps를 보이는 것이 특징이며, 대역폭 공격과 다르게 대규모의 트래픽을 발생시키지 않아도 서비스 접속 불가를 유도할 수 있다.

(2) 공격원리

① 공격자는 사전에 다수의 좀비PC/단말(봇넷)을 확보한 후 피해서버에서 수신하고 있는 TCP Port를 스캔

② 확보한 봇넷을 사용하여 IP를 위/변조한 후 피해서버의 수신하고 있는 TCP Port를 향해 대규모의 SYN 패킷 전달

③ 피해서버는 좀비PC/단말 들이 요청한 SYN 패킷에 대한 응답으로 SYN/ACK 패킷을 좀비PC/단말 들에게 전달

④ 피해서버는 SYN/ACK에 대한 ACK응답을 기다리기 위해 SYN 연결을 지속적으로 Backlog Queue[2]에 저장하며 기다리는 상태가 됨

⑤ 공격자는 ACK 패킷을 보내지 않고 계속 SYN 패킷만 보내서 피해서버에서 가용할 수 있는 Backlog Queue를 전부 소모하여 정상 사용자 연결을 차단

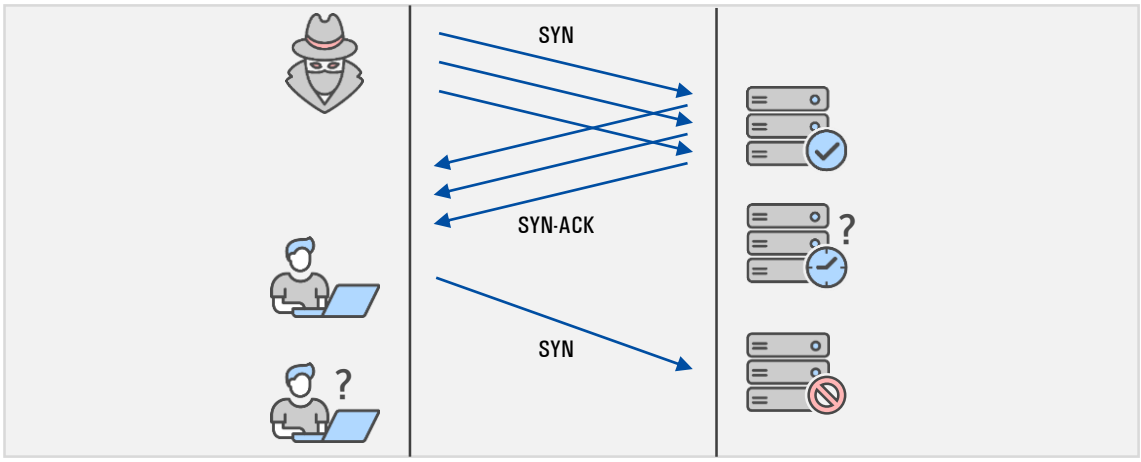
[1] 3-way-handshake : Client와 Server간 Session을 맺기 위하여 Syn–Syn/Ack–Ack 순서로 인증하는 방식

[2] Backlog Queue : TCP 세션을 맺기 위해 요청된 세션정보를 저장하는 공간

PART 2 공격 유형 및 대응 방안

III. 자원 소진 공격

1. SYN Flooding



SYN Flooding 공격 원리

(3) 대응 방안

① SYN Cookie 룰 적용

- SYN Packet 이후 보내는 SYN/ACK Packet의 sequence값에 임의의 Cookie값을 추가하여 대응하는 방법으로, 정상 3-way-handshake를 거치지 않으면 Backlog Queue를 소모하지 않도록 하는 차단 기법
- 방화벽이나 보안장비에서 설정하게 되면 서버까지 도달하는 SYN은 정상적으로 3-way-handshake를 맺은 Packet만 전달됨
- Centos에서 적용 시 sysctl –w net.ipv4.tcp_syncookies=1 명령어 사용

② TCP 연결유지 시간 조정

- 장시간 TCP Connection을 소모하게 만드는 패킷에 대하여 일정시간이 초과할 경우 세션을 끊어서 Backlog Queue를 확보하는 방어 기법
- 아래 1, 2(apache서버 설정)처럼 /etc/httpd.conf 또는 /etc/apache2/httpd.conf 파일에서 해당 설정을 적용

```
#
# Timeout: The number of seconds befo
#
Timeout 60
```

[예시1 connection Timeout 설정]

```
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of secc
# same client on the same connecti
#
KeepAliveTimeout 15
```

[예시 2 KeepAlive 설정]

PART 2 공격 유형 및 대응 방안

III. 자원 소진 공격

1. SYN Flooding

(3) 대응 방안

③ 임계치 기반 차단

- 대량의 SYN Packet을 유발하는 IP를 확인하여 임계치를 초과하는 IP 차단 설정

항목	기준 시간	임계치	차단 시간
TCP SYN Flooding	1초	120개	300초

예시 - 임계치 기반 차단 설정

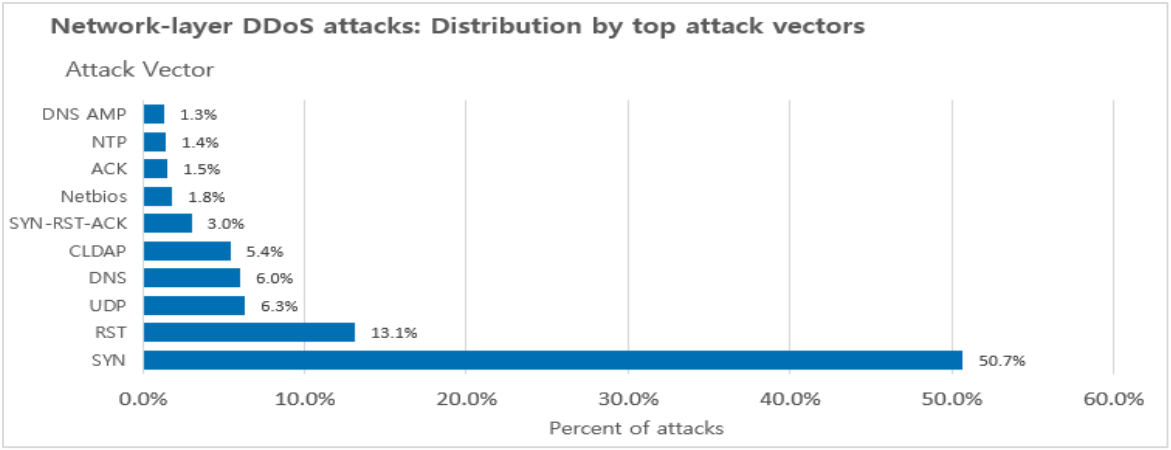
(1개의 IP에서 1초 동안 120개 이상의 SYN 패킷을 보낼 경우 해당 IP를 300초 동안 차단)

④ First SYN Drop 룰 적용

- 출발지 IP별 최초로 들어오는 SYN 패킷을 차단하는 설정
- 공격이 아닌 정상 접속은 첫 번째 SYN을 차단하더라도 SYN을 재전송하므로 동일 IP에서 두 번째 SYN 패킷은 정상 접속이 이루어지는 반면 출발지 IP를 스푸핑하는 공격 도구는 그렇지 않기 때문에 효과적으로 차단할 수 있음
- 첫 번째 SYN 패킷이 차단되었을 때 출발지에서 SYN 패킷을 바로 재전송하지 않을 경우에는 서비스 지연이나 장애가 발생할 수 있음(First SYN Drop 룰 적용 이전에 사전 검토)

최근 동향

- 최근 DDoS 공격 중 가장 많은 비중을 차지하고 있는 공격유형
- CloudFlare의 2021년 1분기 DDoS 보고서에 의하면 L4 Layer의 공격에서 가장 많은 비중을 차지함(아래 그림 참조)



2021년 1분기 L4 Layer 공격 유형 비율

(출처: CloudFlare, DDoS attack trends for 2021 Q1)

PART 2 공격 유형 및 대응 방안

III. 자원 소진 공격

2. ACK Flooding

(1) ACK Flooding 개념

ACK Flooding은 SYN Flooding과 유사하게 3-way-handshake의 특성을 악용한다. 다량의 ACK Packet을 피해대상에게 보내서 자원을 소모하게 만드는 공격기법이다.

피해서버는 ACK Packet을 수신하면 자신이 보낸 Packet에 대한 응답인지 확인하기 위해 서버의 컴퓨팅 성능을 많이 소모하게 되며, 결과적으로 정상 사용자들이 접속할 수 없게 된다.

SYN Flooding 과 동일하게 높은 pps를 보이며, IP 위/변조가 가능하다. 또한 DRDoS 형태로 공격이 가능하다는 특징이 있다.

(2) 공격 원리

① 공격자는 다수의 좀비PC/단말(봇넷)기기를 확보

② 공격자는 확보한 봇넷을 이용하여 피해자의 IP로 대규모 ACK Packet을 전달

③ 피해서버는 수신한 ACK Packet이 자신이 보낸 Packet에 대한 응답인지 확인하면서 서버 자원을 소모

④ 이 같은 과정이 대규모로 반복되면서 서버 컴퓨팅 성능을 소모하게 만들어서 정상 사용자들의 접속을 방해

PART 2 공격 유형 및 대응 방안

III. 자원 소진 공격

2. ACK Flooding

(3) 대응 방안

① 임계치 기반 차단

- 정해진 임계치 이상으로 유입되는 ACK packet에 대하여 요청IP를 확인 후 차단하도록 설정

항목	기준 시간	임계치	차단 시간
TCP ACK Flooding	1초	1000개	10초

[예시 - 임계치 기반 차단 설정]

(1개의 IP에서 1초 동안 1000개 이상의 ACK 패킷을 보낼 경우 해당 IP를 10초 동안 차단)

② 비정상 TCP Packet 차단

- 방화벽의 stateful inspection[1] 기능을 통해, 3-way-handshake 를 거치지 않고 발생하는 비정상적인 ACK Packet에 대해서 차단하도록 설정

[1] stateful inspection : Session 정보를 저장하고 추적하여 비정상 Packet을 차단할 수 있도록 지원하는 방화벽 기능

PART 2 공격 유형 및 대응 방안

III. 자원 소진 공격

3. DNS Query Flooding

(1) DNS Query Flooding 개념

DNS Query Flooding은 DNS서버에 대량의 DNS 질의를 보내서 정상 서비스를 할 수 없게 만드는 공격이다.

DNS 서버는 UDP 프로토콜 53번을 통해 도메인 정보에 대한 IP주소를 요청을 받으면 해당하는 IP값을 응답하는 역할을 한다.(반대 질의도 응답을 줄 수 있다.) 이런 서비스 구조를 이용하여 DNS서버로 단시간에 대량의 DNS 질의를 보내면 DNS서버는 요청한 DNS 질의에 대한 응답을 보내기 위해 자원을 소모하기 때문에 결과적으로 정상 사용자의 IP주소 질의에 대해서는 응답을 할 수 없게 된다.

(2) 공격 원리

① 공격자는 다수의 좀비PC/단말(봇넷) 및 피해 DNS서버에서 서비스하는 도메인 정보 확보

② 공격자는 확보한 봇넷들을 이용하여 확보한 도메인정보를 대량으로 질의함

③ DNS 리졸버 서버들은 질의한 도메인에 대한 응답을 받기 위하여 피해 DNS서버로 재질의함

④ 피해 DNS서버는 수신 받은 DNS의 응답을 주기 위해 소유한 영역정보를 확인하고 응답 줌

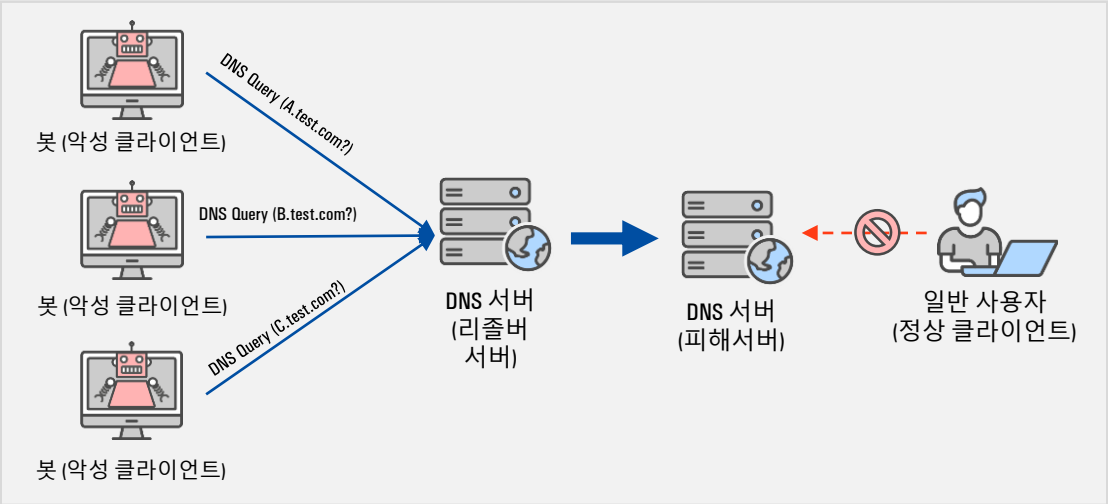
⑤ 이 같은 과정이 대규모로 반복되면서 DNS 서버 컴퓨팅 성능을 소모하게 만들어서 정상 사용자들의 DNS 질의를 방해함

PART 2 공격 유형 및 대응 방안

III. 자원 소진 공격

3. DNS Query Flooding

(2) 공격 원리



DNS Query Flooding 공격 원리

(3) 대응 방안

① 임계치 기반 차단

- 정해진 임계치 이상으로 유입되는 DNS 질의 packet에 대하여 요청IP를 확인 후 차단하도록 설정(※ 해당 임계치 설정을 위해선 평상 시 DNS Query 수준을 파악하고 있어야 함)

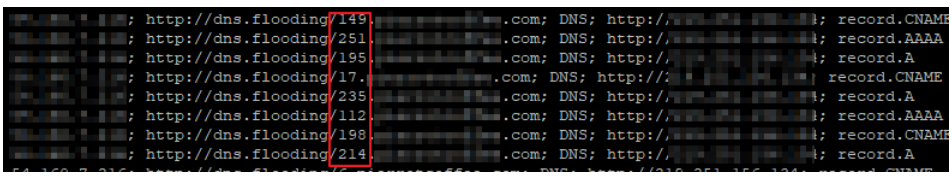
항목	기준 시간	임계치	차단 시간
DNS Query Flooding	1초	100개	10초

[예시 - 임계치 기반 차단 설정]

(1개의 IP에서 1초에 100개 이상의 DNS Query 패킷을 보낼 경우 해당 IP를 10초 동안 차단)

② 비정상 질의 패킷 차단

- 존재하지 않는 도메인에 대한 DNS 질의를 한다 거나, 도메인의 호스트 값만 랜덤하게 변경하여 대량으로 질의할 경우 해당 IP를 확인하여 차단하도록 설정



비정상 DNS Query Packet (샘플)

PART 2 공격 유형 및 대응 방안

Ⅳ.웹/DB 부하 공격

1. GET Flooding

(1) GET Flooding 개념

GET Flooding은 웹과 DB 부하 공격의 가장 대표적인 공격방식으로 최근에도 활발하게 이루어지고 있는 공격 방법이다.

공격자는 TCP Protocol의 3-way-handshake를 통해 서버와 세션을 맺은 후, HTTP GET 메소드 요청을 통해 웹서버의 자원을 소진함과 동시에 DB서버까지 자원을 소진 시켜서 정상적인 사용자의 웹서비스 이용을 차단한다.

자원 소진 공격과 유사하게 bps에 비해 높은 pps를 보인다. 정상 요청과 유사한 요청을 보이기 때문에 사전 대비가 어렵고 적은 개수의 좀비PC/단말로도 서비스 장애를 유도 할 수 있다는 특징이 있다.

(2) 공격 원리

① 공격자는 다수의 좀비PC/단말(봇넷)을 확보한 후 공격 대상 웹서버의 HTTP 혹은 HTTPS Port를 확인

② 공격자는 확보한 봇넷으로 공격대상 웹서버와 3-way-handshake를 통해 세션을 맺음

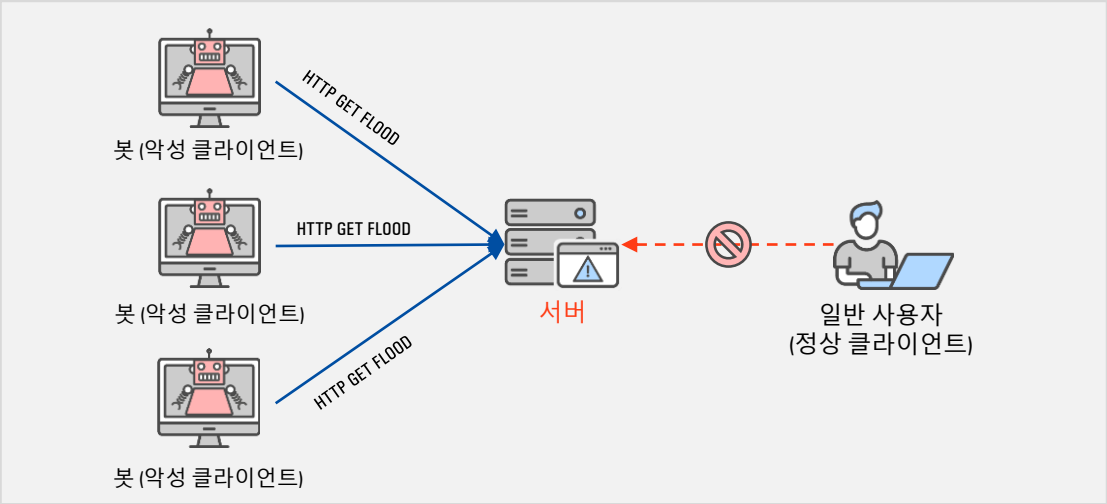
③ 세션을 맺은 후 피해 웹 서버의 특정 페이지 혹은 데이터를 요청하는 GET Request를 대량으로 요청

④ 웹/DB서버에서는 요청에 대한 응답을 주기 위해 자원을 소모하여 정상 사용자는 접속할 수 없는 상태가 됨

PART 2 공격 유형 및 대응 방안

IV.웹/DB 부하 공격

1. GET Flooding



GET Flooding 공격 원리

(3) 대응 방안

① 웹서버에 존재하지 않는 URL을 과다 요청

- 서버 상태코드 중 4xx(잘못된 요청)를 유발시키는 악성 클라이언트를 식별하여 차단 IP로 설정
- 임계치 기반 차단 룰을 적용하여 단시간에 대량의 Request를 보낸 악성 클라이언트를 식별, 차단

② 웹서버에 존재하는 URL을 과다 요청(Case를 나눴지만 차단 방식은 동일)

Case 1. 동일한 URL을 대량으로 요청하는 경우

- 요청이 많은 URL에 임계치 차단 룰을 적용시키고 임계치를 초과한 악성 클라이언트 IP를 차단
- 클라이언트 요청에 쿠키 값을 추가하여 응답을 보낸 후, 보낸 쿠키 값을 포함하지 않은 응답은 비정상 사용자로 판단하여 차단

Case 2. 다른 URL을 대량으로 요청하는 경우

- 클라이언트 요청에 쿠키 값을 추가하여 응답을 보낸 후, 보낸 쿠키 값을 포함하지 않은 응답은 비정상 사용자로 판단하여 차단
- 클라이언트의 요청에 Javascript를 추가하여 응답을 보낸 후, 클라이언트에서 실행한 Javascript의 결과값이 서버에서 보유한 결과값과 다를 경우 비정상 사용자로 판단하여 차단

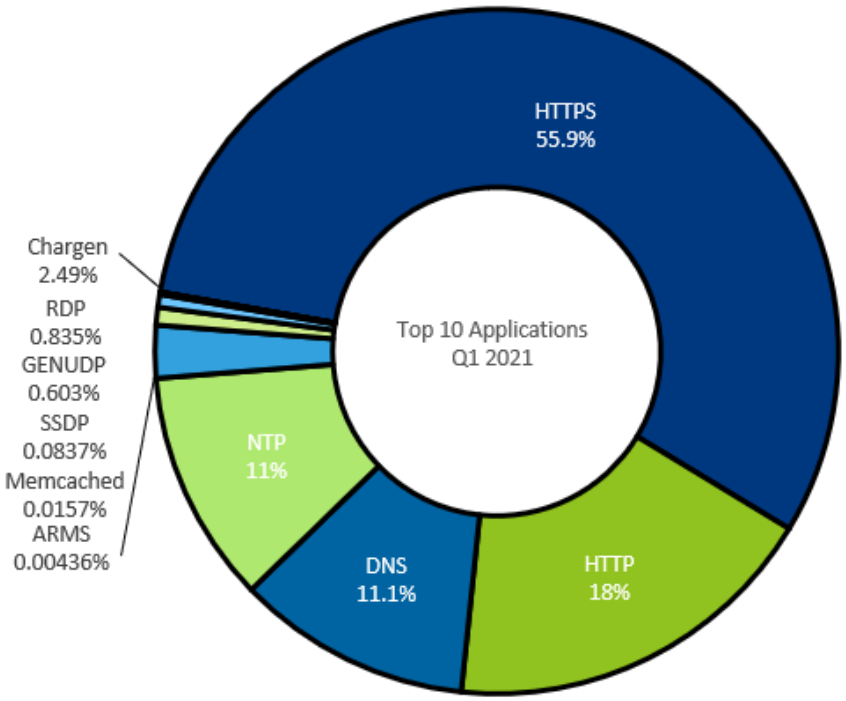
PART 2 공격 유형 및 대응 방안

IV.웹/DB 부하 공격

1. GET Flooding

최근 동향

- GET Flooding은 어플리케이션 공격에서 가장 대표적인 공격유형
- 최근 GET Flooding은 보안장비를 우회하기 위해 HTTPS(443번 Port)를 사용하여 공격하는 방식이 증가하고 있음
- 2021년 글로벌 DDoS 방어 업체인 Radware 보고서에 의하면 어플리케이션 공격에서 HTTP 공격이 18%인 반면, HTTPS 기반 공격은 55% 비율을 차지한 것으로 나타남(아래 그림 참조)



2021년 1분기 공격 유형

(출처: Radware, Quarterly DDoS Attack Report)

PART 2 공격 유형 및 대응 방안

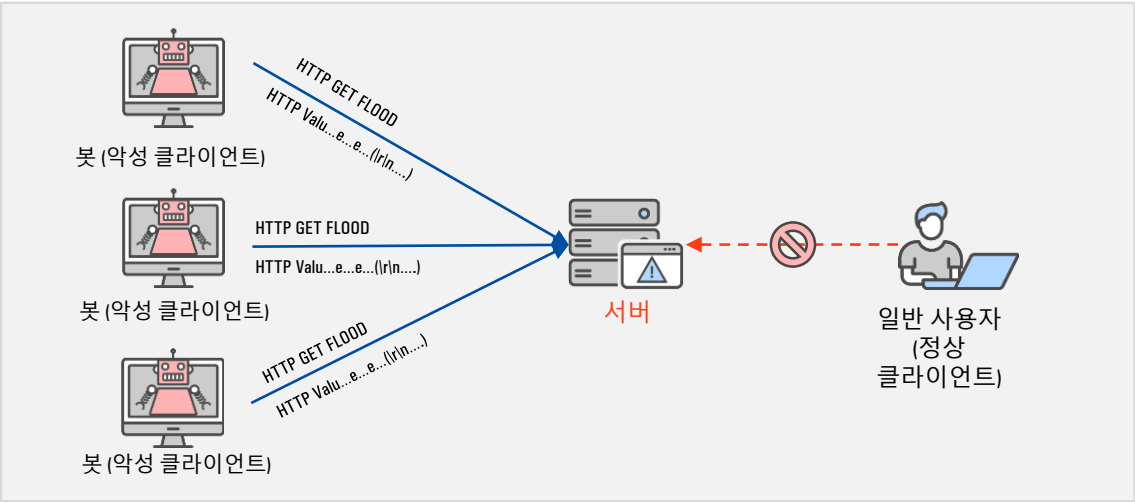
Ⅳ.웹/DB 부하 공격

2. Slowloris Attack

(1) Slowloris Attack 개념

Slowloris Attack은 GET Flooding에 비해 상대적으로 규모가 작은 공격이다. HTTP GET 메소드 요청과 유사하지만 단시간 내 폭발적으로 요청하는 공격이 아니라 오랜 시간 동안 지속적으로 공격을 수행한다는 차이점이 있다.

정상적인 HTTP 패킷의 헤더는 Carriage Return & Line Feed(이하 개행 문자)가 두 번 나타난다. 첫 번째 개행 문자는 헤더의 종료이며 두 번째 개행 문자는 전체 헤더의 종료를 의미한다. 만일 헤더의 마지막에 개행 문자를 하나만 전송하면 웹서버는 헤더가 모두 도착하지 않은 것으로 간주하고 연결을 유지하며 대기상태를 유지한다. 즉, 지속적인 공격으로 서버의 자원을 잠식하는 공격이다.



Slowloris Attack 원리

(2) 대응 방안

① Session Timeout 설정

- 웹서버에서 클라이언트와 Timeout 설정 값을 조절하여 일정시간동안 Session을 유지하고 있는 요청을 차단하는 설정 적용

② 시그니처 차단

- GET 요청의 개행 문자(\r\n)가 두 번 반복되지 않고 한번만 표시되는 패킷을 시그니처로 등록하여 차단

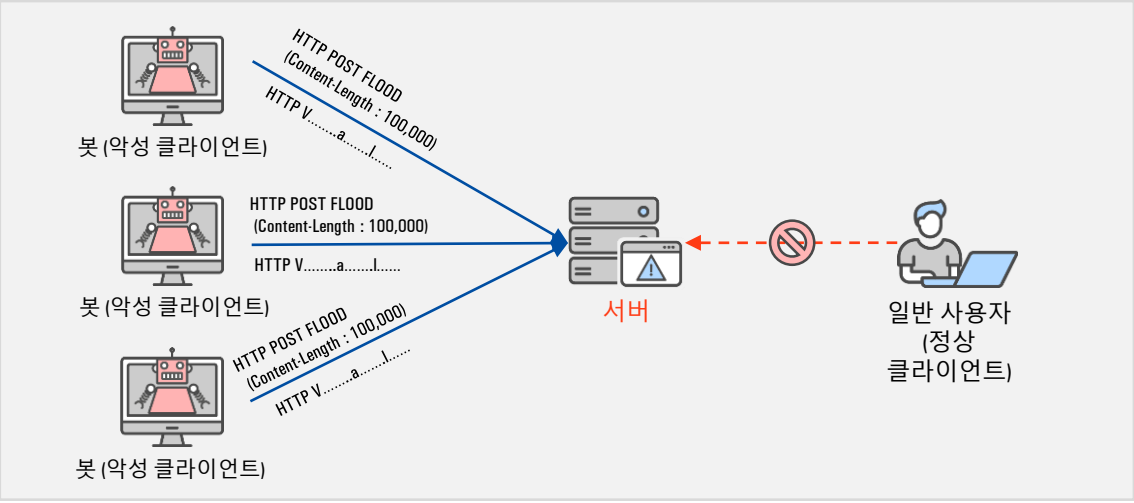
PART 2 공격 유형 및 대응 방안

Ⅳ.웹/DB 부하 공격

3. RUDY Attack

(1) RUDY Attack 개념

RUDY(R-U-Dead-Yet) Attack이란 POST Method를 이용하는 대표적인 Slow 공격 유형이다. POST 요청은 전달할 데이터의 크기를 Content-Length 헤더에 삽입하여 보내게 되는데, RUDY Attack은 이 크기를 매우 크게 설정한 후 서버로 전달할 데이터를 장시간에 걸쳐 조금씩 분할하여 전달하게 한다. 그렇게 되면 서버는 아직 모든 데이터가 수신되지 않았다고 판단하여 장시간 연결을 유지하게 되며 결과적으로 정상 사용자들의 요청을 서비스할 수 없게 된다.



RUDY Attack 원리

(2) 대응 방안

① Content-Length 확인 및 임계치 설정

- Content-Length 및 실제 인입 Packet Size를 임계치로 설정하여 차단(Content-Length가 설정한 크기보다 큰 POST 패킷이 인입될 때 지정된 시간동안 지정한 크기 이하의 패킷이 n개 이상 확인될 경우 차단하도록 설정)

② Session Timeout 설정

- 일정시간 이상동안 연결을 유지하고 있는 요청을 차단하는 설정 적용 (Session Timeout = 60초 : 60초 이상 지속적으로 연결을 유지하고 있는 세션 종료 및 IP 차단)

PART 2 공격 유형 및 대응 방안

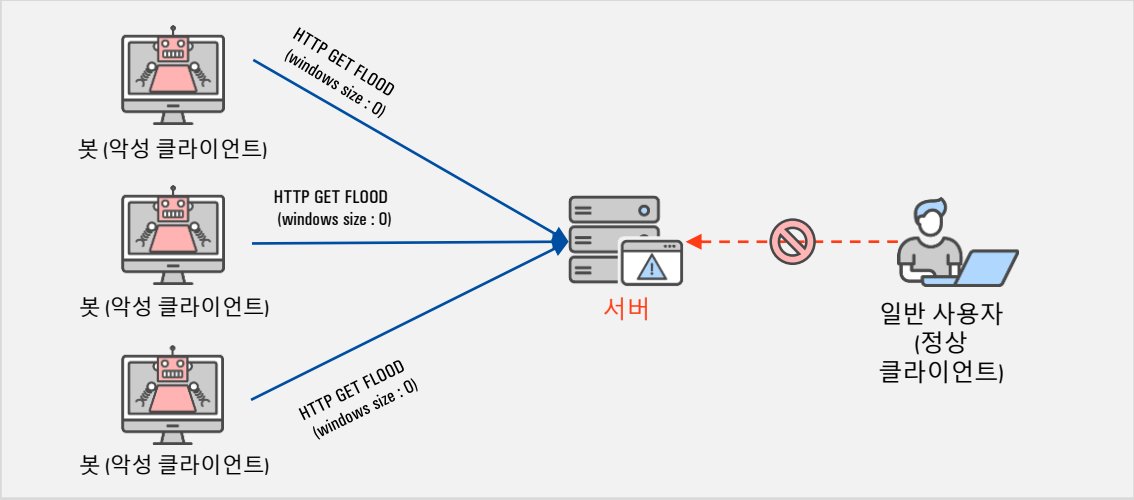
Ⅳ.웹/DB 부하 공격

4. Slow read Attack

(1) Slow read Attack 개념

Slow read Attack은 TCP 통신에서 사용되는 windows size를 악용한 공격기법이다. Client마다 한번에 처리할 수 있는 패킷의 크기가 다르기 때문에 해당 크기를 windows size 필드를 통해 전달하며, windows size를 기준으로 패킷을 주고받게 된다.

Slow read Attack은 windows size를 낮게 설정하여 서버로 전달하고, 해당 size를 기준으로 통신하면서 데이터 전송이 완료될 때 까지 Connection을 유지하게 만들어 서버의 Connection 자원을 고갈시키는 공격이다.



Slow read Attack 원리

(2) 대응 방안

① 비정상적 windows size Packet 차단

- 지속적으로 windows size를 비정상적으로 낮게 설정하여 보내는 패킷이 확인될 경우 차단 (windows size = 0byte 패킷이 일정시간동안 지정된 임계치 이상 인입될 경우 connection 종료 후 IP 차단)

② Session Timeout 설정

- 일정시간 이상동안 연결을 유지하고 있는 요청을 차단하는 설정 적용 (Session Timeout = 60초 : 60초 이상 지속적으로 연결을 유지하고 있는 세션 종료 및 IP 차단)

PART 3

대응 프로세스

I. DDoS 예방대책

II. DDoS 방어대책

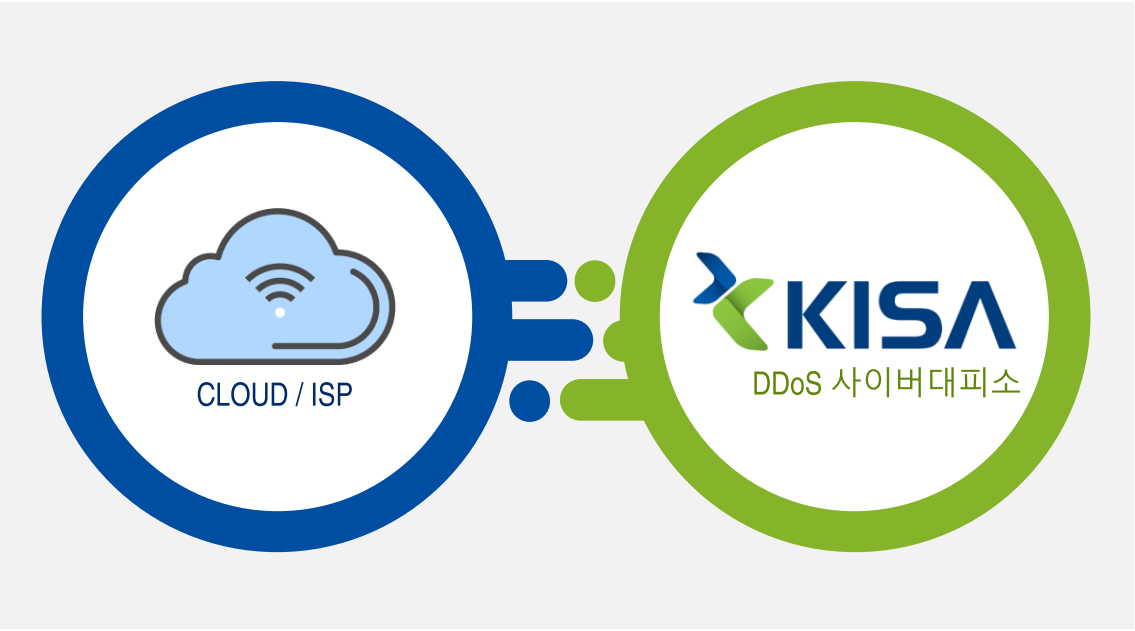
PART 3 대응 프로세스

I. DDoS 예방대책

1. DDoS 대응 서비스 가입

1Gbps 이상의 대규모 DDoS 공격을 대응하기 위한 자체 인프라 구축에는 인력과 비용 측면에서 현실적인 한계가 생긴다. 보다 효과적인 대응을 위해서 인터넷 회선 제공업체(ISP)나 클라우드 서비스에서 제공하는 DDoS 방어서비스를 이용하는 것을 권장한다.

또한 중소기업은 한국인터넷진흥원에서 제공하는 사이버대피소[1] 서비스를 이용 할 수 있다.



대규모 DDoS 공격 대응 서비스

[1] 사이버대피소: 한국인터넷진흥원에서 중소기업을 대상으로 DDoS공격을 방어해주는 서비스 https://www.boho.or.kr/webprotect/samCompany.do 에서 온라인 신청 가능

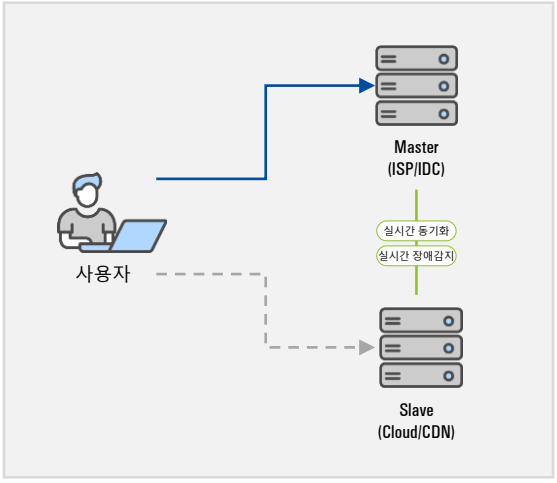
PART 3 대응 프로세스

I. DDoS 예방대책

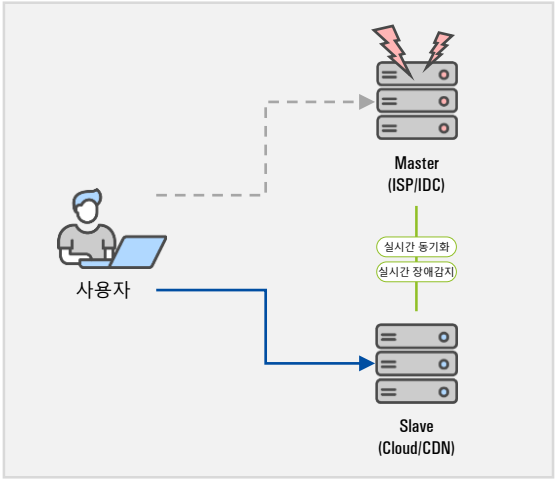
2. 백업 서버 구축

DDoS 공격에 의한 서버 장애를 대비하여 중요서버들은 서로 다른 회선에 이중화 구성을 해야 한다. 서로 다른 회선을 이용해서 이중화를 구성하면 Master 서버의 회선에 DDoS 공격으로 인한 장애가 발생해도, 다른 회선에 있는 Slave 서버가 동작하여 서비스 장애를 최소화 할 수 있다.

※ 구성예 : Master Server → ISP 회선사업자 혹은 IDC, Slave Server → Cloud 혹은 CDN



일반 접속 시
(Master 서버로 접속)



Master 서버 장애 발생 시
(Slave 서버로 접속)

PART 3 대응 프로세스

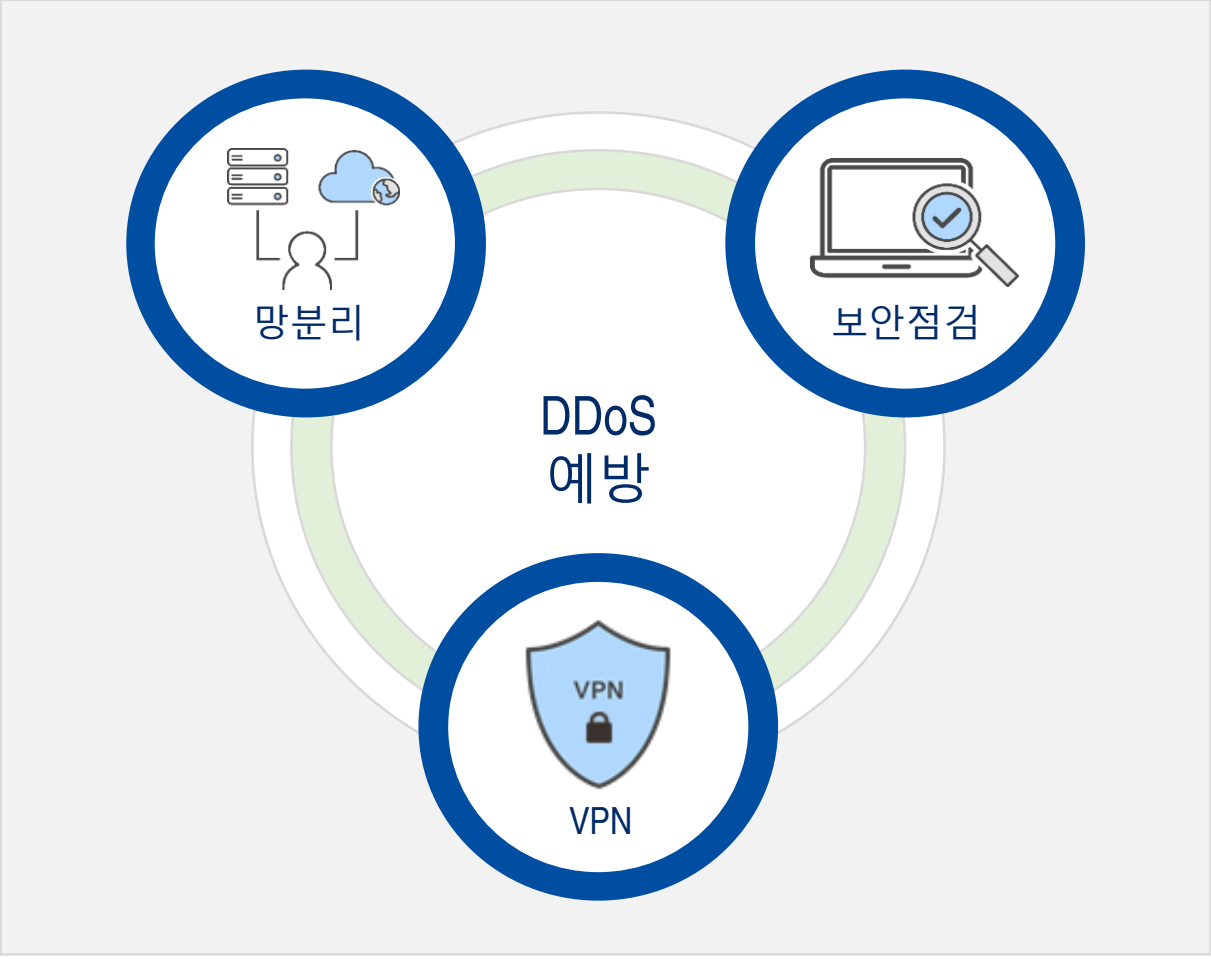
I. DDoS 예방대책

3. 공격 대상의 최소화

외부에 노출된 웹 서비스 외 기업 내부용 서버는 외부에 노출되지 않도록 내부망으로 망 분리 조치 후 운영한다.

내부용 서버는 DDoS 공격 및 기타 사이버 공격을 예방하기 위해 기업의 내부 서버 IP 및 서비스가 외부에 OPEN 되어 있는지 주기적인 스캐닝을 시행하고, Shodan 또는 다크웹 노출여부를 확인한다.

외부에서 부득이하게 내부망으로 접속이 필요할 경우에는 DDoS 대응 및 방어 설정이 가능한 가상 사설망(VPN)등의 별도 서비스를 이용한다.



공격 대상을 최소화하기 위한 요소

PART 3 대응 프로세스

II. DDoS 방어대책

1. 개요

DDoS를 대응하기 위한 방어대책으로는 자체적으로 방어를 대비하는 방법과 DDoS 방어서비스를 제공하는 업체를 이용하는 방법으로 나뉜다.

자체 방어준비

- 1. TCP 기반 DDoS 방어준비
- 2. 이상 트래픽 모니터링
- 3. WhiteList 방식 보안설정
- 4. 서버분산을 통한가용성확보

DDoS 대응 서비스를 통한 방어준비

- 0 단계 – 사 전 준 비
- 1 단계 – 공 격 인 지
- 2 단계 – 공격 정보 파악
- 3 단계 – 방어서비스 적용
- 4 단계 – 서비스 모니터링
- 5 단계 – 사 후 조 치

PART 3 대응 프로세스

II. DDoS 방어대책

2. 자체 방어 준비

충분한 회선용량과 DDoS 방어장비가 없다면 서버 가용량 이하의 소규모 공격에 한해서만 일부 방어가 가능하다.

① TCP 기반 DDoS 방어준비

- TCP 계열의 DDoS 공격을 방어하기 위해 방화벽 및 Proxy Server와 같은 주변장치에서 "TCP Keepalive" 및 "최대연결"을 설정하여 SYN Flooding등과 같은 공격을 방어할 수 있도록 준비

② 이상 트래픽 모니터링

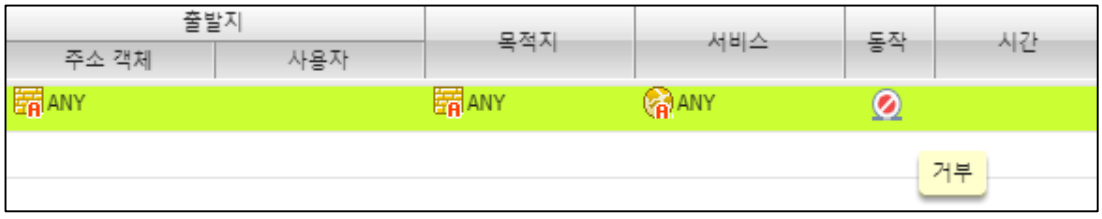
- 평시 발생하는 기본 트래픽(bps, pps, 동시 접속 수)정보를 인지하고, 이상 트래픽의 발생을 주기적으로 모니터링 해야함
- 비정상적인 트래픽 증감이 확인될 경우 웹 로그(Access Log) 또는 기타 보안장비에서 확인할 수 있는 트래픽 로그를 확인하여 이상 유무를 식별

  예시) 미사용 URL로 분당 100회 이상 GET 요청이 지속적으로 발생하면 GET Flooding으로 의심

Whitelist 방식의 방화벽 설정

- 필요한 서비스에 대한 최소한의 정책만 Open하고 모든 프로토콜과 Port를 차단(All Deny) 하는 설정을 통해 기타 포트로 들어오는 공격에 대한 방어 가능

  ※ 단, 서비스하고 있는 모든 Port에 대한 정보를 반드시 알고 있어야 함



예시 Whitelist 기반 방화벽 설정

④ 서버 분산을 통한 가용성 확보

- Load Balancer를 이용하여 서버 부하를 분산함으로써 서버 장애를 최소화할 수 있음

PART 3 대응 프로세스

II. DDoS 방어대책

3. DDoS 대응서비스를 통한 방어준비

충분한 회선용량과 DDoS 대응장비가 없어서 자체적으로 방어가 어렵다면, 전문 방어서비스를 이용하는 프로세스를 수립하여 공격발생 시 즉각 대응할 수 있도록 숙달한다.

(1) 0단계 – 사전준비

- DDoS 공격상황에 즉시 적용할 수 있는 방어서비스를 알아보고, 적용 절차 및 시간 등을 미리 파악해야 한다.
- 담당자 직통번호 및 긴급연락망을 확보하고, 방어서비스 적용 프로세스를 사전에 시뮬레이션 하면서 방어서비스 적용 설정과 실제 설정에 대한 정보를 최신화한다.

(2) 1단계 – 공격인지

- 웹 사이트 헬스체크 등의 모니터링 시스템을 구축하여 주기적으로 모니터링을 수행하고, 사이트의 이상정보 탐지 시 DDoS 공격에 의한 현상인지 서버 자체 원인인지 파악한다.

(3) 2단계 – 공격 정보 파악

- DDoS 공격으로 판단될 경우 해당 공격의 정보(유형, 규모, 시간 등)를 파악해야 한다.
- DDoS 공격유형은 크게 앞서 말한 ①대역폭 공격, ②자원 소진 공격, ③웹/DB부하 공격으로 나뉘며, 각각의 특성에 맞게 공격정보를 신속히 파악하여 대응한다.

PART 3 대응 프로세스

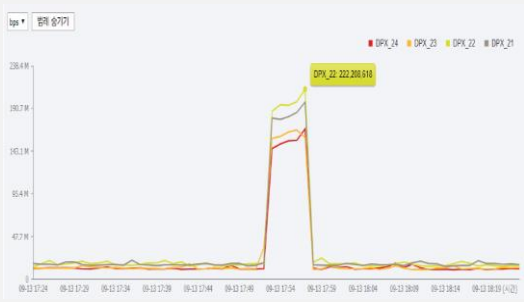
II. DDoS 방어대책

3. DDoS 대응서비스를 통한 방어준비

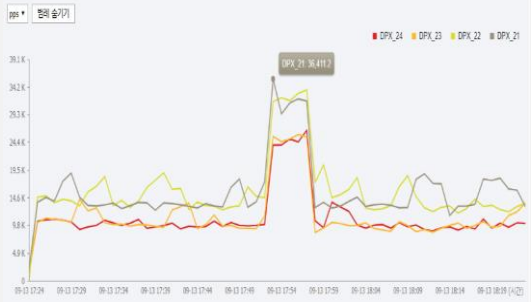
(3) 2단계 – 공격 정보 파악

① 대역폭 공격

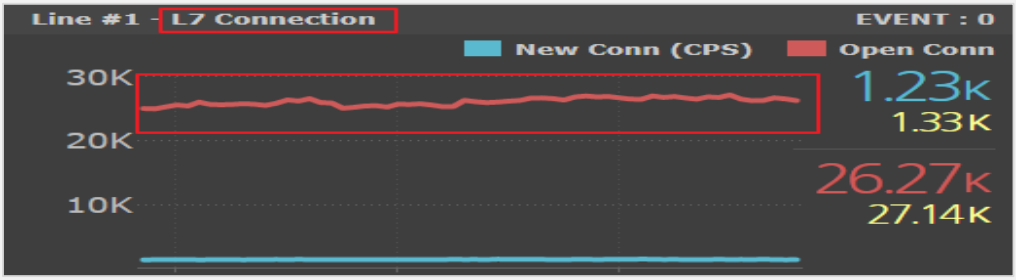
- 대역폭 공격이란 회선 대역폭의 가용량을 가득 채워 정상사용자가 통신하지 못하게 만드는 DDoS 공격 유형이다.
- 대역폭 공격은 평시보다 bps, pps는 높지만 Connection(동시 접속 수)값은 변동사항이 없다는 특징이 있다.
- 위 특징의 이유는 대역폭 공격으로 사용되는 DDoS 공격들은 주로 UDP 프로토콜을 사용하기 때문이다. UDP 프로토콜 공격은 Connection을 맺지 않고 단순히 과도한 트래픽만 발생시키는 특징이 있기 때문이다.



예시1 대역폭 공격 bps



예시2 대역폭 공격 pps



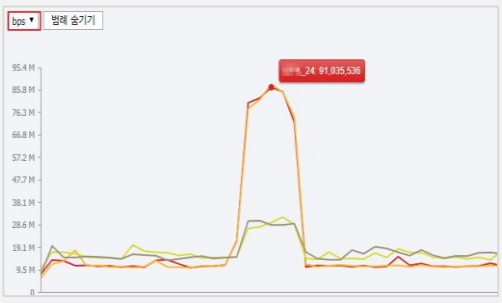
예시3 대역폭 공격 동시 접속 수

- 예시 1, 2와 같이 대역폭 공격이 발생하면 bps, pps 트래픽이 크게 증가한다.
- 반면에 예시 3과 같이 Connection(동시 접속 수)은 변동사항이 없는 현상이 나타난다.

PART 3 대응 프로세스

② 자원 소진 공격

- 자원 소진 공격은 대역폭 공격 대비 bps가 높지 않지만 pps가 높다는 특징이 있다.
- 따라서 평시 트래픽 대비 pps만 급증한다면 자원 소진 공격을 의심해 볼 수 있다.
- 정확한 공격식별을 위해 네트워크 트래픽을 확인/분석할 수 있는 장비 혹은 도구(wireshark[1], tcpdump[2] 등)를 이용한다.
- 자원 소진 공격은 주로 TCP 프로토콜을 사용하며 SYN Flooding, SYN/ACK Flooding등의 공격기법을 사용한다.
- 따라서 평소보다 많은 SYN, ACK Packet이 확인될 경우 자원 소진 공격으로 의심할 수 있다.



예시4 자원 소진 공격 bps

예시5 자원 소진 공격 pps

Time	Source	Destination	Protocol	Length	Frame	Info
1 0.000000	[redacted]1.232	[redacted].118	TCP	66	Yes	63225 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2 0.634252	[redacted].129	[redacted].118	TCP	62	Yes	3261 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1000 SACK_PERM=1
3 0.731221	[redacted].27	[redacted].118	TCP	62	Yes	36339 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
4 0.853070	[redacted].251	[redacted].118	TCP	62	Yes	3778 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
5 1.310400	[redacted].232	[redacted].118	TCP	66	Yes	63230 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6 1.397817	[redacted].74	[redacted].118	TCP	62	Yes	58746 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1408 SACK_PERM=1
7 1.489394	[redacted].151	[redacted].118	TCP	62	Yes	3934 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

예시6 자원 소진 공격 SYN Packet 샘플

- 예시 4,5와 같이 bps, pps가 높게 확인되지만 대역폭 공격에 비해 bps가 낮다.
- 해당 시간대의 인입 트래픽을 확인해볼 때 예시 6 처럼 대량의 SYN Packet이 확인된다면 SYN Flooding으로 판단할 수 있다.

[1] wireshark: 오픈소스 트래픽 분석도구
[2] tcpdump: 리눅스 기반의 오픈소스 트래픽 분석도구

PART 3 대응 프로세스

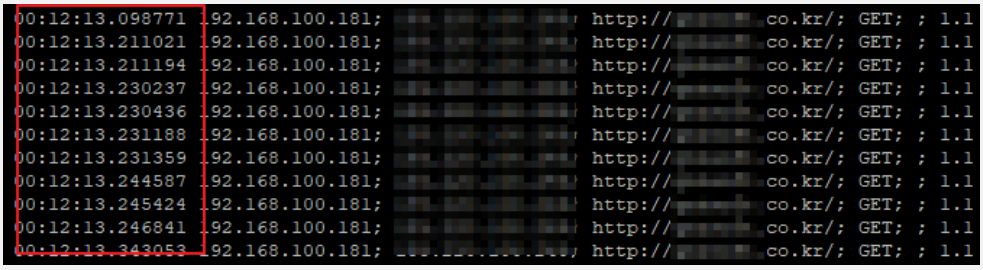
II. DDoS 방어대책

3. DDoS 대응서비스를 통한 방어준비

(3) 2단계 – 공격 정보 파악

③ 웹/DB 부하 공격

- 웹/DB 부하 공격은 다량의 HTTP 요청을 통해 웹서버와 DB서버 연동에 부하를 유발하는 공격으로 Connection 수치가 높은 것이 특징이다.
- Connection수가 급증하면 wireshark 및 웹 서버 Access Log등을 확인, 원인을 파악해야 한다.
- 웹/DB 부하 공격의 대표적인 공격유형은 GET Flooding 공격으로, 과도한 GET 요청을 보내 웹서버의 부하를 유발하는 공격이다.
- 평시 대비 과도한 HTTP 요청이 확인되거나, 비정상적인 HTTP 요청이 확인될 경우 GET Flooding 공격으로 판단하여 차단한다.



예시 7 (샘플)웹 로그 (Access Log)

- Connection(동시 접속 수)값이 증가하며, Access Log에서 위 예시7과 같이 평시 트래픽 대비 짧은 시간대에 대량의 GET 요청이 발생할 경우 GET Flooding으로 판단할 수 있으며 요청IP를 차단해서 대응할 수 있다.

PART 3 대응 프로세스

II. DDoS 방어대책

3. DDoS 대응서비스를 통한 방어준비

(4) 3단계 - 방어서비스 적용

- DDoS 공격에 의한 서버장애가 확실할 경우 '0단계' 에서 구축한 방어서비스 적용 프로세스를 수행하여 신속하게 대응할 수 있도록 조치해야 한다.

※ DDoS 공격이 빈번하거나 중요한 서비스일 경우에는 공격이 발생 이전 시점부터 방어서비스를 적용하여 운영할 수도 있다.

(5) 4단계 – 서비스 모니터링

- DDoS 공격은 차단되었으나 이미 점유된 세션 혹은 서버 부하로 인해 서비스 복구가 느려질 수 있다.
- 따라서 DDoS 공격을 차단한 이후 서비스 및 장비 모니터링을 통해 이미 유입된 공격에 의한 장비 상태를 확인하여 조치해야 한다.

(6) 5단계 – 사후조치

- DDoS 공격이 종료된 후 공격을 받은 시스템을 다시 한번 점검하여 특이사항이 없는지 확인해야 한다.
- 공격 대응 프로세스를 보완하여 추후 발생할 수 있는 DDoS 공격 피해를 대비해야 한다.

DDoS 공격 대응 가이드

KISA 한국인터넷진흥원

발 행 일 2021년 8월
발행 및 편집 한국인터넷진흥원 인터넷침해대응센터
주 소 서울시 송파구 중대로 135 IT벤처타워

☞ **해킹•스팸개인정보침해 신고 118, 디도스 사이버대피소 이용 문의 02-405-4769**