Anti-DDoS 솔루션

kt 클린존 서비스 소개자료

2023. 12

Contents

1. DDoS 공격 침해사례(1)

수년간 국내외적으로 공공 및 금융기관 전반에 대용량 DDoS 공격에 의한 침해사고가 주기적으로 발생하고 있으며, 최근에는 기업/공공/금융기관을 대상으로 지속적으로 공격을 반복하고 있습니다.

한국 금융기관대상 DDoS공격 협박

- 해킹단체 'Armada Collective' 에서 국내 다수 금융회사를 대상으로 SYN Flooding, NTP 등 DDoS(디도스) 공격
- 공격을 멈추기 위해 비트코인을 요구하는 협박메일을 발송

연합뉴스 2017-06-21

국내 은행 7곳 디도스공격 협박받아…" 26일까지 비트코인 보내라"

국제 해킹그룹 아르마다 콜렉티브(Armada Collective)는 국내 시중은행 7곳에 이메일을 보내서 26일까지 비트코인을 보내지 않으면 디도스 공격을 가하겠다고 협박

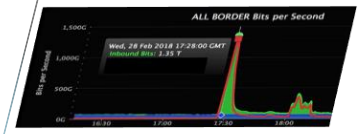
공격은 때때로 1초당 1TB에 달할정도로 강력할 것으로 주장

역사상 가장 큰 규모의 DDoS 공격 받은 Github

- 일반적으로 알려진 DDoS 공격기법이나 대규모 봇넷과는 다른 방식으로 이루어짐
- 사이버 공격이 점점 진화하고 규모가 커지고 있다는 것을 알려주는 사례

ZDNet Korea 2018-03-16

소스공유 사이트 깃허브, 최대 DDoS 공격 당해



1초당 1.35Tbps 규모의 DDoS 공격을 받아 10분가량 운영장애 발생

국내 기업/공공/금융기관 대상 DDoS 공격

- 최근 3년간 DDoS공격 10배 증가 및 금전 요구 협박성 공격 지속 발생
  - 10Gbps~40Gbps의 대역폭 공격이 대다수

유선 인터넷망 등 5차례 DDoS 공격받은 L통신사

- 23.1월~2월 L통신사 DDoS공격 발생('5차례 공격발생)

東亞日報 2017-06-21

L사 디도스 공격으로 하루 두차례 인터넷 서비스 차질

L사의 초고속인터넷 서비스에 대해 해킹 공격으로 추정되는 장애가 하루에만 두 차례 발생해 이용자들이 불편을 겪었다. 29일 L사에 따르면 이날 오전 2시56분부터 약 19분 간, 오후 5시58분경부터 약 22분 간 초고속인터넷 가입자들의 유선 인터넷과 와이파이 접속이 끊기는 현상이 나타났다.

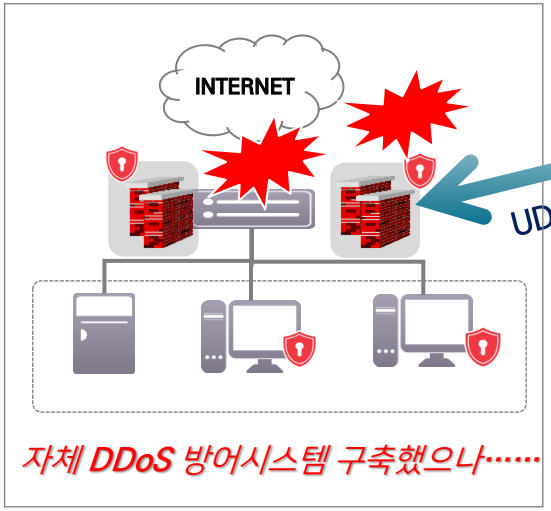
국내 다수 PC방 포함 기업 대상 DDoS 공격

- 22.8월 국내 다수 PC방 대상 공격으로 생계 위협 폐업 속출
- 2020년 603건, 2021년 640건, 2022년 944건 등으로 매년 증가 추세

1. DDoS 공격 침해사례(2)

자체 DDoS 방어시스템을 구축했지만 대역폭 고갈 공격으로 1차 전산마비로 서비스 불가 피해와
2차 악성 코드 활용한 고객정보 탈취 및 배포 협박 등 금품 요구로 막대한 금전적 피해 발생

OO社(클린존 미가입 고객)



자체 DDoS 방어시스템 구축했으나……

대역폭 고갈 공격

UDP, ICMP Flooding 공격 5회 발생

외부해킹

1차 피해

전산마비로 온라인 중단

앱/홈페이지 3시간 넘게 접속 안 돼 시민들 불편…… 복구 중

2차 피해

악성코드 활용 고객정보 탈취

고객정보 유출 미끼로 금품 요구 등 금전적 피해 발생

A 홈쇼핑
1Tbps 이상 공격
인터넷 쇼핑몰과
모바일 앱 마비
(80억원 이상 피해)
'22.1

B 은행
2Tbps 이상 공격
인터넷/모바일 뱅킹,
상담센터 등 마비
(160억원 이상 피해)
'22.2

C 증권사
500Gbps 이상 공격
온라인 주식거래
시스템 마비
(45억원 이상 피해)
'22.3

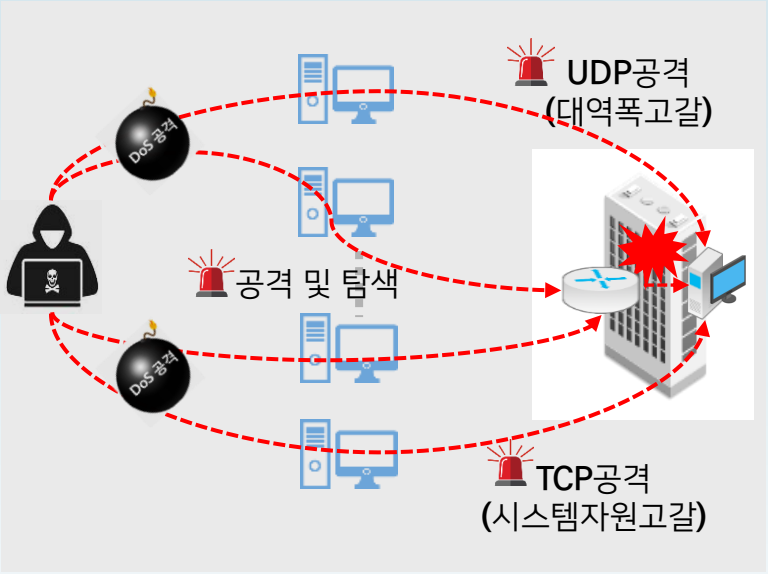
국내 중소형기업
DDoS 공격 언론상
보도 기준
총 100 건 이상
(500 억원 이상 피해)
'22년도

2. DDOS 공격 개요 및 최신 동향

최근 몇 년간 사물인터넷(IoT) 보급이 확산되면서 동시에 대용량의 사이버 공격이 증가하고 있습니다.

DDoS 공격이란?

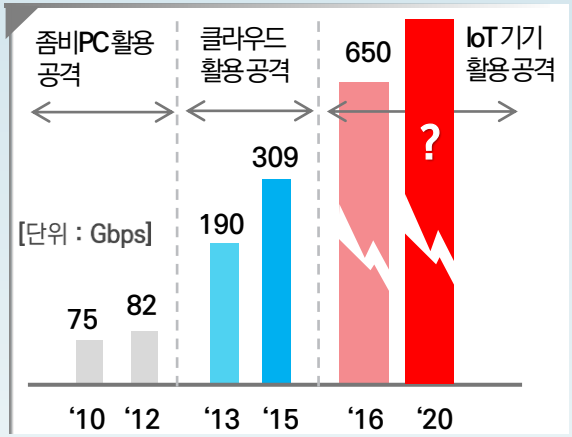
▪ DDoS 공격 개요



- 봇넷(BotNet)으로 Single or Multiple 서버 공격
- 악성 Bot Client에 감염된 디바이스들의 네트워크
- 네트워크 대역폭, 컴퓨팅 파워, 시스템 자원 고갈 등

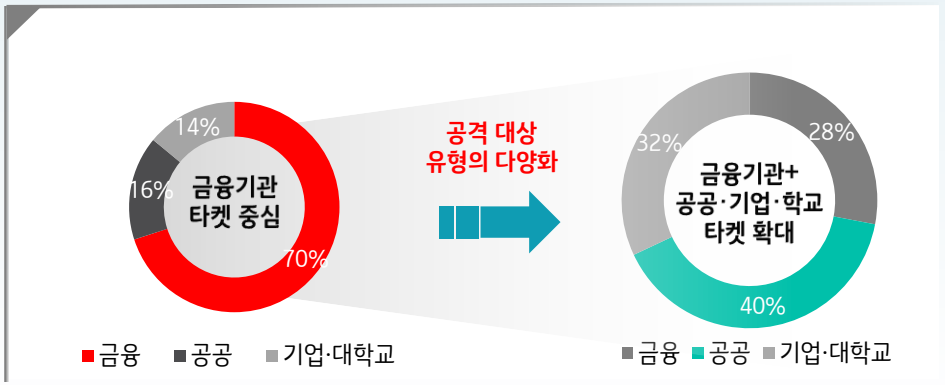
DDoS 공격 최신동향

▪ 연도별 최대 DDoS 공격 규모 변화



- IoT 기기를 활용한 초대형 DDoS 공격 증가(좀비IoT)
- CCTV, 가정용 AP 등 네트워크 접속 기능한 IoT 디바이스 타겟 (미라이 봇넷)
- 비트코인 등 금전적 요구 사례 (아르마다 콜렉테브)

▪ 해커에게 빈번하게 표적이 된 산업부문



3. 고객 환경 및 주요 이슈사항

최근 정부, 금융, 서비스 등 전 산업에 걸쳐 **DDoS** 대응시스템 구축, 복구훈련 등 대응체계를 강화하고 있습니다.

환경변화

- 인터넷사용량 및 Big Data 증가
- Internet기반 대국민서비스의 증가
- 취약고객 찾기 위한 주기적 반복 및 탐색 증가

고객별 DDoS방어 유형

중앙정부, 지자체	행정망: NIRS 대외망: 통신사
일반기업	중소기업: KISA 대기업: 통신사
금융기관	금융보안원 & 통신사

시사점

- 대용량 백본기반 DDoS방어 구축이 필요 (공격용량의 대형화 추세)
- 지능화된 방어시스템 필요 (실시간 악성IP/URL기반 **DDoS**대응시스템)
- 공격 유무와 상관없이 상시 보안대책 필요

DDoS 대응 전략

소용량 TCP 공격 대응

고객사 내부 관제
& IPS 활용 방어

+

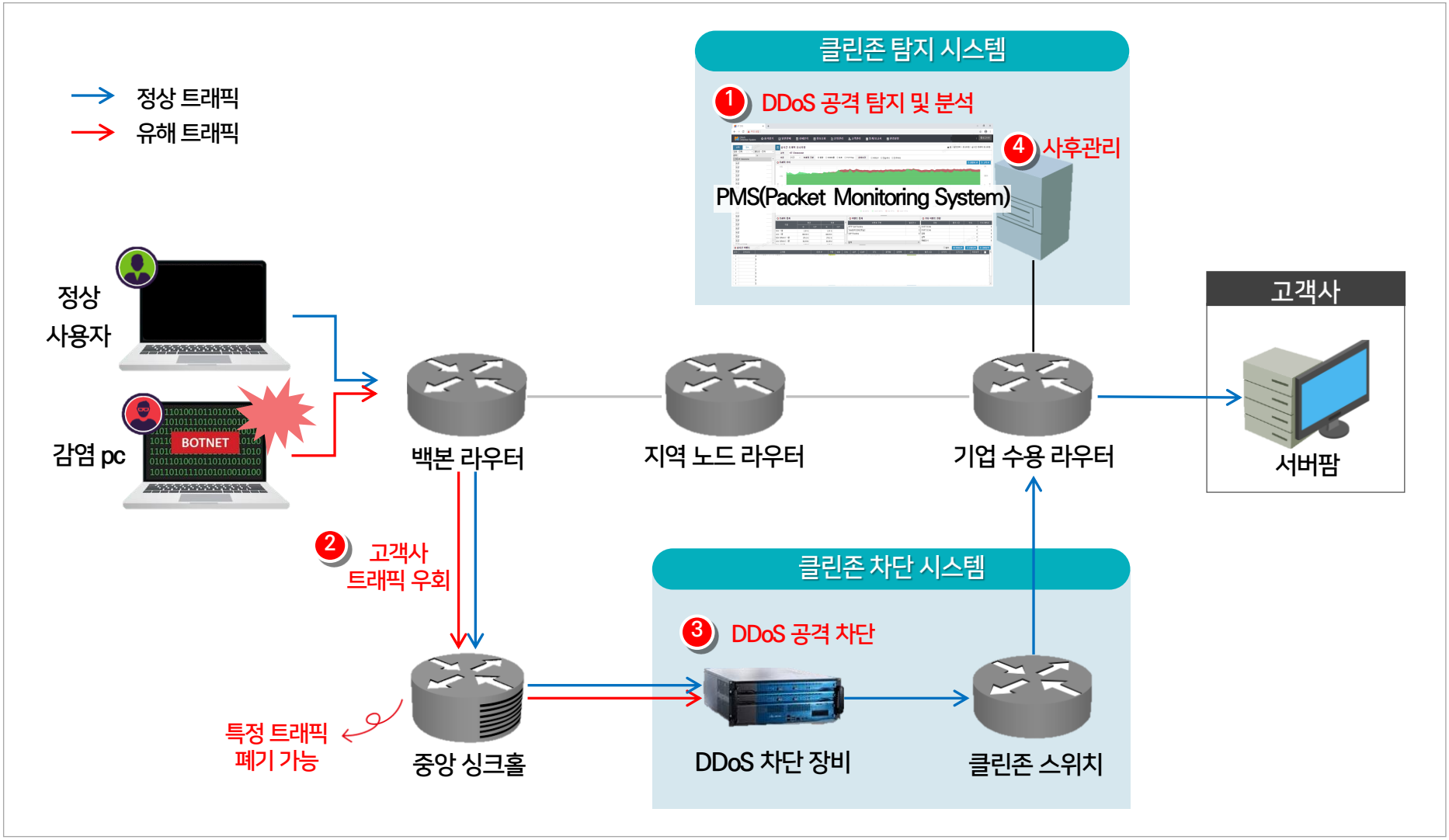
회선대역폭 공격

대용량 DDoS방어
서비스 이용

kt 클린존 서비스

4. 클린존 서비스 개요

KT 클린존 서비스는 DDoS 공격을 조기에 탐지 및 분석하고 유해 트래픽에 대한 차단서비스를 제공합니다.

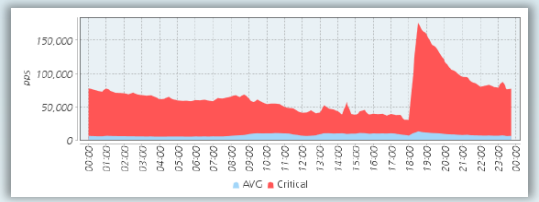


5. 서비스 제공 프로세스

KT는 국내외 인터넷 트래픽에 대해 365일 관제 중이며, DDoS 공격발생 시 긴급 대응뿐만 아니라 고객사와 모의 훈련을 시행하는 등 안정적인 서비스 제공체계를 갖추고 있습니다.

평상시

- 고객사 트래픽 임계치 학습
  - 이상 수치의 트래픽 유입 시 감지하기 위한 학습
  - 클린존 탐지시스템에서 고객사별 **netflow** 분석을 통해 시간대별 트래픽 임계치 설정



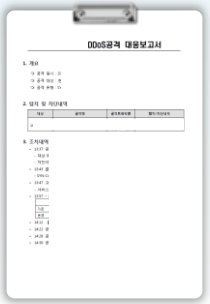
- 보안 관제
  - **24**시간 **365**일 **KT** 직원 직접 관제
- 보안 컨설팅(고객 요청 시)
  - 보안 네트워크 디자인
  - 웹서버 취약점 점검
- 산출물 – 월 정기 보고서

DDoS 공격 발생 시

- **DDoS** 공격 대응 프로세스

1. DDoS 탐지/분석
   - 클린존 탐지시스템에서 이벤트 발생 시 트래픽 분석
   - 고객 협의 후 클린존 차단시스템으로 우회
2. DDoS 방어
   - 망기반 트래픽 차단
   - 클린존 차단시스템에서 유해 트래픽 차단 후 정상트래픽만 고객사로 전송
3. 상황종료
   - 공격종료 확인(서비스 정상 유무 체크)
   - 망 차단 해제
4. 사후관리
   - 대책 협의 및 적용
   - 대응 보고서 제공

- 산출물 – **DDoS** 공격 대응 보고서



모의 훈련 시

- 고객사와 모의훈련 일정 및 방식 협의

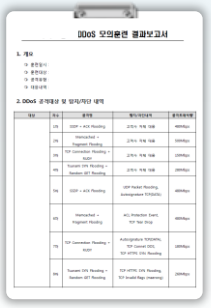
방식 1

실제 **DDoS** 공격 상황과 동일 방식
: **DDoS** 공격 실제 발생 시 방어프로세스와 동일하게 진행

방식 2

클린존 차단 시스템으로 선 우회 방식
: 서비스 안정성 확보를 목적으로 고객의 사전 동의 하에 클린존 차단시스템으로 선 우회하여 **DDoS** 트래픽 전송

- 산출물 – 모의 훈련 보고서



6. 서비스 특장점

클린존 서비스는 대용량시스템, 고품질 서비스 체계, 경제성 및 편의성 확보를 통한 차별적 서비스를 제공합니다.

대용량 DDoS 공격 대응체계

01 대용량 DDoS 공격 대응 체계

- DDoS 방어장비 용량(200Gbps) 이상의 공격에도 고객의 서비스 보호

02 검증된 레퍼런스 & 시스템

- ISP 최초로 DDoS 방어시스템 구축
- 다수의 공공기관 및 금융권 레퍼런스 보유
- DDoS 전용 시스템으로 OUT-OF-PATH* 방식 구축 (특허보유)

AI 기반 선제적 대응 & 고품질 서비스

03 Big-Data기반 선제적 대응체계

- 좀비PC 등 Black List DB(위협정보) 530만건 보유
- 선제적 대응을 통한 사전차단 등 공격리스크 사전 경감

04 고품질 관제서비스

- 고객사 웹사이트 모니터링 강화 및 집중 모니터링을 통해 공격발생 시 즉각 조치
- DDoS 탐지시스템을 별도 구축하여 공격을 정확하게 실시간으로 탐지
- 협박장 등 직접적인 위협 발생 시 클린존 사전 우회조치 및 긴급상황 대응체계 확보

DDoS 전문인력 & 경제성/편의성

05 DDoS 전문대응팀 보유

- KT통합관제센터(과천 소재)에서 백본 네트워크와 통합관제
  → 외부공격에 유기적 대응
- 다양한 공격 대응 경험을 보유한 KT직원으로만 구성된 DDoS 대응 전문팀 운영

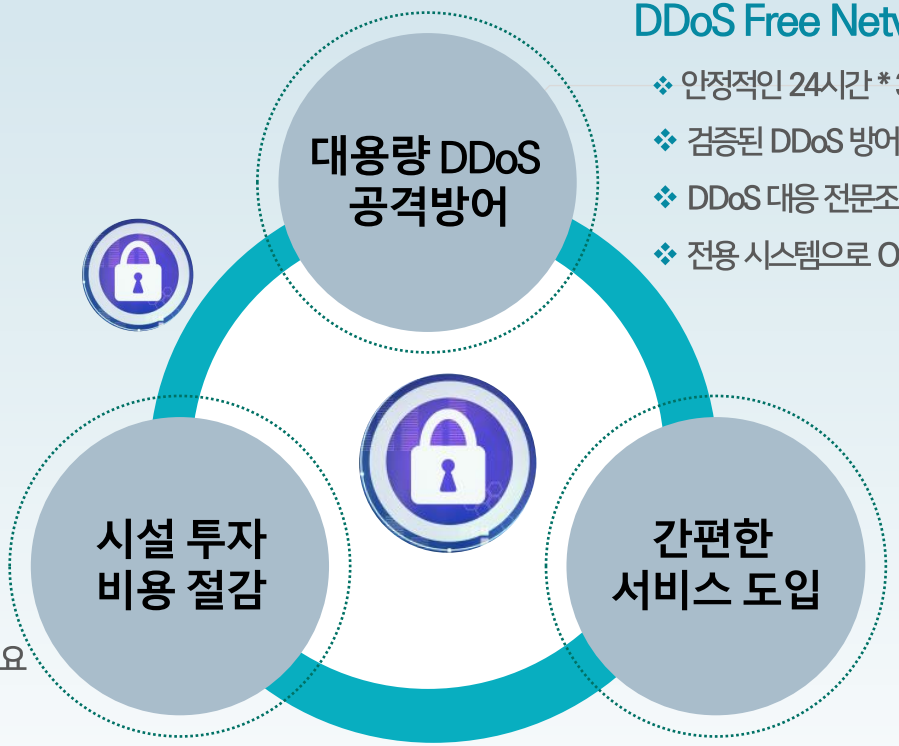
06 경제성 & 서비스 편의성 우위

- DDoS 대응인력 고용 및 DDoS방어 장비/솔루션 직접 투자 불필요
- 장비 설치 및 사내 네트워크 환경 변화 없이 서비스 가입만으로 24시간 * 365일 DDoS 대응체계 구축 효과

* OUT-OF-PATH: DDoS 공격 발생 시 방어장비로 트래픽 우회 처리하는 방식

7. 기 대 효 과

클린존을 통해 안전하게 대용량 DDoS 공격을 방어할 수 있으며, 서비스 도입에 따른 시설도 필요하지 않으며 비용도 절감하여 IT 시설을 보호할 수 있습니다.



DDoS Free Network 구현

- ❖ 안정적인 24시간 * 365일 관제
- ❖ 검증된 DDoS 방어 시스템 구축
- ❖ DDoS 대응 전문조직 운영
- ❖ 전용 시스템으로 OUT-OF-PATH* 방식 구축 (특허보유)

Cost Down

- ❖ 초기 투자비 대폭 절감
- ❖ 시설 유지보수 불필요
- ❖ DDoS 보안전문가 확보 불필요

Easy to Control

- ❖ 고객사 내부에 추가 시설 불필요
- ❖ 고객 네트워크 현재와 동일한 확장성 유지

8. 클린존서비스 vs. 자체구축 비교

클린존 서비스는 KT백본을 이용하는 고객이 이용하는 공통 플랫폼으로 방어용량 및 품질, 경제성면에서 유리합니다.

특징 비교

구분	클린존서비스	*자체구축*
방어용량	200Gbps+α	*회선 대역폭 이하*
제공방안	공통플랫폼	*전용플랫폼*
운용인력	DDoS 전문인력	*IT관제·* *운용인력*
탐지시스템	탐지시스템을 별도 운용→ 공격을 정확하게 실시간탐지	*탐지·방어* *통합시스템 운용*
대응체계	AI기반 분석을 통한 선제적 대응체계	*별도 TI구매 및* *실시간 업데이트 필요*
서비스 강점	대역폭고갈공격 방어에 유리	*TCP공격 방어 및 자체 분석에 활용*
비용측면	회선 용량에 따라 월정액 부과되어 자체 구축대비 매우 저렴	*장비 투자 이외 별도 인터넷 회선 및 관제 인건비* *유지보수 비용 투입 필요* *(서비스 이용 시 보다 1G 기준 5~6배 높음)*

9. DDoS 공격대응 성공사례

KT는 그 간의 대응경험과 노하우를 바탕으로 DDoS 공격에 대응하여 안정된 서비스를 제공하고 있습니다.

OO 은행(클린존 기 가입 고객)

OO은행에 최대 32G 디도스공격 발생 후 비트코인 요구 협박 메일 수신 (총4회공격)

"돈 안 주면 금융거래 해킹"
은행에 또 '디도스 공격' 협박

입력 2020.10.06 17:31 | 수정 2020.10.07 02:38 | 지면 A14

대응 개요

① 모의훈련을 통해 DDoS공격 대응능력 확보
② 1차공격→약 2분 후 방어 및 정상서비스 전환
③ 협박메일 수신에 따른 사전우회 적용
④ 추가공격(3회) 서비스 무중단 방어

핵심 성공요소

▶ 모의훈련 및 실무협의 등을 통한 고객사 – KT간 DDoS 대응프로세스 사전 확립
▶ 최신 공격패턴에 대한 대응능력 확보

[별첨] FAQ(5-1)

KT는 그 간의 대응경험과 노하우를 바탕으로 DDoS 공격에 대응하여 안정된 서비스를 제공하고 있습니다.

Q 클린존 서비스 어떤 서비스인지?

A KT 인터넷(코넷) 네트워크에 수용된 고객사 대상으로 대용량 DDoS 공격으로 고객의 네트워크를 마비시킬 경우에 대비하여 공격을 **탐지**하고, 공격 발생 시에는 **유해 트래픽을 우회/차단**하는 서비스를 제공하고 있습니다.

Q 클린존 탐지시스템의 동작 방식과 탐지 기준은?

A 공격 발생 이전에는(우회 전) 패킷 및 payload를 볼 수는 없으며, 고객사로 인입되는 **netflow 정보를 샘플링**해서 모니터링하고 있으며, 탐지시스템의 탐지 기준은 학습 임계치 및 Flooding 류(TCP Flooding 등) 기반으로 진행하고 있습니다. 학습임계치는 학습된 데이터 이상으로 트래픽이 발생하여 생긴 이벤트를 의미하며, 학습은 해당 IP에서 특정시간에 평소에 얼마만큼의 트래픽이 발생했는지에 대해서 평일 기준 20일치의 데이터를 분석해 학습임계치 이벤트 데이터로 활용합니다.

Q 클린존 서비스 기본적인 구조와 동작방식(탐지시스템, 차단시스템, GRE 터널) 에 대해서 설명해주세요.

A 평시에 고객사 트래픽은 코넷 백본 라우터 <-> 지역 노드 라우터 <-> 기업 수용라우터 <-> 고객사 서버팜 경로로 흐르게 되고, 기업 수용라우터에서 500:1로 샘플링된 netflow 정보를 클린존 탐지시스템에서 받아서 트래픽을 모니터링하고 있습니다. 공격이 발생하게 되면 백본 라우터에서 중앙 싱크홀(혜화/구로)로 static-route를 설정하여 클린존 차단시스템을 타게 됩니다. 공격 트래픽은 DDoS 차단 장비에서 차단되고, 정상 트래픽은 클린존 GRE 스위치를 통해서 다시 기업 수용 라우터로 보내지게 됩니다.

Q 클린존 평상 시와 공격 발생시 어떻게 동작하는지?

A 평상 시에는 고객사별로 **트래픽 임계치를 학습**하고, 임계치 이상의 트래픽 유입 시 netflow 분석을 통해 공격 여부를 판단하며 공격으로 판단될 경우에는 기업용 라우터 최상단의 **백본 라우터에서 중앙 싱크홀**로 라우팅 설정하여 트래픽을 우회하고, 차단 시스템에서 고객사별 차단 정책(임계치 및 패턴 기반)에 맞게 비정상 트래픽을 차단하여 정상 트래픽은 다시 고객이 수용된 기업용 라우터로 보내줍니다.

[별첨] FAQ(5-2)

KT는 그 간의 대응경험과 노하우를 바탕으로 DDoS 공격에 대응하여 안정된 서비스를 제공하고 있습니다.

Q 클린존 서비스 수용을 위해서 고객사에서 네트워크 설정 이나 구성을 별도로 조작 해줘야 하는 사항이 있나요?

A 클린존 서비스를 수용하기 위해서 기본적으로 KT 측으로 BGP 광고만 하고 있다면 고객사에서 별도로 네트워크 설정이나 구조를 변경 내용은 없습니다. 다만, 고객사에 수용된 라우터에서 클린존 탐지시스템으로 netflow 정보를 받아야 하기 때문에, 해당 고객사가 수용된 기업용 라우터(ECA)가 netflow 전송 및 클린존 서비스 수용에 문제가 없는지 사전에 확인이 필요합니다.

Q DDoS 공격 발생 시 공격 대응 프로세스가 어떻게 되나요?

A 탐지시스템에서 공격 트래픽으로 판단이 되는 경우, 사전에 고객사와 구성하고 있는 비상연락망을 통해 상황을 전파하고, 우회 여부를 결정합니다. 우회를 진행하게 될 경우, 즉시 탐지시스템에서 공격이 발생된 목적지 IP 기반으로 우회를 진행하게 됩니다.

Q DDoS 공격 발생 시 클린존 서비스 우회/차단까지 대응 소요 시간은?

A 탐지시스템에서 공격 인지는 이벤트 발생 후 즉시(~3분이내) 가능하며, 고객사와 음성통화로 우회 여부 결정(~5분이내), 클린존 우회(라우팅 변경) (~10분 이내)로 공격 인지부터 공격 우회까지 약 20분 정도 소요되고 있습니다.

Q 클린존 차단시스템이 수용할 수 있는 공격 트래픽과 그를 초과하는 공격이 발생했을 때는 어떤 식으로 대응하시나요?

A 클린존 차단시스템의 용량은 차단시스템 200Gbps의 공격을 수용할 수 있습니다. 다만, 해당 수용량은 클린존 서비스를 제공받고 있는 고객사들이 공용으로 사용하는 양으로, 한 고객사 당 200G가 아닙니다. 다수의 고객사 대상으로 동시다발적으로 공격이 발생한 경우, 200Gbps 내에서 고객사 별로 공격을 대응하고 있으며, 이를 초과하는 공격 발생 시 일부 미차단 트래픽이 고객사로 유입될 수 있습니다.
(이용약관 참고) * 200Gbps를 초과하는 공격 시 싱크홀 구간에서 해외구간 BGP Flowpsec을 차단할 수 있습니다. 이 경우에는 해외구간에서 목적지 IP로 접근하는 트래픽이 폐기되므로 해외구간에서 접근하는 서비스가 제공 불가능하게 됩니다.

[별첨] FAQ(5-3)

KT는 그 간의 대응경험과 노하우를 바탕으로 DDoS 공격에 대응하여 안정된 서비스를 제공하고 있습니다.

Q 클린존 차단시스템 정책 임계치 정보와 임계치 변경이 가능한가요?

A 고객사에서 요청하실 경우 차단 정책 임계치와 임계치 수정은 가능합니다.

* 차단 정책 임계치는 클린존 고객사 대상으로 진행 중인 DDoS 모의훈련과 공격 대응 등으로 지속 최적화 중입니다.

Q 클린존 서비스 차단 관련 설정값, 타당성 등 설정기준 어떻게 되나요?

A 차단 관련 정책들은 실제 DDoS 공격 트래픽 대응 시 분석된 정보와 매년 진행되는 고객사들의 모의훈련 결과를 통해 얻은 데이터를 바탕으로 차단 정책을 업데이트하고 있습니다.

Q 클린존 서비스에서 공격 발생에 대비해 자동 우회/ 사전 우회를 제공해주실 수 있나요?

A 클린존 서비스는 대용량 DDoS 공격을 대응하기 위한 서비스로, 트래픽을 임계치 기반으로 차단하기 때문에, 자동우회 및 사전우회 시에 일부 정상 트래픽이 차단될 수 있는 Risk가 존재합니다. 이러한 이유로 클린존 서비스는 자동 우회 및 사전 우회는 제공하지 않습니다.

Q 클린존 차단시스템 우회 시에 대역으로 우회도 주시나요?

A 클린존 서비스는 목적지 IP에 대한 **호스트 단위(/32)로 우회**를 진행하고 있습니다. 대역으로 우회는 하고 있지 않습니다.

Q 클린존 서비스 개통 후 트래픽에 대한 학습기간 및 이후 학습은 어떻게 진행 되나요?

A 개통 후 IP를 등록하고 등록한 IP로 발생한 트래픽 데이터로 학습이 시작되며 학습 기간은 약 1개월 정도 진행합니다. 이후에도 평상시 데이터를 모니터하면서 학습된 데이터가 갱신하며, 학습이 되면서 이벤트 오탐 감소 등 정교해집니다.

[별첨] FAQ(5-4)

KT는 그 간의 대응경험과 노하우를 바탕으로 DDoS 공격에 대응하여 안정된 서비스를 제공하고 있습니다.

Q 클린존 서비스 개통 시 TAB 적용하면서 서비스 단절(순단 포함) 되는지 ?

A 고객 상단 위 KT 라우터에서 고객으로 내려가기전의 트래픽을 모니터링 하는 것으로 단절 없습니다. 공격 발생 시에도 라우팅을 고객으로 내려보내기 전 클린존을 거쳐서 가도록 변경하는 것으로 단절 없습니다.

Q 평상시 및 DDoS 공격 대응 시 제공되는 보고서 종류는?

A 평상시에는 월 1회 정기보고서 및 공격 대응과 관련된 정보(일시, 차단량, 차단정책, 그래프 등)가 포함된 DDoS 공격 대응 보고서를 제공 중입니다. 또한 모의훈련 후 모의훈련 보고서를 제공됩니다.

Q 클린존 서비스 월간보고서 내용과 모의훈련에 대한 방식은 어떻게 되는지?

A 월간보고서에는 기본 가입 정보, 이벤트 발생 현황, 이벤트 대응 내역, 한 달간 트래픽 추이, 차단정책, 월간 보안동향 등의 정보가 포함됩니다. 모의훈련은 년1회 고객과 협의하여 일정을 정하여 KT에서 트래픽 발생하여 진행하며, 기본적인 Flooding 류의 트래픽을 최대 2G 정도까지 발생하여 훈련을 진행하게 됩니다.

Q 클린존 서비스에서 발생하는 이벤트나 로그들을 고객사 측과 연동 또는 웹뷰 형태로 제공이 가능한가요?

A 고객사로 로그 전송이나 웹뷰 제공하지 않습니다.

Q 클린존 서비스 C-Class 수용 대역 제한하고 있나요?

A 50M ~1G 속도에 따라 C-Class 1개 ~ 7개로 제한합니다. 자세한 사항은 이용약관을 참고하시기 바랍니다.

[별첨] FAQ(5-5)

KT는 그 간의 대응경험과 노하우를 바탕으로 DDoS 공격에 대응하여 안정된 서비스를 제공하고 있습니다.

Q 클린존 서비스에 수용된 타 고객사들의 IP대역 용도가 주로 어떻게 되나요?

A 웹 서비스 뿐만 아니라, DNS, DB 등 다양한 용도의 IP 대역이 수용되어 있습니다.

Q 클린존 서비스는 DDos 공격 트래픽 용량에 따라 계약/과금 영향을 받는지요?

A 아닙니다. 회선 트래픽 용량에 따라 계약하고 과금됩니다.

Q 클린존 서비스 이용 요금은 구조는 어떻게 되어 있나요?

A 코넷 속도별 차등하여 월정액 형태로 부과됩니다. 자세한 사항은 이용약관을 참고하시기 바랍니다.

Q 클린존 서비스에 수용된 고객 사들 레퍼런스가 어떻게 되나요?

A 코넷을 이용하고 있는 공공/금융기관/기업 등이 클린존 서비스를 이용하고 있습니다.

[별첨] 월간보고서 및 모의훈련보고서

월간보고서

OOO고객사	KT 클린존 3월 정기보고서	
	문서번호: OOO고객사-2023-03	작성일자 : 2023-04-19

목 차

공격대응 및 모의훈련보고서

A社 DDoS 모의훈련 결과보고서

1. 개요

- 공격 발생일시 : 2022.10.20(목) 15:10 ~ 16:00(50분)
- 공격 출발지 : 다수 해외 IP
- 공격 대상 : X.X.X.X(abc.com)
- 공격 유형 : UDP Flooding
- 공격 대응 : 클린존 우회 방어

2. DDoS 공격대상 및 탐지/차단 내역

대상	공격명	탐지/차단내역	공격트래픽량
X.X.X.X (abc.com)	UDP Flooding	UDP Traffic 임계치초과, UDP Flooding-Packet 개수 초과, UDP Tear Drop 등	약 2.1Gbps

3. KT사이버보안센터 조치내역

[공격 대응]

- 15:10 클린존 DDoS 탐지시스템 DDoS 공격 인지
  - 공격 대상 IP : X.X.X.X
  - 탐지 이벤트 : UDP Traffic 임계치초과, UDP Flooding-Packet 개수 초과 등
  - 공격량 : 약 2.1Gbps
  - 서비스 영향 : 홈페이지 정상 접속
- 15:11 고객사 상황 공유 및 클린존 DDoS 차단시스템 우회 검토 요청
- 15:12 클린존 DDoS 차단시스템 우회 완료
  - 우회 대상 IP : X.X.X.X
  - 차단 이벤트: UDP Tear Drop
  - 공격량: 약 2.1Gbps
- 15:13 클린존 DDoS 차단시스템 UDP 임계치 일부 수정
- 16:00 공격 종료(클린존 DDoS 차단시스템 우회 유지)

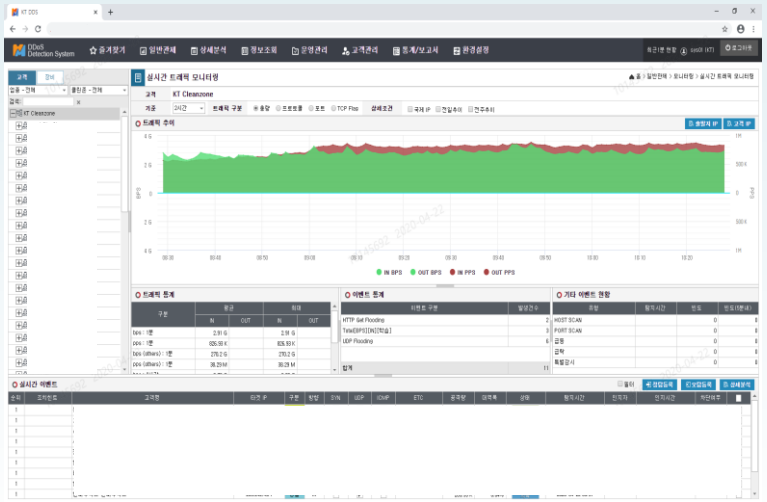
[별첨] 클린존 서비스 시스템 기능

클린존 탐지 시스템 PMS(Packet Monitoring System)

- **Netflow** 데이터 분석으로 유해 트래픽을 실시간 감지하며 고객별 트래픽, 이벤트 발생에 대한 실시간 모니터링 및 관제 솔루션

- **NBA(Network Behavior Analysis)** 기반 탐지
  - 일정 기간동안 고객사별 **netflow** 분석 및 학습 진행 후 시간대별 트래픽 임계치 설정
  - 임계치 이상의 트래픽 유입 시 이벤트 인식 또는 공격 탐지

- PMS 화면



클린존 차단 시스템

- **NBA+패턴 분석+인공지능 기반 차단**
  - 실시간 트래픽 분석 후 임계치 및 특성에 맞는 방어
  - 미리 정의해 놓은 일정 패턴의 트래픽(시그니쳐) 차단
  - 미리 정의되어있지 않은 패턴이라도 일정 패턴의 트래픽 수치가 높을 경우 자동 시그니쳐 생성 및 차단

- **DDoS** 차단 장비
  - **WINS Sniper ONE 20G 6**개로 구성
  - 다단계 방어 엔진 사용**(00**개**)**

WINS Sniper ONE 20G

Multi Layered Mitigation Flow

- **DDoS** 차단 유형
  - 서비스거부**(Syn Flooding, HTTP Get Flooding, UDP Flooding** 등**)**
  - 패턴블럭**(NTP Monlist, SSDP DrDoS,** 악성코드 문자열 포함 등
  - 임계치 이상 동일패턴 패킷 자동 차단**, Syn Cookie** 차단 등