최근 DDoS 보안위협 사례분석을 통한

7.7 DDoS에 따른 ISP의 대응전략

I. 최근 DDoS 침해공격 현황

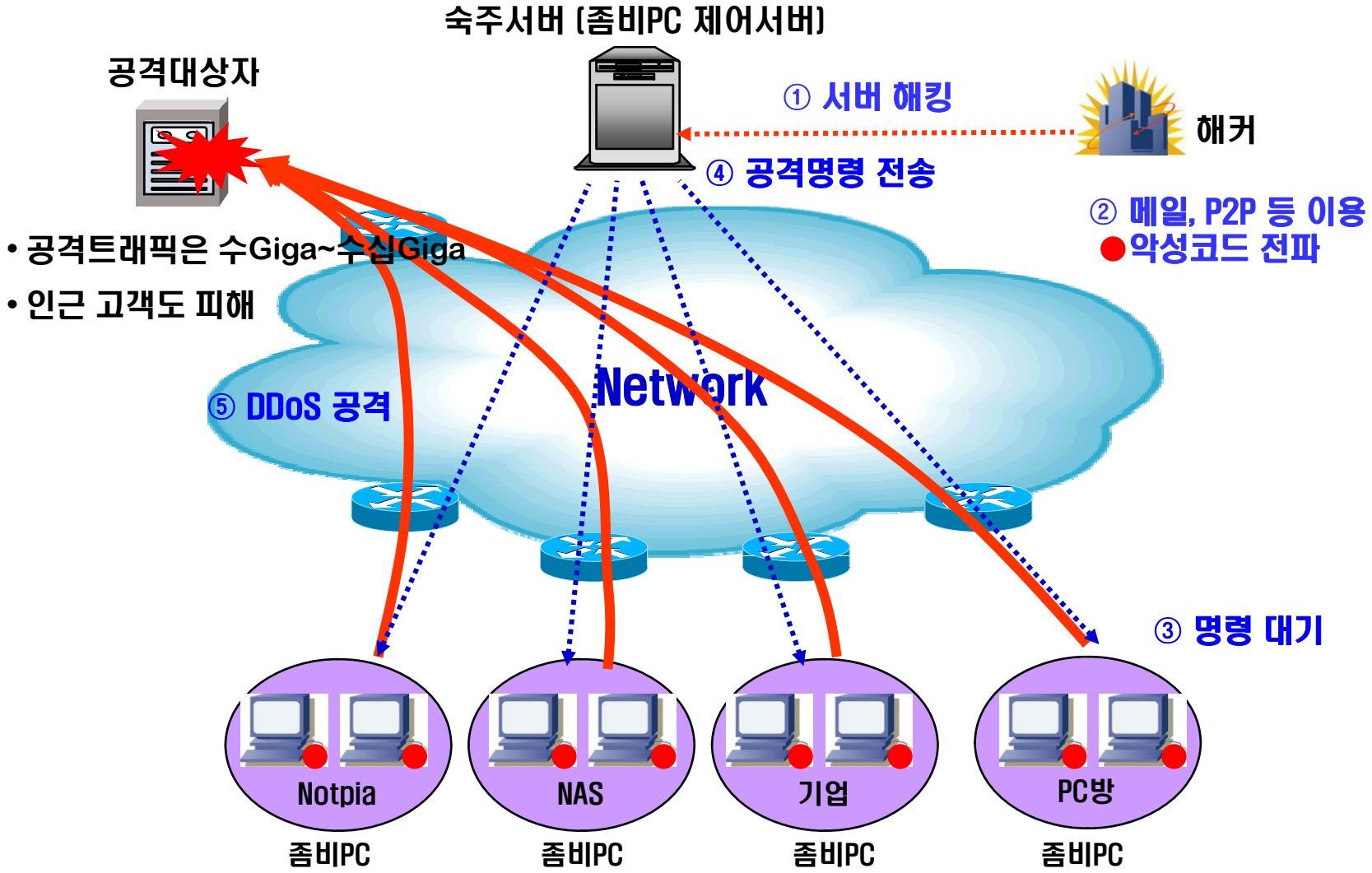
II. 7.7 사이버 침해공격 대응

III. 주요 보안이슈 사항

IV. 전사 DDoS 침해대응 방안

2009. 10. 22 | 고객지원본부 정보보호담당

I. 최근 DDoS 침해공격 현황

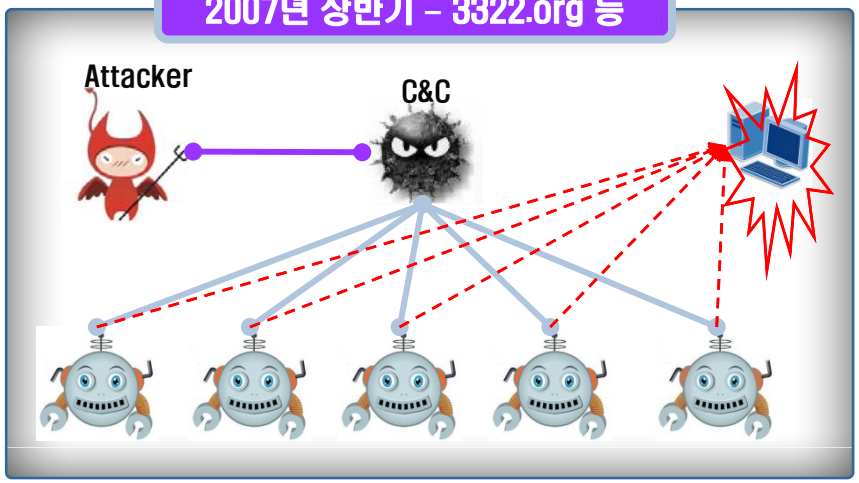


* 좀비PC의 수는 수백~수십만대로 좀비PC의 수가 많을수록 피해규모도 급증

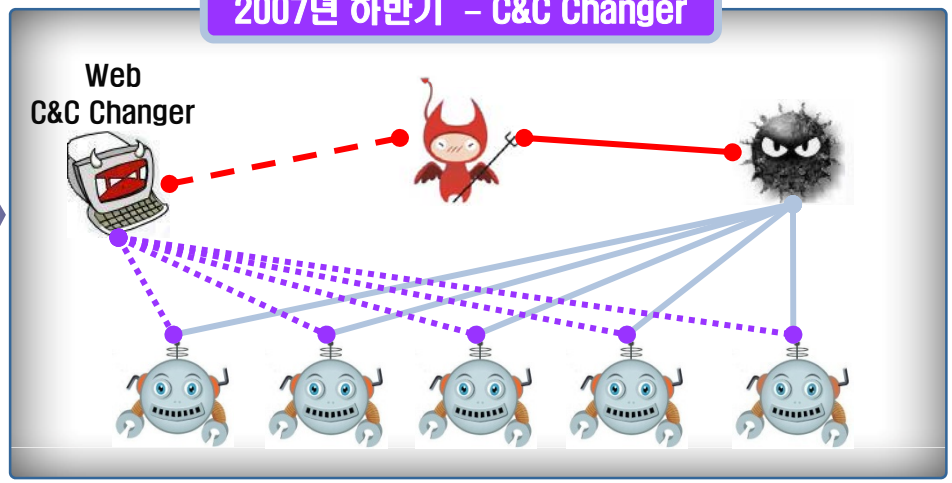
I. 최근 DDoS 침해공격 현황

BOTNET 지능화 추세 (주요 DDoS BOTNET)

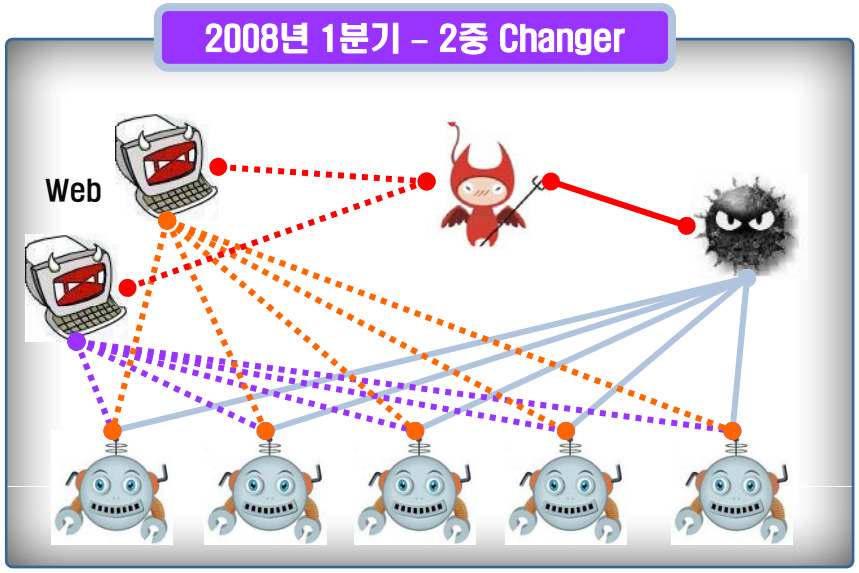
2007년 상반기 – 3322.org 등



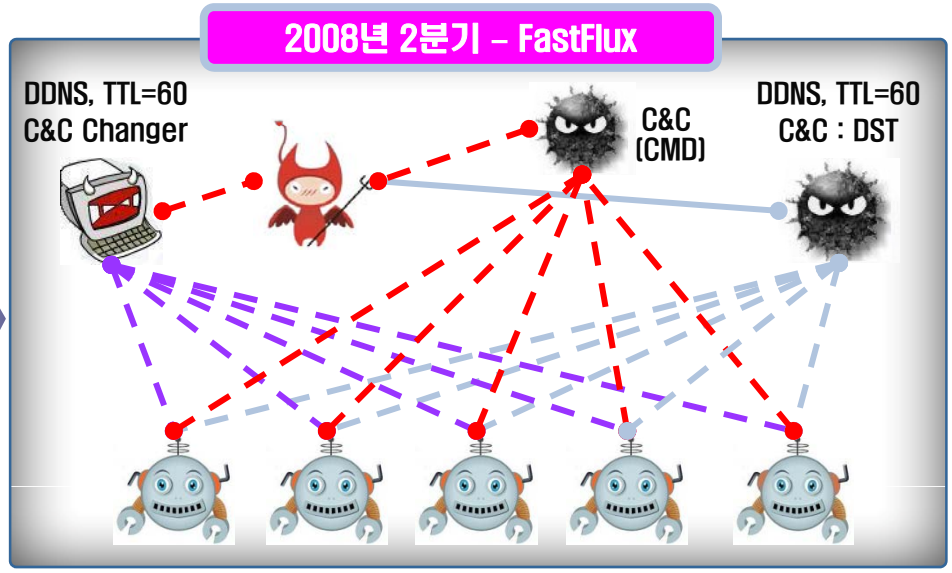
2007년 하반기 – C&C Changer



2008년 1분기 – 2중 Changer



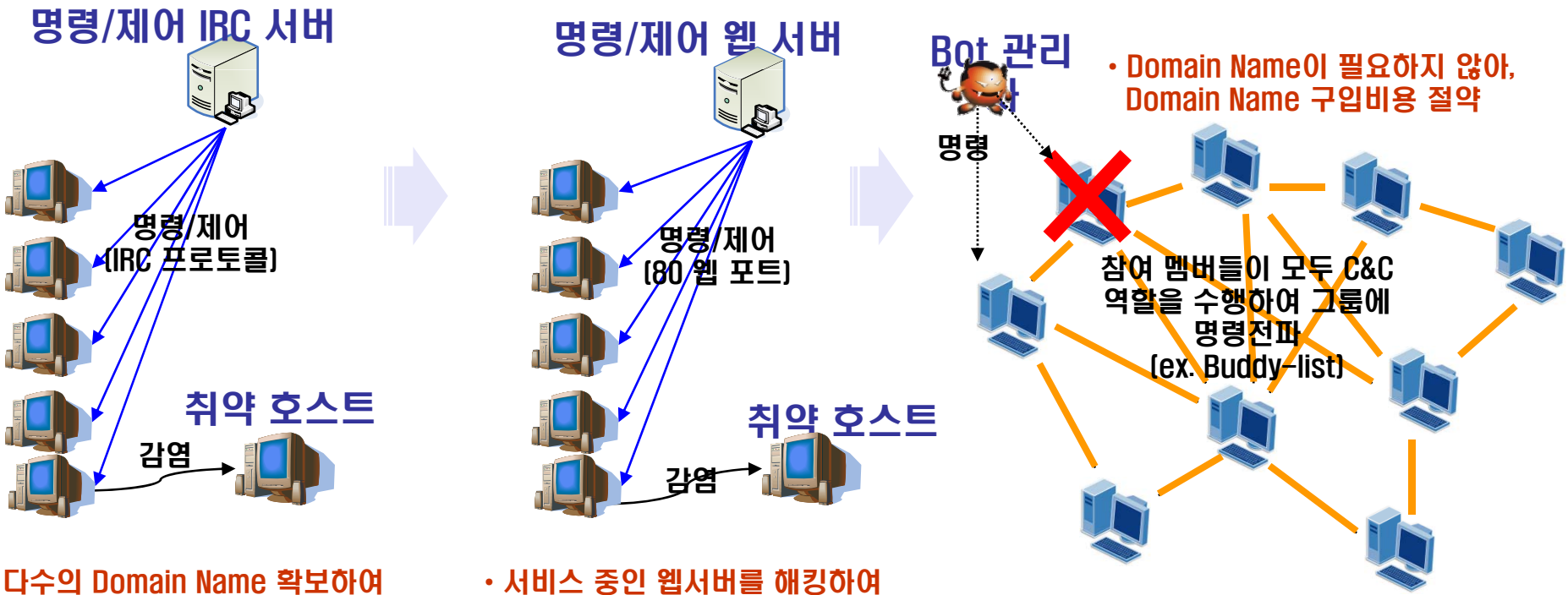
2008년 2분기 – FastFlux



I. 최근 DDoS 침해공격 현황

명령/제어 프로토콜의 진화

- 중앙집중형(IRC, HTTP) 방식➔ 분산형(P2P) 명령/제어 방식으로 발전
- 중앙집중형 방식에 있어서, IRC 방식 ➔ 탐지가 어렵도록 HTTP 방식으로 전환



- 다수의 Domain Name 확보하여 C&C 서버 등록(Fast-Flux 적용)
- 중앙집중형 제어
- 암호통신(SSL) 및 포트 변경
- 대표적인 IRC 봇넷 : Rbot

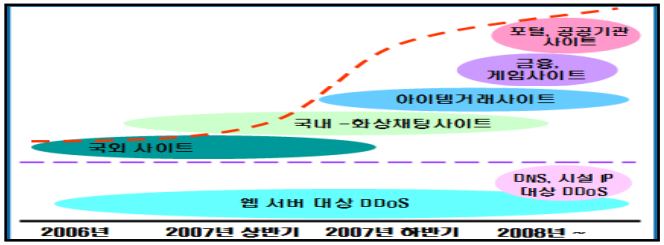
- 서비스 중인 웹서버를 해킹하여 C&C 서버로 악용
- 중앙집중형 제어
- 웹 프로토콜 → 탐지/차단 어려움
- 대표적인 HTTP 봇넷 : Robax

- 분산 제어 (Distributed control)
- 탐지 및 차단이 어려움
- 대표적인 P2P 봇넷 : Storm

I. 최근 DDoS 침해공격 현황

1 공격 특징

[DDoS 공격 트래픽 추이]



[DDoS 공격 대상의 변화]

	Country	% Traffic
1	China	27.59
2	United States	22.15
3	South Korea	7.53
4	Germany	2.95
5	Brazil	2.60
6	Sweden	2.48
7	Taiwan	2.22
8	Poland	1.87
9	Romania	1.83
10	Japan	1.79

[09년 공격 근원지 TOP 10]

□ DDoS 트래픽의 급속한 증가 (08년말 최대 58G 발생, 국내 → 일본)

※ 주요원인 : 고객PC의 高 사양화, 좀비PC(악성코드 감염PC)의 증가, 대역폭(FTTH) 증가 등

□ 공격대상은 사회적 이슈가 되는 정부 및 금융기관 등으로 다양화 추세

□ 공격 근원지(좀비PC 수)는 한국이 세계 3위

2 공격 변화

□ 03~04년 → 웜 바이러스에 의한 공격 (네트워크를 통해 불특정 서버/PC 감염/전파)

□ 04~05년 → 피싱 및 스팸 (금전목적의 금융사이트 위조, 대출/악성코드 전파)

□ 05~08년 → Bot에 의한 DDoS 급증(금전요구 및 PC방 등 경쟁사 공격)과 DDoS 공격도구 판매

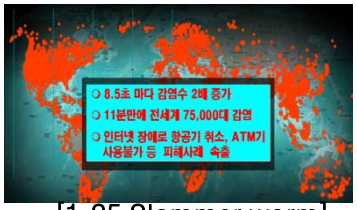
□ 09년 ~ → Bot에 의한 DDoS 공격의 지능화 (7.7 DDoS 사이버공격)

I. 최근 DDoS 침해공격 현황

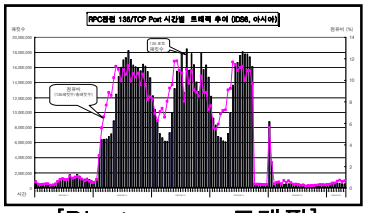
3 주요 사례

□ 웜 바이러스

- ❍ 03년 1월 Slammer 웜에 의한 1.25 인터넷대란
- ❍ 03년 8월 Welchia, Blaster 웜 (웜 전파 포트차단)
- ❍ 04년 1월 Mydoom, Bagle 웜 (웜 전파 포트차단)



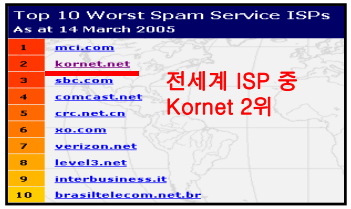
[1.25 Slammer worm]



[Blaster worm트래픽]

□ 피싱 및 스팸메일

- ❍ 04년 4월 스팸메일 급증 (OECD 스팸 워크샵 개최, 부산)
- ❍ 04년 5월 피싱피해 증가 (국내 피싱 전세계 2위)

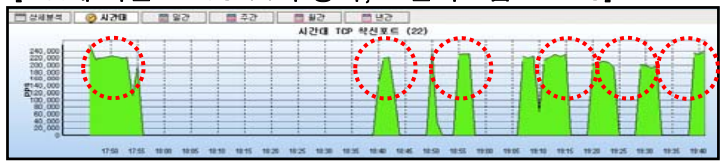


[스팸메일 급증] [출처: www.spamhaus.org, 05년 3월 기준]

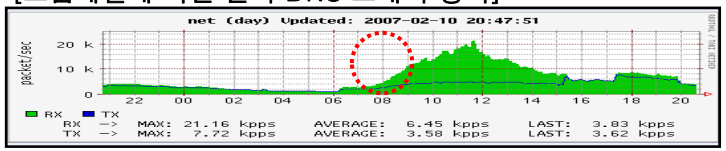
□ DDoS 침해공격

- ❍ 05년 6월 BOT에 의한 대형 DDoS 발생 (14회/1일 공격)
- ❍ 07년 DNS 공격 및 스팸메일에 의한 인터넷 지연
  - – 스팸 대량발송으로 DNS 응답지연 (VOC 163건)
  - – 9월 3.8G DDoS 공격 등 다수 (서비스 장비고장 등)
- ❍ 08년 DNS 및 주요기관 DDoS 공격
  - – 전국 DNS(2월),청와대(4월),미래에셋(3월),국민은행(4월)등
  - – 08년 DDoS 대응 약 3,000건 (고장 216건)
- ❍ 09년 7.7 DDoS 사이버대란 발생

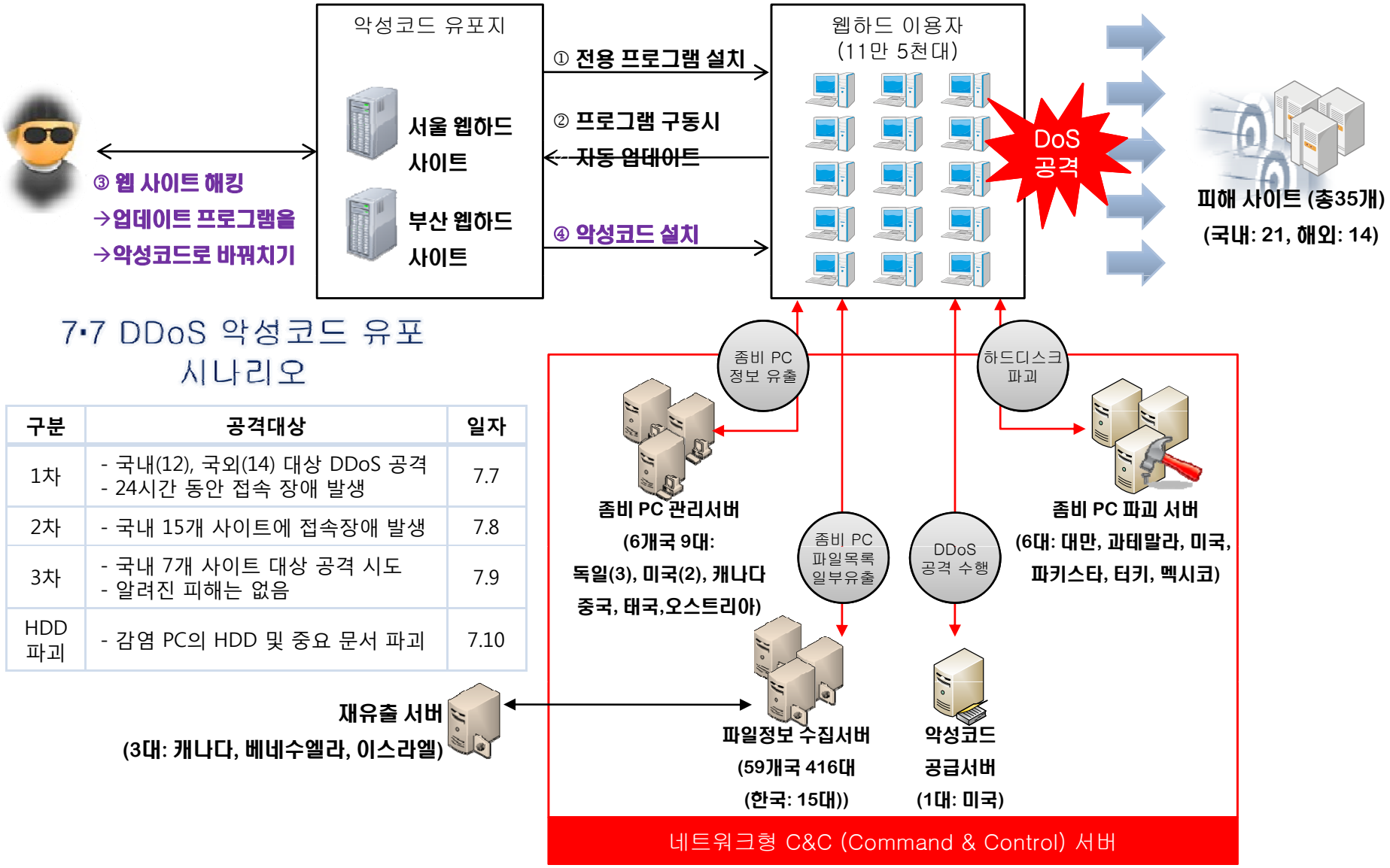
[Bot에 의한 DDoS 14회 공격, 보안시스템: KAPS]



[스팸메일에 의한 전국 DNS 트래픽 증가]



II. 7.7 사이버 침해공격 대응



7·7 DDoS 악성코드 유포 시나리오

구분	공격대상	일자
1차	- 국내(12), 국외(14) 대상 DDoS 공격 - 24시간 동안 접속 장애 발생	7.7
2차	- 국내 15개 사이트에 접속장애 발생	7.8
3차	- 국내 7개 사이트 대상 공격 시도 - 알려진 피해는 없음	7.9
HDD 파괴	- 감염 PC의 HDD 및 중요 문서 파괴	7.10

II. 7.7 사이버 침해공격 대응

7.7 DDoS 공격 및 피해현황

공격 개요

□ 일시 : 7.7 ~ 7.9 18:00 ~ 24시간 (총 3회 공격)

□ 대상 : 국내외 총 34개 사이트 (국내 23개 사이트)

– 청와대, 국방부, 국정원, 조선일보, 국민은행 등

□ 피해

– 공격 웹 사이트 접속불가 및 지연

– PC 정보 유출 및 하드디스크 손상(약 1,446건)

약 16만대(국내 7만8천, KT 3만7천) 국내외 총 34개(국내 23개)

공격 특징

□ 하나가 아닌 다수의 악성코드가 유기적으로 연동

□ 계획된 시나리오로 동시에 다수 웹 사이트 공격

□ PC 정보유출(파일목록 등) 및 하드디스크 파괴

KT 대응 (전사침해사고대책상황실)

피해 사이트 고객Care

□ 청와대, 국정원 등 피해고객 긴급 지원

– 고객 회선증설 및 해외발 공격트래픽 차단

□ 조선일보, 한나라당 웹 서버 긴급보호 조치

– 유해트래픽 차단서비스(IDC Clean Zone) 수용

악성코드 분석 및 대응

□ 신속한 DDoS 악성코드 샘플 확보 및 분석

– 공격대상 기관 리스트 및 신종 악성코드 확인

□ 악성코드 첫 입수를 통한 백신치료 지원

– KSIA 및 백신업체 악성코드 제공 및 공조대응

감염고객 Care 및 홍보

□ TM 및 PC 팝업공지 홍보 및 백신설치 유도

– 감염고객 치료(3만7천), 전체고객(670만)

□ 국내 손상된 고객PC 긴급 현장복구

– IT 서포터즈, 피해접수 고객 현장복구(716건)

III. 주요 보안이슈 사항

공격의 다양화

□ DDoS 공격의 대형화로 수백Giga 트래픽 공격 가능 (일부/전국 인터넷서비스 고립 가능)

□ 금전요구 및 정치/사회적 목적의 DDoS 공격 지속

- 정부, 금융, 언론 등 주요기관
- 일반(Ntopia) 고객(게임/채팅 등 웹사이트 운영) 및 IMO(아이템거래사이트, 웹 호스팅 사이트 등)
- DDoS 전용 공격도구(Netbot) 판매(약 30만원) 및 보편화로 DDoS 공격이 쉬움

□ 대량 스팸발송에 따른 DNS 트래픽 증가 (스팸+DDoS+정보유출+전파 등 복합 공격)

□ 인터넷 서비스 시설을 향한 공격 (DNS, 라우터 등)

대응 문제점

□ 좀비PC 제어서버(숙주) 분석 어려움

- 좀비PC와 제어서버간 암호화 통신 등 복잡하게 변화
- 생존성 확보를 위한 악성코드의 은폐, 자기방어 기능 등 지능화

□ DDoS 트래픽 선별 차단의 한계

- 네트워크망에서 공격 트래픽만 구분하여 차단 불가

□ 다수의 공격발생 고객단말에 대한 실시간 차단 어려움

□ 고객의 보안의식 미흡 (백신의 의미 모름)

IV. 전사 DDoS 침해사고 대응방안

1 DDoS 침해 대응력 향상

□ 3분인지 및 10분 초동대응의 전사 침해사고 대응체계 강화
- KAPS, IPS-ESM, NMS 등을 통한 DDoS 공격 3분인지
- KAPS, SinkHole라우터, 싱크홀DNS, ACL, DDoS 전용장비 등을 통한 10분 대응체계 유지

□ DDoS 공격용 악성코드 확보 및 분석을 통한 경로차단 대응 강화
- 확보된 악성코드의 동작경로 분석을 통한 숙주서버 차단 대응 강화
  - MEPS, HoneyNet, NERAS, 네트워크트래픽분석장비 등 활용

□ 대내외 협력기관간 DDoS 공조체계 강화
- 고객 DDoS 공조대응 프리미엄 서비스 강화(보안관제시스템 구축 및 운영 고객에 한함)
- 방송통신위원회, KISA, 국정원, 경찰청, NSF(네트워크시큐리티포럼), 백신회사, 보안회사 등

2 정보보호 인프라 고도화

□ DDoS 전용 보안장비 구축
- KORNET 백본(추진중), IDC구간 DDoS 전용장비 구축(추진완료)

□ 악성코드 감염PC 의 인터넷 접속차단 체계 구축
- 비상시, 고객단말 배치 형식의 차단기능 개발 및 구축

4 감염고객 Care 추진

□ 악성코드 조치를 위한 백신반영 프로세스 강화
- 안철수연구소와 이스트소프트와 MOU 및 NDA 계약 체결

□ 고객공지를 통한 백신설치 유도 및 인식 강화
- 감염고객 자가조치를 위한 고객공지(온라인) → 백신설치 강제유도 및 치료 안내

□ 긴급시, 고객 현장지원 체계 확립
- IT 서포터즈 및 현장요원(현장 NSC 및 현장 기술지원팀 등)

IV. 전사 DDoS 침해사고 대응방안

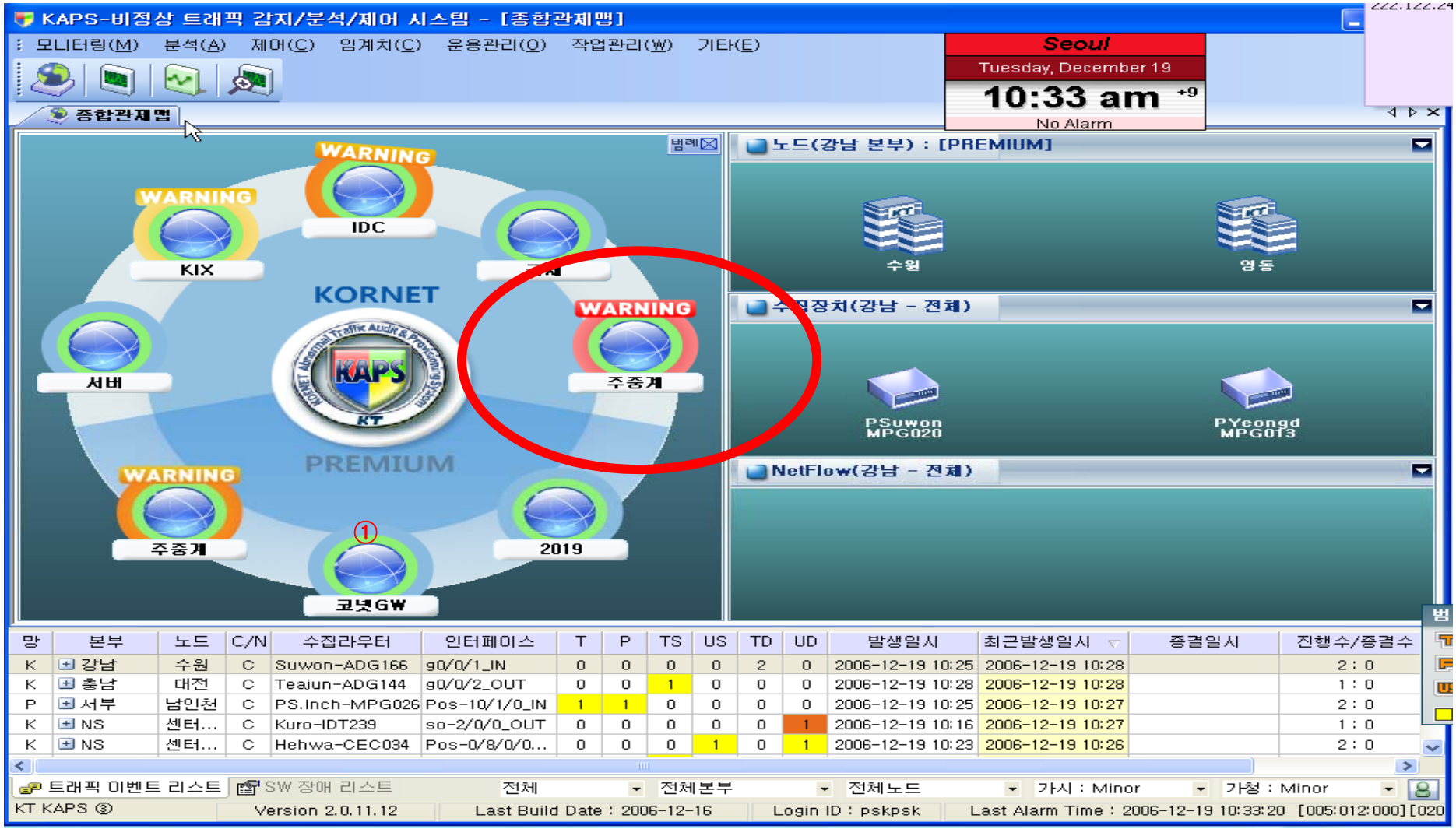
전사 대응조직

IV. 전사 DDoS 침해사고 대응방안

IV. 전사 DDoS 침해사고 대응방안

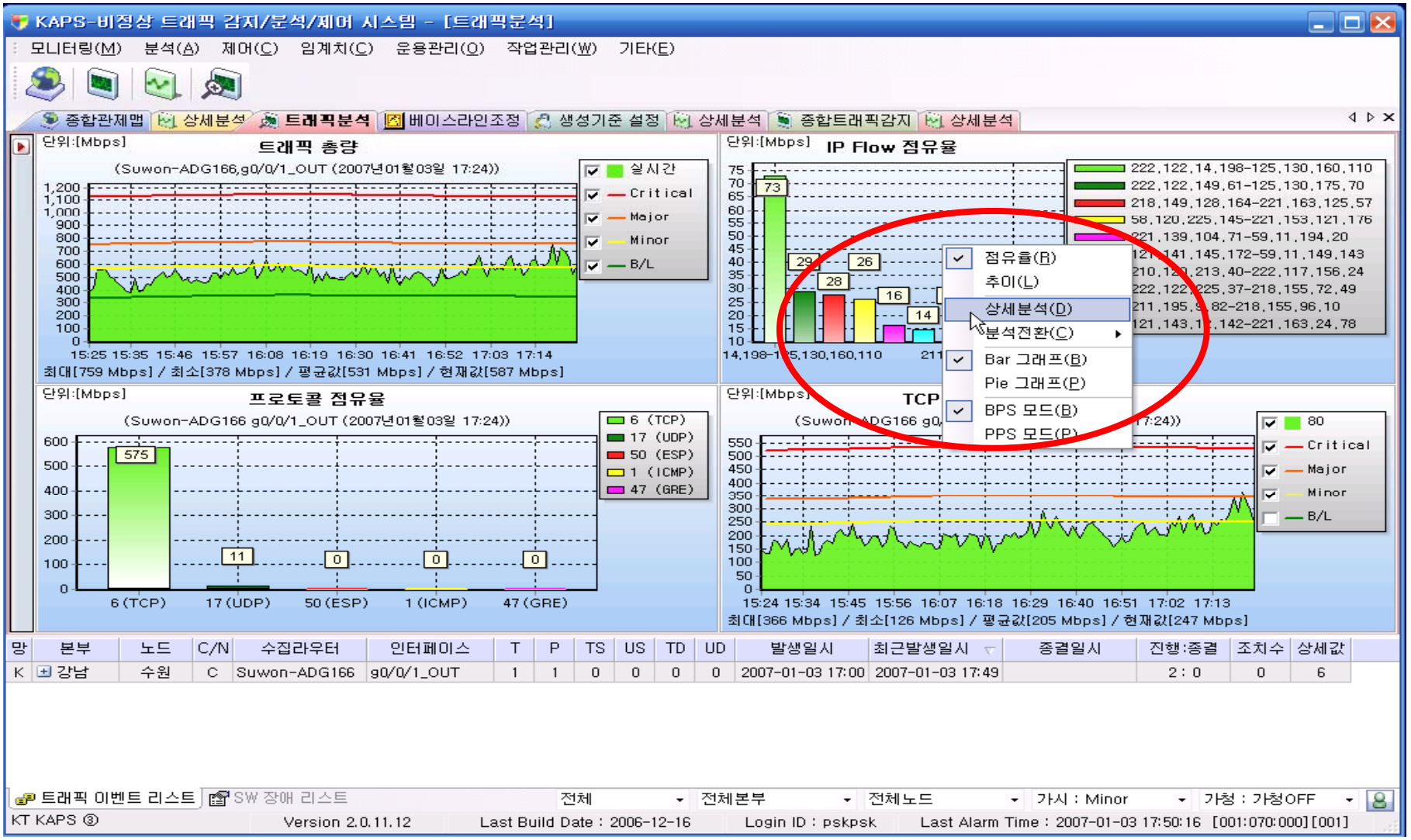
IV. 전사 DDoS 침해사고 대응방안

KAPS:비정상트래픽감시분석제어시스템

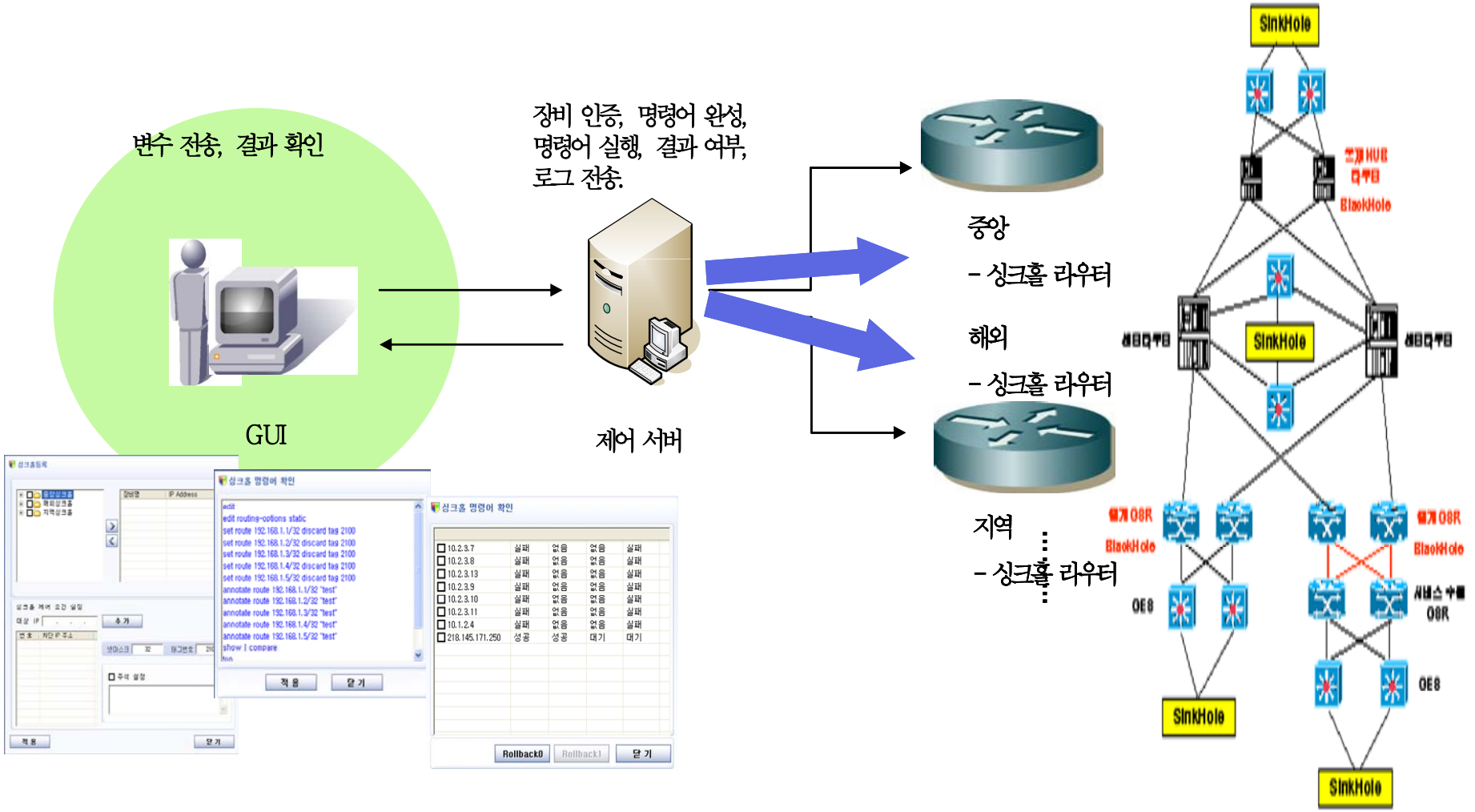


IV. 전사 DDoS 침해사고 대응방안

KAPS:비정상트래픽감시분석제어시스템



싱크홀라우터 구성 개략도



❖유해트래픽 탐지 및 차단이 10분이내에 해결가능

IV. 전사 DDoS 침해사고 대응방안

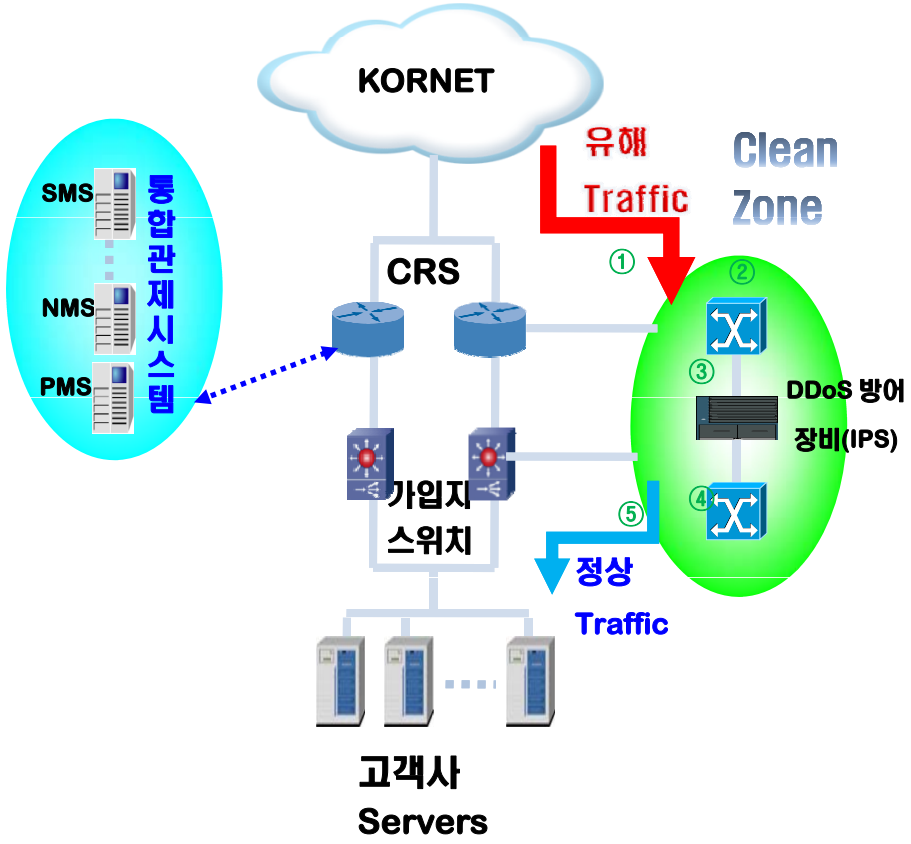
KT-ICC : Clean Zone DDoS 대응

DDoS공격 발생 시, 탐지된 공격 Traffic을 우회시켜 유해 Traffic을 제거한 후 정상적인 Traffic만을 통과시켜 KT-ICC 고객이 DDoS공격에 영향을 받지 않고 정상적인 서비스를 제공할 수 있도록 구성된 DDoS공격 전용 차단 영역을 Clean Zone 확대 운영 강화

Clean Zone 구성

<동작절차>

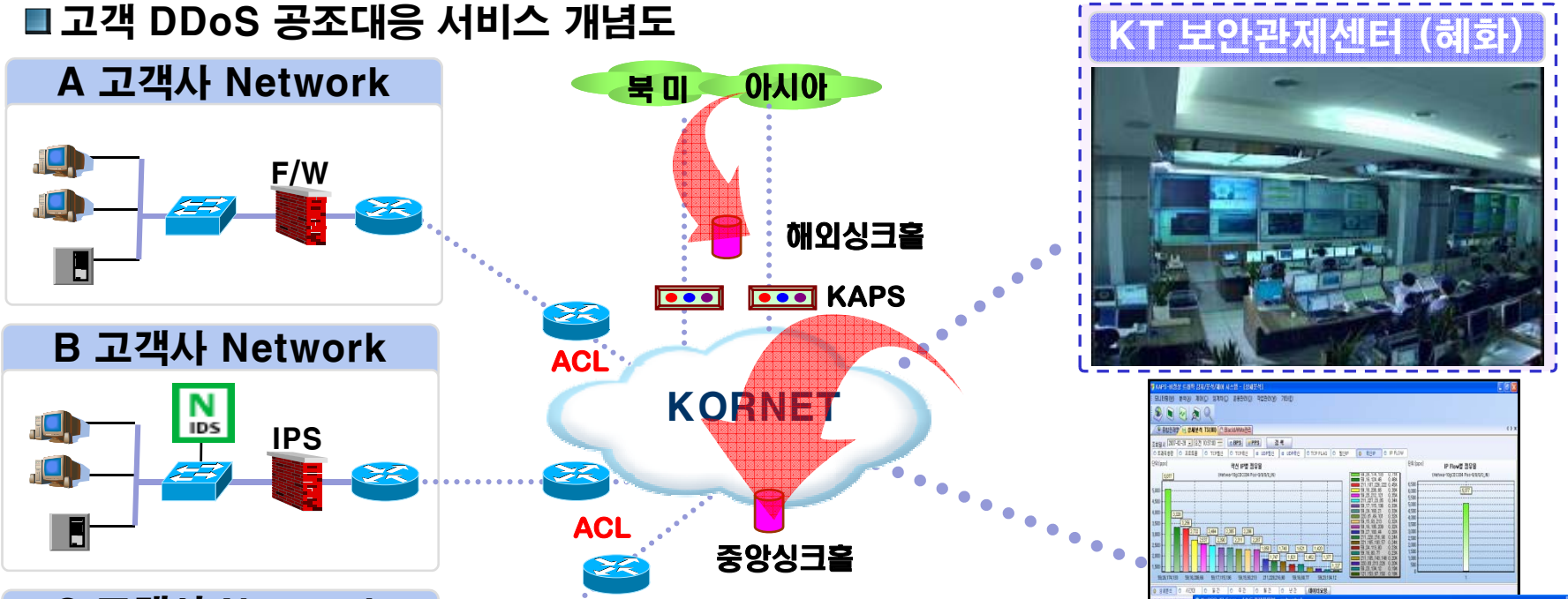
- 유해 트래픽 탐지
- 유해Traffic확인
- 유해트래픽 경로우회
- Filtering
- 정상 Traffic의 고객전송



IV. 전사 DDoS 침해사고 대응방안

고객사와 KT 보안관제센터와의 긴밀한 협조 체계를 통하여 대규모 DDoS 공격에 대한 실시간 감시 및 공조 대응으로 고객 주요 서버/네트워크 시설을 보호하고 피해를 최소화하는 공조 대응 서비스

■ 고객 DDoS 공조대응 서비스 개념도



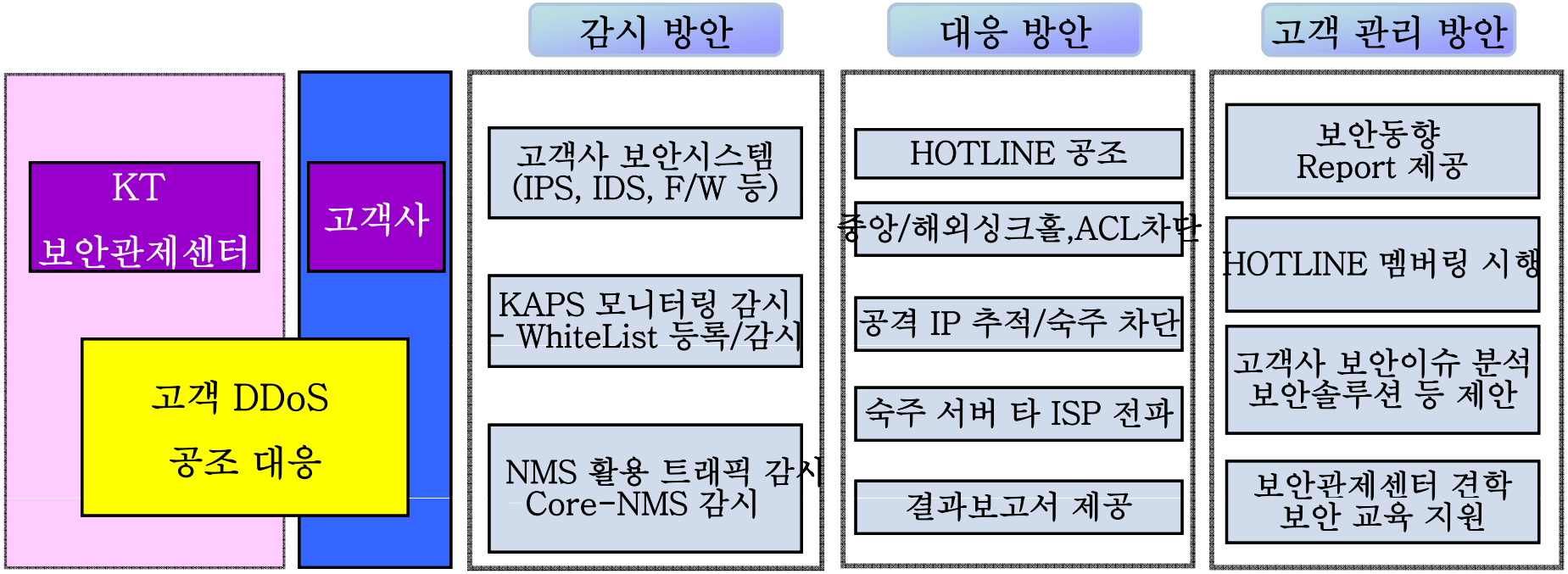
- 대상고객 : 대형 고객 (금융권, 대형기업, 포털, 공공기관등)
  - 조건 : 자체 보안시스템 구축, 보안팀 구성 대형고객
  - 최근 DDoS 공격에 대한 이슈가 있는 고객/ KT 기업용 인터넷 전용회선 고객
  - 협조 사항 : 최근 다양한 형태의 DDoS 공격은 고객 보안 시스템을 통한 자체 관제 중요

IV. 전사 DDoS 침해사고 대응방안

고객 DDoS 공조 대응 추진 범위

- KAPS 보안시스템 활용 고객 WhiteList 감시 ➔ 대규모 DDoS 사전 인지
- NMS(CORE NMS) 활용 고객 회선 감시 ➔ 고객 회선별 이상트래픽 인지
- 싱크홀, ACL 활용 DDoS 차단 ➔ 대규모 DDoS 트래픽 차단
- 공격 악성코드 분석 및 숙주 서버 차단 ➔ 고객 DDoS 2차 공격 재발 방지
- 고객 <-> 보안관제센터간 실시간 공조 대응 ➔ ISP 공조로 신속 상황 통제 가능

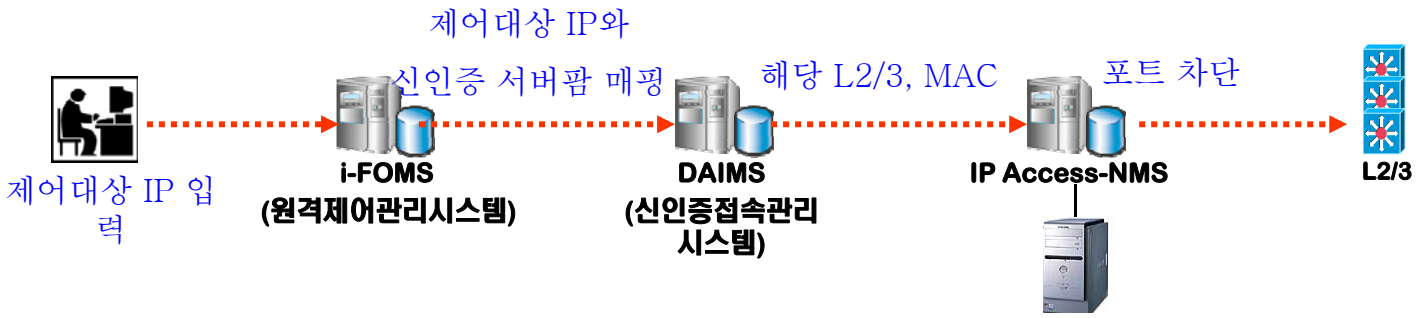
※ 트래픽 관제 및 샘플링 보안관제로 WEB 세션 공격, 공격IP 등은 KT 미인지 가능
(고객사 보안시스템 활용 초동 공조 대응 필요)



IV. 전사 DDoS 침해사고 대응방안

❑ 좀비PC 인터넷접속 차단절차

차단 절차	소요시간 및 방법		단축 시간
	현행	개선	
공격PC IP 추출	1시간	0.5시간	0.5시간
	▪ 라우터에서 Netflow 시행 ▪ 공격IP 선별추출	▪ 중앙 DDoS 전용장비 구축 ▪ 공격시스템 IP 추출	
IP정보 추출	6시간	0.5시간	5.5시간
	▪ KAMS (대량 IP조회 기능부재)	▪ IP운용센터 접속제공플랫폼 DB 추출	
해당지역 및 L3 검출	3시간	1시간	2시간
	▪ IP별 조회 (DAIMS) ▪ L3 및 수용포트 확인	▪ 시스템화 (i-FOMS) – 좀비PC 차단기능개발 (12월)	
차단작업	3시간	1시간	2시간
	▪ L3 수동접속 ▪ 수작업에 의한 MAC/포트 차단	▪ 시스템화 (i-FOMS) – 좀비PC 차단기능 개발(12월)	
총 소요시간	13시간	3시간	10시간



DDoS 공격의 효율적 대응을 통한 유사 시 서비스망의 가용성을 확보함으로써 안정적인 서비스 제공을 통한 고객 신뢰 제고에 기여