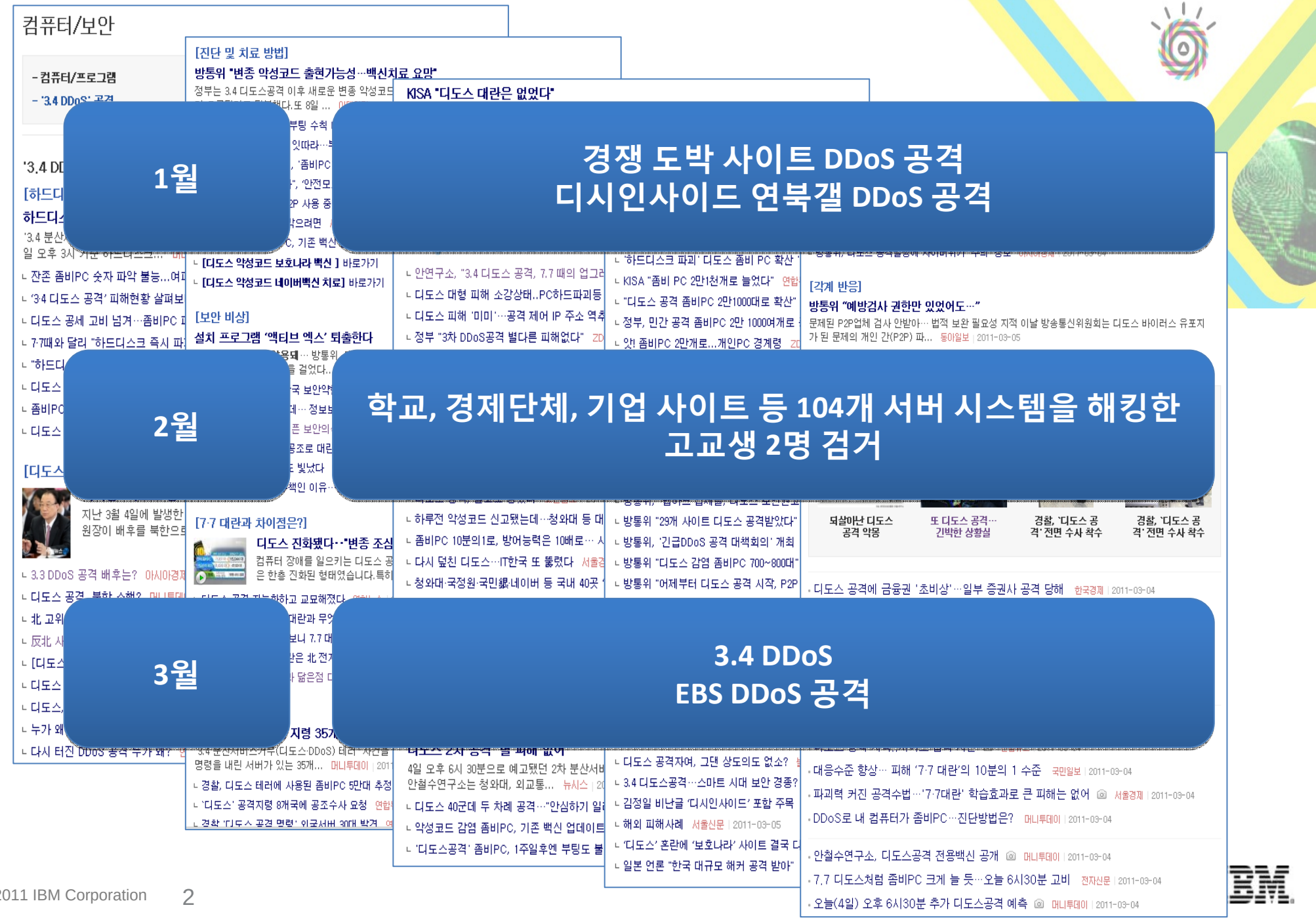
# DDoS 공격 대응의 새로운 패러다임

Cloud, Cluster, RealTime and WireSpeed

2011/05/18
Woo-Kyum Kim, AhnLab Inc.

IBM Security Summit
IBM Security Solutions. Secure By Design.



# DDoS 공격 대응의 새로운 패러다임

Cloud, Cluster, RealTime and WireSpeed

2011/05/18
Woo-Kyum Kim, AhnLab Inc.

IBM Security Summit
IBM Security Solutions. Secure By Design.

# Agenda

- 진화하고 있는 보안 위협 동향
- DDoS 공격 방어, 그리고 예방의 요건
- 새로운 DDoS 공격 방어 패러다임
- Summary

# History of Wars

**과거 전쟁 : Wall 을 기점으로 공격 vs 수비**

**냉전 종식 후 : 국지전, 테러 형태로 변화**

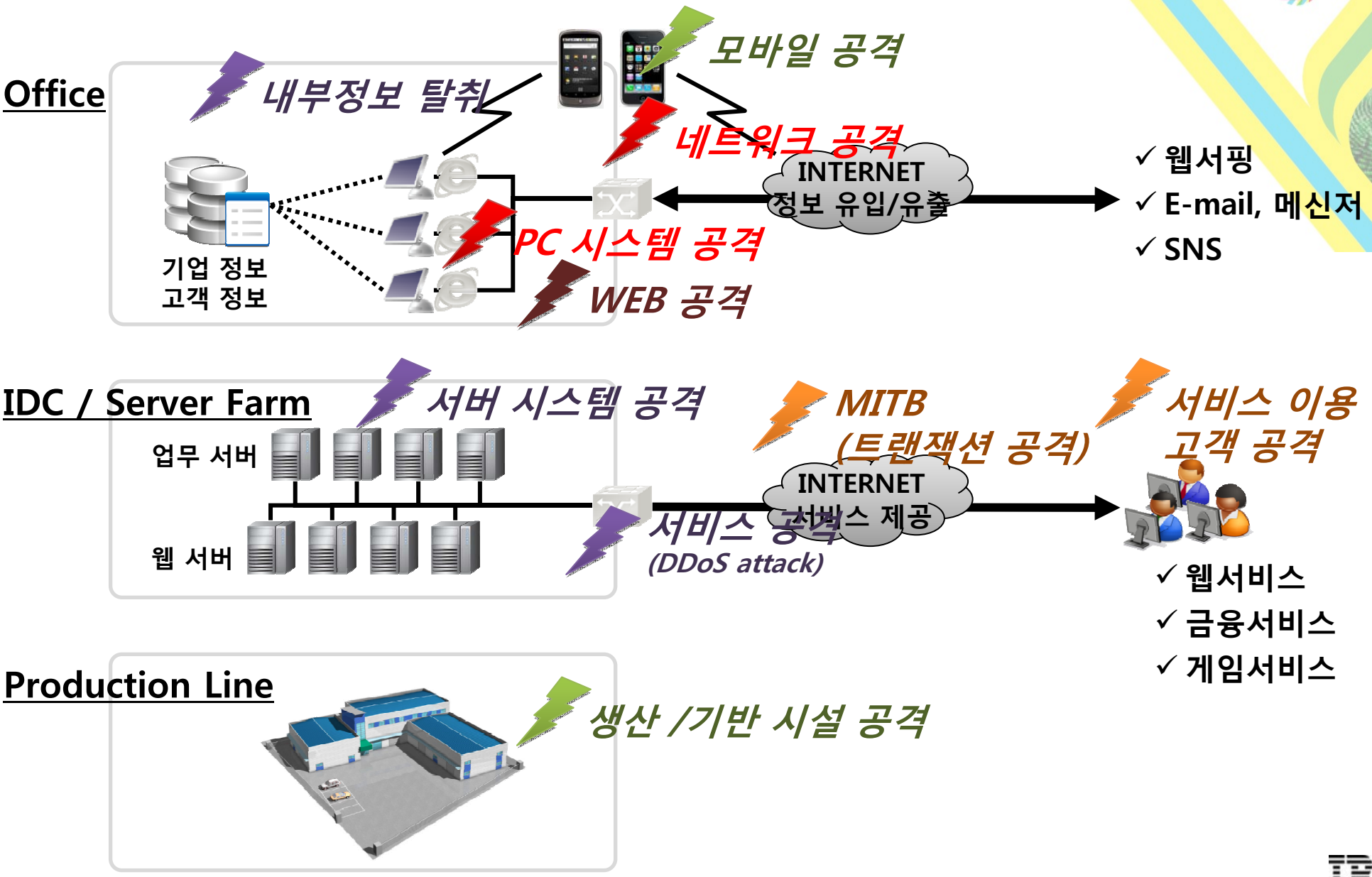
# 실제 전쟁 vs 사이버 전쟁


**사이버 공격은 조직적, 지능화**
**범행 장소는 사람이 많은 WEB**



6

# 입체적, 지능화된 공격으로의 변화



# 보안 위협 동향 – 2010년 vs 2011년

## 2010년도 보안 위협 동향

| | | |
|---|---|---|
| 사회 기반시설을 노린 스턱스넷 (Stuxnet) | 스마트폰 보안 위협의 현실화 | 정보의 허브 SNS, 악성코드의 허브로 악용 |
| 국제적 이슈 악용한 사회공학 기법 만연 | 악성코드 배포 방식의 지능화 | 제로데이 취약점 |
| 개인정보 노출의 2차 피해 | 금전 노린 악성코드에도 '한류' 열풍 | 온라인 게임 해킹 툴 급증 |

**DDoS 공격용 악성코드의 변종 등장**

## 2011년도 보안 위협 전망

| | |
|---|---|
| 제로데이 공격 기법 고도화 | 무선 인터넷 취약점 노린 공격 등장 |
| 클라우드, 가상화 기술 이용한 위협 등장 | 금전 노린 스마트폰 위협 증가 |
| 사회기반시설 겨냥한 타깃형 공격 증가 | SNS 활용한 다양한 공격 범용화 |

**DDoS 공격 지능화**



8

# 보안 위협 사례 #1

Zeus PKG 구매
맞춤 제작

↓

위장 메일 발송

↓

Zeus 감염

↓

금융 정보 탈취

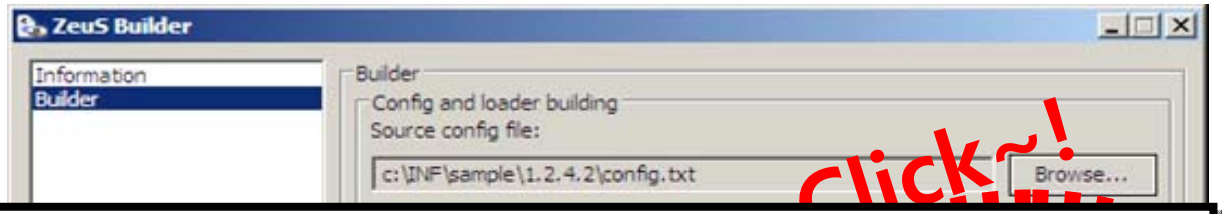
↓

또 다른 공격

✓ $3~4,000 정도로 Zeus Kit 구매

✓ 공격 Target, 공격 종류 등 설정

✓ 맞춤형 Zeus 제작 (기하급수적 Zeus 변종 발생)




Config.txt

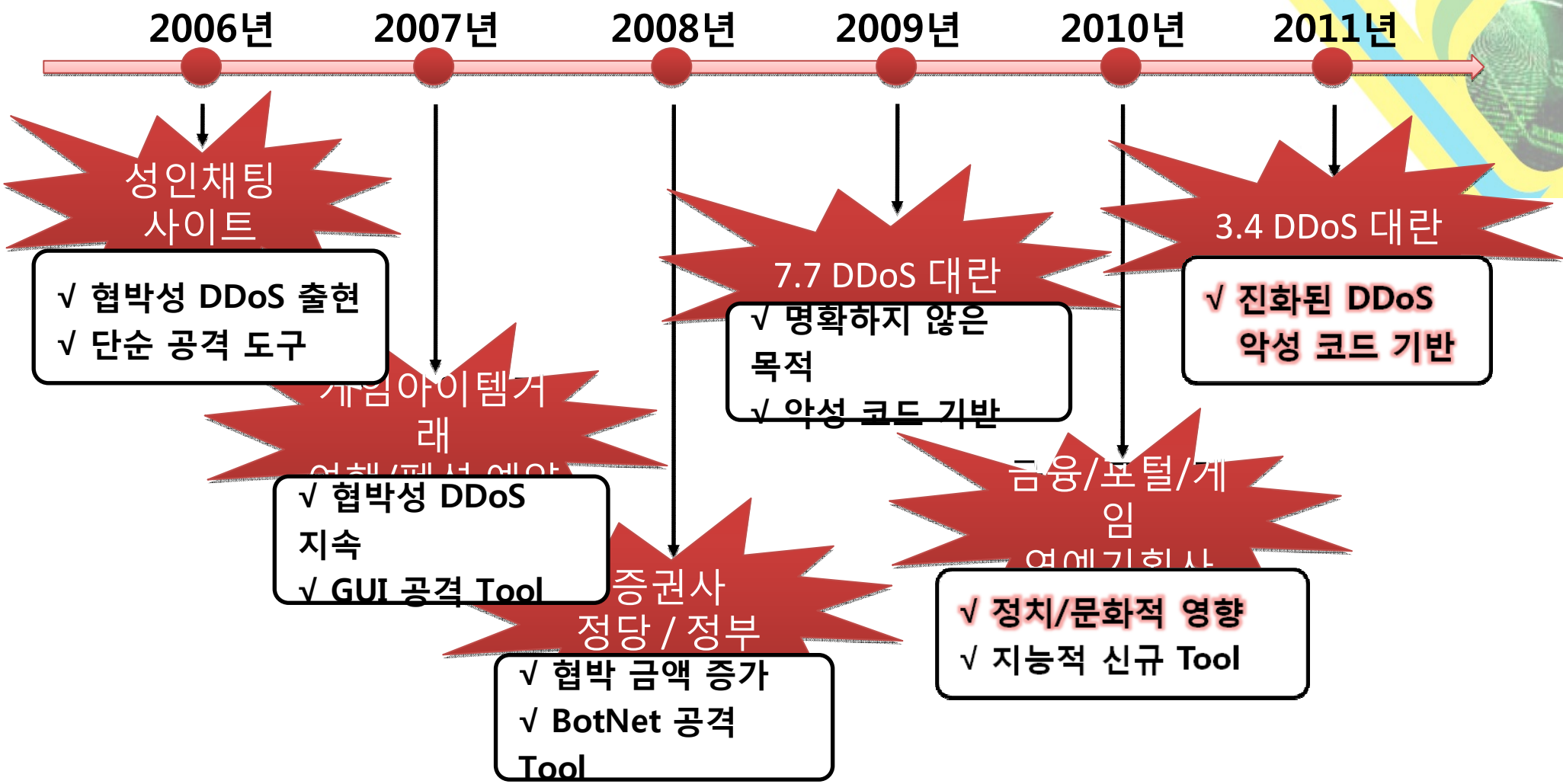
```
entry "WebDataFilters"
  ;"http://mail.rambler.ru/*" "passw;login"
end

entry "WebFakes"
  ;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""
end

entry "TANGrabber"
  "https://banking.*.de/cgi/ueberweisung.cgi/*" "S3R1C6G" "*&tid=*" "*&betr
  "https://internetbanking.gad.de/banking/*" "S3C6" "*" "*" "KktNrTanEnz"
  "https://www.citibank.de/*/jba/mp#/SubmitRecap.do" "S3C6R2" "SYNC _ TOKEN
end

entry "DnsMap"
  ;127.0.0.1 microsoft.com
end
```

# 보안 위협 사례 #2

## 악성 코드 기반 보안 사고도 DDoS 사고를 동반할 가능성이 매우 높음


**사회 공학적 기법의 악성 코드 유포 → Zombie 감염 → DDoS 등 보안 사고 유발**

# 국내 DDoS 공격 현황




**DDoS 공격 목적의 변화/변질/범죄화 + DDoS 공격 목표의 확대**

# DDoS 공격의 과거, 현재, 그리고 미래

지속적인

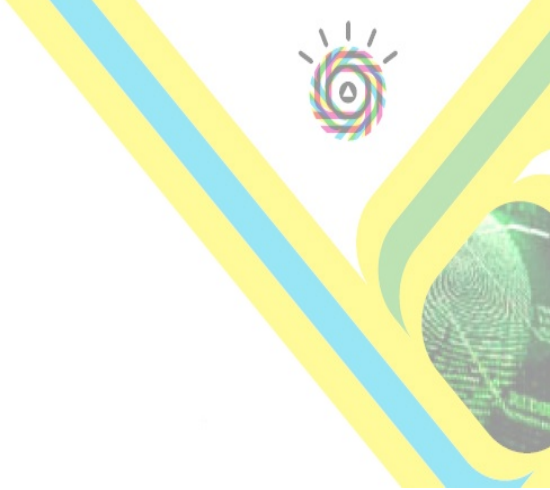
다양한

새로운 공격툴과

악성 코드 유포와 DDoS 의 전문화

# Agenda

- 진화하고 있는 보안 위협 동향
- DDoS 공격 방어, 그리고 예방의 요건
- 새로운 DDoS 공격 방어 패러다임
- Summary



# 국내 웹 사이트 위협 현황

## ※ 공공기관 웹사이트 침해 사고 현황

◆ 행정안전부 '2009 국가정보화에 관한 연차보고서' 기준

정부 및 지자체 운영 웹사이트 1600여개의 보안수준은 65.6%로, 경유지 악용 984건, 홈페이지 변조 228건

■ 지난해 공공기관 사이버 사고 (단위 : 건)

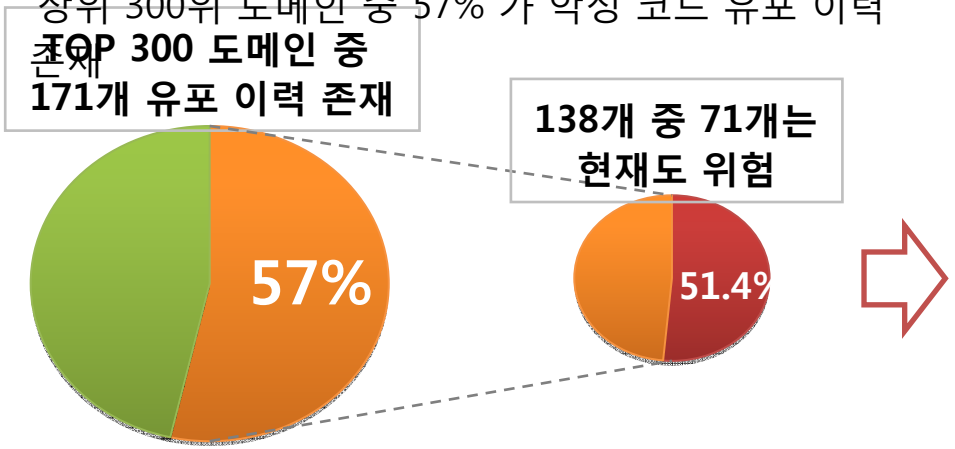
| 구 분 | 웜·바이러스 감염 | 경유지 악용 | 홈페이지 변조 | 자료훼손 및 유출 | 기타 | 합계 |
|---|---|---|---|---|---|---|
| 국가기관 | 813 | 67 | 23 | 204 | 80 | 1187 |
| 지방자치단체 | 2443 | 224 | 64 | 283 | 53 | 3067 |
| 연 구 소 | 698 | 31 | 6 | 65 | 18 | 818 |
| 교육기관 | 1210 | 454 | 82 | 73 | 48 | 1867 |
| 산하기관 | 418 | 104 | 36 | 92 | 22 | 672 |
| 기 타 | 73 | 104 | 17 | 72 | 88 | 354 |
| 합 계 | 5655 | 984 | 228 | 789 | 309 | 7965 |

〈자료 : 행정안전부〉

## ※ AhnLab SiteGuard 수집 통계

◆ 코리안클릭 UV Top 300 도메인 검사 결과,

상위 300위 도메인 중 57% 가 악성 코드 유포 이력 존재



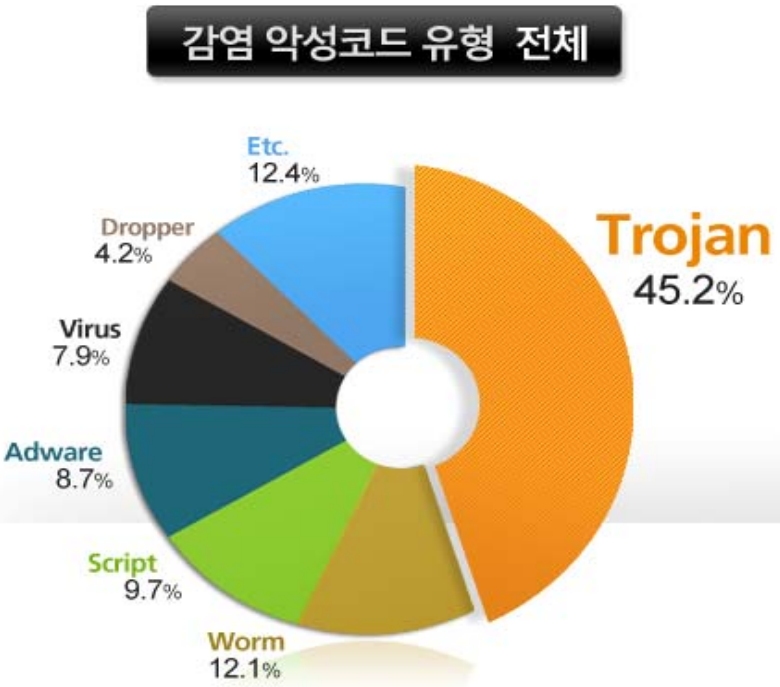

| UV 순위 | 위험 도메인 | 위험 URL 수 |
|---|---|---|
| 2 | da .net | 1662 |
| 10 | tis .com | 463 |
| 14 | pa .com | 203 |
| 1 | na .com | 194 |
| 3 | na com | 60 |
| 35 | egloos.com | 50 |
| 8 | auction.co.kr | 35 |

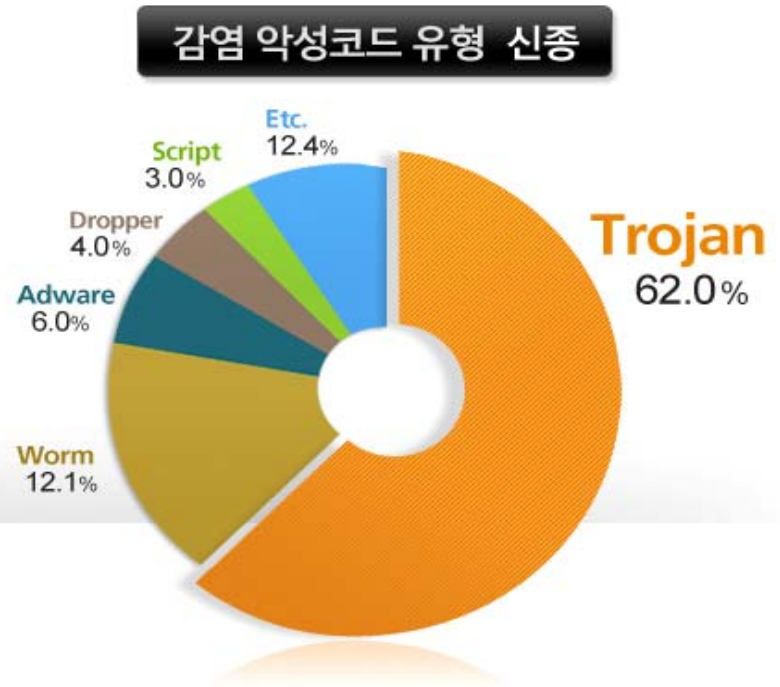
# 2010년도 악성코드 유형 분포 통계

- 2010년에 **감염 보고된 악성코드 유형을** 살펴보면, **트로잔(Trojan)류가 45.2%**로 가장 많았으며,

웜(Worm)류가 12.1%, 스크립트(Script)류가 9.7%로 그 뒤를 이었다.

- 2010년에 처음으로 보고된 **신종 악성코드 유형에서도** 역시 **트로잔류가 62%**로



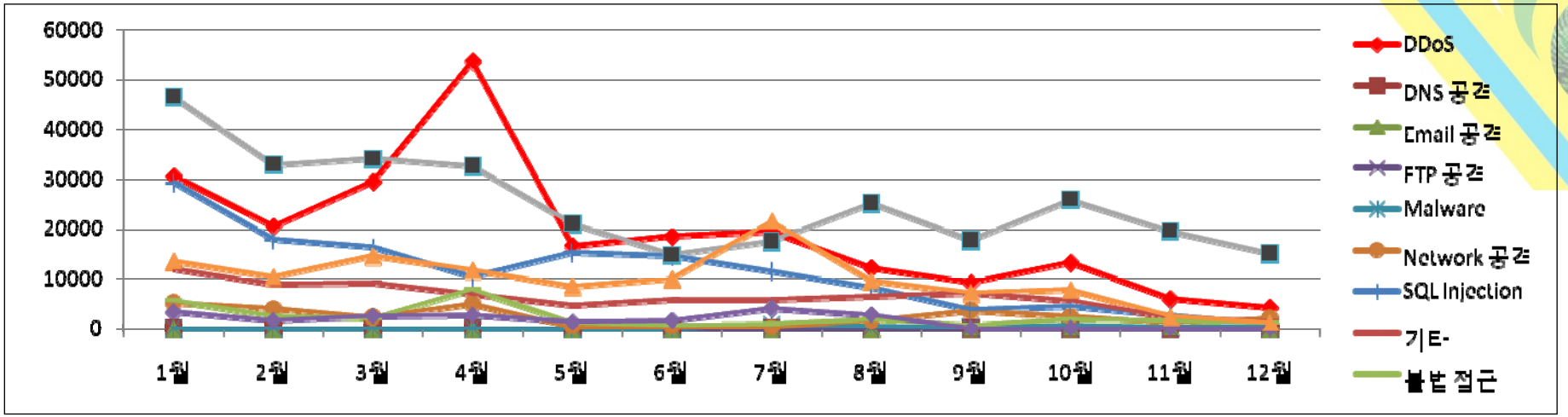






15

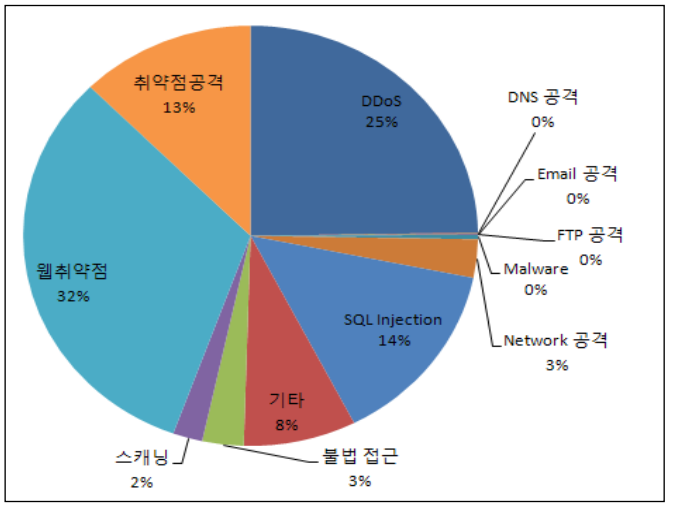
# 2010년도 Network 위협 분석 동계

## 2010년 공격 동향 분석 (출처 : 안철수연구소 CERT, 2010. 12)



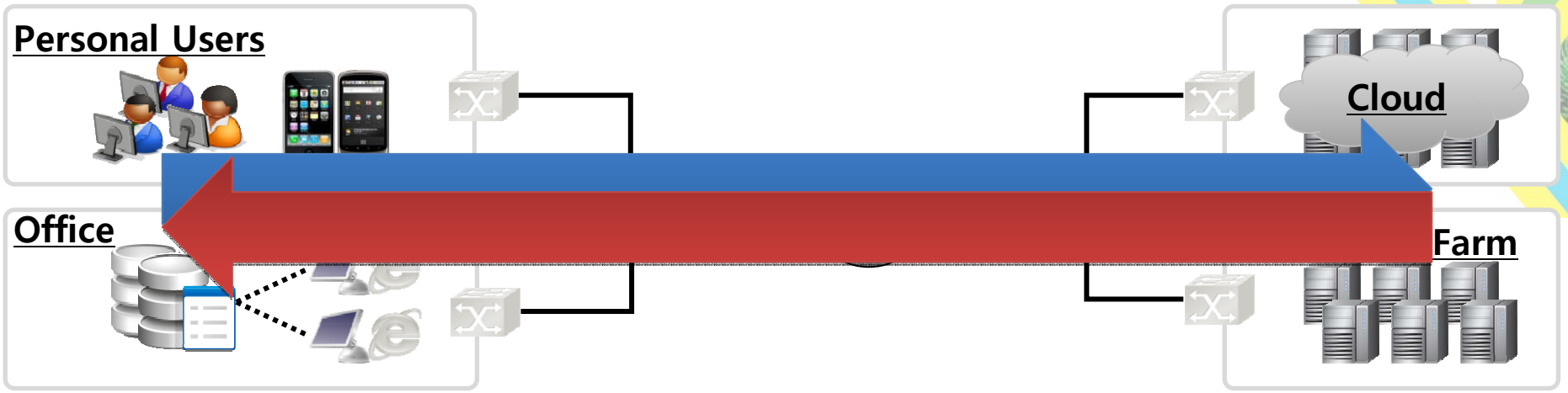

**Network 기반 전체 유효 이벤트 : 약 94만건**

| 웹 취약점 32% | DDoS 25% | SQL Injection 14% |
|---|---|---|




**다량의 Fragments/UDP/ICMP Flooding + 정밀 타격 HTTP DDoS 공격 지속 발생**

# DDoS 공격의 피해와 대응의 범위




DDoS
FW/IPS
UTM

**DDoS 공격 방어 (내부 Network)**

Outbound DDoS 방어
Service 가용성 보장

**DDoS 공격 방어 (Network**

Inbound DDoS 방어
Service 가용성 보장

DDoS
통합 DDoS 대응 체계

Anti-Virus
URL/DNS Filter
좀비 PC 대응

**DDoS 공격 예방 (Client PC)**

내부 PC 보안 수준 강화
신종 악성 코드 대응력 강화

**DDoS 공격 예방 (Server)**

서버 보안 수준 강화
악성 코드 유포 행위 방지

IPS
WAF
웹 보안 모니터링

# DDoS 공격 방어와 예방의 요건

**새로운 DDoS 공격 방어 패러다임**

**소규모 정밀 타격형 DDoS 공격**

**대규모 DDoS 공격**

**신종 DDoS 공격 도구 분석**

**DDoS 조기 경보 및 긴급 대응**

**DDoS 공격 방어 프로세스 확립**

**새로운 DDoS 공격 예방 패러다임**

**평시 보안 수준 확립 및 유지**

**C&C Server 탐지 및 방어**

**유해 URL 접근 탐지 및 방어**

**신종 악성 코드 선제 대응**

**DDoS 공격 예방 프로세스 확립**

**System – Network – Operation Level**
**융복합적 보안 위협 대응 체계 필요**



18

# Agenda

- 진화하고 있는 보안 위협 동향
- DDoS 공격 방어, 그리고 예방의 요건
- 새로운 DDoS 공격 방어 패러다임
- Summary

# 7.7 DDoS vs 3.4 DDoS

| | 7•7 DDoS (2009) | 3•4 DDoS (2011) |
|---|---|---|
| 유포지 및 공격대상 | ✓ P2P 사이트를 통한 유포<br>✓ 청와대, 백악관 등 한국과 미국 주요 사이트 | ✓ P2P 사이트를 통한 유포<br>✓ 청와대, 네이버 등 국내 주요 사이트 |
| 공격형태 | ✓ 7일부터 사흘간 공격 지속<br>✓ 같은 파일 구성에 의한 공격 | ✓ 공격자에 의해 변화<br>✓ 공격 때마다 변화하는 파일 구성 → 분석의 어려움 증가 |
| 하드디스크 손상 | ✓ 지정된 마지막 공격날짜에 하드디스크 손상.<br>✓ PC 날짜 변경 시, 이상 없음. | ✓ 공격자가 임의로 날짜를 변경하며 하드디스크 손상.<br>✓ 감염시간보다 이전으로 시간을 변경하는 경우 하드디스크 손상. |

**진화된 DDoS 유발 악성 코드로 인한 3.4 DDoS 공격 발생**

# 7.7 DDoS vs 3.4 DDoS

| | 7•7 DDoS (2009) | 3•4 DDoS (2011) |
|---|---|---|
| 좀비 PC 수 | ✓ 115,044대 (정부 발표) | ✓ 116,299대 (정부 발표) |
| HTTP 공격 특징 | ✓ HTTP 1.1<br>✓ 1 HTTP Request / 1 TCP Session<br>✓ URL Redirect 반응 안함<br>✓ Cache-Control 사용 & 사용안함<br>✓ User-Agent 변경 | ✓ HTTP 1.1<br>✓ 1 HTTP Request / 1 TCP Session<br>✓ URL Redirect 반응 안함<br>✓ Cache-Control 사용 & 사용안함<br>✓ User-Agent 변경<br>✓ Accept 변경 |
| UDP /ICMP | ✓ Src IP Spoofed & Non-Spoofed<br>✓ 가변 Packet Size (4~48 Byte) | ✓ Src IP Non-Spoofed<br>✓ 고정 Packet Size<br>(UDP 1024 Byte /ICMP 204 Byte) |
| 좀비당 공격양 | ✓ 103 PPS (전체) | ✓ 389 PPS (전체) |

**3.4 DDoS 는 전혀 새로운 공격 유형이 아님 ➔ 피해 규모는 적음**

# DDoS 공격의 과거, 현재, 그리고 미래

## 과거 단순한 형태에서 정상 응답까지 가능한 매우 정교한 공격 형태로 진화


### Resource Exhausted

- Packet based Flooding
  - TCP Syn Flooding
  - UDP/ICMP Flooding
- High Technique for Attack Control
  - Using IRC Channel
  - Using Traditional Hacking Technology

### Intelligent Attack

- Various Flooding Type
  - All TCP Flag Type
  - Various Type of Packets
    1) Fragmentations
    2) Random Size
    3) Random Protocols
- Easy Technique for Attack
  - Using BotNet Channel
  - GUI Based Control

### Complicated Attack

- Combined DDoS Attack
  - Multiple Attack
- Looks like the Normal Traffic
  - Connection Based Attack
  - Slow and Steady Attack
- More Easy for Attack Control
  - Automated Zombie Creation
  - GUI Based Control
  - Black Market for contract

**√ 정상적인 HTTP 요청 트래픽을 가장한 DDoS 공격 기법 유행**

**√ 단순한 정적인 Web Site 공격에서 Dynamic Web 으로의 공격 목적지 변화**

**√ 기존의 방어 방식을 회피하는 새로운 공격 도구의 빠른 배포**

**√ 특정 목적지를 대상으로 한 소규모 정밀 타격형 DDoS 공격으로 진화**

# 최근 DDoS 공격과 대응의 변화

## 최근 DDoS 공격은 소규모 정밀 타격형 공격이거나 대규모 트래픽으로 양극화됨

| 신종 DDoS 공격 | 대역폭 고갈형 DDoS | 패킷 과다 DDoS |
|---|---|---|
| 과부하 정책 회피 | 대역폭 잠식 목적 | 패킷 처리 과부하 목적 |
| 패킷 크기가 작음 | 패킷 크기가 큼 | 패킷 크기가 작음 |
| 초당 패킷 수는 작음 | 초당 패킷 수는 작음 | 초당 패킷 수는 높음 |
| 0.1 Gbps 수준 | 수십 Gbps 의 BW | 10Gbps BW 상회 |
| ↓ | ↓ | ↓ |
| 소규모 정밀 타격형 DDoS 대응이 가능한 DDoS Solution | 수십 Gbps 대역폭이 처리 가능한 DDoS Solution | 초당 1천만 PPS 이상이 처리 가능한 DDoS Solution |

**높은 대역폭과 패킷 처리 성능이 보장되는 단일 DDoS 대응 제품은 없음**

**여러 대의 장비를 통하여 기존 HA 개념을 뛰어넘는 Cluster 등 새로운 접근 방식이 필**

# 최근 DDoS 공격과 대응의 변화

## HTTP Web 을 대상으로 한 소규모 정밀 타격형 공격의 실제 진화 사례

| ~2009년 | 2010년 | 2011년 |
|---|---|---|
| HTTP Get Flooding 공격 Tool 등장 | HTTP 1.1 Protocol 규약 이용 Multi-HTTP Request per 1 TCP Session 등장 | HTTP 1.1 Protocol 규약 이용 Multi-HTTP Request per 1 TCP Session 등장 |
| 사용자가 직접 웹 브라우저에서 F5 Refresh | HTTP Cookie 에 응답하는 공격 Tool 등장 | HTTP Get + Post Method 를 이용하는 Tool 등장 |
| 조금 더 편리하게 공격할 수 있는 웹 브라우저에서 실행 가능한 자동 Refresh Script 제작 | 자발적 공격 또는 Zombie PC 에서 유발시키는 중앙 공격 명령 형태 | 10초에 1개의 Packet 만을 발송하는 극단적인 소규모 공격 |
| **"방법 2007", "NetBot Attacker" 등** | **"69성전 Tool" 등** | **"신종 공격 Tool" 등** |

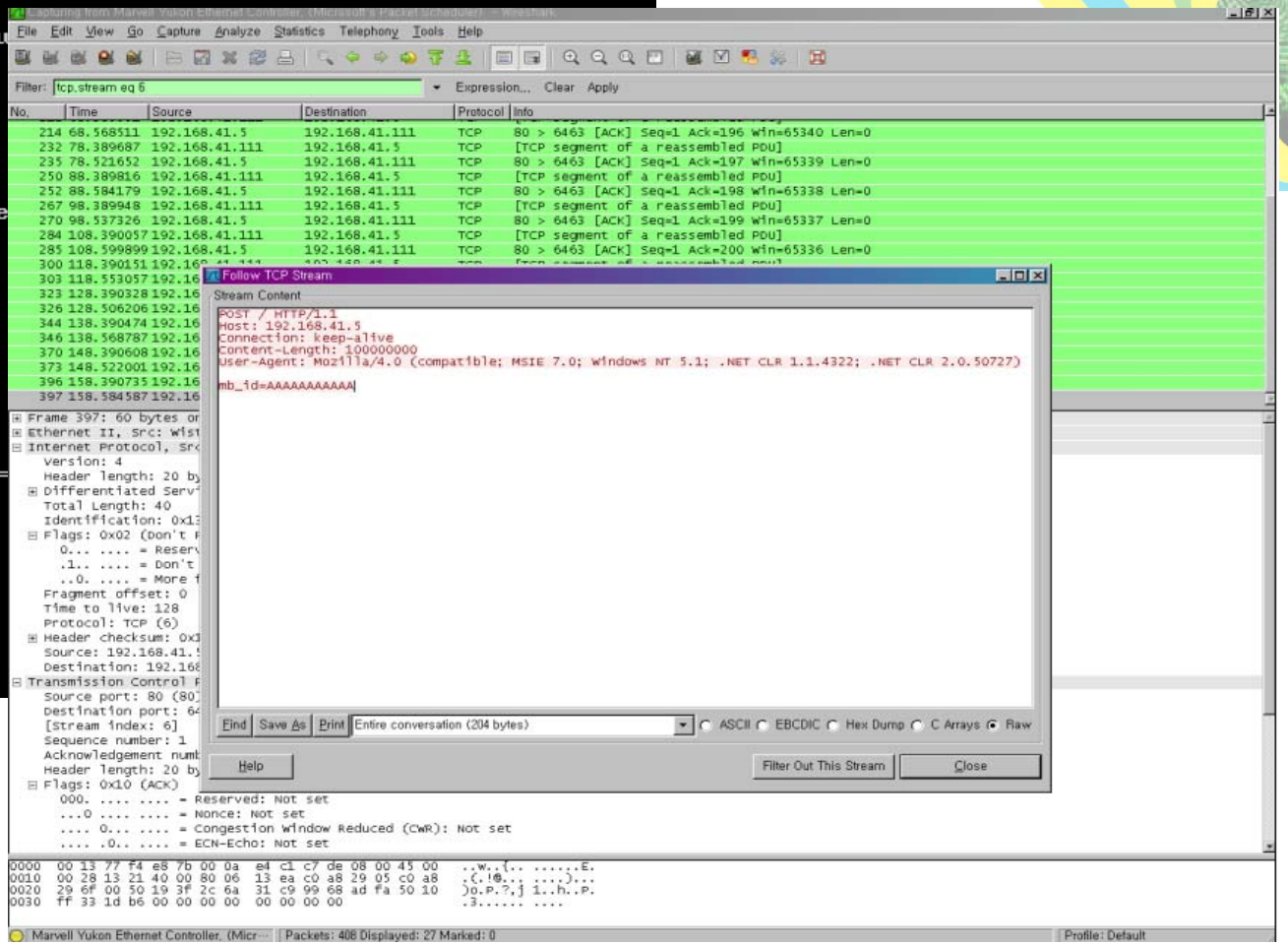
**√ 가장 사용자가 많이 접속하는 "Web" 을 대상으로 한 DDoS 공격 지속 발생**

**√ DDoS 공격 효과의 극대화 및 차단 회피를 위한 다양한 DDoS 공격**

# 최근 DDoS 공격과 대응의 변화

## HTTP 1.1 POST Method 를 이용한 신종 DDoS 공격

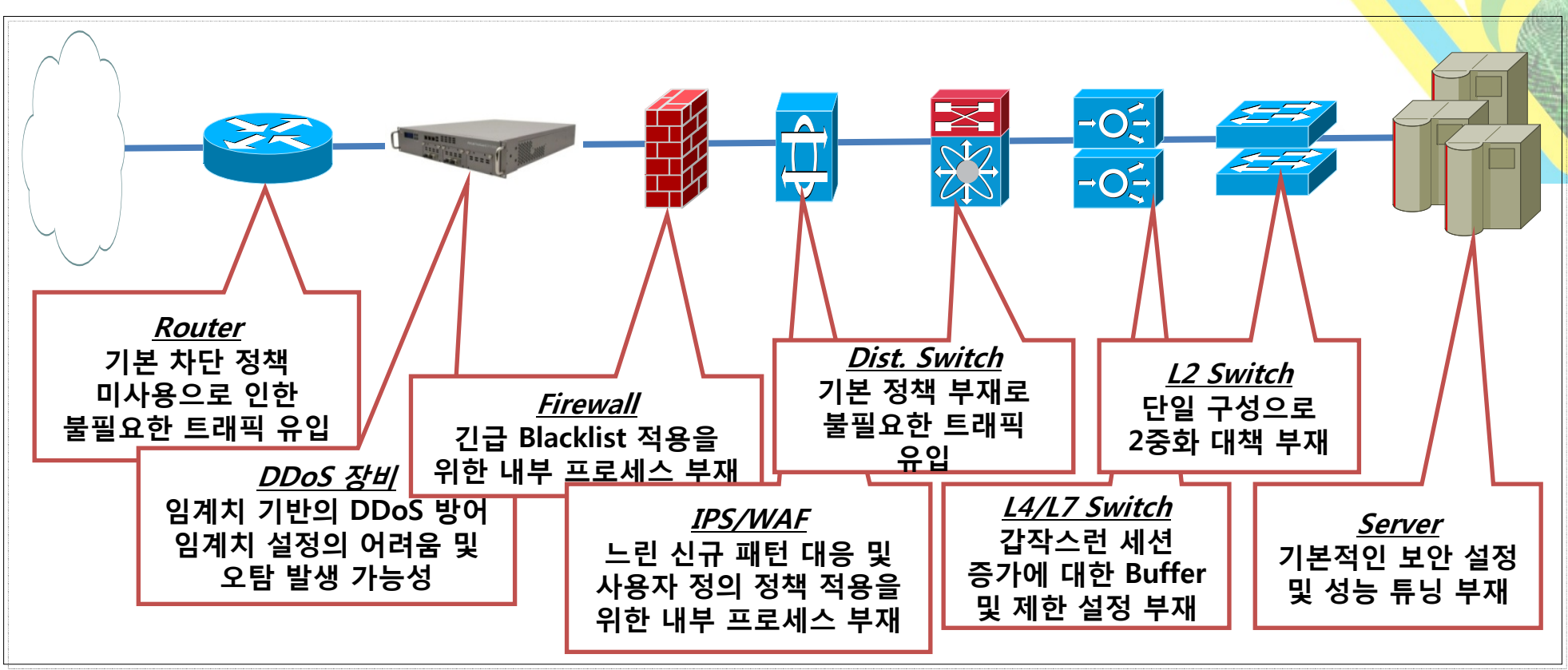
```
C:₩Python32>r-u-dead-yet-v2.2.exe http://192.168.41.5/bbs/rg4_member/login.php

Found 1 forms to submit. Please select nu

1 > http://192.168.41.5/?

> 1

Found 4 parameters to attack. Please sele

1 > form_mode
2 > ret_url
3 > mb_id
4 > mb_pass

> 2

Number of connections to spawn: (default=

> 5

Use SOCKS proxy? [yes/no] (Default=no)
>
[!] Attacking: http://192.168.41.5/?
[!] With parameter: ret_url
```




**DDoS 공격의 고도화 : Session Based 의 Slow 기반 DDoS 공격으로 지속 진화**

# DDoS 공격으로 인한 피해

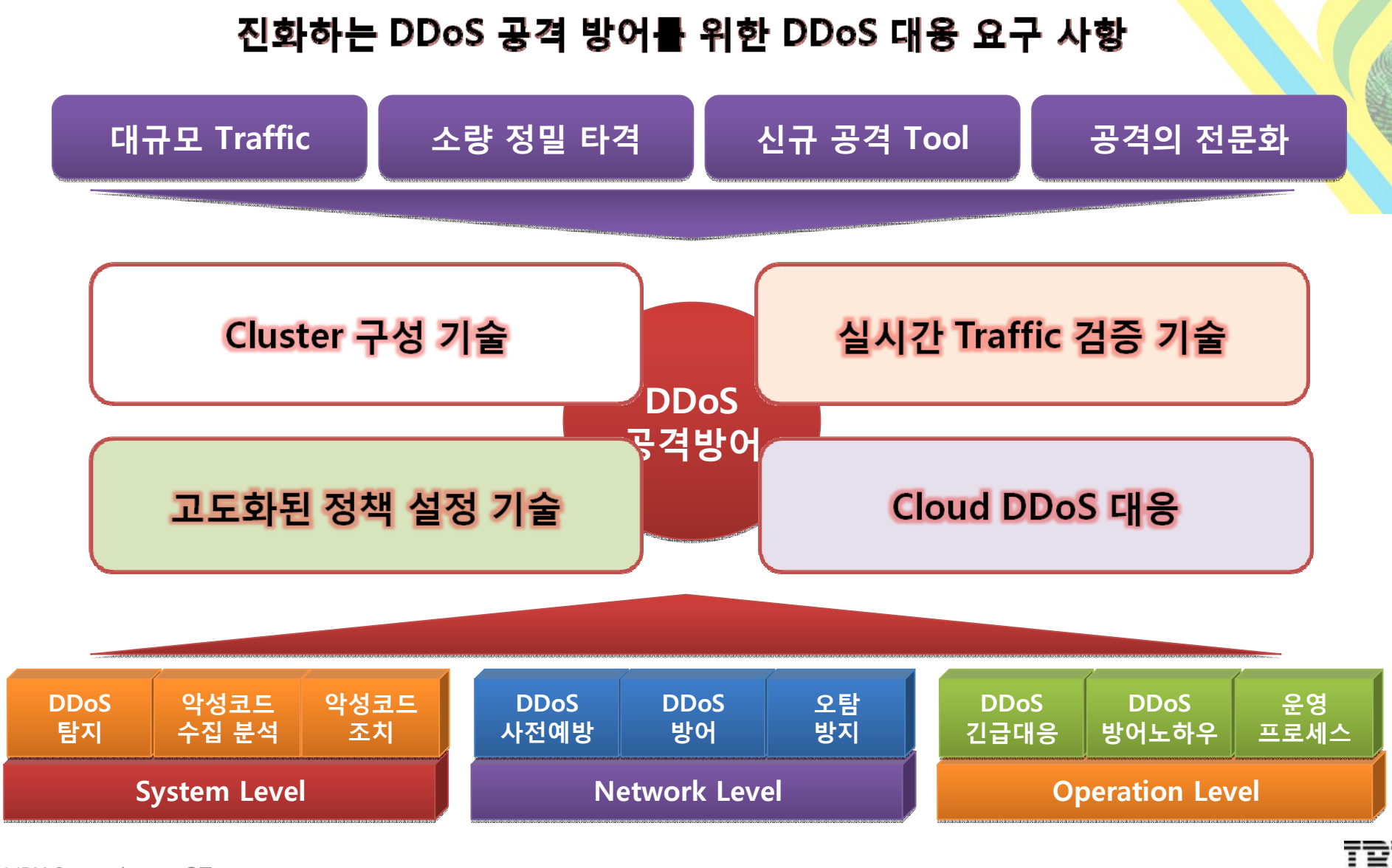
## DDoS 공격의 피해는 전체 Service 인프라에 영향을 줌




**기본 DDoS 대응 조치가 없을 경우 순간적으로 유입되는**

**소량의 DDoS Traffic 로 인하여 서비스 가용성에 영향을 미칠 수 있음**

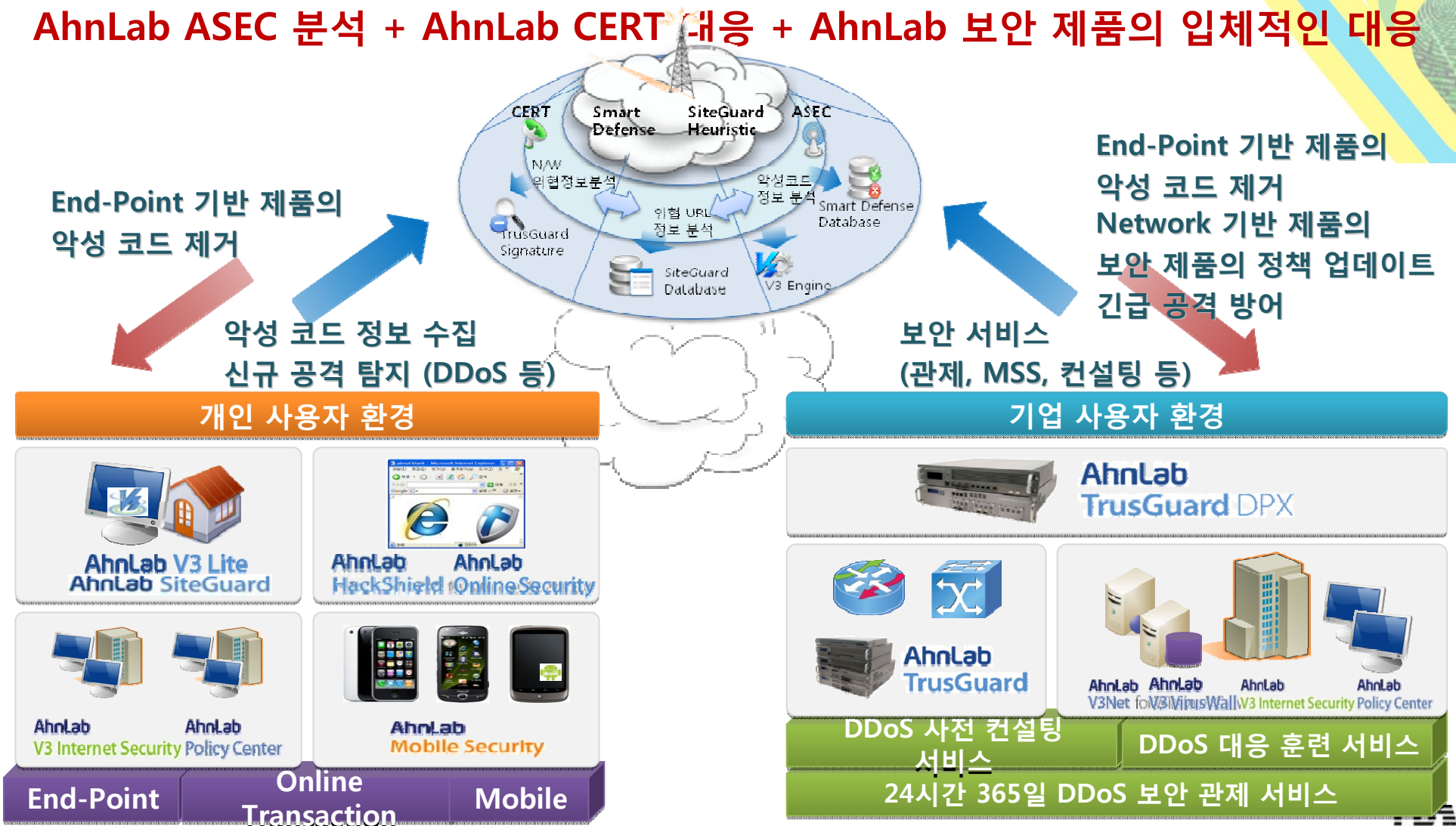
# DDoS 공격 방어를 위한 요구 사항



# DDoS 대응 전략 – ACCESS 전략

**ACCESS : 클라우드 컴퓨팅 기반의 입체적인 보안 대응 체계**

**AhnLab ASEC 분석 + AhnLab CERT 대응 + AhnLab 보안 제품의 입체적인 대응**



# DDoS 대응 전략 – TrusGuard DPX 의 주요 특징

## AhnLab TrusGuard DPX 의 종합적인 DDoS 공격 대응 프로세스

### 신규 공격 분석 및 사전 예방

- AhnLab 의 Security Agent 기반 중심의 악성코드 수집 및 분석
- Agent 기반 DDoS 모니터링 시스템 연동
- PC/서버 Zombie 화 방지 Signature 제공
- 신규 공격 유형 방어정책 Update 및 권고

### 다양한 DDoS 공격 유형 방어

- 상세한 Traffic 유형별 정책 설정 기능
- Traffic 유형별 다양한 DDoS 공격방어
- DDoS 의 단방향성 트래픽 특성에 맞는 탐지/차단의 WireSpeed 성능 제공

### 운영 프로세스 제공

- 사전 DDoS 컨설팅 서비스 및 DDoS 모의 공격 대응 훈련 서비스를 통한 운영 프로세스의 가이드라인 제시
- DDoS 보안 관제 서비스를 통한 TrusGuard DPX 의 운영 대행 및 긴급 대응 프로세스 제공

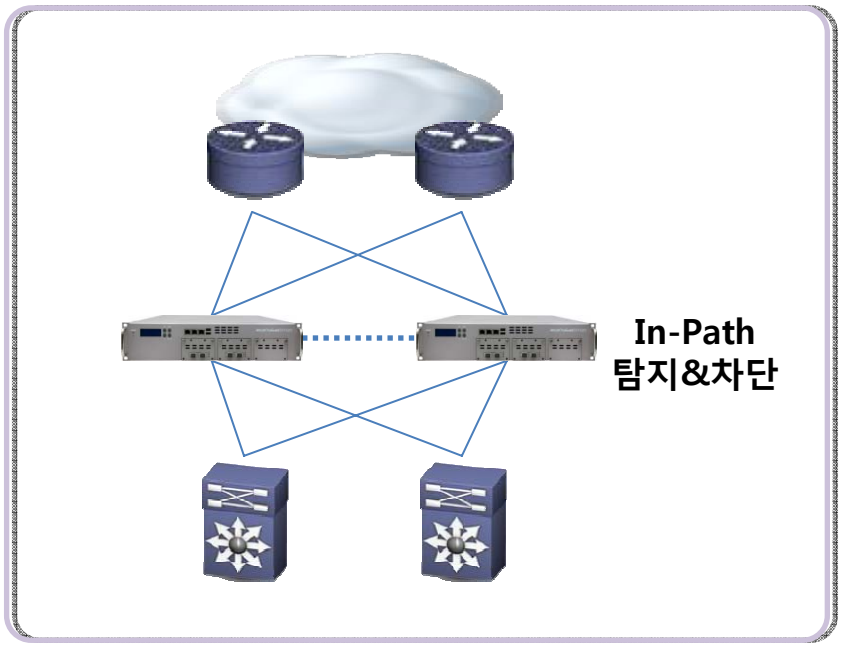
### 오탐 회피 기능 제공

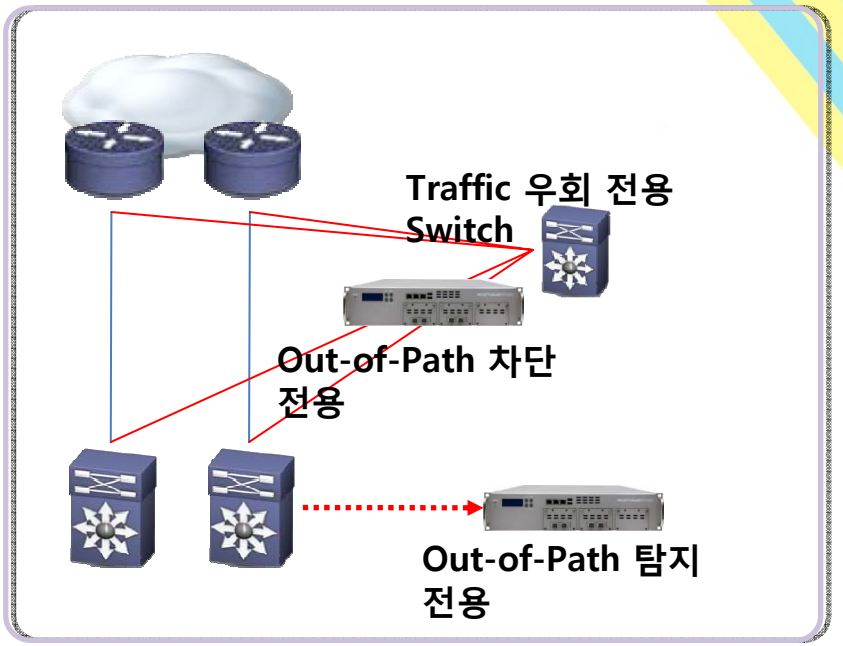
- 자동 학습 기능을 통한 Traffic 유형별 Source IP 임계치 자동 설정
- TCP Session 및 HTTP 의 정상 트래픽과 비정상 트래픽의 정확한 판단
- DDoS 공격 방어 동작 중 오탐의 최소화 기능 제공

# TrusGuard DPX 의 DDoS 공격 방어 기능

# DDoS 대응 전략 - Cluster & WireSpeed

## Inline 구성 방식과 Out-of-Path 구성 방식을 동시에 지원




√ Network 형태별 적합한 구성 방식 선택 가능 (Out-of-Path License)

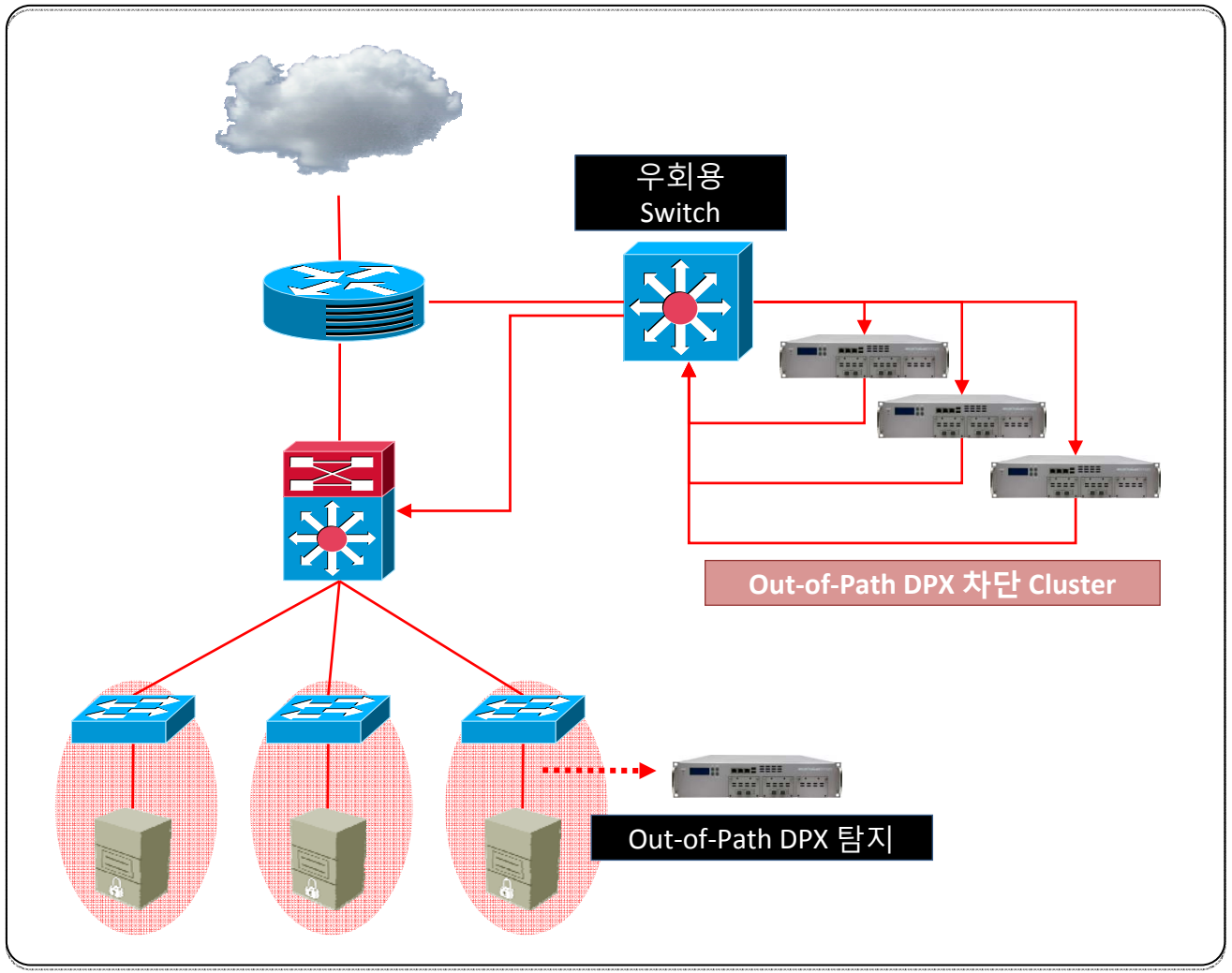
√ Bypass 가 내장된 1G/10G Interface 제공 (TrusGuard DPX 6000 기준)

√ In-Path / Out-of-Path 모두 동일한 공격 방어 기능 제공 (HTTP 검증 기능 포함)

√ Cluster 구성을 통한 대규모 DDoS Traffic 처리 가능

# DDoS 대응 전략 - Cluster & WireSpeed

## Cluster 구성 방식을 통한 대규모 DDoS Traffic 방어 (최대 12대 동기화)




**Cluster 구성**

- B/W 고갈형 공격 (Max 120 Gbps+)
- Packet Flood 공격 (Max 10M PPS)
- 장애 대응 (다중 장비 방어)
- 유연한 확장 (일시 증설)
- 관리의 일원화

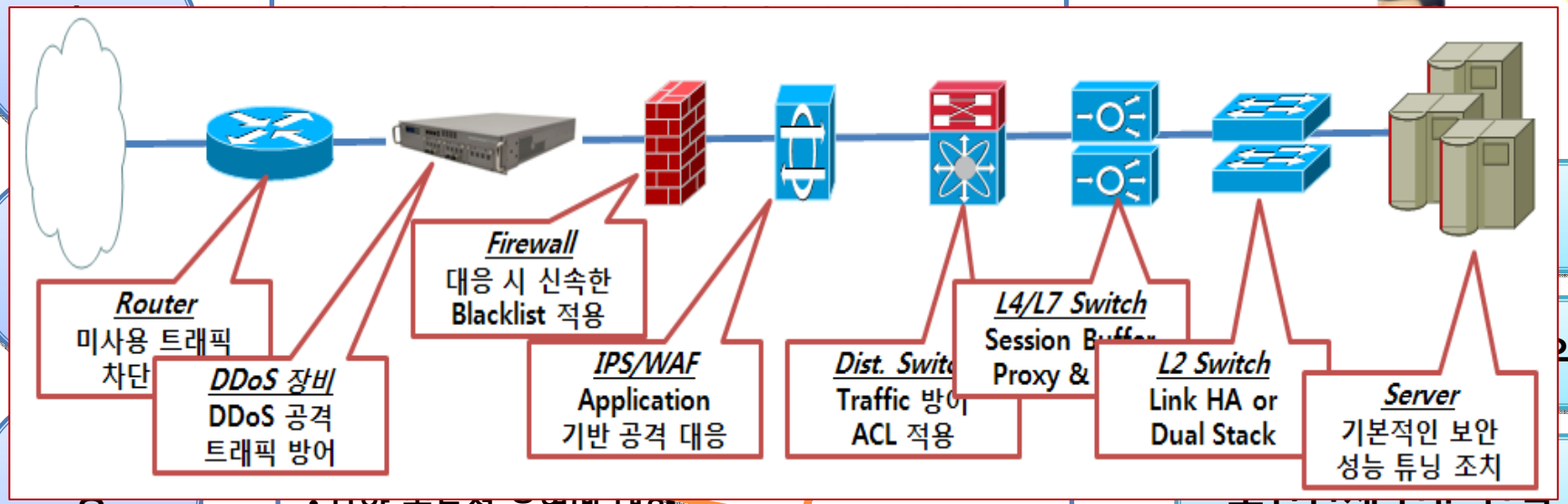
***안정된 서비스 기반의 다양한 DDoS 공격 대응***

# DDoS 대응 전략 - Cloud & Operation Process

## 담당자의 고민

증가하

• 상업화(개인정보 거래를 위한 Black Market 형성)




한계

• 침해 시도에 대한 실시간 대응체제의 어려움
• 야간/휴일 대비 체제 미흡

**기업은 핵심 비즈니스에 모든 역량을 집중하고,**
**이를 위한 보안관리는 전문가에 맡기는 것이 효율적!!**

# DDoS 서비스 상품을 통한 운영 프로세스 제공

## 사전 예방 + DDoS 대응 운영 + DDoS 대응 가이드라인 + DDoS 모의 대응 훈련

**Take 1**

DDoS 방어 전용 장비

**Take 2**

시큐리티대응센터(ASEC)

**Take 3**

보안 관제 서비스

**Take 4**

보안 컨설팅

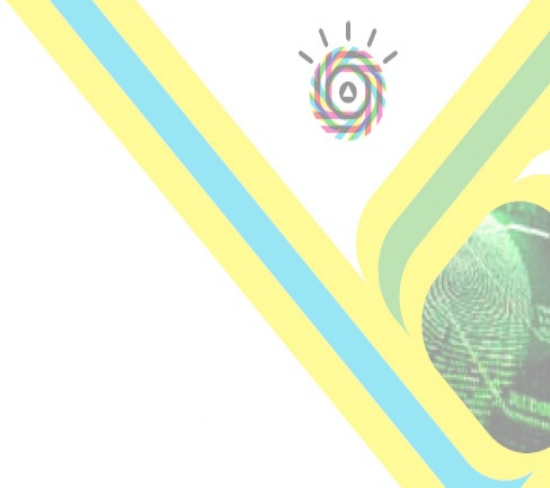
| 신규 DDoS 공격 분석 및 방어 연동 | DDoS 사전 컨설팅 서비스 상품 | DDoS 모의 공격 대응 훈련 서비스 상품 | DDoS 보안 관제 서비스 상품 |
|---|---|---|---|
| System Level 의 DDoS 유발 악성 코드 분석 및 대응 정책 제공 | DDoS 와 관련한 보안 수준 점검 및 DDoS 공격 대응 가이드라인 제시 | DDoS 모의 공격을 통한 DDoS 대응 체계 점검 | 24시간 365일 DDoS 대응 운영의 아웃소싱 서비스 |

**√ 전문가 기반의 DDoS 공격 대응을 위한 입체적인 대응 프로세스 제공**

**√ DDoS 대응 능력의 극대화와 긴급 대응을 통한 효과적인 DDoS 대응 체계 제공**

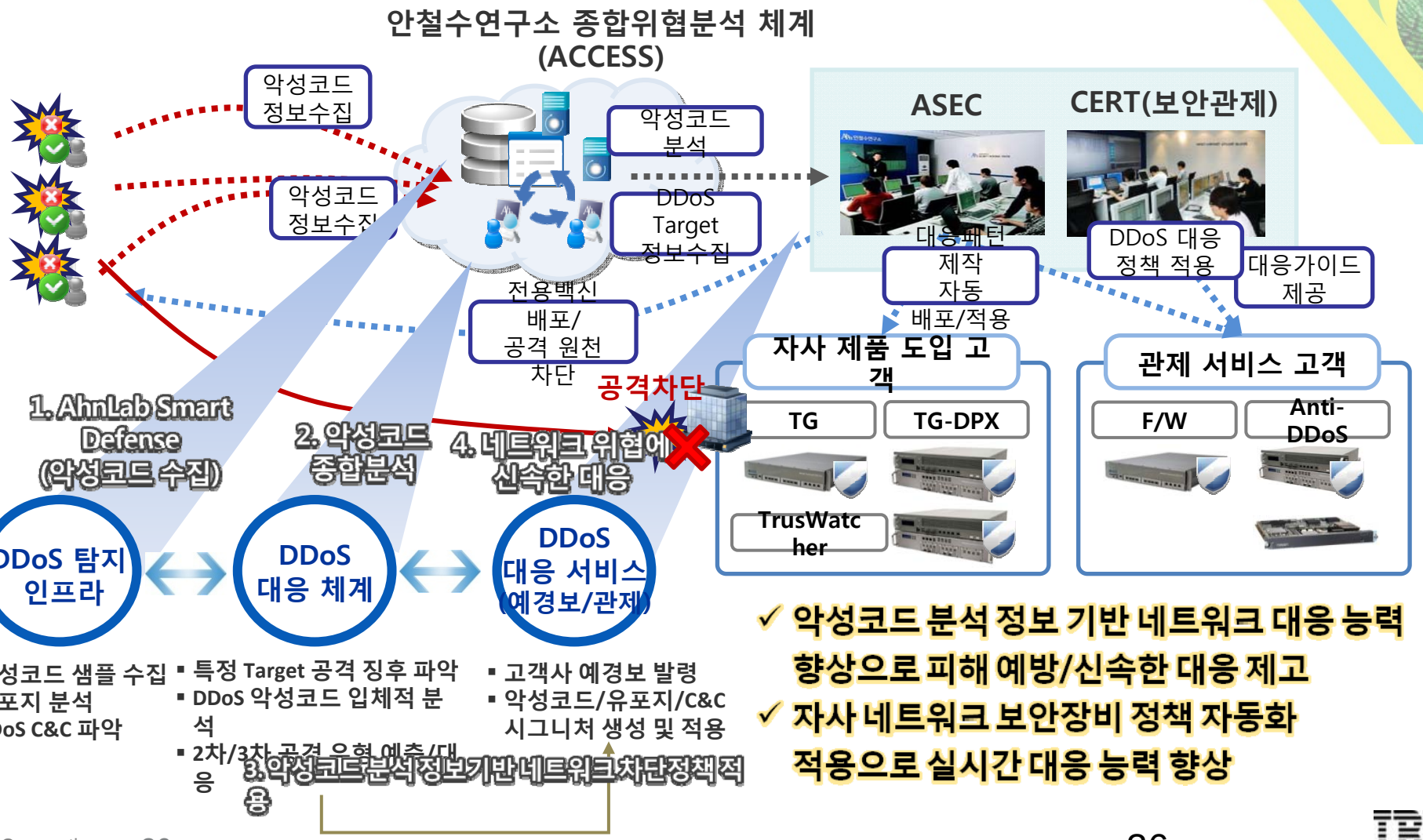
# Agenda

- 진화하고 있는 보안 위협 동향
- DDoS 공격 방어, 그리고 예방의 요건
- 새로운 DDoS 공격 방어 패러다임
- Summary



# DDoS 전방위 대응 조치 체계

## 악성코드 분석정보를 기반한 네트워크 위협 자동/실시간 대응




✓ 악성코드 분석 정보 기반 네트워크 대응 능력 향상으로 피해 예방/신속한 대응 제고

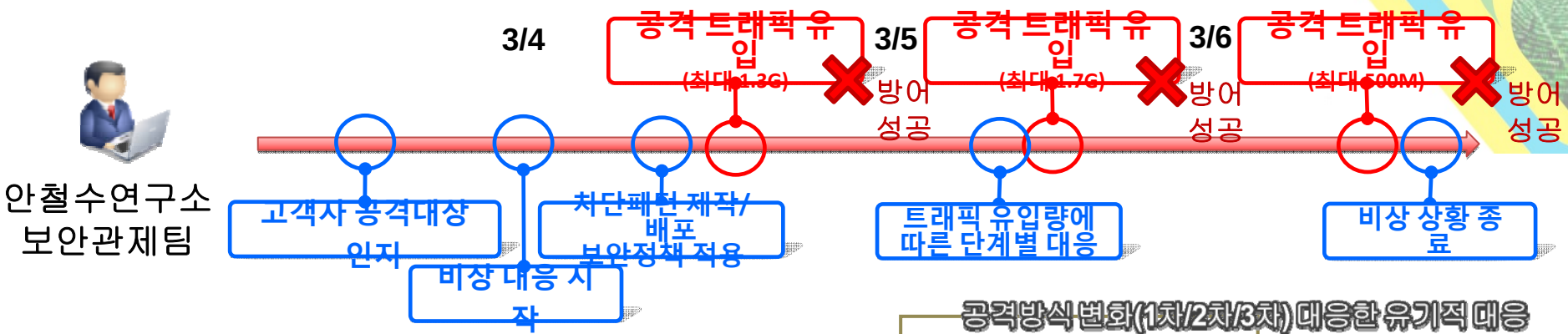
✓ 자사 네트워크 보안장비 정책 자동화 적용으로 실시간 대응 능력 향상



36

# 3•4 DDoS 대응 성공사례

## 시나리오별 사전 모의훈련과 종합위협분석 체계를 통한 완벽한 대응




| 성공 요인 | 시나리오별 대응 준비 | 고객 및 보안관제팀의 완벽한 협업 체계 | ASEC + 관제팀 + N/W기술지원팀의 신속/입체적인 대응 |
|---|---|---|---|
| | DDoS 공격에 대응한 프로세스 수립 | 관제사의 정확한 분석 정보 제공 | ACCESS를 이용한 조기 예경보 |
| | DDoS 보안장비 최적화 적용 | 대응 시나리오에 따른 팀별 협업 | ASEC을 통한 신속/정확한 분석 |
| | 대응 노하우 및 경험 축적 | 관제사 + 고객간의 비상대응체계 | 현장지원을 통한 한박자 빠른 대응 |



37

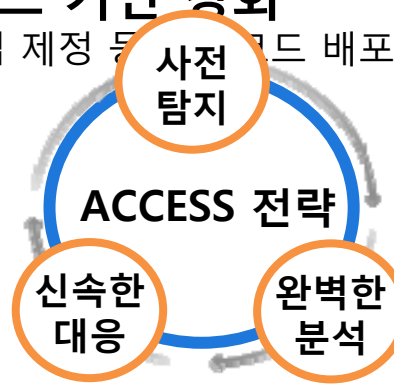
## 3•4 DDoS 대응의 시사점 및 향후 개선을 위한 제언

**시사점**

- 제품이 아닌 서비스 관점이 중요
- 적극적인 샘플 수집으로 신속한 대응 가능
- 분석 인프라/DB에 대한 중요성
- 사후 대응보다 사전 예방이 중요
- 피해기업 단독 대응의 한계점 노출
- 공공기관과 기업과의 공조는 필수

- **프로세스, 사람, 제품의 체계적인 대응**
  - 위협 시나리오별 대응 방안 수립 필요
  - 교육, 모의훈련 등을 통한 대응 역량 강화 필요
- **악성코드 분석과 보안관제 대응의 공조**
  - 악성코드분석에서 보안관제에 이르는 입체적인 대응 필요
  - 공격 원인 분석과 대상 간의 상관분석 필요
- **악성코드 분석 정보의 확대/자동화된 대응**
  - 악성코드 샘플 추가 확보를 위한 수집처 확대 필요
  - 악성코드 분석 정보와 네트워크 보안기술의 연계 강화 요구
- **컴플라이언스 기반 강화**
  - 좀비PC 방지법 제정 등 [illegible]드 배포자에 대한 법적 강화 필요

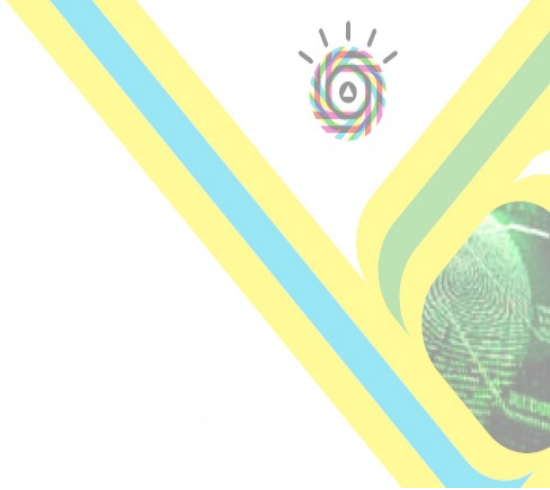
✓ Preventive
✓ Proactive




✓ Real-time
✓ Accuracy
✓ Smart



38



# 감사합니다

세상에서 가장 안전한 이름

Ahn 안철수연구소




IBM