Comprehensive Approach to Security

Hyperconnected 세상에서의 보안을 위한 대응

Young Bach, Solution Engineer. Senior.

보안에 대한 아카마이의 시각

Hyperconnected 세상에서의 혁신

CLOUD

클라우드 서비스 시장 - 2015년까지 $177B[1]로 성장

MOBILE

2020[2]까지 인터넷 사용자의 connected 장비 비율 – 10:1

MEDIA

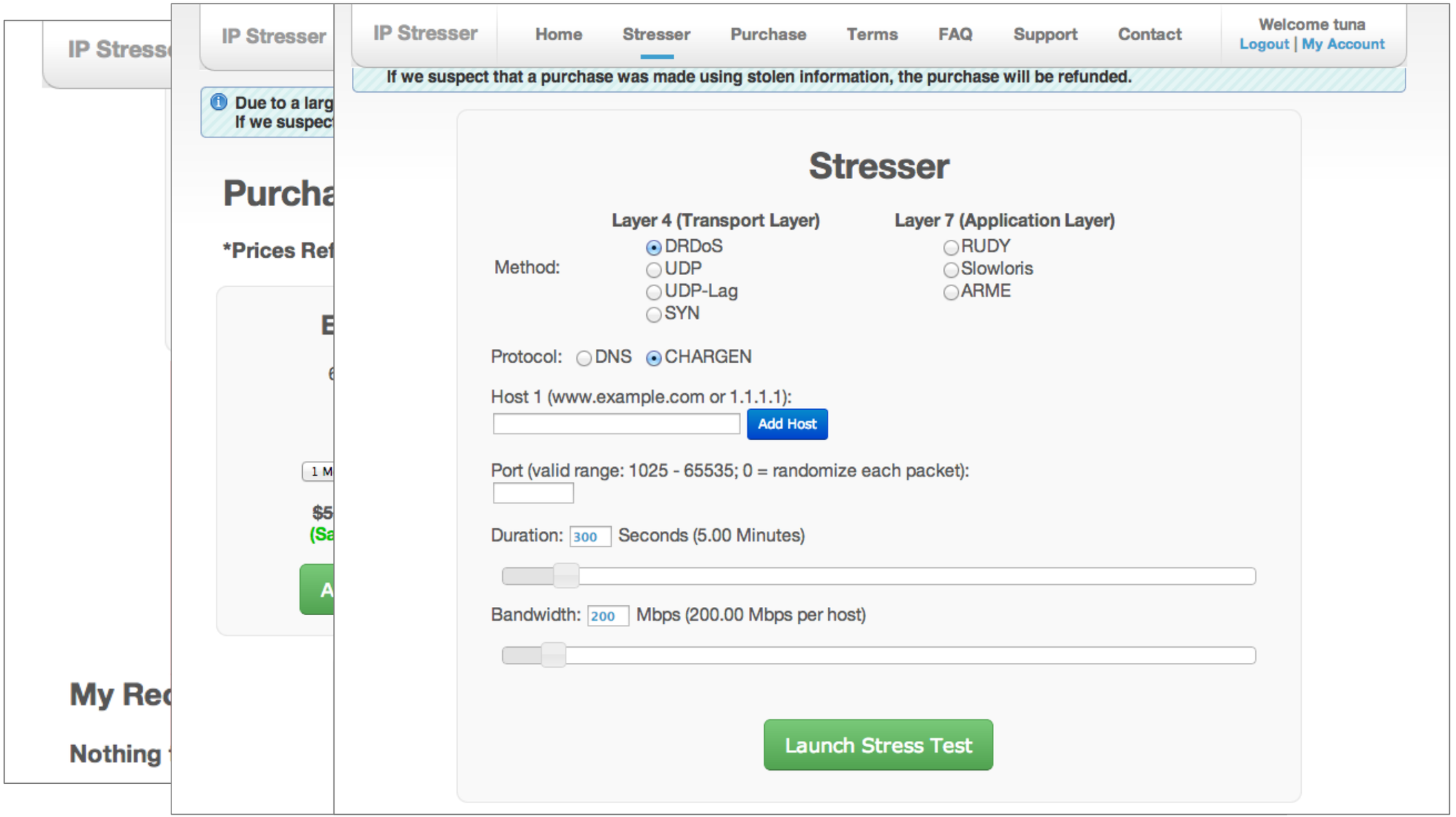
2 년[3]이내에 비디오 트래픽이 인터넷 트래픽 비율- 90%

SECURITY

사이버 공격 비용 - $100,000/분[4]까지 증가

1 Gartner, 3 Akamai, 2 Cisco, 4 McAfee

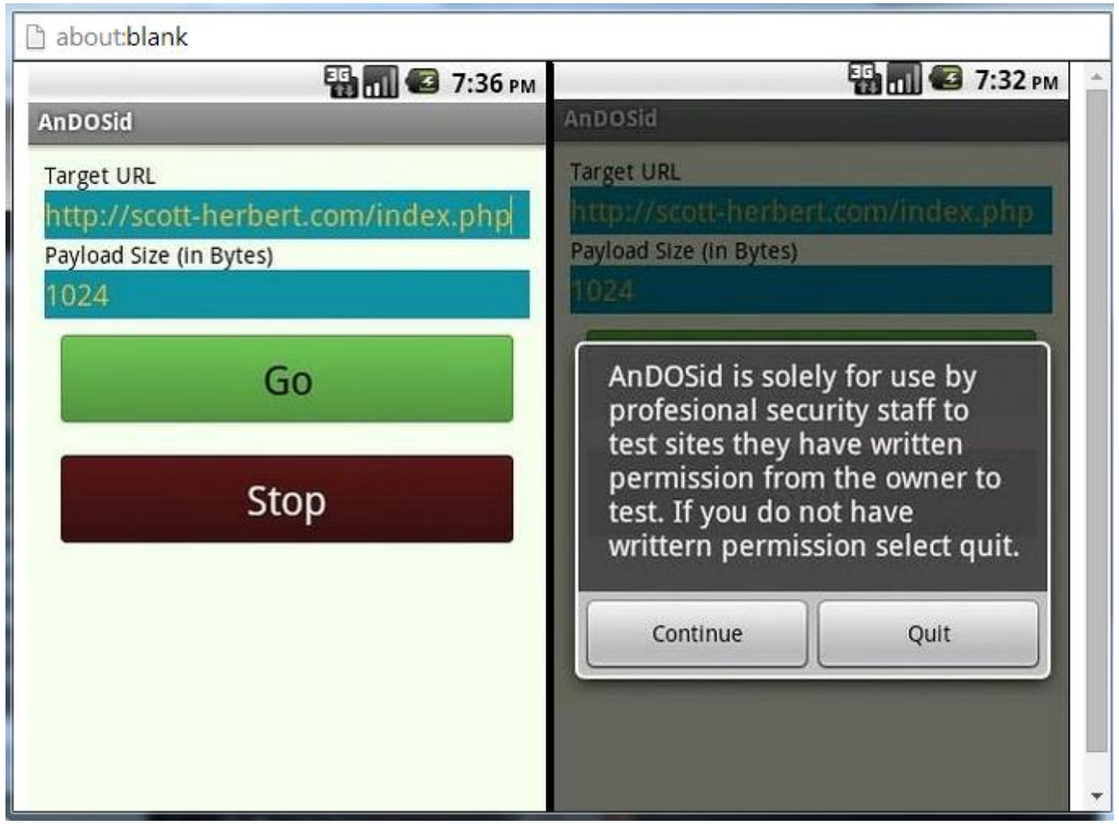
DDoS Stresser Sample



DDoS 공격의 최근 동향

DDoS 공격의 숙주로 모바일 장비 사용

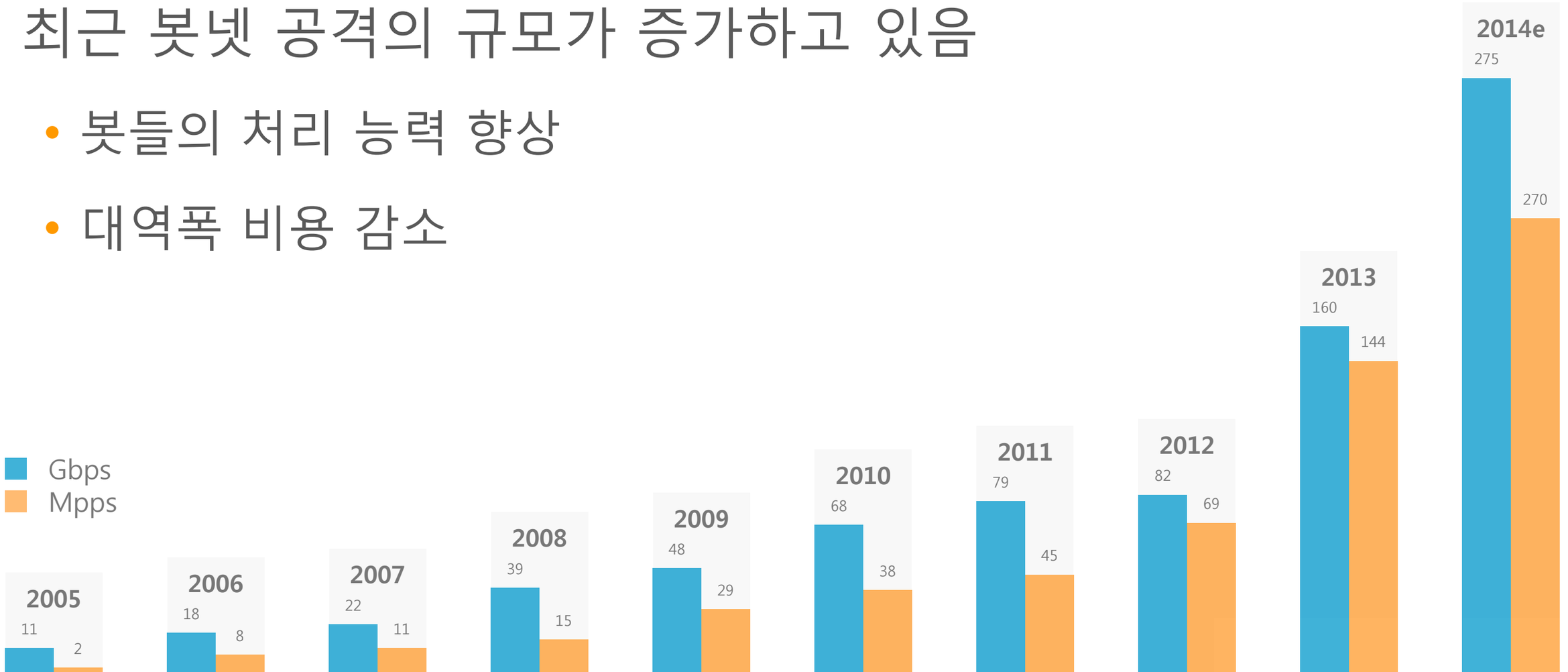
- AnDOSid - Android DoS 공격 툴
- HTTP POST Flood 공격 발생



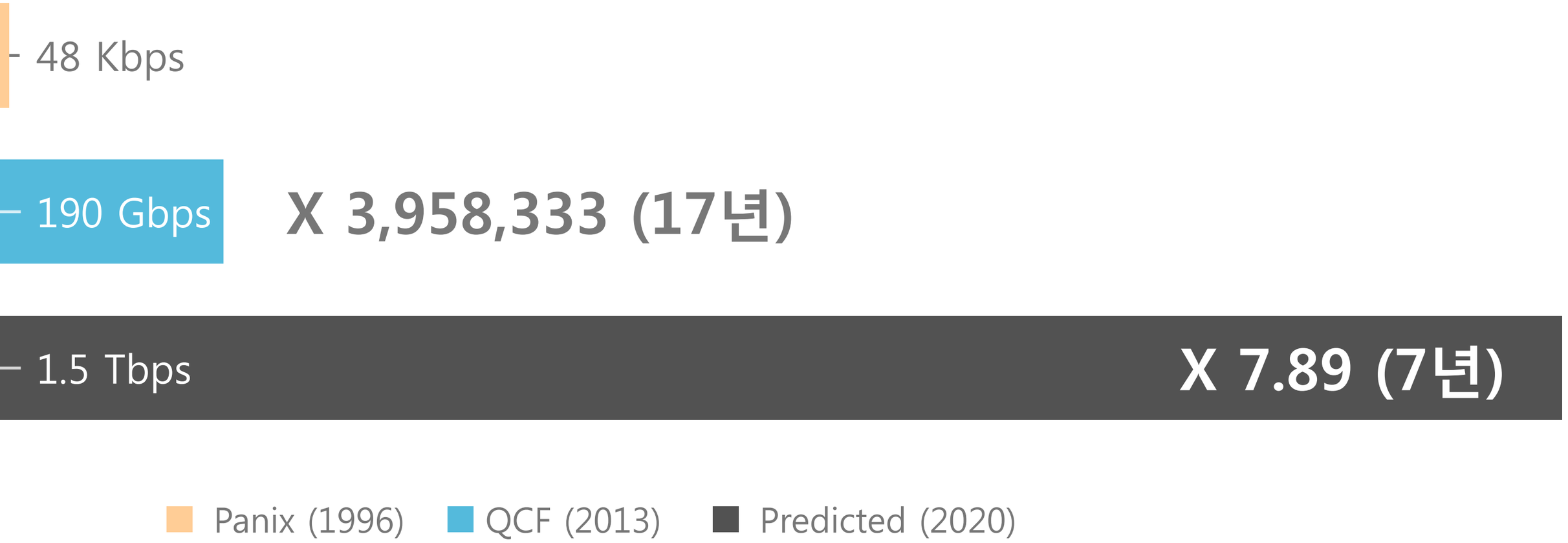
공격 규모의 증가

최근 봇넷 공격의 규모가 증가하고 있음

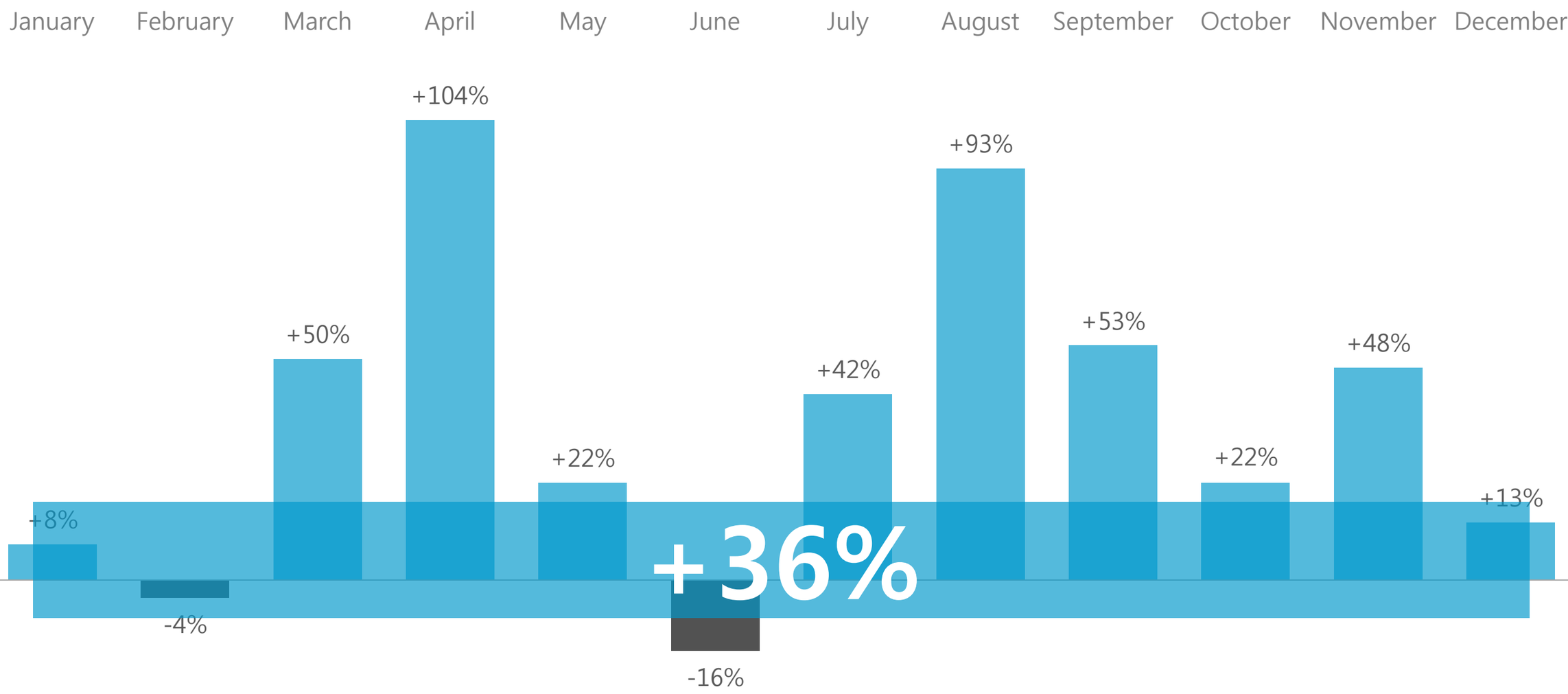
- 봇들의 처리 능력 향상
- 대역폭 비용 감소



공격 규모의 증가



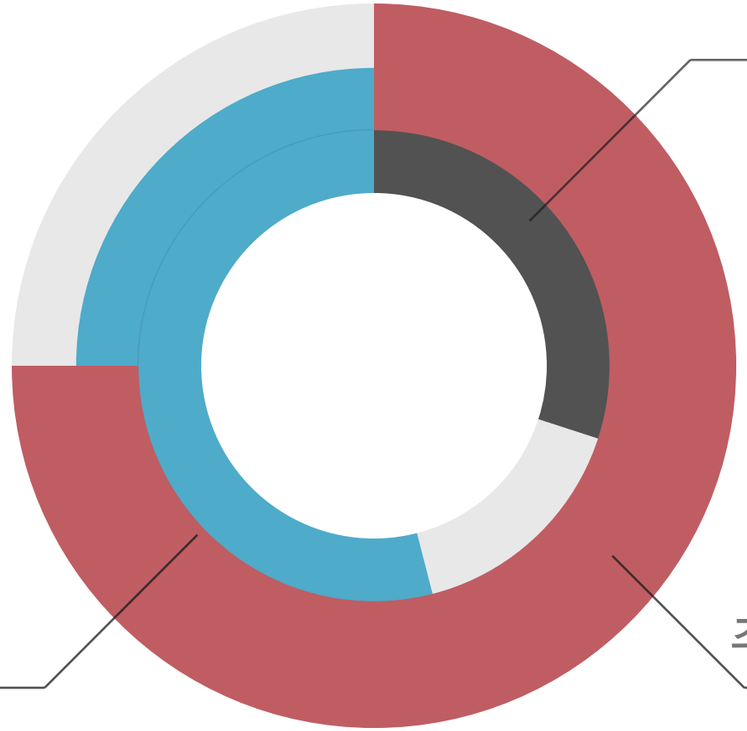
공격 빈도의 추이



Source: Prolexic DDoS Attack Report Q413

데이터 유출을 위한 어플리케이션 공격

- Data 및 금융 자료 유출을 목적으로 하는 공격의 증가
  - 공격자들이 공격 의도를 숨기기 위해서 DDoS 트래픽을 동시에 유발시킴



SQL Injection을 통한
데이타 유출 - **30%**

웹 어플리케이션 해킹을
통한 데이타 유출 - **54%**

4개중 3개가
웹 어플리케이션
취약점을 대상으로 발생

Source: Veracode

Top 10 DDoS Stressers

- DDoS Stands for ATTACK!

#1: Minecraft Stresser - http://Minecraftstresser.com (120GB/seconds)(Skype Resolver)(Stop Button)(Cheapest)(Strongest Ever)(Admin's Choice)

#2: Pantheon Stresser - http://Pantheonstresser.com (80GB/seconds)(Skype Resolver)(Good Staff)(Powerful)

#3: Dark Booter - http://darkbooter.com (Up for 2 years)(Good Price)(Great Support)

#4: IP Stresser - http://ipstresstest.com (Powerful)(Up for 3 years)

#5: Power Stresser - http://powerstresser.com (Strong Power)

#6: Titanium Stresser - http://titaniumstresser.net

#7: DejaBooter Stresser - http://www.dejabooter.com/ (Max Time)

#8: Legion Booter - http://legion.cm/ (Strong)

#9: Masterboot - http://www.masterboot.net/ (Hard Hitting)

#10: Avenge Stresser - www.avengestresser.com/ (Great Price)

보안에 대한 새로운 접근

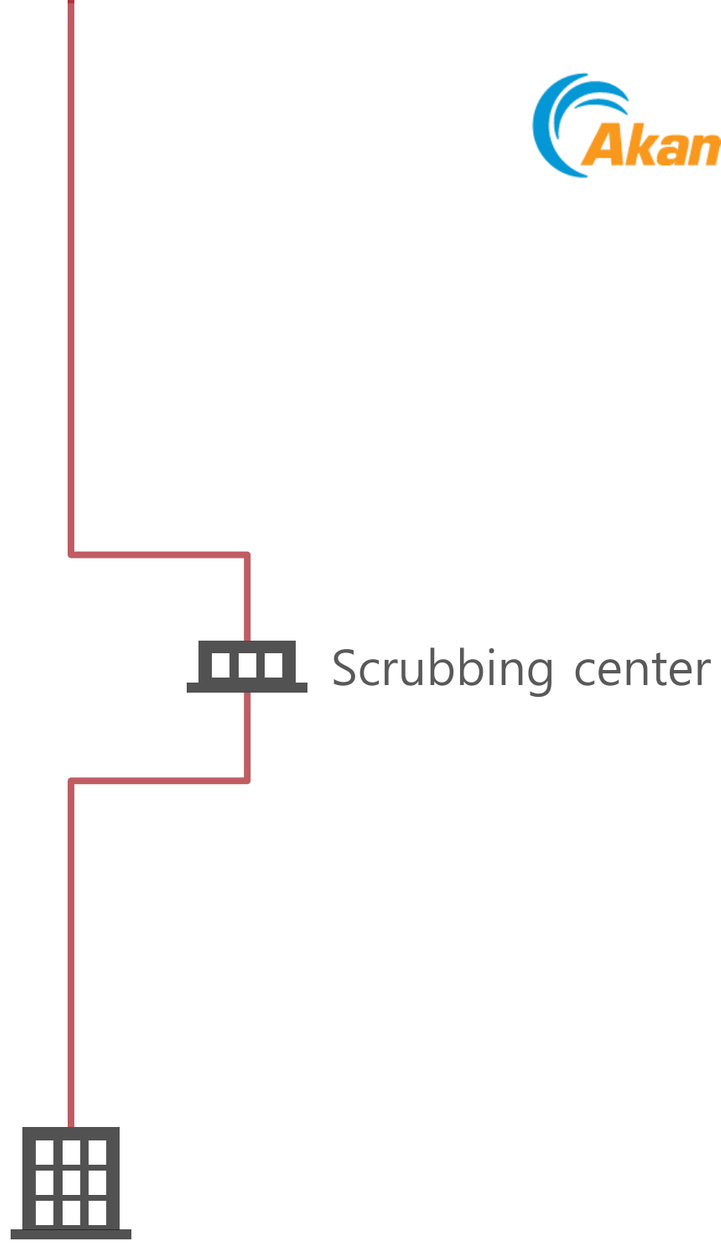
원격 제어 서비스 – AS IS

- 스크러빙 서비스:

  - 차단 서비스가 활성화 되기 전의 대응상의 어려움

  - 데이타 유출 및 낮은 트래픽의 느린 공격에 대한 탐지의 어려움

  - 성능 저하 발생: 수익 및 생산성 기반의 웹 어플리케이션에 대한 피해 발생



설치 기반의 하드웨어 – AS IS

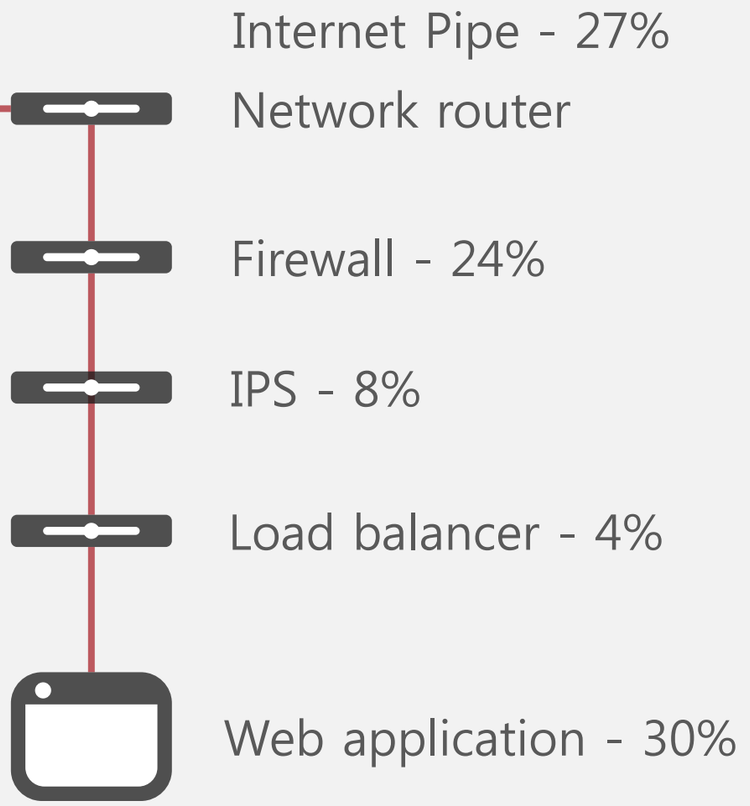
- 데이터 센터에서 제공하는 하드웨어 – 고려사항:

  - 대용량 DDoS 공격 방어를 위한 네트웍 대역폭 확보

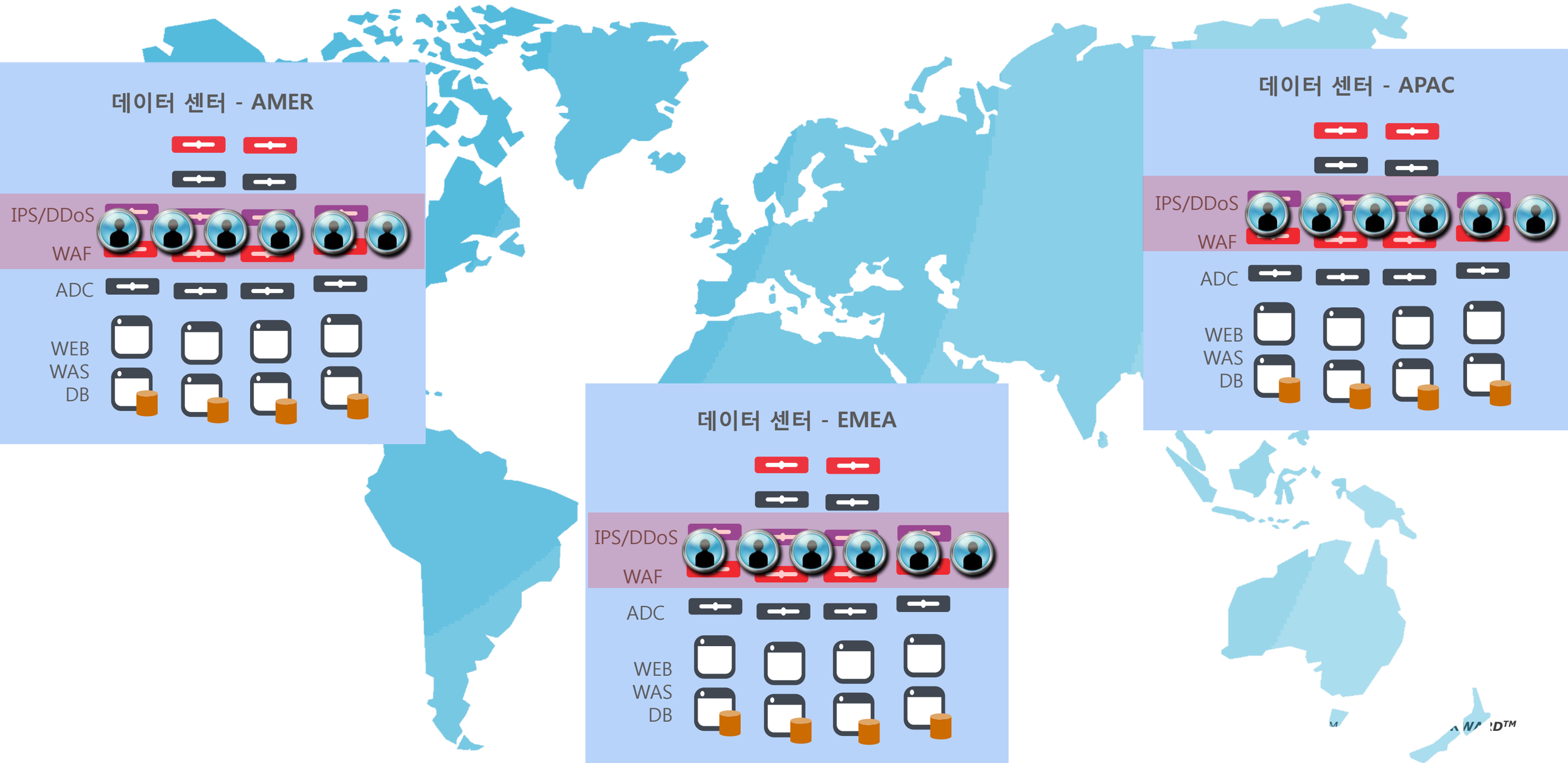
  - 시스템 내의 모든 구성에 대한 확장성

  - 자원에 민감한 어플리케이션 계층 공격을 방어하기 위한 하드웨어 장비의 처리 능력

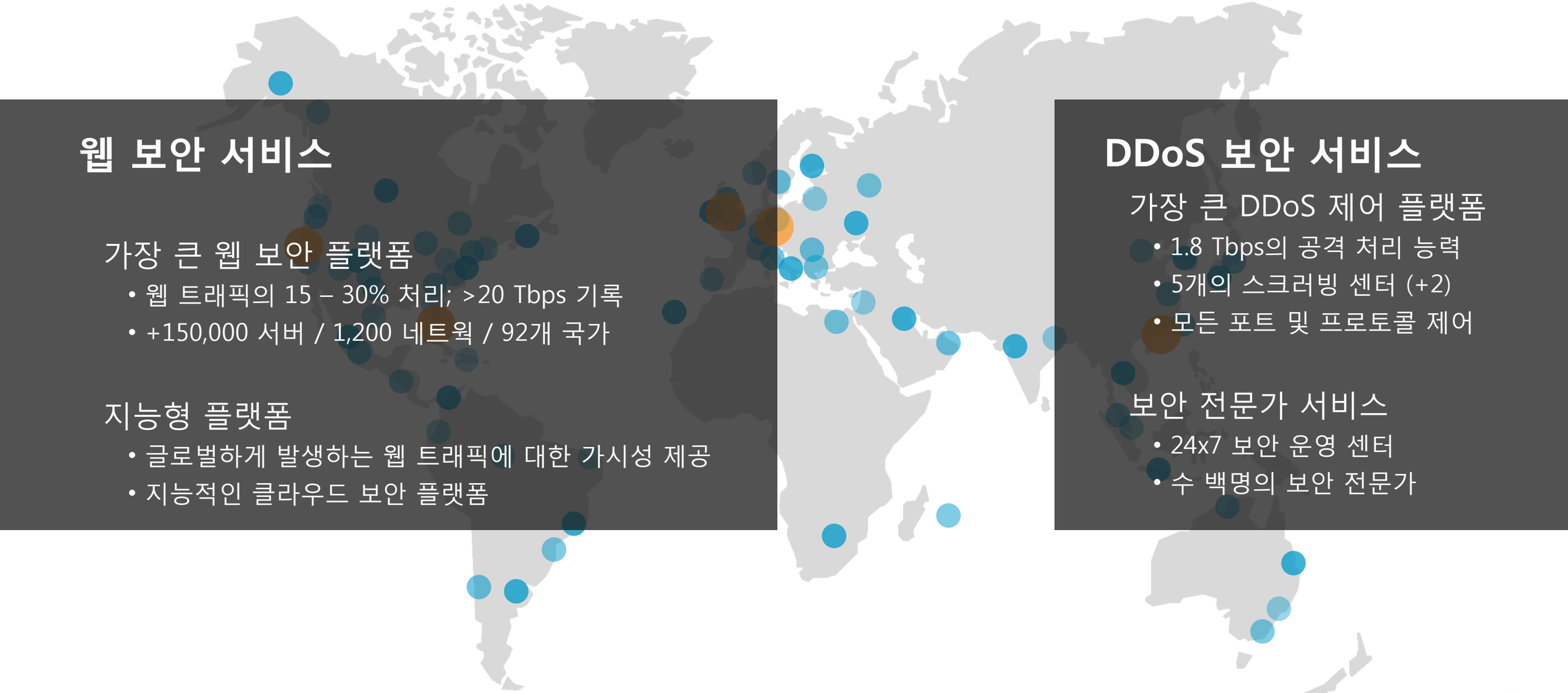
  - 지속적으로 증가하는 공격의 규모를 대비하기 위한 투자



물리적인 데이터 센타 기반의 보안 관제



클라우드의 보안 서비스



웹 보안 서비스

가장 큰 웹 보안 플랫폼

- 웹 트래픽의 15 – 30% 처리; >20 Tbps 기록
- +150,000 서버 / 1,200 네트웍 / 92개 국가

지능형 플랫폼

- 글로벌하게 발생하는 웹 트래픽에 대한 가시성 제공
- 지능적인 클라우드 보안 플랫폼

DDoS 보안 서비스

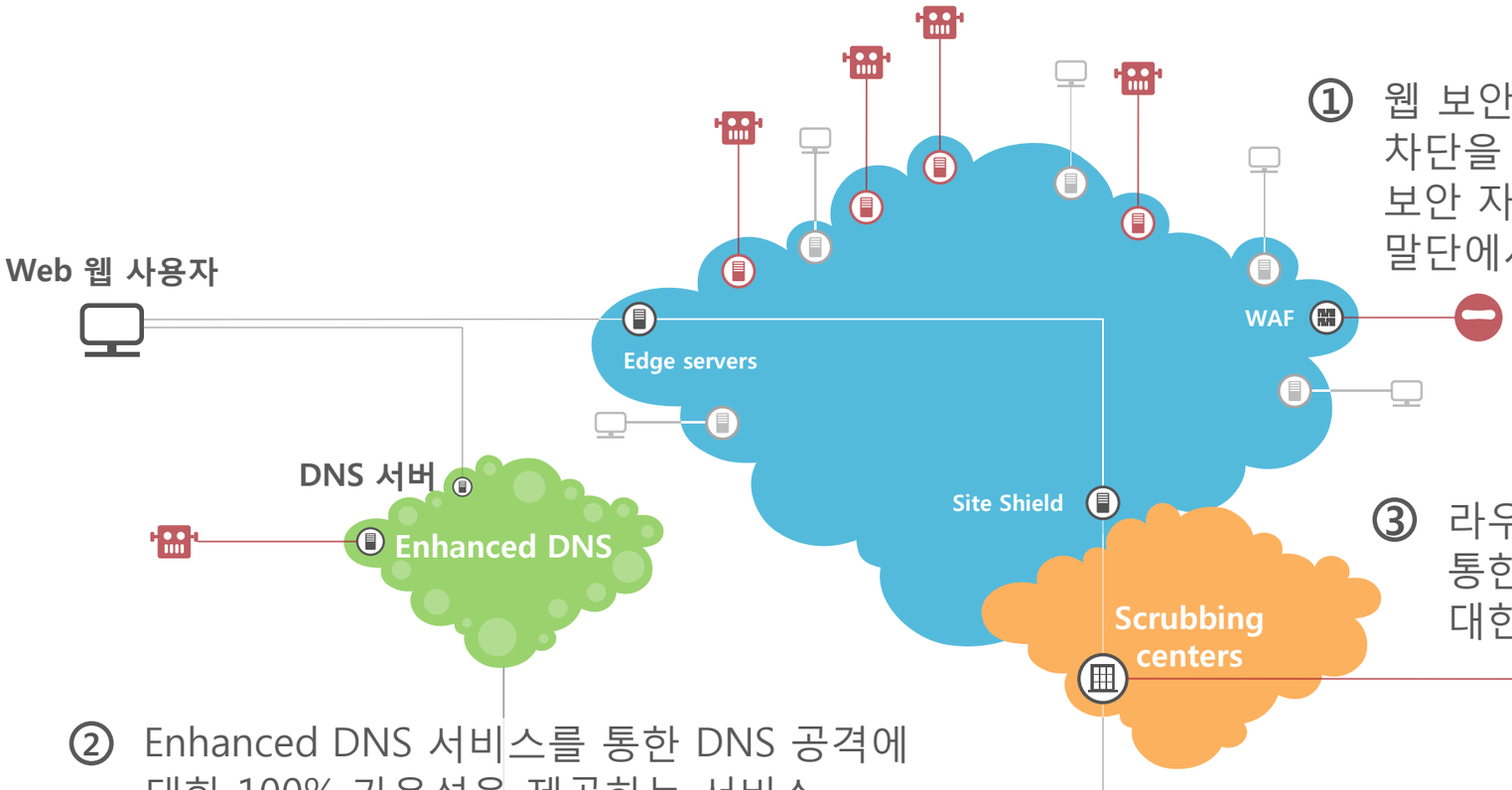
가장 큰 DDoS 제어 플랫폼

- 1.8 Tbps의 공격 처리 능력
- 5개의 스크러빙 센터 (+2)
- 모든 포트 및 프로토콜 제어

보안 전문가 서비스

- 24x7 보안 운영 센터
- 수 백명의 보안 전문가

클라우드 기반의 다계층 공격 제어



① 웹 보안 서비스를 통한 웹 자산에 대한 상시 차단을 통한 DDoS 및 웹 공격 제어 – 고객 보안 자산에 영향을 받지 않도록 인터넷 말단에서 제어하는 보안 서비스

② Enhanced DNS 서비스를 통한 DNS 공격에 대한 100% 가용성을 제공하는 서비스

③ 라우팅 기반의 DDoS 공격 제어 서비스를 통한 웹 및 IP 기반의 어플리케이션 공격에 대한 제어

④ 아카마이의 보안 전문가를 통한 보안에 대한 중장기 적인 대응 체계 수립

Data Center

② DNS

① Web application

Web and IP applications

③ Network infrastructure

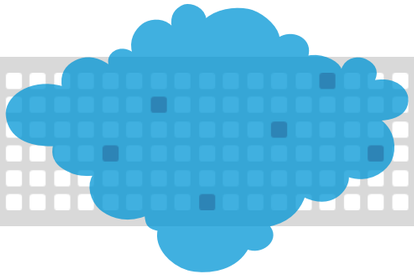
Edge에서의 공격 방어

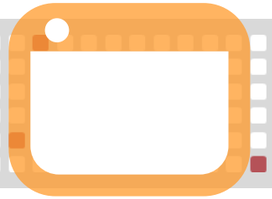
Data Center로 공격이 도달하기 전에 차단

아카마이에서 투자한 인프라를 통해서 대규모 공격 방어

상시 접속 보안

대부분의 어플리케이션 계층 공격들은
일반 어플리케이션과 함께 발생

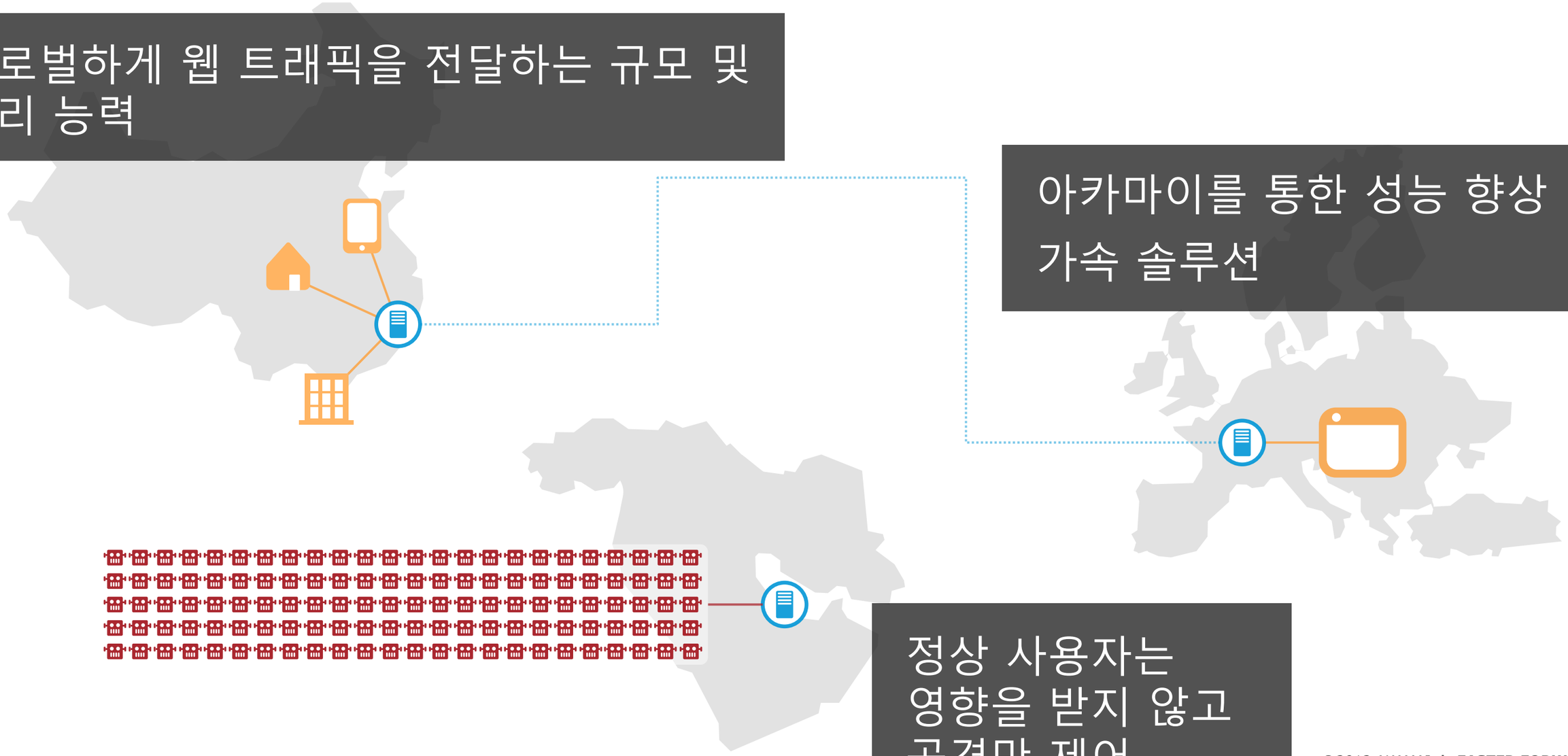




상시 접속되어 있는
인라인 보안 솔루션에서
공격 탐지 가능

방어 및 성능

글로벌하게 웹 트래픽을 전달하는 규모 및 처리 능력



아카마이를 통한 성능 향상 가속 솔루션

정상 사용자는 영향을 받지 않고 공격만 제어

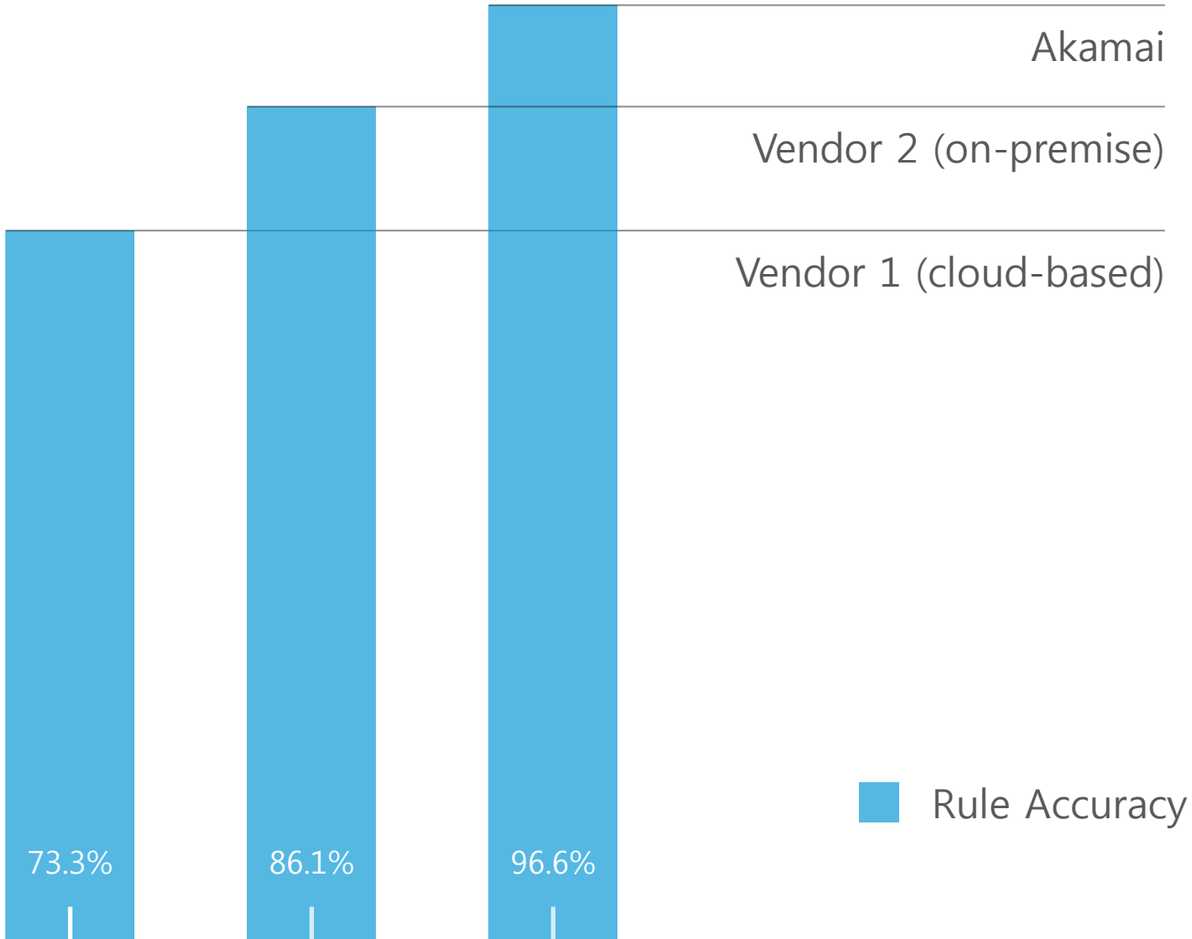
글로벌 규모의 인터넷 보안

지능형 플랫폼을 통한 웹 트래픽 처리
(>20 Tbps, 2013)

DDoS 공격 처리 플랫폼
(1.8 Tbps, Q1 2014)

대용량 DDoS 공격
(240 Gbps, February 2014)

지능형 플랫폼의 장점



- 처음으로 출현하는 공격에 대한 가시성
- 신규로 발견한 공격에 대한 신속한 대응을 통한 위험 감소
- 높은 정확성을 통한 효율적인 보안 및 높은 신뢰도

사례 분석

사례 연구: 2012년 런던 올림픽

직면 과제

널리 알려진 국제적인 이벤트에서
수백만명의 전세계 사용자들에게
신속하고 안전한 웹 경험 전달

솔루션

높은 확장성과 글로벌하게 분산된 웹 전달은
DDoS 공격에 대한 유연한 방어를 제공함

40X
INCREASE
IN TRAFFIC

25M
FIREWALL RULES
TRIGGERED

23
DIFFERENT ATTACK
TYPES BLOCKED

사례 연구: 2012년 런던 올림픽 *25 July through 9 September*

공격 유형 #1

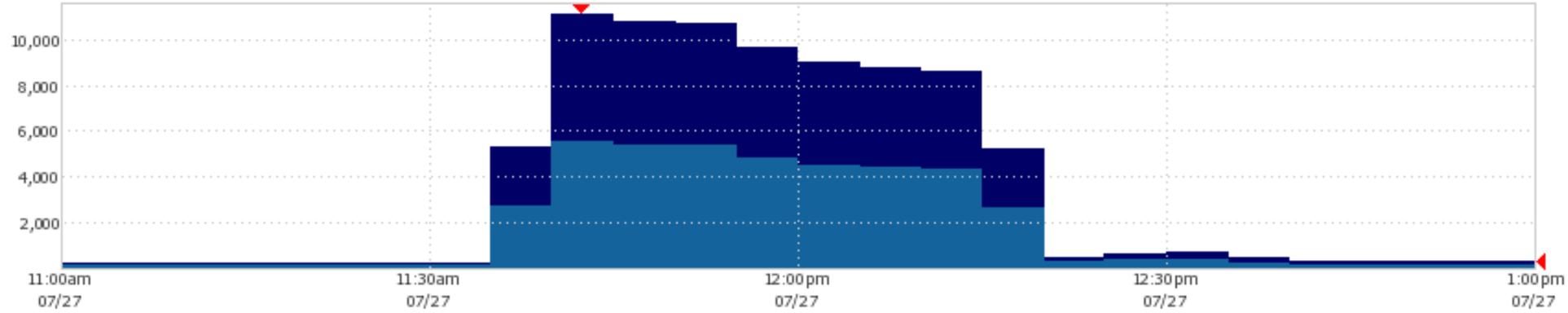
TRIGGERED RULES

Firewall rules triggered.

Total Triggered Rules **25.3 Million**

Peak: **11094 Rules/sec** at 11:40AM

Latest: **275.82 Rules/sec** at 12:55PM



Eastern Daylight Time

	TOTAL TRIGGERED RULES	%TRIGGERED RULES
Denied Rules	12.6 Million	50.1
Warned Rules	12.6 Million	49.9

사례 연구: 2012년 런던 올림픽 *25 July through 9 September*

공격 유형 #2

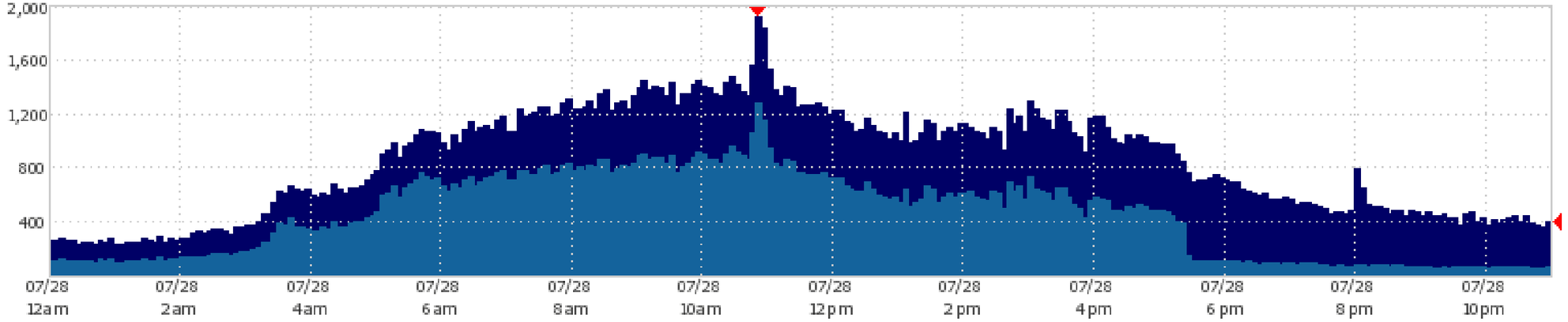
TRIGGERED RULES

Firewall rules triggered.

Total Triggered Rules **70.1 Million**

Peak: **1918.45 Rules/sec** at 10:50AM

Latest: **401.73 Rules/sec** at 10:55PM



Eastern Daylight Time

	TOTAL TRIGGERED RULES	%TRIGGERED RULES
Denied Rules	36.4 Million	51.8
Warned Rules	33.8 Million	48.2

사례 연구: 대형 금융 기관

직면 과제

지능형 공격자들에 의한 다양한 유형의 공격이 발생하는 동안 고객의 웹에 대한 꾸준한 경험 유지

솔루션

클라우드 기반의 웹 보안 - 어플리케이션으로 공격이 유입되기 전에 edge에서 공격 차단

Day 1

홈페이지에 HTTP flood 공격

30 Gbps, 최대 4백만개의 Request 발생(초당)

공격이 발생하는 동안 일반 고객에제 정상 트래픽 제공

Day 2

40 Gbps의 대용량 DNS 공격 발생

100%의 가용성 제공

Day 3

방어 솔루션이 없는 웹 사이트에 HTTP flood 발생

페이지 뷰 에러가 최대 1,327% 발생

사례 연구: 대형 금융 기관 #1

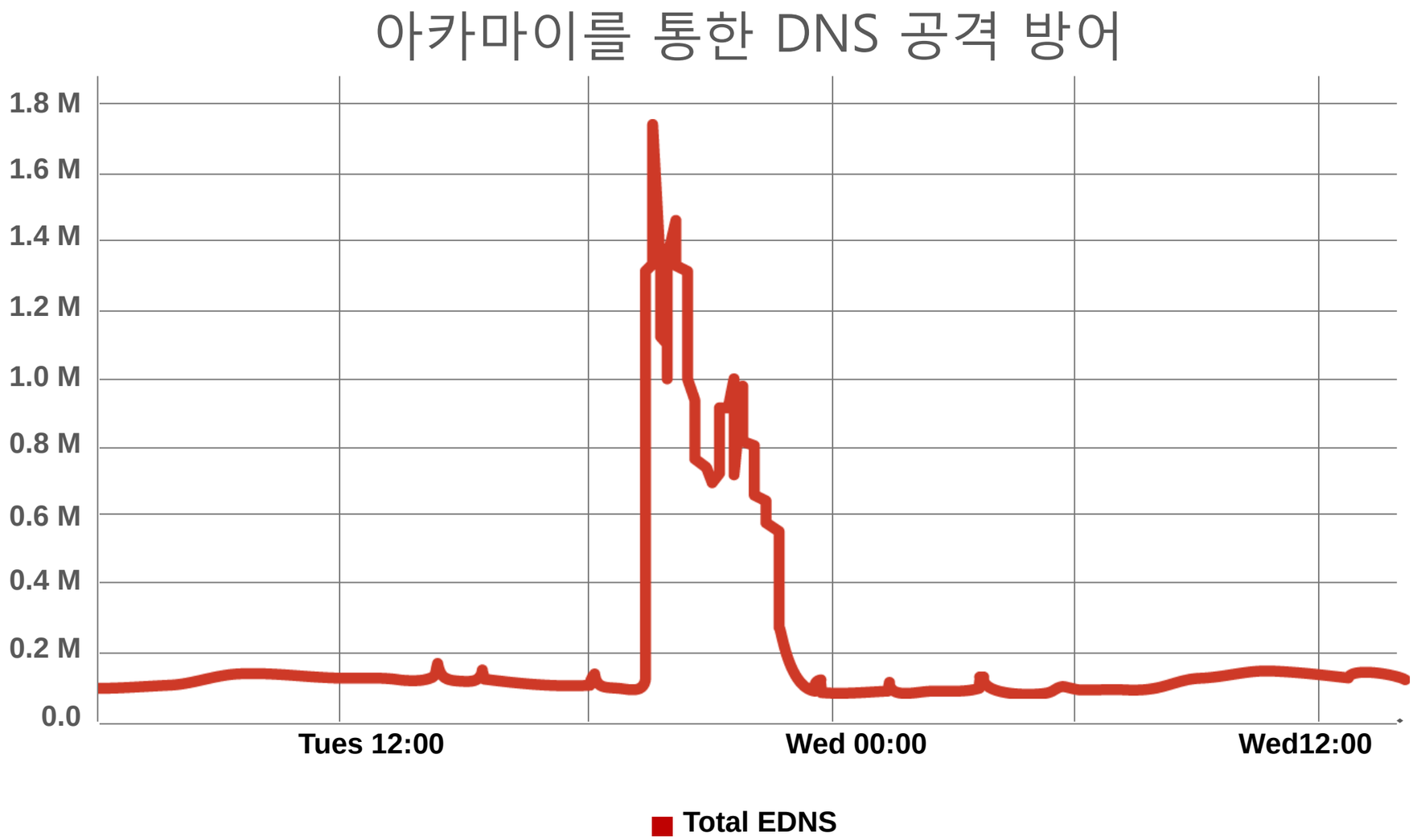
Attack Traffic:

23 Gbps

(10,000X normal)

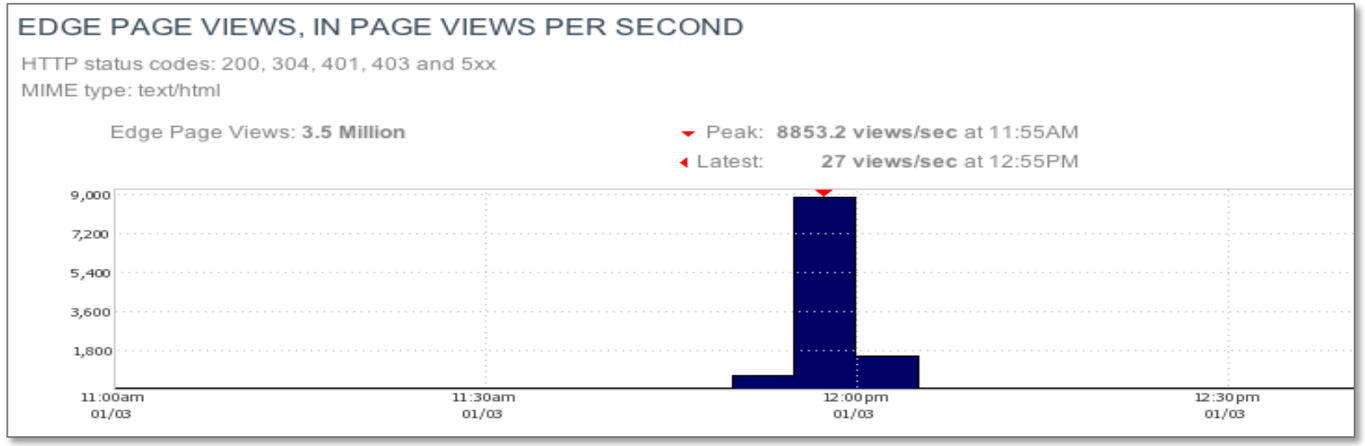
Duration:

4.5 Hours

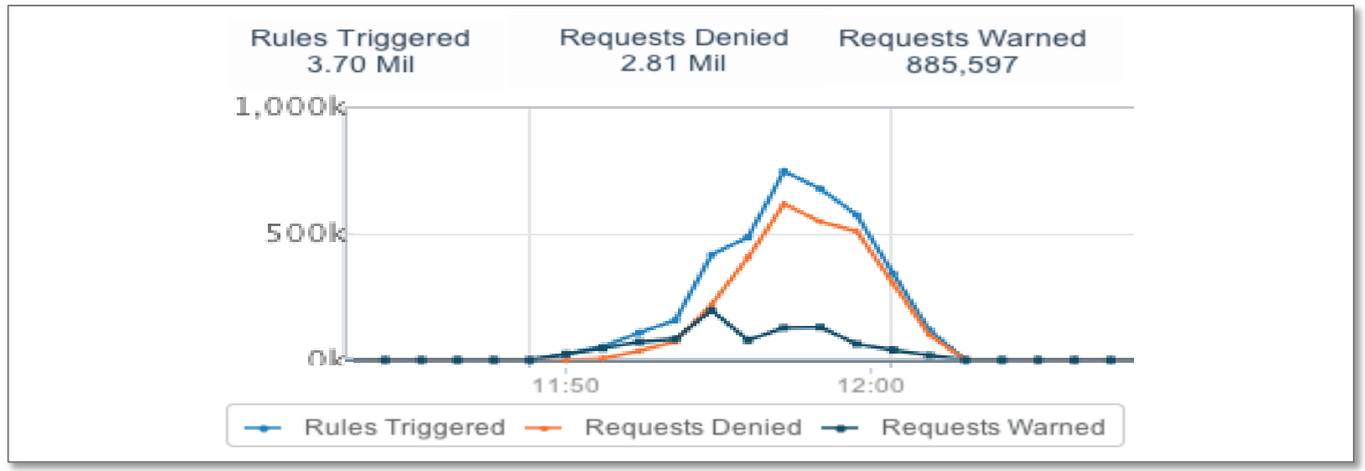


사례 연구: 대형 금융 기관 #2

"Probe" attack was then seen at another bank 25 minutes later.

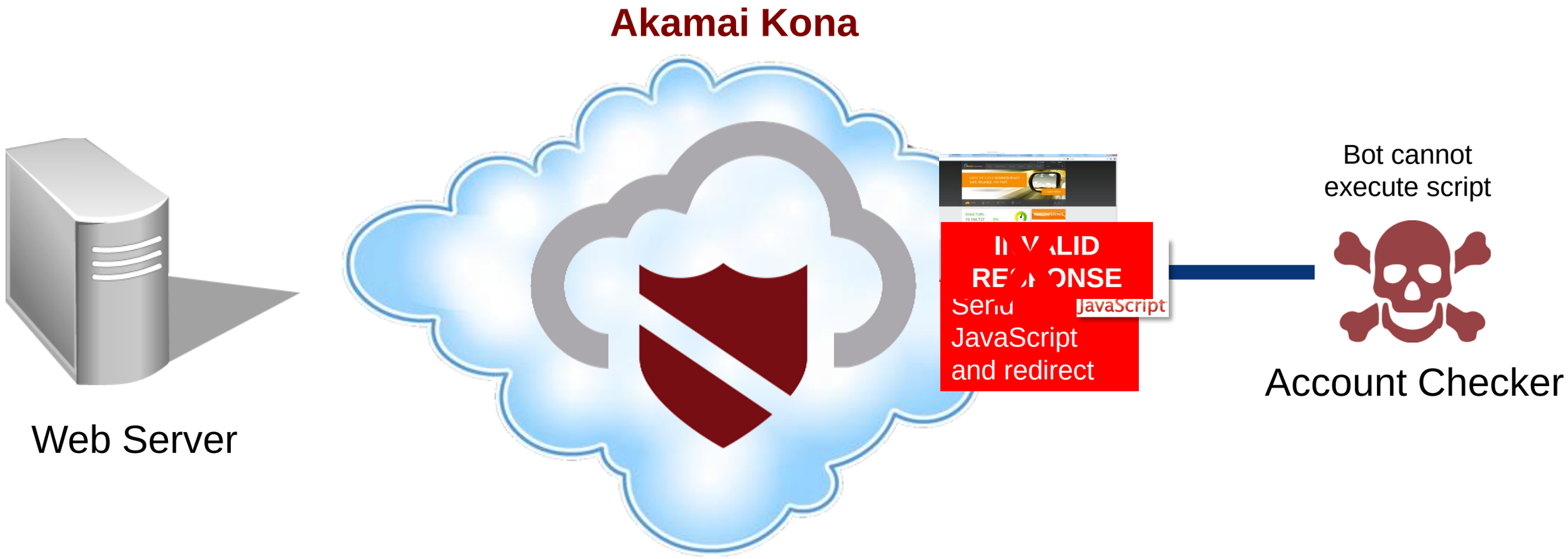


Akamai Kona in place, and rate controls automatically activated.



사례 연구: 어카운트 체커

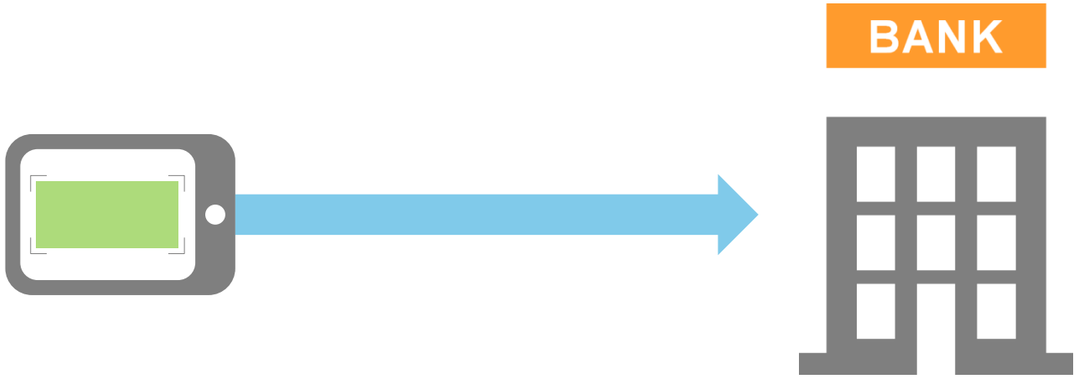
1. 낮은 비율의 공격이 글로벌하게 발생
2. 실제 사용자의 요청과 유사하게 Request 전송



사례 연구: 어카운트 체커

발생 경위

어노니머스 공격자가 모바일 수표 예금 어플리케이션으로 URL들에 4시간 동안 120,000번의 접속을 함



아카마이의 활동

아카마이에서 의심스러운 행위의 탐지 → 해당 접속 요청들에 대한 자동 차단

사례 연구: 어카운트 체커

발생 경위

조직화된 범죄 조직이 툴킷을 사용해서 사용자 로그인 정보로 여러 이커머스 사이트로 접속하여 범죄 행위를 함

아카마이의 활동

아카마이에서 여러 이커머스 사이트로 접속 시도를 하는 패턴을 탐지하고 고객에게 정보를 제공함

PROTECT & PERFORM