# 성공적인 디지털 혁신을 위한 클라우드 보안 정복하기

라임라이트 네트웍스 코리아 지사장 | 박대성

# LIMELIGHT AT A GLANCE

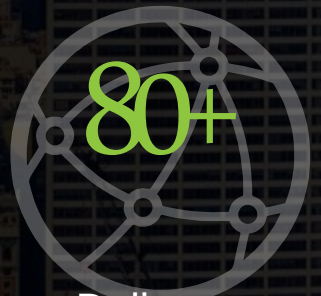
## GLOBAL PRIMEIER CDN COMPANY

32+

Tbps
Egress Capacity

900+

Connected Networks



80+

Delivery
Locations

2001

Founded

# 라임라이트 인프라 현황


Vancouver
Seattle
San Jose
To Tokyo
To Sydney
Los Angeles
Phoenix
Dallas
Mexico City
Minneapolis
Chicago
Toronto
Montreal
Halifax
New York
D.C.
Atlanta
Miami
Medellín
Bogotá
São Paulo
Santiago
Buenos Aires
Stockholm
Amsterdam
London
Paris
Marseille
Madrid
Palermo
Düsseldorf
Frankfurt
Zurich
Vienna
Milan
Tel Aviv
Baghdad
Kuwait City
Doha
Dubai
Johannesburg
Delhi
Mumbai
Chennai
Hong Kong
Bangkok
Kuala Lumpur
Singapore
Manila
Seoul
Tokyo
Osaka
To San Jose
To San Jose
Sydney
Current PoPs
Future PoPs

# 라임라이트 서비스 포트폴리오

## CDN / 웹가속

- 다운로드
- 웹사이트 캐싱
- 동적 컨텐츠 가속 (API)

## 비디오 플랫폼

- 통합 비디오 플랫폼
- 멀티 디바이스

## 클라우드 보안

- CDN 보안
- DDoS 완화
- 웹 어플리케이션 방화벽

## 매니지드 DNS

- 글로벌 DNS 서비스
- 트래픽 디렉터

## 오리진 스토리지

- 클라우드 오리진
- 자동 마이그레이션

## 라임라이트 글로벌 인프라스트럭처

**Limelight**가 소유/ 관리하는 고속 사설망

대형 **POP** 전략을 통한 높은 캐시 적중률

긴밀한 **ISP** 피어링을 통한 높은 사용자 접근성

# 최근 주요 사이버 공격 사례

2017.06.25
국내 최대 가상화폐 거래소 B사 접속 부하에 따른 장애인지, 디도스 공격인지 모를 웹사이트 마비 사태 발생.
-보안뉴스-

2018.02.02
북한 연구자 노린 공격, 플래시 제로데이 취약점 활용
-보안뉴스-

2017.03.02
L 인터넷 면세점 사이트 디도스 공격으로 마비됐다가 3시간 만에 복구.
-조선 비즈-

2017.12.13
비트코인 겨냥 '디도스 공격' 잇따라…서비스 장애 호소
-이데일리-

2018.03.28
'봇 공장' 놀이터 된 온라인 광고 시장
-The PR news-

2017.02.07
해커조직 '그룹123', 최근 어도비 제로데이 취약점으로 한국 집중 공격중.
-데일리시큐-

2017.06.26
금융결제원 및 은행 3곳 디도스 공격으로 인한 전산시스템 마비
-연합 뉴스-

2017.02.23
북한 해킹그룹 'APT37', 제로데이 취약점으로 남한 타깃 공격 지금도…
-데일리 시큐-

2018.03.29
악성 봇 트래픽, 2017년 동안 9.5% 성장했다
-보안뉴스-

2018.04.03
제로데이 취약점 쓰는 레드아이즈 해킹 그룹 정체는?
-전자신문-

2017.03.28
외교부 홈페이지에 대한 중국발 디도스 공격 시도 간헐적으로 발생
-연합뉴스-

2018.01.19
가상화폐 마이닝 봇, 보안사고의 31%
-데이터넷-

2017.12.23
디도스 공격, 글로벌 기업 24% 피해…
-전자신문-

2017.09.29
美 대선, 가짜 뉴스 퍼나른 건 '트위터 봇'
-전자신문-

2017.04.04
돈받고 도박사이트 디도스 공격 돈을 받아 챙긴 해킹팀이 경찰에 붙잡힘
-노컷뉴스-

# 진화하는 봇을 이용한 공격

2018.03.28
'봇 공장' 놀이터 된 온라인 광고 시장
-The PR news-

2018.01.19
호텔·여행업계 부정 로그인 시도 82%
악성 봇넷
-데이터넷-

2017.09.29
美 대선, 가짜 뉴스 퍼나른 건 '트위터 봇'
-전자신문-

2018.03.29
악성 봇 트래픽, 2017년 동안 9.5% 성장했다
-보안뉴스-

# DDOS, 커지는 규모 다양해지는 공격

2017.12.13
비트코인 겨냥
'디도스 공격'
잇따라…서비스
장애 호소
-이데일리-

2017.06.25
국내 최대 가상화폐 거래소
B사 접속 부하에 따른
장애인지, 디도스 공격인지
모를 웹사이트 마비 사태
발생.
-보안뉴스-

2017.03.02
L 인터넷 면세점
사이트 디도스
공격으로
마비됐다가 3시간
만에 복구.
-조선 비즈-

2018.03.28
'봇 공장' 놀이터
된 온라인 광고
시장
-The PR news-

2017.06.26
금융결제원 및
은행 3곳 디도스
공격으로 인한
전산시스템 마비
-연합 뉴스-

2018.03.29
악성 봇 트래픽,
2017년 동안
9.5% 성장했다
-보안뉴스-

2017.03.28
외교부 홈페이지에
대한 중국발
디도스 공격 시도
간헐적으로 발생
-연합뉴스-

2017.12.23
디도스 공격,
글로벌 기업 24%
피해…
-전자신문-

2017.04.04
돈받고 도박사이트
디도스 공격 돈을
받아 챙긴 해킹팀이
경찰에 붙잡힘
-노컷뉴스-

# 제로데이 공격의 위협

2017.06.25
국내 최대 가상화폐 거래소 B사 접속 부하에 따른 장애인지, 디도스 공격인지 모를 웹사이트 마비 사태 발생.
-보안뉴스-

2018.02.02
북한 연구자 노린 공격, 플래시 제로데이 취약점 활용
-보안뉴스-

2017.03.02
L 인터넷 면세점 사이트 디도스 공격으로 마비됐다가 3시간 만에 복구.
-조선 비즈-

2017.12.13
비트코인 겨냥 '디도스 공격' 잇따라…서비스 장애 호소
-이데일리-

2018.03.28
'봇 공장' 놀이터 된 온라인 광고 시장
-The PR news-

2017.02.07
해커조직 '그룹123', 최근 어도비 제로데이 취약점으로 한국 집중 공격중.
-데일리시큐-

2017.06.26
금융결제원 및 은행 3곳 디도스 공격으로 인한 전산시스템 마비
-연합 뉴스-

2017.02.23
북한 해킹그룹 'APT37', 제로데이 취약점으로 남한 타깃 공격 지금도...
-데일리 시큐-

2018.03.29
악성 봇 트래픽, 2017년 동안 9.5% 성장했다
-보안뉴스-

2018.04.03
제로데이 취약점 쓰는 레드아이즈 해킹 그룹 정체는?
-전자신문-

2017.03.28
외교부 홈페이지에 대한 중국발 디도스 공격 시도 간헐적으로 발생
-연합뉴스-

2018.01.19
가상화폐 마이닝 봇, 보안사고의 31%
-데이터넷-

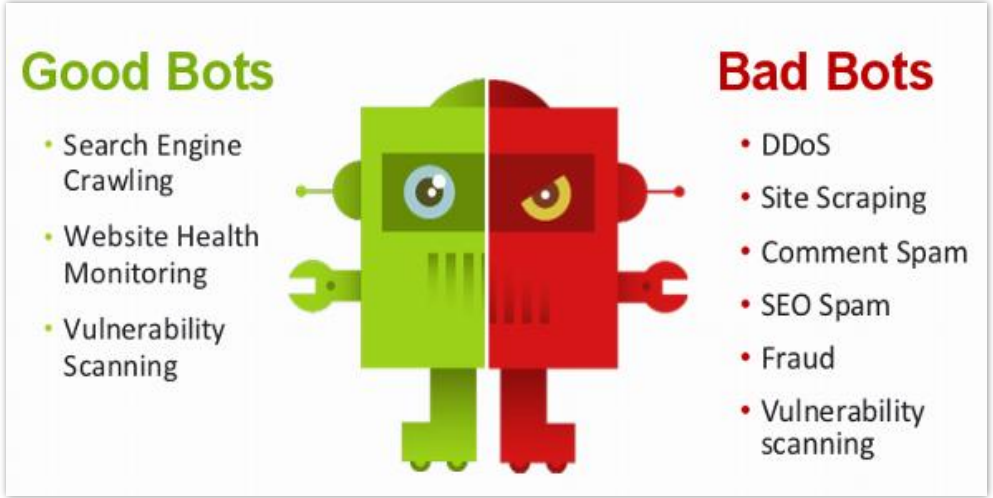
2017.12.23
디도스 공격, 글로벌 기업 24% 피해…
-전자신문-

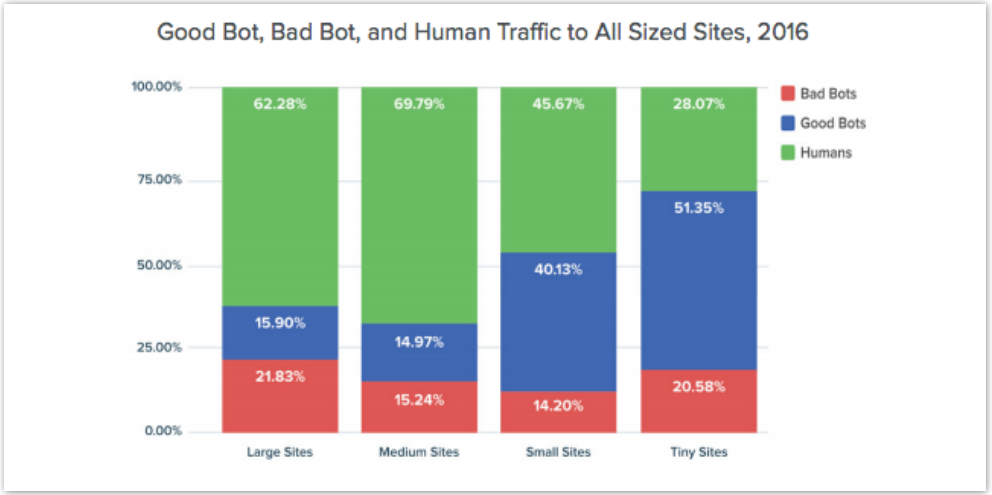
2017.09.29
美 대선, 가짜 뉴스 퍼나른 건 '트위터 봇'
-전자신문-

2017.04.04
돈받고 도박사이트 디도스 공격 돈을 받아 챙긴 해킹팀이 경찰에 붙잡힘
-노컷뉴스-

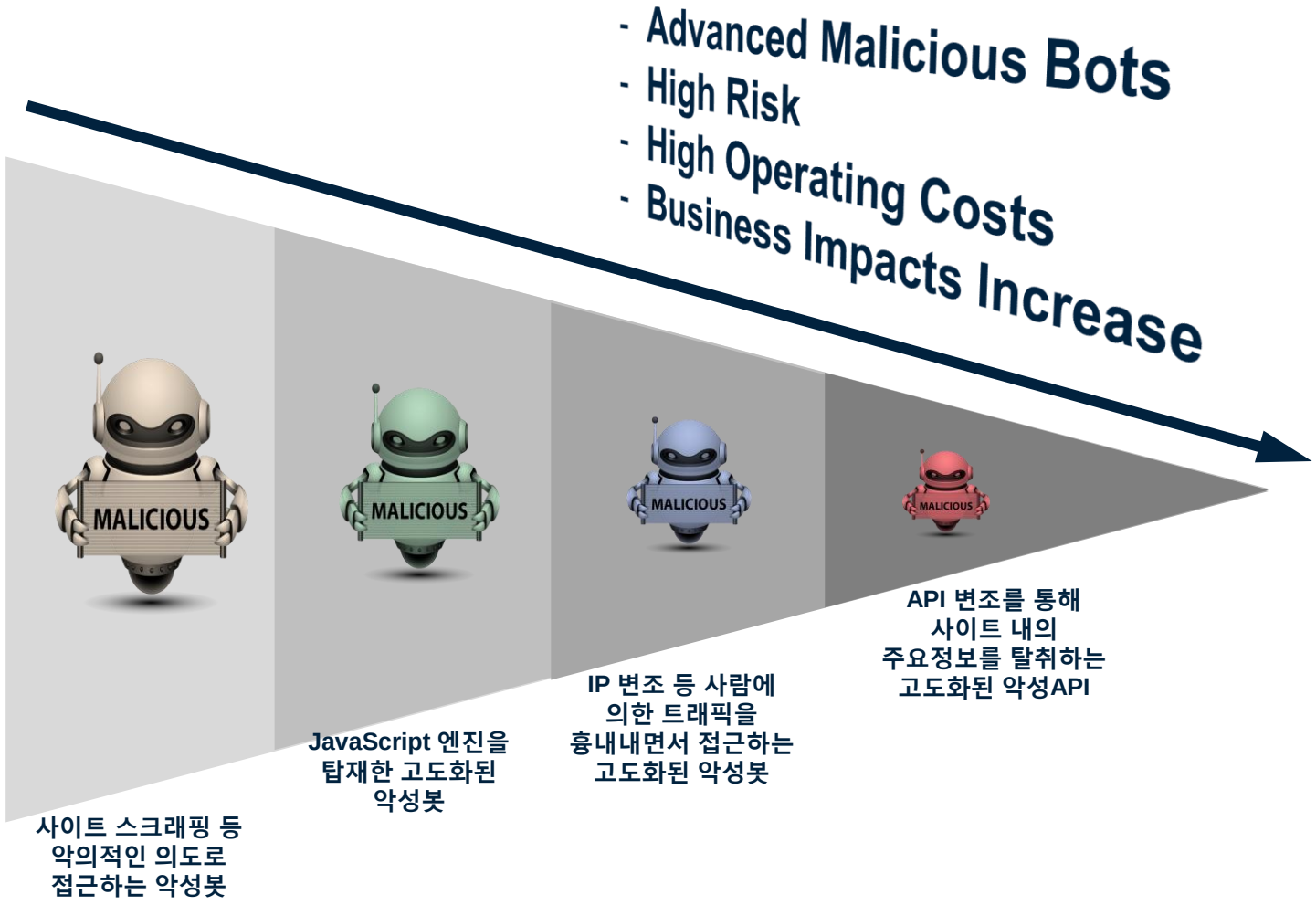
# 악성 봇 트래픽 탐지 및 차단

# 악성 봇 트래픽의 증가 – 비즈니스 임팩트 증가

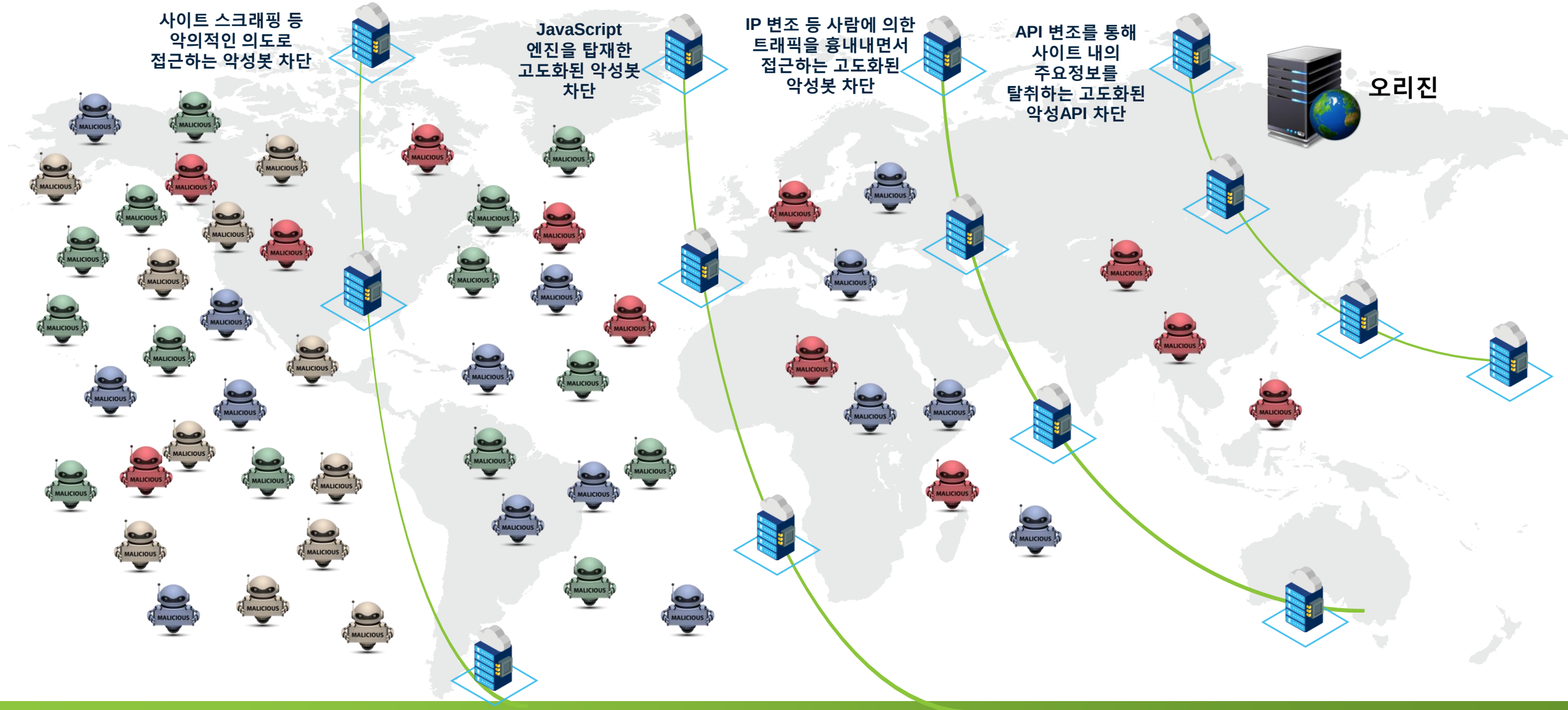


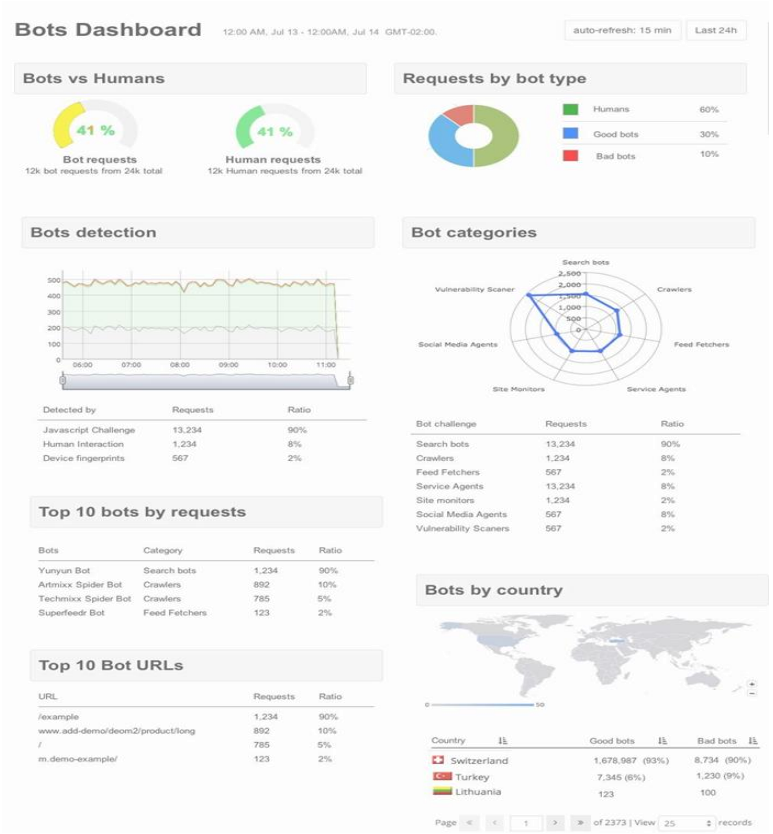

*Source: Distil networks "2016 Bad bot report"*

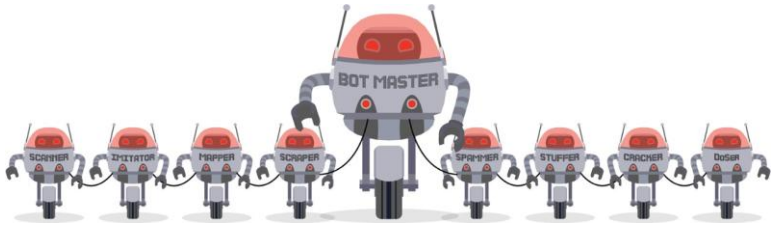


# 점점 변종으로 진화하는 악성 봇 트래픽



# 포괄적인 봇 트래픽 관리




**(Rate Limiting)**

특정시간 동안 단일 IP에서 웹 어플리케이션으로 동일한 요청에 대한 임계값을 설정하고, 임계값을 초과하면 지정된 시간동안 모든 요청을 차단하는 방식

**(CAPTCHA)**

스크립팅된 봇은 보안 문자를 해석하고 대응할 수 없기 때문에, 신속하고 간단하게 사용자-정의 가능한 챌린지로서 합법적인 사용자 외에 접근을 차단하는 방식

**(Java Script Challenge)**

모든 사용자, 공격자, 클라이언트에게 자바 스닛펫을 보내고, 합법적인 사용자는 통과하게 되며 자바 스크립트가 탑재되지 않은 봇 트래픽은 차단하는 방식

**(Human Interaction Challenge)**

소수의 봇이 표적 공격을 할 때 유용하게 활용할 수 있는 방식으로, 봇이 따라할 수 없는, 마우스 움직임, 특정 웹페이지에 머문 시간 및 페이지 스크롤과 같은 휴먼 인터랙션을 찾는 터닝 테스트 기법을 적용

**(Device Fingerprinting)**

50개 이상의 속성을 기반으로 실제 또는 가상 브라우저에 대한 해시서명을 생성해서 정교한 봇 툴킷을 차단하고, 이 해시서명에 대한 실시간 상관관계 분석해서 악의적인 봇을 식별하고 차단하는 방식 → **IP를 지속적으로 변경하여 공격해오는 봇 공격을 원천적으로 봉쇄 가능**

# 악성봇 탐지 및 분석 사례 1

| IP address | Country | Alerts | Actions |
|---|---|---|---|
| 80.80.3.130 | Denmark | 109,445 | View logs |
| 14.29.124.53 | China | 16,600 | View logs |
| 178.238.42.164 | Czech Republic | 7,113 | View logs |
| 185.8.239.16 | Czech Republic | 2,145 | View logs |
| 52.74.46.77 | Singapore | 1,967 | View logs |
| 14.29.124.52 | China | 1,794 | View logs |
| 113.107.136.48 | China | 1,548 | View logs |
| 110.77.183.34 | Thailand | 1,389 | View logs |
| 46.229.76.2 | Russian Federation | 1,123 | View logs |
| 60.21.209.114 | China | 1,106 | View logs |

Page « ‹ 1 › » of 1 | View 250 records

## IP belongs to infare.com

- 봇 매니저 도입 전까지 중국으로부터의 봇 공격만 인지
- 봇 매니저 도입 후, 10만 건 이상 덴마크에서 휴먼 인터랙션 챌린지 및 자바스크립트 챌린지를 통과하지 못한 봇 공격으로 의심되는 트래픽 감지
- 로그 분석 후, 덴마크에서 발생되는 80% 이상의 트래픽이 infare.com에서 발생한 것을 인지하고 해당 IP 차단
  **Infare.com** - 항공사의 운항, 운임, 가격 정보 등을 스크래핑하여 다른 항공사에 판매하는 웹사이트

63,411 logs found from 6:45:00 PM October 22 to 6:44:59 PM October 23, 2016, GMT -04:00

| Time | Log type | IP | Response | Action | Request |
|---|---|---|---|---|---|
| 6:44:57pmOct 23 | JS Challenge | 80.80.3.130 Denmark | | Alert | /Select.aspx |

| | |
|---|---|
| Date | 6:44:57pm, Oct 23 -04:00 |
| Type | JS Challenge |
| Action | Alert |
| Client IP | 80.80.3.130 |
| Country name | Denmark |
| User agent | Mozilla/5.0 (Windows NT 6.3; rv:31.0) Gecko/20100101 Firefox/31.0 |
| HTTP verb | GET |
| Request URL | /Select.aspx |
| HTTP headers | 14 headers |
| HTTP version | 1.1 |
| Incident ID | 2016-10-23T22:44:46Z\|6d1aa26335\|80.80.3.130\|BDMwJY2ijB |
| Fingerprint | |
| Country code | DK |

# 악성봇 탐지 및 분석 사례 2

| IP address | Country | Alerts | Actions |
|---|---|---|---|
| 80.80.3.130 | Denmark | 109,445 | View logs |
| 14.29.124.53 | China | 16,600 | View logs |
| 178.238.42.164 | Czech Republic | 7,113 | View logs |
| 185.8.239.16 | Czech Republic | 2,145 | View logs |
| 52.74.46.77 | Singapore | 1,967 | View logs |
| 14.29.124.52 | China | 1,794 | View logs |
| 113.107.136.48 | China | 1,548 | View logs |
| 110.77.183.34 | Thailand | 1,389 | View logs |
| 46.229.76.2 | Russian Federation | 1,123 | View logs |
| 60.21.209.114 | China | 1,106 | View logs |

Page « ‹ 1 › » of 1 | View 250 records

## End user on AWS?

- AWS에서 요청이 오는 트래픽을 탐지
- 이를 기반으로 AWS 혹은 호스팅 업체를 통해 들어오는 트래픽을 분석하여 케이스 별로 차단 또는 허용

```
# The following results may also be obtained via:
#
https://whois.arin.net/rest/nets;q=52.74.46.77?showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ext=netref2
#

NetRange:       52.64.0.0 - 52.79.255.255
CIDR:           52.64.0.0/12
NetName:        AT-88-Z
NetHandle:      NET-52-64-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        1991-12-19
Updated:        2015-03-20
```

# 악성봇 탐지 및 분석 사례 3

| IP address | Country | Alerts | Actions |
|---|---|---|---|
| 80.80.3.130 | Denmark | 109,445 | View logs |
| 14.29.124.53 | China | 16,600 | View logs |
| 178.238.42.164 | Czech Republic | 7,113 | View logs |
| 185.8.239.16 | Czech Republic | 2,145 | View logs |
| 52.74.46.77 | Singapore | 1,967 | View logs |
| 14.29.124.52 | China | 1,794 | View logs |
| 113.107.136.48 | China | 1,548 | View logs |
| 110.77.183.34 | Thailand | 1,389 | View logs |
| 46.229.76.2 | Russian Federation | 1,123 | View logs |
| 60.21.209.114 | China | 1,106 | View logs |

Page « ‹ 1 › » of 1 | View 250 records

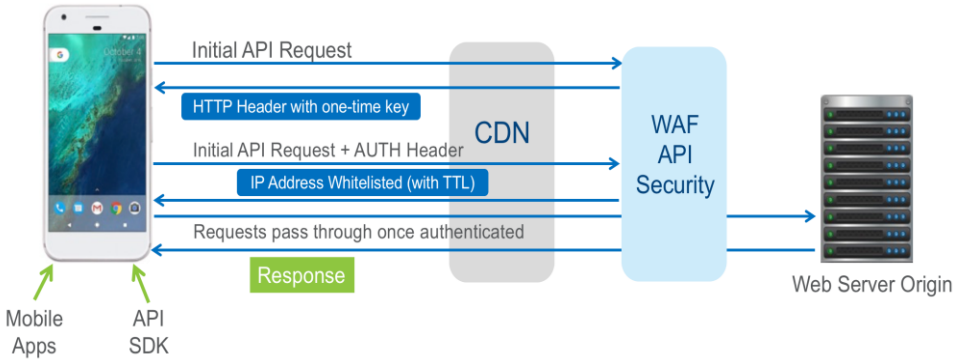
## China Telecom Guangdong province

- 중국 광동에서 동일한 디바이스를 활용하여 IP를 지속적으로 변경하여 운임 가격을 스크래핑 하는 것을 탐지
- 디바이스 핑거 프린팅 기능을 통해 해당 트래픽 원천적으로 봉쇄
- 로그를 클릭하면 기기 정보 및 핑거 프린트를 확인 가능

| 14.29.124.53 IP address location & more: | |
|---|---|
| **IP address [?]:** | 14.29.124.53 [Whois] [Reverse IP] |
| **IP country code:** | CN |
| **IP address country:** | China |
| **IP address state:** | Guangdong |
| **IP address city:** | Guangzhou |
| **IP address latitude:** | 23.1167 |
| **IP address longitude:** | 113.2500 |
| **ISP of this IP [?]:** | China Telecom Guangdong |
| **Organization:** | China Telecom Guangdong |
| **Local time in China:** | 2016-10-24 07:07 |

# 고급 API Security


API INTERFACE




## 악의적 API 사용, 자동 API 스크래핑 및 API 하이재킹에 대한 고급 보안 서비스

***1.* API 엔드 포인트 보안** (End Point Security)

- 고도화 알고리즘을 통한 API 데이터 추출이나 탈취를 방지
- 손쉬운 모바일 SDK 개발을 통한 인증 방식 사용으로 기존의 IP Rate Limiting을 통하여 방어하지 못하는 공격 감지
- Layer 3/4/7 DDoS 방어

***2.* API 엑세스 컨트롤** (Access Control)

- API 요청에 대한 IP Blacklist / Whitelist
- Geo Blocking고도화 알고리즘을 통한 API 데이터 추출이나 탈취를 방지

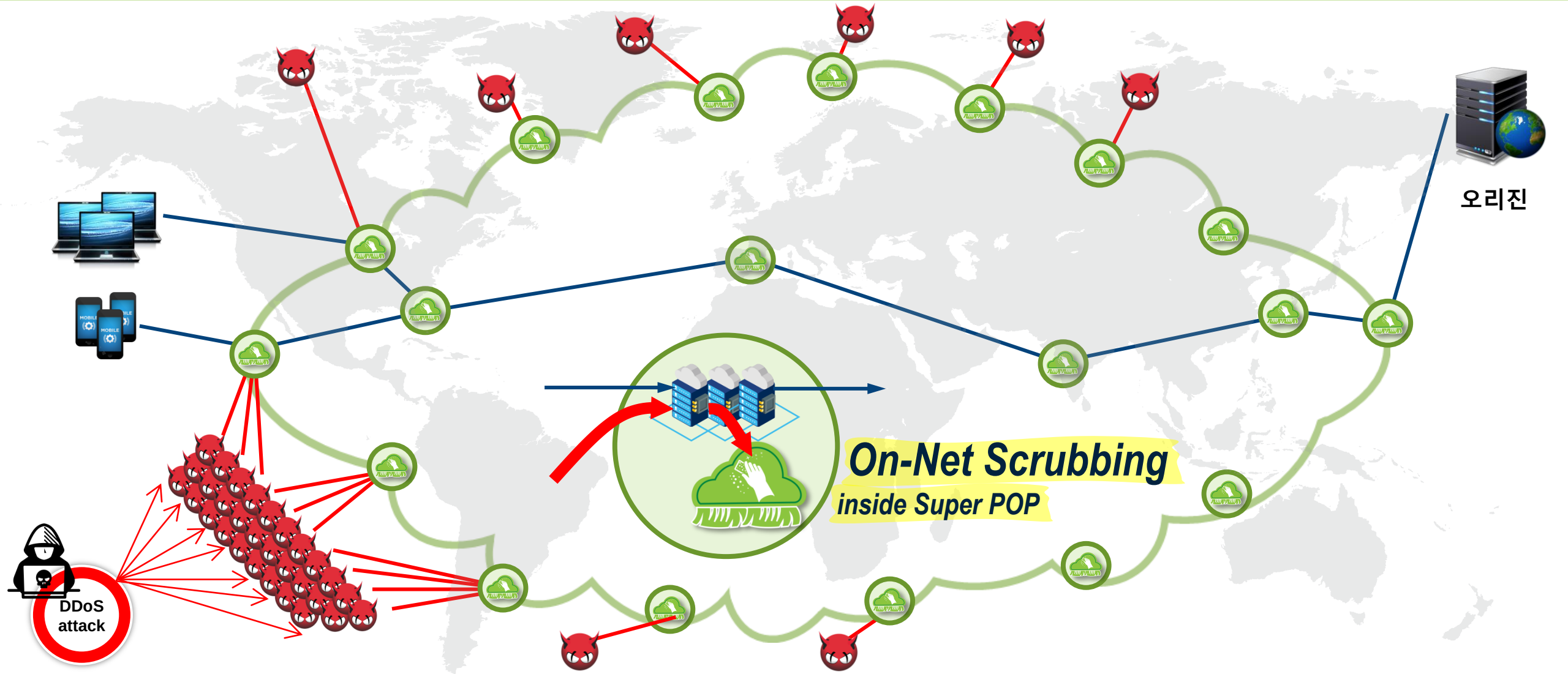
***3.* API 보안 룰** (Security Rules)

- API 요청에 대하여 Rule을 셋팅하여 방어

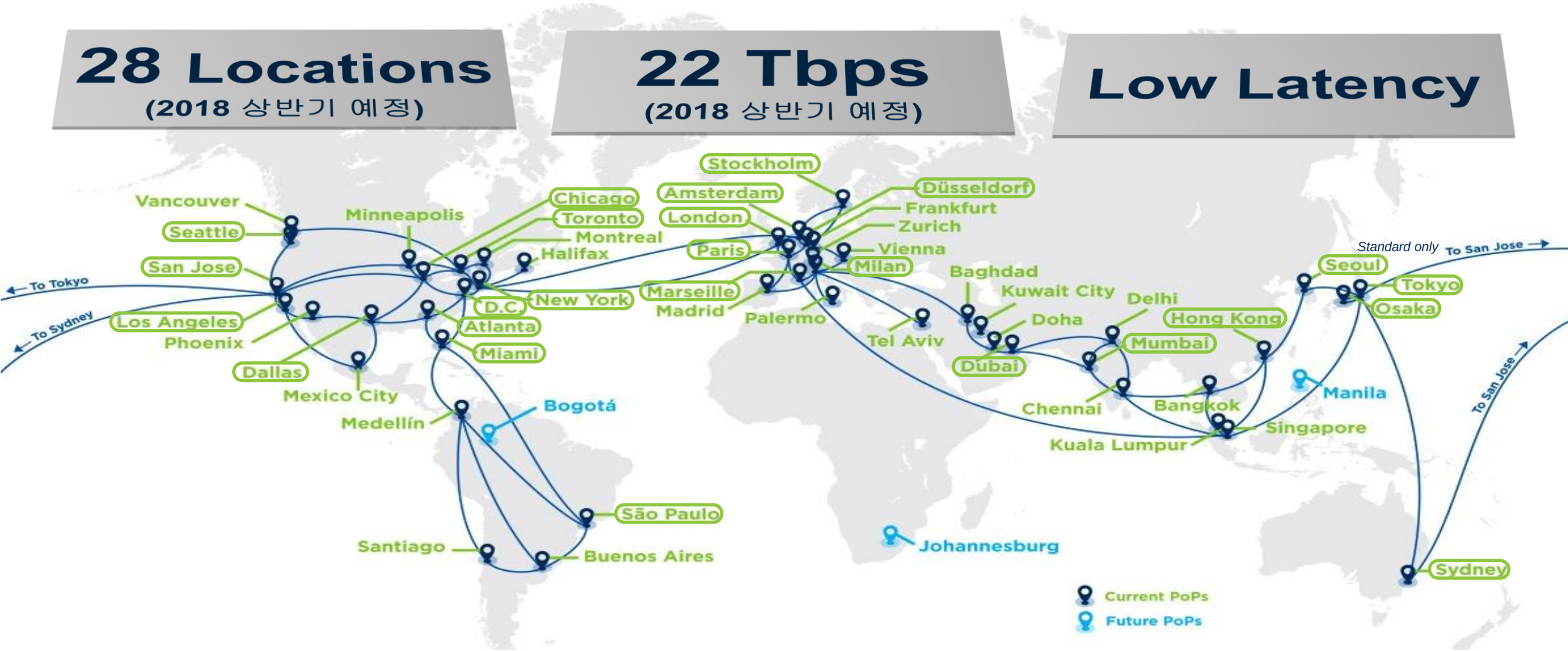
# 대용량 디도스 공격 방어

# 퍼블릭 클라우드 스크러빙 방식 – 이슈들

# 28개 지역 Scrubbing Center 및 On-Net Scrubbing을 통한 Latency 최소화



# 22 Tbps + On-Net Scrubbing

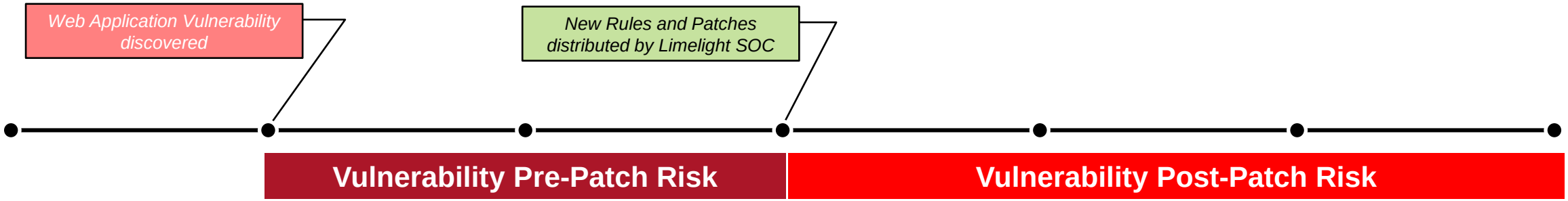



# 제로 데이 취약점

# AI 기법을 활용한 제로 데이 공격 탐지

***Behavioural-based determination of maliciousness to trigger blocking***

- AI WAF는 인공지능 머신러닝 프로세싱으로 새로운 유형의 악성 트래픽을 스스로 탐지하고 보고합니다.
- AI WAF는 관리자의 학습지도를 통해 더욱 정확해 집니다. 관리자의 판단에 의한 학습지도를 통해서 악의적이고 신뢰할 수있는 모델을 AI WAF에 가르치고, AI WAF는 학습한 모델에 따라서 반복적으로 스스로 탐지하고 보고합니다.
- 궁극적으로 AI WAF는 악의적인 요청을 인식하고 보다 정확한 신뢰할 수 있는 요청을 이해하도록 심화학습을 받습니다.



# 머신 러닝을 통한 Zero-Day 탐지 및 오탐률 최소화

| Date | Request | Score | Learn action |
|---|---|---|---|
| 4:26:01pm Feb 22 | /membership/index.do?a=ftp.exe | 48% | Trusted Malicious |
| 4:23:19pm Feb 22 | /membership/index.do?a=telnet.exe | 48% | Trusted Malicious |
| 4:23:15pm Feb 22 | /membership/index.do?a=telnet.exe | 48% | Trusted Malicious |

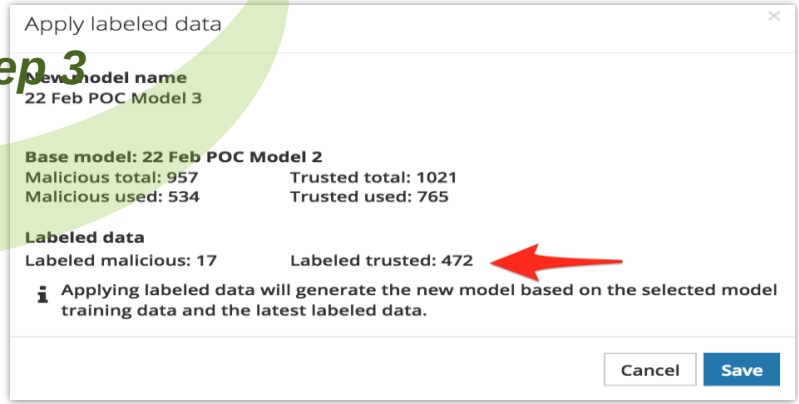
Step 1

| Date | Request | Score | Learn action |
|---|---|---|---|
| 4:26:01pm Feb 22 | /membership/index.do?a=ftp.exe | 48% | Trusted Malicious |
| 4:23:19pm Feb 22 | /membership/index.do?a=telnet.exe | 48% | Trusted Malicious |
| 4:23:15pm Feb 22 | /membership/index.do?a=telnet.exe | 48% | Trusted Malicious |

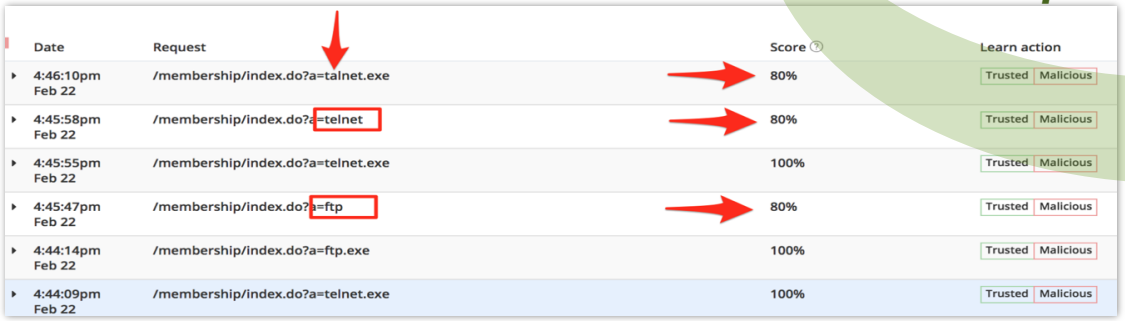
Step 2

**Supervised Machine Learning**
**반복적인 심화학습**

Step 3

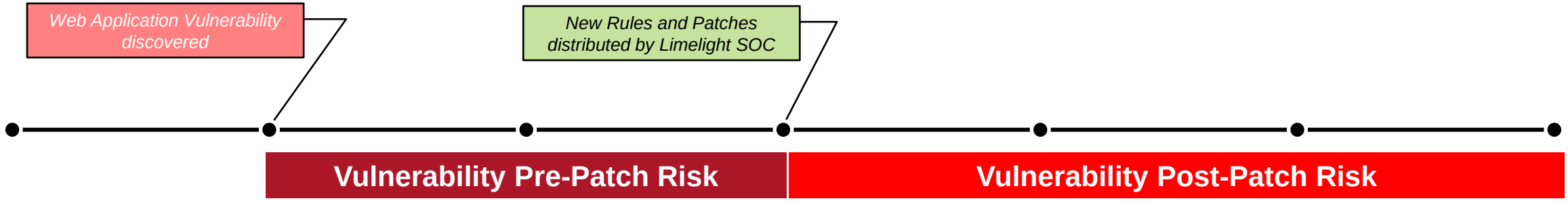



Step 4



| Date | Request | Score | Learn action |
|---|---|---|---|
| 4:46:10pm Feb 22 | /membership/index.do?a=talnet.exe | 80% | Trusted Malicious |
| 4:45:58pm Feb 22 | /membership/index.do?a=telnet | 80% | Trusted Malicious |
| 4:45:55pm Feb 22 | /membership/index.do?a=telnet.exe | 100% | Trusted Malicious |
| 4:45:47pm Feb 22 | /membership/index.do?a=ftp | 80% | Trusted Malicious |
| 4:44:14pm Feb 22 | /membership/index.do?a=ftp.exe | 100% | Trusted Malicious |
| 4:44:09pm Feb 22 | /membership/index.do?a=telnet.exe | 100% | Trusted Malicious |

# N-Day 취약점 – 고객과 밴더 보안전문가 협업




**57%**

Cyberattack victims who say an available patch could have prevented their breach

Source: ServiceNow study conducted by the Ponemon Institute

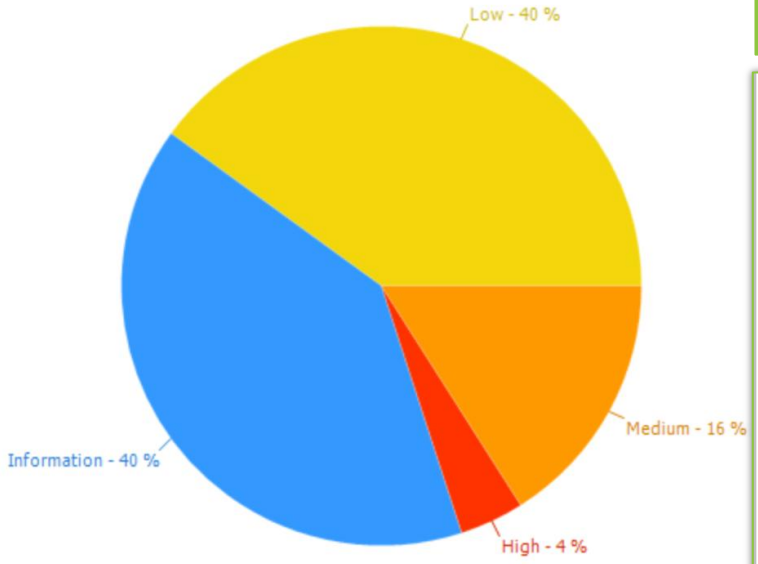
**74%**

Companies can't patch fast enough because they don't have enough staff

Source: ServiceNow study conducted by the Ponemon Institute

# Advanced Service를 통한 주기적인 취약점 분석 서비스

*Developing, testing, and deploying a virtual patch to mitigate Open Redirect vulnerability*




데이터 사이언스 팀의
위험도 분석 결과

The custom rule template to mitigate the open redirect flaw

```
SecRule REQUEST_URI "^\/accounts\/v1\/MBR\/signInGate" \
  "phase:request, \
  id:400544,\
[redacted]
  chain, \
  deny, \
  log, \
  t:none,\
  severity:CRITICAL,\
  msg:' Netsparker - Open Redirection: /accounts/v1/MBR/signInGate [goBackURL]
Matched Data: %{TX.0}',\
  tag:'Custom',\
  logdata:'Open Redirection: /accounts/v1/MBR/signInGate, Matched Data: %{TX.0}
found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\
  capture,\
  setvar:'tx.msg=%{rule.msg}',\
  setvar:tx.anomaly_score=+%{tx.critical_anomaly_score},\
  setvar:'tx.%{rule.id}-OpenRedirection-%{matched_var_name}=%{matched_var}'
```

Cancel

This log entry shows the rule triggered as a result of a test exploit script.

1 logs found from 5:30:53 PM February 20 to 5:45:53 PM February 20, 2018, GMT -05:00 — to Excel | Refresh

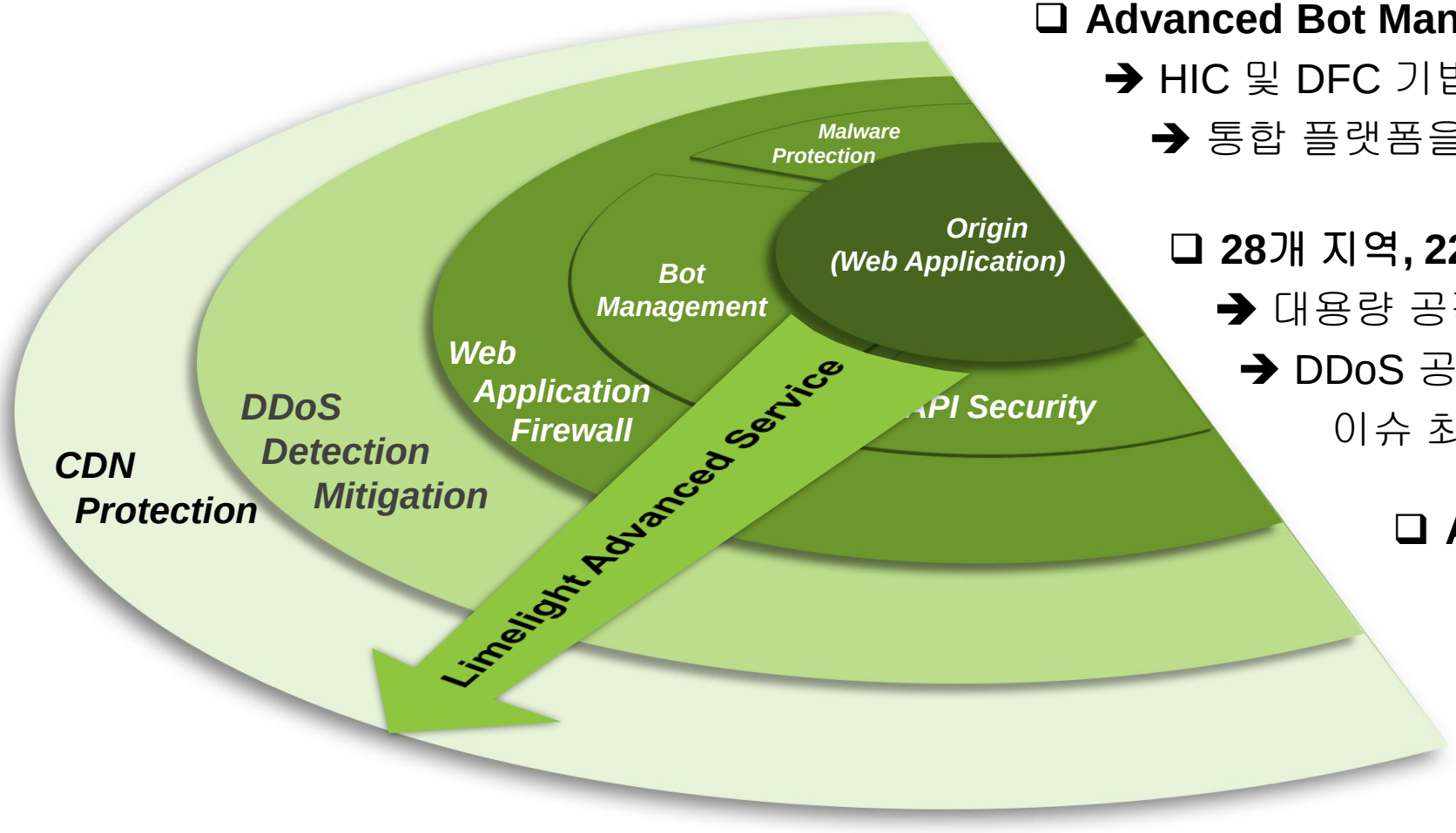
| Time | Log type | IP | Response | Action | Request |
|---|---|---|---|---|---|
| 5:41:51pm Feb 20 | WAF | [redacted] | | Alert | /accounts/v1/MBR/signInGate?MarcosNe&id=htpp://Mars&goBackURL=%3c%3a%2f%5c |

| | |
|---|---|
| Date | 10:41:51pm, Feb 20 +00:00 |
| Type | WAF |
| Client IP | [redacted] |
| User agent | Mozilla / Marcos Negreira |
| Domain | [redacted] |
| WAF alerts | 2 alerts |

| Rule ID | Alert message |
|---|---|
| 960034 | Message: HTTP protocol version HTTP/2.0 is not allowed by policy. Allowed are HTTP/1.0 HTTP/1.1<br>Message details: Warning. Match of "within %{tx.allowed_http_versions}" against "REQUEST_PROTOCOL" required. |
| 400544 | Message: Netsparker - Open Redirection: /accounts/v1/MBR/signInGate [goBackURL] Matched Data: /accounts/v1/MBR/signInGate<br>Message details: Warning. Pattern match "<\|%3c\|:\|%3a\|/\|%2f\|\\\|%5c" at ARGS: goBackURL. |

| | |
|---|---|
| HTTP verb | GET |
| Request URL | /accounts/v1/MBR/signInGate?MarcosNe&id=htpp://Mars&goBackURL=%3c%3a%2f%5c |
| HTTP headers | 6 headers |
| HTTP version | HTTP/2.0 |
| Action | Alert |

# 라임라이트 다계층 심층 방어 전략




❑ **Advanced Bot Management를 통한 어플리케이션 보호**

➔ HIC 및 DFC 기법을 통한 지능화된 Bot 방어

➔ 통합 플랫폼을 통한 API 공격 방어 지원

❑ **28개 지역, 22Tbps 용량 + On Net Scrubbing**

➔ 대용량 공격에 대한 잠재적 위협 해소

➔ DDoS 공격 시 발생할 수 있는 Latency 이슈 최소화

❑ **AI WAF를 통한 Zero Day 공격 방어**

❑ **N-Day 공격 방어를 위한 Advanced Service 지원**

Limelight Networks (NASDAQ: LLNW), a global leader in digital content delivery, empowers customers to better engage online audiences by enabling them to securely manage and globally deliver digital content, on any device. For more information visit our website http://www.limelight.com/.

# 감사합니다

Limelight NETWORKS