

효과적인 Multi Cloud 보안을 위한 WAAP 전략

모니터랩 | 박호철

Contents

- WAF => WAAP로의 변화
- WAAP에서의 주된 기능
API protection, Bot mitigation, DDoS
- Hot issue: credential stuffing
- CDN과 결합한 Cloud 기반 WAAP

WAAP (Web Application & API Protection)



By 2026, 40% of organizations will select a WAAP provider on the basis of its advanced API protections and web application security features.



Web Security

- SQLi, Commandi, XSS, CSRF 등 웹 사이트에 직접적이고 위협적인 공격들을 차단합니다.



API Security

- API 트래픽의 완전한 구문분석과 토큰 무결성 검증을 통해 접근 제한 및 공격 차단, API Request 위변조를 감지 합니다.



Bot Mitigation

- 크리덴셜 스테핑, 콘텐츠 스크래핑 등 악의적인 목적의 Bot 트래픽을 식별 하고 접속을 제한 합니다.



L7 DDoS Mitigation

- GET 플러딩, RUDY, Slowloris, SlowRead 등 HTTP 기반의 서비스 거부 공격을 완화합니다.

생활속의 API(Application Programming Interface)

https://data.kma.go.kr/api/selectApiDetail.do

기상청 기상자료개방포털

국가기후데이터센터 소개 | 국가-기 | 로그인 | 사이트맵 | 즐겨찾기

'관측'을 검색하세요

기상자료개방포털이란? | 데이터 | 기후통계분석 | 간행물 | 소통과 참여

Open-API

• 자료설명

기상청에서 제공하는 Open-API 목록을 조회하고 활용 신청할 수 있도록 링크를 제공합니다.

• Open-API 이용방법

기상자료 개방포털 접속 > Open-API 목록 확인 > Open-API 이용방법 확인 및 신청 > Open-API를 이용 어플리케이션에 적용

• Open-API 활용신청 방법

- 공공데이터포털 이용가이드를 참고하시기 바랍니다.
- 공공데이터포털: data.go.kr



https://www.data.go.kr/data/15000314/openapi.do#

DATA .GO.KR

데이터찾기 | 국가데이터맵 | 데이터요청 | 데이터활용

종 > 국가데이터맵

오픈API 상세

XML | JSON | 서울특별시_버스도착정보조회 서비스

특정 정류소에 대한 버스 도착예정 정보 제공

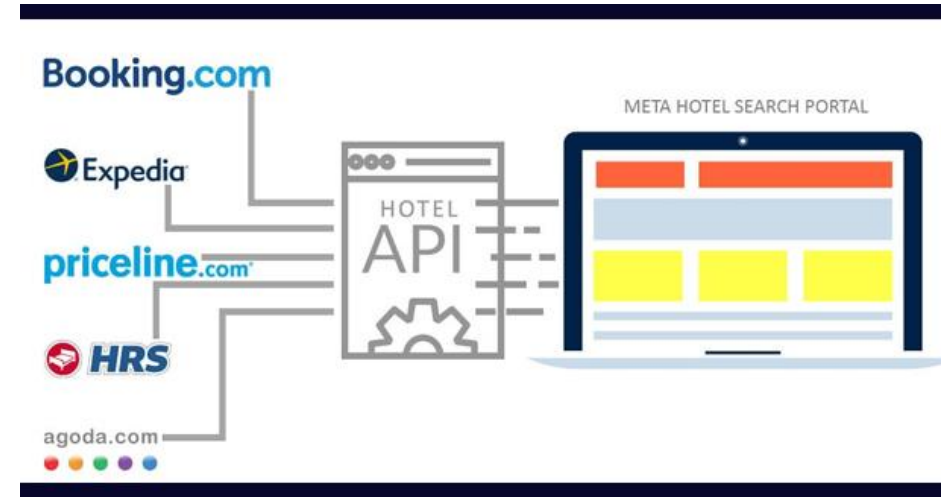
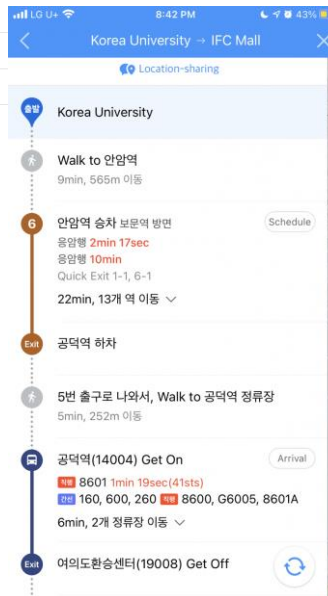
특정 정류소의 모든 버스 도착정보는 "서울특별시_정류소조회 서비스"에서 제공

11 1 관심

OpenAPI 정보

메타데이터 다운로드 | 오픈API 에러코드

분류체계	교통및물류 - 도로
관리부서명	미래첨단교통과
API 유형	REST



Skyscanner

Flights | Hotels | Car Rental

New York (Any) - Barcelona (BCN)

1 adult | Economy

Get Price Alerts

1099 results

Sort by Best

Want to know the latest travel restrictions for Spain? See travel info

Best \$597 (9h 50m (average))

Cheapest \$494 (25h 38m (average))

Fastest \$1,340 (8h 10m (average))

Book with confidence

Change your travel dates with our flexible rebook guarantee

More info

7:45 PM JFK -> 10:00 AM¹ BCN

Non-stop

12:00 PM BCN -> 3:00 PM JFK

Non-stop

Sponsored \$1,340

Select ->

flylevel.com

New York - Barcelona Flight - Flights at the Best Price - Flexible Booking

flytap.com

Flights Barcelona - Book Now on FlyTAP - FlyTAP.com

airfrance.us

New York-Barcelona \$491 - Best Fares with Air France®

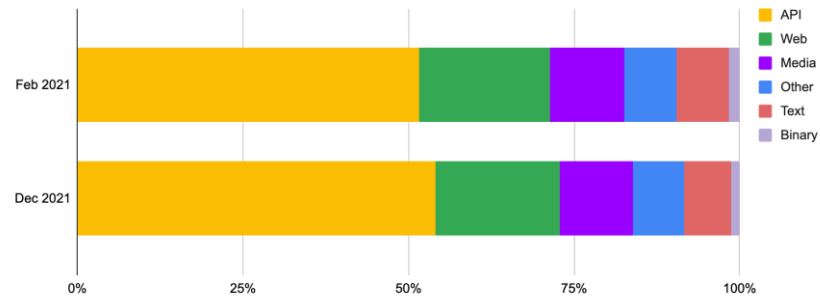
API 트래픽의 증가

절반 이상의 트래픽이 API

Response type:

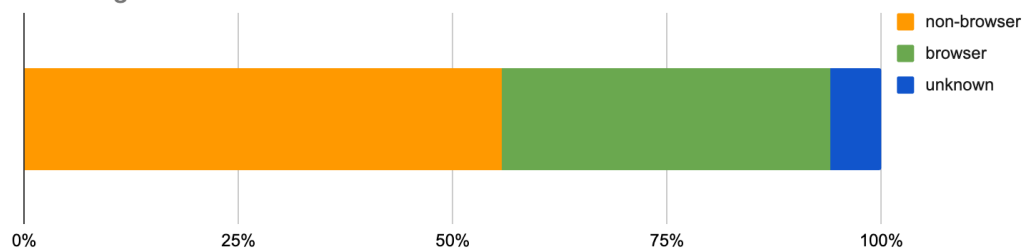
application/json, application/xml, text/xml

Traffic composition by content type

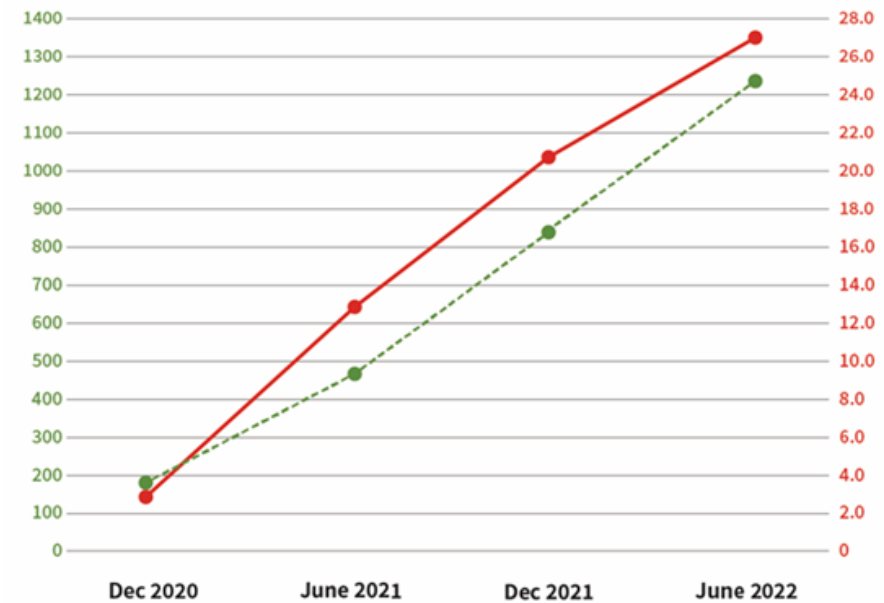


Browser(38%) Ajax API Call
Non-browser(56%) Mobile Apps, IOT devices

User-Agent distribution for API traffic



API call Volume
in millions



API Security가 이슈인 이유?

- ✓ API관련 보안 사고가 지속적으로 발생



VB VentureBeat

Twitter API security breach exposes 5.4 million user...



Security Magazine

Clubhouse API allows everyone to scrape ...

- ✓ API사용증가(Mobile, IOT, Cloud, MSA등)
- ✓ API 사용에 따른 보안의식 부재
기존의 WAF에서는 차단 불가
WAF: signature, pattern (' or 1=1--;)
API: logic /users/gildong/info => /users/admin/info

- ✓ OWASP API Security 2023



T-Mobile

Learn From The T-Mobile API Breach

Improve your API Security program in 2023



BOLA
(Broken Object Level Authorization)

API Discovery – OAS, Profiling

Web Application & API Protection

Domain Info

Analytics

Security Event

CDN Settings

Access Control

API Security

Web Security

Bot Management

Security Settings

Report

Alarm Setting

API Discovery

WEB Application & API Protection / API Discovery

Return to API Security List

Authentication Header	Block: None	Changed
Schema Validation	Off: 18case(s) Detect: 0case(s) Block: 1case(s)	Changed
Request Rate Limit	Off: 19case(s) Detect: 0case(s) Block: 0case(s)	Changed

Swagger Petstore - OpenAPI 3.0

This is a sample Pet Store Server based on the OpenAPI 3.0 specification. You can find out more about Swagger at [\[https://swagger.io\]](https://swagger.io) (<https://swagger.io>). In the third iteration of the pet store, we've switched to the design first approach! You can now help us improve the API whether it's by making changes to the definition itself or to the code. That way, with time, we can improve the API in general, and expose some of the new features in OAS3. If you're looking for the Swagger 2.0/OAS 2.0 version of Petstore, then click [\[here\]](https://editor.swagger.io/?url=https://petstore.swagger.io/v2/swagger.yaml) (<https://editor.swagger.io/?url=https://petstore.swagger.io/v2/swagger.yaml>). Alternatively, you can load via the "Edit > Load Petstore OAS 2.0" menu option! Some useful links: - [\[The Pet Store repository\]](https://github.com/swagger-api/swagger-petstore) (<https://github.com/swagger-api/swagger-petstore>) - [\[The source API definition for the Pet Store\]](https://github.com/swagger-api/swagger-petstore/blob/master/src/main/resources/openapi.yaml) (<https://github.com/swagger-api/swagger-petstore/blob/master/src/main/resources/openapi.yaml>)

/pet/findByStatus

GET /pet/findByStatus

/pet/findByTags

GET /pet/findByTags

Schema Validation

Schema validation protects the API service from invalid API requests. Validation works against the registered API schema for each request.

Q

Path Search

Total		Off	Detect	Block
GET	/pet/findByStatus	Off	Detect	Block
GET	/pet/findByTags	Off	Detect	Block
GET	/pet/{petId}	Off	Detect	Block
POST	/pet/{petId}	Off	Detect	Block
DELETE	/pet/{petId}	Off	Detect	Block
POST	/user	Off	Detect	Block
POST	/user/createWithList	Off	Detect	Block
GET	/user/logout	Off	Detect	Block
GET	/user/{username}	Off	Detect	Block
DELETE	/user/{username}	Off	Detect	Block
PUT	/user/{username}	Off	Detect	Block
POST	/pet	Off	Detect	Block

Change token validation rules

Return to Token Validation Rule List

Body inspection

Rule Name

22

Rule Description

22

Authentication header value(Token)

Add

h

Token Validation Control

☐ Verify JWT integrity
 ☐ Authentication server verification

Target API

test

Path Search

Target API

☐ Total
 ☒ GET /account-api-admin/account
 ☐ GET /account-api-admin/account/all

Action

☒ Detect
 ☐ Block

Select

Token, Payload validation

API Security 기능

Change Priority

Rate limit rule list + Create a new rule

Use	Rule Name	API Name	Target API	Condition	Action	Changed	Delete
	222	wfwd	API 1case(s)	Period : 10 Counts : 100 Block : 60	Detect		
	333		API 1case(s)	Period : 10 Counts : 100 Block : 60	Detect		
	111	test	API 1case(s)	Period : 10 Counts : 100 Block : 60	Detect		

1 to 3 of 3 entries

10 / pag Prev 1 Next

Rate limit

MONICLOUD

Web Application & API Protection

Change access control rules

[Return to the list of access control rules](#)

Rule Name

Rule Description

Client IP ☒ Bypass ☐ Block Add

Blocked countries list

Country list
Afghanistan
Aland Islands
Albania
Algeria
American Samoa
Andorra
Angola

Block Country

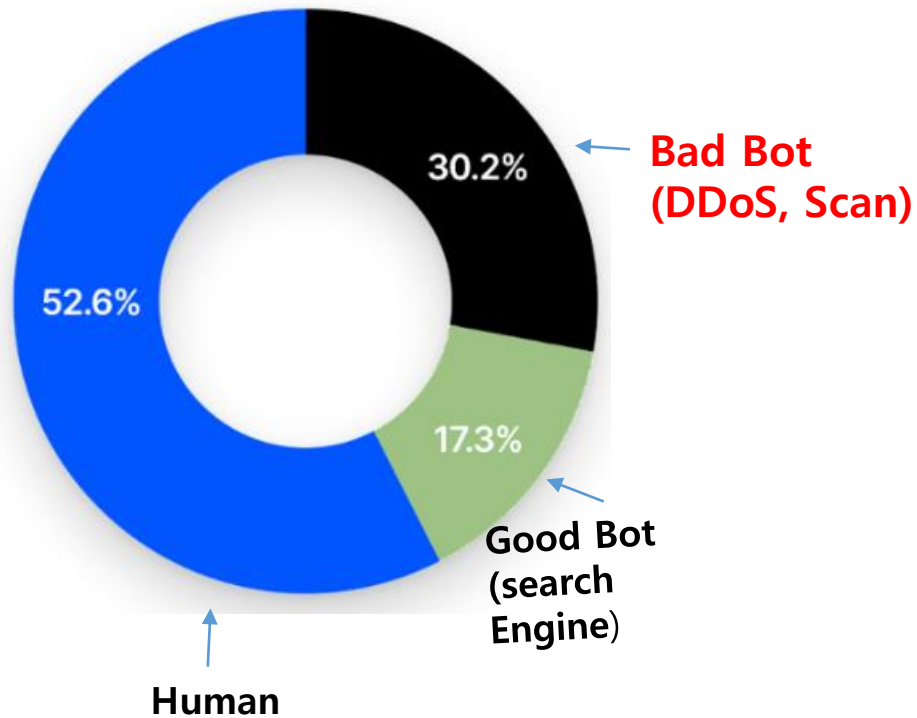
Claim Name Claim Value Add

Allow Claim

Target API

Path Search

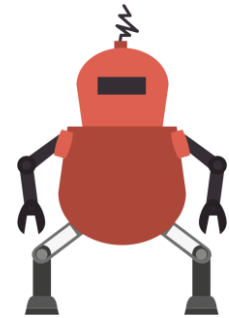
Access control



Bad Bot의 기능

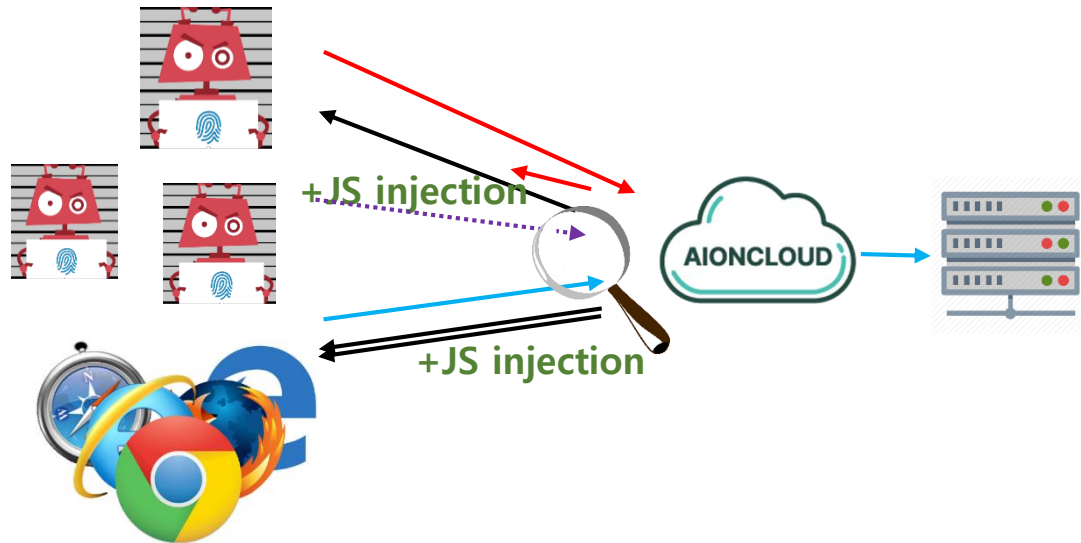
- ✓ Credential stuffing (brute force)
- ✓ DDoS 공격
- ✓ Site, contents scraping
- ✓ 취약점 scanning

=> 많은 트래픽과 과도한 시스템 부하 유발



#badbots

Bot mitigation



- ✓ JS injection을 통해 signature 검증
 - ✓ browser 인지 bot인지 검증
 - ✓ Mouse 이동이나 keyboard 등의 움직임이 있는지 또는 동일한 fingerprint를 가진 client가 있는지

Bot mitigation

Domain Info

Analytics

Security Event

CDN Settings

Access Control

API Security

Web Security

Bot Management

IP Reputation

Rate Limit

Forced Browsing

Advance

Credential Stuffing

Challenge Page

Security Settings

Report

Alarm Setting

Identifies and detects the Bot using Bot Management IP reputation information.

Security Settings

Tor Exit Node	'Tor Exit Node' is a term used in Tor, a privacy tool, which is designed to protect personal information. When using Tor, it is possible to hide one's IP address when browsing the internet or using online services. The last node (exit node) changes the user's IP address, which is called Tor Exit Node. You can take action on such requests that use Tor Exit Node.	Off	Detect	Verify	Block
Fake crawler	'Fake Crawler' is a fake bot that scrapes websites or collects data, and it is classified as a security threat. These fake bots are categorized as automated programs that websites do not permit, so blocking is recommended.	Off	Detect	Verify	Block
Known attack source	'Known attack source' is when HTTP traffic is detected from an IP address previously classified as malicious behavior. These IP addresses are classified as security threats and are recommended to be blocked because they can be used for attacks or hacking attempts on websites, spamming, and malicious server access.	Off	Detect	Verify	Block
Cgi Proxy	'CGI Proxy' is an online proxy service used for accessing websites. It is used to hide the IP address associated with the content used by a website. For example, users can use a CGI Proxy to hide their real IP address and anonymously access websites. Measures can be taken in response to requests made through a CGI Proxy.	Off	Detect	Verify	Block
Anonymizing VPN Service	'Anonymizing VPN Service' is a virtual private network (VPN) service that is used to hide Internet users' IP addresses and protect their privacy. With this service, Internet users connect to the Internet through a VPN server, which hides the actual IP address of the Internet user and uses the IP address of the VPN server instead. However, since it can be used for malicious purposes, you are recommended to block requests over Anonymizing VPN.	Off	Detect	Verify	Block
Web Proxy	'Web Proxy' refers to the proxy server that Internet users use to connect to the Internet. This server is used to hide your IP address and to anonymously protect your online activities. However, you are recommended to block the request because it can be used for malicious purposes.	Off	Detect	Verify	Block
Web Scraper	'Web Scraper' is a term used to refer to a program or script that collects information from a website on the Internet. These programs are used to extract and analyze data from websites, compare prices, recommend products, and collect information. However, some 'Web Scrapers' are recommended to be blocked because they may violate the website's terms of use, send spam messages, or cause legal problems such as copyright infringement	Off	Detect	Verify	Block

Hot issue: Credential stuffing

ITB IT비즈니스(ITBizNews)

“지금 당장 비밀번호 바꿔라”...개인정보 위협하는 '크리덴셜 스테핑' 주의보

불법으로 유통되는 계정 정보를 획득한 해커가 웹사이트에 무작위로 대입해 이용자의 정보를 탈취하는 크리덴셜 스테핑(Credential Stuffing) 공격이...



ABC

Byron Bay woman's Paypal data breach nightmare exposes risks of credential stuffing. So how do you avoid it?

A cyber security researcher says reusing passwords is like creating a skeleton key hackers can use to hijack accounts through a process...



조선비즈

“상품권이 사라졌다” 지마켓, 고객 계정 도용 피해 속출 - 조선비즈

온라인 쇼핑몰 지마켓의 고객 계정이 도용된 정황이 동시다발적으로 포착되면서 사용자들의 불안감이 커지고 있다. 19일 온라인 커뮤니티와 소셜...



시사포커스

정부 운영 '워크넷' 중국발 '크리덴셜 스테핑' 피해...개인정보 유출

[시사포커스 / 이창원 기자] 정부가 운영하는 취업 사이트인 '워크넷'에 중국 등 해외 IP의 무단접속으로 구직자의 성과와 출생연도, 주소...



보안뉴스

스타벅스, '크리덴셜 스테핑' 공격으로 일부 회원 계정정보 유출... 충전금 결제 도용까지

스타벅스코리아(이하 스타벅스)에서 일부 고객의 계정정보가 유출돼 해외 IP를 통해 애플리케이션에 부정 로그인이 시도된 것으로 알려졌다.



뉴스워커

지속해서 발생하고 있는 '크리덴셜 스테핑' 공격, 대응 방안 없나

많은 기업과 기관에서 '크리덴셜 스테핑(Credential Stuffing)'이라 불리는 해킹 공격이 반복해서 발생하고 있다. 특히 대부분 공격 시도는 포인트나...



보안뉴스

페이팔 사용자 3만 5천 명, '크리덴셜 스테핑' 공격으로 개인정보 잃어

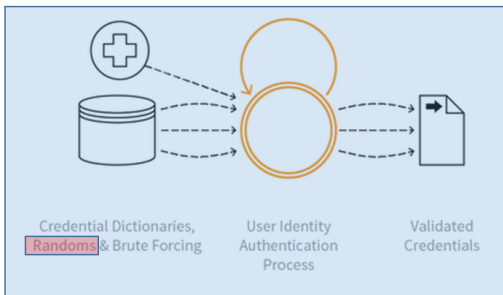
3만 5천 명에 달하는 페이팔 사용자 계정이 최근 발생한 크리덴셜 스테핑 공격으로 침해됐다. 이 때문에 약 3만 5천 명의 페이팔 사용자들의 개인정보...



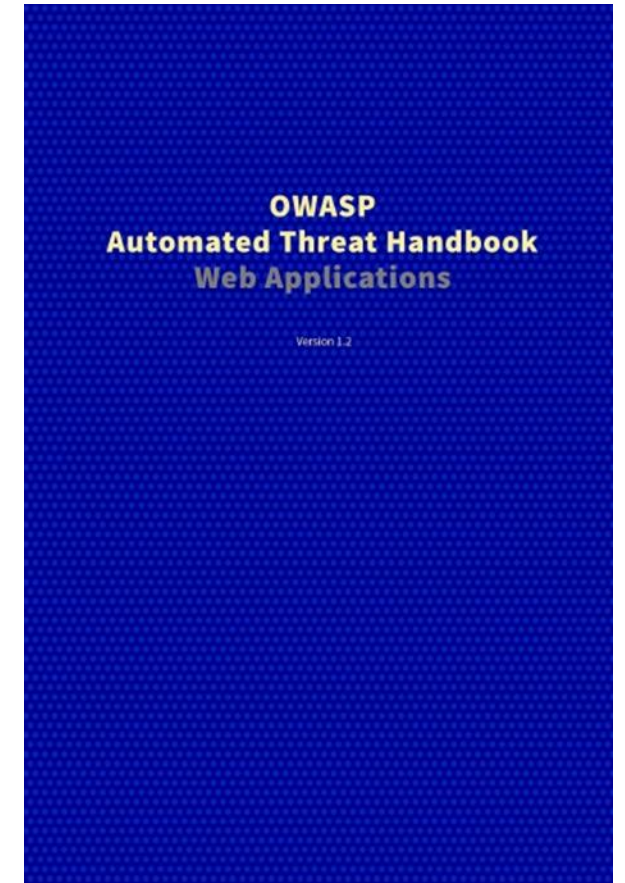
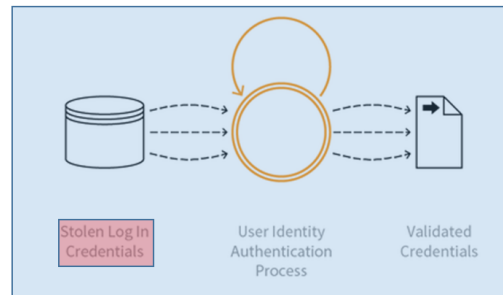
Credential stuffing과 관련된 통계

- ✓ 65%: passwords를 재사용함
- ✓ 73%: 개인 계정과 회사 계정의 암호를 동일하게 사용함
- ✓ 34% : 인증 트래픽의 다수가 malicious함(by OKTA)
- ✓ 0.2%~1%: credential stuffing 공격의 성공율

OAT-007 Credential Cracking(brute force)



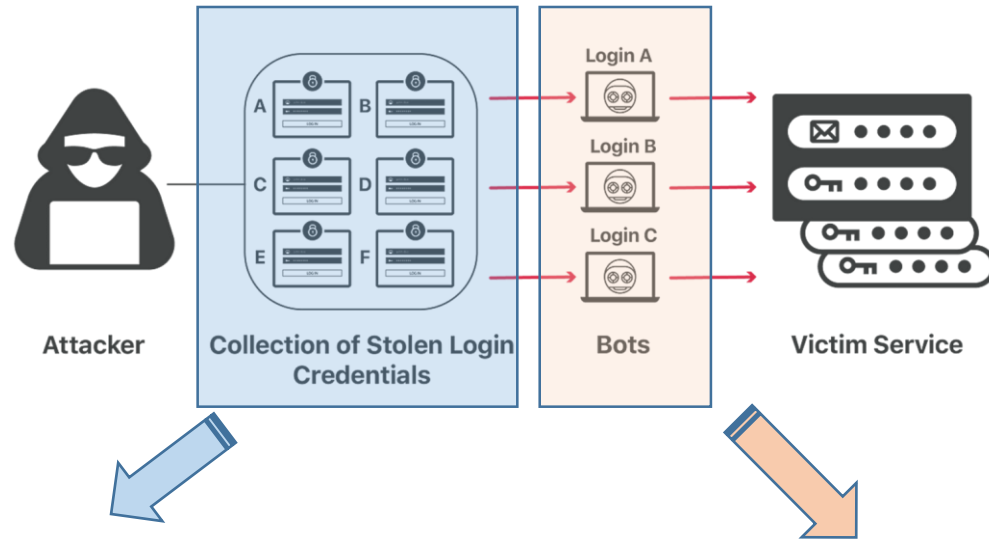
OAT-008 Credential Stuffing



OAT: OWASP Automated Threats

<https://owasp.org/www-project-automated-threats-to-web-applications/>

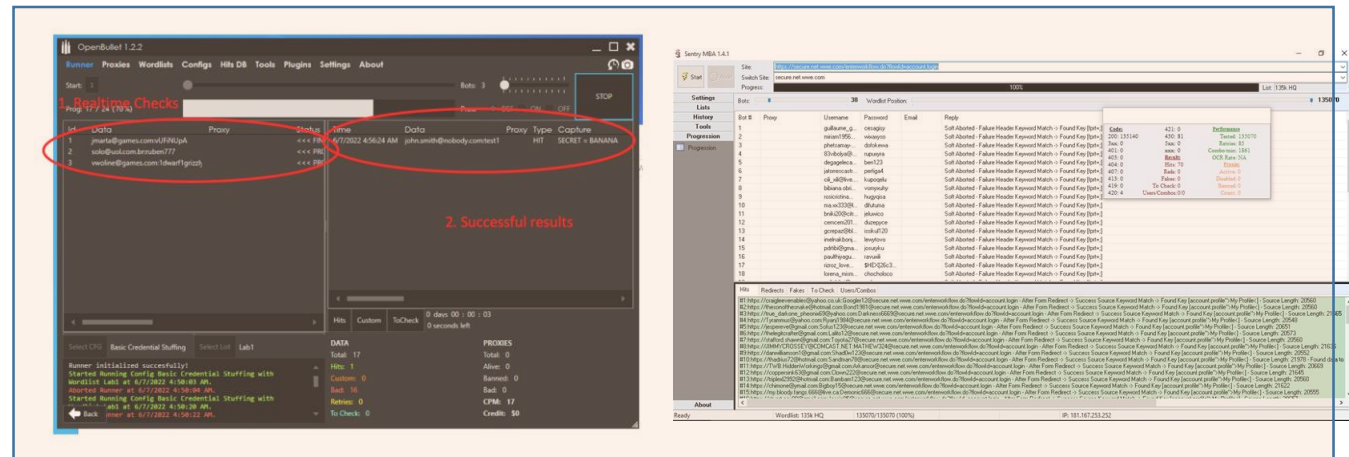
Credential stuffing 공격 작동 방식



Hacked databases store

Press **7** or **CTRL-F** on keyboard to search our database. Click table header to sort databases.

Year	Database	Site	Records	Price	Buy
2022	National Police database NEW!	cn	1,022,398,123	\$1064	buy
2021	zenship database NEW!		37,198,240	\$72	buy
2015	ghost Database	most.com	13,545,468	\$46	buy
2021	Database		8,661,578	\$41	buy
2013	ew Database	ew.to	18,965	\$20	buy
2014	N Database	om	586	\$19	buy
2016	ia (17) Database		28,052,322	\$62	buy
2011	Chinese Database	em	9,755,600	\$42	buy
2011	atabase		9,072,977	\$41	buy
2018	atabase Collection		80,115,532	\$117	buy
2018	Database	em	14,870,303	\$48	buy
2011	atabase		14,928,048	\$48	buy
2018	abase		15,025,407	\$48	buy



Open Bullet, MBA Sentry 등

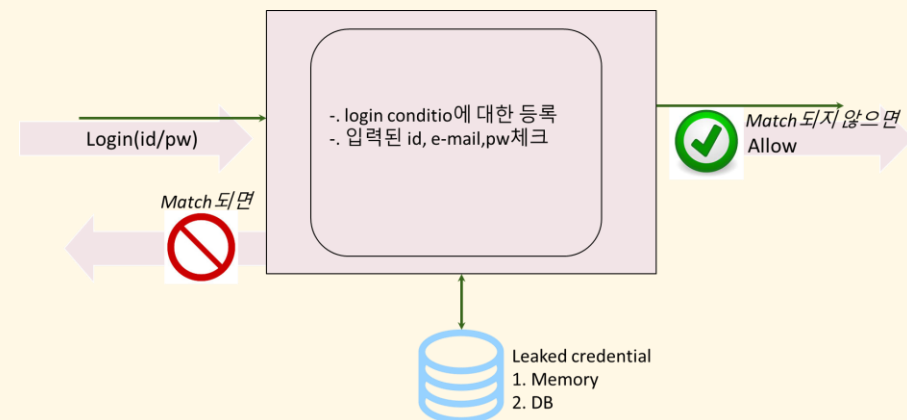
User 입장

- ✓ MFA 활성화
- ✓ 암호 자주 변경(90일)
- ✓ 암호 관리툴을 이용, 서로 다른 암호 사용
- ✓ 국가별, device별 접근 제어 적용
- ✓ Login 목록 체크

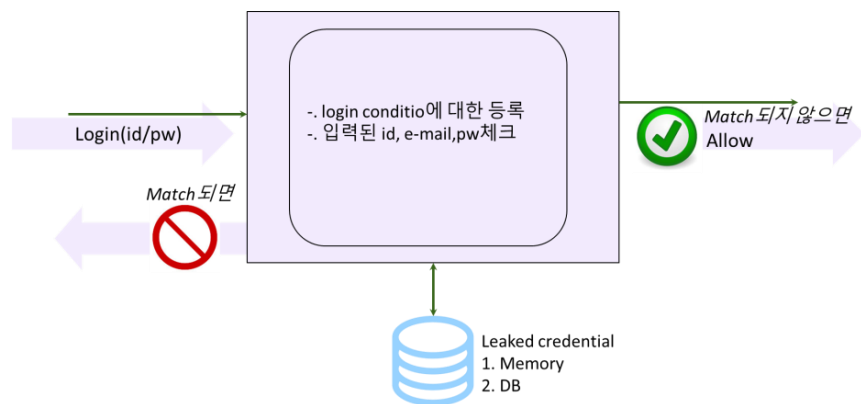
The screenshot shows the '기본보안설정' (Basic Security Settings) section of the MONITORAPP interface. It includes fields for '비밀번호' (Password) with a '수정' (Edit) button, and '2단계 인증' (2-step authentication) with a '관리' (Manage) button. Below this is the '로그인 차단 설정' (Login Blocking Settings) section, which has a toggle for '타지역 로그인 차단' (Block login from other regions) set to OFF and a toggle for '해외 로그인 차단' (Block login from overseas) set to ON. The '새 기기 로그인 알림' (New device login notification) section has a toggle for '로그인 알림' (Login notification) set to ON and a '확인' (Check) button for '로그인 알림 제외 목록' (Login notification exclusion list). At the bottom, there is a green status bar indicating '새로운 환경' (New environment) login notification is being provided.

서비스 제공자 입장

- ✓ /login에 대한 rate limit (느리게, proxy이용)
- ✓ Bot protection 활용
- ✓ Credential stuffing 기능 적용
 - 1개의 IP에서 서로 다른 username
 - **Leaked credential DB 활용**



Credential stuffing 공격 대응 기능



- Domain Info
- Analytics
- Security Event
- CDN Settings
- Access Control
- API Security
- Web Security
- Bot Management
 - IP Reputation
 - Rate Limit
 - Forced Browsing
 - Advance
 - Credential Stuffing**
 - Challenge Page
- Security Settings
- Report
- Alarm Setting

Blocks attacks that attempt to log in to web applications or APIs using leaked account information

Product Upgrade

Use ☒ On ☐ Off

Target URL junote.aionscloud.click / Add

Request field name Enter the name of the field that represents the user ID/email (ex: username, user_id, user_email) and password (ex: password, password) in the login request.

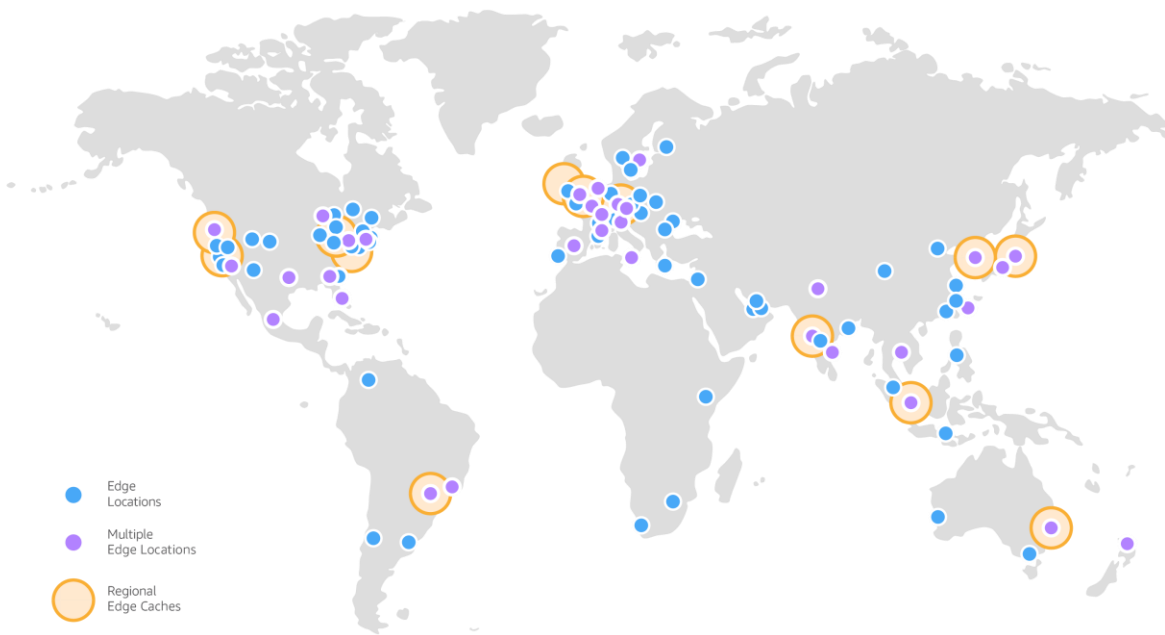
Types of credentials used Select the type of credentials used in the login request. (OR condition)
Account leakage will be assessed based on the selected type of credentials.

☐ ID ☐ Password ☐ Email

Action ☐ Detect ☒ Block

Apply

CDN과 결합한 WAAP Cloud 인프라

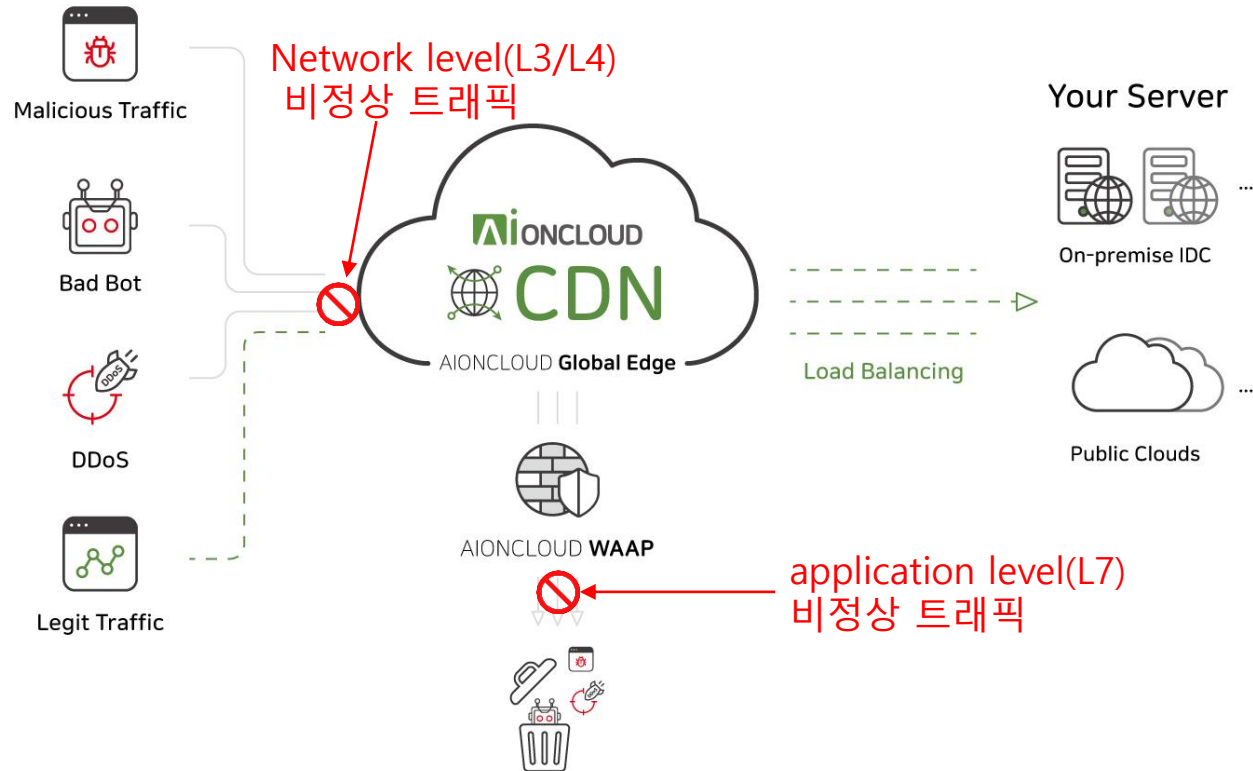


CDN Edges



- ✓ WAAP edges
- ✓ 15개국, 40여개의 IDC등에 인프라 운영중
- ✓ 지속 증가중

CDN과 WAAP의 결합으로 완벽한 DDoS대응



Type of DDoS	CDN INFRA	WAAP
SYN Flooding	O	
TCP/UDP/ICMP flooding	O	
UDP Amplification (DNS/NTP/SSDP)	O	
Smurf,teardrop,etc.	O	
Slowloris, RUDY,Hash		O
HTTP Flooding		O
Other L7 attack		O

클라우드 구독형 서비스 Vs CSP Native 보안 솔루션

	Security as a service	CSP Native 보안 솔루션
통합	독립적인 단일 지점	클라우드 플랫폼과의 강력한 통합
보안 기능	풍부한	제한된
전문 지원	자체 보안 전문가 보유	직접 운영 및 관리
Multi Cloud	다중 클라우드 지원	클라우드 플랫폼에 종속
비용	플랜별	개별 상품 구독(상품별 비용 발생)

Cloud는 선택이 아닌 필수이며 Cloud 전환에 보안은 가장 큰 고려 요소

웹 애플리케이션 프로덕션 환경과 독립적인 단일 지점에서 강력한 보안을 구성하고 관리

5분만에 설정하는 AIONCLOUD

Domain Type

☐ Root Domain

☒ Sub Domain

A domain with the prefixes such as www in front of the root domain, as shown in the example below.
ex) www.aioncloud.com , portal.aioncloud.com

Domain

Domain Check

CDN
(Content Delivery Network)

☐ Use

☒ Not Use

Accelerate your website, API downloads, streaming and more.

Origin Server
Protocol & Port

HTTPS

443

Add

HTTP

80

✕

HTTPS

443

✕

Address Type

CNAME

origin.example.com

Add

origin.example.com

✕

Origin Server
Address

☐ My Certificate

☒ AIONCLOUD Certificate

Use the SSL certificate provided by AIONCLOUD.

Domain
Certificate

Option to user certificate provided by AIONCLOUD for HTTPS connection without uploading the web server's certificate.
Issuing a certificate starts after changing the domain's DNS record to the WAAP address, and may take up to 5 minutes.

✕ Until the certificate is successfully issued, a certificate error may occur when accessing web services.

☒ Disagree

☐ I Agree

http → https Redirect

☐ Use

☒ Not Use

Apply → CNAME 정보 출력됨

✓ Security team이 필요없음

- . 설정이 쉽고 5분안에 설정완료
- . 룰 튜닝이 필요없음. No False positive.

✓ 추가적인 보안 솔루션이 필요없음: 완벽한 보안을 위한 One Stop solution

- . CDN: 무제한의 Network(L3,L4) DDoS attack 방어
- . WAAP: OWASP top10, L7 DDoS attack, Bot attack, API attack 대응
- . hidden cost가 없고 어떠한 서비스 업체보다 저렴함.

THANK YOU.

THANK YOU.