

Introducing

MBUSTER

매크로 탐지 및 차단 솔루션

STCLab Inc.



Bot Management

- 좋은 봇, 나쁜 봇
- 악성 봇 피해 사례
- 매년 증가하는 악성 봇
- 악성 봇 관리 포인트
- 손쉬운 매크로 접근성과 사용 용이성
- 악성 봇 매니지먼트 솔루션, 엠버스터

좋은 봇, 나쁜 봇

봇은 다양한 작업을 자동화하여 생산성 향상, 비용 효율성 및 고객 경험 개선, 서비스 운영에 도움을 주는 효과적인 프로그램이지만, 사용자에 따라 계정 유출, 사이트 공격, 불공정한 경쟁, 불법 이익 취득 등 악의적인 의도로 이용되는 경우가 있습니다.

봇(Bot)

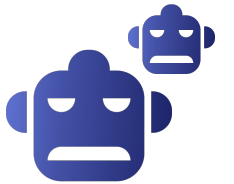


1. 특정한 반복 작업을 수행하도록 프로그래밍된 소프트웨어 응용 프로그램
2. 봇은 사람의 개입 없이 독립적으로 실행되며, 특정 명령에 따라 사람의 행동을 모방하지만 사람보다 더 빠르고 정확함

- **챗봇**: 프로그래밍된 응답으로 특정 문구에 응답함으로써 인간의 대화를 흉내내는 봇
- **웹 크롤러(Googlebots)**: 인터넷 전체의 웹페이지의 콘텐츠를 검색하는 봇
- **스크래퍼**: 인터넷에서 특정 콘텐츠를 스캔하고 다운로드하는 봇
- **쇼핑 봇**: 여러 웹 사이트에서 제품 가격을 검색하거나 개인별 추천을 전송
- **모니터링 봇**: 시스템에서 버그와 악성 소프트웨어를 지속적으로 검사
- **트랜잭션 봇**: 전자 상거래 사이트에서 결제 세부 정보가 올바른지 확인

※ 악성 봇 활동

- **크리덴셜 스테핑 봇**: 사용자 계정에 무단으로 접근하고 고객 포인트, 신용 카드 정보 등의 자산을 탈취
- **재고 사재기 봇**: 운동화, 콘서트 티켓 등 고부가가치 상품을 선점해 실제 이용자의 상품 구매를 제한
- **스팸 봇**: 스팸 메일 발송자가 사용할 이메일 주소를 구하기 위해 웹 사이트 검색
- **파일 공유 봇**: 사용자 검색 쿼리를 관찰, 컴퓨터를 감염(바이러스, 멀웨어)시킬 수 있는 가짜 링크 제공
- **트래픽 봇**: 웹에서의 인간의 활동을 모방해 트래픽 및 웹사이트 클릭 수 증가
- **소셜 미디어 봇**: 가짜 계정으로 특정 사용자 또는 계정의 아이디어를 지지하거나 팔로워 확대
- **다운로드 봇**: 소프트웨어 자동 다운로드로 애플리케이션 순위를 인위적으로 상승



악성 봇 피해 사례

악성 봇으로 인해 피해는 공공 재화에 대한 이용권 선점, 재판매를 통한 불법 이익 취득, 계정 도용 및 유출, 여론 및 순위 조작, 악의적 사이트 마비 등 전 산업군에 걸쳐 다양한 형태로 나타나고 있습니다.

홈플러스 “크리덴셜 스테핑 공격…
고객 정보 유출은 없어“

2019. 09. 26 보안뉴스

...

홈플러스에 따르면 이번 사건은 미상의 특정인(범죄자)이 **다른 사이트에서 불법으로 수집한 불특정 다수의 아이디와 패스워드를 홈플러스 온라인쇼핑몰에서 무작위로 입력해 무단 로그인을 시도** (크리덴셜 스테핑 공격, Credential Stuffing)했고, 이 중 성공한 계정(다른 사이트와 동일 아이디 및 패스워드 이용 고객)에 범죄자 본인의 OK캐쉬백 카드번호를 입력해 타인이 쇼핑한 내역을 자신의 OK캐쉬백 포인트로 절취한 사건이다.

경북경찰, ‘매크로 이용, 24억
암표판매 일당 18명 검거‘

2022. 12. 19 프레시안

...

매크로 프로그램을 이용해 각종 콘서트, 스포츠 경기 티켓 등 총 2만2000여매를 불법 구매해 암표 등으로 재판매해 도합 24억 상당의 부당 이익을 챙긴 혐의로 일당 18명이 검거됐다.

일당은 구매한 티켓을 액면가의 2배 이상을 받고 재판매했고 특히 인기 K-POP 콘서트티켓의 경우 16만5000원 짜리를 449만원에 재판매해 최대 28배의 부당이익을 챙겼다.

국내 포털서 압도적 중국 응원…
해외IP로 매크로 조작

2023. 10. 05 SBS

국가	응원 비율	클릭 수
중국	93.2%	3,130만 건
한국	6.8%	-

포털사이트 다음에서 지난 1일 열린 아시안게임 한중 축구 8강전 응원 클릭은 모두 3,130만 건. 이 가운데 한국 응원은 6.8%에 그친 반면, 중국 응원은 93.2%에 이릅니다. 한국 응원이 94%였던 네이버와 비교되며 조작 논란이 일었습니다.

다음 운영사 카카오는 응원 클릭은 로그인이 필요 없고 클릭 횟수 제한도 없었다며, **네덜란드와 일본 IP 두 곳을 거쳐 단시간 대규모 클릭이 발생한 것으로 파악했습니다.**

아카마이 “아태지역 금융 서비스,
전 세계에서 가장 많은 공격받는 산업“

2023. 10. 11 디지털데일리

...

한편 아카마이 보고서에 따르면 **아태지역의 악성 봇 트래픽은 2022년 대비 128% 증가**했다. 이는 금융 서비스 고객과 데이터에 대한 공격이 계속되고 있음을 나타낸다. 사이버 범죄자들은 봇을 사용해 공격의 규모, 효율성, 효과를 증폭한다.

아태지역은 금융 서비스에 대한 악성 봇 요청이 세계에서 두 번째로 많이 발생하는 지역으로, 전 세계 악성 봇 요청의 39.7%를 차지하는 규모다. **사용 사례로는 피싱 사기를 위해 금융 서비스 브랜드의 웹사이트를 사칭하는 웹 사이트 스크레이핑과 올진 사용자 이름과 비밀번호를 자동 삽입해 계정을 탈취하는 크리덴셜 스테핑 등이 있다.**

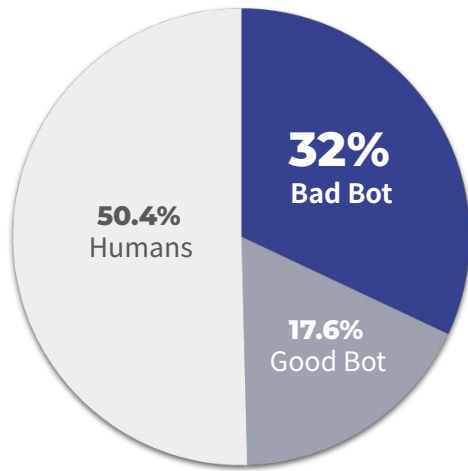
악성 봇은 서비스 공정성 훼손, 계정 도용 및 유출 등 **정당한 이용자의 피해**는 물론, **시스템 성능 저하**와 운영 비용 확대 등 **기업 운영 효율에 악영향**을 미칩니다.

매년 증가하는 악성 봇

악성 봇은 전체 인터넷 트래픽의 약 32%에 해당하며, 악성 봇에 의한 사이트 공격은 매년 증가해 서비스 공정성을 훼손하고 시스템 운영 효율을 저하하고 있습니다.

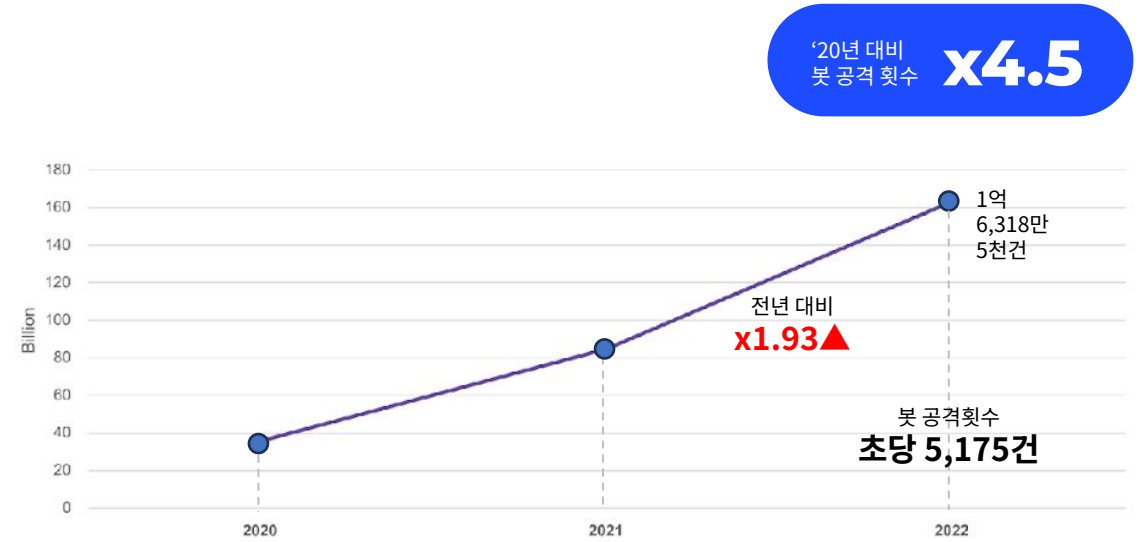
봇 트래픽 유형(2023)

출처 : 정보보안그룹 임퍼바(Imperva)



봇 공격 횟수(2020~2022)

출처 : CDNNetworks



매년 증가하는 악성 봇의 공격을 관리함으로써 **비즈니스를 보호**하고, **공정한 서비스로 온라인 관계의 신뢰성**을 지킬 수 있어야 함

악성 봇 관리 포인트

악성 봇 관리를 위해서는 봇 활동에 대한 탐지 과정과 함께, 개별 트래픽이 사람인지 봇인지 구분하는 검증과 차단 설정 등의 프로세스가 필요합니다.



손쉬운 매크로 접근성과 사용 용이성

누구나 인터넷 사이트를 통해 간단히 매크로 프로그램을 구매하거나 다운로드할 수 있으며, 기본적인 컴퓨터 지식만으로도 쉽게 매크로 프로그램을 작성하고 실행하는 것이 가능해졌습니다.

이러한 점은 매크로 프로그램의 사용을 대중화하고, 그로 인한 불공정한 경쟁을 촉진시키는 요인이 되고 있습니다

The screenshot displays a web interface for a macro program marketplace. At the top, there is a search bar containing the text "예약 매크로" (Reservation Macro) and a magnifying glass icon. Below the search bar, a horizontal navigation bar includes several filters: "카테고리 선택" (Category Selection), "세금계산서 발행" (Invoice Issuance), "MASTER 전문가" (Master Expert), "예산" (Budget), "prime", and "빠른응답" (Fast Response). The main content area shows a grid of macro products. The first row includes: "웹 매크로" (Web Macro) with sub-points like "자동입력 방지문자 자동화", "SMS 인증 자동화", "원우파일 자동 업로드", "주소 자동 입력", and "각종 입력, 클릭 자동화"; "웹 매크로 전문" (Web Macro Specialist); "자동화 프로그램" (Automation Program) with "맞춤 제작" (Custom Production); "예약, 맞춤 매크로" (Reservation, Custom Macro); and "선착순 예약 매크로" (First-come, first-served reservation macro). The second row includes: "예약 매크로" (Reservation Macro) with the tagline "손쉽게 끝내는!" (Finish easily!); "예약 자동화 윈도우 프로그램" (Reservation automation Windows program); "골프장 예약" (Golf course reservation) with "골프장 예약 '초차기' 솔루션 & 입원/퇴원 이전 완벽하게" (Golf course reservation 'first round' solution & perfect before admission/discharge); "자동 프로그램 매크로 제작" (Automatic program macro production); and "파이썬 매크로 자동화 크롤링" (Python macro automation crawling). Each product card features a heart icon in the top right corner.

악성 봇 매니지먼트 솔루션, 엠버스터

MBUSTER(엠버스터)는 실시간으로 접속하는 악성 봇을 다양한 방식으로 탐지하고 관리하여 불공정 거래로부터 이용자를 보호하고, 시스템 성능을 보장해 서비스 신뢰도를 확보할 수 있습니다.



- 실 사용자의 접속자 행위 추적 로그 생성
- 다양한 방법을 활용한 실시간 악성 봇 탐지
- 실시간 접속자에 대한 사람 / 봇 구분

정적 분석(시그니처 기반)

전세계 7만개의
봇 DB 활용한 탐지

동적 분석(휴리스틱 분석)

악성 봇 특징에 맞는
통계적 정책 활용한 탐지

머신러닝

이산사건 알고리즘을 활용한
악성 봇 접속 특정 및 패턴 분석

AI Manager

챗봇(ChatBot) 기능을 통한 대화형 대시보드 모니터링, 현황 분석 및 정책 설정

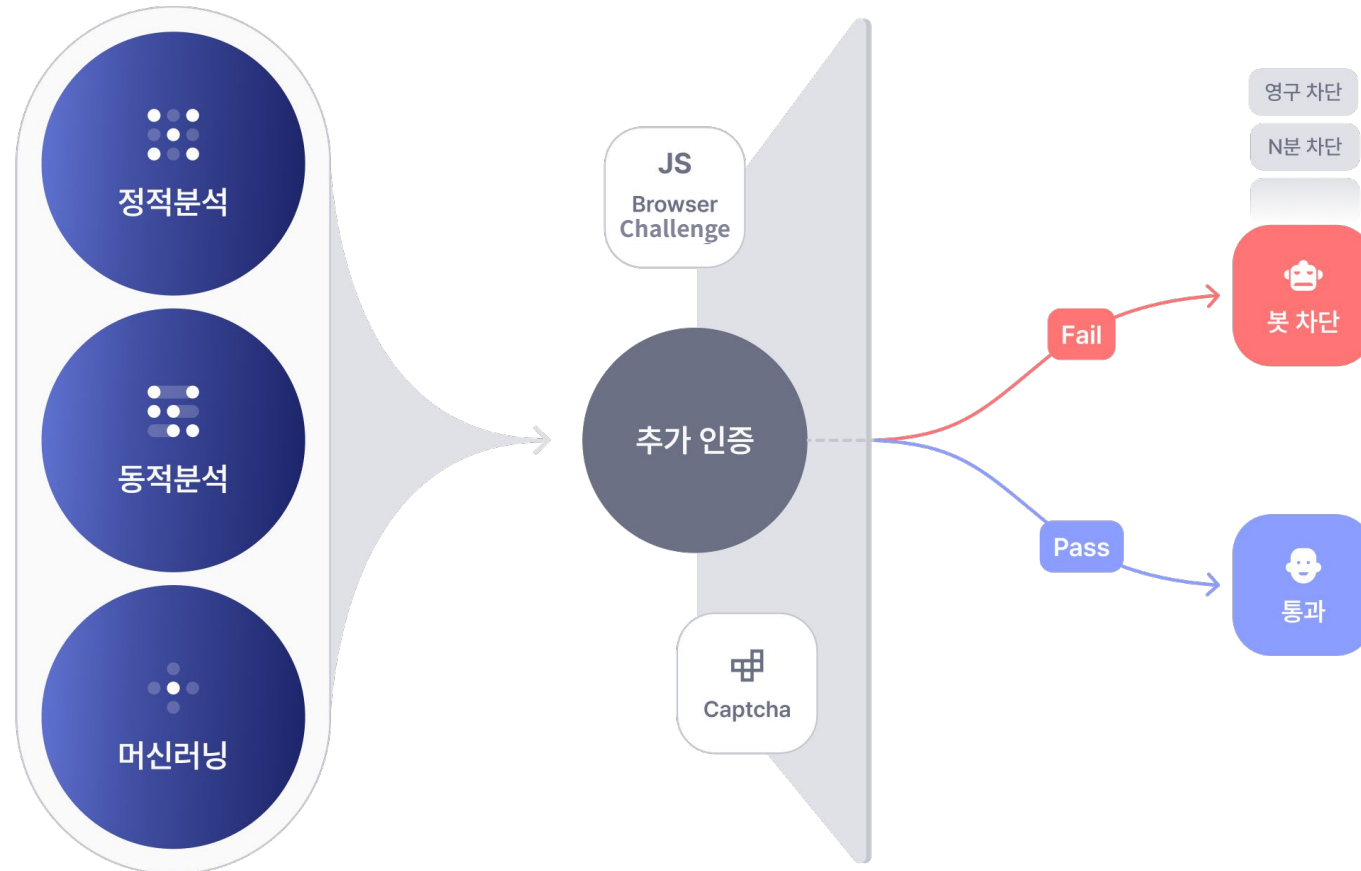
MBUSTER

- 로직
- 구성
- 주요 기능
- 주요 기능 비교
- 손쉬운 API 연동

로직

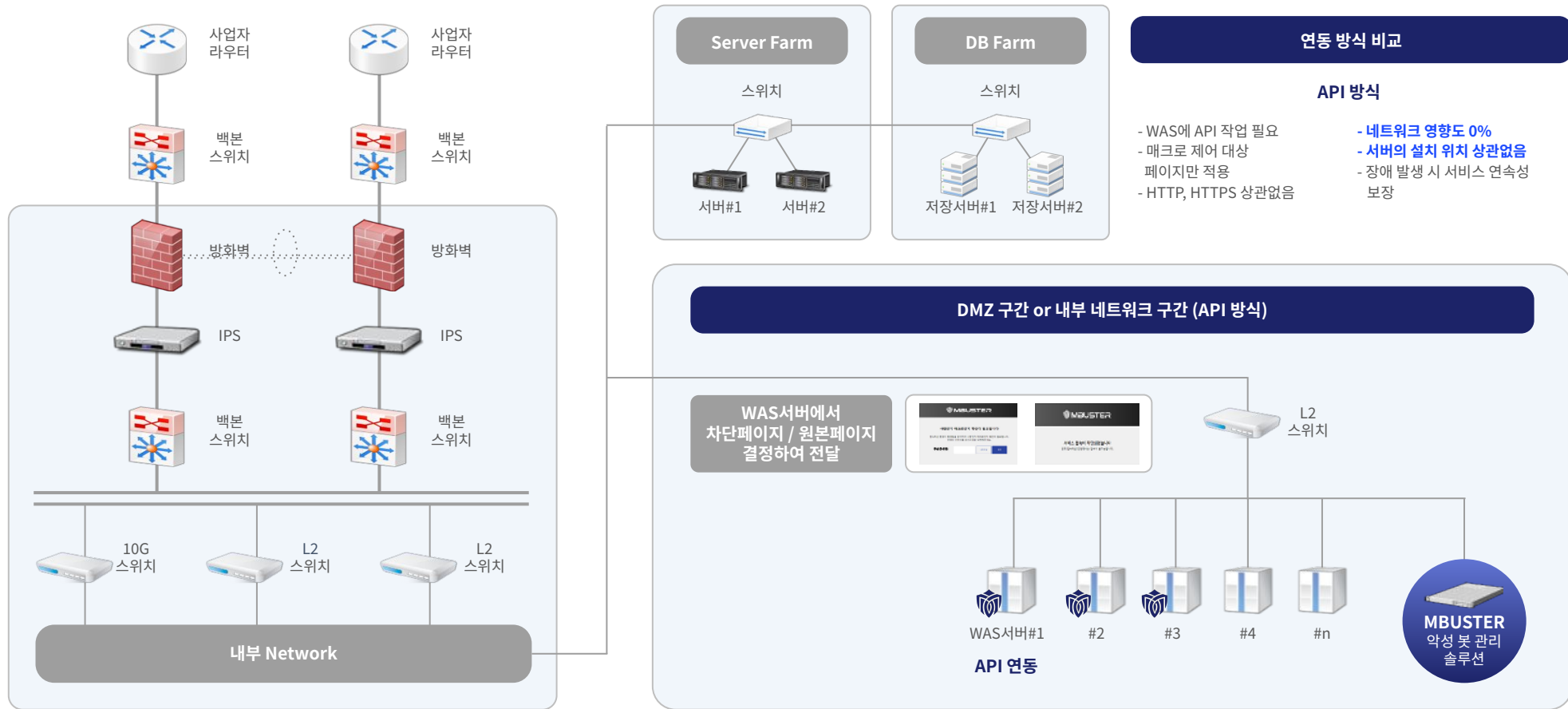
MBUSTER는 정적 분석을 통한 선제적 탐지 이후에도, 이용자의 서비스 이용 패턴에 따른 악성 봇 의심 트래픽에 대한 탐지 및 관리 프로세스를 진행합니다.

악성 봇 의심 트래픽에 대해서는 추가 인증을 통해 정상 서비스 이용 또는 차단 조치합니다.



구성

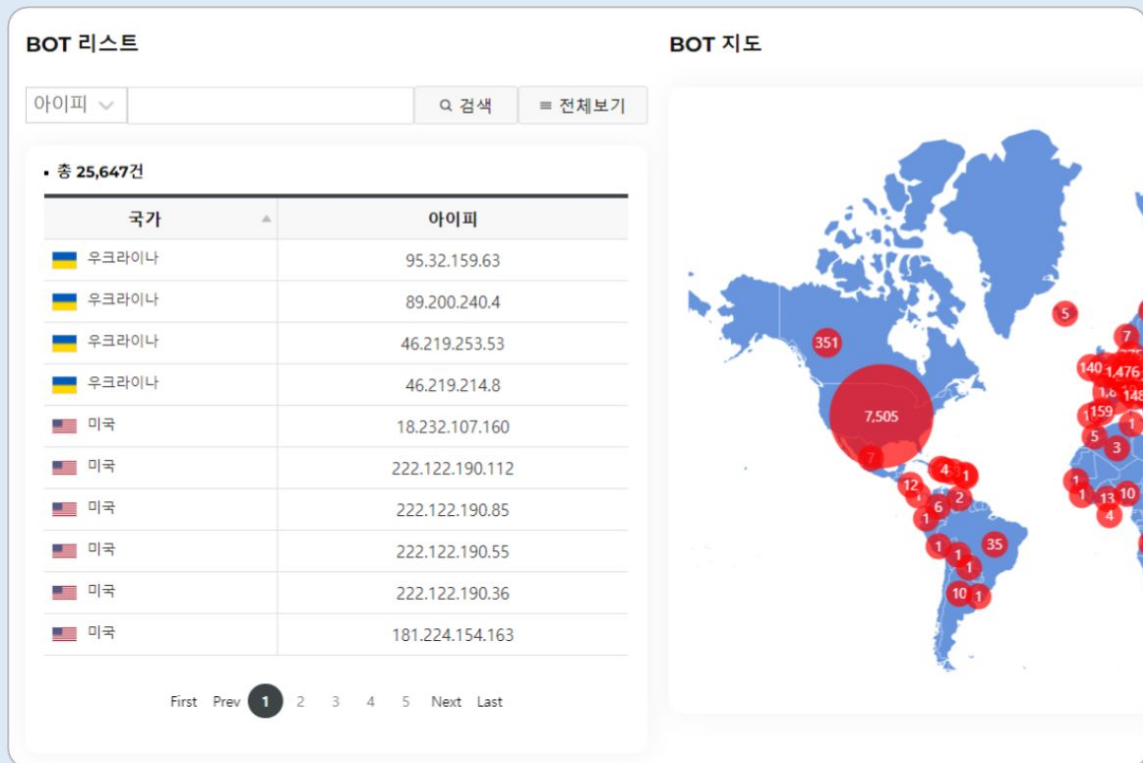
MBUSTER는 클라우드에서도 즉시 적용할 수 있는 소프트웨어 구성 환경을 지원합니다.



주요 기능(1)

정적분석: Header 분석, IP 관리, 접속 통계 분석

기존 차단 이력과 악성 봇 DB를 활용하거나 HTTP Header 요소를 분석해 악성 봇으로 의심되는 IP를 탐지하고 차단합니다.



STEP 1

HTTP Header 분석

필수 HTTP Header 요소 / 불필요 HTTP Header 요소 분석 진행
 사용자 Request Header 정보에 의한 이상 정보 탐지
 브라우저가 아닌 접근 탐지

STEP 2

IP 분석

악성 봇 의심 IP 분석 / 기존 차단 이력을 통한 분석 진행
 악성 행위 원천지 IP 리스트(DB)를 활용한 탐지
 사용자의 IP 및 개인식별아이드를 통한 탐지 및 차단, 관리 제공

STEP 3

접속 통계 분석

최근 5분간의 접속자별 평균 접속 통계 분석 진행
 최근 5분간의 접속자 평균 접속 횟수를 기준으로,
 과도하게 접속하는 사용자에게 대한 실시간 탐지 및 차단 제공

주요 기능(2)

정적분석: 매크로 개발 툴(셀레니움) 탐지

셀레니움이라는 파이썬 기반 도구를 사용함으로써 누구나 쉽게 매크로 프로그램을 제작할 수 있습니다.
이러한 매크로 프로그램은 온라인을 통해 쉽게 거래하고 사용할 수 있습니다.

MBUSTER는 **고급 탐지 기술을 활용해 이러한 매크로 시그니처를 선제적으로 탐지하고 차단**함으로써,
효과적인 방어가 가능합니다.

도메인별 정책을 세부적으로 설정할 수 있습니다.

정적분석 + 모두 열기

- Header 분석을 통한 차단 ② ☐ ▼
- 아이피 관리를 통한 차단 ② ☐ ▼
- 접속통계분석을 통한 차단 ② ☐ ▼
- 개발자 도구 탐지 ② ☐ ▼
- 셀레니움 탐지 ②** ☒ ▼

python

연중 22:32:27 04 20(목) 2023년

목동 테니스장 예약 정보 ver 1.2.0

ID

PW

실행 상태 

☒ 테스트 모드

예약 시작

캠핑장 URL

전화 코드

전화 회사

예약 날짜 선택

4월, 2023

	일	월	화	수	목	금	토
13	26	27	28	29	30	31	1
14	2	3	4	5	6	7	8
15	9	10	11	12	13	14	15
16	16	17	18	19	20	21	22
17	23	24	25	26	27	28	29
18	30	1	2	3	4	5	6

예약자 정보

대표자(단체명)

참가인원

이용 목적

주요 기능(3)

동적분석: 해외 접속자 분석, 행위분석, 2차 인증

개인별 접속 횟수 및 주기에 대한 변화량을 분석해 이용 정책을 설정하고, 악성 봇 의심자로 판단되면 2차 인증(Captcha, JS 챌린지)을 시행합니다.

★ 정책 범위

B

 : 브라우저 챌린지(Browser Challenge) ,

C

 : 캡차(Captcha) ,

R

 : 차단(Reject)

21 건

전체

Q 검색

No	추출구	정책	적용	설정	
1	페이지 과다조회 페이지 반복조회 페이지 비정상접속 조회 페이지 우회접속 조회	접속자로 ...	B	ON	⚙
2	페이지 과다조회	1초를 기준으로, 한 접속자로 ...	C	ON	⚙
3	페이지 비정상접속 조회	하나의 IP에서 여러개의 개인...	R	ON	⚙
4	페이지 우회접속 조회	test.html에 대하여 정해진 시...	R	ON	⚙
5	페이지 과다조회	특정 URL을 과다하게 요청하...	R	OFF	⚙
6	페이지 과다조회	하루를 기준으로, 한 접속자로...	R	OFF	⚙
7	페이지 과다조회	index.jsp을 과다하게 요청하...	R	OFF	⚙

STEP 1

해외 접속자 분석

국가별 IP 대역을 확인하는 알고리즘 적용, 접속자 국가 식별
불필요한 해외 접속자 탐지(한국인터넷진흥원 서비스 연계)

STEP 2

행위분석

매크로 행동 패턴을 정의하고, 접속자 로그를 동적으로 분석해 탐지
행위분석 룰셋 제공

- 하나의 IP에서 여러 개의 개인식별 아이디를 발급하는 경우
- 하나의 개인식별 아이디를 여러 개의 IP에서 접근하는 경우
- 1초 기준, 한 접속자로부터 과도하게 URL 요청이 발생하는 경우
- URL 호출 횟수가 분 단위로 동일한 패턴으로 반복되는 경우 등

STEP 3

2차 인증

정적분석 / 동적분석을 통한 매크로 의심자 발생 시
CAPTCHA 및 JS 챌린지 검증을 통한 매크로 여부 2차 검증

*행위분석 정책 및 활용

정책 그룹	정책	활용
페이지 과다조회	하루를 기준으로, 한 접속자로 부터 과도하게 URL 요청이 발생하는 경우(일 1000회 이상)	잔여석 확인을 위한 요청이 하루 종일 반복된 요청이 발생하는 서비스(수강신청, 예약 서비스)
	1초를 기준으로, 한 접속자로 부터 과도하게 URL 요청이 발생하는 경우(초당 3회 이상)	빠른 결과 확인을 위해 서비스 오픈 시점에 요청이 집중되는 서비스, 선착순 이벤트 (수강신청, 예약 서비스, 선착순 이벤트, 합격자 발표 서비스)
	1분을 기준으로, 한 접속자로 부터 과도하게 URL 요청이 발생하는 경우(분당 60회 이상)	빠른 결과 확인을 위해 서비스 오픈 시점에 요청이 집중되는 서비스, 선착순 이벤트 (수강신청, 예약 서비스, 선착순 이벤트, 합격자 발표 서비스)
	특정 URL을 과도하게 요청하는 경우(100회)	빠른 결과 확인을 위해 서비스 오픈 시점에 요청이 집중되는 서비스, 선착순 이벤트 (수강신청, 예약 서비스, 선착순 이벤트, 합격자 발표 서비스)
페이지 반복조회	URL 호출 횟수가 분 단위로 동일한 패턴으로 반복되는 경우(일 5회 이상 반복)	모든 서비스에서 활용 가능, 2차 인증을 통한 추가 확인 권장
페이지 비정상 접속 조회	하나의 IP에서 여러개의 개인식별 아이디를 발급받는 경우	NAT 환경에서의 사용자 고려, whitelist 등록 관리
	하나의 개인식별 아이디를 여러개의 IP에서 접근하는 경우	모든 서비스에서 활용 가능
	특정 URL을 반복적으로 직접 접속하는 경우(100회)	일반적인 접근이 아닌, 특정 URL로 직접 접속하는 경우 탐지 이벤트 페이지 오픈 시점을 확인하기 위한 접속
	특정 동작이 비정상적인 속도로 발생한 경우(시작 URL <---> 종료 URL 사이 소요 시간 제한)	여러 단계를 거쳐야하는 서비스가 있을 때, 시작 단계부터 끝 단계까지 사람이 처리하기 어려울 정도로 빠르게 처리하는 매크로 탐지 List > detail > setDate > Reservation (List부터 Reservation까지 소요 시간 비교)
페이지 우회접속 조회	특정 URL에 대하여 정해진 시간 이외에 접속이 발생한 경우(이벤트 시간: 13시 ~ 15시)	정해진 이벤트 시간 이외에 접속을 방지하고자 할 경우

주요 기능(4)

AI 매니저

챗봇 형태의 관리자 페이지를 통해 운영자 누구나 AI와 대화하며
접속 현황 및 정책 적용에 대한 가이드를 손쉽게 받고, 추천된 정책을 실시간으로 적용할 수 있습니다.

“단순 기능 설명 및 통계 현황 확인부터 **접속 트래픽 분석 데이터에 기반한 가장 효율적인 정책 추천**까지 제공하는 챗봇 기반의 AI 매니저를 통해 누구나 쉽게 솔루션 운영이 가능”

- 현재 접속 현황 / 정책 적용 현황 확인
- 정책 별 탐지율 확인
- 정책 추천 및 설정 / 행위분석 엔진 활성화 설정
- 주요 기능 안내 및 정책 가이드 제공
- 통계 정보 활용한 요약 정보 페이지 커스터마이징 구성

유형별 접속 통계

접속자 리스트

매크로 리스트

매크로 통계

국가별 통계

오늘 접속 현황을 알려줘



현재 운영중인 사이트의 접속 상태가 궁금하신가요?

금일 총 123,521건의 접속 요청이 있었고,
이 중 64,094건의 악성 봇을차단하였습니다.

이를 통해 하루 동안 51.8%의 불필요한 트래픽을 절감하였습니다.
아래에서 더 자세히 조회하실 수 있습니다.

접속자 리스트

악성 봇 리스트

어떤 정책을 적용해야 좋을까?



어떠한 정책을 설정하는 것이 좋을지 궁금하시군요.

행위 분석 룰셋 확인 결과

[/mbster/eventpage.do을 과다하게 요청하는 경우-3] 정책이 가장 높은
탐지율을 보이는 것으로 확인되었습니다.

위 정책을 적용하시겠습니까?

정책 적용하기

주요 기능 비교

구분		STCLab - MBUSTER	Akamai - Bot Manager	Micro Focus - Arcsight
차단방식		개인식별 ID / IP별 차단 제공	IP별 차단 제공	디바이스 정보 차단 제공(디바이스명, 주소, 포트 등)
정적 분석	셀레니움 탐지	매크로 개발툴(셀레니움) 탐지 제공	미제공	미제공
	IP 관리를 통한 차단	악성행위 원천지 IP 리스트(DB) 약 3만개 탐지 (지속적 업데이트), 관리자 IP 수동 차단 제공	봇 디렉토리 1,700여개 제공 봇 이름으로 차단 제공 (지속적 업데이트)	블랙리스트 제공
	접속 통계 분석을 통한 차단	최근 5분간 접속자별 평균 접속 통계 분석을 통한 차단 제공	미제공	미제공 : 탐지를 위한 사용자 정의 플레이북 작성 필요
동적 분석	해외접속자 차단	한국인터넷진흥원(KISA)의 후이즈 서비스와 연계하여 해외접속자 탐지 및 차단 제공	미제공	미제공 : 탐지를 위한 사용자 정의 플레이북 작성 필요
	행위분석 룰셋에 의한 차단	행위분석을 통한 매크로 탐지 및 차단 (행위분석 룰셋 약 10개 제공 / 지속적 업데이트)	탐지된 모든 봇에 점수를 부여해 봇의 점수 임계치 설정에 의해 탐지 및 차단 제공	수집 데이터의 실시간 상관관계 분석을 통한 이벤트 및 위협 탐지(상관관계 분석을 위한 40가지 룰셋 제공)
머신러닝 행위분석		학습데이터 기반으로 머신러닝 알고리즘을 활용한 행위분석 룰셋 추천 및 임계치 자동 설정 제공	머신러닝을 통한 매크로 탐지 임계치 자동 설정 제공	머신러닝을 통한 새로운 위협 탐지 (부가 옵션으로 비용 발생)
모니터링 / 보고서		실시간 대시보드 및 다양한 통계정보 템플릿 기반 보고서 및 매크로 차단 증거자료 제공	실시간 대시보드 / 보고서 제공	대시보드 / 보고서 제공
관리기능		기본 관리 UI 제공, AI 대화형 Chat Manager 제공	기본 관리UI 제공	기본 관리UI 제공

손쉬운 API 연동

손쉬운 API 연동을 통해 MBUSTER를 적용하고, 차단 페이지로 전환하거나 2차 인증을 진행할 수 있습니다.

2. API 호출

```
<script type="text/javascript" src="/js/jquery-3.5.1.js"></script>
<!-- << 엠버스터 적용 시작 >> -->
<script type="text/javascript" src="/js/mbuster_meta.js"></script>
<script type="text/javascript" src="/js/mbuster_api.js"></script>
<script type="text/javascript">
    var userIpAddress = '<%= request.getRemoteAddr() %>';

    $(document).ready(function(){
        MBUSTER_API({
            clientId: userIpAddress,
            user_login_id: "userID"
        });
    });
</script>
<!-- << 엠버스터 적용 끝 >> -->
```

1. 필수 라이브러리 추가

Utilization

- 가치
- 성공사례

가치

MBUSTER는 서비스 공급자와 이용자 모두에게 새로운 가치와 디지털 서비스 경험을 제공합니다.



#서비스_공정성_확보

특정 이용자가 상품을 독점하거나,
불법 취득한 상품을 재판매하는 등의
불공정 거래를 사전에 방지할 수 있습니다.



#불필요_트래픽_필터링

악성 봇 차단으로 불필요한 트래픽 급증 및
이로 유발되는 추가 시스템 부하를 방지하여
서버 장애에 효과적으로 대응하며,
리소스 운영 비용을 최적화할 수 있습니다.



#브랜드_신뢰도_향상

· 불법적인 이용자들을 차단함으로써 실사용자 권리 보호
→ 부정거래로 인한 민원을 감소시키고, 브랜드 신뢰도 확보

성공사례: 항공사 PoC

“기존 글로벌 CDN 서비스의 매크로 솔루션이 탐지하지 못했던 매크로를 MBUSTER를 통해 다양한 유형으로 추가 탐지, 분석할 수 있었습니다.”

글로벌 CDN 솔루션 대비 **+30% 추가 탐지 성능 확보**
[글로벌 경쟁사 대비 x4배 탐지 및 차단]

배경

- 기존 사용중인 글로벌 CDN 서비스의 매크로 솔루션은 단순 IP 차단만을 제공, 해당 IP 이외의 세부 탐지 및 정책 수립 제한적임
- 국내 사용자에게 특화된 매크로 탐지 및 차단 기능 필요

적용

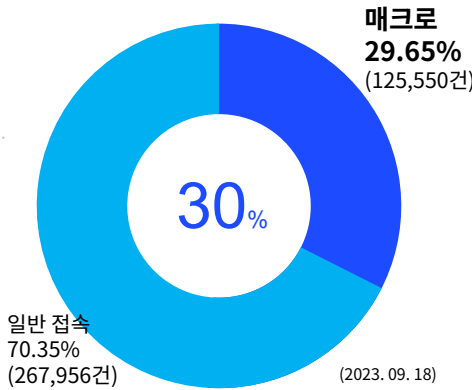
- 항공예약 서비스 도메인 내 매크로 탐지 진행

의의

- 다양한 정책 설정으로 기존 글로벌 CDN 서비스를 넘어선 매크로 탐지 성능 향상
- 실제 서비스 트래픽에 대한 모니터링 및 매크로 트래픽 현황 분석
- 매크로 이용자를 방지해 불필요 트래픽 및 리소스 비용 절감
- 서비스 안정성, 공정성, 신뢰성 보장

항공 티켓 예약
서비스 도메인 내 매크로 탐지

약 30%의
불필요한 트래픽 부하 절감 기회 제공
공정한 서비스 보장



- 기존 매크로 탐지 솔루션에서 정상으로 판별된 사용자 중, 매크로 사용자 30% 추가 탐지
- 다양한 매크로 접속 유형에 대한 분석 가능

구분	매크로 차단 유형		건수
정적분석	Header 분석을 통한 차단: Header 정보에 의한 이상정보, 매크로 개발 툴(셀레니움) 탐지		7,831건(6.24%)
	접속 통계 분석을 통한 차단: 최근 5분간 평균 접속 통계 기준으로 과도한 접속자 탐지		77,949건(62.09%)
동적분석	행위분석 탐지		39,016건(31.08%)
	행위분석 탐지정책	하나의 IP에서 여러개의 개인식별 아이디를 발급받는 경우	4,466건
		1초를 기준으로, 한 접속자로부터 과도하게 URL 요청이 발생하는 경우	500건
		URL 호출 횟수가 분 단위로 동일한 패턴으로 반복되는 경우	34,050건
	해외접속자 차단: 접속자 국가 식별		754건(0.06%)

- 페이지별 / 국가별 매크로 탐지 현황 제공

성공사례: 공기업 PoC

“단 5개의 동적분석 정책만을 테스트 했음에도
이렇게 많은 매크로 이용자가 존재할 줄 몰랐습니다.”

배경

- 자체 온라인 쇼핑몰 운영 중, 예약 이벤트 기간 내 비정상적 접속 분석 필요
- 매크로 방지 시스템 부재, 실시간 모니터링 운영 불가

적용

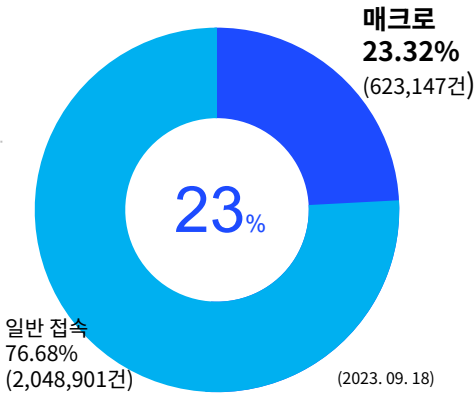
- 쇼핑몰 예약 서비스 도메인 내 동적 분석(22개 정책 중 5개 정책 적용) 매크로 탐지

의의

- 비정상적인 예약 이벤트 접속 트래픽을 탐지, 분석, 차단 기회 제공
- 매크로 사용 계정을 방지해 실 사용자에게 공정한 서비스 기획 제공
- 불필요한 시스템 운영 및 네트워크 비용 절감

자체 온라인 쇼핑몰 예약
서비스 도메인 내 매크로 탐지

약 23%의
불필요한 트래픽 부하 절감 기회 제공
공정한 서비스 보장



- 다양한 매크로 접속 유형에 대한 분석 가능

구분	매크로 차단 유형		건수
동적분석	행위분석 탐지		477,010건
	행위분석 탐지정책	URL 호출 횟수가 분 단위로 동일한 패턴으로 반복되는 경우	294,786건
		1분 기준, 한 접속자로부터 과도하게 URL 요청이 발생하는 경우(분당 60회)	5,265건
		1분 기준, 한 접속자로부터 과도하게 URL 요청이 발생하는 경우(초당 03회)	176,959건
	해외접속자 차단: 접속자 국가 식별		93,170건

- 페이지별 / 국가별 매크로 탐지 현황 제공
- 이벤트 기간 중 시간대 별 상세 분석 제공

성공사례: 대학 PoC

“절반에 가까운 매크로 이용자가 전체 트래픽의 98%를 차지하며
인프라 리소스를 낭비하고, 정상 이용자에게 피해를 끼치고 있다는 것을 알 수 있었습니다.”

약 50%의 매크로 IP가 전체 트래픽의 98%를 차지
불필요한 매크로 트래픽 절감을 통해 정상 이용자들의 원활한 서비스 보장이 가능

배경

- 대학 수강신청 기간 내 매크로 사용 행위에 대한 정황 파악
- 수강신청 서비스에 대한 비정상적 트래픽 모니터링 및 분석 툴 부재

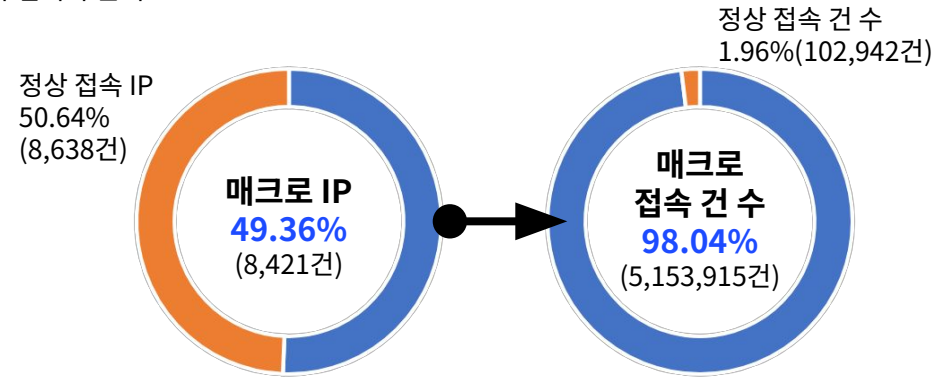
적용

- 수강신청 서비스 도메인 내 매크로 탐지 진행

의의

- 수강신청 일자별(학년별), 시간별 매크로 트래픽 모니터링 및 분석
- 비정상적인 접속을 제외시켜, 수강신청 서비스 공정성 확보 가능
- 불가능한 매크로 트래픽 접속을 차단시켜 서버 부하 및 리소스 절감 가능

A 대학 접속자 분석



- 정상 접속 대비 매크로 접속 비율을 IP와 접속 건 수 기준으로 파악
- 매크로 IP가 차지하는 다수의 인프라 리소스 확인

구분	전체 접속 건 수	정상 접속 건 수	매크로 접속 건 수
접속 건 수	5,256,857건	102,942건 (1.96%)	5,153,915건 (98.04%)
IP	17,059건	8,638건 (50.64%)	8,421건 (49.36%)

Thank you.

STCLab, Inc.

Korea Office

3F, CAMP G, 5, bongseunsa-ro 37-gil, Gangnam-gu, Seoul, Republic of Korea

solution@stclab.com

