MUBUSTER

매크로 탐지 및 차단 결과 보고서(샘플)

사 업	악성 매크로 탐지 결과 보고서
수요기관	ㅇㅇ 항공사 항공 예약 서비스
기 간	2024. 02. XX ~ 02. XX

STC LAB

1. 개요

• 배경

- 항공예약시스템은 클라우드로 운영 중이며, A사의 CDN 서비스를 통해 매크로 탐지를 진행중임. 하지만 해당 서비스는 Bot Net(IP, IP 대역)에 대한 차단만을 제공하기에 세부 정책 수립이 어려움
- 항공편 예약 관련해 지속적인 매크로 유입이 의심되어 추가 매크로 탐지 진행
- 특히, 국내 사용자에 특화된 매크로 탐지 기능을 확인해보고자 함

• 기간 및 서비스 대상

- 기간: 2024. 02. XX ~ 02. XX
- 장소: ㅇㅇ항공사 전산실(클라우드 LIVE망 - Web 구간)
- 대상 도메인

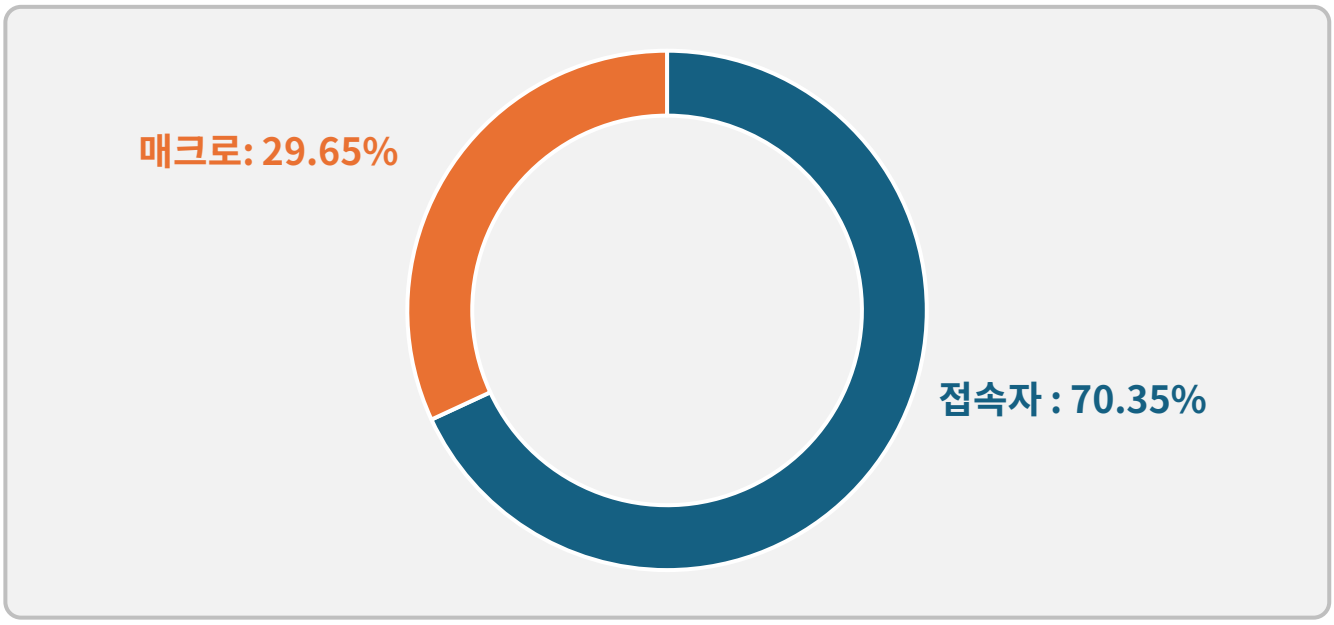
No.	대상 서비스	비고
1	항공예약시스템(ㅇㅇ.com)	항공편 예약 과정에서 발생하는 **매크로 탐지만 우선 진행**

• 매크로 탐지 정책

분석 기술	매크로 탐지 정책	적용 여부
정적 분석	Header 분석을 통한 탐지	적용
	IP 관리를 통한 탐지	적용
	접속통계분석을 통한 탐지	적용
동적 분석	행위분석 탐지	적용
	해외 접속자 차단	적용

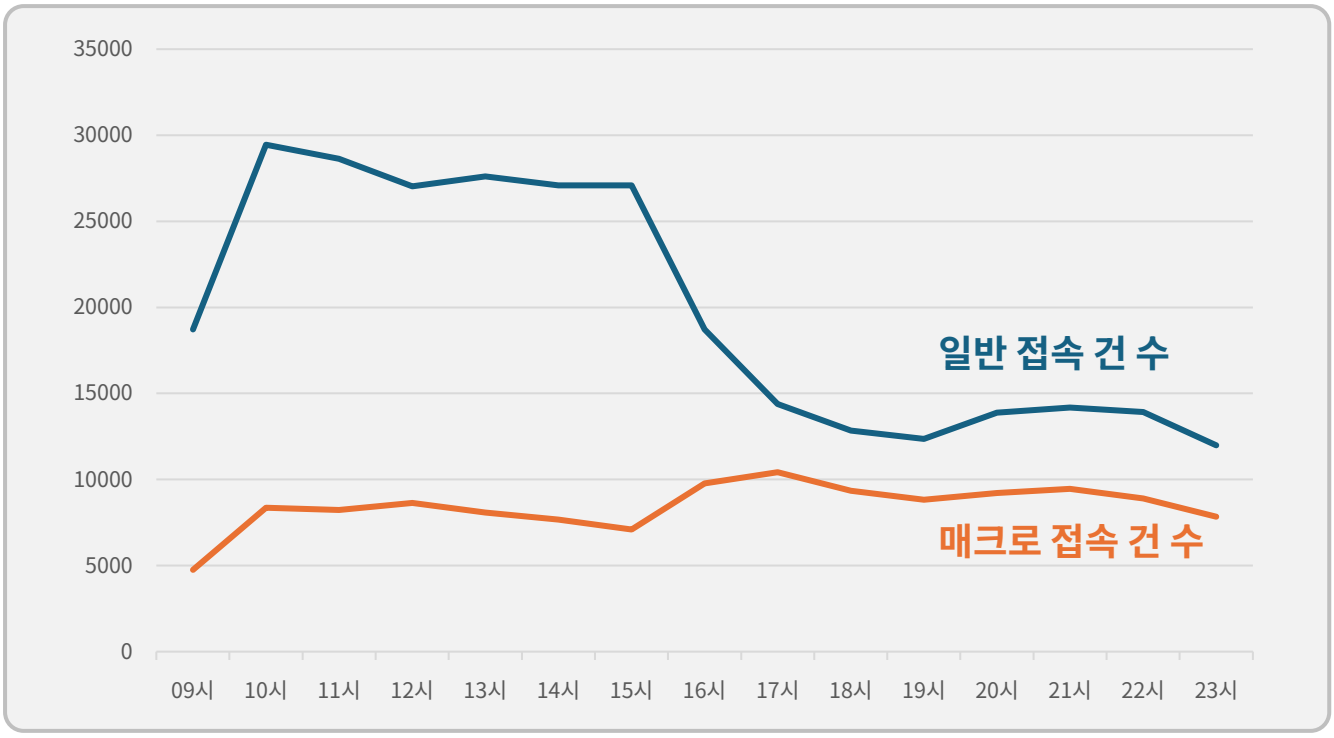
2. 매크로 탐지 결과

- **조회기간 내 접속자 및 매크로 전체 비율**

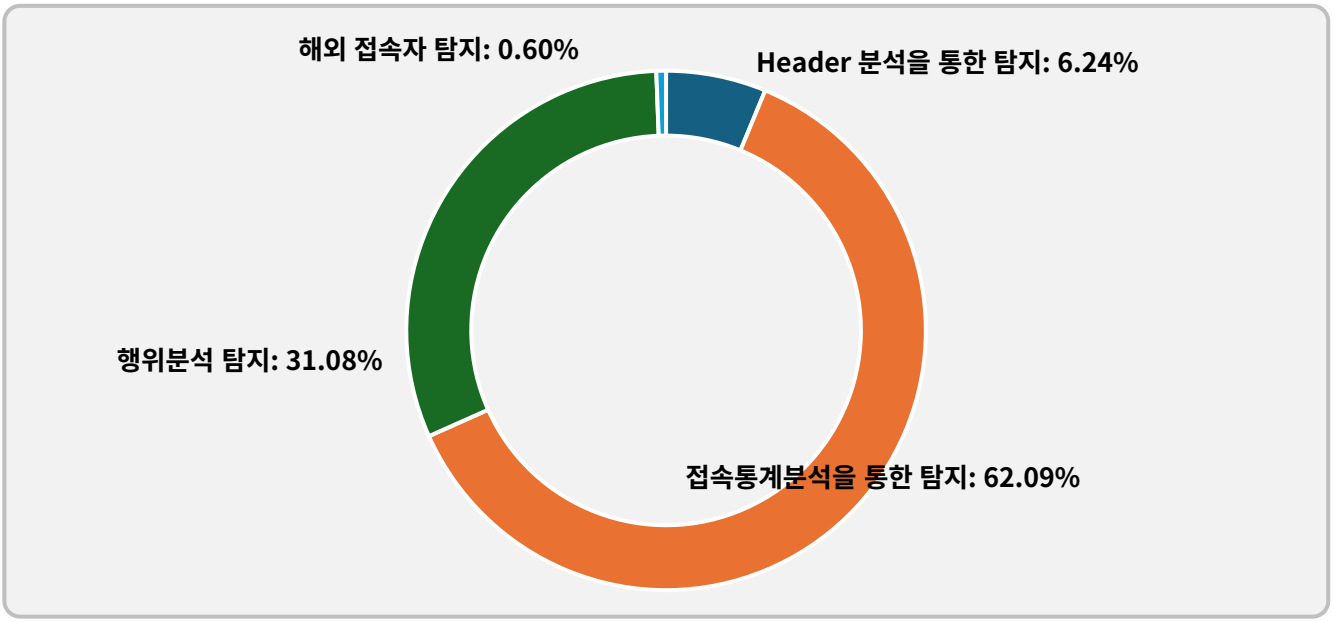


탐지 기간	정상 접속 건 수	매크로 접속 건 수
2024. 02. XX ~ 02. XX	297,956건(70.35%)	**125,550건(29.65%)**

- **시간별 매크로 탐지 분석**

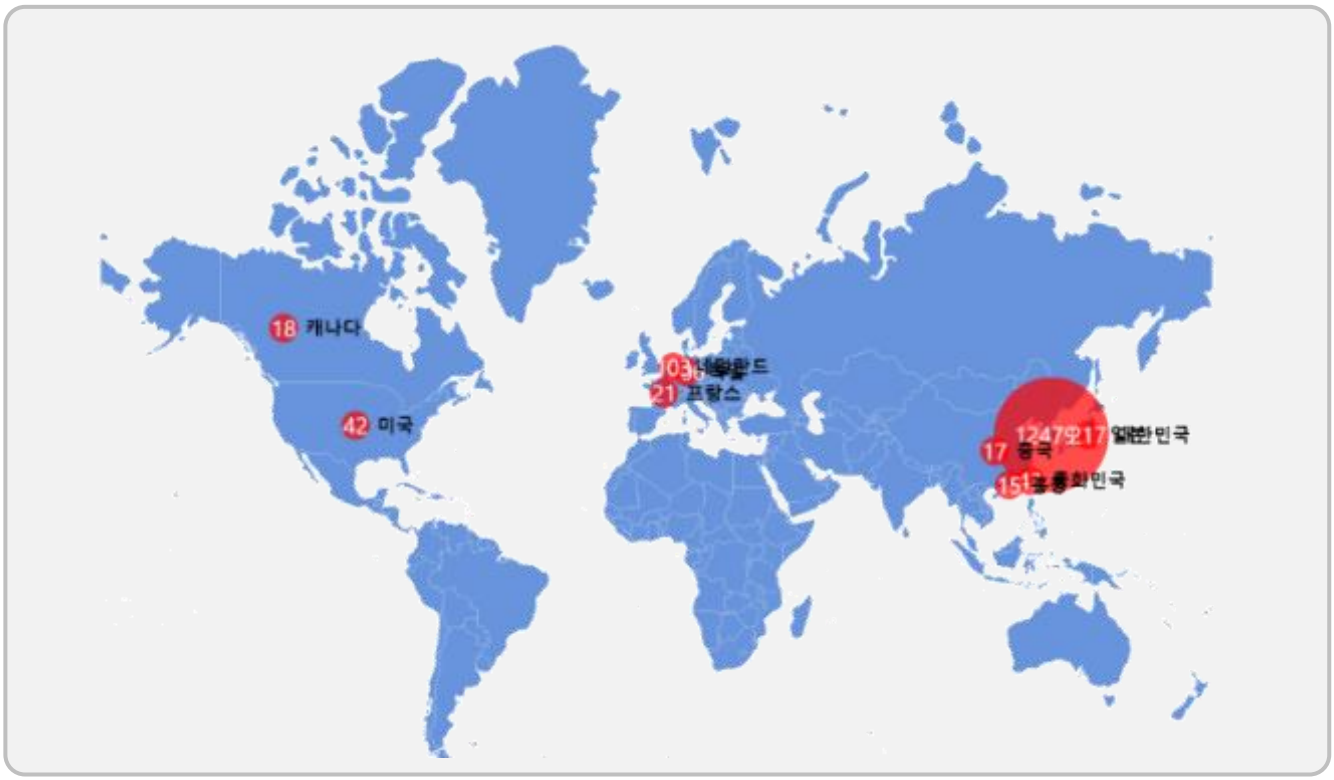


• 매크로 탐지 유형별 비율



분석 기술	매크로 탐지 정책			탐지 건 수
정적 분석	Header 분석을 통한 탐지			**7,831**
	IP 관리를 통한 탐지			**0**
	접속통계분석을 통한 탐지			**77,949**
	소계			**85,780**
동적 분석	행위 분석	페이지 비정상 접속	하나의 IP에서 여러 개의 개인 식별 ID를 발급받은 경우	**4,466**
			하나의 개인 식별 ID로 여러 개의 IP에서 접근하는 경우	**0**
		페이지 과다 조회	1일 1천회 이상, 한 접속자로부터 과도한 URL 요청 발생	**0**
			1분당 60회 이상, 한 접속자로부터 과도한 URL 요청 발생	**0**
			1초당 3회 이상, 한 접속자로부터 과도한 URL 요청 발생	**500**
		페이지 반복 조회	매 분마다 동일한 패턴으로 URL 반복 (1일 5회 이상)	**34,050**
	해외 접속자 탐지			**754**
	소계			**39,770**

• 국가별 IP 종합 분석



No.	접속 국가	평균 건 수
1	대한민국	**124,790**
2	일본	**217**
3	독일	**206**
4	네덜란드	**103**
5	중화민국	**43**
6	미국	**42**
7	프랑스	**21**
8	캐나다	**18**
9	중국	**17**
10	홍콩	**15**

※ 해외 IP 진입을 허용할 것인지는 고객사별 정책 수립 필요

3. 결론 및 가이드

- **현재 탐지된 결과는, 기존 클라우드 CDN 서비스에서 정상 사용자로 판별된 사용자 중 매크로 추가 탐지된 사용자를 나타냄**
  - 기존 매크로 탐지 솔루션 대비, 약 30%의 탐지 성능 향상을 기대할 수 있음

- **정적분석 중 'Header 분석을 통한 탐지'를 통해 매크로 개발 툴인 셀레니움을 통한 접속을 비정상적인 활동으로 감지하여 차단할 수 있음**
  - '접속통계 분석을 통한 탐지'의 경우, 최근 수 분 동안의 평균값을 기준으로 탐지하는 정책으로 특정 시간을 기준으로 상황에 따라 실시간으로 달라지는 유의미한 접속 데이터를 제공합니다.

- **행위분석 정책은 항공예약서비스만의 의미 있는 수치를 찾을 수 있음**
  - 이번 진단에서는 '매 분마다 동일한 패턴이 반복(1일 5회 이상)'되는 행위가 가장 많이 탐지됨
  - 항공권 예약 이후, 예매 취소 등을 통한 잔여석을 선점하기 위해 지속적으로 매크로를 이용하는 것으로 의심됨

- **이번 서비스는 매크로 사용자로 의심되는 경우를 '탐지'만 진행하였으며, 실제 '차단' 정책을 적용할 경우, 2차 인증(Captcha, 브라우저 챌린지)을 통해 더욱 신뢰도를 높일 수 있음**

[붙임] 매크로 탐지 수준에 따른 정책 적용 기준

<table>
<tr><th>분석 기술</th><th colspan="3">정책(총 7개)</th><th>중요도</th></tr>
<tr><td rowspan="3">정적 분석</td><td colspan="3">Header 분석을 통한 탐지</td><td>필수</td></tr>
<tr><td colspan="3">IP 관리를 통한 탐지</td><td>권장</td></tr>
<tr><td colspan="3">접속통계분석을 통한 탐지</td><td>권장</td></tr>
<tr><td rowspan="11">동적 분석</td><td rowspan="10">행위 분석</td><td>유형</td><td>룰셋</td><td></td></tr>
<tr><td rowspan="4">페이지
비정상
접속 조회</td><td>하나의 IP에서 여러 개의 개인 식별 ID를 발급받은 경우</td><td>권장</td></tr>
<tr><td>하나의 개인 식별 ID로 여러 개의 IP에서 접근하는 경우</td><td>제외</td></tr>
<tr><td>특정 동작이 비정상적인 속도로 발생한 경우</td><td>권장</td></tr>
<tr><td>특정 URL을 반복적으로 직접 접속하는 경우 1~5</td><td>권장</td></tr>
<tr><td rowspan="4">페이지
과다 조회</td><td>1초 기준, 한 접속자로부터 과도한 URL 요청 발생</td><td>필수</td></tr>
<tr><td>1분 기준, 한 접속자로부터 과도한 URL 요청 발생</td><td>필수</td></tr>
<tr><td>1일 기준, 한 접속자로부터 과도한 URL 요청 발생</td><td>필수</td></tr>
<tr><td>특정 페이지를 과다하게 요청하는 경우 1~5</td><td>필수</td></tr>
<tr><td>페이지
반복 조회</td><td>매 분마다 동일한 패턴으로 URL 반복 (1일 5회 이상)</td><td>필수</td></tr>
<tr><td>페이지
우회 접속
조회</td><td>특정 페이지에 대해 정해진 시간 이외에 접속 발생 1~5</td><td>권장</td></tr>
<tr><td colspan="3">해외 접속자 탐지</td><td>제외</td></tr>
</table>

※ 고객사별 정책 중요도를 고려해 적용

- 필수: 분명하게 매크로로 규정할 수 있는 정책으로 즉시 차단정책 운영 가능
- 권장: 일반적으로 매크로에 해당하지만, 임계치에 의해 정상 접속자도 검출될 가능성이 있는 정책으로 2차 검증과 조합하여 운영 권고