[인터넷 보안 현황 보고서]

커머스 업계의
위협 트렌드 분석

코로나19 팬데믹 이후 커머스 기업의 지속적인 디지털화는 비즈니스 성장을 이끌었지만, 기업 경계와 고객은 보안 리스크에 노출되고 말았습니다.

커머스 기업에 대한 공격

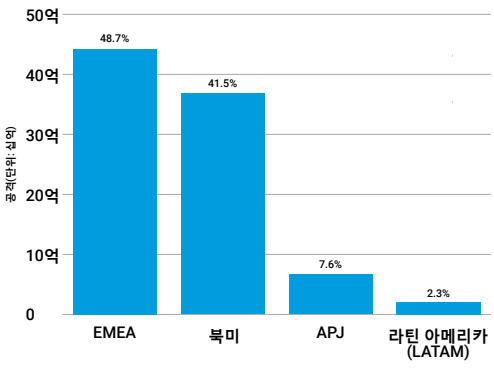
140억 건 이상

커머스 업계에서 발생한 웹 애플리케이션 및 API 공격

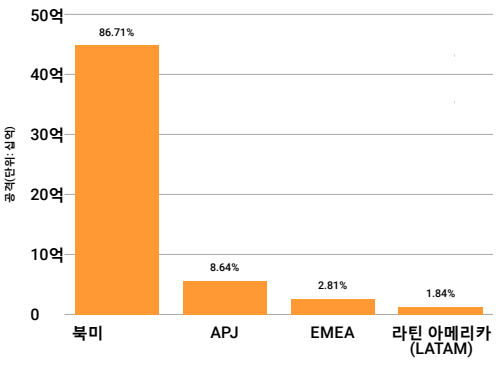
314%

2021년 3분기부터 2022년 3분기까지 LFI(Local File Inclusion) 공격 증가

SSRF(Server-Side Request Forgery)와 SSTI(Server-Side Template Injection) 같은 새로운 공격 기법은 데이터 탈취와 원격 코드 실행으로 이어지는 피해를 일으킬 수 있어 커머스 및 기타 업계에 심각한 위협이 되고 있습니다.



유럽, 중동, 아프리카(EMEA) 지역에서 리테일 기업을 대상으로 북미지역보다 더 많은 애플리케이션 및 API 공격이 발생했습니다.



호텔 및 여행 분야에서 웹 애플리케이션 및 API 공격이 가장 많이 발생한 지역은 북미 지역이며, 아시아 태평양 지역과 일본이 그 뒤를 잇고 있습니다.

커머스 고객에 대한 공격 지속

30.2%

2023년 1분기에 커머스 브랜드를 사칭한 피싱 캠페인

5조 건 이상

악성 봇 요청
(2022년 1월~2023년 3월)

악성 봇 사용 사례

- 피싱 사이트를 위한 웹 사이트 콘텐츠 스크레이핑
- 계정 탈취로 이어지는 크리덴셜 스터핑 공격에 사용
- 스캘퍼는 봇을 사용해 한정판 제품을 구매하고 일반 가정용품의 재고를 대량으로 비축합니다.

커머스 업계의 공격 트렌드에 대한 자세한 정보와 인사이트는 보고서 전문을 참조하세요.

보고서 전문 다운로드

지원

2023년 06월 발행