혁신의 중대성

금융 서비스 업계의 공격 트렌드

전례 없는 디지털 전환의 시대를 맞아 금융 서비스 업계는 혁신과 리스크의 교차로에 서 있습니다. 기술이 금융 거래의 판도를 재편하면서 동시에 경제적 안정성의 핵심을 공격하는 새로운 위협의 시대가 열렸습니다.

금융 서비스 및 고객에 대한 공격

90억 건
금융 서비스에 대한 웹 애플리케이션 및 API 공격 건수

1순위
게임 업계를 앞지르며 DDoS 공격이 가장 많이 발생한 금융 서비스 업계

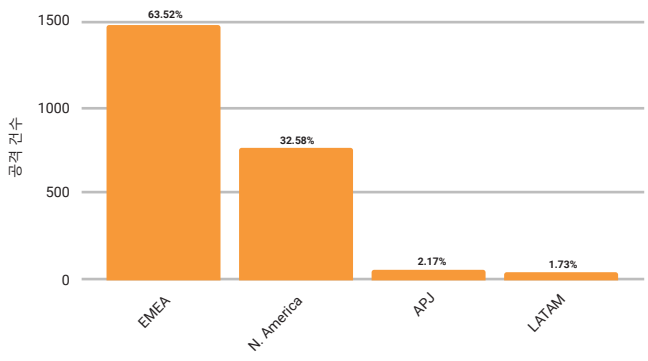
50.6%
2023년 2분기 가장 많은 피싱 공격을 받은 금융 서비스

1조 건 이상
악성 봇 요청 수

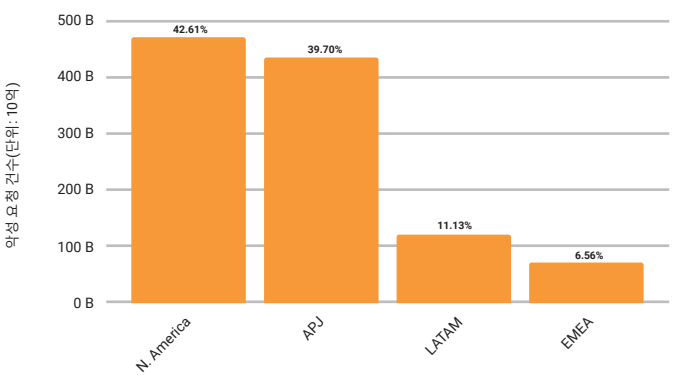
지역별 스냅샷

유럽, 중동 및 아프리카(EMEA)에서 발생한 레이어 3 및 레이어 4 DDoS 공격 건수는 북미 지역의 거의 두 배 수준

지역별 DDoS 공격 건수: 금융 서비스
2020년 1월 1일~2023년 6월 30일



지역별 악성 봇 요청 건수: 금융 서비스
2020년 1월 1일~2023년 6월 30일



아시아 태평양 및 일본(APJ)은 악성 봇 요청이 가장 많이 발생하는 지역

경계해야 할 잠재적 보안 리스크

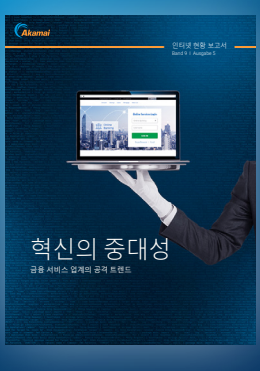
섀도우 API
문서화되지 않고 추적되지 않는 API를 누가 어떻게 사용하는지 파악하지 못하는 기업은 모니터링 문제가 발생할 수 있습니다.

써드파티 스크립트
공격자는 클라이언트 측 취약점을 악용하거나 웹 사이트의 일부로 로드된 써드파티 스크립트에 악성 코드를 주입할 수 있습니다. 이로 인해 금융 서비스가 웹 스키밍의 리스크에 노출되어 고객의 데이터가 도난당하거나 무단 트랜잭션에 이용될 수 있습니다.

금융 애그리게이터
공격자가 금융 애그리게이터와 데이터 수집 방법 사이에 존재하는 보안 격차를 새로운 악용 경로로 이용해 ID 도용 문제가 발생할 수 있습니다.

보안 권장 사항 및 모범 사례

- 공격표면을 파악해 방어 전략 수립 및 보안 제어 구축
- 악성 API 탐지 및 모니터링을 위한 API 보안 툴 배포
- OWASP API 보안 상위 10대 취약점 및 MITRE ATT&CK 프레임워크를 사용해 레드팀 및 침투 테스트 그룹을 위한 교육 및 테스트 계획 수립
- 정기적인 보안 감사 실행과 고급 탐지 및 방어 구축을 포함하는 멀티레이어 방어 전략 사용
- 클라이언트 측 공격으로 인한 리스크를 방어할 수 있는 Client-Side Protection & Compliance와 같은 솔루션 도입
- 엣지 기반 거버넌스 모델을 구축해 봇 및 API 트래픽에 대한 가시성 제공
- 지난 3분기 동안 DDoS 공격이 발생하지 않은 경우 실제 훈련 실시, 플레이북 검증, 규모와 속도에 대한 트렌드를 추적해 현재 기능을 기반으로 리스크 평가



금융 서비스 업계의 공격 트렌드에 대한 자세한 정보와 인사이트는 보고서 전문을 참조하세요.

보고서 다운로드하기

 | 지원 | 2023 년 10 월 발행