핵심 인사이트

34%

금융 서비스 기관이 경험한 레이어 3 및 4 DDoS 공격 이벤트의 비율

금융 서비스는 여전히 레이어 3 및 4의 분산 서비스 거부(DDoS) 공격 이벤트가 가장 빈번하게 발생하는 업계입니다. 다음으로 게임이 18%, 하이테크가 15%로 그 뒤를 잇고 있습니다. 이러한 만연한 위협은 전 세계적으로 핵티비스트 활동이 급증한 이스라엘-하마스, 러시아-우크라이나 전쟁 등 지정학적 긴장이 지속되고 있기 때문인 것으로 보입니다.

API 증가로 인한 레이어 7 DDoS 공격 증가

웹 애플리케이션은 전통적으로 사이버 공격의 주요 표적이었지만, 이 보고 기간 동안 API에 대한 레이어 7 DDoS 공격이 눈에 띄게 증가했습니다. 진화하는 컴플라이언스 및 규제 요구사항을 충족하기 위해 금융 서비스에서 API 도입이 증가한 것이 주요 원인입니다. 기업이 API에 더 많이 의존함에 따라 공격자들은 기법을 조정하고 있으며, 이에 따라 API 보안은 현대 비즈니스의 중요한 우선 순위가 되었습니다.

트래픽이 급증하면서 DDoS를 빈도 및 규모별로 평가해야 할 필요성 발생

금융 서비스에서의 DDoS 공격은 중요한 인사이트를 보여줍니다. 이벤트 빈도와 공격 강도가 항상 상관관계가 있는 것은 아닙니다. 공격이 거의 발생하지 않았던 달도 있지만, 해당 Gbps 데이터는 상당한 트래픽 급증을 나타내며 DDoS 공격의 영향을 평가할 때 공격 빈도와 규모 모두 고려해야 한다는 것을 보여줍니다.

36%

금융 기관을 표적으로 삼는 의심스러운 도메인의 비율

금융 서비스 고객을 노리는 피싱 공격이 증가하면서 신원 도용 및 계정 탈취의 리스크가 높아지고 있습니다. 이러한 공격 트렌드로 인해 규제 기관이 금융 기관을 더 면밀하게 조사하게 되고, 유출로 인해 고객의 신뢰 문제가 발생합니다.

30%

피싱 및 브랜드 사칭 사이트로 연결되는 페이지 방문 비율

공격자는 정상적인 금융 서비스 웹사이트와 앱을 모방해 사기성 사이트로 트래픽을 성공적으로 유도합니다. 공격자는 금융 기관이 보유한 민감한 정보를 얻기 위해 피싱을 통해 금융 기관을 지속적으로 표적으로 삼고 있습니다.