보고서의 핵심 인사이트

APJ 스냅샷은 대규모 보안 애플리케이션 SOTI 보고서인 위협받는 디지털 요새: 최신 애플리케이션 아키텍처를 향한 위협(영어로만 제공)의 보조 자료입니다. 공격자들이 확장되는 공격표면을 악용하는 방법, 기업을 보호하기 위한 권장사항, 리서치 방법론에 대한 자세한 설명은 해당 보고서를 참조하시기 바랍니다.

개요

지난 20년 동안 웹 애플리케이션은 그 수와 기능 면에서 기하급수적으로 성장해 비즈니스 운영을 간소화하고, 고객 경험을 개선하고, 실시간 통신, 데이터 애널리틱스, 프로세스 자동화와 같은 기능을 통해 성장을 주도해 왔습니다. 애플리케이션 간 통신의 기반이 되는 API도 확산되어 이제 기하급수적인 도약을 준비하고 있습니다.

애플리케이션은 비즈니스의 거의 모든 측면에서 실행되기 때문에 수조 건의 연결은 더 쉬워졌지만 공격에는 더 취약해졌습니다. 2023년 1월부터 2024년 6월까지를 대상으로 하는 이 APJ 스냅샷에서는 웹 공격, 분산 서비스 거부(DDoS) 공격, 중요 워크로드에 대한 위협 등 애플리케이션에 영향을 미치는 위협에 대해 살펴보고, 특히 이런 위협이 기업에게 무엇을 의미하는지 집중적으로 설명합니다.

애플리케이션 및 API에 대한 웹 공격은 아시아 태평양 및 일본(APJ) 지역에서 2023년 1분기부터 2024년 1분기까지 65% 증가했으며, 지속적으로 증가해 2024년 6월에 48억 건으로 정점을 찍었습니다. 이전 보고와 마찬가지로, 금융 서비스 및 커머스 부문이 이 지역에서 가장 많은 웹 공격을 경험했습니다.

APJ 지역에서 레이어 7 DDoS 공격이 5배 증가해 이 기간에 총 5조 1000억 건의 공격이 발생했고, 북미에 이어 두 번째로 큰 규모를 기록했습니다. 가장 큰 영향을 받은 업계는 소셜 미디어로, 지정학적 사건과 긴장으로 인해 핵티비즘 및 국가와 연계된 공격자들이 소셜 미디어 업계에 대한 레이어 7 DDoS 공격을 늘렸기 때문입니다.

랜섬웨어와 애플리케이션 및 이들 사이의 내부 워크로드에 대한 다른 공격에 대한 우려가 커지고 있습니다. 기업들은 이렇게 확장되는 공격표면을 보호하는 데 필요한 가시성과 정밀한 제어를 위해 소프트웨어 기반 마이크로세그멘테이션으로 전환하고 있습니다.