SOTI

10 YEARS
OF SECURITY INSIGHT

10권, 04호

최신 애플리케이션 아키텍처를 향한 위협

APJ 스냅샷

Akamai

인터넷 보안 **현황 보고서**

목차

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.

웹 애플리케이션 및 API: 보안 리스크가 많이 발생하는 곳

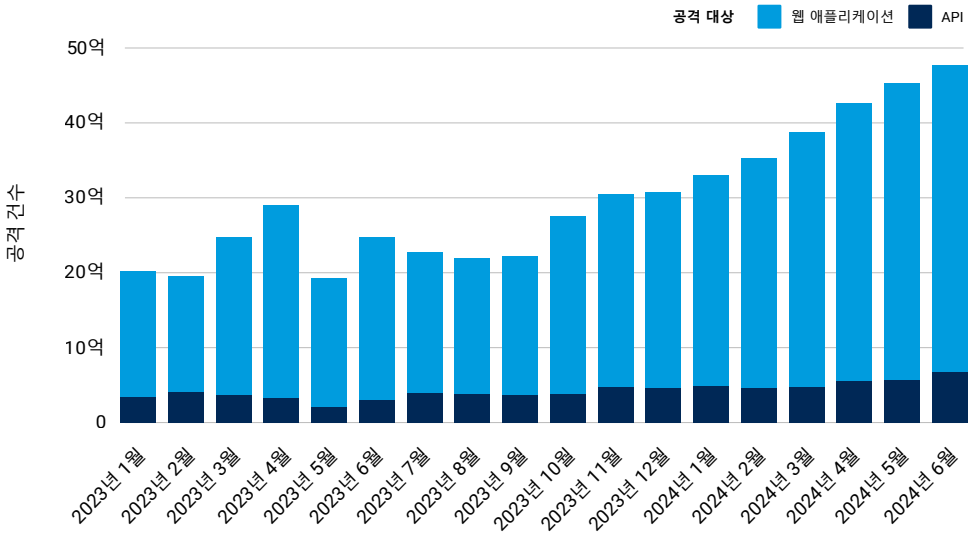
기업들이 고객 경험을 개선하고 비즈니스를 확대하기 위해 애플리케이션을 서둘러 배포하면서 웹 애플리케이션 및 API 공격이 급증하고 있습니다. 공격자들은 이렇게 확장하는 공격표면(코딩 및 디자인 결함이 있는 웹 애플리케이션, 수년 된 취약점 등)을 이용하고 있습니다. 게다가, API 경제의 급속한 확장은 사이버 범죄자들에게 취약점 악용 및 비즈니스 로직 남용의 기회를 더 많이 제공했습니다.

숫자로 보는 공격 트렌드

2024년 첫 번째 SOTI 보고서에서는 전체 웹 애플리케이션 공격의 맥락에서 2023년 API 공격 트렌드를 살펴봤습니다. Akamai 연구원들은 2023년 1월부터 2024년 6월까지 지난 18개월을 되돌아본 결과 APJ에서 발생한 월별 웹 애플리케이션 및 API 공격이 18개월 만에 최고치를 기록했으며, 2024년 6월에는 48억 건으로 정점을 찍었음을 발견했습니다. 이는 2023년 1분기부터 2024년 1분기까지 웹 공격이 65% 증가했고 이후 분기에도 계속 증가할 것임을 시사합니다. API에 대한 공격은 소폭 증가해 이 기간 말에는 6억 7000만 건에 달했습니다(APJ 그림 1).

APJ: 월별 웹 애플리케이션 및 API 공격

2023년 1월 1일~2024년 6월 30일



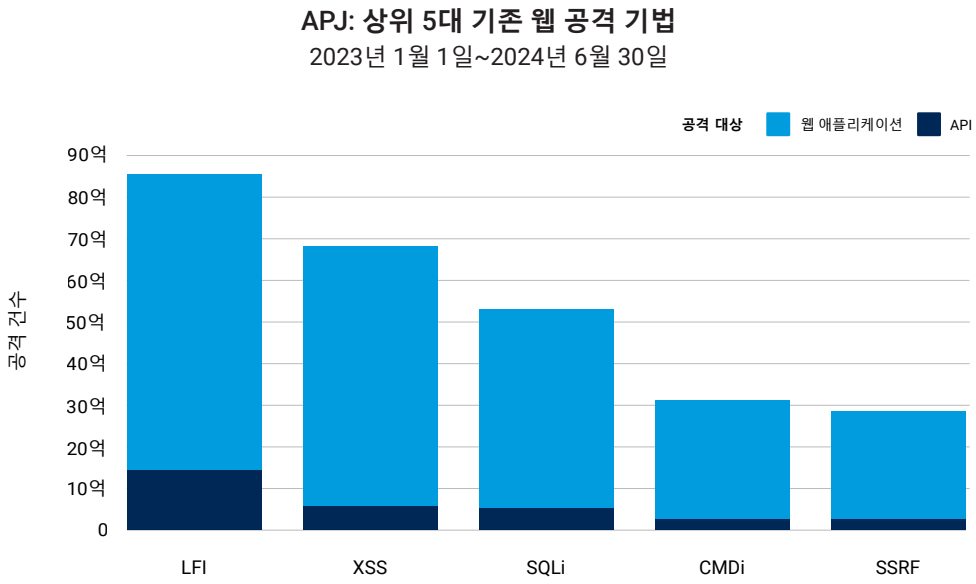
APJ 그림 1: 전년 대비 65% 증가한 웹 애플리케이션 및 API 공격

APJ 지역에서는 호주(146억 건), 인도(120억 건), 싱가포르(107억 건)가 해당 기간에 웹 애플리케이션 및 API 공격을 가장 많이 받았으며, 중국(43억 건), 일본(40억 건), 뉴질랜드(21억 건), 대한민국(16억 건), 홍콩특별행정구(15억 건)가 그 뒤를 이었습니다.

Akamai는 또한 여러 웹 공격 기법을 추적했습니다. 이 보고서에서는 기존의 기법 기반 공격 방법 중 상위 다섯 가지에 집중합니다.

Akamai 연구원들은 APJ에서 발생한 월별 웹 애플리케이션 및 API 공격이 2024년 6월에 48억 건으로 정점을 찍으며 18개월 만에 최고치를 기록했습니다.

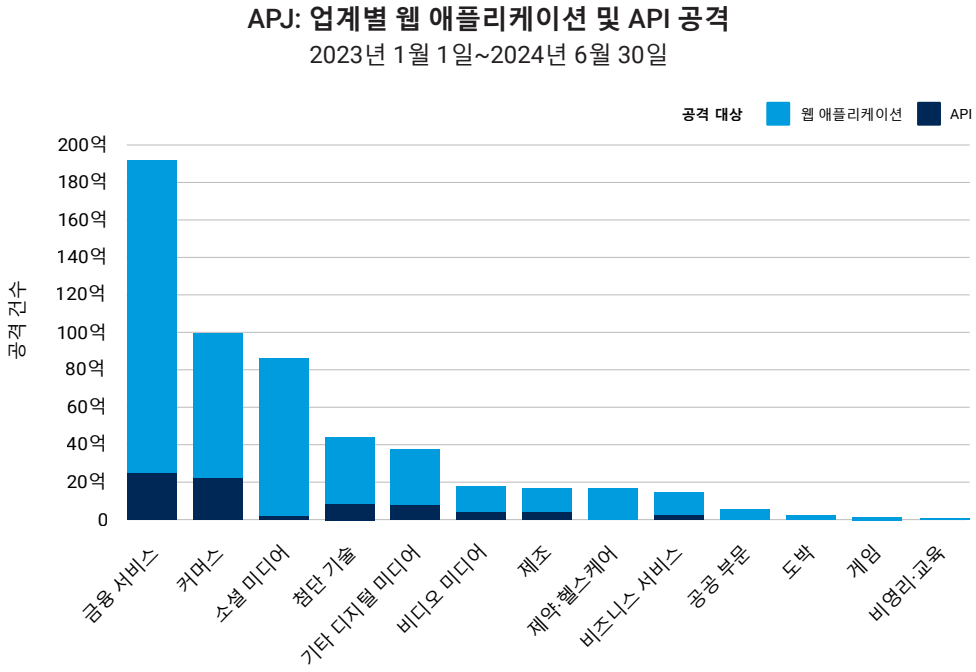
이전 보고서와 마찬가지로 로컬 파일 인클루전(LFI)이 여전히 선호되는 공격 기법이지만 크로스 사이트 스크립팅(XSS), 구조화된 쿼리 언어 인젝션(SQLi)과 같은 다른 기법도 계속해서 리스크를 야기하고 있습니다(APJ 그림 2).



APJ 그림 2: 웹 애플리케이션 및 API 공격의 증가를 주도하는 LFI, XSS, SQLi

공격자들이 LFI와 XSS와 같은 기존의 기법을 사용해 목표로 하는 데이터에 접근하는 것은 드문 일이 아닙니다. 또한, LFI는 공격자들이 의도한 표적으로의 진입점을 확보하고 원격 코드를 실행해 보안을 위협합니다.

업계 기준으로 살펴보면 웹 애플리케이션 및 API 공격의 영향을 가장 많이 받는 상위 다섯 개 업계는 이전 보고서와 일치하며, 금융 서비스와 커머스가 선두를 차지했습니다. API 공격을 구체적으로 살펴보면, 게임 부문에 대한 공격 건수가 많이 감소하면서 API 보안 SOTI 보고서와 차이가 있었습니다(APJ 그림 3). 이러한 변화가 공격자들이 게임을 공격 대상으로 삼지 않는다는 것을 의미하지는 않습니다. 이 보고서의 뒷부분에서 살펴보겠지만, 게임은 레이어 3, 4 DDoS 공격의 가장 많이 받은 업계 중 한 곳이었습니다.



APJ 그림 3: 계속해서 금융 서비스를 노리는 사이버 범죄자들

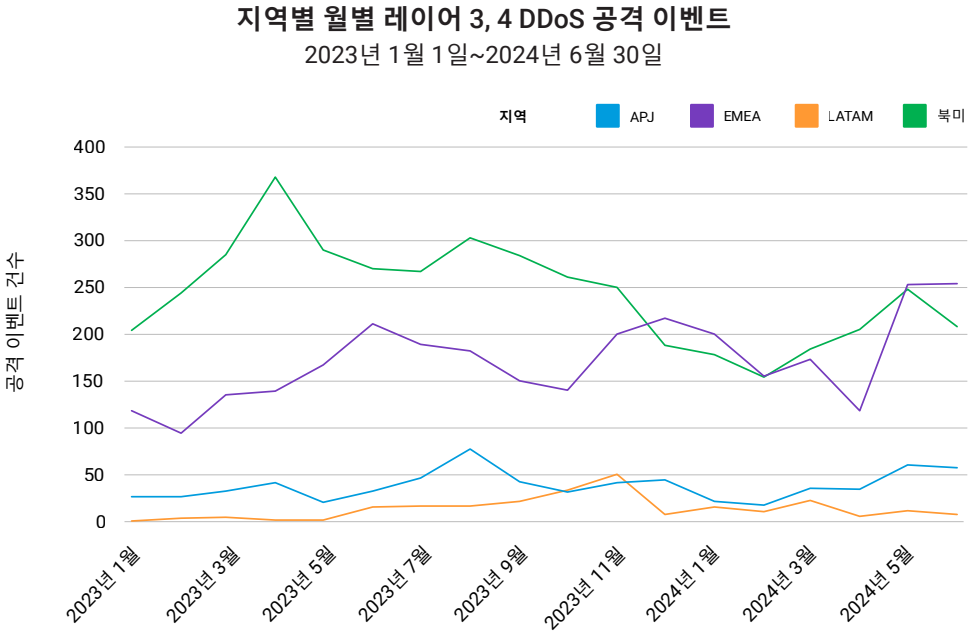
애플리케이션 가동 시간을 위협하는 DDoS 공격

공격표면이 계속 확장됨에 따라 애플리케이션에 영향을 미치는 DDoS 공격 종류도 증가하고 있습니다. 글로벌 SOTI 보고서에서 자세히 설명한 것처럼 기존의 레이어 3 및 레이어 4 DDoS 공격이 가장 오래 지속돼왔고, 네트워크 또는 애플리케이션 서버 용량을 장악하는 것을 목표로 합니다. 애플리케이션 레이어(레이어 7) DDoS 공격은 취약점을 악용하고 애플리케이션 레이어의 비즈니스 로직의 허점 또는 결함을 악용합니다. 비교적 적은 양의 악성 트래픽으로도 상당한 피해를 줄 수 있습니다. 공격 기법에 관계없이 DDoS 공격이 성공하면 애플리케이션이 중단됩니다.

최근 리서치에 따르면, 애플리케이션을 구동하는 인프라뿐 아니라 애플리케이션 자체에 대한 레이어 3, 4 및 레이어 7 DDoS 공격이 지속적으로 위협을 가하는 것으로 나타났습니다.

인프라 DDoS 공격

2023년 1월부터 2024년 6월까지 18개월의 보고 기간 동안 Akamai 연구원들은 APJ 지역이 다른 지역보다 낮은 수준의 레이어 3, 4 DDoS 공격 이벤트를 경험한 것을 발견했습니다. 하지만 2024년 2월부터 공격 이벤트가 증가한 것을 확인할 수 있습니다(APJ 그림 4).



APJ 그림 4: APJ에서 레이어 3, 4 DDoS 공격 이벤트 건수는 다른 지역보다 낮지만 2024년에는 증가하는 추세

가장 많은 영향을 받은 지역은 대만(409건)이며 호주(105건), 파키스탄(51건), 홍콩특별행정구(49건), 일본(38건), 싱가포르(29건)가 그 뒤를 이었습니다. 여기와 애플리케이션 레이어 공격에 대한 다음 섹션에서 살펴보겠지만, 지정학적 불안과 긴장으로 인해 국가와 연계된 공격자와 핵티비스트 모두 더 많이 관여하고 있는 상황에서 DDoS 공격은 APJ에서 대표적인 사이버 무기가 되고 있습니다.

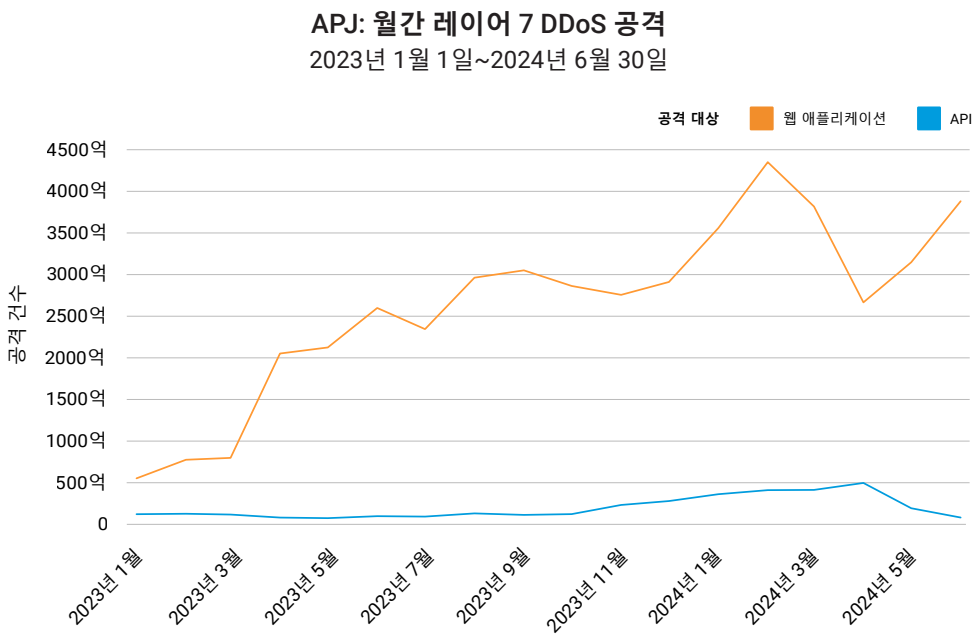
업계 기준으로 살펴보면 커머스(207건)와 게임(158건) 업계에서 가장 많은 레이어 3, 4 DDoS 공격이 발생했으며, 금융 서비스(120건), 비디오 미디어(91건), 하이테크(63건) 업계가 그 뒤를 이었습니다.

애플리케이션 레이어 DDoS 공격

APJ는 레이어 3, 4 DDoS 공격 외에도 표적 애플리케이션 레이어(레이어 7) DDoS 공격도 받았습니다. 2023년 1월부터 2024년 6월까지 18개월의 보고 기간 동안 Akamai 연구원들은 APJ가 5조 1000억 건의 레이어 7 DDoS 공격을 경험하며 8조 7000억 건의 북미에 이어 두 번째로 많은 공격을 받았다는 사실을 발견했습니다.

2023년 1월부터 2024년 6월까지 18개월의 보고 기간 동안 Akamai 연구원들은 APJ가 5조 1000억 건의 레이어 7 DDoS 공격을 경험하며 8조 7000억 건의 북미에 이어 두 번째로 많은 공격을 받았다는 사실을 발견했습니다.

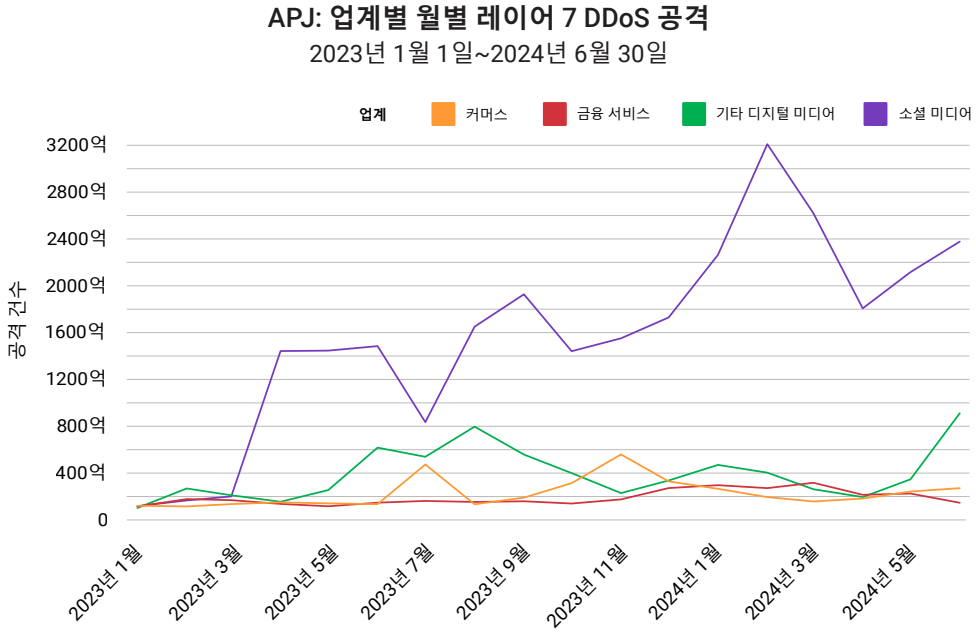
데이터를 자세히 살펴보면 이 보고 기간 동안 2023년 1월에는 700억 건, 2024년 6월에는 5배 이상 증가해 3990억 건을 기록하며 레이어 7 DDoS 공격의 월별 규모가 많이 증가했습니다. 게다가 APJ에서 발생한 레이어 7 DDoS 공격 중 API를 표적으로 삼은 공격은 10% 미만이었지만(APJ 그림 5) 리스크는 증가 추세에 있었습니다. 끊임없이 변화하는 환경이며, APJ 지역의 API 도입이 계속 증가함에 따라 리스크에 대한 노출도 증가할 것입니다.



APJ 그림 5: 2023년 1월부터 2024년 6월까지 5배 증가한 레이어 7 DDoS 공격

싱가포르가 2조 9000억 건으로 가장 많은 공격을 받았으며 인도(9590억 건), 대한민국(5440억 건), 인도네시아(2600억 건), 중국(1880억 건), 일본(830억 건), 호주(740억 건), 대만(500억 건)이 그 뒤를 이었습니다.

업계별 트렌드를 살펴보면 레이어 7 DDoS 공격 활동의 증가는 주로 소셜 미디어 부문에 대한 공격 시도에 기인한 것으로 나타났습니다(APJ 그림 6).



APJ 그림 6: 소셜 미디어 공격의 증가는 더 큰 글로벌 트렌드와 맞물려 있으며, 전 세계적으로 광범위한 군사적 갈등 및 고도로 중재된 선거 이벤트와 관련이 있음

소셜 미디어 플랫폼은 지정학적 격변에 따라 많은 공격 트래픽을 받는 것으로 알려져 있으며, APJ도 이러한 급증에서 벗어나지 못했습니다. 글로벌 SOTI에서 자세히 설명한 바와 같이, 이러한 활동에는 분열적인 정치 주제를 증폭시키기 위해 설계된 사기성 친러시아 소셜 미디어 계정과 가짜 뉴스 사이트의 급증이 포함되었습니다. 이러한 공격은 전 세계적으로 진행 중인 지정학적 격변과도 관련이 있습니다. 고도로 중재된 대규모 선거 이벤트와 대통령 및 국가 지도자 문제는 종종 여러 지역에서 DDoS 공격을 비롯한 정치적 동기에 기반한 사이버 공격으로 이어지는데, 이는 공격자들이 고조된 정치적 분위기를 악용해 자신들의 의제를 달성하려고 하기 때문입니다. 현재 진행 중인 러시아-우크라이나 전쟁과 이스라엘-하마스 전쟁과 관련된 핵티비즘도 공격 증가에 영향을 미쳤을 수 있습니다.

인공지능(AI) 툴의 발달로 설득력 있는 허위 콘텐츠가 더 쉽게 퍼지고 있으며, 소셜 미디어 플랫폼은 모든 종류의 콘텐츠를 위한 거대한 통신 채널이 되었습니다. 2024년에 APJ와 미국에서 선거가 있다는 점과 맞물려 모든 지역에서 소셜 미디어 플랫폼을 노리는 공격자는 계속 증가할 것으로 보입니다.

이 보고서의 공격 트렌드 데이터는 공격자들이 끊임없이 혼란과 금전적 이득을 추구하며 업계, 지역, 기법을 신속하게 전환할 수 있다는 것을 보여줍니다. 따라서 모든 기업은 경계를 늦추지 말고 모든 종류의 공격에 대해 적절한 방어 체계를 구축해 애플리케이션이 중단되지 않도록 보호해야 합니다.

애플리케이션 워크로드에 집중하는 공격자들

제로 트러스트는 일반적으로 네트워크 보안 측면에서 언급됩니다. 그러나 웹 애플리케이션 및 이들 사이의 내부 워크로드도 의도한 목표에 도달하기 위해 모든 엔트리 포인트와 경로를 찾는 랜섬웨어와 같은 위협에 노출될 수 있습니다.

글로벌 보고서에서 자세히 설명했듯이 클라우드, 온프레미스, 하이브리드 환경 등 애플리케이션이 제대로 작동하려면 모든 개별 워크로드가 원활하게 작동해야 합니다. 워크로드는 네트워크를 통해 이동할 때 여러 보안 관할 구역을 통과하며, 새로운 관할 구역마다 침입자의 잠재적 진입 지점이 추가됩니다. 이렇게 확장된 공격표면을 보호하는 것은 전반적인 보안 체계를 강화하는 데 매우 중요하지만, 보안팀의 업무를 훨씬 더 복잡하게 만듭니다.

기존의 하드웨어 기반 접근 방식으로 제로 트러스트 프레임워크를 구축하는 것은 많은 리소스와 시간이 필요하며 다운타임이 불가피합니다. 또한, 진정한 제로 트러스트를 구축하려면 랜섬웨어나 워크로드 자체에 대한 공격을 방어할 수 있는 마이크로세그멘테이션이 필요합니다.

소프트웨어 기반 마이크로세그멘테이션은 빠르고 쉽게 구축하고 운영할 수 있기 때문에 실행 가능한 인시던트 대응 조치로 활용할 수 있으며, 컴플라이언스를 지원하기 위해 중요 시스템을 격리하는 제어 수단으로도 활용할 수 있습니다. 이러한 장점 때문에 동적 데이터 센터, 클라우드, 하이브리드 클라우드 환경 전반에서 리스크에 노출된 워크로드 또는 컨테이너를 탐지하고 방어하기 위해 이 접근 방식을 사용하는 기업이 점점 많아지고 있습니다.

애플리케이션 워크로드 보안에 대한 실제 교훈

이 섹션에서는 기업들이 중요 워크로드를 보호하고 제로 트러스트를 발전시키는 방법을 보여주는 APJ 지역의 사례 연구 두 가지를 소개합니다.

APJ 사례 연구 #1: 메시징, 게임, 소셜 미디어 등의 서비스와 금융 서비스 구매 기능을 갖춘 한 소셜 네트워크는 고객 통신의 보안을 보장할 수 있는 방법이 필요했습니다. 최고 정보 보안 책임자의 최우선 과제는 해커들이 고객 대화에 접속한 후 다른 네트워크와 데이터베이스로 측면 이동하는 것을 방지하는 것이었습니다. 고객이 사용하는 운영 체제와 애플리케이션이 다양하기 때문에 어떤 디바이스가 취약한지 파악하는 것은 불가능합니다. 이 기업이 통신에 필요한 신뢰를 유지하는 근본적인 방법은 정밀한 세그멘테이션 정책으로 디바이스와 네트워크를 분리하는 것입니다.

APJ 사례 연구 #2: 전 세계에 진출해 금융 서비스 부문의 수많은 고객에게 서비스를 제공하는 한 대표적인 IT 유통업체가 있습니다. 무엇보다 중요한 것은 은행의 비즈니스 운영에 핵심적인 결제 서버를 보호하는 것입니다. 이 기업은 가장 복잡한 환경에서 대규모로 네트워크 시각화 및 매우 세분화된 거버넌스 제어를 배포하고 지원하는 마이크로세그멘테이션에 대한 심층적인 전문 지식을 바탕으로 고객 신뢰와 제로 트러스트 기능의 강점에 기반해 성장을 가속할 수 있었습니다.

워크로드는 네트워크를 통해 이동할 때 여러 보안 관할 구역을 통과하며, 새로운 관할 구역마다 침입자의 잠재적 진입 지점이 추가됩니다.

결론

이번 APJ 스냅샷에서는 공격자들이 애플리케이션과 API를 표적으로 삼는 다양한 방법에 대한 종합적인 관점을 제공하려고 노력했습니다. 기업들은 보안 및 리스크 관리 측면에서 애플리케이션과 API, 인프라, 중요 워크로드에 대한 위협을 이해하고 방어해야 합니다. 또한, 기존 법률과 새로운 개혁으로 인해 애플리케이션 보안이 필수가 되었습니다.

최근 싱가포르의 사이버 보안 법안 개정, 일본의 국가 인시던트 대비 및 사이버 보안 전략 센터 법안 업데이트, 결제 카드 업계 데이터 보안 표준 v4.0 등 새로운 입법 조치(예: 디지털 개인 데이터 보호 법안 통과를 시작으로 한 인도 IT법 개편, 2023~2030 호주 사이버 보안 전략 등)가 APJ의 변화하는 환경을 반영합니다. 게다가 APJ 지역은 유럽, 중동, 아프리카에서의 API 사용을 촉진하며 다른 지역으로 확산할 가능성이 높은 오픈 뱅킹 지침에 앞서 나갈 기회가 있습니다.

애플리케이션은 기업에게 그 어느 때보다 중요하지만 공격에는 더 취약합니다. 기업들은 계속 확장되는 공격표면으로 인한 도전 과제를 해결할 수 있는 역량과 모범 사례를 통해 성능이나 고객 경험을 손상시키지 않고도 언제 어디서나 구축하는 애플리케이션을 보호할 수 있습니다.

자세한 내용은 다음 글로벌 보안 애플리케이션 SOTI 보고서를 확인하세요. '위협받는 디지털 요새: 최신 애플리케이션 아키텍처를 향한 위협'

방법론

웹 애플리케이션 및 레이어 7 DDoS 공격

이 데이터는 웹 애플리케이션 방화벽(WAF)을 통해 관측된 트래픽에 대한 애플리케이션 레이어 알림을 설명합니다. 애플리케이션 공격 알림은 보호하고 있는 웹사이트, 애플리케이션, API에 대한 요청에서 악성 페이로드를 탐지하면 트리거됩니다. 레이어 7 DDoS 알림은 보호하고 있는 웹사이트, 애플리케이션, API에 대한 요청 건수에서 대규모 비정상을 탐지하면 트리거됩니다. 이러한 알림은 악성 요청과 정상 요청 모두에 의해 트리거될 수 있습니다. 일반적으로 요청 자체는 정상이지만 요청의 양이 많다는 것은 악의적인 의도가 있음을 시사합니다. 알림이 트리거됐다고 해서 공격이 성공한 것은 아닙니다. 이러한 제품은 높은 수준의 사용자 맞춤화가 가능하지만 Akamai가 여기에 제공한 데이터는 프로퍼티의 맞춤형 설정을 고려하지 않는 방식으로 수집했습니다.

이 데이터는 130여 개국 약 1300개 네트워크, 4000개 이상의 위치, 약 34만 대의 서버로 구성된 Akamai Connected Cloud에서 탐지된 보안 이벤트를 분석하는 내부 툴에서 추출한 것입니다. Akamai 보안 팀은 매달 페타바이트 규모의 데이터를 활용하여 공격을 연구하고, 악성 행동을 식별하며, Akamai 솔루션에 인텔리전스를 추가합니다.

이 데이터는 2023년 1월 1일부터 2024년 6월 30일까지 18개월 동안 수집되었습니다.

2024년 데이터 업데이트

Akamai는 10주년을 기념해 데이터 세트에 대한 몇 가지 업데이트를 발표하게 된 것을 기쁘게 생각합니다. Akamai의 웹 애플리케이션 공격 데이터 세트에 몇 가지 업데이트가 있었습니다. 수집 방법이 변경되고 간소화되고 최적화되었으며, 인사이트가 더 깊어지고 범위가 넓어졌습니다. SSRF와 같은 추가 공격 기법에 대한 항목이 추가되었으며, API 엔드포인트를 표적으로 하는 공격에 대한 식별도 데이터 세트에 추가되었습니다. 이번 보고서에서 이러한 새로운 개선 사항 중 일부를 소개하게 되어 기쁘게 생각합니다. 인터넷 보안 현황 보고서의 이번 이정표를 기념하면서 앞으로 독자 여러분과 함께 이런 업데이트를 계속 공유할 수 있기를 기대합니다.

DDoS(레이어 3, 4)

Akamai Prolexic Routed는 모든 포트와 프로토콜을 포함해 애플리케이션, 데이터 센터, 클라우드, 하이브리드 인터넷 기반 인프라(퍼블릭 또는 프라이빗)에 도달하기 전에 공격 및 기타 원치 않는 악성 트래픽을 차단해 DDoS 공격으로부터 기업을 방어합니다. Akamai SOCC(Security Operations Command Center)의 전문가들은 공격을 즉각적으로 탐지 및 차단하기 위해 선제적인 방어 제어를 조정하고 나머지 트래픽에 대한 실시간 분석을 진행해 필요에 따라 추가적인 방어 조치를 결정합니다. 이렇게 방어된 공격은 공격 이벤트로 정리 및 그룹화되며, 모든 관련 데이터는 SOCC에서 분석하기 위해 기록됩니다.

이 데이터는 2023년 1월 1일부터 2024년 6월 30일까지 18개월 동안 수집되었습니다.

저자 소개

리서치 책임자

미치 메인(Mitch Mayne)

편집 및 작성

트리샤 하워드 (Tricia Howard)
바데트 트리비 (Badette Tribbey)
샬럿 펠리치아 (Charlotte Pelliccia)
마리아 블라삭 (Maria Vlasak)
랜스 로즈(Lance Rhodes)

검토 및 주제별 기여

스벤 더버 (Sven Dummer)
메나헴 펄먼 (Menacham Perlman)
루벤 코 (Reuben Koh)
샌딥 라스 (Sandeep Rath)
토니 라우로 (Tony Lauro)
스티브 윈터펠드 (Steve Winterfeld)
리차드 메우스(Richard Meeus)

데이터 분석

첼시 터틀(Chelsea Tuttle)

홍보 자료

바니 빌(Barney Beal)

마케팅 및 출판

조지나 모랄레스(Georgina Morales)
에밀리 스핑크스(Emily Spinks)

인터넷 보안 현황 보고서 정보

Akamai의 지난 인터넷 보안 현황 보고서를 읽고 다음 보고서를 확인하세요. **akamai.com/soti**

Akamai 위협 연구팀 정보

akamai.com/security-research에서 최신 위협 인텔리전스 분석, 보안 보고서, 사이버 보안 리서치 내용을 확인하세요.

이 보고서의 데이터 확인

이 보고서에 참조로 사용된 그래프와 차트의 고품질 버전을 확인하세요. Akamai가 제공한 소스라는 점이 정식으로 인정되고 Akamai 로고가 보존되는 경우 이러한 이미지를 무료로 사용 및 참조할 수 있습니다. **akamai.com/sotidata**

Akamai 솔루션 정보

애플리케이션 및 API 공격에 대한 Akamai 솔루션은 **애플리케이션 및 API 보안 페이지**에서 확인하세요.

Akamai는 구축 및 전송되는 장소에 상관 없이 만들어지는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 직원, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 **akamai.com**와 **akamai.com/blog**를 확인하거나 X(기존의 Twitter) LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 8월 발행.