SOTI

10 YEARS
OF SECURITY INSIGHT

10권, 01호

API 위협에 대한 공격 트렌드 분석

APJ 스냅샷

Akamai

인터넷/보안 현황 보고서

목차

2 | 보고서의 핵심 인사이트

3 | APJ에서 주목할 만한 API 공격

7 | 방법론

8 | 부록

10 | 저자 소개

보고서의 핵심 인사이트

APJ 스냅샷은 대규모 API 보안 SOTI 보고서, 숨어 있는 API 위협에 대한 공격 트렌드 분석 (영어로만 제공)과 함께 제공됩니다. 공격자들이 본 스냅샷에서 설명하는 공격 기법을 활용하는 방법, 기업을 보호하기 위한 권장사항, 리서치 방법론 및 새로운 데이터 세트에 대한 설명은 해당 보고서를 참조하시기 바랍니다.

개요

디지털 혁신과 API 경제가 직원 및 고객 경험을 개선함에 따라 사이버 범죄자들은 새로운 악용 기회를 얻게 되었습니다. API에 초점을 맞춘 공격은 재정적 손실, 브랜드와 평판 실추 뿐만 아니라 기밀 데이터 손실 및 고객의 신뢰 하락으로 이어질 수 있습니다. API 공격의 규모가 급증하고 민감한 금융 정보를 교환하는 데 API가 점점 더 많이 사용됨에 따라 사이버 보안 규제 감독 및 보고 의무가 증가하면서 API 보안이 그 어느 때보다 중요해졌습니다.

API 위협 환경을 더 잘 이해하기 위해 웹 애플리케이션과 API 공격을 전체적으로 살펴보는 대신, Akamai 연구원들은 2024년에 2가지 종류의 공격을 구분하고 API를 대상으로 한 공격 비율에 집중하기 위해 새로운 데이터 세트를 사용하고 있습니다. 2023년 1월부터 12월까지 아우르는 이 APJ 스냅샷에서는 여러 공격 트렌드와 이것이 무엇을 의미하는지 살펴봅니다.

- 전 세계적으로 아시아 태평양 및 일본(APJ) 지역에서 API 공격 비율은 15.0%로, 유럽, 중동 및 아프리카(EMEA) 지역(47.5%), 북미 지역(27.1%)에 이어 세 번째로 높았습니다.
- 전반적인 웹 공격을 살펴본 이전 보고서와 마찬가지로, 로컬 파일 인클루전(LFI)은 APJ에서 API에 대한 공격 기법으로 널리 사용되고 있습니다. 또한, 새로운 데이터 세트에 따르면 명령 주입(CMDi)과 서버 측 요청 위조(SSRF)도 API 공격에서 널리 사용되는 기술입니다.
- 봇 요청도 우려되는 부분입니다. 2조 건 이상의 의심스러운 봇 요청 중 40%가 API를 겨냥한 것으로 나타났습니다.
- API 공격 비율은 제조업계가 31.2%로 가장 높았으며 게임(25.2%), 첨단 기술(24.4%), 비디오 미디어(24.0%), 커머스(22.3%) 순이었습니다.

APJ에서 주목할 만한 API 공격

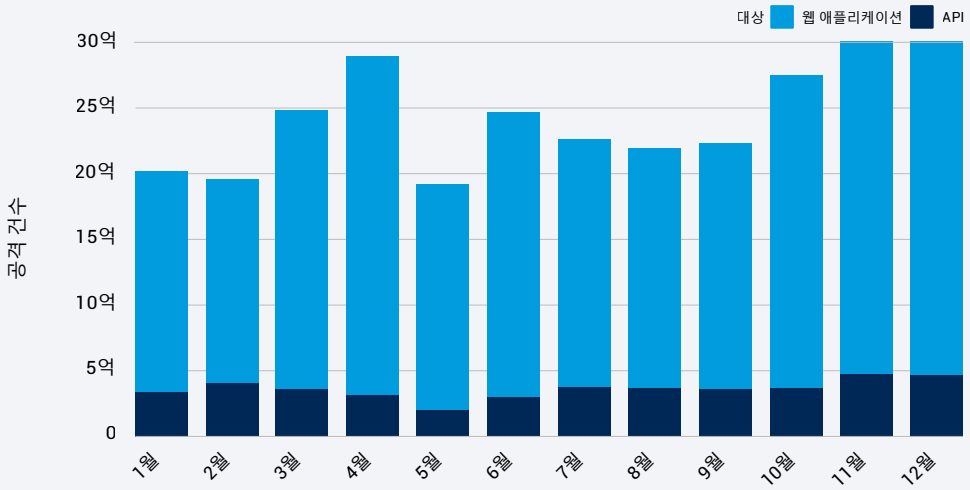
API 공격 트래픽을 집중적으로 추적하는 새로운 데이터 세트 기반의 Akamai 리서치에 따르면 APJ 지역에서 발생한 전체 웹 공격 중 15.0%가 API를 대상으로 한 것으로 나타났습니다. 전세계적으로 APJ 지역은 EMEA 지역(47.5%), 북미 지역(27.1%)에 이어 세 번째로 높은 API 공격 비율을 보였습니다.

2023년 1월부터 12월까지 API를 대상으로 한 웹 공격은 월별로 11~21% 사이에서 변동했습니다(APJ 그림 1). 이런 상대적으로 낮은 비율의 공격(다른 지역에 대한 공격 비율과 비교했을 때)은 부분적으로 오픈 API 시장 규모가 유럽 및 북미에 비해 상대적으로 작아서 APJ 지역 기업들의 도입률이 낮기 때문이라고 할 수 있습니다.

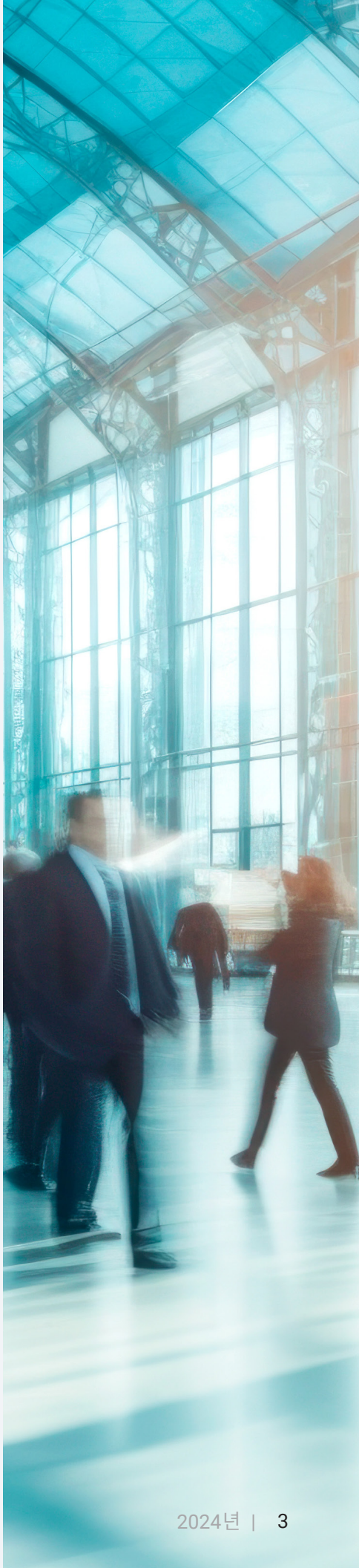
APJ: 월간 웹 공격 건수

2023년 01월 1일~2023년 12월 31일

APJ 그림 1: 전체 웹 공격이 증가했음에도 불구하고 API를 대상으로 한 공격은 평균 15.0% 기록

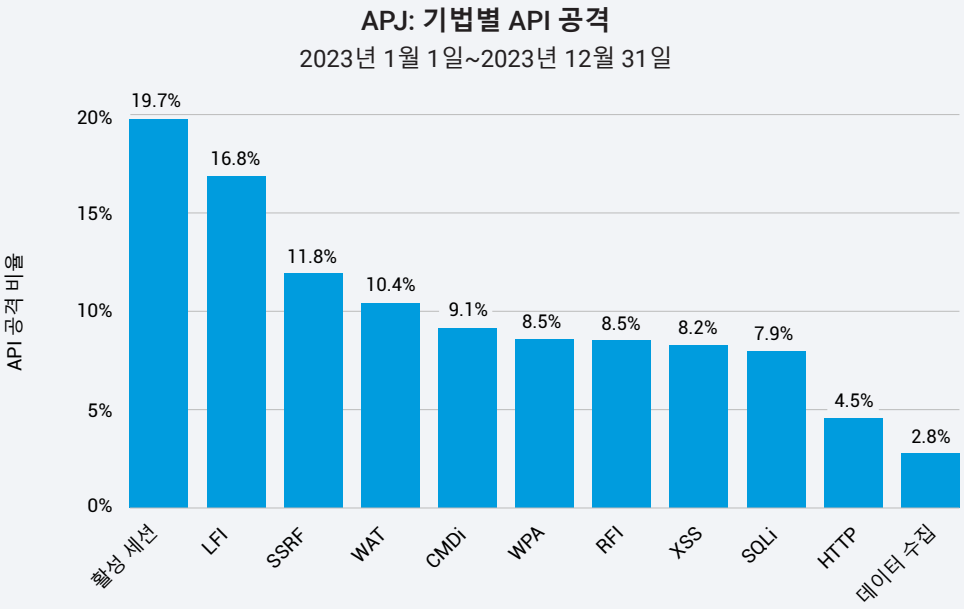


APJ 지역에서 API를 겨냥한 웹 공격 비율이 가장 높은 국가는 한국(47.9%), 인도네시아(39.6%), 홍콩특별행정구(38.7%), 말레이시아(26.4%), 일본(23.4%), 인도(19.0%), 호주(15.6%), 싱가포르(5.8%), 필리핀(5.5%), 뉴질랜드(4.8%)입니다.



공격받고 있는 API: 트래픽 분석

전반적인 웹 공격을 살펴본 이전 보고서와 마찬가지로 LFI는 APJ에서 API에 대한 주요 공격 기법입니다. 그러나 특히 API 공격과 관련해 크로스 사이트 스크립팅(XSS) 및 구조화된 쿼리 언어 인젝션(SQLi)은 목록에서 순위가 더 낮아졌습니다(APJ 그림 2).



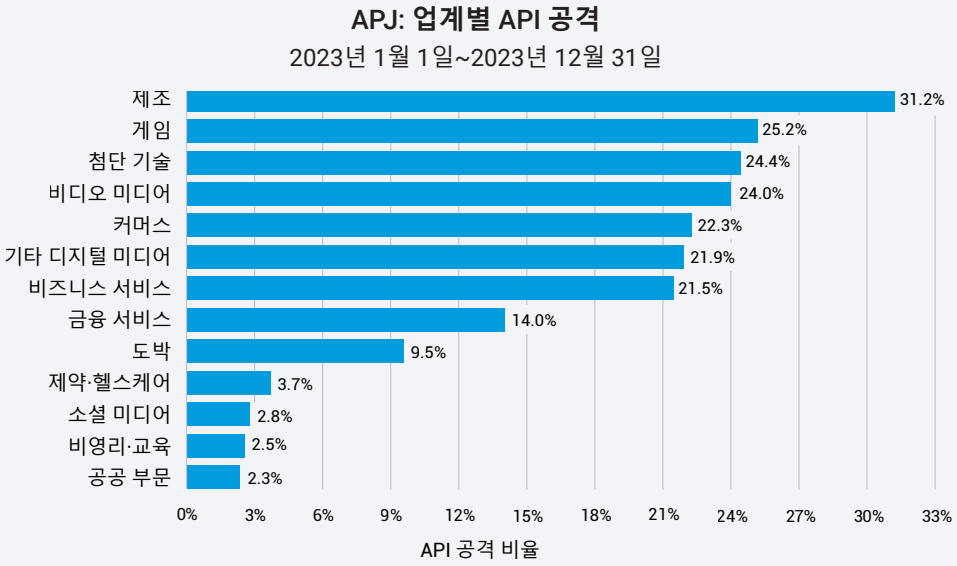
APJ 그림 2: LFI는 여전히 널리 사용되는 공격 기법이며 새로운 데이터 세트를 사용해 API를 공격할 때 선호되는 공격 기법을 추가로 확인했습니다.

새로운 데이터 세트를 통해 선호되는 API 공격 기법을 추가로 확인할 수 있습니다. 예를 들어, CMDi는 API 공격에서 널리 사용되는 기술이며, SSRF(2023 보고서에서 설명)는 현재 가장 자주 사용되는 기법 중 하나입니다. 참고로, 활성 세션은 해당 세션 중에 의심스러운 행동을 나타내며 이로 인해 일시적 차단이 발생합니다. (공격 기법 정의에 대한 전체 목록은 부록을 참조하시기 바랍니다.)

Akamai 리서치에 따르면 봇 요청이 우려되는 부분이라는 사실도 밝혀졌습니다. 동일한 12개월의 보고 기간 동안 2조 건 이상의 의심스러운 봇 요청 중 40%가 API를 겨냥한 것으로 나타났습니다.

업계 전반에 걸친 API 공격

Akamai 연구원들은 보고 기간 동안 API를 대상으로 한 전체 웹 공격 중 제조업계가 31.2%로 가장 높은 비율을 차지했으며, 뒤를 이어 게임 25.2%, 첨단 기술 24.4%, 비디오 미디어 24.0%, 커머스 22.3%를 차지했다고 밝혔습니다(APJ 그림 3).



APJ 그림 3: 제조업계에 대한 API 공격 비율이 가장 높은 이유는 핵심 인프라가 API를 통해 점차 더 많이 연결되고 있고 공급망 중단 가능성이 존재하기 때문입니다.

결론

API 방어는 보안 및 리스크 관리 측면에서 분명한 필수 요소입니다. 또한 사이버 보안 법안을 위협 환경에 맞춰 유지하기 위한 기존의 법 및 규정과 새로운 개혁 역시 API 보안의 필요성을 강조합니다.

예를 들어, 인도는 2023년 8월의 디지털 개인 데이터 보호 법안 통과를 시작으로 IT 법안의 대대적인 개편이 될 디지털 인도 법안 초안을 작성하는 과정에 있습니다. 호주 정부는 2023년 11월 23일에 안전한 기술과 디지털 제품 및 소프트웨어에 대한 신뢰를 보장하는 데 중점을 둔 2023-2030 호주 사이버 보안 전략을 발표했습니다. 또한, 예정된 결제 카드 업계 데이터 보안 표준(PCI DSS) v4.0의 섹션 6은 유출 리스크를 줄이기 위해 특히 시스템과 소프트웨어의 개발 및 유지 관리 과정에서 API 사용에 대한 새로운 표준을 포함합니다.

규제 당국은 민감한 금융 정보를 교환하는 데 점점 더 많이 사용되고 있는 API에 대한 사이버 보안 표준을 강화하기 위해 계획과 정책을 수립하고 있습니다. API를 보안 프로그램에 통합하여 가시성을 개선하고, 방어를 강화하며, 컴플라이언스 요구사항을 적용할 수 있도록 모범 사례와 지침을 이해하는 것이 중요합니다.

자세한 내용은 글로벌 API 보안 SOTI 보고서, 숨어 있는 API 위협에 대한 공격 트렌드 분석을 참조하시기 바랍니다.

방법론

웹 애플리케이션 및 봇 공격

이 데이터는 웹 애플리케이션 방화벽(WAF)과 봇 관리 툴을 통해 관측된 트래픽에 대한 애플리케이션 레이어 알림을 설명합니다. 보호하고 있는 웹사이트, 애플리케이션 또는 API에 대한 요청에서 악성 페이로드가 탐지되면 웹 애플리케이션 공격 알림을 트리거합니다. 보호하고 있는 웹사이트, 애플리케이션 또는 API에 대한 요청에서 봇 페이로드가 탐지되면 봇 알림을 트리거합니다. 이런 봇 알림은 악성 봇과 정상 봇 모두에 의해 트리거될 수 있습니다. 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 130개국 이상에서 4000개 이상의 엣지 네트워크 거점으로 구성된 글로벌 네트워크인 Akamai Connected Cloud에서 탐지된 보안 이벤트를 분석하는 내부 툴에서 추출한 것입니다. Akamai 보안팀은 매달 페타바이트 규모의 데이터를 활용해 공격을 연구하고, 악성 행동을 식별하며, Akamai 솔루션에 인텔리전스를 추가합니다.

이 보고서의 데이터는 2023년 1월 1일부터 2023년 12월 31일까지 12개월 동안 수집되었습니다.

2024년 데이터 업데이트

Akamai는 10주년을 기념해 데이터 세트에 대한 몇 가지 업데이트를 발표하게 된 것을 기쁘게 생각합니다. Akamai의 웹 애플리케이션 및 봇 공격 데이터 세트에 몇 가지 업그레이드가 있었습니다. 각각의 수집 방법이 변환, 간소화, 최적화되었습니다. 인사이트의 범위가 넓어지고 깊어졌습니다. SSRF와 같은 추가 공격 기법에 대한 항목이 추가되었습니다. API 엔드포인트를 겨냥한 공격의 식별도 각 데이터 세트에 추가되었습니다. 이 보고서에서 새로운 개선 사항에 대해 공유할 수 있어 기쁘게 생각하며 독자들과 함께 인터넷 보안 현황 보고서의 중요한 이정표를 기념하면서 2024년과 그 이후에도 이러한 업데이트를 계속 공유할 수 있기를 기대합니다.

Akamai API Security 인사이트

API Security 알림을 기반으로 API 리스크와 잠재적 영향에 대해 자세히 살펴보고 실제 인사이트를 제공해 주신 Akamai API Security 솔루션 엔지니어링 팀에게 특별히 감사드립니다.

부록

공격 기법	정의
활성 세션	최근 클라이언트에 대한 공격 트래픽이 플래그 지정되었으며 반복되는 요청은 세션 기간 동안 차단됩니다.
명령어 인젝션(CMDi)	공격자는 기존 명령에 새로운 항목을 삽입해 의도된 것과 다르게 자신이 선택한 동작으로 수정합니다.
크로스 사이트 스크립팅(XSS)	공격자는 콘텐츠에 악성 스크립트를 포함시켜 콘텐츠가 웹 브라우저에 제공될 때 대상 소프트웨어가 사용자의 권한 수준으로 스크립트를 실행하도록 합니다.
데이터 수집	공격자는 대상 및 통신의 설계 또는 설정에서 약점을 악용해 의도한 것보다 더 많은 정보를 공개합니다. 다른 종류의 공격에 대비해 데이터를 수집하기 위해 종종 실행되지만 정보에 대한 접속 권한을 얻는 것이 공격자의 최종 목표일 수도 있습니다.
HTTP 프로토콜(HTTP)	공격자는 클라이언트와 서버가 예상치 못한 작업을 수행하기 위해 통신하는 프로토콜의 약점을 이용합니다. 다양한 종류의 프로토콜을 악용하면 공격의 최종 목표가 달라질 수 있습니다.
로컬 파일 인클루전(LFI)	공격자가 대상 소프트웨어에 대한 입력을 조작해 접속 권한이 없는 파일 시스템 영역에 접속하거나 수정할 수 있습니다.

공격 기법	정의
리모트 파일 인클루전(RFI)	공격자는 원격 임의 코드를 로드하고 실행하여 대상 애플리케이션을 가로채고 자체 명령을 실행하도록 강제합니다.
서버 측 요청 위조(SSRF)	공격자는 서버의 기능을 악용하여 내부 리소스를 읽거나 업데이트합니다.
구조화된 쿼리 언어 인젝션(SQLi)	공격자는 입력 문자열을 조작하여 대상 소프트웨어가 사용자 입력을 기반으로 SQL 문을 구성하려고 할 때 결과로 생성되는 SQL 문이 공격자가 의도한 작업을 대신 수행하도록 합니다. 주입에 성공하면 정보 유출이 발생할 수 있을 뿐 아니라 데이터베이스에서 데이터를 추가하거나 수정할 수도 있습니다.
웹 공격 툴(WAT)	공격자는 악의적 목적으로 활용될 수 있는 정보를 요청하도록 설계된 방식으로 표적을 적극적으로 조사합니다. 이러한 조사를 통해 표적의 보안, 설정 또는 잠재적인 취약점을 추론하는 데 도움이 되는 정보를 얻을 수 있습니다.
웹 플랫폼 공격(WPA)	다른 공격 그룹으로 분류되지 않은 소프트웨어 플랫폼(클라우드, 웹 또는 애플리케이션 레이어)에 대한 공격

저자 소개

편집 및 작성

바데트 트리비(Badette Tribbey) – 편집장
샬럿 펠리치아(Charlotte Pelliccia) – 수석 작가(지역 대표)

편집 기고자

제임스 케이시(James Casey)
에드워드 로버츠(Edward Roberts)
스티브 윈터펠드(Steve Winterfeld)

검토 및 주제별 기여

톰 에몬스(Tom Emmons)
루벤 코(Reuben Koh)
롭 레스터(Rob Lester)
리처드 메우스(Richard Meeus)
아비게일 오제다(Abigail Ojeda)
메나헴 펄만(Menachem Perlman)
야리프 시베크(Yariv Shivek)

데이터 분석

첼시 터틀(Chelsea Tuttle)

마케팅 및 출판

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

인터넷/보안 현황 보고서

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

Akamai 위협 연구팀 자세히 살펴보기

akamai.com/security-research에서 최신 위협 인텔리전스 분석, 보안 보고서, 사이버 보안 연구 리서치를 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 자세히 알아보기

API 공격에 대한 Akamai 솔루션을 자세히 살펴보려면, **앱 및 API Security 페이지**를 참조하시기 바랍니다.

2024년 03월 발행.