Akamai

백서

고객 신뢰를 위협하는 공격 기법

보안과 브랜드 신뢰는 지금 그 어느 때보다 상호 의존적입니다. 전 세계적으로 사이버 공격이 급증하고 애플리케이션과 API는 브랜드가 세상에 보여지는 방식을 주도하고 있습니다. 이런 가운데 고객 경험을 저해하지 않으면서 디지털 애플리케이션을 보호하는 것은 전 세계 보안팀의 최우선 과제가 되었습니다.

강력한 고객 경험은 브랜드 신뢰를 구축하며, 이는 사업 성과에 분명한 영향을 미칩니다. 웹사이트 성능부터 데이터 보안에 이르기까지, 보안과 관련된 기업의 선택은 고객 경험에 부정적인 영향을 미치는 경우가 많습니다. 사업을 보호하기 위한 번거로운 제어는 고객 불편을 일으켜 고객의 신뢰를 잃고 결국에는 매출 감소로 이어질 수 있습니다.

보안과 관련된 선택은 성장과 혁신에도 영향을 줍니다. 기업이 계속해서 디지털 방식으로 확장하고 데이터와 애플리케이션을 클라우드로 전환함에 따라 수많은 공격자가 이러한 움직임으로 인해 가능해진 공격 기법에 주목하고 있습니다. 이제 보안 솔루션은 기업 그리고 고객의 브랜드에 대한 신뢰를 지킬 수 있는 솔루션을 선택해 공격자의 변화하는 기법과 정교한 멀티 기법 공격(여러 종류의 공격을 동시에 또는 빠르게 연이어 진행하는 것)보다 더 빨리 발전하는 것을 목표로 삼아야 합니다.

어떤 공격 기법을 최우선으로 고려해야 할까요?

가장 최근에 등장한 새로운 공격 대상은 API

애플리케이션은 비즈니스의 거의 모든 측면을 이끌고 있으며 소프트웨어를 연결하고 다양한 애플리케이션 간의 통신을 가능하게 하는 애플리케이션 프로그래밍 인터페이스(API)는 공격자가 선호하는 새로운 표적이 되었습니다. 왜 그럴까요? API와 관련된 애플리케이션과 사업 절차가 보안팀이 평가할 수 있는 속도보다 더 빠르게 시작 및 배포되어 설정 오류와 취약점을 초래하는 경우가 매우 많기 때문입니다. 공격자는 이러한 결함을 노리고, 비즈니스 로직 남용을 활용합니다. API 공격이 성공하면 사용자 환경에 접속해 데이터를 훔치고 추가 공격을 시작합니다. 공격자가 노리는 것은 웹 애플리케이션 방화벽(WAF)을 통과하는 API 뿐만이 아닙니다. API는 WAF로 인증된 경우에도 여전히 공격에 취약할 수 있으며, 이는 공격자가 정기적으로 정찰을 통해 악용할 만한 API를 탐지하고 있다는 것을 의미합니다.

모든 API가 잠재적으로 표적이 될 수 있다는 점을 기억해야 합니다. 예를 들어, 헬스케어와 같은 업계에서는 IoT 디바이스의 상호 운용성으로 인해 API가 개인 식별 정보(PII)를 훔치거나 랜섬웨어 공격을 시작하려는 범죄자에게 큰 표적이 되고 있습니다. 따라서 API 보안은 기업과 관련된 모든 API, 즉 API 자산에 대한 가시성을 확보하는 것에서 시작됩니다.

Akamai API Security는 실제로 자산 인벤토리 파악을 지원해 모든 API의 과거 행동에 대한 가시성을 제공하기 때문에 정상적인 API 행동과 악의적 API 행동이 무엇인지 알 수 있습니다. 이러한 지식을 바탕으로 활성 위협을 추적해 공격자가 목표를 달성하기 전에 남용을 신속하게 차단할 수 있습니다.

그 어느 때보다 정교하고 쉽게 배포되는 악성 봇

봇은 웹사이트를 통해 끊임없이 이동합니다. 검색 엔진의 최적화를 위한 모든 노력은 사실 봇에게 매력적인 요소로 작용합니다. 정상 봇 중에는 다양한 사이버 공격을 일으키는 악성 봇도 섞여 있습니다. 악성 봇은 한정판 운동화나 다량의 콘서트 티켓, 호텔 예약 등 한정된 재고를 독점하는 것으로 가장 잘 알려져 있지만, DDoS(Distributed Denial-of-Service) 공격 시 과도한 양의 요청으로 사업 운영에 부담을 주어 오프라인으로 전환하게 만들고자 할 때도 거의 동일한 방법을 사용합니다.

많은 사람이 모르는 사실은 DDoS가 비교적 쉽고 저렴한 공격 형태로 자리 잡으면서 새로운 공격자가 수십억 달러 규모의 기업과 학교, 병원, 공항, 공공 서비스 공급업체 등 중대한 공공 인프라를 무너뜨리는 데 사용된다는 것입니다. 이러한 공격은 대규모 서비스 중단을 일으켜 피해자에게 막대한 분당 매출 손실을 입힙니다. 과거의 공격과 확연하게 다른 점은 거의 대부분의 공격이 정교한 국가 행위자, 정치적인 핵티비스트, 전문 사이버 범죄자가 봇넷(봇에 의해 감염 및 제어되는 사용자 디바이스 또는 간소한 IoT 디바이스 등 커넥티드 디바이스로 이루어진 대규모 네트워크)의 도움을 받아 이루어진다는 것입니다.

봇은 또한 계정 탈취로 이어지는 크리덴셜 스터핑 공격을 시작하는 데 사용됩니다. 크리덴셜 스터핑은 공격자가 대규모 데이터 유출로 얻은 사용자 이름과 비밀번호 목록을 사용해 다른 기관에 로그인을 시도할 때 해당 인증정보를 대량으로 제출하면서 발생합니다. 봇은 수백만 건의 계정 탈취 시도를 위해 배포되며, 많은 사람들이 사용자 이름과 비밀번호를 재사용하는 경향이 있기 때문에 그중 일부만 성공합니다. 공격자가 계정에 접속하면 이는 계정 탈취 공격이 됩니다.

크리덴셜 스터핑은 공격자가 정상적인 계정을 탈취하기 위해 사용하는 여러 방법 중 하나일 뿐입니다. 계정을 장악하고 나면 멤버십 포인트를 빼돌리고, 디지털 자산을 이전하며, 기프트 카드 잔액을 빼내고, 저장된 신용 카드 정보를 사용해 사기성 구매를 할 수 있습니다. 심지어 전체 계정을 다른 공격자에게 판매할 수도 있습니다. 이러한 일이 고객에게 발생하면 거의 항상 돌이킬 수 없을 정도로 신뢰가 깨집니다. 하지만 실패한 크리덴셜 스터핑 공격도 브랜드에 치명적일 수 있습니다. 공격이 시도되는 동안 사이트에 봇 트래픽이 폭주하면 리소스 가용성이 크게 줄고 응답 시간이 느려져 고객과 사이트 방문자가 실망스러운 경험을 할 수 있기 때문입니다.

마지막으로 스크레이퍼 봇은 정상 목적과 악성 목적 모두를 위해 사용되지만, 존재 자체가 사이트 성능을 저하시키고 기업이 중요한 의사결정을 하는 데 필요한 지표를 오염시킬 수 있어 스크레이핑으로 인한 부작용이 잠재적으로 브랜드에 더 큰 피해를 줄 수 있습니다.

Akamai는 악성 봇으로 인한 위협을 방어하기 위해 특별히 설계된 다음과 같은 솔루션을 제공합니다.

멀웨어 방어 기능이 포함된 Akamai App & API Protector는 데이터, PII 및 기타 계정 정보의 도난을 방지하고 봇 기반 DDoS 공격과 랜섬웨어, 멀웨어 등을 차단하는 기본 솔루션입니다. 이를 통해 고객은 웹 자산에 지속적으로 접속할 수 있으며 공격이 발생하더라도 사이트 성능이 저하되는 것을 방지할 수 있습니다.

Akamai Bot Manager는 모든 봇 트래픽을 탐지하고 엣지에서 악성 봇을 방어합니다. AI 모델을 사용해 봇 행동을 분석하고 브라우저 핑거프린팅 및 머신 러닝(ML) 알고리즘을 배포해 탐지 정확도를 높여 사용자 불편을 줄이면서 동시에 사기성 활동으로부터 사용자를 보호합니다.

Akamai Content Protector는 스크레이퍼가 웹 콘텐츠를 도용해 악의적인 목적으로 사용하는 것을 방지하는 동시에 사이트 성능 저하를 방어합니다. ML 기반 탐지를 통해 잠재적으로 악성 봇 스크레이퍼 활동을 리스크별로 분류해 적절한 대응 방법을 알려줍니다.

고객 보호를 위한 또 다른 기본 솔루션은 보안 계정 접속을 강화하는 것입니다. Akamai Account Protector는 봇과 연계해 사람이 주도하는 사기를 차단하는 동시에 신뢰할 수 있는 사용자가 사이트에 원활하고 안전하게 접속하도록 지원해 로그인 상태를 오래 유지하고 자주 재방문하도록 유도합니다.

악성 스크립트로 인한 비용: 클라이언트측 위협

봇과 마찬가지로 써드파티 스크립트는 대체로 기업에 유익합니다. 기능, 마케팅 툴, 애널리틱스 등을 통해 전반적인 사용자 경험(UX)을 개선합니다. 하지만 웹 브라우저를 중요한 클라이언트측 위협 표면으로 전환시키기도 합니다.

클라이언트측 위협은 고객을 속여 악성 콘텐츠에 접속하도록 유도하는 것을 목표로 합니다. 이는 사용자(일반적으로 고객, 여기서는 클라이언트라고 함)가 직접 운영하는 컴퓨터에서 실행 중인 애플리케이션의 취약점을 이용합니다. 따라서 클라이언트측 보안은 웹 페이지에서 발생하는 악성 활동으로부터 고객을 보호하는 데 사용되는 기술과 정책을 포괄합니다.

스크립트 공격은 기업에 심각한 금전적 피해를 입히고 고객, 파트너, 결제 처리업체의 신뢰를 떨어뜨릴 수 있습니다. 당연히 클라이언트측 보안은 PCI DSS(Payment Card Industry Data Security Standard) v4.0에 새롭게 도입된 요구사항의 핵심입니다. 이를 준수하려면 온라인에서 결제 카드를 처리하는 모든 기업은 사이트에서 어떤 스크립트가 실행 중인지, 언제 변경되는지, 언제 실행이 중지되는지 파악해야 합니다.

이러한 공격은 방어하기 쉽지 않습니다. 써드파티 스크립트는 매우 많고 지속적으로 변경되기 때문에 모니터링하기가 매우 어렵습니다. 스크립트 공격 자체도 웹 스키밍, 폼재킹 등 다양한 형태를 취합니다. 모든 범죄 단체(Magecart가 가장 악명 높음)는 이러한 기술을 중심으로 조직을 구성해 결제 카드 데이터와 PII를 훔쳤습니다.

디지털 결제와 온라인 쇼핑 및 리서치의 세계에서 클라이언트측 보안은 지금 그 어느 때보다 중요하며, 특히 개인 및 금융 데이터가 수집되는 결제 및 지불 페이지에서 더욱 중요합니다. 따라서 사이트에서 실행되는 모든 스크립트에 대한 가시성, 의심스러운 행동을 탐지하는 기능, 공격을 방어할 수 있는 방어 조치를 갖추어야 합니다. Akamai는 이러한 위협에 대응할 수 있는 다음의 구체적인 솔루션을 제공합니다.

Client-Side Protection & Compliance는 웹 스키밍, 폼재킹, Magecart와 같은 클라이언트측 공격으로부터 모든 사용자를 보호해 브라우저 내에서 고객의 개인정보와 신뢰를 유지합니다.

인프라를 보호함으로써 고객 경험 보호

고객 경험의 핵심에는 브랜드의 모든 것을 뒷받침하는 기본 디지털 인프라가 있습니다. DNS 보안, 안정성, 성능은 고객이 필요할 때 언제든 서비스에 접속할 수 있게 합니다. DNS 시스템은 본질적으로 기업의 온라인 입지와 동일합니다. 이 시스템이 다운되면 디지털 세계에서 기업의 존재도 함께 사라집니다. 따라서 공격자는 DNS 시스템을 대상으로 끊임없이 DDoS 공격을 일으킵니다. 모든 업계가 직면한 치열한 경쟁 환경을 고려할 때, 고객과 잠재 고객이 브랜드가 제공하는 최고의 경험을 누리려면 무중단 DNS 가용성과 100% 가동 시간이 보장되어야 합니다.

Akamai는 다양한 DDoS 공격으로부터 디지털 인프라를 보호하기 위해 다음과 같은 최고의 솔루션 포트폴리오를 제공합니다.

Akamai Prolexic은 가장 강력한 DDoS 방어를 위해 전 세계 32개 이상의 지역에 위치한 스크러빙 센터와 20Tbps의 전용 방어 용량 등 다양한 보안 옵션을 제공합니다.

Akamai Edge DNS는 특별히 설계된 포괄적인 권한 DNS 솔루션으로, Akamai Connected Cloud의 규모, 보안, 용량을 사용해 DNS 영역을 관리합니다.

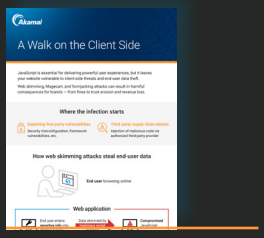
동적 보안 정책 적용 기능을 갖춘 양방향 DNS 프록시 솔루션인 Akamai Shield NS53은 온프레미스, 클라우드, 하이브리드 등 오리진 DNS 인프라의 주요 구성요소를 리소스 고갈 공격으로부터 보호합니다.

고객의 신뢰를 보장하는 파트너

Akamai는 25여 년간 브랜드를 지원하는 데 집중해 왔습니다. 콘텐츠 전송 네트워크(CDN)의 선구자로 시작해 최초의 디지털 스토어의 속도 문제를 해결했습니다. 지난 10년 동안 세계 최대 규모의 CDN이 제공하는 트래픽 가시성을 활용해 매일 위협을 모니터링하고 분석했으며, 공격 기법이 지속적으로 발전하고 변함에 따라 유기적으로 보안 솔루션을 변화시키고자 리서치를 진행해 왔습니다. 고객의 핵심 보안 파트너로서 고객의 사업 운영과 고객 경험을 보호하는 동시에 업계를 선도하는 새로운 디지털 경험을 실험할 수 있는 자신감을 제공하고자 최선을 다하고 있습니다.

다음 단계

다음은 브랜드 보호를 위한 최선의 조치를 고려하는 데 도움이 될 만한 리소스입니다.



클라이언트측 보안 기능으로 웹 페이지 무결성을 강화하세요.

웹사이트, 애플리케이션, API에 대한 타협 없는 원스톱 보안을 확보하세요.

봇 관리 전략의 주요 고려 사항을 알아보세요.

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.com와 akamai.com/blog를 확인하거나 X(기존의 Twitter), LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다.
2024년 6월 발행.