Akamai

백서

올바른 애플리케이션 레이어 DDoS 플랫폼으로

혼란을 방지하는 방법

오늘날 애플리케이션 레이어 DDoS가 의미하는 것

전 세계 보안 전문가들도 익히 잘 알고 있듯이 DDoS (Distributed Denial of Service)는 웹 사이트나 네트워크 리소스에 악성 트래픽을 대량으로 보내 운영이 불가능하게 만드는 사이버 공격입니다. DDoS 공격은 공격자들이 여전히 가장 많이 사용하는 공격 기법으로 지난 5년 동안 꾸준히 증가해왔습니다. 일례로 가장 최근에 발생한 대규모 공격 중 하나(초당 패킷인 PPS 기준)는 약 2분 동안 809 MPPS를 기록했습니다.

공격이 증가하는 상황에서 Akamai가 관측한 한 가지 트렌드는 애플리케이션 레이어 DDoS 공격의 증가입니다. 레이어 7 DDoS라고도 하는 이 공격은 전체 네트워크가 아닌 특정 웹 애플리케이션을 마비시킵니다. 따라서 보안팀 직원이 예방하고 방어하기는 어렵지만, 자동화와 클라우드 서비스 같은 기술이 많이 도입되면서 공격자가 이러한 공격을 실행하는 데 필요한 툴에 쉽게 접속하고 애플리케이션 레이어를 감염시키는 것이 그 어느 때보다 쉬워졌습니다.

실제로 이러한 종류의 공격에 사용되는 요청은 정상적인 최종 사용자 요청처럼 보이기 때문에 공격이 얼마나 정교한지 측정하기 어렵습니다. 표적 서버와 네트워크 모두에 영향을 미치는 효율적인 공격은 적은 양의 총 대역폭으로 더 많은 피해를 입힐 수 있습니다. 한마디로 애플리케이션 레이어 공격은 실행하기 쉽지만 속도를 늦추거나 멈추기는 어렵고, 특정 대상을 표적으로 합니다.

애플리케이션 레이어 DDoS 공격이 기업에 미치는 고유한 영향을 이해하려면 모든 범주에서 DDoS 공격이 어떤 영향을 미치는지 알아야 합니다. DDoS 공격의 범주는 파티의 함정과 같습니다. 예를 들어, 특별한 날을 축하하거나 주말에 즐거운 시간을 보내기 위해 집으로 손님 몇 명을 초대했다고 가정해 보겠습니다. 그러나 다음과 같은 몇 가지 시나리오가 발생할 수 있습니다.

DDoS 공격 종류

시나리오 1
증폭 공격

파티를 즐기는 동안 흥분한 손님들이 소셜 미디어를 통해 너무 많은 정보를 공유합니다. 파티가 누구도 놓치고 싶지 않은 이벤트라는 소문이 퍼지면서 파티 당일에 갑자기 수많은 낯선 이들이 찾아옵니다. 초대받지 않은 사람이 모든 리소스를 사용하는 이러한 상황은 증폭 DDoS 공격과 유사합니다.

시나리오 2
프로토콜 공격

믿을 수 있다고 생각했던 손님의 상태가 좋지 않습니다! 파티에 초대받고 싶지만 초대받지 못한 사람들이 초대받은 손님들에게 파티에 대해 자세히 알고 싶다며 대량의 요청을 보낸 것입니다. 초대받은 손님이 파티에 대한 정보를 주면 초대받지 않은 사람들이 파티에 난입할 수 있습니다. 파티의 기밀을 유지해야 하는 누군가가 기밀을 유지하지 않았다는 점에서 이는 프로토콜 DDoS 공격과 유사합니다.

시나리오 3
애플리케이션 공격

악당이 파티에 대한 소식을 듣고 절도를 계획, 파티 손님으로 위장하고 집에 침입해 강도를 저지르기로 결정합니다. 정식으로 초대받은 손님을 모방하는 것이므로 이는 애플리케이션 DDoS 공격과 유사합니다.

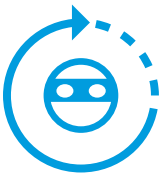
이 모든 시나리오에는 이벤트를 위해 집을 개방했다는 공통된 취약점이 있습니다. 애플리케이션 레이어는 기업이 사용자와 상호 작용하는 레이어이기 때문에 애플리케이션 레이어 DDoS 공격이 악용할 수 있는 취약점은 존재할 수밖에 없습니다. 또한 사용자에게 직접 서비스를 제공하기 때문에 제어할 수 있는 레이어가 적어 애플리케이션 레이어 DDoS 공격을 방어하기가 더 어려울 수 있습니다.

더불어 이러한 문제가 생길 경우 추가 비용이 발생할 수 있습니다. 음식과 음료 소비량이 증가하고 낯선 사람이 내 개인 정보를 알아내거나 집이 공격의 영향을 받는 등 혼란스러운 파티는 많은 비용을 발생시킵니다.

수많은 보안 솔루션이 현재 가장 흔하고 방어하기 가장 어려운 공격 중 하나인 애플리케이션 레이어 DDoS 공격으로부터 시스템, 리소스, 민감한 정보를 보호한다고 약속합니다. 기업은 자산을 보호하기 위해 이런 솔루션을 신뢰해 왔습니다. 결과적으로 DDoS 방어는 보안 기능을 제공하는 플랫폼의 성능에 의해 좌우됩니다. 다음은 애플리케이션 레이어 DDoS 방어 플랫폼을 선택할 때 알아두어야 할 최신 변동 사항과 트렌드를 살펴보겠습니다.

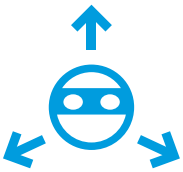
트렌드 및 변화

항상 그렇듯이 특정 공격에 대한 솔루션을 만들면 해커는 이에 대응할 목적으로 기존 전략을 수정합니다. 이러한 경쟁을 모니터링한 결과, 다음과 같은 4가지 트렌드와 변화를 관측했습니다.



1. 반복적인 단기간 공격으로 전환

DDoS 공격의 기간은 점점 짧아지는 반면, 공격의 규모와 빈도는 점점 더 커지고 있습니다. Akamai는 ARM, SYN 플러드, UDP 리플렉션(DNS, WS-Discovery 등), HTTP 플러드 등 9가지 이상의 공격 기법이 결합된 복잡한 공격을 확인했습니다.

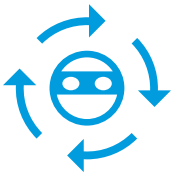


2. 다중 기법 공격의 빈도 증가

공격자의 20% 이상이 여러 가지 DDoS 공격 방법을 결합해 하나의 짧은 공격으로 만든 후 짧은 시간 안에 반복하는 다중 기법 DDoS 공격을 일으키고 있습니다. Link11에 따르면 가장 많이 관측된 동시 공격 기법의 수는 2021년 대비 50% 증가한 18개로 나타났습니다.

3. 탐지 및 후속 방어를 회피하는 역량 확대

특히 애플리케이션 레이어의 경우 공격 트래픽과 정상 트래픽을 구분하는 것이 어렵습니다. 예를 들어 봇넷은 피해자의 서버를 대상으로 HTTP 플러드 공격을 펼칩니다. 봇넷의 각 봇은 겉으로는 정상적인 네트워크 요청을 하는 것처럼 보이기 때문에, 트래픽이 스푸핑되지 않고 오리진에서 '정상'인 것으로 나타날 수 있습니다.



4. 선 자동화 후 기법 조정

클라우드 플랫폼과 IaaS/PaaS가 널리 보급됨에 따라 공격자는 자동화와 컴퓨팅 성능을 손쉽게 활용해 공격을 자동화하고 대규모 공격을 빠르게 시작할 수 있습니다. 따라서 이러한 공격은 단순한 증폭 공격보다 더욱 분산되고, 무작위적이고, 정교한 형태(요청의 매개변수 무작위화 등)를 보입니다.

파티 시나리오에서 언급했듯이 여러분의 집이 리소스 소비, 취약한 손님, 위장한 공격자의 세 가지 원인으로 손상될 수 있습니다. 애플리케이션 레이어 공격의 트렌드와 변화로 인해 사용자의 레이더망을 피하도록 설계된 혼란이 발생할 수 있습니다. 또는 집에 출입구가 몇 개 있는지 미리 파악하거나, 파티 드레스 코드를 미리 알아내거나, 가짜 소셜 미디어 프로필을 생성해 파티 주최자가 파티에 참석한 모든 손님이 친한 친구라고 생각하도록 속이는 등 모든 것이 이 세 가지 범주에 걸쳐 조율되고 은밀하게 이루어집니다.

애플리케이션 레이어 DDoS 공격의 복잡성이 증가한 만큼, 이전보다 더 종합적인 방어 전략을 세우는 것이 도움이 됩니다. 예전에는 자체적으로 구축된 WAAP(Web Application and API Protection)를 비롯한 모든 WAAP가 사용자의 요구사항을 충족할 수 있었습니다. 이제 WAAP는 현재 발생하는 애플리케이션 레이어 공격의 복잡성을 뛰어넘어야 합니다.

애플리케이션 레이어 DDoS 방어에 대한 종합적인 접근 방식

애플리케이션 레이어 DDoS 공격을 탐지하기 어려운 이유는 다중 기법 공격에 명백한 패턴이 포함되어 있어도 강력한 동기를 가진 공격자가 공격 응답을 모니터링하고 이를 수정해 방어자를 회피하기 때문입니다. 이 문제를 보다 일관되고 정확하게 해결하려면 WAAP의 탐지, 방어, 셀프 서비스 기능을 전반적으로 개선해야 합니다.

궁극적으로 WAAP가 현관문을 지키는 것만으로는 부족합니다. 모든 진입 지점을 방어하고, 손님으로 위장한 공격자를 식별하는 방법을 이해하고, 한 번에 여러 공격을 받는 경우 확장이 가능해야 합니다. 다행인 점은, 올바른 플랫폼을 도입함으로써 애플리케이션 레이어 DDoS의 혼란을 방어하고 평소와 같이 비즈니스를 계속할 수 있다는 사실입니다. DDoS 방어 전략은 보다 종합적인 전략이 되어야 하며 다음에 중점을 두어야 합니다.

플랫폼의 확장성

WAAP가 일상적으로 아무리 잘 작동하더라도 증폭 공격을 흡수할 수 있도록 확장할 수 없다면 금세 실패하게 됩니다. 따라서 WAAP 아래의 플랫폼 역시 WAAP만큼이나 중요합니다. 또한 플랫폼이 실행되는 위치도 중요합니다. 예컨대 Akamai는 전 세계에 엣지를 보유하고 있으며, 종종 공격이 발생하는 지역에도 엣지를 보유하고 있습니다. 공격이 시작된 곳에서 공격을 방어할 수 있다면 DDoS 공격을 훨씬 쉽게 막을 수 있습니다. 또한 확장성을 바탕으로 전송률 제한과 맞춤형 룰 같은 필수적인 운영이 훨씬 쉬워집니다.

보호 상태를 알려주는 데이터 리소스 및 아웃풋

모든 WAAP가 트래픽을 모니터링하고 생성된 데이터를 보고할 수 있지만, 글로벌 관점에서 데이터를 집계할 수 있는 솔루션을 고려하는 것이 좋습니다. 솔루션 공급업체가 수천 개의 기업에서 발생하는 트래픽에 대한 가시성을 확보하면 동일한 위협에 직면한 기업 간에 생성된 데이터를 맥락화할 수 있으며, 솔루션에 구축된 머신 러닝 시스템에 더 나은 정보를 제공할 수 있습니다. 그런 다음 내부 팀에서 이 데이터를 소싱해 솔루션에 적용하고 맞춤화하기 위해 사용할 수 있습니다.

솔루션의 가시성 및 정확성

수신 클라이언트 트래픽을 넘어 오리진 연결 속도와 서버 성능 매개변수에 초점을 맞춘 행동 및 이상 기반의 탐지 방법이 기본적으로 제공되어야 합니다. 하지만 강력한 데이터 세트에 기반한 확장 가능한 솔루션이 있다면 WAAP의 타기팅과 정확도가 훨씬 더 높아질 것입니다. 또한 적응형 솔루션을 활용하면 인터넷의 개방형 프록시 뒤에 숨어 있는 공격처럼 공격이 숨어 있는지 파악할 수 있으므로 트래픽에서 발생하는 상황을 더 자세히 이해할 수 있습니다. 이 모든 기능을 통해 오탐률을 대폭 줄이면서 적절한 사람에게 알림을 보낼 수 있습니다.

이러한 장점을 모두 결합하는 동시에 원활하게 진행되는 파티를 계획하고 있다면 초대받지 않은 손님들도 추가로 수용할 수 있을 만큼 확장 가능한 충분히 큰 집이 있어야 합니다. 이전에 좋지 않은 파티를 경험한 사람들(데이터 리소스)과 이야기해 어떤 보호 조치를 취해야 할지도 미리 알아야 합니다. 또한 손님 명단을 미리 공유하고 손님이 방문하기 전에 모든 손님과 인사를 나눔으로써(가시성 및 정확성) 모두가 안전하도록 만들 수 있습니다.

이 모든 걸 직접 하기 어렵다면 신뢰할 수 있는 누군가를 고용해 일을 대신 하도록 할 수 있습니다. 매니지드 서비스는 일반 손님과 악성 손님을 구분하기 위해 주의를 기울여야 하는 모든 신호를 모니터링할 수 있습니다. 또한, 점점 더 빈번해지고 탐지하기 어려워지는 공격을 막기 위해 직원들이 시간에 쫓기면서 시간과 전문 지식을 투입해야 하는 스트레스를 덜 수 있습니다.

애플리케이션 레이어 DDoS에 대한 논의는 애플리케이션 레이어의 일부로 자연스럽게 발생하는 변수와 취약점으로 가득 차 있습니다. 애플리케이션 레이어 DDoS 공격은 기업에 막대한 피해를 줄 수 있기 때문에 매우 신중하게 논의해야 합니다. 하지만 전략적이고 확장 가능한 데이터 중심의 솔루션으로 이러한 종류의 공격을 어렵지 않게 확실히 방어할 수 있습니다.

Akamai가 레이어 7 DDoS 방어를 통해 고객을 지원하는 방법에 대해 자세히 알아보세요.