Cloudflare로 DDoS 보호

현대 DDoS 공격의 진화

2016
1Tbps
IoT 봇넷 계층 7 공격

Mirai IoT 봇넷을 사용한 사상 최대 규모의 계층 7 공격 발생 공격은 입체적이었으며 서버 리소스를 활용

2014
400Gbps
NTP 증폭 공격

단 87Mbps의 원본 서버로부터 공격을 증폭하기 위해 4,529개의 NTP 서버가 사용된 공격

2013
120Gbps
계층 3/4 DDoS 공격

Spamhaus 공격은 당시 최대 규모의 공격 중 하나로 여겨졌으며, '인터넷을 거의 마비시킨 공격'이라고 불림

DDoS(분산 서비스 거부) 공격은 점점 증가하고 있으며, 조직에 대한 복잡하고 대응하기 힘든 보안 위험으로 발전했습니다. DDoS 공격이 최근 시작된 현상은 아니지만, 이러한 공격을 실행하고 위장하는 데 사용되는 방법과 리소스가 급격히 발전해 왔습니다. DDoS 공격이 진화하는 데 결정적인 계기가 된 것은 Mirai 봇넷의 형성입니다. 이 봇넷은 현재 알려진 최대 규모의 DDoS 공격을 만들어내는 데 사용된 300,000개 이상의 해킹된 IoT 장치로 구성되었으며, 최대 공격 트래픽 처리량은 1Tbps가 넘습니다. 이러한 규모의 공격은 새로운 표준이 되어가고 있습니다.

DDoS 공격은 단발성 공격에 그치지 않는 경우가 많고, 피해자는 대개 일 년에 여러 차례 공격 대상이 됩니다. Cloudflare의 경험으로 미루어 볼 때 크고 작은 모든 조직이 대상이 될 수 있습니다. 대다수의 사법당국에서 법률을 통해 DDOS 공격을 불법으로 규정하고 있음에도 여러 DDOS 서비스(DDOS-as-a-Service) 공급자가 구독을 제공하고 있으며, 일부 공급자는 월 최저 5~10달러부터 시작합니다.

매출 손실은 이러한 공격이 웹 사이트나 비즈니스에 미칠 수 있는 다양한 위협 중 하나에 불과합니다. 심지어 Amazon의 웹 사이트(2015년 기준 990억 달러 규모의 매출액)도 과거에 알 수 없는 이유로 여러 번 다운된 적이 있습니다. 예를 들어 2013년에 Amazon.com이 약 15~45분 동안 다운되었을 때는 180~530만 달러의 매출 손실을 보았습니다(11만 7,882달러의 분당 평균 매출액 기준). 그뿐만 아니라, 사이트 액세스 차단과 같은 문제는 브랜드 평판 악화와 고객 만족도 저하 등 정량화하기 어려운 손실도 뒤따르게 됩니다.

확장성 있고 정확한 DDoS 솔루션

Cloudflare의 10Tbps 전역 Anycast™ 네트워크는 역대 최대 규모의 DDoS 공격보다 10배 큰 규모로, 엄청난 규모의 최신 DDoS 공격으로부터 Cloudflare 네트워크 상의 모든 인터넷 자산을 보호해 줍니다. Cloudflare의 계층 3, 4, 7용 DDoS 보호는 네트워크 에지에서 현대의 대규모 위협으로부터 서버를 보호하는 서비스로 활용할 수 있으며, 모든 형태와 규모의 DDoS 공격을 완화하는 데 사용할 수 있습니다. 속도 제한은 응용 프로그램 계층에 대한 가장 정교한 공격을 정확하게 완화할 수 있게 해줌으로써 Cloudflare의 DDoS 보호를 강화합니다.

계층 3 및 4 DDoS 공격으로부터 보호

계층 3 및 계층 4 DDoS 공격은 일반적으로 DDoS 증폭, DDoS 폭주, DDoS SYN 폭주 공격과 같은 입체적인 공격입니다. 이러한 공격은 일반적인 유니캐스트 기반 네트워크를 압도할 수 있지만, Cloudflare의 Anycast 기반 네트워크는 102개가 넘는 Cloudflare 데이터 센터 및 다른 네트워크와의 다양한 고대역폭 연결로 공격 트래픽을 분산함으로써 기본적으로 공격 표면을 늘려 공격 트래픽을 거뜬히 흡수합니다.

DDoS 보호 기능

- 계층 3, 4, 7 DDoS 보호
- DNS 공격 보호
- 속도 제한을 통해 세분화된 위협 차단
- IP 평판 데이터베이스로 예측 보안

"API와 게이트웨이 서버에 대한 DDoS 공격을 걱정하는 대신 안심하고 제품 개선에 집중할 수 있습니다."

-Jake Heinz, Discord
소프트웨어 엔지니어

Cloudflare의 네트워크

- 102개가 넘는 데이터 센터의 전역 Anycast™ 네트워크
- 입체적 공격을 흡수할 수 있는 10Tbps의 처리량
- 인터넷 속성 600만 개
- 고정 대역폭 가격

"Cloudflare를 사용하는 이유는 보안 기능이 뛰어나고, CDN 성능이 우수하며, 이러한 솔루션이 하나의 패키지에 포함되어 편리하게 사용할 수 있다는 점입니다. 그래서 모든 것을 쉽게 관리할 수 있고 핵심 비즈니스에 초점을 맞출 수 있습니다."

-Amanda Kleha GM, Zendesk
온라인 사업부

계층 7 응용 프로그램 취약성으로부터 보호

계층 7 공격의 일반적인 유형에는 SQL 삽입과 XSS(교차 사이트 스크립팅)가 포함되며, 이러한 공격을 통해 공격자는 고객 또는 다른 모든 종류의 응용 프로그램 데이터에 액세스하여 성능을 저해할 수 있습니다. Cloudflare는 WAF(웹 응용 프로그램 방화벽)를 통해 이러한 위협을 처리합니다. WAF에서는 OWASP의 상위 10개 규칙 집합, Cloudflare의 응용 프로그램 규칙 집합, 커뮤니티/고객이 만든 사용자 지정 규칙에서 발견된 위협을 자동으로 차단합니다. Cloudflare는 Shellshock 취약성과 Heartbleed 버그를 비롯한 주요 제로 데이 취약성으로부터 고객을 보호할 수 있었습니다.

속도 제한

세분화된 트래픽 제어가 가능한 Cloudflare 속도 제한을 활성화하여 Cloudflare의 DDoS 보호와 WAF(웹 응용 프로그램 방화벽) 서비스를 보완하세요. 속도 제한은 서비스 거부 공격, 무차별 암호 대입 시도 및 응용 프로그램 계층을 대상으로 하는 기타 악의적인 동작으로부터 지켜줍니다. 요청 임계값을 구성하고, 완화 조치(챌린지 또는 CAPTCHA)나 응답 코드와 같은 사용자 지정 대응을 정의하고, 웹 사이트, 응용 프로그램 또는 API의 끝점에 대한 분석 자료를 확인해 보세요.

예측 보안

Cloudflare는 네트워크 트래픽이 실시간으로 분석되어 비정상적이거나 악의적인 요청을 식별하는 자동 학습 플랫폼을 제공합니다. 새로운 공격이 확인되면 Cloudflare는 특정 웹 사이트와 전체 커뮤니티에 대해 해당 공격 유형을 자동으로 차단하기 시작합니다. Cloudflare가 네트워크와 커뮤니티를 계속 확장해갈수록 Cloudflare 사용자에 대해 효과적인 DDoS 공격을 실행하는 것은 점점 더 어려워집니다.

고정 대역폭 가격

Cloudflare는 엔터프라이즈급 DDoS 보호를 고정된 월간 요금으로 무제한 제공합니다. Cloudflare는 DDoS 공격과 관련된 네트워크 트래픽의 급증에 따른 비용을 고객이 부담해서는 안 된다고 생각합니다. Cloudflare DDoS 보호 솔루션을 사용하는 고객은 웹 사이트가 온라인 상태를 유지하고 예측 가능한 월간 요금을 지불할 것이라는 확신을 가질 수 있습니다.

Cloudflare 등록

Cloudflare에 등록하고 속도 제한을 활성화하여 DDoS 공격으로부터 웹 사이트, 응용 프로그램 또는 API를 보호하는 동시에, 대기 시간을 줄이고 최신 웹 기술을 활용해 보세요. 간편하게 설정할 수 있으며 실행되기까지 5분도 걸리지 않습니다. www.cloudflare.com에서 무료 버전부터 엔터프라이즈 버전까지 여러 요금제를 확인해 보세요.