Akamai

사이버 보안 셰프:

레이어 7 DDoS 안정성을 위한 최고의 요리책 만들기

목차

서론

오늘날의 분산 서비스 거부(DDoS) 공격에 대한 적절한 방어 전략을 구축하는 것은 보안 전문가들 중에서도 가장 경험이 많은 사람조차도 쉽지 않은 도전 과제입니다. 특히 추가적인 문제가 발생하는 레이어 7 DDoS 공격에서는 더 어렵습니다. 한 가지 유용한 방법으로 다양한 위협에 대한 다양한 접근 방식이 포함된 단계별 지침, 즉 레이어 7 DDoS 요리책이 도움이 될 수 있습니다.

공격자마다 DDoS 공격을 준비하는 방식이 다를 것입니다. 레이어 3 및 4 공격은 힘을 변수로 하는 함수라 할 수 있습니다. 즉 공격자와 방어자 중 누가 더 많은 네트워크 용량을 가지고 있는지가 중요합니다. 반면 레이어 7 공격은 OSI(Open Systems Interconnection) 모델의 애플리케이션 레이어를 표적으로 합니다. 이 애플리케이션 레이어는 소프트웨어 애플리케이션과 직접 상호 작용하는 역할을 합니다. 공격자는 이러한 시스템의 용량, 메모리 할당 또는 요청 처리 방식의 약점을 악용해 웹 서버, 데이터베이스 또는 애플리케이션을 압도하는 것을 목표로 합니다.

따라서 레이어 7 DDoS 공격은 정상적인 트래픽으로 보이는 경우가 많아 정상 사용자에게 영향을 주지 않으면서 악성 요청을 필터링하기가 어렵기 때문에 방어하기가 특히 어렵습니다. 또한, 자동화 및 클라우드 리소스를 사용하게 되면서 공격자들이 이러한 공격을 빠르고 대규모로 실행하는 것이 더욱 쉬워졌습니다.

이 백서에서는 공격자가 사용하는 툴과 기법, 공격자를 막는 탐지 및 방어 기법, 이벤트 사후 분석 및 복구 제안 등이 들어간 자세한 레시피를 통해 레이어 7 DDoS 공격 방어의 도전 과제를 다룹니다.

Akamai는 콘텐츠 전송, 사이버 보안, 전 세계적으로 4200개 이상의 네트워크 거점이 있는 분산형 클라우드 플랫폼에 다양한 경험을 가지고 있으며, 이를 바탕으로 오늘날의 DDoS 공격을 독자적인 관점으로 바라봅니다. 애플리케이션 레이어 DDoS 공격이 갈수록 복잡해지고 다면적으로 진행됨에 따라 이러한 관점과 철저한 방어 전략을 갖추는 것이 중요합니다. 그리고 Akamai는 이를 실현합니다.

특정 위협이나 취약점에 대한 도움을 찾고 있는 일선 보안 전문가나 보안 체계를 개선하고자 하는 CISO에게 이 요리책은 성공의 비결을 제공합니다.

레이어 7 DDoS 공격의 일반적인 표적 및 사례

레이어 7 DDoS 공격은 OSI 모델의 상위 레이어, 즉 애플리케이션 레이어를 표적으로 합니다. 이러한 공격은 웹 애플리케이션이 요청을 처리하는 방식을 악용하여 표적 리소스를 압도하는 것을 목표로 합니다. 레이어 7 DDoS 공격의 일반적인 표적은 다음과 같습니다.

웹 서버: 공격자는 웹 서버를 표적으로 삼아 정상 사용자에게 콘텐츠를 전송하는 것을 방해합니다. 이로 인해 웹 사이트가 느리게 로딩되거나 완전히 접속할 수 없게 될 수 있습니다.

웹 애플리케이션: 데이터베이스 또는 백엔드 서비스에 의존하는 애플리케이션은 레이어 7 DDoS 공격에 취약합니다. 공격이 애플리케이션 쿼리 구문 분석, 프로세스 요청 또는 세션 관리 방식의 약점을 악용할 수 있기 때문입니다.

애플리케이션 프로그래밍 인터페이스(API): API는 최신 웹 서비스 및 모바일 애플리케이션의 중요한 구성요소입니다. 공격자들은 API를 표적으로 여러 소프트웨어 서비스 간의 상호 작용을 방해하여 해당 API를 사용하는 애플리케이션의 기능에 영향을 미칩니다.

DNS 서비스: DNS 공격은 다른 레이어에서도 발생할 수 있지만, 레이어 7 공격은 도메인 이름 레졸루션을 방해하는 악성 요청으로 DNS 서비스를 폭격해 대규모 접속 문제를 일으킬 수 있습니다. DNS over HTTP/TLS 도입이 증가함에 따라 이러한 공격이 증가할 가능성이 있습니다.

이메일 서버: 이메일 서버를 표적으로 삼으면 통신을 방해하여 인바운드 및 아웃바운드 이메일 모두에 영향을 미칠 수 있습니다.

결제 게이트웨이 및 금융 서비스: 이는 거래를 방해하고 금융 서비스 운영 과정에 혼돈을 일으키고자 하는 공격자에게 매력적인 표적입니다.

Akamai의 인터넷 보안 현황(SOTI) 보고서와 보안 인사이트는 레이어 7 DDoS 공격의 진화하는 환경을 정기적으로 조사해 공격 기법의 다양성과 가장 위험한 업계를 조명합니다.

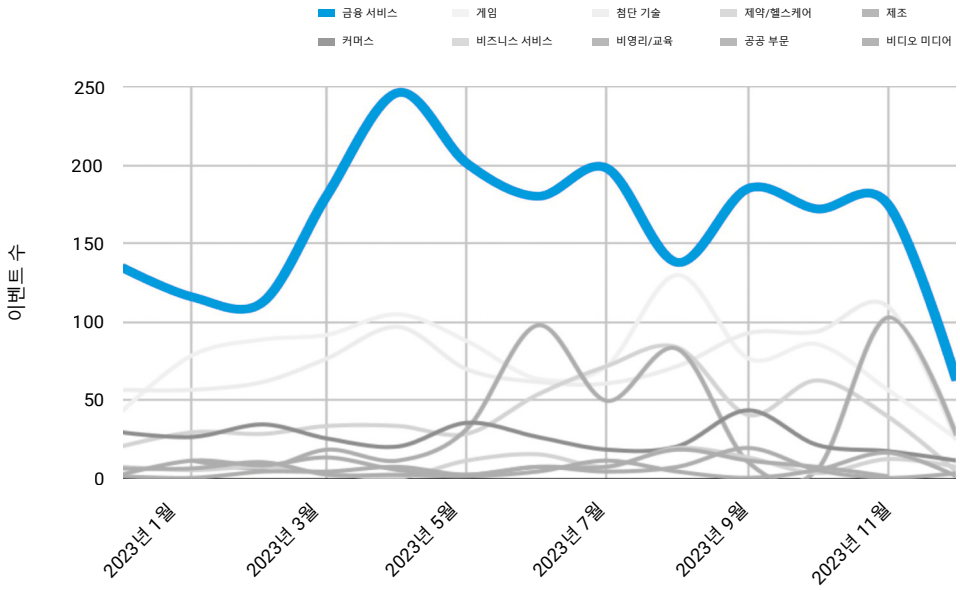
공격 기법

- 웹 애플리케이션 및 API 공격: 공격자는 일반적으로 콘텐츠나 설정으로 인해 일반적으로 캐싱되지 않는 API 엔드포인트를 포함한 웹사이트 엔트리 포인트를 표적으로 삼습니다. 일반적으로 확인되는 표적 경로에는 '/', '/home', '/en-us', '/pricing/' 등이 있습니다.
- 흔하게 볼 수 있는 공격 기법은 다음과 같습니다.
  - 홈페이지의 HTTP GET/POST 플러드
  - 무작위 경로 및 쿼리 문자열에 대한 HTTPS GET 플러드
  - 느린 읽기 공격
  - 대용량 파일 업로드 플러드

DDoS 공격을 받는 기업의 수는 해마다 증가해왔고 이제는 공격 방법도 변화하고 있습니다. 첫째, 공격을 받는 자산의 종류와 규모가 달라졌습니다. 예를 들어, 동일하거나 유사한 엔드포인트에 대한 10건의 공격 대신 네트워크 공간에서 서로 다른 IP를 겨냥한 100건의 공격이 발생할 수 있습니다. 이러한 공격은 레이어 3뿐만 아니라 레이어 7도 동시에 표적으로 삼습니다.

공격 대상 업계

금융 서비스, 도박, 제조 부문에 대한 분산 서비스 거부(DDoS) 공격 이벤트는 2023년에 증가했으며, 특히 EMEA 지역에서 다른 모든 지역의 공격 건수를 합친 것보다 더 많이 발생했습니다.

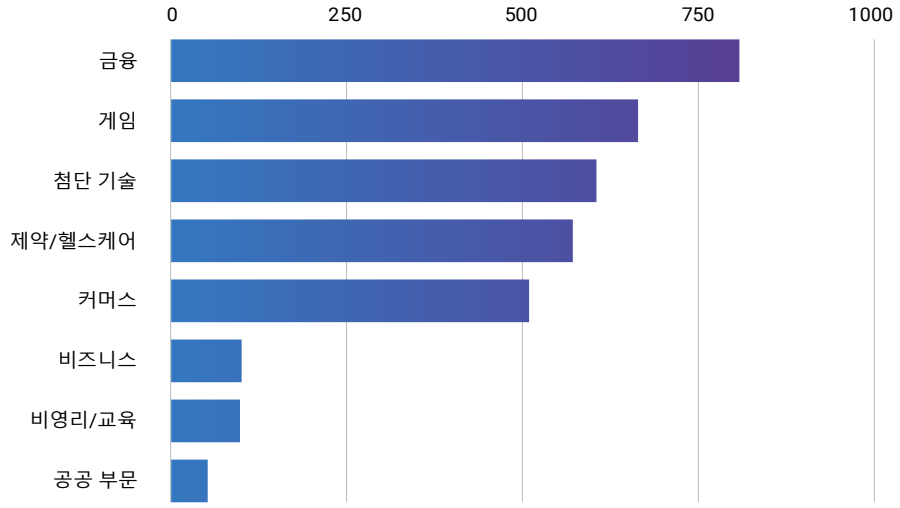


DDoS: Here to Stay, 2024년 3월

특히 금융 서비스는 레이어 7 DDoS 공격의 표적으로 점점 더 큰 주목을 받고 있습니다. Akamai는 2021년 이후 금융 서비스 기업을 겨냥한 DDoS 공격이 뚜렷하고 눈에 띄게 급증한 것으로 파악했습니다. 2023년 전체 업계에 대한 공격 중 3분의 1 이상(35%)이 금융 서비스 기관에 대한 공격이었으며, 이 분야는 게임 분야보다 더 매력적인 표적이 되었습니다. Akamai의 분석에 따르면 전 세계적으로 DDoS 공격의 63%가 은행을 표적으로 삼은 것으로 나타났습니다. EMEA 지역에서는 약 3분의 1(72%), APAC 지역에서는 91%의 공격이 은행에 초점을 맞추고 있었습니다. 그러나 미주 지역에서는 은행, 보험, 기타 금융 서비스 기관으로 DDoS 공격이 보다 고르게 확산되는 경향을 보였습니다.

미주 지역: DDoS 공격의 28%가 금융 서비스 분야에서 발생

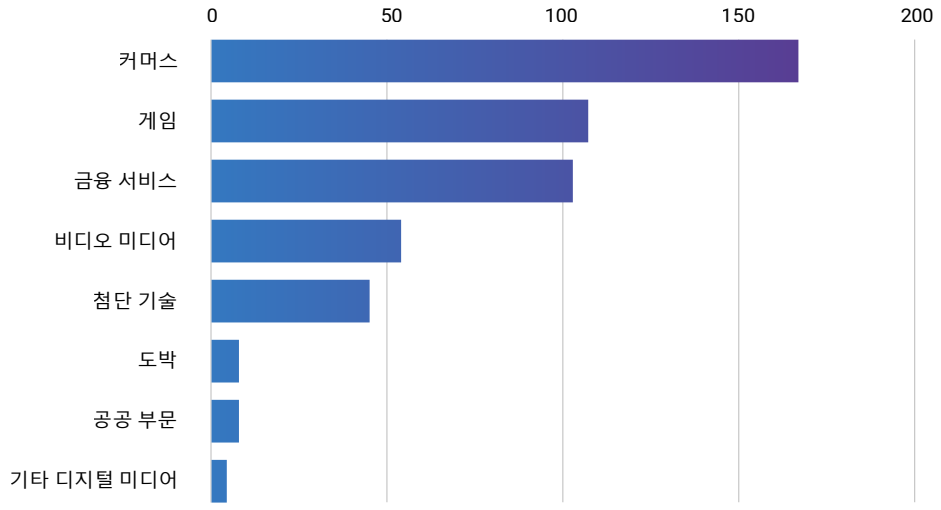
2023년 6월~2023년 12월



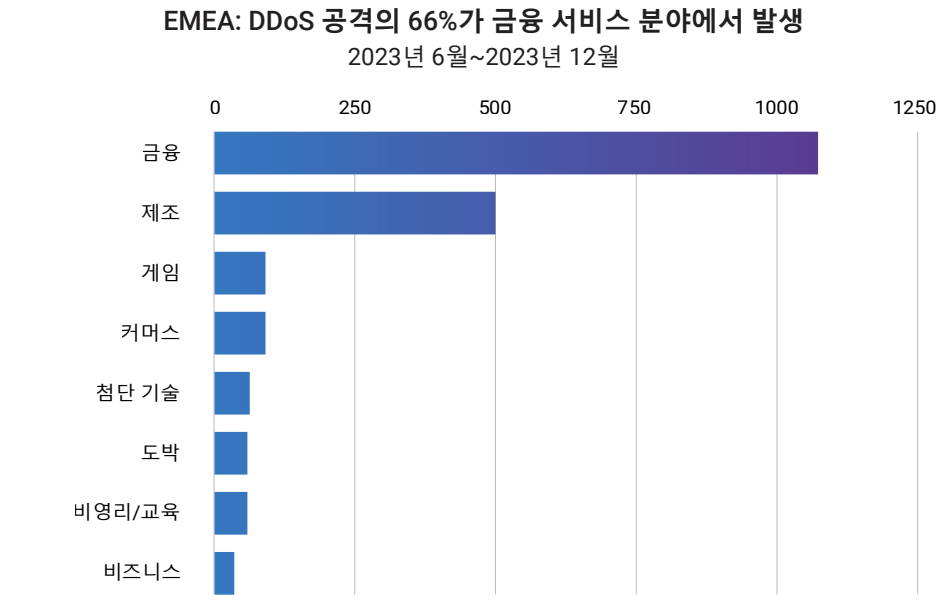
DDoS: Here to Stay, 2024년 3월

APAC: DDoS 공격의 11%가 금융 서비스 분야에서 발생

2023년 6월~2023년 12월



DDoS: Here to Stay, 2024년 3월



DDoS: Here to Stay, 2024년 3월

최근 Akamai의 금융 서비스 고객 한 곳을 대상으로 정교한 레이어 7 DDoS 공격이 발생했습니다. 이 사례에서 사이버 공격자는 자동화 기술을 사용해 고도로 분산된 공격을 일으켰습니다. 이 공격에서는 HTTP GET 플러드를 사용하여 주로 캐싱할 수 없는 URL(예: 홈페이지, 로그인 엔드포인트 등)을 표적으로 공격을 가했습니다. 이 공격은 다양한 사전 예방적 제어를 활용해 고객 오리진에 아무런 영향을 끼치지 않고 성공적으로 방어되었습니다. 이 공격 소스 히트 맵은 클라우드 서비스 사업자, Tor 출구 노드, 익명 또는 개방형 프록시 노드의 사용이 증가하고 있음을 시사합니다.

자율 시스템을 통한 DDoS 공격

2024년 1분기에 금융 기관을 표적으로 100여 개 국가에서 발생한 애플리케이션 레이어 공격을 시각화한 것으로 Akamai가 공격 방어를 지원했습니다

DDoS 공격자들은 전 세계 여러 국가와 지역에 걸쳐 있는 광범위한 네트워크를 통해 동적 IP 주소를 활용하여 광범위하게 분산된 공격 인프라를 구성 및 조정할 수 있습니다.

Akamai

최신 DDoS 공격 레시피의 재료

공격자들이 사용하는 툴 및 기법

불행하게도 DDoS 공격자와 이들이 사용하는 방법은 계속 진화합니다. 공격자들은 자신들의 행위로 수익화할 수 있는 방법을 계속 찾으면서 기술을 조정하고 새로운 툴을 활용하며 새로운 방법을 찾아냅니다. 이러한 진화를 보여주는 여러 가지 요인이 있습니다.

자동화: 공격자는 정상 사용자의 행동을 모방하는 자동화된 스크립트와 봇을 사용하여 탐지를 훨씬 더 어렵게 만들고 있습니다. 또한, 공격자들은 기존의 탐지에 적응하고 우회하는 머신 러닝 알고리즘을 시도하고 있습니다.

멀티기법 공격: 공격자들은 네트워크 및 애플리케이션 리소스를 압도하기 위해 다양한 공격 종류(GET 및 POST 플러드)와 DNS 표적(증폭 및 프래그먼트 공격)을 다른 조합과 결합하는 멀티기법 전략을 점점 더 많이 사용하고 있습니다.

API 타게팅: API에 의존하여 애플리케이션을 구동하는 기업이 늘어남에 따라 공격자들은 API 취약점을 악용하여 DDoS 공격에서 새로운 기회를 찾아내고 있습니다. 이러한 공격은 수천 개의 연결을 동시에 요청함으로써 서버 리소스를 고갈시키거나 로직 취약점을 악용하여 서비스 중단을 야기하는 것을 목표로 합니다.

IoT 디바이스 악용: 보안이 취약한 IoT 디바이스가 확산됨에 따라 봇넷은 수많은 병사들을 얻게 되었습니다. 이러한 디바이스는 종종 탈취되어 네트워크 연결과 연산 능력을 악용해 대규모 DDoS 공격을 실행하는 데 사용됩니다.

더 정교해지는 공격

이러한 새로운 툴과 기법이 등장함에 따라 DDoS 공격의 복잡성과 빈도가 증가하고 있으며, 공격자들은 정교한 방법을 사용하여 기존의 방어 체계를 우회하고 있습니다. 몇 가지 주목할 만한 트렌드를 소개하자면 다음과 같습니다.

암호화: 공격이 HTTPS 기반 DDoS 공격으로 전환됨에 따라 방어가 더 어려워졌습니다. 이러한 공격은 암호화되어 정상적인 트래픽으로 위장하기 때문에 탐지 및 필터링이 더 어려워졌으며, 기존의 DDoS 방어 조치로는 애플리케이션 레이어 SSL/TLS 트래픽을 해독하는 데 한계가 있습니다.

봇넷 및 프록시: DDoS 봇넷이 크게 증가하고 공격자들이 익명의 프록시를 빈번하게 사용함에 따라 이제는 다수의 IP 주소(일반적으로 공격당 IP 1만개 이상)에서 요청이 전송됩니다. 공격자는 이러한 전략을 사용해 단일 IP에서 발생하는 요청 수를 확인하는 방어 조치를 우회할 수 있습니다. 클라우드 호스팅 플랫폼의 보급과 클라우드 기반 서비스의 도입으로 인해 이러한 고강도 분산형 공격이 더욱 쉬워지고 있습니다.

자율 시스템을 통한 DDoS 공격

최근 Akamai 금융 고객을 대상으로 발생한 애플리케이션 레이어 DDoS 공격 (초당 65만 TPS, 20Gbps, 총 90억 건 이상의 요청)의 시각화

DDoS 공격자들은 고도로 분산된 공격 인프라를 구축하고 조정할 수 있으며, 대부분 클라우드 공급업체를 활용합니다.

방어자가 도입하는 발전된 접근 방식 중 하나는 암호 종류 및 순서 등 다중 TLS 레이어 신호로 구성된 TLS 핑거프린트당 요청을 추적하는 것입니다. 이러한 접근 방식은 오탐이 발생하기 쉽지만, 공격자가 다양한 머신과 IP에서 활동하는 경우 감염된 디바이스에 동일한 소프트웨어가 설치되어 있기 때문에 올바르게 사용하면 보다 효과적인 방어 기능을 제공할 수 있습니다. 이러한 디바이스는 유사한 환경 특성을 보이며, 그 중 하나는 공유된 TLS 라이브러리입니다.

재료 공급

시중에 나와 있는 툴은 자주 바뀌지만, 공격 기법이 진화한다는 것은 더 정교하고 탐지가 어려운 방법으로 발전하고 있다는 의미입니다. 여기에는 다음이 포함됩니다.

- **감염된 IoT 디바이스:** 공격자들은 봇넷에서 감염된 IoT 디바이스를 대규모 DDoS 공격의 수단으로 계속 사용하고 있으며, 이러한 디바이스의 취약점이 지속적으로 부각되고 있습니다.
- **DDoS 공격 대행 서비스:** DDoS 공격 대행 서비스의 등장으로 공격 시작의 진입 장벽이 낮아져 방대한 기술 지식이 없는 개인도 상당한 규모의 공격을 수행할 수 있게 되었습니다.

- **회피 기법:** 무작위 헤더 매개변수와 동적 요청 인수 등 고급 회피 기법이 보편화되었습니다. 이러한 기법은 악의적인 트래픽을 정상적인 요청과 구별하기 어렵게 만들어 기존의 탐지 및 방어 접근 방식에 어려움을 안겨줍니다.

이러한 공격에서 일반적으로 악용되는 취약점

공격자가 레이어 7 DDoS 공격에서 악용하는 취약점은 웹 애플리케이션이 사용자 인풋을 처리하고 데이터를 관리하는 방법과 관련이 있는 경우가 많습니다. 이러한 취약점을 방어하기 위해서는 보안 조치를 함께 사용하는 것이 중요합니다.

최근 몇 년 동안 공격자들이 애플리케이션 레이어 DDoS 공격을 수행할 때 악용한 가장 중요한 취약점 중 하나는 2023년 말에 널리 공개된 HTTP/2 Rapid Reset 취약점입니다. 이들 공격에서 인터넷 및 모든 웹사이트 운영에 필수적인 HTTP/2 프로토콜의 취약점이 악용되었습니다. 이 취약점을 악용한 공격으로 인해 분기 내 HTTP DDoS 공격 트래픽이 전 분기 대비 65% 증가했으며, 이는 이 취약점을 이용한 공격의 심각성과 영향력의 규모를 보여줍니다.

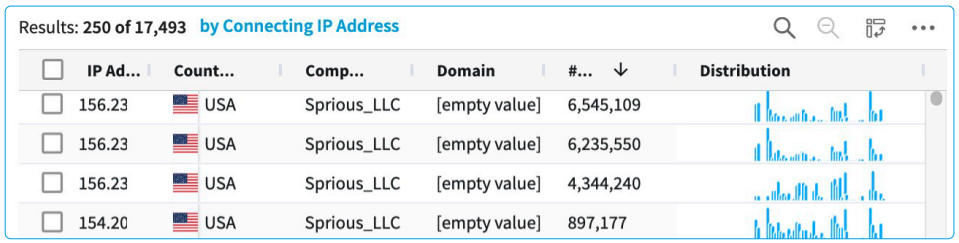
이 특정 취약점을 사용한 공격자는 클라우드 컴퓨팅 플랫폼과 HTTP/2를 악용하여 상대적으로 작은 봇넷으로 초증폭 DDoS 공격을 수행할 수 있었으며, 그 영향은 막대했습니다. 이러한 공격의 주요 표적은 게임, IT, 암호화폐, 컴퓨터 소프트웨어, 통신 업계였으며, 미국, 중국, 브라질, 독일, 인도네시아가 이 공격의 가장 큰 발생 국가였습니다.

이에 대응해 업계 전반의 공동 노력으로 HTTP/2 Rapid Reset 취약점(CVE-2023-44487)이 공개되어 이 취약점을 이용한 DDoS 공격이 명확히 밝혀졌습니다. 이러한 노력은 선도적인 클라우드 및 CDN 서비스 공급업체를 비롯한 다양한 공급업체를 대상으로 이루어졌습니다.

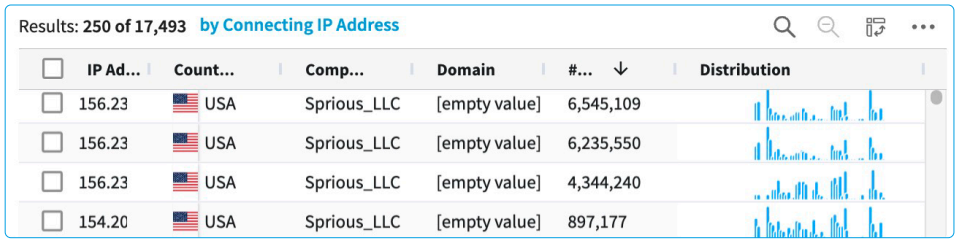
실제 사례: DDoS 공격에 자동화 사용

공격자들은 동일한 디도스 공격을 수행하기 위해 다양한 DDoS 툴을 사용하는 경우가 많습니다. 각 툴은 여러 가지 기법을 서로 결합하여 보안 제품을 우회하거나 최소한 그 효용성을 줄이기 위해 사용됩니다. 아래는 Akamai Web Security Analytics를 사용하여 분석한 한 공격의 사례입니다.

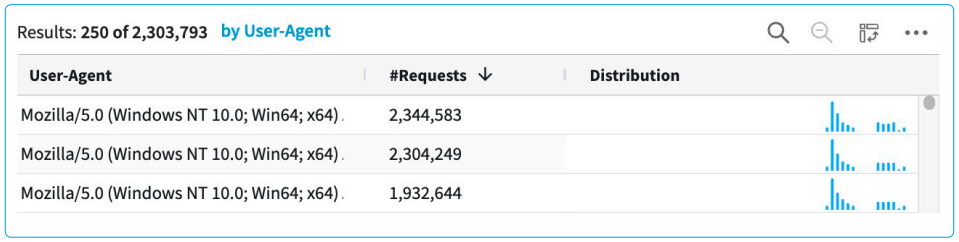
- 1만 7000개 이상의 IP 주소에서 관측된 공격



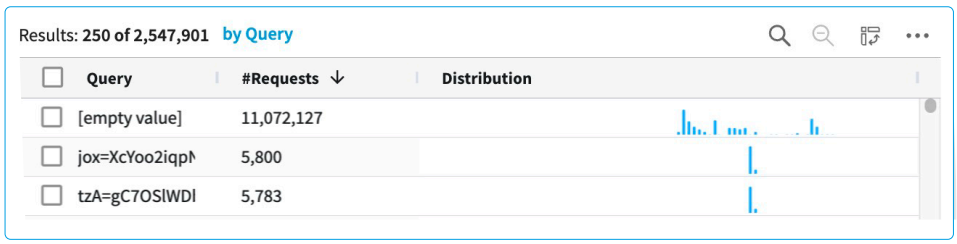
- 400개 이상의 네트워크에서 발원한 공격 소스



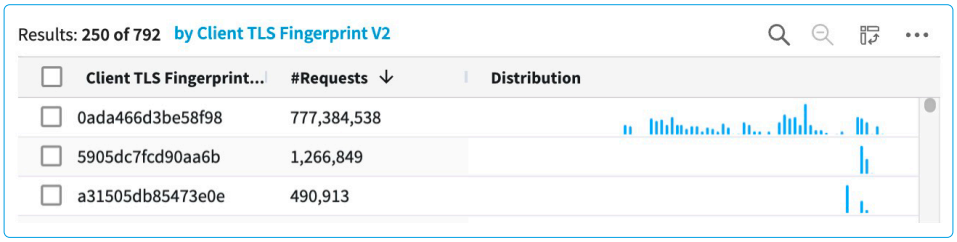
- 230만 3793개의 고유 사용자 에이전트



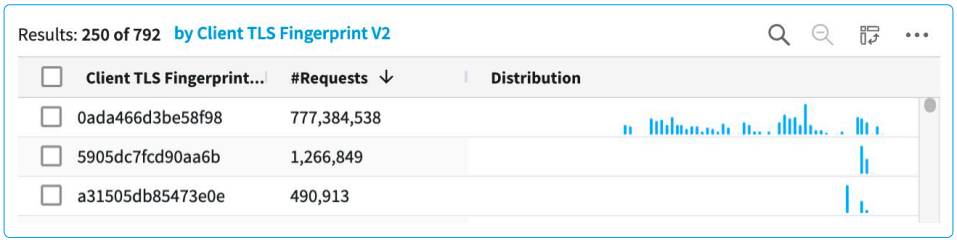
- 254만 7901개의 고유 및 무작위 쿼리 문자열



- HTTP 헤더 회전(예: Accept-Language, Referer)



- TLS 설정 회전



이러한 정교한 공격을 방어하려면 레이어화된 보안 전략이 필요합니다. 전송률 제한에서 요청 일치와 소스 트래픽 특성의 고급 조합, 소스 평판 제어와 같은 사전 예방적 및 사후 대응적 제어를 모두 사용하는 것이 도움이 될 수 있습니다.

공격자 수준 상승: TLS 신호 사칭

최근 관찰에 따르면 악의적인 공격자들은 정상적인 Chrome 브라우저에서 연결되는 것처럼 보이게 해 탐지를 회피하기 위해 DDoS 툴에서 TLS 신호를 더 자주 사용하는 것으로 나타났습니다. 공격자들은 공격 속도가 느려질 수 있는 리소스 집약적인 헤드리스 버전의 Chrome을 사용하는 대신 수정된 버전의 TLS 라이브러리를 사용해 모든 정품 브라우저의 TLS 신호를 설정하고 사칭할 수 있습니다. TLS 핑거프린팅을 복제하기 위해 설계된 툴이 있지만 DDoS 공격 툴에서는 흔히 찾아볼 수 없습니다. 이러한 종류의 공격을 사용하는 것은 공격자의 기술적 능력과 방어 체계에 대한 지식이 증가했음을 의미합니다. 따라서 레이어 7 DDoS 공격 방어 전략에서는 최신 공격 트렌드에 대한 정기적인 리서치가 필요합니다. 이는 또한 TLS 스푸핑 기능을 갖춘 DDoS 툴의 사용 빈도가 증가하고 있다는 의미이기도 합니다.

방어 레시피 준비하기

살펴보기: 리스크 평가 및 취약점 식별

중요한 자산을 파악하고 자산의 어떤 부분이 DDoS 공격에 취약한지 확인함으로써 레이어 7 DDoS 방어 전략을 크게 개선할 수 있습니다. 이 리스크 평가는 중요성과 취약점에 따라 보호할 리소스의 우선 순위를 정하는 데 도움이 됩니다. 잠재적인 공격 기법과 그 영향을 이해함으로써 기업은 전송률 제한, 웹 애플리케이션 방화벽, 행동 분석 등 구체적인 대응 조치를 구축하여 리스크를 효율적으로 방어할 수 있습니다. 또한 지속적인 리스크 평가를 통해 새로운 위협과 변화하는 비즈니스 요구사항에 맞춰 발전하는 방어 전략을 구현할 수 있습니다.

업계와 기업마다 애플리케이션 레이어 DDoS 리스크 평가에 대한 접근 방식이 다를 수 있습니다. 그 사례는 다음과 같습니다:

> **이커머스:** 대규모 세일 이벤트를 앞두고 리스크 평가에서 결제 프로세스가 중요한 취약점으로 식별될 수 있습니다. 방어 조치에는 서비스 보호를 위한 웹 애플리케이션 방화벽(WAF) 구축 및 전송률 제한 등이 포함될 수 있습니다.
>
> **금융 서비스:** 은행 애플리케이션의 경우 리스크 평가를 통해 로그인 페이지가 DDoS 공격의 주요 표적인지 확인할 수 있습니다. 그다음 은행은 엔드포인트 맞춤형 전송률 제한 및 행동 탐지 기능을 조합하여 정상 사용자와 공격 트래픽을 구분할 수 있습니다.

특정 취약점을 이해하면 공격받는 중 표적화된 방어를 수행하고 중요한 서비스를 강화할 수 있습니다.

사공이 많으면 배가 산으로 간다: 역할 및 책임

명확한 역할과 책임을 설정하는 것은 공격 발생 시 조율되고 효율적인 대응의 기회를 극대화하기 때문에 효과적인 레이어 7 DDoS 전략을 위한 중요한 단계입니다. 명확한 역할이 없으면 대응 노력이 혼란스러워지고 업무가 중복되며 방어에 공백이 생길 수 있습니다. 책임을 정의하면 트래픽 모니터링, 비정상 식별에서 방어 전략 구축, 이해관계자와의 의사 소통까지 각 팀원의 구체적인 작업을 파악하는 데 도움이 됩니다. 이러한 조정을 통해 공격의 영향을 최소화하고, 서비스 가용성을 유지하며, 중요한 자산을 보호할 수 있습니다.

실제로 명확한 역할 없이 의사 결정권자가 너무 많으면 DDoS 공격 시 대응이 지연될 수 있습니다. 예를 들어, 네트워크 운영 본부와 사이버 보안 팀이 서로 협조하지 않고 독립적으로 서로 다른 방어 접근 방식을 선택하면, 의도치 않게 서로의 노력이 상쇄되거나 중요한 취약점을 놓치게 될 수 있습니다. 올바른 전략에는 지정된 인시던트 대응 리더, 커뮤니케이션 코디네이터, 기술 대응팀 등의 역할이 사전 정의되어 있기 때문에 공격에 대한 신속하고 통합된 조치를 보장하고, 다운타임을 최소화하며, 인시던트 후 분석을 간소화할 수 있습니다.

주방을 위한 적절한 툴 선택

애플리케이션 레이어 공격은 정상 트래픽과 악성 트래픽을 구분하기가 매우 어렵기 때문에 탐지 및 방어가 어려울 수 있습니다. 이같이 진화하는 위협에 대응할 수 있도록 Akamai는 방어에 대한 다각적인 접근 방식을 권장합니다.

- **온디맨드가 아닌 상시가동형(always-on)에 초점 맞추기:** 새로운 위협에 신속하게 대응할 수 있도록 DDoS 보안 제어가 항상 활성화되어 있도록 하고 인시던트 대응 계획을 업데이트해야 합니다.
- **안정적이고 신뢰할 수 있는 아키텍처 구축:** 공격자는 일반적으로 DNS, 웹 애플리케이션, API, 데이터 센터 및 네트워크 인프라 등 다수의 서비스를 표적으로 삼기 때문에 단일 장애 지점을 예측해야 합니다. 레이어 7 DDoS 공격을 방어하려면 적절한 아키텍처를 선택하는 것이 매우 중요합니다. 이러한 아키텍처 고려 사항에는 상시가동형 엣지 또는 CDN 기반 DDoS 방어 기능을 선택하는 것이 포함될 수 있습니다. 안정성을 과대평가하지 마세요. 오늘날의 DDoS 공격 규모는 대부분의 인프라를 쉽게 압도할 수 있습니다.
- **공급업체의 SLA를 평가하고** 전략에 맞게 조정해야 합니다.
- **공급업체의 준비 상태를 검토하세요:** 주요 네트워크 구성요소를 정기적으로 검토하고 다양한 DDoS 방어 메커니즘을 평가하여 현재 공격 방식에 대한 효과를 파악하는 공급업체를 선택해야 합니다.
- **DDoS 공격 대응 플레이북을 확인하세요:** IT, 운영, 보안 및 고객 커뮤니케이션 직원들을 한데 모으면 공격 발생에 대비한 준비를 강화할 수 있습니다.
- **긴급 DDoS 방어:** 위기 발생 시 DDoS 방어 솔루션 공급업체를 온보딩할 수 있는 계획을 준비하는 것이 좋습니다. DDoS 방어 벤더사 파트너가 있는 경우 해당 DDoS 지원 핫라인에 연락하세요.

탐지 및 방어 레시피

레이어 7에서 효과적인 DDoS 방어를 가능하게 하려면 다수의 탐지 및 방어 전략이 필요합니다. 적용할 수 있는 몇 가지 방법론이 있으며, 각 방법론에는 강점과 주요 고려 사항이 있습니다.

행동 및 비정상 기반 탐지

장점: 이 접근 방식은 머신 러닝과 통계 분석을 사용하여 일반적인 트래픽 패턴을 파악하고 DDoS 공격을 나타낼 수 있는 편차를 식별합니다. 이 방식은 이전에는 볼 수 없었던 복잡한 공격에 대해 매우 효과적입니다.

고려 사항: 효과적인 탐지를 위해서는 '정상' 트래픽의 기준선을 설정하는 데 최대 몇 주가 소요될 수 있는 학습 기간이 필요하며, 이 기간 동안에는 탐지 효과가 떨어질 수 있습니다. 모델이 정확하게 학습되지 않은 경우 오탐을 반환할 수 있습니다.

전송률 및 처리량 기반 탐지

장점: 구축이 간편한 이 방식은 요청 전송률 및 규모를 모니터링하여 트래픽이 미리 정의된 임계치를 초과할 때 알림 또는 방어 프로세스를 트리거합니다. 이 방식은 대규모의 증폭 공격을 신속하게 확인하는 데 효과적입니다.

고려 사항: 프로모션 이벤트 기간과 같은 정상적인 트래픽 급증을 DDoS 공격으로 오인할 수 있습니다. 레이더에 탐지되지 않는 낮은 규모의 저속 공격은 탐지하지 못할 수 있습니다.

시그니처 기반 탐지

장점: 이 방식은 알려진 공격 패턴 데이터베이스에 트래픽을 대조함으로써 인식된 위협을 신속하게 식별하고 차단할 수 있습니다. 일반적이고 이전에 탐지된 적이 있는 공격 기법에 대해 매우 효과적입니다.

고려 사항: 기존 시그니처와 일치하지 않는 새로운, 또는 개조된 공격을 탐지할 수 없습니다. 효과를 유지하려면 정기적으로 업데이트해야 합니다.

챌린지-응답 테스트

장점: 이 접근 방식은 수신 트래픽이 인간이나 봇에 의해 생성되었는지 확인하기 위해 트래픽에 챌린지를 제시합니다. CAPTCHA 또는 JavaScript 계산은 봇과 자동화된 공격 툴을 효과적으로 방어할 수 있습니다.

고려 사항: 챌린지를 공격적으로 구축하면 사용자 경험이 저해될 수 있습니다. 보다 정교한 봇은 일부 챌린지-응답 테스트를 통과할 수 있기 때문에 챌린지 메커니즘을 정기적으로 업데이트해야 합니다.

하이브리드 접근 방식

여러 탐지 및 방어 전략을 결합하면 보다 포괄적인 보호를 제공할 수 있습니다. 예를 들어, 비정상 기반 탐지 기능을 사용해 잠재적인 공격을 탐지하고, 여기에 전송률 기반 및 시그니처 기반 방법을 추가해 더 넓은 범위를 커버하면 더욱 강력한 방어 메커니즘을 구축할 수 있습니다. 또한 챌린지-응답 테스트를 통해 정상 사용자로부터 정교한 봇을 더욱 효과적으로 걸러낼 수 있습니다.

기존 방법

IP 및 지리적 필터링: 특정 IP/CIDR 범위 및 비즈니스와 관련이 없는 지리적 위치의 트래픽을 차단하거나 제한하면 해당 지역에서 발생한 공격에 대한 노출을 줄일 수 있습니다. 이 방법은 비즈니스 사용자의 오리진이 알려져 있고 제한적인 경우 유용할 수 있지만, 지속적인 유지 관리와 허용되는 소스 목록을 업데이트하는 데 어려움이 있을 수 있습니다. 또한 숙련된 해커들은 프록시를 사용하여 지리적 차단을 우회할 수 있습니다. 그러나 여전히 이 방법은 레이어 7 DDoS 공격에 대한 초기 방어 전략으로 인기가 있습니다.

애플리케이션 레이어 프로토콜 분석: 이 방법은 비정상 또는 악성 패턴을 탐지하기 위해 애플리케이션 레이어 프로토콜 내에서 데이터를 면밀히 조사하여 사전 예방적 방어 메커니즘을 구현함으로써 레이어 7 DDoS 공격을 방어할 수 있습니다. 이는 기존 보안 조치를 우회하는 정교한 DDoS 공격을 방지할 수 있지만, 심층 패킷 검사에 리소스를 많이 소비하고 오탐 가능성이 높아 정상적인 트래픽을 실수로 차단할 수 있다는 단점이 있습니다.

멀티레이어 DDoS 방어 전략을 위한 적절하고 균형 잡힌 레시피 찾기

멀티레이어 DDoS 방어 전략을 수립하는 과정에는 기업의 특정 리스크 프로필과 진화하는 사이버 위협 환경에 맞춰 미세 조정된 접근 방식이 포함됩니다. 이 전략의 핵심은 초기 평가를 통해 주요 자산과 가능성 있는 공격 기법을 파악하고, 그 다음에는 전송률 제한, 방화벽 등 기본적인 보호를 구축하는 것입니다. 고급 단계에서는 새로운 위협에 대한 비정상 기반 탐지, 알려진 공격에 대한 시그니처 기반 탐지, 봇을 필터링하는 챌린지-응답 메커니즘을 혼합해 사용해야 합니다.

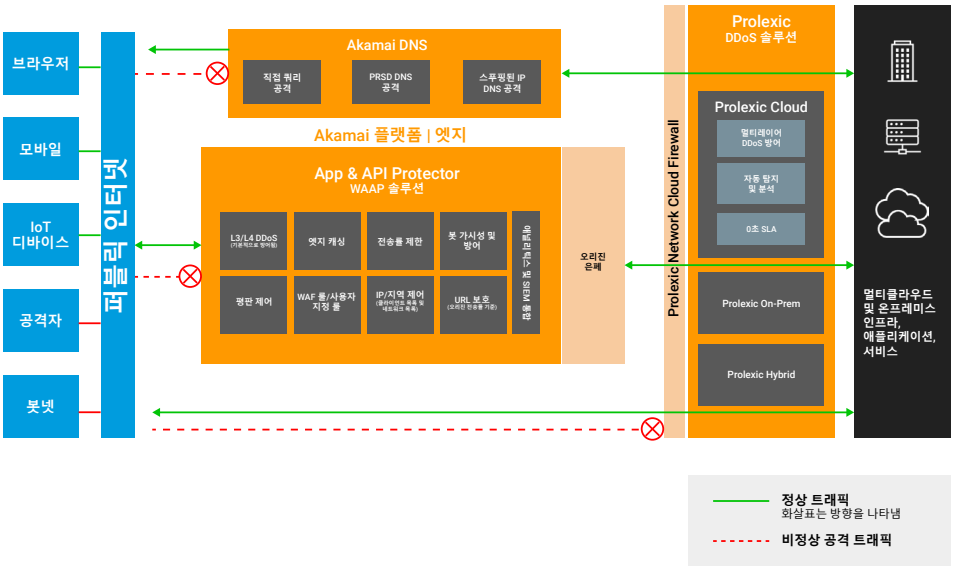
보안 시스템은 알려진 공격과 새로운 DDoS 공격 소스의 TLS 지문 패턴을 파악하는 알고리즘과 같은 적응형 위협 인텔리전스를 통합함으로써 해당 지문을 나타내는 트래픽을 차단하거나 챌린지를 제시하도록 자동으로 방어 기능을 조정해 공격을 효과적으로 방어할 수 있습니다. 포괄적인 인시던트 대응 및 복구 계획은 공격을 받는 동안은 물론 공격 이후에도 피해를 최소화하고 신뢰를 유지하기 위해 매우 중요합니다. 과거의 공격과 새로운 트렌드에 기반하여 지속적으로 학습하고 조정하면 효과적이고 안정적인 방어 전략을 구축할 수 있습니다.

정교한 멀티 기법 DDoS 공격에 직면하고 있는 금융 기관을 보면 균형 잡힌 멀티레이어 방어 전략을 수립하는 것이 얼마나 중요한지 명확히 알 수 있습니다. 중단 시간이 기관 운영과 고객 신뢰에 미칠 수 있는 영향 때문에 이러한 기관은 주요 표적이 됩니다.

트래픽 비정상 탐지와 같은 탐지 및 방어 수단을 조합하고, 전송률 제한, IP/지역 필터링, IP 평판, 실시간 위협 인텔리전스 등의 기존 방법을 사용하며, 여기에 더해 강력한 인시던트 대응 계획을 함께 사용함으로써 고객에 대한 서비스의 연속성을 보장하는 동시에 중요한 자산을 중단으로부터 보호할 수 있습니다. 이러한 포괄적인 접근 방식은 기업이 오늘날의 디지털 환경에서 다면적 특성을 지닌 DDoS 공격을 방어하는 방법을 보여주는 사례입니다.

준비: Akamai Edge 아키텍처를 통한 심층 보안 전략

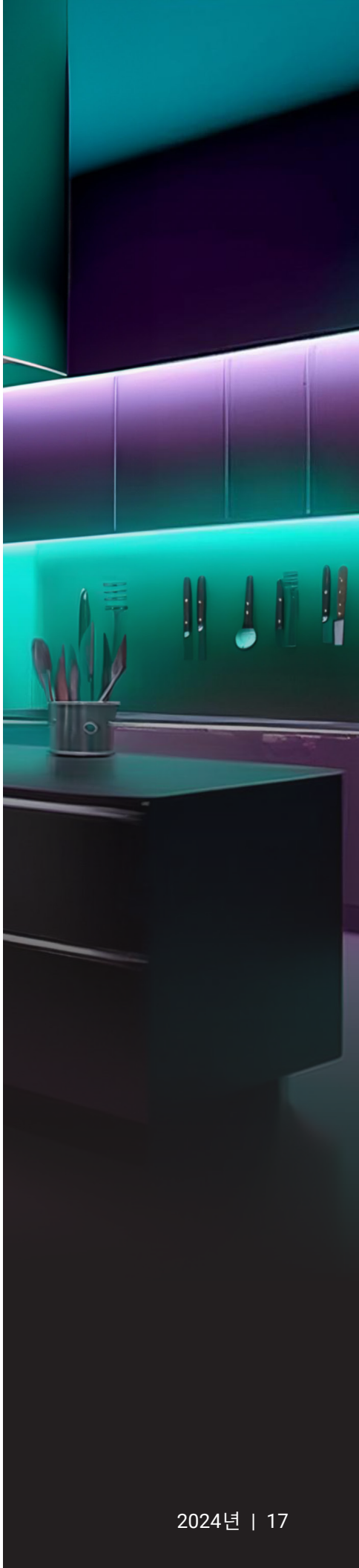
애플리케이션 레이어 DDoS 방어에 대한 Akamai의 접근 방식은 가장 정교한 공격으로부터 웹사이트, 애플리케이션, API를 안전하게 보호할 수 있도록 설계된 포괄적이고 적응성이 뛰어난 멀티레이어 방식입니다. App & API Protector는 포괄적인 보호를 제공하는 여러 가지 주요 기능을 활용합니다. 또한 웹 애플리케이션 방화벽, 봇 가시성 및 방어, API 보안, 레이어 7 DDoS 방어 기능을 단일 제품에 결합해 광범위한 보호를 제공합니다.



Edge DNS, App & API Protector, Prolexic solutions를 사용하여 종합적인 DDoS 방어를 제공하는 레퍼런스 아키텍처

Akamai의 DDoS 방어 전략은 실시간으로 모든 요청을 검사하는 Akamai의 대규모 분산 플랫폼을 통해 트래픽을 라우팅하는 엣지 보안 아키텍처를 기반으로 구축되었습니다. 이 설정은 DDoS, 웹 애플리케이션 및 API 공격, 악성 봇이 애플리케이션이나 인프라에 도달하지 못하도록 엣지에서 바로 방어합니다. 이렇게 하면 공격에 맞춰 확장 가능한 빠르고, 매우 안전한 상시가동형 아키텍처를 유지함으로써 비즈니스 연속성을 강화할 수 있습니다.

Akamai의 강력한 툴 및 재료 제품군은 사전 예방적 및 사후 대응적 제어를 모두 제공합니다. 각 제어 방법은 전반적인 방어 전략에서 고유한 목적을 가지고 있습니다.



사전 예방적 제어

사전 예방적 제어는 보안 체계를 강화하여 취약점을 최소화하는 데 중점을 두어 공격이 발생하기 전에 이를 방지하는 데 도움이 됩니다. 그 사례는 다음과 같습니다.

- **IP 제어(블록 IP, CIDR 범위 및 ASN):** 기본적인 방어 레이어인 이 제어 기능은 알려진 악성 IP 주소 또는 위협 인텔리전스를 통해 탐지된 범위를 차단합니다.
- **지역 제어(특정 지역 차단):** 특정 지역의 트래픽을 허용 또는 제한함으로써 기업은 고위험 지역에서 발생한 공격에 대한 노출을 사전에 제한할 수 있습니다.
- **웹 애플리케이션 방화벽(WAF) 룰:** FiberFox와 같은 DDoS 툴 등 알려진 취약점 및 공격 기법에 대한 룰을 구축하면 강력한 1차 방어선을 구축할 수 있습니다.
- **IP 평판 제어:** DDoS, 웹 스크레이핑, 기타 악성 활동의 알려진 악성 리소스에 대한 휴리스틱을 통해 인텔리전스를 사용하면 의심스러운 트래픽을 선제적으로 차단하거나 정밀 조사할 수 있습니다.
- **플랫폼 DDoS 인텔리전스:** 전 세계적으로 분산된 Akamai Edge 플랫폼의 DDoS 공격 인사이트를 활용하면 애플리케이션 레이어 DDoS 공격에 맞서 사전 예방적 방어 전략을 수립하는 데 도움이 됩니다.
- **캐싱:** 콘텐츠 캐싱을 최적화하면 오리진 서버에 대한 부하를 크게 줄일 수 있으며, 엣지 캐시의 요청을 처리하여 DDoS의 영향을 간접적으로 방어할 수 있습니다.
- **Site Shield:** Akamai Edge 네트워크를 통한 오리진에 대한 요청만 허용하는 오리진 은폐 기술을 사용하면 서버 부하를 추가적으로 줄일 수 있습니다.

사후 대응적 제어

사후 대응적 제어는 탐지된 공격에 대한 대응으로, 영향을 방어하고 서비스 가용성을 유지하기 위한 목적을 갖고 있습니다.

- **전송률 제한(전송률 정책):** 이 방법은 DDoS 공격을 나타낼 수 있는 갑작스러운 트래픽 급증을 방어하는 데 중요합니다. 설정을 구성할 수 있으며 고객별 트래픽 프로필에 맞게 조정이 가능합니다. 전송률 제한은 증폭 공격 및 분산 DDoS 공격으로부터 고객 오리진을 보호하는 첫 번째 방어선으로서 도움이 되는 경우가 많습니다.
- **슬로우 POST 보호:** 이 기능은 슬로우 HTTP POST 공격만 집중적으로 타게팅하며 서버 리소스를 고갈시키려는 비정상적인 트래픽 패턴에 대응합니다.

- **WAF의 사용자 지정 룰:** 새로운 위협에 대한 대응으로 신속하게 룰을 조정하여 유연하고 동적인 방어 메커니즘을 제공할 수 있는 것이 중요합니다.
- **봇 가시성 및 방어:** 브라우저 사칭을 탐지하는 머신 러닝을 사용하면 자동화를 통해 이루어지는 정교한 DDoS 공격을 탐지하고 차단할 수 있습니다.
- **지능형 부하 분산을 통한 URL 보호:** 오리진에 대한 과도한 요청을 제한하고 악성 트래픽보다 정상 사용자의 우선 순위를 높게 지정하는 제어 기능을 통해 DDoS 공격 중에도 서비스 가동 시간을 유지할 수 있습니다.
- **플랫폼 DDoS 인텔리전스:** 부하 분산은 URL 보호의 한 카테고리로, 전세계적으로 분산된 Akamai 플랫폼의 DDoS 공격 인사이트를 활용하여 고객사가 애플리케이션 레이어 DDoS 공격을 방어할 수 있는 사전 예방적 방어 전략을 수립할 수 있도록 지원합니다.

재료 혼합, 레시피와의 균형 달성

- **예:** 대규모 금융 서비스 기업은 Akamai WAAP 솔루션과 심층 보안 전략을 결합하여 사용합니다.

일부 기업은 다른 기업보다 더 빈번하게 DDoS 공격의 표적이 될 수 있습니다. 예를 들어, Akamai의 2023년 리서치에 따르면 DDoS 공격의 3분의 1 이상이 금융 서비스 기관을 표적으로 삼았습니다. Akamai 고객사인 한 대형 금융 서비스 기업은 로그인 페이지에서 표적 공격에 직면한 적이 있습니다. 그리고 이 기업은 검증된 방어 레시피를 따를 수 있었습니다. 누구나 이러한 방어가 가능합니다.


공격자 프로필: 핵티비스트


표적: 로그인 엔드포인트


방법: HTTP POST 플러드


공격 발생지: 최대 6만 6천개의 IP 주소 및 140여 개 국가

Akamai

레시피
HTTP POST 플러드 공격 방어

재료:

사전 예방적 제어:

- **IP 제어**: 위협 인텔리전스를 사용하여 알려진 악성 엔티티와 연결된 IP 주소 또는 CIDR 범위를 차단합니다.
- **지역 제어**: 핵티비스트 그룹이 있는 것으로 알려진 지역(예: 'Anonymous Sudan'과 관련된 지역)의 트래픽을 차단 목록에 추가합니다.
- **웹 애플리케이션 방화벽(WAF) 룰**: HTTP GET 플러드의 일반적인 패턴을 포함해 알려진 DDoS 툴 및 기법에 대응하기 위해 특별히 고안된 룰을 구축합니다.
- **IP 평판 제어**: 평판 점수가 낮은 소스의 트래픽을 주의 깊게 모니터링하거나 능동적으로 (실시간으로) 차단합니다.
- **플랫폼 DDoS 인텔리전스**: Akamai의 글로벌 DDoS 공격 데이터에서 얻은 인사이트를 활용하여 새로운 위협 기법을 예측하고 대응합니다.
- **Site Shield**: 방화벽 ACL(Access Control list)을 활성화하여 Akamai Edge 네트워크의 트래픽만 허용하고 나머지는 차단합니다.

사후 대응적 제어:

- **전송률 제한**: 트래픽 급증을 방어하기 위해 전송률 정책을 수립하여 홈페이지에 대한 초당 요청의 적절한 임계값을 설정합니다. (1) 요청 속도를 측정하는 시간 창을 초당 1건의 요청으로 낮추고, (2) 금융 기관의 기업 IP 주소 및 파트너와 같은 소스를 허용 목록에 추가하면서 연결 IP 소스의 지역 및 평판 점수를 기반으로 전송률 제한을 적용해 전송률 제한을 최적화할 수 있습니다.
- **WAF의 사용자 지정 룰**: 공격이 탐지되면 공격 고유의 특성에 대응하여 맞춤형 룰을 생성합니다. 사용자 지정 룰에서 트래픽 샘플링 제어를 사용하면 트래픽 분석에 도움이 되어 주요 공격 소스를 보다 효율적으로 파악할 수 있으며, 사용자 지정 룰에서 IP/지역 제어를 사용하면 신속한 방어에 도움이 될 수 있습니다.
- **봇 가시성 및 방어**: 브라우저 사칭 탐지 기능을 사용해 정상 사용자 행동을 모방하지만 플러드의 일부인 요청을 식별하고 차단합니다.
- **URL 보호**: 요청률을 제한하기 위한 제어 기능을 특별히 로그인 URL에 적용하여, 정상 사용자의 대역폭을 보존할 수 있습니다. 프록시, Tor 출구 노드, 기본 봇, 평판이 낮은 IP 등의 카테고리로 지능적인 부하 분산 기능을 설정하면 실제 사용자 트래픽을 이러한 악성 소스보다 높은 순위로 지정할 수 있습니다.

준비 방법:

검토 단계:

- **설정 검토**: 현재 보안 체계를 철저히 검토합니다. 알게 된 내용을 기반으로 사전 예방적 제어를 설정하여 모든 관련된 지리 제어 및 IP 제어가 적절하게 관리되도록 합니다.
- **설정 최적화**: HTTP POST 플러드 공격의 특징을 포함하여 비정상적인 트래픽 패턴을 인식하고 방어하도록 설정을 조정합니다.

탐지 및 방어 단계:

- **모니터링 및 알림**: Akamai의 엣지 방어 아키텍처는 수신 트래픽을 모니터링하여 DDoS 공격을 나타낼 수 있는 패턴을 감지할 수 있습니다. HTTP POST 플러드 등 알려진 DDoS 수단과 일치하는 비정상적인 트래픽 급증 또는 패턴에 대한 알림을 설정할 수 있습니다.
- **탐지 및 방어**: IP 평판, 캐싱, IP/지역 제어 등 다양한 사전 예방적 제어 기능이 올바르게 설정된 경우 자동으로 탐지 및 방어 기능을 제공합니다.

공격이 감지되면 전송률 제한, URL 보호, 브라우저 사칭 탐지 등의 제어 기능이 사용자 개입 없이 자동으로 시작됩니다.

- **분석 및 적응**: 공격 패턴을 지속적으로 분석하고 방어 조치를 실시간으로 적응시킴으로써 발전하는 기법에 대응합니다. 예를 들어, 최신 공격 트래픽 분석을 기반으로 맞춤형 룰 또는 전송률 제한 정책을 만들 수 있습니다.

복구 및 공격 후 분석:

- **로그 분석**: 공격 후에는 상세한 트래픽 로그 분석을 수행하여 공격 기법과 배포된 제어 기능의 효과를 파악합니다.
- **조정**: 공격 분석에서 얻은 인사이트를 바탕으로 사전 예방적 및 사후 대응적 제어 기능을 필요에 따라 조정합니다.

요리 서빙 방법 제안:

- 발전하는 DDoS 기법에 맞춰 방어 전략을 정기적으로 검토 및 업데이트합니다. 특정 요구 사항, 위협 노출 및 업계 모범 사례에 따라 검토에 대한 세부 사항은 기업마다 크게 다를 수 있습니다. 금융 서비스 기업은 매 분기마다 이러한 검토를 수행해야 하는 반면, 이커머스 플랫폼은 시즌별 쇼핑이 몰리는 시기에 대비해야 하므로 연 2회의 검토를 목표로 삼을 수 있습니다.
- 보안 팀이 새로운 DDoS 공격 기법을 인식하고 대응할 수 있도록 지속적인 교육을 실시합니다.
- 모의 공격을 실시하여 배포한 조치의 효과를 테스트하고 실제 인시던트에 대한 팀의 대비를 확립합니다.

복구 및 공격 후 분석

애플리케이션 레이어(레이어 7) DDoS 공격을 방어하는 데 있어서 공격 후 단계는 향후 방어 체계의 강화를 위해서 뿐만 아니라 적의 이해를 위해서도 매우 중요합니다. 여기에는 두 가지 중요한 단계, 즉 공격 패턴을 분석하고 분석을 기반으로 방어 체계를 강화하는 단계가 포함됩니다. 이러한 단계는 안정적인 방어 전략을 수립하고 온라인 서비스의 지속성과 무결성을 보장하는 데 핵심적인 역할을 합니다.

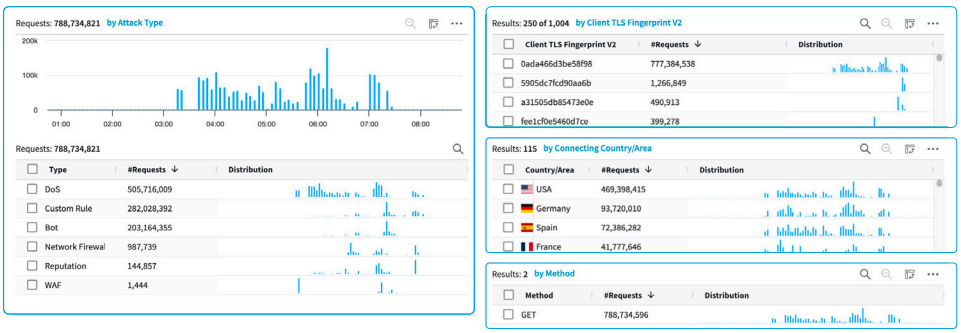
트래픽 및 공격 패턴 분석

공격을 방어한 후 다음 단계는 인시던트를 분석하여 어떤 전략이 효과가 있었는지, 그리고 어떤 전략이 예상대로 작동하지 않았는지 파악하는 것입니다. 이 평가에는 고객의 신뢰에 대한 영향, 데이터 무결성 및 잠재적인 금전적 손실 등 장기적인 요소가 포함됩니다. Akamai Web Security Analytics와 같은 포괄적인 보안 애널리틱스 시스템은 이 단계에서 필수적인 툴로서, 기업이 공격 트래픽과 그 영향을 이해할 수 있도록 지원합니다.

이 분석에는 공격자들이 사용한 기법, 기술, 절차(TTP)를 분해하는 과정이 포함됩니다. 주요 질문은 다음과 같습니다.

- 트래픽 급증의 성격은 무엇이었나요?
- 특정 애플리케이션 기능이 표적으로 지정되었나요?
- 이 공격이 알려진 취약점을 악용했나요?

Akamai Web Security Analytics는 트래픽 패턴의 비정상을 파악하고 공격의 지리적 오리진을 정확히 찾아내며 관찰된 행동을 기반으로 공격 종류를 분류할 수 있습니다. 다음 사례는 DDoS 공격을 조사하기 위해 적용할 수 있는 트래픽 특성 또는 차원을 보여 줍니다.



표시된 이미지는 보안 이벤트에 대한 전례 없는 가시성과 사전 예방적 분석을 제공하는 Web Security Analytics의 이미지입니다

공격 분석을 기반으로 방어 전략 검토 및 업데이트

공격 분석을 기반으로 방어 전략을 검토하고 업데이트하는 것은 기업의 사이버 보안 체계를 강화하는 데 있어 중요한 구성요소입니다. 과거 공격의 구체적인 내용을 살펴봄으로써 기업은 현재의 방어 체계가 지닌 취약점을 식별하고 정보에 입각한 조정을 할 수 있습니다. 다음은 Akamai Web Security Analytics를 사용하여 이 프로세스를 적용하는 몇 가지 예입니다.

사례 1: 공격 패턴을 기반으로 WAF 룰 업데이트

시나리오: 어떤 기업이 애플리케이션 홈페이지를 표적으로 악성 요청을 쏟아내는 웹 애플리케이션을 표적으로 한 레이어 7 DDoS 공격에 직면하고 있습니다.

검토: 공격 분석 결과, 기존 웹 애플리케이션 방화벽(WAF) 룰이 공격 트래픽의 90% 이상을 적절히 탐지하고 차단했지만 나머지 약 10%는 해당 지역의 공격 소스가 애플리케이션을 압도하도록 허용하는 명시적 지리적 허용 목록이 있었기 때문에 유출된 것으로 나타났습니다.

업데이트: 기업은 이러한 분석을 바탕으로 WAF 설정을 업데이트하여 해당 지역에서 발생한 공격 트래픽 고유의 특성에 맞는 맞춤형 WAF 룰을 사용했습니다. 재정의는 지역을 계속 허용하지만 공격 트래픽의 특정 속성을 차단할 수 있습니다. 또한 해당 지역에 대한 전송률 제한 설정이 더 엄격해졌습니다.

사례 2: 오리진 보안 강화

시나리오: 리테일 업체 웹사이트의 로그인 프로세스가 자동화된 봇을 활용하는 고도로 분산되고 정교한 레이어 7 DDoS 공격을 받습니다.

검토: 공격 후 분석 결과, 공격 트래픽은 150개 이상의 국가에서 고도로 분산되어 있었고 정상 브라우저처럼 보이는 수백 개의 TLS 지문을 통해 전송된 것으로 나타났습니다. 트래픽의 상당 부분은 클라우드 공급업체에서 발생했으며, 그 중 일부는 신뢰할 수 있는 파트너 소스로 허용 목록에 올라와 있었습니다. 공격은 효과적으로 방어했지만 추가 방어 조치가 필요하다는 분석 결과가 나왔습니다.

업데이트: 이 기업은 결제 프로세스와 같이 연산량이 많은 URL을 보호할 목적으로, 고도로 분산된 애플리케이션 레이어 DDoS 공격으로부터 연산량이 많은 URL과 API 엔드포인트를 보호하기 위해 특별히 설계된 기능인 URL 보호 기능을 구축했습니다. 또한 보안 아키텍트는 봇, 프록시, IP 평판 등에 대한 지능적인 부하 분산 기능도 활성화했습니다. URL 보호의 하위 기능인 이 기능은 악성 소스로부터의 요청을 먼저 거부하여 실제 사용자 트래픽을 우선 순위로 지정하는 데 도움이 됩니다.

또한 이러한 고속 공격이 발생하는 동안 확장할 수 없는 온프레미스 봇 솔루션의 존재로 인해 이전에는 비즈니스에서 제대로 고려하지 않았던 봇 방어 기능을 WAF에 내장하기로 결정했습니다.

사례 3: API 엔드포인트에 대한 전송률 제한 구축

시나리오: 금융 서비스 애플리케이션의 API 엔드포인트가 사기성 거래 요청 플러드로 인해 과부하가 걸립니다. 이는 서버 리소스를 고갈시킬 목적으로 진행되는 레이어 7 DDoS 공격을 나타냅니다.

검토: 공격 패턴 분석 결과 공격자들은 대량 요청을 처리할 수 없으며 잘 보호되지 않는 API 엔드포인트를 특별히 표적으로 삼은 것으로 나타났습니다.

업데이트: 이에 대응하여 기업은 모든 API 엔드포인트, 특히 취약다고 확인된 엔드포인트에 엄격한 전송률 제한을 구축했습니다. 또한 API 보안에 고급 레이어를 제공하는 전용 API 보안 추가 기능도 도입했습니다.여기에는 API 논리 악용, 섀도 API 위협, API 취약점 모니터링이 포함되어 있습니다.

전략적 요점

- **지속적인 모니터링 및 로깅:** 강력한 모니터링 및 로깅 시스템을 구축하여 비정상을 즉시 탐지하고 공격 도중은 물론 공격 후 피해를 정확하게 평가합니다.
- **취약점 관리:** 알려진 취약점을 방어하고 악용의 리스크 줄이기 위해 시스템을 정기적으로 업데이트하고 패치합니다.
- **공격 패턴 분석:** 공격자의 방법론과 의도를 이해하기 위해 적절한 가시성 툴을 사용하여 공격 패턴을 심층적으로 분석합니다.

공격 후 분석

피해 평가 및 공격 패턴 분석은 강력한 레이어 7 DDoS 방어 전략의 중요한 구성요소입니다. 이 단계는 공격의 즉각적인 영향을 이해하고 방어하는 데 도움이 될 뿐만 아니라 방어 메커니즘의 지속적인 개선을 위한 정보를 제공해 향후 위협에 대한 대비도를 높일 수 있습니다.

레시피 유지 및 업데이트

강력한 레이어 7 DDoS 방어 체계를 유지하려면 최신 트렌드와 기법을 지속적으로 모니터링해야 합니다.

공격자들은 새로운 툴과 취약점을 활용하여 공격 패턴을 끊임없이 섞습니다. 이러한 위협에 선제적으로 대응하기 위해 기업은 방어 체계를 리서치, 모니터링, 평가하며, 보호를 자동화하고, 위협 인텔리전스 커뮤니티와 협력하는 데 시간과 노력을 투자해야 합니다.

주요 사이버 보안 포럼을 모니터링하는 것은 좋은 시작이지만 충분하지는 않습니다. Akamai는 보다 규범적인 접근 방식을 권장합니다.

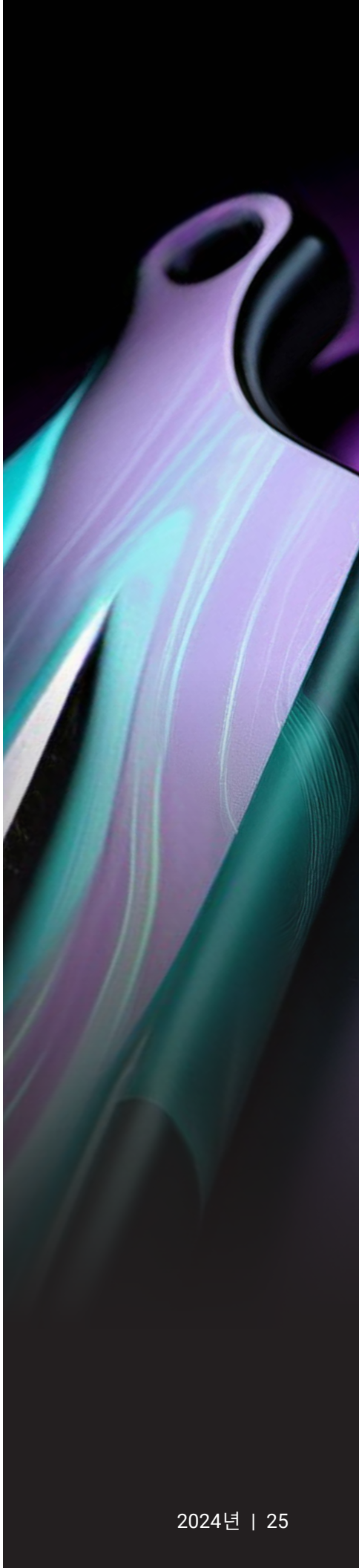
지속적인 모니터링 및 평가 - 네트워크 및 애플리케이션 성능을 정기적으로 모니터링하여 새로운 위협을 나타내는 새로운 패턴이나 비정상을 탐지합니다. 그리고 이 데이터를 사용하여 기존 방어 메커니즘의 효과를 평가하고 개선 또는 조정이 필요한 부분을 파악합니다.

DDoS 대응 팀 조직 - DDoS 공격 현황을 리서치, 모니터링하고 최소한 분기별로 주요 조사 결과 및 권장 사항을 바탕으로 전체 기업에 보고하는 전문가 또는 팀을 기업 내에 만듭니다.

위협 인텔리전스 커뮤니티 참여 - 공격자들은 가장 효과적인 최신 방법에 대해 서로 소통하고 있습니다. 따라서 다른 회사 및 업계 사람들과 함께 최선의 방어 방법에 대한 정보를 공유하지 않을 이유가 없습니다. 최신 위협 인텔리전스에 대해 최신 소식을 항상 놓치지 마세요. 보안 피드를 구독하고 사이버 보안 포럼에 참여하며 업계의 동료들과 협업하는 것이 좋습니다. 이렇게 얻은 정보는 새로운 공격 기법을 예측하고 그에 따라 방어 체계를 조정하는 데 도움이 될 것입니다.

사이버 보안 벤더사 활용 - 기술 벤더사에는 종종 전문 위협 리서치 팀이 있으며, 콘텐츠 전송 네트워크(CDN)를 보유한 벤더사는 다른 곳에서는 얻을 수 없는 인사이트를 제공할 수 있습니다. 언제 어디서나 이러한 배움의 기회를 활용하는 것이 좋습니다. 또한 정기적으로 보안 컨설팅 전문가를 찾는 것도 도움이 됩니다.

내 방어 체계 테스트 - '호미로 막을 것을 가래로 막는다', '공든 탑이 무너지랴'는 진부하게 들릴 수 있지만 그 메시지는 정직합니다. 정기적인 테스트와 훈련은 절대 배신하지 않을 것입니다.



주기적인 검토와 모의 공격 시나리오(공격자 훈련)를 실시해 방어 전략의 안정성을 테스트하세요. 이러한 훈련은 현재 설정의 취약점을 노출하고 공격자가 시스템을 악용하는 방법에 대한 인사이트를 제공합니다.

적어도 일 년에 한 번 네트워크 테스트를 수행하는 것이 좋습니다. 최근의 공격 프로필, 특히 같은 업계에 속한 회사에 발생한 공격 프로필도 테스트 사례에 좋은 참고 자료가 될 수 있습니다.

커뮤니티와 배운 내용 공유 - 다시 한번 강조하지만, 공격자들이 툴과 기법을 공유하는 것처럼 기업 또한 성공적인 방어 전략에 대한 지식을 공유해야 합니다.

사이버 보안 전문가는 성공과 실패를 모두 문서화함으로써 현실적인 인사이트를 제공할 수 있으며, 이는 집단 기술 자료를 풍부하게 만듭니다. 업계 포럼에서 활동하고, 분야에 새로 발을 들인 사람들에게 멘토링을 제공하며, 협업 프로젝트에 참여하는 것은 강력한 방어 생태계를 구축하는 데 있어 핵심적인 요소입니다. 이와 같은 노력은 보다 효과적인 전략 및 툴을 개발하는 데 기여할 뿐만 아니라 변화하는 공격자의 기법에 적응할 수 있는 다양한 경험과 인사이트를 제공합니다. 이러한 협력 정신은 사이버 보안 환경에서 앞서가기 위해 필수적이며, 모든 기여는 더욱 강력하고 안정적인 디지털 세상을 구축하는 데 중요한 역할을 합니다.

요점 정리

DDoS 위협에 대한 환경은 역동적이며, 공격자들은 끊임없이 방어 체계를 우회하기 위한 새로운 방법을 모색하고 있습니다. 레이어 7 DDoS 방어 전략을 유지 및 업데이트하는 것은 경계, 적응력, 사전 예방적 접근 방식이 필요한 지속적인 프로세스입니다. 항상 최신 정보를 유지하고, 정기적인 테스트 및 검토에 참여하며, 지속적인 개선 문화를 배양함으로써 현재와 미래의 위협에 대한 강력한 방어 체계를 유지할 수 있습니다.

결론

레이어 7 DDoS 공격은 보다 정교해졌을 뿐만 아니라, 자동화의 발전 및 공격자들 사이의 조율로 인해 공격을 진행하기가 더욱 쉬워졌습니다. 한편, 기업들은 실패로 인한 비용이 증가함에 따라 더 크고 복잡한 환경을 방어해야 합니다.

실제로 방어 레시피를 만들어 내는 것은 쉽지 않습니다. 하나의 방어 수단은 절대로 레이어 7 DDoS 공격에 대한 만병통치약이 될 수 없습니다. 지금까지 논의한 바와 같이 여러 탐지 및 방어 전략을 결합한 다중 접근 방식이 가장 강력한 방어 기능을 제공합니다.

또한 보호가 필요한 애플리케이션이나 서비스의 특정 요구사항, 트래픽 패턴 및 리스크 프로필에 따라 적절한 방법을 선택해야 합니다. 비즈니스, 트래픽 및 취약점에 대한 이해 없이는 방어 체계를 구축할 수 없습니다. 이러한 전략에 대한 정기적인 업데이트 및 조정은 발전하는 DDoS 위협 환경에 적응하기 위해 필수적입니다.

마지막으로, 공격이 끝나더라도 여기서 끝난 것이 아닙니다. 공격 후 분석 및 조정은 지속적인 성공을 위해 매우 중요할 뿐만 아니라 지식을 공유하고 경력을 개발하는데 있어서도 큰 역할을 합니다.

다행히도 Akamai는 모든 단계에서 지원을 제공할 수 있는 강력한 역량을 갖추고 있습니다. 앱 및 API 보안에서부터 글로벌 트래픽에 대한 탁월한 인사이트, 전문적인 공격 후 분석에 이르기까지 많은 기업들이 필요한 레이어 7 DDoS 방어 체계를 단일 공급업체로부터 모두 확보할 수 있는 기회를 활용하고 있습니다.

Akamai의 레이어 7 DDoS 방어 솔루션을 직접 확인해보세요.
App & API Protector의 무료 체험을 시작하세요.

저자 소개

편집 및 작성

아시 아메드(Aseem Ahmed)
바니 빌(Barney Beal)

검토 및 주제별 기여

압데슬람 벨라 (Abdeslam Bella)
신 플린(Sean Flynn)
알렉스 마크스블러스 (Alex Marks-Bluth)
니테쉬 쉬리바스타바 (Nitesh Shrivastava)
프라트메쉬 베르마 (Prathmesh Verma)
데니스 버차드 (Dennis Birchard)
리안 가오(Ryan Gao)
파완 사즈나니 (Pawan Sajnani)
패트릭 설리번 (Patrick Sullivan)
대니엘 월터 (Danielle Walter)

마케팅 및 출판

조지나 모랄레스 햄프(Georgina Morales Hampe)
쉬방기 사후(Shivangi Sahu)

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com 및 akamai.com/blog를 확인하거나 X (기존의 Twitter), LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 10월 발행.