AKAMAI 백서

Client Reputation: 웹 애플리케이션 보안 강화 솔루션

Akamai
FASTER FORWARD

목차

소개

웹 애플리케이션의 데이터 유출과 웹사이트 변조는 현재 많은 기업들이 직면하고 있는 큰 도전과제입니다. 웹 애플리케이션은 사이버 공격, 성능 저하, 가용성 문제에 특히 취약합니다. 대표적인 사례가 2015년 6월 미국 정부를 겨냥해 발생한 대형 해킹 공격입니다. 이 공격으로 인해 미국 연방 정부 소속 직원 4백만 명의 개인 정보가 유출되었습니다.

기업 보안팀은 사이버 보안을 강화하고 온라인 자산을 보호하기 위해 일반적으로 전송률 제어(Rate Control), 페이로드 탐지, 클라이언트 평판(client reputation) 모니터링 등 여러 방식을 종합적으로 사용합니다. 예를 들어, 과거에 비해 범죄율이 증가하는 와중에 이웃집에 강도가 들기라도 하면 많은 사람들이 가정용 보안 시스템을 기꺼이 장만할 것입니다. 마찬가지로 전송률 제어는 악성 웹 트래픽이 증가할 때 경고 메시지를 보내기 때문에 웹 공격을 방어할 수 있습니다. 창문과 출입문에 경보 시스템을 설치해 놓으면 외부 침입자가 물건을 훔쳐가기가 훨씬 어렵고 위험해지는 것처럼 웹 애플리케이션 방화벽(WAF)은 페이로드를 기반으로 사용자 요청을 제한해 동일한 목적을 달성할 수 있습니다. 감시 카메라로 문 밖에 있는 사람이 절도범인지 파악해 범죄가 발생하기 전에 경찰에 신고하는 것처럼 Akamai의 클라이언트 평판 모니터링 서비스 역시 악성 트래픽의 근원을 차단해 공격을 방어할 수 있습니다.

이 백서에서는 클라이언트 평판 서비스를 웹 애플리케이션에 적용하여 사용자 IP별로 점수를 책정했을 때 보안 측면에서 어떤 효과를 거둘 수 있는지에 대해 자세히 살펴보도록 하겠습니다. 기업들은 클라이언트 평판 데이터를 바탕으로 클라우드 보안에 대해 보다 정확한 의사결정을 내릴 수 있고 특정 IP 주소로부터 발생되는 보안 위협을 미연에 차단할 수 있습니다.

WAF 모범 사례가 필요한 이유

보안 위협이 점차 고조되어 가고 있는 오늘날과 같은 환경에서는 멀티레이어 방식의 보안 시스템이 필수적입니다. 전송률 제어는 1차 방어선입니다. 웹 애플리케이션에 대한 사용자 요청 전송률을 모니터링 및 제어하여 레이어 7 디도스(DDoS·분산 서비스 거부) 공격을 방어하는 역할을 합니다. 단 몇 초 만에 요청 건수가 급증하는 경우 IP 주소 및 여타 변수(parameter)를 기준으로 공격자를 식별해 차단하도록 행동 룰(behavioral rule)을 설정할 수 있습니다.

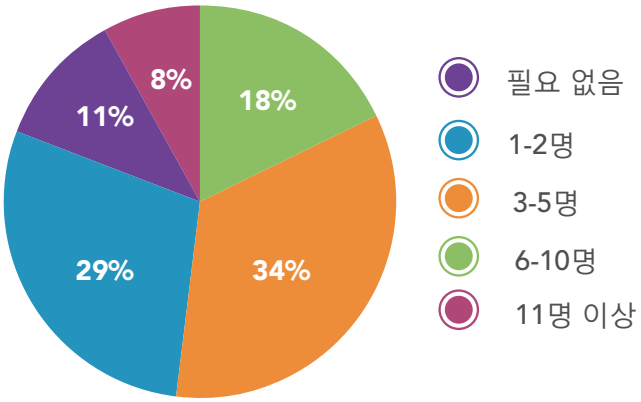
2차 방어선은 악성 공격으로부터 웹 애플리케이션을 보호하는 WAF입니다. WAF는 HTTP 통신 과정에서 감시자 역할을 합니다. 룰 세트를 통해 트래픽을 감시하면서 IP 요청이 악성 공격인지 정상인지 확인합니다. WAF 룰 세트를 설정하는 과정은 매우 복잡하기 때문에 이해를 돕기 위해 몇 가지 사례가 제공됩니다. 하지만 비즈니스 환경 변화에 따라 룰 세트를 세밀하게 조정해야 하는 경우가 종종 발생하는데 이는 기업들에게 큰 부담으로 작용합니다.

WAF는 악의적 공격일 가능성이 높은 사용자 요청을 탐지하는 능력이 탁월하지만, 동시에 높은 가용성과 우수한 성능을 기대하는 협력사와 고객들의 정상적인 요청을 차단하지 않는 것 역시 중요합니다. WAF 모범 사례에 따르면, 공격 기법의 변화에 발맞춰 룰 역시 정기적으로 수정될 필요가 있습니다. 동시에 이 과정에서 정상적인 HTTP 트래픽을 허용해 쾌적한 사용자 경험을 지속적으로 제공해야 합니다. Akamai의 후원을 받아 *Ponemon Institute*가 2015년 실시한 WAF 활용 실태에 대한 *연구조사*에 따르면 안타깝게도 웹 애플리케이션에 대한 전문적인 보안 지식을 갖춘 IT 인력의 부족으로 인해 WAF 가 제대로 관리되지 않는 경우가 상당히 많았습니다.

이 연구조사에 참여한 응답자의 30%는 웹 애플리케이션 공격이 점차 증가하고 있는 상황에도 불구하고 WAF를 구매한 후 실제로 배치하지 않았다고 답변했습니다. 이는 WAF를 관리할 수 있는 전문 인력을 찾기가 그만큼 어렵다는 점을 방증합니다. 하지만 응답자 3명 중 2명은 WAF 가 애플리케이션 성능 저하 없이 공격을 방어할 수 있는 우수한 보안 능력을 갖추고 있다고 생각한다고 답변했습니다. 웹 애플리케이션의 성능 저하 없이 WAF 모범 사례를 실행에 옮길수 있는 한 가지 검증된 방법은 클라우드 기반 보안 서비스 제공업체와 손을 잡는 것입니다. 클라우드 기반 보안 서비스 제공업체의 WAF 솔루션은 우수한 확장성을 갖추고 있을 뿐만 아니라 보안 운영 센터(SOC) 전문가들로부터 컨설팅 서비스도 받을 수 있습니다.

WAF 전문 인력의 부족

Q. 귀사에서 WAF를 제대로 관리하려면 몇 명의 인력이 필요합니까? (FTE 기준)



이런 매니지드(managed) 클라우드 보안 솔루션을 이용해 보안 소프트웨어 유지·관리에 관한 모범 사례를 점차 확장해 나갈 수 있습니다. 또한 클라우드 기반 WAF는 탁월한 확장성을 바탕으로 우수한 성능을 제공하고 지연 시간 역시 매우 짧습니다.

사내에서 자체적으로 WAF를 관리할 수 있는 충분한 경제적 여력과 시간이 있다 하더라도, WAF로 인해 발생하는 여러 사소한 문제들을 해결해줄 수 있는 솔루션을 사용하면 IT 보안팀의 업무 부담을 크게 경감시킬 수 있습니다. 클라이언트 평판 모니터링은 사이버 보안을 강화할 수 있는 신개념 웹 애플리케이션 보안 서비스입니다. 이 서비스는 제대로 설정된 WAF를 보완하는 역할을 하며 보안 위협이 WAF에 도달하기 전에 발원지에서 위협 요소를 차단합니다. 이제는 소 잃고 외양간 고치는 방법 대신, 공격이 발생하기 전에 선제적으로 공격을 탐지하고 차단할 수 있습니다.

클라이언트 평판 모니터링과 WAF는 함께 매끄럽게 작동함으로써 악의적인 요청과 그 요청의 발원지를 모두 차단합니다.

보안 관련 의사 결정을 뒷받침하는 클라이언트 평판 모니터링

웹 애플리케이션뿐만 아니라 전체 웹 환경을 보호하기 위해 선제적으로 대책을 마련하는 기업들이 점차 늘고 있습니다. 클라이언트 평판 모니터링은 WAF, 디도스 방어 등 다른 보안 서비스를 보완하는 역할을 함으로써 한층 더 보안을 강화할 뿐만 아니라 악의적 공격 발원지에 대한 폭넓은 가시성을 제공합니다.

또한, 공격 기법이 아닌 위협의 근원이 되는 클라이언트를 집중적으로 모니터링하며 악성 트래픽이 WAF에 도달하기 전에 공격을 차단하는 역할을 합니다.

이런 접근 방식은 웹 클라이언트에 관한 광대한 데이터를 기반으로 고급 알고리즘을 사용해 악의적인 공격자를 식별합니다. 4가지 공격 유형(애플리케이션 레이어 공격, 웹사이트 스캐닝 및 스크레이핑, 기타 웹 공격 실행, DoS 공격)에 가담할 가능성과 과거 행동 패턴을 기준으로 악의적 웹 클라이언트에 대해 개별적으로 점수를 책정합니다.

가장 중요한 점은 기업들이 클라이언트 평판 모니터링을 이용하면 특정 클라이언트 IP 주소의 과거 행동 패턴을 파악해 해당 클라이언트가 웹 애플리케이션 플랫폼 상에서 향후 공격에 가담할 가능성을 예측할 수 있습니다. 또한 이 데이터를 이용해 특정 클라이언트 IP 주소에서 발생하는 요청의 의도 역시 예측할 수 있습니다.

클라우드 보안 인텔리전스

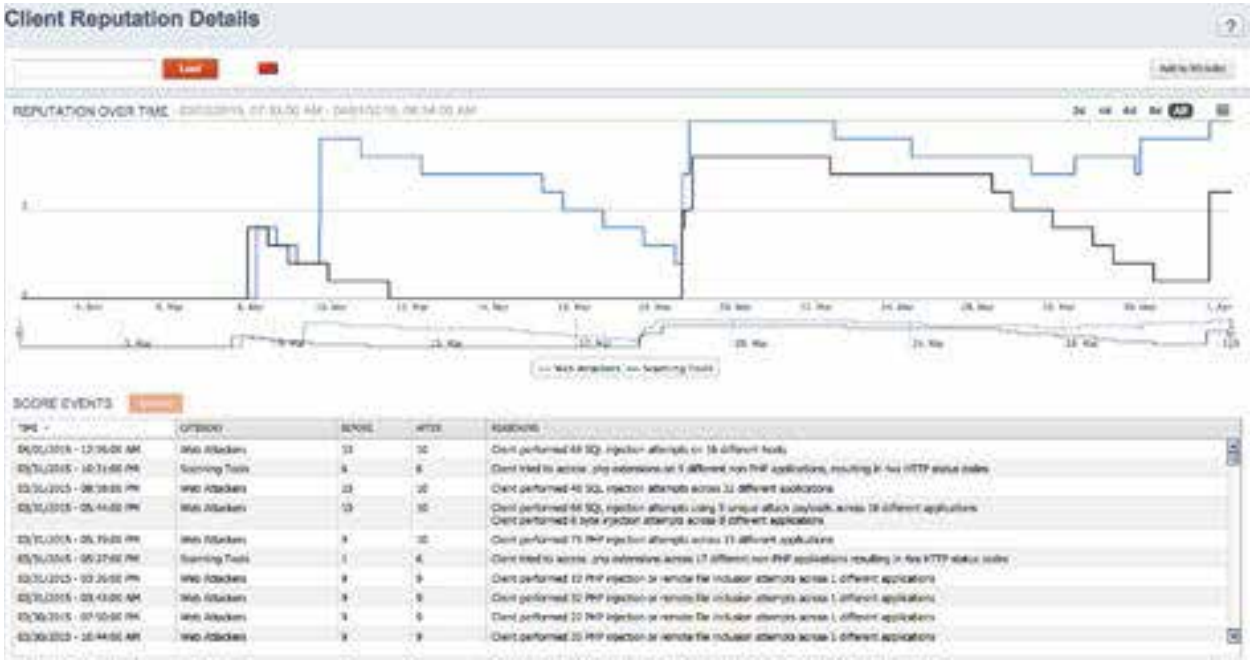
클라우드 보안 인텔리전스(Cloud Security Intelligence)는 Akamai의 보안 플랫폼으로서 매 분기마다 수십억 개의 클라이언트 IP 주소가 이 플랫폼을 통과하고 있습니다. 데이터의 양과 평판 서비스의 품질은 비례합니다.

Akamai는 Hadoop 클러스터(Hadoop cluster)에 4PB(페타바이트)의 데이터를 저장하고 있고, 이 데이터는 20TB(테라바이트) 이상의 일일 공격 관련 데이터로 구성되어 있습니다. 데이터는 WAF 탐지 내용, Akamai 고객사 WAF에서 취합된 데이터, 콘텐츠 전송 네트워크(CDN) 로그 등으로 구성되어 있습니다. Akamai의 데이터 전문가들은 휴리스틱(heuristic)을 사용해 매 시간마다 이 데이터를 쿼리하고, 이를 통해 공격 패턴과 클라이언트 행동을 파악하고 오탐률을 낮춥니다.

정확한 의사 결정을 위한 보안 위협에 대한 가시성

Akamai의 클라이언트 평판 모니터링 서비스는 다음과 같은 2가지 핵심 역량을 기업들에게 제공합니다. 첫째, 기업 서버에 접속하는 특정 클라이언트 차단 여부를 결정할 수 있습니다. 이 때, 클라이언트 리스크 점수와 공격 유형(데이터 스크레이퍼, 스캐너, 디도스, 웹 애플리케이션 공격) 등을 고려해 결정을 내립니다. 둘째, 특정 클라이언트의 서버 접속을 어떤 수준에서 차단할지 자유롭게 결정할 수 있습니다. 이와 같이 유연하게 클라이언트 접속을 제어할 수 있는 이유는 아래와 같은 여러 핵심 기능 덕분입니다.

- **고객사 데이터의 연관성 파악** – 많은 고객사의 서버에 접속하는 클라이언트를 통합적으로 들여다 봄으로써 공격 의도가 있는 클라이언트를 찾아내고, 결과적으로 특정 클라이언트 차단 여부에 대해 보다 정확한 판단을 내릴 수 있습니다.
- **항목별 분류** – 악의적인 행동과 웹 취약점을 악용하려는 공격자를 연관시키는 기능입니다. SQL 인젝션(SQLi), 원격 파일 인클루전(RFI), 크로스 사이트 스크립팅(XSS) 같은 악의적 행동, LOIC(Low Orbit Ion Cannon) 및 HOIC(High Orbit Ion Cannon) 등의 도구를 사용하는 디도스 공격자, 웹 애플리케이션의 취약성을 스캐닝하는 스캐너 및 웹 스크레이퍼와 같은 웹 공격자를 연관시키는 경우가 이에 해당됩니다.
- **클라이언트 리스크 점수** – 여러 사이트에서 발견된 공격의 지속성, 공격 강도, 공격 규모, 분산 정도를 기준으로 리스크를 점수화함으로써 의사 결정 시 활용할 수 있는 자세한 정보를 제공합니다.
- **평판 기반 필터링** – 클라이언트의 행동과 리스크 점수를 기준으로 악의적 클라이언트를 필터링해 접속을 차단하거나 탐지(alert) 결정을 내립니다.
- **헤더 인젝션 추가** – 클라이언트 행동과 리스크 점수 정보가 포함된 요청 헤더를 추가해 백엔드 시스템에서 적절히 대응할 수 있도록 합니다.
- **심층 원인 조사** – 지난 30일 동안 축적된 데이터에 접속해 리스크 점수가 책정된 원인을 조사합니다. 리스크 점수가 변경되는 상황이 발생할 때마다 관련 정보를 수집해야 합니다.



집단지성이 중요한 이유

최근 Akamai 고객 사이트의 WAF가 웹 애플리케이션 공격을 탐지한 사례가 발생했습니다. Akamai 측에 조사해 달라는 요청이 접수되었고, Akamai 보안 운영 센터(SOC) 기술 전문가들은 워드프레스(WordPress) 애플리케이션을 겨냥한 원격 파일 인클루전(Remote File Inclusion) 공격임을 확인했습니다. 일반적으로 흔히 사용되는 공격 전략인 것처럼 보였지만, 실제로 하이퍼텍스트 프로세서(PHP) 사이트뿐만 아니라 다른 취약점을 스캐닝하고 있다는 점에서 차이가 있었습니다.

Akamai의 SOC 기술 전문가들은 이 공격 클라이언트와 다른 악의적 클라이언트 사이에 공통적인 공격 특징이 있는지 분석하기 시작했고, 분석 결과 이 클라이언트는 272 멤버 봇넷의 하나로 약 1,700개의 웹 애플리케이션을 대상으로 130만 건 이상의 공격을 감행했다는 사실을 확인했습니다. 이 분석은 여러 웹사이트에서 발생하는 악의적 활동을 통합적으로 들여다보고 상관관계를 발견하는 것이 얼마나 중요한지 보여줍니다. 해당 조사 과정은 SOC 기술 전문가들에 의해 수동으로 진행되었지만, 클라이언트 평판 모니터링 서비스가 도입된 이후부터 모든 과정은 실시간 자동으로 이루어지고 있습니다.

Akamai는 매일 전세계 웹 트래픽의 15~30%를 처리하기 때문에 정상적인 사용자의 웹 애플리케이션 사용 방식, 공격자의 행동 패턴, 공격 기법의 발전 방식 등에 대한 방대한 데이터를 보유하고 있습니다. Akamai는 CSI 플랫폼을 통해 축적된 이 방대한 데이터를 활용해 보안 룰을 지속적으로 개선하고 보다 효과적인 클라우드 보안 서비스를 고객들에게 제공하며 정확도를 높일 뿐 아니라 새로운 유형의 공격을 철저하게 방어합니다.

클라이언트 평판 모니터링을 이용하는 모든 고객들은 Akamai의 인텔리전스를 십분 활용해 특정 클라이언트로부터 발생되는 요청의 차단 여부에 대해 정확한 의사 결정을 내릴 수 있습니다.

권장사항: 멀티레이어 방어 전략 도입

기업들의 니즈를 충족시키는 SaaS(software-as-a-service)부터 소비자 모바일 애플리케이션에 이르기까지 웹 애플리케이션은 인터넷의 중요한 부분을 차지하고 있습니다. Gartner는 2016년이 되면 대형 은행의 25%가 뱅킹 애플리케이션 스토어를 만들어 애플리케이션 노출도를 높이고 사용자 경험을 개선시킬 것으로 전망하고 있습니다[1]. 하지만 웹 애플리케이션 수가 증가한다는 것은 다시 말해 공격자들이 데이터 도난 목적으로 공격할 수 있는 표적 역시 늘어난다는 것을 뜻합니다. 악의적 공격자들은 애플리케이션을 악용해 수익을 추구하는 만큼 WAF의 중요성 역시 점차 커질 것으로 예상됩니다.

웹 애플리케이션 공격은 대규모 봇넷(botnet) 뿐만 아니라 소규모 봇넷에서도 발생하고 있습니다. 소규모 봇넷은 통신사 네트워크 안에 숨어 있기 때문에 탐지하기가 더 어렵습니다. 클라우드 보안 솔루션을 판단하는 핵심 기준은 끊임 없이 변화하는 보안 위협을 한 발 앞서 나갈 수 있는 역량입니다. 결과적으로 기업의 사내 보안팀이 지속적으로 WAF 룰과 공격 시그니처를 업데이트해야 하는 업무 부담을 경감시켜줄 수 있는 보안 서비스 시장이 빠르게 성장하고 있습니다. 그러나 웹 애플리케이션 보안을 위한 만병통치약은 없기 때문에 대부분의 보안 전문가들은 여러 방어 기술을 긴밀하게 사용하는 방어 전략을 세울 것을 권장하고 있습니다.

전송률 제어(Rate Control)

- 여러 HTTP 트랜잭션 검사
- 단시간에 공격 탐지
- 클라이언트 요청 전송률 초과 시 탐지 개시

WAF(Web Application Firewall)

- 단일 HTTP 트랜잭션 검사
- 실시간 공격 탐지

클라이언트 평판 모니터링

- 공격의 발원지에서 공격 차단
- 클라우드 플랫폼 로그를 바탕으로 한 행동 분석
- 공격 가능성을 예측하기 위해 악의적 의도 발견 시 탐지 개시

결론

모든 측면을 모니터링하는 가정용 보안 시스템과 마찬가지로, 기업들 역시 사이버 보안에 대해 비슷한 방식으로 접근해야 합니다. 예전에는 문과 창문을 모니터링하는 것만으로 충분했던 반면, 오늘날 가정용 보안 시스템에는 동작 센서와 카메라까지 사용되고 있습니다. 기업들 역시 사이버 공격 유형에 따라 각기 다른 방어책을 준비해야 하는데, 이런 접근 방식은 이제 보안 업계에서 모범 사례로 자리 잡아가고 있습니다. 전송률 제어와 WAF는 활용도가 높은 필수적인 요소이고 클라이언트 평판 모니터링은 현관문 밖에 설치된 카메라처럼 보안을 한층 더 강화해 주는 역할을 합니다.

클라우드 보안 전략을 세울 때 클라이언트 평판 모니터링을 포함시키면 악성 공격을 발원지에서부터 차단할 수 있을 뿐만 아니라 보안 인텔리전스를 얻게 되기 때문에 보다 스마트한 의사 결정을 내릴 수 있고 정확하게 리스크를 평가할 수 있습니다. 웹 애플리케이션 보안 레이어가 늘어남에 따라 얻을 수 있는 가장 큰 장점은 기업의 소중한 웹 애플리케이션의 가용성과 성능을 유지할 수 있다는 점입니다. 결과적으로 기업 브랜드 이미지를 제고하고 고객의 신뢰를 쌓을 수 있으며 프로비저닝이 진행 중인 WAF를 통해 리스크를 줄일 수 있습니다.

전송률 제어, WAF, 클라이언트 평판 모니터링, 디도스 방어, 클라우드 보안 등을 모두 종합적으로 사용해야만 다양한 종류와 규모의 사이버 위협을 방어할 수 있습니다. 모든 방어 레이어를 관리, 조율, 튜닝, 업데이트하는 일이 기업 입장에서는 큰 부담이기 때문에 대다수 기업들은 클라우드 서비스 제공업체의 서비스를 적극 이용하고 있습니다.

1. Gartner 보도 자료, "Gartner는 2016년까지 50대 글로벌 은행 중 25%가 고객용 뱅킹 앱 스토어를 출시할 것이라 전망합니다." 2014년 6월, http://www.gartner.com/newsroom/id/2758617

Akamai FASTER FORWARD

전 세계 콘텐츠 전송 네트워크(CDN) 분야를 이끌고 있는 Akamai는 빠르고 안전하며 신뢰할 수 있는 인터넷 환경을 제공합니다. Akamai는 웹 성능, 모바일 성능, 클라우드 보안, 미디어 전송과 관련된 우수한 솔루션을 공급하고 있으며 이 과정에서 사용 기기나 장소에 상관없이 소비자, 기업, 엔터테인먼트 경험을 최적화하는 방법을 크게 바꿔놓고 있습니다. Akamai의 인터넷 전문가들과 솔루션이 어떻게 기업의 성장을 뒷받침하고 있는지 자세히 알아보려면 Akamai 홈페이지(www.akamai.co.kr) 혹은 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 Akamai(@Akamai)를 팔로우하십시오.

Akamai는 미국 매사추세츠주 케임브리지에 본사를 두고 있으며 전세계 57여 개의 지사를 운영하고 있습니다. Akamai의 우수한 솔루션과 고객 서비스는 기업들이 사용자들에게 쾌적한 인터넷 경험을 제공할 수 있도록 도와줍니다. Akamai Korea는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다.

2015년 7월 발행.