Akamai

새롭게 부상하는 웹 애플리케이션 위협

웹 기반 비즈니스에 악영향 미치는 봇 리스크를 관리하라

아카마이 봇 매니저

SPECIAL REPORT Byline Network

PART 02

웹 기반 비즈니스에 악영향 미치는 봇 리스크를 관리하라

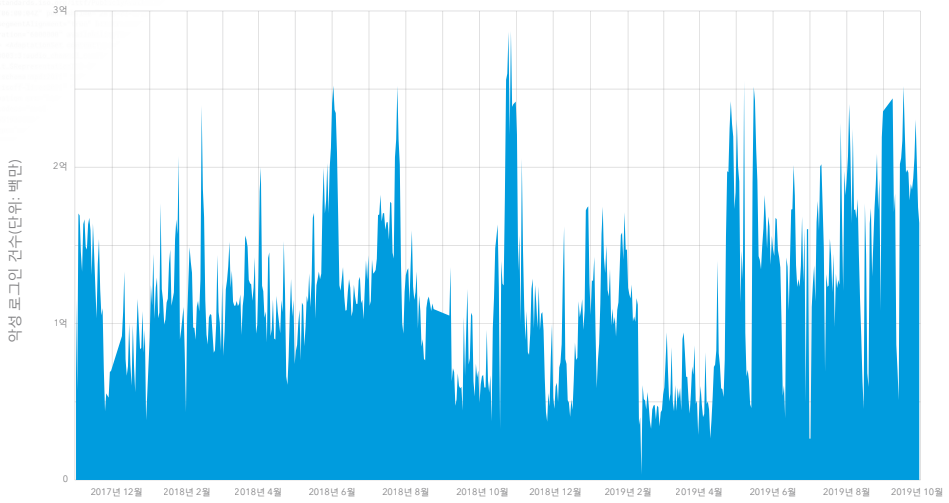
크리덴셜 스터핑(Credential Stuffing) 공격이 기승을 부리고 있다. 탈취된 사용자 로그인(인증) 정보로 봇(Bot)과 같은 자동화 도구를 활용해 수많은 웹사이트들을 대상으로 무차별 접속을 시도하는 계정 도용 공격이 갈수록 증가하고 있다.

범죄자들은 다양한 웹사이트에 동일한 아이디와 비밀번호를 사용하는 사람들이 많다는 점을 노려 또 다른 사용자 정보를 탈취하고 판매해 큰 수익을 거두고 있다. 만일 사용자 계정정보가 결제 페이지·계정에 연결돼 있으면 접속에 성공한 공격자들은 사기·부정 거래까지 수행할 수 있다.

이같은 공격은 업종에 관계없이 로그인 페이지가 있는 웹사이트를 운영한다면 모두 표적이 될 수 있다.

크리덴셜 스터핑 공격을 조사해온 아카마이는 2017년 하반기부터 게임, 금융, 미디어·엔터테인먼트, 유통·커머스 업계에서 매일 수억건, 연간 수백억건의 공격이 관측되고 있고, 또 매년 증가하고 있다고 밝힌 바 있다. 이에 따르면, 2017년 11월부터 2019년 3월까지 총 17개월간 전 산업군에 걸쳐 총 550억건의 크리덴셜 스터핑 공격이 발생했다.

일일 악성 로그인 시도 건수
2017년 11월~2019년 9월



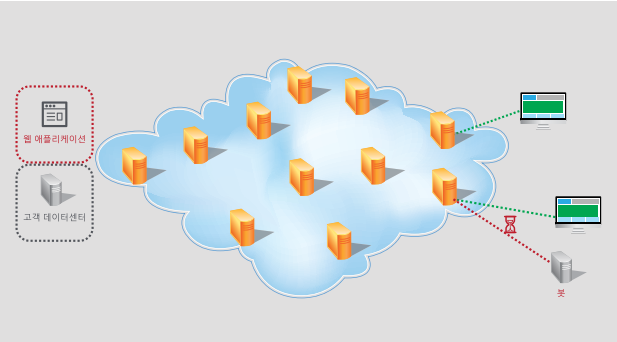
늘어나는 웹사이트 봇 트래픽, 무작정 '차단' 아닌 '관리' 필요

이러한 공격 피해를 막기 위해 많은 기업들은 웹사이트 접속에 캡챠(Captcha)를 추가로 사용하고 있다. 하지만 캡챠도 크리덴셜 스터핑 공격을 모두 방지할 수는 없다는 게 아카마이 전문가의 이야기다. 공격자가 합법적인 사용자 계정과 비밀번호 조합을 파악하게 될 경우, 얼마든지 계정에 접속해 범죄를 저지를 수 있다는 이유에서다.

공격자가 중요한 애플리케이션과 시스템에 접속하기 전에 봇이 수행하는 악의적인 행위를 탐지해 막을 수 있는 기술이 추가로 필요하다는 설명이다. 실제로 금융사 등 보안이 철저한 기업들은 크리덴셜 스터핑을 방어하기 위해 이같인 기술을 적용하는 추가 조치를 취하고 있다.

아카마이는 이같은 악성 봇에 의한 계정 및 데이터 탈취, 사기 행위 등을 차단할 수 있는 '아카마이 봇 매니저(Akamai Bot Manager)' 솔루션을 제공한다.

아카마이 봇 매니저는 웹을 기반으로 비즈니스를 수행하는 기업들이 다양한 봇 활동을 효율적으로 탐지·대응 조치할 수 있도록 지원하는 것이 특징이다. 크리덴셜 스터핑같은 사이버위협뿐 아니라 웹사이트 성능을 저하시키고 비즈니스에 악영향을 미치는 다양한 봇의 활동에 총체적으로 대응할 수 있다고 회사 측은 강조한다.



아카마이는 악성 봇을 막기 위해 웹사이트에 접근하는 자동화된 웹 트래픽을 모니터링해 차단하는 방법은 적절한 대응책이 아니라고 지적한다. 단순하게 일괄 '차단'하는 정책보다는 적절하게 '관리'해야 한다고 제시하고 있다. 웹사이트에 침투하는 봇 트래픽의 유형을 구분해 최적의 조치를 취하는 한편, 봇이 비즈니스와 IT에 미치는 긍정, 부정적 영향을 통제할 수 있어야 한다는 것이다.

아카마이가 자사 인텔리전트 플랫폼 트래픽을 분석한 결과에 따르면, 기업의 웹 트래픽 가운데 50% 이상이 봇에 의해 생성되고 있는 상황이다. 그러나 확인된 봇 트래픽은 전체의 30%에도 못 미친다. 이같은 트래픽에는 ▲크리덴셜 스터핑이나 디도스(DDoS) 공격과 ▲검색엔진 최적화(SEO) 스팸 등을 수행하는 자동화 도구 ▲재고 자산·가격 정보 등을 가져가는 웹 스크래핑(Web Scraping) ▲부정하게 광고 수익을 올리기 위한 자동 클릭 ▲한정판 제품과 서비스를 구입해 정상 고객이 사용할 수 없도록 만드는 거래 봇처럼 나쁜 용도로 사용되는 봇의 활동이 포함돼 있다.

반면에 챗봇을 통한 고객지원, 검색엔진 크롤러, 웹 아카이브, SEO, 고객 분석과 마케팅을 위한 웹·소셜미디어 스크래핑, 웹사이트 성능 모니터링, 특정 뉴스기사 또는 가격변동 콘텐츠 확보 등에도 봇을 널리 활용하고 있다. 사람이 직접 수행하기에 매우 비효율적인 업무나 업무수행이 어려운 시간과 상황에서 봇과 같은 자동화 기술이 이미 널리 쓰이고 있다. 디지털화가 확산되면서 보다 다양한 용도로 봇이 활용될 것으로 보인다.

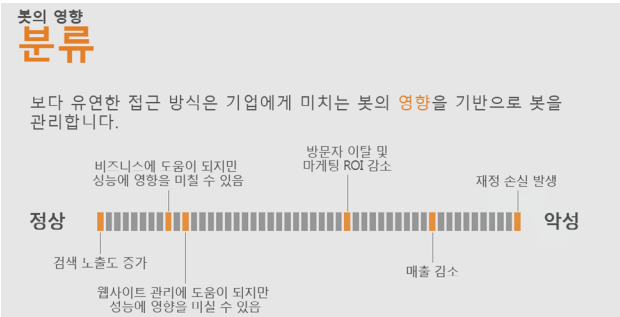
하지만 정상적으로 사용되는 봇이더라도 자사 웹사이트 성능을 떨어뜨리거나 인프라 자원을 많이 소모해 서비스에 영향을 미친다면 적절한 조치가 필요하다. 웹사이트 방문자 이탈, 마케팅 투자대비성과(ROI) 효과 감소, 금전 손실, 매출 감소에까지 영향을 줄 수 있기 때문이다.

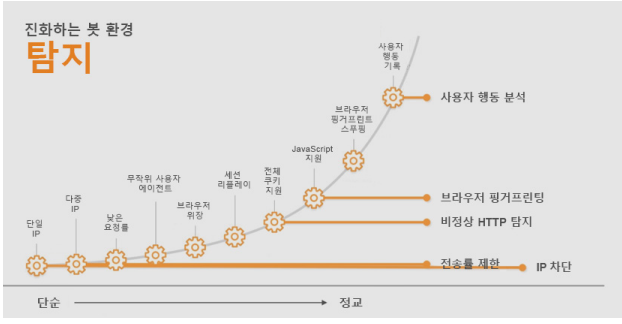
광범위한 봇 가시성과 인텔리전스 기반 탐지·분류·관리·보고 수행

아카마이는 기업의 웹사이트에 접속하는 봇 트래픽의 규모와 특징을 파악해 가시성을 확보하고 인텔리전스를 기반으로 효과적으로 관리해야 한다고 제시하고 있다.

웹사이트에 접근하는 활동이 실제 사용자인지, 봇에 의한 요청인지, 또 좋은 봇인지 나쁜 봇인지 탐지하고 구분하고 판별해 봇이 유발하는 영향도 평가할 수 있어야 한다고 강조한다.

더욱이 웹사이트를 방문하는 나쁜 봇들은 회피 기술을 사용해 탐지 기법을 우회하거나 좋은 봇으로 위장한다. IP주소를 여러 개 사용하거나 변경해 감추고, '로우앤슬로우(low and slow)' 기법으로 적은 수의 요청을 보내고, 쿠키를 변조·삭제하는 등 다양한 방식을 사용한다. 이같은 지능적이고 정교한 봇의 활동도 식별할 수 있어야 한다.

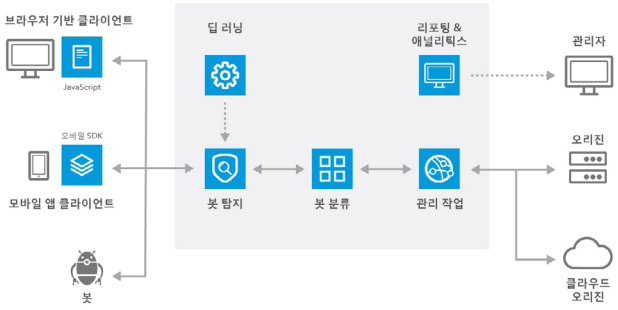




아카마이 봇 매니저는 봇에 대해 단순 차단 이상의 기능을 제공해 기업이 최적의 조치를 취하고 봇 트래픽이 비즈니스와 IT에 미치는 긍정적, 부정적 영향을 통제할 수 있도록 하는데 초점을 맞췄다.

전세계적으로 분산 배치돼 있는 아카마이 인텔리전스 플랫폼을 기반으로 세계 곳곳에서 광범위하게 활동하는 봇에 대한 높은 가시성과 인텔리전스를 확보해 기업의 웹사이트에 접속하는 봇 트래픽에 대한 효과적인 탐지·분류·관리·보고 기능을 수행한다.

아카마이 인텔리전트 플랫폼은 시간당 4억8500만개의 봇 요청과 매일 2억8000만건 이상의 로그인, 하루 평균 13억개의 클라이언트에 접속해 이뤄지는 상호작용, 최대 82테라비트(Tbps)의 트래픽을 바탕으로 봇 트래픽에 대한 가시성을 확보한다. 아카마이 엣지 서버에서 미리 설정된 봇 활동에 대한 작업을 수행하고 정상 트래픽만 오리진 서버로 전달하도록 설계돼 있다.



아카마이 봇 매니저의 탐지 기능은 시그니처와 평판 기반의 알려진 봇 탐지 뿐 아니라 브라우저와 쿠키 검사, 세션 검증, 행위 기반의 실시간 능동 탐지를 수행한다. 봇이 정교하게 진화함에 따라 탐지 기법을 계속 고도화하고 있다.

아카마이는 사용자가 웹사이트에 침투하는 봇 트래픽의 유형을 보다 쉽게 구분해 이해하고 세분화된 통제를 수행할 수 있도록 17개 카테고리로 분류하고 있다. 웹 검색, SEO, 애그리게이터, 모니터링 등의 유형으로 분류하고 있다. 이같은 카테고리를 바탕으로 1400여개의 알려진 봇의 시그니처 디렉토리를 운영한다. 아카마이 클라우드 보안 인텔리전스의 데이터 분석 엔진과 고객 기반을 활용해 알려진 봇을 지속적으로 업데이트하고 있어, 널리 사용되는 봇 트래픽을 신속하고 간편하게 식별할 수 있다.

비즈니스와 IT인프라에 미치는 영향을 고려해 고객사에서 직접 봇 시그니처와 카테고리를 커스터마이징하고 손쉽게 관리정책을 생성할 수 있도록 지원한다.

또한 알려지지 않은 새로운 봇을 식별할 수 있도록 행동 분석, 브라우저 핑거프린팅 인식, 비정상 HTTP 탐지, 높은 요청률, 워크플로우 인증 등의 다양한 기법을 사용한다. 아카마이 인텔리전트 플랫폼은 머신러닝을 통해 봇의 행동 특성과 평판 점수 등 인텔리전스 정보를 자동 업데이트하고 있다.

아카마이 봇 매니저는 봇 트래픽의 차단 또는 속도 저하, 응답 잠시 대기나 조건부 응답, 대체 콘텐츠제공, 대안 오리진으로 리디렉션 수행, 캡챠나 자격증명 요구 등 다양한 방법으로 봇에 대해 전략적으로 대응 조치를 취할 수 있도록 제공한다. 이를 통해 기업은 비즈니스에 미치는 부정적인 영향을 최소화하면서 봇을 적절히 관리할 수 있다.

아카마이 봇 매니저는 기업의 웹사이트에 영향을 줄 수 있는 봇 트렌드와 영향을 미친 봇 트래픽을 분석한 보고서를 제공한다. 카테고리, 탐지 방식, 최상위 URL 등 봇 트래픽 개괄적인 특성은 물론 시간 흐름에 따른 봇 행위 등 히스토리를 제공한다. HTTP 요청과 응답 샘플 로그도 포함돼 있다. 보고서는 기업이 봇 트래픽 활동을 보다 잘 이해하고 다양한 봇 유형에 대해 최적의 대응 방안을 결정할 수 있도록 세밀하고 자세한 정보를 준다. 기업이 사용하는 보안정보이벤트관리(SIEM) 솔루션과 연동해 웹 트래픽에 대한 가시성을 확장하고 경보(Alert)도 받아볼 수 있도록 지원한다.

아카마이 봇 매니저는 포레스터리서치가 13개 엔터프라이즈급 봇 관리 솔루션 제공업체와 제품을 평가해 2020년에 발간한 최신 '포레스터 뉴 웨이브 : 봇 관리' 리포트에서 리더로 선정됐다. 이 보고서에서 아카마이 봇 매니저는 봇 공격 탐지와 대응, 관리 사용자인터페이스(UI), 보고 및 분석, 피드백 루프, 성능 메트릭스, 로드맵, 시장 접근 측면에서 차별성을 인정받았다.

포레스터리서치는 "아카마이는 광범위하게 사전 정의돼 있고 커스터마이징이 가능한 공격 대응 방법을 제공한다"라면서 "엣지에서 봇에 대응하는 기업으로 가장 적합하다. 아카마이의 콘텐츠전송네트워크(CDN) 및 보안 고객은 봇 관리를 보다 쉽게 구축해 다른 기능과 통합할 수 있다"는 점을 강점으로 꼽았다.

Akamai

새롭게 부상하는 웹 애플리케이션 위협

웹 기반 비즈니스에 악영향 미치는 봇 리스크를 관리하라

아카마이 봇 매니저

Byline Network
byline.network
발행 바이라인네트워크 **취재/글** 이유지 기자 yjlee@byline.network **문의** byline@byline.network