



새롭게 부상하는 웹 애플리케이션 위협 개인 신용카드·금융정보 빼가는 웹 스크립트 공격을 막아라

아카마이 페이지 인티그리티 매니저

SPECIAL REPORT

Byline Network



PART 01

개인 신용카드·금융정보 빼가는 웹 스크립트 공격을 막아라

비대면 서비스 이용이 확산되면서 전자상거래(이커머스)가 크게 성장하고 있는 가운데, 물품 구매를 위해 웹페이지에 사용자가 입력하는 신용카드 결제정보를 가로채는 웹 스키밍(Skimming) 공격이 기승을 부리고 있다.

웹페이지에 악성 스크립트 코드를 심어 결제정보를 가로채는 이 공격은 웹 스키밍 또는 폼재킹(Formjacking) 공격이라고 불린다. 폼재킹은 입력양식(Payment Form)에 담긴 정보를 가로채간다(Hijacking)는 의미를 담은 합성어다.

지난 2018년 하반기부터 올해까지 계속해서 이같은 공격 피해가 대거 발생하고 있다. 온라인상에서 구매와 결제 서비스가 일어나는 크고 작은 유통·소매 서비스 기업 사이트들이 줄줄이 당했다. 38만 건의 고객 신용카드 결제정보를 유출한 영국항공을 비롯해 9개월 넘게 침해 공격이 진행됐지만 알지 못했던 티켓마스터, 유명 백화점 체인인 메이시스(Macy's) 등이 대표사례다. 대부분 사이버범죄집단인 '메이지카트(Magecart)' 소행으로 지목되고 있다.

여러 공격그룹들로 이뤄진 것으로 보이는 메이지카트는 웹 기반 카드 스키머라 할 수 있는 악성 자바스크립트 코드를 타겟 결제 페이지에 심어놓는다. 사용자가 웹사이트에서 물품을 구매한 뒤 이름, 주소, 지불카드 등의 정보를 입력하고 결제하기 버튼을 눌러 해당 정보를 제출할 때 악성코드를 이용해 해당 정보를 자신

의 서버로 전송한다. 공격자는 이 정보를 다크웹에서 금융정보와 개인정보를 판매하거나 부정거래를 시도해 수익을 거둔다.

사실 스크립트를 변경해 악성코드를 삽입하는 공격 기법은 새로운 것은 아니다. 하지만 공격자들은 결제정보를 몰래 가져가기 위해 스키머 코드 사용뿐 아니라 점점 더 다양하고 정교한 수법을 쓰는 것으로 보고되고 있다. 메이지카트는 초창기에는 주로 온라인 쇼핑 장바구니 시스템으로 사용되는 마젠토(Magento) 플러그인 취약점을 악용해 해킹하는데 중점을 뒀지만, 다양한 방식의 폼재킹과 공급망공격 기법을 동원하고 있다. 공격에 성공하기 위해 표적에 따라 전술과 기법을 바꾸면서 맞춤형 공격을 벌이고 있는 것으로 분석된다.

이들은 파트너사가 개발한 웹페이지나 플러그인, 소프트웨어의 취약점을 이용해 코드를 변경하고 스키밍 코드를 삽입함으로써 수많은 사용자가 이용하는 최종 표적 웹사이트에 악성코드를 심는 방식을 주로 이용한다.

티켓마스터 침해사고의 경우, 메이지카트는 고객지원에 사용된 챗봇업체인 인벤타, 소시아플러스 등 파트너사 프로그램의 취약점을 이용해 악성 자바스크립트 코드를 삽입·실행시키는 방식으로 티켓마스터 웹사이트까지 영향을 미칠 수 있게 했다. 이를 통해 티켓마스터 고객의 카드 정보를 캡처해 자신들의 명령제어(C&C) 서버로 전송했다.



2019년 11월 이커머스 사이트 지불결제 페이지에 자바스크립트 스키머 공격을 벌여 탐지된 핍카(PIPKA)는 인코딩 및 암호화로 콘텐츠를 숨겼고, HTML 이미지 소스 태그 요청을 사용해 공격자가 제어하는 웹사이트로 유출한 뒤 스스로 코드를 삭제했다. 이 핍카 공격은 비자(VISA)가 발견했다.

이러한 웹 스키밍 공격은 리테일, 미디어, 서비스 업계를 중심으로 다양한 산업에서 일어나며 꾸준히 증가하고 있다. 메이지카트 그룹이 처음 이같은 악성 웹페이지 스크립트 공격을 대중화시킨 후 다른 공격자들도 널리 사용하고 있는 것으로 분석된다. 온라인에서 사이버범죄자들끼리 악성코드를 공유하기도 한다.

보안전문가들은 지금까지 알려진 이같은 웹 스키밍 공격 사례는 빙산의 일각으로, 실제 공격 건수는 훨씬 많을 것이라고 경고하고 있다. 전세계 수만개에서 수백만 사이트가 당했다고 보는 경우도 있다. 메이지카트를 지속적으로 추적하고 있는 한 보안업체는 200만개 넘는 웹사이트가 침해됐다는 분석을 내놓기도 했다.

수많은 서드파티 소스로
구성되는 웹사이트, 보안관리에 취약

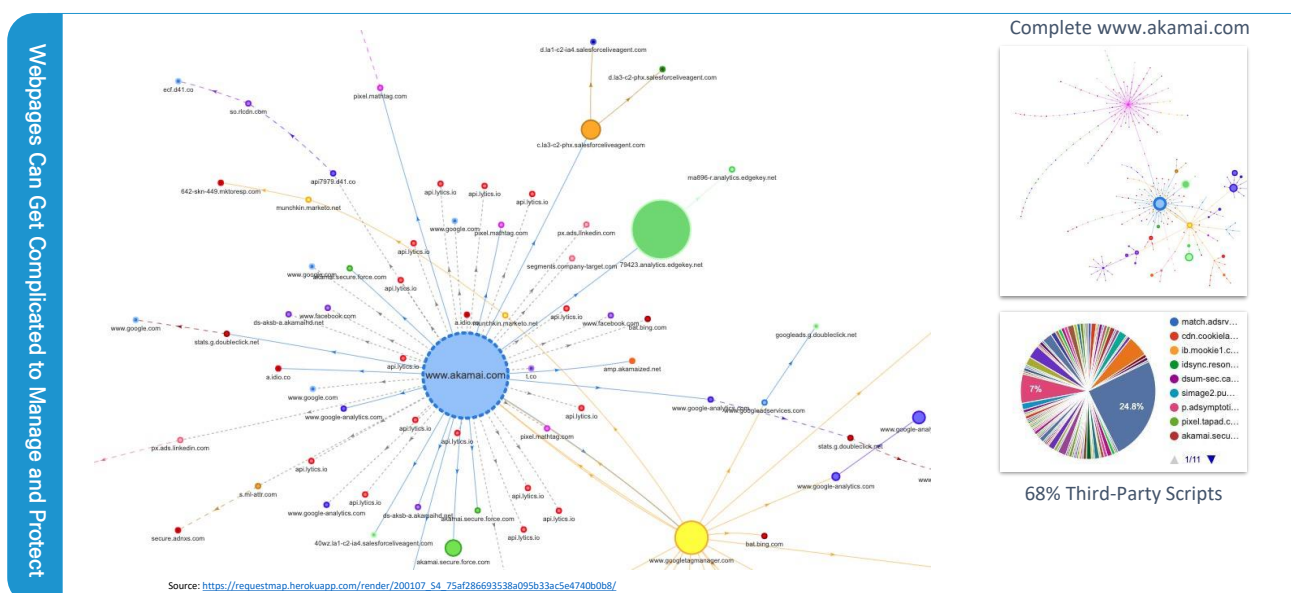
웹 스키밍 공격이 기승을 부리고 있고, 수많은 웹사이트가 유사 리 피해를 입는 이유는 무엇일까. 간단하게 말하면 웹 보안성이 미비하기 때문이다.

아카마이가 최근 7일 동안 1억1000만 페이지뷰에서 거의 50억 개의 자바스크립트 실행을 분석한 결과, 약 1000개의 취약점을 발견했다. 그만큼 웹 스키밍 공격에 노출되기 쉬운 상황이다. 단 한 개의 취약점만으로도 민감한 사용자 데이터 도난으로 이어질 수 있지만, 보안을 강화하는 것이 간단치는 않다.

요즘 웹사이트는 서로 다른 개발사가 만든 수많은 웹페이지와 스크립트로 구성된다. 대개 수십개의 서드파티 소스를 사용한 다. 오픈소스와 상용소스, 라이브러리를 조합해 웹사이트를 만든다고 볼 수 있다. 이 가운데 다수는 사용자 브라우저에서 스크립트를 실행한다.

지불결제 서비스, 계정 관리, 개인정보 양식에 사용되는 민감한 정보 페이지를 포함하는 서드파티 스크립트는 사용자 경험을 향상시키기 위한 필수요소다. 손쉽게 필요한 서비스를 추가하거나 수정할 수 있고, 개발사에서 유지관리도 해주는 것이 장점이다.

아카마이에 따르면, 수많은 웹사이트에서 타사 스크립트를 사용하는 비중은 평균 56%이다. 아카마이가 고객의 아카이브된



HTTP 데이터를 바탕으로 분석한 결과 데스크톱 웹 콘텐츠의 61%, 모바일 콘텐츠의 68%가 서드파티 콘텐츠였다. 아카마이는 자체 홈페이지에서 수십개의 스크립트를 사용하고 있는데, 이 가운데 약 70%가 외부 소스로 나타났다.

하지만 타사에서 제공·관리하는 스크립트에 대한 가시성과 통제력을 가질 수 없는 것이 현실이다. 여기에서 보안 문제가 발생한다. 빠르고 편리하게 웹서비스를 만들 수 있지만 보안관리가 취약해질 수 있다.

통 레이튼 아카마이 최고경영자(CEO)는 “일반적인 웹사이트는 대부분의 콘텐츠가 제3자 콘텐츠로 구성된다. 오픈소스 라이브러리에서 온 코드이거나 마케팅, 사이트 성능 분석, 광고 등 서드파티 파트너와 연결된다. 서드파티 코드는 제4, 제5의 출처와 연결된다. 때문에 사이트를 온전하게 제어할 수 없다. 사용자가 웹 사이트에 방문하면 서로 다른 출처의 콘텐츠를 다운받게 되는데, 여기에 악성코드가 포함돼 있다는 문제가 있다”고 지적했다.

레이튼 CEO는 “해당 웹사이트가 보안상 문제가 없더라도 해킹된 제2, 제3의 출처에서 악성코드를 다운로드하게 되면 신용카드 번호, 휴대폰 번호, 주소 등 양식(Form)에 기입하는 모든 정보를 유출할 수 있다”면서 “폼재킹 위협이 두드러지고 있다”고 말했다.

웹사이트 운영사에서 파트너사가 시큐어코딩 등 보안 개발은 물론, 취약점과 보안성을 면밀하게 테스트, 분석하고 검증해 빠르게 조치하도록 강제하는 것은 쉬운 일이 아니다. 더욱이 웹페이지 스크립트는 잦은 변경으로 매우 동적인 특성을 띠기 때문에 보안 결함이나 취약점을 노출하기 쉽다. 보안 개발을 하는데 시간도 오래 걸린다.

웹 스키밍같은 스크립트 공격은 사용자 브라우저단에서 실행해 정보를 탈취하기 때문에 탐지하기 어렵다. 네트워크 침입차단 시스템, 침입방지시스템(IPS)은 물론 웹 서버를 보호하기 위한 웹애플리케이션 방화벽도 방어하기 힘들다. 애플리케이션 보안 정책을 너무 엄격하게 적용할 경우 스크립트가 제공하는 이점이 줄어들 수 있다는 문제도 있다.

결국 공격을 막기 위해서는 웹사이트 소스코드와 스크립트를 지속적으로 모니터링하고 검사해 무결성을 유지할 수 있어야 한다. 그리고 서버는 물론 클라이언트(사용자)단 브라우저 대상 감시와 보호 조치를 수행하는 것이 매우 중요하다. 기존 정책 기반 보호를 넘어 의심스러운 행위를 실시간 탐지할 수 있어야 효과적으로 지능적인 스크립트 공급망공격을 감지하고 대처할 수 있다.

최신 웹브라우저에서 제공하는 CSP(Content Security Policy)와 SRI(Subresource Integrity) 보안 기능을 적용하면 무단으로 소스코드가 변경·삽입되거나 악성코드가 실행되는 위험을 완화하는데 도움이 된다. 나아가 전체 보호 대상 페이지에 스크립트를 심어 브라우저상에서 감시해 데이터 탈취·전송 시도와 같은 악성 활동을 인지하고 막을 수 있는 방안을 마련해야 한다.

바로 아카마이의 ‘페이지 integrity 매니저(Page Integrity Manager, 이하 PIM)’가 제공하는 방식이다.

웹사이트 구축 단계에서 감시와 모니터링을 위한 자바스크립트 코드를 전부 집어넣는 것은 쉽지 않은 일이다. 아카마이 PIM은 클라우드 기반 엣지 플랫폼을 활용해 원래의 소스를 전혀 손대거나 웹사이트·페이지 개발·운영사가 수정하지 않아도 스크립트 코드를 손쉽게 추가·적용할 수 있는 것이 특징이다.



아카마이는 전세계 콘텐츠전송네트워크(CDN) 선두기업이다. 클라우드 기반의 아카마이 인텔리전트 플랫폼(Akamai Intelligent Platform)은 세계 140여개국 1000개 도시와 4000여 지역에 분산 구축돼 있는 20만여대의 엣지 컴퓨팅 서버로 구성돼 있다. 이같은 분산 엣지 플랫폼을 기반으로 이용자들이 웹사이트와 콘텐츠·애플리케이션 서비스를 빠르고 안정적으로 보다 안전하게 이용할 수 있도록 지원한다. 아카마이가 주력하는 사업 분야는 크게 대용량 미디어와 콘텐츠의 빠른 전송, 웹 성능 향상, 보안 서비스로 구분된다.

아카마이는 최근 기업의 인프라와 웹사이트, 사용자를 보호하기 위한 투자를 강화하면서 다양한 보안 서비스를 확대 제공하고 있다. 디도스(DDoS)와 해킹으로부터 웹사이트와 애플리케이션을 보호하는 보안 솔루션으로는 ▲코나 사이트 디펜더(Kona Site Defender) ▲프로렉시(Prolexic) ▲웹 애플리케이션 프로텍터(Web Application Protector) ▲페이지 integrity 매니저(Page Integrity Manager) ▲봇 관리를 위한 봇 매니저(Bot Manager) 등이 있다. 멀웨어와 피싱 공격, 데이터 유출 공격으로부터 안전하게 기업을 보호하는 제로트러스트·엔터프라이즈 보안 솔루션으로 ▲엔터프라이즈 애플리케이션 액세스(Enterprise Application Access) ▲엔터프라이즈 디펜더(Enterprise Defender) 등도 제공한다.

아카마이 PIM, 스크립트 위협·공급망공격으로부터 웹 보호

아카마이 PIM은 신용카드 스키밍과 크리덴셜·개인정보를 훔치는 폼재킹 공격을 비롯해 웹브라우저단에서 발생하는 스크립트 위협을 탐지, 웹사이트를 보호하는데 특화된 서비스다.

취약한 자바스크립트 리소스에서 실시간 행위 기반 탐지 기술로 악의적이거나 의심스러운 활동을 탐지해 은밀하게 이뤄지는 공급망공격을 효과적으로 차단할 수 있도록 설계됐다.

아카마이 PIM은 실제 사용자 세션에서 스크립트 동작을 지속적으로 분석해 악의적인 행위를 식별한다. 머신러닝과 휴리스틱 분석, 서명, 위험지수화 모델을 이용해 자바스크립트 워크로드와 브라우저 안에서의 활동을 모니터링한다. 아카마이 보안 위협 인텔리전스를 활용해 위협 정보에 대한 정확성을 높여 대응 조치에 대한 판단을 내릴 수 있도록 돕는다. 아울러 공개 노출된 취약점(CVE) 데이터베이스도 지속적으로 분석해 실행되는 자바스크립트 코드에서 알려진 취약점을 파악해 관련 악성 행위를 차단한다.

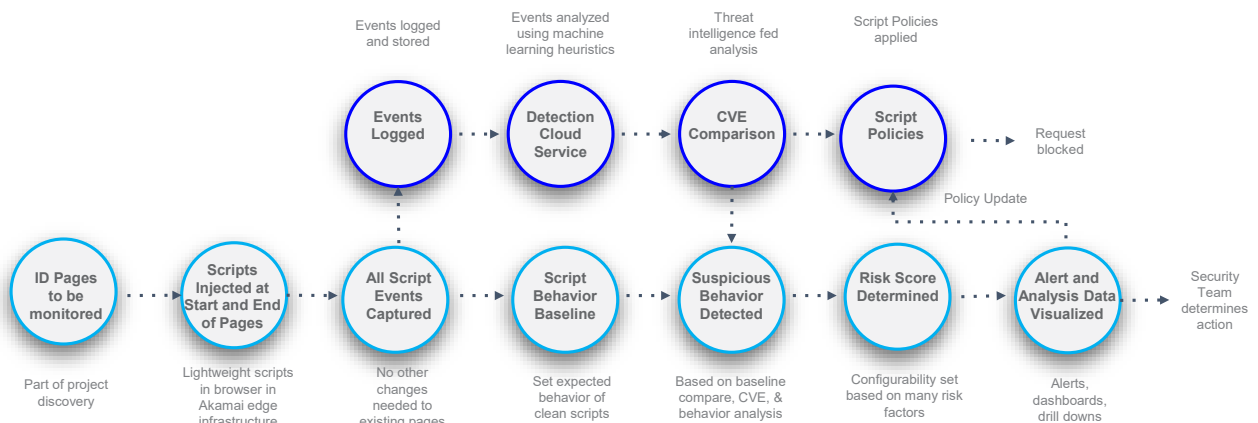
악성 행위 모니터링을 위해 아카마이의 클라우드 엣지 인프라를 활용해 웹페이지나 인프라 변경 없이 경량 스크립트를 삽입

한다. 이를 통해 몇 분 내에 구축해 바로 스크립트 행동 분석을 시작할 수 있는 것이 특징이다. 이 때 쿠키, 네트워크 목적지, 로컬 스토리지, 중요 데이터 입력 또는 오리진 도메인별 이벤트 접근을 모니터링하거나 스크립트 행위를 제한하는 런타임 자바스크립트 실행 정책을 미리 설정할 수 있다. 또한 클린 스크립트에서 기대되는 행위를 기준으로 삼아 비교해 의심스런 행위도 탐지할 수 있다.

아카마이 PIM은 의심스러운 동작이 탐지되면 바로 보안팀에 알려준다. 감염된 사용자 수, 접속된 데이터, 내보내기 대상 등과 같은 다양한 위험요소를 바탕으로 위험수준을 점수로 나타낸다. 위험지수가 높은 이벤트에 우선순위를 부여해 실시간 알림 기능을 제공한다.

대시보드에서는 웹페이지에서 실행되는 모든 스크립트를 직관적으로 확인할 수 있다. 보안팀은 스크립트 카테고리 및 개수, 인시던트 종류 및 건수 등 세부정보를 한 눈에 살펴볼 수 있으며, 인시던트와 정책 위반, 취약점(CVE) 탐지 관련 내용을 보고서로 볼 수 있다.

How Does Page Integrity Manager Work?





새롭게 부상하는 웹 애플리케이션 위협 개인 신용카드·금융정보 빼가는 웹 스크립트 공격을 막아라

아카마이 페이지 integrity 매니저

Byline Network
byline.network

발행 바이라인네트워크

Copyright © 2020 BylineNetwork

취재/글 이유지 기자 yjlee@byline.network

문의 byline@byline.network