RiskIQ JavaScript Threats Module

Challenge

Digital businesses are successful online when their customers trust their brands, their e-commerce experiences, and the security of their personal data. In recent years, however, cybercriminals have targeted many companies' payment web pages with stealthy JavaScript attacks designed to steal customer payment information. Malicious code designed to capture data entered into web forms has become the primary attack pattern for breaches in the Retail, Professional Services, Finance, and Manufacturing industries.[1] Security executives need to be confident in their defensive postures outside the firewall, especially regarding their companies' own and third-party JavaScript in critical e-commerce assets. The alternative is headline-making breaches, reduced customer trust, loss of market share, lawsuits, and fines in the hundreds of millions of dollars.[2]

RiskIQ Solution

RiskIQ JavaScript Threats Module ensures customer trust in e-commerce by protecting companies' high-traffic payment pages and other critical web applications from JavaScript attacks. The module is part of a comprehensive platform for reducing threats to companies' internet attack surfaces. JavaScript Threats is the only enterprise-scale product trusted by the largest financial and e-commerce companies and powered by the insight of industry-leading experts on Magecart cybercriminals and JavaScript attacks. With JavaScript Threats, Security, IT, and web asset owners can gain visibility into their dynamic web attack surfaces, respond immediately to incidents, and preserve customer trust.

Benefits

Increased Visibility

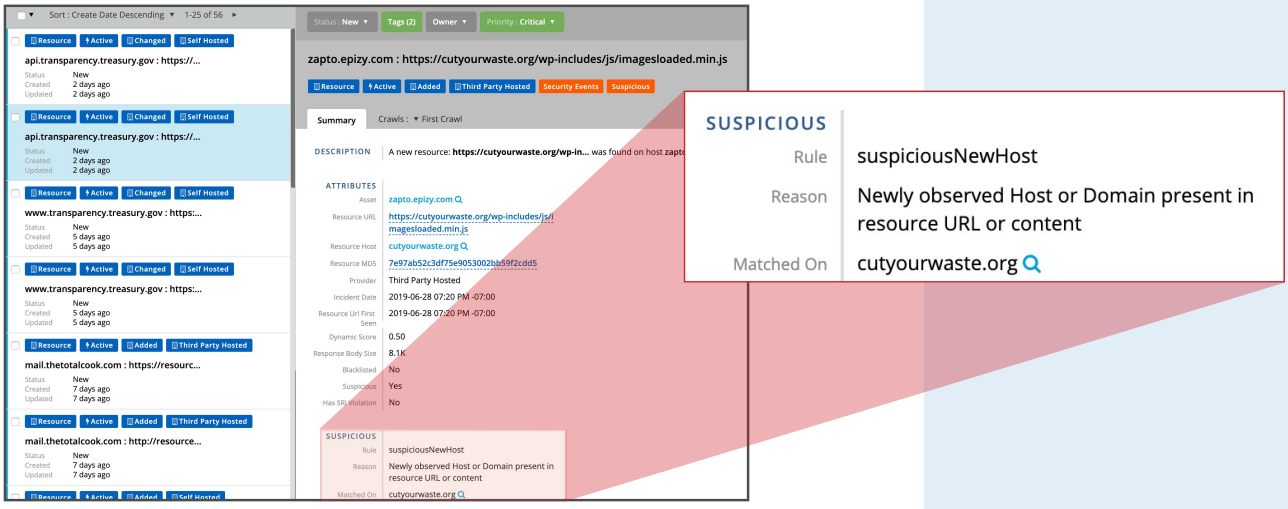
Gain visibility of web applications, JavaScript, third-party JavaScript, and associated data to increase the effectiveness of security programs outside the firewall.

Greater Efficiency

Accomplish more with current resources through automated JavaScript discovery, change tracking, alerting, and prioritization.

Faster Mitigation

Decrease response time to mitigate malicious and suspicious JavaScript changes and preserve customer trust.



Suspicious JavaScript resource detected by predictive detection engine

Key Features

Discovery and Inventory

JavaScript Threats discovers companies' JavaScript, third-party JavaScript, and associated data in minutes. This is accomplished through proprietary data-processing of virtual user web crawling, internet scanning, and collected data sets. The module automatically indexes, classifies, and assesses JavaScript resources to build complete, dynamic inventories. Each discovered web page has a list of current JavaScript resources, and each JavaScript resource has the following associated data: resource URL, resource host, dates when the resource was first and last seen, last observed hash of the resource code, last observed Subresource Integrity (SRI) validation and violation, and expected and actual SRI hashes. Security teams that automatically discover and inventory their web applications, JavaScript, third-party JavaScript, and associated data gain continuously updated visibility into their web attack surfaces, including third-party exposures.

Monitoring and Events

The module monitors web applications, JavaScript, and third-party JavaScript daily for changes that can trigger events for investigation by Security, IT, and web asset owners. Daily monitoring identifies added or changed JavaScript resources that may be hosted by the organization or by third parties and summarizes the results in a daily count with drill-downs into detailed lists. Each new or changed JavaScript resource has the following associated data: web asset where the change occurred, self- or third-party-hosted resource, parent host on which the change was observed, resource host from which the JavaScript is being loaded, JavaScript resource URL, and last observed hash of the resource code. Once an organization establishes a policy for change monitoring, based on the priority of web assets and probability of malicious JavaScript, events may be configured to automatically trigger for certain changes. Highly customizable classifiers and policies enable triaging and action on prioritized events. With change monitoring, security teams can immediately see a prioritized list of JavaScript changes and associated locations.

Threat Detection

JavaScript Threats detects malicious and suspicious JavaScript using blacklists and a predictive detection engine, both powered by the insights of RiskIQ threat research group. Malicious JavaScript is detected through blacklists of known malicious domains. When a known malicious domain appears within JavaScript code or resource URL, a blacklist incident is generated with the following associated data: artifact from the JavaScript resource that was matched on a blacklist, the matched blacklist, why the matched artifact was blacklisted, and blacklist incident information. Suspicious JavaScript is detected through a predictive detection engine that inspects code based on threat detection rules and correlates with proprietary data sets. Some detection rule examples include inspecting JavaScript code or resource URLs for IP addresses, newly observed hosts and domains, generic top-level domains, recent changes in typically static resources, and more advanced techniques. With JavaScript Threats, security teams can detect malicious and suspicious JavaScript changes and mitigate faster.

---

[1] *Verizon Data Breach Investigations Report: Executive Summary*, 2019.

[2] Information Commissioner's Office, "Intention to fine British Airways £183.39m under GDPR for data breach," July 8, 2019.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com