Fight Magecart

Protect your enterprise website against advanced attacks

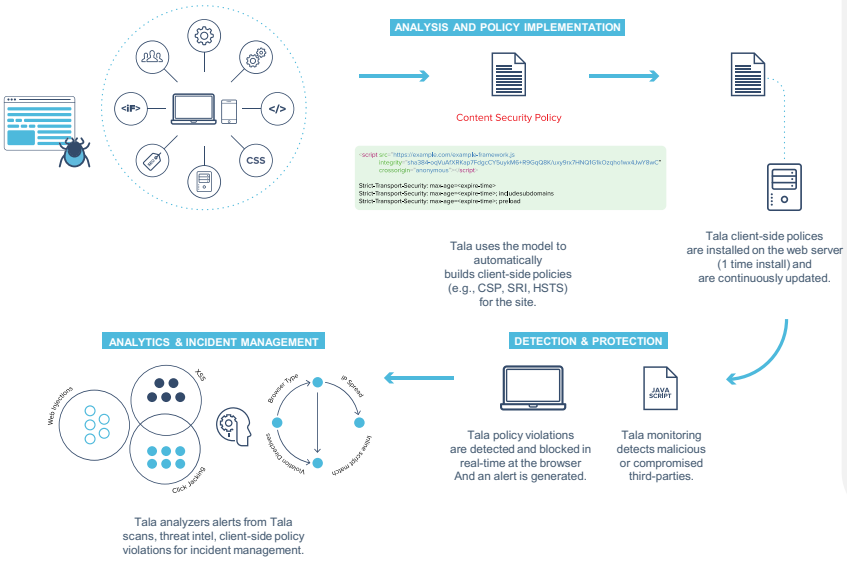
TALA

Challenge

Cybercriminal groups unleashed a wave of attacks against enterprise websites and web applications in 2018. Magecart is one the largest group of cyber-criminals targeting enterprise websites - security researchers have held Magecart responsible for breaches on websites belonging to British Airways, Ticketmaster, NewEgg, OXO and hundreds of other enterprises. Symantec estimates that 4,800+ websites are “formjacked” every month by groups like Magecart.

What is the problem? Magecart primarily launches their attacks by adding “card skimming” code into legitimate JavaScript files served on a site. When a user visits the site and types sensitive data such as credit card numbers, the “card skimming” code sniffs the information via the browser and sends it to a malicious server. Magecart has compromised Javascript files served from both first-party servers as well as third-parties integrated into the site.

- Traditional security mechanisms such as web application firewalls or SSL do not have any visibility into JavaScript execution at the client-browser level, and thus are unable to detect compromised JavaScript libraries or determine client-side malicious activity. This is illustrated by the fact that many of these websites had been breached for over 2 years, undetected. What’s worse, 1 in 5 of these sites were re-infected only a few days after the breach had been detected.
- There has been an explosion in third-party services on e-commerce sites without Infosec oversight, which has expanded the attack surface. Compromised or malicious domains could be inadvertently added to the site.
- Sensitive application and user PII data can be exposed to unauthorized third-parties. For e.g., third-party services could collect sensitive information such as credentials, passwords, SSNs as the user is typing them into forms on the site.
- Third-party services could allow “piggybacking” of other fourth- or fifth- party services that could expose the site to a broader attack surface that may go undetected.



Solution

Tala’s enterprise website security platform helps you protect your mission critical websites against Magecart-style attacks.

- **Understand your risks.** Tala’s cloud-based app behavior analysis provides a comprehensive risk assessment to help you understand data exposure and third-party related risks on your web applications and websites.
  - Tala automatically enumerates all third-party sources where content, code and iFrames are loaded from. Tala captures fine-grained behavior of third-party JavaScript.
  - Tala automatically detects pages where users input sensitive PII data., as well as third-parties that have access to the data.
- **Real-time protection and incident response.** Tala (once installed) monitors for anomalous data collection activity indicative of Magecart-style attacks and blocks attacks in real-time.
  - Tala monitors third-party Javascript behaviors while they execute in the browser, ensuring that they are only collecting data that they should have access to.
  - Tala continually monitors all the sources of JavaScript on the site and alerts if any of the domains are compromised.
  - Tala combines the power of threat intelligence, AI and our own fine-grained behavioral model to provide precise attack analytics and incident response capabilities.

Features & Benefits

- Comprehensive risk assessment: Tala provides comprehensive risk analysis of first- and third-party (and “piggybacked”) services on the site that could be exploited in a Magecart-like attack.
- Real-time detection and protection: Tala monitors client-browsers for anomalous behaviors and blocks compromised scripts.
- Full visibility into attack surface for incident response: Tala uses AI to classify attacks and notifies your incident response team if the system has detected a Magecart-style attack.
- Installs in minutes: Tala installs in minutes without requiring any changes to the application and without requiring any user-agents. We support all major web technologies like Apache, Nginx, etc.
- No impact to performance: Tala is not intrusive and adds minimal latency to page loads.

© Tala Security. All Rights Reserved

info@talasecurity.io / www.talasecurity.io