Protecting against 3rd Party APIs

haltdos

Adapting WAF to secure against 3rd Party APIs

This case study is about how Haltdos team added capability to enhance its WAF to provide 3rd party protection for a large multi-national organization for securing their ERP solution.

Background

Haltdos WAF, like any other WAF, works in reverse proxy mode. In reverse proxy, the client when connecting to a website firsts makes connection with the reverse proxy. After due validation, the reverse proxy then makes a connection with the webserver and mediates data transfer. Any connection initiated by the web server does not go through the reverse proxy as that is deemed internal to the webserver.

For anonymity sake, lets call the multi-national organization – "Big MNC". For compliance reasons, Big MNC had to share all invoicing data to regulatory authorities using APIs provided by the regulators. Due to sensitivity of the data, Big MNC wanted to implement a WAF solution to protect against internal threats as well as these 3rd party APIs.

Problem

A WAF should ensure comprehensive security for the protected web application. This includes blocking malicious requests, inspecting file uploads and preventing sensitive information leakage. However, there is no WAF solution the also ensures protection against 3rd part APIs implemented in the protected web application. As more and more applications are becoming distributed – with microservices and cloud adoption becoming the new norm, most applications do not work standalone. In fact, they are interwined and interdependent on specialized applications doing specific jobs. Protecting a web application against possible infection against these dependent APIs and services has become equally important.

Solution

The engineering team got to work on this new problemset and transformed Haltdos WAF to be capable of working as a reverse proxy as well as a forward proxy for intercepting all traffic to and fro from webservers. With this capability, Haltdos WAF was transformed to work as follows:

Blocking Malicious Requests: Haltdos WAF blocks malicious requests to protected web applications using a combination of signatures and machine learning.

Data Leak Prevention: Haltdos WAF prevents sensitive data leakage by masking webserver response.

Intercepting Webserver Requests: As a forward proxy, Haltdos WAF intercepts all requests initiated by the webserver and implements Data Leak Prevention techniques to protect against sensitive data leakage.

Intercepting 3rd Party Response: Haltdos WAF uses its existing signatures and machine learning capabilities to intercept and validate response from various 3rd Party APIs and block malicious response payload that might affect the web application.

Conclusion

Today, Haltdos WAF is a Industry-First Web Application and API protection solution that is capable of mitigating attacks vertically (incoming and outgoing request / response) as well as laterally (left / right traffic for inspecting API traffic) and provide 3rd party protection to protected web applications.

If you need to know more about how Haltdos WAF solution functions, reach us at support[at]haltdos.com