Signal Sciences

Preventing Wire Fraud with Signal Sciences

CHALLENGE

Snapdocs offers a loan closing automation application for the mortgage industry that provides a workflow for buyers, lenders, title and escrow representatives, and notaries. They needed technology that could provide the real-time visibility necessary to prevent account takeovers and upgrade their overall security posture.

Given the number of parties involved in a real estate transaction, there are numerous threat vectors: notaries, for example, do not always use strong passwords on their email accounts and sometimes share the same login credentials across websites. The net result: the mortgage industry is a major target of wire transfer fraud as attackers execute phishing campaigns against actors within the transaction chain to take over accounts. The attacker's ultimate goal is to utilize account takeovers to redirect funds to bogus third-party accounts.

To prevent fraud, Snapdocs sought to identify malicious actors' requests and other attack event patterns to prevent account takeovers. Additionally, they wanted faster visibility into attackers' web requests in order to trigger alerts to stop them.

"Aside from defending against the OWASP Top 10 attacks, Signal Sciences gives us enhanced visibility: we can now easily set up Power Rules to monitor and block activity that we couldn't before."

Evan Arnold, CTO

SOLUTION

To enhance the security of their digital toolset for mortgage closing, Snapdocs installed the Signal Sciences NGINX module and enabled blocking mode in production within 48 hours. After doing so, they not only blocked potential attacks but gained significant visibility provided by Power Rules.

Gain additional flexibility necessary to prevent attacks against known tactics

Requests originating from outside the United States are not common among the Snapdocs user base, so they utilized Signal Sciences Power Rules to block specific traffic emanating from non-U.S. IP addresses. Additionally, they've noted the possibility for high rates of fraudulent behavior associated with the Opera web browser due to its included VPN that anonymizes web traffic -- so Snapdocs tagged and blocked some user groups using the Opera web browser by evaluating the agent header in HTTP requests.

Streamline operations with alerts that surface security events quickly

With Signal Sciences, the Snapdocs security staff can investigate security threats faster by leveraging relevant alerts to surface events as they happen. "Signal Sciences has become our tool of choice for monitoring, tagging, and blocking traffic," Neel Palrecha, VP Engineering, says. "The Slack integration is extremely useful to watch events as they happen."

> People always say their tools are easy to install, but Signal Sciences really was. The team is fast and friendly, and the product is a powerful tool to combat bad actors.

Neel Palrecha, VP Engineering

Any App

Cloud, Containers, PaaS, and Serverless

Web Servers and Languages

Gateways and Proxies

Any Attack

OWASP Top 10

Application DoS

Brute force attacks

+ MORE

Any DevOps Toolchain

Slack

HipChat

Datadog

Webhooks

Splunk

SIEM/SOC tools via APIs

+ MORE