Identifying and Stopping Bad Bots

Web applications and APIs are the digital gateways to your company’s most valuable assets. But the combination of large-scale user credential data dumps that result from breaches, and cheap (or even free) automated toolsets make it easy for sophisticated adversaries to exploit web properties.

The Bot Threat

Bad bots present a constant threat to organizations: Over 90% of websites with login pages experience bot attacks related to credential stuffing or credential cracking. Moreover, 80% of sites with sign-up or application form pages are victims of bot activity aimed at creating fraudulent new accounts.

Bots can repeatedly carry out a number of different attacks—including content scraping, credential stuffing, application DDoS, web form abuse, token guessing, and more—without human intervention.

Defeating the Bot Threat with Signal Sciences

A proactive bot mitigation strategy empowers organizations to understand and block bot activity before it impacts your applications. An effective bot mitigation solution must provide two key features:

**Bot Visibility:** By inspecting specific attributes in HTTP requests and responses, Signal Sciences detects bots by observing and examining the context of incoming request traffic. This context is determined by our rules, lists, and classifications from 100 different types of bots, and can be displayed on our dashboards. Lists allow you to parameterize advanced Power Rules with business data you have collected, such as IPs, user agents, countries, wildcards, and more.

**Blocking Capabilities:** A powerful combination of thresholding, advanced Power Rules and predetermined lists allow organizations to customize their protections from known bots and bad behavior. Power Rules determine if incoming bot traffic is malicious and blocks those web requests from reaching the app origin or API endpoint.

SUMMARY

To protect web applications and APIs from bot activity, Signal Sciences provides our customers with the bot visibility and blocking capabilities needed to keep their web properties safe.
Signal Sciences patented thresholding and advanced Power Rules stop bots from exploiting your web applications and APIs, without impacting app performance or customer experience.

Advanced Power Rules provide customers a deeply customizable way to block traffic based on several criteria, including IPs, country of origin, submission behavior, and additional signals from our Network Learning Exchange (NLX), our IP reputation feed based on confirmed malicious activity collected from our customer base. The more bot signals we receive and parse, the more robust our protection against future attacks becomes for our entire customer base.

To protect web applications and APIs from bot activity, Signal Sciences provides our customers with the bot visibility and blocking capabilities needed to keep their properties safe.

---

1, 2 “Don’t Treat Your Customer Like a Criminal” — Tricia Phillips, Gartner Research