Detecting and Mitigating Bad Bots

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.

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

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.

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[1]. Moreover, 80% of sites with sign-up or application form pages are victims of bot activity aimed at creating fraudulent new accounts[2].

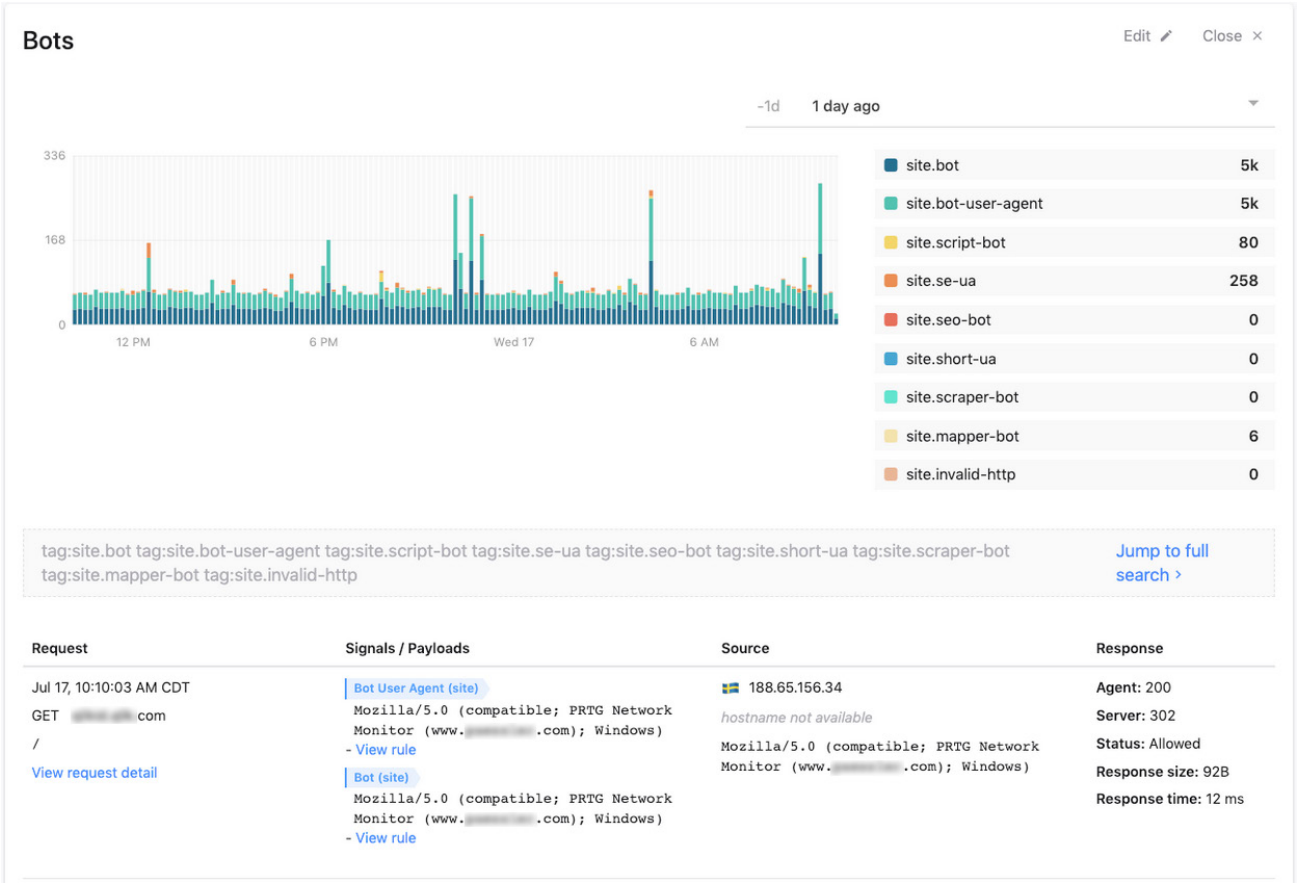
Bots can repeatedly carry out a number of different attacks—including content scraping, credential stuffing, application DDoS, web form abuse, token guessing, and more—without human intervention.

Meeting the Bot Threat Challenge 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:

- **Determine intent of automated traffic:** via our core rules, signals, and lists we enable customers to identify the intent of specific automated bot traffic and block those with malicious intent.
- **Classify malicious bots from good bots:** this classification helps customers determine what automated bot traffic should be blocked or allowed based on customer preferences.
- **Reject bad traffic and manage good traffic:** customers can block bad bad traffic and manage good traffic (i.e. traffic shaping or rate limiting via thresholds) from partners, specific IP lists, or specific types of configurable bots.
- **Determine bot traffic thresholds:** customers can leverage thresholding and rate limiting to defeat malicious bots.

With these four key capabilities, customers can derive risk scores per user session based on the surfaced data.



Example of a visualization in Signal Sciences console of determining and classifying requests based on the User Agent string along with other web request context.

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