THREATX

DATA SHEET

ThreatX Bot Defense

Stop bot attacks and other forms of malicious traffic automation.

The Rise of Bot Traffic

Malicious bots interfere with a customer's online experience, affect product availability, erode application performance, steal data, and even take over user accounts. And bot traffic continues to rise; up to 50 percent of Internet traffic is now generated by bots.

Organizations are awash in a sea of automated visitors, and the situation is only getting worse.

Attackers are now using solver services — software packages for purchase on the dark web that have "solved" vendors' bot detection defenses — to evade detection, along with other techniques like cycling IPs to avoid geo-location and low/slow bot attacks. All in all, attackers are finding new ways to make their botnets smarter and harder to detect.

Bots' Role in Modern Attacks

Savvy attackers know they can use bots to map your applications and create more sophisticated, successful attacks designed to target the discovered weaknesses. Let's break down how bots are used in the various stages of an attack.

- **Bot Reconnaissance:** Attackers use bots in this phase to gather information, allowing them to test systems without much effort. Common reconnaissance techniques are enumeration, web scraping, or probing an application to see how it reacts to requests from various locations.
- **Tuning Bot Tasks:** In this stage, attackers will begin tuning the botnet's activity based on the results from their reconnaissance. These requests are focused on targeting out-of-date API endpoints to steal sensitive data or programming the bots to only use IPs from certain locations.
- **Bot Evasion:** Modern botnets are getting smarter at evading detection thanks to solver services, IP rotation, as well as low-and-slow attacks. If an attacker can determine which bot defense solutions an organization has, attackers can program their botnets to evade that solution's detection.
- **Bot Diversion:** Bots are being used as a diversion so attackers can go unnoticed. To create this needle in a haystack effect, the botnet will generate large volumetric attacks to trigger thousands of alerts and overwhelm security teams while their exploitation attempts get buried.

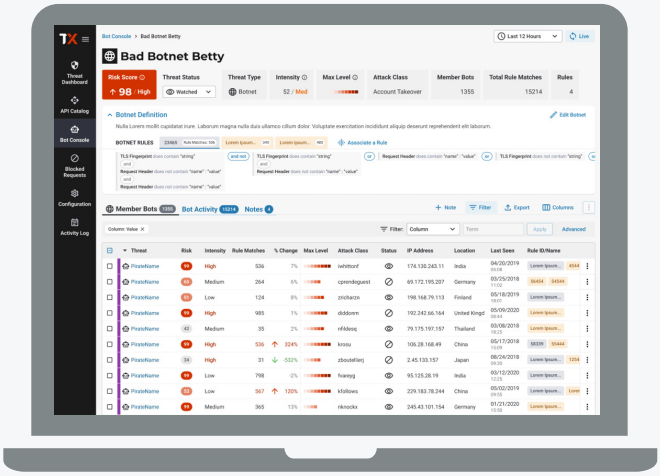
SEGPAY

Digital payment company Segpay was experiencing attacks from bots attempting combinations of credit card numbers to see if transactions would go through, running up operational costs with failed transaction fees. The bots were cycling through IP addresses, making blocking especially challenging. After partnering with ThreatX, the team is now tracking attackers' movements and blocking risky behavior at its onset. The Segpay team noted that:

> *"We look at our ThreatX dashboard and pinpoint whether attackers are just getting their feet wet, or really trying to exploit us. It's a good visual because we can see clearly what to focus on.*

ThreatX Bot Capabilities

ThreatX's managed API and application protection platform defends organizations from attacks by detecting, tracking, and blocking threats automatically, based on risk. ThreatX has many customers that rely on us to detect and block large-scale botnets as well as low-and-slow bot activity.



Distinguish Human From Automated Traffic

The number of advanced bots that can bypass security controls is increasing as they become smarter, easier to create, reprogram, and even rent. These advanced bots make a strong effort to evade detection while carrying out their attacks. ThreatX uses a combination of techniques to detect a wide range of automated threats without introducing additional friction like CAPTCHAs and other bot mechanisms that negatively impact customers' experiences.

- **Active Interrogation:** ThreatX challenges suspicious actors with active interrogation to see how they react when tar pitting traffic or returning web cookies.
- **Application Profiling:** ThreatX automatically profiles the application's "normal" behavior by monitoring usage and underlying services, enabling early identifiers of usage deviation.

Monitor Bot Activity at Scale

ThreatX's bot console provides teams with a powerful view for monitoring botnets and other forms of malicious, automated traffic. With its enhanced visibility, security teams can quickly identify and respond to changing automated threats before APIs and applications are affected or breached. Given the increasing use of bots to carry out volumetric attacks, such as credential stuffing, account takeover, and DDoS, the bot console is a necessity for maintaining a strong security posture in today's threat landscape.

- **Botnet Analytics:** Gain visibility into all bot activity and identify the top botnets generating malicious automated traffic – all within one view.
- **Effective Protection:** Investigate rapidly evolving bot activity to track and tune the effectiveness of ThreatX detections as attack patterns change.

Detect, Track, and Confidently Block Evolving Threats

The ThreatX platform is always monitoring, assessing, and blocking attacks – automatically. ThreatX uses attacker fingerprinting to track threat behavior over time no matter if they attempt to evade detection by cycling IP or user agents. It learns what threats to your system look like and stops them based on their risk level, so you can keep sites available and business humming.

- **Detect Automated Threats:** Stop various types of attack patterns like recon or automated threats.
- **Risk-Based, Real-Time Blocking:** Assess, monitor, and block malicious attempts automatically without manual intervention or worry of false positives.

ThreatX protects your APIs and applications against bot attacks and automated malicious traffic all while providing zero-day coverage with our Protection-as-a-Service, a dedicated team of experts that act as an extension of your team.

To learn more, get a demo of ThreatX bot defense.