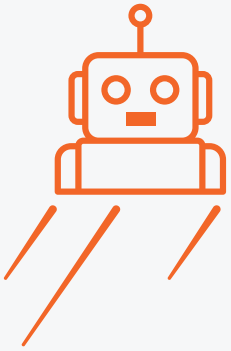
THREATX

DATA SHEET

Bot Management

Stop bot attacks and other forms of malicious traffic automation.

Bad bots can interfere with a customer's online experience, affect product availability, erode application performance, steal data, and even take over user accounts. ThreatX's integrated platform protects organizations from API and web application attacks with attacker behavior detection, real-time blocking, and more. ThreatX has many customers that rely on us to detect and block large-scale botnet attacks as well as low and slow bot activity.



The Rise of Bot Traffic

Bot traffic continues to rise and, in fact, up to 50 percent of Internet traffic is generated by bots, leaving organizations awash in a sea of automated visitors. Attacks against APIs and web apps almost always involve bots or botnets, and botnets are getting bigger and more sophisticated. Here are a few examples of how bots are becoming smarter:

- **Bots Avoiding Geo-blocking** - attackers use botnets made up of thousands of IP addresses; when they realize that certain countries, continents, or regions are getting blocked, they simply swap out those IPs and move where the requests are getting through.
- **Low and Slow Bot Attacks** - these attacks rely on using a wide range of distributed IPs. Each of these IP addresses is only executing one request, and doing so slowly — maybe once a minute, or maybe even once every five minutes. These look like legitimate requests, but they're enumerating through accounts to steal credentials.

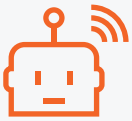
Bots' Role in Modern Attacks

Savvy attackers know that they can map your applications to understand which pages or API calls consume resources such as memory, session handles, or CPU cycles. Armed with that information, they can design a targeted and sophisticated multi-mode attack to consume resources, degrade your app's performance, and generally muddy the water while trying more pointed exploits. This is the outline of a modern bot-based attack.

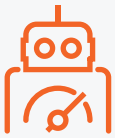
There are many ways attackers use bots in their cyberattacks, let's break down how these bad bots are used in the stages of a sophisticated, multi-mode attack.

read on for bot attack stages »

STAGES OF BOT ATTACKS



» **Bot Reconnaissance** - Attackers use bots in this phase to gather reconnaissance information because it allows them to quickly explore and test systems of potential vulnerabilities without being detected and without much effort on their part. Common reconnaissance actions for bots are API fuzzing or enumeration attempts, web scraping, credential harvesting, or seeing how an application reacts to requests being sent from IP addresses from certain countries.



» **Tuning Bot Tasks** - In this stage, attackers will begin acquiring or renting botnet capacity and tuning the bot's activity based on the results from their recon attempts. These tasks could be sending requests to an old, out of date API endpoint that was discovered to steal user data, using user credentials to access a vulnerable system, or flood an application past its resource capacity to be taken offline.

» **Launching a Multi-mode Attack** - Now that the attacker has bots targeting known weaknesses in the attack surface of their victim, it's time to launch the attack. A federated network of attack bots can make the attack "low and slow" and thus hard for defenders to detect. Each IP address is only making one request, maybe every minute, or maybe even five minutes. These requests look legitimate, but they're trying to steal credentials or sensitive data.

» **Bot Evasion** - More and more, attackers are using bots as distraction so they can go after the real target unnoticed. To create this needle in a haystack approach, they'll generate large, volumetric but "obvious" attacks like DDoS, SQLi, or XSS to overwhelm a security solution or trigger thousands of alerts for security to chase down. Then, the attacker's targeted exploitation attempts get buried under the alerts and are left unnoticed.

BEYOND IP BLOCKING

SEGPAY

Digital payment processing company, Segpay was experiencing cyberattacks that featured bots inputting a series of different credit card numbers into the system to see if any would get approved, which ran up their operational costs with failed transactions fees. The bots were cycling through multiple IP addresses, making blocking the attacks especially challenging. After partnering with ThreatX, the team is now following and learning about an attacker's movements over time, and, rather than trying to block every suspicious IP address, only blocking an attacker when there are clear signs of malicious behavior.

"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."

see how ThreatX can help »

THREATX

Bot Capabilities

Attacker Behavior Detection

ThreatX detects and follows a wide range of threats and malicious behaviors throughout the entire attack lifecycle. The phases of attacks are considered "states" and include the following:

- Reconnaissance
- Scanning
- Mapping
- Brute Force
- DDoS
- Exploitation
- Malware Communication

Attack Tactics are grouped into "classifications". These classifications include categories like:

- SQL Injection
- Software Detection
- Botnet Activity
- Evasion
- Directory Traversal

Our platform is designed to integrate multiple attack types over multiple toolchain variants, changing IPs, and time periods to stop modern, sophisticated attacks.

Active Interrogation

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, and some classes of their attacks may never be identified without advanced techniques. ThreatX employs advanced bot detection techniques like active interrogation and tar-pitting of traffic to see how suspicious actors react when challenged. Our bot detection techniques include:

- Testing support for redirection and cookie storage
- Javascript-based challenges
- Browser fingerprinting
- Testing how the suspicious entity handles other deceptive responses.
- Tarpit traffic to see if the entity goes away

Distinguish Human from Automated Traffic

The combination of bot detection techniques such as active interrogation and application profiling means ThreatX can reveal a wide range of automated attacks such as account takeover (ATO), credential stuffing, reputation attacks and more. To identify threats, ThreatX automatically profiles the application's "normal" behavior by monitoring usage and underlying services. Deviations often provide early indicators of threats without introducing additional user friction with CAPTCHAs and other bot mitigation mechanisms that negatively impact customers' experiences.

Detect and Block Attacks in Real-Time

ThreatX analyzes all inbound API traffic in real time, identifying and blocking attacks instantly, without the need to transfer threat data to another solution. This real-time monitoring enables ThreatX to execute advanced threat engagement techniques, such as IP fingerprinting, interrogation, and tar-pitting. These capabilities allow ThreatX to immediately identify and stop the most complex attacks, including large-scale bots and DDoS-level threats.

Advanced Attack Forensics

ThreatX uses AI/ML-powered single risk engine to identify key attributes of an attack with continuous monitoring all entity behaviors and correlates them into a unified risk score. Enumeration, fuzzing, reverse engineering, injections, broken authentication, all of these tactics will come together in some form of an attack, whether it be large scale or low and slow. That's why keeping the history of each suspicious actor is so important and allows ThreatX to identify the coordinated, stop the "low and slow" attacks that would normally fly under the radar.

Partner with AppSec Experts

ThreatX provides Managed Services and Security Operations to ensure our customers get the highest protection possible by streamlining deployment with onboarding support, followed by immediate protection with dedicated resources focused on threat hunting, zero-day protection, and 1:1 AppSec expertise.

ThreatX protects your APIs and apps against botnet attacks and automated malicious traffic while also providing zero-day coverage with our 24X7 SOC to act as an extension of your team.