Bot Attack Intelligence

NETACEA

Malicious bots are blindsiding businesses

According to the latest research around 25% of all web, API and mobile app traffic is made up of bad bots. These scaled, automated and increasingly sophisticated attacks equate to almost a 4% loss of revenue on average for businesses.

Malicious bots can breach customer data, steal intellectual property and cause damage to your brand and reputation. Any business with an online presence needs protection from these types of attacks that's based on solid threat intelligence.

Netacea's Bot Attack Intelligence is an up-to-the-minute intelligence feed containing information on where bot threats have been detected by Netacea in the wild.
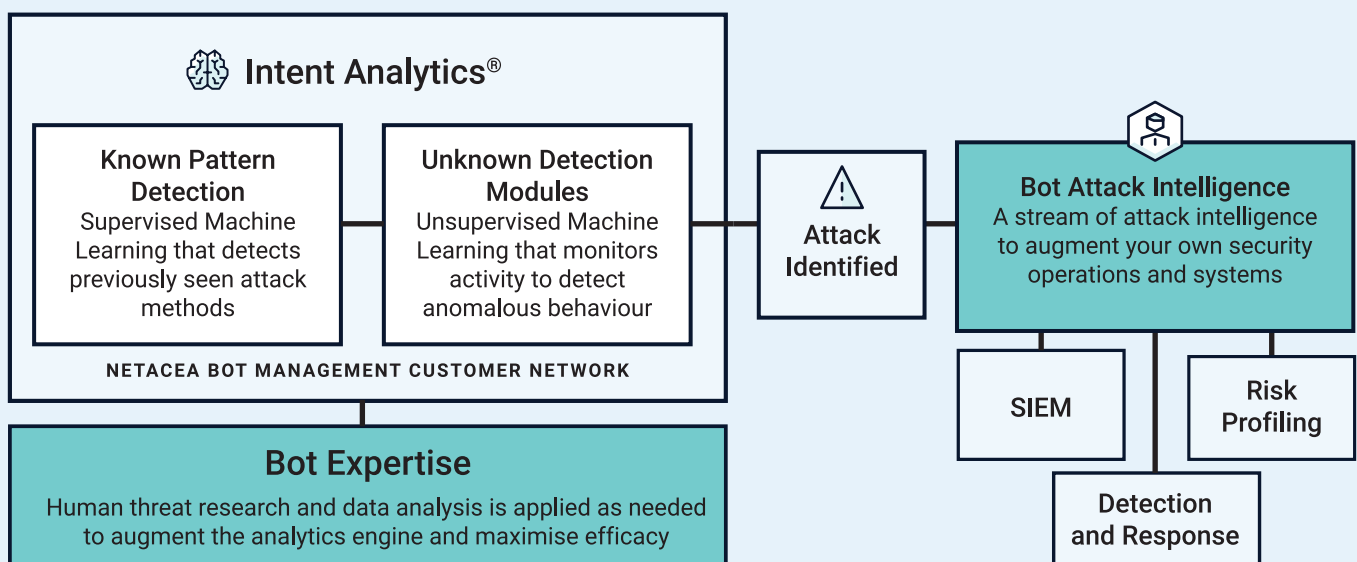
A unique view of malicious bot attack origins

This intelligence comes from Netacea's enterprise-grade Bot Management solution. Our technology uses machine learning to perform behavioral analysis of web and API traffic across billions of web requests every day.

This data is also correlated with information on proxy services used in bot attacks (including residential and data centre services) and augmented by Netacea's human threat research expertise.

The result is a feed of tens of thousands of malicious IP addresses validated for accuracy by some of the world's most highly visited websites who use Netacea to protect their brand and customers.

How can Bot Attack Intelligence be used?

This machine-readable data can then be rapidly integrated into existing security technologies like SIEM, SOAR and XDR platforms to aid in mitigating threats from bots.

Intent Analytics®

Known Pattern Detection
Supervised Machine Learning that detects previously seen attack methods

Unknown Detection Modules
Unsupervised Machine Learning that monitors activity to detect anomalous behaviour

NETACEA BOT MANAGEMENT CUSTOMER NETWORK

Bot Expertise
Human threat research and data analysis is applied as needed to augment the analytics engine and maximise efficacy

⚠️ **Attack Identified**

Bot Attack Intelligence
A stream of attack intelligence to augment your own security operations and systems

SIEM

Risk Profiling

Detection and Response

The Netacea difference

Purpose built to detect the most sophisticated bots

Bots can't hide their intent at the server level. We analyze all visitor behavior to websites, mobile apps and APIs protected by Netacea. This happens on the server side to identify attack patterns and anomalies to detect traffic from bad bots.

Continuous detection

Other bot detection tools only check a visitor on first arrival. Instead, Netacea reassesses every user after every request to ensure bots are detected even if they appear human on first contact.

6 times better bot detection

Our approach is radically different to other outdated bot management solutions, by focussing on using behavior to identify malicious intent inside across all visitors we can provide detection of bots that's up to 6 times better than the rest.

Unmatched bot threat expertise

Netacea's human threat research team augments our detection technology through proactive research into known threat actors, their tactics and techniques.

Netacea receives the highest score in the Bot Detection criterion in The Forrester Wave: Bot Management, Q2 2022 report

Forrester, a leading research organisation that provides advice on existing and emerging technology, identified Netacea as a Strong Performer in its 2022 evaluation of the bot management market, despite being "among the smallest vendors in this Forrester Wave." Netacea also received the highest possible score for Threat Research.