Botnet Detection - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Botnet Detection Market size is estimated at USD 1.12 billion in 2024, and is expected to reach USD 3.59 billion by 2029, growing at a CAGR of 26.18% during the forecast period (2024-2029).

Botnet detection has accumulated widespread attention among cybersecurity professionals and technology companies worldwide. As technology progresses across the globe, the risk connected with the misuse of advanced technology has also grown over the past years. Botnet attack is one such violation of the user's privacy where a user's computer is being controlled and managed by a third party. The botnet has been developing as one of the principal threats owing to the growing cybercriminals' capacity to infiltrate any of the devices which are attached to the internet across the globe.

Key Highlights
-In recent years, there has been a proliferation in the Internet of Things (IoT) technology, which added additional endpoints for attackers. The emergence of new distributed denial of service (DDoS) bots at an increasing regularity attributes to the changes in the landscape. After the reporting of the Mirai botnet in 2016 and the subsequent leak of the malware's source code, the number of variants of this family of botnets has been growing steadily, its success being augmented by an environment of poorly-managed IoT devices.
-Due to the growth of mobile devices and cloud computing that act as attack surfaces, it has become easier for malicious bots to disguise themselves. The hackers traditionally used malicious bots for money-making activities. Now, they are increasingly used for industrial espionage and even influencing elections. Companies have to index attacks intensively and study them before countering them with their strategies. In December 2021, Google disrupted the 'key command and control infrastructure' of Glupteba, a botnet that compromised nearly one million Windows devices worldwide, and filed a lawsuit against its operators.
-The convergence of physical security with the IP network expands the attack surface for cybercriminals. Criminals have expanded

from targeting specific user accounts or regions to conquering entire internet entities. In September 2021, the Russian search engine Yandex was attacked at a record level by a distributed denial of service attack by the Meris botnet. The attack destroyed the company's web infrastructure with millions of HTTP requests before hitting a peak of 21.8 million requests per second (RPS) and destabilizing its existing infrastructure. The Russian DDoS mitigation service Qrator Labs identified the attack and noted that the DDoS attacks leveraged HTTP pipelining originating from over 250,000 infected network devices from Mikrotik.
-However, the lack of skilled cybersecurity professionals to disrupt such attacks continues to be a vulnerability that companies face. The companies are recruiting new cybersecurity professionals to train them with the evolution of botnets and use detection software to prevent potential attacks. Mergers among the big players in the market are another solution the companies have come up with to strengthen their services and product portfolio.
-COVID-19 spam was a prevalent issue during the lockdown period and can be primarily divided into two types: with and without attachments. Vendors have had to rapidly roll out new offerings that match the pace of attackers worldwide. In July 2021, as the second wave of the virus surged, Neustar Inc. introduced UltraBot Protect to deliver enhanced capabilities to users to examine traffic patterns to determine risk, easily set rules, and block nefarious web application traffic through an intuitive and comprehensive user interface or the company's extensible API, which deliver actionable data to manage incoming traffic or risks better.

Botnet Detection Market Trends

Media and Entertainment Industry is Expected to Register Significant Growth

- Media & entertainment enterprises spend a significant share on advertisements to create brand awareness and attract new customers. Botnet detection techniques are majorly adopted in media & entertainment industries to reduce vulnerabilities towards advertisements. This sector is expected to be the fastest growing due to the increasing bot attacks on this sector through ad frauds. The involved risks and end-points increase with the rising number of advertisements on different platforms.
- Botnet attacks may run illegal activities such as spreading fraudulent content, price scraping, and others that affect the brand. Advertisers constantly monitor networks and servers to detect unusual traffic patterns and evaluate the reason for declining sales performance. This helps save organizations and users from cyber-attacks, data breaches, and monetary and information losses.
- With digitalization and the proliferation, the media and entertainment companies have realized the need for botnet detection solutions to protect and secure their databases, applications, and websites. Due to the increasing acceptability, the online media and entertainment industry is expanding at a high pace and is primarily driven by digital media.
- Netflix has been one of the prominent over-the-top, or OTT platforms globally. The company's annual revenue accounted for USD 29,697 million, recording a growth of 19% compared to the previous financial year. Furthermore, the company partners with diverse TV makers to offer its application to smart TVs, which is expected to further increase the number of users. As a result, the incident for botnet attacks is projected to increase, which is likely to foster market growth.

North America to Hold a Major Market Share

- North America is expected to be one of the most significant revenue-generating regions for botnet detection management vendors. The US and Canada focus on innovations obtained from Research and Development (R&D) and technologies. The region owes its growth as a significant contributor to the rising investments in botnet detection solutions to safeguard websites, APIs, and mobile apps from bot attacks.
- Further, the region is anticipated to be a markedly productive regional market. The rising menace of the damage that botnets can do across the government in countries of these regions is boosting the demand.

- The US government has regularly taken stringent measures against prevalent and mass-level botnet threats. In April 2022, the United States Department of Justice announced a court-authorized operation conducted in March 2022 to disrupt a two-tiered global botnet of thousands of infected network hardware devices under the control of a threat actor known as Sandworm. The operation copied and removed malware from vulnerable internet-connected firewall devices that Sandworm used for command and control (C2) of the underlying botnet.
- Also, this can be attributed to the growing awareness among the population regarding data privacy which is supposed to promote the demand for botnet detection solutions across North America. Furthermore, increasingly harsh government regulations regarding data privacy are considered to promote the market's future growth significantly.

Botnet Detection Industry Overview

The botnet detection market is moderately competitive and consists of several major players. In terms of market share, few significant players currently dominate, with new players entering the market. The demand for services is directly related to the adoption level of botnet detection solutions among organizations. These companies leverage strategic collaborative initiatives to increase their market share and profitability. The companies operating in the market are also acquiring start-ups working on enterprise network equipment technologies to strengthen their product capabilities.

- July 2022 - Fastly, Inc. announced a reseller partnership with HUMAN Security, Inc. The partnership would offer customers bot protection and fraud and account abuse prevention to keep cybercriminals out of their online applications and services.
- April 2022 - Akamai Technologies, Inc. announced the availability of Audience Hijacking Protector, a new solution designed for online businesses to maximize revenue opportunities and minimize marketing fraud. Akamai also unveiled several new application security features designed to help organizations defend customers from threats across all online environments, including internet browsers, managed alerting for Bot Manager, mobile applications, during API interactions, and at the edge.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Botnet Detection - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-05
		Signature