Skillmine
Technology • Consulting • Services

infosec
Miners

BOTS

Did you know?

National Geographic had built a conversational app which conversed like Albert Einstein would have, to promote their show Genius.

Here is a deep dive into bots.

- A bot is a computer program that uses Artificial Intelligence (AI) and Natural Language Processing (NLP) to understand customer needs and automate responses, simulating human conversation.
- Bots can take text input, audio input, or both, in the same way to give the output without human intervention.
- They carry useful functions, such as customer service or indexing search engines, but they can also be malware – used to gain control over a computer or service.

SOME EXAMPLES OF BOT

Messenger apps such as Facebook Instant Messenger, WhatsApp, Telegram and Signal.

Chatbots such as Google Assistant, Alexa and Siri.

TYPES OF BOTS

1 Chatbots:

Bots that imitate human conversation by responding to specific phrases with programmed responses.

2 Social Bots:

These bots that operate on social media are used to automatically generate messages, advocate ideas, and act as followers or fake accounts to gain followers themselves.

3 Shop Bots:

These bots can observe a user's patterns in navigating a website and then customize that site for the user

4 Knowbots:

KnowBots collect information for users by automatically visiting websites to retrieve data which fulfils specific criteria.

5 Monitoring Bots:

These bots monitor the health of a website or system. Downdetector.com is an example of an independent site that provides real-time status, including outages and other kinds of services.

6 Malware Bots

Malware bots and botnets can be programmed to break user accounts, scan the internet for information, send spam, or perform harmful activities.

Attackers may distribute bad bots in botnets – i.e. a bot network. A botnet refers to several internet-connected devices, each running multiple bots under the control of an attacker.

7 Spambots:

Spambots may collect email address details from contact or guestbook pages. Alternatively, they may post promotional content in forums or comment sections to drive traffic to specific websites.

8 Malicious Chatterbots

These chatterbots pretend to be people, emulating human interaction and often fooling people. This bot aims to obtain unsuspecting victims' personal information, including credit card numbers.

9 DoS or DDoS Bots:

These bots create traffic intentionally to down a server's resources and prevent a service from operating.

10 Click Fraud Bots:

These bots create massive malicious bot traffic targeting paid ads to engage in ad fraud.

11 Vulnerability Scanners

These bots can scan millions of sites for vulnerabilities and report them to the bot owner. But in simple bots that would inform the website owner.

WHY DO CYBERCRIMINALS USE BOTS?

- To extort money from victims
- To attack legitimate web services
- To make money from botnet (zombie) systems
- To steal financial and personal information

PROS OF COMPUTER AND INTERNET BOTS

- Customizable
- Multi Purpose
- Available 24/7
- Offers the Best User Experience
- Reduce Labour Costs for Organizations
- Faster Than Humans at Repetitive Tasks
- Saves Time for Customers and Clients
- Organizations Can Reach Large Numbers of People via Bots

CONS OF COMPUTER AND INTERNET BOTS

- Requires Human Assistance
- Can be Used in Illegal Activity
- Can be Programmed and Created as Malicious
- Risk of Misunderstanding Users and Causing Frustration for Them

Steps to Protect your Computers from Bots

1. Install a Firewall
2. Use a Bot Manager
3. Use a Strong Password
4. Only Click on Links You Trust
5. Install Anti-malware Software.
6. Avoid Untrustworthy Websites and Ads
7. Make Sure that All of our Software is Up to Date

Skillmine
Technology • Consulting • Services
India | KSA | UK | USA

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

Follow us on