SOCIAL MEDIA BOTS OVERVIEW

Social Media Bots can propagate hate, with randomness, to act together, and attempt to gain mainstream popularity. They can be used to overwhelm the user’s account to the point of deactivation. Social Media Bots allow a user to program a set of parameters, but may have or require additional user interaction or a greater degree of management. These types of Social Media Bots are typically fake accounts with fake personalities and are run at least partially by humans or click farms, rather than artificial intelligence, big data analytics, and other programs or databases to imitate legitimate users posting content.

OCA defines Social Media Bots as programs that vary in size depending on their function, capability, and design; and can be used on social media platforms to do various useful and malicious tasks while simulating human behavior. These programs use artificial intelligence, big data analytics, and other programs or databases to imitate legitimate users posting content.

**Social Media Bot Signature Behaviors**

- Social Media Bots often congregate together, and act with randomness, making them easier to identify.
- Social Media Bots tend to use emoticons, exclamation points, or other content in more regular patterns as compared to human users on social media.
- Social Media Bots often have higher levels of activity (typically automated Social Media Bots) as compared to human social media behavior.

**Activity Levels**

- Social Media Bots often have higher levels of activity (typically automated Social Media Bots) as compared to human social media behavior.

**Common Attack Methods of Social Media Bots**

- Click Farming or Like Farming: inflate fame or popularity on a website through liking or reposting of content via Click Farms, which provide fake user accounts (typically semi-automated Social Media Bots) and management of the Social Media Bots (e.g., bot herder) for purchase.
- Hashtag Hijacking: use hashtags to focus an attack (e.g., spam, malicious links) on a specific audience using the same hashtag.
- Repost Storm: use a parent Social Media Bot account, or martyr Social Media Bot, to initiate an attack by reposting something, which an associated group of Social Media Bots (aka botnet) instantly reposts.
- Sleepers Bots: remain dormant for long periods of time, wake up to launch their attack of thousands of posts or retweets in a short period of time (perhaps as a Retweet Storm, or spam attack), then return to a dormant state.
- Trend Jacking and Watering Hole Attack: use top trending topics to focus on an intended audience for targeting purposes.

**Social Media Bot Uses**

- **Commercial Activity:** Social Media Bots facilitate company-to-customer relations, including selling of products or services.
- **Counterterrorism and Terrorism:** Social Media Bots are used on social media specifically to find, add or create, the illusion of online fame or popularity.
- **Entertainment:** Social Media Bots are used on social media to sway public opinion, limit free speech, and manipulate information operations.
- **Hate Speech:** Social Media Bots can propagate hate speech on social media platforms, making the subject matter appear to gain mainstream popularity.
- **Information Operations:** The intentional spread of propaganda to sway public opinion, limit free speech, and manipulate democratic processes and elections.
- **Notifications:** Social Media Bots provide automated watching capabilities to capture breaking news, ideas, or events.
- **Social and Civic Engagement:** Social Media Bots post to encourage and heighten civic engagement and participation.

**Activity Level Comparison**

- Social Media Bots
- Humans

**Conclusion**

Social Media Bots are becoming more prevalent and better at mimicking human behavior on social media platforms. As of 2017, technology companies are seeking investments and further incorporation of Social Media Bots into social media services and platforms, expanding “future digital communication” to provide a myriad of services as automated assistants. As Social Media Bots gain a greater foothold in social media and daily life, the potential uses, for good and malicious purposes, are ever expanding.