Mayur Suresh

CSC 301

11-04-21

Article Review #4

Article Review of “Spammers Are Becoming “Smarter” on Twitter

I choose this article out of the others because this is a more current event topic and also a link to the previous article review. This is also important as seen with the 2016 elections. This article focuses on how spamming in this internet century has increased drastically especially in twitter. Due to its success in luring regular users to “commercial or malicious sites containing malware downloads, phishing, drug sales, scams, and more.” compared to spam emails. The article goes on to talk about various methods that have been proposed to combat this. This includes identifying spammers via their tweet history, detecting unordinary behavior and classifying tweet-embedded URLs. Despite the use of these methods spamming activities have not decreased due to spammers always creating new strategies. These strategies include “posting behavior, finite-state-machine-based spam template, and passive spam.”

The article goes on to talk about well know spamming strategies, and the basic spamming technique is the use of various Twitter features like @ and #. By using these not only do these mimic regular users and is hard to detect but can be spread to a huge number of users in trending topics. Some of the other Twitter functions spammers use are “reply”, “following” and others to blend in. Further in the article goes into detail about spamming coordinated by groups (specifically in 2013). The article spreads spamming into 17 groups and then monitor it. Then they found the majority of the spam (more than 75%) comes from URLs embedded in tweet with a .ru domain which is of Russian origins. It further studies how the various groups related to such spam acted in relation to one another. When one group ends their activity (stops sending spam) another group picks up the activity. With this type of behavior, it is difficult to detect because spammers change the groups of accounts.

The article goes on to talk about another spamming technique called “Finite-State Machine-Based Spam Template” which, according to the article, are set of templets with number of states and edge is denoted by a word which then follows with a URL. One example used in the article where there were many nodes which can be pieced together. By using these there are 2,160 different spam tweets produced with little expense and harder to detect.

Lastly the article covers a much harder to detect and less interactive spam called “Passive Spam”. This type of spam does not use any type of Twitter features previously mentioned (@ and #) which is very hard to detect because programmed spam detection cannot catch this. This is also less interactive because this does not trend but target specific users. Passive spam is used when users look up topic with specific keywords. Most of the time these spams are mostly cracked games, software, and pirated movies. The article keys in on the fact that 50% were in Russia but victims were mostly non-Russians but still clicked on the spam. The spam was to interesting that the victims used translators to use the content.

The article ends by saying that there are more spamming strategies that are being used than those mentioned in the article and still being developed. So the fight against spammers is not going to be over any time soon and should develop more strategies to make Twitter safer.

This article really is interesting, although I don’t use Twitter, I use other social media such as snap chat where I have seen spam and advertisement. The fight against spam is going to be fiercer due to the increase in the use of Twitter and also with the influx of younger and more naïve users who is going to fall victim to these type of malicious acts.