Ennio Cruz

Professor Duvall

CYSE201s

30 SEP 2023

Article Review 1:

Digital fingerprinting for identifying malicious collusive groups on Twitter.

https://doi.org/10.1093/cybsec/tyad014

The article I chose to review discusses the issue of malicious actors that use social media platforms to commit cybercrimes like phishing and drive-by downloads using shortened links posted specifically on Twitter to lure potential victims. The proliferation of social media platforms has allowed more people to engage with one another online. Social media has provided multiple ways to interact socially by posting pictures, reels, and videos. Criminals have also taken advantage of these interactions to victimize people. Relating this topic to the principle of relativism, as the technology system develops, the nature in which people interact within the social system, both positive and negative, has also developed. Criminal actors have used Twitter to spread malicious links that funnel unsuspecting victims who click them to end-points that lead to exploitation. To increase the chance of luring a victim, it is suspected that criminal actors collude with each other or control multiple Twitter accounts that coax or promote other users to click malicious links. If this is true, the article poses the question, “Are there any similarities in the actions these criminal actors perform online?” and “whether these similarities can be used to identify collusion?”

The article presents a method for identifying criminal actors who collaborate in spreading these malicious links by analyzing their online behavior and forming a digital fingerprint. The collection of common online behaviors amongst the identified criminal actors is used to form digital personas that are further used as a cluster of similar digital personas to identify potential colluding criminal actors.

The hypothesis is that criminal actors who exhibit similar digital personas can be grouped and identified as colluding with one another. Relating this to the principle of parsimony, the article has presented the process of identifying colluding criminal actors very simply.

To test this hypothesis, the researchers of the article performed a combination of archival and case study research. The researchers gathered a total of 1,255,178 COVID-19-related tweets between 11 March 2020 and 21 March 2020 to analyze for any malicious external links. Tweets containing external links were fed into a free cloud-based anti-virus aggregator called Virus Total. Virus Total scans the links for any malware signature matches, and those that do match are labeled malicious. Once the malicious links are identified, creating a digital persona for the accounts that have posted the links begins. Case studies were used to identify four main malicious online characteristics: URL fingerprint, Account fingerprint, Post/Content fingerprint, and Activity fingerprint.

URL fingerprint – detailed analysis of the malicious link, like the length of the URL, hostname, host IP, and other parameters in the URL.

Account fingerprint – detailed analysis of the characteristics of the malicious account that creates the posts, like when the account was created, the geo-location of the account, the number of followers, etc.

Post/Content fingerprint – detailed analysis of the content of the malicious post, like the language used, grammar, punctuations, emoticons, hashtags, etc.

Activity fingerprint – detailed analysis of the online actions performed, posts per day, retweets, post intervals, unique tweets, etc.

The following detailed characteristics are attributed to the criminal actor to form digital personas. The results of grouping digital personas with similar characteristics produced distinct clusters, validating that the method can identify coordinated dissemination of malicious tweets. The gathering and analysis of the data relied on empirical data, relating it to the principle of empiricism.

The article was very interesting. It demonstrated how the study of cybercrime involves the concept of interdisciplinary studies, as discussed in class. It draws from computer science disciplines, understanding the technology used by criminal actors and social sciences to understand the behavior in which these criminal actors perform and coordinate their malicious postings.

The article also focused on analyzing tweets from a specific event, the height of the COVID-19 pandemic in March 2020. The reason is that the mandated lockdowns have caused an increase in social interaction using social media, particularly Twitter, to remain updated during those times. Since everyone was eager to stay updated with developments regarding COVID-19, criminal actors have also taken advantage of this to disseminate false and malicious links within COVID-19 tweets. Two marginalized groups that were most possibly affected by these criminal groups are the elderly, who were looking for links to information regarding vaccination, and the working class, who lost their jobs and were looking for links to information regarding the stimulus checks.

Because of the conditions during that time, the concept of victim precipitation can also be related to the topic of the article. Most people were suffering financial struggle, had their guard down, and could be easily fooled into clicking malicious false links of COVID-19 stimulus checks.

The same financial distress that may have caused victims to lower their guard can also be the factor that influenced the behavior of these criminal actors to engage in these activities to make money, making a convincing case that the concept of behavioral theories can explain why certain individuals engage in cybercrime. The article presents a valuable contribution to society by developing an effective way to identify collusion between criminal actors who perform cybercrimes. Going further, using the method to develop legislation that would crack down on these activities would be ideal.

The topic is also very relevant and can be applied in other ways to contribute to society. The method for identifying collusion among cyber criminals can also be modified to identify collusion and coordination of individuals who perform disinformation campaigns. The model can be used to create legislation that would reduce the proliferation of fake news while minimizing impacts on freedom of speech. It could also be a basis for performing a study regarding the victims. Identifying the factors that increase the likelihood of clicking malicious links and identifying the necessary controls social media platforms can employ to limit these activities.