In their article “Spammers Are Becoming ‘Smarter’ on Twitter,” Chao Chen, Jun Chang, Yang Xlang, Wanlei Zhou, and Jonathan Oliver discuss the current conditions of hackers spreading malware via Twitter. With over 500 million tweets per day, Twitter has become one of the most used platforms for social media, making it a hotspot for hacker attention. While various methods have been brainstormed to try and reduce spamming and scamming on Twitter such as “identifying spammers based on tweeting history or social attributes, detecting abnormal behavior, and classifying tweet-embedded URLs,” researchers worry that hackers are also getting smarter.

Basic strategies by spammers include using Twitter function such as @ and # to put a spam tweet on someone’s feed without having to be followed by the intended recipient. Spammers may also use the “reply,” “favorite,” and “following” functions to spread spam in a similar manner. To avoid detection, spammers try to normalize their spam accounts by getting more followers, posting more often, and otherwise using twitter like an average user might so that the detection system will not see it as a spam account. As a better defense, researches propose analyzing the geographical data of friends to determine whether or not an account is spam by analyzing how clustered their followers are. However, coordinated posting behavior and finite-state machine-based spam templates are much more in-depth spamming techniques that focus on variety to fool the Twitter spam-defense mechanisms. Passive spam, while it reaches less users, is also effective because since it reaches less users, Twitter unknowingly lets it slip through its spam-defenses because it is not seen as a threat.

Having started reading about spamming techniques from 2004, it is crazy to see how evolved spam and malware strategies had become by 2016, and also how much more in depth the defense strategies are. Seeing how long spamming and hacking has perpetuated, it makes me wonder what is in it for the spammer or hacker. How much money could they possibly be getting from their efforts (especially spammers)? What makes putting the effort in to writing programs for coordinated posting behavior and finite-state machine-based spam worth it? Especially considering the spam-awareness of my generation, I imagine the profits of spamming are reducing over time.