

Determining Selection Behavior of Malicious Bots within Twitch Chat

Andrew Yarbrough

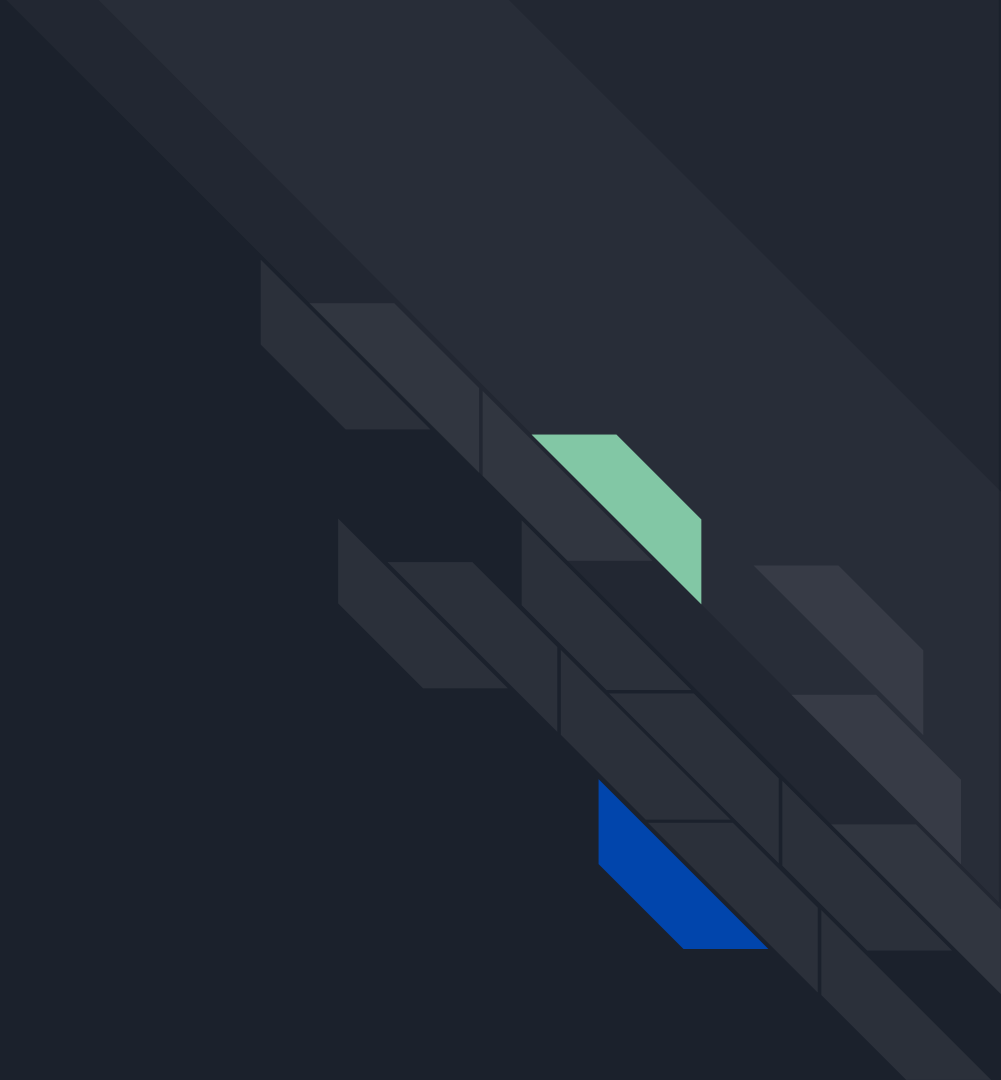
Tanner Bonds



Overview

- Introduction
 - Twitch
 - Malicious Bots
 - Selection Behavior
- Related Work
 - Twitter
- Approach
 - Data Gathering
 - Methodology
 - Analysis & Twitter Comparison
- Results

Introduction



Twitch & Twitch Chat



- Popular Internet Live Streaming Service
- Users Can Comment Directly In Real-Time
- Owned By Amazon
- Average Daily ~1.2 Million Concurrent Viewers
- Tends to Peak in March

May 2019	1,262,560	48,294	939M hrs	3,933,404
April 2019	1,234,112	51,261	889M hrs	4,184,467
March 2019	1,273,772	54,934	947M hrs	4,389,867
February 2019	1,311,802	56,286	880M hrs	4,205,001
January 2019	1,276,009	55,794	949M hrs	4,537,807



Malicious Bots

- Bots
 - A bot is any sort of user that runs an automated task, also known as a script, over the internet.
- What is Spam?
 - Spamming is the act of sending unsolicited messages, often repeatedly, on the same website. These spam messages are typically used for advertising purposes
- How It Works (In Twitch)?
 - Bots post links in high frequency that typically lead to some advertisement
- What Is Phishing?
 - The fraudulent attempt to obtain sensitive info such as usernames, passwords, credit card details, etc. by disguising oneself as a trustworthy entity in an electronic communication
- How It Works (In Twitch)?
 - Create a bot that says it claims to post something that helps you but is malicious



Selection Behavior

- What Is Selection Behavior?
 - Determining how the next target of the bot will be chosen.



Twitter

- John Seymour and Philip Tully with SNAP_R
 - Targets groups of users on Twitter and sends them appropriate phishing tweets based on machine learning techniques.
 - Uses general phishing tweets on Twitter to create learning model and then creates groups and categorizes users into these groups based on profile, job, types of things they tweet, etc.
- Grant Stafford and Louis Lei Yu
 - Spammers make use of trending topics in Twitter to produce large quantities of spam tweets to acquire more users to click on their links.

Approach





Data Gathering

- Week & A Half / March 18 - March 29
- Spring Break Overlap
- Twitch Chat Logger on Github



Methodology

- 10 Instances Each. 20 Total.
- 10 Monitored the Top 10 Streamers w/ Most Viewers
- 10 Monitored the Top 10 Streamers w/ Most Viewers < 1,000.
- Ran for Several Hours
- Stored as .log Files.



Analysis

- Privacy
 - Find Links In Messages, Remove All Others
- Enter Links into Google's Safe Browsing API
- Patterns
 - Similar Bots with Similar Links across Multiple Channels
 - Similar Bots with Different Links across Multiple Channels
 - Different Bots with Similar Links across Multiple Channels



Twitch & Twitter

- Comparison of Findings
- URL Shorteners
- Similar Phishing Attacks

Results



Our Excel Doc

Total Number of Chat Messages	Total for 1000 benchmark	Total for Top 10	1000 benchmark number of links	Top 10 number of links	Total Number of Malicious Links for 1000 benchmark	Total Number of Malicious Links for Top 10
11508772	770734	10738038	16966	102241	0	4
		454 Files				
		4540 Removed				
		Original: 10742578				
		Unique Links: 10706				
Link			Occurences	Date	Time	Threat
https://simplenordy.fun			103	03-24	11:14:55 AM - 11:46:27 AM	Social Engineering
https://simplehot.fun			99	03-25	08:06:50 AM - 09:00:34 AM	Social Engineering
https://simplehot.fun?referral=5359			1	03-25	8:10	Social Engineering
https://simplehot.fun?referral=8645			1	03-25	8:17	Social Engineering
			Total Number of Links:			
			119207			

Malicious Links

- Google's API reported 4 links as malicious
- All 4 links occurred in the same 2 Twitch streams
 - One occurred 103 times, another 99, then 1, and 1

Current status

 This site is unsafe

The site <https://simplenordy.fun> contains harmful content, including pages that:

- Try to trick visitors into sharing personal info or downloading software

Links	Occurrences	Date	Timeframe
https://simplenordy.fun	103	3-24	11:14:55 AM - 11:46:27 AM
https://simplehot.fun	99	3-25	08:06:50 AM - 09:00:34 AM
https://simplehot.fun?referral=5359	1	3-25	8:10:09 AM
https://simplehot.fun?referral=8645	1	3-25	8:17:23 AM



Advertising Links

- Sponsored Links
- Promoted Links
- Replay Clips



Streamer Security

- Thankfully, our results and suspicions about Twitch were wrong.
- Streamers take much better care about the security of their viewers than most individuals do about themselves.
- Most streamers turn on a setting that makes it so that only they, and those they allow, can post links in chat.



Twitch & Twitter

- Inconclusive, Comparison cannot be made.
- This itself is a result!
- Twitch appears to have little to no malicious presence, the same cannot be said for Twitter.



Comments and Questions?