Fake News Research Project

Research Report

John Cook, Huyen Le, Zubair Shafiq
Department of Computer Science
The University of Iowa

June 26, 2017
## Contents

1 Introduction .................................................. 1

2 Related Work .................................................. 2

3 Data .................................................................. 3

4 Results ................................................................

4.1 Url Popularity .................................................. 5

4.2 Temporal Patterns .............................................. 11

4.3 The User Landscape .......................................... 15

  4.3.1 Account Automation ...................................... 15

  4.3.2 Verified, Deleted and Suspended Accounts .......... 17

  4.3.3 URL Analysis .............................................. 19

5 Conclusion ......................................................... 23
1 Introduction

In the year and many months leading up to the 2016 U.S. Presidential Election social media platforms such as Twitter became a bastion to express political discourse. Political leanings, sentiment, and political discussion could all be seen flying at speed of tweets, retweets, follows, shares and likes. For this reason we chose to select tweets as a dataset from the the two U.S. Presidential candidates Hillary Clinton and Donald Trump. The tweets were previously collected from Oct 25, 2016 through Nov 7, 2016, using Twitter’s streaming API targeting the keywords “Trump” and “Hillary Clinton”.

Political actors, Governments and political candidates have used social media as vehicle to persuade, suppress and steer public opinion [13]. Previous research has identified that Political Candidates and parties have previously paid to create false information such as trending topics in attempt to create a false environment on social media [13]. Recent U.S. Federal investigators have suggested that a “Blitz of Bots” proliferated large amounts of Pro Trump “links” (urls) on social media near and around the campaign period [14] seeking to persuade public opinion and shape the U.S. Presidential Election. One type of persuasion is carried out by exaggeration and the spreading of false stories and rumors in order to captivate a listening audience. In the short term persuasion through falsities is an effective strategy to muddy the waters of truth until fact checking can be performed. However even when sufficient fact checking can be performed and presented it always lags the propagated rumor [15] and recent research suggest those that propagate fake news tend to believe it and continue sharing it. [11, 19]

In order to understand the intersection of fake news, political discourse and social media (through Twitter) we chose to analyze over 18.6 million tweets (Clinton: 9,331,653 and Trump: 9,345,946), selected from a compressed, yet emotionally and politically charged time period, the two weeks prior and leading up to the 2016 U.S. Presidential Election.

We conducted an in depth study to understand the dissemination of fake-news among twitter users by identifying tweets that contained known fake news domains. We selected fake news domains from three sources from previous work. Our selected sources came from Jonathan Albright’s Group 306 List, created to understand fake news sources and url propagation behavior [8], B.S. Detector, which uses a professionally curated “fake-news” list to aid in the detection and identification of fake news within a browser extension [2] and fakenewswatch.com, a trusted website [18] that frequently compiles an up to date list of known fake news domains, and draws from other fact checking sites such as snopes.com. In order to form our own list, we selected domains that only appeared in all three of these sources, to form a stable ground truth of known fake news sites. We explored the dissemination of fake news by taking a multi-dimensional approach motivated by previous work [8, 9, 11, 12, 19]. In our study, we defined “fake-news” by identifying tweets that contained a url whose canonical domain appeared in our ground truth, which we discuss in the data section. We explored dimensions such as temporal tweet activity, likelihood of account automation, tweet volume, temporal persistence of widely shared urls, and candidate affinity. We explored each of these dimensions and their relationships over the set of our fake news domains as well as each candidate to form a characterization of the dissemination of fake news during this time period.
2 Related Work

Our motivation to analyze the spread of fake-news urls was influenced by previous work and research. To analyze the spread of fake news, we exercised both a quantitative and qualitative perspective.

Shao et. al. [18] investigate the temporal relationship between the spread of misinformation and fact checking using a public tweet dataset [18]. The dataset was formed by collecting tweets that contained URLs from fact checking domains as well as fake news domains. This research supports that URL’s are the most common method to share news articles on platforms that limit the amount of user expression (such as Twitter’s imposed 140 character limit) [18]. Their implemented system, Hoaxy, provides an automated solution for identifying fake-news stories by comparing them against known news sources and fact checking websites. The research found there are a few highly active users responsible for fake news on social media [18]. They additionally identified that correcting rumors through fact checking takes 13 hours on average. Our research builds upon investigating temporal propagation of misinformation, by focusing only on the spread of fake news urls. Furthermore we build a more stable ground truth for identifying fake news urls by using the common intersection among three credible fake-news lists.

Jin et. al. [15] conducted a study to identify rumors spread by tweets. The study used a corpus of over 8 million tweets collected from the followers of the two Presidential Candidates and matched text in tweets against a collection of debunked rumors from snopes.com. The researchers evaluated five matching algorithms used to match and identify tweets against a truth base. While our study does not utilize text matching methods, we use some key findings as motivation to investigate attributes of the user landscape. Specifically, their study found that users that tweeted more ‘rumor tweets’ had a higher tweet ratio, or put another way a handful of users were responsible for the spread of the majority rumors. Additionally their study found that rumor tweet activity was more or less stable in the earlier months of their 6 month study (Apr. 2016 - Oct. 2016), but increased progressively as election day drew near. We use this result as motivation to analyze the time-period of the final two weeks within our corpus.

Forelle et. al. [13] conducted a study to understand the influence social media on political elections. Previous research indicates political candidates, leaders and political parties have paid large sums of money to influence social media through bots. Forelle et. al.’s research tracked the twitter feeds of six Venezuelan politicians in order to understand bot interaction. Their findings suggest that political bots during this time period in Venezuela tend to impersonate members of political parties or common citizens. Of the politicians sample, political bots in Venezuela during this study tended to retweet more politically radical tweets in nature. Additionally, identifiable characteristics of ‘botnet’ users included temporal characteristics and known bot tweeting platforms. Our research explores account automation and hypothesizes that candidate affinity characterized by a combination of negative sentiment and disproportionate tweet volume may be an play a role in inferring bot presence.

Kollanyi et. al. [16] explored account automation through hashtag frequency among twitter users during the U.S. Presidential Election. Their data set of tweets was obtained by Twitter’s API by counting tweet frequency of ‘major hashtags related to the U.S. Presidential election’ (Nov. 1-9 2016). Their findings revealed that Pro-Trump affinity increased by a large margin during the final week of the election period. We use this detail to explore candidate affinity over several dimensions.
Anagnostopoulos et. al. [11] found that users that share fake news on social media, tend to consume content of that of like-minded users with similar beliefs, described as homophily. Similarly Starbird’s [19] research supports that users exposed to conspiracy theories tend to continue to believe (are difficult to persuade otherwise). Additionally, these users tend to be vulnerable to re-share new conspiracy theory content. We use this as a springboard to the understand the spread of fake-news urls within our tweet set.

Allcott et. al [9] conducted a quantitative study to understand the influence of fake-news on social media during 2016 U.S. Presidential Election and its impact upon U.S. voters. Their study measured the importance of fake-news by gathering web statistics reported by Alexa’s browser plugin [6], as well as querying for Facebook shares of urls though buzzsumo.com ‘an online database that connects to Facebook through its public API’. This study explored user exposure to the fake news by measuring ‘recall’ and ‘believability’, though a controlled survey. This research only explores url’s shared from 21 fake news domains ‘curated from Craig Silverman of BuzzFeed’. Our research draws from three sources, resulting in a common intersection of 58 fake news domains among three sources.

3 Data

Tweets for the selected time period of Oct 25, 2016 to Nov 7 2016 were obtained using Twitter’s streaming API by filtering on keywords “Hillary Clinton” and “Trump”. We began with an initial tweet corpus containing over 18.6 million tweets (9.3 M tweets for each candidate). To identify fake-news, we obtained domain names of 679 known fake-news domains gathered from three separate sources. For continuity across sources we used only domain names that appeared with each our chosen fake-news lists. In total we matched urls against a common intersection of 58 known fake news domains.

Our approach to understanding the spread of fake news depended on a process to target tweets containing URLs whose domains matched against our truth base. To begin, we selected the ‘expanded_url’ attribute from the ‘url’ entity of each tweet. We then expanded any url, still represented as short urls, that appeared in the ‘expanded_url’ attribute. In total, we expanded 4,618,595 urls from tweets obtained from our ‘Hillary Clinton’ stream and 4,638,649 urls from tweets obtained from our ‘Trump’ stream. With this expanded url tweet set we extracted the domain name’s from each url within a tweet. We then matched each extracted domain against the domains within our fake news truth base. We matched 29 of the 58 domains from our truth base to form a filtered set containing 43,340 tweets propagated by 21,182 unique users.

We applied a measure to understand the the prevalence of account automation by utilizingTruthy’s BotOrNot API [1], discussed in our results section. We identified BotOrNot scores for 19,658 users. In addition to identifying automated accounts, we identified 24 verified accounts, 550 suspended accounts, and 469 deleted accounts. We discuss our findings in more detail in the Results section below.
Table 1: Fake News Domain Statistics

<table>
<thead>
<tr>
<th>Site</th>
<th>#Users Total</th>
<th>% Users Total</th>
<th>% Users Clinton</th>
<th>% Users Trump</th>
<th>#Tweets Total</th>
<th>% Tweets Clinton</th>
<th>% Tweets Trump</th>
<th>% Deleted Tweets Clinton</th>
<th>% Deleted Tweets Trump</th>
<th>% Deleted Tweets Total</th>
<th>Deleted Tweets Clinton</th>
<th>Deleted Tweets Trump</th>
<th>Deleted Tweets Total</th>
<th>BON Score Avg. Clinton</th>
<th>BON Score Avg. Trump</th>
</tr>
</thead>
<tbody>
<tr>
<td>infowars.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>dclothesline.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>reddragon.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Clematisconsin.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>globalresearch.ca</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>truthfrequencyradio.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>infowars.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>dclothesline.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>reddragon.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Clematisconsin.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>globalresearch.ca</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>truthfrequencyradio.com</td>
<td>1000</td>
<td>70.68</td>
<td>54.18</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
</tbody>
</table>

Table 1 contains a collection of 43,304 identified tweets that contain fake news domains collected from 21,182 unique users. We found that fake news domains appeared overwhelmingly more frequent in our stream collected for “Hillary Clinton” than “Trump”. Of the tweets identified containing fake news domains, 5.878 (13%) originated from the stream collected for “Trump”, dwarfed by 37,426 (87%) appearing in the stream collected containing “Hillary Clinton”. More interesting, over 75 percent of tweets containing fake news URLs were concentrated among a few domains, most notably infowars.com. Deleted tweets exhibited a similar proportionality with 3,284 deleted tweets originating in our “Hillary Clinton” stream and 474 from our “Trump” stream. BotOrNot scores tended to be slightly higher (likely-bot) among users appearing in our “Trump” (0.38 avg.) stream than our “Hillary Clinton” (0.36 avg.) stream.
4 Results

4.1 Url Popularity

We first begin exploring the spread of fake-news urls by understanding URL popularity within our data set. We selected the most popular three sites from each candidate based on tweet activity. The most active sites contained tweets filtered from the “Hillary Clinton” stream were infowars.com, dcclothesline.com and redflagnews.com (Figure 3). The highest activity sites filtered on keyword “Trump” were infowars.com, beforeitsnews.com, and conservativeoutfitters.com (Figure 4). To understand URL popularity we modeled the percentage of URLs against the number of tweets that contained those URLs (Figure 1 and Figure 2).

We found that the most popular domain ‘infowars.com’ among each candidate exhibits a pattern in line with the Pareto Principle, motivating our hypothesis that a handful of URLs are widely shared among a large number of tweets. In (Figure 3(a)) and (Figure 4(a)) we see that nearly 70 percent of the URLs containing fake news domains are shared less than 10 times. The remaining 30 percent are shared greater than 10 times, suggesting that fake-news tends to propagate among a few fake news stories. Figure 5 displays the behavior pattern of user url sharing. The dark blue lines in the figure indicate widely shared URLs among a large amount of users, and the red lines indicate active users, sharing many urls. The behavior in this figure demonstrates that a handful of urls are widely shared among many users. Building upon this finding, we chose to select the most popular URLs from the tail of our plots and analyze their temporal patterns. We discuss this analysis in further detail in Temporal Patterns section below.

Of the six popular URLs selected, their content exhibits sentiment of either “Pro-Trump” or “Anti-Clinton”. Of the most widely shared URLs much of the content is motivated by the “Podesta Email’s” hack. On March 19, 2016 “a campaign staffer was incorrectly informed that an email instructing John Podesta to change his password was legitimate” [17]. “Oct. 3, 2016 Wikileaks promised to release information on the U.S. Presidential campaign for the next 10 weeks. On Oct. 7, 2016 a Wikileaks ‘dump’ was released to the general public containing ‘a trove of emails’ of the account belonging to John Podesta” [17]. The most popular url was shared over 6000 times, accounting for nearly 14 percent of the fake news urls that appeared in our corpus. The tweet shared accuses John Podesta of participating in a dinner party that centers around a Satanic Ritual known as “Spirit Cooking” [7]. According to the the fake-news url target landing page Spirit Cooking is “‘a sacrament in the religion of Thelema which was founded by Aleister Crowley’ and involves an occult performance during which menstrual blood, breast milk, urine and sperm are used to create a ‘painting’ ” [7]. This rumor was contested and claimed false by Snopes.com [3]. While Podesta did receive an email from his brother to attend a ‘spirit cooking’ dinner, the dinner had nothing to do with the ritual described in the rumor. Furthermore the Wikileaks dump revealed that Clinton was not included within the e-mail chain nor did Podesta respond to the invitation[3]. Similar relate URLs were widely shared claiming that Clinton was involved with the occult church as a witch and Clinton’s Satanic network is exposed.


(c) http://www.redflagnews.com/headlines-2016/breaking-julian-assange-next-leak-will-lead-to-arrest-of-hillary-clinton

Figure 1: Temporal Propagation for three most popular URLs with Candidate Clinton
Figure 2: Temporal Propagation for three most popular URLs with Candidate Trump

(a) http://www.infowars.com/video-hillary-personally-ordered-donald-duck-to-troll-trump-rallies/

(b) http://www.nowtheendbegins.com/black-america-goes-donald-trump-record-numbers-election-day-approaches/

Figure 3: Cdf of tweet counts for three most popular fake domains with candidate Clinton.
Figure 4: Cdf of tweet counts for three most popular fake domains with candidate Trump
Figure 5: Behavioral Pattern.
4.2 Temporal Patterns

We turn our attention to temporal patterns as a second dimension to further explore the spread of fake-news URLs during the 2016 Presidential Election. Figure 6. shows the hourly temporal patterns and tweet volume over the 29 identified fake news domains from Oct 25, 2016 through Nov 27, 2016. We organized tweets by domain and candidate in order to capture statistics with those attributes in mind. We captured the time and date by extracting the ‘created_at’ attribute from each tweet. We notice right away some peaks dominate the temporal activity in irregular intervals and used this as a springboard to investigate further.

We chose to plot temporal patterns over all 29 domains separating time-series between each candidate. We selected content from prominent ‘spikes’ that appeared within the time-series plots for each of the most popular domains, keeping in mind cyclic daily tweeting patterns by only selecting ‘spikes’ that dominated the time-series pattern. We investigate the content of spikes by filtering out tweets between the beginning and end of each spike period and selecting the most widely shared urls. In figures 7 and 8 we display the tweet activity for the two most active domains. We’ve numbered each peak and provided the most tweeted url and the number of times it was shared for each label.

In Figure 7, infowars.com resembles similar activity seen in the overview temporal patterns of all 29 domains. This coincides with the percentages we see in Table 1 as infowars.com urls account of over 75 percent of all identified fake news urls. We analyzed each peak by selecting the most widely shared urls. We then manually analyzed the content of each URL. We find that spikes that appear in Clinton tweets tend to be Anti-Clinton and spikes in Trump peaks tend to be Pro-Trump. Common Anti-Clinton themes include Clinton Satanic involvement, internal turmoil and infighting among democrats, Clinton Rape allegations, and Election Rigging. There are far fewer spikes from tweets filtered from Trump. We identify peak [3] from the Figure 7 as a widely shared URL that prematurely declared Donald Trump the Presidential victor on Oct. 27, 2016.

We previously identified popular URLs by plotting their occurrence percentage against tweet activity. Figure 1(a) shows the temporal patterns of the most widely shared URL occurring in our tweet set. This URL accounted for 14 percent of the total URLs shared within our corpus and made an aggressive appearance on Nov. 4, 2016, degrading to nearly no activity 16 hours later. Within the time period of peak [9] of Figure 7, it was shared a total 5,865 times, 118 times by one individual. Figure 8 displays temporal patterns from the second most active fake-news domain selected from our corpus, dcclothesline.com. We found similar themes of Anti-Clinton and Pro-Trump sentiment as that of infowars.com however daily activity appeared more cyclic in nature and we find less aggressive periods of high tweet activity. We labeled prominent peaks similarly with the most widely shared URL and their occurrence. We provide temporal activity for the 3 most widely shared URL of each candidate in Figure 1 and Figure 2. From the six most widely shared URL we point several common characteristics:

1. There are considerably more URLs shared concerning Hillary Clinton.
2. Of the URLs shared sentiment seems to be Pro-Trump or Anti-Clinton.
3. Temporal persistence of aggressively shared URLs seems to stabilize no longer than 48 hours and typically less than 12 hour of a spike.

We next get a sense of the user landscape by exploring attributes of user accounts including account automation, and user account type.
Figure 6: Tweets per hour on all fake domains.
Figure 7: Tweets per hour for highest activity - Inforwars.com

  Tweet Count: 898
  Sample Tweet Text: ‘RT @RealAlexJones: Violence at Trump events was coordinated by Clinton campaign.’

  Tweet Count: 237
  Sample Tweet Text: “Hillary Clinton 'Haunted House' Goes Viral - https://t.co/KlpsSBstgDn #HillNo #TrumpAHorrorMovie”

  Tweet Count: 298
  Sample Tweet Text: “Donald Trump Has Won The 2016 Presidential Election https://t.co/RFcaWvNH0G”

  Tweet Count: 607
  Sample Tweet Text: “Clinton Insider: Rigging Only Way Hillary Can Win https://t.co/FmASmP2jnD via @realalexjones”

  Tweet Count: 362
  Sample Tweet Text: Crokked Hillary is facing indictment but not for Weiner gate! Video of breaking news. https://t.co/WqbYa2SRf8”

  Tweet Count: 902
  Sample Tweet Text: “Internal Coup Against Hillary Clinton Has Begun. Renowned State Dept. psychological warfare expert exposes...https://t.co/b6m4AF3NPZ”

  Tweet Count: 859
  Sample Tweet Text: “RT @RealAlexJones: Internal Coup Against Hillary Clinton Has Begun: Red Alert - https://t.co/Y8wTf6jD3t #tcot #tlot”

  Tweet Count: 290
  Sample Tweet Text: “RT @RealAlexJones: Hillary Clinton’s Rape Allegations Revealed - https://t.co/iKOA4jJ66u #ClintonRape #Hillary2016”

  Tweet Count: 5,587
  Sample Tweet Text: RT @PrisonPlanet: Hillary’s top guy is into satanic rituals. Let that sink in. #SpiritCooking https://t.co/GsPaxPyyUR”

  Tweet Count: 388
  Sample Tweet Text:RT @Joe_America1776: Hillary Clinton’s Darkest Secrets Will Be Revealed #TCOT #WakeUpAmerica #MAGA #PJNET https://t.co/HYKucyhSzn”
Figure 8: Tweets per hour for popular domain dcclothesline.com

  Tweet Count: 112
  Sample Tweet Text: "RT @PatriotGeorgia: BOOM! Irrefutable Proof Obama Lied to Protect Hillary Clinton’s Run for the White House — https://t.co/26OgEOmQOj"

  Tweet Count: 118
  Sample Tweet Text: "Wikileaks: Bill Clinton BOASTS of Hillary’s ‘Working Relationship’ with Muslim Brotherhood https://t.co/jTPjiYKUy via @DCClothesline"

  Tweet Count: 75
  Sample Tweet Text: "LYING/NARCISSIST Hillary Clinton On New FBI Probe: ’I Urge Everybody To Get Out & Vote Early!’ https://t.co/jvM6CiE6a via @DCClothesline"

  Tweet Count: 43
  Sample Tweet Text:"RT @DCClothesline: Proof Hillary Clinton and her foundation are working with the Russians to destroy America https://t.co/eRuTxApu0n https:...."

  Tweet Count: 32
  Sample Tweet Text: "WikiLeaks Email: New Clinton DOJ Investigator Tipped Off Hillary’s Campaign During First Investigation #TCOT https://t.co/jaOFTuH4j"

  Tweet Count: 39
  Sample Tweet Text: "Assange: ISIS and Hillary Clinton Both Get Their Money From the Same Sources — https://t.co/UM6tkMHvzK"

  Sample Tweet Text: ‘MOP SECRET’ – Hillary Clinton Directed Her Maid to Print Out Classified Materials https://t.co/YhAilMBh
4.3 The User Landscape

4.3.1 Account Automation

Previous research and reporting have linked bots to the proliferation of fake-news urls on social media [14]. We investigated automation by utilizing Truthy’s BotOrNot API [1]. The BotOrNot API allows developers to query a user account, identified by a user id, and performs a query on ‘several classes that identify whether an account exhibits bot-like features or human features’ [12]. The API returns an overall score of each account as well as six additional sub-categories on a 0 to 1 scale. Accounts that appear more ‘bot-like’ are given an overall score that ranges between 0.5 and 1 and accounts that are scored more ‘human-like’ contain an overall score between 0 to 0.5. We performed a query using the BotOrNot API over the entire set of users within our tweet data set.

Based on previous research we hypothesized that the highest activity users would be classified as more bot-like than human-like. We first calculated the average BotOrNot score across all domains and further broke down our results per candidate. Additionally, we performed a correlation between bot-scores and tweet activity for each user. A user’s tweet was considered the sum of their tweets occurring across all domains. We classified users as likely-human/low-activity, likely-bot/low-activity, likely-human/high-activity and likely-bot/high-activity.

Our correlation and calculations yielded unexpected results. We find that the highest average BotOrNot score occurred in one of the lowest-activity domains. Average BotOrNot scores were slightly higher for users found in tweets from our ‘Trump’ stream and scores overall were categorized as likely human. In general, our correlation follows a normal distribution among BotOrNot scores and tweet activity (Figure 9).

We performed a simple test to check the validity of BotOrNot scores. We plotted the Cumulative Normal Distributions of BotOrNot scores across all users and a randomly selected set of 1000 users selected from our corpus. Figure 10 shows the CDF of the randomly selected set of users shifted left. To investigate whether the samples exhibited any difference in distribution we performed a KolmogorovSmirnov 2-sample test between the randomly selected users CDF and our total users CDF. Our calculations are summarized in the Table 2. We cannot reject the null hypothesis and cannot conclude that there is any difference between the two samples.

Table 2: 2-Sample K-S test of 1000 randomly selected User’s and Entire Population

<table>
<thead>
<tr>
<th>p-value</th>
<th>statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.2589896</td>
<td>0.0030405</td>
</tr>
</tbody>
</table>
Figure 9: BON Score vs. # Tweets - All Domains - Clinton/Trump

Figure 10: BotOrNot CDF - Random Sample vs. All Users
4.3.2 Verified, Deleted and Suspended Accounts

Twitter features a capability that allows some accounts (typically those of public interest) to register as a verified user. According to Twitter’s Help Center this feature “lets people know that an account of public interest is authentic” [5]. We classified user account type within our corpus by querying the “Verified” attribute of each user account using Twitter’s API. We identified 24 verified accounts, 469 deleted accounts and 550 suspended accounts. The nearly 1,000 missing accounts from our corpus may have contributed to bot activity. We know from previous research that detected bot activity came to halt near and slightly after the end the Presidential Election [16]. Additionally Bot behavioral patterns such as aggressive following or aggressive tweeting have historically been detected by twitter and suspended. These suspended and deleted accounts may have contributed to a potential bot population. Table 4 summarizes a list of verified user screen names and the number of fake news urls shared. Most notable is the Twitter account associated with the @RealAlexJones, founder of infowars.com and Ann Coulter, a well known conservative commentator as they are the highest contributors, from our verified user set, of fake news URLs. Another interesting observation during analysis of the verified accounts was the presence of the ‘OK’ hand-gesture emoji (Figure 12). It has been debated that this symbol is associated with such hate groups as the ‘KKK’ but according to the Anti Defamation League “The ‘OK’ hand gesture hoax originated in February 2017 when an anonymous 4channer announced ‘Operation O-KKK’, telling other members that ‘we must flood Twitter and other social media websites’ claiming that the OK hand sign is a symbol of white supremacy.’ [4]. It has since become popular among ‘alt-right’ sympathizers as “troll bait” to attract arguments among opposition [10]. While the emoji does not appear on the twitter front pages of 2 of the 24 verified users(@PrisonPlanet and @JeffTutorials - Figure 13) it does appear on our saved bookmarks (Figure 12). Sentiment among these two users tended to be xenophobic, misogynistic, peppered with ‘Pro-Trump’ and ‘Anti-Democrat’ sentiments.

Table 3: Account/Unique User Status Breakdown

<table>
<thead>
<tr>
<th>Total Accounts</th>
<th>Verified</th>
<th>Not Found</th>
<th>Susp</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>21196</td>
<td>20153</td>
<td>469</td>
<td>550</td>
<td>24</td>
</tr>
</tbody>
</table>
Table 4: Verified Accounts and Tweet Activity of Fake News URLs

<table>
<thead>
<tr>
<th>Screen</th>
<th># Tweets</th>
</tr>
</thead>
<tbody>
<tr>
<td>@RealAlexJones</td>
<td>26</td>
</tr>
<tr>
<td>@kevinvaccaro</td>
<td>11</td>
</tr>
<tr>
<td>@PrisonPlanet</td>
<td>3</td>
</tr>
<tr>
<td>@scottisbell_</td>
<td>2</td>
</tr>
<tr>
<td>@AnnCoulter</td>
<td>1</td>
</tr>
<tr>
<td>@CassandraRules</td>
<td>1</td>
</tr>
<tr>
<td>@EricWilliamsYO</td>
<td>1</td>
</tr>
<tr>
<td>@FreeJesseJames</td>
<td>1</td>
</tr>
<tr>
<td>@GerryCallahan</td>
<td>1</td>
</tr>
<tr>
<td>@JeffTutorials</td>
<td>1</td>
</tr>
<tr>
<td>@KenWahl</td>
<td>1</td>
</tr>
<tr>
<td>@KimDotcom</td>
<td>1</td>
</tr>
<tr>
<td>@StefanMolyneux</td>
<td>1</td>
</tr>
<tr>
<td>@Tess_Townsend</td>
<td>1</td>
</tr>
<tr>
<td>@bronk</td>
<td>1</td>
</tr>
<tr>
<td>@cate_long</td>
<td>1</td>
</tr>
<tr>
<td>@davelucas</td>
<td>1</td>
</tr>
<tr>
<td>@georgegalloway</td>
<td>1</td>
</tr>
<tr>
<td>@larryelder</td>
<td>1</td>
</tr>
<tr>
<td>@mitchellvii</td>
<td>1</td>
</tr>
<tr>
<td>@thowardtrowne</td>
<td>1</td>
</tr>
<tr>
<td>@sabena_siddiqi</td>
<td>1</td>
</tr>
<tr>
<td>@swin24</td>
<td>1</td>
</tr>
<tr>
<td>@AlyssaEinDC</td>
<td>1</td>
</tr>
</tbody>
</table>
4.3.3 URL Analysis

To explore the user landscape we performed source analysis upon each of the three most popular URLs for each candidate. We captured the first (source) account that shared the URL, the time it was created and the URL shared. Our results are summarized in Table’s 5 and 6. The most widely shared URLs exhibited classic bot activity. Screen name “AV38914670” shared http://www.infowars.com/spirit-cooking-clinton-campaign-chairman-invited-to-bizarre-satanic-performance/, 99 times over a 45 minute period, then again 19 times over a period of 10 minutes. While this tweet frequency is completely within the realm of possibilities of human capabilities, we looked closer at the smallest intervals between posts and find many consecutive postings spaced as small as 9 - 11 seconds apart. We performed a manual inspection of the user account belonging to screen name @AV38914670 on May, 8 2017. This account exhibits attributes consistent of bot activity such as low account duration, high follower to followee ratio and a high tweet activity. @AV38914670 joined twitter in Oct. 2016, has tweeted over 6,535 times, contains a low amount followees (14) and only follows (118), and has received 2,841 likes since joining (Figure 11). We suspect bot behavior patterns such as following, and tweet frequency may have adjusted to remain inconspicuous to twitter’s algorithms that detect and suspend for such activities. We manually inspected tweeting patterns in the remaining five URLs and did not identify such aggressive tweeting. However, two of the three most popular URLs from the “Hillary Clinton” stream, originate from accounts associated with two fake-news domains within our truth base, @PrisonPlannet and @redflagnews.
### Table 5: Clinton Popular Urls - First Tweet

<table>
<thead>
<tr>
<th>Date</th>
<th>Screen Name</th>
<th>URL</th>
</tr>
</thead>
</table>

### Table 6: Trump Popular Url - First Tweet

<table>
<thead>
<tr>
<th>Date</th>
<th>Screen Name</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Oct 25 00:00:54 +0000 2016</td>
<td>mhankin9737</td>
<td><a href="http://www.infowars.com/video-hillary-personally-ordered-donald-duck-to-troll-trump-rallies/">http://www.infowars.com/video-hillary-personally-ordered-donald-duck-to-troll-trump-rallies/</a></td>
</tr>
</tbody>
</table>
Figure 11: @AV338914670 Twitter Page and BotOrNot Score
Figure 12: ‘ok’ hand gesture emoji used as troll-bate among alt-right sympathizers

Figure 13: @PrisonPlanet and @JeffTutorials Twitter Profiles
5 Conclusion

We conducted a study that explored the spread of fake news across Twitter’s social media platform during the time period of Oct. 25, 2016 to Nov. 7, 2016. In summary, we find that the most popular fake news URLs were aggressively shared over a short time period with frequency and volume diminishing within 12 to 48 hours. We feel our exploration to understand the user landscape regarding account automation was more revealing using manual inspecting to detect classic attributes of bots such as high follower/followee ratio, aggressive tweeting, from newly established accounts. Additionally it is the main author’s opinion that BotOrNot should be used with caution in establishing any conclusion to identify account automation. Manual use of BotOrNot’s Web API among users in this corpus (who seemed to be bot-like) and real word users (who are not bots) have shown to have similar overall scores. Clearly this is a point of contention and further research should be conducted to improve the algorithms accuracy. Further analysis not mention in this study reveal no significant difference between the sub categorical scores and overall scores of BotOrNot. Our analysis of the most popular urls propagated throughout the last two weeks of the campaign period revealed, in general, “Anti-Clinton” and “Pro-Trump” sentiment, and two users from verified accounts that seem to sympathize with the ‘alt-right’. Fake-news urls seem to originate from fake news sites, among which the most popular seem to at some point be propagated very aggressively by accounts that exhibit bot-like behavior.
References


