

SHARK20385

A look into automated weaponization of stolen credentials
and the impact to Internet forum and social media discourse.

JULY 24, 2018



groupsense.io

ABOUT THIS REPORT

GroupSense is a cyber reconnaissance company focused on targeted intelligence for enterprise clients and governments. As a matter of course, GroupSense performs research to identify possible threat actors and indicators affecting their clients. The findings in this report are the result of research related to GroupSense's election monitoring clients. While the data in the report appears to make a compelling case for robot network (botnet) activity and election interference, it is not comprehensive; further research is being conducted.

It is important to note that given the ephemeral nature of social media content, much of the material associated with the researched accounts has been removed. This report is based on information acquired through July 24, 2018.

GroupSense investigated an email address listed in the Mueller indictment, Case 1:18-cr-00032-DLF UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC; filed 02/16/18. The email address "allforusa@yahoo.com" was identified as being "engaged in operations to interfere with elections and political processes." The email address was found in the GroupSense BreachRecon database along with its password. That password appeared to be computer generated and inspired further investigation, **netting 9.5 million addresses with similar seemingly computer generated passwords.** The "allforusa@yahoo.com" email address was associated with an active Reddit account used to aggressively push AllforUSA stories. GroupSense research also shows the possible use of compromised addresses to operate Facebook and Twitter accounts that distributed a wide variety of inflammatory memes. Further, some of the addresses are associated with comments posted on the FCC Net Neutrality debate site.

There may be a pattern of combining these stolen email addresses with other identity data to create false but credible user data. It is plausible that email addresses involved in major breaches are being harvested and reassigned for myriad uses. AllforUSA was linked to Russia's Internet Research Agency (IRA), and it is possible the account was hijacked or created for the sole purpose of "...engaging in operations to interfere with elections and political processes" by the IRA. It is more likely that the IRA simply purchased a group of orphaned, hijacked accounts from a dark net market. Regardless, the pervasiveness of breaches and the prevalence of unmonitored or unused accounts creates a powerful combination for fraud and manipulation of social outreach.

EXECUTIVE SUMMARY



GroupSense discovered 9.5 million email addresses with seemingly similar computer generated passwords.

The initial investigation conducted by GroupSense resulted in the following findings:

- Reverse searches matching third-party breached data revealed 9.5 million email accounts apparently related¹ to "allforusa@yahoo.com."
 - Hijacked email accounts have been paired with other stolen credential data to carry out campaigns. In addition, there may be examples of new online personas created using additional hijacked email accounts.
 - Many of the associated email accounts were used to post potentially fraudulent comments to the FCC Net Neutrality filing site.
 - Online activity including a website and social media accounts associated with "AllforUSA."
 - Compromised email accounts promoted biased content in an attempt to influence global issues.
 - Compromised email accounts are used in site-for-hire activities.
-
- Compromised email accounts are being used to influence public opinion on important topics.
 - The availability and sheer volume of these compromised accounts enables threat actors to conduct campaigns under the guise of actual citizens.
 - Threat actors, including the operators of AllForUSA, are using common tools such as freelancing sites to conduct illicit activity, leveraging search engine optimization (SEO) and other common marketing tools.

THE BREAKDOWN

WHAT IT MEANS



SEO stands for "search engine optimization." It is the process of getting traffic from the "free," "organic," "editorial" or "natural" search results on search engines.²

¹ Relation is due to similar seemingly machine-created passwords.

² <https://searchengineland.com/guide/what-is-seo>

On Friday, February 16, 2018, Special Counsel Robert Mueller announced the indictment of 13 individual Russians and three Russian commercial entities, accusing them of conspiring to interfere with the 2016 US presidential election. The indictment cites several incidents in which members of these Russian organizations attempted to influence the American public to support Republican presidential candidate Donald Trump, while at the same time working to heighten feelings of anger and distrust toward Trump's Democratic opponent, Hillary Clinton.

As this news broke, the GroupSense research team took note of a table on page 33 of the Mueller Indictment.

92. On or about the dates identified below, Defendants and their co-conspirators obtained and used the following fraudulent bank account numbers for the purpose of evading PayPal's security measures:

Approximate Date	Card/Bank Account Number	Financial Institution	Email Used to Acquire Account Number
June 13, 2016	xxxxxxxx8902	Bank 2	wemakeweather@gmail.com
June 16, 2016	xxxxxx8731	Bank 1	allforusa@yahoo.com


Figure 1: Page 33 of the Mueller Indictment contains information provided to the Justice Department and indicating that the accused were using email addresses, social security numbers, home addresses and birth dates of real US persons in order to create PayPal accounts.

Within the Mueller indictment, the Justice Department listed multiple email addresses and other data used by the Russian defendants in the activities described in the indictment. It appears the email address "allforusa@yahoo.com" was included in the Anti-Public breach in December 2016. The Mueller indictment connects that email address with the creation of fake PayPal accounts to pay for various expenses, including Facebook ads supporting Trump and attacking Clinton.

GroupSense researchers were able to link one of the breached email addresses, "allforusa@yahoo.com," to a Reddit account that pushed links for pro-Trump stories from the website allforusa.com.

According to Facebook's own estimates³, ads such as the ones funded by the fake PayPal accounts tied to the "allforusa@yahoo.com" email address reached up to 126 million Americans.

The "allforusa@yahoo.com" email address is just one. There are as many as 9.5 million other email addresses just like it.



The "allforusa@yahoo.com" email address is one of 9.5 million compromised email addresses.

³ <https://www.axios.com/facebook-year-of-a-thousand-cuts-1528501241-ca826c23-9760-4ef3-802f-2c968622ff22.html>

Email Address	Password	Username	Email Provider	Email Domain	Database 1	Database 2	Database 3	Database 4	Database 5
@mtorola.com	shark00		mtorola	mtorola.com	Online Spambot	Yahoo.com			
@yahoo.com	shark00		yaho	yaho.com	Yahoo.com				
@hotmail.com	shark00		hotmail	hotmail.com	Online Spambot	Yahoo.com			
@html.com	shark00		html	html.com	MySpace	Online Spambot	Yahoo.com	Exploit In	
@espn.com	shark00		espn	espn.com	Online Spambot	Yahoo.com		Anti Public Combo List	
@hotmail.com	shark00		hotmail	hotmail.com	Online Spambot	Yahoo.com		Anti Public Combo List	
@roadrunner.com	shark00		roadrunner	roadrunner.com	Evony	MySpace		Online Spambot	Exploit In
@live.co.uk	shark00		live	live.co.uk	iMesh	Lastfm	MySpace	Online Spambot	
@hotmail.co.uk	shark00		hotmail	hotmail.co.uk	MySpace	Online Spambot	Yahoo.com	Exploit In	
@live.fr	shark00		live	live.fr	Yahoo.com				
@gmx.de	shark00		gmx	gmx.de	Anti Public Combo List	Exploit In	Yahoo.com		
@gmx.de	shark00		gmx	gmx.de	MySpace	Exploit In		Anti Public Combo List	
@tonline.de	shark00		tonline	tonline.de	Yahoo.com	Exploit In			
@yahoo.co.id	shark00		yahoo	yahoo.co.id	iMesh	Yahoo.com	Exploit In	Anti Public Combo List	mail.ru Dump
@yahoo.com	shark00		yahoo	yahoo.com	Dailymotion	Evony	MySpace		Yahoo.com
@web.de	shark00		web	web.de	Online Spambot	PSX-Scene	Yahoo.com	Exploit In	Anti Public Combo List
@nadianu.com	shark00		nadianu	nadianu.com	Twitter.com	Exploit In	Anti Public Combo List		
@gmail.fr	shark00		gmail	gmail.fr	Yahoo.com				
@yahoo.com	shark00		yahoo	yahoo.com	iMesh	Dailymotion	Adobe		Twitter.com
@yahoo.com	shark00		yahoo	yahoo.com	Furimotion	MySpace	Online Spambot	Yahoo.com	Exploit In
@hotmail.com	shark00		hotmail	hotmail.com	iMesh	Yahoo.com	Exploit In	mail.ru Dump	
@yahoo.com	shark00		yaho	yaho.com	Yahoo.com	Exploit In	Anti Public Combo List		
@tmail.com	shark00		tonline	tmail.com	Yahoo.com	MySpace	Online Spambot	Anti Public Combo List	
@161.com	shark00		161	161.com	Yahoo.com				
@gmail.com	shark00		gmail	gmail.com	Twitter.com	Exploit In			
@web.de	shark00		web	web.de	Twitter.com				
@gmail.com	shark00		gmail	gmail.com	Twitter.com	Exploit In		Bitcoin Security Forum Gmail Dump	
@gmail.com	shark00		gmail	gmail.com	BTSec	Evony	LinkedIn	Online Spambot	
@gmail.com	shark00		gmail	gmail.com	Yahoo.com	Exploit In	MySpace		Bitcoin Security Forum Gmail Dump
@hotmail.com	shark00		hotmail	hotmail.com	Yahoo.com				
@yahoo.com	shark00		yahoo	yahoo.com	Yahoo.com	Exploit In	Anti Public Combo List		
@yahoo.com	shark00		yahoo	yahoo.com	Yahoo.com	Anti Public Combo List			
@yahoo.com	shark00		yahoo	yahoo.com	Yahoo.com	Anti Public Combo List			
@yahoo.com	shark00		yahoo	yahoo.com	Yahoo.com	Anti Public Combo List			
@yahoo.com	shark00		yahoo	yahoo.com	MySpace	Yahoo.com			
@yahoo.com	shark00		yahoo	yahoo.com	Yahoo.com	Anti Public Combo List			

Figure 2: List of email addresses that may be compromised and centrally controlled.

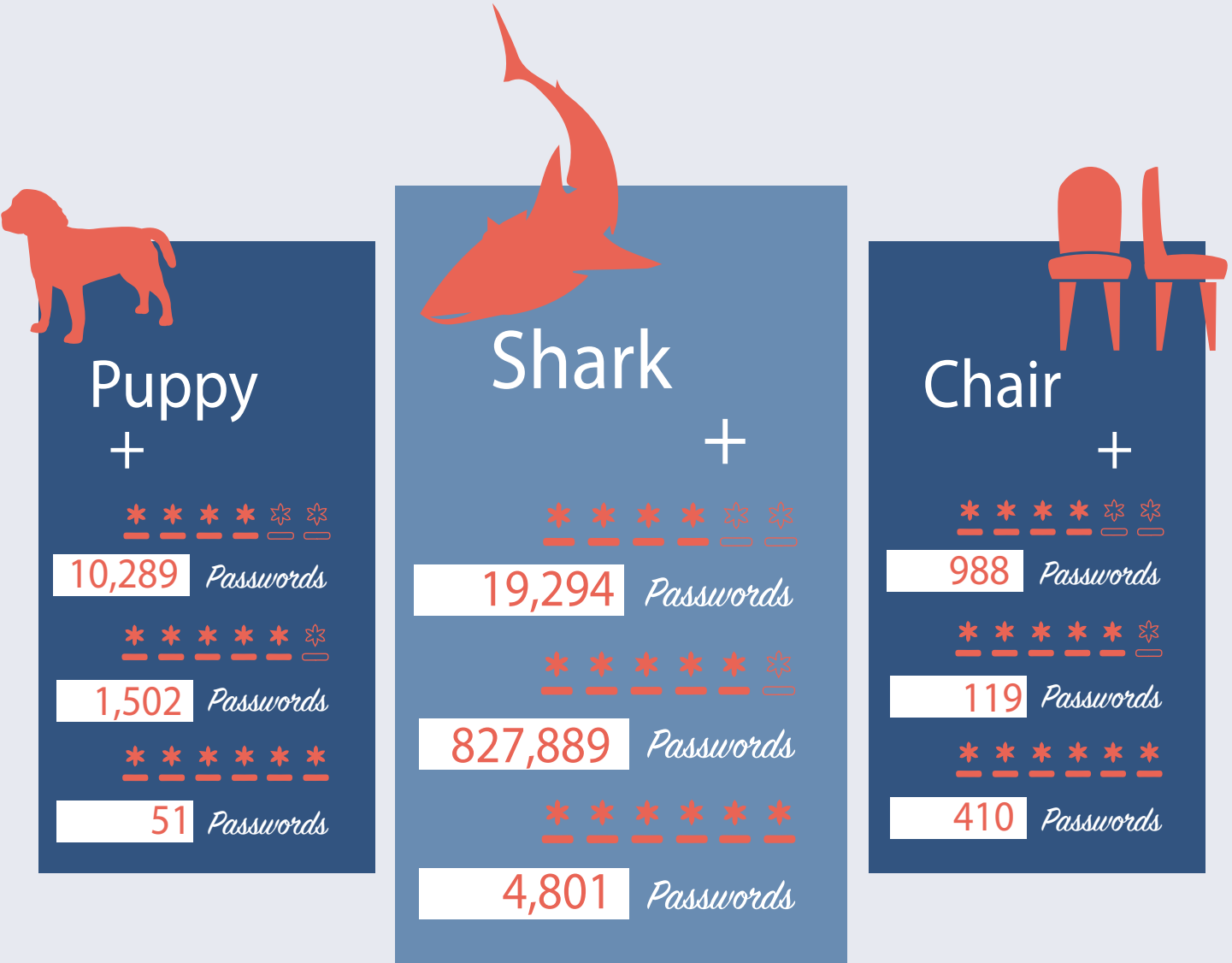
The GroupSense BreachRecon database contained the email address “allforusa@yahoo.com” with a password of “shark” followed by five digits. First, the GroupSense team ran a **reverse search** to see if other accounts used the same password, discovering between 10-15 email addresses with an exact match. While this is a small number, it led GroupSense to believe it was possible that all of these accounts were centrally controlled.



Reverse search is done by looking for inputs which generate the same output.

As a result, GroupSense conducted additional research. It is a common technique for threat actors to reuse passwords or use very similar passwords, so GroupSense searched for slight variations on the original password used by “allforusa@yahoo.com.” The expanded search produced 1,346,534 hits, an exceptionally high number. For comparison, researchers

analyzed two other random words with five characters, chair and puppy. As expected, as the number of total characters in the password increases, the total number of passwords decreases. This is because people commonly use as few characters as possible so that they can remember their passwords.



Generally, the number of longer passwords decrease as the passwords increase in character count.

With the word Shark+ some number of characters, researchers observed an overall higher number of passwords, along with the 40X increase from Shark+4 to Shark+5, which is unusual. The overall higher volume of passwords is a strong indicator that the Shark+5 passwords were automatically generated.

When analyzing the 1,346,534 passwords, researchers observed that only 168 of them contained the number 9. For comparison purposes, 599,776 passwords contained the number 3 and 598,514 passwords contained the number 6. Given the low prevalence of the number 9 in the larger data set, it is likely that due to a computational reason, the number 9 is excluded from the password generation.

GroupSense searched their BreachRecon database with a **regular expression** pattern to identify all 10-character passwords starting with five letters and ending with five digits. This search resulted in a list of seven passwords types containing a five-letter word and the same incremental number pattern.

SIGNIFICANCE OF PASSWORDS WITH "SHARK" PLUS FIVE CHARACTERS



People tend to use short passwords they can remember, so seeing 40 times more passwords with nine characters than with eight characters is highly unusual.

The seven words were:

1

shark

2

march

3

lunch

4

glass

5

table

6

frame

7

phone

These words (plus five numbers) produced lists with approximately 1.3 million credentials each. Strangely, most of the passwords did not contain the number 9, as above. **After removing duplicates and excluding the small number of accounts containing a 9 in the password, GroupSense found 9,453,137 email accounts matching the "allforusa@yahoo.com" password pattern.**

In the Mueller indictment, many of the email handles could have represented organizations ("unitedvetsofamerica@..." and "patriotus@...") while others could have been based on ideological stereotypes (staceyredneck@...). Many of the 9.5 million compromised email addresses seemed like personal email accounts.

WHAT WE DON'T KNOW ABOUT THE HIJACKED ACCOUNTS

Based on the initial email addresses that matched the password pattern, researchers used various people lookup services, user name checkers, and other open source intelligence tools to find details like phone numbers, alternative email addresses, and physical addresses for a small sample of the email accounts discovered in this list.

GroupSense contacted two people from the list. One individual confirmed some personal information, but had no knowledge of the email address in question. The email address is a Gmail account, and this individual said he would not have used the naming convention firstname.lastname because of privacy concerns.

The second person GroupSense reached said there was no one by the name associated with the email address from the breach database at their address. These results led GroupSense to conclude that threat actors combined email addresses with other unrelated identity data to create plausible fake identities.

Testing this premise on a large scale is costly and requires significant human effort. GroupSense has published free access to the query against the breached accounts and encourages individuals who are affected to reach out. The public can access the tool at <http://breachrecon.com>.

In an effort to find evidence supporting the automated leveraging of compromised addresses, researchers investigated the FCC Net Neutrality site.

COMPROMISED ACCOUNTS USED IN THE NET NEUTRALITY DEBATE

Net neutrality is the principle that internet service providers (ISPs) treat all data on the internet equally, and do not discriminate or charge differently by user, content, website, platform, application, type of attached equipment or method of communication. Prior to ruling on Net Neutrality, the FCC provided an internet forum for feedback. Nearly 22 million comments were posted between April 27 and August 30, 2017. Since the FCC publishes an API facilitating a programmatic ability to post, researchers believe bots were utilized to post false comments en masse.⁴

- The Pew Research Group estimated that just 6% of the comments were unique; the other 94% of the comments were duplicates.^{5,6}
- Fiscalnote found that hundreds of thousands of comments came in just two days.⁷
- Platform developer Gravwell found that more than one million comments in July 2018 had a pornhub.com email address. In January 2018, Gravwell could only find 55 people with pornhub email addresses.⁸

GroupSense analyzed the FCC Net Neutrality proceedings to see how many commenters used compromised email addresses from the BreachRecon findings. GroupSense found 33,053 unique email addresses from a random subest of approximately half of the 9.5 million compromised email addresses used to post at least one comment. Breaking that down even further, 27,559 email addresses were used to post only one comment, while another 5,514 commenters used the email addresses to post at least two comments. A total of 40,041 filings were submitted using the compromised email addresses.

“Don’t kill net neutrality. We deserve a free and open Internet with strong Title II rules. This will ensure that the flow of data is determined by the interests of Internet users.”

Figure 3: An example of an automated posting to the FCC site during the Net Neutrality comment period. To view a sample of the filings, see the Appendix.

⁴Examples of the FCC comment language are available in the Appendix.

⁵<http://www.pewinternet.org/2017/11/29/public-comments-to-the-federal-communications-commission-about-net-neutrality-contain-many-inaccuracies-and-duplicates/>

⁶Many of the duplicates may not be bot generated, but a result of multiple email campaigns urging citizens to post specific content. Of course, these email campaigns could also be malicious in nature.

⁷<https://www.wired.com/story/bots-broke-fcc-public-comment-system/>

⁸<https://www.gravwell.io/blog/discovering-truth-through-lies-on-the-internet-fcc-comments-analyzed>

GroupSense researchers took a closer look at the 18 entities who filed ten comments, noting that none of the commenters using compromised emails initiated more than 10 filings.



The repetitive nature of the posted comments indicates that they were likely posted by a machine, or bot.

- Of the 180 filings from these 10 commenters, only five were used just once by a single commenter.
- A single commenter posted 10 in total, seven on the same day and four of those in the exact same second.
- Six commenters used the same filing all ten times.

WHY THIS IS IMPORTANT

Using the Net Neutrality issue, which sparks heated debate along partisan lines, allows us to transition from general information to a specific use case that illustrates the extent of the compromised accounts. Members of the Democratic Party generally support regulations making all users of the internet equal, whether they are individuals or corporations. Republicans, who tend to oppose such regulation, usually side with those who believe changes to net neutrality could fuel new growth and technological innovation. The total content of the allegedly false net neutrality comments does not consistently align with either party. However, the filings posted by compromised email accounts with 10 or more filings were all in support of the Democrats' position on net neutrality.



In an effort to better understand the use case for the compromised accounts, GroupSense dug deeper into the activities of “AllForUSA.” As of June 2018, they have found the following web properties, all pushing politically charged content:

- Website: allforusa.com
- Twitter account: @allforusa
- Potentially related Twitter account: @allforusa11
- Reddit account, removed since initial discovery
- Freelancer.com posts recruiting bloggers to create content for US readers
- Business registration: All for One

ASSOCIATED ACTIVITY

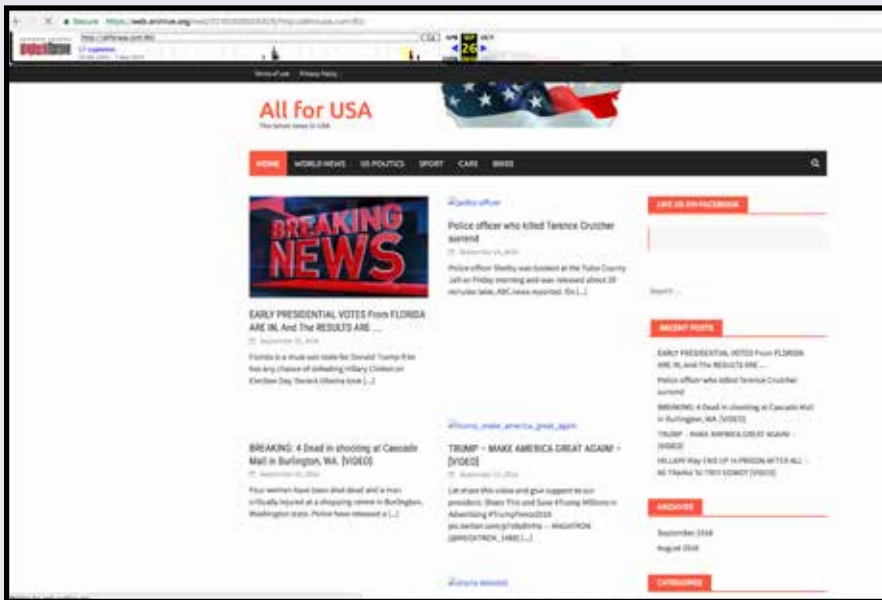


Figure 4: Screenshot of AllforUSA.com.

GroupSense investigated the website allforusa.com, which appeared to be dedicated to sharing material denigrating Hillary Clinton and former President Barack Obama. Using the Wayback Machine, a digital archive of the World Wide Web and other information in the internet, researchers pieced together the site's past content.

ALLFORUSA.COM

The timeline below shows the digital history of the domain allforusa.com.



Figure 5: Screenshot of the Wayback Machine.



Figure 6: Screenshot of the site creation message, dated February 10, 2005.



Figure 7: The July 2005 Whois record for allforusa.com. See section titled "All for One - A Business Associated with allforusa.com" for more information.

February 10, 2005

This is the first record GroupSense researchers found; it shows a message indicating an account has been created and that when DNS servers are updated, the user could access the site at its permanent address, allforusa.com

July 7, 2005

Jesse Allen, 71, of Brownsburg, Indiana, registered the domain.



Figure 8: allforusa.com from January 12, 2006, indicating the site is closed.

January 12, 2006

allforusa.com was closed. Researchers were unable to locate any digital record of the domain's content until a January 12, 2006 record indicating that the site was closed.

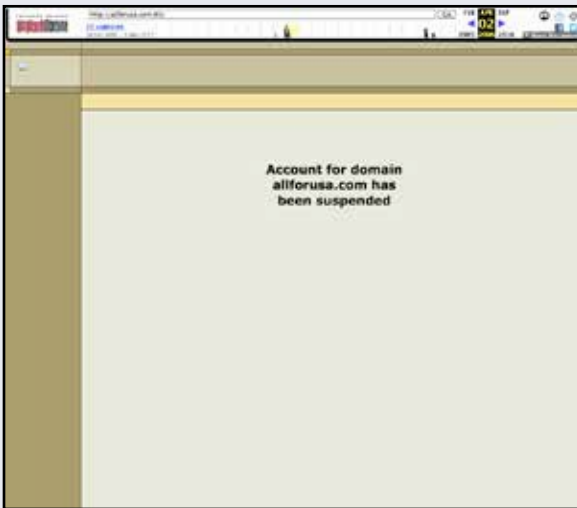


Figure 9: Screenshot of allforusa.com from April 2, 2006 indicating the domain has been suspended.

April 2, 2006

The allforusa.com domain was suspended.

April 28, 2015

Jesse Allen, the domain's owner of record, dies. GroupSense researchers were unable to reach any family members to confirm whether they were aware that he had been operating allforusa.com. Researchers from the Washington Post are conducting additional outreach



Figure 10: Screenshot of AllforUSA from September 1, 2016.



Figure 11: Screenshot of whois record from September 5, 2016 showing ownership is now private.



Figure 12: Pro-Trump and anti-Clinton content being promoted.

September 1, 2016

The Wayback Machine captures a new page in use for the first time in over a decade. The page contains links to pro-Trump, anti-Clinton stories.

September 5, 2016

Domain ownership for allforusa.com becomes private.

November 20, 2016

Post election, the site continued to promote pro-Trump and anti-Clinton stories.

December 20, 2016

The Wayback Machine captured the url <http://allforusa.com/cgisys/suspendedpage.cgi>, which leads to a blank web page with the message "page not found."



Figure 13: Screenshot of Russian-operated gaming site taken on June 8, 2018.



Figure 14: Screenshot validating that allforusa.com is now a Russian-operated gaming site. (Translation by Google.)

June 8, 2018

Allforusa.com appears to be a Russian operated gaming site.

GroupSense researchers identified a number of subreddits pushing stories from the website allforusa.com. Reddit's use of vague language such as "submitted 1 year ago" indicates the observed posts were added anywhere between 365 to 720 days prior to the date of this report.

ALLFORUSA ON REDDIT



Figure 15: Screenshot of subreddits pushing content from allforusa.com.

In an attempt to determine what email address was associated with this Reddit account, GroupSense researchers conducted an experiment with the password reset function on Reddit. In order to reset a password on a Reddit account, a user must provide the Reddit username and the email address associated with that account. When using the email address "allforusa@yahoo.com," the researchers received a message saying "an email will be sent to that account's address shortly."

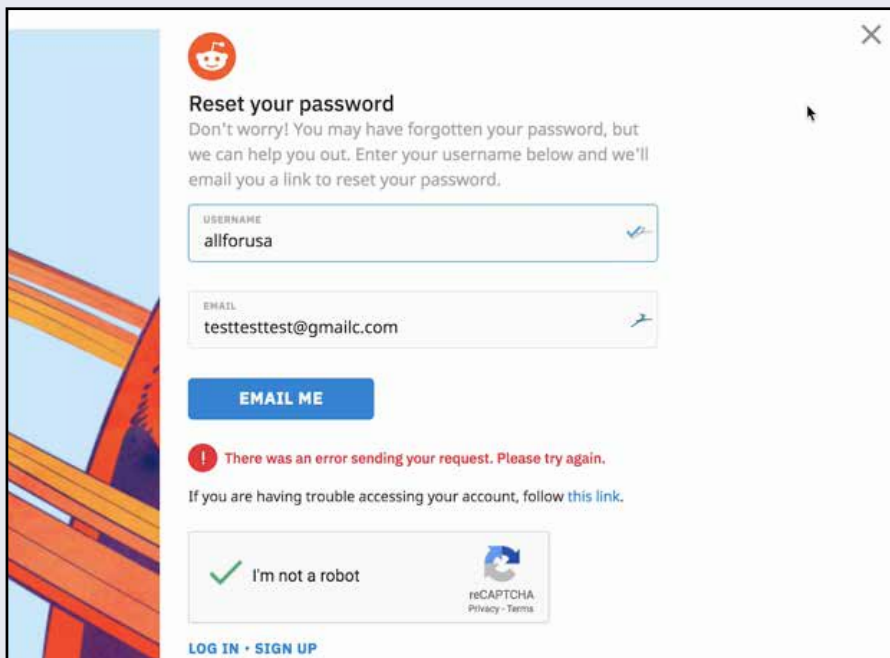


Figure 16: Failure message when researchers attempted to reset the password with a Gmail address.

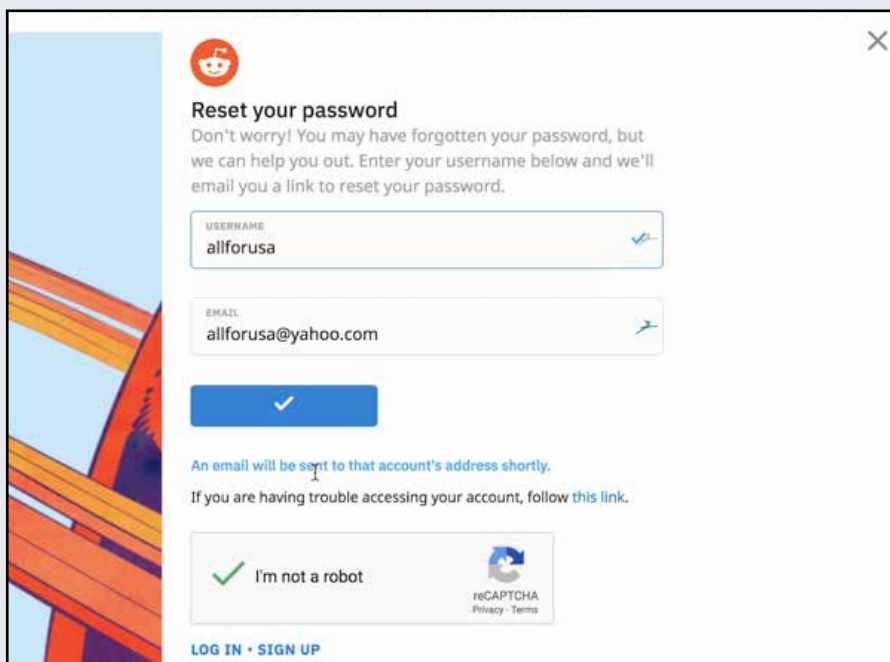


Figure 17: Success message when researchers attempted to reset the password with the "allforusa@yahoo.com" email address.

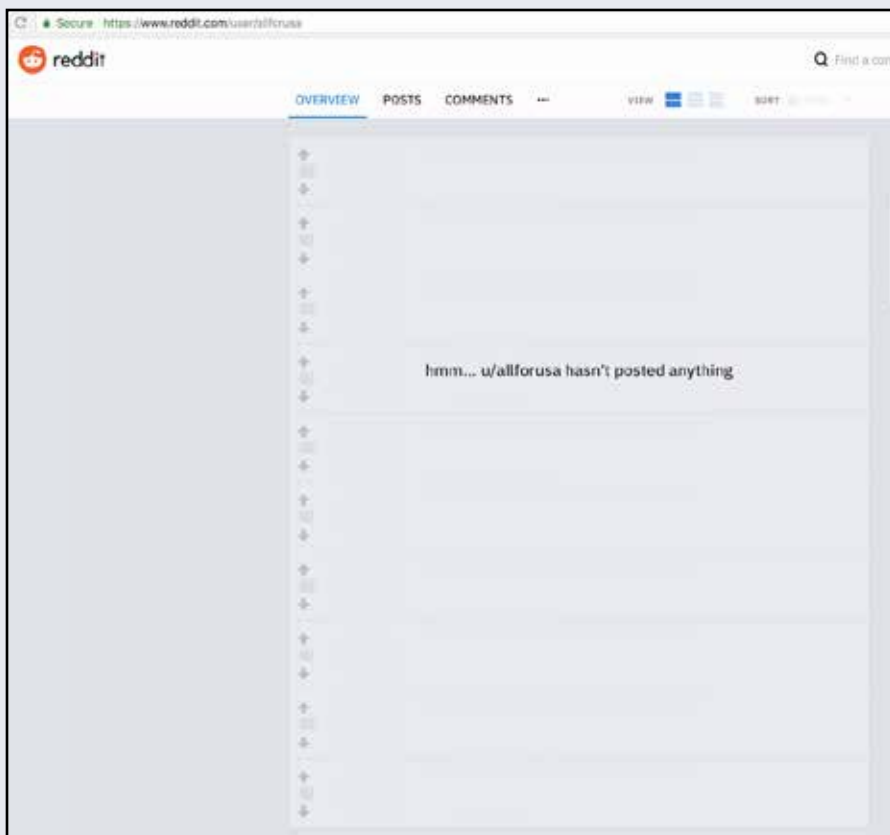


Figure 18: Screenshot illustrating the removal of all content associated with AllforUSA. (On the user details screen from reddit.com, the images are slightly different because Reddit has undergone cosmetic updates.)

This indicates that the email address “allforusa@yahoo.com” is connected to a Reddit thread called “allforusa.” **Shortly after attempting the email verification test, the AllForUSA account history was removed from Reddit.**

The timing of the removal of content could indicate that the operators were actively in control of the account and were alarmed by the password reset test.



Shortly after attempting the email verification test, the AllForUSA account history was removed from Reddit.

The Twitter handle @allforusa, which appeared to belong to “makingsenseofamerica,” published politically charged content. On December 10, 2010, the account featured a tweet saluting Senator Bernie Sanders for his filibuster on the US Senate floor, referring to that day’s news of Sanders’ 8½ hours speech on the Senate floor criticizing President Barack Obama’s proposed tax cut compromise with Republicans. While this is only one example of politically charged activity, it is plausible much of the tweet data has been deleted by the operator.

ALLFORUSA ON TWITTER



Figure 19: Screenshot of a tweet sent from the @allforusa Twitter account.

GroupSense searched Twitter for other mentions of "AllforUSA." Among the results were three tweets from @skipyourcommute, all of which point to a freelancer.com post attempting to recruit someone to run three different blogs.

OTHER ALLFORUSA TWITTER FINDINGS

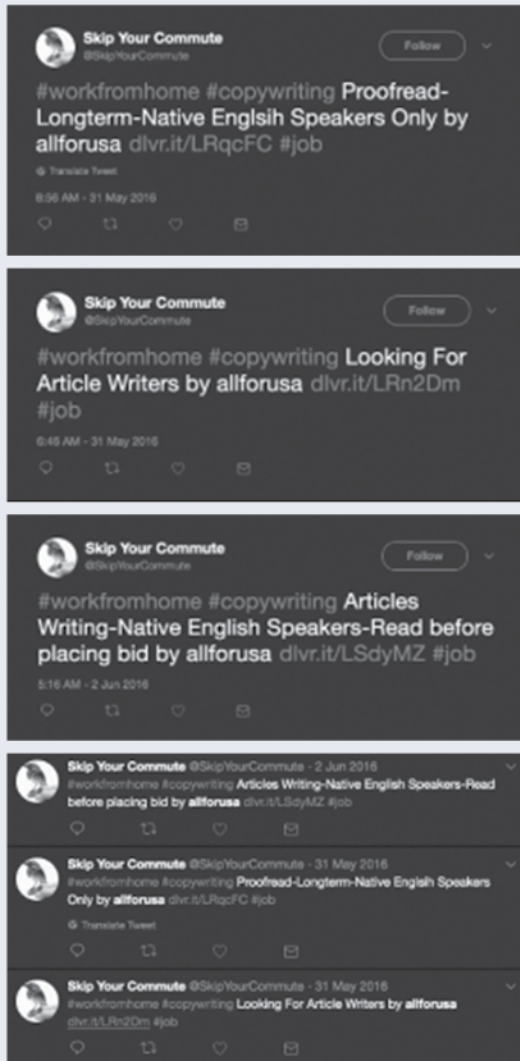


Figure 20: Collection of tweets from @skipyourcommute recruiting freelance writers to create content.

⁹<https://twitter.com/SkipYourCommute/status/737641308928380929>
<https://twitter.com/SkipYourCommute/status/737674050722398208>
<https://twitter.com/SkipYourCommute/status/738343474508922881>

GroupSense researchers determined that the shortened URLs pointed to the following freelancer posts:

- <https://www.freelancer.com/projects/articles/looking-for-article-writers-10653927/>
- <https://www.freelancer.com/projects/articles/articles-writing-native-english-speakers/>
- <https://www.freelancer.com/projects/articles/proofread-longterm-native-english/>

The freelance recruiting posts are no longer active, but examination of the posts determine that at least one of the contracts was awarded to the user profile "destinyoawaits."

It is a common practice to recruit guest bloggers to syndicate content to increase search engine optimization (SEO) and promote website traffic. In the post shown below, AllforUSA is looking for three individuals to run blogs promoting content of interest to US readers. Given that AllforUSA is referenced by @skipyourcommute via the tweets for the advertised freelancing, it is plausible that AllforUSA used this freelancing service to recruit bloggers.

freelancer

Connexion S'inscrire Publier un projet

Guest blogger needed (3) BUDGET \$30-250 USD

Freelancer > Employers > Article Writing > Guest Blogger needed (3)

We are looking for a guest blogger to run 3 (different) blogs for one month.

Each one of the (3) blogs will need a minimum of 22 posts per month.

The posts do not need to be original or written by you, it can be taken from other sources on the internet - as long as they are relevant to the topic (sport blog need to have only 100% sport posts on it). ALL blogs are dealing with USA based issues, and will need to have the posts refer to US readers (so there is no point in talking about Asian sports in those blogs). At least 10 of the posts need to have photos in them (text + photo).

All posts need to be clean and clear, they need to address the topic and can not deal with anything that is illegal or immoral. There should be no links placed in the body of the posts, it is however allowed to post credit for the original text on the bottom of no more than 10 posts.

You will need to log into the blogs, create and schedule the posting for the whole month, only after the work will be reviewed and accepted you will get the full payment.

In short:

3 different blogs, each one with at least 22 posts (total of a minimum 66 posts), 10 posts need to have photos in them (total 30 photos), all for USA readers and should address the particular topic of the blog, no need for original writing. Any live sample of actual blog work could help.

Thanks.

Compétences : Article Writing, Blog, Rédaction

en voir plus : work as blogger, work as a blogger, to create blogger, run blogger, looking for a blogger to work for, quest of a guest, get help for writing a blog, get a blogger, blogger looking for work, guest blogger needed, text writing on photo, help blogger, blogger work, blogger blogger, sports blog, need a blogger, guest writing, guest posts, guest post, guest blogs, guest blogger, guest blog post, blogger, blogger blog, blog blogger

Concernant l'employeur :

4.8 ★★★★★ (24 commentaires) Tortoise, France

N° du projet : 8834595

Vous cherchez à gagner de l'argent ? PROJET TERMINE

Votre adresse e-mail

Adresse e-mail

Postuler à des emplois similaires

Autres travaux de cet employeur

- Site Analysis Report (on 2 sites) (\$30-250 USD)
- 16 Fictional articles (1) (\$30-250 USD)
- 500 articles (not original) needed (scraping) #2 (\$30-250 USD)
- 12 Articles #2 (for walmart only) (\$30-250 USD)
- gmail + social site accounts set up (\$30-250 USD)

Travail antérieur Travail suivant

Travaux similaires

- Rédacteur pour des fiches de présentation d'entreprise (K250-750 EUR)
- Articles Sportifs (K8-30 EUR)
- Ecrire des articles en français (K50-80 EUR / heure)
- écrire un article (\$8-15 USD / heure)
- Articles about wall animal decoration (\$30-250 USD)
- SEO Content Writer (\$10-30 AUD)
- Story book writing needed (\$30-250 AUD)
- Blog writer for logo website. (\$10-30 USD)
- Need Ongoing Articles on Fashion (\$15-25 AUD / heure)
- Need content writer (1600-1500 INR)

Figure 21: Screenshot of post on Freelancer.com recruiting bloggers for allforusa.

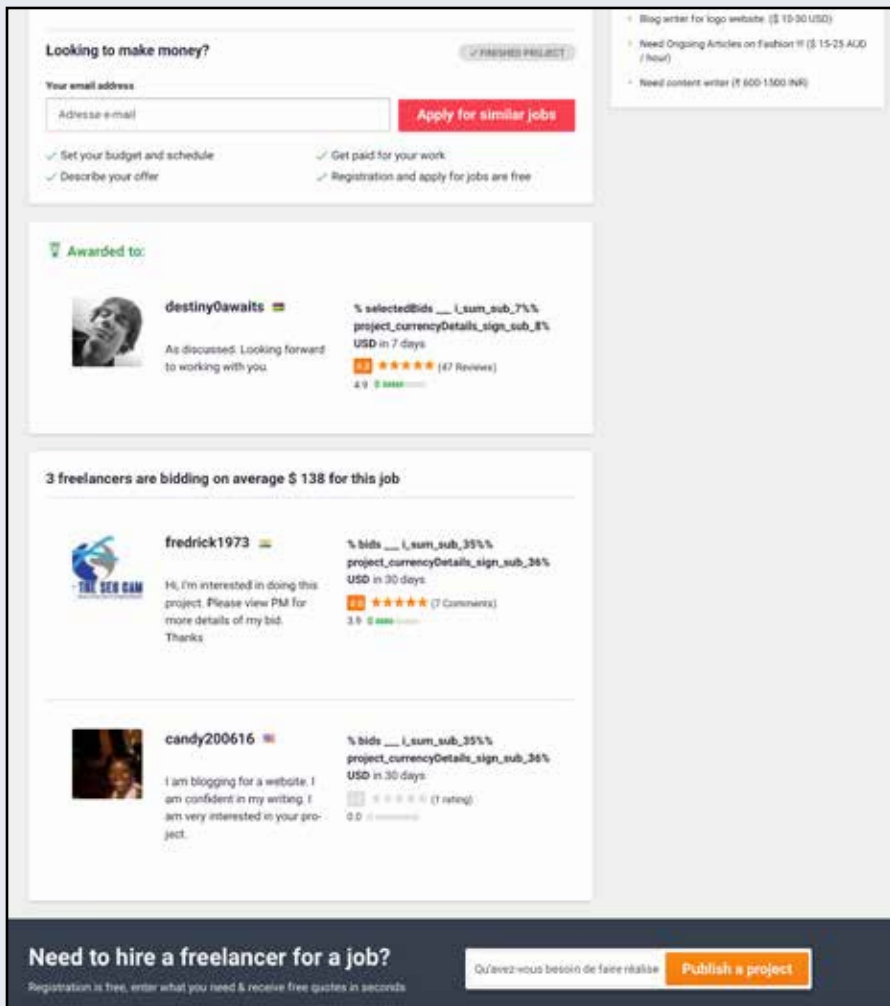



Figure 22: Screenshot showing user destinyoawaits won the contract to post blog content for @skipyourcommute. It is a common practice to recruit guest bloggers to syndicate content to increase search engine optimization (SEO) and promote website traffic. In the post shown below, three individuals are being recruited to run blogs promoting content of interest to US readers. The tweets by @skipyourcommute reference AllforUSA, as does the freelancer post. This led GroupSense analysts to conclude with some confidence the AllforUSA persona attempted to outsource blog publications in order to disseminate their content.

freelancer Login Register Publish a project



destiny0awaits

Language Expert / Writer / Translator / Proofreader / Social Media Management and Promotion

Throughout my experience as a freelancer, i have been able to fully use my language and journalism skills. Fluent in Dutch, English, French, German and Spanish, i completed a good number of projects including Article writing, Translations, Proofreading of blog and website contents. I also had some successful experience with Blog Management and SEO backlinking projects.

@destiny0awaits


Vancouver, MA (British Columbia)

Member since 28 February 2012

1 Recommendation

hire

\$35 USD/hr

5.4  74 reviews

81% completed work

99% According to the budget


99% On time

75% Refers rate


Freelancer > Freelancers and Maestros > Article Writers > destiny0awaits

Portfolio


Recent reviews [View destiny0awaits's Full Profile](#)




Translations English to French


5.0  \$50.00 USD


"Excellent Work, will hire again. Thank you very much"

IMAA  2 years ago

Certifications

US English Level 1  99%

UK English 1  83%

French to English Translation  82%


SEO Level 1  75%

Figure 23: Profile of recruited freelancer destiny0awaits. Given the nature of this account, there is a high probability that the user's photo is stolen from a legitimate account or gathered from a stock photography service.

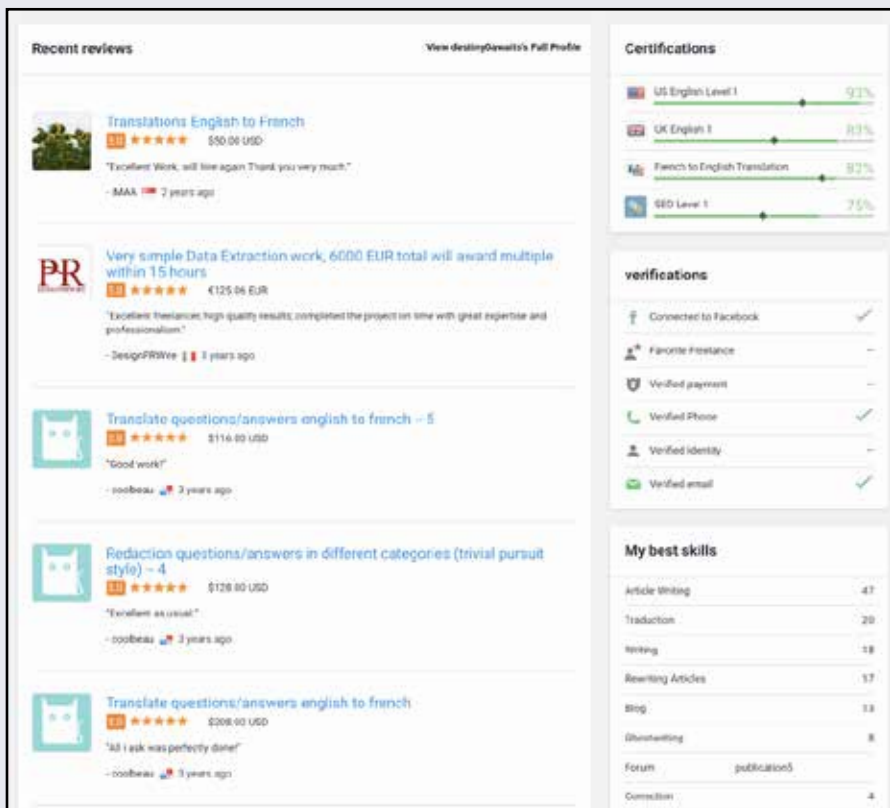


Figure 24: Screenshot of reviews of destinyoawaits.

Search results about the information in the destinyoawaits profile on freelancer.com turns up a travel blog hosted in Mauritius. While it is possibly a coincidence, a zero (0) separates the two words in the URL, similar to the user's handle.

GroupSense researchers created a profile on Freelancer.com and invited destinyoawaits to apply. Destinyoawaits responded to the request. When asked for work history, destinyoawaits stopped responding.

GroupSense researchers found stories pushing allforusa.com and other second hand political content on Google+. The researchers observed large time gaps in submissions and an eclectic mix of posts ranging from suggestions on Christmas gifts to political messages criticizing Mitt Romney for “made-up” tax returns. The post style and behavior are indicative of content-for-hire. Typically, the owner of a site-for-hire account will promote any content submitted to them in exchange for payment. The screenshots below demonstrate manifestations of the Google+ account owned by Meiling Chee, including promoted political content including from “AllforUSA.”

ALLFORUSA ON GOOGLE+

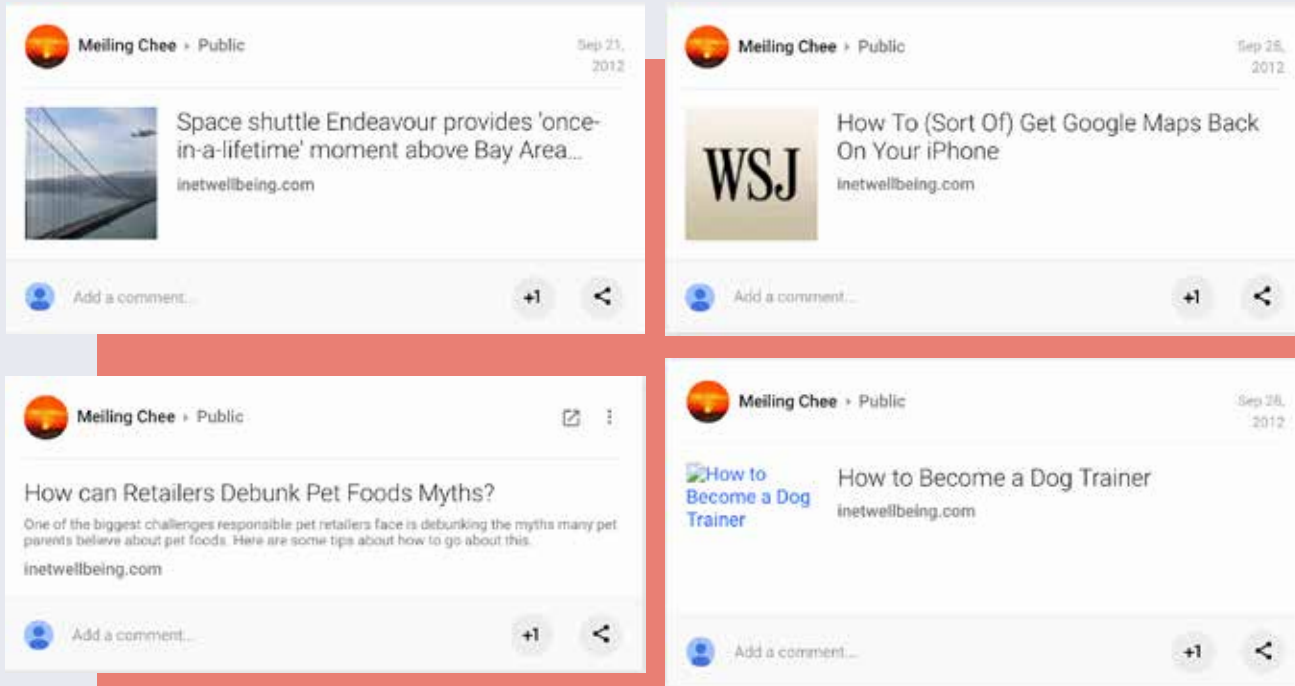


Figure 25: inetwellbeing.com post on Google+.

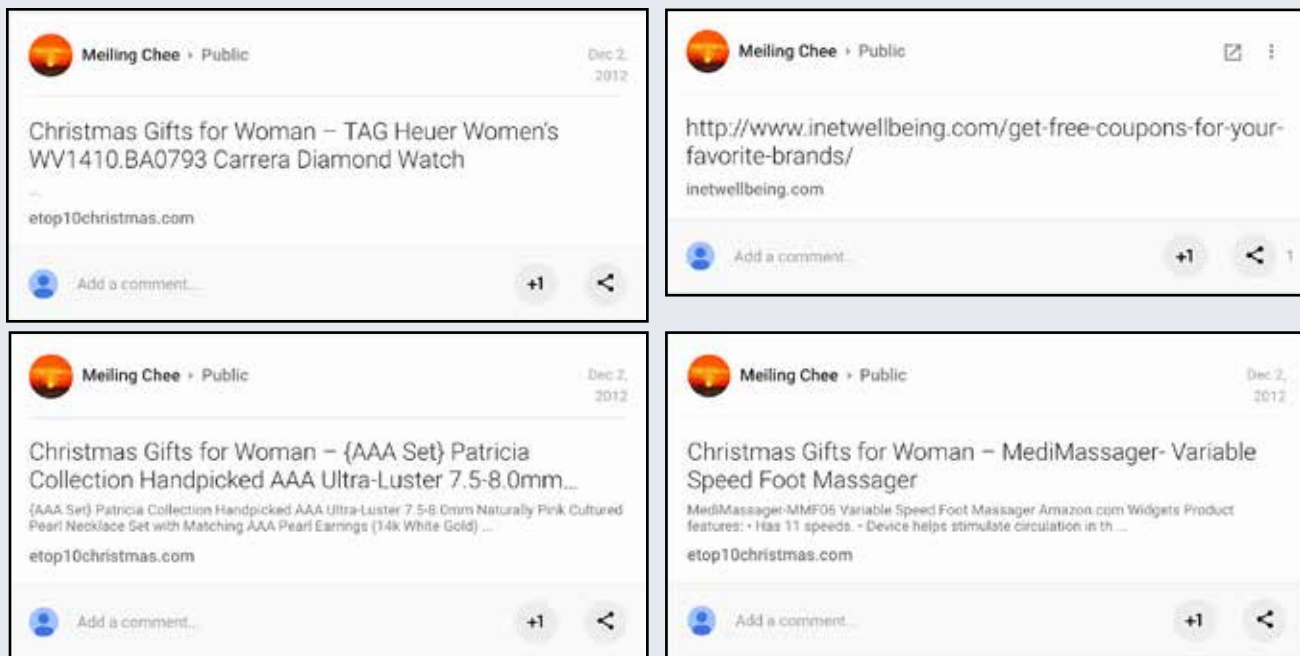


Figure 26: A series of posts promoting Christmas gifts.

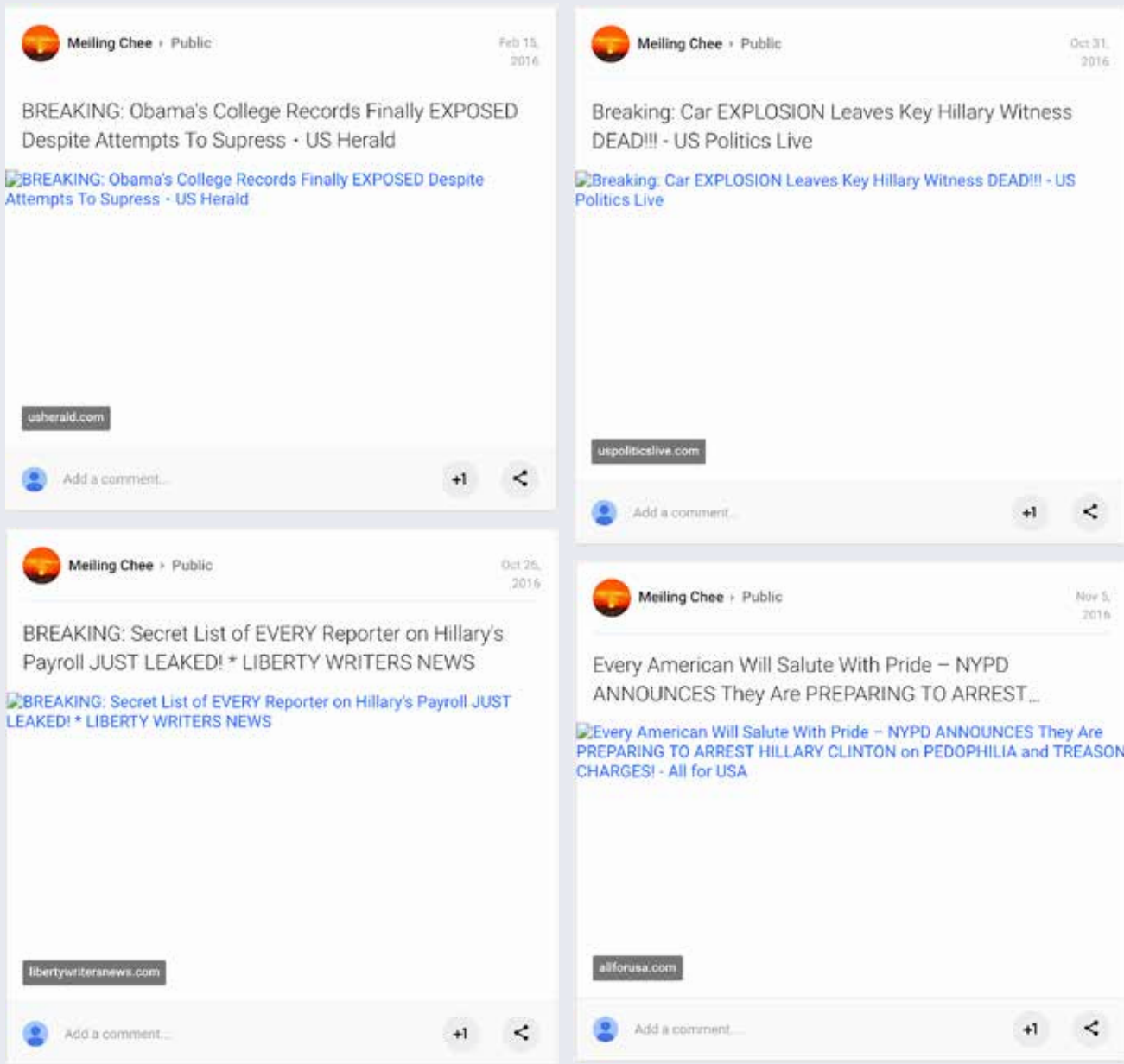


Figure 27: A series of political posts.

Jesse Allen registered All for One as a business with the Marion County Recorder's office on January 28, 2005. Allen would have been 70 years old at the time he registered the business. To date, researchers have not found any activity other than the domain registration related to this business.

ALL FOR ONE, A BUSINESS
ASSOCIATED WITH
ALLFORUSA.COM



Figure 28: DBA registration found on Marion County Recorder's website.

GroupSense researchers requested a small business credit check on All for One. The report indicated that the business registered with the credit reporting agency in February 2005. The credit report showed no indication of bankruptcies, liens, judgements or collections in the 13 years the business has been registered. The report further stated that there was no credit score or financial stability risk rating established due to a lack of available information on the business.

CONCLUSION

The pervasive problem of hijacked accounts and automated account takeover is concerning. These stolen accounts and identities have become a commoditized asset that can be bought and sold on illicit markets. They are being leveraged to promote products, create false brand credibility, weigh in on social issues, and disrupt the political landscape. Fueled by poor password practices and coupled with public breach fatigue, this problem is only going to worsen. This report details a single botnet; there are undoubtedly many more. It is unfortunate that most of the remediation for these issues lies on the general public. Educating the public and politicians on the nature of subversive bot activity and nation-state influence is a tough road. Influence on this scale with credible user data is relatively new and daunting to mitigate. There is much work to do, starting with education, enabling multifactor authentication wherever possible, and effectively leveraging breach notification services.

The research contained in this report documents findings up to July 31, 2018. GroupSense researchers continue to investigate and update the public. Current information can be located at [GroupSense.io/sharks/](https://groupsense.io/sharks/).

RESEARCHERS: If you are interested in contributing to this effort, contact us at sharks@groupsense.io.

APPENDIX

The Appendix contains a number of comments (also referred to as filings) left by suspect accounts on the FCC's website during the open comment period ahead of announced changes to Net Neutrality regulations.

Some comments were repeated by multiple users, while others were not. All comments included in this section can be traced to suspect accounts like those referred to elsewhere in this report.

COMMENTS POSTED MULTIPLE TIMES BY MULTIPLE USERS

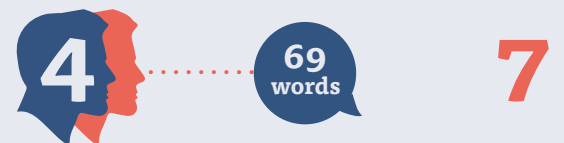
368-word comment used 49 times by nine users

"The FCC's Open Internet Rules (Net Neutrality rules) are extremely important to me. I urge you to protect them. I don't want ISPs to have the power to block websites, slow them down, give some sites an advantage over others, or split the Internet into \"fast lanes\" for companies that pay and \"slow lanes\" for the rest. Now is not the time to let giant ISPs censor what we see and do online. Censorship by ISPs is a serious problem. Comcast has throttled Netflix, AT&T blocked FaceTime, Time Warner Cable throttle the popular game League of Legends, and Verizon admitted it will introduce fast lanes for sites that pay-and slow lanes for everyone else-if the FCC lifts the rules. This hurts consumers and businesses large and small. Courts have made clear that if the FCC ends Title II classification, the FCC must let ISPs offer \"fast lanes\" to websites for a fee. Chairman Pai has made clear that he intends to do exactly this. But if some companies can pay our ISPs to have their content load faster, startups and small businesses that can't pay those fees won't be able to compete. You will kill the open marketplace that has enabled millions of small businesses and created the 5 most valuable companies in America-just to further enrich a few much less valuable cable giants famous for sky-high prices and abysmal customer service. Internet providers will be able to impose a private tax on every sector of the American economy. Moreover, under Chairman Pai's plan, ISPs will be able to make it more difficult to access political speech that they don't like. They'll be able to charge fees for website delivery that would make it harder for blogs, nonprofits, artists, and others who can't pay up to have their voices heard. I'm sending this to the FCC's open proceeding, but I worry that Chairman Pai, a former Verizon lawyer, has made his plans and will ignore me and millions of other Americans. So I'm also sending this to my members of Congress. Please publicly support the FCC's existing net neutrality rules based on Title II, and denounce Chairman Pai's plans. Do whatever you can to dissuade him. Thank You!"



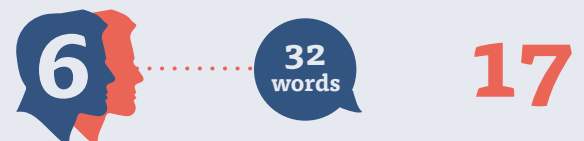
69-word comment used seven times by four users

"The FCC's Open Internet Rules (Net Neutrality rules) are extremely important to me. I urge you to protect them. I don't want ISPs to have the power to block websites, slow them down, give some sites an advantage over others, or split the Internet into \"fast lanes\" for companies that pay and \"slow lanes\" for the rest. I don't support Chairman Pai's proposal to repeal Net Neutrality. Thank you."



32-word comment used 17 times by six users

"Don't kill net neutrality. We deserve a free and open Internet with strong Title II rules. This will ensure that the flow of data is determined by the interests of Internet users."



146-word comment used 20 times by two users

"Our country has benefitted from the internet in many ways, and Americans have come to depend on an open internet and the crucial open internet principles of transparency, no blocking, no censorship and no discriminatory throttling. But, internet rules should not change each time a new political party takes office or a new person is appointed to lead the



Federal Communications Commission. That's why I am writing to ask that you work together to preserve these crucial internet principles by creating legislation that codifies them into law. The FCC's action to overturn the current law designed 80 years ago, before the Internet was created, is a great first step. However, legislation is the only way to permanently preserve the open internet principles that we rely on. Thank you for working to keep the internet a place where all citizens can find new opportunities and communication freely."

94-word comment used three times by three users

"Net neutrality guarantees a free and open internet. Without it, internet service providers could block or censor websites, or create \u00d2fast\u00d3 and \u00d2slow\u00d3 lanes. ISPs can't be allowed to abuse their position, potentially hurting businesses and consumers across the country, and privileging their own content over competitors. Revoking net neutrality by changing the Title II classification of internet access would be bad for people, bad for competition and entrepreneurship, and it's bad for the internet. I fully support keeping the current Title II classification of internet access and keeping the internet free and open."



4

76-word comment used four times by four users

"The FCC's job is to stand up for consumers, not big cable companies. To do that, the FCC must keep in place the current rules that protect net neutrality and the free and open internet. Without the current rules, cable companies can tell internet users like me what I can or cannot access on the internet. Cable companies cannot be trusted to protect the free and open internet -keep the current open internet rules in place!"



4

70-word comment used three times by three users

"A free and open internet is critical for Americans to connect with their friends and family, exercise their freedom of speech, and create innovative new businesses. In 2015, the FCC established strong net neutrality rules to protect the free and open internet Americans depend on. Please reject any plan from Trump or his FCC Chair to roll back net neutrality rule sand open the door to a corporate controlled internet."



3

141-word comment used 10 times

"I am writing today to encourage you to work together and move quickly on permanent legislative fix to preserve and open internet that is transparent and free from blocking, censorship and discriminatory throttling. I believe only legislation can ensure we have permanent, enforceable open internet rules that apply equally to everyone and won't change depending on which party is in power or who is running the FCC. The FCC's move to make sure the internet isn't subject to heavy-handed laws created for the rotary phone is the right first step, but only legislation can put this issue beyond politics and ensure that vital consumer protections are stable and secure. After almost two decades of the FCC and the courts arguing this issue it's time for Congress to provide permanent and strong open internet protections to consumers and the entire internet community."



10

**COMMENTS POSTED
MULTIPLE TIMES BY
SINGLE USERS**

93-word comment used 10 times

"I am writing today to urge you to work with your fellow members of Congress and the FCC to permanently preserve an open internet by supporting bipartisan legislation that would turn the principles of transparency, no blocking, no censorship and no discriminatory throttling into law once and for all. It's vital that our country, and our citizens, have strong and permanent rules to ensure that internet regulation cannot change course depending on which political party is in the White House. Passing bipartisan legislation is a step toward protecting it for years to come."

93
words

10

105-word comment used 10 times

"I urge you to keep the internet open and free for all to use. Net Neutrality describes the current rules in place to ensure that Internet Service Providers (ISPs) treat all content equally and do not block, slow or otherwise discriminate against user access to web content. Eliminating Net Neutrality incentivizes ISPs to create Internet \"fast lanes\" that will go to the highest bidder. This will discourage competition by tilting the playing field in favor of large enterprises that have the resources to outspend smaller competitors. Which means... Internet-enabled small businesses would be among those hit hardest by new fees and tiered services. Thank you."

105
words

10

102-word comment used 10 times

"I am writing to encourage you to work together in support of an open internet, one that is transparent and free from blocking, censorship and discriminatory throttling. After nearly 20 years of FCC commissioners and court rulings wrangling over how the internet is regulated, it is time for Congress to provide clear direction by passing legislation that provides certainty for consumers and internet companies alike. Bipartisan legislation can help end the years-long political back-and-forth around an open internet that creates little more than confusion. Internet users and internet providers deserve clear and permanent rules that ensure the internet remains open and thriving."

102
words

10

110-word comment used 10 times

"I am writing today in support of preserving an open internet that is transparent and free from blocking, censorship and discriminatory throttling and to encourage you and other members of Congress to work together to pass open internet legislation. Congress has the power to end the political back and forth and create lasting open internet protections that apply to everyone and will remain in place regardless of which party is in power. I agree with the current FCC that heavy-handed regulations will do more harm than good. But, we need legislation to put this issue to rest once and for all and ensure an open internet for decades to come."

110
words

10

193-word comment used three times

"The FCC should safeguard Internet freedom by keeping the bright-line net neutrality protections in place and upholding Title II. The FCC should reject Chairman Pai's plan to give the telecom giants like Comcast, AT&T, and Verizon free rein to engage in data discrimination, stripping consumers of the necessary access and privacy protections we fought for and won just two years ago. I'm worried about creating a tiered Internet with \"fast lanes\" for certain sites or services because Users will have fewer options

193
words

3

and a less diverse Internet. Thankfully, the current net neutrality rules ensure that ISPs can't block or slow customers' access to certain websites or create Internet \"fast lanes\" by charging websites and online service money to reach consumers faster. That's exactly the right balance to ensure the Internet remains a level playing field that benefits consumers and small businesses as well as larger players. Pai's proposal would help turn ISPs into gatekeepers with an effective veto right on innovation and expression. That's not how the Internet was build, and that not what we want. Thank you for keeping Title II net neutrality rules in place to protect Internet users like me."

192-word comment used seven times

"The FCC needs to stand up for Internet users like me and keep the net neutrality rules that are already in effect. The FCC should throw out Chairman Ajit Pai's proposal to hand the government-subsidized ISP monopolies like Verizon, Comcast, and AT&T the legal cover to create Internet fast lanes, stripping Internet users of the vital privacy and access safeguards we worked for and so recently won. I'm afraid of a pay-to-play Internet where ISPs can charge more for certain websites because 3. Thankfully, the existing Open Internet rules mean that ISP monopolies can't slow or block consumers' ability to see certain web services or engage in data discrimination by charging online services and websites more money to reach people faster. That's the right kind of forward-looking approach to make sure competition in the Internet space is fair and benefits small businesses and Internet users as well as entrenched Internet providers into Internet gatekeepers with the ability to veto new expression and innovation. That's contrary to the basic precepts on which the Internet was built. I appreciate you maintaining Title II net neutrality rules and the rights of Internet users like me."

192
words

7

Six-word comment used 10 times

"Preserve Net Neutrality and Title II."

6
words

10

77-word comment used once

"The FCC needs to stand up for Internet users like me and keep the net neutrality rules that are already in effect. I'm concerned about ISPs being allowed to discriminate against certain types of data or websites because ISPs could have too much power to determine what I can do online. That's not the kind of Internet we want to pass on to future generations of technology users. Please keep the current open internet rules in place."

77
words

1

40-word comment used once

"I'm worried that the protections that are in place will be weakened if we change the way they're enforced. I would support a new regulation style if it guarantees the same or better protections, but NOT if we lose any."

40
words

1

20-word comment used once

"Strong net neutrality rules make America great – keep these regulations in place and lets keep equality as an American value!"

20
words

1

ABOUT GROUPOSENSE

GroupSense is a leading provider of cyber intelligence services. GroupSense's unique cyber reconnaissance approach is trusted by the largest companies in the healthcare, manufacturing, and financial sectors. In addition, GroupSense is trusted by governments to assist in cyber intel program development, election monitoring, and anti-fraud and risk measures worldwide. Contact GroupSense to learn how you can leverage tailored cyber reconnaissance for your organization.

GroupSense
4040 North Fairfax Drive, Arlington, VA 22203
+1-877-469-7226
sharks@grouposense.io
www.grouposense.io