

# Domain Squatting Attack: Antifa.com Pointing to JoeBiden.com

Peter Foytik

# Fascism Definition

Merriam Webster:

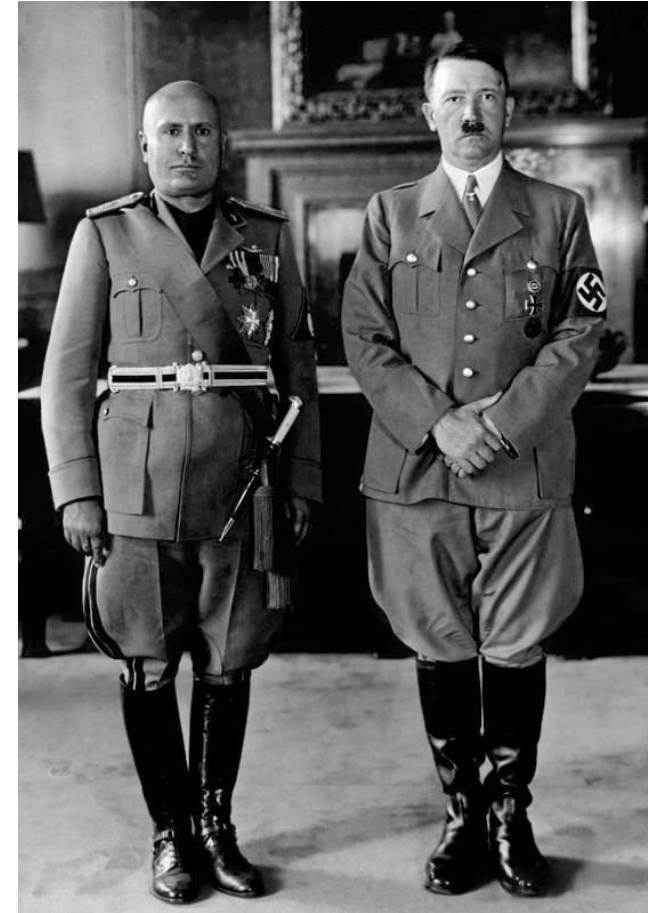
- A political Philosophy, movement or regime that,
- exalts nation and often race above individual and,
- stands for a centralized autocratic government headed by a dictatorial leader,
- severe economic and social regimentation,
- and forcible suppression of opposition

<https://www.merriam-webster.com/dictionary/fascism>

Most notable examples are pictured:

- Fascist Italy lead by Benito Mussolini
- Nazi Germany lead by Adolf Hitler

<https://en.wikipedia.org/wiki/Fascism>



By Unidentified photographer -  
[http://img.audiovis.nac.gov.pl/PIC/PIC\\_2-12512.jpg](http://img.audiovis.nac.gov.pl/PIC/PIC_2-12512.jpg), Public Domain,  
<https://commons.wikimedia.org/w/index.php?curid=41283482>

# Antifascist Movement (Antifa)

Ideological movement against fascist government, capitalism



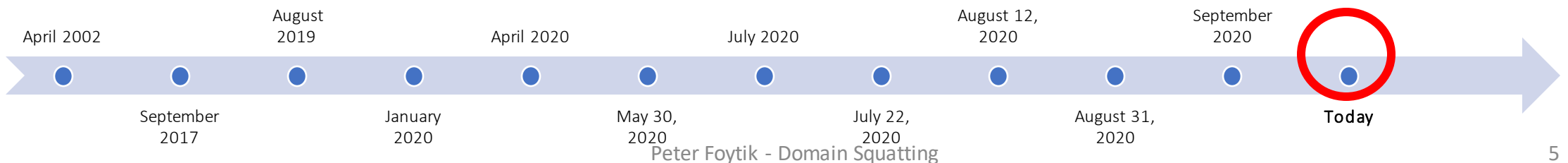
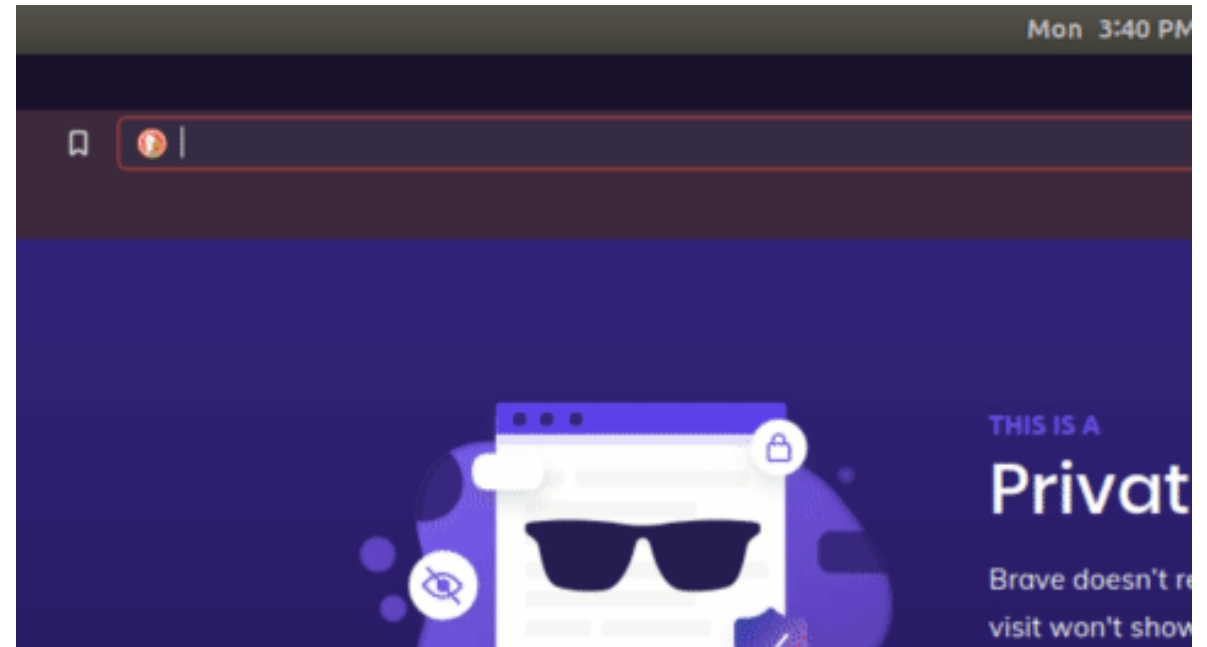
# Political parties and their perspective to Antifa

- Leaders in the major political parties have denounced the group
- 2017, Nancy Pelosi as house minority leader for Democratic party
  - <https://web.archive.org/web/20170829224007/http://www.democraticleader.gov/newsroom/82917/>
- Various Republican senators have attempted to classify Antifa as a terrorist organization
  - <https://web.archive.org/web/20201109182524/https://www.washingtonpost.com/politics/2019/07/20/senators-want-antifa-activists-be-labeled-domestic-terrorists-heres-what-that-means/>
- 2020 Democratic party presidential elect Joe Biden also condemned Antifa violent actions:
  - [https://web.archive.org/web/20200912100728if\\_/https://www.washingtonpost.com/outlook/five-myths/five-myths-about-antifa/2020/09/11/527071ac-f37b-11ea-bc45-e5d48ab44b9f\\_story.html](https://web.archive.org/web/20200912100728if_/https://www.washingtonpost.com/outlook/five-myths/five-myths-about-antifa/2020/09/11/527071ac-f37b-11ea-bc45-e5d48ab44b9f_story.html)

# Antifa.com domain and Biden campaign website

- Today if you go to antifa.com
  - Domain redirects the user To joebiden.com

```
(base) pfoytik@Latitude-5490:~/Documents/s  
HTTP/1.1 302 Found  
Server: nginx  
Date: Tue, 10 Nov 2020 21:58:42 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 44  
Connection: keep-alive  
Location: https://joebiden.com/  
X-Served-By: Namecheap URL Forward  
  
<a href='https://joebiden.com/'>Found</a>.
```



# Public reactions to Antifa and Biden



Chanel Rion reporter with far-right network One America News asked Trump about Antifa pointing to Biden

<https://www.dailymail.co.uk/news/article-8181867/Fake-conman-dad-questionable-resume-Truth-Chanel-Rion-Trumps-favorite-reporter.html>



Charlie Kirk  
@charliekirk11

Go to [ANTIFA.com](https://antifa.com) and you will see who is truly supportive of the domestic terrorism campaign slaughtering black people and destroying America.

8:50 PM · Aug 31, 2020 · Twitter Web App

3.2K Retweets 155 Quote Tweets 7.2K Likes



URI-R:

<https://twitter.com/charliekirk11/status/1300596885774712832>



Steve Milloy  
@JunkScience

[Antifa.com](https://antifa.com) takes you to [JoeBiden.com](https://joe Biden.com)... although it really should be the other way around.



Joe Biden for President: Official Campaign Website  
We are the United States of America. There is not a single thing we cannot do. Are you with us? Join our campaign to elect Joe Biden today!  
[joebiden.com](https://joebiden.com)

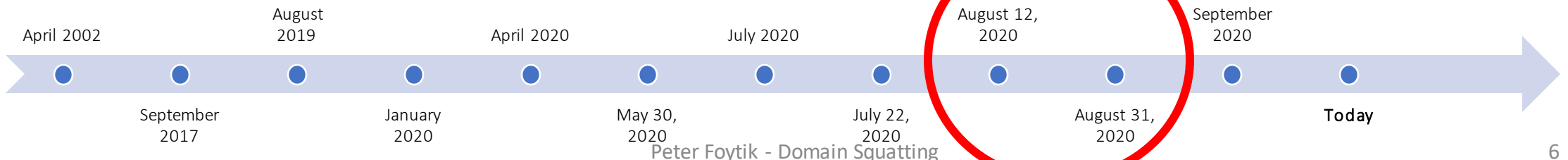
3:52 PM · Aug 12, 2020 · Twitter Web App

8 Retweets 2 Quote Tweets 23 Likes



URI-R:

<https://twitter.com/JunkScience/status/1293636430800064514>

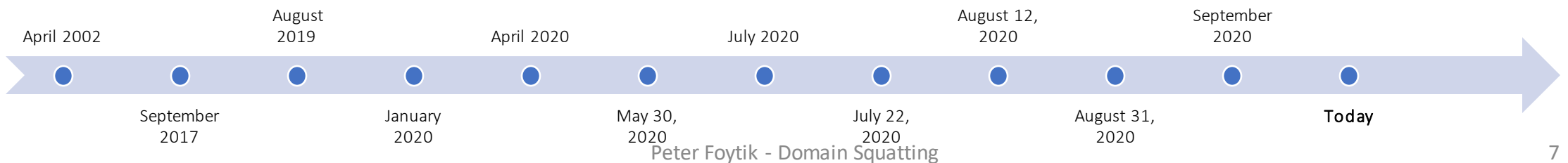


# Google Trends for antifa.com from July 1 to October 15, 2020

Interest over time ?



<https://trends.google.com/trends/explore?date=2020-07-01%202020-10-15&geo=US&q=antifa.com>





# Cyber/Domain squatting definition and examples it all comes down to intent

GoDaddy

websitenew.com

Premium Domain

websitenew.com is available

**\$2,095.00**  
+\$17.99/yr<sup>?</sup>

Why it's great.

- ✓ "New" is a widely used keyword.
- ✓ "Websitenew.com" is easy to remember.
- ✓ Includes Basic Privacy Protection.

What are premium domains?

Buy It Now

Domains include Basic Privacy Protection. <sup>?</sup>

Available Alternate Domains

.net \$14.99	.co \$11.99	.org \$9.99	.info \$2.99	.o
--------------	-------------	-------------	--------------	----

Web.archive.org/web/20000815232140/http://juliaroberts.com

Peter Foytik - Domain Squatting

web.archive.org/web/20000815232140/http://juliaroberts.com...

Apps Bookmarks music

http://juliaroberts.com/

16 captures

20 Jun 2000 - 20 Nov 2000

web.archive.org says

Julia Roberts has no association with or editorial-control or influence- over this site; nor do any of her associates.

OK

I begin this site with an expression of t  
Julia Roberts and Lyle Lovett. On late  
Jekyll and Hyde dichotomy resulting from my adoration for Julia and  
my simultaneous rebellion at her rather unfriendly attempts to take  
this site away from me, demonstrating a disregard for the basic  
freedoms of speech and property ownership ostensibly bestowed upon  
every American.

In the beginning, like many of you, I was a servile purring kitten, a  
gamboling puppy dog wafted along by Julia's charisma. Now I have  
become drunk on the increasingly distant and muffled voices of those  
brave men who are spinning in their Arlington graves; those bloodied  
and torn sons who died for the basic freedoms that have made  
America a country like no other in the world.

Everyone who enters here should k  
this battle, not me, but it is not just  
attacks everyone whose voice would  
avalanche of fame and corporate po

So whatever you see here, remembe  
this with a phone call, for I am not

However, I begin the battle with a c  
portrait and poem of two humans l  
just like you and me, whose image a  
and heard, will forever endear and  
your hearts.

Continue by pressing here---->> **Click at your Own Risk**

Dear Lyle: This is a provocative, haunting, and heart-breaking poem. This poem, and this picture, tell a very long  
complex story. They make me see and feel the inexpressible and divine value in your humanity...in yours Lyle...a  
yours Julia. If you think that because of this silly site that I don't respect and admire you both, you are mistaken.  
Forgive my smallness...if you can, for I am a sad and tiny man who has lost sight of the lighted paths.

Fiona  
(Lyle Lovett)

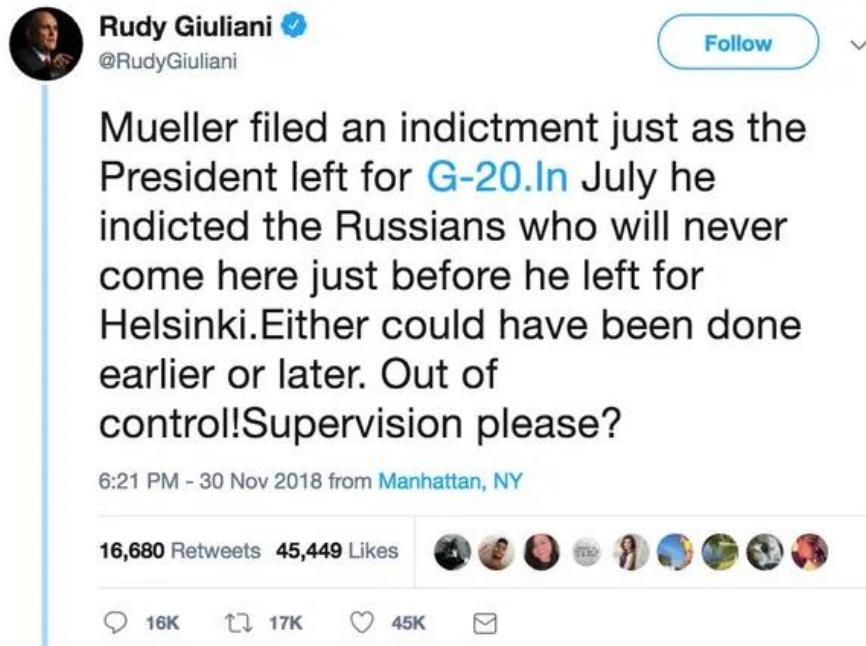
Way down yonder on the bayou  
There lives a little girl-o

8

For Better or for



# Political domain attacks from typos and/or false flag attacks



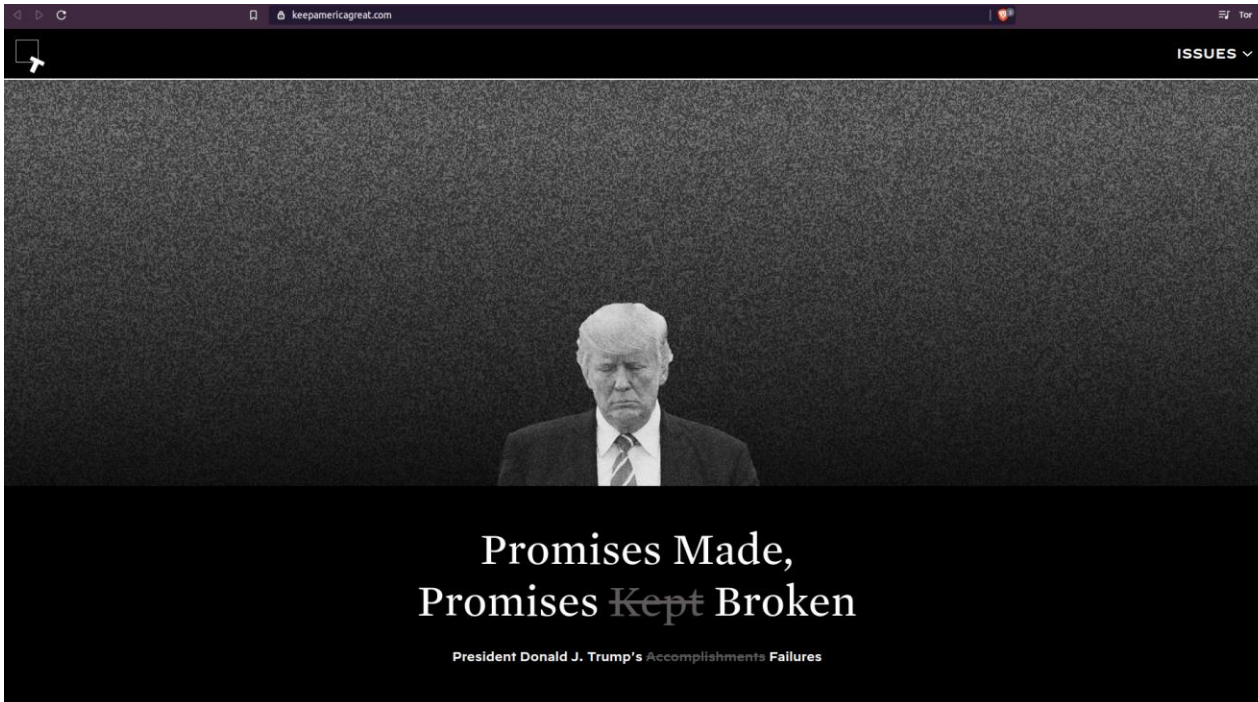
G-20.In website



<https://www.theguardian.com/us-news/2018/dec/05/rudy-giuliani-helps-create-anti-trump-protest-website-with-twitter-typo>

# Additional examples of domain attacks/squatting

Keepamericagreat.com



URI-M:  
<https://web.archive.org/web/20201108114017/https://keepamericagreat.com/>

Republicannazis.com redirects to tedcruz.com



Loading...

`http://republicannazis.com/ |`  
`20:40:33 November 01, 2020`

Got an HTTP 302 response at crawl time

Redirecting to...

`https://www.tedcruz.org/`

[Impatient?](#)

URI-M:  
<https://web.archive.org/web/20201101204033/http://republicannazis.com/>

# Questions

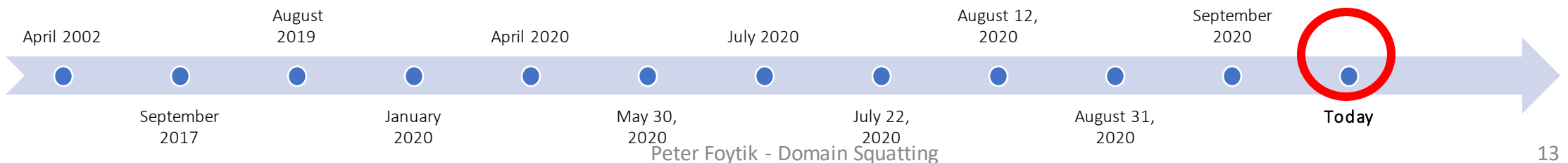
- Is Joe Biden's campaign a victim of potential domain attack/squatting?
- Can we identify a sequence of events to show sources and/or actors of the attack?

# Tools used to understand the context and effect of Antifa.com redirect

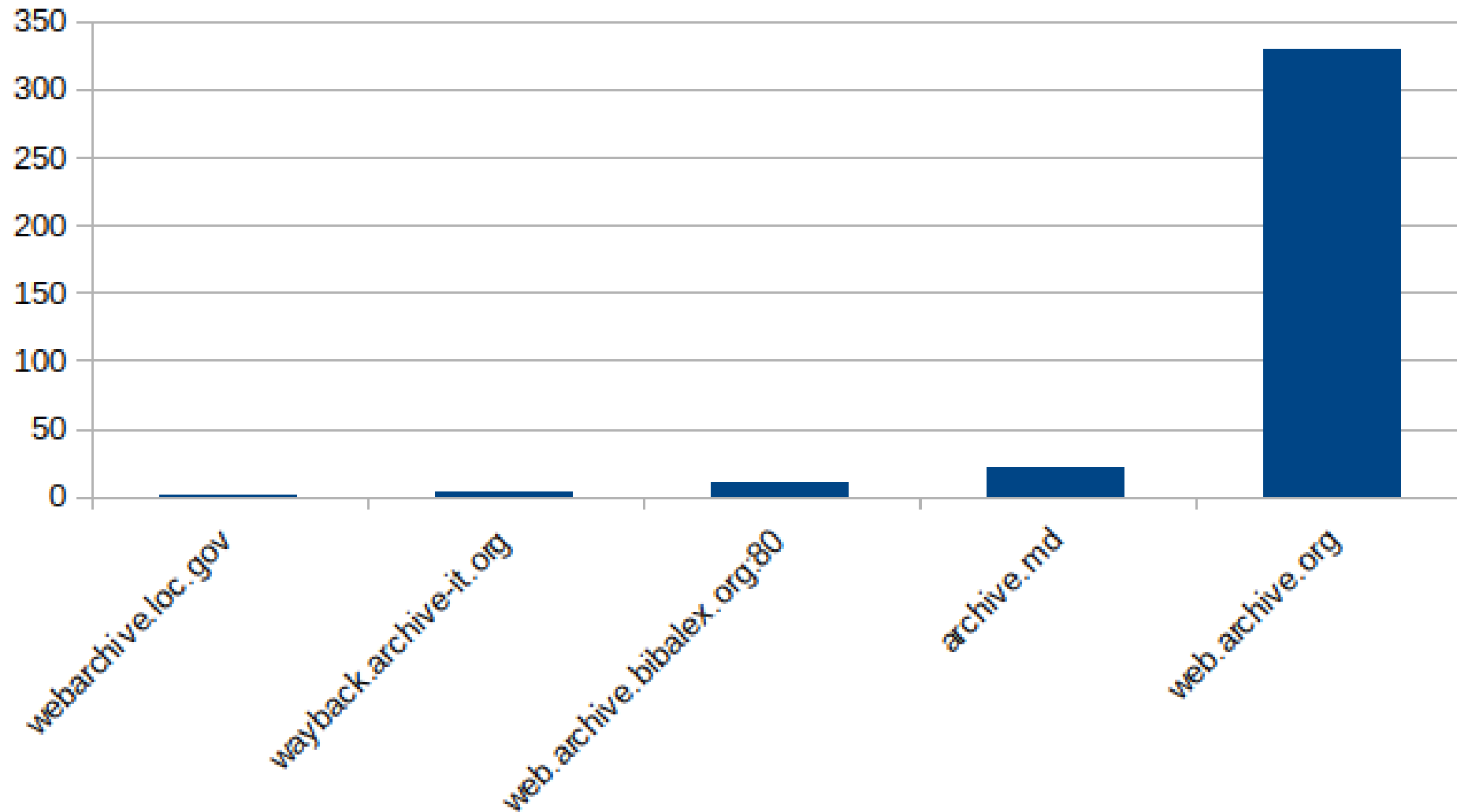
- Memgator
- Web Archives
  - Wayback Machine
  - Archive.is
- Whois/Whoisology
- Twitter
  - Twint
- Google Trends

# Today on the timeline

- Today antifa.com still points to joebiden.com
- No announcement of who is responsible for redirecting domain
- Use Wayback machine observe any prior version of the website antifa.com

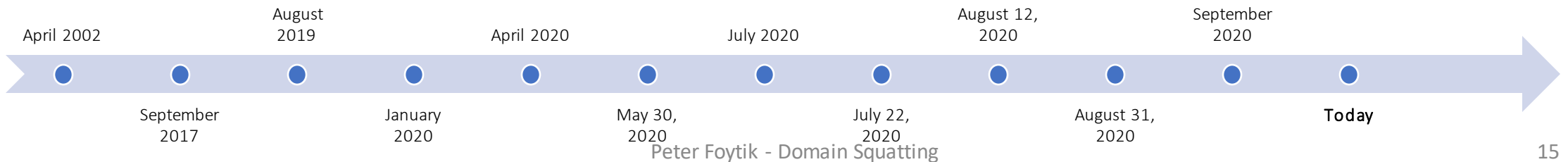
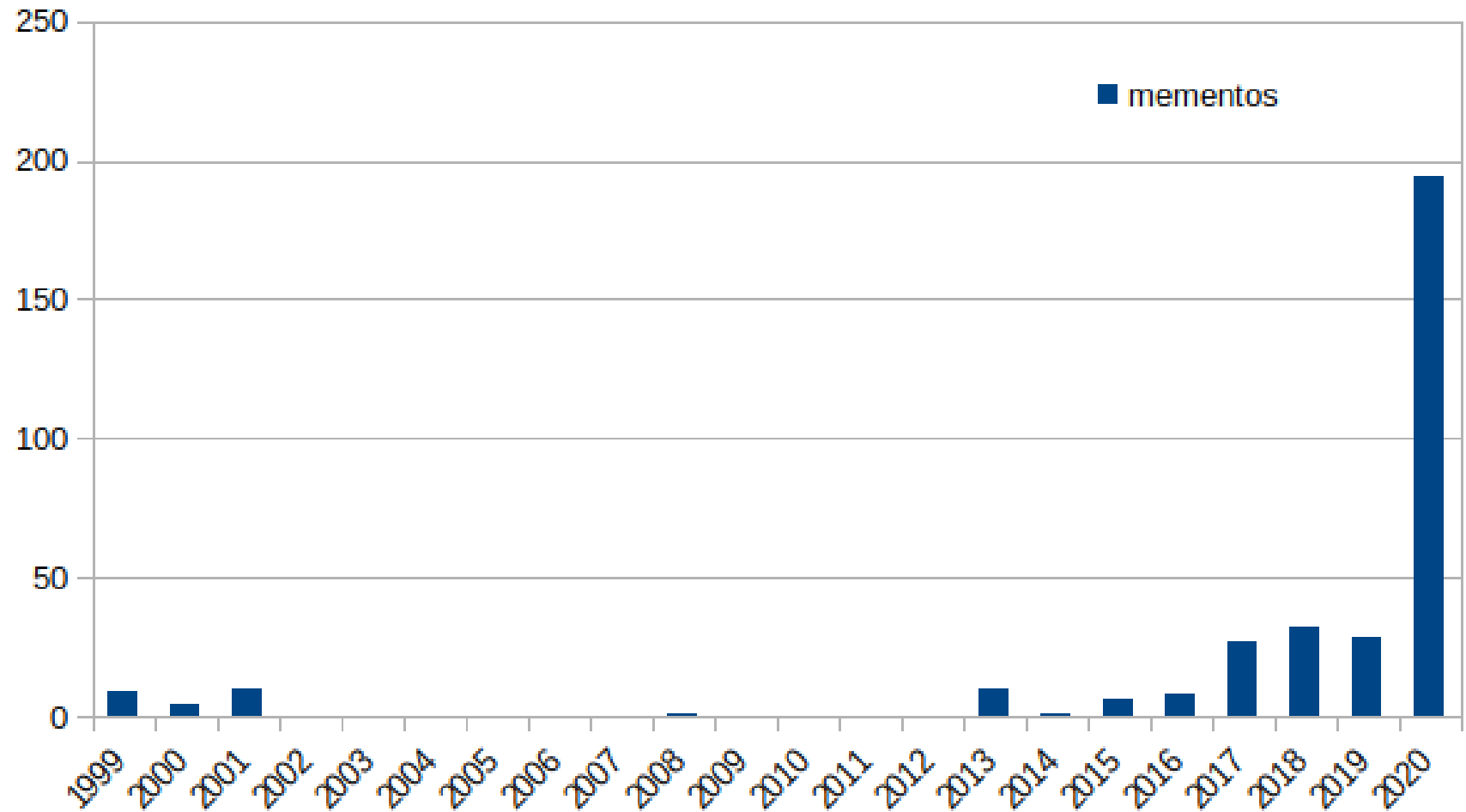


# Mementos by archive from Memgator

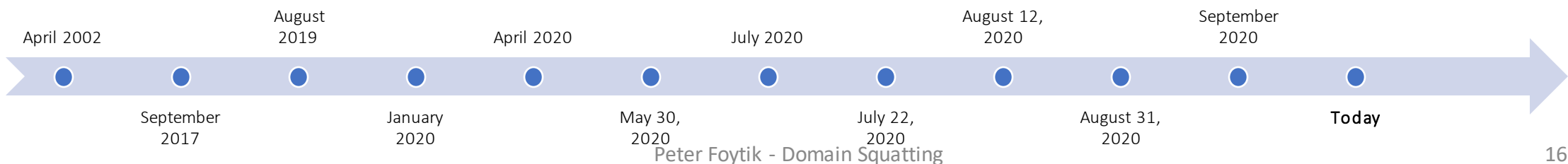
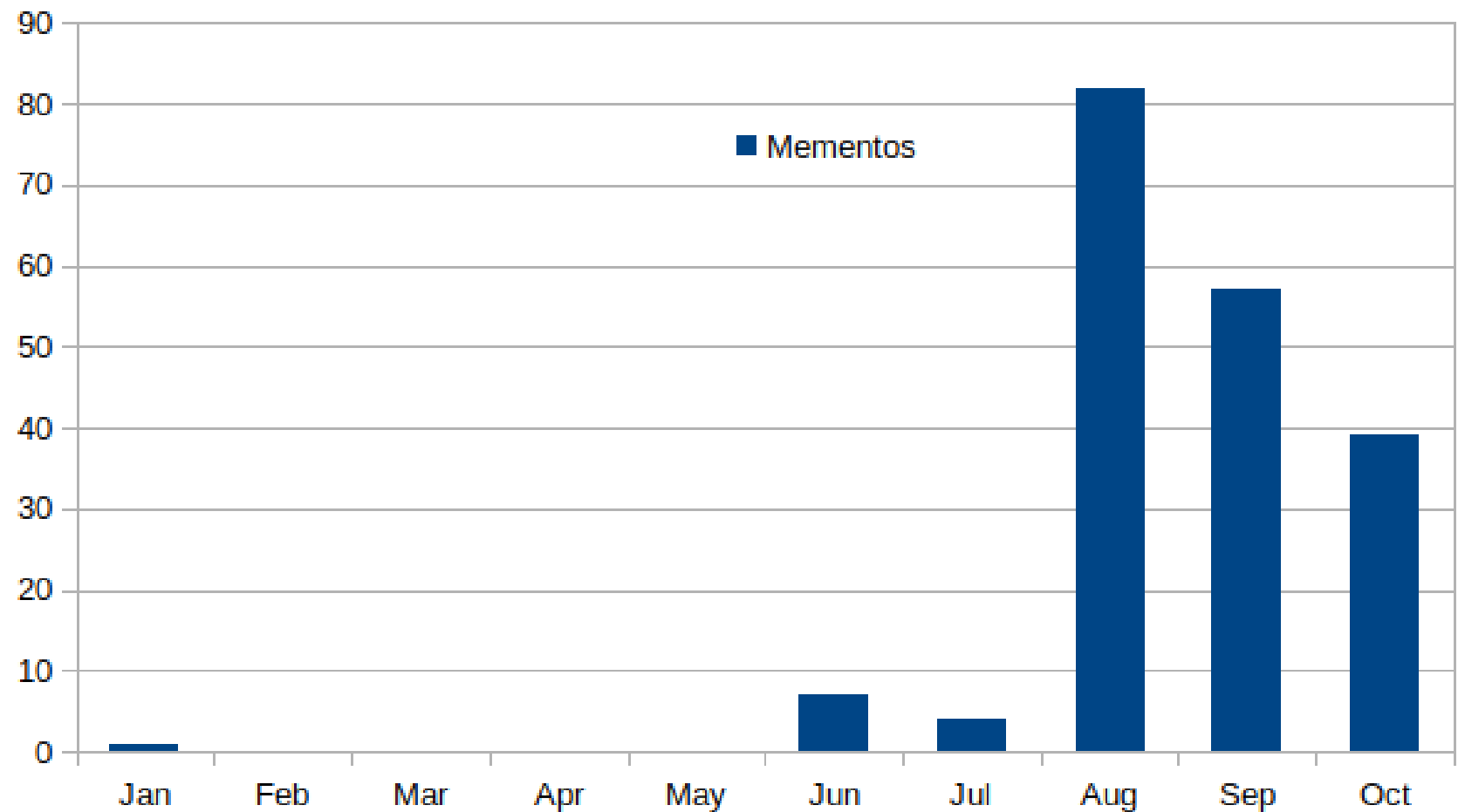




# Timemap information from Memgator for antifa.com



# Mementos for 2020 by month



# Archived history of antifa.com for sale

web.archive.org/web/20190810210142/http://antifa.com/

Apps Bookmarks music food IOT\_Sim sentara VMASC

INTERNET ARCHIVE Wayback Machine <http://antifa.com/> Go JUL AUG 10 OCT 2018 2019 2020 255 captures 20 Jan 1999 - 29 Sep 2020

[antifa.com](http://antifa.com/)  
This domain is for sale

If you are interested

in purchasing domain name, please submit this form.

\* We will contact you back with [two business days](#) with price and terms

\* Price Offer in USD  
Offers under \$500 US are usually not considered

\* First Name  
\* Second Name  
\* E-Mail  
\* Confirm E-Mail  
Phone  
\* UNITED STATES  
Not USA  
Comment

\*Fields are required  
( all except phone )

Verify that you are a human  
CAPTCHA

Get Price

<https://web.archive.org/web/20190810210142/http://antifa.com/>

archive.today Saved from <http://antifa.com/> search 8 Feb 2017 05:33:06 UTC

webpage capture All snapshots from host antifa.com history prior next

Webpage Screenshot share download .zip report bug or abuse donate

Best offer

antifa.com > This domain is for sale  
[Click here to make an offer](#)

antifa.com

Sök annonser

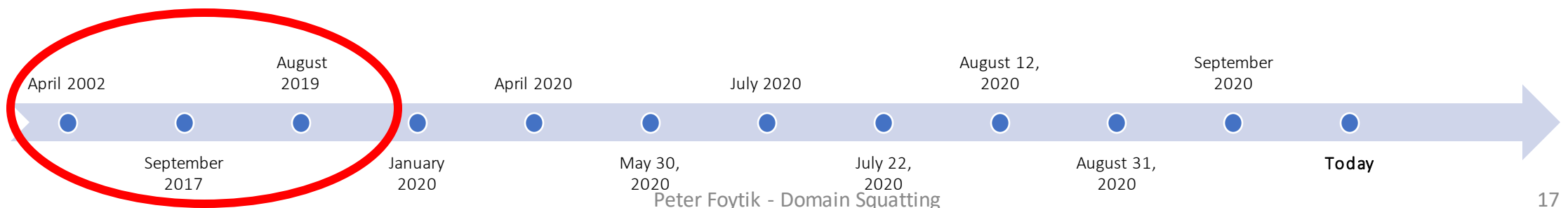
Relaterade länkar

- Forex Game
- Dress M
- Free Apps Free Games
- A Chat Room
- Dating A
- Free M
- Mobile App Software
- Free Chat Software
- Browser App
- Mobile Browser Games

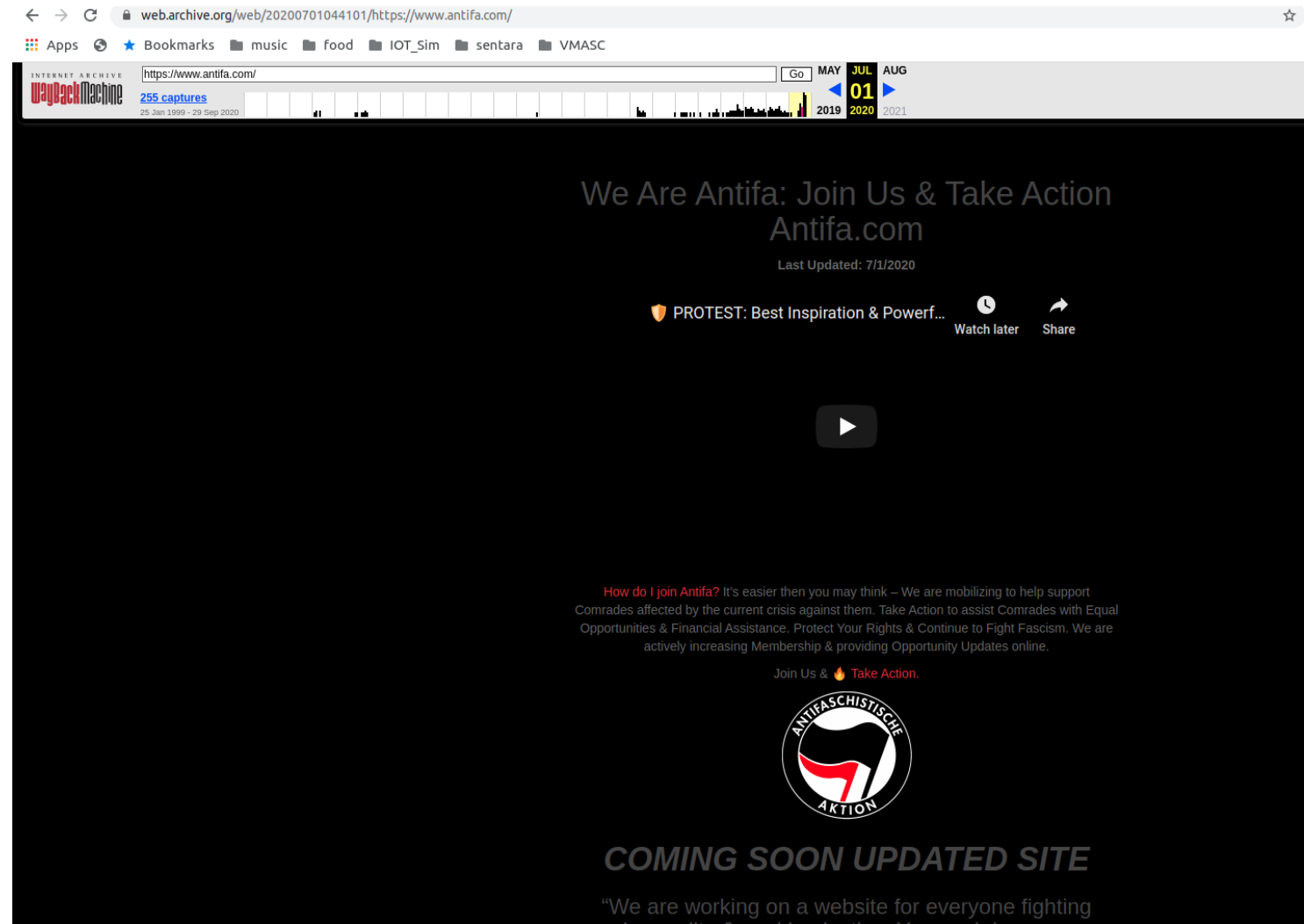
Relaterade länkar

- Antifa
- Antifa T Shirts
- Photo
- Antifa Shop
- Old School T Shirt
- Antifa
- A Game Online Games
- Free Forex Demo
- A Game com
- Games a Go Go
- A Forex
- A Free Phone
- Watch Video Games
- Free Dating Apps
- A Software
- Cool M
- M Chat
- M Games

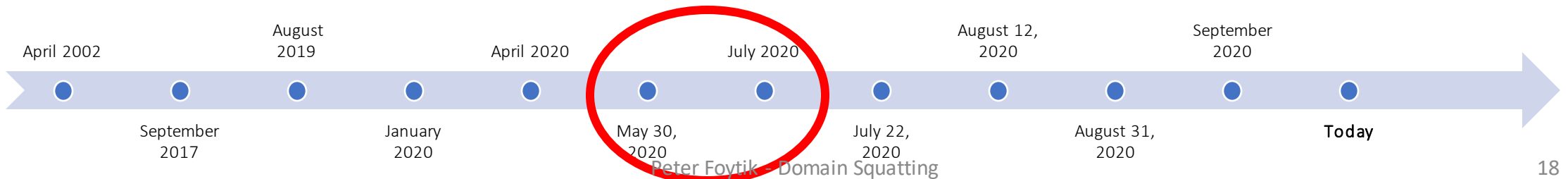
<http://archive.today/2017.02.08-053306/http://antifa.com/>



Archived history  
of antifa.com as  
website earliest  
archived record is  
May 30, 2020

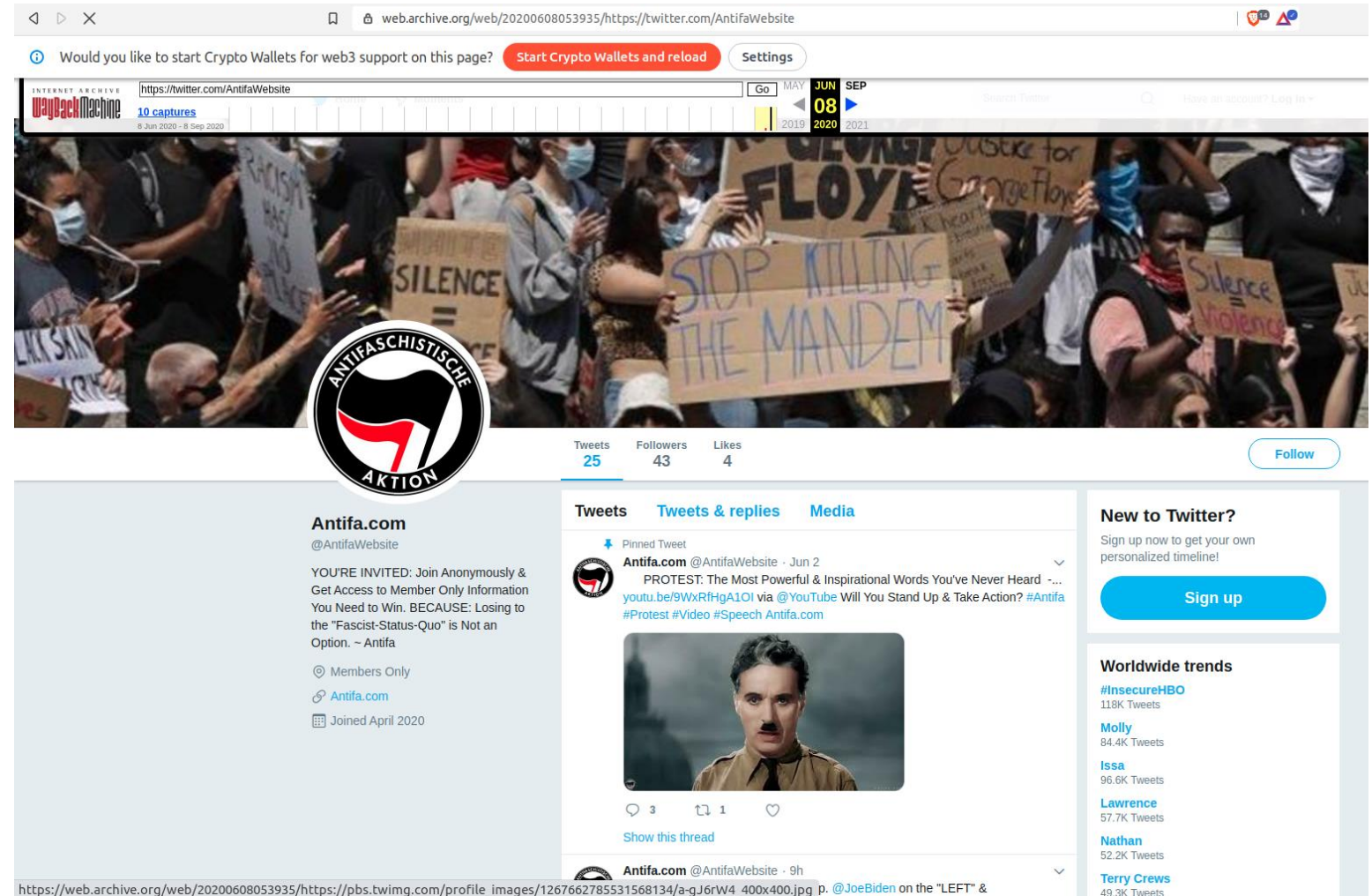


<https://web.archive.org/web/20200701044101/https://www.antifa.com/>

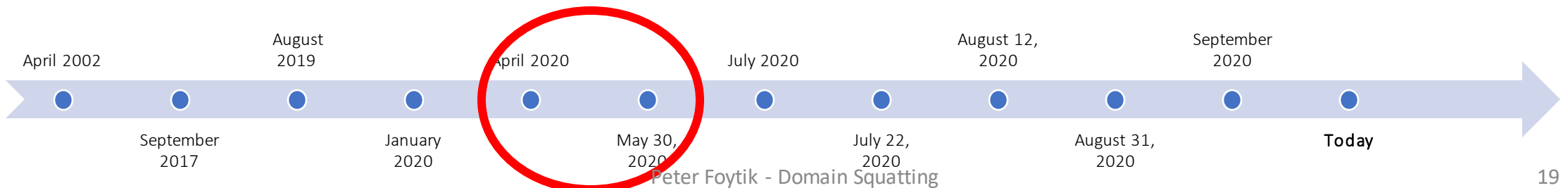


Associated Twitter  
account  
@AntifaWebsite  
Joined April 2020  
(Twitter Removed)

Earliest reply May 31,  
2020



[https://web.archive.org/web/20200608053935/https://pbs.twimg.com/profile\\_images/1267662785531568134/a-gJ6rW4\\_400x400.jpg](https://web.archive.org/web/20200608053935/https://pbs.twimg.com/profile_images/1267662785531568134/a-gJ6rW4_400x400.jpg) p. @JoeBiden on the "LEFT" &  
<http://web.archive.org/web/20200608053935/https://twitter.com/antifawebsite>



# Twitter account terminations for violations of user agreement

[https://en.wikipedia.org/wiki/Twitter\\_suspensions](https://en.wikipedia.org/wiki/Twitter_suspensions)

## Account suspended

Twitter suspends accounts which violate the **Twitter Rules**

Unity 2020 @ArticlesOfUnity



<http://archive.today/2020.08.17-153029/https://twitter.com/articlesofunity>

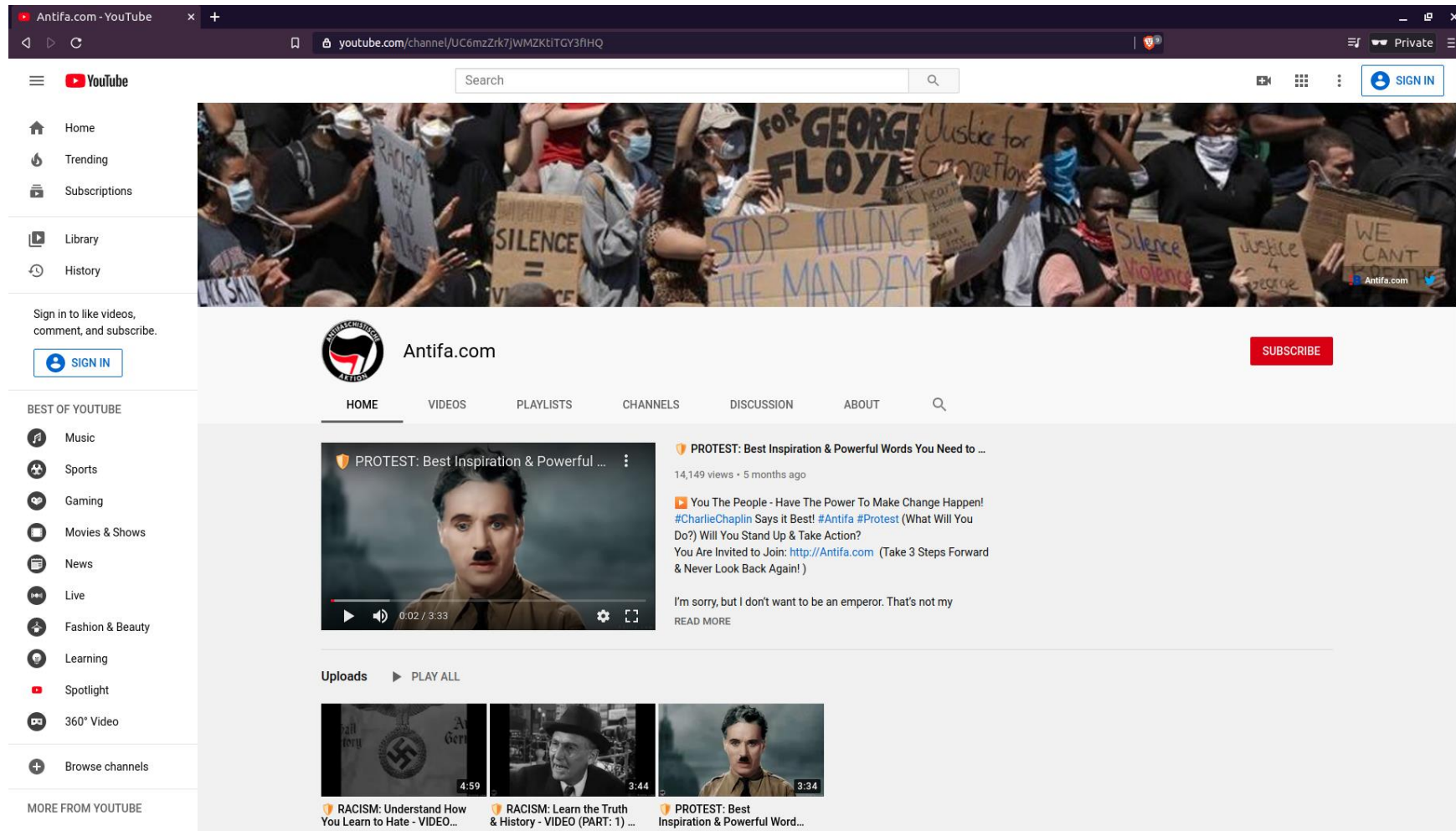
Steve Bannon @WarRoomPandemic



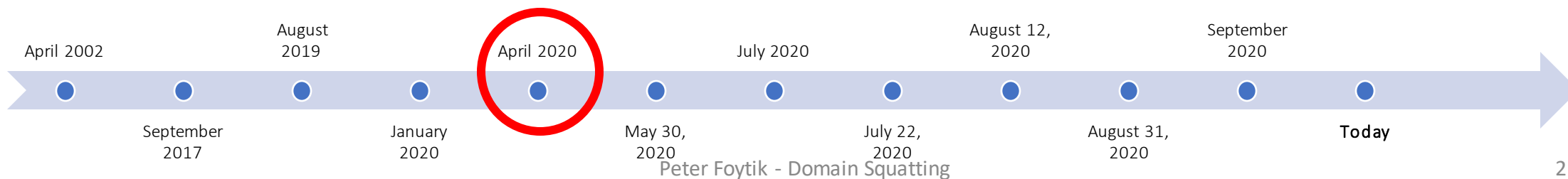
<http://archive.today/2020.10.27-174755/https://twitter.com/warroompandemic>



Associated  
Youtube  
account  
joined April  
17, 2020  
(Still Active)

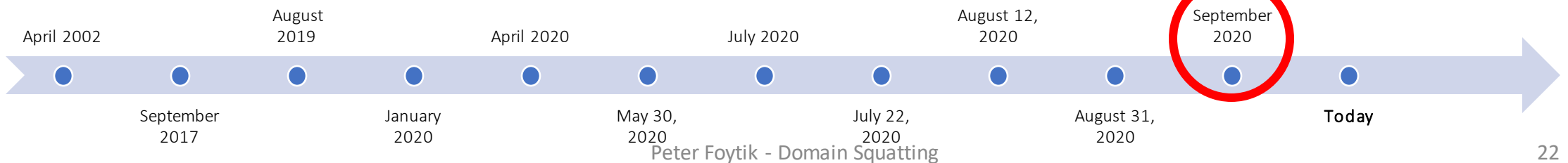
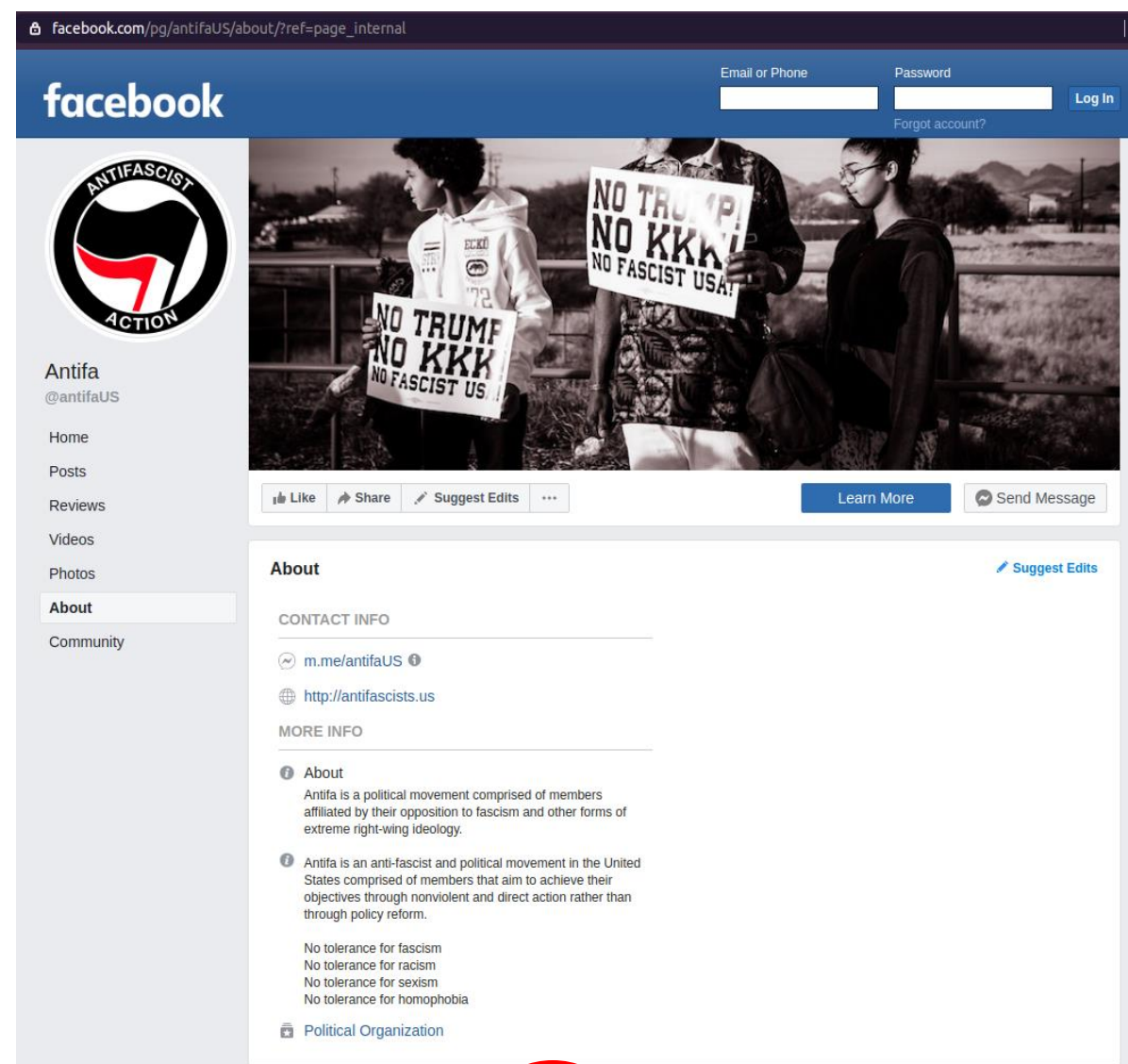


<https://www.youtube.com/channel/UC6mzZrk7jWMZKtiTGY3fIHQ>

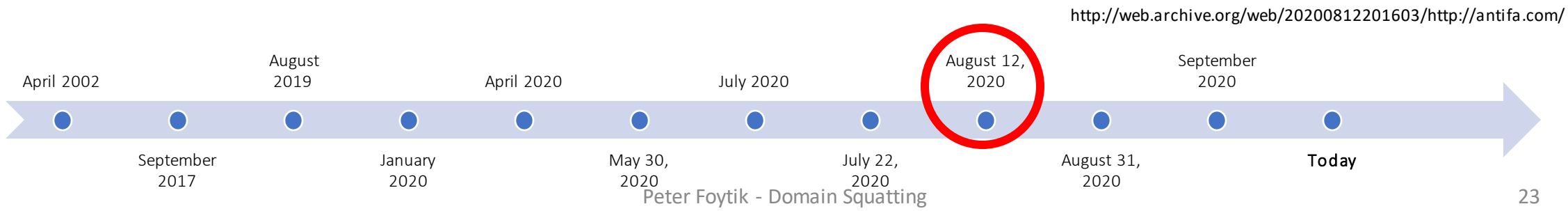
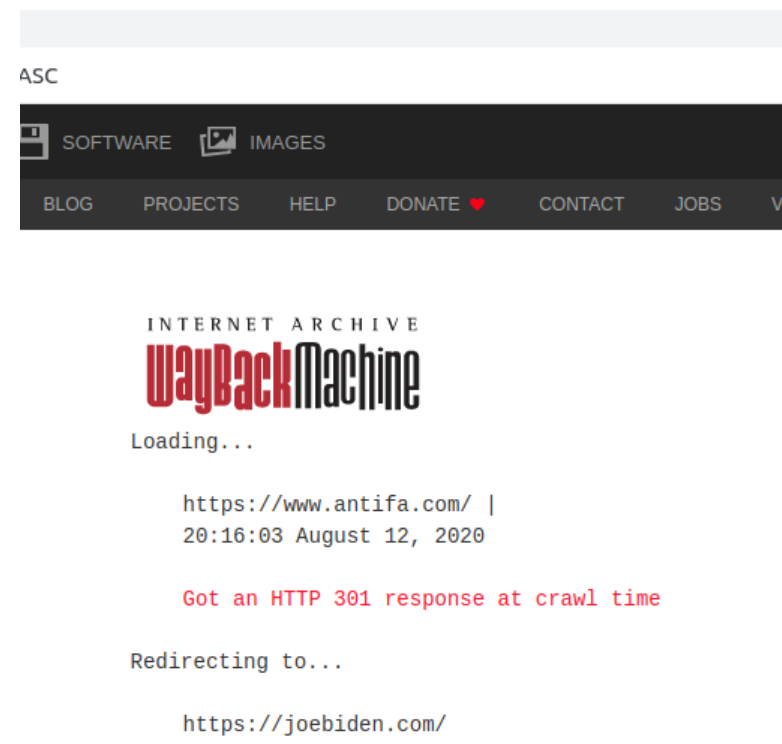
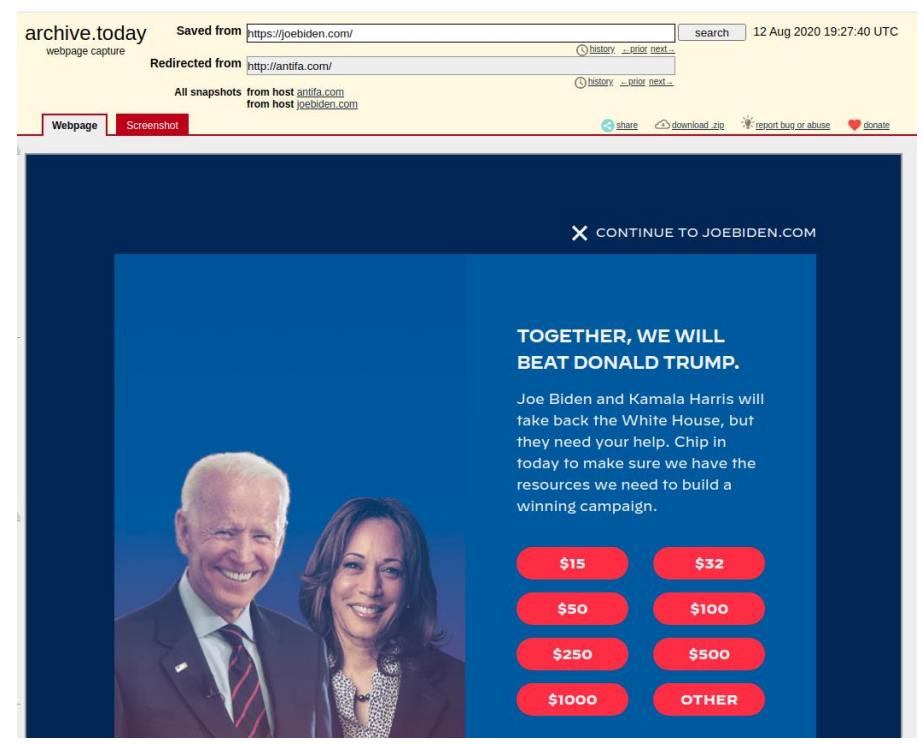


# AntifaUS Facebook page does not appear to be associated with antifa.com

- Started in September 2020
- Points to a different live website
- Antifascist.us
- No records in Wayback

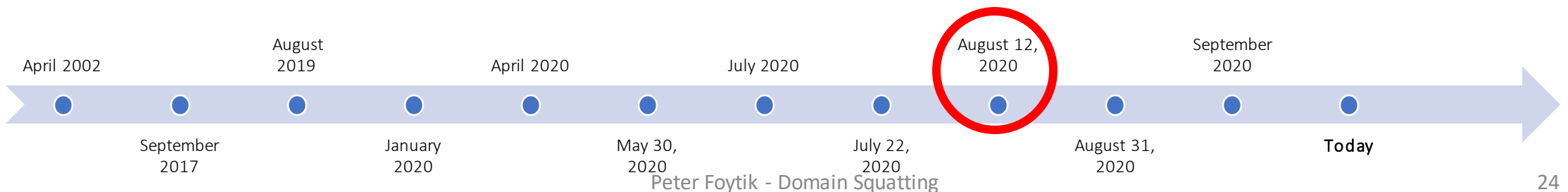


# Archives showing the redirect to JoeBiden.com August 12, 2020



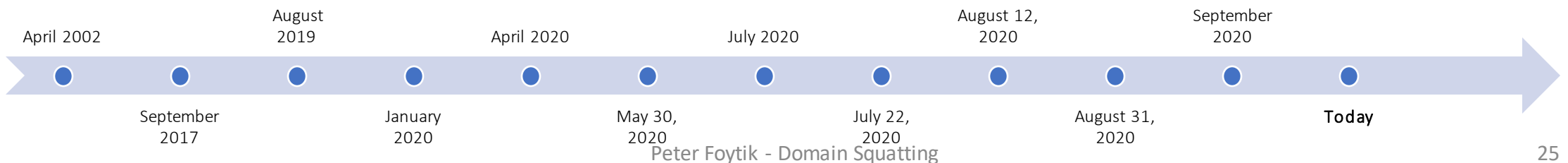
# Web.archive http response to antifa.com shows 301 response and redirect to joe Biden.com

```
<p class="code">Loading...</p>
  <p class="code shift target">http://antifa.com/ |
    20:16:03 August 12, 2020</p>
<p class="code shift red">Got an HTTP 301 response at crawl time</p>
<p class="code">Redirecting to...</p>
<p class="code shift target">https://joe Biden.com/</p>
  <p class="impatient"><a href="http://web.archive.org/web/20200812201603/https://joe Biden.com/">Impatient?</a></p>
```



# WhoIS results don't provide much

```
1 whois antifa.com
2   Domain Name: ANTIFA.COM
3   Registry Domain ID: 85915752_DOMAIN_COM-VRSN
4   Registrar WHOIS Server: whois.namecheap.com
5   Registrar URL: http://www.namecheap.com
6   Updated Date: 2020-08-14T19:04:21Z
7   Creation Date: 2002-04-24T12:35:11Z
8   Registry Expiry Date: 2021-04-24T12:35:10Z
9   Registrar: NameCheap, Inc.
10  Registrar IANA ID: 1068
11  Registrar Abuse Contact Email: abuse@namecheap.com
12  Registrar Abuse Contact Phone: +1.6613102107
13  Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
14  Name Server: DNS1.REGISTRAR-SERVERS.COM
15  Name Server: DNS2.REGISTRAR-SERVERS.COM
16  DNSSEC: unsigned
17  URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
18 >>> Last update of whois database: 2020-09-30T03:00:17Z <<<
```





Whoisology  
provides a  
little more!

September 2016  
April 2016  
August 2015  
December 2014  
April 2014  
August 2013  
December 2012

August 2014  
December 2013  
April 2013

\* Indicates the archive you are currently viewing

Disabled archives  
do not contain WHOIS data for this domain.

DATA WAREHOUSE SERVICES ▶

BIG DATA ANALYTIC TRENDS ▶

DATA ANALYSIS COURSES ▶

DATA ANALYSIS WORKSHEET ▶

DATA MANAGEMENT SKILLS ▶

Sponsored | Business Focus ▶

Admin Contact

The Admin Contact is the person or organization who controls the domain.

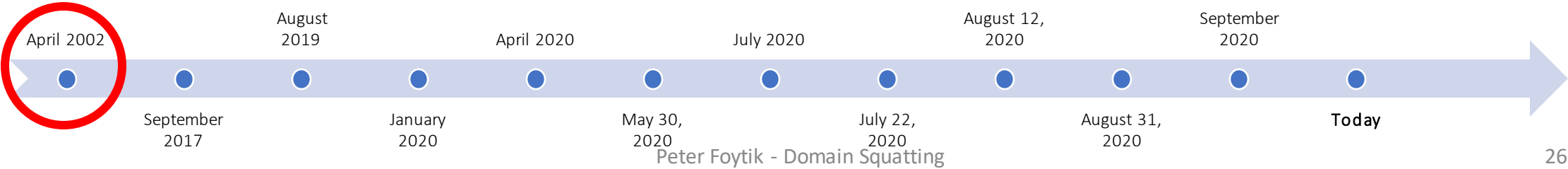
Name	WhoisGuard Protected (3,985,139) Changes: +249,671 ccTLD: 29,782
Org.	WhoisGuard, Inc. (3,857,141) Changes: +270,534 ccTLD: 24,689
Email	32508841545c4c54bd7a97ae9509eb3a.protect@whoisguard.com (1) Changes: +0 ccTLD: 0
Street	P.O. Box 0823-03411 (3,985,785) Changes: +249,737 ccTLD: 27,223
Street 2	-
City	Panama (4,021,931) Changes: +245,696 ccTLD: 29,964
Region	Panama (3,994,841) Changes: +248,762 ccTLD: 30,444
Zip / Post	-
Country	PANAMA (5,689,686) Changes: +683,234 ccTLD: 140,635
Phone	5078365503 (3,985,791) Changes: +249,725 ccTLD: 27,223
Fax	5117057182 (3,986,531) Changes: +249,760 ccTLD: 27,008

Other Details

These are technical details & related, connected to the domain.

Registrar Name	NameCheap, Inc.(7,641,701) Changes: +776,927 ccTLD: 315,988
Created Date	2002-04-24(38,355) Changes: +1,163 ccTLD: 1,784
Whois Servers	whois.namecheap.com(8,810,864) Changes: +1,082,875 ccTLD: 429,561
Updated Date	2019-10-23(361,514) Changes: +172,107 ccTLD: 75,088
Expires Date	2021-04-24(46,310) Changes: +328 ccTLD: 103,859
Name Servers	NS1.DOMAINRECOVER.COM(30,627) Changes: -855 ccTLD: 0 NS2.DOMAINRECOVER.COM(30,625) Changes: -855 ccTLD: 0
Archive Date	2019-12-21

<https://whoisology.com/antifa.com>





# Whoisology prior to 2019 record

[https://whoisology.com/archive\\_21/antifa.com](https://whoisology.com/archive_21/antifa.com)

March 2017  
September 2016  
April 2016  
August 2015  
December 2014  
April 2014  
August 2013  
December 2012

December 2015  
April 2015  
August 2014  
December 2013  
April 2013\*

\* Indicates the archive you are currently viewing

Disabled archives  
do not contain WHOIS data for this domain.

lookup.

Admin Contact

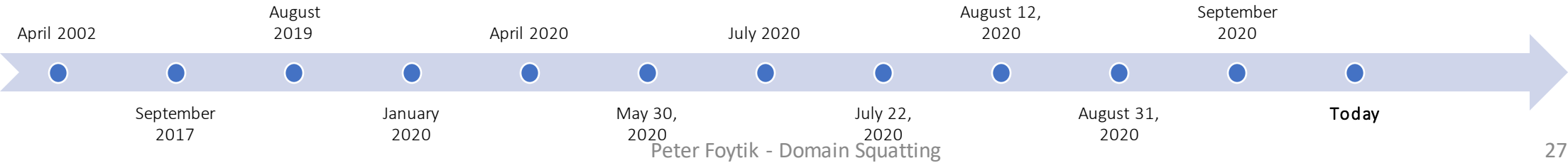
The Admin Contact is the person or organization who controls the domain.

Name	[Reserved For Advanced Members]
Org.	[Reserved For Advanced Members]
Email	[Reserved For Advanced Members]
Street	[Reserved For Advanced Members]
Street 2	[Reserved For Advanced Members]
City	Saint-Petersburg (110,408) Changes: +0 ccTLD: 45
Region	-
Zip / Post	[Reserved For Advanced Members]
Country	RUSSIAN FEDERATION (318,810) Changes: +0 ccTLD: 7,030
Phone	[Reserved For Advanced Members]
Fax	[Reserved For Advanced Members]

Other Details

These are technical details & related, connected to the domain.

Registrar Name	DOMREG LTD.(19,371) Changes: +0 ccTLD: 0
Created Date	2002-04-24(49,096) Changes: +0 ccTLD: 1,784
Whois Servers	whois.libris.com(19,371) Changes: +0 ccTLD: 0
Updated Date	2013-04-25(342,906) Changes: +0 ccTLD: 471
Expires Date	2014-04-24(339,728) Changes: +0 ccTLD: 0
Name Servers	NS1.DOMAINRECOVER.COM(51,686) Changes: +0 ccTLD: 0 NS2.DOMAINRECOVER.COM(51,675) Changes: +0 ccTLD: 0
Archive Date	2013-07-23



# Twitter user response to antifa.com

- Can we identify accounts that promoted antifa.com early based on dates of the Youtube account and website purchase?
- Are these accounts bot like or human like?
- What kind of influence were they able to achieve?
- The following Twitter analysis is retrieved with twitter tool Twint
  - All tweets containing antifa.com were obtained
  - Analysis is done with verified users and unverified Twitter accounts
  - `twint -s antifa.com --verified`

Earliest verified  
tweet containing  
antifa.com  
(now removed)  
Sep 03, 2017

Louise Mensch

- British conservative  
tweeted that  
Russians have  
bought the domain

URI-M

[http://web.archive.org/web/20170903231623if\\_/https://twitter.com/louisemensch/status/903783537006059524](http://web.archive.org/web/20170903231623if_/https://twitter.com/louisemensch/status/903783537006059524)

https://twitter.com/louisemensch/status/903783537006059524

Go AUG SEP MAY 03 2017 2019

9 captures 3 Sep 2017 - 16 Jun 2020

**Louise Mensch** @LouiseMensch Theo dõi

Well, well, well. If you thought #Antifa was a pathetically obvious Russian plot you were right. Antifa Dot Com registered in Russia #FAIL

**Reverse Whois:**

abuse@registrar.libris.com

whois.privacy@privacyid.com

Domain Name: ANTIFA.COM

Registry Domain ID: 85915752\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.libris.com

Registrar URL: http://libris.com

Updated Date: 2016-04-25T04:16:03Z

Creation Date: 2002-04-24T08:35:11Z

Registrar Registration Expiration Date: 2017-04-24T12:35:10Z

Registrar: DomReg Ltd. d/b/a LIBRIS.COM

Registrar IANA ID: 381

Registrar Abuse Contact Email: abuse@registrar.libris.com

Registrar Abuse Contact Phone: +7.8129140281

Domain Status: clientUpdateProhibited

Domain Status: clientTransferProhibited

Domain Status: clientDeleteProhibited

Registry Registrant ID:

Registrant Name: Whois privacy services provided by DomainProtect LLC

Registrant Organization: Whois privacy serv

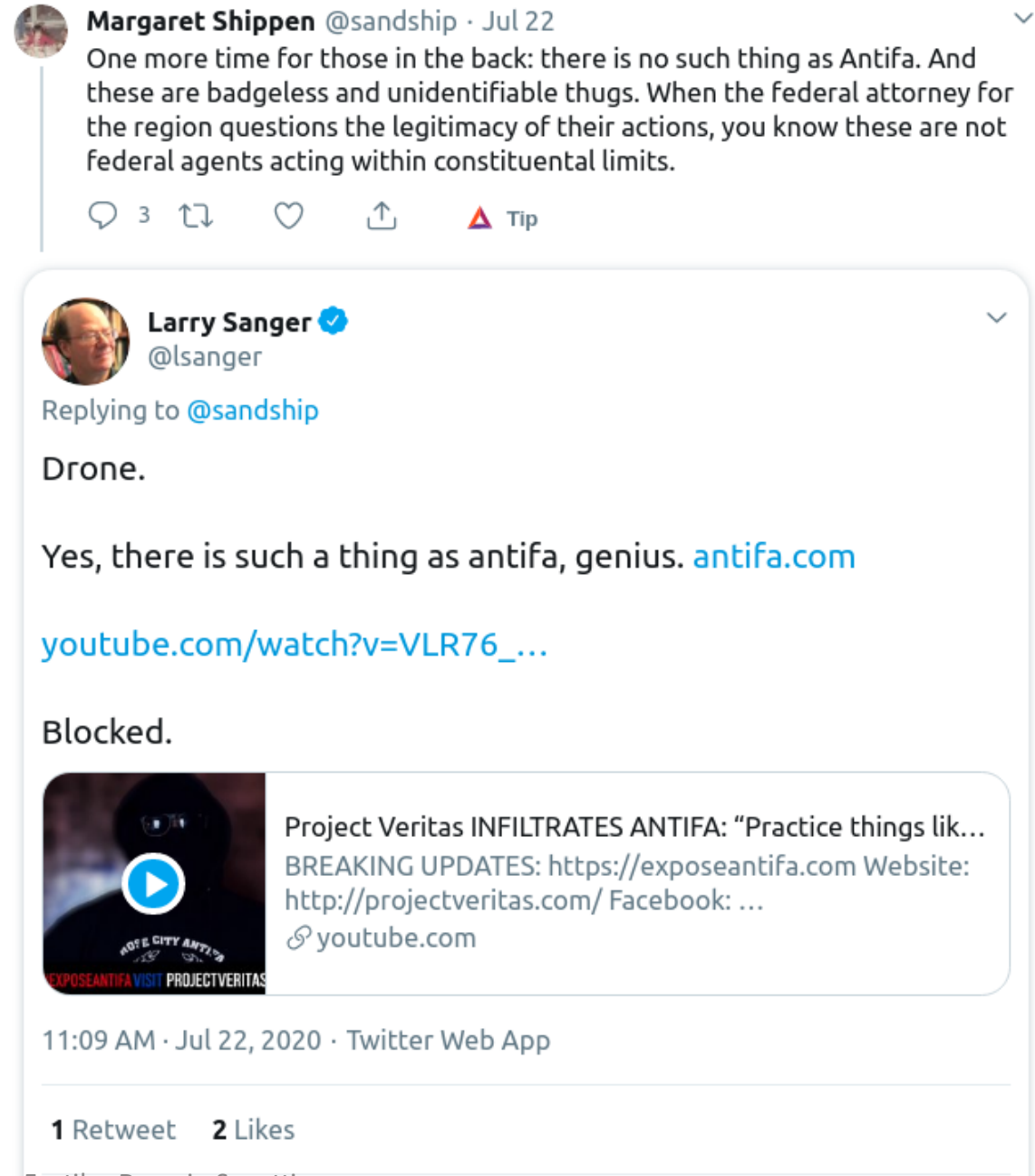
17:56 - 1 thg 9, 2017

# Earliest verified tweet referring antifa.com to the movement July 22, 2020

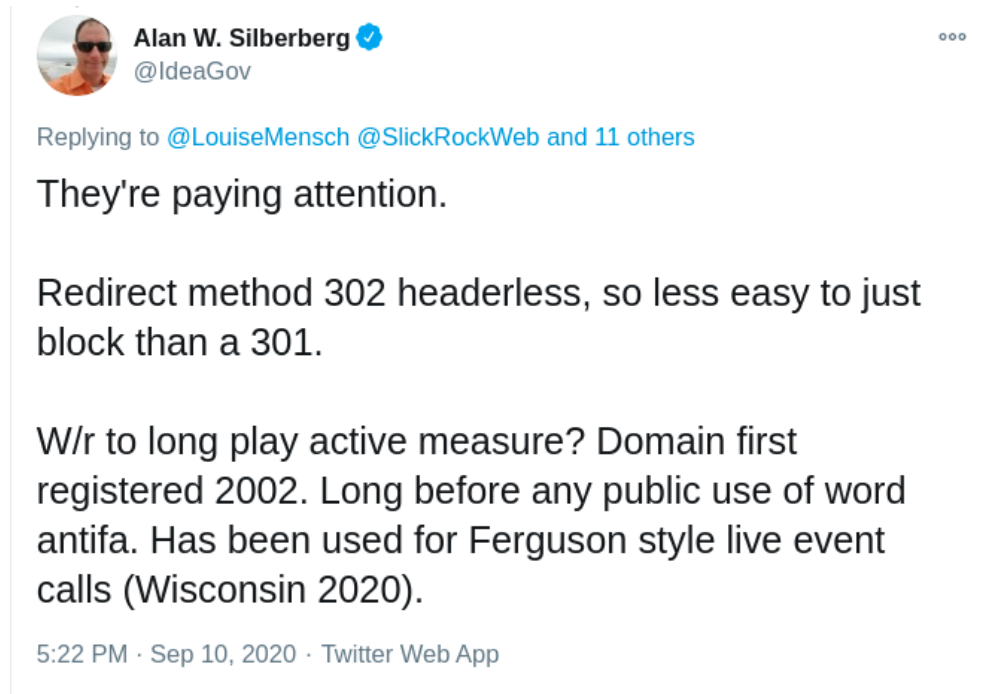
- Larry Sanger
- Co-founder of Wikipedia

URI-M:  
<http://web.archive.org/web/20200722234254/https://twitter.com/lsanger/status/1285955088259915776>

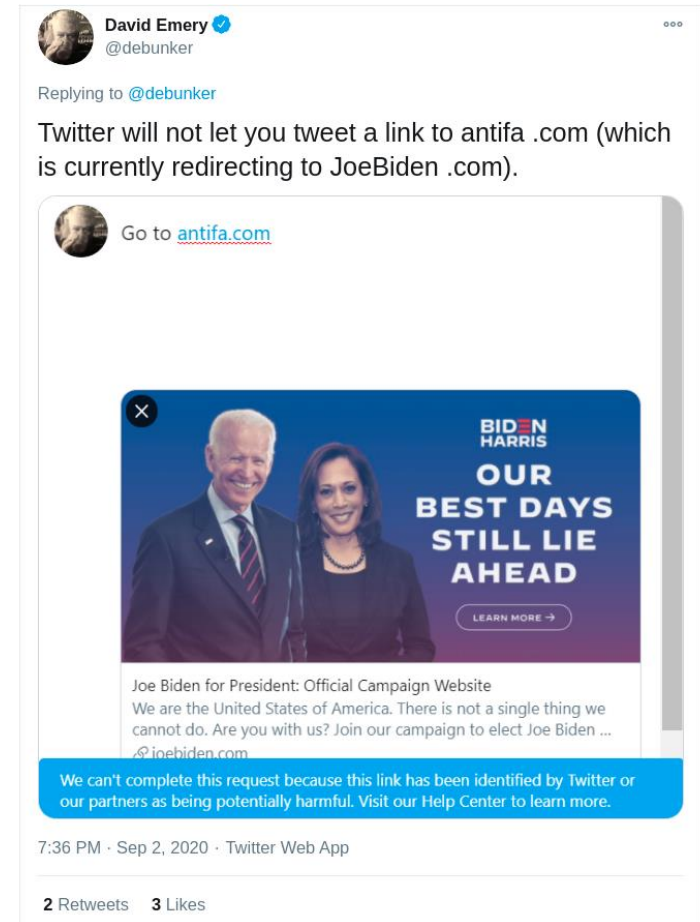
URI-R:  
<https://twitter.com/lsanger/status/1285955088259915776>



# Ranking by number of tweets involving antifa.com two accounts worked to raise awareness and debunk the redirected domain



<https://twitter.com/IdeaGov/status/1304168326130618368>

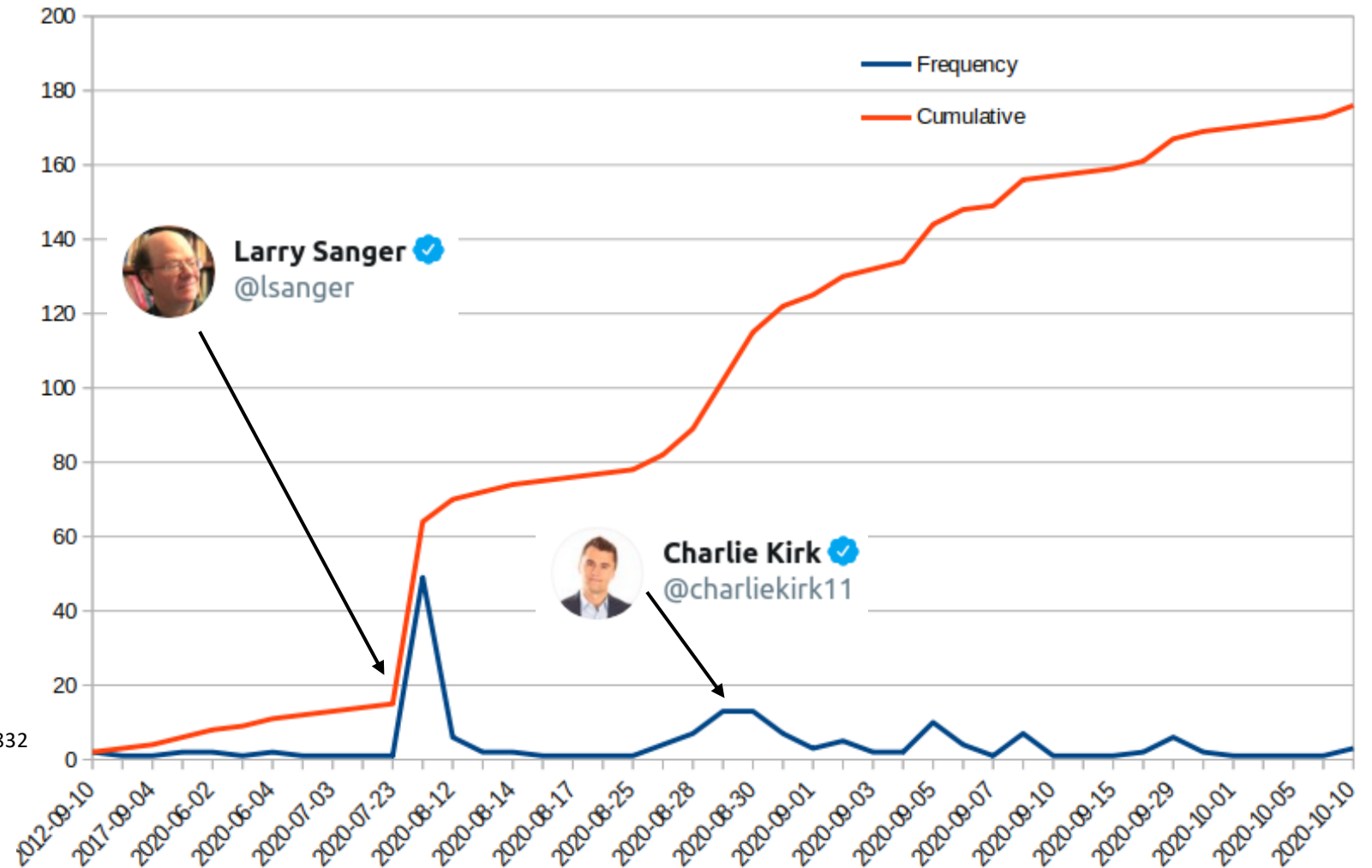


<https://twitter.com/debunker/status/1301303086741217281>

# Twitter verified user tweets containing antifa.com

URI-R Larry Sanger:  
<https://twitter.com/lsanger/status/1285955088259915776>

URI-R Charlie Kirk:  
<https://twitter.com/charliekirk11/status/1300596885774712832>



April 2002

August  
2019

April 2020

July 2020

August 12,  
2020

September  
2020

September  
2017

January  
2020

May 30,  
2020

July 22,  
2020

August 31,  
2020


Today

Peter Foytik - Domain Squatting




# Unverified Twitter accounts top ten tweeters, 2 registered as bots from Botometer

Account	Tweets	Botometer
fredgsanford18	21	4.7
towlecarolyn	13	1.8
li58653910	10	1.6
proud_vet1776	9	0.3
joetrela	9	1
terrilfricke	9	0
thedaily1birdy	9	3.8
repealbagfee	8	1
sebastian_usa	8	0.4
susanwh68243181	7	1.4




@TheDaily1BirdY

3.8 / 5




✕



@FredGSanford18

4.7 / 5



✕

Bot type scores

Astroturf0.2

Fake follower3.0

Financial0.4

Self declared3.9

Spammer1.3

Other4.7

Bot score based on

All features:4.7

10% of accounts with a bot score above 4.7 are labeled as humans.

Language-independent:4.2

Majority tweet language:en

Profile

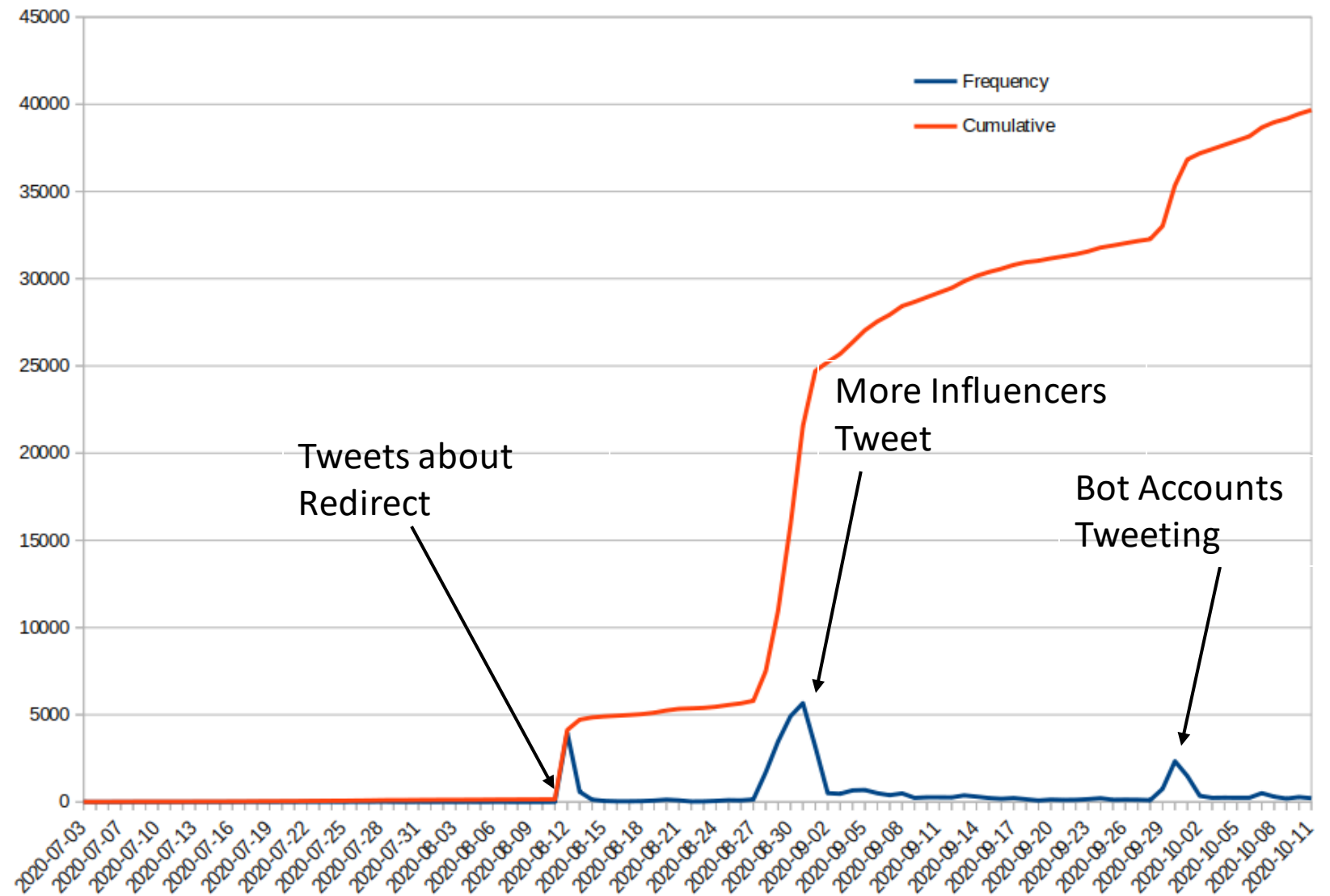
Tweet

Details

Feedback

# Twitter unverified user tweets containing antifa.com

Peaks match the google  
trends peaks\*



April 2002

August  
2019

April 2020

July 2020

August 12,  
2020

September  
2020

September  
2017

January  
2020

May 30,  
2020

July 22,  
2020

August 31,  
2020

Today

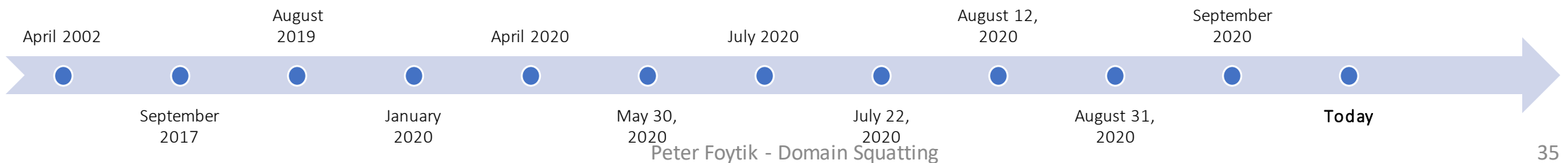
Peter Foytik - Domain Squatting

# Google Trends for antifa.com from July 1 to October 15, 2020

Interest over time ?



<https://trends.google.com/trends/explore?date=2020-07-01%202020-10-15&geo=US&q=antifa.com>



# Final Thoughts

- Was Joe Bidens campaign a victim of potential domain attack/squatting?
  - Evidence shows potential Russian involvement from purchase of the domain
  - No evidence of support from the political left
- Can we identify events showing potential sources of the attack?
  - A lot of effort from the political right on the domain
  - Identified accounts that are potential bots contributing to the spread antifa.com
- Just because a domain points to a website does not mean affiliation