

Quick writeup of the OSINT Challenge

Summary: OSINT challenge from hacktm Feb2020. This challenge had us searching through Twitter, Google G Suite, and Github. Going back in time was a huge part in finding clues that led to the flag. We sidestepped false positives in the form of images and a religious OS. It culminated in a grand map search where we finally found the flag.

Writeup by: HughBZ

Shoutout to:

RHD for the python script and map suggestion

Tahiti and others for the initial push

====

Title of Challenge: OLD Times

485 Points SOLVED

There are rumors that a group of people would like to overthrow the communist party.

Therefore, an investigation was initiated under the leadership of Vlaicu Petronel. Be part of this ultra secret investigation, help the militia discover all secret locations and you will be rewarded.

Author: Legacy + FeDEX

Flag Format: HackTM{SECRET}

====

Start by googling Vlaicu Petronel. You will find a twitter account:

<https://twitter.com/petronelvlaicu>



Using the wayback time machine, you will find some tweets he posted, but deleted. These tweets included a Hash and a reference to Google G Suite.

HASH from wayback time machine

1XhgPI0jpK8TjSMmSQ0z5Ozcu7EIIWhlXYQECJ7hFa20

<https://web.archive.org/web/20191206221653/https://twitter.com/PetronelVlaicu/>



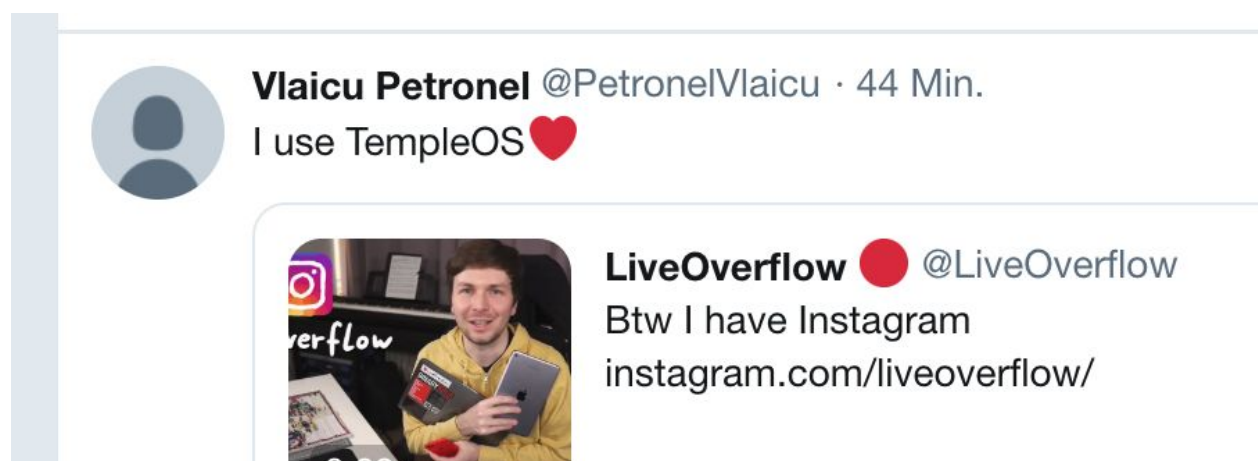
Ok, he also likes G Suite

<https://web.archive.org/web/20191207122850/https://twitter.com/PetronelVlaicu/>



And TempleOS

<https://web.archive.org/web/20191206224037/https://twitter.com/PetronelVlaicu/>



The TempleOS was a false lead. So focus on the other two items we found. Because he likes Google G Suite, we know that there are multiple services he can use from there. Looking at the way Google handles URLs for various services, you can try and access them if they are open to the public.

docs.google.com/spreadsheets/d/<hash of the file>

docs.google.com/documents/d/<hash of the file>

****KEY TTP for OSINT - how to search Google Public Docs*****

So because we had a hash from the wayback machine of the twitter account, we can then use that to find a hidden doc.

<https://docs.google.com/document/d/1XhgPI0jpK8TjSMmSQ0z5Ozcu7EIIWhlXYQECJ7hFa20/edit>

Report - Week VII

The local activity is under control. People seek their daily routine, and have no doubts about the party, except for one man: lovescu Marian.

Profile:



Name: lovescu Marian

Address: Romania, Timisoara, str. Hurta, nr. 35

Activity: IT Programmer

Description: lately, his activity has been suspicious. Therefore, I followed him closely for a week and found out that he was setting up an anti-communist uprising. He has been working for a while on a secret program that wants to motivate the population to overthrow the communist system. The problem is that two days ago he realized that I was following him and deleted all the work that he published on a free and open platform.

Signed: lovescu Marian

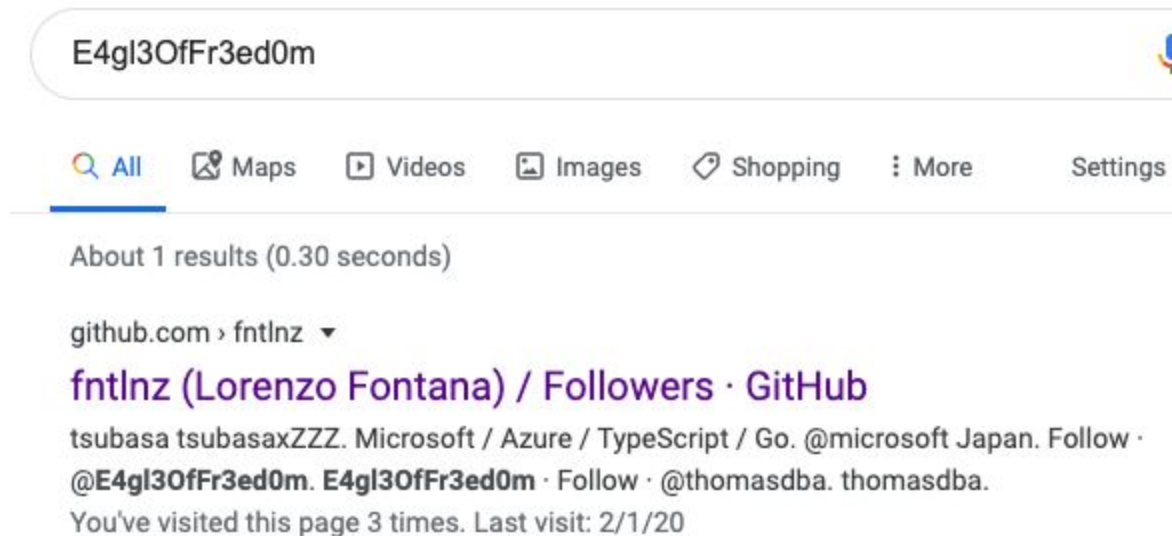
This document has a quite a bit of information. But the main piece to focus on is the small font text

except for one man: lovescu Marian - who goes by the name of E4g30fFr3edom

Take the text from the file and copy it to another document and you can then zoom in or increase the font. The small font is: who goes by the name of E4g30fFr3edom

E4g30fFr3edom

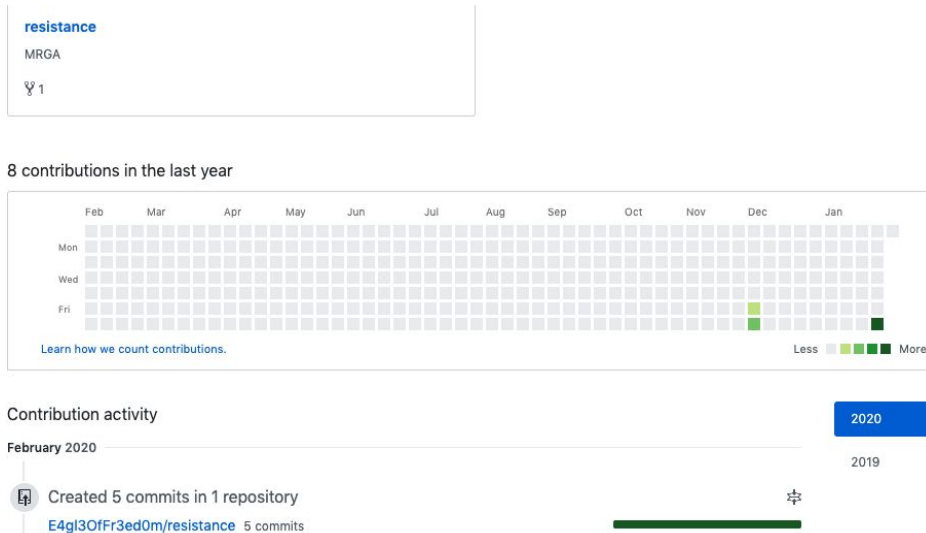
This was the keyword to continue with the search. Google this term and you will find a github entry.



Go to <https://github.com/fntlnz?tab=followers> and you will then find [E4gl3OfFr3ed0m](https://github.com/E4gl3OfFr3ed0m) github.



Below is his dashboard at <https://github.com/E4gl3OfFr3ed0m>



From here you will see a small github for that user. Even has resistance in the path so we are on the right trail. Recalling what the doc said: The problem is that two days ago he realized that I was following him and deleted all the work that he published on a free and open platform.

So, checking the history of the git, we can find some more hidden pieces.

<https://github.com/E4gl3OfFr3ed0m/resistance/commit/e5988df76e62f01b1017ad14f510b69e7761337d#diff-04c6e90faac2675aa89e2176d2eec7d8>

The screenshot shows a GitHub commit diff for the file 'README.md'. It indicates 1 changed file with 1 addition and 0 deletions. The diff shows the following changes:

```
...  ... @@ -1,2 +1,3 @@
1 1  # resistance
2 2  there is nothing to see in the picture 🤪
3 + <!-- http://138.68.67.161:55555/ -->
```

Further checks of the commits reveals more files.

MRGA

 **6 commits**


 **1 branch**

Branch: **master** ▼

New pull request

 **E4gl3OfFr3ed0m** Update README.md

 [README.md](#) Up

 [heart.jpg](#) Ac

Commits on Jan 31, 2020

Update README.md

 **E4gl3OfFr3ed0m** committed yesterday

Update README.md

 **E4gl3OfFr3ed0m** committed yesterday

Add files via upload

 **E4gl3OfFr3ed0m** committed yesterday

Delete spread_locations.php

 **E4gl3OfFr3ed0m** committed yesterday

top secret

 **E4gl3OfFr3ed0m** committed yesterday

Commits on Dec 7, 2019

Initial commit

 **E4gl3OfFr3ed0m** committed on Dec 7, 2019

By looking at the “top secret” commit, you will find the php code of spread_locations.php.

```
<?php
```

```
$myfile = fopen("locations.txt", "r") or die("Unable to open file!");  
$locs = fread($myfile,filesize("locations.txt"));  
fclose($myfile);  
$locs = explode("\n",$locs);  
  
$reg = $_GET["region"];  
if($reg < 129 && $reg >= 0){  
    echo "<b>[".$reg."]:</b> ";  
    echo $locs[$reg];  
}  
else{  
    echo "<b>Intruder!</b>";  
}  
  
?>
```

Combining the IP address we found and the php, you will get this:

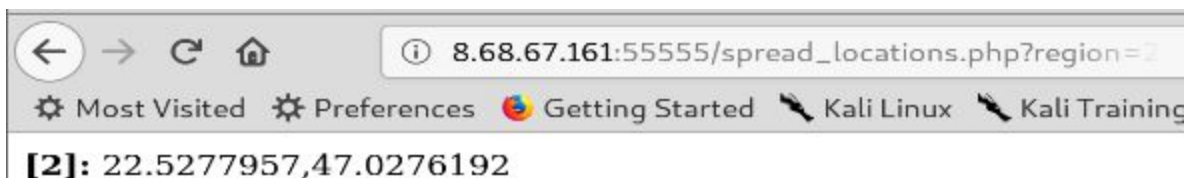
http://138.68.67.161:55555/spread_locations.php

And if you go to the web page, this is the result.



[]:

In the php code, you can see a region parameter that will spit out something if the values are between 0-128, else it will output "Intruder!"



The below python script below will give all the values when you use 0-128.

====begin script

```
import requests
```

```
baseurl = 'http://138.68.67.161:55555/spread_locations.php?region={}'
```

```
for i in range(0,129):
    r = requests.get(baseUrl.format(i))
    coords = r.text.split(' ')[1]
    print(coords)
```

====end script

Also, Bash one liner

```
===begin script
for ((i=0;i<=128;i++)); do curl
"http://138.68.67.161:55555/spread_locations.php?region=$i"; echo " "; done
===end script
```

We can see that the output looks like some decimal numbers, but they are really lat/long or GPS coordinates.

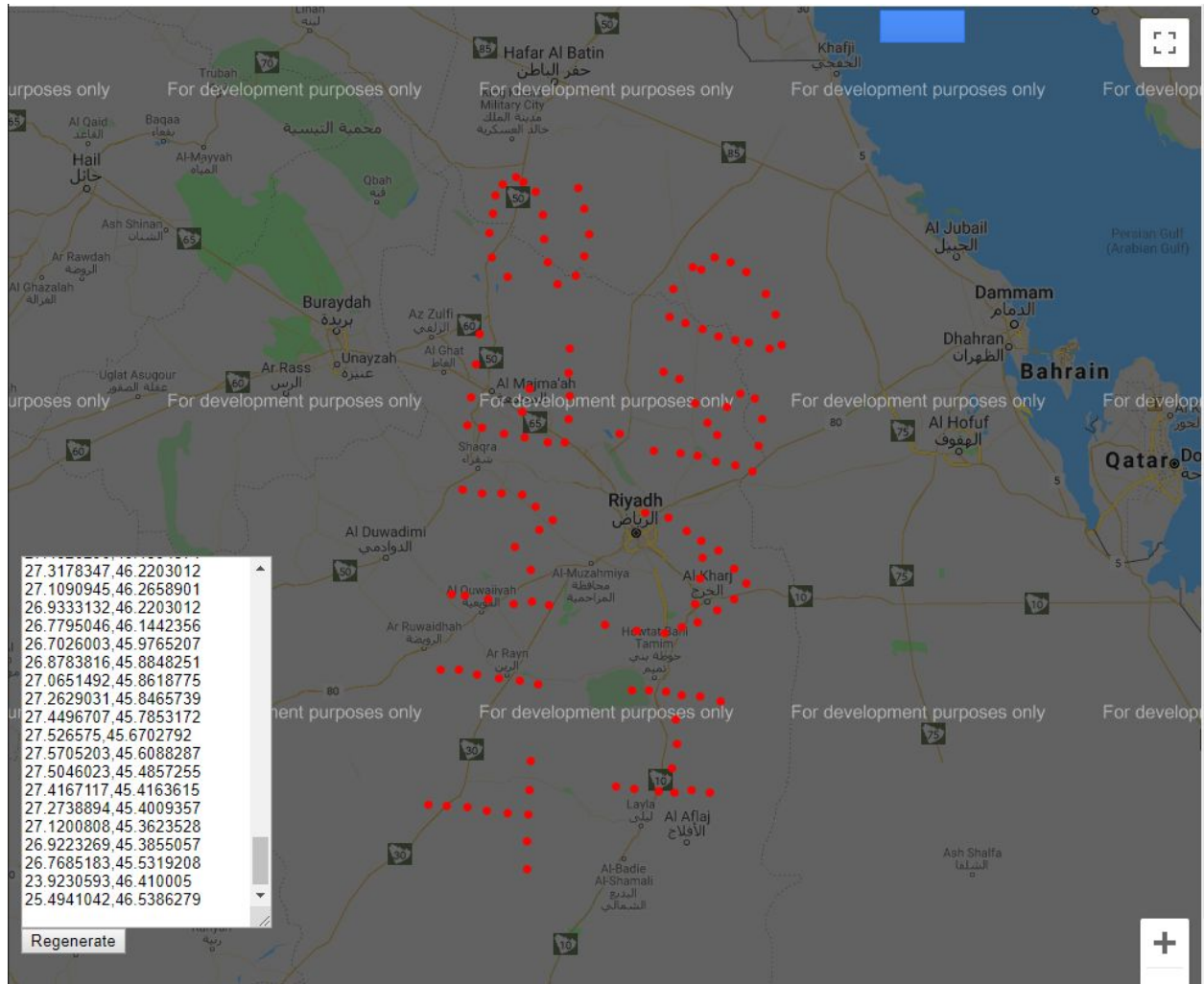
```
22.5277957,47.3561089
22.5497683,47.184652
22.5277957,47.0276192
```

...

<deleted for saving space, see Supplemental Info: at the end of this document for complete list>

You can then take these values and input them into map software that allows multiple markers. We used hamstermap. Take the list of values received from the secret_locations.php, and paste them into the form as in the picture below, it will then place a dot for each coordinate, creating letters on the map.

<http://www.hamstermap.com/quickmap.php>



Reflected, it spells HARD TIMES.

This text is the flag for the challenge and must be submitted as:

HackTM{HARDTIMES}

END

Key Lessons for OSINT learned from the challenge

- Use wayback time machine and git history to see if anything was left behind
- You can view public documents in Google G Suite products if you know the hash and link
- Check followers of accounts, they can lead you to other possibilities.
- There are multiple map apps you can use.

Supplemental Info:

Things we tried while hunting for the flag on this challenge, kept for historical reference
<https://twitter.com/petronelvlaicu>

@PetronelVlaicu

- Joined December 2019
- Following @nicolaeceausesc
-

@nicolaeceausesc

- Joined January 2011
- Probably not CTF controlled

@NicolaeCeauesc2

- Joined September 2019
- Following @nicolaeceausesc
- Maybe ctf controlled?

<https://twitter.com/pitarresg>

This user has been actively replying to the @PetronelVlaicu account

Tried:

Looking up image name

Word scramble on the Vlaciui name

Steg on romanian flag

Ciphertext decrypt:

Frombase64

Hope that the php will spit out the flag was destroyed :(

Complete list of Lat/Long of the secret_locations.php and locations.txt

22.5277957,47.3561089
22.5497683,47.184652
22.5277957,47.0276192
22.538782,46.8851427
22.5607546,46.6669469
22.5827273,46.508391

22.7365359,47.0051481
22.9342898,47.0500808
23.14303,47.0425947
23.2968386,47.4527737
23.3297976,47.2667225
23.3407839,47.1024545
23.3737429,46.9601776
23.3847292,46.8024828
23.3847292,46.6443244
23.879114,46.6970954
24.2636355,47.6825664
24.8459109,46.7648681
25.1864871,47.7343156
25.351282,46.8475858
24.1317996,47.5715023
24.0439089,47.4156159
23.945032,47.2443522
23.9010867,47.1024545
23.8571414,46.945179
24.3844851,47.5715023
24.5382937,47.4230496
24.615198,47.2741771
24.6921023,47.1398328
24.8019656,46.9826676
24.0988406,47.2145105
24.3075808,47.2592668
24.4723757,47.2890833
25.2304324,47.5863245
25.2633914,47.4081812
25.318323,47.2368934
25.3293093,47.0874959
25.4831179,47.4156159
25.3952273,47.7860133
25.6149539,47.8229089
25.7797488,47.756478
25.8236941,47.6233616
25.7138308,47.5047505
25.5819949,47.3263302
25.7358035,47.2145105
25.9335574,47.072533
25.9994753,46.9376782
26.2192019,47.9996428
26.1862429,47.8892548

26.2301882,47.7047509
26.2521609,47.5789139
26.2851199,47.4230496
26.3400515,47.2890833
26.4609011,47.9481577
26.625696,47.8524065
26.8014773,47.6825664
26.8783816,47.5344284
26.3949832,47.1323592
26.9223269,47.3933087
26.82345,47.2741771
26.4389285,46.9901622
26.6696414,47.0201299
26.8454226,47.1921182
21.8905886,45.7009791
22.1213015,45.7009791
22.3520144,45.7086515
22.5497683,45.723993
22.7914675,45.7316622
23.4286746,45.8006377
24.0878542,45.9001182
24.7909792,45.9383326
25.4281863,46.0451929
25.6149539,46.0756865
25.8017214,46.0833073
25.988489,46.0756865
26.1862429,46.090927
22.3630007,45.5242242
22.3849734,45.3391904
22.406946,45.161297
22.4179324,44.9828465
22.4289187,44.8116333
23.4616335,45.6395623
23.4836062,45.4549076
23.5165652,45.2541805
23.5495242,45.0915349
23.5495242,44.9206461
24.1208132,45.7469975
24.9008425,45.7776553
24.0988406,45.5780782
24.1317996,45.3469122
24.1647585,45.1458017
24.1757449,45.0216875

24.9997195,45.6626015
25.0107058,45.4703187
25.0107058,45.2928371
25.0326785,45.1225508
24.5712527,45.5934555
24.7030886,45.8082963
24.3734988,45.7316622
25.4281863,45.8848251
25.4611453,45.6779557
25.4941042,45.4934274
25.5380496,45.3005653
25.5600222,45.1690431
25.7907351,45.2000169
26.054407,45.246446
26.3070925,45.2773776
25.6698855,45.6626015
25.8566531,45.723993
27.4826296,46.1594571
27.3178347,46.2203012
27.1090945,46.2658901
26.9333132,46.2203012
26.7795046,46.1442356
26.7026003,45.9765207
26.8783816,45.8848251
27.0651492,45.8618775
27.2629031,45.8465739
27.4496707,45.7853172
27.526575,45.6702792
27.5705203,45.6088287
27.5046023,45.4857255
27.4167117,45.4163615
27.2738894,45.4009357
27.1200808,45.3623528
26.9223269,45.3855057
26.7685183,45.5319208
23.9230593,46.410005
25.4941042,46.5386279