

Bjorka

Majestic Cassowaries

Daftar Isi

1. [OSINT] - Threat Actor Local [90]	2
2. [OSINT] - Threat Actor Local - 2 [55]	4
3. [OSINT] - Threat Actor Local - 3 [148]	6
4. [OSINT] - Threat Actor Local - 4 [150]	10

Write Up

Majestic Cassowaries

1. [OSINT] - Threat Actor Local [90]

Challenge

2 Solves

×

Threat Actor Local

90

Dikabarkan seorang threat actor lawas telah kembali ke indonesia untuk melancarkan kembali aksinya, berikut adalah rekam jejak digital yang dia tinggalkan pada tahun 2017.
<https://virusresearch.org/remove-mafiaware-ransomware-file-virus-locked-mafia-extension/> ditahun ini dia menargetkan beberapa instansi pemerintah. pada pesan ancamanya dia menggunakan email baru yaitu dompetspresiden@gmail.com.

bisakah anda membantu kami melakukan tracking informasi terbaru terkait threat actor ini? informasi terakhir yang kami dapatkan bahwa dia akan bertemu seseorang dengan inisial MR.K.

format flag : ObyteCTF{\w+}

Author:Rio

Flag

Submit

Diberikan sebuah Challenge sebagai berikut, dimana tujuannya mencari Informasi terbaru mengenai Threat Actor, salah satunya Pertemuan sang Threat Actor dengan MR.K, pada challenge ini terdapat 2 **Clue** yang dimana salah satunya merupakan sebuah Kunci untuk menemukan flagnya, yaitu akun gmail terbaru sang Threat Actor.

Disini saya melakukan analisa menggunakan Tools Osint bernama [GHunt](#), lalu setelah tools tersebut di running kita mendapatkan sebuah result pada "Calendar Data" yang bernama "Meeting w/ Mr. K" sesuai dengan informasi pada Challenge.

```
Calendar ID : dompetspresiden@gmail.com
Calendar Timezone : Asia/Jakarta

[+] 1 event dumped ! Showing the last 1 one ...
```

Name	Datetime (UTC)	Duration
Meeting w/ Mr. K	2021/02/27 23:00:00	1 hour

```
Download link :
⇒ https://calendar.google.com/calendar/ical/dompetspresiden@gmail.com/public/basic.ics
```

Setelah file "basic.ics" di download dan dibuka, flag pun ditemukan.

```
1 BEGIN:VCALENDAR
2 PRODID:-//Google Inc//Google Calendar 70.9054//EN
3 VERSION:2.0
4 CALSCALE:GREGORIAN
5 METHOD:PUBLISH
6 X-WR-CALNAME:dompetspresiden@gmail.com
7 X-WR-TIMEZONE:Asia/Jakarta
8 BEGIN:VEVENT
9 DTSTART:20210227T230000Z
10 DTEND:20210228T000000Z
11 DTSTAMP:20240818T131618Z
12 UID:4qohdcfanh7fh6opotd08u8a77@google.com
13 CLASS:PUBLIC
14 CREATED:20240806T230355Z
15 DESCRIPTION:Flag : gl4d_y0ur3_h3r3_th1s_1s_y0ur_1sT_St3p
16 LAST-MODIFIED:20240806T230355Z
17 LOCATION:Indonesia
18 SEQUENCE:0
19 STATUS:CONFIRMED
20 SUMMARY:Meeting w/ Mr. K
21 TRANSP:OPAQUE
22 END:VEVENT
23 END:VCALENDAR
24
```

Flag:

**0byteCTF{gl4d_y0ur3_h3r3_th1s_1s_y0ur_1sT_St3p
}**

2. [OSINT] - Threat Actor Local - 2 [55]

Challenge

9 Solves

X

Threat Actor Local - 2

55

lakukan profiling lebih dalam pada threat actor tersebut, cari forum dimana dia akan berdiskusi terkait ransomware.

format flag : 0byteCTF{\w+}

Author: Rio

Flag

Submit

Diberikan sebuah challenge sebagai berikut, Tujuan saya adalah melakukan profiling secara mendalam dengan Petunjuk yang diberikan adalah forum underground tempat dia berdiskusi/berinteraksi terkait Ransomware.

Dengan informasi email terbaru dari challenge sebelumnya. saya menggunakan nama email tersebut sebagai username pada forum underground tersebut. dan ditemukan sebuah profil seperti pada gambar dibawah ini.

Home

Databases

Upgrades

Search

Hidden Service

Escrow

Extras

Bjorka

212

412

87495

BreachForums

Profile of dompetspresiden

Mark all as read

Today's posts

dompetspresiden

Breached

Status: Offline (Last Visit: 08-07-2024, 07:36 AM)

Add to Ignore List

Report User

dompetspresiden's Forum Info

MEMBER

Joined: 08-06-2024

Time Spent Online: 42 Minutes, 7 Seconds

User Identifier: 273539 (Copy Profile Permalink)

Gift this user a Rank.

Members Referred: 0

dompetspresiden's Contact Details

Private Message: Send dompetspresiden a private message.

dompetspresiden's Forum Statistics

Total Threads: 1 (0.08 threads per day | 0 percent of total threads) [Find All Threads](#)

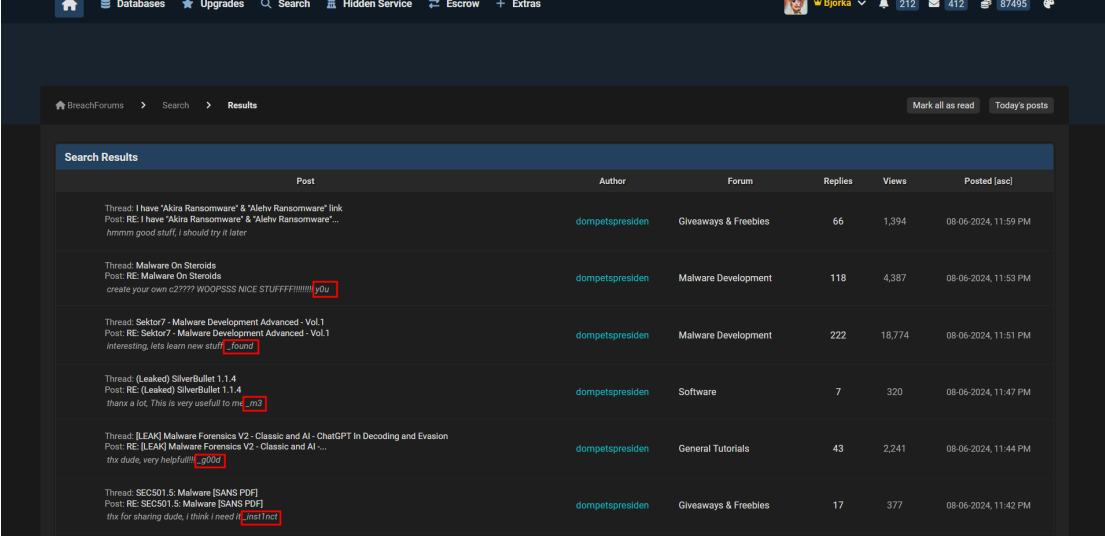
Total Posts: 7 (0.57 posts per day | 0 percent of total posts) [Find All Posts](#)

Reputation: 0 [Details](#)

dompetspresiden's awards.

This user has no awards at this time.

Setelah membuka Total Post dari akun tersebut, ditemukan berbagai Diskusi sang Threat Actor mengenai Ransomware. Dan tiap akhir diskusi tersebut tersebar potongan flagnya seperti pada gambar dibawah ini.



Post	Author	Forum	Replies	Views	Posted [asc]
Thread: I have "Akira Ransomware" & "Alehv Ransomware" link Post: RE: I have "Akira Ransomware" & "Alehv Ransomware" link hmmmm good stuff, I should try it later	dompetsyresiden	Giveaways & Freebies	66	1,394	08-06-2024, 11:59 PM
Thread: Malware On Steroids Post: RE: Malware On Steroids create your own c2???? WOOPSSS NICE STUFF!!!!!! y0u	dompetsyresiden	Malware Development	118	4,387	08-06-2024, 11:53 PM
Thread: Sektor7 - Malware Development Advanced - Vol.1 Post: RE: Sektor7 - Malware Development Advanced - Vol.1 interesting, lets learn new stuff _found	dompetsyresiden	Malware Development	222	18,774	08-06-2024, 11:51 PM
Thread: (Leaked) SilverBullet 1.1.4 Post: RE: (Leaked) SilverBullet 1.1.4 thats a lot, This is very usefull to me _m3	dompetsyresiden	Software	7	320	08-06-2024, 11:47 PM
Thread: [LEAK] Malware Forensics V2 - Classic and AI- ChatGPT In Decoding and Evasion Post: RE: [LEAK] Malware Forensics V2 - Classic and AI- ChatGPT In Decoding and Evasion thx dude, very helpful _g00d	dompetsyresiden	General Tutorials	43	2,241	08-06-2024, 11:44 PM
Thread: SEC501.5: Malware [SANS PDF] Post: RE: SEC501.5: Malware [SANS PDF] thx for sharing dude, I think I need it _inst1nct	dompetsyresiden	Giveaways & Freebies	17	377	08-06-2024, 11:42 PM

Flag:

0byteCTF{y0u_found_m3_g00d_inst1nct}

3. [OSINT] - Threat Actor Local - 3 [148]

Challenge

3 Solves

×

Threat Actor Local - 3

148

temukan lokasi gedung/tempat terakhir dia singgah.

format flag : ObyteCTF{\w+}

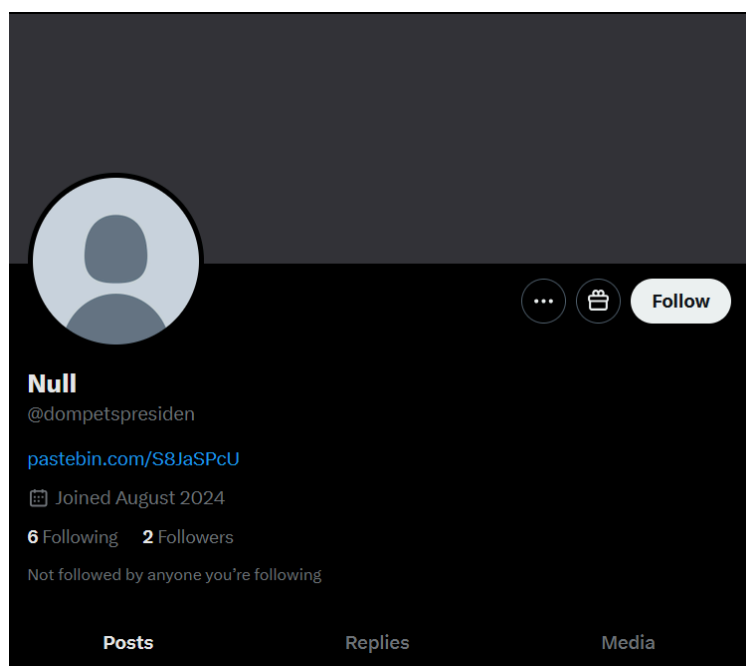
Author:Rio

Flag

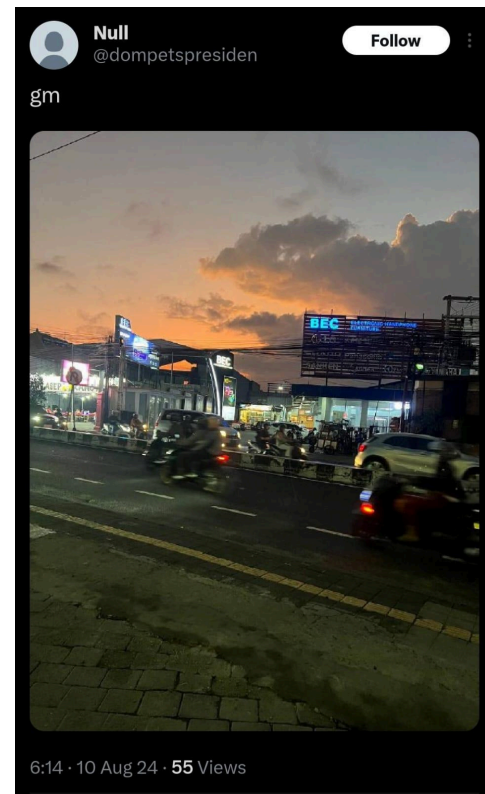
Submit

Diberikan sebuah challenge sebagai berikut, challenge ini masih berlanjut dari challenge-challenge sebelumnya, Pada challenge ini kita harus menemukan lokasi tempat sang Threat Actor singgah.

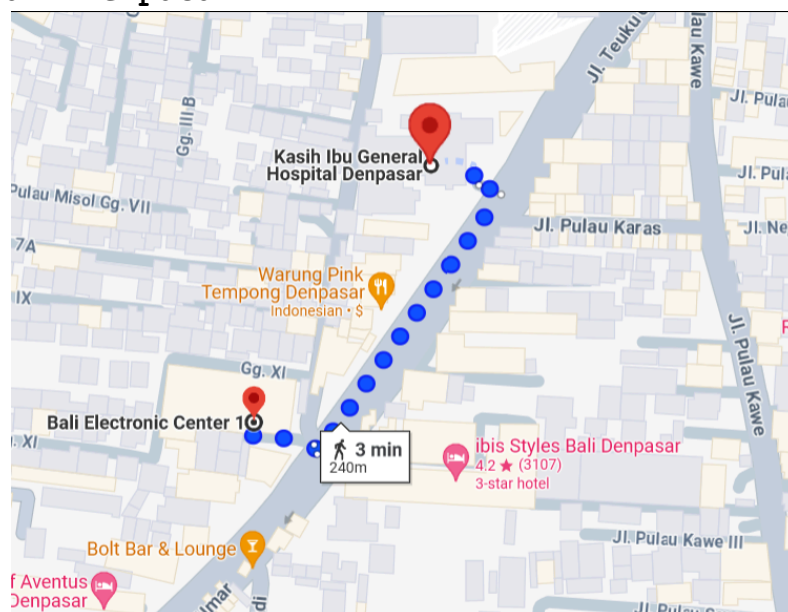
Dengan informasi email terbaru dari challenge sebelumnya. saya menggunakan nama email tersebut sebagai username pada Sosial Media X. Lalu saya menemukan akun yang dicari seperti pada gambar dibawah ini.



Setelah melakukan analisa pada dua tweet dibawah ini. Saya pun mendapatkan informasi jika lokasi Threat Actor Berada di Bali dan menginap di sebuah Hotel yang berada dekat dengan **RS Kasih Ibu Denpasar** dan **Bali Electronic Center**.



Ditemukan bahwa hotel terdekat yang berada di tengah-tengah kedua lokasi tersebut adalah **Hotel "ibis Styles Bali Denpasar"**



Ketika saya melakukan analisa pada Review Hotel tersebut, terdapat sebuah review dari user yang tidak asing. Review tersebut dilakukan melalui Tripadvisor

←

ibis Styles Bali Denpasar

Q

X

Overview

Prices

Reviews

About

Rp 700.776 · 3-star hotel

Aug 26 – 27


CHECK AVAILABILITY

d

dompets p

5/5

a week ago on

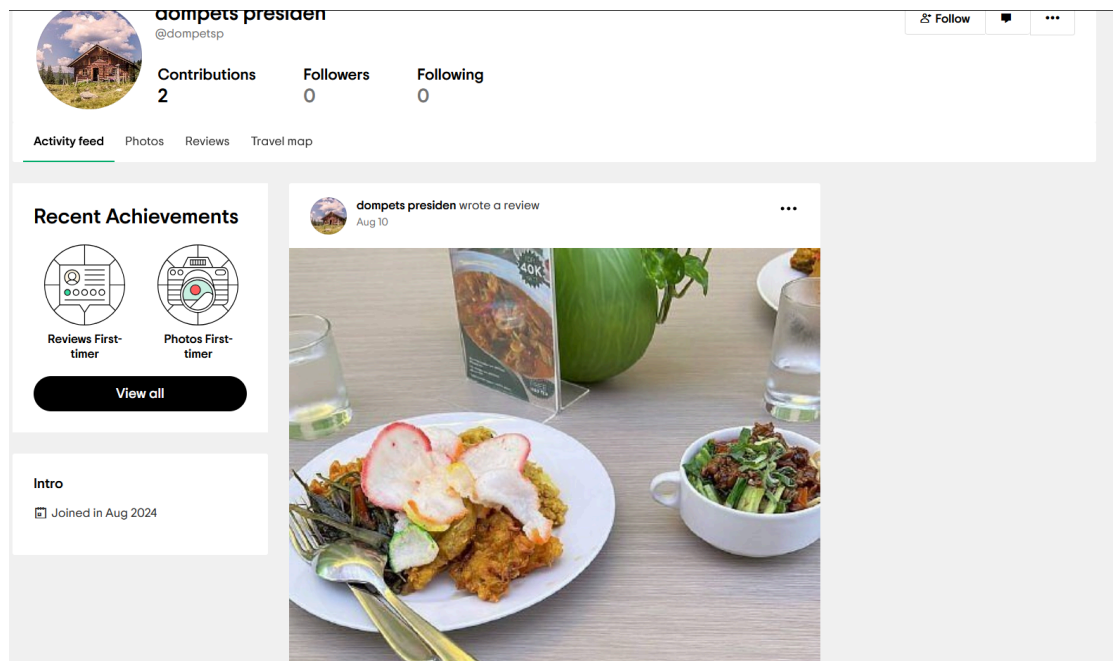


Tripadvisor

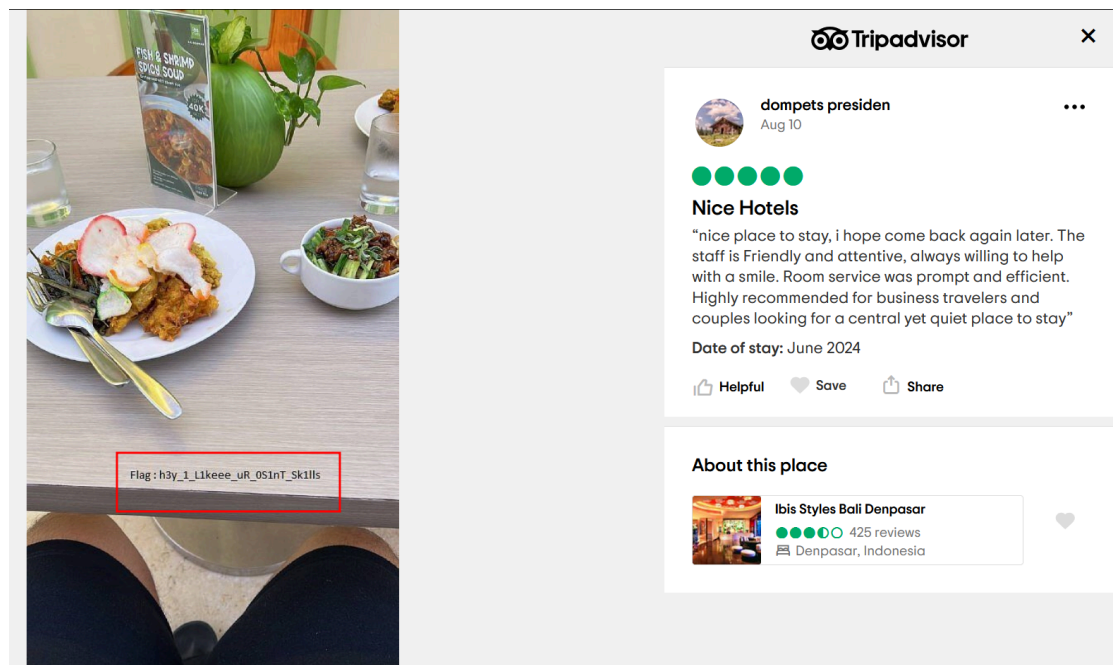
NEW

nice place to stay, i hope come back again later. The staff is Friendly and attentive, always willing to help with a smile. Room service was prompt and efficient. Highly recommended for business travelers and couples looking for a central yet quiet place to stay

Berikut tampilan dari Halaman Profil @dompetsp pada Tripadvisor, bisa dilihat profil tersebut mengupload sebuah gambar.



Ketika gambar tersebut dibuka, flag yang dicari akhirnya ditemukan



Flag:

0byteCTF{h3y_1_L1keee_0S1nT_Sk1lls}

4. [OSINT] - Threat Actor Local - 4 [150]

Challenge

1 Solves

×

Threat Actor Local - 4

150

temukan akun github terbaru dari threat actor tersebut.

format flag : ObyteCTF{w+}

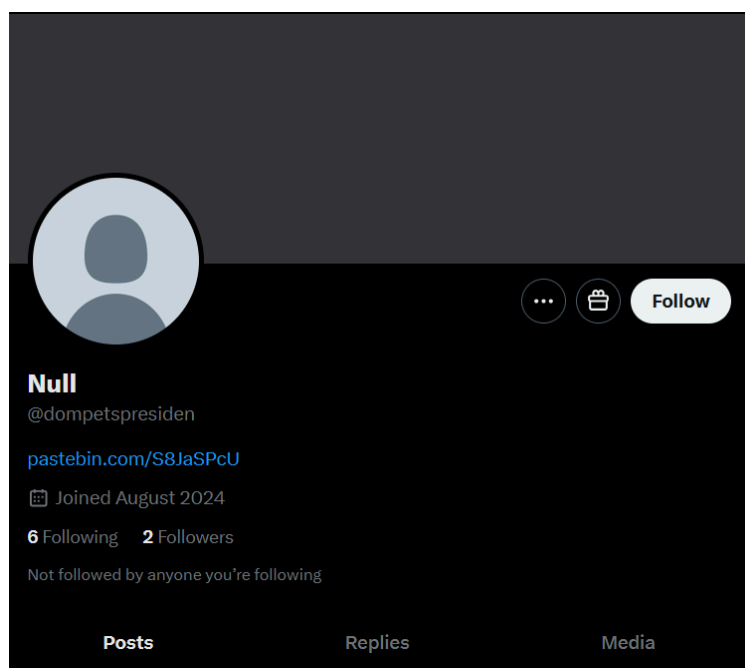
Author:Rio

Flag

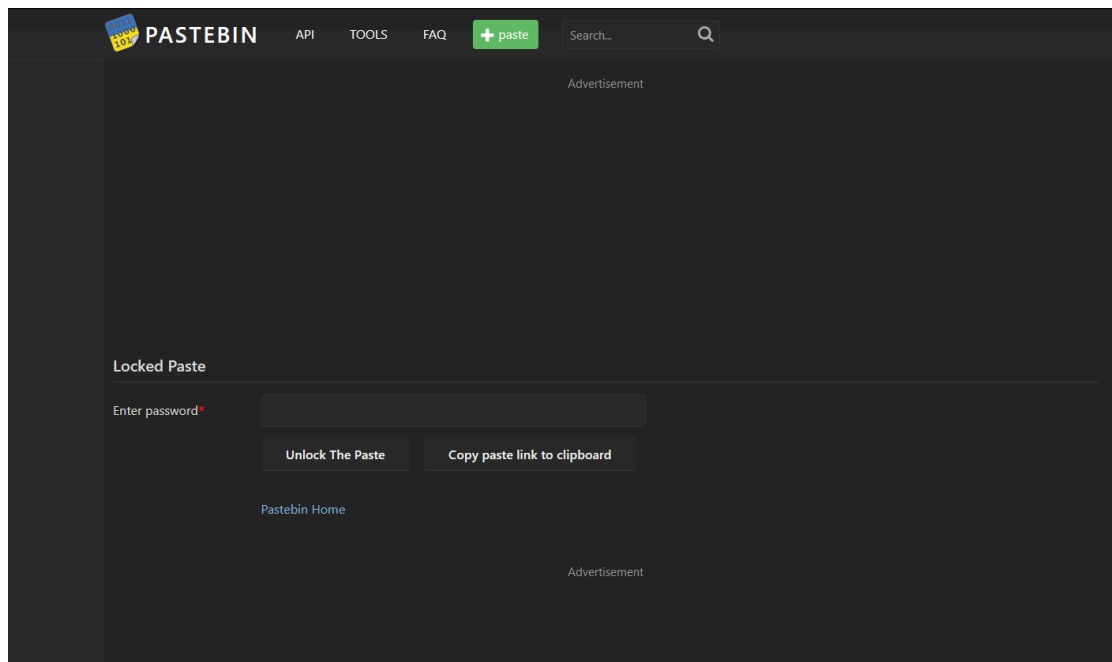
Submit

Diberikan sebuah challenge sebagai berikut, challenge ini masih berlanjut dari challenge-challenge sebelumnya, Pada challenge ini kita harus menemukan akun github terbaru sang Threat Actor.

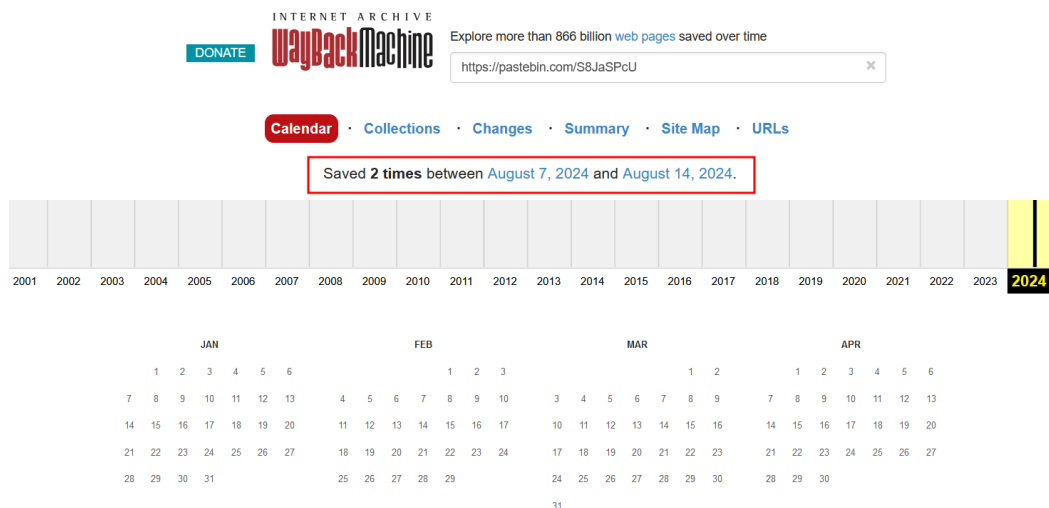
Dengan informasi email terbaru dari challenge sebelumnya. saya menggunakan nama email tersebut sebagai username pada Sosial Media X. Lalu saya menemukan akun yang dicari seperti pada gambar dibawah ini.



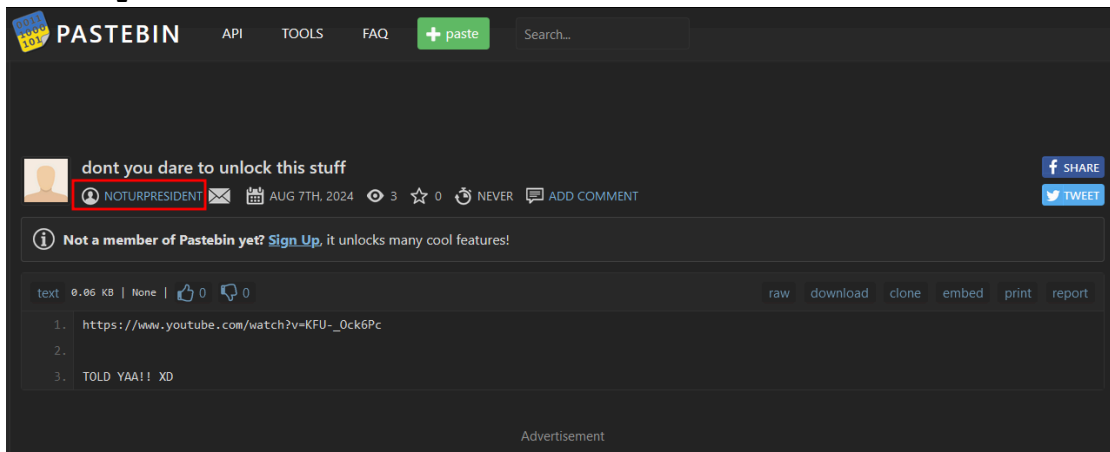
Terdapat sebuah link **pastebin** pada bio profil, yang ketika diakses ternyata terkunci dan harus dibuka menggunakan password seperti pada gambar dibawah ini.



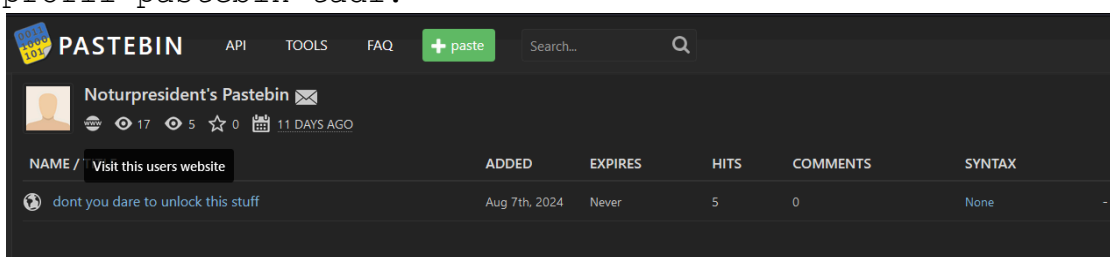
Lalu saya memiliki ide untuk melakukan analisa terhadap link pastebin tersebut menggunakan **"Wayback Machine"**, bisa dilihat pada gambar dibawah. Url Pastebin yang telah ditemukan sebelumnya sudah di Archive selama 2 kali dalam bulan agustus ini.



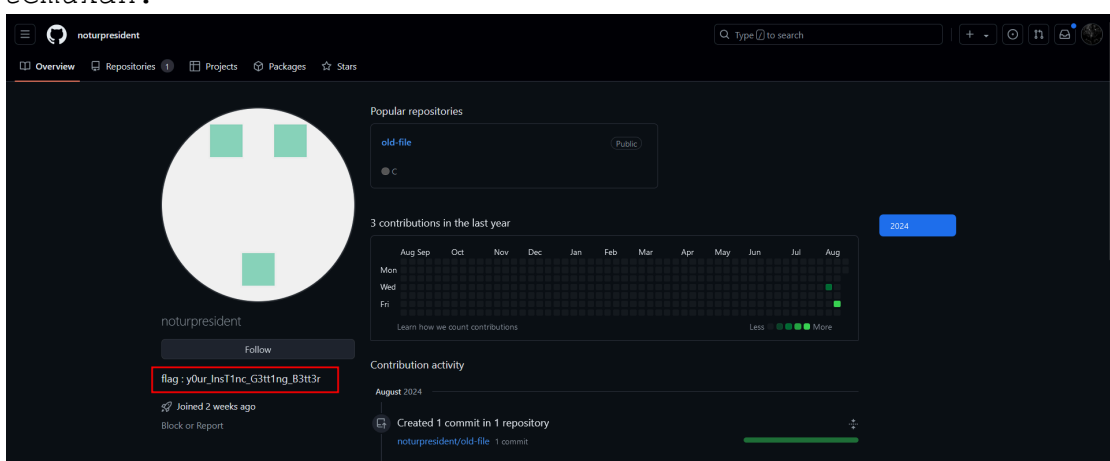
Ternyata setelah Archive pada tanggal 7 Agustus dibuka, Isinya adalah sebuah link yang mengarah ke platform youtube dan merupakan sebuah gocekan. Namun disini saya menjadi tau jika username pastebin nya adalah "noturpresident"



Setelah profil tersebut saya buka, saya mendapatkan sebuah link yang mengarah pada github yang berada pada profil pastebin tadi.



Lalu ketika akun github tersebut dibuka, flag pun telah temukan.



Flag:

0byteCTF{y0ur_Inst1nc_G3tt1ng_B3tt3r}