GrabThePhisher Lab

Scenario:

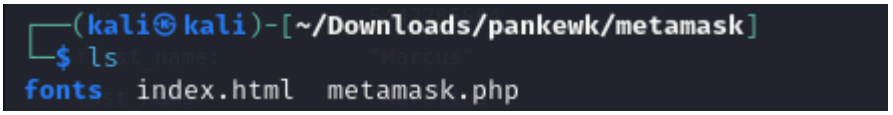
A decentralized finance (DeFi) platform recently reported multiple user complaints about **unauthorized fund withdrawals**. A **forensic review uncovered a phishing site impersonating the legitimate PancakeSwap exchange**, luring victims into entering their **wallet seed phrases**. The phishing kit was 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).**

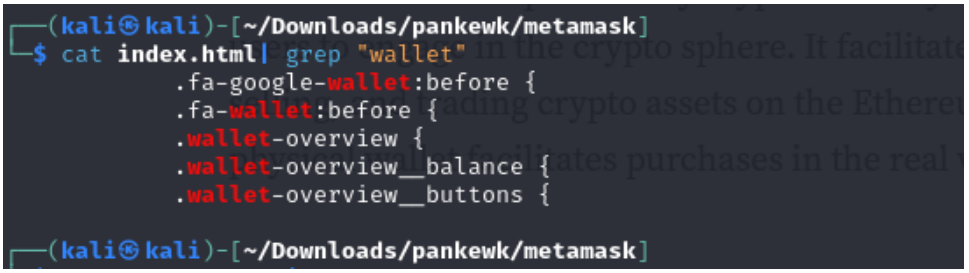
Given the nature of the attack, it was evident that the phishing attempt targeted cryptocurrency wallets. The presence of Metamask in the collected evidence suggested that it was the primary wallet used in this scam. Metamask is a well-known wallet that facilitates buying, exchanging, and selling cryptocurrencies, making it a prime target for phishing attacks.

Upon extracting the contents of the 95-GrabThePhisher.zip file, I found a folder named pankewk, which contained a directory labeled metamask.

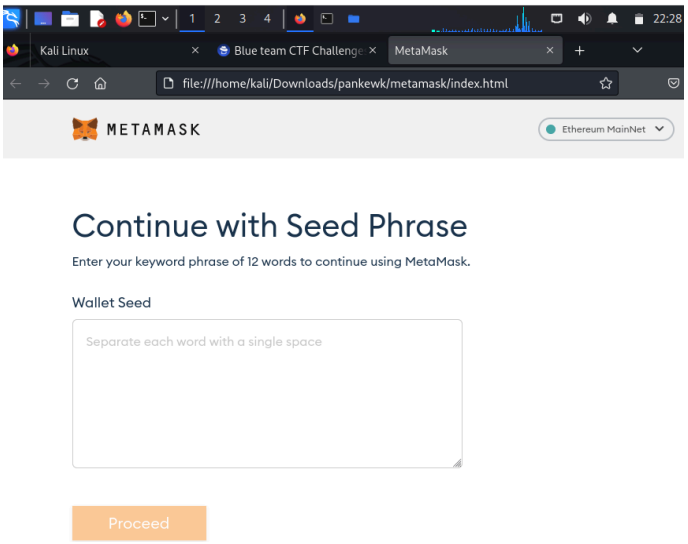
Filtering for the keyword wallet within this directory revealed three key files: metamask.php, index.html, and a fonts directory.



Using the pipe and grep command, I confirmed that the term wallet appeared in the index.html file. This indicated that Metamask was being used as the wallet for harvesting seed phrases.

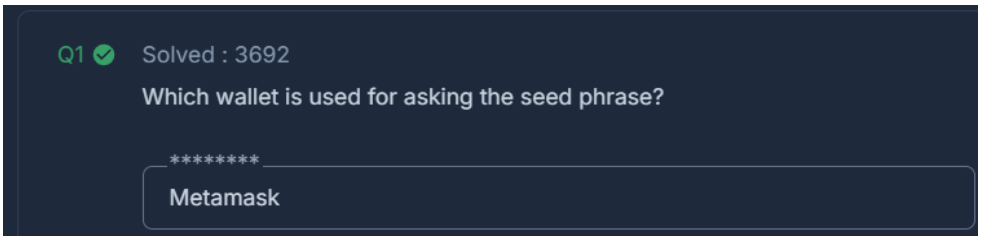


Opening **index.html** in a browser confirmed that the site prompted users to enter their seed phrases with the text: *"Continue with the Seed Phrase."* This confirmed that the phishing site was designed to harvest wallet credentials.

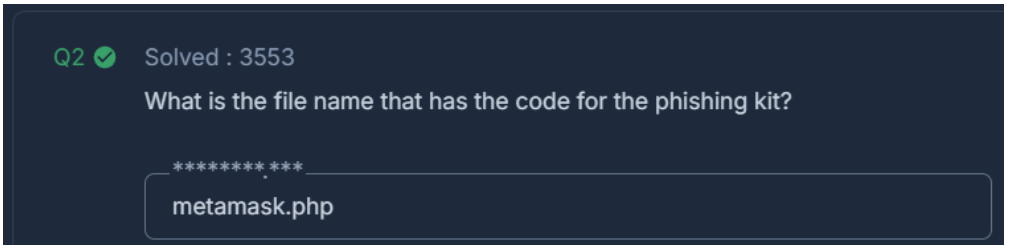


Q1. Which wallet is used for asking the seed phrase?

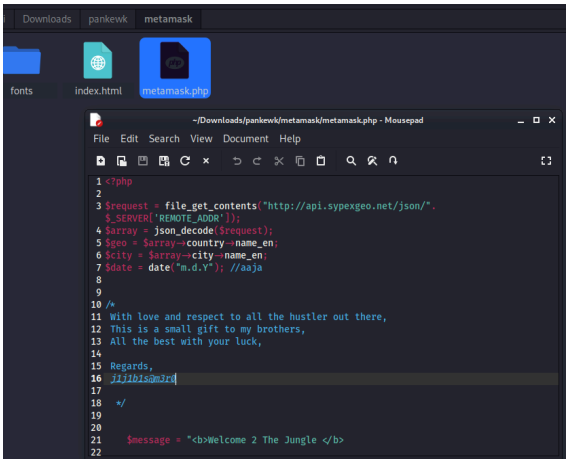
From the information gathered **Metamask,** was the wallet used for requesting seed phrases from victims.



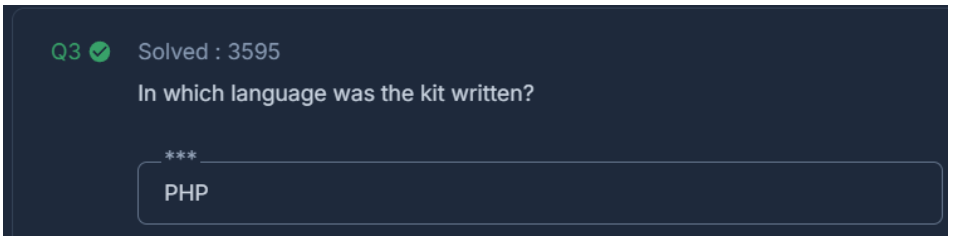
Q2. What is the file name that has the code for the phishing kit?



The **metamask.php** file contained the phishing kit's code. It was designed to redirect victims to the index.html page, making the site appear legitimate while secretly harvesting seed phrases.

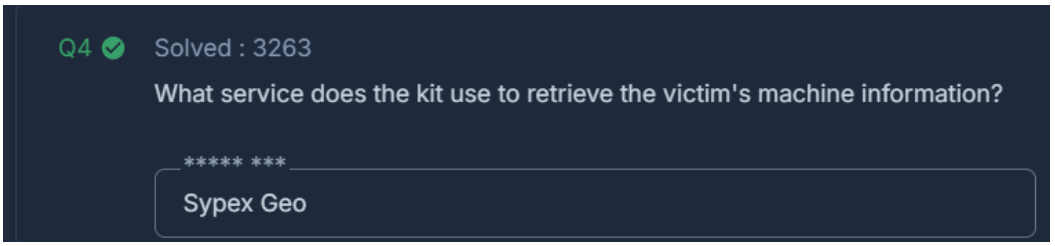


Q3. In which language was the kit written?

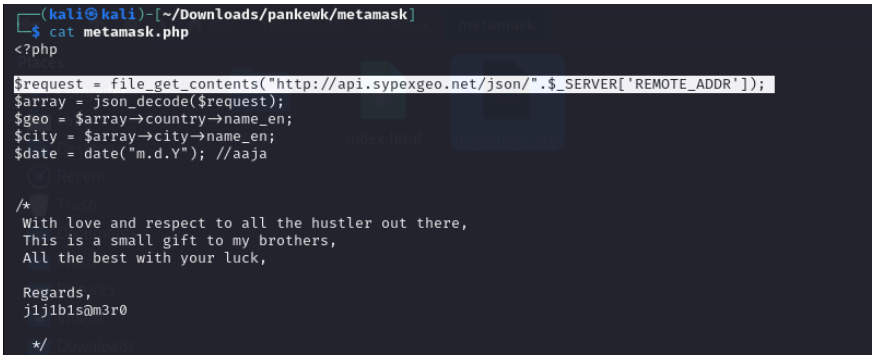


-PHP (Hypertext Preprocessor) is a scripting language used to create dynamic web pages. It's a popular, open-source language that's embedded in HTML

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

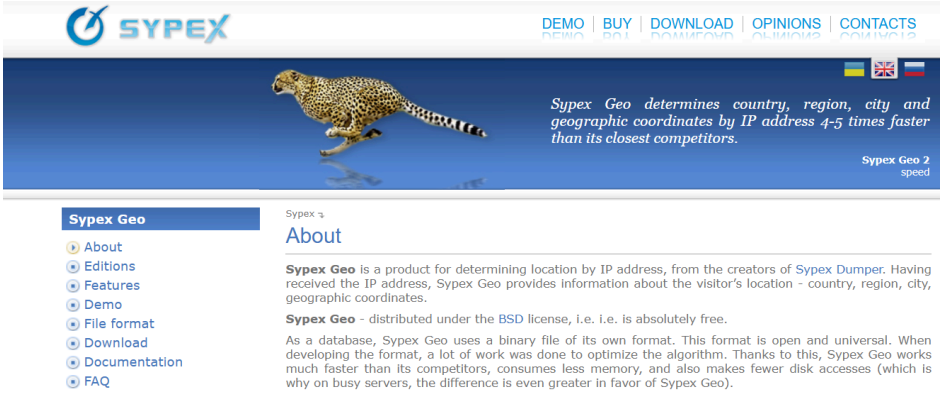


When you access the file metamask.php file you get to see the request of getting information content from the Sypex Geo

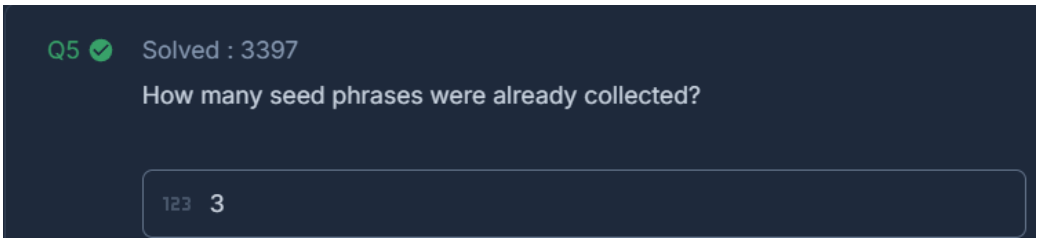


Upon doing information on it, one gets to see that Sypex Geo is a product for determining location by IP address, from the creators of Sypex Dumper. Having received the IP address, Sypex Geo provides information about the visitor's location - country, region, city, and geographic coordinates. Sypex Geo - distributed under the BSD license, is absolutely free.

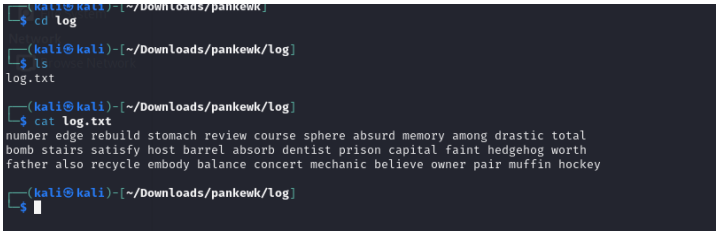
The attacker used the tool to get full information on the clients.

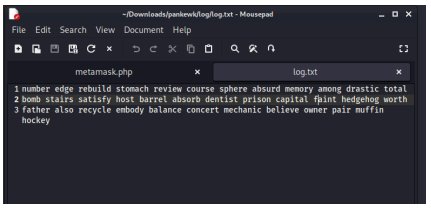


Q5. How many seed phrases were already collected?



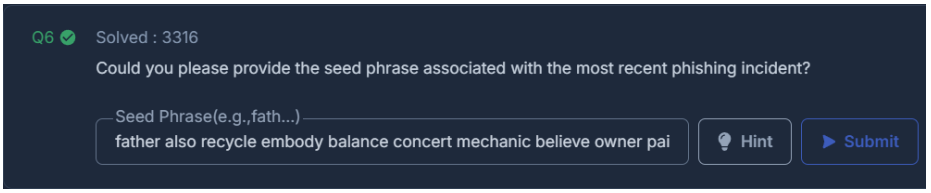
I went through the directory which was called “log”, I wanted to understand what kind of logs are inside the directory, inside the directory the was a file called the log.txt, which when you open it on the terminal you get to see three lines of phrases. I then searched on how many words are in the seed phrase from Metamask. Since a Metamask seed phrase consists of 12 words, this indicated that three victims had already been compromised.





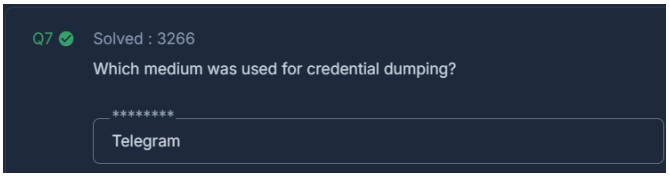
You can tell that the threat actors were so strategic in having a folder “log” that stores the seed phrase of the clients, from the oldest to the most recent.

Q6. Could you please provide the seed phrase associated with the most recent phishing incident?

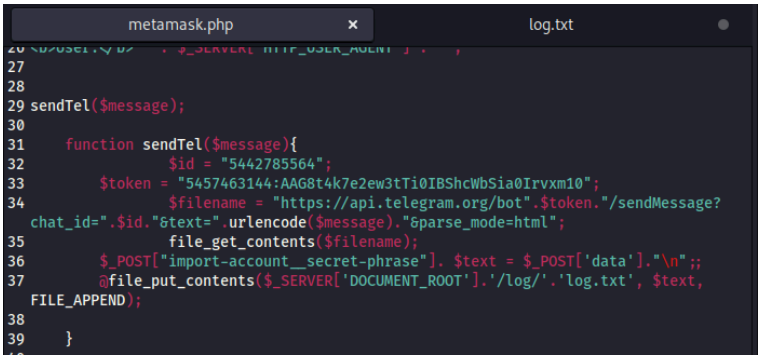


“father also recycle embody balance concert mechanic believe owner pair muffin hockey”

Q7. Which medium was used for credential dumping?

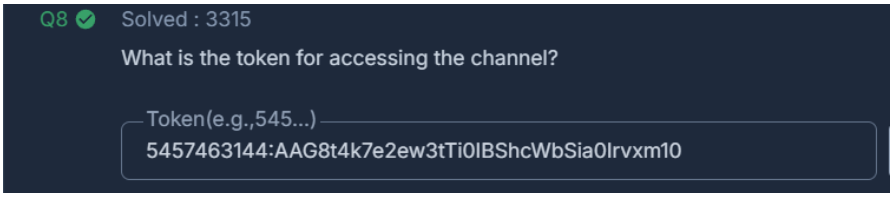


Get to know this also from the case study which said that 'the phishing kit was hosted on a compromised server and exfiltrated credentials **via a Telegram bot.** *This was confirmed in the metamask.php file, where the bot's command was present.*



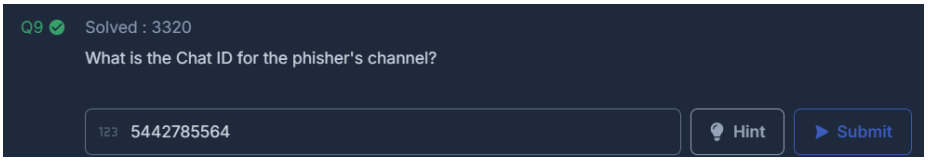
Q8. What is the token for accessing the channel?

'5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10' We get this information from the token on the command which was given



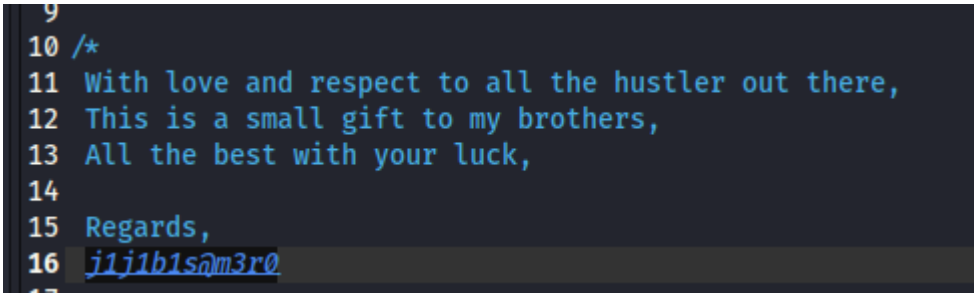
Q9. What is the Chat ID for the phisher's channel?

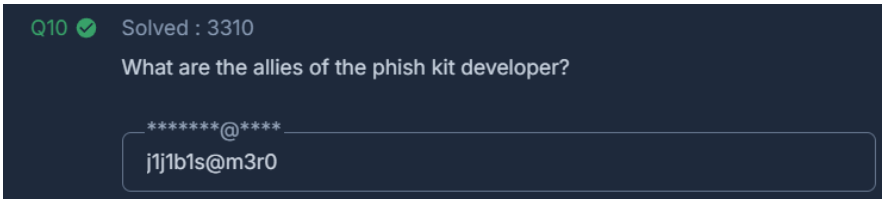
'5442785564' on the command line you get to see that it provides the ID number.



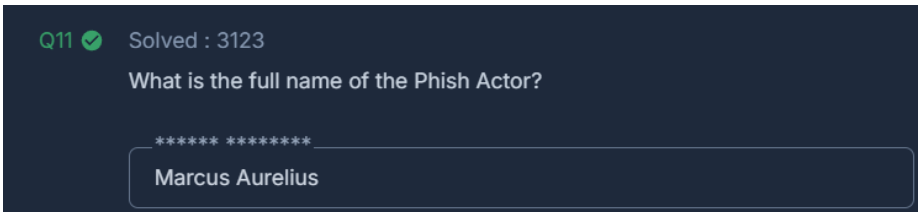
Q10.What are the allies of the phish kit developer?

j1j1b1s@m3r0. On the message that was sent, you get to see that the developer did send his/her "Regards"

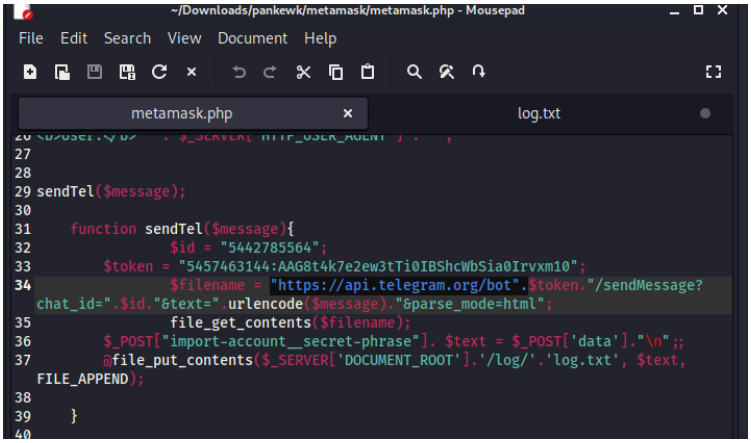




Q11. What is the full name of the Phish Actor?

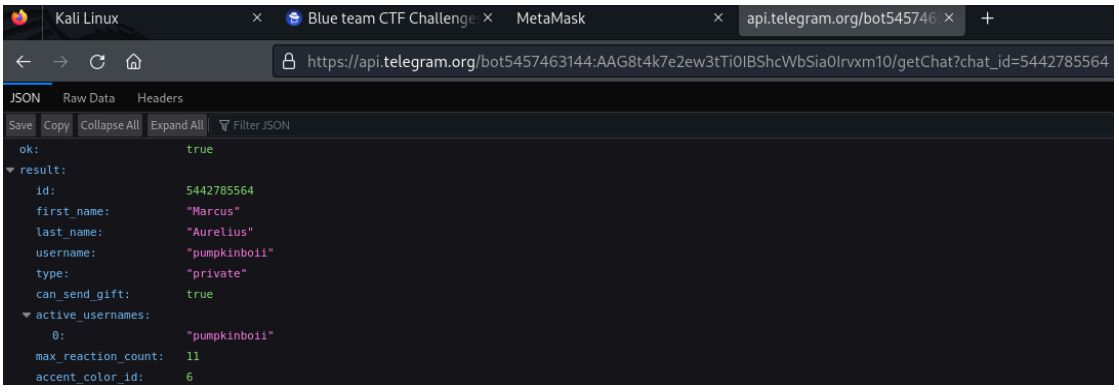


In the metamask.php file, the was a URL "https://api.telegram.org/bot"



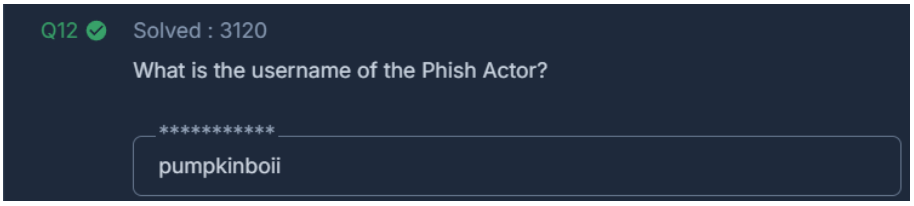
By analyzing the metamask.php file and following the Telegram bot's API URL, I gathered information on the actor responsible for the phishing attack. This led me to identify the individual.

"https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/getChat?chat_id=5442785564"



Q12. What is the username of the Phish Actor?

Pumpkinboii, as retrieved from the Telegram API response.



From the information gathered as a **Cyber Threat Intelligent** the breakdown of the attack vector**:**

1. **Phishing Tactic**
    - He impersonated PancakeSwap, a legitimate DeFi exchange.
    - Sent phishing emails to lure victims.
    - Used a fraudulent **Metamask login page** to steal seed phrases.
2. **Technical Implementation**
    - Embedded PHP scripts in `index.html`.
    - Used **Sypex Geo** to collect victims' IP addresses and geographical locations.
    - Logged seed phrases for unauthorized access to wallets.
3. **Flaws in His Attack**
    - The phishing email contained a **username**, which helped trace back to him.
    - The hosted site leaked information about him (name, last name, and username).
    - This flaw allowed further **OSINT (Open-Source Intelligence)** to uncover his real identity.

After analyzing Marcus Aurelius' phishing attack, it's clear that **awareness and preventive measures** are key to stopping such threats. To prevent future attacks, we need to **educate users, enforce security best practices, and strengthen defenses** against phishing attempts.

MetaMask already warns users:

-Never share your seed phrase—not even with MetaMask staff.
- If you lose your seed phrase, nobody can recover it for you. Store it securely.

Best Ways to Store a Seed Phrase Securely

- **Write it down** and keep it in a secure location.
- **Never store it digitally** (not in emails, notes, or screenshots).

This investigation was both fun and insightful, as it allowed me to think critically about cybersecurity threats and their solutions. By conducting an investigation, understanding the motives behind and security measures

Cybersecurity is an ongoing battle, but with the right approach, can reduce the risk and stop attackers like Marcus Aurelius from succeeding. Being aware of what is happening in the field, is also helpful. Thank You