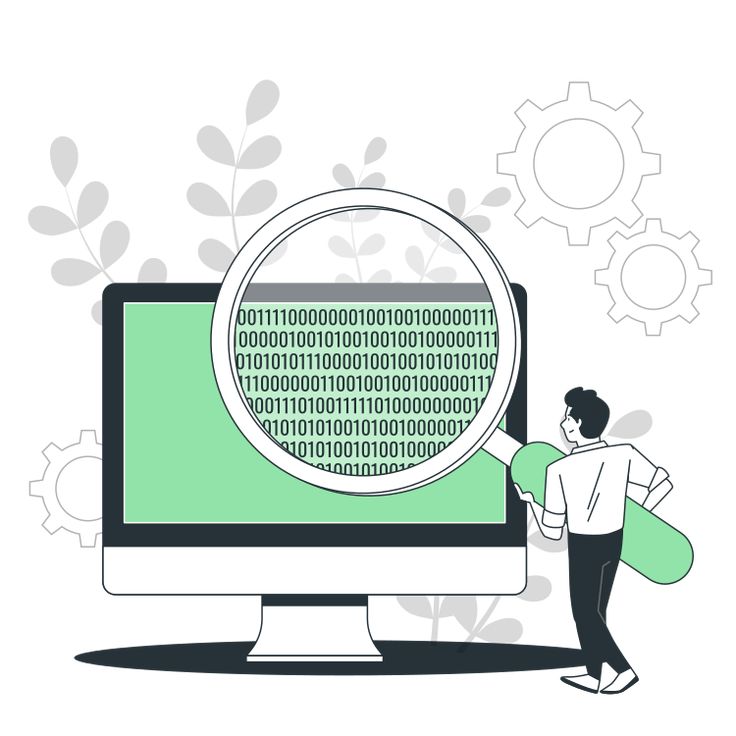
**CTF Topic: Malware Detection with Dr.Web Online Scanner**

A green shield with a spider logo

Description automatically generated

**Introduction**

****

Dr.Web Online Scanner is a tool for scanning files and URLs to detect malware and other security threats. In this challenge, you will use the provided scan result from Dr.Web to answer questions related to malware detection.

**Tools and Requirements**

To perform this CTF, you will need the following tools and resources:

* Virus file or .exe file
* Understanding of malware detection reports.

**Link**

File: <https://zippyshare.day/VK00N6ZstV6eq2K/file>

Website Link: <https://online.drweb.com/result2/>

**Scenario**

****

You are a cybersecurity analyst tasked with identifying and analyzing malware in a suspicious executable file. Your mission is to use Dr.Web Online Scanner to scan the provided file and answer specific questions based on the scan results.

**Process to Perform**

**Step 1: Open the Dr.Web Online Scanner**

* Go through this link: <https://online.drweb.com/result2/>

**Step 2: Upload the exe file and analyze the result.**

* For the file go through this link: <https://zippyshare.day/VK00N6ZstV6eq2K/file>
* Note down significant details such as the name of the detected malware, the MD5 hash of the file, the file size, and the scan result.

**Let's Begin the Challenge**

With the tools and techniques outlined above, let's dive into the challenge. Use the provided scan result to uncover details about the malware detection. Document each step you take and any findings along the way.

**Questions**

1. What is the name of the detected malware found in the scan?

Answer: Trojan.Encoder.11432

2. What is the MD5 hash of the infected file?

Answer: 84c82835a5d21bbcf75a61706d8ab549

3. What is the size of the infected file?

Answer: 3514368

4. What was the scan result for the file?

Answer: Infected

**Happy hunting!**

**Hint**

**A green and white text box

Description automatically generated**

**A screenshot of a computer error message

Description automatically generated**