## **Lab 5: Malware Detection**

### **Overview**

Since the invention of the computer, there have been viruses. And since the invention of viruses, there has been the need for antivirus software: your trusty friend who protects your computer. But how does antivirus software actually *detect* virus files?

In this lab, we will download (safe!) [EICAR Anti-Virus test files](https://en.wikipedia.org/wiki/EICAR_test_file) and explore whether they can be detected by local antivirus scanning software. Next, we’ll upload these files to the virus-detecting web service [VirusTotal](https://www.virustotal.com/) and inspect their signatures.

### **🎯 Goals**

By the end of this lab you will be able to...

* Understand basic antivirus and virus detection.
* Learn how to use VirusTotal and why it is useful.

### **Lab Outline**

#### **Part 1: Observing Virus Detection**

* Download anti-malware test files and test how antivirus responds.
* Upload the downloaded 'virus' files to VirusTotal.

#### **Part 2: Looking Under the Hood**

* Get an API key for VirusTotal.
* Use the VirusTotal CLI to make an API call to VirusTotal.
* Check if your created files are detected

### **Resources**

* [EICAR](https://www.eicar.org/download-anti-malware-testfile/)
* [VirusTotal CLI](https://github.com/VirusTotal/vt-cli)

## **Lab Instructions**

### **Part 1: Observing Virus Detection**

#### **Step 0: Antivirus check!**

Make sure that you have some form of antivirus installed on your machine. (If you don't have one, you can install any free antivirus (except Malwarebytes, it doesn't work for this lab) -- Just make sure you're downloading from an official website and not a third-party link.)

* Windows: [ESET](https://www.eset.com/ca/home/online-scanner/)
* Mac: [BitDefender Virus Scanner](https://apps.apple.com/app/bitdefender-virus-scanner/id500154009?mt=12)

For optimization reasons, popular antivirus tool Malwarebytes has chosen to [opt-out of detecting EICAR's testfiles](https://forums.malwarebytes.com/topic/191650-malwarebytes-3-frequently-asked-questions/?do=findComment&comment=1077438). Malwarebytes is still an excellent antivirus, but if it's what you use, you'll want to download an alternative option for this lab.

#### **Step 1: Observe (harmless) virus files**

Okay, let's get some (fake) viruses! Fortunately, the European Institute for Computer Antivirus Research (EICAR) has us covered with their [Anti Malware Testfile website](https://www.eicar.org/download-anti-malware-testfile/).

* Be sure to read the text on the download page thoroughly, as it contains important information!

Now it's time to get started:

* Download each of the 4 harmless antivirus test files to your own computer (not Kali).

There are 4 files for download to facilitate various scenarios:

1. eicar.com
2. eicar.com.txt (The same file as eicar.com, but named differently)
3. eicar\_com.zip (A zip containing eicar.com)
4. eicarcom2.zip (A zip containing a zip containing eicar.com)

🤔 Why do you think EICAR distributes the same file in four different ways?

Click here for an answer!

EICAR is checking to make sure your antivirus isn't fooled by easy tricks to hide the virus, such as:

* Renaming the file with a different extension (eicar.com.txt)
* Hiding the file inside a zip archive (eicar\_com.zip)
* Hiding the file inside MULTIPLE zip archives (eicarcom2.zip)

After you've downloaded the virus files, your antivirus might react automatically.

* If nothing pops up, open your antivirus program and run an antivirus scan.
* How did your computer respond to the viruses? Compare with others in the lab! Was it the same or different?

🤔 How do you think your antivirus is able to detect the EICAR files as "dangerous"?

🎯 **Checkpoint 1**: You should have downloaded the four EICAR files and seen your antivirus detect them.

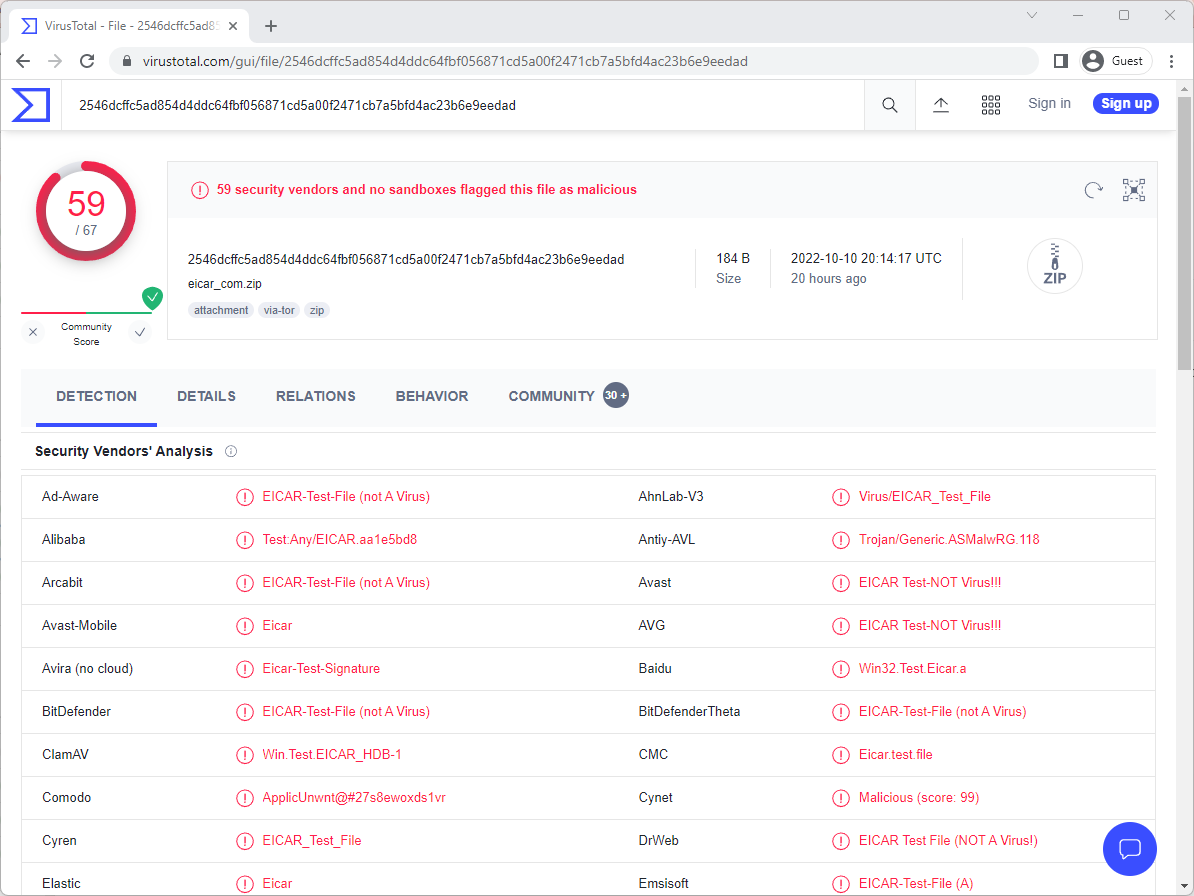
#### **Step 2: Upload these files to Virus Total**

In this next step,Next, we'll upload the files to a virus monitoring website to get more information on how they're detected.

* Go to [VirusTotal](https://www.virustotal.com/gui/home/upload) web page.
* Upload the files that you have created or downloaded from EICAR.

**VirusTotal** will analyze the file if it's suspicious. It will also automatically share the results with the security community. You can do this any time you have a file you're unsure of!

💡 TIP: If you can't upload the EICAR file, here's a screenshot of our results:



Feel free to play with VirusTotal. Try uploading some other files and see what their results show up as. What happens if you modify the existing file?

🎯 **Checkpoint 2**: VirusTotal lets you see whether an uploaded file is marked as malware by a particular anti-virus scanner once you upload it.

🎉 You've completed Part 1 of this lab! 🎉 With whatever time you have left, try to go as far as you can with Part 2!

### **Part 2: Looking Under the Hood**

APIs provide a powerful way to access remote data from within a terminal, script, or other computer program. For this lab's stretch features, we'll learn how to use the VirusTotal API to check out a file on our Kali box through the terminal. Along the way, we'll also learn a little more about *how* files are recognized using **file signatures**.

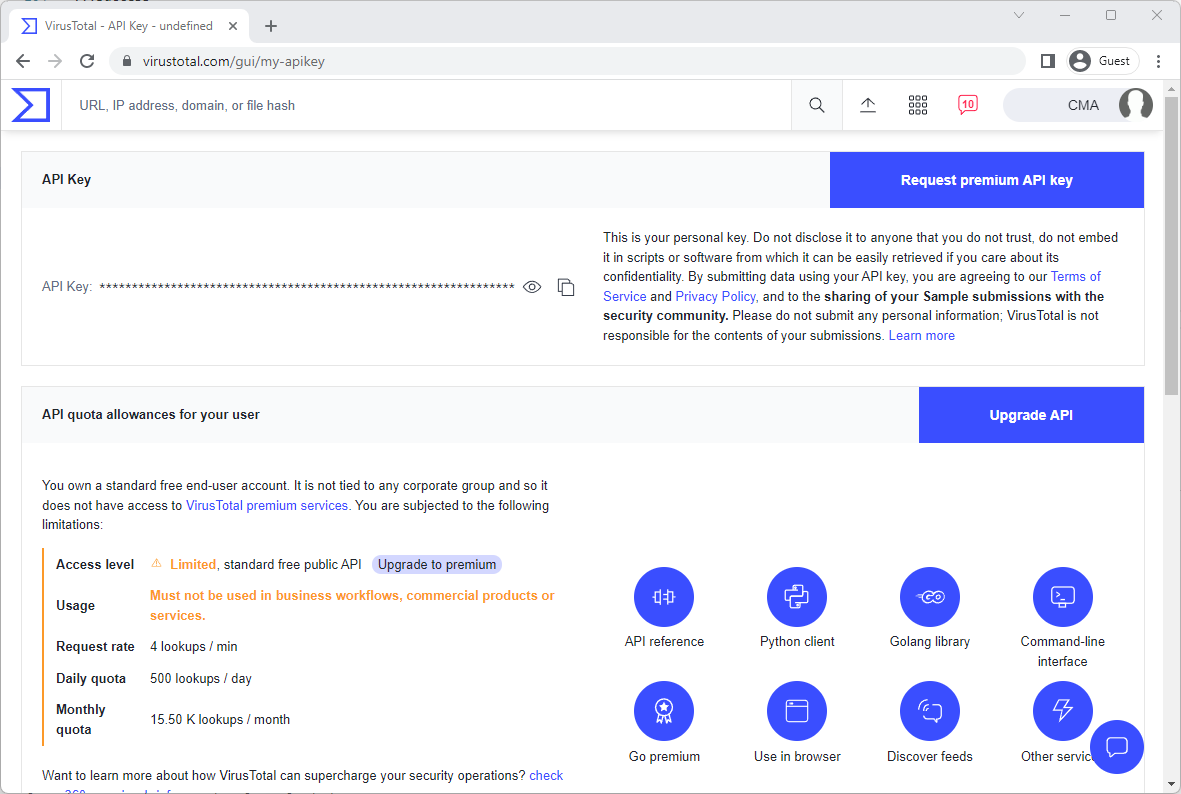
#### **Step 3: Get your API key for Virus Total.**

In this step, you will obtain your API key from VirusTotal site. Take note of your API key for this will be used in the following steps.

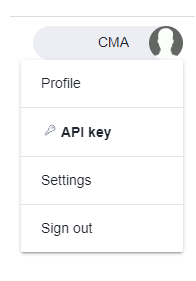
⚠️ Keep your API key secure at all times! Treat it like a password!

1. Go to the [VirusTotal](https://www.virustotal.com/gui/home/upload) website.
2. Either sign in or create a free account.
3. Once signed in, go to the [VirusTotal API key page](https://www.virustotal.com/gui/my-apikey) to access your key.

💡 HINT: The screenshot below shows what your VirusTotal API Key page should look like!



An alternative location of your VirusTotal API key can also be found in your account user menu!



🎯 **Checkpoint 3**: You should have a 🔑 to VirusTotal's API.

#### **Step 4: Install the VirusTotal CLI**

In this step, you will install the [vt-cli](https://github.com/VirusTotal/vt-cli#virustotal-cli) tool in your Kali VM. In the following steps, you will download the vt-cli source code and compile it yourself:

* Sign into your Kali VM (either via SSH, or RDP and open a terminal)
* Clone vt-cli from github:
  + git clone https://github.com/VirusTotal/vt-cli
* After cloning the project, we need to **c**hange **d**irectory into the vt-cli directory.
  + cd vt-cli
* Install the required language library:
  + sudo apt install golang
* Next, we'll compile and build the project.
  + make install

At this point, vt-cli is installed. But if you run a command like vt init, you'll get a "command not found" error. So the next step is to let the terminal know *where* to find the vt program. Fortunately, VirusTotal provides us the commands we need:

* Run the following commands:
  + export GOBIN=`go env GOPATH`/bin
  + export PATH=$PATH:$GOBIN

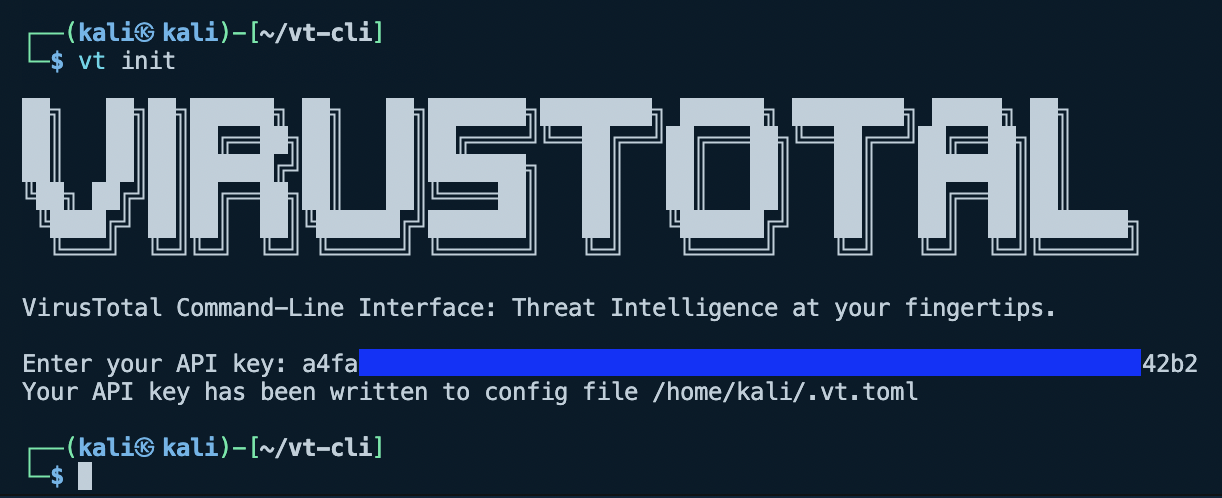
#### **Step 5: Configure vt-cli tool with your API key**

Once you have installed vt-cli in your machine, configure the vt-cli tool with your API key:

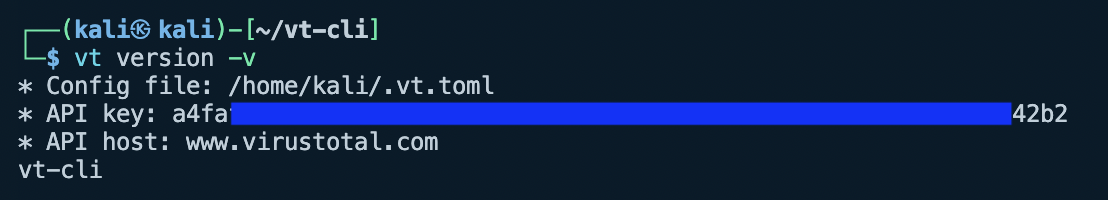
* Run the following command:
  + vt init
* Paste in your api key when prompted

VirusTotal will save your key for future use. If you're curious, you can find this config in your home directory (~) in a file called .vt.toml.

💡 HINT: Click here for an example of vt-cli configuration!



🎯 **Checkpoint 4**: If you run the vt version -v command, you should see the following:



#### **Step 6: Get your file's signature**

It's time to reveal the trick that *most* antivirus software uses to recognize viruses... file signatures. File signatures work using a [cryptographic hashing function](https://en.wikipedia.org/wiki/Cryptographic_hash_function), which is a fancy piece of math that assigns every input a *distinct* but *predictable* output -- usually called a **hash**.

What does that mean?

* **Distinct** means that no two **different** files will produce the same **hash**.
* **Predictable** means the same file will **always** produce the same **hash**.

We can try it out with a command in kali: sha1sum.

* Try using ls to list the files in your current directory, then use sha1sum <filename> to see the SHA1 hash for that given file.
* If you want, try creating some different text files and calculating their hash. Changing even one letter will change the result!

Okay, so now let's get the signature for the EICAR testfiles.

* Using the [wget](https://en.wikipedia.org/wiki/Wget) command, download the EICAR testfiles to Kali:
  + cd ~ (Go back to your home directory)
  + wget https://secure.eicar.org/eicar.com
  + wget https://secure.eicar.org/eicar.com.txt
  + wget https://secure.eicar.org/eicar\_com.zip
  + wget https://secure.eicar.org/eicarcom2.zip
  + *(If these commands don't work correctly, you can always RDP and open a web browser, then download from the EICAR website as you did in Part 1 -- but it's often easier to just use wget for quick file downloads!)*
* Next, use sha1sum to get the hash of each file.
  + Which ones are the same? Which are different?

🎯 **Checkpoint 5**: You should be able to see the hashes for each of the four EICAR testfiles.

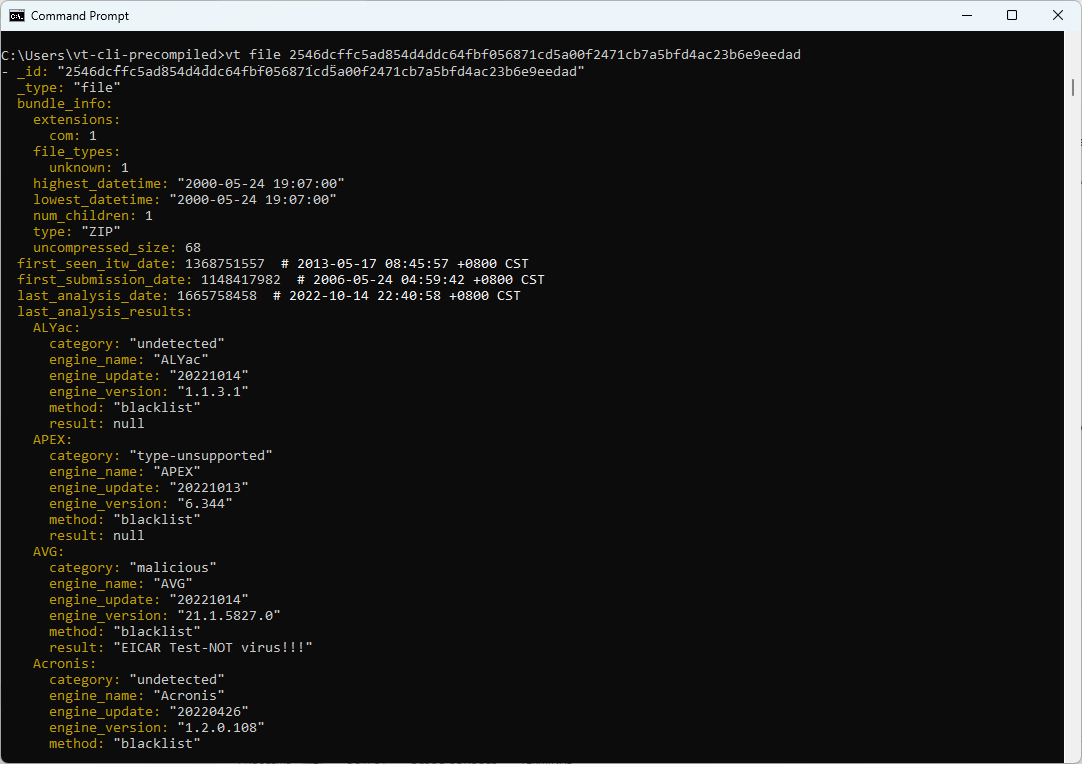
💡 HINT: Stuck? Click here to see an example of using sha1sum to get hashes!

Screenshot on how to get the hash of a file

#### **Step 7: Check if file is malicious using vt-cli**

All right, so now let's see if EICAR recognizes these files. To poll the EICAR database, we have to give it a way to look up the file... You guessed it, it's the file's hash.

* Use the vt file <File Hash Value> command to check each of your files!



Now the picture is coming together... VirusTotal doesn't store actual *malware files* (that would be a bad idea), but instead it stores the ***hashes*** of malware files. That allows users to check if their file is a virus by comparing its hash with those in the database. In the future, if you download something you're uncertain of, consider using VirusTotal to check it out!

🎉 Congratulations 🎉

You've completed this lab!