I Love Python :)

written by Mert SARICA | 25 March 2010

I, like many ethical hackers, have been busy with the C programming language for years, have examined a lot of source code, have written many programs, and have often thought, “I’m glad I learned C programming language” because whenever I look at source code written in another programming language, I can easily understand it and it has always been beneficial to me.

I spent many years working with the C programming language, examining and writing many source codes and often thinking, “I’m glad I learned C programming because whenever I look at source code written in other languages, I can easily understand it.” Over time, the transition of exploitation tools from C to Python increased my interest in Python. One day, I decided to take the plunge and enter the world of Python. Whenever I need a program for security testing, I realize how good a decision it was because the time it takes to go from needing the program to coding and using it ranges from an average of 1-2 days to a minimum of 15 minutes, depending on the complexity of the program.

If I tried to write these programs in C, I would have to write and spend twice as much time on code. But thank goodness for Python. Here are the powerful aspects of Python:

- You don’t have to worry much about syntax, { } ( ) ;
- You don’t have to spend 100 hours compiling. Just code, and execute.
- It comes with bunches of modules, import, and call the function.
- Your code is more readable and efficient for code reuse.
- It’s platform-independent; code it in Windows, test it in Linux, and use it on Mac.
- You don’t have to worry about data types like in other languages, “1” + “1” = “11”, 1 + 1 = 2

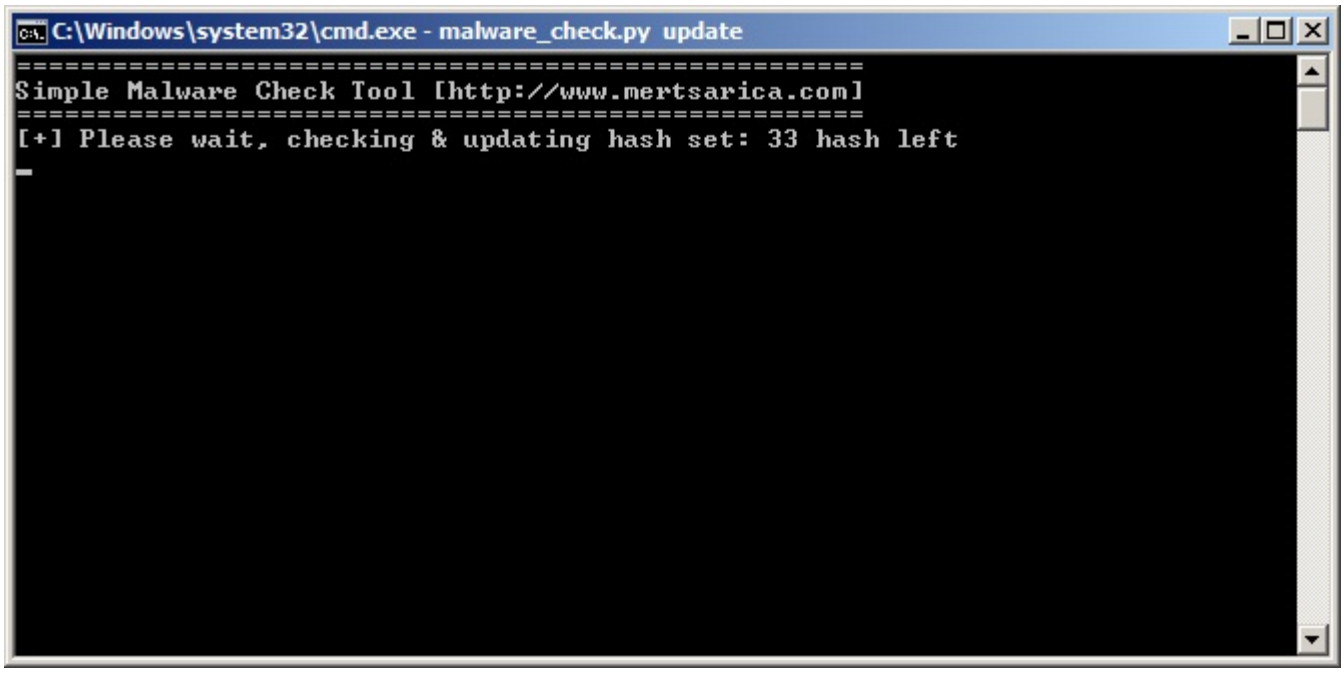
Whether for daily tasks or when I’m bored and thinking, “I wonder if I could write a program that would be beneficial to the community,” I can quickly develop a program. If you want to enter the world of Python, I strongly recommend watching the videos of the Python lessons given to Google’s own employees.

While bored, I thought that if I write a program with Python that goes to the

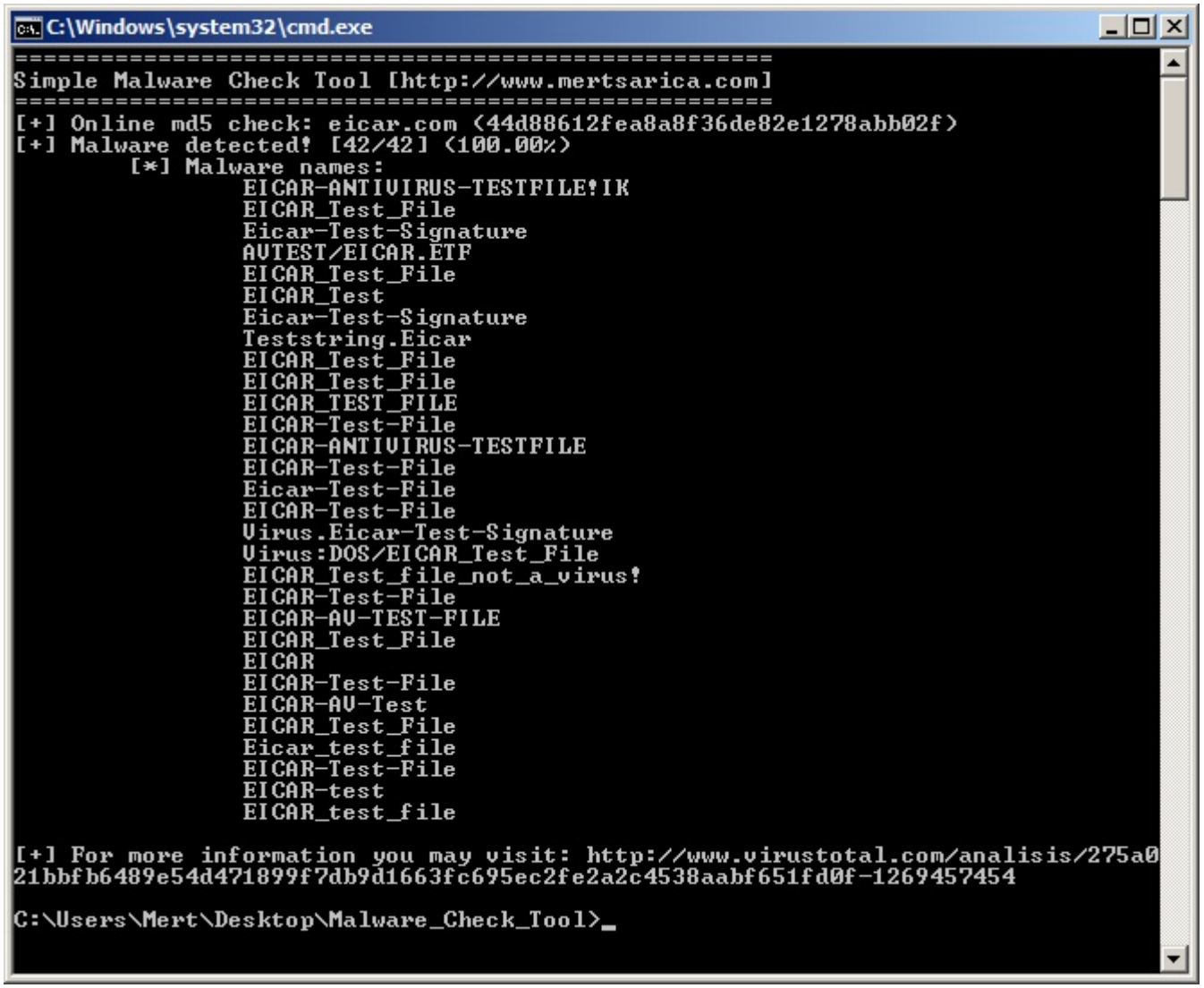
Avira's website and collects the md5 hash information of all the listed malicious files and records it in a file, takes the md5 hash of any file on my disk, and determines whether it has harmful content with this hash set. In addition, it even goes further to send the obtained md5 hash to the Virustotal site and show the result, and it also has the feature to update the Avira hash set. I thought that developing such kind of a tool would be beneficial for the community, so, the Malware Check Tool application, which includes proxy support, came out.

The usage of the program is quite simple, it works with 3 commands: online, offline, and update.

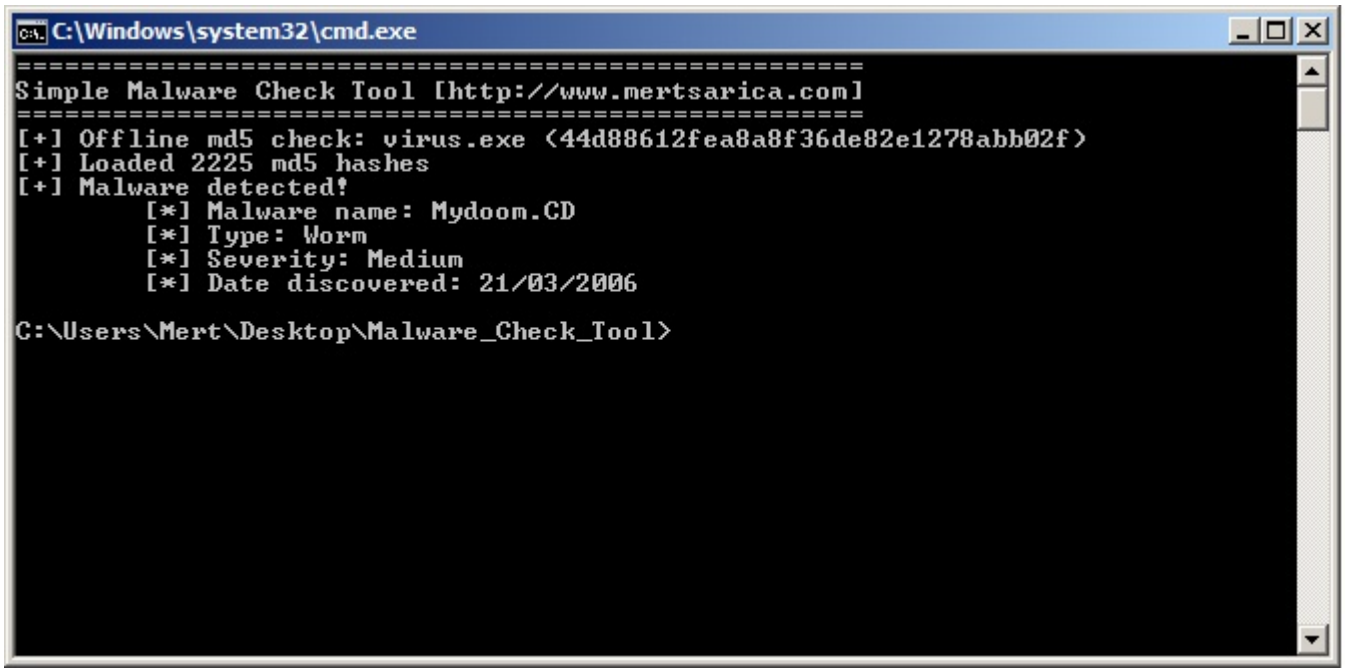
The update command (e.g. malware_check.py update) updates the hash set used by the program to detect malicious content to the latest version by visiting the Avira website.



The online command (e.g. malware_check.py online eicar.com) runs the program and sends the md5 hash of the file you specified to the Virustotal site, showing you the result.



The offline command (e.g., malware_check.py offline virus.exe) runs the program and searches the specified file's md5 hash in the hash set stored in the local disk, showing you the result.



I also added an http proxy feature to the program. To set the proxy settings, you need to modify the following part inside the malware_check.py file.

```
proxy_info = {
‘user’ : ‘test’, # proxy username
‘pass’ : ‘test’, # proxy password
‘host’ : “127.0.0.1”, # proxy host (leave it empty if no proxy is in use)
‘port’ : 8080 # proxy port
}
```

This is all from me for this week. You can access the Malware Check program from here. Have a good weekend everyone…