Simple Malware Check Tool v1.2 Released!

written by Mert SARICA | 5 September 2010

I released the first version of the program on March 25 and notified several information security related sites and Darknet was one of them. At that time Darknet did not make any news but suddenly in last week, they changed their decision and made a news about a 6 months old software. It was old and got broken (online check was broken due to changes in Virustotal's site) in 6 months and I did not have chance to fix bugs in a time. Recently massive download attempts forced me to fix bugs and release a new version.

Today I have released v1.2 which includes bug fixes. I highly recommend you to download and run the latest version.

Download Malware Check Tool v1.2

——————————————————————————————-

ABOUT

——

This program intends to detect a malicious file in two ways; online and offline.
It calculates the md5 hash of a specified file and searches it in its current hash set (offline) or on virustotal site (online) and show the result.
It has http proxy support and update (for hash set) feature.
Coded for fun so enjoy it :)

CHANGELOG

———

v1.2 – New Virustotal changes implemented.
v1.1 – Wrong implementation of md5 calculation fixed. (Credit goes to roynal [.] smith [@] gmail [.] com)

USAGE

——

python malware_check.py update

- This command updates its current hash set (hashset.txt) by crawling threat information from http://www.avira.ro
- Hashset.txt includes virus name, virus type, md5 hash of the virus, severity and discovered date.
- If there is no hashset.txt file, it will visit http://www.avira.ro and start gathering virus name,vvirus type, virus md5, severity and discovered date
- If there is a hashset.txt it just up to date its current hash set to the latest.

```
python malware_check.py online malware.exe
```

- This command calculates the md5 hash of a specified file (ex: malware.exe), submits it to http://www.virustotal.com and then shows the result.

```
python malware_check.py offline malware.exe
```

- This command takes the md5 hash of the specified file (ex: malware.exe) and searches it in its current hash set (hashset.txt) and then shows the result.

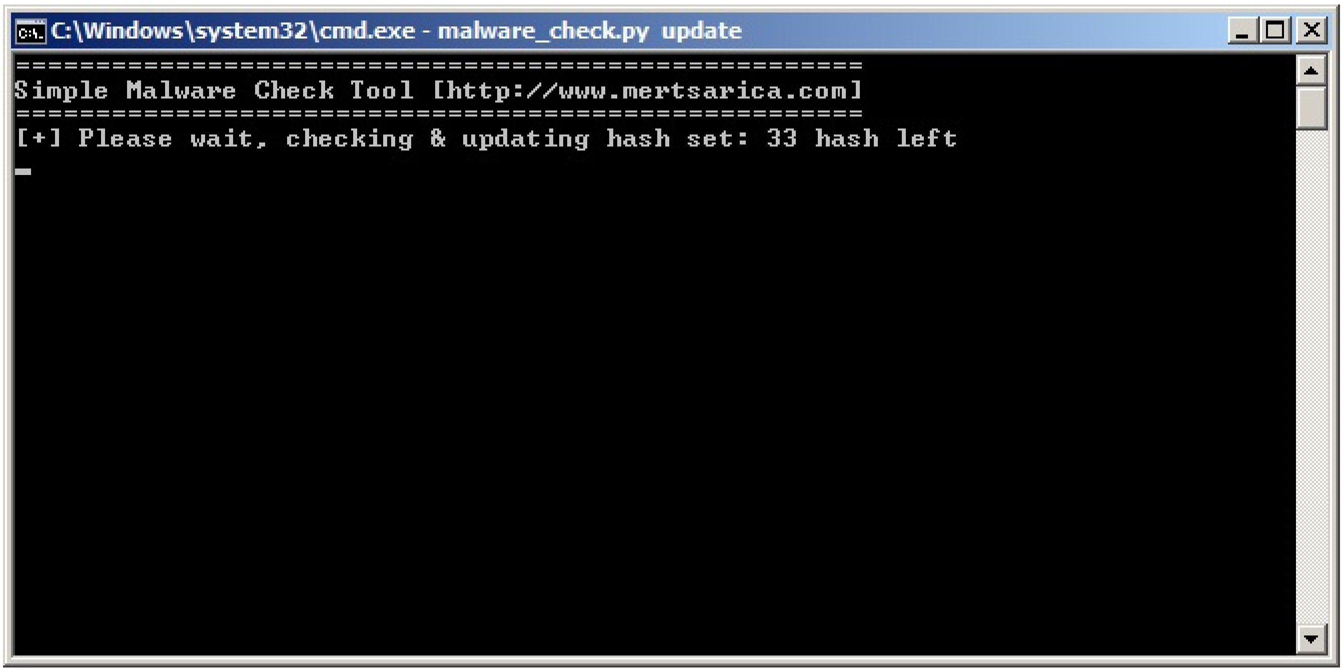
Note: For http proxy support you have to edit malware_check.py and modify the required fields as shown below.

```
proxy_info = {
‘user’ : ‘username’, # proxy username
‘pass’ : ‘password’, # proxy password
‘host’ : “proxy host”, # proxy host
‘port’ : 8080 # proxy port
}
```

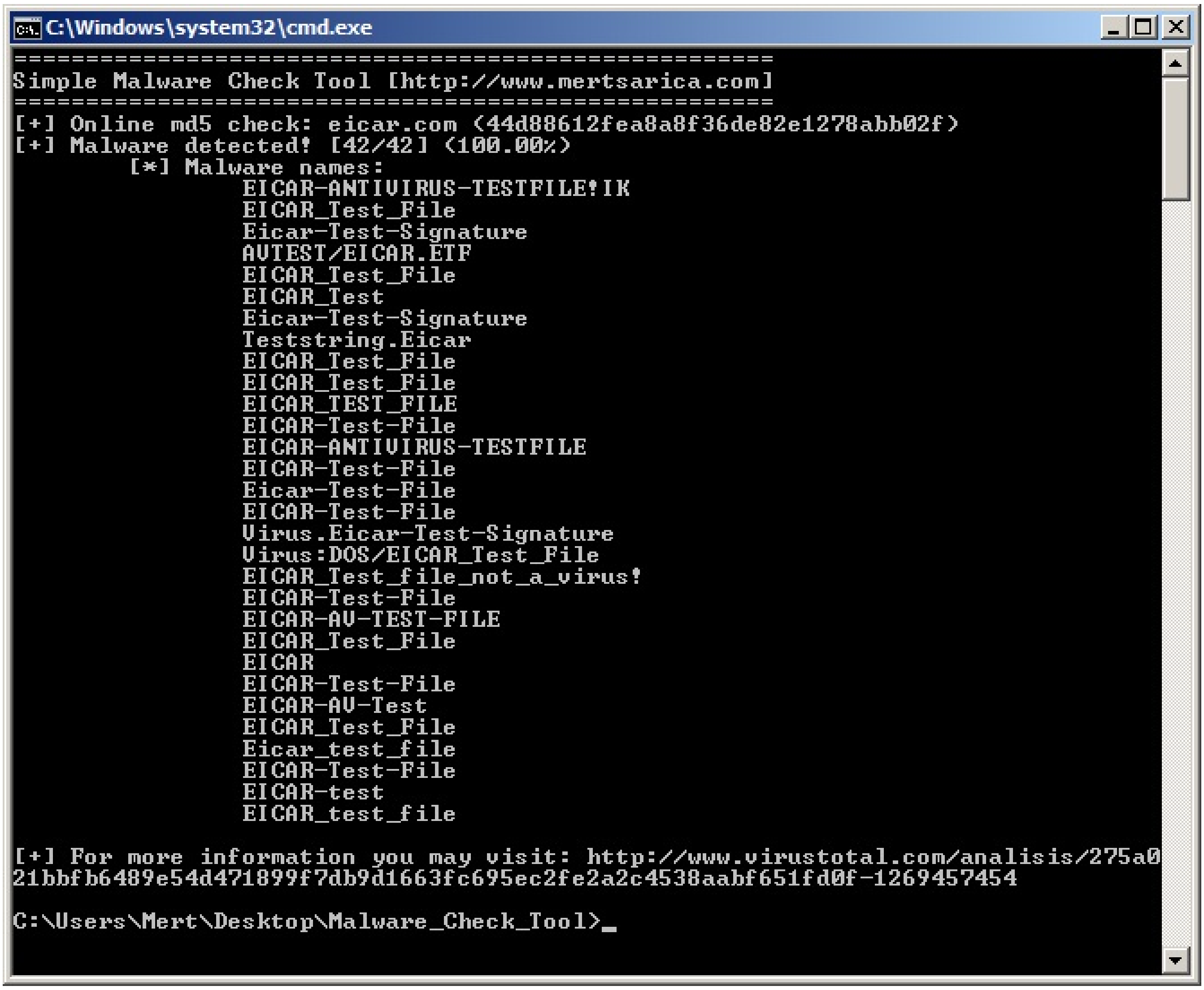
CONTACT
——-

Author: Mert SARICA
Email: mert [.] sarica [@] gmail [.] com
URL: http://www.mertsarica.com

SCREENSHOTS
———–



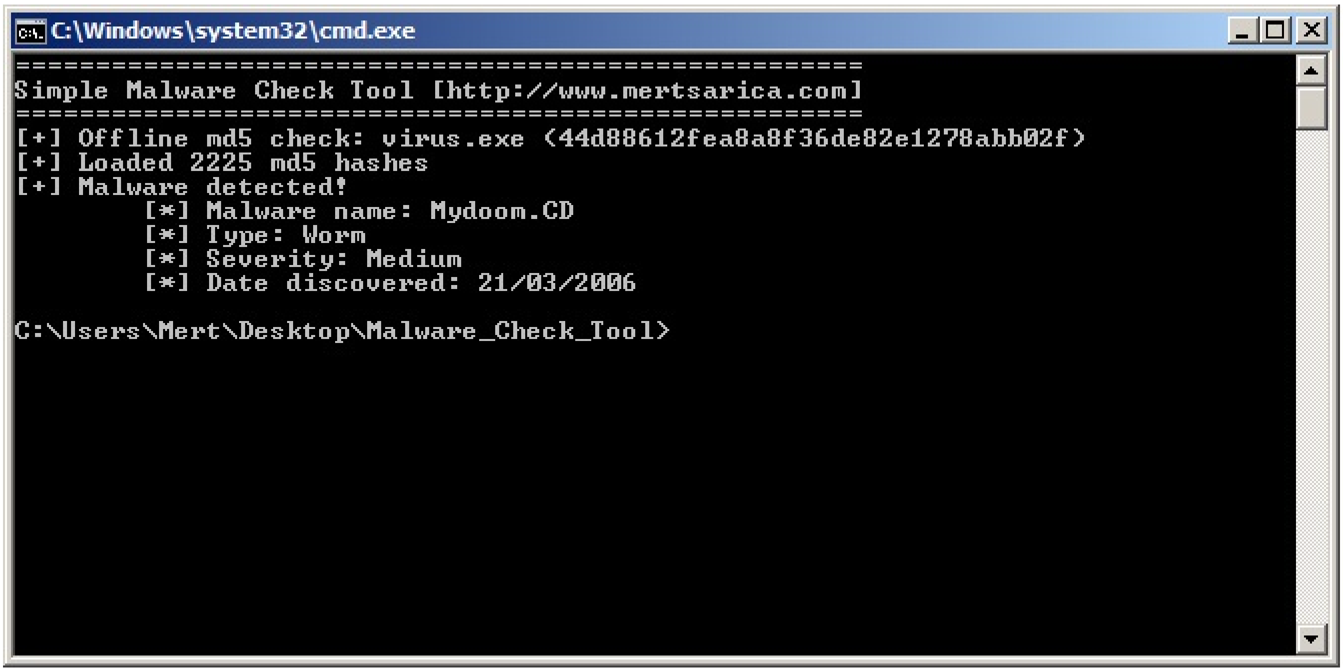
```
=====================================================
Simple Malware Check Tool [http://www.mertsarica.com]
=====================================================
[+] Please wait, checking & updating hash set: 33 hash left
_
```



```
=====================================================
Simple Malware Check Tool [http://www.mertsarica.com]
=====================================================
[+] Online md5 check: eicar.com (44d88612fea8a8f36de82e1278abb02f)
[+] Malware detected! [42/42] (100.00%)
        [*] Malware names:
                EICAR-ANTIVIRUS-TESTFILE!IK
                EICAR_Test_File
                Eicar-Test-Signature
                AVTEST/EICAR.ETF
                EICAR_Test_File
                EICAR_Test
                Eicar-Test-Signature
                Teststring.Eicar
                EICAR_Test_File
                EICAR_Test_File
                EICAR_TEST_FILE
                EICAR-Test-File
                EICAR-ANTIVIRUS-TESTFILE
                EICAR-Test-File
                Eicar-Test-File
                EICAR-Test-File
                Virus.Eicar-Test-Signature
                Virus:DOS/EICAR_Test_File
                EICAR_Test_file_not_a_virus!
                EICAR-Test-File
                EICAR-AV-TEST-FILE
                EICAR_Test_File
                EICAR
                EICAR-Test-File
                EICAR-AV-Test
                EICAR_Test_File
                Eicar_test_file
                EICAR-Test-File
                EICAR-test
                EICAR_test_file

[+] For more information you may visit: http://www.virustotal.com/analisis/275a0
21bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f-1269457454

C:\Users\Mert\Desktop\Malware_Check_Tool>_
```



```
=======================================================
Simple Malware Check Tool [http://www.mertsarica.com]
=======================================================
[+] Offline md5 check: virus.exe (44d88612fea8a8f36de82e1278abb02f)
[+] Loaded 2225 md5 hashes
[+] Malware detected!
        [*] Malware name: Mydoom.CD
        [*] Type: Worm
        [*] Severity: Medium
        [*] Date discovered: 21/03/2006

C:\Users\Mert\Desktop\Malware_Check_Tool>
```