ARTICLE TITLE

DETECTING MALWARE / KEYLOGGER THROUGH NETSTAT AND TCPVIEW

INTRODUCTION:

Internet is widely used network all over the world. Although, it is beneficial in many aspects, but, there is always a risk of the malicious activities and virus attacks because the internet is not fully secure and we are surrounded by these malwares from all of the directions. These malwares or keylogger attacks can affect our work files locally as well. To detect and terminate these viruses, malwares and keyloggers locally from our PCs files, there are the two simple tools and methods. The one of them is “Netstat technique” i.e. the malware or keylogger within any file is detected through the command prompt interface or CLI. The another one is ”TCPview Technique” i.e. A platform that uses User Interface to detect the malware or keylogger that may exist in our files locally within the hard drive.

What Is Malware?

Malware is one of the very popular terms in the globe of machine technology. It can be defined as, “*The collective name for a variety of malicious softwares that are originated for the purpose of damaging the data and information stored in a certain computational equipment, and attaining an unlawful and unauthorized access to these computer machines*.”

Malwares includes many well-known names that describe different ways of causing harm to the computer machines. These include, spywares, Trojan horse, keyloggers, ransomware, cyber-attacks and many other ferocious viruses that could easily cause destructions in the security and the data of a computer machine.

What Is Keylogger?

The word “Keylogger” is used in the sense of *keystroke logging* or *keyboard capturing*. It refers to a software program that is used to hack and track the keyboard activities that are performed by a computer user. It captures and records the keyboard tasks and

stores these keystrokes in a particular file which is accessed by the hacker directly or even through emails.

Keyloggers can be considered as one of the most desperate malwares in the computational world, as the user hasn't any idea that this malicious activity is running in the background of his tasks. Thus, results in the clever hacking of the data and harming the security by getting an easy access to the credentials generated by a user through the keyboard.

The Netstat Technique:

Defining Netstat:

Netstat is a network based interrupt detection approach. It comes built-in with the installation of Windows as well as Linux operating systems. This tool is basically used to examine and explore the established connections on the TCP networks. It can also display Network protocol statics, process IDs, port numbers, Number of Network Interfaces, etc. All of the process of retrieving information about the TCP networks, detecting malware, and killing the keyloggers is carried out through the commands which we have to run on the command prompt.

Netstat Commands to Detect Malware / Keylogger:

The commands that are utilized for the purpose of detecting and killing the malware and keylogger are briefly described as under:

- **netstat ? –** This command shows the options by which we can analyze different information.
- **netstat –a:** This command reveals the connections of TCP that are Active and also listening ports. This helps in knowing that our system is connected to which IPs.
- **netstat –b:** Through this command, we can display names of the applications that create connections as well as their IPs. It also reveals the protocols of these IPs.

- **netstat –bno:** This command shows the names of the applications, their IPs, and process ID together.

- **taskkill /pid "PID" /F:** This command terminates the process (that may contain any malware) through its process ID (PID).

Advantages of Netstat:

- It is a very helpful tool to display the current network and internet connections on the PC.

- It provides the count of non-unicast and byte-unicast packets.

- It can repudiate errors, malwares and the unknown protocols that might effect the PC.

- It can re-display selected statistics in the regular intervals of time.

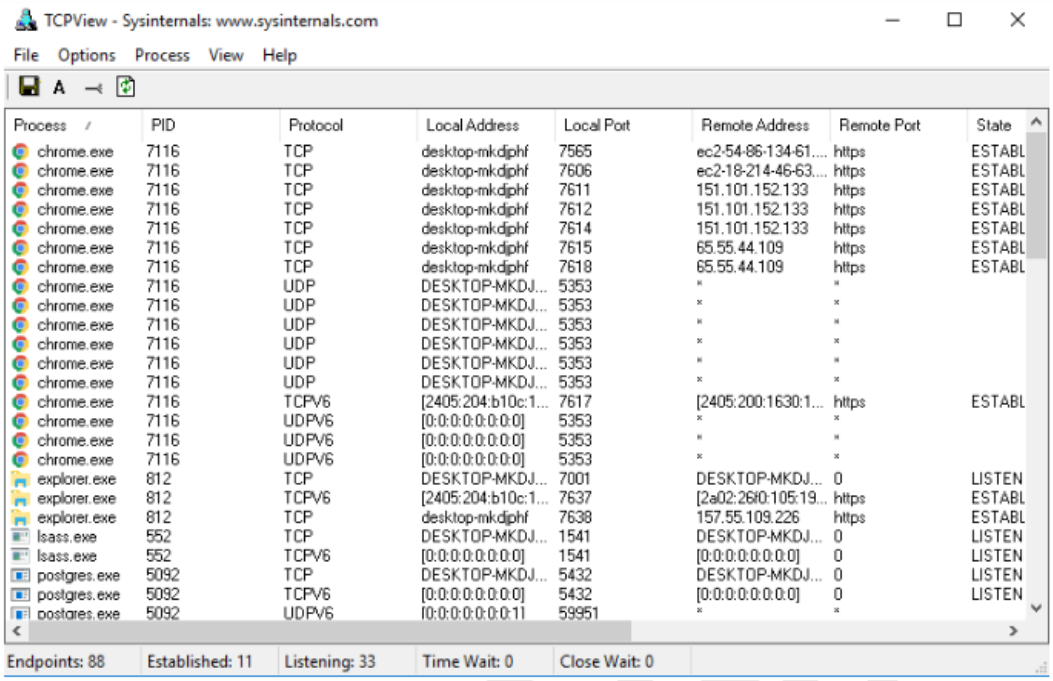
- It comes built-in with the Windows as well as the Linux Operating Systems.

The TCPview Technique:

Defining TCPview:

TCPview is a Windows program that displays a comprehensive listing of all the TCP and UDP endpoints on the PC, which include the remote as well as the local addresses and the state of TCP connections. This tool contains GUI for the user to execute and manipulate the functions easily. This makes it user-friendly as there is not a need to type the commands and instructions on this platform for the process of the detection as well as the termination of the malware or the keylogger files and even the false and harmful IP Addresses. Any changes that occur in network connections are shown in color. A change in state is shown in yellow; a closed connection, in red; new connections, in green.

The framework of the TCPview software looks like:



Methodology of TCPview:

As the program displays applications that are in the running mode, their IP Addresses, protocols, ports and also the data packets that are being sent or received by them, If we observe any of the processes as doubtful or uncertain and it may be sending our data packets to another anonymous port, We have to simply just right click on that process and then click on "End process". As soon as we click the "End process" option, the process terminates, thus, we protect our data as well as our PC from the malicious and keylogger attack.

Advantages of TCPview:

- The most important and speakable advantage of the TCPview software is that it has a user-friendly environment.
- Another advantage of TCPview is that the user doesn't have to type any command for its usage, just click and go system.
- TCPview facilitates admin a concise and informative way to observe and track the network endpoints and the processes.

CONCLUSION:

These applications (Netstat and TCPview) are very beneficial and productive to take care of our systems in order to prevent them from malwares, keyloggers and viruses. As we know that in these days, the internet is full of malicious material and there is not a chance to survive for any of its user without discretion. We should utilize these kind of tools whenever we perceive any skeptical activity in our systems. We can easily check up our systems on a daily basis without the help of any expert and it can be considered as a plus point.

Compiled & Written by:

Salman Abdul Rahim

(BS-Computer Science)