Ex.No. :09 **Monitoring Malware Using Rootkit Hunter**

AIM:

To install a rootkit hunter and find the malwares in a computer.

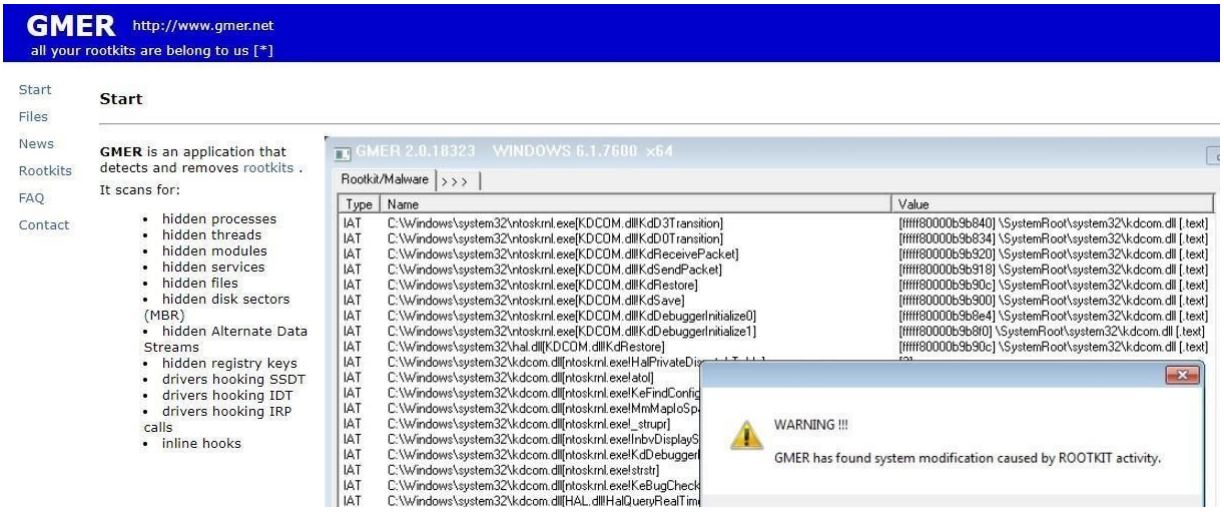
ROOTKIT HUNTER:

- rkhunter (Rootkit Hunter) is a Unix-based tool that scans for rootkits, backdoors andpossible local exploits.
- It does this by comparing SHA-1 hashes of important files with known good ones in online databases, searching for default directories (of rootkits), wrong permissions, hidden files, suspicious strings in kernel modules, and special tests for Linux and FreeBSD.
- rkhunter is notable due to its inclusion in popular operating systems (Fedora, Debian,etc.)
- The tool has been written in Bourne shell, to allow for portability. It can run on almostall UNIX-derived systems.

GMER ROOTKIT TOOL:

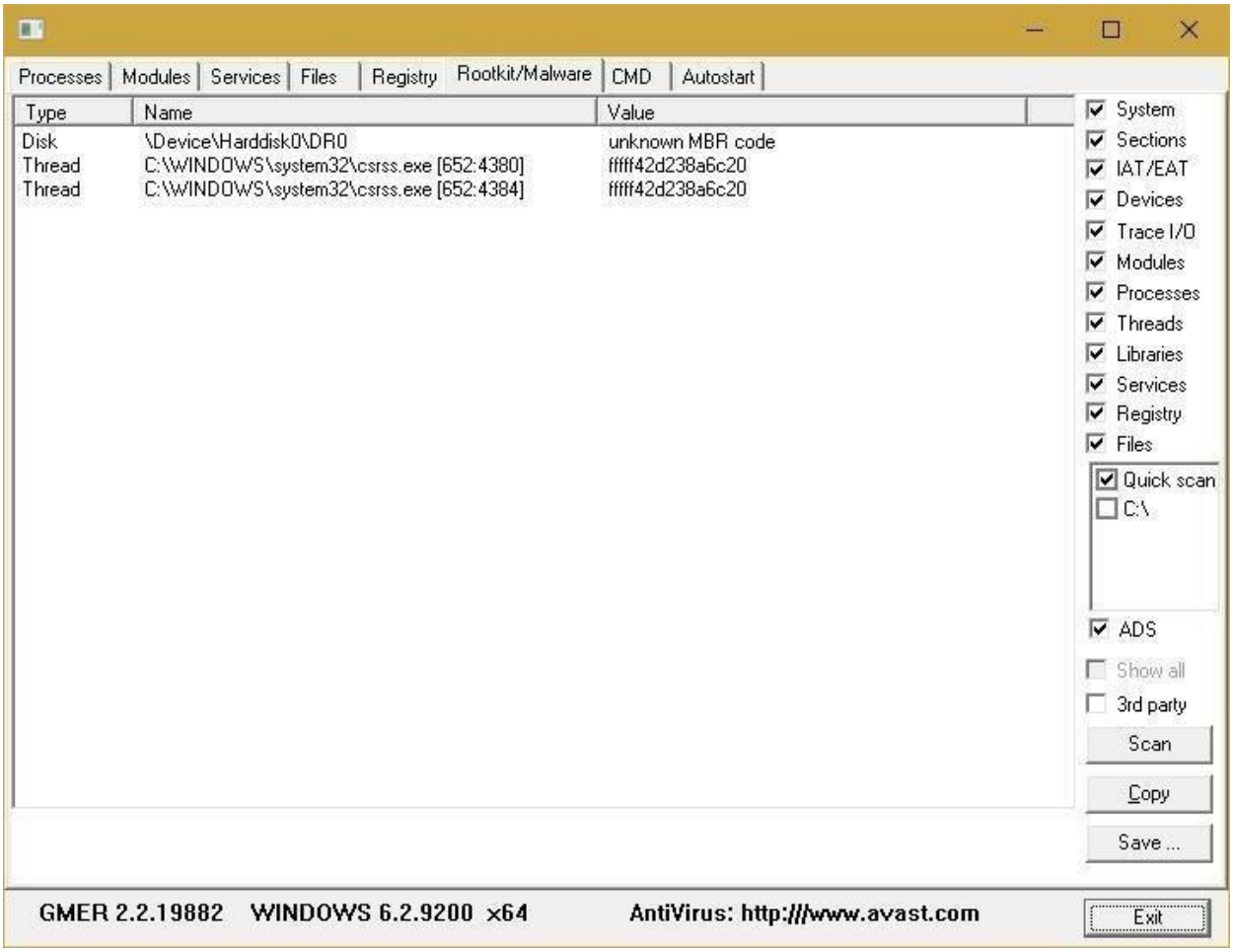
- GMER is a software tool written by a Polish researcher Przemysław Gmerek, fordetecting and removing rootkits.
- It runs on Microsoft Windows and has support for Windows NT, 2000, XP, Vista, 7, 8
  and 10. With version 2.0.18327 full support for Windows x64 is added.

Step 1



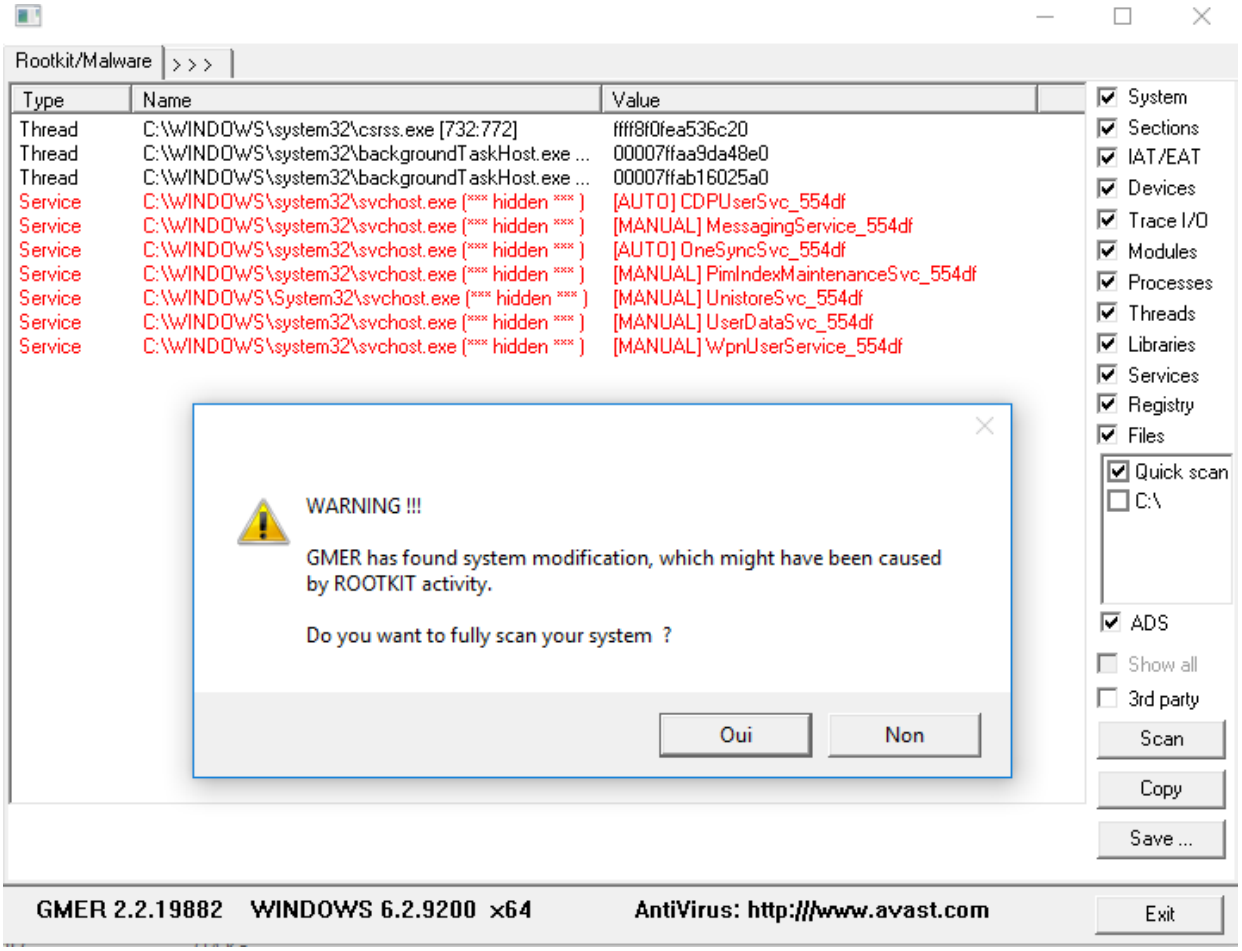
Visit GMER's website (see Resources) and download the GMER executable. Click the "Download EXE" button to download the program with a random file name, assome rootkits will close “gmer.exe” before you can open it.

Step 2



Double-click the icon for the program.
Click the "Scan" button in the lower-right corner of the dialog box. Allow the program toscan your entire hard drive.

Step 3



When the program completes its scan, select any program or file listed in red. Right-click it and select "Delete." If the red item is a service, it may be protected. Right-click the service and select "Disable." Reboot your computer and run the scan again, this time selecting "Delete" when that service is detected. When your computer is free of Rootkits, close the program and restart your PC.

RESULT:

A rootkit hunter software tool *gmer* has been installed and the rootkits have been detected.