# BVM Tool to inject virus into victim machine

BVM Tool is a windows virus making software with other tools. It can make a variety of viruses such as here I have taken the example of making a virus that will delete the pictures, .mp3 extension files, .mp4 extension files, documents and to disable the anti-virus software of the victim machine.

1.Installing the BVM tool from the internet and in order to run it one must disable the anti-virus of the windows along with any real-time protection. Now we can start making a virus.
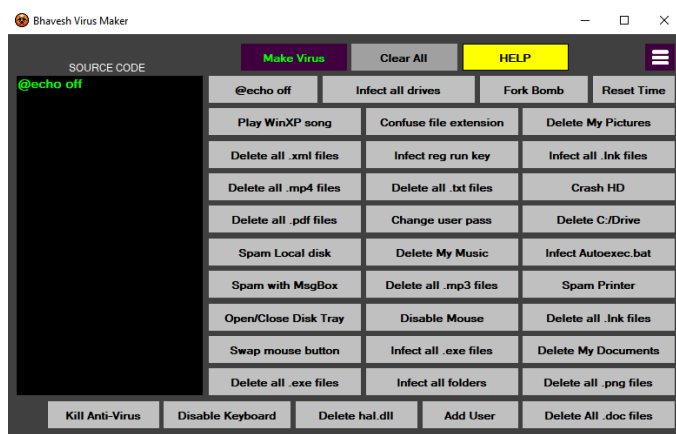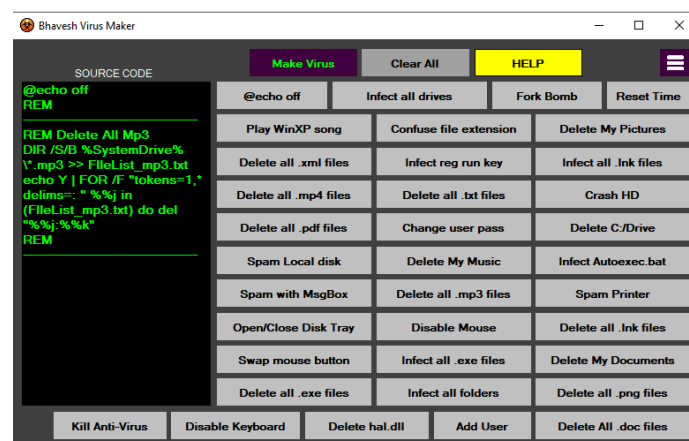

2. Making a virus that deletes the pictures from the victim's machine.
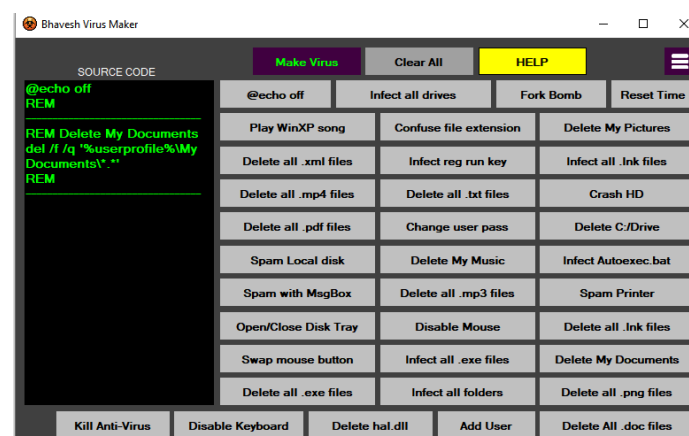

3. Making a virus that deletes the files with .mp4 extension from the victim's machine.

4. Making a virus that deletes the .mp3 extension files from the victim's machine.

5. Making a virus that deletes the documents from the victim's machine.

The above viruses that are made and saved as windows batch file in the hacker's computer.

In order to get into the victim's machine there are many ways a hacker can do that. By doing so, the hacker will take control of the victim's machine having all his private information at his disposal to use change, manipulate, delete or just lurk around by creating a backdoor and snooping around whenever they need something from the victim. Sometimes the hacker even has a political, economical or personal gain by using the confidential information from the victim.

As the viruses are in windows batch file format it is easy to boot it onto the victim's computer from there. Multiple ways can used to do so. It can be as simple as a file transfer from the hacker's machine to the victim's machine by a pendrive which is what I have done in this case.

Hackers use Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Your mobile devices and smartphones can become infected with mobile viruses through shady app downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files.

To avoid contact with a virus, it's important to exercise caution when surfing the web, downloading files, and opening links or attachments. To help stay safe, never download text or email attachments that you're not expecting, or files from websites you don't trust.

6. This is the victim's machine.
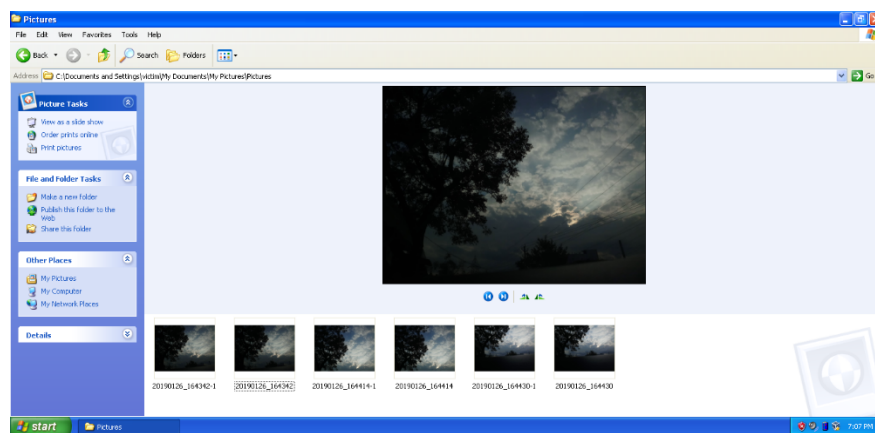
The virus is booted into the system and the batch files are executed without any intervention from the command prompt window.

7. All the below screenshots are from the victim's machine where the pictures, documents, files with .mp3 & .mp4 extensions are deleted.
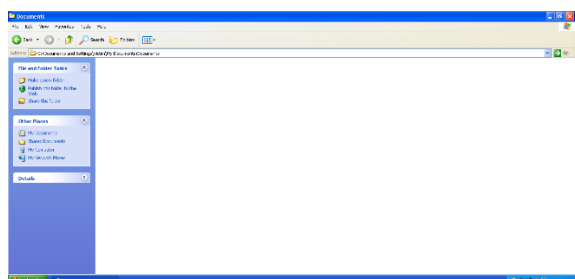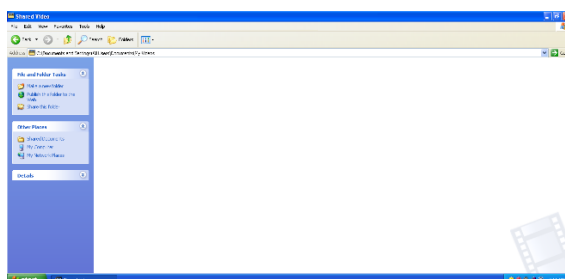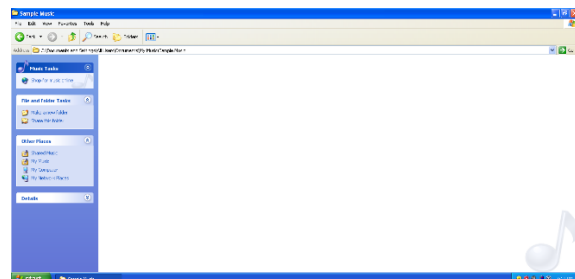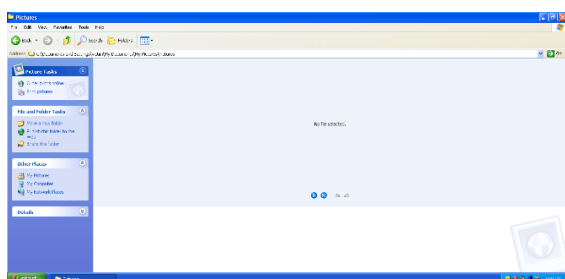
In Conclusion , I have used the BVM tool in order to make different types of viruses and ensured to boot it into the victim's machine. The virus executed as intended to delete specific files.