Click here to Ask Techrena For Solutions 

Saturday, November 1, 2008

How to Delete/Remove Surabaya virus/worm/Spyware from your Computer?

Many people are facing problem with the new USB worms coming up,one such worm is Surabaya Virus[As it calls itself by that name!]

Some info:Surabaya is the second largest city in Indonesia,the name and language suggests that the worm was actually originated in Indonesia by some spammer.Ok,enough about it's history,Let's get into the details of the worm's operation.

When the virus enters your system,the following message would come up:

"*Surabaya in my birthday*
Don't kill me, i'm just send message from your computer
Terima kasih telah menemaniku walaupun hanya sesaat, tapi bagiku sangat berarti
Maafkan jika kebahagiaan yang kuminta adalah teman sepanjang hidupku
Seharusnya aku mengerti bahwa keberadaanku bukanlah disisimu, hanyalah lamunan dalam sesal
Untuk kekasih yang tak kan pernah kumiliki 3r1k1m0"

And it creates a lot of '.SCR' files and also changes Shell Extensions for all Drives(C,D,E,F,G,H..whatever).

So when you try to open any drive,or if you right-click on any drive you'll be amazed to find "Test,Configure" instead of standard "Open/Explore".

It also changes the registry to hide all the hidden folders and also disables 'FOLDER OPTIONS'.

Let's See How to Remove Surabaya virus

THE SOLUTION:

>>**STEP1:** Download free Clamwin AnitVirus, install, update then boot into safe mode, disable any other antivirus software that you have, and perform a full scan:

http://www.download.com/ClamWin-Antivirus/3000-2239_4-10369483.html?tag=mncol&cdlPid=10514511

This is a small freeware which detects Surabaya. After deleting all the viruses by the antivirus perform the steps below.

Note: You can proceed to next step if you have already deleted the virus with any other anti-virus.

>>**STEP2:** Delete file 'Autorun.inf' which allows the malicious script to run automatically when you click/double click on the drive.

If you are not able to delete it from Windows Explorer,then you can try using 'DOS Command Prompt'. To enter into this,

Go to Start Menu>Click on RUN>Type 'cmd' ,Click 'OK'.

Now the command prompt will be opened up,

the default root will be 'C:\Documents and Settings\Administrator>'

You have to change it to 'C:\',to do that type 'cd/' and it'll take you to 'C:\'.

Now type attrib -s -h –r autorun.inf [And Hit 'Enter'-This is to change attributes if the file so that we can delete it]

Now Type 'del autorun.inf'

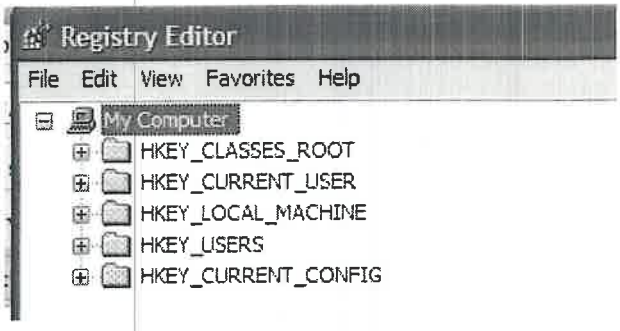
>>**STEP3:**The Second step is very important because you need to work with 'Windows Registry'

Warning:Any unwanted mistakes in the registry, I'll guarantee you that your OS will be dumped.

Ok let's start it:

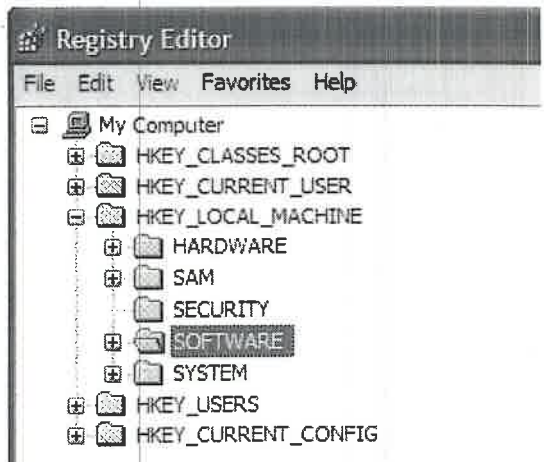
As in the first step,go to Start>Click on RUN>type 'REGEDIT' and press 'ok'.

[Note:'REGEDIT' stands for Windows Registry Edit]



Then Click on>"HKEY_LOCAL_MACHINE"[Click onthe '+' sign]

Then find 'SOFTWARE' and Again Click on the '+' sign next to it.

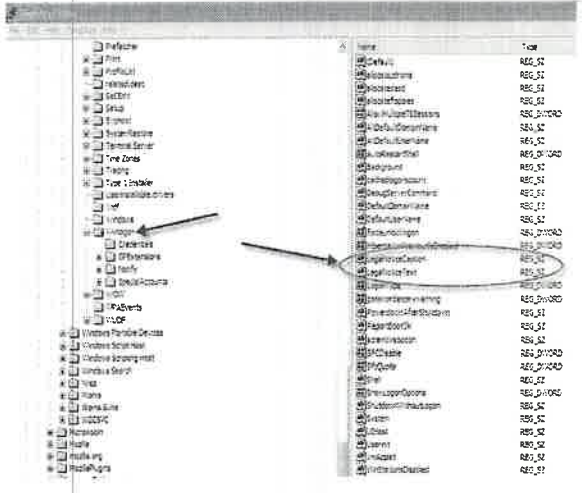


Next Find 'Microsoft' under it and then 'WINDOWS NT'

Next 'CURRENT VERSION' and finally find 'WINLOGON'.

The path you've followed is
HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>CURRENT VERSION' >WINLOGON

on the right windows (under data) modify or delete "LegalNoticeCaption" & "LegalNoticeText".



This removes any message coming up in the start up.

>>**STEP4:** Visit the link below and enable your Show Hidden folder Options:

http://techrena.blogspot.com/2008/11/how-to-show-hidden-files-and-folders-in.html

This will enable the 'FOLDER OPTIONS' and will show hidden files/folders if checked.

I hope this will clear your problem,if still problem exists or have any trouble while doing this,please post them in comments section below.