Browser Fake Virus Attack

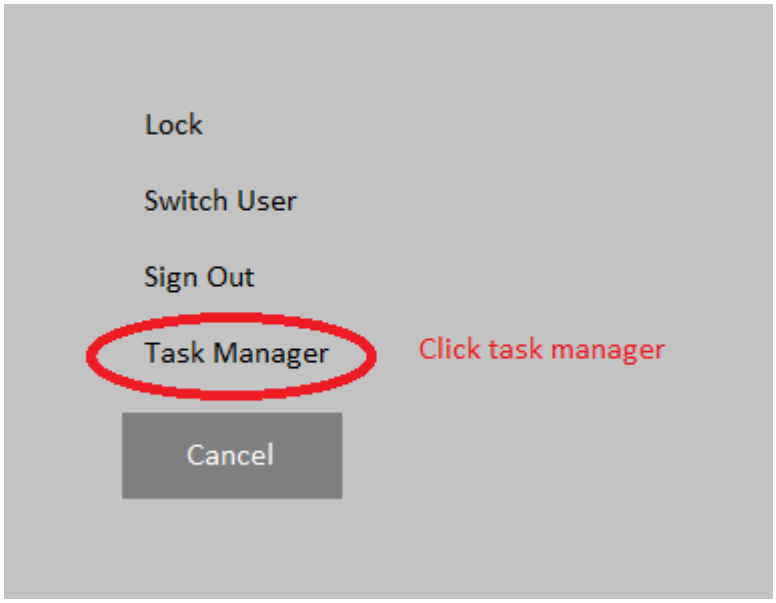
Either starting your internet browser or by clicking on a button or link, connects you to a Virus scam. In this case the user tries to go to the Activities Unlimited webpage. Many variations exist but here is one example:

The common thread of all these fake virus scams is that the browser is automatically redirected to open this page if the browser is closed and then started again. The user is blocked from being able to access other apps or windows features. Therefore, it appears as if the PC has been hijacked. But other than taking control of the PC nothing on the PC has been done.

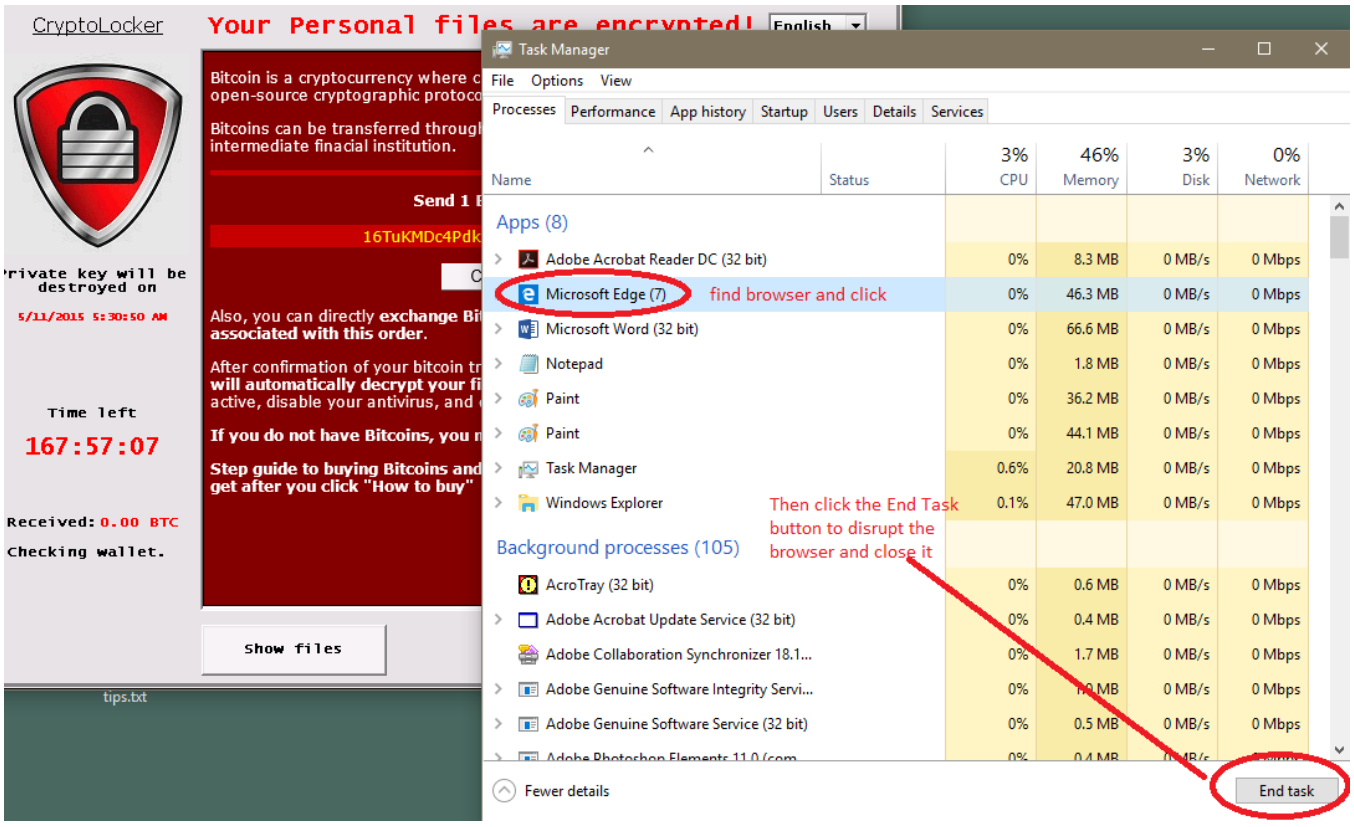
One method to determine if this is a fake is to invoke the task manager. While most control of the PC is been blocked using the 3 keys Ctrl ALT Delete can launch the task manager. Once accessed it can be used to stop the browser. Then do not retry the browser but rather go to the installed virus protection app on the PC. Breaking a circular browser restart loop is one of the things a good virus protection app should do.

Another method upon breaking the browser redirection loop would be to re-install the browser.

When the Ctrl Alt Delete keys are used it should invoke this screen:



Then the task manager looks as follows:



The virus is a fake because it has not taken over the PC but rather it has launched an app (or webpage) that only appears to be in control. IE it is only one of the many tasks the PC has running at the moment. The task manager is there to override control of a task and shut it down (end task).

This is similar to an app which has a bug that causes the app to enter an infinite loop. This typically appears as if the PC (or app) is frozen. The same method can be used in this case.

The Task Manager is your friend !