**=====> Code Explanation**

Attacker share "cert-test" folder across the network.

"cert-test" contain following folder and files:

-> "bin" : certutil.exe to install BrpSuite Certificate (certutil.exe is firefox NSS tool https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS\_Tools\_certutil)

-> "cacert" : place BurpSuite certificate here (This is the location from where all the certificate will install. Place all your certificate here.)

-> "db" : no changes required (sample firefox database which keep record of user setting. "key4.db" and "cert9.db" files are used to track certificate in firefox)

-> "add-cert.cmd" : This file will run "certutil.exe" to install certificate at appropriate firefox location and different firefox profile. This file does not require any changes.

-> proxy.bat :

-First it will download "cert-test" folder from attacker system

-then it will run another batch file "add-cert.cmd"

-then it will add ip and port in "pref.js" file which is located at C:\Users\$username$\AppData\Roaming\Mozilla\Firefox\Profiles\\*.default

-"pref.js" stores firefox preference.

=====================================================================================

**======> Process of Sending file to victim and execution :**

-> Only "proxy.bat" is required to send to the victim

-> To fool victim convert "proxy.bat" to "AnyName.exe" using any batch to exe converter. while converting select "RUN AS ADMIN" option.

-> You can also change ICON of "AnyName.exe" using EXE ICON changer

-> Before Sending file "AnyName.exe" to victim, Setup BurpSuite to Listen on "ALL INTERFACE" and PORT which is in "proxy.bat"

-> The File "AnyName.exe" starts executing when victim double clicks on it.