

**ന്യൂന സൈബർ ആക്രമണങ്ങൾ പ്രതിരോധിക്കാനുള്ള നിർദ്ദേശങ്ങൾ.**

ഇന്നലെ മുതൽ ആഗോളവ്യാപകമായി രണ്ടു പുതിയ തരം കമ്പ്യൂട്ടർ റാൻസംവെയറുകൾ (Ransomware) പ്രചരിക്കുന്നതായി അറിയുന്നു. കമ്പ്യൂട്ടറിൽ ഇവ ബാധിച്ചാൽ പ്രധാനപ്പെട്ട ഫയലുകളെ ഇവണ്ണോക്ക് ചെയ്യുന്നു, പിന്നീട് അവ തുറന്നു കിട്ടണമെങ്കിൽ ഓൺലൈൻ കറൻസി ആയ ബിറ്റ് കോയിൻ നിക്ഷേപിച്ചു മോചിപ്പിച്ചെടുക്കേണ്ട അവസ്ഥയാണ് ബ്രിട്ടനിലെയും സ്പെയിനിലെയുമൊക്കെ സർക്കാർ സംവിധാനത്തെയും ഫെഡ് എക്സ് തുടങ്ങിയ കമ്പനികളെയും ഇവ ഗുരുതരമായി ബാധിച്ചുവെന്ന് ഈ രംഗത്തെ വിദഗ്ദ്ധർ അറിയിക്കുന്നു. ലക്ഷക്കണക്കിന് പ്രധാനമായും ആശുപത്രി ശൃംഖല ഇവ ലക്ഷ്യം വച്ചിട്ടുള്ളത് എന്നാണ് മനസ്സിലാക്കുന്നത്. ഇത്തരം സൈബർ ആക്രമണങ്ങൾക്കെതിരെ അപരിചിതമായ ലിങ്കുകൾ, ജാഗ്രത പാലിക്കേണ്ടത് അത്യാവശ്യമാണ്, സംശയാസ്പദമായ ഇ-മെയിലുകൾ, അവയിലെ അറ്റാച്ച്മെന്റുകൾ എന്നിവ തുറക്കാതെ നോക്കുക, നിങ്ങളുടെ കമ്പ്യൂട്ടറിലെ ആന്റി വൈറസ് അപ്ഡേറ്റ് ചെയ്ത് വേണ്ട മുൻകരുതലുകൾ എടുക്കണം.

**അതോടൊപ്പം താഴെ പറയുന്ന നിർദ്ദേശങ്ങൾ കൂടി കൃത്യമായി പാലിക്കേണ്ടതാണ് .**

- 1) സംശയാസ്പദമായ സാഹചര്യത്തിൽ കിട്ടുന്ന ഇമെയിൽകൾ ഓപ്പൺ ചെയ്യുകയോ അനുബന്ധ അറ്റാച്ച്മെന്റുകൾ തുറക്കാതിരിക്കുകയോ ചെയ്യുക.
- 2) വിശ്വാസയോഗ്യമല്ലാത്ത സ്രോതസ്സുകളിൽ നിന്നും വരുന്ന മെയിലുകൾ, ലിങ്കുകൾ തുടങ്ങിയവയുടെ ആധികാരികത ഉറപ്പു വരുത്തിയ ശേഷം മാത്രം തുറക്കുക
- 3) വ്യക്തിപരമോ, സാമ്പത്തികമോ ആയ വിവരങ്ങൾ ആവശ്യപ്പെടുകൊണ്ടുള്ള അന്വേഷണങ്ങൾക്ക് മറുപടി നൽകേണ്ടതില്ല.
- 4) മെയിൽ സന്ദേശങ്ങളുടെ ആധികാരികത ഉറപ്പുവരുത്തുക.
- 5) വ്യക്തിപരമായി പുകഴ്ന്ന മെയിലുകൾ, മനഃപൂർവ്വം വരുത്തുന്ന പിശകുകൾ എന്നിവ സസൂക്ഷ്മം നിരീക്ഷിച്ചു മെയിലുകൾ കൈകാര്യം ചെയ്യുക.
- 6) ഇമെയിൽ അറ്റാച്ച്മെന്റുകൾ സസൂക്ഷ്മം തുറക്കുക.
- 7) മെയിൽ വഴി ലഭ്യമാവുന്ന ഫോമുകളിൽ വ്യക്തിപരമായ വിവരങ്ങൾ നൽകാതിരിക്കുക. ഇത്തരം വിവരങ്ങൾ ട്രാക്ക് ചെയ്യപ്പെടാൻ സാധ്യത ഉള്ളതിനാൽ ആണിത്.
- 8) വ്യക്തിഗത വിവരങ്ങൾ കൈമാറുന്നതിന് മുൻപ് വെബ്സൈറ്റിന്റെ ആധികാരികത ഉറപ്പു വരുത്തുക.
- 9) ഔദ്യോഗിക ഇമെയിലുകൾ വ്യക്തിപരമായ ആവശ്യങ്ങൾ ഉപയോഗിക്കാതിരിക്കുക.
- 10) സമൂഹമാധ്യമങ്ങളിൽ സംശയകരമായ സാഹചര്യങ്ങളിൽ നിന്ന് ലഭിക്കുന്ന ഇമേജുകൾ, വീഡിയോകൾ തുറക്കാതിരിക്കുക.
- 11) സമ്മാനങ്ങൾ ഓഫർ ചെയ്യുകൊണ്ടുള്ള മെയിൽകൾക്ക് സാമ്പത്തിക വിവരങ്ങൾ നൽകരുത്.

12) ബാങ്ക് വിവരങ്ങൾ ആവശ്യപ്പെടുകൊണ്ടുള്ള വിവരങ്ങൾക്ക് മറുപടി നൽകാതിരിക്കുക.

13) ഓൺലൈൻ ഷോപ്പിംഗ് പോലുള്ള വ്യക്തിപരമായ ആവശ്യങ്ങൾക്ക് പ്രത്യേക മെയിൽ ഐഡി ഉപയോഗിക്കുക.

## Precautionary measures against Ransomware Attack

**Ransomware Attack:** Ransomware is a creative malware that infects systems and locks down data, preventing users from accessing it until a ransom is paid. It can affect individuals and businesses alike, but can become a critical threat for enterprises dealing with huge amounts of data. You are advised to kindly take the following preventive measures to protect their computer networks from ransomware infection/ attacks:

1. Ensure that ports TCP/UDP 445, 137, 138, 139 are blocked on all perimeter devices and internal access control devices.
2. Ensure that ports TCP/UDP 445 are blocked on all clients & servers using host firewalls through host antiviruses and HIPS.
3. Apply all patches of Microsoft Windows (client and server) for the vulnerability mentioned in the Microsoft Security Bulletin MS17-010.
4. Secure mail server with antivirus and anti spamware solution.
5. Maintain updated Antivirus software on all user client systems urgently ON PRIORITY.
6. Update operating system, third party applications (MS office, browsers, browser Plugins) and antivirus software with the latest patches ON PRIORITY.

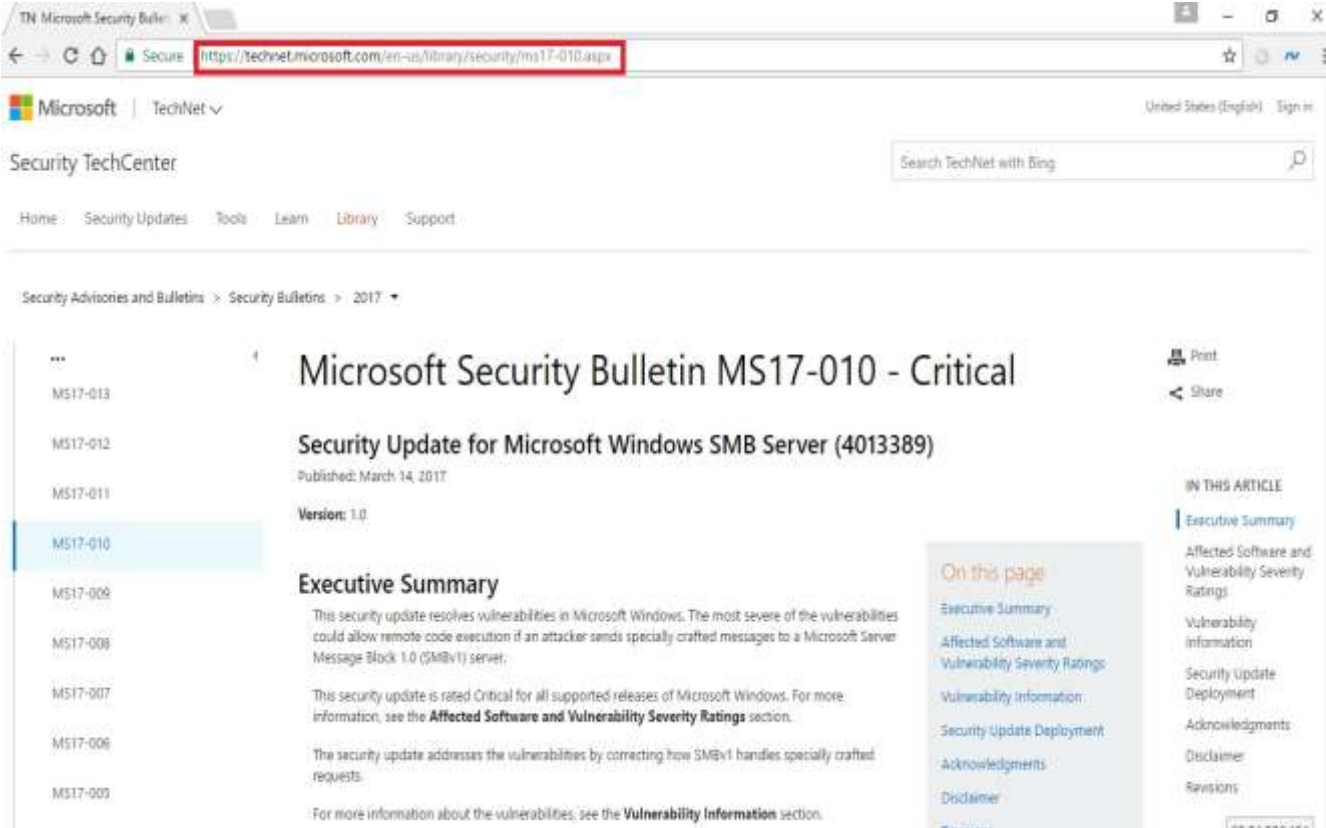
All system administrators to ensure this is done in the organizations ASAP.

1. Alert all users in the organization of the attack. Hence the above step of updating softwares on the computer needs to be ensured before the user accesses email or internet.
2. Users should be alerted not to open attachments in unsolicited e-mails, even if they come from people in your contact list; never click on a URL contained in an unsolicited e-mail unless you are sure it is genuine. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.

3. Block Tor, Peer to Peer(P2P) /Torrent traffic in Systems and Network.
4. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.\*
5. Check regularly for the integrity of the information stored in the databases.
6. Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
7. Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
8. Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
9. Application white listing/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
10. Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
11. Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
12. Disable remote Desktop Connections, employ least-privileged accounts. Limit users who can log in using Remote Desktop, set an account lockout policy. Ensure proper RDP logging and configuration.
13. Restrict access using firewalls and allow only to selected remote endpoints, VPN may also be used with dedicated pool for RDP access
14. Use strong authentication protocol, such as Network Level Authentication (NLA) in Windows.

## How to install Windows update as per Microsoft Security Bulletin MS17-010 – Critical

1. Go to <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx> in browser.



Microsoft Security Bulletin MS17-010 - Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

### Executive Summary

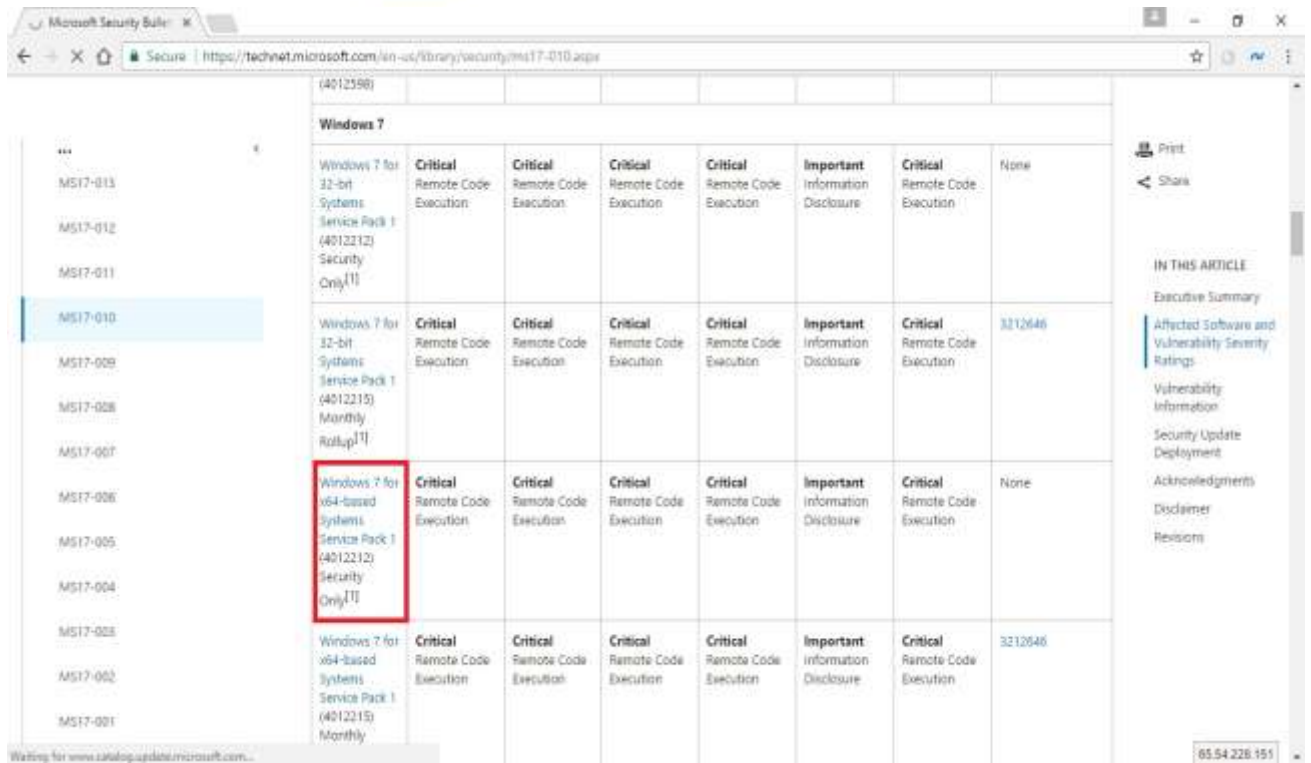
This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

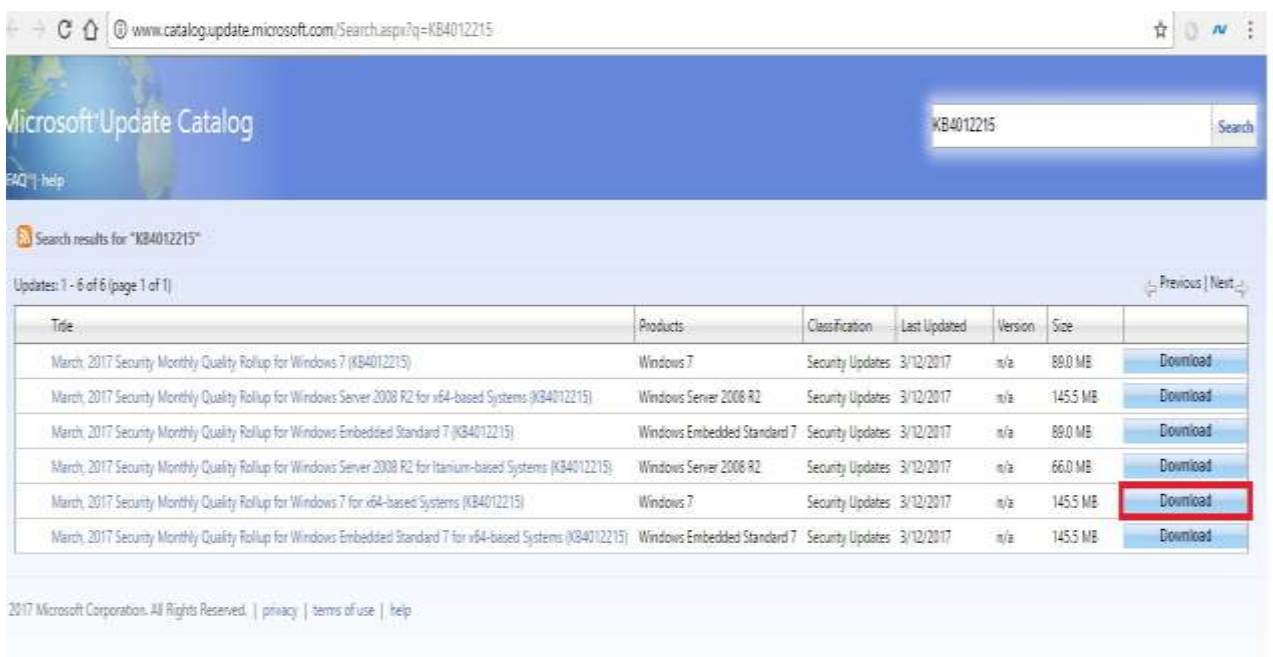
For more information about the vulnerabilities, see the **Vulnerability Information** section.

2. Patches for various versions of windows are listed. Select appropriate version.



Update ID	Product	Classification	Severity	Impact	Resolution	KB Number
MS17-013	Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Only <sup>[1]</sup>	Critical	Remote Code Execution	Critical	Remote Code Execution	None
MS17-010	Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Only <sup>[1]</sup>	Critical	Remote Code Execution	Critical	Remote Code Execution	3212646
MS17-009	Windows 7 for 32-bit Systems Service Pack 1 (4012215) Monthly Rollup <sup>[1]</sup>	Critical	Remote Code Execution	Critical	Remote Code Execution	None
MS17-010	Windows 7 for x64-based Systems Service Pack 1 (4012212) Security Only <sup>[1]</sup>	Critical	Remote Code Execution	Critical	Remote Code Execution	None
MS17-008	Windows 7 for x64-based Systems Service Pack 1 (4012215) Monthly	Critical	Remote Code Execution	Critical	Remote Code Execution	3212646

3. A new *Microsoft update catalog window* will open and then select *download* option corresponding to *March, 2017 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4012215)* as shown below:



Microsoft Update Catalog

Search results for "KB4012215"

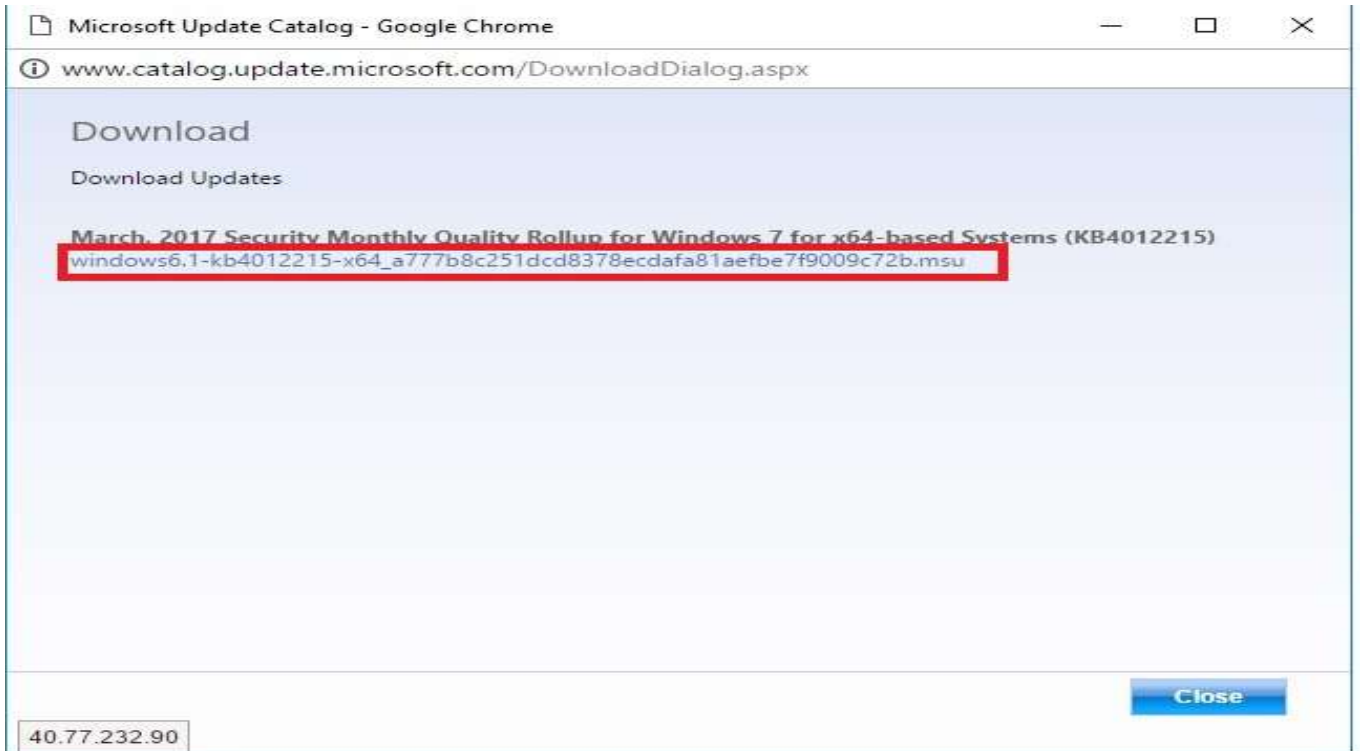
Updates: 1 - 6 of 6 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	Download
March, 2017 Security Monthly Quality Rollup for Windows 7 (KB4012215)	Windows 7	Security Updates	3/12/2017	n/a	89.0 MB	Download
March, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4012215)	Windows Server 2008 R2	Security Updates	3/12/2017	n/a	145.5 MB	Download
March, 2017 Security Monthly Quality Rollup for Windows Embedded Standard 7 (KB4012215)	Windows Embedded Standard 7	Security Updates	3/12/2017	n/a	89.0 MB	Download
March, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for Itanium-based Systems (KB4012215)	Windows Server 2008 R2	Security Updates	3/12/2017	n/a	66.0 MB	Download
March, 2017 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4012215)	Windows 7	Security Updates	3/12/2017	n/a	145.5 MB	Download
March, 2017 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems (KB4012215)	Windows Embedded Standard 7	Security Updates	3/12/2017	n/a	145.5 MB	Download

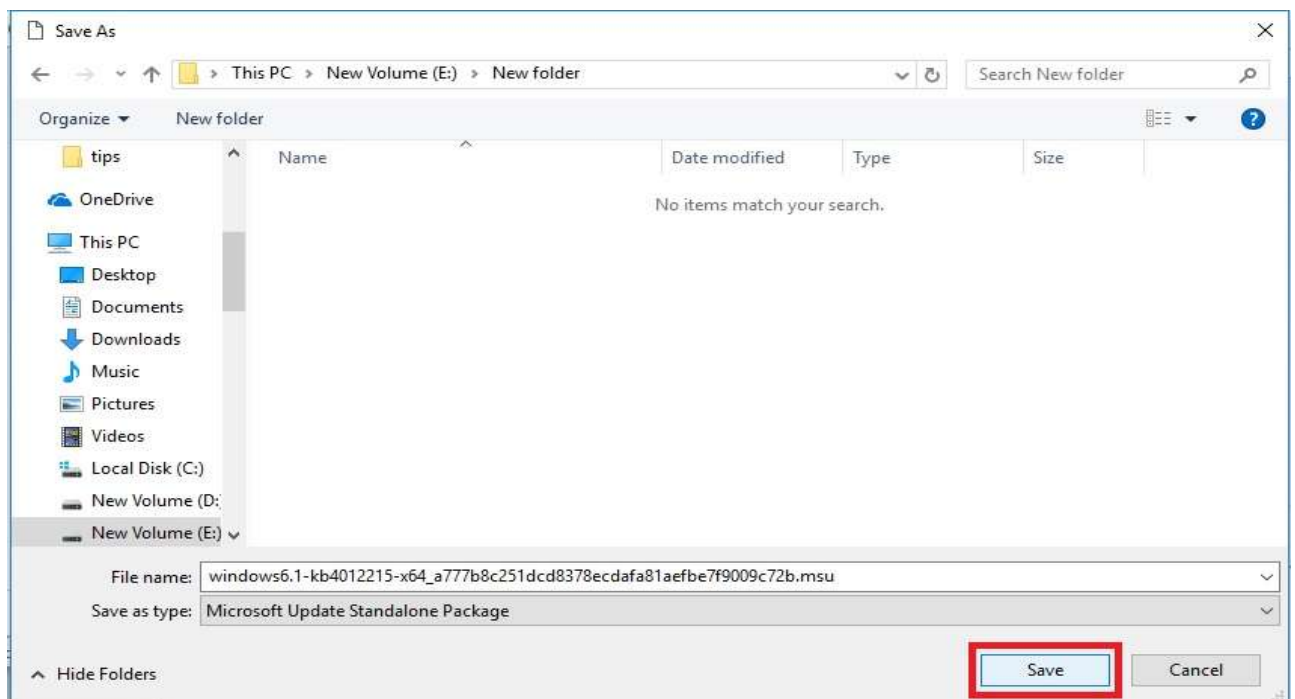
2017 Microsoft Corporation. All Rights Reserved. | [privacy](#) | [terms of use](#) | [help](#)

4. On the download page

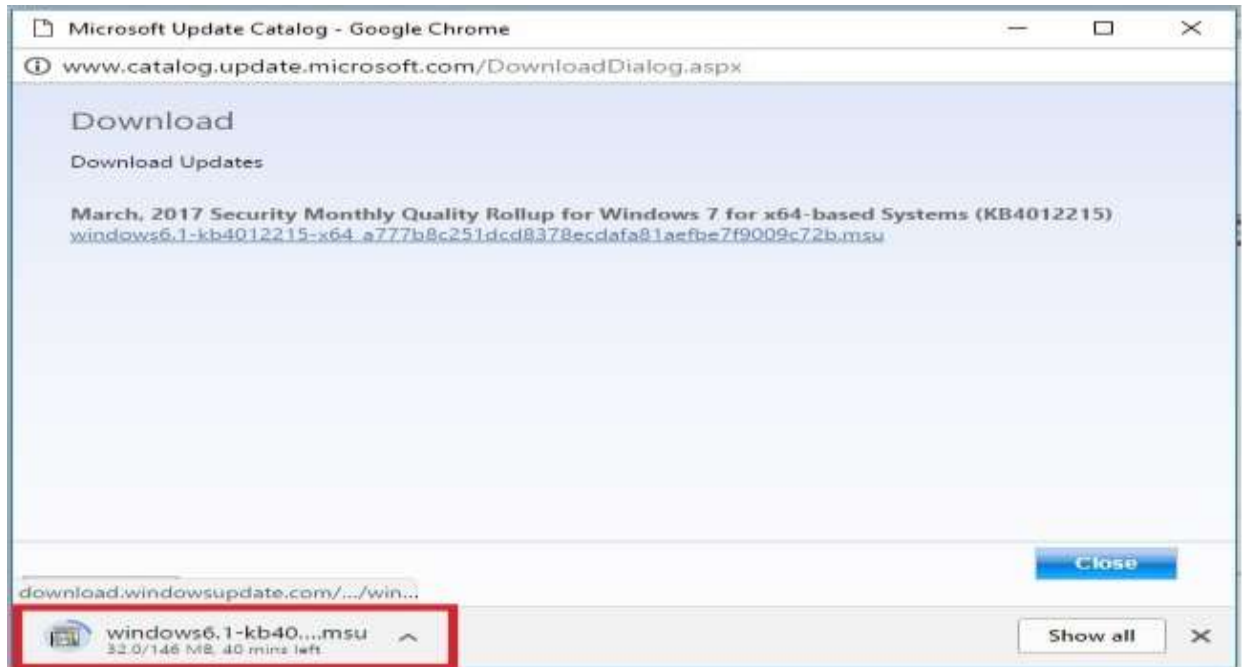
Click: [windows6.1-kb4012215-x64\\_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.msu](http://windows6.1-kb4012215-x64_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.msu) as shown below:



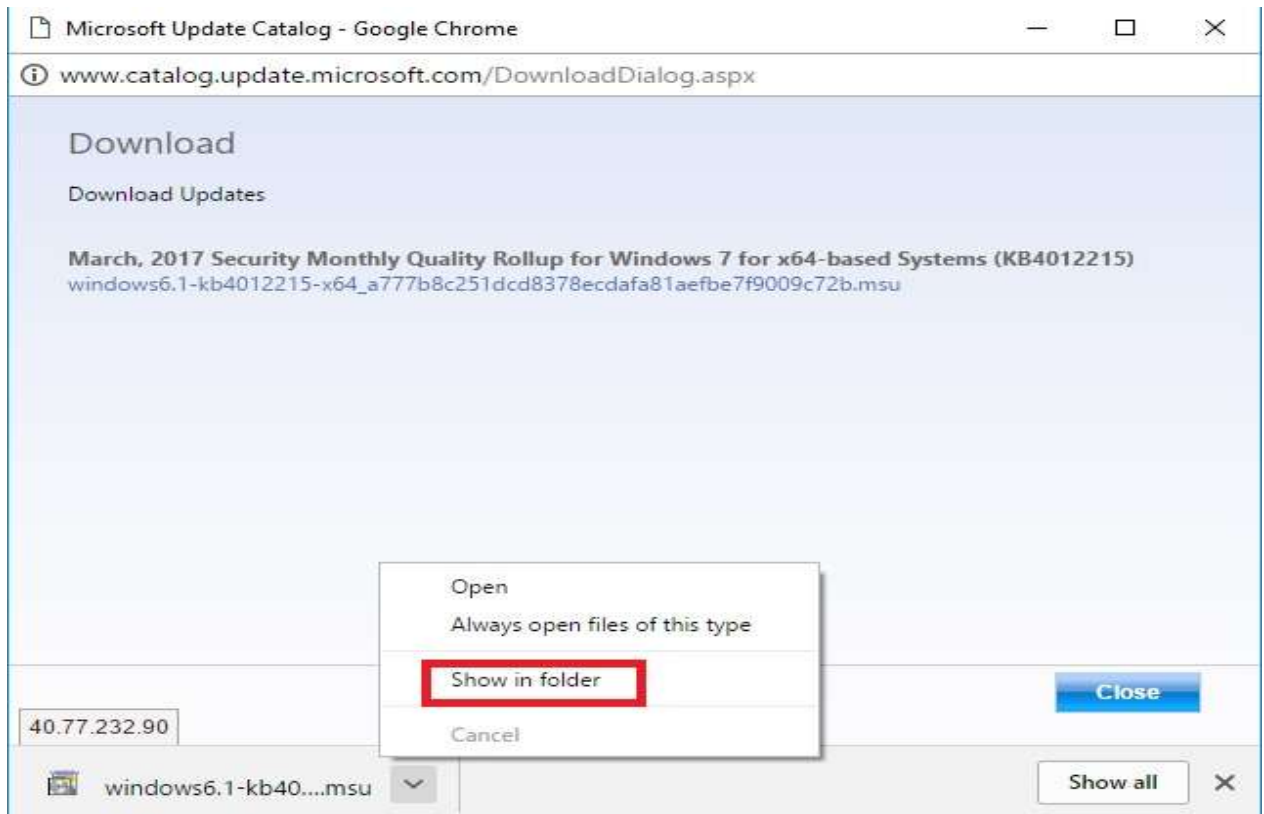
5. A save window as shown below is opened and then browse the location where need to save the installation file and then click save:



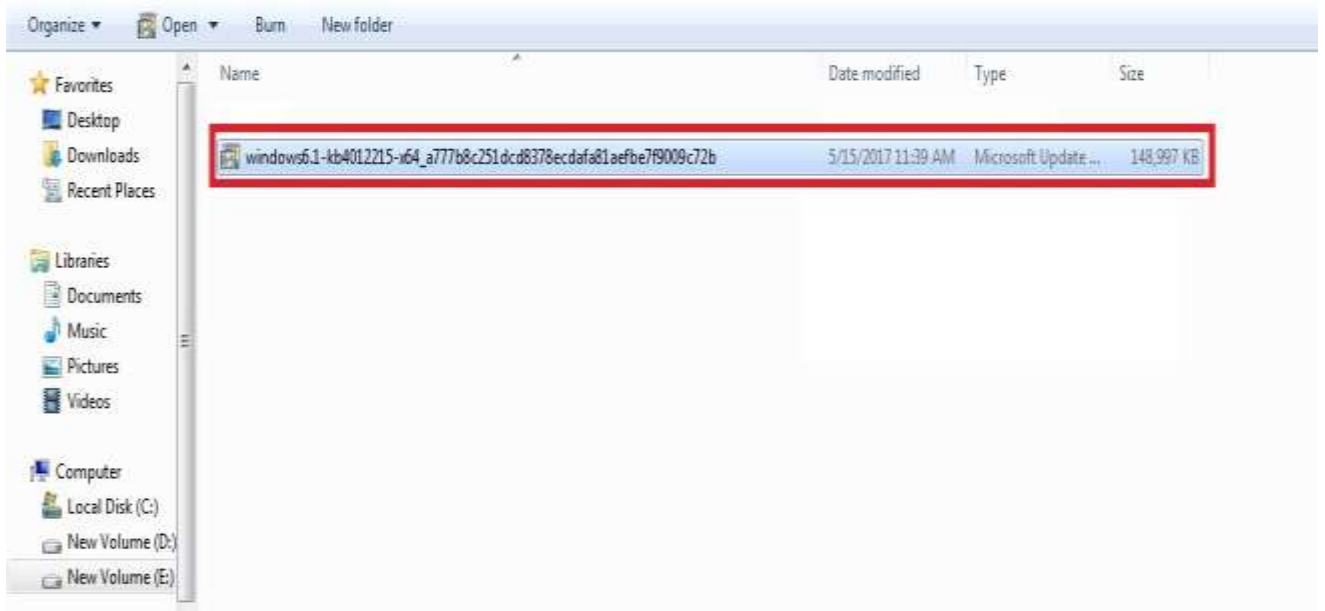
6. Download is in progress.



7. After completing the download, click the arrow and then select show in folder or browse to the location where the downloaded software resides.



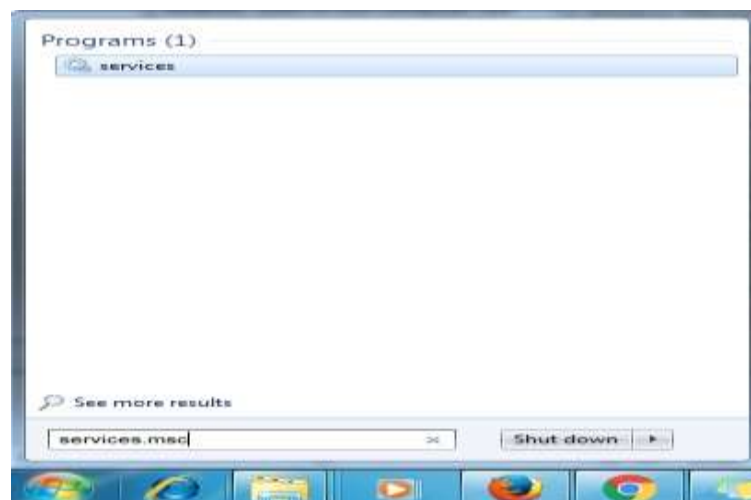
8. Double click the installation file



9. If any error occurred as shown below follow the next step otherwise go to step 20:

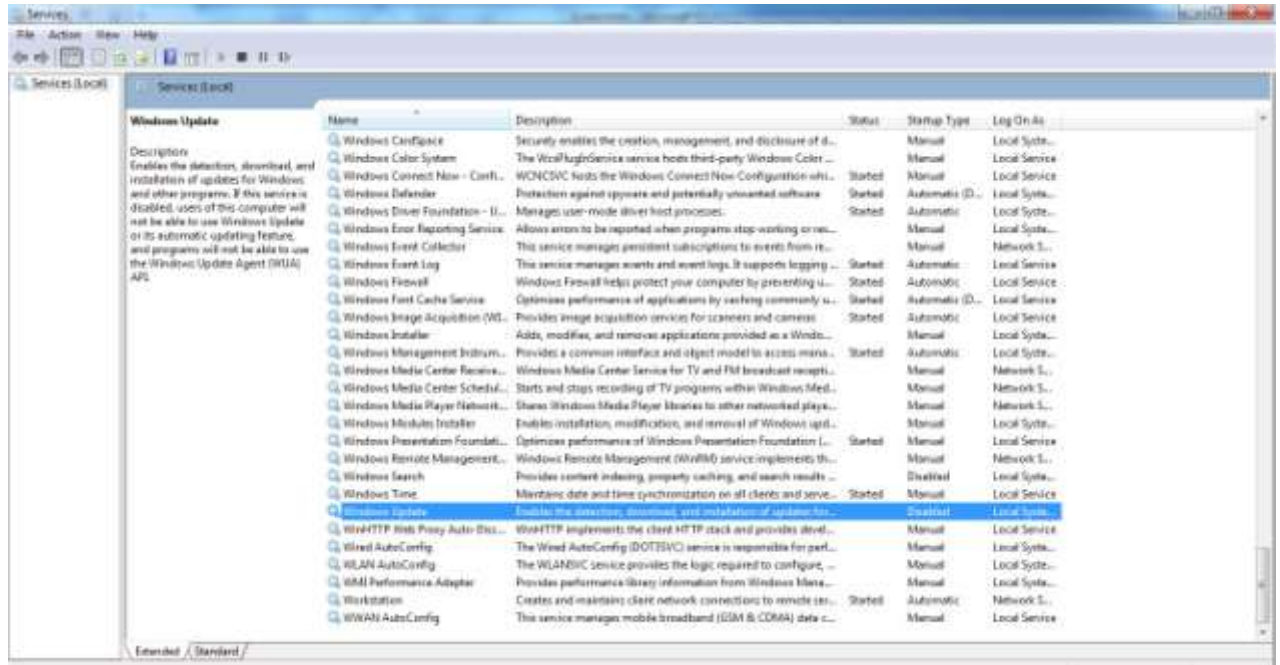


10. On windows start menu search bar type: **services.msc**

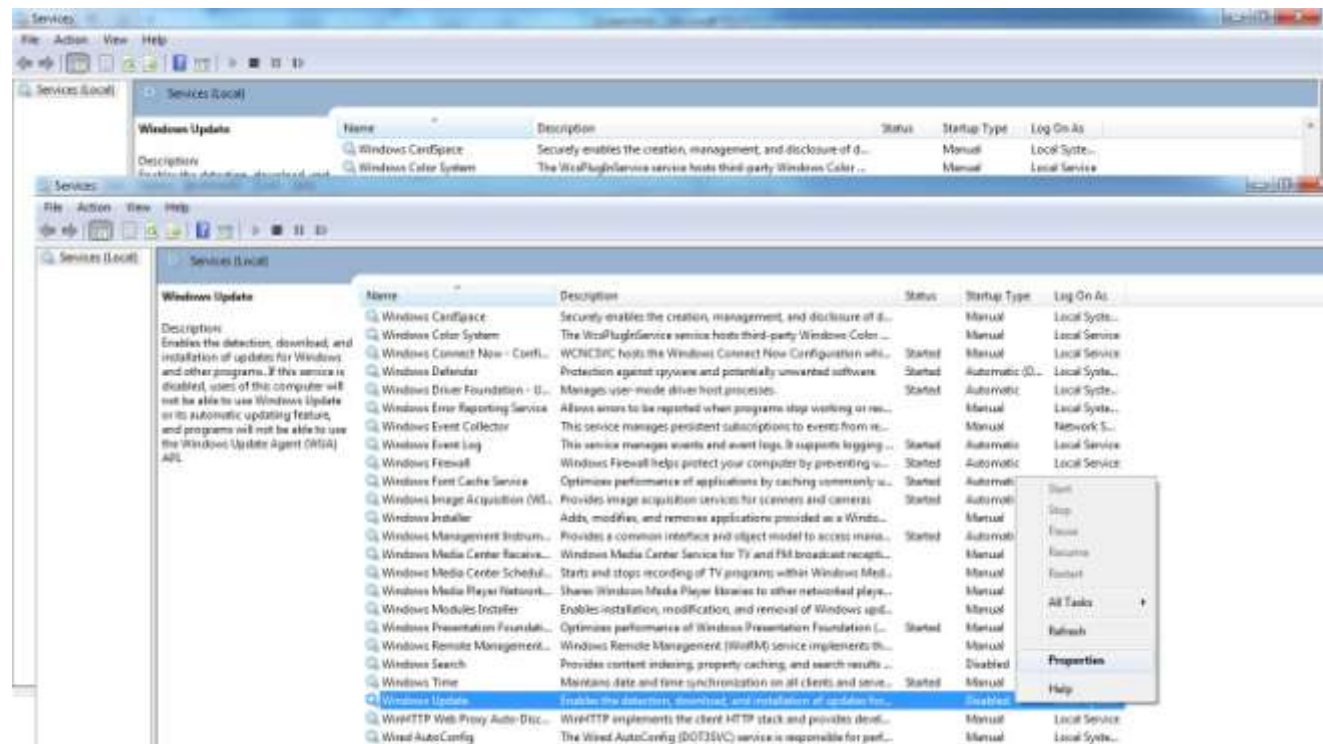




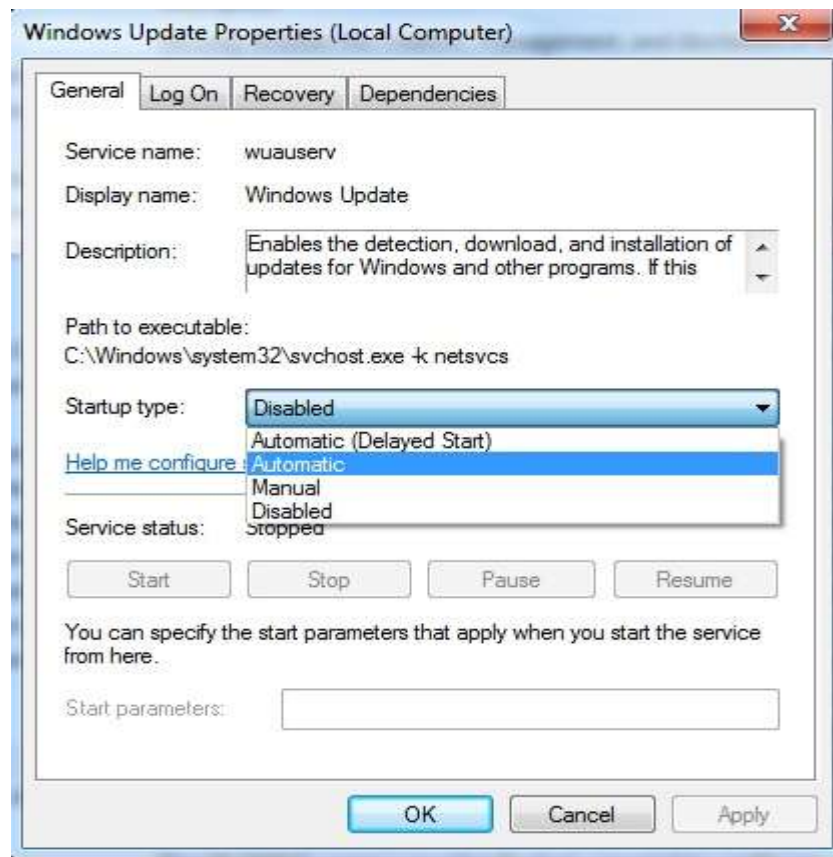
11. New window open as shown below. Scroll down for the windows update and check status disabled.



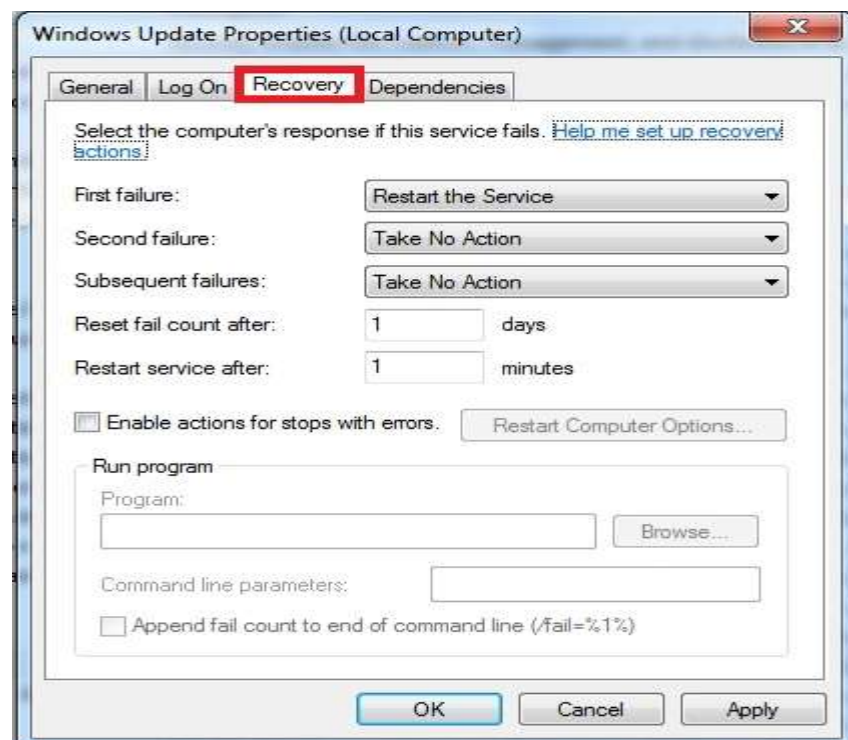
12. On the option right click and then select properties



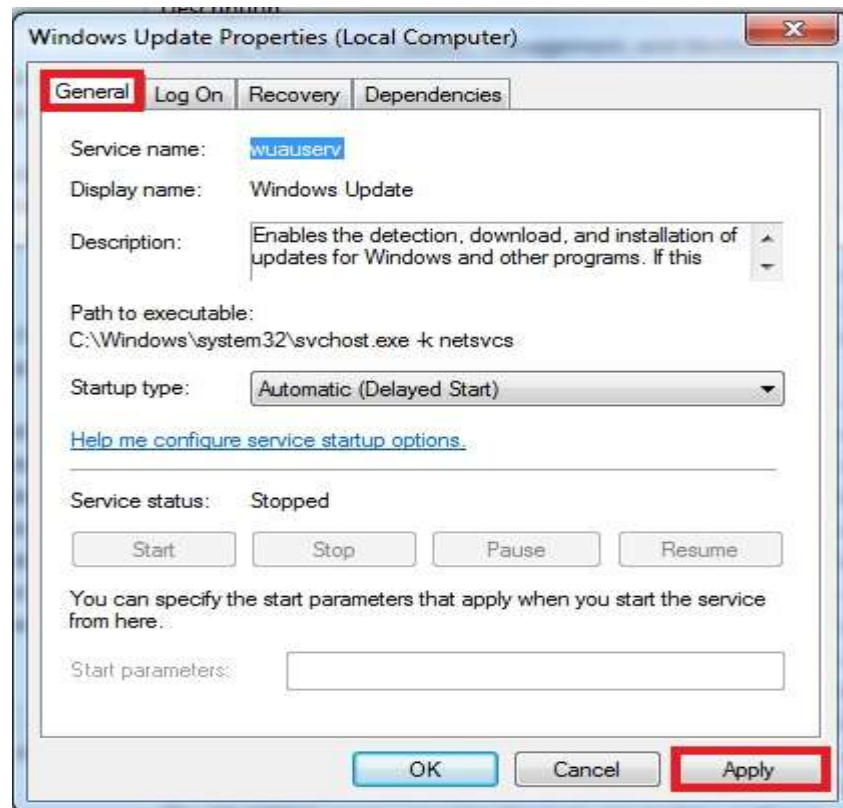
13. Check start-up type and then select *automatic*



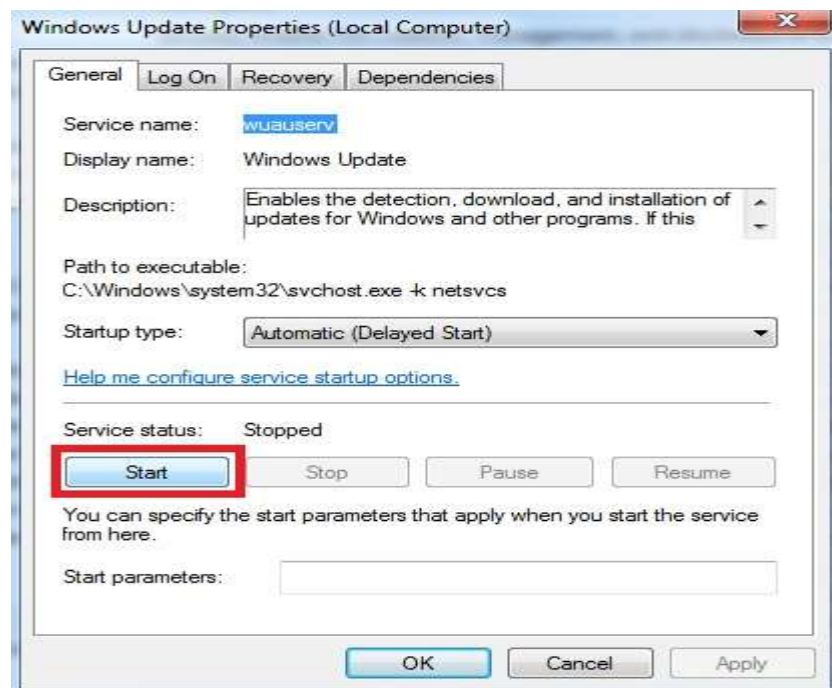
14. Then go to *recoverytab* and then *select first failure type to restart the service*



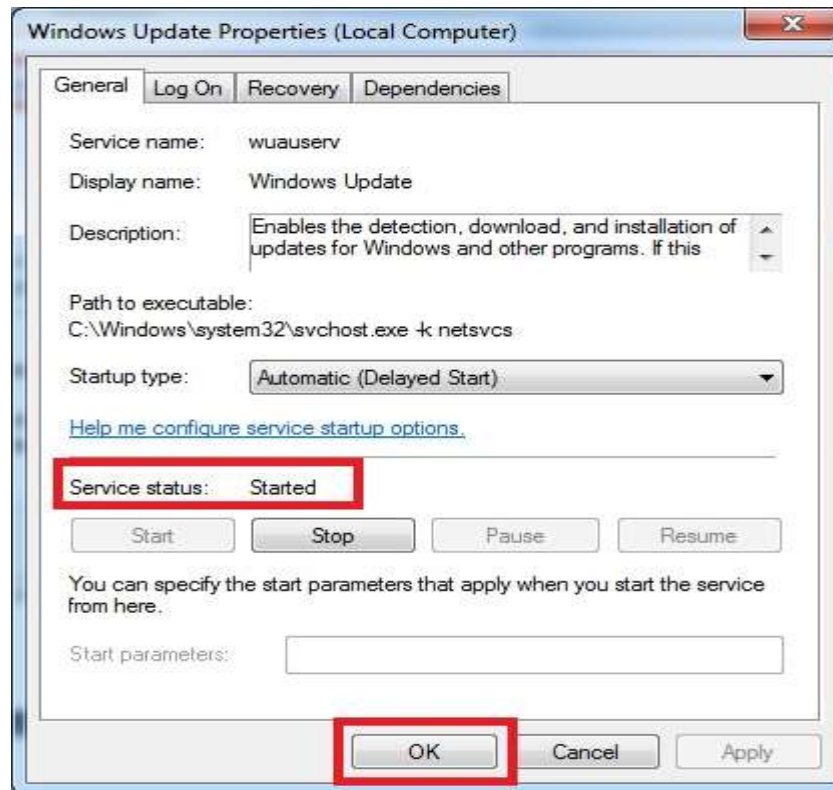
15. Go to **general tab** and then **select option apply**



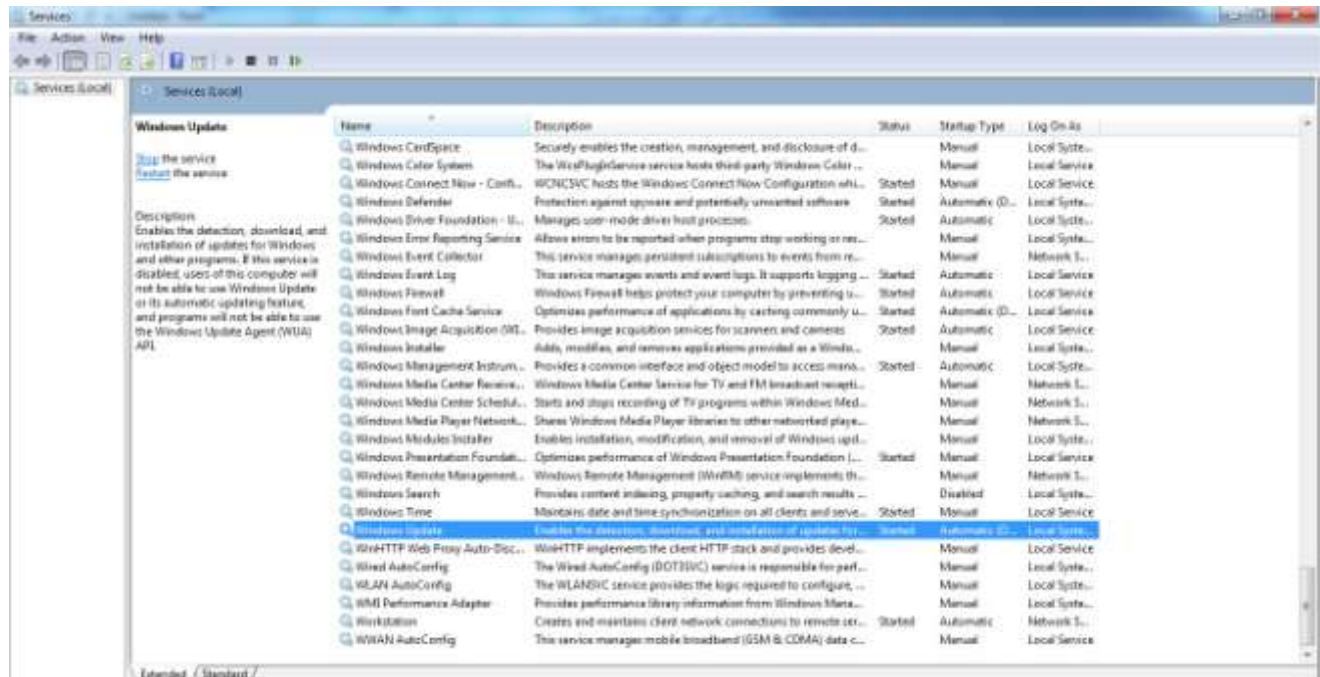
16. After that the start button will be active and click on start button on the window



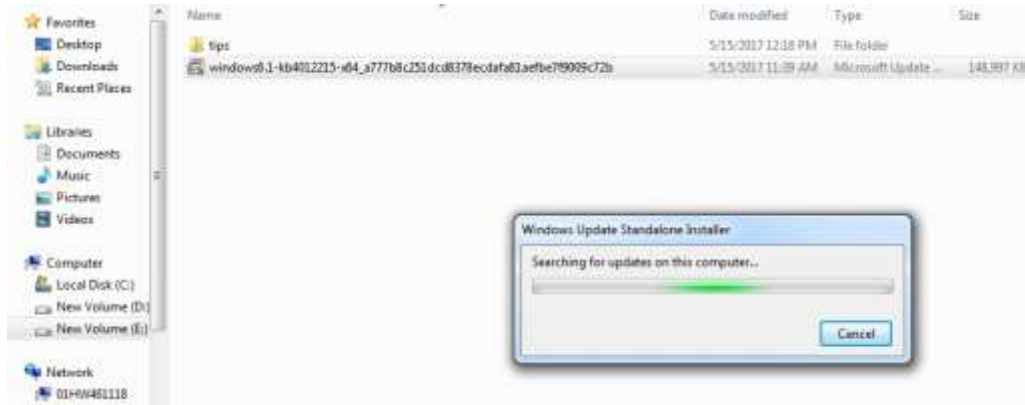
17. Then select Ok



18. Then the window shows status like started



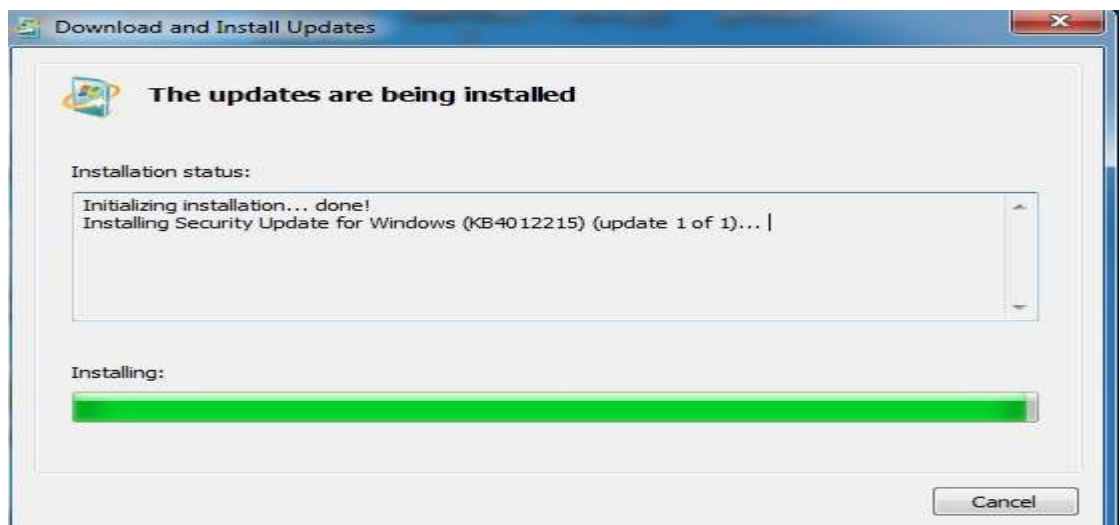
19. Double click the installation file already downloaded and then new window shown like below will be displayed.



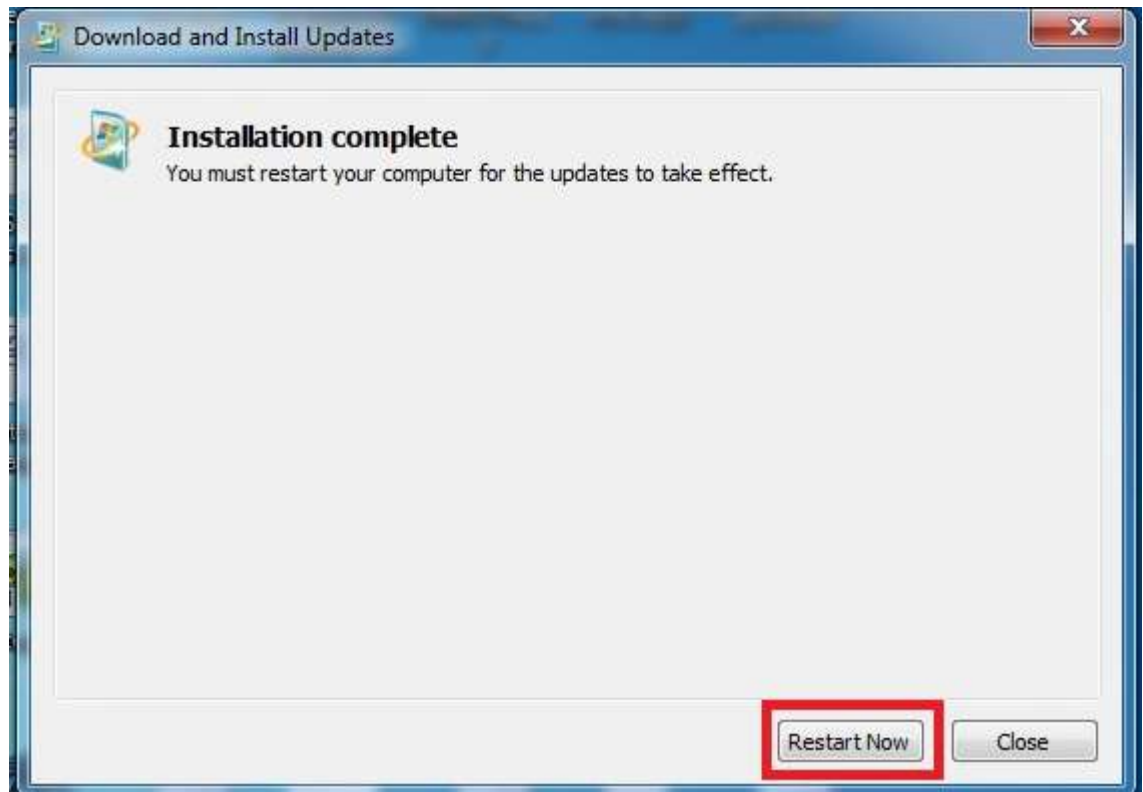
20. Select yes on the message box



21. Installation begins



22. Select Restart option on the final box displayed



## SMB

The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Using the SMB protocol, an application (or the user of an application) can access files or other resources at a remote server. This allows applications to read, create, and update files on the remote server. It can also communicate with any server program that is set up to receive an SMB client request.

### How to Disable SMB on Windows Machines to prevent WannaCry

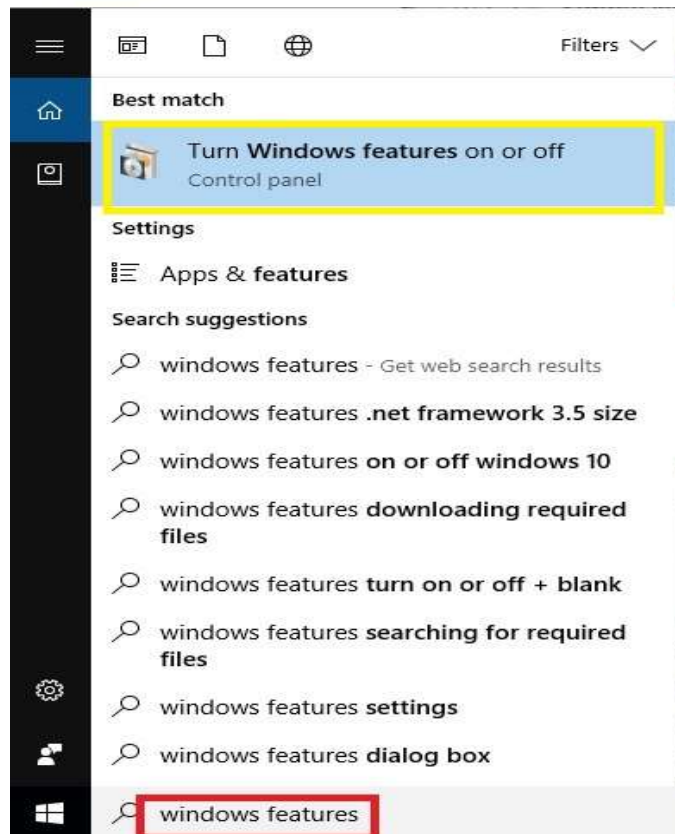
#### Ransomware

Before proceeding further it is strongly advised to take a backup of the machine because you will in some case might require to change the Windows Registry. If the steps are not carefully followed it might even crash the machine.

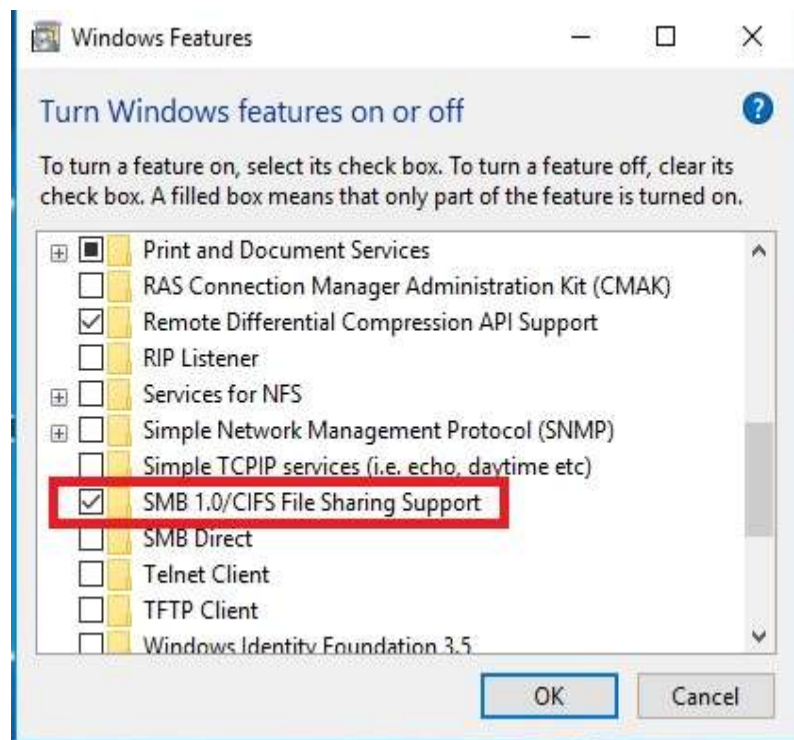
#### For Windows 10/8/7

Windows users can disable the SMB feature by following these simple steps:

1. Click on the **Search option** and search for **“Windows Features”** and you will see the result as **“Turn Windows Feature on and off.”**

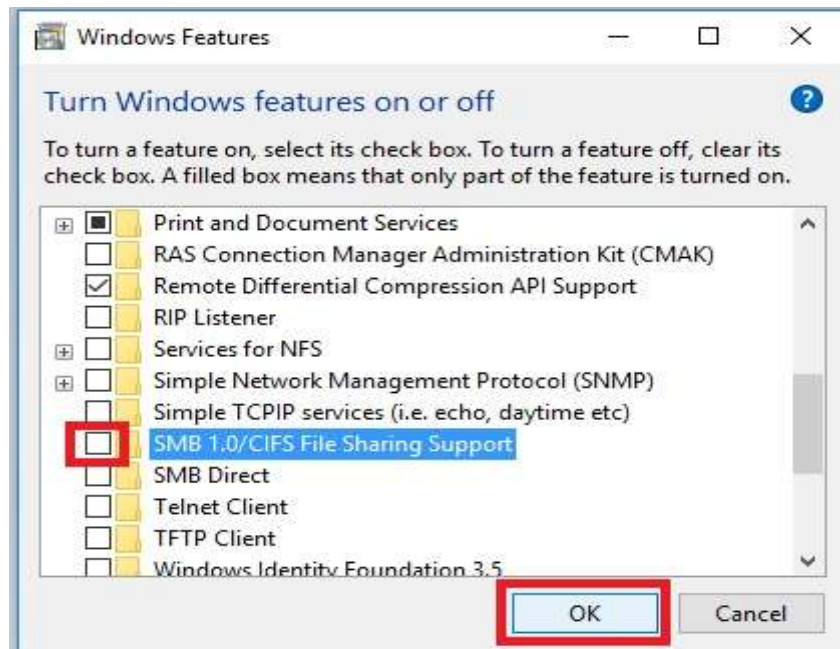


2. Upon clicking the option, the following screen will be prompted:

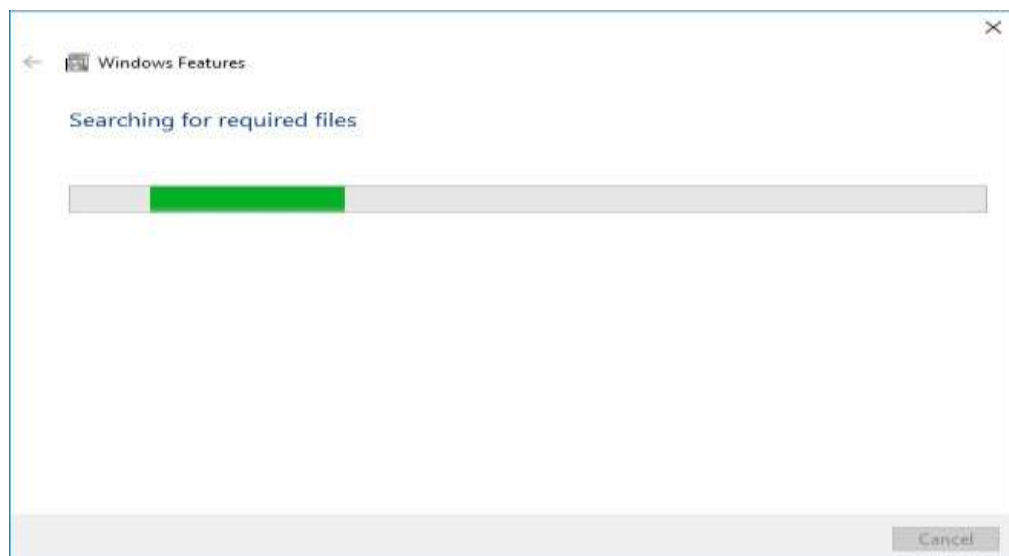




3. Now **untick the box** and **click on “Ok”**.



4. Wait for some moments when displaying the following window:





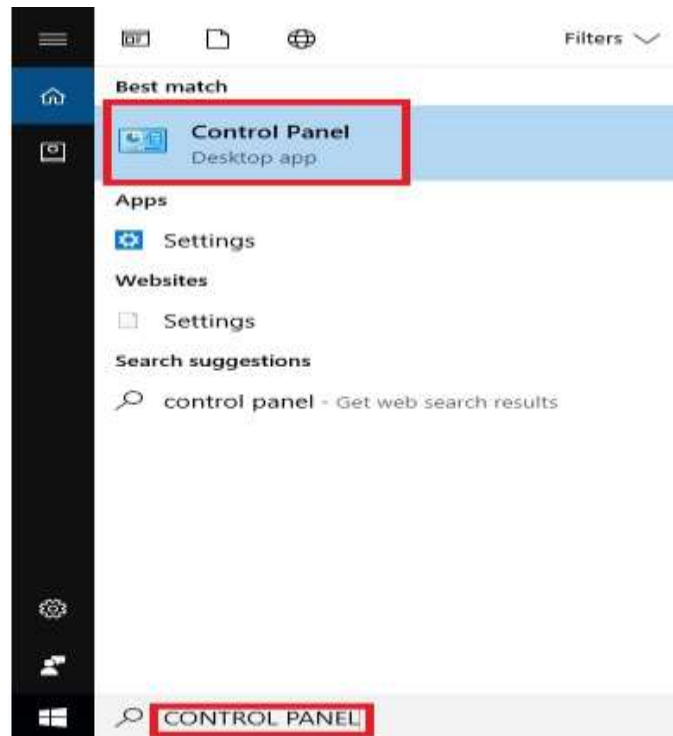
5. Finally the completed wizard displayed **click restart** button



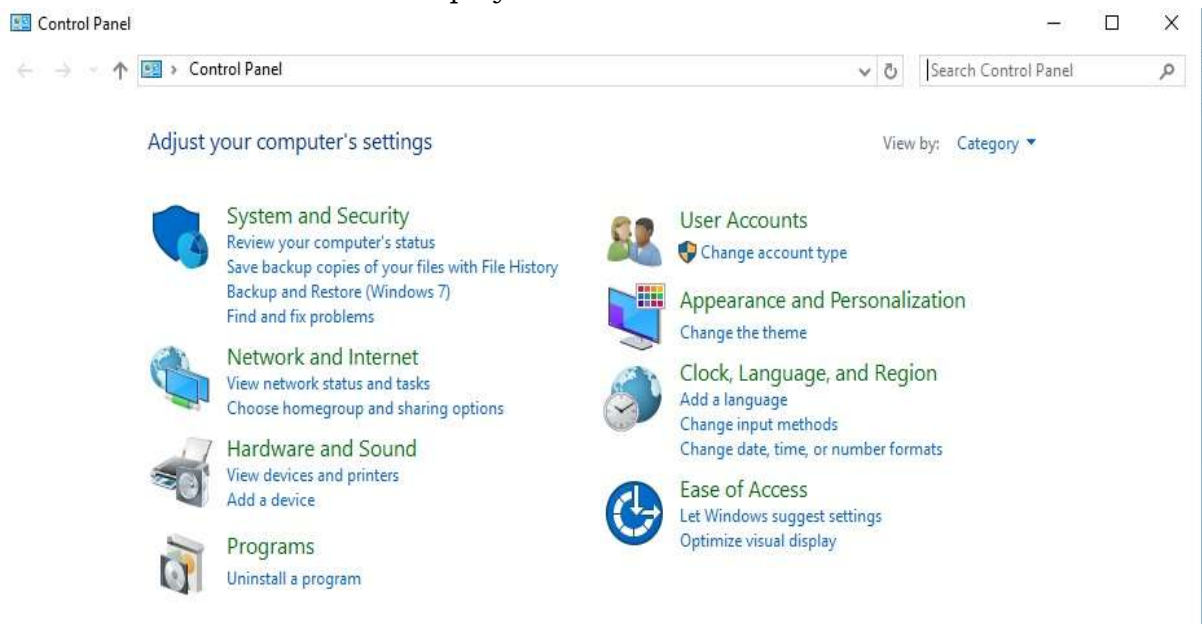
## **BLOCK PORTS**

### **How to block all traffic requesting port 445**

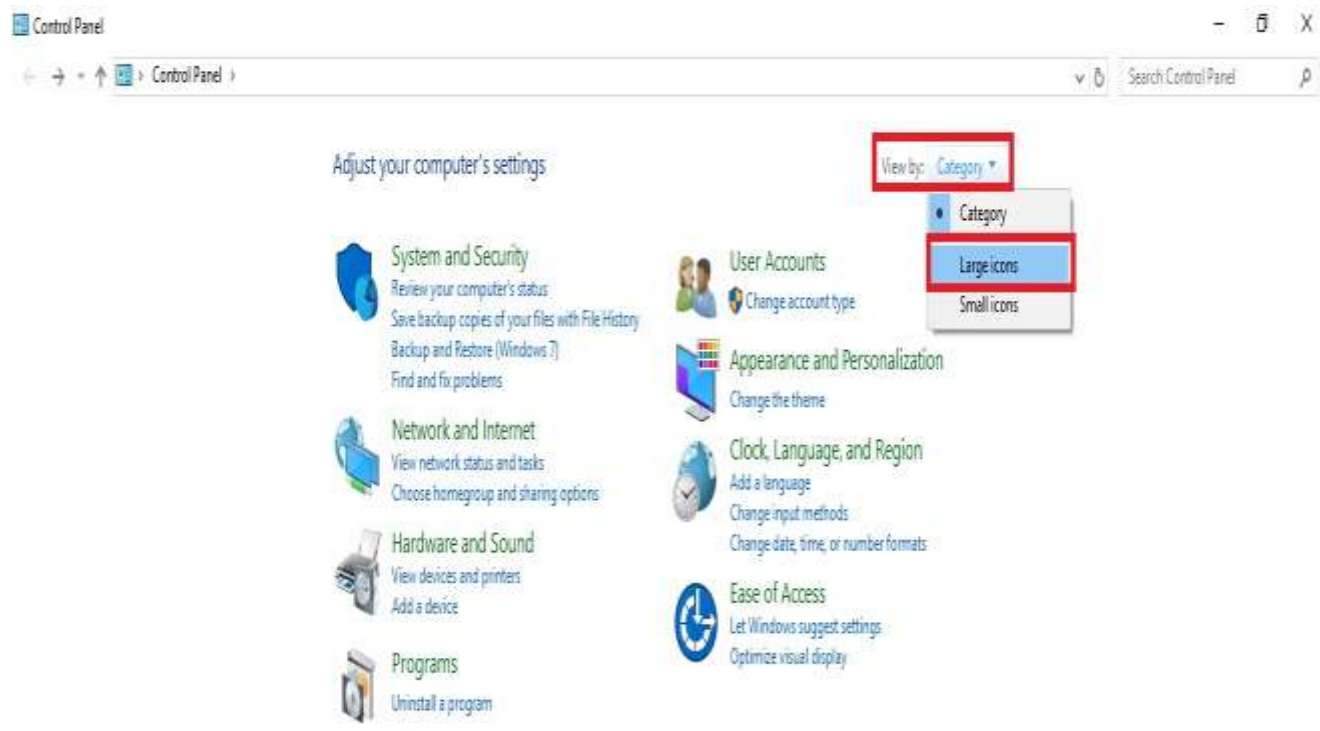
1. Open **Control Panel** from the Start menu.



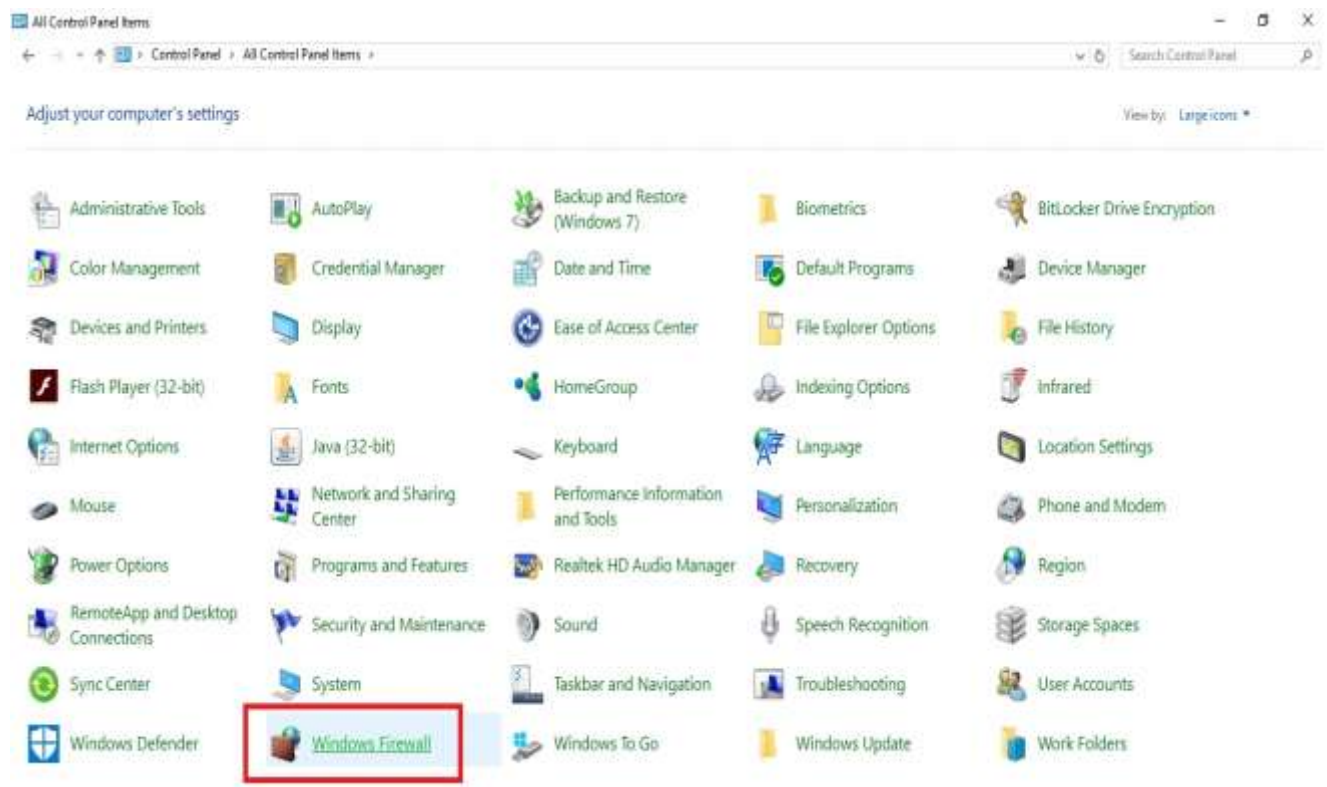
2. The window shown below is displayed



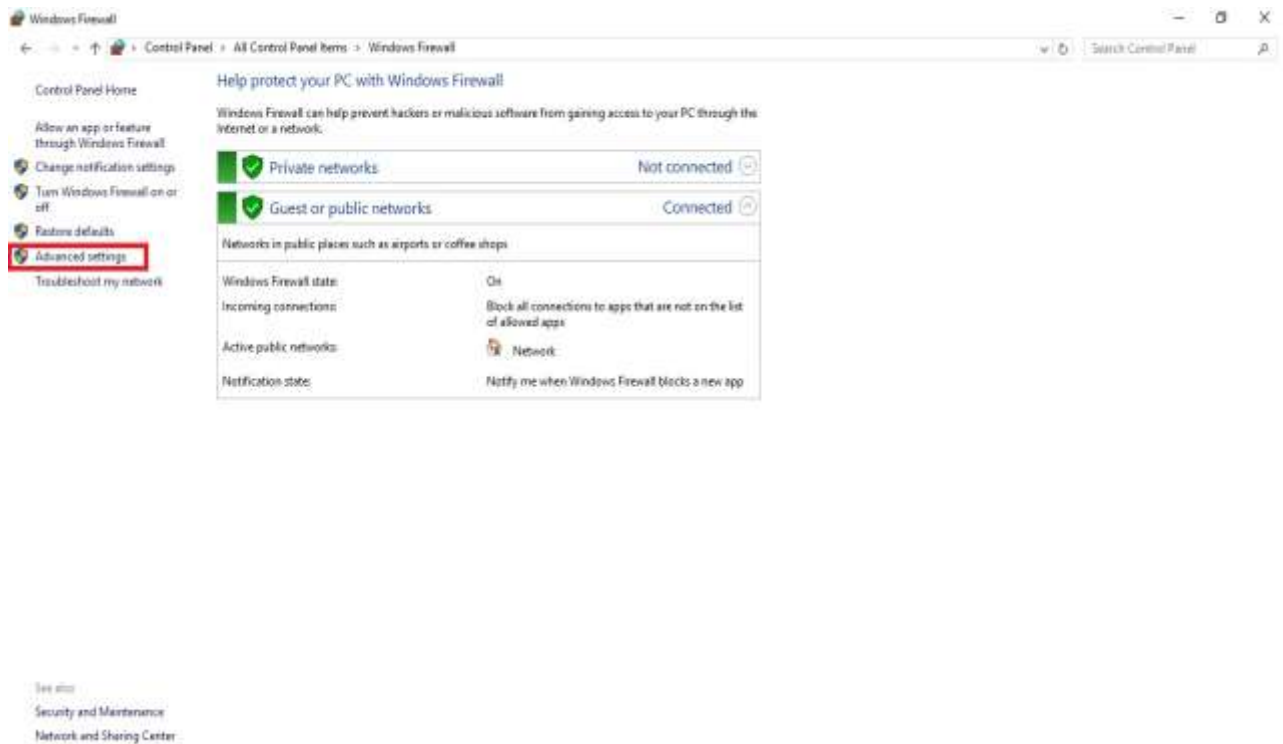
3. If windows firewall option present on the above window then go to step: otherwise select the **large icons options** from the dropdown box



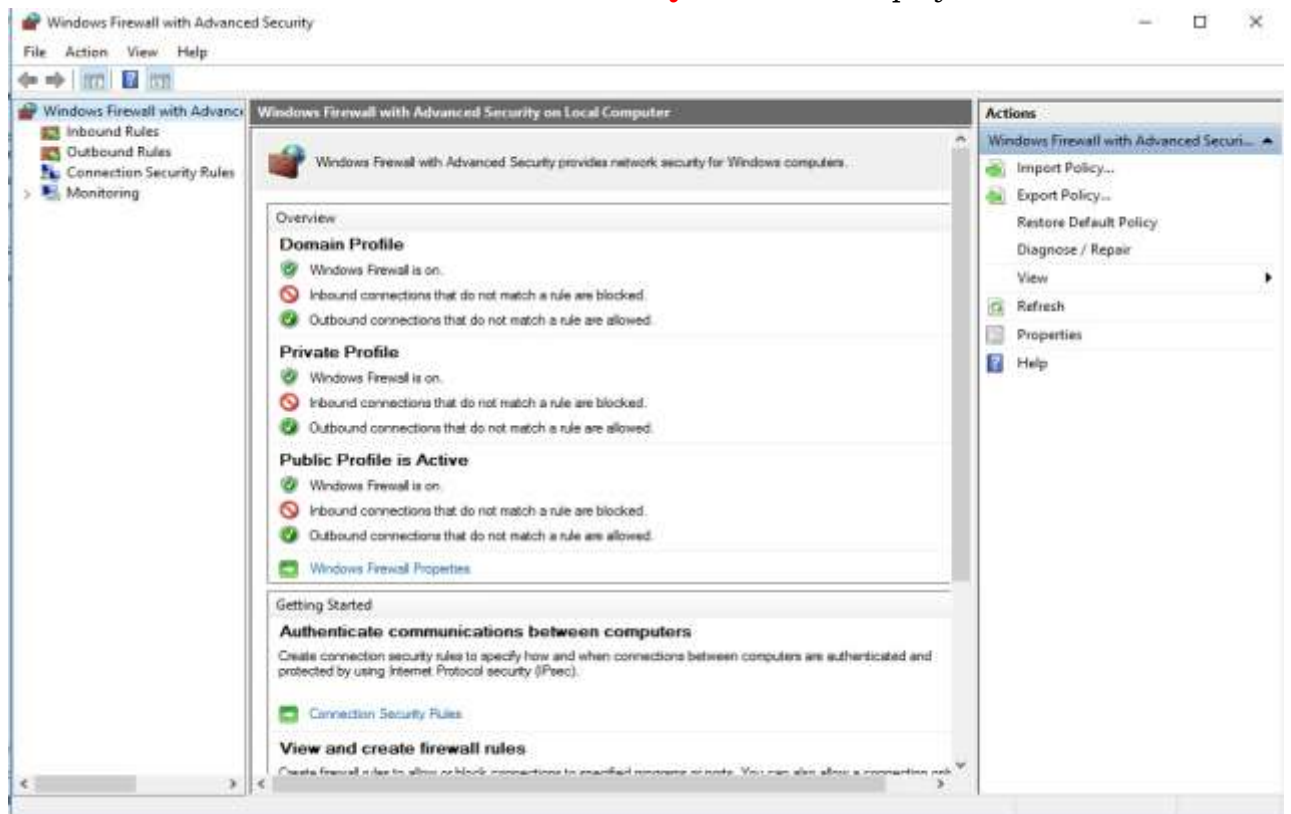
4. Select **windows firewall** option and **click** on it



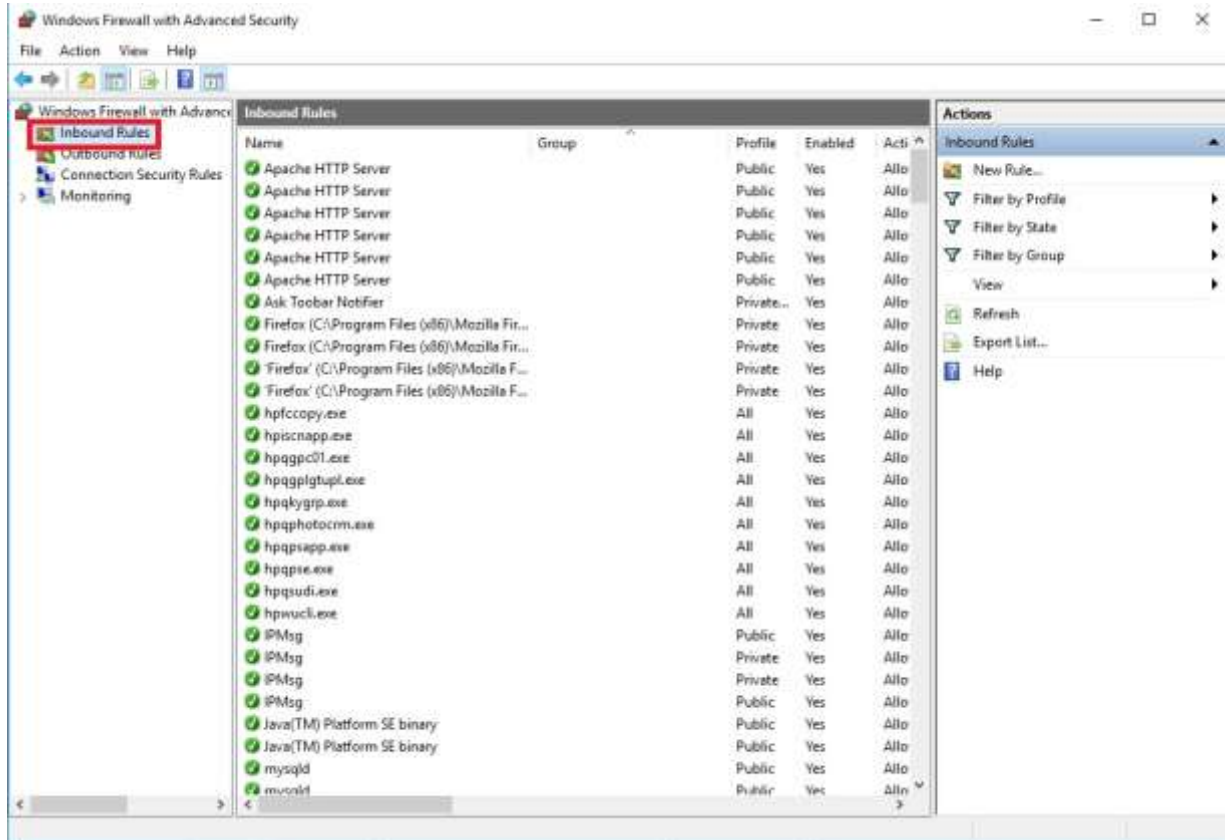
- On the **windows firewall window** displayed, select **advanced setting** option from the left side.



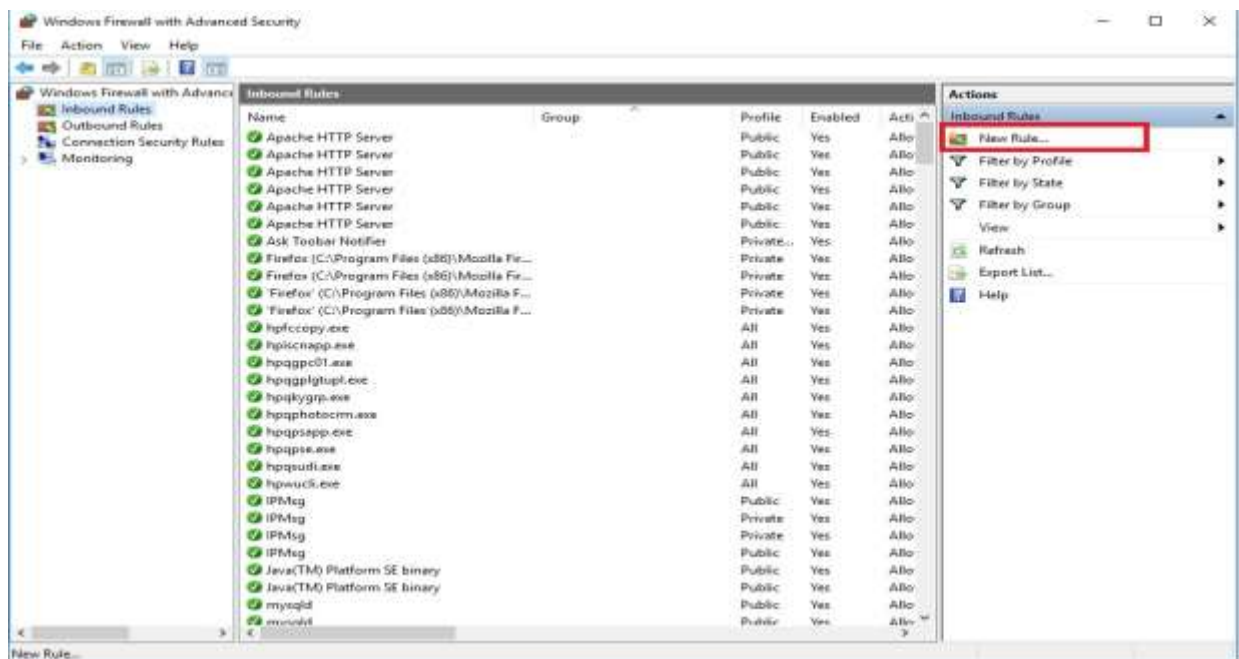
- The **windows firewall with advanced security** window is displayed



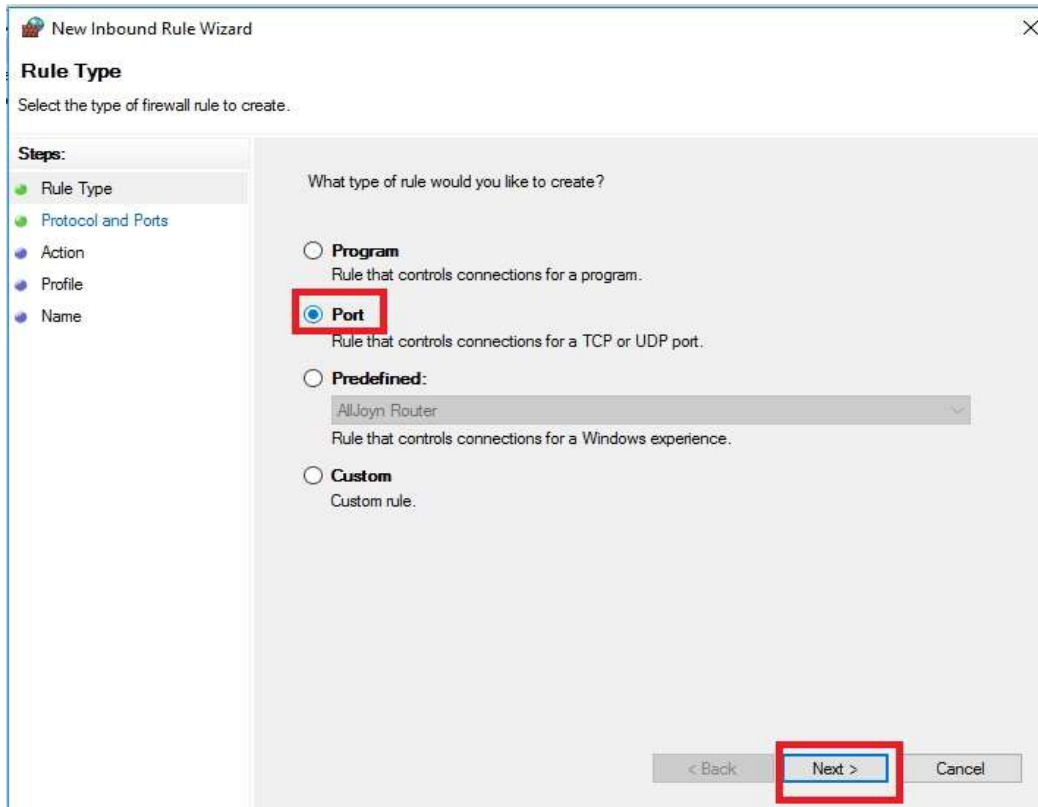
7. **Select** the **Inbound Rules** option displayed on left side of the window



8. Then **select** the **New Rules** option displayed on right side of the window

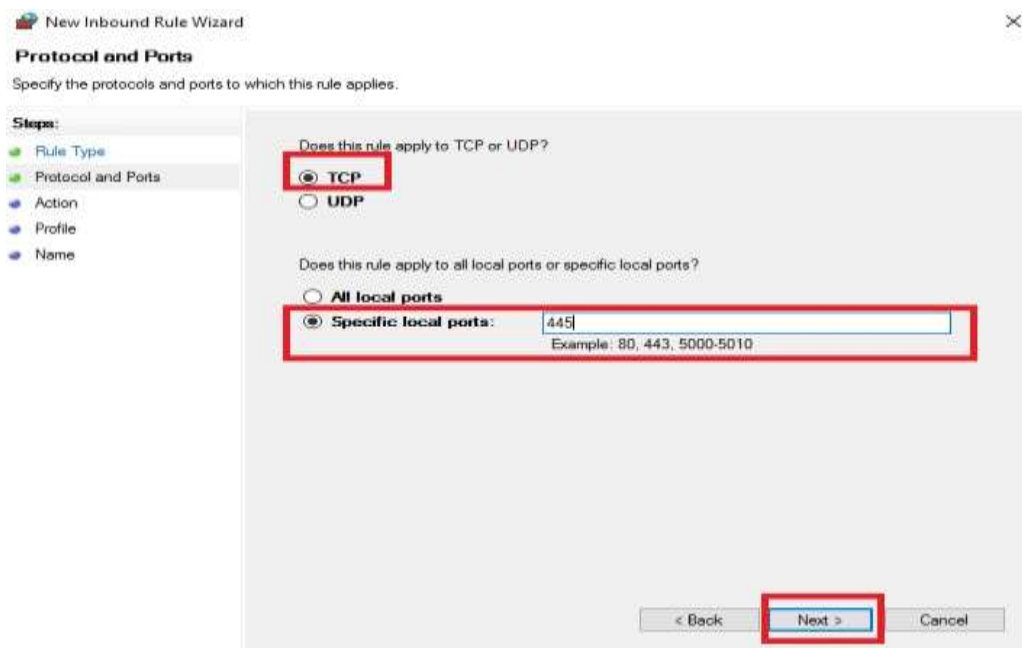


9. **New Inbound Rule Wizard** is displayed & Select **Port** and then **click Next** as shown below:



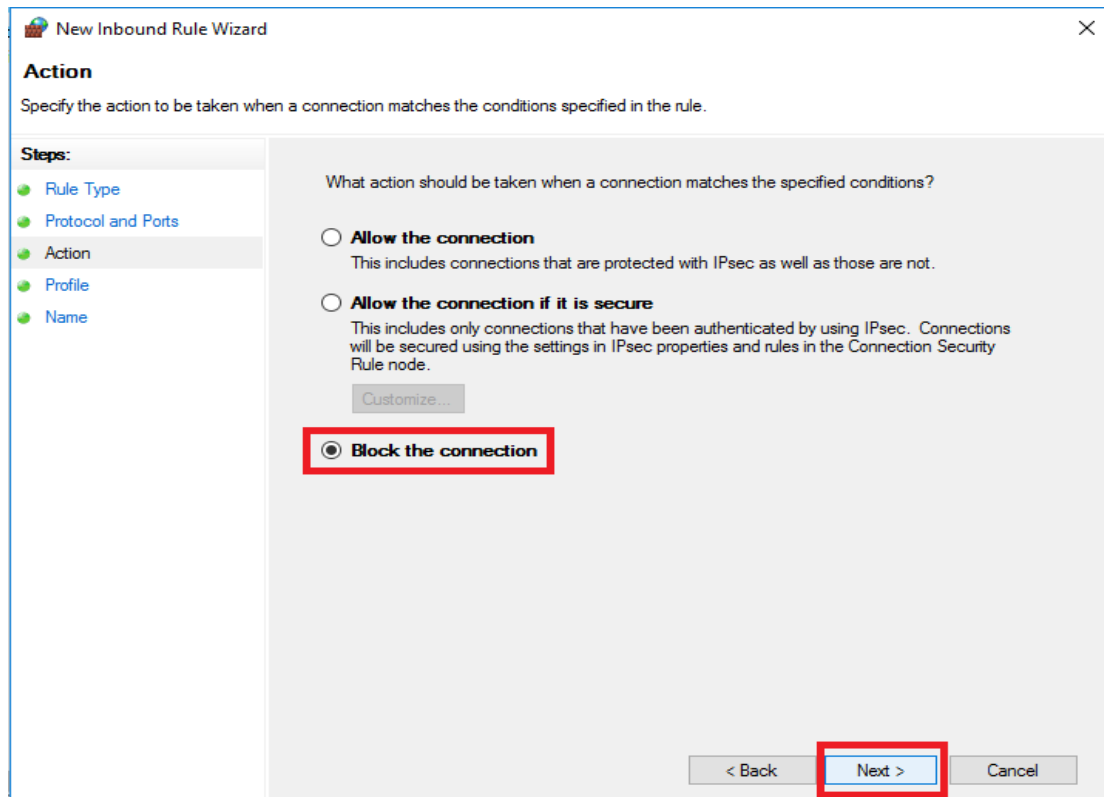
The screenshot shows the 'New Inbound Rule Wizard' dialog box. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.'. On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?' and offers four options: 'Program' (Rule that controls connections for a program.), 'Port' (Rule that controls connections for a TCP or UDP port.), 'Predefined:' (with a dropdown menu showing 'AllJoyn Router' and the description 'Rule that controls connections for a Windows experience.'), and 'Custom' (Custom rule.). The 'Port' option is selected and highlighted with a red box. At the bottom right, the 'Next >' button is also highlighted with a red box, along with '< Back' and 'Cancel' buttons.

10. On the next page **select TCP** and **select Specific local ports** and on the **text box type:445** and then **click Next**.

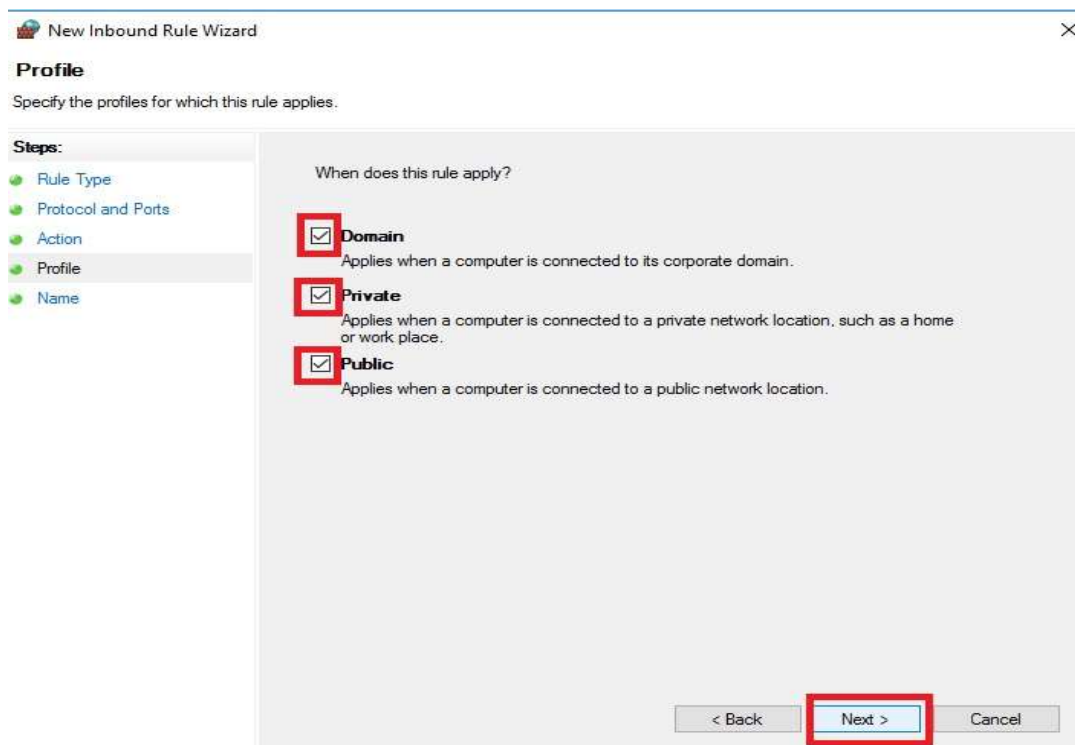


The screenshot shows the 'New Inbound Rule Wizard' dialog box at the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.'. On the left, the 'Steps:' pane shows 'Rule Type' and 'Protocol and Ports' as completed steps. The main area asks 'Does this rule apply to TCP or UDP?' with 'TCP' selected and highlighted by a red box. Below, it asks 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports:' selected and highlighted by a red box. A text input field next to it contains '445' and is also highlighted by a red box. Below the input field, an example is shown: 'Example: 80, 443, 5000-5010'. At the bottom right, the 'Next >' button is highlighted with a red box, along with '< Back' and 'Cancel' buttons.

11. On the next page **select Block the connection** and then **click Next**.

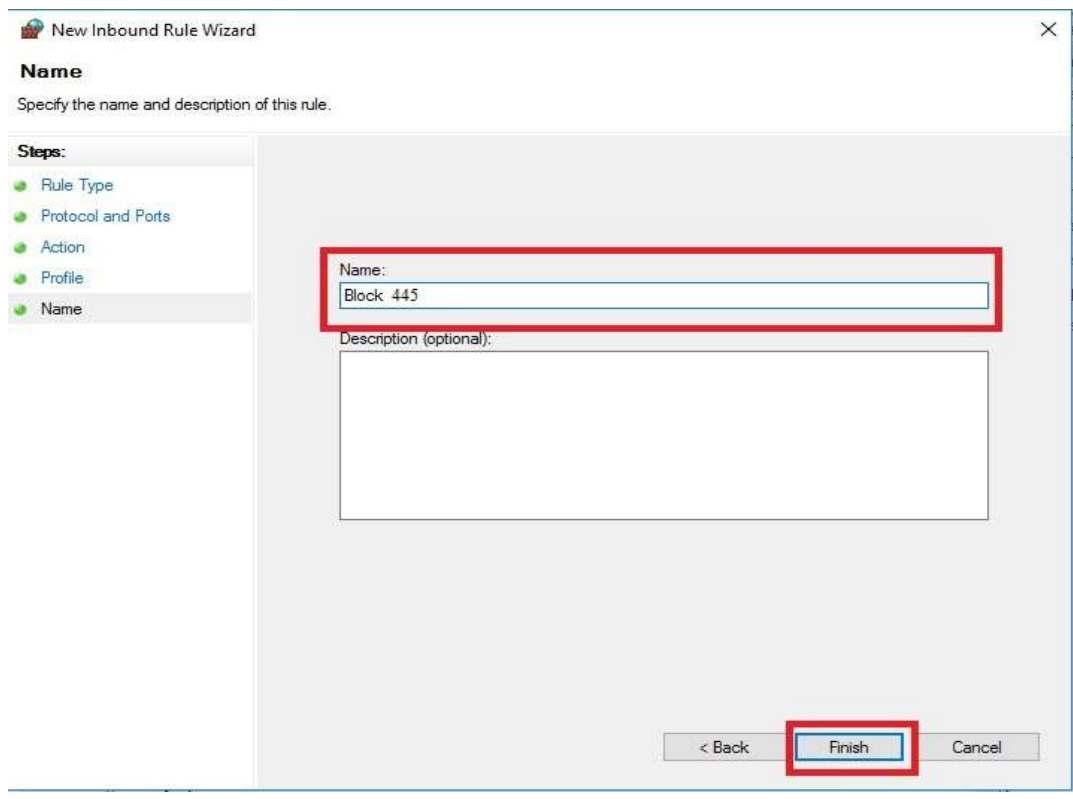


12. **Tick** all the options **Domain, Private, Public** as shown below & then **click Next**





13. On the next window **give any name** to identify the rules created now **example: Block 445** as shown below and then select Finish.



New Inbound Rule Wizard

**Name**  
Specify the name and description of this rule.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:  
Block 445

Description (optional):

< Back **Finish** Cancel

## Recovery measures from Ransomware Attack

**Disconnect and Isolate the affected machine from entire network/internet. Do not connect any external USB medium like Pendrives, Harddisks, to the infected machine. Be cautious on while copying any files from the infected machine's hard disk during the recovery process.**

### 1) If your web browser is locked

You can try to unlock your browser by using Task Manager to stop the web browser's process:

1. Open Task Manager. There are a number of ways you can do this:
  - **Right-click** on an empty space on the taskbar and click **Task Manager** or **Start Task Manager**.
  - Press **Ctrl+Shift+Esc**.
  - Press **Ctrl+Alt+Delete**.
2. In the list of **Applications** or **Processes**, click on the name of your web browser.
3. Click **End task**. If you are asked if you want to wait for the program to respond, click **Close the program**.
4. In some workplaces, access to Task Manager may be restricted by your network administrator. Contact your IT department for help.

When you open your web browser again, you may be asked to restore your session. Do not restore your session or you may end up loading the ransomware again.

### 2) If your PC is locked

- **Method 1: Use the Microsoft Safety Scanner in safe mode**



First, download a copy of the [Microsoft Safety Scanner](#) from a clean, non-infected PC. Copy the downloaded file to a blank USB drive or CD, and then insert it into the infected PC.

Try to restart your PC in safe mode:

- [In Windows 10](#)
- [In Windows 8.1](#)
- [In Windows 7](#)
- [In Windows Vista](#)
- [In Windows XP](#)

When you're in safe mode, try to run the Microsoft Safety Scanner.

- **Method 2: Use Windows Defender Offline**

Because ransomware can lock you out of your PC, you might not be able to download or run the Microsoft Safety Scanner. If that happens, you will need to use the free tool Windows Defender Offline. please go through the link below

<https://support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc>

### **3) Steps you can take after your PC has been cleaned**

Make sure your PC is protected with antimalware software.

Microsoft has [free security software](#) that you can use:



- If you have Windows 10 or Windows 8.1, your PC comes with antimalware software: [Windows Defender](#).
- If you're using Windows 7 or Windows Vista, you should install antimalware software, such as [Microsoft Security Essentials](#).
- You can update Microsoft security software on Microsoft [updates page](#).

If you don't want to use Windows Defender or Microsoft Security Essentials, you can download other security software from another company. Just make sure it is turned on all the time, fully updated, and provides real-time protection.

**Refer:- Microsoft Advisory**

<https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>