

#### ന്തതന സൈബർ ആക്രമണങ്ങൾ പ്രതിരോധിക്കാനുള്ള നിർദേശങ്ങൾ.

ഇന്നലെ മുതൽ ആഗോളവ്യാപകമായി രണ്ടു പുതിയ തരം കമ്പ്യൂട്ടർ റാൻസംവെയറ്റകൾ )Ransomware) പ്രചരിക്കുന്നതായി അറിയുന്നുകമ്പ്യൂട്ടറിൽ ഇവ ബാധിച്ചാൽ പ്രധാനപ്പെട്ട ഫയലുകളെ . ഇവണ്ലോക്ക് ചെയ്യുന്നു, പിന്നീട് അവ ഇറന്നു കിട്ടണമെങ്കിൽ ഓൺലൈൻ കറൻസി ആയ ബിറ്റ് കോയിൻ നിക്ഷേപിച്ചു മോചിപ്പിച്ചെടുക്കേണ്ട അവസ്ഥയാണ് ബ്രിട്ടനിലെയും സ്പെയിനിലെയുമൊക്കെ . സർക്കാർ സംവിധാനത്തെയും ഫെഡ് എക്സ് ഇടങ്ങിയ കമ്പനികളെയും ഇവ ഇരുതരമായി ബാധിച്ചുവെന്ന് ഈ രംഗത്തെ വിദഗ്ദ്ധർ അറിയിക്കുന്നലെകളെയാണ് പ്രധാനമായും ആശുപത്രി ശൃംഖ . ഇവ ലക്ഷ്യം വച്ചിട്ടുള്ളത് എന്നാണ് മനസ്സിലാക്കുന്നത് ഇത്തരം സൈബർ ആക്രമണങ്ങൾക്കെതിരെ . അപരിചിതമായ ലിങ്കുകൾ .ജാഗ്രത പാലിക്കേണ്ടത് അത്യാവശ്യമാണ്, സംശയാസ്പദമായ ഇ -മെയിലുകൾ, അവയിലെ അറ്റാച്ച് മെന്റുകൾ എന്നിവ ഇറക്കാതെ നോക്കുക, നിങ്ങളുടെ കമ്പ്യൂട്ടറിലെ ആന്റി വൈറസ് അപ്ഡേറ്റ് ചെയ്ത് വേണ്ട മുൻകരുതലുകൾ എടുക്കണം.

#### അതോടൊപ്പം താഴെ പറയുന്ന നിർദേശങ്ങൾ കൂടി കൃത്യമായി പാലിക്കേണ്ടതാണ് .

1 ) സംശയാസ്പദമായ സാഹചര്യത്തിൽ കിട്ടുന്ന ഇമെയിൽകൾ ഓപ്പൺ ചെയ്യുകയോ അന്ദബന്ധ അറ്റാച്മെന്റകൾ തുറക്കാതിരിക്കുകയോ ചെയ്യുക.

2) വിശ്വാസയോഗ്യമല്ലാത്ത സ്രോതസ്സുകളിൽ നിന്നും വരുന്ന മെയിലുകൾ, ലിങ്കുകൾ തുടങ്ങിയവയുടെ ആധികാരികത ഉറപ്പ വരുത്തിയ ശേഷം മാത്രം തുറക്കുക

3) വ്യക്തിപരമോ, സാമ്പത്തികമോ ആയ വിവരങ്ങൾ ആവശ്യപ്പെട്ടുകൊണ്ടുള്ള അമ്പേഷണങ്ങൾക്ക് മറുപടി നൽകേണ്ടതില്ല.

4) മെയിൽ സന്ദേശങ്ങളുടെ ആധികാരികത ഉറപ്പവരുത്തുക.

5) വ്യക്തിപരമായി പുകഴ്ഛന്ന മെയിലുകൾ,മനഃപൂർവം വരുത്തുന്ന പിശകുകൾ എന്നിവ സസൂക്ഷൂം നിരീക്ഷിച്ച മെയിലുകൾ കൈകാര്യം ചെയ്യുക.

6 ) ഇമെയിൽ അറ്റാച്മെന്റകൾ സസൂക്ഷൂം തുറക്കുക.

7) മെയിൽ വഴി ലഭ്യമാവുന്ന ഫോമുകളിൽ വ്യക്തിപരമായ വിവരങ്ങൾ നൽകാതിരിക്കുക.ഇത്തരം വിവരങ്ങൾ ട്രാക്ക് ചെയ്യപ്പെടാൻ സാധ്യത ഉള്ളതിനാൽ ആണിത്.

8) വ്യക്തിഗത വിവരങ്ങൾ കൈമാറുന്നതിന് മുൻപ് വെബ്സൈറ്റിന്റെ ആധികാരികത ഉറപ്പ വരുത്തുക.

9) ഔദ്യോഗിക ഇമെയിലുകൾ വ്യക്തിപരമായ ആവശ്യങ്ങൾ ഉപയോഗിക്കാതിരിക്കുക.

10 ) സമൂഹമാധ്യമങ്ങളിൽ സംശയകരമായ സാഹചര്യങ്ങളിൽ നിന്ന് ലഭിക്കുന്ന ഇമേജുകൾ, വീഡിയോകൾ തുറക്കാതിരിക്കുക.

11 ) സമ്മാനങ്ങൾ ഓഫർ ചെയ്തകൊണ്ടുള്ള മെയിൽകൾക്ക് സാമ്പത്തിക വിവരങ്ങൾ നൽകരുത്.



12 ) ബാങ്ക് വിവരങ്ങൾ ആവശ്യപ്പെട്ടുകൊണ്ടുള്ള വിവരങ്ങൾക്ക് മറുപടി നൽകാതിരിക്കുക.

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

# **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.



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

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

TN Microsoft Security Baller X	6		🖾 - o x
← → C ① B Secure Inte	ss://technet.microsoft.com/en-us/library/security/ms17-018.aspx		\$ 0 M
Microsoft   TechNet ~			Onited States (Explicit) — Eign in
Security TechCenter		Search TechNet with Bing	P
Home Security Updates 3	ools Learn Bbrary Support		
Security Advisories and Bulletins >	Security Bulletins > 2017 -		
M517-013	Microsoft Security Bulletin MS17-010 -	Critical	ட் Pent < Share
M517-012 M517-011	Security Update for Microsoft Windows SMB Server (40133 Published: March 14, 2017 Version: 1.0	89)	IN THIS ARTICLE
M517-010 M517-009	Executive Summary This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities	On this page Executive Summary	Affected Software and Vulnerability Seventy Ratings
M517-008	could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.	Affected Software and Vulnerability Seventy Ratings	Information Security Unitate
M517-007	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.	Vulnerability Information	Deployment Acknowledgments
MS17-006	The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.	Acknowledgments	Disclaimer
M517-009	For more information about the vulnerabilities, see the Vulnerability Information section.	Disclamer	[as as the star

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



X 🖸 🕯 Secure	https://technet.	microsoft.com/in-	a/itinaŋ/wecum	y/mi17-010.acp	í					¥ 0 M
		(4012598)								
		Windows 7								
MS17-012 MS17-012 MS17-011		Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Onig[1]	Critical Remote Code Execution	Critical Remote Code Execution	Critical Hemote Code Execution	Critical Remote Code Execution	Important Information Disclosure	Critical Remote Code Execution	None	Shine     Shine     Shine     IN THES ARTICLE
MS17-010		Windows 7 for	Critical	Critical	Critical	Critical	Important	Critical	3212646	Affected Software a
M517-009		32-bit Systems Service Pack 1 (401/2215)	Remote Code Execution	Remote Code Execution	Remote Code Execution	Remote Code Execution	Disclosure	Remote Code Execution		Vulnerability Second Ratings Vulnerability
M517-028 M517-007		Manthly Rottup <sup>[1]</sup>								Security Opdate Deployment
MS17-006		Windows 7 for x64-based	Critical Remote Code Execution	Critical Remote Code	Critical Remote Code	Critical Remote Code Execution	Important Information	Critical Remote Code	None	Acknowledgments Disclaimer
M517-005		Service Pack 1 (4012212)			0.04641900	0.0000000	- 160 0000 ()	10002454.01		Revision
M517-004		Security Only[1]								
M517-028		Windows 7 for	Critical	Critical	Critical	Critical	Important	Critical	3212646	
M512-002		Service Pack 1	Execution	Execution	Execution	Execution	Disclasure	Besution		
MS17-001		(4012215)								

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:

C 🕜 () www.catalogupdate.microsoft.com/Search.aspx?q=KB4012215						±0 ₩ :
osoft Update Catalog			KB4012	215		Search
earch results for "K84012215"						
es: 1 - 6 af 6 (page 1 af 1)						(p Previous   Next <sub>cip</sub>
Tite	Products	Classification	Last Updated	Version	Size	
March, 2017 Security Monthly Quality Rollup for Windows 7 (884012215)	Windows 7	Security Updates	3/12/2017	s/a	89.0 MB	Download
March, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (K84012215)	Windows Server 2008 R2	Security Updates	3/12/2017	1/2	145.5 MB	Download
March, 2017 Security Monthly Quality Rollup for Windows Embedded Standard 7 (K84012215)	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 (K3401221	Windows Server 2008 R2	Security Updates	3/12/2017	6/2	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 Rolling for Windows Embedded Standard 7 for old-based Systems (8840)	215) Windows Embedded Standard 7	Security Lipdates	3/12/2017	n/z	145.5 MR	Download

2017 Microsoft Corporation. All Rights Reserved. | privacy | terms of use | help



#### 4. On the download page

Click: *windows6.1-kb4012215-x64\_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.msu*as shown below:

🗅 Microsoft Update Catalog - Google Chrome		<u></u> :		$\times$
www.catalog.update.microsoft.com/DownloadDialog.aspx				
Download				
Download Updates				
March. 2017 Security Monthly Quality Rollup for Windows 7 fo windows6.1-kb4012215-x64_a777b8c251dcd8378ecdafa81aefbe7f9	r x64-based Systems (1 1009c72b.msu	(B4012	2215)	
			Close	-
40.77.232.90				

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.

Microsoft Update Catalog - Google Chrome	100		$\times$
Www.catalog.update.microsoft.com/DownloadDialog.aspx			
Download			
Download Updates			
March, 2017 Security Monthly Quality Rollup for Windows 7 for x64-b windows6.1-kb4012215-x64_a777b8c251dcd8378ecdafa81aefbe7f9009c7;	based Systems (KB401. 25.msu	2215)	
download.windowsupdate.com//win		Close	
	(	10 10	1 30

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

🗋 Microsoft Update Catalog -	Google Chrome	1444		$\times$
www.catalog.update.mi	crosoft.com/DownloadDialog.aspx			
Download				
Download Updates				
March, 2017 Security Mo windows6.1-kb4012215-x6	nthly Quality Rollup for Windows 7 for x64-based 4_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.ms	I Systems (KB401)	2215)	
	Open Always open files of this type			
40.77.232.90	Show in folder Cancel		Close	ł
windows6.1-kb40m	su 🔽	S	show all	×



8. Double click the installation file

🛊 Favorites 🔺	Name	Date modified	Туре	Size
E Desktop Downloads	🛃 windows5.1-kb4012215-x64_a777b8c251dcd8378ecdafa81aefbe7f900	9c72b 5/15/2017 11:39 AM	Microsoft Update	148,997 KB
Libraries				
Music				
Videos				
Computer				
👗 Local Disk (C:)				
🕞 New Volume (D:)				
🕞 New Volume (E)				

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

rograms (1)		
162 services		
See more results		
See more results services.mscl	× 5	hut down 🕨



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

ienvices (Local)	Services (Lance)						
	Windows Update	Name	Description	30541	Same Type	LegOnAs	
	Description Enables the statistics, skewellast, and installation of applicate for Windows and other programs. If this assess in disaded, uses of the computer with on the state uses of the computer with on the state state on Windows (padding of the statements of one take state save the Windows Up date Agent (MUA) APD	Windows Calification     Windows Calification     Windows Calification     Windows Calification     Windows Calification     Windows Dates Nation     Windows Earch Reporting Service     Windows Faret Calification     Windows Faret Calification     Windows Faret Calification     Windows Nation     Windows Nation     Windows Mada Report     Windows Report     Windows Report     Windows Report     Windows Report     Windows     Windows Report     Windows     Windows	Security enables the contrion, management, and disclinate of di- The Weell kapfolimics and service house their pury Workson Color - WCNCSVC Faults the Workson Connect None Configuration while Databation applies and partnership variantical subscass Management to be reported when programs stop variant contrasts Management to be reported when programs stop variant contrasts Management to be reported when programs stop variant contrasts Management of the reported when programs stop variant form. This service management and event large. It supports larging a Windows Freewall helps ported your computer to protecting screen. This wave ensures and applications by variants and contents Adds, modifies, and remove applications provided as a Window. Provide a convension interface and signations provided in a content. Windows Natio Control Fermion 4 To protect the transmitted barrest and stops recording of TV programs while Windows stell. Data stops recording of TV programs while Windows and Optimizes performance of Windows Powershild Jacks, Patients Matelia Stops Management (WVMM) provide in pro- tection in the Stop Powershiles Transmitter To Management and Management (WVMM) provide in a store in Management and the powers while Windows Made Data in the second Windows Powershile Frankation 1. Windows Rescet Management (WVMM) provide in advance in Market and the powers while a store and and when Management and the powers while a store in advance in Market and the powers while a store and and when Management and the powers while a store in advance in Windows Rescet Management (WVMM) provide in advance in Market and the powers when a store and powers when the Management and the powers when a store and powers when Management and the powers when a store and powers when Management and the power and the store and powers when the Management and the power and the store and power and the store in WALARDC device powers the logic regularity to complete, to market and base powers the logic regularity for and power and the WALARDC device	Noted Sostel Sostel Sostel Sostel Sostel Sostel	Menual Menual Menual Automotic (D., Automotic Menual Automotic Automotic Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual Menual	Lood Syste Lood Service Lood Service Lood Service Lood Service Lood Syste Network 1. Lood Service Lood Service Lood Service Lood Service Lood Syste Lood Syste Lood Syste Lood Syste Lood Syste Lood Syste Lood Service Lood Syste Lood Service Lood Service Lood Service Lood Service Lood Service Lood Service Lood Syste Lood Service Lood Syste	
		C, KMI Performence Adapter C, Workstation C, WWAN AutoComfig	Provides performance library information from Windows Mana, Creates and maintains clare network connections to minute into This service manages mobile broadband (ESM & CONA) defe c	Ratel	Sitemael Automotic Mercuel	Local System Network E., Local Service	

12. On the option right click and then select properties

Services		and the second	Dances Blood State					ALC: NO.
File Action Ven	Heb							
Services Local	<ol> <li>Services Rocal)</li> </ol>							
	Windows Update	Name -	Description	Refus	Statue Type 1	Ag Ce As		
	Contraction (	a Windows Certifipate	Securely enables the creation, management, and disclosure of d		Menuel 1	ocel Syste		
	Excellent the state man altered and	Windows Color System	The WesPlugBellervice service hosts think party Windows Color		Manual L	anial Service	_	Louis and
Dis Action	Case Made							New York
**								
Services Boo	4. Service Broat							
	Windows Update	Aberra	Description	Status	Startus Tupe	Leg On As		
		C. Windows Canflance	Security makies the creation, management, and disclasure of a	-	Billamuch	Local System		
	Evables the detection download and	d 🔍 Windows Color System	The WcsPlugleGevice service hosts third-party Windows Color .		Marrout	Local Service		
	installation of updates for Waldows	Windows Connect Now - Cord		. Status	Billantunde	Lancal Service		
	and other programs. If this service is	Windhiss Defender	Protection egenet opywere and potentially unwanted software	Statut	Hutematic (0.	Local Syste		
	not be able to use Wendows Update	Windows Druer Foundation - 1	Manages user-mode driver host processes	Stated	Automatic	Lece Syste.		
	enits automatic updating feature,	Wedness Error Reporting Server	<ul> <li>Allows among to be replicited when programs dop working or re- This section between programs dop for the sector form.</li> </ul>		R. Barrisson	Local System		
	send programs will not be able to user the UKe (knot the date Assert OVDA)	Washing Frank Last	This service manages previously station provide to exercise normal.	Statut	indercostin.	Lecial Gambon		
	APL	G. Windows Fermal	Windows Rewall helps parted your computer by preventing w	Stated	Automatic	Local Service		
	1000	Westing Fort Cache Service	Optimizes parformance of applications by caching commonly a	. Shartan	Automati	And the last	-	
		Q Windows Image Acquisition (M	L. Provides image acquisition services for scenners and cameras	Stated	Automotic .	1000		
		🔍 Weedowe leenallar	Adds, modifies, and removas applications provided as a Winite.		Martual	199		
		G Windows Management Britrum	Provides a common interface and object model to access mana	Sated	Automati .	Emone		
		🔍 Windows Media Center Receivo	<ul> <li>Windows Media Carbin Service for TV and FM broadcast reception</li> </ul>		Riversaul	Relation		
		Windows Media Center Scheits	6 Starts and stops recording of TV programs within Windows Med	6	Atlanced	Finitert		
		Wentere Media Payer Return		t i	Metual	All Tarks		
		Windows Modules Installer	Enables installation, modification, and removal of Windows upd	-	Manual	1. Status	226	
		Weithout Presentation Presentation	<ul> <li>Optimizes participarties of thirdcost Presentation Presidential Models - Results Management of Initiality Presentation (2019)</li> </ul>	States	Riperson .	Eatrach		
		Washing Seath	<ol> <li>minipuls remote startigenere, providely service impendence on Decision context indexing acception and search configuration.</li> </ol>		Disabled	Properties		
		Windows Time	Moretanic date and time supchronization on all clerifs and serve	Stated	Manual			
		Western Lipster	Evaluation the determined should and restal after of cardidae for	-	Fratient	They .		
		Welefitte Web Proxy Auto-Dip			Manual	Local Service		
		Ca. Winud AutorCorrfig	The Wied AutoConfig (DOF3SVC) service is reportable for perf.	ě.	Blancet	Local System		



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

General	Log On	Recovery Dependencies				
Service	name:	wuauserv				
Display name:		Windows Update				
Descrip	tion:	Enables the detection, download, and installation of updates for Windows and other programs. If this				
Path to C:\Win	executabl dows\syst	le: tem32∖svchost.exe -k netsvcs				
Startup type:		Disabled 🗸				
Help me	e configure	Automatic (Delayed Start)				
Service	status:	Manual Disabled Stopped				
5	Start	Stop Pause Resume				
Vallan	n specify t re.	the start parameters that apply when you start the servic				

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

eneral L	.og On F	Recovery	Depender	ncies			
Select the	computer	's respons	se if this ser	vice fails. <u>Help me set up recover</u> y			
First failure	<b>):</b>		Restart th	e Service 🔹			
Second fa	ailure:		Take No	Action 🗸			
Subseque	nt failures	ŝ	Take No Action				
Reset fail	count afte	r:	1	days			
Restart se	rvice after		1	minutes			
Enable	e actions fo gram	or stops w	ith errors.	Restart Computer Options			
Program	n:						
Comma	and line pa	rameters: ount to en	d of comma	nd line (/fail=%1%)			



15. Go to general tab and then select option apply

eneral Log On	Recovery Dependencies
Service name:	Wulauserv
Display name:	Windows Update
Description:	Enables the detection, download, and installation of updates for Windows and other programs. If this
Path to executabl C:\Windows\syst	le: em32\svchost.exe -k netsvcs
Startup type:	Automatic (Delayed Start)
Help me configure	e service startup options.
Help me configure Service status:	Stopped
Help me configure Service status: Start	Stopped Stop Pause Resume

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

Service name:       WUBUSERY         Display name:       Windows Update         Description:       Enables the detection, download, and installation of updates for Windows and other programs. If this         Path to executable:       C:\Windows\system32\svchost.exe +k netsvcs         Startup type:       Automatic (Delayed Start)         Help me configure service startup options.         Service status:       Stopped		)n   Recovery   Dependencies
Display name: Windows Update Description: Enables the detection, download, and installation of updates for Windows and other programs. If this Path to executable: C:\Windows\system32\svchost.exe +k netsvcs Startup type: Automatic (Delayed Start) Help me configure service startup options. Service status: Stopped	Service name	wuauserv
Description: Enables the detection, download, and installation of updates for Windows and other programs. If this Path to executable: C:\Windows\system32\svchost.exe +k netsvcs Startup type: Automatic (Delayed Start) Help me configure service startup options. Service status: Stopped	Display name:	Windows Update
Path to executable: C:\Windows\system32\svchost.exe +k netsvcs Startup type: Automatic (Delayed Start) • Help me configure service startup options. Service status: Stopped	Description:	Enables the detection, download, and installation of updates for Windows and other programs. If this
Startup type: Automatic (Delayed Start)           Help me configure service startup options.           Service status:         Stopped	Path to execu C:\Windows\	able: system32\svchost.exe -k netsvcs
Help me configure service startup options. Service status: Stopped	Startup type:	Automatic (Delayed Start)
Service status. Stopped	Help me confi	<u>rure service startup options.</u>
	<b>6</b>	· · · · · · · · · · · · · · · · · · ·
Start Stop Pause Resume	Service status	: Stopped
You can specify the start parameters that apply when you start the service from here.	Service status	Stopped



#### 17. Then select Ok

Jeneral	Log On	Recovery	Depender	icies		
Service	name:	wuauserv				
Display	name:	Windows U	pdate			
Descrip	tion:	Enables the updates for	e detection Windows	, download, a and other pro	and installation o grams. If this	f 🌲
Path to C:\Win	executabl dows\syst	e: em32\svchos	st.exe -k ne	tsvcs		
Startup	type:	Automatic	(Delayed S	tart)		-
Help m	e configure	e service start	up options	÷.		
Service	status:	Started				
3	Start	Stop		Pause	Resume	
	n specify ti re.	he start paran	neters that	apply when y	you start the ser	vice
You ca from he Start pa	arameters:	1.00				

18. Then the window shows status like started

Services (Local)	(2) Services Rocal						
	Windows Undets	Name	Description	2004	Mattan Total	Los Ce ás	
	Description Enables the detection, download, and installation of apdities for Windows and allow programs. If the service in distribut, users of this computer will not be allow to use Windows to Dipder or its statements updating fortant, and programs will not be allow to asse the Windows Update Agent (WUA) API	Windows Certifyster     Windows Certifyster     Windows Certifyster     Windows Certifyster     Windows Certify Line - Certify,     Windows Diver Frandation - U.,     Windows Diver Frandation - U.,     Windows Divert Cellector     Windows Divert Cellector     Windows Prent     Windows Tent Ling     Windows Tent Ling     Windows Netter Reserves     Windows Res	Securely enables the creation, management, and disclosure of di- The Wirell-bagindervice service heat their party Wirelevice Cells ( CREAS) Constraints the Wirelevice Connect Nov Configuration while Particular against approach and particularly uncontrol activation Manages soon mode dates in the programma tare working or me. This service manages persistent subscriptions to events from m. The service manages exploited on science of subscriptions and events from m. The service manages exploited on science of subscriptions and events the person from the person of applications are events and work by enventing u- Optimises performance of applications for science and connect data, modular, and enverse againstraine gravitations (modules a service from Windows Mindia Centre Service for 17 using MM longations fleds). Services installation, modification, and memory of Windows (Media Developes for the service for Window Passettation Foundation ). Windows Samote Management (Windfid) service implements the Frances event single registration gravity and law in results of Management events and using property calling and advects developed to advect and any service produce tables of a cleants and services Management (Windfid) service implements the Frances event singlements the cleant HTTE stack and provides level to Windfight service and the provides the layer registration for official services.	Stated Stated Stated Stated Stated Stated Stated Stated	Menual Menual Advanatic Advanatic Advanatic Advanatic Advanatic Advanatic Advanatic Advanatic Advanatic Advanatic Menual Menual Menual Menual Menual Menual Menual Menual Menual	Local Syste Local Syste Local Service Local Syste Local Syste Local Syste Network 1 Local Syste Local Service Local Service Local Syste Network 1 Network 1 Network 1 Network 1 Network 1 Network 1 Local Syste Network 1 Local Syste Network 1 Local Syste Local Syste	
		Winkstation     Winkstation	Creates and maintains clarit retwork connections to remote ser- This service manages mobile broadband (GSM & CDMA) data c	Stated	Automatic Menual	Netwirk 1 Lood Service	1



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

The updates are being installed	
Installation status: Initializing installation done! Installing Security (Indate for Windows (KB4012215) (undate 1 of 1)	
Installing Secondy opdate for windows (who reactory (opdate 1 or 1))	
Installing:	



22. Select Restart option on the final box displayed

Installation complete
You must restart your computer for the updates to take effect.



## <u>SMB</u>

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:

 Click on the Search option and search for "Windows Features" and you will see the result as "Turn Windows Feature on and off."



	Q	windows features .net framework 3.5 size
	Q	windows features on or off windows 10
	Q	windows features downloading required files
	Q	windows features turn on or off + blank
	Q	windows features searching for required files
ŝ	Q	windows features settings
2	Q	windows features dialog box
	R	windows features

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

Wind W	ows Features	<u></u> 1		×
Turn V	vindows features on or off			6
To turn a check bo	feature on, select its check box. To turn x. A filled box means that only part of th	a feature ne feature i	off, clear is turned	its on.
H 🔲	Print and Document Services			-
	RAS Connection Manager Administrat	tion Kit (Cl	MAK)	
$\square$	Remote Differential Compression API	Support		
	RIP Listener			
±	Services for NFS			
• 🗌	Simple Network Management Protoco	ol (SNMP)		
	Simple TCPIP services (i.e. echo, dayti	me etc)		
	SMB 1.0/CIFS File Sharing Support			
	SMB Direct			
	Telnet Client			
	TFTP Client			
	Windows Identity Foundation 3.5			N
		ОК	Can	cel



## 3. Now untick the box and click on "Ok".

🛃 Wind	ows Features	1000		×
Turn V	Vindows features on or off			0
To turn a check bo	a feature on, select its check box. To turn ox. A filled box means that only part of th	a feature ( e feature i	off, clear s turned	its on.
÷ .	Print and Document Services			^
	RAS Connection Manager Administrati	on Kit (CN	ИАК)	
	Remote Differential Compression API S	upport		
	RIP Listener			
• 🗆	Services for NFS			
± 🗆	Simple Network Management Protoco	I (SNMP)		1000
	Simple TCPIP services (i.e. echo, daytin	ne etc)		
	SMB 1.0/CIFS File Sharing Support			
	SMB Direct			
	Telnet Client			
	TFTP Client			
	Windows Identity Foundation 3.5			~
		ОК	Can	cel

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
Control Panel



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





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



Tee etc. Security and Maintenance Network and Sharing Center

#### 6. The **windows firewall with advanced security** window is displayed





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

• • 2 🔟 🔄 🖬 🛛	0					
Windows Firewall with Adva	Inbound Rules	2				Actions
Inbound Rules	Name Group	<u></u>	Profile	Enabled	Acti *	Inbound Rules
Connection Security Rule	Apache HTTP Server		Public	Ves	Allo	Mew Rule_
Monitoring	Apache HTTP Server		Public	Yes	Allo	T Filter by Profile
and the second se	Apache HTTP Server		Public	Yes	Allo	
	Apache HTTP Server		Public	Ves	Allo	T Filter by State
	Apache HTTP Server		Public	Ves	Allo	T Fiher by Group
	Apache HTTP Server		Public	Ves	Allo	View
	🚱 Ask Toobar NotiFier		Private	Yes	Alte	Patronh
	Firefox (C:\Program Files (x86)\Mozilla Fir		Private	Yes	Alto	C Serein
	Firefax (CAProgram Files (x86)\Mazilla Fir		Private	Ves	Allo	Export List
	🔮 Firefox' (C/\Program Files (x86/\Mozilla F		Private	Yes	Allo	Help
	Firefox' (C/\Program Files (x86)/Mozilla F		Private	Ves	Allo	110 C 11
	Apple App		All	Yes	Allo	
	O hpiscnapp.exe		All	Yes	Allo	
	Apggpc01.ere		All	Ves	Allo	
	hpqgplgtupl.exe hpqkygrp.exe hpqbydcorm.exe		All	Yes	Allo	
			All	Yes	Allo	
			All	Ves	Allo	
	C hpqpsapp.ese		All	Ves	Allo	
	🕲 hpqpse.exe		All	Ves	Allo	
	🕲 hpqsudi.exe		AB	Ves	Allo	
	O hpwucil.exe		All	Yes	Alto	
	() IPMsg		Public	Ves	Alle	
	() IPMsg		Private	Yes	Allo	
	@ IPMsg		Private	Ves	Allo	
	(2) IPMsg		Public	Yes	Allo	
	Java(TM) Platform SE binary		Public	Yes	Allo	
	Dava(TM) Platform SE binary		Public	Yes	Allo	
	🔮 mysqld		Public	Yes	Allo	
	🖓 musald		Public	Vec	Alln 👻	

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

hie Action View Help							
Windows Firewall with Advance	Inboand flutes					Actions	
Windows fucewal with Advance in Indown Rules Outbound Rules Combaction Security Rules Monitoring	Internet Hitte: Name Apache HTTP Server Apache HTTP Server Apache HTTP Server Apache HTTP Server Apache HTTP Server Apache HTTP Server Apache HTTP Server Ask Tooher Notifier Tindra: (C\/Program Files (x80)\/Mooilla Fil- Findra: (C\/Program Files (x80)\/Mooilla Fil- Filefor: (C\/Program Filefor: (x80)\/Mooilla Filefor: (x80)\/Mooilla Filefor: (x	Group	Profile Public Public Public Public Public Private Private Private All All All All All All All All All Al	Enabled Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	A cti A bio A bio	Actions Interest Rules Place Rules Filter by Profile Filter by Group View Export List Help	



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



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





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 t	his rule.	
Steps:		
Bule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name	Block 443	
	< Back Finish Cance	
	< Back Finish Cance	el



## **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<u>.</u>

## 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 <u>Microsoft Safety Scanner</u> from a clean, noninfected 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
- <u>In Windows XP</u>

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-defenderoffline-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 <u>free security software</u> that you can use:



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

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