Mencegah Penyebaran Ransomware Wannacry di Windows

Beberapa hari terakhir Ransomware wannacry telah menghebohkan dunia IT dan telah masuk di lebih dari 99 negara, termasuk di Indonesia. **Ransomware** adalah salah satu jenis **malware** yang bertujuan untuk meminta tebusan kepada korban. Ransomware, sesuai dengan namanya, *ransom* = tebusan (dalam bahasa Inggris), jenis malware ini bertujuan untuk memeras korban yang komputernya terinfeksi ransomware dengan meminta sejumlah uang sebagai tebusan.

Berikut ini adalah beberapa extensi file yang menjadi target dari Malware Ransomware Wannacrypt :

- Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
- Less common and nation-specific office formats (.sxw, .odt, .hwp).
- Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
- Emails and email databases (.eml, .msg, .ost, .pst, .edb).
- Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
- Developers' sourcecode and project files (.php, .java, .cpp, .pas, .asm).
- Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
- Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
- Virtual machine files (.vmx, .vmdk, .vdi).

Berikut ini adalah beberapa tindakan pencegahan untuk meminimalisir terinfeksi Malware Ransomware Wannacrypt atau wannacry:

- 1. Jangan terkoneksi di LAN/WIFI & Lakukan Back Up Data
- 2. Lakukan Update AntiVirus
- 3. Lakukan Update Patch MS17-010 pada OS Windows Untuk update patch windows dapat di download di : http://openstorage.gunadarma.ac.id/wannacry/

4. Non Aktifkan Fungsi SMB v1 & SMB v2

Server Message Block disingkat SMB adalah protokol standar yang dibuat oleh Microsoft yang digunakan pada sistem windows. Fungsi SMB dalam windows adalah sebagai protokol yang digunakan untuk membagi data (sharing file), baik dari perangkat CD-ROM, harddisk, maupun perangkat output seperti printer untuk dapat digunakan bersama-sama.

Cara Mematikan fitur SMB V1 untuk windows 7

Klik start-run di kotak pencarian ketikan regedit – run as administrator – lalu klik ok

🌠 regedit	Open
6	Run as administrator
2	Edit with Notepad++
	Add to archive
	Add to "regedit.rar"
	Compress and email
	Compress to "regedit.rar" and email
	WinZip •
	Pin to Taskbar
	Pin to Start Menu
	PowerISO +
	Scan With Smadav
	Restore previous versions
	Send to +
	Cut
	Сору
	Delete
	Open file location
See mo	Properties
gedit	× Shut down +

Langsung saja kita pergi ke PATH

 $Computer \ HKEY_LOCAL_MACHINE \ SYSTEM \ Current Control Set \ Services \ Lanman Server \ Parameters$

🕱 Registry Editor					
File Edit View Favorites Help					
⊿ ₁∎ Computer	Name	Туре	Data		
HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_LOCAL_MACHINE HKEY_USERS HKEY_CURRENT_CONFIG	ab) (Default)	REG_SZ	(value not set)		
	•	III	۴.		
Computer\HKEY_LOCAL_MACHINE					



💣 Re	egistry	Editor							×
File	Edit	View	Favorites Help						
File	Edit	View	Favorites Help intelide intelppm IPBusEnum IpFilterDriver IPMIDRV IPMIDRV IPNAT isapnp iScsiPrt kbdclass kbdhid KeyIso KSecDD KSecPkg	Name (Default) AdjustedNullSes autodisconnect EnableAuthentic. enableforcedlog enablesecuritysi Guid Lmannounce NullSessionPipes requiresecuritysi ServiceDII ServiceDII Size	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_BINARY REG_BINARY REG_DWORD REG_MULTI_SZ . REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (value not set) 0x00000003 (3) 0x0000000 (15) 0x0000000 (0) 0x0000000 (1) 0x0000000 (0) ff 24 32 92 c4 b9 4f 45 a5 8c 5 0x00000000 (0) 0x00000000 (0) 0x00000000 (0) 0x00000000 (0) 0x00000000 (0) 0x00000000 (1) 0x00000001 (1) 0x00000001 (1)	New d bd 1c f3 46 e9 vsvc.dll	Key String Value Binary Value DWORD (32-bit) Value QWORD (64-bit) Value Multi-String Value Expandable String Value	
Com	puter\H	IKEY_L		//CurrentControlSet\serv	rices\LanmanServer\Pa	arameters			

Isikan nilai nya menjadi 0 = disable, lalu ok

💣 Re	gistry Edi	tor	Contract Press	-					trees Present) 🕅	
File	Edit Vi	ew	Favorites Help										
			intelide intelide iPBusEnum iPBusEnum iphipsvc iphipsvc iphipsvc iPMDRV iPNAT iRENUM isapnp iScsiPrt kbdclass kbdhid kbdhid kbdhid kbdhid kbdhid kbdhid kbdhid kbdhid		Name Matudolisconnect EnableAuthentic enableforcedlog Guid Linannounce NullSessionPipes Requiresecuritysi ServiceDII ServiceDIIUnloa Sisze SMB1 SMB2	Type REG_DWORD REG_DWORD	Data 0x0000000 (15) 0x0000000 (0) 0x0000000 (1) 0x0000000 (0) ff 24 32 92 c4 b9 4f 0x0000000 (0) 0x0000000 (1) %SystemRoot%sys 0x0000000 (1) 0x0000000 (1) 0x0000000 (0) 0x0000000 (0)	, () ()	Edit DWORD (32-bit) Value Value name: SMB1 Value data: 2	Base	ncel		4 III
Comp	uter\HKE	Y_LO	CAL_MACHINE\SYS1	EIM/(.urrentControlSet\servi	ces\LanmanServer\Pa	rameters						

Setelah semua konfigurasi udah selesai di buat jangan lupa untuk merestart windows anda.

5. Aktifkan firewall di windows control panel

Control panel - System and Security - Windos Firewall - Customize Settings

The TANK BERRY AND A CONTRACT STATE	
🚱 🕗 🗢 📾 « System and Security 🕨 Windows Firewall 🕨 Customize Settings 💿 🔹 🍫 Search Control Panel	Q
Customize settings for each type of network You can modify the firewall settings for each type of network location that you use. What are network locations? Home or work (private) network location settings Image: State in the intervent loc	
OK Cancel	

6. Blokir port TCP & port UDP yang di gunakan sebagai media Wannacry yaitu port 135-139, 445, 3389

Tambahkan juga port lainnya seperti port 135-139, 445, 593, 1024-1030, 3389, 4444

Block port TCP 135-139, 445, 593, 1024-1030, 3389, 4444

Untuk memblok nya kita perlu mengaturnya di contol panel windows anda.

Start - Control Panel



System and Security



Windows Firewall



Advanced settings



Klik kanan pada Inbound Rules - New Rule

Windows Fermall or	th Adlance Information	Rules					Actions
Connection 1 Connection 1 Mentaring	New Rule Filter by Proble Filter by State Filter by Group Vew Refeath Expert List	Program Filed Mooila Filefox) Vrogram Filed Mooila Filefox) Vrogram Filed Mooila Filefox) Kice Groove Hice Groove Hice Groove Hice Oveloste Hice Oveloste Nice Oveloste Server	Gring	Profile Private Public Public Public Public Public Public	Enabled Yes Yes Yes Yes Yes Yes Yes Yes	Action + Action 1 Altern 1 Altern Altern Altern Altern Altern Altern	New Rule. New Rule. Files by Profile Files by State Files by State Very Selepth Refer
	Help 9 F000 9 F000	b Sarver CTI Heb Sarver CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik CTIModulet/Nik		Public Public	van Van Van Van Van Van Van Van Van Van V	Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon Albon	Hulp Forter (C) Peopen Filer Dustle Fule Cut Cut Cut Deten Properties Hulp

Lalu checklist Port => klik Next

🔗 New Inbound Rule Wizard		×
Rule Type		
Select the type of firewall rule to cr	eate.	
Steps:		
 Rule Type 	What type of rule would you like to create?	
Protocol and Ports		
 Action 	Program	
 Profile 	Rule that controls connections for a program.	
 Name 	O Port	
	Rule that controls connections for a TCP or UDP port.	
	Predefined:	
	BranchCache - Content Retrieval (Uses HTTP) 👻	
	Rule that controls connections for a Windows experience.	
	© Custom	
	Custom rule.	
	Learn more about rule types	
	< Back Next > Can	cel

Checklist => TCP

Checklist => Specific local ports, isikan : 135-139, 445, 593, 1024-1030, 3389, 4444 Klik Next

🔗 New Inbound Rule Wizard		×
Protocol and Ports		
Specify the protocols and ports to	which this rule applies.	
Steps:		
Rule Type	Does this rule apply to TCP or UDF	??
Protocol and Ports	TCP	
Action	O UDP	
Profile		
 Name 	Does this rule apply to all local port	s or specific local ports?
	All local ports	
	Specific local ports:	135-139, 445, 593, 1024-1030, 3389, 4444
		Example: 80, 443, 5000-5010
	Learn more about protocol and por	ts
		< Back Next > Cancel

Checklist => Block the connection, next



Checklist => Domain, Private & Public. next

🔐 New Inbound Rule Wizard	
Profile	
Specify the profiles for which this r	ule applies.
Steps:	
Rule Type	When does this rule apply?
Protocol and Ports	
 Action 	✓ Domain
Profile	Applies when a computer is connected to its corporate domain.
Name	V Private
	Applies when a computer is connected to a private network location.
	V Public
	Applies when a computer is connected to a public network location.
	Learn more about profiles
	Cancel

Isikan profile nama nya = Block Port Ransomware TCP, lalu klik finish

🔐 New Inbound Rule Wizard		×
Name		
Specify the name and description	i of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name: Plack Part Paragenuizer TCP	
Name	Block Foit Nansomware ICF	
	Description (optional):	
	Karaka Kar Karaka Karaka Kar Karaka Karaka Ka Karaka Karaka Kar Karaka Karaka Ka Karaka Karaka Kar	

Untuk memblok port UDP sama langkahnya memblock port TCP yang baru kita buat di atas, hanya yang membedakan pada **Protocol and Ports** kita checklist => **UDP**

💣 New Inbound Rule Wizard			3
Protocol and Ports			
Specify the protocols and ports to	which this rule applies.		
Steps:			
Rule Type	Does this rule apply to TCP or UDF	2?	
Protocol and Ports	© TCP		
 Action 	ODP		
 Profile 			
Name	Does this rule apply to all local port	s or specific local ports?	
	All local ports		
	Specific local ports:	135-139, 445, 593, 1024-1030, 3389, 4444	
		Example: 80, 443, 5000-5010	
	Learn more about protocol and por		
		< Back Next > Cancel	

Dan buat profil nama nya => Block Port Ransomware UDP

🔐 New Inbound Rule Wizard		×
Name		
Specify the name and description	of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name	Block Port Ransomeware UDP	
	Description (optional):	
	< Back Finish Cance	-

Selesai & Selamat Mencoba !!!