

# Merit LILIN Application Note How to Protect LILIN NAV System from the Virus WannaCry 2.0

Document Number : A00123 Date : 2015/05/26 Dept: Technical Support, Taipei

**Subject:** This document describes how to prevent the virus WannaCry 2.0 for LILIN Navigator systems.

#### **Products:**

NAV3025 · NAV2036 · NAV1036/1072/1108 · NAV16036/16072/16108 · NAV24036/24072/24108

### Step #1. Check whether the LILIN NAV system has got the Virus WannaCry 2.0

- 1-1 Remove all network connections (wire & wireless), and then reboot Windows system.
- 1-2 After you log in to the NAV system, press "Ctrl + Alt + Del" to run Task Manager, choose processes page and check whether there is tasksche.exe or mssecsvc.exe on the list. If so, your system might have the virus.

#### Step #2. How to remove the WannaCry 2.0

- 2-1 Re-install Windows, since this NVR contains embedded Windows, please contact your local LILIN dealer or branch for getting an embedded Windows module.
- 2-2 If Windows is not re-installed on the hard disk, **DO NOT** put this hard disk into the others PC to avoid affecting another PC from the virus.

#### Step #3. Protect LILIN NAV from WannaCry 2.0

Enable Windows automatic updates, and update fully your system.

3-1 Press "Ctrl + Alt + Del" to run Task Manager, choose services page and make sure if Windows Update service is running.

le Options View Help				Action View Help				
Applications Processes Serv	ices Performance Ne	etworking Users						
Name VaultSvc simptcp Sam5s ProtectedStorage NetTcpPortSharing NetTcpActivator NetPipeActivator NetMsmqActivator NetMsmqActivator NetBogon KeyIso	PID 1836 724 2276 2276 2276 3588 724	Description Credential Manager Simple TCP/IP Services Security Accounts Manager Protected Storage Net.Tcp Port Sharing Service Net.Tcp Listner Adapter Net.Msmq Listner Adapter Net.Msmq Listner Adapter Net0gon CNG Key Isolation	A 111	ices (Loca) Windows Update Stop the service Restart the service Description: 敵用(滑渕、下載並安裝 Windows 或其他程式的更新。 如果停用此服務。遠部電腦的 使用非複筆法等。使用 Windows	Name Name Windows Media Play Windows Modules In Windows Process Act Windows Process Act Windows Remote M Windows Search Windows Time Windows Update	Status Started Started Started	Startup Type Disabled Manual Manual Manual Disabled Automatic Automatic (	Log On As Network S Local Syst Local Serv Local Syst Network S Local Syst Local Serv Local Sys
IISADMIN idøvc EFS CISVC AppHostSvc	1632 1548 1936	IIS Admin Service Windows CardSpace Encrypting File System (EFS) Indexing Service Application Host Helper Service	۲ /ices	Update 或其自動更新功能。 而且程式將無法使用 Windows Update Agent (WUA) API。	Wired AutoConfig Wired AutoConfig WIAN AutoConfig WIAN AutoConfig WIP Performance A Workstation Workstation Workstation World Wide Web Pu WWAN AutoConfig	Started Started Started	Manual Automatic Manual Automatic Automatic Manual	Local Syst Local Syst Local Syst Local Syst Local Syst Local Syst



General	Log On	Recovery	Depender	ncies			
Service	name:	wuauser	v				
Display	name:	Window	s Update				
Descrip	otion:					* *	
Path to C:\Wind	executab lows∖syst	le: em32\svcho	ostexe -k ne	etsvcs			
Startup	type:	Automa	tic (Delaye	d Start)		•	
<u>Help m</u>	e configu	re service st	artup optior	n <u>s.</u>			
Service	status:	Started					
	Start	S	top	Pause		Resume	
						service from	
You can here.	n specify	the start par	ameters tha	it apply when y	ou start the	Service nom	

3-3 Execute Windows Update and make sure that all hotfixes are installed (Control Panel\System and Security\Windows Update).







## Step #4. Disable TCP 455 Port

4-1 Click Advanced settings.





4-2 Click Inbound Rules, and then Import Policy.



#### 4-3 Choose Port and go next.

Prev Inbound Rule Wizard	Tagen a			×
Rule Type Select the type of firewall rule to create.				
Steps: Protocol and Ports Action Profile Name	What type of rule would you like to create?  Program Rule that controls connections for a program.  Protefined: BITS Percaching Rule that controls connections for a Windows experience. Custom Custom rule.  Learn more about rule types	< Back	Next >	Cancel



4-4 Choose TCP & Specific local ports, key-in 135,137,139,445, and then go next.

Prev Inbound Rule Wizard				×
Protocol and Ports				
Specify the protocols and ports to whic	h this rule applies.			
Steps:				
<ul> <li>Rule Type</li> </ul>	Does this rule apply to TCP or UDP?	,		
<ul> <li>Protocol and Ports</li> </ul>	ICP			
<ul> <li>Action</li> </ul>	O UDP			
<ul> <li>Profile</li> </ul>				
<ul> <li>ivame</li> </ul>	Does this rule apply to all local ports	or specific local ports?		
	All local ports			
	Specific local ports:	135,137,138,139,445		
		Example: 00, 445, 5000-3010		
	Learn more about protocol and ports			
			< Back Next >	Cancel
			- Dava	Cantel

4-5 Choose Block the connection and go next.

P New Inbound Rule Wizard				×
Action				
Specify the action to be taken wh	en a connection matches the conditions specified in the rule.			
Steps:				
<ul> <li>Rule Type</li> </ul>	What action should be taken when a connection matches the specified conditions?			
<ul> <li>Protocol and Ports</li> </ul>	Allow the connection			
<ul> <li>Action</li> </ul>	This includes connections that are protected with IPsec as well as those are not.			
Profile	Allow the connection if it is secure			
<ul> <li>Name</li> </ul>	This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.			
	Customiza			
	Block the connection			
	Learn more about actions			
		< Back	Next >	Cancel
		- DOVA		Genova



4-6 Check all checkboxes and go next.

Prev Inbound Rule Wizard			×
Profile			
Specify the profiles for which this	rule applies.		
Steps:			
Steps: Rule Type Protocol and Ports Action Profile Name	When does this rule apply?		
		< Back	Next > Cancel

4-7 Give a name for this rule and press Finish button.

Prew Inbound Rule Wizard	× · · · · · · · · · · · · · · · · · · ·
Name	
Specify the name and description of this ru	ıle.
Steps:	
<ul> <li>Rule Type</li> </ul>	
<ul> <li>Protocol and Ports</li> </ul>	
<ul> <li>Action</li> </ul>	Name:
Profile	Disable 445 Port (TCP)
<ul> <li>Name</li> </ul>	Description (optional):
	Disable 445 Port (TCP) WannaCrypt0R
	< Back Finish Cancel



4-8 The new rule Disable 445 Port (TCP) is on the Inbound Rules list. For setting UDP, please go through 3-4 ~ 3-7 and name this rule to Disable 445 Port (UDP).

Action view He	IP		
/indows Eirewall with	Ar Inbound Rules		Actions
Inbound Rules	Name	un Drofila Enable A	
Outbound Rules	Disable 445 Dect (TCD)	All Ver	Inbound Rules
Le Connection Security R	R B C Disable 443 Port (TCP)	All Yes E	🔜 New Rule
Monitoring	Archive Manager	Domain No	Filter by Profile
	Archive Manager	Private Yes	Filter by State
	Archive Manager	Private Yes	- The by state
	Marchive Manager	Domain No	Filter by Group
	Control Center 64 bits	Private Yes	View
	Control Center 64 bits	Private Yes	G Refresh
	O Database Manager	Private Yes	
	O Database Manager	Private Yes	Export List
	Database Manager	Domain No	Help
	Database Manager	Domain No	Disable 445 Port (TCP)
	OB Center	Private Yes	Disable 445 Fort (TCF)
	DB Center	Domain No	Disable Rule
	Ø DB Center	Private Yes	🔏 Cut
	DB Center	Domain No	Copy
	ODisable 445 Port	All No	
	ODisable port 135 - TCP	All No	X Delete
	ODisable port 135 - TCP	All No	Properties
	S Disable port 135 - TCP	All No	Help
	ODisable port 135 - UDP	All No	- LostPa
	ODisable port 135 - UDP	All No	
	ODisable port 137 - TCP	All No	
	ODisable port 137 - TCP	All No	
	ODisable port 137 - UDP	All No	

Step #5. After Windows Update completes, follow the steps below to adjust settings to make the system safer.

5-1 Select 'Download updates but let me choose whether to install them for Important updates.'

5-2 Check 'Give me recommended updates the same way I receive important updates.'

5-3 Check 'Allow all users to install updates on this computer.'

File Edit View To	ols Help	
	Choose how Windows can install updates	Í
	When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer. How does automatic updating help me?	
	Important updates Download updates but let me choose whether to install them	Ш
	Install new updates: Every day 🔹 at 3:00 AM 🔹	
	Image: Commended updates         Image: Co	
	Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.	



NOTE: To avoid automatic Windows Update for system rebooting, disable Window Update by default, but we recommend you do Windows Update regularly.

**Contact** Contact <u>lilin.zendesk.com</u> for technical support.