WannaCry 加密勒索軟件

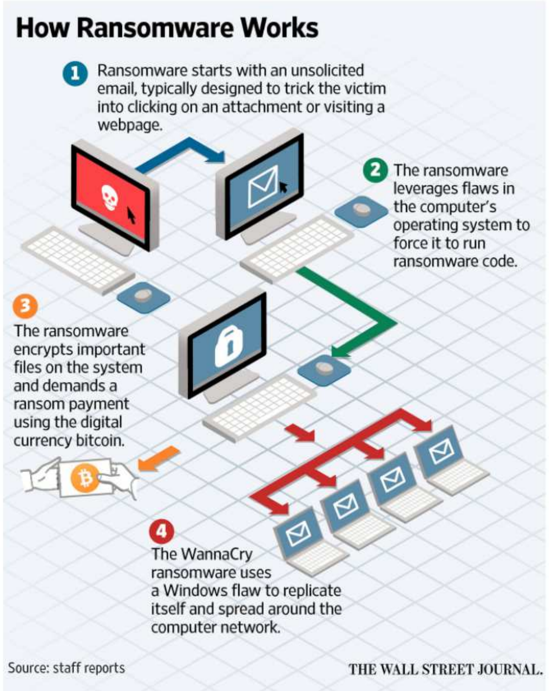
Kelvin Woo

環速集團
Speedy Group

加密勒索軟件

- 在2013年起首次在學校發現
- 2016年3-5月最頻繁
- 2016年常見散播模式:
  垃圾郵件
  網頁連結
  Remote Desktop (RDP)

- WannaCry: 利用SMB漏洞進行攻擊,
  無需用戶互動亦可感染



How Ransomware Works

1. Ransomware starts with an unsolicited email, typically designed to trick the victim into clicking on an attachment or visiting a webpage.
2. The ransomware leverages flaws in the computer's operating system to force it to run ransomware code.
3. The ransomware encrypts important files on the system and demands a ransom payment using the digital currency bitcoin.
4. The WannaCry ransomware uses a Windows flaw to replicate itself and spread around the computer network.

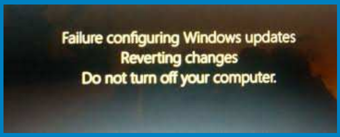
Source: staff reports

THE WALL STREET JOURNAL.

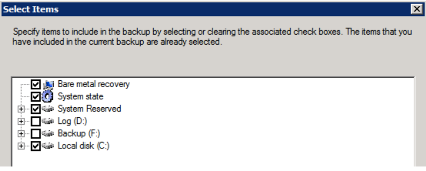
5月12日早上

- 風險評估: 危險程度是中度等級
- 學校毋須特別恐慌

- 大部都有安裝防火牆，能夠阻擋外來的直接攻擊
- Server/高危設備: 先Backup後Update



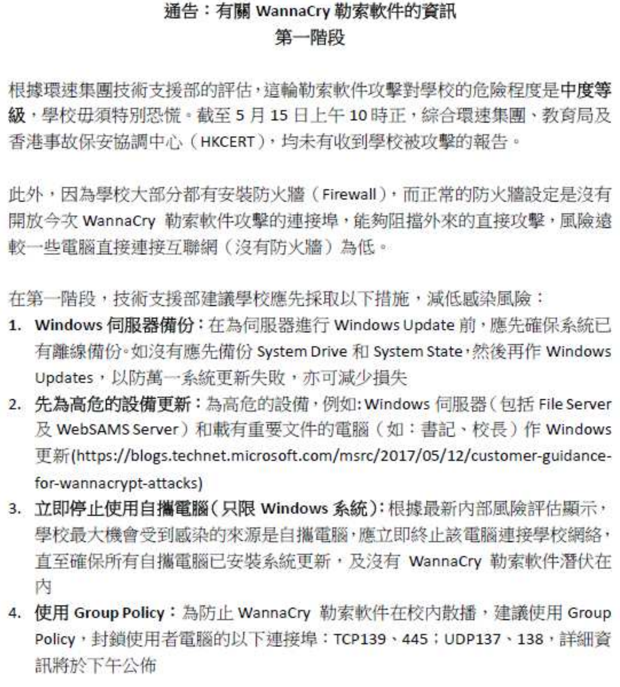
Failure configuring Windows updates
Reverting changes
Do not turn off your computer.



Select Items

Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

☑ Bare metal recovery
☑ System state
☑ System Reserved
☐ Log (D:)
☐ Backup (F:)
☑ Local disk (C:)



通告：有關 WannaCry 勒索軟件的資訊

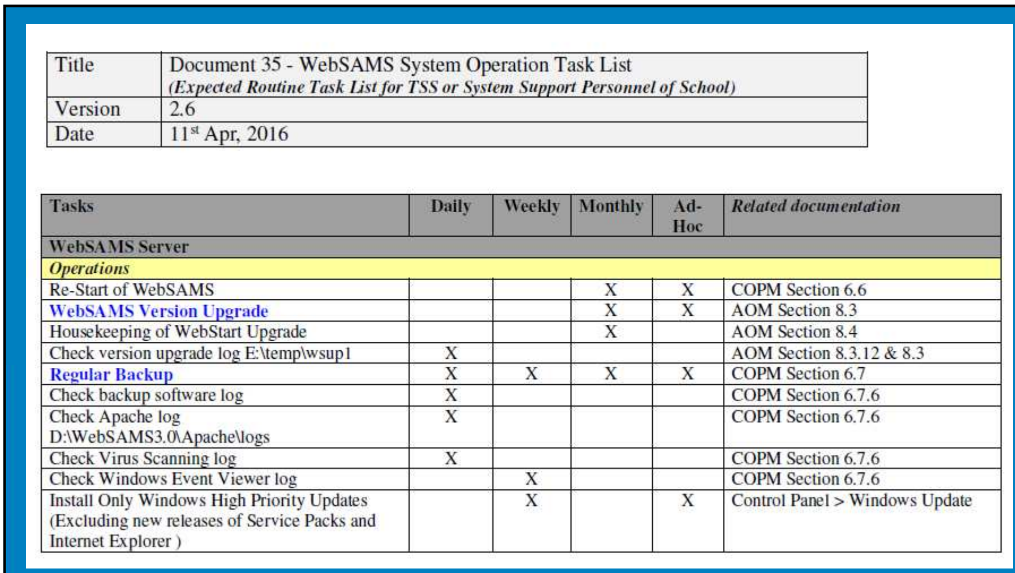
第一階段

根據環速集團技術支援部的評估，這輪勒索軟件攻擊對學校的危險程度是**中度等級**，學校毋須特別恐慌。截至 5 月 15 日上午 10 時正，綜合環速集團、教育局及香港事故保安協調中心（HKCERT），均未有收到學校被攻擊的報告。

此外，因為學校大部分都有安裝防火牆（Firewall），而正常的防火牆設定是沒有開放今次 WannaCry 勒索軟件攻擊的連接埠，能夠阻擋外來的直接攻擊，風險遠較一些電腦直接連接互聯網（沒有防火牆）為低。

在第一階段，技術支援部建議學校應先採取以下措施，減低感染風險：

1. **Windows 伺服器備份**：在為伺服器進行 Windows Update 前，應先確保系統已有離線備份。如沒有應先備份 System Drive 和 System State，然後再作 Windows Updates，以防萬一系統更新失敗，亦可減少損失
2. **先為高危的設備更新**：為高危的設備，例如: Windows 伺服器（包括 File Server 及 WebSAMS Server）和載有重要文件的電腦（如：書記、校長）作 Windows 更新(https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks)
3. **立即停止使用自攜電腦（只限 Windows 系統）**：根據最新內部風險評估顯示，學校最大機會受到感染的來源是自攜電腦，應立即終止該電腦連接學校網絡，直至確保所有自攜電腦已安裝系統更新，及沒有 WannaCry 勒索軟件潛伏在內
4. **使用 Group Policy**：為防止 WannaCry 勒索軟件在校內散播，建議使用 Group Policy，封鎖使用者電腦的以下連接埠：TCP139、445；UDP137、138，詳細資訊將於下午公佈



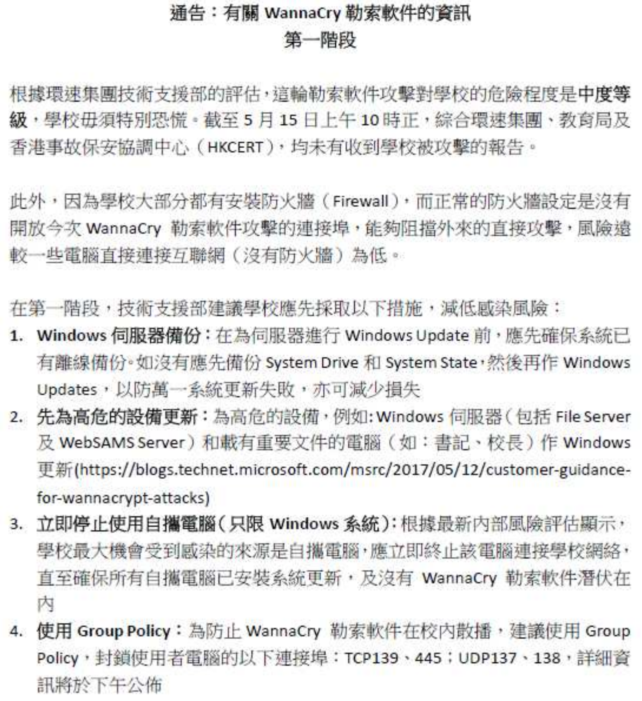
Title	Document 35 - WebSAMS System Operation Task List *(Expected Routine Task List for TSS or System Support Personnel of School)*
Version	2.6
Date	11st Apr, 2016

Tasks	Daily	Weekly	Monthly	Ad-Hoc	*Related documentation*
WebSAMS Server					
Operations					
Re-Start of WebSAMS			X	X	COPM Section 6.6
WebSAMS Version Upgrade			X	X	AOM Section 8.3
Housekeeping of WebStart Upgrade			X		AOM Section 8.4
Check version upgrade log E:\temp\wsup1	X				AOM Section 8.3.12 & 8.3
Regular Backup	X	X	X	X	COPM Section 6.7
Check backup software log	X				COPM Section 6.7.6
Check Apache log D:\WebSAMS3.0\Apache\logs	X				COPM Section 6.7.6
Check Virus Scanning log	X				COPM Section 6.7.6
Check Windows Event Viewer log		X			COPM Section 6.7.6
Install Only Windows High Priority Updates (Excluding new releases of Service Packs and Internet Explorer)		X		X	Control Panel > Windows Update

環速集團
Speedy Group

5月12日早上

- 內部風險評估:自攜電腦最高危
- 立即停止使用自攜電腦（Windows系統）



通告：有關 WannaCry 勒索軟件的資訊
第一階段

根據環速集團技術支援部的評估，這輪勒索軟件攻擊對學校的危險程度是**中度等級**，學校毋須特別恐慌。截至 5 月 15 日上午 10 時正，綜合環速集團、教育局及香港事故保安協調中心（HKCERT），均未有收到學校被攻擊的報告。

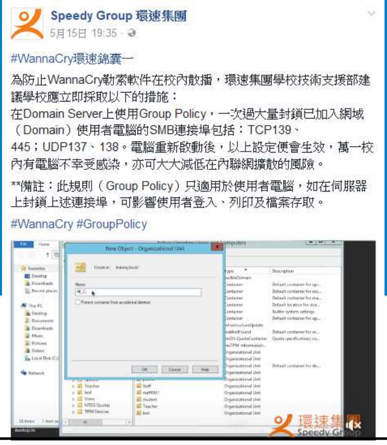
此外，因為學校大部分都有安裝防火牆（Firewall），而正常的防火牆設定是沒有開放今次 WannaCry 勒索軟件攻擊的連接埠，能夠阻擋外來的直接攻擊，風險遠較一些電腦直接連接互聯網（沒有防火牆）為低。

在第一階段，技術支援部建議學校應先採取以下措施，減低感染風險：

1. **Windows 伺服器備份**：在為伺服器進行 Windows Update 前，應先確保系統已有離線備份。如沒有應先備份 System Drive 和 System State，然後再作 Windows Updates，以防萬一系統更新失敗，亦可減少損失
2. **先為高危的設備更新**：為高危的設備，例如: Windows 伺服器（包括 File Server 及 WebSAMS Server）和載有重要文件的電腦（如：書記、校長）作 Windows 更新(https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks)
3. **立即停止使用自攜電腦（只限 Windows 系統）**：根據最新內部風險評估顯示，學校最大機會受到感染的來源是自攜電腦，應立即終止該電腦連接學校網絡，直至確保所有自攜電腦已安裝系統更新，及沒有 WannaCry 勒索軟件潛伏在內
4. **使用 Group Policy**：為防止 WannaCry 勒索軟件在校內散播，建議使用 Group Policy，封鎖使用者電腦的以下連接埠：TCP139、445；UDP137、138，詳細資訊將於下午公佈

Group Policy

一次過大量封鎖已加入網域（Domain）
使用者電腦的SMB連接埠
包括：TCP IN 139、445；UDP IN 137、138



Speedy Group 環速集團
5月15日 19:35

#WannaCry環速錦囊一

為防止WannaCry勒索軟件在校內散播，環速集團學校技術支援部建議學校應立即採取以下的措施：
在Domain Server上使用Group Policy，一次過大量封鎖已加入網域（Domain）使用者電腦的SMB連接埠包括：TCP139、445；UDP137、138。電腦重新啟動後，以上設定便會生效，萬一校內有電腦不幸受感染，亦可大大減低在內聯網擴散的風險。

**備註：此規則（Group Policy）只適用於使用者電腦，如在伺服器上封鎖上述連接埠，可影響使用者登入、列印及檔案存取。

#WannaCry #GroupPolicy

speedygrouphk

Find us on facebook

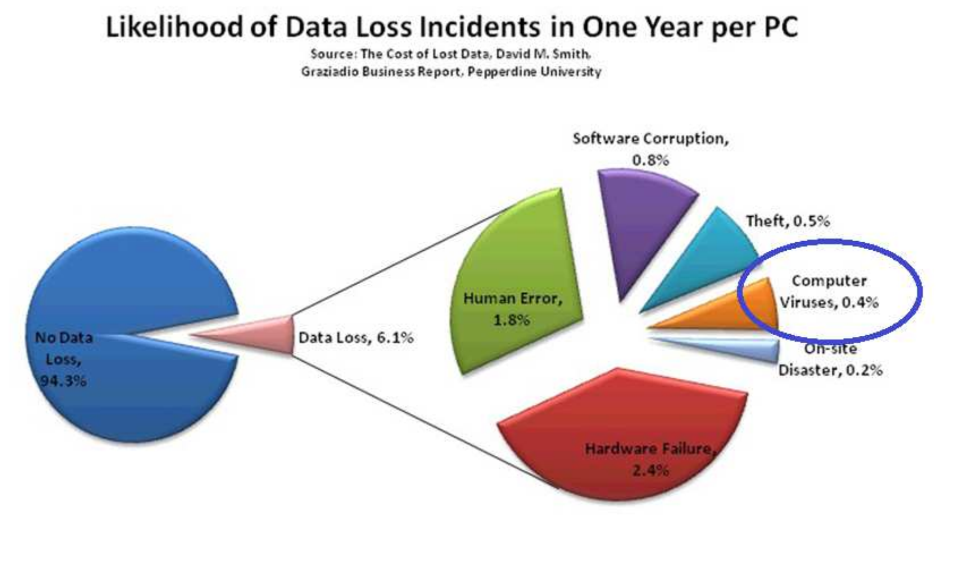
環速集團 Speedy Group

我們建議只有一個

環速集團
Speedy Group

就是備份

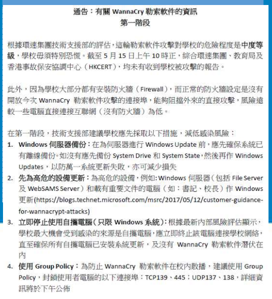
環速集團
Speedy Group



加密勒索軟件=流感

預防流感措施
避免到人多擠迫或空氣欠流通的地方
高危人士宜佩戴口罩
勤洗手包括進食前
注射流感疫苗
打噴嚏或咳嗽後要徹底洗手
出現呼吸道感染症狀病童應避免上學
保持室內空氣流通
保持均衡飲食、恒常運動及充足休息
資料來源：衛生防護中心、曾德賢醫生

急救



通告：有關 WannaCry 勒索軟件的資訊
第一階段

根據環速集團技術支援部的評估，這輪勒索軟件攻擊對學校的危險程度是**中度等級**，學校毋須特別恐慌。截至 5 月 15 日上午 10 時正，綜合環速集團、教育局及香港事故保安協調中心（HKCERT），均未有收到學校被攻擊的報告。

此外，因為學校大部分都有安裝防火牆（Firewall），而正常的防火牆設定是沒有開放今次 WannaCry 勒索軟件攻擊的連接埠，能夠阻擋外來的直接攻擊，風險遠較一些電腦直接連接互聯網（沒有防火牆）為低。

在第一階段，技術支援部建議學校應先採取以下措施，減低感染風險：

1. **Windows 伺服器備份**：在為伺服器進行 Windows Update 前，應先確保系統已有離線備份。如沒有應先備份 System Drive 和 System State，然後再作 Windows Updates，以防萬一系統更新失敗，亦可減少損失
2. **先為高危的設備更新**：為高危的設備，例如: Windows 伺服器（包括 File Server 及 WebSAMS Server）和載有重要文件的電腦（如：書記、校長）作 Windows 更新(https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks)
3. **立即停止使用自攜電腦（只限 Windows 系統）**：根據最新內部風險評估顯示，學校最大機會受到感染的來源是自攜電腦，應立即終止該電腦連接學校網絡，直至確保所有自攜電腦已安裝系統更新，及沒有 WannaCry 勒索軟件潛伏在內
4. **使用 Group Policy**：為防止 WannaCry 勒索軟件在校內散播，建議使用 Group Policy，封鎖使用者電腦的以下連接埠：TCP139、445；UDP137、138，詳細資訊將於下午公佈

治療

預防

不要開啟不明電郵
更新保安軟件
使用防垃圾防病毒郵件伺服器
更新系統及軟件
定時備份
BYOD 政策
良好網絡架構
良好Windows Group Policies

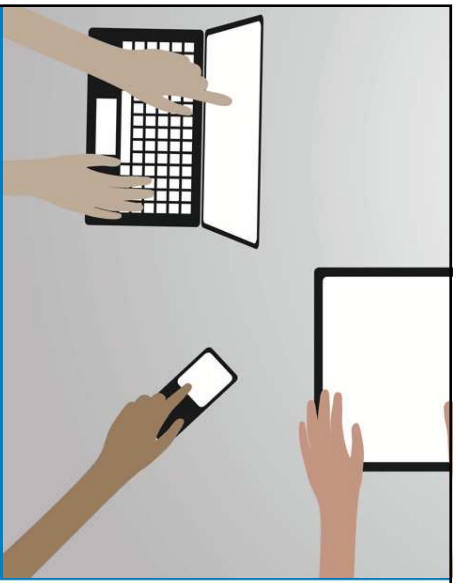
加密勒索軟件防範措施

定立清楚容易了解的BYOD政策

抵禦因「自攜裝置」遺失或被入侵所引致的風險
例如:

1. 允許使用器材的種類、作業系統?
2. 防毒軟件/安全軟件要求?
3. 甚麼檔案不可存在本機?
4. 定期安全檢查

"自攜裝置安全問題
亦是
學校安全問題"



環速集團
Speedy Group

加密勒索軟件防範措施

- 使用防垃圾防病毒郵件伺服器
- 安全與防毒軟體
- DNS- SPF Record (Sender Policy Framework)
- OpenDNS
- VLANs
- Patch Management

ITED	SAMS	MMLC/ITLC
WiFi	CCTV	VoIP

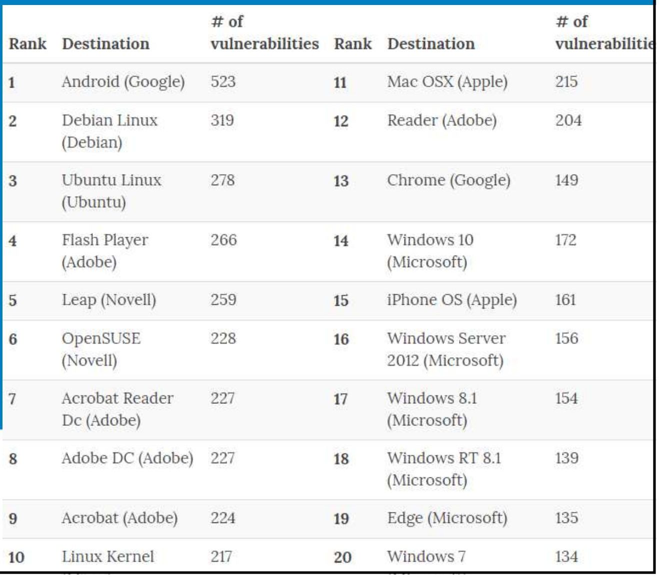
環速集團
Speedy Group

Windows Update Patch Management

環速集團 Speedy Group

Windows Update Patch Management

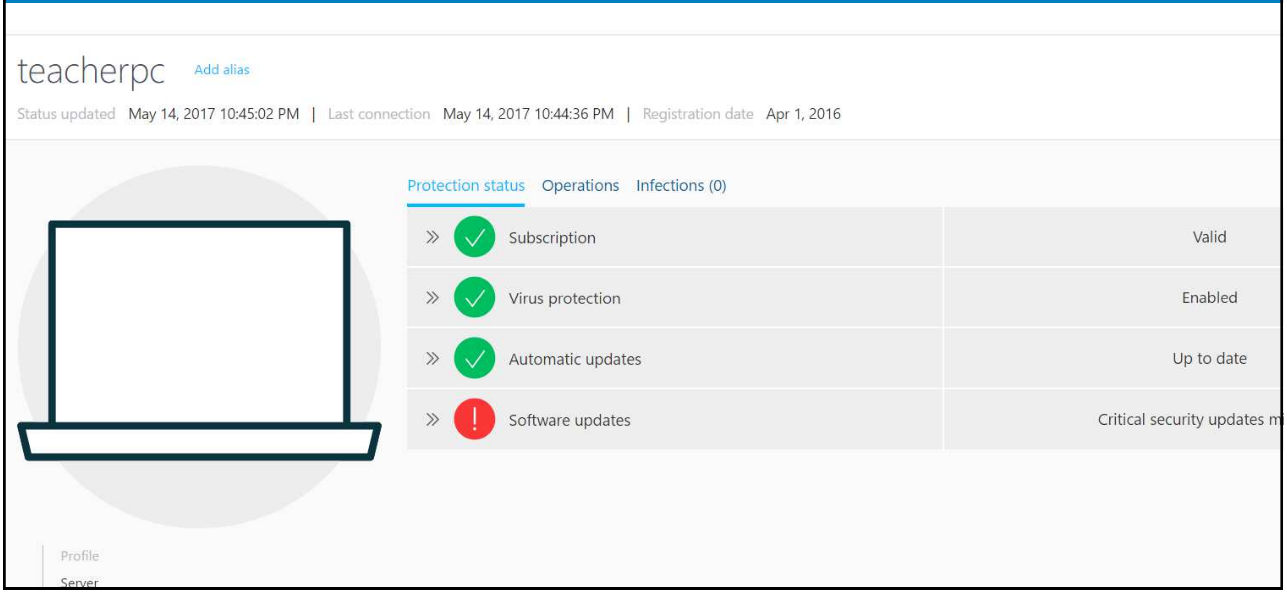
安全漏洞排名2016



Rank	Destination	# of vulnerabilities	Rank	Destination	# of vulnerabilitie
1	Android (Google)	523	11	Mac OSX (Apple)	215
2	Debian Linux (Debian)	319	12	Reader (Adobe)	204
3	Ubuntu Linux (Ubuntu)	278	13	Chrome (Google)	149
4	Flash Player (Adobe)	266	14	Windows 10 (Microsoft)	172
5	Leap (Novell)	259	15	iPhone OS (Apple)	161
6	OpenSUSE (Novell)	228	16	Windows Server 2012 (Microsoft)	156
7	Acrobat Reader Dc (Adobe)	227	17	Windows 8.1 (Microsoft)	154
8	Adobe DC (Adobe)	227	18	Windows RT 8.1 (Microsoft)	139
9	Acrobat (Adobe)	224	19	Edge (Microsoft)	135
10	Linux Kernel	217	20	Windows 7	134

Source: cvedetails.com

Windows Update / Patch Management



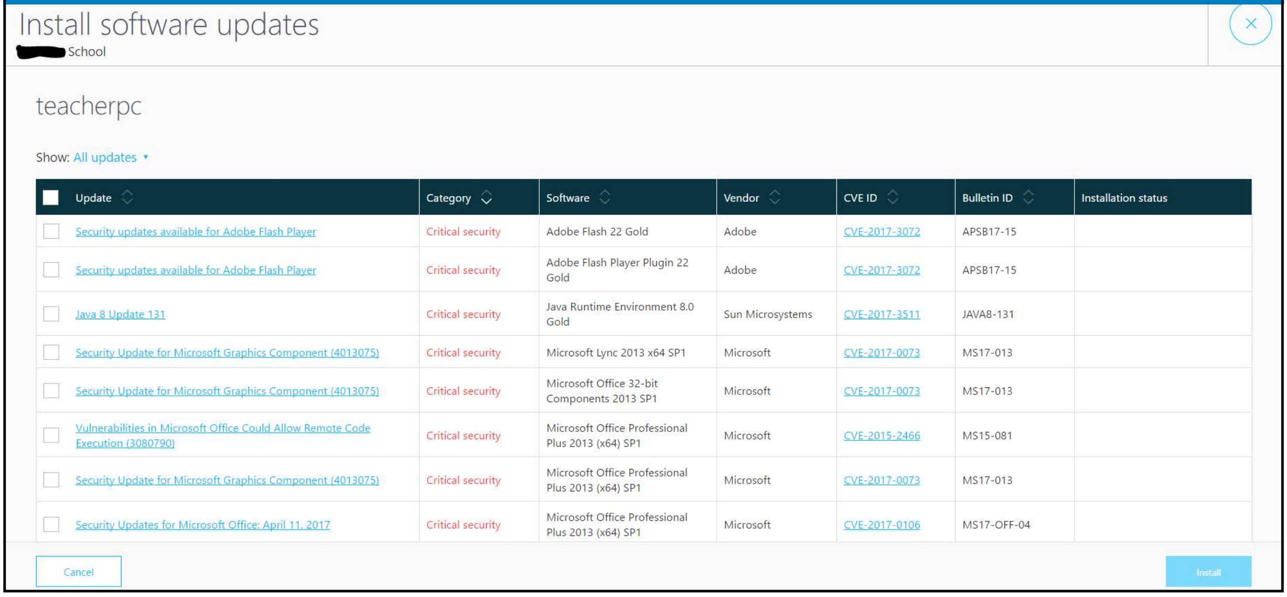
teacherpc Add alias

Status updated May 14, 2017 10:45:02 PM | Last connection May 14, 2017 10:44:36 PM | Registration date Apr 1, 2016

Protection status Operations Infections (0)

✓ Subscription	Valid
✓ Virus protection	Enabled
✓ Automatic updates	Up to date
! Software updates	Critical security updates m

Windows Update / Patch Management



Install software updates

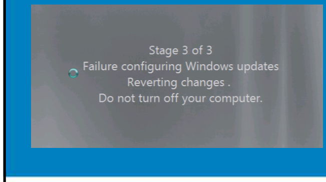
[redacted] School

teacherpc

Show: All updates

☐ Update	Category	Software	Vendor	CVE ID	Bulletin ID	Installation status
☐ Security updates available for Adobe Flash Player	Critical security	Adobe Flash 22 Gold	Adobe	CVE-2017-3072	APSB17-15	
☐ Security updates available for Adobe Flash Player	Critical security	Adobe Flash Player Plugin 22 Gold	Adobe	CVE-2017-3072	APSB17-15	
☐ Java 8 Update 131	Critical security	Java Runtime Environment 8.0 Gold	Sun Microsystems	CVE-2017-3511	JAVA8-131	
☐ Security Update for Microsoft Graphics Component (4013075)	Critical security	Microsoft Lync 2013 x64 SP1	Microsoft	CVE-2017-0073	MS17-013	
☐ Security Update for Microsoft Graphics Component (4013075)	Critical security	Microsoft Office 32-bit Components 2013 SP1	Microsoft	CVE-2017-0073	MS17-013	
☐ Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)	Critical security	Microsoft Office Professional Plus 2013 (x64) SP1	Microsoft	CVE-2015-2466	MS15-081	
☐ Security Update for Microsoft Graphics Component (4013075)	Critical security	Microsoft Office Professional Plus 2013 (x64) SP1	Microsoft	CVE-2017-0073	MS17-013	
☐ Security Updates for Microsoft Office: April 11, 2017	Critical security	Microsoft Office Professional Plus 2013 (x64) SP1	Microsoft	CVE-2017-0106	MS17-OFF-04	

為什麼這次那麼多電腦要更新及費時



Stage 3 of 3
Failure configuring Windows updates
Reverting changes .
Do not turn off your computer.

- 學校的使用者電腦，為了避免上課途中突然更新，大部分都停用了Windows更新設定
- 伺服器亦因避免更新後出現意料之外的反應，只會在長假期才更新
- 一般學校也不會設立自己的Windows Update Server，所以這次不能只夠內聯網更新，只能使用 Offline更新

環速集團
Speedy Group

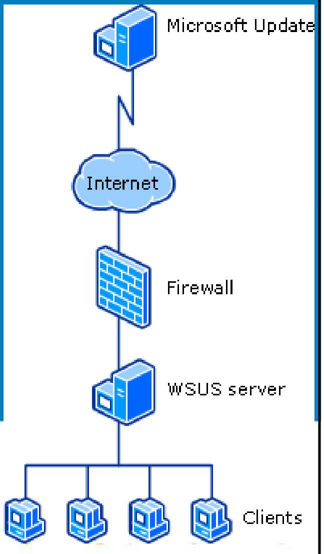
Management Software Comparison

	WSUS	SCCM	Third Party
Free of charge	Y	N	N
Easy to Manage	N	Y	Y
Easy to Setup	Y	N	N
Require Agent in Client	N	N	Y
Can manage Non-MS software	N	Y	Y
Can Push Install	N	Y	Y
Cache Windows Update Content	Y	Y	N

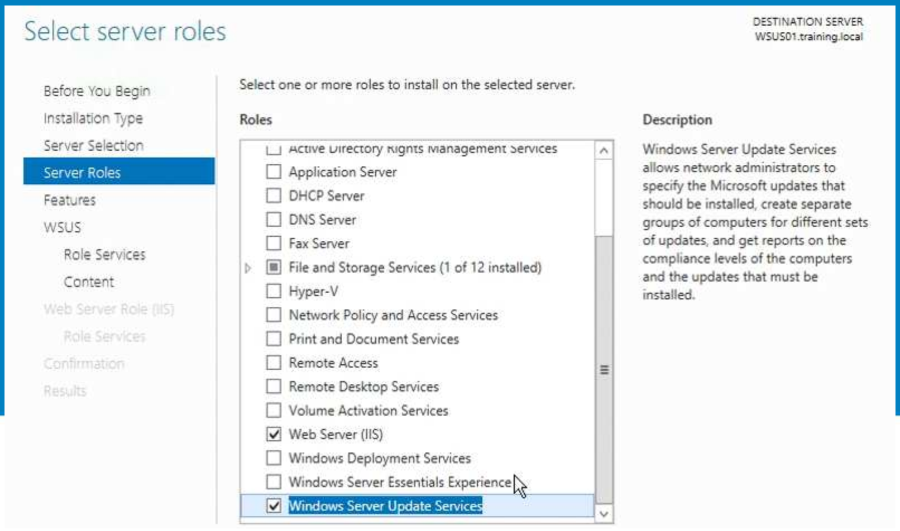
環速集團
Speedy Group

Windows Server Update Services

- 由 Windows Server 2008 R2 開始, WSUS 納入為伺服器角色之一
- 不可以在網域伺服器(Domain Controller)上安裝
- 只能管理已經加入網域的電腦
- 我們建議只用來管理使用者電腦



WSUS 安裝快照 – Step 1



Select server roles

DESTINATION SERVER
WSUS01.training.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- WSUS
  - Role Services
  - Content
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

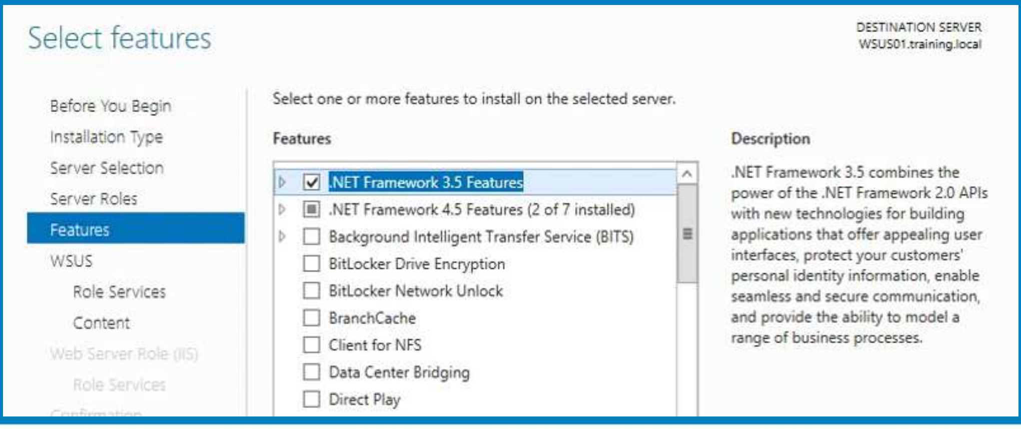
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☑ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☑ Windows Server Update Services

Description

Windows Server Update Services allows network administrators to specify the Microsoft updates that should be installed, create separate groups of computers for different sets of updates, and get reports on the compliance levels of the computers and the updates that must be installed.

環速集團
Speedy Group

WSUS 安裝快照 – Step 2



Select features

DESTINATION SERVER
WSUS01.training.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- WSUS
  - Role Services
  - Content
- Web Server Role (IIS)
  - Role Services
- Confirmation

Select one or more features to install on the selected server.

Features

- ☑ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play

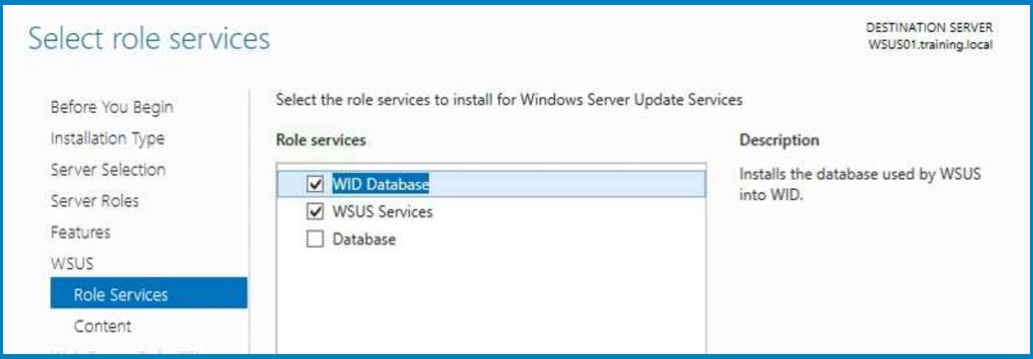
Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

WSUS Report 工具須要使用 .NET 2.0

環速集團
Speedy Group

WSUS 安裝快照 – Step 4



Select role services

DESTINATION SERVER
WSUS01.training.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- WSUS
  - Role Services
  - Content

Select the role services to install for Windows Server Update Services

Role services

- ☑ WID Database
- ☑ WSUS Services
- □ Database

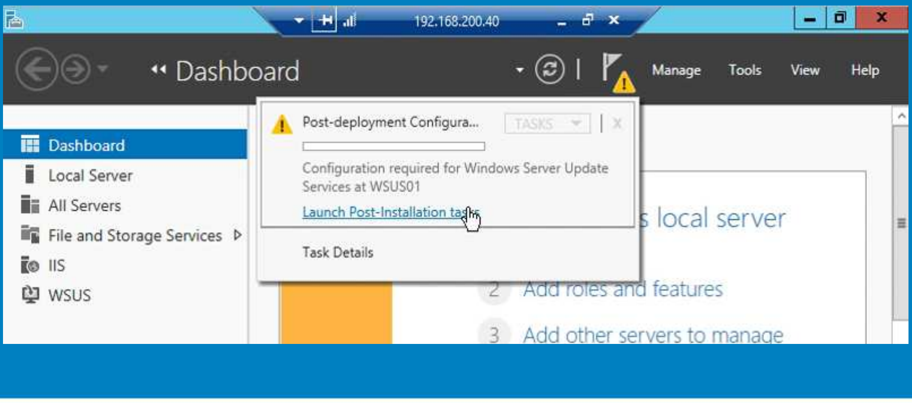
Description

Installs the database used by WSUS into WID.

為了使程序簡單點，使用內建資料庫

環速集團
Speedy Group

WSUS 安裝快照 – Step 5



Post-deployment Configura...

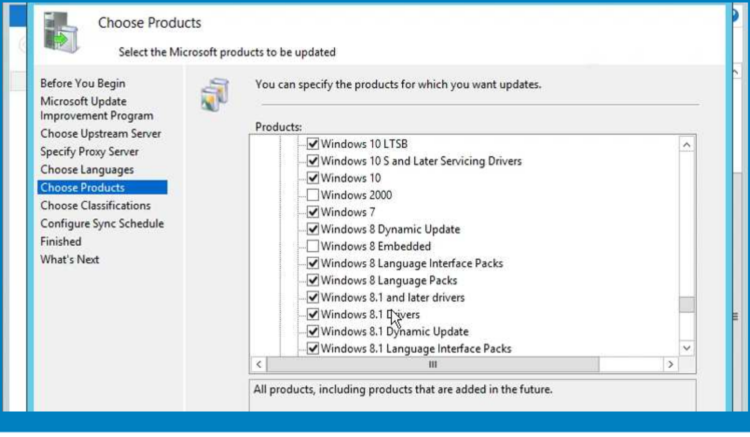
Configuration required for Windows Server Update Services at WSUS01

Launch Post-Installation tasks

安裝完成後，WSUS 伺服器 必須執行更新才可進行下一步

環速集團 Speedy Group

WSUS 安裝快照 – Step 6



Choose Products

Select the Microsoft products to be updated

You can specify the products for which you want updates.

Products:

- ☑ Windows 10 LTSB
- ☑ Windows 10 S and Later Servicing Drivers
- ☑ Windows 10
- □ Windows 2000
- ☑ Windows 7
- ☑ Windows 8 Dynamic Update
- □ Windows 8 Embedded
- ☑ Windows 8 Language Interface Packs
- ☑ Windows 8 Language Packs
- ☑ Windows 8.1 and later drivers
- ☑ Windows 8.1 Drivers
- ☑ Windows 8.1 Dynamic Update
- ☑ Windows 8.1 Language Interface Packs

All products, including products that are added in the future.

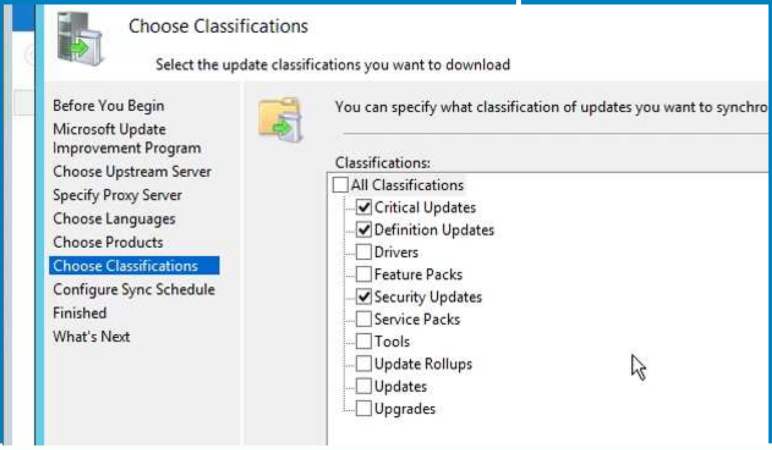
- 我們選了
  Windows 7
  Windows 8
  Windows
  Windows 10

  大概用了80GB Storage

也是不要全選。過了這個設定，WSUS的前置設定差不多完成了

環速集團 Speedy Group

WSUS 安裝快照 – Step 7



Choose Classifications

Select the update classifications you want to download

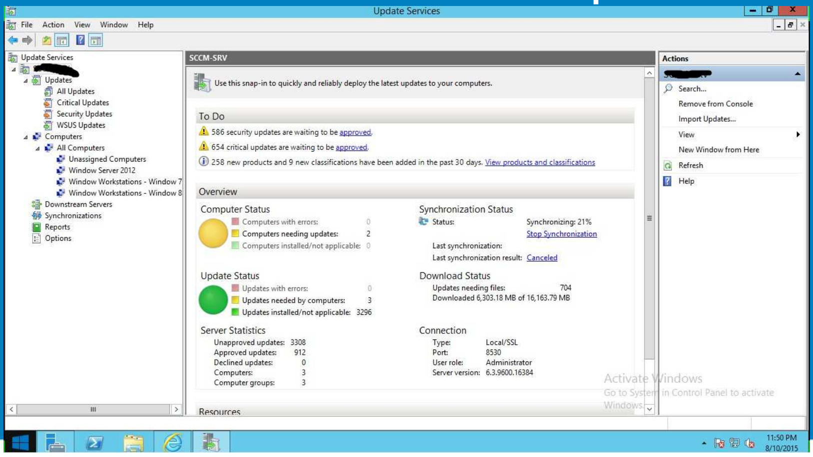
You can specify what classification of updates you want to synchro

Classifications:

- □ All Classifications
  - ☑ Critical Updates
  - ☑ Definition Updates
  - □ Drivers
  - □ Feature Packs
  - ☑ Security Updates
  - □ Service Packs
  - □ Tools
  - □ Update Rollups
  - □ Updates
  - □ Upgrades

也是不要全選。過了這個設定
WSUS的前置設定差不多完成了

WSUS 安裝快照 – Step 8



SCCM-SRV

Use this snap-in to quickly and reliably deploy the latest updates to your computers.

To Do

- ⚠ 586 security updates are waiting to be approved.
- ⚠ 654 critical updates are waiting to be approved.
- ⓘ 258 new products and 9 new classifications have been added in the past 30 days. View products and classifications

Overview

Computer Status

```
Computers with errors:              0
Computers needing updates:          2
Computers installed/not applicable: 0
```

Synchronization Status

```
Status:                        Synchronizing: 21%
                               Stop Synchronization
Last synchronization:
Last synchronization result:   Canceled
```

Update Status

```
Updates with errors:              0
Updates needed by computers:      3
Updates installed/not applicable: 3296
```

Download Status

```
Updates needing files:          704
Downloaded 6,303.18 MB of 16,163.79 MB
```

Server Statistics

```
Unapproved updates: 3308
Approved updates:    912
Declined updates:      0
Computers:             3
Computer groups:       3
```

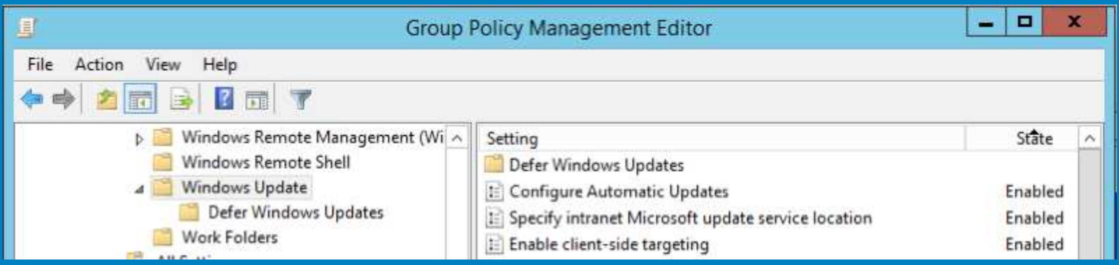
Connection

```
Type:            Local/SSL
Port:            8530
User role:       Administrator
Server version:  6.3.9600.16384
```

Resources

來到WSUS主畫面，我們可以看到簡單的資料

WSUS 安裝快照 – Step 9



Windows Remote Management (Wi
Windows Remote Shell
Windows Update
Defer Windows Updates
Work Folders

Setting	State
Defer Windows Updates	
Configure Automatic Updates	Enabled
Specify intranet Microsoft update service location	Enabled
Enable client-side targeting	Enabled

接著回到網域控制站，我們利用Group Policy來設定使用者電腦的更新行為

環速集團 Speedy Group

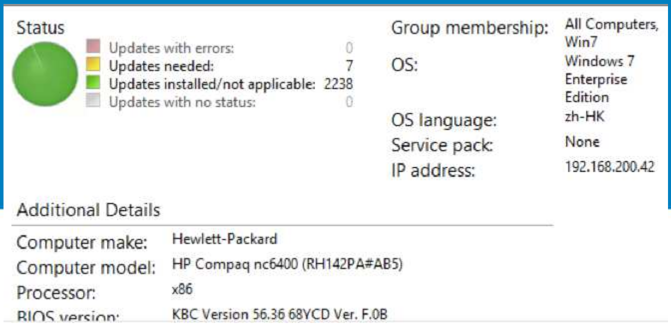
WSUS 安裝快照 – Step 9

- WSUS 相關的 GroupPolicy
  - 相關的 GroupPolicy 所在地
    - Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Update
  - Configure Automatic Updates - 要啟用自動更新才可配合WSUS
  - Enable client-side targeting - 令使用者電腦知道自己在WSUS那個更新群組
  - Specify intranet Microsoft update service location - 令使用者電腦知道WSUS的路徑在哪裡

環速集團 Speedy Group

WSUS 安裝快照 – Step 10

- 接著到使用者電腦更新Group Policy。
- 為確保GroupPolicy能成功套用到使用者電腦上，請使用gpupdate /sync指令來更新
- 重啟後，使用wuauctl.exe /detectnow與WSUS聯繫
- 另使用wuauctl.exe /reportnow 通知WSUS在本機已安裝的更新



Status

🟥 Updates with errors:	0
🟨 Updates needed:	7
🟩 Updates installed/not applicable:	2238
⬜ Updates with no status:	0

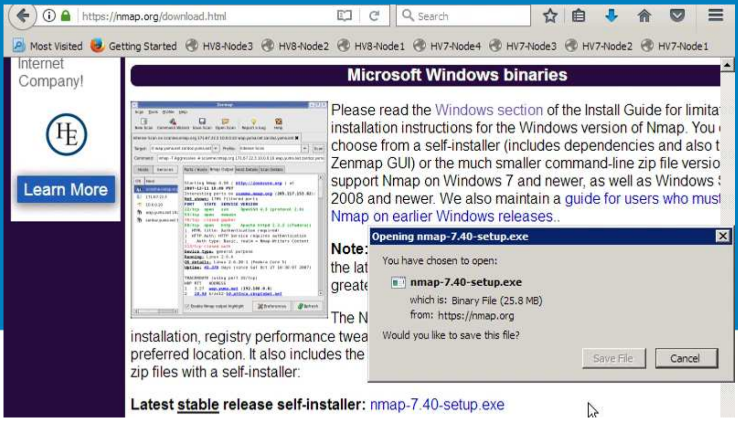
Group membership:	All Computers, Win7
OS:	Windows 7 Enterprise Edition
OS language:	zh-HK
Service pack:	None
IP address:	192.168.200.42

Additional Details

Computer make:	Hewlett-Packard
Computer model:	HP Compaq nc6400 (RH142PA#AB5)
Processor:	x86
BIOS version:	KBC Version 56.36 68YCD Ver. F.0B

快速偵測學校防火牆對外設定

- 在校外任一電腦安裝 nmap 軟件



Microsoft Windows binaries

Please read the Windows section of the Install Guide for limita installation instructions for the Windows version of Nmap. You choose from a self-installer (includes dependencies and also t Zenmap GUI) or the much smaller command-line zip file versio support Nmap on Windows 7 and newer, as well as Windows 2008 and newer. We also maintain a guide for users who mus Nmap on earlier Windows releases..

Note: the lat greate

The N installation, registry performance twea preferred location. It also includes the zip files with a self-installer:

Latest stable release self-installer: nmap-7.40-setup.exe

Opening nmap-7.40-setup.exe

You have chosen to open:

nmap-7.40-setup.exe

which is: Binary File (25.8 MB)

from: https://nmap.org

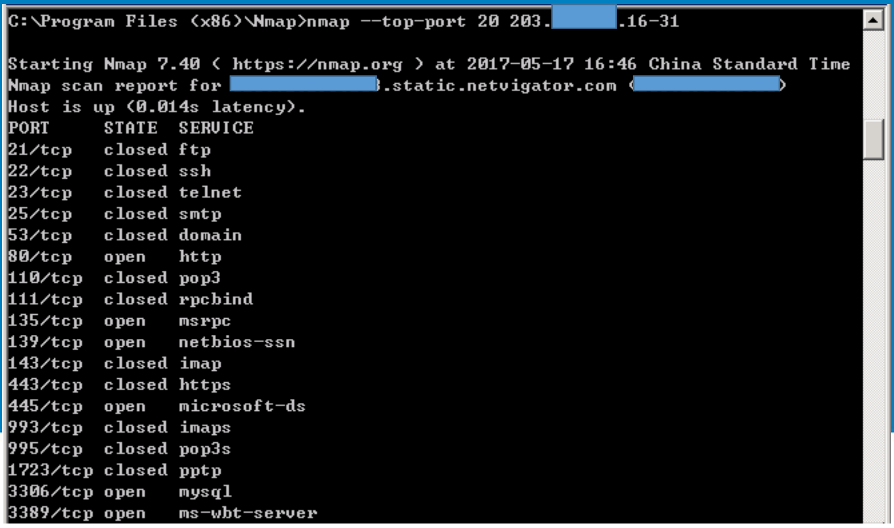
Would you like to save this file?

快速偵測學校防火牆對外設定

- 然後在Command Prompt移到 nmap 安裝位置
- 執行 nmap –top-port 20 x.x.x.y-z
- x.x.x.y 即校內起始的Pubilc IP, z 即結尾數字

環速集團 Speedy Group

快速偵測學校防火牆對外設定



```
C:\Program Files (x86)\Nmap>nmap --top-port 20 203.[redacted].16-31

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-17 16:46 China Standard Time
Nmap scan report for [redacted].static.netvigator.com ([redacted])
Host is up (0.014s latency).
PORT      STATE  SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    open   http
110/tcp   closed pop3
111/tcp   closed rpcbind
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
143/tcp   closed imap
443/tcp   closed https
445/tcp   open   microsoft-ds
993/tcp   closed imaps
995/tcp   closed pop3s
1723/tcp  closed pptp
3306/tcp  open   mysql
3389/tcp  open   ms-wbt-server
```

環速集團 Speedy Group

- WannaCry 資訊分享平台

www.facebook.com/SpeedyGroupHK

speedygrouphk

Find us on facebook

環速集團
Speedy Group