教育體系資安檢核

臺灣大學計資中心網路組
游子興
davisyou@ntu.edu.tw
02-33665008

個人電腦/網域主機
安全防護檢核

檢核項目

* 作業系統
* 應用程式
* 防毒軟體
* 惡意程式檢測

作業系統版本
Windows 10

Windows 10 versions

Version	Codename	Marketing name	Build	Release date	Support until (and support status by color)			
					Home · Pro · Pro Education · Pro for Workstations	Enterprise · Education	LTSC	Mobile
1507	Threshold 1	N/A	10240	July 29, 2015	May 9, 2017		October 14, 2025	N/A
1511	Threshold 2	November Update	10586	November 10, 2015	October 10, 2017		N/A	January 9, 2018
1607	Redstone 1	Anniversary Update	14393	August 2, 2016	April 10, 2018	April 9, 2019	October 13, 2026	October 9, 2018
1703	Redstone 2	Creators Update	15063	April 5, 2017	October 9, 2018	October 8, 2019	N/A	June 11, 2019
1709	Redstone 3	Fall Creators Update	16299	October 17, 2017	April 9, 2019	October 13, 2020		January 14, 2020
1803	Redstone 4	April 2018 Update	17134	April 30, 2018	November 12, 2019	November 10, 2020		N/A
1809	Redstone 5	October 2018 Update	17763	November 13, 2018	November 10, 2020	May 11, 2021	**January 9, 2029**	
1903	19H1	May 2019 Update	18362	May 21, 2019	December 8, 2020		N/A	
1909	19H2	November 2019 Update	18363	November 12, 2019	May 11, 2021	May 10, 2022		
2004	20H1	May 2020 Update	19041	May 27, 2020	**December 14, 2021**			
20H2	20H2	TBA	19042	TBA	18 months	30 months	TBA	
Dev Channel			20197	N/A	Rolling Builds in Development		N/A	

Legend: Old version · Older version, still maintained · **Latest version** · Preview version

* https://en.wikipedia.org/wiki/Windows_10_version_history

smb: ms17-010/EternalBlue

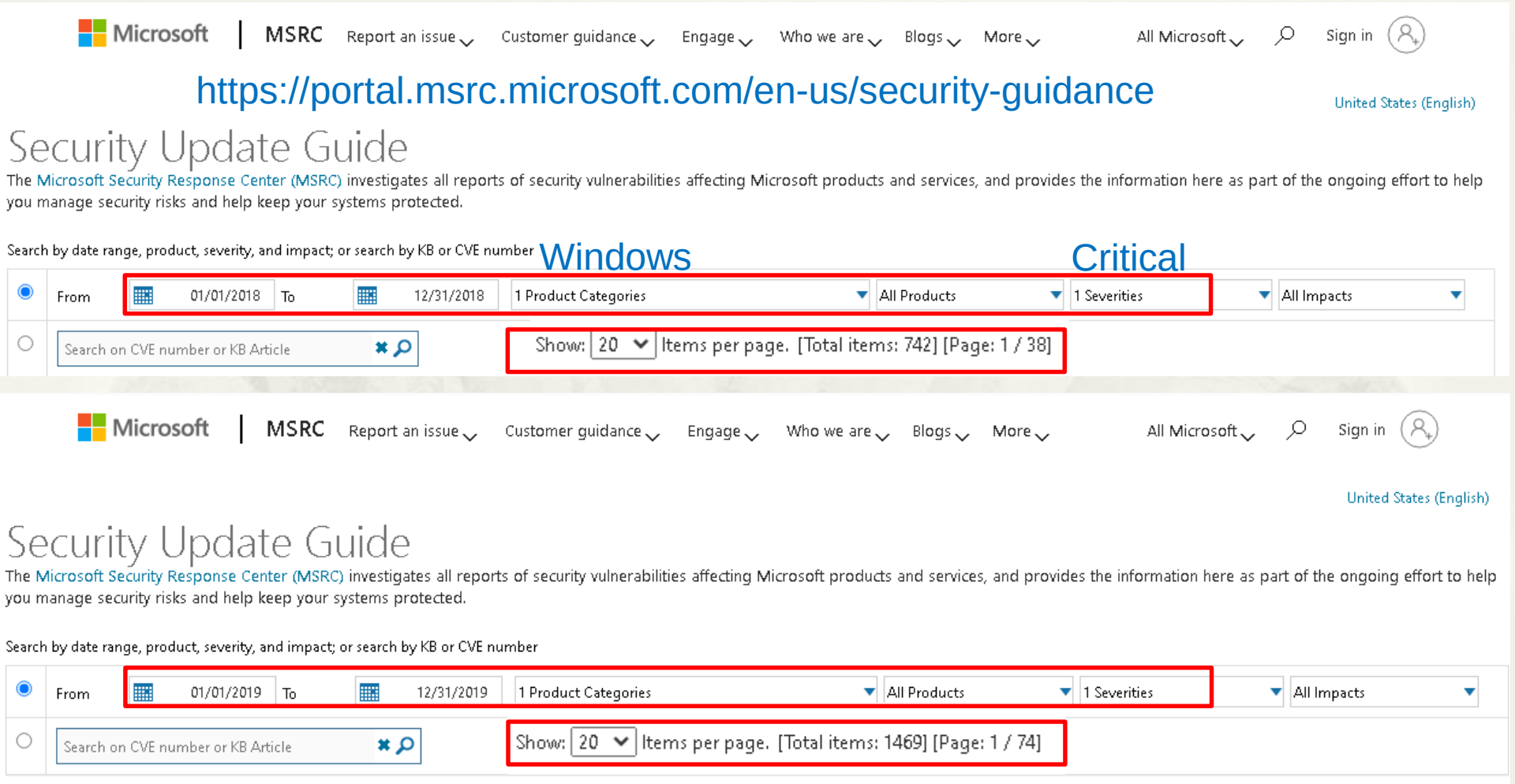
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
- CVE-2017-0143 ~ CVE-2017-0148

Windows 7
[Windows 7 for 32-bit Systems Service Pack 1] (http://catalog.update.microsoft.com/v7/site/ q=kb4012212) (4012212) Security Only[1]
[Windows 7 for 32-bit Systems Service Pack 1] (http://catalog.update.microsoft.com/v7/site/ q=kb4012215) (4012215) Monthly Rollup[1]
[Windows 7 for x64-based Systems Service Pa (http://catalog.update.microsoft.com/v7/site/ q=kb4012212) (4012212) Security Only[1]
[Windows 7 for x64-based Systems Service Pa (http://catalog.update.microsoft.com/v7/site/ q=kb4012215) (4012215) Monthly Rollup[1]

Windows 10
[Windows 10 for 32-bit Systems] (http://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012606)[3] (4012606)
[Windows 10 for x64-based Systems] (http://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4012606)[3] (4012606)
[Windows 10 Version 1511 for 32-bit Systems] (http://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013198)[3] (4013198)
[Windows 10 Version 1511 for x64-based Systems] (http://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013198)[3] (4013198)
[Windows 10 Version 1607 for 32-bit Systems] (http://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013429)[3] (4013429)
[Windows 10 Version 1607 for x64-based Systems] (http://catalog.update.microsoft.com/v7/site/search.aspx?q=kb4013429)[3] (4013429)

Vulnerability title	**CVE number**	**Publicly disclosed**
Windows SMB Remote Code Execution Vulnerability	[CVE-2017-0143] (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0143)	No
Windows SMB Remote Code Execution Vulnerability	[CVE-2017-0144] (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144)	No
Windows SMB Remote Code Execution Vulnerability	[CVE-2017-0145] (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0145)	No
Windows SMB Remote Code Execution Vulnerability	[CVE-2017-0146] (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0146)	No
Windows SMB Remote Code Execution Vulnerability	[CVE-2017-0148] (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0148)	No

Microsoft Security Response Center

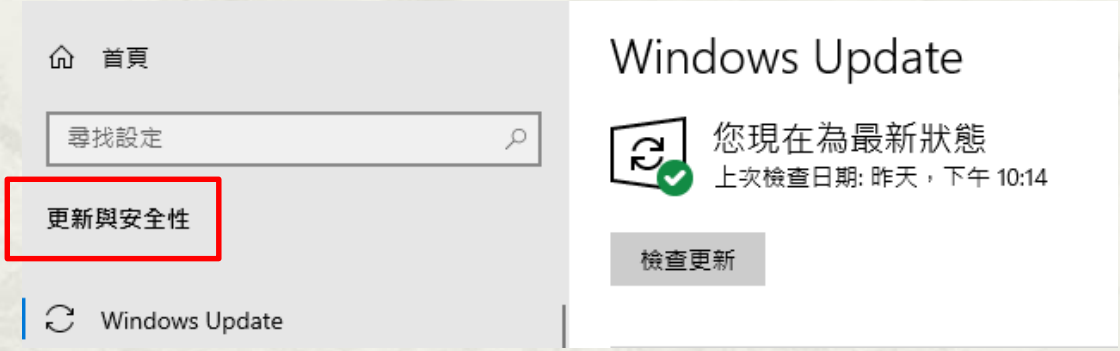


作業系統版本
Windows 10

* 設定 -> 系統 -> 關於

作業系統更新
Windows

* 三種方法
  * 1.設定 -> 更新與安全性
    * 上次更新時間
    * 是否啟用自動更新



  * 2.Microsoft Baseline Security Analyzer (win10 不支援)
  * 3.Windows Update offline scan file (wsusscn2.cab) to Scan for Updates

Microsoft Baseline Security Analyzer 微軟基準安全分析器(win10 不支援)

- 掃描 Windows 電腦，檢查作業系統和其他已安裝的元件 有沒有安全性組態錯誤，以及是否具備最新的安全性 Hotfix 和修補套件。
- 使用 HFNetChk 工具來識別系統是否已套用了安全性更新檔。HFNetChk 是藉由參考 Microsoft 不斷更新的可延伸標記語言 (XML) 安全性 Hotfix 資料庫來執行這項工作。
- 雖然 MBSA 版本2.3 推出了 Windows Server 2012 R2 和 Windows 8.1 的支援，但它已被棄用，且不再開發。MBSA 2.3 沒有更新成完全支援 Windows 10 和 Windows Server 2016。
- https://docs.microsoft.com/zh-tw/windows/security/threat-protection/mbsa-removal-and-guidance

Windows Update offline scan file wsusscn2.cab

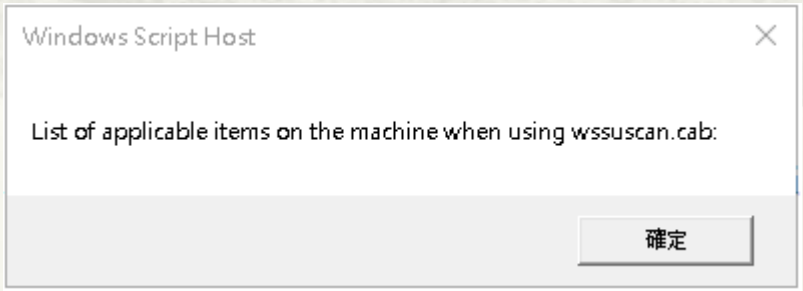
- a cabinet file contains info about security-related, but it doesn't contain the security updates themselves.
- For the computers that aren't connected to the Internet can be scanned to see whether these security-related updates are present or required.
  - wsusscn2.cab Download:
  - http://go.microsoft.com/fwlink/p/?LinkID=74689

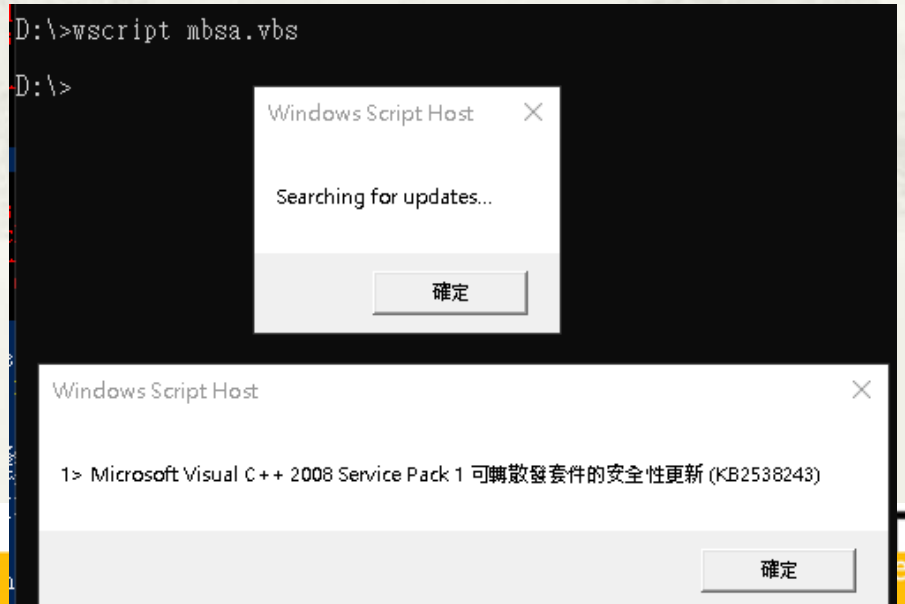
Using WUA to Scan for Updates Offline with VBscript

- Using WUA to Scan for Updates Offline
  - https://docs.microsoft.com/en-us/windows/win32/wua_sdk/using-wua-to-scan-for-updates-offline
- Copy & save to file mbsa.vbs
- Modify wsusscn2.cab file path

```
Set UpdateSession = CreateObject("Microsoft.Update.Session")
Set UpdateServiceManager = CreateObject("Microsoft.Update.ServiceManager")
Set UpdateService = UpdateServiceManager.AddScanPackageService("Offline Sync Service", "d:\wsusscn2.cab", 1)
Set UpdateSearcher = UpdateSession.CreateUpdateSearcher()
```

- 系統管理者身份執行
  - wscript mbsa.vbs





Using WUA to Scan for Updates Offline with PowerShell

- Using WUA to Scan for Updates Offline with PowerShell
  - https://gallery.technet.microsoft.com/Using-WUA-to-Scan-for-f7e5e0be
  - Copy & save to file Scan-UpdatesOffline.ps1
  - Modify wsusscn2.cab file path

```
$UpdateSession = New-Object -ComObject Microsoft.Update.Session
$UpdateServiceManager  = New-Object -ComObject Microsoft.Update.ServiceManager
$UpdateService = $UpdateServiceManager.AddScanPackageService("Offline Sync Service", "d:\wsusscn2.cab", 1)
$UpdateSearcher = $UpdateSession.CreateUpdateSearcher()
```

  - 系統管理者身份開啟 Powershell 執行
    - ./Scan-UpdatesOffline.ps1

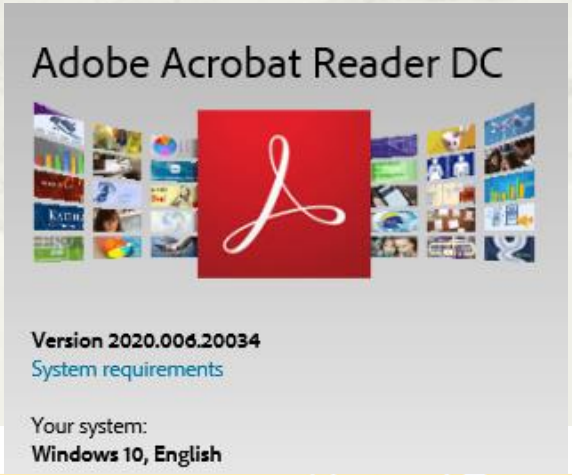
```
PS D:\> ./Scan-UpdatesOffline.ps1

安全性警告
只執行您信任的指令碼。來自網際網路的指令碼雖然可能很有用，但是這個指令碼有可能會傷害您的電腦。若信任此指令碼，請使用
Unblock-File Cmdlet 來允許執行指令碼，而不顯示此警告訊息。您要執行 D:\Scan-UpdatesOffline.ps1 嗎?
[D] 不要執行(D)  [R] 執行一次(R)  [S] 暫停(S)  [?] 說明 (預設值為 "D"): r
Searching for updates...

List of applicable items on the machine when using wssuscan.cab:

0> Microsoft Visual C++ 2008 可轉散發套件的安全性更新 (KB973924)
1> Security Update for Microsoft ASP.NET MVC 2 (KB2993939)
2> Microsoft Visual C++ 2008 Service Pack 1 可轉散發套件的安全性更新 (KB2538243)
PS D:\>
```

尚未安裝的更新

應用程式更新檢核
人工檢查

* Java
  * https://www.java.com/en/download/

* Adobe Acrobat Reader
  * https://get.adobe.com/reader/



應用程式更新檢核
批次檢查

* 匯出目前電腦所有安裝程式列表
  * wmic product get /format:csv > software.csv

Column15	Column26	Column27
Name	Vendor	Version
Office 16 Click-to-Run Extensibility Component	Microsoft Corporation	16.0.10356.20006
Office 16 Click-to-Run Localization Component	Microsoft Corporation	16.0.10356.20006
Office 16 Click-to-Run Licensing Component	Microsoft Corporation	16.0.10356.20006
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005	Microsoft Corporation	12.0.21005
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005	Microsoft Corporation	12.0.21005
Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.24215	Microsoft Corporation	14.0.24215
Java 8 Update 241	Oracle Corporation	8.0.2410.7
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005	Microsoft Corporation	12.0.21005
Adobe Refresh Manager	Adobe Systems Incorporated	1.8.0
Adobe Acrobat Reader DC - Chinese Traditional	Adobe Systems Incorporated	20.006.20034
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005	Microsoft Corporation	12.0.21005
Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.24215	Microsoft Corporation	14.0.24215
Google Update Helper	Google LLC	1.3.35.441
64 Bit HP CIO Components Installer	Hewlett-Packard	16.2.1
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022	Microsoft Corporation	9.0.21022
VMware Remote Console	VMware	Inc.
Java Auto Updater	Oracle Corporation	2.8.241.7

防毒軟體檢核

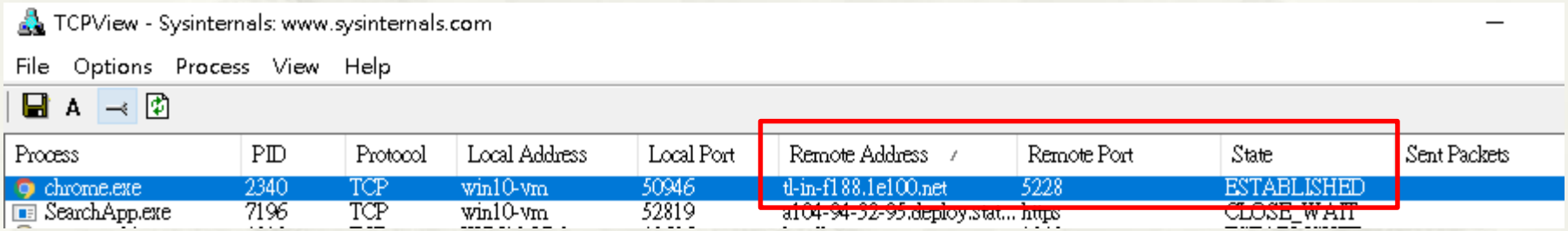
- Antivirus Version Check
- Signature pattern update
- Full Scan Frequency
  - at least half year.
- Win10
  - 設定 -> 更新與安全性 -> Windows 安全性 -> 病毒與威脅防護

惡意程式檢測
網路連線

- TCPView v3.05
  - https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
  - Options -> Resolve Addresses= Uncheck
  - 連線檢核
    - 忽略 Process= browser(ie,chrome,firefox) and Remote port = 80/443
    - Remote Address <> 0.0.0.0/127.0.0.1 and State= ESTABLISHED
  - Listen Port 檢核
    - Local Address = 0.0.0.0 and State= LISTENING

惡意程式檢測
網路連線

* Google Search
  * chrome port 5228

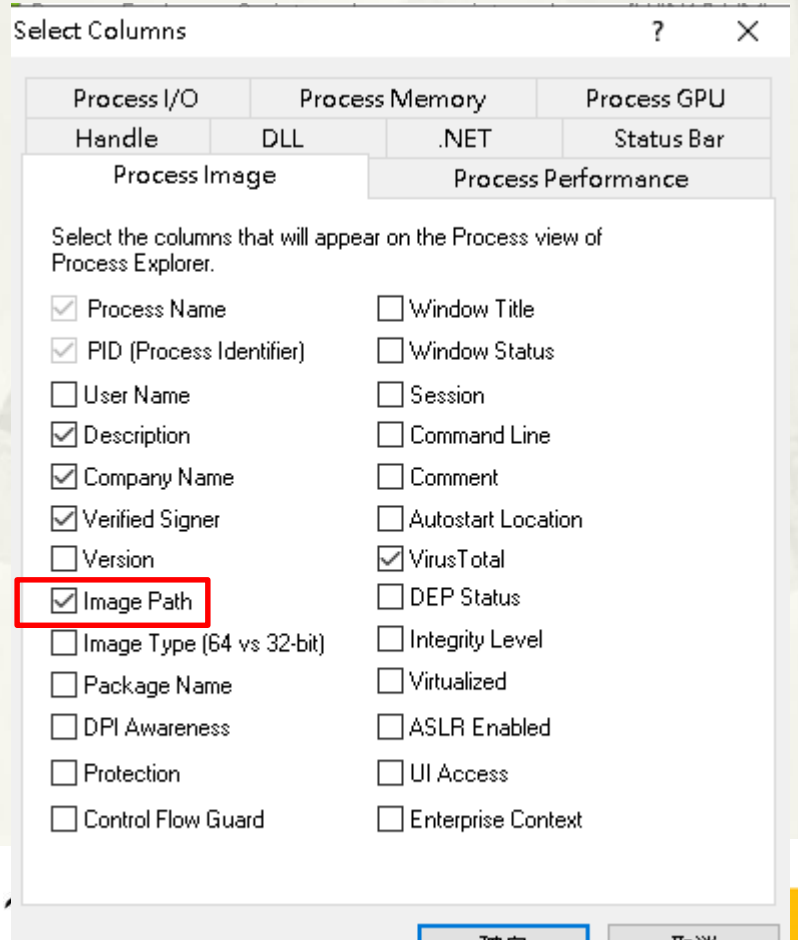


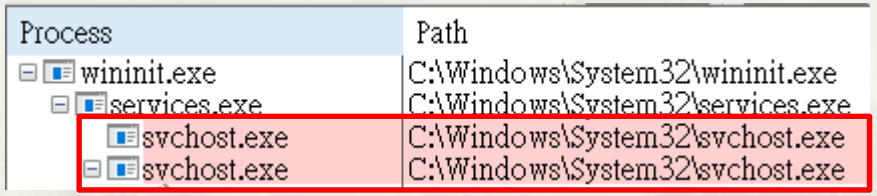
惡意程式檢測
執行程序

- Process Explorer
  - https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
  - 建議用系統管理者權限執行
  - 程式簽章檢核
    - Option -> Verify Image Signatures
  - VirusTotal 檢核
    - Option -> VirusTotal.com -> Check VirusTotal.com

惡意程式檢測
執行程序

* 程式執行目錄檢核 (run in wrong folder)
  * View -> Select Columns





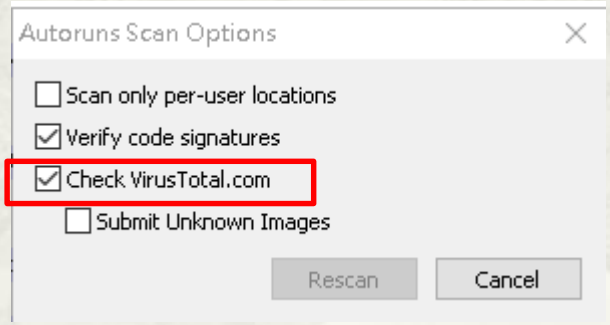
異常:
C:\Windows\Setup Library\svchost.exe /service

惡意程式檢測
執行程序 psinfo (補充)

- PsTools v1.78 06/29/2016
  - https://docs.microsoft.com/en-us/sysinternals/downloads/pstools
  - psinfo -h -s -d >info.log 2>NUL
    - -h Show installed hotfixes.
    - -s Show installed software.
    - -d Show disk volume information.
  - pslist -t
    - -t Show process tree.

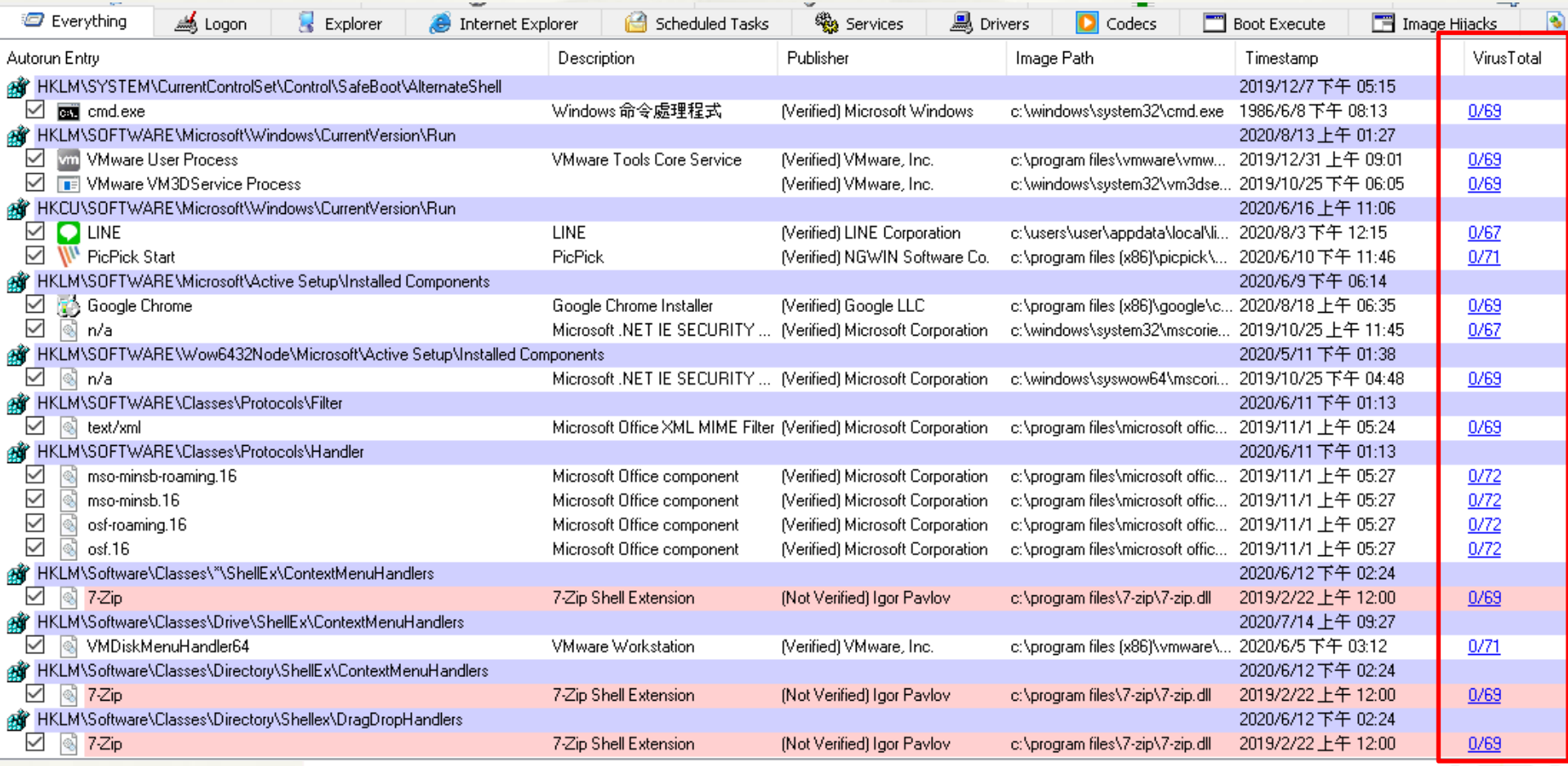
惡意程式檢測
開機啟動程式

* Autorun
  * https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
  * Options -> Scan Options



惡意程式檢測
開機啟動程式

* Everything



Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot Execute | Image Hijacks

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019/12/7 下午 05:15	
cmd.exe	Windows 命令處理程式	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1986/6/8 下午 08:13	0/69
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2020/8/13 上午 01:27	
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware\vmw...	2019/12/31 上午 09:01	0/69
VMware VM3DService Process		(Verified) VMware, Inc.	c:\windows\system32\vm3dse...	2019/10/25 下午 06:05	0/69
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2020/6/16 上午 11:06	
LINE	LINE	(Verified) LINE Corporation	c:\users\user\appdata\local\li...	2020/8/3 下午 12:15	0/67
PicPick Start	PicPick	(Verified) NGWIN Software Co.	c:\program files (x86)\picpick\...	2020/6/10 下午 11:46	0/71
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020/6/9 下午 06:14	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\c...	2020/8/18 上午 06:35	0/69
n/a	Microsoft .NET IE SECURITY ...	(Verified) Microsoft Corporation	c:\windows\system32\mscorie...	2019/10/25 上午 11:45	0/67
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020/5/11 下午 01:38	
n/a	Microsoft .NET IE SECURITY ...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscori...	2019/10/25 下午 04:48	0/69
HKLM\SOFTWARE\Classes\Protocols\Filter				2020/6/11 下午 01:13	
text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	2019/11/1 上午 05:24	0/69
HKLM\SOFTWARE\Classes\Protocols\Handler				2020/6/11 下午 01:13	
mso-minsb-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	2019/11/1 上午 05:27	0/72
mso-minsb.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	2019/11/1 上午 05:27	0/72
osf-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	2019/11/1 上午 05:27	0/72
osf.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft offic...	2019/11/1 上午 05:27	0/72
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers				2020/6/12 下午 02:24	
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll	2019/2/22 上午 12:00	0/69
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				2020/7/14 上午 09:27	
VMDiskMenuHandler64	VMware Workstation	(Verified) VMware, Inc.	c:\program files (x86)\vmware\...	2020/6/5 下午 03:12	0/71
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				2020/6/12 下午 02:24	
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll	2019/2/22 上午 12:00	0/69
HKLM\Software\Classes\Directory\Shellex\DragDropHandlers				2020/6/12 下午 02:24	
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll	2019/2/22 上午 12:00	0/69

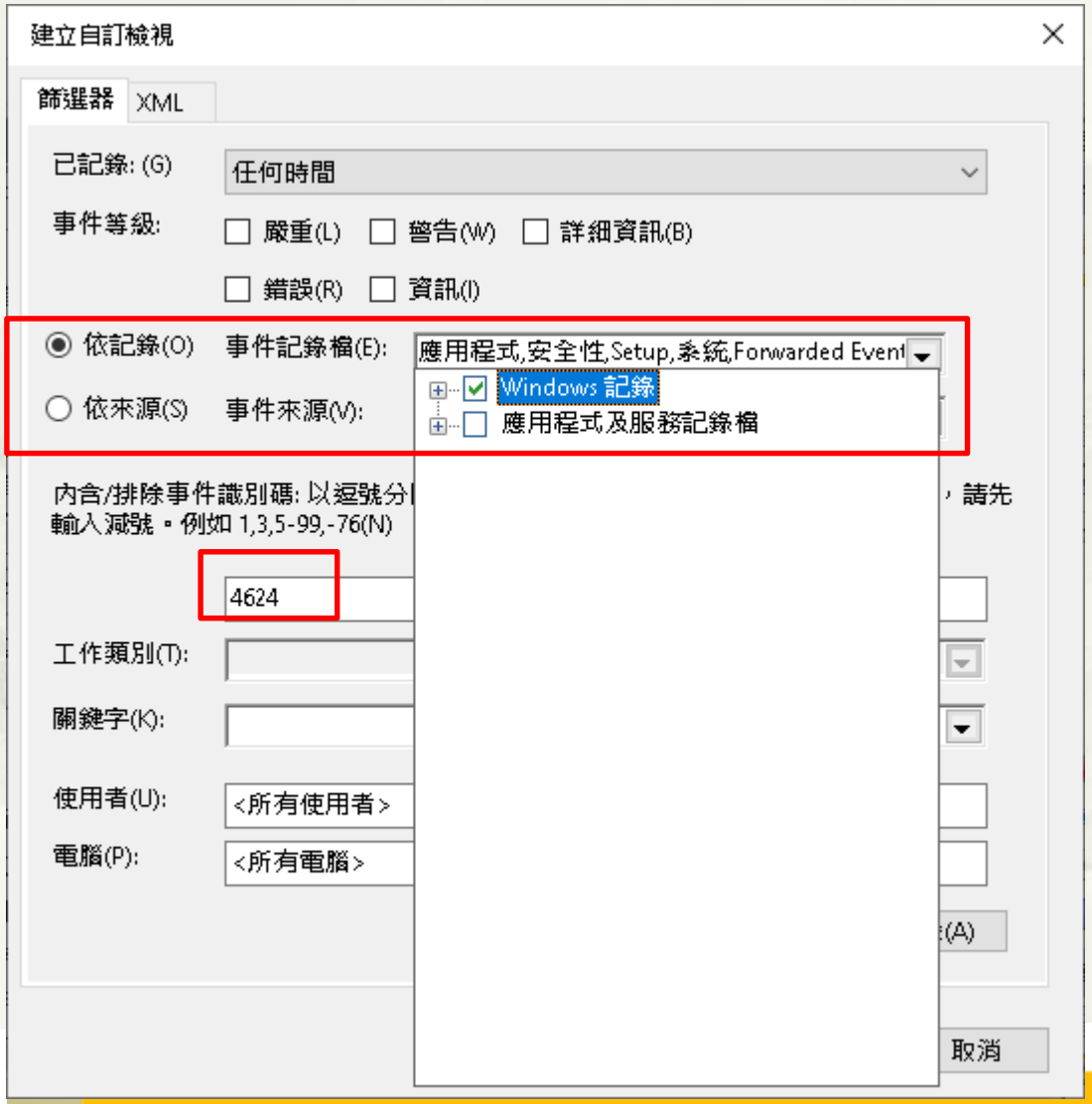
惡意程式檢測
Log Review (Windows)

* Windows Events
  * event.code 4624
    * 帳戶已順利登入
  * event.code 4625
    * 帳戶無法登入
  * event.code 7045
    * 服務已經安裝在系統中

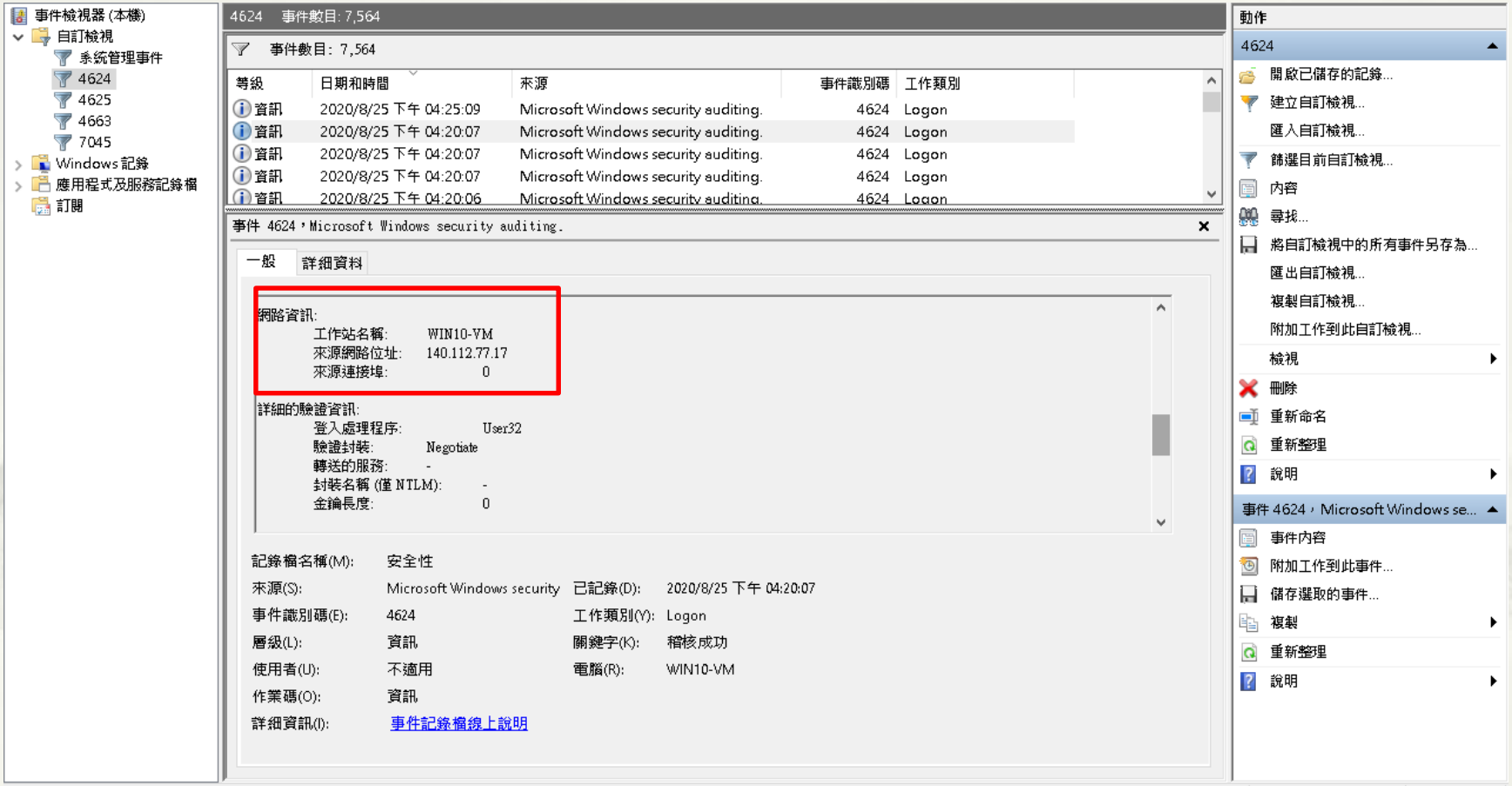
惡意程式檢測
Log Review (Windows)

* 事件檢視器
  * 開始 -> Windows 系統工具 -> 事件檢視器
  * 開始 -> 執行: eventvwr.msc

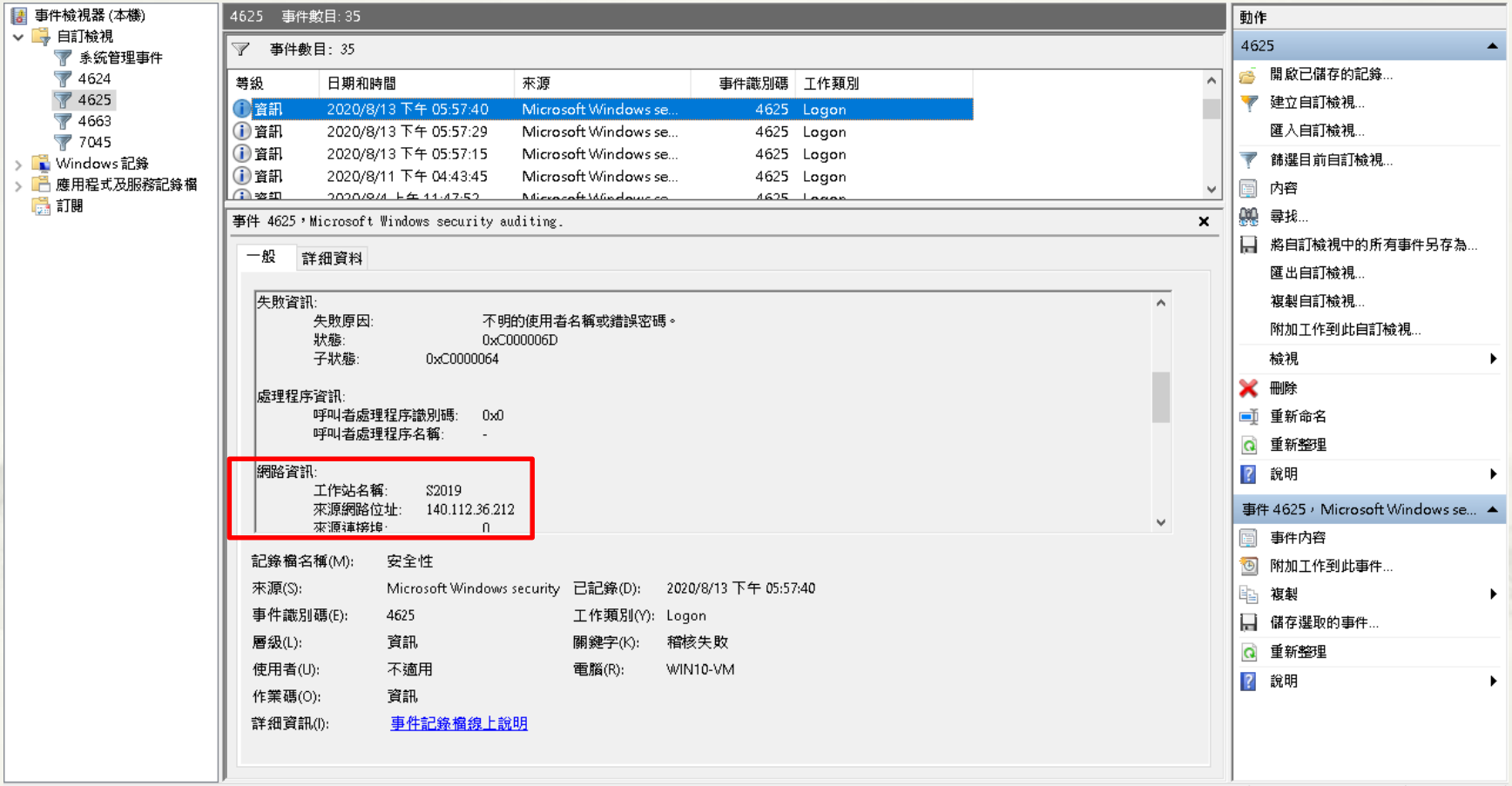
惡意程式檢測
Log Review (Windows)



event.code 4624
帳戶已順利登入



event.code 4625
帳戶無法登入



event.code 7045
服務已經安裝在系統中

服務名稱: mNHIICC
服務檔案名稱: C:\Program Files (x86)\NHI\mNHIICC\mNHIICCService.exe
服務類型: 使用者模式服務
服務啟動類型: 自動啟動
服務帳戶: LocalSystem

健保卡元件程式安裝

其他檢測

* 系統時間是否精準
  * 自動校時設定: NTP
* 螢幕保護程式
  * 15min、密碼鎖定

簡報完畢
謝謝