

# 學術網路資安事件案例分析& 主機檢測工具

北區ASOC 二線工程師：劉家維

# 外部攻擊趨勢

- 以針對IOT或網路設備的弱點掃描攻擊占大宗。
- 從趨勢圖中可以發現幾個異常攻擊事件增加的時間與該設備爆發漏洞的時間相符。
- 例如：
  1. 一月中旬的DVR影像主機漏洞
  2. 四月的DrayTek路由器，與DD-WRT韌體漏洞

# 惡意軟體行為

---

1. 加密勒索
2. 散播BOT
3. 挖礦劫持
4. 竊取資料

# 目標式勒索病毒攻擊台灣企業

## 趨勢揭露鎖定臺灣企業的勒索軟體攻擊行動，1 事故是否有關

鎖定石化工業與高科技製造業的攻擊，從5月4日開始接連發生，其中有些是利用勒索軟體發動的攻擊。趨勢科技也發現一波新的勒索軟體攻擊行動，發生時間也是在5月初，不過沒有指出這起行動與前述攻擊事件有無關連。

文 / 周峻佑 | 2020-05-08 發表

讚 6.1 萬 按讚加入iThome粉絲團



The screenshot shows the top portion of a web article. At the top left is the Trend Micro logo. To its right is the 'SECURITY INTELLIGENCE Blog' header with the tagline 'SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS'. A search bar is located to the right of the header. Below the header is a navigation menu with 'Home' and 'Categories' options. The main content area shows the breadcrumb 'Home » Malware » Targeted Ransomware Attack Hits Taiwanese Organizations' and the article title 'Targeted Ransomware Attack Hits Taiwanese Organizations'. At the bottom of the article preview, it states 'Posted on: May 6, 2020 at 5:00 am', 'Posted in: Malware', and 'Author: Trend Micro'.

自由財經

首頁 > 財經政策

## 中油、台塑、力成 連遭勒索病毒攻擊

2020-05-06 05:30



中油及台塑四日起陸續遭惡意軟體攻擊，國安及資安體系研判此非個案，不排除是針對五二〇蔡英文總統就職典禮前的

# 視訊監控主機遭駭，成為DDoS攻擊幫兇



**iCATCH** 繁體中文 / English Search

首頁 公司介紹 產品資訊 最新消息 下載專區 支援服務 合作夥伴 聯絡我們

## 可取國際聲明啟事

<< 資安通報 >>  
近日來可取國際公司資訊管理部門監測到多起網路異常活動，針對我司數位錄放影機進行網路攻擊。

在此強烈建議所有用戶依照下列方式，修改您錄放影機的設定：

1. 請將韌體更新至最新版本；
2. 更新完成後，務必修改管理者的出廠預設密碼，以提升安全層級。  
(強烈建議混合英文、數字和特殊字元為最佳安全保障)

若有發生其他相關狀況的客戶，請聯絡我們全省合作夥伴，可取國際會協同我們的合作夥伴一同面對並盡速處理。謝謝您！

2020.01.16



新聞

## 又有臺廠DVR設備被揭露資安漏洞，過去半年遭多個攻擊組織鎖定用以傳播殭屍網路

近日有資安業者揭露，多個攻擊組織鎖定利凌企業 (Lilin) 視訊監控主機 (DVR) 的零時差漏洞，散布殭屍網路。利凌企業在收到通報已立即修補，用戶儘速更新，避免淪為DDoS攻擊幫兇。此事件還可能牽扯供應鏈安全議題，因為，與之前可取國際 (iCatch) DVR遭駭的IoT攻擊事件，存在韌體寫死相同敏感資料的狀況。

文/ 羅正漢 | 2020-03-31 發表

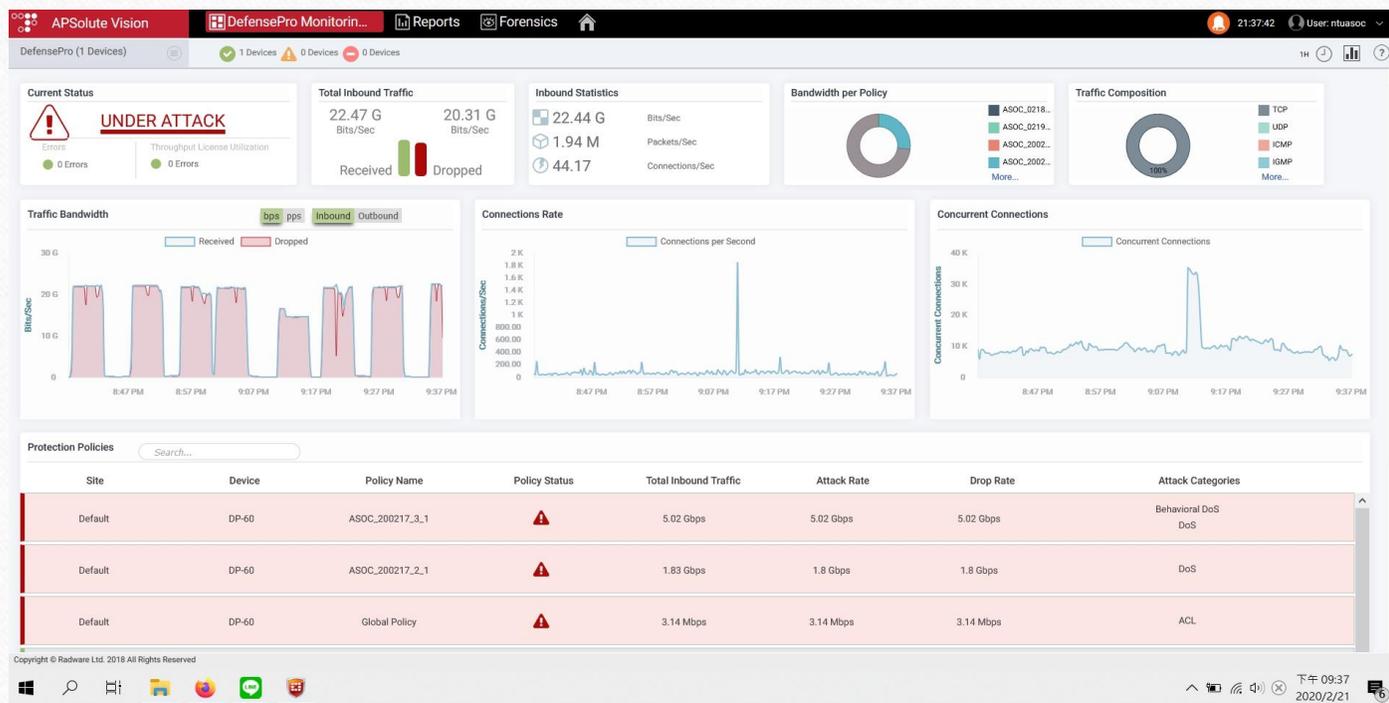
讚 6.1萬 按讚加入iThome粉絲團 讚 0 分享

20 MARCH 2020 / LILIN DVR

## LILIN DVR 在野0-day 漏洞分析報告

iThome 2020臺灣雲端大會  
2020/9/8 (二) 09:00 - 16:30  
台北國際會議中心 (TICC)

# 實際偵測之DDoS攻擊流量



# 利用IoT搜尋引擎查詢攻擊來源

 **175.183.80.178** 175-183-80-178.adsl.dynamic.seed.net.tw

self-signed

City	Nantou
Country	Taiwan
Organization	Taiwan Infrastructure Network Technologie
ISP	New Century InfoComm Tech. Co.
Last Update	2020-03-14T00:03:25.712607
Hostnames	175-183-80-178.adsl.dynamic.seed.net.tw
ASN	AS18049

## Ports

80

443

554

## Services

80

tcp

http



HTTP/1.1 401 Unauthorized  
Server: mini\_httpd/1.19 19dec2003  
Date: Thu, 12 Mar 2020 01:39:31 GMT  
Cache-Control: no-cache,no-store  
WWW-Authenticate: Basic realm="DVR"  
Content-Type: text/html; charset=%s  
Connection: close

443

tcp

https



HTTP/1.1 401 Unauthorized  
Server: mini\_httpd/1.19 19dec2003  
Date: Sat, 14 Mar 2020 00:09:09 GMT  
Cache-Control: no-cache,no-store  
WWW-Authenticate: Basic realm="DVR"  
Content-Type: text/html; charset=%s  
Connection: close

# DVR影像主機案例

# 異常DVR主機封包範例

關鍵字：uc-httpd 1.0.0、雄邁韌體漏洞

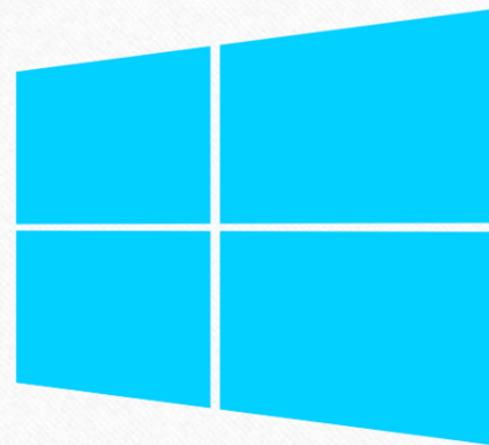
No.	Time	Source	Destination	Protocol	Length	SourcePort	DestinationPort	Info
4601	2020-02-27 07:09:58.503515	140.112.254.4	163.28.16.80	DNS	89	53	42228	Standard query response 0x1998 A xmsecu100.net A 156.255.121.99
4602	2020-02-27 07:09:58.503559	140.112.254.4	163.28.16.80	DNS	168	53	42228	Standard query response 0x1de8 AAAA xmsecu100.net SOA monovm.mars.orderbox-dns.com
4604	2020-02-27 07:09:58.505223	8.8.8.8	163.28.16.80	DNS	89	53	42228	Standard query response 0x1998 A xmsecu100.net A 156.255.121.99
4605	2020-02-27 07:09:58.505816	163.28.16.80	8.8.8.8	ICMP	117	53	42228	Destination unreachable (Port unreachable)
4606	2020-02-27 07:09:58.508626	8.8.8.8	163.28.16.80	DNS	165	53	42228	Standard query response 0x1de8 AAAA xmsecu100.net SOA monovm.mars.orderbox-dns.com
4607	2020-02-27 07:09:58.509182	163.28.16.80	8.8.8.8	ICMP	193	53	42228	Destination unreachable (Port unreachable)
4631	2020-02-27 07:10:22.822996	163.28.16.80	140.112.254.4	DNS	75	33559	53	Standard query 0xc9d4 A 54cq.zhaoyx.xyz
4632	2020-02-27 07:10:22.823042	163.28.16.80	8.8.8.8	DNS	75	33559	53	Standard query 0xc9d4 A 54cq.zhaoyx.xyz
4633	2020-02-27 07:10:22.823069	163.28.16.80	140.112.254.4	DNS	75	33559	53	Standard query 0xce84 AAAA 54cq.zhaoyx.xyz
4634	2020-02-27 07:10:22.823131	163.28.16.80	8.8.8.8	DNS	75	33559	53	Standard query 0xce84 AAAA 54cq.zhaoyx.xyz
4635	2020-02-27 07:10:22.824036	140.112.254.4	163.28.16.80	DNS	139	53	33559	Standard query response 0xce84 AAAA 54cq.zhaoyx.xyz SOA ns1.myhostadmin.net
4636	2020-02-27 07:10:22.824134	140.112.254.4	163.28.16.80	DNS	262	53	33559	Standard query response 0xc9d4 A 54cq.zhaoyx.xyz A 45.113.200.137 NS ns3.myhostadmin.net
4638	2020-02-27 07:10:22.824989	8.8.8.8	163.28.16.80	DNS	139	53	33559	Standard query response 0xce84 AAAA 54cq.zhaoyx.xyz SOA ns1.myhostadmin.net
4639	2020-02-27 07:10:22.825020	8.8.8.8	163.28.16.80	DNS	91	53	33559	Standard query response 0xc9d4 A 54cq.zhaoyx.xyz A 45.113.200.137
4640	2020-02-27 07:10:22.825648	163.28.16.80	8.8.8.8	ICMP	167	53	33559	Destination unreachable (Port unreachable)
4641	2020-02-27 07:10:22.825691	163.28.16.80	8.8.8.8	ICMP	119	53	33559	Destination unreachable (Port unreachable)
4682	2020-02-27 07:11:23.207650	163.28.16.80	140.112.254.4	DNS	73	41536	53	Standard query 0x8d91 A www.duote.com
4683	2020-02-27 07:11:23.207693	163.28.16.80	8.8.8.8	DNS	73	41536	53	Standard query 0x8d91 A www.duote.com
4684	2020-02-27 07:11:23.207718	163.28.16.80	140.112.254.4	DNS	73	41536	53	Standard query 0x9291 AAAA www.duote.com

# DVR影像主機蘊含的風險

---

- DVR廠商，共用韌體情形嚴重。
- 使用者經常為修改預設密碼
- 設備內部主機板及韌體多為中國公司出品。
- 設備韌體未經改寫，當漏洞爆發時，將造成受害範圍擴大。
- 設備暴露於Internet且管理網頁未設定ACL限制存取。

# Windows 系統基礎檢測



# Windows 檢測步驟

---

1. 檢查是否有異常的對外連線行為
  2. 檢查是否有異常的process
  3. 檢查登錄檔是否遭串改
- 推薦工具：Tcpview、Process Explore、WhatChanged

# 對外連線檢查

1. 可透過windows 命令提示字元視窗 輸入指令 `netstat -ano -p tcp` 查看該台設備tcp對外連線情形。

- `-ano` 表示顯示所有建立的連線、Port、PID
- `-p` 指定通訊協定例:TCP、UDP、TCPv6、UDPv6

```
TCP 192.168.1.57:139 0.0.0.0:0 LISTENING 4
TCP 192.168.1.57:13866 40.90.189.152:443 ESTABLISHED 4388
TCP 192.168.1.57:13874 147.92.249.2:443 ESTABLISHED 9896
TCP 192.168.1.57:14411 172.217.160.78:443 ESTABLISHED 6856
TCP 192.168.1.57:14461 172.217.160.78:443 ESTABLISHED 6856
TCP 192.168.1.57:14510 172.217.160.67:443 ESTABLISHED 6856
TCP 192.168.1.57:14630 172.217.160.99:443 ESTABLISHED 6856
TCP 192.168.1.57:14678 31.13.87.1:443 ESTABLISHED 6856
TCP 192.168.1.57:14679 31.13.87.1:443 ESTABLISHED 6856
TCP 192.168.1.57:14860 163.28.16.71:8443 ESTABLISHED 2476
TCP 192.168.1.57:14890 163.28.16.14:80 ESTABLISHED 6856
TCP 192.168.1.57:14900 172.217.160.106:443 ESTABLISHED 6856
TCP 192.168.1.57:14924 108.177.97.189:443 ESTABLISHED 6856
TCP 192.168.1.57:14929 74.125.203.189:443 ESTABLISHED 6856
TCP 192.168.1.57:14996 172.217.24.3:443 ESTABLISHED 6856
TCP 192.168.1.57:14998 104.22.26.227:443 ESTABLISHED 6856
TCP 192.168.1.57:15007 216.58.200.35:443 ESTABLISHED 6856
TCP 192.168.1.57:15014 74.125.132.94:443 ESTABLISHED 6856
TCP 192.168.1.57:15021 163.28.16.14:80 ESTABLISHED 6856
TCP 192.168.1.57:15023 216.58.200.46:443 ESTABLISHED 6856
TCP 192.168.1.57:15027 216.58.200.234:443 ESTABLISHED 6856
TCP 192.168.1.57:15030 172.217.160.110:443 ESTABLISHED 6856
TCP 192.168.1.57:15035 52.109.12.23:443 ESTABLISHED 5364
TCP 192.168.1.57:15036 52.109.8.19:443 ESTABLISHED 5364
```

# Tcpview

The screenshot displays the TCPView application window. The main window title is "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Options", "Process", "View", and "Help". The main area contains a table of network connections. A context menu is open over one of the entries, showing details for "chrome.exe: 6856".

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Recv Pack
[System Process]	0	TCP	desktop-12kac87.ssg5...	15500	172.217.160.99	https	TIME_WAIT			
[System Process]	0	TCP	desktop-12kac87.ssg5...	15531	172.217.160.67	https	TIME_WAIT			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	14678	edge-sta-shv-01-pe...	https	ESTABLISHED	4		128
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	14679	edge-sta-shv-01-pe...	https	ESTABLISHED	4		128
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	14924	tw-in-f189.1e100.net	https	ESTABLISHED	2		344
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	14929	th-in-f189.1e100.net	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15021	w3-gate14.atu.edu.tw	http	ESTABLISHED	3		3,778
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15023	tsa01s08-in-46.1e10...	https	ESTABLISHED	7		3,382
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15047	tsa01s09-in-5.1e100...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15282	tsa01s09-in-f14.1e10...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15290	tsa03s06-in-f10.1e10...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15296	tsa03s01-in-f227.1e1...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15326	w3-gate14.atu.edu.tw	http	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15336	tsa03s01-in-f228.1e1...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15339	tsa03s02-in-f130.1e1...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15341	tsa03s01-in-f1.1e100...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15342	tsa03s02-in-f130.1e1...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15343	tsa01s08-in-f54.1e10...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15344	tsa01s09-in-f2.1e100...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15349	172.67.161.173	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15354	104.31.69.115	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15357	172.67.70.220	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15359	58.70.201.35.bc.goo...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15376	tsa03s06-in-f10.1e10...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15377	tsa01s08-in-f10.1e10...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15380	104.26.4.103	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15383	ip-103-132-192-30.r...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15391	104.27.167.4	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15394	58.70.201.35.bc.goo...	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15397	th-in-f157.1e100.net	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15404	172.67.70.220	https	ESTABLISHED			
chrome.exe	6856	TCP	desktop-12kac87.ssg5...	15411	104.28.13.210	https	ESTABLISHED			

**Properties for chrome.exe: 6856**

- Google Chrome
- Google LLC
- Version: 84.00.4147.0089
- Path: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Buttons: End Process, OK

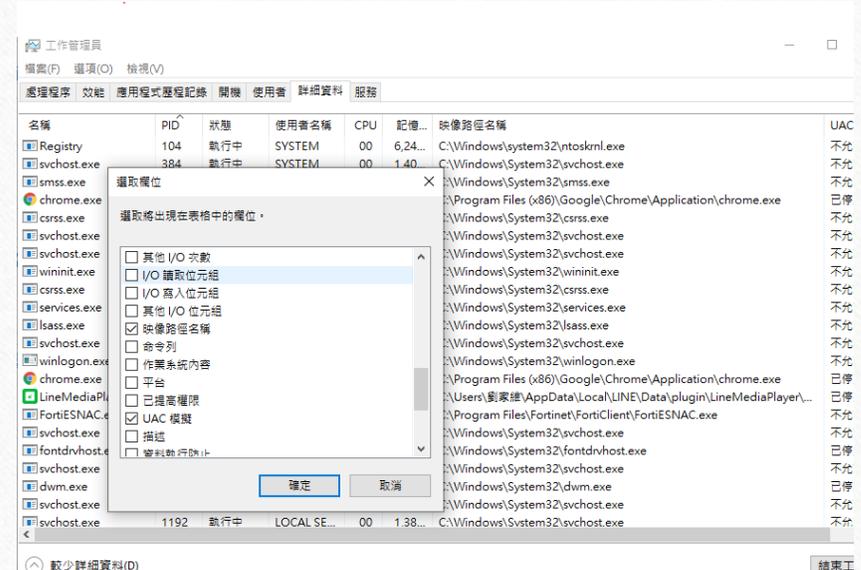
# PROCESS 檢查

- 確認svchost、csrss、wininit 等的映像路徑是否位於 Windows\system32\ 目錄下執行



工作管理員

名稱	PID	狀態	使用者名稱	CPU	記憶體(使...	UAC 模擬
系統攔斷	-	執行中	SYSTEM	00	0 K	
系統開置處理程序	0	執行中	SYSTEM	54	8 K	
System	4	執行中	SYSTEM	00	20 K	
Registry	104	執行中	SYSTEM	00	6,116 K	不允許
svchost.exe	384	執行中	SYSTEM	00	1,376 K	不允許
smss.exe	416	執行中	SYSTEM	00	256 K	不允許
chrome.exe	592	執行中	劉家維	00	25,576 K	已停用
csrss.exe	600	執行中	SYSTEM	00	1,080 K	不允許
svchost.exe	608	執行中	LOCAL SE...	00	1,440 K	不允許
svchost.exe	628	執行中	NETWOR...	00	15,972 K	不允許
wininit.exe	692	執行中	SYSTEM	00	1,004 K	不允許
csrss.exe	700	執行中	SYSTEM	00	1,216 K	不允許
services.exe	764	執行中	SYSTEM	00	4,564 K	不允許
lsass.exe	788	執行中	SYSTEM	00	6,968 K	不允許
svchost.exe	828	執行中	SYSTEM	00	2,624 K	不允許
winlogon.exe	840	執行中	SYSTEM	00	1,632 K	不允許
chrome.exe	848	執行中	劉家維	00	46,508 K	已停用
LineMediaPlayer.exe	856	執行中	劉家維	00	7,120 K	已停用
FortiESNAC.exe	952	執行中	SYSTEM	00	3,284 K	不允許
svchost.exe	972	執行中	SYSTEM	00	660 K	不允許
fontdrvhost.exe	992	執行中	UMFD-0	00	1,260 K	已停用
svchost.exe	1008	執行中	SYSTEM	00	27,516 K	不允許
dwm.exe	1068	執行中	DWM-1	01	71,244 K	已停用



工作管理員

名稱	PID	狀態	使用者名稱	CPU	記憶...	映像路徑名稱	UAC
Registry	104	執行中	SYSTEM	00	6,24...	C:\Windows\system32\ntoskml.exe	不允
svchost.exe	384	執行中	SYSTEM	00	1,40...	C:\Windows\System32\svchost.exe	不允
smss.exe						\\Windows\System32\smss.exe	不允
chrome.exe						\\Program Files (x86)\Google\Chrome\Application\chrome.exe	已停
csrss.exe						\\Windows\System32\csrss.exe	不允
svchost.exe						\\Windows\System32\svchost.exe	不允
wininit.exe						\\Windows\System32\wininit.exe	不允
csrss.exe						\\Windows\System32\csrss.exe	不允
services.exe						\\Windows\System32\services.exe	不允
lsass.exe						\\Windows\System32\lsass.exe	不允
svchost.exe						\\Windows\System32\svchost.exe	不允
winlogon.exe						\\Windows\System32\winlogon.exe	不允
chrome.exe						\\Program Files (x86)\Google\Chrome\Application\chrome.exe	已停
LineMediaPl...						\\Users\劉家維\AppData\Local\LINE\Data\plugin\LineMediaPlayer\...	已停
FortiESNAC.exe						\\Program Files\Fortinet\FortiClient\FortiESNAC.exe	不允
svchost.exe						\\Windows\System32\svchost.exe	不允
fontdrvhost...						\\Windows\System32\fontdrvhost.exe	已停
svchost.exe						\\Windows\System32\svchost.exe	不允
dwm.exe						\\Windows\System32\dwm.exe	已停
svchost.exe						\\Windows\System32\svchost.exe	不允
svchost.exe	1192	執行中	LOCAL SE...	00	1.38...	C:\Windows\System32\svchost.exe	不允

選取位置

選取將出現在表格中的位置。

- 其他 I/O 次數
- I/O 讀取位元組
- I/O 寫入位元組
- 其他 I/O 位元組
- 映像路徑名稱
- 命令列
- 作業系統內卷
- 平台
- 已提高權限
- UAC 模擬
- 描述
- 資料執行禁止

確定 取消

# Process Explorer範例

The screenshot displays two windows from Windows Task Manager. On the left is the 'Properties' window for 'svchost.exe:596 (RPCSS -p)'. On the right is the 'Process Explorer' window showing a list of running processes.

**svchost.exe:596 (RPCSS -p) Properties**

Image File: Windows Services的主機處理程序

Version: 10.0.18362.1  
Build Time: Sat Jan 11 06:26:24 1997

Path: C:\Windows\System32\svchost.exe

Command line: C:\Windows\system32\svchost.exe -k RPCSS -p

Current directory: C:\Windows\System32

Autostart Location: HKLM\System\CurrentControlSet\Services\WpnUserService\_2

Parent: services.exe(776)  
User: NT AUTHORITY\NETWORK SERVICE

Started: 上午 09:16:56 2020/7/22 Image: 64-bit

Comment:

VirusTotal:

Data Execution Prevention (DEP) Status: Enabled (permanent)  
Address Space Load Randomization: High-Entropy, Bottom-Up  
Control Flow Guard: Enabled  
Enterprise Context: N/A

**Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-L2K0C87\劉家維] (Administrator)**

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	0.10	9,180 K	33,464 K	596	Windows Services的主機處理...	Microsoft Corporation
svchost.exe	0.02	1,528 K	6,204 K	1296	Windows Services的主機處理...	Microsoft Corporation
svchost.exe	< 0.01	2,212 K	10,420 K	1280	Windows Services的主機處理...	Microsoft Corporation
svchost.exe	< 0.01	2,300 K	12,468 K	1292	Windows Services的主機處理...	Microsoft Corporation
svchost.exe	< 0.01	6,580 K	16,300 K	1376	Windows Services的主機處理...	Microsoft Corporation
svchost.exe	< 0.01	7,192 K	17,984 K	1428	Windows Services的主機處理...	Microsoft Corporation
svchost.exe	< 0.01	22,136 K	4,492 K	9472	HD Audio Background Process	Realtek Semiconductor
svchost.exe	< 0.01	5,440 K	18,048 K	1312	Windows 工作的主機處理程序	Microsoft Corporation
svchost.exe	< 0.01	2,852 K	12,408 K	1444	Windows Services的主機處理...	Microsoft Corporation
svchost.exe	< 0.01	15,952 K	17,808 K	1504	Windows Services的主機處理...	Microsoft Corporation

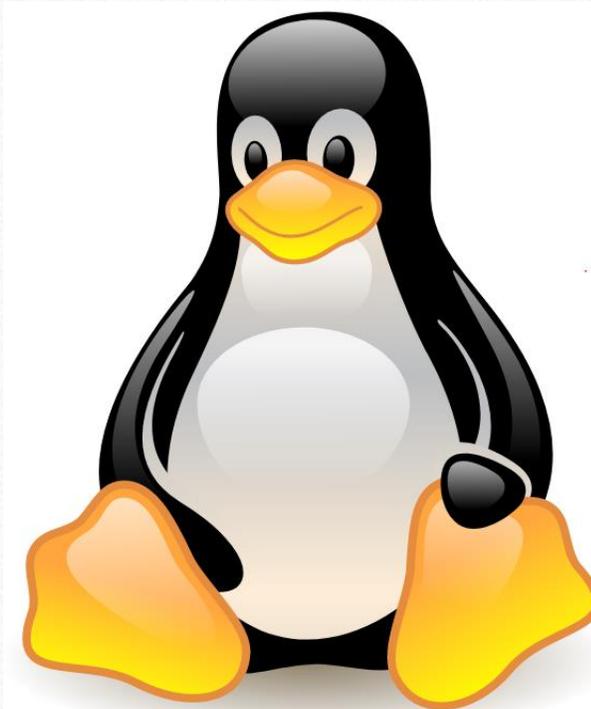
CPU Usage: 35.22% Commit Charge: 14.38% Processes: 202

# 登錄機碼檢查

- 於開始選單點擊右鍵”執行”輸入 regedit 進入登錄碼編輯視窗。



# Linux 系統基礎檢測



# Linux 系統檢測&安全性稽核

---

1. 檢查是否有異常的對外連線行為
2. 檢查是否有異常的process占用系統資源
3. 檢查系統排程是否有遭到串改
4. 安全設定稽核

- 推薦工具：top、lynis

# 對外連線檢查

1. 可透過Terminal 輸入指令 `netstat -an -p -t` 查看該台設備tcp對外連線情形。

```
root@kali:~# netstat -an -t
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.253.134:53718   117.18.237.29:80        ESTABLISHED
tcp        0      0 192.168.253.134:35816   172.217.160.68:443      ESTABLISHED
tcp        0      0 192.168.253.134:42900   172.217.160.78:443      ESTABLISHED
tcp        0      0 192.168.253.134:43508   216.58.200.35:443      ESTABLISHED
tcp        0      0 192.168.253.134:48906   210.61.248.195:80       ESTABLISHED
tcp        0      0 192.168.253.134:36650   216.58.200.46:443      ESTABLISHED
tcp        0      0 192.168.253.134:39564   216.58.200.227:80       ESTABLISHED
tcp        0      0 192.168.253.134:32900   172.217.160.66:443      ESTABLISHED
tcp        0      0 192.168.253.134:58592   172.217.27.130:443      ESTABLISHED
tcp        0      0 192.168.253.134:47580   172.217.24.2:443        ESTABLISHED
tcp        0      0 192.168.253.134:44622   172.217.24.10:443       ESTABLISHED
tcp        0      0 192.168.253.134:41982   99.84.238.26:443       ESTABLISHED
tcp        0      0 192.168.253.134:47124   172.217.160.67:80       ESTABLISHED
tcp        0      0 192.168.253.134:41124   34.211.106.52:443      ESTABLISHED
tcp        0      0 192.168.253.134:43510   216.58.200.35:443      ESTABLISHED
tcp        0      0 192.168.253.134:43330   210.61.248.210:443     ESTABLISHED
tcp        0      0 192.168.253.134:43078   13.35.34.78:443        ESTABLISHED
tcp6       0      0 :::22                  :::*                     LISTEN
```

# PROCESS 檢查

- 輸入指令 `ps aux | less` 查看正在執行之 process，是否有異常的程式於背景執行
- 也可輸入 `top` 及時查看最消耗資源的 process

```
root@kali: ~  
File Edit View Search Terminal Help  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1  0.0  0.3 182332 7640 ?        Ss   Jul07   0:06 /sbin/init  
root         2  0.0  0.0      0     0 ?        S    Jul07   0:00 [kthreadd]  
root         3  0.0  0.0      0     0 ?        I<   Jul07   0:00 [rcu_gp]  
root         4  0.0  0.0      0     0 ?        I<   Jul07   0:00 [rcu_par_gp]  
root         6  0.0  0.0      0     0 ?        I<   Jul07   0:00 [kworker/0:0H-kblockd]  
root         7  0.0  0.0      0     0 ?        I    Jul07   0:02 [kworker/u64:0-events_unbound]  
root         8  0.0  0.0      0     0 ?        I<   Jul07   0:00 [mm_percpu_wq]  
root         9  0.0  0.0      0     0 ?        S    Jul07   0:00 [ksoftirqd/0]  
root        10  0.0  0.0      0     0 ?        I    Jul07   0:04 [rcu_sched]  
root        11  0.0  0.0      0     0 ?        I    Jul07   0:00 [rcu_bh]  
root        12  0.0  0.0      0     0 ?        S    Jul07   0:00 [migration/0]  
root        14  0.0  0.0      0     0 ?        S    Jul07   0:00 [cpuhp/0]  
root        15  0.0  0.0      0     0 ?        S    Jul07   0:00 [cpuhp/1]  
root        16  0.0  0.0      0     0 ?        S    Jul07   0:00 [migration/1]  
root        17  0.0  0.0      0     0 ?        S    Jul07   0:00 [ksoftirqd/1]  
root        19  0.0  0.0      0     0 ?        I<   Jul07   0:00 [kworker/1:0H-kblockd]  
root        20  0.0  0.0      0     0 ?        S    Jul07   0:00 [cpuhp/2]  
root        21  0.0  0.0      0     0 ?        S    Jul07   0:00 [migration/2]  
root        22  0.0  0.0      0     0 ?        S    Jul07   0:00 [ksoftirqd/2]  
root        24  0.0  0.0      0     0 ?        I<   Jul07   0:00 [kworker/2:0H-kblockd]  
root        25  0.0  0.0      0     0 ?        S    Jul07   0:00 [cpuhp/3]  
root        26  0.0  0.0      0     0 ?        S    Jul07   0:00 [migration/3]
```

```
top - 15:29:03 up 3 days, 5:58, 1 user, load average: 0.01, 0.09, 0.06  
Tasks: 225 total, 1 running, 224 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 3.9 us, 0.7 sy, 0.0 ni, 95.2 id, 0.1 wa, 0.0 hi, 0.1 si, 0.0 st  
MiB Mem : 1988.8 total, 120.9 free, 1157.9 used, 710.0 buff/cache  
MiB Swap: 2045.0 total, 2034.7 free, 10.3 used, 639.4 avail Mem  
  
PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM  TIME+  COMMAND  
1280 root       20   0 3803956 336300 84468 S 17.9 16.5 6:52.29 gnome-shell  
1182 root       20   0 292364 68740 43748 S  0.7  3.4 0:12.36 Xorg  
12609 root       20   0 13284  3724  3020 R  0.3  0.2 0:00.02 top  
1 root       20   0 182332  7640  5536 S  0.0  0.4 0:06.91 systemd  
2 root       20   0      0      0      0 S  0.0  0.0 0:00.09 kthreadd  
3 root       0 -20   0      0      0 I  0.0  0.0 0:00.00 rcu_gp  
4 root       0 -20   0      0      0 I  0.0  0.0 0:00.00 rcu_par_gp  
6 root       0 -20   0      0      0 I  0.0  0.0 0:00.00 kworker/0:0H-kblockd  
7 root       20   0      0      0      0 I  0.0  0.0 0:02.56 kworker/u64:0-events_unbound  
8 root       0 -20   0      0      0 I  0.0  0.0 0:00.00 mm_percpu_wq  
9 root       20   0      0      0      0 S  0.0  0.0 0:00.07 ksoftirqd/0  
10 root      20   0      0      0      0 I  0.0  0.0 0:04.84 rcu_sched  
11 root      20   0      0      0      0 I  0.0  0.0 0:00.00 rcu_bh  
12 root      rt    0      0      0      0 S  0.0  0.0 0:00.50 migration/0  
14 root      20   0      0      0      0 S  0.0  0.0 0:00.00 cpuhp/0  
15 root      20   0      0      0      0 S  0.0  0.0 0:00.00 cpuhp/1  
16 root      rt    0      0      0      0 S  0.0  0.0 0:00.38 migration/1
```

# 系統排程檢查

- 檢查路徑/etc 下

cron.d、cron.daily、cron.hourly、cron.weekly

cron.monthly等檔案目錄&

crontab 文件是否包含異常工作排程

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo
rt /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo
rt /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo
rt /etc/cron.monthly )
#
```

# 系統安全稽核工具Lynis

---

- Lynis 是由 CISOfy 所維護的工具程式
- 提供的主要功能如下：
  1. 法遵測試
  2. 自動稽核
  3. 漏洞檢測
  4. 滲透測試
  5. 改善建議



# 支援作業系統

---

- AIX
- FreeBSD
- HP-UX
- Linux
- macOS
- NetBSD
- NixOS
- OpenBSD
- Solaris



# 安裝使用流程

---

- 建議利用git clone 指令自 <https://github.com/CISOfy/lynis> 抓取最新版本
- cd至lynis 檔案目錄
- 利用指令新增執行權限 `chmod +x ./lynis`

# 執行檢測

- Lynis 使用上非常簡單，執行時請給予 root 權限以確保取得最佳的檢測效果。
- 執行指令：`sudo ./lynis audit system`
- 稽核分數：

進度條越滿表示安全性越高

Tests performed 表示總共的測試項目

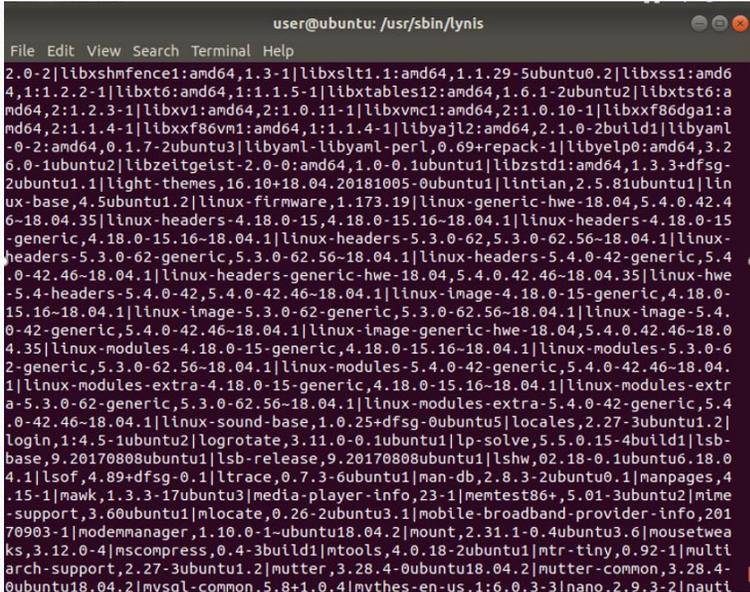
Plugins enabled 外掛程式啟用數量

```
Lynis security scan details:
```

```
Hardening index : 57 [#####          ]  
Tests performed : 249  
Plugins enabled : 1
```

# 檢測報表

- 檢測報告產生於/var/log/lynis.log 路徑下的lynis.log、lynis-report.dat
- 原始報表為純文字檔閱讀不易
- 利用開源工具lynis-report-converter
- 轉換為易於閱讀的格式



```
user@ubuntu: /usr/sbin/lynis
File Edit View Search Terminal Help
2.0-2|libxshmfence1:amd64,1.3-1|libxslt1.1:amd64,1.1.29-5ubuntu0.2|libxss1:amd64,1.1.2-2-1|libxt6:amd64,1:1.1.5-1|libxtables12:amd64,1.6.1-2ubuntu2|libxtst6:amd64,2:1.2.3-1|libxv1:amd64,2:1.0.11-1|libxvmc1:amd64,2:1.0.10-1|libxxf86dga1:amd64,2:1.1.4-1|libxxf86vm1:amd64,1:1.1.4-1|libyajl2:amd64,2.1.0-2build1|libyaml-0-2:amd64,0.1.7-2ubuntu3|libyaml-libyaml-perl,0.69+repack-1|libyelp0:amd64,3.26.0-1ubuntu2|libzeitgeist-2.0-0:amd64,1.0-0.1ubuntu1|libzstd1:amd64,1.3.3+dfsg-2ubuntu1.1|light-themes,16.10+18.04.20181005-0ubuntu1|lintian,2.5.81ubuntu1|linux-base,4.5ubuntu1.2|linux-firmware,1.173.19|linux-generic-hwe-18.04,5.4.0.42.4.6-18.04.35|linux-headers-4.18.0-15,4.18.0-15.16-18.04.1|linux-headers-4.18.0-15-generic,4.18.0-15.16-18.04.1|linux-headers-5.3.0-62,5.3.0-62.56-18.04.1|linux-headers-5.3.0-62-generic,5.3.0-62.56-18.04.1|linux-headers-5.4.0-42-generic,5.4.0-42.46-18.04.1|linux-headers-generic-hwe-18.04,5.4.0.42.46-18.04.35|linux-hwe-5.4-headers-5.4.0-42,5.4.0-42.46-18.04.1|linux-image-4.18.0-15-generic,4.18.0-15.16-18.04.1|linux-image-5.3.0-62-generic,5.3.0-62.56-18.04.1|linux-image-5.4.0-42-generic,5.4.0-42.46-18.04.1|linux-image-generic-hwe-18.04,5.4.0.42.46-18.04.35|linux-modules-4.18.0-15-generic,4.18.0-15.16-18.04.1|linux-modules-5.3.0-62-generic,5.3.0-62.56-18.04.1|linux-modules-5.4.0-42-generic,5.4.0-42.46-18.04.1|linux-modules-extra-4.18.0-15-generic,4.18.0-15.16-18.04.1|linux-modules-extra-5.3.0-62-generic,5.3.0-62.56-18.04.1|linux-modules-extra-5.4.0-42-generic,5.4.0-42.46-18.04.1|linux-modules-extra-5.4.0-42-generic,5.4.0-42.46-18.04.1|linux-sound-base,1.0.25+dfsg-0ubuntu5|locales,2.27-3ubuntu1.2|login,1:4.5-1ubuntu2|logrotate,3.11.0-0.1ubuntu1|lp-solve,5.5.0-15-4build1|lsb-base,9.20170808ubuntu1|lsb-release,9.20170808ubuntu1|lshw,02.18-0.1ubuntu6,18.04.1|lsof,4.89+dfsg-0.1|ltrace,0.7.3-6ubuntu1|man-db,2.8.3-2ubuntu0.1|manpages,4.15-1|mawk,1.3.3-17ubuntu3|media-player-info,23-1|memtest86+,5.01-3ubuntu2|mime-support,3.60ubuntu1|mllocate,0.26-2ubuntu3.1|mobile-broadband-provider-info,20170903-1|modemmanager,1.10.0-1-ubuntu18.04.2|mount,2.31.1-0.4ubuntu3.6|mousetweaks,3.12.0-4|mscompress,0.4-3build1|mtools,4.0.18-2ubuntu1|ntr-tiny,0.92-1|multi-arch-support,2.27-3ubuntu1.2|mutter,3.28.4-0ubuntu18.04.2|mutter-common,3.28.4-0ubuntu18.04.2|mysq-common,5.8+1.0.4|mvthes-en-us,1:6.0.3-3|nano,2.9.3-2|nauti
```

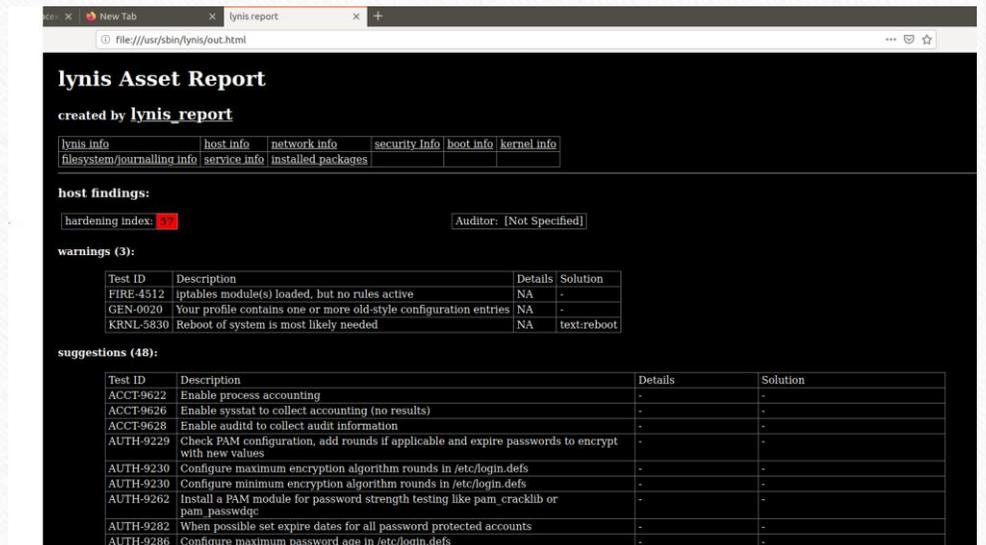
# 報表轉換工具安裝

---

- 利用 `wget` 指令安裝 <https://raw.githubusercontent.com/d4t4king/lynis-report-converter/master/lynis-report-converter.pl>
- 安裝以下函式庫
  1. `apt install htmldoc`
  2. `cpan install HTML::HTMLDoc`
  3. `apt install libxml-writer-perl`
  4. `apt install libarchive-zip-perl`
  5. `cpan install Excel::Writer::XLSX`

# 執行報表產出

- 執行指令
  1. `./lynis-report-converter.pl -o report.html`
  2. `./lynis-report-converter.pl -E -o report.xlsx`



The screenshot shows a web browser window displaying a "lynis Asset Report". The report is titled "lynis Asset Report" and was created by "lynis\_report". It features a navigation menu with links for various report sections: lynis info, host info, network info, security info, boot info, kernel info, filesystem/journaling info, service info, and installed packages. The "host findings" section shows a "hardening index" of 37 and an "Auditor" of [Not Specified]. The "warnings (3)" section contains a table with the following data:

Test ID	Description	Details	Solution
FIRE-4512	iptables module(s) loaded, but no rules active	NA	-
GEN-0020	Your profile contains one or more old-style configuration entries	NA	-
KRNL-5830	Reboot of system is most likely needed	NA	text.reboot

The "suggestions (48)" section contains a table with the following data:

Test ID	Description	Details	Solution
ACCT-9622	Enable process accounting	-	-
ACCT-9626	Enable sysstat to collect accounting (no results)	-	-
ACCT-9628	Enable auditd to collect audit information	-	-
AUTH-9229	Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values	-	-
AUTH-9230	Configure maximum encryption algorithm rounds in /etc/login.defs	-	-
AUTH-9230	Configure minimum encryption algorithm rounds in /etc/login.defs	-	-
AUTH-9262	Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc	-	-
AUTH-9282	When possible set expire dates for all password protected accounts	-	-
AUTH-9286	Configure maximum password age in /etc/login.defs	-	-