IP-SCAN-TCP-80、CODERED、NIMDA

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - 賽門鐵克、Linux.Slapper.Worm
    - 賽門鐵克、NIMDA
    - 賽門鐵克、CODERED
    - 賽門鐵克、W32.Mydoom.B@mm
    - 賽門鐵克、W32.Welchia.C.Worm
    - 賽門鐵克、W32.Gaobot.gen!poly (2004/04/29)
    - 趨勢科技、WORM_AGOBOT.HM (2004/04/29)
    - 賽門鐵克、W32.Spybot.Worm (2004/09/01)

IP-SCAN-UDP-137

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - W32/Opaserv.worm
    - W32/Bugbear@MM
    - Internet Storm Center: Bugbear & Scrup
    - NIMDA

IP-SCAN-TCP-443、IP-SCAN-TCP-1052、IP-SCAN-UDP-1812、IP-SCAN-UDP-1978、IP-SCAN-UDP-2002、IP-SCAN-UDP-4516

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - 賽門鐵克: Linux.Slapper.Worm
    - Red Hat: Linux.Slapper.Worm–What Red Hat customers can do about it
    - F-Secure: Slapper

IP-SCAN-TCP-445、IP-SCAN-TCP-1025、IP-SCAN-TCP-139

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - Symantec: W32.HLLW.Lovgate.G@mm (2003/03/24)
    - Trend: WORM_LOVGATE.F (2003/03/23)

- Trend: WORM_DELODER.A (2003/03/09)
- CERT Advisory CA-2003-08: Increased Activity Targeting Windows Shares (2003/03/11)
- Symantec: W32.HLLW.Deloder (2003/03/08)
- Trend: WORM_LIOTEN.A (2002/12/17)
- Symantec: W32.HLLW.Lioten (2002/12/16)
- Alert:IraqiWorm tcp/445 worm
- CERT: W32/Lioten Malicious Code
- Symantec: W32.HLLW.Gaobot (2002/10/22)
- Trend□TROJ_KILLWIN.C (2002/12 /30)
- 賽門鐵克□W32.Welchia.C.Worm
- 賽門鐵克□W32.Gaobot.gen!poly (2004/04/29)
- 趨勢科技□WORM_AGOBOT.HM (2004/04/29)
- 賽門鐵克□W32.Sasser.B.Worm (2004/05/20)
- 賽門鐵克□W32.Spybot.Worm (2004/09/01)

IP-SCAN-TCP-1433

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - Digispid.B.Worm

IP-SCAN-TCP-25□DOS-TCP-25□EMAIL-VIRUS

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - W32.Sobig.B worm 資訊（2003/05/31）
        - 賽門鐵克 W32.Sobig.C@mm
    - W32.Sobig.B worm 資訊（2003/05）:
        - 賽門鐵克 W32.Sobig.B@mm
    - Brid.A worm 資訊（2002/11）:
        - 賽門鐵克 W32.Brid.A@mm
        - 趨勢科技 PE_BRID.A
    - Myparty worm 資訊:
        - 賽門鐵克 w32.myparty@mm
    - Shoho worm 變種資訊:
        - 趨勢科技□WORM_SHOHO
    - Shoho worm 資訊:
        - 賽門鐵克 w32.shoho@mm
        - 趨勢科技 WORM_SHOHO.A
    - Nimda worm 變種資訊:
        - 賽門鐵克: W32.Nimda.E@mm
        - 趨勢科技: PE_NIMDA.E
    - Nimda worm 資訊:

        - CERT Advisory CA-2001-26 Nimda Worm

IP-SCAN-UDP-1434

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - W32.SQLExp.Worm 資訊
        - 賽門鐵克、W32.SQLExp.Worm
        - 趨勢科技、WORM_SQLP1434.A
        - 賽門鐵克、W32.Spybot.Worm(2004/09/01)

IP-SCAN-TCP-3127、IP-SCAN-TCP-3128、IP-SCAN-TCP-2766、IP-SCAN-TCP-8080、IP-SCAN-TCP-10080

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - W32.HLLW.Deadhat.B 資訊
        - 賽門鐵克、W32.HLLW.Deadhat.B
    - W32.Mydoom.A 資訊
        - 賽門鐵克、W32.Mydoom.A@mm
    - W32.Mydoom.B 資訊
        - 賽門鐵克、W32.Mydoom.B@mm

IP-SCAN-TCP-135

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - W32.Blaster.Worm 資訊
        - 賽門鐵克、W32.Blaster.Worm
    - W32.Welchia.C.Worm 資訊
        - 賽門鐵克、W32.Welchia.C.Worm
    - W32.Gaobot.gen!poly 資訊
        - 賽門鐵克、W32.Gaobot.gen!poly、2004/04/29、
        - 趨勢科技、WORM_AGOBOT.HM (2004/04/29)
    - W32.Spybot.Worm 資訊
        - 賽門鐵克、W32.Spybot.Worm (2004/09/01)

IP-SCAN-ICMP-0

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - W32.Welchia.Worm 資訊
        - 賽門鐵克W32.Welchia.Worm
        - W32.Welchia 蠕蟲
        - 微軟MS03-026 及MS03-007重大安全通告

IP-SCAN-TCP-32773

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - 安全通報 TW-CA-2002-178-[CERT Advisory CA-2002-26:Buffer Overflow in CDE ToolTalk] 資訊
        - TWCERT (台灣電腦網路危機處理/協調中心)
        - CERT Advisory CA-2002-26

IP-SCAN-TCP-5554IP-SCAN-TCP-9996

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - W32.Sasser.B.Worm 資訊
        - 賽門鐵克W32.Sasser.B.Worm

IP-SCAN-TCP-22

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - 賽門鐵克Trojan.Linux.Typot
    - 賽門鐵克Trojan.Linux.Zab

IP-SCAN-TCP-3306

1. 可以進行「網路回報」作業

2. 根據網路系統記錄，您的電腦可能中了下列病毒之一。但是，病毒的種類日新月異，我們不保證一定囊括在內，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - MySQL UDF Worm (Wootbot/Spybot)
    - 賽門鐵克、W32.Spybot.IVQ
    - 趨勢科技、WORM_WOOTBOT.FV

IP-SCAN-TCP-10000、IP-SCAN-UDP-0、SSH-ATTACK

1. 可以進行「網路回報」作業
2. 根據網路系統記錄顯示，您的電腦可能因中毒或其他因素，產生不當的網路使用行為，詳情請直接與我們聯絡(行政區、教學區：分機 31225；宿舍區：分機 31178)，謝謝！

- IP-SCAN-UDP-0、中心依使用者提供的資訊發現，當您使用“影音先鋒”或為了觀看新浪高畫質體育網路直播而下載“撥放軟體”時，可能會符合系統偵測異常網路協定使用規則而被中心封鎖。

MAIL-SPAM、OPEN-PROXY、OPEN-RELAY

1. 可以進行「網路回報」作業
2. 根據網路系統記錄，您的電腦有 Mail Spam、OPEN-PROXY、OPEN-RELAY 問題，您可以參考相關的網路安全資訊，以獲得最新的資訊。排除問題後，請記得回報，謝謝！
    - TANet 濫發廣告信處理原則及設限清單
3. 不當使用 SMTP 伺服器寄發大量信件之參考處理方式。

下列資料摘自：教育部 TANet ANTI-SPAM 網頁

1. 何謂 mail spam ?
   mail spam 為將一份相同內容的電子信件送給很多人，通常信件的內容都是一些商業廣告，這些 spam 在 Internet 是很不受歡迎的，因為收信人需花費撥接時數去收這些垃圾信件，而寄信者為了不被抓到都會使用假的 E-mail address 及利用其它單位的 mail server作為 relay 來送信。
2. 如何避免被當成 relay ?
   如果你的 mail server 是 UNIX 系統的話請 upgrade 你的 sendmail 到 8.9 版。
   如果你的 mail server 是 microsoft exchange 則請廠商更新到最新版並將防止 spam 的設定設上去。
   一般的設定是只允許貴單位內的 IP 將 SMTP server 設到該 mail server、其他單位的 IP 都應拒絕，就如同 news server 一樣只允許單位內的人 post。
3. Proxy Server會寄信? 危險的Open Proxy
   最近數個月，偶有某些連線單位的proxy server、被教育部列為 mail spam的名單中，最近類似的案例有逐漸增加的趨勢，這是因為proxy 未限定服務對象的範圍，攻擊者就會利用這些proxy server當中繼站，來建立smtp或telnet的服務，以寄發大量廣告信或攻擊內部網路。
4. 個人電腦被封鎖? 可能中毒或被植入後門程式
   許多使用者自己並未發廣告信(SPAM)、也沒有scan他人主機、更沒有發動阻斷式攻擊，可是卻接獲檢舉或抱怨。這種情形發生時，有可能是被植入後門程式，建議使用者以防毒軟體做全機掃瞄，但是不一定候每次都可以掃瞄出後門程式或木馬程式，有時候依防毒軟體及病毒種類不同，雖然中毒卻卻無法正確掃瞄出。

PCRI

疑似侵權檢舉

1. 無法進行「網路回報」作業
2. 教學、行政區：疑似侵權需以書面回報，請至網路系統組/表單下載篇網頁下載 “疑似侵權處理回報暨IP復用申請單”填妥後送交計通中心二樓服務台(聯絡電話：分機 31225)，謝謝！
3. 宿舍區：疑似侵權需停用30天後以書面回報，請至網路系統組/表單下載篇網頁下載 “學生宿舍網路復用申請單”填妥後送交計通中心二樓服務台(聯絡電話：分機 31178)，謝謝！
4. 清華大學智慧財產權疑似侵權處理程序

DNS-ANOMALY

1. 可以進行「網路回報」作業
2. 根據網路系統記錄顯示，您的電腦可能因中毒或其他因素，對校園 Domain Name Server 產生不當的網路使用行為(例如：持續對 server 發出巨量重複無效的domain name查詢或Open DNS resolver)，詳情請直接與我們聯絡(分機31225)，謝謝！
3. 中心目前觀察到如下狀況會導致您的電腦符合上述原因而被中心封鎖
   - 電腦遭植入木馬，該木馬欲尋找某台Domain Name已無效的電腦，此時會持續重複無效的查詢。
   - 您的電腦有安裝“BitComet”此套 P2P 軟體，此軟體會持續重複查詢無效的Tracker Server

TACERT

1. 無法進行「網路回報」作業
2. 教育機構資安通報平台通知，您的電腦可能因中毒或其他因素產生資安事件，需提供事件相關資訊至abuse@cc.nthu.edu.tw信箱，以供計通中心回報至教育機構資安通報平台，並進行後續解除網路阻斷流程。
3. 如您為住宿生，請先至申請宿網時所填寫之電子郵件信箱收取事件通知信。
4. 如有相關問題，請直接與我們聯絡(分機：31225 李先生)，謝謝

OPEN-DNS-RESOLVER

1. 可以進行「網路回報」作業
2. 根據網路系統記錄顯示，您的電腦**具有open DNS resolver問題**，如須瞭解發生原因及影響，請參閱open DNS resolver，謝謝！
3. **如你的電腦作業系統為Windows 7 / 8可能解決方法請參閱本網站常見問題之DNS問題**

OPEN-NTP-SERVER

1. 可以進行「網路回報」作業
2. 根據網路系統記錄顯示，您的資訊設備**具有open NTP server問題**，如須瞭解發生原因及影響，請參閱open NTP server，謝謝！

OPEN-SNMP-SERVER

1. 可以進行「網路回報」作業
2. 根據網路系統記錄顯示，您的資訊設備**具有open SNMP server問題**，如須瞭解發生原因及影響，請參閱open SNMP server，謝謝！

NTP-ATTACK

1. 可以進行「網路回報」作業
2. 根據網路系統記錄顯示，您的電腦具有 **NTP ATTACK** 問題，如須瞭解原因與影響及如何解決此問題，請參閱NTP Attack，謝謝！

Audit

您的設備於本校內外部稽核檢測發現存在弱點，因屬於特殊情形，無法透過網路回報解除IP阻斷，詳情請直接與我們聯絡(分機 31225)，謝謝！

OTHERS

您的電腦可能因中毒、校外單位檢舉或其他因素，產生不當的網路使用行為。因屬於特殊情形，無法透過網路回報解除IP阻斷，詳情請直接與我們聯絡(教學區：分機 31225；宿舍區：分機 31178)，謝謝！

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/security:netguard:type

Last update: **2023/08/15 15:30**