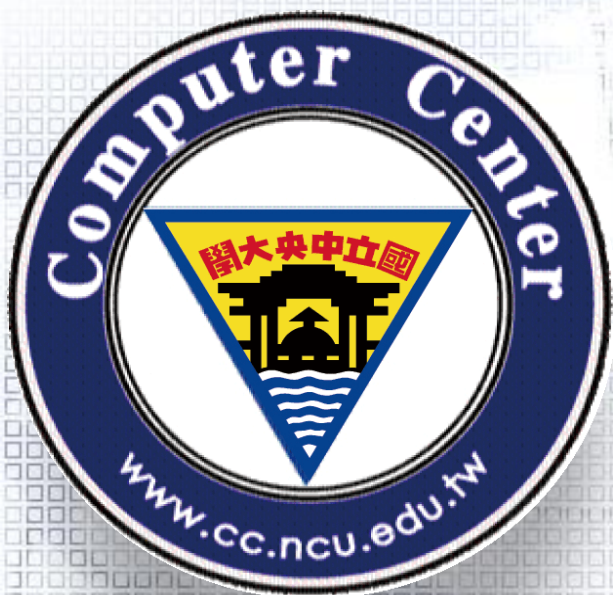


桃園區網中心 第59次區網會議

國立中央大學電算中心
106年05月04日



印表機勒索訊息說明及建議

國立中央大學電算中心
邱惠隆

106年05月04日



印表機勒索訊息事件說明

- 事件說明：106年2月有一證券商發現印表機自動列印出勒索訊息，陸續有學校也發生同樣的事件。
- 2/17 TACER開始印表機遭列印勒索訊息損害調查。
- 查詢過後發現只要是印表機預設在9100 port並使用公開IP的話，勒索訊息就會經由9100port 且並不需要裝驅動 telnet [ip] 9100或nc [ip] 9100就可以印出訊息來。



My name is Emerson Rodrigues

Your network will be destroyed starting 03/01/2017 if you
don't pay protection fee - 3 Bitcoins @
[REDACTED]

If you don't pay by 02/20/2017, my virus will start to
destroy your files and the price to stop will increase to 5
BTC and will go up 10 BTC for every day of attack.

This is not a joke.

If you do not pay, the virus will destroy all your files. Its
propagating in your network right now while you re
Reading this print job.

Prevent it all with just 3 BTC @
[REDACTED]

Contact El [REDACTED] @[Openmailbox.org](mailto:[REDACTED]@Openmailbox.org) for instructions.

Bitcoin is anonymous, nobody will ever know you
cooperated.



印表機勒索訊息事件說明(續)

- ❑ 包含 Canon、Epson、HP、Brother 等品牌的印表機，他藉由網路列印協定 IPP、線上印表機公用 Line Printer Daemon、以及開放的 **9100 連接埠**，進行網路印表機的入侵，約有 **15 萬台印表機**被成功駭入。
- ❑ 被入侵的上萬台印表機，則是自動列印了以 ASCII 碼製作的機器人，上頭還表明用戶的印表機已經成為殭屍網路的一部分。
 - 暱稱Stackoverflowin的駭客在自己的 Twitter 上表示這只是開個玩笑，並藉此提醒大家留意**網路印表機的防護能力**。

資料來源參考<https://twcertcc.org.tw/twcert/news/10>



防護建議措施修正

□ 防護建議措施修正。

- 將辦公室所有電腦檔案作“**離線**”備份(例如複製到行動硬碟上，且複製完後不要接在電腦上)，避免它轉而攻擊其他有資料的電腦。
- 將該印表機的IP改掉，並且將 gateway 亂設為某個無法連線的IP，mask 改為255.255.255.255，讓印表機無法對外界連線作出回應。
- 請確認每一台電腦都有**定期更新病毒碼**，並**全面掃毒**。

資料來源參考<https://twcertcc.org.tw/twcert/news/10>



防護建議措施修正(續)

- 系統上非必要的服務程式亦建議移除或關閉。
- 建議裝置設備不要使用公開的網際網路位置，如無法避免使用公開的網際網路位置，建議裝置設備前端需有防火牆防護，並採用白名單方式進行存取過濾。
- 檢驗防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠

資料來源參考<https://twcertcc.org.tw/twcert/news/10>



工商廣告宣導

□ 網管通訊錄更新

- 若單位名稱、網管人員及聯絡方式有變動請與區網聯絡更新。

□ 教育訓練/講座/會議

- 原則上都安排在星期四

區網連絡人：

邱惠隆

center38@cc.ncu.edu.tw

03-4227151#57516

□ 校園資安推廣

- 推廣對象：教職員及學生均可
- 徵求連線單位講師支援(具有資安相關證照及相關研究)



Computer Center, National Central University.



感謝你的耐心聆聽!

Q&A