NPASCAN v1.7
惡意程式偵查工具使用說明

警政署
npascan@npa.gov.tw

NPASCAN特色

- 由警政署自行研發，採用行為比對，無須病毒特徵碼之惡意程式偵查工具。
- 本工具並非防毒軟體，防毒軟體系於檔案尚未執行時，發現病毒特徵而加以阻攔，NPASCAN運作於可能已感染惡意程式之電腦，掃描系統所有啟動項目，辨識檔案是否為可疑程式，並提供移除之功能。
- 因採行為比對，可偵測出防毒軟體偵測不到，但行為異常之可疑程式，為一種通用型可疑程式偵查工具，亦可作為現場惡意程式鑑識工具。
- 目前版本為1.7版，請持續注意警政署全球資訊網最新消息，查看是否有更新版本。

NPASCAN問與答(1/2)

- Q：**NPASCAN需要一直常駐於系統嗎？**
  - A：NPASCAN不需常駐於系統，偶爾執行掃描，即可檢測電腦目前是否有可疑檔案在執行，這一點與防毒軟體有很大差異。
- Q：**NPASCAN找出來的檔案一定有問題嗎？**
  - A：本程式採行為分析，不排除有誤判的情況，例如:你發現高速公路上有車搖搖晃晃，會認為駕駛喝醉了，但也有可能他開車本來就是搖搖晃晃的，這是行為分析最大的問題，我們也一直蒐集各位的使用經驗持續在調校。
  - A：本程式可以確保不會誤刪系統檔案。
- Q：**NPASCAN使用時機？**
  - A：當你覺得電腦怪怪、或任何時候皆可拿到該台電腦上檢測。
- Q：**NPASCAN掃出的檔案我都要按是刪除嗎？**
  - A：基本上都可以刪除，除非你確定檔案是系統檔或絕對沒問題之檔案，這個部份就有可能是問題二所描述的誤判情況，此時請把log與檔案壓縮後寄至npascan@npa.gov.tw，以利本署修正與判讀。

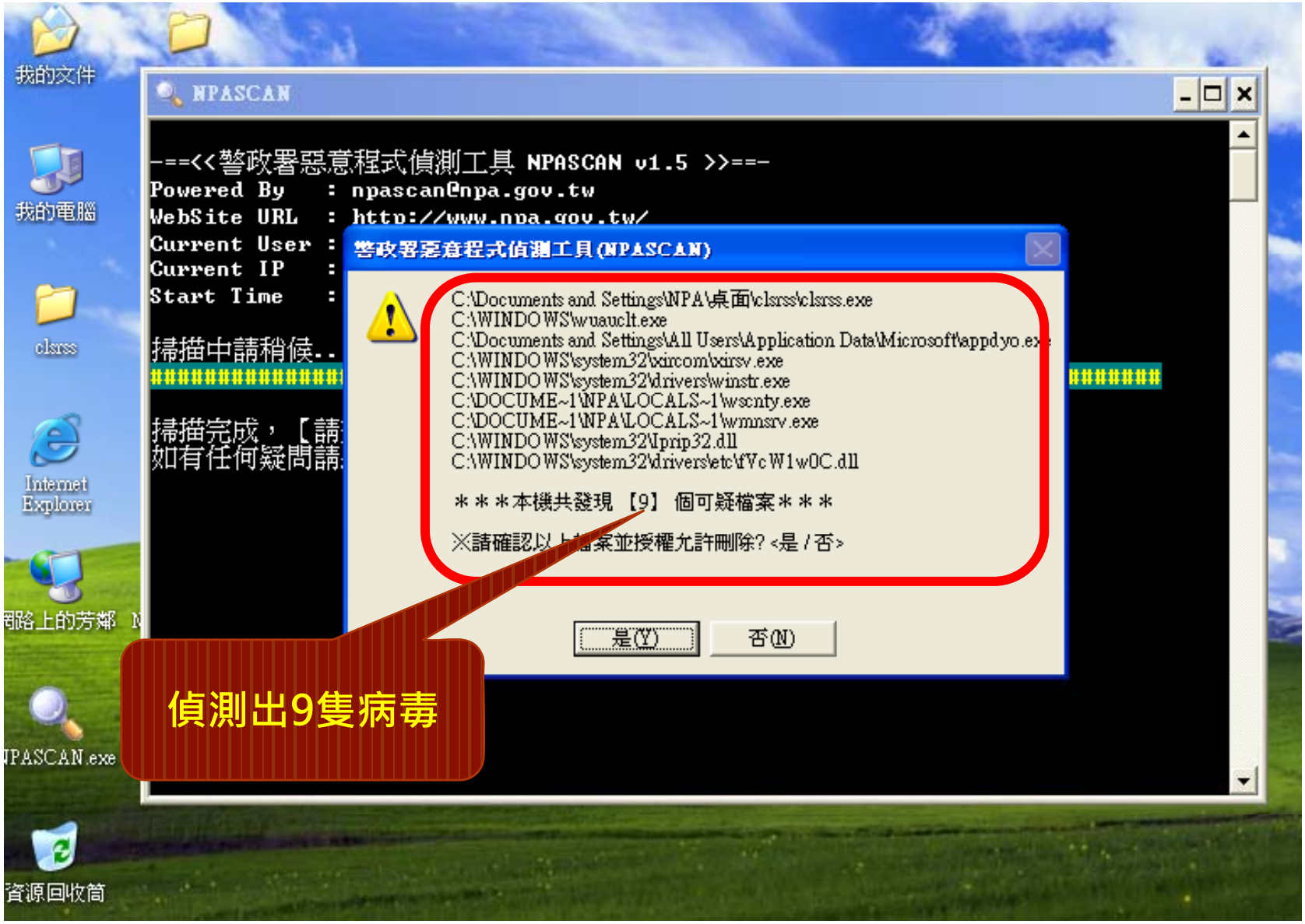
NPASCAN問與答(2/2)

- Q：**NPASCAN可以運作的作業系統環境？**
  - A：Win2000之後所有Microsoft作業系統。
- Q：**NPASCAN可以運作的作業系統語系？**
  - A：以繁體中文為主，非中文之作業系統部分採英文顯示。
- Q：**NPASCAN掃很久出現超時異常?**
  - A：請重新開機或切斷網路連線後再試一次。
- Q：**NPASCAN出現非預期的系統檔案分析失敗?**
  - A：表示NPASCAN部分功能無法在您電腦正確執行，為避免最終判斷結果，本程式停止對該台電腦檢測動作。
- Q：**NPASCAN會蒐集使用者資訊嗎？**
  - 不會。

NPASCAN使用方式

- 使用NPASCAN非常簡單，只需執行NPASCAN.exe後等待10~20秒，掃描結果即以視窗彈出、亦會保留log。
- 如發現可疑檔案，按『是』後，下次重開機後即可清除。
- NPASCAN掃描後會於該目錄下產生NPASCAN_電腦名稱.txt之log檔案，可以協助使用者確認，如有疑問亦可將Log檔與檔案壓縮加密後寄至 npascan@npa.gov.tw 提供本署分析。
- 每次刪除檔案後會保留一份原始檔案於Sbak目錄，如需還原請至該目錄執行Recovery.bat檔案進行還原。

NPASCAN檢測實況



1.7版的改變

- 修正對某些第三方軟體的誤判。
- 提升對某些類型惡意程式的檢查能力。
- 提升對某些病毒檔案的刪除能力。
- 修正對非中文作業系統之字體顯示。

- 有關NPASCAN程式民眾可於警政署全球資訊網下載。
- 如有任何問題可e-mail至npascan@npa.gov.tw