WORM_SHOHO.A

別名:

WELYAH.A, WELYAH, W32/Shoho@MM, W32/Welyah.A

風險指數: 低風險

病毒種類: Worm

具破壞性: 會

說明:

This destructive, memory-resident worm propagates via email using SMTP commands and arrives in the following format:

```
Subject:Welcome to Yahoo! Mail
Message Body: Welcome to Yahoo! Mail
Attachment: README.TXT_____________.PIF
```

The attachment name contains 125 spaces between the .TXT and .PIF extensions, which helps to disguise its .PIF extension from its email recipients. This worm uses a known vulnerability in Internet Explorer-based email clients to execute the file attachment automatically. This vulnerability is also known as Automatic Execution of Embedded MIME type.

This worm has a destructive payload of randomly deleting files in the current directory.

解決方案:

方法 一.

1. 下載清除程式 FIX_SHOHO1.01.EXE, 將 FIX_SHOHO1.01.EXE 存至磁片中或儲存至一暫存目錄中
2. 關閉防毒軟體及所有正在執行的程式
3. 點選 開始 \ 執行
4. 輸入 FIX_SHOHO1.01.EXE
5. 開啟防毒軟體掃瞄所有檔案 將所有偵測出病毒檔案刪除

方法 二.

手動清除步驟

1. 請選擇「開始｜執行」，然後輸入 REGEDIT，並按下確定
2. 依序尋找下列機碼
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
   利用滑鼠右鍵點選右邊視窗中的 WINL0G0N.EXE 並選擇刪除
   HKEY_CURRENT_USER\Software\Microsoft\Windows\

CurrentVersion\Run

利用滑鼠右鍵點選右邊視窗中的 WINL0G0N.EXE 並選擇刪除

HKEY_USER\Default\Software\Microsoft\Windows\

CurrentVersion\Run

利用滑鼠右鍵點選右邊視窗中的 WINL0G0N.EXE 並選擇刪除

3. 開啟防毒軟體掃瞄所有檔案 將所有偵測出病毒檔案刪除

註：此病毒會隨機刪除系統檔案.若發生此問題,請由平時備份檔案還原

趨勢科技是全球網路防毒及內容安全防護的領導者，提供企業集中控管伺服器防毒軟體以及家庭用個人電腦安全防護軟體。