卡巴斯基防毒軟體操作說明

日　　期：96年12月13日
地　　點：中央警察大學

奕瑞科技 陳世煌 Allen@kaspersky.com.tw

Kaspersky for Windows Workstations

綱　　要

- 卡巴斯基企業版Workstation簡介
- 防護功能、訊息與通知
- 事件與報告
- 病毒特徵碼更新與手動掃瞄
- 駭客防護簡介
- 惡意程式簡介
- 卡巴斯基技術支援

Kaspersky for Windows Workstations

操作介面－防　護

Kaspersky for Windows Workstations

操作介面－防　護

Kaspersky for Windows Workstations

操作介面－掃　瞄

Kaspersky for Windows Workstations

操作介面－服　務

Kaspersky for Windows Workstations

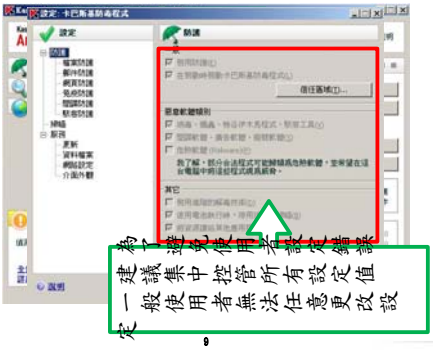
操作介面－資 訊

Kaspersky for Windows Workstations

操作介面－線上支援

Kaspersky for Windows Workstations

操作介面－設 定



Kaspersky for Windows Workstations

防 護 功 能

- 檔案防護
- 郵件防護
- 網頁防護
- 免疫防護
- 間諜防護
- 駭客防護
- 垃圾郵件防護

◆支援微軟Outlook及Outlook Express
◆可自訂黑白名單及規則，過濾垃圾郵件。
◆利用訓練模式自動學習辨別垃圾郵件。

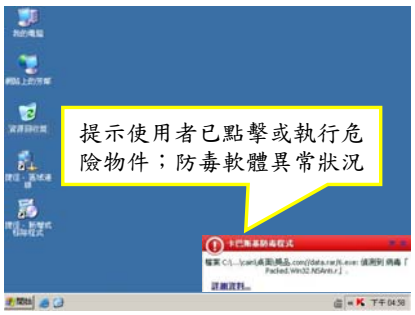
Kaspersky for Windows Workstations

訊息與通知－圖 示

- 卡巴斯基各項元件與運作正常
- 正在更新病毒特徵碼
- 正在執行病毒掃描工作
- 正在掃瞄網頁指令碼
- 正在掃瞄郵件
- 即時防護已停用，仍可更新及掃瞄(使用者自行關閉)
- 部份或全部元件毀損，特徵碼毀損或失效(病毒或程式衝突)

Kaspersky for Windows Workstations

訊息與通知－即時訊息



Kaspersky for Windows Workstations

訊息與通知－即時訊息

超過2天以上未執行更新

超過2天以上未執行更新

更新過程中發生錯誤

更新過程中發生錯誤

Kaspersky for Windows Workstations

訊息與通知－即時訊息

程式衝突、元件毀損、病毒碼毀損

網路中有惡意程式或病毒自行散佈

偵測到含有病毒檔的網頁（連結）

偵測到病毒或遭病毒染感的檔案

系統日期錯誤，將無法更新病毒碼

Kaspersky for Windows Workstations

訊息與通知－即時訊息

偵測到病毒並自動刪除

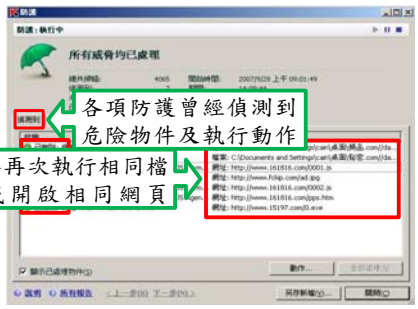
即時防護停止，通常是使用者關閉

自動阻擋惡意網頁或下載病毒檔

偵測到病毒，必須重新開機才能刪除

Kaspersky for Windows Workstations

事 件 與 報 告



各項防護曾經偵測到危險物件及執行動作

不要再次執行相同檔案或開啟相同網頁

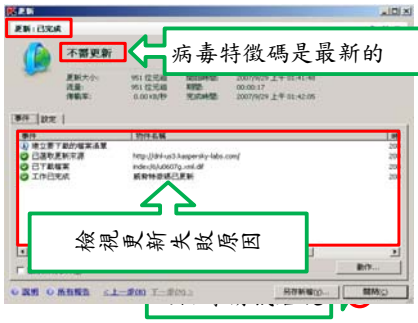
Kaspersky for Windows Workstations

病 毒 特 徵 碼

- 病毒特徵碼為卡巴斯基防毒軟體，判定某物件（檔案）是否為病毒的依據
- 病毒特徵碼是否定時完成更新，對防毒軟體的防護能力有很非常大的影響
- 建議由管理者統一排程執行病毒特徵碼更新工作
- 使用者也可隨時手動更新
- 執行更新時，網路必須連線

Kaspersky for Windows Workstations

更新與檢視事件



病毒特徵碼是最新的

檢視更新失敗原因

Kaspersky for Windows Workstations

掃描與檢視事件

Kaspersky for Windows Workstations

駭客防護（防火牆）

- 駭客防護保護您的電腦和應用程式對抗來自網路的威脅，並且遮蔽電腦以防範網路攻擊。
- 駭客防護提供兩種規則：
  - ➢**封包篩選規則**：用來限制一般的網路活動，不論是哪一種應用程式。
    舉例來說，當您封鎖21埠進入的流量，則任何應用程式都無法從外部存取這個埠。
  - ➢**應用程式規則**：用來限制特定應用程式的網路活動。
    舉例來說，假如封鎖所有應用程式連線80埠，您可以新增一條規則只允許**Firefox** 連結。

應用程式和封包篩選規則有兩種動作類型：**允許**和**封鎖**。

Kaspersky for Windows Workstations

駭客防護（防火牆）

Kaspersky for Windows Workstations

駭客防護（防火牆）

防火牆防護層級

- **全部允許**:允許所有網路活動
- **低安全性**: 允許所有應用程式的網路活動，除了應用程式規則有明確禁止者 (預設值)
- **訓練模式**:會在任何應用程式嘗試連線到本地網路或網際網路時出現提示。
- **高安全性**:只會允許定義在規則內的連線。
- **全部封鎖**:防止電腦存取網際網路或本機網路。所有的連線嘗試均會被封鎖。

Kaspersky for Windows Workstations

駭客防護（防火牆）

網路狀態分為三種：信任網路、本機網路或網際網路

- **信任網路**—應用程式不受管控，只會新增一條「全部允許」的規則。在預設下，隱形模式是停用的。
- **本機網路**—允許檔案和印表機共享，允許交換**ICMP**封包，並會套用封包篩選和應用程式規則。預設下，隱形模式是停用的。
- **網際網路**—封鎖檔案和印表機共享，封鎖交換**ICMP**封包，但會套用封包篩選和應用程式規則。預設下，隱形模式是啟用的。

隱形模式是**駭客防護**特別的功能之一，它能讓電腦不被外部偵測到。

Kaspersky for Windows Workstations

惡意程式的定義

- 惡意程式(**Malicious programs**，簡稱**Malware**)是指在未明確提示用戶或未經用戶許可的情況下，在用戶電腦上進行安裝、侵害或竊取用戶系統資訊的程式。
- 惡意程式包含病毒、蠕蟲及木馬。廣義來說，凡具有下列特徵之一的程式即為惡意。
  1. 強制安裝
  2. 難以移除
  3. 首頁綁架（**hijacking** ）
  4. 廣告彈出
  5. 惡意收集用戶資訊
  6. 惡意移除用戶端程式

Kaspersky for Windows Workstations

惡意程式的危害

- 造成網路服務超載
- 資料遺失或遭竊取
- 程式損毀
- 消耗電腦資源－處理器、記憶體、硬碟
- 消耗網路資源－區域網路
- 分散式阻斷服務（**DDoS**） 攻擊
- 影響電腦操作
- 影響應用程式與檔案關連性
- 無法開機
- 降低電腦安全性

Kaspersky for Windows Workstations

網路威脅的種類

- 需要使用目標電腦程式元件的威脅
  - ➢**電腦病毒 Computer Viruses**
  - ➢**蠕蟲 Worms**
  - ➢**木馬/後門軟體 Trojan/Backdoor Software**
  - ➢**危險程式 Riskware**
- 不需嵌入程式元件的威脅
  - ➢**垃圾郵件 SPAM**
  - ➢**網路釣魚 Phishing**
  - ➢**不當廣告 External Advertisement**
  - ➢**駭客攻擊 Hacking**

Kaspersky for Windows Workstations

惡意程式的進化

- **使用加殼程式**
  - ➢ 隱藏程式碼不被防毒軟體所掃瞄。可保護程式碼免於遭到反組譯，讓惡意程式更難以分析。
- **關閉防毒軟體**
  - ➢ 惡意軟體停用電腦的安全解決方案，或是讓防護軟體無法偵測
- **隱藏程序技術**
  - ➢ 隱藏惡意程式的操作，讓防毒軟體及所有系統處理程序皆無法察覺。

Kaspersky for Windows Workstations

Q & A

Q. 電腦中毒後該如何處理？

a. 立即解毒

b. 工作優先

c. 評估風險後再處理

Kaspersky for Windows Workstations

Q & A

風險（Risk）=威脅X弱點

若是控制其中一個，風險就不會成立！

1. 評估威脅是否會造成損失？
2. 評估威脅會造成多少損失，該做哪些防護？

對企業而言，竊取線上遊戲帳號密碼的木馬，並不是威脅
對個人而言，針對**SQL Server**的攻擊，同樣不是威脅

Kaspersky for Windows Workstations

防範惡意程式

- ◆安裝正版作業系統及應用程式，並定期更新（修補）
- ◆安裝卡巴斯基防毒軟體，並定期更新病毒特徵碼
- ◆避免使用不明儲存媒體，在使用前先掃毒
- ◆避免安裝/執行不明的應用程式或檔案
- ◆避免瀏覽不明網頁，或下載不明物件
- ◆安裝（啟用）防火牆，停用不使用的系統服務
- ◆減少使用**P2P**共享程式
- ◆定期清理系統暫存檔與執行掃毒
- ◆養成良好電腦操作習慣，例如定期變更系統登入密碼，設定複雜密碼

Kaspersky for Windows Workstations

如何完整清除病毒

- 更新防毒軟體至最新的**病毒特徵碼**（線上或手動）
- 拔除網路線
- 清除瀏覽器和系統**暫存檔**
- 關閉**Windows系統還原**
- 重新開機進入**安全模式**
- 透過**防毒軟體掃描**與清除惡意程式
- 防毒軟體沒有作用時，透過救援光碟開機進行掃毒
- 利用工具**收集系統資訊**
- 刪除登錄檔中的相關鍵值，檢查檔案有無遺失或毀損
- 傳送可疑檔案，請防毒軟體廠商分析

Kaspersky for Windows Workstations

病毒無法清除

- 無法自行處理，應請求防毒軟體廠商協助
- 備份重要資料
- 在惡意程式未完全清除前，盡量避免使用網路社交工具與線上金融交易
- 確認惡意程式完全清除後，建議立即更改密碼
- 針對此次威脅入侵事件，執行相對應安全性政策

Kaspersky for Windows Workstations

卡巴斯基技術支援

技術支援專線：(02)2791-5365

技

F/ 常見問題解答 -AQ.htm

資

Kaspersky for Windows Workstations

簡報完畢
敬請指教