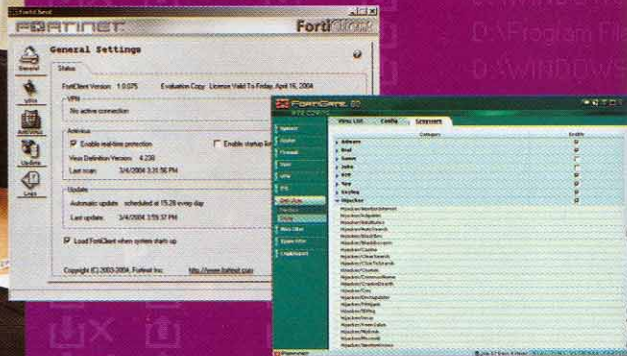


T: Fortinet香港與東南亞區董事總經理譚敦敏 A: TNA

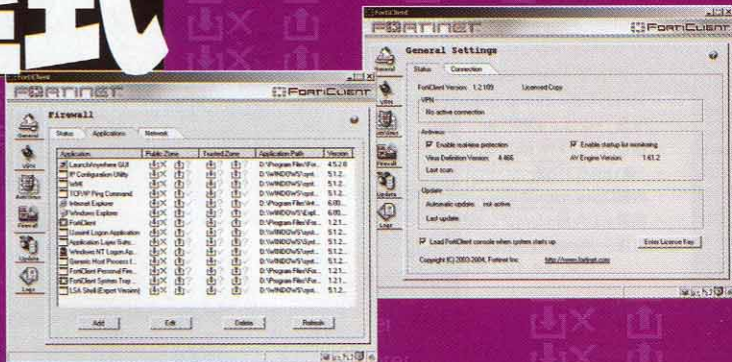


干擾程式 (Grayware) 是指多類型的威脅，例如運作模式追蹤、侵犯私隱和盜取資料，此類程式會在用戶毫不知情、毋須執行任何程式的情況下下載至電腦，隱蔽地進行破壞，並在未獲用戶的准許下，追蹤或向外界匯報電腦內的資料。

## 電腦干擾程式

### 解碼多面睇

干擾程式可以從多個途徑進入電腦，例如下載共享軟件和免費軟件、使用其他形式檔案共享服務、開啟受感染電郵、點擊彈出式廣告、瀏覽假冒網站，或者安裝特洛伊應用程式。當電腦感染干擾程式後，其運作會變得緩慢、彈出式廣告增多，或瀏覽網站時會被重新指引至其他網站。



### 干擾程式層出不窮

此外，黑客會利用瀏覽器載入和執行程式，以開啟接達點、收集資料、追蹤按鍵記錄、修改系統設定或進行其他形式破壞。干擾程式可分為廣告程式、撥接器、遊戲、開玩笑程式 (Joke)、對等網絡 (Peer-to-Peer)、間諜程式、按鍵記錄程式、劫持程式 (Hijacker)、插入程式 (Plug-ins)、網絡管理、遙距管理工具、BHO (Browser Helper Objects)、工具列和下載程式等。

電腦感染干擾程式後，操作速度會被拖慢，最常見的徵狀包括數據機顯示列在未有上網活動下不停閃動；電腦未有連接至互聯網時自動彈出訊息；網絡瀏覽器的首頁設定、「我的最愛」清單、搜尋工具列遭更改；電話費因未曾使用過的通話記錄而上升；抗病毒程式或防間諜程式的軟件停止運作。

### 防範干擾程式的威脅

為免電腦受到威脅，用戶必須從多方面著手：

#### 1. 用戶教育

公司向員工講解干擾程式的特性和帶來的危險，並推行措施防止員工下載，和安裝公司不許可的應用程式。用戶應先仔細閱讀供應商網站內的資料，並詳閱「最終用戶使用權證同意書」的各項細則。用戶應在電郵系統內，解除自動下載HTML電郵內的互聯網圖片或其他資料、關掉自動檢視功能，並經常更新操作系統和應用程式的保安修補程式。

#### 2. 主機型防間諜程式

公司要為所有電腦安裝防間諜程式和客戶端的軟件應用保護程式，在企業的私人網絡接駁至互聯網的周邊範圍安裝保安裝置，但這種中央解決方案有其弱點，就是當用戶離開辦公室後，電腦就只能依靠安裝在電腦的保安程式提供保護。

#### 3. 以策萬全的解決方案

要有效對付干擾程式，用戶必須同時應用網絡型和主機型的保安系統。網絡型的保護需要包括抗病毒的防火牆，阻截病毒、蠕蟲、特洛伊程式、入侵、濫發電郵、不適當的網絡內容和干擾程式。主機型的保護則包括虛擬專用網用戶的保安軟件、抗病毒保護系統、個人防火牆保護，以及干擾程式偵測效能。

保安平台結合各種主要保安措施在單一網閘，各種保安措施分享不同的保安威脅資訊，並相互配合提供一種獨特的保安效能。此做法亦可識別和阻止新出現和混合型的威脅，超越傳統保安裝置的防線，例如標準型防火牆、防病毒或入侵偵測系統等。

最理想的實時保護是包括以記號為基礎的威脅識別和保護防護，兼備啟發式和變種威脅偵測技術，可以在數據保護服務供應商加添新辨認記號前，探測新混合型威脅的存在。

現時各種保安威脅和危險日益增多，FortiGate保安平台提供一個動態型防止威脅系統 (Dynamic Prevention System)，提供偵測、清除和阻截所有已知或新增的威脅和變種危機。當新種威脅出現，這個系統便會自動更新辨認記號，與傳統的保安解決方案需要人手更新，完全截然不同，有助大幅減低受新種保安威脅侵擾的機會。

LISTS  
DIY Product  
Price Hunter  
Blogs

Pro User