

趨勢科技2008年資安威脅摘要暨 2009年資安趨勢預測

作為對抗資安威脅的第一道防線，趨勢科技TrendLabs持續密切觀察惡意程式技術領域的最新發展。TrendLabs 2008年資安威脅年終報告與2009年趨勢預測將摘述最值得注意的惡意程式相關技術，並針對未來一年內企業及個人可能遭遇的網路惡意行為進行深入的剖析。

2008年與亞洲有關的資安威脅

對網路罪犯而言，2008年是生存、探索及創新的一年。過去幾年來網路地下經濟體持續蓬勃發展，惡意程式作者的動機也逐漸轉向以謀利為目的。熟悉電腦技術的使用者對於 Web 資安威脅的認知程度逐漸提高。相對於此，網路罪犯也紛紛使用新的媒介或針對舊媒介進行改良，用以謀取利益。

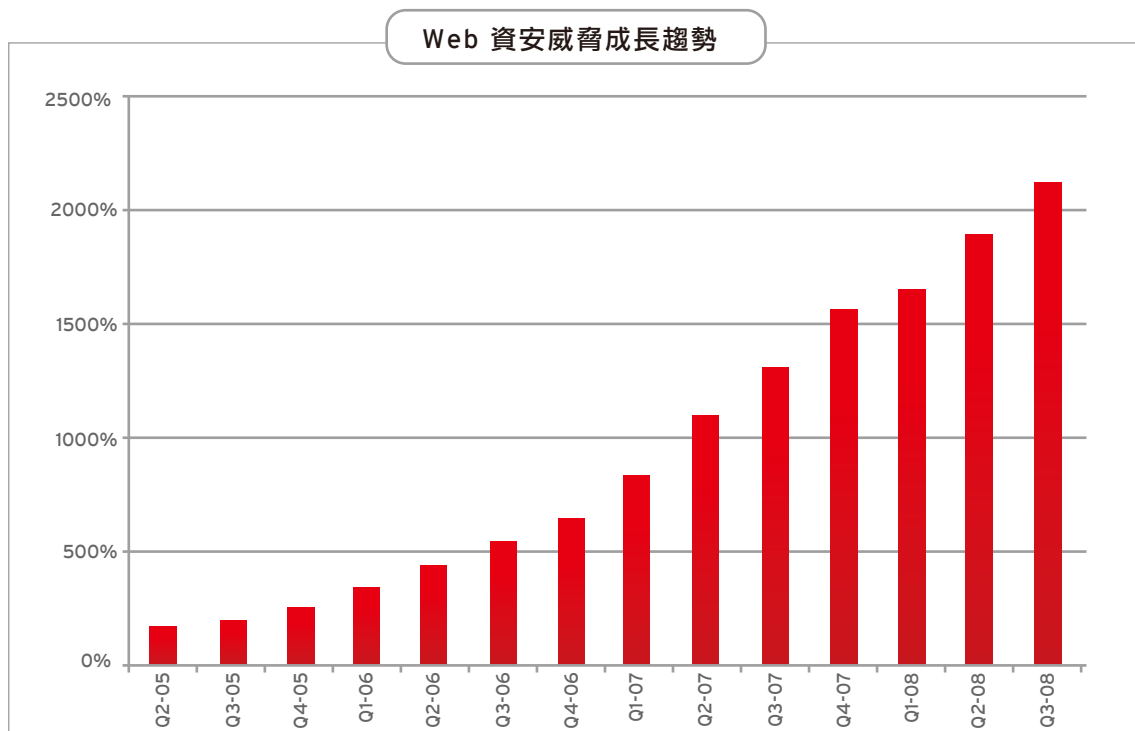
以下是趨勢科技 TrendLabs歸納出2008年與亞洲相關的重大資安威脅：

1. 大規模Web入侵攻擊
2. AUTORUN 惡意程式暴增
3. 社交工程詐騙手法
4. 區域性資安威脅

大規模Web入侵攻擊

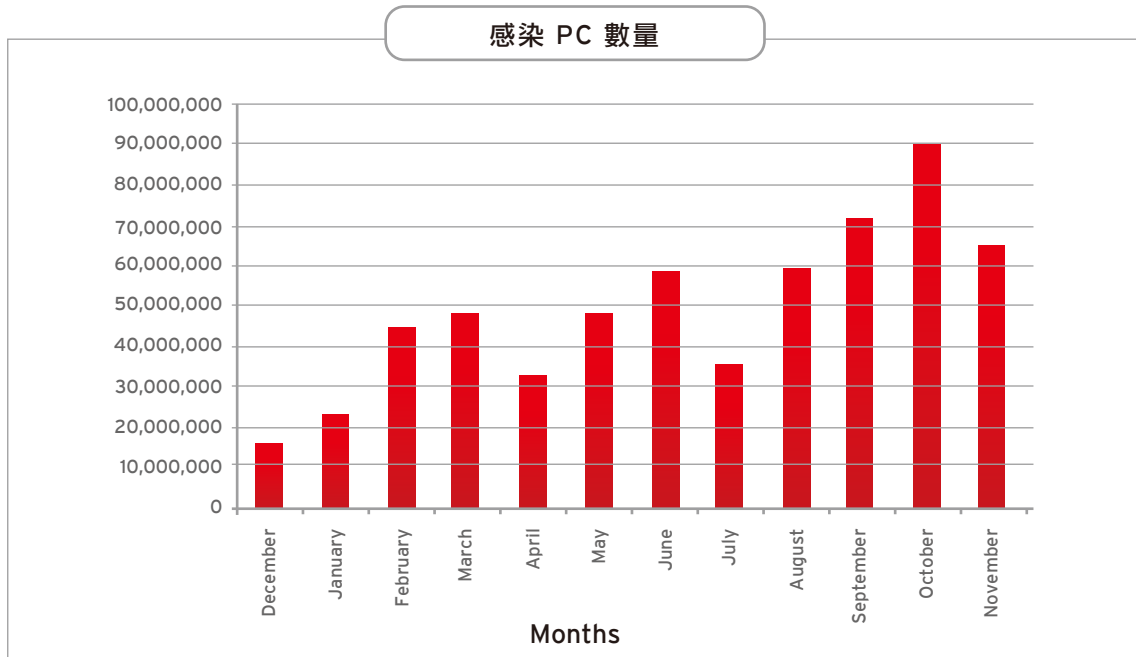
鎖定特定使用者族群與熱門網站為目標的攻擊手法，在2008年可說是相當猖獗，包括娛樂、政治、線上購物、社交網路等網站皆成為被鎖定入侵的目標，用以散播惡意程式。入侵行動在五月達到最高峰，全球許多網站被植入惡意程式碼，藉此感染不知情的網際網路使用者。不幸的是，這個趨勢似乎正以令人無法想像的速度持續發展。

Web 資安威脅持續展現驚人的成長率，如下圖所示：



圖．現有的 Web 資安威脅自 2005 年起的每季偵測總數，由圖中可看出每一年的第四季都會出現數量激增的現象。

下圖顯示自 2007 年 12 月至 2008 年 11 月期間遭感染的 PC 數量持續成長。遭感染 PC 數在 10 月達到最高峰，若加上 9 月與 11 月的數字，則較前三個月成長了將近 50%。就年度統計數據來看，整體亦呈現成長的趨勢。



資料來源：趨勢科技全球病毒即時監控中心

遭入侵網站對上網使用者構成相當嚴重的威脅，使用者可能以為所瀏覽的是值得信賴的網站，但事實上 PC 可能因此而遭惡意程式所感染。其運作方式非常簡單：利用程式設計的漏洞，在熱門網站中植入惡意程式碼，然後就等著無知的使用者自投羅網。2008年五月是大規模入侵攻擊最盛行的一個月（如下表）。亞洲也出現大量的日文和中文網站遭入侵。

日期	遭入侵網站數量
5月7日	9,000
5月10日	500,000
5月19日	327,000
5月21日	197,000

AUTORUN 惡意程式

經由可卸除式磁碟機散播的惡意程式在亞洲與澳洲地區佔了15%的比例，且在大多數亞洲國家，最盛行的惡意程式幾乎清一色都是AUTORUN惡意程式；而在歐洲、中東及非洲(EMEA)地區感染數最高的惡意程式當中，AUTORUN 惡意程式也名列其中。連NASA與美國國防部網路都遭滲透。

根據趨勢科技「台灣企業2008年度資安分析彙整」報告指出，利用USB移動儲存裝置當做傳播媒介的相關惡意程式比例最高，而且網頁威脅已經結合USB、Email整合成為無所不在的攻擊行為。由於企業內部USB移動儲存裝置控管不易，造成竊取私密資料越來越方便，甚至興起了地下經濟，盜賣個人資料。混合式攻擊也使得處理病毒問題日趨複雜，MIS人員很難找出造成問題的惡意程式檔案，造成企業生產力降低。病毒感染途徑範圍越來越大，光靠單一防護措施已經越來越難以防止，若是沒做好個環節中的其中一項，將導致企業內部用戶感染病毒頻繁。

年度前十大惡意程式

排名	病毒名稱	感染途徑
1	Mal_Infostl	Web Treat
2	Mal_Otorunl	USB
3	PE_LOOKED	Web Treat
4	TSPY_OMLINEG	Web Treat
5	Mal_Otorun2	USB
6	PE_Chir	Mail
7	HTML_IFRAME	Web Treat
8	Mal_NSAnti-1	USB
9	WORM_AUTORUN	USB
10	HTML_FUJACKS	Web Treat

圖：台灣企業感染的年度十大惡意程式，USB 與 Web Threat 網頁威脅成為主流

社交工程詐騙手法，運用了在地關心事件

下表中列出了現實世界中的重大事件，以及利用這些事件作為社交工程詐騙圈套誘餌的惡意程式攻擊，包含去年的四川地震、奧運：

真實事件	惡意程式攻擊
1月22日，達賴喇嘛呼籲抗議北京奧運	1月29日，垃圾郵件散播內含 TROJ_MDROPPER 的Word 檔案
5月12日，中國四川大地震	5月20日，詐騙郵件假借救災名義騙取捐款
8月8日至24日，北京奧運	7月9日，惡意 XLS、PPT 與 DOC 檔大肆散播，利用程式瑕疵植入並執行後門程式 7月15日，北京奧運樂透詐騙郵件 8月10日 仿效 419 詐騙手法的奧運詐騙圈套
9月22日，Bank of America 併購美林集團 (Merrill Lynch)	9月26日，美林集團 (Merrill Lynch) 垃圾郵件散播 ZBOT 傀儡程式

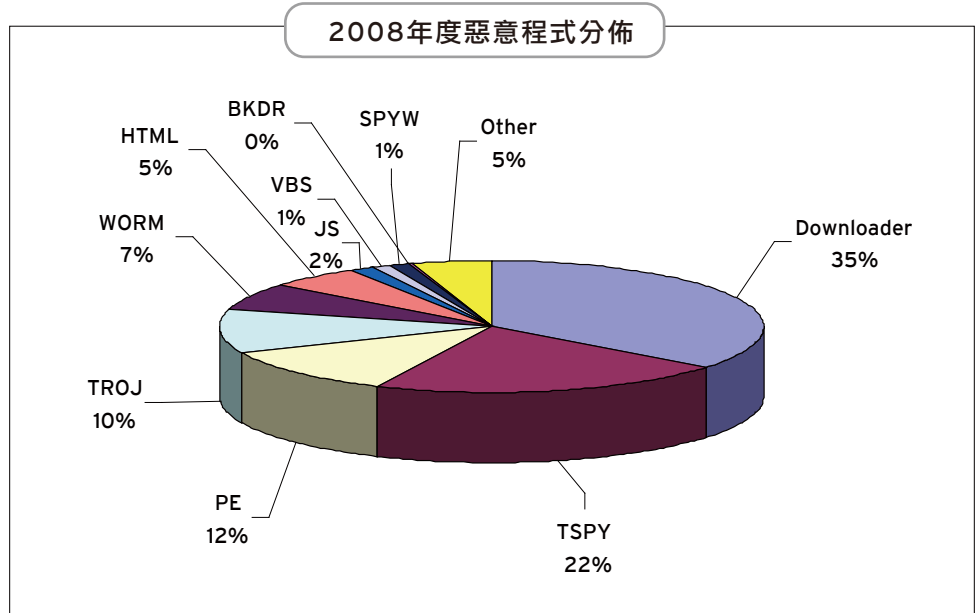
區域性資安威脅-亞洲案例

針對特定區域的獨特背景設計出不同的攻擊模式在 2008 年依然相當活躍而且有效：2 月時，惡意程式作者利用線上遊戲平台聯眾網站的安全弱點，在網站中設下陷阱等待中國的線上遊戲玩家上鉤。被植入網站中的弱點攻擊程式會將多種不同的 MMORPG 密碼竊取程式下載到瀏覽者的系統中。另外一案例為，網路釣魚詐騙郵件鎖定 Yahoo! Japan 拍賣網站使用者為攻擊目標，使他們面臨帳號資訊遭竊的風險

2008年台灣企業感染最多的惡意程式

根據趨勢科技「台灣企業2008年度資安分析彙整」報告指出，台灣企業在2008年感染的惡意程式前三種類型分別為：

1. Downloader病毒佔35%
2. TSPY病毒類型佔22%
3. PE病毒類型12%。



Downloader病毒

主要透過插入USB或是瀏覽被植入惡意連結的網站後遭植入此類型病毒。其主要危害在於執行後在連結至其他惡意網址下載病毒程式，透過不斷的更新病毒程式，讓中毒的電腦多重感染不同的病毒，造成資訊人員需要花大量的時間在解毒上，降低資訊人員的工作效率。

TSPY病毒類型

TSPY主要目的為竊取網路銀行與線上遊戲帳號密碼，其通常是從網路下載而來，執行之後會偵測受害者開啟的瀏覽器標題列中特定的字串，接著記錄下受害者所按的按鍵，然後再將這些資訊傳送給遠端使用者。當遠端的惡意程式使用者取得帳戶登入憑證之後，就能把受害人的銀行帳戶提領一空。

除此之外，這些惡意程式使用者還可以透過線上遊戲進行「實體金錢交易」(RMT)。RMT指的是線上遊戲玩家可用實際金錢來交易線上遊戲中的貨幣、物品以及任何遊戲配備。

PE病毒類型

指Portable Executable，也就是一般Windows可執行檔案格式。這種病毒被趨勢科技產品偵測為“PE_病毒名稱”。

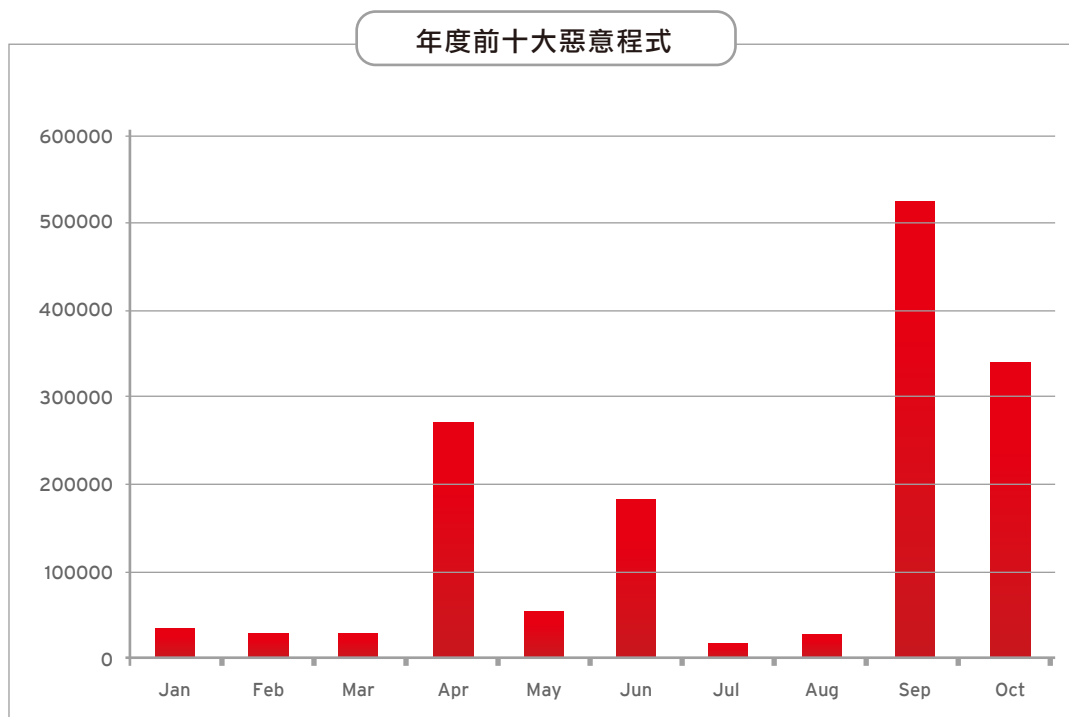
2008年資安相關統計數據

垃圾郵件：每天大約為1150億封

目前每天產生的垃圾郵件大約為1150億封，相較於2005到2006年期間每天約為750億封，成長幅度相當驚人。99%的垃圾郵件都是利用遭入侵的電腦以遠端搖控方式所散發。

在Spamalytics：垃圾郵件行銷成功率實證分析 (Spamalytics：An Empirical Analysis of Spam Marketing Conversion)這份報告中，資安研究人員實際模擬風暴傀儡網路散發垃圾郵件的運作，試圖確認垃圾郵件的銷售成功率，研究人員將此定義為垃圾郵件最後促成交易的或然率。研究人員在26天內發出了3億5千萬封電子郵件，結果促成了28件交易，成功銷售率為十萬分之一(0.00001%)。

趨勢科技的電子郵件誘捕系統所攔截的電子郵件也確認此一趨勢，經分析發現內含惡意附件檔的垃圾郵件數量在今年9月及10月期間出現激增的現象：

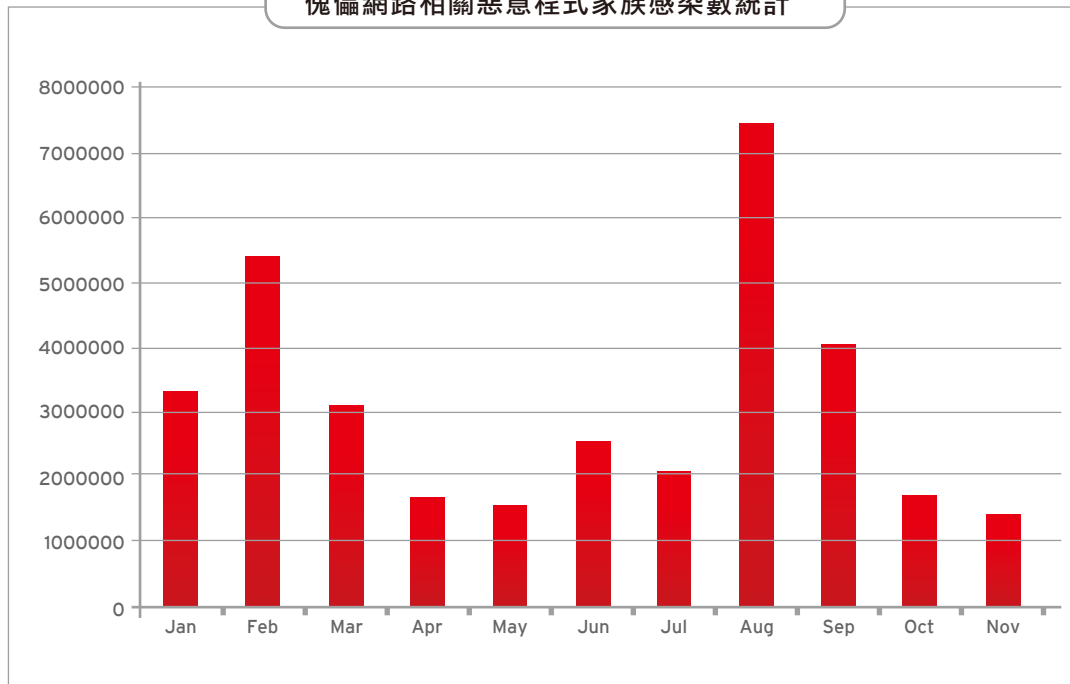


惡意附件檔在2008年9月及10月期間出現激增的現象。

惡意附件檔激增的原因可能是這類媒介可讓網路罪犯者任意結合社交工程手法變換攻擊策略，或是可透過特別設計的附件檔攻擊安全弱點。

傀儡網路：每月至少有超過1百萬台PC遭傀儡網路相關惡意程式感染

在2008年1月到11月期間，經常與傀儡網路掛鈎的惡意程式家族所感染的PC數多達3億4千3萬台。每月至少有超過1百萬台PC遭傀儡網路相關惡意程式感染。6-8月為感染高峰，感染數出現最大幅度的成長，高達476%。最高的是8月，高達750萬台，最低的是11月，只有140萬台。

傀儡網路相關惡意程式家族感染數統計


每月至少有超過 1 百萬台 PC 遭傀儡網路相關惡意程式感染。

安全弱點攻擊：超過 500,000 台的主機成為單隻漏洞攻擊蠕蟲的受害者

根據趨勢科技 TrendLabs 統計，2008年光是單一Internet Explorer未修補的安全弱點(MS08-067)，至少已成為兩波大規模線上攻擊利用的工具：一波大規模的資訊竊取行動，以及一波攻陷將近 6,000 個網站的大規模 SQL 隱碼攻擊。只要利用這些程式瑕疵，網路罪犯幾乎不需要依賴使用者互動即可成功達成其目的。

以 WORM_DOWNAD.A 為例，其利用 MS08-067 中所描述的安全弱點攻擊電腦系統，自首次發現至今，已有分布於不同國家、超過 500,000 台的主機成為這隻蠕蟲的受害者。

變更 DNS 設定的惡意程式：受害者數量估計已達到 100 萬人以上

這可說是最難追蹤的資安威脅，以 TROJ_AGENT.NDT 與 BKDR_AGENT.CAHZ 兩個變更 DNS 設定的惡意程式為例，它們會在網路上安裝惡意動態主機配置協定 (DHCP) 伺服器，藉此影響同一子網路區段上的其他主機。只要使用者連線到網路，電腦就會傳送要求給 DHCP 伺服器，伺服器收到要求時，會指派 IP 參數給該用戶端，讓用戶端可在網路中運作。去年 11 月，這類型安全威脅的受害者數量估計已達到 100 萬人以上。

2008年資安威脅總結

- Web Threat以及USB移動式儲存裝置已經成為最主要的病毒入侵管道
- 造成企業內部病毒流竄的主要途徑已經發展到各種途徑都有可能，病毒已經發展到複合多種的途徑(共享資料夾、USB等)來達到傳播的目的
- 網頁管理需要花更多的時間做資安的維護，對於網站管理員或是網頁程式開發人員，勢必增加更多的挑戰。一旦公司網頁被植入惡意連結，公司商譽必定受到很大的影響。
- 防毒並不是單一環節做好就可以，需要投入更多的人力以及物力來達到良好的防護效果

2009年的資安趨勢

Web 資安威脅自 2005 年至今已成長了將近 2000%。據趨勢科技資安威脅研究人員表示，2008 年的前 100 大惡意程式有一半以上均來自於網際網路，並且往往是不知情的使用者在瀏覽不明或惡意網站時所下載。

Web 2.0 成惡意程式散播平台

隨著可進行高度互動的Web 2.0的普及以及不斷發展的可利用應用漏洞，使得Web威脅愈演愈烈。趨勢科技CTO Raimund Genes 預言2009年將有更多惡意程式將大肆利用 Web 2.0 功能散播。無名小站、MySpace、Secondlife、YouTube、Flickr 以及 Wikipedia 等社交網站的設計讓真實世界中彼此不認識的消費者在線上進行互動。這個現象已經讓許多消費者逐漸習慣集體合作的社交網站的概念，在這個空間中，彼此不認識的使用者慣常地相互共享連結、照片、影片以及其他資訊。有許多網路詐騙行為可能藉由經常上網從事具有風險的Web 2.9使用者來滲透。一旦安全弱點加上 Web 2.0 使用者的認知不足，這類網站將成為Web 資安威脅的最大散播之管道。

駭客將繼續利用瀏覽器與其他 Web 應用程式，作為首選的感染媒介

駭客將使用與正常程式碼極為相似的惡意程式碼。舉例來說，IFRAME 已問世多年，而在駭客開始利用它們來散播惡意程式之前，已廣泛運用於許多網頁中。如2008年5月在大陸與台灣發聲大規模的SQL Injection 網頁攻擊的惡意程式碼HTML_IFRAME.NG，讓不知情的使用者一旦瀏覽這些遭感染的網頁，隨即會被轉向內含多種弱點攻擊程式的三個惡意網址之一。

除此之外，駭客將繼續利用Internet瀏覽器與其他 Web 應用程式，例如 Flash 與串流媒體播放程式等作為感染媒介。Google Chrome 推出，IE8 即將推出正式版，瀏覽器平台應用程式如 Microsoft Silverlight 與 Adobe Integrated Runtime的風行，將為惡意程式提供新的散播管道。資安威脅運作模式搶搭「Internet即時服務 (in-the-cloud)」熱潮，將目標鎖定提供這類功能的軟體與服務 (例如 Microsoft Azure)。

為躲避偵測 惡意程式家族將日益茁壯

趨勢科技統計發現43%的惡意程式，是系統先前所感染的未清除病毒，這些病毒往往會下載一個以上的惡意程式，藉以隱藏特定檔案，然後再與遠端位置取得聯繫，下載實際進行破壞的惡意程式，例如竊取資料的惡意程式。惡意程式作者將持續開發出以躲避偵測及防止被移除為目標的程式碼。因此，惡意程式家族數量將會增加。如此一來，防毒軟體業者開發智慧型啟發式/通用性病毒碼來偵測這些惡意程式的難度將會提高。

Mac 與 Linux 攻擊將增加

針對「替代性」作業系統程式瑕疵進行攻擊的資安威脅將會持續增加，尤其因為 Mac 與 Linux 愈來愈普及 (後者在筆記型電腦市場急速成長)。

駭客將挑戰Windows 7「可免於病毒危害」的說法

Microsoft 仍將是惡意程式作者最喜愛的目標，由於 Windows 7 將於 2009 年推出，網路犯罪者必將設法揭穿新版 Windows 作業系統宣稱「可免於病毒危害」的說法。概念驗證惡意程式將利用 Microsoft Surface 作為散播工具，此外如前文所述，Silverlight 與 Azure 也將成為資安威脅攻擊的對象。

利用行動裝置散播惡意程式的時機將在2009年達到高峰

網路罪犯利用行動裝置散播惡意程式的時機已逐漸成熟，並將在 2009 年達到高峰。此外由於行動電話與手持裝置與桌上型電腦互通程度愈來愈高，因此可預期更多資安威脅將嘗試透過共通的應用程式平台（例如 .NET、JAVA 等技術）「跨足」許多機器與裝置。當然，利用行動技術作為網路犯罪謀利工具的時代也相距不遠。

全球經濟危機2009年將繼續被駭客操作

網路罪犯將繼續利用時事、名人與政治人物的新聞作為社交工程圈套的誘餌。美國新任總統相關惡意程式將持續活動，此外熱切期待 Starcraft 2 與 WoW: Wrath of the Lich King 推出的遊戲玩家也應提高警覺。而全球經濟危機也將會成為惡意程式所利用的主題，因為此已成為人人都感興趣的話題，正剛好可用為惡意程式作者行網路詐騙之誘餌。

因應可能的威脅趨勢：Cloud-client 安全防護架構提供最即時的保護

有鑑於 Web 資安威脅的數量與技術均不斷提升，若要確保線上安全，建議採用多層架構的即時防護系統。趨勢科技的產品及服務已採用Cloud-client安全防護架構，不僅具備以網際網路層級 (in-the-cloud) 資安威脅資料庫為依據的信譽評等技術，此外還採用 Web 與電子郵件資安威脅資料關聯比對功能為輔助。這種獨特的 Cloud-client 安全防護架構可提供趨勢科技客戶最即時的保護，防範最新的網際網路威脅，盡享安心上網的樂趣。

個人消費者則可使用TrendMicro Internet Security Pro 旗艦版中內建之網頁信譽評等功能，防止使用者不慎瀏覽惡意網站，被植入專門竊取信用卡或其他寶貴資訊的惡意程式碼，導致個人資訊外洩。

趨勢科技 www.trendmicro.com.tw