IBM X-Force® 2010
年中趨勢與風險報告

2010 年 8 月

貢獻者

X-Force 年中趨勢與風險報告是 IBM 各部門協同作業的成果。我們要感謝下列人員對這份報告出版所付出的心力。

貢獻者	職稱
Bryan Williams	X-Force 研發（保護技術）
Carsten Hagemann	X-Force 軟體工程師（內容安全）
Dr. Jens Thamm	資料庫管理內容安全
Frank (Jamie) Licitra	X-Force 產品經理
Harold Moss	安全策略 — 新興科技與雲端運算技術架構設計師
Jon Larimer	X-Force 進階研究（惡意軟體）
Leslie Horacek	X-Force 威脅回應經理
Marc Noske	資料庫管理（內容安全）
Mark E.Wallis	X-Force 資料庫團隊、資深資訊開發人員
Michael Waidner	IBM 安全策略、安全技術長
Michelle Alvarez	MSS 情報中心（又稱鷹眼）團隊主管
Mike Warfield	X-Force 資深專家
Ralf Iffert	X-Force 內容安全經理
Ravi Srinivasan	IBM 軟體事業處、Tivoli 資深產品經理
Robert Freeman	資深技術人員及 Web 弱點攻擊守衛
Ryan McNulty	IBM Managed Security Services 及 SQL Querier Extraordinaire
Scott Moore	X-Force 軟體開發人員及 X-Force 資料庫團隊主管
Tom Cross	X-Force 進階研究經理
Wangui McKelvey	X-Force 產品行銷經理

關於 X-Force

IBM X-Force® 研發團隊研究並監看最新的風險趨勢，包括漏洞、弱點攻擊與主動攻擊、病毒與其他惡意軟體、垃圾郵件、網路釣魚及惡意網路內容。X-Force 會建議客戶與一般大眾如何回應全新與重大威脅，另外還提供安全內容，保護 IBM 客戶免受這些威脅。

目錄
第一部分

目錄
第二部分

概觀

隨著 2010 上半年過去，即將邁入下半年；在這個不斷變化的世界上，有一件事情仍舊維持原狀：攻擊者持續利用科技的快速發展取得經濟上的利益（包括竊取智慧財產權）。2009 年即將結束時，我們將威脅趨勢的評估做了總結，包括安全專業人員與攻擊者兩方面。更多技術、更優秀的自動化、更容易上手的使用者體驗，概括了雙方所使用的工具。我們看到專門設計的惡意軟體逐漸興起，而具備大量功能，其精密程度可與商業軟體比擬。這些最新威脅不只將重點放在單一入口，還積極瞄準企業的多重資源、確保弱點攻擊的成功。單一、公眾資源已不再是最大風險，取而代之的是，每名員工和端點都成了潛在的入口。漏洞攻擊、垃圾郵件、網絡釣魚、惡意 URL 與社交工程的精密組合，相較於以往，現在更容易混碼、自動化和進行部署。

企業與全球經濟正處於過渡階段。由於新技術有助於簡化任務，許多公司開始合併部門、縮減組織的規模。我們瞭解組織風氣的轉變可能導致混亂，員工也會有適應新環境的迫切需求。我們必須保護什麼東西？隨著我們逐漸進入新市場、採用新技術，安全前景有了什麼樣的改變？

我們看到傳統安全解決方案，面對新型混碼或小量攻擊媒介完全無法發揮效用。透過 SQL 資料隱碼和跨網站指令碼，針對 Web 伺服器攻擊早已不是新鮮事，但仍舊能夠讓人意想不到地隱藏起來，繞過眾多安全產品。員工平日使用文件時（無論是 PDF 檔案或 Office 文件），很容易受到直接攻擊。

威脅動態持續以驚人速度演變，認清當前趨勢顯得更加重要，因此我們要爲自己的未來做好準備。

全新的版面設計

今年的年中報告中，我們重新設計結構與版面，涵蓋兩個主要部分。第一部分介紹熱門話題與最新的重要趨勢；第二部分則介紹我們的傳統內容：IBM 安全解決方案的深度威脅資料與周全分析，也是讀者最期待的部分。

2010 年中重點

漏洞與弱點攻擊

- 進階持續威脅 - 說到這些經驗豐富的攻擊者，X-Force 最在意的事情是：儘管網路安全技術和實務都有顯著進展，但他們還是能成功滲透防禦完備的網路。我們特別關注數量持續增加的混碼攻擊，以及在現代安全系統的雷達下，四處流竄的隱密惡意軟體指揮控管通道。
- 混碼、混碼、混碼 - 透過 JavaScript 和 PDF 混碼，攻擊者不斷找到新方法來掩蓋惡意資料流量。混碼 (Obfuscation) 是一種供軟體開發人員與攻擊者之類用來隱藏或遮蔽所開發應用程式碼的技術。如果網路安全產品可以只封鎖 JavaScript 混碼，事情會變得容易許多，但不幸的是：許多合法網站也會使用混碼技術，企圖防止不懂世故的 Web 開發人員竊取他們的程式碼。這些合法網站成了惡意攻擊網站的掩護；尋找惡意攻擊就好像大海撈針一樣。
- 由於攻擊者找到新方法詐騙使用者，使得 PDF 攻擊持續增加。要瞭解 PDF 爲何成爲攻擊目標，您可以思考一下，在企業組織中端點通常是最弱的鏈結，而攻擊者當然知道這個事實。例如，在特定端點上可能沒有機密資料，但該端點可能會存取具有機密資料的端點，或者，該端點可以作爲特定的彈跳點，以啓動對其他電腦的攻擊。
- 漏洞舉報來到歷史新高點 - 在 2010 年，我們看到大量的漏洞揭露，這是因爲公開的弱點攻擊發布數目大量增加，以及多家大型軟體公司致力於識別及降低漏洞。
- Web 應用程式漏洞逐漸逼近 55% 的關卡，佔了 2010 上半年漏洞揭露的一半。
- 弱點攻擊付出的精力與潛在報酬 - 攻擊者追求的到底是什麼？隨著漏洞公布的數量不斷上升、供應商急著提供修補程式並保護問題區域，企業該如何爲 IT 管理人員的工作排定優先順序，以提供足夠的保護？弱點攻擊付出的精力與潛在報酬矩陣提供簡易模型，可從攻擊者的角度思考漏洞分級。

惡意軟體與惡意網站

- Conficker 蠕蟲是過去幾年來最大的電腦安全事件之一，因此現在正是更新這份趨勢報告的好時機。2009 年後，Conficker 蠕蟲發生了什麼事？
- Zeus 傀儡網路工具箱持續嚴重摧殘組織，Zeus 傀儡網路套件在 2010 年初發行更新版 Zeus 2.0。此版本中的主要新功能爲攻擊者提供更新功能。
- BlackHat SEO 以及假防毒軟體的弱點攻擊，仍然藉由誘騙使用者以滲透企業。
- 惡意網站工具箱 - 廣爲流傳的 Gumblar 工具箱能佔據有利的位置 對 Adobe 產品發動弱點攻擊；而 PDF 和 Flash 弱點攻擊，在許多其他弱點攻擊工具箱中也十分常見。另一項 2009 下半年的變化也相當有趣：ActiveX 已退出前五名之列（至少目前如此）。

垃圾郵件與網路釣魚

- 最常見的垃圾郵件網域已從中國 (**.cn**) 轉到俄國 (**.ru**)。
- 從 2010 年 3 月中開始，垃圾郵件的平均大小增加一倍；而影像垃圾郵件的百分比沒有任何變化。接下來幾星期內，垃圾郵件的平均位元組大小持續增加；到六月初爲止，平均大小已達到 10 KB。
- 2010 上半年，金融機構仍是第一名的目標，但現在只佔所有網路釣魚電子郵件目標的 49%。
- 2010 年前六個月，超過三分之二的金融網路釣魚目標皆位於北美洲；剩下的 32% 位於歐洲。
- 巴西依舊是最大的網路釣魚傳送端；印度則位居第二；南韓位居第三。

2010 後的新主題

- 虛擬化 — 爲提供更多功能給企業與客戶，組織正面臨著強大壓力。虛擬化是轉型的核心。然而，虛擬化最終的成功除了需仰賴能源效率、效能和易用性之外，還必須能夠提供這些利益，卻又不影響 IT 基礎架構的整體安全性、可靠性和可用性。
- IPv6 部署 — 什麼加速了採用新型網路的趨勢？
- 雲端運算是一種新興技術；其漏洞與傳統新興技術所發現的漏洞完全相同，不過日常遠端管理活動卻使情況變得更爲複雜。雲端運算目前仍處於發展初期；它涉及以設計和使用率爲基礎的實作範圍，故屬於多面性的技術。

IBM 安全協同作業

IBM 安全代表數個提供廣泛安全能力的品牌。X-Force® 研發團隊忙於分析最新趨勢與攻擊者使用的方法時，其他 IBM 團隊也努力爲客戶將這些豐富的資料匯入保護技術。

- IBM X-Force 研發團隊負責揭露、分析、監測與記錄各式各樣的電腦安全威脅與漏洞。
- IBM Managed Security Services (MSS) 負責監測端點、伺服器（包括 Web 伺服器），以及一般網路基礎架構的弱點攻擊。MSS 負責追蹤 Web 弱點攻擊，也包含其他媒介，例如電子郵件和即時傳訊。
- Professional Security Services (PSS) 提供全方位的企業層面安全評估、設計與部署服務，有助於建立有效的資訊安全解決方案。
- 我們的「Whiro」搜索器結合內容安全團隊 MSS 的警示資料與獨立分析，監測 Web 來源的弱點攻擊。Whiro 使用專門技術，甚至可以辨識混碼程度最高例子中的弱點攻擊，包括工具箱嘗試多個弱點攻擊的情況。
- 我們的內容安全團隊透過編目、獨立探索，以及 MSS 和 Whiro 所提供的摘要，進行獨立搜尋並分類網頁。
- IBM 已透過安全測試，從 IBM Rational AppScan onDemand Premium 服務整理了過去三年來的實際漏洞資料。這項服務結合應用程式安全評估的結果（從手動安全測試與驗證的 IBM Rational AppScan 處取得）。
- IBM 雲端安全服務讓客戶透過代管訂閱模式使用安全軟體的功能，有助於降低成本、改善服務供應品質，並提高安全性。
- 身分與存取管理解決方案提供全方位的身分管理、存取管理以及使用者遵規審核功能。這些解決方案可集中化並自動化管理使用者、鑑別、存取、審核原則和使用者服務供應。

2010 年應瞭解的熱門趨勢

企業的隱密威脅

2010 上半年，討論電腦安全實務時，幾乎在每個談話中都會談到這個新名詞：進階持續威脅。從前網路威脅，通常是一群無聊的青少年電腦駭客在網路上胡作非爲；近來，攻擊者已轉變成以金錢爲目的的專業電腦犯罪集團。現在更加詭計多端的威脅逐漸興起 — 也就是資金充足，並且由國家贊助的情報組織。進階持續威脅並非新的話題，這類攻擊已持續多年。真正令人感到新鮮的是：各式各樣的組織都在談論這類威脅，並在網路上與它展開激烈對抗。

說到這些經驗豐富的攻擊者，X-Force 最在意的事情是：儘管網路安全技術和實務都有顯著進展，但他們還是能成功滲透防禦完備的網路。我們特別關注數量持續增加的混碼攻擊，以及在現代安全系統的雷達下，四處流竄的隱密惡意軟體指揮控管通路。對抗這些威脅需要發展新的程序，最終必須採用全新的網路安全技術。

進階持續威脅

進階持續威脅 (APT) 一詞起源於美國政界，是指不同民族國家的各種不同團體，對電腦網路發動攻擊以竊取情報資訊；這跟以金融爲目的之團體有所不同（這類團體中，有些是以儲存的信用卡號爲目標）。「持續」一詞是用來描述 APT 團體的能力：即使網路操作員知道他們的存在，並積極採取對抗的措施，但他們仍舊能維持電腦網路存取與控制權。APT 團體非常有耐心，他們逐步取得想要的資訊，並保持在可能吸引注意的臨界點下。

APT 案例中的攻擊技術，其精密程度往往與網路維護人員能力的精密程度成正比。APT 團體似乎具備各式各樣的工具與能力，可從中選擇完成某項工作所需的最低限度的精密能力。網路維護人員發現入侵並做出回應時，就會出現更精密的工具與技術。

所有鎖定目標的精密攻擊，其共同點是攻擊者的第一步都是「偵察」。雖然談到電腦入侵，我們通常會想到傳統的網路探測與掃描活動，但經驗豐富的攻擊者往往會跳出這種思考模式。

今日，對於許多商業人士而言，很多資訊都可在網際網路上取得。我們將個人與專業資料發佈到社交網站上；送出狀態更新，告知我們正在旅行；我們加入與工作有關的線上論壇；在公開會議進行討論；撰寫文章與報告；並且接受新聞媒體採訪，做這些事情時，留下了大量的足跡，惡意人士不僅可重建自己的個人生活狀況，甚至連我們所屬組織的狀況以及我們如何融入組織，都被他們看得一清二楚。

經驗豐富的攻擊者

經驗豐富的攻擊者使用此公開資訊，便能充分掌握目標組織的全貌：誰在什麼地方工作？做些什麼？他們向組織內的什麼人報告？這些情報讓攻擊者可找到某些有權存取他們想要資訊的特定人員。這些人成了各種社交工程攻擊的目標，意圖騙他們執行惡意攻擊程式。攻擊者的最初目的是獲得受害者工作站的控制權。此後，受害者的工作與通訊全部一覽無遺。

這些攻擊往往涉及惡意文件或網頁，利用混碼對零時差漏洞展開攻擊。攻擊可能以電子郵件的形式呈現：事業夥伴或同事寄來的電子郵件可能帶有惡意附件，乍看之下與受害者職務直接相關。它可能是連至對手網站的鏈結，可下載一份有利可圖的文件；或者是商展上交給受害者的 USB 記號，裡面存有一份有趣的簡報。

透過弱點攻擊所安裝的自訂惡意軟體會使用隱密通道，透過網路通訊而不被發現。一旦攻擊者在受害者機器上執行惡意軟體，通常會進一步掌控目標網路內的其他系統。他們也會嘗試運用業務關係，利用受害者在公司的網路控制權入侵其他公司。

對私人企業的網路安全專業人員而言，以情報爲主的 APT 活動和以金融爲目的之攻擊，兩者間的界線並不明顯。發電廠曾遭到國家贊助的網路戰士攻擊，而只對勒索感興趣的犯罪集團，也同樣發動過類似攻擊。此外，精密的魚叉式網路釣魚 (spear phishing) 攻擊，過去是用來瞄準政府的軍事家，現在也用來瞄準能夠存取資金轉帳系統的金融機構主管。

從某些方面來說，這簡化了我們的工作 - 我們開發用來對抗這類攻擊的技術，可應用到各種不同的環境。然而，重要的是要明白：APT 一詞並未涵蓋所有企業面臨到的精密鎖定攻擊。雖然最近所有 APT 的討論可幫助加強人們對這類攻擊技術的意識，但我們不希望人們過度集中於情報相關的活動。不論攻擊者的動機爲何，設法保護網路免遭襲擊，就是網路安全從業人員應負的責任。

以金融爲目的之攻擊

在 2008 年度 X-Force 趨勢與風險報告中，我們介紹了一個簡易模型，也就是：從以金融爲目的之攻擊者的角度來思考漏洞分級，進而製作了「弱點攻擊付出的精力」與「潛在報酬」矩陣（先前稱作弱點攻擊機率矩陣）。此圖表標示出不同漏洞給電腦罪犯帶來的機會，以及利用這些機會需付出的精力。本報告第 21 頁的新版圖表說明：網際網路上被廣泛利用的漏洞，往往能與甜蜜點 (sweet spot) 融合 - 非常容易遭受弱點攻擊，這對心存惡念的人而言是大好機會。有組織的犯罪集團最愛見到這類漏洞，他們會對大量端點系統展開大規模的弱點攻擊。

然而，X-Force 發佈某些漏洞的警示與建議之後，攻擊者就必須付出高昂的代價才能進行弱點攻擊。經驗豐富的攻擊者若有能力自行開發攻擊工具，則可利用這類漏洞進行攻擊（儘管成本較高昂）。此外，某些漏洞過了一段時間之後，攻擊者不必付出太大代價，便可進行弱點攻擊。多數情況下，經驗豐富的攻擊者會先發現漏洞，再進行鎖定攻擊。最後安全專業人員發現攻擊活動、公開揭露此漏洞並加以修補。隨著越來越多漏洞資訊被公開（最終也會公開弱點攻擊的程式碼），與此漏洞相關的攻擊活動模式，便會從鎖定目標的攻擊，轉變成大範圍的弱點攻擊。

就此而言，鎖定目標的 APT 式攻擊和大範圍的傀儡網路活動，兩者間的關係十分密切；因爲由經驗豐富的團隊所開發的混碼技術及漏洞，用於鎖定目標的攻擊，最終會落入有組織犯罪集團手中，成爲大量弱點攻擊工具箱。結果是各層級的攻擊者變得越來越純熟。攻擊者的進化，最令人感到麻煩的地方是：各層級的攻擊者之能力持續成長，足以躲開各種商用現成網路安全解決方案的保護網，並能在網路管理員的雷達下隱密運作。這樣的發展給安全業界帶來很大壓力，他們必須找出更有效的方法，偵測現實世界中的威脅，而非只是在實驗室裡紙上談兵。

JavaScript 混碼 - 常見的躲避技術

這類躲避技術最重要的範例是 JavaScript 混碼。JavaScript 是一種靈活的語言，允許資料以程式碼的形式執行，讓資料可以被操控，也可以加密。現實環境的攻擊中，弱點攻擊內容通常透過 JavaScript 傳遞，並且隱藏在大量編碼資料中，成爲 JavaScript 的一部分；在網路上進行檢驗需花費大量財力物力，可是一旦這些編碼資料傳遞至端點，便會在瀏覽器和文件檢視軟體上解開。如果網路安全產品可以只封鎖 JavaScript 混碼，事情會變得容易許多，但不幸的是：許多合法網站也會使用混碼技術，企圖防止不懂世故的 Web 開發人員竊取他們的程式碼。這些合法網站成了惡意攻擊網站的掩護；尋找惡意攻擊就好像大海撈針一樣。

解決 APT 問題，不要期待能找到一勞永逸的方法。現成的安全解決方案可提供一些有幫助的工具，但您絕對買不到可輕鬆解決這類問題的產品。許多組織正在評估新的程序與技術，例如大量採用實體網段、通用電子郵件簽署，以及應用程式白名單。這些方法能夠提高安全標準，但也不是沒有破解的方法。混碼這類基本問題，需要全新的技術解決方案。安全業界必須負起責任，在這塊領域推動創新，爲網路管理員提供防禦的武器。

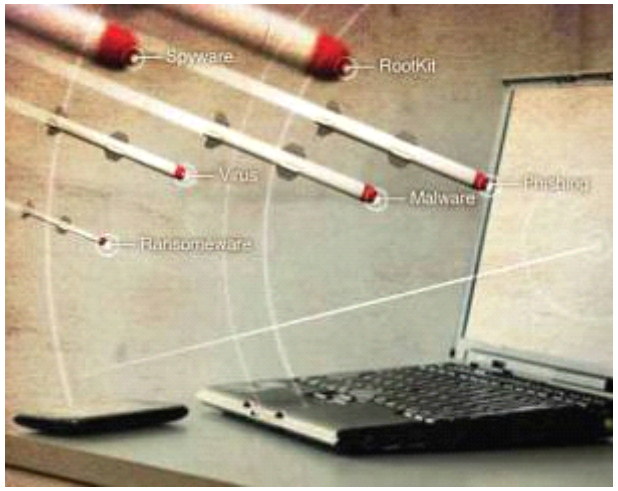
對抗 APT

根據我們的經驗，對抗這類網路威脅最有效的方式是：請您的員工一同加入這場戰役。有人認爲訓練使用者對精密魚叉式網路釣魚攻擊保持警戒是不可能的任務，但我們反對這種想法，因爲它確實能夠發揮效用。如果您可以找出組織內部哪些員工最容易遭受攻擊，可以坐下來跟他們解釋威脅的性質及其運作方式，便可讓這些員工成爲您的第一道防線。他們可以向您回報可疑的電子郵件；一旦您有了弱點攻擊的範例，便可以此爲立足點。您或許可以查出其他鎖定的受害者、找出惡意軟體指揮控管的模式，並開始解除這類侵擾。

最新的 PDF 弱點攻擊！

2009 上半年，X-Force 開始觀察大量使用的 PDF 弱點攻擊。之後，根據我們蒐集到的資料，它已經佔據了四處流竄的五大瀏覽器弱點攻擊其中的三項。要瞭解 PDF 爲何成爲攻擊目標，您可以思考一下，在企業組織中，端點通常是最弱的鏈結；而攻擊者當然知道這個事實。例如，在特定端點上可能沒有機密資料，但該端點可能會存取具有機密資料的端點，或者可以作爲特定的彈跳點，以啓動對其他電腦的攻擊。這還是不能充分解釋 PDF 攻擊爲何會如此頻繁，尤其 Internet Explorer 和 ActiveX 攻擊早已盛行多年。

我們在此提供一些有用的推測。首先，如果攻擊者對特定瀏覽器投入大量心力，一旦瀏覽器市佔率產生變化，可能會造成相當大的不便；相比之下，軟體卻能在大多數瀏覽器上運行，例如 PDF 和 Flash 的 Adobe 外掛程式。其次，特定瀏覽器的漏洞攻擊可能過於複雜，他們不得不轉向鎖定目標的攻擊。換句話說，某人若投入許多時間尋找確實可攻擊的 IE 或 Firefox（或其他瀏覽器）錯誤，便會以比一般漏洞更高的價格，出售瀏覽器漏洞細節或「武器化」的概念驗證。



難道 PDF 漏洞比較容易發現？與 ActiveX 錯誤相比，沒有明顯的證據可證明這點。然而，Microsoft 一直努力透過「kill bits」將易受攻擊的 ActiveX 介面列入黑名單（協力廠商所提供的也包含在內）。若將今年 IE 所揭露的「dangling pointer」錯誤的複雜性也算在內，PDF 漏洞已相對變少。

PDF 弱點攻擊勝過特定瀏覽器的攻擊，另外一個因素是：PDF 文件規格十分複雜，攻擊者可以輕易將資料植入 PDF 文件的其他地方，之後用程式擷取，再透過解碼器演算法傳回惡意指令碼。 133 這種混碼方法與早期的技術有很大不同；先前大都是透過弱點攻擊工具箱常見的 JavaScript 編碼常式進行 1:1 的轉換。我們會在 **Web 瀏覽器弱點攻擊趨勢**的部分，對逐漸演變的混碼做進一步的討論。雖然擷取植入 PDF 其他物件中的資料有時可被察覺，但阻止 PDF 弱點攻擊的進階技術若是過度依賴成品偵測，便有可能產生誤判。

零時差 PDF 攻擊在修補程式出現前，可獲得前置時間，從攻擊者的角度來看，可爲 PDF 攻擊創造更大的價值。目前，Adobe 正積極處理攻擊活動；X-Force 希望這種趨勢能持續下去。此外，有傳言稱：Acrobat Reader 下一個主要版本將會內建沙盤推演 (Sandbox) 技術，以降低殘餘錯誤 (bug) 遭受弱點攻擊的機率。我們期待見到這種技術對四處流竄的 PDF 攻擊所造成的影響。X-Force 認爲此技術所帶來影響取決於：和其他瀏覽器外掛程式以及隨處可見的文件與多媒體格式比起來，該技術對成本/利益比的影響有多大？其他 PDF 檢視器也無法避免錯誤（雖然很少受到瞄準攻擊），而且實作上的差異，也可能會帶來極大的安全風險。例如，引發廣泛討論的 PDF「啓動」功能，在替代的 Foxit Reader 中並不會出現任何提示。當然執行 Adobe 產品時，還是有可能出現詐騙的提示欄位。可是 Foxit 也和 Adobe 一樣，正試圖提升產品的安全功能，例如使用「安全模式」。

防範 PDF 攻擊

下列事項可幫助使用者防範 PDF 攻擊。可以在 Acrobat Reader 中停用 ActionScript（Adobe 的 JavaScript 延伸版本），雖然這樣並不能阻止某些 PDF 攻擊，但仍舊能發揮不錯效果。雖然此處只提到 Acrobat Reader，並未提到其他供應商的 PDF 檢視器，但大多數選項或應用程式偏好設定應該都是大同小異。除此之外，其他多媒體格式可嵌入 PDF 文件（例如視訊和 Flash 影片），這點也值得特別注意；在 Acrobat 偏好設定中有一個選項可停用此功能。X-Force 認爲大多數企業不會用到這項功能；多數情況下，一般使用者也不會用到。

展望 2010 下半年並進入 2011 年，很難想像攻擊者對 PDF 會逐漸失去興趣。不論 PDF 漏洞揭露的數量多寡，X-Force 竭誠希望有天這會成爲事實。某個在 2006 年修補過的 ActiveX 問題在修補程式發佈數年之後，仍舊持續被 Web 瀏覽器攻擊者使用。最重要的未知因素是：未來 Acrobat 沙盤推演技術會對已知及未知的攻擊，造成何種程度的影響？

PDF 弱點攻擊活動

先前提過 PDF 弱點攻擊近來變得十分熱門；IBM Managed Security Services (MSS) 的資料也贊同這點。我們見到此弱點攻擊技術持續主導整個威脅趨勢。PDF 攻擊事件活動在今年 4 月大幅躍升（請參見圖 1）。該月事件活動幾乎比 2010 上半年的平均多了 37%。出現高峰的主要原因是：該月份惡意垃圾郵件的流通率急劇上升。受害人收到了含有特製 Adobe Acrobat (PDF) 檔案的電子郵件，利用 /Launch 指令的漏洞發動攻擊。

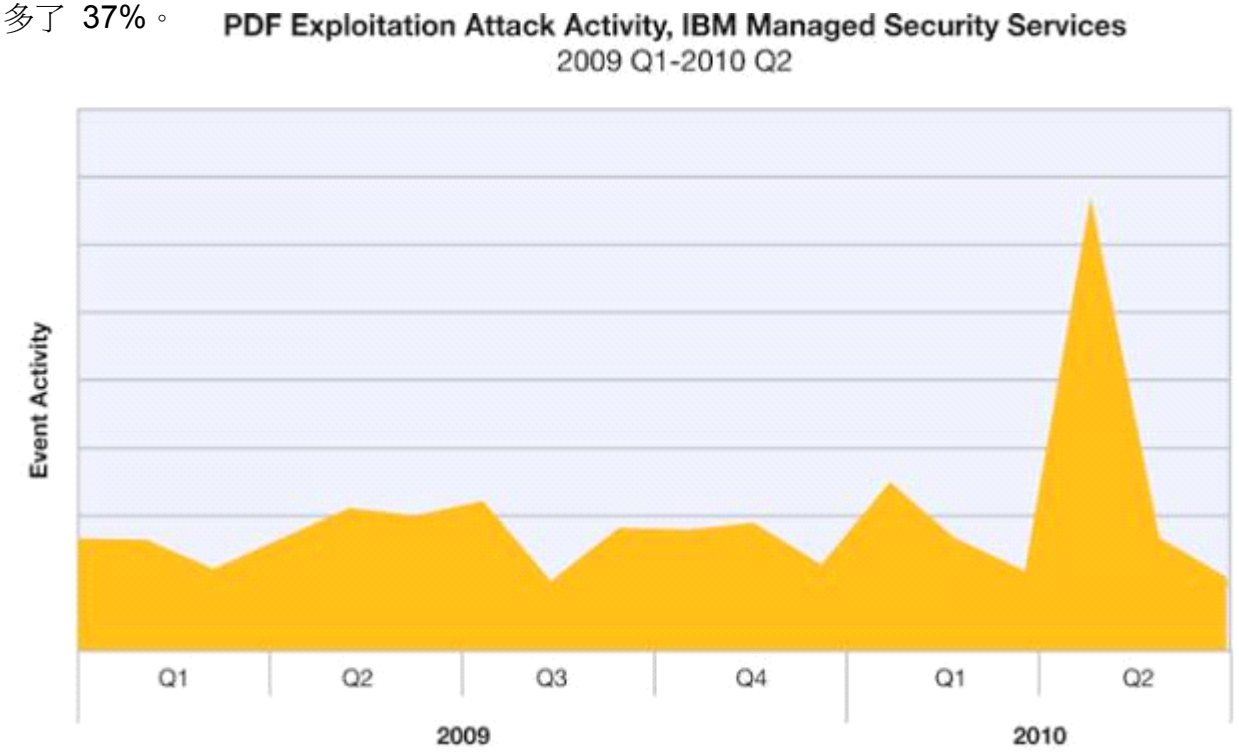


圖 1： 2009 年第 1 季到 2010 年第 2 季 PDF 弱點攻擊活動 (IBM Managed Security Services)

IBM Managed Security Services (MSS) 對最常見的客戶端漏洞攻擊類型做了詳細的觀察。MSS 提供全方位即時安全管理的委外解決方案，包括系統監控、緊急應變，以及全年無休的保護。

這些服務涵蓋多種平台及作業系統；支援不同的網路、伺服器、端點、無線應用程式，並提供事件監控。MSS 能穩定查看網際網路上的整體攻擊活動。這份報告使用了 MSS 資料子集，以找出攻擊趨勢。

Pushdo（也稱爲 Cutwail）及 Zeus 傀儡網路也和 PDF 惡意軟體有關。透過網路傳輸的 PDF 檔案，被嵌入可執行程式的啓動指令，這類事件在 2010 年 4 月呈現上升趨勢。該月份中，偵測到 HTTP 訊息中含有 Pushdo 木馬程式的事件也大幅增長。

說到 Pushdo，IBM X-Force 與 MMS 觀察到在今年年初，此傀儡網路發動分散式阻斷服務 (DDoS)，攻擊某些啓用 SSL 的網站。從那時起，讓 SSL 伺服器阻斷服務的特製訊息，被偵測到的數量明顯上升。我們猜想大多數這類活動都是由 Pushdo 所造成的；事實上 Pushdo 從 2007 年就開始四處流竄。

我們會在這份報告後面的章節，進一步探討 Zeus 傀儡網路的真相與迷思。

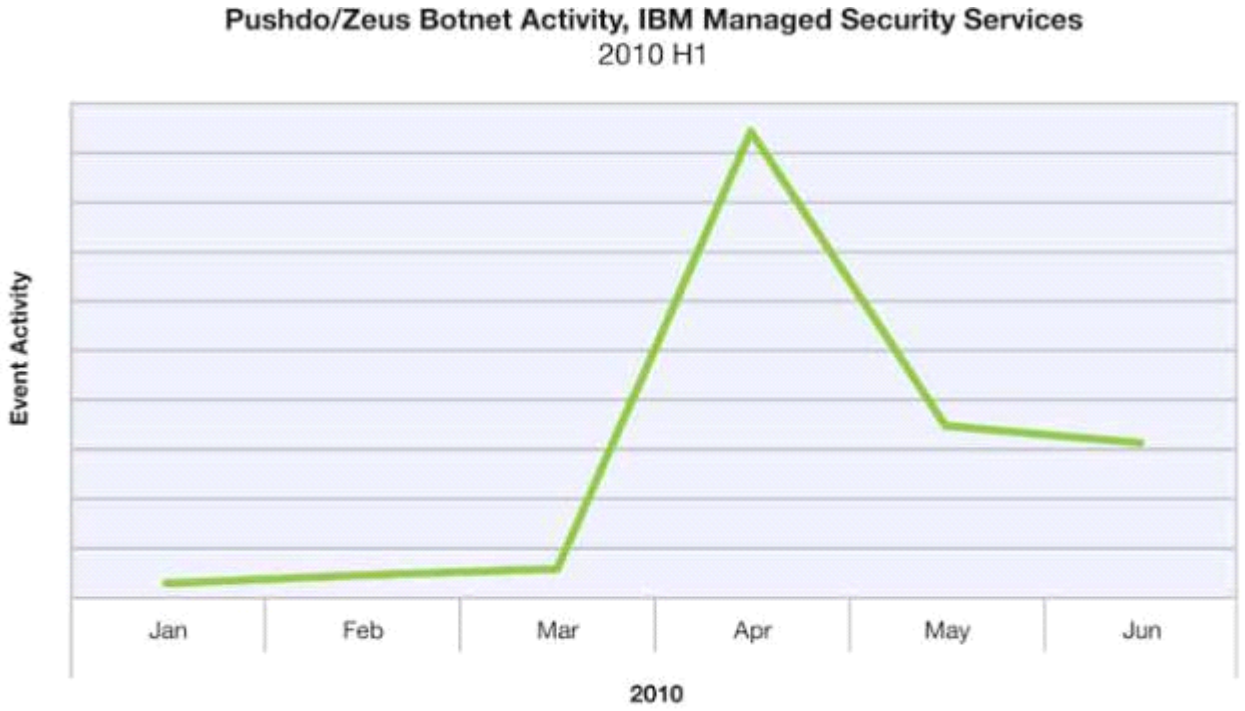


*圖 2：*2010 上半年 Pushdo/Zeus 傀儡網路活動 (IBM Managed Security Services)

惡意混碼趨勢

2010 上半年可見到 2009 年就存在的高度惡意混碼。在 2009 年，大多數 JavaScript 混碼的主要內容是：從惡意指令碼本身取得解碼金鑰；因此任何分析修改只會產生無用的訊息。JavaScript 混碼中有一些值得注意的詐騙手法。其中一個詐騙手法是：運用不同物件範圍來阻撓分析工具；做法是將函數指標放到物件裡，再用不同方式擷取。另一個值得注意的詐騙手法是：先用一些指令碼檢查物件或影像的狀態，然後再運行更多程式碼。

弱點攻擊工具箱套件（後面會有詳細探討）還是比較偏愛惡意 Adobe Flash 與 PDF，以及 Java 檔案。混碼專爲這些格式所開發。歷史上，混碼程式碼是從早期的 JavaScript 實作演變而來。2010 年，爲了阻礙分析，使用針對特定格式的設備變得越來越普遍。例如，許多 PDF 文件中的物件可包含文字；之後可透過 ActionScript（本質上屬於 JavaScript）用程式進行存取。攻擊者通常不會在其他物件中用純文字封裝惡意指令碼；因此，當他們使用這種混碼方法時，通常都會配上解碼器演算法 - 較舊的工具箱中也許可以找到。

以 Visual Basic Script (VBS) 作爲混碼方法的案例變得越來越少。我們的資料指出：2009 年的普及率是 3.6%；我們也觀察到：2010 上半年的普及率甚至下降到只有 2%。過去幾年來，我們常討論到 VBS 的使用，它是 Internet Explorer 的專屬語言，一直以來作爲混碼方法使用都相當有效；主要是因爲缺乏開放原始碼的 VBS 處理專案。雖然目前尚不清楚爲何 VBS 使用率會持續下降，但我們相信這會是長期趨勢。

2009 下半年，我們觀察到一個潛在的新興趨勢，也就是用程式碼註解讓偵測啓發法故障，並在視覺上遮蔽基礎程式碼。使用此技術時，通常會看到註解字串隱藏在函數呼叫參數中。2010 上半年，這項技術尚未定期出現在網路上。X-Force 預計這種混碼方法會成爲週期性的熱潮。

何謂混碼 (Obfuscation)？

「Obfuscate」在字典上的定義是：讓東西被遮蔽或變得不清楚，攪亂一池泥水，這麼說也未嘗不可。

在程式設計語言中，軟體公司與攻擊者都試圖將自己的傑作隱藏。爲什麼軟體公司要隱藏或混淆程式碼？目的是爲了保護智慧財產、預防程式邏輯的反向工程，或者避免竄改。

更深一層來看，這就好像人們會使用密碼以防止別人看到自己的私人訊息。

攻擊者能夠成功利用這些常見標準來隱藏他們的活動是因爲：多數安全產品無法解讀所有可能的編碼/解碼組合，故無法偵測到這類攻擊。若想提供完備的偵測服務，就必須持續檢討新型攻擊方法。

混碼攻擊活動

2009 年觀測到的高度混碼在 2010 上半年持續蔓延。雖然混碼攻擊活動在今年前四個月無太大變化，但到了 2010 年 6 月卻有了大幅度躍升。該月事件數量上升至 2010 上半年平均的 1.4 倍。

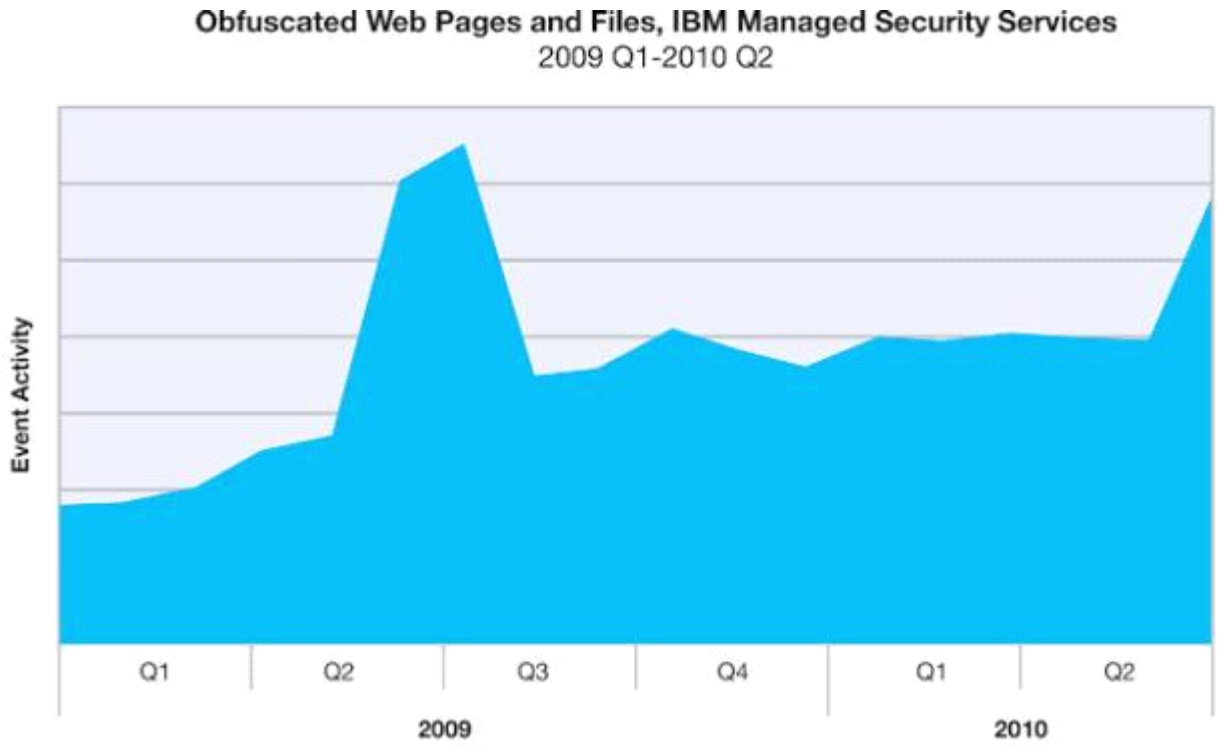


*圖 3：*2009 年第 1 季到 2010 年第 2 季的混碼網頁與檔案 (IBM Managed Security Services)

瞬息萬變的威脅趨勢

漏洞揭露 - 2010 上半年回報的數量遠超過 2009 年

2010 上半年漏洞揭露計數

X-Force 分析並記錄 2010 上半年 4,396 個新漏洞，相較於 2009 上半年，增加 36%；這是從有記錄以來，新揭露數量最多的上半年。

2007 年，漏洞計數首度滑落，但之後在 2008 年創下新高。雖然 2009' 年較低的漏洞揭露率，看起來似乎已進入停滯期；可是今年上半年的激增，讓人不禁對此趨勢感到懷疑。現在看起來，2009 年不過是短暫的沉寂，在那之後漏洞揭露便不斷上升。如果今年上半年的趨勢延續下去，預計 2010 年將會創下新高。

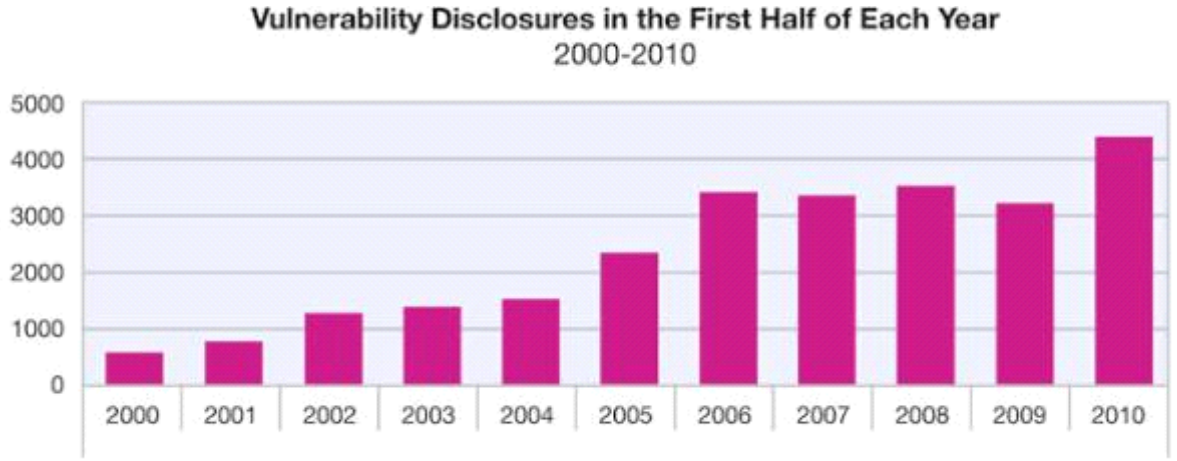


圖 4： 2000-2010 每年上半年的漏洞揭露

漏洞揭露的大量增加意味著什麼？我們可以確定一件事：所有供應商與其他來源所通報的漏洞，遠遠超過以往的數量。例如，2009 年 milw0rm 揭露超過 2000 個弱點攻擊。他們在那一年年底停止運作，由 Offensive Security Exploit Database 接手。2010 年到目前爲止，Offensive Security 已揭露超過 2000 個弱點攻擊。光是這個單一來源在 2010 年所發佈的弱點攻擊，就比往年多了 60%。

每年的漏洞揭露比率似乎在 6000 至 8000 筆新漏洞之間起伏。

爲避免關於漏洞特徵的說明有任何疑義，本報告採用以下的 IBM 安全服務定義。

「漏洞」是指多方面的條件，導致（或可能導致）資訊系統的機密性、完整性或可用性，出現明確或不明確的故障。

修補程式比率

2010 上半年所有揭露的漏洞，超過半數 (55 %) 始終沒有供應商提供修補程式。這略高於 2009 年的 52%。

漏洞修正程式與修補程式的可用性

前十名揭露漏洞最多的供應商，比上述 55% 的比率要好得多，只有 3% 至 24% 的漏洞並未修補。表 1 列出前十名揭露漏洞最多的供應商，以及他們在 2010 上半年和 2009 一整年的修補程式比率。

X-Force 發現 2009 年終報告使用的方法有一些問題，使調查結果產生缺陷。2010 年中報告中，我們已糾正這項方法；目前使用的公式更爲精確。我們已將這項新方法套用到此處 2009 年的資料以提高精確度。

此次比較提供若干有趣的結果。雖然 2009 年，Sun 修補程式比率爲 2.6%，表現可謂相當傑出；可是到了 2010 上半年，其未修補率卻排名第一，高達 24%。Microsoft 以些微差距排在第二名，共有 23.2% 的揭露漏洞未修補。

十大有漏洞的供應商與 2010 上半年的修補程式比率	
供應商	未修補 %
Sun	24.0%
Microsoft	23.2%
Mozilla	21.3%
Apple	12.9%
IBM	10.3%
Google	8.6%
Linux	8.2%
Oracle	6.8%
Cisco	6.0%
Adobe	2.9%

十大有漏洞的供應商與 2009 年的修補程式比率	
供應商	未修補 %
Microsoft	15.8%
HP	14.5%
Mozilla	12.1%
Apple	9.7%
Cisco	8.9%
Linux	5.0%
IBM	4.3%
Oracle	3.3%
Sun	2.6%
Adobe	2.0%

*表 1：*2010 年揭露最多的供應商，其漏洞未修補的百分比

2010 上半年漏洞未修補的百分比，通常遠高於 2009 年全年的百分比。這可能表示修補程式比率呈現下降趨勢；也可能只是因爲我們的資料截止日期爲六月底，無法反映出整年的趨勢。相信時間會證明一切。

目前，Adobe 是唯一能夠進入前十名，又能佔據「低於 5%」之類別的供應商，2010 上半年只有 2.9% 的揭露漏洞未修補，表現非常出色。

最佳與最差的修補者

表 2 顯示 2010 上半年無修補程式的揭露百分比，以及無修補程式的重大揭露與高嚴重性揭露百分比。Web 應用程式平台（如 WordPress 與 Joomla!）被排除在此分析之外。

最佳與最差修補者的圖表反映了公開通報，並且列入我們資料庫的資訊，但不一定能反映出某些情況，像是供應商默默修補漏洞，或者評估某些公開漏洞的通報無關緊要，所以並未對漏洞影響發表公開回應。

這份表格的分類依據是：供應商未對漏洞揭露提供修補程式的百分比，從最高到最低。

供應商	2010 上半年無修補程式的揭露百分比	2010 上半年無修補程式的重大與高嚴重性揭露百分比
所有供應商 - 2010 上半年平均	55%	71%
Microsoft	23%	7%
Mozilla	17%	4%
Apple	12%	0%
IBM	9%	29%
Sun	8%	0%
Oracle	7%	22%
Cisco	6%	2%
Novell	5%	10%
HP	4%	5%
Linux	3%	0%
Adobe	3%	2%
Google	0%	0%

表 2： 2010 上半年最佳與最差的修補者

弱點攻擊付出的精力與潛在報酬矩陣

隨著漏洞公佈數量不斷上升，供應商也盡力提供修補程式並保護問題區域，企業該如何安排 IT 管理人員的優先任務，以提供足夠的保護？弱點攻擊付出的精力與潛在報酬矩陣提供簡易模型，可從攻擊者的角度思考漏洞分級。

2010 上半年，X-Force 發佈了漏洞警示與建議，以平面圖表做呈現（請參見**表 3**）。橫軸（弱點攻擊付出的精力）代表攻擊者利用漏洞攻擊必須付出的精力。縱軸（潛在報酬）代表攻擊者可能獲得的潛在利益。

X-Force 警示與建議展示的漏洞，都往右上方象限聚集（以紅色標示）。此象限代表這類問題可提供攻擊者高報酬，而且較容易實行。這些漏洞在網際網路上往往會遭受大量弱點攻擊；相比之下，左下方象限顯示的漏洞（以黃色標示）代表此漏洞較不容易受到弱點攻擊，但所提供的潛在報酬也不多。

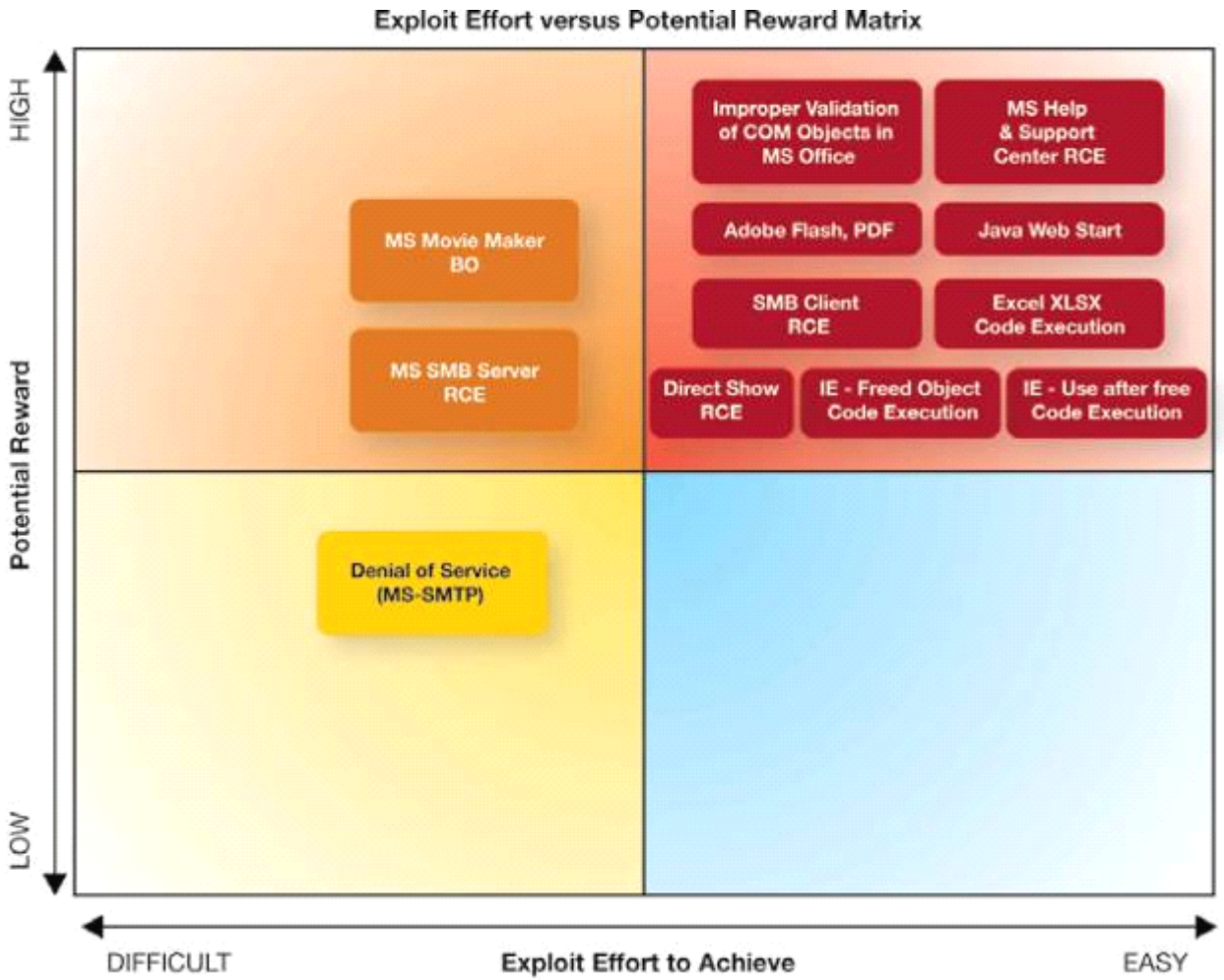


*圖 5：*弱點攻擊付出的精力與潛在報酬矩陣

之後在這份報告的第 **24** 頁，我們會討論在供應商提供修補程式之前先公佈重大漏洞，對客戶活動會造成什麼影響，且多快會成爲真正必須應付的問題。我們會進一步討論位於矩陣右上方、引起關注的兩個漏洞。位於另一側是：影響 Microsoft SMTP 服務的阻斷服務問題。雖然電子郵件阻斷服務對網路操作員而言算是相當嚴重的威脅，但這類攻擊對攻擊者而言，幾乎找不到任何經濟契機。沒有人會去公佈這類漏洞的公開弱點攻擊，所以也不容易被當成攻擊目標。

「Internet Explorer Freed Object Code Execution」漏洞適合用來說明：當越來越多資訊被揭露，漏洞可能會從左邊跨到矩陣的另一邊。這個問題是先被攻擊者發現，然後被當作攻擊目標。找出並利用獨特、未公開、未修補的漏洞需要付出大量時間精力，但一旦問題被公開揭露，弱點攻擊就會被公開傳播；此時，心存惡念的人只需付出少量時間精力，便可鎖定問題攻擊。

日期	警示/建議	漏洞名稱
2010 年 6 月 14 日	警示 370	**Microsoft Windows Help and Support Center Could Allow Remote Code Execution** 這個 Microsoft 說明中心內的漏洞是由特製 hcp 要求中的無效 Unicode 字元資料隱碼所造成。
2010 年 4 月 20 日	警示 367	**Java Web Start** 某個啓動並安裝應用程式的 Java 功能在設計上有缺失，允許任意指令直接傳送到 Java 虛擬機器。
2010 年 6 月 08 日	警示 368	**Improper Validation of COM Objects in Microsoft Office** Microsoft Office 應用程式無法對嵌入複合文件的 COM 物件進行正確驗證；允許攻擊者繞過 Office 的安全設定，並在 Office 檔案裡嵌入已知有缺陷的物件。一旦攻擊者利用控制項內的現有缺陷進行弱點攻擊，便可以執行任意程式碼。
2010 年 3 月 9 日	警示 364	**Microsoft Internet Explorer Use-after-free Code Execution** Microsoft Internet Explorer 可能允許遠端攻擊者在系統上執行程式碼，此問題起因於無效指標參照錯誤。
2010 年 6 月 7 日	警示 369	**Flash Player, Adobe Acrobat and Acrobat Reader Remote Code Execution** 如果受害者打開特製的 PDF（可攜式文件格式）檔或 SWF 檔，此漏洞可能會允許遠端程式碼執行。

表格接續到第 23 頁

日期	警示/建議	漏洞名稱
2010 年 1 月 15 日	警示 359	**Microsoft Internet Explorer Freed Object Code Execution** 網頁弱點攻擊工具箱以瀏覽器和瀏覽器相關的弱點攻擊爲目標而惡名昭彰（例如此處的漏洞）。 根據通報，此漏洞涉及知名的 Google 攻擊事件，也包括其他 20 多個大公司。
2010 年 4 月 13 日	警示 366	**Microsoft DirectShow Remote Code Execution** 此漏洞存在於所有新款 Microsoft Windows 作業系統。成功利用此問題進行弱點攻擊，可讓攻擊者完全控制端點目標。惡意媒體檔案的使用（如影像和電影）在過去幾年十分盛行。
2010 年 3 月 9 日	警示 363	**Microsoft Excel XLSX Code Execution** Microsoft Excel 可能允許遠端攻擊者在系統上執行任意程式碼，此問題起因於 Excel 試算表檔案格式的不當剖析。
2010 年 2 月 9 日	警示 360	**Microsoft Windows SMB Client Remote Code Execution** 此漏洞出現在最新 Microsoft Windows 作業系統的核心元件中（包括 Windows 7）。 最簡單的攻擊媒介需要攻擊者建立一個 SMB 伺服器，然後誘使使用者按下連到該伺服器的鏈結。 成功的弱點攻擊讓攻擊者能完全控制使用者的系統。
2010 年 3 月 9 日	警示 362	**Microsoft Movie Maker Buffer Overflow** Microsoft Movie Maker 容易受到緩衝區溢位的攻擊，此問題起因於剖析惡意 Movie Maker (.mswmm) 檔案時，不正確的界限檢查。
2010 年 2 月 9 日	警示 361	**Microsoft Windows SMB Server Remote Code Execution** 此漏洞出現在最新 Microsoft Windows 作業系統的核心元件中（包括伺服器版本）。如果製作得當，此攻擊會提供完整遠端程式碼執行，無需任何使用者互動（但發生阻斷服務的機率也比較高）。然而，攻擊者必須先擁有系統的鑑別權限，訪客帳戶在這種情況下無法發揮作用。
2010 年 4 月 13 日	警示 365	**Denial of Service Conditions in Microsoft Exchange and Microsoft SMTP Service** 成功的弱點攻擊可能導致 SMTP 服務重新啓動；重複攻擊可完全中斷 Microsoft Exchange 服務。SMTP 服務經常接觸網際網路，一般認爲電子郵件屬於重要商業功能，所以此漏洞所造成的商業影響會比典型阻斷服務問題更爲嚴重。

*表 3：*2010 上半年 X-Force 警示與建議

影響深遠的公開揭露

2010 上半年揭露的兩個最重大的漏洞是 Java Web Start 以及 Microsoft Windows 說明與支援 中心中的遠端程式碼執行漏洞。Tavis Ormandy 研究人員在供應商提供修補程式前，公開揭露了這兩個漏洞。如果弱點攻擊的細節在提供修補程式前被公開，這樣攻擊者便能以少量精力換取大量機會，這些在現實世界中，與漏洞有關的迅速弱點攻擊活動，符合我們的模型所預測的結果（請參見圖 6）。

以 Java Web Start 漏洞爲例，在 2010 年 4 月 20 日，IBM 安全發佈新的簽章以保護我們的客戶，並在網站公佈此威脅。如同右側資料所呈現的 :2010 年 4 月 21 日開始部署這些新簽章的客戶，得到了立竿見影的效果。第一天，在客戶群當中可見到超過 100 個安全事件，此數字持續攀升到六月底，之後在七月份開始出現緩慢下降。

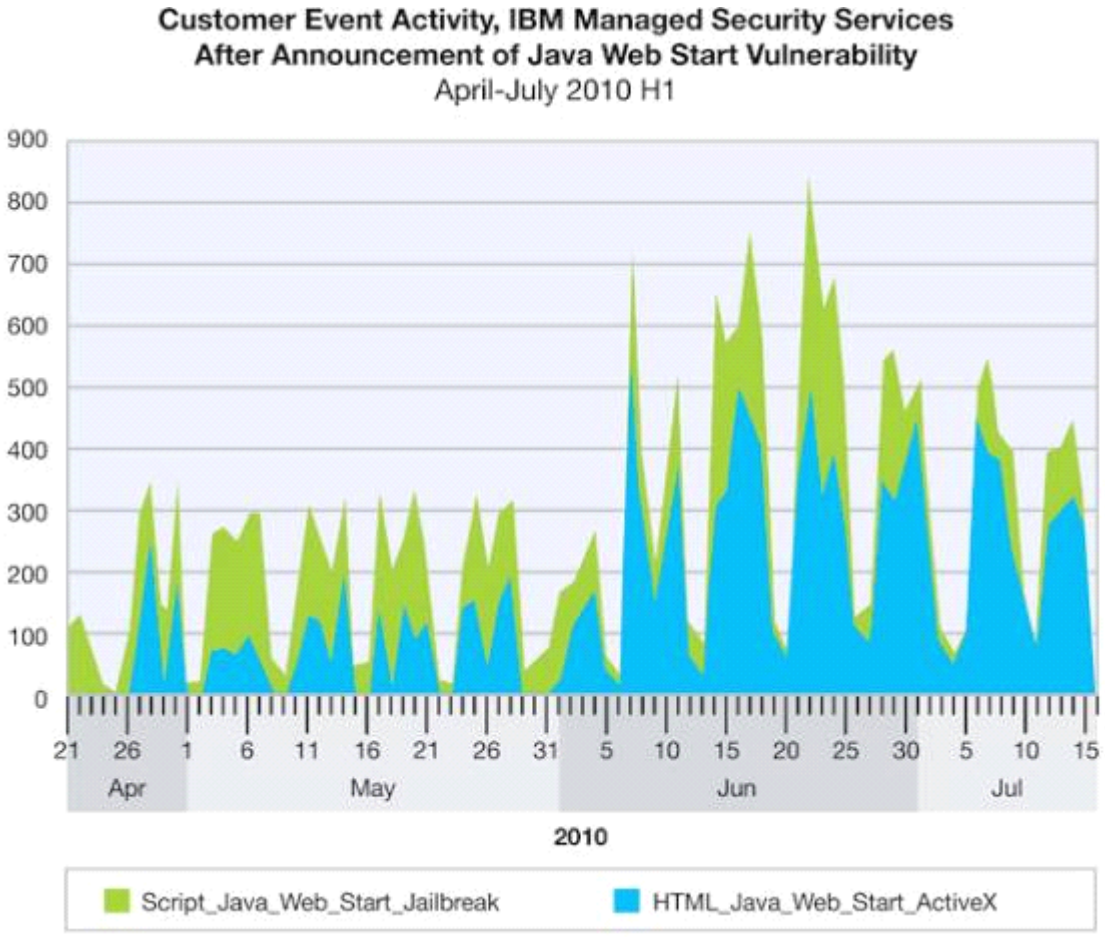


*圖 6：*2010 上半年 4 月至 7 月 Java Web Start 漏洞公佈後的 MSS 客戶事件活動

Conficker 更新 - 2009 年底後發生了什麼事？

Conficker 蠕蟲是過去幾年來最大的電腦安全事件之一。現在正是更新這項趨勢報告的好時機；但在這之前，讓我們先談一點它的歷史。

Conficker 在 2008 年秋天首次展開蔓延。最初的變種（稱爲 Conficker.A）以 Microsoft RPC 堆疊中的遠端程式碼執行漏洞爲目標，此漏洞最近才做了修補。和歷史上鎖定類似漏洞的蠕蟲大爆發比起來（如 2003 年 Blaster 蠕蟲），Conficker.A 並未取得巨大成功，主要是因爲網際網路回應漏洞揭露的速度得到改善。截至 2008 年底，只有數十萬部主機受到 Conficker 的感染。

2008 年 12 月底，新版 Conficker（也就是 Conficker.B）開始出現。Conficker.B 將一大群替代傳播媒介加入 Conficker 製造中心。Conficker.B 可透過 USB 金鑰、檔案共享，或破解 Windows 網域上的簡單密碼而四處蔓延。這些替代媒介使 Conficker 更爲靈活。它可以使用不同媒介在各種網路建立據點；導致受感染的主機數量大幅擴增。

到了 2009 年冬季，一個名爲 Conficker Working Group 的保衛隊成立，專門對付 Conficker。Conficker.A 與 Conficker.B 的節點，每天會嘗試聯繫 500 個隨機生成的網域名稱，尋找是否有更新項目。

Conficker Working Group 會將那些網域名稱全部登錄，使 Conficker 操作員無法更新機器人程式。不幸的是，某個新版 Conficker 能夠克服這項障礙。新變種稱爲 Conficker.C。

Conficker.C 將網域清單從 500 個擴增到 5 萬個，並新增加密 P2P 更新機制，不再倚賴 Conficker Working Group 可登錄的網域。這些新功能使 Conficker Working Group 無法阻止 Conficker.C 更新。幸運的是：Conficker.C 未包含傳播程式碼，所以無法感染起始節點以外的地方。

2003 年 8 月，Blaster 蠕蟲開始在網際網路上傳播。它利用 Microsoft Windows RPC 堆疊中的漏洞 (MS03-026) 進行弱點攻擊，與 Conficker.A 所利用的漏洞十分類似。Blaster 釋出後 8 小時就達到傳播的高峰，最終網際網路上有 800 萬到 1600 萬部主機受到感染。Blaster 針對 WindowsUpdate.com 發動分散式阻斷服務攻擊，但因爲 Microsoft 使用不同位址更新主機，所以並未造成太大影響。

X-Force 針對 Conficker 所做的回應

X-Force 研究人員將 Conficker 程式碼做了反向工程轉換，並且在我們的 IPS 產品中開發一套簽章，可偵測並封鎖 Conficker.C P2P（點對點）流量。圖 7 顯示流量的總數隨時間慢慢衰退。不過引用最新資料時，我們注意到六月份的活動量微幅上升（這也是我們即將印製這份報告的時候）。X-Force 研究人員將繼續調查：此活動出現變動的原因，一旦有了進一步的訊息，便會讓我們的讀者透過 **Frequency X** 部落格得到最新資訊。

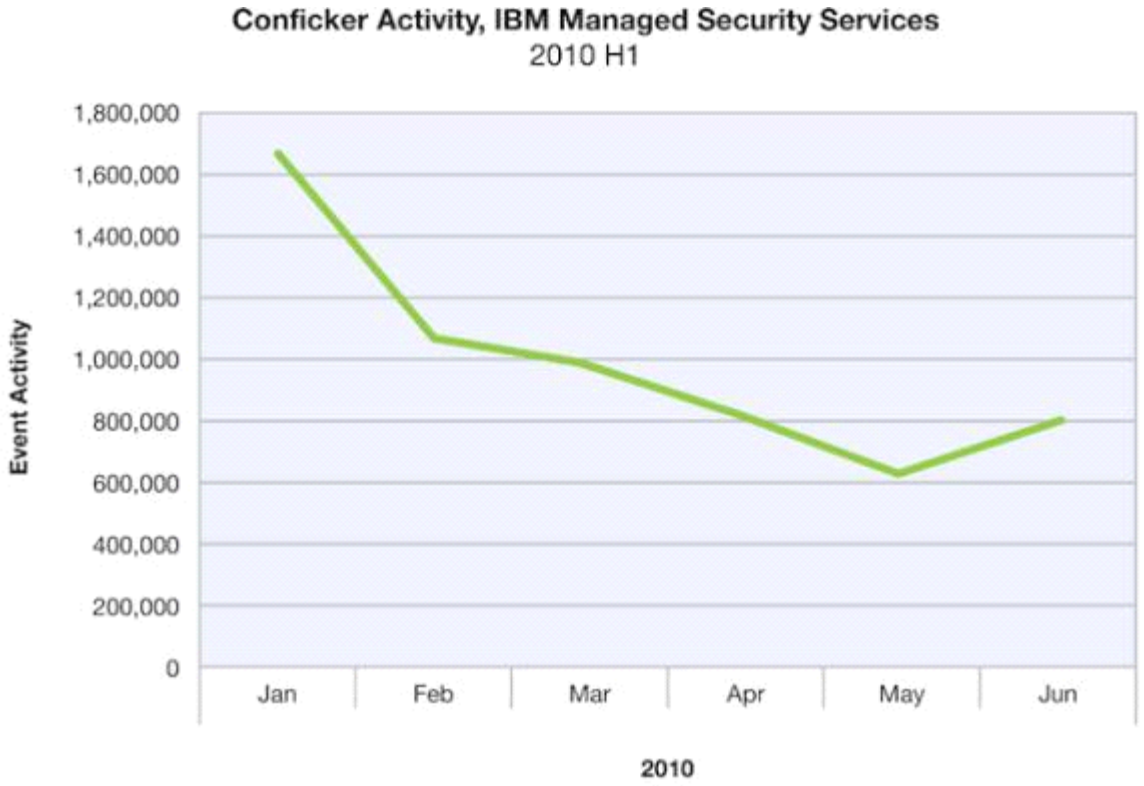


*圖 7：*2010 上半年 Conficker 活動 (IBM Managed Security Services)

這與來自 X-Force's Darknet 的 Conficker.C 資料一致（下圖 8）。

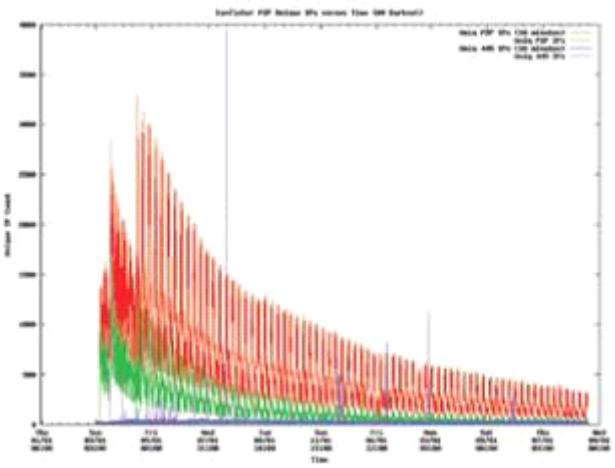


圖 8： Conficker Working Group

由於受感染的節點已用防毒軟體清除，或因故障而從網際網路上移除，所以 Conficker.C 正逐漸消失。Conficker.C 無法感染新節點，所以也無法在網際網路上維持其數量。這是件好事，畢竟 Conficker Working Group 無法阻止傀儡網路操作員更新 Conficker.C 節點。將近 20 萬個 Conficker.C 節點依舊停留在網際網路上等待更新。到目前爲止，更新項目並未廣泛流傳。

Conficker Working Group's Sinkholes 也是如此（圖 9）

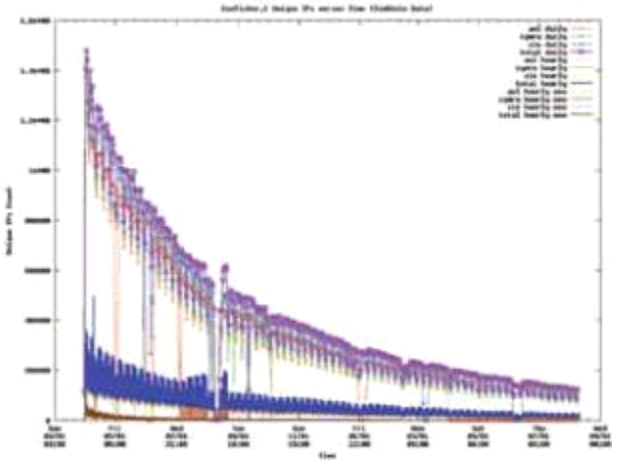


圖 9： Conficker Working Group

根據 Conficker Working Group 統計（上圖 10），Conficker.A/B 傀儡網路的範圍要大得多，其範圍涵蓋五、六百萬個節點。此傀儡網路在 2009 年 11 月左右達到高峰，並穩定維持 9 個月之久。試想：每天都有一些 Conficker.A/B 節點消失；基於同樣的理由，Conficker.C 節點也會消失 - 防毒軟體的安裝或系統故障。然而，Conficker.A/B 節點

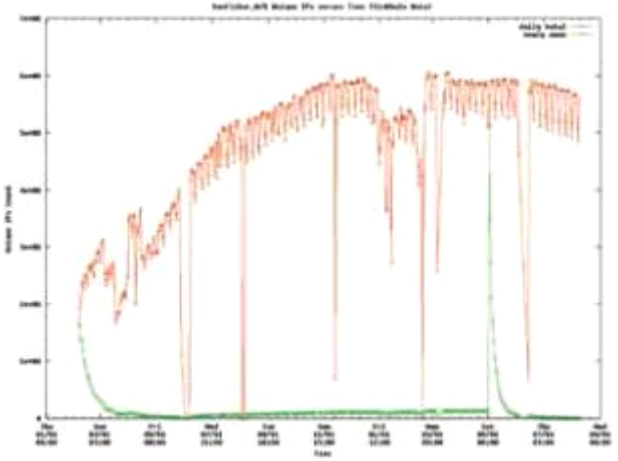


圖 10： Conficker Working Group

仍舊會藉由入侵新系統而蔓延。若要維持數量，新節點的感染率必須與節點死亡率相同。值得注意的是：在這麼長的一段時間裡，速率一直維持十分穩定的狀態。

Conficker 的未來？

幸運的是，即使 Conficker 設計者擁有感染了五、六百萬個節點的 Conficker.A/B 傀儡網路，也無法做壞事，因爲 Conficker Working Group 每天還是將這些節點試圖聯繫的 500 個網域名稱全部登錄。如果 Conficker Working Group 放棄努力，就等於把龐大的傀儡網路控制權拱手送給攻擊者；這將對網際網路基礎架構構成嚴重威脅。

儘管從 Conficker 病毒開始傳播到現在已將近兩年，但它尚未滅絕；就像一對沉睡的巨龍，其中一頭已受到控制，另一頭則隨時可能甦醒。我們從這次的經驗學到不少教訓，其中大部分都是負面的，顯然蠕蟲仍舊可在現今的網際網路上，構建非常龐大的傀儡網路。顯然這些傀儡網路可以維持多年、擁有數量龐大的節點，並用來做壞事。而 Conficker.C 顯然不可能建立傀儡網路控管系統，這種系統無法達到全球緩解。

然而，Conficker 經驗及 Conficker Working Group 的組成，已經將基礎架構操作員與安全公司結合成一個緊密的防護網。若下一個重大蠕蟲爆發時，此社群將會立即提出因應措施。

不爲人知的趨勢 - 惡意資料流量有何特徵？

IBM 分析師手上擁有許多資料資源可用來分析趨勢。其中一個資源是暗網 (darknet)，也稱黑洞網路。這個空間持續受到監控；所有傳入的資料流量會被全面捕獲並儲存，藉此進行分析和長期保存。此暗網擁有 25,600 個位址的口徑，屬於大型資訊收集網路的一部分。就暗網的本質而言，不曾有封包源自於這些位址；合法的資料流量也不曾被指派到這些位址。此外，這些位址從不曾分配給網際網路上任何作用中的合法裝置或服務。儘管如此，它們還是被宣稱屬於合法 "/16" 網路的一部分，而且可從廣大的網際網路完整路由傳送。因此，所有進入這個網路的資料，都會被視爲惡意的流量。

欺騙式阻斷服務攻擊

綜觀過去幾年的資料，有幾個值得注意的模式逐漸顯現。第一個趨勢是：僞造退信 (Backscatter) 活動逐漸增加（圖 11）。事實上，僞造退信屬於欺騙式阻斷服務 (DoS) 攻擊的連帶後果。它會僞造網際網路通訊協定 (IP) 封包中的來源位址，並發送給受害者；受害者的系統無法分辨封包真僞，而將回應發送給僞造的封包，這些回應的封包就稱爲「僞造退信」。

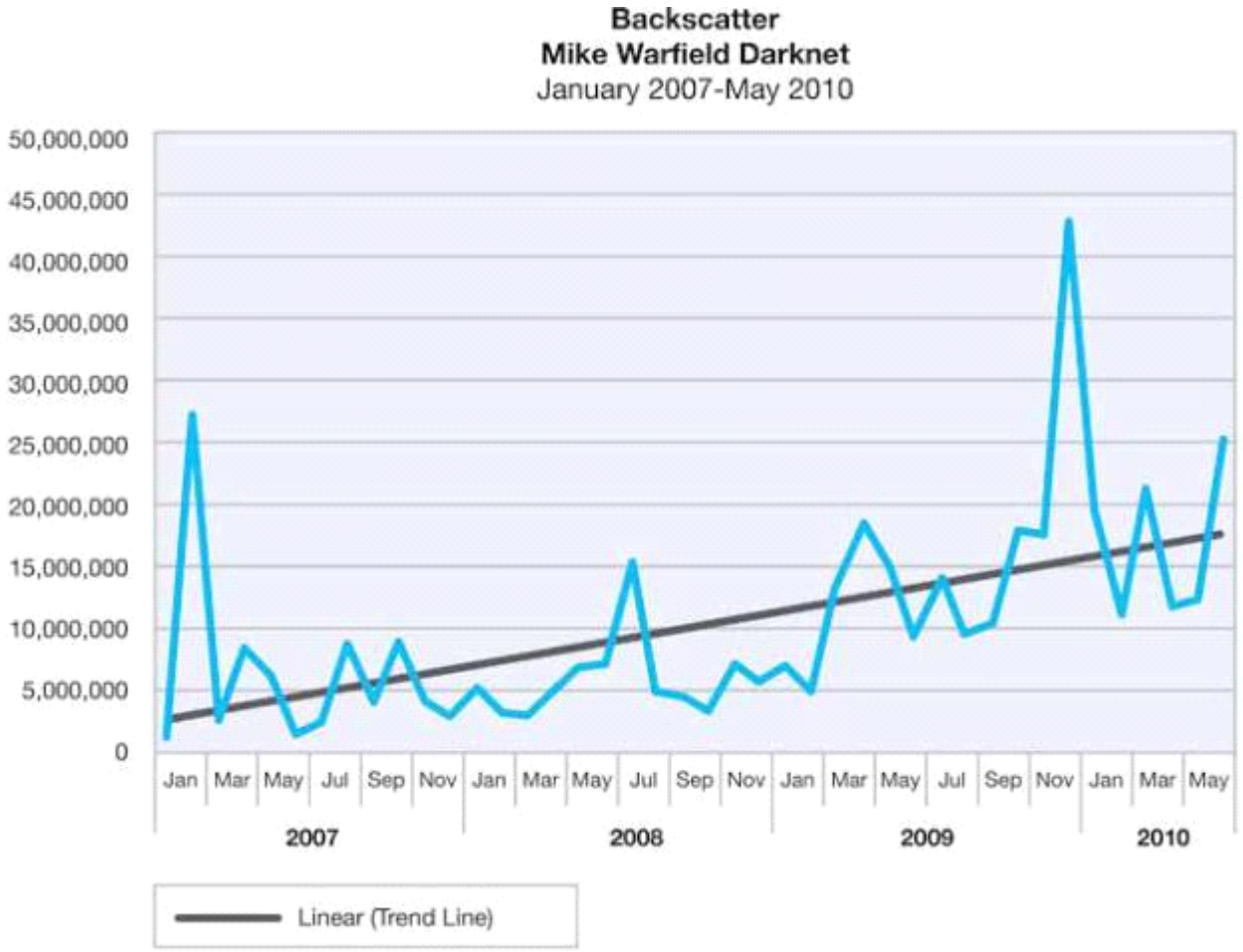


圖 11： 2007 年 1 月至 2010 年 5 月的僞造退信 (Mike Warfield Darknet)

在 Mike Warfield 暗網中，每收到一個 SYN-ACK 僞造退信封包就表示：攻擊者發送僞造封包到機器上的常用服務埠；而該機器正遭受 Mike Warfield 暗網地址所發動的僞造攻擊。

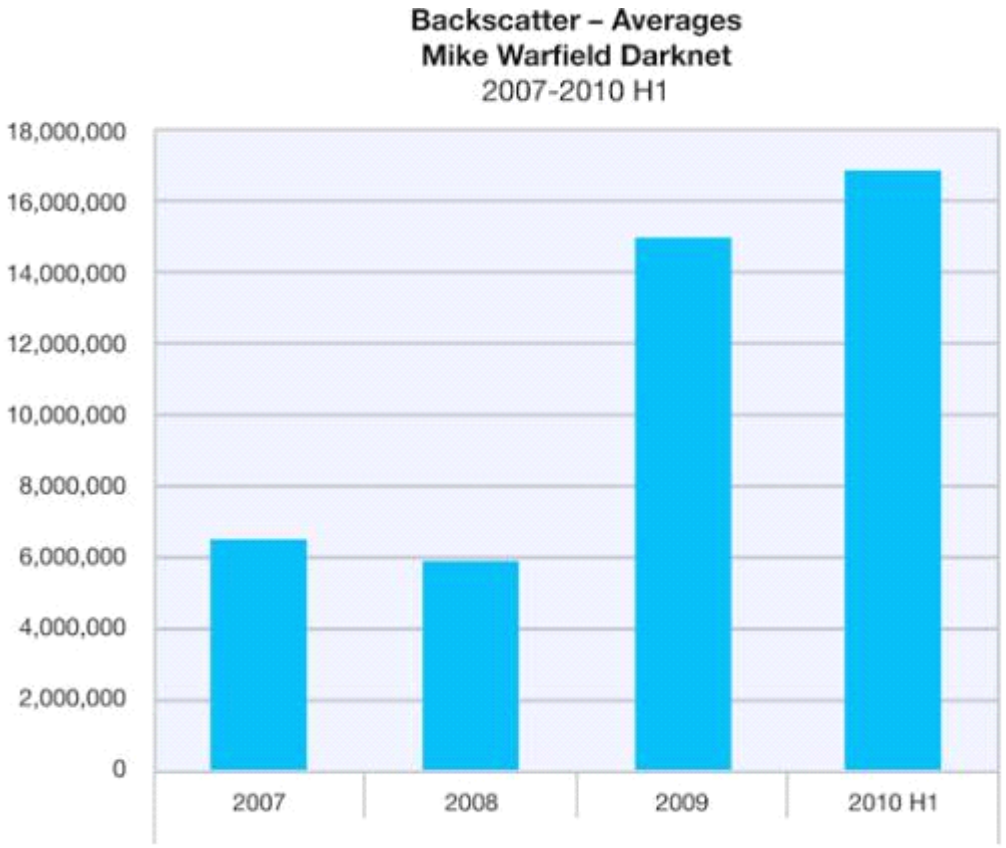


圖 12 : 2007-2010 上半年僞造退信 - 平均值 (Mike Warfield Darknet)

自 2007 年以來，僞造退信活動逐漸增加，但在 2008 到 2009 年之間的數量與同期相比，卻有著大幅度的躍進；部分原因是 2009 年出現了活動的高峰，這是三年半來活動量最大的一次。這種高於前一年平均的趨勢延續到 2010 年。第二季結束前，2010 上半年的平均計數略高於 2009 年的總平均。圖 12 其實是在回顧網際網路上欺騙式阻斷服務攻擊從 2007 到 2010 年增加的數量。

從僞造退信資料的逐漸增加（以及某些情況下，該活動的大幅躍升），我們可以推斷出什麼？由於大部分僞造退信資料是由 DoS 攻擊所造成，我們可以推斷：欺騙式 DoS 攻擊自 2007 年以來呈現穩定上升趨勢。然而，由於收集與發生的事物性質有很大差異，因此僞造退信會受某種高度可變因素的影響。某些僞造退信劇烈變動的時期起因於：不同攻擊者之間或攻擊者內部發生內訌。在衝突期間，一組人馬阻撓或接管另一組人馬的資源。交戰陣營彼此間的「隔空交火」可能導致僞造退信流量與僞造退信來源位址激增。這種衝突來得快，去得也快。2007 年 2

月和 2009 年 12 月出現驚人的高峰很有
可能是這類活動造成的結果（參見圖 **11**。）

暴力破解法

Mike Warfield 暗網也讓我們見識到暴力破解法的世界。從電腦安全的角度來看，暴力破解法是指：攻擊者在未經授權之下，試著以大量密碼組合來存取系統。經常被暴力破解法鎖定的某些服務爲：SSH（TCP 埠 22）、Telnet（TCP 埠 23）、RealVNC（TCP 埠 5900），以及 Microsoft 遠端桌面（TCP 埠 3389）。

圖 13 比較這些連接埠自 2008 年以來的平均活動。RealVNC 與 Microsoft 遠端桌面連接埠上的活動呈現緩慢上升趨勢；相比之下，SSH 則呈現慢而穩定的下降，而 Telnet 從 2009 年開始出現大幅度的滑落。

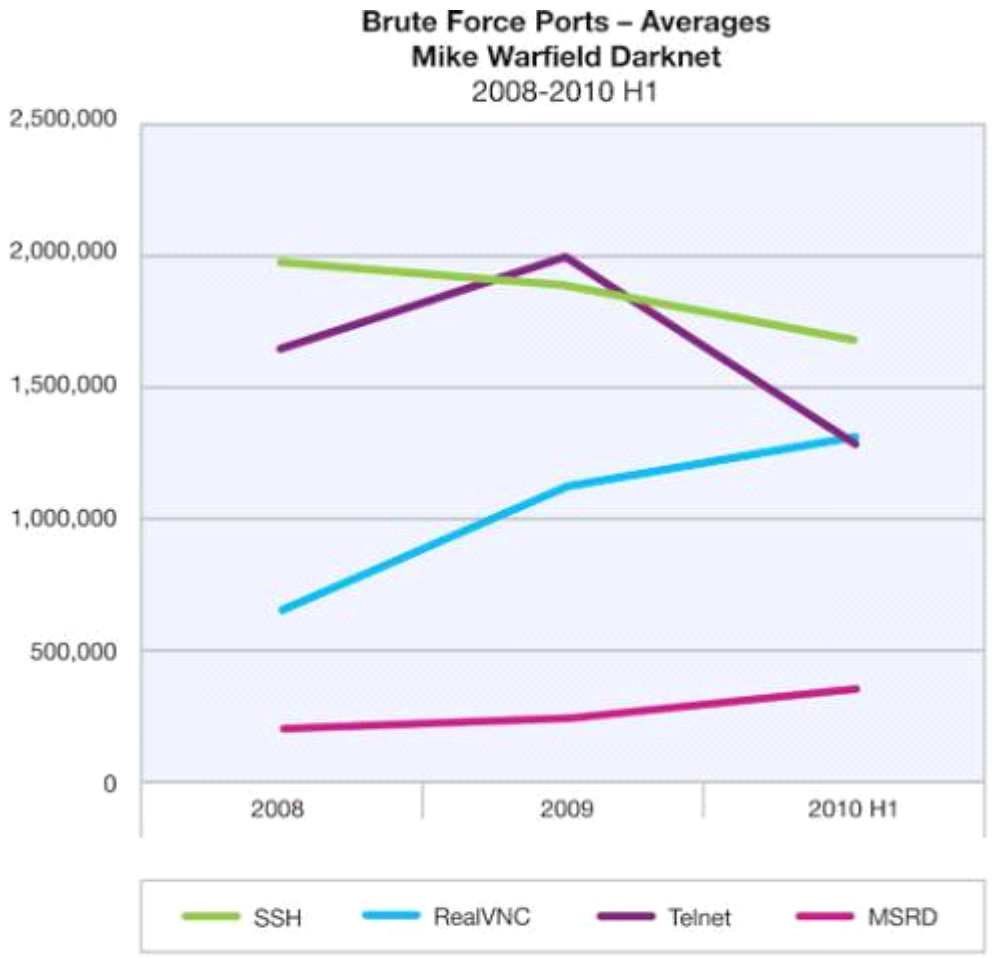


圖 13： 2008-2010 上半年的暴力破解連接埠 - 平均值 (Mike Warfield Darknet)

這些資料顯示：過去一年半以來，人們似乎對於鎖定 SSH 和 Telnet 連接埠的攻擊不太感興趣，而 RealVNC 與 MS 遠端桌面連接埠則是越來越受歡迎。這些通訊協定的漏洞所發佈的時間，是否與此趨勢互有關聯？圖 14 顯示：過去兩年半以來，這四個連接埠上暗網活動的總和。某些增加可能與漏洞揭露有關；舉例來說，今年 5 月初以 RealVNC 爲目標的漏洞，可能是它在第二季結束前出現小幅上升的原因。2008 年 5 月發佈了 6 個以 SSH 爲目標的漏洞；我們觀察到暗網圖表上該月份的活動也跟著大幅提升。SSH 活動在 2008 年 12 月呈現更大幅度的增長；以 FreeSSHd 爲目標的漏洞在該月被揭露。

然而，如果資料中所有高峰都用發生在同一時間的漏洞揭露來解釋，似乎也說不過去。事實上，上一個對 Telnet 造成影響的公開漏洞是在 2005 年 3 月被揭露。此外，某些活動雖然出現顯著成長（如 RealVNC 在 2009 年 8 月的高峰），但同一時間並沒有漏洞被揭露出來。這種跡象顯示：攻擊者並非總是利用最新的漏洞，他們往往需要依賴舊的漏洞來進行弱點攻擊。

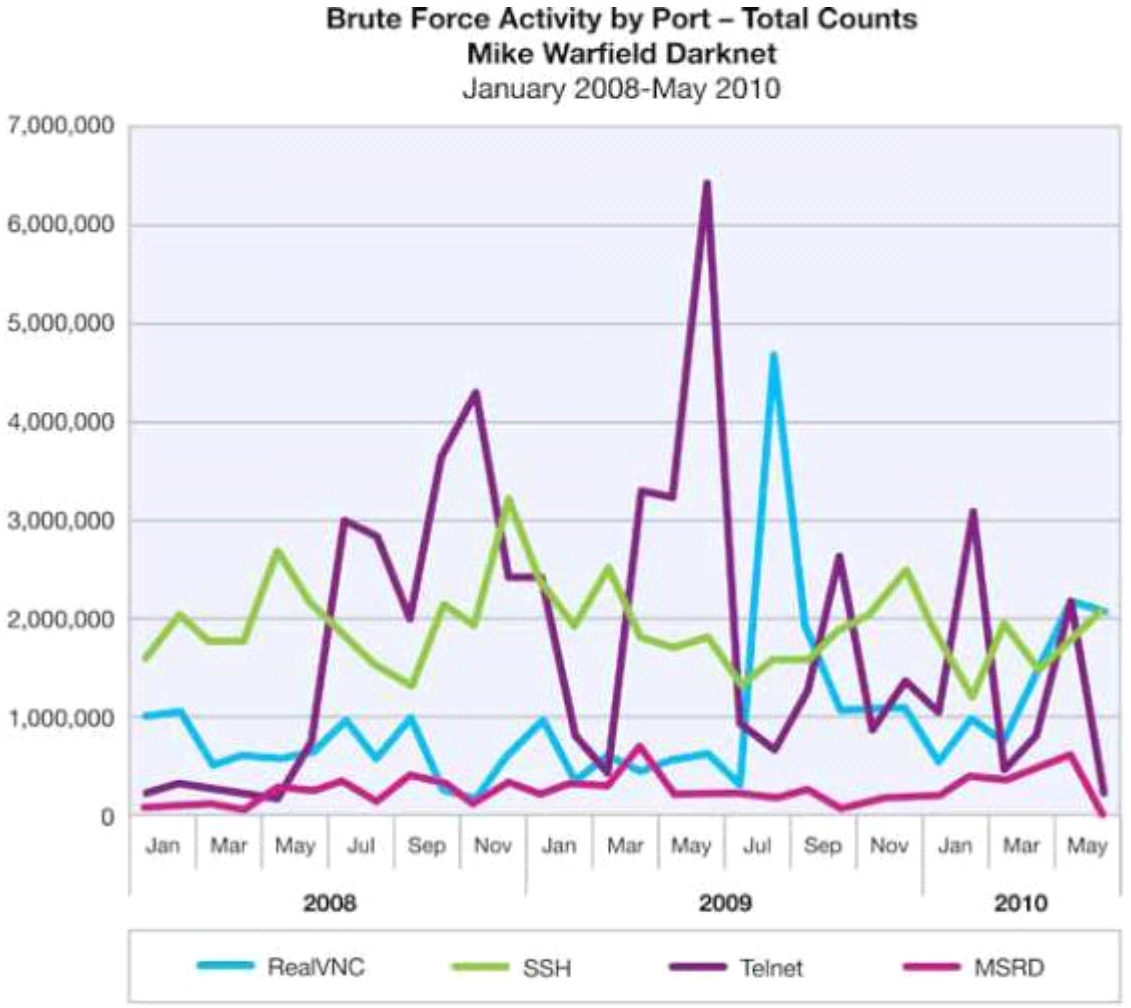


*圖 14：*2008 年 1 月至 2010 年 5 月的暴力破解活動 (以連接埠計算)- 總數 (Mike Warfield Darknet)

電腦犯罪 - 誰在騙誰？

Zeus 傀儡網路 - 真相、迷思並理解傀儡網路運作的方式

Zeus/Zbot 傀儡網路系列多年來不斷侵擾網際網路。威脅持續進化，新版本與新功能不斷出現。據媒體報導：Zeus 透過竊取個人資訊，已讓公司與個人損失了數百萬美元。

Zeus 傀儡網路操作員感染新 PC 的方式，通常是透過大量寄送惡意文件給受害者，或將受害者導向暗藏惡意內容的網站，以安裝 Zeus 機器人程式。安裝 Zeus 後，會監視感染的電腦網路流量，並將資訊回報給指揮控管 (C&C) 中心的伺服器。所收集到的資訊主要取決於操作員如何配置機器人程式，多數情況下，它會收集銀行帳戶資訊。即使 PC 上有安全與加密設定，Zeus 還是可以收集這些資訊，可以直接將程式碼植入 Web 瀏覽器以收集個人資訊。

收集受害者的資訊後，傀儡網路操作員可能會直接利用這些資訊，或出售給其他線上犯罪集團。

Zeus 的迷思

Zeus 以及其運作的方式存在許多迷思；某些經由大眾媒體散佈，甚至很大一部分都是科技知識 IT 媒體傳播出去的。很多時候，這些迷思和誤解是誤用術語所造成的，有些人認爲語義不是那麼重要，但 X-Force 深信：對惡意軟體做出嚴謹的定義，才能夠精確描述威脅。

只存在一個 Zeus 傀儡網路

這是錯的。線上出售的 Zeus Builder 工具箱允許任何人建立並管理自己的 Zeus 傀儡網路。數以百計、甚至數以千計的獨立 Zeus 傀儡網路一直都非常活躍。abuse.ch Swiss security blog 提供的服務 - Zeus Tracker (**https://zeustracker.abuse.ch/**)，負責監視活動中的 Zeus 指揮控管伺服器。我們正在製作這份文件時，總共有 644 個活動中的 Zeus C&C 伺服器正被追蹤，每個伺服器可能是由不同的群組或個人所操控。

Zeus 是病毒或蠕蟲

錯。病毒在傳統定義上指的是一種程式，透過某些使用者互動來傳播並感染機器，例如：插入軟碟或 USB 隨身碟、運行程式、打開電子郵件附件等等。蠕蟲與病毒類似，但不需使用者互動便可傳播，蠕蟲通常利用漏洞來做到這點。Zeus 並不符合上述這些定義。它沒辦法自行傳播，將它定義爲後門程式（提供對使用者電腦的存取權）或木馬程式（非字面上意義）會比較精確。當人們談到：「Zeus 正在蔓延。」可能會讓人以爲 Zeus 有能力自行傳播，但事實並非如此。

Zeus 利用漏洞與弱點自行安裝

這也是錯的。Zeus 本身就是後門或木馬程式。然而，許多使用 Zeus 竊取資訊的群組和個人會透過漏洞來傳送 Zeus。在此情況下，Zeus 是弱點攻擊所攜帶的內容，但本身與弱點攻擊無關。我們見到許多漏洞可用於傳送 Zeus，包括 PDF 弱點攻擊、各種 Web 型 ActiveX 控制項弱點攻擊等等。每當新的漏洞公開揭露時，就會有人用它來傳送 Zeus。這些漏洞與 Zeus 本身或 Zeus Builder 設計者無關，Zeus 本來就對竊取受害者的財務資訊，特別能夠發揮效用。

新版 Zeus 傀儡網路工具箱

Zeus 傀儡網路套件在 2010 年初發行更新版 Zeus 2.0。新版本的主要新功能有：支援從 Firefox Web 瀏覽器攔截個人資料；舊版 Zeus 只能從 Internet Explorer 攔截資料。

還有許多其他衍生自 Zeus 早期版本的變更。

Zeus 2 的變更

下面只列出 Zeus 2 其中一些變更。許多變更讓 Zeus 在企業環境中有效地感染機器，即便使用者不具備電腦管理權限。

自動啓動技術 - 若受感染的使用者具備管理者專用權時，舊版 Zeus 會利用 HKLM\Microsoft\WindowsNT\CurrentVersion\Winlogon 中的登錄機碼，自行安裝「於系統啓動時自動運行」的功能；如果使用者不具備管理者專用權，則安裝在 HKCU\Microsoft\Windows\CurrentVersion\Run。將它移除十分困難，因爲 Zeus 機器人程式會持續監控該機碼並防止任何修改。即使在安全模式下啓動 Windows，只要有用到 Winlogon 機碼，Zeus 還是會載入。新版 Zeus 中不論使用者專用權層次爲何，都使用 HKCU\Software\Microsoft\Windows\CurrentVersion\Run，讓 Zeus 自動啓動；從登錄表偵測並清除此項目變得更容易。這也使 Zeus 只能在最初感染的使用者帳戶上運行。

檔案位置 - 如果使用者具備管理員權限，舊版 Zeus 在未修改的情況下，會將自身的副本放到 Windows\System32 目錄；如果沒有管理員權限，則放在使用者的 Application Data 目錄。文件通常會命名爲 sdra64.exe。新版 Zeus 會將自身副本隨機命名，並放在使用者 Application Settings 目錄中一個隨機命名的子目錄。

網路流量 - 用來與指揮控管 (C&C) 伺服器通訊的通訊協定，基本上與網路上的通訊協定相同。HTTP POST 資料會以 RC4 加密。Zeus HTTP 要求比較明顯的變更是：目前在 HTTP 要求標頭中使用的是「Cache-control:no-cache」指令，而非早期 HTTP-1.0 樣式所包含的「Pragma: no-cache」標頭。

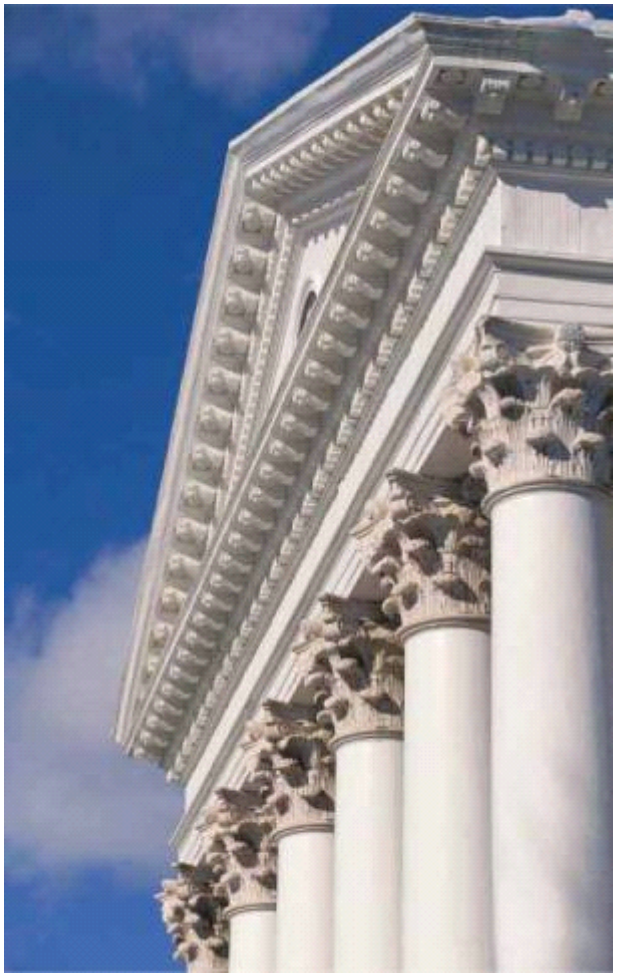
獨特的感染二進位檔 - Zeus 混入使用者的 Application Settings 目錄時，會對本身副本做少量隨機修改。這意味著：如果將一個 Zeus 安裝程式發送給許多人，感染時會出現略微不同的執行檔；只有一小部分的位元組會改變，但已足夠讓檔案產生不同的 SHA 或 MD5 雜湊。其檔案大小也不盡相同。

綁定機器的二進位檔 - 現在 Zeus 使用的技術類似商業軟體複製保護，使分析安裝的執行檔變得更爲困難。一旦機器受到感染，原始的執行檔會被刪除，而儲存於磁碟上的檔案，無法在另一台電腦上運行。藉由檢查開機磁碟的容量 GUID 和執行檔所儲存的目錄，便能做到這點。若該資訊不符合儲存於 EXE 本身的內容，Zeus 便無法運行。這意味著：常見的自動分析技術將無法發揮功用。

配置檔位置 - Zeus 1.3 及先前版本的配置檔是從伺服器下載，並儲存成「local.ds」，放在 Windows\System32 下的隱藏目錄裡（如果使用者不具備管理員權限，則改在 Application Data 目錄）。現在 Zeus 下載配置檔時，會以隨機名稱儲存在使用者的 Application Settings 目錄下。因爲檔案爲隨機名稱，所以比舊版的固定命名更難偵測。

作業系統支援 - Zeus 2.0 現在可運行於 Vista 與 Windows 7。舊版本試圖運行時就會當掉，不過新版本能成功在最新的 Microsoft 桌面作業系統上運行。Zeus 2.0 還能成功在上述作業系統的 64 位元版本上運行。

最初感染媒介 - Zeus 新舊版本的散佈方式並無太大區別，方法是抓住一切有利時機 - 每當新漏洞出現，網路罪犯會試圖用來製造新感染，以擴大現有的 Zeus 傀儡網路。由於 Zeus 在地下論壇是以傀儡網路建立套件進行兜售，並由許多不同的群組與個人使用，每個人可以用不同的方法進行散佈。今年我們看到的方法包括：電子郵件附帶的 .zip 檔案暗藏 Zeus 機器人程式；電子郵件中的鏈結連到 .zip 或 .exe 檔案；電子郵件中的鏈結連到藏有弱點攻擊套件的網站並會安裝 Zeus；利用 /Launch 弱點與其他漏洞的 .pdf 附件。這並非完整的清單，人們會不斷創造新方法，盡量讓惡意軟體（包括 Zeus）安裝在更多的機器上以獲取金錢利益。



保護自己不受 Zeus 侵擾

保護自己不受 Zeus 侵擾並沒有特效藥；安全上網習慣可保護電腦使用者不受任何惡意軟體的感染。

PC 安全

- 以非管理員使用者運行電腦。雖然 Zeus 還是有可能感染您的 PC，但這能將傷害減到最小、感染也更容易清除。
- 隨時更新電腦上的最新修補程式。藉此限制能在 PC 上運行的惡意軟體數量，並限制可用的攻擊媒介。特別注意定期更新您的作業系統、辦公室軟體、文件軟體，以及 Web 瀏覽器與外掛程式。
- 安裝防毒軟體並隨時保持更新。雖然防毒軟體無法預防所有惡意軟體的威脅，但還是能提供不少幫助。

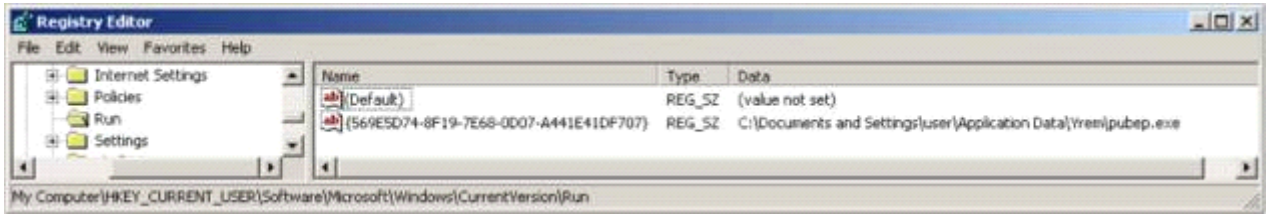
電子郵件與傳訊安全

- 留意電子郵件的附件。如果附件是來自您認識的人，務必確認他們就是原始寄件者。檢查電子郵件是否從他們常用的電子郵件位址寄出。
- 也要留意電子郵件中的鏈結。許多釣魚攻擊使用貌似合法的電子郵件，但其中暗藏連到惡意網站的鏈結。若您從銀行收到一封電子郵件，請使用瀏覽器書籤直接進入銀行的網站登入。此建議也可以用在即時通訊服務或社交網站上所收到的訊息。

感染跡象

懷疑感染 Zeus 時，可觀察幾個跡象以確認：

HKCU\Software\Microsoft\Windows\CurrentVersion\Run 登錄機碼中某個項目會出現 GUID 格式的名稱，並指向使用者的 Application Data 目錄中的檔案。下面的範例可讓您了解大概是什麼樣子：



有人嘗試刪除登錄機碼時，它會不斷地復原；機碼若被刪除也會立即回復。您可以用 Microsoft 程序監視器確定此行為。在此範例中，Explorer.exe 程序不斷重新寫入登錄值：

重新啓動電腦進入安全模式，刪除兩個登錄項目與 EXE 檔便可移除 Zeus，但我們仍建議重新安裝已遭惡意軟體破壞的機器或重新製作映像。我們無法預料是否有其他惡意軟體潛伏在電腦中，移除 Zeus 只能消除一部分已安裝的惡意軟體之生態系統。

BlackHat 搜尋引擎下毒

BlackHat 搜尋引擎下毒這種技術最初被垃圾郵件發送者使用，目的是讓他們的搜尋結果出現在搜尋引擎頂部，藉此獲得廣告收入。近來，其他網路罪犯不斷利用這些技術擴大惡意軟體的感染。他們往往利用重大新聞事件，讓惡意鏈結出現在眾多搜尋引擎的搜尋結果頁頂部。

爲了完成這項任務，網路罪犯會監測搜尋引擎和社交網站的趨勢話題。若某個新話題迅速延燒時（例如重大新聞事件），攻擊者會使用標準 SEO（搜尋引擎最佳化）技術，讓他們連到那些搜尋結果的鏈結，出現在搜尋引擎的頂部。因爲此程序基本上是自動的，所以有時在重大事件的真實新聞大量公布前，這些惡意鏈結就會搶先出現在搜尋引擎結果的頂部。

惡意鏈結本身通常會隱藏在數個循環的混碼中。許多時候這些鏈結會連到標題含有搜尋詞彙的 PHP 網頁（這是 SEO 技術之一），而生成頁面的程式碼會檢查 HTTP 參照位址，以確保其來自有效的搜尋引擎。這麼做是爲了阻礙 Web 搜索器與惡意軟體分析師。一旦證實 Web 瀏覽器來自搜尋引擎，就會使用其他重新導向技術。可能有 JavaScript 混碼、內嵌的 Adobe Flash 檔案，甚至是在 PDF 文件中暗藏連到其他頁面的鏈結。這麼做是爲了讓鏈結難以透過自動化工具追蹤（例如許多防毒公司使用的惡意搜索器）。在多達五層（或更多）的重新導向後，使用者的瀏覽器最終到達某個暗藏弱點攻擊工具箱的頁面；它會先檢查瀏覽器版本和可用的外掛程式，然後傳送惡意內容。而其他時候，網頁會出現一則假警告，通知使用者電腦上發現假病毒，並請求安裝詐騙軟體（如假冒的防毒產品）。

爲了保護自己免受威脅，網站瀏覽者應留意搜尋結果中點選的鏈結。若您正在尋找某樣東西，卻不小心連到假冒防毒軟體的頁面，請勿安裝此軟體；如果鏈結的網域名稱與您要尋找的東西完全無關，請勿點選鏈結。我們看過許多合法網站被駭客入侵，然後被用來從事 BlackHat SEO 的活動。

假冒的防毒軟體

假冒的防毒軟體、僞防毒軟體與詐騙軟體。這些不同名稱指的都是同樣的軟體，雖然號稱是防毒解決方案，實際上卻什麼也不做。這些產品會假裝掃描您的硬碟、假裝發現惡意軟體，他們會詢問您的信用卡資訊，要求您支付 60 美元以上以刪除發現到的病毒。當然一旦您付了錢，唯一會發生的事就是讓假冒的防毒軟體停止回報假病毒。

假冒的防毒軟體已存在好幾年。2009 和 2010 年的最新消息是：他們正在利用 BlackHat SEO 技術進行散佈。在網路上搜尋任何東西、點選鏈結，最後在頁面上通知有病毒正感染您的電腦 - 使用者很容易落入這個陷阱。

如果您選擇下載並執行該軟體，電腦會變得無法使用的，每隔幾秒鐘，另一個關於假病毒的假警告又會出現，彈出式氣泡框會出現在您的任務欄。在您刪除假冒的防毒軟體或支付費用之前皆無法瀏覽網頁。

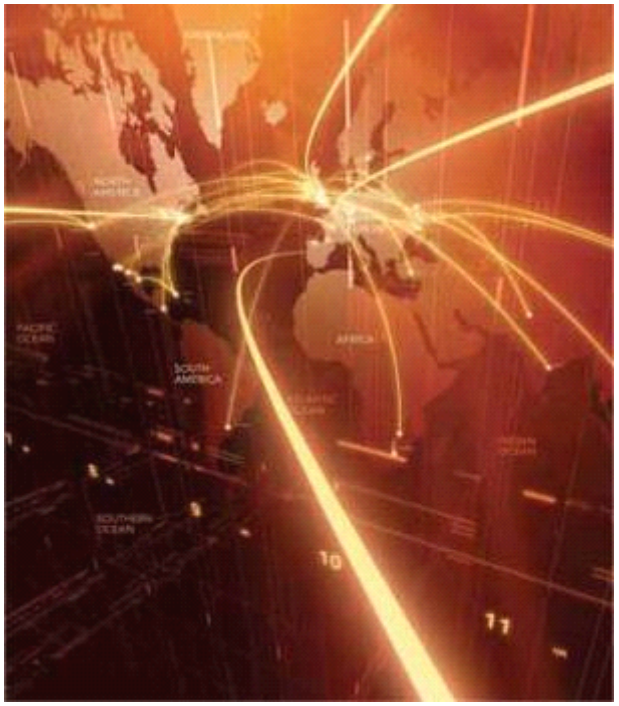
垃圾郵件 - 網際網路上的模仿藝人

垃圾郵件發送者的網域從 .cn 移到 .ru

下表顯示每月垃圾郵件最常用的最上層網域前五名。下表中，我們只考慮實際管理垃圾郵件內容的 URL。

排名	2010 年 1 月	2010 年 2 月	2010 年 3 月	2010 年 4 月	2010 年 5 月	2010 年 6 月
1.	com	ru（俄羅斯）	ru（俄羅斯）	com	ru（俄羅斯）	ru（俄羅斯）
2.	cn（中國）	com	com	ru（俄羅斯）	com	com
3.	net	net	net	net	de（德國）	de（德國）
4.	ru（俄羅斯）	cn（中國）	cn（中國）	de（德國）	net	net
5.	info	info	biz	cn（中國）	org	org

表 4： 2010 上半年包含真正垃圾郵件內容的常見最上層網域



或許令人驚訝的問題是：中國 **(.cn)** 發生了什麼事？剛開始在 1 月時排名第二，之後就逐月下滑。2010 年 6 月，中國排名第 75。回顧前幾年的資料，這更加令人困惑。

過去幾年中，中國網域 (**.cn**)，一直是垃圾郵件發送者的最愛網域。然而，中國自 2009 年 12 月中開始限制註冊 **.cn** 網域的規則（請參見 **http://www.cnnic.net.cn/html/Dir/2009/12/12/5750.htm**），這似乎阻礙到垃圾郵件發送者，迫使他們轉往新的地方。在中國 NIC（網路資訊中心）關閉大門之前，垃圾郵件發送者還在繼續使用已註冊的網域池 (pool)。六週後池子顯然已被清空。之後，活動便從中國移到俄羅斯。下列圖表顯示過去 18 個月內，垃圾郵件發送者每月使用的最上層網域 (TLD)。

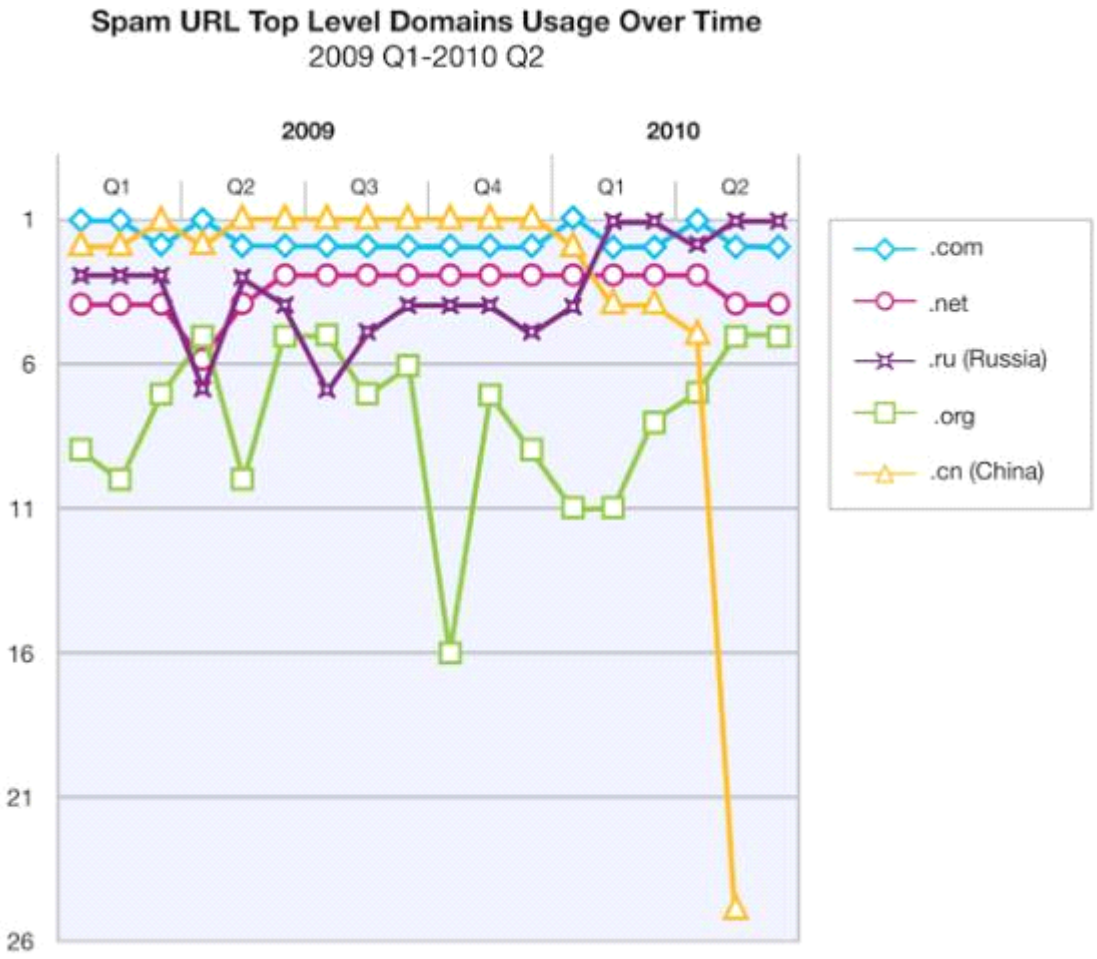
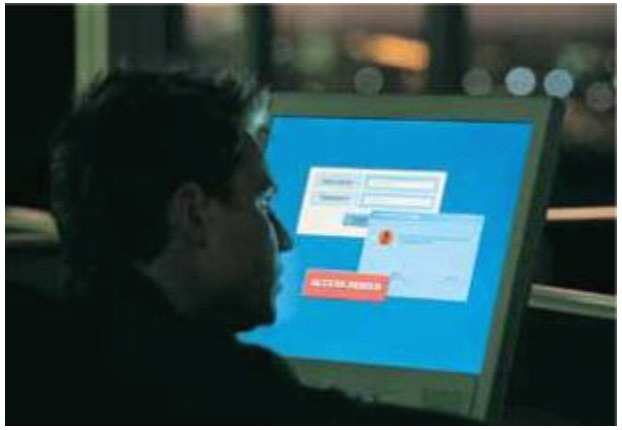


*圖 15：*2009 年第 1 季到 2010 年第 2 季垃圾郵件 URL 最上層網域的用量變化

2010 年 4 月 1 日，俄國 NIC 同樣也限制註冊新網域的規則（詳情請參見 **http://www.nic.ru/dns/service/en/faq_identification.html#q9**）。然而，垃圾郵件發送者還是選擇 **.ru** 網域來提供他們的服務。2010 年 6 月，**.ru** 仍然是最常用的垃圾郵件最上層網域。不妨拭目以待這種現象還會持續多久。但接下來呢？垃圾郵件發送者是否會選擇其他容易註冊網域的國家？或者是否會把焦點放在透過 Web 管理服務提供惡意軟體，而不必像其他垃圾郵件發送者一樣註冊自己的網域？



我們可以做些什麼以改善這類網域註冊？

防止以管理垃圾郵件內容爲目的而大量註冊網域的好方法：要求公司提供註冊證明，或要求個人提供身分文件證明（包括文件檢查）。這樣就能找出是誰在利用網域發送垃圾郵件。中國自 2009 年 12 月起已要求提供這類證明，而且獲得不錯的成效。俄國也有類似的新規定（4 月 1 日起生效），但迄今似乎並未強制執行。

註冊是法律上的問題，每個國家的處理方式都不同。爲垃圾郵件發送者敞開大門的寬鬆註冊程序可能無法完全避免。此外，註冊網域只是其中一個管理垃圾郵件內容的方法，另一種方式是：利用影像或其他內容的主機服務提供者，包括 Google (**googlegroups.com**) 或 Microsoft (**livefilestore.com**) 這類大廠。請參見 **URL 垃圾郵件常見網域**的部分。

頻寬無關緊要：垃圾郵件的位元組大小大幅增加

2007 年底的垃圾郵件平均位元組大小變化最大，同時影像垃圾郵件的數量滑落。2008 年，位元組大小開始微幅增加，直到該年下半年關閉 McColo 爲止。隨著影像垃圾郵件在 2009 年夏季復甦，一年半內的平均大小首度超過 5 KB。2009 年第四季下降到 4 KB 以下。下列圖表將垃圾郵件的平均位元組大小與影像垃圾郵件的百分比做比較（統計到 2009 年年底）。

關閉 McColo

2008 年 11 月關閉加州的網路託管公司 McColo 之後，垃圾郵件量滑落至先前水準的 25 % 左右。關閉之後的巨幅極端數量變化，以及國家分佈的改變，顯示 McColo 是全球垃圾郵件機器人的運營基地。更多關閉 McColo 以及後續發展的資訊，請參見 IBM Security 2008 與 2009 年 X-Force 趨勢與風險報告。

*圖 16：*比較垃圾郵件的平均位元組大小與影像垃圾郵件的百分比（2006 年第 3 季到 2009 年第 4 季）

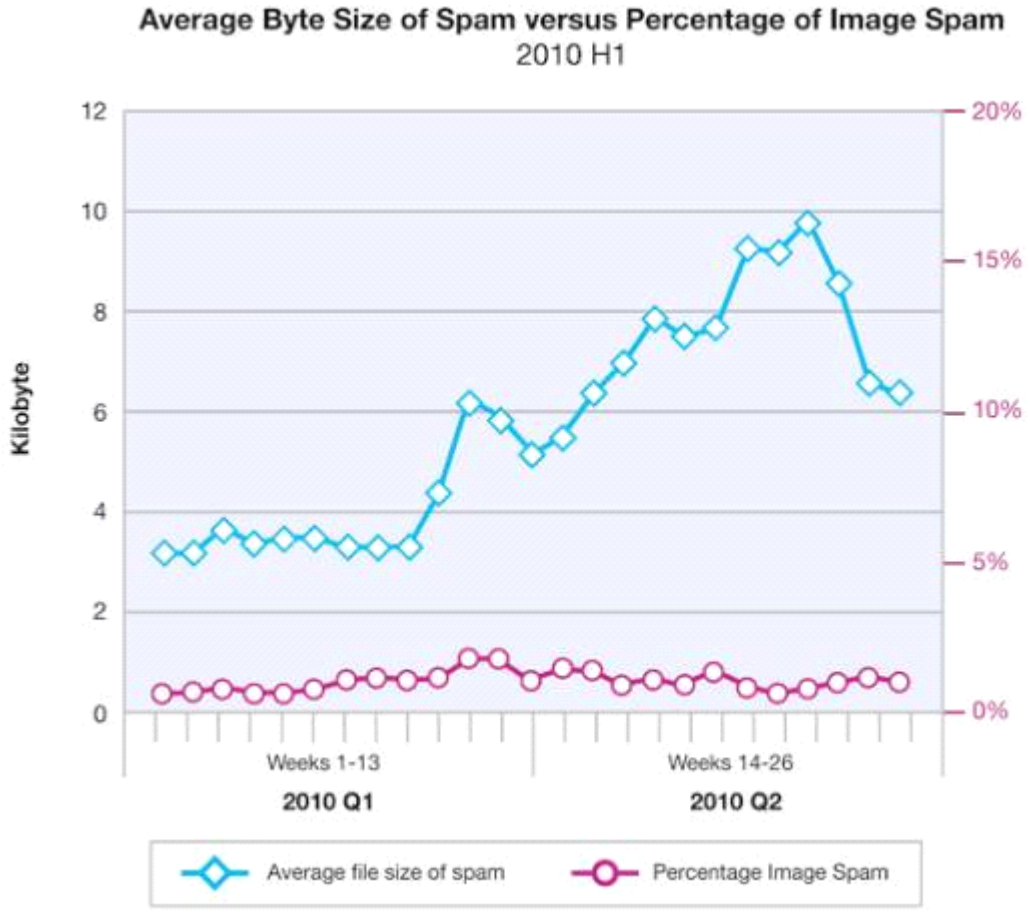


*圖 17：*比較垃圾郵件的平均位元組大小與影像垃圾郵件的百分比（2010 上半年）

兩條曲線呈現並列的走向，但 3 月中之後發生重大變化。短短數天，垃圾郵件平均大小增了一倍，不過影像垃圾郵件的百分比沒有任何變化。接下來幾星期內，平均位元組大小持續增加；到 6 月初爲止，平均大小達到 10 KB。6 月期間，大小下降至約 6.5 KB，但與最初隨機文字垃圾郵件的攻擊數量相比，還是增加兩倍以上。影像垃圾郵件的百分比在整段時期維持不變。

查看垃圾郵件時，可發現隨機從網際網路選取的大量文字片段。隨機文字是早期垃圾郵件發送者，爲了讓垃圾郵件看起來更合法而使用的技術，這對文字型垃圾郵件分析模組特別有用。然而，最近的反垃圾郵件技術已解決了這個問題。那麼垃圾郵件發送者爲何故技重施？也許他們希望大量隨機文字可混淆 Bayesian 分類器。尤其是具備智慧學習功能的 Bayesian 分類器比較適應非商業環境，所以這些垃圾郵件的攻擊，可能是以非商業使用者爲目標。

您可以在「當前趨勢」的部分，閱讀更多關於垃圾郵件的報導與技術。

網路釣魚 - 您是否上當？

2009 年，金融機構無疑是網路釣魚電子郵件的頭號目標。60% 以上的網路釣魚電子郵件，就是以這些機構爲目標。2010 上半年，以金融機構爲目標的釣魚郵件佔 49.1%，信用卡佔 27.9%、政府組織佔 11.2%、線上付款機構佔 5.5%、拍賣則佔 4.6%。剩下 1.7 % 網路釣魚目標包含其他產業，例如通訊服務與線上商店。

網路釣魚技術的新焦點

根據第 71 頁「**Web 應用程式威脅與漏洞**」所描述的百分比，每年的目標分佈呈現大幅變動；另外根據第 94 頁「**URL 垃圾郵件常見網域**」所述，攻擊者逐漸將目標轉移到利用受信任網站的好名聲，讓使用者卸下心房，並隱藏攻擊以躲過保護技術。

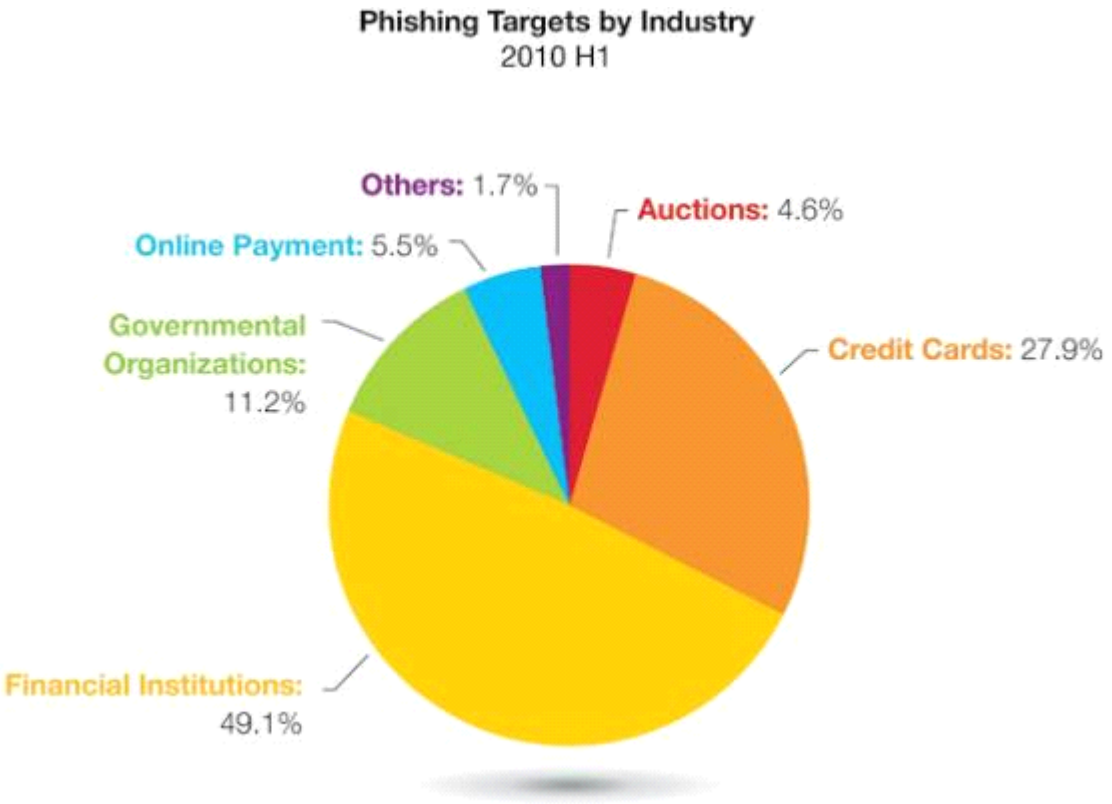


*圖 18：*2010 上半年各產業的網路釣魚目標

過去 18 個月內，網路釣魚電子郵件將金融機構當成主要目標。2009 上半年，網路釣魚電子郵件中很大一部分是以線上付款爲目標。然而，該年下半年可見到更多釣魚郵件是以政府機構（主要是美國稅務相關網站）、信用卡及拍賣爲目標。同時，以線上付款組織爲目標的網路釣魚電子郵件，其百分比呈現下降趨勢。2010 年第 1 季，金融機構及信用卡的比率再次下降，拍賣則呈現上揚。進入 2010 年第 2 季後，可見到各產業呈現衰退的趨勢，網釣客再次聚焦於金融機構及信用卡，現在加起來佔了所有網路釣魚電子郵件的 96%。

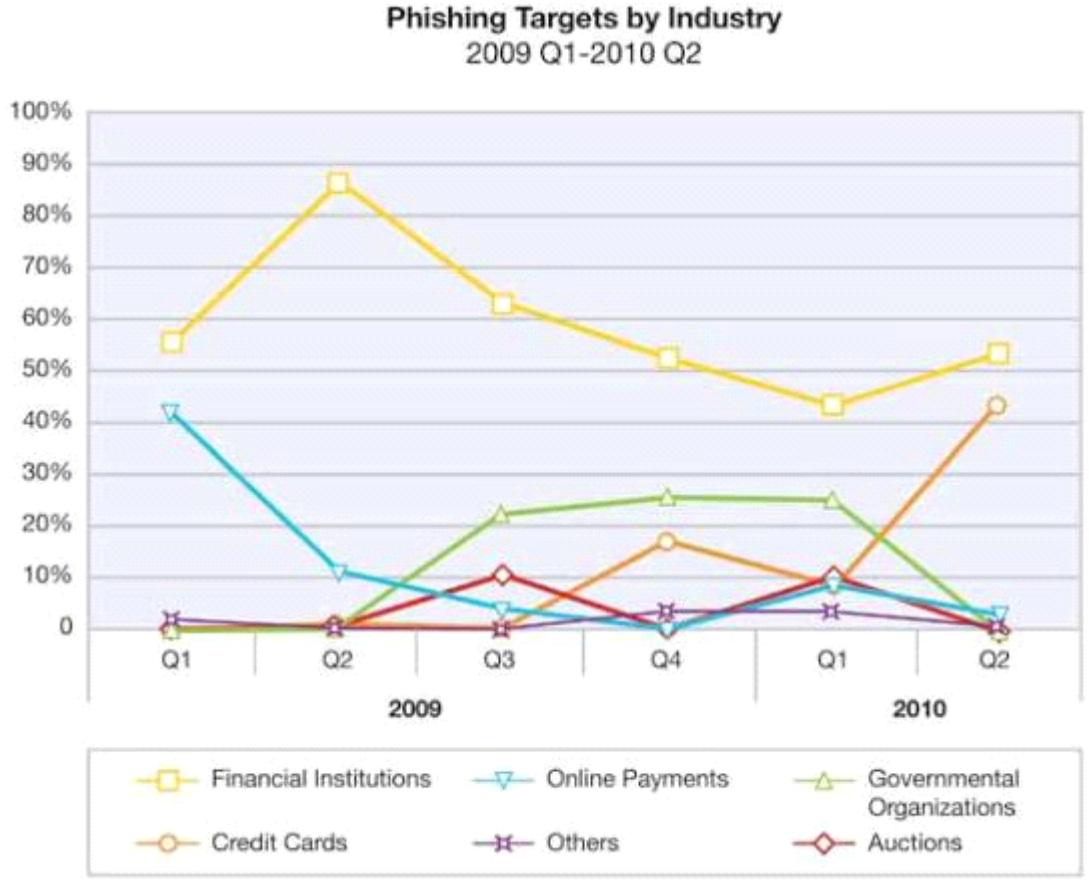


圖 19： 2009 年第 1 季至 2010 年第 2 季各產業的網路釣魚目標

網釣客爲何會停止鎖定政府機構（此處專指美國稅務相關網站），而把矛頭轉向銀行及信用卡？原因之一可能是：以稅務相關網站爲目標經過 9 個月的時間，利益逐漸下滑，網釣客現在開始把矛頭轉向傳統且行之有效的目標 - 信用卡與銀行。

以美國銀行爲目標的金融網路釣魚

由於金融機構仍然是網釣客攻擊的重點，值得進一步觀察他們主要活動的地理分佈位置。2010 上半年，超過三分之二的金融網路釣魚目標皆位於北美洲。剩下的 32% 位於歐洲。

*圖 20：*2010 上半年金融網路釣魚目標的地理分佈

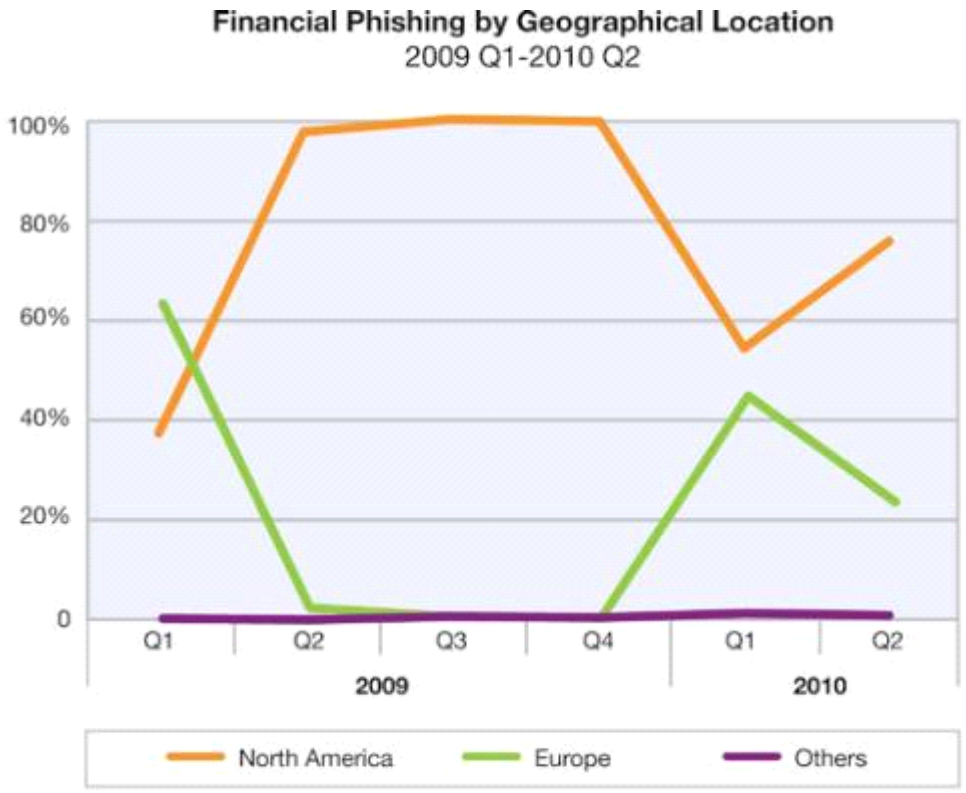


*圖 21：*2009 年第 1 季至 2010 年第 2 季金融網路釣魚目標的地理分佈

然而，若以更短的時間範圍進一步分析，便可明顯看出更多變化。下列圖表顯示：2009 和 2010 上半年地理分佈的轉移。雖然 2009 年後三季比率最高的是以美國銀行爲目標的金融網路釣魚郵件（佔了 95% 以上），但 2010 年第一季有將近 45% 的金融網路釣魚郵件是以歐洲爲目標。到了第二季，歐洲下滑至 24%。爲什麼金融網釣客在 2010 年第一季轉向歐洲，然後又轉回美國？第一季，從金融危機中復甦的歐洲變成顯著的目標；而第二季，希臘與其他一些歐洲國家的預算危機，引發了整個歐洲的金融危機。

在本報告之後的章節，我們將繼續討論最新的網路釣魚趨勢。

2010 年及未來的新主題

IPv6 部署 - IPv4 位址即將用盡；我們準備好了嗎？

舊世代的網際網路 IPv4，不論是位址或路由表，都以爆炸性的速度持續成長。目前位址激增，已逼近可用的極限，預計會在 2011 年某個時間點用盡網際網路號碼分配局 (IANA) 所分配的位址，之後區域網際網路註冊管理機構 (RIR) 的也會用完。不過位址發展到最後，並不會立即終止，而是會慢慢流入黑市或被當成商品交易。回收未使用的空間也不是辦法，因爲路由分割造成路由表以爆炸性的速度成長，逼近路由器容量的上限。位址恢復和重新分配只會加劇路由表的壅塞，無法明顯紓緩位址耗盡的問題。目前路由器已經擠得水洩不通。

這些 2007 年 1 月至 2010 年 5 月 IPv4 與 IPv6 BGP 公告資料來自亞太網路資訊中心 (APNIC)，由 CIDR-Report 專案 **www.cider-report.org** 的自訂圖形產生器所生成。這份報告中，APNIC 收集了自 2003 年以來的 IPv6 統計資料，以及自 1998 年以來的 IPv4 統計資料。

IPv6 擴充與部署

新一代網際網路 IPv6 已存在多年，不但在歐洲、亞洲持續擴張，在美國與其他地方也是如此。多年前，可透過 IPv6 網路進行路由傳送的數量，超過了可透過 IPv4 位址進行路由傳送的數量，但會帶來些許路由表負載。2009 年可見到政府與國防進一步部署 IPv6。IPv6 目前的容量足以應付好幾倍的舊 IPv4 網際網路，不存在逼近極限的問題。

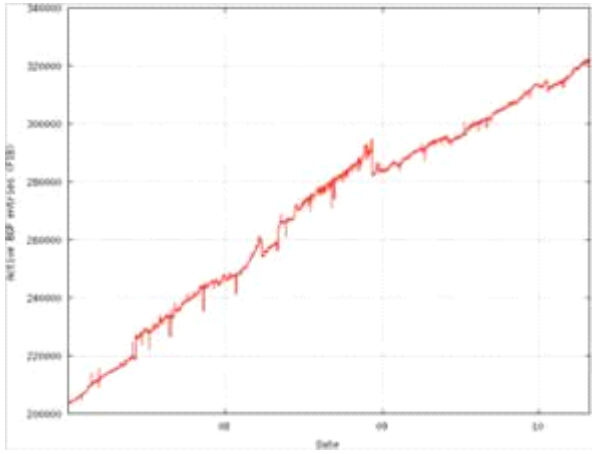


*圖 22：*2007 年 1 月至 2010 年 5 月 IPv4 BGP 公告。資料來源：亞太網路資訊中心/CIDR-Report 專案

下列兩張圖 - 左邊 IPv4 與右邊 IPv6 的顯示：核心網際網路路由器中，透過邊界閘道通訊協定 (BGP) 公告路由的數量。這些資料證實每種通訊協定的路由數量會繼續擴大。

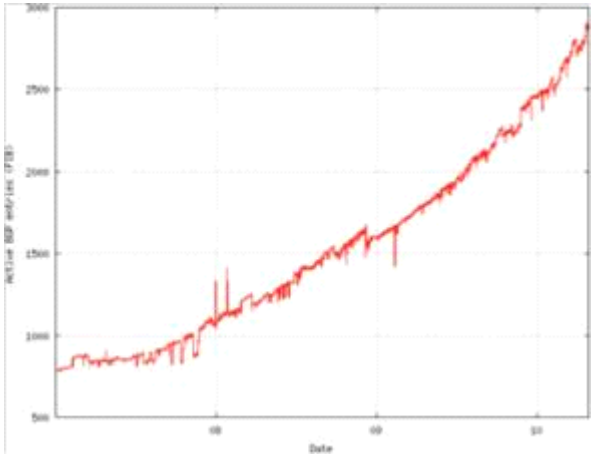


*圖 23：*2007 年 1 月至 2010 年 5 月 IPv6 BGP 公告。資料來源：亞太網路資訊中心/CIDR-Report 專案

然而，觀察縱軸的標示，目前核心網際網路中有超過 30 萬個公告的 IPv4 路由，而公告的 IPv6 路由則低於 3000。只需低於百分之一的路由數量，這些公告便能發送 IPv6 中完整 /48 網路位址（約等於單一 IPv4 主機位址的數量）。每個公告的 IPv4 位址只需以路由器中低於百分之一的路由數量爲代價，便可享有整個龐大的 IPv6 網路。由於每個 IPv6 網路容量不同，即使將 IPv4 位址數量與單一 /48 IPv6 網路做比較也毫無意義。IPv4 路由數量的擴展似乎已趨緩；而 IPv6 路由與網路公告的數量似乎正在增加。

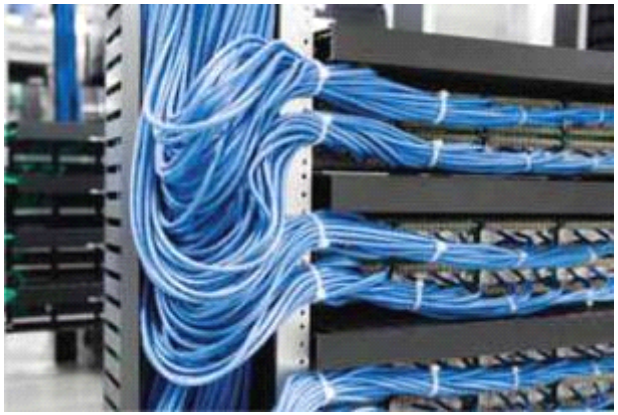
所有最新作業系統皆支援 IPv6，而且大多數網路中已存在 IPv6 的流量，尤其是當前的 Windows Vista、Windows 7、Mac OS/X，以及 Linux 都有支援。不幸的是，人們仍舊忽略 IPv6，認爲它是未來的產物。不知不覺中，大多數網路已預設部署了 IPv6。從去年起，Vista 與 Windows 7 加快此趨勢，而且這個趨勢應該還會繼續下去。未意識到此趨勢，或者刻意忽視此趨勢的操作員都有可能受到威脅，因爲 IPv6 已廣泛部署於整個基礎架構中。

有線電視與寬頻供應商 Comcast 多年來一直使用 IPv6 管理內部裝置，目前已耗盡管理裝置的 10.*.*.* 私有位址空間。他們現已開放一個測試版測試程式，將 IPv6 提供給他們的使用者與客戶。Comcast 也使用 IPv6 Adoption Monitor 追蹤 IPv6 的部署。更多詳細資訊，請造訪下列鏈結：
http://ipv6monitor.comcast.net/

Hurricane Electric 是一間相當受歡迎的 ISP，範圍涵蓋歐洲、亞洲與澳洲，他們提供一系列 IPv6 工具與設備，以及免費的通道代理人 (Tunnel Broker) 服務：**www.tunnelbroker.net**，可提供免費的 IPv6 連線能力。該網站上有一個「末日鐘」，倒數離 IPv4 位址空間耗盡還剩下多少天（也有許多其他的 IPv4 與 IPv6 統計資料）。他們也爲個人與組織提供免費的「認證」，可訓練、測試自己對 IPv6 知識與網路了解多少。

許多著名網站，如 Google 和 YouTube 已完全啓用 IPv6。Google 最近報導：美國在部署 IPv6 方面位居世界第五，這主要是因爲 Apple Mac 與無線存取點已經啓用 IPv6，而且會自動透過已建立的自動轉換通道進行連線。若原生 IPv6 無法使用時，Windows Vista 和 Windows 7 會自動連接到 Teredo 轉換機制。雖然用戶端系統以 IPv6 爲主（在可用的狀態下）的比例還是很小，但目前數量正不斷地擴增中。

種種跡象顯示 IPv6 在未來幾年會不斷擴大，而且這種趨勢不會變慢。前些時間，IPv6 被稱爲「新一代」IP 通訊協定。現在，如果說 IPv6 是「當代」IP 通訊協定而 IPv4 正逐漸「走入歷史」，這也不無道理。



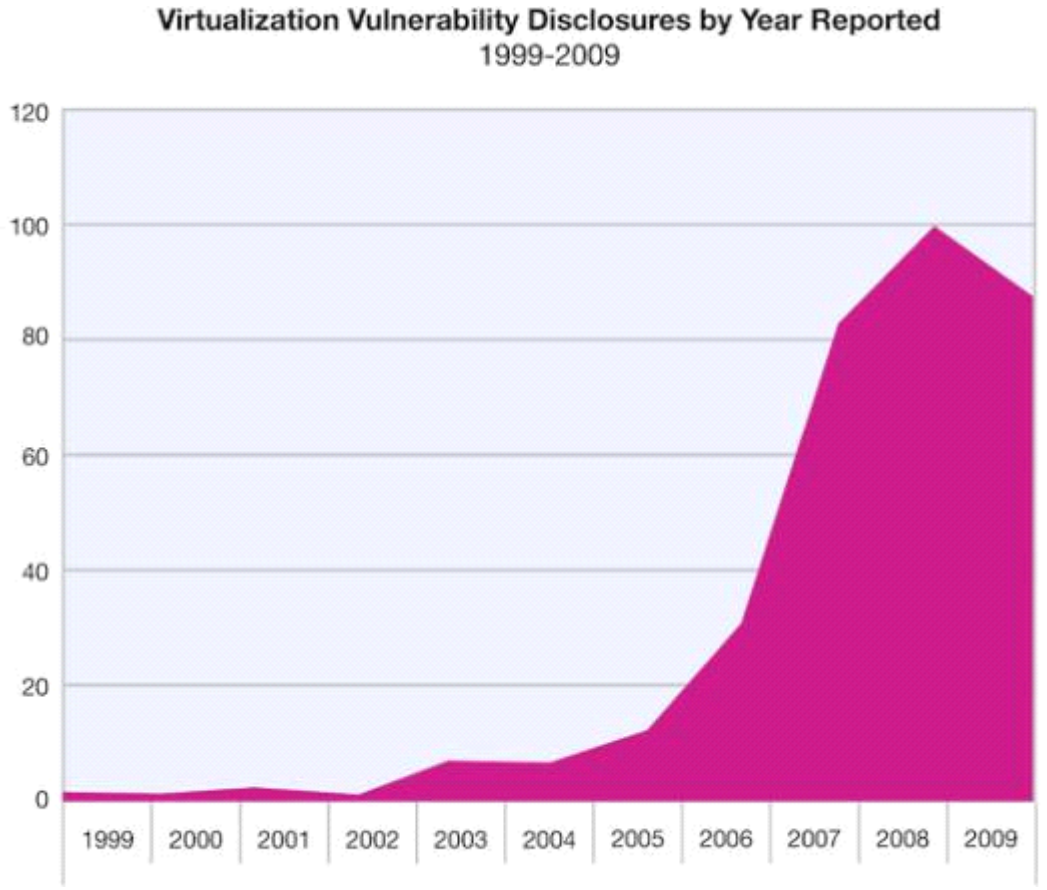
虛擬化 - 與虛擬空間整合，這對安全而言代表何種意義

虛擬化技術日益受到重視。根據最新 IDC 新聞稿[1]，2009 年第四季所有新出貨的伺服器中，18.2% 都是虛擬化伺服器，與 2008 年第四季出貨量的 15.2% 比起來，增加了 20%。虛擬化市場規模在 2009 年爲 152 億美元。雲端運算日益受到關注，也刺激了虛擬化解決方案的需求。因此，了解虛擬化技術的安全隱憂變得越來越重要。本節針對下列供應商所提供的虛擬化產品，介紹過去十年來漏洞揭露的分析：

- Citrix
- IBM
- Linux VServer
- LxCenter
- Microsoft
- Oracle
- Parallels
- RedHat
- VMware

虛擬化漏洞揭露趨勢

1999 至 2009 年底，揭露 373 個影響虛擬化解決方案的漏洞。虛擬化漏洞揭露數的趨勢如圖 24 所示。這些揭露只佔所有揭露的一小部分，而且只在 2007 至 2009 年之間超過 1% 的水平。



[1] http://www.idc.com/getdoc.jsp?containerId=prUS22316610

*圖 24：*1999-2009 每年通報的虛擬化漏洞揭露

由於虛擬化產品已經出現在市面上，自然可以預期漏洞揭露的數量將逐年上升。雖然 2002 至 2008 年的確是這樣，揭露數目在 2008 年達到 100 的高峰，但在 2009 年卻下降了 12 個百分點，來到 88；而且可望在 2010 年再次微幅下降（2010 上半年揭露 39 個虛擬化漏洞）。此虛擬化漏洞趨勢表示：虛擬化供應商自 2008 年以來已經更注重安全，而且（或者）安全研究人員將他們的努力集中在比較容易達成的目標。

虛擬化漏洞的嚴重程度

正如圖 25 所示：此處被列入年分析的高、中嚴重漏洞在虛擬化漏洞中已超過半數。每年高嚴重漏洞在所有漏洞中已超過三分之一（2006 年除外）。這些特性也適用於 2010 上半年。整體而言，40% 漏洞通報屬於高嚴重、26% 爲中嚴重、34% 爲低嚴重。由於高嚴重漏洞往往最容易被攻擊，而且受攻擊的系統有可能完全被控制，因此虛擬化漏洞可能會造成重大安全威脅。特別是考慮到：許多漏洞取消了虛擬化通常會提供的隔離功能，讓攻擊者可存取遭受攻擊的虛擬機器的外部資料。

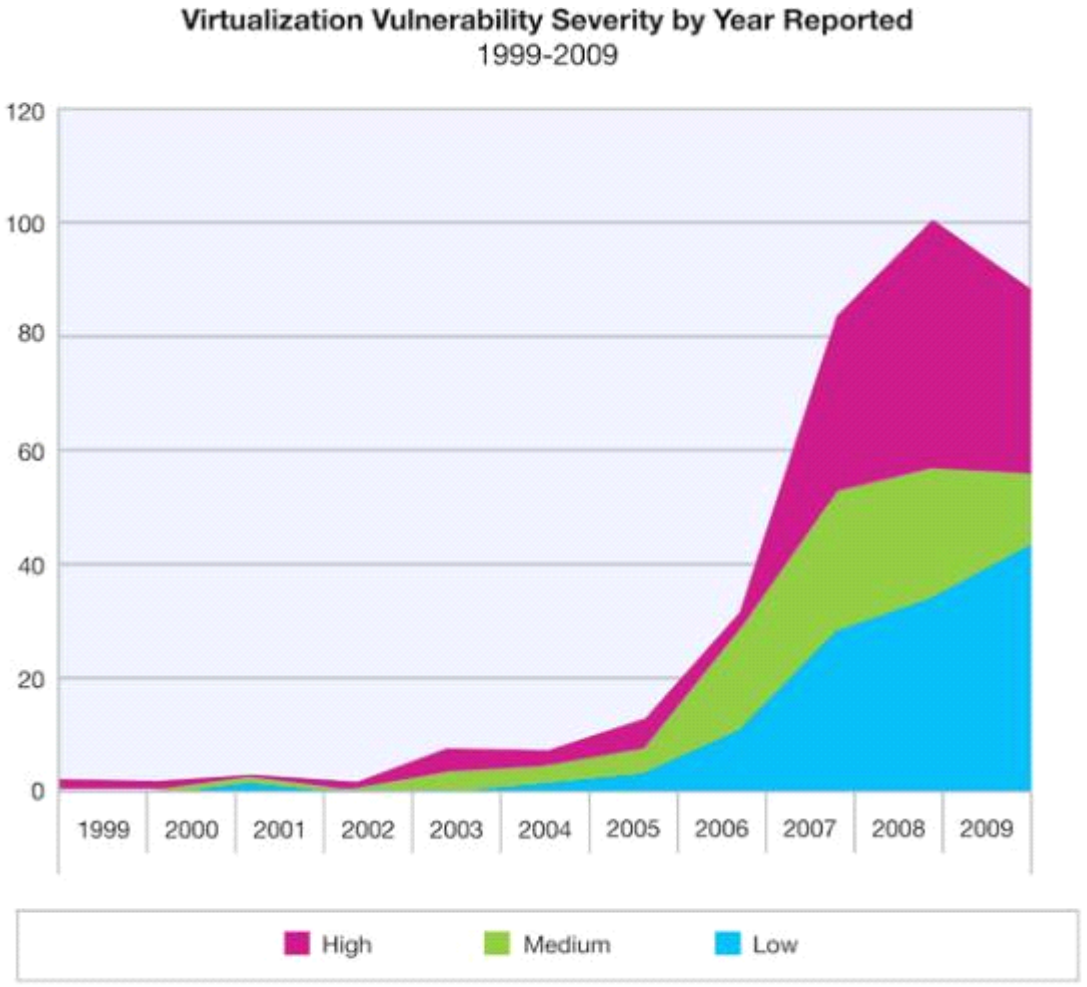


圖 25： 1999-2009 每年通報的虛擬化漏洞之嚴重程度

虛擬化漏洞的位置

了解虛擬化漏洞的位置非常重要（即它們出現在程式碼哪些地方），這影響到供應商必須耗費多少力氣才能修補。圖 26 比較虛擬化產品供應商程式碼的漏洞數量，以及虛擬化產品所使用的第三方元件中的漏洞數量。自 2005 年起，每年（除了 2007 年）第三方元件中的漏洞數已超過供應商程式碼中的數量。這種特性也大致適用 2010 上半年，當時供應商程式碼中出現 20 個漏洞，而第三方元件中有 19 個漏洞。這表示：虛擬化供應商必須小心選擇第三方元件，且應建立相關機制，元件漏洞被通報時，才能迅速加以更新。

這些統計資料分成工作站專屬和伺服器專屬的產品。工作站產品包括運行在主機作業系統上的產品；伺服器產品包括運行在「空機上」的產品（也就是把 Hypervisor 本身當成作業系統使用）。工作站產品漏洞所顯示的趨勢，與圖表趨勢正好相反，只有 24% 出現在第三方元件上。伺服器產品漏洞則是將這種趨勢發揮到極致，這類漏洞有 70% 出現在第三方元件上。

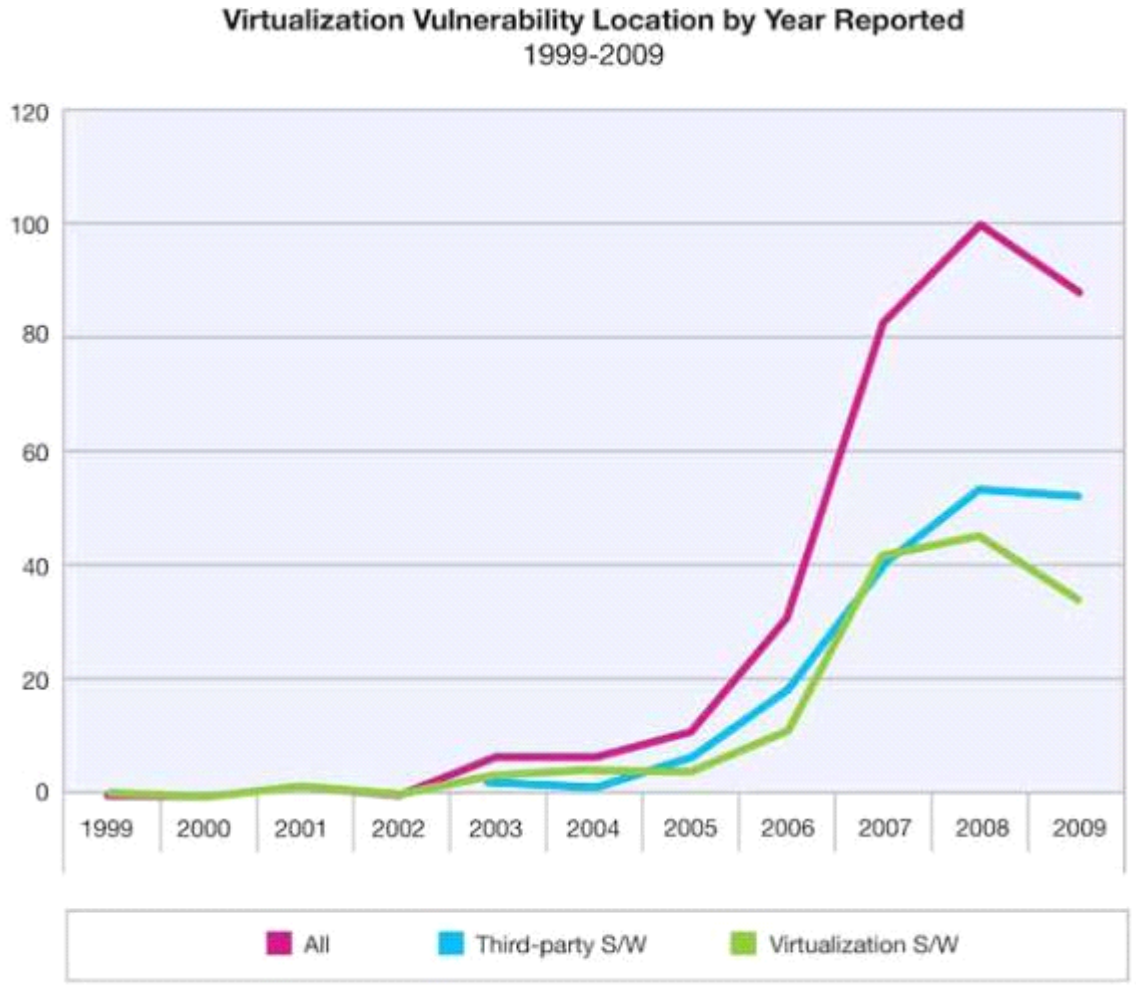


圖 26： 1999-2009 每年通報的虛擬化漏洞位置

虛擬化漏洞的產品類型

圖 27 顯示工作站產品漏洞與伺服器產品漏洞相比的趨勢。如前所述，工作站產品包括運行在主機作業系統上的產品；伺服器產品包括運行在「空機上」的產品（也就是把 Hypervisor 本身當成作業系統使用）。2005 年起，每年虛擬化伺服器產品的漏洞都超過工作站產品的漏洞。這可能代表：伺服器產品更爲複雜，而且多數人會把心思都集中在找出伺服器產品的漏洞。

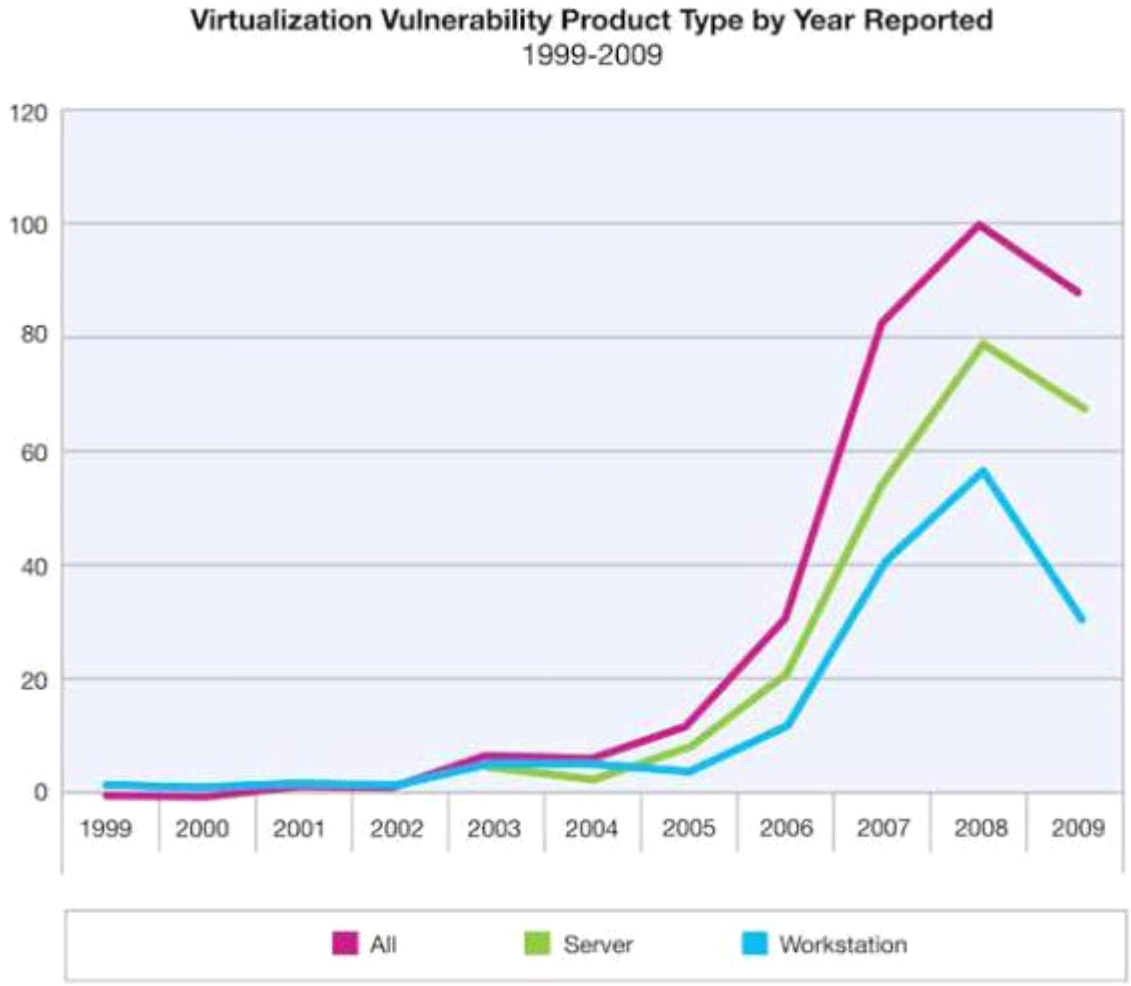


圖 27： 1999-2009 每年通報的虛擬化漏洞之產品類型

虛擬化漏洞的漏洞類型

圖 28 和 **29** 分別顯示工作站和伺服器產品的漏洞類型分佈。本分析只包括：存在於虛擬化系統程式碼中的漏洞（第三方元件中的漏洞已排除）。

漏洞類型的定義，以及工作站與伺服器產品各佔的百分比如表 5 所示。

類型	說明	工作站百分比	伺服器百分比
主機	影響主機作業系統的漏洞，該系統上已安裝虛擬化系統，但並未執行虛擬機器。	30.8%	0%
客體	影響客體虛擬機器的漏洞，但並未影響 Hypervisor 或主機作業系統。	26.3%	15.0%
逃逸到主機	允許攻擊者從客體虛擬機器「逃逸」的漏洞，這會影響執行虛擬化系統的主機作業系統。	24.1%	0%
Web 應用程式	Web 應用程式（通常是管理應用程式）中，影響執行用戶端瀏覽器之系統的漏洞。	9.8%	10%
虛擬化系統	影響虛擬化系統本身（即整個虛擬化環境）的漏洞，但排除起因於客體虛擬機器的漏洞。	4.5%	37.5%
逃逸到 Hypervisor	允許攻擊者從客體虛擬機器「逃逸」的漏洞，這會影響其他虛擬機器或 Hypervisor 本身。就工作站產品而言，這類漏洞並不會影響主機作業系統。	3.8%	35.0%
主控台	影響自訂管理主控台的漏洞。	0.8%	0%
Web 伺服器	影響 Web 伺服器的漏洞，該伺服器實行虛擬化系統所用的 Web 應用程式。	0%	2.5%

*表 5：*虛擬化漏洞的漏洞類型（包括工作站及伺服器產品）

漏洞類型的影響

主機漏洞、Web 應用程式漏洞、Web 伺服器漏洞以及主控台漏洞並非虛擬化系統所獨有；他們與傳統應用程式的漏洞十分類似。這些只影響遠端元件的漏洞（Web 應用程式和主控台漏洞），與傳統應用程式相比，並未帶來較大風險。主機漏洞與 Web 伺服器漏洞帶來的伺服器端風險，與那些傳統應用程式帶來的風險類似，但有可能影響到多個在虛擬化系統下執行的虛擬機器。客體機器漏洞、逃逸到 Hypervisor 的漏洞、逃逸到主機的漏洞，以及虛擬化系統漏洞爲虛擬化系統所獨有，需要額外分析以了解它們帶來的風險。

客體機器漏洞

客體機器漏洞與非虛擬化系統的主機漏洞十分類似，因爲它們只影響在受害的客體機器上執行的應用程式。就這方面而言，它們並不會構成新風險 - 某個系統中的漏洞只會影響該系統。

逃逸到主機的漏洞

逃逸到主機的漏洞會構成新風險，也就是在某個系統（客體虛擬機器）中的漏洞會影響到另一個系統（虛擬化系統主機）的安全性，無需透過網路傳播。對主機作業系統所做的漏洞評估無法揭露所有主機漏洞。若主機存在逃逸到主機的漏洞，則其風險預測就必須將執行在該主機上的虛擬機器的額外風險列入考量。虛擬機器影像的啓動和停止，可能會讓這種風險逐漸產生變化。

逃逸到 Hypervisor 的漏洞

與逃逸到主機的漏洞一樣，逃逸到 Hypervisor 的漏洞涉及某個系統（客體虛擬機器），不需透過網路傳播，便可影響其他系統。在此情況下，執行在相同 Hypervisor 上的虛擬機器之風險，取決於其他執行在相同 Hypervisor 上的虛擬機器之漏洞。

虛擬化系統漏洞

最後，虛擬化系統漏洞帶來的風險類型與主機漏洞類似，其潛在影響超越虛擬化系統本身，進而影響到執行在虛擬化系統上的客體機器。

工作站產品漏洞

圖 28 呈現工作站產品供應商程式碼漏洞，我們可見到這類漏洞中，超過半數都屬於前兩個類別，也就是主機與客體。這些漏洞不會透過虛擬機器散佈威脅，它們屬於傳統漏洞。令人驚訝的是：工作站產品供應商程式碼漏洞超過 25% 都與從虛擬機器逃逸有關。此產品類別中，「逃逸到主機的漏洞」之普及率是「逃逸到 Hypervisor 的漏洞」的六倍。

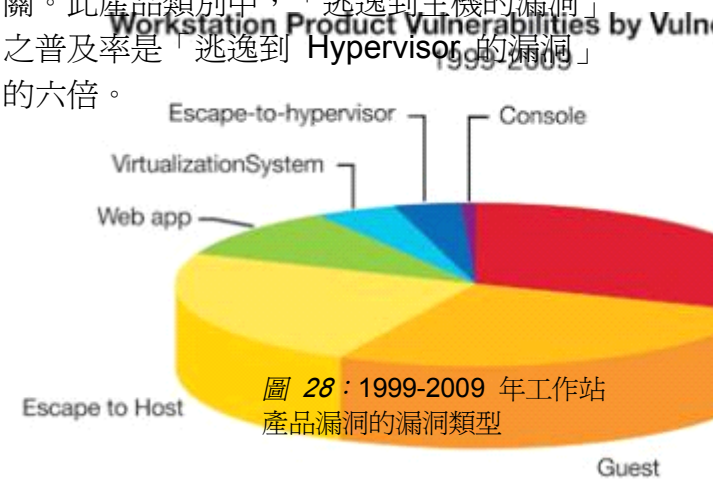
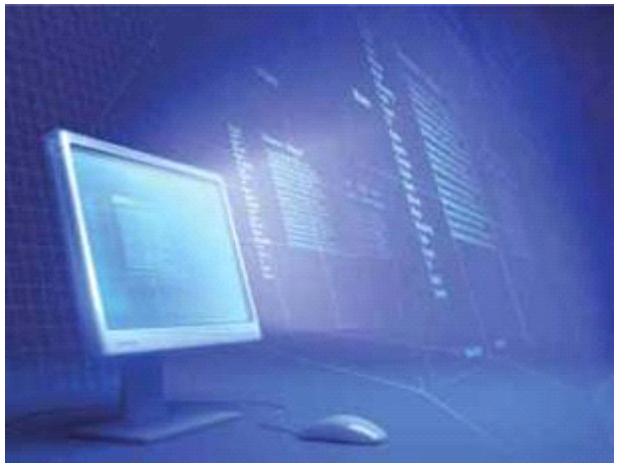


*圖 28：*1999-2009 年工作站產品漏洞的漏洞類型

伺服器產品漏洞

從圖 29 中我們可看到：伺服器產品中供應商程式碼漏洞的最大類別爲虛擬化系統漏洞，佔了 38%。逃逸到 Hypervisor 的漏洞緊跟在後，佔了 35%。逃逸到 Hypervisor 的漏洞在伺服器產品供應商程式碼漏洞中，佔了三分之一以上。伺服器級逃逸到 Hypervisor 的供應商程式碼漏洞已影響 Citrix、Parallels、RedHat 及 VMware 產品。其中五個屬於阻斷服務漏洞，一個屬於遠端程式碼執行漏洞。



伺服器級逃逸到 Hypervisor 漏洞的存在，會影響到虛擬伺服器的部署。一般推測：市場上不存在會影響伺服器級系統的逃逸到 Hypervisor 的漏洞，因此在相同實體硬體上，執行安全敏感度不同的虛擬伺服器，這是可以接受的。此處的結果顯示：逃逸到 Hypervisor 的漏洞確實存在於伺服器級系統，這不禁讓人懷疑，安全敏感度不同的虛擬伺服器是否適合執行在相同實體機器上。此處的觀察突顯了確保虛擬伺服器不被入侵的重要性，也強調爲虛擬化系統及時修補管理的重要性。

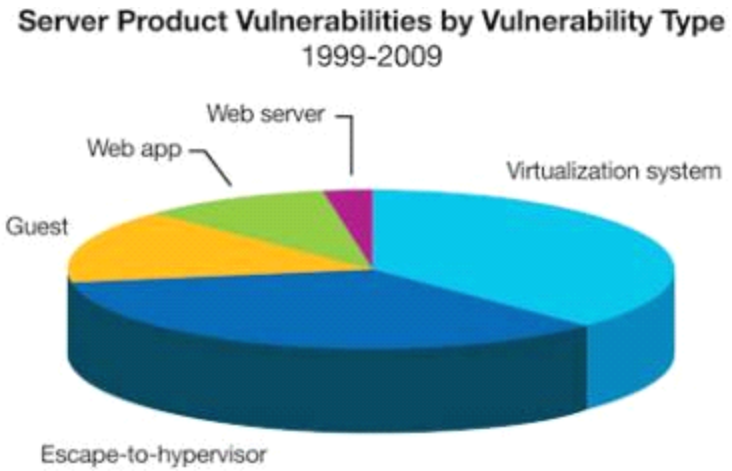


*圖 29：*1999-2009 年伺服器產品漏洞的漏洞類型

各供應商的虛擬化漏洞

圖 30 顯示列入此分析中各供應商的虛擬化漏洞揭露。VMware 產品所通報漏洞的數量最多，這並不令人意外，畢竟 VMware 處於市場領導者的地位。在通報的漏洞中，VMware 產品佔了 80% 以上，緊接在後的是 RedHat 與 Citrix，分別佔了約 7% 和 6%。其餘供應商（包括 IBM、Microsoft 與 Oracle/Sun）的表現都相當不錯，在通報的漏洞中，每家供應商只佔約 1%，可能是這些供應商在產品安全方面表現傑出；也有可能是漏洞研究人員尚未詳細檢視他們的產品。

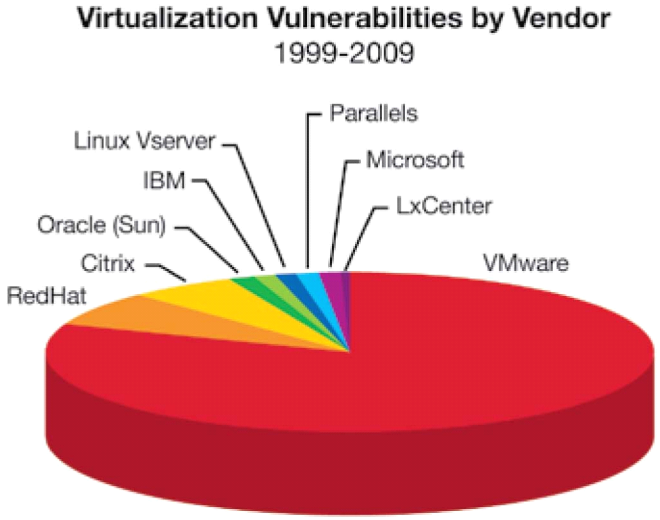


*圖 30：*1999-2009 年各供應商的虛擬化漏洞

弱點可用性

各類已知漏洞攻擊的數量，可用來估量漏洞被攻擊的可能性。1999 年以來，373 個通報的虛擬化漏洞中，有 51 個 (14%) 存在已知的弱點攻擊方式。與此相比，整個 X-Force 資料庫中，有 25% 的漏洞存在已知的弱點攻擊方式。由此可知：虛擬化漏洞的弱點攻擊可用比率，大約是全部漏洞可用比率的一半。這點反映弱點攻擊開發人員比較不容易利用虛擬化漏洞，而且（或者）也比較不注重虛擬化產品。

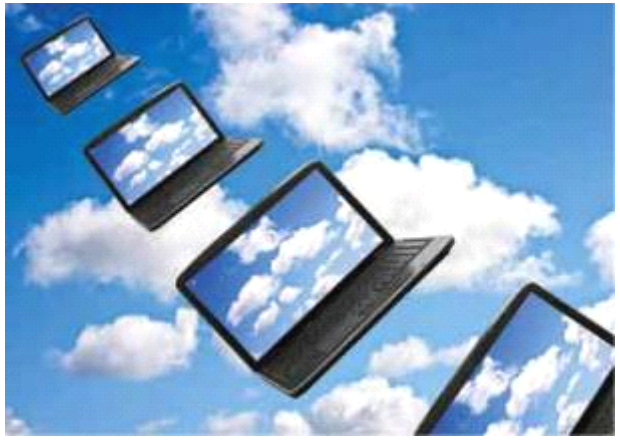
特別值得注意的漏洞類型是：伺服器產品中逃逸到 Hypervisor 的漏洞（因爲這些漏洞的風險極高）。28 個這類漏洞中，只有 2 個存在已知的弱點攻擊方式。雖然只佔了一小部分，但這類產品的漏洞存在弱點攻擊的方法，才是真正令人擔憂的事情。

新興的雲端技術：採用雲端服務，爲將來做好準備

雲端運算對組織而言有成本與效率上的利多，因此被認爲是市場上的突破性新技術。對組織而言，除了嘗鮮新技術外，更重要的是確保新技術不會爲自身帶來新風險。也難怪目前許多組織暫緩移轉到雲端，對雲端運算仍抱持觀望的態度。

最新研究指出：安全性是企業採用雲端技術最大的障礙；另一項障礙則是「可用性」。事實上極少數企業已全面採用雲端模式，大部分的企業只轉移了風險較低的部分到雲端上。許多受益於雲端技術的中小型企業，反而期待藉由主機服務機構所提供的功能增強本身的安全性。

雲端技術無法被廣泛採用的主因是：雲端產品及其功能太過複雜與多變。組織在評估雲端技術前，往往會先觀察個別供應商及其功能。



然而，IBM 主張：組織採用雲端技術前，應先考慮打算放在雲端上的工作量。

根據工作量來評估雲端技術，組織便可進一步理解：哪些必備要素可幫助選擇合適的雲端部署方案。例如，從醫療資料的工作量便可看出安全與稽核的需求，也能看出管制條例中共同承諾的需求。這類考量爲組織提供了其他的益處，例如：進一步了解組織內部資料，也能明白這些資料對於企業的重要性。

依照安全與管制需求分類資料後，組織便可利用此資訊，判定保護雲端資料時需要哪些屬性；並可依此制定標準來評估各種部署供應商。有個關於屬性的例子：組織有明確 eDiscovery 需求或義務時，基於法律上的需要，那些資料就必須保存好並隨時可取用。

其他關於在公共雲端進行部署的疑慮爲主機服務機構的金融穩定度與部署策略的因素。例如，客戶可能想避開將客戶集結成群的供應商，以免某個租戶的法律問題連帶影響其他共同租戶。

總之，組織採用雲端服務前，必須先擬定策略方針。這代表尋找供應商前，必須先深入了解機會與需求。只要預先做好功課，就不怕找不到最合適的商業合作夥伴。

第二部分
概觀

IBM X-Force® 研發團隊負責揭露、分析、監測與記錄各式各樣的電腦安全威脅與漏洞。根據 X-Force 的觀察，2010 上半年出現了一些新趨勢。希望本報告提出的趨勢相關資訊，能做爲您規劃 2010 下半年及未來資訊安全的有用基礎。

2010 年中重點

漏洞

- 今年上半年新漏洞揭露數已創歷史新高。這與 2009 年中報告形成強烈對比，當時新漏洞揭露爲過去四年的最低點。Web 應用程式漏洞（特別是跨網站指令碼及 SQL 資料隱碼）持續主導威脅趨勢。
- Apple 仍舊是揭露漏洞最多的供應商，在所有揭露中足足佔了 4%。Microsoft 連續三年蟬聯揭露漏洞最多供應商後，已經滑落至第二名。由於 PDF 與 Flash 漏洞揭露通報大幅增加，所以 Adobe 排名第三。
- 在作業系統方面，今年上半年 Linux 的作業系統新漏洞揭露排名第一，Apple 緊跟在後。如果光看重大揭露與高作業系統揭露，Microsoft 就佔了 73%，其他對手相比之下就顯得微不足道了。

弱點攻擊

- 在所有漏洞揭露中，Web 應用程式仍舊佔了 55%。
- PDF 弱點攻擊在 2010 年十分普遍，攻擊者會使用混合式詐騙（包括僞裝過的垃圾郵件、網路釣魚與混碼）來擾亂使用者。
- Internet Explorer 率先處理漏洞揭露以及積極尋求方法以利用這些新漏洞的攻擊者。

漏洞

2010 上半年漏洞揭露計數

先前在本報告的第一部分，我們討論到 2010 上半年所揭露的漏洞數量令人難以置信。我們預計 2010 年的揭露數目將會創下歷史新高。

在本報告 Web 章節，我們討論到：影響 Web 應用程式的漏洞，在所有通報揭露中佔了整整一半。排在 Web 應用程式之後的是客製化應用程式、Web 瀏覽器以及 PDF - 上述這些都證實 2010 上半年通報的紀錄。

爲避免關於漏洞特徵的說明有任何疑義，本報告採用以下的 IBM 安全服務定義。

「漏洞」是指多方面的條件，導致（或可能導致）資訊系統的機密性、完整性或可用性，出現明確或不明確的故障。

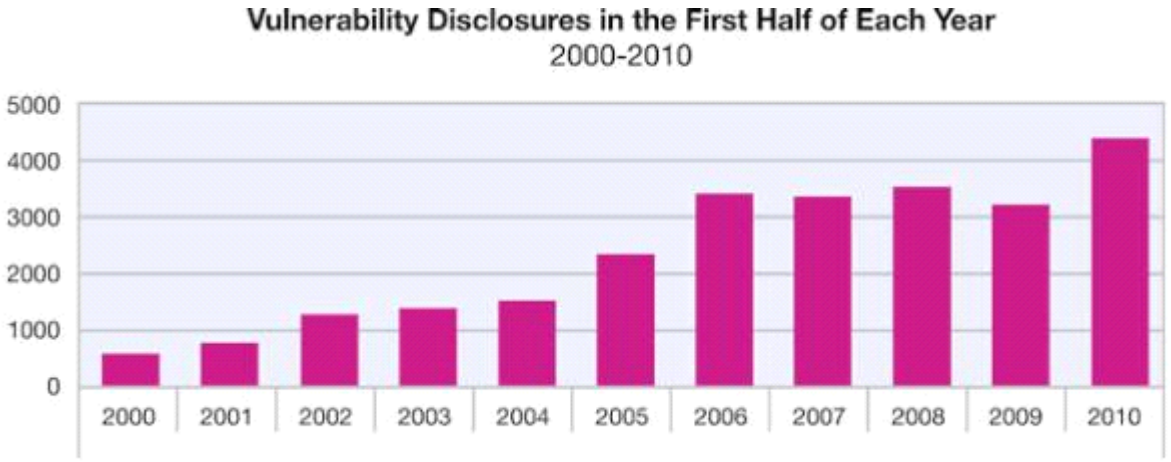


*圖 31：*2000-2010 每年上半年的漏洞揭露

所揭露漏洞的嚴重程度

共通弱點評估系統（Common Vulnerability Scoring System，CVSS）是業界評估漏洞嚴重程度與風險的標準，以公式、基本指標及暫時指標爲基礎。基本指標的特性是：在一段時間內通常不會改變，例如存取向量、複雜度、鑑別與影響偏差。暫時指標的特性是：特定漏洞一段時間後往往會改變，包括弱點攻擊性、補救層次與報告機密性。

CVSS 指標認定的重大漏洞，是指預設設置的漏洞，而且可網路路由傳送，不需要鑑別即可存取，並允許攻擊者取得系統或根層次的存取權。

表 6 說明基本與暫時 CVSS 分值的嚴重程度。

CVSS 分值	嚴重程度
10	重大
7.0-9.9	高
4.0-6.9	中
0.0-3.9	低

表 6： CVSS 分值與對應的嚴重程度

有關 CVSS 的詳細資訊，包括完整 CVSS 說明及其指標，請參閱 First.org 網站：
http://www.first.org/cvss/

CVSS 基本分值

如圖 32 所示，重大漏洞仍舊維持在 1%，與 2008 和 2009 年的百分比類似。

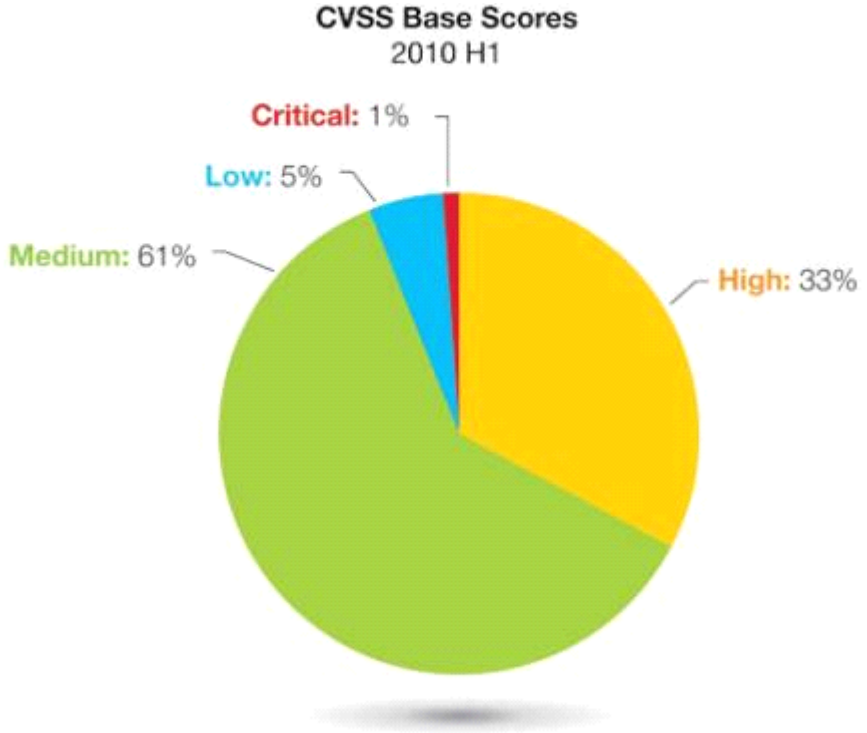


圖 32： 2010 上半年 CVSS 基本分值

相對百分比與 2009 年的資料相當一致。低、中嚴重性漏洞小幅下滑，高嚴重性漏洞則相應增加。中嚴重性漏洞包含兩種最常見的漏洞揭露：SQL 資料隱碼與跨網站指令碼。相較於 2008 年的 36%，以及 2009 上半年的 30%，高嚴重性漏洞增加到 33%，如圖 33 所示。

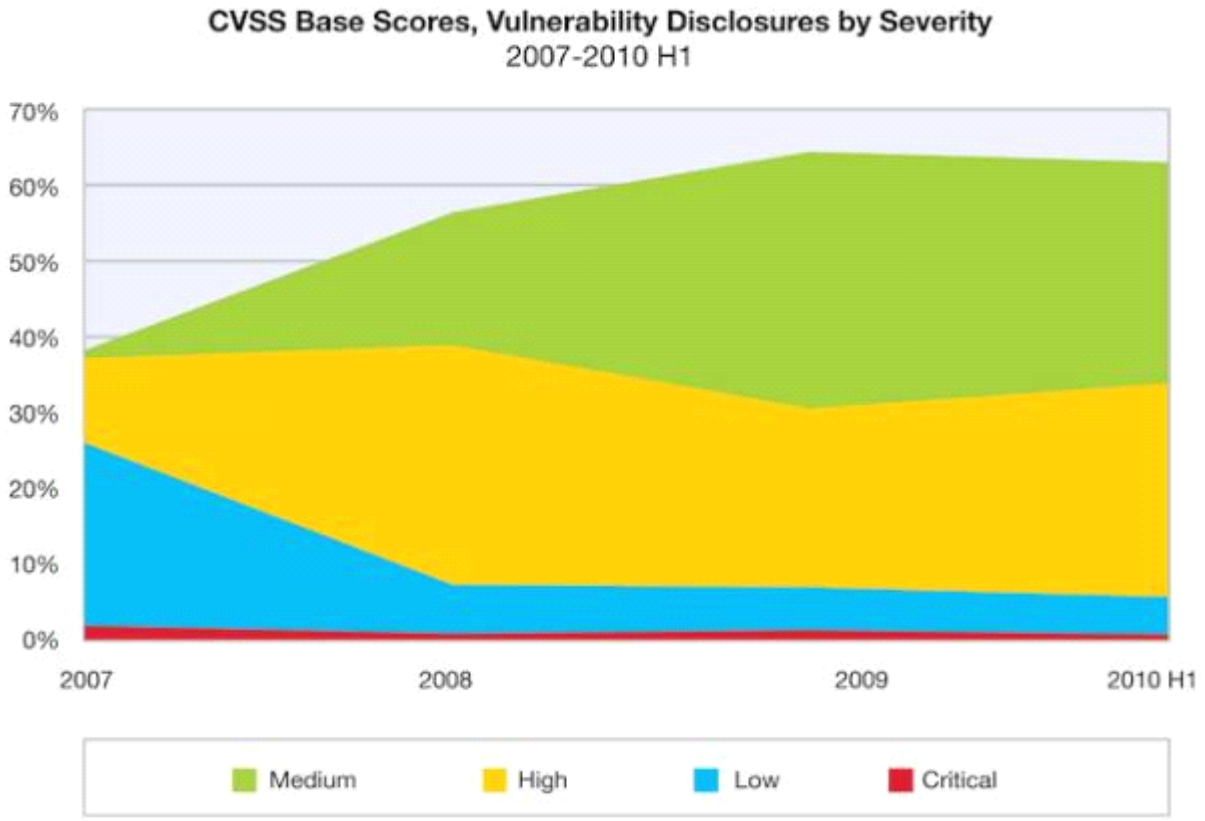


*圖 33：*2007-2010 上半年 CVSS 基本分值、所揭露漏洞的嚴重程度

揭露漏洞最多的供應商

2010 上半年揭露漏洞最多的前十大供應商，佔了所有揭露漏洞五分之一，略低於 2009 年 (23%)，而略高於 2008 年 (19%) 以及 2007 年 (18%)。

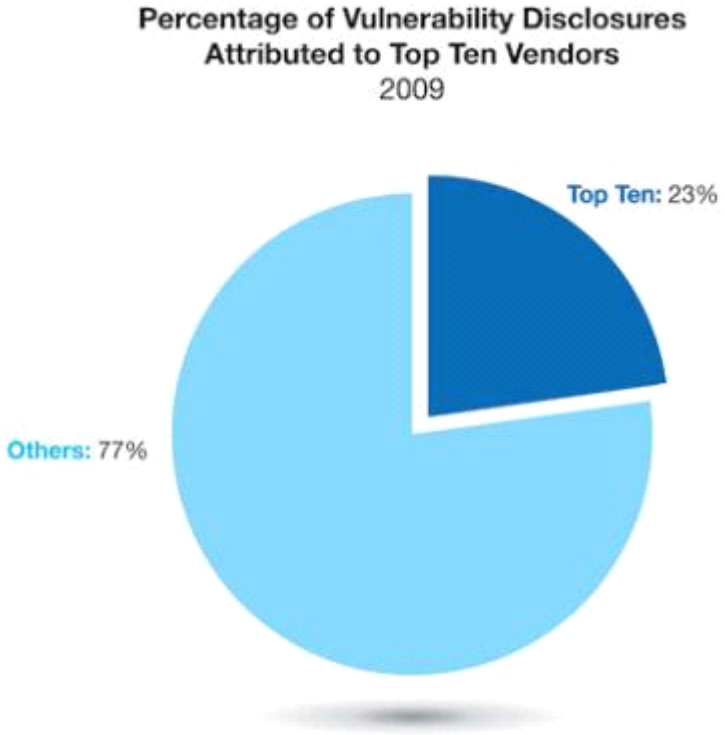


圖 34： 2009 年前十大供應商漏洞揭露百分比

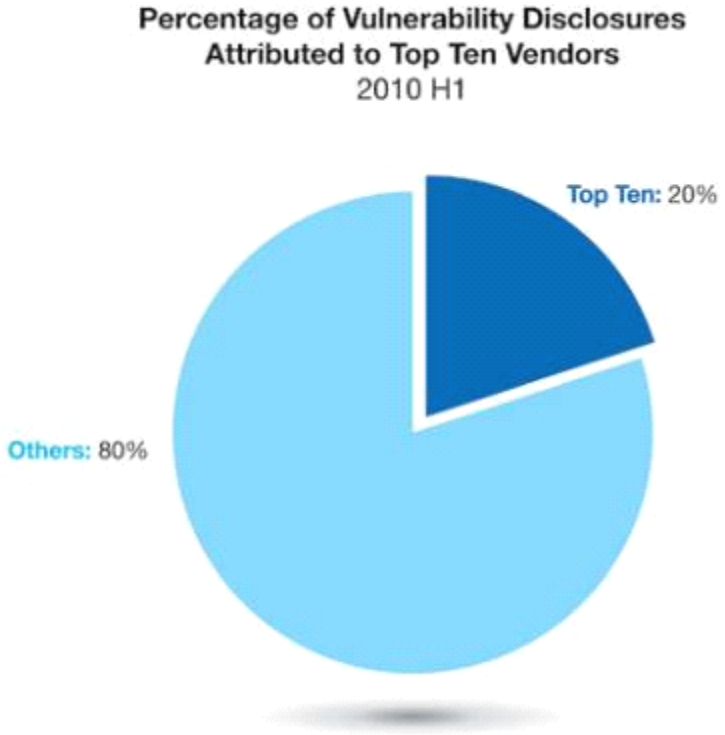


圖 35： 2010 上半年前十大供應商漏洞揭露百分比

前十大供應商名單的變化

X-Force 資料庫團隊利用共通平台列舉（Common Platform Enumeration，CPE）這項業界標準，決定各供應商與供應商產品的漏洞分配。請參閱 **http://cpe.mitre.org/** 以取得更多資訊。

表 7 爲 2010 上半年的前十大供應商及其漏洞百分比；另外也提供 2009 年的比較。請注意：這些統計資料並未根據市佔率、產品數目，或各家供應商所產出的程式碼行數，調整揭露漏洞所佔比例。一般而言，量產與大量發行或容易取得的軟體，揭露漏洞數目比較多。

一些觀察：

- Apple 在所有漏洞揭露中足足佔了 4%，連續兩年蟬聯第一。
- Sun 從去年的第二名跌到名單的底部 - 2009 年期間最爲顯著的變化。雖然 Oracle 在 2009 年 4 月收購 Sun，但他們的產品線在我們的資料庫中還是有所區別，所以我們仍然將他們分別列出。
- Microsoft 在 2006 至 2008 年，蟬聯三年供應商冠軍寶座後，又從第三名進到第二名。

2010 上半年		
排名	供應商	揭露頻率
1.	Apple	4.0%
2.	Microsoft	3.4%
3.	Adobe	2.4%
4.	Cisco	1.9%
5.	Oracle	1.7%
6.	Google	1.6%
7.	IBM	1.5%
8.	Mozilla	1.4%
9.	Linux	1.4%
10.	Sun	1.1%

2009（全年）		
排名	供應商	揭露頻率
1.	Apple	3.8%
2.	Sun	3.3%
3.	Microsoft	3.2%
4.	IBM	2.7%
5.	Oracle	2.2%
6.	Mozilla	2.0%
7.	Linux	1.7%
8.	Cisco	1.5%
9.	Adobe	1.4%
10.	HP	1.2%

表 7：揭露漏洞最多的供應商

- Adobe 從第九名上升到第三名，這可能是因爲 2010 上半年，PDF 與 Flash 通報的漏洞大幅增加。
- HP 已從名單上除名，而 Google 隨之加入，位居第六。

漏洞修正程式與修補程式的可用性

在第一部分，我們討論了漏洞可用性與修補程式比率。我們證實主要供應商在解決與修復已知漏洞方面頗有成效，而我們也列出主要供應商中最佳與最差的修補者。接下來，我們會處理遠端攻擊漏洞的議題。

遠端攻擊漏洞

最嚴重的漏洞是可從遠端攻擊的漏洞，因爲這種漏洞不需要有漏洞的系統實體存取權便可進行攻擊。遠端漏洞可透過網路或網際網路進行攻擊，而本端漏洞則需要直接系統存取權。同時屬於遠端及本端的漏洞，可透過這兩種媒介進行弱點攻擊。

過去四年半以來，在所有漏洞揭露中，遠端攻擊漏洞已從 85% 成長到 94%。2009 年，遠端漏洞佔 92%；到了 2010 上半年，已攀升到 94%。圖 36 顯示過去十年來，遠端攻擊漏洞與同期相比呈現穩定的增長。

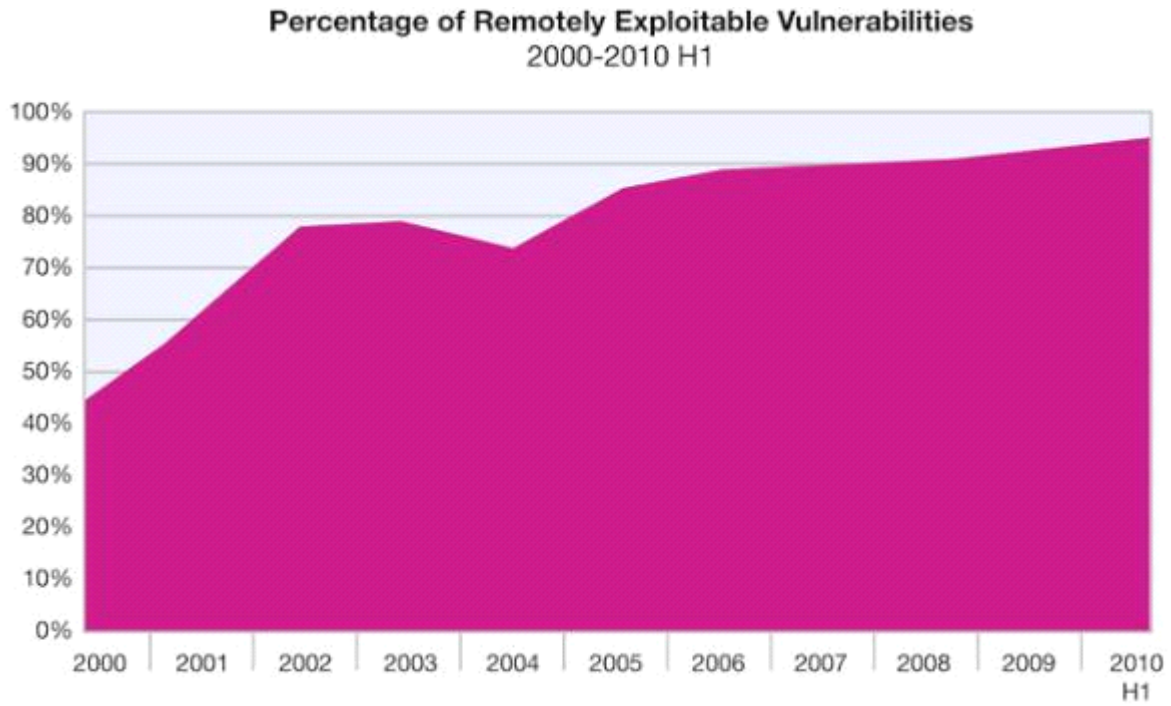


*圖 36：*2000-2010 上半年遠端攻擊漏洞的百分比

弱點攻擊後果

IBM X-Force 按弱點攻擊的後果分類漏洞，這些後果主要是攻擊漏洞所能帶給攻擊者的好處。表 8 說明各項後果。

後果	定義
避過安全性限制	越過防火牆或 Proxy、IDS 系統或病毒掃描程序這類安全性限制
竄改資料	竄改服務或應用程式相關主機所使用或儲存的資料
阻斷服務	損毀或中斷服務或系統，讓網路癱瘓
竄改檔案	建立、刪除、讀取、修改或改寫檔案
取得存取權	取得本端與遠端存取權，包括攻擊者可用來執行程式碼或指令的漏洞，因爲這類漏洞通常讓攻擊者得以存取系統。
取得權限	只能在本端系統取得權限
取得資訊	取得檔案與路徑名稱、原始碼、密碼或伺服器配置詳細資料等資訊
其他	其他種類未涵蓋的部分

*表 8：*漏洞後果定義

漏洞攻擊最常見的後果還是取得存取權，在所有漏洞後果中佔了 52%。2008 年急劇下降後，取得存取權又反彈到 50% 的關卡之上，回到 2006 與 2007 年的百分比。取得系統存取權讓攻擊者完全控制受害的系統，之後便可竊取資料、操作系統，或從該系統發動其他攻擊。

2008 年達到 22% 的高峰後，允許攻擊者操作資料的漏洞目前來到 21%，反映出明顯的 SQL 資料隱碼活動。

從百分比來看，其他大多數攻擊媒介跟往年類似。

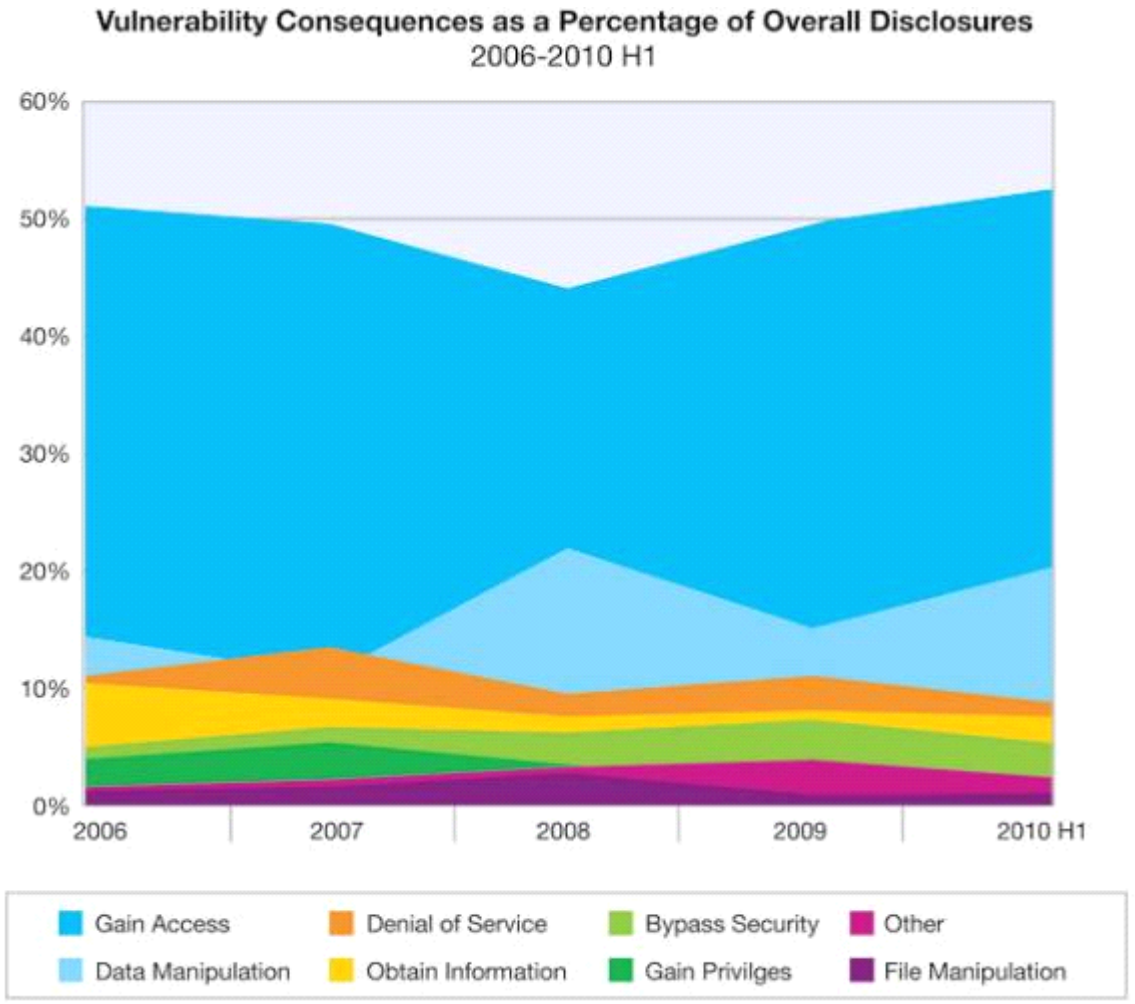


圖 37： 2006-2010 上半年各類漏洞後果佔整體揭露的百分比

揭露漏洞最多的作業系統

下列作業系統的分析計算針對單一作業系統類型提報的唯一漏洞。例如，本分析比較針對 Microsoft 作業系統提報的所有漏洞，以及同期針對 Apple 作業系統提報的所有漏洞。如果某個漏洞適用於該類型作業系統的多個版本，只會計算一次。例如，如果某個 CVE 同時適用於 Apple Mac OS X 與 Apple Mac OS X 伺服器，在 Apple 類型只會計算一次。

所有作業系統的漏洞

2010 上半年，Linux 作業系統漏洞揭露佔的比例最大，Apple 緊跟在後，位居第二。Microsoft 在 2009 年曾達到低峰，後來上升到第三名。Sun Solaris 的漏洞揭露一度大幅下滑，現已進到第四名。BSD 仍舊維持第五的位置；而 2008 年排名第五的 IBM AIX，連續兩年都在榜單之外。

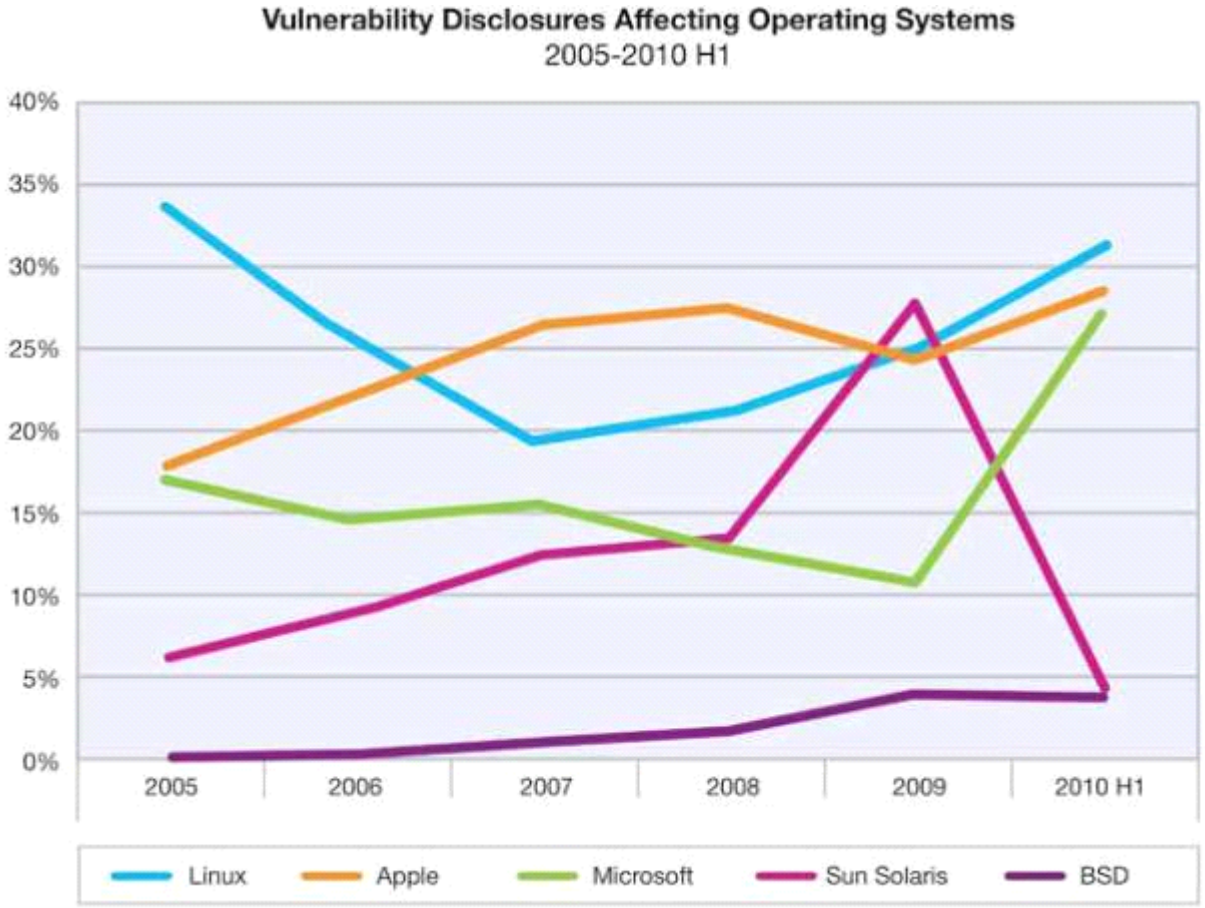


*圖 38：*2005-2010 上半年影響作業系統的漏洞揭露

重大與高嚴重性作業系統漏洞

分析作業系統漏洞的另一種方式，就是著眼於重大漏洞與高嚴重性漏洞。就防護角度而言，此類高嚴重性漏洞通常最令人憂心，經常導致完全的遠端侵入，成爲攻擊者的囊中物。排除中嚴重性漏洞與低嚴重性漏洞後，Microsoft 作業系統於 2008、2009 及 2010 上半年居冠。Linux 目前名列第二；Apple 位居第三。HP-UX 位居第四；Sun Solaris 緊跟在後，名列第五。IBM AIX 曾於 2009 上半年位居第五，現已從榜上除名。

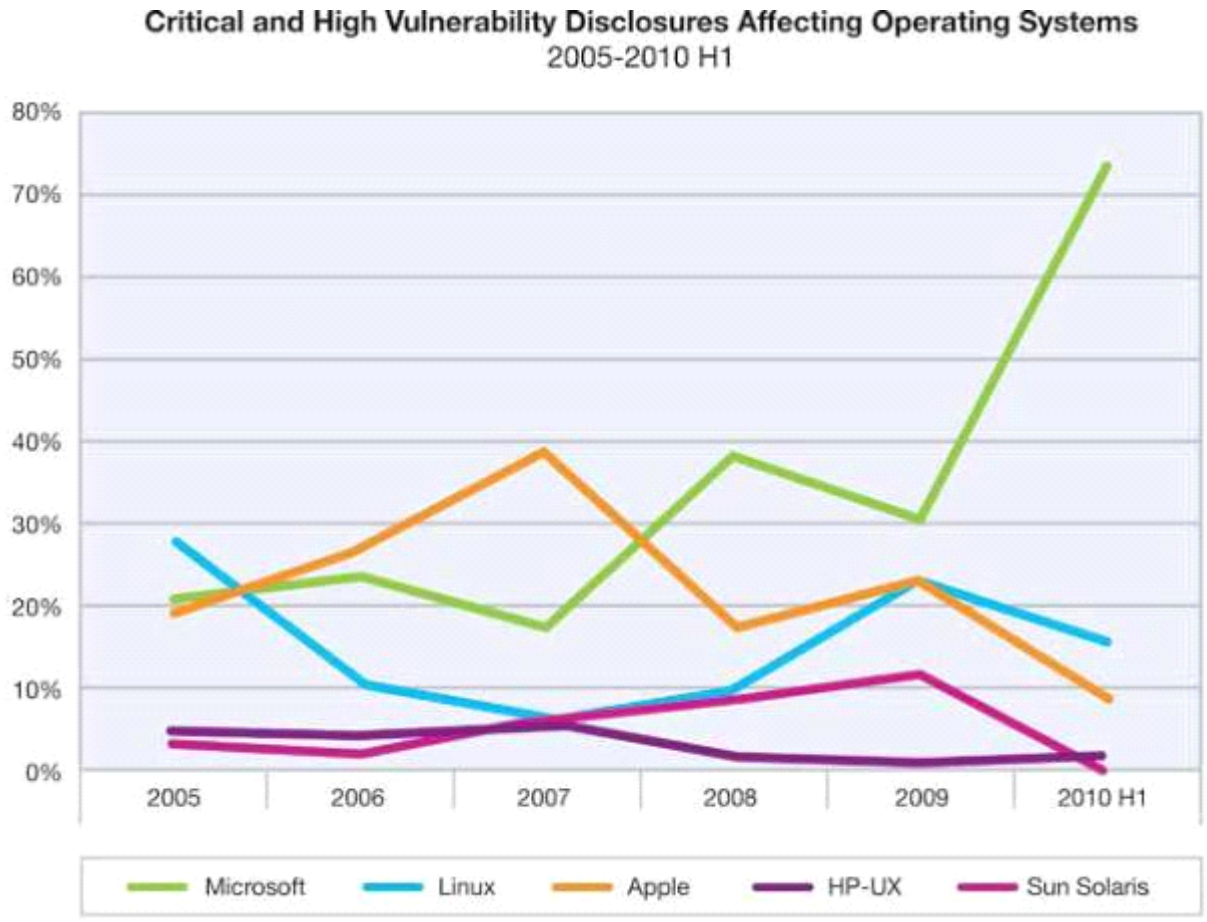


*圖 39：*2005-2010 上半年影響作業系統的重大與高嚴重性漏洞揭露

列於表 9 的五大作業系統，佔了 2010 上半年所有重大與高嚴重性作業系統漏洞揭露的 98%，相比之下，2009 上半年只佔 93%。五大作業系統佔了上半年所有作業系統漏洞揭露的 95%。

作業系統	重大與高嚴重性漏洞百分比	所有作業系統漏洞百分比
Microsoft	73%	27%
Apple	9%	29%
Linux	16%	31%
HP-UX	2%	1%
Sun Solaris	0%	4%
BSD	0%	4%
IBM AIX	0%	2%
其他	2%	4%

*表 9：*2010 上半年重大與高嚴重性漏洞揭露最多的作業系統

我們爲何不用 CPE 計算作業系統？

回顧 2008 年報告，當時 X-Force 分析了漏洞最多的作業系統。根據各供應商透過共通平台列舉（Common Platform Enumeration，簡稱 CPE）提報自家平台的情形計算漏洞。各供應商的平台分類方式稍有出入，舉例來說，針對「Linux kernel」平台通報的漏洞也可能影響其他 Linux 版本，即使該漏洞已透過 CPE 通報，也可能未正式通報爲該平台的漏洞。其他差異還包括供應商的平台分類方式。例如，Apple 將所有版本的 Apple Mac OS X 軟體結合爲單一「平台」，僅以軟體的伺服器與桌面版本區別。Microsoft 則是一律將主要作業系統稱爲「平台」，即使其他人可能將某些平台視爲不同的 Windows「版本」。

所以這份報告並非根據 CPE 內具名的「平台」計算漏洞，而是將類似平台全部合併（所有 Windows、所有 Apple），即使某個漏洞影響到該類型作業系統的多個版本，還是只會計算一次。

對作業系統漏洞建立正確的觀念

作業系統漏洞總是引起大量關注。不過真正引起的問題是執行在作業系統上的各種應用程式，本報告中許多重要統計資料已闡明這點。2010 上半年所有揭露漏洞中，作業系統的漏洞揭露約佔 11%。組織的修補方案已準備就緒多年，確保作業系統能以最快速度修補並予以保護。因此，儘管作業系統隨處可見，這些因素卻讓攻擊者難以成功發動攻擊。其他元件（例如 Web 應用程式、Web 瀏覽器以及 PDF 這類惡意文件）已超越作業系統，成爲最令人擔憂的威脅媒介。

Web 應用程式的威脅與漏洞

Web 應用程式漏洞仍然是當前影響伺服器最常見的漏洞類型。從百分比來看，Web 應用程式漏洞越過 55% 的關卡，在 2010 上半年佔了所有漏洞揭露的一半以上。

Web 應用程式的漏洞數量，以每年揭露 3,000 到 4,000 的穩定速率持續攀升。以下數據並未包含自訂開發的 Web 應用程式，或這些標準套件的自訂版本，此類自訂程式也會出現漏洞。

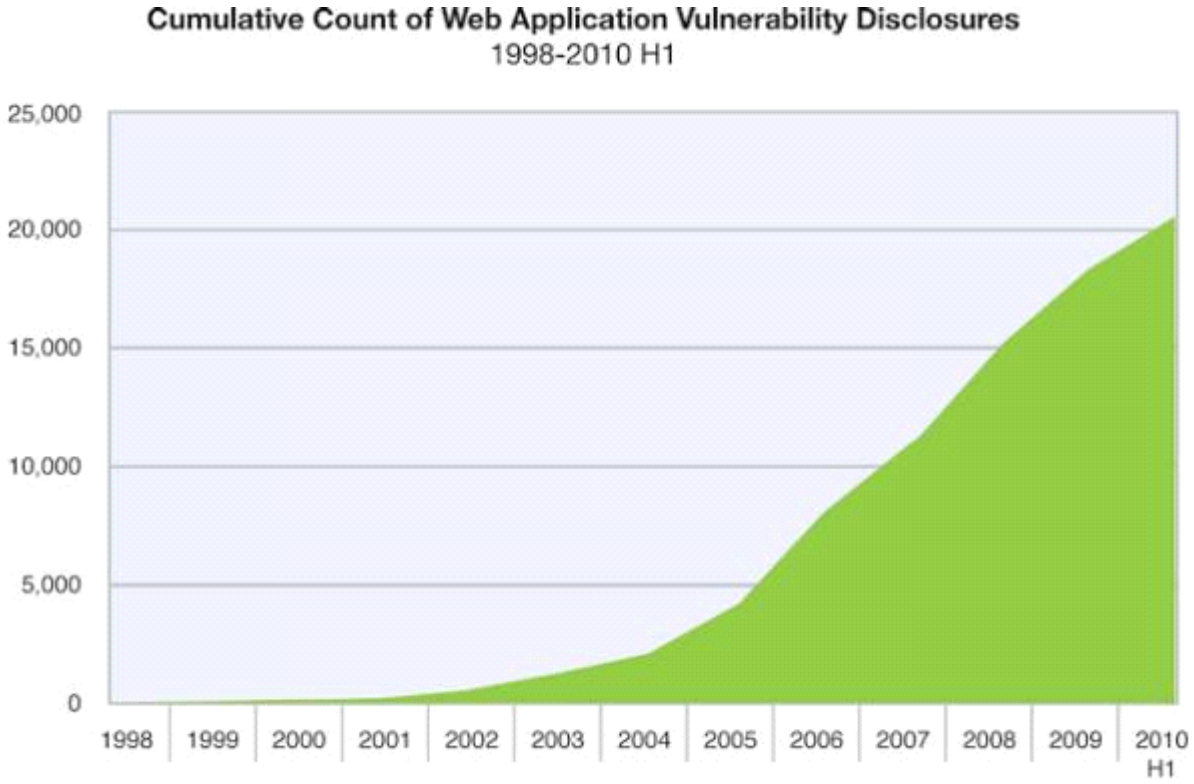


圖 40： 1998-2010 上半年 Web 應用程式漏洞揭露累加計數

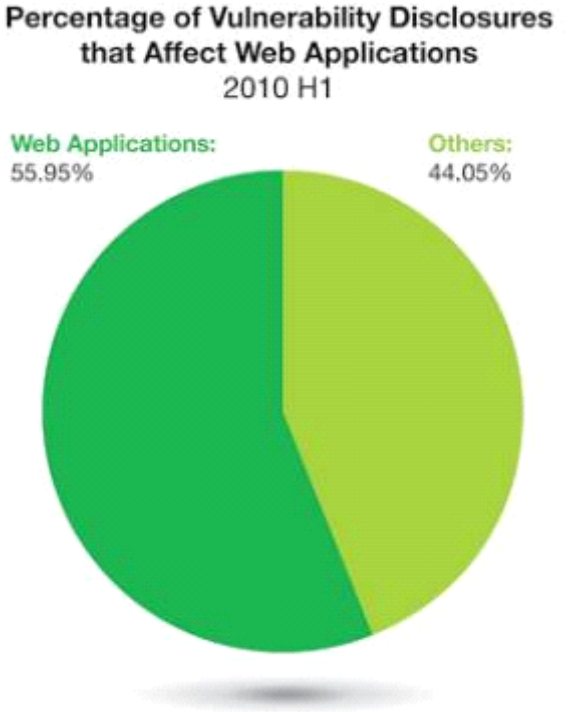


圖 41 2010 上半年影響 Web 應用程式的漏洞揭露百分比

因此，對存在於網際網路上的應用程式漏洞總數而言，這些漏洞可能只是冰山一角。

Web 應用程式漏洞揭露的攻擊種類

跨網站指令碼 (XSS) 與 SQL 資料隱碼漏洞，在 2010 上半年是影響 Web 應用程式最主要的漏洞類型。

圖 42 顯示跨網站指令碼、SQL 資料隱碼、檔案嵌入，以及其他漏洞揭露隨時間變化的相對優勢，**表 10** 則說明每種類別，包括對組織及客戶的影響。

先前在 2009 年底發佈的 X-Force 趨勢報告顯示 SQL 資料隱碼漏洞揭露與同期相比大幅衰退，當時我們把它視爲進步的跡象。過去幾年來，SQL 資料隱碼漏洞一直是網際網路上大量弱點攻擊活動的目標，而揭露的下滑可能表示這些漏洞變得越來越難尋找，因爲低垂的果實都已被摘光。不幸的是，SQL 資料隱碼揭露在 2010 上半年似乎又回到原來的數量；顯然我們並未完全渡過 Web 應用程式漏洞的難關。

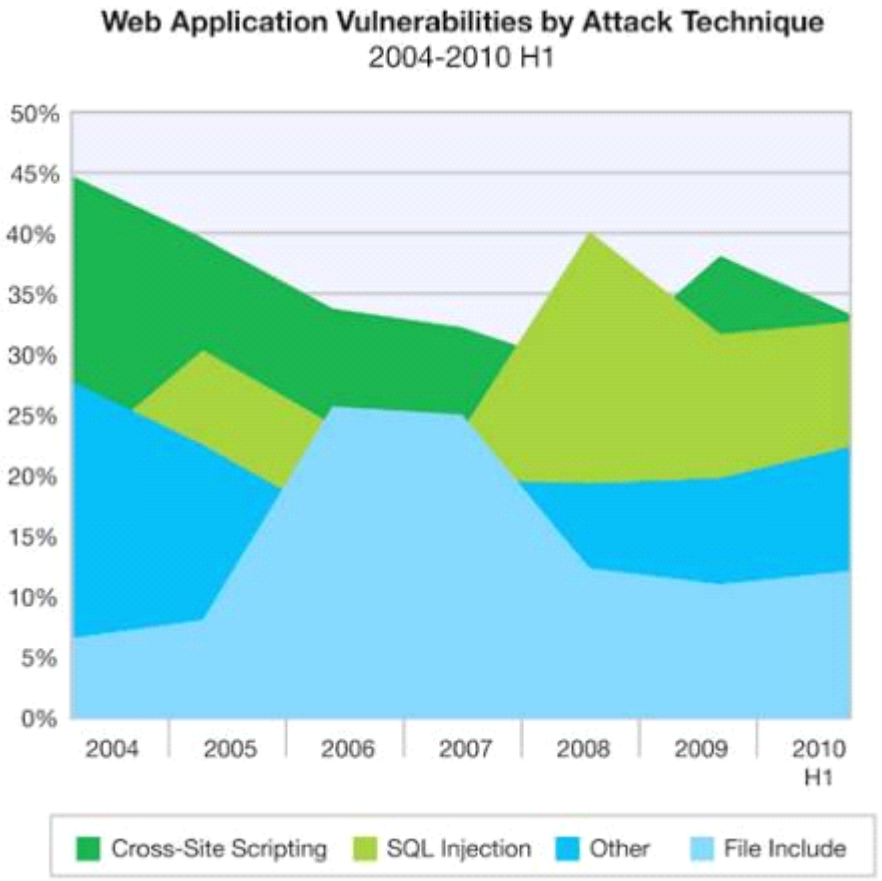


*圖 42：*2004-2010 上半年 Web 應用程式漏洞的攻擊技術

針對 Web 應用程式所發動的跨網站指令碼攻擊

「**Web 應用程式漏洞揭露的攻擊種類**」章節指出：跨網站指令碼 (XSS) 漏洞揭露在 2010 上半年相當普遍。MSS 的實際資料表明：這類 Web 應用程式漏洞的確是攻擊者最愛用的弱點攻擊方法。

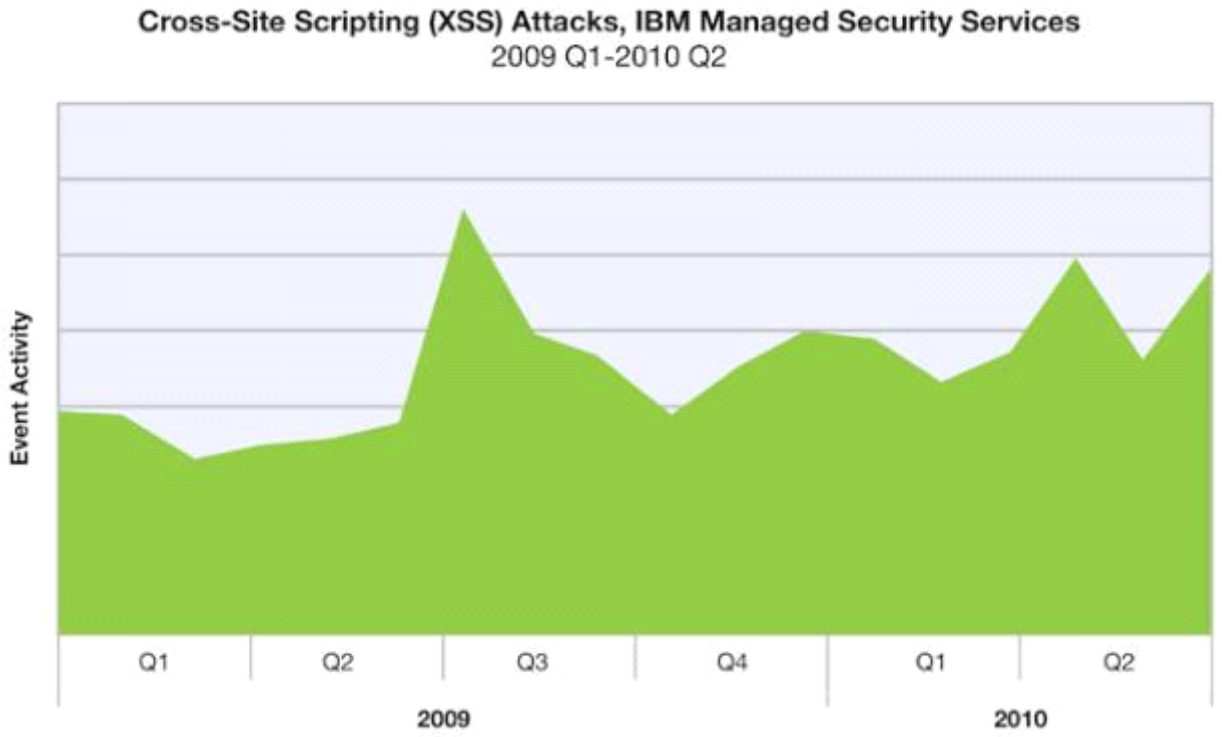


圖 43： 2009 年第 1 季到 2010 年第 2 季跨網站指令碼 (XSS) 攻擊 (IBM Managed Security Services)

攻擊技術	說明
跨網站指令碼	Web 應用程式如果未正確驗證表單欄位的使用者輸入內容、URL 語法等，就會出現跨網站指令碼漏洞，讓攻擊者可在使用者正造訪的頁面嵌入自己的指令碼，竄改頁面的行爲或外觀。這類頁面變更可用來竊取機密資訊、以惡意方式竄改 Web 應用程式，或在攻擊其他漏洞的頁面嵌入更多內容。 攻擊者首先必須建立特製的 Web 鏈結，然後誘使受害者點選（利用垃圾郵件、使用者論壇等）。由於 URL 的網域名稱屬於受信任或熟悉的公司，使用者更可能受騙進而點選該鏈結。從使用者的角度來看，攻擊來自此受信任的組織，而非侵入組織漏洞的攻擊者。
SQL 資料隱碼	SQL 資料隱碼漏洞也與不當驗證使用者輸入內容有關，如果輸入內容（例如從表單欄位）能夠動態包含 SQL 陳述式，然後由資料庫加以執行，便可能出現這類漏洞。存取後端資料庫可讓攻擊者讀取、刪除與修改機密資訊，有時候還可執行任意程式碼。 SQL 資料隱碼漏洞會外洩機密客戶資訊（像是信用卡資料），也會讓攻擊者得以於資料庫嵌入其他攻擊，用來對付網站使用者。
檔案嵌入	應用程式從遠端來源擷取程式碼，然後在本端應用程式執行時，就會出現檔案嵌入漏洞（常見於 PHP 應用程式）。遠端來源往往並未接受確實性驗證，讓攻擊者得以利用 Web 應用程式從遠端執行惡意程式碼。
其他	這類攻擊包含某些阻斷服務攻擊、目錄挖掘 (directory traversal)，以及其他各種技術，讓攻擊者得以檢視或取得未獲授權資訊，變更檔案、目錄、使用者資訊或其他 Web 應用程式元件。

*表 10：*Web 應用程式最常見的漏洞種類說明

OWASP 前十大

以 Web 應用程式、服務與資料爲目標的攻擊與日俱增，組織不得不強化整個企業的安全執行。這些攻擊包括跨網站指令碼 (XSS)、SQL 資料隱碼攻擊、阻斷服務攻擊，以及其他技術（如目錄挖掘等）。這類攻擊讓攻擊者得以檢視或取得未獲授權資訊，變更檔案、目錄、使用者資訊與其他 Web 應用程式元件的各種技術。

OWASP Top 10（開放 Web 應用程式安全計畫）提供 Web 應用程式安全意識文件，並闡明重大 Web 應用程式安全缺失的普遍共識。計畫成員包括來自世界各地的各類安全專家，分享他們的專業知識，製作這份清單。

某些漏洞像是「遭破壞的鑑別與連線管理」讓攻擊者可破壞密碼、金鑰、階段作業記號，或利用其他實作缺陷冒用使用者的身分。疏於限制 URL 存取、安全組態不當配置，以及未經驗證的重新導向與轉發，會將商業機密資料與資訊洩漏給未經授權的使用者。我們建議組織應評估外部化應用程式與服務的風險與漏洞，並實施適當安全控制以管理整個企業的使用者身分及存取權。

2010 OWASP 前十大威脅	關鍵因素
A1：資料隱碼缺陷	來自使用者提供的應用程式指令或查詢的個別不受信任資料。 **誰可以將資料傳送**到系統？
A2：跨網站指令碼 (XSS)	來自作用中瀏覽器的個別不受信任資料。
A3：遭破壞的鑑別與連線管理	需要能在登出時使階段作業狀態失效以
A4：不安全的直接物件參照	是否有任何使用者具有**部分存取權**
A5：跨網站的偽造要求 (CSRF)	需要能「拒絕」、「逐步」或「重新鑑別」使用者以
A6：安全組態不當配置	您是否已經對整個應用程式堆疊執行
A7：不安全的加密儲存	**加密**機密資料。使用安全記號保護加密資源。
A8：疏於限制 URL 存取	需要**控制**入口網站上 URL 求？
A9：傳輸層保護不足	是否有人可監控使用者的網路流量？
A10：未經驗證的重新導向與轉發	是否有人可**騙使用者**對您的網站送出要求？

*表 11：*2010 OWASP 前十大威脅清單

Web 應用程式平台與漏洞

計算 Web 應用程式平台漏洞會比計算一般 Web 應用程式的漏洞更複雜一些。分析 Web 應用程式平台時，我們發現將基礎平台與 Web 應用程式平台使用的外掛程式區分開來會很有幫助。外掛程式未必是由 Web 應用程式供應商本身製作。雖然外掛程式擴充 Web 應用程式平台的功能，但可能缺乏嚴謹的編碼，或者其更新的速度趕不上所支援的平台。最重要的是：絕大多數的漏洞都發生於外掛程式中。

圖 44 顯示 2010 上半年主要 Web 應用程式平台，以及其外掛程式漏洞揭露的百分比。我們只列入含十個以上揭露漏洞的 Web 應用程式平台及相關外掛程式。

兩者合計，主要 Web 應用平台及其外掛程式，在 2010 上半年所有通報的漏洞揭露中，佔了將近 14%。

根據觀察，與 Web 應用程式平台有關的揭露漏洞大多屬於外掛程式 (88%)，而 Web 應用程式平台本身只佔 12%。

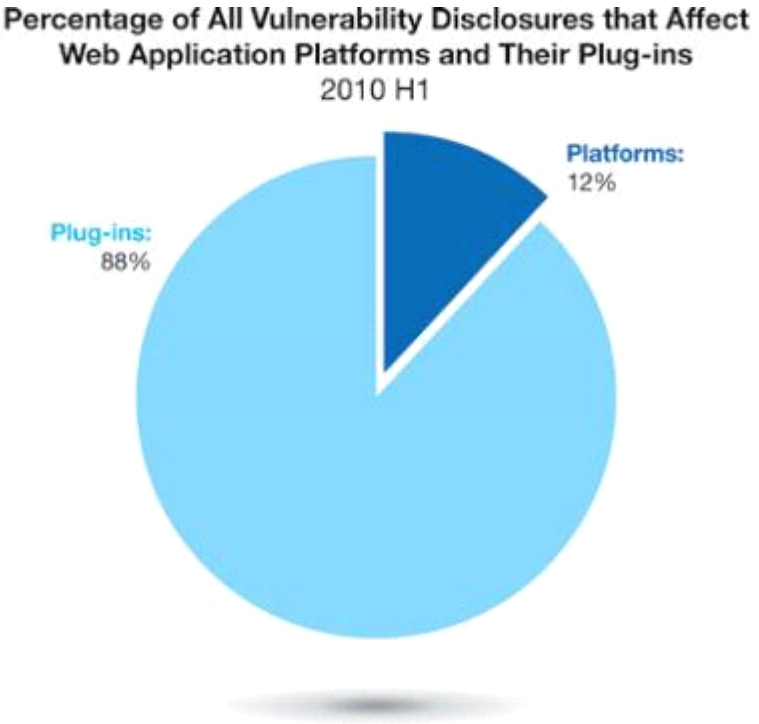


*圖 44：*2010 上半年影響 Web 應用程式平台及其外掛程式所有漏洞揭露的百分比。

下圖顯示外掛程式與 Web 應用程式平台揭露漏洞的相對計數。

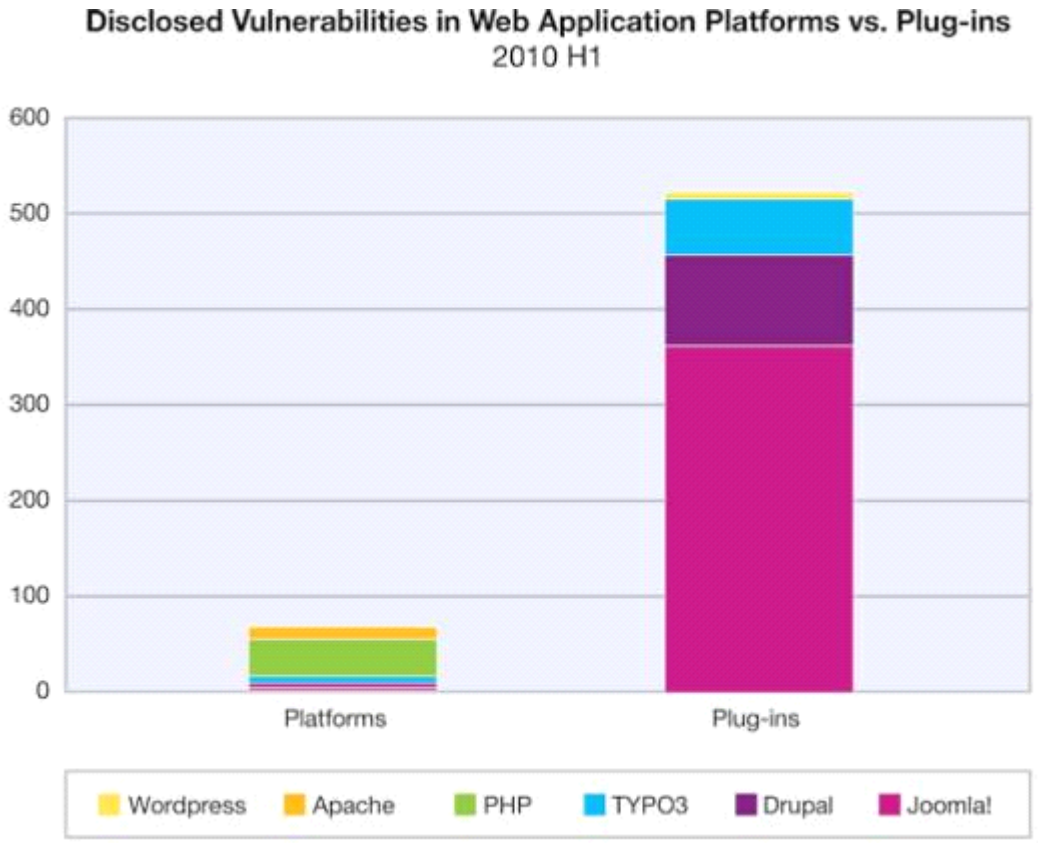


圖 45： 2010 上半年 Web 應用程式平台與外掛程式中的揭露漏洞

我們可以從中學到什麼？

雖然 Web 應用程式供應商很少有漏洞是起因於他們所製作的程式碼，但如果您的組織相當依賴眾多支援這些應用程式的外掛程式，最好花一些時間來調查，並補救任何揭露的漏洞。最好的方法是：部署前先使用 Web 應用程式掃描器充分評估成品，確保不存在任何未揭露的漏洞，而且開發過程中並未出現新漏洞。確保應用程式的安全後再予以部署，這樣做可防止您的網站成爲駭客的跳板。

瀏覽器與其他用戶端的漏洞與弱點攻擊

熱門用戶端軟體 - 重大與高嚴重性漏洞揭露百分比

回顧 2009 年終報告，該年用戶端漏洞與 2008 年相比下降了 5%。儘管如此，影響個人電腦的漏洞仍然排在 Web 應用程式漏洞之後，是第二大類的漏洞揭露，佔了所有漏洞揭露的五分之一左右。

圖 46 環顧各類型的用戶端應用程式，呈現目前重大與高嚴重性類別的明細。

2009 年中到年底可見到圖表呈現下降趨勢（提醒您這只是爲期六個月的資料）。2010 上半年可見到：文件讀取器與編輯器以及多媒體應用程式，幾乎超過 2009 年底的總數。今年，瀏覽器應用程式掉到只剩一半，預計這個趨勢將會持續下去。如果 2010 年繼續維持高漏洞揭露數，預計年底這些領域將會創下新紀錄。

如同我們在前幾個小節討論到的，攻擊者正積極利用這些創下紀錄的揭露數量，可見未來還是會出現許多重大安全問題。

影響用戶端的主要漏洞，可分成四個主要類別（如表 12 所示）。

種類	說明
瀏覽器	用戶端 Web 瀏覽器軟體與外掛程式。
文件讀取器與編輯器	允許使用者建立或檢視文件、試算表、簡報和其他類型檔案的軟體（影像、音樂、電影除外）。
多媒體	允許使用者檢視或建立音樂及電影的軟體。
作業系統	基本作業系統，不包括其他三個類別中的應用程式。

*表 12：*用戶端漏洞揭露的相關主要漏洞類別

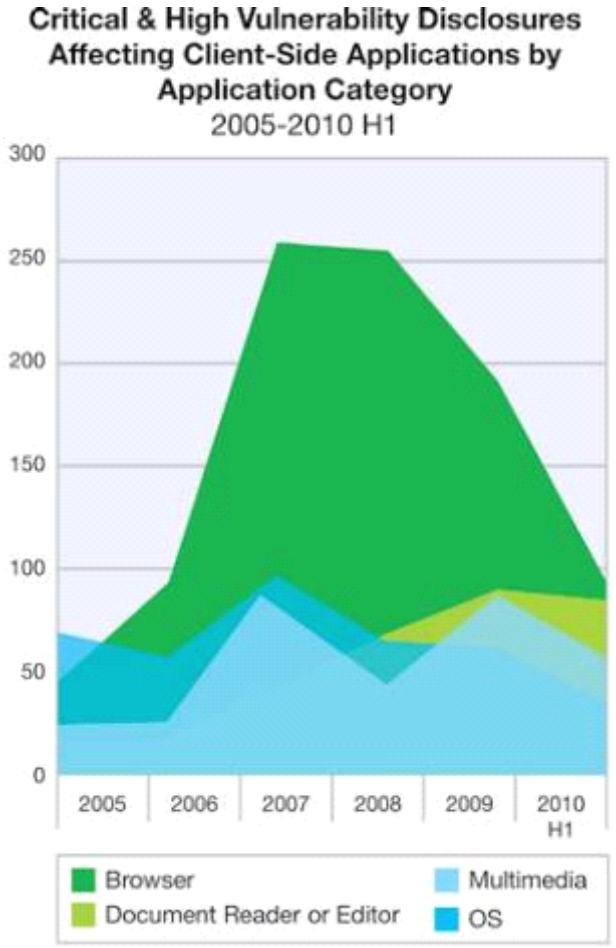


*圖 46：*2005-2010 上半年影響用戶端應用程式的重大與高嚴重性漏洞揭露（按應用程式分類）

瀏覽器漏洞 - Internet Explorer 在 2010 年遙遙領先

瀏覽器類的用戶端漏洞仍舊是數量最多的類別。此類別不僅包括瀏覽器本身，也包含許多可安裝在瀏覽器上的外掛程式。我們看到受影響的 ActiveX 控制項呈現下降趨勢。

如同我們所預期的，無論 Mozilla Firefox 或 Microsoft Internet Explorer，在 2010 上半年的揭露數量都有增加。在這方面，兩種瀏覽器相對都有各自的揭露，不過今日看來，Internet Explorer 已輕鬆達到 2009 年瀏覽器通報總數的三分之二。

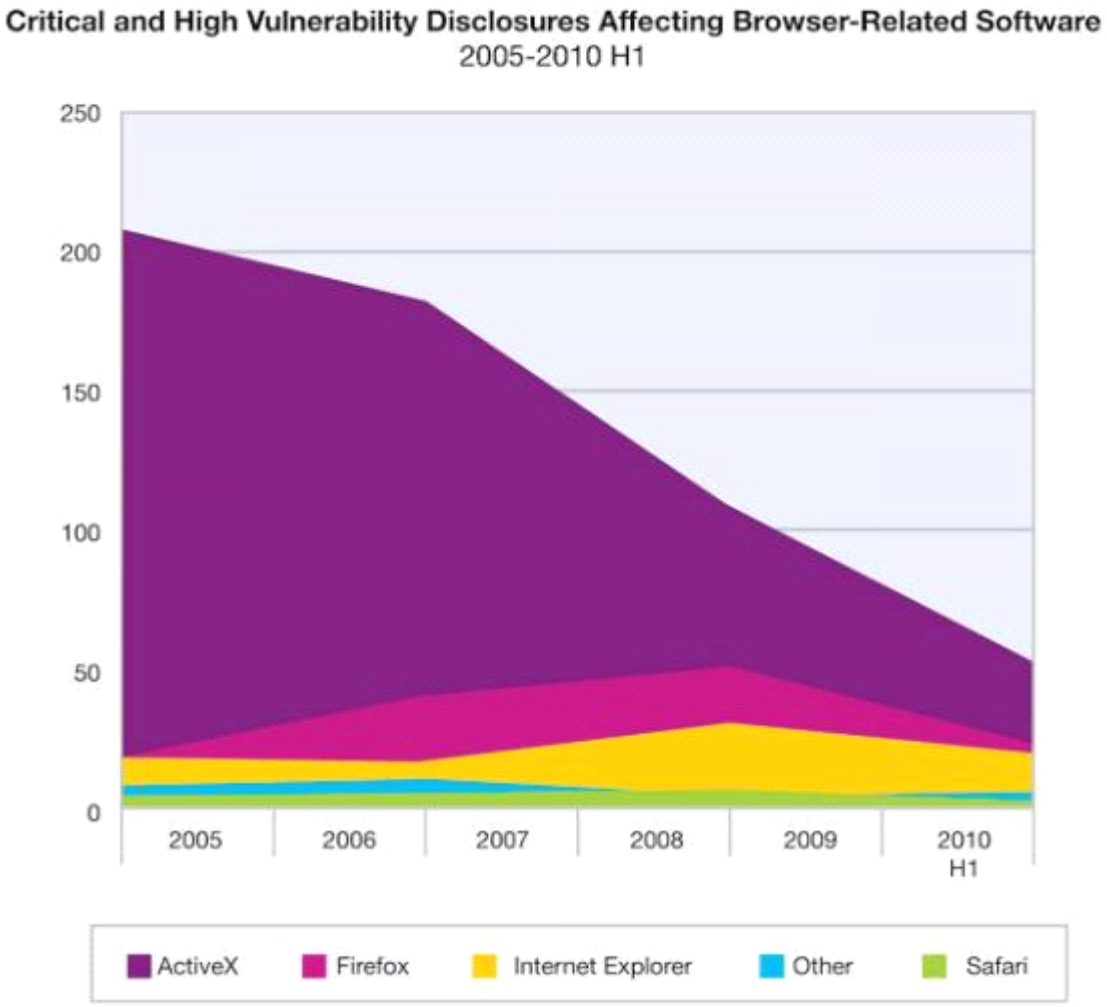


圖 47： 2005-2010 上半年影響瀏覽器相關軟體的重大與高嚴重性漏洞揭露

文件格式漏洞

在文件漏洞方面，最盛行的兩種文件漏洞種類可想而知，分別爲：Office 文件與可攜式文件格式 (PDF) 文件。

目前 PDF 在今年年中的漏洞約佔 2009 年終總數的 49%。下圖 48 中可見到 Office 文件漏洞數量正在下降，而 PDF 漏洞則持續上升。

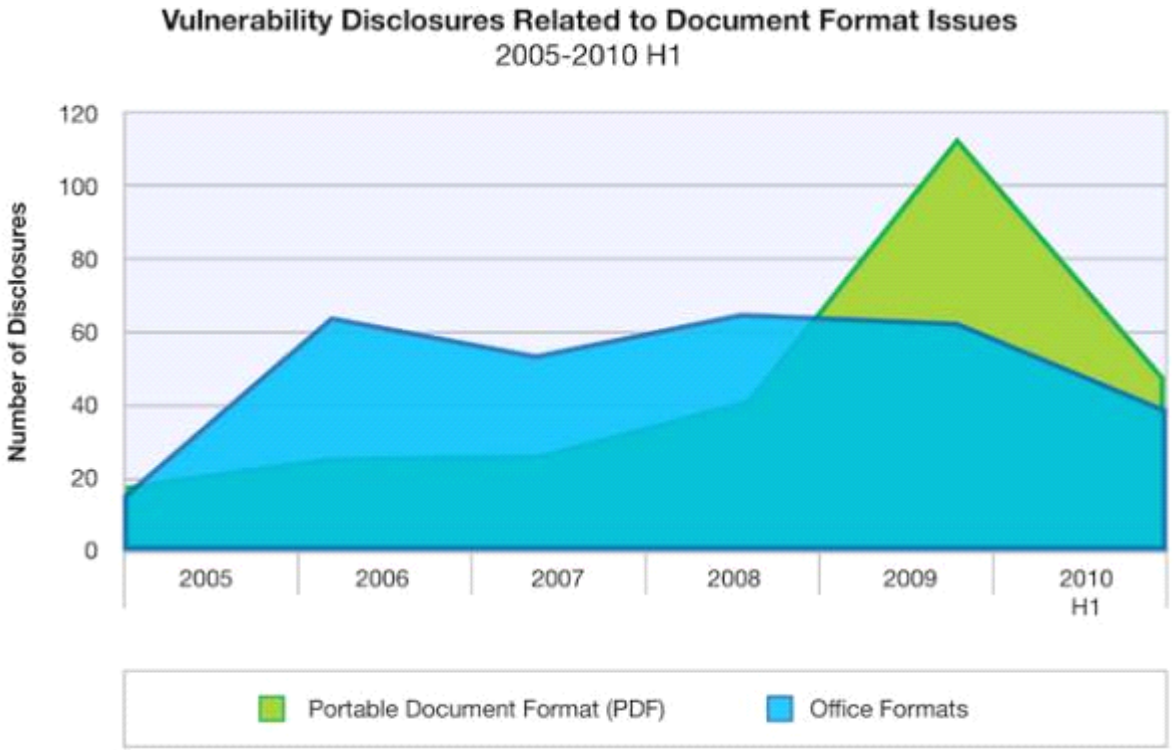


圖 48： 2005-2010 上半年文件格式的相關漏洞揭露

縱觀此威脅趨勢，我們曾報導過 PDF 已成爲許多攻擊者的首選武器。我們的感應器偵測到今年 2 月份出現一波攻擊 - 附帶混碼 PDF 附件的垃圾郵件利用 Acrobat 漏洞安裝惡意軟體。我們的研究人員在部落格討論到這種結合不同方法以避開當前防毒軟體與垃圾郵件過濾器的攻擊。今年 4 月，我們的感應器偵測到另一波惡意 PDF 垃圾郵件顯著激增。這波攻擊使用 Javascript Launch 指令，在受害者的電腦上安裝 Zeus 傀儡網路。

我們提醒安全專家應該對這類方法保持警惕，並讓使用者了解這些文件可能構成的威脅。

用戶端弱點攻擊趨勢

X-Force 透過數個專案和服務，監測用戶端的弱點攻擊。

- IBM Managed Security Services (MSS) 負責監測端點、伺服器（包括 Web 伺服器）以及一般網路基礎架構的弱點攻擊。這類資料會追蹤透過 Web 進行的弱點攻擊，也包括其他媒介，例如電子郵件和即時傳訊。
- 我們的「Whiro」搜索器結合 MSS（我們的 C-Force）的警示資料與獨立分析，監測 Web 來源的弱點攻擊。Whiro 使用專門技術，甚至可以辨識高度混碼的弱點攻擊，包括工具箱嘗試多個弱點攻擊的情況。
- 我們的內容團隊透過編目、獨立探索，以及 MSS 和 Whiro 提供的摘要，獨立搜尋並分類網頁。

Web 瀏覽器弱點攻擊趨勢

X-Force 透過 Whiro 搜索器與 IBM Managed Security Services 作業警示資料的分析，持續追蹤 Web 瀏覽器弱點攻擊的成長。我們決定製作類似的 Web 弱點攻擊工具箱普及率統計時，我們了解這雖然可做到但不容易完成（因爲這涉及到程式碼相似度與程式碼竊取）。隨著時間的推移，我們也持續追蹤個別弱點攻擊以及 Web 瀏覽器弱點攻擊工具箱中使用混碼技術的趨勢。我們會繼續投資新技術，改善我們在這個領域中的成果。

正當四處流竄的單獨 Web 瀏覽器弱點攻擊日漸式微，弱點攻擊工具箱與群組逐漸躋身 Web 瀏覽器弱點攻擊的前列，我們見到反分析的領域中，出現了一些令人不安的因素。四處流竄的弱點攻擊套件不止一次阻止特定網際網路通訊協定 (IP) 位址取得服務內容，而且次數越來越多。此功能對攻擊者而言有兩個實際益處：1) 感染只會發生一次，可防止受害者呈現不穩定的狀態；2) 阻礙分析。這種過濾方法並非全新，參照位址檢查也非新方法，只是重新浮上檯面而已。藉由封鎖缺乏有效參照位址的要求（如被入侵網頁的 URL 或惡意廣告），只分享惡意 URL，這麼做並不足以取得惡意樣本。

2010 上半年最常見的弱點攻擊

1. CVE-2007-5659, PDF Collab.CollectEmailInfo
2. CVE-2009-0927, PDF getIcon
3. CVE-2008-2992, PDF Util.Printf
4. CVE-2007-0071, SWF Scene Count
5. CVE-2008-5353, Java Object Deserialization

廣爲流傳的 Gumblar 弱點攻擊工具箱/群組，能佔據有利的位置，對 Adobe 產品發動弱點攻擊，而 PDF 和 Flash 弱點攻擊在許多其他弱點攻擊工具箱也十分常見。另一項 2009 下半年的變化也相當有趣：ActiveX 已退出前五名之列（至少目前如此）。在 2009 全年報告中，我們預計 Adobe 產品仍舊會榜上有名，但並未明確表示 PDF 或 Flash 之間哪個佔得比較多。根據 2010 年到目前爲止的觀測，我們可以肯定地說：PDF 弱點攻擊在 2010 年將會延續它的主導地位。

此外，某個較舊的 Java 漏洞意外進入前五名的底部。考慮到 Java、PDF 與 Flash 在不同瀏覽器環境中仍舊能維持一致性，顯然攻擊者會對誘捕「非 IE 瀏覽器」使用者比較感興趣，這樣他們就不需要投入時間和金錢於特定瀏覽器的攻擊。攻擊者會進一步鎖定主要瀏覽器供應商，利用他們逐漸減弱的修補週期，但不一定會鎖定瀏覽器與跨瀏覽器的外掛程式供應商。2010 年，X-Force 預測瀏覽器外掛程式供應商會開始解決零時差攻擊，而且速度將遠遠超過過去。然而，如果電腦使用者不使用自動更新功能、通知，或手動嚴格管理修補狀態，即使修補程式加快進入市場的速度，仍舊毫無助益。

2010 上半年最常見的弱點攻擊工具箱

1. Gumblar
2. Fragus
3. Eleonore
4. Phoenix
5. JustExploit

將弱點攻擊套件普及率製成表格並不是件容易的事。程式碼相似度、具有獨特混碼的套件分支，這類長期存在的問題使這項任務更加困難。我們判定普及率的方法是：將啓發法應用到去除混碼的惡意內容中。雖然 X-Force 對結果很有信心，但我們也承認：弱點攻擊搜索器在偵測最新 Neosploit 套件時遇到一些困難。我們估計：Neosploit 應該介於 Eleonore 與 Phoenix 之間，這也造成 JustExploit 掉到名單之外。回顧 2009 年中與全年最常見的弱點攻擊工具箱的調查結果，可見到 Gumblar 仍舊佔據主導的地位。

新套件 Fragus 已飆升至第二名，而 Eleonore 已從 2009 下半年的第五名，躍升至 2010 上半年的第三名。Phoenix 仍舊榜上有名，不過這是一整年延續下來的結果，並非只計算下半年。本趨勢報告的忠實讀者可能會注意到：受攻擊者青睞的工具箱呈現不小的流失量。因此，嘗試預測 2010 全年結果可能不太容易。X-Force 認爲 Gumblar 仍舊會佔據工具箱的首位，而且如同先前所提到的，我們也預計 JustExploit 將會從榜

上除名。然而，另外三個工具箱可能還是會很吃香，不過如果有其他工具箱出現，其中一、兩個可能會默默退出舞臺。

Web 內容趨勢

本章節將概述有違社會原則與企業政策的「不當」Web 內容數量與分佈。不受歡迎或「不當」網際網路內容與三種類型的網站有關：IBM Web 過濾器種類會對應到這些網站類型。

Web 過濾器種類的詳細定義請見：**http://www-935.ibm.com/services/us/index.wss/detail/iss/a1029077?cntxt=a1027244**

本節提供下列分析：

- 視爲不當、不必要的 Web 內容百分比與分佈
- 匿名 Proxy 數量增加
- 網頁暗藏連到惡意 URL 的鏈結

網站類型	說明與 Web 過濾器種類
成人	色情 情色/性愛
社會偏差	政治極端/仇恨/歧視 教派
犯罪	匿名 Proxy 電腦犯罪/駭客入侵 違法活動 違法藥物 惡意軟體 暴力/極端 盜版軟體/軟體盜版

表 13： Web 過濾器種類與對應的不當 Web 內容

分析方法

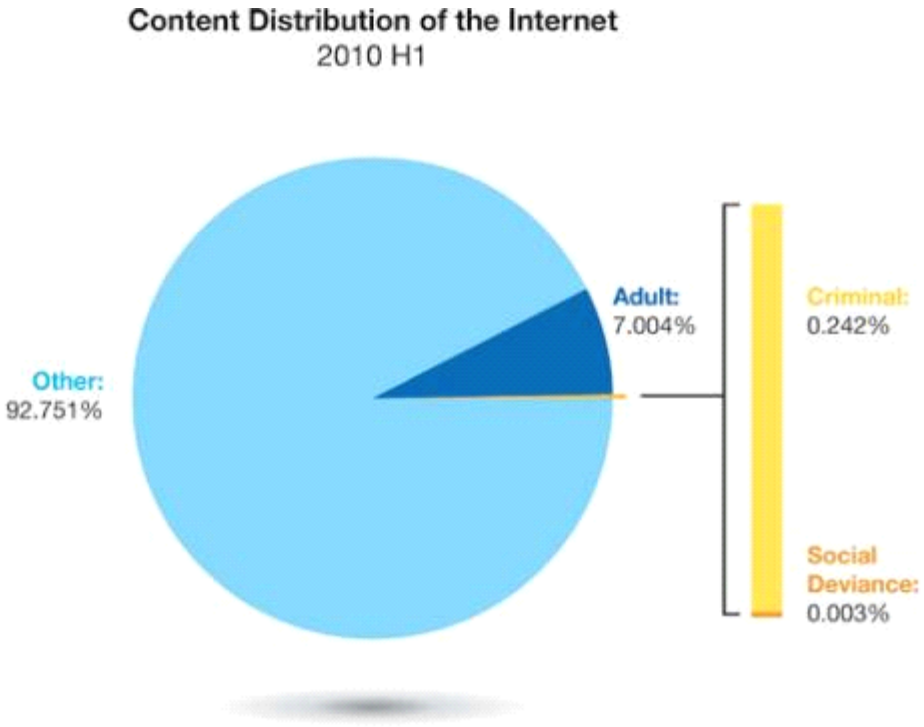
X-Force 計算 IBM 安全解決方案 Web 過濾資料庫所分類的主機，來掌握網際網路上內容分佈的相關資訊。計算主機是種可接受的方法，能用於判斷內容分佈並提供最實際的評估。若採用其他方法（像是計算網頁與子頁面）結果可能有所不同。

IBM 內容資料中心持續審閱並分析新的 Web 內容資料。IBM 內容資料中心每月分析 1 億 5 千萬個新網頁與影像，自 1999 年來已分析 130 億個網頁與影像。

IBM Web Web 過濾資料庫具備 68 種過濾器以及 6500 萬筆項目，每天增加 15 萬筆全新或更新項目。

不當網際網路內容百分比

網際網路目前約有 7.2% 的不當內容，例如色情或犯罪網站。



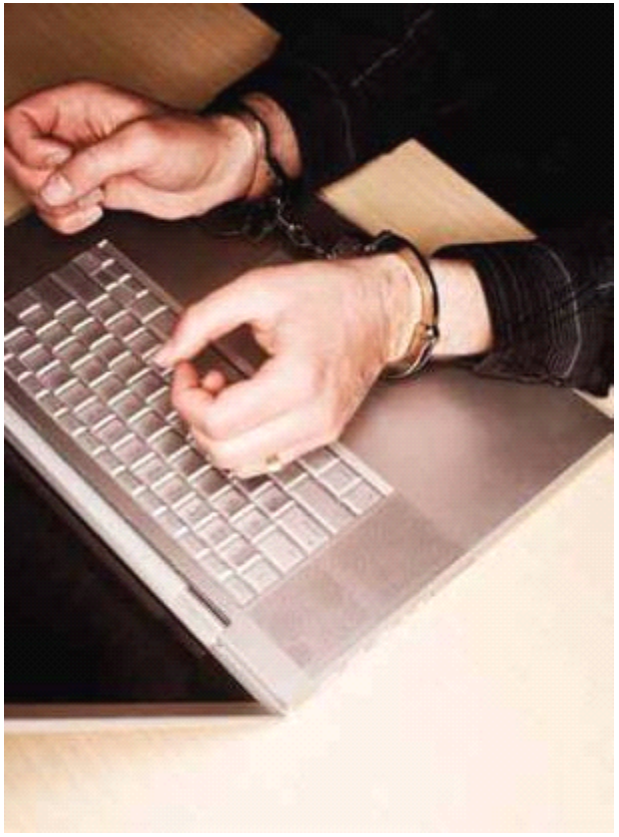


*圖 49：*2010 上半年網際網路內容分佈

匿名 Proxy 增加

網際網路不僅成爲家中不可獲缺的一環，對於工作與學校也是如此，因此負責維護理想環境的組織，逐漸覺得有必要控制人們在公共場合所瀏覽的內容。

內容過濾系統是控制方式之一，可預防存取不被允許或不當的網站。有些人嘗試用匿名 Proxy（也稱爲 Web Proxy）以規避網頁過濾技術。

Web Proxy 讓使用者得以在 Web 表單輸入 URL，不用直接造訪目標網站。利用 Proxy 會讓 Web 過濾器無法發現目標 URL。如果沒有設定 Web 過濾器，要求監控或封鎖匿名 Proxy，則原本會被阻止的這項活動，就會避開過濾器，讓使用者得以連到不允許的網頁。

匿名 Proxy 網站數量的增加（如圖 50 所示）反映出這項趨勢。

過去三年來，匿名 Proxy 穩定成長，在數量上翻了四倍之多。匿名 Proxy 讓人得以輕鬆隱匿潛在的惡意內容，因此追蹤這類網站顯得十分重要。

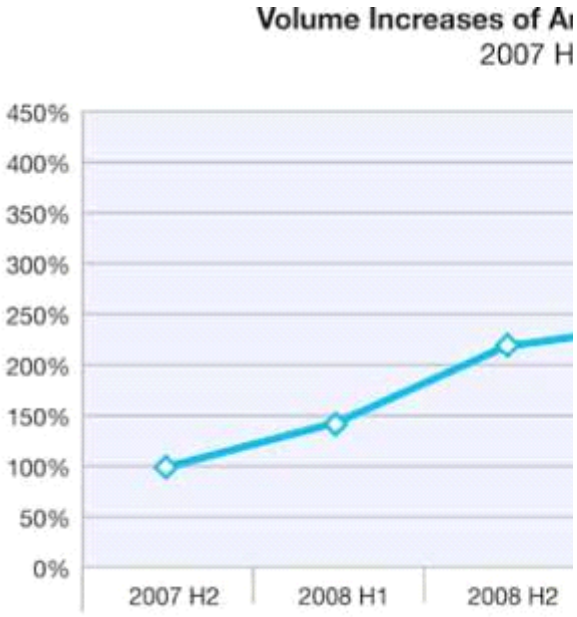


*圖 50：*2007 下半年到 2010 上半年的匿名 Proxy 網站數量增加

匿名 Proxy 的最上層網域

圖 51 顯示新註冊匿名 Proxy 的最上層網域 (TLD)。

2006 年新註冊匿名 Proxy 有超過 60% 都是 **.com** 網域，但從 2007 年中到 2010 年初則是 **.info** 居冠（**.com** 大部分時間排名第二）。

但爲何 **.info** 會將冠軍位置拱手讓人？多年來 .info 一直是備受肯定的 TLD 匿名 Proxy。原因可能在於：.info 的名稱跟 **.com** 一樣逐漸不敷使用。所以問題來了：爲什麼現在匿名 Proxy 是由 **.cc** 與 **.tk** 最上層網域來提供？

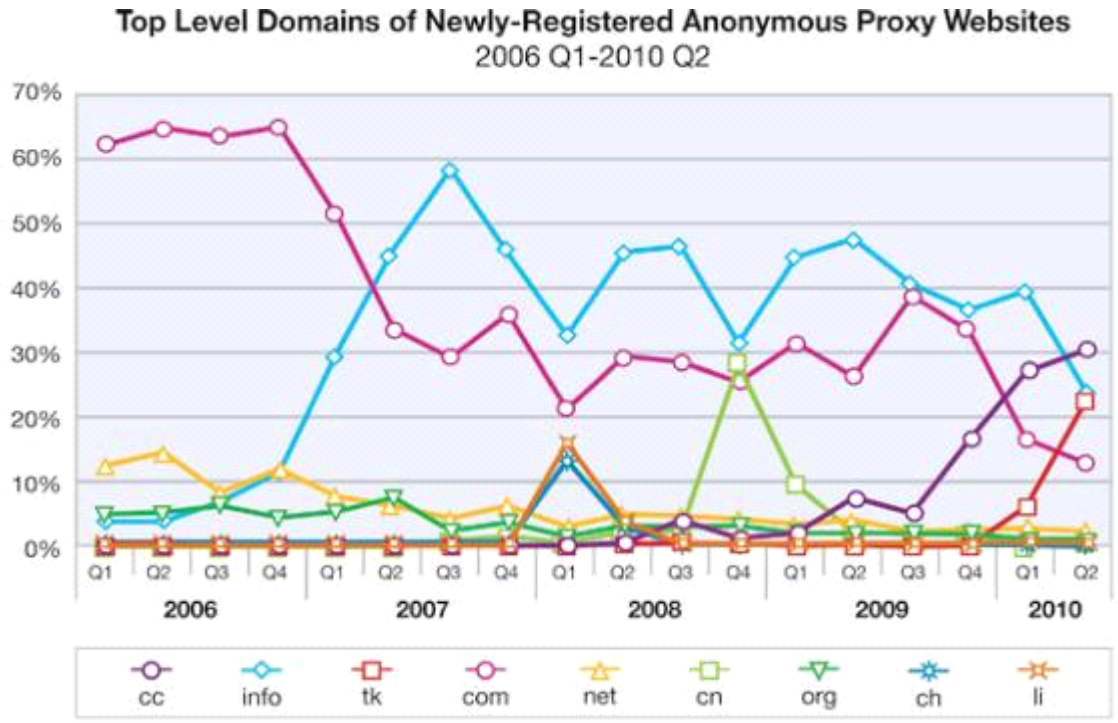


圖 51： 2006 第 1 季到 2010 第 2 季新註冊匿名 Proxy 網站的最上層網域

這些網域分屬可可群島（**.cc**，澳洲領土），以及托克勞群島（**.tk**，紐西蘭的領土）。網域 **.cc** 是由 VeriSign 所管理。幾乎所有 **.cc** 匿名 Proxy 網站都是在網域 **.co.cc** 上註冊。註冊任何 **.co. cc** 網域是免費的（請參閱 **http://www.co.cc/?lang=en**）；**.tk** 也是如此（請參閱 **http://www.dot.tk/**）。因此，在 **.co.cc** 或 **.tk** 上安裝新的匿名 Proxy 費用低廉，而且極具吸引力。

其他趨勢：

- 2008 年初，瑞士 (**.ch**) 與列支敦斯登 (**.li**) 這兩個相鄰國家的最上層網域相加便佔了新註冊匿名 Proxy 的 30%。
- 2008 年第 4 季，中國最上層網域佔了新註冊匿名 Proxy 近 30 %。
- 2009 年底，**.cc**（可可群島）開始大量增加；2010 年第 2 季甚至升到第一名。
- 2010 年第 2 季，另一個 Proxy 天堂的新星 **.tk**（托克勞群島），在新匿名 Proxy 中佔了 23% 左右。
- 同一時期 **.info** 急劇下降；2007 年以來首次低於 30%。
- 2010 年第 1 季，甚至連 **.com** 都首次低於 20%。

匿名 Proxy 網站發源國

在匿名 Proxy 發源國方面，美國蟬聯數年冠軍。四年半以來，新註冊匿名 Proxy 超過 70% 都位於美國。這個百分比從 2008 年中至 2009 年底攀升到 80% 以上。2010 上半年，所有新註冊匿名 Proxy 大約 75% 都位於美國。

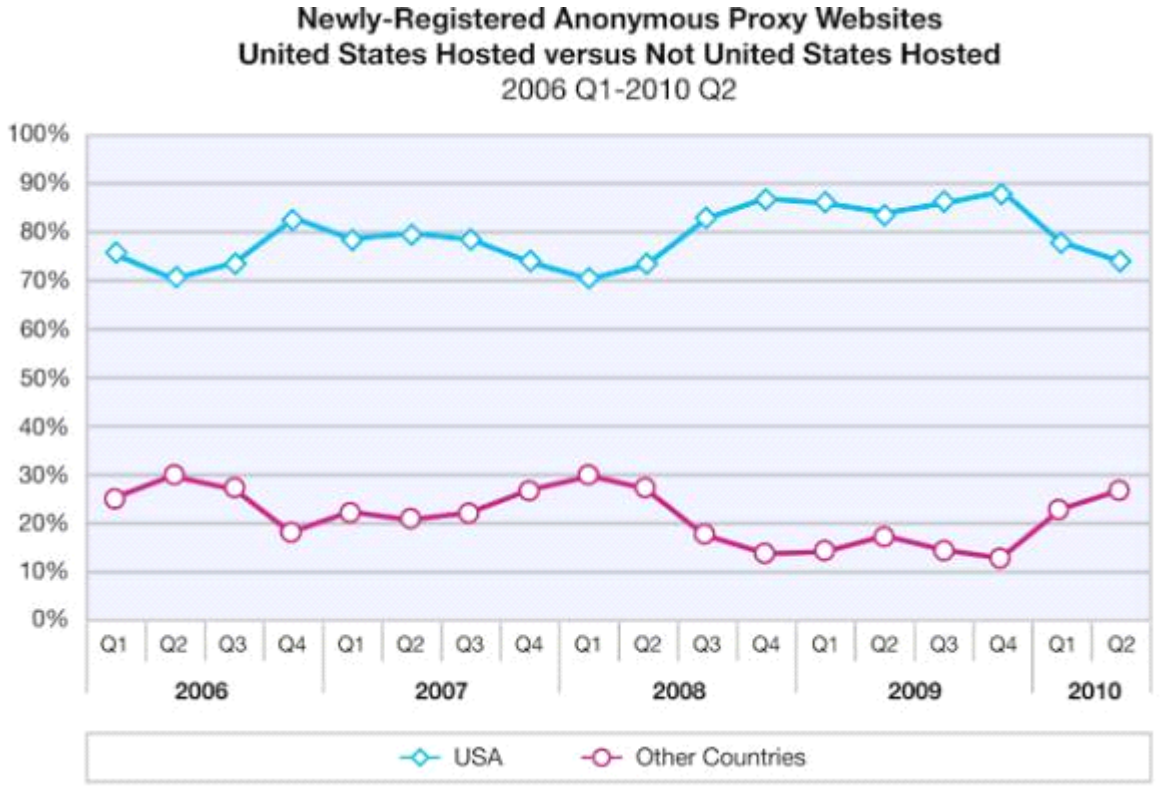


圖 52： 2006 第 1 季到 2010 第 2 季發源自美國與其他國家的新註冊匿名 Proxy 網站

2010 上半年所有新註冊匿名 Proxy 中，剩下的 25% 也值得我們關注。剩下的匿名 Proxy 中，加拿大在第 1 季佔最多 (7.9%)；第 2 季則是英國佔最多 (7.8%)。2010 年迄今，發源自其他國家的匿名 Proxy 都不到 4%。

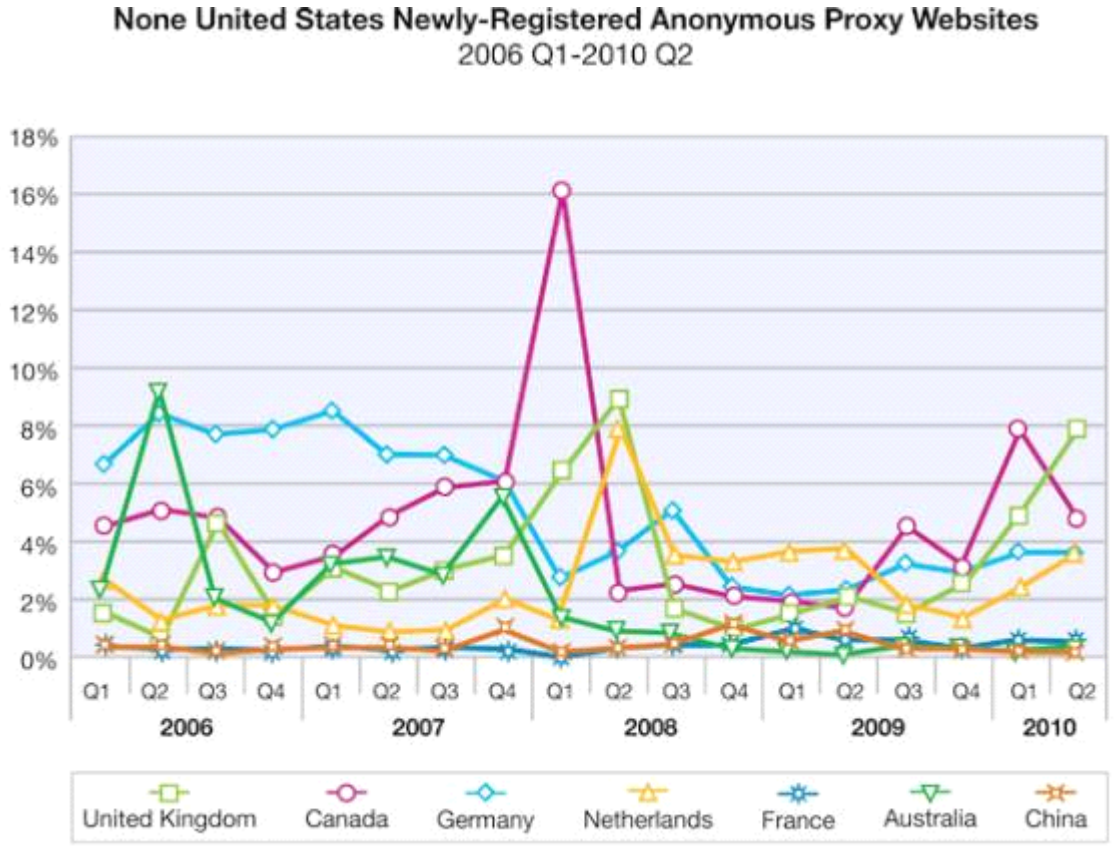


圖 53： 2006 第 1 季到 2010 第 2 季美國以外的新註冊匿名 Proxy 網站

含不當鏈結的正當網站

如同第 71 頁「**Web 應用程式威脅與漏洞**」與第 94 頁「**URL 垃圾郵件常見網域**」所述，愈來愈多攻擊者開始利用受信任網站的好名聲，讓使用者放下心房，並運用混碼來躲過保護技術。惡意 Web 內容的使用情況並沒有改變，我們可以從下列分析一窺最常包含連往已知惡意鏈結的網站類型。

某幾大類可能早在意料之中，例如，一般人可能預期色情會名列前茅，這的確是事實，而且過去 12 個月來狀況變得越來越糟。但在次要的網站類型，卻出現了較爲「受信任的」網站。

部落格、公佈欄、個人網站、搜尋引擎、教育、線上雜誌與新聞網站，都是次要的網站類型；這類網站多半讓使用者上傳內容或自行設計網站，例如大學網站的個人內容，或是購物網站的「購物經驗談」。換句話說，這些類型的網站並非有意成爲惡意鏈結發源地。這樣的分佈可能更能說明攻擊者喜愛光顧的網站類型，目的在於找到可以置入惡意鏈結的缺口（例如漏洞，或是可讓使用者提供內容的區域），以誘騙不疑有他的受害者。

圖 54 列出至少有一個鏈結指回已知惡意網站的最常見網站類型。

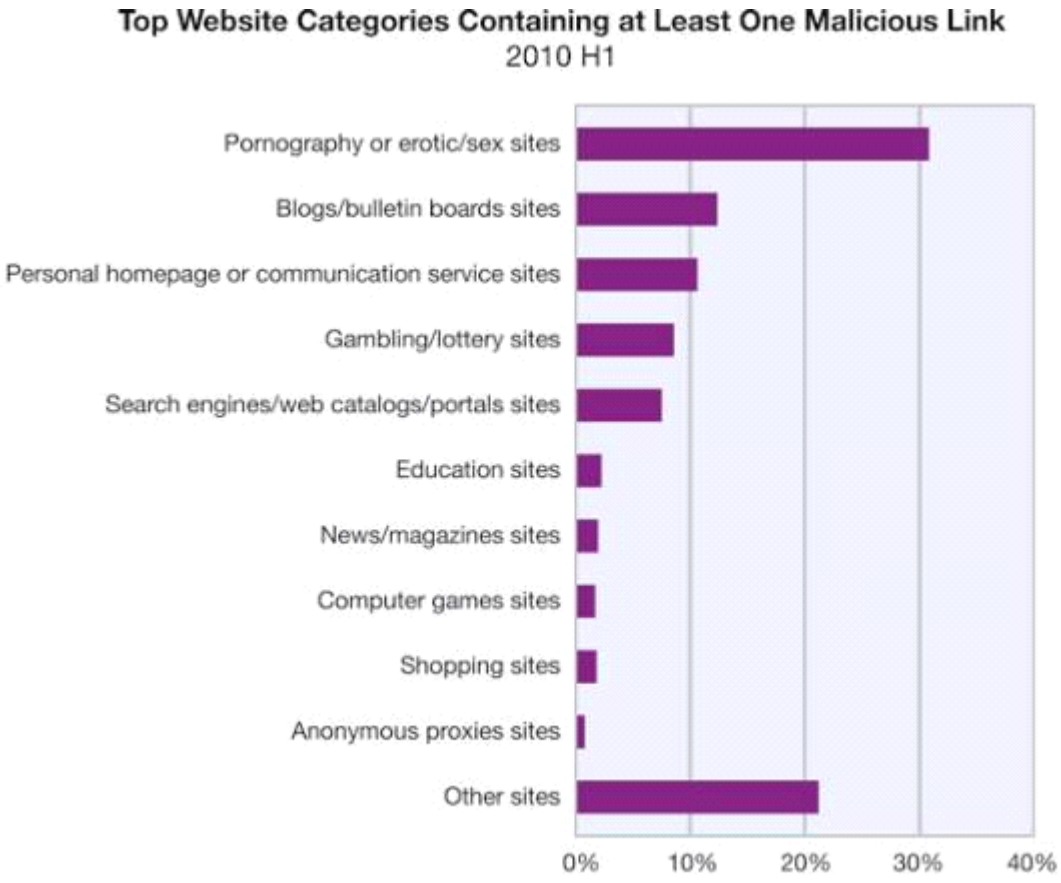


圖 54： 2010 年第 1 季至少包含一個惡意鏈結的前幾名網站類別

參閱圖 55，若將目前資料與 6 個月甚至 12 個月前的資料比較，可發現一些值得注意的趨勢。「不當」專業網站（如色情或賭博網站）連到惡意軟體的鏈結數量逐漸增加，看來似乎是有「專業人士」正努力以有系統的方式散佈惡意軟體。

部落格與公佈欄也可見到惡意軟體鏈結增加；可能是因爲攻擊者的入侵率上升，但部落格或公佈欄的主人並未充分控管。過去 6 個月來，此趨勢已經減緩，但我們注意到電腦遊戲與匿名 Proxy 網站卻呈現上升趨勢。

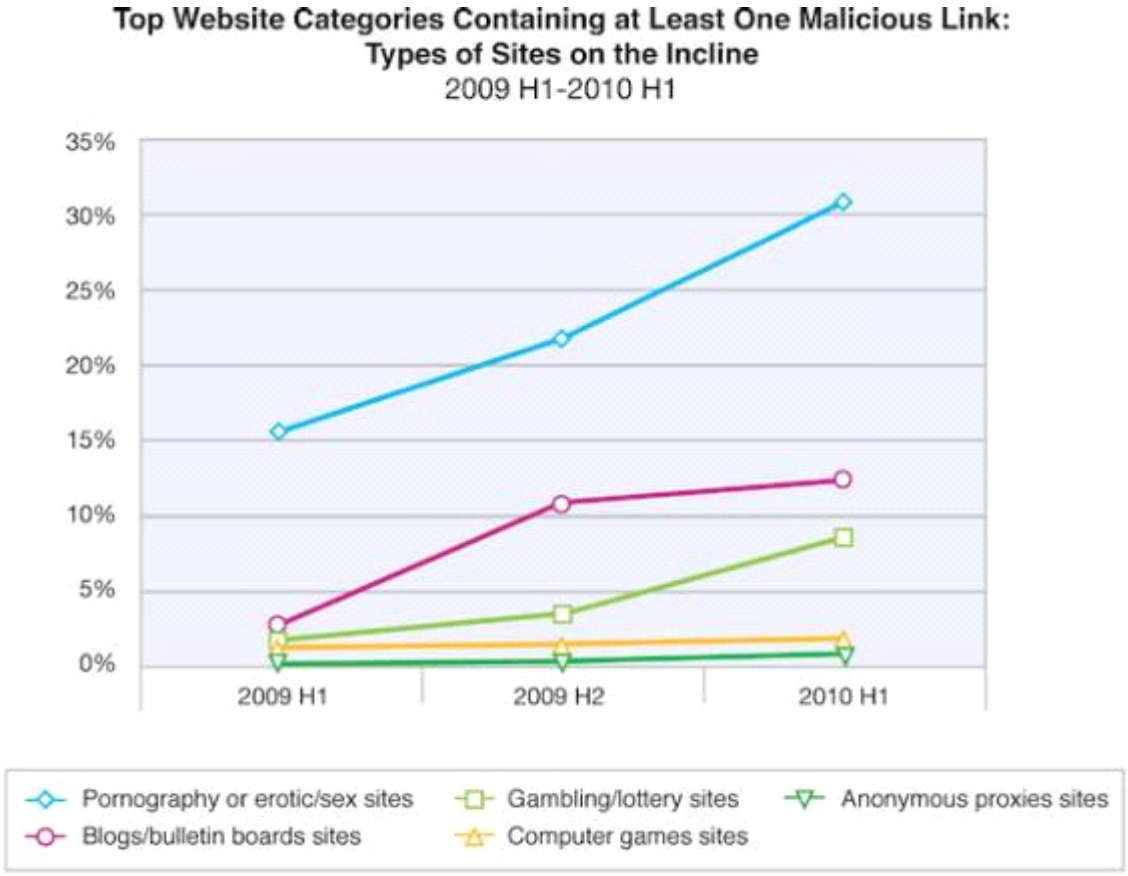


*圖 55：*2009 上半年到 2010 上半年至少包含一個惡意鏈結的前幾名網站類別：呈現上升趨勢的網站類型

至少有一個惡意鏈結的最常見類別已經不包括個人首頁。相較於 2009 上半年，個人首頁已有改善，其中一個原因可能是：與個人首頁及 Web2.0 的應用（如社交與商業網路概況）相比，個人首頁已經過時。搜尋引擎、入口網站，購物網站、教育，以及新聞網站也有所改善。這些「傳統」合法互動網站，多年來一直用於資訊與意見交流。因此這些服務供應商，很可能在 IT 安全方面投入了更多的努力。

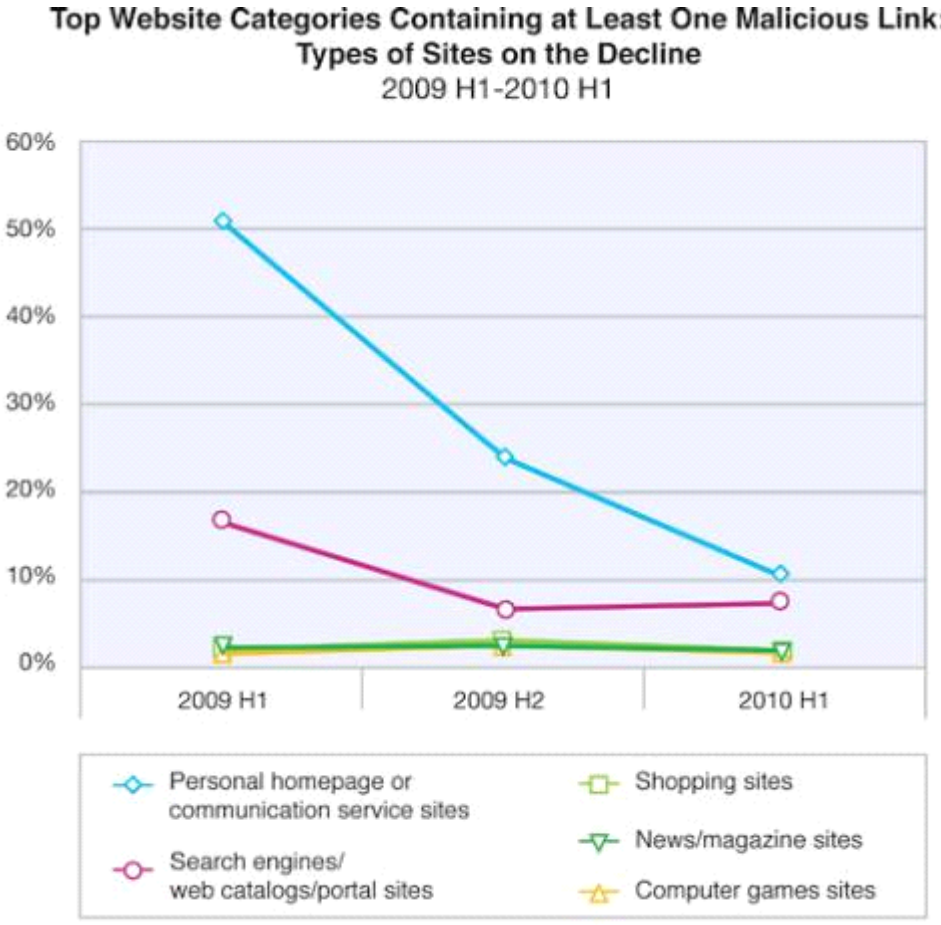


*圖 56：*2009 上半年到 2010 上半年至少包含一個惡意鏈結的前幾名網站類別：呈現下降趨勢的網站類型

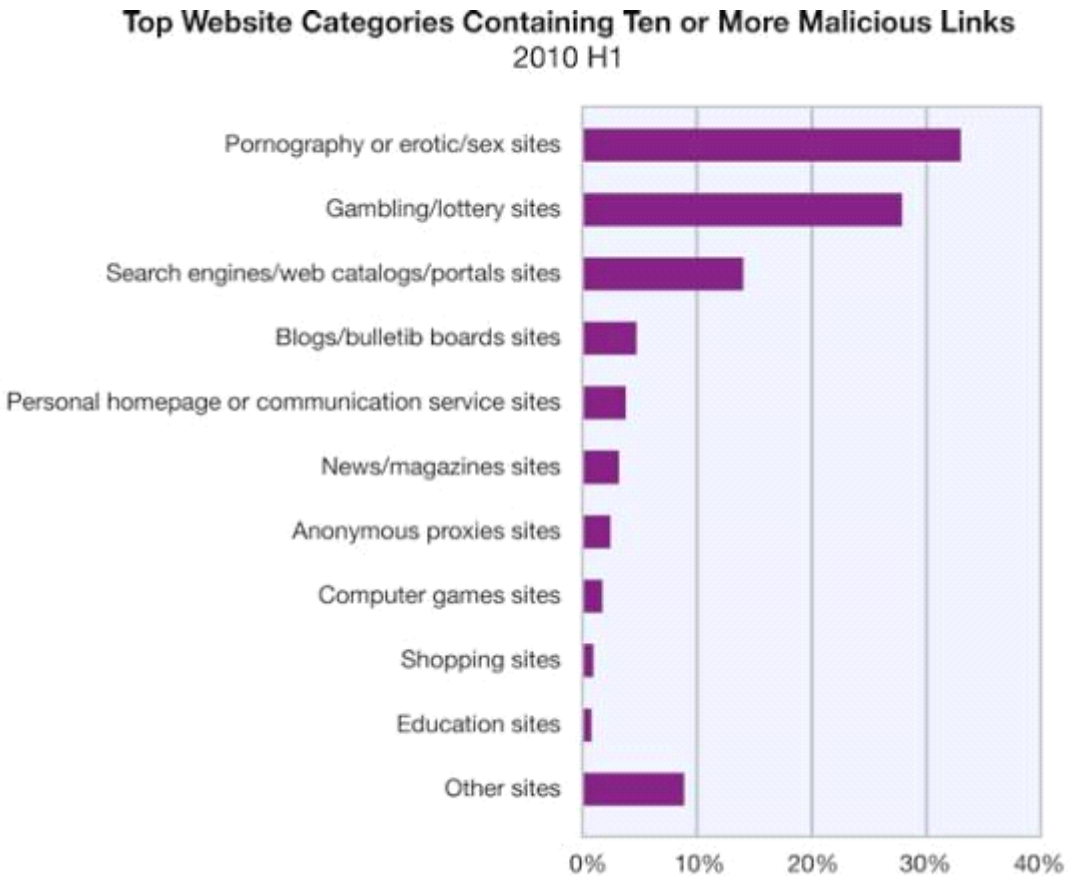


*圖 57：*2010 年第 1 季包含 10 個以上惡意鏈結的前幾名網站類別

研究這個問題的另一種方法是：檢視顯然包含大量惡意網站鏈結的網站。分析包含 10 個以上惡意鏈結的網站後，點出了另一件事實，那就是某些這類網站的經營者，可能也從侵入所帶來的利益分得一杯羹。包含 10 個以上惡意鏈結的網站類別中，色情網站佔了近 33%，賭博網站佔了約 28%。有人可能認爲，這些網站是蓄意利用這類鏈結牟利。某些網站似乎是以有系統的方式，在整個網站置入這類鏈結。

相較於 6 個月前的資料，大多數類別中的數值都出現低於 4% 的變化。但色情網站卻增加了 6%，賭博網站更是增加了 11.4%。因此，惡意軟體逐漸集中於這些網際網路上受歡迎的地下網站。以 0.6% 賭博成癮（請參閱 **http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence**）成年人口爲基礎的賭博網站，一直是惡意軟體散佈的熱門目標。

垃圾郵件

IBM 垃圾郵件與 URL 過濾資料庫，針對垃圾郵件與網路釣魚攻擊提供全方位的觀點。透過對數百萬電子郵件位址的主動監控，內容團隊已辨識出攻擊者所使用的垃圾郵件與網路釣魚技術的多項進展。

目前我們的垃圾郵件與 URL 過濾資料庫包含四千多萬相關垃圾郵件簽章。每封垃圾郵件細分爲數個邏輯部分（句子、段落等）。針對每部分以及數百萬垃圾郵件 URL，計算出一個唯一的 128 位元簽章。每日垃圾郵件過濾資料庫約都有約一百萬個全新、更新或刪除的簽章。

本節主題如下：

- 垃圾郵件量
- 垃圾郵件類型新趨勢
- 垃圾郵件最常用的網域
- 垃圾郵件最常用的最上層網域 (TLD)，以及這些最上層網域熱門的原因
- 垃圾郵件 URL 的名聲
- 垃圾郵件的來源國家[1] 趨勢，包括垃圾郵件網頁 (URL)
- 垃圾郵件平均位元組大小變化
- 垃圾郵件最常見的主旨

垃圾郵件量

2009 年初，垃圾郵件量停滯數月。到了 2009 年 5 月，垃圾郵件量開始增加，逐漸超過 **McColo 關閉**前的水準。

2009 年第 4 季，垃圾郵件發送者又開始重振旗鼓。該年 11 月，他們寄出比 McColo 關閉前多兩倍的垃圾郵件。2010 年，垃圾郵件發送方起初維持穩定的狀態，但到了 4 月，垃圾郵件的數量又開始增加，最後在 6 月達到前所未有的新高點。

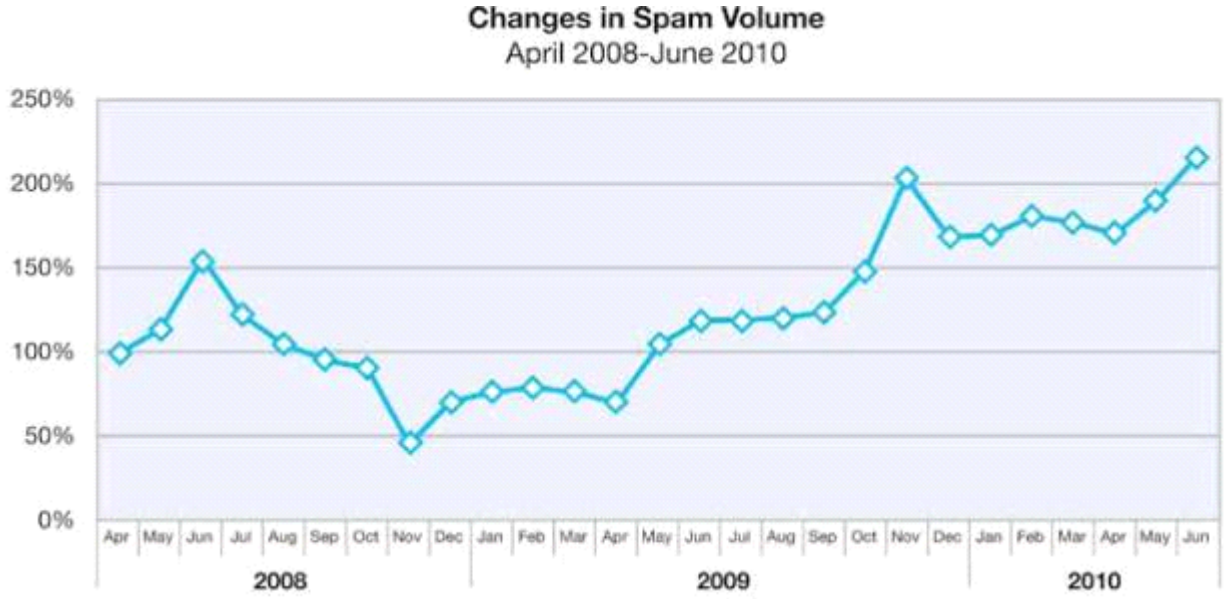


*圖 58：*2008 年 4 月到 2010 年 6 月的垃圾郵件量變化

[1] 本報告的垃圾郵件、網路釣魚與 URL 統計資料，採用 **WebHosting.Info** 所提供的 IP-to-Country Database 資料庫，可從 **http://ip-to-country.Webhosting.info** 取得。地理分佈取決於要求主機 IP 位址（就內容分佈而言）或傳送郵件伺服器主機 IP 位址（就垃圾郵件與網路釣魚而言）至 IP-to-Country 資料庫的主機 IP 位址。

垃圾郵件類型

多年來，垃圾郵件發送者主要利用最不易令人起疑的電子郵件類型，也就是沒有附件的 HTML 垃圾郵件。下圖顯示這類垃圾郵件在 2009 年初呈現大幅增長，而純文字垃圾郵件（無其他電子郵件部分或附件）同一時期則呈現下滑趨勢。

2009 年第 2 季以來，HTML 垃圾郵件一直介於 81-84% 之間。2009 年第 2 與第 3 季，影像垃圾郵件死灰復燃。純文字垃圾郵件從 2009 年底到 2010 年初呈現上升趨勢。同時，影像垃圾郵件逐漸下滑，在 2010 上半年並未造成太大影響。

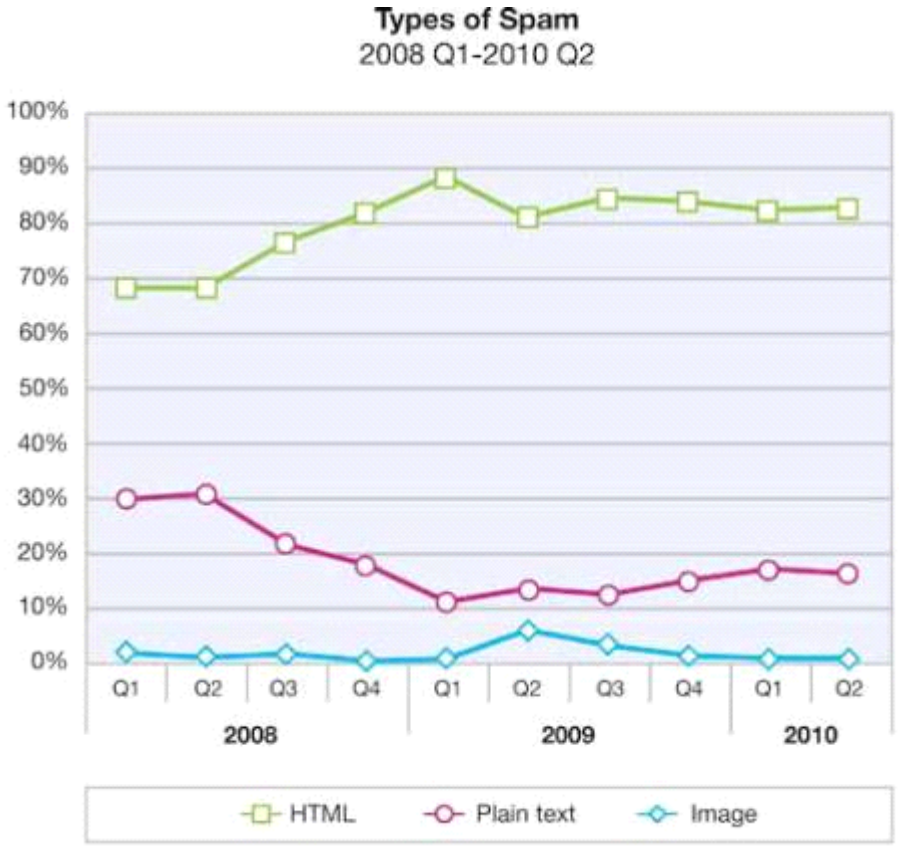


*圖 59：*2008 年第 1 季到 2010 年第 2 季的垃圾郵件類型

URL 垃圾郵件常見網域

多數垃圾郵件（超過 90%）屬於 URL 垃圾郵件，也就是在垃圾郵件訊息中，包含可讓人點選以檢視垃圾郵件內容之 URL。

*圖 60 :*2006 年第 3 季到 2010 年第 2 季的 URL 垃圾郵件

URL 垃圾郵件最常用的網域名稱，值得進一步觀察。表 14 顯示 2010 上半年每月前十大網域。我們會特別強調知名網域、已註冊很長一段時間的網域，以及不是專爲裝載垃圾郵件內容而註冊的網域。

排名	2010 年 1 月	2010 年 2 月	2010 年 3 月	2010 年 4 月	2010 年 5 月	2010 年 6 月
1.	flickr.com	radikal.ru	liveflestore.com	liveflestore.com	imageshack.us	imageshack.us
2.	imageshack.us	imageshack.us	imageboo.com	imageshack.us	imageshost.ru	imageshost.ru
3.	radikal.ru	liveflestore.com	radikal.ru	imageshost.ru	myimg.de	pikucha.ru
4.	liveflestore.com	flickr.com	imageshack.us	imgur.com	xs.to	imgur.com
5.	Webmd.com	live.com	googlegroups.com	myimg.de	imgur.com	myasvir.com
6.	picsochka.ru	imageboo.com	live.com	xs.to	tinypic.com	mojoimage.com
7.	live.com	capalola.biz	akamaitech.net	icontact.com	liveflestore.com	myimg.de
8.	superbshore.com	feetorder.ru	gonestory.com	tinypic.com	icontact.com	twimg.com
9.	tumblr.com	laughexcite.ru	bestanswer.ru	live.com	googlegroups.com	icontact.com
10.	fairgreat.com	hismouth.ru	wrotelike.ru	binkyou.com	images-amazon.com	twitter.com

表 14 : 2010 上半年 URL 垃圾郵件的最常見網域

其中大多數都是知名且受信任的網域名稱，延續了過去幾年的趨勢。圖 61 顯示 2008 上半年到 2010 上半年，垃圾郵件前十大網域中「垃圾郵件網域」與「受信任網域」的百分比。

部分知名網站包括：

- **akamaitech.net**（Akamai Technologies 的網站）
- **googlegroups.com**（Google 提供的免費服務，讓一群人可以討論共同的興趣）
- **icontact.com**（電子郵件行銷服務公司）
- **images-amazon.com**（Amazon.com, Inc. 所擁有的網域）
- **live.com**（Windows Live 服務之一，允許使用者建立個人化首頁）
- **livefilestore.com**（Microsoft 的 Web 儲存服務）
- **tumblr.com**（部落格平台）
- **twimg.com**（Twitter 所擁有的網域）
- **twitter.com**（Twitter 的網站）
- **Webmd.com**（WebMD Health Corporation 的官方網站，美國的健康資訊服務供應商）

鎖定的主要圖片空間網站是：

- **flickr.com**（Flickr 官方網站）
- **imageshack.us**（ImageShack 官方網站）

另外還有一些小型與中型的圖片空間網站：

- **imageboo.com**
- **imageshost.ru**
- **imgur.com**
- **mojoimage.com**
- **myimg.de**
- **mytasvir.com**
- **pikucha.ru**
- **radikal.ru**
- **tinypic.ru**
- **xs.to**

上述網站不僅提供知名度高（又值得信任）的 Web 鏈結給使用者，垃圾郵件訊息也可在垃圾郵件中利用這些合法鏈結，成功躲過某些反垃圾郵件的技術。

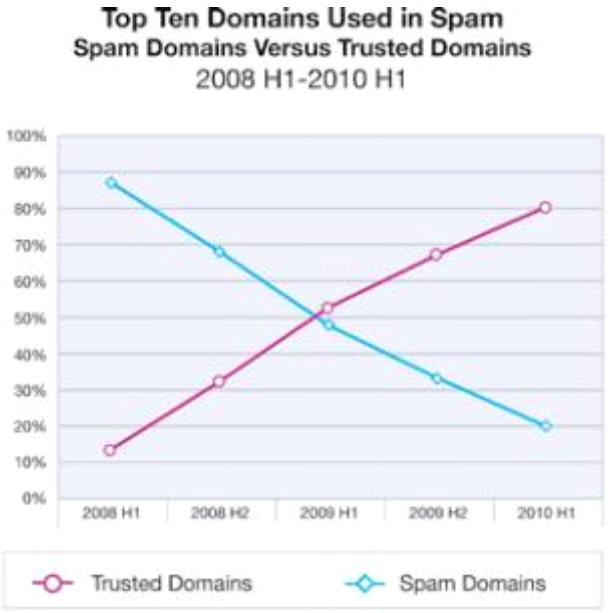


*圖 61：*2008 上半年到 2010 上半年垃圾郵件前十大網域中，垃圾郵件網域及受信任網域的比較

每個最上層網域隨機 URL 的百分比

在前面的章節中，我們討論了最上層網域 (TLD) 從中國移到俄羅斯，可能是因爲中國對註冊網域名稱訂定了更嚴格的限制。進一步探討這個主題前，我們先來談談使用隨機命名結構的最上層網域。

就最上層網域而言，在通用最上層網域（如 **.com** 與 **.net**）與國家最上層網域之間，有個值得注意的現象，垃圾郵件發送者可運用許多技術，讓他們發送的訊息看起來更合法。其中一個技術是使用合法的隨機網域名稱（如 **ibm.com**）。許多情況下，這些合法 URL 隱藏在電子郵件的 HTML 原始碼內。使用者只看得見且只能點選某個連到真正垃圾郵件內容的 URL。

分析國碼最上層網域（如**.cn**、**.ru**、與 **.es**）時，可發現這些網域並非隨機使用。有別於通用最上層網域（如 .com 位址），這類 URL 如果用於垃圾郵件訊息，幾乎 100% 都會確實裝載垃圾郵件內容（或者會自動重新導向垃圾郵件內容）。圖 62 顯示最常使用隨機網域的通用最上層網域（並未包含垃圾郵件內容）。「隨機網域」一詞是指：網域名稱是隨機選擇的，不論該網域是否真實存在。

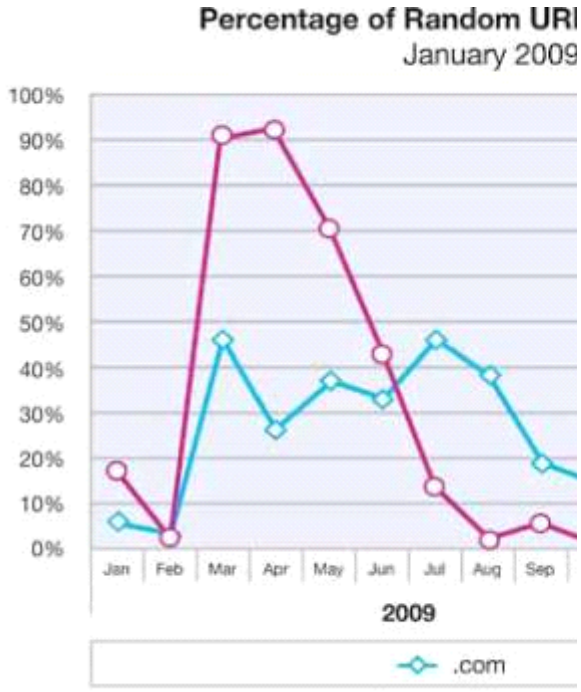


圖 62： 2009 年 1 月到 2010 年 6 月每個最上層網域隨機 URL 的百分比

如圖 62 所示，垃圾郵件內的 **.net** URL 一般皆爲隨機生成。2009 年春夏兩季，僞造的 URL 使垃圾郵件變得更合法。但 2009 年 8 月到 2010 年 3 月間，隨機 **.net** URL 幾乎完全停止使用。之後，隨機 **.net** URL 再次成爲垃圾郵件發送者的常用工具。2010 年 3 月，大約 30% 垃圾郵件內的 **.net** URL 皆爲隨機生成。

垃圾郵件 URL 的名聲：這些 URL 是否會連回網際網路？

幾乎所有真正包含垃圾郵件內容的 URL 都是來自新註冊的網域。很少有人能透過搜索網際網路，找出已知的垃圾郵件 URL。研究這個問題的另一種方法是透過聲譽排名，也就是檢查垃圾郵件網頁是否連到網際網路其他地方。圖 63 顯示垃圾郵件 URL 含有連到其他 URL 的鏈結百分比。

如圖 63 所示，垃圾郵件發送者不傾向於連到網際網路其他地方。2008 上半年，在所有垃圾郵件 URL 中，約有 6% 含有鏈結。該時期前後，只有不到 2% 的垃圾郵件 URL 連到 Web 其他地方。

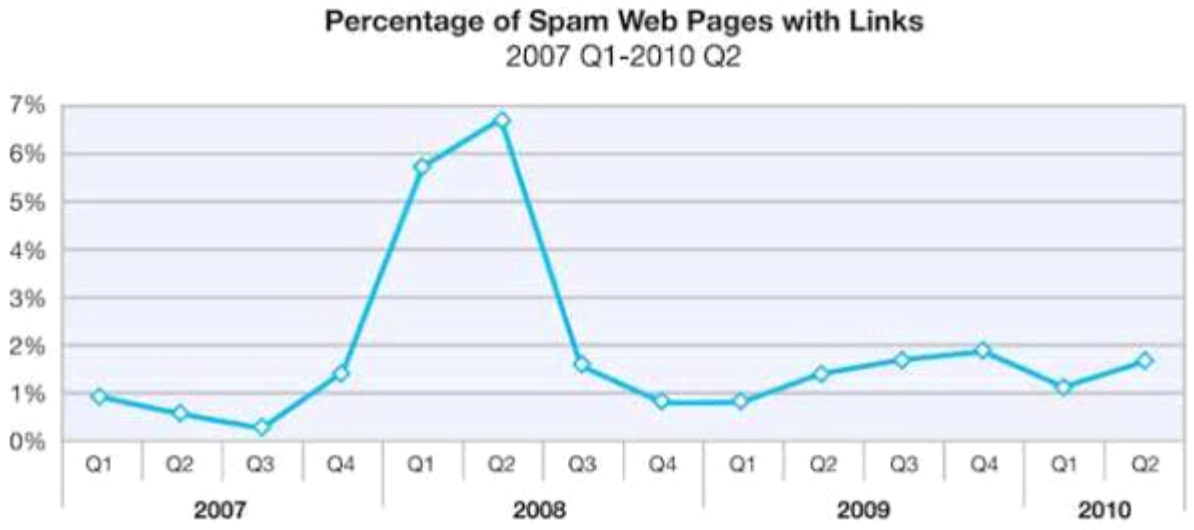


圖 63： 2007 年第 1 季到 2010 年第 2 季含有鏈結的垃圾郵件網頁百分比

然而，整個 2009 年，垃圾郵件發送者逐漸提升含有其他鏈結的垃圾郵件 URL 百分比。2010 年初卻退回 1.1%，但年中時，又達到將近 2%。讓我們進一步瞭解這些郵件通常連到什麼類型的 URL。

圖 64 將這些 URL 分爲兩類：正當的類別（如一般商務、購物、軟體、硬體等等）與不當的類別（如色情、惡意軟體、匿名 Proxy 等等）。

大部分鏈結指向正當的 URL，很可能是垃圾郵件發送者試圖爲垃圾郵件 URL 取得好評。重要的是要記住：只有不到 2% 的垃圾郵件 URL 含有鏈結。

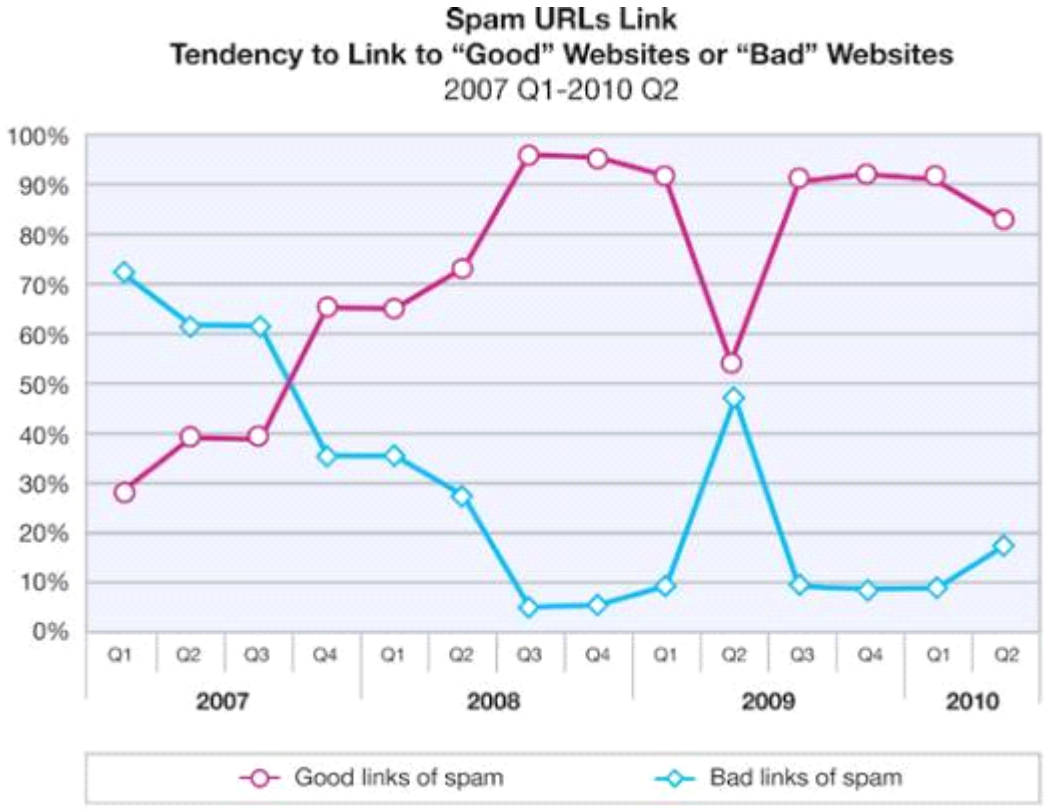


圖 64： 2007 年第 1 季到 2010 年第 2 季垃圾郵件 URL 鏈結連到「正當」網站或「不當」網站的趨勢

垃圾郵件 URL 連到的網站類型

根據我們的分析，大多數垃圾郵件 URL，如果確實連至網際網路，往往會連至傳統上屬於「正當」的網站。然而，我們將資料分解成 68 個類別時，最常被造訪的網站則落在「不當」的類別 - 色情。圖 65 顯示色情鏈結與其他鏈結相比的百分比。請注意：色情類別總數曾經超越正當網站（回溯到 2007 上半年時）。過去 9 個月以來，在垃圾郵件 URL 放置色情鏈結呈現微幅上升趨勢。含有色情鏈結的垃圾郵件 URL 百分比，每季約增加 1%。

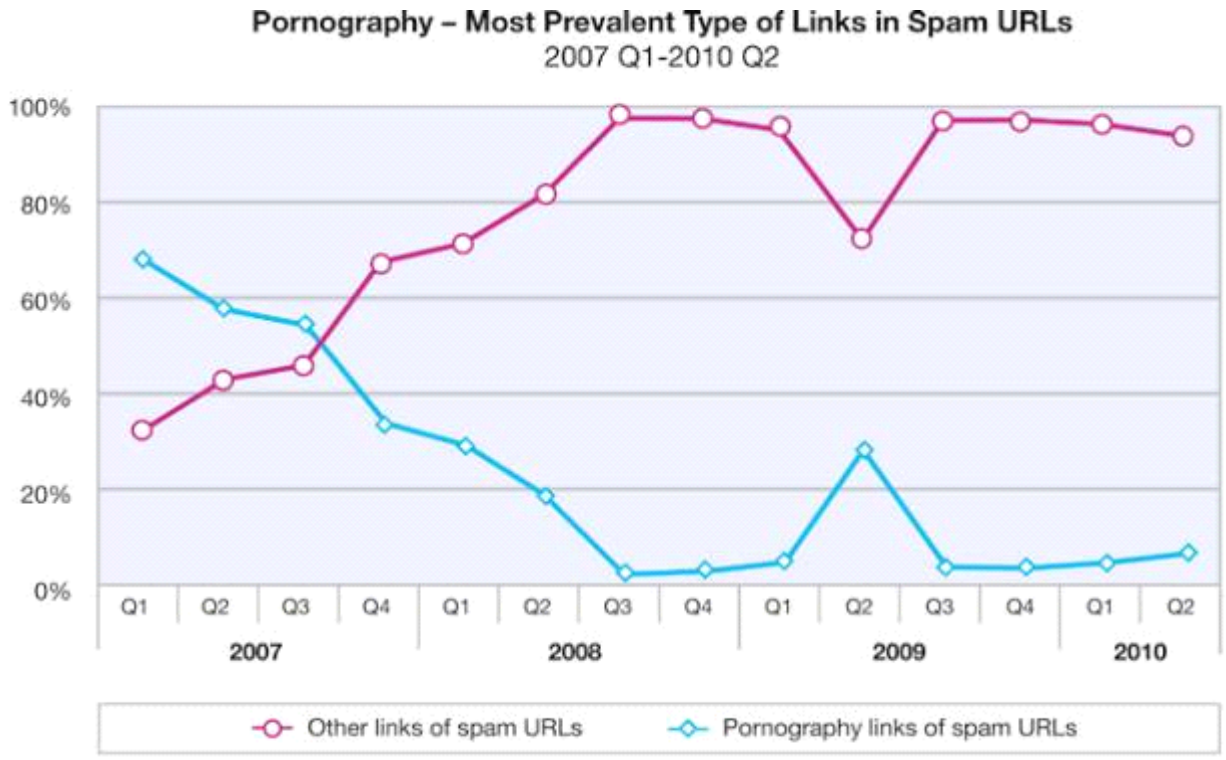


*圖 65：*色情 - 垃圾郵件 URL 中最常見的鏈結類型（2007 年第 1 季到 2010 年第 2 季）

其他主要類別皆爲正當的類別：一般商務、社交網路與購物。2008 年底，社交網路首次帶來巨大影響，在所有 URL 鏈結中佔了 18% 以上。雖然 2009 上半年，社交網路鏈結呈現下降趨勢，但 2009 年底卻微幅上升至將近 2%，不過 2010 年第 2 季又下滑到 1.4%。由於一般商務與購物可讓垃圾郵件 URL 獲得好名聲，所以從 2010 上半年開始，這兩種類別越來越能吸引垃圾郵件發送者。

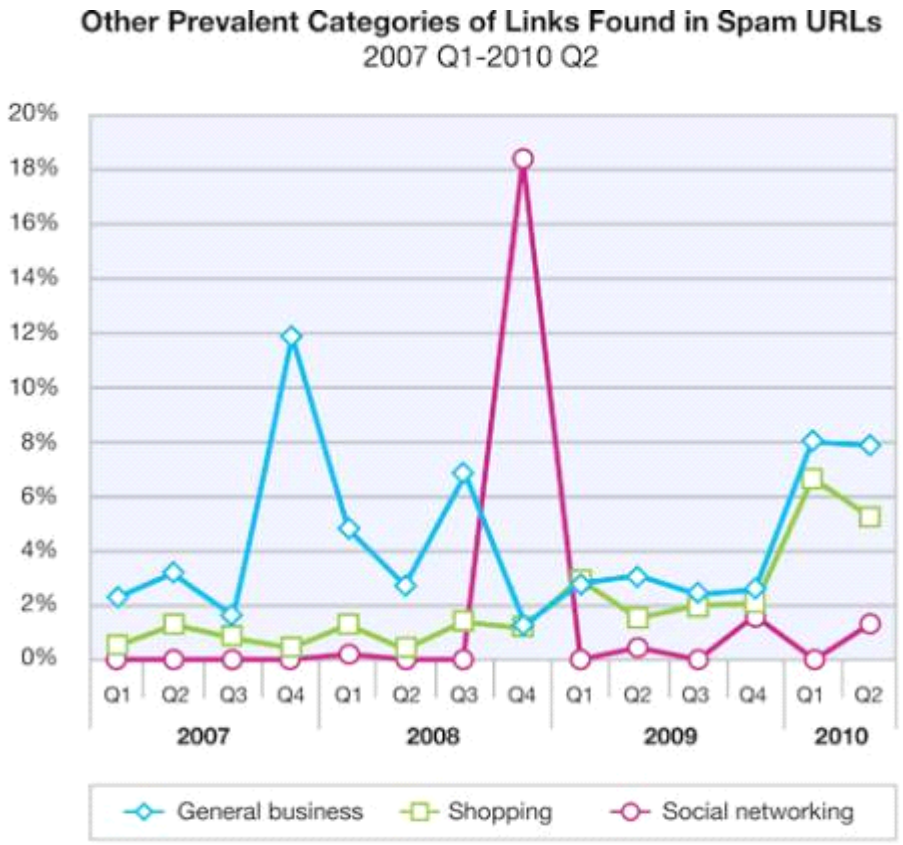


*圖 66：*其他垃圾郵件 URL 中常見的鏈結類別（2007 年第 1 季到 2010 年第 2 季）

垃圾郵件 URL - 來源國家

表 15 列出 2010 上半年全球垃圾郵件的發源地[2]。巴西、美國及印度就佔了全球垃圾郵件總數四分之一以上。美國再次回到第一，並將巴西擠到第二。印度仍然維持第三名的位置，俄羅斯取代越南成爲第四名，越南則取代南韓成爲第五名。德國、英國、烏克蘭和羅馬尼亞是第一次進入前十名；波蘭、土耳其、中國及哥倫比亞原本 2009 年還在名單中，可是到了 2010 上半年卻已退出十大垃圾郵件發送者的名單。

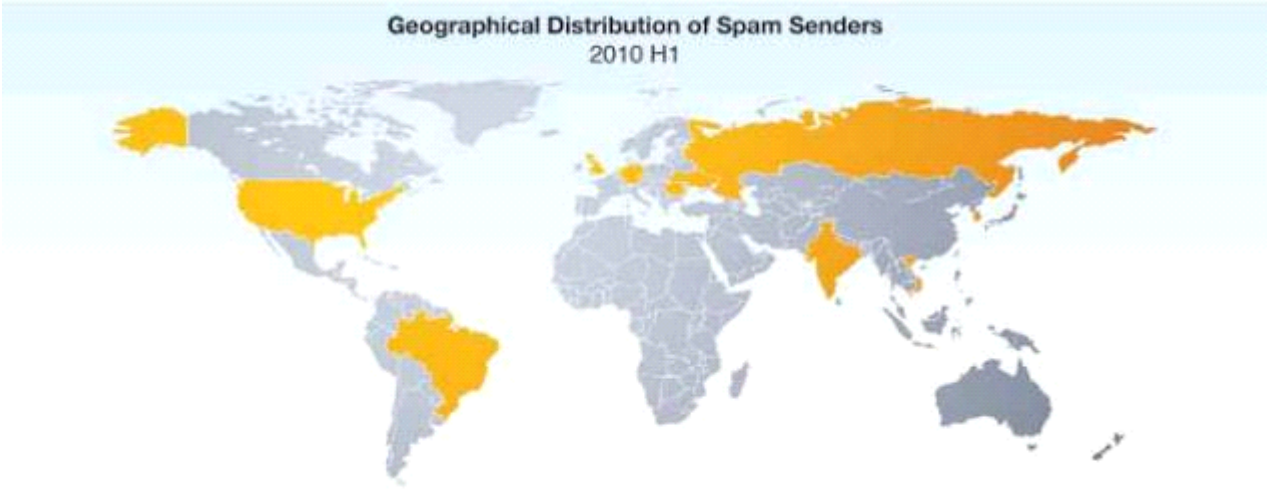


*圖 67：*2010 上半年垃圾郵件發送者地理分佈

國家	垃圾郵件百分比
美國	9.7%
巴西	8.4%
印度	8.1%
俄羅斯	5.3%
越南	4.6%

國家	垃圾郵件百分比
南韓	4.1%
德國	3.7%
英國	3.3%
烏克蘭	3.1%
羅馬尼亞	3.0%

[2] 來源國家是指發送垃圾郵件伺服器的位置。X-Force 認爲大多數垃圾郵件透過傀儡網路寄送。由於機器人程式可從任何地方進行操控，因此躲在垃圾郵件背後的真正攻擊者的國籍，可能與垃圾郵件來源國家不同。

表 15 : 2010 上半年垃圾郵件發送者地理分佈

從短期來看（包括去年），某些趨勢越來越明顯。2009 年，巴西排名第一，甚至不斷創下新紀錄。除了巴西以外，在 2009 年第 4 季，越南是唯一發送的垃圾郵件佔了 9% 以上的國家。另一方面，美國、俄羅斯和土耳其在垃圾郵件發送國中的重要性已降低。但到了 2010 上半年，巴西顯著下降，美國則是恢復原狀。越南衰退，印度則是維持一年多的增長。2010 第 2 季，印度首次躍升爲亞軍，而且與第一名只差了 0.6%。

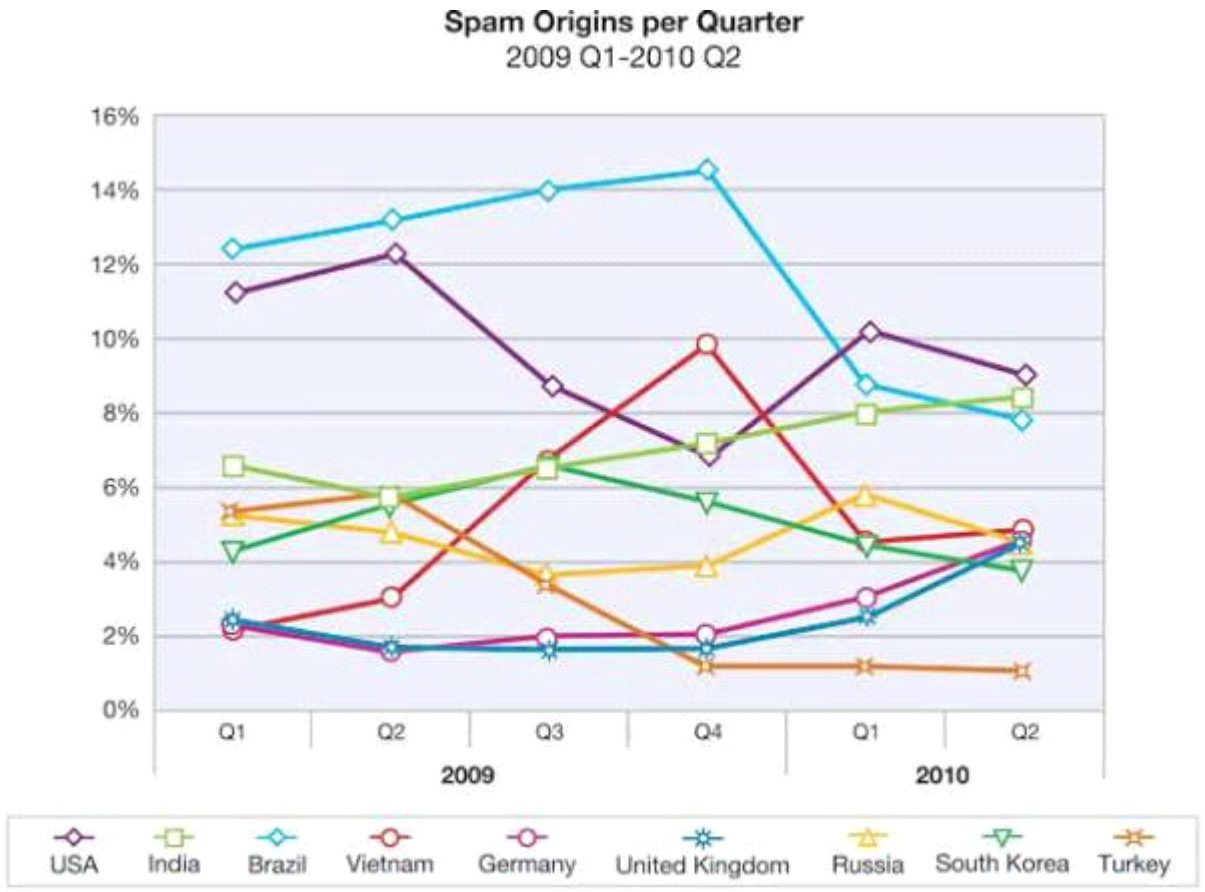


*圖 68：*2009 年第 1 季到 2010 年第 2 季每季垃圾郵件來源

金磚四國的成長

身爲金磚四國[3]成員的巴西與印度，在垃圾郵件與網路釣魚產業都有迅速的成長。2010 上半年，巴西是網路釣魚發送者最多的國家（細節請見後面章節）。其他兩個金磚國俄羅斯與中國在這方面也不遑多讓，如前一頁圖 66 所示，俄羅斯的最上層網域 **.ru** 常被用來裝載垃圾郵件內容。而且如表 16 所示，中國是垃圾郵件 URL 最大的發源地。對金磚四國來說，垃圾郵件與網路釣魚這兩項產業跟其他類型的產業一樣發展相當迅速。

然而，爲何會是越南與巴西？成爲垃圾郵件發送國之首，必須先滿足兩個主要條件：

- 網際網路使用人口大量成長
- 大量居民

巴西和越南已滿足這兩項條件。巴西 2 億 1 百萬居民中，38% 使用網際網路。這個數字過去十年來增加超過 1,419%。[4] 越南 9 千萬居民中，27% 使用網際網路。這個數字過去十年來增加了 12,035%。[5] 這使得大量新手開始使用個人電腦；這些電腦可能並未得到適當修補或保護。此外，他們可能比較容易受到社交工程的欺騙、更容易遭受惡意軟體的攻擊，變成傀儡網路操控的傀儡。值得一提的是：垃圾郵件發送者在先進國家（如德國和英國）也佔有一席之地。上述兩者在 2010 年第 2 季，讓他們的垃圾郵件發送的「市佔率」增加 4% 以上。

增加的原因可能如下：

- 越來越多新手使用個人電腦。
- 越來越多病毒可越過防護完善的系統，成功將個人電腦變成傀儡網路操控的傀儡。
- 就算是經驗豐富的人，也無法完全避開常見軟體產品中急劇增加的漏洞。

如同先前在**第 18 頁**所描述，2010 上半年通報漏洞增長速度令人難以置信，而新興經濟體金磚四國也無法倖免於此。

[3] 金磚四國 (BRIC) 是首字母的縮寫，代表巴西、俄羅斯、印度和中國這些快速成長的經濟體。

[4] **http://www.internetworldstats.com/stats15.htm**

[5] **http://www.internetworldstats.com/stats3.htm**

垃圾郵件 URL - 來源國家

表 16 列出垃圾郵件 URL 的來源位置。

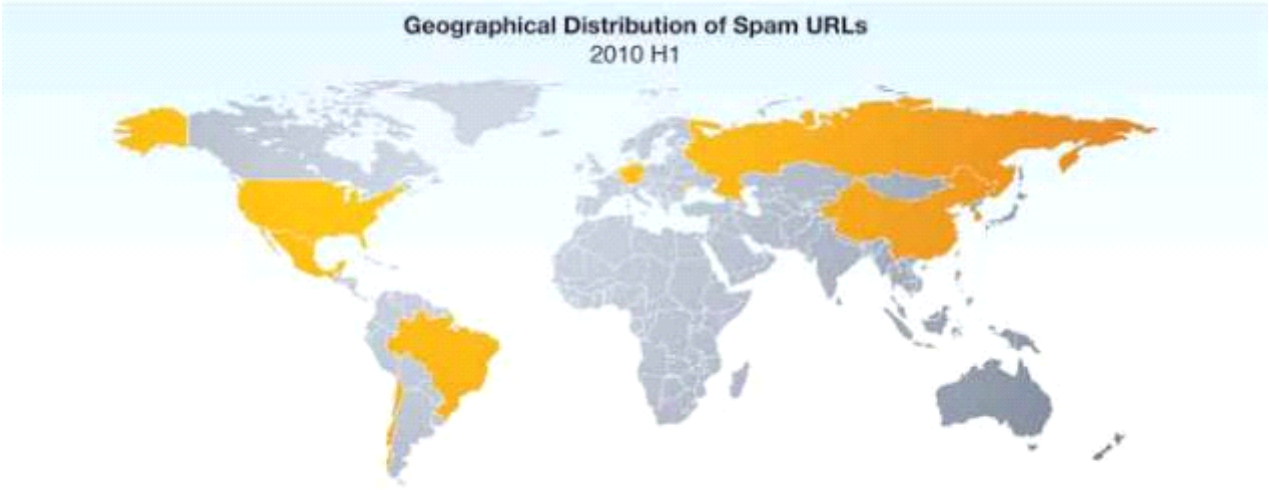


*圖 69：*2010 上半年垃圾郵件 URL 地理分佈

國家	垃圾郵件百分比
中國	37.5%
美國	16.6%
南韓	8.9%
摩爾多瓦	4.7%
俄羅斯	3.4%

國家	垃圾郵件百分比
巴西	1.9%
墨西哥	1.6%
荷蘭	1.5%
智利	1.5%
台灣	1.5%

*表 16：*2010 上半年垃圾郵件 URL 地理分佈

垃圾郵件 URL - 來源國家趨勢

從過去幾年一直到 2009 年底，源自中國伺服器的垃圾郵件 URL 大量增加；其他國家則是呈現停滯或下降趨勢（尤其是美國）。2010 上半年，往中國集中的趨勢已減緩，事實上過去兩年來，中國首次下滑。不過目前中國還是名列第，三分之一以上的垃圾郵件 URL 都源自中國。其他國家（尤其是美國）已恢復常態，目前 17% 的垃圾郵件 URL 皆源自於美國，而將近 9% 的垃圾郵件 URL 源自於南韓。最近新加入前十名的是摩爾多瓦，4.7% 的垃圾郵件 URL 皆源自於此。

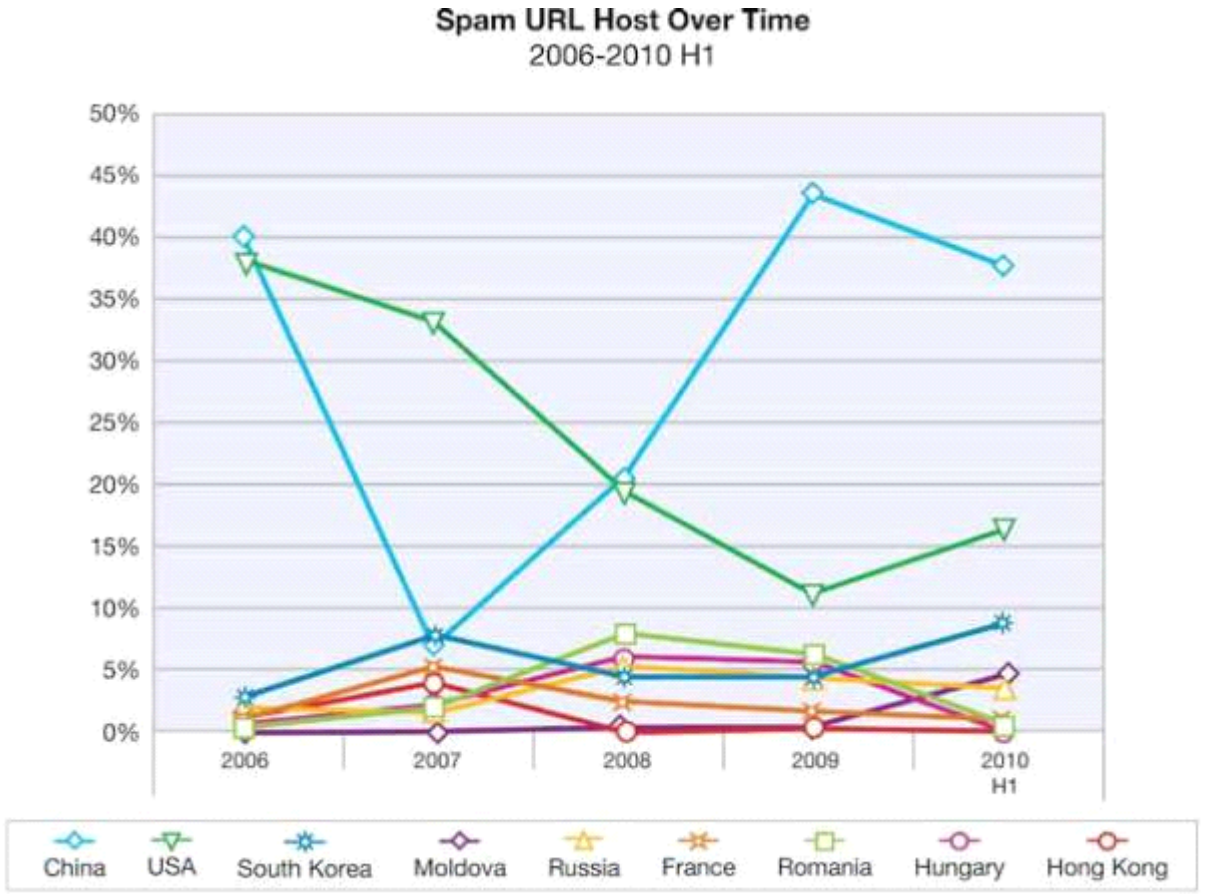


*圖 70：*2006-2010 上半年垃圾郵件 URL 主機變化

垃圾郵件全球化

由於在垃圾郵件 URL 發源地方面，中國仍佔據首要地位，因此我們應進一步檢視這些 URL，特別是思考垃圾郵件發送者使用 .cn 網域比例大幅下降的原因。圖 71 顯示垃圾郵件發送者所使用源於中國的最上層網域之分佈。

六成以上源於中國的垃圾郵件網域皆附帶俄羅斯的最上層網域 **.ru**。中國自己的最上層網域 **.cn** 低於 30%，僅位居第二。

所以全球化對垃圾郵件有何意義？一般垃圾郵件會從美國、印度或巴西的機器上發送，含有源自於中國的 **.ru** URL。

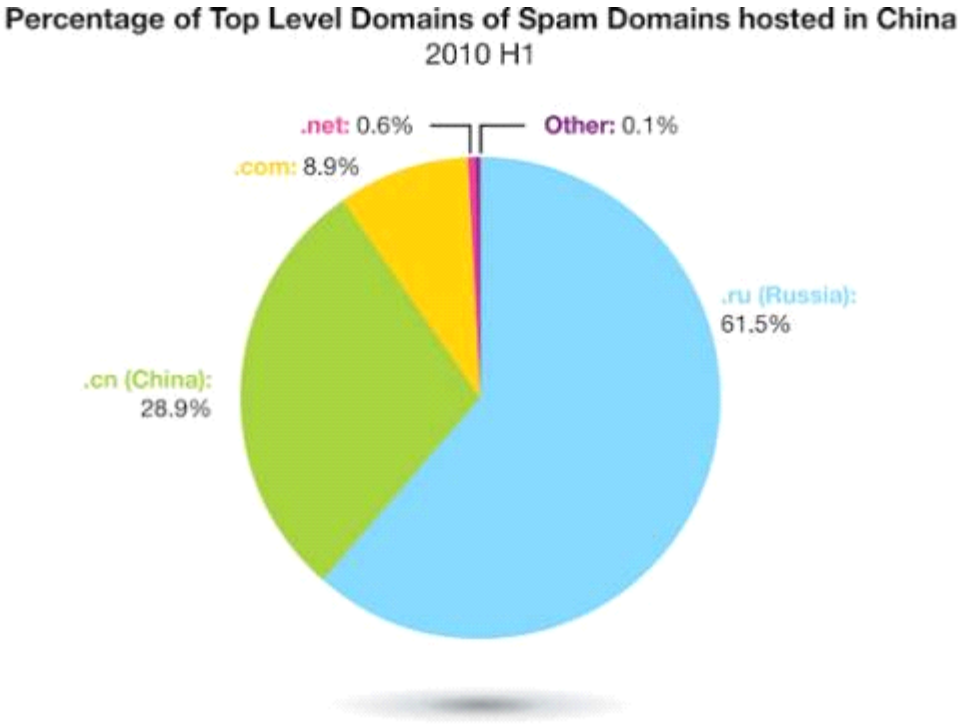


*圖 71：*2010 上半年源自中國的垃圾郵件網域最上層網域百分比

垃圾郵件 - 最常見的主旨

2007 到 2008 年垃圾郵件主旨越來越多樣化，但這股趨勢在 2010 年卻停滯不前。2010 上半年前十大主旨佔所有垃圾郵件主旨的 3.3% 左右，比 2009 年的 2.6% 及 2008 年的 3% 稍高，但仍遠低於 2007 年創下的 20%。

隨著 Web 2.0 和社交網路日漸普及，垃圾郵件發送者會使用與這些主題相關的主旨吸引使用者的興趣。此外，醫療產品或仿冒手錶這類「典型」主題也常用來吸引使用者的注意。垃圾郵件主旨如果出現 Pfizer 醫療產品通常會特別受到歡迎。垃圾郵件發送者在此會使用他們的傳統方法 - 玩弄大小寫、將「O」改成「0」（零）、使用不同百分數字等等。顯然 70% 是他們最喜愛的百分比（這也是唯一進入前十名的百分數字）。

表 17 列出 2010 上半年最熱門的垃圾郵件主旨。

主旨	%
You have a new personal message（您有新的個人訊息）	0.50%
Replica Watches（仿冒手錶）	0.44%
RE:SALE 70% 0FF on Pfizer（RE：Pfizer 提供 70% 的折扣）	0.40%
News on myspace（myspace 上的新聞）	0.35%
Important notice: (重要通知：) Google Apps browser support（Google Apps 瀏覽器支援）	0.35%
重要通知：Google	0.34%
Please read（請閱讀）	0.29%
Exquisite Replica（精美仿冒品）	0.23%
Watches（手錶）	0.19%
Confirmation Mail（確認郵件）	0.17%

表 17： 2010 上半年最常見的垃圾郵件主旨

網路釣魚

在本報告的第一部分，我們分享了一些精彩的故事，說明網路釣魚技術的重心爲何會轉向不同產業。

本節將進一步探討與下列主題有關的發展趨勢：

- 網路釣魚佔垃圾郵件的百分比
- 網路釣魚來源國家趨勢，包括網路釣魚網頁 (URL)
- 最常見的主旨與網路釣魚目標

網路釣魚量

2008 一整年，網路釣魚量平均佔整體垃圾郵件量的 0.5%。2009 上半年，網路釣魚攻擊大幅減少，僅剩垃圾郵件量的 0.1%。我們以爲除了傳送貌似銀行的郵件等簡單電子郵件外，網路釣魚犯罪網路還會利用其他方法來竊取身分；但事實並非如此。

跟我們在 2009 上半年見到的正好相反，網釣客在第 3 季捲土重來。2009 年 6 月可見到數量微幅上揚。然而到了 8 月，網路釣魚數量已逼近 2008 年最活躍的月份；9 月份的數量甚至完全超過 2008 年任何一個月份的數量。

並非只有我們注意到這點，其他研究組織也在談論此變化。到了 2009 年底，網路釣魚數量逐漸趨緩，且接近 2008 年底的數量，但仍明顯高於 2009 上半年。2009 年 12 月微幅增加後，在 2010 上半年，網路釣魚電子郵件再次趨緩，且接近 2009 上半年的數量。

經過 1、2 月份的下滑，3、4 月份可見到網路釣魚數量呈現上升趨勢，今年 5 月又出現另一波下滑。

這可能起因於 5 月初逮捕到羅馬尼亞網路釣魚集團（請參閱 **http://www.h-online.com/security/news/item/Police-apprehend-Romanian-phishing-gang-997151.html**）。6 月份再次達到 3、4 月份的水準，但仍遠不足 2009 年夏季的數量。過去兩年網釣客在夏秋二季都曾發動猛烈攻擊，未來幾個月是否也是如此？且讓我們拭目以待。

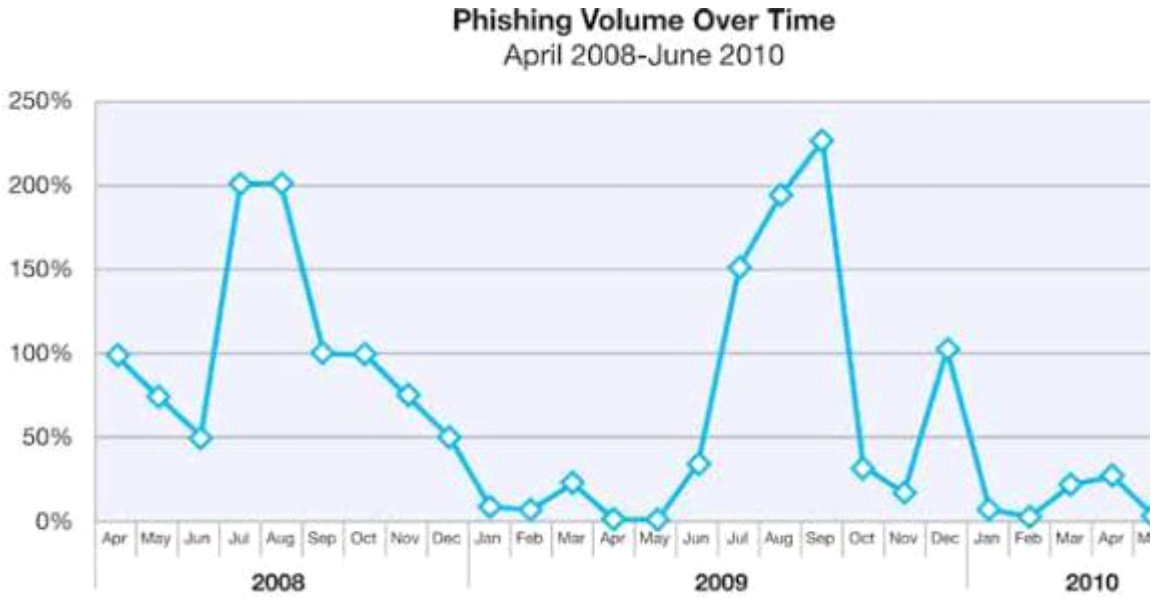


*圖 72：*2008 年 4 月到 2010 年 6 月網路釣魚量變化

網路釣魚 - 來源國家

巴西仍是最大的網路釣魚量傳送端，印度位居第二，南韓則位居第三。與 2009 年相比，前十名的名次變化最多上升或下降三名；只有俄羅斯的排名從第三降到第十。德國首次進入前十名，土耳其則已退出榜單。表 18 列出 2010 上半年網路釣魚電子郵件主要來源國家。

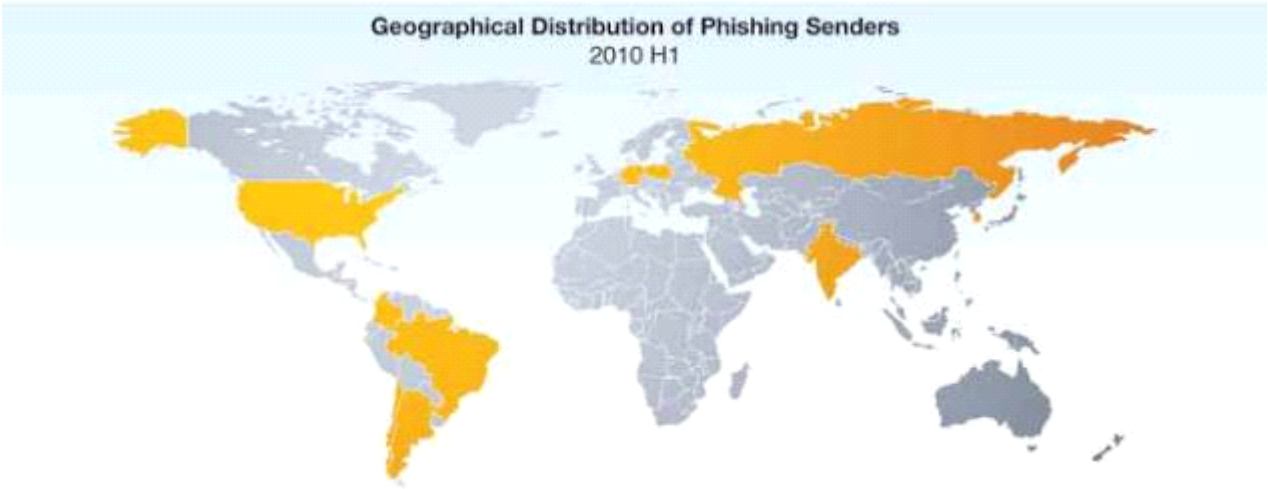


*圖 73：*2010 上半年網路釣魚發送者地理分佈

國家	垃圾郵件百分比
巴西	14.3%
印度	8.2%
南韓	7.8%
美國	5.6%
哥倫比亞	3.4%

國家	垃圾郵件百分比
阿根廷	3.8%
智利	3.3%
德國	3.1%
波蘭	2.9%
俄羅斯	2.6%

*表 18：*2010 上半年網路釣魚發送者地理分佈

網路釣魚 URL - 來源國家

表 19 顯示網路釣魚 URL 的來源位置。前十名的國家與 2009 年相比並無改變，而相對排名也只有稍微變動。俄羅斯的排名從第八降到第十，西班牙和波蘭則向上攀升一名。

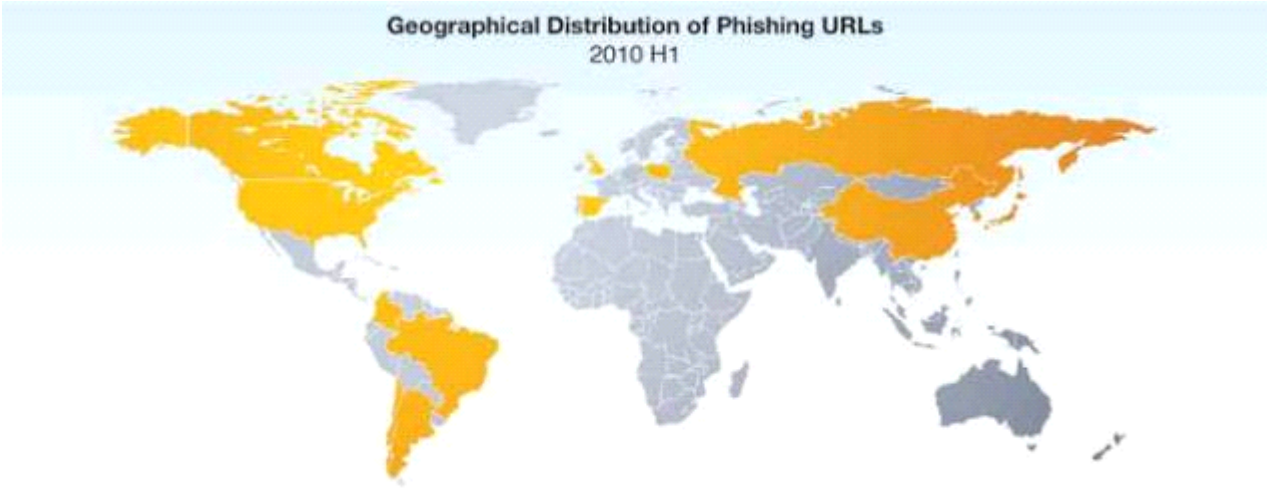


*圖 74：*2010 上半年網路釣魚 URL 地理分佈

國家	垃圾郵件百分比
羅馬尼亞	18.8%
美國	14.5%
中國	11.3%
南韓	9.8%
英國	7.2%

國家	垃圾郵件百分比
加拿大	4.7%
日本	4.3%
西班牙	3.2%
波蘭	3.0%
俄羅斯	2.9%

*表 19：*2010 上半年網路釣魚 URL 地理分佈

網路釣魚 - 最常見的主旨

2008 年最顯著的變化之一，就是常見的主旨不再熱門。2007 年最常見的主旨佔所有網路釣魚電子郵件的 40% 以上；2008 年最常見的主旨卻僅佔所有網路釣魚主旨的 6%。由此可見，2008 年網釣客的目標越分越細，比 2007 年的主旨變化更多。

2009 年，這類趨勢完全逆轉。前十大最常見主旨佔所有網路釣魚電子郵件的 38% 以上。2010 上半年，前十大最常見主旨佔所有網路釣魚電子郵件的 36% 左右。

「漏報收入」的文字已連續四次出現在前十名的網路釣魚主旨中，這類網路釣魚威脅已持續將近一年，與某個美國稅務網站有關。剩下的 6 個主旨也相當普遍，大部分主旨包含需要使用者緊急處理的事情。多數情況下，要求使用者依照電子郵件中的鏈結登入銀行帳戶，事實上則是會連到詐騙網站。

表 20 列出 2010 上半年最熱門的網路釣魚主旨。

主旨	%
Security Alert - Verification of Your Current Details（安全警示 - 驗證您目前的詳細資料）	15.75%
American Express Online Form（美國運通線上表格）	6.22%
important notification（重要通知）	1.95%
Official information（官方資訊）	1.78%
Your Account Has Been Limited（您的帳戶受到限制）	1.73%
Notice of Underreported Income（漏報收入的通知）	1.70%
Underreported Income Notice（漏報收入通知）	1.67%
the CP2000 notice (Underreported Income Notice)（CP2000 通知（漏報收入通知））	1.67%
official “Underreported Income Notice” to taxpayer（給納稅人的官方「漏報收入通知」）	1.66%
Final notice（最後通知）	1.40%

*表 20：*2010 上半年最常見的網路釣魚主旨

IBM 全球服務事業部
技術諮詢熱線：0800-000-700
台北市松仁路 7 號 3 樓
台灣

台灣印製
2010 年 8 月

WGL03003-USEN-01