

網上攻擊與其對策

2008 年 2 月

©香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 現今的網上攻擊.....	3
趨勢與影響.....	3
II. 攻擊的行徑.....	5
III. 對策與應變.....	6
網上應用程式擁有者的指引.....	6
給終端用戶的提示.....	7

摘要

網上應用系統連線後常常受到攻擊，過去幾年以來我們見到許多網站遭受攻擊的事件發生，突顯了網絡伺服器的漏洞與網站程式在設計上的缺陷。近年來隨著MySpace、Facebook、Wikipedia、聊天室、討論區等網絡社群¹的出現及增長，終端用戶與他們的工作站變成了被攻擊的目標。

因應網絡上越來越厲害的攻擊手段，提供網上服務的機構和終端用戶也需要保護自己的網絡及電腦系統免受攻擊，避免轉而變成攻擊其它系統的武器。

¹ <http://www.firstmonday.org/issues/issue4/valauskas/>

I. 現今的網上攻擊

趨勢與影響

除了伺服器原有的弱點及網絡程式的漏洞外，攻擊者也會利用終端用戶對其瀏覽網站的信任而進行攻擊，攻擊的方式不外乎引誘受害者進入惡性網站，或當受害者從網站下載檔案如音樂、影片、珍藏品等其它資料時，把受害者重新導向其它有害的網站。機構和終端用戶若無法適當地保護自己的電腦系統，便有可能蒙受巨大財務損失甚至毀壞名譽的風險。以下是瞄準終端用戶與其電腦的幾個攻擊事例：

1. ‘Italian job’ 網站攻擊事件

2007年6月，超過10000個網站〔包括義大利政府機構的網站在內〕受到攻擊，感染的網站被插入一小段HTML “iFrame”程式。用戶一旦進入這些網站，便會被引導至另一個含有惡性JavaScript的網站。這時，有害的鍵盤側錄程式（Keylogger）與木馬程式便會下載及安裝到用戶的電腦中，更進一步測試電腦內的其它漏洞^{2,3}。

2. MySpace 仿冒詐騙〔Phishing〕/ Drive-by 攻擊事件

同樣在2007年6月，幾百個MySpace的個人簡介網頁被植入仿冒詐騙網址的連結⁴。當MySpace用戶進入感染惡性JavaScript的個人簡介網頁時，就會受到感染同一問題的風險，用戶會被悄悄引導至有害網站，並偵測其瀏覽器是否有任何弱點，若有的話，代理伺服器網絡漫遊器「flux bot」就會被安裝在用戶的電腦中，此程式會透過不斷改變代理伺服器來隱藏其仿冒詐騙網址⁵。

3. 跨網址程式編程〔Cross-site scripting or XSS〕蠕蟲

2005年10月，MySpace受到跨網址程式編程的攻擊，Samy蠕蟲的作者上傳跨網址程式編程攻擊的程式碼到MySpace的個人網頁。當其他MySpace用戶瀏覽他的網頁時，這蠕蟲就會強迫訪客將Samy加入其好友名單，並在訪客的個人資料中放入竊取資料的程式。這隻Samy蠕蟲快速地在用戶瀏覽任何一個受感染的網頁時繼續散播出去，此舉造成一百多萬名用戶受到感染⁶。

4. 其它攻擊方式

仿冒詐騙方法可被歸類為一種社交工程的攻擊，犯罪者引誘毫無戒心的網絡用戶登入外表看起來相似的網頁，eBay或網絡銀行的網站也曾被這種攻擊困擾⁷。

² http://www.infoworld.com/article/07/06/18/Italian-job-Web-attack-hits-10000-sites_1.html

³ <http://blog.trendmicro.com/another-malware-pulls-an-italian-job/>

⁴ <http://www.scmagazineus.com/MySpace-users-warned-of-drive-by-exploit-attack/article/35125/>

⁵ <http://isc.incidents.org/diary.html?storyid=3060>

⁶ <http://www.whitehatsec.com/downloads/WHXSSThreats.pdf>

⁷ <http://googleonlinesecurity.blogspot.com/2007/06/thwarting-large-scale-phishing-attack.html>

網絡搜尋引擎也會助長網上攻擊。2004年12月，一隻名為Santy.A的蠕蟲攻擊phpBB的網絡論壇軟件。它並不像其它網上攻擊隨意地挑選目標來攻擊，反而是利用Google搜尋引擎來搜尋容易攻擊的新目標，繼而透過phpBB的弱點進行攻擊⁸。

⁸ <http://isc.sans.org/diary.html?date=2004-12-21>

II. 攻擊的行徑

網絡攻擊，如the Italian job、MySpace仿冒詐騙/Drive-by攻擊以及其它跨網址程式編程攻擊蠕蟲，大致都是以下列模式出現：

1. 攻擊者尋找一個有跨網址程式編程漏洞及可被攻擊的網站。
2. 攻擊者執行下列其中一種方法：
 - 在有漏洞的網站伺服器中成功插入程式碼（例如Java Script程式），當終端用戶連接到已受感染的伺服器時，跨網址程式編程攻擊便會在終端用戶處發生；或
 - 在網頁中編制一個具惡性的手稿程式，可與跨網址程式編程攻擊一起使用，藉著引誘目標用戶選取此網頁，隱藏在內的手稿程式開始在用戶的瀏覽器運作，造成更惡性的攻擊如下載木馬程式或將cookie資訊傳送給攻擊者。

在Samy蠕蟲病毒案例中，惡性程式只感染MySpace網絡社群的正式會員，如此，已經造成極大範圍的感染。在某些案例中，惡性程式無須連接到網站外的伺服器。

在仿冒詐騙中，受害者透過社交工程渠道如電子郵件被騙取身份、信用卡帳號甚至銀行帳號登入認證。攻擊者不需要侵入任何網站，只是簡單植入一個詐騙網址，就能引誘毫無戒心的用戶上當。

以往，惡性程式多是採用隨機尋找互聯網規約地址的方式來尋找目標，隨着網絡搜尋引擎的便利與精準，反而幫助攻擊者更容易尋找新目標。除此之外，如果機構內的機密資料沒有妥善的保安措施，很容易讓網絡搜尋引擎找到這些資料編成索引。萬一這些資料呈現在攻擊者的螢幕上，就會導致資料外洩了。

III. 對策與應變

隨著互聯網上出現越來越多技巧純熟的網站攻擊，為了免於洩密或被利用轉為攻擊他人之跳板，終端用戶和提供網站服務的機構必須實行適當的保安措施來保護他們的系統。

網上應用程式擁有者的指引

為避免被利用作為網絡攻擊的跳板，採用保安科技可協助並預防和偵測任何不正常行為。沒有一個網站可以保證完全安全，實施合適的保安事故處理程序是必須的。

當網站管理者發現資料已經外洩或網站客戶的安全已被入侵，可能已經過了一段時間。在許多案例中，通常是第三者如客戶，首先發現提供網絡服務的網站已經出現問題。在仿冒詐騙中，詐騙網站通常分屬不同區域管轄權，真正網站的管理者只能提醒客戶注意與原本網站相似的網頁，不要去瀏覽這些詐騙網站。另一個可能的做法，就是告知及要求詐騙網站所寄存的網絡服務供應商，將此詐騙網站相關連線刪除。

研究系統與應用程式中的記錄有助於調查網上攻擊事故的行徑。本文先前所述之跨網址程式編程攻擊蠕蟲案例中，MySpace受害者的網頁只扮演一個將顧客引導至惡性網站的角色，客戶電腦裡查不到任何攻擊者留下的線索。因此，任何可能受害的網頁或網站，都必須能夠追蹤任何跨網站指令攻擊的方法，並清除受影響的網頁，杜絕更多病毒的感染。

若想讓跨網址程式編程攻擊成功，攻擊者需先將惡性程式植入受害者的網上應用系統。為了預防此事發生，此類惡意訪客的輸入資料需先經過濾。在Samy蠕蟲病毒案例中，MySpace的確有用戶驗證機制，但事實證明並無法真正防範攻擊者入侵。除了移除輸入資料中的特殊字元並將輸出作動態編碼之外，需建立「白名單」（white-list）法則。在「白名單」法則中，唯有符合先前設定的型態資料才被允許進入，其它則全部過濾清除。與「黑名單」（black-list）法則比較---也就是只封鎖先前設定好的不符資料型態條件的方式，「白名單」法則更能夠讓網上應用系統只允許那些透過正確並經認可的資料進入，這是「黑名單」法則做不到的。

對保安事故的偵測與監控、遏制及預防機制是有必要建立的。應保留系統記錄與其它支援資訊，作為提供回溯保安事故時的佐證。為了隨時面對更糟的情況，應該建立、記錄並維護關於網站應用系統安全機制的處理與報告程序。所有員工也應有警覺訓練，確保能完全掌控任何保安事故的處理與報告程序。對於任何可疑的系統入侵，應立即有跟進行動，且應遵照保安事故處理程序與報告之指引方針。

此外，應由一群獨立、可靠及可信賴的第三者來定期評估網上應用系統，以決定網站以最低限度的控制去遏制可接受的風險。對保安風險評估的執行，也應比較其它網上應用系統的更新或改變優先。

另一個可能的預防措施是聘用外部專家去定期檢查網上現存的詐騙網站。一旦發現詐騙網站，便可立即通知客戶與網站用戶，讓仿冒詐騙事故降到最低。

其它技術性和管理上的措施請參考“網上應用系統保安”一文。

給終端用戶的提示

為防止您的電腦洩密並成為攻擊他人的武器，建議網上應用系統及網上用戶：

1. 確認你的作業系統和關鍵系統元件如瀏覽器，完整安裝並隨時更新修補程式；
2. 安裝個人防火牆與最新版病毒碼的防毒工具，可偵測惡性軟件如鍵盤側錄程式（Keylogger）；
3. 在各網上應用系統與服務中，使用不同的帳號與密碼組合；
4. 在未支援限用一次密碼的重要網上應用系統中，需經常變更密碼；及
5. 瀏覽任何陌生網站前，應關掉瀏覽器中支援JavaScript 或ActiveX的功能。