

# 網路疫情 通報

12/29/2008-01/11/2009

賽門鐵克大中華安全機制應變中心

## 內容

[熱門病毒排行](#)

[病毒趨勢](#)

[垃圾郵件趨勢](#)

[熱門釣魚網站](#)

[賽門鐵克安全專家建議](#)

# 網路疫情通報

12/29/2008-01/11/2009

## 熱門病毒排行

排名	名稱	類型	風險級別	表現/描述
1	W32.SillyFDC	病蟲	非常低	W32.SillyFDC 表明偵測到 W32.Silly 系列病蟲的變體。這一系列的病蟲透過將自身複製到可移除介質上進行傳播，而且可能會下載其他惡意應用程式。
2	Downloader	木馬	非常低	Downloader 會連線到 Internet 並下載其他木馬或元件。
3	Trojan Horse	木馬	非常低	Trojan Horse 表明偵測到各種木馬程式。
4	Trojan.Giframe	木馬	非常低	Trojan.Giframe 表明偵測到特定 GIF 圖像。這些圖像可能包含將使用者重定向到惡意網站的 HTML 標籤。
5	Adware.WhenUSearchBar	廣告軟體	低	Adware.WhenUSearchBar 是一個桌面工具列，它會監控 Internet 流量、收集搜索設定檔，並能利用自己的更新功能從遠端伺服器執行程式碼。
6	W32.Pagipef.I!html	病蟲	非常低	W32.Pagipef.I!html 表明偵測到感染了 W32.Pagipef.I 的 .html 文件。被感染的 HTML 檔案可能會連結到惡意程式碼。
7	Infostealer.Gampass	木馬	非常低	Infostealer.Gampass 這類木馬專門盜取網路遊戲帳戶，例如天堂、仙境傳說、羅漢和熱血江湖等遊戲。
8	Backdoor.Trojan	病蟲	低	Backdoor.Trojan 是一種大型郵件病蟲，可將其自身發送至使用者 Microsoft Outlook 通訊錄中的所有電子郵件位址。它只會在其首次執行時進行大規模的寄件活動。大規模的寄件活動會停止，直至其進行第 21 次執行。然後，它會繼續進行大規模的寄件活動。病蟲還會將其自身複製到所有的共用網路磁碟機。
9	Bloodhound.SONAR.2	木馬	非常低	Bloodhound.SONAR.2 專門指代賽門鐵克防病毒產品利用賽門鐵克 Bloodhound 技術發現的潛在未知風險。Bloodhound 技術包含啓發式演算法，可用來偵測未知風險。
10	Backdoor.Graybird	木馬	非常低	Backdoor.Graybird 是一種後門木馬，其建立者能夠對電腦執行未經授權的存取。如果在電腦中發現 Svch0st.exe，則表示可能感染了此木馬。Backdoor.Graybird 是一種 Delphi 應用程式。

## 病毒趨勢

最近，病蟲 W32.Downadup.B 的活動日趨活躍。W32.Downadup.B 透過微軟 Windows 伺服器服務 RPC 的遠端執行弱點 (BID 31874) 進行傳播。使用弱密碼保護的網路共用也會感染此病蟲，此外，它還會攔截對安全性相關網站的存取。同時，W32.Downadup.B 的演變十分迅速。從第一次發現此種病毒至今，已經偵測到其 20 種變形。賽門鐵克建議使用者安裝針對 MS08-067 的最新修正程式，並下載賽門鐵克防病毒產品的最新安全更新，以保護電腦不受到侵害。

## 垃圾郵件趨勢

賽門鐵克最近偵測到一些新的垃圾郵件攻擊。這些垃圾郵件看來像是來自受信任網站的正式通知，有著與其相同的主旨行格式。郵件的標頭，例如郵件 ID、接收人、甚至自訂 X 標頭都經過精心製作以求逼真模仿合法電子郵件。此類郵件通常會邀請收件者按下電子郵件中的連結，將使用者引到其預先設計好的 URL，讓使用者在該位置填寫個人資訊表格。此資訊會被出售給營銷公司或用於進一步的垃圾郵件活動。賽門鐵克建議您不要接受任何陌生人的電子郵件邀請。

## 熱門釣魚網站

目標網域	URL	解析後的 IP
msn.com	<a href="http://littlest.devil.piclooks.com/indexx.php">http://littlest.devil.piclooks.com/indexx.php</a>	202.64.61.208
	<a href="http://bl106w-blu106-folderid-0000000000-0000-0000-0000-00000000000001.3322.org/bl106w.blu106.mail.live.com.mail.InboxLi">http://bl106w-blu106-folderid-0000000000-0000-0000-0000-00000000000001.3322.org/bl106w.blu106.mail.live.com.mail.InboxLi</a>	222.66.13.82
taobao.com	<a href="http://action1-taobao.com/auction/item_detail-0db2/93726/loginbz.asp">http://action1-taobao.com/auction/item_detail-0db2/93726/loginbz.asp</a>	221.231.140.164
	<a href="http://taobaotbv.cn">http://taobaotbv.cn</a>	222.189.238.152
	<a href="http://auction.tlxbao.cn/auction/item_detail-0db1-b50cfd6eb7cceb27eccd6f51212360.html">http://auction.tlxbao.cn/auction/item_detail-0db1-b50cfd6eb7cceb27eccd6f51212360.html</a>	222.73.165.152
paypal.com	<a href="http://mail2.intnet.com.cn/~jun_xie/payment_cancel_webscr_24234/webscr_cmd=_login-submit_main=0000.html">http://mail2.intnet.com.cn/~jun_xie/payment_cancel_webscr_24234/webscr_cmd=_login-submit_main=0000.html</a>	203.94.0.27
	<a href="http://paypal.com.459-727-927.u76m9gw6n53is23ag3.account19.bz/cmd-confirm">http://paypal.com.459-727-927.u76m9gw6n53is23ag3.account19.bz/cmd-confirm</a>	218.242.158.100
myspace.com	<a href="http://profile.myspace.com.fuseaction.user.viewprofile.dg.11523822.cn">http://profile.myspace.com.fuseaction.user.viewprofile.dg.11523822.cn</a>	222.186.12.137
ebay.com	<a href="http://ligf.cn:80/cacti/include/singinsecurisedloginwww-ebay-it.html">http://ligf.cn:80/cacti/include/singinsecurisedloginwww-ebay-it.html</a>	211.86.9.6

## 賽門鐵克安全專家建議

賽門鐵克大中華安全機制應變中心建議所有使用者和管理員遵循安全專家給出的以下建議。

### ► 預防攻擊和病毒感染

- 務必套用最新修正程式，尤其是那些託管有公共服務（例如 HTTP、FTP、郵件和 DNS 服務）、允許透過防火牆存取的電腦。如果一個或多個網路服務受到病毒攻擊，請在套用適當的修正程式之前禁用或阻止對這些服務的存取。
- 關閉並刪除不必要的服務。預設情況下，許多作業系統都會安裝一些並非必要的輔助服務，例如 FTP 伺服器、telnet 以及 Web 伺服器。這些服務是招致病毒的途徑。如果刪除這些服務，病毒攻擊的途徑就更少，您需要套用修正程式更新的服務也隨之減少。
- 如果您使用的是 Windows XP，請暫時關閉「系統還原」功能。此功能被預設啟用，作用是在電腦上檔案受損時還原這些檔案。如果病毒、病蟲或木馬感染了電腦，「系統還原」可能會備份電腦上的病毒，防病毒程式或工具無法刪除系統還原資料夾中的病毒。

參考資料：[如何關閉或打開 Windows XP 的系統還原功能](#)

- 對於從 Internet 上下載的軟體，請在執行前先進行病毒掃描。如果瀏覽器漏洞沒有部署修正程式，那麼瀏覽受侵害的網站時則可能會感染上病毒。
- 使用密碼保護。即便電腦受到侵害，複雜的密碼也能加大破解密碼檔的難度。這有助於在電腦受到侵害時避免損失或降低損害程度。
- 配置電子郵件伺服器，使之阻止或刪除帶有可疑附件的電子郵件，例如 .vbs、.bat、.exe、.pif 和 .scr 之類的檔案附件常常被用於傳播病毒。
- 迅速隔離被感染的電腦以防感染範圍擴大。執行取證分析並使用信任的介質恢復電腦。



**注意** 此外，我們還強烈建議您遵循以下建議：

- 使用 **Symantec Security Check** (<http://security.symantec.com/sscv6/home.asp?langid=ie&venid=sym&plfid=23&pkj=UMOUORVWHFHMFNZMBBX>) 測試電腦的安全級別
- 在不確定 URL 的安全性時請先造訪 **Norton Safe Web** (<http://safeweb.norton.com>) 以評估該 URL
- 將懷疑感染了病毒的檔案上傳到賽門鐵克大中華安全機制應變中心，網址為：<https://submit.symantec.com/websubmit/retail.cgi>

## ► 如何在受到感染後刪除病毒

注意：根據病毒的類別，您可能只需執行以下操作中的一部分，但也可能需要執行額外的操作。如需詳細資訊，請在 [http://www.symantec.com/business/security\\_response/index.jsp](http://www.symantec.com/business/security_response/index.jsp) 上搜索具體病毒，並根據刪除步驟進行操作。

### • 更新病毒定義

取得最新病毒定義的方式有兩種：

- a. 啟動您的賽門鐵克程式並執行 LiveUpdate
- b. 使用 Intelligent Updater 下載定義並手動安裝

參考資料：[Intelligent Updater 病毒定義](#)

[如何使用 Intelligent Updater 更新病毒定義檔](#)

### • 移除病毒

- a. 按「開始」>「設置」>「控制台」>「新增/移除程式」，選擇要卸載的目的程式，然後按下「新增/移除」、「變更/移除」或「移除」（視您使用的作業系統而定），然後遵循提示進行操作
- b. 使用 Windows 檔案總管瀏覽至 %ProgramFiles% 目錄並刪除剩下的檔案 (如果有的話)。

### • 執行掃描

- a. 啟動您的賽門鐵克防病毒程式，然後執行完整系統掃描

參考資料：[如何架構 Norton AntiVirus 掃描所有檔案](#)

[如何檢驗賽門鐵克企業防病毒產品是否已設置為掃描所有檔案](#)

- b. 如果檢測到檔案，遵循防病毒程式所顯示的指示進行操作

注意：如果您無法啟動賽門鐵克防病毒產品或產品報告無法刪除檢測到的檔案，則可能需要停止該風險程式的運行，然後再嘗試刪除。為此，請在安全模式下執行掃描。刪除檔案後，以正常模式重新啟動電腦，然後繼續執行後續步驟。

### • 從登錄中刪除值

注意：賽門鐵克強烈建議您在修改登錄之前先進行備份。如果對登錄執行了錯誤的更改，可能導致永久性資料遺失或檔案損壞。

- a. 按下「開始」>「執行」，鍵入 regedit，然後按「確定」

**注意：**如果登錄編輯器無法打開，則表示病毒可能已修改了登錄以阻止對登錄表編輯器的瀏覽。賽門鐵克大中華安全機制應變中心開發的一個工具可解決此問題

([http://www.symantec.com/security\\_response/writeup.jsp?docid=2004-050614-0532-99](http://www.symantec.com/security_response/writeup.jsp?docid=2004-050614-0532-99))。

b. 找到病毒添加的子機碼或值並刪除它們

**注意：**要檢閱添加了哪些子機碼或值，請在

[http://www.symantec.com/business/security\\_response/index.jsp](http://www.symantec.com/business/security_response/index.jsp) 上搜索具體病毒，然後閱讀相關的技術資訊。

c. 如有必要，將病毒所修改的登錄子機碼或項目恢復到之前的值

- **清空 INTERNET 暫存檔案文件夾**

a. 啓動 Internet Explorer，按下「工具」>「網際網路選項」

b. 在「Temporary Internet Files」部分，按下「刪除檔案」按鈕

c. 勾選「刪除所有離線內容」，然後按下「確定」

### ▶ 防範網路釣魚攻擊

- 確保您造訪的網路銀行或組織的網址正確

- 在位址欄中手動輸入 URL，或使用我的最愛連結

- 不要直接從郵件裏剪貼鏈結並粘貼到 Web 瀏覽器

- 不要按電子郵件內的連結

- 小心處理電子郵件和個人資料

- 不要回復要求提供個人財務資訊的電子郵件

- 不要透過電子郵件發送有關個人、信用卡或線上帳戶的詳細資訊

- 不要在不確定其真實性的網站上輸入有關個人、信用卡或線上帳戶的資訊

- 定期檢查線上帳戶