# 網路疫情通報

## – 大中華地區

2013/02/18-2013/03/03

賽門鐵克安全機制應變中心

內 容

## 熱門病毒排行

| 排名 | 走勢 | 名稱 | 類型 | 風險級別 | 表現/描述 |
|---|---|---|---|---|---|
| 1 | → | W32.Almanahe.B!inf | 病毒 | 非常低 | W32.Almanahe.B!inf 表明偵測到了受 W32.Almanahe 病蟲感染的檔案。 |
| 2 | → | W32.Downadup.B | 病蟲 | 低 | W32.Downadup.B 是一種病蟲，可透過利用 Microsoft Windows Server Service RPC Handling Remote Code Execution 漏洞 (BID 31874) 進行散佈。該病毒試圖散佈至受簡易密碼保護的網路共用，並攔截對安全相關網站的存取。 |
| 3 | ↑ | XM.Mailcab@mm | 病毒 | 非常低 | XM.Mailcab@mm 是一種大量郵件巨集病毒，會在受感染的電腦上，將自己插入到任何開啓的 Microsoft Excel 文件中進行散佈。然後將自己寄送給 Microsoft Outlook 通訊錄中的所有聯絡人。 |
| 4 | ↓ | Trojan Horse | 木馬 | 非常低 | Trojan Horse 表明偵測到了各種木馬程式。 |
| 5 | ↓ | Trojan.Gen | 木馬 | 非常低 | Trojan.Gen 表明偵測到了多種木馬程式。 |
| 6 | ↑ | W32.SillyFDC.BDP!lnk | 病毒 | 非常低 | W32.SillyFDC.BDP!lnk 表明偵測到了由 W32.SillyFDC.BDP 病蟲建立的 .lnk 檔案。 |
| 7 | ↓ | Trojan.Gen.2 | 木馬 | 非常低 | Trojan.Gen.2 表明偵測到了許多形形色色的木馬程式，其特定的定義檔尚未建立。使用一般偵測，因爲它可以防範許多共用類似特性的木馬程式。 |
| 8 | ↓ | X97M.Laroux.gen | 病毒 | 非常低 | X97M.Laroux.gen 表明偵測到了 Excel 巨集病毒的 X97M.Laroux 系列。 |
| 9 | ↑ | Trojan.Maliframe!html | 木馬 | 非常低 | Trojan.Maliframe!html 表明偵測到了包含隱藏 iframe 元素的 HTML 檔案，其會嘗試在電腦上執行惡意動作。造訪惡意網頁時通常會偵測到此病毒，該惡意網頁試圖在目前頁面載入期間悄無聲息地將使用者導向至惡意 URL。 |

## 病毒趨勢

Adobe Flash 是網際網路上散佈最爲廣泛的產品之一。由於很受歡迎且在全球擁有龐大的客戶群，它往往會成爲網路罪犯的目標。網路罪犯使用社交工程方法，透過虛假的 Flash 更新網站來散佈惡意軟體，通常迫使那些可能需要軟體更新，但卻毫無戒備的使用者在無意中安裝惡意軟體。

最近，我們碰到了一個將自身僞裝成 Adobe Flash Player 更新頁面的惡意網站。在這個網站上，攻擊者向使用者提供兩個選項來確保使用者成功安裝完成：1) 彈出訊息要求使用者下載 flash_player_updater.exe 檔案；2) 彈出「立即下載」按鈕要求使用者下載 update_flash_player.exe 檔案。

攻擊者建立了一個看似非常可信的登陸頁面；但是，也有一些矛盾之處。頁面內的大多數連結都連結回攻擊網域，除轉至惡意軟體本身的連結之外，所有其他連結都連結回網站的根目錄，從而導致 404 錯誤。

賽門鐵克已提供安全防護，並將這些檔案偵測爲 Trojan Horse。

爲確保您不會成爲受害者，首先請確保經常更新您的防毒定義檔，還需定期更新您的軟體套件。切勿從第三方網站上下載更新，並始終仔細核查所提供之下載的 URL。

## 熱門病毒

| | |
|---|---|
| 病毒名稱 | Trojan.Betabot |
| 病毒類型 | 木馬 |
| 受影響的系統 | Windows 98, Windows 95, Windows XP, Windows Server 2008, Windows 7, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000 |

執行後，Trojan.Betabot 會將自身複製到 %ProgramFiles%\Common Files\[木馬資料夾名稱]，然後重新命名爲 Flash Update Client 或 Windows Licence Check。隨後，該木馬會修改和建立登錄項目，以實現開機自啓動，並降低 Internet Explorer 的安全性設定。

Trojan.Betabot 會建立一個隱藏的 iexplore.exe 程序實例，並向其中插入惡意程式碼。隨後，該木馬會嘗試連線至遠端位置 http://webho[removed]tection.info/icool/orde[removed] 和 http://assler.hfgfr5[removed]g.com/cakes/sale[removed]，並開啓後門以允許遠端攻擊者存取受感染的電腦。最後，該木馬會結束所有開啓視窗的程式，包括 explorer.exe。

## 垃圾郵件趨勢

過去幾年，發佈的眾多報告、白皮書和部落格都詳細介紹了鎖定目標的攻擊。例如，一些攻擊利用複雜的感染方法 (如水坑攻擊)，另一些攻擊則依賴文件檔案中隱藏的侵入代碼，並混合運用社交工程手法。不久前，將虛假電子郵件用作感染方法的大量郵件病蟲仍然主導著惡意軟體世界，但有一種手法是冒充知名防毒廠商發出的詐騙性授權續購通知。一些人可能認爲這種手法已經絕跡，但最近有證據表明該手法仍然十分活躍。

垃圾電子郵件的附件具有 .doc.exe 副檔名，這很可疑。雖然此檔案使用 MS Word 圖示，但卻是一個可執行檔，因此不論電腦上是否安裝 MS Word，此檔案都會執行。賽門鐵克將此檔案偵測爲 Trojan.Dropper。該檔案一旦執行，它便會在電腦上植入一個簡單的後門 (偵測爲 Backdoor.Trojan)，該後門會連線至指令和控制 (C&C) 伺服器，並等待遠端攻擊者的指令。攻擊者可能會控制電腦，並隨心所慾地執行任何動作，包括竊取資訊以用於後續攻擊。

雖然使用防禦系統來抵禦複雜攻擊是絕對必要的，但通常一個簡單的老把戲就足以破壞電腦。在使用了安全軟體並且此類電子郵件很少進入到您的收件匣時，使用者往往就會忘記基本的安全作法。請務必記住一句話：「災難會趁您不備時來襲」。

## 熱門釣魚網站排行

| 目標網域 | URL | 解析後的 IP |
|---|---|---|
| citibank.com | http://42.96.128.6/ssl/online.citi.com/US/JPS/portal/garyc6@hotmail.com | 42.96.128.6 |
| taobao.com | http://taobao12.net.tf/member/login.jhtml.asp | 147.255.92.163 |
| | http://taobaoa11.net.tf/member/stolen_verify_yzm2.htm.asp | 147.255.106.4 |
| runescape.com | http://secure.runescape.com.iiok.asia/m=weblogin/pass.htm | 122.49.44.49 |
| | http://secure.runescape.com.q.aagp.asia/m=weblogin/loginform.html | 115.47.51.18 |