# 網路疫情通報

## – 大中華地區

2013/09/09–2013/09/22

賽門鐵克安全機制應變中心

內 容

# 熱門病毒排行

| 排名 | 趨勢 | 病毒名稱 | 病毒類型 | 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 伺服器服務 RPC 的遠端代碼執行漏洞 (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 | ↑ | Trojan Horse | 木馬 | 非常低 | Trojan Horse 表明偵測到了各種木馬程式。 |
| 4 | ↑ | Trojan.Gen | 木馬 | 非常低 | Trojan.Gen 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。 |
| 5 | → | 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。 |
| 6 | ↓ | Trojan.Malscript!html | 木馬 | 非常低 | Trojan.Malscript!html 是賽門鐵克用來識別包含惡意 JavaScript 的 HTML 檔案的一個特徵名稱。 |
| 7 | → | 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。 |
| 8 | ↑ | 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。 |
| 9 | ↓ | Trojan.Gen.2 | 木馬 | 非常低 | Trojan.Gen.2 表明偵測到了各種木馬程式。 |
| 10 | → | Trojan.Malscript | 木馬 | 非常低 | Trojan.Malscript 表明經啓發式偵測到了利用漏洞及 (或) 執行堆積填充的網路型惡意程序檔檔案。 |

## 病毒趨勢

Microsoft 最近發布了一則公告，通報 Internet Explorer 發現新的零日漏洞：Microsoft Internet Explorer 記憶體損毀漏洞 (CVE-2013-3893)。這則公告指出，此漏洞可能會損毀記憶體，讓攻擊者得以執行任意程式碼。攻擊手法是，引誘使用者透過 Internet Explorer 造訪特別架設的包含此漏洞的網站。Microsoft 還表示，目前已知利用此漏洞進行鎖定目標的攻擊爲數並不多。

Microsoft 尚未發布此漏洞的修補程式。爲確保客戶免受這個 Internet Explorer 零日攻擊的侵害，賽門鐵克已經採取如下防護措施：

防毒：

- Bloodhound.Exploit.513

入侵預防系統：

- Web Attack: Microsoft Internet Explorer CVE-2013-3893
- Web Attack: MSIE Memory Corruption CVE-2013-3893 3

與此同時，賽門鐵克將持續調查此攻擊，以確保提供最佳的防護措施。

## 熱門病毒

| | |
|---|---|
| 病毒名稱 | Trojan.Hesperbot |
| 病毒類型 | 木馬 |
| 受影響系統 | Windows 2000、Windows 7、Windows Me、Windows NT、Windows Server 2003、Windows Server 2008、Windows Vista、Windows XP |

Trojan.Hesperbot 是賽門鐵克安全機制應變中心近期偵測到的一種木馬，其會試圖竊取使用者資訊。

執行後，Trojan.Hesperbot 會建立新的登錄機碼，以便在每次 Windows 系統啓動時執行自身。然後，它會在使用者電腦上開啓後門。此後門會連接到 plxjd[removed]rxykeq.com，並開展一系列木馬行爲，如記錄使用者的鍵盤輸入資訊、擷取螢幕抓圖以及下載其他病毒模組。

## 垃圾郵件趨勢

最近我們觀察到有一波利用電子郵件的連結附檔進行的攻擊活動。連結的目標經過僞裝，看起來像連結到文字檔，引誘使用者開啓它，而使用者並不知道他們開啓的不是文字檔。

開啓連結檔案之後，就會發生一連串的事件，包括下載和執行多個程序檔。此程序結束時會顯示一個假冒的錯誤訊息，接著向遠端指令和控制 (C&C) 伺服器開啓一個後門，遠端攻擊者便得以在受感染的電腦上執行各種活動。

由此應認識到，在開啓連結檔案之前，請先仔細檢查該檔案實際所指向的位置。使用者從不應放鬆警惕，尤其是在收到帶有附件的電子郵件時。

## 熱門釣魚網站排行

| 目標網域 | URL | 解析後的 IP |
|---|---|---|
| taobao.com | http://as2s3.de.vu//error.asp | 112.213.118.137 |
| | http://taobaojinqian.tk | 108.186.214.66 |
| | http://ddtaobao.tk/index.asp | 142.0.131.186 |
| national.com.au | http://wssp.gl.gov.cn/faq/index.html | 218.5.1.72 |
| | http://club.doers.cn/css/nb/index.html | 221.181.73.48 |
| paypal.com | http://worldtrans.com.cn/cert/LoginAUD8Australiamonthlybupaypalcommunit6548cutor568453w47Complete/wr54i6rktdjfhdt567tyru.htm | 210.22.101.234 |