網路疫情通報

– 大中華地區

2013/01/21-2013/02/03

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 表明偵測到了被 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) 進行散布。該病毒試圖散布至受簡易密碼保護的網路共用，並攔截與安全相關的 Web 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 文件上來進行散布。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	↑	W32.Pinfi	病毒	非常低	W32.Pinfi 是一種常駐記憶體的變種病毒，會感染 .EXE 和 .SCR 檔案。此病毒還可透過對應磁碟機及網路共用散布。
8	↓	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。
9	↓	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。
10	↑	Trojan.ADH	木馬	非常低	Trojan.ADH 表明偵測到了不具備傳統特徵的全新惡意軟體威脅。此手法目標在於偵測由攻擊者刻意變異或變形的惡意軟體。

病毒趨勢

2012 年 2 月，我們曾通報過 Android.Bmaster (亦稱 Rootstrap)，此病毒感染了數十萬台裝置。當時，它是有史以來最大的行動殭屍網路。最近，Bmaster 殭屍網路則由新發現的 MDK 殭屍網路超越。

根據賽門鐵克的分析指出，MDK 木馬是 Android.Backscript 的新變種。我們在 2012 年 9 月便偵測到了這個威脅系列。MDK 的程式碼與 Android.Backscript 非常類似，而且兩者使用相同的憑證簽署 APK。不過，有別於之前的版本，這個新變種使用進階加密標準 (AES) 演算法來檔案中的加密資料，例如伺服器和指令。

一旦安裝之後，此木馬就可讓攻擊者遠端控制使用者的裝置，採集使用者資料，下載其他 APK，以及產生令人煩擾的廣告軟體。此木馬已被重新包裝在合法的應用程式內，包括 Temple Run (神廟逃亡)以及 Fishing Joy (捕魚達人)等熱門遊戲，引誘使用者安裝惡意軟體。此木馬也利用動態載入、資料加密以及混碼等手法來躲避偵測。

賽門鐵克將此 MDK 行動殭屍偵測爲 Android.Backscript。我們再次呼籲 Android 使用者只從知名且經過授權的應用程式廠商下載應用程式。此外，在裝置上安裝信賴的安全軟體也可保護您不受這類威脅侵犯。

熱門病毒

病毒名稱	Trojan.Spachanel
病毒類型	木馬
受影響系統	Windows 98, Windows 95, Windows XP, Windows Server 2008, Windows 7, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

Trojan.Spachanel 是賽門鐵克安全機制應變中心近期偵測到的木馬，此木馬會注入系統程序並且盜取使用者資訊。

執行後，Trojan.Spachanel 會建立新的登錄項目，以實現開機自我啓動。此外，該木馬會將自身注入系統程序中，尤其是瀏覽器程序，如 iexplore.exe、chrome.exe、firefox.exe 等，並從受感染電腦中竊取電腦所在區域、硬碟資訊、作業系統版本等資訊，並將竊取的資訊發送到 http://46.10[REMOVED]1.121。

垃圾郵件趨勢

賽門鐵克安全機制應變中心獲報最近有假冒的聯邦快遞 (FedEx) 電子郵件流竄。這些電子郵件聲稱使用者必須按下連結來列印收據，然後親自到最近的聯邦快遞辦公室收取包裹。很顯然地，這些包裹並不存在。而按下連結的使用者會在電腦上產生 PostalReceipt.zip 檔案，其中包含惡意的 PostalReceipt.exe 執行檔。使用者不是收到從未訂過的包裹，而是在電腦上收到 Trojan.Smoaler 這份大禮。

傳遞此惡意軟體的所有假聯邦快遞電子郵件內容幾乎都相同，只有訂單編號和裝載 zip 檔的網站不同。電子郵件的訂單日期都一樣，這可能是惡意軟體開發者懶得改，或沒注意到細節。不過，裝載 Trojan.Smoaler 的網域確實每天變換。

聯邦快遞已在其網站上發布警告，並提供關於線上安全的進一步資訊。和往常一樣，我們建議使用者將防毒軟體維持在最新狀態，並避免按下從不明寄件者收到的電子郵件中的連結。如果可疑的電子郵件是來自您通常沒有個人往來的組織，應可認定這些電子郵件可能是惡意的，不應開啓來看。

熱門釣魚網站排行

目標網域	URL	解析後的 IP
poste.it	http://sistema.sicurezza.jjrup4vc.kuzeyyapiinsaat.com.tr/servizi/poste.php	183.232.10.67
	http://211.95.64.88/postaclick/cliente/utente/index.html	211.95.64.88
battle.net	http://us.battle.net.jjwow.asia/login/en/password.htm	118.244.132.16
	http://hourms-gooled.tk/login.asp	112.213.97.34
runescape.com	http://secure.runescape.com.qqweb.asia/m=weblogin	118.244.132.16