網路疫情通報

– 大中華地區

2012/01/09-2012/01/29

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.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。
2	↑	Trojan Horse	木馬	非常低	Trojan Horse 表明偵測到了各種木馬程式。
3	↓	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。
4	→	Trojan.Gen	木馬	非常低	Trojan.Gen 表明偵測到了多種木馬程式。
5	→	Trojan.Gen.2	木馬	非常低	Trojan.Gen.2 表明偵測到了各種木馬程式。
6	→	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。
7	↑	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。
8	↑	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。
9	↑	Trojan.ADH.2	木馬	低	Trojan.ADH.2 表明偵測到了不具備傳統特徵的全新惡意軟體威脅。

病毒趨勢

賽門鐵克安全機制應變中心獲報有惡意軟體利用 Microsoft Windows Media Player 的 winmm.dll MIDI 檔案剖析遠端緩衝區溢位漏洞 (BID 51292) 進行擴散。

這項進行中的攻擊涉及多個病毒檔案：mp.html 和 i.js (兩者經偵測皆爲 Trojan.Malscript)、baby.mid (經偵測爲 Trojan Horse)，以及 a.exe (經偵測爲 Downloader.Darkmegi)。

在此同時，Microsoft 已發布修正程式來防堵此漏洞。建議使用者務必套用此修正程式。

熱門病毒

名稱	VBS.Sojax
類型	木馬
受感染系統	Windows 95/98/Me/NT/2000/XP/Vista、Windows Server 2003

VBS.Sojax 是一個惡意程式碼，它會在被感染的電腦中收集網路、程序、檔案清單及系統資訊等，存放到 %WINDOWS%\NtUninstallKB 下，然後將收集的資訊打包上傳到遠端攻擊者的指令控制中心。此外，它還會從遠端攻擊者的指令控制中心讀取 html 網頁檔，分析出其中的指令並執行。這些指令包括上傳檔案到指令控制中心、從指令控制中心下載檔案、執行指令等。

VBS.Sojax 通常由惡意 PDF 和 Word 檔案釋放到電腦中。

垃圾郵件趨勢

每逢佳節或特殊事件臨近，垃圾郵件必定大增。賽門鐵克研究人員發現，隨著西洋情人節越來越接近，垃圾郵件也跟著暴增。與西洋情人節相關的垃圾郵件多半以珠寶首飾、情人節大餐和昂貴禮物下殺驚人折扣爲主軸。另外常見的假促銷活動還包括：網上銷售藥品、假電子賀卡、禮券、巧克力和花束。這些假促銷活動的目的是爲了獲取使用者的個人和財務詳細資料。

與西洋情人節相關的垃圾郵件很容易辨認，可以觀察「寄件者」標頭，例如「寄件者: 情人節禮物 <info@」；主旨列通常類似於「主旨:立即訂購！情人節花束和禮物只要美金 19.99 元起！」。

此外，我們也發現還有以西洋情人節爲目標的其他明顯攻擊，例如釣魚網站和下載電子賀卡的惡意軟體。這些攻擊預計今年也不會缺席。我們建議使用者在進行任何線上交易之前，務必遵循一般安全準則。

熱門釣魚網站排行

目標網域	URL	解析後的 IP
taobao.com	http://item.taobao.com-aiopj.osa.pl/item.asp	210.56.56.45
	http://iten.taobao.com-vmsdr.osa.pl/item.htm.asp	112.213.118.186
	http://mai123taobaocom5888.osa.pl/member/minilogin.asp	175.41.25.99
paypal.com	http://bjszkj.com/2011314ad/sk/login.html	210.51.7.220
	http://pppayyppall.is-saved.org/aus/paypal.com.au/paypal.com.au/webscr.html	124.162.53.184
alipay.com	http://110.75.133.25/read-htm-tid-5924640.html	110.75.133.25