網路疫情通報

– 大中華區

11/23/2009-12/06/2009

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	→	Trojan Horse	木馬	非常低	Trojan Horse 表明偵測到了各種木馬程式。
2	↑	W32.SillyFDC	病蟲	非常低	W32.SillyFDC 表明偵測到了 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。
3	↑	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與安全相關的 Web 網站的存取。
4	↓	Downloader	木馬	非常低	Downloader 會連線到 Internet 並下載其他木馬或元件。
5	↓	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、洛汗和熱血江湖等遊戲。
6	↑	W32.Downadup!autorun	病蟲	非常低	W32.Downadup!autorun 表明偵測到由 W32.Downadup 系列病蟲置入的 autorun.inf 檔案。
7	↓	W32.Fujacks!html	病蟲	非常低	W32.Fujacks!html 表明偵測到 .htm、.html、.php、.asp 或 .jsp 檔案感染了 W32.Fujacks 系列病蟲。
8	→	Backdoor.Trojan	木馬	非常低	Backdoor.Trojan 表明偵測到試圖在受害電腦上開啟後門的木馬。
9	↑	W32.SillyDC	病蟲	非常低	W32.SillyFDC 表明偵測到了 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。
10	→	Trojan.Dropper	木馬	非常低	Trojan.Dropper 是一種木馬，可將木馬病毒或後門木馬置入受感染的電腦。

病毒趨勢

Mozilla Firefox 瀏覽器一直都深受使用者歡迎。最近的一項有關市場份額的調查顯示，世界範圍內共有 24% 的使用者在使用 Firefox。Firefox 成功的一個重要方面在於，使用者可以透過使用外掛程式或延伸元件輕鬆地延伸其功能。正因如此，此受歡迎且靈活易用的軟體已經成為了惡意軟體作者所垂涎的目標。

賽門鐵克最近觀察到可以安裝惡意 Firefox 延伸元件的惡意軟體正在增加，其目的是最大化地影響使用者的電腦。此外，在 Firefox 中，可以將延伸元件作為未經處理的元件直接安裝到 Firefox 的核心資料夾內。這意味著，元件能夠在使用者毫不知情的情況下被載入。使用者沒有任何方法能夠將其從瀏覽器內停用或移除。當瀏覽器崩潰或發生故障時，使用者亦不會聯想到故障與惡意元件有關，或者停用該元件。

為了解決此問題，Mozilla 的開發者們現在決定刪除該功能，並且在 Firefox 3.6 及更新版本中僅上載其公司內的核心元件。這能夠防止惡意附加程式在將來利用該方法，但不幸的是，這並不是病毒攻擊者攻擊的唯一伎倆。同時，當有提示詢問使用者是否要安裝附加程式至瀏覽器時 (無論是何種附加程式)，請在允許程式執行之前仔細檢驗發行者的身分。

熱門病毒

病毒名稱	Backdoor.Tidserv.I!inf
病毒類型	木馬
受感染系統	Windows 2000/XP/Vista/NT、Windows Server 2003

Backdoor.Tidserv 是一種具有 Rootkit 功能的後門程式，自出現以來它就一直在演化以躲避安全軟體的偵測。在以往的版本中，Backdoor.Tidserv 會透過感染系統 dll 檔案如 advapi32.dll 來載入自身。現在，它開始採用感染驅動程式的方式來載入惡意程式碼。這些被感染的驅動檔案被偵測為 Backdoor.Tidserv.I!inf，新增的惡意程式碼通常被放置在目標驅動檔案程式碼的資源節中。當感染後的驅動被載入時，將首先執行其中的病毒程式碼，它將會試圖讀取並執行存放在硬碟最後幾個磁區上的惡意程式碼。

該後門程式主要透過網路掛馬等方式散佈。因此，建議使用者盡量不要造訪可疑網站，不要輕易從網上下載來歷不明的應用程式。

垃圾郵件趨勢

鑒於目前嚴峻的 H1N1 形勢，新啟動的政府 H1N1 疫苗接種項目廣泛引起了民眾的關注。因此，人們對和該主題相關的資訊與通知會格外留意。當與該主題相關的電子郵件進入使用者的郵箱時，使用者很有可能會將其開啟，甚至按照電子郵件的指導說明進行作業。

垃圾郵件攻擊者自然不會放過這一絕佳機會。賽門鐵克最近偵測到了與 H1N1 疫苗接種相關的垃圾郵件活動，這些垃圾郵件聲稱來自政府機構。垃圾郵件目的在於假借「建立個人醫療檔案」的名義收集使用者的個人資訊，或者提示使用者按下一些 URL 連結，實際上卻是將使用者重新導向至一些惡意網站或將惡意代碼下載至使用者的電腦。我們建議使用者在執行任意作業前，先慎重檢查電子郵件並檢驗發件人的身分，以避免潛在的病毒感染您的電腦。

熱門釣魚網站

目標網域	URL	解析後的 IP
yahoo.com	http://login-yaboo.com/config/computer1.htm	221.231.138.37
	http://login-yahoo.net/config/phone2.htm	221.231.140.164
	http://businesssoft.org/mc191/en/login_verify2.asp	61.164.109.113
msn.com	http://jay_dasilva.woooh-i-got-your-pics.com	202.181.203.146
	http://login-live-com.twvista.com/logon.srfwa=wsignin2.0&rpsnv=10&ct=12	220.207.2.8
taobao.com	http://taobaooo.web013.boothost.com/2010/index2.htm	61.191.55.28
	http://item.taobao.com.aciuoon.sov.tw/auction/aitem_detail3.asp	60.191.221.177
sina.com.cn	http://qq393.com/sina/index1.htm	121.11.69.78
	http://qq393.com/sina/index1.htm	221.5.10.156