網路疫情通報

– 大中華地區

2013/01/07–2013/01/20

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	↑	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。
5	↓	Trojan Horse	木馬	非常低	Trojan Horse 表明偵測到了各種木馬程式。
6	↓	Trojan.Gen	木馬	非常低	Trojan.Gen 表明偵測到了多種木馬程式。
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	→	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。
10	↑	Downloader.Trojan	木馬	非常低	Downloader.Trojan 是賽門鐵克用來識別惡意軟體程式的一個偵測名稱，這些惡意軟體程式的主要功能就是下載內容。

病毒趨勢

當某個病毒與另一個病毒聯合行動時，二者的病毒能力可能會成倍增長。在最近分析 W32.Virut 範例的過程中，我們發現該病毒會下載一種名爲 Waledac (也稱爲 Kelihos) 的殭屍網路變種，賽門鐵克將其偵測爲 W32.Waledac.D。電腦一旦受到感染，它即會透過伺服器，從指令伺服器提供的清單傳送垃圾電子郵件。最近分析的一台特定受感染電腦表明，可從每個 Bot 傀儡程式傳送的垃圾郵件數目非常巨大，而多台受感染的電腦相結合可能導致每天送出數十億封垃圾郵件。

賽門鐵克上個月的遙測資料 (圖 1) 顯示，受 W32.Waledac.D 感染的電腦數目在繼續增長，而美國則是目前最大的感染集中地。

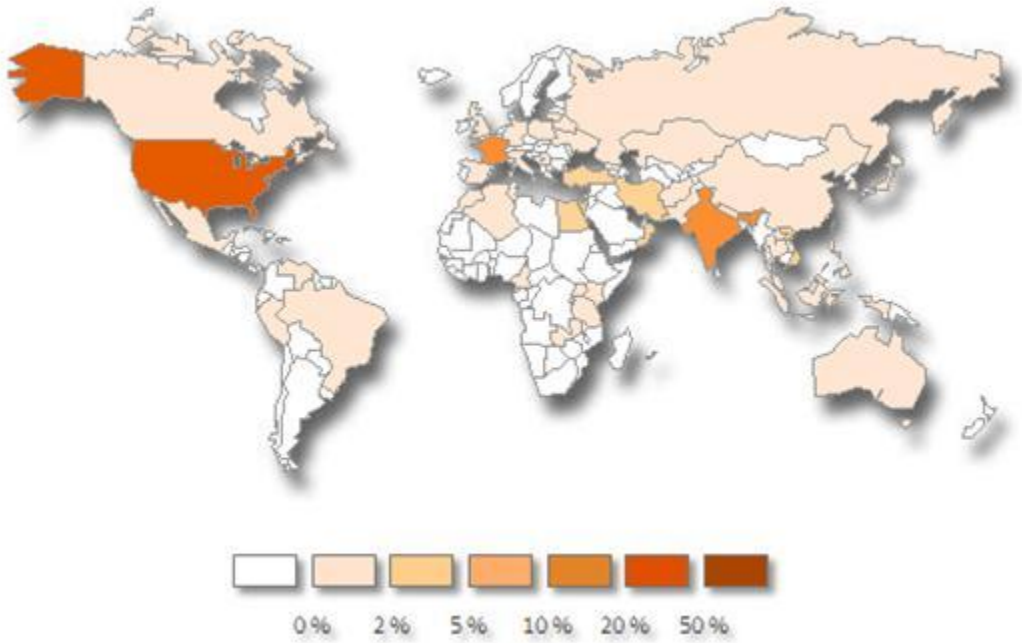

圖 1. *根據近期遙測資料統計的全球 Waledac.D 偵測結果*

賽門鐵克安全機制應變中心將繼續監控這些疫情，並在遇到新變種時更新或新增偵測結果。賽門鐵克建議您採用最新的賽門鐵克技術，以協助防範殭屍網路感染。

熱門病毒

病毒名稱	PHP.Brobot
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

PHP.Brobot 是一種 PHP 特洛伊木馬程式，它會允許遠端攻擊者利用裝載 Web 伺服器的受感染電腦，來發動分散式阻絕服務攻擊 (DDoS)。攻擊者會向 PHP.Brobot 提供目標位址、目標通訊埠號、資料緩衝區大小及攻擊持續時間。在攻擊者傳送 start 指令並提供上述參數後，該木馬程式即會向目標發動 DDoS 攻擊。此外，攻擊者可能還會傳送停止指令來終止攻擊，以及 status（狀態） 指令來檢查特定電腦是否已受感染。

垃圾郵件趨勢

最近，我們偵測到一個先進的網路間諜網路，其目標是知名度較高的組織 (如能源和電信部門) 及政府機構。其主要使用的攻擊方法爲魚叉式網路釣魚。這些魚叉式網路釣魚電子郵件包含了利用數個已知漏洞來感染電腦的 Word 文件或 Excel 試算表附件。利用的漏洞包括：

- Microsoft Excel FEATHEADER 記錄遠端程式碼執行漏洞 (CVE-2009-3129) – MS Excel，經偵測爲 Bloodhound.Exploit.306
- Microsoft Office RTF 檔案堆棧緩衝區溢位漏洞 (CVE-2010-3333) – MS Word，經偵測爲 Bloodhound.Exploit.366
- Microsoft Windows 通用控制項 ActiveX 控制項遠端程式碼執行漏洞 (CVE-2012-0158) – MS Word，經偵測爲 Bloodhound.Exploit.457
- Oracle Java SE Rhino 程序檔引擎遠端程式碼執行漏洞 (CVE-2011-3544)，經偵測爲 Trojan.Maljava 和 Trojan.Maljava!gen27。我們的入侵預防特徵 Web Attack: Oracle Java Rhino Script Engine CVE-2011-3544 和 Web Attack: Oracle Java Rhino Script Engine CVE-2011-3544 3 也會攔截這種漏洞

備受矚目的攻擊活動利用魚叉式網路釣魚電子郵件並不是頭一次見。而作爲一種常見方法，類似這樣的攻擊也可能不是最後一次。我們建議您確保作業系統和軟體均爲最新狀態，並避免點選可疑連結及開啓可疑的電子郵件附件。

熱門釣魚網站排行

目標網域	URL	解析後的 IP
battle.net	http://us.battle.net.ttwow.asia/login/en	118.244.130.28
	http://bolack-lackds.tk/login.asp	175.41.17.230
	http://sanred-bolack.tk/login.asp	112.213.97.34
bankofamerica.com	http://vippiao.com.cn/bofa/joe@asi-sd.com	223.4.212.54
runescape.com	http://secure.runescape.com.sswow.asia/m=weblogin/loginform.html	118.194.237.51