網路疫情通報

– 大中華地區

2014/03/31–2014/04/13

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.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。
3	→	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 的遠端程式碼執行漏洞 (BID 31874) 進行散佈。該病毒還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。
4	→	XM.Mailcab@mm	病毒	非常低	XM.Mailcab@mm 是一種大量郵件巨集病毒，透過在受感染的電腦上，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。
5	→	Trojan Horse	特洛伊木馬程式	非常低	Trojan Horse 是賽門鐵克用來識別惡意軟體程式的一個偵測名稱。有些惡意軟體程式僞裝成爲良性應用程式或檔案，賽門鐵克會使用此偵測來識別這些惡意軟體程式。
6	→	Trojan.Gen	特洛伊木馬程式	非常低	Trojan.Gen 表明偵測到了許多形形色色的特洛伊木馬程式，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特洛伊木馬程式。
7	→	Trojan.Gen.2	特洛伊木馬程式	非常低	Trojan.Gen.2 表明偵測到了多種特洛伊木馬程式。
8	↑	ALS.Bursted.B	病毒	非常低	ALS.Bursted.B 是以 AutoCAD 使用的 AutoLisp 程序檔命令語言所編寫的病毒。
9	↓	X97M.Laroux.gen	病毒	非常低	X97M.Laroux.gen 表明偵測到了 X97M.Laroux 系列的 Excel 巨集病毒。
10	↑	W32.Sality.AE	病毒	非常低	W32.Sality.AE 是一種病毒，藉由感染可執行檔的方式散佈，並會嘗試從網際網路下載可能惡意的檔案。

病毒趨勢

新發現的 Heartbleed 漏洞，也稱爲 OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability (CVE-2014-0160)，會對任何未修補的伺服器造成立即且嚴重的危險。它會影響 OpenSSL 一個稱爲 Heartbeat 的元件。OpenSSL 是 SSL (安全通訊端層) 和 TLS (傳輸層安全性) 通訊協定最廣泛使用的實作之一。

此漏洞可讓攻擊者截取安全通訊，然後竊取登入憑證、個人資料，甚至是解密金鑰等敏感性資訊。它是如何運作的？Heartbeat 會將一則訊息傳送到 OpenSSL 伺服器，再由伺服器將該訊息轉送回寄件者，藉此驗證連線。此訊息包含兩部分：稱爲酬載的資料封包 (大小可達 64 KB) 以及酬載大小的資訊。然而，OpenSSL 中的 Heartbleed 漏洞可讓攻擊者謊報酬載大小的資訊。例如，他們可以傳送大小只有 1 KB 的酬載，卻指出它有 64 KB。OpenSSL 伺服器無法驗證酬載是否與訊息所指出的大小相同。相反，它會假定酬載的大小正確無誤，並嘗試將它傳送回寄出的電腦。但是，由於它沒有完整的 64 KB 資料，因此反而會自動使用應用程式記憶體中儲存在其旁邊的資料「填滿」酬載。這可能包括使用者的登入憑證、個人資料，在某些情況下，甚至還包括 session (階段作業) 和私密加密金鑰。

給企業的忠告：

1. 使用 OpenSSL 1.0.1 至 1.0.1f 的任何人應該更新到最新修正版的軟體 (1.0.1g)，或是重新編譯不含 heartbeat（心跳）擴充功能的 OpenSSL
2. 移到修正版 OpenSSL 之後，如果您認定您的 Web 伺服器憑證可能因爲漏洞利用，導致已遭受感染或遭到盜取，請聯絡憑證授權中心進行更換
3. 最後，最佳實務準則是，企業應該同時考量重設在受感染伺服器記憶體中可能可見的一般使用者密碼

熱門病毒

病毒名稱	W32.Pixipos
病毒類型	病蟲
受影響系統	Windows XP, Windows Server 2008, Windows 7, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

執行後，W32.Pixipos 會建立新的登錄機碼項目，以實現開機自動啓動。隨後，該病蟲會從 PoS (銷售點，Point of Sales) 系統收集資料，並將其上載到指定的遠端位址 yo.u-[removed]ho.com/ss/gate.php。該病蟲主要透過將自身複製到卸除式儲存裝置進行傳播。

垃圾郵件趨勢

垃圾郵件活動不一定都鎖定在大量的收件者。我們最近發現一個含有資訊竊取惡意軟體附件的新垃圾郵件活動，該活動將其目標限定爲線上購物網站的管理員。

攻擊者可能基於各種原因，鎖定這些收件者。由於大多數的網路商店都會在網頁上提供聯絡人詳細資料，因此成爲容易下手的目標，因爲他們的電子郵件地址很容易透過檢索(crawl) 網站來收集。攻擊可也可能鎖定收件者來取得公司的帳戶詳細資料，以便竊取商店所維護的資料。攻擊者可能也想要攻破購物網站，以便對商店的訪客執行進一步的攻擊。

隨附的惡意軟體可能會在受感染的電腦中執行各種惡意動作，像是記錄按鍵輸入、取得剪貼簿資料，以及竊取數個應用程式的帳戶憑證。線上商店的店主在處理不明寄件者所寄出的來路不明的電子郵件時，應該小心，並且無論所在地區爲何，都應該奉行最佳安全實務準則。

熱門釣魚網站排行

目標網域	URL	解析後的 IP
alipay.com	http://xili8.us.cdshijue.net/b1.asp	103.242.2.237
	http://1.5968963720.kttshijue.com/tuikuan/b1.asp	182.236.241.163
	http://hzycgps.com.cn/tuikuan/a1.asp	182.236.250.148
taobao.com	http://taobaovsu.com/index1.asp	103.27.109.30
	http://taobaowce.com/index1.asp	113.10.157.169
battle.net	http://battle.net.blizzardentertainmentfreeactivitiesu.com/6.html	122.10.94.86