HKCERT 資訊保安報

本月內容

免費短訊服務

短訊警告服務是新增的免費服務，讓你在何時何地均可接收及時的保安警報，作出相應的防範。

詳情請瀏覽：

https://www.hkcert.org/chinese/subscribe_ssl.html

中小型企業資訊保安指南

香港電腦保安事故協調中心、政府資訊科技總監辦公室及香港警察推出了第三版的「中小型企業資訊保安指南」，內容也增加了對中小企業適用的持續業務運作規劃。

如欲取得此指南之最新版本，可至本中心網站下載，網址爲：

http://www.hkcert.org/chinese/sguide_faq/sguide/sme_guideline.pdf

電腦保安警報

保安警報					
日期/資料來源	**名稱**	**操作平台/軟件供應商**	**受影響之系統**	**影響**	**緩和措施/解決方案**
2008/05/02	Novell GroupWise "mailto:" URI 遠端緩衝區滿溢漏洞	Novell	- Novell GroupWise v 7.0 及之前的版本	- 阻斷服務 - 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/02	IBM Lotus Expeditor "cai:" URI 處理器指令碼插入漏洞	視窗	- IBM Lotus Expeditor Client for Desktop 6.1 版本	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/14	雅虎助手 "ynotifier" ActiveX 控制器執行程式碼漏洞	視窗	- 雅虎助手 3.6 及之前的版本	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/14	微軟視窗 CE 處理圖像漏洞	視窗	- 微軟視窗 CE 5.0	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/14	微軟 Jet 引擎 MDB 檔案剖析堆疊溢位漏洞	視窗	- 微軟 Jet 4.0 資料庫引擎 ・ 微軟視窗 2000 ・微軟視窗 XP ・微軟視窗伺服器 2003	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/14	微軟 Publisher 物件處理常式驗證漏洞	視窗	- 微軟 Office 2000 - 微軟 Office XP - 微軟 Office 2003 - 2007 微軟 Office System - 微軟 Publisher 2000 - 微軟 Publisher 2002 - 微軟 Publisher 2003 - 微軟 Publisher 2007	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報

日期/資料來源	名稱	操作平台/軟件供應商	受影響之系統	影響	緩和措施/解決方案
2008/05/14	微軟 Word 兩個漏洞	視窗/Mac	- 微軟 Office 2000 - 微軟 Office XP - 微軟 Office 2003 - 2007 微軟 Office System - 微軟 Word 2000 - 微軟 Word 2002 - 微軟 Word 2003 - 微軟 Word 2007 - 微軟 Outlook 2007 - 微軟 Word Viewer 2003 - 適用於 Word、Excel 及 PowerPoint 2007 檔案格式的 Microsoft Office 相容性套件 - 微軟 Office 2004 for Mac - 微軟 Office 2008 for Mac	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/19	Debian/Ubuntu OpenSSL 隨機數字產成器漏洞	Linux	- Debian GNU/Linux、Ubuntu 及其他以 debian 爲基礎的作業系統。	- 遠端執行程式碼 - 中間人攻擊	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/21	CA 產品執行程式碼及操縱檔案漏洞	視窗	- CA ARCserve Backup r11.5 (從前稱爲 BrightStor ARCserve Backup r11.5) - CA ARCserve Backup r11.1 (從前稱爲 BrightStor ARCserve Backup r11.1) - CA ARCserve Backup r11.0 (從前稱爲 BrightStor ARCserve Backup r11.0) - CA Server Protection Suite r2 - CA Business Protection Suite r2 - CA Business Protection Suite for Microsoft Small Business Server Standard Edition r2 - CA Business Protection Suite for Microsoft Small Business Server Premium Edition r2	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/26	FileZilla GnuTLS 多個漏洞	視窗	- FileZilla 3.0.10 之前的版本	- 阻斷服務 - 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報					
日期/資料來源	**名稱**	**操作平台/軟件供應商**	**受影響之系統**	**影響**	**緩和措施/解決方案**
2008/05/28	Adobe Flash Player 不明的遠端執行程式碼漏洞	視窗	- Adobe Flash Player 9.0.124.0 及之前的版本	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/29	Samba "receive_smb_raw()" 遠端緩衝區滿溢漏洞	所有	- Samba 3.0.29 及之前的版本	- 遠端執行程式碼 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/05/30	CiscoWorks Common Services 遠端執行程式碼的漏洞	Cisco	- CiscoWorks Common Services 3.0.3 版本 - CiscoWorks Common Services 3.0.4 版本 - CiscoWorks Common Services 3.0.5 版本 - CiscoWorks Common Services 3.0.6 版本 - CiscoWorks Common Services 3.1 版本 - CiscoWorks Common Services 3.1.1 版本 - 思科 Unified Operations Manager (CUOM) 1.1 版本 - 思科 Unified Operations Manager (CUOM) 2.0 版本 - 思科 Unified Operations Manager (CUOM) 2.0.1 版本 - 思科 Unified Operations Manager (CUOM) 2.0.2 版本 - 思科 Unified Operations Manager (CUOM) 2.0.3 版本 - 思科 Unified Service Monitor (CUSM) 1.1 版本 - 思科 Unified Service Monitor (CUSM) 2.0 版本 - 思科 Unified Service Monitor (CUSM) 2.0.1 版本 - CiscoWorks QoS Policy Manager (QPM) 4.0 版本 - CiscoWorks QoS Policy Manager (QPM) 4.0.1 版本 - CiscoWorks QoS Policy Manager (QPM) 4.0.2 版本	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報					
日期/資料來源	**名稱**	**操作平台/軟件供應商**	**受影響之系統**	**影響**	**緩和措施/解決方案**
			- CiscoWorks LAN Management Solution (LMS) 2.5 版本 - CiscoWorks LAN Management Solution (LMS) 2.5.1 版本 - CiscoWorks LAN Management Solution (LMS) 2.6 - CiscoWorks LAN Management Solution (LMS) 2.6 版本更新 - CiscoWorks LAN Management Solution (LMS) 3.0 版本 - CiscoWorks LAN Management Solution (LMS) 3.0 版本 2007 年 12 月更新 - 思科 Security Manager (CSM) 3.0 版本 - 思科 Security Manager (CSM) 3.0.1 版本 - 思科 Security Manager (CSM) 3.0.2 版本 - 思科 Security Manager (CSM) 3.1 版本 - 思科 Security Manager (CSM) 3.1.1 版本 - 思科 Security Manager (CSM) 3.2 版本 - 思科 TelePresence Readiness Assessment Manager (CTRAM) 1.0 版本		
2008/05/30	蘋果 Mac OS X 多個漏洞	Mac	- Mac OS X 10.4.11 版本 - Mac OS X 10.4.11 伺服器版本 - Mac OS X 10.5 至 10.5.2 版本 - Mac OS X 10.5 至 10.5.2 伺服器版本	- 遠端執行程式碼 - 繞過保安 - 跨網站指令碼 - 洩露系統資料 - 洩露敏感資料 - 權限提升 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

***** 在安裝修補程式前，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。

焦點新聞

公務員局失 USB 手指
載紀律研訊資料 分分鐘變金手指
2008 年 5 月 1 日

再有公職人員遺失載有個人資料的 USB 記憶體（俗稱「USB 手指」），公務員事務局轄下公務員紀律秘書處一名職員，上周遺失 USB 手指，載有涉及公務員行爲不當紀律研訊個案資料，當中包括 25 名公務員姓名及職銜，事件交警方處理。個人資料私隱專員公署表關注。
有立法會議員促政府暫時禁止員工用 USB 手指儲存重要資料：「今次可能會洩露投訴人資料，到時 USB 手指變金手指。」

繼衞生署、聯合、九龍及東區醫院先後遺失病人資料，公務員紀律秘書處昨公佈，一名研訊人員在 4 月 23 日報稱遺失一個 USB 手指，內存兩宗涉及兩名公務員的紀律研訊資料，內提及共 25 名在職公務員姓名及職銜，但沒有電話住址，也沒涉及公眾人士。發言人稱，已通知受影響人士並致歉，也已在 4 月 29 日報警，局方亦已向私隱署報告。她說已口頭警告該名員工，並提醒他及所有員工處理資料時需遵守指引，包括小心看管 USB 手指，並須爲內存資料設密碼。公務員事務局局長俞宗怡對此表關注。
[蘋果日報]

黑客程式扮鬼扮馬 Facebook 私隱易泄
2008 年 5 月 2 日

在電視節目中，BBC 的程式設計師皮特（Pete）示範用幾台手提電腦就輕易編寫了一個特別程式供使用者新增，整個過程不需 3 小時。他寫了一個叫「Miner」的惡意蒐集資料程式，Miner 可輕易僞裝成一個遊戲、小測驗或笑話來吸引用戶安裝。但無論這程式僞裝成什麼樣子，目的都是蒐集你及你朋友的個人資料，之後電郵到一個指定的電子郵箱。

事實上，Facebook 的用戶在新增應用程式後，除非有特別要求，否則你已經容許那程式讀取你大部分個人資料，包括你好友清單上的朋友資料。由於這些程式是在第 3 者的伺服器上運作而非 Facebook 伺服器，這令 Facebook 很難監測這些程式到底在做什麼，以及得悉它們所蒐集的資料用途。
[明報]

DHC 網站也傳會員資料外洩 數十人受害
2008 年 5 月 4 日

購物網站陸續傳出資料外洩事件，知名化妝品 DHC 的網站最近也被淪陷。警方調查，歹徒掌握會員訂購明細和付款方式，假冒客服人員打電話向消費者謊稱，因爲扣款錯誤，要前往 ATM 操作，才能退還誤扣款項，目前已知有數十名被害人報案。DHC 公關副理張珈銘表示，公司在得知消息，立即採取反制措施。

警方則是表示，DHC 緊急公告詐騙手法，也通知會員更改密碼，至今受騙人數已經大幅降低。警方也指出，不論超商取貨或者宅配到府，都不會因爲單據簽錯，一次付清改成分期付款，客服也不會要求會員操作 ATM，呼籲民眾要提高警覺。
[Yahoo!奇摩]

醫局 1 年失 6000 病人資料 5 醫院 9 宗 電腦相機被偷 千人資料沒加密
2008 年 5 月 6 日

醫院管理局遺失病人資料愈揭愈多，過去一年在 5 間醫院共發生 9 宗遺失病人資料事件，其中瑪麗及屯門醫院更發生電腦及手提電腦遺失事件；以宗數計，東區醫院是重災區。9 宗事件涉及 6000 名病人，其中 1000 人的身分證及基因等資料沒有加密，醫管局卻無通知所有受影響病人，只就 4 宗個案作通知。個人資料私隱專員吳斌表示嚴重關注事件。醫管局遺失的儲存病人資料電子儀器，除 USB 電子儲存卡（俗稱「手指」）外，還包括電子手帳、中央處理器、手提電腦、數碼相機及 MP3 機等。
[明報]

微軟恢復 XP 和 Vista 更新
2008 年 5 月 7 日

微軟 6 日表示，XP SP3 已開放網路下載，Vista SP1 的自動更新也已恢復。微軟已完成一項過濾機制，防止執行 Dynamics RMS 的主機下載更新。但過濾機制沒有解決之前的相容問題。

該公司以聲明表示：「這個問題的解決方案目前正在微軟進行測試，我們希望能在本月內提供給大眾。在此之前，微軟建議 Microsoft Dynamics RMS 的顧客不要安裝這兩個更新組件。」那些已經下載安裝這兩個 Windows 更新的 Dynamics RMS 顧客，應立即聯絡微軟的顧客支援部門。
[ZDNet 台灣]

匯豐失伺服器載 16 萬客資料
2008 年 5 月 8 日

匯豐銀行觀塘分行遺失一部電腦銀行伺服器，失去的帳戶資料多達近 16 萬個，包括帳戶號碼、姓名、交易金額及種類，觀塘重案組已接手調查。

伺服器於上月 26 日失竊，但匯豐至昨日方發出聲明交代事件，有客戶炮轟匯豐隱瞞錯失；匯豐則強調伺服器有多重保安，即使落入他人手中，資料失竊危機仍微，又指若客戶有任何損失，銀行均會負責。

事發的觀塘分行於上月 24 日開始裝修以增設

理財中心，於 26 日即失去一部電腦伺服器，內藏 15.9 萬個帳戶資料。警方發言人表示，匯豐銀行即日得悉事件並報警，案件列作盜竊案，由觀塘重案組跟進，至今無人被捕。匯豐發言人表示，伺服器有多重保安措施，遺失資料的危機甚微，但會去信通知受影響客戶，倘有客戶因事件蒙受損失將毋須承擔責任。
[明報]

你被偷的資料值多少錢？
2008 年 5 月 9 日

你被偷的資料值多少錢？你認爲個人資料無價？但凡是都有個價碼，包括你被偷的銀行帳號資料。McAfee Avert Labs 實驗室發現一張歹徒買賣個人資料的價目表，從信用卡號、銀行帳號登入、到各類從不知情網友身上騙來的消費資料都有一定行情。

「上週五在法國，我們的研究員找到這個網站，提供高於一般行情的"優質資料"價格。」McAfee 的 Francois Paget 表示。「但我們看了一下價格後發現，這跟其他買賣一樣，一分錢一分貨。」比如，一個在美國的華盛頓互助銀行（Washington Mutual Bank）帳戶餘額有 14,400 美元，售價 600 歐元（約 924 美元）；另一個英國花旗銀行帳號餘額 10,044 英磅則要價 850 歐元（約 1310 美元）。
[ZDNet 台灣]

趨勢：七成 PC 遭到灰色及犯罪程式感染
2008 年 5 月 12 日

趨勢科技今日指出全球遭灰色程式及犯罪程式感染的電腦已高達 72.5%。
此項報告顯示，透過線上掃毒軟體 HouseCall 針對包含台灣、澳洲、美國等二十個國家及地區的 291,084 台電腦進行掃瞄，結果顯示各類不懷好意的灰色程式早已攻佔其中，並且被植入廣告程式 (Adware) 的比例更高達 38.6%。

趨勢科技指出，遭駭客工具(Hacking Tools)入侵的電腦也有 15.8%，代表一般傳統病毒攻擊模式早已過去，潛藏其中以方便進行資料竊取或是成爲僵屍電腦家族一員藉以散發垃圾郵件才是駭客的首要目的。
[ZDNet 台灣]

智利 600 萬人資料外泄
黑客挑戰政府
2008 年 5 月 13 日

香港最近的熱門話題是公立醫院接連發生病人資料外泄的醜聞，在智利，政府部門的電腦系統上周五則遭黑客入侵，包括總統女兒在內的 600 萬名國民個人資料外泄，這些被盜資料包括身分證號碼、住址、電話號碼、電郵地址及教育背景等，黑客更一度將之張貼在網上任人看，聲稱這樣做是要顯示當局疏於保護機密資料。

智利當局周日表示，一名自稱「匿名儒夫」的黑客上周五入侵教育部、軍方及選舉部門的電腦系統，盜取 600 萬國民的個人資料。其後，這些資料被張貼在「FayerWayer」和「ElAntro」兩個熱門網站數小時，至周六早上，FayerWayer 網站的管理員通知警方。這些個人資料已從網上移除，當中有大批接受公共交通費優惠學生的資料，包括智利總統巴切萊特的其中一名女兒。這些交通證上有學生的相片和校名，沒有其他敏感資料。
[明報]

微軟公告五月份安全更新
2008 年 5 月 14 日

本月安全公告包括： MS08-26 ： Microsoft Word 中的弱點可能會允許遠端執行程式碼 (951207)。最高嚴重性等級爲重大。 MS08-027 ： Microsoft Publisher 中的弱點可能會允許遠端執行程式碼 (951208)。最高嚴重性等級爲重大。 MS08-028 ： Microsoft Jet 資料庫引擎的弱點可能會允許遠端執行程式碼 (950749)。最高嚴重性等級爲重大。 MS08-029 ： Microsoft Malware Protection Engine 中的弱點可能會允許拒絕服務 (952044)。最高嚴重性等級爲中度。

微軟強烈呼籲所有客戶立即使用「Windows Update 自動更新」功能隨時更新程式，避免惡意程式攻擊，或是立刻下載補充程式，以確保電腦使用的安全。微軟於 Windows Server Update Services (WSUS)、Windows Update(WU) 及下載中心發行新版的 Microsoft Windows 惡意軟體移除工具（網址： http://go.microsoft.com/fwlink/?LinkId=40573）。
[ZDNet 台灣]

網上保安軟件 難偵測假網站
2008 年 5 月 15 日

網絡上經常出現一些假冒網站，騙取用戶的個人資料，例如戶口密碼及信用卡資料。以爲安裝了網上保安軟件就萬無一失？消委會 《選擇》月刊引述國際消費者研究及試驗組織的測試，發現絕大部分樣本都未能預防網絡釣魚（phishing），用戶隨時誤闖假冒網站，令個人資料外泄。而綜合各方面的表現，「G DATA」的網上保安效能最理想，其次爲「BitDefender」及「F-Secure」。

網絡釣魚是指透過各種途徑，把用戶誘騙到假冒網站，騙取個人資料。是次測試發現大部分保安軟件都未能偵測到假冒網站，只有「Symantec」的表現顯著較佳，在 12 個假冒網站中，能偵測到 11 個。在防惡意程式及防火牆的保護效能上，表現較好的有「G DATA」、「F-Secure」及「Kaspersky」。
[明報]

黑客入侵紅會網站騙善款
2008 年 5 月 18 日

四川大地震牽動海內外人士的心，紛紛慷慨解囊捐助災民，但不法分子竟趁機大發國難財。寧波銀監局日前接獲中國銀監會緊急通報，稱經公安部核實，有不法分子入侵紅十字會官方網站，竄改抗震救災募捐的專用賬號進行詐騙。事件引起網友激憤，紛紛痛罵：「這些人該千刀萬剮，碎屍萬段！」

寧波銀監局通過提醒市民，在出救災捐款時，要仔細核實捐款賬號，盡量使用中央電視台、

電台、報紙等主流媒體上公佈的救災捐款專用賬號資訊，或在銀行櫃面獲取已經核實的相關救援組織名稱、開戶銀行、捐款專用賬號等資訊。
[蘋果日報]

BitDefender 偵測出新木馬程式擴散
2008 年 5 月 19 日

該公司之防護分析師發現一個拜占庭式的垃圾郵件散佈詭計，表示在含有影片連結的垃圾郵件中發現此木馬程式，當使用者試圖要點擊並觀看郵件中影片時，他們會被提示要下載一個媒體播放器(Media Player)。

這個媒體播放器事實上是一個名爲 Backdoor.Edunet.A 的惡意程式，透過受害者的電腦發送一系列的命令給郵件伺服器，這些專門被用來發送垃圾郵件的郵件伺服器大部分都是在.edu 或.mil 的網域中。因此提醒學校與軍事單位注意防範。伺服器的名單被木馬程式傳回到一系列位於攻擊者網路的網路伺服器中。網路伺服器的名單正持續的改變中，但是目標伺服器維持不變。
[明報]

假借川震搞鬼 駭客入侵 10 萬中文網頁
2008 年 5 月 20 日

四川地震撼動華人世界，不少人都會上網搜尋地震相關的訊息，甚至會透過網上平台捐款。資安公司發現，近日駭客就趁此新聞熱潮，針對中文網站發動一波惡意程式攻擊，許多慈善機構的網站都因此受害，目前已經有超過十萬個中文網頁被植入惡意連結。

資安公司趨勢科技指出，駭客主要是利用企業網站的漏洞入侵資料庫，然後在其網頁上以「資料隱碼」(SQL injection)的方式植入惡意連結，統計已經有超過十萬個中文網頁遭到入侵，受駭的中文網頁涵蓋了台灣、中國、香港和新加坡等地區，其中，中國大陸的網頁高達九成，多以非營利機構爲主，而且不乏知名的全球性慈善團體，不難想像駭客是想要利用民眾對四川地震的關心與善心而擴大攻擊。 趨勢科技資深技術顧問簡勝財 ：『是有駭客特別針對華人語系的網站或網頁，去做漏洞入侵及攻擊的動作。有一部份是蠻知名的公益網站，所以我們懷疑這些駭客是有意搭四川賑災的順風車，讓更多的 電腦使用者去中木馬或後門病毒。』
[Yahoo!奇摩]

Google 推網上病歷 病人權益組織憂泄私隱
2008 年 5 月 21 日

Google 周一推出名爲「Google Health」的網上病歷紀錄服務，讓美國用戶可在網上儲存及管理個人病歷資料，並可隨時隨地取得個人病歷資料的電子副本，包括處方、化驗結果、住院日數及醫療狀　等。Google Health 網頁亦可連結到藥房、診所及化驗室，互相交換資料，並可讓用戶取得醫療資訊，服務費用全免。

不過，Google Health 服務引起私隱權爭議，因電子醫療紀錄仍屬起步階段，美國只有少數法例保障網上紀錄私隱。Google 表示，已另建安全平台儲存醫療紀錄，有關資料會與 Google 搜尋系統分開處理，以保護用戶資料。
[明報]

「3」用戶流傳偽賑災短訊
2008 年 5 月 22 日

【明報專訊】有「3」用戶昨日向本報查詢，指一則聲稱由「3」發出的手機短訊(圖)，內容指用戶把有關短訊轉送予他人，「3」即會爲四川地震捐款 0.5 元，或有機會獲贈通話分鐘等。「3」接獲本報查詢後澄清，該公司未曾發出該短訊，短訊內容亦非事實。發言人表示昨日亦收到小量客戶致電查詢，事件已交由警方處理。

另外，「3」已在其公司網站 Planet 3 中設立捐款渠道，客戶可利用手機捐款，善款將存入「民政事務局局長法團——捐款」銀行帳戶，再轉交香港紅十字會、香港世界宣明會、救世軍、樂施會及聯合國兒童基金。詳情可致電 3162 3333 查詢。
[明報]

駭客藉地震新聞傳木馬病毒　民眾要當心！駭客藉地震新聞傳木馬病毒　民眾要當心！
2008 年 5 月 23 日

四川大地震是現在許多人最關心的新聞，但是卻有駭客利用這個機會傳播含有木馬病毒的電子郵件，已經有不少人受害。

根據了解，這封惡意電子郵件內容，主要是新華社的新聞報導四川地震死亡人數攀升到 3 萬 4 千多人，裡面有一個微軟公司的 WORD 程式檔案，只要一打開這份文件檔，木馬程式就會被植入用戶的電腦中，竊取個人的敏感機密資料，如果民眾看到這一類的電子郵件應該立即刪除以免受害。
[Yahoo!奇摩]

大規模攻擊事件主因：駭客工具結合 Google Hacking
2008 年 5 月 23 日

本週以來發生在亞洲地區、以中文網頁爲主要目標的大型資料隱碼(SQL Injection)攻擊事件，疑爲駭客透過專業工具結合 Google 搜尋引擎快速尋找網頁弱點所致。
上週起針對台灣及中國大陸地區中文網頁的大規模攻擊行爲有了初步分析結果，阿碼科技在分析攻擊行爲後表示，駭客疑似結合了當前流行的駭客自動攻擊工具與 Google 的搜尋能力，透過 Google 搜尋出網頁中可用來注入程式碼的「注入點」，再利用撰寫好的駭客工具在這些「注入點」中填入程式語法，以自動化手法，快速攻下大量網頁。
[ZDNet 台灣]

zip 包裝木馬 靠伊媚兒駭人
2008 年 5 月 26 日

台北市警方最近接獲不少民眾報案，指稱自己的電子郵件帳號和密碼遭盜用，或線上遊戲帳

號密碼遭入侵後，寶物或點數遭竊盜賣成爲「一無所有」，更有民眾上網以信用卡進行交易後，有使用期限等帳號資料竟遭盜用大量盜刷；警方發現被害人均曾接獲親友親切的問候信，並曾下載或打開附加檔案，結果中毒，遭駭客植入木馬程式爲所欲爲。

警方調查，幾乎只要使用過上網郵寄電子郵件功能者，都會接到類似的僞裝信，這種「包著糖衣的病毒」，往往採取附加「com」或「zip」檔案模式騙取善良的收信者下載，只要接獲類似要求下載打開郵件附加檔案者，應先求證，以免中毒。

[Yahoo!奇摩]

Foxy 疑泄放蛇警員身分

2008 年 5 月 27 日

今年 4 月 4 日及 5 月 7 日，警方及入境處先後承認有內部檔案經 Foxy(檔案共享軟件)外泄，不過，讀者羅先生投訴，不滿警方沒汲取教訓，機密繼續外泄。他指在 5 月 23 至 25 日，透過 Foxy 用「pol」字眼，找到及下載多個懷疑警隊內部機密檔案，包括：警隊銷 ㄖ 離職警員個人資料的程序、西鐵朗屏站今年初發生企圖搶槍案，以及警員放蛇買毒品經過等。有資深前線警員坦言，檔案格式與真的內部文件很像。

警察回應時，並無回應懷疑外泄檔案真僞，只是指商業罪案調查科科技罪案組正跟進了解事件。警察員佐級協會主席鍾錦華指若泄密文件屬實，性質嚴重，因放蛇警員身分外泄可能影響到同僚人身安全，會方會積極與警方管理層了解事件。

[明報]

泄密 3 警或處分 Foxy 再漏口供紙

2008 年 5 月 28 日

消息人士透露，3 名警員疑因使用裝有 Foxy 軟件私人電腦處理文件，導致警隊機密不慎外泄到互聯網，包括內有「放蛇」警員身分的文件，3 人可能須接受紀律處分。但本報發現，昨日仍繼續有其他警隊內部文件包括口供紙透過 Foxy 外泄，導致疑犯的父母及未成年女友的姓名、地址或電話號碼等個人資料曝光。

私隱專員吳斌非常關注有警隊機密外泄，他指公署可能需要作正式調查。對於警方及入境處接連有機密外泄，保安局長李少光昨日表示非常關注，指現正緊急檢討使用私人電腦及處理機密資料的程序，但沒有 ㄖ 象顯示警隊電腦被入侵。他強調，一向不鼓勵同事把機密文件帶回家工作，強調有嚴格程序去監管。

[明報]

政府部門公營機構 3 年泄 4.6 萬人私隱

2008 年 5 月 29 日

政府透露，政府部門及公營機構於過去 3 年發生多達 30 宗泄漏私隱事故，涉及多達 4.6 萬名市民的資料，其中九成半(4.4 萬)受害人資料由公營機構外泄。爲加強監管，立法會議員涂謹申建議立例強制公營機構，日後若發生大量市民私隱外泄事件，必須通知政府及私隱專員公署。

對於上述立法建議，政制及內地事務局回應指出，現時許多海外地區均沒有這項規定，故政府需要與私隱專員仔細研究才作決定。私隱專員公署則認同上述立法建議。

[明報]

評論：利用 DOS 攻擊盜版 好萊塢會不會太過火？

2008 年 5 月 30 日

一家公司合法透過 P2P 來傳送影片節目，卻遭大量流量攻擊導致上週斷線三天。可能的嫌疑犯竟是：一家受雇於影音製片大廠來打擊盜版的公司。這裡到底出了什麼問題？ Web TV 公司 Revision3 上週末發現公司的伺服器遭到大量流量攻擊而斷線，這是所謂的阻斷服務攻擊（DOS）的斷線手法。許多原本透過網路來接收娛樂/新聞資訊的用戶突然間都無法收訊了。

[ZDNet 台灣]

如有任何查詢，請聯絡
香港電腦保安事故協調中心
電話: **(852) 8105 6060**
傳真: **(852) 8105 9760**
電郵: hkcert@hkcert.org
網址：http://www.hkcert.org