我們能否應付未來的超級電腦病毒和蠕蟲

作者: 林兆康

未來互聯網上會有超級電腦病毒和蠕蟲嗎？它們會有多利害呢？我們能應付它們嗎？在討論這些問題前，先讓我們對近年的電腦病毒和蠕蟲作一個小小的回顧。

回顧

電腦病毒和蠕蟲都屬於惡意程式（malicious code）。它們能透過電腦操作系統裡的保安漏洞入侵電腦系統。在侵入系統後，它們會自我復製並尋找其他宿主（受害者）繼續傳播。蠕蟲是指不需要人手協助而能自我傳播的程式，例如在 2003 年 1 月爆發的 MS SQL Slammer worm。它能自動尋找並入侵宿主，在傳播過程中完全不需要人手協助。病毒是指需要人手協助才能傳播的程式，例如電子郵件內的附件程式。

近年的電腦病毒和蠕蟲已經開始擁有對方的特性。例如在 2001 年 8 月爆發的 Nimda 蠕蟲，它不但感染電子郵件和共享檔案，還會主動入侵 IIS 伺服器。同時，它們的傳播速度也越來越快。根據 CERT 的報告，2001 年 Code Red 能在 24 小時內感染 26 萬 5 千台電腦，而 2003 年爆發的 Blaster 卻能在相同時間內感染 33 萬 6 千台電腦。圖 1 顯示了 Code Red 和 Blaster 在首 18 個小時內的感染率。另外，Blaster 也擁有持久的感染力。在高峰期過後，當大部份電腦已安裝了修復程式，它依然能維持以每小時約 3 萬台電腦的速度繼續擴散。就算是今年 8 月的

北美大停電也只能令它的傳播延遲了數小時（見圖 2）。

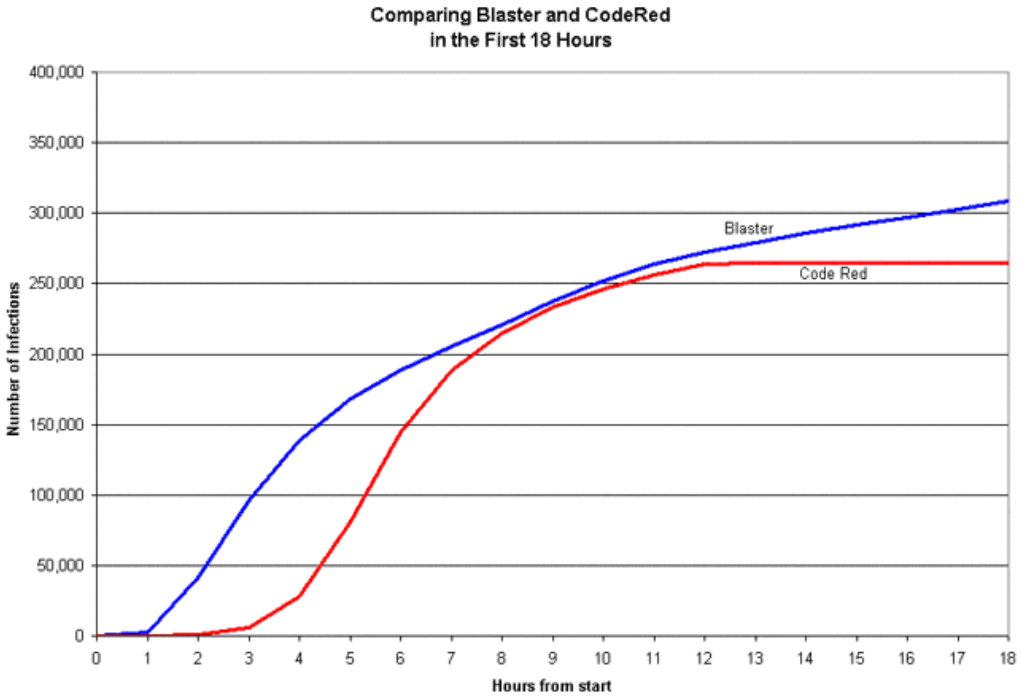

圖 1（來源：CERT）

圖 2（來源：CERT）

電腦病毒和蠕蟲對經濟的打擊相當驚人。根據 Computer Economics 估計，2003 年 8 月爆發的 Blaster worm，到 9 月為止已造成 5 億多美元的經濟損失。其他病毒和蠕蟲所造成的經濟損失見下表。

年份	名稱	全球經濟損失（美元）
2003	Slammer	10 億
2001	Nimda	6 億 3 千 5 百萬
2001	Code Red	26 億 2 千萬
2001	SirCam	11 億 5 千萬
2000	Love Bug	87 億 5 千萬
1999	Melissa	11 億
1999	ExploreZip	10 億 2 千萬

所有的病毒和蠕蟲都是利用已知的保安漏洞入侵電腦系統。在大規模爆發前，相應的修復程式已在互聯網上發放。但仍然有許多電腦因未能及時安裝而受到感染。修復程式的發放時間與病毒和蠕蟲的產生和爆發時間相距越短，越多電腦因未及安裝修復程式而受到感染。2003 年 1 月 Slammer worm 爆發，相對的保安漏洞修復程式早在 2002 年 7 月已經發佈。但在 2003 年 8 月 17 日爆發的 Blaster worm，其修復程式只在不足一個月前（2003 年 7 月 16 日）發佈。

超級病毒或蠕蟲的特性

從以上的例子看起來電腦病毒和蠕蟲似乎變得越來越利害和難以對付。將來會否出現我們無法對付的超級病毒或蠕蟲呢？要對付超級病毒或蠕蟲，我們首先需要預測它的特性。一個超級病毒或蠕蟲，需要俱備以下各項條件：

- 高傳播效率

  快速和多途徑的傳播能提高感染機會和持續擴散。傳播途徑不再局限於電子郵件或網頁，將包括新聞組、伺服器上的對外開放服務（例如：FTP，DNS 程式）、掌上電腦（PDA）或手提電話。除了視窗系統外，也可入侵其他操作系統，例如：各種 UNIX 系統（Linux，Solaris）、Cisco IOS 或 PALM OS，以增加傳播效率。

- 高度隱藏性及反追蹤能力

  能長期留在宿主內執行任務，例如收集資料、持續擴散或等待時機攻擊目標。反追蹤能力使病毒或蠕蟲不輕易暴露始作俑者身份及其運作原理。

- 高分佈率及高統籌效率

  能遍佈全球網絡並擁有相當規模的組織性。除了定時向始作俑者匯報進展及接收指令外，也會不時與同伴交換消息，並設有分區組長協調網絡傳播及攻擊。

- **多方面攻擊及摧毀互聯網基礎建設設施能力**

  能執行拒絕服務（Deny Of Service, DOS）攻擊、發放垃圾電子郵件、竄改網上資料（例如修復保安漏洞的程式）、刪除重要資料或改變網絡信息路徑。它們能攻擊並破壞重要網絡伺服器，例如：域名系統（Domain Name Service, DNS）伺服器或路由器（router），使其不能運作。頂層域名系統（Top Level DNS）伺服器和互聯網交換中心（Internet Exchange, 例如：HKIX）的路由器是互聯網最重要的基建設施。如果這些設施受到攻擊而停止運作，那互聯網就不是「大塞車」而是完全癱瘓，就像全球大停電一樣。

- **高智能及高度自決能力**

  根據實際客觀環境而自我調整，甚至自我演化。它們會分析宿主及其周邊網絡環境而選擇最有效的傳播途徑或攻擊方式。當與始作俑者或其他同伴失去聯絡時，會自行決定如何執行任務，例如：獨自攻擊或靜候東山復出時機。它們也會自行選出分區組長，重整架構並統籌運作。這種能力賦予病毒或蠕蟲頑強的生命力。

將來會有這樣的超級病毒或蠕蟲嗎？這看來好像天方夜譚，但隨　科技的進步和軟硬件的不斷提昇，筆者對它們的出現一點也不驚訝。在 1943 年，沒有人相信電腦將會像今天般普遍，IBM 更曾宣佈全球電腦市場只有 5 台。資訊科技一日千里，變化萬千，我們應該持有開放的思維去接受新事物和未知的可能性。

互聯網的隱憂

這樣的超級病毒或蠕蟲對我們的沖擊有多大呢？在討論這個問題前，先讓我們來看看互聯網的隱憂。現在全球共有超過 1 億 7 千萬台電腦連接互聯網，而且數字正在不斷增加。只要一小部份電腦沒有安裝適當的修復程式，這些電腦已足夠讓病毒或蠕蟲進行廣泛的破壞。同時電腦設備和寬頻頻寬的不斷提昇，也會促進病毒或蠕蟲的傳播能力。

雖然每天都有新的保安漏洞警告和相應的修復程式在互聯網上發佈，但是並非所有電腦都能及時安裝這些修復程式。箇中原因來自多方面。系統管理員因工作量大增，沒有足夠時間安裝程式。另一方面，越來越複雜的操作系統和應用軟件也阻礙了安裝速度。有時候，安裝了某個修復程式後，其他的應用軟件因受影響而不能如常運作。所以系統管理員在安裝修復程式前需要制定週詳的應變計劃，確保所有操作系統和應用軟件運作正常。通常越複雜的操作系統和應用軟件，需要越多時間作安裝調整。

除此之外，軟件或硬件生產商往往把一些良好的保安功能（例如：防火牆）從預設安裝中刪除，雖然這樣可以減低售後服務成本，但卻將用家的電腦置於險境中。隨　互聯網越來越普及，各階層人仕都有機會上網，但大部份用戶的資訊保安意識都不高。他們經常因貪圖一時之便而繞過原有的保安功能或程序，結果付出沉重的代價。甚至有些資訊經理也因為資源問題而把資訊保安優先權降低，這些短視的行為往往為他們帶來得不償失的後果。

最壞的狀況

根據以上的分析，當超級電腦病毒和蠕蟲出現時，對我們的打擊有多大呢？請大家想像以下的情況。假設一個超級蠕蟲利用一個尚未發現的保安漏洞去傳播。這現象稱為零點攻擊（zero-day exploit）。以現在互聯網的狀況，其感染率和滲透率會非常高，可能在數小時內已感染了大部分的電腦。由於其高度隱藏性，沒有人察覺到差不多所有互聯網及內聯網上的電腦都已受感染，不論它們是採用哪種作業系統。這些超級蠕蟲會默默地在背後收集有用資料，安排有利條件，為日後的襲擊做好準備。當時機成熟時，所有的蠕蟲會一起發難。最先受襲擊的目標會是互聯網的基建設施，包括頂層域名系統伺服器和互聯網交換中心主路由器。當這些設施受損並不能及時補救時，互聯網就會進入完全癱瘓狀態。為了延長網絡的修復時間，蠕蟲可能會作出無法還原的破壞（例如：刪除硬碟內的資料及程式），使受害電腦不能在短時間內修復。幾經辛苦，當互聯網終於恢復正常運作時，可能已浪費了無數的人力物力。由於超級蠕蟲具有頑強的生命力，只要有一兩個漏網之魚，它們就有機會捲土重來，作第二次甚至第三次的攻擊。這種無止境的攻擊將使互聯網無法長期正常運作。超級蠕蟲不但能造成爆發性的破壞，還可以默默地收集機密資料，如信用卡資料或用戶私人電郵。它們可以利用這些資料造成市場混亂，例如：公開機密資料或盜用他人名義發放虛假消息。當我們的資料不再安全和準確時，我們的經濟活動還能正常運作嗎？面對這種威脅，我們可以做什麼呢？要預防它們，需要各階層人仕通力合作。

預防措施

首先我們要提昇各階層的資訊保安意識和知識。在管理決策層面上，資訊保安不再是「附加項目」，而是「必需條件」。資訊保安的資源優先權應排在前位。每個網絡都要採用有效的風險評估和保安政策，網上有相關的文獻供公眾參考。

政府應該帶頭鼓勵採用優質資訊保安產品，在其合約和招標書中列明資訊保安為先決條件。在科研方面，政府應投放資源在大學進行資訊保安的科技研究。香港正進入知識型經濟，金融和物流是其支柱，兩者都非常依賴資訊科技。如果資訊保安做得不好，經濟就難以起飛。政府也可以和非牟利機構合作，定期舉辦資訊保安講座或培訓班，使各階層人士都能掌握資訊保安知識。

互聯網基建設施應有完善的後備系統和應變計劃。一旦受到病毒或蠕蟲的攻擊也能即時還擊並有效地維持正常運作。系統管理員應不斷增進保安知識並好好掌握各種技術以便預防未知的病毒和蠕蟲襲擊。保護好各自的網絡無形中也幫助了其他網絡。你的網絡不受感染，病毒或蠕蟲就不能利用你的網絡去攻擊其他網絡。

軟件和硬件公司應提高其產品的資訊保安水平。不應為了盡快推出市場而忽略產品的品質和安全性。例如沒有完全測試產品在非正常運作情況時的反應，或為了方便和彈性而沒有限制執行外來輸入程式。更不應為了方便顧客而將保安水平預設值降至最低，並假設用家已具有相當的資訊保安知識。

用家本身也應該提高資訊保安意識。就算自己的電腦是多麼平凡或不重要，

也需要好好保護它。你的電腦不受感染，病毒或蠕蟲就不能利用你的電腦去入侵其他電腦。用家也可以利用市場力量，只選用高保安質素的產品。

我們不知道超級電腦病毒或蠕蟲何時會出現，但我們知道它們的出現將帶來重大的損失。防患未然，我們應該從以上各方面入手，提高我們應付它們的能力。

References:

1. Viruses and Worms: What Can We Do About Them?
   http://www.cert.org/congressional_testimony/Pethia-Testimony-9-10-2003/
2. Internet Worms: Walking on Unstable Ground
   http://www.giac.org/practical/GSEC/Jon_Maurer_GSEC.pdf