資料來源：資訊安全網

時刻保持警覺 提防病毒與惡意程式碼

在現今資訊科技發達的年代，電腦與人們生活密不可分。然而，往往會有不法之徒利用電腦病毒和惡意程式碼進行攻擊，藉此入侵使用者的電腦，竊取重要的個人資料，甚至操控電腦的運作。對個人還是企業而言，都應該時刻提高警覺，保護資訊系統不受惡意攻擊。

何謂病毒與惡意程式碼？

惡意程式碼是指範圍廣泛，會對電腦或網絡造成損害或不預期影響的程式。潛在的損害可以包括修改、破壞或竊取資料、允許未經授權的系統接達、產生非期待的螢幕畫面，以及執行用戶絕不想要的功能等，對軟件及資訊處理設備存在嚴重的威脅，因此用戶及管理者必須採取預防措施來偵測並避免惡意程式碼的爆發。惡意程式碼的例子包括：電腦病毒、蠕蟲、特洛依木馬、邏輯炸彈、間諜軟件、廣告程式及後門程式 (backdoor)。

電腦病毒是最常見的惡意程式碼。病毒是一種會藉由附著在其他檔案來使一部電腦受到感染的程式，並且在程式執行時會自我繁殖。另一個經常遇到的惡意程式碼是蠕蟲，一種會自我複製的電腦程式，透過系統連結來傳播，消耗受影響電腦的資源或導致其他損害。

某些惡意程式碼，包括大部分的電腦病毒，是程式其中的一個片段，無法單獨執行，需要先附著在主機程式上。其他類別的惡意程式碼（例如蠕蟲）則能夠自行散佈並複製，也能夠透過網絡從一台電腦接著一台地繁殖下去。

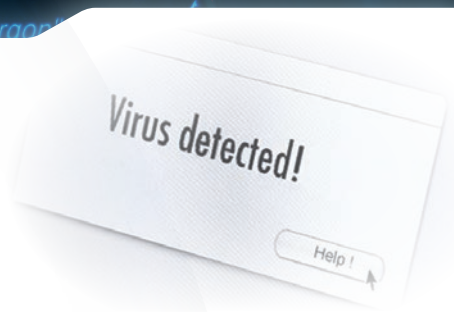
要注意的是，某些惡意程式能夠表現一種以上惡意程式碼的行為。例如，特定程式可能既是電腦病毒也同時為特洛依木馬。

增長的風險

惡意程式碼所導致的風險正日漸增加，以往的惡意程式碼只會做出騷擾及一般的破壞，但現今的攻擊動機則更多是在於金錢上的掠奪。攻擊者採取類似傳統軟件發展及商業應用等方式來攻擊，使攻擊日益複雜並更有組織。

研究顯示，發現軟件漏洞與透過新型電腦病毒／蠕蟲來發現漏洞之間的時間相隔有縮短的趨勢。此外，發展抗電腦病毒軟件是需要時間的，所以使用者的抗電腦病毒軟件可能無法及時偵測到最新發現的惡意程式碼。因此，如果沒有裝置其他的保安最佳作業實務，使用者的電腦就仍會受到電腦病毒攻擊的威脅。

若果用戶安裝或打開來自不可信任來源或濫發電郵的惡性附件／程式／外掛程式、造訪惡性網站、電腦未做適當修補、更新和配置等，這些情況都會讓攻擊者找到機會與漏動，令使用者的電腦有可能會受到感染。



一般最佳作業實務

以下的最佳作業實務可以保護使用者的電腦，而且有效地對抗電腦病毒與惡意程式碼的攻擊。

要做的事

- ✓ 安裝抗電腦病毒軟件來保護機器，並確保已使用最新病毒識別碼和偵測修復引擎。有些提供抗電腦病毒能力的保安產品，能夠同時提供其他的保安特點，例如個人防火牆、反間諜軟件及反仿冒詐騙等功能。這些產品有時候會以不同的名稱（例如「互聯網保安套裝軟件」）等作為品牌包裝。電腦使用者應該選擇符合個人需求的抗電腦病毒套裝軟件。
- ✓ 安裝並啟動個人防火牆。
- ✓ 啟用並妥善地配置即時掃描功能，掃描機器以偵測電腦病毒及惡意程式碼，而掃描是特別針對在執行中的程序、執行檔與文件檔。
- ✓ 在使用所有可移式磁碟及從互聯網下載檔案（特別是那些來源不明的下載）之前，利用抗電腦病毒軟件作檢查。
- ✓ 使用者應每日替電腦執行病毒掃描，可考慮在非繁忙時間（例如午飯時間）定時進行。
- ✓ 避免視覺仿冒。一些犯罪方式是嘗試利用視覺仿冒科技來蒐集個人資料，或者讓使用者相信正在安裝或接受的軟件／外掛程式／執行中內容的來源是安全的。
- ✓ 安裝任何軟件之前，要驗證軟件本身完整性的審查（例如檢驗和值），並確保沒有任何電腦病毒或惡意程式碼。
- ✓ 確保電腦擁有最新的保安修正檔，以降低遭受詐騙電郵或網站侵入軟件漏洞的攻擊機率。同時，這樣可以協助保護電腦不受其他的保安或病毒攻擊。目前，許多套裝軟件與作業系統擁有自動更新的特點，使用者可以考慮啟用這些特點，確保系統處於自動更新的狀態。
- ✓ 定期為程式與資料進行備份。遭受病毒攻擊後，最安全的方式是以乾淨的備份進行復原。
- ✓ 了解互聯網詐騙。香港警務處的網頁上提供一些避免科技罪行的技巧，詳情請瀏覽：〈www.police.gov.hk〉。
- ✓ 在遭受惡意程式碼感染時，停止所有電腦上的活動。若果繼續使用受到感染的電腦，可能會讓病毒或惡意程式碼繼續散播下去。
- ✓ 啟動應用程式及軟件的保安功能，並確保這些功能已經適當地設定。
- ✓ 注意任何可疑的活動，例如檢查電腦上是否有任何不正常的活動，包括不正常的硬件使用、不正常的互聯網通訊等。不正常的活動可能是受到惡意程式碼感染的徵兆。

不要做的事

- ✗ 不要在任何情形下使用來歷不明的軟件。
- ✗ 不要執行電子郵件或即時訊息客戶上的附件，除非十分確定沒有任何問題。要注意來自不明來源的電子郵件或即時訊息附件上的電腦病毒，因為有些電腦病毒／蠕蟲會偽裝成為歡迎卡片或訊息。
- ✗ 不要造訪可疑網站。
- ✗ 除非有一定的需要，否則在使用公共或不安全的電腦連結互聯網時，不要許可他人接達個人檔案或使用個人密碼。

網絡／通訊閘管理者的進階技巧

- 採取完善的資訊科技保安政策或架構，並參考一些資訊保安國際認可標準、指引及有效保安作業實務的指引。
- 確保所有用戶認識資訊科技保安政策，特別在使用免費／分享軟件。
- 針對可疑活動（例如突然的網絡通訊激增），監視並定期複查審計追蹤。

- 安裝抗電腦病毒及內容過濾保安功能於通訊閘，以掃描所有輸入或輸出的信息及檔案是否含有惡性內容。通訊閘應配置為可阻截、隔離及刪除含有惡性內容的信息或檔案，以及建立審計記錄以供日後參考。
- 裝設保安措施以對抗遠端執行惡意程式碼的攻擊，因為針對這些惡意程式碼的病毒定義可能尚未提供。建立自動或手動過濾機制，以確認並阻隔可疑通訊及惡意程式碼。
- 確保所有工作站安裝了帶有最新病毒定義與偵測修復引擎的抗電腦病毒軟件。電腦病毒識別碼與惡意程式碼定義更新應要自動執行，更新頻率也應設定為至少一天一次。如果無法自動更新，手動更新的執行則至少要一週一次，並盡量在可能時候執行。
- 所有全新的電腦在允許連結至機構網絡之前，必須執行整個系統的掃描。
- 將相同資訊保安需求與程序應用到未開發或作測試用途的系統上。

在管理伺服器時，局部區域網絡／系統管理員應遵循以下保安指引：

- 透過主硬磁碟啟動伺服器。如電腦須透過抽取式儲存媒體啟動，在啟動前必須掃描抽取式儲存媒體是否附帶電腦病毒，這樣可以防止伺服器受開機磁區電腦病毒感染。
- 使用接達控制功能保護伺服器的應用程式，例如儲存應用程式的目錄應設定為「唯讀」。此外，應按照「需要賦予」原則賦予接達權，尤其是「寫入」及「修改」權。
- 考慮運用文件管理解決方案共用文件，從而減低受感染檔案在不受控制下傳播的機會。
- 在供用戶使用前，應先將所有新安裝的軟件，進行病毒掃描。
- 宜預設檔案伺服器在開機後自動執行一次全面病毒掃描。
- 執行定期資料備份與復原。
- 定期檢查所有備份，確保需要時可以復原。

此外，局部區域網絡／系統管理員應取得最新的安全警告信息，並教導用戶防範電腦病毒及惡意程式碼的最佳作業實務：

- 登記接收保安通知／警告信息，以便盡早取得重要的電腦病毒／惡意程式碼警告。
- 立即將所有電腦病毒警告轉達給每一個終端用戶，並採取必要的措施來減輕問題。
- 教導用戶明白大規模電腦病毒攻擊帶來的影響，以及了解感染電腦病毒及惡意程式碼的各種途徑，以免感染電腦病毒。（例如教導用戶了解一些含有電腦病毒及惡意程式碼的電郵，很可能會仿冒為其朋友或同事發出。）

偵測及消除病毒

以下是一些電腦感染病毒或惡意程式碼的症狀：

- 執行程式的時間比正常情況長。
- 可供使用的系統記憶體或磁碟容量銳減。
- 出現來歷不明／新建立的檔案、程式或程序。
- 彈出新窗口或瀏覽器廣告。
- 電腦出現異常重啟／死機。
- 網絡負擔增加。

如果用戶懷疑電腦感染病毒或惡意程式碼，應終止一切活動，因為繼續使用懷疑受感染的電腦可能會讓電腦病毒或惡意程式碼進一步傳播開去。用戶應立即向管理人員及局部區域網絡／系統管理員匯報有關事故。刪除電腦病毒或惡意程式碼並不代表能夠復原或取回受感染或被刪除的檔案。

復原已損壞檔案的最有效方法是以原來的檔案取代。因此，檔案應定期備份，而且應保存足夠備份複本，以便在有需要時復原。從電腦中刪除病毒後，用戶宜對個人電腦及其他抽取式儲存媒體進行全面掃描，確保沒有任何電腦病毒。忽略這一步驟可能導致電腦從這些媒體中再次受感染。

電腦病毒與惡意程式碼的類型及保護步驟

以下將會列出不同類型的電腦病毒與惡意程式碼，除了文中提到的防範技巧外，也可以遵循上述的一般最佳作業實務，妥善保護電腦，並有效對抗惡意的攻擊。

病毒種類	特點
常駐記憶體病毒	這種病毒會常駐在主程式上。每當作業系統執行檔案時，病毒就會感染像是程式檔等合適目標。
程式檔病毒	這種病毒會感染副檔名為 exe 、com 、sys 等檔案。
多構式病毒	病毒會使用各種多樣態科技來改變形狀。
開機磁區病毒	這種病毒會在磁碟初始化或開機後，感染磁碟的系統區。
隱形病毒	這種病毒會使用各種隱形科技來隱藏自己，避免遭到抗電腦病毒軟件的偵測。
巨集病毒	這種病毒和其他病毒型態不同，攻擊的是資料檔而非執行檔。因為下列原因，巨集病毒常常出現： 1. 附著在那些獨立於平台的文件與檔案。 2. 文件藉由像是電子郵件或檔案交換等方式送到其他電腦上，收件者收到的感染文件是來自於「 可信任 」的寄件者。
電子郵件病毒	透過電子郵件訊息散佈的病毒。

電腦病毒

電腦病毒是一種自我複製的電腦程式，會附著在其他檔案／程式上，並且在主程式／檔案啟動時秘密地執行。病毒在執行時會進行一些作業，例如刪除檔案／硬件、顯示騷擾資訊、附著在其他檔案上等。

蠕蟲

蠕蟲是一種可自我複製的程式，不需要附著在主程式／檔案上。和電腦病毒不同的是，蠕蟲是可以自我執行的。蠕蟲有能力透過網絡傳播，也可以在短時間內進行大規模毀滅性的攻擊。

特洛依木馬

特洛依木馬是一種非複製型病毒，看起來是正當的程式，但實際上在執行時會出現惡性及非法活動。攻擊者使用特洛依木馬竊取用戶密碼資訊，或者只是簡單地破壞硬件上的程式或資料。特洛依木馬難以偵測，因為其設計是透過執行某些功能來隱藏外貌。

特洛依木馬是非常危險的，因為此病毒能夠打開後門，進入系統，並允許攻擊者在電腦上安裝進一步的惡意程式。Back Orifice 和 Subseven 是兩個著名的遠端進入特洛依木馬，允許攻擊者操控受害者的電腦。

防範技巧

- 安裝檔案及目錄完整性檢查器。
- 注意可疑硬磁碟活動及／或網絡活動，例如硬磁碟 LED 指示燈總是亮著時。
- 注意可疑的檔案刪除或修改。
- 檢查電腦系統是否在不知道的情況下被非法使用，例如電子郵件帳戶。

間諜軟件及廣告軟件

間諜軟件是一種在沒有用戶的同意下，秘密轉寄用戶資料給第三方的軟件。資料包括了用戶的線上活動、電腦的檔案許可或敲鍵內容。

廣告軟件則是一種執行程式時顯示廣告橫幅的軟件，某些廣告軟件同時也是間諜軟件。首先，這些軟件會潛入受害者的電腦並收集資料，接著顯示與所蒐集資料有關的廣告橫幅。

被安裝了間諜軟件／廣告軟件的系統可能顯示下列一個或多個徵兆：

- 網站瀏覽器的「 首頁 」會變更成另一個網站，而且／或者在沒有用戶同意下，在「 我的最愛 」中加入新的項目。用戶無法對變更做任何改變，並且這些瀏覽器攻擊者會迫使用戶造訪不想要的網站，大量提高該網站的點擊率以提高廣告值。

- 即使用戶的瀏覽器並未開啟或者系統沒有連結到互聯網，帶有廣告的彈出視窗還是會出現在螢幕上。
- 未經用戶許可下，在電腦上安裝新的軟件組件，例如瀏覽器工具列等。
- 用戶並未執行任何線上活動時，可疑的網絡通訊還是會出現在電腦上。

無論如何，某些間諜軟件的程式設計十分小心，避免被用戶注意到，因此也無法藉由以上不正常情況來進行篩選。這種間諜軟件只能透過抗電腦病毒軟件產品／工具來加以偵測並移除。

防範技巧

- 不要從可疑來源（例如網站、同儕架構的檔案分享資源等）下載／安裝軟件。
- 在下載與安裝合法軟件之前，要先閱讀使用條款與條件，因為他們可能會要求安裝一些廣告軟件或間諜軟件系統。
- 當造訪某些網站時，如被要求安裝外掛程式或使用權同意，請仔細閱讀使用條款。
- 檢查特定搜尋引擎所提供的資訊，他們的搜尋結果可能包括了惡意程式碼。這可以在搜尋連結時避免危險或不可信賴的網站。
- 安裝可以過濾間諜軟件及廣告軟件的瀏覽器工具列。
- 安裝反間諜與反廣告的軟件。

Rootkit

Rootkit 是一整套檔案，以惡性竊取的方式改變一個作業系統的標準功能。藉由作業系統的改變，Rootkit 允許攻擊者在受害者系統中扮演系統管理者的角色。（在 Unix 系統中則是「根」目錄用戶的角色，因此稱為“Rootkit”。）

許多 Rootkit 的設計，都會隱藏自身以及其對系統所做的改變。因此，在判定系統中是否有 Rootkit 與被 Rootkit 改變的內容時，會變得很困難，例如 Rootkit 可能會將連結到他們自身檔案的目錄與程序列表項目隱匿起來。

主動式內容

與傳統的靜態資料檔使用軟件程式的方法不同，現行的資料物件（包括網頁、電子郵件及文件）可以讓資料與程式碼交織在一起，允許程式碼在用戶電腦上進行動態執行。這些資料物件經常在用戶之間轉換，成為有效的病毒載具，而程式碼執行的透明度會成為保安上的顧慮。

ActiveX 元件控制與 Java 語言是兩種主要的「主動式內容」科技。一般而言，ActiveX 元件控制可直接接達當地視窗呼叫 (native Windows calls)，從而接達任何系統功能，因此所造成的威脅較大。另一方面，Java 語言的 Java 虛擬機器會讓自己成為一個所謂的「沙包」，或與作業系統服務有所隔離。然而，這並不表示沒有 Java 病毒。

防範技巧

- 注意任何不正常的徵兆
  - 程式在執行時花了比平常更久的時間
  - 系統記憶量或磁碟可使用空間突然降低
  - 瀏覽器的首頁遭到改變
  - 無法再接達某些網站
- 不要安裝任何來自可疑網站的主動式內容。不要選擇安裝頁上的拒絕選項，而是關閉瀏覽器。因為有些安裝頁可能是一種視覺詐騙，無論選擇那一個選項都會安裝主動式內容，或者使用者可考慮使用作業管理程式來強迫關閉瀏覽器。

殭屍電腦及殭屍網絡

殭屍電腦是指一部已接達上互聯網、並在電腦擁有者不知情況下被破解操縱的電腦。殭屍網絡是指由殭屍電腦所組成的網絡，並已經遭到攻擊者接管及遠端控制，其中可能包括幾百台的殭屍電腦。這些殭屍網絡會囊括遍及世界各地的家用、學校、商業，以及政府的電腦。

殭屍電腦可能只是在速度上輕微地降低，或者顯示奇怪的訊息。然而攻擊者可以使用殭屍網絡對另一個系統或網絡進行大規模攻擊，例如DDoS（分佈式拒絕服務攻擊）。由於殭屍網絡裡的機器數量眾多，當這些機器集中針對單一目標進行分佈式拒絕服務攻擊時，所匯集的計算量是十分龐大的。因此，電腦使用者應該保護機器或系統，以免成為殭屍電腦。

恐嚇軟件

恐嚇軟件，又名流氓軟件，包括各類植入了惡意程式碼的勒索軟件或詐騙軟件。此軟件會假裝為正當的抗電腦病毒軟件或類似產品，實質是一些沒有功能的贗品，甚至是可竊取受害人個人資料、密碼或信用卡資料的惡意程式碼。勒索軟件使電腦使用者無法存取電腦上的檔案，受害人被要求支付費用（「贖金」），才能夠重新存取檔案。

恐嚇軟件通常誘使受害人誤信其電腦已經感染了病毒，然後建議下載抗電腦病毒軟件（需付款的）來移除病毒。很多時候，所謂的病毒完全是假的，而安裝的軟件根本就是恐嚇軟件本身。受害人除了損失用作購買恐嚇軟件的金錢外，購買恐嚇軟件時所提供的個人詳情和信用卡資料，也可能被犯罪分子用作其他欺詐活動或在黑市上出售。

勒索軟件是由恐嚇軟件演化而成的另一種惡意軟件，勒索軟件可以「綁架」用戶的電腦，例如，令電腦停止工作、加密主要的操作系統檔或鎖死一些個人資料，從而索取贖金。受害人需支付贖金，才能重新控制電腦和存取檔案。

保護電腦免受恐嚇軟件和勒索軟件侵害，需要針對惡意程式碼的最佳作業實務，用戶必須謹慎，凡事用常識判斷，並使用可靠的保安軟件。一些防範恐嚇軟件、勒索軟件，以及其他病毒和惡意程式碼攻擊的最佳作業實務包括：

- 經常把重要資料備份和不要把備份資料連接電腦。
- 不要瀏覽可疑網站及從中下載任何檔案。
- 不要開啟可疑的電郵及即時短訊，或當中的附件及超連結。
- 檢查及更新抗惡意程式碼軟件和識別碼至最新版本。
- 為使用中的軟件安裝最新的修補程式。
- 不要設定 Microsoft Word／Excel 及其他辦公室軟件內的巨集功能。
- 開啟系統和瀏覽器上的保安功能。
- 只安裝來源可靠的軟件和流動應用程式，如有可疑的權限要求，切勿安裝。
- 公司內一些有較大機會受電腦病毒感染的部門，例如經常處理電郵的客戶服務部，應為他們安排一部沒有共享硬碟資源及限制接駁致公司內部網絡的電腦，以減低一旦感染電腦病毒對公司的影響。此外，所有處理的同事亦要對各潛在電腦病毒有所提防。
- 若對電腦內任何可疑活動有所疑問，可向香港電腦保安事故協調中心尋求協助和建議。

若電腦裝置不幸受到勒索軟件等電腦病毒感染，用家可考慮以下的即時措施：

- 切斷受感染電腦的網絡連線，以免影響網絡驅動器及其他電腦。
- 關上電腦的電源，防止勒索軟件把電腦內更多檔案加密。
- 記下發現事件前所作過的電腦操作，例使用過的程式、檔案、電郵及網站。
- 向香港警務處舉報有關罪行。
- 從備份復原數據至未受感染的電腦裝置。

其他

惡作劇電子郵件

惡作劇電子郵件是一種假的病毒警告，通常以電子郵件訊息形式出現。它會建議讀者將訊息轉寄給其他人，導致電子郵件數目迅速激增，令系統超出負荷量。

流動裝置病毒／蠕蟲

流動裝置也容易遭到惡意程式碼的攻擊。目前，針對手提設備與智能手機的惡意程式碼並非普遍，但很可能隨著流動式應用程式功能和設備裝設普及化而有所增加。流動式應用程式發展環境的開放式架構，以及經常伴隨大量的軟件發展文件與工具，都是很容易允許攻擊者製造這些平台的惡意程式碼。

惡意程式碼會以幾種方式感染流動裝置，包括：

透過 SMS 或 MMS 電子郵件	含超連結至惡意程式碼的訊息會傳送給用戶，誘使該用戶選擇該連結並下載惡意程式碼。另一方式是以電子郵件的附件形式傳送至用戶，並在執行時感染設備。惡意程式碼也會以類似狀況透過 MMS 訊息來繁殖。SymbOS/Commarrior.M 是一種能夠透過 MMS 訊息在 Symbian 系列上散佈的蠕蟲。
經由桌面同步化	Cxover 是一種概念檢驗式蠕蟲，會同時影響個人電腦及流動裝置的視窗系統。如果在流動裝置的視窗系統上執行，會透過 ActiveSync 連結，自我複製到電腦上。如果在個人電腦視窗系統上執行，則會透過 ActiveSync 搜尋任何手提設備並自我複製到該設備上。
經由藍芽、紅外線或 Wi-Fi 裝置	第一隻能夠透過藍芽散佈的蠕蟲是在 2004 年 1 月發現的，命名為 Cabir。這是針對 Symbian 作業系統系列 60 智能手機的概念檢驗式蠕蟲，但之後沒有大量出現。蠕蟲需要接受者好幾個的互動步驟才能夠執行。意圖傳送惡意程式欺騙接受者接受的攻擊者，也會盤剝藍芽的潛在弱點。

邏輯炸彈

邏輯炸彈是一種嵌入其他程式的程式碼，遇到特定的、預先的定義條件就會啟動。例如，時間炸彈在某個系統裡未發現另一個程式碼或密碼匙，就會攻擊該系統並刪除所有資料。在某些情況下，邏輯炸彈會透過互聯網通知攻擊者，炸彈已經準備要攻擊受害者。

陷阱門

陷阱門是程式的一個秘密進入點，刻意包含在程式碼之中，可以用來幫助程式除錯，但也可能是用於惡性目的。

常見的模糊技術

惡意程式碼發展者與寫作者會使用下列常見的模糊技術來逃避偵測與刪除：

綑綁工與包裝者	多數病毒識別碼是以檢驗和值的方式，使用檔案特徵和惡意程式碼的前幾個二進位數元來製造。綑綁工技術是將病毒與惡意程式碼檔案綁在另一個檔案上，並改變它的格式。包裝者技術則在嵌入病毒碼之前先進行壓縮。
自我加密與自我解密	惡意程式碼會自我加密解密，甚至會使用好幾層加密及解密技術並／或在加密及解密過程使用亂數匙。這樣就難以被直接檢查出來。
多態	惡意程式碼會在自我加密過程中改變預設的加密設定及解密碼。這樣會讓偵測困難許多。
變形	惡意程式碼會藉由如重新安排程式碼段，或藉由在來源程式碼中加入沒有用的程式行，重新編譯成新格式，來改變原來的格式。
程式碼轉換成 Visual Basic 的手稿程式	這種方法將一個執行檔程式 (.exe) 轉換成 Visual Basic(.vbs) 的手稿程式，以附著在一個文件、資料檔或電子郵件訊息中。
隱形	這種技術是藉由自我隱藏程式碼的設計來逃避抗電腦病毒軟件偵測系統。有一種例子是監察系統對檔案的呼叫；惡意程式碼就可以修改程序對呼叫的回傳資訊，並且只回傳原來的資訊。

處理電腦病毒與惡意程式碼爆發

由於攻擊者的動機是基於經濟掠奪，其攻擊形式不只是騷擾或破壞活動，而是變得更複雜，甚至成為不少機構的嚴重隱憂。大規模惡意程式碼攻擊，是指惡意程式碼爆發，導致機構廣泛的損害與崩潰，這是需要很長的復原時間與努力。因此，採取適當的預防步驟是很重要的，例如裝設保護與偵測工具，以保衛機構不受到惡意程式碼的攻擊。

然而，在資訊保安世界裡並沒有所謂的「防彈保護」。機構發展功能強大的資訊保安事故處理程序尤其重要，如此一來行政人員才能夠以更具組織化、更方便和更有效的方式做足準備，處理惡意程式碼的爆發。

面對有保安事故發生，一般而言有三個階段，包括「規劃和準備」、「應變」及「事後跟進」。對於完善處理惡意程式碼爆發事故，「應變」和「事後跟進」是非常重要的。

「應變」階段：偵測與確認

確認惡意程式碼爆發是否已經發生

惡意程式碼爆發的典型徵兆包含：

- 用戶抱怨接達互聯網緩慢，系統資源減少，磁碟接達緩慢，或系統啟動緩慢；
- 主機入侵偵測系統 (HIDS)，或抗電腦病毒或惡意程式碼偵測軟件產生一些警告；
- 網絡的使用明顯增加；
- 周邊路由器或防火牆已經記錄到一些違反接達進入；
- 偵測到來源於內部互聯網規約地址的對外簡單郵遞傳送規約 (SMTP) 通訊激增；
- 偵測到大量的埠掃描以及連結失敗的企圖；
- 注意到不尋常的典型網絡通訊流來源；
- 許多主機上的保安控制如抗電腦病毒軟件與個人防火牆遭到關閉；
- 一般性的系統不穩定與失敗；

若發現上述的任何一項徵兆，資訊科技人員應該立即檢查並驗證所有可疑活動，以確定爆發是否發生。一旦確認這是惡意程式碼引致的違反保安事件，便需要蒐集關於該惡意程式碼的資訊，因為這是遏制與杜絕程序所必需的。

若這種惡意程式碼已經從抗電腦病毒與惡意程式碼偵測軟件的覆檢，以及防火牆與路由器記錄檔檢查中得知存在一段時間，就可以從抗電腦病毒軟件經銷商網站獲得該惡意程式碼的資訊。下列問題能夠幫助辨別惡意程式碼的特徵：

- 這是哪一種類的惡意程式碼（網絡蠕蟲、大量郵件蠕蟲或是特洛伊木馬等）？
- 這種惡意程式碼如何散播（透過具漏洞的網絡服務攻擊還是透過大量郵件）？
- 如果惡意程式碼透過攻擊具漏洞的網絡服務來散播，那什麼漏洞會遭到攻擊？處理該漏洞的修補程式是否已經公佈？什麼服務或埠會遭到攻擊？
- 惡意程式碼是否在受感染的系統上植入後門？
- 如何從受影響的系統上移除惡意程式碼？有任何可用的移除工具嗎？

執行初步評估

一旦辨別出一項爆發，資訊科技人員應該評估爆發的範圍、損害及衝擊，以便作有效的處理。

記錄所有採取的措施

資訊科技人員應該記錄所有處理爆發的採取措施以及任何反應的結果。這些記錄有助確認和評估事故，為檢控提供證據，並為往後的事故處理階段提供有用的資料。整個保安事故應變過程都應保留記錄。

「應變」階段：升級處理

事故應變的第二階段是通知適當的人員，並根據既定的升級處理程序將事故提升到適當的級別。升級處理程序所提供的資訊應該要清楚、簡要、準確並符合事實。 不準確的、誤導的或不完整的資訊可能會延誤應變程序或甚至可能使情況惡化。務必緊記，關於事故的資訊應該只在需要知道的基礎上被揭露。

「應變」階段：遏制

惡意程式碼事故應變的第三階段是遏制。下列事項是遏制階段所應該執行的活動：

確認受感染系統

清楚確認受感染系統總是遏制的第一步驟。不幸地，基於目前資訊科技環境的動態特性，這也是非常複雜的程序。下列的建議可以在管理環境中協助確認受感染的系統：

- 使用最新病毒識別碼和更新過的抗電腦病毒偵測與修復引擎，在所有系統上執行完整的病毒掃描。因為沒有任何單一抗電腦病毒軟件或惡意程式碼偵測工具能夠涵蓋所有種類的惡意程式碼，所以需要使用一種或以上的抗電腦病毒掃描工具，以確保能夠偵測到所有的惡意程式碼。
- 複查所有路由器與防火牆的記錄檔。
- 提供如何確認感染的指引給用戶。
- 配置 IPS 或 IDS 以辨認與感染相關的活動。
- 執行封包追蹤，以尋找符合惡意程式碼特徵的網絡通訊。

遏制爆發

以下是一般遏制爆發的常見策略：

使用自動化工具	像抗電腦病毒軟件或惡意程式碼偵測工具，IDS 與 IPS 等自動化工具可以遏制惡意程式碼的散播。倘使現存的抗電腦病毒保護系統無法偵測到惡意程式碼，甚至應用最新簽名檔也無效時，就應該尋找抗電腦病毒軟件供應商的支援，以建立可以涵蓋惡意程式碼的新簽名檔。
中斷網絡連接	立刻切斷受感染系統與整個網絡的連接，可以有效遏制惡意程式碼爆發。可以透過在網絡裝置上加上接達控制，或實體地切斷網絡導線中斷網絡的連接。某些情況下，為了遏制惡意程式碼散播到機構的其他區域，暫時將網絡段從主幹網絡上切斷是必要的。無論如何，遏制策略將一定會影響該網絡與其他未受感染系統的作業。
停用服務	惡意程式碼會透過網絡服務，如可分享的網絡磁碟等來散播。暫時性地堵截或甚至關閉被惡意程式碼利用的網絡服務可協助遏制事故。
消除漏洞	惡意程式碼會透過攻擊具漏洞的網絡服務而散播。例如安裝保安修補程式在具漏洞的系統上，來處理甚至已遭惡意程式碼盤剝的漏洞，消除繁殖的管道，進而遏制惡意程式碼的散播。此外，某些如可分享網絡磁碟喪失接達控制等錯誤配置，也會被惡意程式碼利用。矯正任何的錯誤配置可以遏制惡意程式碼的散播。
用戶的參與	像在一個小型遠端分部辦公室或非管理辦公室環境中，可處理爆發的技術支援人員是有限的，用戶參與的效果在這個時候對於遏制程序就十分顯著。當系統確定遭到感染時，應提供用戶如何確認感染以及該採取什麼步驟的清楚指示，例如在受感染系統上執行抗電腦病毒移除工具。

保存所有已採取行動的記錄

在這個階段保存所有已採取行動的記錄是很重要的，因為某些遏制步驟需要對網絡基建與系統的配置或設定作暫時性修改。這些修改在事故之後需要移除。

UPM Finesse Classic Matt, 90 gsm

最重要，是要了解停止了惡意程式碼的進一步感染並不代表防止了受感染系統被進一步的損害。例如，停用網絡連接可以遏制感染。然而，惡意程式碼仍可刪除受感染系統上的檔案。因此，要盡快地或與遏制程序同步進行完整的杜絕程序。

「應變」階段：杜絕

杜絕惡意程式碼爆發應從所有受感染的系統與媒體上移除惡意程式碼。在執行杜絕程序之前，建議先蒐集所有必要資訊，包括可能必須在刪除程序裡刪除或重設所有的記錄檔，這對於事後跟進調查是有幫助的。

杜絕的基本方法，一般是使用抗電腦病毒或惡意程式碼掃描軟件以及移除工具。然而，在某些情況下，重新安裝受感染系統是必要的。例如，當惡意程式碼已在受感染系統上植入後門時，為了復原系統的完整性，重新安裝所有受感染的系統會是最值得信賴的行動。系統重建一般包括下列幾個行動：

- 從可信賴來源重新安裝系統，如系統安裝片或可信賴且乾淨的系統像。
- 確保新安裝的系統安全，如檢查並確保最新病毒識別碼以及更新的抗電腦病毒偵測與修復引擎，加上必要的保安修補程式已經應用於每一台機器上。
- 從未受染的備份媒體上復原資料。

「應變」階段：復原

這個階段的主要目的是將系統復原至正常運作狀態。很多時候，「杜絕」及「復原」階段都是不能分割，因為受感染的系統的功能及其資料已在「杜絕」階段中被恢復。除了復原受感染系統，移除所有暫時性的遏制措施，例如被暫時中斷的網絡接連，是復原程序中另一個主要部分。在移除遏制措施前，其中的一項重要工作是進行生產前保安評估，以確保沒有系統受到感染，並確定感染的根源已被刪除。

在恢復系統操作前，應事先通知所有相關人士。在受控制的情況下，資訊科技人員應該按照需求的緩急次序逐步恢復功能／服務，例如可優先恢復最重要的服務或以大多數人為對象的服務。復原中止服務之後，其中的一項重要工作是檢驗復原操作是否成功，系統是否已恢復正常操作。另外還可以實施額外的監視措施，以觀察相關網絡區段有否任何可疑的活動。

「事後跟進」階段

受感染的系統恢復正常操作並不代表惡意程式碼爆發處理程序的結束。採取必要的跟進行動十分重要。跟進行動包括評估事故所造成的破壞、系統改良以防止再度發生事故、保安政策和程序更新及為日後的檢控進行個案調查。這個階段的行動包括下列事項：

- 檢驗現存病毒／惡意程式碼保護程序與機制的有效性，包括病毒識別碼分佈與偵測修復引擎的更新，定期規律的病毒掃描等的中央控制與管理。
- 在需要時更新相關政策，指引與程序。
- 執行經檢驗政策／指引／程序後所引進新的保安措施，以保護系統對抗未來的攻擊。
- 提醒用戶遵循保安最佳作業實務，例如不可從未知／可疑的電子郵件來源開啟郵件，養成更新保安修補程式與病毒定義的習慣等。■

如果想了解更多有關資訊保安管理的內容，請聯絡香港特區政府資訊科技總監辦公室製作和管理的「資訊安全網」：

資訊安全網

網址：www.infosec.gov.hk
電郵：webmaster@infosec.gov.hk
傳真：+852 2989 6073
地址：香港數碼港道一百號數碼港一座六樓