武裝自己 - 資安篇

森美力 (Samiux) 編著

二零一七年五月十九日　第一版
二零一七年七月八日　　修訂版
二零一七年八月廿七日　修訂二版
二零一七年十一月九日　修訂三版

本書是在安卓 (Android) 手機利用 Google Docs 軟件完成。頁面是 B5 大小。

本書是免費版本，可以在我的個人網站 (https://www.infosec-ninjas.com) 下載。歡迎在你的親戚朋友之間轉閱，更歡迎將其翻譯成其他國家語言。

雖然是免費版本，但版權仍然歸於本人。

目錄

前言

網絡在設計時並沒有考慮到安全問題，因為在初期的時候，它是在一個非常信任和安全的環境下運作。後來網絡開放給所有人使用，就形成了現在的互聯網，加上網絡使用技術愈來愈複雜，電腦程式設計在邏輯上或編程上的錯誤時有發生，安全問題就隨之而來。那些程式設計漏洞經常被非常聰明和技術優秀的惡意黑客 (所謂駭客) 所利用來取得利益或名譽，網絡攻擊相繼發生，所以在本質上互聯網是不安全的。

最近，二零一七年五月十二日 (中國香港時間)，不出一日，全球超過一百個國家及地區，超過數十萬台微軟視窗 (Microsoft Windows) 系統被感染一個名為「想哭」 (WannaCry) 的勒索惡意軟件 (蠕蟲，Worm)。被感染的電腦內的大部份檔案會被加密，並要求付出贖金作為復原的代價。

作為一個普通的互聯網使用者，我們沒有高層次的電腦和網絡知識，更對資訊科技安全一知半解。如何在這個資訊時代安全和健康地生存，確是一個非常大的考驗和挑戰。

本書將會討論如何武裝自己，不論在軟件和硬件上，更會在使用者行為和心態上的強化及武裝都會討論到。希望各位閱讀後有所得益和啓發。

由於這是本人第一次寫書，加上本人不才，其中難免有所錯漏，歡迎讀者指正與交流！

森美力 (Samiux) (網名)
寫於二零一七年五月十七日，中國香港

關於作者

森美力 (Samiux) (網名) 是一名資訊科技安全 (Information Security, InfoSec) 愛好者，他擁有由美國 Offensive Security 發出的 OSCE (Offensive Security Certified Expert)，OSCP (Offensive Security Certified Professional) 及 OSWP (Offensive Security Wireless Professional) 專業認證。他對網絡攻擊有深入認識，了解惡意黑客的行為。他是一名黑客，但並不是惡意黑客，嚴格來說，讀者可以稱他為灰客 (Grey Hat，灰帽子)。他的格言是「未知攻，焉知防」。

他曾在警隊服務，具有多年刑事偵緝經驗，對罪犯行為心態略有研究。

他是 Linux 系統的愛好者，他喜歡使用 Ubuntu Linux。

他擁有多個活躍的資訊科技安全研究項目，例如防禦入侵系統，匿名瀏覽系統，高安全性網頁伺服器設定，「抓我吧，若果你有能力的話」系列等。他也是一名博客 (Blogger)。他閒時會編寫程式及閱讀，他更會在其滲透測試 (Penetration Testing) 實驗室中作實驗時而自得其樂。他有建設同時亦有破壞。

他的其他著作有「知彼知己 - 資安篇」。

讀者可以在這裡接觸他 ：

(1) 其博客 - https://samiux.blogspot.com
(2) 其網站 - https://www.infosec-ninjas.com
(3) IRC freenode - #infosec-ninjas

關於本書

在寫作本書時，我考慮到一般的電腦書籍都因為軟件與硬件的更新，而令書中所描述的題材和內容脫節。所以我想寫一本較為長春的書籍。並且會用較為深入淺出的書寫方式去完成。

本書主要論述的是如何改變一般網絡使用者的行為與心態。從認識科技罪案，罪犯的行為，來避免成為下一個科技罪案的受害者。

本書亦會提及一些軟件或方法去武裝你的電腦來減低被入侵的機會。

本書對象

讀者無需具有資訊科技安全知識，但必須具有普通使用電腦常識及上網經驗。本書是寫給那些想在網上滑浪時倍加安心的讀者。

致謝

出書是個浩大的工程項目，在本書寫作其間，經常遇到很多困難，經過數天時間的努力才完成。借此機會感謝所有使本書能夠順利出版及提供幫助的專家及朋友。

特別感謝我女友在背後的支持。感謝我的家人和朋友，你們為我付出很多！

在此，我要感謝活躍在網絡上的資訊科技安全專家們，你們的公開文章和技巧讓我學到了很多優秀的技術。

聲明

第一章　基本概念

甚麼是惡意軟件?
惡意軟件 (Malware) 具有不良企圖的軟件。例如，病毒 (Virus)，木馬 (Trojan)，蠕蟲 (Worm)，勒索軟件 (Ransomware) 等。其出現形態包括執行檔或腳本 (Script)，如 JavaScript。

病毒有自我複製及感染其他檔案的能力。木馬就是所謂的後門 (Backdoor)。蠕蟲具有滲透能力，即會攻擊下一個目標。勒索軟件可能會具備以上所有特徵及加上將受害者的檔案加密，並要求贖金來解密。

當下幾乎所有網站都有使用 JavaScript 來製作互動網頁。JavaScript 是在瀏覽者的電腦上運行。若果網站被騎劫或者該網站由惡意黑客所建立，在其網頁植入惡意的 JavaScript 的話，受害者多數在不知情的情況下受到感染而被入侵。

甚麼是社會工程？
社會工程 (Social Engineering) 是一種欺騙的手段和技巧。出現的形態可以千變萬化，可以是經電話，電郵，連結，網站及下載等。我們經常聽到的「釣魚」 (Phishing)，就是其中一種。誘使受害者作出或不作出某種行為，而達到目的。

甚麼是中間人攻擊？
中間人攻擊 (Man-In-The-Middle Attack) 是受害者的通訊被脅持，其通訊被脅持者篡改或監聽 (Sniffing)。有時已加密的通訊亦可以被脅持者篡改或監聽。

有時可以在受害者下載或上載檔案時，植入惡意軟件。這的確是防不勝防。

甚麼是漏洞？
漏洞 (Vulnerability) 是指程式設計時在邏輯上或編程上出錯。這可以看作是一個「臭蟲」(Bug)。不是所有臭蟲都是漏洞，不是所有的漏洞都可以被利用 (Exploit)。可被利用的漏洞是可以入侵受害者的系統。

通常漏洞可以經更新而修復。但是在某些情況下，有些系統在有更新的情況下，也不能作出更新，例如若果更新了，系統就會崩潰。

甚麼是密碼強度？
從前的密碼長度建議是八個位，但是因為現今的硬件運算能力非常強大，八個位長度的密碼可以在十五分鐘內破解。

所以我現時建議至少十六個位的長度，其組合包括大細楷英文字母，數目字及標點符號。而且其組合不能有意思或可以推算得到。

因為這麼長的密碼是非常難記憶的，所以讀者應該要有密碼策略 (Password Policy)。再者，盡可能不要重用密碼。因為只要密碼被洩漏，你的所有賬號就會全軍覆沒。

甚麼是保安設備？
常見的保安設備有防毒軟件及防火牆。但尚有統一威脅管理系統 (Unified Threat Management System, UTM) 及防禦入侵系統 (Intrusion Detection and Prevention System, IDPS) 等。

現在的統一威脅管理系統和防禦入侵系統十分相似。所以在選購時要清楚了解產品的特性和自己的需求。現在流行一種叫做下世代防火牆 (Next-Generation Firewall)，其實它與統一威脅管理系統和防禦入侵系統相當近似。

甚麼是備份？
備份 (Backup) 是將你的有價值的檔案做一個複製品，並安置於一個安全地方。備份有分日，月，年。而當中亦有雙單日，雙單月，雙單年之分。以防數據流失，最好有超過一個複製品。

甚麼是黑客？
黑客 (Hacker) 一般是指技術精湛的人，能令設備做出一些不在設計情況之下運作。

在資訊科技安全領域下，黑客是指一個具有精湛電腦技術的人，能使電腦在不在其設計的情況下運作。在我等來說，黑客有分黑帽子 (Black Hat)，白帽子 (White Hat)，灰帽子 (Grey Hat) 及腳本小子 (Script Kiddies)。

黑帽子是指所謂駭客，他們是作奸犯科之流。

白帽子是指資訊科技安全專家或研究員，他們測試系統漏洞，並公報結果給有關開發人員或機構。

灰帽子也是資訊科技安全專家或研究員，他們也測試系統漏洞，但他們大多數不會向有關開發人員或機構公報其發現，他們會直接披露 (Full Disclosure)。他們多數走在法律邊緣，但並沒有惡意。

至於腳本小子，他們並不是資訊科技界中人。他們會利用黑客工具作樂或者作惡。

第二章　行為心態

我的朋友當中，大多數都認為他們不會是惡意黑客的目標。原因是他們自以為不具知名度，沒有有價值的資料在電腦或智能手機中。

有的就較為灰色，認為不具備知識和能力去阻止被入侵。有的是知道風險的，但礙於要玩電子遊戲，所以不設防。有的更完全不知道有何風險。

有些則經常瀏覽不良網站，經常被不停彈出的所謂廣告所滋擾。

有的使用老舊的無綫路由器 (Router)，加密協議 (Protocol) 已經過時或有漏洞。也有的不設定無綫網絡密碼，他們不介意別人使用他們的無綫網絡。

有的是為了要省下一些上網數據流量，而使用公用無綫網絡 (Public WiFi) 或公用電腦。有的更用來作銀行交易或處理敏感資料。

有些則認為更新作業系統和應用程式是浪費時間。

有些朋友則認為蘋果公司的 macOS 和開源的 Linux 作業系統是固若金湯，不需要用保安設備。

更多的朋友認為不隨便下載，不隨便點擊連結或附件和不到不良網站，就沒有機會感染病毒及被入侵。所以防毒軟件是不需要安裝的。

最近的「想哭」勒索軟件蠕蟲 (WannaCry) 事件，確實喚醒很多愛理不理和一知半解的電腦用戶。他們因為沒有更新其作業系統，導致被蠕蟲入侵並被加密檔案。

經常更新

因為電腦程式設計時在邏輯上或編程上出錯，而做成臭蟲或漏洞。有些開發人員知道的就發出補丁 (Patch)，用戶應該立刻更新。但有些並未被開

發人員發現的，有可能會被惡意黑客利用，這是所謂的零日攻擊 (0Day)。

更新包括作業系統及所有應用程式，例如防毒軟件，瀏覽器及路由器固件 (Firmware)。

防毒軟件

雖然大多數的防毒軟件都是後知後覺，當發現有新品種或變種的惡意軟件時，他們才開發病毒定義 (Signature)。但大多數的防毒軟件都可以擋隔一些入侵攻擊。

大多數蘋果公司和開源類 Unix (如 Linux) 系統的使用者都認為不需要安裝防毒軟件。原因是，他們認為此等產品在設計上是非常安全的。但事實不是如此，任何電腦系統都有可能感染惡意軟件。所以，我個人認為任何電腦系統都應該有防毒軟件的保護。

防火牆

基本上防火牆是可以被高級技術的惡意黑客所繞過。又例如應用程式使用了一個埠 (Port)，而該應用程式存在可被利用漏洞的話，防火牆並不能發生作用。

但我個人仍然認為，防火牆是必須安裝和設定。除非有特殊情況，大多數都是不准外界連入，只准向外連出。在網絡內每一部電腦都應該設定防火牆。

中間人攻擊

中間人攻擊 (Man-In-The-Middle Attack) 多在內聯網發生。地址解釋協議 (Address Resolution Protocol, ARP) 被欺騙 (Spoofing) 後，中間人攻擊就可以發生。你的所有通訊都會被脅持和監聽 (Sniffing)。所有通訊內容，包括加密了的通訊，都可以被篡改及監聽。

如果在同一個網絡段 (Subnet) 內，例如在家中使用有綫或無綫網絡，其中有一部電腦或設備具有惡意的意圖，發動了地址解釋協議欺騙。你的所

有通訊都會被脅持及監聽。你的通訊內容會被篡改，更甚者，會在你下載或上載的其間植入惡意軟件。

基本上，大多數商業用途的路由器和集綫器 (Switch) 都會有防止地址解釋協議欺騙的設定。但多數家用的就不會有了。

所以，不要使用公用電腦或公用無綫網絡，包括需要密碼和加密了的。而且，家中的無綫網絡密碼要設定為高強度 (見第一章)，如果可以的話，至少每月改變密碼一次。更不可以不設定密碼。再者，無綫路由器的加密協議應當不是 WEP 和 WPA，至少需要是 WPA2。

社會工程

社會工程 (Social Engineering) 是一種欺騙手段和技巧。它的攻擊手法千變萬化，可以經電郵，附件，連結，下載，電話及網站等。

不論資訊由何人發出，讀者都要小心行事。不要立即相信其是由可信任的來源發出。應先查證其來源，不要不加思索地點擊任何連結或下載任何附件。不要瀏覽不良網站，包括色情網站，侵犯版權的網站等。原因是那些網站的保安不會太強，又或者該等網站是由惡意黑客所建立。

很多檔案都可以被植入惡意軟件，例如 PDF, Word 的 Doc 及 docx, 多謀體檔案等。

網站安全

我們其實並不知道自己瀏覽中的網站是否安全。所以我們不要輕易地將個人資料，包括信用咭資料，交給網站。若果該網站被入侵，我們的資料便會被洩漏。如果要網購，在付款時，應該選擇付款閘道 (Payment Gateway)，如 PayPal 等。

有些網站的保安做得十分陽春，被入侵的機會大增。當一個網站被入侵後，惡意黑客除了會盜取資料外，他們更會植入惡意軟件，例如惡意的 JavaScript。當瀏覽這樣的網站時，瀏覽者就會感染惡意軟件而被入侵。

被入侵的後果

當受害者的電腦被入侵後，惡意黑客可以放下任何東西或同時取走電腦內的資料。惡意黑客可以利用受害者的電腦作非法用途，例如作為跳板攻擊其他電腦或設施。又可發佈不良資訊，例如侵犯版權的多謀體，兒童色情謀體等。又或者將其變成殭屍網絡 (Botnet)，發動大型網絡攻擊。

受害者的電腦和網絡頻寬將會變慢，除此之外，受害者有可能沒有察覺到其電腦已被入侵。所以不要小看這個風險。

結論

讀者的電腦或者是智能手機要視如寵物，要經常照顧。除了以上所提及的情況，惡意黑客經瀏覽器入侵時有發生，這是大部份人所忽略的。所以，除了要糾正以往錯誤的觀念與行為外，還要在軟硬件下功夫。

第三章　招兵買馬

路由器

首先，我覺得路由器是必需品。路由器是內聯網的最前線。大多數的路由器都有防火牆，有的更有多種額外功能，例如虛擬私人網絡 (Virtual Private Network) 等。

千萬不要開啟遠端控制 (Remote Access Control) 功能。我不能接受在內聯網以外操控路由器。如有必要遠端控制的話，至少要經虛擬私人網絡作出操控。若果路由器暴露在互聯網上是非常危險的，因為路由器的登入密碼有可能被爆破 (Brute Force)。又或者不排除路由器有漏洞而受到攻擊。

至於無綫網絡方面，至少要設為 WPA2 (或 WPA2-Personal)，而加密協議至少為 AES。再加上非常強的密碼強度 (見第一章)。最好是每月更改無綫密碼一次。

若果讀者的路由器有地址解釋協議設定的話，必須將其下所有電腦及電子設備的硬體地址 (MAC Address) 加到設定中。其他沒有加入的設備是不可能通過路由器的，這可以避免中間人攻擊。

如果讀者有相當好的電腦知識又想自己建設一部路由器的話，我會建議使用 pfsense。

集綫器

如果有需要使用集綫器，我建議使用有地址解釋協議的商業用途集綫器。因其具備地址解釋協議設定。

保安設備

保安設備如防禦入侵系統，統一威脅管理系統，下世代防火牆等的大多是商業產品，它們是非常昂貴。家庭用戶是不能接受的。但我們仍然有一些較為相宜的方案。

防禦入侵系統方面，我會建議使用 pfsense 和它的 Suricata 插件 (Plug-in)。又或者使用我開發的牛角包 (Croissants)。

至於統一威脅管理系統，我會建議使用 Untangle。

以上的軟件是可以免費獲得的，有的是需要付年費的。但牛角包是不需要年費，是完全免費的開源項目，詳情可以瀏覽我的個人網站。

瀏覽器

我較為鍾情於火狐瀏覽器 (Firefox)，所以我只可介紹火狐瀏覽器的插件 (Add-on)。

(1) NoScript
(2) WebRTC Control
(3) Cookies AutoDelete
(4) HTTPS Everywhere

以上的插件可加強瀏覽網頁時的安全性，大大減少受感染或被入侵的機會。

Ubuntu Linux 系統

如果讀者是使用 Ubuntu Linux 系統的話，我建議安裝以下軟件。

(1) ArpON
(2) Apparmor
(3) ClamAV

至於安裝詳情，請參閱我的博客 (https://samiux.blogspot.com)，是英文版本的。

附件一　牛角包

牛角包 (Croissants) 是一個設計十分獨特的防禦入侵系統。它是一個開源項目，由我獨自開發，它是完全免費。它獨特之處在於它能夠識別惡意黑客的企圖，進而作出攔截反應。

雖然設計簡單，沒有華麗的使用介面，但是它的效率非常高，能處理 1000 Mbps 或以上流量。它的低延遲特性，對綫上遊戲的影響減至最少。適合用於個人，家庭，小型企業等。

它近似於統一威脅管理系統和下世代防火牆。它具有抵擋病毒，偵測掃描，堵塞漏洞等等功能。

硬件基本要求 ：

(1) Intel i5 四核心處理器
(2) 16 GB 記憶體
(3) 256 GB 硬碟
(4) 3 個 1000 MB 網絡界面

詳情請瀏覽我的個人網站 (https://www.infosec-ninjas.com)，是英文版本的。

全書完