ＸＸ科技有限公司網站被駭調查報告

一．緣起

ＸＸ科技（以下簡稱ＸＸ）於 2024/5/20 連絡本工作室，因為公司網站（網址: https://example.com.tw）被駭客入侵，被主機商ＸＸ因為一直傳送垃圾郵件而通知當事人，並且將網站暫時鎖上密碼以避免進一步的損害。

二．調查過程

本工作室以ＸＸ提供之主機後台帳號密碼，進入主機後台之檔案管理員查看，發現除了幾個核心的 PHP 程式被篡改，加入惡意程式代碼之外，也在網站的各個資料夾發現許多不應該存在的檔案，這些檔案都含有惡意程式在裡面。

三．處理過程

1. 首先將有問題的檔案包含 WordPress 核心程式檔案全部刪除
2. 尋找夾雜在用戶上傳資料以及外掛目錄中的惡意程式檔案並將它刪除
3. WordPress 核心程式及各個外掛檔案從官方網站下載最新版本壓縮檔，上傳之後解壓縮（舊外掛檔案會先刪除）
4. 使用的付費佈景主題 Flatsome 由於本工作室也有購買，所以從購買網站下載最新版本，刪除舊檔案之後上傳解壓縮
5. 檢查資料庫檔案發現除了最早建站的網頁設計公司（ＸＸ科技）開立的 eric 管理員帳號之外，多出一個疑似駭客新增的 trpwaxnfkw 管理員帳號，先將這兩個帳號降級為訂閱者以避免進一步的傷害

6. 檢看網站的存取記錄，發理在 5/5 日就有駭客利用程式漏洞建立上述管理員帳號，並於 5/8 開始以該帳號進入後台上傳惡意程式並觸發使其運作
7. 另外 5/8 以後駭客用不同的 IP 登入，也經將這些 IP 使用主機後台封鎖
8. 檢查網站使用的 PHP 版本，發現使用的是已經停止更新不安全的 7.4 版，已經由主機後台更改為目前安全的版本 8.1 版
9. 確認所有檔案就緒之後，請 XX 停用密碼保護
10. 本工作室新增一名 Gordon 的管理員帳號，然後以此帳號進入網站後台進一步調查
11. 後台出現佈景主題的授權無效的警告，原因後面說明
12. 進一步發現網站的更新機制被人停用，所以網站不會出現某些程式要更新的通知
13. 還有許多安裝的外掛實質上並沒有使用，已經先將這些外掛停用，觀察網站也都正常運作，確認外掛是多餘的
14. 在網站的頁腳又發現被插入一個不知是什麼網站的連結，造成頁面最下方有一大段的黑色，也將它移除
15. 加裝安全防護外掛並設定相關安全措施，像是：登入頁面加上驗證碼以防止機器人大軍試網站密碼等等
16. 至此網站清除作業已告一段落

四．被駭原因說明

1. 網站程式因為更新功能被關閉，所以兩年多來都沒有更新，這是第一個被駭的管道
2. 主機的 PHP 版本也是太舊沒換成新版本，這是第二個被駭的管道
3. 5/5 被註冊管理員帳號有收到通知信，但是相關人員沒有處理導致後續的嚴重狀況
4. 安裝太多沒在用的外掛而且也沒更新，更增加被駭的風險
5. 沒有安裝任何安全防護外掛，也沒有任何後台防護機制，讓駭客可以放心的試網站的弱點（有安全防護機制會把重覆試密碼的 IP 都封鎖）
6. 還有網站從建站以來就一直有一個網頁公司建立的管理員帳號 eric 存在著，而這個帳號如果對方意圖不良或是密碼外流都會成為網站被駭的漏洞
7. 綜合上述就是網站需要一個管理安全的管理員才是常久之計

五．額外發現

在檢查網站在 Google 的收錄狀況的時候（在網址列輸入 site:example.com.tw），意外發現 Google 收錄了幾千個網址，這些被 Google 收錄的網頁叫**垃圾索引**。這些網址之前點進去應該是有效的，也就是說網站已早被駭客入侵，而且利用當成別人網站的跳板，而會收錄這麼多網址不是一天兩天就可以達成的，這一點還有待調查

關於**垃圾索引**產生的原因有：

- 網站遭到駭客入侵，駭客在網站上植入了惡意程式碼，自動生成大量垃圾內

容。

- 網站本身存在漏洞，被 SEO 黑帽業者利用來植入垃圾內容。
- 網站內容品質低落，被 Google 判定為垃圾內容。

垃圾內容收錄會對網站造成以下負面影響：

- 降低網站排名：Google 會降低含有垃圾內容的網站排名，使其在搜尋結果中更難以被使用者找到。
- 損害網站形象：垃圾內容可能會誤導使用者，使其對網站產生負面印象。
- 影響使用者體驗：垃圾內容可能會干擾使用者瀏覽網站，降低使用者體驗。

再詳細檢視這個網站在搜尋引擎相關的關鍵字ＸＸＸＸ、ＸＸＸ等都無排名，這樣子無法透過網站讓潛在客戶找上門，實在可惜

已處理問題

1. 網站被駭並植入惡意程式本工作室理完畢，並且會持續監看三個月
2. 不該存在的帳號也會一併刪除
3. 網站已加上安全外掛並強化安全措施短期內應該不會再有問題
4. 網站也加上快取外掛，網站速度比原先快上許多
5. 在監看的三個月期間，本工作室會設定也會收到系統的通知信
6. 到期後將會刪除 Gordon 帳號並不再接收網站通知

待解決問題

1. 網站使用佈景主題因為當初的建立公司將同一份購買的版權使用在很多網

站，這樣是不合法的，貴公司可以要求ＸＸ科技再買一份你們專屬的序號給你們用（視當初合約簽定的權益為準），如果對方不願意那就要貴公司自行購買一份版權（購買網址 https://themeforest.net/item/flatsome-multipurpose-responsive-woocommerce-theme/5484319 費用美金$59 元）

2. 網站有許多外掛並沒有使用，請貴公司人員確認網站都正常後，本工作室會將它們刪除
3. 網站建議**連絡我們**要有一個表單的接客戶的詢問，這是基本的網站功能，不應該沒有
4. 上述管理問題本工作室有提供網站代管服務，如果在三個月內購買此服務可以折價 NT$ 1,000 元，購買網址 https://gordon168.tw/managed-hosting/ B3 方案
5. 或者在ＸＸ主機合約到期後轉到本工作室主機，這樣會更安全（上述購買連結的 A1 方案）
6. 搜尋引擎垃圾索引及關鍵字優化 SEO 的問題，本工作室也有提供服務，費用雙方協議內容後再報價，搜尋引擎優化的好處：你們在搜尋**網站被駭**找到排名第一的本工室，進而尋求協助，這就是商機所在，這是目前ＸＸ公司網站存在的最主要目的，但是往往被不懂搜尋引擎優化 SEO 的網頁設計公司忽略了，這樣花大錢建立的網站卻無法達成功效實屬可惜

以上為ＸＸ公司網站被駭的處理過程及建議事項　報告人：高登工作室