程式設計期末書面報告

第七組 PeekDOGS 組員：許晉洋、許晉芳、洪瑋廷、黃資翔、莊雅雯

A. 主題

”The quieter you are, the more you are able to hear.” 以此當作設計基本原則，PeekDOGS 能夠被在背景執行，側錄鍵盤輸入的內容，隱匿的將檔案存在指定的地點，在超過一定容量時，自動以附件方式寄出內容。這種不具破壞性的病毒讓受害者難以察覺，但給施放病毒者更大的實質收穫。PeekDOGS 也附加了自動螢幕截圖功能，方便監看受害者正在使用的網站，搭配上鍵盤側錄信件所寄發的時間，加害者可以輕易的解讀鍵盤記錄的內容，達到偷取帳號密碼的目的。此外 PeekDOGS，同時會監看 USB 插口，在插入隨身碟時自動備份所有內容。PeekDOGS 在首次執行時，會將自己加入開機自動執行程式，擅長長期監控。

B. 系統設計及演算法

系統主要分為兩大部分，一是鍵盤記錄與螢幕監控，二是檔案備份。兩者都以函數分別編寫，並使用 multithread（多線程）的方式並行，不互相影響，讓程式的擴充性增加，所有不相干的功能，都可以以一個新的 thread 來加入程式。

第一個功能以鍵盤記錄為基礎，每當受害者點「左鍵」如果距離上次點擊的時間超過 2 秒則紀錄螢幕，並且以紀錄的時間（time(0)，即 1970 年 1 月 1 日至今的秒數）來命名檔案，這樣就可以知道確切時間受害者正在使用的網站。擷取螢幕所使用的函數來自<window.h>，用 GetSystemMetrics 的函數取得螢幕的長寬、用 BitBlt 的函數取得畫面，最後用 CImage 的 classes 將圖案存成 bmp 檔。

a.螢幕截圖 picture 函數

1) 需要 include <windows.h> 跟 "stdafx.h" 的標頭檔
2) 首先先用 GetSystemMetrics 的函數取得螢幕的長寬
3) 用 BitBlt 的函數取得電腦畫面的圖案
4) 最後用 CImage 的 classes 將圖案存成 bmp 檔，並可指定要存在哪

值得注意的是當我們將圖片存檔時，一定要讓檔案名稱每一次都不一樣，才不會使最新的檔案取代舊的，因此我們讓檔案名稱為現在的時間，所以需要 include <ctime> ，檔案名稱為 time(nullptr)，也就是 1970 年到現在的秒數。未來可以把檔案名稱存成年月日，這樣會比較方便。

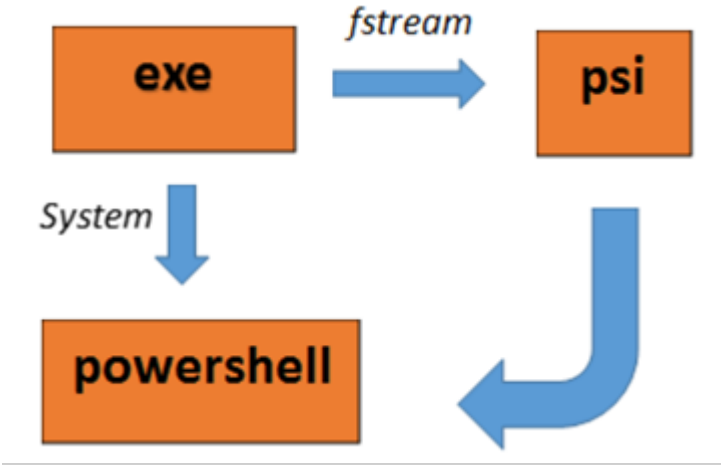
檔案備份的功能包含在電腦上的備份與發出電子郵件，備份隨身碟的功能首先利用，<dirent.h> 的 opendir 函數來開啟 F ：（目前只是為了示範，所以沒有加入 D ：），如果可以開啟就執行 copydir()，若否則持續偵測。這邊老師可能會懷疑這樣持續的偵測會不會因為大量的 while loop 讓 CPU 有過高的使用率，答案是否定的，我們特意在每次迴圈前加入：

std::this_thread::sleep_for(std::chrono::milliseconds(1000))，如此一來，偵測每一秒只會發生一次。

copydir()是以遞迴的方式寫成，只要在參數中填入想複製的檔案夾（在專案中就是整個隨身碟）就會複製整個隨身碟的內容，檔案的類型沒有任何限制，.pdf .docx .ppsx .exe 等都能複製。函數首先複製裡面每個「非檔案夾」的檔案，對於檔案夾內的檔案夾，函數則會將其當作新的參數呼叫 copydir()，來遞迴呼叫，除此，對於大小超過 10MB 的檔案，我們選擇將其跳過以提升效率，這個部分可以自己任意調整。目前為了 debug 的方便，複製的檔案都會被存在 C:\Users\user\Desktop\fake 路徑。

b.信件檔案寄送:

為了將竊取的輸入資料傳出，採用了 windows 內建命令列殼程式，只要電腦使用 windows system 都能夠使用這樣的方法傳輸。使用的方法也相當簡單，powershell 能夠讀取.ps1 檔案並執行指令，因此利用 fstream 建立一個我們需要使用到的 ps1 檔，用 system 呼叫 cmd 來執行 powershell 並把剛剛建立的檔案交由 powershell 執行，最後將 fstream 建立的.psi 檔移除，如此一來，如果對方想得知信件寄出的方向就不會那麼容易。



C. 心得

1. 洪瑋廷：其實一開始我本來想做的是一個德州撲克的 AI 自動打牌機器，不過我的組員似乎沒什麼興趣，所以這就變成我寒假想做的事之一啦。我們這組做的是病毒，算是相當令人耳目一新的題目。我負責一部分的 Key logger，也就是紀錄鍵盤的動作的部分。我後來發現，難處主要是在熟悉 windows 的指令的部分。這部分由於課堂上並沒有教過，所以只能上網慢慢學習摸索。不過在做完 project 後，算是對 windows 的指令模主有了初步的了解。在看其他組報告時，其實大部分的組別都會認為熟悉一套新的語言或模組是整個 project 中最困難也最花時間的部分，我十分的認同。然而這樣的開放式 project 讓我們有機會自學，而我也見識到網路的強大，幾乎所有 code 方面的問題在網路上

都有解答，尤其是英文的網站。在未來，我想一定還有許多機會需要自學，因為學校教的東西畢竟過於侷限，所以培養自學的能力十分重要。在經過一個學期的扎實訓練後，我想我已經有能力能看懂網路上大多數的文章的大致內容，這應該能說是相當大的收穫吧。雖然我不是資管系的本科生，但我覺得寫程式其實蠻好玩的，也可以做到許多令我感到驚奇的事。我相信我以後一定會繼續寫程式，完成更多有趣的 project。

2. 黃資翔：我覺得這次我們做的東西很特別，一開始認為病毒這種東西很難，根本做不到，但事實上每一組要做的東西大部分都是上課沒教過的，所以就覺得我們要做的病毒也沒比較複雜，於是我就很認真地上網查很多資料，我發現幾乎找不到中文的資料，大部分的資源都是英文，因此我的確花了蠻多時間在理解上面。我做的是螢幕截圖，一開始我以為只要叫一兩個函數出來就搞定了，沒想到過程遇到許多問題，於是就上網找解決方法，也尋求助教救援。一開始用 dev c++ 寫的時候它要我 link 一堆函數，我實在是搞不太懂，之後用 visual c++ 它就已經幫忙 link 好了。透過這次期末報告我收穫的比期中更多，讓我知道資訊這塊的知識學也學不完，只有當我們需要的時候，上網查資料是最快的方法。我們程式已經學一學期了，說真的我覺得我進步很多，但當我學到的知識愈多，我發現自己不會得愈多，真是奇妙，也謝謝我們這組的各位，你們都好厲害。

3. 許晉洋：當初一時興起問教授可不可以寫電腦病毒當作期末專案的主題，教授豪不猶豫的答應後，我傻傻地就開始這次挑戰，這種非法的東西資料本身就不是非常好查，真的是不知道爬了多少文、試過多少最後根本沒用的方法，並且這些少部份能用的方案中，又有很多沒辦法「安靜」的在背景執行，不時就會跳出命令提示字元的黑色視窗，畢竟寫病毒不會有人幫你寫好好用的人性化函數，只要隨便叫叫就能完成工作。中間其實還蠻想放棄的，但礙於顏面，加上拖了 4 個人下水，也不是隨隨便便就能換個題目從頭來過，還是硬著頭皮走了下去。過程中因為程式碼來自每個同學，大家使用不同的編譯器，在整合的時候面臨的很大的困難，編碼問題、使用函數的規範（visual studio 就是喜歡特立獨行）、標頭檔、內建函式庫等等都有地方無法整合，最討厭的是，編譯失敗的錯誤訊息十分難讀，尤其當以上這些問題混雜在一起，就更難找出出錯的地方，最後甚至有一部分的程式必須砍掉重練，才終於完成最後的成品，對於同組的同學們，我想說：「大家辛苦了」。這個專案大概有 80%的東西都是上課完全沒有教過的，相信大家雖然過程跟我一樣很挫敗，但學到了很多東西。

4. 許晉芳：基本上這次寫 project 沒有用到很多上課直接授課的東西，唯一用到大概是字串處理，而且用的還是 string 居多，因此也遇到很多之前沒想到的問題，例如：怎麼讓複製檔案、傳輸檔案…，甚至是如何讓執行視窗不要一直出現，很多都必須要自己去找答案，自己嘗試，比起照本宣科的寫題目要困難上

許多。在過程中慢慢發現什麼地方可能出現需要的答案，雖然有些問題到最後還是沒解決，但也寫出了整體大略的雛形，是一次很棒的經驗。

5. 莊雅雯：這次本來有負責個檔案加密的部分，但由於修改太久導致時間不夠，無法加入最後的程式感到稍嫌可惜，但在寫的過程中是挺愉快的。看到組員們幾乎達成最初設下的目標，內心真的感到相當佩服，並且期許自己未來能跟他們一樣厲害，不過就目前來看是任重而道遠了。

D. 組內分工：

主 coder：許晉洋
鍵盤記錄：洪瑋廷
螢幕截圖：黃資翔
寄信功能：許晉芳
檔案加密：莊雅雯
報告彙整：莊雅雯