PeekDOGS

”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。

系統設計：

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。

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。

心得：

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。