主動式惡意程式自動化蒐集系統與樣本搜尋分析服務

指導老師：曾俊元 博士

專題生：李建瑩、李思賢、涂俊全、陳映綸

前言

現今網路上惡意程式不斷的翻新，市面上各家防毒軟體對於防堵這些新種惡意程式不斷的改版更新。但對於這些病毒和防毒軟體，似乎沒有一個適合的平台來做為一個統一比較的基準。

摘要

在病毒相關的研究當中存在了一個相當嚴重的問題，那就是---缺乏穩定的樣本來源。另一個問題：市面上各家掃毒軟體對於病毒的定義不同，對於比較各家產品的偵測率產生的極大的困難。

為了解決這個問題，我們利用了目前網路上常使用的 P2P 軟體來蒐集可疑的檔案。並使用一個擁有大量掃毒軟體的網站資源來做為基本分類所蒐集到的檔案是否為惡意程式。最後架設一個網站，做為提供相關研究人員一個簡單的分析工具。

專題架構

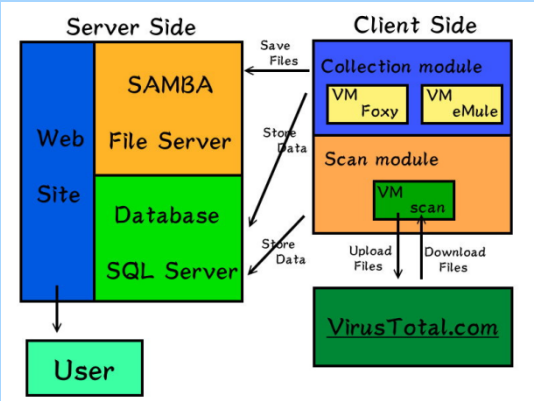

圖 1、系統架構圖

我們將此實驗系統大致分為兩個架構：Server 端和 Client 端。Server 端儲存可疑檔案和其資訊和 Web Site。Client 端可大致分為「病毒蒐集模組」和「病毒掃描模組」。前者使用了 Foxy 和 eMule 兩個 P2P 軟體做為蒐集程式，後者使用了 VirusTotal.com 這個網站提供的 API 做為各家掃毒軟體對檔案偵測結果的資訊來源。

貢獻

建立了一個 P2P 自動化蒐集病毒系統，目前共蒐集了 6825 隻病毒樣本(其中 4310 個樣本被 5 家以上的防毒軟體視為病毒)，且樣本持續增加更新中、提供研究人員做相關研究的分析介面。

圖 2、分析網站截圖

惡意程式與防毒軟體分析

圖 3、各家防毒軟件在各月的偵測量

銘謝

感謝曾俊元老師在專題整個過程中的指導，使我們在整個專題想法上更加周全、成熟。也要感謝學長們，剛進實驗室時，對環境、使用系統相當不熟悉。在他們熱心的幫助下，漸漸的步上軌道。