

致理技術學院

資訊網路技術系 實務專題報告

行為檢測與可疑程式分析系統

指導教師：蕭勝華

學生：謝毓書 (19734106)

蔡政達 (19734108)

古淳仁 (19734127)

謝承恩 (19734136)

劉必寬 (19734139)

陳奕亘 (19734140)

中華民國 100 年 12 月

目 錄

專題研究授權書.....	i
誌 謝.....	ii
摘 要.....	iii
目 錄.....	iv
圖 目 錄.....	vi
表 目 錄.....	ix
第壹章 緒論.....	1
第一節 重要性與發展演進.....	1
第二節 研究動機與目的.....	9
第貳章 常見攻擊方式與解決方法.....	11
第一節 病毒介紹.....	11
第二節 隱藏的行程之歷史演進.....	17
第三節 主開機記錄(MBR)的攻擊.....	20
第四節 ROOTKIT.....	26
第五節 開機型病毒與隱藏在登錄表的攻擊.....	29
第六節 本軟體提供之檢測方式略述.....	37
第參章 軟體功能技術.....	40

第一節 行程管理.....	40
第二節 監控配置.....	45
第三節 驅動模組列舉.....	49
第四節 監控訊息.....	50
第五節 SSDT.....	51
第六節 檔案管理器.....	53
第七節 網路防火牆.....	55
第八節 PE 檔案訊息.....	57
第肆章 系統實作與呈現.....	61
第一節 行程管理.....	61
第二節 監控配置.....	66
第三節 列舉驅動模組.....	76
第四節 監控訊息.....	78
第五節 SSDT.....	80
第六節 檔案管理器.....	81
第七節 網路防火牆.....	83
第八節 檔案資訊.....	86
第伍章 結論.....	88
參考文獻.....	90

圖目錄

圖 2-1 檔案型病毒感染示意圖	12
圖 2-2 Taiwan NO.1 心算遊戲.....	14
圖 2-3 Taiwan No.1 調侃文件.....	14
圖 2-4 巨集型病毒感染示意圖	14
圖 2-5 開機型病毒感染示意圖	15
圖 2-6 SetWindowsHookEx 函數示意圖	19
圖 2-7 鬼影病毒感染示意圖	23
圖 2-8 ring 級別示意圖	27
圖 3-1 rin0 和 ring3 連繫示意圖	51
圖 3-2 PE 檔案結構圖	59
圖 4-1 行程管理	61
圖 4-2 列舉 Process	62
圖 4-3 行程管理功能選項	63
圖 4-4 複製行程路徑	63
圖 4-5 警告視窗	64
圖 4-6 列舉模組與 Thread.....	64
圖 4-7 選定模組後的右鍵表單	65

圖 4-8 選定 Thread 後的右鍵表單.....	65
圖 4-9 監控配置介面	66
圖 4-10 Process 監控	67
圖 4-11 執行失敗警告視窗	68
圖 4-12 登錄表監控	68
圖 4-13 修改登錄表	69
圖 4-14 模組監控	69
圖 4-15 Kavo 病毒殺手	70
圖 4-16 隨身碟批次檔工具	71
圖 4-17 登錄表流量監控	72
圖 4-18 登錄表修改工具	73
圖 4-19 登錄編輯程式	74
圖 4-20 本機安全性設定值	74
圖 4-21 事件檢視器	75
圖 4-22 工作管理員	76
圖 4-23 驅動模組列舉(使用前)	77
圖 4-24 驅動模組列舉(使用後)	78
圖 4-25 監控訊息(使用前)	79
圖 4-26 監控訊息(使用後)	79

圖 4-26 SSDT 列表	80
圖 4-27 使用 SSDT 恢復功能的警示視窗	81
圖 4-28 檔案管理器介面	82
圖 4-29 刪除方式的選擇	83
圖 4-30 網路防火牆	84
圖 4-31 規則配置	85
圖 4-32 Net Message	86
圖 4-33 檔案資訊	86
圖 4-34 載入檔案資訊	87

表 目 錄

表 1-1 新病毒程式數量.....	2
表 1-2 目前常見的木馬的種類及威脅.....	7
表 2-1 病毒分配比例.....	17