附件二

經濟部資通安全事件調查結果報告

事件說明		
事件編號	(MOEA-AIR-西元年-流水號3碼，流水號每年由001開始累計，AIR：Accident investigation report)	
事件發現日期	**年　月　日　時　分**	
作業人員		
事件描述		
通報單 ID	（國家資通安全通報應變作業發配之編號，無則免填）	
通報作業日期	**通報日期：　年　月　日** **通報結案日期：　年　月　日**	
設備及證物(硬碟)資訊		
設備資訊	IP：	OS：
設備使用者或用途	主機名稱： 主機用途：	
設備 Patch 狀態	OS:	Office：
防毒軟體版本		
證物廠牌	（未保留證物則不需要）	
證物型號	（未保留證物則不需要）	
證物容量	（未保留證物則不需要）	
證物外觀	（證物照片，未保留證物則不需要）	
調查暨處理過程描述		
使用工具	調查時使用之軟硬體工具	
檢查項目	使用者電腦登入紀錄、系統機碼、處理程序及應用程式、檔案異動紀錄、USB 使用紀錄、上網紀錄、E-mail 紀錄、軟體使用紀錄以及記憶體暫存資料等項目	
發現狀況說明	遭植入惡意程式、有被打包資料殘留等	
疑有資料遭竊	□是　□否	
處理作業說明	停用網路服務、清除惡意程式等	

經濟部資通安全事件調查結果報告

惡意程式或工具樣本分析			
檔名			
存在路徑			
日期資訊	建立：	修改：	存取：
擁有者			
檔案大小(Bytes)			
MD5			
連線標的			
防毒軟體掃描結果			
行為描述			

檢討及建議事項

資料檔案檔名列表					
序號	檔名	檔案大小 (Bytes)	建立日期	修改日期	擁有者