延宇資訊股份有限公司

機密等級：■一般 □限閱 □密 □機密	文件編號：YAN-ISMS-04-53	保存年限：2年
日期： 115 年 03 月 31 日	紀錄編號：YAN-ISMS-G-53-11503-01	版本：1.0

威脅情資收集與處理記記錄單

登錄人員： 黃韋霖

項次	威脅情資收集日期	威脅情資來源/威脅情資內容	受影響之資通系統	採取相關控制措施								備註
1	115/03/30	Hinet SOC/病毒通告：Trojan.Inject6.30933 病毒 Trojan.Inject6.30933 是一種具備高度偽裝能力的惡意木馬程式。根據最新技術分析，該病毒被添加到病毒庫的時間為 2026 年 3 月 22 日。其主要危害在於將惡意程式碼注入到合法的系統程序%WINDIR%\syswow64\svchost.exe 中執行，藉此逃避安全軟體的行為監控，並在受感染系統上執行非法指令。	公司筆電、Veeam 9.5	掃毒檢查							蒐集人員	黃韋霖	
											處理人員	黃韋霖	
	向相關關注方通報：■否 □是，關注方通報窗口：_____		通報時間：2026/03/30 通報人員：黃韋霖	預計完成日期	115/03/30	實際完成日期	115/03/30	是否列入風險管理	否		主管確認	延宇資訊股份有限公司 梁維志	
2	115/03/31	Hinet SOC/Google 於03/31 公布將最新桌機版Chrome瀏覽器Windows/Mac版146.0.7680.177/178及Linux版146.0.7680.177版本釋出到穩定（Stable）通道，修補一個已發生攻擊或出現攻擊程式的漏洞。	公司筆電、Veeam 9.5	立即更新程式							蒐集人員	黃韋霖	
											處理人員	黃韋霖	
	向相關關注方通報：■否 □是，關注方通報窗口：_____		通報時間：2026/03/31 通報人員：黃韋霖	預計完成日期	115/3/31	實際完成日期	115/3/31	是否列入風險管理	否		主管確認	延宇資訊股份有限公司 梁維志	
3	115/02/26	國家資通安全研究院/研究人員發現Microsoft Windows與Office存在5個高風險安全漏洞，類型包含安全功能繞過(Security Feature Bypass)漏洞(CVE-2026-21510、CVE-2026-21513及CVE-2026-21514)與本機提權(Local Privilege Escalation)漏洞(CVE-2026-21519與CVE-2026-21533)，前者可使未經身分鑑別之攻擊者於使用者互動情境下繞過系統安全機制；後者可使已通過身分鑑別之攻擊者在既有權限基礎上提升權限。以上漏洞皆已遭駭客利用，請儘速確認並進行修補。	公司筆電、Veeam 9.5	立即執行設備軟體更新							蒐集人員	黃韋霖	
											處理人員	黃韋霖	
	向相關關注方通報：■否 □是，關注方通報窗口：_____		通報時間：2026/02/16 通報人員：黃韋霖	預計完成日期	115/02/26	實際完成日期	115/02/26	是否列入風險管理	否		主管確認	延宇資訊股份有限公司 梁維志	
											蒐集人員		
											處理人員		
	向相關關注方通報：□否 □是，關注方通報窗口：_____		通報時間：_____ 通報人員：_____	預計完成日期		實際完成日期		是否列入風險管理			主管確認		
5											蒐集人員		
											處理人員		
	向相關關注方通報：□否 □是，關注方通報窗口：_____		通報時間：_____ 通報人員：_____	預計完成日期		實際完成日期		是否列入風險管理			主管確認		