Kaspersky Lab Asia Limited
105 台北市松山區
民權東路三段 178 號 8F

(02) 7736 7376
www.kaspersky.com.tw
www.securelist.com

卡巴斯基聲明 – 回應行政院資通安全處與經濟部工業局對卡巴斯基軟體安全之疑慮

卡巴斯基重申，**卡巴斯基與任何政府並無任何關係，甚至在公司 25 年的歷史中，證明從無濫用公司資安技術。**事實上，我們一直在採取措施來保證產品的品質與安全性。截至今日相關新聞，皆因國際情勢與政治因素影響決定，並非對產品的技術進行驗證，卡巴斯基仍嚴守資安廠商對客戶的承諾。

鑒於行政院資通安全處與經濟部工業局因俄烏戰爭與國際新聞等因素，對於卡巴斯基端點安全軟體所延伸之資安風險疑慮，卡巴斯基提供下方技術聲明以釋疑政府風險控管之需求。

一、卡巴斯基軟體是安全的

(一)卡巴斯基軟體程式更新的主控權由客戶掌握

卡巴斯基的端點安全產品更新組成共三部分 - 程式、病毒碼與卡巴斯基安全網路資料庫(Kaspersky Security Network)。**其中軟體程式的產品更新由授權客戶的主控平台所控制，在無任何主控平台的權限下，用戶端的安全軟體並不會主動更換版本與軟體程式。**卡巴斯基主控平台的權限則建構於作業系統的主要權限之下，倘若客戶發現任何存疑，仍可透過作業系統移除。現今任何實用的軟體應用程式，皆有可能因有意或無意隱藏後門或其他惡意代碼，其中包含作業系統、應用軟體甚或是由未經認證的軟體開發團隊開發之相關系統，因此軟體開發與更版的流程所產生的資安風險遠高於地緣政治考量。

(二)卡巴斯基的產品和資料處理遵循標準認證方法

卡巴斯基的產品處理和/或傳輸的所有資料都通過加密、數位證書、隔離存儲和嚴格的資料訪問政策得到保護。此外，為確保我們用戶的最高安全性，卡巴斯基的數據服務已通過 TÜV AUSTRIA 的 ISO/IEC 27001:2013 認證（國際公認最佳實踐和適用的安全標準 https://www.kaspersky.com/about/iso-27001），並於 2022 年再次獲得擴大延伸範圍的認證，進而涵蓋網路威脅資料處理與數據統計的服務認證。該認證適用於公司位於蘇黎世、法蘭克福、多倫多等資料中心的數據服務。

卡巴斯基工程實踐的安全性和完整性也得到了獨立第三方評估的確認：公司成功通過了四大審計師的 SOC 2 審計（服務組織控制）（https://www.kaspersky.com/about/compliance-soc2）**，確認了卡巴斯基針對未經授權的開發和發佈軟體更新過程的安全性。**

- 卡巴斯基的旗艦企業產品卡巴斯基端點安全 (KES) 也通過了通用標準 (CC) 認證：
https://commoncriteriaportal.org/files/epfiles/2018-37-INF-2718.pdf

- 卡巴斯基企業產品的控制台卡巴斯基安全中心 (KSC) 也通過了通用標準 (CC) 認證：
https://ocsi.isticom.it/documenti/certificazioni/kaspersky/cr_ksc13_v1.0_en.pdf

這些認證符合歐洲對 IT 安全產品的要求，並為卡巴斯基產品的安全性和完整性提供了公正的技術證明。
卡巴斯基多年來一直致力於提高透明度，甚至不斷超越與提升。自 2018 年以來，卡巴斯基一直提供客戶和合作夥伴（包括各國政府）權益，可於卡巴斯基在全球（包括瑞士、巴西、西班牙、馬來西亞和加拿大）的透明中心檢查我們產品的程式源代碼和軟體更新內容。

重要的是，沒有證據顯示卡巴斯基產品曾被直接或間接用於非法行為。這已得到歐洲議會和整個歐洲的監管機構的認可，包括法國國家資訊安全局 (ANSSI)；意大利國家網路安全局（ACN）；瑞士國家網路安全中心（NCSC）；荷蘭國家網路安全中心（NCSC）和數位信任中心（DTC）；比利時網絡安全中心（CCB）；奧地利 CERT；和盧森堡的計算機事件響應中心。有鑑於此，我們非常關注任何對卡巴斯基的不當攻擊。我們致力於安全、透明和相互對話，並要求 NCSC 為我們提供機會，讓我們以公開和客觀的方式解決任何問題和疑慮，包括訪問卡巴斯基透明中心以審查我們產品的架構、程式源代碼和軟體更新。

(三)卡巴斯基更新主機的資訊流向

卡巴斯基的更新伺服器位於許多國家與區域，包括加拿大、荷蘭、德國、法國、中國、香港、墨西哥、新加坡等。卡巴斯基的產品初始值會自行選擇最近且高可用度的伺服器來提供軟體更新，卡巴斯基用戶更可依自選需求設置特定位置的更新主機。**卡巴斯基亦於 2020 年開始將台灣用戶的產品更新初始值從香港轉移至新加坡，目前台灣客戶僅會向新加坡、荷蘭、德國、法國與加拿大的更新主機更新軟體、病毒碼與卡巴斯基安全網路資料庫(Kaspersky Security Network)，以保障客戶的隱私與下載安全。**相對於在台灣仍有營利的全球資安業者，卡巴斯基更主動對台灣客戶承擔資安廠商應負的責任。

二、遵循台灣法令政策與管理

卡巴斯基身為全球知名的資安業者，過去參與全球 IT 安全社群和國際組織的聯合行動和網路威脅調查互動，這些組織包含國際刑警組織、歐洲刑警組織、執法機關和全球的 CERT 等，身為協助打擊網路犯罪的一員，我們深知遵循法律的重要性。**卡巴斯基是一家跨國獨立的私營公司，我們遵循各國的商業或資安法令政策與管理，我們也深信法律保障著每一位用戶與廠商的權益，**倘若卡巴斯基有任何主動或被迫違反當地法令，隨即而來面臨的訴訟與求償都將可能讓卡巴斯基退出全球的市場。卡巴斯基願意以完全透明、公開和客觀的方式（包括通過卡巴斯基透明中心）協助解決台灣客戶包含政府和監管機構對我們的營運和產品可能存在的任何擔憂。

三、持續承諾保障台灣用戶的資訊安全

網路犯罪無國界，犯罪技術近年進步神速，網路威脅與攻擊也越變複雜，不僅偽裝形式各異，更透過許多不同的媒介攻擊，沒有任何單一資安方案能夠提供全方位資安防護。過往台灣卡巴斯基曾協助政府相關部門有效阻擋已知的惡意程式，並建置「落地型沙箱」協助偵測來至特定區域的未知程序並有效阻絕相關針對式攻擊，防護的效益是非常顯而易見。

卡巴斯基的企業宗旨在於協助全球防範各類型的網路威脅，我們了解唯有長期持久的關係才能持續為客戶帶來信任與保障。卡巴斯基承諾會持續參加全球評測中心的檢測，透過中立的評測中心檢定卡巴斯基產品的品質；我們會持續執行透明中心計畫，為卡巴斯基產品的安全性、完整性與透明度提供公正的技術證明。**台灣卡巴斯基承諾依舊會在台灣的資安技術崗位上保障每一位持續對我們信任的客戶。**

台灣卡巴斯基

2022 年 4 月 11 日

kaspersky