「防彈」主機服務供應商：網絡犯罪基礎設施的盔甲出現裂痕

成功的網絡罪犯依賴安全、隱蔽且穩健的基礎設施。每宗網絡入侵、憑證盜竊、勒索軟件攻擊，或在非法論壇上出售偷竊數據案件背後，都有一個能讓罪犯藏身並持續運作的基礎設施。

然而，對網絡罪犯而言，維持隱蔽行蹤日漸困難。各國政府、執法機構與私營部門的全球協作，令罪犯難以在網上保持匿名。更關鍵的是，能夠獨立管理及維護安全基礎設施的網絡罪犯非常少。因此，他們轉向尋求非法基礎設施供應商代為提供服務，使其能專注於鎖定目標與牟利。

「網絡犯罪即服務」正是指專門為各類惡意網絡攻擊者提供支援的地下市場。該市場提供不斷擴充且演變的工具、服務與情報，協助罪犯侵害網絡目標。潛在犯罪者能購買網絡存取權限、規避安全措施的工具，以及用於竊取個人資料的惡意軟件。「防彈主機」（BPH）供應商正是此生態圈一環，專門為罪犯提供安全基礎設施。值得注意的是，單一BPH供應商便能直接助長數百名罪犯跨境犯案。

何謂「防彈」主機服務供應商？

簡言之，BPH供應商向罪犯出租虛擬及/或實體運作基礎設施。BPH供應商屬於特殊類別的網絡基建服務，專為惡意行為者（包括網絡罪犯）提供在網絡上寄存非法內容及進行活動。

所謂「防彈」實為營銷話術。實際上，這些服務與其他基礎設施一樣，都可能受到打擊和干擾。但不同的是，BPH　服務商會拒絕配合執法機構的內容移除要求，並無視受害者的投訴與訂閱者舉報。這意味罪犯能放心進行通訊、運作非法論壇與網站、發動惡意軟件與釣魚攻擊，以及洗黑錢，無需擔心服務商因執法要求終止服務。

BPH供應商實質上是明知故犯地參與網絡犯罪生態，助長嚴重的金融網絡犯罪。澳洲多宗對企業及其客戶造成影響的重大網絡安全事故，皆因罪犯利用BPH服務所致。這些事故的後果包括破壞性勒索軟件攻擊、數據勒索及敏感資料竊取。

地下論壇的
BPH服務廣告範例：

BPH供應商如何運作?

不同BPH供應商的商業模式各異。最常見手法是向罪犯客戶出租IP位址，並運用複雜網絡轉換技術隱藏其位置、身份與活動。很多時候，BPH供應商會從合法主機服務商、數據中心或網絡服務供應商（ISP）轉售或租賃IP位址與伺服器。這些「上游」供應商可能並不知情，未有察覺他們的資源最終被用來支援 BPH 服務商，進而服務「下游」的網絡罪犯。

BPH供應商會刻意配置網絡與系統架構，令調查人員更難追蹤其客戶的身份。例如，他們經常更換客戶活動所使用的外部識別碼，例如指定的 IP 位址和域名。此類手法使防禦者與調查人員難以即時將攻擊事件與特定IP位址連結。此外，BPH供應商多選用網絡管制寬鬆國家的基建。這些地區對惡意網絡活動的調查與防制措施往往缺位或鬆散。

防彈主機供應商與合法基建供應商有何區別?

打擊BPH供應商如何影響網絡犯罪威脅

BPH供應商提供了一次性瓦解數百至數千名罪犯的關鍵機會。各類網絡罪犯和其他惡意網路行為者使用此類服務來降低犯罪難度，深信他們的活動能夠在面對下架或投訴要求時繼續隱密且不受干擾。

然而，執法機關、政府部門與私營機構正透過協作鎖定並瓦解這些非法基建供應商，包括主動封鎖已知BPH供應商的網絡流量等防禦措施。這些行動有效減少澳洲及盟國網絡遭遇的網絡犯罪，其中包括哪些在不知情的情況下為BPH供應商提供網絡存取並為網路犯罪分子提供安全的基礎設施的合法「上游」基建供應商與ISP。

雖然 BPH 並非「網絡犯罪即服務」生態中唯一的基礎設施供應者類型。但這些服務透過積極支援犯罪活動與蓄意阻撓合法調查，持續助長對澳洲的網絡威脅。針對BPH供應商的行動，正暴露此類服務及其用戶的脆弱本質。