◎資訊安全宣導

—公務機關遭中國駭客攻擊，破口在供應商—

調查局發現大陸駭客組織長期駭入承接政府機關資訊服務的供應商，再伺機發動攻擊，初步已發現六個政府單位及四家資訊服務供應商受害，成立專案小組，全面清查駭客利用供應鏈在台網路攻擊行動。

包括經濟部投審會、水利署水資源局、台北市府市長室、國家地震工程中心、國立大學等六個政府單位陸續遭駭客入侵，竊取機敏資訊及民眾個資，溯源發現攻擊來自大陸的駭客組織，包括 MustangPanda、APT40 及 Blacktech 與 Taidoor。

調查局發現，承接政府標案的資訊服務供應商，因負責政府機關重要資訊系統的開發及維運，成為駭客主要攻擊目標，作為跳板攻擊政府機關，有四家資訊服務供應商被鎖定攻擊。調查局分析，駭客為了能以多途徑方式持續取得受駭單位內部網路控制權，也在受駭單位內部伺服器安裝ＶＰＮ連線軟體。

Blacktech 駭客組織活躍於東南亞地區，民眾未對設備進行更新或修改預設設定，就會被駭客利用，作為惡意程式中繼站，並以另一途徑攻擊國內資訊服務供應商或政府機關的對外服務網站、破解員工ＶＰＮ帳號密碼及寄送帶有惡意程式的釣魚郵件，成功滲透內部網路後，利用模組化惡意程式進行橫向移動。

調查局說，有證據顯示攻擊來自大陸湖北，部分受駭單位被查出有中共支持的 Taidoor 駭侵活動足跡。

【文章擷取-聯合報】

臺中榮民總醫院提醒你!也關心你!