【政風宣導-機關安全宣導】中國駭客組織對我國資訊供應鏈發動攻擊

廉政檢舉專線：0800-286-586

調查局近來偵辦數起我政府機關遭駭案件，調查過程中發現中國駭客組織 Blacktech 與 Taidoor，已長期滲透國內政府機關及其資訊服務供應商，尤其是承接政府標案之資訊服務供應商，因其負責政府機關重要資訊系統之開發及維運，故成為駭客主要攻擊目標，作為跳板攻擊政府機關，試圖竊取機敏資訊及民眾個人資料。為全面清查中國駭客組織利用供應鏈在臺灣網路攻擊活動及遏止我國政府機關持續受駭，調查局成立專案小組積極偵辦。

調查發現，中國駭客組織深知政府機關為求便利，常提供遠端連線桌面、VPN 登入等機制，提供委外資訊服務廠商進行遠端操作與維運，由於國內廠商大多缺乏資安意識與吝於投入資安防護設備，亦未配置資安人員，故形成資安破口，以 Blacktech 駭客組織為例，該集團主要活動於東南亞地區，駭客先鎖定國內存在尚未修補之 CVE 漏洞的網路路由器設備，因多數民眾未對設備做韌體更新或修改預設設定，故遭駭客利用此 CVE 弱點取得該路由器控制權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之對外服務網站、破解員工 VPN 帳號密碼及寄送帶有惡意程式之釣魚郵件等，成功滲透內部網路後，利用模組化惡意程式進行橫向移動，本局經分析惡意程式為 Waterbear 後門程式，受感染電腦會向中繼站報到並以加密連線的方式傳送竊取資訊；另外，駭客為能以多途徑方式持續取得受駭單位內部網路控制權，亦在受駭單位內部伺服器安裝 VPN 連線軟體，如 SoftEtherVPN，其亦可以被利用來對外向其他單位進行攻擊或存取網頁型後門(Webshell)進行竊資。

Waterbear 後門程式係為中共背後支持的中國駭客組織 Blacktech 近年常用之惡意程式，並有證據支持其攻擊來源來自中國湖北，另在受駭公司發現另一中共支持的中國駭客組織 Taidoor 的駭侵活動足跡，顯見 Blacktech 及 Taidoor 正透過供應鏈攻擊我政府機關，值得社會大眾注意，

並請各政府單位與企業組織協助注偵內部可疑的網駭活動，並建議委外系統維護不提供遠端操作或是使用多因子認證方式，以降低被駭客入侵之風險。

以上內容轉載自調查局網站

https://www.mjib.gov.tw/news/Details/1/624

109.11.

新北市八里區公所政風室關心您