國家資通安全會報 技術服務中心
漏洞/資安訊息警訊

發布編號	ICST-ANA-2012-0005	發布時間	2012/07/02
事故類型	攻擊活動預警	發現時間	2012/07/02
通告名稱	DNS Changer 活動警訊通知		
內容說明	技服中心接獲外部情資，表示美國聯邦調查局(FBI)於100年11月8日執行「Ghost Click行動」，該行動係破獲從事網路犯罪行為DNSChanger集團。使用者若遭DNSChanger惡意程式感染，將修改電腦或路由器的DNS設定，指向犯罪集團所架設之DNS主機，可能導致使用者連至錯誤的網站或植入其他惡意程式。 FBI於破案後，透過提供正常DNS伺服器取代該網路犯罪集團的伺服器，讓感染DNS Changer的電腦可以正常運作，惟此DNS伺服器預計將於101年7月9日關閉，可能造成使用者無法上網之情形。 檢查是否已遭DNSChanger惡意程式感染，可透過檢視DNS設定方式(確認DNS是否遭修改為以下惡意DNS IP列表)，或至通報應變網站下載DNS Changer檢測軟體(網址為 https://www.ncert.nat.gov.tw/1.jsp?url=1-main-doc.jsp)，檢測上網電腦是否感染DNS Changer，以免遭感染電腦所使用的DNS伺服器產生無法上網的情形。 如發現遭植入DNSChanger惡意程式，請盡速清除DNSChanger惡意程式，並依通報應變作業程序，至通報應變網站執行通報作業。 惡意DNS IP列表： 85.255.112.0-85.255.127.255 67.210.0.0-67.210.15.255 93.188.160.0-93.188.167.255 213.109.64.0-213.109.79.255 64.28.176.0-64.28.191.255		

影響平台	所有平台
影響等級	中
建議措施	1.請至通報應網站下載檢測程式(https://www.ncert.nat.gov.tw/1.jsp?url=1-main-doc.jsp)，確認是否遭感染 DNS Changer。 2.若確認該資訊設備已遭入侵，建議可以使用免費軟體移除 DNSChanger 惡意程式(請參考http://www.cib.gov.tw/news/news01_2.aspx?no=3571)，亦建議更換系統使用者之相關密碼，並至通報應變網站執行通報作業。若暫時未發現異常行為，建議持續觀察一個星期左右。 3.注意個別系統之安全修補，包含作業系統與辦公室常用文書處理軟體，若僅移除惡意程式而不修補，再次受相同或類似攻擊的機率極高。修補程式須持續更新，Windows 自動安裝更新程式機制可參考微軟資訊安全錦囊。Linux 系統可使用 yum 或 apt 等更新機制。若您所使用的作業系統已不再提供更新程式，建議升級至較新版本作業系統。 4.教育使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔，以防被植入後門程式。
參考資料	刑事局呼籲民眾檢查個人電腦是否感染 DNSChanger http://www.cib.gov.tw/news/news01_2.aspx?no=3571 DNS Working Group http://www.dcwg.org/