

聰明防 詐騙



反詐騙專線: **165**

報案專線: **110**

臺中市政府警察局網址/

www.police.taichung.gov.tw



預防犯罪宣導—最新治安訊息

案例



警方呼籲民眾檢查個人電腦是否感染 DNSChanger

美國聯邦調查局(FBI)於日前執行「Ghost Click 行動」，查緝從事犯罪行為之 ROVE DIGITAL 公司涉及網路惡意軟體攻擊、垃圾郵件攻擊、伺服器攻擊或分散式阻斷服務攻擊等網路犯罪行為。

刑事局國際科接獲美國聯邦調查局通報，上述 R 公司之近 4 百萬個分布於 240 個國家及地區所註冊之 IP，其中發現計逾 3 千多筆係屬於我國內註冊之網路服務提供者「ISP」之可能受感染 IP 資料，我國潛在被害者疑似包括我國電信業者及眾多學術網路使用者等。

該集團利用綁架電腦或路由器的 DNS 設定，藉由顯示廣告以賺取不法收入超過 1400 萬美元。美國 500 大企業有一半的企業遭感染，總計全球各地共約有上百萬台電腦遭到感染。惟本案係該集團透過竄改電腦路由 DNS 設定以獲取不法廣告收益模式，而截至目前為止本案尚未發現有個資外洩情形，請民眾無須恐慌。

依據 FBI 所提供資料，我國有許多電腦亦遭受 DNS Change 感染，可能造成使用者無法上網之情形。

民眾自我檢測及排除步驟：

刑事局特別研發與設計 DNS Changer 檢測軟體(DNS Checker)，提供民眾自動分析電腦是否遭 DNS Changer 感染，並提供遭感染電腦重新設定 DNS 之方式。

(連結網址如下：http://www.cib.gov.tw/news/news01_2.aspx?no=3571)。

民眾個人可於 7 月 9 日前依上述連結所示步驟，自行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。



反詐騙小叮嚀：

警方呼籲：請民眾加強個人電腦防護工作，若您的電腦已遭受 DNS Changer 感染，建議您可以使用下列免費軟體移除 DNS Changer 及相關資安威脅。

軟體名稱 **Hitman Pro (32bit and 64bit versions)**

網址 <http://www.surfright.nl/en/products/>

軟體名稱 **Kaspersky Labs TDSSKiller**

網址 <http://support.kaspersky.com/faq/?qid=208283363>

軟體名稱 **McAfee Stinger**

網址 <http://www.mcafee.com/us/downloads/free-tools/stinger.aspx>

上列軟體係由 <http://www.dcwg.org> 整理提供

臺中市政府警察局



關心您

