TLP:WHITE

家用路由器安全風險與防護建議

Announcement Advisory Report (ANAR)

2018-06-05

TWCERTCC-ANAR-2018006

Summary

- 隨著物聯網設備的普及，越來越多的智慧型連網設備被應用於家庭生活上，造成家用路由器連接網際網路使用需求的倍增，家用路由器因此也成為駭客攻擊的主要目標。
- 家用路由器設備供應商應鼓勵漏洞通報，並積極修補漏洞外，使用者也應該注重並落實家用路由器的安全設定、預設帳號密碼修改及軟韌體版本更新，以避免家用路由器遭攻擊造成敏感資訊外洩，並進一步遭利用成為殭屍網路的一員。
- 使用者應關注資安新聞與設備商之漏洞通報，當有發生相關資安攻擊事件時，應儘速檢查其路由器設定是否遭竄改，如其網域名稱系統(DNS)設定，若遭竄改為非預期之設定，應立即修正。

Description

近來全球發生數萬起家用路由器遭駭客攻擊事件：駭客入侵路由器並竄改網域名稱系統設定(DNS)，將使用者網路連線導至惡意網站，並誘導 Android 系統使用者下載惡意程式，竊取其銀行帳戶、手機通聯紀錄等敏感資訊，該事件以南韓、日本、中國、香港及台灣等亞洲地區國家為主要攻擊目標[1][2]。2018 年 5 月，台灣居易科技公司(DrayTek)所生產的路由器弱點被揭露[3]，導致用戶的 DNS 設定遭駭客竄改，並將連接該路由器用戶的網址導向惡意伺服器，使駭客得以用釣魚網站蒐集用戶的資訊，受影響的家用路由器超過 25 款；同月 Cisco 公司亦發現專門攻擊家用路由器及網路儲存設備的 VPNFilter 病毒，影響超過 50 萬個網路裝置[4]，顯見駭客已鎖定家用路由器進行攻擊。

卡巴斯基實驗室研究人員在2018年第一季的APT攻擊趨勢報告[5]中表示，家用路由器已成為駭客愈來愈常攻擊的標的。2018 年 3 月起，趨勢科技與卡巴斯基分別不約而同地偵測到了因家用路由器遭駭侵並導致使用者行動裝置遭植入惡意 APP 之攻擊案例(趨勢科技命名為 XLoader、卡巴斯基命名為 Roaming Mantis、行政院國家資通安全辦公室技術服務中心命名為少爺[6])，其攻擊手法皆為竄改使用者家用路由器之 DNS 設定，當使用者以行動裝置連接該受駭路由器上網時，會將使用者連線導到惡意伺服器，並誘騙使用者下載安裝惡意 APP 程式，如圖 1 所示。

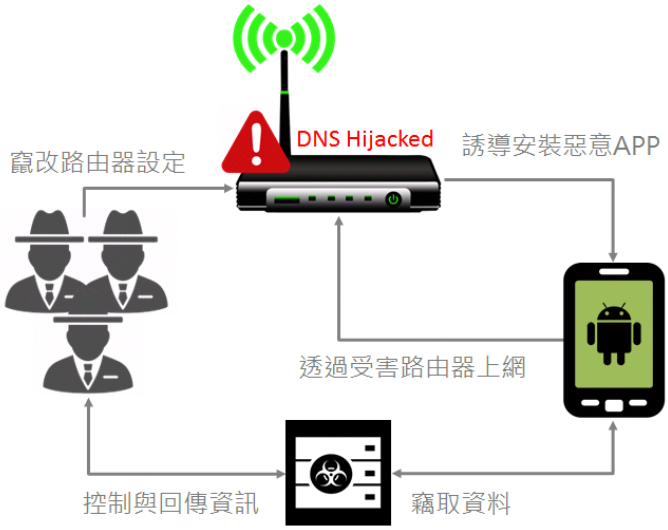


圖 1. 劫持家用路由器的駭侵手法

駭客成功入侵一般家用路由器後，會竄改路由器的 DNS 設定。一旦有使用者之行動裝置透過該受駭路由器上網，將會出現提示視窗誘導使用者於行動裝置上安裝應用程式。為了增加行動裝置惡意程式的安裝率，駭客會利用使用者正在瀏覽的網頁，結合「請安裝 Facebook 擴展工具包提升安全性及流暢性」或「請安裝最新版 Chrome 應用程式以提升安全性及流暢性」等有關安全與效能的重要文字，來取信使用者。

例如當使用者正在瀏覽 securelist.com 網站時，會跳出提示視窗「securelist.com says: To better experience the browsing, update to the latest chrome version.」，讓使用者誤認為是原廠網站對用戶系統效能與安全提升的建議，便進行下載與安裝。取信使用者的內容支援多達 27 種語言，包含英文、日文及正體中文等，如圖 2、圖 3 所示。

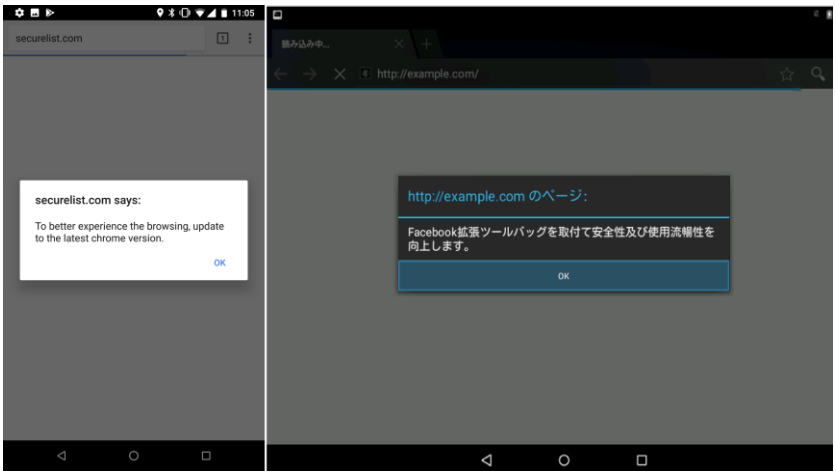


圖 2. 誘導使用者安裝 APP 更新之英文、日文版提示視窗

圖 3. 誘導使用者安裝 APP 更新之正體中文版提示視窗

駭客所提供的 chrome.apk 或 facebook.apk 行動裝置惡意程式，將於安裝時要求 SMS 簡訊、通聯紀錄、網路、錄音功能及外部儲存裝置等存取權限。

除了竊取行動裝置用戶的資訊外，該惡意程式在開啟時亦會利用詐騙方式盜取受害者帳號密碼。當裝置被喚醒時將跳出「Google 帳號危險 認證後使用」的提示視窗，在使用者點擊確認後，會啟動瀏覽器開啟釣魚網頁誘騙使用者輸入姓名、生日與身分證號，如圖 4 所示。

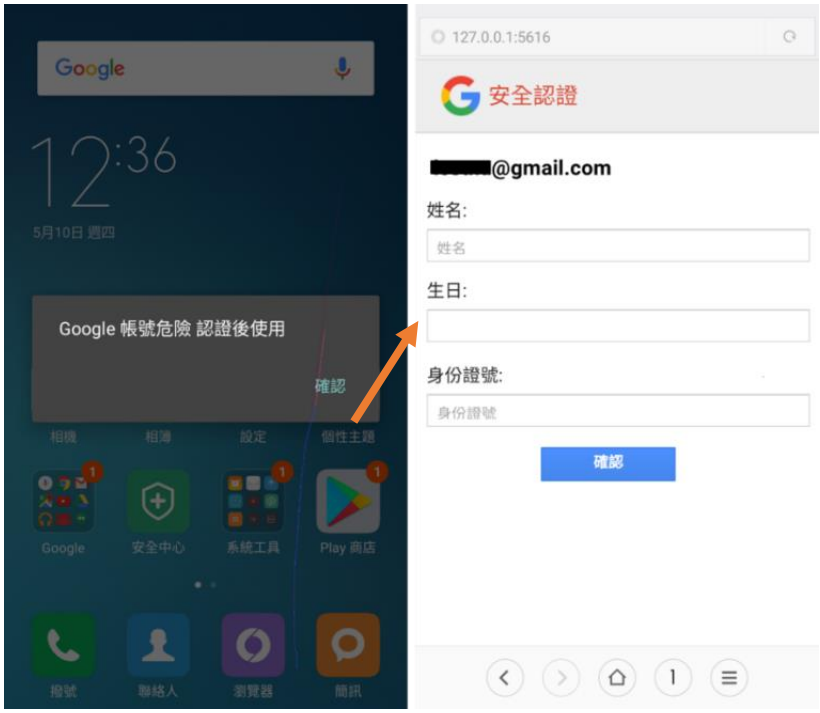
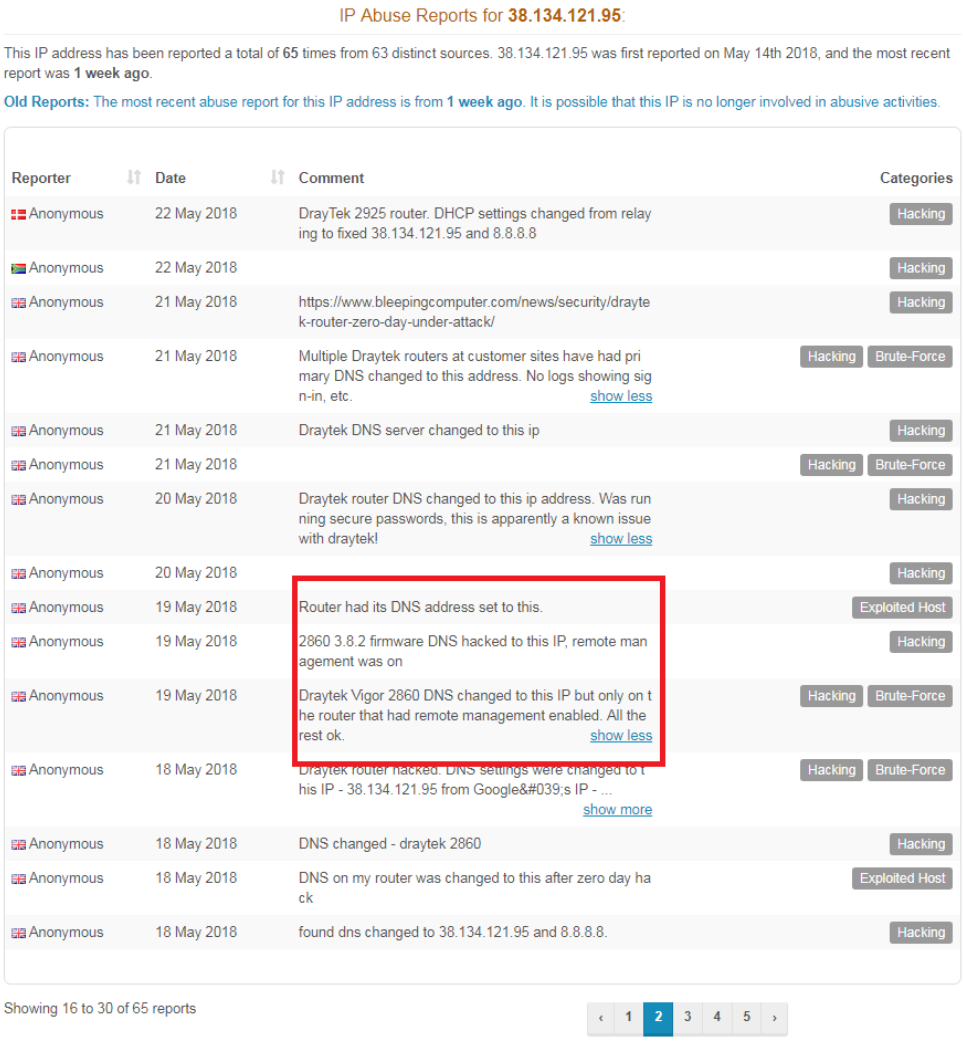


圖 4. 駭客偽冒 Goolge 安全認證網站騙取使用者資料

無獨有偶，2018 年 5 月開始有歐洲用戶投訴台灣居易科技(DrayTek)所生產

的路由器，其 DNS 伺服器位址無故遭設定為 38.134.121[.]95，而提供檢測惡意 IP 及網域之 AbusedIPDB 組織亦陸續於 5 月 14 日起收到 65 次 DNS 位址遭竄改的通報[7]，並將此 IP 列為惡意的 DNS 網域，如圖 5 所示。



IP Abuse Reports for **38.134.121.95**:

This IP address has been reported a total of **65** times from 63 distinct sources. 38.134.121.95 was first reported on May 14th 2018, and the most recent report was **1 week ago**.

Old Reports: The most recent abuse report for this IP address is from **1 week ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	Date	Comment	Categories
Anonymous	22 May 2018	DrayTek 2925 router. DHCP settings changed from relay ing to fixed 38.134.121.95 and 8.8.8.8	Hacking
Anonymous	22 May 2018		Hacking
Anonymous	21 May 2018	https://www.bleepingcomputer.com/news/security/drayte k-router-zero-day-under-attack/	Hacking
Anonymous	21 May 2018	Multiple Draytek routers at customer sites have had pri mary DNS changed to this address. No logs showing sig n-in, etc. show less	Hacking Brute-Force
Anonymous	21 May 2018	Draytek DNS server changed to this ip	Hacking
Anonymous	21 May 2018		Hacking Brute-Force
Anonymous	20 May 2018	Draytek router DNS changed to this ip address. Was run ning secure passwords, this is apparently a known issue with draytek! show less	Hacking
Anonymous	20 May 2018		Hacking
Anonymous	19 May 2018	Router had its DNS address set to this.	Exploited Host
Anonymous	19 May 2018	2860 3.8.2 firmware DNS hacked to this IP, remote man agement was on	Hacking
Anonymous	19 May 2018	Draytek Vigor 2860 DNS changed to this IP but only on t he router that had remote management enabled. All the rest ok. show less	Hacking Brute-Force
Anonymous	18 May 2018	Draytek router hacked. DNS settings were changed to t his IP - 38.134.121.95 from Google's IP - ... show more	Hacking Brute-Force
Anonymous	18 May 2018	DNS changed - draytek 2860	Hacking
Anonymous	18 May 2018	DNS on my router was changed to this after zero day ha ck	Exploited Host
Anonymous	18 May 2018	found dns changed to 38.134.121.95 and 8.8.8.8.	Hacking

Showing 16 to 30 of 65 reports

‹ 1 2 3 4 5 ›

圖 5. 網路設備之 DNS 位址無故遭設定為 38.134.121[.]195

居易科技已證實韌體存在弱點，讓駭客有機會竄改路由器的 DNS 設定，但該弱點細節並未公開。該事件受影響的路由器超過 25 款，為此居易科技 5 月 18 日緊急發布安全更新通知[3]，並建議用戶主動檢查路由器之 DNS 設定、啟用 TLS 1.2 的加密連線及關閉遠端管理者存取權限，在此 TWCERT/CC 呼籲使用者應儘速檢查並安裝最新版軟韌體。

除了駭客劫持路由器並竄改 DNS 設定的駭侵手法外，Cisco 旗下的威脅情報組織 Talos 在 2018 年 5 月 23 日及 6 月 6 日的研究中[4][8]，揭露了 VPNFilter 惡意程式，發現該惡意程式已攻擊全球 54 個國家並影響超過 50 萬個裝置，包含 Linksys、MikroTik、NETGEAR、ASUS、D-Link、中興、華為與 TP-Link 等品

牌的路由器，以及 QNAP 網路儲存裝置。

多數家用路由器都是採用嵌入式的 Linux 平台，並配備精簡版的 Unix 程式套件 BusyBox。研究人員從目前受駭狀況推測，駭客係透過掃描網路上使用 BusyBox 的裝置，檢測其是否開啟 Telnet 或 SSH 之遠端控制服務，再暴力破解路由器密碼成功後植入 VPNFilter。遭植入 VPNFilter 裝備會連到 Photobucket[.]com 或 ToKnowAll[.]com 下載變造過的圖檔來取得 C&C 伺服器 IP 位址，成功連上 C&C 後會下載其他監控程式。不同於其他物聯網裝置惡意程式(例如 Mirai)，VPNFilter 會修改家用路由器之非揮發性記憶體(Non-Volatile Memory)內容，並透過 Linux 的排程指令 crontab 將 VPNFilter 加入到例行性工作排程中，達到常駐於家用路由器的目的。因此，即便使用者將路由器重新開機，仍無法將惡意程式完全移除。

若路由器遭植入 VPNFilter 惡意程式，與其連接的網路流量都將遭受監控進而造成連網資料外洩，例如使用者之帳號、密碼或銀行帳戶等敏感資訊。目前美國聯邦調查局(FBI)已取得美國法院的命令，將存取 ToKnowAll[.]com 等惡意網域名稱的連線都導入 sinkhole，以阻絕受駭裝置與駭客的聯繫管道[9]。

TWCERT/CC 提醒，隨著越來越多物聯網裝置應用在日常生活中，相關的使用與控制皆是透過家用路由器來連接網際網路，家用路由器已成為駭客的主要攻擊對象。使用者必須了解家用路由器和相關物聯網設備連接網際網路所可能帶來的資安風險，物聯網設備所帶來的便利性與安全性才能兼顧。

Recommendations

針對近期家用路由器遭駭侵事件，TWCERT/CC 提出以下 7 項防護建議：

1. 選擇安全可靠的路由器廠牌，並隨時關注相關資安新聞，及即時更新原廠發布之軟、韌體，以封鎖駭客對已知漏洞攻擊的管道。

2. 修改家用路由器預設帳號及密碼，且應避免使用 admin、12345678 或 password 等容易猜測的弱密碼組合，建議使用混合英文、數字及符號，並且超過 8 個字元長度的強密碼。

3. 使用者應參考原廠路由器說明書，隨時檢視家用路由器(以 Asus WL-500gP V2 為例)之 DNS 伺服器 1 與 DNS 伺服器 2 之設定是否遭竄改(如圖 6 所示)，若遭竄改為非預期之設定(例如被改為

38.134.121[.]95)，應立即修正。台灣常使用的 DNS 伺服器為中華電信 (168.95.192[.]1、168.95.1[.]1) 或 Google 提供之 Public DNS (8.8.8[.]8、8.8.4[.]4) 。

圖 6. 確認家用路由器之 DNS 設定

4. 為防止駭客透過路由器遠端進入使用者的網路，應停用路由器內不必要的功能，例如通用隨插即用(UPnP)、WPS、Telnet/SSH 遠端管理功能，並限制 WEB 遠端管理的連線 IP。

5. 啟用家用路由器(以 Asus WL-500gP V2 為例)之防火牆基本防護功能(如圖 7 所示)。

圖 7. 啟用家用路由器之防火牆功能

6. 若要防止惡意程式(例如 VPNFilter)常駐於路由器中，使用者可將家用路由器重置/回復出廠設定，再進行安全設定與更新。系統重置通常可以使用迴紋針或類似物品，按壓設備上的「reset」標示按鈕五至十秒鐘，以完成此動作。須注意系統重置會導致設備所有的使用者設定都將消失。

7. 家用路由器設備供應商應鼓勵漏洞通報，積極修補其產品的資安漏洞，並即時進行產品漏洞揭露，讓使用者掌握所用設備的資安風險，以維護品牌形象及商譽。

References

[1] Kaspersky Lab. (2018, April 16). "Roaming Mantis uses DNS hijacking to infect Android smartphones", Retrieved June 7, 2018, from the World Wide Web: https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

[2] Trend Micro. (2018, April 17). "XLoader Android Spyware and Banking Trojan Distributed via DNS Spoofing", Retrieved June 7, 2018, from the World Wide Web: https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-and

roid-spyware-and-banking-trojan-distributed-via-dns-spoofing/

[3] Dray Tek. (2018, May 18). "Notification of Urgent Security Updates to DrayTek routers", Retrieved June 7, 2018, from the World Wide Web: https://www.draytek.com/en/about/news/2018/notification-of-urgent-security-updates-to-draytek-routers

[4] Talos. (2018, May 23). "New VPNFilter malware targets at least 500K networking devices worldwide", Retrieved June 7, 2018, from the World Wide Web: https://blog.talosintelligence.com/2018/05/VPNFilter.html

[5] Kaspersky Lab. (2018, April 12). "APT Trends report Q1 2018", Retrieved June 7, 2018, from the World Wide Web: https://securelist.com/apt-trends-report-q1-2018/85280/

[6] 行政院國家資通安全會報技術服務中心. (2018, June 7). "14 萬韓製路由器與行動裝置遭少爺駭客掌控", Retrieved June 7, 2018, from the World Wide Web: https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=en&RSSType=news&seq=16110

[7] AbuseIPDB. "IP Abuse Reports for 38.134.121.95", Retrieved June 7, 2018, from the World Wide Web: https://www.abuseipdb.com/check/38.134.121.95

[8] Talos. (2018, June 6). "VPNFilter Update - VPNFilter exploits endpoints, targets new devices", Retrieved June 7, 2018, from the World Wide Web: https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

[9] The New York Times. (2018, May 27). "F.B.I.'s Urgent Request: Reboot Your Router to Stop Russia-Linked Malware", Retrieved June 7, 2018, from the World Wide Web: https://www.nytimes.com/2018/05/27/technology/router-fbi-reboot-malware.html