物聯網的資訊安全

驊達科技 程正孚整理

物聯網（IoT）裝置的安全一直是一項熱門討論話題，其中IP監視攝影機的安全尤其受到矚目。2020年初始，全台灣發生多起網路駭客攻擊，引發業界議論紛紛。這波攻擊的目標主要是網路攝影機，廠牌不分台灣或大陸，設備不管是錄放影主機或是監視器等監控系統，都發現不正常的流量暴衝，導致用戶端的網路異常，影響多達10萬設備與用戶，包括一般消費者住家網路、超商監視器或是商辦空間都傳出災情。許多品牌業者和代理商均發出聲明，呼籲用戶盡快升級更新韌體，緩解或阻斷攻擊。

不管是DDoS（Distributed Denial of Service）分散式阻斷服務，或植入殭屍病毒程式，都是常見的癱瘓式攻擊，除了狂丟訊號封包導致尖峰流量暴漲、影響網路正常效能之外，更使得攝影機用戶暴露在個資洩漏、影像外流，甚至成為國際駭客的攻擊跳板而不自知。像這類的攻擊非常頻繁，特別是在IoT物聯網時代，任何連網設備都可能成為攻擊的目標。

家裡如果有裝監視器，要留意一下自家「其他設備網路」是否變慢了！監視器主機用戶「被駭客入侵」，透過有網路連線的監視器主機，不斷丟檔案上傳，藉此癱瘓使用者的網路，發現監視器不能遠端連線了，發覺怎麼自家網路變慢，查問後才知道問題出在監視器上！「不管是防盜，保全或是居家照護，很多人會像這樣，透過監視器來多一層保障，但現在監視器竟然也變成，駭客攻擊的主要目標！」「他就不斷轉圈圈（遠端要看的話）就連線失敗。」

類似這樣，遠端看不到自家監視器畫面，不管MADE IN TAIWAN台產或大陸製，許多主機都被入侵，甚至有超商監視器也被駭！但更多人沒發現自家監視器主機出問題，直到家用網路動不了，才去查原因。「有一些它不是店家，它可能家裡面，有很多其他的網路設備，它會造成說，它的監視器中毒了，導致他們家的網路被癱瘓掉了。」

追查發現，駭客IP來自荷蘭、東歐和中南美等境外區域，駭入台灣監視器主機，植入惡意程式，這裡當跳板，再不斷朝大陸等地，不斷丟出錯誤封包，意思就是上傳大量檔案，藉此讓你家網路變慢甚至中斷。針對數位錄放影機受到網路攻擊，相關原始廠商已經開啟強力救援模式，加派人力更新軟體解決困境！

DVR駭客風暴，起因於IoT/Linux的"Tsunami"僵屍網路新變體Amnesia病毒，僵屍網路是一種目前發現的較新的僵屍網路，它允許攻擊者利用未修補的遠端代碼執行漏洞攻擊其錄影設備DVR。該漏洞就被安全研究人員在DVR設備中被發現，此次波及了

全球70多家的供應商品牌。全球有超過22萬台設備受影響，而臺灣、美國、以色列、土耳其和印度為主要分佈區。

因此為有效避免DVR主機受到網路駭客DDoS攻擊的方法：

1. 升級DVR到最新韌體
2. 將雲服務關閉
3. 密碼建議設定英文與數字混合
4. 不要使用主機預設TCP PORT，例如將34567改成2950

IP攝影機目前已是駭客優先鎖定的攻擊目標，因為這類裝置的運算效能和網路頻寬都較為充裕。眼前最好的例子就是2016年底一個名為「Mirai」的殭屍網路病毒利用監視攝影機發動了有史以來最大的一樁分散式阻斷服務（DDoS）攻擊。結果造成網際網路流量瞬間暴增至平常的50倍，創下1.2Tbps的歷史新高。而這些網路流量都是因為IP監視攝影機遭到駭客挾持，駭客從遠端下達攻擊指令所造成。

發現又出現了多個類似Mirai的惡意程式變種，且更善加利用這些含有漏洞的IP監視攝影機。當然，網路資安現已成為IP監視攝影機的首要問題，某些政府機構也開始著手制定一些規範來要求這類裝置提升其網路資安能力。這勢必將成為IP監視攝影機市場一項新的競爭要素。

歹徒攻擊IP監視攝影機的背後動機

歹徒駭入IoT裝置的主要動機是為了賺錢。IP監視攝影機之所以成為歹徒的重要目標，有以下幾點原因：

1. 無時無刻的網路連線。如同許多其他裝置一樣，IP攝影機必須仰賴網際網路連線來運作。然而也因為隨時暴露在網際網路上，因此駭客很容易找到這些攝影機並攻擊其裝置漏洞。這些裝置一旦被駭入，就會成為駭客的工具。
2. 駭客投入的成本低廉。與駭入 PC 不同的是，駭客一旦找到方法來破解某種IoT裝置的安全機制（例如IP攝影機），同樣的方法就可以套用在類似的型號上，所以每一裝置的駭入成本相當低廉。
3. 缺乏監督管理。有別於一般 PC（尤其是辦公室環境的 PC），IP攝影機通常不太需要使用者操作，而且缺乏安全控管，還不能在上面安裝市售惡意程式防護軟體。
4. 充裕的效能。IP攝影機平常閒置的運算效能通常就足以執行一些駭客想要的工作（例如挖礦）而不會引起使用者注意。
5. 充裕的網際網路頻寬。IP攝影機需要傳輸視訊，因此需要隨時、高速、高頻寬的連線，正好成為歹徒發動DDoS攻擊的良好條件。

典型感染過程

IP監視攝影機遭駭的典型過程如下：

1. 初次感染。駭客會先搜尋裝置是否開放了某些連接埠，如Telnet、Secure Shell以及Universal Plug and Play（UPnP）所使用的連接埠。接著，便利用裝置預設的帳號密碼來試圖登入裝置（這就是 Mirai 的作法），或者攻擊尚未修補的系統漏洞（這就是 Persirai 和 Reaper 的作法），進而掌控裝置。
2. 幕後操縱。在掌控裝置之後，駭客就會下

載一些惡意腳本或惡意程式到裝置上執行，讓裝置向幕後操縱（C&C）伺服器回報。接著，伺服器會發送指令給被入侵的IP攝影機來執行一些不法活動，例如：加密虛擬貨幣挖礦，或者利用UDP洪水攻擊對特定目標發動阻斷服務攻擊。

3. 繁衍散布。視惡意程式而定，惡意程式可能會掃瞄網路上是否有可感染的裝置，然後利用相同手法將自己植入其他含有漏洞的裝置。此過程有可能自動執行（例如一些具備蠕蟲能力的殭屍網路病毒）或者由駭客手動從C&C伺服器下達指令。

IP攝影機的層層防禦

1. IP攝影機硬體。駭客要能入侵IP攝影機，最重要的關鍵就是找到系統的漏洞，因此IP攝影機製造商無不努力監控其產品韌體是否出現任何漏洞並盡速修補。然而除此之外，廠商還可採取一些作法來進一步強化整體安全性，例如：
   - 強制使用者變更預設密碼。
   - 利用安全開機功能不讓已遭入侵的裝置運作。
   - 加入韌體無線更新（FOTA）功能，必要時可方便修補韌體。
   - 採取最少功能原則，非必要的連接埠盡量不要開放。
2. 網路。將IP攝影機部署在封閉式網路內，已經是一種確保裝置安全相當普遍的作法。此外還可透過虛擬私人網路（VPN）連線來確保遠端存取的安全。其他網路相關的安全機制還有：
   - 採用加密連線來防止遭到入侵。
   - 經由安全通道來連線。
   - 將加密金鑰儲存在硬體上。
3. 雲端。雲端服務所提供的功能越多，雲端安全就越形重要。好處是，許多服務廠商（即使不是全部）都已認知到這點。大部分主流的服務廠商，其雲端基礎架構都有充分的安全防護。此外，密切整合的資安防護產品（如趨勢科技產品）也是雲端防護的重要一環。

到2020年，新部署的IoT裝置預期將增加12億。這是一個令人吃驚的數字。現在已有連網洗碗機、烤箱、麵包機、冰箱和咖啡機；無人機將有它們自己的領空，用於遞送包裹和監視服務。未來將有更多攝影機監視交通、行人、大樓和住家。一些特定商店將變成完全自動化和自動結帳，例如舊金山Standard Market17利用保全攝影機監看客戶挑選的商品，然後自動扣款。該公司估計，這項技術到2020年時將每月增加一百個店面。

最容易受感染的IoT裝置，以它們參與殭屍網路活動的數量為依據，發現是家用路由器，其次是IP網路攝影機、DVR和閉路電視。

最常見的攻擊類型是DDoS，然而，攻擊者在2018年轉移到多用途攻擊殭屍，提供DDoS和其他許多類型的攻擊，包括安裝Proxy伺服器以發動任何攻擊、挖礦劫持、安裝Tor節點、封包嗅探器（Packet Sniffer）、發動PDoS攻擊、DNS劫持、帳密收集、帳密填充與詐欺木馬等。

攻擊者發現，最終使用惡意軟體並感染IoT裝置的最常見手法是透過全球Internet掃描，搜尋開啟的Telnet遠程終端連接服務，包括IoT裝置製造商的特定HNAP、UPnP、SOAP和CVE，以及一些TCP埠。

最令人關切的是，IoT基礎設施就如同IoT裝置本身一樣很容易被攻擊者利用脆弱的帳密發動認證攻擊。

F5 Labs最近與資料夥伴Loryka合作，以行動網路IoT裝置為對象展開調查，結果發現行動網路IoT閘道就如同傳統有線和無線IoT裝置一樣脆弱。事實上，62%受測裝置容易遭受攻擊者利用廠商預設的脆弱帳密發動遠端存取攻擊。這些裝置當成Out-of-band網路，建立網路後門，並已在全球廣泛使用。

最易遭受攻擊的十個IoT埠

從IoT裝置最常使用的服務和通訊埠收集攻擊資料，以掌握全球IoT攻擊態勢。

表1為IoT裝置最易遭受攻擊的10個IT埠。SSH Port 22暴力攻擊是全球排名第一的攻擊類型，其次是Port 80 HTTP網路流量、Telnet、SIP Port 5060以及HTTP Port 8080，IoT裝置使用這所有埠。

表1 IoT裝置最易遭受攻擊的10個IT埠

Service	Port	IoT Device Type
SSH	Port 22	*Includes IoT
HTTP	Port 80	Mainly web apps but includes common IoT devices, ICS and gaming consoles
Telnet	Port 23	ALL
SIP	Port 5060	ALL VoIP phones, video conferencing
HTTP_Alt	Port 8080	SOHO routers, smart sprinklers, ICS
TR069	Port 7547	SOHO routers, gateways, CCTV
Applications	Port 8291	SOHO routers
Telnet	Port 2323	ALL
HTTP	Port 81	*Can include IoT: Wificams
SMTP	Port 25	*Can include IoT: Wificams, Game consoles

全球Mirai感染未曾歇止

要瓦解一個殭屍物聯網所面對的挑戰在於：很多遭感染的IoT裝置無法接受韌體更新、它們的所有人或運營者欠缺安全維護技術，或者設置在電信公司內部而電信公司對於更換或切斷連接的意願很低，因為那可能會同時中斷他們的服務。

自從Mirai原始碼被公開後，至少出現了10個變種，例如Annie、Satori/Okiru、Persirai、Masuta、PureMasuta、OMG、SORA、OWARI、Omni、Wicked。企業必須自我武裝以面對衝擊，因為IoT為攻擊者提供了無窮的機會，而且殭屍物聯網的構築現在非常普遍。預期在觀察中的IoT攻擊將建構新的殭屍物聯網，並且已發現的殭屍物聯網也會擴充規模。企業需要做好承受攻擊的準備，安全管控機制必須能夠偵測足以發動攻擊的殭屍網路與規模。在應用周邊建立殭屍網路防衛是很重要的，同時也必須擁有一個可延展的DDoS防護方案。 在達到任何有效的IoT安全保護之前，IoT裝置製造商或建置這些裝置的企業組織最終將面對實質的營收和成本風險。

參考：Securing IP Surveillance Cameras in the IoT Ecosystem
https:// www.netadmin.com.tw/netadmin/zh-tw/trend/25E36EEDDF6240159DEF3256C4EE218B