

家居智能裝置防護

趨勢科技顧問總監李浩然



大綱

- 智能家居裝置事故
- 家居智能化及危機
- 黑客階段性攻擊
- 智能家居裝置安全要點
- Q & A



智能家居裝置事故

智能家居裝置事故

變色慳電 Wifi LED燈泡

- 黑客利用產品漏洞，在30公呎外取得加密的密碼，破解後即可攔截利用此Wifi傳輸的資訊。



智能家居裝置事故

嬰兒監察器

- 黑客利用產品漏洞，將具備網路功能的嬰兒監視器變成竊聽裝置，讓任何人都可以聽到被監視的嬰兒（或屋內的談話）。
- 任何使用與嬰兒監視器相同技術的設備（即同一產品線上的任何產品）都可以被快速輕易地轉成竊聽設備。



智能家居裝置事故

兒童聊天洋娃娃

- “兒童聊天洋娃娃”可透過網絡連接來跟兒童聊天
- 由於“兒童聊天洋娃娃”需要與流動裝置配對、連網使用，所以黑客可以先入侵用戶的流動裝置，再取用娃娃的音響設備竊聽。
- 黑客可透過藍芽連線，在15公尺的範圍內竊聽孩子與娃娃之間的對話，甚至透過娃娃的麥克風和孩子說話。



家居智能化及危機

家居智能化

從前的家庭網絡



家居智能化

今日的家庭網絡



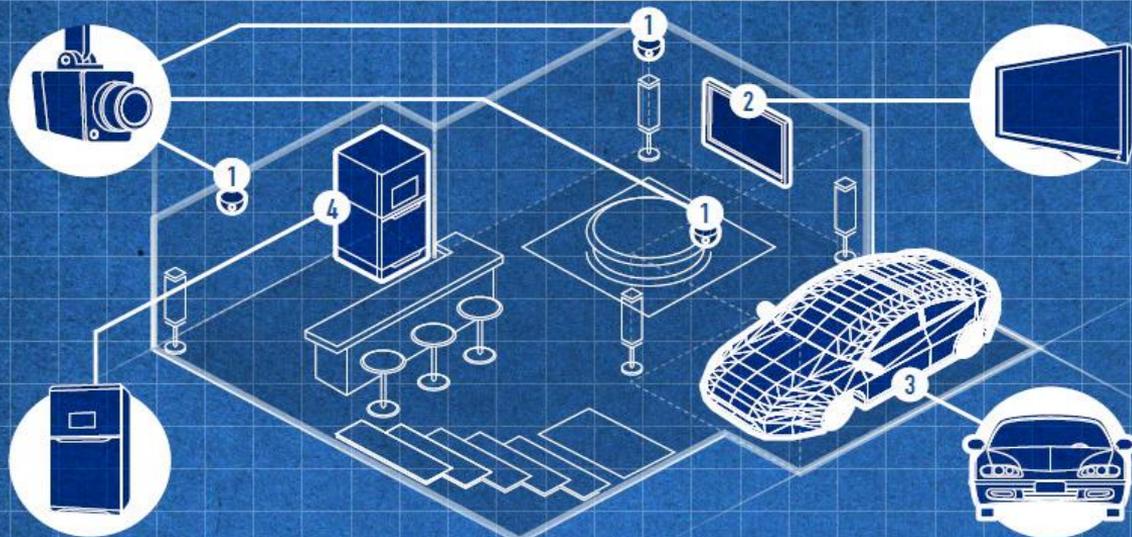
智能家居裝置

- 傳統資訊安全領域（PC、平板或智能手機）以外的消費型裝置。
- 具備運算能力可獨立運作、且可直接或間接連上互聯網的裝置。
- 主要用於家居環境，而非穿戴式裝置或智能汽車之類非以家用為主的裝置。家用智能裝置的範例包括：家電 (如智能洗碗機、智能冰箱)、視聽設備 (如智能電視、影音接收器、電玩遊戲主機、智能喇叭)、儲存與管理裝置 (如智能集線器、感應器)、能源計量表等等。

智能家居

有多麼容易遭到網路犯罪攻擊？

只要您能夠連上網際網路，那麼網際網路上的駭客就有辦法連上您。隨著連網家電逐漸受到青睞，您該思考一下您的家庭將面臨什麼樣的潛在安全風險。



潛在損失：



財產



金錢



身分



安全威

智能家居危機處處

① 監視攝影機、動作感應器、門鎖、保全裝置



優點：

家庭保全系統可自動將窗戶和出入口上鎖來保障家庭安全。此外，更搭配警報系統與監視攝影機來防止歹徒入侵。當保全系統連上網際網路時，屋主就能從遠端直接遙控管理。

缺點：

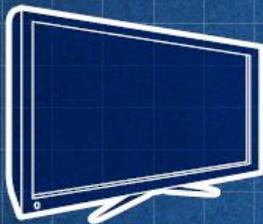
連上網際網路的保全系統有可能遭到駭客入侵。

萬一遭到駭客入侵：

網路犯罪者若能從網際網路進入您的保全系統，就能掌握您不在家的時間以便闖空門，此外，必要時還能隨時關閉您的保全系統。



② 智慧型電視



優點：

內建攝影機和麥克風的智慧型電視可具備臉部辨識和語音辨識功能，如此就能針對不同的使用者與使用時機套用專屬設定。

缺點：

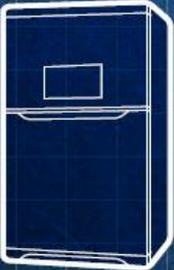
網路犯罪者可能入侵連網的智慧型電視並暗中操控它來錄下您的活動影像或聲音。

萬一遭到駭客入侵：

您可能哪天會突然發現自己和家人的影片被人上傳到不當的網站。此外，網路犯罪者還可能會利用智慧型電視所拍攝的影片或照片來竊取您的身分或向您勒索。



智能家居危機處處

<h3>③ 汽車</h3> 	<p>優點： 車用電腦系統可讓您將某些重要的系統設定自動化，包括馬力、煞車、定速巡航。</p> <p>缺點： 網路犯罪者若能透過一些網際網路服務（如影音串流、導航或網頁瀏覽）入侵車用電腦系統，即可對您車子的功能動手腳，並且/或者追蹤您車輛的定位資訊。</p>	<p>萬一遭到駭客入侵： 如果網路犯罪者讓您的煞車失靈，您將陷入嚴重的危險當中。</p>    
<h3>④ 智慧型冰箱</h3> 	<p>優點： 智慧型冰箱可讓您透過 LCD 螢幕在線上採購日用品，某些機種還能協助您遵從飲食計劃，根據已儲存選單來追蹤食物的存量。</p> <p>缺點： 網路犯罪者可能竊取您線上採購日用品的登入資訊，冒用您的名義購買一些不是您要的東西。</p>	<p>萬一遭到駭客入侵： 您可能得支付一些您從未訂購的日用品。</p>    

智能家居裝置可能洩漏的資訊

- **用戶名稱和密碼**：用來遠端存取或遙控用戶的家用智能裝置。
- **即時視訊或音訊資料**：用來從遠端蒐集用戶家中和家人的即時音訊或影像。
- **是否在家**：可從遠端觀察用戶通常在家的時間，這可從門鎖、窗戶感應器、動作感應器、恆溫控制動作、燈泡、數位錄影機 (DVR)、電視、網際網路收音機等裝置蒐集這項資料。
- **漏洞資料**：可用於評估用戶家中智能裝置的漏洞，這可從智能裝置的韌體版本或從韌體檔案本身來判斷。
- **醫療資料**：可用來從遠端蒐集有關用戶健康狀況的詳細資料，這可從體重計、血壓監視器、糖尿病監視器等等來取得。

黑客階段性攻擊

黑客手法

- “G Brand” 自動溫度調節器
- 功能
 - 可使用手機遠端控制這個裝置
 - 這個裝置掌控室內所有溫控裝置
- 黑客手法
 - 先研究產品規格
 - 利用後門 啟動裝置的服務順便放一個遙控程式
 - 連線並取得控制



黑客攻擊第一階段

- 研究與探勘階段

- 黑客在本階段主要是以POC 為主, 發揮黑客的想像力來研究這些智能裝置的弱點與取得控制

- 代表性型態

- PoC
- Oday vulnerability
- Hardware implementation
- Demo Video
- 裝置本身DOS或功能失效

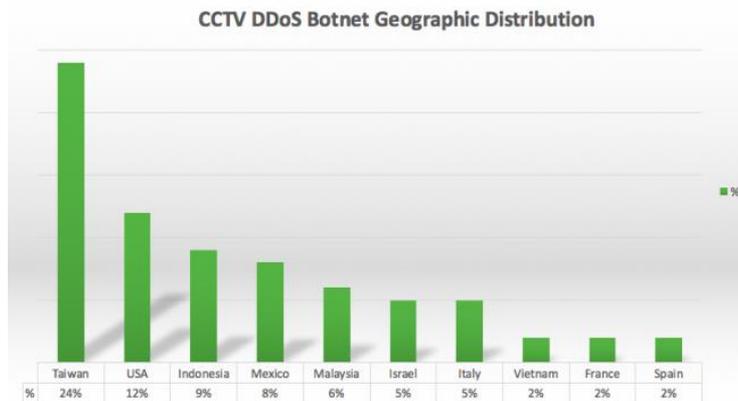
黑客攻擊第二階段

• 佔領與攻擊階段

- 這個階段黑客將會利用不同智能裝置的弱點取得控制權後，進一步攻擊背後的伺服器，雲端主機，或是變成跳板攻擊他人

• 代表性攻擊型態

- Botnet
- DDOS他人
- Worm
- Lateral movement
- 植入挖礦機



黑客攻擊第三階段

- 勒索與危害階段

- 在 這個階段, 犯罪者會使用這些智能裝置的弱點勒索金錢或進行實際的危害

- 代表性例子

- 植入勒索軟體
 - 汽車煞車鎖死
 - 心律調節器失效
 - 大眾運輸對撞
 - 遠端開家門, 車手闖空門
 - 讓ATM吐鈔



智能家居裝置安全要點

添置智能家居裝置時應注意的要點

- 智能裝置是否具備安全認證功能？

- 智能裝置是否需要輸入使用者名稱和密碼才能存取？許多智能裝置完全不具備安全認證功能。設計良好的智能裝置應具備某種認證功能來讓擁有者管制存取權限。

- 智能裝置在首次安裝時是否會要求您變更使用者名稱和密碼？

- 設計良好的智能裝置在第一次安裝時會要求用戶修改預設的登入帳號和密碼。修改預設的帳號和密碼可防止黑客利用公開的預設用戶名稱和密碼來登入裝置。

添置智能家居裝置時應注意的要點

- 智能裝置更新方便性如何？

- 裝置會自動更新嗎？裝置會通知您應該更新嗎？更新裝置會很複雜嗎？裝置更新可以讓智能裝置運作起來順暢又安全，但接收更新的方式可能是一項挑戰。在今日，裝置更新既是廠商的責任、也是消費者的責任。用戶必須考量更新程序的影響，包括更新的複雜性及所需的時間。

- 智能裝置是否會將韌體更新和網絡通訊確實加密？

- 即使智能裝置可能宣稱已採用加密，但某些廠商可能並未確實完整加密。用戶應上網搜尋裝置是否曾經出現安全問題。

添置智能家居裝置時應注意的要點

- **智能裝置是否需要開放任何連接埠？**
 - 開放連接埠會增加智能裝置的攻擊面，因此開放的連接埠越少越好。
- **廠商面對裝置漏洞的處理能力如何？**
 - 裝置有多少已公開的漏洞？這些漏洞有多少已修補？廠商平均過了多久才釋出修補程式？漏洞會讓不法之徒或網絡路犯罪集團有機會入侵裝置。廠商如何解決這些問題，將決定用戶是否能免於進一步風險。

自我防護要點

- 向會定期更新產品韌體的廠商購買物聯網產品
 - 任何系統都會有缺陷或漏洞，也因為如此，廠商會定時釋出韌體更新來修補其設備漏洞。

- 保護網絡
 - 任何連到家庭網絡的設備都必須具備安全和防護入侵的能力。這包括了路由器和所有連接到它的電腦和流動設備。

謝謝！

TRENDMICRO.COM.HK