今年IoT惡意程式數量已較去年倍增

資安業者卡巴斯基實驗室(Kaspersky Lab)於6/19指出，截至2017/5，該實驗室已蒐集了7242種鎖定物聯網裝置(Internet of Things, IoT)的惡意程式，遠高於去2016年的3219種，顯示光是今年就出現逾4000種新IoT惡意程式。一年來基於IoT裝置的殭屍網路持續現身，從Mirai、Leet、Amnesia到可直接癱瘓IoT裝置的BrickerBot，駭客利用龐大的IoT殭屍網路，於全球發動分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊。卡巴斯基實驗室透過誘捕系統捕獲了各式各樣的IoT惡意程式，並進行分析。調查顯示全球的IoT惡意程式數量正迅速增加中，從2013年只有46種、2014年的193種、2015年的696種到去年的3219種，而今年則是捕獲了7242種。

全球IoT殭屍網路主要由監視器與IP攝影機組成，佔了所有殭屍裝置的63%，另有20%為各式各樣的網路裝置與路由器，還有1%為Wi-Fi中繼器、電視調諧器、VoIP裝置、印表機，甚至是智慧家庭裝置，還有20%無法辨識裝置類別。被駭的IoT裝置有13.95%位於中國，12.26%在越南，俄國、巴西、土耳其分別為6.92%、6.21%、5.97%，台灣也佔了5.73%。IoT裝置之所以成為駭客攻擊目標有兩大原因，一是韌體更新政策不足，二為使用一致的登入帳號密碼。

研究指出，IoT裝置製造商不是很少釋出韌體安全更新，就是從未更新過韌體，還有一些裝置甚至不具備韌體更新的能力。此外，製造商經常採用同樣的帳號與密碼，替駭客大開方便之門，有時不只是同一型號的產品採用一致的帳密，甚至是所有產品線的帳密都是一樣的，也因為這樣的作法已行之有年，於是這些帳密資訊光明正大地曝露在網路上，唾手可及。根據統計，鎖定telnet傳輸埠的IoT惡意程式最常使用的帳密包括root與xc3511、root與vizxv、admin與admin、root與admin、root與xmhdipc、root與123456、root與888888、root與54321等。基於SSH的IoT惡意程式所內建的入侵帳密則有admin與default 、admin與admin、support與support、admin與1111、admin與空白、user與user、Administrator與admin、admin與root等。

卡巴斯基實驗室指出，IoT裝置的安全威脅不再是概念性的，而已非常真實，全球的IoT裝置數量將從目前的數十億成長到2020年的200至500億台，更顯現其安全問題的急迫性。在製造商還未採取行動的狀況下，卡巴斯基實驗室建議使用者不要讓裝置曝露在公開網路上，關閉裝置未使用的所有網路服務，變更裝置的預設帳密，以及定期更新韌體，只要遵行這幾項建議，即可躲過大多數的IoT惡意程式。

資料來源：

https://securelist.com/honeypots-and-the-internet-ofthings/78751/

http://www.ithome.com.tw/news/115017

國家資通安全會報技術服務中心整理

2017/7/7 0:00:00