臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

Mirai 惡意程式探討與防範

臺灣大學計資中心網路組
北區學術資訊安全維運中心

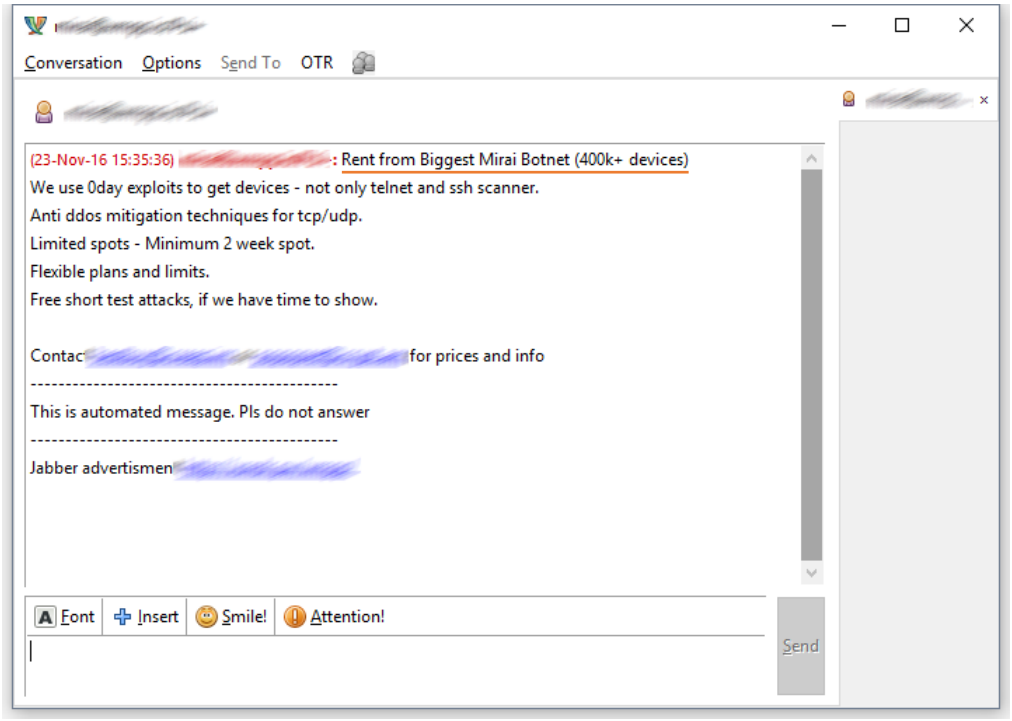
● 摘要

生活在科技蓬勃發達的時代，幾乎每個人都至少擁有一支智慧型手機，許多場所也提供免費的無線網路供人使用。大家是否思考過，在您身邊的物聯網(IoT)裝置，或許已經遭不明人士偷偷植入惡意程式了呢?

根據去年 iThome 的一篇報導： 「駭客們在網路論壇上發布消息，想要出租以 Mirai 惡意軟體為主的殭屍網路，其殭屍網路所控制的裝置數量已達到四十萬個」。從這篇報導看來，受 Mirai 感染的裝置數量龐大，如果利用大量的 IoT 裝置攻擊某一目標，所造成的損失將難以估計。

目前 Mirai 主要的攻擊方式是用分散式阻斷服務攻擊(Distributed Denial of Service — DDoS)，目的是要癱瘓攻擊目標的網站服務。去年發生過數次透過 Mirai 操控的 DDoS 攻擊，例如去年十月，Dyn 公司提供的 DNS 服務被 DDoS 攻擊，導致一些網站無法正常運作。

在使用高科技產品的同時，潛在的危險也一直存在著。大家可以透過閱讀本篇文章，進一步了解 Mirai。



圖一：出租 Mirai 的廣告訊息

● Mirai 介紹

Mirai 是一個惡意軟體，它的行為表現類似電腦蠕蟲。Mirai 的主要感染目標是物聯網裝置；當裝置被植入 Mirai 後，攻擊者可以操控該裝置，且把該裝置轉變為殭屍網路的成員，攻擊者可利用殭屍網路進行大規模網路攻擊。Mirai 的原始碼(Source Code)已經在駭客論壇公開，以開源原始碼(Open Source Code)的形式發布，將導致入侵 IoT 設備的技術，可能用在更多新的惡意軟體上.。

物聯網(Internet of Things，簡稱 IoT)，廣泛定義為各類裝置設備透過連上網際網路，互相建立連線以傳送與接收資訊(或是資料)。例如網路印表機、智慧型電視、網路監控攝影機、家用路由器以及電器用品等等，都是物聯網的裝置。

● Mirai 攻擊行為

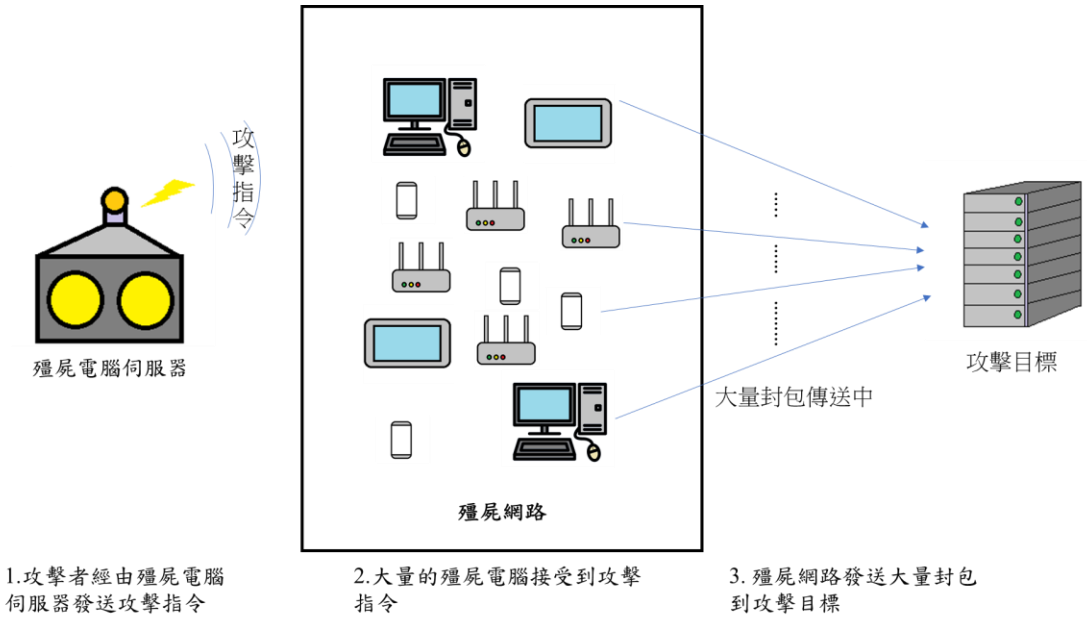
(一) 受 Mirai 感染的裝置，會持續地在網際網路上(先從相同網段開始，之後擴張到外面)掃描物聯網裝置的 IP 位址和連接埠。

(二) 掃描到其他未受感染裝置的 IP 位址和連接埠之後，Mirai 會通過多種常用預設帳號和密碼嘗試攻擊該裝置，如果可以登入該裝置，隨即開始安裝 Mirai。雖然受感染的裝置比面上看起來正常運作，但有時候會有些延遲，而且網路頻寬流量也發生異常狀況。

(三) Mirai 成功感染後，會刪除該裝置上同類型的惡意軟體，而且會關閉遠端管理連接埠。

(四) 只要裝置未重新啟動，會一直處在受感染的狀態。一旦裝置重新開機之後 Mirai 不會運作，但是短時間內該裝置還是很有可能被感染。

- **Mirai 攻擊手法:分散式阻斷服務攻擊**



圖二：Mirai DDoS 攻擊示意圖

DDoS 攻擊是阻斷服務攻擊(Denial of Service — DoS)的進階版。DoS 是一種惡意的攻擊手法，攻擊者會使用多種方式對目標傳送大量的封包，並要求目標傳送回覆訊息，讓目標的網路頻寬擁塞或是系統資源耗盡，造成目標無法提供服務給需要的使用者。

以 DoS 攻擊為基礎，DDoS 攻擊是利用其數量龐大的殭屍電腦所建立的殭屍網路來發動大規模攻擊，此種攻擊可以讓目標的服務暫時無法提供。有心人士利用這種方式進行惡意的商業活動或政治行為，例如攻擊商業上的競爭對手、癱瘓投票網頁等。

DoS 攻擊和 DDoS 攻擊的區別	
DoS 攻擊	DDoS 攻擊
一對一或是一對多攻擊	多對一或是多對多攻擊

● 建議措施

1. 購買物聯網裝置時，需確認裝置能修改帳號密碼；使用前，修改原裝置的預設帳號密碼，建立強健的密碼(英文大小寫、數字符號混用)。
2. 物聯網裝置的軟體版本需定期更新，以防止有心人士利用漏洞取得裝置使用權限。
3. 請關閉物聯網裝置未使用的服務(例如遠端存取功能)。

● 參考資料

1. 陳曉莉。2016-11-30。40 萬裝置的 Mirai 殭屍大軍竟然上網公開出租。iThome。網址：http://www.ithome.com.tw/news/109941。
2. Mirai(惡意軟體)介紹。維基百科。網址：https://zh.wikipedia.org/wiki/Mirai_(%E6%81%B6%E6%84%8F%E8%BD%AF%E4%BB%B6)。
3. Symantec Security Response。2016-10-27。Mirai: what you need to know about the botnet behind recent major DDoS attacks。網址：https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks。
4. 李美雯。2016-02-18。WordPress Pingback DDoS 攻擊分析。網址：http://cert.ntu.edu.tw/Document/TechDoc/Analysis_of_WordPress_Pingback_DDoS_Attack.pdf。
5. TREND LABS 趨勢科技全球技術支援與研發中心。2014-09-15。《 IoT 物聯網安全趨勢 》採購智慧型裝置該注意些什麼? 網址：https://blog.trendmicro.com.tw/?p=9617
6. 物聯網定義。維基百科。網址：https://zh.wikipedia.org/wiki/%E7%89%A9%E8%81%94%E7%BD%91

● 圖片來源

1. Mirai 出借的廣告，來源網址：https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/。