個案分析-

物聯網 IoT 監視器 Telnet 暴力入侵攻擊事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/7

I. 事件簡介

1. 近期學術網路內許多單位陸續被開立 Telnet.Login.Brute.Force 資安事件單，經由追查發現似乎都來自特定廠牌型號的 IoT 監視器主機。
2. 物聯網（英語：Internet of Things，縮寫 IoT）是網際網路、傳統電信網等資訊承載體，讓所有能行使獨立功能的普通物體實作互聯互通的網路。
3. 該監視器有個統一特性是，網頁管理介面的帳號密碼都是用出廠預設值 admin，輕易能夠登入設定並監看影像內容。
4. 本單位有與該設備廠商詢問過，廠商回應是雲端伺服器同步的誤判事件。
5. 為了驗證是否為廠商所言誤判，故與其中一個單位聯絡，協助進行封包側錄並進行數位鑑識工作。

原發布編號	[redacted]	原發布時間	2016-06-07 09:41:41
事件類型	對外攻擊	原發現時間	2016-06-06 02:49:09
事件主旨	通報:[redacted]140.[redacted]249 Telnet.Login.Brute.Force		
事件描述	ASOC發現貴單位([redacted])所屬 140.[redacted]249 疑似對外進行 Telnet.Login.Brute.Force 攻擊		
手法研判	Telnet協議是TCP/IP協議族的其中之一，是Internet遠端登錄服務的標準協議和主要方式，常用於網頁伺服器的遠端控制，可供使用者在本地主機執行遠端主機上的工作。貴單位疑似對外進行非法攻擊行為，遠端攻擊者可利用暴力密碼猜測攻擊，嘗試登入Telnet伺服器，攻擊者在1分內進行60次的登入請求，如攻擊成功將可以連入未經授權的系統，進行非法的存取。		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常或未經許可的連接埠，並查看記錄是否有外界對貴單位內部IP之異常連線。 2.如發現為非授權的連線，建議將該IP於防火牆阻擋。 3.建議針對被攻擊的主機做好相關主機系統服務檢查及弱點修補確認的工作，並關閉不需要的服務。 4.將所使用的密碼複雜度提高。 5.攻擊名稱相關參考資料網站： FortiGuard http://www.fortiguard.com/encyclopedia/vulnerability/#id=20940		

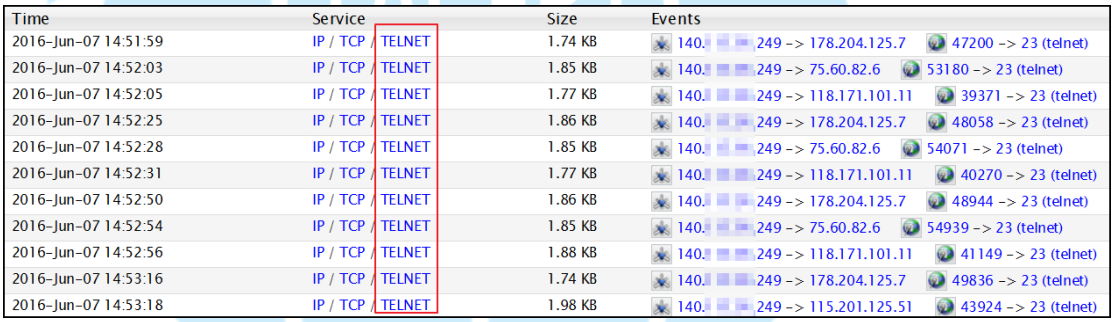
II. 事件檢測

1. 通常監視器主機都有開起 Web service，方便讓管理者能夠登入監看操作，輸入主機 IP 可以看到登入的頁面，帳號密碼為預設值。

2. 使用預設帳密登入後，查看日誌並無明顯可疑的登入紀錄，同時檢查系統韌體版本當時為 2015-01-30 的版本。

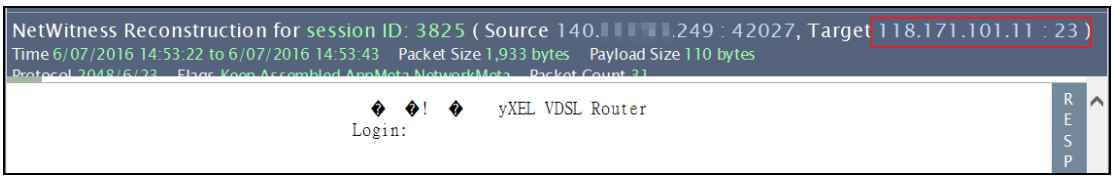
3. 從 Web 登入的介面只有基本的監視器功能，並無法於作業系統核心進行操作，因此只能先從側錄的封包紀錄中去檢查。

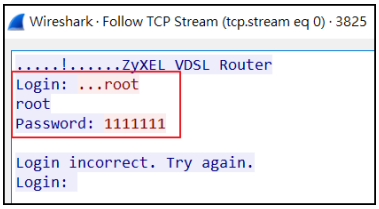
4. 首先驗證是否該監視器主機有對外攻擊現象，透過封包紀錄來看該主機確實短時間內密集對外部進行 telnet 連線行為。



Time	Service	Size	Events
2016-Jun-07 14:51:59	IP / TCP / TELNET	1.74 KB	140. 249 -> 178.204.125.7 47200 -> 23 (telnet)
2016-Jun-07 14:52:03	IP / TCP / TELNET	1.85 KB	140. 249 -> 75.60.82.6 53180 -> 23 (telnet)
2016-Jun-07 14:52:05	IP / TCP / TELNET	1.77 KB	140. 249 -> 118.171.101.11 39371 -> 23 (telnet)
2016-Jun-07 14:52:25	IP / TCP / TELNET	1.86 KB	140. 249 -> 178.204.125.7 48058 -> 23 (telnet)
2016-Jun-07 14:52:28	IP / TCP / TELNET	1.85 KB	140. 249 -> 75.60.82.6 54071 -> 23 (telnet)
2016-Jun-07 14:52:31	IP / TCP / TELNET	1.77 KB	140. 249 -> 118.171.101.11 40270 -> 23 (telnet)
2016-Jun-07 14:52:50	IP / TCP / TELNET	1.86 KB	140. 249 -> 178.204.125.7 48944 -> 23 (telnet)
2016-Jun-07 14:52:54	IP / TCP / TELNET	1.85 KB	140. 249 -> 75.60.82.6 54939 -> 23 (telnet)
2016-Jun-07 14:52:56	IP / TCP / TELNET	1.88 KB	140. 249 -> 118.171.101.11 41149 -> 23 (telnet)
2016-Jun-07 14:53:16	IP / TCP / TELNET	1.74 KB	140. 249 -> 178.204.125.7 49836 -> 23 (telnet)
2016-Jun-07 14:53:18	IP / TCP / TELNET	1.98 KB	140. 249 -> 115.201.125.51 43924 -> 23 (telnet)

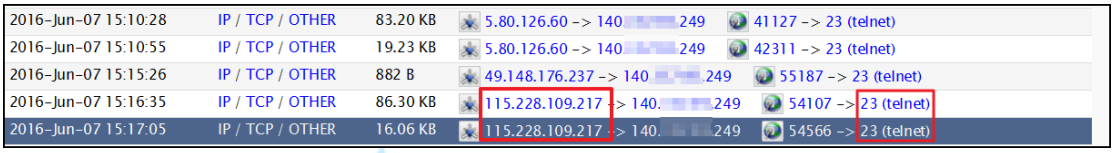
5. 檢查其中一個連線內容來看，可以看到確實有嘗試以 root/1111111 登入失敗紀錄。



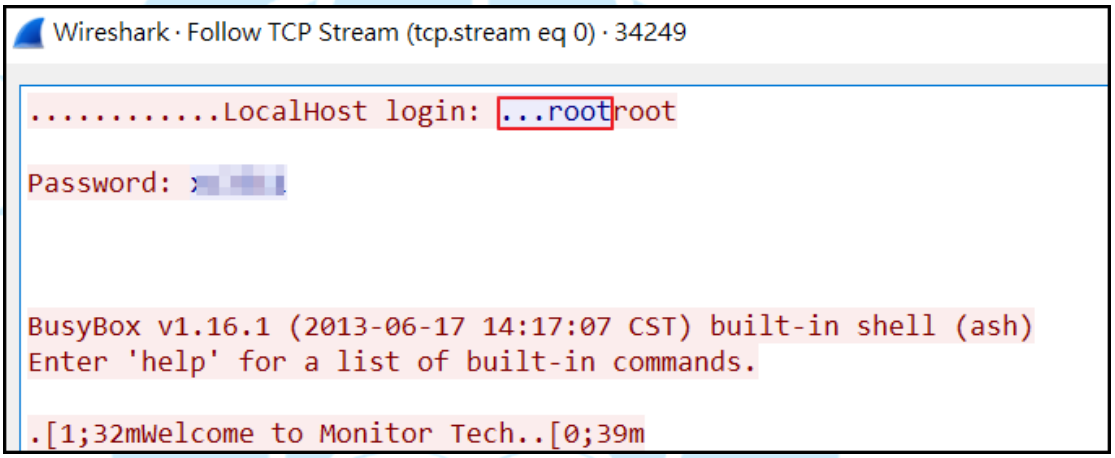


6. 找到對外攻擊的事證後，接著要查找監視器主機可能被入侵的原因。從封包紀錄中得知監視器主機的 port 23 也是開啟的，表示有啟用 Telnet 的服務讓其他人能登入。

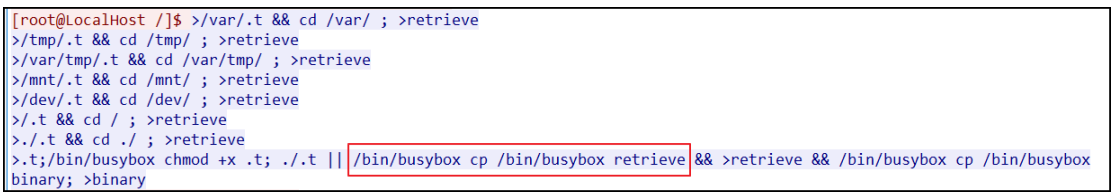
7. 封包紀錄中看到多筆外部 IP 如中國 115.228.109.217 成功登入監視器的 TELNET 服務。



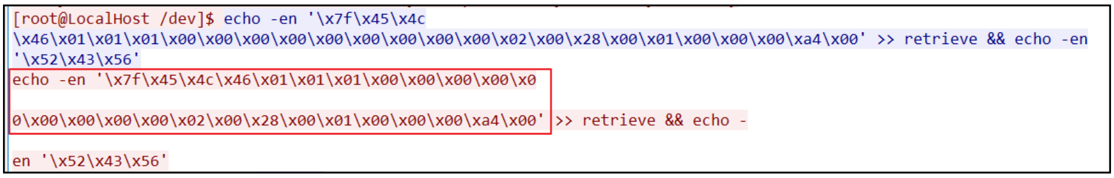
8. 檢查紀錄查看內容，得知駭客使用的帳號密碼為 root/****** ，應為廠商預留的後門，以及底層為 linux-based 的 Busybox v1.16.1。

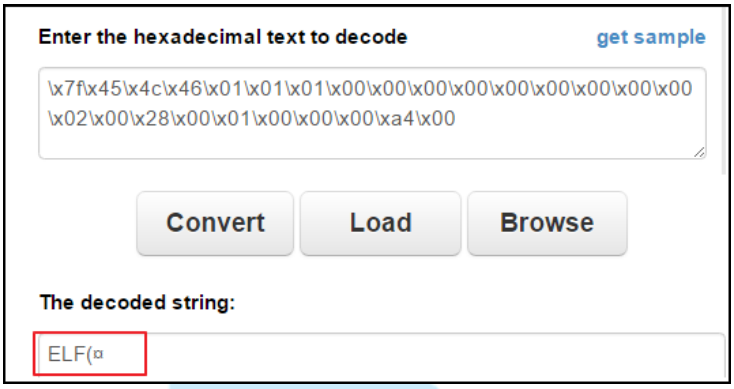


9. 該 busybox 作業系統能使用的指令相對較簡陋，無法透過外部下載方式或內部檔案編輯指令“vi”寫入後門惡意程式，因此駭客透過指令“>”建立所需的檔案名稱，並在透過“>”將欲執行指令批次寫入 retrieve 中。

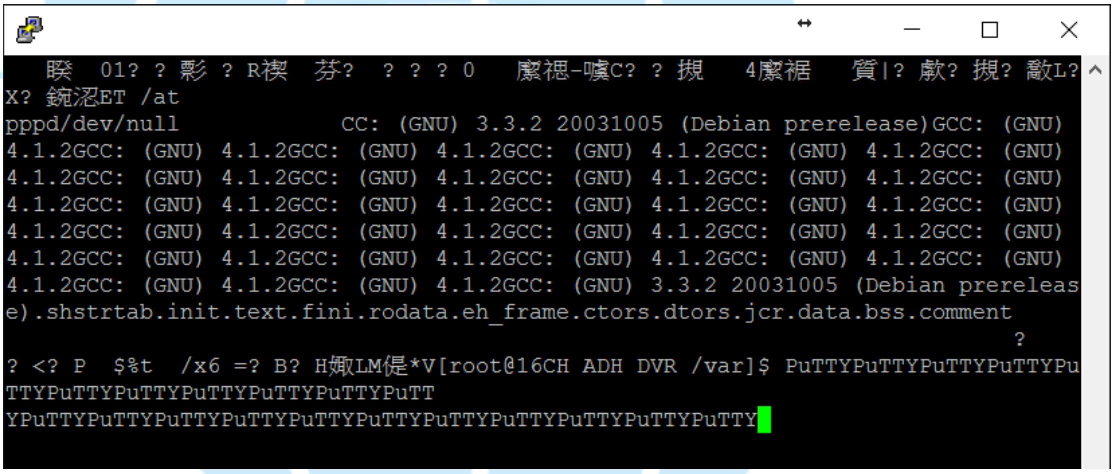


10. 駭客先將可執行的 shell 指令 busybox 寫入 retrieve，接著透過 echo 方式將指令用 16 進位的 ASCII 編碼顯示並用 >> 寫入到 retrieve，透過 decoder 將部分編碼解開，開頭是“ELF”的執行檔。

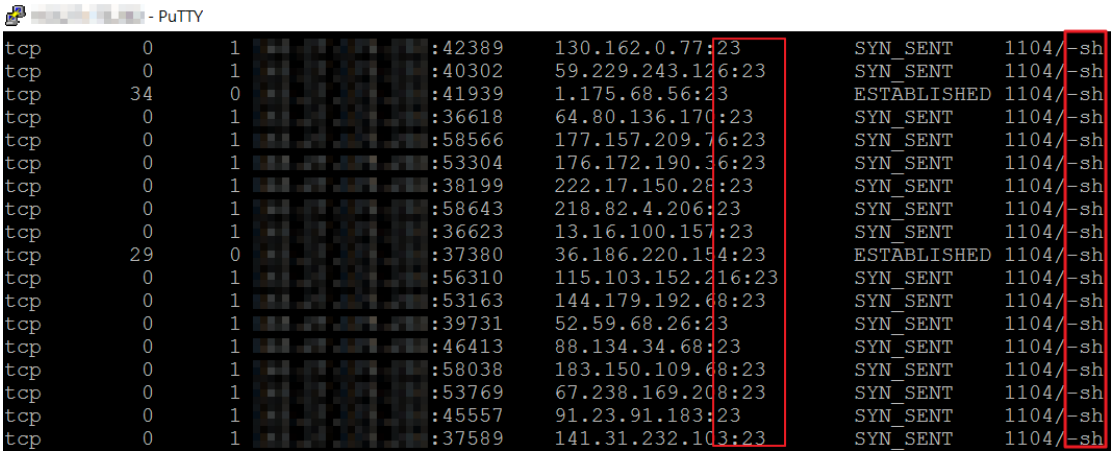




11. 由於指令 echo 後內容較多，但透過指令 cat 顯示其 retrieve 執行檔內容為如下，其行為就是對外進行 telnet 暴力破解攻擊。

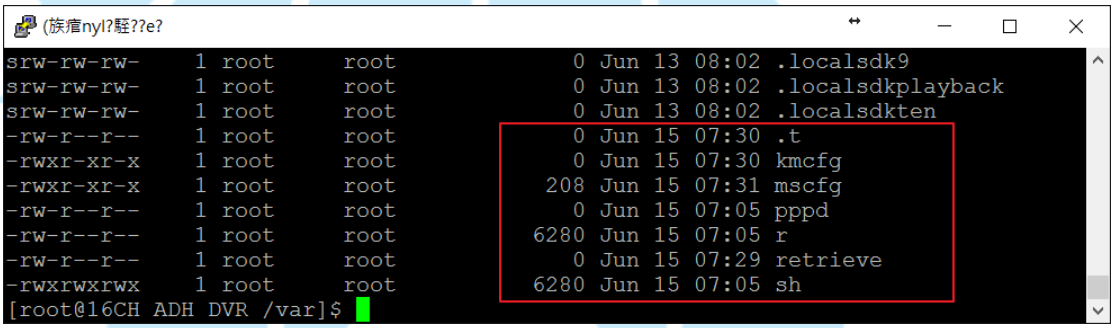


12. 實際透過後門的帳密 Telnet 登入，並 netstat 查看網路連線狀態，可以看到有大量的對外 telnet 連線。

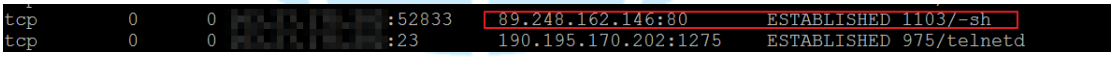


13. 雖得知攻擊程式顯示為 - sh 的程序，事實上為 retrieve 的執行成果，因為駭客在執行攻擊程式後會刪除執行檔，避免程式碼外流。

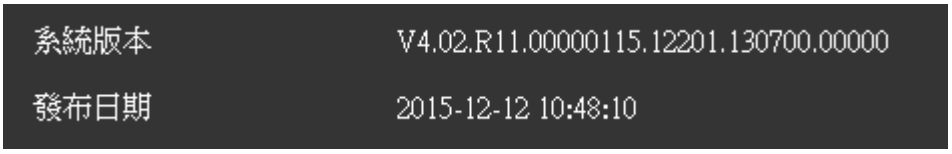
14. 駭客習慣在 /var/ 路徑下建立修改需要的檔案，因為連入的駭客不只一個，所以駭客建立的檔案通常變動很快也不完整。



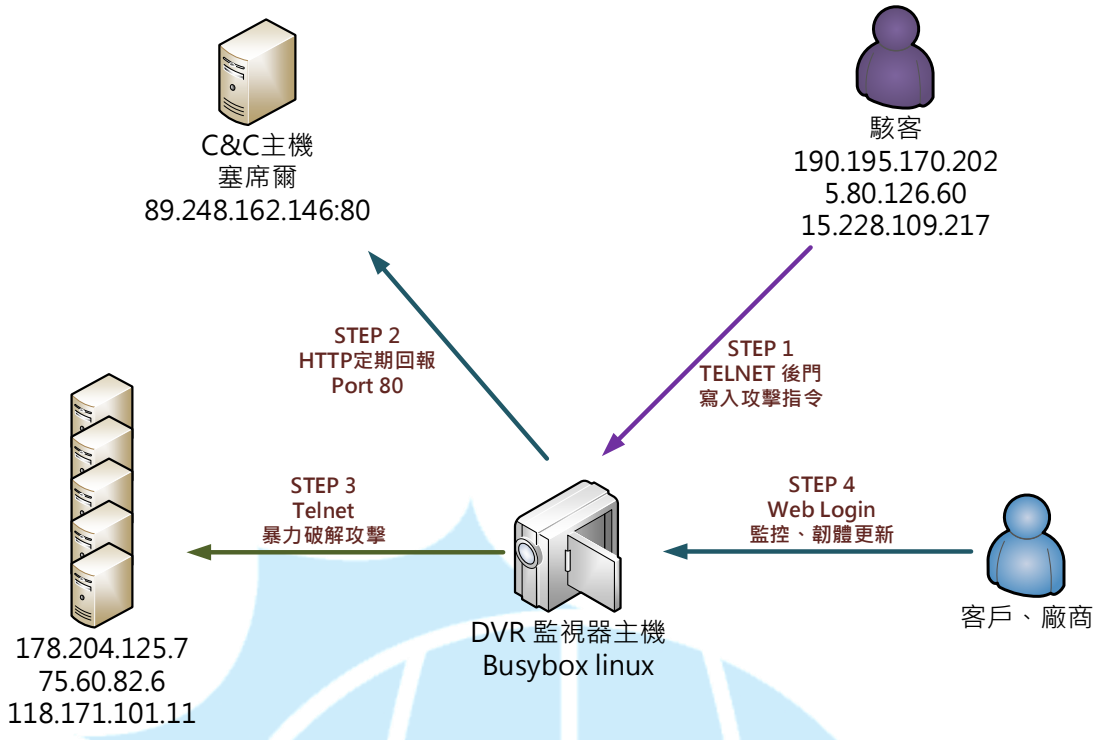
15. 監視器也會持續建立連線到上層 C&C 塞席爾 89.248.162.146 的 port 80，作為監控的報到用途，而阿根廷 190.195.170.202 連線表示其中一個駭客已經 telnet 登入中。



16. 此案例推測為韌體的漏洞後門導致遭受入侵，因為在廠商進行線上更新韌體版本並重開機，原本的 telnet 服務就被關閉無法登入，在此之後的 telnet 攻擊流量也就消失。韌體版本已經更新至 2015-12-12。



III. 網路架構圖



1. 駭客透過監視器韌體版本漏洞，從 TELNET 後門使用預設帳密入侵。
2. 監視器會固定連線回報到上層 C&C。
3. 駭客透過 echo 指令寫入攻擊程式碼，對外部大量主機進行 Telnet 暴力破解攻擊。
4. 客戶端和廠商透過 Web 介面登入，並且能夠線上更新系統韌體修補漏洞。

IV.建議與總結

1. 此個案主機在 Web 服務介面就無變更過帳號密碼，只要使用預設值任何人都能登入操控監視器。
2. 駭客透過監視器韌體版本漏洞，並使用 root 和預設密碼從 Telnet 的 port 23 登入，進行對外 telnet 攻擊。
3. 監視器的底層 OS 為 busybox，能夠使用的指令很少，故駭客透過 echo 指令取代一般的文書編輯指令去寫入惡意程式碼。
4. 駭客執行完惡意程式後可能刪除檔案，不讓其他人能夠存取，故主機從開機後駭客必須再次登入操作才能發動攻擊。
5. 經測試發現當系統韌體更新後，原本的 TELNET 後門就無法登入，表示新

的韌體已經作出修正。

6. 此監視器為台灣自製的品牌，可能為工程師在製作過程中預留的後門，反而成為駭客輕易入侵的漏洞。