個案分析-

V 大學透過 VNC 入侵的伺服器事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/10

I. 事件簡介

A. 今年偕同行政院技服中心前往至該大學，鑑識一台疑似遭受入侵有 APT 惡意網路行為的主機。

B. 詢問該主機管理人員得知為某學生宿舍的一台桌上型的主機，IP 位址為 140.X.Y.252，作業系統為舊版的 Windows XP，用途為集中監視器畫面管理。

C. 預設有安裝 UltraVNC 的遠端桌面軟體，方便維護廠商外部連線管理。

D. 遠端登入的帳號和密碼極為簡易，密碼是統計最常見的排行榜前十名，只有六位數字排序。

E. 主機並無限制外部來源端網段或 IP，其為了方便廠商連入維護。

F. 本單位側錄該主機的網路封包，並觀察系統的網路運作狀態。

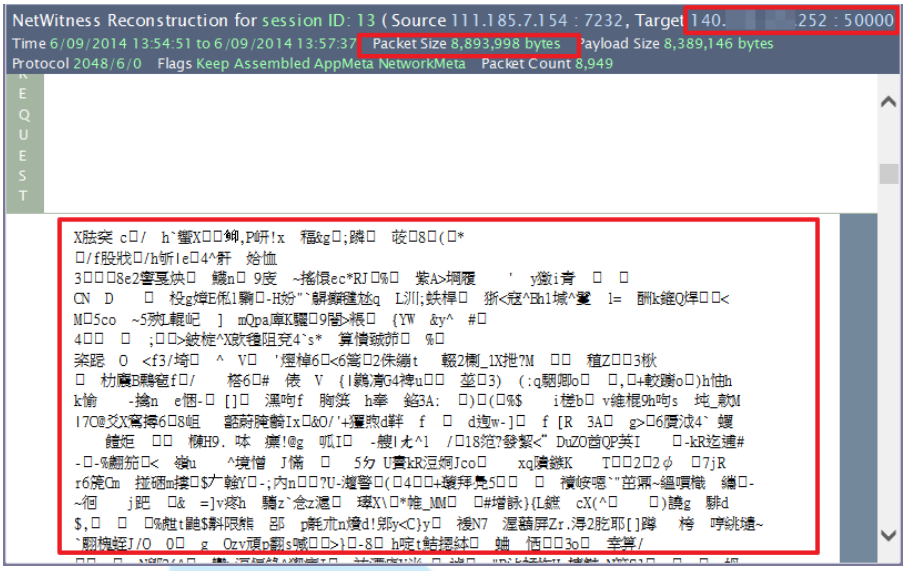
II. 事件檢測

A. 首先透過 netstat 指令檢測紀錄中已開啟的通訊埠，主要有 TCP Port 80、443、5800、5900、9988、40000 和 50000。

Active Connections

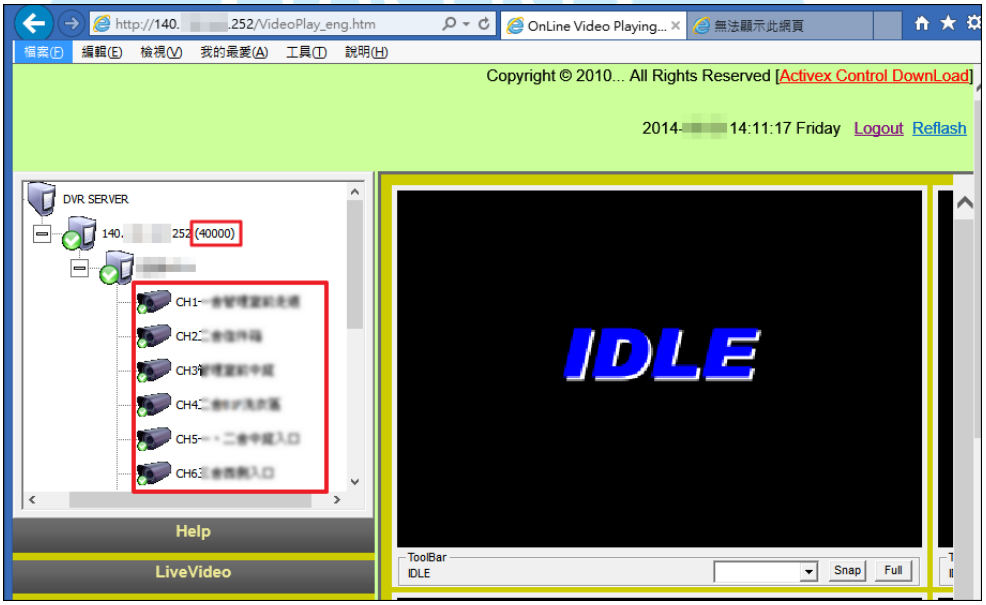
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	3580
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1072
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	3928
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5800	0.0.0.0:0	LISTENING	528
TCP	0.0.0.0:5900	0.0.0.0:0	LISTENING	528
TCP	0.0.0.0:9988	0.0.0.0:0	LISTENING	3928
TCP	0.0.0.0:40000	0.0.0.0:0	LISTENING	160
TCP	0.0.0.0:50000	0.0.0.0:0	LISTENING	2864

B. 經過封包分析得知，Port 40000 和 50000 主要是由兩個台灣的 IP 111.185.7.154 和 114.198.173.241 連入，其中封包傳輸的資料都是經過加密無法解析，且主要流量都是透過主機 port 50000 回覆給主機 111.185.7.154，平均一個檔案都有 8MB 左右。



C. 從 netstat 命令資料中得知 port 80 是啟用的，表示有啟用 Web Service， 且從 process 程序中看出的確有啟用 Apache 的服務。

1. 嘗試透過瀏覽器直接輸入該主機位址 140.X.Y.252，為 DVR 的登入畫面，但隨意輸入帳號密碼後雖然無法登入成功，卻可以列出監視器的相關資訊，例如 Channel 的說明和使用的 Port 40000。



2. 因此我們判斷程序 Apache、ChateauSVR、ChateauHD 分別使用 port 80、40000、50000 為監視器廠商所使用。

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	3580
TCP	0.0.0.0:40000	0.0.0.0:0	LISTENING	160
TCP	0.0.0.0:50000	0.0.0.0:0	LISTENING	2864

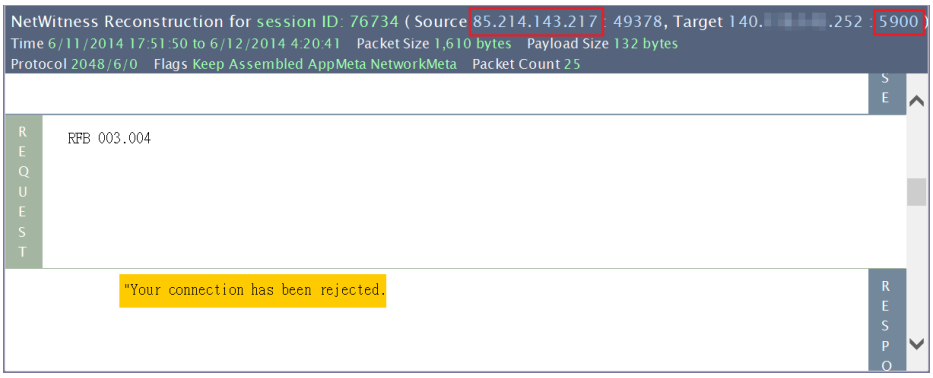
Name	Pid	Pri	Thd	Hnd	VM	WS	Priv
ChateauSVR	160	8	11	247	136316	9492	14904
ChateauHD	2864	8	32	792	529204	64880	211224
Apache	3580	8	1	47	16980	2464	796
Apache	2116	8	51	190	68120	4396	2980

3. 再來 port 5800 和 5900 所使用的 PID 程序為 UltraVNC，這是一款常見的遠端桌面操控軟體，主要是讓維護商可以遠端管理，但是因為密碼過於簡單導致駭客成功登入控制。因為安裝的是舊版 VNC，內無登入 IP 的 LOG 紀錄可追查。

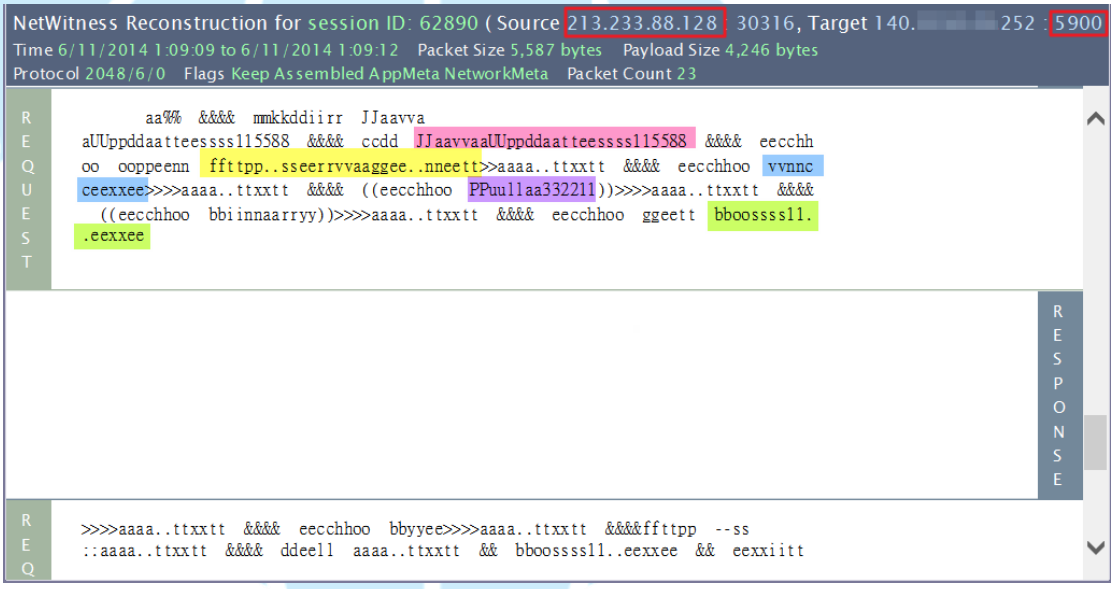
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:5800	0.0.0.0:0	LISTENING	528
TCP	0.0.0.0:5900	0.0.0.0:0	LISTENING	528

Name	Pid	Pri	Thd	Hnd	VM	WS	Priv
services	824	9	16	367	42644	13160	3832
WinVNC	528	8	4	119	39780	4616	3304

4. 然而從側錄的封包中我們發現到有幾筆 IP 嘗試登入的紀錄，表示可能已經被入侵成功過，主要有 85.214.143.217、202.153.164.126、213.233.88.128 和 185.56.80.101 等。
5. 其中來自德國的 85.214.143.217 嘗試登入數量最多，但記錄上並沒有成功登入，都出現存取拒絕的訊息，可能正在嘗試做大量破解入侵準備。

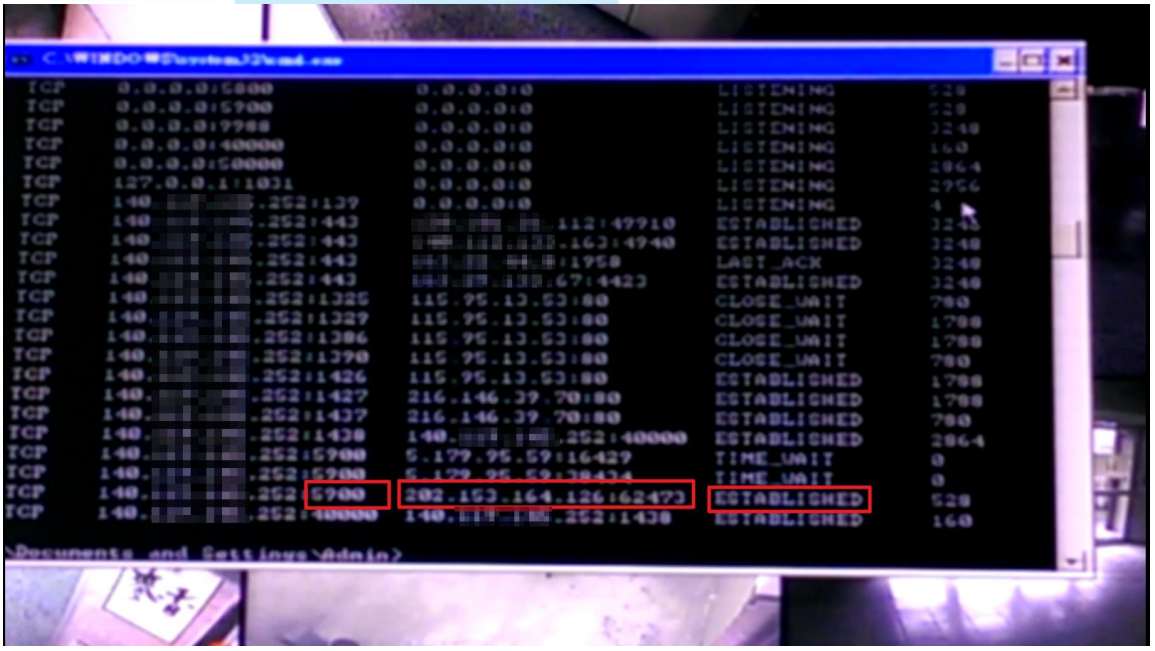


6. 而來自羅馬尼亞的 213.233.88.128 則是成功登入 UltraVNC，從封包紀錄發現駭客使用一個相當簡易的編碼方式傳送指令，就是重複字元編碼，創立了一個名為「JavaUpdatess158」的資料夾，並且連到「ftp.servage.net」，並且用帳號「vncexe」和密碼「Pula321」登入下載檔案「boss1.exe」的檔案，並隨後再刪除。



7. 嘗試用以上的帳號密碼果然能夠登入該網站 ftp.servage.net，並且內部有兩個執行檔案，分別為「svchost.exe」和 「wget.exe」，此「svchost.exe」疑似是客製化的惡意程式，透過 Virustotal 線上病毒掃描的檢測率為 0。

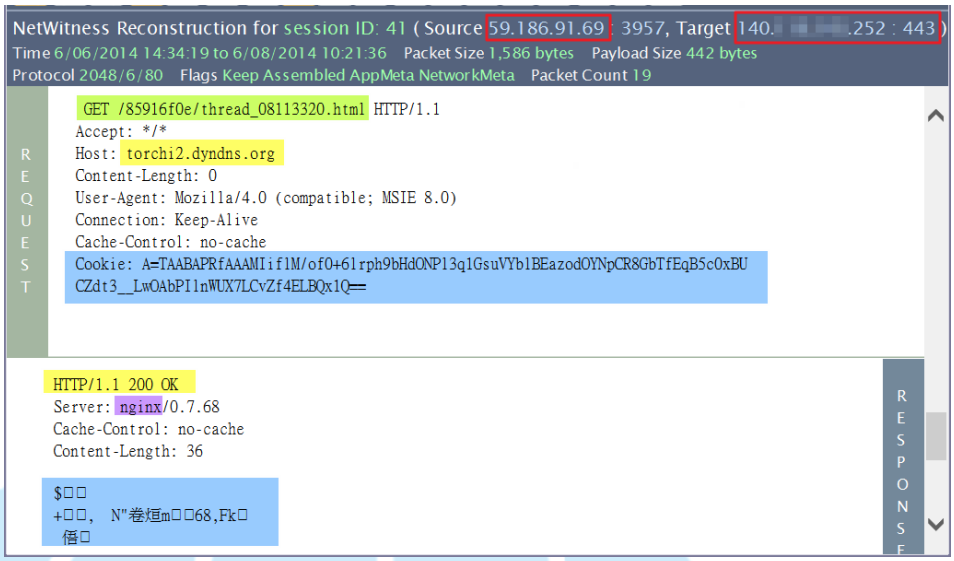
8. 特別的是 IP 202.153.164.126 有成功登入主機，並且是來自是台灣方電信的 IP 而非國外，登入的時候剛好被我們錄影下來存證。從封包來看是從 UltraVNC 的 port 5900 登入，駭客很俐落的打開 cmd.exe 視窗，並且檢查 netstat 的網路狀態服務是否有被關閉，該主機事實上被用來作為線上遊戲(射擊對戰遊戲)的私人伺服器，因為有發現到該遊戲的資料夾而非管理員安裝，以下為駭客正在操作的錄影截圖(背景為 DVR 畫面)。



9. 最後 Port 443 都是被同一支程式所啟用，從 process explore 看只能知道為 svchost.exe，然而從側錄封包中可以看到 port 443 所回應內容中有 nginx 的 web service，研判應該是變異過的 nginx 套

件。

a. 從封包中知道外部的人透過 GET method 方式並帶有特定加密的 cookie 參數，而伺服器則同樣回應加密字串。



b. 連入主機 port 443 的 IP 約有 7 個國家，大多數為台灣和韓國，並且固定使用的網域名稱「torchi2.dyndns.org」作解析。

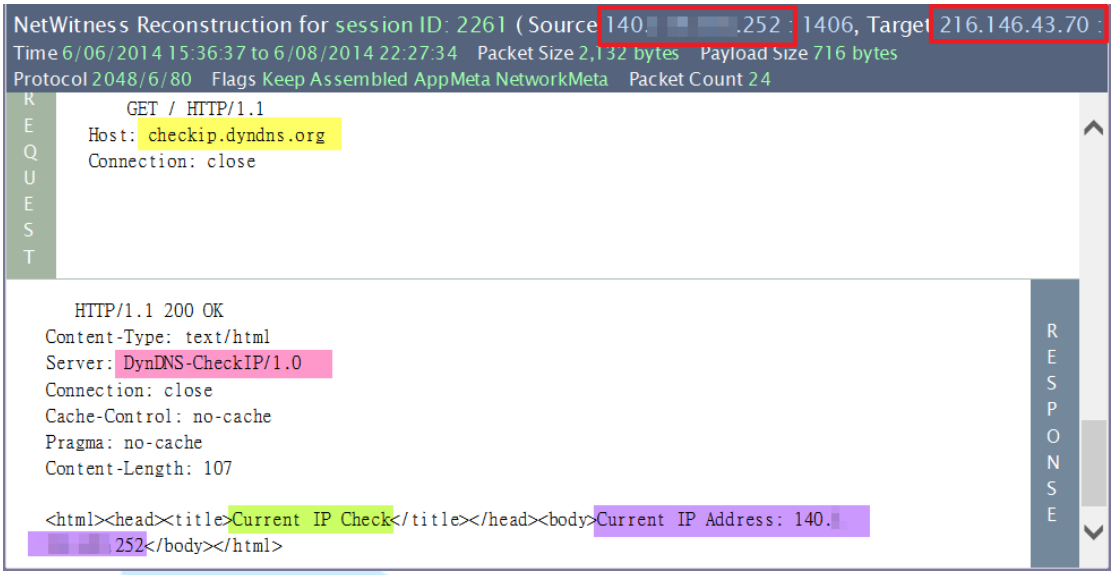
c. 然而目前此名稱「torchi2.dyndns.org」的 IP 已經變成另一個受害者 59.120.116.245，為 Hinet 的固定制 IP。

d. 稍微檢測目前「59.120.116.245」主機發現一樣有開啟 port 80、443、5800、5900，其中 5800 和 5900 為 VNC 服務所用，埠 443 則是為 nginx 所用，透過 zenmap 掃描得知 port 80 則應為 skype 所用。經網頁測試 port 5800 發現因為 Java 特殊權限無法正常開啟，但是透過 html code 可以看出黃色圈選部分帶有某公司名稱及 UltraVNC 字樣，猜測此主機可能也遭受相同手法入侵。

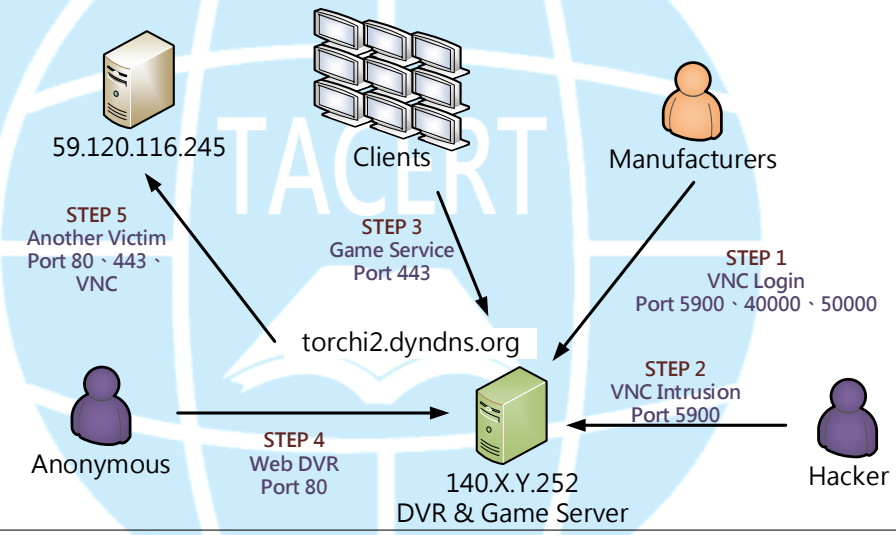
e. 若嘗試輸入 http://torchi2.dyndns.org:443 則會回覆自己的主機 IP 位址，以此案件學校的封包分析來看也是如此，如下圖藍色圈選之 IP。

f. 因為封包內容都經過加密，我們也無法明確知道其內容，但研判作為私人線上遊戲伺服器供外部使用者連入使用。

10. 駭客將主機內部設定動態網域名稱，定期會向免費網域網站「checkip.dyndns.org」進行檢查動作，確保該網域名稱「torchi2.dyndns.org」維持正常使用，下圖中紫色為報到主機。



III. 網路架構圖



STEP 1：維護廠商安裝VNC服務從外部連入140.X.Y.252維護管理。
STEP 2：駭客破解VNC的超級弱的密碼後植入其他軟體。
STEP 3：主機被駭客用來作為遊戲伺服器供外部使用者從「torchi2.dyndns.org」連入。
STEP 4：任何匿名者也都能登入到或破解原服務 Web DVR介面進行畫面監視。
STEP 5：「torchi2.dyndns.org」後來解析到其他企業主機進行可能入侵的行為。

IV. 建議與總結

A. 此主機主要是因為維護廠商在宿舍的監視器用途主機上安裝 VNC 的遠端桌面軟體，目的是可以從外部方便連入維護。

B. 然而因為設定的密碼超級簡單導致駭客輕易破解入侵，並且防火牆並無限制來源端的網段或 IP 存取。

C. 在現場封包側錄時候剛好遇到駭客連入 VNC 並進行網路狀態操作，追查來源端 IP 為是方電信所有，可能為駭客的跳板 IP。

D. 主機本身裝有 Apache 服務提供 Web DVR 的登入管理，就算輸入錯誤的帳號密碼，Web DVR 依然會條列出所有監視器 camera 的註解，若密碼被破解則監視器影像紀錄就可能被修改。

E. 建議主機管理員設置 VNC 和 Web DVR 的防火牆白名單，除了特定 IP 和網段能夠連入，其他一律拒絕存取。

F. 建議 VNC 和 DVR 的登入密碼每半個月更改一次，並且搭配數字、英文及符號來增強密碼安全。

G. 很多時候電腦中毒重灌之後依然再次發生的原因，很可能就是使用習慣照舊，軟體密碼防火牆的設定都要加強防護，全面性的審查才能降低再次被感染的風險。