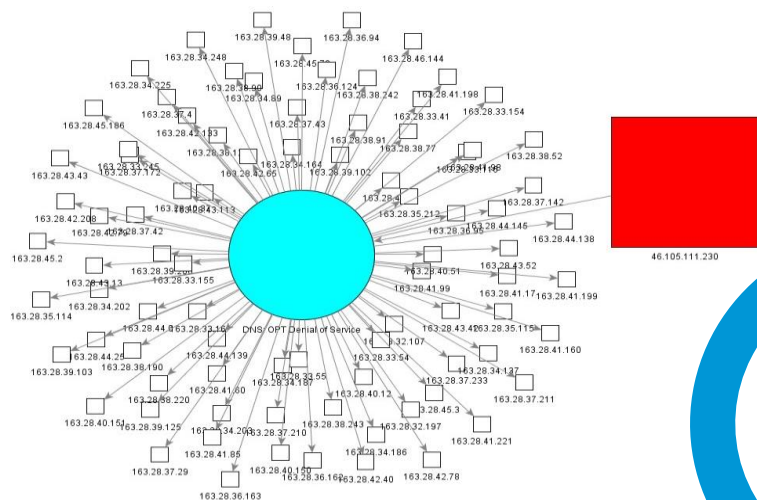


資安案例分析大綱

- DNS放大攻擊一直都在
- NAS 設備隱藏的資安風險
- 寬宏售票系統隱藏的資安風險
- 從相片複製指紋 駭客手法新知介紹
- 知名遊戲更新檔遭植入惡意程式
- 電子郵件社交工程案例

資安案例攻擊手法分析現場說明

DNS放大攻擊一直都在

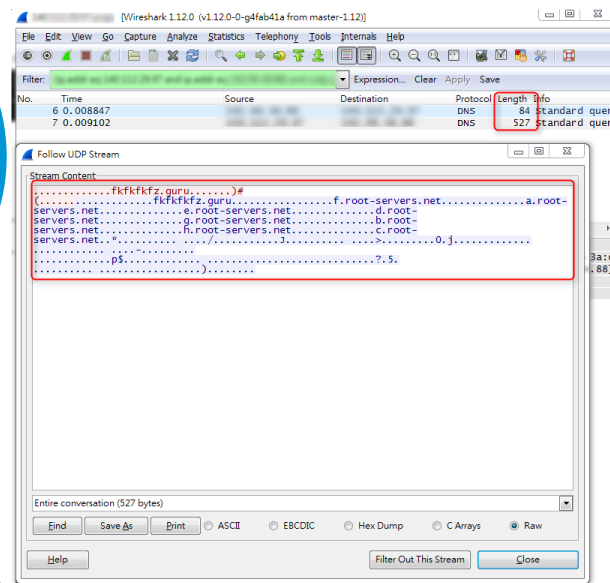


#偵測 目前各區網IPS仍偵測到為數不少的DNS放大攻擊事件

偵測

分析

防治



#分析 經北區ASOC團隊分析後，確認為DNS放大攻擊

攻擊者假造受害主機向未做好安全設定的DNS server發送大量UDP查詢封包，藉此阻斷DNS server正常服務，並塞爆受害主機網路頻寬。

建議設定ACL，僅允許符合ACL設定的網段進行遞迴查詢服務或限制單一IP的查詢次數，可大幅降低此類型的攻擊事件

國立臺灣大學計算機及資訊網路中心
Computer and Information Networking Center, National Taiwan University

北區學術資訊安全維運中心

Academic Security Operation Center

相關連結

- 台北區網中心
- 台北區網中心
- 桃園區網中心
- 南投區網中心
- 宜蘭區網中心
- 竹苗區網中心

技術文件

- Windows Server 2003 終止支援後防護之選 (已下載44次)
- ShellShock檢測與修補方法 (已下載346次)
- BOT H-Worm技術報告 (已下載368次)
- IE零時差弱點(CVE-2014-0322)簡介與防制 (已下載332次)
- 惡意公共無線熱點側錄帳號手法分析 (已下載840次)
- 手持移動裝置惡意程式分析方法簡介 (已下載1160次)
- 網頁主機目錄遊走攻擊-簡介與防制 (已下載605次)
- DNS amplification attack分析報告 (已下載407次)
- Personal NAS實安防護 (已下載33次)
- Windows XP終止支援後之防護策略 (已下載229次)
- Mudrop惡意程式簡介與防制 (已下載348次)
- OpenSSL技術報告 (已下載263次)
- 如何利用Windows Update 進行更新 (已下載294次)
- 勒索軟體CryptoLocker-簡介與預防措施 (已下載197次)
- Chargen放大攻擊分析與解決方案 (已下載613次)

#防治 透過撰寫相關分析報告，讓使用者了解相關攻擊手法同時提供相關建議措施達到宣導及防治之功效

NAS 設備隱藏的資安風險 (1/2)

#簡介

NAS為Network Attached Storage的縮寫，顧名思義為透過網路連結的資料儲存設備，可以讓不同區域的使用者透過網路來集中管理檔案，身兼多種功能，可以為檔案伺服器甚至影音串流伺服器。而設備本身作業系統多為Linux核心，一般來說，使用者只需要開機，即可透過網路來操作NAS(多利用web方式)。

現今的NAS設備已將相關設定大幅簡化，原先伺服器上繁雜的設定已不復存，使用者只需要將設備開機接上網路後，幾個簡單的步驟就可將設備上線。

也由於這種簡單易用的特性，加上一般使用者不容易察覺NAS所產生的異常流量，因此有許多新型態的攻擊便是針對NAS，其中一種手法就是透過最近相當熱門的Shell Shock漏洞，來執行未經授權的程式碼意圖感染NAS設備，若主機遭受感染，不但NAS上的機敏資料可能外洩，甚至會淪為攻擊者的跳板，不斷對外發送攻擊封包，異常流量可能導致區域網路的壅塞，影響整體網路環境運作。

接下來將就本月份於流量中所偵測到透過Shell Shock漏洞攻擊NAS設備的真實案例進行分析探討，亦希望藉此能讓使用者更重視NAS設備的安全性，定期的進行系統更新修補漏洞以避免受此攻擊風險影響。



#QNAP TS-869L 8-Bay NAS Server

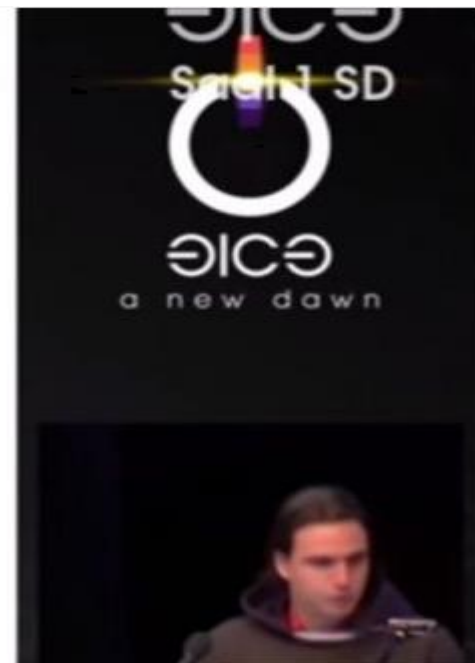


#LG N2B1 NAS SERVER WITH BLU-RAY BURNER



從相片複製指紋 駭客手法新知介紹

... und ich sage dir, wer du bist



在今年歐洲駭客年會上，來自德國的研究人員示範了利用一般的影像辨識軟體，從公眾人物參加公開場合的照片，成功擷取出指紋資料。生物特徵一向是被認為最難以複製的個人識別方式，並廣泛的應用在多種系統中，如iPhone及門禁系統等。在以往，若需要取得目標對象的指紋特徵時，大多需要透過物理接觸的方式，如目標所觸摸過的物品中，來取得指紋資料，此次於歐洲駭客年會中所發表的方式，是以拍攝高解析度的照片，再透過VeriFinger軟體分析，以數位方式取得目標指紋資料，這過程中，與目標完全不會有任何物理上的接觸，目標可能在完全未知情的情況下，就被取得個人生物特徵。研究人員以這種方式來讓大眾了解指紋辨識脆弱的一面，提醒大家沒有任何一項安全技術是牢不可破的，唯有透過多種驗證方式，才能提高安全性。

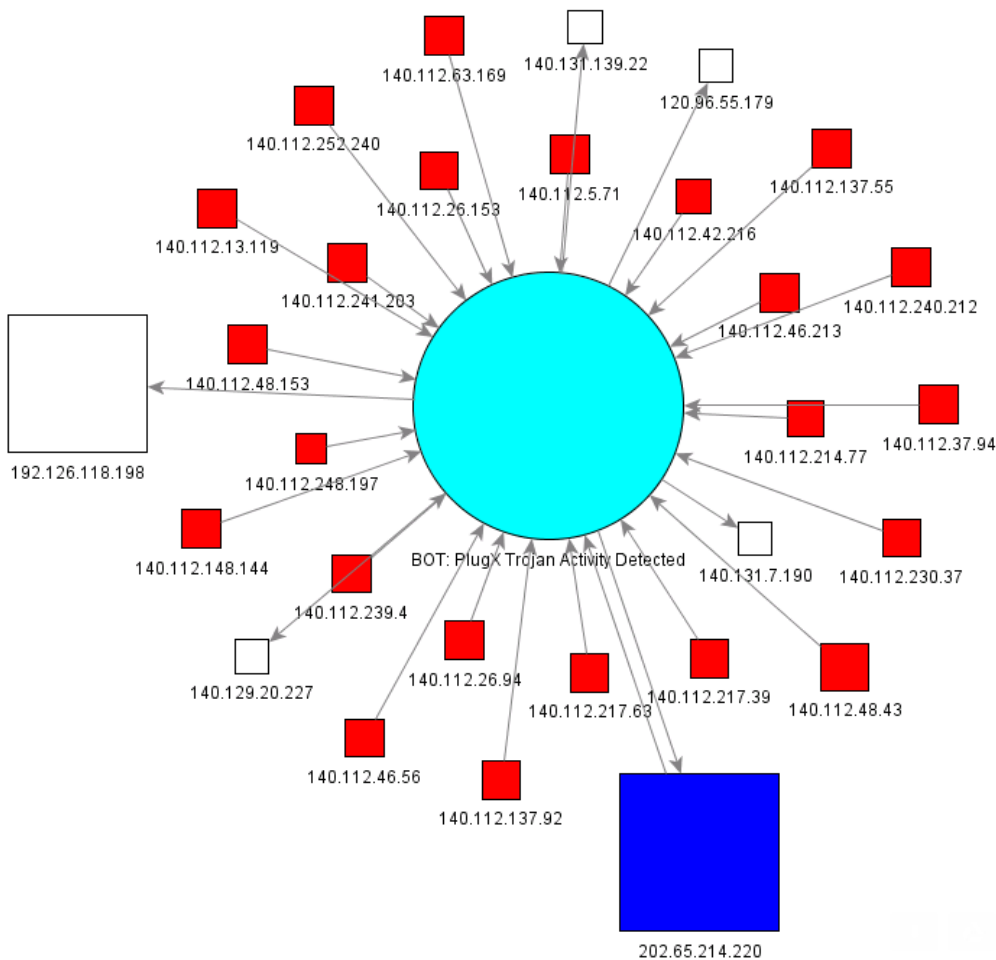


英雄聯盟及流亡黯道遊戲更新檔遭植入惡意程式

PlugX 木馬程式偵測

✓ 事件偵測說明

- 遠端存取木馬PlugX變種，為103年11月份台北區網最多的資安事件
- 疑似大規模感染
- 北區ASOC針對此惡意程式進行深入分析，透過封包及Sandbox分析，了解此惡意程式感染路徑及影響範圍



PlugX Trojan Activity Detected事件圖

電子郵件 社交工程攻擊(1/2)

➤ 偽造臺大差假系統通知電子郵件

林xx 教授您好！

有一筆申請單：

姓 名：陳xx

起迄時間：2015/04/07 13:00 ~ 2015/04/21 17:00

項 目：休假(國內)

正等候您進行線上簽核請點選或複製下列網址：

[請點選此連結](#)

若無法點選上述連結，請複製下列完整網址至瀏覽器：

<https://my.ntu.edu.tw/login.aspx?url=https://my.ntu.edu.tw/attend/ask.aspx>

進入差勤系統進行簽核。謝謝！

<http://mail.ntu.edu.linkin.tw/login2/p1.asp>

若要取消此類簽核通知信，請點選或複製下列網址：

[請點選此連結](#) 至「簽核作業」>「簽核通知Email設定」進行取消。

若無法點選上述連結，請複製下列完整網址至瀏覽器：

<https://my.ntu.edu.tw/login.aspx?url=https://my.ntu.edu.tw/attend/ask.aspx>

若有問題或意見，請依下列方式聯絡：

1. 教職員工、行政主管之操作或流程問題 請洽人事二組 Tel: (02)

33665942 <mailto:emailto%3Aperstwo@ntu.edu.tw>

2. 計畫人員、計畫主持人之操作或流程問題 請洽研發處計畫服務組 Tel: (02) 3366-

3267~9 <mailto:emailto%3Aeducenter@ntu.edu.tw>

3. 差勤系統問題排除 請洽計資中心 程式設計組 Tel: (02) 33665040 <mailto:emailto%3Aprog@ntu.edu.tw>

4. 帳號問題 請洽計資中心 作業管理組帳號室 Tel: (02) 33665016 <mailto:emailto%3Aacchelp@ntu.edu.tw>

電子郵件社交工程攻擊防護

➤ 技術層面

- 修補系統漏洞
- 安裝防毒軟體
- 關閉郵件預覽

➤ 行為層面

– 停、想、看

- 不隨意點選郵件中的連結
- 不隨意開啟郵件的附件檔案

➤ 請參考:

http://cert.ntu.edu.tw/Module/Security/social_engineering.php