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

N-ASOC DNS資安事件處理說明

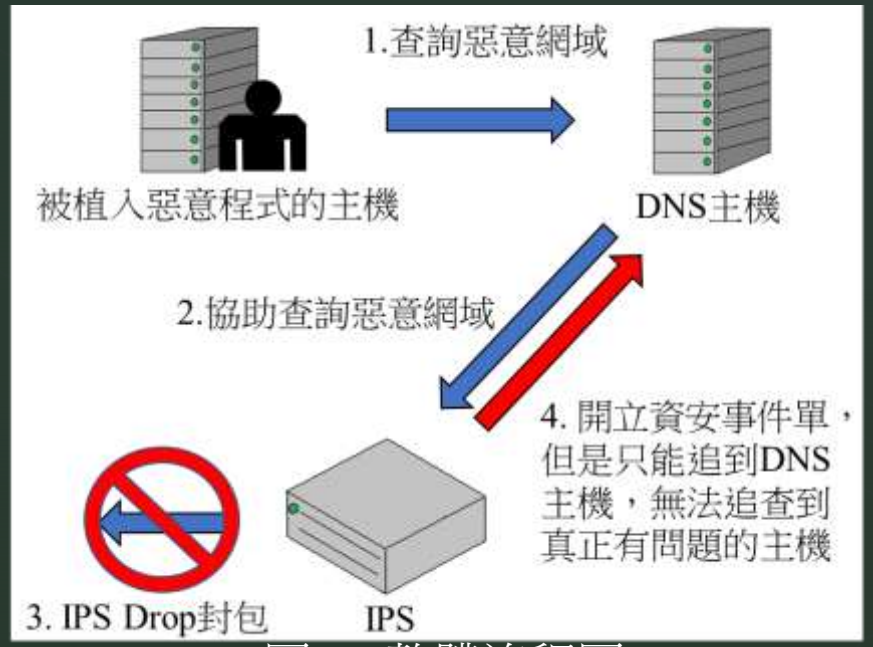
史賀文 shihewon@asoc.cc.ntu.edu.tw

林宜進 tjline01@asoc.cc.ntu.edu.tw

童鵬哲 lparrival@asoc.cc.ntu.edu.tw

前言

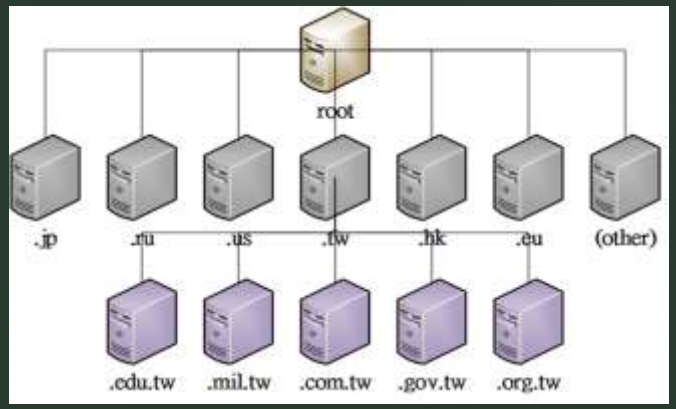
- 因DNS相關的資安事件處理較為困難，DNS主機可能因協助查詢惡意網域而觸發事件，但是DNS主機並非是問題來源，以至於回報為誤判事件
- 本文製作目的是讓區網老師理解IPS偵測機制和N-ASOC開單原則，並請區網老師協助查詢log記錄，以便後續追蹤資安事件，並非是誤判事件
- 本文內容有
  1. 網域名稱介紹
  2. 偵測機制
  3. DNS 資安事件處理說明
  4. DNS資安事件探討
  5. 參考資料



圖一: 整體流程圖

網域名稱介紹

- 網路上，由於IP(如：140.112.8.116) 不易記憶，因此改以有意義的英文網址作為紀錄 (如：www.ntu.edu.tw)，當使用者欲連線至網路時，再透過DNS 伺服器 (Domain Name System)查詢作為IP與網址間的轉換。
- 如網址：www.ntu.edu.tw (台灣大學)， 網域名稱可分類為tw (國家\區域)、edu (教育)、ntu (台灣大學)，由後往前分類各種不同的網域，且越往前範圍越小 (tw包含edu，edu包含ntu…等)。



圖二: DNS Server樹狀結構圖

偵測機制

- 目前IPS (入侵阻擋偵測設備) 針對惡意網域查詢，會以網域(domain name)為主要偵測機制並依情況搭配查詢頻率閥值作輔助(如：10秒內查詢10次)，如下圖。

Destination	Dest port	Protocol	Length	info
37.[redacted]	53	DNS	93	Standard query 0x2749 A send-monitoring.bit
8.8.8.8	53	DNS	93	Standard query 0x6753 A send-monitoring.bit
130.[redacted]	53	DNS	88	Standard query 0x75d1 A trumplines.bit
8.8.4.4	53	DNS	93	Standard query 0x534e A send-monitoring.bit
188.[redacted]	53	DNS	88	Standard query 0xbd11 A trumplines.bit
5.[redacted]	53	DNS	85	Standard query 0x5855 A updated.bit
62.[redacted]	53	DNS	84	Standard query 0xce95 A letit2.bit
188.[redacted]	53	DNS	85	Standard query 0x369f A updated.bit
62.[redacted]	53	DNS	84	Standard query 0x6e23 A letit2.bit
151.[redacted]	53	DNS	85	Standard query 0x98dd A updated.bit
217.[redacted]	53	DNS	85	Standard query 0xd68f A updated.bit
37.[redacted]	53	DNS	85	Standard query 0x8cd8 A updated.bit
8.8.8.8	53	DNS	85	Standard query 0xda72 A updated.bit
31.[redacted]	53	DNS	84	Standard query 0xead6 A letit2.bit
8.8.4.4	53	DNS	85	Standard query 0x16b7 A updated.bit
5.[redacted]	53	DNS	84	Standard query 0x59a2 A letit2.bit

圖三: 在wireshark上查看DNS封包

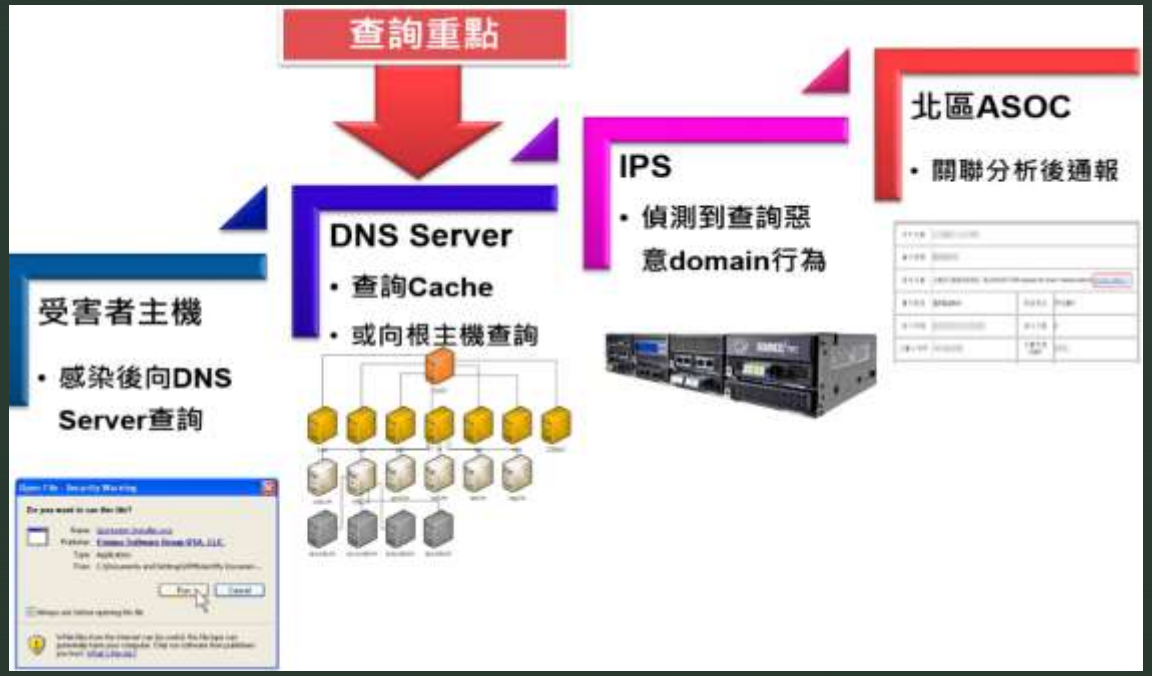
➢ .bit網域因已遭判定為**惡意網域**，因此關於.bit的DNS查詢，如：send-monitoring.bit、trumplines.bit…等，皆會觸發規則並形成資安事件。

DNS 資安事件處理說明

- 目前N-ASOC針對DNS資安事件之開立原則：
  - ✓ 開單目標：協助查詢之DNS主機、及使用者自行查詢 。
  - ✓ 開單規則：針對特定網域內之查詢，並依情況搭配查詢頻率閥值作輔助，進行開單。
- ◆ 本次將以DNS伺服器主機為主要探討範圍。

DNS資安事件探討

- DNS觸發資安事件主要以惡意網域查詢為大宗，其背後行為可能是疑似異常主機透過DNS查詢讓DNS主機觸發資安事件，並非為DNS主機自身問題。



圖四: 惡意domain query流程圖

DNS資安事件探討

- 如先前提到，使用者進行上網行為時，會先透過DNS主機進行網域查詢，因此N-ASOC並無法得知其背後真正使用者的IP。若欲追查問題來源，便須開啟DNS資料紀錄，以利追查使用者來源及了解其行為。
- 若欲解決DNS惡意網域查詢問題，除透過N-ASOC開立資安單之外，也須仰賴DNS管理人員進行log查詢，追尋來源使用者，以杜絕潛在的資安威脅。

參考資料

1. 北區學術資訊安全維運中心。DNS Amplification Attack: http://cert.ntu.edu.tw/Module/ASOC/openFile.php?id=6