

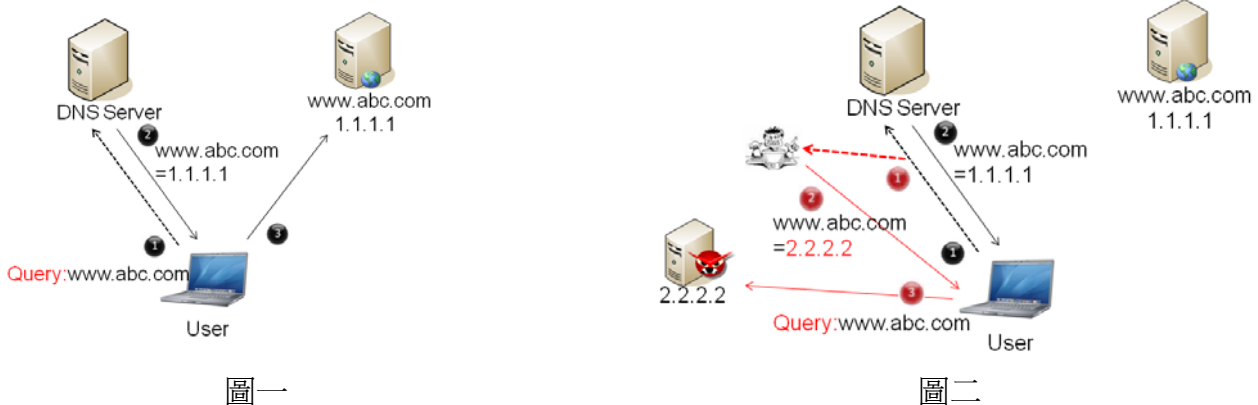
漫談內網資安管理(三)

作者: 葉華裔
捷宇網安股份有限公司 總經理
E-Mail:santayeh@netaxle.com.tw

攻擊技術皆為惡意？

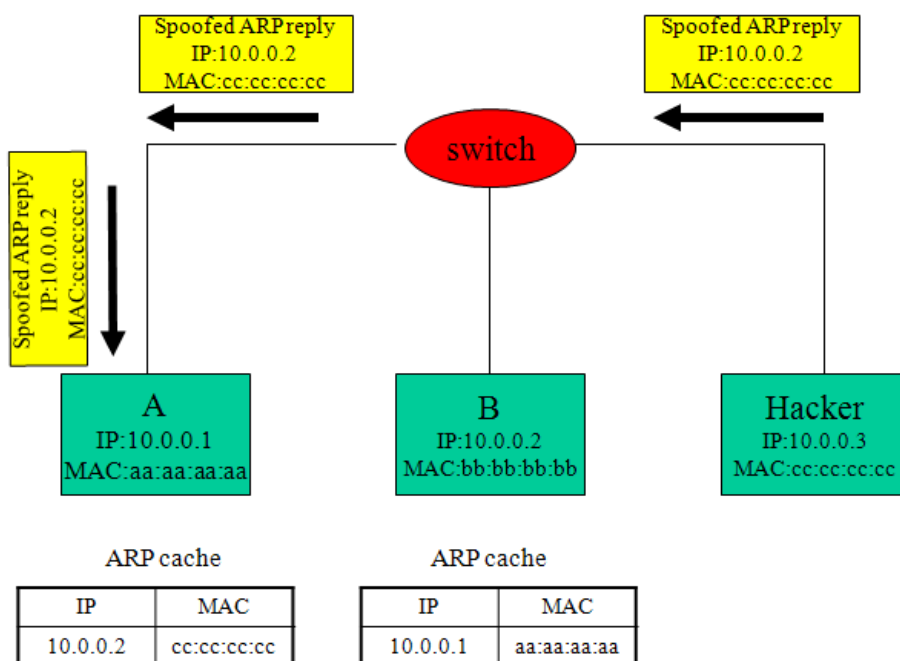
網路應用的發達與普及成就了許多的企業，然而也造成些許多困擾。網路攻擊與非法使用就是網管人員常常需要面對處理的兩大問題。網路攻擊種類眾多，甚至在 Internet 上就可下載各種不同的攻擊工具，例如 ARP Spoofing、Broadcast storming、DNS Hijack 等。

然而各種攻擊技術本身並無好壞之分，而是看使用人員將其應用在那個地方。以 DNS Hijack 而言，其目的是為改變主機名稱與 IP 位置對照，若依據正常的 DNS 運作模式其流程如圖一。若一個駭客可以攔截到使用者所發出的 DNS Query 封包，並在 DNS Server 回應前先回應一個假的回應封包，那就可以將使用者的存取導向到另一個網頁並進而進行一些詐騙手法(圖二)。



DNS Hijack 的運作原理與實作並不難，但有兩個重要關鍵因素：1、成功攔截到使用者的 DNS Query 封包；2、在 DNS Server 回應封包前先回應假 DNS Reply 封包給使用者。因此若能將 DNS Hijack 應用在使用者管控機制，當發現一個使用者為非法使用者則開始攔截其 DNS Query 封包，將其重導致告警網頁並顯示告警訊息，這樣一來 DNS Hijack 對網管人員而言不僅不是一種攻擊而是一種有用的工具。

ARP Spoofing 也是相同的道理。一般而言，網管人員聽到 ARP Spoofing 都認為是一種惡意的攻擊，用以欺騙或假冒他人的 IP，但若將 ARP Spoofing 應用在使用者控管機制上，有時也能保護網路的正常運作。例如：使用者 A 電腦的 MAC 地址為 MAC A，但不小心使用了他人的 IP 地址 IP B，此時只要在網路上利用 ARP Spoofing 方式向網路上其他使用者節點宣告 IP B 的 MAC 為 MAC B，則所有要傳送到 IP B 的封包就會傳送到 MAC B，因此使用者 A 就不會收到封包而認為網路已斷線。當然使用 ARP Spoofing 機制也有一些需注意的地方：1、非法使用者會一直送出 ARP 封包，所以必需持續使用 ARP Spoofing 干擾。2、ARP 封包只能在同一 broadcast domain 中運作。



圖三

除將攻擊技術轉而成為防禦方式之外，傳統的防禦方式還包括 Switch Port Shutdown、IP ACL、MAC ACL 等。當然每種方式各有優缺點，應用上也有其限制。

Switch Port Shutdown

Switch Port Shutdown 可說是最安全的防禦機制，因為一旦攻擊者的 switch port 被關閉後，攻擊者已完全失去網路連線，當然不可能再攻擊網路。然而 switch port shutdown 有一些要求和限制需配合與小心使用：1、Switch 設備需支援 SNMP 功能，如此才能將 switch port 成功 shutdown；2、在 shutdown Switch Port 時需能避免關閉到不該關閉的 port，例如 Uplink port 等。以現在網路普及的程度，管理的需求越來越重要，而 Switch 設備不僅功能越來越強且價格越來越平民，因此支援 SNMP 功能已不是大問題；然而在

越來越複雜的網路環境中要確保關閉的不是 uplink port 可不是一件簡單的事，因此 shutdown switch port 雖然是最安全的機制，但除非有很好的管理機制配合，最好小心使用。

Switch Port Shutdown 的另一個限制是攻擊者或使用者必需在可控制的網路環境中，若攻擊者是在遠處 Internet 中，當然就不可能將其 switch port 關閉。

IP ACL

在稍微高階的 Router 與 Switch 上都可看到 IP ACL 功能。IP ACL 可用來限制某一 IP 對網路的存取。

上面曾提到 Switch Port Shutdown 無法用來阻擋遠處 Internet 上的攻擊，但利用 IP ACL 就可簡單防止遠處 Internet 上的攻擊。但若是使用在區域網路使用者控管環境中，IP ACL 可能就不是那麼適合使用。例如：使用者 A 的合法 IP A 被使用者 B 盜用，此時若使用 IP ACL 方式將 IP A 阻擋掉，使用者 B 雖然無法使用網路，但對合法使用者 A 而言也一樣無法使用 IP A 上網。

MAC ACL

特定的 Router 與 Switch 才會支援 MAC ACL。與 IP ACL 不同的是，MAC ACL 是以 MAC Address 做為阻擋的依據。

一般的攻擊使用偽冒的 IP 較多，較少使用偽冒 MAC 地址，因若能針對 MAC 做 ACL 就能提供較好的保護。以上例使用者 A 的合法 IP A 被使用者 B 盜用，雖然不能使用 IP ACL 將 IP A 阻擋，但若能使用 MAC ACL 將使用者 B 的 MAC B 阻擋掉，就能成功的防止非法使用者，同時合法使用者 A 依舊可使用網路。

然而能支援 MAC ACL 的設備不多，Extreme Switch 是少數中的特例可以支援 MAC ACL；此外，MAC ACL 只能使用在 Layer 2 的環境下。

一招半式走天下

不論是 DNS Hijack、ARP Spoofing、Switch Port Shutdown、IP ACL、MAC ACL 都各有優缺點：其中 Switch Port Shutdown、IP ACL、MAC ACL 是必需要相關設備的支援，而

DNS Hijack 與 ARP Spoofing 反而較不受設備影響，因此可能會有種假象，感覺其適合用在使用者控管中的防禦機制，然而實際分析後，可能會另人大失所望。

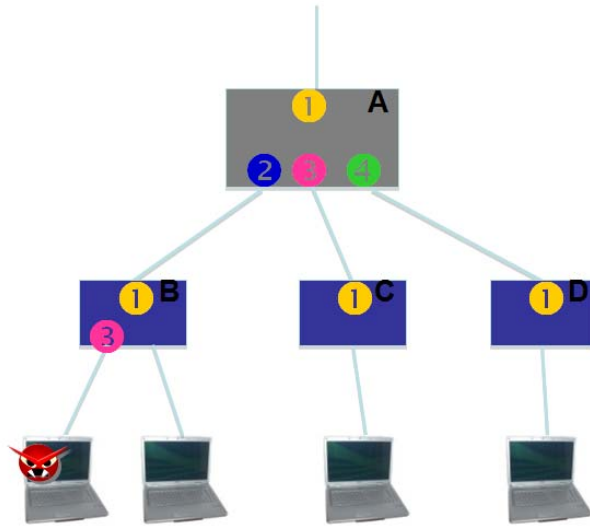
以 DNS Hijack 而言，當初駭客使用此方式的目的是為了重導使用者到非法網站以進行詐騙。但前提是必需要攔截得到使用者的 DNS Query 封包，然而現今的作業系統都會使用 DNS Cache (例如在 windows 下可執行 ipconfig/displaydns 即可看到 DNS Cache)，因此使用者不一定會對外發出 DNS Query，就算使用者送出 DNS Query 封包，由於 DNS Query 是 unicast 封包，所以要攔截還不是那麼簡單。再者 DNS Hijack 必需在合法 DNS Server 回應前先送回假冒的 DNS Reply 封包，這也不是簡單的事，因為回應的快慢往往不是只看距離遠近，還包含處理效能；若 DNS Hijack 主機效能稍差，延遲個 0.1 秒可能就使攔截失敗。

因此 DNS Hijack 成功的機率可能不大，但對駭客而言，千分之一的成功率可能就已能得到很大的好處；但若將 DNS Hijack 用於使用者管控的防禦機制，千分之一的成功率，網管人員可能就等著罰站了。

對使用 ARP Spoofing 做為防禦機制而言，除之前所提限制外，也需考慮使用環境與人員。一般會使用 ARP Spoofing 防禦機制，前提都是假設網路內的所有使用者都是善良合法的使用者，其對 IP 與網路的使用知識沒有那麼了解，因此若會盜用他人 IP，一定是不小心設錯，此時只要使用 ARP Spoofing 影響使其無法正常使用網路，使用者必會察覺可能是 IP 地址設錯，進而將 IP 更正。

然而若網路中存在有一個惡意的使用者，ARP Spoofing 防禦機制反而可能適得其反。舉例來說，一個使用者從網路上取得一個 ARP Spoofing 程式，發送了 10 萬筆假冒的 ARP 封包，其目的只是為了影響或攻擊網路而不是需要網路的存取，但在 ARP Spoofing 防禦機制中看到了 10 萬筆非法 ARP 封包，防禦機制自動以 ARP Spoofing 反擊回去，且為有效防禦其反擊封包為 10 倍數攻擊封包，因此防禦機制送出了 100 萬筆反擊封包。可想見的，這 110 萬筆封包對網路的影響有多大，對惡意使用者而言，其目的本身就是攻擊網路而不是存取網路，因此這 100 萬筆反擊封包對惡意使用者毫無影響；但是原本惡意使用者擔心 10 萬筆非法封包無法攻擊癱瘓掉網路，但因為防禦機制送出了 100 萬筆反擊封包反而可能使網路因此而癱瘓。

Switch Port Shutdown 最困難的地方在於如何精準的確定攻擊者所連接的交換器與連接埠。以最常見的網路架構為例，一個攻擊者真正連接設備為 Switch B 的第 3 埠(圖四)，然而利用網路查詢的方式卻會發現攻擊者連接在 Switch A 的第 2 埠，Switch B 的第 3 埠，Switch C 的第 1 埠與 Switch D 的第 1 埠，原因在於攻擊者的資訊也會出現在其他交換器的 uplink 埠上。所以若不能精確判斷最終端連接設備而不小心將交換器的 uplink 埠給關閉，那影響的層面就非常廣泛且嚴重。



圖四

IP ACL 與 MAC ACL 也面臨同樣的問題—是否可精準的確定攻擊者所連接的交換器。假若不能精準的確定攻擊者所連接的交換器，那 ACL 應該下在那台交換器上呢？有一個較為投機的方式，把 ACL 下在每台交換器上，反正總有一台是對的。但使用這種投機方式要注意一點，若網路上的攻擊太多或有惡意使用者製造攻擊可能會造成在交換器上執行了太多的 ACL 指令，輕則降低了交換器效能，嚴重者更可能造成交換器停擺，可就變成更大的問題了。

沒有任何一種防禦機制是百分百完美，因此想靠一招半式走天下絕不可能，唯有組合多種防禦機制，依不同環境與條件使用不同機制才能提供較佳的解決方案。