



臺灣大學計算機及資訊網路中心電子報

投稿日期	民國 105 年 2 月 18 日	編 號	請空 白
投稿類別	<input type="checkbox"/> 校務服務 <input checked="" type="checkbox"/> 技術論壇 <input type="checkbox"/> 專題報導		
題目標題	WordPress Pingback DDoS 攻擊分析		
摘要	<p>駭客團體「匿名者」亞洲支部 (Anonymous Asia) 於 104 年 7 月 30 日，針對教育部網站進行 DDoS 攻擊，分析其攻擊流量發現 WordPress Pingback 為攻擊手法之一。</p> <p>本技術報告分析 WordPress Pingback 擊擊手法，並提供相關建議之防禦措施。</p>		
姓名	李美雯		
服務機構/ 職稱	臺灣大學計算機及資訊網路中心		
聯絡電話	0233665010		
電子郵件 信箱	mli@ntu.edu.tw		
聯絡地址	106 台北市羅斯福路四段 1 號		
備註			

WordPress Pingback DDoS 攻擊分析

臺灣大學計算機及資訊網路中心程式設計師
作者：轉載自臺灣大學計資中心北區學術資訊安全維運中心

高中課綱微調引發教育部網站遭 DDOS 攻擊

教育部於 103 年初推動高中課綱微調，計畫 104 年 8 月 1 日正式上路，由於高中課綱微調之相關資訊未公開，加上部分內容引發爭議。反對課綱微調的學生在教育部、立法院前抗議，並要求政府相關人員出面說明。

臺灣反課綱微調抗議行動也引起知名駭客團體「匿名者 (Anonymous)」的關注，「匿名者」亞洲支部 (Anonymous Asia) 於 104 年 7 月 30 日在社群網站上 (目前已遭關閉，下圖 1 所示) 發文聲明將支持臺灣的反課綱微調抗爭行動，對相關的政府機關組織進行網路攻擊。

「匿名者」(Anonymous) 為聲援反課綱微調行動，在發表聲明後，接著對多個政府部門網站發動網路攻擊，此次攻擊行動癱瘓了包含教育部、經濟部、國民黨等多個政府部門在內的網站，主要目的要影響網站正常運作，讓這些網站無法正常對外提供服務。

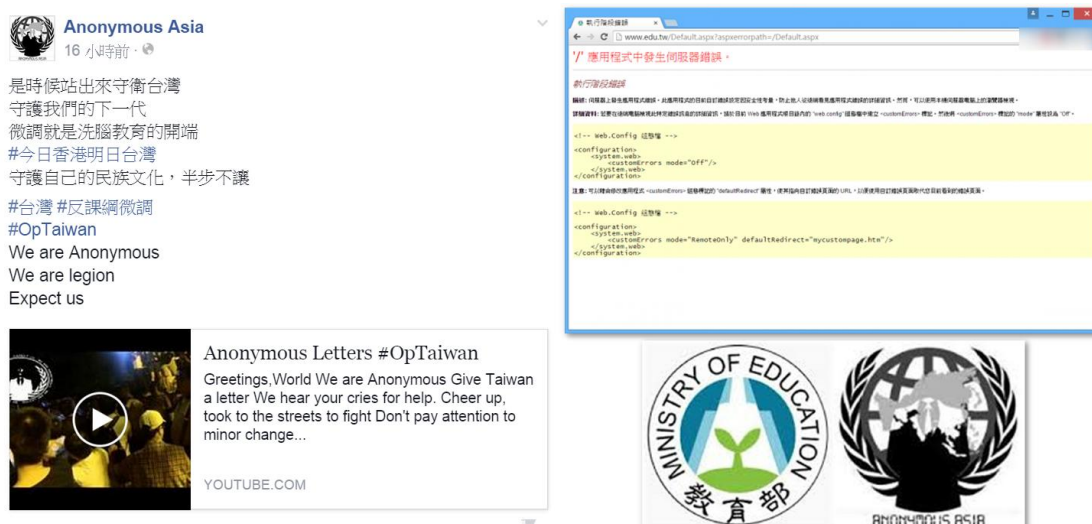


圖 1

分散式阻斷服務攻擊(DDoS, Distributed Denial Of Service)

DDoS (Distributed Denial of Service) 分散式阻斷服務攻擊是 DoS (Denial of Service) 阻斷服務攻擊的進階版。DoS 是一種明確且惡意的網路攻擊手段，攻擊者利用各種方式對目標主機發送大量封包，並要求目標主機傳送回覆訊息，使得目標主機的網路資源或系統資源耗盡，進而使得目標主機無法提供服務或主機管理者無法存取使用網路資源。

而 DDoS 則是指分散式的 DoS 行為的集合，此種攻擊手段建立在 DoS 的基礎上，同時利用了分散於各地的主機（這些主機許大多都是被攻擊者攻陷的電腦，通稱為「肉雞」或「殭屍」主機）來組成所謂的殭屍網路以發動大規模的 DDoS 攻擊，這種攻擊除了可以癱瘓目標主機的網路，有心人士甚至可以利用它進行惡意的商業活動或是政治行為，像是攻擊商業上的競爭對手、癱瘓投票網頁等等。

簡而言之，DoS 屬於一種利用自身主機攻擊目標主機（一對一或一對多）的惡意行為，而 DDoS 攻擊則是一種使用各種方式操作及利用多台主機攻擊癱瘓目標主機（多對一或多對多）的惡意行為。

舉例來說，某家餐飲業者只有電話外送的服務，同行為了打擊此競爭對手，於是負責人瘋狂撥打此餐飲業者的訂餐電話（即為 DoS 行為），造成其他客人無法撥打電話進來進行訂餐的服務，餐飲業者也無法對上游廠商撥打電話訂購原物料，此時這家餐飲業者就有可能被誤以為已經沒有營業或是其他原因而惡性倒閉（DoS 目的）。同上面的狀況，若是負責人雇用了多名人手進行同樣撥打電話的惡意行為，則延伸為所謂的 DDoS 行為。

前面所提到的 DDoS 攻擊手法屬於早期常見的直接性的 DDoS 攻擊，但隨著攻擊手法的演變，現在也出現了所謂的反射性的 DDoS 攻擊。

直接性的攻擊最為常見且明確，主要就是利用消耗頻寬或資源的手段，來達成使用者無法存取網路資源的目的。而反射性的攻擊，則是攻擊者利用已經被控制的多台殭屍電腦，在成功偽照目標主機的 IP 位址後，對多台管理不夠嚴謹之主機發出詢問封包並要求回覆，而這些被詢問的主機群回覆大量封包給偽照 IP 位址時，造成真正的目標主機接收到來自四面八方大量的回覆封包，進而造成放大且反射的攻擊效果。這種方式也能達到 DDoS 放大攻擊的效果，造成目標主機無法正常存取網路資源，並增加攻擊者被追查到的難度。

DDoS 手法-WordPress Pingback

這次反課綱微調引發的攻擊，除了較為知名的 Torshammer 以外，也參雜了利用參考或連線 WordPress 網站回報的 Pingback 功能進行 DDoS 攻擊。

Pingback 是 WordPress 中內建的功能之一，當有人引用文章時，此功能可以用來通知作者相關資訊。在此次的教育部攻擊事件中，此功能卻遭有心人濫用成為 DDoS 的攻擊手法。

Pingback 的功能本意上是希望當網路上的文章彼此交流時，能有一個互相告知的機制，但是惡意攻擊者利用此機制，偽造受害主機的 IP，並針對大量預設開啟 Pingback 的 WordPress 主機，透過特製的 XML-RPC 內容發送請求（圖 2 編號 1），利用 Pingback 的功能對受害主機發出大量 HTTP Request 封包（圖 2 編號 2），藉此達到 DDoS 的攻擊效果。

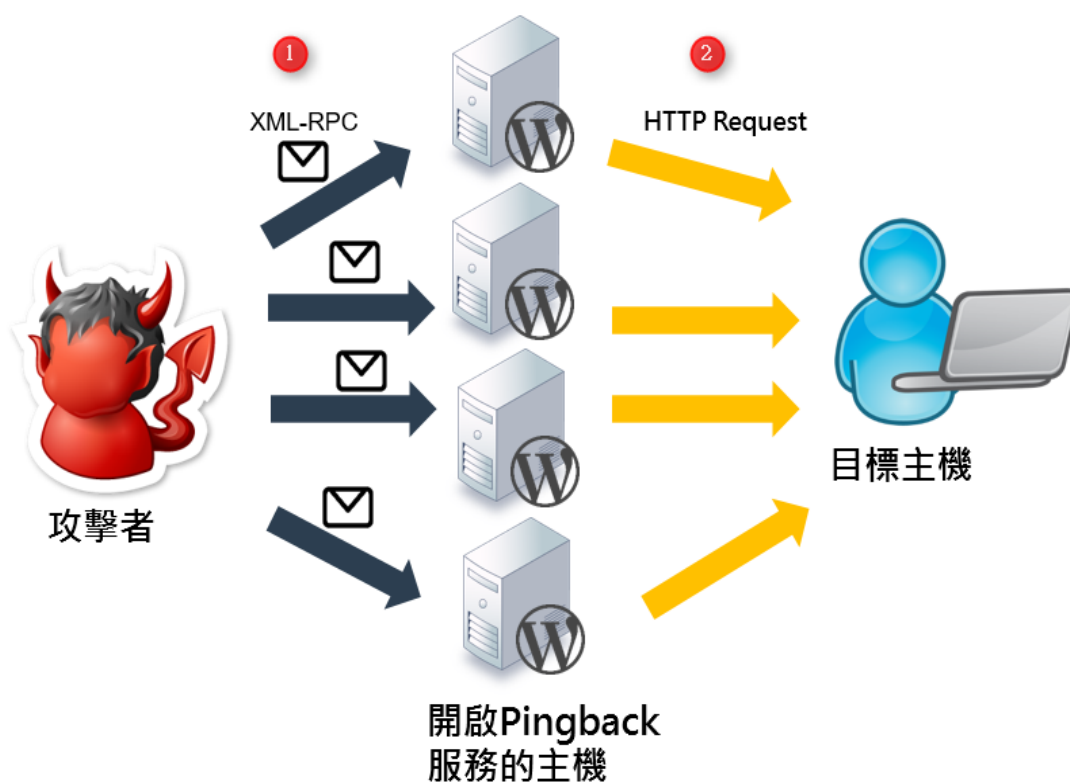


圖 2

為了深入了解其運作機制，我們側錄 WordPress 使用 Pingback 功能時得到的封包資訊(如圖 3 所示)並說明如下。惡意攻擊者會置換編號 1 中黃底標記的 IP，並向一組或多組的紅底標記 IP（開啟 Pingback 功能的 WP 網站）發送引用文章的請求（特製的 XML-RPC 內容）。此時，紅底標記 IP 的 WP 主機便會對受害主機發出大量 HTTP Request 封包，達到 DDoS 的攻擊效果。

對於網路管理者而言，需特別注意封包中編號 2 綠底標記的「Pingback.ping」

字串，此字串是針對此類型攻擊進行封包過濾的最佳判斷依據。除了這部分，編號 3 藍底標記部分則是有關引用網站（受害主機）的文章網址資訊；橘底標記部分則是有關被引用網站（WP 主機）的文章網址資訊，網路管理者對於此類型之攻擊防禦時，可特別注意這些細部資訊，以確認其攻擊類型進而採取有效防禦措施。

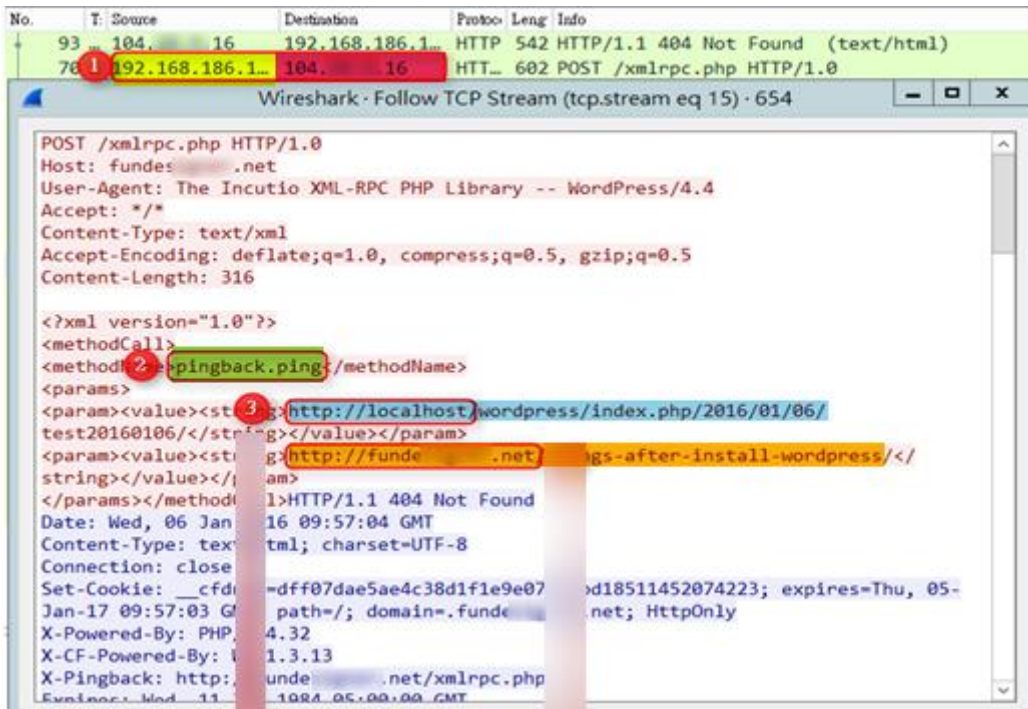



圖 3

管理者的整體資安建議

現今很多工具都可以測試網站是否含有 Pingback 的相關漏洞，建議使用 WordPress 的管理者，若是要避免淪為 DDoS 的一員，請採取下列措施：

1. 關閉網站的 Pingback 功能。



討論設定

預設文章設定

- 試著去通知文章中鏈結到的任何網誌。
- 允許其他網誌傳送引用通告至新文章
- 允許他人對新文章發表迴響

(這些選項可以在發表文章時個別調整。)

其他迴響選項

- 發表迴響者必須輸入姓名及電子郵件
- 使用者要註冊並登入才能發表迴響
- 14 天之後自動關閉文章迴響
- 啟用階層式迴響，5 層深
- 將迴響分頁，每頁 50 則首要迴響，預設顯示 最後 頁

每頁應將 較舊 的迴響顯示在上方

2. 刪除 xmlrpc.php 。

3. 下載 WordPress 官方網站所提供的修補套件：

<https://wordpress.org/plugins/disable-xml-rpc-pingback/> 。

4. 升級 WordPress 至最新版本。

針對阻斷式服務攻擊的防禦方式，通常透過封包深入檢測，讓正常合法的封包通過，並阻擋非法的網路流量。通常在得知攻擊方式後，可以嘗試瞭解利用何種類型的協定攻擊，並封鎖相關埠號，藉以達到阻隔攻擊流量之目的，此種方式雖較粗糙但卻是基本處理原則。有工具互相搭配為佳，相關工具列舉如下：

(1) 防火牆(Firewall)

防火牆可以設置一些簡單的規則來阻擋或允許特定的通訊協定、IP 及 Port。但防火牆規則通常較為簡單，無法防禦較為複雜的攻擊方式，如果設定得不恰當，也有可能阻擋正常的流量，造成服務無法正常運作。

(2) 交換器(Switch)、路由器(Router)

一般來說，多數的交換器與路由器都有一定的 ACL 及速率的限制功能，但是普通的路由器卻很容易因為 DDoS 的攻擊而影響效能。這時可以使用防火牆或是 Router 上的入口過濾功能，利用此功能，可以將不符合規則的封包阻擋在 Router 之外。這種方法或許可以限制自身主機對外連線的能力，以避免成為對外發起間接攻擊的主機，但卻較難阻擋內網發起的間接攻擊。

(3) 阻斷服務防禦系統(DDS based defense)

阻斷服務防禦系統(DDS, DoS Defense System)除了可以辨識並阻擋以連線方式進行的 DDoS 攻擊，它也可以辨識以通訊協定式 (像是 Ping of death) 及頻率式(Rate-based) 的攻擊。

(4) 異常網路流量清洗系統

這種防禦方式是將可疑的異常網路流量導入「洗滌中心」或是「清洗

中心」，經過應用層的進階檢查後，透過 GRE Tunnels 或 BGP FlowSpec 等方式將流量區分出正常及異常的網路流量，將異常的封包丟棄，再將正常的網路流量導回目的地。

除了上述所採取的防範方式，也建議伺服器的相關管理者可以進行一些預防性措施。除了關閉伺服器沒有使用到的 Port 以阻擋不必要的連線以外，也可以管控內部對外可用之網路流量，並預留一些網路頻寬以便發生網路攻擊時可調配使用或應變措施。

DDoS 攻擊涉及法律相關問題

《刑法》第 358 條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

根據《刑法》第 359 條規定，入侵後如「取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人時，可處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

入侵電腦或癱瘓網站（如本次多個政府網站遭癱瘓）的行為，可能觸及刑事違法，即使不在我國發動攻擊，只要受害的電腦或網站在我國境內，即有觸法的疑慮。

參考資料

1. 蘇文彬。2015-08-03。「匿名者」聲援反課綱微調行動，教育部、國防部、經濟部等網站陸續遭攻擊。iThome。網址：
<http://www.ithome.com.tw/news/97854>。上網日期：2015-12-28。
2. 李貴敏。2015-08-04。《貴在立法》國內網站遭入侵 國際駭客也有罪。卡優新聞網。網址：
http://www.cardu.com.tw/news/detail.php?nt_pk=22&ns_pk=27000。上網日期：2015-12-28。
3. 洪海，曹志華，鮑旭華（2014.07）。DDoS 分散式阻斷服務攻擊深度解析（初版）。臺北市：碁峰資訊。