教育機構ANA通報平台

|  |  |  |  |
| --- | --- | --- | --- |
| 發佈編號 |  | 發佈時間 |  |
| 事故類型 | ANA-攻擊預警 | 發現時間 | 2015-08-06 09:04:41 |
| 影響等級 | 高 |  |  |
| [主旨說明:]【攻擊預警】近期發生政府機關遭網路攻擊事故，促請各會員提高警覺，注意防範 | | | |
| [內容說明:]  轉發國家資通安全會報 技術服務中心 漏洞/資安訊息警訊 ICST-ANA-201508-0001  近期發生政府機關遭阻斷式服務攻擊，癱瘓網路或系統資源。其中自稱為「Anonymous Asia」駭客組織活動頻繁，從跡象顯示，下一波攻擊對象會以民生系統與網站入侵為主，該組織於104年7月31日起，陸續於網路上公布攻擊情形，並表示此一事故僅為一連串攻擊行動的開端。促請各會員提高警覺，注意防範。  目前已知攻擊手法如下：  [1] 攻擊者透過利用TOR匿名網頁瀏覽及訊息傳遞服務隱藏來源，並進一步發動大規模DDoS攻擊。目前已知TOR使用之IP列表請參考以下網址 [https://torstatus.blutmagie.de/，請各會員進行相關偵測與阻擋作業。](https://torstatus.blutmagie.de/%EF%BC%8C%E8%AB%8B%E5%90%84%E6%9C%83%E5%93%A1%E9%80%B2%E8%A1%8C%E7%9B%B8%E9%97%9C%E5%81%B5%E6%B8%AC%E8%88%87%E9%98%BB%E6%93%8B%E4%BD%9C%E6%A5%AD%E3%80%82)  [2] 攻擊者租用Amazon雲端主機 52.76.1.116，大量連線至目標網路以發起DDoS攻擊。  [3] 攻擊者利用WordPress套件中「Pingback」漏洞進行攻擊：駭客使用Pingback漏洞進行DDoS攻擊時，封包中會帶有固定特徵字串 “verifying pingback from”，可於應用程式防火牆/IPS過濾包含此字串的封包，以避免遭受此類攻擊。  [4] 亦有發現零散IP參與癱瘓政府機關網站之攻擊行為，IP列表請詳見網址：[http://cert.tanet.edu.tw/pdf/ip.txt。](http://cert.tanet.edu.tw/pdf/ip.txt%E3%80%82)  目前已知有明確受害情勢，請各會員加強監控並留意網站連線狀況，以防止遭受相關攻擊。    此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發。 | | | |
| [影響平台:]  所有平台 | | | |
| [建議措施:]  1. 請各會員針對上述主要攻擊IP位址進行阻擋，建議優先針對TOR網路位址(<https://torstatus.blutmagie.de/>)進行阻擋，並加強網路監控與相關防範。  2. 請SOC會員持續監控客戶網站連線、帳號登入等使用情形，如發現針對民生系統客戶攻擊之狀況，請立即通知技服中心。  3. 請NCC-ISAC 與 A-ISAC 通知所轄單位若發現針對民生系統攻擊之狀況，應依循通報機制向通傳會與教育部通報。 | | | |
| [參考資料:]  Pingback 攻擊說明：  <http://john.cuppi.net/blocking-wordpress-pingback-ddos-attacks-with-nginx-and-apache/> | | | |

|  |
| --- |
| (此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的 內容有疑問或有關於此事件的建議，歡迎與我們連絡。 |
| 教育機構資安通報應變小組 網址：<https://info.cert.tanet.edu.tw/> 專線電話：07-5250211 網路電話：98400000 E-Mail：[service@cert.tanet.edu.tw](mailto:service@cert.tanet.edu.tw) |