

比網釣更可怕

全球 DNS 伺服器

將面臨被 Pharming 下毒的風險

避免 Pharming 攻擊 5 大方法

項目	觀察重點	注意事項
1	稍覺怪怪的網頁	Pharming 網頁多多少還是會與合法網頁會有些許的差別
2	要求太多不必要動作的網頁	Pharming 網頁多半會對受害者要求填寫一些額外的個人資訊或機密的行為
3	瀏覽器上沒有 SSL 安全鎖	只要是合法網址一定會對整個對話流量做 SSL 加密動作，所以只要是瀏覽器上沒有 SSL 安全鎖，那就可能是 Pharming 網頁
4	網址列中無法顯示 https://	只要是安全的網上，瀏覽器的 URL 網址列中會包含 https:// 的提示字元。但在 Pharming 網頁則沒有，而且只會秀出 http://
5	瀏覽器跳出 SSL 憑證錯誤警告訊息	只要是遇到冒用 SSL 憑證的假網頁，瀏覽器就會發出警告訊息

資料來源：Fortinet 提供，電子時報整理，2005/6

製表：曹乙帆、柯博偉

(記者曹乙帆/台北) 在網路釣魚 (Phishing) 搞得全球雞犬不寧的同時，另一隻系出同門的網路轉接 (Pharming) 更造成全球網站的一片恐慌，Pharming 最大的特點就是透過直接篡改網域名稱系統 (Domain Name System; DNS) 的手法，將連結到合法網址的使用者被轉接到假網站上。面對此一新興威脅，多功能閘道器商 Fortinet 並於網站上，正式對外發佈揭露 Pharming 網址的 5 大方法。

據 Fortinet 表示，Pharming 可說是網路釣魚的另一種更精緻手法的延伸，也就是專門針對 DNS 伺服器展開混合式攻擊的一種全新攻擊手法。Pharming 與網路釣魚的攻擊手法完全不同，後者是透過誘騙的方式，讓「願意上鉤」的使用者進入到與合法網站長相幾乎一樣的假網站中，然後再誘騙使用者填寫一些個人機密資訊。但細心的使用者可以發現網釣的假網站網址是與合法網站不一樣

的，所以只要在瀏覽器中輸入正確網址即可破解。

但 Pharming 卻不一樣，駭客會採取謂「DNS 快取記憶體下毒」(DNS Cache Poisoning) 的手法展開對 DNS 伺服器的攻擊，同時向其他 DNS 伺服器提供造假的資訊。Pharming 會將原先連接到合法網址的使用者，不知不覺導入到駭客映射自原合法網站的假網頁中，即使使用者跳過連結，直接輸入正確網址仍然會被導入到假網站中。

在一些 Pharming 攻擊事件中，終端主機會在不知不覺的情況下，被植入木馬或間諜程式，並且受到擊鍵側錄或網址轉向等攻擊。對此，Fortinet 宣稱，透過 Fortinet FortGate 整合式安全設備所提供的動態防火牆規則、防毒與入侵防護等功能，可以保護 DNS 伺服器並阻擋 Pharming 攻擊。為了消弭 Pharming 攻擊持續不斷昇高的威脅，Fortinet 並對外發佈 5 大檢視與揭露 Pharming 網址的方法。