麻煩射擊 Troubleshooting - Wordpress 或其它網站被自動轉址到釣魚網站

scicube602 - 2025-04-04 - Troubleshoot

因爲曾經嘗試搜尋過Google好像完全沒有類似的解決方案教學(有的都是叫你買服務)，所以嘗試寫一次，但請留意

- 以下內容主要針對自動轉址的問題，衍生的其它問題(例如File Injection)並未有提及
- 如果有網站發生自動轉址到釣魚網站的問題，用戶應該第一時間聯絡我們處理以免持續惡化以及確保最壞情況下我們可以透過備份還原解決。
- 沒有把握完全解決問題的話我們**”不建議”**客戶自行處理，因爲這樣會影響檔案修改時間，令我們不能查找網站漏洞源頭

自動轉址到釣魚網站的成因

- 經FTP修改檔案 – 這個可以透過更改密碼直接解決

- 網站安全漏洞 – 例如使用舊版本的Wordpress及其Plugin

理論上一星期內發生的改動我們都可以翻查。

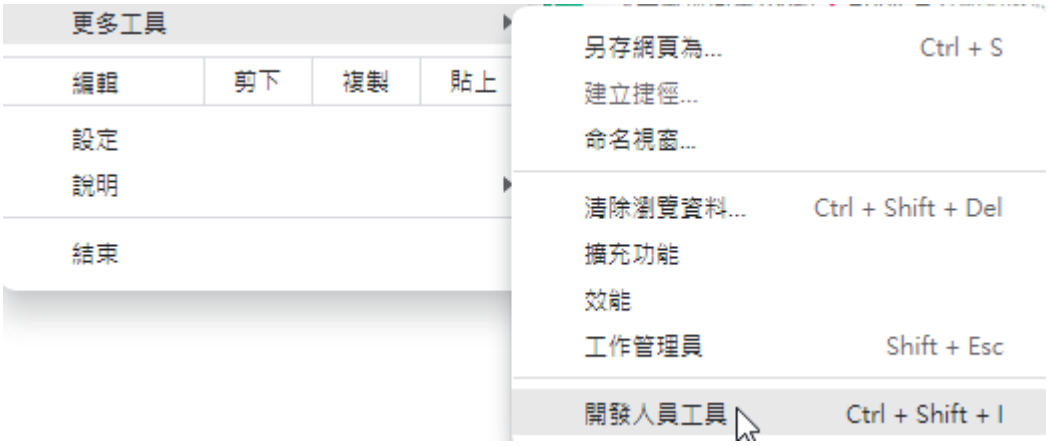
如何避免？

世界上沒有100%避免網站被入侵的辦法，只有相對安全。

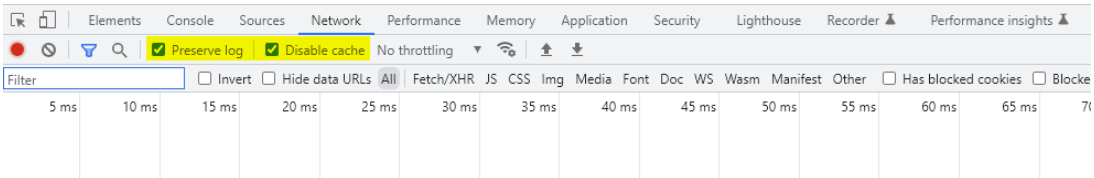
- 如果使用開源軟體(如Wordpress)，請確保有定期更新。尤其買回來的，未必會有提供自動更新
- 請勿使用免費，但其實需要授權的付費plugin/theme.....
- 定期備份確保在最壞情況下有後備方案作還原程序
- 盡量避免一個戶口寄存多於一個域名避免交叉感染，尤其多用戶計劃，虛擬主機及獨立主機可以建立子用戶的服務計劃，我們強烈建議一個用戶一個域名。
- 網頁寄存客戶預設有Web Application Firewall部署，一旦出現入侵情況我們可以進行詳細掃描。
- 虛擬主機及獨立主機沒有提供Web Application Firewall，但我們有代辦購買及安裝服務，單次收費爲HK$500 ，請參考（ https://www.configserver.com/cp/cxs.html ），如需要購買請電郵到 info@scicube.com 。

追蹤轉址來源

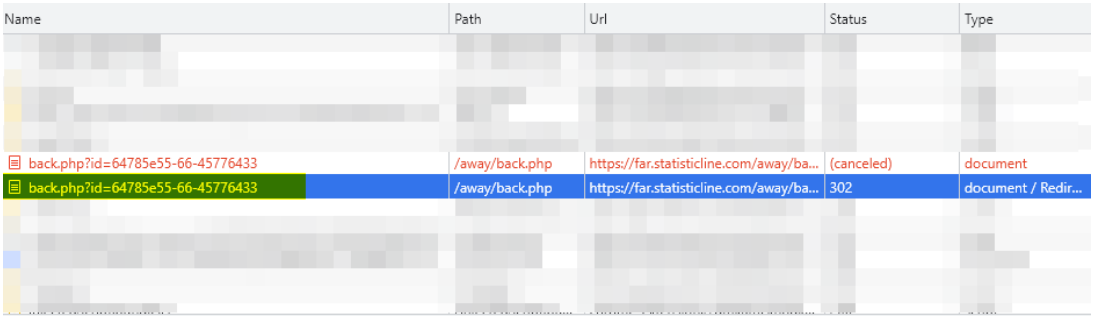
1) 使用Google Chorme啓用Developer Mode



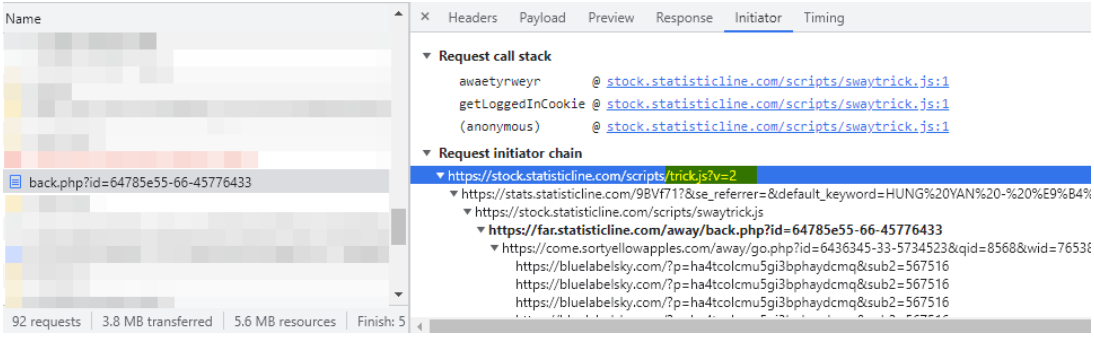
2) 在”Network”，啓用Preseve Log及Disable cache



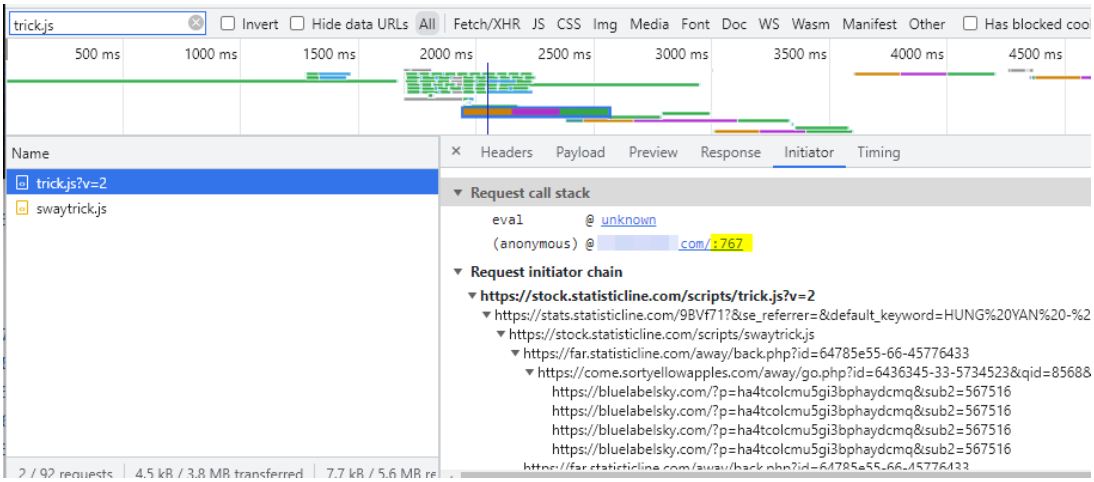
3) 開啟有問題的網站，轉址到釣魚網站後Network下方會順次序顯示瀏覽器下載過的所有資源，其中第一個Status是”302”的就是觸發轉址的資源。



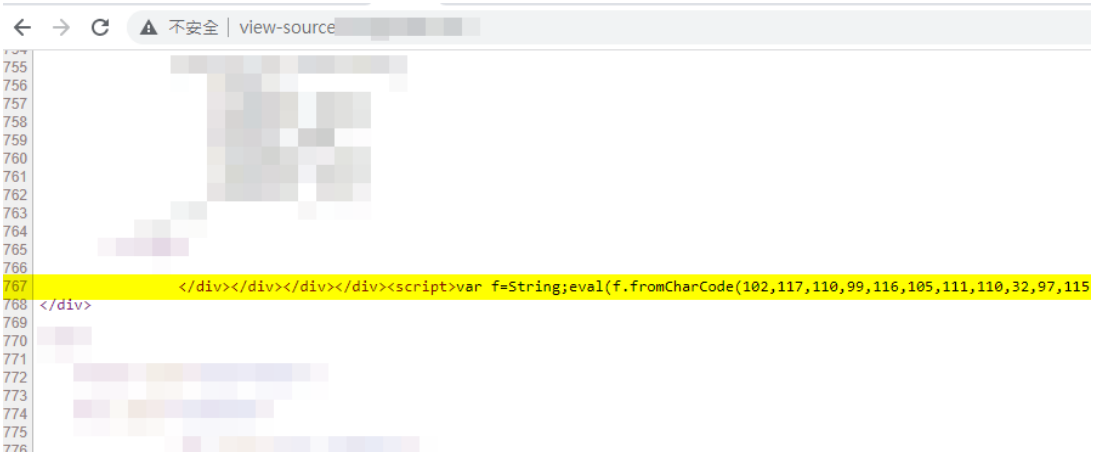
4) 單按檔案名稱，再按Initiator便可以看到資源是由另一檔案”trick.js”觸發



5) 用上方filter尋找trick.js 從trick.js的initiator 可以看到Script是從網站的767行源碼所觸發



6) 在網址列輸入 view-source:domain.com 查看第767行源碼，找到源頭



7）找到來源之後，需要確定問題源碼從何而來，如果從plugin或者theme產生便需要檢查其源碼，如果已經植入到數據庫，可能需要逐行刪除，這個情況便需要評估還原備份會否比較直接(如果有的話)。