You Can't See Me！！

看不見的網站攻擊

Unohope / Trueman

HIT Conference 2008

講者簡介

- **Trueman**
- **http://roamer.cc**
- 網駭科技技術顧問，曾任職於入口網站、金融業、資安原廠與專業資安服務廠商；專長於網路滲透測試、駭客攻擊手法研究。並曾擔任多場資安研討與發表會主講人。

看不見的網站攻擊手法

- 網站管理者在面對網站攻擊時的反應通常總是慢半拍，往往等到網站淪陷了！才有所警覺！！
- 有許多的間接式網站攻擊手法是管理者所難以偵測的，在這種情況下，網站管理者該如何保障網站使用者的安全呢？

近期常見間接式網站攻擊手法

- **XSS**
- **CSRF**
- **Redirect**
- 信任網站
- **And…**

XSS

- **Cross Site Scripting**
- 跨站腳本攻擊
- 輸入值驗證錯誤（**Input Validation Error**）的安全弱點
- 攻擊對象非網站本身
- 『你出包，我倒楣，他真爽！』

Cross-Site Scripting

- 在 **Web** 應用程式中，當 參數 或 資料 顯示成 **HTML** 網頁前，未檢查內容是否含 **HTML tag** 或網頁腳本，導致被駭客利用，攻擊其他瀏覽網站的無辜使用者
- 簡單的攻擊例子
  - **http://www.victim.com/function.cgi?data=<script>alert("XSS!")</script>**
  - **http://www.victim.com/function.cgi?data=<iframe src="<*evilURL*>"></iframe>**

常見利用

- 竊取**cookie**等機敏資訊
  - <script>alert(document.cookie)</script>
- 掛馬
  - <iframe src=”惡意連結位址”></iframe>
- 網路釣魚
  - <iframe src=”釣魚網站位址”></iframe>

常見散播管道

- 廣告信
- 論壇發文
- 縮網址
- 關鍵字與網頁看板廣告
- ...**etc**

Cross-Site Request Forgery

- 簡稱**CSRF**或**XSRF**
- 廣義**XSS**的一種
- 針對登入後的網站執行操作

Alice轉帳100元給Bob時

- POST http://bank.com/transfer.do HTTP/1.1
- . . .
- . . .
- . . .
- Content-Length: 19;
- user=BOB&money=100

惡意使用者Maria

- 而另一位惡意的使用者Maria留意到在轉帳的過程中，網頁程式會執行底下的URL與參數：

  GET http://bank.com/transfer.do?acct=BOB&amount=100

- Maria打算利用這個網頁程式的特性來誘騙Alice轉帳給自己，只要Alice是在登入bank.com的狀態下執行底下語法，將會自動從戶頭中轉帳100000到Maria的戶頭：

  http://bank.com/transfer.do?acct=MARIA&amount=100000

- 接下來Maria就只要思考該怎樣偽裝這段連結讓Alice或其他該銀行的用戶不小心執行，就可以坐著等待大筆鈔票被匯進自己的戶頭了！

相關慘案

- **Samy Worm**
  - http://en.wikipedia.org/wiki/Samy
- **Gmail**
  - http://www.gnucitizen.org/blog/google-gmail-e-mail-hijack-technique/
- **CSRFDB**
  - **http://csrf.0x000000.com/csrfdb.php**

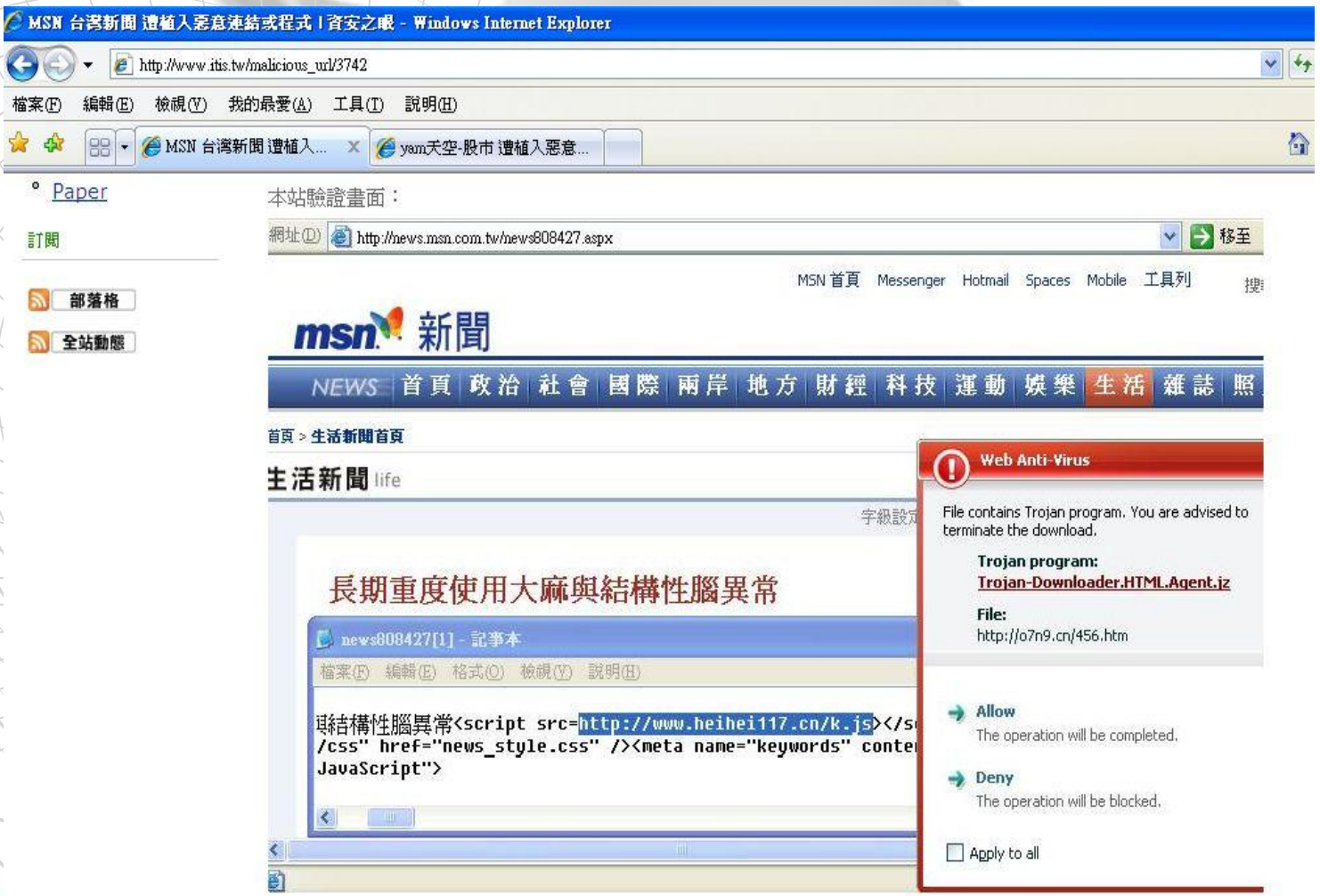
Redirect

- 各大入口網站普遍存在的問題
- 使用者可能被導引至任意網站
- 大量遭垃圾信件利用
- 可利用來繞過部份網站偵測機制

案例分析與進階利用

信任網站

MSN新聞網站被掛馬？



內含可疑連結：**http://www.heihei117.cn/k.js**

真實情況

- 被入侵的頁面皆為國際厚生網站提供之新聞
- 實際被入侵的網站為國際厚生網站
- **MSN**網站引用國際厚生網站提供之資料，但並未做檢驗與過濾，導致刊登的新聞內容包含惡意連結