TLP:WHITE

# 網站遭轉址服務利用的資安風險

Announcement Advisory Report（ANAR）

2017-08-14

TWCERTCC-ANAR-2017008

## Summary

- 釣魚網站是駭客散布惡意程式的管道之一，駭客可利用網域名稱轉址服務特性散布釣魚網站，讓使用者瀏覽正常網站時，不小心連到釣魚網站。
- 網站管理者可主動於網路上搜尋自己的網站、網址及關鍵字等資訊，查看企業網站是否遭網域名稱轉址利用。
- 網域名稱轉址服務平台對服務申請者身分應加以驗證，以防有心人士以非授權方式利用他人網站進行轉址。

## Description

垃圾郵件及釣魚網站的目的是誘騙使用者點選偽冒網路連結的社交工程網路犯罪手法之一。藉由此手法誘騙使用者去做對攻擊者有利的行為，例如增加目標網站點擊率、竊取使用者帳號密碼等重要個資或更進一步的入侵攻擊。

大部份網頁伺服器的存取紀錄，儲存了有關瀏覽者來源和如何瀏覽網站的詳細資料，但是有關使用者點選哪些連結而離開該網頁的上網習慣操作，網頁伺服器並不會記錄；因此，若網站要追蹤使用者習慣，可透過網域名稱轉址方式獲取這樣的紀錄[1]。若使用者點選有轉址服務的網站時，會先向原網頁伺服器發出請求並記錄下來，使用者才被導向網址連結的伺服器，然而這樣網域名稱轉址方式卻可能讓有心人士拿來非法利用。

TWCERT/CC 接獲國內企業通報，表示他們的官方網站遭到非法轉址利用，該官方網站未經授權，遭不明人士向國內免費的網域自動轉址服務公司申請網站轉址服務，將該企業官網嵌入於免費轉址服務的網域中。除了該公司遭未授權申請網域轉址外，經查，有多達數千個網站都遭同樣手法申請網域轉址利用，其中不乏 Yahoo!奇摩電影、中央通訊社等台灣民眾經常瀏覽的知名網站，遭利用的原網站網址可能被以”企業名.轉址平台名.com.tw”或”xxxxxxx.轉址平台名.com.tw”網址形式發布，例如：若企業原官網為 abc.com.tw，經轉址後可能為 abc.ufc.com.tw 或 1060711.ufc.com.tw 等網址，該新的網址除內含原官網內容外，也可能會遭有心人士內嵌廣告或有害連結，來誤導使用者不小心點選連結，遭網站釣魚攻擊，如圖 1 所示。

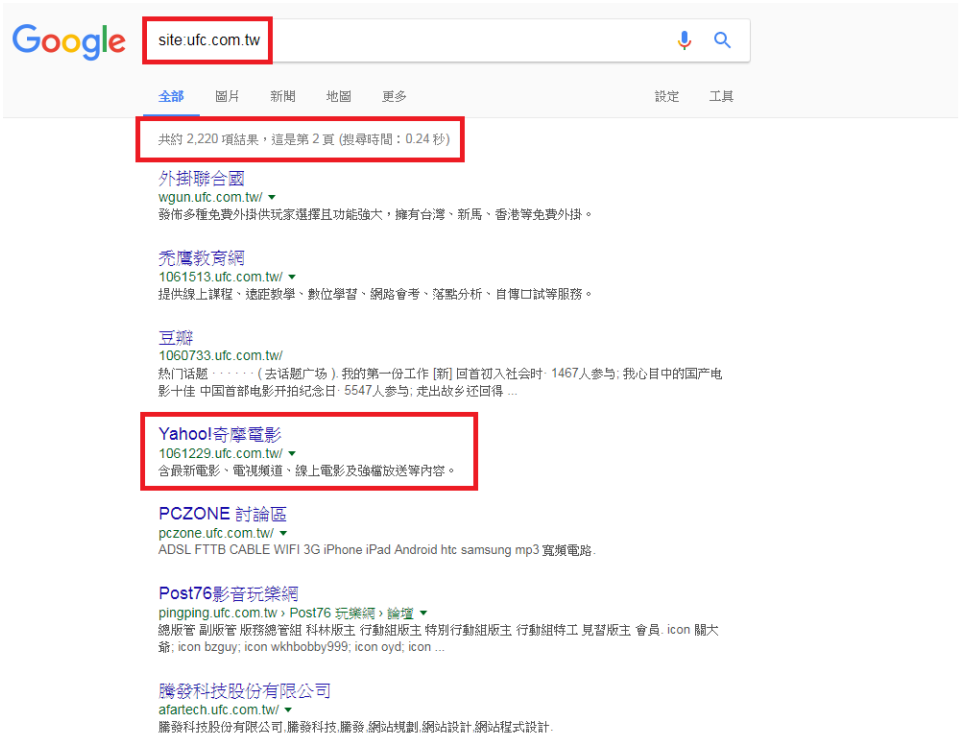


圖 1、Yahoo 奇摩電影網站遭利用轉址服務

一般的網路連結轉址服務[2]，使用者於申請帳號密碼後，登入其平台即可使用轉址的服務。


圖 2、一般轉址平台使用情況

網路上有許多提供免費網域轉址服務的網站，為了獲取廣告收入，針對申請

者的身分認證機制並不嚴謹，有些甚至連驗證都沒有，然而有心人士可利用這樣的網址轉址服務平台，不經同意就可將知名網站加工轉換成其他網域，網站管理者通常不知道已經遭到利用作為其他用途或加入廣告頁框，如圖 3。以國內某旅行社為例，被利用並轉址成其它網域，如圖 4 及圖 5。

```
<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.0 Transitional//EN' 'http://www.w3.org/TR/REC-html40/loose.dtd'>
<html>
<head>
<title>[redacted]</title>
<meta name='keywords' content='[redacted]'>
<meta name='description' content=''>
<meta name='revisit-after' content='14 days'>
<meta name='robots' content=''>
</head>
<frameset rows='25,*' frameborder='NO' border='0' framespacing='0'>
<frame name='TOP_MENU' src='http://[redacted]ufc.com.tw/?PUT=ad' noresize scrolling='no'>
<frame name='MAIN' src='http://www.[redacted].com.tw'>
</frameset>
<noframes>
<body bgcolor='#FFFFFF' text='#000000'>
進入 <a href='http://www.[redacted].com.tw'>[redacted]</a>
</body>
</noframes>
</html>
```

圖 3、某網站非經授權加入頁框

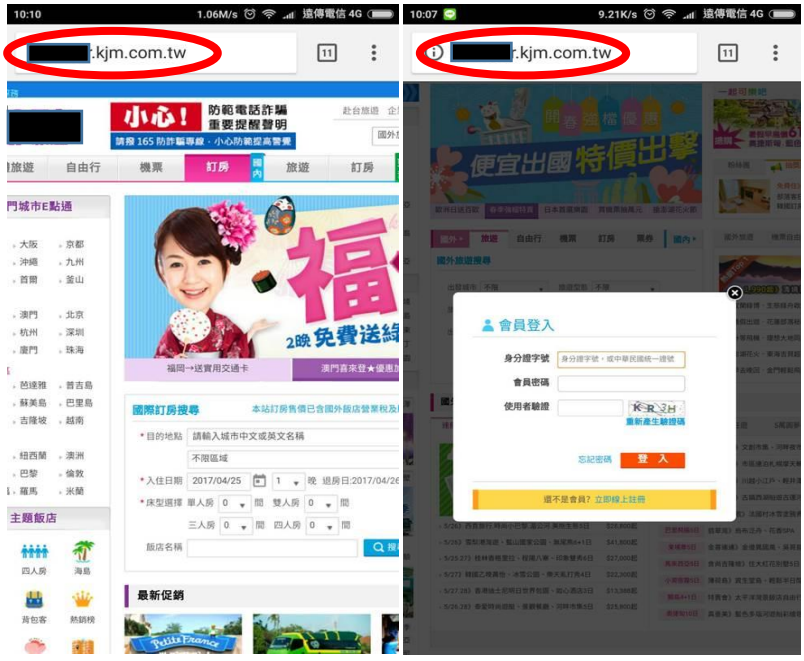


圖 4、某旅行社遭偽冒的網頁


圖 5、某旅行社原本的網址及其網頁

經本中心查詢後，該旅行社遭有心人士以假郵件帳戶「sercive@旅行社.com.tw」名義，同時向 5 個網域轉址服務平台申請轉址服務，如圖 6，但該旅行社表示並無此「sercive@旅行社.com.tw」帳號。偽冒的網址都是以旅行社的英文名稱為首，企圖混淆使用者。


圖 6、旅行社遭 5 個自動轉址服務利用

在台灣，提供自動轉址類似服務的平台眾多，經查，常見的網域轉址服務平台如表 1 所示。若提供網域轉址服務平台商對於轉址服務申請人的身分未加以驗證，容易成為有心人士利用的管道。

表 1、台灣常見的轉址服務平台

| Domain Name | IP |
|---|---|
| kjm.com[.]tw; jnd.com[.]tw; jtg.com[.]tw<br>amm.com[.]tw | 61.31.226[.]225 |

| | |
|---|---|
| omap.com[.]tw; ufc.com[.]tw; 2at.com[.]tw<br>xweb.com[.]tw; iman.com[.]tw;<br>88u.com[.]tw; idun.com[.]tw | 61.31.226[.]226 |
| ii9.com[.]tw; wit.com[.]tw; ttj.com[.]tw | 61.31.226[.]228 |
| kmg.idv[.]tw | 61.31.228[.]2 |
| fol.com[.]tw | 60.199.209[.]170 |
| ioca.com[.]tw | 60.199.209[.]161 |

透過反查網站的 IP，其中 omap.com[.]tw、ufc.com[.]tw、2at.com[.]tw、xweb.com[.]tw、iman.com[.]tw、88u.com[.]tw、idun.com[.]tw 等 7 個服務主網站的 IP 皆為 61.31.226[.]226，並經 VirusTotal 中的 Fortinet 與 Google Safebrowsing 網址掃瞄器判定為惡意網址，如圖 7 所示。此外，自動轉址服務也造成網站管理者的困擾，擔心遭駭客冒用來散播惡意程式，影響商譽。因此有部分平台，已經發布聲明：由於少數會員，利用轉址平台濫寄廣告信件或販賣違法物品，導致該平台成為檢警查緝的重點網站。


圖 7、VirusTotal 判定 61.31.226[.]226 有惡意行為

TWCERT/CC 在接獲企業通報其官方網站遭利用後，即透過政府資安資訊分享與分析中心(Government Information Sharing and Analysis Center, G-ISAC)將情資通報台灣網路資訊中心(Taiwan Network Information Center, TWNIC)以移除該網頁，但是卻無法有效遏止這類非企業授權的網域轉址服務利用的偽冒行為，建議網域監管單位應重視這個問題，降低企業遭非法利用及誤導民眾點選偽冒網址的機會。根據國際反網路釣魚工作組織(Anti-phishing Working Group,

APWG)在 2017 年 6 月發布的報告[3]，大多數主要的轉址服務提供商已經為惡意轉發目的地設置了篩選機制，TWCERT/CC 鼓勵所有轉址服務提供商實施 IP 紀錄與身分驗證，並提醒使用者勿以身試法。

## Recommendations

因應近期此類利用網站知名度，非經授權申請該網站網址轉址服務，並移為它用的不正當手法，TWCERT/CC 建議有以下因應措施：

1. 網站管理者應該經常以自己的網站名稱、網域等關鍵字進行搜尋，是否遭非法冒用，若發現有非網站管理者意願之重製行為，應向網域轉址服務平台反映並通報當地 CERT/CSIRT 組織或網域管理單位，協助移除。

2. 使用者在瀏覽網頁時，應該小心其網站名稱與網址是否有異，勿認為從搜尋引擎找到的連結都是正確的。

3. 網域轉址服務平台商應對申請者建立更嚴謹的身分驗證機制，以防止有心人士利用網域轉址服務作為網路釣魚用途。

## References


[1] Wikipedia, "URL redirection", Retrieved Aug 14, 2017, from the World Wide Web: https://en.wikipedia.org/wiki/URL_redirection

[2] Google, "Google URL Shortener", Retrieved Aug 14, 2017, from the World Wide Web: https://goo.gl/

[3] APWG, June 26, 2017, "Global Phishing Survey: Trends and Domain Name Use in 2016", Retrieved Aug 14, 2017, from the World Wide Web: http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf

## 聯繫資訊

台灣電腦網路危機處理暨協調中心

免付費專線：0800-885-066

- 資安事件通報03-4115387 或02-23776418
- 電子郵件：twcert@cert.org.tw
- 官方網站: https://www.twcert.org.tw/
- Facebook: http://www.facebook.com/twcertcc