「搜尋引擎毒化」攻擊手法簡介

一、 攻擊概述：

搜尋引擎毒化，英文又稱 Search Engine Poisoning, Spamdexing, Search Spam, Search Engine Spam, Web Spam. 簡單來說，就是攻擊者利用某些手段使得搜尋條件與對應的搜尋結果並不相符。而這些不相符的搜尋結果通常都掛有惡意軟體或是惡意程式碼。

二、 攻擊平台：

由於該手法是利用搜尋引擎最佳化(Search Engine Optimization, SEO)的手法來欺騙搜尋引擎，導致搜尋者搜到的是惡意頁面，因此除非搜尋引擎能夠判別該頁面的真偽，否則任何平台都有可能受到該類型的攻擊。

三、 攻擊手法介紹：

擴展外部連結，不一定是靠交換友情連結。 有很多地方可以散佈連結。 例如：BLOG 評論、網頁評論、留言本、論壇等等。在上述的這些地方時常可以看到 Spamdexing。以下是一些 Spamdexing 常用的連結作弊伎倆：

甲、BLOG 作弊：

BLOG，是一種交互性很強的工具。這幾年，各式 BLOG 網站（微博、無名小站…）的興起，成為了 Spamdexing 一個新的製造連結的福地。

i. **BLOG 群作弊**：BLOG 群建作弊就是通過程序或者人為的手段，大量申請 BLOG 帳戶。然後通過發表一些帶有關鍵詞連結的文章，通過這些連結來推動關鍵詞的搜索引擎排名。

ii. **BLOG 隱藏連結作弊**：作弊者通過提供免費的 BLOG 樣式，在樣式文件裡增加隱藏連結以增加網站隱藏連結，達到提供搜索引擎排名。

乙、留言板群發：

使用留言板群發軟體可以自動發布自己的關鍵詞 URL，在短時間內迅速提高外部連結。

丙、連結工廠

“連結工廠”是指由大量網頁交叉連結而構成的一個網絡系統。這些網頁可能來自同一個網域或多個不同的網域，甚至可能來自不同的伺服器。一個站點加入這樣一個“連結工廠”後，它可得到來自該系統中所有網頁的連結，

然而同時它需要“奉獻”自己的連結，籍此方法來提升連結得分，進而達到干預連結得分的目的。

丁、隱藏連結

隱藏連結一般被 SEO 用在客戶網站上，透過在自己客戶的網站上使用隱藏連結的方式連接自己的網站或者是其他客戶的網站。

戊、假連結

將連結添加到 Java Script、框架或者是表單裡面。這種方式的連結對搜尋引擎蜘蛛來說，根本無法讀取出來。因此連結只是做給人看的，搜索引擎根本無法識別。

己、網頁綁架

這就是我們經常所說的 Page Hijacking，是將別人的網站內容或者整個網站全面複製下來，偷梁換柱放在自己的網站上。但是這個做法是相當冒險的，因為搜索引擎的專利技術能從多個因素上來判斷這個被複製的網頁或者網站並非原創，進而不予以收錄。

庚、網站鏡像

通過複製整個網站或部分網頁內容並分配以不同域名和服務器，以此欺騙搜索引擎對同一站點或同一頁面進行多次索引的行為，這也是為什麼有的網站註明禁止未授權不得做網站鏡像的原因了，兩個網站的完全一樣，相似度過高必然會導致自己的網站受到影響。

辛、掛黑鏈

掃描 FTP 或者伺服器的密碼、漏洞，然後駭進網站後把連結掛進去。然而，這些掛進去的連結是可以透過 SeoQuake 這個瀏覽器外掛發現的。

壬、隱形法

隱形法(cloaking)簡單來講就是網站站長用了兩版不同的網頁來達到最佳化的效果。一個版本只給搜索引擎看，一個版本給自己看。搜索引擎說這類做法是不違反規定，提供給搜索引擎的網站版本是經過優化的，通常不能如實反映網頁所包含的真實內容。但倘若被發現該網站會永久從搜索引擎名單中被剔除。

癸、關鍵詞堆積

大量的在網頁原始碼、META 標籤、TITLE、註解、圖片 ALT 中重複某個關鍵字，使這個關鍵字的密度非常高，讓搜索引擎以為網頁具有相關性。關鍵詞堆積技術利用一長串重複性的關鍵詞來蒙混搜索引擎，而實際上，這些關鍵詞有時候與網頁內容相關、有時候無關。

四、 實際事件：

以近期來說，最暢銷熱門的遊戲我想莫過於暗黑破壞神 3(Diablo III)了，而也因為它如此的廣為人知，便成為了駭客下毒的對象。趨勢科技發現如果搜尋「diablo 3 free download (暗黑破壞神三免費下載)」，其中有些排行前面的結果會導入網路釣魚（Phishing）頁面,最終結果會導向一個問卷調查詐騙頁面,藉以蒐集受害者個資。而他們便是利用了搜尋引擎毒化的手法，將惡意頁面自然搜尋排名擺到前面佯裝下載頁面。過程中，還會要求依照指示利用臉書 Facebook 常見的分享手法散播惡意連結，但最終當然還是沒有免費的暗黑破壞神三(Diablo 3 free download)可下載。

再舉更久遠以前的事件,相信很多人都聽過3D肉蒲團之極樂寶鑑這部電影，號稱是史上第一部在院上片的 3D 成人片，在剛上映時可說是非常的熱門。而在 3D 肉蒲團之極樂寶鑑在港台開出亮眼票房成績之際，在市場人口最大的大陸卻無法上映，這除了造成許多大陸網友發起要趁「五一假期」組團赴港、台觀賞外，也出現大陸網友在網路上熱搜，卻都慘遭木馬程式入侵，導致電腦中毒。不少大陸網友為了想要一睹為快，紛紛上網搜尋 3D 肉蒲團，而「恰巧」(當然是毒化後的成果）發現一個名為「完整版下載」的檔案，更是讓許多網友以為挖到寶，沒想到下載後才發現是個惡意程式。

五、 檢測方法：

Chrome、Firefox、Opera 和 Safari 都有 SEOquake 這個外掛可以協助檢測。也有學者提出論文說他們實作出了一套系統，叫做 SURF（Search User Redirection Finder)，聲稱在蒐集七個月的資料中，只有 0.9%的網頁是誤判（false positive）的。而在實作了這個系統後，他們也為如何判別下毒事件訂定了一些準則。

六、 防護方法：

Google 宣布他們讓使用者的搜尋變得更加安全。他們宣稱登入 Google 服務的使用者會有更安全的搜尋體驗。這代表兩件事：第一，現在搜尋的查詢和

結果都是透過 HTTPS 傳遞。這可以保護使用者，當他們所使用的是不安全的網路環境時，比如大多數的無線網路環境。Google 在 HTTP 參照位址標頭（HTTP referrer header）內不再包含用來連到網站的搜尋字串。由於一般的網站無法得知他們的哪些字串是流行的。因此，想要自己進行優化(毒化)變得很困難。

不過像上面實際事件提到的那些就比較難防了，因為就算 Google 有機制不讓那些惡意網頁爬上熱門搜尋，但假若使用者執意想要並且真的認為可以下載到這些熱門檔案的話，他們依舊會點進該網頁瀏覽，因此加強宣導資安概念也是非常重要且必須執行的。

七、 參考資料：

1. http://blog.trendmicro.com.tw/?p=305
2. http://baike.baidu.com/view/1064169.htm
3. http://www.seoquake.com/
4. http://www.poly.edu/sites/polyproto.poly.edu/files/csaw2011_submission_21.pdf