GoogleHacking 入侵與防範技術之研究

莊芳昇* 鄭進興†
*樹德科技大學資管所 †高雄第一科技大學資管系
fangshen@mail.hwai.edu.tw

摘要

近年來網際網路已成為資訊快速交換的媒介，伴隨著網路應用及複雜性的增加，資訊網路系統的漏洞層出不窮，使得網路蠕蟲的發生頻率增高、潛伏性更長、覆蓋面更廣，網路蠕蟲已成為網路安全研究的重要議題。

搜尋引擎是網路蓬勃發展下的科技產物，成為我們網路生活中不可或缺的最佳伙伴。而 Google 更被公認為世界上最大的搜尋引擎，幾乎沒有什麼是 Google 所找不到的。曾經它是網路搜尋資料的好幫手，但隨著網路蠕蟲不斷的變種，搜尋引擎進而成為網路蠕蟲的幫兇。成為駭客搜尋未進行修補漏洞網站的利器，透過 Google 強大快速的搜尋大大縮短蠕蟲搜尋弱點目標的時間。因此網路主機被攻擊的機率大幅提昇，本文將深入探討 GoogleHacking 的入侵原理與防禦技術，協助網管人員早期發現與防禦 GoogleHacking 的不當存取。

關鍵詞：網路安全、網路蠕蟲、GoogleHacking

1. 前言

隨著網際網路的發展，網路蠕蟲對資訊網路系統的威脅日益嚴重。近年來，多樣化傳播路徑和複雜的應用環境使得蠕蟲發生頻率大幅增高、涵蓋面更廣及造成的損失也更大。從 1998 年 Morris 蠕蟲事件到現在的 Internet 安全事件回報統計[5]，每年均以倍數增長(圖 1)。這顯示出在作業系統與應用程式上有許多的漏洞，而網路蠕蟲也不斷的變形，對於網路安全著實是很大的威脅，因而引起整個網路的壅塞、癱瘓，使社會與經濟蒙受鉅大損失。

Google 搜尋引擎是網路蓬勃發展下的科技產物，它不斷改變我們網路生活方式，已經有數億網路人口正在使用它，產生了一種宗教般的熱情，它使每個人與任何問題的答案，就好像只有食指與滑鼠左鍵之間那麼遠。但隨著網路蠕蟲的不斷的變種，已成為網路蠕蟲的幫兇。

Google 已支援超過 35 種搜尋語系，並可以快速地傳回相關搜尋結果。Google 到目前為止已建置了近七千部的 RedHat Linux 伺服器，這些分佈在世界各地的螞蟻雄兵，至 2005 年 7 月已搜尋了 80 億頁的網頁內容、10 億筆論壇討論訊息。對全球 80 億的網頁內容、每天上億、每秒上萬次的查詢，Google 仍以少於一秒的反應時間回傳結果。至今 Google 已被公認為世界上最大的搜尋引擎[12]，幾乎沒有什麼是 Google 找不到的。

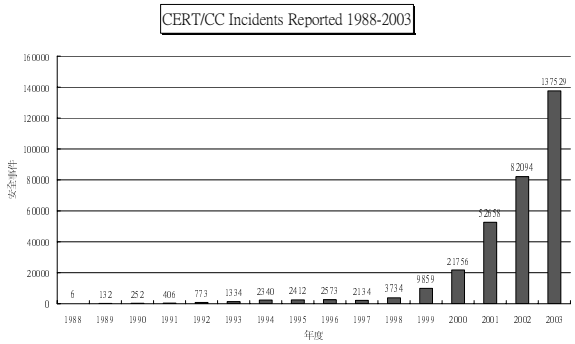

圖1 Internet Incidents Reported 1988-2003

它曾是網路搜尋資料的好幫手，如今 Google 已搖身一變，成為駭客搜尋未進行修補漏洞網站的利器，透過 Google 強大快速的搜尋大幅縮短蠕蟲搜尋弱點目標的時間。因此網路主機被攻擊的機率大幅提昇。GoogleHacking 是利用 Google 搜索引擎快速搜尋未修補漏洞的弱點主機及敏感資料的手法[9]，而這種以前由駭客手動進行的攻擊，已經可經由蠕蟲來自動完成。本文將深入探討 GoogleHacking 的入侵原理與防禦技術，協助網管理人員早期發現與防禦 GoogleHacking 的不當存取。

2. GoogleHacking 相關不當行為之探討

從最近的資訊安全威脅中，漏洞發佈與攻擊程式推出的時間差越來越短，也就是初始攻擊(Zero-day)的時代來臨。搜尋引擎又稱為「出口網站」，近年來發展迅速，逐漸取代「入口網站」。企業和政府相關機構對網路的依賴性越來越大，也不斷的累積了豐富的資料，同時也把這些放置在伺服器上的資料推向了危險邊際。諸如：伺服器的不當配置、系統的漏洞和人為的疏失等，導致許多資料成了公開的祕密。如果我們沒有做好適當的防範，那麼搜尋引擎就有可能會把一切都洩露出去。其實我們只要掌握搜尋引擎的原理就不難整理出一套可行的防禦措施來阻擋 GoogleHacking 之類的攻擊。

搜尋引擎主要由三部份所構成「網路機器人(Robot)、索引資料庫和查詢服務」。只要被網路機器人找到的網頁內容都將會被記錄到搜尋引擎資料庫中，當使用者下達特定的搜尋語法時，就可以獲得使用者所想要的資訊。而網路機器人其實是一個程式，它能夠把網頁中的關鍵內容、網頁中所包含的 URL 指向的網頁內容都保存到搜尋引擎的資

料庫中，並建立索引。這類的程式通常稱之為「蜘蛛(Spider)、網路流浪漢(web wanderer)或網路蠕蟲(web worms)」等。大部份的搜尋引擎都是利用這類程式來完成自動搜尋工作。

它們會以非常快的速度瀏覽整個網際網路，那麼幾乎大部分網站內容都會被搜尋引擎所掌握，而這並不是我們所希望的，我們不希望這些網路機器人擷取非公開的資料。因為一旦被搜尋引擎收集，這些資料將迅速流通各角落。隨著隱私資料洩露，將衍生嚴重的社會問題。

2.1 MyDoom 電子郵件病毒

2004 年 1 月 MyDoom(Novarg)一隻名為悲慘命運的電子郵件蠕蟲[16]，主要透過電子郵件及 P2P 檔案分享軟體進行散佈，最高以一秒鐘 1200 封電子郵件進行散佈，並對 www.sco.com 網站發動阻斷式服務攻擊(DoS)，造成全球網路重大損失。它強大的電子郵件位址搜集能力及合適的發佈時間，使得 MyDoom 在當時被稱為史上最厲害的電子郵件病毒。MyDoom 也不斷的變形，之前的版本只會在受感染電腦硬碟中搜尋電子郵件位址，在 2004 年 7 月 27 日下午出現了 MyDoom 變種 M 蠕蟲[17]，它除了利用電子郵件瘋狂傳播外，最大的特點是一旦電腦被感染後，一台電腦就可以發動成千上萬個請求，利用 Google、Yahoo、Altavista、Lycos 等搜尋引擎來蒐集更多的電子郵件位址，MyDoom 的傳播行為並造成上述搜尋引擎在很長的一段時間反應速度變得相當緩慢。

2.2 Santy 惡性蠕蟲

在 MyDoom 蠕蟲造成搜尋引擎癱瘓數小時後，這些搜尋引擎並未學到教訓。在 2004 年 12 月 21 日出現了名為 Santy 蠕蟲[13][2]，利用 Google 向 phpBB 2.0.11 之前版本的論壇發動攻擊，成為史上第一隻利用 Google 來搜尋弱點目標進而攻擊的蠕蟲。以前駭客需人工利用程式系統漏洞來攻擊論壇，再竊取使用者資料。而 Santy 蠕蟲將這些程序自動化了，從搜尋具有漏洞的論壇到發動攻擊，都是由蠕蟲自行完成(圖 2)。Santy 蠕蟲在爆發後，在數小時內迅速感染了至少 38000 台主機。

該蠕蟲利用 Google 搜尋引擎進行自動化攻擊，以含有「viewtopic.php」字串為條件進行搜尋，並將搜尋結果製作成為攻擊目標的伺服器列表。利用 phpBB 的安全漏洞“PHPBB Remote URL Decode Input Validation Vulnerability，藉由程式設計者不對輸入「include()、require()」這些函數的參數進行充份的驗證，試圖對含有 phpBB 弱點的目標伺服器進行遠端存取，最嚴重的情況下攻擊者能控制整個系統。

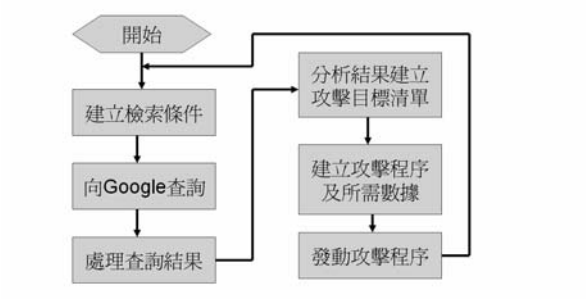

圖 2 GoogleHacking 自動化流程

該蠕蟲會在被感染的伺服器上進行自我複製，並覆蓋帶有「.asp、.htm、.jsp、.php、.phtm、.shtm」等副檔名的檔案，竄改在被侵入的網頁伺服器網站上顯示「This site is defaced!!! NeverEverNoSanty WebWorm generation X」訊息，generation X 就表示蠕蟲已經到了第 X 代了(圖 3)。

圖 3 被 Santy 蠕蟲感染網站

Google 也很快的採取行動壓抑了 Santy 蠕蟲的傳播，但很快的 Santy 蠕蟲的變種就出現，有的變成利用 Yahoo 搜尋引擎，有的利用巴西版的 Google 搜尋引擎及其它諸如 AOL 等也都被利用。當然這些搜尋引擎要封殺特殊的搜尋請求並不是問題，最根本的還是要修補系統的漏洞，才不會受到感染。

2.3 Anti-Santy 善意蠕蟲

在 Santy 蠕蟲出現後第 10 天，出現了一隻名為 Anti-Santy 的善意蠕蟲[4]。這隻蠕蟲跟 Santy 蠕蟲一樣利用 Google 搜尋執行 phpBB 論壇的網站，對這些網站進行感染，進而對這些網站安裝更新套件使這些網站看起來更加安全，使得 Anti-Santy 蠕蟲有”益蟲”之稱。網站被感染後，會顯示「viewtopic.php secured by Anti-Santy-Worm V4」(圖 4)。提醒您雖然已幫助您增強了 viewtopic.php 的安全性，但您仍必須將 phpBB 論壇升級到 2.0.11 以上版本。

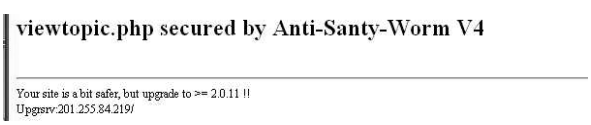

圖 4 Anti-Santy 蠕蟲感染示意圖

2.4 Google 簡易滲透技術

GoogleHacking 的滲透技術我們把它區分成簡易及深層兩種[1][3][14][18][19]，簡易的

GoogleHacking 滲透技術大部份為有心人士用來竊取重要資料或個人隱私等資料。只要在 Google 或利用 Apollo 等工具[10]任意輸入關鍵字，就可輕易獲取個人隱私資料如：身份證字號、出生年月日、大哥大，甚至是銀行帳號等等。我們就好像赤裸裸地在網路向別人公開了自己的一切，著實令人恐慌。

如果我們想獲取可用的行動電話資料，我們可以輸入「大哥大 numrange :0900000000..0999999999」即可獲得網頁中刊載大哥大而且範圍從 0900000000 到 0999999999 間的資料(圖 5)。也可輸入「身份證字號 filetype:xls」來搜尋含有身份證字號標題的 Excel 檔案(圖 6)。如果我們想找記者，也可以輕易透過「記者 filetype:xls」輕易的找到一堆記者的資料(圖 7)。

2005 年為「反詐騙行動年」，個人資料的外洩使得詐騙集團輕易獲得個人資料再利用人性弱點進行詐騙，使得人心惶惶，嚴重影響社會治安甚鉅。但在我們的測試過程中，仍然發現不少政府機關、大專院校都有暴露個人資料之情況，未落實「個人資料保護法」，使得這些資料暴露在網路上。

圖 5 Google 查詢大哥大號碼結果

圖 6 某大學電子工程學系雪霸旅遊名單

府會	台視CH12	電視	戴榮懋	記者	0932-[redacted]8
府會	年代CH37	電視	林義峰	記者	0932-[redacted]3
府會	TVBS CH39	電視	黃志偉	記者	0932-[redacted]6
府會	東森新聞CH40	電視	尤宏源	記者	0920-[redacted]9
府會	中天新聞CH41	電視	陳廣瑞	記者	0937-[redacted]1

圖 7 某縣駐縣記者名冊

2.5 Google 深層滲透技術

2.5.1 “intitle:index.of abyss.conf”

Abyss 網頁伺服器是微軟作業平台中，除了 IIS、Personal Web Server 外的另一項選擇。但卻比 IIS 更輕薄短小且支援 PHP、PERL，更具備操作簡易的介面。但它卻有著暴露系統設定配置檔的風險，我們透過「intitle:index.of abyss.conf」即可獲得 Abyss 網站的系統配置檔，諸如 MD5 密碼(圖 8)。

圖 8 Abyss 設定檔暴露管理者密碼

2.5.2 "# -FrontPage-" inurl:service.pwd

FrontPage Server Extensions 會將其授權的使用者帳號密碼存放在 service.pwd 檔案中，利用「"# -FrontPage-" inurl:service.pwd」，即可利用目錄瀏覽的權限設定疏失，管理員的帳號及密碼立刻就暴露在眼前(圖 9)。

圖 9 FrontPage Service.pwd 暴露管理者密碼

2.5.3 利用網站系統漏洞

在 2.2 節當中我們提到了 Santy 蠕蟲利用 phpBB 論壇系統的漏洞，但這只是其一而已。滲透攻擊型的駭客在實施攻擊之前，往往會先進行資訊搜集工作，而後才是網路系統的漏洞確認和最終的漏洞利用、擴大他的戰績。我們在實作過程中，利用 Google 來搜尋被人安裝 php webshell 後門的主機，並測試可利用的範圍。

首先，利用 Google 的 intitle 及 filetype 語法，在 Google 搜尋框輸入「intitle:"php shell*" "Enable stderr" filetype:php」，則可以找出在網頁伺服器上執行 PHP Shell 的弱點主機。透過 PHP Shell 可以利用設定不當的弱點主機來執行 System()函數，例如使用 echo 指令來竄改網頁「echo “被駭了” > index.htm」。也可以利用 uname –a; cat /etc/passwd 來獲取系統帳號(圖 10)。

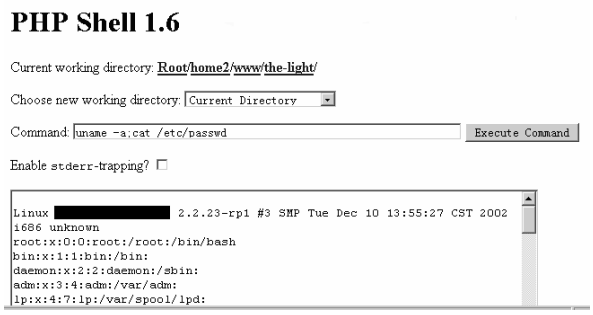

圖 10 PHP Shell 漏洞竊取帳號密碼

同樣的手法，可以如法泡製來檢測 MySQL 資

料庫線上管理系統～phpMyAdmin，該系統需要透過 config.inc.php 來設定 MySQL 的帳號及密碼，有許多管理者貪圖方便沒有設定管理者的密碼，形成一個漏洞。我們使用「intitle:phpMyAdmin "Welcome to phpMyAdmin ***" "running on * as root@*"」語法進行搜尋，同樣搜尋到一堆由懶惰管理者所管理的 MySQL 資料庫(圖 11)。

圖 11 沒有設管理者密碼的 phpMyAdmin

GoogleHacking 深層滲透技術不勝枚舉，我們只是舉了幾個冰山一角的例子，希望能讓網管人員重新審視自己管理的網站，GoogleHacking 可以做的事還有很多，不可等閒置之。例如：搜尋一些提供網頁介面的路由器等，都將嚴重危害網路安全。

2.6 GoogleEarth 3D 地圖檢索技術

繼 GoogleMap 之後，Google 整合了 GoogleMap 和 GoogleLocal 推出 GoogleEarth 這套軟體[8]。透過這套軟體可以看到 3D 的建築物，而不只是只有衛星空照圖。而且這個軟體的影像效果也相當出色，一開始就以 3D 模式顯示地球圖形，您可以由遠至近來嘗試搜尋您想找的地方，我們可以輕易來個虛擬旅行。

然而，衛星空照圖也使得有心人士可以軍事部署相繼曝光，而且 3D 又比 2D 多了一維，而這個維度指的就是「高度」，也就是說使用者可以藉由不同仰角的瀏覽，區別出點與點高度上的差異。任何人都可以粉簡單的透過 GoogleEarth 來瀏覽地形或是建築物高度的能力，也可以輕易得知其在地球的精確位置，包括經、緯與海平面高等。重要政府機關、軍事基地、空軍機場、海軍軍港、學校(圖 12)等一向被視為最高機密的據點都一覽無遺。

3. 防禦措施

3.1 防止病毒搜集電子郵件位址

以往我們都直接在網頁中刊登電子郵件位址，如 lewis.chuang@msa.hinet.net。這種純文字的電子郵件位址標示方式，很容易就被有心人士撰寫程式大量搜集，就像 MyDoom 等蠕蟲一樣。曾經有人提出將 @. 等字元以中文全形標示，但這樣做的話，非中文語系國家人士其實很難理解的，也因如此唯有將電子郵件位址圖像化[6][7](圖 13)，才能有效避免蠕蟲的暴力搜集並可以有效提高其識別度。

圖 12 某大學空照圖

圖 13 筆者 GMail 電子郵件位址圖示

3.2 robots.txt 抵制搜尋引擎機器人

robots.txt 是一個純文字檔案，我們可以在網站上透過建立 robots.txt 來防止「搜尋引擎機器人」，在這個檔案內主要用來聲明拒絕讓搜尋引擎檢索的網站部份或全部內容，或者指定讓搜尋引擎收錄的內容，如此就不會被搜尋引擎給收錄。

各家搜尋引擎公司都有自己的搜尋引擎機器人名稱來識別，例如：Googlebot、BaiDuSpider、MSNBot、FAST-WebCrawler、Inktomi Slurp、Openfind data gather。當搜尋引擎機器人開始瀏覽網站時，首先會檢查網站根目錄下是否有 robots.txt 這個檔案，如果存在，搜尋引擎機器人會根據這個檔案所規範的內容來確認它的搜尋範圍，如果該檔案不存在，那麼搜尋引擎機器人就會隨著鏈結抓取內容。

robots.txt 檔案內容可包含一組或多個群組規則，每個群組規則可由 User-agent、Disallow 等所組成。下面我們會舉幾個例子，來示範如何防禦搜尋引擎機器人的蒐集(如表 1)。

表 1 robots.txt 使用範例

指令	使用範例
User-agent: Disallow:	User-agent: * Disallow: * Disallow: /cgi-bin
禁止所有搜尋引擎搜尋網站任何內容	User-agent: * Disallow: /
禁止搜尋特定網站內容	User-agent: * Disallow: /cgi-bin/ Disallow: /private/
禁止特定搜	User-agent: Googlebot

尋引擎搜尋網站內容	Disallow: /

網管人員在建置好 robots.txt 時，可利用 Searchinworld 網站所提供的 robots.txt 驗證功能來檢測您的 robots.txt 正確性[15]。要注意的是，Googlebot 一天只會下載一次 robots.txt 檔，所以 Googlebot 要經過一段時間後才會發現網站中的 robots.txt 檔可能已經更改過了。而且 ，Googlebot 是分散在很多電腦上，每個 Googlebot 分別保留一份您的 robots.txt 檔，所以建立好 robots.txt 後得經過一段時間 Googlebot 才會全部更新。

3.3 Robots META 標籤

在上一小節我們使用了 robots.txt 來限制整個網站或目錄的搜尋範圍，而 Robots META 標籤則跟網頁其它的 META 標籤存在每個頁面 <head></head> 中。

Robots META 語法主要由 meta name 及 content 組成，meta name 用來定義欲防禦的搜尋引擎機器人名稱，在這裏 Robots 代表著所有搜尋引擎機器人；content 部份有四個參數可定義：index、noindex、follow、nofollow，參數間以,來區隔。因為目前大部份搜尋引擎機器人大都遵循著 robots.txt 規範，只有 Googlebot 完全支援 Robots META，在 Googlebot 中還多了個 content 參數：archive。下面我們舉幾個標籤設定範例，來示範如何防禦搜尋引擎機器人的蒐集(如表 2)。

表 2 Robots META 使用範例

指令	使用範例
允許延著網頁鏈結抓取	<meta name="Googlebot" content="index,follow">
允許延著網頁鏈結抓取	<meta name="Googlebot" content="noindex,nofollow">
禁止複製網頁內容	<meta name="Googlebot" content="index,follow,noarchive">

3.4 網站主機防禦

自由軟體在經過長時間的發展後，逐漸被商業公司所接受，在 2005 年 7 月 Netcraft 網路調查公司對全球網站主機進行調查，自由軟體 Apache 的占有率高達 69.6%[11]。所以，在我們網站主機防禦實作中，我們將以 Apache 網頁伺服器為例。

3.4.1 禁止瀏覽目錄

在 <Directory>….</Directory> 中，可以設定每個目錄下的各別權限。有許多人的網站是允許使用者瀏覽目錄的，往往許多資料就這樣外洩出去，我們可以用 –Indexes 的指令來防止使用者瀏覽目錄檔案清單(如表 3)。

表 3 Apache 禁止瀏覽目錄使用範例

指令	範例說明
Options –Indexes	禁止產生目錄檔案清單

3.4.2 禁止不當 User-Agent 存取

當使用者透過瀏覽器瀏覽網站時，會透過使用者的 http-user-agent 向網站發出請求，藉此可以得知使用者所使用的瀏覽器名稱、版本及作業系統名稱。例如：Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)，表示使用者使用 WINXP、IE 6.0。而 Google、BaiDu、MSN 等搜尋引擎機器人也都有專屬的 User-Agent 識別。同樣在 Apache 網頁伺服器設定中，對 <Directory>….</Directory> 目錄進行 Http-User-Agent 的比對。首先，您必須確認您的 Apache 有載入 mod_setenvif 模組，這個模組可以提供的指令允許伺服器對每個請求，對特殊請求的特性進行環境變數的設定。例如：可以僅在一個特殊的瀏覽器(Http-User-Agent)進行請求時，在發現時進行環境變數的設置。以下我們對 Googlebot、BaiDuSpider、MSNBot 等特殊瀏覽器發出請求時，透過 BrowserMatch 比對 Http-User-Agent，並對特殊 Http-User-Agent 給予 bots 的別名，拒絕對 bots 的 Http-User-Agent 提供存取服務，以達到防禦功效。

```
BrowserMatch “Googlebot” bots
BrowserMatch “BaiDuSpider” bots
BrowserMatch “MSNBot” bots
<Directory /usr/local/www/data>
   Order deny,allow
   Deny from env=bots
   Allow from all
</Directory>
```

另外，我們也可在 PHP 網站系統或以其它程式語言建構的網站，來分析不當的 Http-User-Agent 存取。當發現 Googlebot User-Agent 時，就發送電子郵件到管理者的信箱中。

```
<?
if(eregi("Googlebot",$HTTP_USER_AGENT))
{
   mail("lewis.chuang@msa.hinet.net",
   "Googlebot detected on www.stu.edu.tw",
   "Google has crawled www.stu.edu.tw");
}
?>
```

3.4.3 Awstats 網站流量分析

Awstats 是一個專門用來分析 Web 站台記錄檔的軟體，可以分析 IIS、Apache 的記錄檔，以及其他大部分的 web、proxy、ftp、wap、streaming 伺服器所產生的紀錄檔。建議網管人員可在網頁伺服器中安裝這套分析軟體，來了解網站的瀏覽狀況(圖 14)。

搜尋引擎網站的漫遊器 (前 10) - 全部列出 - 最近參觀日期

5 個漫遊器*	點擊數	位元組	最近參觀日期
BaiDuSpider	35	35.60 KB	2005年 7月 14日 22:19
Inktomi Slurp	6	7.56 KB	2005年 7月 14日 21:18
Googlebot	2	6.99 KB	2005年 7月 14日 13:30
MSNBot	1	19.11 KB	2005年 7月 14日 18:40
Openfind data gatherer	1	186 Bytes	2005年 7月 14日 14:20

* 這些搜索機器人(Robots)會增加參觀者"看不到"的點擊數或流量, 所以不包括在其他統計表中.

圖 14 曾造訪過的搜尋引擎機器人

3.5 GoogleEarth 3D 地圖檢索防禦

GoogleEarth 強大的地圖檢索只是個警訊，敵軍若想以衛星空照圖來發動斬首行動，仍稍嫌不足，敵軍仍必須掌握空中與陸地優勢才有可能發動斬首行動。但我國已暴露的重要軍事據點在未來戰爭勢必成為敵軍首要攻擊目標，國防部應加強軍事設施的偽裝、欺敵防護措施及長程空中預警雷達設施建置，讓重要軍事指揮中心、通訊中心地下化，積極因應以保存戰力。

3.6 Google 自我防禦

在 Google 發現 Santy 蠕蟲大量拖垮搜尋速度後，我們實際對 Google 發出 http://www.google.com/search?q=inurl:viewtopic.php 請求後，Google 即顯示(圖 15)提示畫面後，並中斷請求，發現 Google 只是過濾掉「inurl:viewtopic.php」達到簡易防禦效果。其主要檢查方法是藉由蠕蟲送出搜尋請求字串時，若字串同時符合「含有 inurl:、.php 及參數含有 num 或 start」三種條件時，則判斷是蠕蟲的攻擊行為，即顯示提示畫面並中斷請求。

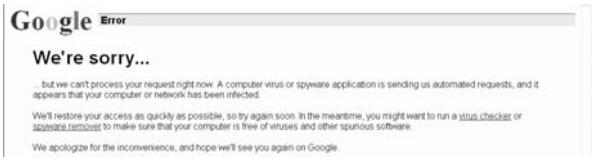

圖 15 Google 防止查詢 viewtopic.php

4. 結論

現在，Google 的安全問題正在步上微軟的後塵，排山倒海的向我們襲擊而來。隨著 Google 的安全危險逐漸加大，宣稱「不作壞事」的搜尋引擎形象大大受損，Google 逐漸成為網路用戶身邊的一顆不定時炸彈。Google 及其它搜尋引擎在提供人們便捷的查詢時，也帶來潛在的資訊安全風險。網路蠕蟲逐漸演變成利用搜尋引擎的搜尋傳回結果來建構攻擊目標列表，也成為網路蠕蟲的發展趨勢。

本文從 GoogleHacking 的技術原理與相關的防禦技術提供給各網站管理人員，但我們認為不論蠕蟲如何的變化，最重要的是要有資訊安全意識及觀念，能夠辨識可能發生的資訊安全問題時，便可避免因為「不知道」而發生的資訊安全危害，網路安全的防禦強度自然會增強。當管理員視資訊安全為常識，把資訊安全作為視為一種習慣時，才會達到最基本的安全。

參考文獻

[1] 吳魯加。“利用 Google 進行入侵與滲透”。2004。http://www.risker.org/tech/GoogleHacking/index.html。

[2] 鄭輝。“Santy 蠕蟲分析報告”。2004。http://202.112.50.218/doc/spark/santywormanalysis.doc。

[3] 鄭輝。”智能蠕蟲防治”。中國網路營運工程師講壇，中國北京，2005。

[4] Anti-SantyWorm, http://www.f-secure.com/weblog/archives/archive-122004.html#00000422.

[5] Cert/CC Statistics, http://www.cert.org/stats/.

[6] Email Signature Generator, http://email.playtime.uni.cc/.

[7] E-Mail Icon Generator, http://services.nexodyne.com/email/.

[8] GoogleEarth, http://earth.google.com/.

[9] Johnny Long, “You found that on Google?”, http://risker.org/tech/GoogleHacking/files/bh-us-04-long-googlehacking.ppt.

[10] Mimi, “Apollo for Google Hacking”, http://worm.ccert.edu.cn/GoogleHacking/Apollo/index.html.

[11] Netcraft, July 2005 Web Server Survey, http://news.netcraft.com/archives/web_server_survey.html.

[12] Nielsen//NetRatings, “Double-Digit Growth In Search Seen By AOL And Ask Jeeves From Q1 to Q2 2005, While Top Search Players Google And Yahoo! Maintain Consistent Growth, According to Nielsen//Netratings”, http://www.nielsen-netratings.com/pr/pr_050721.pdf.

[13] Perl.SantyWorm, http://securityresponse.symantec.com/avcenter/venc/data/perl.santy.html.

[14] Robert Masse and Jian Hui Wang, “Hacking with Google for fun and profit!”, http://www.gosecure.ca/SecInfo/library/WebApplication/GOOGLE-HACKING-GS1004.ppt.

[15] Searchinworld robots.txt Validator, http://www.searchengineworld.com/cgi-bin/robotcheck.cgi.

[16] W32.Mydoom.A, http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html.

[17] W32.Mydoom.M, http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.m@mm.html.

[18] Xclusive, “Google Tricks And Hacks”, http://securityprotocols.com/modules.php?name=News&file=article&sid=1629.

[19] Zhao Huan, “GoogleHacking 的實現以及應用”, http://www.xfocus.net/articles/200502/775.html.