TLP:WHITE

SEO 中毒攻擊 IIS 伺服器之分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 09 月

一、事件簡介

1. 2024/11 有 33 間學校的網站遭受 SEO 中毒攻擊，導致在 Google 搜尋這些學校網站時出現大量與「投資、當沖或鬥地主」等有關的不當用字的連結。經鑑識幾所學校發現受攻擊的網站以老舊版本的 XAMPP 架站居多，而攻擊者應用 CVE-2024-4577 漏洞，又有些網站主機的管理者帳戶使用弱密碼，以致於造成事件發生。
2. 2025/3 趨勢科技研究人員觀察到 SEO 攻擊的新手法，利用惡意程式 BadIIS 攻擊 IIS 伺服器，將使用者導向惡意網站。
3. 2025/9 資安公司 ESET 研究人員發現新的中國駭客組織 GhostRedirector 攻擊 IIS 伺服器， 操縱 Google 搜尋結果、進行 SEO 詐騙。
4. 為了瞭解新的 SEO 中毒攻擊手法，故進行分析。

二、 利用 BadIIS 之 SEO 中毒攻擊

1. 2025/03 趨勢科技人員發現惡意程式 BadIIS 專門攻擊 Internet Information Services(IIS)服務來從事 SEO 詐騙，或將惡意內容注入到使用者所瀏覽的網頁。這類攻擊的受害地區包括：印度、泰國、越南、菲律賓、新加坡、台灣、南韓、日本和巴西，而受害的 IIS 伺服器遍及政府機關、大學、科技公司以及電信產業。

2. BadIIS 的運作方式

駭客利用 IIS 伺服器的漏洞，將惡意程式 BadIIS 安裝到伺服器上。當使用者發送請求到已受駭入的伺服器時，會收到駭客竄改過的 HTTP 回應內容，而有兩種連線結果。

(1) **連線非法賭博網站**：在 SEO 詐欺模式下，惡意程式會檢查使用者的搜尋紀錄。當使用者來自 Google、Bing 和百度等搜尋引擎時，將使

用者導向涉及非法賭博活動的網站。

(2) **連線惡意伺服器**：在注入模式下，它會將惡意 JavaScript 注入網頁，將不知情的使用者重新導向駭客所控制的網站伺服器，這些伺服器可散播惡意程式或執行網路釣魚詐騙。

為了確保成功，駭客使用來自搜尋入口網站的關鍵字來確定瀏覽者是真正的使用者，還是搜尋引擎機器人。然後，惡意程式會操縱 HTTP 回應來誤導 SEO 追蹤器，並最大限度地提高非法內容的可見性。

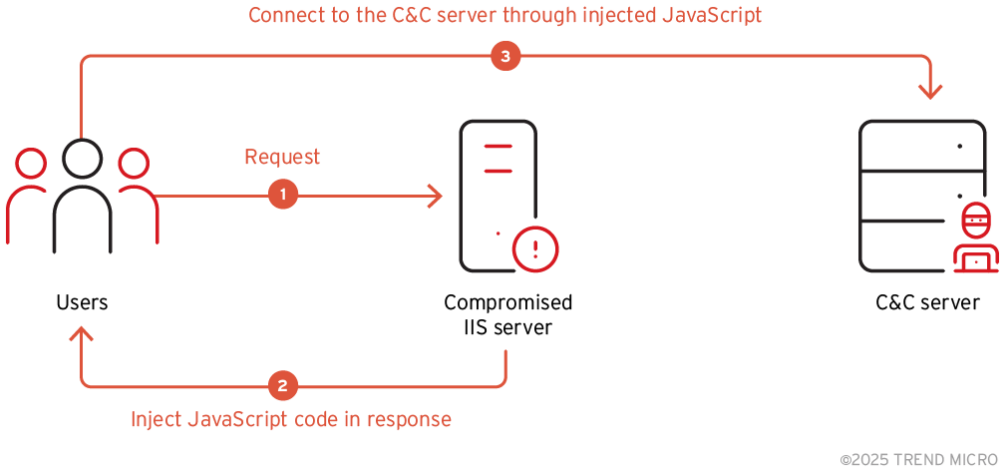
3. 從 BadIIS 樣本中發現的資訊 (例如：擷取到的網域、簡體中文程式碼字串) ，推測這些樣本可能是由中國駭客集團所製作和散播。

4. 當安裝好 BadIIS 後，它會修改網站伺服器回應的 HTTP 請求標頭資訊，檢查 「User-Agent」、「Referer」兩個欄位。當這些欄位含有特定的搜尋入口網站或關鍵字時，BadIIS 會將使用者重新導向某個非法賭博的網站 。

User-Agent 欄位檢查的關鍵字	Referer 欄位檢查的關鍵字
360	baidu.com
baidu	bing.com
bing	Coccoc
coccoc	daum.net
daum	google
google	naver.com
naver	so.com
sogou	sogou.com
yisou	sm.cn

資料來源:趨勢科技

5. 安裝好的 BadIIS 會在瀏覽者所收到的回應中注入可疑的 JavaScript 程式碼，以便將瀏覽者重新導至惡意網站。



圖片來源:趨勢科技

三、 駭客組織 GhostRedirector 之 SEO 中毒攻擊

1. 駭客組織 GhostRedirector 至 2025 年 6 月至少已成功入侵全球 65 台 Windows 伺服器，主要受害國位於巴西、泰國和越南，而其他受攻擊地區包括秘魯、美國、加拿大、芬蘭、印度、荷蘭、菲律賓和新加坡等地。
2. 由於該駭客組織的攻擊目標類型多元，橫跨教育、醫療、保險、交通、科技和零售等多個產業，顯示駭客並非鎖定特定產業，而是以任何可入侵的伺服器為目標。
3. 它攻擊的主要目標是執行 Windows Server 作業系統的伺服器，駭客利用未知的存取途徑成功入侵伺服器後，會放入其客製化的惡意程式來建立持久性的後門，例如:利用 Rungan 後門和 Gamshen IIS 模組。
4. **GhostRedirector 之攻擊手法**

   GhostRedirector 的主要攻擊手法是透過後門程式「Rungan」和「Gamshen」IIS 模組來遠端執行指令，其中 Gamshen 模組可提供「SEO 詐騙即服務」，藉由操縱受害網站的搜尋引擎結果，來提升第三方網站的排名。

   (1) Rungan 後門程式

   一個被動式的 C++後門程式，不會主動向外部發送訊息，而是在等

待攻擊者的指令。當駭客下達指令時，它被啟動執行遠端命令、上傳或下載檔案。它在被入侵的伺服器中容易潛伏更長時間，增加偵測的難度。

(2) Gamshen IIS 模組

Gamshen 屬於木馬病毒，主要功能是執行 SEO 詐騙，專門用於伺服器端。在 IIS 內部運作，監視伺服器的所有傳入請求。

(3) GoToHTTP

在受感染的 Web 伺服器上安裝它，它允許建立可從瀏覽器存取的遠端連線。

5. Gamshen 執行 SEO 詐騙之運作方式有三個步驟如下。
   (1) 偵測 GoogleBot：它會偵測來自 Google 搜尋引擎爬蟲（GoogleBot）的請求。
   (2) 動態篡改內容：當請求來自 GoogleBot，Gamshen 會劫持並修改伺服器回應的內容。
   (3) 建立反向連結：它會透過在受害網站的頁面中插入隱藏的連結，將流量或權重導向駭客指定的第三方網站。這是一種「黑帽 SEO」技術，主要在欺騙 Google 的演算法，使被推廣的第三方網站排名上升。
6. 為了達到持久化與韌性，駭客採取以下措施來確保對受害伺服器的長期控制。
   (1) 多重後門部署：在受害伺服器上安裝多個遠端存取工具，即使其中一個被發現或移除，仍有備用方案來維持存取權。
   (2) 建立惡意用戶帳號：利用如 EfsPotato 和 BadPotato 等已知的權限提升漏洞，並在受害伺服器上建立具有特權的虛假用戶帳號，作為持續存取的備用管道。從樣本中提取了用於建立這些惡意用戶帳號的使用者名稱如下: MysqlServiceEx、MysqlServiceEx2 與 Admin。
7. IIS 伺服器建立的網站遭受 GhostRedirector 攻擊後可能面臨的風險如下。

(1) 網站聲譽受損

如果網站被用於 SEO 詐騙，其在 Google 搜尋引擎上的聲譽和排名可能會受到嚴重影響，甚至被列入黑名單，導致網路流量下降。

(2) 資料外洩風險

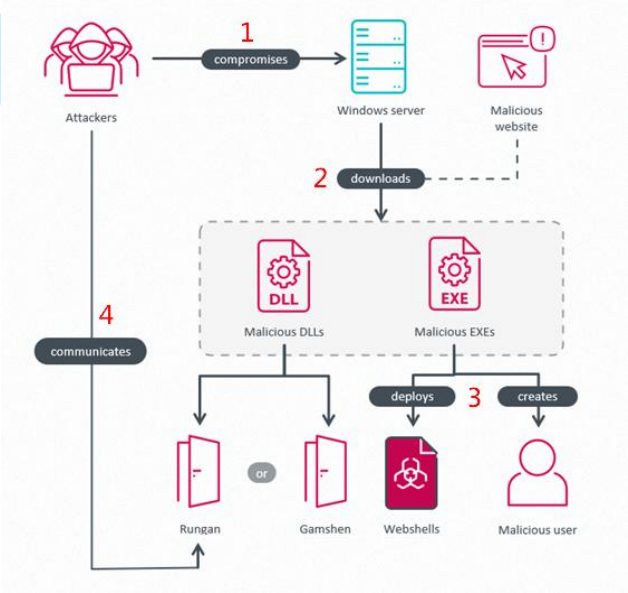
Gamshen 與 Rungan 結合後，可使駭客能夠在不被察覺的情況下，同時進行資料竊取或植入勒索軟體等更具破壞性的攻擊。

(3) 供應鏈攻擊的威脅

若一個軟體或服務供應商的伺服器被入侵，駭客可以將惡意代碼植入到客戶的軟體或服務中，造成更大範圍的供應鏈攻擊。

8. **GhostRedirector 之攻擊行為示意圖**

攻擊者入侵 Windows 伺服器，下載並執行各種惡意工具，例如 :權限提升工具，部署多個 webshell 的惡意軟體、後門 Rungan 或 IIS 木馬 Gamshen，透過 Rungan 讓攻擊者與伺服器連線、下達執行指令。其中權限提升工具的目的是在管理員群組中建立特權帳號，以便 GhostRedirector 可以利用此帳號執行特權操作，或在群組失去對受感染伺服器的存取權限時作為備用管道。



圖片來源: ESET

9. GhostRedirector 所用工具的多個樣本都包含硬編碼的中文字串，攻擊中使用了頒發給一家中國公司的代碼簽署證書，並且在受感染伺服器上 GhostRedirector 建立的使用者密碼之一包含單字 huang，它的中文意思為黃色，推測 GhostRedirector 是一個與中國有關的攻擊組織。

四、 總結與建議

1. SEO 的攻擊事件在 2025 年上半年是很常見的資安事件，從 2024 年年底發現利用漏洞搭配 SEO 黑帽技術來進行攻擊，2025 年 3 月又發現利用 BadIIS 惡意程式來進行 SEO 中毒攻擊，至 9 月出現駭客組織 GhostRedirector 的獨特攻擊手法。由此可知，預防 SEO 攻擊事件的重要性。
2. 使用 IIS 伺服器架設網站的單位很多，而駭客可藉由 IIS 的漏洞入侵網站，然後發送惡意內容給瀏覽該網站的訪客。近期該類攻擊行動中，發現新的 BadIIS 變種主要用來散布線上賭博相關的內容。
3. GhostRedirector 攻擊手法的出現，代表不再滿足於傳統的資料竊取或破壞，而是將受害的 IT 資產轉化為其非法謀利的工具。例如:利用 Gamshen 模組透過可疑的 SEO 策略操縱 Google 搜尋結果，導致濫用被駭網站的信譽來推廣第三方賭博網站，推測該賭博網站可能是「SEO 詐騙即服務」計劃的付費客戶。
4. IIS 伺服器遭受 SEO 中毒攻擊，使得網站擁有者面臨嚴重的風險，包括：商譽損失、潛在法律後果，以及喪失使用者的信任，這些全都是網站伺服器的安全性不足所導致。隨著攻擊者不斷改進攻擊策略，管理者必須保持警惕，監控並保護其 Web 基礎架構免受 BadIIS 等威脅。為了降低這類風險，管理單位可採用以下措施：

   (1) 找到可能遭受駭客攻擊的設備，確保設備定期檢查與安裝最新的資

安修補程式。

(2) 監控 IIS 是否安裝異常模組，檢視是否有安裝在奇怪目錄的檔案。

(3) 管控 IIS 伺服器的系統管理員存取權限，具有高權限帳號需要強制使用高強度、非重複的密碼，並搭配多重認證(MFA) 。

(4) 使用防火牆來監控 IIS 伺服器的進出流量，並持續檢查該伺服器紀錄檔(如 IIS log)，以偵測異常狀況或查找入侵跡象，例如:發生異常的模組安裝，不預期的伺服器行為。

(5) 停用非必要的服務與功能來確保組態設定的安全，縮小可能攻擊面並強化伺服器的整體安全。

參考資料

1. **SEO 詐騙新手法！BadIIS 攻擊瞄準 IIS 伺服器，使用者恐遭導向惡意網站**
https://www.trendmicro.com/zh_tw/research/25/b/chinese-speaking-group-manipulates-seo-with-badiis.html
2. **GhostRedirector poisons Windows servers: Backdoors with a side of Potatoes**
https://www.welivesecurity.com/en/eset-research/ghostredirector-poisons-windows-servers-backdoors-side-potatoes/
3. **BadIIS Malware Exploits IIS Servers for SEO**
https://www.infosecurity-magazine.com/news/badiis-malware-iis-servers-seo/