TLP:WHITE

利用 WinSxS 資料夾的 DLL 搜尋劫持攻擊分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2024 年 01 月

一、事件簡介

1. 2022 年 11 月學術網路陸續發現 Waterbear 中繼站攻擊事件。分析 Waterbear 系列案件發現駭客採用幽靈 DLL 挾持與 DLL 側載 (DLL Side Loading) 的方式載入惡意 DLL，接著利用檔案過大之 DLL，透過它將登錄檔的 Shellcode 解密後連線中繼站。由此可知，來自 DLL 的攻擊不容忽視。
2. 2024 年 1 月資安公司 Security Joes 發現一種新的 DLL 搜尋順序劫持的攻擊手法。該方法利用受信任的 WinSxS 資料夾中常見的可執行檔，允許駭客在攻擊中無需額外添加二進位檔案的情況下繞過高權限要求，進而在 WinSxS 資料夾內的應用程式中執行惡意程式碼。
3. 它不需要引入自己的二進位檔案，因為已經有各種可利用的檔案儲存在 WinSxS 資料夾中。與傳統的 DLL 搜尋順序劫持技術相比，這種方法降低了被防毒軟體和事件回應程式偵測到的可能性，因為惡意程式碼是從位於 C://Windows / WinSxS 資料夾內的二進位檔案的記憶體空間中執行的。

二、 DLL 搜尋順序劫持技術

1. DLL 搜尋順序劫持技術(DLL Search Order Hijacking)是指攻擊者可以透過劫持用於載入 DLL 的搜尋順序來執行自己的惡意 payload。
2. 根據 MITRE ATT&CK 資料，攻擊者可以採用多種方法來劫持 DLL 載入的過程，但所有這些方法都有一個共同點：目標應用程式未指定所需內容的完整路徑， 故駭客將惡意 DLL 放置在搜尋順序優先於合法 DLL 的目錄中。通常，此操作的首選位置是目標應用程式的工作目錄，因為它在搜尋順序中佔據顯著位置。
3. Windows 系統會尋找所需的 DLL 以載入到程式中，其所遵循的大致搜尋位置如下。

   (1)啟動應用程式的目錄。

(2)資料夾「C:\Windows\System32」。

(3)資料夾「 C:\Windows\System」。

(4)資料夾「 C:\Windows」。

(5)目前工作目錄。

(6)系統 PATH 環境變數中列出的目錄。

(7)在使用者的 PATH 環境變數中列出的目錄。

4. 關於應用 DLL 搜尋順序劫持技術的駭客團體有哪些，可從 MITRE ATT&CK 資料得知一些在入侵中已使用此技術的駭客團體如下，更多資訊可參閱本文參考資料。

駭客團體	說明
APT41	利用搜尋順序劫持技術來執行惡意 payload，例如 Winnti RAT。
Aquatic Panda	使用 DLL 搜尋順序劫持技術將 exe、dll 和 dat 檔案載入到記憶體中。
Downdelph	使用 DLL 搜尋順序劫持技術執行 sysprep.exe 來提升權限。
Evilnum	使用惡意軟體變種 TerraTV 載入位於 TeamViewer 目錄中的惡意 DLL，而不是位於系統資料夾中的原始 Windows DLL。
Hikit	使用 DLL 搜尋順序劫持技術來載入 oci.dll 作為持久機制。
RTM	使用搜尋順序劫持技術來強制 TeamViewer 載入惡意 DLL。
Threat Group-3390	已執行 DLL 搜尋順序劫持技術來執行其有效 payload。
Tonto Team	濫用合法且經過簽署的 Microsoft 執行檔來啟動惡意 DLL。
WEBC2	其變種透過使用 DLL 搜尋順序劫持技術來實現持久性，通常是將 DLL 檔案複製到系統目錄下(如 C:\WINDOWS\ntshrui.dll)。
Whitefly	使用搜尋順序劫持技術來執行載入程式 Vcrodat。

三、 WinSxS 資料夾

1. WinSxS（Windows Side by Side）資料夾是 Windows 作業系統維護和復原的關鍵元件存放區，通常位於 C:\Windows\WinSxS。

2. 它的主要功能是儲存各個版本的重要系統檔案。 當 Windows 進行更新時，它會在 WinSxS 資料夾中保留先前版本的元件。 因此，WinSxS 資料夾的大小往往會隨著每次 Windows 更新而增加。

3. 在安裝 Windows 元件、更新軟體期間，系統檔案儲存在 WinSxS 資料夾中。 該資料夾充當系統檔案（特別是 DLL）的集中儲存庫，這些檔案在各種應用程式和元件之間共享，以確保相容性並防止潛在的衝突。

4. WinSxS 資料夾的主要用途如下:

(1) 版本管理

它儲存 DLL 和多個版本的系統檔案，確保根據需要進行高效存取。 此功能對於保持與各種應用程式的相容性至關重要，因為不同的程式可能需要同一元件的特定版本。

(2) 系統完整性

WinSxS 資料夾透過防止不正確或損壞的系統檔案版本取代正確的系統檔案，來維護系統的完整性，這保證了作業系統的

穩定性和可靠性。

(3) 動態啟動

此資料夾有助於使用者根據需要動態啟用或停用 Windows 的特定功能，無需單獨安裝。

5. 有關 WinSxS 資料夾的二進位檔案相依性劫持技術，是針對位於 WinSxS 資料夾中的應用程式，改進了傳統的 DLL 搜尋順序劫持技術。其主要優點如下:

(1) 規避高權限要求

透過針對 WinSxS 資料夾中的應用程式，無需提升權限即可在應用程式中執行惡意程式碼。

(2) 消除對額外二進位檔案的需求

由於 Windows 已經在 WinSxS 資料夾中索引了這些二進位檔案，因此無需駭客攜帶自己易受攻擊的應用程式。

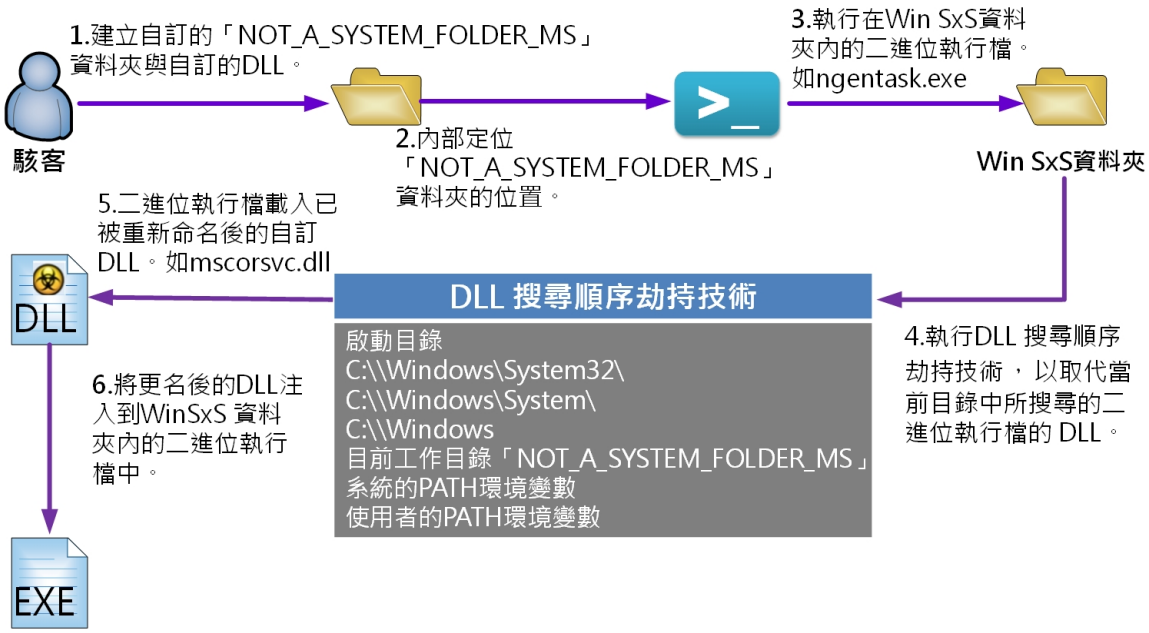
(3) 增強隱蔽性

在從 WinSxS 資料夾執行的應用程式的記憶體空間中執行惡意程式碼，可以增強隱蔽性並最大限度地降低檢測風險。

四、 攻擊流程

針對 WinSxS 資料夾內應用程式的 DLL 搜尋順序劫持技術的

攻擊流程如下圖。首先，駭客會先建立自訂的「NOT_A_SYSTEM_FOLDER_MS」 資料夾與自訂的 DLL，接著在主機內部定位該資料夾的位置，之後執行在 Win SxS 資料夾內的二進位執行檔，例如:執行 ngentask.exe。執行它後，主機會啟動執行 DLL 搜尋順序劫持技術，來取代當前目錄中所搜尋的二進位執行檔的 DLL。之後二進位執行檔會載入已被重新命名的自訂 DLL，例如:mscorsvc.dll。最後會將更名後的 DLL 注入到 WinSxS 資料夾內的二進位執行檔中。



五、 總結與建議

1. 本文所介紹之攻擊手法是指利用搜尋二進位執行檔所用之 DLL 時，以駭客自訂的 DLL 更名後讓系統優先搜尋到它。這種取代原

先 DLL 的方式為 DLL 搜尋順序劫持攻擊，而此攻擊所需之二進位執行檔都存在 WinSxs 資料夾內。

2. 這種技術將傳統的 DLL 搜尋順序劫持與複雜的 WinSxS 資料夾結合，展示了網路威脅不斷演變的本質。它讓駭客不需要準備要執行的二進位執行檔，只需利用一個命令列與注入自訂的 DLL 即可進行攻擊，而且它能有效避開防毒軟體偵測，讓使用者不易察覺異常。

3. 關於此類攻擊手法可能造成的影響，由於 DLL 搜尋順序劫持技術會以自訂的惡意 DLL 取代原二進位執行檔所用的 DLL，所以會對 CIA 中的完整性造成衝擊。

4. 下面有兩項偵測此類型攻擊與其預防措施，提供大家參考。

(1) 程序分析

(1.1) 可利用微軟 Process Explorer 工具查看程序執行時呼叫哪些 DLL，再查看程序所用 DLL 是否有儲存在異常位置。

(1.2) 檢查程序之間的父、子程序關係，尤其是受信任的二進位檔案。 可尋找涉及以下內容的活動：

(a)從 WinSxS 資料夾呼叫二進位檔案的異常程序。

(b)在 WinSxS 資料夾內二進位檔案產生意外的子程序。

(2) 行為分析

監視 WinSxS 資料夾內二進位檔案執行的所有活動，例如:網路連線和檔案操作。可以尋找以下的活動：

(a)連接到遠端伺服器的 WinSxS 二進位檔案。

(b)WinSxS 二進位檔案從不常見的資料夾載入模組。

參考資料

1. **Hijack Execution Flow: DLL Search Order Hijacking**
   https://attack.mitre.org/techniques/T1574/001/
2. **Hide and Seek in Windows' Closet: Unmasking the WinSxS Hijacking Hideout**
   https://www.securityjoes.com/post/hide-and-seek-in-windows-closet-unmasking-the-winsxs-hijacking-hideout
3. **How to Find Out What DLLs Are Loaded by a Process**
   https://forums.ivanti.com/s/article/How-to-find-out-what-DLLs-are-loaded-by-a-process?language=en_US