



保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

DLL 側載攻擊 --隱蔽的攻擊途徑

2025 年 11 月 18 日發布



點擊此處可獲取--最完整的賽門鐵克解決方案資訊

DLL 側載是一種常見且複雜的網路安全攻擊手法，其利用 Windows 作業系統載入動態連結函式庫 (DLL) 的機制進行攻擊。其運作原理在於：攻擊者將惡意 DLL 檔案放置於合法應用程式預設搜尋位置，該位置通常是受信任應用程式會搜尋並載入必要合法 DLL 的預設路徑。由於 Windows 系統對這些檔案的搜尋順序機制，合法程式會被誘導載入攻擊者植入的惡意 DLL。此舉使攻擊者得以在受信任程序的掩護下執行惡意程式碼--從安裝勒索軟體到建立持久化機制皆有可能--往往能成功躲避安全軟體的偵測。

本公告著重技術層面，將探討近期發現的一款 PowerShell 腳本，該腳本會下載 Microsoft 軟體安裝程式 (MSI)。MSI 是 Windows 安裝程式服務用於在 Windows 作業系統上安裝、維護及移除軟體的檔案套件。

PowerShell 腳本

該 PowerShell 腳本是透過 ClickFix 詐騙手段下載的。ClickFix 詐騙是一種複雜的社交工程技術，攻擊者藉此誘騙使用者在電腦上手動執行惡意程式碼。此方法能繞過許多傳統安全防護措施，因為使用者是自行執行操作，使得安全軟體誤判其為合法行為。

當經過高度混淆的 PowerShell 腳本被還原並執行後，我們可觀察到腳本的最後一條指令會開啟網頁瀏覽器，顯示合法網址「hxxps://admin.booking.com」，同時從網域「hxxp://maut-swiss.com」下載 MSI 檔案。

MSI 安裝程式檔案

下載的 MSI 檔案由 PowerShell 腳本中的「msiexec.exe」執行。該 MSI 會安裝一個可執行檔 (EXE)、若干 DLL 檔案及資料檔案。此 EXE 檔預設為首個執行項目，其會載入 sciter-x.dll 檔案--此為合法 DLL 檔案的修改版本，該合法 DLL 廣泛用於網路存取功能。

Tables	File	Component	FileName	FileSize	Version
AdminExecuteSequence	whSkWDPV5P	whSkWDPV5P	ip1p_mkn.exe\CIDrive16.exe	7988592	10.48.20.0
AdminUISequence	bw8KwzFGjNpMYvb4N3v	bw8KwzFGjNpMYvb4N3v	Breebgoo.rh	1566062	
AdvExecuteSequence	tmo4TLarNO39IM0Iusgc	tmo4TLarNO39IM0Iusgc	iwcbbqw-w.r\Deegbortkcloud.rl	33159	
Component	viM6fon1J7MG1Wb	viM6fon1J7MG1Wb	libcurl.dll	798032	8.10.1.0
CustomAction	PtxuLQ8mcFo	PtxuLQ8mcFo	MSVCP140.dll	575088	14.40.33810.0
Directory	BgAVGDNMMN6yK1c	BgAVGDNMMN6yK1c	x1oiaigm.dll\ProtobufLite.dll	544112	10.48.20.0
Feature	EFExzCj4J5z	EFExzCj4J5z	sciter-x.dll	4217720	11.0.54.0
FeatureComponents	oK513eMOI7	oK513eMOI7	ovihkqlt.dll\VCRUNTIME140.dll	118896	14.40.33810.0
File	hG3vvZDdOfpOjoWGpIXU	hG3vvZDdOfpOjoWGpIXU	et4g40qb.dll\vcruntime140_1.dll	49792	14.44.35112.1
InstallExecuteSequence					

Sciter-x

Sciter-x DLL 檔案已修改，使其在 DLL 初始化時載入 libcurl.dll。

```
.rdata:0000000180316DE0 dq offset sub_180001C50
.rdata:0000000180316DE8 dq offset sub_180001CA0
.rdata:0000000180316DF0 dq offset sub_180001CF0
.rdata:0000000180316DF8 dq offset sub_180001D40
.rdata:0000000180316E00 dq offset sub_180001D90
.rdata:0000000180316E08 dq offset sub_180001DE0
.rdata:0000000180316E10 dq offset sub_180001E30
.rdata:0000000180316E18 dq offset sub_180001E80
.rdata:0000000180316E20 dq offset hacked_func1
.rdata:0000000180316E28 dq offset sub_180001F00
.rdata:0000000180316E30 dq offset sub_180001F50
.rdata:0000000180316E38 dq offset sub_180002010
.rdata:0000000180316E40 dq offset sub_180002090
.rdata:0000000180316E48 dq offset sub_1800020D0
.rdata:0000000180316E50 dq offset sub_1800020E0
.rdata:0000000180316E58 dq offset sub_180002110
```

sciter-x.dll 包含上述一組函式庫清單，這些函式庫會在 DLL 附加至程序時 (即載入時) 被呼叫。其中一個函式庫顯然存在疑慮。

```
.text:0000000180001EA0 hacked_func1 proc near ; DATA XREF: .rdata:0000000180316E20j0
.text:0000000180001EA0 ; .rdata:000000018031736Cj0
.text:0000000180001EA0 ; .pdata:00000001803CE1D4j0
.text:0000000180001EA0 ; .pdata:00000001803CE1E0j0
.text:0000000180001EA0 arg_0
.text:0000000180001EA0
.text:0000000180001EA0
.text:0000000180001EA4
.text:0000000180001EA9
.text:0000000180001EAE
.text:0000000180001EB3
.text:0000000180001EB6
.text:0000000180001EB8
.text:0000000180001EBE
.text:0000000180001EC6
.text:0000000180001EC9
.text:0000000180001ECB
.text:0000000180001ED2
.text:0000000180001ED5
.text:0000000180001ED9
.text:0000000180001EDC
.text:0000000180001EE2
.text:0000000180001EE2 loc_180001EE2 ; CODE XREF: hacked_func1+29Tj
.text:0000000180001EE2 lea rcx, sub_180312998 ; void (__cdecl *)( )
.text:0000000180001EE9 add rsp, 28h
.text:0000000180001EE9 jmp atexit
.text:0000000180001EE0 hacked_func1 endp
```

該函式庫保留了幾乎相同的程式碼，但首次呼叫指令的目標與正版函式庫不同。此呼叫目標透過 LoadLibraryW API 載入「libcurl.dll」。相較之下，相同版本的正版 sciter-x.dll 並沒有「libcurl.dll」呼叫 LoadLibraryW 的行為。

```
.text:00000001800088A0 HACKED_LOCATION: sub rsp, 258h ; CODE XREF: hacked_func1+91p
.text:00000001800088A7 lea rax, off_1803B89C4 ; "libcurl.dll"
.text:00000001800088AE mov [rsp+368h+var_118], rax
.text:00000001800088B6 lea rax, [rsp+368h+var_328]
.text:00000001800088BB mov [rsp+368h+var_330], rax
.text:00000001800088C0 mov rax, [rsp+368h+var_118]
.text:00000001800088C8 mov rax, [rax]
.text:00000001800088D0 mov [rsp+368h+var_338], rax
.text:00000001800088D0 loc_1800088D0 ; CODE XREF: sub_180008670+291j
.text:00000001800088D0 mov rax, [rsp+368h+var_338]
.text:00000001800088D5 mov rcx, rax
.text:00000001800088D8 add rcx, 2
.text:00000001800088DC mov [rsp+368h+var_338], rcx
.text:00000001800088E1 mov cx, [rax]
.text:00000001800088E4 mov rax, [rsp+368h+var_330]
.text:00000001800088E9 mov rdx, rax
.text:00000001800088EC add rdx, 2
.text:00000001800088F0 mov [rsp+368h+var_330], rdx
.text:00000001800088F5 mov [rax], cx
.text:00000001800088F8 mov rax, [rsp+368h+var_338]
.text:00000001800088FD cmp word ptr [rax], 0
.text:0000000180008901 jnz short loc_1800088D0
.text:0000000180008903 mov rax, [rsp+368h+var_330]
.text:0000000180008908 mov rcx, rax
.text:000000018000890B add rcx, 2
.text:000000018000890F mov [rsp+368h+var_330], rcx
.text:0000000180008914 mov word ptr [rax], 0
.text:0000000180008919 lea rcx, [rsp+368h+var_328] ; lpLibFileName
.text:000000018000891E call cs:LoadLibraryW
.text:0000000180008924 mov [rsp+20h], rax
```

Libcurl

libcurl.dll 檔案亦遭修改，並執行惡意行為。

```
.text:0000000180034400 sub rsp, 1C8h
.text:0000000180034400 lea rax, off_1800086509 ; 'Deegbortkcloud.rl'
.text:0000000180034407 mov [rsp+1C8h+var_188], rax
.text:0000000180034413 mov rax, [rsp+1C8h+var_188]
.text:0000000180034418 mov [rsp+1C8h+var_48], rax
.text:0000000180034418 ; DATA XREF: .rdata:00000001800AF1ECj0
.text:0000000180034418 ; .rdata:00000001800AF200j0
.text:0000000180034418 ; .pdata:00000001800BE00Cj0
.text:0000000180034418 ; .pdata:00000001800BE018j0
.text:0000000180034420
.text:0000000180034425 mov rax, [rsp+1C8h+var_188]
.text:0000000180034429 mov rcx, [rax+60h] ; lpModuleHane
.text:0000000180034437 call cs:GetModuleHandleW
.text:000000018003443F mov [rsp+1C8h+var_30], rax
.text:0000000180034444 call mal_get_export_table
.text:0000000180034449 mov rax, [rsp+1C8h+var_188]
.text:000000018003444C mov edx, [rax+58h]
.text:0000000180034454 lea rcx, [rsp+1C8h+var_78]
.text:0000000180034459 call hacked_func2_get_api_by_hash
```

修改後的 libcurl.dll 會讀取由 MSI 安裝的「Deegbortkcloud.rl」檔案。此檔案為加密資料檔，經解密後執行。

賽門鐵克防護機制

- 經修改的 DLL 檔案將被偵測為 Trojan.DllhiJack!gen7 與 Trojan.DllhiJack!gen8
- 惡意 MSI 及 PowerShell 腳本將被偵測為 Trojan.Gen.2、Trojan.Gen.MBT 及 Trojan Horse
- 檔案「Deegbortkcloud.rl」可能被偵測為資訊竊取程式、後門程式，或作者決定作為最終有效載荷的任何其他惡意軟體

欲深入瞭解更多有關賽門鐵克端點安全完整版 (SESC) 的詳細資訊--Symantec Endpoint Security Complete，請[點擊此處](#)。

Symantec
A Division of Broadcom

是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦 (CA Technologies) 以及雲端運算及「硬體虛擬化」的領導廠商--VMware，也是博通軟體事業部的成員。) 2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署 (CISA) 宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵召的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (Broadcom)，美國晶片代號 AVGO，全世界國際網路流量有 99.9% 經過博通的網通晶片，軟體事業部的企業安全部門 (SED) 以及雲端運算，近年來以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公開機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢能提供更快速有效的技術支援回應。深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信賴的資安建議者、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的求助諮詢對象。

保安資訊連絡電話：0800-381-500。