Lancefly：該組織使用客製化後門攻擊政府、航空以及其他行業

2023 年 5 月 15 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

Metdoor 是一個低度使用率但確有高度針對性攻擊的後門

Lancefly 進階持續性滲透攻擊 (APT) 組織正在攻擊南亞和東南亞地區的機構，其攻擊活動已持續數年，並使用客製化的後門。

Lancefly 可能與以前已知的組織存在一些聯繫，但相關證據不足。因此 Symantec (屬於 Broadcom Software) 的研究人員將這些活動歸類為一個新群組。

Lancefly 的客製化惡意軟體被我們稱為 Merdoor，是一個功能強大的後門，從 2018 年開始就存在。Symantec的研究人員觀察到它在 2020 年和 2021 年的某些攻擊活動中被使用，並在近期的攻擊活動中更常見且一直延續到 2023 年第一季。這兩項活動背後的動機被認為是在從事情報收集。

這個後門的使用非常有選擇性與針對性，多年來只在少數網路和少量機器上出現。在這次攻擊中，攻擊者還使用更新版本的 ZXShell rootkit。

最近的攻擊活動始於 2022 年中期，一直延續到2023年，目標位於南亞和東南亞地區，涵蓋政府、航空、教育和電信等行業。Symantec的研究人員此前在 2020 年至 2021 年的攻擊活動中也觀察到 Merdoor 後門被用於攻擊這些地理區域內的政府、通訊和技術領域。與這次最近的攻擊活動類似，那次攻擊活動也表現出高度的針對性，只有少數機器受到感染。

Merdoor 後門

Merdoor是一個功能齊全的後門，從2018年開始存在。

該後門具有以下功能：

- 將自身安裝為服務
- 鍵盤側錄
- 使用多種方法與命令及控制 (C&C) 伺服器進行通訊 (HTTP、HTTPS、DNS、UDP、TCP)
- 能夠監聽本地通訊埠以接收指令

Merdoor後門的實例除了嵌入和加密的設定之外，通常都是完全相同。這些設定定義：

- C&C通訊方法
- 服務細節
- 安裝目錄

通常，該後門被注入到合法處理程序 perfhost.exe 或 svchost.exe 中。

Merdoor 病毒散播程式是一個自動解壓縮的 RAR(SFX) 檔，包含三個檔案：

- 一個含有 DLL 搜尋順序劫持漏洞且具有合法數位簽章的可執行檔
- 一個惡意程式載入器 (Merdoorloader)
- 一個包含最終有效負載的加密檔案 (.pak，Merdoor 後門)

當病毒散播程式被開啟後，它會自動解開檔案並執行合法的可執行檔，以載入Merdoor loader。

目前已發現 Merdoor 的變種，它們濫用五個不同合法應用程式的舊版本來進行 DLL 側載：

合法可執行檔	版本	簽名日期	載入器 (Merdoor loader)	加密有效負載 (Merdoor後門)
SiteAdv.exe (McAfee SiteAdvisor)	1.6.0.23	08/10/2006	SiteAdv.dll	SiteAdv.pak
ssr32.exe (Sophos SafeStore Restore)	1.3.0.1	11/17/2017	safestore32.dll	safestore.pak
chrome_frame_helper.exe (Google Chrome Frame)	27.0.1453.110	05/29/2013	chrome_frame_helper.dll	chrome_frame_helper.pak
wsc_proxy.exe (Avast wsc_proxy)	1.0.0.3	10/28/2019	wsc.dll	proxycfg.pak
coInst.exe (Norton Identity Safe)	2014.7.3.12	06/26/2014	msvcr100.dll	coinstcfg.dat

表1. 遭受 Merdoor 濫用於 DLL 側載的合法應用程式列表

攻擊鏈

證據顯示 Lancefly 早在 2020 年開始進行攻擊活動，在那次活動中，該組織可能使用一個以第 37 屆東盟峰會為誘餌的釣魚郵件作為初始感染媒介。

在近期的攻擊活動中，初始感染媒介並不完全清楚。我們在兩個受害者中看到一些初始感染媒介的跡象，雖然這仍不確定。

- 在一個受害的政府部門中，有跡象表明初始感染媒介可能是 SSH 暴力破解。多個開放原始碼軟體中發現，該攻擊活動威脅者使用的 IP 位址之一與 SSH 暴力破解有相關聯，這表明初始感染媒介可能是 SSH 暴力破解。
- 在另一個受害者中，檔案路徑 (Csidl_program_files\loadbalancer\ibm\edge\lb\servers\bin) 表明負載平衡器可能已被利用以獲取存取權限，這表明初始感染媒介可能是一個直接位於網際網路對公眾開放的伺服器。

儘管這些感染媒介的證據並非確定的，但它似乎表明 Lancefly 在使用感染媒介方面具有適應性。

使用非惡意軟體技術進行認證竊取

在早期 2020/2021 年活動中，攻擊者使用多種非惡意軟體技術來竊取受害者電腦上的認證：

- 使用 PowerShell 啟動 rundll32.exe，並使用 comsvcs.dll 的 MiniDump 函式功能傾印處理程序的記憶體。這種技術通常用於傾印 LSASS服務的記憶體。
- 使用 Reg.exe 傾印 SAM 和 SYSTEM 註冊表。
- 攻擊者安裝 Avast 的一個合法工具，並用於傾印 LSASS 記憶體。

攻擊者還使用了偽裝的壓縮解壓縮工具 WinRAR 在數據洩漏之前對檔案進行暫存和加密。

值得注意的攻擊鏈工具和 TTP (戰術、技術和過程)：

- **Impacket Atexec**：這是一個雙重用途工具，惡意行為者可以使用它通過 SMB 在遠端目標上建立和執行即時排程工作，以執行目標系統上的命令。Lancefly 將其用於在受害者網路之間進行橫向移動，還可能用於 Shellcode 執行和迴避。它也可能被用於刪除 cmdline 輸出的檔案。
- **可疑的 SMB 活動**：多個受害者電腦上觀察到可疑的 SMB 活動。這可能與攻擊者使用 Impacket 有關。
- **WinRAR**：一個用於壓縮或解壓縮檔案的管理軟體，例如：在數據洩漏之前。目前不清楚攻擊者如何從受害者電腦中外傳數據，但最有可能是通過 Merdoor進行。
- **LSSAS Dumper**：允許攻擊者迅速竊取認證，然後用於在受害者網路中進一步獲取存取權限。
- **NBTScan**：開源命令行 NetBIOS 掃描器，可用於收集網路訊息。
- **Blackloader 和 Prcloader**：該組織使用的載入器。這些載入器在早期的 2020 年和 2021 年 Merdoor 活動中也被使用過。它們與 PlugX 的傳播有關。這兩個載入器似乎都被側載到受害者電腦上。目前不清楚這些載入器是否僅由 Lancefly 使用，還是它們在多個組織之間共享使用。

在受害者電腦中可以發現典型的 Merdoor 攻擊鏈包括：

- Merdoor 被注入到 perfhost.exe 或 svchost.exe 中。
- 接著通常觀察到可疑的 SMB 活動，並且後門連接到其 C&C 伺服器。
- 通常緊隨其後的是可疑的 Living-off-the-Land 活動，例如：執行 mavinject.exe (可用於處理程序注入) 和 createdump.exe (可用於傾印處理程序，例如：LSASS) 等命令。
- 然後使用偽裝的 WinRAR (wmiprvse.exe) 文件暫存和加密檔案，大概是在洩漏之前。我們實際上並沒有看到從受害者網路中洩露的檔案，但我們假設 Merdoor 後門本身就是用來洩露它們。

ZXShell Rootkit 技術細節

ZXShell Rootkit 最早是在思科 2014 年報告中出現，但 Lancefly 使用的版本已經更新，表明它仍在積極開發中。Rootkit 原始碼是公開可用的，所以可能被多個不同的組織使用。Lancefly 使用新版本 Rootkit 似乎體積更小，同時還具有額外的功能，並且針對額外的防毒軟體進行停用。

載入器

Rootkit的載入器是一個32位元的 DLL檔，檔案名稱為 "FormDll.dll"(SHA256: 1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7)。

它具有以下匯出函式：

- "CallDriver"
- "DoRVA"
- "KillAvpProcess"
- "LoadSys"
- "ProtectDllFile"

函式 "LoadSys"

每當執行匯出函式 "LoadSys" 時，它會根據處理器架構引入以下檔案之一：

- "[Windows目錄]\system32\drivers\TdiProxy.sys"
- "[Windows目錄]\system64\drivers\TdiProxy.sys"

這些文件是惡意的 Windows 核心驅動程式。這是幾年前在 RSA 部落格中首次記錄的變種驅動程式。

它的 PDB 檔案名稱為："c:\google\objchk_win7_amd64\amd64\Google.pdb"

樣本建立一個名為 "\Device\TdiProxy0" 的設備。

它還建立一個符號鏈接 "\DosDevices\TdiProxy0"，以便可以使用路徑名稱 "\.\TdiProxy0" 來控制它。

之後，載入器通過從 "[Windows目錄]\system32\drivers\http.sys" 檔案複製時間戳記來為導入的檔案設置時間戳記。

然後它使用以下參數建立一個服務：

- ServiceName = "TdiProxy0"
- DisplayName = "TdiProxy0"(後來替換為"TdiProxy")
- BinaryPathName = "[Windows目錄]\system32\drivers\TdiProxy.sys"

函式"CallDriver"

"CallDriver" 開啟由惡意核心驅動程式所建立的 “\.\TdiProxy0” 設備。

它使用 DeviceIoControl API 與該設備進行溝通。

該匯出函式使用兩個參數。第一個參數決定當呼叫 DeviceIoControl API 時使用 dwIoControl Code 參數，它應該是以下字串之一：

- "-init",
- "-file",
- "-pack",
- "-port",
- "-removetcpview",
- "-tcpview",
- "-clearall",
- "-clear",
- "-transport",
- "-waitport",
- "-kill",
- "-antiscan",
- "-removeprocessnotify",
- "-setprocessnotify",
- "-antiantigp",
- "-hideproc",
- "-hidekey",
- "-hidefile",
- "-setprotect",

其他任何值都會導致看起來像是錯誤的 dwIoControlCode 值。第二個參數是一個字串，在呼叫 DeviceIoControl API 時，在使用 MultiByteToWideChar API 進行轉換後，作為 lpInBuffer 參數傳遞。

函式"DoRVA"

當執行匯出函式 "DoRVA" 時，它會讀取以下檔案：

- "[DLL的檔案目錄]\Form.hlp"

該檔案會以特殊的字串 "AP32" 開頭，並以壓縮形式包含要執行的 Shellcode。

函式"KillAvpProcess"

它會列出正在運行的處理程序，並對選定的處理程序呼叫自己的匯出函式 "CallDriver"，並使用以下參數：

- 第一個參數："-kill"
- 第二個參數："[ProcessID]"

該匯出函式使用單一的字串參數，與正在運行的處理程序的執行檔進行比較，以便選擇。

函式"ProtectDllFile"

它使用以下參數呼叫自己的匯出函式 "CallDriver"：

- 第一個參數："-file"
- 第二個參數："[DLL的檔案路徑]"

接下來，它設置以下的登錄值：

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.ptdf\"ptdffile" = "[DLL的檔案路徑]"

載入點

這是一個 32 位元的執行檔，其 PDB 檔案名稱為："M:\Project\database\10.0.18362\Form\Release\Form.pdb"。(SHA256: 180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e)

每當執行樣本時，它載入以下的 DLL：

- "[正在運行的執行檔的路徑]\FormDll.dll"

它還呼叫其匯出函式："DoRVA"。

安裝和更新公用程式

安裝和更新公用程式是一個 32 位元的PE執行檔 (SHA256: a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221)，與 Merdoor 載入器共用小片段的獨特的程式碼，這表明它們是同一工具集的一部分。

每當樣本被執行時，它會嘗試讀取並刪除包含其設定資料的以下檔案：

- "[正在運行的執行檔的目錄]\res.ini"

更新功能

接下來，它檢查以下內容：

- "\\.\TdiProxy0" 設備是否可用，並且

・它自己的處理程序是否是以命令行參數 "-up" 啟動的。

如果兩個檢查都通過，樣本將嘗試使用 "\.\TdiProxy0" 設備對各種防毒軟體進行干擾。例如：它可能終止處理程序 "egui.exe"、"ekrn.exe" 和 "msmpeng.exe"。

接下來，它嘗試將文件 "[正在運行的執行檔的目錄]\res.dat" 重新命名為以下之一 (取決於Windows版本)：

・"[SystemDrive]\Users\All Users\Windows Defender\temp.temp"
・"[Windows目錄]\temp.temp"。

根據程式碼的結構，上述文件會以特殊的字串 "AP32" 開頭，並且可能以壓縮形式包含一個 DLL 檔。然後，樣本解壓縮重新命名的 "temp.temp" 檔。在解壓縮時，它會在同一資料夾中建立臨時的檔案 "temp.temp.pack"。

接下來，樣本在解壓縮檔的末端附加一個特定標記，後面跟著 "[正在運行的執行檔的目錄]\res.ini" 的內容 (使用 XOR 運算對金鑰 0x12 進行轉換)。

此外，它還建立了以下登錄值：

・HKEY_CLASSES_ROOT\.udf\"BINTYPE" = [使用 XOR 運算對金鑰 0x12 進行轉換的 "[正在運行的執行檔的目錄]\res.ini" 的內容]

然後，樣本檢查以下檔案是否存在：

・"[SystemDrive]\Users\All Users\Windows Defender\DefenderSvc.dll"

如果存在，則將使用已更新的 "temp.temp" 檔重新命名並替換它。
否則，它檢查以下登錄值以取得要替換的路徑名稱：

・HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.ecdf\"ecdffile"

如果失敗，則使用設定資料中的預設值。
最後，它檢查以下登錄值以獲取服務名稱：

・HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.tudf\"tudffile"

然後，它重新啟動引用的服務。

安裝功能

樣本嘗試解壓縮以下檔案：

・"[正在運行的執行檔的目錄]\google64.p"(64位元處理器架構)，或
・"[正在運行的執行檔的目錄]\google32.p"(32位元處理器架構)

解壓縮為：

- "[Windows目錄]\Microsoft.NET\Framework64\iesockethlp.dll"(64元位處理器架構)，或
- "[Windows目錄]\Microsoft.NET\Framework\iesockethlp.dll"(32位元處理器架構)

然後，它可能修改以下登錄值之一，以劫持相應的服務：

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\exfat\"ImagePath" = "\??\[上述解壓縮檔的路徑名]", 或
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RDPWD\"ImagePath" = "\??\[上述解壓縮檔的路徑名]"

接下來，它啟動相應的服務，然後刪除登錄值。然後，它嘗試使用 "\.\TdiProxy0" 設備對各種防毒軟體進行干擾。

然後，它建立具有以下參數的服務：

- ServiceName: "[根據設定資料]"
- ImagePath:
  - "%SystemRoot%\System32\svchost.exe -k netsvcs"，或
  - "%SystemRoot%\System32\svchost.exe -k ntmssvcs"
- Parameters:
  - ServiceDll:
    - "C:\WINDOWS\Microsoft.NET\Framework64\[根據設定資料]"，或
    - "C:\WINDOWS\Microsoft.NET\Framework\[根據設定資料]"

然後，它建立以下登錄值：

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.tudf\"tudffile" = [建立的服務名稱]

然後，它刪除以下登錄值：

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.ptdf\"ptdffile"
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.ecdf\"ecdffile"

接下來，它將以下檔案重新命名：

- "[正在運行的執行檔的目錄]\res.dat"

為：

- "[Windows目錄]\Microsoft.NET\Framework64\[根據設定資料].back"(64位處理器架構)，或
- "[Windows目錄]\Microsoft.NET\Framework\[根據設定資料].back"(32位元處理器架構)

根據程式碼結構，上述文件應以特殊的字串 "AP32" 開頭，並且可能以壓縮形式包含一個 DLL 文件(使用 aPLib 進行壓縮)。

接下來，樣本將被重新命名的 "[根據設定資料].back" 解壓縮為 "[根據設定資料]"。

然後，樣本在解壓縮檔的末端附加特定標記，後面是 "[正在運行的執行檔的目錄]\res.ini" 的內容(使用 XOR 運算對金鑰 0x12 進行轉換)。

此外，它還建立以下登錄值：

- HKEY_CLASSES_ROOT\.udf\"BINTYPE" = ["[正在運行的執行檔的目錄]\res.ini" 的內容(使用 XOR 運算對金鑰 0x12 進行轉換)]

最後，當設定資料包括選項 "OneSelfKey" 時，它會對本身的執行檔產生壓縮副本 (使用 aPLib 進行壓縮)：

- "[Windows目錄]\SysWOW64\nethlp.hlp"(64位處理器架構)，或
- "[Windows目錄]\system32\nethlp.hlp"(32位元處理器架構)。

一些樣本包含帶有最終有效負載的嵌入式檔案：

- "Msrpcsvc.dll"

這是ZXShell後門的變體(SHA256: d5df686bb202279ab56295252650b2c7c24f350d1a87a8a699f6034a8c0dd849)

可能與其他組織聯繫

Lancefly 使用的 ZXShell rootkit 由 "Wemade Entertainment Co. Ltd" 簽名的憑證，此憑證曾被報導與 APT41(又稱Blackfly/Grayfly) 有關聯。然而，已知中國的 APT 組織 (例如：APT41) 經常與其他 APT 組織共享憑證。ZXShell 後門此前也曾被 HiddenLynx/APT17 組織使用，但由於 ZXShell 的原始碼現在已經公開，這並不能明確將這兩個組織聯繫起來。

值得注意的是，ZXShell rootkit 的載入器元件名為 "formdll.dll"，它具有讀取 "Form.hlp" 檔案並將其內容作為 shellcode 執行的能力。在之前的報告中詳細描述 Iron Tiger(又稱Budworm/APT27) 組織的活動，提到使用這些檔案名稱將 PlugX 後門加載到受害機器上。這些檔案的普及率非常低，這可能表明該活動與該組織之間存在潛在聯繫。

Lancefly 還使用 PlugX。PlugX 是一種遠端存取特洛伊木馬 (RAT)，具有後門存取和數據竊取等多種功能。PlugX 存在已經超過十年的時間。最初由中國的 APT 組織使用，但現在已被廣泛使用，因此很難將其作為活動歸因的方式。

這些攻擊者還使用 ShadowPad。ShadowPad 是一種模組化的RAT，被認為是中國的 APT 組織獨家使用。它的功能類似於 PlugX，並經常被稱為 PlugX 的後繼者。

儘管這些相同點和共享工具可能表明 Lancefly 的活動與其他 APT 組織的活動之間存在一些聯繫，但沒有任何足夠的相同證明，可將這種活動和 Merdoor 後門開發歸因給已知的攻擊組織。

值得注意的後門和有針對性的活動

最近的 Lancefly 活動之所以引人注目，是因為它使用 Merdoor 後門，而且該後門的普及率很低，而且這些攻擊似乎具有高度針對性。雖然 Merdoor 後門似乎已經存在好幾年，但在那段時間裡它似乎只被用於少數攻擊。對該工具的謹慎使用可能表明 Lancefly 希望將其活動保持低調。

所使用的工具和針對的部門都表明該攻擊活動的動機是情報收集。最近的活動與 Lancefly 之前活動之間的相似之處表明該組織可能沒有意識到早期活動已被發現，因此不擔心兩者之間的聯繫。這一活動的曝光是否會導致該組織開展活動的方式發生任何改變，還有待觀察。

防護方案／緩解措施

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (IOCs)

Merdoor Backdoor

SHA256 Filename Description

13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581 – a.exe – Merdoor Dropper

8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead – chrome_frame_helper.exe – Merdoor Dropper

8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38 – siteadv.exe – Merdoor Dropper

89e503c2db245a3db713661d491807aab3d7621c6aff00766bc6add892411ddc – siteadv.exe – Merdoor Dropper

c840e3cae2d280ff0b36eec2bf86ad35051906e484904136f0e478aa423d7744 – siteadv.exe – Merdoor Dropper

5f16633dbf4e6ccf0b1d844b8ddfd56258dd6a2d1e4fb4641e2aa508d12a5075 – chrome_frame_helper.dll – Merdoor Loader

ff4c2a91a97859de316b434c8d0cd5a31acb82be8c62b2df6e78c47f85e57740 – chrome_frame_helper.dll – Merdoor Loader

鎮14edb3de511a6dc896181d3a1bc87d1b5c443e6aea9eeae70dbca042a426fcf3 – chrome_frame_helper.dll – Merdoor Loader

db5deded638829654fc1595327400ed2379c4a43e171870cfc0b5f015fad3a03 – chrome_frame_helper.dll – Merdoor Loader

e244d1ef975fcebb529f0590acf4e7a0a91e7958722a9f2f5c5c05a23dda1d2c – chrome_frame_helper.dll – Merdoor Loader

f76e001a7ccf30af0706c9639ad3522fd8344ffbdf324307d8e82c5d52d350f2 – chrome_frame_helper.dll – Merdoor Loader

dc182a0f39c5bb1c3a7ae259f06f338bb3d51a03e5b42903854cdc51d06fced6 – smadhook64c.dll – Merdoor Loader

fa5f32457d0ac4ec0a7e69464b57144c257a55e6367ff9410cf7d77ac5b20949 – SiteAdv.dll, chrome_frame_helper.dll – Merdoor Loader

fe7a6954e18feddeeb6fcdaaa8ac9248c8185703c2505d7f249b03d8d8897104 – siteadv.dll – Merdoor Loader

341d8274cc1c53191458c8bbc746f428856295f86a61ab96c56cd97ee8736200 – siteadv.dll – Merdoor Loader

f3478ccd0e417f0dc3ba1d7d448be8725193a1e69f884a36a8c97006bf0aa0f4 – siteadv.dll – Merdoor Loader

750b541a5f43b0332ac32ec04329156157bf920f6a992113a140baab15fa4bd3 – mojo_core.dll – Merdoor Loader

9f00cee1360a2035133e5b4568e890642eb556edd7c2e2f5600cf6e0bdcd5774 – libmupdf.dll – Merdoor Loader

a9051dc5e6c06a8904bd8c82cdd6e6bd300994544af2eed72fe82df5f3336fc0 – chrome_frame_helper.dll – Merdoor Loader

d62596889938442c34f9132c9587d1f35329925e011465c48c94aa4657c056c7 – smadhook64c.dll – Merdoor Loader

f0003e08c34f4f419c3304a2f87f10c514c2ade2c90a830b12fdf31d81b0af57 – SiteAdv.pak – Merdoor encoded payload

139c39e0dc8f8f4eb9b25b20669b4f30ffcbe2197e3a9f69d0043107d06a2cb4 – SiteAdv.pak – Merdoor encoded payload

11bb47cb7e51f5b7c42ce26cbff25c2728fa1163420f308a8b2045103978caf5 – SiteAdv.pak – Merdoor encoded payload

0abc1d12ef612490e37eedb1dd1833450b383349f13ddd3380b45f7aaabc8a75 – SiteAdv.pak – Merdoor encoded payload

eb3b4e82ddfdb118d700a853587c9589c93879f62f576e104a62bdaa5a338d7b – SiteAdv.exe – Legit McAfee executable

1ab4f52ff4e4f3aa992a77d0d36d52e796999d6fc1a109b9ae092a5d7492b7dd – chrome_frame_helper.exe – Legit Google executable

fae713e25b667f1c42ebbea239f7b1e13ba5dc99b225251a82e65608b3710be7 – SmadavProtect64.exe – Legit SmadAV executable

ZXShell Rootkit

SHA256	檔案名稱	描述
1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7	formdll.dll	Kernel driver loader
180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e	form.exe	Kernel driver loadpoint
a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221	update.exe	Kernel driver installation and update utility
592e237925243cf65d30a0c95c91733db593da64c96281b70917a038da9156ae	update.exe	Kernel driver installation and update utility
929b771eabef5aa9e3fba8b6249a8796146a3a4febfd4e992d99327e533f9798	formdll.dll	Kernel driver loader
009d8d1594e9c8bc40a95590287f373776a62dad213963662da8c859a10ef3b4	tdiproip.sys	Kernel driver x64
ef08f376128b7afcd7912f67e2a90513626e2081fe9f93146983eb913c50c3a8	tdiproip.sys	Kernel driver x32
ee486e93f091a7ef98ee7e19562838565f3358caeff8f7d99c29a7e8c0286b28	iehlpsrv.dll	Kernel driver x64 old
32d837a4a32618cc9fc1386f0f74ecf526b16b6d9ab6c5f90fb5158012fe2f8c	USBHPMS.sys	Kernel driver x32 old
d5df686bb202279ab56295252650b2c7c24f350d1a87a8a699f6034a8c0dd849		ZXShell

其他檔案

SHA256	檔案名稱	描述
a1f9b76ddfdafc47d4a63a04313c577c0c2ffc6202083422b52a00803fd8193d	ssmuidll.dll	Possible PlugX DLL loader
3ce38a2fc896b75c2f605c135297c4e0cddc9d93fc5b53fe0b92360781b5b94e	tosbtkbd.dll	Possible ShadowPad loader
210934a2cc59e1f5af39aa5a18aae1d8c5da95d1a8f34c9cfc3ab42ecd37ac92	klcsstd2.dll	Possible ShadowPad loader
530c7d705d426ed61c6be85a3b2b49fd7b839e27f3af60eb16c5616827a2a436	comhlpsvc.dll	Client to interact with driver
5018fe25b7eac7dd7bc30c7747820e3c1649b537f11dbaa9ce6b788b361133bf	comhlpsvc.dll	Client to interact with driver
efa9e9e5da6fba14cb60cba5dbd3f180cb8f2bd153ca78bbacd03c270aefd894	searchsrvc.exe	Client to interact with driver
a5a4dacddfc07ec9051fb7914a19f65c58aad44bbd3740d7b2b995262bd0c09e	comhlpsvc32.dll	Client to interact with driver
10b96290a17511ee7a772fcc254077f62a8045753129d73f0804f3da577d2793	a.exe	LDAP enumerator tool
0dcfcdf92e85191de192b4478aba039cb1e1041b1ae7764555307e257aa566a7	intel.exe	Mimikatz
415f9dc11fe242b7a548be09a51a42a4b5c0f9bc5c32aeffe7a98940b9c7fc04	tfc_windows_amd64.exe	GO Socks5 client
947f7355aa6068ae38df876b2847d99a6ca458d67652e3f1486b6233db336088	deliver.exe	Hacktool - CMD.exe injector
8d77fe4370c864167c1a712d0cc8fe124b10bd9d157ea59db58b42dea5007b63	tool.exe	Hacktool - webshell encoder
d8cc2dc0a96126d71ed1fce73017d5b7c91465ccd4cdcff71712381af788c16d	browser.exe	Infostealer
e94a5bd23da1c6b4b8aec43314d4e5346178abe0584a43fa4a204f4a3f7464b9	python27.dll	Recon DLL
5655a2981fa4821fe09c997c84839c16d582d65243c782f45e14c96a977c594e	frpc.exe	FRPC
19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169	ssf.exe	SSF
41d174514ed71267aaff578340ff83ef00dbb07cb644d2b1302a18aa1ca5d2d0	intel_drive.exe	LSASS dumping tool
67ebc03e4fbf1854a403ea1a3c6d9b19fd9dc2ae24c7048aafbbff76f1bea675	wsc.dll	BlackLoader
f92cac1121271c2e55b34d4e493cb64cdb0d4626ee30dc77016eb7021bf63414	wsc.dll	BlackLoader
859e76b6cda203e84a7b234c5cba169a7a02bf028a5b75e2ca8f1a35c4884065	smbver.exe	SMB enumeration Tool
fcdec9d9b195b8ed827fb46f1530502816fe6a04b1f5e740fda2b126df2d9fd5	smb2os.exe	SMB enumeration Tool
9584df964369c1141f9fc234c64253d8baeb9d7e3739b157db5f3607292787f2	ntmsvc.dll	PrcLoader
711a347708e6d94da01e4ee3b6cdb9bcc96ebd8d95f35a14e1b67def2271b2e9	ntmsvc.dll	PrcLoader
f040a173b954cdeadede3203a2021093b0458ed23727f849fc4c2676c67e25db	ntmsvc.dll	PrcLoader
90edb2c7c3ba86fecc90e80ac339a42bd89fbaa3f07d96d68835725b2e9de3ba	ntmsvc.dll	PrcLoader
b0d25b06e59b4cca93e40992fa0c0f36576364fcf1aca99160fd2a1faa5677a2	lsassunhooker.exe	LsassUnhooker
4c55f48b37f3e4b83b6757109b6ee0a661876b414283452390078829931273 97	ladon.exe	Ladon
3e1c8d982b1257471ab1660b40112adf54f762c570091496b8623b0082840e9f	nbt.exe	NBTScan
9830f6abec64b276c9f327cf7c6817ad474b66ea61e4adcb8f914b324da46627	pot.exe	PortScan
79ae300ac4f1bc7636fe44ce2faa7e5556493f7013fc5c0a3863f28df86a2060	rubes.e	Rubeus

檔案雜湊碼簡要表

13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581
8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead
8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38
89e503c2db245a3db713661d491807aab3d7621c6aff00766bc6add892411ddc
c840e3cae2d280ff0b36eec2bf86ad35051906e484904136f0e478aa423d7744
5f16633dbf4e6ccf0b1d844b8ddfd56258dd6a2d1e4fb4641e2aa508d12a5075
ff4c2a91a97859de316b434c8d0cd5a31acb82be8c62b2df6e78c47f85e57740
14edb3de511a6dc896181d3a1bc87d1b5c443e6aea9eeae70dbca042a426fcf3
db5deded638829654fc1595327400ed2379c4a43e171870cfc0b5f015fad3a03

e244d1ef975fcebb529f0590acf4e7a0a91e7958722a9f2f5c5c05a23dda1d2c
f76e001a7ccf30af0706c9639ad3522fd8344ffbdf324307d8e82c5d52d350f2
dc182a0f39c5bb1c3a7ae259f06f338bb3d51a03e5b42903854cdc51d06fced6
fa5f32457d0ac4ec0a7e69464b57144c257a55e6367ff9410cf7d77ac5b20949
fe7a6954e18feddeeb6fcdaaa8ac9248c8185703c2505d7f249b03d8d8897104
341d8274cc1c53191458c8bbc746f428856295f86a61ab96c56cd97ee8736200
f3478ccd0e417f0dc3ba1d7d448be8725193a1e69f884a36a8c97006bf0aa0f4
750b541a5f43b0332ac32ec04329156157bf920f6a992113a140baab15fa4bd3
9f00cee1360a2035133e5b4568e890642eb556edd7c2e2f5600cf6e0bdcd5774
a9051dc5e6c06a8904bd8c82cdd6e6bd300994544af2eed72fe82df5f3336fc0
d62596889938442c34f9132c9587d1f35329925e011465c48c94aa4657c056c7
f0003e08c34f4f419c3304a2f87f10c514c2ade2c90a830b12fdf31d81b0af57
139c39e0dc8f8f4eb9b25b20669b4f30ffcbe2197e3a9f69d0043107d06a2cb4
11bb47cb7e51f5b7c42ce26cbff25c2728fa1163420f308a8b2045103978caf5
0abc1d12ef612490e37eedb1dd1833450b383349f13ddd3380b45f7aaabc8a75
eb3b4e82ddfdb118d700a853587c9589c93879f62f576e104a62bdaa5a338d7b
1ab4f52ff4e4f3aa992a77d0d36d52e796999d6fc1a109b9ae092a5d7492b7dd
fae713e25b667f1c42ebbea239f7b1e13ba5dc99b225251a82e65608b3710be7
1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7
180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e
a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221
592e237925243cf65d30a0c95c91733db593da64c96281b70917a038da9156ae
929b771eabef5aa9e3fba8b6249a8796146a3a4febfd4e992d99327e533f9798
009d8d1594e9c8bc40a95590287f373776a62dad213963662da8c859a10ef3b4
ef08f376128b7afcd7912f67e2a90513626e2081fe9f93146983eb913c50c3a8
ee486e93f091a7ef98ee7e19562838565f3358caeff8f7d99c29a7e8c0286b28
32d837a4a32618cc9fc1386f0f74ecf526b16b6d9ab6c5f90fb5158012fe2f8c
d5df686bb202279ab56295252650b2c7c24f350d1a87a8a699f6034a8c0dd849
a1f9b76ddfdafc47d4a63a04313c577c0c2ffc6202083422b52a00803fd8193d
3ce38a2fc896b75c2f605c135297c4e0cddc9d93fc5b53fe0b92360781b5b94e
210934a2cc59e1f5af39aa5a18aae1d8c5da95d1a8f34c9cfc3ab42ecd37ac92
530c7d705d426ed61c6be85a3b2b49fd7b839e27f3af60eb16c5616827a2a436
5018fe25b7eac7dd7bc30c7747820e3c1649b537f11dbaa9ce6b788b361133bf
efa9e9e5da6fba14cb60cba5dbd3f180cb8f2bd153ca78bbacd03c270aefd894
a5a4dacddfc07ec9051fb7914a19f65c58aad44bbd3740d7b2b995262bd0c09e
10b96290a17511ee7a772fcc254077f62a8045753129d73f0804f3da577d2793
0dcfcdf92e85191de192b4478aba039cb1e1041b1ae7764555307e257aa566a7
415f9dc11fe242b7a548be09a51a42a4b5c0f9bc5c32aeffe7a98940b9c7fc04
947f7355aa6068ae38df876b2847d99a6ca458d67652e3f1486b6233db336088
8d77fe4370c864167c1a712d0cc8fe124b10bd9d157ea59db58b42dea5007b63

d8cc2dc0a96126d71ed1fce73017d5b7c91465ccd4cdcff71712381af788c16d
e94a5bd23da1c6b4b8aec43314d4e5346178abe0584a43fa4a204f4a3f7464b9
5655a2981fa4821fe09c997c84839c16d582d65243c782f45e14c96a977c594e
19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169
41d174514ed71267aaff578340ff83ef00dbb07cb644d2b1302a18aa1ca5d2d0
67ebc03e4fbf1854a403ea1a3c6d9b19fd9dc2ae24c7048aafbbff76f1bea675
f92cac1121271c2e55b34d4e493cb64cdb0d4626ee30dc77016eb7021bf63414
859e76b6cda203e84a7b234c5cba169a7a02bf028a5b75e2ca8f1a35c4884065
fcdec9d9b195b8ed827fb46f1530502816fe6a04b1f5e740fda2b126df2d9fd5
9584df964369c1141f9fc234c64253d8baeb9d7e3739b157db5f3607292787f2
711a347708e6d94da01e4ee3b6cdb9bcc96ebd8d95f35a14e1b67def2271b2e9
f040a173b954cdeadede3203a2021093b0458ed23727f849fc4c2676c67e25db
90edb2c7c3ba86fecc90e80ac339a42bd89fbaa3f07d96d68835725b2e9de3ba
b0d25b06e59b4cca93e40992fa0c0f36576364fcf1aca99160fd2a1faa5677a2
4c55f48b37f3e4b83b6757109b6ee0a661876b414283452390078829931273973
e1c8d982b1257471ab1660b40112adf54f762c570091496b8623b0082840e9f
9830f6abec64b276c9f327cf7c6817ad474b66ea61e4adcb8f914b324da46627
79ae300ac4f1bc7636fe44ce2faa7e5556493f7013fc5c0a3863f28df86a2060

關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2023/5

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，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、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 很少出現在由公關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，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招的一線廠商，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 年起就全心全力於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，以及基於比原廠更孰悉用戶環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。保安資訊連絡電話：**0800-381-500**。