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

賽門鐵克端點防護技術，有效應對近期遽增的側載攻擊

2024 年 7 月 9 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

側載

Wikipediade 將側載定義為『在兩台本地裝置之間進行檔案傳輸的過程，尤其是指在一台電腦和一台行動裝置，例如：行動電話、智慧型手機、個人數位助理、平板電腦、可攜式媒體播放器或電子閱讀器』。

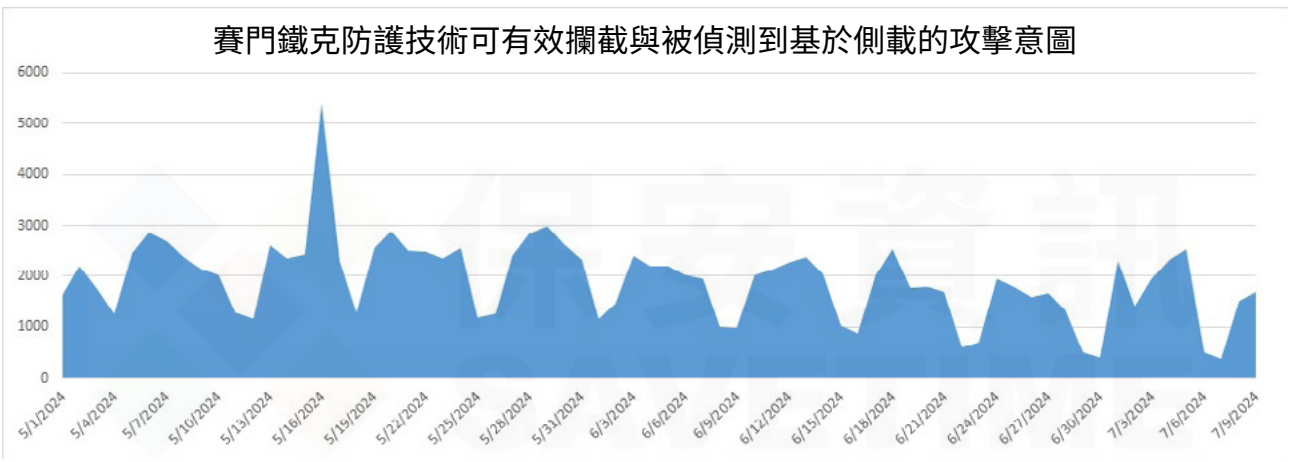
在本公告中，我們將討論與網路安全領域相關的側載問題。MITRE 在 T1574.002 中將側載攻擊定義為一種 (搜尋順序) 劫持執行流程，它利用 Windows 應用程式載入 DLL 的伎倆。攻擊者將惡意 DLL 存放在他們知道作業系統會搜尋的位置，以便將合法檔案載入到記憶體中執行。但是，當與該檔案相關的應用程式運行時，它會載入攻擊者的 DLL，而不是合法的 DLL，進而執行惡意程式碼。由於採用這種技術，如果有人在遭入侵的電腦上尋找惡意程序，很可能找不到。惡意 DLL 會有效地隱藏在合法名稱的檔案程序中，以執行攻擊者的預期的操作。這不僅使惡意程序難以被發現，也讓惡意軟體在系統重啟後依然存在。它也可用來協助權限升級。這種有效的攻擊技術已經使用很長時間，目前仍在使用。

惡意程式載入器和 DLL

下面列出一些試圖使用 DLL 側載技術惡名昭彰的惡意軟體檔名

合法可執行檔	可執行檔發佈者	側載 DLL 檔案
vlc.exe	VideoLAN	libvlc.dll
iTunesHelper.exe	Apple	CoreFoundation.dll
kinit.exe	Oracle Corporation	jli.dll
ccsvchst.exe	Symantec	cci80u.dll
vmtoolsd.exe	VMware, Inc.	glib-2.0.dll
atkexComSvc.exe	ASUSTeK Computer, Inc.	AsIO.dll
notepad++.exe	Don Ho	mimeTools.dll
DTShellHlp.exe	Disc Soft Ltd.	DTCommonRes.dll
KeyScrambler.exe	QFX Software Corporation	KeyScramblerIE.dll

最近的側載攻擊趨勢



請注意，圖表中包括被攔截與被偵測到。已偵測是否會產生如上區塊取決於產品的特定配置／設定，因為它與 Adaptive 和 EDR 等防護技術有關。

我們最近撰寫多份關於利用側載的威脅公告，可參考包括以下內容：

- Trojan.Darkgate，一種同時具有惡意竊密和檔案加密功能的惡意軟體。
  - 每周防護公告第十四頁--2024/05/03 最近傳播 DarkGate 惡意程式的垃圾郵件行動
  - 每周防護公告第四頁--2024/04/29 DarkGate惡意程式載入器仍在大肆傳播
- Trojan.Casbaneiro 一種銀行金融木馬惡意軟體，透過惡意垃圾郵件行動傳播，誘騙使用者點擊 HTML 附件。
  - 每周防護公告第四頁--2024/05/29 Metamorfo 銀行木馬
- Trojan.Wikiloader 一種惡意程式下載器，可將單獨的惡意軟體有效酬載注入到目標電腦上。
  - 原廠防護亮點分享--又見 WikiLoader 惡意程式載入器強勢回歸

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Darkgate
- Trojan.Darkgate!gen7
- Trojan.Casbaneiro!gen1
- Trojan.Wikiloader!gen2
- Trojan.Sysilod!gen1
- Trojan.Sysilod!gen2
- Trojan.Dllhijack!gen2
- Trojan.Dllhijack!gen3
- Trojan.Dllhijack!gen4

基於行為偵測技術(SONAR)的防護：

- SONAR.DllHijack!gen2
- SONAR.DllHijack!gen3
- SONAR.DllHijack!gen4
- SONAR.DllHijack!gen5
- SONAR.SuspLoad!g55
- SONAR.SuspLaunch!g373
- SONAR.SuspLaunch!g374
- SONAR.SuspLaunch!g375
- SONAR.SuspLaunch!g376
- SONAR.SuspLaunch!g377
- SONAR.SuspLaunch!g378
- SONAR.SuspLaunch!g379
- SONAR.SuspLaunch!g380
- SONAR.SuspLaunch!g381
- SONAR.SuspLaunch!g382
- SONAR.SuspLaunch!g383
- SONAR.SuspLaunch!g384
- SONAR.SuspLaunch!g385

自適應防護技術(包含於SESC)：

- ACM.Lsass-LoadDll!g1

基於端點偵測與回應(EDR)：

- IF.HijackExecFlow!g4

欲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。

欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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**。