

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



基於VB6的惡意軟體 威脅在2024年依然活躍

2024年2月27日發布



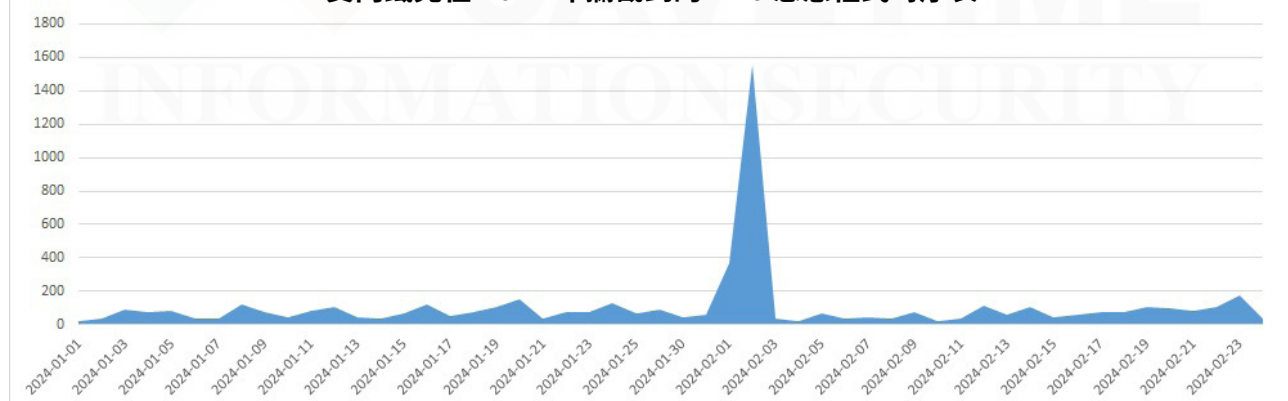
點擊此處可獲取--最完整的賽門鐵克解決方案資訊

根據維基百科，經典的 Visual Basic(通常稱為『VB』)於 1991 年首次發佈，是基於 BASIC 程式設計語言(早在 1963 年就發佈了!) 和微軟 Windows 整合式開發環境 (IDE) 的第三代程式設計語言。其最終版本是 1998 年發佈的第 6 版 (VB6)。2008 年 4 月 8 日，微軟停止對 VB6 IDE 的支援，取而代之是微軟為新的 .NET Framework 設計之 VB.NET，突破傳統模式的許多限制。

儘管已經過 25 年，但由於微軟確保 VB6 應用程式在受支援 Windows 作業系統上的相容性，因此 VB6 可執行檔仍然可以在最新的 Windows 版本上運行。得益於這種相容性，我們仍然可以在工廠、醫院和企業中，還看得到許多採用 VB6 設計的系統還在運作。但另一方面，攻擊者仍然可以利用 VB6 建立新病毒，這可能是希望安全研究人員更難分析和檢測這些使用老式工具製作的可執行檔。

Vilsel 蠕蟲就是這樣一種一段時間就會出風頭的 VB6 惡意軟體。自 2015 年底安全研究人員首次發現以來，Vilsel 已被修改過好多次，2024 年我們仍能在全球範圍內看到它的存在，它是整個 VB 惡意軟體生態系的要角。

賽門鐵克在 2024 年攔截到的 VB6 惡意程式時序表



Vilsel 是在過時的 Visual Basic 編譯器編譯選項中利用 PCode(Pseudo-code) 或偽代碼/虛擬代碼建立。PCode 不是本地 (Native) 的 CPU 程式碼，而是 VB6 特定的中間程式碼，由微軟的相容程式逐步執行。因此，許多常用的現代分析工具都無法分析這些檔案，需要使用 VB 反編譯器或類似工具才能分析它們。Vilsel 某些變種會進一步將 VB6 可執行檔封裝在原生代碼混淆程式中，導致一些不太強大的反 VB6 保護功能失靈。

我們分析的一個 Vilsel 的特定版本是這樣運作：

- 建立一個自身副本，在程式碼末尾新增部份額外位元組
- 將自身複製到現有資料夾，對系統中的所有資料夾重複此動作
- 使用以下檔案名稱：backup.exe、System Restore.exe、update.exe、data.exe

有趣的是，選擇 System Restore.exe、update.exe 和 data.exe 的概率分別為 1/30，因此選擇 backup.exe 的概率為 27/30，即 90%，這意味著該檔最終很可能使用這個名稱，將自己隱藏在名稱相似的合法系統檔中。

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：

- W32.Vilsel!gen1
- W32.Vilsel!gen2

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

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。



保安資訊
KEEPSAFE
INFORMATION SECURITY

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, 以及基於比原廠更熟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。

業界公認 保安資訊--賽門鐵克解決方案專家
We Keep IT Safe, Secure & Save you Time, Cost

服務電話：0800-381500 | +86 4 23815000 | <http://www.savetime.com.tw>