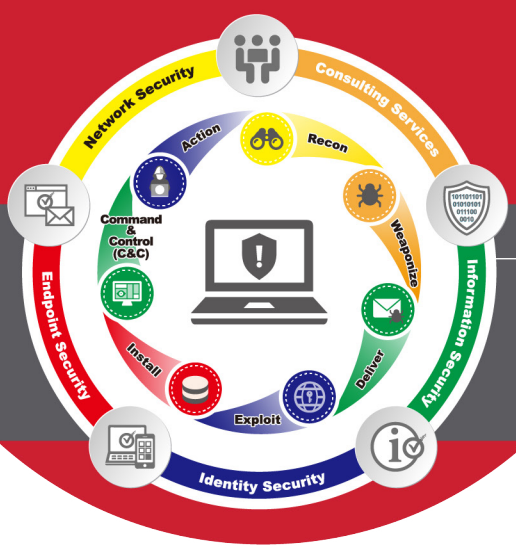

基於VB6的惡意軟體威脅在2024年依然活躍

2024 年 2 月 27 日發布

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。

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。