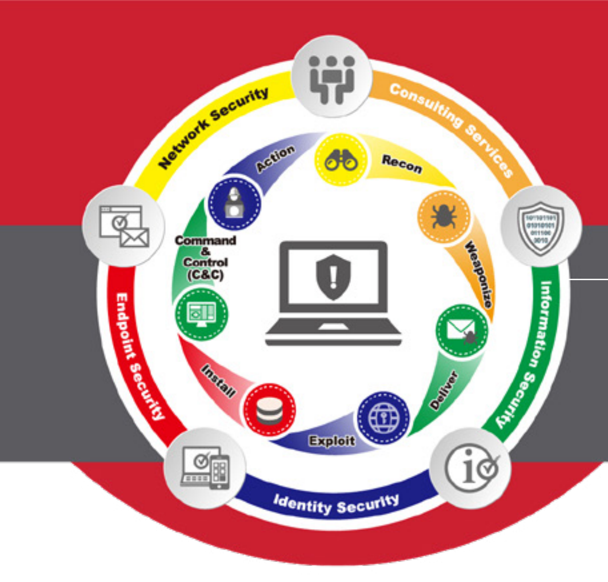


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

賽門鐵克的用戶～免驚！特定資料壓縮軟體的使用者成為駭客利用異常 ZIP 壓縮檔發動攻擊的目標

2024 年 10 月 29 日發布

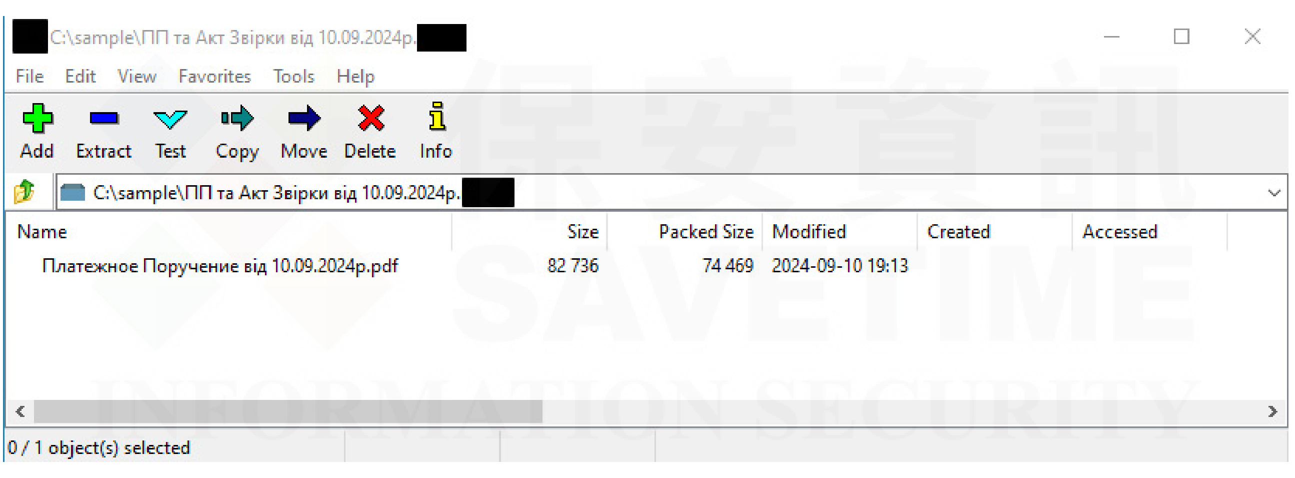
點擊此處可獲取--最完整的賽門鐵克解決方案資訊

ZIP 資料壓縮格式於 1989 年首次推出，是一種廣泛使用於各種作業系統的壓縮檔格式，許多人每天都要使用它。它主要用於將一個或多個檔案合併到單一位置，通常使用壓縮來減少檔案大小。可節省儲存空間，並加快檔案傳輸速度。接收者可以解壓縮 (英文常用 extract 或 unzip) ZIP 檔案，然後以原始格式使用檔案。目前有多種資料壓縮軟體可處理 ZIP 檔案 (例如：RAR/7z)，但它們的行為可能有很大差異，尤其是在處理異常的壓縮檔時。

如果要將兩個或更多 ZIP 壓縮檔合併為單一檔案 (此過程稱為拚接--concatenation)，該如何處理？不同的資料壓縮軟體有不同的回應方式。大多數資料壓縮軟體只能存取第一個壓縮檔中的檔案，或將拚接檔案回報為已損毀。然而，有一個特定的資料壓縮軟體會特別地允許存取拚接序列中最後一個壓縮檔中的檔案。

最近，有人觀察到攻擊者利用這個不一致，針對特定資料壓縮軟體的使用者，使用後門程式：Smokeloader 家族的 JavaScript 惡意程式下載器。他們刻意使用通常與該資料壓縮軟體相關的副檔名來拚接 ZIP 壓縮檔。

攻擊者將兩個 ZIP 檔案連結在一起。第一個壓縮檔包含一個無害的 PDF 檔案，而第二個壓縮檔則包含兩個具有相同有效酬載的 JavaScript 下載程式--兩個程式都是用來下載和執行 Smokeloader 惡意軟體。以下是截圖，顯示各種資料壓縮軟體如何處理此畸形 ZIP 壓縮檔。

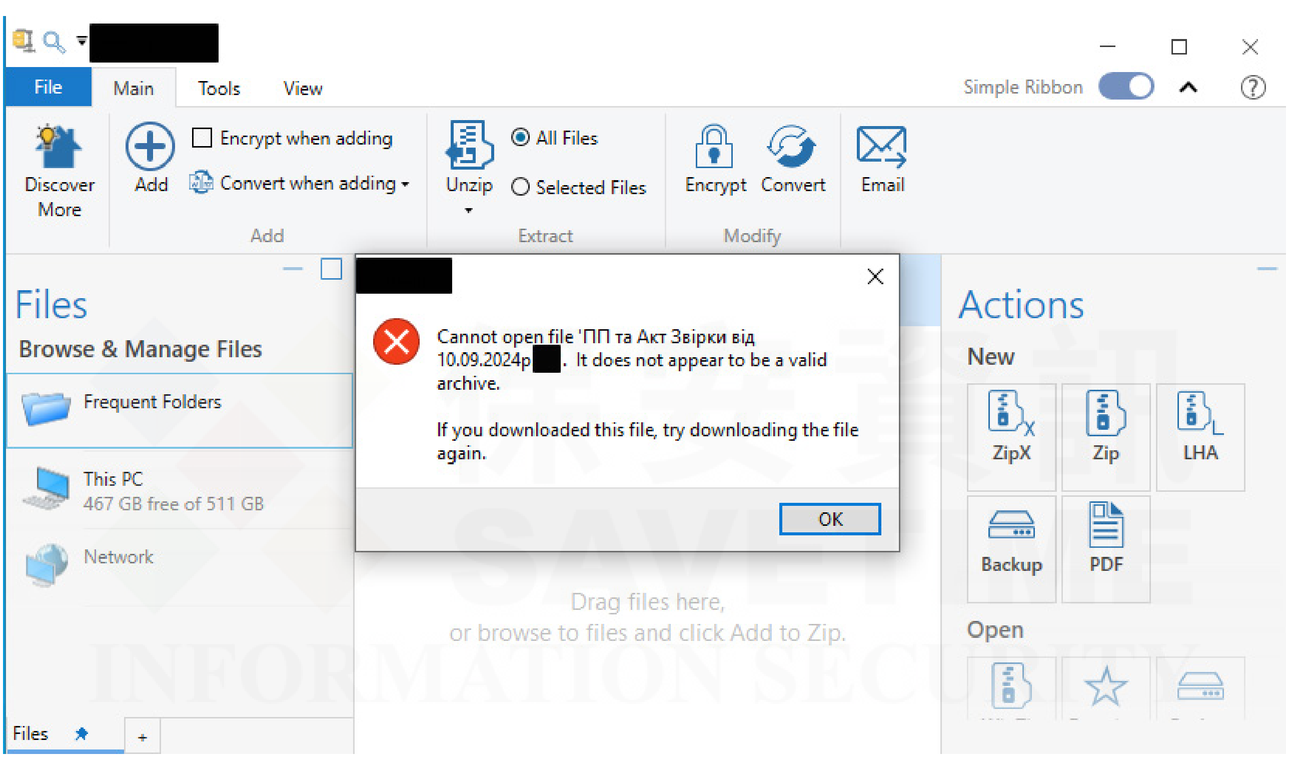

[redacted] C:\sample\ПП та Акт Звірки від 10.09.2024p.[redacted]

C:\sample\ПП та Акт Звірки від 10.09.2024p.[redacted]

Name	Size	Packed Size	Modified	Created	Accessed
Платежное Поручение від 10.09.2024p.pdf	82 736	74 469	2024-09-10 19:13		

0 / 1 object(s) selected

資料壓縮軟體 #1，只能存取第一個壓縮檔中的 PDF 檔案。


[redacted]

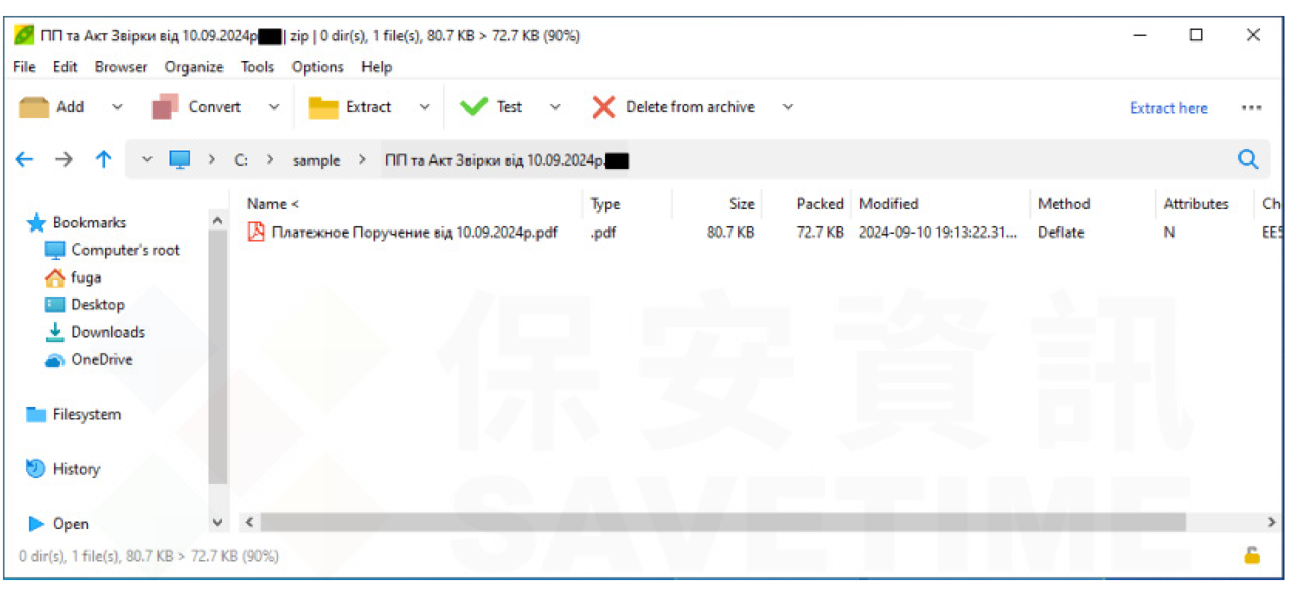
[redacted]

Cannot open file 'ПП та Акт Звірки від 10.09.2024p[redacted]. It does not appear to be a valid archive.

If you downloaded this file, try downloading the file again.

OK

資料壓縮軟體 #2 ，回報拚接的壓縮檔已損毀。

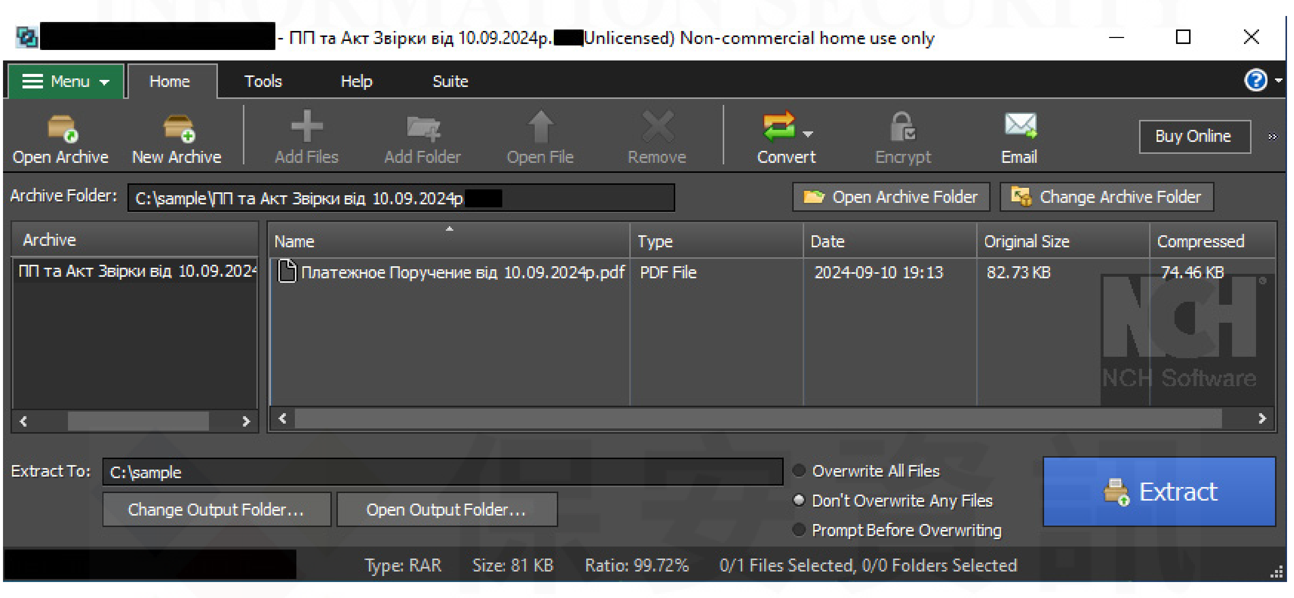

ПП та Акт Звірки від 10.09.2024p[redacted]| zip | 0 dir(s), 1 file(s), 80.7 KB > 72.7 KB (90%)

C: > sample > ПП та Акт Звірки від 10.09.2024p[redacted]

Name	Type	Size	Packed	Modified	Method	Attributes
Платежное Поручение від 10.09.2024p.pdf	.pdf	80.7 KB	72.7 KB	2024-09-10 19:13:22.31...	Deflate	N

0 dir(s), 1 file(s), 80.7 KB > 72.7 KB (90%)

資料壓縮軟體 #3，只能從第一個壓縮檔存取 PDF 檔案。


[redacted] - ПП та Акт Звірки від 10.09.2024p.[redacted]Unlicensed) Non-commercial home use only

Archive Folder: C:\sample\ПП та Акт Звірки від 10.09.2024p[redacted]

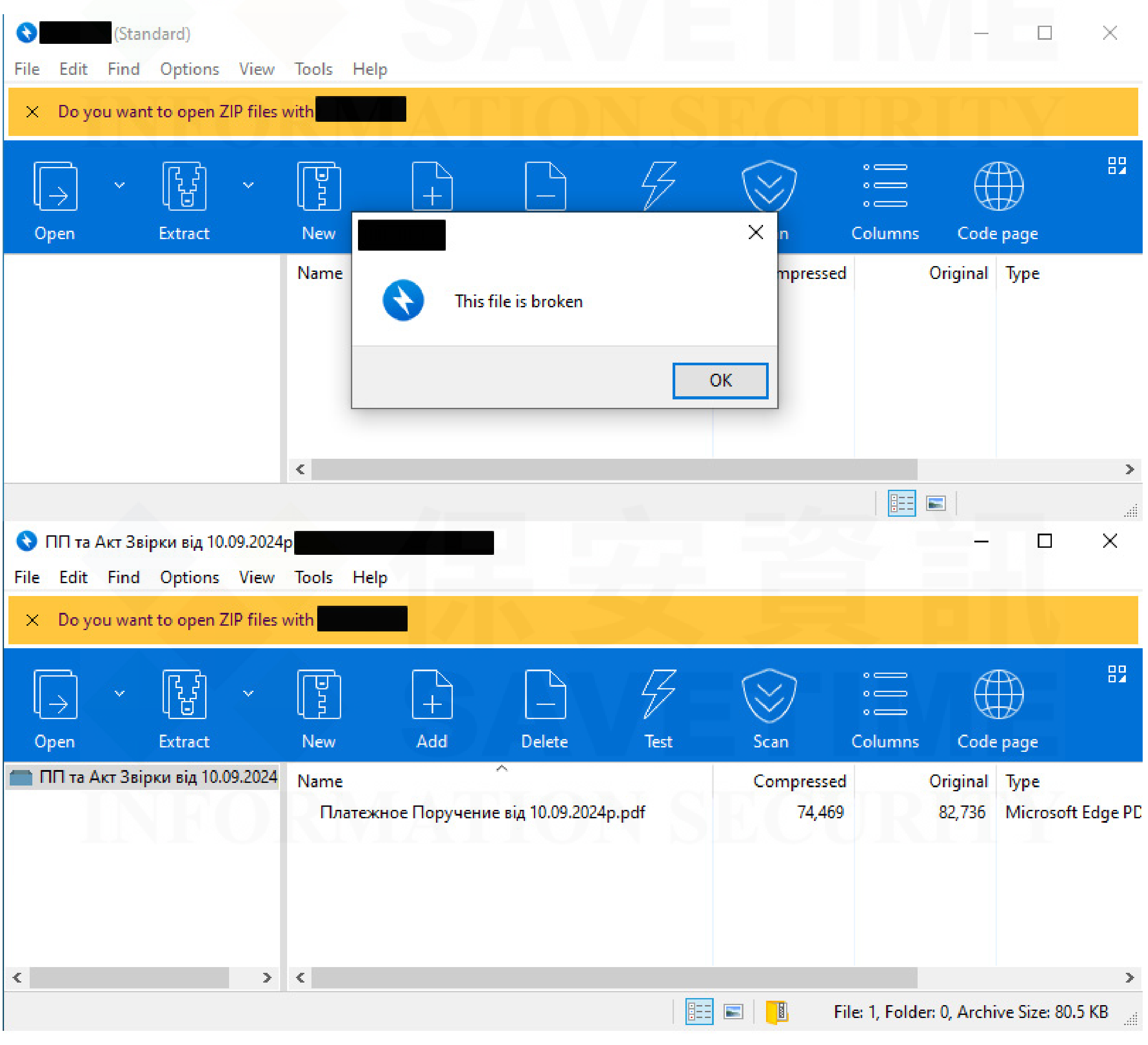
Name	Type	Date	Original Size	Compressed
Платежное Поручение від 10.09.2024p.pdf	PDF File	2024-09-10 19:13	82.73 KB	74.46 KB

Extract To: C:\sample

Don't Overwrite Any Files

[redacted] Type: RAR Size: 81 KB Ratio: 99.72% 0/1 Files Selected, 0/0 Folders Selected

資料壓縮軟體 #4，只能從第一個壓縮檔存取 PDF 檔案。


[redacted](Standard)

Do you want to open ZIP files with [redacted]

[redacted]

This file is broken

OK

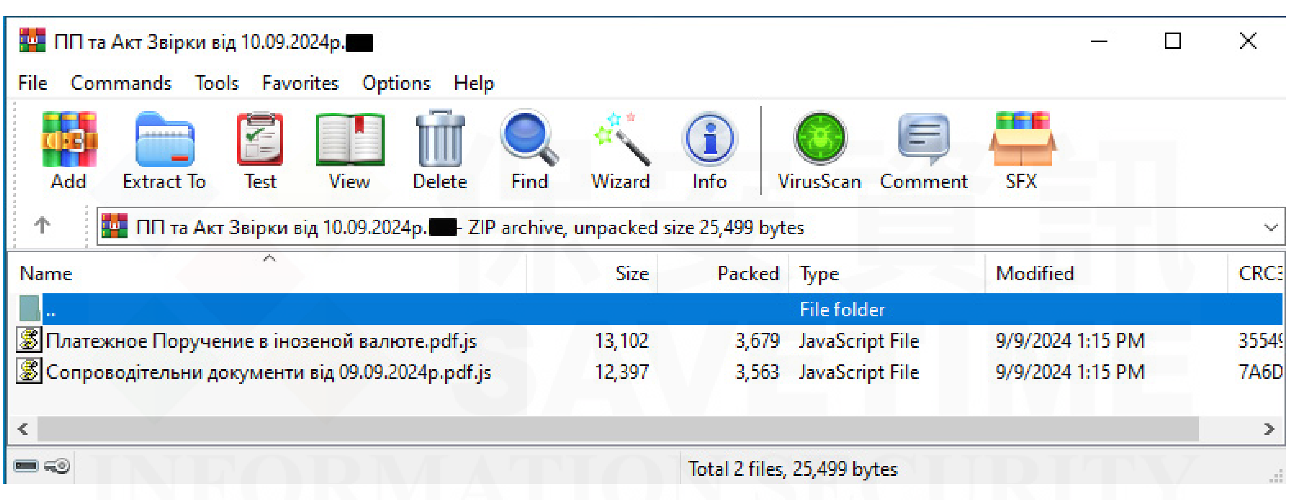
ПП та Акт Звірки від 10.09.2024p[redacted]

Do you want to open ZIP files with [redacted]

Name	Compressed	Original	Type
Платежное Поручение від 10.09.2024p.pdf	74,469	82,736	Microsoft Edge PD

File: 1, Folder: 0, Archive Size: 80.5 KB

資料壓縮軟體 #5 ，回報拚接壓縮檔已損毀，並顯示第一個壓縮檔中的 PDF 檔案。


ПП та Акт Звірки від 10.09.2024p.[redacted]

ПП та Акт Звірки від 10.09.2024p.[redacted]- ZIP archive, unpacked size 25,499 bytes

Name	Size	Packed	Type	Modified	CRC3
..			File folder		
Платежное Поручение в iнозеной валюте.pdf.js	13,102	3,679	JavaScript File	9/9/2024 1:15 PM	3554
Сопроводiтельни документи від 09.09.2024p.pdf.js	12,397	3,563	JavaScript File	9/9/2024 1:15 PM	7A6D

Total 2 files, 25,499 bytes

只有資料壓縮軟體 #6 ，有顯示出第二個壓縮檔中的 JavaScript 檔案。

此伎倆可確保安裝特定資料壓縮軟體的使用者能夠存取第二個壓縮檔中的惡意 JavaScript 檔案。然而，並非所有安全軟體都能有效處理這種畸形的 ZIP 壓縮檔，因此難以擷取和偵測惡意 JavaScript 檔案。這種手法大大增加惡意軟體成功傳送的成功率。

賽門鐵克靜態資料掃描 (Static Data Scanner：SDS) 的進階剖析技術是專為掌管此類異常現象而設計。它可以準確剖析拚接的 ZIP 檔案，確保提取並有效偵測惡意檔案，例如：Smokeloader 攻擊中使用的 JavaScript 惡意程式下載器。

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：

- Scr.Malarchive!gen9
- Scr.Malcode!gen164
- Trojan.Smokeloader!g1

欲深入瞭解更完整的的賽門鐵克端點／重要主機／郵件安全/網頁安全解決方案，請點擊此處。
欲深入瞭解更多關於賽門鐵克先進的防護技術在真實網路情境的優異防護能力，請點擊此處。

關於賽門鐵克 (Symantec)

Symantec
A Division of Broadcom

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
KEEPSAFE
INFORMATION SECURITY

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**。