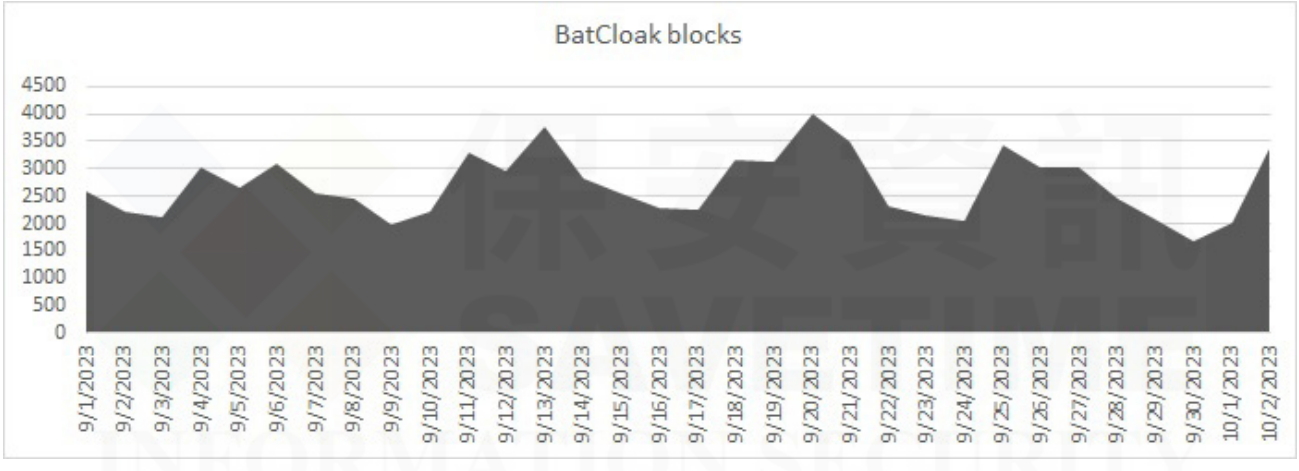
BatCloak 使威脅形勢雪上加霜

2023 年 10 月 3 日發布

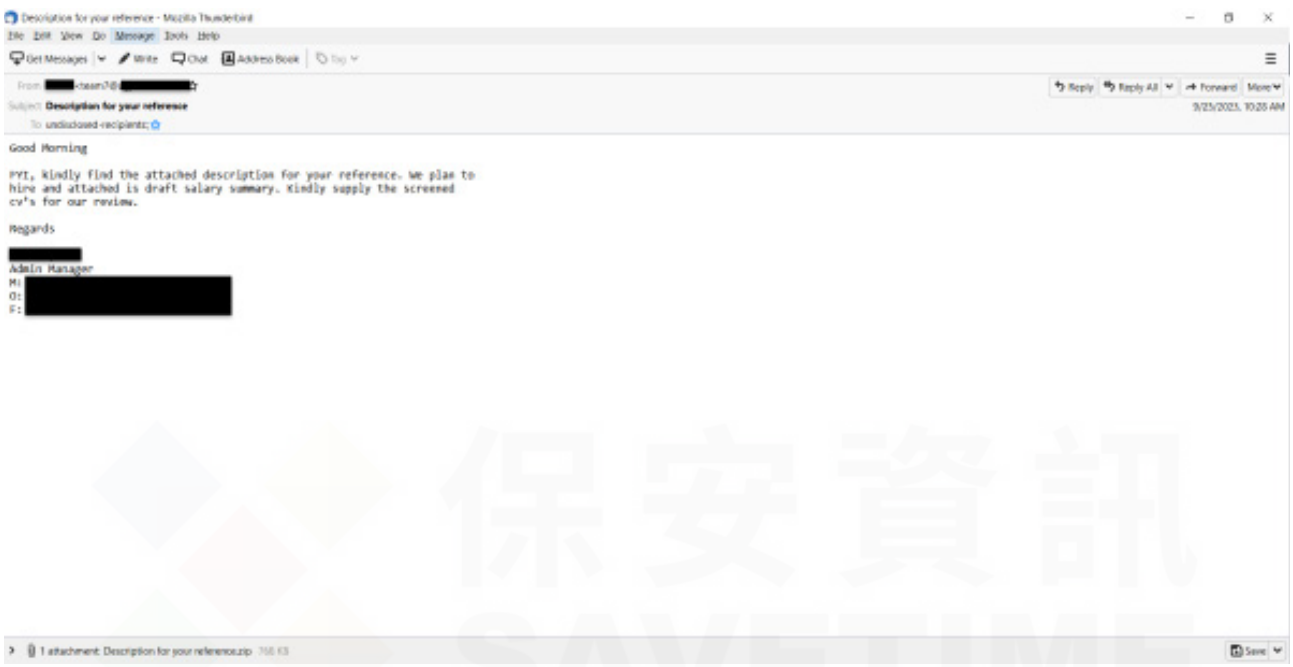
點擊此處可獲取--最完整的賽門鐵克解決方案資訊

.BAT 的批次檔由於其簡單性、也是 Windows 內建的功能、容易隱藏的特性和具有腳本編寫功能…等，長期以來一直被網路上的壞蛋用於各種目的，但主要還是用作惡意程式載入程式。

就在幾個月前，一種被稱為 BatCloak 的批次檔混淆工具引起安全研究人員的關注，多份報告顯示惡意批次載入程式被該工具混淆，並在世界各地的攻擊行動中用於傳遞惡意籌載，例如：資訊竊取程式、遠端存取木馬等。賽門鐵克安全產品截至 9 月記錄的偵測顯示，正在發生相當一致的攻擊浪潮。



賽門鐵克最近觀察到一名冒充印度人力資源公司的參與者，主要向工程、酒店和零售業提供人力資源服務。惡意電子郵件被偽裝成人力招募優惠發送世界各地的公司和政府機構。該附件偽裝成履歷，採用 zip 壓縮檔的形式，其中包含一個 bat 檔案 (參考說明.zip＞參考說明.bat)。



如果毫無戒心的用戶下載該批次檔並執行，他們實際上將執行 Agent Tesla--一個惡名昭彰且非常熱門的竊密程式，我們已多次在此發布。

賽門鐵克的多重防護技術已經於第一時間提供最有效的護**(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：

基於行為偵測技術(SONAR)的防護：

- SONAR.BatCloak!gen1
- SONAR.BatCloak!gen2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.BatCloak
- Trojan.BatCloak!gen1
- Trojan.BatCloak!gen2

欲深入了解更多有關於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。
欲了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，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，以及基於比原廠更孰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**。