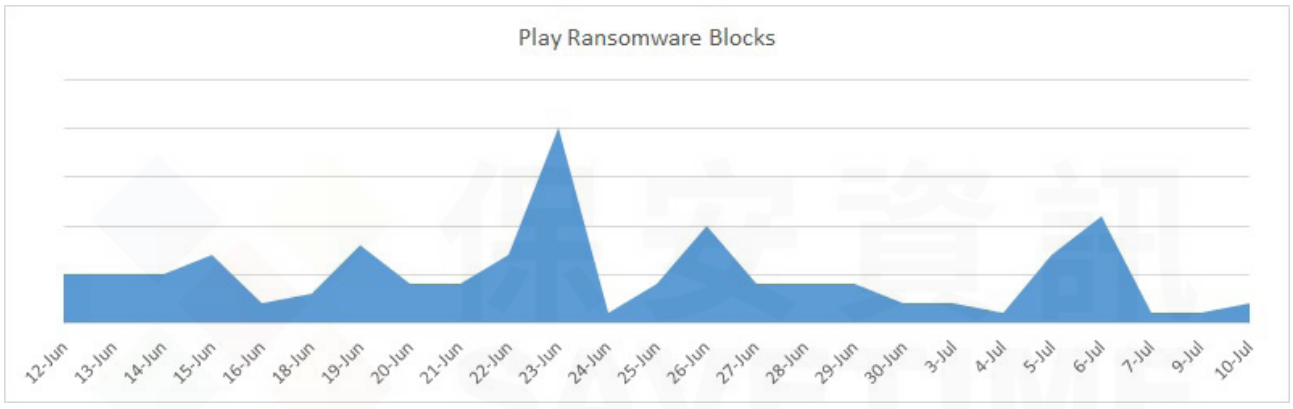
Play 勒索軟體

2023 年 7 月 10 日發布

Play 勒索軟體 (也稱為 PlayCrypt) 於 2022 年中左右首次出現，是當今威脅領域最活躍的勒索軟體之一，與 LockBit、Mallox、Clop 等其他惡名昭彰的勒索軟體家族旗鼓相當。該駭客集團已駭入超過 25 名受害者，目標包括各種規模的不同行業等公共與私人組織。與惡名昭彰的同行一樣，該駭客集團因採用雙重勒索伎倆而聞名，受害者將遭到威迫，如果不支付贖金，他們的資料將被出售。



就感染途徑而言，Play 勒索軟體背後的歹徒一直在開採利用已知的漏洞（ProxyNotShell 就是一個例子），並以從其他專門販售存取權限的駭客集團所購得的登入憑證來進行入侵。攻擊者還使用各種駭客工具（例如：Cobalt Strike、MimiKatz、Empire 和遠端存取木馬 (RAT)）進行橫向移動和常駐。Play 勒索軟體一旦安裝在系統上，就會加密所有檔案並冠上 .PLAY 的副檔名，並建立檔名為『ReadMe.txt』的贖金支付說明。眾所周知，贖金支付說明內容很短，通常只包含『Play』一詞以及歹徒的洋蔥加密網站的鏈接或用於聯繫他們的電子郵件地址。

賽門鐵克針對 Play 勒索軟體，提供完整的零時差保護，具體說明如下：

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomPlay!gen1
- SONAR.RansomPlay!gen2
- SONAR.RansomPlay!gen3

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.PlayCrypt
- Ransom.PlayCrypt!g1
- Ransom.PlayCrypt!g2

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!200

基於安全強化政策(適用於使用DCS)：

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅的零時差攻擊，當然預設強化安全政策就能偵測到以前從未見過的 Play 勒索軟體變種和行為。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

欲深入瞭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。
欲瞭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。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。
欲瞭解更多有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，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**。