賽門鐵克 WebPulse 網頁安全生態系統，每天偵測到由 VipersoftX 觸發的百萬次惡意網址連結，為用戶提供更高層級的保護

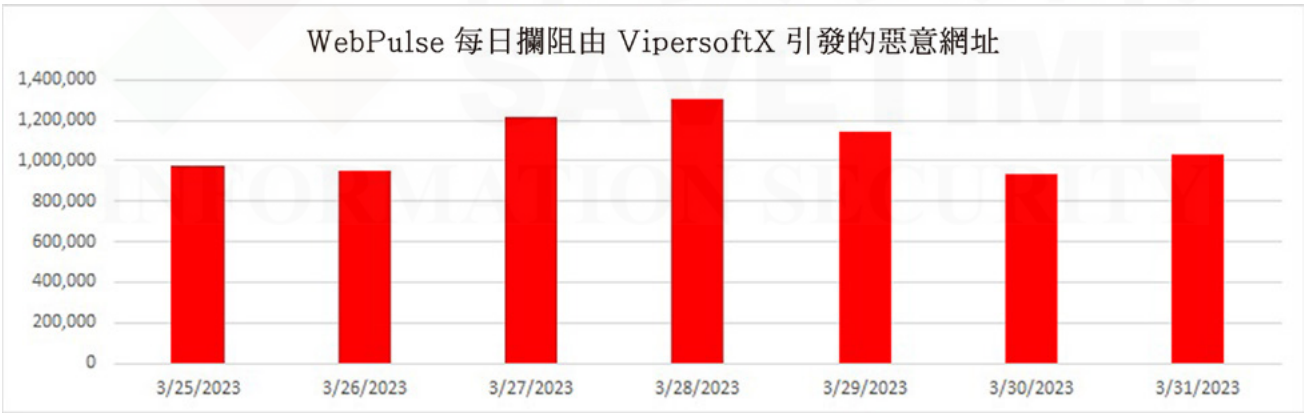
2023 年 4 月 10 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

VipersoftX 是一種相當詭異的竊密惡意軟體，至少從 2019 年底開始就存在。它一種經過高度混淆並定期更新的遠端存取木馬 (RAT)，透過使用破解的軟體經由世界各地的種子 (torrents) 和軟體共享站台進行傳播。最近觀察到它部署為隱藏的小型 PowerShell 腳本在大型系統檔中試圖避免檢測。它主要目標是竊取加密貨幣，採用諸如剪貼簿置換、主機數位指紋識別以及將其他惡意籌載下載到受感染電腦上等技術。

較新版本 ViperSoftX 包含用於安裝瀏覽器擴充元件的有效籌載，該擴充元件有效地為其提供對受害者瀏覽每個頁面的存取權限，使其能夠對瀏覽器發動中間人攻擊來執行加密貨幣錢包地址置換並竊取憑證以及其他剪貼板內容。它透過檢查剪貼簿的內容來竊取加密貨幣，比對是否持有與加密貨幣錢包地址匹配的特徵。如果找到匹配的特徵，它會用自己的錢包地址覆蓋剪貼簿內容。這些方法，簡單但有效。

賽門鐵克 WebPulse 網頁安全生態系統，長期以來一直專注在檢測並阻止來自 VipersoftX 散布惡意瀏覽器擴充元件的大量流量。平均每天有超過一百萬個 URL 請求。



惡意瀏覽器外掛會生成大量 DGA 網域產生演算法生成惡意軟體搭配 C&C 伺服器域名與 IP 位址的虛假網域，這些網域會出現在我們客戶的網頁流量中。在其廣泛的武器庫中，WebPulse 有為數眾多的先進“殭屍網路流量檢測機制”，其中一些會自動觸發此流量。賽門鐵克客戶可以在他們的日誌中使用這些 WebPulse 檢測（被歸類的網頁類別是“惡意離埠數據／殭屍網路”）快速找出他們組織內發送此惡意流量的電腦。

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 **零時差**防護技術偵測到的惡意程式名稱及有效對應的防護機制：

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被歸類的網頁類別：惡意離埠數據／殭屍網路。

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**。