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

面對Snake鍵盤側錄程式，賽門鐵克用戶～高枕無憂

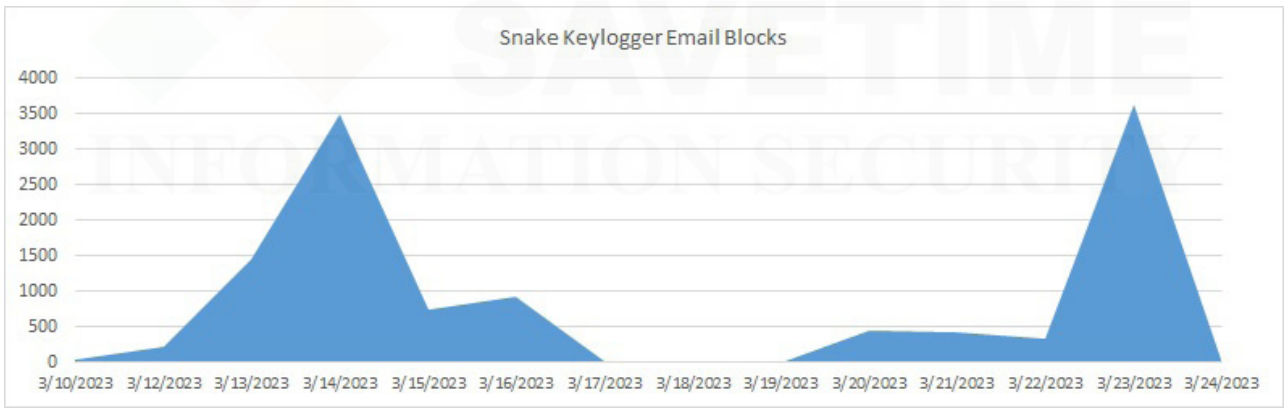
2023 年 3 月 27 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

Snake 鍵盤側錄程式是一種基於 .NET 開發的惡意軟體，已經存在多年，但仍然非常流行。它主要在暗中記錄電腦上的按鍵、螢幕截圖和剪貼簿資料一起傳輸到遠端伺服器，它被世界各地的多個駭客組織和個體戶用於發動各種規模的目標式和隨機式垃圾郵件攻擊行動。

其主要的傳播方法與其他兩個非常熱門的竊密程式：Formbook 和 Agent Tesla 相似，多採用夾帶特定附件的電子郵件，例如：Microsoft Office 或 PDF 類型的檔案。電子郵件顯示常見的社交工程主旨，包括報價單、採購訂單、發票、付款、SWIFT、運輸等關鍵字。附件通常是一個壓縮檔案，在解壓和執行時，可能會採用多種規避伎倆來試圖避免檢測，包括嵌入文件、呼叫或下載遠端漏洞利用工具和加密 shellcode，最終部署該竊密程式的效籌載。

如下圖所示，Snake 鍵盤側錄程式在威脅領域中持續活躍，並且賽門鐵克擁有為數最多的防護科技。我們的首要任務是透過阻止威脅來保護我們的客戶，最好的保護策略是各種不同防護技術都能攔截到各種不同的惡意軟體，而不是特定的技術對應特定的威脅，只能攔截一種特定的攻擊（雖然我們每個防護技術也能做到 --> Trojan.SnakeKeylogger)。



圖表只是賽門鐵克全天候監控的一個時間區間，很清楚顯示攻擊行動明顯增加。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn*
- Scr.Malcode!gen*
- Packed.NsisPacker!g*
- Msil.Packed.*
- Bloodhound.RTF.*
- WS.Malware.*
- WS.SecurityRisk.*
- Trojan.Gen.*
- Trojan Horse
- Trojan.SnakeKeylogger

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

基於機器學習的防禦技術：

- Heur.AdvML.*

*這表示存在多個類似名稱的檢測，例如：Scr.Malcode!gen25、Scr.Malcode!gen34等

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。

欲深入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。

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。

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**。