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

Chaos勒索軟體持續肆虐全球造成錯亂

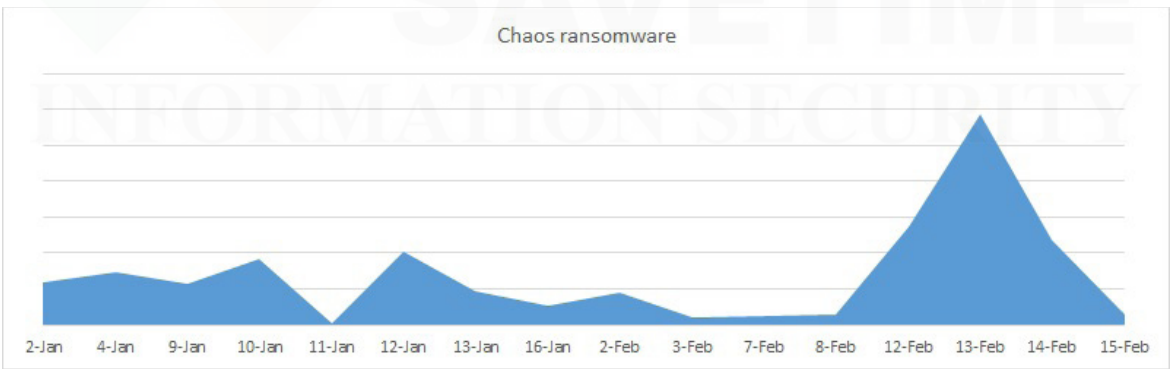
2023 年 2 月 20 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

在過去一年左右的時間裡，我們已經發布十幾個直接或間接與 Chaos 勒索軟體相關的公告，顯示它在威脅領域的普遍性。Chaos 勒索軟體於 2019 年首次出現，對全球企業和個人發起多次攻擊。現在有如此多的變種，惡意軟體以各種不同的方式傳播，但通常仍透過網路釣魚電子郵件或惡意網站傳播，目的是利用老舊軟體中的漏洞來獲得對受害者系統的存取權限。安裝後，Chaos 會加密受害者的檔案並顯示勒索資訊，要求支付贖金以換取解密密鑰。

Chaos 勒索軟體在威脅領域存在如此多變種的原因之一是該惡意軟體的原始碼於 2020 年在網路上被公開洩露。這使得網路犯罪分子更容易建立新的勒索軟體變種，根據自己的攻擊需求對其進行客製化。全球多個駭客組織和個體戶目前都在使用 Chaos 勒索軟體，針對不同規模和行業的消費者和組織，感染單獨一台或大量的電腦。

Chaos 變種激增的另一個原因是，勒索軟體的攻擊行動通常是一項有利可圖的業務。勒索軟體攻擊可以產生可觀的利潤，特別是如果受害者是一個願意支付大筆贖金以恢復其資料的大型組織。之前 Chaos 攻擊的成功可能鼓勵其他威脅攻擊者建立他們自己的勒索軟體版本。也因此更該應採用用信譽良好的安全解決方案來保護您的網路，該解決方案必須具有多層級的保護機制，並能優化其配置以確保您的安全狀況堅如磐石。



由於有新變種出現的緣故，2月12~14日這三天有一波很明顯的攻擊增加。

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 Royal 勒索軟體變種和行為，如下所示：

基於行為偵測技術(SONAR)的防護：

- SONAR.*

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：SONAR.Heur.Dropper、SONAR.Psdownloader!g1；Heur.AdvML.B、Heur.AdvML.C 等

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。
欲深入了解賽門鐵克行為安全技術如何提供針對零時差攻擊的保護，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**。