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

Hunters International (*獵人國際)勒索軟體

2024 年 1 月 9 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

在過去幾個月裡，我們持續觀察到一些新的勒索軟體，駭客集團以世界各國各種規模的企業為目標。其中包括 Hunters International、Meow、DragonForce、Werewolves、Malekteam……等駭客集團。賽門鐵克不間斷監控這些攻擊者，無論他們是透過資料滲漏或檔案加密進行單一勒索手法，還是同時採用資料滲漏和檔案加密的雙重勒索伎倆。

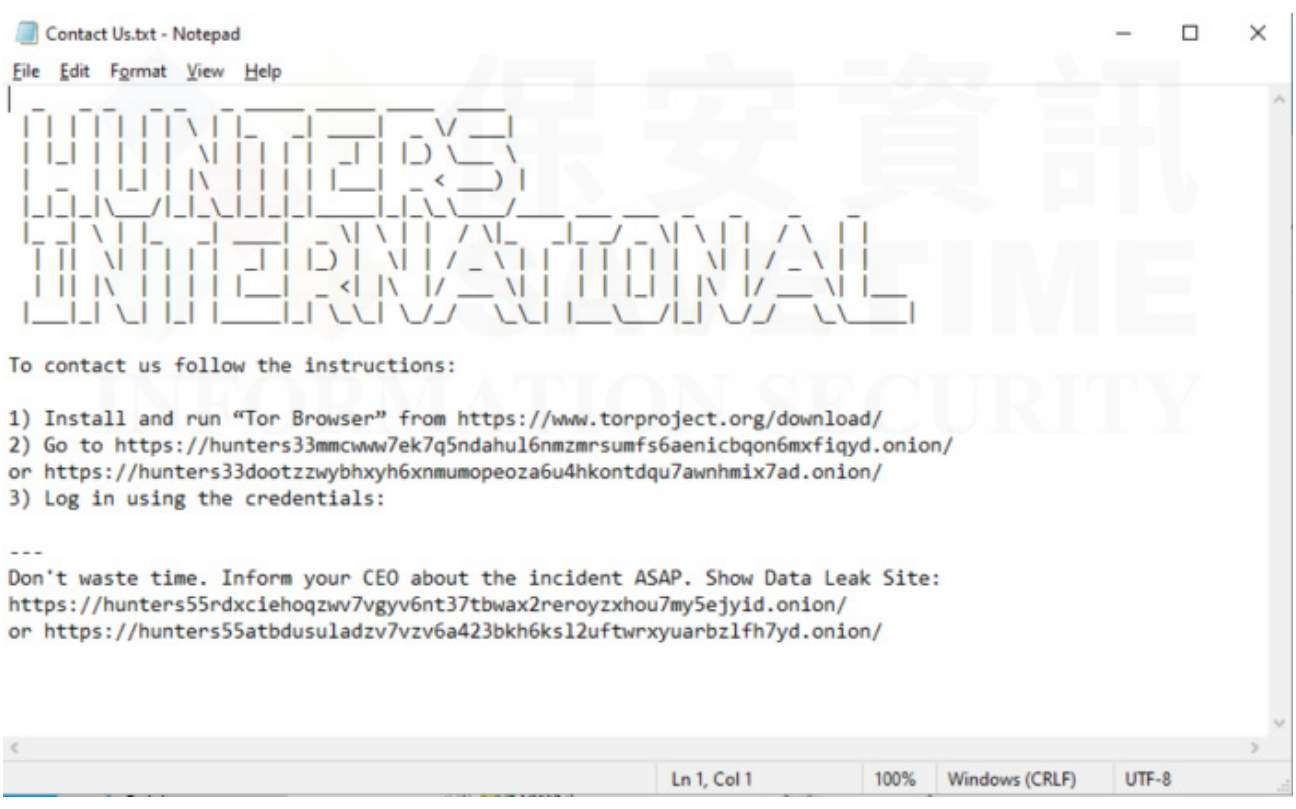
在本篇防護亮點中，我們將介紹 Hunters International 駭客集團，該勒索軟體駭客集團在 2023 年底宣稱有多名受害者上了新聞，進入 2024 年後又聲稱有更多受害者。該駭客集團使用的勒索軟體似乎與惡名昭章的 Hive 勒索軟體之程式碼有密切相關，2023 年初美國 FBI 已瓦解 Hive 勒索軟體犯罪網路。

截至目前，Hunters International 駭客集團的全部策略、技術和程序 (Tactics, Techniques, and Procedures，TTPs) 仍未完成分析。不過，已知他們會在受害者的基礎架構內橫向移動，一旦發現他們認為有價值的目標，就會洩漏出敏感性資料並加密檔案--這是大多數雙重勒索贖的經典作案手法。

與之前的樣本類似，如果勒索軟體二進位檔案 (1 月份收集) 在遭入侵的機器上成功觸發，它將試圖停掉進程和服務。接下來，它會執行刪除備份和禁用回復機制的命令。然後，它會搜尋本機和對應磁碟機，以及透過 NetServerEnum 和 NetShareEnum API 在區域網路上發現的共用磁碟，並對發現的檔案進行加密。它會在每個加密檔案上冠上 .lock 附檔名，並在同一目錄下存放名為『Contact Us.txt』的勒索 (熟金支付) 說明。雖然目標是檔案加密，但它會跳過以下內容來加快重要檔案的加密速度：

- 包含以下字串名稱資夾內的檔案：$Recycle bin、$windows.~bt、$windows.~ws、all users、appdata、boot、config.msi、default、google、intel、mozilla、msocache、perflogs、system volume information、tor browser、internet explorer、windows、windows.old、windows nt
- 檔名為：autorun.inf、bootfont.bin、boot.ini、bootsect.bak、desktop.ini、iconcache.db、ntldr、ntuser.dat、ntuser.dat.log、ntuser.ini.log、thumbs.db 的檔案
- 具有以下副檔名的檔案：386、adv、ani、bat、bin、cab、cmd、com、cpl、cur、deskthemepack、diagcab、diagcfg、diagpkg、dll、drv、exe、hlp、hta、icl、icns、ico、ics、idx、key、ldf、lnk、lock、mod、mpa、msc、msi、msp、msstyles、msu、nls、nomedia、ocx、pdb、prf、ps1、rom、rtp、scr、shs、spl、sys、theme、themepack、wpx

以下為受害者機器上留下的勒索(贖金支付)說明檔案內容截圖。



如上所述，賽門鐵克透過監控新的勒索／洩密網站以及來自外部和內部的其他資料，不斷追蹤新的勒索軟體攻擊者。雖然所使用的惡意軟體和工具並非現成或容易找到，但我們會繼續積極尋找樣本並識別所有 TTPs。這是一場持續的『貓捉老鼠』遊戲，保持資訊暢通和獲取入侵指標 (IOC) 是有效檢測和緩解威脅的關鍵要素。

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 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：

- Ransom.Hunters!g1
- Trojan.Gen.MBT
- Trojan Horse

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g195
- SONAR.SuspLaunch!g253
- SONAR.RansomPlay!gen1
- SONAR.RansomGen!gen3
- SONAR.SuspLaunch!g193

基於機器學習的防禦技術：

- Heur.AdvML.B!100

基於安全強化政策(適用於使用DCS)：

Symantec DCS Hardening policy for Windows 可提供針對 Hunter's Hive 勒索軟體的 0-day 防護。預設沙箱可控制防止安裝 webhell 和惡意軟體工具，並防止特權應用程式執行任意系統命令。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Ransomwares/HunterInternational/

欲深入瞭解有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。
欲深入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。
欲深入瞭解賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。
欲深入瞭解賽門鐵克端點偵測與回應 (EDR) 的更多資訊，請點擊此處。

** 賽門鐵克端點偵測和回應（EDR）使用機器學習和行為分析來檢測和揭露可疑的網路活動。EDR 會對潛在的有害活動發出警告，對事件進行優先級別排序以便快速分類，並允許事件回應人員瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。

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**。