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

Nokoyawa勒索軟體

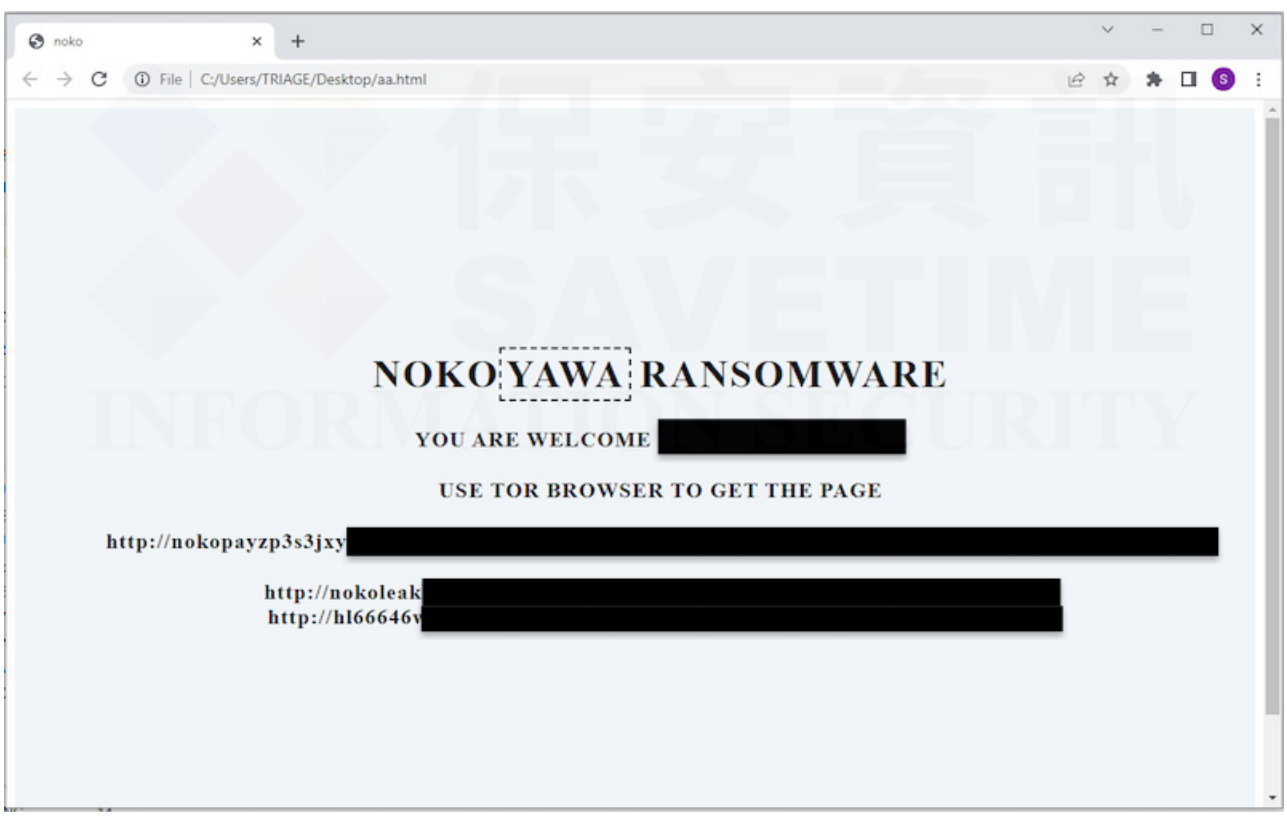
2023 年 8 月 1 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

Nokoyawa 勒索軟體自 2022 年初以來就非常活躍，並因開採利用存在於 Windows 系統的 Common Log File System（CLFS）服務的漏洞 CVE-2023-28252 而引起關注。隨著時間的推移，Nokoyawa 的作者對勒索軟體進行大改版，將其轉換為 Rust 語言。

與其他讓人聞風喪膽的勒索軟體攻擊者一樣，作者在他們的攻擊鏈中採用一系列策略、技術和程序 (TTPs)。2022 年底，發現他們利用 IcedID 的受害者來獲得初始存取權限。

成功入侵後，被加密檔案將被冠上 .NOKONOKO 副檔名，並在電腦上存放勒索贖金支付說明檔（最新版本中為 NOKONOKO-readme.txt 或 NOKONOKO-readme.html）。下面是一個例子：



Nokoyawa 勒索軟體的主要目標是企業和組織，特別是醫療保健、金融服務、政府和製造業等行業。鎖定這些機構通常是因為它們擁有敏感資料、關鍵作業以及可能支付大量贖金的意願。報告顯示，贖金通常平均價值約為 20 萬美元的比特幣。

在Nokoyawa攻擊鏈中所採用的 TTPs 依MITRE 所分類的包括以下內容：

- Command and Scripting Interpreter: Windows Command Shell [T1059.003]
- Windows Management Instrumentation [T1047]
- Data Encrypted for Impact [T1486]
- Impair Defenses: Disable or Modify Tools Defacement [T1491]
- Defacement [T1491]

賽門鐵克提供的單一解決方案內建多層級防護技術，個別技術多能在第一時間就具備**零時差**防護的能力並有明確的定義，僅就不同防護技術說明如下：

基於行為偵測技術(SONAR)的防護：

- SONAR.WMIC!gen12
- SONAR.RansomPlay!gen1
- SONAR.Ransom!gen35
- SONAR.Ransomware!g13
- MEMSCAN.Ransom!gen1
- MEMSCAN.Ransom!gen8
- SONAR.SuspLaunch!g258
- ACM.Wmip-Ps!g1
- MEMSCAN.Ransom!gen2
- SONAR.Ransom!gen98
- SONAR.RansomGen!gen3
- SONAR.RansomNoko!g3

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訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Ransomwares/Nokoyawa.

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Nokoyawa

基於機器學習的防禦技術：

- Heur.AdvML.B

基於安全強化政策(適用於使用DCS)：

賽門鐵克重要主機防護系統：DCS～Data Center Security 內建的預設強化政策，即能提供針對未知威脅的零時差防護，包括以前未見過的勒索軟體變種和相關行為。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。

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**。