勒索軟體攻擊者可能利用權限提升漏洞作為零時差漏洞

2024 年 6 月 12 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

某些證據顯示，與 Black Basta 有關的攻擊者在修補之前就編譯 CVE-2024-26169 漏洞

經營 Black Basta 勒索軟體的 Cardinal 網路犯罪組織 (又稱 Storm-1811、UNC4393) 可能一直在利用最近修補的 Windows 權限提升漏洞作為零時差漏洞。

此漏洞 (CVE-2024-26169) 發生在 Windows 錯誤報告服務。如果在受影響的系統上利用，它可以讓攻擊者提升其權限。該漏洞已於 2024 年 3 月 12 日修復，當時微軟表示沒有證據顯示漏洞已被利用。然而，對最近攻擊中被植入的漏洞利用工具分析顯示，有證據顯示該漏洞可能在修補之前就已被編譯，這意味著至少有一個組織可能已將該漏洞作為零時差漏洞進行利用。

與 Black Basta 的連結

賽門鐵克威脅獵人團隊最近調查的一次勒索軟體攻擊嘗試中發現該漏洞利用工具。儘管攻擊者在這次攻擊中沒有成功部署勒索軟體有效負載，但所使用的策略、技術和程序 (TTP) 與 Microsoft 最近詳細介紹 Black Basta 活動報告中描述的內容非常相似。其中包括使用偽裝成軟體更新的批次腳本。

儘管沒有部署有效負載，但 TTP 的相似性，使得這很可能是一次失敗的 Black Basta 攻擊。

漏洞利用工具

對漏洞利用工具的分析顯示，它利用 Windows 檔案 werkernel.sys 在建立註冊表項目時使用 null 安全描述。由於父項目具有子項目的「建立者擁有者」存取控制項目 (ACE)，因此所有子項目都將由目前程序的使用者擁有。此漏洞利用此點建立「HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WerFault.exe」登錄項，並將「Debugger」值設定為其自己的可執行路徑名稱。此方式則可利用管理權限啟動 shell。

此攻擊中使用的工具變種 (SHA256: 4aae231fb5357c0647483181aeae47956ac66e42b6b134f5b90da76d8ec0ac63) 的編譯時間戳記為 2024 年 2 月 27 日，即修復前幾週。

Virus Total 上發現的該工具的第二個變種 (SHA256: b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0) 的編譯時間較早，時間為 2023 年 12 月 18 日。

可攜式執行檔中的時間戳記值是可修改，這表示時間戳記並不是攻擊者將該漏洞用作零時差漏洞的關鍵證據。然而在這情況下，攻擊者似乎沒有什麼動機將時間戳更改為更早的日期。

威脅再次出現

Cardinal 於 2022 年 4 月推出 Black Basta，從一開始，該勒索軟體就與 Qakbot 殭屍網路密切關聯，Qakbot 殭屍網路似乎是其主要感染媒介。

Qakbot 是世界上最多產的惡意軟體傳播殭屍網路之一，直到 2023 年 8 月執法行動後將其關閉。然而，雖然此次攻擊導致 Black Basta 活動有所下降，但 Cardinal 此後恢復攻擊，且現在似乎已轉向與 DarkGate 加載程序的操作員合作，以接觸潛在的受害者。

防護方案／緩解措施

有關 Alpha 最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

4aae231fb5357c0647483181aeae47956ac66e42b6b134f5b90da76d8ec0ac63 – 漏洞利用工具

b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0 – 漏洞利用工具

a31e075bd5a2652917f91714fea4d272816c028d7734b36c84899cd583181b3d – 批次腳本

3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d – 批次腳本

2408be22f6184cdccec7a34e2e79711ff4957e42f1ed7b7ad63f914d37dba625 – 批次腳本

b0903921e666ca3ffd45100a38c11d7e5c53ab38646715eafc6d1851ad41b92e – 螢幕連接

關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
(好記：幫您節省時間.的公司.在台灣)

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**。