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

好工具總會淪為壞凶器～AutoIt如何遭惡意軟體濫用來發動網路攻擊自動化

2025 年 3 月 4 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

AutoIt 是一種用於 Windows 圖形使用者介面和系統任務的自動化多功能腳本語言，在網路安全方面已成為一把雙面刃。雖然它為系統管理員和開發人員提供簡單和靈活的應用，但其功能已遭惡意使用者濫用來製造精密的惡意軟體，足以迴避傳統的安全機制。

AutoIt常遭濫用於惡意軟體攻擊行動

最近攻擊鏈揭露幾個惡名昭彰的惡意軟體家族已將 AutoIt 納入其作業中，包括但不限於：

- Formbook
- DarkGate
- Agent Tesla
- VipKeylogger
- MassLogger
- DarkCloud
- RedLine Stealer

這些威脅濫用 AutoIt 的腳本功能來混淆惡意程式碼，使偵測和分析變得更具挑戰性。

AutoIt作為惡意軟體載入程式

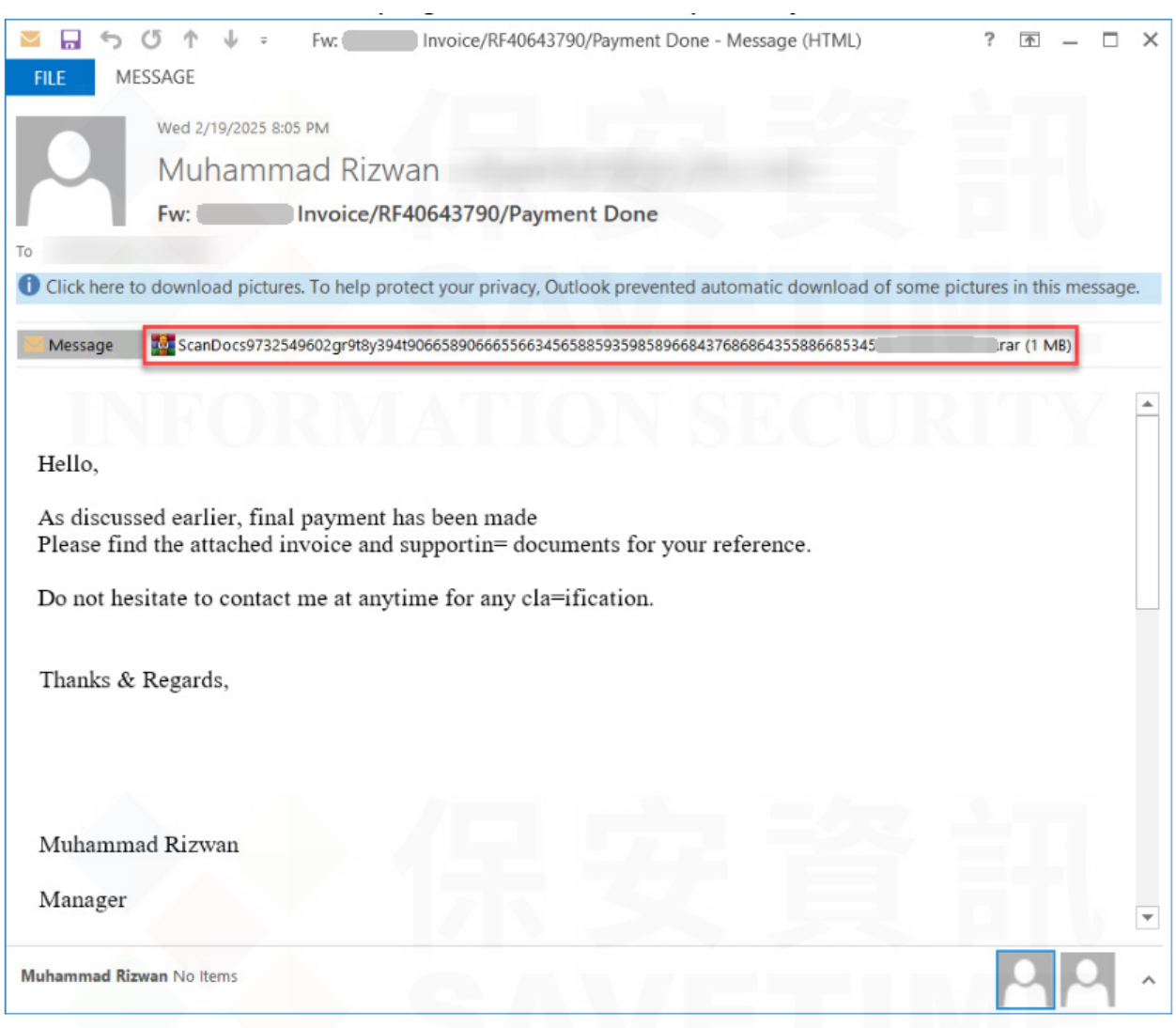
在 AutoIt 涉入的惡意軟體攻擊行動中，常見手法是使用 AutoIt 作為次要有效酬載的載入程式。攻擊者會在 AutoIt 腳本中嵌入加密 shellcode 和最終有效酬載，這些腳本可以是嵌入式字串，也可以從外部檔案載入。

以AutoIt運作載入程式的執行流程

1. 注入有效酬載：執行時，AutoIt 腳本會先將加密的有效酬載注入到系統之 TEMP 資料夾。
2. 執行 shellcode：然後腳本會解密 shellcode 並利用 Windows API 功能傳輸執行，如 ：
   - EnumWindows
   - CallWindowProcA
   - 透過 DllCallAddress 直接濫用 AutoIt API
3. 有效酬載解密與注入：shellcode 會讀取經加密的有效酬載檔案，並將其解密，然後將惡意程式碼注入 suspended 以及 hollowed processes，有效地繞過傳統檔案特徵的偵測機制。

透過利用 AutoIt 腳本的彈性和直接 API 呼叫，這些惡意軟體家族可以避開傳統的安全機制，同時在遭感染的系統中取得常駐／持久性。

DarkCloud 涉入之攻擊行動是濫用包含 AutoIt 可執行「載入程式」的電子郵件傳播



為了對抗這些不斷演進的威脅，我們開發了一系列偵測，專門針對 AutoIt 的惡意使用：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Malautoit!g2
- Trojan.Malautoit!g3
- Trojan.Malautoit!g4
- Trojan.Malautoit!g5
- Trojan.Malautoit!g6
- Trojan.Malautoit!g7

基於行為偵測技術(SONAR)的防護：

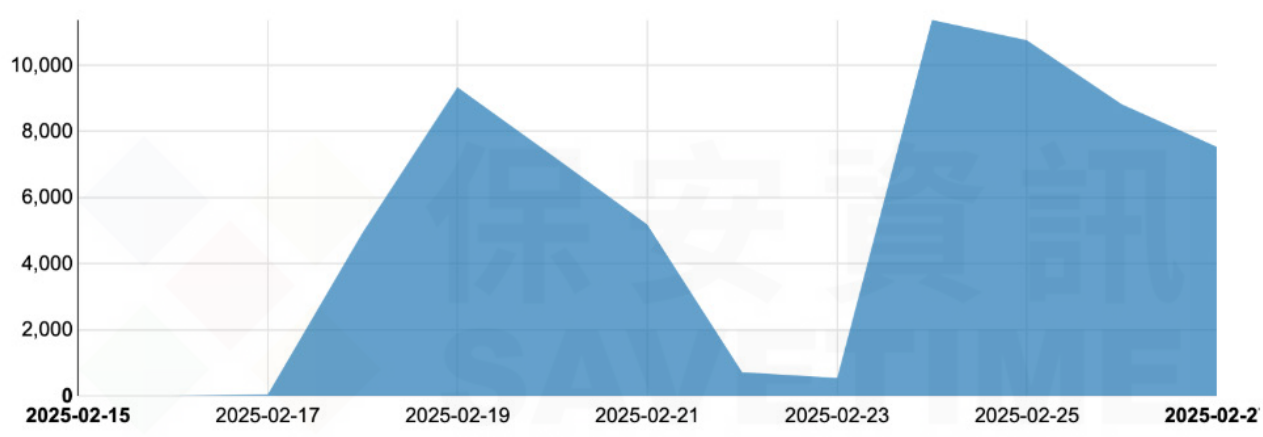
- SONAR.SuspLaunch!g529
- SONAR.SuspLaunch!g532

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- [33074] System Infected: Agent Tesla Infostealer Activity
- [33302] System Infected: Trojan Remcos Activity
- [33407] System Infected: Trojan.Formbook Activity 5
- [33471] System Infected: Redline Stealer Activity 2
- [34948] System Infected: Agent Tesla Infostealer Activity 2
- [34260] System Infected: Trojan.Backdoor Activity 757

最近的偵測到的濫用AutoIt 的惡意威脅數量



這些偵測主要在識別並攔截惡意 AutoIt 指令碼，針對利用此指令碼語言的威脅提供強大之防護。透過持續更新偵測功能和監控新出現的攻擊模式，我們可確保客戶免受濫用 AutoIt 的最新惡意軟體變種的攻擊。

儘管 AutoIt 對於合法的自動化任務而言仍是非常有價值的工具，但意識到其可能被濫用是非常重要的。佈署進階的安全措施並持續了解不斷演進的威脅，是保護系統免於惡意軟體濫用 AutoIt 功能的必要步驟。

欲深入了解更多有關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。

欲了解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。

欲了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。

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 年起就全心全力專注在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，以及基於比原廠更熟悉用戶使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。