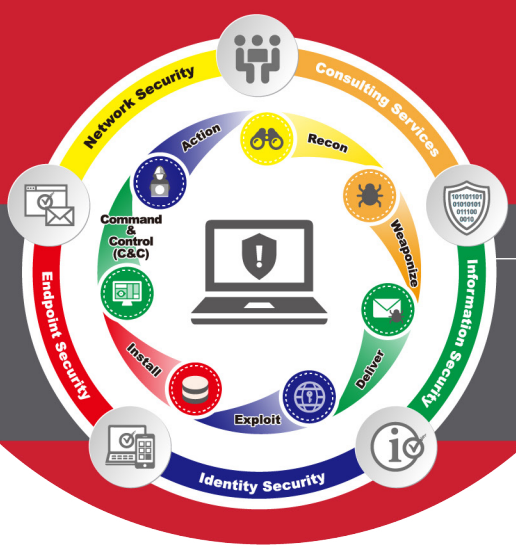


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

賽門鐵克的行為分析技術(SONAR)徹底拆解BatCloak混淆技術！

2024 年 9 月 17 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

批次檔淪為混淆化惡意程式的自動化載入工具

批次檔 (通常簡稱為 “.BAT” 檔) 是一種簡單的純文字檔，它包含一系列命令，用於在 Windows 作業系統上按順序來自動執行程式和應用程式，而無須逐一手動操作。它們已經存在很長時間，與許多其他常見作業系統工具一樣，也可以用於惡意目的。有越來越多的 BAT 檔被濫用於載入攻擊鏈不同階段的惡意程式。

BatCloak 惡意軟體混淆引擎，以高明手法掩護惡意軟體躲避安全軟體的偵測(FUD)

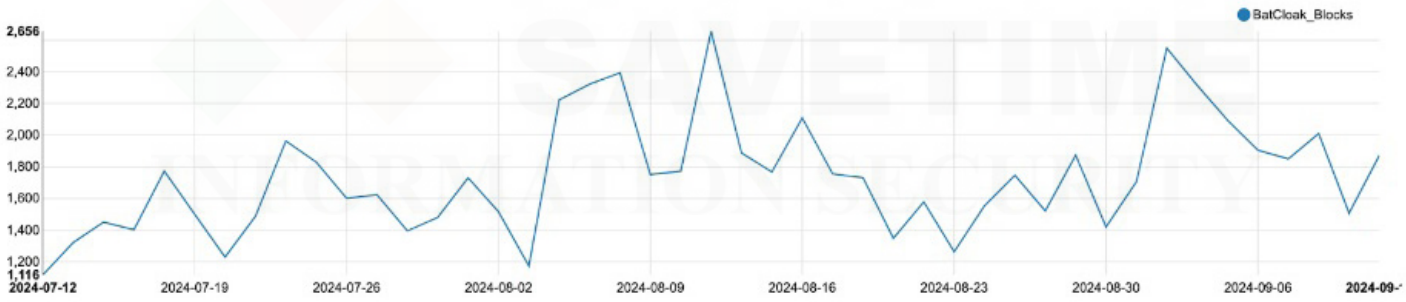
BatCloak 就是這樣一種惡意工具，用來繞過安全軟體、滲入電腦網路並傳遞各種惡意軟體。BatCloak 產生的批次檔案會混合使用壓縮、加密、多型 (polymorphism) 等手法進行高度混淆，以躲避檔案掃描和模擬引擎的偵測。在安全產業中，這些惡意軟體通常被稱為「完全無法被偵測有異的惡意軟體」或 FUD(Fully Undetectable)， (請勿與該縮寫的另一種用法混淆，該縮寫用於描述目的在散佈恐懼 (Fear)、不確定性 (Uncertainty) 和懷疑 (Doubt) 的可疑資訊)，但必須說這些惡意軟體顯然並非完全無法偵測，它們只是期望不被偵測到而已。這些批次檔案接著會利用 LOTL(就地取材) 攻擊鏈 (LOTL 或「Living Off The Land」攻擊是一種網路攻擊，利用被入侵系統上已有的合法工具) 來載入並執行各種有效酬載。BatCloak 已在多個攻擊行動中被用來傳送各種惡意軟體，包括各大家族的惡意竊密程式和遠端存取木馬 (RAT)，例如：AgentTesla、AsyncRAT 和 Snake Keylogger。

賽門鐵克端點防護／安全上的行為分析技術(SONAR)

SONAR 是賽門鐵克安全防護中，多掃毒引擎之一也是不可或缺的一層，非常適合偵測和攔截具有攻擊性混淆的惡意軟體。SONAR 會追蹤並分析所有程序的行為，包括作業系統的行為。透過檔案掃描和模擬很難偵測到的 LOTL 攻擊和惡意軟體，可以在早期階段透過行為方式偵測，並在有效酬載執行之前加以攔截。

Symantec 透過下列偵測成功阻擋數以千計的 BatCloak 攻擊：

- SONAR.BatCloak!gen1
- SONAR.BatCloak!gen2



欲瞭解有關賽門鐵克端點防護／安全上的多掃毒引擎之一的行為分析技術 (SONAR：Symantec Online Network for Advanced Response)？請點擊此處。

欲瞭解管理行為分析 (SONAR)，請點擊此處。

欲瞭解 SONAR 如何與賽門鐵克雲端沙箱 (Symantec Cloud Sandbox) 整合，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，以及基於比原廠更孰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**。