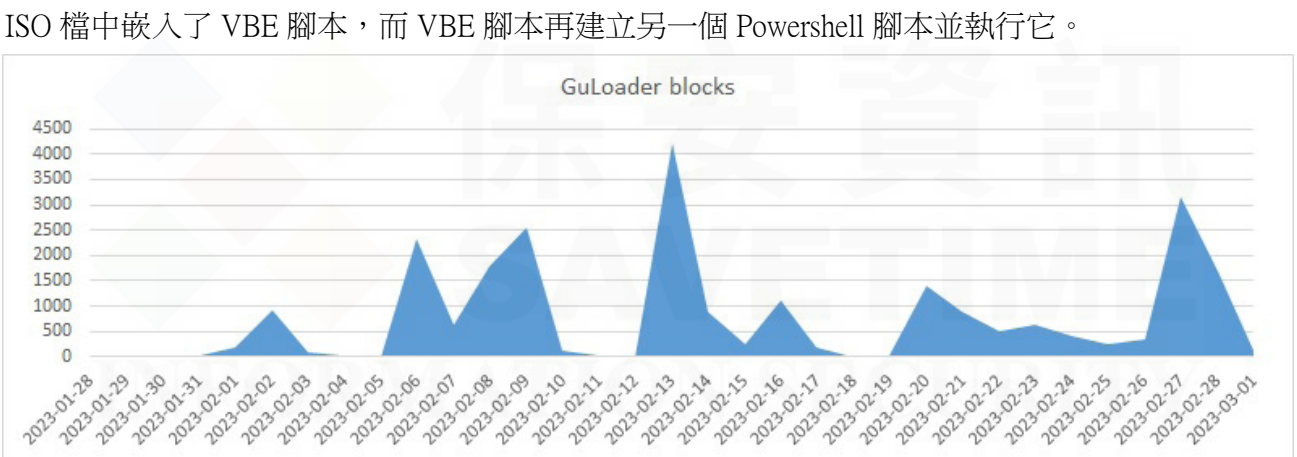
第一時間成功攔截～GuLoader隱藏在眾目睽睽之下的先進惡意軟體下載程式

2023 年 3 月 6 日發布

GuLoader 是一種進階型的 shellcode (利用軟體漏洞讓 CPU 執行特定程序的機械碼)，GuLoader利用多種對抗分析的方式來增加反向工程的難度，使得它更難被偵測到。它的終極目標是傳遞一系列的惡意軟體，包含勒索軟體 (ransomware)、偷取敏感資訊的惡意軟體 (infostealers)、偷取金融資訊的惡意軟體 (banking Trojans)、遠端存取木馬 (RAT)、代理程式 (Proxy) 等。賽門鐵克威脅獵手團隊最近在一篇名為『Bluebottle：發動攻擊非洲法語系國家銀行行動的駭客組織』(Bluebottle campaign targeting banks in French-speaking African countries) 的網誌中介紹了關於 GuLoader 的初階攻擊方式。

我們經常觀察到 GuLoader 是透過垃圾郵件的方式來散佈包含多種版本的 ISO 檔案，這些 ISO 檔中嵌入了 VBE 腳本，而 VBE 腳本再建立另一個 Powershell 腳本並執行它。



有多種 *GuLoader* 被偵測到，此處僅顯示 *Scr.Malcode!gen36*

雖然 GuLoader 不是什麼新的惡意軟體，但有趣的是作者為了不被偵測到而採取的措施。上面提到的 ISO/VBE 攻擊大致流程是……一開始一個經過代碼混淆的 Powershell 腳本去 Google Drive 下載並取出 GuLoader shellcode(使用 base64 編碼格式)，然後藉由 Windows API (CallWindowProcA) 將 shellcode 解碼 (base64)。從這裡開始 GuLoader 的作者就已進行避免偵測或延緩分析的措施。這些公告並不打算過於強調細節或技術性資訊，因此我們將儘量簡化說明。

GuLoader的反偵測技巧

- 反防毒軟體 #1：GuLoader 首先試圖防止作業系統從與 GuLoader 相關的 shellcode 區塊生成可執行檔，這是一個非常古老的技巧。
- 反除錯 #1：GuLoader 透過 Windows API 設置一個向量例外狀況處理常式(VEH)，並將代碼執行流指向到受管理的異常處理程序，該程序會嘗試捕捉由 EXCEPTION_SINGLE_STEP(TrapFlag) 引起的異常。 TrapFlag 允許處理器在單步模式下運行，可以操縱它以防止追踪。
- 反除錯 #2：反硬體間斷點和反軟體間斷點。硬體和軟體的間斷點是指在除錯時的暫停事件。GuLoader 會檢查這些事件並試圖防止它們。
- 反虛擬機 #1：記憶體分頁掃描。GuLoader 使用 NtQueryVirtualMemory API 掃描整個記憶體和處理程序，檢查是否有任何虛擬機 (VM) 或除錯工具相關的字串。
- 防禦逃避 #1 : Heaven's Gate 是一種在 2000 年代中期為了相容性目的而使用的一種方法，允許在 32 位元程序中執行 64 位元程式碼。GuLoader shellcode 使用 Heaven's Gate 執行一個 64 位元程式碼中介(stub)使其不被注意。
- 反虛擬機 #2 : GuLoader 檢查是否存在與 QEMU(VM) 模擬器相關的文件，例如：C:\Program Files\Qemu-ga\qemu-ga.exe 和 C:\Program Files\qga\qga.exe。
- 反除錯 #3：GuLoader 對 DbgBreakPoint 和 DbgUiRemoteBreakin 進行修補，來避免除錯器將其加入主機的執行程序當中。
- 防禦逃避 #2：移除 NTDLL32 中的 Hooks(用來插入自定義程式碼或函數)。GuLoader shellcode 掃描 NTDLL 中的 SYSCALL 狀態模式，提取 SYSCALL 編號並將函數代碼恢復到原始狀態。
- 反沙箱 #1：列舉視窗。GuLoader 呼叫 EnumWindows API 來計算在受害者機器上運行的上層視窗(無論可見與否)。如果數量低於 12，則 shellcode 終止。
- 反除錯 #4：ThreadHideFromDebugger。一種常見的反除錯技術，利用 NtSetInformationThread API 來有效的將執行緒標記為對除錯器不可見。
- 反沙箱 #2：GuLoader 使用各種 API 來列舉 Windows 驅動程式、已安裝的軟體和服務，並將它們的雜湊值與預先儲存的雜湊值進行比較。
- 反除錯 #5：ProcessDebugPort。Guloader 呼叫 NtQueryInformationProcess 來檢測是否有除錯器附加到它的處理程序中。

在多次嘗試隱藏之後，GuLoader shellcode 使用執行程序掏空技術 (Process Hollowing) 將自己注入到另一個執行程序當中，執行程序掏空技術是一種代碼注入技術，可以將記憶體中合法執行程序的可執行區段替換(或附加)為惡意代碼。

最後，在經過一連串的反偵測技巧 (在我們的案例中顯然是不成功的) 之後，GuLoader 將下載最終有效負載。在這個特定的案例中，有效負載是臭名昭張的 Agent Tesla。

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅的**零時差**攻擊，能通過以下方式識別 GuLoader：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen36

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

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。

欲深入瞭解更多有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，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**。