TLP:WHITE

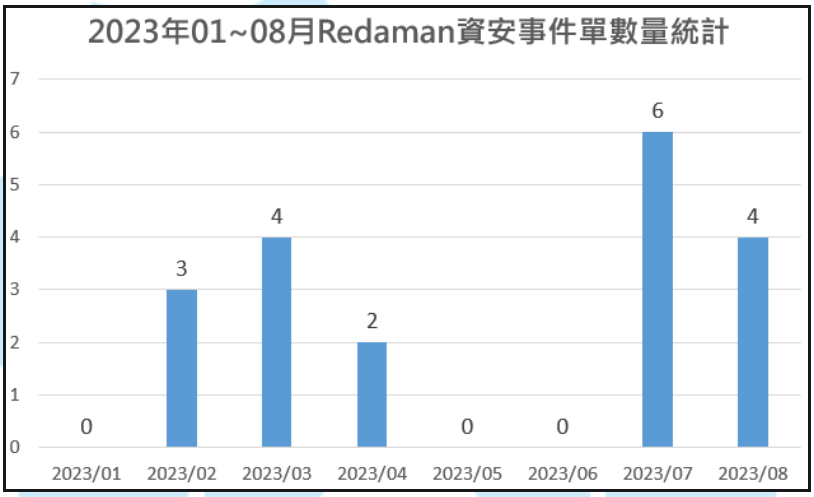
資訊竊取木馬 REDAMAN 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2023 年 10 月

一、事件簡介

1. 在 2023 年 7 月底~8 月初某高中持續觸發偵測規則「MALWARE-CNC Win.Trojan.Redaman outbound connection」，但學校無法有效處理，導致重複觸發。該校發生同一網段中有 5 個 IP 被攻擊，而且攻擊時間相近，其連線目的 IP 皆為 94.X.X.112 :80 (德國)，推測有橫向移動攻擊之情形。
2. 在學術網路中 2023 年 01~08 月共有 19 件 Redaman 資安事件發生，其中大學有 9 件、高中有 10 件。



3. REDAMAN 在 2015 年首次出現，是高危險的資訊竊取木馬。在大多數情況下，REDAMAN 是通過垃圾郵件活動進行散播的。它的威脅類型屬於特洛伊木馬、竊取密碼的病毒、銀行惡意軟體與間諜軟體等。
4. 其感染途徑為社交工程，如受感染的電子郵件附件、惡意線上廣告、軟體破解等。網路罪犯基本上是發送數千封的欺騙性電子郵件，鼓勵收件者打開附件(例如: Microsoft Office 文件、存檔的可執行文件等) ，進而將 REDMAN 感染到系統中。
5. 為了解 Redaman 之攻擊行為，故進行該樣本檢測作業。

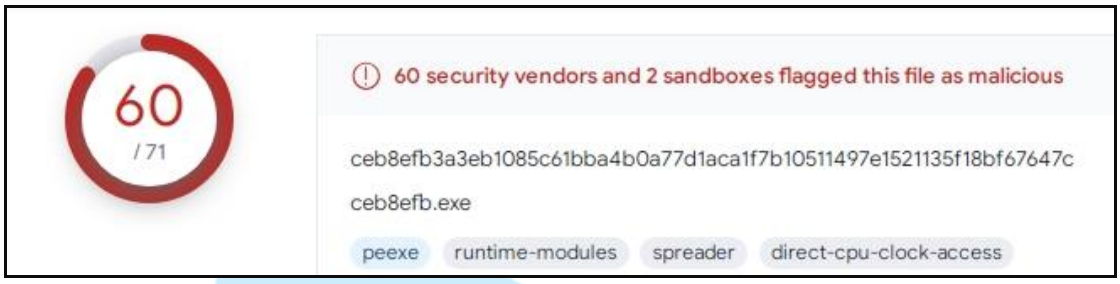
二、 事件檢測

1. 在 64 位元的 Windows 7 環境下，執行樣本 ceb8efb.exe

(MD:df725667733410f1a023a76d36fcbd31)，在執行 7 秒後該樣本在所在資料夾內消失。

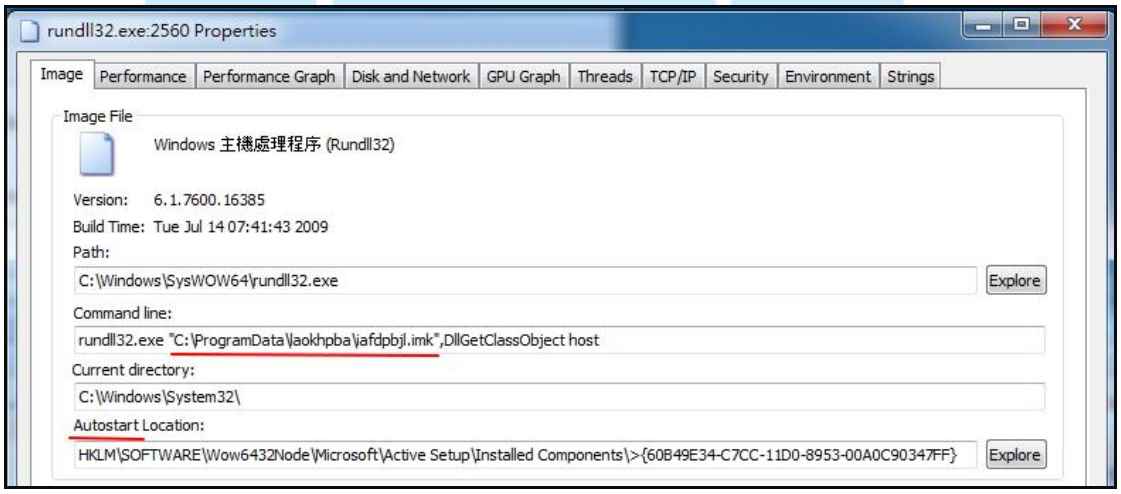
Process	Image Path	Command	Start Time	End Time
ceb8efb.exe (2752)	C:\Users\TEST\Downloads\ceb8efb.exe	"C:\Users\TEST\Downloads\ceb8efb.exe"	2023/9/22 上午 10:05:49	2023/9/22 上午 10:05:56

2. 該樣本經 Virustotal 檢測其惡意比例為 60/71。



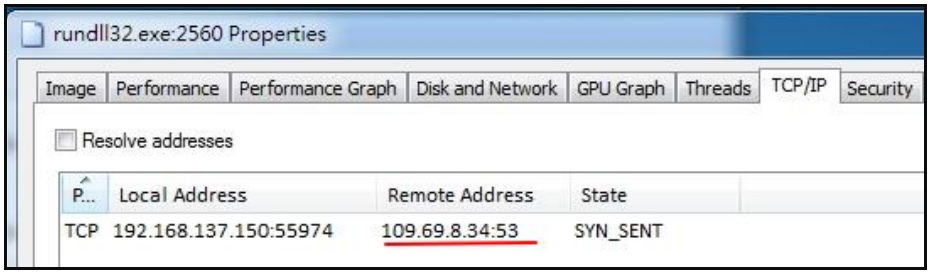
3. 該樣本執行後會建立工作排程，呼叫 rundll32.exe 來執行。

4. Rundll32.exe 會讀取 C:\ProgramData\laokhpba\iafdpbjl.imk 檔案，而且該 Rundll32.exe 會每次開機後自動執行。

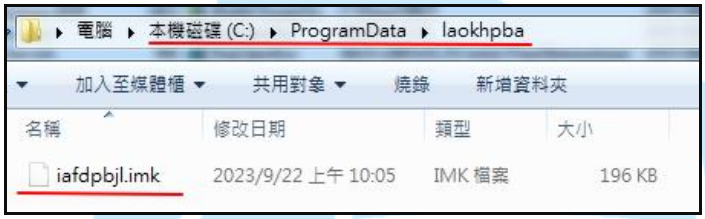


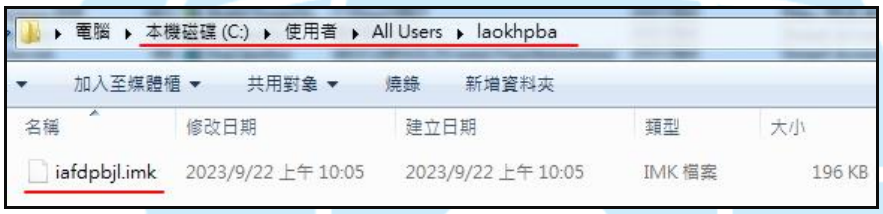
5. Rundll32.exe 執行時會一直對外連線下列目的 IP 之 53port，而且在每次開機後執行 rundll32.exe 就會連線。所連線目的 IP 有 188.165.200.156 (法國) (Virustotal:12/89)、5.135.183.146 (法國) (Virustotal:6/89)、109.69.8.34 (西班牙) (Virustotal:4/89)、151.80.147.153 (法國) (Virustotal:9/89)與 185.190.82.182 (美國) (Virustotal:1/89)等，而且這些 IP 設備為 DNS Server。檢視這些連線之封

包，發現僅有連線未傳輸任何資料，推測此行為僅在建立連線管道。

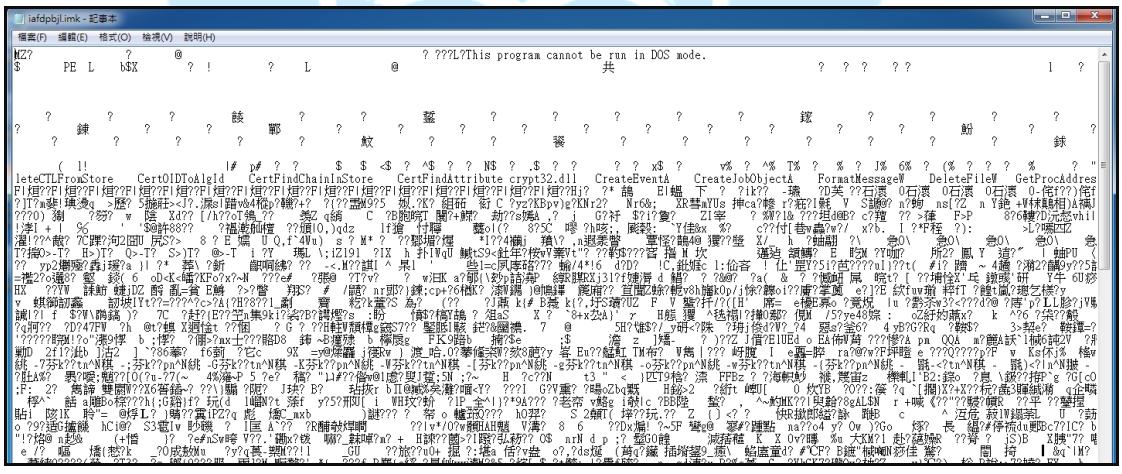


6. 樣本 ceb8efb.exe 執行後，會在 C:\ProgramData\與 C:\使用者\All Users 產生含有 iafdpbjl.imk 檔案之 laokhpba 資料夾。laokhpba 為隱藏資料夾，iafdpbjl.imk 為一個隱藏檔，因為使用隱藏功能，導致使用者不容易發現到它們的存在。



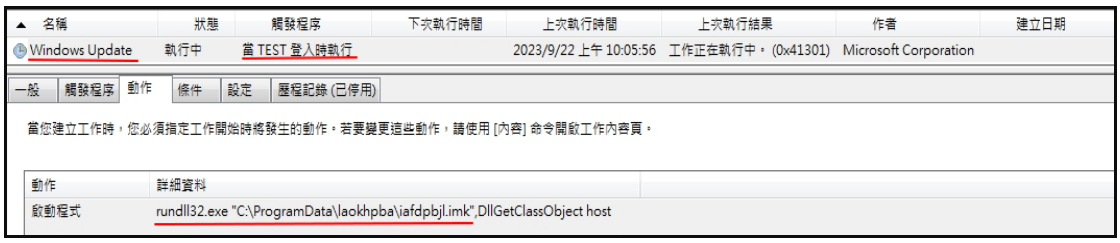


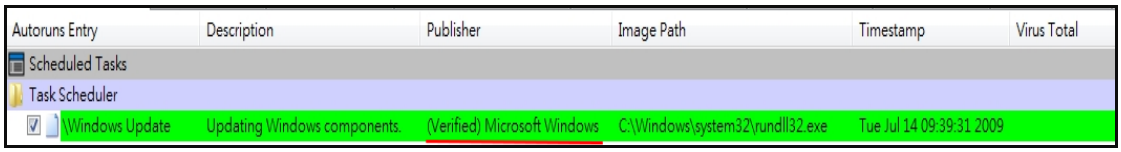
7. 檢視 iafdpbjl.imk 內容，發現為亂碼。



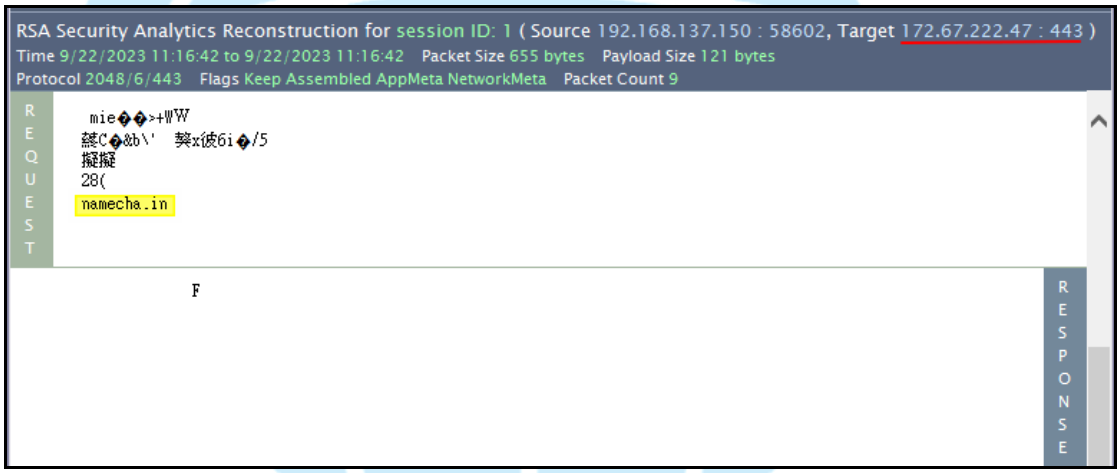
8. 檢視工作排程內容，發現一個 Windows Update 的工作排程。該排程在使用者 TEST 登入時執行，而且會啟動 rundll32.exe 來執行 C:\ProgramData\laokhpba\iafdpbjl.imk。該工作排程偽裝為合法的 Windows 更

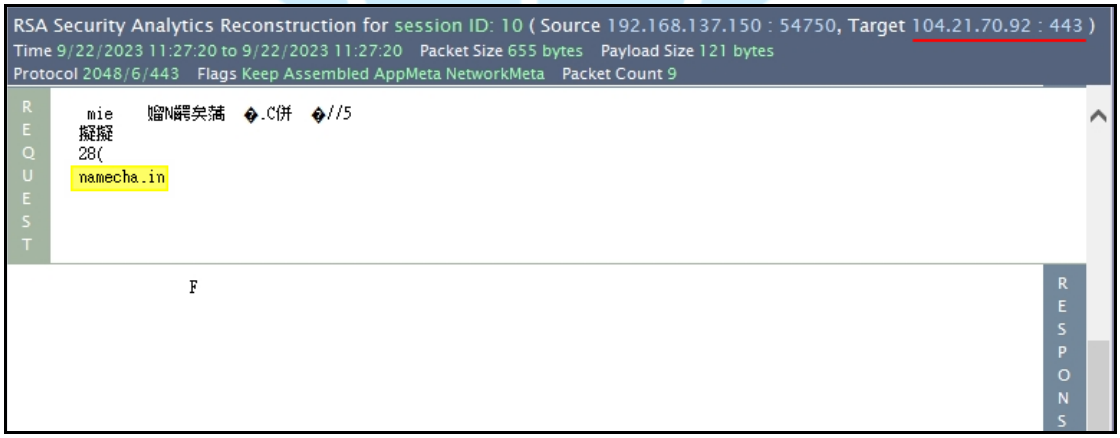
新排程，不容易讓使用者發現異常。





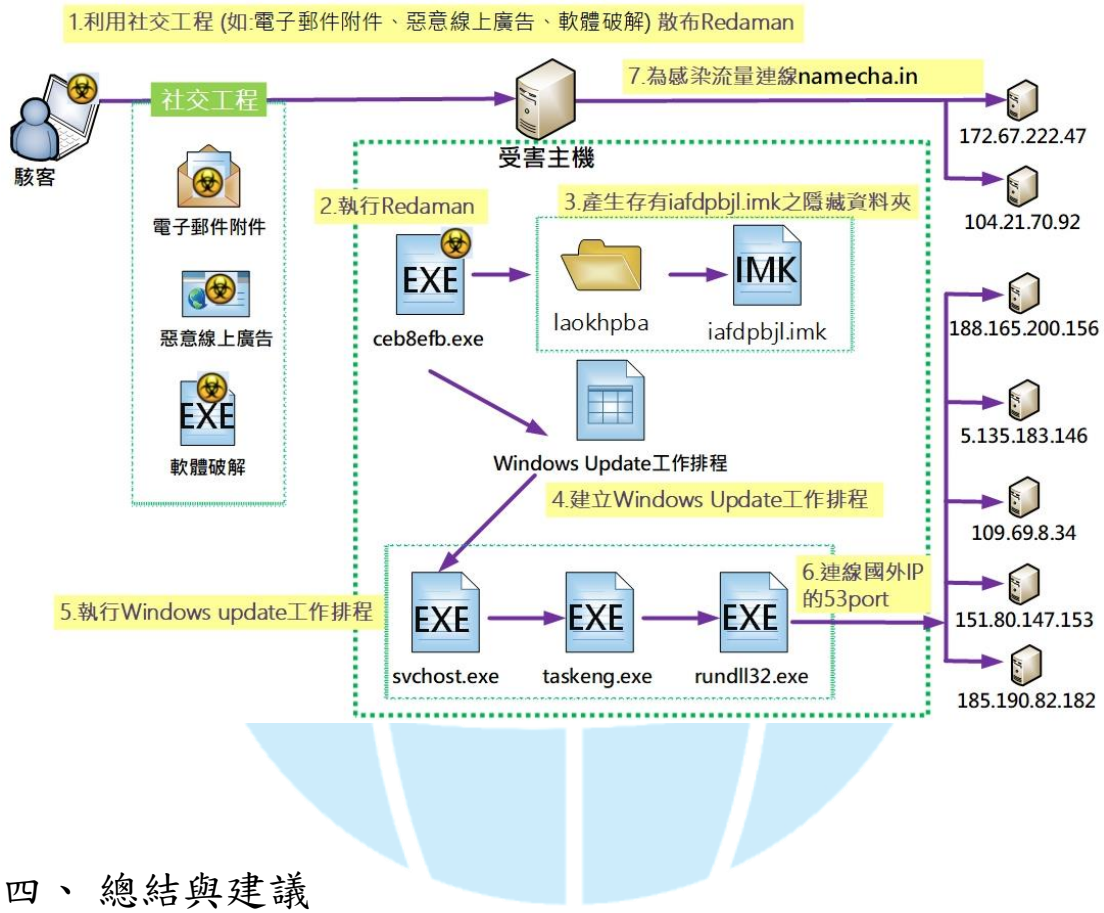
9. REDAMAN 有感染流量之特徵，故檢視其側錄封包，發現有連線 namecha[.]in 之 IP 情形，但並未有進一步連線後續感染流量之 IP(C2 server)行為。所連線 IP 有 172.67.222.47:443 與 104.21.70.92:443(皆為美國 IP，Virustotal 檢測為非惡意 IP)。此外，namecha[.]in 是一個 Namecoin 區塊瀏覽器，而 Namecoin 是一種可用於去中心化 DNS 的加密貨幣系統。





三、 攻擊行為

經由檢測可推測出駭客攻擊手法如下圖。首先，Redaman 利用社交工程方式散播本身。待 Redaman 感染受害主機後，會產生存有 iafdpbjl.imk 的隱藏資料夾。接著它會建立 Windows update 的工作排程來執行，而當這排程執行時會執行 rundll32.exe 來連線國外 IP 的 53port。為感染流量，它也會連線 namech.in，以利後續連線之後的 C2 Server。



四、 總結與建議

1. 經檢測後總結 REDAMAN 特徵如下。

(1) REDAMAN 主要透過社交工程方式散播，在主機感染後會建立隱藏資料夾，並新增 Windows Update 工作排程，來持續執行 rundll32.exe 去對外連線。

(2) 在建立工作排程並載入 DLL 後，初始的 Redaman 執行檔會自行刪除。除受害主機外，它也會橫向移動攻擊網域內其他主機。

(3) 它會竊取資訊，能夠截取螢幕截圖、記錄擊鍵以及竊取信用卡資訊。它也能記錄基本的系統資訊，並將收集的資訊保存到遠端伺服器內。

(4) 該木馬旨在秘密地滲透到受害者的主機並保持沉默，因此在受感染的主機上沒有明顯可見的特定症狀。

(5) 有數十種木馬類型病毒與 REDAMAN 一樣會竊取資訊，例如:TrickBot、Emotet、LokiBot 和 Adwind。

2. 在 REDAMAN 可能造成的影響方面，由於 REDAMAN 會竊取資訊，所以會對 CIA 中的機密性造成衝擊。
3. 關於感染 REDAMAN 的處理方式，使用者若最近有打開過任何可疑的電子郵件附件，建議檢查 Windows 工作排程器中列出的可疑排程。若使用者懷疑 REDAMAN 可能已滲透到主機內，建議可使用防毒軟體或反間諜軟體掃描系統，來移除檢測到的惡意軟體。
4. 在未來預防 REDAMAN 的方面，因 REDAMAN 是透過社交工程方式散播，建議使用者不要開啟不明來源的郵件附件、不要從不明來源網站下載與安裝軟體， 以杜絕其散播管道。

五、 參考資料

1. REDAMAN Trojan
https://www.pcrisk.com/removal-guides/13783-redaman-trojan
2. Russian Language Malspam Pushing Redaman Banking Malware
https://unit42.paloaltonetworks.com/russian-language-malspam-pushing-redaman-banking-malware/
3. TrojanSpy.Win32.REDAMAN.AA
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojanspy.win32.redaman.aa