TLP:WHITE

新型態竊密軟體 Prynt Stealer

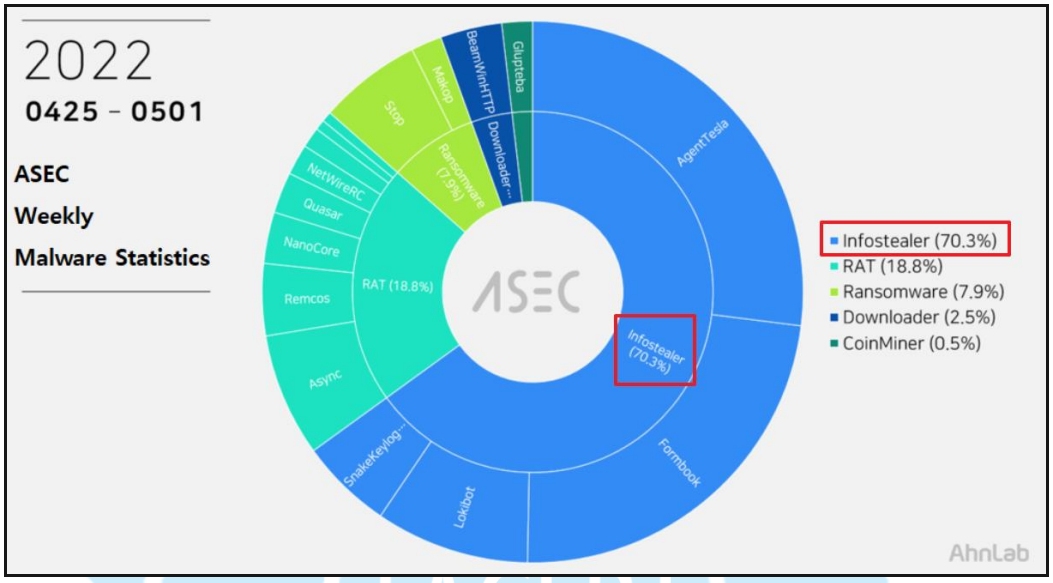
分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2022 年 05 月

一、事件簡介

1. 由 ASEC 分析團隊每週惡意軟體數量統計顯示，發現近期竊密軟體持續排名第一(70.3%)。統計學網中竊密軟體之資安事件數量，發現在 2022/3~4 月資安事件數量有上升趨勢。由此可見，竊密軟體的攻擊逐漸增多。



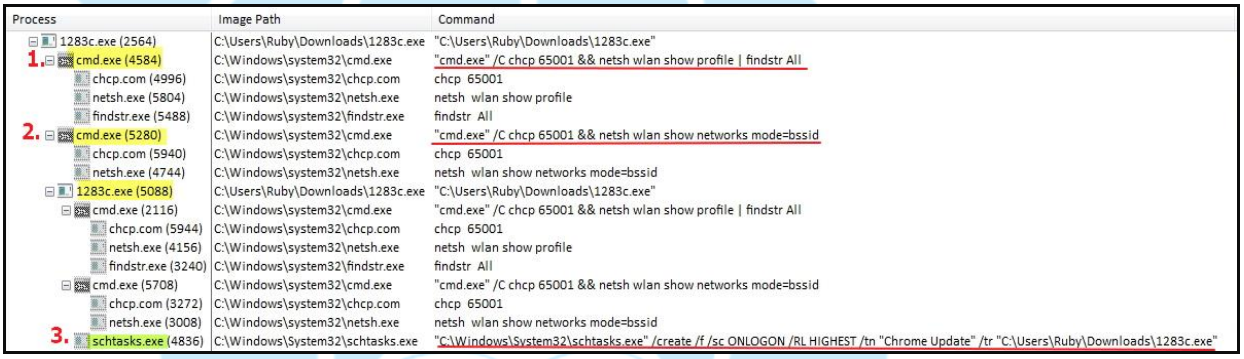
(資料來源:ASEC Weekly Malware Statistics)

2. 新型態之竊密軟體 Prynt Stealer 有別於傳統只使用 keylogger 來竊密。它提供了強大的功能和額外的鍵盤記錄器和剪輯器模組。
3. 它的開發者採用以時間為單位的訂閱方式銷售該軟體，例如每月 100 美元，也可用 900 美元終身買斷出售。它讓買家利用該軟體的 builder 自行設定該軟體之功能，來產生新 Prynt Stealer 樣本。
4. 為了瞭解這個新型態之竊密軟體所具備之功能與攻擊行為，本中心對其樣本進行分析。

二、 事件檢測

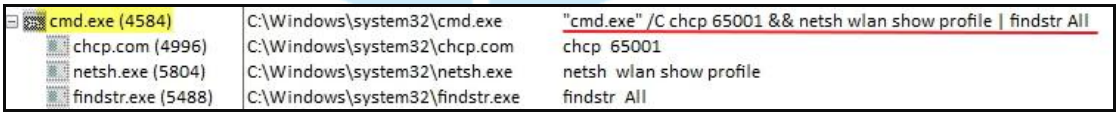
1. 首先，將樣本 1283c.exe(MD5:ab913c26832cd6e038625e30ebd38ec2)放於一台具有 32 位元 Windows 7 作業系統之主機上執行，執行後該樣本仍在原地未消失。查看 1283c.exe 之內容，發現其原始檔名為 Prynt Stealer Reborn.exe。

2. 1283c.exe 執行後會使用 cmd.exe 呼叫 chcp.com、netsh.exe 與 findstr.exe 等三個程式來執行，之後再次呼叫自己執行一次(約 45 秒後)，最後則執行 schtasks.exe 來新增一個工作排程 Chrome Update。



Process	Image Path	Command
1283c.exe (2564)	C:\Users\Ruby\Downloads\1283c.exe	"C:\Users\Ruby\Downloads\1283c.exe"
1. cmd.exe (4584)	C:\Windows\system32\cmd.exe	"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All
chcp.com (4996)	C:\Windows\system32\chcp.com	chcp 65001
netsh.exe (5804)	C:\Windows\system32\netsh.exe	netsh wlan show profile
findstr.exe (5488)	C:\Windows\system32\findstr.exe	findstr All
2. cmd.exe (5280)	C:\Windows\system32\cmd.exe	"cmd.exe" /C chcp 65001 && netsh wlan show networks mode=bssid
chcp.com (5940)	C:\Windows\system32\chcp.com	chcp 65001
netsh.exe (4744)	C:\Windows\system32\netsh.exe	netsh wlan show networks mode=bssid
1283c.exe (5088)	C:\Users\Ruby\Downloads\1283c.exe	"C:\Users\Ruby\Downloads\1283c.exe"
cmd.exe (2116)	C:\Windows\system32\cmd.exe	"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All
chcp.com (5944)	C:\Windows\system32\chcp.com	chcp 65001
netsh.exe (4156)	C:\Windows\system32\netsh.exe	netsh wlan show profile
findstr.exe (3240)	C:\Windows\system32\findstr.exe	findstr All
cmd.exe (5708)	C:\Windows\system32\cmd.exe	"cmd.exe" /C chcp 65001 && netsh wlan show networks mode=bssid
chcp.com (3272)	C:\Windows\system32\chcp.com	chcp 65001
netsh.exe (3008)	C:\Windows\system32\netsh.exe	netsh wlan show networks mode=bssid
3. schtasks.exe (4836)	C:\Windows\System32\schtasks.exe	"C:\Windows\System32\schtasks.exe" /create /f /sc ONLOGON /RL HIGHEST /tn "Chrome Update" /tr "C:\Users\Ruby\Downloads\1283c.exe"

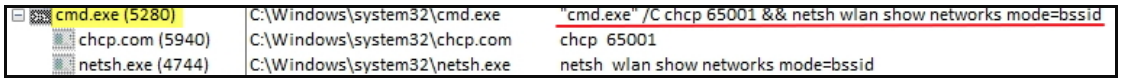
(1) 1283c.exe 執行後呼叫 cmd.exe 來變更編碼方式為 UTF-8，列出主機曾經連接過的所有 Wifi 資訊，並且快速搜尋主機的所有檔案內是否含有特殊字串。



cmd.exe (4584)	C:\Windows\system32\cmd.exe	"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All
chcp.com (4996)	C:\Windows\system32\chcp.com	chcp 65001
netsh.exe (5804)	C:\Windows\system32\netsh.exe	netsh wlan show profile
findstr.exe (5488)	C:\Windows\system32\findstr.exe	findstr All

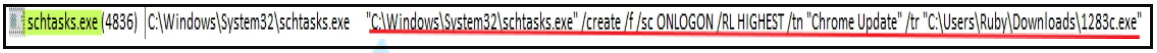
- **chcp.com chcp 65001** 將 CMD 命令視窗編碼方式設定為 UTF-8 編碼
- **netsh.exe netsh wlan show profile** 此命令可以列出主機曾經連接過的所有 WiFi 網路配置資訊(記錄 WiFi 網路名稱)。
- **findstr.exe findstr All** 如同 Windows 上的 grep (快速搜尋檔案)，findstr 為用於在特定檔案中搜索特定字串的命令。

(2) 接著再次呼叫 cmd.exe 變更編碼方式為 UTF-8 後，查詢當前掃描到的 AP 資訊。(AP 為 Wireless Access Point)



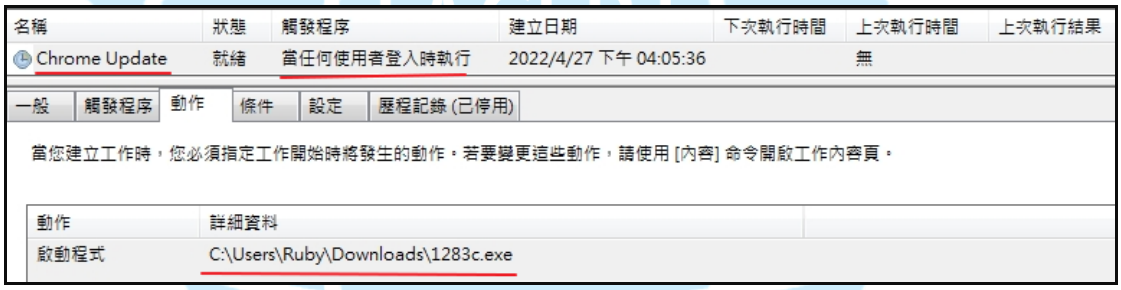
- **chcp.com chcp 65001** 將 CMD 命令視窗編碼方式設定為 UTF-8 編碼
- **netsh wlan show networks mode=bssid** 查詢當前掃描到的 AP 資訊

(3) 最後新增一個名為 Chrome Update 排程來執行 1283c.exe。

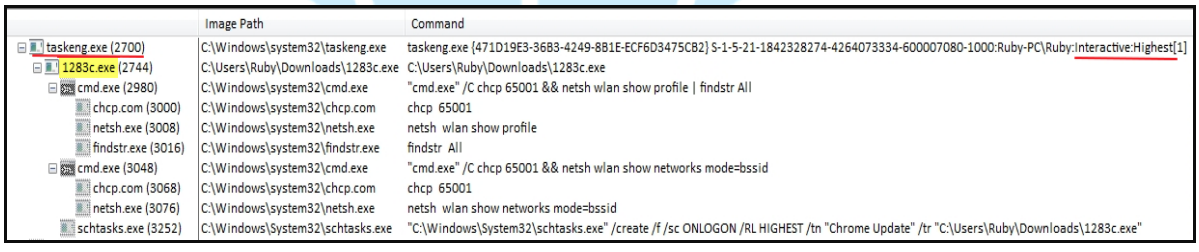


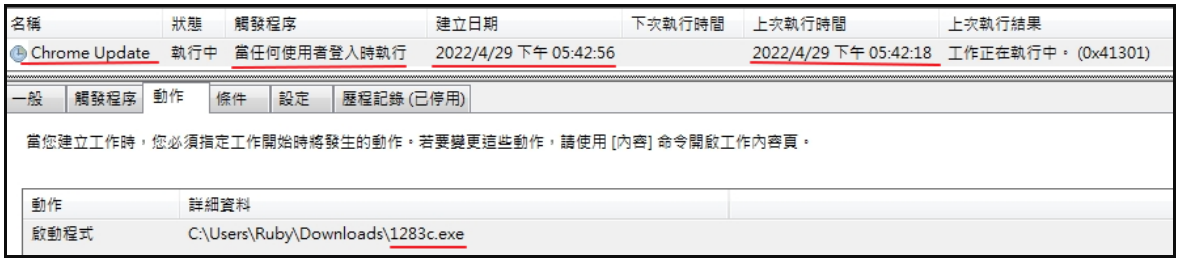
- **schtasks.exe /create /f /sc ONLOGON /RL HIGHEST /tn "Chrome Update" /tr "…1283c.exe"** 新增一個名為 Chrome Update 之工作排程來執行 1283c.exe，該排程在每當使用者登入時就會以最高權限執行。

3. 在工作排程器發現一個新增排程 Chrome Update，該排程在每次主機開機而且使用者登入時，會以最高權限來執行 1283c.exe。

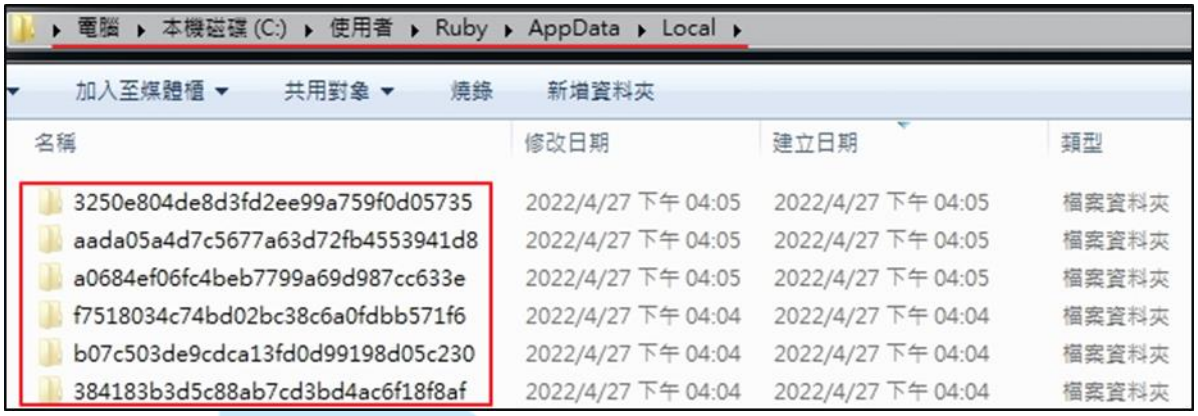


4. 執行 1283c.exe 後會重複執行著前述 cmd.exe 命令行為，最後再次重複新增排程 chrome update，故這個排程的建立時間會在上次排程執行時間之後。

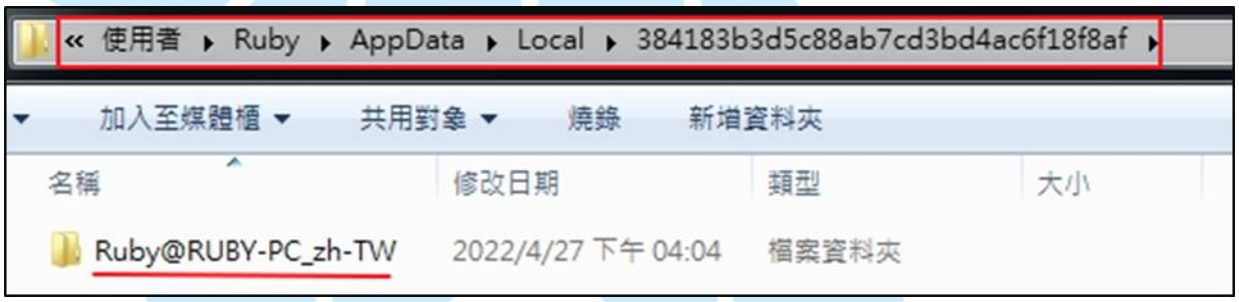




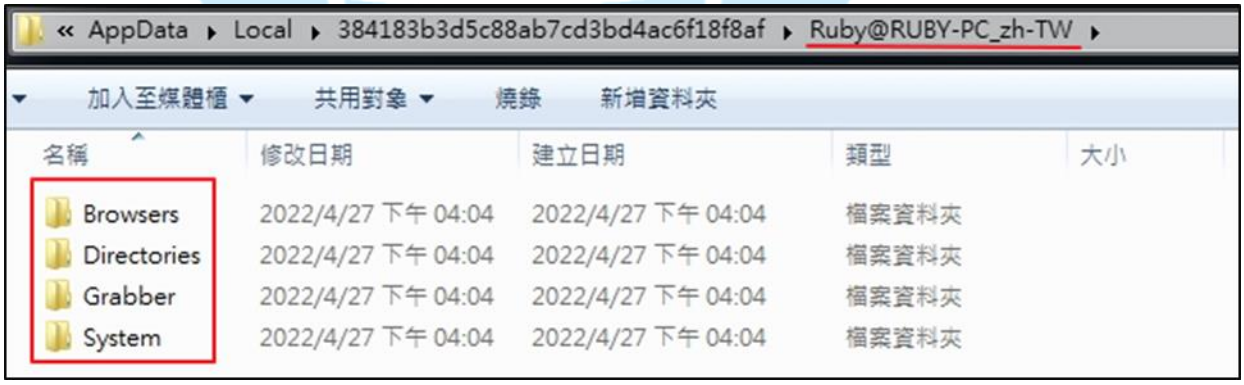
5. 1283c.exe 執行後在使用者 AppData\Local 資料夾內建立幾個隱藏資料夾，這些資料夾名稱使用 MD5 Hash 值命名。



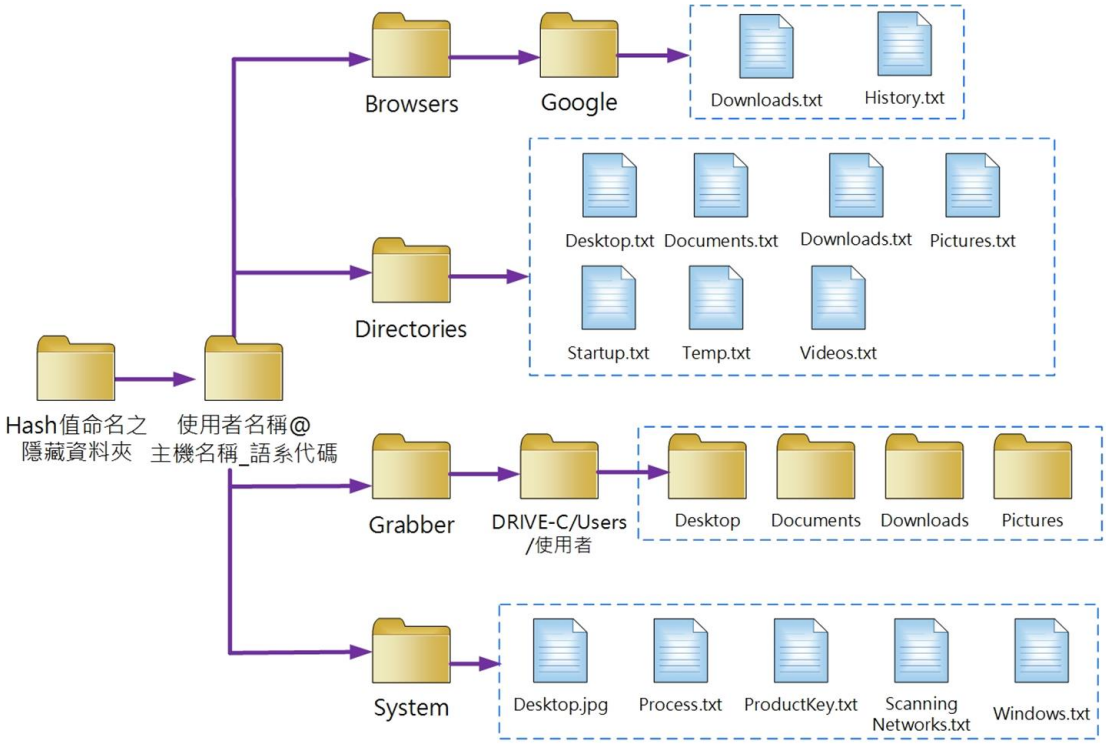
6. 隱藏資料夾內會建立一個子資料夾，並使用「使用者名稱@主機名稱_語系代碼」格式命名。



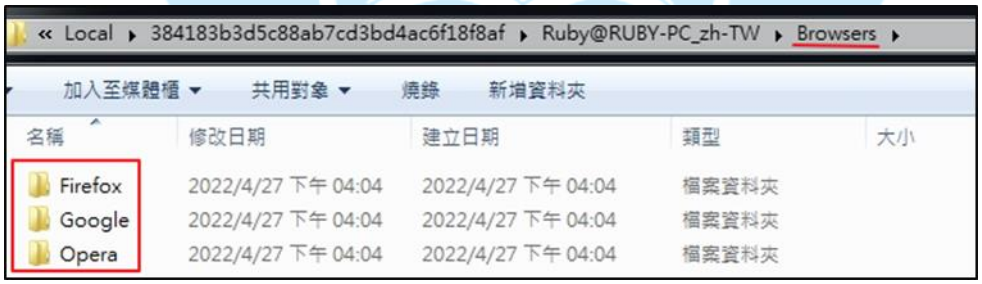
7. 在子資料夾中會建立 4 個資料夾(Browsers、Directories、Grabber 與 System 等)，而這些資料夾用於保存從各個來源竊取到的資料。

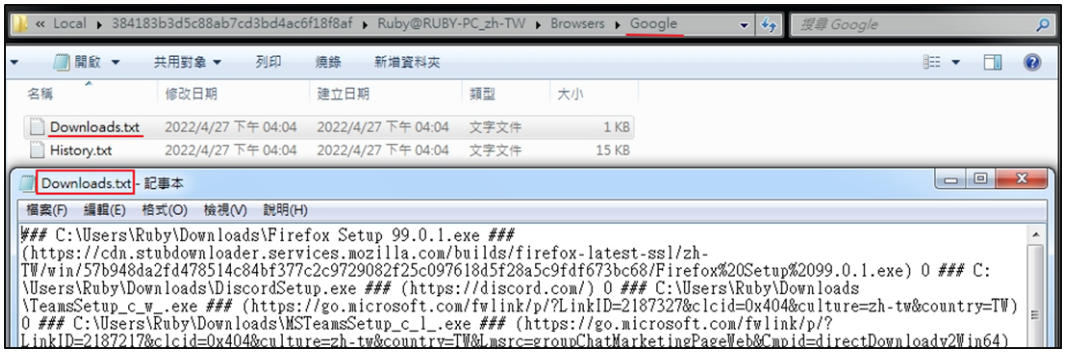


整理隱藏資料夾內容如下圖所示。



8. 檢視「Browsers」資料夾，內有以瀏覽器命名之資料夾，在 Google 資料夾內有兩個檔案 Downloads.txt 與 History.txt。Downloads.txt 記錄該主機曾經下載過之檔案，而 History.txt 記錄該主機曾經瀏覽過的網站。此外，在 Firefox 與 Opera 兩資料夾內皆存放 Bookmarks.txt(書籤)與 History.txt(瀏覽紀錄)兩個檔案。





9. 檢視「Directories」資料夾，該資料夾主要用於獲取目錄結構並將其寫入文字檔中。所針對的目錄包括最初用於複製資料的目錄。

(1) Desktop.txt　桌面所存檔案目錄結構與檔案路徑。

(2) Documents.txt　記錄 Documents 文件夾所存檔案目錄。

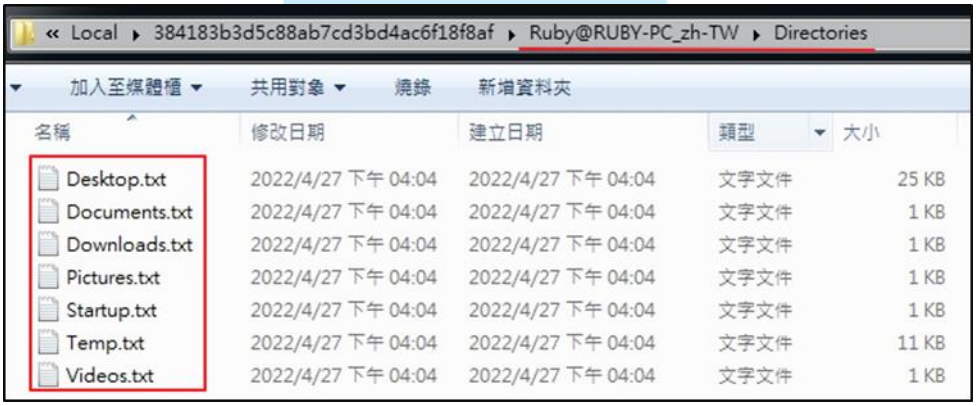
(3) Downloads.txt　下載資料夾內所有檔案目錄。

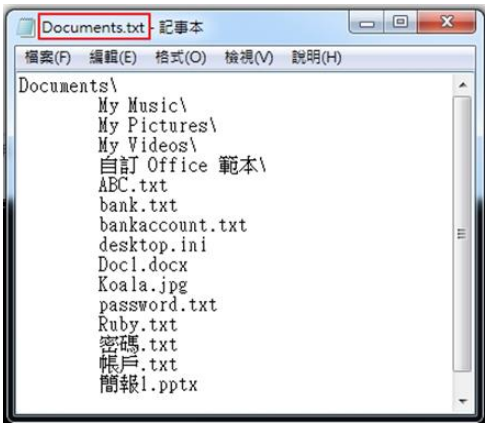
(4) Pictures.txt　記錄 Pictures 資料夾之檔案目錄。

(5) Startup.txt　記錄啟動資料夾之檔案目錄。

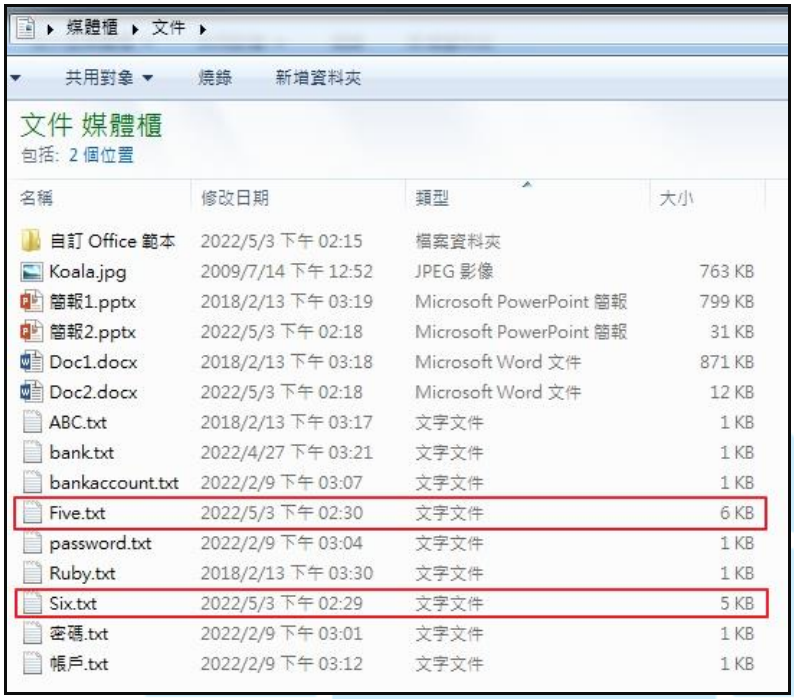
(6) Temp.txt　記錄在 Temp 資料夾內的檔案目錄結構與檔案路徑。

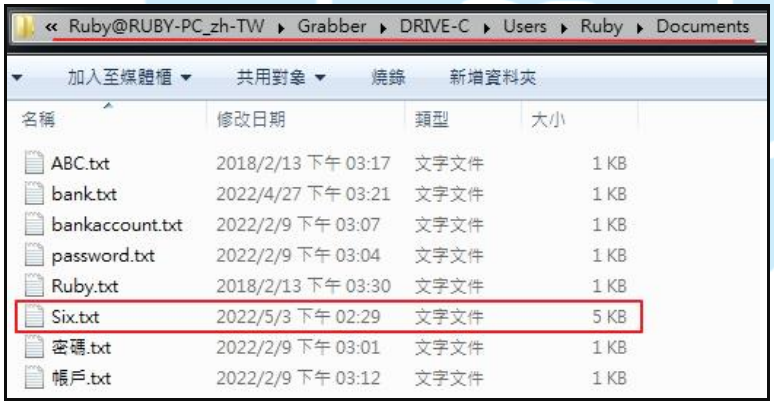
(7) Videos.txt　記錄 Videos 資料夾之檔案目錄。





10.檢視「Grabber」資料夾，發現該惡意程式將主機使用者所屬「Desktop、Documents、Downloads 與 Pictures」等資料夾內特定檔案類型之檔案複製一份存於此處，但僅複製等於或小於 5KB 大小之檔案。例如: Five.txt (6KB)沒有被複製，而 Six.txt(5KB)有被複製。





11.查看「System」資料夾，發現該惡意程式儲存有關運行中之程式資訊、網路詳細資訊和受害者系統截圖等資料。

(1) Desktop.jpg 對受害主機桌面進行截圖。

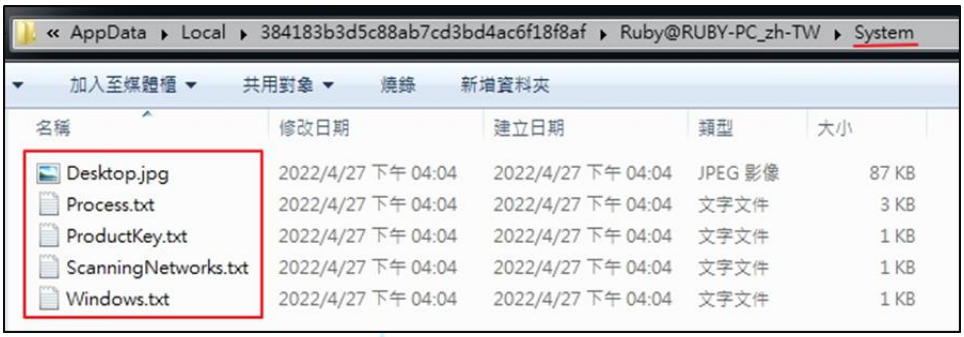
(2) Process.txt 記錄受害主機執行中的背景程式內容。

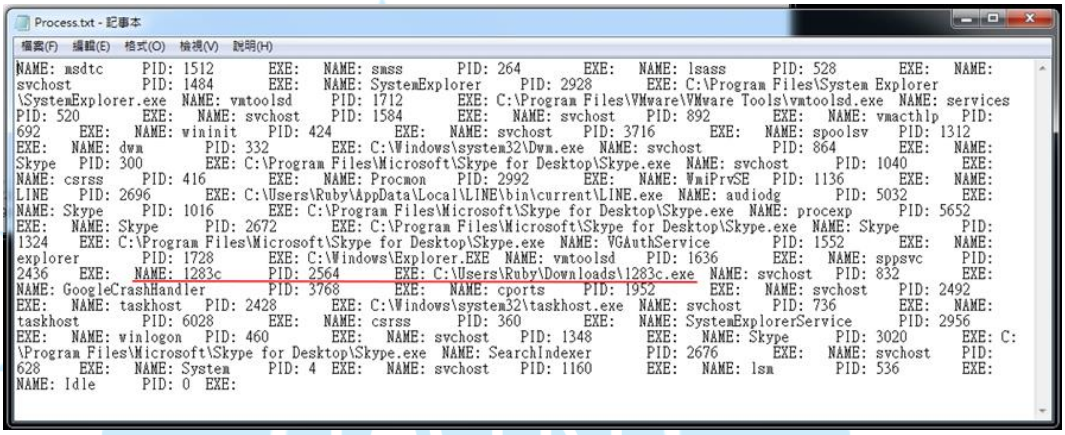
(3) ProductKey.txt 記錄 Windows 產品金鑰。

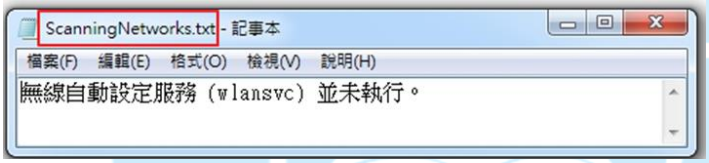
(4) ScanningNetworks.txt 記錄網路服務資訊。使用「/C chcp 65001 && netsh

wlan show networks mode=bssid」命令，獲取可用網路清單並保存到此 txt 檔內。

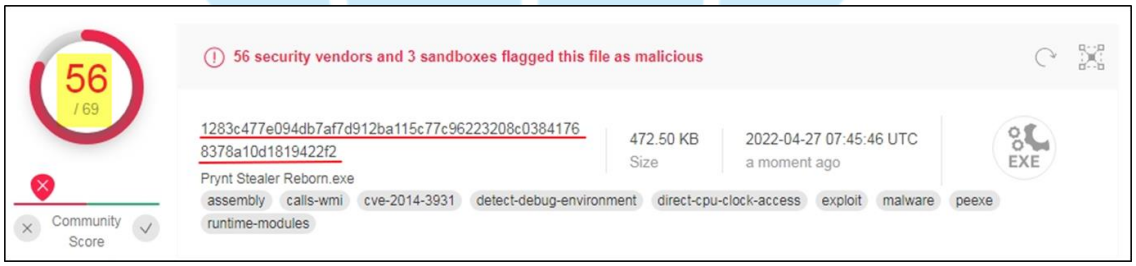
(5) Windows.txt　記錄執行中的視窗程式資訊。







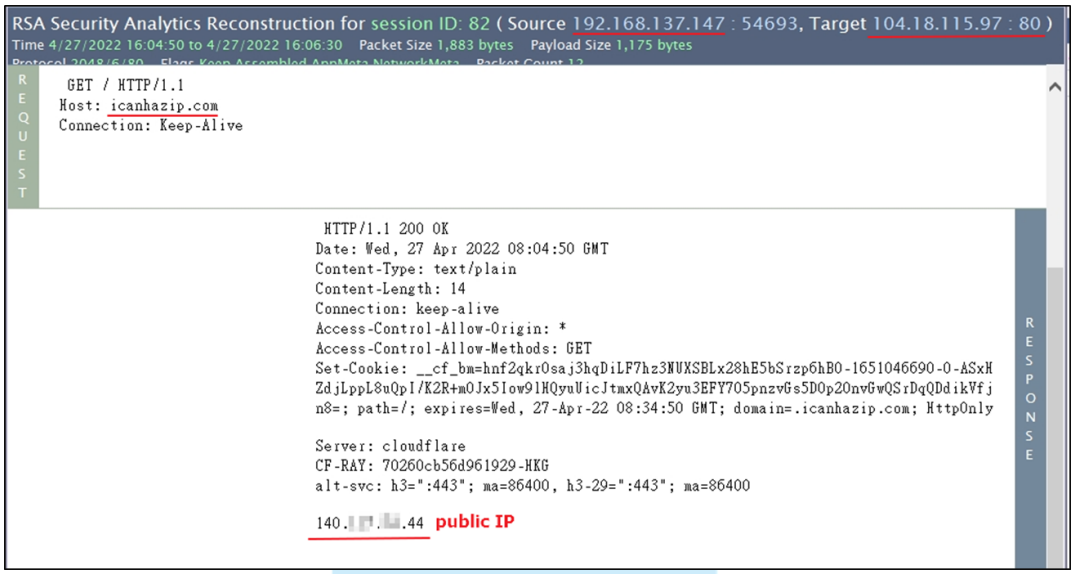
12.1283C.exe 經 Virustotal 檢測其惡意比例為 56/69。



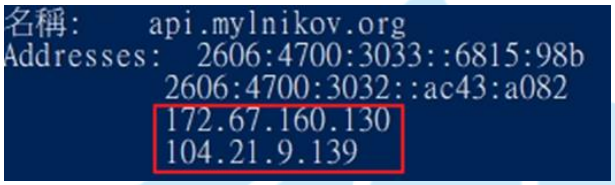
13.查看主機對外連線狀態，發現 1283c.exe 會對外連線 3 個美國 IP(IP:104.18.115.97、172.67.160.130 與 104.21.9.139)。

2022/4/27 下午 04:04:50	Added	1283c.exe	TCP 192.168.137.147:54693	104.18.115.97:80
2022/4/27 下午 04:04:52	Added	1283c.exe	TCP 192.168.137.147:54694	172.67.160.130:443
2022/4/27 下午 04:04:54	Added	1283c.exe	TCP 127.0.0.1:54697	127.0.0.1:8808
2022/4/27 下午 04:04:56	Removed	1283c.exe	TCP 127.0.0.1:54697	127.0.0.1:8808
2022/4/27 下午 04:05:33	Added	1283c.exe	TCP 192.168.137.147:54699	104.18.115.97:80
2022/4/27 下午 04:05:33	Added	1283c.exe	TCP 192.168.137.147:54700	104.21.9.139:443
2022/4/27 下午 04:05:35	Added	1283c.exe	TCP 127.0.0.1:54704	127.0.0.1:8808
2022/4/27 下午 04:05:37	Removed	1283c.exe	TCP 127.0.0.1:54704	127.0.0.1:8808
2022/4/27 下午 04:06:32	Removed	1283c.exe	TCP 192.168.137.147:54693	104.18.115.97:80
2022/4/27 下午 04:06:34	Removed	1283c.exe	TCP 192.168.137.147:54694	172.67.160.130:443
2022/4/27 下午 04:07:12	Removed	1283c.exe	TCP 192.168.137.147:54699	104.18.115.97:80
2022/4/27 下午 04:07:14	Removed	1283c.exe	TCP 192.168.137.147:54700	104.21.9.139:443

14.從封包分析發現，為了識別主機所使用之公用 IP(Public IP)，它會向 http[://]icanhazip.com (美國 IP:104.18.115.97)發送請求，來取得公用 IP 資訊。

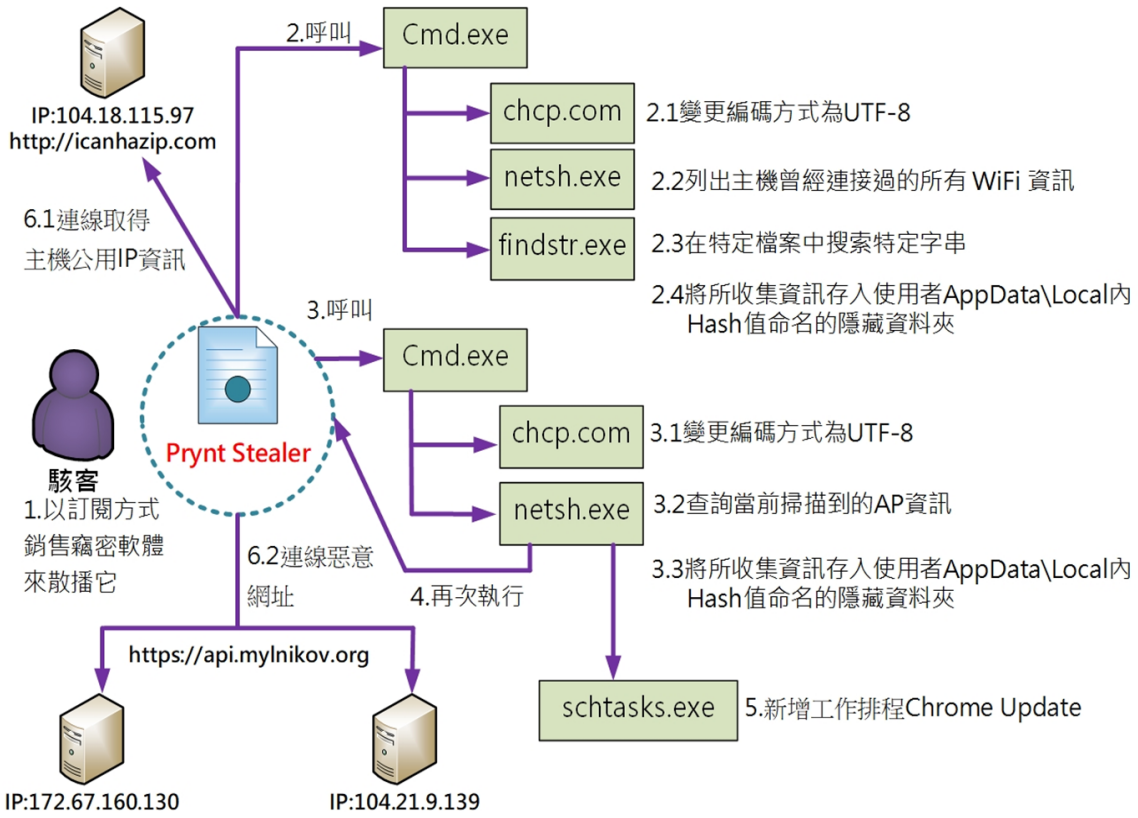


15.檢視 IP:172.67.160.130 與 104.21.9.139 之封包內容，發現兩個 IP 對應到相同網址 https[://]api.mylnikov.org。與使用 nslookup 查詢 IP 與網址對應相同結果，而且該網址經 Virustotal 檢測為惡意網址。



三、 事件攻擊行為

由下圖攻擊行為示意圖可得知，駭客散播竊密軟體，一旦主機感染竊密軟體後，開始呼叫 cmd.exe 來執行資訊收集，並且將資訊存入隱藏資料夾內。之後新增工作排程讓竊密軟體每次開機啟動，而最後會連線惡意網址。



四、 總結與建議

1. 竊密軟體 Prynt Stealer 是最近網路犯罪論壇上的新成員，具備多種功能。 它不只是記錄受害者鍵盤輸入內容，它還會複製受害者主機內使用者的檔案，將資料竊取走。它也會記錄目前受害主機程式運作狀態與網路資訊，以及對主機桌面截圖。它的行為與目前學網中所看到的竊密軟體(如 Redline)著重側錄使用者輸入內容有所不同。
2. 它除了竊取受害者的資料外，還可以使用剪輯器和鍵盤記錄操作進行財務盜竊。此外，它也可以針對瀏覽器、VPN、FTP、通訊軟體和遊戲應用軟體等進行資料竊取。
3. 由於它在每次開機時會以管理者權限自行啟動，建議在處理受害主機時應先中斷 Prynt Stealer 程式後再刪除 Chrome Update 排程，最後再移除 Prynt Stealer 程式。

4. 為避免遭受此軟體竊密，有下列幾點建議提供參考。

(1) 避免從不明來源網站下載盜版軟體，例如:一些網站提供的軟體工具可能包含此類惡意軟體。

(2) 盡可能使用強密碼並執行多因素身份驗證來登入系統。

(3) 在電腦、手機和其他連網設備上開啟自動軟體更新功能。

(4) 在所用設備上安裝防毒軟體，並且定期更新病毒碼。

(5) 請勿在未驗證其真實性的情況下打開不受信任的連結和電子郵件附件。

(6) 監控校內對外網路是否有異常紀錄，以阻止惡意軟體洩露資料。