TLP:WHITE

資訊竊取木馬 Agent Tesla

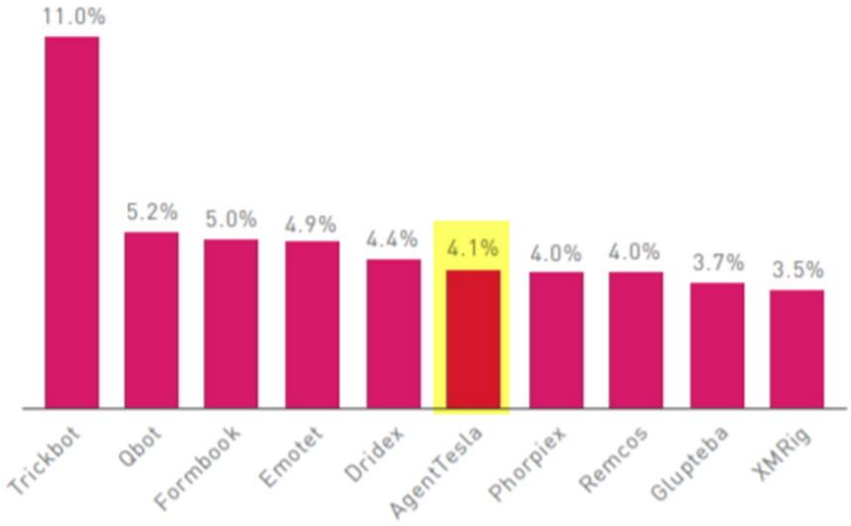
分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2022 年 02 月

一、事件簡介

1. 惡意軟體家族 Agent Tesla 自 2014 年出現，攻擊者將其運用來竊取主機上的機密。
2. 它主要是透過電子郵件附件挾帶為感染途徑，而且是以服務型態提供的惡意軟體（Malware-as-a-Service），這意味者攻擊者只要付費就能取得作案工具。
3. 資安公司 CHECK POINT 在 2022/1 所發布「CYBER SECURITY REPORT 2022」提到在 2021 年全球最流行的十大惡意軟體中，Agent Tesla 也名列其中。



資料來源：CHECK POINT 公司 2022/1 所發布「CYBER SECURITY REPORT 2022」報告

4. 根據 ASEC 分析團隊最新一次每週惡意軟體數量統計顯示(2022/01/31~2022/02/06)，在主要類別中，資訊竊取軟體以 61.6% 排名第一，其次是 RAT 惡意軟體，佔 18.9%，銀行惡意軟體佔 11.3%，勒索軟體佔 4.4%，下載程式佔 3.8%。在資訊竊取軟體中， Agent Tesla 再次以 40.3% 排名第一。

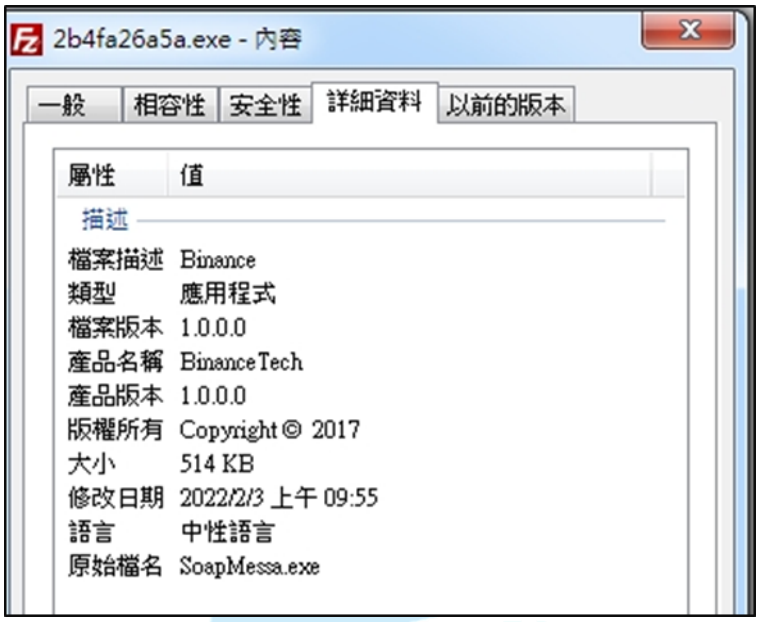
資料來源 :ASEC (AhnLab Security Emergency-response Center)

5. 有鑑於惡意軟體 Agent Tesla 感染事件流行頻繁，為了解其竊取資料的手法，故進行檢測作業。

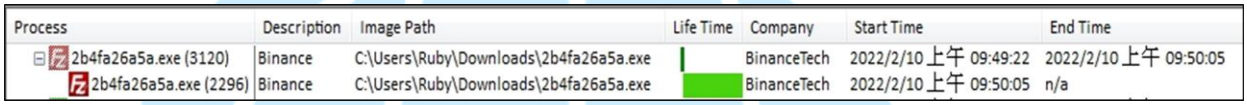
二、事件檢測

1. 首先，在 32 位元之 Windows 7 作業系統上，執行 Agent Tesla 樣本 2b4fa26a5a.exe (MD5:611e2838acaba7b86ed0f40c3d0c81fb) 。

2. 從樣本內容發現，該軟體之詳細資料具有一般合法軟體所該有的基本資訊。在該軟體之「詳細資料」中看到產品名稱與產品描述皆有「Binance」，它是一家全球性的加密貨幣交易所，為超過 100 種加密貨幣提供交易平台。2018 年初以來，幣安 Binance 在交易量方面被認為是全世界上最大的加密貨幣交易所。

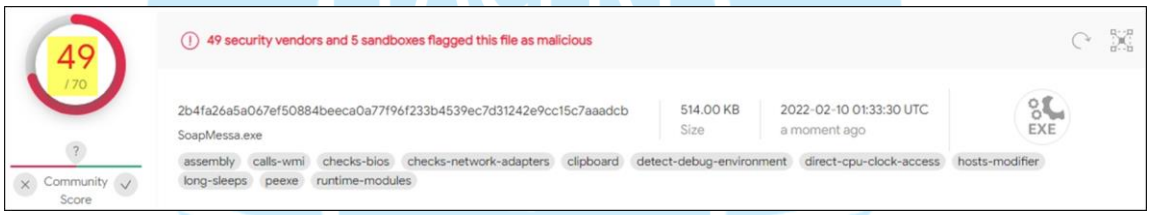


3. 2b4fa26a5a.exe 執行後會再次呼叫自己來執行， 之後默默在背景中執行。

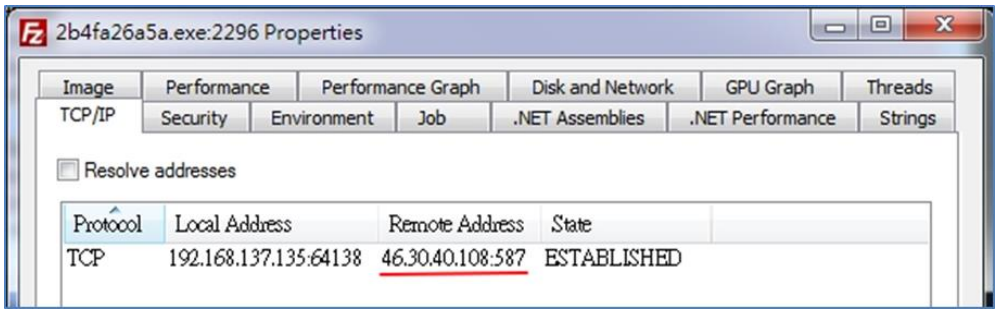


Process	Description	Image Path	Life Time	Company	Start Time	End Time
2b4fa26a5a.exe (3120)	Binance	C:\Users\Ruby\Downloads\2b4fa26a5a.exe		BinanceTech	2022/2/10 上午 09:49:22	2022/2/10 上午 09:50:05
2b4fa26a5a.exe (2296)	Binance	C:\Users\Ruby\Downloads\2b4fa26a5a.exe		BinanceTech	2022/2/10 上午 09:50:05	n/a

4. 2b4fa26a5a.exe 經 Virustotal 檢測其惡意比例為 49/70。它是 2022/2 初首次被上傳至 Virustotal 檢測，為非常新的樣本。

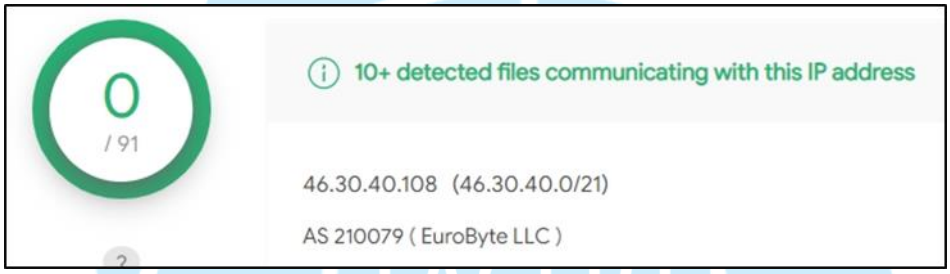


5. 2b4fa26a5a.exe 執行後約 10 分鐘會連線俄羅斯 IP:46.30.40.108:587，之後約每隔 10 分鐘會定時連線該俄羅斯 IP。它使用 587port (SMTP 傳送的預設 Port) 來進行 SMTP 協定的傳輸。



2022/2/10 上午 10:00:35 Added	2b4fa26a5a.exe	TCP 192.168.137.135:64100 46.30.40.108:587
2022/2/10 上午 10:01:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:64138 46.30.40.108:587
2022/2/10 上午 10:10:33 Added	2b4fa26a5a.exe	TCP 192.168.137.135:56064 46.30.40.108:587
2022/2/10 上午 10:11:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:56138 46.30.40.108:587
2022/2/10 上午 10:20:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:56179 46.30.40.108:587
2022/2/10 上午 10:30:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:56180 46.30.40.108:587
2022/2/10 上午 10:40:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:56181 46.30.40.108:587
2022/2/10 上午 10:50:35 Added	2b4fa26a5a.exe	TCP 192.168.137.135:56183 46.30.40.108:587
2022/2/10 上午 11:00:35 Added	2b4fa26a5a.exe	TCP 192.168.137.135:56200 46.30.40.108:587
2022/2/10 上午 11:01:36 Added	2b4fa26a5a.exe	TCP 192.168.137.135:50967 46.30.40.108:587
2022/2/10 上午 11:10:35 Added	2b4fa26a5a.exe	TCP 192.168.137.135:51385 46.30.40.108:587
2022/2/10 上午 11:11:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:61503 46.30.40.108:587
2022/2/10 上午 11:20:33 Added	2b4fa26a5a.exe	TCP 192.168.137.135:61591 46.30.40.108:587
2022/2/10 上午 11:21:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:61593 46.30.40.108:587
2022/2/10 上午 11:30:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:61595 46.30.40.108:587
2022/2/10 上午 11:40:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:61599 46.30.40.108:587
2022/2/10 上午 11:50:34 Added	2b4fa26a5a.exe	TCP 192.168.137.135:61602 46.30.40.108:587

6. 該俄羅斯 IP:46.30.40.108 經 Virustotal 判定為「非惡意 IP」。

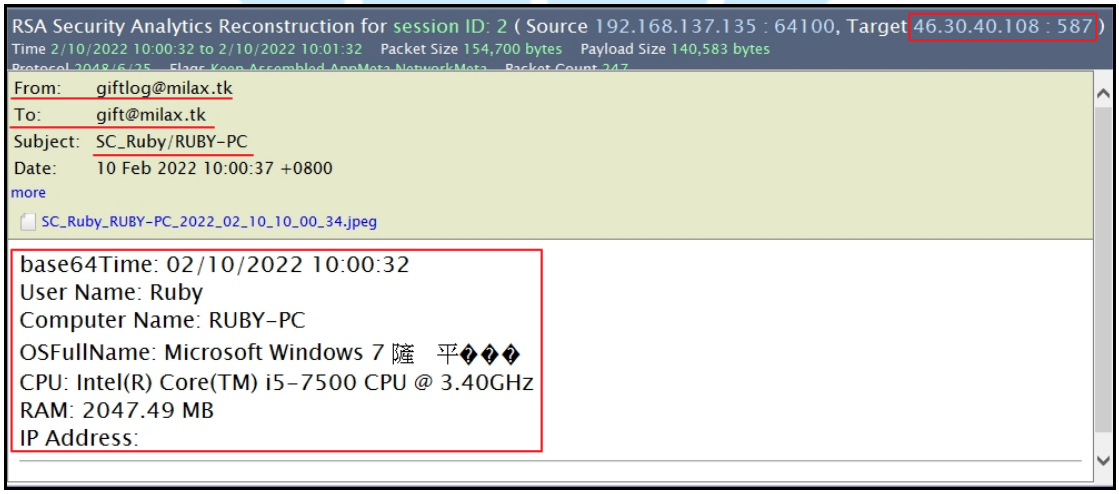


7. 檢視主機連線俄羅斯 IP 之封包，發現主機以信件方式傳送主機資訊給該 IP。

(1) 寄件者:giftlog@milax.tk、收件者 gift@milax.tk。

(2) 由「主旨:SC_Ruby/RUBY-PC」可看到使用者帳號與主機名稱。

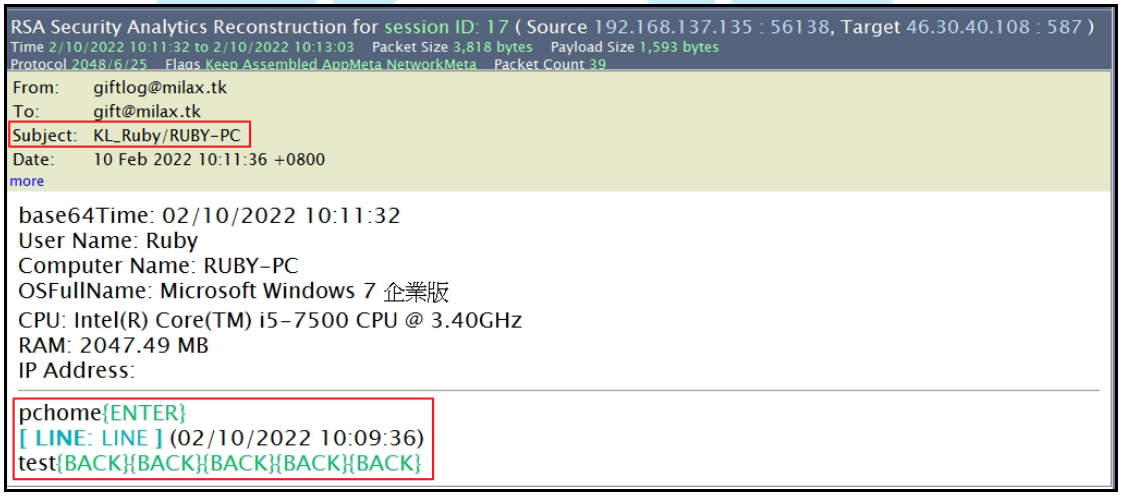
(3) 傳送內容包含使用者帳號、主機名稱、作業系統、CPU 與 RAM 資訊。



除了傳送主機資訊外，也傳送使用者於主機上所輸入與複製的內容，具有

Keylogger 功能。由下圖所傳送內容可得知使用者曾經複製一個網址，開啟 LINE 軟體輸入 gasdf1290，之後曾在瀏覽器頁面上輸入 msn 進行搜尋。其中輸入 LINE 之動作部分，在檢測當下檢測者開啟 LINE，而帳號輸入部分因系統已記錄，故僅輸入登入 LINE 之密碼 gasdf1290。若系統沒有記錄而輸入帳號，則登入 LINE 之帳號與密碼已被駭客取得。

從下圖中發現使用者曾經輸入 pchome，並且開啟過 LINE 軟體輸入 test 後又按倒退鍵。



由下圖可得知，使用者在瀏覽器頁面上輸入 pchome 後又輸入 msn，之後開啟 MSN 帳戶登入頁面。

RSA Security Analytics Reconstruction for session ID: 1317 (Source 192.168.137.135 : 50967, Target 46.30.40.108 : 587)
Time 2/10/2022 11:01:32 to 2/10/2022 11:03:05 Packet Size 3,896 bytes Payload Size 1,671 bytes
Protocol 2048/6/25 Flags Keep Assembled AppMeta NetworkMeta Packet Count 39

From: giftlog@milax.tk
To: gift@milax.tk
Subject: KL_Ruby/RUBY-PC
Date: 10 Feb 2022 11:01:36 +0800
more

base64Time: 02/10/2022 11:01:32
User Name: Ruby
Computer Name: RUBY-PC
OSFullName: Microsoft Windows 7 企業版
CPU: Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz
RAM: 2047.49 MB
IP Address:

[Google Chrome: 新分頁 - Google Chr] (02/10/2022 10:54:09)
pchome{ENTER}
msn{ENTER}
[Google Chrome: 登入您的 Microsoft 帳戶 - Google] (02/10/2022 11:01:21)

在下圖中可得知，使用者開啟 LINE 後點擊倒退鍵多次。

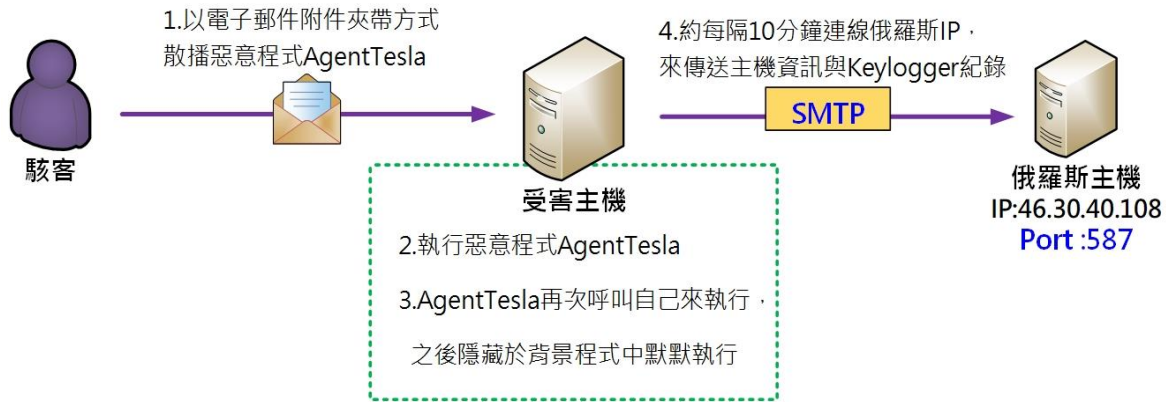
RSA Security Analytics Reconstruction for session ID: 1345 (Source 192.168.137.135 : 61593, Target 46.30.40.108 : 587)
Time 2/10/2022 11:21:31 to 2/10/2022 11:23:06 Packet Size 4,296 bytes Payload Size 2,071 bytes
Protocol 2048/6/25 Flags Keep Assembled AppMeta NetworkMeta Packet Count 39

From: giftlog@milax.tk
To: gift@milax.tk
Subject: KL_Ruby/RUBY-PC
Date: 10 Feb 2022 11:21:36 +0800
more

base64Time: 02/10/2022 11:21:32
User Name: Ruby
Computer Name: RUBY-PC
OSFullName: Microsoft Windows 7 企業版
CPU: Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz
RAM: 2047.49 MB
IP Address:

[LINE: LINE] (02/10/2022 11:19:19)
{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}{BACK}

三、攻擊行為示意圖



1. 以電子郵件附件夾帶方式散播惡意程式 Agent Tesla。

2. 在受害主機上執行惡意程式 Agent Tesla。
3. 執行後 Agent Tesla 會再次呼叫自己來執行，之後則隱藏自己於背景程式中默默執行。
4. 受害主機約每隔 10 分鐘以 SMTP 協定連線俄羅斯 IP，來傳送主機資訊與 Keylogger 紀錄。

四、總結與建議

1. Agent Tesla 是一個資訊竊取木馬(info stealer RAT)，它可通過記錄擊鍵和使用者輸入內容來收集有關受害者行為的資訊，使攻擊者能夠查看在運行中程式和 Web 瀏覽器內所輸入的所有內容。
2. 它在出售此惡意軟體的專用網站上被錯誤地宣傳為合法軟體。網站錯誤地聲稱該程式是為個人使用而建立的合法鍵盤記錄程式，因此 Agent Tesla 惡意軟體在駭客社群中變得非常流行。它會流行不僅是因為它的易用性和技術支援，而是它可以在攻擊者出售該惡意軟體之「官方」網站上獲得。
3. 它使用 SMTP 作為惡意軟體與控制伺服器連線的通訊協定。因為 SMTP 只能進行單向傳輸，而且只能傳送文字檔，無法傳送其他型態的檔案。又 SMTP 可輕易混在一般網路傳輸流量中，不容易被發現，而且使用簡單便利。
4. Agent Tesla 惡意軟體不容易被識別。 保持安全的最有效方法是在打開可疑電子郵件或訪問未知連結時保持謹慎。 最重要的是，必須小心下載來自未知送件人的電子郵件中之附件，並嘗試識別詐騙。