TLP:WHITE

竊密軟體 RedLine Stealer 分析報告

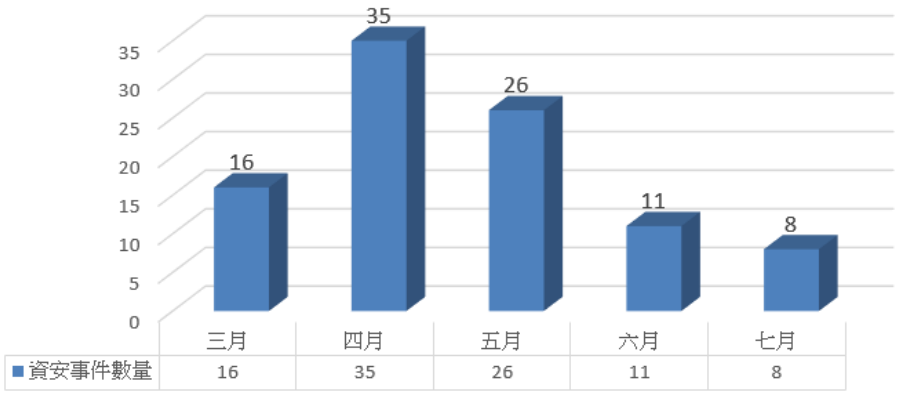
臺灣學術網路危機處理中心團隊(TACERT)製

2022 年 08 月

一、事件簡介

1. 在 2022/3~2022/7 期間學術網路發生 Redline 攻擊事件共有 96 件，其中在 2022/4 達攻擊高峰(有 35 件)，受攻擊對象以大專院校居多。

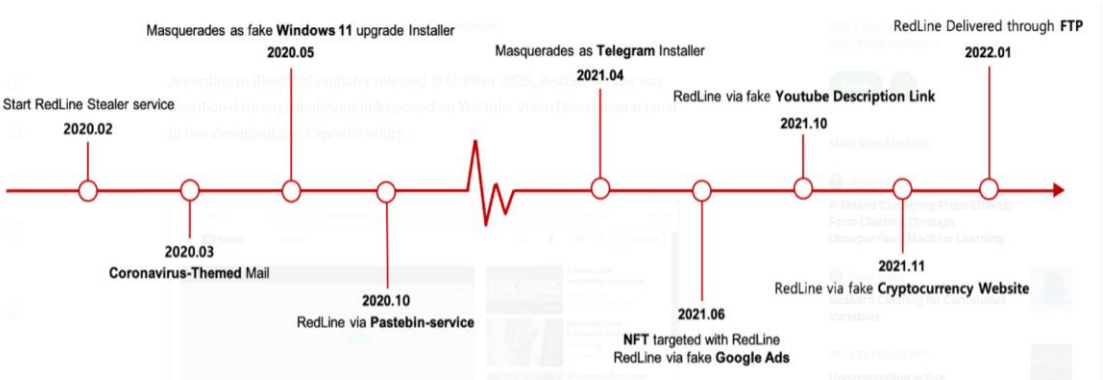
	資安事件數量
大專院校	66
高中職	8
國小	4
國中	5
縣市區網路中心	13
總計	96



2022/03~07期間每個月Redline攻擊事件數量統計圖

2. RedLine Stealer 於 2020/2 首次被發現，它主要通過釣魚郵件或偽裝成安裝檔案的惡意軟體（如 Telegram、Discord 和破解軟體）進行散播。

3. 下圖為其散播方式歷程，近期它利用 YouTube Video Description 和 Google Ads 下載包含 Redline Stealer 的 Chrome 擴展程式的網路釣魚連結，或通過 FTP 執行 Redline Stealer 的 Python 腳本正在散播。



資料來源:

https://medium.com/s2wblog/deep-analysis-of-redline-stealer-leaked-credential-with-wcf-7b31901da904

4. 為了解 RedLine Stealer 的攻擊行為，故對其樣本進行檢測作業。

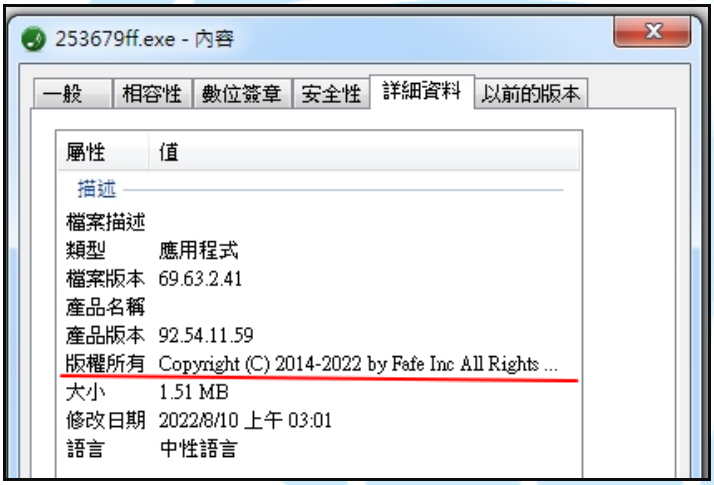
二、 事件檢測

1. 在 32 位元的 Windows7 作業系統上，分別執行兩個 Redline Stealer 樣本，來觀察它們的行為。

(1)樣本 1 為 59455ab.exe (MD5:2fda110a8763ef6d0d50d02c77d1de9c)

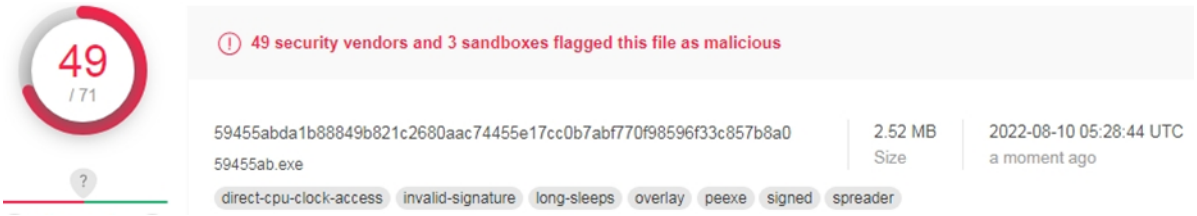
(2)樣本 2 為 253679ff.exe (MD5:189b13d2054550c98e1e248723c43475)

253679ff.exe 之內容與 59455ab.exe 不同，有檔案所屬版權資訊。



2. 兩樣本經 Virustotal 檢測其惡意比例如下。

59455ab.exe 之 Virustotal 檢測結果為 49/71。



253679ff.exe 之 Virustotal 檢測結果為 55/71。

3. 兩個樣本執行後之程式運作與連線行為如下。

(1) 樣本 1

59455ab.exe 執行後會呼叫 AppLaunch.exe 來執行。

Process	Command	Start Time	End Time
59455ab.exe (5704)	"C:\Users\Ruby\Downloads\59455ab.exe"	2022/8/10 下午 01:38:08	2022/8/10 下午 01:38:12
AppLaunch.exe (187764)	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"	2022/8/10 下午 01:38:12	n/a

AppLaunch.exe 執行後會連線俄羅斯 IP:185.186.142.127。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State	Added On
AppLaunch.exe	187764	TCP	54736	192.168.137.147	17355	185.186.142.127	Syn-Sent	2022/8/10 下午 01:40:20

由連線紀錄發現約每隔 20 秒會連線一次。

```
2022/8/10 下午 01:40:20 Added          AppLaunch.exe     TCP 192.168.137.147:54736  185.186.142.127:17355
2022/8/10 下午 01:40:20 Removed        AppLaunch.exe     TCP 192.168.137.147:54735  185.186.142.127:17355
2022/8/10 下午 01:40:40 Added          AppLaunch.exe     TCP 192.168.137.147:54737  185.186.142.127:17355
2022/8/10 下午 01:40:40 Removed        AppLaunch.exe     TCP 192.168.137.147:54736  185.186.142.127:17355
2022/8/10 下午 01:41:01 Added          AppLaunch.exe     TCP 192.168.137.147:54740  185.186.142.127:17355
2022/8/10 下午 01:41:01 Removed        AppLaunch.exe     TCP 192.168.137.147:54737  185.186.142.127:17355
2022/8/10 下午 01:41:23 Added          AppLaunch.exe     TCP 192.168.137.147:54742  185.186.142.127:17355
2022/8/10 下午 01:41:23 Removed        AppLaunch.exe     TCP 192.168.137.147:54740  185.186.142.127:17355
2022/8/10 下午 01:41:43 Added          AppLaunch.exe     TCP 192.168.137.147:54743  185.186.142.127:17355
2022/8/10 下午 01:41:43 Removed        AppLaunch.exe     TCP 192.168.137.147:54742  185.186.142.127:17355
```

(2) 樣本 2

253679ff.exe 執行後會呼叫 InstallUtil.exe 來執行。

Process	Command	Start Time	End Time
253679ff.exe (3128)	"C:\Users\Ruby\Downloads\253679ff.exe"	2022/8/10 下午 03:08:47	2022/8/10 下午 03:08:54
InstallUtil.exe (2156)	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"	2022/8/10 下午 03:08:54	n/a

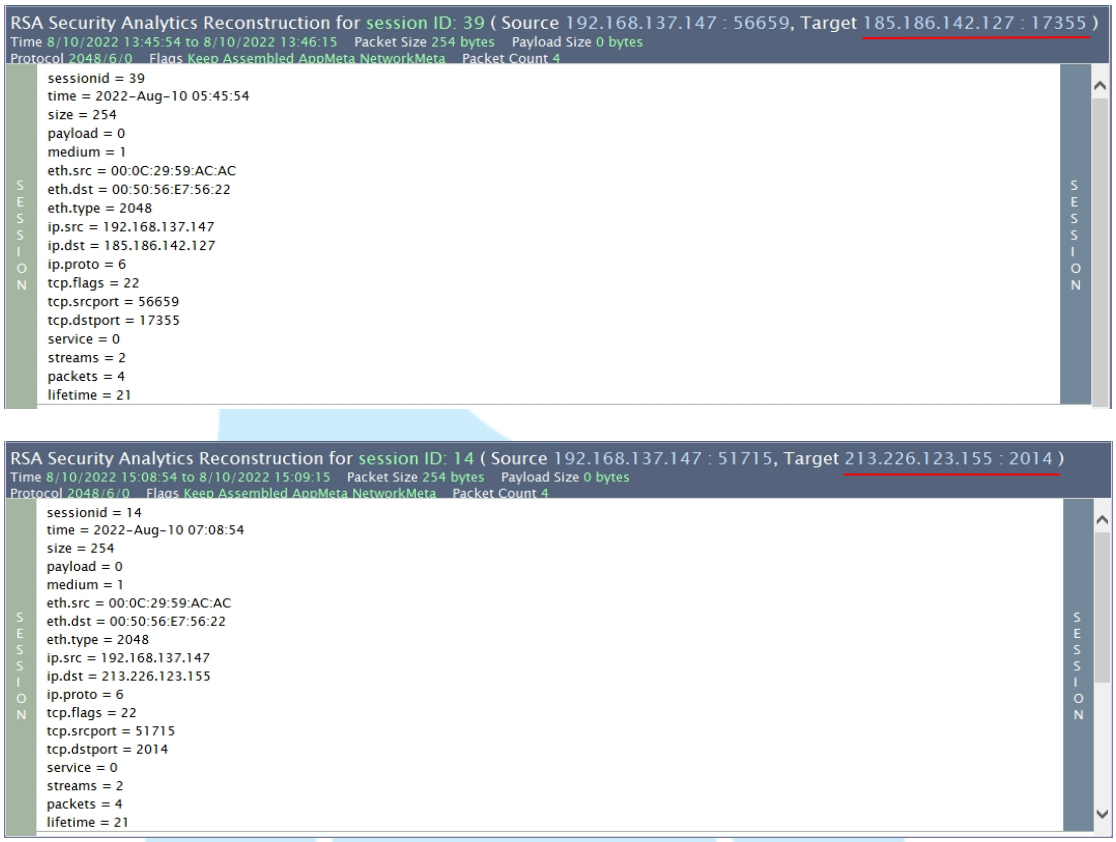
InstallUtil.exe 執行後會連線俄羅斯 IP:213.226.123.155。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State	Added On
InstallUtil.exe	2156	TCP	51723	192.168.137.147	2014	213.226.123.155	Syn-Sent	2022/8/10 下午 03:12:23

由連線紀錄發現約每隔 20 秒會連線一次。

```
2022/8/10 下午 03:08:56 Added          InstallUtil.exe   TCP 192.168.137.147:51715  213.226.123.155:2014
2022/8/10 下午 03:09:17 Removed        InstallUtil.exe   TCP 192.168.137.147:51715  213.226.123.155:2014
2022/8/10 下午 03:09:21 Added          InstallUtil.exe   TCP 192.168.137.147:51716  213.226.123.155:2014
2022/8/10 下午 03:09:43 Removed        InstallUtil.exe   TCP 192.168.137.147:51716  213.226.123.155:2014
2022/8/10 下午 03:09:47 Added          InstallUtil.exe   TCP 192.168.137.147:51717  213.226.123.155:2014
2022/8/10 下午 03:10:09 Removed        InstallUtil.exe   TCP 192.168.137.147:51717  213.226.123.155:2014
2022/8/10 下午 03:10:13 Added          InstallUtil.exe   TCP 192.168.137.147:51718  213.226.123.155:2014
2022/8/10 下午 03:10:34 Removed        InstallUtil.exe   TCP 192.168.137.147:51718  213.226.123.155:2014
2022/8/10 下午 03:10:40 Added          InstallUtil.exe   TCP 192.168.137.147:51719  213.226.123.155:2014
2022/8/10 下午 03:11:00 Removed        InstallUtil.exe   TCP 192.168.137.147:51719  213.226.123.155:2014
2022/8/10 下午 03:11:06 Added          InstallUtil.exe   TCP 192.168.137.147:51720  213.226.123.155:2014
2022/8/10 下午 03:11:26 Removed        InstallUtil.exe   TCP 192.168.137.147:51720  213.226.123.155:2014
```

4. 分析兩個樣本所連線的俄羅斯 IP 封包，發現檢測時未傳輸任何內容，僅單獨建立連線。



三、 攻擊行為

1. 駭客通過社交工程攻擊散播 Redline stealer。
2. 在受害主機上執行 Redline stealer 程式來呼叫其他程式進行連線，例如:樣本 1

呼叫 AppLaunch.exe，樣本 2 呼叫 InstallUtil.exe。

3. 受害主機約每 20 秒連線一次俄羅斯 IP。

四、 總結與建議

1. Redline Stealer 是學術網路中常見的惡意程式，也是惡意程式檢測網站 ANYRUN 每週上傳程式樣本數量之前五名之一。
2. 它可從瀏覽器、系統和安裝的軟體中收集使用者的機密資料，收集的資訊包括系統資訊、瀏覽器憑證、加密錢包資訊、FTP 資訊、Telegram 和 Discord 資訊等。在收集和洩露資訊後，Redline Stealer 還具有下載可執行檔案和執行附加惡意行為的能力。
3. 本次檢測兩個樣本發現其會每隔 20 秒持續連線俄羅斯 IP，保持對受害主機的連線。
4. 在處理此類型攻擊事件時，受害主機可透過掃毒、檢視連線行為與背景程式，來查找惡意程式所在之處，以利移除它。