

TLP:WHITE

勒索病毒 Stop 分析報告



臺灣學術網路危機處理中心團隊(TACERT)製

2021 年 07 月

一、事件簡介

1. 2021/6 中旬某學校一台主機感染勒索病毒，因有掛載 NAS 資料夾為網路磁碟機，導致 NAS 共用資料夾內檔案被加密。
2. 從被加密檔案的修改時間發現檔案被加密時間點在 2021/6/18 下午 12:21，而且被加密檔案之副檔名皆為 sspq。
3. 經 TACERT 檢測判定該校主機感染勒索病毒的種類為 STOP 勒索軟體家族 2021 年新變種 sspq 病毒。
4. STOP 的變種病毒 Sspq 是一種由提供下載種子、破解遊戲、免費軟體、密鑰生成器、激活器等網站散播的惡意軟體。
5. 根據 EMSISOFT 公司的 2021 年第一季最常被通報的勒索軟體之數據統計，可看到 STOP/Djvu 的勒索軟體家族位居第一，是迄今為止最常見的病毒，佔所有通報數據的 51.4%。

Top 10 most commonly reported ransomware strains of Q1 2021 (STOP included)

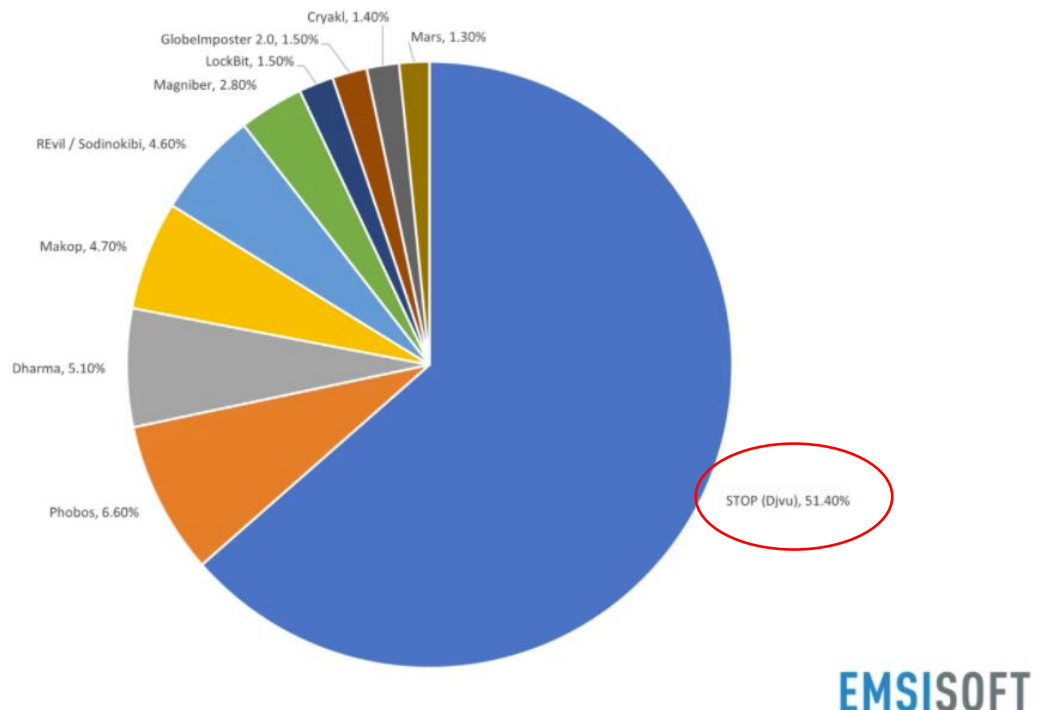
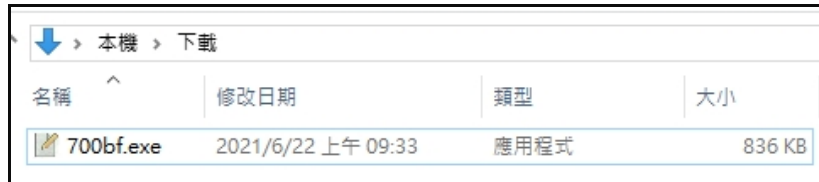


圖 1 2021 年第一季最常被通報的 10 種勒索軟體(包含 STOP 勒索軟體)

資料來源:EMSISOFT 公司

二、事件檢測

1. 首先，在 64 位元的 Windows 10 作業系統上，執行 STOP 樣本 700bf.exe (MD5: 5986e0b21fb07b57e8841601154e5110)，而 700bf.exe 在主機重新開機後會被加密(副檔名會變成 sspq)。



名稱	修改日期	類型	大小
700bf.exe	2021/6/22 上午 09:33	應用程式	836 KB



名稱	修改日期	類型	大小
700bf.exe.sspq	2021/6/23 下午 02:50	SSPQ 檔案	836 KB

2. 在 700bf.exe 執行後會在「%AppDataLocal%」建立兩個子資料夾，並產生 700bf.exe 副本。一個放副本，另一個放下載的檔案。



名稱	建立日期	修改日期	類型
8aff4d3a-e594-41b6-88cf-027ce1475a59	2021/6/23 下午 02:45	2021/6/23 下午 02:50	檔案資料夾
399d6c7a-35d4-4129-ad72-f73b2ffab0a1	2021/6/23 下午 02:45	2021/6/23 下午 02:45	檔案資料夾



名稱	修改日期	建立日期	類型	大小
700bf.exe	2021/6/22 上午 09:33	2021/6/23 下午 02:45	應用程式	836 KB

(註 1: 「%AppDataLocal%」是指本地應用程式資料夾，在 Windows Vista, 7, 8, 8.1, 2008(64-bit), 2012(64-bit) and 10(64-bit)系統上則是指 C:\Users\{user name}\AppData\Local 。

本案的惡意軟體還具有 downloader 的功能，若成功連線命令和控制伺服器(C&C)，則 C&C 會回傳加密密鑰(在線密鑰 Online ID) 以及必須在受害者主機上執行的其他命令和惡意軟體。此時這些東西就會放在下載檔案的資料夾中。另外，它添加了互斥體以確保在任何時候只有一個資料夾的惡意程式執行。在檢測時，C&C 並沒有回應受害主機，故放下載檔案的資

料夾是空的。)

3. 檢視背景程式碼發現:

(1) 700bf.exe 會呼叫 icaccls.exe 來授予惡意軟體建立資料夾的訪問權限。

使用指令:

```
icaccls "%AppDataLocal%\{GUID}" /deny *S-1-1-0:(OI)(CI)(DE,DC)
```

(2) 700bf.exe 會以管理員身份執行，而不是透過自動啟動或任務啟動它的程序。

```
"{Executed Malware File Path}\700bf.exe"--Admin IsNotAutoStart
```

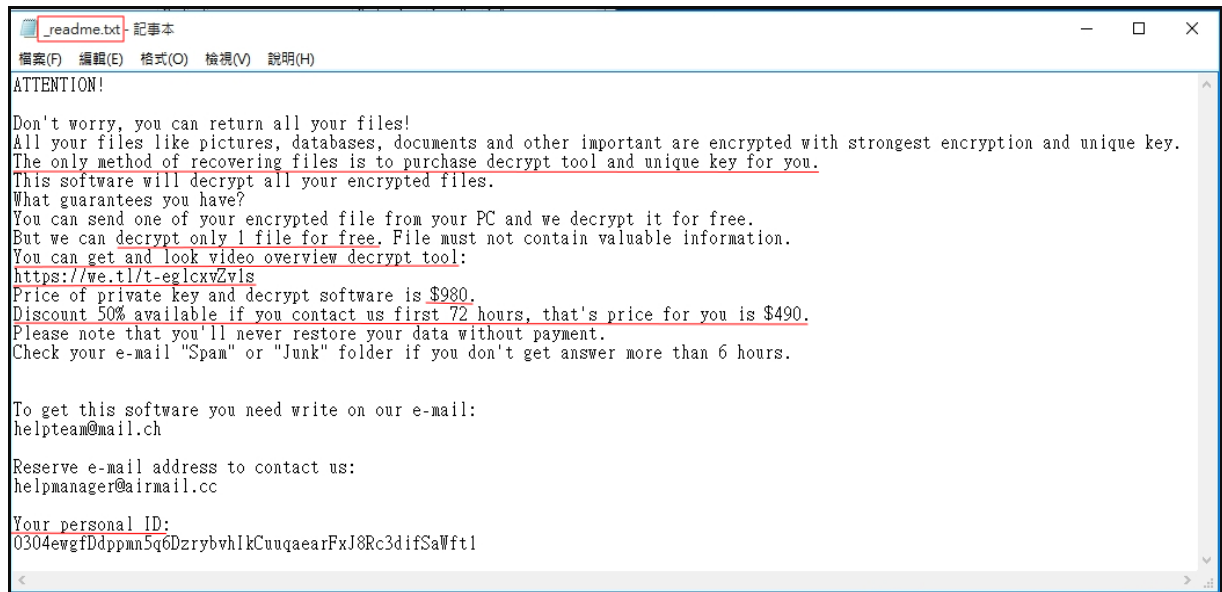
```
IsNotTask
```

Process	Command
700bf.exe (5420)	"C:\Users\AMY\Downloads\700bf.exe"
700bf.exe (4920)	"C:\Users\AMY\Downloads\700bf.exe"
icaccls.exe (964)	icaccls "C:\Users\AMY\AppData\Local\8aff4d3a-e594-41b6-88cf-027ce1475a59" /deny *S-1-1-0:(OI)(CI)(DE,DC)
700bf.exe (5804)	"C:\Users\AMY\Downloads\700bf.exe" --Admin IsNotAutoStart IsNotTask
700bf.exe (6064)	"C:\Users\AMY\Downloads\700bf.exe" --Admin IsNotAutoStart IsNotTask

(註:icaccls.exe 為系統檔，來自 C:\Windows\SysWOW64\icaccls.exe。)

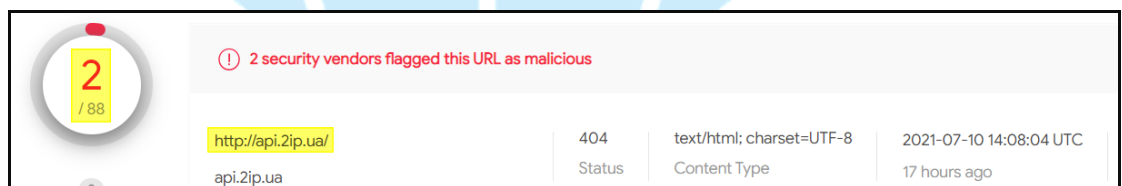
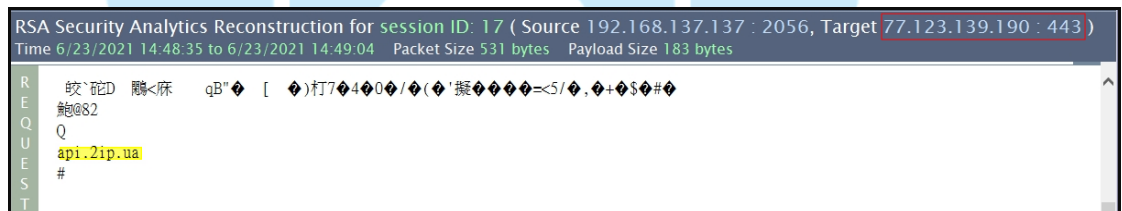
4. 勒索通知信_readme.txt 告訴受害者:

- (1) 只有購買解密器與唯一金鑰才能解開被加密的檔案，可以免費解密 1 個檔案。
- (2) 購買私鑰與解密軟體需要 980 美元，如果在 72 小時內聯絡他們只要半價 490 元。
- (3) 駭客隨信提供查看解密器的影片網址、E-mail 聯絡信箱與 Personal ID 等資訊。

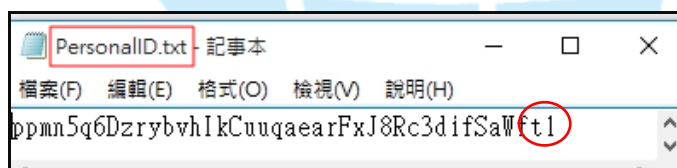
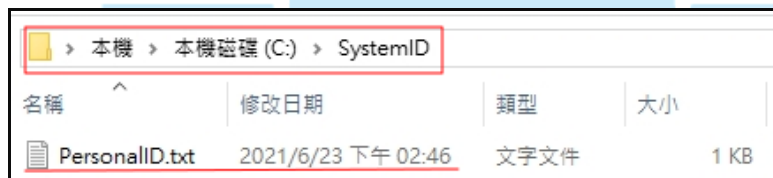


5. 在 700bf.exe 執行後發現會連線烏克蘭 IP:77.123.139.190:443(疑似 C&C)。從所側錄的封包可看到該主機 REQUEST 內容有網址 api.2ip.ua，但烏克蘭 IP 卻沒有回傳任何內容。該網址經 Virustotal 檢測判定其惡意比例為 2/88，有兩家資安公司認為其為惡意網址。

2021/6/23 下午 02:48:33	Added	svchost.exe	TCP	192.168.137.137:2055	8.241.177.126:80
2021/6/23 下午 02:48:33	Removed	svchost.exe	TCP	192.168.137.137:2053	8.241.177.126:80
2021/6/23 下午 02:48:37	Added	700bf.exe	TCP	192.168.137.137:2056	77.123.139.190:443
2021/6/23 下午 02:48:37	Added	svchost.exe	TCP	192.168.137.137:2057	8.255.192.126:80



6. 在 C:\發現除了新增_readme.txt 外，還產生 SystemID 資料夾，內存放 PersonalID.txt。所有被加密的檔案其副檔名皆為 sspq，而被病毒訪問過的每個資料夾都會產生一個_readme.txt。除了 C:\Windows 與 C:\Program Files 內的檔案外，其餘檔案都會被加密。



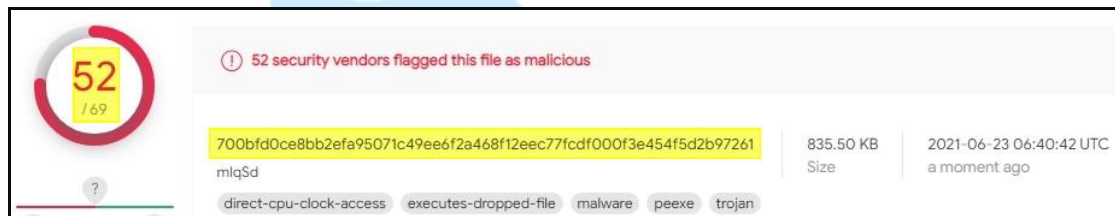
(註 2:由於 Sspq 檔案解密工具只對使用離線密鑰加密的檔案進行解密，因此每個勒索軟體受害者都需要找出用於加密檔案的密鑰。「個人 ID (PersonID)」不是密鑰，它是與用於加密檔案的密鑰相關的識別碼。如果 ID 以「t1」結尾，則檔案使用離線密鑰加密。如果 ID 不以「t1」結尾，則 Sspq 勒索軟體使用了在線密鑰。)

7. 檢視主機重新開機後會自動啟動的程式，發現在登錄檔

「HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run」內被新增「SysHelper」。它會在主機每次開機後自動執行「%AppDataLocal%\{GUID}」內存放的 700bf.exe 副本。

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021/6/23 下午 02:45
<input checked="" type="checkbox"/> SysHelper			c:\users\amy\AppDataLocal\8aff4d3a-e594-41b6-88cf-027ce1475a59\700bf.exe	2020/4/24 上午 10:45

8. 700bf.exe 經 Virustotal 檢測其惡意比例為 52/69。



9. 被加密檔案與_readme.txt 經 ID Ransomware 勒索軟體識別網站檢測為 STOP 勒索軟體，而且可能解密。

STOP (Djvu)

⚠ This ransomware **may be decryptable** under certain circumstances.

Please refer to the appropriate guide for more information.

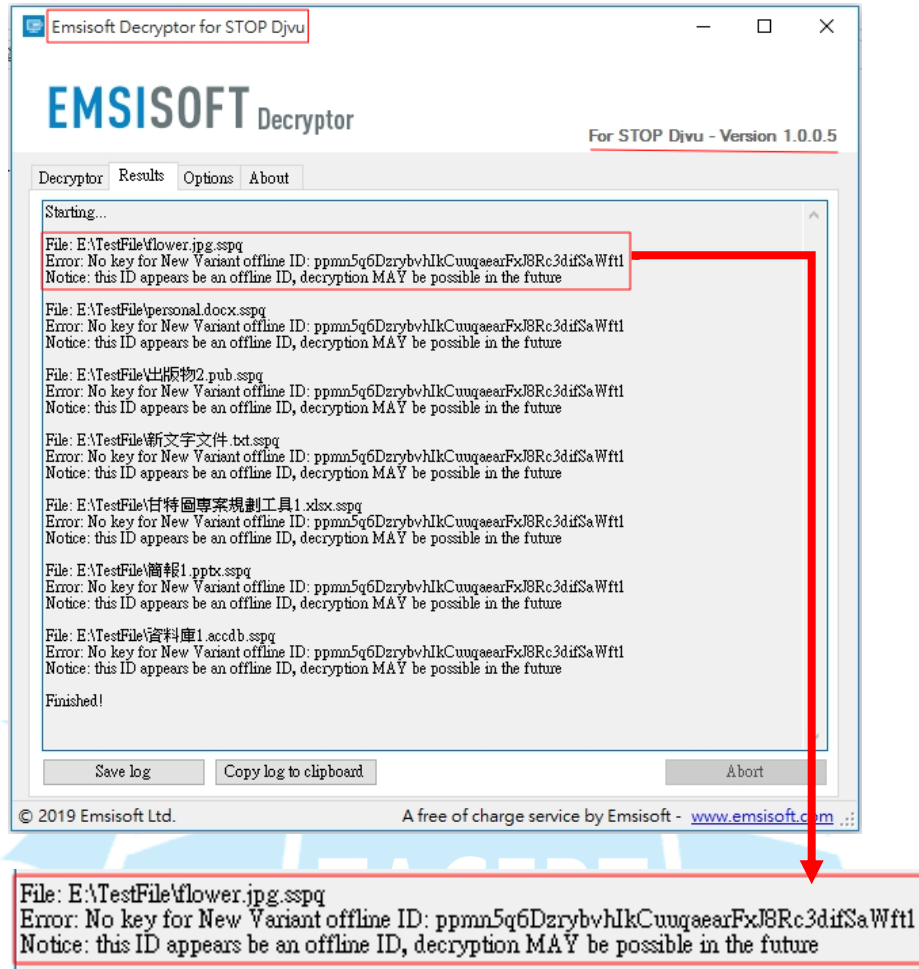
Identified by

- ransomnote_filename: _readme.txt
- ransomnote_email: helpmanager@airmail.cc
- sample_extension: .sspq
- sample_bytes: [0x396A - 0x3990]

0x7B33364136393842392D443637432D344530372D424538322D3045433542313442344446357D

[Click here for more information about STOP \(Djvu\)](#)

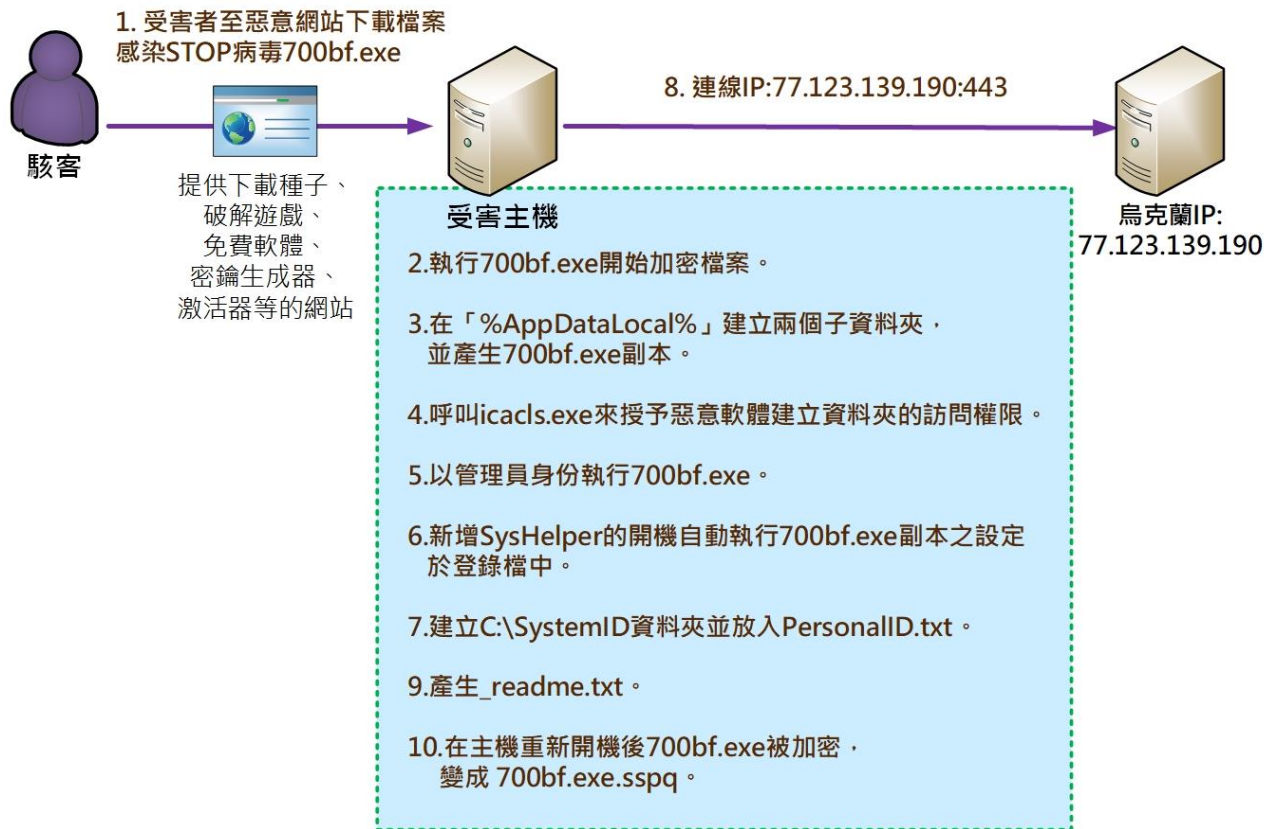
10. 使用 EMSISOFT 公司的 STOP 解密器進行解密，結果因為病毒為新變種無法解密，又因為 ID 為 offline ID，可能在未來可以解密。



(註 3: 1.本案的勒索病毒會收集有關受害者主機的信息，然後嘗試與其命令和控制伺服器 (C&C) 建立連線。如果連線已建立，則它會將有關受感染主機的信息發送到伺服器，而伺服器則會回傳加密密鑰（即所謂的「在線密鑰」Online ID）以及必須在受害者主機上執行的其他命令和惡意軟體。如果病毒無法與其命令和控制伺服器(C&C)建立連線，則它使用固定密鑰（即所謂的「離線密鑰」Offline ID）。本案由 EMSISOFT 解密器的解密結果可得知使用固定密鑰(Offline ID)。)

2. 若 Sspq 檔案使用解密工具解密檔案後出現「No key for New Variant online ID」，這意味著您的檔案是使用「在線密鑰」加密的，因此無法解密，因為只有 sspq 作者擁有解密所需的密鑰。)

三、攻擊行為示意圖



- 1.受害者至惡意網站下載檔案感染 STOP 病毒 700bf.exe
- 2.執行 700bf.exe 開始加密檔案。
- 3.在「%AppDataLocal%」建立兩個子資料夾並產生 700bf.exe 副本。
- 4.呼叫 icacls.exe 來授予惡意軟體建立資料夾的訪問權限。
- 5.以管理員身份執行 700bf.exe。
- 6.新增 SysHelper 的開機自動執行 700bf.exe 副本之設定於登錄檔中。
- 7.建立 C:\SystemID 資料夾並放入 PersonalID.txt。
- 8.連線 IP:77.123.139.190:443。(沒有取得烏克蘭 IP 的回應 Offline ID)
- 9.產生_readme.txt。
- 10.在主機重新開機後 700bf.exe 被加密，變成 700bf.exe.sspq。

四、總結與建議

1. STOP 勒索病毒可透過存有密鑰產生器與破解程序等工具的網站，讓瀏覽
者想免費激活付費軟體時下載這些工具，進而感染 STOP 病毒。
2. 當主機感染 STOP 病毒時，若有連線 NAS 設備的資料夾、USB 或外接硬
碟，則這些連線設備內的檔案將被加密。
3. STOP 病毒的副本會在每次主機開機時自動執行，若主機有存取新檔案，
則新檔案將會被加密。在處理主機時，需先將 STOP 病毒的副本優先移除
才行。
4. STOP 病毒會連線 C&C 伺服器，若連線成功，則取得加密金鑰(OnlineID)、
要執行的其他命令和惡意軟體。若連線無回應，則加密使用固定金鑰
(OfflineID)。(Online ID 無法解密，而 Offline ID 等待未來解密。)
5. 對於預防 STOP 勒索病毒方面，除了平時定期備份資料外，因 STOP 病毒
的散播方式來自惡意網站下載檔案造成，建議若有下載軟體需求時，需確
認下載來源的安全性。
6. 校園中發生 NAS 感染勒索病毒的事件頻繁。許多學校人員因為方便性，
習慣將 NAS 資料夾掛載於主機上使用，又有些學校會開放 NAS 讓校外 IP
存取，這些行為將使 NAS 存在資安風險。在 NAS 的管理上，建議限制存
取 NAS 的 IP(Ex:僅限校內 IP 存取)，以及定期備份 NAS 內資料。

五、相關參考資料

1.Ransomware statistics for 2021: Q1 report

<https://blog.emsisoft.com/en/38619/ransomware-statistics-for-2021-q1-report/>