

個案分析-

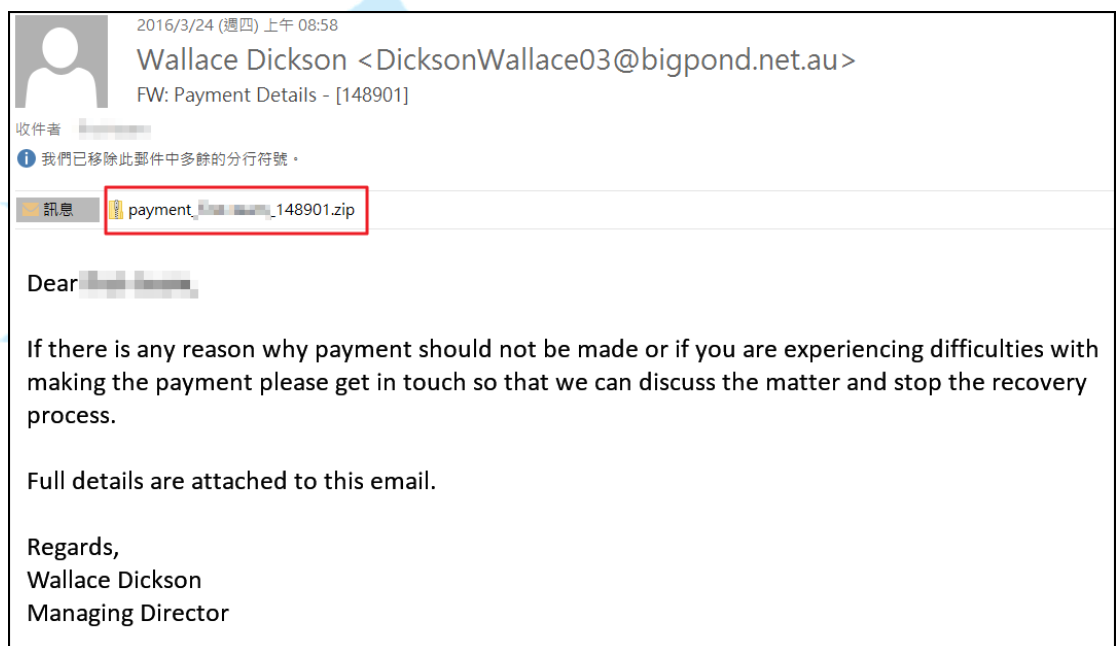
新型態的加密勒索惡意程式 分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/4

I. 事件簡介




1. 近年來惡意程式越來越多樣化，以往都只是感染主機成為中繼站或殭屍電腦，但另一種的惡意程式卻會破壞使用者的檔案資料，並且勒索使用者相當的金額，造成嚴重損害。
2. 近期內學術網路或相關組織信箱出現大量的 APT 社交工程郵件，透過向關議題進行誘騙開啟附加檔案。此例中的郵件主旨是要求檢查收款資訊，並夾帶 zip 的壓縮檔案。



3. 受害者往往必須向駭客以比特幣作為支付方式，贖回檔案的解密金鑰。
4. 本單位取得的惡意程式樣本進行研究分析，主要以 Locky 變種的惡意勒索軟體測試。

II. 事件檢測

1. 使用 VM 虛擬主機並且為 Windows 7(32 bit)系統進行隔離環境測試，若使用 64 位元系統則會測試失敗。
2. 惡意程式 zip 解壓縮之後會有三個附檔名為 js 的檔案，雖然並非常見的 exe 執行檔，js 事實上是用 javascript 撰寫的執行檔案。

 (scanned_doc) - 388526 - copy.js	2016/3/24 上午 0...	JScript 指令檔	11 KB
 (scanned_doc) - 388526.js	2016/3/24 上午 0...	JScript 指令檔	11 KB
 (wire) - e870d.js	2016/3/24 上午 0...	JScript 指令檔	10 KB

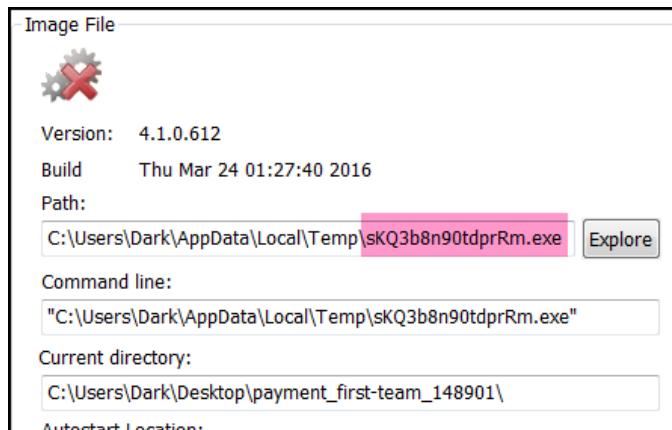
3. 透過 Virustotal 線上掃毒，該三個 JS 執行檔病毒的檢測比例 3/57，為新型態的加密勒索軟體，且偵測比例相當低。

SHA256: 9165b395fd52b9c8c0047c056d55a20702a3de04993a0bfce4be1d9b4a014d67
File name: %28scanned_doc%29+-+388526+-+copy.js
Detection ratio: 3 / 57
Analysis date: 2016-03-23 23:53:11 UTC (1 week, 1 day ago)

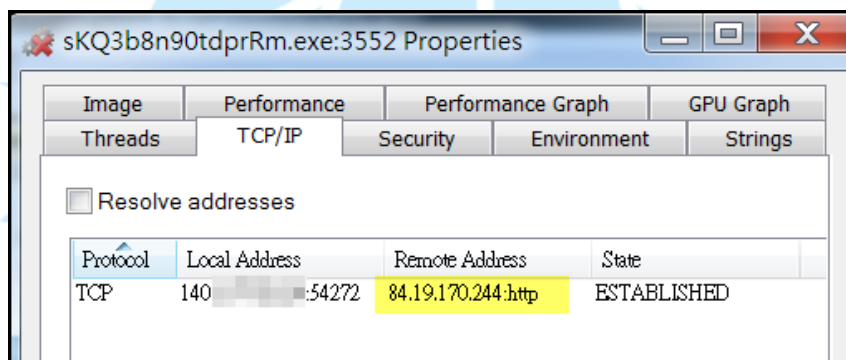
Analysis Relationships Additional information Comments 0 Votes

Antivirus	Result
Arcabit	HEUR.JS.Trojan.b
Fortinet	JS/Agent.GE!tr
Kaspersky	HEUR:Trojan-Downloader.Script.Generic

4. 首先執行 js 的檔案，系統會使用預設 javascript 程式去執行，執行後一段時間內系統會看不出任何異常現象，事實上惡意程式已經在背景執行中。
5. 透過 procexp 工具查看背景程式執行狀態，可以看到一隻位於隱藏路徑中 \AppData\Local\Temp\ 的 sKQ3b8n90tdprRm.exe 惡意程式正在執行，而該程式確實就是透過原本的 js 檔案產生的。



6. 惡意程式最主要的行為之一就是會有對外的網路連線產生，因此查看該程式 sKQ3b8n90tdprM.exe 的網路狀態可以發現，確實有正在對外部 84.19.170.244 的網路連線，該 IP 位址位於 RU 俄羅斯國家。












7. 使用 TCPview 查看所有網路連線狀態，也能觀察到該程式除了有對外 IP 建立連線，也會針對內部網段其他 IP 進行 scan 動作，判斷為找尋可存取的網路檔案進行檔案加密。

System	4	TCP	54294	140.140.140.139	netbios-ssn	140.140.140.139	ip:140.140.140.139	Sent
Unknown	0	TCP	54273	140.140.140.139	netbios-ssn	140.140.140.139	ip:140.140.140.139	Time W...
Unknown	0	TCP	54276	140.140.140.139	netbios-ssn	140.140.140.139	ip:140.140.140.139	Time W...
Unknown	0	TCP	54274	140.140.140.139	netbios-ssn	140.140.140.139	ip:140.140.140.139	Time W...
Unknown	0	TCP	54275	140.140.140.139	netbios-ssn	140.140.140.139	ip:140.140.140.139	Time W...
Unknown	0	TCP	54278	140.140.140.139	netbios-ssn	140.140.140.139	ip:140.140.140.139	Time W...

8. 當所有磁碟內部或外部的關聯檔案都被加密後，在桌面會跳出一個圖片檔「_HELP_instructions.bmp」以及一個「_HELP_instructions.txt」說明檔，主要內容是引導受害者如何進行繳付勒索贖金，此時發現所有可開啟文件都已經無法開啟。



9. 此時隨意開啟資料夾查看原有文件檔，發現所有文件檔的確都被置換檔案名稱以及副檔名為 locky，並附上一個贖金引導的 txt 說明檔，其內容同於黑底紅字的圖片內容。

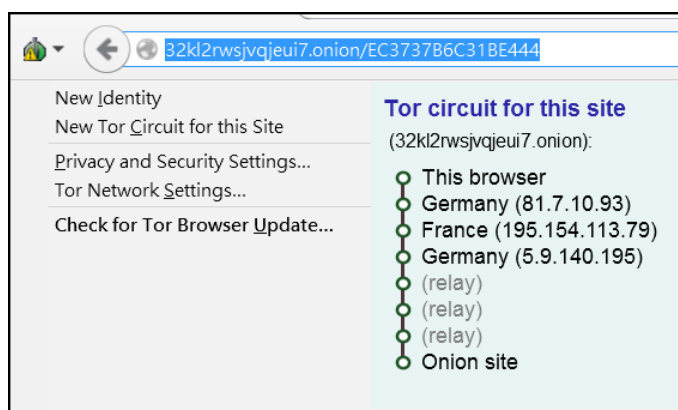
 _HELP_instructions.txt	2016/3/30 下午 02:56
 EC3737B6C31BE444BED67029F4884F7A.locky	2016/3/30 下午 02:56
 EC3737B6C31BE444CD206A176889B5EB.locky	2016/3/30 下午 02:57
 EC3737B6C31BE444F7C442B89722639A.locky	2016/3/30 下午 02:57
 EC3737B6C31BE444F952C4A33A360B17.locky	2016/3/30 下午 02:56
 EC3737B6C31BE4443B3EB9A4DB9E7C5A.locky	2016/3/30 下午 02:57
 EC3737B6C31BE44407A2FB9D1DBA3FF1.locky	2016/3/30 下午 02:57
 EC3737B6C31BE44461AC55A396E63116.locky	2016/3/30 下午 02:57
 EC3737B6C31BE4449845F47BF69639B8.locky	2016/3/30 下午 02:56

10. 根據引導說明檔的內容操作，勒索的網址必須透過 Tor 的匿名網路瀏覽器去開啟，無法使用一般 DNS 解析出正常 IP，而這是駭客很常用來規避 IP 追蹤的方法之一。

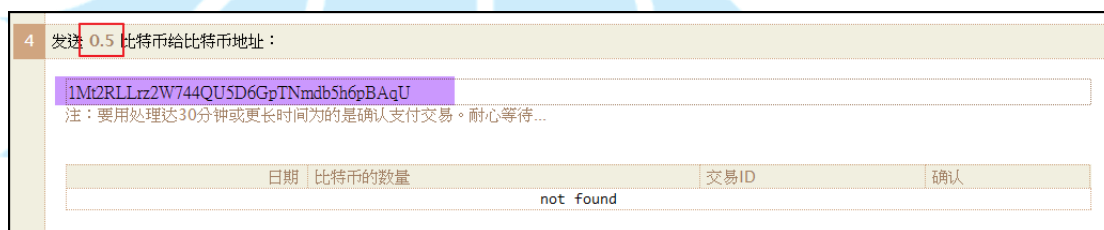
只有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。
如要接收您的私人金鑰，請點擊以下其中一個連結：

1. <http://32kl2rwsjvqjeui7.tor2web.org/EC3737B6C31BE444>
2. <http://32kl2rwsjvqjeui7.onion.to/EC3737B6C31BE444>
3. <http://32kl2rwsjvqjeui7.onion.cab/EC3737B6C31BE444>

11. 此例開啟特殊 onion 網域位址後看到至少經過三次的 Relay IP，才轉跳至未知的目的地 onion site。



12. 透過 Tor 瀏覽器成功開啟網址後，出現的是簡體中文的 Locky Decryptor 網頁，意思是受害者必須向該網站購買解密的金鑰程式，才能還原被加密過的檔案，並且必須透過以比特幣作為支付方式，將 0.5 BTC 付款至指定位址，大約是 7000 台幣。



13. 駭客為了希望能夠勒索到比特幣，還特地提供一些網站，引導教學受害者如何購買取得比特幣，根據受害者所在國家不同也有不同的取得方式。

Locky Decryptor™

我們將推出 **Locky Decryptor™** 專門的軟件。
它可以讓您解碼和監控所有的加密文件。

如何購買 Locky Decryptor™?

您可以使用比特幣付款，您可以使用各種方法來得到它們。

您必須註冊比特幣錢包：

[最簡單的方法是網上錢包](#) 或 [其他方式來創建一個錢包](#)。

儘管購買比特幣仍然只是不容易，在日常生活購買比特幣變得更加容易。

我們的建議：

localbitcoins.com (WU)	使用Western Union(西聯匯款)來購買比特幣。
coincafe.com	推薦用於快速和簡單維修的方便。
	付款方式：Western Union, Bank of America通過FedEx(聯邦快遞)獲得現金匯款。在紐約：比特幣ATM，
	親自。
localbitcoins.com	該服務允許您在您的社區找人誰願意直接賣給您比特幣。
cex.io	使用VISA/MASTERCARD/万事達卡或銀行轉帳來購買比特幣。
btcdirect.eu	對於歐洲最好的網站。
bitquick.co	用現金來即時購買比特幣。
howtobuybitcoins.info	國際比特幣兌換文件目錄。
cshintocoin.com	用現金來購買比特幣
coinjar.com	在CoinJar網站可以直接購買比特幣。
anxpro.com	
bittylicious.com	

14. 此變化型的加密勒索病毒不同於以往的案例，它不會要求必須在多久時間內交付贖金，否則將會將贖金漲價或者銷毀金鑰，只是很單純的等待受害者交付贖金。網站表示一旦收到贖金後，將會轉跳至下載解碼軟件的頁面，然而此例並無真實測試過。

使重新頁並下載解碼軟件。

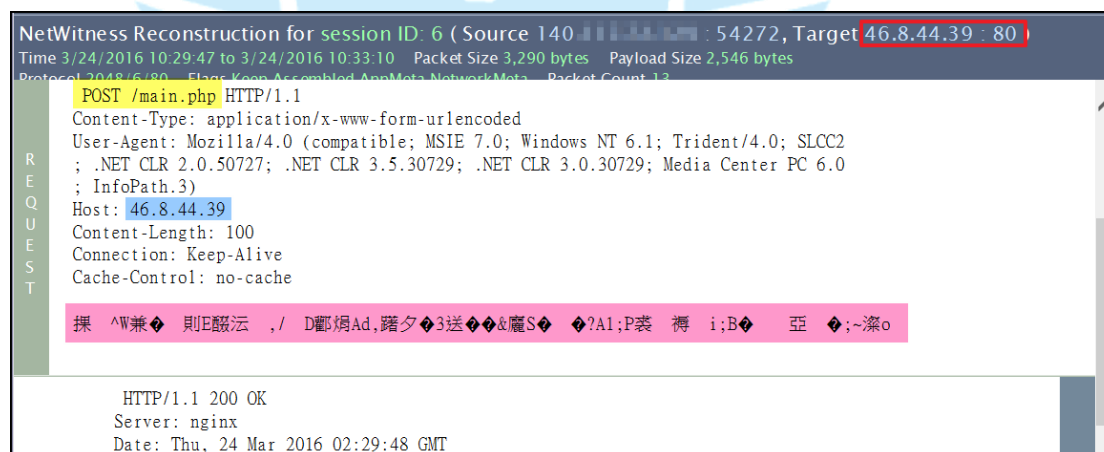
接收確認比特幣交易後，您會被重定向到下載解碼軟件的頁。

15. 因為比特幣的錢包地址具有完整的匿名性及不可被否認性，一旦支付出去就無法追討回來，也無法知道帳號擁有者身分，所以現在很多犯罪組織喜歡用比特幣作為交易工具。
16. 在所有檔案都被加密後，原本的惡意程式 js 檔案和 skQ3b8n90tdprRm.exe 檔案也都會自我移除不留痕跡，透過 Virustotal

掃描 skQ3b8n90tdprM.exe 可以很清楚看到是高偵測比例 46/57 的勒索軟體，檢測名稱是 2.exe。

SHA256:	7a6cf27dda962107e9b439c25c95db92e13f3587985eea656185a49ed1f4a72f
File name:	2.exe
Detection ratio:	46 / 57
Analysis date:	2016-04-05 14:53:55 UTC (10 hours, 57 minutes ago)
Antivirus	Result
ALYac	Trojan.Ransom.LockyCrypt
AVG	Crypt5.ASCM
AVware	Trojan.Win32.Generic!BT
Ad-Aware	Trojan.GenericKD.3118559
AegisLab	Troj.Crypt.Zpack!c
AhnLab-V3	Win-Trojan/Lockycrypt.Gen

17. 從網路封包中可以看到，主機感染惡意程式一開始會連到烏克蘭的 C&C 主機「46.8.44.39」，並且透過 HTTP POST 方式將加密內容送出，判定可能是勒索加密的私鑰。



18. 當主機向上層 C&C 報到並送出私鑰後，惡意程式開始對內部網路進行 netbios 的掃描，並嘗試針對能夠存取的共享資料夾進行加密，若有連接網路磁碟或 NAS 就有可能遭受破壞。

Time	Service	Size	Events	Display
2016-Mar-24 10:29:55	IP / TCP SMB	2.10 KB	140. -> 140. 54278 -> 139 (netbios-ssn)	
2016-Mar-24 10:29:55	IP / TCP SMB	2.10 KB	140. -> 140. 54279 -> 139 (netbios-ssn)	
2016-Mar-24 10:29:55	IP / TCP SMB	2.10 KB	140. -> 140. 54280 -> 139 (netbios-ssn)	
2016-Mar-24 10:29:55	IP / TCP SMB	2.10 KB	140. -> 140. 54281 -> 139 (netbios-ssn)	
2016-Mar-24 10:31:49	IP / TCP SMB	2.90 KB	140. -> 140. 54301 -> 445 (cifs)	
2016-Mar-24 10:31:49	IP / TCP SMB	2.32 KB	140. -> 140. 54302 -> 445 (cifs)	
2016-Mar-24 10:31:49	IP / TCP SMB	2.32 KB	140. -> 140. 54303 -> 445 (cifs)	
2016-Mar-24 10:32:35	IP / TCP SMB	2.37 KB	140. -> 140. 54308 -> 445 (cifs)	
2016-Mar-24 10:32:35	IP / TCP SMB	1.94 KB	140. -> 140. 54309 -> 445 (cifs)	
2016-Mar-24 10:32:35	IP / TCP SMB	1.94 KB	140. -> 140. 54310 -> 445 (cifs)	
2016-Mar-24 10:46:39	IP / TCP SMB	2.90 KB	140. -> 140. 54295 -> 445 (cifs)	
2016-Mar-24 10:47:26	IP / TCP SMB	2.37 KB	140. -> 140. 54300 -> 445 (cifs)	

19. 此封包紀錄顯示惡意程式向同網段其他的主機 port 139 (netbios)嘗試進行存取，然而因為該主機共享有設置登入密碼，因此訊息回覆 public key 錯誤而沒有成功入侵。

```

NetWitness Reconstruction for session ID: 269 ( Source 140. : 54276, Target 140. : 139 )
Time 3/24/2016 10:44:44 to 3/24/2016 10:44:44 Packet Size 2,162 bytes Payload Size 1,428 bytes
Protocol 2048/6/139 - Flags Keep Assembled AppMeta NetworkMeta - Packet Count 13

R
E
Q
U
E
S
T

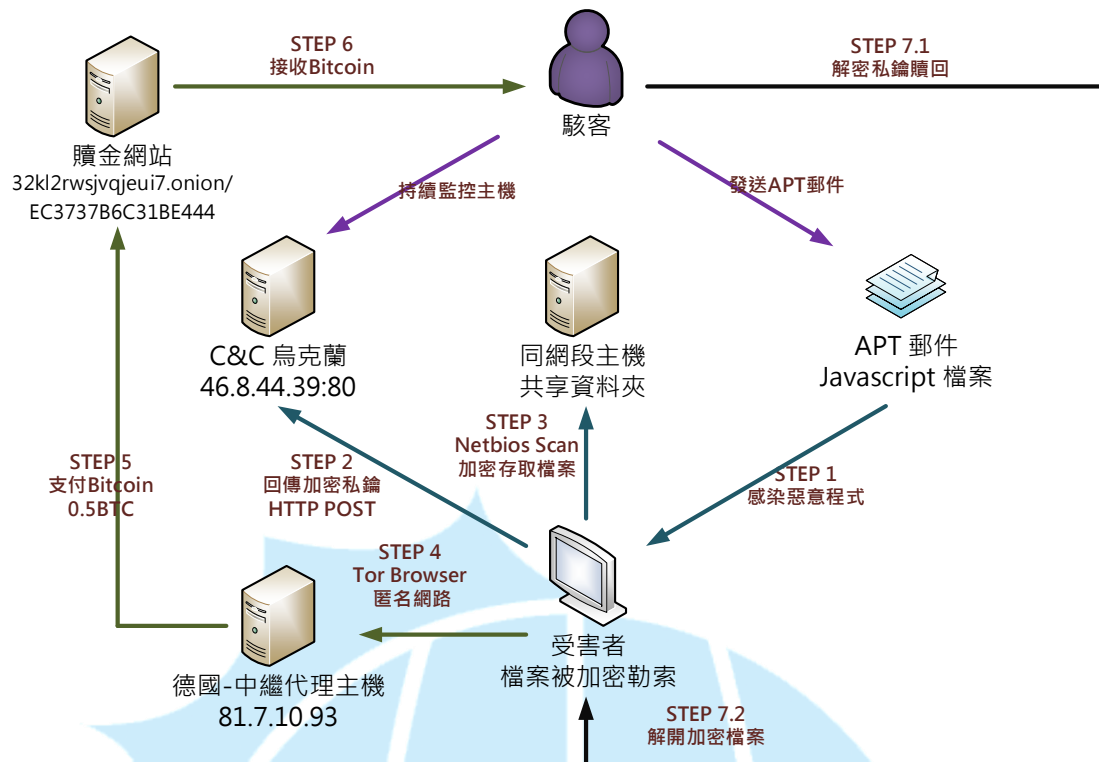
h MB@ $ 9
酯 8F

R
E
S
P
O
N
S
E

瞬SMB@ 允)離缺ω ~0+x企 濺\ @`<+00,0
+7
+7
EGOEXTS`p響瀟耗 uj+X.% I&訝n \嬭 S 莖*價?( &`3S瀉M絃J綜n髒EGOEXT
S@ 湍湍 uj+X.% 3S瀉M絃J綜n髒XOV OR0' %0#1!OUToken Signing Public Key0' %0#1
!OUToken Signing Public Key

```

III. 網路架構圖



1. 使用者透過 APT 郵件攻擊感染 Locky 的加密勒索病毒。
2. 主機感染後向烏克蘭的 C&C 主機回傳加密的私鑰。
3. 感染主機開始向同網段的共享資料夾掃描存取並且加密檔案。
4. 受害者必須透過 Tor Browser 進入洋蔥匿名網路，使用中繼代理主機。
5. 開啟了贖金網站，若是選擇付款則需要用 Bitcoin 支付 0.5BTC。
6. 駭客收到 Bitcoin 贖金後理論上會將加密私鑰 decryptor 給受害者。
7. 受害者可能夠利用駭客提供的私鑰 decryptor 進行檔案解密還原。

IV. 建議與總結

1. 使用者透過 APT 郵件遭受感染副檔名為 JS 的 Locky 加密勒索病毒。
2. 主機一旦被感染後，惡意程式會開始加密本機磁碟和網路資料夾中的文件檔、圖片檔和影音檔案。
3. 惡意程式一旦加密完各類檔案後會自我刪除，不讓使用者取得惡意程式。
4. 惡意程式隨後會跳出網頁和文件資訊，引導受害者如何去支付贖金來取得解密私鑰。

5. Locky 病毒號稱使用 RSA-2048 和 AES-128 加密，因為沒有私鑰基本上是無法救回檔案，建議使用者要定期備份重要資料避免無法挽回。
6. 理論上付了贖金給駭客，取得解密私鑰及工具就能解開，然而也無法保證能成功救回檔案，可能導致檔案遺失又損失金錢。
7. 此病毒主要透過 APT 郵件感染，有別於傳統的 EXE 檔案，務必安裝防毒軟體多能偵測抵擋此類病毒攻擊。

