駭客用勒索病毒進行資料綁架勒贖, 可能構成什麼犯罪？

文:李昕（認證法律人） · 刑事犯罪 · 2023-05-24

案例

A利用作業系統的漏洞，透過非自製勒索病毒攻擊不特定多數使用者的電腦。B開啟筆電時，發現筆電內的全數檔案均被加密，桌面出現「Read Me」檔案，要求A必須在三天內支付贖金才能取回資料，否則就會將全數資料刪除。A涉及什麼犯罪？

本文

一、資料綁架勒贖案例增多

一般民眾較常遇到的網路犯罪，大多屬於網路釣魚[1]、未涉及網路技術的刑事犯罪[2]。然而，資料綁架勒贖的案例近年逐漸增多，受害者除了一般民眾外，同時擴及掌有大量民眾敏感資料的商業[3]、醫療與政府機構。最為人所熟知的案例，就是2017年蔓延全球的WannaCry勒索病毒（ransomware）[4]。

二、駭客涉及的犯罪（見圖1）

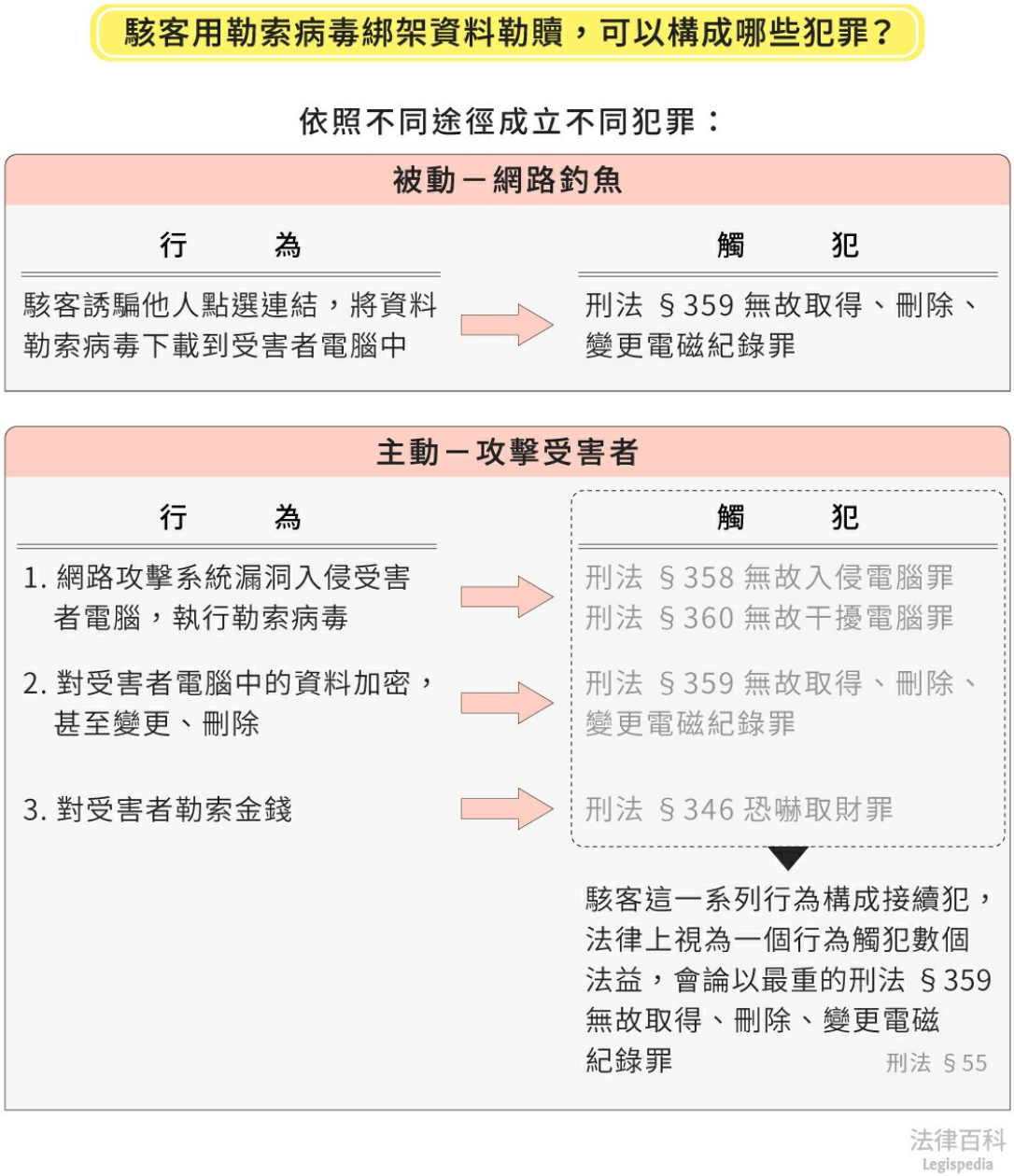

圖1　駭客用勒索病毒綁架資料勒贖，可以構成哪些犯罪？

資料來源：李昕　/　繪圖：Yen

（一）途徑：網路釣魚

如果A誘騙使用者點選特定連結，將資料勒索病毒下載到受害者的電腦中，構成的犯罪與《駭客用釣魚網站騙取個人資料，可能構成什麼犯罪？》文中的情形相同，構成刑法第359條的「無故取得、刪除、變更電磁紀錄罪[5]」

（二）途徑：主動攻擊

案例中A攻擊作業系統的漏洞入侵B的電腦執行勒索病毒，屬於利用電腦系統漏洞入侵他人電腦與干擾電腦運

作的行為，並使公眾或他人受到損害，觸犯刑法第358條的「無故入侵電腦罪[6]」與第360條的「無故干擾電腦罪[7]」；對資料加密（甚至刪除）的變更與刪除電磁紀錄行為，構成第359條的「無故取得、刪除、變更電磁紀錄罪[8]」。而A對B勒索金錢，還會構成刑法第346條的「恐嚇取財罪[9]」。

在檢察官起訴與法院審判的論罪上，根據最高法院針對第一銀行ATM盜領案[10]的見解[11]，駭客基於不法意圖，在入侵電腦後，往往緊接著下一步就會去取得、刪除或變更電磁紀錄，藉而獲取不法利益。依據社會通念，這一系列的行為構成接續犯，法律上應該評價為本於同一個犯意所從事的一個行為，而不該分開評價。

在本文的案例中，A一個行為同時觸犯刑法第346條[12]、第358條[13]、第359條[14]與第360條[15]罪名。其中第358條[16]、第359條[17]與第360條[18]同樣保護電腦使用安全法益，根據法條競合的補充關係，三項罪名中A只會構成刑度較重的刑法第359條[19]。另外的刑法第346條[20]，則保護自由法益與財產法益。A的一個行為侵害了數個不同法益（電腦使用安全法益、自由法益、財產法益），依刑法第55條[21]應論以較重罪名。因此，A的行為最後會構成刑法第359條[22]犯罪。

三、法律因應措施

除非受害者的設備屬於公務機關的電腦或相關設備，而屬於非告訴乃論，檢察機關可以主動偵查，不然像是本案中的B僅為一般民眾，屬於私人電腦資料受勒贖情況，按刑法第363條[23]規定須告訴乃論，必須先經由B的告訴，執法機關才能繼續偵查、起訴或審判的流程。

A所涉及的犯罪中，雖然同時包含了告訴乃論與非告訴乃論的罪，但資料綁架勒贖案件若未主動通報，往往無從令執法機關獲知而開啟偵查[24]。若要提起救濟，建議先將受病毒感染的硬碟取出作為提告證據，以新硬碟嘗試其他備份還原或資料緊急救援措施，避免證據滅失難以追查。

雖然網路的匿名性讓駭客難以被追溯，如果駭客位於海外，縱使刑法上具有管轄權[25]，仍需要透過跨境合作，因而增加偵查、蒐證、逮補與審判的困難。但若交由國家機關進行追查，至少仍能盡可能獲得駭客與勒索病毒相關資訊，以利後續管理措施的改善。

註腳

[1] 詳見本網站中李昕（2023），《駭客用釣魚網站騙取個人資料，可能構成什麼犯罪？》。

[2] 僅透過「網路」這個媒介從事的犯罪行為，並沒有破壞電腦或網路的運作效能，這一類犯罪的構成，並不會因為透過網路而實施而特別成立刑法妨害電腦使用罪章的罪。

[3] 自由時報（2018），《中勒索病毒近3千客戶資料沒了！老闆拒給錢寧賠數十萬》（最後瀏覽日：2023/5/24）。

[4] WannyCry病毒影響了全球各地的商業、醫療與政府機構；我國亦有多臺公務電腦受害。例如：ETtoday新聞雲（2017），《勒索病毒WannaCry全球肆虐！ 公家機關226部電腦淪陷》（最後瀏覽日：2023/5/24）；iThome（n.d.），《史上第一勒索蠕蟲WannaCry》（此為相關事件系列報導）（最後瀏覽

日：2023/5/24）。

[5] 中華民國刑法第359條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。」

[6] 中華民國刑法第358條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。」

[7] 中華民國刑法第360條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。」

[8] 中華民國刑法第359條。

[9] 中華民國刑法第346條第1項、第2項：「

I 意圖為自己或第三人不法之所有，以恐嚇使人將本人或第三人之物交付者，處六月以上五年以下有期徒刑，得併科三萬元以下罰金。

II 以前項方法得財產上不法之利益或使第三人得之者，亦同。」

[10]iThome（2016），《一銀行ATM疑遭植入惡意程式盜領7000餘萬元，全台400多台ATM停用》（最後瀏覽日：2023/5/24）。

[11]最高法院106年度台上字第2603號刑事判決：「所謂接續犯，係指基於單一之犯意，以數個舉動接續進行而侵害同一法益，在時間及空間上有密切關係，依一般社會健全觀念，難以強行分開，在刑法評價上，以視為數個舉動之接續實行，合為包括之一行為予以評價，較為合理，於此情形，即得依接續犯論以包括一罪。原判決已敘明被告3人與其他盜領犯罪集團成員，共同意圖為自己不法所有，利用銀行電腦系統之漏洞，入侵銀行內部電腦網路，製作、存放盜領ATM款項之惡意電腦程式，變更、刪除他人電腦之電磁紀錄，遠端操控，以盜領第一銀行ATM之現鈔，係在密切接近之時間所為，侵害同一被害人即第一銀行之財產法益，依前開說明，其等各行為之獨立性極為薄弱，在刑法評價上，以視為數個舉動之接續施行，合為包括之一行為予以評價，較為合理等旨綦詳。」

[12]中華民國刑法第346條。

[13]中華民國刑法第358條。

[14]中華民國刑法第359條。

[15]中華民國刑法第360條。

[16]中華民國刑法第358條。

[17]中華民國刑法第359條。

[18]中華民國刑法第360條。

[19]中華民國刑法第359條。

行為人一行為同時觸犯刑法第358條與第359條，法院從重論第359條之罪的例子，請見臺灣高雄地方法院102年度簡字第2515號刑事判決：「……被告係基於盜用告訴人前述臉書帳號之目的，以輸入告訴人前述電子信箱及臉書帳號、密碼方式，入侵告訴人前述電子信箱及臉書帳號並變更密碼，觸犯前述罪名，因前述罪名之保護法益同為電腦使用安全，應依法條競合之補充關係，論以較重之無故變更他人電腦相關

設備之電磁紀錄罪。」

[20]中華民國刑法第346條。

[21]中華民國刑法第55條：「一行為而觸犯數罪名者，從一重處斷。但不得科以較輕罪名所定最輕本刑以下之刑。」
這項在學理上又稱為「想像競合」，指一行為觸犯數法益時，應處以所觸犯的罪名中較重者。詳見最高法院107年度台上字第32號刑事判決：「刑法第55條前段所謂一行為而觸犯數罪名，即學理上所謂之想像競合犯，係指行為人以一個構成犯罪要件內容之行為，同時侵害數法益，而觸犯數個罪名而言。」

[22]中華民國刑法第359條。

[23]中華民國刑法第363條：「第三百五十八條至第三百六十條之罪，須告訴乃論。」

[24]刑事訴訟法第228條第1項：「檢察官因告訴、告發、自首或其他情事知有犯罪嫌疑者，應即開始偵查。」

[25]中華民國刑法第4條：「犯罪之行為或結果，有一在中華民國領域內者，為在中華民國領域內犯罪。」

標籤

勒索， 妨害電腦使用罪， 告訴乃論， 電磁紀錄， 競合