淺談資安監控及事件反應：以勒索軟體為例

蘇柏鳴 / 金融聯合徵信中心 資安部

一、勒索軟體

（一）何謂勒索軟體[1]

勒索軟體（Ransomware），又稱勒索病毒，是一種特殊的惡意軟體，又被人歸類為「阻斷存取式攻擊」（denial-of-access attack），其中一種勒索軟體僅是單純地將受害者的電腦鎖起來，而另一種則系統性地加密受害者硬碟上的檔案。所有的勒索軟體都會要求受害者繳納贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的解密金鑰以便解密檔案。勒索軟體通常透過木馬病毒的形式傳播，將自身為掩蓋為看似無害的檔案，通常會通過假冒成普通的電子郵件等社交工程學方法欺騙受害者點擊連結下載，但也有可能與許多其他蠕蟲病毒一樣利用軟體的漏洞在聯網的電腦間傳播，個人、政府機關及企業組織皆可能成為被攻擊的對象，已逐漸成為嚴重的資安威脅之一。

目前可簡易分類為下列兩種：

1. 非加密型勒索軟體

將受駭者的資訊設備鎖起來，破壞受駭者對設備的存取權。

2. 加密型勒索軟體

加密受駭者硬碟上的檔案，破壞受駭者對資料的存取權，通常要求受駭者以加密貨幣支付贖金，以取回檔案的存取權。

（二）勒索軟體之影響

2018年最為人知道「台積電產線中毒大當機」事件，因安裝人員未依造SOP操作，而是先將機台連上網路，再開始進行防毒處理，導

[1] 維基百科，https://zh.wikipedia.org/wiki/%E5%8B%92%E7%B4%A2%E8%BB%9F%E9%AB%94。

[2] IThome，深度剖析台積產線中毒大當機始末（下），https://www.ithome.com.tw/news/125101。

致一台機器感染病毒，造成竹科、中科、南科廠區的相關設備受到大規模感染，造成新台幣52億元 的損失，創下台灣資安史的紀錄，除此之外屬於重大關鍵基礎設施的中油、日月光集團、仁寶、宏碁、廣達、研華……等近兩年都受到勒索軟體的攻擊，Cybersecurity Ventures預測，到 2031年勒索軟體每年將給受害者帶來約 2650億美元的損失，這一金額是其基於未來10年損害成本同比增長30%的基礎所得出，代表該機構認為未來勒索軟體造成的傷害的成長比例非常驚人。

（三）勒索軟體介紹

1.Pysa[3]

Pysa勒索軟體是Mespinoza勒索軟體的變種，於2019年12月被首次命名，最初被加密的檔被Mespinoza使用 .locked作為副檔名，然後轉而使用 .pysa作為尾碼，目前此勒索軟體可能會交替使用Pysa和Mespinoza 這兩個名稱來命名被加密的檔。Pysa與許多已知的勒索軟體系列一樣，被歸類為勒索軟體即服務（RaaS[4]）工具，這意味著其開發人員已將這種現成的勒索軟體出租給犯罪組織，這些犯罪組織在技術上不夠精通，無法製作自己的勒索軟體。Pysa客戶可以根據RaaS提供的選項對其進行自訂，並根據自己的喜好進行部署，Pysa能夠在加密要勒索的檔之前從受害者那裡竊取資料。

2.Conti[5]

Conti勒索軟體現身於去年7月，屬於新興的雙重勒索軟體陣營，在以勒索軟體加密系統之前，會先下載未加密的機密資料，以在受害者拒絕支付贖金以換取解密密鑰時，作為進一步的勒索籌碼，已有部分案例顯示有受害者最終是為了保護資料而選擇支付贖金。

在2021年2月，趨勢科技的研究人員收到了一系列與Conti勒索軟體團伙攻擊有關可疑事件的警報，這些事件是由Trend Micro Vision One平台發現的。Conti被認為是流行的Ryuk勒索軟體家族的變種，越來越多的攻擊者現在通過與過去傳播Ryuk相同的方法傳播惡意軟體，台灣工業電腦大廠研華（Advantech）就是遭到此軟體的攻擊。

3.Avaddon[6]

Avaddon 勒索軟體是一種勒索軟體即服務 （RaaS），將加密和資料竊取與勒索結合在一起。自2019 年以來一直存在，但自 2020 年 6 月開始變得更加突出且更具侵略性。該服務的「會員」或客戶會利用夾帶JavaScript檔案的惡意垃圾郵件和網路釣魚活動，將 Avaddon 散布到多個國家/地區的廣泛目標。遭 Avaddon 勒索軟體攻擊的企業不僅資料會被加密，還會被威脅公開在 Avaddon 解密網站上，最近甚至還有分散式阻斷服務（DDoS） 攻擊會中斷營運的風險。

3 新型勒索軟體PYSA淺析，https://blog.csdn.net/MSB_WLAQ/article/details/121575844。
4 資安趨勢部落格，https://blog.trendmicro.com.tw/?p=69932。
5 Conti勒索軟體分析，https://read01.com/zh-tw/BJ5yokG.html#.YcQXTGhBw2w。
6 Avaddon 勒索軟體攻擊防範須知，https://www.cio.com.tw/avaddon-ransomware-attack-precautions/。

4.LockBit [7]

LockBit 是範圍廣泛的勒索網路攻擊中的一種新型勒索軟體攻擊，它以前被稱為“ABCD”勒索軟體，而這種特定攻擊已經發展成為同類勒索工具中的一種獨特威脅。LockBit 是被稱為「加密病毒」的勒索軟體的一個子類，因為它構造了與財務付款有關的勒索請求，以換取解密。它主要針對的是企業和政府組織，而不是個人。

攻擊最初始於 2019 年 9 月，當時被稱為「abcd 病毒」，這個名稱是指加密受害者檔時使用的檔副檔名。過去的主要目標包括美國、中國、印度、印尼、烏克蘭的公司；此外，歐洲各地的許多國家/地區（法國、英國、德國）也遭受了攻擊。

可行的目標是那些因中斷而感到業務受阻並願意為消除阻礙而支付鉅款的公司，並且這些公司有足夠的資金支付贖金，因此，這可能導致針對大型企業發起廣泛攻擊。在自動審查過程中，該惡意軟體似乎也有意避免攻擊俄羅斯或獨立國家聯合體內任何其他國家/地區的本地系統，可能是為了避免在這些地區遭到檢舉；LockBit 採用了勒索軟體即服務（RaaS）的形式。

5.REvil[8]

REvil勒索軟件，又稱Sodin或Sodinokibi，是一種勒索軟件病毒，最早在2019年初有人發現，是一個對網絡保安構成極具威脅性的電腦病毒。最初，REvil是透過Oracle WebLogic服務器漏洞及網絡釣魚活動進行大規模的傳播，並勒索受害者電腦及竊取電腦及公司內部資料。

近年來俄羅斯駭客組織REvil逐漸壯大，在勒索軟體的排行中名列前茅，被列為最危險的勒索軟體之一，該駭客組織自2019年起，針對全球從製造業、金融業到電信業等20個領域進行攻擊，REvil專門鎖定全球各地企業進行勒索攻擊，台灣多家企業也深受其害。REvil勒索軟件的威脅性之所以那麼大，是因為它的目標主要為美國託管服務供應商，並從中竊取大量敏感數據。當受害人的電腦被REvil勒索軟件攻擊並感染後，電腦內的文件會被加密並發出勒索信息，要求受害人在時限內以比特幣或其他加密貨幣繳付贖金，若未能及時支付，勒索的贖金將會增加一倍。

6.Maze[9]

他們採取「雙面剝削」，當遭到加密及勒索的企業不願支付高額贖金，它就會利用公開網站和「新聞稿」方式公布這些通常是知名企

7 LockBit 勒索軟體-須知信息，https://www.kaspersky.com.cn/resource-center/threats/lockbit-ransomware。

8 全球逾千家企業遭REvil勒索軟體攻擊，建議落實資安防護，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9324。

9 Maze勒索軟體也宣布退出江湖，Egregor接手資產，https://www.ithome.com.tw/news/140826。

業的受害者，先讓企業顏面無光。若企業最後還是不付款，Maze背後的駭客就會公布這些資料。

最近一名涉及知名書店Barnes and Noble勒索軟體攻擊的駭客告知媒體，Maze組織從今年9月起就不再加密新受害者的電腦了，而連鎖書店的攻擊算是他們幹的最後一票。Maze的受害企業多不勝枚舉，今年之前還曾攻擊Canon、全錄、LG、Cognizant等知名企業，也曾被受害者告上法院。

7.DoppelPaymer[9]

DoppelPaymer 應該是從BitPaymer勒索病毒（首次出現於 2017 年）所衍生出來，因為它們的程式碼、勒索訊息、付款網站都有相似之處。不過值得注意的是 DoppelPaymer 與 BitPaymer 還是有些差異，例如，DoppelPaymer 使用「2048 位元 RSA + 256 位元 AES」加密機制，但 BitPaymer 卻是使用「4096 位元 RSA + 256 位元 AES」加密機制 （舊版則使用「1024 位元 RSA + 128 位元 RC4」）。此外，DoppelPaymer 也改善了 BitPaymer 的加密速度，使用多重執行程序來執行檔案加密。

兩者還有另一項差異是 DoppelPaymer 在執行惡意行為之前，它必須收到正確的指令列參數。根據我們蒐集到的樣本顯示，不同的樣本需要不同的參數。這樣的技巧很可能是歹徒為了躲避沙盒模擬分析而設計，此外也為了防止資安研究人員對樣本進行研究。

8.LV[10]

Secureworks Counter Threat Unit（CTU）[12]分析LV勒索軟體，發現它和REvil具有相同的程式架構，顯示它背後的組織Gold Northfield可能是向REvil的營運組織Gold Southfield買原始碼　或與REvil共享程式碼，就是REvil程式碼被黑吃黑，竊走了程式碼。

9.Egregor[13]

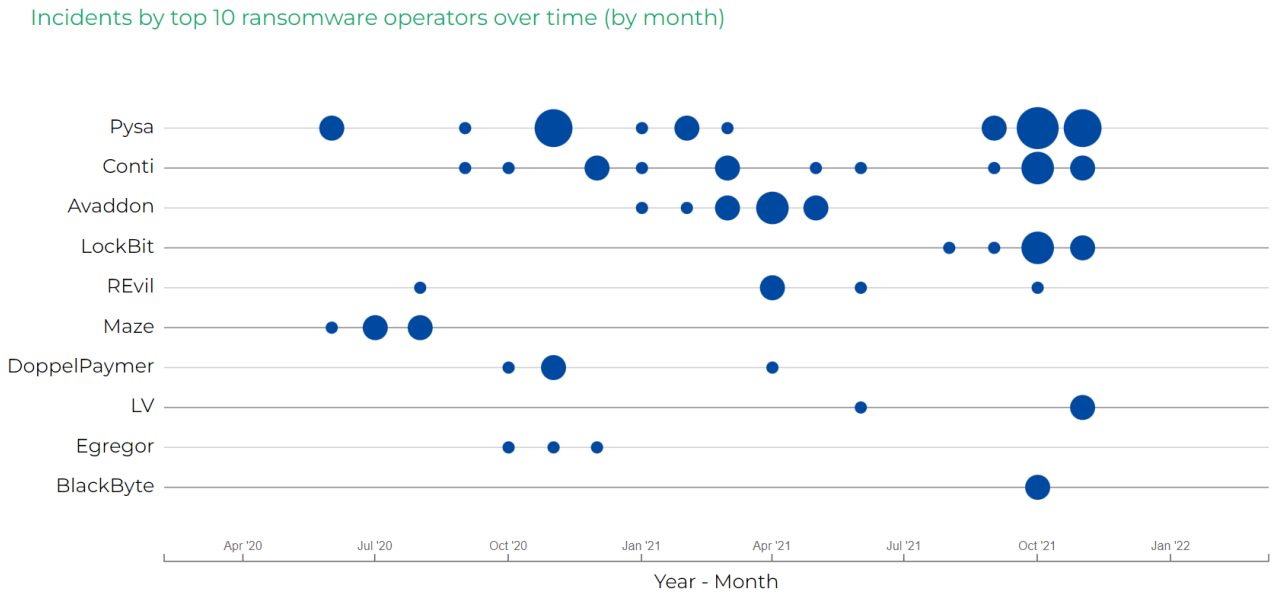
Egregor是在2020年Maze宣佈退出江湖後，接手其攻擊程式等資產而興起，FBI發出的TLP:White「私人企業通知」（Private Industry Notification，PIN）指出，從2020年9月FBI首度觀測到Egregor以來，全球已經有超過150家企業遭到Egregor變種攻擊的消息。

Egregor使用多種不同機制駭入企業，包括發送具惡意附件的釣魚信件到員工個人帳號，或是開採遠端桌面協定（RDP）或VPN漏洞駭入企業網路。而進入公司網路後，攻擊者也可能利用Egregor的RDP開採能力。

當Egregor成功存取企業網路後，會使用常見的滲透測試法及工具，像是CobaltStrike、Qakbot/Qbot、IP 掃瞄工具和AdFind等，以擴張權限並在內部網路橫向移

10 剖析FBI 向企業發出警告的DoppelPaymer 勒索病毒，https://blog.trendmicro.com.tw/?p=66821。
11 致敬？REvil勒索軟體出現山寨版，https://www.ithome.com.tw/news/145220。
12 CTU，https://www.secureworks.com/about/counter-threat-unit。
13 FBI警告企業Egregor勒索軟體來襲，https://www.ithome.com.tw/news/142108。

圖1、Incidents by top 10 ransomware operators over time（by month）[14]



動。加密企業重要檔案的同時，Egregor也會利用同步軟體Rclone及7zip等工具，有時也會偽裝成svchost行程將資料竊取傳送出去。而且它還經常利用受害者機器的列印功能，把勒索訊息列印出來。

二、資安監控防護

（一）勒索軟體感染途徑[15]

1. 網站瀏覽

（1）瀏覽網站時，倘若使用者電腦存在Java/Flash/Adobe/瀏覽器等軟體漏洞，當輪播到惡意廣告，便可能遭受勒索軟體入侵。

（2）點選到網站內的惡意連結（如：廣告、新聞），便可能遭受勒索軟體入侵。

（3）誘騙使用者連到看似真正銀行或政府機關網站的假網站（山寨網站）。

2. 電子郵件感染

當使用者點選或開啟電子郵件中的惡意網站或內嵌惡意程式的附件檔案，便可能遭受勒索軟體入侵。

3.非法軟體感染

網路上非法軟體或小工具可能含有惡意程式，若使用者下載安裝這類非法軟體或小工具，惡意程式可能在安裝過程中讓使用者授權以存取機密資料或加密資料。

14 https://cit.cyberpeaceinstitute.org/explore?utm_source=google&utm_medium=cpc&utm_campaign=CIT_explore&utm_content=1&gclid=CjwKCAiAtouOBhA6EiwA2nLKHx9u8c6NXqEGrH22vC5MXN3p_sArHANC4jovApsZ-tH-b3Gh-y5mNhoCzAQQAvD_BwE。

15 行政院國家資通安全會報技術服務中心-勒索軟體防護專區，https://www.nccst.nat.gov.tw/RansomwareProtection?lang=zh。

4.被已遭受勒索軟體攻擊的電腦或裝置感染

勒索軟體可能透過已遭受攻擊的電腦或裝置掃描使用者電腦所連結的磁碟機，包括本機的硬碟、連結電腦的USB磁碟、網路芳鄰磁碟機、雲端硬碟及檔案伺服器的檔案，只要能被循線找到，就都有可能遭受勒索軟體入侵。

（二）資安監控及事件反應

筆者於2020年參加RSA Conference 2020[16]的Cyber Defense Matrix （CDM）Learning Lab，CDM是由曾經在美國銀行擔任首席安全科學家Sounil Yu在2016 RSA Conference所發表的一種安全模型，該模型結合了NIST Cybersecurity Framework（CBF） 的操作功能–識別（Identify）、保護（Protect）、檢測（Detect）、回應（Respond）和恢復（Recover），並新增了資產類別-設備（Device）、應用程序（Application）、網絡（Network），數據（Data）和使用者（User）。

就此模型整理出一份目前相關資安防護機制的CDM圖（圖二），此圖很清楚的將目前主流防護機制展現在這個矩陣中，以勒索軟體攻擊為主軸，就CDM內之防護機制做以下探討：

1.辨識（Identity）

(1)防毒軟體：辨識出是否有主機中毒，及時阻斷，避免擴散。

(2)弱點掃描：找出主機上弱點，避免弱點被利用。

(3)威脅情資：藉由情資交換，得知目前發生之資安事件，提早因應資安攻擊事件。

(4)郵件防護：擋掉惡意郵件，並發出警告，讓資安人員知道有人意圖使用社交工程方式進行資安攻擊。

(5)社交工程演練及資安教育訓練：建立組織人員對於資安警覺性。

(6)資安健檢：整體資訊系統健康程度檢視。

2.防禦（Protect）

藉由防火牆、WAF、IP阻擋外部之攻擊，帳號管理避免被提權，導入安全資訊系統開發（SSDLC）強化系統開發安全。

3.偵測（Detect）/ 因應（Respond）

藉由端點防護監控（EDR）端點是否有異常執行非預期作業，並經由各系統Log蒐集分析偵測出異常資安行為，並快速告知系統管理人員，快速執行相關應對措施。

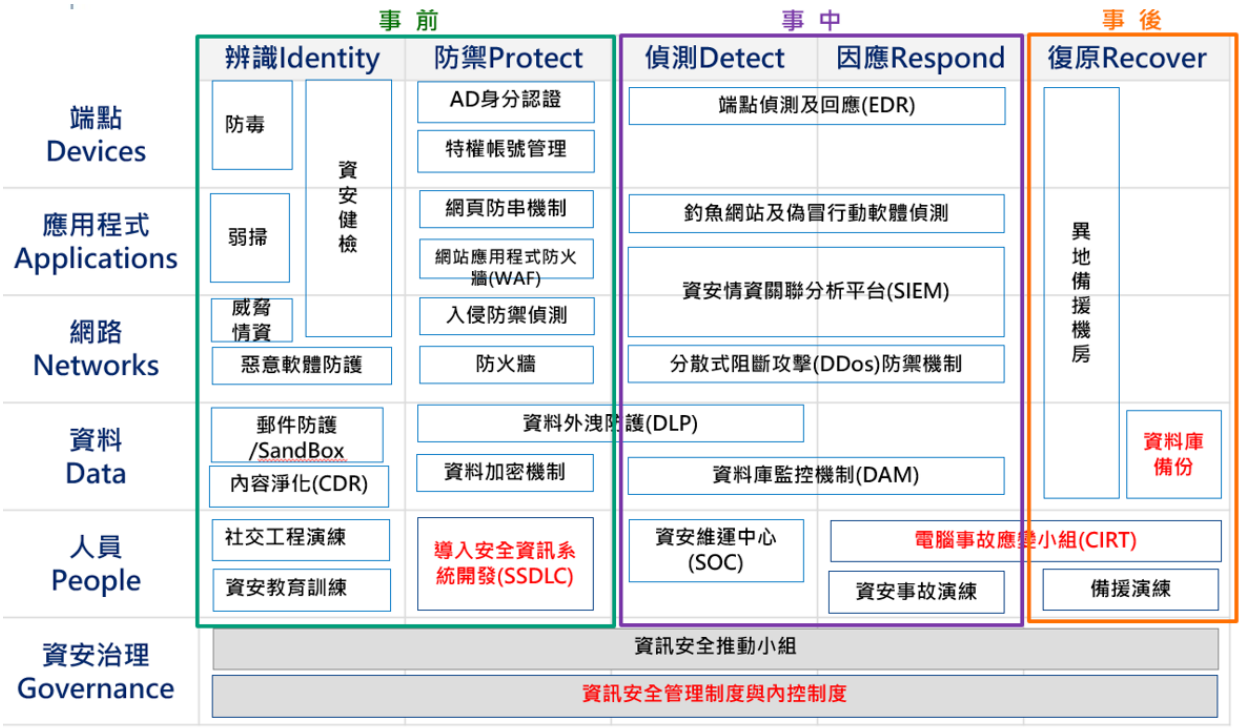
4.復原（Recover）

異地或第三地備援能在主中心端被癱瘓後接手維持營運，而資料庫備分避免重要資料被加密後無法復原。

定期檢視整個事前事中事後對應之防護措施，配合MITRE ATT&CK攻擊手法瞭解，可以更有效對於資安事件的預防及反應。

16 蘇柏鳴, RSA Conference 2020研習紀要-財團法人金融聯合徵信中心https://www.jcic.org.tw/main_ch/fileRename/fileRename.aspx?fid=1140&kid=1。

圖2、Cyber-Defense Matrix



三、結論

資通安全管理法子法「資通安全事件通報及應變辦法[17]」將資安事件分為四級，且規定公務機關及非特定公務機關之事件發生等級之回覆時間，並取規定於時間內完成復原作業，此法規定對於時效要求非常嚴格，在實務面執行上會造成非常大的壓力，往往在事件發生後光掌握實際狀況就非常耗時，在分秒必爭的狀況下，如沒有一個完成的監控及反應機制，是很難在目前的要求下完成資安事件回報及恢復運作，所以檢視目前防護機制，掌握事前事中事後對應之防護措施，對於組織在面對資安事件發生時，是否能快速反應起了非常關鍵的作用。

17 https://nicst.ey.gov.tw/File/300A43072E85B6D0?A=C。