「看不見的英雄」系列報導（二十一）

鮮乳坊
首家由乳牛獸醫師把關的好農鮮乳品牌

刁曼蓬

前言

以「獸醫現場把關」、「嚴選單一牧場」、「無成份調整」、「公平交易」爲經營理念，乳牛獸醫師龔建嘉、郭哲佑、林曉灣等三位青年，2015年在食安風暴時，以群眾募資方式成立「鮮乳坊」，打造「單一牧場」高質量鮮奶的利基市場。從近5,000名群眾募資的支持者、小眾市場起步，現今有逾千名直送客户，有機、大型超市的通路；市占率從零至3%，2021年營收近6億元。其間耗時三年打造「鮮乳2.0革命」，推出台灣第一瓶A2β酪蛋白鮮乳（蛋白結構貼近母乳成分），提供消費者高品質鮮乳的另一選擇。成立以來致力實踐ESG，爲亞洲首家「B型企業」（用商業模式解決社會問題、ESG核心精神）認證的乳品品牌；使企業、社區、員工、客户、環境共好，爲青年創業模式的典範。

食安危機中催生

2014年間「黑心油」事件引發食安危機，掀起國人「吃乾淨食物」的健康意識。時任農場乳牛獸醫師的龔建嘉，與致力協助小農產品行銷的郭哲佑，決定透過群眾募資打造「由獸醫師把關、讓消費者可以安心食用」的優質鮮奶，得到公眾迴響，集資新臺幣608萬元。

1985年次的龔建嘉，是「鮮乳坊」發起人。大學、研究所就讀獸醫，在同學們多走向貓、狗等伴侶動物（家庭寵物）的獸醫行列，龔建嘉決心做「一直以來地球上飼養群體廣大、最需要獸醫師照顧的大型經濟動物，如豬、牛、馬等被視為冷門」的獸醫。

立志做牛醫師

「台灣經濟動物以雞、豬為主，就獸醫專業來看，多屬群體防疫、實驗治療，很少單體治療。惟單價介於新臺幣10萬元的牛隻，會做單體診療、如開刀等，相對有趣。」再加上父母家人都屬牛，龔建嘉把興趣專注在乳牛研究上。

就讀研究所時，龔建嘉追隨專研大型經濟動物的蕭火城老師，跟隨其進行農場實習，經常6:00出門，晚上收工；出診結束後，再進研究室工作，習得紮實訓練。成為國內少數未滿30歲、得以獨立出診的大型動物獸醫師（國內大型動物獸醫師只有二、三十位，年齡多在50歲以上）。

畢業後，龔建嘉先在乳牛營養品公司任職，後至美國康乃爾大學進修乳牛營養學課程。回國後，家在台北的龔建嘉，選擇到南部牧場擔任獸醫。在全職投入的過程中，發現台灣現有500家牧場的酪農產業，正遭遇瓶頸。

台灣酪農的困難

乳牛怕熱，最適溫度為攝氏15度；但隨著氣候變遷使夏季變長、動輒攝氏36~37度高溫，牛隻緊迫、影響進食，精神差、泌乳降低、營養不夠、易罹患代謝性疾病，造成乳牛飼養的困難。

其次，酪農面臨從業人口老化、人力不足的棘手問題。但現有法令僅有特定條件下開放乳牛場申請外勞，包括養殖技術（獸醫、營養）、管理（牧場環境、分群等）、基層工作（擠奶、放草、清洗牛舍）等牧場人力都不敷需要。

再加上台灣乳品市場收購機制，長時間來為大型乳品廠主導，生乳收購價格，由產官學每年議定一次。不論牧場管理、牛奶品質的變動，全按照統一價格，未能反映酪農的真實狀況。對管理良好的牧場而言，努力與付出不成比例，阻礙年輕一輩的投入。而消費者喝到的牛奶，是大廠收購來的牛奶混合處理，無法確認牧場來源與品質。

理解酪農的瓶頸，具行動力的龔建嘉積極尋找解決方案。他走訪歐洲、日本、考察在地乳品業，發現德國、日本的超市有許多琳瑯滿目的獨立品牌；在地優良酪農，不將乳品賣給大廠家，而以獨立品牌銷售。

受到德、日乳品獨立品牌的啟發，龔建嘉思考酪農產銷體系變革，計畫從零售端為酪農建立銷售平台起步。惟限於乳品網路訂購仍尚未養成消費者的習慣、不易推動，以及已有的獨立農民品牌其牧場飼養水準不一，此一想法未竟全功。

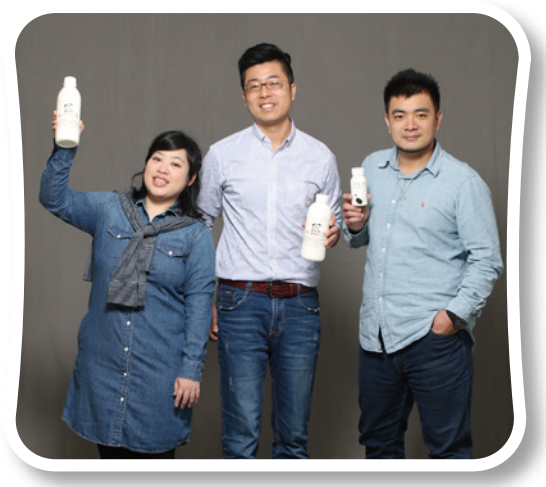
▲鮮乳坊創辦人暨乳牛獸醫在產地建立擁有乳牛專業營養師、藥師、數據分析師等的專業生產團隊

龔建嘉不放棄，改從源頭著手，規劃建構一個由獸醫師把關、優良牧場飼養、有身分證的牛奶品牌。他找到大學時就認識的豐樂牧場合作，「牧場負責人為中生代，技術導向、對其飼養水準很具信心，但是自有品牌發展有其困難。」

牛奶怎麼群眾募資？

當時僅有5年全職獸醫師經驗的龔建嘉，除對酪農的了解與滿腔熱情外，欠缺創業經驗與資源。就在這當口，國內發生食安風暴。1990年次、大學時已有3次創業經驗（協助有機、小農產品網購社會企業）的郭哲佑，決定一起攜手以「獸醫現場把關、嚴選單一牧場、無成分調整、公平交易」為訴求，用「預購牛奶、公開募資」，向群眾募集資金。2個月時間，支持者5,000名、集資達新臺幣608萬元。

「當時目標為新臺幣100萬元，在第二周達到300萬元時，反而壓力大增，開始找夥伴成立公司，思考如何找加工廠、銷售通路等。」龔建嘉、郭哲佑、加上一位擔任中小企業老闆特助的國中同學林曉灣，3人集資300萬為股本，成立台灣第一家由獸醫師與酪農聯手打造品牌的「鮮乳坊」。



▲創辦人合照

2015年5月「鮮乳坊」開始運作。龔建嘉負責生產端把關，郭哲佑肩負市場開發重責，林曉灣負責掌理組織、財務、人力運營管理。龔建嘉一週5天馳騁於中南部牧場、源頭把關，另外兩天的時間北上處理「鮮乳坊」業務，大夥幾近全年無休。

人生字典中沒有「退縮、畏懼，只有朝向目標前進」的年輕團隊，在推動青年創業的「時代基金會」免費提供籌備地點的協助下，開啟創業之路。龔建嘉說服中華民國農會的台農鮮乳廠代為加工，籌建物流、倉儲冷藏，用股本半數購買第一台冷藏運送車。

週末假日全員到市場指標的微風廣場超市，進行試飲。並從有機店、藥房、補習班等非傳統通路進軍。七個月的時間，營業額將近3,000萬元，反映市場對「乳牛獸醫把關與單一牧場乳源」的品牌理念認同。

2016年持續挺進，龔建嘉、郭哲佑經由各種場合、包括TED Talk視頻等與大眾分享「鮮乳坊」理念。負責通路的郭哲佑，幾經折衝奮力打開微風超市，在期間取得優異的銷售成績單，很快地在第二年也敲開「全家」便利商店通路的門，以第二家嘉明牧場小包裝210cc的產品投入市場，當時兩個牧場旗下已近1,000頭乳牛，每日有7噸供應量，市佔率0.8%。

漸次拓展至包括主婦聯盟、Jason超市、家樂福、全聯等大型超商，開拓路易莎咖啡、天仁茗茶、喫茶小鋪等業務市場。「鮮乳坊」接觸到更多的消費大眾。

與牧場共好

隨著業務不斷提升，「鮮乳坊」辦公室先後搬遷到新莊五股附近工業大樓，省去大部分裝潢費用，以高於市場平均收購價向酪農收購，將盈餘回饋給牧場。牧場增加的收益則用於改善牛舍環境，提升牧場養殖技術。如裝設地墊、風扇，引進自動榨乳機、灑水設備、水床、導入數據管理系統等。其他盈餘則用於提升「鮮乳坊」公司經營管理，如建置ERP、員工教育訓練，並發起「大型獸醫師復育」的社會回饋計畫。

「我們把錢用在員工經營專業的課程教育支出上，幾年來已經媒合59位實習獸醫師的訓練，培養3位獨立獸醫師至合作牧場做醫療服務，」共同創辦人林曉灣指出。

有生產履歷的鮮奶

採單一牧場乳源生產的「鮮乳坊」，乳品生產履歷可以溯源。產銷履歷認證、營養師原料把關、牧草飼料經過檢驗、獸醫用藥管理、抗生素快篩檢驗。牛隻健康採E化4.0管理，生乳運送與加工產線，採獨立乳槽、乳桶、管線。出品的鮮奶包裝上，會標明牧場出處。資深的員工熟稔分辨各家牧場因飼料配方而展現出特有的鮮乳風味。

並與合作牧場啟動「鮮乳革命2.0」，開創全台僅有0.1%珍貴乳源，生產台灣第一瓶A2β酪蛋白鮮乳（蛋白結構貼近母乳），親和人體、更好吸收，適合孩子銜接母乳的第一瓶鮮奶，以及體質敏感者食用。

由於經營理念受到消費者肯定，「鮮乳坊」業務成長快速，目前往來合作的牧場有六家之多。

力拼ESG的B型企業

「鮮乳坊」力拼ESG，友善環境、發展綠色農牧循環。70%的合作牧場牛糞、污水、沼渣進行二次發酵處理後，再利用於牧草施肥。計畫將牛隻排泄物發展為農牧循環綠能中心（沼氣可發電），鼓勵合作畜牧場、建置太陽能板，將能源售予台電再利用。也曾安排合作客戶參訪牧場，近身體驗，串接使用者與牧場。

「鮮乳坊」經英國SROI社會投資報酬率認證（每投資1元，即產生4.05元社會影響力），2020年通過國際B型企業認證，成為受到國際認可的社會企業，且為亞洲第一瓶無添加認證的乳品品牌。「以商業模式的架構，致力成為台灣最具正面影響力的乳品品牌，打造消費者信任、農民驕傲、動物健康的新食農生態」，為其守護的經營理念。

▲鮮乳坊第一個合作的牧場-豐樂牧場主人與女主人

創業心情

「過去是上班族，遇到解決不了的問題就丟給老闆。創業後變成大家將解決不了的問題，都丟給我們。從不負責到當責扛責，心態轉變很重要。」負責後勤支援運作管理的林曉灣說，創業就像「越級打怪」、永遠挑戰超出自己能力範圍的任務。從實戰錯誤中，快速累積經驗、學習。「最有成就感的是，團隊推著不斷持續學習新的事務，相信未來團隊會是一個強大、相互支援、讓前線打仗的夥伴無後顧之憂的在戰場上衝刺的隊伍。」

「人才的培育，組織強化是支持營運推展的動能。」負責品牌通路行銷的郭哲佑，於2020年底接手執行長後，即著手組織人力盤點，推動「人力2.0計畫」；投入1,000多萬元巨資導入ERP系統。「經由量化、數據管理找出問題癥結，優化系統、調整組織體質、評估未來發展優勢等…，以使組織運行跟得上發展步伐，讓鮮乳坊在疫情期間得以更上層樓，間獲得市場肯定。」謙虛、不斷的學習、讓組織賦能，為郭哲佑扛下CEO心得。過去兩年儘管疫情嚴峻，鮮乳坊營收成長分別為22%、40%，以「創造客戶價值」取勝的訴求，獲得市場認同。

▲鮮乳坊新書發表會

時代基金會執行長趙如媛說，「鮮乳坊創業的過程並非一帆風順，他們的失敗經驗早於開創鮮乳坊之前就開始了。但他們都沒有被當年的數次失敗和挫折嚇到，反而從中找到自己的使命和前進力量！」

「 鮮乳坊」的共同創辦人和多數主管是來自時代基金會Epoch School，創業的起點也是時代基金會的Garage 育成計劃。「計畫初始為社會培養人才，沒想到多年之後他們努力實踐，所創造的價值超越當初想望。」趙如媛說，創業，若能與社會共好，比起成為「獨角獸」，更有價值。也是鮮乳坊長期訂戶的趙如媛表示，每天早晨打開冰箱看見鮮乳坊可愛的logo和胖胖的罐子，「提醒我：社會有一群年輕人正努力讓世界變得更好，很安心、很開心、很受祝福。」

彰銀觀點

彰化銀行新莊分行經理張文杰透過創辦人獸醫師「阿嘉」在YouTube上的「TEDxTaipei」演講、郭哲佑在「食力」的分享，及透過創新商業模式、解決社會問題發起的「白色革命」中，進而接觸到鮮乳坊這群有理想的年輕人。

張文杰經理指出，經由發現酪農產業的困境及消費者對食安的期待，透過群眾募資、結合獸醫專業協助酪農及非典型通路，以創新商業模式與消費者緊密連結，並把賺到的錢成立公益循環基金，幫助酪農購買新設備、培育新獸醫師、協助偏鄉，落實「企業社會責任SDGs」（實現小規模農戶收入增加一倍），且經英國SROI社會投資報酬率認證，2020年通過國際B型企業認證，是非常有理想性的企業。也是貨真價實的『社會企業』，與彰銀致力推動之ESG價值一致，奠定彼此深化往來的基礎。

新莊分行經由深度對談，透過二維判斷法計量方法，確認鮮乳坊在市場市佔率業已達到經濟規模，且為非財團乳品之首位。分析測算其107～110年之財務報表，藉由綜合指標評析「發展狀況（營收增長率、營業淨利增長率、資產增長率）」、「獲利水平（內在投資價值、ROE、ROA）」、「經濟效益」，均呈現大幅增長，堪稱乳品界的「隱形冠軍」。其中，鮮乳坊的「內在投資價值」受到市場高度認同，於110年發行新股以每股溢價150元增資發行即為投資價值的具體展現。

新莊分行與創辦人龔建嘉、林曉灣對談探討公司營運現狀願景及二維法分析，發現鮮乳坊是一家具有高度價值的成長潛力公司。公司初期公司財務運作採輕資產經營模式，惟伴隨營收成長、連鎖賣場通路比重漸增，鮮乳坊考量未來更能有效掌握乳源及品質，擬規劃向上垂直整合，計畫購買部分農場，因此資金需求日益增加。就前述鮮乳坊的未來發展，新莊分行建議鮮乳坊公司應善用資產負債表的資源，強化應收帳款金流管理及融資，挹注所需流動性，並能增加資金效能。規劃有效配置長短期授信以支援向上垂直整合資金需求，及有效調整財務結構。可善用溢價現金增資與長期融資適當配比，取得資本性支出資金，既能有效充實營運及長期資金，又不至於大幅稀釋每股EPS。

新莊分行企盼可以全面性的提供鮮乳坊金融服務，並在其發展過程扮演夥伴關係，一起實踐ESG及社會共好。

◀新莊分行經理張文杰（右二）與創辦人（左二）合影留念

▼創辦人於牧場例行巡診

附記

「鮮乳坊」於源頭把關的創辦人乳牛獸醫師龔建嘉，2022年10月前往荷蘭參訪，以下為其參訪心得分享。

十月初到荷蘭做乳品與酪農產業交流，透過在地朋友的安排，認識不少在地的農民和特色乳品經營品牌與公司。

在這歷史悠久的乳品文化國家當中，他們的牧場牛隻飼養的頭量並不多；對照台灣超過200頭的平均規模，他們僅有不到一百頭牛，許多都是傳承好幾代的小型家庭農民。而這些牧場在乎對於畜牧文化、特色風味，與土地生態和動物的關係。

這讓我想到在幾年前到以色列考察時的觀察，兩個國家很不一樣。

以色列，是個社會主義精神強烈的國家，有許多人民公社形式的農場，利潤共享，並且高度合作。他們的經營思維是高度的資本主義、追求效益最大化，密集精準管理；每頭牛的平均生產乳量，在前幾年超過美國，成為世界第一。在追求產量的同時，也是全世界少數用計劃性生產的配額制來做產銷控管的國家。

荷蘭，是一個乳品歷史豐富且民主思辯成熟的西方國家，透過各種標章與維護的組織來展現他們在乎的價值主張。包括有機奶、放牧奶、母嬰同室奶。例如放牧的牛隻他們同時在乎該地區的植被生物多樣性，而不是單一高效率芻料的栽種。這些價值主張讓產量的追求無法達到最有效率的最大化，因此他們的平均乳量也並不是排名在世界之巔。因為具有成熟的產業生態，從配額制走到現在全部以市場機制定價，但能夠有效分配。

若要用幾個關鍵字來描述，以色列的乳業會是育種、效率、精準管理、科技整合。而荷蘭的乳業是有機、友善、共存、尊重、生物多樣性。而他們能成為世界級的產業，也有一個共同點：強大的合作平台。以色列透過協會與政府的力量，以每瓶販售出去的乳品抽出一個金額比例來成立一個基金，支持長期產業發展與數據分析資料庫，讓乳品廠、獸醫檢驗、牧場動物健康、通路消費等資料等全部開放該國內產業分析與使用。而荷蘭則是透過政府成立基金，提供給瓦赫寧恩大學WUR成立Dairy Campus平台，讓所有的國內企業與協會能夠共享產業研究資源，針對包括動物行為、牛隻溫室氣體排放等重大議題，提升產業永續能量。

台灣雖不是乳業發展歷史悠久的國家，但乳品自給率超過80%，有學習能力強且飼養水準高的農民。當前面對開放國外乳品競爭，台灣酪農事業要走出什麼樣的一條路，取決於我們的思維與追求目的。

銀行業導入網路威脅情資（Cyber Threat Intelligence）機制之探討 - 上

王宏敦

緒論

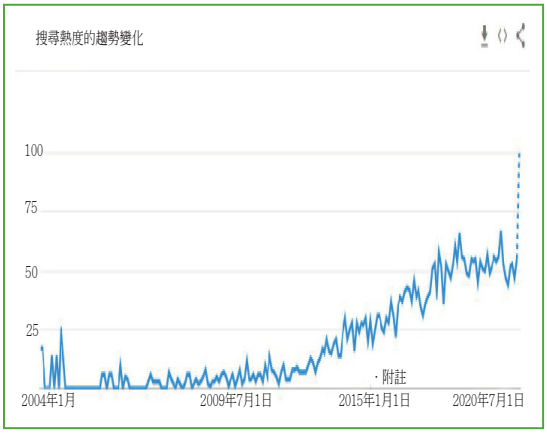
研究背景與動機

為了強化資訊安全，一般企業組織花費的大量資源定期執行弱點掃描、滲透測試、社交工程演練及建置資安事件管理平台等機制，再由漏洞的探測與事件分析，來瞭解企業組織本身在資訊系統架構、人員、及管理流程上的脆弱點進行強化，以減少資安風險，但大多數企業組織並不瞭解想要攻擊自己的駭客所慣用的手法與策略。因此，企業組織與駭客的對抗，長期就是一直保持著敵暗我明的狀態，當駭客花費大量資源鎖定攻擊目標，探測企業組織內部的資安防禦機制、人員、與流程上的脆弱點並進行利用時，企業組織往往因缺乏相關的威脅情報，無法瞭解現行駭客慣用之攻擊手法與流程，而處於劣勢。

本文在探討企業組織如何有效利用網路威脅情資（Cyber Threat Intelligence），來協助瞭解當下所面臨的資安威脅，越能瞭解駭客慣用的攻擊手法與戰略，企業組織就越能立於不敗之地。

以「Cyber Threat Intelligence」作為關鍵字，透過Google關鍵字趨勢分析可發現，自2004年起至今，在全球搜尋熱度仍持續攀升中，由此可見網路威脅情資（Cyber Threat Intelligence）仍為大家所關注的重要資安議題之一。

Google Trend 關鍵字趨勢分析
Cyber Threat Intelligence



資料來源：Google Trend https://trends.google.com.tw

情資彙整分析第一步要能先取得資料，威脅情資的資料來源種類，可依據來源區分為內部與外部情資，內部情資指的是企業組織對於內部資安設備所留下的記錄資料，例如：防火牆、入侵防禦系統、網路設備或主機服務所產生的日誌；而外部情資的來源相當豐富且多元，也是本文探討的重點，例如：資安服務供應商所發布的威脅情資報告、公開來源情報（Open-source intelligence, OSINT）平台提供的情資、國際資訊安全組織（CERT、ISAC等）所發布的資安通報及暗網（Dark Web）論壇等，都是可利用的外部情資來源。

蒐集情資資料後，再對資料進行分析產出可利用之情報，常見分析方式主要為網路攻擊狙殺鏈（Cyber Kill Chain）方式，搭配映射在MITRE ATT&CK資訊安全框架上，對事件行為進行分類，透過分析的結果，調整企業組織對資安檢測方式與環境佈署，擬定對應策略。

2017年金融監督管理委員會為提升金融體系資安防護能量，打造「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」，服務對象包含銀行、保險、證券期貨、投信投顧等各業別金融機構，提供資訊安全事件通報、情資研判分析、資訊安全資訊分享，也是目前本行主要外部威脅情資來源。

依據國家資通安全會報技術服務中心訂定「政府領域聯防監控作業規範」內容要求，本行於2021年完成資訊安全威脅情資傳輸平台（eXtensible Security Operation Center, X-SOC）系統建置，以自動化方式整合本行現有資安事件管理平台（Security Information and Event Management, SIEM）監控數據，傳輸情資至金融領域資訊安全防護（Financial Security Operation Center, F-SOC），並採用資安威脅情資傳輸STIX（Structured Threat Information eXpression）標準格式封裝，回傳資安監控資料至F-SOC進行情資分析，再透過金融單位間情資分享，強化資安事件預警能力，有效提升本國金融產業之資安防禦能量。

研究目的

本研究以「銀行業導入網路威脅情資（Cyber Threat Intelligence）機制」為研究目標，探討網路威脅情資類型、來源與實際應用場景，並藉由本行資訊安全威脅情資傳輸平台（eXtensible Security Operation Center, X-SOC）系統建置為範例，結合金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）與本國F-SOC運作機制，建構出銀行業的威脅情資分析與使用方式，以提供銀行業透過本研究作為網路威脅情資（Cyber Threat Intelligence）導入之參考依據。

第一章 技術文獻

第一節、網路威脅情資（Cyber Threat Intelligence）定義

壹、網路威脅情資（Cyber Threat Intelligence）

全球有許多資安研究機構與資安服務供應商對於網路威脅情資（Cyber Threat Intelligence）一詞進行解釋與說明，本文採用美國國家標準技術研究院（National Institute Of Standard and Technology, NIST）的定義較具權威與代表性，在NIST Special Publication 800-150文件中清楚定義網路威脅Cyber Threat一詞為「經由未經授權的存取、破壞、揭露、修改訊息或阻絕服務，而影響組織運營的情況或事件」。除此之外，也針對威脅情報Threat Intelligence一詞定義為「威脅資訊經過彙整、分析及轉譯後，可提供決策者進行決策之參考依據」。綜合上述，網路威脅情資（Cyber Threat Intelligence）即代表著「未經授權的存取、破壞、揭露、修改訊息或阻絕服務，而影響組織運營的情況或事件，經過資料彙整、分析及轉譯後所形成的情報資訊，可做為決策者進行決策之參考依據」。

貳、威脅情資類型

依據美國國家標準技術研究院（National Institute Of Standard and Technology, NIST）在NIST Special Publication 800-150文件中，對於威脅情資類型共區分為五大類，說明如下：

一、指標（Indicators）

指標（Indicators）指的是在資訊安全技術上可量化之威脅資訊，並明確顯示正在進行或已發生的資安攻擊入侵事實。藉由指標可用於檢測和防禦潛在的資安威脅。常見的指標類型包括以下四個型態：

（一）網際網路協定地址（Internet Protocol Address, IP）：駭客在攻擊過程中，常使用連線中繼站達到遠端控制存取等目的，在此類中繼站常稱之為C&C或C2（Command & Control, C&C）中繼站，中繼站具備命令與控制能力的伺服器服務功能，呈現方式採用網際網路協定地址（Internet Protocol Address, IP）方式呈現。

（二）網域名稱系統（Domain Name System, DNS）：偽冒網站或社交工程之資安威脅資訊可能透過DNS（Domain Name System, DNS）名稱或統一資源定位符（Uniform Resource Locator, URL）方式呈現。

（三）惡意檔案之雜湊值（Hash Value）：雜湊演算法（Hash Function）藉由雜湊值（Hash Value）產生後，無法反推出原來訊息與雜湊值（Hash Value）必須隨明文改變而改變的兩個特性，用來形成檔案唯一之特徵值，也稱為檔案的數位指紋（Digital Fingerprint）藉以偵測比對是否具有同樣檔案存在企業組織內部，以達到預警效果。

（四）惡意電子郵件的主題與內容：藉由惡意電子郵件的主題、內容進行警示，以提升電子郵件社交工程防禦能力。

二、戰術、技術手法和程序（Tactic Technique Procedure, TTP）

戰術、技術手法和程序（Tactic Technique Procedure, TTP）主要在描述攻擊者的攻擊行為。

戰術（Tactic），屬於較高階的威脅資訊，主要讓高階經理人作為防護策略的參考依據，在企業組織營運面臨資訊安全風險時，需要採取那些策略可避免危害。

技術手法（Technique），屬於較低階的威脅資訊，此類型情報資訊週期短、變化快，主要用於資訊安全設備參數調校，透過手動或自動化資安環境部署，可加速資安威脅的偵測與阻擋。

程序（Procedure），主要針對駭客攻擊的技術手法及運作方式描述，例如，惡意軟體、攻擊工具、網路釣魚及系統漏洞之利用等，提供更詳細的說明。

三、安全警報（Security alerts）

也稱為資訊安全建議、公告或漏洞說明，主要針對作業系統、軟體、硬體或韌體等資訊安全漏洞進行說明，並揭露漏洞遭利用後所造成的資安問題，其內容通常是一般人可讀的技術通知。資安警報來源可由計算機應急響應小組（Computer Emergency Response Team, CERT）、資訊安全資訊分享與分析中心（Information Sharing and Analysis Center, ISAC）、美國國家漏洞資料庫（National Vulnerability Database, NVD）、產品資安事件應變小組（Product Security Incident Response Team, PSIRT）及資訊安全服務提供商等單位取得。

四、威脅情報報告（Threat intelligence reports）

通常是描述戰術、技術手法和程序（Tactic Technique Procedure, TTP）、攻擊者、系統類型、攻擊目標資訊及其他威脅相關的訊息，有助於企業組織更瞭解現行資安威脅趨勢的文件。威脅情報是經過整合彙整、分析、解釋後產生豐富詳細的資安威脅資訊，提供資安決策過程中之重要參考依據。

五、系統配置（Tool configurations）

以資訊安全為前提下，針對系統、設備與安全控管機制提供最佳的安全參數設定與建議指導方針，以強化組織之資安防禦能力。例如，如何偵測惡意程式和刪除的實用程序說明，或是如何創建和自定義入侵檢測規則、存取控制清單、防火牆規則或網頁應用程式防火牆過濾配置文件的說明。

參、內部與外部威脅情資

依據依據美國系統網路安全研究機構（System Administration Networking and Security, SANS）將網路威脅情資，依據來源區分為內部及外部兩大類型，詳細說明如下：

一、內部威脅情資（Internal Threat Intelligence）

企業組織分析內部偵測到的相關資訊與系統日誌，以研判及預測潛在的惡意行為。例如，內部員工使用駭客工具軟體、程式等，表面看似隨機且無關的日常事件，經過組織內部的資安團隊透過這些資訊的收集、分析與整理，進一步形成有意義的資安威脅情資。

許多企業組織將大量數據與日誌，傳送到中央監控平台，常使用資訊安全事件管理平台（Security Information Event Management, SIEM），將企業組織內部的資訊設備與相關日誌，進行收容與關聯分析，並建立分析規則產生警事件，提升組織內部對資安事件的應變速度與處理能力。例如，勒索軟體影響該電腦正常業務運作時，企業組織內的資安團隊可透過相關資訊設備日誌，進行事件分析與調查，以偵測出可能的感染路徑、識別惡意軟體所利用的漏洞及觀察其傳播方式進行阻絕，避免災情持續擴大，減少額外的損害。

二、外部威脅情資（External Threat Intelligence）

分為免費及付費兩類，免費威脅情資係指公開發布的惡意網站、中繼站IP位址、釣魚郵件網域、惡意程式檔案雜湊值（Hash Value）等；付費威脅情資則是由專業資安服務供應商提供的資訊，例如，資安監控威脅報告、暗網（Dark Web）駭客市場資訊等。

簡言之，外部威脅情資主要為企業組織從自身外部獲取的威脅情報，由於外部威脅情資通常不是特定且直接適用於組織內部，因此組織內部資安團隊必須花時間評估情報的適用性，外部威脅情資可區分三大類，如下說明：

（一）數據訂閱（Data Feeds）：許多資安威脅情資服務供應商提供數據饋送（Data Feeds），為特定需求類型設置交付機制，採用定期或每隔一段時間發送一次電子郵件，例如，每小時、每天或每週，提供各種不同的交付格式，常見格式有JSON或CSV，也可利用應用程式介面（Application Programming Interface, API）方式與從數據源中提取訊息，藉以取得惡意網站、中繼站IP位址、釣魚郵件網域、惡意程式檔案雜湊值（Hash Value）與暗網（Dark Web）駭客論壇等資訊。

當組織取得威脅情資供應商的報告後，饋送的情資需要經過整理分析，才能應用到企業組織內部環境中，調整防火牆、資安事件管理平台（Security Information and Event Management, SIEM）、端點代理程式和網路設備之相關參數設定。數據饋送還可能包括攻擊者的TTP或研究報告，所有的威脅情資都必須經由內部資安團隊分析彙整後，採取實際行動，以發揮外部威脅情資之價值。

（二）產業別的共通性情資：駭客團體針對不同產業別攻擊時，採用手法與戰術略有差異，而具有相似利益的產業，透過共同創建的資訊共享平台，有助於該產業別的網路威脅情資交換，例如，以本國金融業而言，金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）所提供的資安威脅情資，對於銀行、證券及保險等金融相關產業而言，具備較大的參考價值，也更貼近該產業所面臨之資安威脅。

（三）政府相關情資：許多企業組織藉由政府的力量與支持，取得更具參考價值的威脅情資，例如，美國InfraGard非營利組織是美國企業與聯邦調查局（Federal Bureau of Investigation）之間的公私合作夥伴關係，並提供網路威脅情資和資訊安全知識交流的特殊單位。

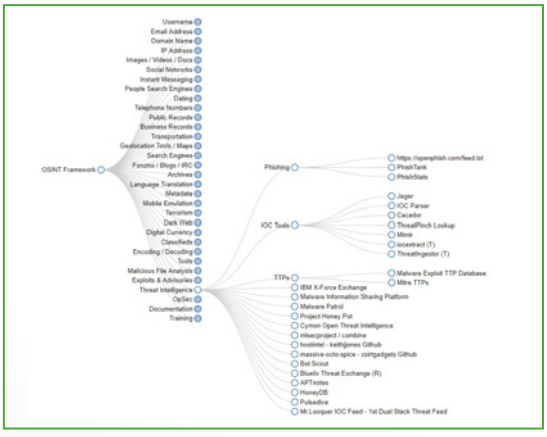
第二節、威脅情資來源

壹、公開來源情報（Open-source intelligence, OSINT）

公開來源情報（Open-source intelligence, OSINT）是從公開來源收集到的情報。以情報機構來看，「公開」是指公然展示的、公眾可見的來源，在OSINT的情報來源包含媒體、社群網路、政府報告、官方數據、觀察報告、學術論文及暗網（Dark Web）等大量公開數據，由於OSINT所蒐集到的資訊是公開的，因此常被企業組織低估其能力與價值。

藉由OSINT Framework顯示的公開資訊中，針對威脅情資（Threat Intelligence）樹狀圖展開如下圖所示：

圖 壹-1 OSINT Framework 威脅情資 Threat Intelligence樹狀圖



資料來源：OSINT Framework https://osintframework.com/

由OSINT Framework之威脅情資（Threat Intelligence）樹狀圖顯示，在展開後項目分為網路釣魚（Phishing）、IOC Tools及TTPs等類別，以下針對常見的重點類別進行說明。

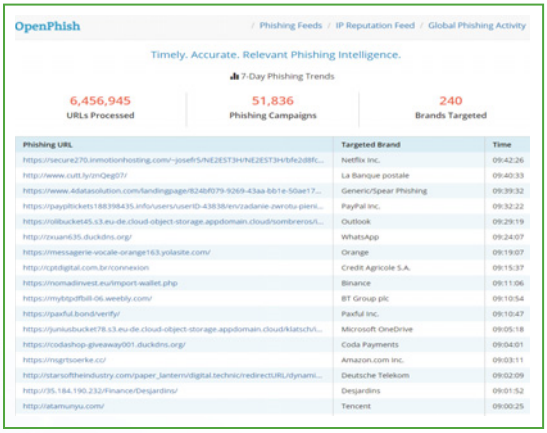
一、網路釣魚（Phishing）

人往往是資訊安全最脆弱的一環，駭客利用人性的弱點，透過社交工程手段進行釣魚信件寄送，誘使組織內部成員開啟信件或點擊惡意連結，此是組織內部若有充足的威脅情資，可用來辨識網路釣魚（Phishing）網站，即可降低企業組織所面臨的資安威脅，阻斷攻擊者的第一步，提升資安防禦上的效益。

在OSINT Framework之威脅情資項目中，網路釣魚（Phishing）項次提供了三個外部情資網站，以下針對主流的釣魚網站情資單位進行說明介紹：

（一）OpenPhish：由OSINT Framework威脅情資（Threat Intelligence）下的網路釣魚（Phishing）類別中，提供的第一個網站為OpenPhish網站，其網址為：https://openphish.com/，該網站可直接取得釣魚網站之威脅情資，內容包含IP、DNS及完整URL，如下圖：

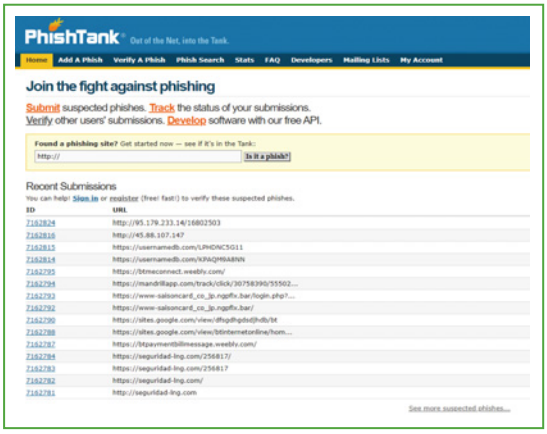
圖 壹-2 OpenPhish 釣魚網站威脅情資圖



資料來源：OpenPhish https://openphish.com/

（二）PhishTank：由OSINT Framework威脅情資（Threat Intelligence）下的網路釣魚（Phishing）類別中，提供的第二個網站為PhishTank網站，其網址為：https://www.phishtank.com/，該網站可以直接取得釣魚網站之威脅情資，內容包含IP、DNS及完整URL外，還提供搜尋介面，提供使用者確認欲連線之網址是否為釣魚網站，如下圖：

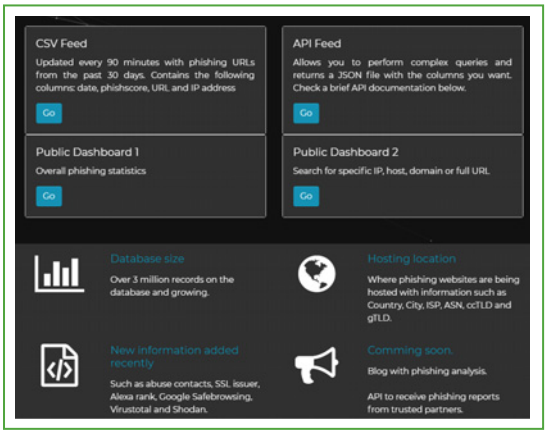
圖 壹-3 PhishTank 釣魚網站威脅情資圖



資料來源：PhishTank
https://www.phishtank.com/

（三）PhishStats：由OSINT Framework威脅情資（Threat Intelligence）下的網路釣魚（Phishing）類別中，提供的第三個網站為PhishStats網站，其網址為：https://phishstats.info/，該網站取得釣魚網站之威脅情資方式有三種，如下圖說明：

圖 壹-4 PhishStats 釣魚網站威脅情資圖



資料來源：PhishStats
https://phishstats.info/

第一種是透過CSV檔案格式直接下載取得情資，威脅情資內容每90分鐘自動更新一次，資料量涵蓋90天的歷史資料；第二種方式是提供API方式與企業組織內部的情資平台對接；最後一種方式採用監控面板（Dashboard）方式呈現釣魚網站相關威脅情資監控資訊，如下圖顯示，近些年釣魚網站藉由SSL憑證加密，試圖規避資安防禦機制的比例逐年上升。

圖 壹-5 PhishStats統計釣魚網站採用HTTPS協定逐年上升

資料來源：PhishStats
https://phishstats.info/

PhishStats網站除了可獲得釣魚信件的網址URL、IP等威脅情資資訊外，並能夠取得釣魚信件的主旨，可提供組織在進行釣魚郵件過濾時的重要參考依據。

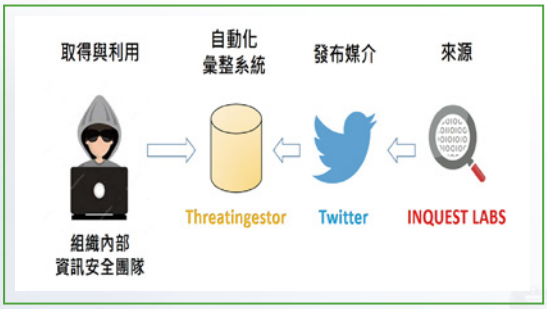
圖 壹-6 PhishStats 釣魚網站威脅情資圖

資料來源：PhishStats https://phishstats.info

二、入侵威脅指標（Indicator of Compromise，IOC）工具

所謂入侵威脅指標（Indicator of Compromise, IOC）工具指的是透過自動化工具進行威脅情資的蒐集與彙整，在OSINT Framework中介紹了許多主流工具，以下將採用ThreatIngestor工具搭配InQuest威脅情資機構作為情資來源，並以Twitter為情資傳遞媒介，進行自動化威脅情資收集與利用，示意圖如下。

圖 壹-7 Threatingestor平台運作示意圖



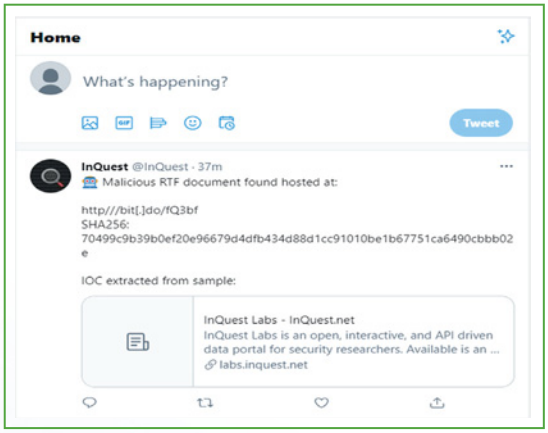
資料來源：本研究整理

InQuest 資安威脅情資機構主要提供資安威脅預防、檢測和追蹤服務，統計時間截自本研究為止，在InQuest Labs中的IOC資料庫，惡意網域資料高達145,715筆、惡意檔案雜湊值（Hash Value）共計67,484筆，惡意中繼站IP位址共計94,079筆及惡意釣魚網址共207,279筆。

InQuest機構藉由Twitter、Github和Blog等媒體，發布大量開源情報（OSINT）以供資安分析師進行研究，而企業組織內部資安研究團隊，可建置ThreatIngestor平台，自動化收集所需要的威脅情資，以提供組織進行資安防禦之參考依據。

以下透過實作ThreatIngestor平台方式，介紹威脅情資（Threat Intelligence）之取得與利用方式，首先透過Twitter社群軟體帳號，跟隨InQuest機構後，即可自動且不定時收到InQuest機構所提供的威脅情資，內容包含有惡意網址URL、檔案雜湊值（hash value），及惡意程式樣本分析報告，如下圖：

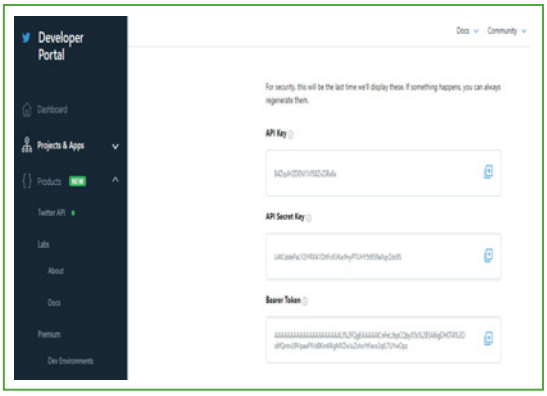
圖 壹-8 由社群軟體Twitter取得InQuest機構提供之威脅情資



資料來源：Twitter

再透過Google雲端服務（Google Cloud Platfor, GCP）架設Ubuntu作業系統，並於Ubuntu作業系統進行ThreatIngestor平台建置，同時依循Twitter Developer申請作業流程，進行API Keys與Token等相關服務申請，在Twitter完成審查作業後，取得API key、API secret key、Access Token與Access Token secret資料，如下圖：

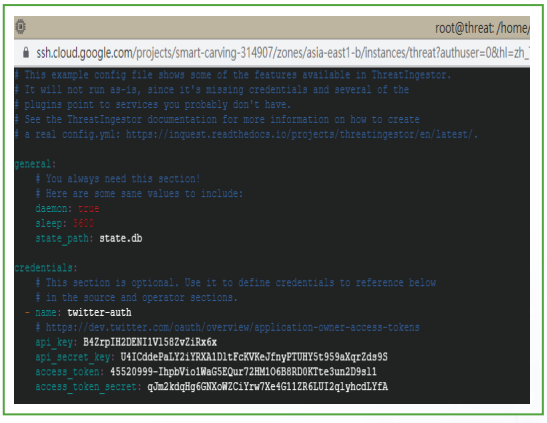
圖 壹-9 申請Twitter Developer取得API Key



資料來源：Twitter Developer

即可開始進行ThreatIngestor平台建置，並與Twitter API進行串接參數設定，部分參數設定如下圖：

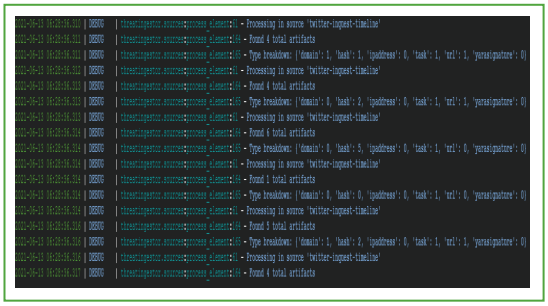
圖 壹-10 由ThreatIngestor平台與Twitter API串接部分參數設定



資料來源：本研究整理

完成ThreatIngestor平台參數設定後，定時自動化取得InQuest的威脅情資（Threat Intelligence），如下圖：

圖 壹-11 由ThreatIngestor定時自動取得InQuest機構威脅情資Threat Intelligence



資料來源：本研究整理

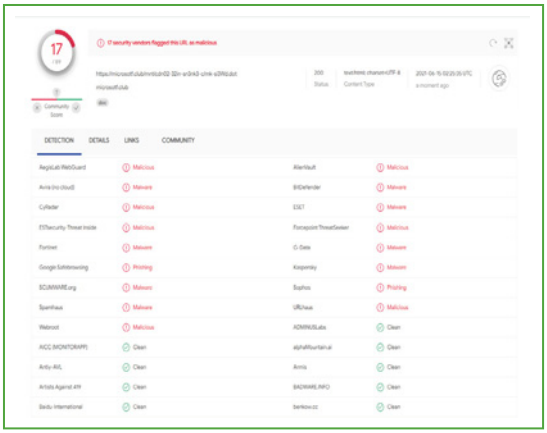
檢視ThreatIngestor平台所取得的InQuest組織所提供的威脅情資（Threat Intelligence）後，經過企業組織內部資安團隊整理、分析後，可將惡意網址、短網址及惡意檔案雜湊值（hash value）進行匯入組織內部資安防禦設備進行偵測與阻擋，以提升資安防禦能力，如下圖：

圖 壹-12 由ThreatIngestor威脅情資Threat Intelligence展現畫面

資料來源：本研究整理

由上圖為例，第一筆取得的威脅情資（Threat Intelligence）為https///microsotf.club/mnt/cdn02-32in-sn3nk3-c/mk-si3Wd[.]dot，由網址列詳細檢查即可發現，雖然網站採用SSL加密，但微軟網域名應該為microsoft，而此網址為microsotf進行偽冒，再經由VirusTotal分析後認定惡意網站，該威脅情資（Threat Intelligence）由InQuest機構揭露後，經過了48小時，全球仍僅約17家資訊安全廠商可辨識該惡意網址，如下圖：

圖 壹-13 由VirusTotal比對InQuest的威脅情資Threat Intelligence內容



資料來源：VirusTotal

三、戰術、技術手法和程序（Tactic Technique Procedure, TTP）

依據美國國家標準技術研究院（National Institute Of Standard and Technology, NIST）針對戰術、技術手法和程序（Tactic Technique Procedure, TTP）情資類型屬於較高階的資安威脅資訊。主要讓高階經理人作為資安防護策略的參考依據，在企業組織營運面對的資安風險時，採取那些策略可讓組織降低或避免危害。

在OSINT Framework中針對戰術、技術手法和程序（Tactic Technique Procedure, TTP）介紹了幾個主要的資訊安全機構，本章節將以MITRE ATT&CK框架進行說明介紹。

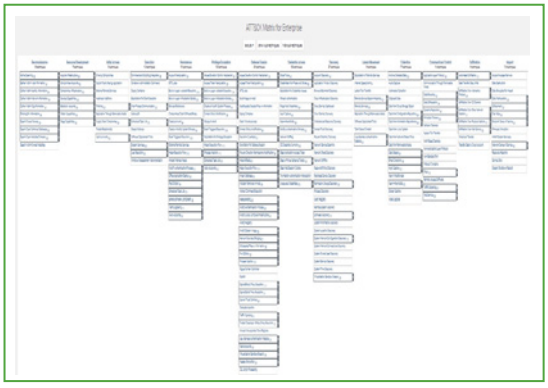
（一）Mitre Corporation介紹：Mitre Corporation是一個非營利組織單位，總部位於美國馬薩塞州，起源於第二次世界大戰期間的麻省理工學院（Massachusetts Institute of Technology, MIT）的實驗室，並於1958年後自MIT分離出來。

MITRE除了協助資訊安全相關研究，也負責維運通用漏洞揭露（Common Vulnerabilities and Exposures, CVE）與通用弱點列表（Common Weakness Enumeration, CWE），並於2015年5月正式發起「MITRE ATT&CK框架」的資訊安全研究計畫。

（二）MITRE ATT&CK介紹：早期的資安防禦策略以防禦面為主，例如，縱深防禦、漏洞修補、佈署資安防禦設備等，由駭客發動攻擊後，再依據組織所產生的傷害，擬定補救措施與未來的預防策略，如此往往陷入被動守勢而受制於攻擊者；而MITRE對此做出反向思考，試圖由駭客的攻擊的動機、目的、技術、方法，建立攻擊者的威脅模型，並做出因應對策，在駭客發動攻擊前，緩解攻擊力道，以降低資安風險。

MITRE維運通用漏洞揭露CVE與通用弱點列表CWE兩項資安威脅指標後，CVE與CWE獲得資安業界、硬體供應商及軟體服務商等機構的高度注目與採用，並作產品弱點補救及預防的重要參考依據之一；而MITRE藉由彙整CVE、CWE的經驗，來分析與探討駭客攻擊動機、採用的技術與方法，進一步規劃出「ATT&CK」資安威脅模型，透過矩陣形式詳細列舉出已知的攻擊技術與方法，並分析攻擊者發動攻擊前的布局與攻擊後的影響，企業組織可利用ATT&CK的資安威脅模型，以見招拆招方式，限縮攻擊者的攻擊的構面，達到「知己知彼者，百戰不殆」，減少攻擊者對企業組織造成的資安衝擊與危害。

圖 壹-14 MITRE ATT&CK Matrix for Enterprise資安威脅模型



資料來源：MITTRE ATT&CK

MITRE的ATT&CK威脅模型中，目前共有14類，高達367種以上的攻擊技術，模型中的資安威脅情境包含Windows、MacOS、Linux、Network及Containers等作業環境，以及Office 365、Azure、Google等雲端平臺，各類型簡述如下：

1. 偵察（Reconnaissance）：攻擊者在發動攻擊前，摸索入侵途徑的方法，共10種技巧。
2. 資源開發（Resource Development）：攻擊者藉由偵查後進一步的開戶、帳號申請等行為，取得相關資源，共7種技術。
3. 初始訪問（Initial Access）：攻擊者透過網路釣魚、供應鏈攻擊技巧進行初始訪問，共9種技術。
4. 執行（Execution）：攻擊者執行惡意程式碼和惡意指令的方法，共12種技術。
5. 持續性（Persistence）：攻擊者成功侵入系統後，能保持伏擊狀態的方法，共19種技術。
6. 權限提升（Privilege escalation）：攻擊者可藉由奪取更高權限來控制受害系統的方法，共13種技術。
7. 防禦規避（Defense evasion）：攻擊者在發動攻擊的同時，繞過系統防禦機制的方法，共39種技術。
8. 憑證存取（Credential access）：攻擊者得到使用者合法登入認證來發動攻擊的方法，共15種技術。
9. 探索（Discovery）：駭客能窺探系統內敏感個人資料和關鍵資訊的種類，共27種技術。
10. 橫向移動（Lateral movement）：攻擊者成功入侵一個系統環境後，對下一個系統環境下手攻擊的方法，共9種技術。
11. 蒐集（Collection）：攻擊者能盜取資料的方式，共17種技術。
12. 指揮與控制（Command & control）：攻擊者奪取系統控制權後，能介入操控的方法，共16種技術。
13. 滲出（Exfiltration）：攻擊者能夠攜出、外流敏感個人資料和關鍵資訊的方法，共9種技術。
14. 衝擊（Impact）：攻擊者成功滲透系統後，對系統造成的危害種類，共種13類型。

MITRE的ATT&CK威脅模型詳述了各種攻擊型態與方法，做為資安專業和軟硬體業者重要參考依據，瞭解已知攻擊者最有可能發動的攻擊的方式，以提前完成資安規劃與部署，擬定相關因應對策，減少駭客攻擊時對系統所造成的衝擊與影響。

MITRE的ATT&CK威脅模型出現後，能讓資安專家更清楚攻擊者可能的模式與途徑，並針對駭客最常發動攻擊手法提前擬定因應對策，並部署相關資安防禦機制。MITRE的ATT&CK威脅模型不僅能預防突發性的駭客攻擊事件，也能藉由平時收集的威脅情資來源進行分析，預防駭客採用進階持續性威脅（Advanced Persistent Threat, APT）之攻擊手法，也能幫助資安專家、軟硬體廠商，藉由MITRE的ATT&CK威脅模型的協助，積極做好漏洞修補、機敏資訊加密等資安作為，以減少企業組織所面臨的資安風險。

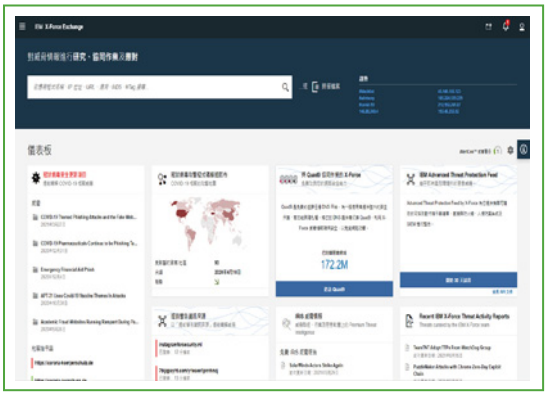
四、OSINT Framework之威脅情資（Threat Intelligence）

除了網路釣魚（Phishing）、IOC Tools及TTPs等類別之外，也提供專業資訊安全廠商或組織的情報資訊，例如，IBM X-Force Exchange、Project Honey Pot、HoneyDB、Mrlooquer，針對以上幾個主流的資安威脅情資來源，個別進行介紹。

（一）IBM X-Force Exchange：IBM X-Force是全球知名大廠IBM公司所成立的資安研究團隊。資安專家會從各式各樣的資安威脅情資來源進行監控、分析其內容，並提供更精準的資安威脅情資，IBM X-Force Exchange提供開放式平台，每分鐘更新即時威脅情資，並提供軟體監控超過250億個網頁，檢測是否有資安疑慮，超過96,000個漏洞分析資料庫作為支援，其中提供數百萬垃圾郵件、網路釣魚攻擊及惡意IP位址之威脅情資，並具備API功能，可整合第三方資安威脅情資，使情資來源更為豐富完整。

申請帳號登入IBM X-Force Exchange平台後，在監控面板顯示多種不同類型的即時威脅情資，如下圖：

圖 壹-15 IBM X-Force Exchange監控平台

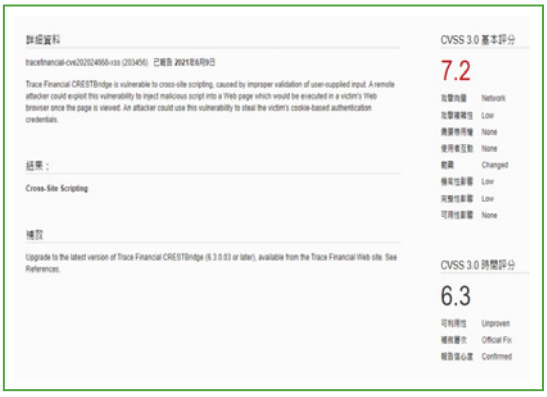


資料來源：IBM X-Force Exchange

除了一般資安威脅情資平台常見的惡意中繼站IP位址及釣魚網站外，同時也提供了漏洞報告與事件響應和情報服務（Incident Response and Intelligence Services, IRIS）報告，針對這兩種類型的資安威脅情資內容進行介紹：

1. 漏洞報告：此報告會針對漏洞事件的內容進行詳細說明，提供影響範圍與補救措施，並提供CVSS 3.0版本的評分，評分內容具備攻擊向量、攻擊複雜性機密性、完整性及可用性影響等參考資訊，如下圖：

圖 壹-16 IBM X-Force Exchange漏洞報告

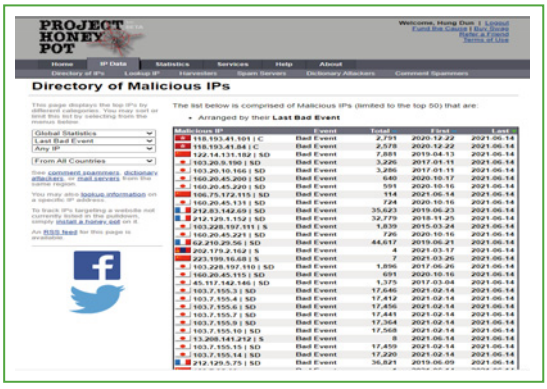


資料來源：IBM X-Force Exchange

2. 事件響應和情報服務（Incident Response and Intelligence Services, IRIS）報告：IBM X-Force IRIS威脅情資分為付費版與免費版本，免費版本報告內容提供威脅類型、概述、威脅指標、建議與參考等資訊，可提供組織內部之高階經理人進行資訊安全計畫擬定及防禦措施之參考依據。

（二）Project Honey Pot：蜜罐計劃Project Honey Pot主要功能在於識別垃圾郵件，參與Project Honey Pot的網站管理者只需在網站上安裝Project Honey Pot軟體即可完成密罐佈署。藉由該平台分析、處理後，所取得的數據，協助企業組織提早發現垃圾或釣魚郵件發送者，進行垃圾郵件過濾系統之參數調整，以降低企業組織內部員工收到釣魚信件或商業電子郵件詐騙（Business E-mail Compromise, BEC）機會，以提升企業組織之資安，蜜罐計劃Project Honey Pot網站提供惡意的IP位址，如下圖：

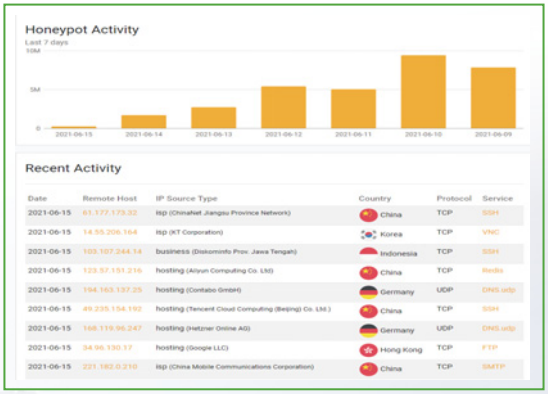
圖 壹-17 蜜罐計劃Project Honey Pot提供惡意IP位址



資料來源：Project Honey Pot

（三）HoneyDB：HoneyDB主要是利用大量參與者使用密罐（Honeypot）佈署，記錄網際網路上的駭客發動的攻擊行為，藉由分析、處理後，所取得的數據。該數據提供攻擊者的IP位址與使用的服務類型，例如，HTTP、FTP、SSH、VNC、SMTP及DNS等通訊協定，如下圖：

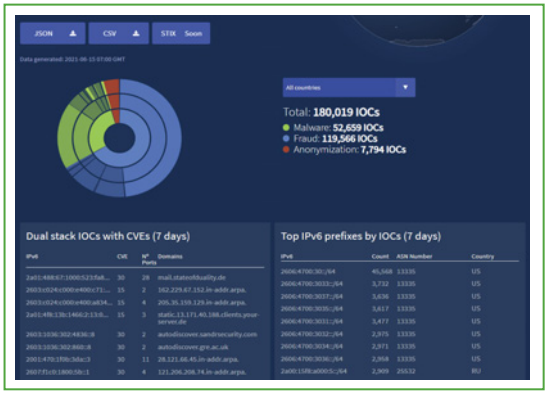
圖 壹-18 HoneyDB提供惡意IP位址與服務



資料來源：HoneyDB

（四）Mrlooquer：由於目前網際網路IP位址的使用仍以IPv4協議為主，因此一般的威脅情資來源，若針對惡意IP也採用IPv4協定，但近些年來，關於IPv6 協議的攻擊事件日益漸增，而Mrlooquer是少數提供IPv6協議的IP威脅情資來源，若企業組織已開始使用IPv6協議提供服務，Mrlooquer更是重要的資安威脅情資來源，如下圖：

圖 壹-19 Mrlooquer提供惡意IPv6協議位址



資料來源：Mrlooque

貳、金融資安資訊分享與分析中心（F-ISAC）

近年來全球金融科技快速發展，使用創新金融業務已成各金融機構主要競爭策略，而如何健全整體金融產業發展，保護消費者資訊安全與隱私，維持金融秩序穩定，成為全球國家金融監理單位的重要課題之一。

美國紐約州金融服務署（New York Department of Financial Services, NYDFS）於2017年發布「金融服務業網路安全規範」，要求受監理機構應遵循特定網路安全標準及訂定以風險基礎的網路安全計畫。我國金融產業透過「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」進行資訊安全威脅情資交流與共享，並以系統性分析、預防資訊安全事件的發生，提升金融產業之資訊安全防禦能量。

網路攻擊事件隨著金融科技快速發展，其攻擊技術與手法變得更多元且複雜，資安威脅情資的共享與取得也就相對重要。全球主要國家陸續設立金融資訊安全資訊分享與分析機構，例如，美國的 Financial Services Information Sharing and Analysis Center （FS-ISAC）、英國的Cyber Security Information Sharing Partnership（CiSP）等資訊安全分享中心。我國行政院為建構國家資訊安全聯防體系，推動八大關鍵領域，並建立資訊安全資訊分享機制，「金融」為其領域之一。如下圖：

圖 壹-20 N-ISAC八大關鍵領域資訊安全分享架構

資料來源：財金資訊季刊

金融監督管理委員會於 2017 年 12 月正式成立「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」，並交由財金資訊公司營運，服務範圍包含銀行、保險、證券期貨、投信投顧等金融業別，目前已有 3 百餘家金融機構加入成為會員，並藉由資訊安全威脅情資分享，協助金融機構因應來自全球的資訊安全威脅。

以下針對「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」與「金融領域資訊安全防護（Financial Security Operation Center, F-SOC）」之服務與發展狀況進行說明。

一、「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」提供下列服務

（一）資安威脅情資的研判分析：蒐集及分析國內外金融資安情資，提供情資研析報告，並適時發出警訊予金融機構。

（二）資訊安全資訊分享：建置金融機構間資安情資通報分享機制，並與政府、通訊等其他領域進行情資交換及聯防。

（三）警訊分享服務：接收金融機構通知之資安警訊，並可依威脅等級發布緊急資安情資通報，以提供金融機構事先防範。

（四）資訊安全諮詢與教育訓練：提供資安諮詢與漏洞評估服務及辦理相關資安研討會。

（五）協助資安事件應變處理：依金融機構之資訊安全事件，引介專業資安廠商或組織，以提供相關之資安技術與數位鑑識支援服務。

（六）建立資安事件改善之良性循環：依據國內外重大資安事件，探究問題發生原因、事件應變處置程序等，檢討分析攻擊事件，以提升金融機融之資安防禦能量。

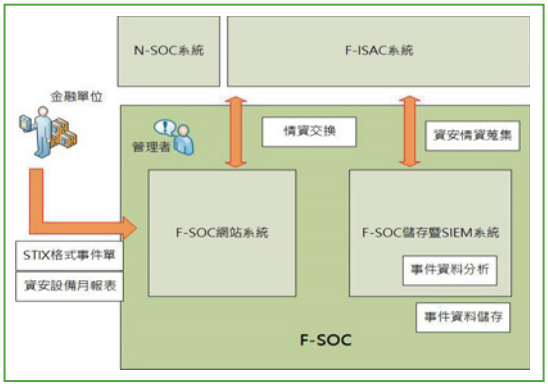
二、「金融領域資訊安全防護（Financial Security Operation Center, F-SOC）」

透過全球各國不同的資安機構取得威脅情資，再分享給國內各金融機構，雖然可提供本國金融機構作為資安防禦上的參考依據，但以資安在聯合防禦的概念而言，建立本國金融機構的威脅情資分享平台，在資安上可獲得更高的效益。

「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」為強化國內金融機構資安威脅情資交流，於2020年推動「金融領域資訊安全防護（Financial Security Operation Center, F-SOC）」平台建置，透過各金融機構與參加單位分享資訊，建置共同監控及防禦機制，以達成國內金融體系之資安分享與聯合防禦能力。

國內各金融單位透過資安威脅情資STIX（Structured Threat Information eXpression）標準格式，提供資安情資給F-SOC，再由F-SOC、N-SOC及F-ISAC單位間進行資安威脅情資的蒐集與交換，示意圖如下：

圖 壹-21 金融單位、N-SOC、F-ISAC與FSOC資訊安全情資分享架構



資料來源：彰化銀行X-SOC建置專案

自2020年由「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」所推動的「金融領域資訊安全防護（Financial Security Operation Center, F-SOC）」平台，目前已完成本國多家金融單位介接完成，其主要功能如下：

（一）建立資安事件監控記錄，並導入資安威脅情資之接收與上傳機制。

（二）收容有關金融相關領域層級之資安事件監控記錄。

（三）組織內部之資安事件分析、審核、追蹤及資安監控記錄。

（四）掌握金融相關領域之整體資安現況及威脅。

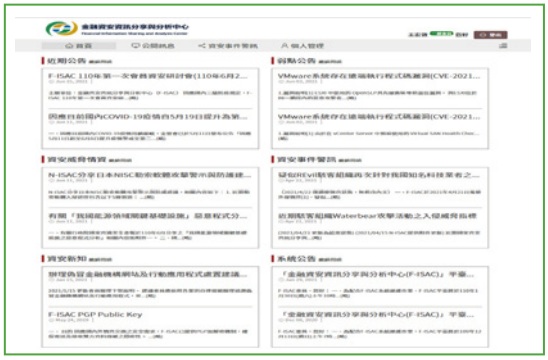
（五）跨產業類別之資安聯合防禦分析與威脅情資之回饋。

（六）制定金融機構監控組態基準及作業指引。

（七）持續擴大推動金融機構參與二線資安監控之中長期計畫，為發展人工智能AI SOC計畫進行準備。

三、「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」所提供之內容可分為六大類別如下圖，以下針對各類別進行介紹：

圖 壹-22 金融資安資訊分享與分析中心所提供之內容



資料來源：F-ISAC網站

（一）近期公告：主要內容為針對F-ISAC進行的公告事項，例如，資訊安全相關研討會資訊或政府相關法令等。

（二）弱點公告：主要內容為針對系統、軟體相關的漏洞與弱點進行揭露，並提漏洞說明、已揭露攻擊程式碼說明、影響平台、CVSS向量、建議措施及緩解措施等資訊。

（三）資安威脅情資：提供全球重大資安威脅情資之分析報告，報告中詳細說明攻擊方式、途徑、流程、影響範圍、漏洞編號、建議之防禦措施等資訊，並提供相關分析報告供會員下載使用，例如，惡意程式分析報告及入侵威脅指標，常見的入侵威脅指標內容包含檔案名稱、檔案雜湊值（Hash Value）、惡意網址及惡意中繼站IP位址等資訊。

（四）資安事件警訊：提供近期資安相關事件的警訊，如國際駭客組織的活動或是重大資安事件資訊，並提供相關入侵威脅指標。

（五）資安新知：揭露最新的資安相關攻擊技術、戰略與威脅趨勢，並提供建議、處置措施與問題解決方案，以提升本國金融機構整體資安防禦能量。

（六）系統公告：針對「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」系統維修、停機時間等系統相關作業公告資訊。

四、資安威脅情資共享的保密原則

針對資安威脅情資分享範圍的限制，多數ISAC組織參考「國際資安事件應變安全組織（Forum of Incident Response and Security Team, FIRST）」制定的Traffic Light Protocol, TLP協定。

TLP 依據情資的類型、提供者的要求及可分享的對象，將資安威脅情資分享區分為：紅燈（Red）、黃燈（Amber）、綠燈（Green）及白燈 （White）4個層次，以協助相關企業組織及成員清楚瞭解如何共享情資，並建立有效溝通與互相信賴的運作模式。

TLP 燈號類別說明彙整如下表所示（詳情請參考FIRST網站：https://www.first.org）。

表 壹-1 國際資安事件應變安全組織制定 Traffic Light Protocol （TLP）協定

類別	條件	分享範圍
紅燈 (Red)	資訊無法被他方有效處理，且遭誤用可能影響某方的隱私、聲譽或營運。	僅限提供者指定的特定群組，以面對面、或口頭方式交換。
黃燈 (Amber)	資訊需有效處理，惟分享至外部組織對於某方的隱私、聲譽或營運可能有風險。	接收者只可分享需瞭解的組織成員及廠商，以進行必要的處理；但提供者仍可自由指定特定的資訊分享限制。
綠燈 (Green)	資訊對組織成員及相關群組有用。	接收者可與組織成員或夥伴（如廠商或客戶）分享，但不得公開散布。
白燈 (White)	資訊遭誤用的風險極小或無可預見。	在標準版權規則下，可以無限制散布。

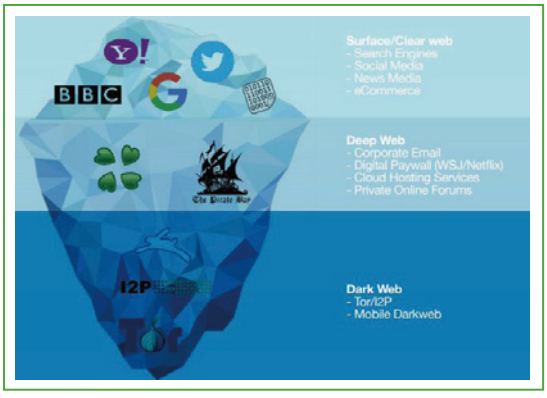
資料來源：F-ISAC網站

參、暗網（Dark Web）

關於網路威脅情資（Cyber Threat Intelligence）的來源有相當多的管道可以取得，如本文所提到的透過公開來源情報（Open-source intelligence, OSINT）及金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）等，均可以提供組織獲得大量的網路威脅情資，而來自暗網（Dark Web）的威脅情資，由於取得難度較高，也往往被大家所忽略。

1990年代中期，美國海軍研究實驗室的研究員為了保護美國線上情報系統而開發了洋蔥路由（Onion routing）。洋蔥路由是一種在電腦網路上匿名溝通的技術，在洋蔥路由網路中，訊息經過一層一層的加密包裝成像洋蔥一樣的封包，並經由一系列被稱作洋蔥路由器的網路節點傳送，因透過這一系列的加密包裝，每一個網路節點（包含目的地）都只能知道上一個節點的位置，無法知道整個傳送路徑以及原傳送者的位址，提供暗網（Dark Web）使用者高度的匿蹤特性，相較於一般使用者所慣用的網際網路而言，暗網（Dark Web）猶如冰山下的部分，藏在深不可見的海底，示意圖如下：

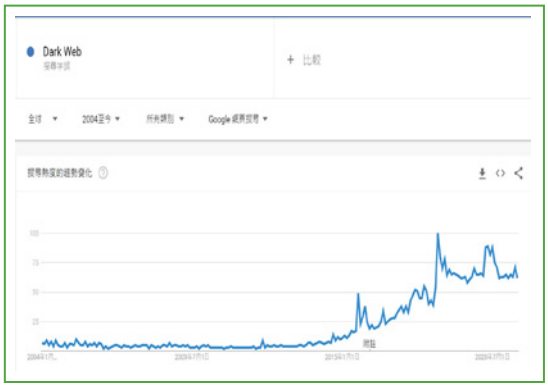
圖 壹-23 暗網（Dark Web）示意圖



資料來源：iThome網站

以「Dark Web」作為關鍵字，使用Google關鍵字趨勢分析可發現如下圖，自2004年起至今，在全球搜尋熱度仍持續攀升中，由此可見暗網（Dark Web）仍為大家所關注的資訊安全議題之一。

圖 壹-24 Google Trend 關鍵字趨勢分析（Dark Web）



資料來源：Google Trend
https://trends.google.com.tw

由於暗網（Dare Web）的威脅情資來源相當隱密，資訊安全服務供應商通常透過專門的團隊與技術，由暗網取得相關資安威脅情資，再以付費訂閱方式提供給企業組織，著名的資安服務供應商有Cyberint、IntSights及SecBuzzer等服務與產品，均可提供暗網（Dark Web）相關的資安威脅情資，企業組織在訂閱威脅情資服務後，再透過組織本身所要密切關注的是識別資料進行監控與蒐集，例如，與組織本身有關的公司名稱、網域名稱、品牌名稱，以及公司高層姓名、電子郵件信箱、與應用系統、網路服務相關的手機App應用程式、社交網站官方頁面、外部IP位址或是在特定產業下所用的識別資料，如金融服務相關的銀行帳戶號碼（BIN NUMBERS）、銀行匯款路線代號（ROUTING NUMBERS）、銀行國際代碼（SWIFT CODES）等機敏資訊。

以下透過幾個比較著名的暗網（Dark Web）位址進行說明，依據資安威脅情資的內容區分為以下兩種類型，分別為零時差系統漏洞與企業組織之機敏資訊，詳細說明如下：

一、零時差系統漏洞資訊

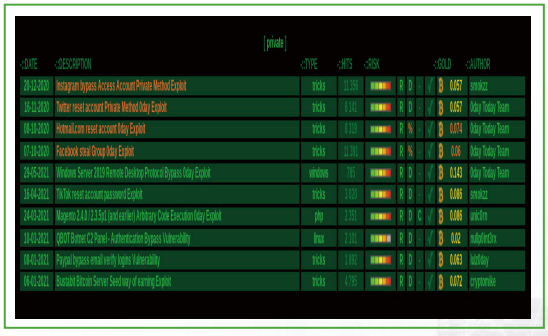
一般企業組織針對系統漏洞往往是透過資訊安全服務供應商通報，或是定期以弱點掃描及滲透測試作業等方式進行揭露，而漏洞是否能有效修補取決於資安服務供應商釋出修補程式的速度，但暗網（Dark Web）中提供大量的零時差系統漏洞資訊進行販售，企業組織內部資安團隊可透過暗網（Dark Web）的資訊蒐集分析，以提前在資訊安全服務供應商通報前，擬定因應對策並執行資安架構調整。以暗網（Dark Web）著名的0day.today就經常揭露零時差系統漏洞資訊，並以高價位販售exploit code，如下圖所示：

圖 壹-25 暗網0day.today零時差系統漏洞販售網站

資料來源：暗網0day.today

由上圖所示，在0day.today網站中，可透過加密貨幣購買最新的零時差系統漏洞exploit code，如下圖所示：

圖 貳壹-26 暗網0day.today零時差系統漏洞販售資訊-1



資料來源：暗網0day.today

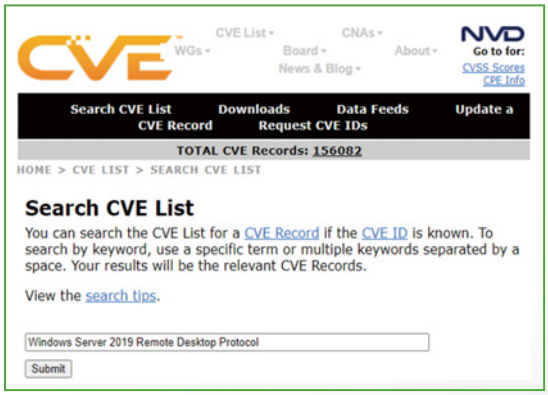
以微軟作業系統Windows Server 2019 Remote Desktop Protocol Bypass 0day Exploit為例，購買exploit code需要花費0.143顆比特幣，如下圖所示：

圖 壹-27 暗網0day.today零時差系統漏洞販售資訊-2

資料來源：暗網0day.today

依據漏洞相關資訊，以關鍵字Windows Server 2019 Remote Desktop Protocol透過CVE通用漏洞資料庫查詢，如下圖：

圖 壹-28 CVE通用漏洞揭露資料庫查詢-1



資料來源：CVE通用漏洞揭露資料庫

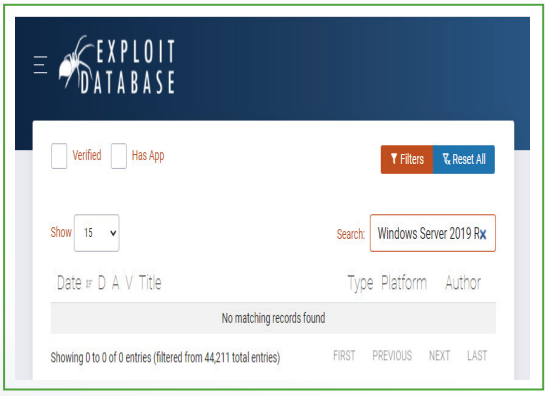
並未查詢到Windows Server 2019對應的漏洞資訊，如下圖：

圖 壹-29 CVE通用漏洞揭露資料庫查詢-2

資料來源：CVE通用漏洞揭露資料庫

另外再透過Exploit DB漏洞資料庫進行查詢，以關鍵字Windows Server 2019查詢，仍然是找不到對應的系統弱點資訊，如下圖：

圖 壹-30 Exploit DB漏洞資料庫查詢畫面



資料來源：Exploit DB漏洞資料庫

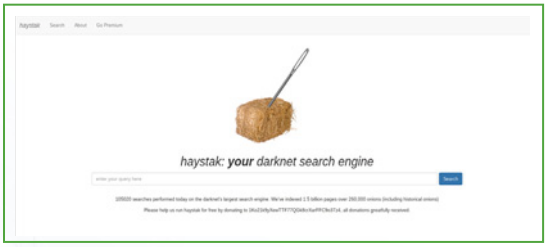
由此可知，此案例為零時差漏洞資訊，當企業組織內部資安分析人員發現暗網（Dark Web）已經有Windows Server 2019 Remote Desktop Protocol Bypass的零時差系統漏洞販售資訊時，並且有現成的exploit code，就應該立即針對組織內部系統進行清查盤點，針對Windows Server 2019版本作業系統之遠端桌面服務，進行強化與其他資安補強措施，如此即可有效利用暗網（Dark Web）情資，在駭客發動攻擊前，強化資安防禦能力，降低資安風險。

二、企業組織之機敏資訊

由於暗網（Dark Web）所具備的匿蹤特性為犯罪者所喜愛，許多非法交易常出現在地下論壇，企業組織內部資安人員，可透過幾個主要知名的暗網搜尋引擎，針對組織網域、電子信箱、金融服務相關的銀行帳戶號碼（BIN NUMBERS）、銀行匯款路線代號（ROUTING NUMBERS）、銀行國際代碼（SWIFT CODES）等機敏資訊進行搜尋，可直接快速搜尋到是否有地下論壇談論到該企業組織或販賣相關之機敏資料。

（一）Haystack：可搜索暗網.onion網站服務，並在其數據庫中索引260,000個網站，包括的15億個歷史頁面資料，如下圖：

圖 壹-31 Haystack查詢畫面



資料來源：暗網Haystack

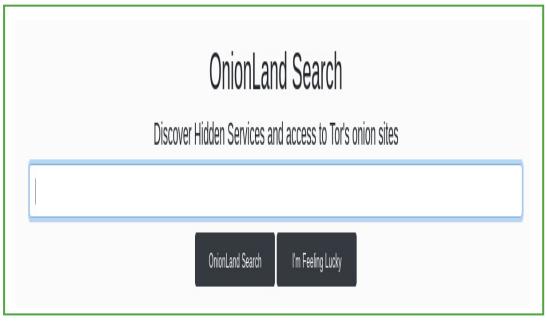
（二）Torch：可搜索暗網超過450,000網站服務的搜索引擎，如下圖：

圖 壹-32 Torch查詢畫面

資料來源：暗網Torch

（三）Tor Onionland：可搜索暗網超過57,000網站服務的搜索引擎，如下圖：

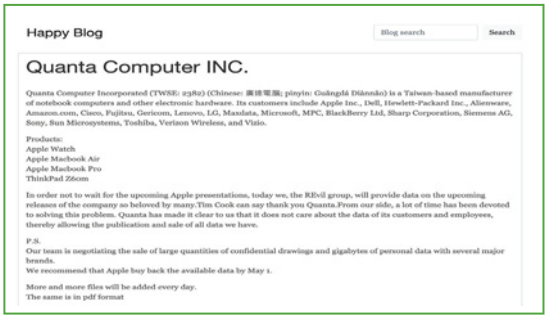
圖 壹-33 Tor Onionland查詢畫面



資料來源：暗網Tor Onionland

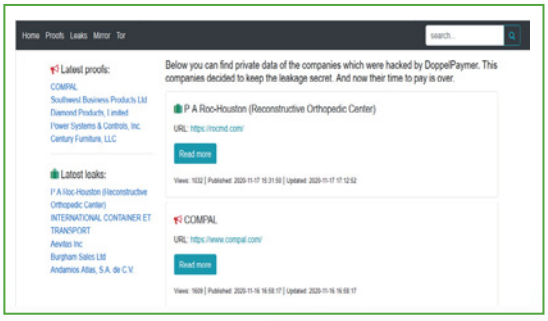
除了透過暗網搜尋引擎查詢來檢視自身組織是否有機敏資料外洩外，也可透過幾個主要暗網的資料外洩網站定期確認，檢視是否有合作廠商遭受攻擊，以減少供應鏈攻擊（Supply Chain Attack）事件發生之可能性，如下圖：

圖 貳-34廣達電腦遭勒索畫面截圖



資料來源：暗網Happy Blog

圖 壹-35仁寶電腦遭勒索畫面截圖



資料來源：暗網Dopple Leaks

～待續～