勒索軟體已然成為企業最大威脅

勒索軟體已然成熟，威脅程度如今已與 APT 不相上下，因為攻擊者使用更好的工具，還會從先前的錯誤中學習。

文／Lucian Constantin 譯／Nica 校／曹乙帆

多年年來，勒索軟體攻擊已然成熟，採用的技術更隱秘也更精細，同時又修正許多先前反覆出現的實作失誤。甚至，部份攻擊如今已經得到更新穎的資料洩密元件，公司受到的傷害不僅止於與勒索軟體相關的傳統資料遺失。

多年趨勢觀察指出，這些攻擊非但沒有消失，而且可能頻率越來越高。

轉移目標

勒索軟體起初威脅的是消費者，展現了恐嚇軟體攻擊更具激進的演化，後者以欺瞞人們支付偽造費用的方式，或購買惡意流氓軟體修補不存在的問題。雖然早期此類攻擊戰已證實對網路犯罪集團而言有利可圖，但消費者勒索軟體版圖已飽和。由於消費者防毒公司改善了勒索軟體偵察能力，為了盡可能得到更多受害者而廣泛撒網，變成沒有效率的技巧。

在2019年八月釋出的一份觀察2018年第二季與2019年第二季間勒索軟體演化的報告中，資安公司Malwarebytes指出：「這個曾經危險但近幾年處於休眠狀態的威脅，如今正大規模捲土重來，從大量針對消費者的惡意活動，轉為針對企業的高目標性、客製化攻擊。」

在這段分析期間，企業環境下的勒索軟體偵測數量增加365%，但消費者面的偵測數量卻下降。2019年接下來的日子這樣的趨勢一直持續著，Malwarebytes Labs 主管 Adam Kujawa 如此表示。「我們發現整體重點都在企業上，各種感染方式皆有增無減，」他如此告知CSO。「有很大的原因是，今日感染企業要比過去幾年容易許多，永恆之藍(EternalBlue)【譯註：美國國安局打造的攻擊程式】與其他漏洞攻擊程式就是因為如此而泛濫。」

EternalBlue可說是專門針對 Microsoft Server Message Block（SMB）通訊協定實作弱點（於2017年三月完成修補）的漏洞攻擊程式，影響及於Windows所有版本。此乃WannaCry、NotPetya與其他勒索軟體蠕蟲，透過公司網路在2017年重擊全球許多企業組織的主要散播方式。

「這或許並非企業越來越注重此類攻擊的唯一原因，但我認為WannaCry與NotPetya所做的事揭露了企業資安的薄弱環節，」Kujawa說道。在此之前，或許很多人會認定這些擁有資安團隊的大型企業是駭客難以突破的，但見到這麼大規模又嚴重的攻擊，不僅因錯誤組態所導致，未能及時執行程式修補也是原因，讓更多網路罪犯們確信用企業目標取代消費者是值得的，他說道。

影響情況不明

由於私人企業在法律上不見得會被要求揭露勒索軟體攻擊事件，所以勒索軟體攻擊在企業領域的影響難以量化：無論是成本與普遍性。這類受害者有多大機率會決定支付贖金也很難知曉，不過對網路

罪犯而言，繼續投資這種威脅的好處顯而易見。

FBI網路犯罪投訴中心(IC3)於2019年十月發出的警告中提出：「據IC3收到的投訴與FBI案件資訊指出，從2018年初，廣泛、無差別的勒索軟體活動事件急劇下降，但勒索軟體造成的損失卻明顯提升。」

「勒索軟體攻擊變得更針對性、更精緻細膩且代價更高，即便整體攻擊頻率仍然保持不變。」該組織說道。上市公司有時會在證券交易委員會(SEC)歸檔紀錄中釋出勒索軟體攻擊相關資訊，因為他們有義務向股東揭露重大網路攻擊事件。這些公司在必須向顧客與合作夥伴解釋重大營運災害時不得不公開這類事件。

舉例來說，運輸業巨擘Maersk由於2017 NotPetya的攻擊，被迫暫緩十七個碼頭的營運，導致等待貨物裝載的隊伍大排長龍，與耗時數個月才解決的後勤惡夢。這個事件讓該公司付出超過兩億美元的代價，對其顧客的營運也造成相當嚴重的影響。

當勒索軟體襲擊的是市政府、醫院、學校或警局這類公家機構時，造成的影響就顯而易見，統計數字也令人堪憂。據資安公司Emsisoft於十二月釋出的報告指出，2019年期間勒索軟體攻擊影響了113個政府機構、市府當局與州政府、764個醫療供應商與89間大學、學院與校區，有高達1,233間獨立學校可能受到影響。

爭議在於，公家機關由於預算限制與過時的IT基礎架構，無法擁有與大型企業相同等級的資安防護機制，因而容易成為攻擊者的目標。在2019年十月釋出的一份報告中，密西西比州稽核員表示：「許多州立機構、董事會、委員會及大學未遵循州資安法，致使密西西比人民資料容易遭受駭客攻擊，」，其總結指出：「許多州立機構的運作就彷彿州及聯邦網路安全法不適用他們一樣。」據Emisoft指出，就公開報告內容來看，密西西比州其實是2019年受勒索軟體影響最小的州之一。

APT級威脅

雖然公家機關較容易成為目標，私人企業遭勒索軟體感染的風險也不會比較低。經過多年，勒索軟體組織採用許多精緻細膩的手法，包括標的性遞送機制、利用系統既有管理工具與公用程式的手動入侵攻擊(亦即名為Living-off-the-Land的攻擊策略，中文翻作「離地攻擊」)、暗中進行網路偵察，以及過去主要與網路間諜組織與國家贊助攻擊者相關的其他攻擊方式。這就是採用進階持續威脅(APT)技術的傳統網路犯罪的大方向之一。

「我們已見識到名為手動感染的事件逐漸增加。」Kujawa說道。這指的是攻擊面對網際網路的伺服器或通訊協定弱點，或者用其他方式讓攻擊者取得系統終端機存取權，把它當成後門。如此做法可以讓網路罪犯停用資安軟體、執行各種任務並將勒索軟體套用在指定目標上，而不是仰賴有其他功能限制的自動化惡意軟體程式，他表示。

可追溯到2016年的勒索軟體程式SamSam，便是專門用這種方式部署而聞名，不過過去幾年觀察到的較新的惡意攻擊組織也採用了像是Ryuk、RobinHood與Sodinokibi等勒索軟體的相同攻擊手法與策略。

甚至，已有跡象顯示勒索軟體正進化到一種全新威脅型態，網路罪犯不只加密資料，也竊取資料並以此威脅將在網路上公佈。此舉令企業組織面臨破壞性公眾資料外洩的風險與相關法規、財務與聲譽的影響。

2019年十二月，駭客組織Maze使用勒索軟體感染企業組織，威脅若不支付贖金將公佈從這些組織偷來的資料。受害者包括佛羅里達的彭薩科拉市，它在12月7日遭受攻擊，導致電話、市政熱線、電子郵件伺服器與帳單支付系統遭到破壞。

其他駭客組織則利用資料外洩做為敲詐手法。2015年，名為Chimera的勒索軟體程式將目標瞄準消費者，同樣威脅會釋出從受害者偷來的私密資訊。然而，就Chimera的例子，不過是恐懼戰術，攻擊者並未實際從受感染的系統裡竊得任何資料。

多年來，諸多網路罪犯威脅要釋出偷來資訊的恐嚇之舉，最終被指揭穿都騙人的，因為擷取大量資料從經驗上來看是有難度的。要對大量受害者做出這些，駭客必須要有可以接收並儲存數TB資料的基礎架構。這會大幅增加其攻擊活動的開銷。然而，雲端基礎架構的崛起，提供更輕鬆維護且更低成本的資料儲存與網路流量，讓這些攻擊

開始變得更可行。

2019年十二月下旬，Maze組織對外公開他們宣稱已竊取的部份資料，結果證明真的握有從受害者身上擷取的潛在機敏資訊。它們由愛爾蘭ISP代管的第一個網站，已遭撤除，但馬上就以在新加坡代管的全新網站上重新上線。

「沒料到這種威脅會這樣發展，」Kujawa表示。「這讓犯罪曝光更多是毫無疑問的，但也成為施加壓力的有效方式。它充份利用了媒體與威脅意識。」

Kujawa深信勒索軟體組織會越來越傾向於使用這類戰術，因為更多企業組織瞭解如何處理勒索軟體與執行穩健可靠的資料復原計畫，罪犯們將發現越來越難僅僅透過鎖住資料就能拿到金錢。「若企業認為他們的資料，極具保存的價值與重要性，如果他們不付這筆贖金就可能會被公開，不論攻擊者是否真的會這麼做，光這樣的威脅本身就可能迫使一些受害者乖乖付錢。」他說道。

新攻擊手法

分散式勒索軟體的主要手法依然是魚叉式釣魚攻擊與不安全的RDP(Remote Desktop Protocol)遠端桌面連線。然而，攻擊者也會購買能長驅直入早被其他惡意軟體感染之系統的存取權限。線上市集有在賣已遭駭電腦與伺服器的存取權限，以及專為願意付費者部署額外惡意軟體的殭屍網路。舉例而言，Emotet垃圾郵件殭屍網路、TrickBot憑證竊取木馬與Ryuk勒索軟體間之間的關係，在資安社群界是眾所周知的。

Ryuk勒索軟體事件中的最初系統劫持幾乎都是透過商品化惡意軟體發動的，代管資安服務供應商Secureworks資安研究員 Chris Yule在2019年11月DefCamp駭客資安大會上的簡報中表示。他的言論，為真實世界大型企業組織的勒索軟體感染提供了深刻見解。

「我們發現Emotet導致TrickBot感染，接著一段時日後，又發現這些TrickBot感染中的一部份導致了Ryuk感染，」Yule表示。「我們當然不知道為什麼會這樣，但合乎邏輯的假設似乎是Ryuk背後的組織付費購買存取權。」

根據Yule的說法，Trickbot執行自動化憑證竊取的正規行動，然而一旦Ryuk攻擊者一接手，一切都變了。這些動作轉而更親力親為，還加入系統管理工具、網路掃描、PowerShell Empire 這類公開攻擊框架的利用，以便停用終端惡意網路偵測等等安全機制。攻擊者花時間瞭解環境、識別出網域控制器與其他重要目標，並做好發動大型勒索軟體攻擊的萬全準備，同時保持不被偵測到，這是APT組織的常見戰術。

好消息是－Emotet最初感染與Ryuk部署之間通常會有一段企業能偵測與處理感染的特殊空窗期。以Yule展示的案例來看，空窗期有48天。

壞消息則是偵測此類手動駭客攻擊與「離地攻擊」戰術的橫向移動攻擊，若沒有更進階網路與系統監控工具會很困難。意即因APT不在其威脅模組之中而未建置APT防禦機制的企業組織，如今也會抓不到勒索軟體與其他手法精緻的網路犯罪攻擊。

部份勒索軟體組織過去幾年所採用另一個感染媒介就是傷害代管服務供應商(MSP)，後者因為它們所提供的服務，而擁有存取許多企業網路與系統的特權。此舉曝露了因中小型企業將其網路與資安管理委外給專業廠商管理的問題，因此當信任第三方或它們所使用的工具程式成為內部威脅時，採取止血手段限制住可能發生的傷害至關重要。

Malwarebytes還觀察到以網站為基礎的漏洞攻擊程式工具集捲土重來，它針對企業部署勒索軟體，特別是RIG漏洞攻擊程式工具集。這是透過遭劫持網站發動的攻擊，這些攻擊者知道這些遭竊持網站會是某些企業部門感興趣的，或者已被鎖定攻擊目標旗下員工拜訪過的。

「我們對於會這樣發展的想法是：因為過去幾年有相當多弱點被發現，」Kujawa說道。「預計的攻擊焦點會落在Chromium引擎上，因為這個通常運在Chrome上的引擎，終於也將運行在Microsoft最新瀏覽器上。因此，嘗試利用該瀏覽器弱點，對網路罪犯與漏洞攻擊套件來說相當重要，因為大部份人都使用該平台。」

難以破解的加密勒索

資安公司一直都在試圖找出勒索軟體程式的檔案加密實作，協助受害者恢復檔案而不必支付贖金。這些努力成果所建立的解密工具多

半免費釋出，可以在Europol維護的 NoMoreRansom.org 網站自由取用。

不過，更老練駭客組織所使用的勒索軟體程式已十分成熟。攻擊者從自身過去的錯誤，或其他勒索軟體開發者的錯誤中學習，並改正實作上的失誤。

有些勒索軟體程式的程式碼已經在網路上洩露，而且可供複製與改善。作業系統亦提供加密API，與審慎檢查過的開放源碼加密框架與函式庫。這一切都表示大部份受歡迎的勒索軟體程式也同時也是最危險的，因為它們使用強健的加密演算法而且無解。

企業組織擁有一套備份計畫與定期測試的資料回復方案相當重要。備份還應該離線保存或遠離網路，避免攻擊者加以刪除或加密鎖住。一些有記錄在案的案例中，企業組織決定或被迫支付贖金，是由於他們的備份遭竄改或復原處理程序會花太久時間，相較之下只好購買解密程式。

打造勒索軟體防禦網

首先最重要的是，企業組織應透過執行內外部滲透測試，並確認是否有任何會曝露在網際網路上之潛在弱點的系統或伺服器，以避免讓自己被列入容易得手的目標攻擊清單。VPN或RDP這類遠端網路連線機制，應擁有強健且獨特的憑證以及雙因素身分認證(2FA)。

在網路內部，企業應確保端點與伺服器執行的作業系統與軟體的修補程式保持在最新版本。網路應以最少特權的原則為基礎進行分段，如此一來單一部門受劫持的工作站才不會輕易導致整個網路被接管。在Windows網路上，網域控制器應審慎監控是否有不正常存取。

仰賴MSP或資安代管服務供應商(MSSP)的企業，應確保來自這些第三方的連線能妥善的被監控與記錄，他們所使用的軟體也要開啟雙因素認證。提供給第三方的網路與系統存取權，應限制在僅用於執行其工作所需的內容上。

企業組織應擁有一份清楚明確的資料清單，這對業務營運而言至關重要。系統儲存亦應嚴密控制。

由於諸多勒索軟體感染始於受感染的工作站，因此端點使用防惡意軟體程式相當重要。移除瀏覽器上不必要的外掛套件與擴充功能、保持軟體最新版本並確保員工帳號僅擁有限制下的權限。

訓練員工如何發現釣魚攻擊電子郵件，並對任何要求他們開啟檔案或點選連結的不請自來訊息抱持質疑的態度。由資安團隊來建立特殊電子郵件位址監控，讓員工可以轉發他們認為有疑慮的電子郵件。

最後，草擬事件回應計畫，並確保參與的每個人都知道當感染發生時自己的角色與需要做的事，包括與你的資安廠商或MSSP或執法單位聯繫。不要輕忽商品化惡意軟體的感染，請徹底調查它們，因為它們多半會是引發更嚴重安全威脅的入侵媒介。

美國IC3網路犯罪投訴中心和美國網路安全暨基礎設施安全局(CISA)雙雙提出預防或回應勒索軟體攻擊的建議。2020年二月，國家標準暨技術研究院(NIST)釋出兩份針對處理勒索軟體最佳實作的實作指南草案。這兩份指南草案分別是《Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events》與《Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events》。