tenable RESEARCH

勒索軟體生態系統

手法和技倆的商品化如何催生全球網路犯罪的產業革命



目錄

簡介 3

參與者：解構勒索軟體生態系統 6

初次存取仲介(IAB) 6

加盟夥伴 7

勒索軟體集團 7

勒索軟體集團經營方式類似企業 8

加盟夥伴是勒索軟體集團成功的關鍵要素 8

生態系統中所有的勒索軟體集團又扮演何種角色？ 8

發展過程：勒索軟體集團透過敲詐手法而蓬勃發展 9

手法：勒索軟體攻擊常用的媒介 12

勒索軟體集團會提供加盟夥伴教戰守則 12

找到阻力最小的途徑 12

魚叉式網路釣魚 12

遠端桌面通訊協定 13

利用安全弱點 13

向 IAB 購買存取權 13

第三方入侵 14

吸收公司和政府中的內部人員 14

Active Directory 在勒索軟體攻擊中扮演重要的角色 14

勒索軟體攻擊將持續存在：以下是進行防禦的方式 15

Tenable 如何提供協助 20

進階持續性威脅(APT)集團組成份子包括以世界各地為民族國家服務的企業和政府為攻擊目標的個人。這些集團包括那些直接作為民族國家的一部分或取得民族國家默許支援(國家贊助)但獨立運作的團體。

簡介

在 2020 年的 RSA 會議上，美國聯邦調查局(FBI)的監督特別探員 Joel DeCapua **披露勒索軟體集團的總收入超過 1.44 億美元**(從 2013 年到 2019 年)，這在當時被認為是一個驚人的數字。然而，光是在 2020 年，勒索軟體集團**就從他們的集體攻擊中賺取了 6.92 億美元(據報導指稱)**，幾乎是過去六年總和的五倍。由於缺乏對所有勒索軟體集團所使用的加密貨幣錢包的深入解析以及接收此類資料時的延遲，真實數字可能不僅於此。然而，這些數字突顯了一個不可否認的事實：勒索軟體已自我強化，成為當今全球企業面臨的最大威脅之一，並且在此過程中更形成有利可圖的犯罪生態系統。

進階持續性威脅(APT)集團長期以來都被許多人視為對企業最具危險性的威脅。這些集團更專注於網路間諜活動，並且較少以財務為導向，這將他們的範圍侷限在鎖定的企業和政府目標。與此同時，網路犯罪世界中的威脅執行者主要受財務收益的刺激，因為正如饒舌歌手 DJ Quik 所言：「如果無利可圖，那就說不通了。」



實際上，沒有任何企業可以真正免於勒索軟體的侵害，因為無論企業規模大小，都可能成為攻擊的目標。

在 Tenable 的《2021 年威脅態勢回顧》報告中，安全應變團隊判斷，在 2021 年，至少有 38% 的資料外洩事件是勒索軟體攻擊的結果，而在 2020 年，此比例為 35%。在醫療保健領域，勒索軟體佔資料外洩事件的 36.2%，而在教育領域，則佔資料外洩事件的 24.7%。這並不表示勒索軟體在其他領域的猖獗程度較低。但是，由於美國對醫療保健企業的通報要求嚴格，因此該領域中通報了大量的勒索軟體攻擊，也就毫不意外了。根據 Sophos 最近的一項調查發現，66% 的企業在 2021 年曾通報遭受過勒索軟體攻擊。實際上，沒有任何企業可以真正免於勒索軟體的侵害，因為無論企業規模大小，都可能成為攻擊的目標。

以下地圖顯示了 2019 年至 2022 年間發生的許多勒索軟體攻擊的抽樣結果，彰顯出勒索軟體的全球性質。

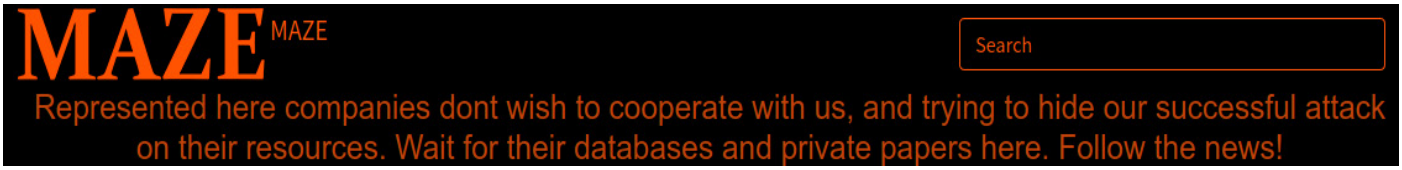


勒索軟體如此猖獗的主要原因之一是勒索軟體即服務(RaaS)的出現。RaaS 讓勒索軟體從一個羽翼未豐的威脅一躍成為一股不可忽視的力量。RaaS 是一種服務模式，就像軟體即服務一樣，勒索軟體集團並不是提供對合法軟體應用程式的存取權，而是提供惡意軟體(勒索軟體)和必要的基礎設施，以協助勒索軟體攻擊，同時仰賴被稱為加盟夥伴的第三方在部署勒索軟體之前完成實際的不法行為，即獲得對企業的初始存取權限。

勒索軟體已成為可自給自足的產業。之前會由開發和傳播惡意軟體的同一勒索軟體集團來發動攻擊，但 RaaS 的出現吸引了多個參與者。每一方都扮演了極其重要的角色，構成了我們所說的勒索軟體生態系統。除了勒索軟體集團，其他主要參與者還包括加盟夥伴和初次存取仲介(IAB)。

RaaS 僅僅是開端而已。勒索軟體目前的主導地位和一種被稱為雙重敲詐技倆的出現有直接的關聯性。

2019 年，Maze 勒索軟體集團**率先採用雙重敲詐技倆，作為其針對公司攻擊的一部分**。這種技倆需要從受害者企業竊取資料，並在公開羞辱網站(通常稱之為洩密網站)的暗網上發布有關這些資料外洩的預告片。



圖片來源：Krebs on Security

自從引進雙重敲詐的手法後，大多數目前營運中的勒索軟體集團都將其納入自家的攻擊中，在暗網上託管了自己的洩密網站。在體育界，率先採用制勝技巧的球隊，經常被其他希望找到類似成功戰術的球隊所仿效。同樣地，勒索軟體集團也複製了 Maze 的技倆，而勒索軟體的巨大成功無疑要歸功於雙重敲詐。

儘管多年來遏止勒索軟體攻擊的努力從未停歇，例如**逮捕勒索軟體攻擊者**的執法行動和政府**對加密貨幣交易所的制裁**，但勒索軟體活動仍有增無減。我們持續看到勒索軟體集團成功地攻擊橫跨各行各業的企業，一些勒索軟體集團甚至**死灰復燃**。

我們撰寫本報告的目的是希望透過探索相關的主要參與者，以及勒索軟體攻擊者及其加盟夥伴用於滲透企業和散布勒索軟體承載攻擊的技倆和策略，協助揭開勒索軟體生態系統的神秘面紗。我們還提供了勒索軟體攻擊中可能被利用的最常見弱點清單，以協助資安從業人員優先採取修復措施。

參與者：解構勒索軟體生態系統

勒索軟體生態系統由三種截然不同的犯罪集團組成





初次存取仲介 (IAB)

IAB 是一個網路罪犯的專業化集團，負責透過各種方式取得企業的存取權。這個類別包括了致力於鑽研此伎倆的個人和集團。IAB 不會直接使用此存取權限，而是利用此權限在受害企業的網路中長期潛伏，並將其出售給網路犯罪生態系統中的其他個人或集團。他們的收費非常低廉，因為會依據他們所入侵的企業類型和存取權類型而有所不同。例如，Digital Shadows 的研究人員分析了 2020 年 IAB 的 500 多個名冊，發現價格差異頗大，平均從控制面板存取權限的 303 美元到遠端桌面通訊協定 (RDP) 存取權限的 9,874 美元不等。

對勒索軟體加盟夥伴而言，IAB 提供了一項非常寶貴的服務，其成本可透過受害者支付的贖金輕鬆回收。加盟夥伴會利用 IAB 來協助加快感染企業的工作。

對 IAB 而言，RaaS 的出現則使其如虎添翼，推進了所提供的服務。Group-IB 最近的一份報告顯示，IAB 市場在 2018 年至 2019 年的一年期間為 160 萬美元，到了 2020 年至 2021 年的一年期間更飆升至 710 萬美元。上述數字遠不及加盟夥伴以及勒索軟體集團所賺取的數百萬美元，但這卻是經過盤算的：出售存取權限而非實際部署勒索軟體，IAB 承擔的風險較小。

雖然 IAB 通常是獨立參與者，但 Google 的研究人員發現了一個名為 EXOTIC LILY 的 IAB，和 Conti 勒索軟體集團有密切的合作。這種類型的關係消除了對中間人 (例如加盟夥伴) 的需求，從而使 IAB 能獲取更多原本提供給大多數加盟夥伴的利潤分紅。對 IAB 而言，直接和勒索軟體集團合作的策略存在額外的風險，因為這可能使得他們直接成為政府或執法機構瞄準的目標，但風險越高，利潤也越多。



加盟夥伴

如果勒索軟體是一輛汽車，那加盟夥伴就宛如負責為勒索軟體攻擊踩油門的司機。這類型的加盟夥伴關係是助長勒索軟體在過去四年蓬勃發展的關鍵因素之一。大多數勒索軟體集團的成就大部分是他們建立的加盟夥伴計劃的副產品。這些加盟夥伴計劃和合法企業的合作夥伴計劃沒有什麼不同。就像合作夥伴會介紹潛在客源給公司一樣，勒索軟體加盟夥伴也會找到受害者並以勒索軟體進行感染，然後將他們帶到勒索軟體集團以「達成交易」(也可以說是談判)。

加盟夥伴會透過 IAB 購買存取權限並使用常見的攻擊媒介，例如魚叉式網路釣魚 (使用惡意軟體)、暴力密碼破解 RDP 系統、利用未修補或零時差弱點以及從暗網購買竊取的憑證來入侵企業。

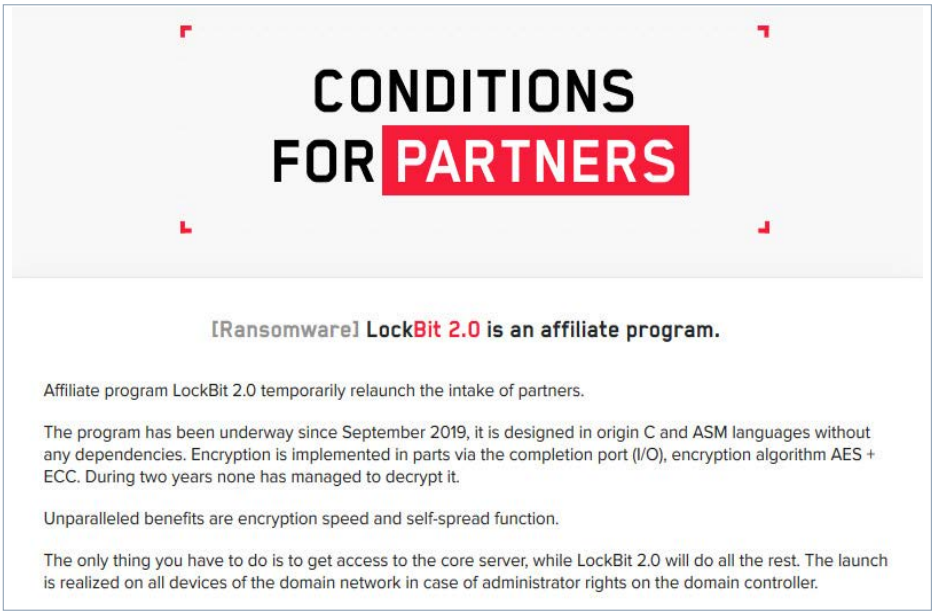
當網路罪犯成為某些勒索軟體集團的加盟夥伴時，他們通常會收到一份關於他們將如何完成任務的教戰守則。這些教戰守則還包括有關如何破壞企業的各種建議。

RaaS 為加盟夥伴提供了額外的優勢，讓他們不需仰賴任何一個勒索軟體集團，可獨立發動攻擊，進而為他們提供了同時和多個集團合作的機會。這種自主權為加盟夥伴提供了穩定性：如果一個勒索軟體集團被淘汰或因執法行動而被瓦解，還有其他集團可取而代之。

勒索軟體集團

勒索軟體集團由負責以下任務的各種成員所組成：開發和測試勒索軟體本身、在暗網上建立和託管洩密網站、管理和每個受害者的談判過程以及其他包括逆向工程、行政工作甚至人力資源或吸收成員的任務。勒索軟體集團由於發動攻擊，因此名聲最狼藉並受到關注，因為 RaaS 在此方程式中是行銷和銷售的「產品」。

圖片來源：
BleepingComputer


CONDITIONS
FOR PARTNERS

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.



勒索軟體集團經營方式類似企業

新型勒索軟體集團**經營方式類似傳統企業**。因為他們會和勒索軟體生態系統中的其他人合作，他們也會像企業一樣推銷自己，以最快的加密速度和自我傳播功能等大膽的訴求來爭取加盟夥伴的青睞。

加盟夥伴是勒索軟體集團成功的關鍵要素

勒索軟體集團若想要成功，就需要吸收加盟夥伴，以執行攻擊並提供源源不絕的「客戶」(受害者)。因此，勒索軟體集團在博取加盟夥伴的青睞時出手非常大方，也就毫不意外了。和他們合作的加盟夥伴可賺取大部分要求的贖金，抽成比例為贖金總金額的 70% 至 80%。有些集團對於給加盟夥伴的開價更猛，例如 ALPHV (又名 BlackCat) 勒索軟體集團**提供加盟夥伴 90% 的抽成**。若您想到如今有多少勒索軟體集團在運作時，就能理解這類集團的確需要積極利誘才能吸收加盟夥伴。

生態系統中所有的勒索軟體集團又扮演何種角色？

在 2021 年，FBI **表示追蹤到超過 100 間活躍中的勒索軟體集團**。REvil、DarkSide 和 BlackMatter 等勒索軟體集團在發動了針對託管服務供應商 (MSP) 和**重大基礎設施**以及**食品加工**領域中高價值目標的著名供應鏈攻擊之後，最近更是聲名大噪。最近，諸如 Conti、LockBit.2.0、Hive 和 ALPHV/BlackCat 等集團的排名上升，填補了勒索軟體集團消失或經由執法行動取締後留下的空白。這是勒索軟體集團生命週期的一部分。剛崛起的集團將能擄獲尋求新合作夥伴關係的加盟夥伴最多的注意力，最終也更容易被政府和執法機構盯上。瞭解這些集團可以讓我們深入解析他們的活動，例如他們瞄準攻擊的行業或地理區域。然而，勒索軟體生態系統在數字遊戲中蓬勃發展，在此更需重視的是數量而不是品質。



這類集團最終都僅是曇花一現。多年來，我們已經看過多個勒索軟體集團消失了，無論是出於自身原因，還是由於政府和執法行動。我們還聽到許多報告表示，新興的集團包含了過去勒索軟體集團的成員。例如，REvil **即為惡名昭彰的 GandCrab 勒索軟體團體的接班人**，而 Conti 則**被認為是 Ryuk 的接班人**。「權力遊戲」冒險故事中 Ironborn 的那句名言即適用於現今的勒索軟體集團：「逝去的可能永不凋零，只會再次崛起，更加穩固和強大。」

由於這些勒索軟體集團的無常性，若在此深入探討其中部分集團，並無法達成任何定論，因為這些參考資料在一年後可能很容易就過時了。但是，IAB 和加盟夥伴在勒索軟體攻擊中扮演的重要角色則是長期不變的。例如，當 BlackMatter 勒索軟體集團關門大吉時，其加盟夥伴**將受害者轉移至 LockBit 2.0**。歸根究柢，我們認為應該將更多注意力放在整個生態系統中的加盟夥伴和 IAB 上。



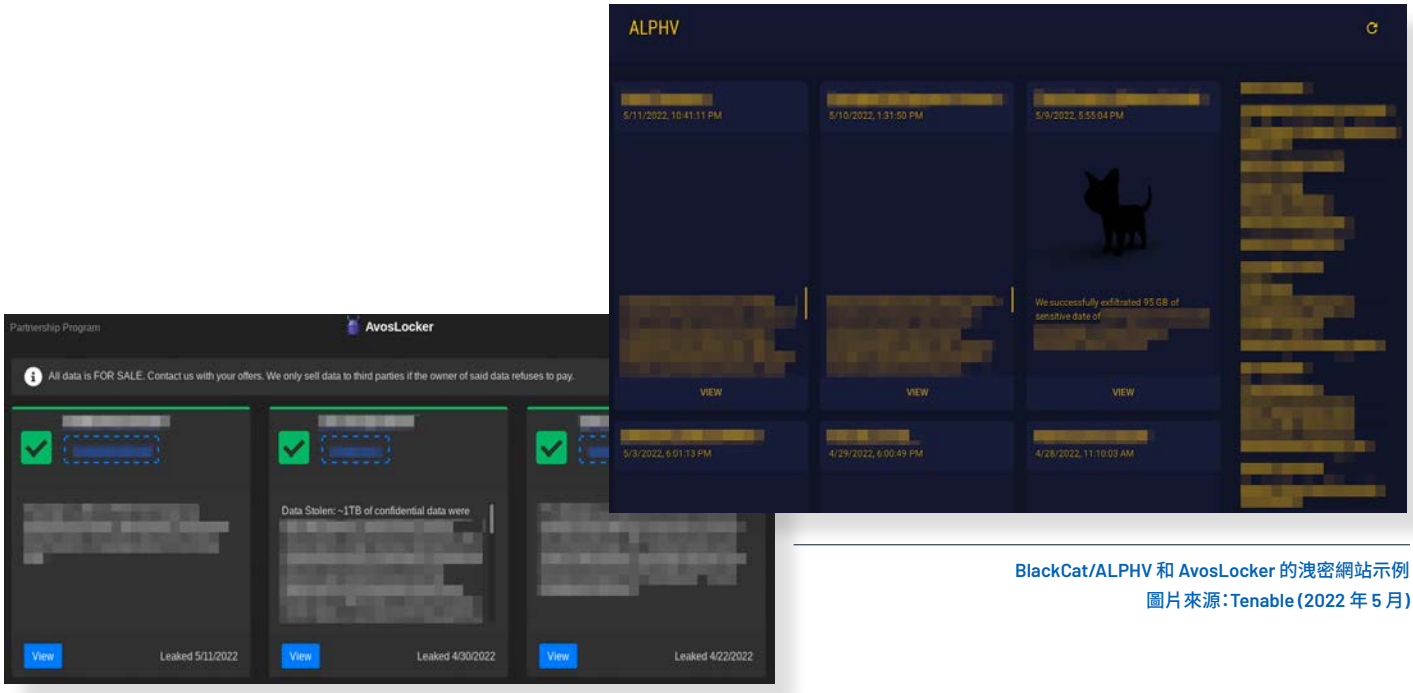
發展過程：勒索軟體集團透過敲詐手法而蓬勃發展

既然我們知道勒索軟體生態系統中的參與者是誰，自然會問：是什麼讓勒索軟體激增並成為現今企業的最大威脅？答案就是「敲詐」這個要素。

傳統上，勒索軟體攻擊的重點是將網路中的檔案加密，作為要求企業支付費用的誘因。這種敲詐方式極為成功。然而，隨著企業開始仰賴從備份中復原被勒索的檔案，勒索軟體集團需要另一種機制來敲詐受害者。這就是雙重敲詐應運而生的地方，並成為勒索軟體集團賺取巨額利潤的催化劑。

這種手法不僅是竊取檔案；並且會威脅將其發布

如本報告前面所述，雙重敲詐手法已被證明是勒索軟體集團的金雞母。然而，這種手法不僅是從受害者的網路中竊取檔案。擁有這些檔案只是開端而已。雙重敲詐如此險惡的原因在於，勒索軟體集團會利用這些竊取的檔案當成誘餌，透過託管在暗網上的個人洩密網站發布樣本來嘲弄企業，並威脅除非對方支付贖金，否則將發布其餘部分。



BlackCat/ALPHV 和 AvosLocker 的洩密網站示例
圖片來源：Tenable（2022 年 5 月）



曝露公司隱私檔案的威脅會產生連鎖效應，因為有關企業客戶的資訊也可能遭受外洩的風險，因而增加了支付贖金的壓力。即使企業能夠從勒索軟體攻擊中恢復正常營運，仍可能決定支付贖金，就像 JBS 在 2021 年 6 月決定向 REvil 勒索軟體集團支付 1,100 萬美元一樣：

「在付款時，公司的絕大多數設施都可正常運作了。在和內部的 IT 專業人員和第三方網路安全專家商議後，該公司決定減緩與攻擊相關的任何不可預見的問題，並確保沒有資料遭到洩漏。」

— JBS 新聞稿

施壓：擴大敲詐手法的類型增加了影響力

雙重敲詐是勒索軟體目前成功的關鍵。然而，這種手法現在已經有將近三年的歷史。隨著勒索軟體集團找到他們的立足點，他們也翻新手法，增加了新的敲詐技倆，藉此對受害企業施加額外的壓力。有些人將這些手法稱為「三重敲詐」或「四重敲詐」，但無論您選擇如何稱呼，這些手法仍屬於同一種敲詐系列。



敲詐手法	奏效的原因
利用分散式拒絕服務(DDoS)攻擊	透過使用 DDoS 讓公司網站停擺，受害者會受到兩種影響：首先，他們無法為線上客戶提供對其商品和服務的存取權限；其次，他們也無法向客戶提供有關資安事端狀態的定期更新，因而對客戶支援造成額外壓力並增加客戶的擔憂。
和勒索軟體受害者的客戶聯絡	勒索軟體集團會和受害企業的客戶聯絡，藉此威脅要洩露和這些客戶相關的檔案，此舉可確保客戶會聯繫受害企業，向他們施加更大的壓力以支付贖金。
和受害者的員工聯絡	和聯繫客戶類似，勒索軟體集團會聯繫受害企業的員工，藉此操弄恐懼手法以說服員工向管理階層施加壓力，進而支付贖金要求。
警告受害者不得讓專業談判人員和/或執法人員參與	透過恐嚇受害者不得聯繫專業談判人員或讓執法部門參與談判，他們能夠對受害企業施加更多壓力，要求他們直接和這些犯罪集團談判，以確保達成贖金支付的預期結果。
威脅若不支付贖金，即拍賣竊取的資料	勒索軟體集團會威脅將竊取的資料拍賣給第三方，希望藉此對受害企業施加更多壓力，使其支付要求的贖金，否則將面臨遭竊取的資料被交給其他網路犯罪幫派的危險。
威脅要在所有受影響的系統上使用磁碟抹除功能	勒索軟體集團會威脅使用磁碟資料抹除程式(這將使得加密系統完全無法使用且無法復原)，目的在迫使受害者支付要求的贖金。

雖然上述的敲詐手法沒有像威脅在洩密網站上發布竊取檔案的方法那麼無往不利並受到廣泛採用，但這些手法確實對受害企業增加了付款壓力。



手法：
勒索軟體攻擊常用的媒介

在詳細說明了勒索軟體生態系統中的參與者以及導致勒索軟體攻擊激增的原因之後，最後一個需要回答的問題是：IAB、加盟夥伴和勒索軟體集團如何進入受害者網路以散佈勒索軟體？使用各種不同的手法、技術和程序，有常見的，也有非正統的。

勒索軟體集團會提供加盟夥伴教戰守則

我們知道勒索軟體教戰守則的存在是因為 2021 年，一個對 Conti（一個成立於 2020 年的多產勒索軟體集團，賺取了超過 1.8 億美元的利潤）心懷不滿的加盟夥伴**洩露了該集團的加盟夥伴教戰守則**。2022 年，Conti 的一名成員公佈了**該集團成員之間的私人對話快取**，這段對話後來被稱為 ContiLeaks。這些外洩的內容揭露了很多關於目前 RaaS 集團（例如，Conti）的營運要素，並有助於我們對於支撐勒索軟體生態系統的內部運作有更深入的瞭解。

然而，加盟夥伴並不受所提供的教戰守則約束，因為他們可以自由地使用自己的方法進行操作，包括透過 IAB 購買存取權限或從公共原始碼儲存庫中取得攻擊程式。

找到阻力最小的途徑

對於勒索軟體的加盟夥伴來說，進入企業的方式主要會受到阻力最小途徑的方法所左右。用於破壞企業防禦的常見攻擊媒介有好幾種。



魚叉式網路釣魚

鎖定企業為目標的最常見方法是透過魚叉式網路釣魚，攻擊者藉此向受害者傳送精心製作的電子郵件，其中包括惡意附件或導向託管惡意軟體的外部網站的連結。這些攻擊中使用的惡意軟體不是勒索軟體本身，而是第一階段下載程式，一種旨在下載二級和三級惡意軟體元件的木馬程式。這些額外的惡意軟體元件最終將通往勒索軟體承載。多年來為勒索軟體攻擊助攻的一些較受歡迎的下載程式包括愛吹噓的 Emotet、Trickbot 和 Qakbot 木馬程式，以及 BazarLoader。



遠端桌面通訊協定

RDP 是勒索軟體加盟夥伴用來攻擊企業的另一種熱門途徑。由於 RDP 是可公開存取的，攻擊者可以使用指令碼嘗試以暴力密碼破解的方式進入這些系統，透過使用已知的預設密碼和**字典攻擊**的組合來鎖定脆弱的密碼以進行攻擊。為了強調攻擊媒介 RDP 的價值，**業界一些人**將其戲稱為勒索軟體部署協議。



利用安全弱點

軟體弱點在協助勒索軟體經由多種途徑發動攻擊方面扮演了關鍵角色。其中包括用作惡意文件一部分的弱點、在安全通訊端層虛擬私有網路 (VPN) 等周邊裝置中發現的弱點，以及旨在提升企業網路內部特權的大量缺陷。

例如，ProxyLogon 和 ProxyShell 是 Microsoft Exchange Server 中的一系列缺陷，我們在 **2021 年威脅態勢回顧**報告中將其封為**最常被鎖定為目標的弱點**，在過去一年中已被多個勒索軟體集團利用。

在 Conti 的加盟夥伴教戰守則中洩密的部分內容中，我們知道加盟夥伴受到指示要利用 PrintNightmare 和 ZeroLogon 等弱點來提升特權。我們**特別強調 Conti 及其加盟夥伴所利用的 30 多個弱點**，而且顯然勒索軟體集團和加盟夥伴都在旁觀望，引領期待下一個納入他們的教戰守則的重大弱點。

雖然勒索軟體集團覬覦零時差弱點，但**大多數的勒索軟體攻擊都仰賴利用未修補的舊型弱點** (在各種軟體解決方案中)。

我們在本報告的附錄部分匯總了一份和勒索軟體攻擊相關的弱點清單，其中包括多年來強調的弱點並和由安全研究人員 Allan Liska 以及另一位化名為「pancake3lullz」的使用者所建立的**缺陷清單**相互參照，以協助找出常被利用來進行初始存取的弱點。

我們在本報告的附錄部分匯總了一份和勒索軟體攻擊相關的弱點清單，其中包括多年來強調的弱點並和由安全研究人員 Allan Liska 以及另一位化名為「pancake3lullz」的使用者所建立的缺陷清單相互參照，以協助找出常被利用來進行初始存取的弱點。



向 IAB 購買存取權

如前面所述，IAB 為勒索軟體加盟夥伴提供了一種經濟實惠且省時的方式，能對已經遭受入侵的企業登堂入室。IAB 已經透過利用上述一些媒介完成了勘察和額外的差事，從傳送魚叉式網路釣魚電子郵件到利用弱點和暴力密碼破解脆弱的 RDP 系統。這些努力使得 IAB 在勒索軟體生態系統中的角色變得無比重要。



第三方入侵

第三方可為勒索軟體攻擊提供更多攻擊媒介。在 ClOp 勒索軟體集團的案例中，他們利用 **Accellion 檔案傳輸設備中的多個弱點**（這是一種能為企業提供傳輸檔案方式的應用程式）從至少 50 家企業中竊取資料。2021 年 7 月，REvil 勒索軟體加盟夥伴**利用 Kaseya 的虛擬系統管理員 (VSA) 中的多個零時差弱點**，勒索和 MSP 合作對其系統進行遠端管理的公司。

以 Kaseya VSA 這類遠端監控和管理軟體為攻擊目標並不常見，但這確實不是什麼新鮮事。在過去，GandCrab 和 Zeppelin 等其他勒索軟體集團曾經以這些產品和使用它們的 MSP 中的缺陷為攻擊目標。



吸收公司和政府中的內部人員

儘管沒有受到大篇幅的討論，但勒索軟體集團的確已經向企業和政府機構的成員明確提出協助勒索軟體攻擊的提議。在這些情況下，內部人員本身就是另一種類型的加盟夥伴。例如，LockBit 2.0 勒索軟體集團**向內部人員提供了「數百萬美元」**，這些內部人員將提供公司電子郵件帳戶、RDP 和 VPN 的憑證，或者願意使用惡意軟體自行感染他們的公司裝置。最近，在 5 月，Conti 勒索軟體集團**聲稱哥斯大黎加政府中有內部人員**在他們針對該國的攻擊中提供協助。

Active Directory 在勒索軟體攻擊中扮演重要的角色

初始存取權是勒索軟體集團和加盟夥伴取得進入企業網路的方式。一旦進入後，他們通常會盯上 Active Directory，因為獲得網域特權可為攻擊者提供在整個網路中散佈其勒索軟體承載的必要能力。這包括使用 Zerologon 和 PetitPotam 等重大弱點。例如，DFIR 報告中的研究人員深入研究了兩個案例，其中威脅執行者能夠在從初始網路釣魚電子郵件開始的 **5 小時**和 **2 小時**內分別在整個網域中啟動 Ryuk 勒索軟體，並在過程中利用 Zerologon。

除了弱點，勒索軟體攻擊者還將利用熱門工具來取得網域特權，包括 AdFind、Bloodhound、Kerberoasting 以及 NTDS 傾印。



勒索軟體攻擊將持續存在：以下是進行防禦的方式

當您考慮到勒索軟體生態系統獲利有多驚人時，就不難找到讓參與者堅持下去並擴大活動的誘因。雖然沒有化解勒索軟體攻擊的靈丹妙藥，但我們知道勒索軟體集團以及加盟夥伴鎖定企業為目標的許多最常見方式。以下是企業可以採取的一些步驟，以設置最佳防禦機制來對抗勒索軟體攻擊。

指引	這個措施有效的原因
對企業內的所有帳戶使用多重因素身分驗證	勒索軟體集團會透過提供憑證或利用能洩露登入憑證的弱點的 IAB 購買對企業的存取權限。透過將多重因素身分驗證新增為登入要求，這可對勒索軟體攻擊者增加另一個必須克服的額外保護層。這可以透過適應性多因素身分驗證進一步強化，其中包括使用者位置在內的多個訊號會用於識別可疑的登入嘗試。
要求帳戶使用強式密碼	仰賴脆弱密碼或預設密碼會使得勒索軟體集團更容易取得對帳戶的存取權限。確保密碼要求包括冗長且非字典上的字詞，並標記已在資料外洩中曝露的密碼，使攻擊者更難進行暴力密碼破解。
持續稽核企業內使用者帳戶的權限	勒索軟體集團一旦闖入企業，將試圖建立具有提升權限的新帳戶或濫用具有提升權限的現有帳戶，甚至使用和不再屬於您企業的員工相關聯的帳戶。這就是為什麼對現有和新建立的使用者帳戶進行稽核，以確保沒有錯誤設定，並在您的企業中採用最低特權原則很重要的原因。
及時識別和修補網路中易受攻擊的資產	我們知道勒索軟體集團擅長利用未修補的舊型弱點，因此企業必須能夠找出其網路中易受攻擊的資產並套用可用的修補程式，這點非常重要。由於攻擊者可利用的時間很長，因此能愈快採取行動愈好。
查看並強化遠端桌面通訊協定 (RDP)	讓 RDP 對網際網路開放，對勒索軟體集團而言是正中下懷。如果您不需要的話，就停用該協定。如果您確實有需要，則請確保 RDP 符合強式密碼要求。
透過解決錯誤設定和偵測常見的 AD 攻擊路徑來強化 Active Directory 安全	勒索軟體集團和加盟夥伴若一旦闖入企業，通常會尋求利用企業的 Active Directory 安全情勢中的錯誤設定。他們還將利用常見的攻擊路徑來試水溫，因此監控您的 Active Directory 環境並解決已知的攻擊路徑極為重要。

針對加密的離線備份建立並定期執行排定的更新	勒索軟體會透過雙重敲詐攻擊成功達成目標，其中包括對企業網路內的檔案進行加密。此流程可能導致非計劃性停機，並可能影響企業是否支付贖金要求的決定。勒索軟體集團並不畏懼以備份為攻擊目標，因此建立離線儲存加密備份的常規做法非常重要。
使用適當的軟體（防毒、反惡意程式軟體）來找出網路上的惡意軟體	由於包含惡意附件或惡意軟體連結的魚叉式網路釣魚通常會導致感染勒索軟體，因此務必使用防毒或反惡意程式軟體等解決方案來協助偵測出木馬下載程式等威脅。
實施安全認知訓練，教育員工了解常見的攻擊媒介	社交工程攻擊（包括經由電子郵件或社群網路進行魚叉式網路釣魚）是網路罪犯將惡意軟體植入您網路中的系統的另一種方式。藉由提供使用者安全認知訓練，您的員工可獲得有關如何辨識網路罪犯使用的常見攻擊媒介的指引，這在保護您的網路方面將發揮重要作用。
透過進行桌上模擬演習來針對攻擊做好計劃	問題通常不在於是否會發生攻擊，而是何時會發生攻擊。這就是為什麼您的企業必須使用桌上模擬演習來排練一場範例場景的原因，這種練習可用於協助為現實世界的攻擊預做準備。CISA 提供了本身的 CISA 桌上模擬演習套件 (CTEP)，能協助引導此流程。

隨著勒索軟體集團的汰換，以及加盟夥伴轉向支援其他團體，勒索軟體生態系統仍維持龐大勢力且不斷演變。儘管有更替，但加盟夥伴和 IAB 仍然是該領域的重要中流砥柱。最後，透過所有這些相異部分的合作，使得勒索軟體生態系統還是能成功並繼續生存。

企業並非完全無計可施。執法單位和政府行動發揮了一定程度的嚇阻作用。例如，美國對 Colonial Pipeline 和 JBS 攻擊的因應措施對好幾個勒索軟體集團施加了更多壓力，促使他們遠離這些行業。雖然這可能無法威嚇住所有勒索軟體集團，但卻肯定能導致一些集團勸告蠢蠢欲動的加盟夥伴某些行業千萬碰不得。

有了 RaaS 和雙重敲詐，潘朵拉的盒子已經打開，而攻擊者絲毫沒有放慢腳步的跡象。只要勒索軟體生態系統繼續蓬勃發展，針對企業和政府發動的攻擊仍將層出不窮。企業和政府實體必須提前做好萬全準備，以便能站穩防禦和因應勒索軟體攻擊的最佳位置。

勒索軟體加盟夥伴和集團所利用弱點的附錄

CVE	說明	CVSS 評分
CVE-2017-0199	Microsoft Office/WordPad 遠端程式碼執行弱點	7.8
CVE-2017-11882	Microsoft Office 遠端程式碼執行弱點	7.8
CVE-2018-13374	Fortinet FortiOS 不當存取控制權弱點	8.8
CVE-2018-13379	Fortinet FortiOS 路徑周遊/任意檔案讀取弱點	9.8
CVE-2018-8120	Microsoft Win32k 權限提高弱點	7
CVE-2018-8174	Microsoft Windows Visual Basic 指令碼引擎	7.5
CVE-2018-8440	Microsoft Windows 進階本機程序呼叫 (ALPC) 權限提高弱點	7.8
CVE-2018-8453	Microsoft Win32k 權限提高弱點	7
CVE-2019-0604	Microsoft SharePoint 不當輸入驗證弱點	9.8
CVE-2019-0708	Microsoft 遠端桌面通訊協定遠端程式碼執行弱點 (「BlueKeep」)	9.8
CVE-2019-1108	Microsoft Windows 遠端桌面通訊協定用戶端資訊洩漏弱點	6.5
CVE-2019-11510	Pulse Secure 任意檔案讀取弱點	10
CVE-2019-11539	Pulse Secure 命令注入攻擊弱點	7.2
CVE-2019-11634	Citrix Workspace 應用程式和接收方錯誤存取控制弱點	9.8
CVE-2019-1224	Microsoft Windows 遠端桌面通訊協定伺服器資訊洩漏弱點	7.5
CVE-2019-1579	Palo Alto Networks PAN-OS 遠端程式碼執行弱點	8.1
CVE-2019-18935	Telerik UI .NET 還原序列化弱點	9.8
CVE-2019-19781	Citrix 應用程式供應控制器 (ADC) 和閘道目錄遊走弱點	9.8
CVE-2019-2725	Oracle WebLogic 伺服器還原序列化弱點	9.8
CVE-2019-3396	Atlassian Confluence Widget Connector 伺服器端範本注入攻擊弱點	9.8
CVE-2019-5591	Fortinet FortiOS 資訊洩露弱點	6.5
CVE-2019-7481	SonicWall SMA100 預先驗證 SQL 注入攻擊弱點	7.5
CVE-2020-0609	Windows 遠端桌面閘道 (RD 閘道) 遠端程式碼執行弱點	9.8
CVE-2020-0610	Microsoft Windows 遠端桌面閘道 (RD 閘道) 遠端程式碼執行弱點	9.8
CVE-2020-0688	Microsoft Exchange 驗證金鑰遠端程式碼執行弱點	8.8
CVE-2020-0787	Microsoft Windows 背景智慧轉移服務權限提高弱點	7.8
CVE-2020-0796	Windows SMBv3 用戶端/伺服器遠端程式碼執行弱點 (「SMBGhost」)	10

CVE-2020-12271	Sophos XG 防火牆 SQL 注入攻擊弱點	9.8
CVE-2020-12812	Fortinet FortiOS 不當驗證弱點	9.8
CVE-2020-1472	Microsoft Netlogon 權限提高弱點(「Zerologon」)	10
CVE-2020-16896	Microsoft Windows 遠端桌面通訊協定資訊洩漏弱點	7.5
CVE-2020-2021	SAML 驗證中的 Palo Alto Networks PAN-OS 驗證迴避弱點	10
CVE-2020-36198	QNAP 惡意軟體掃毒命令注入攻擊弱點	6.7
CVE-2020-5135	SonicWall SonicOS 拒絕服務弱點	9.4
CVE-2020-5902	F5 BIG-IP 流量管理使用者介面(TMUI)遠端程式碼執行弱點	10
CVE-2020-8195	Citrix ADC 和閘道不當輸入驗證弱點	6.5
CVE-2020-8196	Citrix ADC 和閘道不當存取控制弱點	4.3
CVE-2020-8243	Pulse Connect Secure 程式碼注入攻擊弱點	7.2
CVE-2020-8260	Pulse Connect Secure 檔案上傳不受限弱點	7.2
CVE-2021-1675	Microsoft Windows 列印多工緩衝處理器遠端程式碼執行弱點(「PrintNightmare」)	8.8
CVE-2021-20016	SonicWall SMA100 SQL 注入攻擊弱點	9.8
CVE-2021-20028	SonicWall 安全遠端存取(SRA)SQL 注入攻擊弱點	9.8
CVE-2021-20655	FileZen OS 命令注入攻擊弱點	7.2
CVE-2021-21972	VMware vSphere 用戶端遠端程式碼執行弱點	9.8
CVE-2021-21985	VMware vSphere 用戶端遠端程式碼執行弱點	9.8
CVE-2021-22005	VMware vCenter Server 遠端程式碼執行弱點	9.8
CVE-2021-22893	Pulse Connect Secure 不當驗證弱點	10
CVE-2021-22941	Citrix ShareFile 不當存取控制弱點	9.8
CVE-2021-22986	F5 BIG-IP iControl REST 遠端命令執行弱點	9.8
CVE-2021-26084	Atlassian Confluence Server Webwork OGNL 注入攻擊弱點	9.8
CVE-2021-26085	Atlassian Confluence Server 任意檔案讀取弱點	5.3
CVE-2021-26855	Microsoft Exchange Server 遠端程式碼執行弱點(「ProxyLogon」)	9.8
CVE-2021-27101	Accellion 檔案傳輸應用程式(FTA)SQL 注入攻擊弱點	9.8
CVE-2021-27102	Accellion 檔案傳輸應用程式(FTA)OS 命令注入攻擊弱點	7.8
CVE-2021-27103	Accellion 檔案傳輸應用程式(FTA)伺服器端要求偽造(SSRF)弱點	9.8
CVE-2021-27104	Accellion 檔案傳輸應用程式(FTA)OS 命令注入攻擊弱點	9.8
CVE-2021-28799	QNAP NAS 不當驗證弱點	9.8
CVE-2021-30116	Kaseya Virtual System Administrator(VSA)憑證外洩和商務邏輯弱點	9.8

CVE-2021-30119	Kaseya VSA 跨網站指令碼 (XSS) 弱點	5.4
CVE-2021-30120	Kaseya VSA 雙因素驗證迴避弱點	7.5
CVE-2021-31166	Microsoft Windows HTTP 協定堆疊遠端程式碼執行弱點	9.8
CVE-2021-31206	Microsoft Exchange Server 遠端程式碼執行弱點 (「ProxyShell」)	8
CVE-2021-31207	Microsoft Exchange Server 安全功能迴避弱點 (「ProxyShell」)	7.2
CVE-2021-34473	Microsoft Exchange Server 遠端程式碼執行弱點 (「ProxyShell」)	9.8
CVE-2021-34523	Microsoft Exchange Server 權限提高弱點 (「ProxyShell」)	9.8
CVE-2021-34527	Microsoft Windows 列印多工緩衝處理器遠端程式碼執行弱點 (「PrintNightmare」)	8.8
CVE-2021-34730	Cisco Small Business RV 路由器不當輸入驗證弱點	9.8
CVE-2021-36942	Microsoft Windows LSA 偽造弱點 (「PetitPotam」)	5.3
CVE-2021-38646	Microsoft Office Access Connectivity Engine 遠端程式碼執行弱點	7.8
CVE-2021-38647	Microsoft Azure Open Management Infrastructure 遠端程式碼執行弱點 (「OMIGOD」)	9.8
CVE-2021-40444	Microsoft MSHTML 遠端程式碼執行弱點	8.8
CVE-2021-40449	Microsoft Win32k 釋放後使用弱點	7.8
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus 驗證迴避弱點	9.8
CVE-2021-41773	Apache HTTP 伺服器路徑周遊弱點	7.5
CVE-2021-42013	Apache HTTP 伺服器路徑周遊弱點	9.8
CVE-2021-42258	BQE BillQuick Web Suite SQL 注入攻擊弱點	9.8
CVE-2022-26134	Atlassian Confluence 和 Data Center OGNL 注入攻擊弱點	10
NO-CVE-ID	EntroLink PPX-Anylink 遠端程式碼執行弱點	不適用

Tenable 如何提供協助

Tenable 已發布 Tenable.io、Tenable.sc 和 Nessus Professional 適用的掃描範本，這些範本已預先設定，能讓您針對本報告中所討論的弱點進行快速掃描。此外，Tenable.io 客戶還可以使用新版的儀表板和小工具程式庫中的小工具，Tenable.sc 使用者的新版儀表板中也會包含勒索軟體生態系統。

Tenable 安全應變團隊簡介

Tenable Research 設法跳脫弱點管理週期，主動制敵機先。我們的安全應變團隊會追蹤威脅與弱點情報摘要，確保我們的 Plugin 團隊能讓我們的產品盡快地涵蓋最新威脅與弱點。SRT 亦努力研究技術詳細資訊並編撰白皮書、部落格和其他宣傳文件，以確保客戶充分掌握這類風險的動向。SRT 在 Tenable 部落格上公布了最新弱點的細部資訊。

Tenable Research 已發布超過 171,000 個 Plugin，在 CVE 涵蓋範圍方面領先整個產業。此團隊全力開發弱點管理基礎所需的各項要素，包括：編寫弱點與資產偵測的 Plugin、制定稽核與合規檢查、加強弱點管理的自動化等。

作者簡介

Satnam Narang 是安全應變團隊的資深研發工程師。

供稿人

Claire Tills，安全應變部門資深研發工程師
Scott Caveza，安全應變部門資深經理

Tenable, Inc.
6100 Merriweather Drive 12th Floor
Columbia, MD 21044
North America
+1 (410) 872-0555

zh-tw.tenable.com

UNIFORCE 創泓科技
台灣區代理商 | 創泓科技股份有限公司
台北市內湖區洲子街77號10樓 | 電話：886 2 2658 3077 | 傳真：886 2 2658 3097
郵件：sales@uniforce.com.tw | www.uniforce.com.tw

關於 Tenable

Tenable® 是一家 Cyber Exposure 分析公司。全球大約有 40,000 家企業仰賴 Tenable 協助瞭解並降低網路風險。身為 Nessus® 的創造者，Tenable 拓展了本身在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。在 Tenable 的客戶中，包含大約 60% 的財星 500 大企業、大約 40% 的全球 2,000 大企業以及大型政府機構。如需深入瞭解，請前往 zh-tw.tenable.com。

tenable®

版權所有 2022 TENABLE, INC. 保留所有權利。TENABLE、TENABLE.IO、NESSUS、ALSID、INDEGY、LUMIN、ASSURE 及 LOG CORRELATION ENGINE 為 TENABLE, INC. 或其子公司的註冊商標。TENABLE.SC、TENABLE.OT、TENABLE.AD、EXPOSURE.AI 及 THE CYBER EXPOSURE COMPANY 為 TENABLE, INC. 或其子公司的註冊商標。
所有其他產品或服務是其各自所有者的商標。