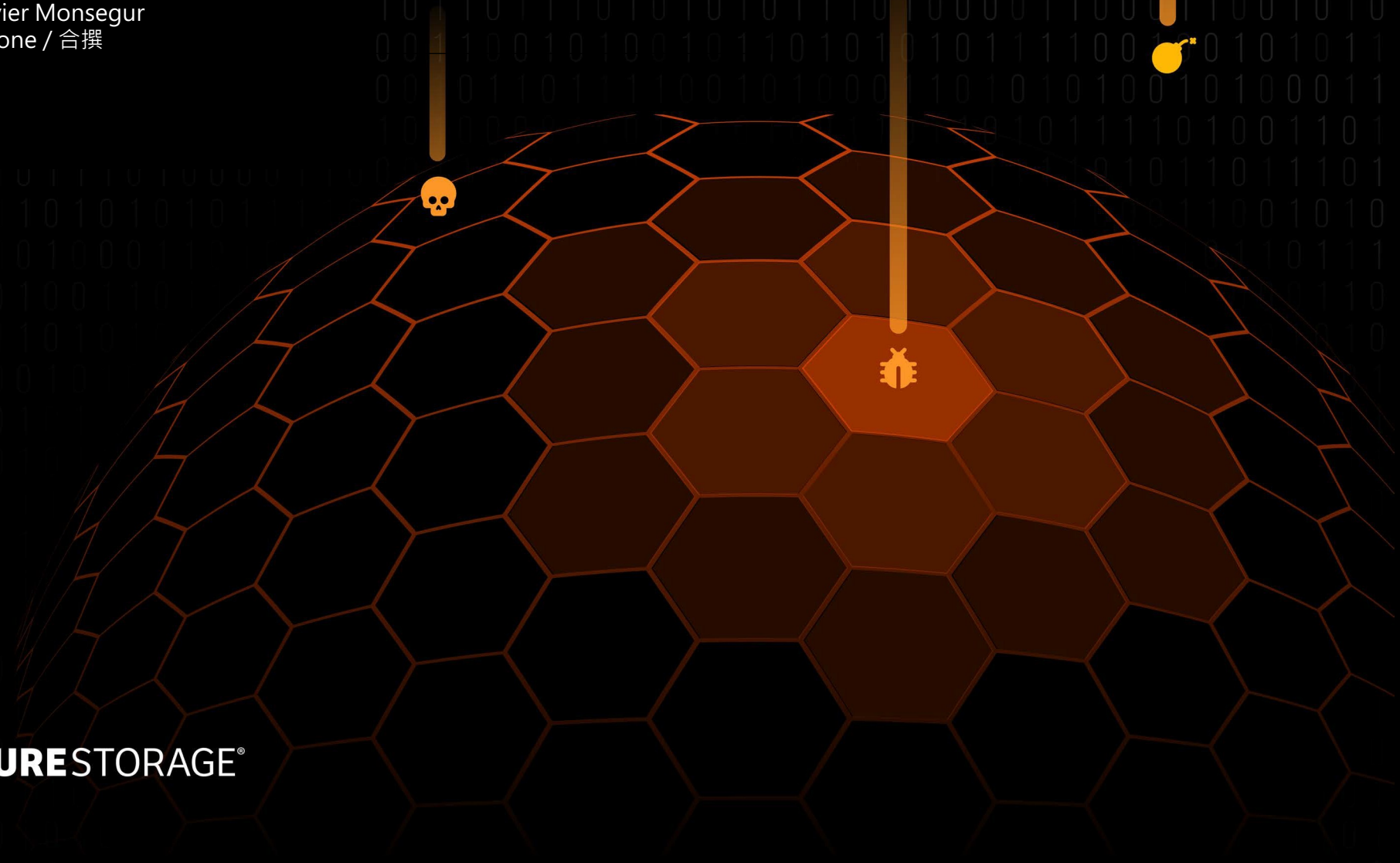
駭客指南

勒索軟體緩解及復原

Hector Xavier Monsegur
與 Andy Stone / 合撰



PURESTORAGE®

目錄

簡介

打擊勒索軟體攻擊的戰鬥愈演愈烈，在 2022 年 4 月至 2023 年 4 月間，勒索軟體攻擊數量增加了 37.75%[1]，令人感到震驚。

最近，大學、醫療系統、公共事業公司，甚至全球最大的連鎖賭場發生的網路安全事故成為頭條新聞，此事件突顯了一個殘酷的現實：沒有組織能夠倖免——而且風險只會越來越高。隨著威脅情勢的不斷演進，網路犯罪份子變得越來越大膽與老練，贖金金額不斷飆升。簡而言之，現在正是優先執行防止勒索軟體威脅、偵測、回應動作的時刻。

著作*《駭客指南：勒索軟體緩解及復原》*的目的是詳細介紹當今勒索軟體威脅情勢、提供專家指導來幫助您為攻擊做好準備，並保護您公司的資料。

您將學習的內容

1. 為何勒索軟體攻擊日益猖獗
2. 攻擊者在攻擊發生前後的作案手法
3. 您可以採取哪些措施來降低遭受攻擊的風險並於發生資料遺失時最大程度地減少損失
4. 如果偵測到進行中的攻擊該怎麼辦
5. 遭受攻擊後如何快速復原及恢復

當今威脅情勢

從 2000 年代中期到 2010 年代初，「駭客社會運動參與者」發動網路攻擊以推動社會或政治訴求的現象頗為常見，但這些組織鬆散的國際組織近年來已大幅減少活動。組織內部安全狀況的改善，大大降低了專注於容易得手的目標的新手駭客的成功機率。針對 Anonymous 和 LulzSec 等駭客社會運動組織成員的逮捕及起訴，有助於暫時阻止攻勢。

然而，儘管駭客活動減少，網路攻擊的威脅仍然存在。2022 年間，世界各地的組織偵測到近 5 億次勒索軟體攻擊，每 11 秒就會發生一次勒索軟體或網路釣魚攻擊。

如今，勒索軟體攻擊的主要來源是由國家資助的勒索軟體恐嚇取財集團，此類集團經常合作，這反映出全球合作與攻擊的複雜性不斷提高。

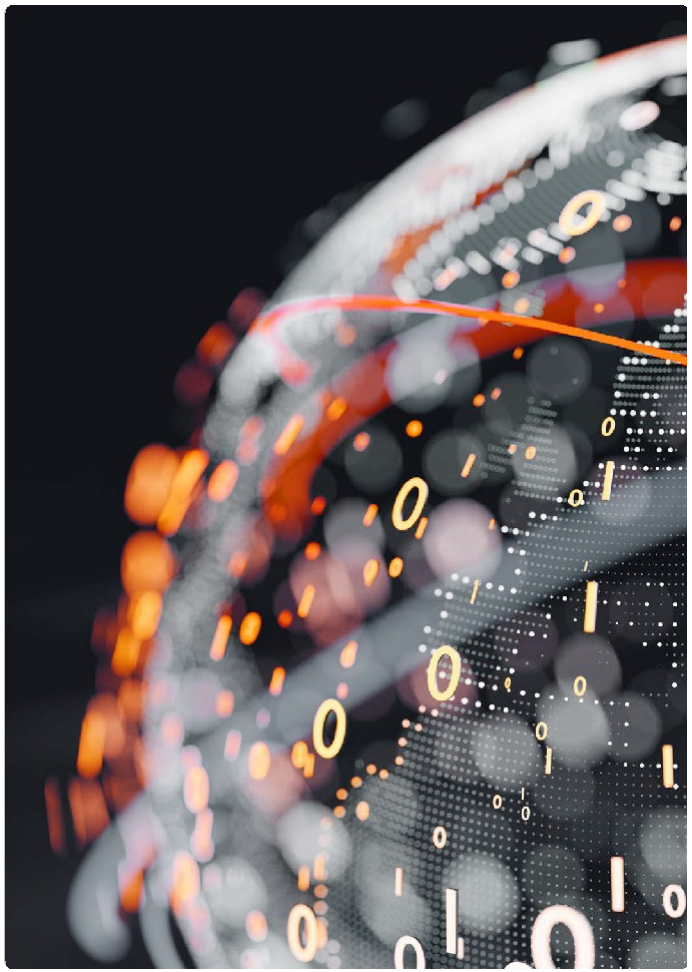
此類組織幫助將勒索軟體作為可以在「暗網」上購買的服務「工具包」分送出去，繼而使熟練 (與此同時，非熟練越來越多) 私部門的攻擊者能夠出租其駭客能力，如同傭兵一般。國家機器發現，這是一種既省錢又有效的方式，來資助意圖造成破壞的勒索軟體運作。

最近的另一個發展是無加密的勒索攻擊，這對於受害者及網路安全專業人員而言，尤其具有挑戰性。在這種情況下，攻擊者會繞過加密直接瞄準並危害重要系統及資料，因此需要了解導致攻擊的技術以制定有效的緩解策略。

在網路安全方面，人工智慧 (AI) 也佔據了主角的位置。勒索軟體團體正在加大力度，使用人工智慧開發的惡意軟體程式碼、聊天機器人等，發展出複雜的方式以繞過傳統的網路安全措施。

為了回應上述不斷升級的網路威脅，美國政府已將勒索軟體列為國家安全議程的首要議題，發布了與勒索軟體支付相關之新政策，並追究窩藏網路犯罪份子之國家的責任。美國政府甚至概述了企業可以採取的加強防禦措施，以回應當前的勒索軟體威脅。

韌性是 2023 年白宮網路安全策略的首要任務



財務動機

隨著攻擊者的轉變，攻擊的動機也隨之改變。多年前，「駭客社會運動參與者」的攻擊動機為政治觀點、文化或宗教信仰之差異、民族自豪感或恐怖主義意識形態。如今，勒索軟體攻擊的主要動機為求取金錢，贖金越開越高，至 2023 年時，平均贖金達到 74 萬美元。[2]

導致贖金金額狂飆的因素之一，是網路保險在勒索事件中扮演的角色。提供網路保險服務的公司，歷來傾向於迅速屈服於攻擊者的贖金要求。這使得駭客更加大膽地行動，並導致網路保險保費急遽增加，條款與條件更加嚴苛，承保人資格審查也更加仔細嚴格。

隨著網路保險承保率逐漸降低，且保費不斷上漲，網路風險管理之基礎設施預算較多的企業，比起小型企業更有可能加保網路保險，也導致其成為不法份子更容易下手的目標。據了解，攻擊者甚至會研究攻擊目標公司已加保多少保險，再要求受害者支付全部保額。當受害者宣稱無法支付時，攻擊者便會指出受害者的保單額度。

然而重點在於：無論大小，各種規模的組織都是網路犯罪份子的目標。只要受害者乖乖支付贖金，不法份子就會持續攻擊，並尋找新的方式剝削受害者。

閱讀電子書

支付贖金只是第一步

當然，當涉及勒索軟體攻擊的總成本時，網路保險保額的影響還不是最嚴重的。

即使有能力支付贖金的組織，在營運過程中也經常發現更大規模、代價更高的問題。根據 FBI[3]的數據，2022 年網路犯罪造成的損失總額達到驚人的 102 億美元，增加了將近 48%。IBM 最新的資料外洩調查報告指出，勒索軟體攻擊對組織造成的平均損失（不包括贖金）目前已超過 450 萬美元[4]。該數據為損失總計，通常包括營運中斷、聲譽損害、新型安全設施的投資、法律訴訟等。

攻擊者面臨的低風險

從攻擊者的角度看來，加密貨幣降低了要求贖金的風險。

例如，JBS 據傳在最近的勒索軟體攻擊後（使用比特幣）支付了 1100 萬美元的贖金，才能恢復網站正常運作。分析師表示，比特幣 (Bitcoin) 以及門羅幣 (Monero) 與 Zcash 等其他加密貨幣，使得向大型企業勒索巨額贖金成為可能。由於加密或幣交易是匿名的，因此被抓到的可能性極小。

勒索軟體專案小組 (Ransomware Task Force) 是一個由政府官員、私部門技術專家與執法部門組成的國際聯盟，該小組指出，由於加密貨幣具有無國界的性質，因此增加了追蹤勒索軟體犯罪份子的難度。

網路安全措施不足

勒索軟體攻擊激增的另一個關鍵因素是：大多數組織沒有足夠的防禦機制。

因此，三分之一的 IT 最高主管，對其復原與恢復基礎設施的安全性表示嚴重擔憂，也就不足為奇了。許多 IT 主管未能解決明顯的安全漏洞。IT 團隊通常專注於吸睛的新式安全技術，但缺乏徹底執行網路衛生習慣，例如密碼身份驗證、身分管理、備份策略、事故管理。上述習慣未能認真執行的結果，便是讓攻擊者變得更輕鬆，通常他們會專注於尋找最簡單、最具成本效益的方式入侵企業組織的系統。

威脅模式及分析[6]

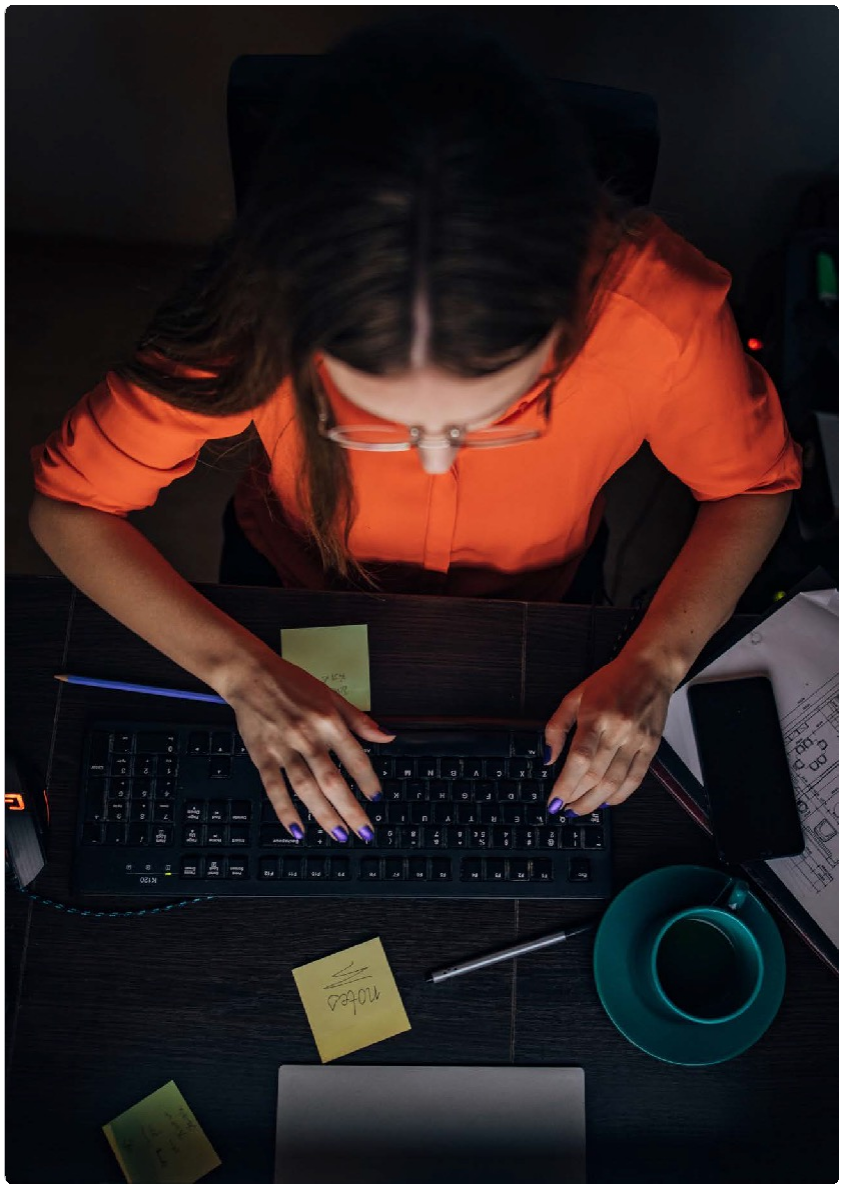
83%

違規行為涉及外部參與者，其中大多數是出於金錢動機。

74%

違規行為涉及人為因素者，
其中包括社交工程攻擊、錯誤或濫用。

別忽視人為因素



網路安全措施通常未考慮人類心理。在我們所見過的所有攻擊中，只有一小部分是利用漏洞、零時差攻擊或直接損害服務的技術攻擊。

大多數攻擊都是從人開始的。此類攻擊使用網路釣魚電子郵件、語音釣魚，或是利用攻擊者及其自動化系統或工具與受害者之間的其他互動，使攻擊者足以竊取使用者的登入憑證。然後，攻擊者可以像其他使用者一樣使用到手的憑證登入網路。

由於許多心理上的因素，人類往往成為上述攻擊手法的受害者。他們可能沒有受到充分的訓練。他們可能想幫助別人。他們可能害怕別人認為他們很無能。他們可能畏懼失去這份工作。出於上述種種原因，如果他們看到執行長提供的連結，便會點選下去。如果攻擊者的前置作業只要花上短短幾天，攻擊成本又可以降低到 100 美元以下，就能夠針對市值十億美元的企業發動社交工程攻擊，那麼攻擊成功便是全方位的勝利，且極為有利可圖。

另一個問題來自內部。我們已經目睹許多國家與其他攻擊者以金錢賄賂員工，在組織內部安裝勒索軟體。

因此，安全措施、賄賂和人類心理 (員工向網路釣魚攻擊者交出存取憑證) 的結合，會導致攻勢成功，使攻擊者能夠在內部網路中橫向移動，到最後足以發動勒索軟體攻擊。

勒索軟體防護的三大支柱

由於大多數企業在過去 12 個月內都遭遇過勒索軟體攻擊，做好準備不僅是一個好主意， 而是現今維持企業運作必須完成的工作。這也表示我們要了解駭客的手法，並制定計畫載明在勒索軟體攻擊發生前、發生時、發生後應確實做到之事項。本人曾從事網路攻擊，並擁有擔任組織合作防禦攻擊顧問之相關經驗，以下為本人提出之具體建議。

三大支柱

1. 攻擊發生前
2. 攻擊發生時
3. 攻擊發生後復原資料

PILLAR 1

攻擊發生前

在網路犯罪份子發動攻擊前，會先進行偵察以確定目標。他們可能會先尋找較有可能支付贖金的、已購買網路保險的公司。他們有一個明確的方法來評估目標的攻擊面、尋找攻擊面的弱點、並建立適當的攻擊路徑。

例如，攻擊者可能鎖定與市值數十億美元的公司合作的小型網路服務業者 (ISP)。攻擊者透過識別以下內容，以發掘該 ISP 的潛在入侵方式：

- 支援會回應攻擊者以社交工程接觸的員工
- ISP 使用的服務、工具或軟體，及攻擊面的廣度
- 已發布 SSL 憑證的內部主機名
- 找出擁有可挾持資源的 DNS 名稱或主機名稱

一旦攻擊者進入 ISP，即可入侵更大型的企業。

在攻擊發生前您可以做什麼

為了阻止上述偵察工作，並防止潛在攻擊，主動與先發制人極其重要。

換句話說，您需要在發生事情之前，制定健全的網路安全計畫。

制定計畫時，請執行下列步驟：

1 提高可視性

第一步是要獲得技術、營運與組織的。

- **技術可視性**需要充分了解您的網路上所有已連接上之設備、其弱點及其面臨的威脅。該任務需要使用正確的工具來了解您的系統，方可辨別出異常情形。例如，快速分析平台可以幫助您在攻擊者入侵之前發現可疑行為、異常等，使您能夠在資料大規模受損之前，指出威脅並消滅之。
- **營運可視性**可防止構成大部分網路安全事故的網路釣魚攻擊。亦即去充分了解大家存取資料的方式與原因，以及您提供的網路安全訓練內容為何。
- **組織可見度**將有助於減少因聲譽受損而造成的業務損失—聲譽受損是造成資料外洩成本的最大原因。該任務需要能夠評估攻擊可能損害公司品牌、聲譽或智慧財產權之程度的能力。

2 取得控制權

一旦您知道您的網路上有什麼，便可藉由執行所有必要的安全衛生措施，消除攻擊面中的明顯漏洞。例如，確保路由器和防火牆配置正確、保持 IT 系統之狀態為修補完成升級至最新版本、定期更新白名單與黑名單、強制執行強式密碼規則與多重要素驗證 (MFA)。

3 減少作業環境之表面積

攻擊面更小，保護您的網路便更容易。減少表面積的方式就是消除重複資料。例如，擁有較少版本的 Windows 或 Linux 可以更輕鬆地以一致的方式管理及維護。

4 增加攻擊成本

攻擊者總是尋找最簡單的存取途徑。當我是敵手時，我專注於攻擊我熟悉的服務與媒介。因此，為了破解攻擊者的詭計，您只需要讓攻擊者感到與其入侵您的環境，不如入侵其他網路環境更為省事即可。您可透過下列方式，讓攻擊者打退堂鼓：

- 部署正確的工具，例如集中式日誌記錄及事件。
- 與您的解決方案供應商合作，了解所提供的功能並正確使用、確實執行解決方案。
- 保持良好的系統衛生。

5 建構分層韌性架構

由 Pure Storage® 建立的 分層韌性架構 足以提供多層次的防禦。

- 對於第一層資料及應用程式（即核心資料庫與應用程式服務，及其定義之相依性）、 FlashArray//X™、FlashArray//XL™，或 FlashArray//C™ 上的 SafeMode™ 快照，存放 3 至 7 天。
- 為 FlashArray//C、FlashBlade//S™ 或 FlashBlade//E™ 上的第二層資料建立快照封存，以滿足長期儲存（三個月以上）或法令遵循上之需求。
- 在極端情境下，可將有獨立軟體供應商 (ISV) 的 FlashArray//C 或 FlashBlade//S 及企業應用程式原生解決方案結合使用，以允許將備份資料直接寫入陣列，並透過不可變快照與 SafeMode 進行保護。您也可以使用 FlashBlade//E 來取代傳統的旋轉磁碟備份。
- 可選配的第四層防禦由一個建構於 FlashArray//C 或 FlashBlade//S 上的單向資料碉堡組成，用於應對大規模災難。

6 建立應變策略

投入時間撰寫一份應變手冊，詳細說明您的組織應如何在攻擊發生前回應攻擊之策略。每家公司的應變策略都是獨一無二的，但可能包括：

- 分析安全性資訊與事件管理 (SIEM) 日誌中的事件，以識別可能已遭入侵之系統及使用者
- 聯絡事故應變團隊與事故應變供應商
- 關閉網際網路連線
- 關閉機器
- 與執法機關溝通
- 為公司高層及董事會準備事故報告

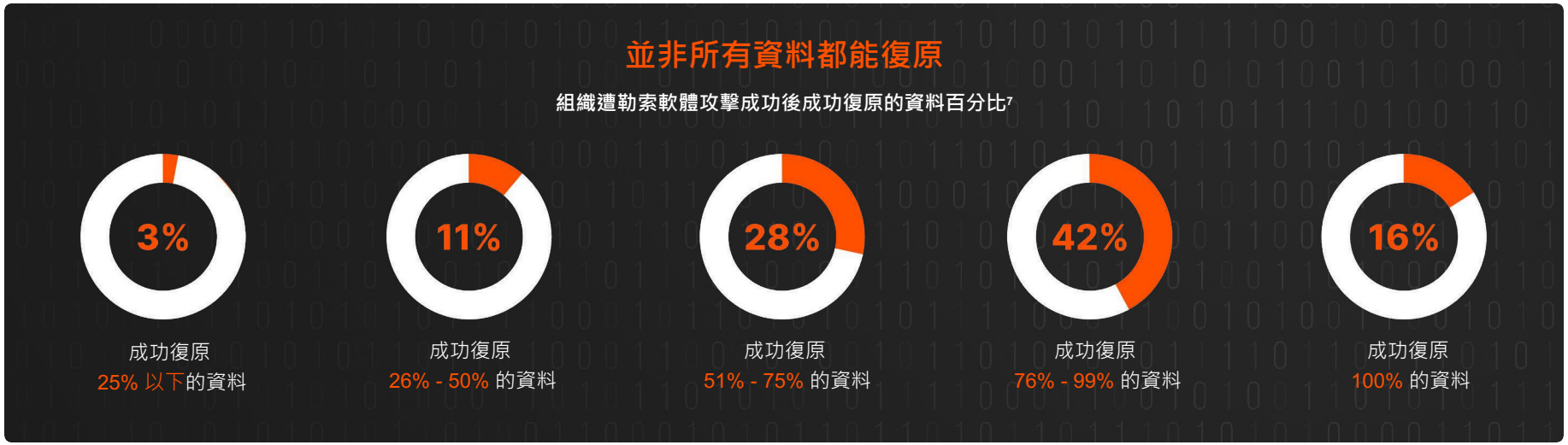
7 提供適當訓練

確保監控安全工具的 IT 人員了解日誌內容的意義，以及在偵測到異常情況時如何反應。

8 制定全面性的業務連續性及災難復原計畫

儘管已主動積極地訂出計畫，網路攻擊仍然可以讓您癱瘓。您需要建立全面性的業務連續性及災難復原 (BCDR) 計畫，做好盡快復原的準備。

- 定義您的環境中有哪些應用程式及系統，並指出哪些最關鍵。
- 與您的業務範圍內的團隊合作，了解他們必須並期望要多快速將資料恢復至線上，以便您可以部署正確的系統與控制來滿足 SLA 之需求。
- 執行正確的架構以備份資料，並建立可回復性層級。
- 請與您的備份供應商詳談，以了解您的產品的用途，以及如何正確執行該產品。由於駭客比以往任何時候都更有可能瞄準備份資料及詮釋資料，因此您選擇的儲存供應商，必須提供備份資料及相關詮釋資料目錄的不可變、唯讀快照。
- 測試所有元件，以確保在發生非計劃性停機時（無論原因為何）您可以快速復原。
- 請注意，攻擊者會將您的關鍵基礎設施作為目標。若您的關鍵基礎設施遭到攻擊，您將無法存取核心系統，或使用遠端存取工具，甚至電子郵件。您需要計劃如何將對的人帶到對的地方。您需要說明清楚該聯絡誰、按照何種順序、每個人該去何處待命，以及需要在待命處做些什麼。



PILLAR 2

攻擊發生時

在攻擊過程中，網路犯罪份子開始針對您的公司攻擊面的弱點攻擊。

例如，假設在監視過程中，攻擊者發現了指向易受攻擊的 WordPress 部落格的 DNS 主機名稱。攻擊者接著可能會破壞該執行個體，以取得託管它的伺服器的存取權限。然後，他們可能會發起網絡釣魚行動，使用包含主機名的 URL 來說服員工點選假網頁的連結，並在該網頁中請求使用者提供公司內部網路或 VPN 的憑證。

一旦攻擊者使用這些竊取到手的憑證進入內部網路，攻擊者便可橫向移動，存取伺服器以滲透資料、竊取智慧財產權或發動勒索軟體行動。上述攻擊的速度非常快，可能會在 30-40 分鐘內傳播到整個企業內部網路，同時進入您的備份並刪除它們及/或更改您的憑證，這樣您就無法進入。或者，在初次進入後，攻擊者可能會紋風不動數星期或數月，同時監視網路以了解您將如何回應，再制定攻擊計畫或策略並部署勒索軟體。因此，網路風平浪靜並不表示攻擊者沒有潛伏於其中。

攻擊發生時該怎麼做

假設您擁有所有得當的網路監控工具（例如 SIEM 日誌），訓練有素的人員在尋找異常及事故時，便能識別出正在發生的攻擊。當攻擊發生時，應該立即採取行動。

1 識別攻擊

您可以藉由尋找事件中的異常狀況、網路流量類型或正在使用的協定來識別攻擊。異常是指沒有道理的事件。舉例來說，您可能會看到一位員工登入網域控制站，或一位秘書登入備份伺服器。上述活動表示攻擊者已經入侵並取得了使用者憑證，並使用其登入他們不應該登入的系統。

攻擊的另一個徵兆，是網路上的流量類型。例如內部網路上的 IPv6 流量通常用於繞過用於監控 IPv4 流量的安全產品，因此在 IPv6 使用量為零的網路上看到此類流量，表示可能已遭到入侵。應該注意的是，Windows 系統可能會發出 DHCPv6 請求，尋找可由敵手提供的連結與 DNS 詳細資訊，但除了偵聽和回應廣播請求之外，沒有太多特權。

進一步的攻擊跡象可能來自 LLMNR 和 NBT-NS 等廣播通訊。上述協定會廣播名稱轉換請求。若伺服器用任意主機回應此類廣播請求，那麼對於防禦者來說，就表示攻擊者藏身在網路中，且漏出了馬腳。攻擊者也常對內部 Windows 網路發動簡易的攻擊。

2 執行您的計畫

一旦您確認自己受到攻擊，就應該執行您先前制定的應變計畫。遵循事故應變計劃及復原程序極為重要。否則，網路與系統管理員只能使用自己的判斷來消除威脅，根據我的經驗，這通常是無效的，甚至可能會帶來災難。

3 準備調查

聯絡負責事故應變的人員，與高階主管及法律團隊溝通，並為您的供應商及/或執法機關執行之調查做好準備。如果您委託一家公司進行調查，請確保他們與執法機關之間確實交接。

4 您應該支付贖金嗎？

一般而言，我認為組織不應該支付贖金，因為這只會鼓勵對方展開更多攻擊。例如，Cybereason 的一份報告發現，80% 支付贖金的組織再度遭到攻擊。

但其中涉及許多變數。舉例來說，如果您經營一家重症病房醫院，如果沒有這些系統，醫生將無法治療患者，您可能需要立刻支付贖金。換句話說，您需要根據您的具體情況，評估是否需要支付贖金。

無論您做什麼，都要小心攻擊者可能會三番兩次找上門。他們不僅會加密資料並逼迫您付款，還可能勒索您支付更多費用，否則他們會將您的資料洩漏至網上。最後，他們會威脅要告訴媒體，讓您的客戶都知道這次攻擊發生過。披露此種訊息可能會導致額外的法律費用支出、必須配合遵循法律向主管機關備案，以及嚴重的聲譽損害。

5 如果您沒有安全計畫，會發生什麼事？

不幸的是，由於缺乏預算或人力等限制，許多組織沒有制定適當的安全及可復原性計畫。若組織擁有安全團隊，則團隊中各成員之角色可能無法適切定義。

如果您沒有應變計畫，情勢可能會變得非常不確定，因為您的安全團隊不知道該怎麼做。如果安全工程師、分析師或事故應變人員識別出攻擊，但在缺乏給予其應變架構的策略的情況下，最終您可能會陷入完全混亂。您可能不了解遭到入侵的全部範圍。他們可能會將不需要下線的系統下線。或者，您可能根本無法向事故應變供應商或內部團隊傳遞足夠的資訊，以幫助解決此災難情境。

越來越多受害者選擇支付贖金[8]

2022	2023	
46%	46%	支付贖金以取回資料
73%	70%	使用備份以取回資料
8%	2%	使用其它方式以取回資料
61%	97%	使用加密以取回資料之總計

PILLAR 3

攻擊發生後復原資料

您的業務離線的每一分鐘都會讓您產生金錢損失。

根據資訊科技情報諮詢公司 (ITIC)，對於大多數企業而言，一小時的停機成本約為 30 萬美元。對於好市多 (Costco)、目標百貨 (Target) 或沃爾瑪 (Walmart) 等大企業來說，成本很容易增加至每分鐘數百萬美元。目前，企業因勒索軟體攻擊而導致的平均停機時間為 24 天。[9] 從攻擊中完全復原需要更長的時間，從數週到數個月不等。

考慮到如此高昂的成本，任何違規行為的持續時間越短越好。攻擊發生後，您需要盡快清理並復原系統。

攻擊發生後需採取的步驟

1 清理您的系統

在攻擊期間，您的防禦團隊應該隔離並將遭入侵的網路系統斷線。攻擊結束後，就需要全面檢查網路上的所有系統，以確保不留下任何痕跡或惡意軟體。否則，您可能會發現自己處於這樣的情況：關閉多個系統、進行搬移、復原資料以及使網路重新連線後，又讓勒索軟體自動重新啟動。因此，在從備份中還原資料並重新連線之前，請確保將網路環境徹底完成消毒。

2 迅速復原

在遭受攻擊之前，您應該建立主動與預先準備好的復原措施，包括執行 BCDR 計畫。計畫中應包括備份，此備份必須可從其中復原未刪除之部分。您也應該確保您能快速復原，因為每一分鐘的停機都會造成金錢上的損失。但是，為了有效且快速地復原，您必須有目前或最近的可復原點。否則，您的復原過程將會減慢，甚至無法復原。確保您的儲存及備份解決方案能夠提供一定程度的可復原性，絕對至關重要。一個好的解決方案是利用現代化儲存技術，防止攻擊者完全刪除您的組織的資料。

請別忽視這樣一個事實：攻擊事件過去後，您現有的陣列將無法再使用。這就表示，被保險或執法機關標記為需要進行鑑識採證調查的所有受影響陣列，皆無法使用。Pure Storage 的勒索軟體復原 SLA 可保證乾淨的陣列與復原計畫，使系統快速復原並重新運作。

Pure 與 Cohesity、Commvault、Rubrik、Veeam 和 Veritas 等出色的資料保護公司合作。我們的系統經過測試，以確保其能與您的軟體無縫協作，並確保您無需進行堆疊式升級。

擁有適當的沙箱環境可用於對快照與備份資料進行鑑識採證分析，同樣非常重要。在不執行鑑識採證審查與徹底清理以移除攻擊者留下的、已識別出的入侵跡象的情形下，您無法直接進行復原。當您試圖在攻擊中找到「零號病人」時，擁有可靠的日誌記錄環境來提供適當的可視性，對於您的復原過程至關重要。

3 適應、復原及應對

當復原完成並重新運作後，最重要的是要回顧發生之事件經過並從中學習，並相應地修正您的系統及策略，如此您才真正學到一課，方可繼續前進。此類事件後之評估不僅應該關注技術，還應該關注人員及流程。例如，您可能會發現需要更全面性地教育使用者，如何識別網路釣魚攻擊。藉由評估所學到的經驗教訓，並將其納入您的計畫及政策中，您便能不斷改進您的準備及應對能力。

結論

透過了解勒索軟體攻擊發生的原因和方式，以及攻擊發生前、發生時與發生後您應該做什麼，您便能做好更堅實的準備以防止攻擊或快速復原。這些行動應包括使用正確的供應商提供的正確工具並適當執行計畫，並為您的技術團隊和終端使用者提供教育訓練。您還應確保正確設定及管理強密碼之執行，並清點您的軟體及資產，以便保護它們並最大限度地減少攻擊面。

Pure Storage 解決方案可以協助完成上述工作，確保您的資料不會被加密、以受保護的方式儲存，並利用頻外管理、多重要素驗證方法，以保證即使是具有管理訪問權限之人員或流程，若沒有來自 Pure Storage 的手動互動與介入，便無法完全刪除資料。Pure Storage 產品與解決方案可確保您有一個可復原性的起點，並提供最快的復原解決方案，讓您的業務迅速復原並運作。

了解更多關於 Pure Storage 勒索軟體解決方案之相關資訊

附註：

1 - Zscaler ThreatLabz 2023 年勒索軟體報告 | Zscaler, 2023

2 - 支付網路贖金之平均金額 | Statista, 2023

3 - FBI 網路犯罪報告 | 聯邦調查局網路犯罪投訴中心，2022

4 - 2023 年資料外洩成本報告 | IBM, 2023

5 - 照亮勒索軟體準備及緩解之路 | ESG, 2023

6 - 2023 年資料外洩調查報告 | Verizon, 2023

7 - 照亮勒索軟體準備及緩解之路 | ESG, 2023

8 - 2023 年勒索軟體現況 | Sophos, 2023

9 - 勒索軟體攻擊後之平均停機時間 | Statista, 2023

作者簡介

Hector Xavier Monsegur

Hector Monsegur 是國際公認的全球網路安全問題專家，也是網路攻擊與網路戰爭議題的引領者。 Monsegur 先前的網路代號為「Sabu」，曾是 Anonymous/LulzSec 駭客組織背後的技術專家。身為一名「黑帽駭客」，他強調許多組織中的關鍵漏洞，包括政府、軍事組織及網路安全公司。後來，在他與美國政府合作時，Monsegur 發現了針對主要聯邦基礎設施（包括美國軍方及 NASA）的關鍵漏洞與潛在攻擊。自從與美國政府和全球的商業安全高階主管合作以來，他已經協助阻止了超過 350 起針對美國政府電腦系統的網路攻擊。如今，Monsegur 致力於識別科技業、醫療保健業、金融業、政府機關等諸多產業的漏洞，並保護客戶系統的安全。在他的領導角色中，他分享了無與倫比的技術經驗，以教育其他從業人員並指導技術研究。

Andy Stone

Andy Stone 於 2019 年 4 月 加入 Pure Storage，擔任美洲地區技術長 (CTO) 的職位，主要督導業務為支援市場推廣及內部產品開發活動。在加入 Pure 之前，Andy 曾在 PwC 擔任美國及全球技術長暨全球安全技術及工程主管，為該公司位於全球 160 個地區之近 30 萬名使用者提供支援。在 PwC 時，Andy 執行了許多全球技術解決方案，以提高整體可用性、可擴充性及安全狀況，同時提高整體 IT 服務之效能。他還是 PwC 桌面虛擬化計畫之領導人，以提高終端使用者的可用性，並防止外部攻擊與內部資料外洩。在加入 PwC 之前，Andy 擔任蘇黎世保險 (Zurich Insurance) 集團旗下 Farmers 保險之資訊安全長暨安全工程、架構、技術及策略全球主管，領導了超過 140 個國家的全球安全轉型。Andy 也曾在 Accenture 工作，督導建立了數種安全產品，包括身分識別及存取管理、應用程式安全性以及 Accenture、Avanade、Microsoft 之間的 Power of 3 聯盟。他也與眾多《財星》世界 500 強企業合作，提供思維領導力並協助設計、實施與支援廣泛的客製化及商業技術解決方案。Andy 擁有印第安那大學布魯明頓分校 (Indiana University, Bloomington) 商業–資訊系統學士學位與南加州大學 (University of Southern California) MBA 學位。Andy 曾在眾多會議上發表演講，並就安全與其他技術的諸多主題發表過文章。最後，Andy 擁有數種身分及存取管理技術的安全領域專利。

PS2534-01-en 01/24