FORCEPOINT
POWERED BY Raytheon

白皮書

網路威脅潛伏時間和內部橫向擴散

全新的網路安全藍圖

目錄

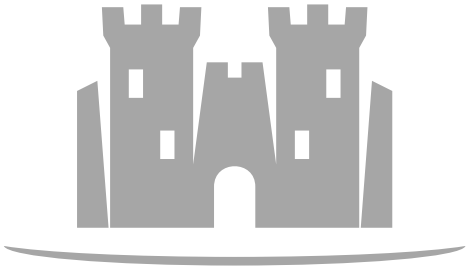
前言

1971 年，一位任職於 Forcepoint BBN Technologies 的年輕工程師 Ray Tomlinson 引進一個目前已無所不在的「@」符號，改變了我們已知的溝通模式。電子郵件的推出、網路和資料共享的擴大，以及網域名稱系統的推動，為全球人類、各行各業和政府機關，帶來技術與創新的契機。然而，這些契機也讓威脅行動者有機可趁。網路罪犯企圖利用協議、應用程式和作業系統，在這些新發明的公開作業中奪取好處。

另一方面，網路防護者卻發現自己處於週而復始的循環中，不斷利用修補程式、覆蓋層和新技術來填補安全缺口。當然，他們的努力值得我們肅然起敬，但最後卻仍功虧一簣，因為他們往往專注於本質上就不夠安全的技術基礎架構。

IT 資安專家，以及掌管業務的行政主管所渴求的，無非是把網路和系統攻擊者拒於門外，但這個遊戲計劃早已被證實為不可能的任務。以下這則頭條新聞早已廣為流傳，當中所揭露的資訊令人驚憂：2015 年威瑞森資料外洩調查 (2015 Verizon Data Breach Investigations) 報告指出，2014 年發生超過 79,790 件的資安事故。[1]

我們要對這句話提出一個問題：如果不可能預防入侵事件，那麼網路資安專家應如何集中精力，將攻擊的影響降至最低呢？



將負擔移轉給攻擊者

我們清楚的瞭解到，「護城河和城牆」法則明顯的不足以建構安全的網路。組織如欲強化其防禦能力，務實的做法包括：

1. **承認當今的現實** – 網路入侵難免會發生，你不能否認它是無法避免的。
2. **辨識威脅的形勢** – 攻擊同時來自組織的內部和外部。若是來自外部，攻擊者也將模仿偽裝成是您的內部員工。
3. **識別攻擊的途徑** – 攻擊者所行經的網路內部路徑，為其入侵意圖和潛在的影響，提供了重要的洞察線索。我們稱此類活動為內部橫向擴散。
4. **限制入侵的壽命** – 採取必要的行動，將攻擊者身處於您網路內部的時間（亦稱為網路威脅潛伏時間）減至最少，從而透過減少入侵的時間，來限制潛在的影響。

本白皮書的重點將聚焦在第 3 和第 4 點，並介紹內部橫向擴散和**網路威脅潛伏時間**的概念。企業組織一旦瞭解這些概念後，可望將威脅的負擔移轉給攻擊者，進而讓企業組織的資產和基礎架構，變成較無吸引力的目標。

1 資料來源: http://www.verizonenterprise.com/DBIR/2015/

2015 年威瑞森資料外洩調查 (2015 Verizon Data Breach Investigations) 報告指出，

2014 年發生超過 **79,790** 件的資安事故。[1]

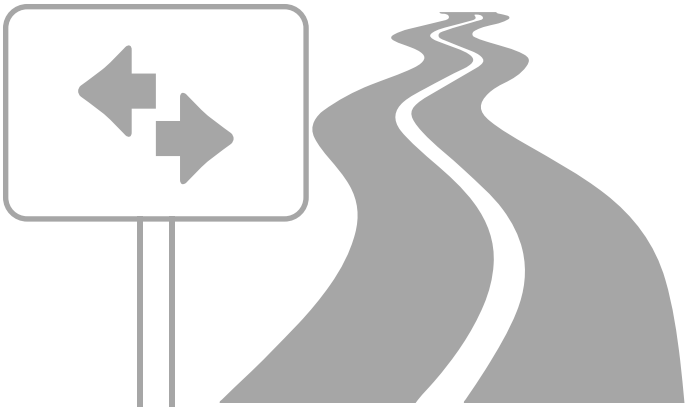
林中小徑：瞭解內部橫向擴散

進階攻擊往往有特定目的，而且企圖明確。如考慮到這點，企業組織便不應該從短期角度來分析這些攻擊。

例如：一旦發現機器已遭受攻擊，我們應問幾個基本的問題：攻擊者穿越過了哪些裝置？怎麼有可能發生這樣的移動？最終目標是什麼？執行了哪些控管作業，讓威脅得以持續進行？

回答這些問題時，資安防護者必須瞭解到，魚叉式網路詐欺、水坑攻擊，以及任何其他惡意程式傳遞法，都會有結束的時候。被感染的系統，儘管本身有多麼的重要，但對進階的攻擊者來說，都是不必要的。他們在乎的是：穿越過企業網路時能不被偵測到。

具體而言，惡意程式首次發生的目的，並非儘可能擷取越多智慧財產越好，而是建立閘道以便潛入未受攻擊者控管的環境。那個被滲透的系統，就成為代理伺服器，以開展橫向擴散的流程。其後可能會有一個橫向或 100 個橫向步驟，以便取得目標智慧財產或控制系統。在許多案例中，威脅者把目標對準個人的憑證，進而偽裝成合法使用者，輕鬆進出網路。瞭解入侵的所在、以及攻擊是如何發生的，才是關鍵的重點，因為我們能深入瞭解其企圖和潛在影響。



攻擊的壽命：遏制網路威脅潛伏時間

就如上方所討論的，務實的企業組織瞭解到，入侵定會發生，而預防入侵發生，儘管是非常必要的做法，卻不能充當為唯一的安全戰略。他們也必須專注於遏制行動。盡速辨識和遏制攻擊者才是最為重要的防禦對策。

就如同破壞公物者會在下班時間潛入學校，遏制網路威脅潛伏停留時間的目標是：確保破壞者的攻擊時間儘可能的縮短，以免造成嚴重損害後，再從企業重要資產中抽身逃脫。研究調查顯示，攻擊者平均能夠在網路內停留 200 天，才會被企業根除。[2] 由此可知，他們足以在這段時間內造成一定程度的損害。所以，若能在較短時間內就遏制攻擊者，讓他們接觸到較少的企業內部網路環境，他們則將耗用更多資源才能竊取想要的資料。

要減少網路威脅潛伏的時間，您必須瞭解其運作概念。網路威脅潛伏的停留時間是從攻擊者潛入您的網路開始，並持續到您趕走他們、或他們自行離開為止（大概是他們已完成惡意行動後）。我們的目標應是儘量減少威脅潛伏及停留時間，讓攻擊者擁有最微小的機會達成內部橫向擴散、或是取走您組織內的關鍵資料。

下一個可能的問題是：「如何測量網路威脅潛伏時間？」評估的方法只有一個：回溯並追蹤威脅的源頭。除了追蹤橫向擴散外，也要找出侵入是發生在何時及何處。

2 資料來源：INFOSEC Institute – 成功網路攻擊的七個步驟 (The Seven Steps of a Successful Cyber Attack)—2015 年 7 月 11 日

減少威脅潛伏停留時間的關鍵領域

- 基本的安全控管作業
- 精細的能見度和相關的情報
- 持續的端點監督
- 針對人類行為進行切實可行的預測
- 使用者的察覺能力

五種移轉負擔的實務作法

企業組織開始減少網路威脅潛伏時間時，應考量幾個基本概念。下列五項實務作法，能幫助企業組織透過偵測、遏制和控制網路威脅，減少威脅潛伏的時間。

1. **基本的安全控管作業。**第一步與遏制橫向擴散特別有關，即是確保您已妥善部署基本的安全控管作業。實施基本的安全控管作業，例如：定期的修補程式、嚴格的行政管理、雙因子認證，以及在適當的情況下進行網路分區。在此等情況下，攻擊者被迫投資更多資源，以尋找潛入的途徑。而我們透過強迫他們增加投資，也許就會讓他們知難而退，另行尋找更具吸引力的獵物。

   在執行最佳安全控管實務作業的過程中，核心的步驟應是辨識高價值的目標，也就是對成功企業組織而言，最為重要的就是系統和人員。這些都是敵人最想要利用、並取得財務或智慧財產權利益的目標。我們應加強這些資產的安全監督。這些方法能促使網路安全小組將作業時間優先放在提出警示的訊息上，同時讓您更能輕鬆專注於控管端點、網路裝置或高價值的目標上。

2. **精細的能見度和相關的情報。**如前文所述，無論您已制訂多麼嚴密的基本安全措施，安全入侵都還是會發生。然而，企業可透過精細的網路和企業溝通提高威脅的能見度，以確實抵禦入侵的發生。

   因此，企業應實行類似 Netflow 的網路監督功能，並收集任何裝置的身份使用狀況之日誌記錄。此舉確保企業組織能每日建立與身份竊盜、資料外洩和異常活動相關的危險警示。這些警示無疑的非常重要，但關鍵功能在於：將每台機器或使用者，與其於網路內或離開網路後的行動互為聯結。與所有傳入電子郵件相關的詳細資訊，例如：完整的標題，甚至是內容，都可讓網路安全小組回溯到事件的源頭。

   一旦攻擊者侵入安全控管的外圍和內部，鑑識的能見度就是當務之急。企業組織可依據鑑識資料，增進其回溯威脅源頭的能力，並計算其潛伏停留的時間。威脅潛伏時間是事件回應者的全新評量標準，也恰好是 Forcepoint 用以評量其資安防護的標準。您的小組在偵測、遏制和控管進階威脅上的效率有多高？

3. **持續的端點監督。**持續監督端點後，企業組織能敏銳辨識人員、流程和機器，其幾乎可在即時的速度內，將使用者在端點上的活動演繹為政策，也反過來把政策演繹為活動。這些何以如此的重要？安全小組把事情做對、並認知真實情況後，就能把事件的架構、和看似不相關的活動互為聯結。這意味著更快速的回應時間，以及花更少時間進行傳統的鑑識工作，便能嘗試瞭解到攻擊者的行動和企圖。

   如前所述，攻擊大部份是在主機或員工身上展開，因此，持續監督端點是資安防護的重大演進，也能對加速事件回應發揮關鍵作用。更深入的端點見解，能促進企業組織更快速地偵測到惡意程式以及使用者的異常行為。此外，也可透過搜尋惡意程式及注意怪異的使用者行為，以減少威脅停留時間。減少停留時間和鑑識佐證，讓您掌握安全狀況，保護更多的系統。

「安全小組察覺到真實情況後，就能把事件的架構和看似不相關的活動互為聯結。」

4. **針對人類行為進行切實可行的預測。**根據敵人可能實踐的計劃來預測攻擊狀況，是用更廣泛的事件來回應主題的科學化作業方法。此舉可讓企業組織預期攻擊者為了奪取高價值的目標獵物所可能採取的行動。更具體來說，瞭解攻擊者過去採取的路徑，也就是他/她曾走過的道路之後，資安專家也可開始預測其未來的途徑。

   這何以如此的重要？預測未來行動的關鍵在於，遏制內部橫向擴散和減少威脅停留時間。理想的狀況是：網路安全小組能預期下一步的攻擊，進而把它隔離。這就好像下棋一樣，對手棋盤上還有多少個棋子，走了哪幾步。攻擊者也有許多已規劃的行動，企圖將您一軍。資安專家可決定應採取哪些步驟，例如：把部份資源抽離網路，或通知使用者注意異常行為，確保不會被人將了一軍。

   為達成有效的行動，網路安全小組必須接受這個觀念：外部與內部攻擊者並無不同。他們和 IT 管理員一樣，全盤瞭解組織的內部系統。他們的活動已和網路內的正常行為融合為一。且拜自訂惡意程式所賜，已被利用的使用者能讓攻擊者以內部使用者之姿，在網路內通行無阻。企業組織應假設所有受矚目的員工（在此指的是：因其對外媒體曝光，或行政主管級的知名度、而被公司外部人士所熟知）是侵入企業網路的入門點，以及通往最終目的地的途徑。作為攻擊者，他們可存取特定資源，而這些資源也能進一步存取其他資源。此舉可針對正常和異常的人類行為，進行切實可行的預測，以便建立一個架構，進一步建立區域、降低權限，並促進安全小組有足夠的能力，打擊已潛入企業的攻擊者。

5. **使用者的察覺能力。**企業組織不僅迫切需要去教育員工以熟悉企業政策和政府規範，更要讓他們瞭解到各種會讓企業組織日益曝露於風險下的進階威脅。透過推動正式的教育課程，資安專家更能取得使用者的認同，同時改變風險性行為的可能性也更為增加。此外，安全小組須能教育員工如何面對特定狀況，例如：當使用者成為威脅行動者的目標對象時。

   辨識攻擊後，無論其成功與否，重要的是向目標使用者提供攻擊的資訊，讓他們能認知到未來的攻擊模式。若攻擊得逞，資安專家不應懲罰使用者，而是明白錯誤總會發生。我們還有機會朝著正確方向糾正未來的行動。實際上，使用者將成為人類的「侵入偵測系統」，提供也許會在網路架構內錯失的資訊。市面上不會有一種產品能找到所有惡意程式、或所有不良的使用者行為。因此，若您結合良好技術、流程以及一流的人員，企業打擊進階威脅、減少威脅停留時間和偵測橫向擴散的能力就能加強及擴大。

「若您結合良好技術、流程以及一流的人員，企業打擊進階威脅、減少威脅停留時間和偵測橫向擴散的能力就能加強及擴大。」

結論

攻擊者在企業待的時間越久（潛伏時間越長），其破壞力就越大，竊取的智慧財產就越多。今天的企業不應僅專注於阻擋攻擊者，而是要確保攻擊者留在網路的時間盡可能縮短，也就是持續竭力減少他們的潛伏停留的時間。攻擊者也許會回頭再進行攻擊，但他們會發現付出的代價太高，投資報酬率太低。當攻擊者經歷到重視威脅停留時間的企業後，他們將快速明白即使找到一道敞開的大門，企業也將立即偵測並趕走他們。然後，他們便會轉移目標，尋找保護層級較低的企業。

聯絡人
www.forcepoint.com/contact

[WHITEPAPER_CYBER_DWELL_TIME_ZH-TW] 200017.011416