tenable.ad

國王的贖金：
如何遏阻勒索軟體透過 AD 散播

光是 2019 年，駭客造成的企業損失金額就高達美金 35 億元。儘管這個是由 FBI 的年度網路犯罪報告所公布的數字，但因為資料有限，很難估算出勒索軟體造成的實際損失金額。真正的影響遠比報告指出的數字要高出許多。IT 安全廠商 Emsisoft 所做的一份類似報告指出，贖金的平均金額約為 $84,000 美元。加上考量業務、時間、薪酬和檔案損失，每年對全球商業造成的影響總額至少高達 $1,700 億美元。由於存在許多未通報的網路犯罪，FBI 網路犯罪投訴中心 (IC3) 登記有案的 2,047 起勒索軟體事件不過是最保守的估計值。

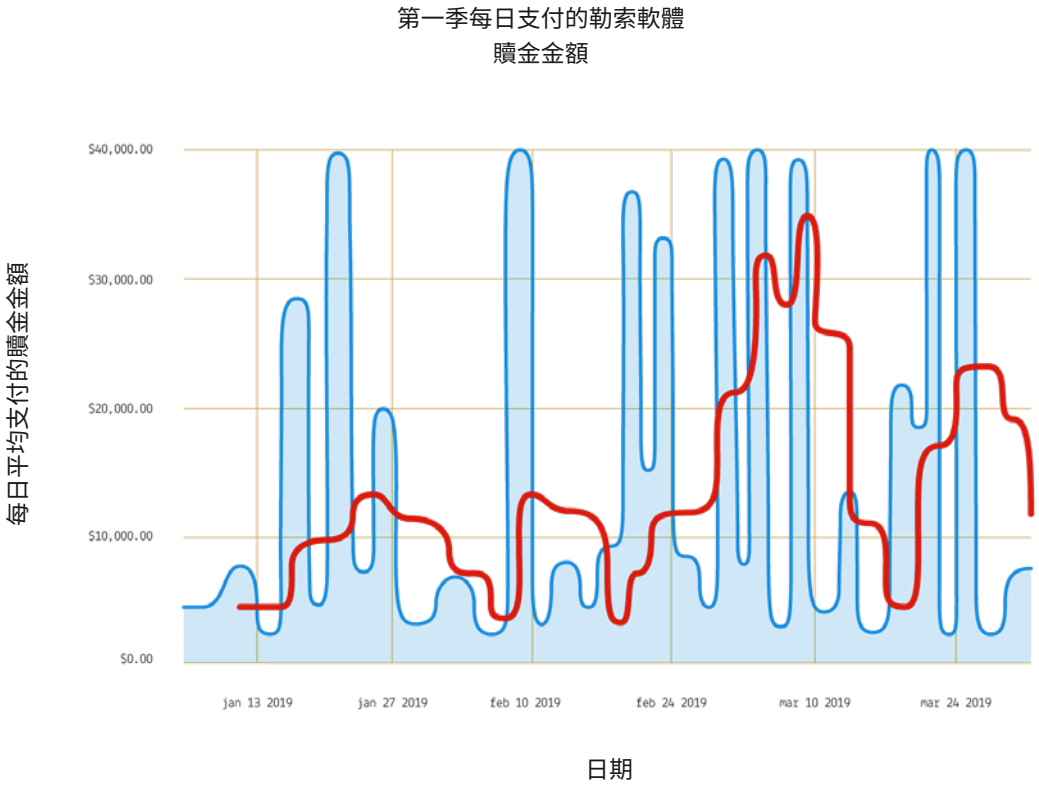
2019 年的勒索軟體發展趨勢

相較於傳統電腦上的惡意軟體，勒索軟體造成的損害更為巨大，因為它不只影響到裝置，還會加密資料。接著，犯罪者便會要求企業支付贖金換取解密金鑰，才能恢復資料存取。但是犯罪者提供的解密金鑰往往不管用。因此 FBI 建議企業不要支付贖金。

駭客的犯罪手法不斷推陳出新，2019 年也不例外。除了加密受感染裝置上的資料，勒索軟體作者亦開始鎖定攻擊裝置本身以外的資源。例如，如果受感染的個人電腦或勒索軟體能夠存取伺服器上的檔案，就有可能會連帶加密這些檔案。勒索軟體可以列舉分析對應磁碟機及網路上可用的共用檔案。

更過分的是，有些駭客甚至會販賣敏感資料。過去曾發生過駭客將資料清除掉後卻仍要求贖金的情況。支付的平均贖金金額比 2018 年的最後一季增加 89%。

美國各地方政府遭受勒索軟體重創，受害的地方包括巴爾的摩、德拉瓦和肯塔基。有些受害者寧可無視 FBI 的建議而選擇支付贖金，也不願意重建系統。這麼做無異於助長罪犯的氣焰，讓他們更加肆無忌憚。



勒索軟體透過 Active Directory 進行散播

過去幾年間開始出現完全不需要散播者的勒索軟體，像是 LockerGoga 和 Samas 即屬此例。惡意軟體大多含有一定的傳播方式，可藉此從最初的受感染裝置散播到相同網路上的其他裝置。與其額外編寫和測試容易失敗的程式碼，駭客更偏好利用企業內的既有機制，也就是 Active Directory。

Windows Server Active Directory (AD) 是 Microsoft 開發的內部部署身分管理產品。AD 讓企業得以集中管理使用者的登入憑證、設置伺服器與工作站上的設定，以及管理企業的其他安全面向，例如公開金鑰基礎架構 (PKI) 和角色型存取控制 (RBAC)。

如果駭客取得 AD 的存取權限，便能易如反掌地控制企業的整個 IT 基礎架構。內部部署和雲端解決方案都容易遭受攻擊。AD 中包含所有使用者、端點、應用程式和伺服器的資訊。標準管理工具可以在不被安全軟體偵測到的情況下查詢目錄。接著駭客就能利用 AD，將勒索軟體傳播到企業中的每部裝置上。

即使企業的 IT 人員已針對網域控制器 (亦即執行 AD 目錄服務的伺服器) 額外進行安全部署，但如果沒有確實遵守安全防護的最佳做法，還是可以透過加入 AD 的終端使用者裝置輕易入侵 AD。

近來勒索軟體攻擊的實例

近幾年來備受矚目的攻擊事件都是利用 Active Directory 作為散播媒介。但 AD 也被用於發動非目標式攻擊。登上新聞頭條的大多為跨國企業和政府機構，然而規模較小的企業和組織同樣也淪為勒索軟體的受害者。

尤其當 IT 服務供應商受到攻擊時，醫療保健、政府、教育及其他產業都會連帶受到波及。勒索軟體攻擊可能會帶來毀滅性的後果。企業的整個網路遭到加密，包括備份資料和 Active Directory 網域控制器。即便有「完好」的備份資料可用來還原系統，還是必須為此投入大量的時間和成本。

下面我們舉幾個實例說明駭客是如何透過操縱 AD 來散播勒索軟體：

Norsk Hydro

挪威的鋁公司 Norsk Hydro 於 2019 年 3 月遭到 LockerGoga 攻擊。感染的起源地是位於美國的一間工廠，而後向外散播到其他廠區。這場勒索軟體疫情的爆發迫使 Norsk Hydro 將旗下的多家工廠轉換成手動作業流程。

Norsk Hydro 選擇設法修復系統而非支付贖金，正因為企業備有周詳的災難復原計畫才得以繼續營運，計畫中包含將內部部署的電子郵件系統自動切換為 Microsoft 的 Office 365 雲端服務。但是對基於管制或合規性理由而必須將資料保存在自身資料中心的公司而言，它們無法將雲端服務納入災難復原計畫的選項之一。

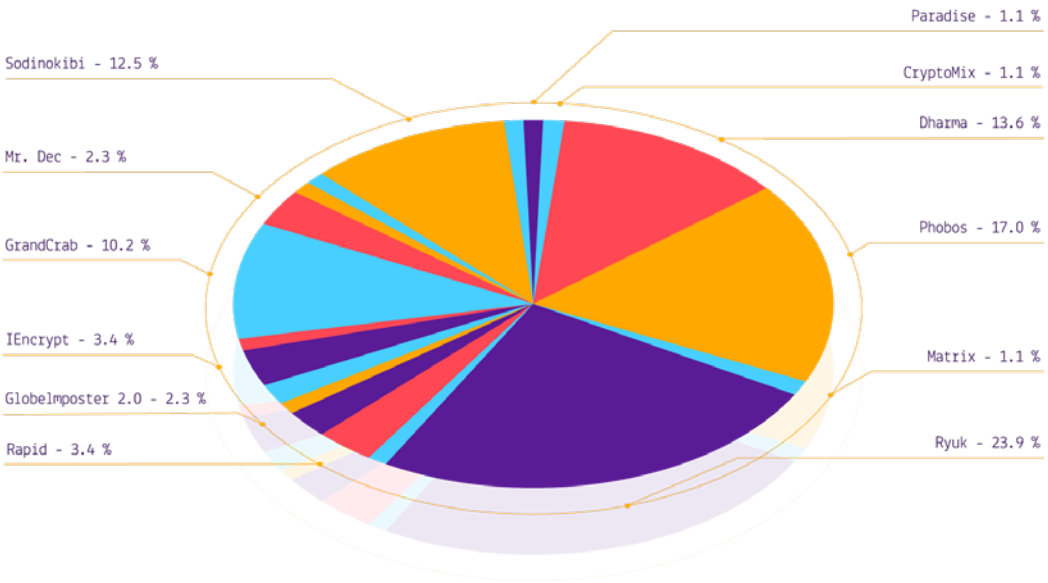
石油和天然氣設施

在 2019 年下半年，還發生了利用 Active Directory 來散播 Ryuk 勒索軟體的攻擊事件。美國的操作技術網路安全服務公司 ThreatGen 通報其數個石油和天然氣產業的企業用戶端遭到 Ryuk 攻擊。

駭客利用 Microsoft 遠端桌面通訊協定 (RDP) 中的一個弱點，成功入侵 Active Directory 並取得特權憑證。Ryuk 勒索軟體隨後會注入登入指令碼中，導致登入 AD 的所有用戶端受到感染。使用者和 IT 員工登入他們的個人電腦或伺服器後，這些裝置即會遭到鎖定和加密。

初步入侵 Active Directory 之後，勒索軟體會先靜靜潛伏數個月，其後才會注入登入指令碼中。潛伏這麼長的時間讓勒索軟體可以好整以暇地收集資訊，深入了解受感染企業的系統和資料，或是增加使用備份還原的難度。一家受影響的公司試圖還原其系統，卻發現備份資料也同樣受到勒索軟體的感染。

各類型勒索軟體的市佔率：
2019 年第 2 季



Kmart

在 2020 年 12 月，美國連鎖百貨 Kmart 成為兇猛的 Egregor 勒索軟體的受害者，此勒索軟體還發出了一封「勒索信」，證實 Kmart 的 Active Directory 網域已在攻擊時淪陷。此勒索軟體以採用「雙重敲詐」手法著稱，亦即公開部份的竊取資料內容，藉此迫使被害人儘速支付贖金。一般而言，此勒索軟體是透過載入程式注入。首次成功入侵之後，勒索軟體即會停用防火牆設定並啟動遠端桌面通訊協定 (RDP)。之後，該惡意軟體會開始在網路中四處橫向移動，以偵測和停用防毒軟體。直到停用最後一道防線後，勒索軟體即會存取並加密入侵的資料。

聯合國

在 2020 年 3 月，聯合國對外表示有三處聯合國辦事處的數台伺服器遭到駭客入侵。其中部分伺服器用於管理使用者/密碼，以及作為防火牆、資料庫和系統管控之用。聯合國發言人證實攻擊者已成功擷取其內部使用者的 Active Directory 清單。攻擊者利用 SharePoint 伺服器上的弱點 (CVE-2019-0604) 來存取網路並在其中橫向移動。這次的駭客入侵殃及將近 4000 名聯合國工作人員，並有各種個人資訊遭到外洩。

SaveTheQueen 勒索軟體

全新的勒索病毒株 SaveTheQueen 於 2020 年初開始肆虐，此勒索軟體首見於 2019 年，它會加密檔案並加上 .SaveTheQueen 副檔名。這株新病毒把自己注入 Active Directory 的 SYSVOL 共用資料夾，而後將資料夾複製到每部網域控制器以進行傳播。所有經驗證的使用者都可以讀取 SYSVOL，但唯獨有權存取 AD 的使用者才能寫入該資料夾。

資安公司 Varonis 表示，新的勒索病毒株 SaveTheQueen 會利用 AD 的 SYSVOL 共用資料夾寫入記錄檔，藉以追蹤對新裝置的攻擊進度。SYSVOL 中會儲存一個排程任務的程式碼，在裝置上執行 PowerShell 指令碼，造成該裝置感染勒索軟體。

Samas 勒索軟體

Samas 勒索軟體早從 2016 年開始便利用 Active Directory 進行散播。它首先使用免費工具來竊取 Active Directory 的特權憑證。接下來，攻擊者會搭配標準管理工具來查詢 AD，找出想要加密的裝置。但是 Samas 加密檔案時，AD 僅止於用來偵查，惡意程式碼的傳播方式則與傳統「蠕蟲」相仿。

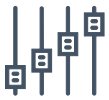
如何避免勒索軟體透過 Active Directory 進行散播

發動攻擊的勒索軟體必須具備存取 Active Directory 的特權，才能使用目錄來傳播病毒或執行偵查。多數企業並未妥善限制或管理特權 AD 帳戶的使用，使得 IT 系統暴露在勒索軟體或其他攻擊的威脅之下。

以下六種方法可協助您保護特權 AD 帳戶的存取安全，提高攻擊者將 Active Directory 武器化的難度：

1 限縮特權 AD 群組的成員資格

2 限制特權 AD 帳戶的使用



3 使用本機帳戶來管理終端使用者裝置

4 使用多重因素驗證來保護特權 AD 帳戶的安全

5 監控 Active Directory 是否有不尋常的活動

6 建置 Active Directory 專用的分層管理模式

1. **限縮特權 AD 群組的成員資格**
   Microsoft 建議減少在 Active Directory 網域中使用特權帳戶，以維持最低限度的使用為宜。限制 Domain Admins (網域管理員) 和企業管理員 (Enterprise Admins) 群組的成員資格固然重要，但 AD 的特權帳戶不只有這兩種。舉例來說，Schema Admins (結構描述管理員) 即為另一個特權群組。
   提示：您可以先從稽核特權 AD 群組的成員資格，並設法限縮其成員資格開始做起。

2. **限制使用特權 AD 帳戶**
   Windows 有提供若干技術可協助降低特權 AD 憑證暴露的可能性，例如 Protected Users (受保護使用者) 群組與 Windows Defender Credential Guard。但是您必須遵守 Microsoft 的最佳做法建議，對於特別加強保護的 Active Directory 專用管理裝置，應限制其特權 AD 帳戶的使用。
   提示：建立數個特權存取工作站 (PAW)，專門用來執行必須對 Active Directory 進行特權存取的管理工作。

3. **使用本機帳戶來管理終端使用者裝置**
   Microsoft 最近修改了用本機管理員帳戶對用戶端裝置進行遠端存取的建議。企業通常會授權使用網域使用者帳戶對用戶端進行遠端存取。如果您設置一個系統來隨機產生和變更每部裝置上的本機管理員密碼，像是使用 Microsoft 的本機管理員密碼解決方案 (LAPS) 工具，那麼就能避免使用網域帳戶支援遠端存取。使用本機帳戶來支援存取終端使用者裝置，有助於防止駭客輕易入侵 Active Directory。
   提示：稽核本機管理員帳戶的密碼。確保每部裝置都具有其專屬的唯一本機管理員帳戶密碼。然後停止使用網域帳戶進行遠端支援。

4. **使用多重因素驗證來保護特權 AD 帳戶的安全**
   密碼不夠安全，因為駭客可以輕易濫用竊取的密碼。但很多企業卻單靠密碼來保護特權 AD 帳戶。Microsoft 表示，多重因素驗證已證實可以阻止 99.9% 的自動化攻擊。多重因素驗證 (MFA) 會要求使用者提供密碼以外的認證，例如生物辨識手勢，或是由驗證器應用程式產生的一次性密碼。
   提示：在 Windows Server Active Directory 中增設多重因素驗證。您可以使用 Azure MFA 及其他產品在 AD 中增設 MFA。

5. 監控 Active Directory 是否有不尋常的活動

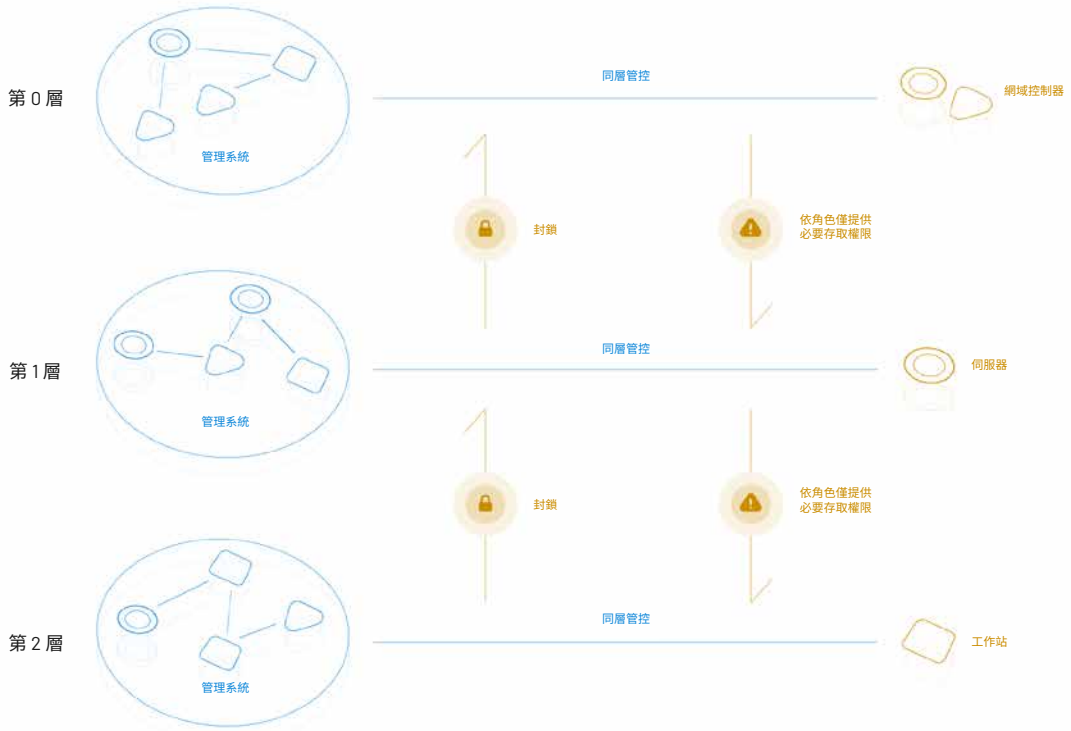
如同使用惡意程式掃毒軟體掃描 Windows 中的異常檔案和程序，監控 Active Directory 是否有不尋常活動也同樣重要。Windows 事件記錄包含很多資訊，其可能揭露特權帳戶遭到誤用或其他惡意行為。只要握有正確的資料，企業便可主動遏止勒索軟體攻擊透過 AD 散播。您可以使用安全資訊和事件管理 (SIEM) 產品，收集從 Windows Server 事件記錄及其他系統轉發的資訊。最新的威脅情報可以協助企業，透過從資安事件收集的資料來自動辨識威脅。不過，單靠 Windows 記錄或 SIEM 產品其中之一，並無法提供足夠的安全防護。

提示：部署 SIEM 並搭配威脅情報，主動阻擋勒索軟體及其他類型的惡意軟體入侵，早一步防止它們感染您的整個網路。

6. 建置 Active Directory 專用的分層管理模式

Microsoft 建議將 Active Directory 中的資源進行組織歸納，採用更加安全的分層模式來管理這些資源。此模式共分為三個層級定義，這些層級相當於緩衝區的作用，旨在將終端使用者的個人電腦等高風險裝置，與網域控制器之類的貴重伺服器分開來管理。第 0 層 (Tier 0) 包含特權 AD 帳戶、網域控制器及特權存取工作站等資源。第 1 層 (Tier 1) 專供成員服務和應用程式使用。而第 2 層 (Tier 2) 則是專供終端使用者的個人電腦，以及 AD 中用來管理個人電腦的物件 (如服務台的使用者帳號) 使用。

提示：採用階段式方法重新組織 Active Directory，以利使用分層管理模式進行管理。



Tenable.ad：主動遏止勒索軟體感染整個網路

要保障 Active Directory 的安全並阻止駭客利用它來散播惡意軟體，遵守 Microsoft 的安全最佳做法是一個不錯的起點。但是，Windows Server 提供的立即可用工具無法即時監控 Active Directory，亦無法提供必要的威脅情報，讓企業自動應對瞬息萬變的威脅態勢。

Tenable.ad 可以在攻擊者利用這些漏洞來散播勒索軟體之前，找出 AD 的安全問題。內建知識與威脅情報，協助企業緩解問題並修復威脅。Tenable.ad 能夠與 SIEM 和安全工具整合，主動改善 AD 安全、提供動態儀表板，並為您呈現唯有專家級安全軟體才能提供的洞見。

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

北美地區 +1 (410) 872-0555

zh-tw.tenable.com