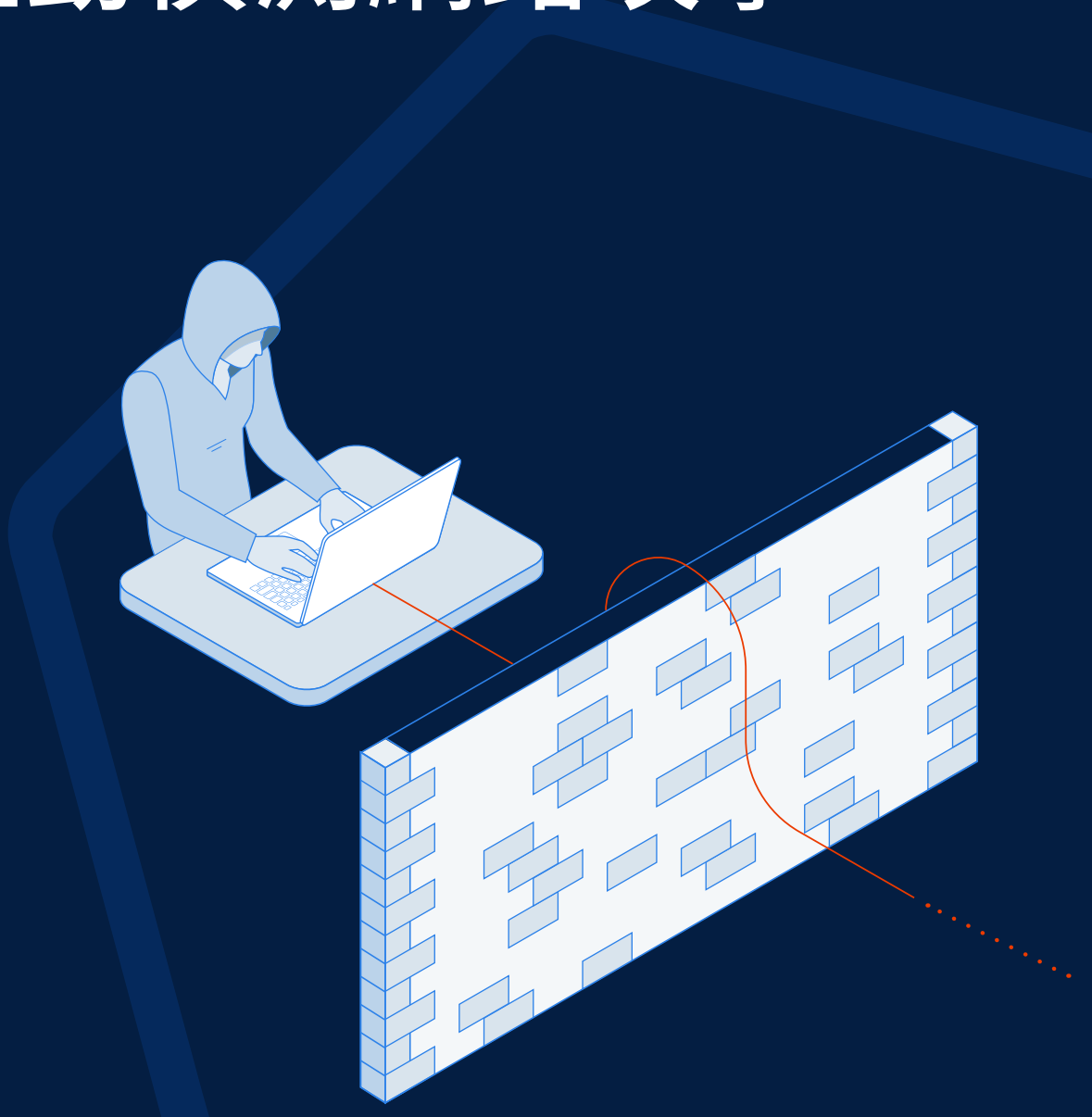
tenable.ad

保障 ACTIVE DIRECTORY 的安全：

如何主動偵測網路攻擊



Active Directory 在過去 21 年中一直是組織的主要身分和存取管理解決方案。它的地位未曾受到撼動，而來自 Microsoft 的技術也未曾變動。這個過時的 IAM 解決方案已經廣為人知，系統管理員和網路攻擊者都深諳其道。

企業必須採取不同的方式保護其 AD 基礎架構，以及網路上所有透過 AD 控制和保護存取權限的資源。網路攻擊者已經開始採取一種高度精密的方式，從外部和內部位置攻擊 AD。攻擊得逞的次數日益增加以及 AD 攻擊路徑的持續存在，證明了傳統的安全管控工具和方式不再具有顯著效果。沒有單一解決方案能夠解決 AD 的安全問題，只有具備正確的工具和方法，才能強化安全和減少攻擊。

AD 紀錄和曝險

Active Directory 在過去二十年間並未大幅變動的說法其實過於含蓄。雖然 Active Directory 已問世 21 周年，部分內容仍維持不變，尤其是基礎架構中所包含的物件和屬性。

這一切事實代表甚麼？首先，由於到目前為止都沒有太大變動，未來發生變動的可能性也很小，不太需要進行 Active Directory 教育訓練。再者也是最重要的，網路攻擊者已經有能力找出隱藏的後門程式，並發展出精密的攻擊方式以取得網域支配權。

兩者相互作用。假若網路攻擊者不斷找出後門程式，企業卻無力持續掌控 Active Directory，則攻擊將繼續向上攀升，而保護 AD 的效能也將持續滑落。

- 環境的基礎是網域和樹系
- 使用者、群組和電腦是核心物件
- 為管理物件，每個網域都細分成組織單位 (OU)
- 優先採用「群組原則」管控使用者和電腦
- DNS 和 DHCP 這類必要的服務則維持不變
- Kerberos 和 NTLMv2 仍然是慣用的驗證通訊協定
- 密碼原則管控措施維持不變且停滯不前

AD 安全解決方案

這些年來，Microsoft 已經發展出好幾種適用於內部部署 AD 的安全解決方案，但這些方案經常曇花一現，或者最終失去支援，或者由其他解決方案取代。其中一項仍堅守在 AD 安全前線的技術是「群組原則」。這些年來，「群組原則」的確也加入了一些強化功能，納入許多 ADM/ADMX 自訂功能、群組原則喜好設定以及進階稽核原則。然而，「群組原則」的核心架構仍維持不變。

這些年引進的其他安全解決方案包括：

- 稽核與進階稽核
- 資訊安全設定精靈 (SCW)
- Security Compliance Manager (SCM)
- Desired State Configuration (DCM)
- 本機系統管理員密碼解決方案 (LAPS)
- 受保護的使用者群組

以上這些解決方案的每一項所面臨的總體問題是無力真正保障大部分的環境。這些解決方案都僅能影響部分電腦、部分安全設定以及部分網路攻擊。即便某個解決方案具備優勢，但卻經常因未能在市場上廣為行銷，並未受到所有 AD 安裝者的採用。

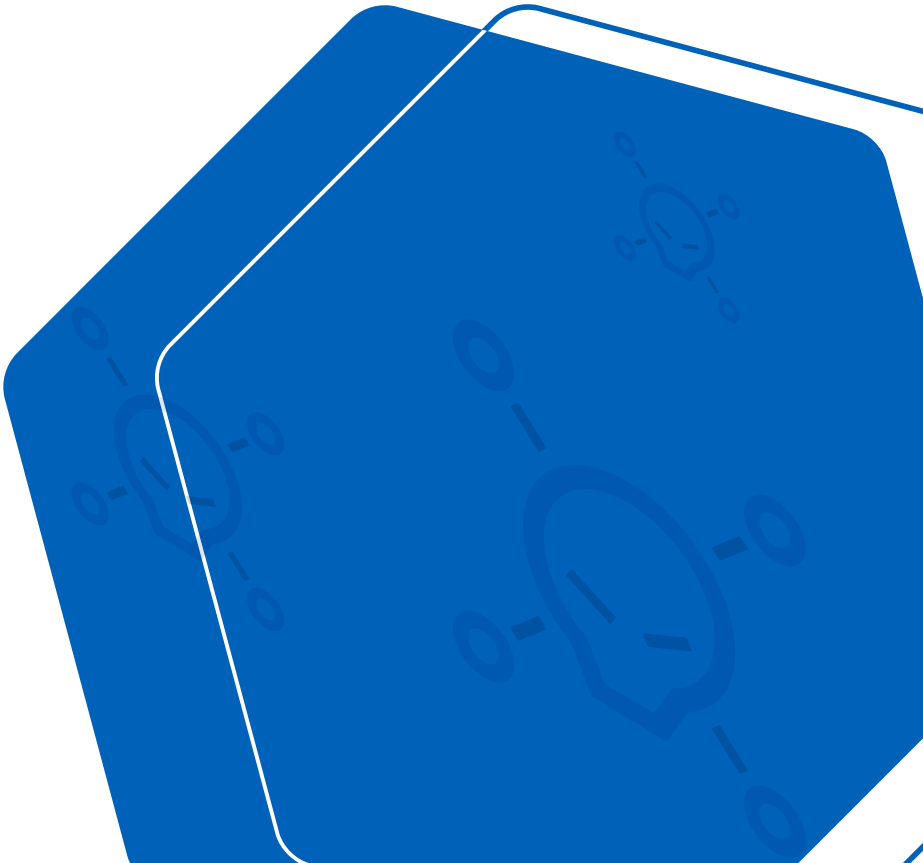
新的攻擊方式複雜而隱匿

現有基礎架構持續不變，安全解決方案也不穩定，讓網路駭客可趁機大肆入侵。對 Active Directory 發動的攻擊大幅上升，攻擊的深度也提高了。多年來網路攻擊者都希望能夠在不產生任何追蹤或事件的情況下，對環境發動攻擊。這正是許多新型態攻擊方式有能力辦到的。

這個產業似乎將此歸咎於 Microsoft 本身，因為 Active Directory 的基礎從一開始就不安全。缺乏任何增強功能的情況下，這些核心安全漏洞與缺口一直存在。

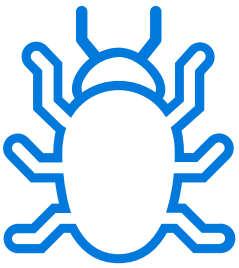
無論如何，這些新型態攻擊都讓傳統的監控解決方案在偵測攻擊或是與攻擊相關的資訊方面變得毫無效用。現今的攻擊方式會利用 AD 和 Microsoft 的基礎概念，迴避這些 AD 監控解決方案多年來就已經能夠查看的任何事件紀錄或變更追蹤。這些攻擊者會運用橫向移動和權限提升，僅需幾小時或幾天的時間，就能達到支配網域的階段。以下是幾種目前讓 AD 深受其害的新型攻擊/概念：

- DCSync
- DCShadow
- 密碼噴濺
- 雜湊傳遞
- 工單傳遞
- Golden ticket
- 服務主體名稱
- AdminCount 和 adminSDHolder



偵測難度大

由於這些攻擊都是在 Microsoft、Windows 和 AD 執行所需的現有技術背後進行破壞，因此幾乎難以偵測出來。攻擊者已經採取了許多不同的方式來略過監控系統和活動紀錄。但是，並非所有的攻擊都遵循相同的方式。



慢速攻擊

某些攻擊的速度很緩慢，這表示此活動會看起來會像是網路上的正常活動。同時，這些活動可在短時間內提供資訊，讓攻擊者獲得深入見解。這些攻擊大部分會追蹤使用者帳戶的密碼，因此不需要特權。僅需對網路的存取權限，以嘗試登入。

這類攻擊的其中一種就是密碼噴濺攻擊。任何環境中的使用者經常都會使用常見密碼。因此如果能取得完整的使用者帳戶清單 (任何人都能從 Active Directory 取得)，就能逐一對每個使用者名稱使用一些常見密碼進行測試。關鍵在於嘗試的密碼次數少於帳戶鎖定原則限制，而網域中的任何使用者都能知道此限制。

使用核心技術和組態的攻擊

仔細想想 Microsoft Active Directory 是在 2000 年時開發出來的。Yahoo 當時還是科技新貴，而 Bill Clinton 還是美國總統。Microsoft 為了確保通訊順暢所內建的技術時至今日仍在使用。過去多年來，這些技術被用來保護 AD 環境，因為我們輕易就能發現與特定特殊權限帳戶相關的資訊。部分用於保護 AD 環境的常見內建技術包括：

- 服務主體名稱
- Admincount 和 adminSDHolder SIDHistory
- 使用者主要群組 ID

這些 AD 環境的基本元素旨在確保安全性和一致性，但如今攻擊者卻會加以利用來建立後門程式，並在不被察覺的情況下取得持續性存取權限。舉例來說，adminCount 和 adminSDHolder 攻擊的概念就相當簡單，假若不持續注意細節，就幾乎不可能阻擋。總而言之，攻擊者會竄改 adminSDHolder 物件中的 ACL，加入他們可以掌控的帳戶，並給予該帳戶「修改」或「完全」控制權。當背景處理程序啟動，將 ACL 放在所有 adminCount 屬性等於 1 的物件上時，攻擊者就能獲得特權物件的權限。

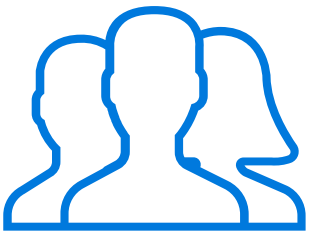
略過登入的攻擊方式

新型態的攻擊方式極為複雜而巧妙。這些攻擊方式確實需要 Active Directory 中的特權，但由於有其他許多攻擊方式可讓攻擊者取得特權，在特權授予後再使用這些攻擊方式即可。特權攻擊的目的是希望在無人察覺的情況下取得持續存取權限。有兩種攻擊方式屬於這種類別，包括：

- **DCSync**
- **DCShadow**

DCSync 的整體目的是取得密碼帳戶的資料，使得離線攻擊可以變成經由攻擊取得的密碼雜湊。DCShadow 攻擊有點不同，因為這種攻擊會建立一個偽造的網域控制器，用於將攻擊插入複寫資料流中，在不留痕跡的情況下改變物件和屬性。

這兩種攻擊方式都不會留下紀錄。這種情況可能發生的原因是兩者都會仿造新的網域控制器，而偽造的網域控制器絕不會留下紀錄！若對象是仰賴安全事件紀錄來查看活動的企業，這是一種理想的攻擊方式。AD 監控、SIEM 解決方案和甚至大部分使用代理程式的解決方案都將無法辨識這些攻擊方式。

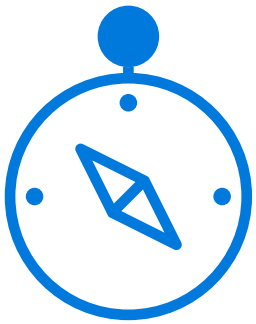


模擬其他使用者的攻擊方式

已經存在一段時間但持續醞釀新選項的攻擊方式包括：

- 雜湊傳遞
- 工單傳遞
- Silver Ticket
- Golden Ticket

這些攻擊都會以某種方式使用遭竊的憑證，以模擬該使用者。當然，遭竊的憑證來自於有特權的使用者，因此可在網域中使用最高等級的特權。雜湊傳遞和工單傳遞會使用原始的雜湊資訊來模擬其他使用者，而 Silver 和 Golden Ticket 則會接管 Kerberos 驗證流程的一部分，以獲得對企業中的服務和所有帳戶的存取權限。



主動偵測各式各樣的攻擊方式

仔細想想，大部分的 AD 環境都是多年前建立的。在安裝 Active Directory 當時，今日的安全問題甚至還不是一種問題。對於可能會讓其基本架構遭攻擊的現存安全問題，每一家使用 Active Directory 的企業都必須能及時獲得相關資訊。不幸的是，AD 監控和 SIEM 解決方案並不提供這種服務或功能。

適用於 AD 的 Tenable.ad 卻可以做到。當安裝適用於 AD 的 Tenable.ad 時，系統會提供一個必須即刻解決的現有問題和設定錯誤的清單。

每一家企業不僅必須清理目前的 AD 安全態勢問題，還必須持續監控，以確保設定錯誤和攻擊不會發生。有許多企業認為，只要有要求安全強化，設定將不會改變。事實上，在任何一個 Active Directory 生產環境中都並非如此。設定會一直隨著錯誤、安裝、更新和攻擊而改變。

因此，假如有任何設定錯誤或是攻擊開始發生，掌握時機是偵測和警告企業的關鍵要素。有些攻擊方式很緩慢，但有些可能只需要幾分鐘的時間。愈快確認攻擊方式，攻擊無法得逞的機率就愈高。

AD 監控和 SIEM 解決方案仰賴安全紀錄，以掌握在 Active Directory 內和周圍正在進行的動作訊息。Tenable.ad 不需要等候活動紀錄。反之，Tenable.ad 會利用原始的 AD 複製資料流獲取資訊，甚至在行動執行前就能取得資訊。在分秒必爭的情況下，這就可能決定攻擊的成敗。(當然，Tenable.ad 可以將所發現的資訊傳送到 SIEM，這是 SIEM 成為任何企業整體安全重要元件的原因。)

總結

由於 Active Directory 廣為人知，技術卻又停滯不前，網路攻擊者能夠在其基本架構中找出全新且具創意的後門程式。這些後門程式極為巧妙，僅需少許或不需特權，便能取得資訊，也使得攻擊者可以在不被察覺的情況下進入網路。部分攻擊需要特權，但這類攻擊可略過安全紀錄，也因此可規避 AD 監控和 SIEM 解決方案。若要偵測出目前所有使用中的攻擊方式，Tenable.ad 這類的主動方式才是最佳解決方案。Tenable.ad 可提供有關設定錯誤的即刻資訊，以及任何新型態設定錯誤或攻擊方式的即時偵測結果。全都不需要使用代理程式或特權。

若想在您的環境中安裝使用 Tenable.ad，請聯絡我們。

tenable.ad™

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

北美地區 +1 (410) 872-0555

zh-tw.tenable.com