

白皮書

導致全網域 淪陷的十大 Active Directory 設定錯誤

導致全網域淪陷的 十大 Active Directory 設定錯誤

目錄

簡介：Active Directory 安全風險

AD 攻擊剖析

AD 錯誤設定為攻擊者開啟大門

後續步驟：保護貴組織免受 AD 威脅

簡介：Active Directory 安全風險

為什麼 Microsoft Active Directory(AD) 會成為商業世界中最常遭鎖定的目標資產？因為攻擊者只需從一台遭入侵的端點對AD發出少數幾次查詢，就能取得竊取網域系統管理員憑證、並橫向移動至高價值資產所需的一切資訊。換句話說：攻擊者只要入侵單一連接網域的端點，就能掌控組織的重要資產。AD資料庫會將企業網路上的所有身分與資源，暴露給任何已連接網域的使用者，而AD更授權使用者(無論是合法使用者或心懷不軌者)使用其內建查詢功能來尋找機敏資訊。

不幸的是，AD也可能是貴公司防護最薄弱的資產。全球十家企業中就有九家使用AD來控管並維護內部資源，但大多數企業的防禦重點都放在端點、應用程式、伺服器、行動裝置與網路上，導致AD長期暴露在毫無防護的高風險狀態下。

您無法停用 AD 查詢功能，也無法偵測出是哪些使用者發出查詢。

這種能夠隱密存取網路資源的能力，說明了為何許多攻擊者偏好進行AD偵察，而非執行網路掃描；也說明了為何攻擊者熱衷於利用AD預設的查詢功能。請參閱下表，其中列出 MITRE 記錄在案的相關攻擊活動。

AD Is a Basic Building Block of APTs^a

駭客組織名稱	別 名	憑證竊取	AD 列舉	時間範圍	來 源
APT 3	Boyusec, UPS	是	是	持續進行中	中國
APT 10	Stone Panda	是	是	持續進行中	中國
APT 28	Sofacy, Fancy Bear	是	是	持續進行中	俄羅斯
APT 29	Cozy Duke, Cozy Bear	是	是	持續進行中	俄羅斯
APT 32	OceanLotus	是	是	持續進行中	越南
APT 33	Charming Kitten	是	是	持續進行中	伊朗
APT 34	Twisted Kitten	是	是	持續進行中	伊朗
APT 35	Newscaster Team	—	—	持續進行中	伊朗
Turla	Snake, Uroburos	是	是	最後偵測於 2017 年	俄羅斯
Shell_Crew	Deep Panda	是	是	最後偵測於 2017 年	中國是
Dark Seoul	Lazarus Group, Hidden Cobra	是	是	持續進行中	北韓

a. <https://attack.mitre.org/groups/G0022>

AD 攻擊剖析

一旦在連接網域的端點上取得立足點，攻擊者便會針對貴組織的資源展開AD偵察。他們會從遭入侵的端點產生並送出對 AD 的查詢，藉此找出定位並存取機敏資料所需的資訊。攻擊者可輕易得知貴組織所有員工的相關資訊(包括身分、角色與權限)，以及執行於資料庫、伺服器、儲存裝置與內部安全元件上的應用程式。接著，他們會竊取網域憑證，並以此為跳板向外橫向擴散。

攻擊者一旦入侵某個端點，僅需短短七分鐘即可完全掌控整個網域（形成全面性的網路入侵）。他們隱身於合法授權使用者之中，偽裝成一般使用者。

連接網域的端點比其他裝置具有更高的安全風險，因為僅僅一台遭入侵的裝置，就足以危及整個組織的安全。貴組織必須針對遭入侵的端點強化 AD 防護，才能有效阻止攻擊者的後續行動。

攻擊者以端點為起點



AD 錯誤設定為攻擊者開啟大門

隨著貴組織的 AD 部署環境經年演變，IT 團隊可能無法妥善維護其設定值，或及時導入安全強化措施。攻擊者則在暗處伺機而動；只要網域與 AD 服務出現弱點，便會立即伺機入侵。他們同時會植入後門與持續駐留機制，以便日後隨時重返。

Symantec 認為，以下十項 AD 錯誤設定所帶來的風險最為嚴重。

1. 群組原則喜好設定密碼外洩

攻擊說明：系統管理員會使用群組原則喜好設定（GPP）來設定本機系統管理員帳戶、排程工作，並在使用者登入時，以指定的憑證掛載網路磁碟機。這些 GPP 設定會寫入網域控制站的 SYSVOL 共用資料夾中。攻擊者可存取 SYSVOL 共用資料夾內的 GPP XML 檔案，並從中擷取 GPP 內儲存的指定憑證。

潛在威脅：攻擊者可取得與所擷取帳戶相同的權限。而設有 GPP 的帳戶，通常對每台端點都具備本機系統管理員使用者權限。

2. 隱藏式安全識別碼（SID）

攻擊說明：攻擊者利用安全識別碼歷程（SID History）物件，繼承其他高權限 SID 帳戶或群組的權限，且使用者不會留下任何新增群組成員資格的痕跡。

潛在威脅：使用 SID 屬性，代表攻擊者正試圖將高權限群組成員資格（例如網域系統管理員）隱藏於低權限帳戶中，藉此掩蓋入侵後留下的網域後門。

3. 黃金票證（Golden Ticket）

攻擊說明：攻擊者一旦取得 krbtgt 帳戶的長期金鑰，即可偽造具有任意使用者權限的登入票證（TGT）。該票證中會包含一個虛構的使用者名稱，並賦予其網域系統管理員成員資格（或攻擊者所選擇的任何其他成員資格）。

潛在威脅：攻擊者可取得網路上任何服務或端點的存取權限，且能在任何地方使用。在系統管理員重設 krbtgt 帳戶之前，這些權限將持續有效。

4. 網域複寫後門

攻擊說明：若將低權限使用者加入網域複寫物件，攻擊者即可在不具備高權限身分的情況下，存取網域中的所有機敏資料（例如網域中的使用者雜湊值）。由於部分網域服務需要具備網域複寫能力，因此複寫權限必須指派給 AD 物件。

潛在威脅：攻擊者可取得對整個公司網域資料庫的完整存取權限。

5. 無權限管理員持有者存取控制清單（ACL）

攻擊說明：攻擊者會利用 AdminSDHolder 的 ACL，例如將無權限使用者加入 AdminSDHolder 安全物件，並賦予完全控制或寫入權限。如此一來，該無權限使用者即可在不具備高權限的情況下，將自己或其他使用者加入具有強大權限的群組（例如網域系統管理員群組）。

潛在威脅：啟用並修改此功能的攻擊者，可在不使用任何網域帳戶的情況下，於網域控制站上留下隱藏的系統管理員權限。

6. 高權限使用者列舉

攻擊說明：已通過驗證的使用者可列舉網域中的任何物件。透過列舉密碼永不過期的使用者，即可揪出網域中的高權限使用者。

潛在威脅：攻擊者一旦取得這些憑證，即可在網路中取得長期有效、無限期持續的高權限存取權。

7. 白銀票證 (Silver Ticket)

攻擊說明：使用者可針對網域中的任何服務，請求以該服務帳戶長期金鑰加密的服務票證。攻擊者會蒐集這些服務票證，並嘗試在本機端對長期金鑰進行暴力破解攻擊。

潛在威脅：攻擊者可取得對執行該服務帳戶之端點的完整權限存取。

8. 允許匿名 LDAP 存取

攻擊說明：未受管理的端點可對 AD 發出查詢，並在未經身分驗證的情況下，蒐集網域環境的相關資訊。

潛在威脅：攻擊者只需一台已連上網路、且未經驗證的使用者與電腦，即可檢視整個目錄結構與權限設定。

9. 啟用 DSRM 登入

攻擊說明：攻擊者會啟用並修改 DSRM (目錄服務修復模式，一種用於在目錄服務故障時修復或還原 AD 的特殊開機模式)，藉此在網域控制站上留下隱藏的系統管理員權限後門，且完全不需使用任何網域帳戶。

潛在威脅：攻擊者可取得對貴組織網域控制站的完整控制權與存取權。

10. 本機系統管理員橫向遊走

攻擊說明：攻擊者會從網路中的某台本機電腦竊取本機系統管理員憑證。由於許多企業使用映像軟體部署系統，本機系統管理員密碼往往在整個企業中都相同。攻擊者便可利用該本機系統管理員的長期金鑰，對遠端端點進行身分驗證。

潛在威脅：攻擊者一旦在單一機器上取得本機系統管理員憑證，即可橫向移動，進而取得對網路中每一台端點的存取權限。

後續步驟：保護貴組織免受 AD 威脅

免費安全評估

Symantec 提供由軟體驅動的免費 AD 威脅評估服務，可自動掃描並偵測 AD 與整體網域環境中的錯誤設定，評估結果並附有最佳實務修復建議。

持續性評估

AD是關鍵的攻擊面，需要持續監控其中的錯誤設定、弱點以及攻擊者的持續駐留行為。Symantec® Endpoint Threat Defense for AD 內建威脅評估服務，可針對網域與 AD 架構的每一項元件提供持續性分析。Endpoint Threat Defense for AD 會偵測錯誤設定與攻擊者留下的後門，一旦發現異常，便會透過中央主控台發出警示，並提供具體的修復建議。

如需進一步瞭解 Symantec Endpoint Threat Defense for AD，

請造訪：www.broadcom.com/info/endpoint-security/threat-defense-for-active-directory

如需更多資訊，請造訪我們的網站：<https://www.savetime.com.tw/>



關於賽門鐵克

賽門鐵克(Symantec)已於2019/11併入全球網通晶片巨擘—博通(Broadcom)，美國股市代號AVGO，全世界網路流量有99.9%經過博通的網通晶片軟體事業部的企業安全部門(SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態整合擴充性，有著脫胎換骨並超越業界的長足進步。博通(Broadcom)是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec持續創新的技術能為日新月異的資安問題提供更好的解決方案。近三年Symantec很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉康創辦的企業軟體公司，組合國際電腦(CA Technologies)以及雲端運算及「硬體虛擬化」的領導廠商—VMware，也是博通軟體事業部的成員)。2021年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署(CISA)宣布聯合民間科技公司，發展全國性聯合防禦計畫JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資安安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業IT專業人員的知識傳承(Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的求助諮詢對象。