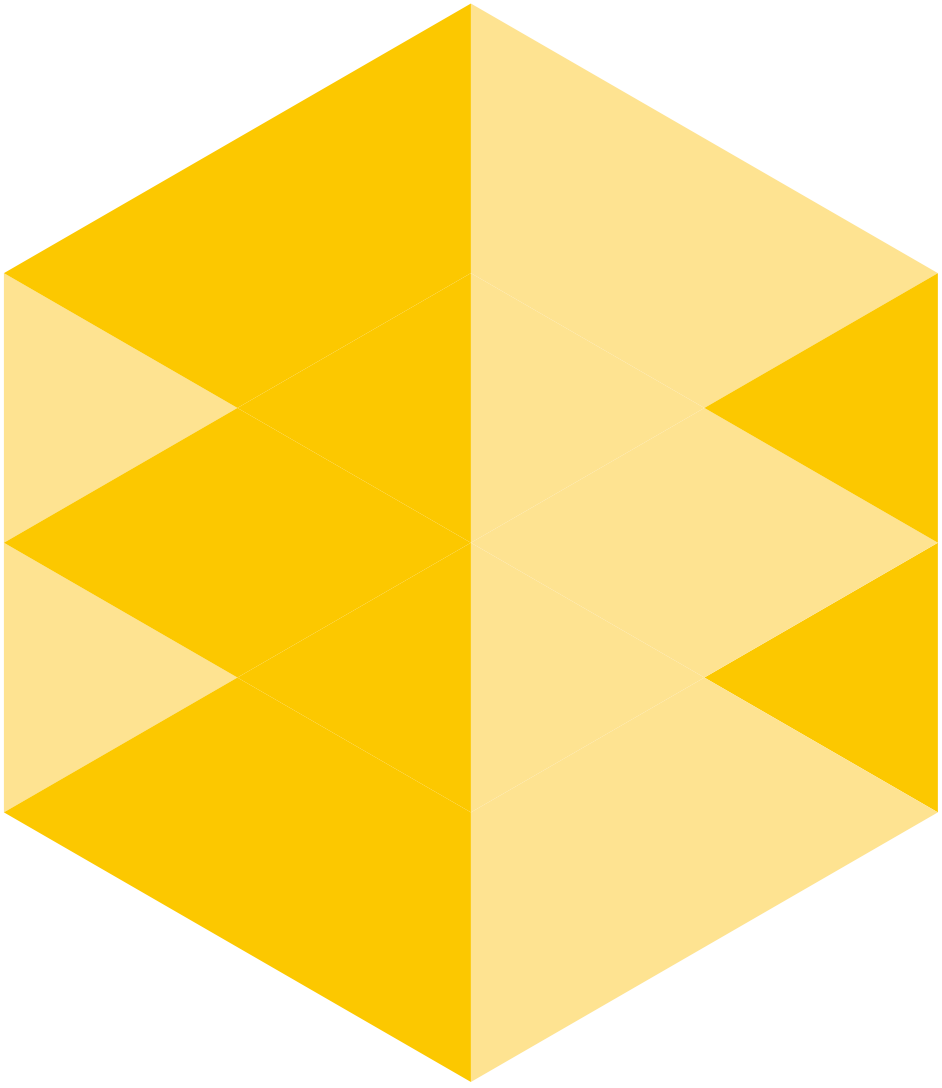

導致 Active Directory 網域完全受損的十種錯誤配置

白皮書

Symantec™
A Division of Broadcom

簡介：Active Directory 安全風險

為什麼Microsoft Active Directory(AD)是企業界最具針對性的資產？因為僅需從受感染的端點向AD進行幾次查詢，攻擊者就可以獲得竊取網域管理員憑證並橫向轉移到高價值資產所需的所有訊息。換句話說，攻擊者只需破壞與網域連接的單個端點，即可控制組織的重要資產。AD資料庫向所有與網域連接的用戶公開公司網路上的所有身份和資源。AD授權用戶（無論合法還是惡意）使用其內置的查詢功能來定位敏感訊息。

不幸的是，AD可能也是您公司中受保護最少的資產。全世界有十分之九的公司使用AD來控制和維護內部資源，但是大多數公司專注於保護端點、應用程序、伺服器、移動設備和網路，進而使AD處於危險的境地。

您不能禁用AD查詢功能，也不能檢測進行查詢的用戶。

這種隱身存取網路資源的能力解釋了為什麼許多攻擊者比網路掃描更喜歡AD偵察。並解釋了為什麼攻擊者熱衷於利用默認的AD查詢功能。請參閱下面MITER記錄的攻擊：

Active Directory 是 APT 的基本構建塊 *

群組名稱	別　　名	憑證盜竊	Active Directory 列舉	時間框架	來　　源
APT 3	Boyusec, UPS	是	是	進行中	中國
APT 10	Stone Panda	是	是	進行中	中國
APT 28	Sofacy, Fancy Bear	是	是	進行中	俄羅斯
APT 29	Cozy Duke, Cozy Bear	是	是	進行中	俄羅斯
APT 32	OceanLotus	是	是	進行中	越南
APT 33	Charming Kitten	是	是	進行中	伊朗
APT 34	Twisted Kitten	是	是	進行中	伊朗
APT 35	Newscaster Team	是	是	進行中	伊朗
Turla	Snake, Uroburos	是	是	最後出現在2017年	俄羅斯
Shell_Crew	Deep Panda	是	是	最後出現在2017年	中國
Dark Seoul	Lazarus Group, Hidden Cobra	是	是	進行中	北韓

*https://attack.mitre.org/groups/G0022

攻擊者從端點開始

初始訪問 | 執行 | 持續 | 權限升級 | 防禦規避 | 憑證訪問 | 發現 | 橫向運動 | 收集 | 滲出 | 命令與控制

Active Directory 攻擊剖析

如果在連接網域的端點上立足，攻擊者將對您的組織資源進行AD偵查。他們從受感染的端點生成查詢並將查詢發送到AD，進而發現定位和存取敏感資料所需的訊息。他們可以輕鬆了解所有員工（包括其身份、角色和權限）以及在資料庫、伺服器、 儲存和內部安全元件上運行的應用程序。然後，他們竊取網域憑證並橫向爬出。

一旦攻擊者攻破了端點，他們只需七分鐘即可完全控制網域（全面的網路漏洞）。隱藏在授權用戶群中，它們顯示為普通用戶。

與網域連接的端點比其他設備具有更高的安全風險，因為只有一個受感染的設備會危害整個組織：您必須在受感染的端點上保護AD，以阻止攻擊者繼續前進。

> 一旦攻擊者攻破了端點，他們只需七分鐘即可完全控制一個網域，建立持久性並開始竊取或加密敏感資料。

Active Directory 錯誤配置為攻擊者敞開了大門

組織隨著時間的推移逐步發展其Active Directory架構，您的IT群組可能無法正確維護其配置設置或實現安全性增強。攻擊者處於等待狀態；當漏洞出現在網域和AD服務中時，它們就會突然出現。他們並且會安裝後門和持久性掛鉤，使它們可以隨時回來。

賽門鐵克認為，這10個Active Directory錯誤配置會帶來最大的風險。

1. 群組政策管理範本可見密碼

攻擊說明：管理員使用群組政策管理範本（GPP）來配置本機管理員帳戶、工作排程，並在用戶登錄時使用指定的憑證掛載網路磁碟。他們將GPP寫入網域控制器的SYSVOL共享資料夾。攻擊者存取SYSVOL共享資料夾內的GPP XML文件並提取儲存在GPP中的指定憑證。

潛在威脅：攻擊者獲得與GPP相同的帳戶權限。 GPP帳戶通常對每個端點都具有本機管理員用戶權限。

2. 隱藏安全標識符（SID）

攻擊說明：攻擊者使用“安全標識符（SID）歷史記錄”從其他高權限SID帳戶（或群組）繼承權限，而不會在其他用戶成員裡留下任何痕跡。

潛在威脅：使用SID屬性表示攻擊者正試圖在低權限帳戶中隱藏高權限群組成員身份（例如，“網域管理員”），以隱藏植入的網域後門。

3. 金票

攻擊說明：具有“krbtgt”帳戶長期密鑰的攻擊者會偽造具有任何用戶權限的登錄權限（TGT）。該權限包含一個假的用戶名稱，該用戶名稱具有網域管理員成員身份（或攻擊者選擇的任何其他成員身份）。

潛在威脅：攻擊者可以獲得網路上任何服務或端點的權限，並且可以在任何地方使用它。這些權限將一直保留，直到管理員重設“kkrbtgt”帳戶為止。

4. 複寫網域的後門

攻擊說明：如果將低權限用戶添加到複製網域物件，則攻擊者將以高權限用戶身份存取所有的網域敏感資料（例如，網域用戶的雜湊值）。由於某些網域服務需要網域複寫功能，因此必須將復寫權限分配給AD物件。

潛在威脅：攻擊者可以完全存取整個公司網域資料庫。

5. 無權限管理員持有的 ACL

攻擊說明：攻擊者利用AdminSDHolder ACL（例如，將具有權限的用戶添加到具有完全控制或寫入權限的AdminSDHolder安全物件中），從而使該非權限用戶能夠將自己或其他用戶添加到較高權限的群組（例如Domain Admins）中，而無需具有高權限。

潛在威脅：啟用和修改此功能的攻擊者無需使用網域帳戶就可以在網域控制器上保留隱藏的管理員權限。

6. 高級用戶列舉

攻擊說明：經過身份驗證的用戶會列舉網域中的任何物件。列舉密碼永不過期的用戶將顯示網域中的高權限用戶。

潛在威脅：有了這些憑證，攻擊者就可以無限期地存取網路中的高權限。

7. 銀票

攻擊說明：用戶請求使用服務帳戶的長期密鑰加密服務權限，以存取網域中的任何服務。攻擊者收集服務權限，並嘗試對長期密鑰進行本地暴力攻擊。

潛在威脅：攻擊者獲得對運行服務帳戶的端點的完全權限存取。

8. 允許匿名 LDAP

攻擊說明：非託管端點查詢Active Directory，並且不進行身份驗證就收集有關網域環境的訊息。

潛在威脅：攻擊者透過未經身份驗證的用戶和具有網路連接的計算機查看整個目錄結構和權限。

9. 啟用 DSRM 登入

攻擊說明：攻擊者啟用和修改DSRM（一種在目錄服務關閉時用於修復或恢復Active Directory的特殊啟動模式），以透過後門在網域控制器上保留隱藏的管理員權限，而無需使用任何網域帳戶。

潛在威脅：攻擊者可以完全控制和存取您組織的網域控制器。

10. 本機管理員橫越

攻擊說明：攻擊者從網路中的本地電腦上竊取本機管理員憑證（許多公司使用映像軟體，因此本機管理員密碼在整個企業中通常是相同的），然後將本機管理員長期密鑰傳遞給遠程端點進行身份驗證。

潛在威脅：攻擊者在一台電腦上獲取本機管理員憑證，然後橫向移動並獲得對網路中每個端點的存取權限。

後續步驟：保護組織免受 Active Directory 威脅

免費安全評估

Symantec提供免費的，軟件驅動的Active Directory威脅

評估。它會自動掃描並檢測AD和整個域環境中的錯誤配置。包括最佳做法修復建議。

向Symantec客戶團隊要求免費的Active Directory威脅評估。

持續性評估

Active Directory是關鍵的攻擊面，需要持續監視錯誤配置、漏洞和攻擊持久性。 Symantec Endpoint Threat Defense for Active Directory包括一個內建的威脅評估服務，該服務提供對網域和Active Directory結構的每個元件的持續分析。 Active Directory的Endpoint Threat Defense查找攻擊者遺留下來的錯誤配置和後門程序，並在識別出該錯誤和後門程序後，透過規範性的修復建議向中央控制台發出警報。

要了解有關適用於Symantec Endpoint Threat Defense for Active Directory的更多訊息，請訪問
https://www.broadcom.com/products/cyber-security/endpoint/threat-defense-for-active-directory

關於賽門鐵克 (Symantec)

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，全世界網際網路流量有 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系整合擴充性，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。(美籍華人王嘉廉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 www.savetime.com.tw

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訊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，以及基於比原廠更孰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、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。
保安資訊連絡電話：**0800-381-500**。