CYBERARK®

有效控制您的企業:

保護網域控制站，遠離 Kerberos 攻擊

目　錄

摘要 3

簡介 4

緩解帳密竊取風險 6

- 減少攻擊面 6
- 管理及安全地保護帳密 6
- 控制及隔離特權連線 6

削弱攻擊者橫向移動的能力 7

- 評估風險 7
- 為本機帳號指派唯一密碼 7
- 使密碼雜湊失效 7
- 建立帳號邊界 8

即時偵測惡意活動 9

- 進行特權使用者及實體行為分析 9
- 收集並分析網路流量 9
- 回應偵測到的事件 9

總結 10

摘要

研究顯示，調查的所有嚴重安全事件中有 80% 到 100% 在整個攻擊過程中獲取並濫用特權帳號[1]。在很多情況下，這些攻擊以網域管理者特權為目標，因為這些特權使攻擊者可以存取網路中的最敏感資產，網域控制站（及 Active Directory），並產生 Kerberos 票證 (tickets) 以未授權、無法偵測而且通常不受約束的方式存取企業環境。如果意圖不軌者取得網域管理者帳密，將會是企業的噩夢。

本 CyberArk 白皮書將：

- 簡要介紹幾種日益流行的 Kerberos 攻擊方法，這些攻擊方法讓攻擊者可以透過強佔網域控制站來控制目標網路；
- 介紹在攻擊過程的兩個關鍵階段，協助減少及粉碎攻擊者企圖（帳密竊取及橫向移動）的策略；
- 重點介紹分析及機器學習在早期偵測異常活動及更快回應正在進行的攻擊方面所扮演的重要角色；
- 解釋先決式分析如何幫助企業偵測常見的 Kerberos 攻擊，如最高權限票證 (Golden Ticket) 攻擊。

1 CyberArk 威脅報告：特權帳號攻擊改變網路安全格局

簡介

進階安全威脅採用一種常見的攻擊模式：首先突破邊界、竊取帳密，然後使用其存取權在網路中橫向移動並提權，直到獲取足夠的特權，使攻擊者可以攻擊主要目標。在很多情況下，攻擊需要或注重獲取網域管理者特權，因為這些帳密在 IT 系統中意味著無限制的存取及控制權限。這些強大的帳號權限使攻擊者可以操作網路中最敏感的資產，即網域控制站（及 Active Directory），而根本不會被其他使用者看到，更不會被設計用於防止此類攻擊的安全解決方案所發現。根據 Microsoft 的說法，如果網域被攻擊，後果非常嚴重，***「如果您的 Active Directory 基礎架構中任何網域控制站的安全性遭到破壞，整個基礎架構的安全性就岌岌可危。」***[2] 鑒於意圖不軌者取得網域管理者帳密會造成如此嚴重的危害，防止攻擊者獲取這些帳密就成為任何企業安全策略的關鍵。

圖 1：特權是整個攻擊生命週期的核心

極具破壞性的攻擊的一個例子是「萬能票證攻擊 (Golden Ticket Attack)」。這種攻擊要求攻擊者獲取金鑰分發中心 (KDC) 密鑰 (krbtgt hash)，使攻擊者可以產生「萬能票證 (Golden Ticket)」，進而獲得對整個企業環境的全面存取權。攻擊者可運用此存取權獲得更多特權，並假冒任何合法使用者而不需要提供帳密，而且被偵測到的可能性非常小，最終導致很難偵測到且事後補救代價高昂的災難性攻擊。在整個攻擊過程中的此刻，當攻擊者獲得網域管理者等級的存取權並全面控制 Active Directory 之後，攻擊者就可控制整個企業，Windows 網域中的所有硬體及軟體也被控制。現在由攻擊者管理及掌握企業所購買、部署並管理的用於防止此類攻擊的安全解決方案。從這種嚴重的攻擊中完成復原是一項艱巨、耗時的工作，而且會造成企業業務中斷。***「在很多情況下，復原過程很漫長，Active Directory 可能在幾天後才能恢復正常執行。」***[3] 此外，在復原過程中，業務營運會中斷或停止，因為使用者不能存取 IT 資源。這種攻擊需要網域管理者帳密；因此，這些帳密自然而然就成為任何狡猾的攻擊者及心懷惡意的內部人員的目標。因此，對於有效管控整個基礎架構，防止攻擊者獲取網域管理者帳密至關重要。透過在整個攻擊過程中的兩個關鍵階段阻止攻擊者的前進步伐，就可以有效地降低網域管理者帳密被竊取所造成的風險：

1. **帳密竊取** – 降低攻擊者竊取帳密並以此作為進入網域控制站缺口的可能性
2. **橫向移動橫向移動** – 削弱攻擊者在網路中移動並獲得網域存取特權的能力

2 Microsoft，《保護 Active Directory 安裝的最佳實踐》，2009 年，第 36 頁。

3 Microsoft，《保護 Active Directory 安裝及日常運營的最佳實踐指南：第 2 部分》，MSDN。

要在這些關鍵階段阻止攻擊，需要多種積極主動的控制措施及即時偵測功能，以便更快發現並阻止正在進行的攻擊。

攻擊手段實例包括：

網域使用者的雜湊傳遞 (Pass-the-Hash) [4] – 當使用者在 Windows 設備上建立互動式連線時，會在設備的記憶體中保存密碼雜湊 (password hashes)。這些雜湊會一直保存在記憶體中，直到連線被正常終止 (登出) 或者設備被重新啟動。

一旦入侵這種以互動式方式連線的設備，攻擊者就可以從設備記憶體中獲取這些雜湊 (帳密)。尤其需要強調的是，攻擊者可以獲取 NTLM 雜湊，然後用 NTLM 雜湊來完成存取其它網路資源所需的 NTLM 身份驗證。在這種攻擊方法中，攻擊者假冒合法網域使用者，其實攻擊者並不知道實際密碼。

Overpass-the-Hash，當使用者透過 Kerberos 身份驗證建立互動式連線時，同樣在設備中保留密碼雜湊。這些雜湊可以用於完成存取網路中的不同目標設備所需的 Kerberos 身份驗證。這種身份驗證使攻擊者可以假冒合法使用者。

票證傳遞 (Pass-the-Ticket)，在 Kerberos 環境中，某些互動式連線會將 Kerberos 票證留在 Windows 設備中。入侵該系統的攻擊者可以獲取這些票證，並假冒成合法使用者來獲取對其它網路資源的存取權限。

PAC 操縱，Kerberos 票證包含稱為特權屬性憑證 (PAC) 的欄位，其中包含群組成員及使用者設定檔等資訊。運用對網域成員電腦的存取權或竊取的 KRBTGT 雜湊，攻擊者就可以在 PAC 中操縱屬性，以升級該票證的特權。然後，攻擊者就可以模仿合法使用者，使用經過修改的票證，獲取對其它網路資源的未授權特權存取權限。

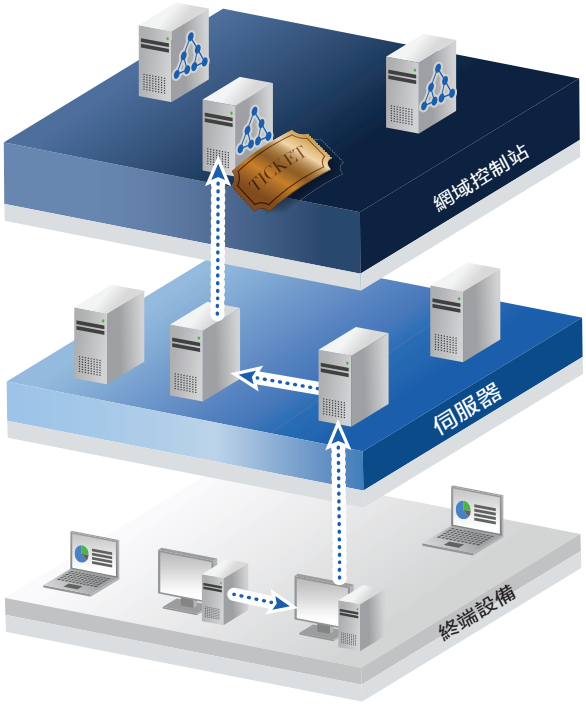

圖 2：攻擊者竊取帳密，橫向移動並獲取更多特權，進入網域控制站並發起破壞性攻擊。

4 雜湊傳遞 (Pass-the-Hash) 攻擊有兩種形式，一種使攻擊者可以作為網域使用者通過身份驗證，另一種使攻擊者可以作為本機使用者通過身份驗證。本文指第一種。

緩解帳密竊取風險

減少攻擊面

對攻擊者來說，擁有更多特權的每個帳密都是攻擊者在 IT 網路中橫向移動的機會。因此，降低攻擊者成功機率的第一步是減少特權帳號的數量，也就是減少攻擊面。顯而易見，應刪除的帳號包括「孤兒帳號 (orphaned)」及不必要的特權帳號。這種帳號在企業中非常常見，是管理者更換後、管理疏忽及缺乏環境能見度的產物。運用 CyberArk 探索及稽核 (CyberArk Discovery and Audit) 等風險評估工具來掃描環境，發現所有特權帳號及特權帳號的當前狀態，包括最後一次使用時間及最後一次密碼更換時間，企業就可以獲得全面能見度，利用此資訊來刪除不必要的特權帳號。然後，企業應考慮刪除個人特權帳號，通常這些帳號具有特殊存取權限，且為了增強安全性與責任歸屬所賦予此種權限。然而，運用 CyberArk 企業密碼金庫等特權帳號安全解決方案，企業就可以恢復使用內建的共用管理者帳號，同時達到對特權帳號使用的相同 (或更全面) 的能見度及可追溯性。透過運用這種解決方案並遵守本文提供的安全指南，企業就可以實現比使用個人特權帳號更出色的安全性，因為所有共用帳號密碼都安全地保存在數位金庫中，而且企業可以控制存取操作並追蹤每個使用者。消除這些主要進入點，即不必要的個人特權帳號之後，攻擊者的攻擊企圖就會在整個攻擊過程中的關鍵點上受挫。此外，運用這些工具對環境進行連續監控，可協助防止「特權帳號蔓延 (privileged account creep)」，防止建立 IT 部門無法控制的新特權帳號。

管理及安全地保護帳密

確定環境中只有必要的特權帳號後，下一步就是集中管理及安全地保護帳密，防止未授權使用特權帳號。由授權使用者保管的特權帳密可能會由於管理疏忽而被盜取，包括將帳密保存在本機電腦中、將密碼寫在紙上、共用帳密及缺乏全生命週期的佈建 (provisioning) 流程。因此，應清查並妥善集中保管所有特權帳密，以降低被內部惡意使用者或外部攻擊者竊取的風險。

在 CyberArk 企業密碼金庫中匯入並安全地保護所有特權帳號之前，可以運用 CyberArk Discovery and Audit 工具來查找這些帳號。然後，可以運用這些解決方案來實作帳密安全保護措施，如定期或在每次使用後自動進行密碼輪換，以及建立一次性密碼來協助達到最有效的保護等。在存取帳密之前實作多因子身份驗證，透過與特權帳號安全解決方案的整合，有效地在存取所有特權帳密前進行多因子身份驗證，就可以增加額外保護層。在保護帳密安全方面，應特別注意網域管理者級帳號，這包括會影響網域控制站的一切因素，包括 DRAC、備份及系統管理程式等管理解決方案。例如，如果您進行網域控制站虛擬化，則 ESX 管理者就是網域管理者，對於這些敏感的憑證，應進一步採用控制流程，如雙重控制 (Dual Control)，此工作流程審核是進一步提高安全性的有效方法。這些主動控制方法的落實，可以防止帳密落入攻擊者手中，在攻擊一開始就遏止攻擊。

控制及隔離特權連線

要防止無意或故意誤用特權密碼，一種有效方法是防止使用者看到或知道密碼。運用跳板機如 (CyberArk 特權連線管理器) 就可以建立連線而不需要將密碼發送到使用者終端設備上，進而使鍵盤記錄及記憶體 Scrapers 等帳密竊取方法毫無用途。此款解決方案的工作原理是將使用者經由代理伺服器連線到目標設備，而不透露密碼給終端使用者。當有使用者請求透過特權連線管理器建立連線時，此解決方案可以自動從安全的數位金庫中取得帳密並直接發送給目標伺服器。運用此解決方案，使用者基本上無法得到有關帳密的任何資訊，可有助於防止因密碼管理疏漏或惡意企圖而使意圖不軌者取得帳密。用於安全保護及隔離使用者連線的這種分層管理帳密的方法及跳板機，可以大幅度降低攻擊者竊取帳密並發起攻擊（包括進行偵察、橫向移動橫向移動及提權）的可能性。

削弱攻擊者橫向移動的能力

橫向移動通常是整個攻擊生命週期的第二個階段。攻擊者運用這種方法來在網路中四處尋找最終目標，從一台設備上竊取帳密，然後從遠端存取或跳越到另一台設備。外洩的密碼、密碼雜湊（完成密碼驗證後保存在設備中的密碼雜湊）及 Kerberos 票證都可以用於各種類型的橫向移動方法中。橫向移動方法包括雜湊傳遞（Pass-the-Hash）、Overpass-the-Hash 及票證傳遞（Pass-the-Ticket）。這些方法使攻擊者可以毫無約束地移動，會造成企業很大風險，因此瞭解遭駭嚴重程度對於如何降低風險非常重要。

評估風險

除了帳號報表外，CyberArk Discovery and Audit 還可以提供直覺的帳密圖，顯示一個帳密遭竊後，可如何用於存取整個網路中的多台設備。這些資訊可以協助企業決定在降低橫向移動風險時，將工作重點放在哪裡。CyberArk Labs 進行的研究顯示，在很多網路中，大多數設備都可以作為攻擊的起始點，使攻擊者可以透過遭竊的帳密成功入侵 80% 以上的網路設備。[5] 這意味著攻擊者只要有一次成功竊得帳密，就可以存取大部分網路設備。若想使企業重新取得優勢，用於防止這種橫向移動橫向移動的主動控制措施及進階偵測技術至關重要。

為本機帳號指派唯一密碼

橫向移動的一個常見罪魁禍首是本機管理者帳號。根據最近對一個零售環境的調查，我們發現幾乎所有系統中都使用相同的本機管理者帳密。[6] 因此，一旦一個本機管理者帳號被破解，攻擊者很可能能夠存取所有系統，也就是整個環境。為了限制橫向移動，防止攻擊者隱身在網路中四處漫遊，最佳策略是幫伺服器上的每個本機帳號設定一個唯一密碼。這樣，攻擊者就不能取得保存在一台伺服器中的密碼雜湊以用來存取另一台與目標系統關係密切的伺服器。然而，如果沒有自動化解決方案，則為每個本機帳號設定並管理唯一的密碼將是一項非常艱巨的任務。CyberArk 企業密碼金庫帳密管理解決方案，專門設計用於管理數千個帳號，建立唯一的密碼並進行管理，而不需要管理者做這些工作。此款解決方案可以大幅度提高環境安全性，而且不會造成 IT 及資安團隊不必要的負擔。

使密碼雜湊失效

我們強烈建議定期輪換帳密來降低帳密被盜的可能性，這也是阻止橫向移動的一個關鍵手段。由於密碼雜湊在橫向移動方面扮演著關鍵角色，因此有必要削弱保存在伺服器中的雜湊的效力。CyberArk 企業密碼金庫及應用程式身份管理器（適用於保存在應用程式及程式碼中使用的密碼）等特權密碼管理工具可用於在每次使用後替換密碼，使身份驗證完成後留在伺服器及工作站上的密碼雜湊對攻擊者來說毫無用處。

5 CyberArk Labs 調查報告：《分析真實環境 Windows 帳密竊取攻擊風險》，2015 年

6 Mandiant，《M-Trends® 2015：前線觀點》，2015 年，第 8 頁。

建立帳號邊界

對企業來說，Microsoft[7] 建議的限制橫向移動的另一種重要方法是建立並實作帳號邊界，或者不允許在不同的設備層中使用相同的帳號。設備層定義如下:

1. **第 2 層：工作站**
2. **第 1 層：伺服器**
3. **第 0 層：網域控制站**

例如，用於存取網域控制站或相鄰解決方案（如網域控制站備份系統）的任何帳密不能同時用於登入伺服器。Microsoft [8] 建議採用這種方法來防止攻擊者竊取某一層的帳密並利用該帳密來存取另一層的資產（例如在入侵工作站之後存取網域管理者帳密）。這種攻擊手段通常稱為提權（privilege escalation）；Mandiant 公司最近重點介紹了這種攻擊手段的真正風險。該公司對一個環境進行了深入調查，發現***「網域控制站共用已經被攻擊者取得本機管理者密碼，因此成為很容易被攻陷的目標。」***[9] 最後，實作帳密層以保護網域控制站存取也非常有幫助，可以有效降低基於 Kerberos 的攻擊的風險。

一般可透過以下方法落實帳密層的實作：從原來一個網域帳號轉換成三個個別的管理者特權網域帳號，每個資產層一個管理者特權網域帳號，然後設定存取權限來防止跨層（cross-tier）使用。這種方法儘管可以達成隔離帳密使用的目的，但同時也會增加複雜性，而且有可能會增加攻擊面，因為此方法會大幅增加特權帳號數量，在使用個人特權帳號作為管理者帳號時尤其如此。此外，管理者現在需要管理三個不同的帳號密碼，這就提高帳密管理不善的可能性。因此，雖然我們的目標是降低橫向移動的風險並防止攻擊者獲取更多特權，但同時造成更嚴峻的身份管理挑戰：企業現在需要管理大量特權帳號，而這些特權帳號都是攻擊者的標的。

使用自動控制及監控可以降低複雜性，也可以簡化帳號邊界的實作，減少攻擊面並讓使用者容易接受。CyberArk 企業密碼管理器及特權連線管理器等解決方案使企業再也不必使用多個個人特權帳號，而是使用用於每個層的共用管理者帳號。對於伺服器及工作站，在大多數應用場景，可以透過使用本機管理者帳號來減少網域帳號。CyberArk 企業密碼金庫可以集中保存、安全地保護及自動輪換共用的本機管理者帳號，而且每次存取操作都受到控制及追蹤，因此幾乎不會出現不透明或無法追查責任的情況。透過額外的跳板機（例如 CyberArk 特權連線管理器），使用者可以無縫地存取帳號而不會看到密碼，因而可以更有效保護帳密安全，同時得到單一簽入存取所有帳號的好處。這種方法的優勢包括減少特權網域帳號、降低網域帳號被破解的風險以及改進終端使用者體驗，因為現在只需要管理一個帳號（最好是必須經多因子身份驗證的帳號）。

除了帳密使用的區隔（segmentation）外，Microsoft 還建議使用專用且經過強化的工作站來用於管理用的存取。[10] 這種風險緩解戰術雖然有效，但會增加環境複雜性及支出。運用跳板機來防止惡意軟體從使用者終端設備上傳播到目標伺服器上，這種方法的附加好處是可以降低對隔離的、經過強化的管理專用工作站的需求，還可以大幅度降低實作帳號邊界的成本及複雜性。對於希望實作 Microsoft 帳密管理建議的企業來說，CyberArk 特權帳號安全解決方案提供一種有效的途徑，能夠比以傳統方法更低成本及複雜性的方式來建立帳密層，而且可以減少不滿的終端使用者。

---

7 Microsoft，《緩解雜湊傳遞及其它憑證或帳密竊取威脅，第 2 版》，Trustworthy Computing，2014 年。

8 Microsoft，《緩解雜湊傳遞及其它憑證或帳密竊取威脅，第 2 版》，Trustworthy Computing，2014 年。

9 Mandiant, 「M-Trends® 2015: 前線觀點》，2015 年，第 8 頁。

10 Microsoft，《緩解 Pass-the-Hash 及其它憑證或帳密竊取造成的風險，第 2 版》，Trustworthy Computing，2014 年，第 18 頁。

即時偵測惡意活動

進行特權使用者及實體行為分析

如同任何關鍵攻擊向量，早期偵測及回應對於緩解進階攻擊的影響至關重要。CyberArk 特權威脅分析等分析解決方案可以用於識別異常使用者行為及預警可能遭受攻擊的系統活動。機器學習演算法可以深入分析各個特權使用者、特權帳號及系統活動的一般模式，以動態建立「正常行為」基準線。透過比較即時活動與該基準線，分析引擎就可以發現不符合基準的行為，進而偵測異常行為並向企業發出告警。

運用特權帳號活動行為分析，包括網域管理者活動，企業就可以偵測到攻擊預兆，包括疑似帳密竊取、橫向移動及提權活動。透過早期偵測，資安團隊就可以在攻擊者入侵目標設備之前做出更有效的回應。

收集並分析網路流量

在企業 Windows 環境中，伺服器、工作站及其它網路設備與網域控制站 (Windows 身份驗證的中央授權單位) 進行通訊。Kerberos 是 Windows 身份驗證協定，而此協定包含攻擊者可以利用的多個潛在安全性漏洞。只需透過能容易取得的工具與幾個簡單的操作，攻擊者就可以操作 Kerberos 票證，假冒成授權使用者來在網路中四處移動而不被發現。傳統的安全監控工具一般不能發現這些類型的攻擊，因為登入活動看起來是經過授權。

然而，我們可以透過一些跡象發現隱藏在 Kerberos 身份驗證流量中深層的攻擊。透過進行深度資料封包檢查，CyberArk 特權威脅分析等工具可以幫助發現表示正在發生 Kerberos 攻擊的異常現象，包括可能會造成企業嚴重後果的 PAC 操縱、超雜湊傳遞及最高權限票證攻擊。儘早發現這些災難性攻擊，是限制攻擊者可以造成的危害的關鍵，透過持續分析網路流量，企業可以即時偵測到 Kerberos 攻擊，包括最高權限票證，並為資安團隊提供更快回應所需的關鍵資訊。

回應偵測到的事件

資安團隊收到出現可疑行為及其它攻擊跡象的告警後，資安團隊必須進行分類並採取行動。運用 CyberArk 特權威脅分析等智慧工具，資安團隊可以輕鬆調查每起安全事件的細節，包括受影響的設備、使用者以及攻擊中所使用的帳號。

除了提供有關每起安全事件的資訊外，CyberArk 解決方案還能夠及時回應偵測到的威脅，因為 CyberArk 解決方案不僅可以偵測可疑被盜取的特權帳密，而且能夠透過 CyberArk 企業密碼金庫立即更換被竊取的密碼。透過阻止攻擊者繼續利用遭竊取的帳密，企業可以有效地限制攻擊者橫向移動並阻斷其在網路中進一步擴散的能力。

總結

雖然進階攻擊具有持久而且破壞性強的特點，但透過結合使用主動保護及威脅偵測方法，企業可以有效打擊攻擊者竊取帳密並在網路中橫向移動的企圖。設計並實作正確的策略來保護對網域管理者帳密的存取，是所有企業都應該大力採用的重要方法，因為如果這些帳密被竊取，攻擊者就能在所有 IT 系統中取得特權，造成嚴重的後果。CyberArk 特權帳號安全解決方案是一種專門設計用於保護特權帳號並偵測進階威脅的平台，可以大幅增強企業的網域控制站安全性，而不會造成不必要的複雜性、成本及終端使用者的負擔。