Active Directory 侵害と推奨対策

slideshare.net/yurikamuraki5/active-directory-240348605

Yurika Kakiuchi

1. 1. Active Directory 侵害と推奨対策 垣内 由梨香 セキュリティ プログラム マネージャ セキュリティ レスポンス チーム マイクロソフト コーポレーション CISSP
2. 2. セッション概要 □ 目的 □ マイクロソフト サポート及びインシデント調査サービスで把握している実態、対応事例から得られた知見を共有 □ マイクロソフトが提唱する対策の解説し Active Directory の保護に役立てていただく □ 目次 □ 標的型攻撃における Active Directory の侵害の概要 □ Active Directory の侵害の特徴 1. “のっとりアカウント”を中心とした侵害の展開 2. 複雑なAD環境に起因する問題 3. 侵害の検出が困難 4. 復旧が困難 □ 推奨する Active Directory 保護策 □ 推奨する対策の概要 □ 資格情報の保護 □ 端末の保護 □ 監視、対応、復旧 2© Copyright Microsoft Corporation. All rights reserved.
3. 3. © Copyright Microsoft Corporation. All rights reserved. 3
4. 4. マイクロソフトにおける観測 □ セキュリティ侵害の事例は、増加傾向にある □ 攻撃手法や対象の広がり、検出技術の向上 □ IT 障害と認識されているケースがみられる □ COVID-19 パンデミック期間に増加 □ 従来の手法＋COVID-19 をベースにしたフィッシング □ 環境の変化に伴う脆弱性の露出 □ クラウド環境利用の増加 □ リモート ワーク 環境の増加 © Copyright Microsoft Corporation. All rights reserved. 4

5. 5. マイクロソフト COVID-19 セキュリティ調査 © Copyright Microsoft Corporation. All rights reserved. 5 New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security
6. 6. 攻撃の一環としてActive Directory の侵害が実施される □ Active Directory ドメインディレクトリの調査 □ 組織内部構造の把握 □ ディレクトリ内のユーザーの情報取得 □ ドメインユーザのアカウントの乗っ取り □ 組織ユーザーになりすましたフィッシング □ より高い権限の取得 □ ドメイン管理権限の取得 □ 任意のドメイン内ユーザーのなりますまし □ 永続的な侵入口の設置 □ 痕跡の消去 © Copyright Microsoft Corporation. All rights reserved. 7
7. 7. 一般的な Active Directory 侵害の流れ © Copyright Microsoft Corporation. All rights reserved. 8 Tier 2 デバイス ローカル 管理者 Tier 0 認証基盤 ドメイン 管理権限 Tier 1 サーバー 管理者 1. ドメインクライアント端末への侵入 1. フィッシング、ソーシャルエン ジニアリング 2. ブルートフォース攻撃 2. ラテラル・ムーブメント Lateral Movement (横方向への移動) 1. 探索活動 2. 別のクライアントへの侵害 1. 特権昇格 1. サーバ管理者権限の取得 2. ドメイン管理者権限の取得 3. ドメイン 2. 目的の実行 1. 情報取得、ランサムウェア 2. 永続的なアクセス口の設置 3. 痕跡の削除
8. 8. Active Directory 侵害の特徴 © Copyright Microsoft Corporation. All rights reserved. 9 “乗っ取り” を中心とした侵 入拡大 複雑なAD環境 に起因する問題 侵入者の追跡が 困難 対応・復旧が 困難
9. 9. Active Directory 侵害の特徴 © Copyright Microsoft Corporation. All rights reserved. 10 “乗っ取り” を中心とした侵 入拡大 複雑なAD環境 に起因する問題 侵入者の追跡が 困難 対応・復旧が 困難
10. 10. “乗っ取りアカウント” を軸に侵入を展開する © Copyright Microsoft Corporation. All rights reserved. 11 ユーザー クライアント端末 サーバー サーバー管理者 ドメイン管理者 認証サーバー ドメインコントローラ フィッシング ソーシャルエンジ ニアリング 総当たり Active Directoryドメイン
11. 11. ドメイン内のユーザーになりすます □ ユーザー名、パスワードを取得し認証する □ 推察しやすい・簡単なパスワードで認証を試みる □ 平文で記載されているパスワードを取得する □ 例：ユーザー、管理者がメモとして記載している □ 例： バッチファイルに記載されている □ “Derived credentials” (プロトコルが利用する派生資格情報) を取得し再利用する □ NTLM 認証： ハッシュ化されたパスワード (NTOWF: NT One Way Function) □ Kerberos 認証： □ TGT, TGS, TGT セッション鍵, TGS セッション鍵 □ DES, RC4 == NTOWF, AES keys 12© Copyright Microsoft Corporation. All rights reserved.

12. 12. ドメイン内のユーザーになりすます □ ユーザー名、パスワードを取得し認証する □ 推察しやすい・簡単なパスワードで認証を試みる □ 平文で記載されているパスワードを取得する □ 例：ユーザー、管理者がメモとして記載している □ 例： バッチファイルに記載されている □ “Derived credentials” (プロトコルが利用する派生資格情報) を取得し再利用する □ NTLM 認証： ハッシュ化されたパスワード (NTOWF: NT One Way Function) □ Kerberos 認証： □ TGT, TGS, TGT セッション鍵, TGS セッション鍵 □ DES, RC4 == NTOWF, AES keys 13 管理の盲点 © Copyright Microsoft Corporation. All rights reserved.
13. 13. 認証で利用される派生資格情報 © Copyright Microsoft Corporation. All rights reserved. 14
14. 14. デバイスには、ログインするユーザーの認証情報が保存されている 15© Copyright Microsoft Corporation. All rights reserved.
15. 15. 標準ユーザーは、認証情報は盗み出せない 16 NTLM NTOWF Kerberos TGT LSASS ドメインユーザー (ローカル管理者権限なし） サーバー管理者 (ローカル管理者権限あり） ローカル管理者 (ローカル管理者権限あり） Kerberos TGT NTLM NTOWF NTLM NTOWF SAM NTLM NTOWF NTLM NTOWF NTLM NTOWF API © Copyright Microsoft Corporation. All rights reserved.
16. 16. ローカル管理者権限では認証情報を盗み出せる 17 NTLM NTOWF Kerberos TGT LSASS ドメインユーザー (ローカル管理者権限なし） Kerberos TGT NTLM NTOWF NTLM NTOWF SAM NTLM NTOWF NTLM NTOWF NTLM NTOWF サーバー管理者 (ローカル管理者権限あり） ローカル管理者 (ローカル管理者権限あり） API API API © Copyright Microsoft Corporation. All rights reserved.
17. 17. 取得した派生資格情報を攻撃に利用するには □ 解明し、利用する □ レインボーテーブルによる解析 □ 危殆化した暗号・ハッシュアルゴリズムの既知の問題を用いた解析 □ 派生資格情報を再利用する □ もともとのパスワードや鍵を取得していない状態で攻撃が可能 □ 攻撃手法の例 □ Pass-the-Hash 攻撃: NTLM 認証において NTOWF を再利用する □ Pass-the-Ticket 攻撃 : Kerberos 認証においてチケット、キーを再利用・偽造する 18© Copyright Microsoft Corporation. All rights reserved.
18. 18. 認証で利用される派生資格情報 © Copyright Microsoft Corporation. All rights reserved. 19
19. 19. ツールの拡大による攻撃手法の広まり □ セキュリティ研究目的などから ツールが開発 □ 2006 年ごろからツール化が盛んに □ 侵入テストの需要増とともにツールの開発も 盛んに □ Windows Credential Editor □ Mimikaz □ ツールの実行にはローカル管理者 権限が必要 □ Post-Exploitation として利用される 20 Windows Credential Editor © Copyright Microsoft Corporation. All rights reserved.

20. 20. ドメイン内の“乗っ取りアカウント” に対する対策が不足している □ “Active Directory ドメイン内 = 安全” とみなし、ドメインユーザーがすでに侵害されていること を前提とした対策が不足している □ 特権分離の不足 □ 特権昇格の脆弱性への対応不足 □ 悪用が多く報告されている脆弱性の例： □ MS14-068 Kerberos の脆弱性により特権が昇格される (3011780) □ MS17-010 Microsoft Windows SMB サーバー用のセキュリティ更新プログラム (4013389) □ CVE-2020-1472 [AD 管理者向け] CVE-2020-1472 Netlogon の対応ガイダンスの概要 – Microsoft Security Response Center © Copyright Microsoft Corporation. All rights reserved. 21
21. 21. 実際の事例 23 ドメインユーザー 資格情報 ローカル管理者 サーバー管理者 ドメイン管理者 クライアント アプリサーバー ドメイン コントローラ クライアント 資格情報 初期アクセス：よくある原因 ・フィッシング、ソーシャルエンジニアリング ・よく知られたマルウェア等の既知の手法 ・リモートデスクトップ接続やVPN接続の安易なパスワード © Copyright Microsoft Corporation. All rights reserved.
22. 22. 実際の事例 24 資格情報 資格情報 よくある原因 ・特権昇格の脆弱性 ・Mimikatzなどの資格情報取得のツール、メモリのダンプ ・よく知られたローカルアカウントの安易なパスワード © Copyright Microsoft Corporation. All rights reserved.
23. 23. 実際の事例 25 資格情報 資格情報 資格情報 よくある原因 ・展開イメージが統一・管理簡素化のために同一アカウントを展開 ・よく知られた既定アカウント ・よく知られたサービスのアカウント ・ブルートフォース © Copyright Microsoft Corporation. All rights reserved.
24. 24. 実際の事例 26 資格情報 資格情報 資格情報 資格情報 © Copyright Microsoft Corporation. All rights reserved.
25. 25. 資格情報 実際の事例 27 資格情報 資格情報 資格情報 資格情報 よくある原因 • サーバ管理者が利用する 端末と業務端末が同一 © Copyright Microsoft Corporation. All rights reserved.
26. 26. 実際の事例 28 資格情報 資格情報 資格情報 資格情報 資格情報 資格情報 よくある原因 ・ヘルプデスク業務 ・管理業務 © Copyright Microsoft Corporation. All rights reserved.
27. 27. 実際の事例 29 資格情報 資格情報 資格情報 資格情報 資格情報 資格情報 資格情報 © Copyright Microsoft Corporation. All rights reserved.
28. 28. 実際の事例 30 資格情報 資格情報 資格情報 資格情報 資格情報 資格情報 資格情報 © Copyright Microsoft Corporation. All rights reserved.
29. 29. Active Directory 侵害の特徴 © Copyright Microsoft Corporation. All rights reserved. 31 “乗っ取り” を中心とした侵 入拡大 複雑なAD環境 に起因する問題 侵入者の追跡が困難 対応・復旧が 困難

30. 30. Active Directory の根本的な構成や管理不足の問題に起因することが多い □ セキュリティ更新が行われていない □ ドメインコントローラ、重要なサーバーへのセキュリティ更新が行われていない □ Active Directory 構成の複雑化による十分なセキュリティ設定の不足、認識ミス □ 複雑なグループポリシー、例外設定により構成把握が実施できていない □ バッチやタスク処理の不十分なセキュリティ（平文パスワード入れ込み） □ ファイルサーバ、アプリケーションサーバーの導入に伴う特権の払いだし □ 管理組織上の問題による管理不足および対策の実施困難性 © Copyright Microsoft Corporation. All rights reserved. 32
31. 31. Active Directory 侵害の特徴 © Copyright Microsoft Corporation. All rights reserved. 33 “乗っ取り” を中心とした侵 入拡大 複雑なAD環境 に起因する問題 侵入者の追跡が困難 対応・復旧が 困難
32. 32. イベントログからは、正規と“乗っ取り” による動作を見分けることが 困難 □ 正規の動作と、侵入者による動作をイベントログからのみ判断することは極めて困難 □ なりすました認証によるアクセスも、正規の認証のアクセスも、認証成功として同様のイベン トログが記録される 34© Copyright Microsoft Corporation. All rights reserved.
33. 33. 既定のツール (“living off the land”) やコマンドの利用 □ Windows コマンド □ Tasklist, ver, whoami, net user, net group, klist 等 □ Powershell, PSExec, サービスの停止、バッチファイル (.bat, .reg) 実行 □ AD 標準ツール・コマンド □ LDAP クエリ □ ADユーザー権限でLDAPクエリを通常の権限・設定で投げ、情報を収集可能 □ 所属しているグループ、アクセス権限 □ インターナルフィッシング □ UPN メールアドレス、電話番号 □ Powershell, PSExec, サービスの停止、バッチファイル (.bat, .reg) 実行 □ 単なるツールのブロック、イベントの検出だけでは検知が難しい。 □ 正常と異常を定義し、ほかのアクティビティと照らし合わせて相関関係を調査する必要がある © Copyright Microsoft Corporation. All rights reserved. 35
34. 34. 140日以上 長期的に侵入されているケースが多い □ セキュリティ対応以外から、AD侵害が発覚する事例 □ (例) 別の障害調査の過程で、意図していないユーザー、構成が発覚する □ (例) バッチ処理の失敗の要因調査過程で不審なファイルが発覚する □ セキュリティ観点からの調査を行った結果、長期的に侵害されていることが判明する □ 初期侵入のログは、アラートとしてあがっていない 最初のホスト侵害 ドメイン管理者侵害 攻撃の検出 調査＆準備 侵害拡大 24-48 時間 © Copyright Microsoft Corporation. All rights reserved. 36
35. 35. Active Directory 侵害の特徴 © Copyright Microsoft Corporation. All rights reserved. 37 “乗っ取り” を中心とした侵 入拡大 複雑なAD環境 に起因する問題 侵入者の追跡が困難 対応・復旧が 困難

36. 36. 特徴 4 ：迅速な対応、完全な復旧が難しい Active Directory侵害の調査および復旧作業は、長期化する傾向にある □ 運用、ビジネスへの影響懸念 □ ドメインコントローラの即時停止、長期停止ができないため時間を要する、限定的な対応に限られる □ 依存するアプリケーションの影響調査 □ 関連組織、影響調査との調整の難航 □ 例：ネットワーク管理部門、アプリ部門との調整 □ 調査のためのログ導入、ツール導入における承認の難航、システム上の制限 □ 限られた予算での限定的な対応 □ 事前に想定している障害対応予算を超える対応が必要となる場合がある □ 侵入者の全容を調査することが困難 □ 長期的な侵害のため、ログが残されていない □ 調査に必要なログが残されていない（例：異常系のイベントログしかない、ネットワークのログがない） □ 十分な復旧が実施できない □ 必要とされてる復旧を正しく理解できていない □ 組織上の問題で対策を実施できない 38© Copyright Microsoft Corporation. All rights reserved.
37. 37. 事例：繰り返し被害にあう組織の増加 □ 一度侵入の痕跡を調査し、対策を行ったが、繰り返し被害に遭うケースがみられる □ よく見られる原因 □ 調査が不十分 □ 例：侵入者が設置した永続的な接続口、すでに侵害されているアカウントをすべて除去しきれていないれていなかった □ 例：フォレスト内の別のドメインの調査を実施していなかった □ 必要十分な対策、根本的な対策を実施していない □ 例：最初に乗っ取られたアカウントをリセット、ドメイン管理者やドメイン鍵 (trbtgt) リセットは実施していない □ 例：ドメインを再構築したが、運用を変更しなかった © Copyright Microsoft Corporation. All rights reserved. 39
38. 38. © Copyright Microsoft Corporation. All rights reserved. 41
39. 39. パンデミックが示唆するこれからのセキュリティ © Copyright Microsoft Corporation. All rights reserved. 42 ユーザに寄り添った セキュリティを意識 させない IT基盤 誰もが ゼロトラストへの 取り組みを進めてい る 多様なデータ セットが優れた 脅威 インテリジェンスに つながる サイバー レジリエンスは 事業運営の 基礎である 後付け型の セキュリティは 終息する
40. 40. Active Directory の保護ロードマップ □ Active Directory 管理階層モデルの導入 □ 特権アクセスの保護 および ID保護 □ 特権アクセスワークステーション (PAW) の保護およびドメインデバイスの保護 □ 適切な監視と迅速な対応 □ 調査と復旧 © Copyright Microsoft Corporation. All rights reserved. 43
41. 41. Active Directory 管理階層モデル: 高い権限の特定と分離 44 Tier 0 認証管理 Tier 1 サーバー管理 Tier 2 端末管理 • フォレスト、ドメイン管理 (特にDomain Admins, Enterprise Admins) • 証明局 (CA) 管理 • アプリケーション、データベース 管理 • クライアント端末、デバイス 管理 © Copyright Microsoft Corporation. All rights reserved.

42. 42. 優先的に保護するべき高い権限をもつアカウント ドメイン管理者 (Domain Administrators) およびドメイン管理者と同レベルの特権を持つアカウント Domain Administrators, Enterprise Administrators, Schema Administrators, Account Operators, Backup Operators BUILTINAdministrators ドメイン コントローラを管理するために利用しているアカウント (例) System Center Operations Manager System Center Configuration Manager の Operations/Configuration Manager administrators 特権アカウントが稼働しているホストの hypervisor server administrators ドメイン内のデバイスで高権限で稼働するアカウント Service accounts used for software installation or updates Service accounts used for security scans Service accounts for backup Shared local administrator accounts ビジネスへの影響が高いシステム、アカウント 電子メール、ファイル共有、コンテンツ共有など 組織のVIP のアカウント、秘書、研究者、IT 管理者 © Copyright Microsoft Corporation. All rights reserved. 45
43. 43. Active Directory 管理階層モデル：管理権限 46 Tier 0 認証管理 Tier 1 サーバー管理 Tier 2 端末管理 (Domain Admins, Enterprise Admins) © Copyright Microsoft Corporation. All rights reserved.
44. 44. Active Directory 管理階層モデル：ログオン制限 47 Tier 0 認証管理 Tier 1 サーバー管理 Tier 2 端末管理 (Domain Admins, Enterprise Admins) © Copyright Microsoft Corporation. All rights reserved.
45. 45. 運用のベストプラクティス © Copyright Microsoft Corporation. All rights reserved. 48 参照：Operational standards based on clean source principle
46. 46. Active Directory 特権アカウントの保護 49 対策 目的 対策の効果 対策作業量 組織内の権限を分離する 攻撃者がドメイン内の異なる端 末へ侵入を広げる機会を減らす 非常に高い 高 特権アカウントの保護 • 通常のドメイン管理は委任し、必要とする作業の みに利用 • 高い特権を持つアカウントを使用してインター ネットを参照禁止 • Enterprise Admins、Domain Admins、 Administrators グループの多用を禁止 • Kerberos 認証のみ、キャッシュ ログオン禁止、 DES/RC4 の禁止, 委任禁止、チケット有効期限 4 時 間 ドメイン管理権限を保護 非常に高い 中 専用の高い権限を持つ端末の利用と要塞化 高い権限を扱う端末を要塞化す ることで攻撃者の機会を減らす 高 中 ～高 © Copyright Microsoft Corporation. All rights reserved.
47. 47. ローカル管理者権限の保護① ローカル端末内での保護 管理者権限がなければ認証情報を取得できない 管理者権限を取られてしまえばあらゆる攻撃が可能となる 50 対策名 目的 対策の効果 対策作業量 既定の Local Administrator の 無効化 既知のアカウントを狙った 攻撃を防ぐ 高 低 一般ユーザーをローカル管理者 グループから外す 資格情報窃取やシステムへ の攻撃を防ぐ 非常に高い 高 セキュリティ更新プログラムの適用 ※特に特権昇格、情報漏洩、バ イパスの脆弱性 脆弱性を悪用する攻撃を防 ぐ 中 中 © Copyright Microsoft Corporation. All rights reserved.

48. 48. ローカル管理者権限の保護② 横展開防止 □ 同じレベルの権限の端末へ侵入を広げることを防ぐ □ 同じパスワードやハッシュの悪用 □ ネットワーク上の攻撃者の操作性を制限する 51 対策名 目的 対策の効果 対策作業量 異なるローカル管理者アカウント資 格情報 ※LAPS ツール 攻撃者がドメイン内の異なる端 末へ侵入を広げる機会を減らす 高 中～高 ローカルアカウントのネットワーク 越しの操作制限、ログオン防止 ※新しい well-known SIDs の活用 遠隔地にいる攻撃者がローカル 管理者を悪用することを防ぐ 高 中
49. 49. Local Administrator Password Solution (LAPS) □ ローカル管理者アカウント資格情報を管理する □ ランダムなパスワード設定 □ 使いまわしを防ぐ □ AD側からの一元管理 □ 注意： □ KB3062591 の追加インストールが必要 □ スキーマ拡張、クライアントサイド拡張が必要 52
50. 50. ローカルアカウント管理者のネットワークログオン制限 □ 遠隔地にいる攻撃者がローカル管理者を悪用することを防ぐ □ グループポリシー □ コンピューターの構成 - Windowsの設定 - セキュリティの設定-ユーザー権利の割り当て - [ネットワーク経由のアクセ スを拒否] □ 新しい セキュリティ識別子 (SID) を活用したログオン制限の実施 □ Windows 8 以降既定、Windows 7 / Windows server 2008 R2 は マイクロソフト セキュリティ アドバイザリ 2871997 (KB2871997) 適用後利用可能 □ S-1-5-113 Local Account □ S-1-5-114 Local Account and member of Administrators group □ 構成 □ ネットワーク経由でコンピューターへアクセスを拒否する
（SeDenyNetworkLogonRight） □ バッチ ジョブとしてログオンを拒否する
（SeDenyBatchLogonRight） □ サービスとしてログオンを拒否する
（SeDenyServiceLogonRight） □ ターミナル サービスを使ったログオンを拒否する
（SeDenyRemoteInteractiveLogonRight） □ プログラムをデバッグ
（SeDebugPrivilege）（権限の昇格とプロセ スの挿入の試みに使用される許可） □ Windows でローカル アカウントのリモート使用をブロックする方法 53
51. 51. 55
52. 52. セキュリティ更新プログラムの適用 □ ドメインコントローラーおよびドメイン内の重要サーバーへの更新プログラムの適用を定期的 に実施する □ [推奨] 公開されているすべてのセキュリティ更新プログラムの早期適用 □ 優先付けが必要な場合はリスクを評価し順次適用 □ 既知の悪用が報告されている脆弱性 □ MS14-068 Kerberos の脆弱性により特権が昇格される (3011780) □ MS17-010 Microsoft Windows SMB サーバー用のセキュリティ更新プログラム (4013389) □ 「ゼロデイ」での悪用が報告されている新規の脆弱性 □ CVSS スコア、悪用可能性指標が高い脆弱性 □ 2020年8月CVE-2020-1472 Netlogon の特権の昇格の脆弱性 □ リモートコード実行を可能とするなど、深刻度「緊急」の脆弱性 □ 特権昇格の脆弱性 (深刻度「重要」） 56

53. 53. 推奨されるセキュリティ設定 Windows セキュリティベースライン、Security Compliance Toolkit □ Windows セキュリティベースライン (Windows security baselines) □ Security Compliance Toolkit (SCT) □ マイクロソフトが策定したセキュリティ設定に関す るベスト プラクティス □ グループポリシー、Microsoft System Center Configuration Manager に適用可能なテンプレート □ 設定一覧ドキュメントも提供 □ 最新バージョン □ Windows 10 Version 2004, Windows Server Version 2004 に対応 (2020/8 時点) □ https://blogs.technet.microsoft.com/secguide/ □ Security Compliance Manager は廃止 57
54. 54. セキュリティ構成フレームワーク (SecCon) □ Windows 堅牢化のためのセキュリティ構成フレームワーク (Security Configuration Framework: SecCon) □ 必要に応じたレベルで組織内の端末 Windows の堅牢化 □ セキュリティ、生産性、そして利便性のバランスを考慮した 5 つのレベル □ Windows セキュリティベースライン = セキュリティ構成フレームワークのレベル 3 58
55. 55. Attack Surface Analyzer □ Attack Surface Analyzer 2.0 □ Windows, Linux, macOS をサポート □ GitHub □ システムの状態を比較 □ ソフトウェアのインストール前後 □ 攻撃対象領域への影響を分析 □ ファイル、レジストリキー、サービス、 ポート 等 59
56. 56. ドメイン管理者の専用端末 (PAW) □ 管理を行うための専用端末 □ 管理者が資格情報を入力しログオンする端末 □ 管理者が RDP 接続などでセッションやツールを実行する端末 □ 特に Tier 0 ドメイン管理権限が利用する端末 □ セキュリティ構成フレームワーク (Level 4, Level 5) による推奨構成 □ 要塞化の対策例 □ 資格情報の盗難に対する保護を有効にする □ クレデンシャルガードを利用する □ Secure Boot /Secure Launchを有効化する □ エクスプロイトガードを有効化する □ ネットワーク分離をする (インターネット接続との分離、DC 接続以外との分離） □ ローカル管理者権限と分離する □ Applocker, Device Guard などを利用してインストールするソフトウェアの制限をする □ Attack Surface Analyzer などを利用して、侵入口の検証をする □ クリーンなインストールイメージであることを確認する □ Bitlocker などを利用してディスク暗号化をする □ USB 接続を禁止する □ マルウェア対策ソフトを実行する 60
57. 57. “乗っ取りアカウント” を軸とした侵入に有効な対策① □ 侵入者は、ドメインデバイスに保存されている資格情報を取得し、侵害を深める □ 各デバイスに、資格情報を残存させない、ローカル管理者でもアクセス不可にすることで、 非常に効果の高い対策となる 61 対策 目的 対策の効果 対策作業量 クレデンシャル ガード • 独立した仮想領域に資格情報を隔離 • LSASS プロセスに対する正当なRPC呼び出 し以外のアクセスを不可能とすることで、 資格情報の窃盗を防ぐ 非常に高い 高
58. 58. Windows 8.1 まで 62 Hypervisor Hardware LSASS User Mode (Ring3) Kernel Mode (Ring0) Memory Process CPU 資格情報 TPM ProcessProcess

59. 59. クレデンシャル ガード 63 Hypervisor Hardware LSASS User Mode (Ring3) Kernel Mode (Ring0) VTL 0VTL 1 Memory LSAISO Process CPU Isolated User Mode 資格情報 TPM コード整合性 (Code Integrity) ProcessProcess Windows 10 Windows Server 2016
60. 60. クレデンシャルガードの資格情報保護 64 TGS Session Key LSAISO
61. 61. リモートデスクトップの資格情報を保護 (Restricted Admin mode) RDP 接続において、接続先へ資格情報渡さず、接続先のローカル管理者権限を利用する 攻撃者はローカル管理者の資格情報しか取得できず攻撃もローカルに限定される (Local Administrators に属している必要がある) 67 資格情報 資格情報 資格情報 資格情報 資格情報 Restricted Admin mode Restricted Admin
62. 62. “乗っ取りアカウント” を軸とした侵入に有効な対策② LSASS プロセスを保護する 資格情報管理する LSASS プロセスへの攻撃を防ぐ 攻撃者は LSASS プロセスへ悪意のあるプラグインを挿入し操作を試みる 68 対策 目的 対策の効果 対策作業量 LSA 保護モードの 有効化 LSASS プロセスに対する悪意のあるプラグイ ンやコードの挿入を防止し、プロセスが保持 している資格情報の窃盗を防ぐ (レジストリで有効化） 高 高
63. 63. “乗っ取りアカウント” を軸とした侵入に有効な対策③ 保存資格情報を減らす 端末が保持している資格情報がなければ攻撃者は盗めない 攻撃の機会を減らすことで防御力を高める 69 対策名 目的 対策の効果 対策作業量 平文パスワード を保存しない LSASSメモリに平文パスワードを保存しないこと で、攻撃者の窃盗を防ぐ 中 低 LM ハッシュを 保存しない LM ハッシュは総当たり攻撃などに対して脆弱で あるため、パスワード解析のリスクを減らす 中 低 ログオフ後の資 格情報消去 ユーザーのログオフ後に LSASS メモリから消去 する 中 低 NTLMプロトコ ルを無効にする NTLM 認証を利用しないことで、NTLM ハッシュ を悪用する攻撃を防ぐ 低 高 ARSO 無効化 Windows 8.1 以降の Automatic Restart Sign-On (ARSO) による資格情報保持をしない 中 低
64. 64. 参考：保存される資格情報一覧 70 平文パスワード (可逆暗号による保存) NT (NTLM) ハッシュ LM ハッシュ TGT,TGS Keys キャッシュ ログオン 検証用 認証方式 ダイジェスト NTLM LM ケルベロス Security Accounts Manager データベース (ローカル) - ○ △1 - - Active Directory データベース （ドメイン) - ○ △1 - - The Credential Manager (CredMan) ストア △2 - - - - Local Security Authority Subsystem (LSASS) プロセスメモリ △3 ○ ○ ○ - ディスク (LSA シークレット) サービスアカウント、 スケジュールタスクなど コンピューター アカウント - - - レジストリ (HKLMSecurity) - - - - ○ 1. Windows Vista/Windows Server 2008 以降は既定で保存されていない。グループポリシーで有効化されている場合は保存される 2. ユーザーがパスワードを保存することを選択した場合のみ 3. セキュリティアドバイザリ 2871997, あるいは Windows 8.1/ Windows Server 2012 R2 以降 は無効
65. 65. 71

66. 66. イベント監視と対応 □ ログ監視だけではADの侵害を効率的に対応は困難 □ 特定のイベントをモニタすればよいわけではない。流れや関係性から見ることが重要 □ 効率の良いイベント監視と対応が必要 □ 攻撃を検知すること + 後から調査をする場合に必要 □ 優先付け、インシデント基準の整備 □ (事例) イベントを取得しているしSOCも用意しているが、検出できていないし迅速に対応がで きない。 □ 多くのイベントを取得しているが、必要なイベントを拾えていない。 □ 調査に必要なログが取得できていない © Copyright Microsoft Corporation. All rights reserved. 72
67. 67. 必要とされる監視 Greater visibility アラート 疑わしい アクティビティ © Copyright Microsoft Corporation. All rights reserved. 73
68. 68. 疑わしいアクティビティ © Copyright Microsoft Corporation. All rights reserved. 74
69. 69. インシデント対応と復旧 □ 運用、ビジネスへの影響を最小限にする必要がある □ Active Directory は完全には停止できない前提で、対応策と復旧案をを検討しておく □ 例：KRBTGT アカウントのリセット手順および影響、特権アカウントのリセット、端末のリストア □ 繰り返し被害を受けないための対応 □ 侵入された端末、侵入口、攻撃糸口をすべて除去できていない場合、 再度甚大な被害を受ける可能性が高い □ 「侵害前提」での対応と復旧が必要となる □ 永続的にADの侵害は発生することを前提に、長期的に最小の運用ができるように □ 構成の健全化、推奨構成での運用を推奨 □ 迅速で効率の良い対応をするために調査や特定に必要なログ、優先付けられた調査フレームワークが必要 75© Copyright Microsoft Corporation. All rights reserved.
70. 70. 76 □ オンプレミスADの脅威をオンプレで分析 □ AD 上の ID/認証情報を利用した不正な アクティ ビティや振舞いを検出対応方法の提示 □ SIEM との統合 ATA デバイス、サーバー SIEM Active Directory Azure Advanced Threat Protection (Azure ATP) Advanced Threat Analytics (ATA) 専用のテナ ント Azure ATP 管理者 管理 送信 Microsoft Threat Intelligence 活用 SIE M ATP セン サー 送信 DC © Copyright Microsoft Corporation. All rights reserved.
71. 71. ドメインコントローラからデータの取得を示すアラート © Copyright Microsoft Corporation. All rights reserved. 79
72. 72. © Copyright Microsoft Corporation. All rights reserved. 82 □ 概要レポート □ アラートと正常性の問題の概要 □ 機密性の高いグループに対する変更 □ Active Directory 内の機密性の高いグループに対するすべての変更 □ クリアテキストでのパスワードの流出 □ ユーザーパスワードをクリアテキストで 流出させたすべての LDAP 認証 □ 重要なアカウントに対する横移動パス □ 横方向の移動で危害を受けるリスクのある重要なアカウント (過去60日分の情報を表示) 指定された管理者に定期的にレポートを提供
73. 73. © Copyright Microsoft Corporation. All rights reserved. 83

74. 74. まとめ • 標的型攻撃、Active Directory 侵害の事例は増加傾向にある • オンプレミス中心の組織も侵害に遭っている • 「IT 障害」のつもりが「セキュリティ インシデント」であるケース • Active Directory 侵害の特徴を理解し対策することが重要 1. 組織内での“乗っ取りアカウント” を中心として拡大する □ ネットワーク、マルウェア観点、強いパスワード、アルゴリズムの対策だけでは対策が不十分 □ 組織内の侵入者を前提とした ID 保護が重要 2. 複雑なAD環境に起因する □ AD環境の複雑化を避け、環境を把握することが予防、検出、対応に重要 3. 侵入者の検出が困難 □ 異常系の監視、イベントログ監視だけでは対応できない、ふるまい検出が必要 4. 復旧が困難 □ 必要な復旧、事後対応ができていない場合、繰り返し被害に遭う • パンデミック後のゼロトラストを基調としたセキュリティ能勢を保つことが重要 • 推奨構成、ID管理（特権管理）、デバイス管理 84© Copyright Microsoft Corporation. All rights reserved.
75. 75. © Copyright Microsoft Corporation. All rights reserved.
76. 76. © Copyright Microsoft Corporation. All rights reserved. 86
77. 77. 参考資料 □ Active Directory のセキュリティ保護に関するベスト プラクティス □ https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/plan/security-best-practices/best- practices-for-securing-active-directory □ 資格情報の保護と管理 □ https://docs.microsoft.com/ja-jp/windows-server/security/credentials-protection-and-management/credentials-protection-and-management © Copyright Microsoft Corporation. All rights reserved. 87