תקיפות מסוג Password Spray כנגד שירות 365 של חברת מיקרוסופט

31/03/2026
י"ג ניסן תשפ"ו

[תקציר]

1. לאחרונה דווח למערך הסייבר הלאומי על עליה ניכרת בניסיונות לביצוע תקיפות מסוג Password Spray כנגד ארגונים ישראליים המשתמשים בשירות הענן 365 של חברת מיקרוסופט.
2. מטרת מסמך זה, הכרת שיטת תקיפה זו ודרכים להתמודדות עימה.

[פעולות מידיות לביצוע]

- הפעילו הזדהות חזקה (MFA) עבור כלל המשתמשים בשירות, ובפרט המנהלנים ובעלי הרשאות גבוהות.
- מומלץ מאד שאמצעי ה-MFA בשימוש הארגון, לכל הפחות עבור מנהלנים ובעלי הרשאות גבוהות, יהיה מסוג העמיד לתקיפות דיוג (Phishing Resistant MFA).
- וודאו כי נוטרלו כל הממשקים העושים שימוש בפרוטוקולי זיהוי ישנים ובלתי מוצפנים כגון IMAP, POP3 וכד'.

[פרטים]

1. Password Spray היא שיטת תקיפה שבה תוקף מנסה לנחש נתוני הזדהות של משתמשים באמצעות מספר מועט של סיסמאות, בדרך כלל סיסמאות ברירת מחדל או סיסמאות המוכרות כפופולריות, למרות היותן חלשות וקלות לניחוש (כדוגמת Password123, MyPassword, qwerty123456 וכד').
2. בשונה משיטות תקיפה כגון Brute Force, בשיטה זו התוקף מנסה **מספר קטן של ניסיונות להזדהות**, על מנת למנוע נעילת החשבון לניסיונות הזדהות נוספים, ורישום מספר רב של ניסיונות גישה בלוג, אירוע אשר עלול להפנות תשומת לב הארגון לתקיפה בעת התרחשותה.
3. התקיפה עלולה להתפרס לאורך זמן רב, וזאת על מנת שספירת ניסיונות הזדהות שגויים תתאפס בין ניסיונות חוזרים לגישה לחשבון מסוים.

[דרכי התמודדות]

1. מומלץ להפעיל Microsoft Entra Password Protection כדי לחסום סיסמאות חלשות, נפוצות או בהתאמה ספציפית לדרישות לארגון, הן בענן והן ב-Active Directory המקומי (Hybrid). תקיפה מסוג Password Spray מתבססת על שימוש בסיסמאות נפוצות. חסימה שלהן מצמצמת משמעותית את אחוזי ההצלחה של התקיפה.
2. הפעלת Multi Factor Authentication לכל המשתמשים (בדגש על בעלי גישה מרחוק, מנהלנים, בעלי הרשאות גבוהות או חשבונות רגישים כגון ההנהלה הבכירה). גם אם ינוחשו נתוני הזדהות בהצלחה, התוקף יצטרך להתמודד עם שיטת ההזדהות הנוספת.

3. מומלץ לוודא שמנגנון ה-Smart Lockout ב-Microsoft Entra ID (Cloud) מופעל ומכויל בהתאם לצרכי הארגון. Smart Lockout מזהה דפוסי ניסיונות כושלים (כולל לפי מקור גיאוגרפי) ומונע נעילה גורפת או המשך התקיפה.
4. מומלץ מאד לבטל ולנטרל שימוש בפרוטוקולים ושיטות אימות ישנות כגון Basic Auth, POP, IMAP, SMTP AUTH, וכד', מאחר ושיטות הזדהות אלו לרוב אינן מוצפנות, ופגיעות לשיטות תקיפה מודרניות.
5. אם שירות זה נמצא בשימוש הארגון, מומלץ להשתמש ב Microsoft Defender XDR לזיהוי, חקירה וסיווג התראות עבור תקיפת Password Spray. השירות מאפשר זיהוי רוחבי (cross tenant / cross user) של ניסיונות התחברות חשודים והפעלת תגובה מהירה.
6. מומלץ לאמץ את Incident Response Playbook של Microsoft לתרחיש Password Spray כבסיס לנוהל התגובה הארגוני לאירוע. ה-Playbook כולל תהליך סדור של איסוף לוגים, חקירה, הכלה (Containment) ושיקום (Recovery).
7. מומלץ להקשיח ADFS ו-Federation Endpoints (On Prem), ולהגדיר הגנות ייעודיות נגד Password Attacks. שירות זה חשוף לאינטרנט ולכן עלול להוות יעד מועדף לתקיפה.
8. מומלץ מאד לוודא כי מוגדרים ונשמרים לוגים מלאים עבור:
    1. Entra ID Sign in Logs
    2. AD / ADFS Security Logs
9. יש לוודא הזרמת הלוגים למערכת ה-SIEM הארגונית. ללא לוגים וניתוחם ארגון מותקף יתקשה מאד לזהות ולהגיב לתקיפה.

[מקורות]

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad
2. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-deploy
3. https://www.microsoft.com/en-us/security/blog/2020/04/23/protecting-organization-password-spray-attacks/
4. https://learn.microsoft.com/en-us/defender-xdr/alert-classification-password-spray-attack
5. https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-password-spray
6. https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/ad-fs-password-protection