קמפיין דיוג ממוקד פעיל בישראל

03/05/2026
ט"ז אייר תשפ"ו

[תקציר]

- לאחרונה דווח למערך הסייבר הלאומי על אירוע בו נפרצה תיבת דוא"ל של משתמש בארגון מסוים, והתוקף ניצל את גישתו לתיבה לצורך הפצת מתווה דיוג למספר רב של תיבות דוא"ל בארגונים שונים.

[פרטים]

- מתווה התקיפה מוכר כ-Device Code Phishing.
- התוקף מבקש ממיקרוסופט "קוד התחברות למכשיר חדש".
- התוקף שולח לקורבן מייל/הודעה מזויפת (כפי שרואים בצילום המסך), שטוענת שנשלח אליו מסמך להתייחסותו.
- כדי לצפות במסמך, הנתקף מתבקש להיכנס לקישור הרשמי של מיקרוסופט ולהזין את הקוד שמופיע בהודעה.
- הזנת הקוד באתר של מיקרוסופט ואישורו נותן לתוקף יכולת להיכנס לחשבון של הנתקף, באמצעות ה-Token שהתקבל ממיקרוסופט. אין צורך בסיסמה.
- ראו צילומי מסך להלן.
- נכון למועד פרסום התרעה זו, ה-URL המופיעים בקובץ המזהים מתויגים כזדוניים ב-Google Safe Browsing וב-Cloudflare, בעקבות פעילות של מערך הסייבר הלאומי.

פעולות מידיות לביצוע:

- להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל מערכות האבטחה הרלוונטיות.
- תשומת לב מוגברת, הן של גורמי ההגנה בסייבר והן של העובדים, למתווי דיוג ממוקדים אפשריים.
- העברת כלל עובדי הארגון, ובפרט מנהלנים, ועובדים הניגשים למערכות מרשת האינטרנט, להזדהות חזקה העמידה בפני דיוג (Phishing Resistant MFA).

[דרכי התמודדות]

- להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.
- נבקש לעדכן את מערך הסייבר הלאומי בכל מקרה של זיהוי אחד או יותר ממזהים אלו במערכותיכם.
- מומלץ לפעול להעלאת מודעות עובדים לגבי הסכנות של הנדסה חברתית, וביצוע תרגילי דיוג ממוקד פנימיים על ידי הארגון, כדי להדגים התקפות מסוג זה לעובדים, על מנת לחדד מודעותם לנושא.
- העברת כלל עובדי הארגון, ובפרט **מנהלנים**, ועובדים הניגשים למערכות מרשת האינטרנט, להזדהות חזקה העמידה בפני דיוג (Phishing Resistant MFA). ראו פרטים נוספים בקישורים
  https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
  https://learn.microsoft.com/en-us/security/zero-trust/sfi/phishing-resistant-mfa
- וידוא כי כלל מערכות סינון הדוא"ל הארגוניות מוגדרות באופן המיטבי להתמודדות עם סיכון של מתקפות דיוג.
- וידוא כי כלל מערכות הארגון, ובפרט המערכות המוזכרות בסעיף הקודם, וכן שרתי הדוא"ל הארגוני ומערכות הקצה של המשתמשים, מעודכנות באופן עיתי עם עדכוני האבטחה העדכניים ביותר של היצרן.

<u>צילומי מסך</u>